

NTU-2V(C)

NTU-2W

NTU-RG-1402G-W

Operation Manual, Version 3.0 (21 May 2018)

Optical Network Terminals

IP address: <http://192.168.1.1>

User name: user

Password: user

Document version	Suitable firmware version	Issue date	Changes
Version 3.0	3.25.5.425 3.25.5.426 3.25.5.427	21 May 2018	Third issue
Version 2.0	3.25.4.917 3.25.4.918 3.25.4.919	29 November 2017	Second issue
Version 1.0	3.25.2.1593	17 April 2017	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.

1 INTRODUCTION	5
2 PRODUCT DESCRIPTION	6
2.1 Purpose	6
2.2 Models.....	6
2.3 Device Specification	7
2.3.1 NTU-2V(C).....	7
2.3.2 NTU-2W	8
2.3.3 NTU-RG.....	10
2.4 Key Specifications.....	11
2.5 Design.....	13
2.5.1 NTU-2V	13
2.5.2 NTU-2VC.....	15
2.5.3 NTU-2W	16
2.5.4 NTU-RG-1402G-W	17
2.6 Light Indication.....	19
2.6.1 NTU-2V	19
2.6.2 NTU-2VC.....	19
2.6.3 NTU-2W	20
2.6.4 NTU -RG-1402G-W	21
2.6.5 Reboot and Reset to Factory Settings	21
2.7 Delivery Package	22
3 DEVICE ARCHITECTURE.....	23
3.1 NTU-2V(C) Architecture	23
3.2 NTU-2W Architecture.....	26
3.3 NTU-RG-1402G-W Architecture	29
4 NTU-RG-1402G-W CONFIGURATION VIA WEB INTERFACE. USER ACCESS	33
4.1 The “Device Info” Menu. Device Information.....	34
4.1.1 The “Summary” Submenu. Device General Information	34
4.1.2 The “WAN” Submenu. The Status of Services.....	34
4.1.2.1. The “General” Submenu. General information	34
4.1.2.2. The “Detail” Submenu. Detailed Information.....	35
4.1.3 The “LAN” Submenu. LAN Ports Monitoring. Wi-Fi Interface Status Monitoring.....	35
4.1.4 The “Statistics” Submenu. Traffic Flow Information for Ports of the Device.....	36
4.1.5 The “Route” Submenu. The Routing Table	37
4.1.6 The “ARP” Submenu. ARP Protocol Cache	38
4.1.7 The “DHCP” Submenu. Active DHCP Leases.....	38
4.1.8 The “Wireless Station” Submenu. Connected Wireless Devices.....	39
4.1.9 The Wireless Monitor Submenu. Detected Wi-Fi Networks.....	39
4.1.10 The “Voice” submenu. Monitoring the phone port states.....	40
4.2 The “Advanced Setup” Menu. Advanced Settings	41
4.2.1 The “LAN” Submenu. Configuration of Main Parameters.....	41
4.2.2 The “PPPoE” menu. PPP Settings	42
4.2.3 The “NAT” Submenu. NAT Settings.....	42
4.2.3.1. The “Virtual Servers” Submenu. Settings of Virtual Servers.....	42
4.2.3.2. The “Port Triggering” Submenu. Port Triggering Configuration.....	44
4.2.3.3. The “DMZ Host” Submenu. DMZ Settings	45
4.2.4 The “Security” Submenu. Security Settings	45
4.2.4.1. The “IP Filtering” Submenu. Addresses Filtering Configuration	45
4.2.4.2. The “MAC Filtering” Submenu. Filtering Settings for MAC Addresses	48
4.2.5 The “Parental Control” Submenu. Parental Control—Restrictions Configuration	49
4.2.5.1. The “Time Restriction” Submenu. Configuration of Session Time Restriction	49
4.2.5.2. The “Url Filter” Submenu. Internet Access Restriction Settings.....	50

4.2.6 The “Dynamic DNS” menu. The Dynamic DNS settings	50
4.2.7 The “Print Server” menu. Print Server Configuration	53
4.2.8 The “UPnP” menu. Automatic setup of Network Devices	53
4.3 The “Voice” menu. SIP settings	54
4.3.1 The “SIP Basic Setting” submenu. Common SIP settings	54
4.3.2 The “SIP Advanced Settings” submenu	55
4.4 The “Wireless” Menu. Wi-Fi Network Setup.....	56
4.4.1 The “Basic” submenu. General information	56
4.4.2 The “Security” Submenu. Security Settings	57
4.4.3 The “MAC Filter” Submenu. MAC Address Filtering Settings	60
4.4.4 The “Wireless Bridge” Submenu. Configuration of Wireless Connection in the Bridge Mode.....	61
4.4.5 The “Advanced” Submenu. Advanced Settings.....	62
4.5 The “Storage Service” menu. File Storage Service	64
4.5.1 The “Storage Device Info” submenu. Connected USB Device Info	64
4.5.2 The “User Accounts” submenu. Configuration of Samba users.....	64
4.6 The “Management” menu. Device Management	65
4.6.1 The “Settings” submenu. Settings.....	65
4.6.1.1. The “Backup” submenu. Backup.....	65
4.6.1.2. The “Update” submenu. Configuration Update	65
4.6.1.3. The “Restore Default” Submenu. Restore Default Settings.....	65
4.6.2 The “PON Password” Submenu. Changing PON Network Password	66
4.6.3 The “Internet Time” Submenu. System Time settings	66
4.6.4 The “Ping” Submenu. Checking the Availability of the Network Devices	67
4.6.5 The “Passwords” Submenu. Access Control Settings (password settings)	67
4.6.6 The “System Log” Submenu. Display and Configuration of the System Log.....	68
4.6.6.1. The “Configuration” Submenu. System Log Configuration.....	68
4.6.6.2. The “View” Submenu. System Log Display	69
4.6.7 The “Update Software” Submenu. Software Update	69
4.6.8 The “Reboot” Submenu. Device Reboot	69
APPENDIX A. POSSIBLE PROBLEMS AND THEIR SOLUTIONS	70
APPENDIX B. ADDITIONAL SERVICE	71
NTU-RG ACCEPTANCE CERTIFICATE AND WARRANTY	73
NTU-2V ACCEPTANCE CERTIFICATE AND WARRANTY.....	74
NTU-2VC ACCEPTANCE CERTIFICATE AND WARRANTY.....	75
NTU-2W ACCEPTANCE CERTIFICATE AND WARRANTY	76

1 INTRODUCTION

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

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

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

- NTU-2V(C) with two Ethernet user network interfaces (UNI): **1 Ethernet 10/100 Base-T port, 1 Ethernet 10/100/1000 Base-T port and 1 FXS port**, and also equipped with the integrated **Triplexer¹** transceiver depending on the device model;
- NTU-2W with two Ethernet user network interfaces (UNI): **1 Ethernet 10/100 Base-T port and 1 Ethernet 10/100/1000 Base-T port**;
- NTU-RG-1402G-W, which are designed to support four UNI: **10/100/1000Base-T, FXS, Wi-Fi, and USB**.

This operation manual describes intended use, main specifications, configuration, monitoring, and firmware update for optical terminals *NTU-2V(C)*, *NTU-2W*, *NTU-RG-1402G-W*.

¹ Only for NTU-2VC

2 PRODUCT DESCRIPTION

2.1 Purpose

NTU-2V(C), *NTU-2W*, *NTU-RG-1402G-W* GPON ONT (Gigabit Passive Optical Network) devices represent high-performance user terminals designed to establish a connection with upstream passive optical network equipment and to provide broadband access services to the end user. GPON connection is established through the PON interface, while Ethernet interfaces are used for connection of terminal equipment.

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

An integrated router allows local network equipment to be connected to a broadband access network. Terminals use firewalls to secure network computers from DoS and virus attacks, provide packet filtering for access control based on ports and source/destination MAC/IP addresses. Users can configure home or office websites by adding one of the LAN-ports to the DMZ. Parental Control feature filters out websites with unwanted content, block domains, and defines the Internet usage schedule. Virtual private network (VPN) provides mobile users and branch offices with a protected communication channel for connection to a corporate network.

FXS ports enable IP telephony and provide 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.

NTU-2VC is equipped with the integrated *Triplexer* transceiver that enables simultaneous data transmission and provisioning of the CaTV services.

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

NTU-2W and *NTU-RG-1402G-W* subscriber routers allow connection of Wi-Fi clients via IEEE 802.11b/g/n standard.

2.2 Models

NTU-2V(C), *NTU-2W* and *NTU-RG-1402G-W* devices are designed to support various interfaces and features – see Table 1.

Table 1 – Models

Model name	WAN	LAN	FXS	Wi-Fi 802.11 b/g/n	USB	Triplexer
<i>NTU-2V</i>	1xGPON	1x1Gigabit 1x100Megabit	1	-	-	-
<i>NTU-2VC</i>	1xGPON	1x1Gigabit 1x100Megabit	1	-	-	+
<i>NTU-2W</i>	1xGPON	1x1Gigabit 1x100Megabit	-	+	1	-
<i>NTU-RG-1402G-W</i>	1xGPON	4x1Gigabit	2	+	2	-

2.3 Device Specification

2.3.1 NTU-2V(C)

Device is equipped with the following interfaces:

- 1 x RJ-45¹/RJ-11² for connection of analogue phones;
- 1 PON SC/APC port for connection to operator's network.
- Ethernet RJ-45 LAN ports for connection of network devices:
 - 1 RJ-45 10/100 Base-T port;
 - 1 RJ-45 10/100/1000Base-T port;
- 1 RF port to connect TV².

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

The device supports the following functions:

- *Network functions:*
 - bridge or router mode;
 - PPPoE (PAP, CHAP, MSCHAP authentication);
 - IPoE (DHCP client and static);
 - DHCP server on LAN side;
 - Multicast traffic transmission;
 - DNS (Domain Name System);
 - DynDNS (Dynamic DNS);
 - UPNP (Universal Plug and Play);
 - IPSec;
 - NAT (Network Address Translation);
 - Firewall;
 - NTP (Network Time Protocol);
 - QoS;
 - IGMP snooping;
 - IGMP proxy;
 - Parental Control;
 - VLAN according to IEEE 802.1Q;
 - TR-069.
- *VoIP*
 - SIP
 - audio codecs: G.729 (A), G.711(A/U), G.723.1;
 - ToS for RTP packets;
 - ToS for SIP packets;
 - echo cancellation (G.164 and G.165 guidelines);
 - silence detector (VAD);
 - comfortable noise generator;
 - DTMF signal detection and generation
 - DTMF transmission (INBAND, RFC2833, SIP INFO)
 - Fax transmission: upspeed/pass-through. G.711, T.38
- *Value Added Services (VAS):*
 - Call Hold;

¹ Only for NTU-2V

² Only for NTU-2VC

- Call Transfer;
 - Call Waiting;
 - Forward unconditionally;
 - Forward on 'no answer';
 - Forward on 'busy';
 - Caller ID Display for ETSI FSK;
 - Anonymous calling;
 - Warmline;
 - Flexible dial plan;
 - Voice mail notifications (MWI);
 - Anonymous call blocking;
 - Call Barring;
 - DND (Do not disturb).
- Firmware updates via web interface, TR-069, OMCI.
 - Remote monitoring, configuration, and setup:
 - TR-069;
 - Web interface;
 - OMCI.

Figure 1 shows a diagram of the NTU equipment connection.

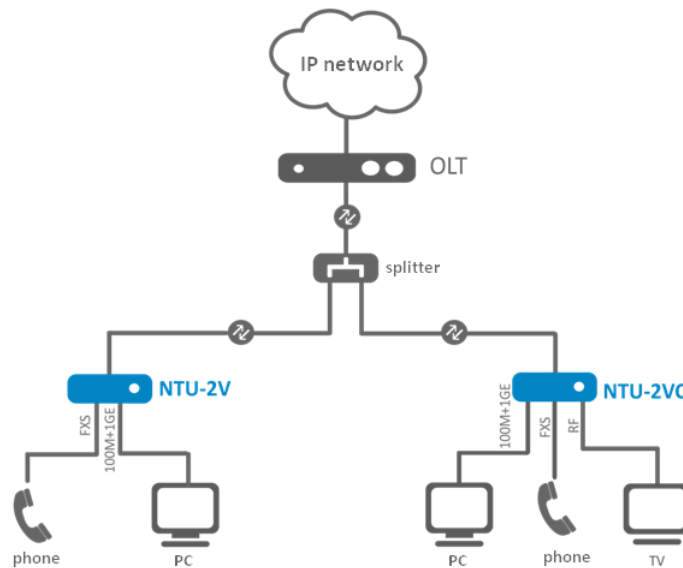


Figure 1 – Connection of NTU-2VC

2.3.2 NTU-2W

The device has the following interfaces:

- 1 PON SC/APC port for connection to operator's network.
- Ethernet RJ-45 LAN ports for connection of network devices:
 - 1 RJ-45 10/100 Base-T port;
 - 1 RJ-45 10/100/1000Base-T port;
- 1 Wi-Fi transmitter/receiver 802.11b/g/n;
- 1 USB 2.0 port for external USB or HDD storages.

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

The device supports the following functions:

- Network functions:
 - TR-069;
 - “Bridge” and “Router” (including virtual ones) operation modes;
 - PPPoE (auto, PAP, MSCHAP and CHAP authentication);
 - IPoE (DHCP client and static);
 - DHCP server on LAN side;
 - Multicast traffic transmission via Wi-Fi;
 - DNS (Domain Name System);
 - DynDNS (Dynamic DNS);
 - UPNP (Universal Plug and Play);
 - NAT (Network Address Translation);
 - NTP (Network Time Protocol);
 - QoS;
 - IGMP Snooping;
 - IGMP Proxy;
 - UPNP, SMB, FTP, DLNA, Print Server;
 - VLAN according to IEEE 802.1Q;
 - Parental Control.

- Wi-Fi:
 - 802.11b/g/n standards.

- Firmware updates via web interface, TR-069, OMCI.

- Remote monitoring, configuration, and setup:
 - TR-069;
 - Web interface;
 - OMCI.

Figure 2 shows a diagram of the NTU-2W equipment application diagram.

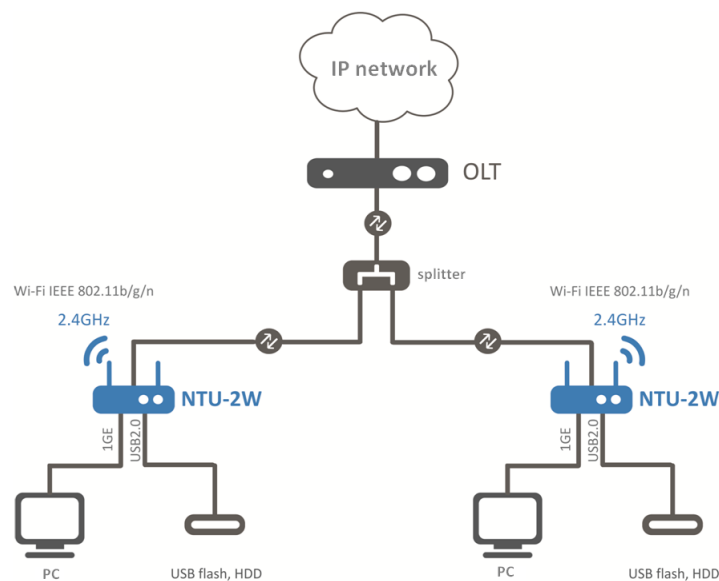


Figure 2 – Application diagram of NTU-2W

2.3.3 NTU-RG

The device has the following interfaces:

- 2 RJ-11 ports for connection of analogue phones
- 1 PON SC/APC port for connection to operator's network.
- 4 Ethernet LAN RJ-45 10/100/1000Base-T ports for connection of network devices
- 1 Wi-Fi transmitter/receiver 802.11b/g/n;
- 2 USB 2.0 ports for external USB or HDD storages.

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

The device supports the following functions:

• *Network functions:*

- TR-069;
- “Bridge” and “Router” (including virtual ones) operation modes;
- PPPoE (auto, PAP, MSCHAP and CHAP authentication);
- IPoE (DHCP client and static);
- DHCP server on LAN side;
- Multicast traffic transmission via Wi-Fi;
- DNS (Domain Name System);
- DynDNS (Dynamic DNS);
- UPNP (Universal Plug and Play);
- NAT (Network Address Translation);
- NTP (Network Time Protocol);
- QoS;
- IGMP Snooping;
- IGMP Proxy;
- UPNP, SMB, FTP, DLNA, Print Server;
- VLAN according to IEEE 802.1Q;
- Parental Control;
- Storage service.

• *Wi-Fi:*

- 802.11b/g/n standards.

• *VoIP*

- SIP
- Audio codecs: G.729 (A), G.711 (A/U), G.723.1;
- ToS for RTP packets;
- ToS for SIP packets;
- Echo cancellation (G.164 and G.165 guidelines);
- Silence detector (VAD);
- Comfortable noise generator;
- DTMF signal detection and generation
- DTMF transmission (INBAND, RFC2833, SIP INFO)
- Fax transmission: upspeed/pass-through. G.711, T.38

• *Value Added Services (VAS):*

- Call Hold;
- Call Transfer;
- Call Waiting;
- Forward unconditionally;

- Forward on 'no answer';
 - Forward on 'busy';
 - Caller ID Display for ETSI FSK;
 - Anonymous calling;
 - Warmline;
 - Flexible dial plan;
 - Voice mail notifications (MWI);
 - Anonymous call blocking;
 - Call Barring;
 - DND (Do not disturb).
- Firmware updates via web interface, TR-069, OMCI.
 - Remote monitoring, configuration, and setup:
 - TR-069;
 - Web interface;
 - OMCI.

Figure 3 shows a diagram of the NTU equipment connection.

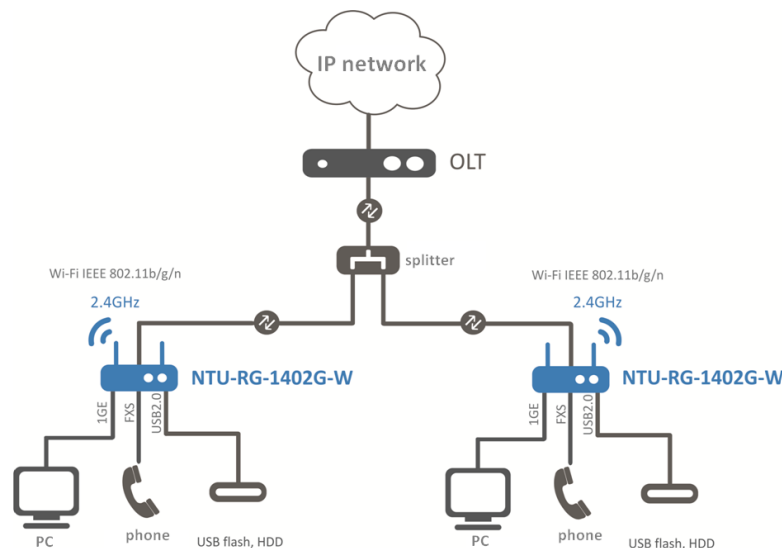


Figure 3 – Connection of NTU-RG-1402G-W

2.4 Key Specifications

The Table 2 provides main specifications of the terminal.

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	NTU-2V(C)	2
----------------------	-----------	---

	NTU-2W	2
	NTU-RG-1402G-W	4
Socket	RJ-45	
Data transfer rate, Mbps	Autodetection, 10/100/1000 Mbps, Duplex/half-duplex	
Standards	IEEE 802.3i 10Base-T Ethernet IEEE 802.3u 100Base-TX Fast Ethernet IEEE 802.3ab 1000Base-T Gigabit Ethernet IEEE 802.3x Flow Control IEEE 802.3 NWay auto-negotiation	

Parameters of PON Interface

Number of PON interfaces	1	
Standards	ITU-T G.984.x Gigabit-capable passive optical networks (GPON) ITU-T G.988 ONU management and control interface (OMCI) specification IEEE 802.1Q Tagged VLAN IEEE 802.1p Priority Queues IEEE 802.1D Spanning Tree Protocol	
Connector type	SC/APC Complies with ITU-T G.984.2	
Transmission medium	Fiber optical cable SMF - 9/125, G.652	
Splitting ratio	up to 1:128	
Maximum range of coverage	20 km	
Transmitter:	1310nm	
Upstream connection speed	1244 Mbps	
Transmitter power	from +0.5 to +5 dBm	
Optical spectrum width (RMS)	1 nm	
Receiver:	1490nm	
Downstream connection speed	2488 Mbps	
Receiver sensitivity	from -8 to -28 dBm	

Parameters of subscriber analogue ports

Port number	NTU-2V(C)	1
	NTU-2W	0
	NTU-RG-1402G-W	2
Loop resistance	up to 2 kΩ	
Dialling	Pulse/frequency (DTMF)	
Caller ID display	Yes	

Wi-Fi interface parameters

Model	NTU-2W, NTU-RG-1402G-W	
Standard	IEEE 802.11b/g/n	
Frequency range	2.400 ~ 2.497 GHz	
Modulation	PSK/CCK, DQPSK, DBPSK, OFDM	
Data transfer rate, Mbps	802.11b: 11, 5.5, 2, 1 802.11g: 54, 48, 36, 24, 18,12, 9, 6 802.11n 20MHz BW: 130, 117, 104, 78, 52, 39, 26, 13 802.11n 40MHz BW: 270, 243, 216, 162, 108, 81, 54, 27	
Maximum transmitter output power	802.11b: 17dBm +/-1.5dBm 802.11g: 15dBm +/-1.5dBm 802.11n: 14.75dBm +/-1.5dBm	
MAC protocol	CSMA/CA model of ACK 32 MAC	
Security	64/128 bit WEP encryption;	

	WPA, WPA2 802.1x AES & TKIP	
Operating system support	Windows XP 32/64, Windows Vista 32/64, Windows 2000, Windows 7 32/64, Linux, VxWorks	
Number of antennae	NTU-RG-1402G-W	2
	NTU-2W	2
Antenna gain	5 dBi	
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	By password

General Parameters

Power Supply	12V DC /220 AC power adapter	
Power consumption	NTU-2V(C)	up to 5 W
	NTU-2W	up to 10 W
	NTU-RG-1402G-W	up to 15 W
Operating temperature range	from +5 to +40°C	
Relative humidity	up to 80 %	
Dimensions	NTU-2V	122×96×24 mm
	NTU-2VC	160×120×24 mm
	NTU-2W	147×110×24 mm
	NTU-RG-1402G-W	187×120×32 mm
Weight	NTU-2V	0.250 kg
	NTU-2VC	0.265 kg
	NTU-2W	0.250 kg
	NTU-RG-1402G-W	0.3 kg

2.5 Design

2.5.1 NTU-2V

NTU-2V devices are designed as 122×96×32 mm desktop device in a plastic housing.

Figure 4 shows the NTU-2V rear panel layout.

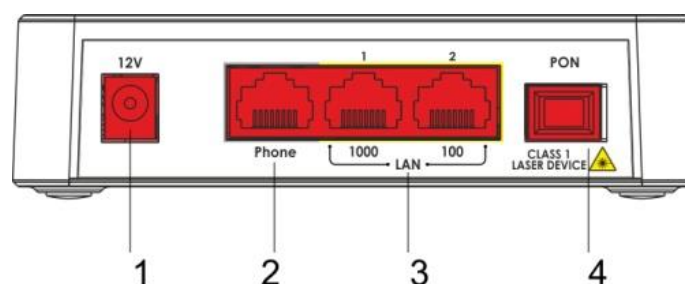


Figure 4 – NTU-2V Rear Panel

The connectors and controls located on the rear panel of NTU-2V are shown in the Table 3.

Table 3 – Description of the LEDs and Controls Located on the Rear Panel

Rear Panel Element		Description
1	12V	Power adapter connector

2	Phone	RJ-11 connector for analogue phone connection
3	LAN 1000	RJ-45 10/100/1000Base-T port for connection of network devices
	LAN 100	RJ-45 100Base-TX port for connection of network devices
4	PON	SC port (socket) for connection to PON with GPON interface

Figure 5 shows NTU-2V side and top panels.

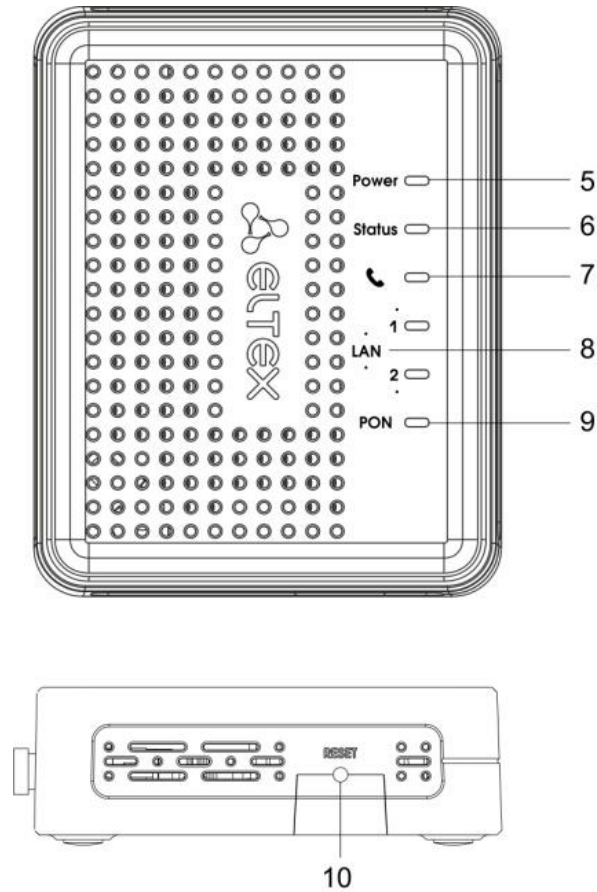


Figure 5 – NTU-2V Top Panel

The controls and LED indicators located on the NTU-2V side and top panels are shown in Table 4.

Table 4 – Description of the LEDs and Controls Located on the Rear Panel

Panel Element		Description
5	Power	Device power and activity status indicator
6	Status	Device authentication indicator
7		Analogue phone indicator
8	LAN	Ethernet ports activity indicators
9	PON	Optical interface indicator
10	Reset	A functional key that reboots the device and resets it to factory settings

2.5.2 NTU-2VC

NTU-2VC devices are designed as 160×120×40 mm desktop device in a plastic housing.

Figure 6 shows the NTU-2VC rear panel layout.

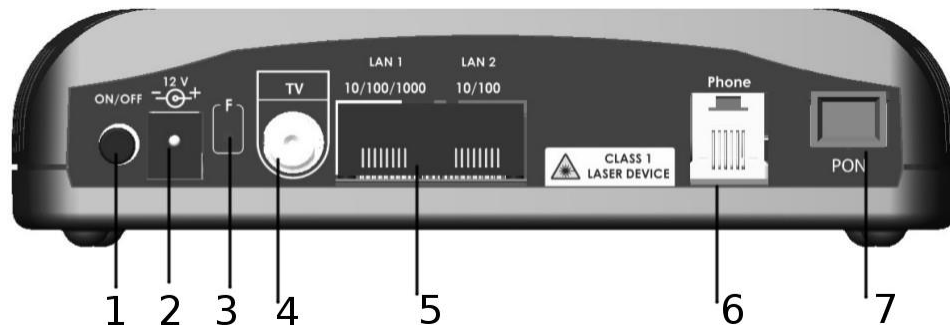


Figure 6 – NTU-2VC Rear Panel layout

Table 5 – Description of the LEDs and controls located on the rear panel

No	Rear Panel Element	Description
1	<i>On/Off</i>	Power supply button
2	<i>12V</i>	Power adapter connector
3	<i>F</i>	A functional key that reboots the device and resets it to factory settings
4	<i>RF port</i>	TV set connector for CaTV
5	<i>LAN 10/100/1000 1</i> <i>LAN 10/100 2</i>	2 RJ-45 ports for connection to network devices
6	<i>Phone</i>	RJ-11 port to connect network devices
7	<i>PON</i>	SC port (socket) for PON with GPON interface

Figure 7 shows a NTU-2VC front panel.

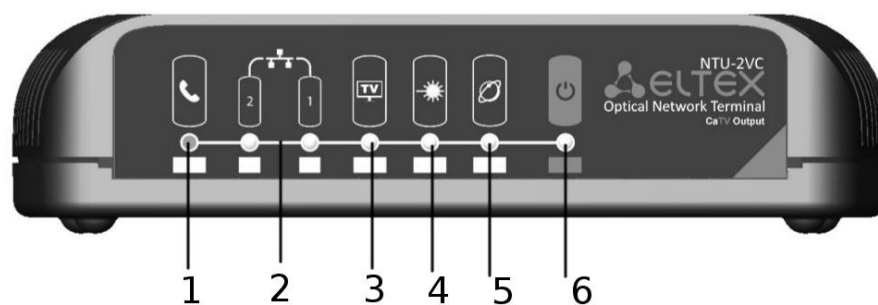


Figure 7 – NTU-2VC Top Panel

The controls and LED indicators located on the NTU-2VC front panel are shown in the Table 6.

Table 6 – Description of front panel LED indicators

Panel Element	Description
1	Analogue phone indicator
2	Ethernet ports activity indicators
3	CaTV signal availability indicator
4	Optical interface indicator

5		Device authentication indicator
6		Device power and activity status indicator

2.5.3 NTU-2W

NTU-2W devices are designed as 147×110×24 mm desktop device in a plastic housing.

Figure 8 shows the NTU-2W rear panel layout.

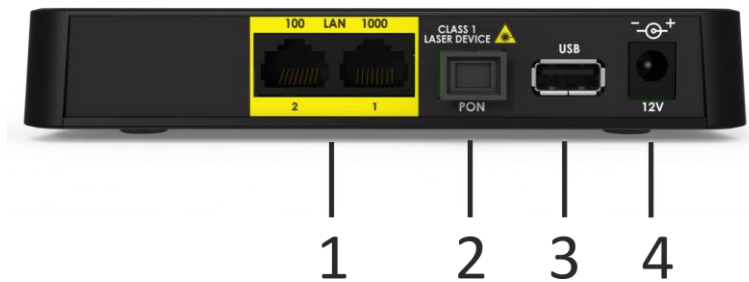


Figure 8 – NTU-2W Rear Panel

The connectors and controls located on the rear panel of NTU-2W are shown in the Table 7.

Table 7 – Description of the LEDs and Controls Located on the Rear Panel

Rear Panel Element		Description
1	LAN 100	RJ-45 100Base-TX port for connection of network devices
	LAN 1000	RJ-45 10/100/1000Base-T port for connection of network devices
2	PON	SC port (socket) for connection to PON with GPON interface
3	USB	Connector for external drives and other devices
4	12V	Power adapter connector

Figure 9 shows NTU-2W side and front panels.

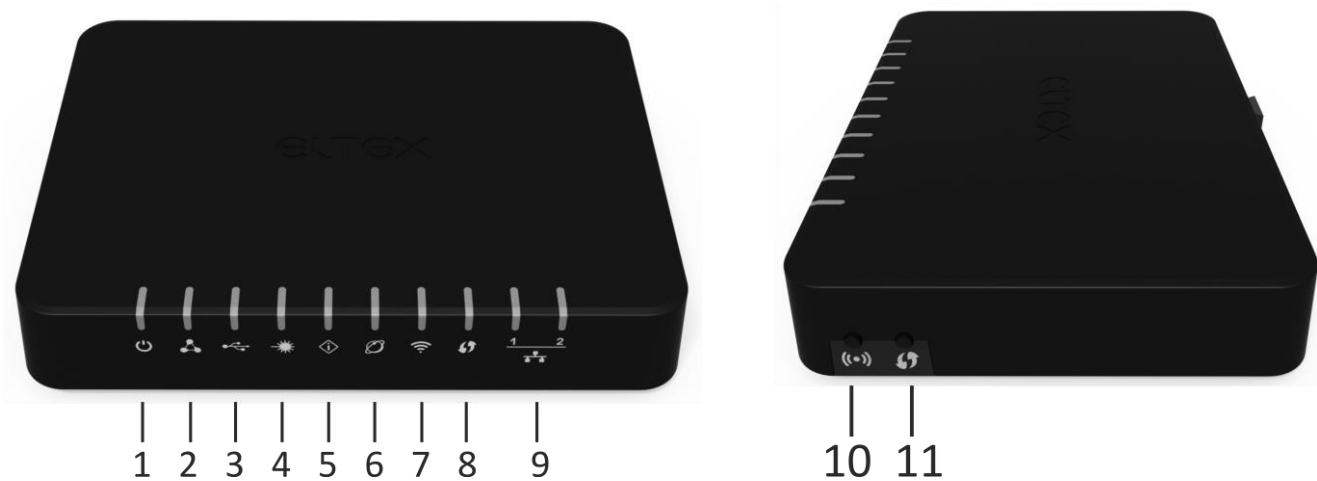


Figure 9 – NTU-2W Top Panel

The controls and LEDs located on the NTU-2W side and top panels are shown in the Table 8.

Table 8 – Description of the LEDs and controls located on the side and top panels (replace the names with corresponding icons)












	Panel Element	Description
1		Power indicator
2		Device configuration and firmware status indicator
3		USB operation indicator
4		Optical interface indicator
5		Optical interface error indicator
6		Internet connection indicator
7		Wi-Fi activity indicator
8		WPS operation indicator
9	 1..2	Ethernet ports activity indicators
10		Wi-Fi enabling/disabling button
11		A button which enables automatic secure Wi-Fi connection

Table 9 – Description of the controls located on the bottom panel

	Bottom Panel Element	Description
F		A functional key that reboots the device and resets it to the factory settings

2.5.4 NTU-RG-1402G-W

The NTU-RG-1402G-W subscriber terminal is designed as 187×120×32 mm desktop device in plastic housing.

Figure 10 shows the NTU-RG-1402G-W rear panel layout.

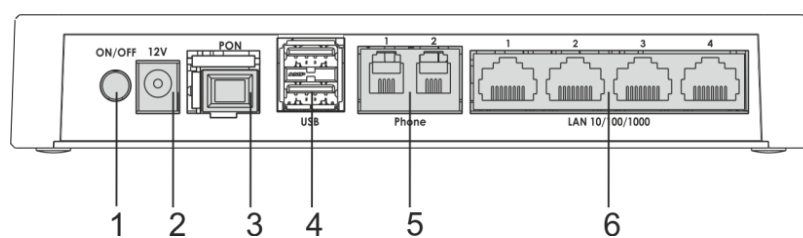


Figure 10 – NTU-RG-1402G-W Rear Panel layout

The connectors and controls located on the rear panel of NTU-2W are shown in the Table 10.

Table 10 – Description of the LEDs and Controls Located on the Rear Panel

No	Rear Panel Element	Description
1	On/Off	Power supply button
2	12V	Power adapter connector
3	PON	SC port (socket) for PON with GPON interface
4	USB	2 connector for external drives and other USB devices

5	Phone 1..2	2 RJ-11 ports for connection of analogue phones
6	LAN 10/100/1000 1..4	4 RJ-45 ports for connection of network devices

Figure 11 shows NTU-RG-1402G-W side and front panels.

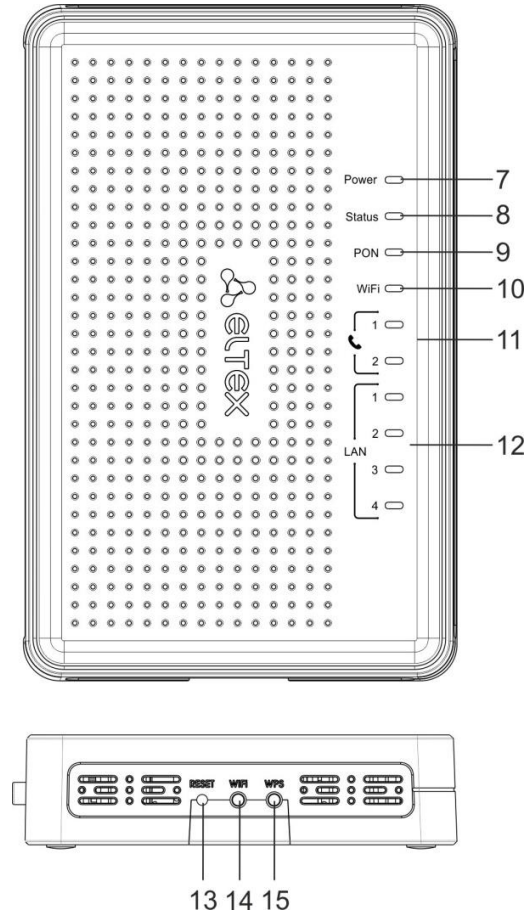


Figure 11 – NTU-RG-1402G-W side and top panels

See Table 11 for detailed information about LED indicators located on the top panel of the device.

Table 11 – Description of front panel LED indicators

No	Top Panel Element	Description
7	Power	Device power and activity status indicator
8	Status	Device authentication indicator
9	PON	Optical interface indicator
10	Wi-Fi	Wi-Fi activity indicator
11	☎ 1..2	FXP port activity indicators
12	LAN 1..4	Ethernet ports activity indicators

See Table 12 for detailed information about LEDs located on the top panel of the device.

Table 12 – Description of front panel LED indicators

No	Side Panel Element	Description
13	Reset	A functional key that reboots the device and resets it to the factory settings

14	Wi-Fi:	Wi-Fi enabling/disabling button
15	WPS	A button which enables automatic secure Wi-Fi connection


2.6 Light Indication

2.6.1 NTU-2V

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

Table 13 provides possible statuses of the LEDs.

Table 13 – Light Indication of Device Status



LED	LED Status	Device Status
PON	off	device booting
	green	connection between optical line terminal and device is established
	flashes green	authentication failed at optical line terminal
	flashes red	no signal from optical line terminal
LAN 1..2	green	established 10/100 Mbps connection
	orange	established 1000 Mbps connection
	flashes	transferring data packets
	on	off-hook
	flashes	port is not registered or SIP authentication is not completed on server
	flashes slowly	receiving a call
Status	off	WAN interface is in static or bridge mode, PPP client is not running
	green	device was successfully authenticated on line terminal (PPP session started in WAN interface)
	orange	device is not authenticated (PPP session is not started in WAN interface)
Power	off	device is disconnected from the power source or faulty
	green	current device configuration differs from the default one
	orange	the default configuration is active
	red	device booting





2.6.2 NTU-2VC

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

Table 14 provides possible statuses of the LEDs.

Table 14 – Light Indication of Device Status

LED	LED Status	Device Status
	on	off-hook
	flashes	port is not registered or SIP authentication is not completed on server
	flashes slowly	receiving a call
 1..2	green	established 10/100 Mbps connection







	orange flashes	established 1000 Mbps connection transferring data packets
	off red orange green	CaTV signal is not available in the provider network CaTV signal power < -10dBm or CaTV signal power > +3dBm CATV signal power is within -10dBm .. -8 dBm or +2 dBm .. +3 dBm -8dBm < CaTV signal power < +2dBm
	off green flashes green flashes red	device booting connection between optical line terminal and device is established authentication failed at optical line terminal no signal from optical line terminal
	off green orange	WAN interface is in static or bridge mode, PPP client is not running device was successfully authenticated on line terminal (PPP session started in WAN interface) device is not authenticated (PPP session is not started in WAN interface)
	off green orange red	the device is disconnected from the power source or faulty current device configuration differs from the default one the default configuration is active device booting




2.6.3 NTU-2W

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

Table 15 provides possible statuses of the LEDs.

Table 15 – Light Indication of Device Status

	LED	LED Status	Device Status
1		off	the device is disconnected from the power source or faulty
		green	power on
2		orange	the default configuration is active
		green	a non-default configuration
		flashes green	updating firmware
3		off	no USB device is connected
		green	USB device is connected
		flashes green	accessing the USB device
4		off	optics is not connected / laser is disconnected on the OLT side
		green	the device is connected and registered on OLT
		flashes green	registering the device on OLT
5		off	the device is connected and registered on OLT
		red	optics is not connected
		flashes red	laser is disconnected on the OLT side
6		off	no IP address for WAN connection
		green	obtained an IP address for WAN connection
		flashes green	connecting the device


7		off	Wi-Fi disabled
		green	Wi-Fi enabled
		flashes green	transmitting data via Wi-Fi
8		flashes green	the device is waiting for WPS connection
9		off	cable is not connected
		green	established 10/100 Mbps connection
		orange	established 1000 Mbps connection
		flashes green/orange	transferring data packets

2.6.4 NTU -RG-1402G-W

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

Table 16 provides possible statuses of the LEDs.

Table 16 – Light Indication of Device Status

LED	LED Status	Device Status
LAN 1..4	green	established 10/100 Mbps connection
	orange	established 1000 Mbps connection
	flashes	transferring data packets
 1..2	on	off-hook
	flashes	port is not registered or SIP authentication is not completed on server
	flashes slowly	receiving a call
Wi-Fi 2.4/5	green	Wi-Fi network is inactive
	flashes	transmitting data via Wi-Fi
	off	Wi-Fi network is inactive
PON	off	device booting
	green	authentication failed at optical line terminal
	flashes green	authentication failed at optical line terminal
Status	flashes red	no signal from optical line terminal
	off	WAN interface is in static or bridge mode, PPP client is not running
	green	device was successfully authenticated on line terminal (PPP session started in WAN interface)
Power	orange	device is not authenticated (PPP session is not started in WAN interface)
	off	the device is disconnected from the power source or faulty
	red	device booting
	orange	the default configuration is active
	green	current device configuration differs from the default one

2.6.5 Reboot and Reset to Factory Settings

To reboot the device press 'Reset' button once on the side panel (for NTU-2VC/NTU-2W, press 'F' button located on the rear/back panel). To load the device with default factory settings, press the Reset (F) button and hold it for 7–10 seconds until the POWER indicator turns red. The factory settings have the following IP addresses: LAN—192.168.1.1, subnet mask—255.255.255.0. Access can be provided from LAN 1 and LAN 2 ports.

2.7 Delivery Package

The *NTU-2V(C)*, *NTU-2W*, *NTU-RG* standard delivery package includes:

- *NTU-2V(C)*, *NTU-2W*, *NTU-RG* subscriber optical terminals;
- 220V/12V power adapter;
- Operation Manual.

3 DEVICE ARCHITECTURE

3.1 NTU-2V(C) Architecture

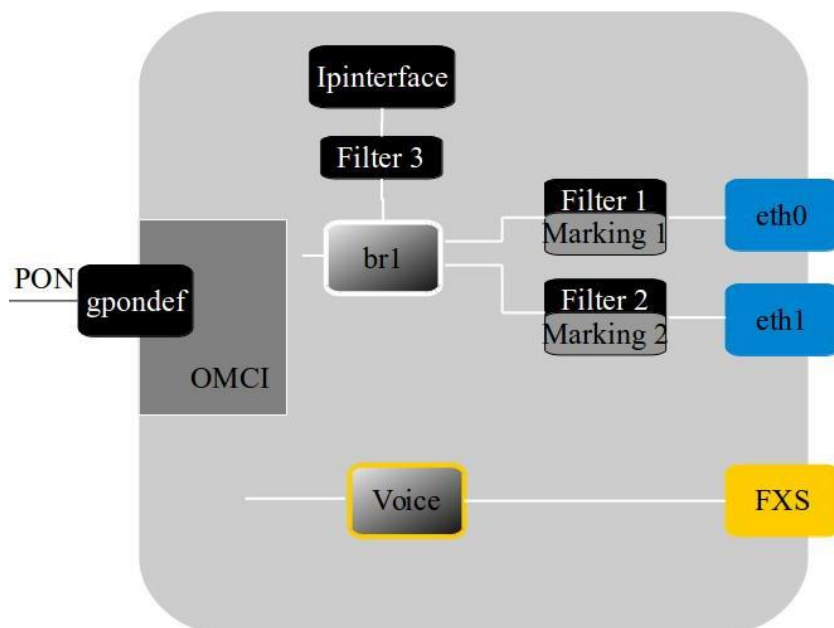


Figure 12 – Logical Architecture of a Device with Factory Settings

Main Components of the Device:

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

A device with factory (initial) settings have the following logical blocks (see Figure 12):

- br1;
- Voice (VoIP block);
- eth0...1;
- FXS;
- IPInterface.

In this case, the **br1** block is used to combine LAN ports into a single group.

The **eth0..1** blocks physically represent Ethernet ports with RJ-45 connector for connection of PC, STB, or other network devices. They are logically included into the **br1** block.

FXS blocks are ports with RJ-11 connectors for connection of analogue phones. They are logically included into the Voice block. The Voice block can be controlled through a web interface or remotely with the ACS server through TR-069 protocol. The block specifies VoIP service parameters (SIP server address, phone numbers, VAS, etc.)

Filter and **Marking** blocks are designed to include local interfaces in one group (**br1**). These blocks are responsible for traffic rules: **Filter** is used for incoming traffic, while **Marking** - for the outgoing one.

The **IPInterface** block is a logical object with an IP address for LAN access and a DHCP server, which assigns addresses to clients.

A connection to the OB device (successful connection to a stationary OLT) additionally creates the **gpondef** blocks with the help of the OMCI protocol (ONT Management and Control Interface). The block ensures connection of the subscriber's ONT device to station-side equipment.

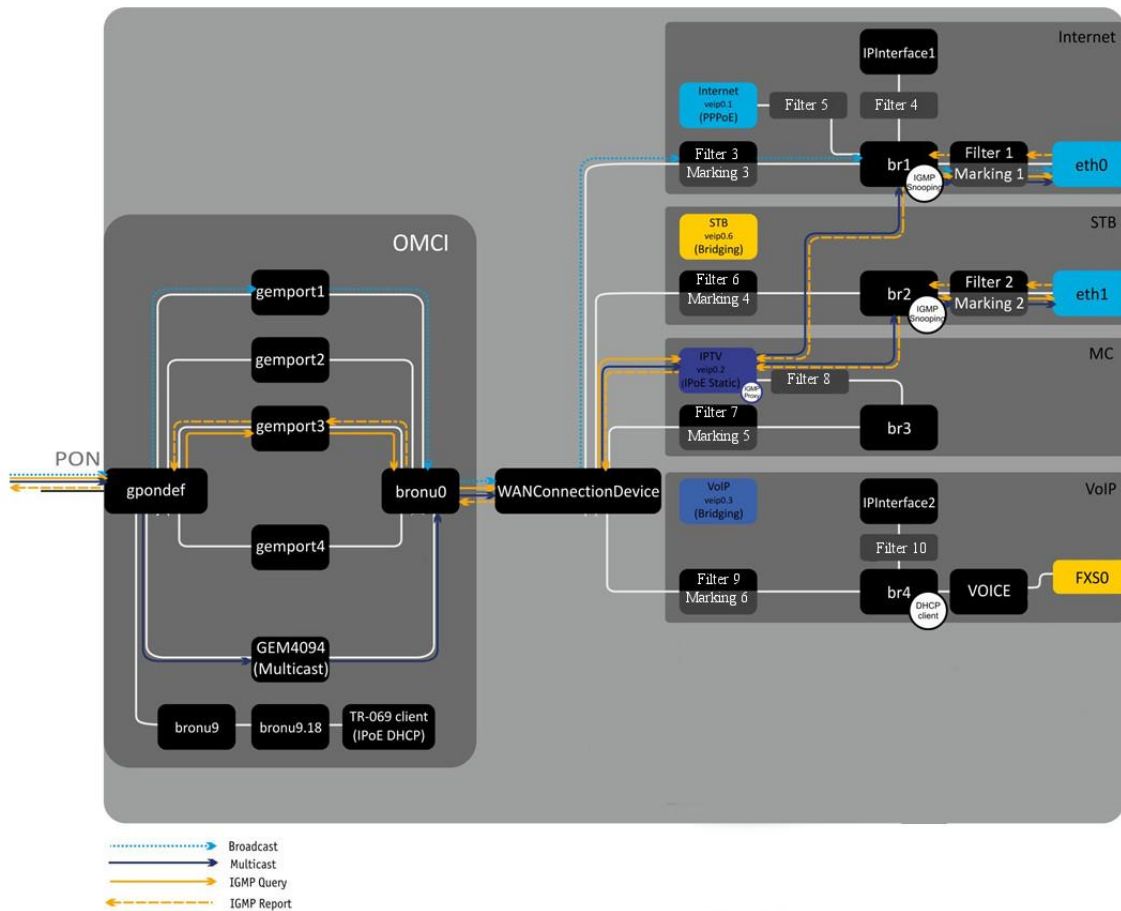


Figure 13 – Architecture of the Device Configured for Triple Play Model 1 Services
Model 1 Services

The blocks created by the OMCI protocol during connection to OLT (left) are shown for clarity and do not describe the real architecture.

The **gempport** blocks represent logical terminals of gem ports that are used for transmitting traffic of various services.

The **GEM4094** block is a logical terminal of the GEM port used for multicasting. It multicasts traffic downstream. WAN Connection Device receives the multicast traffic from this block and sends it further to Bri interfaces based on the table of IGMP groups.

The **bronu0, 9** blocks are MAC bridge service profiles (recommendation G.988).

The **TR-069 client** block is used for device remote control with the help of the ACS server (Auto Configuration Server) via TR-069 protocol. The block is used to establish communication between ACS and subscriber's equipment, process ONT queries, and configure services.

The **WANConnectionDevice** block is an object associated with WAN interface. It is an interim interface between the OMCI and RG parts of the device.

The **veip 0.n** blocks are WAN interfaces of the device's router; each of the interfaces is used to provide a certain type of services. In this example:

- veip0.1 is for the Internet;
- veip0.2 controls the multicast traffic;
- veip0.3 provides VoIP services;
- veip0.6 provides VoD and IPTV on STB.

These WAN interfaces have the following operation modes:

- PPPoE—starts PPP client;
- IPoE DHCP—starts DHCP client;
- IPoE Static—uses a static address;
- Bridging—operates in the bridge mode.

The **br1** blocks are the objects of the 2nd level and operate as bridges between the LAN and WAN interfaces to include the interface into one group. The **br1** block is connected to the veip0.1 interface, which operates in the PPPoE mode, and to the eth0 port. The **br4** block operates in bridge + DHCP mode in order to use the address of this interface for SIP client (Voice block). The **br2**, **br5**, **br6** blocks operate as a bridge, which allows transparent traffic transmission to the LAN ports of the router.

The **eth0..1** blocks represent LAN interfaces for connection of subscriber's equipment.

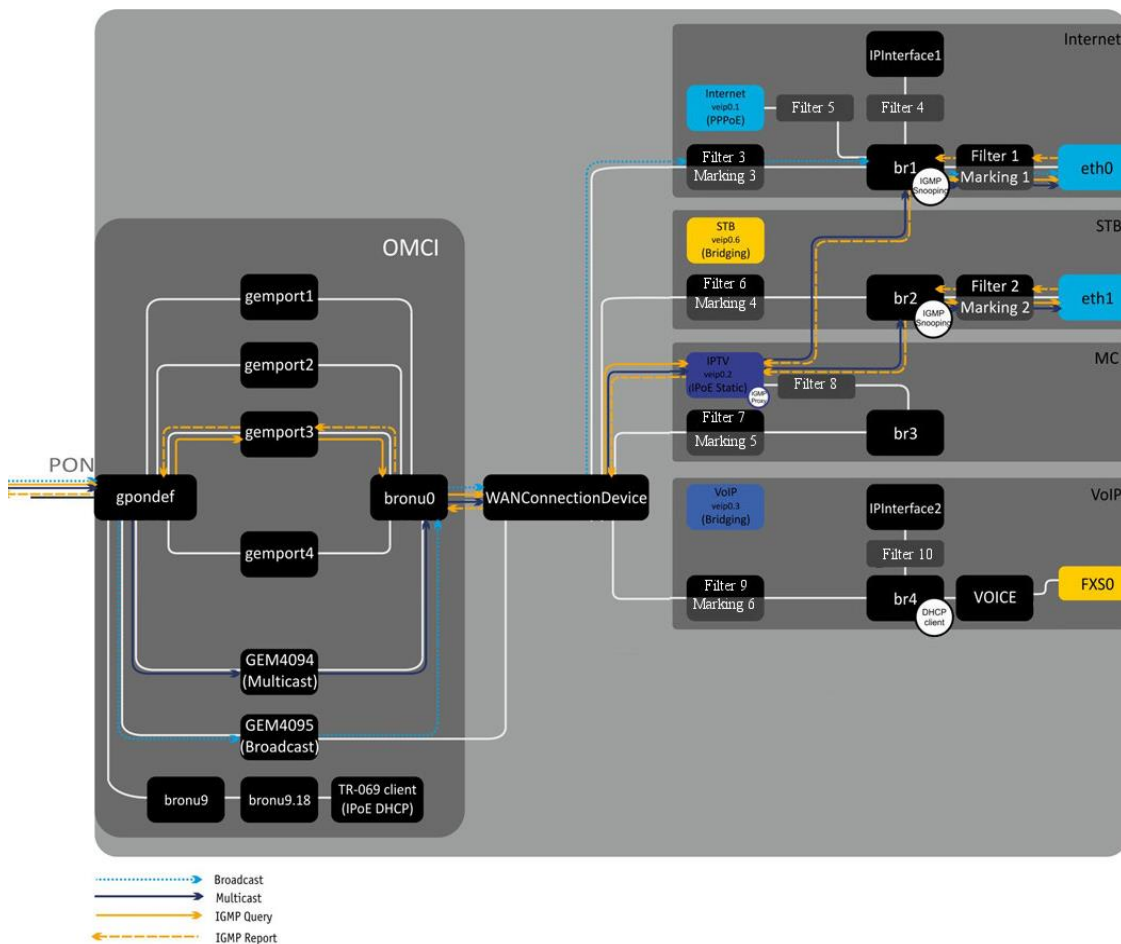


Figure 14 – Architecture of the Device Configured for Triple Play Model 2 Services
Model 2 Services

The difference between the models is the **GEM4095** block, which is a logical terminal of the GEM port for broadcasting. It broadcasts traffic downstream. Broadcast packets are sent from the **GEM4095** block to **WANConnectionDevice** and then are further transmitted to **br1** according to VLAN ID.

3.2 NTU-2W Architecture

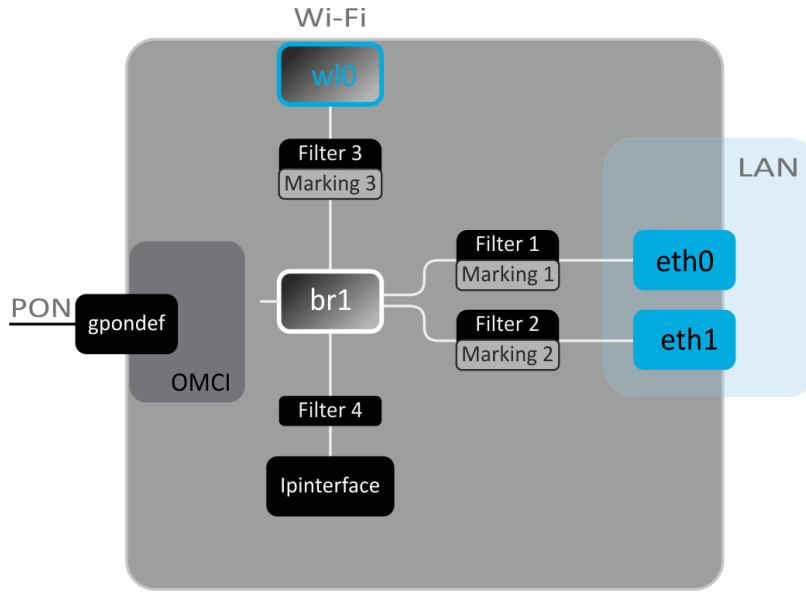


Figure 15 – Logical Architecture of a Device with Factory Settings

Main Components of the Device:

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

A device with factory (initial) settings have the following logical blocks (see Figure 15):

- br1;
- eth0...1;
- w10;
- IPInterface.

In this case, the **br1** block is used to combine LAN ports in one group.

The **eth0..1** blocks physically represent Ethernet ports with RJ-45 connector for connection of PC, STB, or other network devices. They are logically included into the **br1** block.

The **w10** block is an interface for Wi-Fi module connection.

The **Filter** and **Marking** blocks are designed to include local interfaces in one group (**br1**). These blocks are responsible for traffic rules: **Filter** is used for incoming traffic, while **Marking**—for the outgoing one.

The **IPInterface** block is a logical object with an IP address for LAN access and a DHCP server, which assigns addresses to clients.

A connection to the OB device (successful connection to a stationary OLT) additionally creates the **gpondef** blocks with the help of the OMCI protocol (ONT Management and Control Interface). The block ensures connection of the subscriber’s ONT device to station-side equipment.

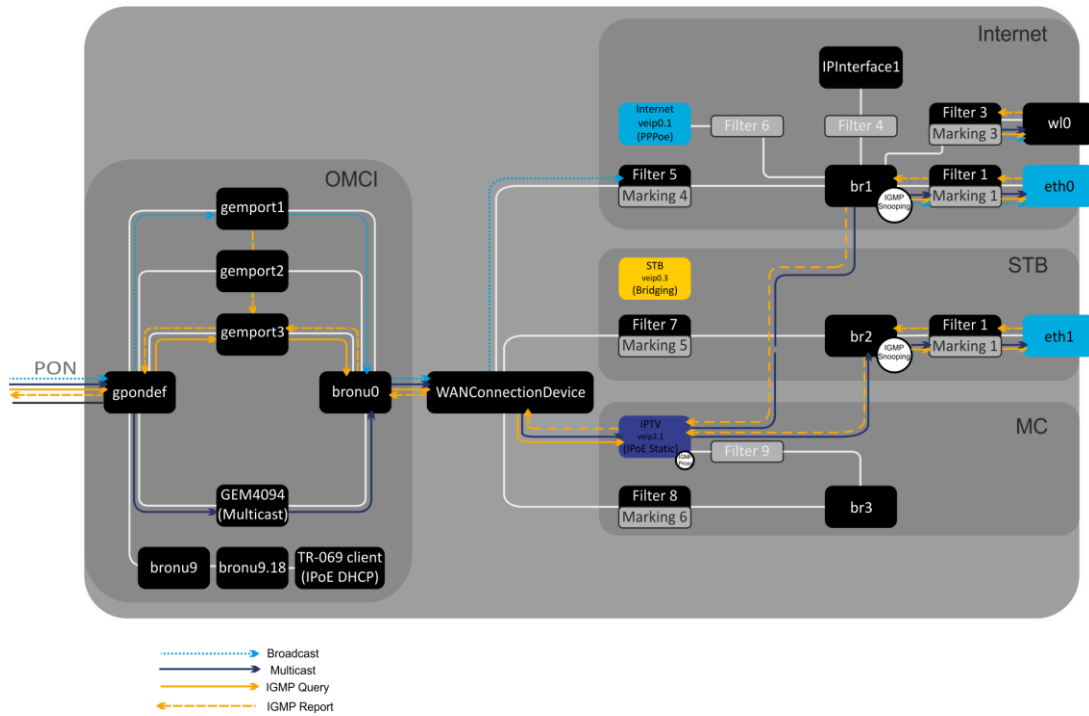


Figure 16 – Architecture of the Device Configured for Triple Play Model 1 Services

The blocks created by the OMCI protocol during connection to OLT (left) are shown for clarity and do not describe the real architecture.

The **gemport** blocks represent logical terminals of gem ports that are used for transmitting traffic of various services.

The **GEM4094** block is a logical terminal of the GEM port used for multicasting. It multicasts traffic downstream. WANConnectionDevice receives the multicast traffic from this block and sends it further to Bri interfaces based on the table of IGMP groups.

The **bronu0,9** blocks are MAC bridge service profiles (recommendation G.988).

The **TR-069 client** block is used for device remote control with the help of the ACS server (Auto Configuration Server) via TR-069 protocol. The block is used to establish communication between ACS and subscriber’s equipment, process ONT queries, and configure services.

The **WANConnectionDevice block** is an object associated with WAN interface. It is an interim interface between the OMCI and RG part of the device.

The **veip 0.n** blocks are WAN interfaces of the device’s router; each of the interfaces is used to provide a certain type of services. In this example:

- veip0.1 is for the Internet;
- veip0.2 controls the multicast traffic;
- veip0.3 provides VoD and IPTV on STB.

These WAN interfaces have the following operation modes:

- PPPoE—starts PPP client;
- IPoE DHCP—starts DHCP client;
- IPoE Static—uses a static address;
- Bridging—operates in the bridge mode.

The **bri** blocks are the objects of the 2nd level and operate as bridges between the LAN and WAN interfaces to include the interface into one group. The **br1** block is connected to the veip0.1 interface, which operates in the PPPoE mode, and to the eth0 port. The **br2**, **br3** blocks operate as a bridge, which allows transparent traffic transmission to the LAN ports of the router.

The **eth0..1** blocks represent LAN interfaces for connection of subscriber's equipment.

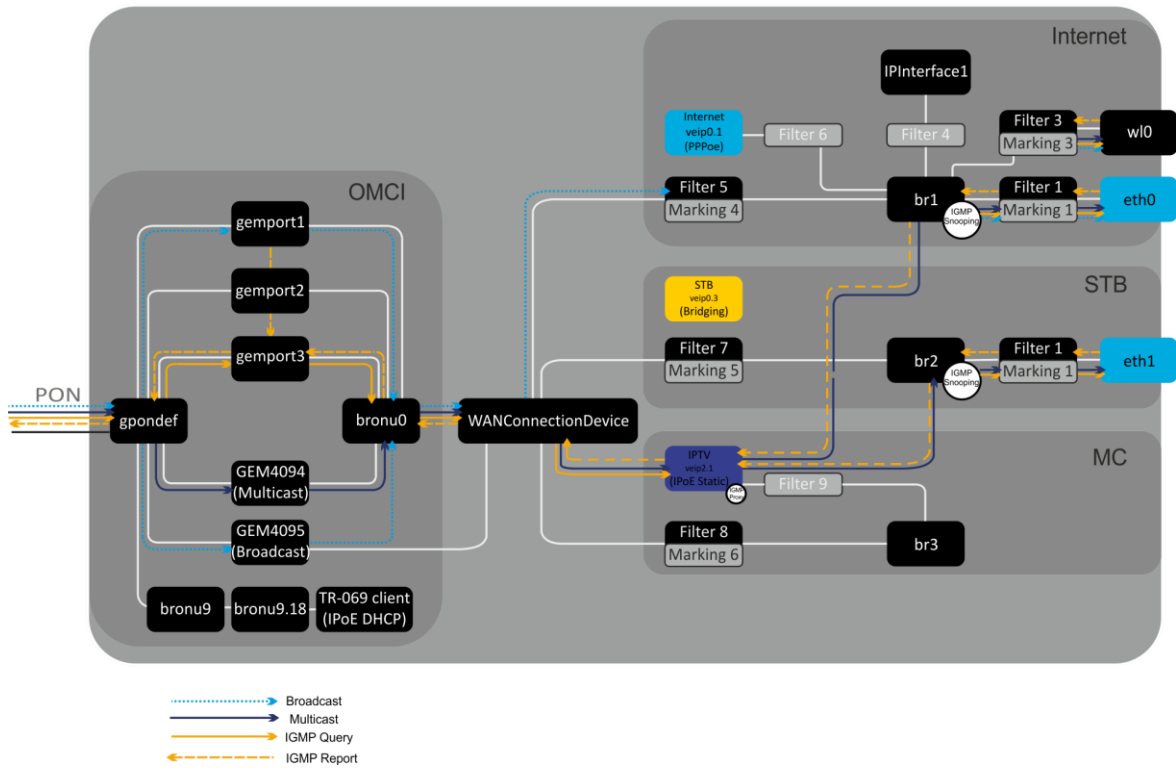


Figure 17 – Architecture of the Device Configured for Triple Play Model 2 Services

The difference between the models is the **GEM4095** block, which is a logical terminal of the GEM port for broadcasting. It broadcasts traffic downstream. Broadcast packets are sent from the GEM4095 block to **WANConnectionDevice** and then are further transmitted to **bri** according to VLAN ID.

3.3 NTU-RG-1402G-W Architecture

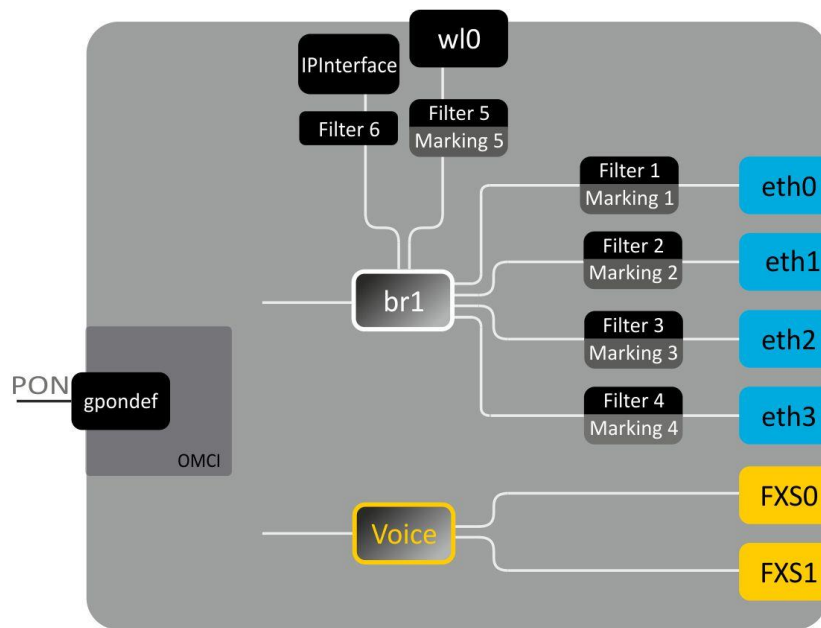


Figure 18 – Logical Architecture of a Device with Factory Settings

Main Components of the Device:

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

A device with factory (initial) settings have the following logical blocks (see Figure 18):

- Br1;
- Voice (VoIP block);
- eth0...3;
- FXS0...1;
- w10;
- IPInterface.

In this case, the **br1** block is used to combine LAN ports in one group.

The **eth0..3** blocks physically represent Ethernet ports with RJ-45 connector for connection of PC, STB, or other network devices. They are logically included into the **br1** block.

FXS0..1 blocks are ports with RJ-11 connectors for connection of analogue phones. They are logically included into the Voice block. The **Voice** block can be controlled through web interface or remotely with ACS server through TR-069 protocol. The block specifies VoIP service parameters (SIP server address, phone numbers, VAS, etc.)

The **w10** block is an interface for Wi-Fi module connection.

The **Filter** and **Marking** blocks are designed to include local interfaces in one group (**br1**). These blocks are responsible for traffic rules: **Filter** is used for incoming traffic, while **Marking**—for the outgoing one.

The **IPInterface** block is a logical object with an IP address for LAN access and a DHCP server, which assigns addresses to clients.

A connection to the OB device (successful connection to a stationary OLT) additionally creates the **gpondef** blocks with the help of the OMCI protocol (ONT Management and Control Interface). The block ensures connection of the subscriber's ONT device to station-side equipment.

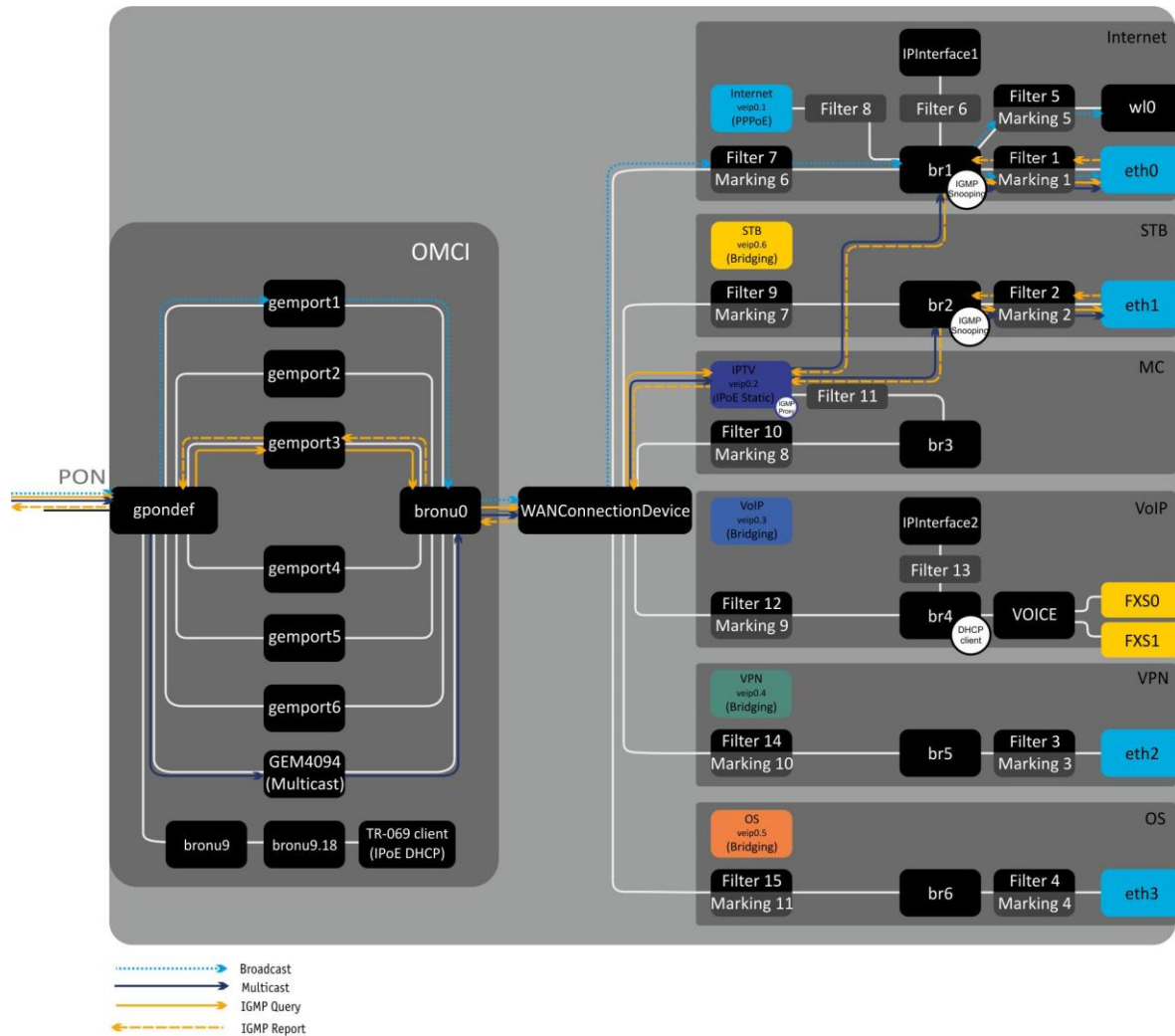


Figure 19 – Architecture of the Device Configured for Triple Play Model 1 Services

The blocks created by the OMCI protocol during connection to OLT (left) are shown for clarity and do not describe the real architecture.

The **gemport** blocks represent logical terminals of gem ports that are used for transmitting traffic of various services.

The **GEM4094** block is a logical terminal of the GEM port used for multicasting. It multicasts traffic downstream. WANConnectionDevice receives the multicast traffic from this block and sends it further to Bri interfaces based on the table of IGMP groups.

The **bronu0,9** blocks are MAC bridge service profiles (recommendation G.988).

The **TR-069 client** block is used for device remote control with the help of the ACS server (Auto Configuration Server) via TR-069 protocol. The block is used to establish communication between ACS and subscriber's equipment, process ONT queries, and configure services.

The **WANConnectionDevice** block is an object associated with WAN interface. It is an interim interface between the OMCI and RG parts of the device.

The **veip 0.n** blocks are WAN interfaces of the device's router; each of the interfaces is used to provide a certain type of services. In this example:

- veip0.1 is for the Internet;
- veip0.2 controls the multicast traffic;
- veip0.3 provides VoIP services;
- veip0.4 provides VPN service on a separated port;
- veip0.5 provides other services (alarm system);
- veip0.6 provides VoD and IPTV on STB.

These WAN interfaces have the following operation modes:

- PPPoE—starts PPP client;
- IPoE DHCP—starts DHCP client;
- IPoE Static—uses a static address;
- Bridging—operates in the bridge mode.

The **bri** blocks are the objects of the 2nd level and operate as bridges between the LAN and WAN interfaces to include the interface into one group. The **br1** block is connected to the veip0.1 interface, which operates in the PPPoE mode, and to the eth0 port. The **br4** block operates in bridge + DHCP mode in order to use the address of this interface for SIP client (Voice block). The **br2, br5, br6** blocks operate as a bridge, which allows transparent traffic transmission to the LAN ports of the router.

The **eth0...3** blocks represent LAN interfaces for connection of subscriber's equipment.

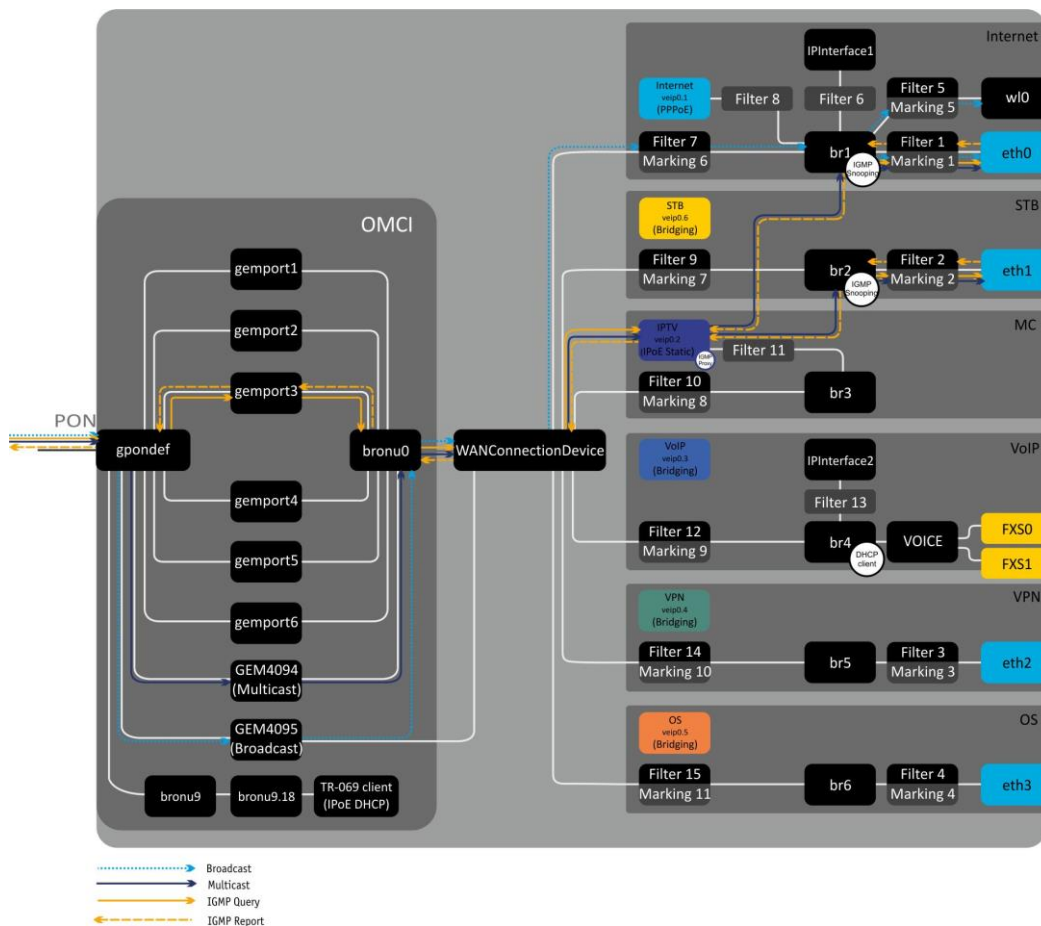



Figure 20 – Architecture of the Device Configured for Triple Play Model 2 Services

The difference between the models is the **GEM4095** block, which is a logical terminal of the GEM port for broadcasting. It broadcasts traffic downstream. Broadcast packets are sent from the GEM4095 block to **WAN Connection Device** and then are further transmitted to **bri** according to VLAN ID.

4 NTU-RG-1402G-W CONFIGURATION VIA WEB INTERFACE. USER ACCESS

Device configuration requires accessing the device through a web browser (a program displaying hypertext documents) such as Firefox or Google Chrome. To do this, enter the device IP address into the address bar of the web browser (the factory default IP —192.168.1.1, subnet mask—255.255.255.0).

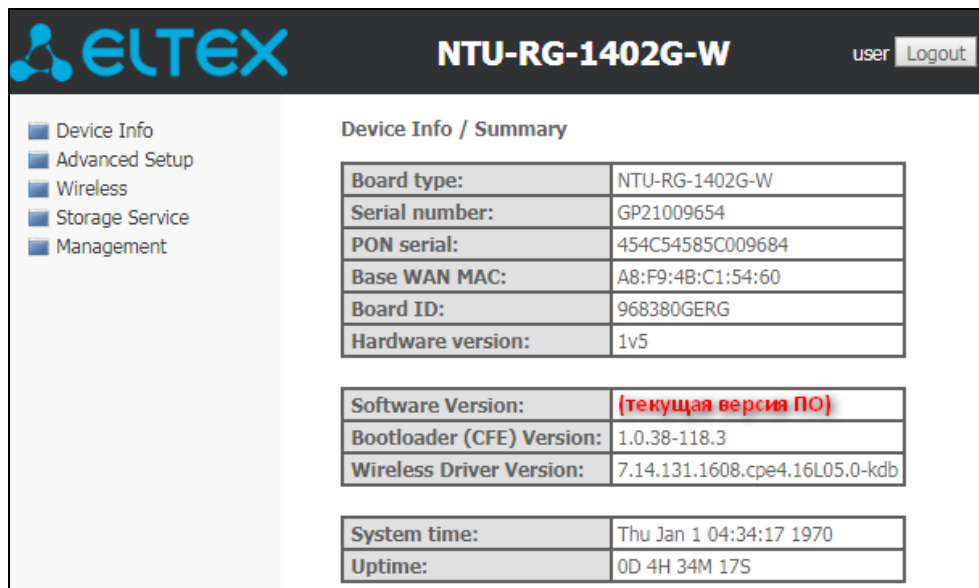
When the IP address is entered, the device will request a user name and a password.



User name: **user**, password: **user**.

To prevent unauthorised access to the device, we recommend to change the password (see section 4.6.5 The “Passwords” Submenu. Access Control Settings (password settings)).

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



Device Info / Summary	
Board type:	NTU-RG-1402G-W
Serial number:	GP21009654
PON serial:	454C54585C009684
Base WAN MAC:	A8:F9:4B:C1:54:60
Board ID:	968380GERG
Hardware version:	1v5
Software Version:	(текущая версия ПО)
Bootloader (CFE) Version:	1.0.38-118.3
Wireless Driver Version:	7.14.131.1608.cpe4.16L05.0-kdb
System time:	Thu Jan 1 04:34:17 1970
Uptime:	0D 4H 34M 17S

4.1 The “Device Info” Menu. Device Information

4.1.1 The “Summary” Submenu. Device General Information

Device Info / Summary	
Board type:	NTU-RG-1402G-W
Serial number:	GP21009654
PON serial:	454C54585C009684
Base WAN MAC:	A8:F9:4B:C1:54:60
Board ID:	968380GERG
Hardware version:	1v5
Software Version:	(текущая версия ПО)
Bootloader (CFE) Version:	1.0.38-118.3
Wireless Driver Version:	7.14.131.1608.cpe4.16L05.0-kdb
System time:	Thu Jan 1 04:39:08 1970
Uptime:	0D 4H 39M 8S

- *Board type*—model of the device;
- *Serial number*—serial number of the device;
- *PON serial*—serial number of the device in the PON network;
- *Base WAN MAC*—WAN MAC address of the device;
- *Board ID*—board identification number;
- *Hardware Version*—version of the hardware installed;

- *Software Version*—version of the firmware installed;
- *Bootloader (CFE) Version*—version of the bootloader installed;
- *Wireless Driver Version*¹—Wi-Fi adapter version;

- System time—the current time settings of the device;
- *Uptime*—time from the last device reboot.

4.1.2 The “WAN” Submenu. The Status of Services

4.1.2.1 The “General” Submenu. General information

The tab displays general information about existing configurations of the WAN interface.

Device Info / WAN / General									
Interface	Description	Type	VlanMuxId	Igmp Pxy	Igmp Src Enbl	NAT	Firewall	Status	IPv4 Address
ppp0.1	HSI_PPP	PPPoE	10	Disabled	Disabled	Enabled	Enabled	Connected	192.168.100.104
veip0.2	br_veip0.-1	Bridge	12	Disabled	Enabled	Disabled	Disabled	Unconfigured	0.0.0.0
veip0.3	br_veip0.-1	Bridge	11	Disabled	Enabled	Disabled	Disabled	Unconfigured	0.0.0.0

¹ Only for NTU-2W, NTU-RG-1402G-W

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:

- *Interface*—name of the interface;
- *Type*—operation mode of the interface;
- *Connection Type*—type of the connection;
- *NAT*—NAT status;
- *Firewall*—Firewall status;
- *Status*—connection status;
- *IPv4 Address*—access address;
- *Default Gateway*—the default gateway;
- *Primary DNS Server*¹—address of the primary DNS server used for work;
- *Secondary DNS Server*¹—address of the secondary DNS server;
- *Bridging to*—list of the linked LAN interfaces.

Device Info / WAN / Detail	
WAN service 0: Internet.1100	
Interface: ppp0.1	
Type: PPPoE	
Connection type: IP_Routed	
NAT: Enabled	
Status: Connected	
IPv4 Address: 192.168.100.110	
Primary DNS Server: 192.168.100.1	
Secondary DNS Server: 10.10.0.2	
Bridging to: eth0,eth1,eth2,eth3,wl0	
WAN service 1: VoIP.1101	
Interface: veip0.2	
Type: IPoE	
Connection type: IP_Routed	
Status: Connected	
IPv4 Address: 192.168.101.179	
Default Gateway: 192.168.101.1	
Primary DNS Server: 192.168.198.102	
Bridging to: eth0,eth1,eth2,eth3,wl0	

4.1.3 The “LAN” Submenu. LAN Ports Monitoring. Wi-Fi Interface Status Monitoring

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

NTU-2V(C):

Device Info / LAN	
Port 1	Up; 1000M full
Port 2	Down

NTU-2W:

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

NTU-RG-1402G-W:

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

¹ Only for the **INTERNET** and **VoIP**

4.1.4 The "Statistics" Submenu. Traffic Flow Information for Ports of the Device

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

LAN interface:

NTU-2V(C)

Device Info / Statistics / LAN

Interface	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
Port 1	127168	909	0	0	0	60	849	0	470580	920	0	0	0	8	912	0
Port 2	43737	359	0	0	0	13	346	0	323908	391	0	0	0	2	389	0

Reset Statistics

NTU-2W

Device Info / Statistics / LAN

Interface	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
Port 1	150214	1098	0	6	0	75	1023	0	658792	1198	0	0	0	39	1159	0
Port 2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Wi-Fi	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0

Reset Statistics

NTU-RG-1402G-W

Device Info / Statistics / LAN

Interface	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
Port 1	393216	2754	0	0	0	135	2619	0	1422907	2949	0	0	0	37	2912	0
Port 2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Port 3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Port 4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Wi-Fi	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Reset Statistics

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
veip0.2	VoIP.1101	24402	283	0	0	0	0	122	161	16995	171	0	0	0	0	171	0
veip0.3	IGMP.30	0	0	0	0	0	0	0	0	492	6	0	0	0	0	6	0
veip0.4	STB.1102	11633	139	0	0	0	0	113	26	168230	677	0	0	4848	71	577	29
veip0.5	VPN.1103	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
veip0.6	OS.1105	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
veip0.7	Wi-Fi Guest.100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ppp0.1	Internet.1100	4141	62	0	0	0	0	62	0	3811	67	0	0	0	0	67	0

Reset Statistics

Optical interface:

Device Info / Statistics / Optical								
Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Optical	3744775	21322	0	0	4055512	7683	0	0

Reset Statistics

Link Status	Optical Signal Level	Transmit Optical Level	Temperature	Vcc Voltage	Bias Current
Up	-21.43 dBm	2.59 dBm	48.4 C	3.35 V	11.66 mA

If a device supports measurement of optical signal parameters¹, the menu displays an additional table:

- *Link Status*—optical link status;
- *Optical Signal Level*—level of the incoming signal (1490 nm);
- *Transmit Optical Level*—level of the outgoing signal (1310 nm);
- *Temperature*—temperature of the SFF module;
- *Vcc Voltage*—power voltage;
- *Bias Current*—offset current;
- *Optical Video Level*— CaTV optical signal power².

To clear the statistics and start gathering it again, click the *Reset Statistic* button.

4.1.5 The “Route” Submenu. The Routing Table

The menu shows the routing table.

Device Info / Route						
Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
0.0.0.0	192.168.101.1	0.0.0.0	UG	0	VoIP.1101	veip0.2
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
192.168.21.0	0.0.0.0	255.255.255.0	U	0	IGMP.30	veip0.3
192.168.21.0	192.168.21.1	255.255.255.0	UG	1	IGMP.30	veip0.3
192.168.100.1	0.0.0.0	255.255.255.255	UH	0	Internet.1100	ppp0.1
192.168.100.1	0.0.0.0	255.255.255.255	UH	0	Internet.1100	ppp0.1
192.168.101.0	0.0.0.0	255.255.255.0	U	0	VoIP.1101	veip0.2
192.168.198.102	192.168.101.1	255.255.255.255	UGH	0	VoIP.1101	veip0.2
192.168.203.0	0.0.0.0	255.255.255.0	U	0		bronu255.19

Flags:
 U - up,
 G - gateway,
 H - host,
 R - reinstate,
 D - dynamic (redirect),
 M - modified (redirect),
 ! - reject

- *Destination*—IP address of the destination;
- *Gateway*—IP address of the gateway;
- *Subnet mask*—subnet mask (Genmask);
- *Flag*—route flag:
 - *U*—an active route;

¹ Optional

² Only for NTU-2VC

- !—an inactive route, packets will be rejected;
- G—a route with a gateway;
- H—the destination is a separate host;
- R—a restored route;
- D—the route was created after receiving a redirected ICMP message;
- M—the route was changed by a redirected ICMP message;

- *Metric*—priority of the route;
- *Service*—corresponding service of the route;
- *Interface*—corresponding network interface of the route.

4.1.6 The “ARP” Submenu. ARP Protocol Cache

ARP performance heavily depends on the ARP cache, which is generated at every host. The cache contains Internet addresses and corresponding hardware addresses. Every record created in the cache is stored for 5 minutes.

Device Info / ARP			
IP address	Flags	HW Address	Device
192.168.101.1	Complete	1c:af:f7:0e:1c:17	vejp0.2
192.168.203.2	Complete	1c:af:f7:0e:1c:17	bronu255.19
192.168.1.2	Complete	08:60:6e:d7:73:30	br0

- *IP-address*—IP address of the client;
- *Flags*—status flags:
 - *Complete*—active client;
 - *Incomplete*—the client is not responding to ARP requests;
- *HW Address*—MAC address of the client;
- *Device*—the interface where the client is located on.

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			
Hostname	MAC Address	IP Address	Expires In
julia	08:60:6e:d7:73:30	192.168.1.2	20 hours, 9 minutes, 49 seconds

- *Hostname*—host name (network device);
- *MAC Address*—MAC address of the device;
- *IP Address*—LAN address of the device chosen by the router from the pool of IP addresses;
- *Expires In*—the time when the lease of the current address expires.

4.1.8 The “Wireless Station” Submenu¹. 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
04:F7:E4:4B:CC:FB	Yes	Yes	ELTEX-0438	wl0

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

- *MAC*—MAC address of the device;
- *Associated*—status of connection with SSID;
- *Authorized*—authorisation status;
- *SSID*—identifier of the network the client belongs to;
- *Interface*—access interface.

Click the *Refresh* button to refresh the data.

4.1.9 The Wireless Monitor Submenu². Detected Wi-Fi Networks

This section shows a list of detected wireless networks.

Device Info / Wireless Monitor

This page shows known wireless networks.

SSID	BSSID	Channel	RSSI
ELTEX-1AB8	A8:F9:4B:C0:1A:B9	6	-52 dBm
ELTEX-1B70	A8:F9:4B:C0:1B:71	6	-51 dBm
SL-test_2G	E8:4E:06:21:DA:3A	6	-71 dBm
My_Eltex_11112	A8:F9:4B:B0:29:40	6	-67 dBm
Keeeenetic2	10:7B:EF:61:A8:D4	5	-64 dBm
ELTEX-202E	A8:F9:4B:64:20:2F	6	-42 dBm
Eltex-Local	A8:F9:4B:B0:21:40	6	-60 dBm
Eltex-Guest	A8:F9:4B:B0:21:41	6	-59 dBm
Egor-TLS	A8:F9:4B:B0:21:42	6	-57 dBm
ELTEX-1A00	A8:F9:4B:C0:1A:01	1	-56 dBm
Default	34:08:04:91:83:EC	3	-61 dBm

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

- *SSID*—name of the wireless network;
- *BSSID*—MAC address of the access point;
- *Channel*—channel of the access point;
- *RSSI*—level of the signal sent by the access point and received by the ONT.

Click the *Refresh* button to refresh the data.

¹ Only for NTU-2W, NTU-RG-1402G-W

² Only for NTU-2W, NTU-RG-1402G-W

4.1.10 The “Voice” submenu¹. Monitoring the phone port states

Use the menu to view FXS port state and parameters of SIP accounts

NTU-RG-1402G-W:

Device Info / Voice		
Voice daemon status	RUNNING	
SIP Proxy	192.168.101.1:5060	
SIP Outbound Proxy	192.168.101.1:5060	
SIP Registrar	192.168.101.1:5060	
SIP Account	1	2
Account enabled	Enabled	Disabled
State	Up	Disabled
Error	None	None
Response code	200 OK	None
Extension	4800	undefined
Display name	4800	undefined
Authentication name	4800	undefined

NTU-2V(C):

Device Info / Voice	
Voice daemon status	STOPPED
SIP Proxy	undefined:5060
SIP Outbound Proxy	undefined:5060
SIP Registrar	undefined:5060
Account enabled	Disabled
State	Disabled
Error	None
Response code	None
Extension	undefined
Display name	undefined
Authentication name	undefined

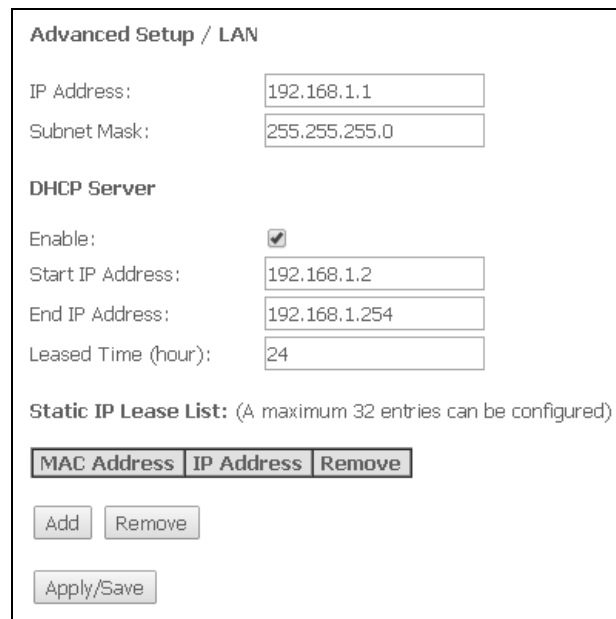
- *Voice daemon status* – the status of voice daemon;
- *SIP Proxy* – SIP Proxy address and port;
- *SIP Outbound Proxy* – address and port of the SIP proxy which will be used to transfer all queries (this server will be used for routing of SIP Proxy and SIP Registrar queries);
- *SIP Proxy* – SIP Proxy address and port;
- *SIP Account* – SIP account (FXS port number);
- *Account enabled* – FXS port status in configuration;
- *Status*—connection status;
- *Error* – SIP server error;
- *Response code* – SIP server response code;
- *Extension* – phone number;
- *Display name* – user name displayed;
- *Authentication name* – user name authentication.

¹ Only for NTU-2V(C), NTU-RG-1402G-W

4.2 The “Advanced Setup” Menu. Advanced Settings

4.2.1 The “LAN” Submenu. Configuration of Main Parameters

The menu allows configuration of the main parameters of the LAN interface.



Advanced Setup / LAN

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

- *IP Address*—address of the device in local network;
- *Subnet Mask*—subnet mask.

DHCP Server:

DHCP Server (Dynamic Host Configuration Protocol) allows you to configure local computers automatically in order to work in a network. DHCP server automatically assigns IP address to each computer within a network.

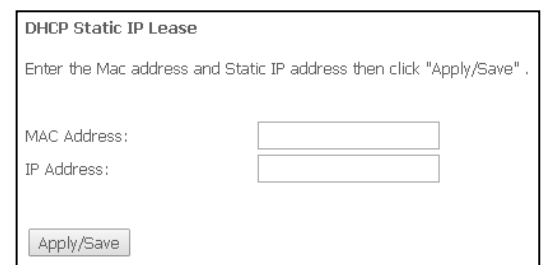
- *Enable*— when checked, use DHCP server (receive IP addresses dynamically from the specified range);
- *Start IP Address*—the first address of the range;
- *End IP Address*—the last address of the range;
- *Leased Time (hour)*—time of the address lease (in hours).

Static IP Lease List:

DHCP Static IP Lease—correspondence between the leased IP addresses and devices' MAC addresses (mapping). To add a record into the table, click *Add*. You can add up to 32 records.

- *MAC address*—MAC address;
- *IP address* — IP address of the device.

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



DHCP Static IP Lease

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

MAC Address:

IP Address:

4.2.2 The “PPPoE” menu. PPP Settings¹

To enable the service, set the *Enable Service* flag.

The Internet service has two available operation modes:

1. **IP_Routed** – mode when PPPoE session starts on a subscriber device;
2. **PPPoE_Bridged** – mode when PPPoE session starts on a user PC.

- *Username* – username for Internet access;
- *Password* – user password for Internet access.



Username and Password fields are not available in the PPPoE_Bridged mode. The username and password are entered on user PC.

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

4.2.3 The “NAT” Submenu. NAT Settings

NAT settings can be useful when the device operates in the router mode.

4.2.3.1. The “Virtual Servers” Submenu. Settings of Virtual Servers

Virtual Server is a router function, which provides users with Internet access to the servers located in their LAN (e. g., email, WWW, or FTP servers). A device may have up to 32 records.

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	Remove
Blizzard Battle.net	4000	4000	TCP	4000	4000	192.168.1.100	ppp0.1	<input type="checkbox"/>
Blizzard Battle.net	6112	6112	TCP	6112	6112	192.168.1.100	ppp0.1	<input type="checkbox"/>
Blizzard Battle.net	6112	6112	UDP	6112	6112	192.168.1.100	ppp0.1	<input type="checkbox"/>

¹ If there is no menu in the configurator, the given settings are already made by your provider

To add a record to the filtration table, click *Add* and fill in the fields in the displayed menu:

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:

Source IP Address: Leave empty, if you want to have connections from any IP

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 ▼		
		TCP ▼		

– *Use Interface*— interface that is used;



Available are only the interfaces configured to work in the router mode with enabled translation of network addresses.

– *Service Name*—service settings:

- *Select a 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 LAN;

– *Source IP Address*—IP address of a source;

– *Enable NAT Loopback*—allows a user of an internal LAN to access the local resources via IP address of an external network;

– *External Port Start*—the first external port of the port range accessible from the Internet;

– *External Port End*—the last external port of the port range accessible from the Internet;

– *Protocol*—select a network protocol;

– *Internal Port Start*—the first internal port of the port range to receive forwarded traffic from an external port of the router;

– *Internal Port End*—the last internal port in the port range to receive forwarded traffic from an external port of the router.

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

4.2.3.2. The “Port Triggering” Submenu. Port Triggering Configuration

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			
ICQ	UDP	4000 4000	TCP	20000 20059	ppp0.1	<input type="checkbox"/>	

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:

Application Name:

Select an application:

Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
<input type="text" value="4000"/>	<input type="text" value="4000"/>	<input type="text" value="UDP"/>	<input type="text" value="20000"/>	<input type="text" value="20059"/>	<input type="text" value="TCP"/>
<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>
<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>
<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>
<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>
<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>
<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>
<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>

– *Use Interface*— interface that is used.



Available are only the interfaces configured to work in the router mode with enabled translation of network addresses.

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

As opposed to the *Virtual Server* function, you don't need to specify a fixed IP address of the computer in LAN.

- *Trigger Port Start*—the first port of the port range to act as a trigger;
- *Trigger Port End*—the last port of the port range to act as a trigger;

- *Trigger Protocol*—the protocol used for the trigger;
- *Open Port Start*—the first port of the port range to be opened by the router;
- *Open Port End*—the last port of the port range to be opened by the router;
- *Open Protocol*—the protocol used for the opened ports.

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

4.2.3.3. The “DMZ Host” Submenu. DMZ Settings

If the *DMZ Host IP Address* field contains an IP address, all requests from the external network that do not correspond the Virtual Server rules will be forwarded to the DMZ host (a trusted host with a specific address in LAN).

Delete the IP address in 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.

4.2.4 The “Security” Submenu. Security Settings

This submenu allows configuration of device security settings.

4.2.4.1. The “IP Filtering” Submenu. Addresses Filtering Configuration

The *IP Filtering* function filters the traffic forwarded to IP addresses and ports through the router.

Filtration Settings for Outgoing Traffic

Advanced Setup / Security / IP Filtering / Outgoing

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

Choose Add or Remove to configure outgoing IP filters.

Filter Name	IP Version	Protocol	SrcMAC	SrcIP/PrefixLength	SrcPort	DstIP/PrefixLength	DstPort	Remove
Security	4	TCP or UDP	11:34:5A:67:4C:38	192.168.15.12	80	192.168.15.52	80	<input type="checkbox"/>



All outgoing traffic will be transmitted by default. Rules created in the menu allow 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*—text description of the filter;
- *IP Version*—select IP protocol version;
- *Protocol*—select protocol (TCP/UDP, TCP, UDP, ICMP);
- *MAC address*—source MAC address;
- *Source IP address[/prefix length]*—source IP address (the prefix length can be specified after a slash);
- *Source Port (port or port:port)*—source port or port range separated by a colon;
- *Destination IP address[/prefix length]*—destination IP address (the prefix length can be specified after a slash);
- *Destination Port (port or port:port)*—destination port or port range separated by a colon.

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

Filtration 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
Security1	ppp0.1	4	TCP or UDP	11:25:34:a6:57:5c		80			<input type="checkbox"/>

When a firewall is enabled in a WAN or LAN interface, it blocks all incoming traffic which does not meet the set rules.

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 Internet/ppp0.1 br0/br0 br1/br1 br2/br2 br3/br3

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

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

- *Select All*—when set, allows selection of all available interfaces. You can also select an interface from the list by setting a flag in front of it.

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

4.2.4.2. The “MAC Filtering” Submenu. Filtering Settings for MAC Addresses

Use MAC Address Filtering to forward or block traffic depending on the source/destination MAC addresses.

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.

Interface	Policy	Change
veip0.4	FORWARDED	<input type="checkbox"/>
veip0.5	FORWARDED	<input type="checkbox"/>
veip0.6	FORWARDED	<input type="checkbox"/>
veip0.7	FORWARDED	<input type="checkbox"/>

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
veip0.6	PPPoE	1C:AF:F7:0E:1C:17		WAN_TO_LAN	<input type="checkbox"/>



MAC address filtering works only for interfaces in the Bridge mode.

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

In the FORWARDED mode, the created rules will block the traffic passing to/from the specified source/destination MAC addresses; in the BLOCKED mode, the rules will permit this traffic.

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:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

- *Protocol type*—select a protocol (PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP);
- *Destination MAC Address*—destination MAC address;
- *Source MAC Address*—source MAC address;
- *Frame Direction*—direction of the frame transmission (LAN<=>WAN, LAN=>WAN, WAN=>LAN);
- *WAN Interfaces (configured in the Bridge mode only)*—select WAN interfaces from the drop-down list (only interfaces in the Bridge mode are available).

To accept and save the settings, click the *Apply/Save* button.

4.2.5 The “Parental Control” Submenu. Parental Control—Restrictions Configuration

4.2.5.1. The “Time Restriction” Submenu. Configuration of Session Time Restriction

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 a 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
Mummy	08:60:6e:d7:73:30	x	x	x	x	x			16:30	23:59	<input type="checkbox"/>

Click the *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 checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

- *User Name*—user name;
- *Browser's MAC Address*—MAC address, which is automatically identified for the computer the schedule is set for;
- *Other MAC Address (xx:xx:xx:xx:xx:xx)*—MAC address, which is manually defined for the computer the schedule is set for;
- *Days of the week*—days of the week when Internet access will be restricted;
- *Start Blocking Time (hh:mm)*—time when the access restriction starts, hh:mm;
- *End Blocking Time (hh:mm)*—time when the access restriction ends, hh:mm.

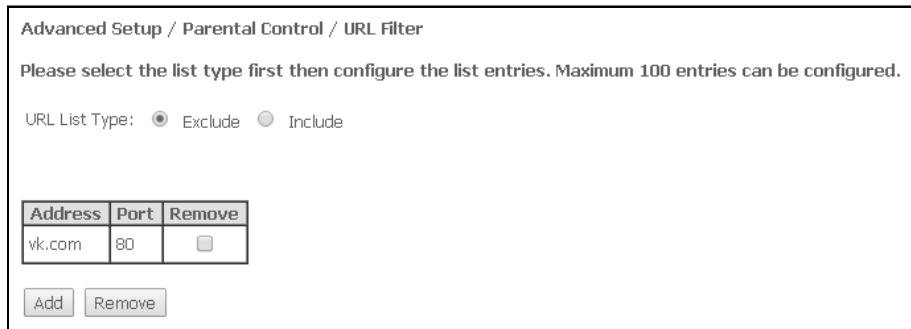


The restrictions apply if the correct system time is set for the device.

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

4.2.5.2. The “Url Filter” Submenu. Internet Access Restriction Settings

Url Filter—a function which performs complete analysis and provides access control to specific Internet resources. This parameter defines a list of denied/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.

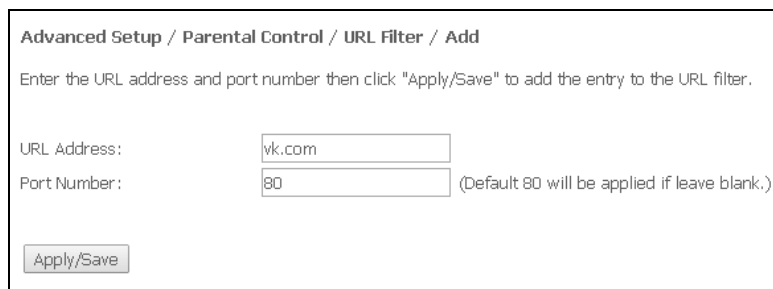
URL List Type: Exclude Include

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

Add Remove

- *URL List Type*—type of the URL list:
 - *Exclude*—denied addresses;
 - *Include*—allowed addresses;

To add a new URL to a list, set the flag in front of 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.)

Apply/Save

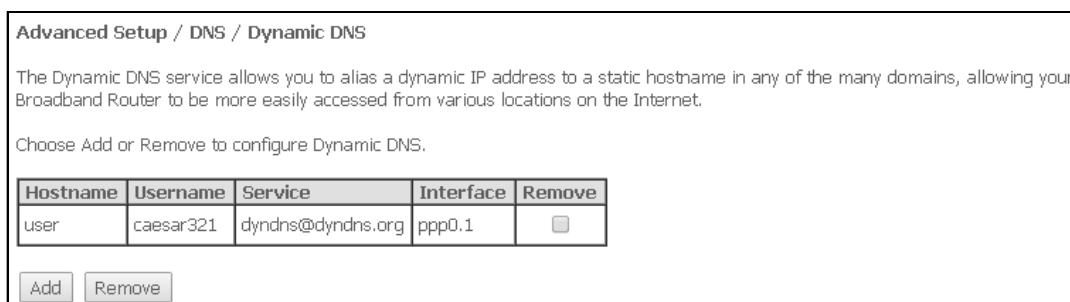
- *URL Address*—URL address;
- *Port Number*—port number (if left empty, port 80 is used).

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

4.2.6 The “Dynamic DNS” menu. The Dynamic DNS settings

Dynamic DNS (dynamic domain name system) allows DNS server information to be updated in real time and (optionally) automatically. It is used to assign a fixed domain name to a device (computer or router, e. g. NTP-RG) with a dynamic IP address. This dynamic IP address can be obtained through IPCP in PPP connections or through DHCP.

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



Advanced Setup / DNS / 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
user	caesar321	dyndns@dyndns.org	ppp0.1	<input type="checkbox"/>

Add Remove

To add a record, click the *Add* button; to remove a record, click the *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*—select a type of the 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*—any other provider selected by the user. In this case, the user will need to specify manually 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

Hostname

Interface

Custom DDNS provider

Username

Password

DDNS Provider Server Name

DDNS Provider URL

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

Depending on the chosen provider the following fields are available:

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

D-DNS provider: TZO.com

Hostname:

Interface: VoIP.1101/veip0.2

TZO Settings

Email:

Key:

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

D-DNS provider: freedns.afraid.org

Hostname:

Interface: VoIP.1101/veip0.2

freedns.afraid.org Settings

Username:

Password:

Advanced Setup / DNS / 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: VoIP.1101/veip0.2

DynDNS Settings

Username:

Password:

DynDNS Type: Dynamic

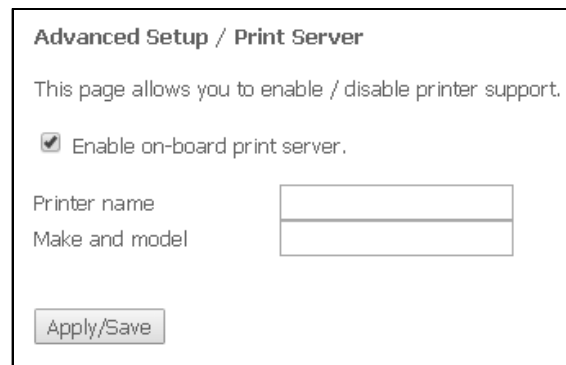
Wildcard:

- *Username*—user name for the DDNS account;
- *Password*—password for the DDNS account;
- *DynDNS Type*—select the type of the service registered at the provider:
 - *Dynamic*—Dynamic DNS service registered;
 - *Static*—Static DNS service registered;
 - *Custom*—Custom DNS service registered;
- *Wildcard*—when checked, a special DNS record is used which is responsible for all subdomains and corresponds to any request to a non-existing domain name. It is indicated as * in the subdomain field, for example *.domain.tld.
- *Email*—email used for authentication;
- *Key*—DDNS account key.

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

4.2.7 The “Print Server” menu¹. Print Server Configuration

The print server is a software or hardware solution that allows users of wired or wireless networks to share a printer at home or at an office. The printer is completely independent from network computers and decreases the load on the user’s working environment. Besides, the print server establishes continuous communication to the printer, AIO, scanner, and other office machines located in the LAN.

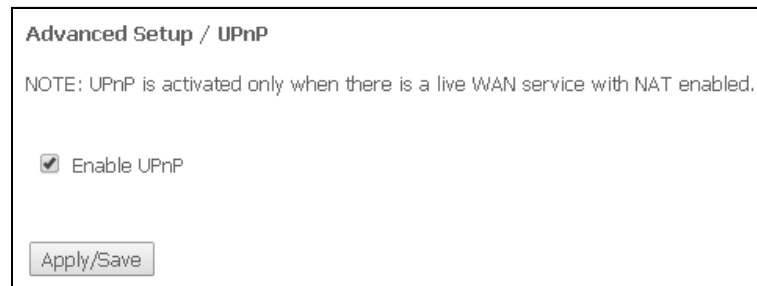


- *Enable on-board print server*—when checked, the print server is enabled, otherwise it is disabled;
- *Printer name*—name of the printer;
- *Make and model*—manufacturer and model of the printer.

To accept and save the settings, click the *Apply/Save* button.

4.2.8 The “UPnP” menu. Automatic setup of Network Devices

Use the menu to configure Universal Plug and Play (UPnP™). UPnP ensures compatibility with network equipment, software and peripheral devices.




Configure NAT on an active WAN interface to use UPnP.

Set the *Enable UPnP* to enable UPnP.

To accept and save settings, click the *Apply/Save* button.

¹ Only for NTU-2W, NTU-RG-1402G-W

4.3 The “Voice” menu. SIP settings¹

4.3.1 The “SIP Basic Setting” submenu. Common SIP settings

Voice / SIP Basic Settings

Service Provider 0

Locale selection*: (Note: Requires vodsl restart to take affect)

SIP domain name*:

Voip Dialplan Setting:

Use SIP Proxy.

SIP Proxy:

SIP Proxy port:

Use SIP Outbound Proxy.

SIP Outbound Proxy:

SIP Outbound Proxy port:

Use SIP Registrar.

SIP Registrar:

SIP Registrar port:

SIP Account	1	2
Enable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Number	<input type="text" value="4810"/>	<input type="text" value="4811"/>
Display name	<input type="text" value="4810"/>	<input type="text" value="4811"/>
Authentication name	<input type="text" value="4810"/>	<input type="text" value="4811"/>
Password	<input type="text" value="*****"/>	<input type="text" value="*****"/>
Preferred ptime	<input type="text" value="20"/>	<input type="text" value="20"/>
Preferred codec 1	<input type="text" value="G.711ALaw"/>	<input type="text" value="G.711ALaw"/>
Preferred codec 2	<input type="text" value="-"/>	<input type="text" value="-"/>
Preferred codec 3	<input type="text" value="-"/>	<input type="text" value="-"/>
Preferred codec 4	<input type="text" value="-"/>	<input type="text" value="-"/>
Preferred codec 5	<input type="text" value="-"/>	<input type="text" value="-"/>
Preferred codec 6	<input type="text" value="-"/>	<input type="text" value="-"/>

- *Local selection* – location selection;
- *SIP domain name* – SIP domain name;
- *VoIP Dialplan Setting* – dialplan configuration (recommended to use 'x.T')
- *Use SIP Proxy* – when checked SIP Proxy is used:
 - *SIP Proxy* – SIP Proxy address;
 - *SIP Proxy port* – SIP Proxy port;
- *Use SIP Outbound Proxy* – when checked, use SIP Outbound-proxy to transmit all requests otherwise SIP Outbound-proxy is not used:
 - *SIP Outbound Proxy* – SIP proxy address which will be used to transfer all requests (this server will be used for routing SIP Proxy and SIP Registrar);
 - *SIP Outbound Proxy port* – SIP proxy port for transmitting all requests;
- *Use SIP Registrar* – when checked, use SIP registrar server :
 - *SIP Registrar* – server address;
 - *SIP Registrar port* – server port;

The table shows SIP parameters that are common for FXS ports.

¹ SIP settings are available for NTU-2V(C) and NTU-RG-1402G-W only. If this menu is absence in the configurator it means settings have already been completed by your service provider.

- *SIP Account* – SIP account (FXS port number);
- *Enable* – when checked, the port is enabled for operation;
- *Number* – phone number;
- *Display name* – username displayed;
- *Authentication name* – username for authentication;
- *Password* – password for authentication;
- *Preferred ptime* – amount of voice data transmitted by one RTP packet (in milliseconds);
- *Preferred codec* – select the preferred codec (1 – with the highest priority).

To accept and save settings, click the *Apply/Save* button.

4.3.2 The “SIP Advanced Settings” submenu

Use this submenu to configure Value Added Services (for more detailed description see APPENDIX B. VALUE ADDED SERVICES USAGE).

Voice / SIP Advanced Settings

Service Provider 0

SIP Account	1	2
Call waiting	<input type="checkbox"/>	<input type="checkbox"/>
Call hold	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Call forwarding number		
Forward unconditionally	<input type="checkbox"/>	<input type="checkbox"/>
Forward on "busy"	<input type="checkbox"/>	<input type="checkbox"/>
Forward on "no answer"	<input type="checkbox"/>	<input type="checkbox"/>
MWI	<input type="checkbox"/>	<input type="checkbox"/>
Call barring	<input type="checkbox"/>	<input type="checkbox"/>
Call barring mode	Allow all	Allow all
Call barring pin	9999	9999
Call barring digit map		
Warm line	<input type="checkbox"/>	<input type="checkbox"/>
Warm line number		
Warm line timeout	1000	1000
Anonymous call blocking	<input type="checkbox"/>	<input type="checkbox"/>
Anonymous calling	<input type="checkbox"/>	<input type="checkbox"/>
DND	<input type="checkbox"/>	<input type="checkbox"/>

Start SIP client

Stop SIP client

Apply/Save

- *SIP Account* – SIP account (FXS port number);
- *Call waiting* – when checked, a notification about incoming call is enabled;
- *Call hold* – when checked, call hold is enabled;
- *Call forwarding number*– call forwarding number;
- *Forward unconditionally*– when checked, unconditional forwarding is enabled;
- *Forward on 'busy'* – when checked, call forwarding on 'busy' is enabled;
- *Forward on 'no answer'*– when checked, call forwarding on 'no answer' is enabled;
- *MWI* – when checked, message waiting indicator for voice mail is enabled;
- *Call barring* – when checked, a subscriber can bar outgoing messages;
- *Call barring mode* – call barring mode;
- *Call barring pin* – password for outgoing calls;
- *Call barring digit map* – digit map which allows/bars outgoing calls;

- *Warm line* – when checked, ‘Warm Line’ service is enabled, otherwise the service is disabled. The service allows you to establish an outgoing connection automatically without dialing the number right after the lifting of a headset (*hot line*), or with delay (*warm line*);
- *Warm line number* – warm line number;
- *Warm line timeout* – a delay before warm line dialing;
- *Anonymous call blocking* – when checked, blocking of calls from subscribers whose numbers were not identified is enabled;
- *Anonymous calling* – when checked, calls from port number are not identified (Caller Identity Restriction service);
- *DND* – when checked, ‘Do Not Disturb’ service is enabled.

To accept and save the settings, click the *Apply/Save* button.

To apply the new settings, stop SIP client by clicking *Stop SIP client* button and start SIP client again by clicking *Start SIP client* button.

4.4 The “Wireless” Menu¹. Wi-Fi Network Setup

4.4.1 The “Basic” submenu. General information

This menu is used for general setup of the LAN wireless interface and allows users 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

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 type="checkbox"/>	<input type="text" value="wID_Guest1"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="wID_Guest2"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="wID_Guest3"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="16"/>	N/A

- *Enable Wireless*—enable Wi-Fi on the device;
- *Hide Access Point*—hidden operation mode of the access point (in this mode, the router does not broadcast wireless network SSID);
- *Clients Isolation*—when checked, disables interaction between wireless clients;
- *Disable WMM Advertise*—disable WMM (Wi-Fi Multimedia—QoS for wireless networks);
- *Enable Wireless Multicast Forwarding (WMF)*—enables wireless multicast forwarding (WMF);

¹ Only for NTU-2W, NTU-RG-1402G-W

- SSID—*Service Set Identifier*—assign a name to the wireless network (case sensitive);



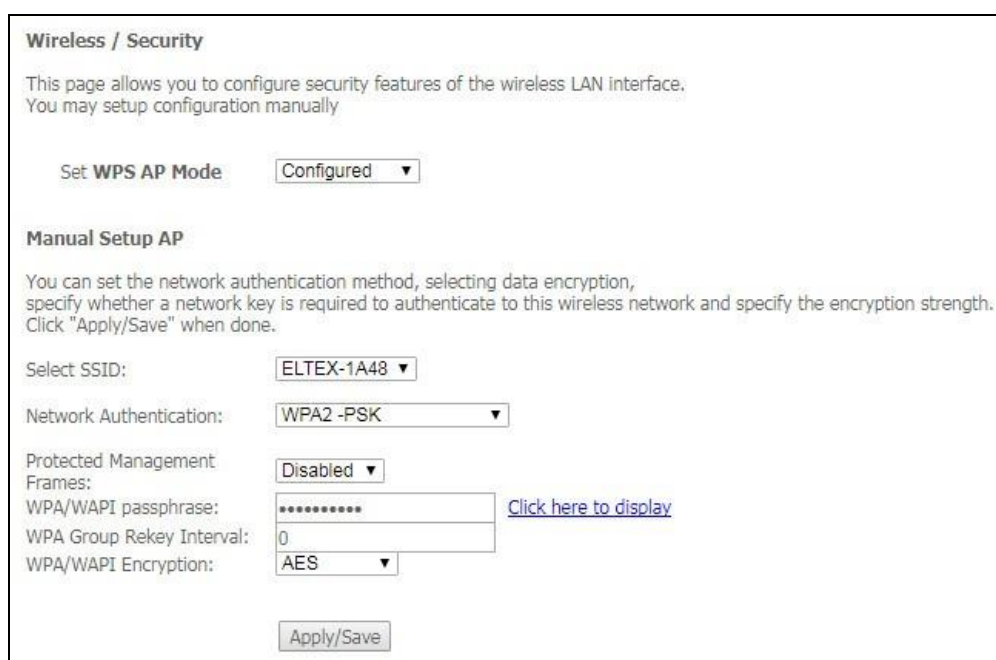
The default name (SSID) of the wireless network is ELTEX-aaaa where aaaa are the last 4 digits of WAN MAC. WAN MAC is labelled on the device housing. The WAN MAC is labelled on the device housing.

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

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

4.4.2 The “Security” Submenu. Security Settings

The menu contains main parameters of data encryption in the wireless network. The client wireless equipment can be configured either manually or automatically with the help of WPS.



WPS (Wi-Fi Protected Setup) is a standard created by Wi-Fi Alliance in order to simplify the configuration of wireless networks. This technology allows the user to perform quick, easy, and secure configuration of a wireless network without getting into the complexity of Wi-Fi and encryption protocols operation. WPS automatically sets the network name and configures data encryption to protect the network from unauthorised access.

These operations should be manually performed without WPS. To establish a connection, the user simply needs to press the WPS button located on the side panel of the device or use web configuration to enter a PIN code.

- Set WPS AP Mode—set the WPS mode of the access point.

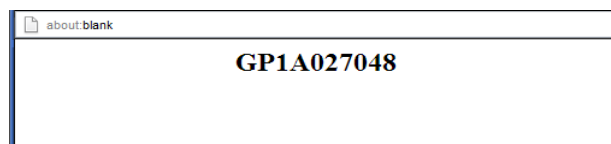


Disadvantages of WPS

Wi-Fi routers supporting WPS technology have a network security vulnerability. The vulnerability can be used to crack passwords of the WPA and WPA2 encryption protocols. It involves brute forcing of the 8-digit network key (PIN code).

Manual Setup AP:

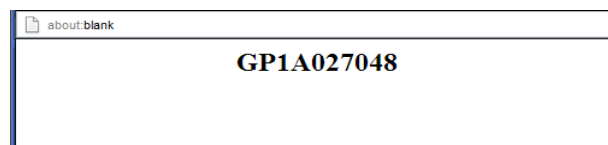
- *Select SSID*—select a name of a wireless network from the list;
- *Network Authentication*—select a network authentication mode from the drop-down list:
 - *open*—without wireless network security features (only WEP key can be used in this mode);
 - *Shared*—this mode enables user authentication by 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*—IP address of the RADIUS server;
 - *RADIUS Port*—port number of the RADIUS server. The default port is 1812;
 - *RADIUS Key*—secret key for access to the RADIUS server;
 - *WPA2*—enable WPA2 (this mode uses WPA2 protocol and requires a RADIUS authentication server);
 - WPA2 Preauthentication;
 - Network Re-auth Interval;
 - *WPA Group Rekey Interval*—the period of time (in seconds) between automatic changes of WPA encryption keys; used to strengthen wireless network security. If no key changes are required, set this field to 0.
 - *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*—secret key for access to the RADIUS server;
 - *WPA/WAPI Encryption*—select a WPA/WAPI data encryption method: TKIP+AES, AES:
 - TKIP—encryption protocol for WPA. It enables more efficient management of key changes compared to WEP;
 - AES—128-bit block encryption algorithm with 128/192/256-bit key, generally used for WPA2;
 - *WPA2-PSK*—enables WPA2-PSK (the mode uses the WPA2 protocol but does not require the RADIUS authentication server);
 - *WPA/WAPI passphrase*—secret phrase. Sets a password; a string of 8–63 ASCII characters. Follow the [Click here to display](#) link to show the secret phrase; the password will be displayed in a pop-up window.



The network key corresponds to the device serial number by default. The serial number is labelled on the device housing. When you change the password, you will need to specify a combination of 10 characters. The password must contain digits and Latin characters in upper and lower cases.

- *WPA Group Rekey Interval*—the period of time (in seconds) between automatic changes of WPA encryption keys; used to strengthen wireless network security. If no key changes are required, set this field to 0.
- *WPA/WAPI Encryption*—select a WPA/WAPI data encryption method: TKIP+AES, AES:
 - TKIP—encryption protocol for WPA. It enables more efficient management of key changes compared to 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 requires a RADIUS authentication server and uses WPA2 and WPA protocols);
 - *WPA2 Preauthentication* – pre-authentication of the wireless client in other wireless access points in the specified range. Connection is established at the current wireless access point during the verification
 - *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 correct 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 no key changes are required, set this field to 0.
 - *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*—secret key for access to the RADIUS server;
 - *WPA/WAPI Encryption*—select a WPA/WAPI data encryption method: TKIP+AES, AES:
 - TKIP—encryption protocol for WPA. It enables more efficient management of key changes compared to 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 a RADIUS authentication server).
 - *WPA/WAPI passphrase*—secret phrase. Sets a password; a string of 8–63 ASCII characters. Follow the *Click here to display* link to show the secret phrase; the password will be displayed in a pop-up window.



The network key corresponds to the device serial number by default. The serial number is labelled on the device housing. When you change the password, you will need to specify a combination of 10 characters. The password must contain digits and Latin characters in upper and lower cases.

- *WPA Group Rekey Interval*—the period of time (in seconds) between automatic changes of WPA encryption keys; used to strengthen wireless network security. If no key changes are required, set this field to 0.
- *WPA/WAPI Encryption*—select a WPA/WAPI data encryption method: TKIP+AES, AES:
 - TKIP—encryption protocol for WPA. It enables more efficient management of key changes compared to WEP;
 - AES—128-bit block encryption algorithm with 128/192/256-bit key, generally used for WPA2;



Make sure that the PC's wireless adapter supports the selected encryption type. The most secure protection of a wireless channel is reached by the joint operation of access point and RADIUS server (for authentication of wireless clients).

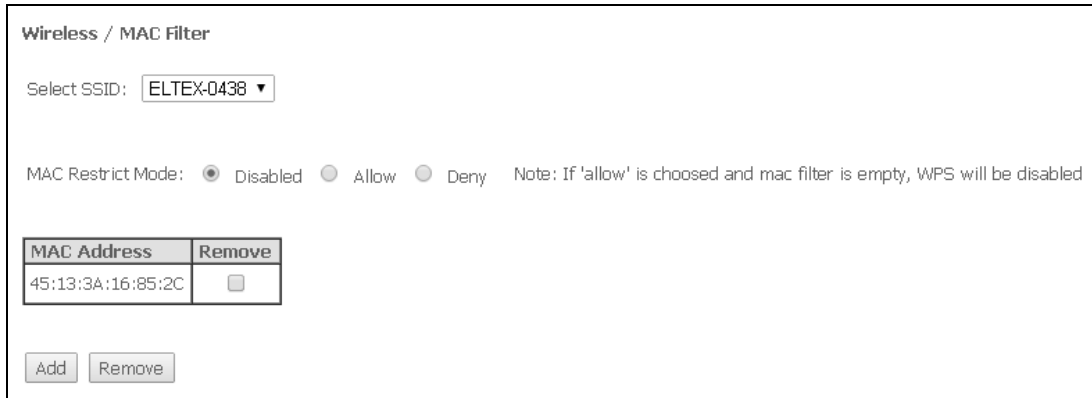
- *WEP Encryption*—select Enable in the drop down list to enable WEP encryption;
 - *Encryption Strength*—64- or 128-bit key encryption;
 - *Current Network Key*—the key that will be used for connection;

- *Network Key 1..4*—allows specification of 4 different keys, which comprise of 10 hex characters of 5 ASCII characters¹ for 64-bit encryption. Other options are 26 hex characters or 13 ASCII characters for 128-bit encryption.

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

4.4.3 The “MAC Filter” Submenu. MAC Address Filtering Settings

Use this menu to configure MAC Address Filtering.



Wireless / MAC Filter

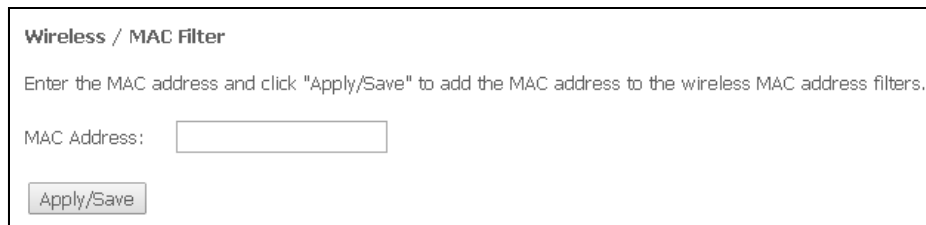
Select SSID:

MAC Restrict Mode: Disabled Allow Deny Note: If 'allow' is choosed and mac filter is empty, WPS will be disabled

MAC Address	Remove
45:13:3A:16:85:2C	<input type="checkbox"/>

- *Select SSID*—select identifier for a wireless network a rule is created for;
- *MAC Restrict Mode*—select a MAC address filtration mode:
 - *Disabled*—no filter;
 - *Allow*—filter by allowed addresses;
 - *Deny*—filter by denied addresses.

To add a MAC address into the filter table, click the *Add* button and enter its value into the MAC address field in the displayed menu:



Wireless / MAC Filter

Enter the MAC address and click "Apply/Save" to add the MAC address to the wireless MAC address filters.

MAC Address:

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

¹ ASCII is a 128-character set designed for machine representation of the Latin characters in the lower and upper case, numbers, punctuation marks, and special symbols.

4.4.4 The “Wireless Bridge” Submenu. Configuration of Wireless Connection in the Bridge Mode

The menu specifies an operation mode of access point: either access point or wireless bridge.

Using the bridge mode requires MAC addresses of remote bridges to be specified. The mode is used for wireless connection between two independent 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:

The Wireless Bridge mode has the following settings:

- *Bridge Restrict*—select a bridge operation mode:
 - *Enabled*—enable the MAC address filter (allowed are only the specified addresses);
 - *Enable (Scan)*—search for remote bridges;
 - *Disable*—no restrictions for MAC addresses;
- *Remote Bridges MAC Address*—addresses of remote bridges.



The router doesn't support the Wi-Fi Multimedia (WMM) function in the bridge mode.

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

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

4.4.5 The “Advanced” Submenu. Advanced Settings

The menu allows advanced configuration of 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: Current: 9 (interference: acceptable)

Channel:

Auto Channel Timer(min):

Auto Channel Set:

Allowed Channels:

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:

Bandwidth: Current: 20MHz

Control Sideband: Current: N/A

802.11n Rate:

802.11n Protection:

Support 802.11n Client Only:

RIFS Advertisement:

RX Chain Power Save: Power Save status: Full Power

RX Chain Power Save Quiet Time:

RX Chain Power Save PPS:

54g™ Rate:

Multicast Rate:

Basic Rate:

Fragmentation Threshold:

RTS Threshold:

DTIM Interval:

Beacon Interval:

Global Max Clients:

XPress™ Technology:

Transmit Power:

Transmit Power Boost:

WMM(Wi-Fi Multimedia):

WMM No Acknowledgement:

WMM APSD:

Enable Traffic Scheduler:

Airtime Fairness:

- **Band**—frequency coverage¹;
- **Channel**—select an operating channel for the router. Interference or any other issues of a wireless network may be solved by changing the channel. The parameter is recommended to be set to Auto to avoid interference caused by adjacent networks;
- **Auto Channel Timer (min)**—the time before the router searches for a better wireless channel. The parameter is available when the Auto channel is selected (enter 0 to disable);
- **Auto Channel Set**—defines a channel autoselection mode:
 - **Full**—autoselection scans all available channels to choose one;
 - **Legacy**—autoselection scans a set of channels supported by old devices (for 2.4 GHz range only) to choose one;
 - **Custom**—autoselection scans channels from the list specified by user in the Allowed Channel settings and chooses one.

¹ NTU-RG-1402G-W models support 2.4GHz, NTU-RG-1402G-Wac models – 2.4/5GHz

- *802.11n/EWC*—compatibility mode for 802.11n Draft2.0 and EWC (Enhanced Wireless Consortium) equipment;
- *Bandwidth*—bandwidth of 20 MHz or 40 MHz. When set to 40 MHz, 2 adjacent bandwidths of 20 MHz are used to broaden the channel's throughput;
- *Control Sideband*—select the second channel (Lower or Upper) in 40 MHz mode;
- *802.11n Rate*—select connection rate;
- *802.11n Protection*—when enabled, enhances the security, but decreases the bandwidth;
- *Support 802.11n Client Only* – when enabled, denies 802.11b/g clients to access the device;
- *RIFS Advertisement*—Reduced Interframe Space, reduces the interval between data units (PDUs), increases Wi-Fi efficiency;
- *RX Chain Power Save* – disables one of the device's antennas to save energy;
- *RX Chain Power Save Quiet Time*—time period when the traffic intensity should be less than the PPS value to activate the power saving function;
- *RX Chain Power Save PPS*—upper limit of the PPS parameter (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 activated.
- *54g™ Rate*—set the transfer rate in 54g™ compatibility mode;
- *Multicast Rate*—set the transfer rate for multicast traffic;
- *Basic Rate*—basic transfer rate;
- *Fragmentation Threshold*—set the fragmentation threshold, in bytes. If a packet size exceeds the value, the packet is fragmented into parts of the corresponding size;
- *RTS Threshold*—if the packet is smaller than the RTS threshold value, the RTS/CTS mechanism (with request to send/clear to send packets) is not used;
- *DTIM Interval*—time period after which the broadcast and multicast packets in the buffer will be delivered to wireless clients;
- *Beacon Interval*—time period for transmission of informational packets, which indicate activity of the access point, to the wireless network;
- *Global Max Clients*—maximum possible number of wireless clients;
- *XPress™ Technology*—provides an increase in throughput in 802.11g networks up to 27 %. XPress™ Technology can increase the throughput up to 75 % in mixed networks (802.11g and 802.11b).
- *Transmit Power*—define the signal power of the access point;
- *Transmit Power Boost* —high signal power of the access point; It is not recommended to use.
- *WMM (Wi-Fi Multimedia)*—enables the Wi-Fi Multimedia (WMM) mode. The mode allows the 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 does not acknowledge the received packets. This increases transmission efficiency of low-interference medium, however decreases the efficiency of high-interference one;
- *WMM APSD*—set automatic transition into the power saving mode (if enabled, automatic transition is allowed);
- *Enable Traffic Scheduler* – use client indicators to balance broadcast usage by directions;
- *Airtime Fairness (ATF)* – function for reducing the negative impact of a slow devices to bandwidth of a wireless network.

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

4.5 The “Storage Service” menu¹. File Storage Service

4.5.1 The “Storage Device Info” submenu. Connected USB Device Info

Use the menu to view the list with all connected data 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
usb1_1	fat	3854	163	Unmount

- *Volumename* – device name;
- *FileSystem* – file system type;
- *Total Space* – total space;
- *Used Space* – used space;
- *Unmount* – a button for device safe disconnection or connection.

4.5.2 The “User Accounts” submenu. Configuration of Samba users

Use the menu to configure Samba accounts.

Storage Service / User Accounts		
Choose Add, or Remove to configure User Accounts.		
UserName	HomeDir	Remove
test	usb1_1/test	<input type="checkbox"/>

Add Remove

Click *Add* button to add a record. To remove a record, select the checkbox in front of the required record in the *Remove* column and click *Remove* button.

- *Username* – username to access a network resource;
- *Password* – password to access a network resource;
- *Confirm Password* – access password confirmation;
- *VolumeName* – path to the network resource (name of the connected storage is displayed in the *Storage Device Info* tab).

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

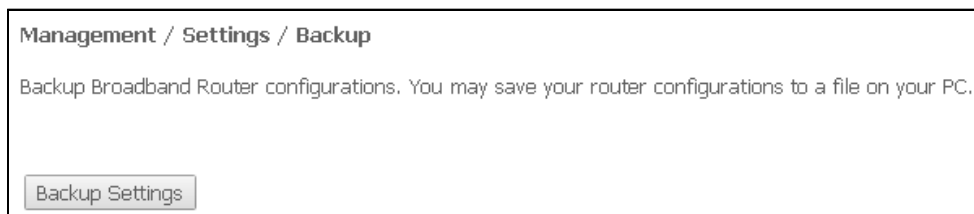
¹ Only for NTU-2W, NTU-RG-1402G-W

4.6 The “Management” menu. Device Management

4.6.1 The “Settings” submenu. Settings

4.6.1.1. The “Backup” submenu. Backup

Use the *Backup Settings* button in this menu to download configuration to a PC.

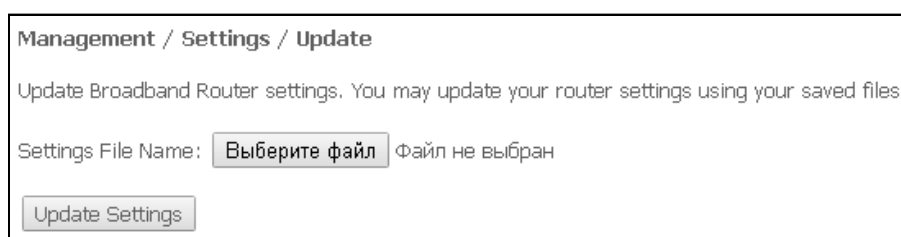


4.6.1.2. The “Update” submenu. Configuration Update

To update configuration, select a configuration file in the *Settings File Name* field (use the *Choose a File* or *Browse* buttons) and click *Update Settings*.

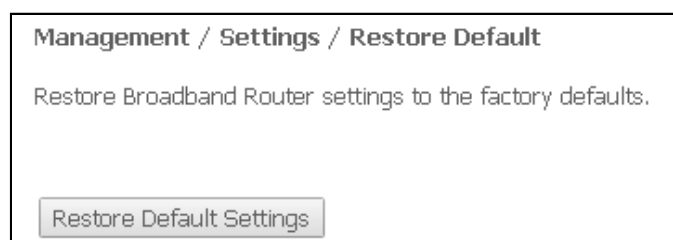


Do not switch off or reboot the device during the update. The process may take several minutes. The device will be automatically rebooted when the update is completed.



4.6.1.3. The “Restore Default” Submenu. Restore Default Settings

The menu restores the default settings. The device will be rebooted in this case.



When 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.

4.6.2 The “PON Password” Submenu. Changing PON Network Password

Use this menu to change the password, which is used for ONT authorisation on a station-side device of a passive optical network.

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 in the *New PON Password* field. Click the *Apply/Save* button to accept and save the changes. The settings will be applied after device restart.



We do not recommend to change the password as the link to the station-side device may be lost in this case.

4.6.3 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:

Second NTP time server:

Third NTP time server:

Fourth NTP time server:

Fifth NTP time server:

Time zone offset:

The tab contains settings for the device system time.

- *Automatically synchronize with Internet time servers* – when checked, time automatically synchronises with Internet time servers;
- *First NTP time server* – select the primary time server;
- *Second NTP time server* – select the second time server (none—do not use additional servers);
- *Third NTP time server* – select the third time server (none—do not use additional servers);
- *Fourth NTP time server* – the fourth time server (none—do not use additional servers);
- *Fifth NTP time server* – select the fifth time server (none—do not use additional servers);;
- *Time zone offset* – set the 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 time server can be manually entered.

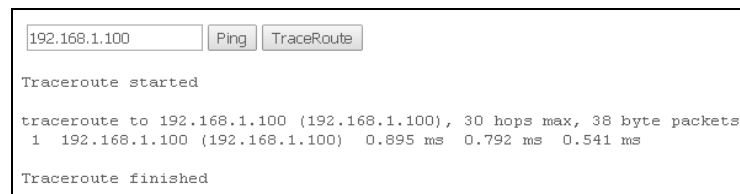
Click the *Apply/Save* button to accept and save the changes.

4.6.4 The “Ping” Submenu. Checking the Availability of the Network Devices

The menu is intended for using the Ping utility to check availability of the network devices connected to the router.

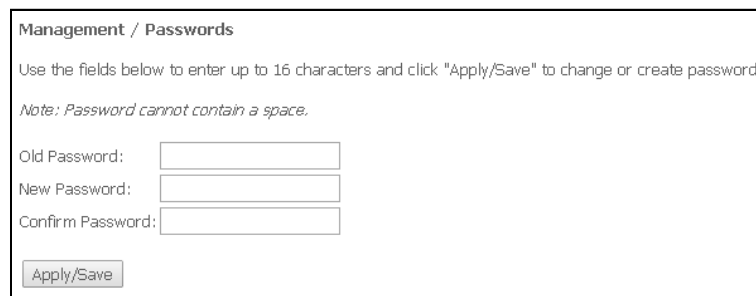


To test the availability of the connected device, enter its IP address into the field and click the *Ping* button. Click the *TraceRoute* button to view the route tracing. Results will be displayed at this page of web configurator.



4.6.5 The “Passwords” Submenu. Access Control Settings (password settings)

Use this submenu to change the device access password.



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

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

4.6.6 The “System Log” Submenu. Display and Configuration of the System Log

4.6.6.1. The “Configuration” Submenu. System Log Configuration

Use this menu to configure the router events.

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:

Display Level:

Mode:

Linux Kernel Console Display Level (printk):

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

Press “View System Log” button to display the system log.

- *Log*—enable/disable system log;
- *Log Level* – sets the verbosity of the event log. Severity levels are in the descending order:
 - *Emergency*;
 - *Alert*;
 - *Critical*;
 - *Error*;
 - *Warning*;
 - *Notice*;
 - *Informational*;
 - *Debugging*;
- *Display Level*—display level of the event log messages;
- *Mode*—mode of the log operation:
 - *Local*—local (all events return to the router via the internal buffer);
 - *Remote*—remote (all events return to Syslog server);
 - *Both*—both modes are enabled;
 - *Flash*—sends events to a USB drive;
- *Linux Level Console Display Level (printk)*—set the Linux console logging level;
- *Send CMS logs to syslog (require reboot)*—enables/disables CMS messages transmission to the system log.

The following settings are available in the Remote mode:

- *Server IP address*—IP address of a Syslog server, which stores all the events;
- *Server IP Port*—Syslog server port number.

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

4.6.6.2. The “View” Submenu. System Log Display

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

Management / System Log / View

Date/Time	Facility	Severity	Message
Jan 1 00:01:00	syslog	emerg	#####
Jan 1 00:01:00	syslog	emerg	## syslogd started: BusyBox v1.17.2 ##
Jan 1 00:01:00	syslog	emerg	#####
Jan 1 00:01:00	kern	err	kernel: i2c i2c-0: Failed to register i2c client gpon_i2c at 0x50 (-16)
Jan 1 00:01:00	kern	err	kernel: i2c i2c-0: Failed to register i2c client gpon_i2c at 0x50 (-16)
Jan 1 00:01:00	kern	err	kernel: i2c i2c-0: Failed to register i2c client gpon_i2c at 0x51 (-16)
Jan 1 00:01:00	kern	err	kernel: i2c i2c-0: Failed to register i2c client gpon_i2c at 0x51 (-16)
Jan 1 00:01:00	kern	err	kernel: sd 0:0:0:0: [sda] No Caching mode page present
Jan 1 00:01:00	kern	err	kernel: sd 0:0:0:0: [sda] Assuming drive cache: write through
Jan 1 00:01:00	kern	err	kernel: sd 0:0:0:0: [sda] No Caching mode page present
Jan 1 00:01:00	kern	err	kernel: sd 0:0:0:0: [sda] Assuming drive cache: write through
Jan 1 00:01:00	kern	err	kernel: sd 0:0:0:0: [sda] No Caching mode page present
Jan 1 00:01:00	kern	err	kernel: sd 0:0:0:0: [sda] Assuming drive cache: write through
Jan 1 00:01:00	kern	crit	kernel: eth0 Link UP 1000 mbps full duplex
Jan 1 00:01:02	kern	crit	kernel: eth0 Link DOWN.
Jan 1 00:01:06	kern	crit	kernel: eth0 Link UP 1000 mbps full duplex

Refresh

Click *Close* to close the log display window. Use the *Refresh* button to refresh the information.

4.6.7 The “Update Software” Submenu. Software Update

To update software, select the software in the *Software File name* field (use the *Choose a File* or *Browse* buttons) and click *Update Software*.



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

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: Файл не выбран

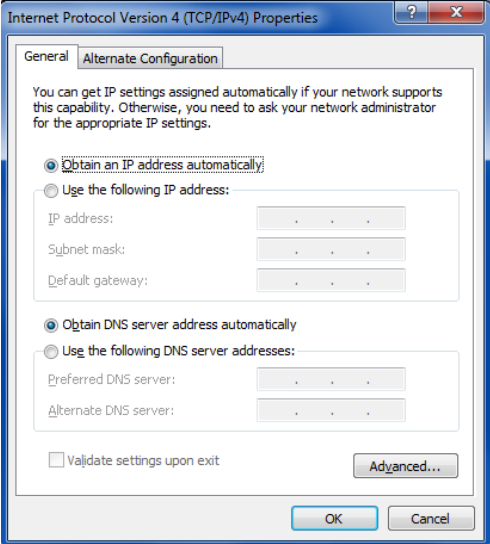
4.6.8 The “Reboot” Submenu. Device Reboot

Management / Reboot

Click the button below to reboot the router.

Click the *Reboot* button to reboot the device. The device reboot may take several minutes.

APPENDIX A. POSSIBLE PROBLEMS AND THEIR SOLUTIONS

Problem	Possible Cause	Solution
Web interface is not available when the router IP address entered (e. g. 192.168.1.1)	The computer is not in the same IP subnetwork for connection to the web interface.	Select the <i>Obtain an IP address automatically</i> checkbox in the Internet connection settings on your PC. 
	Javascript is disabled in the web browser installed on the PC.	Enable Javascript in the web browser or use another web browser.
	Defective cable	Check the physical connection by checking status LEDs (all LEDs should be on). If the LEDs are off, use another cable or connect to another port of the device if available. If your computer is switched off, LEDs may also be off.
	Access is denied by some Internet security software installed on your PC.	Disable the Internet security software (firewalls) installed on your PC.
Error signal in the phone connected to the FXS port	Invalid port configuration	Check settings in the VoIP menu (see section 4.3.2 “SIP Advanced Settings” submenu).
The password to web interface of the device is lost or does not work.	_____	Reset the router to default settings using the F button on the rear panel. Unfortunately, all changes you made in the settings will be lost in this case.

APPENDIX B. ADDITIONAL SERVICE

1. Call Waiting

The service uses a definite signal to notify user about a new incoming call when the line is already busy with another call.

Having received the signal, the user may decide to pick up the waiting call.

The service can be chosen by setting *Call waiting* flag in the *VoIP/SIP Advanced Setting* menu (see section **4.3.2 “SIP Advanced Settings”** submenu).

Service usage:

When you receive the new call notification while you are already talking, press R to hold the current call and take the waiting one. All further pressing R button will be processed according to the algorithm described in sections **2** Call transfer and **3** Conference.

- R – flash.

2. Call transfer

The *Calltransfer* service allows temporary interruption of connection with active subscriber (subscriber A), connection to another subscriber (subscriber C), and transfer of the call with disconnection of subscriber B (the subscriber providing the service).

Service usage:

While being connected to the subscriber A, hold the call by pressing the flash release (R), wait for the *station response* signal, and dial the subscriber C. When the subscriber C answers your call, hang up.

3. Conference

Conference is a service allowing three and more subscribers to have shared phone conversation. The service can be chosen by setting *Call waiting* flag in the *VoIP/SIP Advanced Setting* menu (see section **4.3.2 “SIP Advanced Settings”** submenu).

Service usage:

While being connected to the subscriber A, hold the call by pressing the flash release (R), wait for the *station response* signal, and dial the subscriber C. When the subscriber C answers your call, press R to switch to the conference mode.

The subscriber who starts the conference is a chairperson; the rest two subscribers are participants. When the chairperson presses flash release in the conference mode, the last called subscriber is disconnected. A participant may put on hold other participants.

The conference ends when the chairperson hangs up; the rest two participants will receive the release signal in this case. If a participant leaves the conference, the chairperson and another participant are switched to a normal two-party call.

4. Message Waiting Indication (MWI)

If a voice message is left on the server for a subscriber, the service allows the subscriber to be timely notified about the message. When the MWI service is enabled and there is a new message on the server, the subscriber will hear a discontinuous buzzer when he picks up the phone.

In order to enable the MWI service, set the flag in the MWI field of the corresponding port on the *VoIP/SIP Advanced Setting* tab (see section 4.3.2 “SIP Advanced Settings” submenu).

5. Call Barring

The service allows phone access restriction to a certain types of outgoing calls.

The service can be configured in the menu with user port settings in the *VoIP/SIP Advanced Setting* tab (see section 4.3.2 “SIP Advanced Settings” submenu) by setting the *Call barring* flag and specifying the required parameters in the *Call barring mode* and *Call barring digit map* fields.

Three options of calls restriction are available depending on the parameter specified in the *Call barring mode* field:

- *Allow all* – all outgoing calls are allowed;
- *Deny all* – all outgoing calls are denied;
- *Deny by digit map* – denied are only the calls to the number specified in the *Call barring digit map* field.

Service usage:

‘*Call barring digit map*’ value is 1150. In order to deny all outgoing calls, choose the *Deny all* option in the *Call barring mode* field. In order to deny all calls to 1150, specify *Deny by digit map* in the *Call barring mode* field.

NTU-RG ACCEPTANCE CERTIFICATE AND WARRANTY

NTU-RG optical network terminal with serial number _____ meets the requirements of technical specifications TU6650-101-33433783-2013, TU6650-108-33433783-2014 and is classified as fit for operation.

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

The manufacturer, Eltex Ltd., guarantees that the subscriber gateway meets the requirements of technical specification TU6650-100-33433783-2013 provided its operation conditions correspond to the ones set forth in this Manual.

Warranty period—1 year. Manufacturing date—see on the package.

The device does not contain precious materials.

Director

signature

A. N. Chernikov

full name

Quality Control Director

signature

S. I. Igonin

full name

Manufacturer:
Eltex Ltd.
29v Okruzhnaya St.,
Novosibirsk
630020
E-mail: eltex@eltex.nsk.ru

Made in Russia



CAUTION!
LASER RADIATION

NTU-2V ACCEPTANCE CERTIFICATE AND WARRANTY

NTU-2V optical network terminal with serial number _____ meets the requirements of technical specification TU6650-100-33433783-2013 and is classified as fit for operation.

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

The manufacturer, Eltex Ltd., guarantees that the subscriber gateway meets the requirements of technical specification TU6650-100-33433783-2013 provided its operation conditions correspond to the ones set forth in this Manual.

Warranty period—1 year. Manufacturing date—see on the package.

The device does not contain precious materials.

Director

signature

A. N. Chernikov

full name

Quality Control Director

signature

S. I. Igonin

full name

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



Made in Russia

NTU-2VC ACCEPTANCE CERTIFICATE AND WARRANTY

NTU-2VC optical network terminal with serial number _____ meets the requirements of technical specification TU6650-100-33433783-2013 and is classified as fit for operation.

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

The manufacturer, Eltex Ltd., guarantees that the subscriber gateway meets the requirements of technical specification TU6650-100-33433783-2013 provided its operation conditions correspond to the ones set forth in this Manual.

Warranty period—1 year. Manufacturing date—see on the package.

The device does not contain precious materials.

Director

signature

A. N. Chernikov

full name

Quality Control Director

signature

S. I. Igonin

full name

Manufacturer:
Eltex Ltd.
29v Okruzhnaya St.,
Novosibirsk
630020
E-mail: eltex@eltex.nsk.ru

Made in Russia



NTU-2W ACCEPTANCE CERTIFICATE AND WARRANTY

NTU-2W optical network terminal with serial number _____ meets the requirements of technical specification TU6650-100-33433783-2013 and is classified as fit for operation.

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

The manufacturer, Eltex Ltd., guarantees that the subscriber gateway meets the requirements of technical specification TU6650-100-33433783-2013 provided its operation conditions correspond to the ones set forth in this Manual.

Warranty period—1 year. Manufacturing date—see on the package.

The device does not contain precious materials.

Director

signature

A. N. Chernikov

full name

Quality Control Director

signature

S. I. Igonin

full name

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

Made in Russia

