

Integrated Networking Solutions



Subscriber terminal **NTU-MD500P**

User Manual Firmware version 2.4.7

Contents

1		List of changes	4
2		Introduction	5
3		Product Description	6
3	3.1	Purpose	6
3	3.2	Overview	6
3	3.3	Technical specifications	7
3	3.4	Design	9
	3.4.1	Front panel layout	9
	3.4.2	Side and back panels of the device	.10
3	3.5	Light indication	.11
3	3.6	Delivery package	.11
4		Installing and connecting NTU-MD500P	.12
4	4.1	Operating conditions and installation procedure	.12
	4.1.1	Safety requirements	.12
	4.1.2	Installation procedure	.12
4	4.2	Connecting the device	.14
5		Device architecture	.15
6		Configuring the device via web interface. Admin access	.16
6	5.1	Status menu. Device information	.18
	6.1.1	Device submenu. General information on the device	.18
	6.1.2	IPv6 Status submenu. IPv6 System Information	.19
	6.1.3	PON submenu. Optical module status	.20
	6.1.4	LAN submenu. Information on the status of LAN interface	.21
(5.2	LAN menu. Configuring LAN interface	.21
(5.3	WAN menu. Configuring WAN interface	.22
	6.3.1	PON WAN submenu	.22
	6.3.2	VPN submenu	.23
6	5.4	Services menu. Configuring services	.26
	6.4.1	DHCP Settings submenu. Configuring DHCP	.26
	6.4.2	DNS submenu	.27
	6.4.3	Firewall submenu. Configuring the firewall	.28
	6.4.4	UPnP submenu. Automatic configuration of network devices	.33
	6.4.5	RIP submenu. Configuring dynamic routing	.34
(5.5	Advance menu. Advanced settings	35
	6.5.1	ARP Table submenu. Viewing the ARP protocol cache	.35

6.5.2	Bridging submenu. Configuring Bridging parameters	35
6.5.3	Routing submenu. Configuring routing	36
6.5.4	Interface grouping submenu. Combining interfaces into groups	37
6.5.5	IP QoS submenu. Configuring the quality of services provided (QoS)	37
6.5.6	PoE Settings submenu. Configuring PoE ports	41
6.5.7	Link mode submenu. Configuring LAN ports	42
6.5.8	Others submenu. Additional settings	42
6.5.9	IPv6 submenu. Configuring IPv6 protocol	43
6.6	Diagnostics menu	50
6.6.1	Ping submenu. Checking the availability of network devices	50
6.6.2	Traceroute submenu. Network diagnostics	50
6.6.3	System Log submenu. Logging system events	50
6.7	Admin menu	51
6.7.1	Settings submenu. Restore and reset settings	51
6.7.2	GPON Setting submenu. Configuring access to GPON	52
6.7.3	Commit/Reboot submenu. Saving changes and restarting the device	53
6.7.4	Logout submenu. Log out the account	53
6.7.5	Password submenu. Setting up access control (setting passwords)	54
6.7.6	Firmware upgrade submenu. Software Update	54
6.7.7	Remote Access submenu. Configuring remote access rules	55
6.7.8	Time zone submenu. Configuring system time	55
6.7.9	TR-069 submenu. Configuring TR-069	56
6.8	Statistics menu. Information about the traffic on the device ports	57
6.8.1	Interface submenu. Information about counters and errors	57
6.8.2	PON submenu	57

1 List of changes

Document version	Software	Release date	Changes
Version 1.1	2.4.7	09.2022	Second publication
Version 1.0	1.0.1	04.2021	First publication

2 Introduction

GPON network belongs to one of the varieties of passive optical PON networks. This is one of the most modern and effective solutions for "last mile", which allows significant savings on cable infrastructure and provides data transmission speed of up to 2.5 Gbps downlink and 1.25 Gbps uplink. The use of GPON-based solutions in access networks makes it possible to provide end users with new IP services together with traditional ones.

The main advantage of GPON is the use of a single line terminal (OLT) for multiple subscriber devices (ONT). OLT is a converter of Gigabit Ethernet and GPON interfaces, which serves to connect the PON network with higher-level data transmission networks. The ONT device is designed to connect customers' equipment to broadband access services. It can be used in residential areas and business centers.

The user manual describes the purpose, main technical specifications, configuration rules and monitoring of the optical network terminal NTU-MD500P.

Notes and Warnings

- The tips contain important information or recommendations for using and configuring the device.
- A The notes contain additional information on using and configuring the device.
- Warnings inform of the situations when actions may harm the device or a user, lead to fault operation of the device or data loss.

3 Product Description

3.1 Purpose

NTU-MD500P is an optical network terminal that has four 10/100/1000BASE-T ports with support for IEEE 802.3at PoE+ technology. NTU-MD500P provides up to 30 W of power on 10/100/1000BASE-T ports with a PoE power budget of 65 W.

Support for PoE technology allows NTU-MD500P to supply power via UTP cable to IP phones, wireless access points, IP cameras and other PoE-enabled devices.

The advantage of GPON technology is the optimum use of bandwidth. This technology is the next step to provide new high-speed internet connection at home and in offices. Designed to deploy a network inside a home or building, NTU-MD500P provides reliable connection with high bandwidth over long distances for users living and working in remote apartment buildings and business centers.

3.2 Overview

NTU-MD500P has the following interfaces:

- 1 PON SC/APC port for connecting to the operator's network (WAN);
- 4 Ethernet RJ-45 LAN ports (10/100/1000BASE-T) for connecting network devices (LAN).

NTU-MD500P supports the following functions:

- · PoE management and monitoring via OMCI:
 - ONU-G::PSE overload yellow;
 - ONU-G::PSE overload red;
 - · Physical path termination point Ethernet UNI::Power control;
 - Power over Ethernet control::Operational state;
 - Power over Ethernet control::Power detection status;
 - Power over Ethernet control::Power classification status;
 - Power over Ethernet control::Current Power Consumption;
 - · Power over Ethernet control::AVC;
 - Power over Ethernet control::Power priority.
- Network functions:
 - support for TR-069;
 - · operation in "bridge" or "router" mode;
 - PPPoE (auto, PAP-, CHAP-, MSCHAP-authorization);
 - IPoE (DHCP client and static);
 - DNS (Domain Name System);
 - DynDNS (Dynamic DNS);
 - UPnP (Universal Plug and Play);
 - VPN in L2TP mode;
 - · L2TP over IPsec;
 - · IPsec (trasport mode);
 - NAT (Network Address Translation);
 - NTP (Network Time Protocol);
 - QoS (quality of service mechanisms);
 - IGMP-snooping;
 - IGMP proxy;
 - VLAN according to IEEE 802.1Q.
- Firmware update via TR-069, OMCI, HTTP, TFTP;
- Remote monitoring and configuration:
 - SNMP-agent OLT;
 - CLI OLT.

The figure below shows the use case of NTU-MD500P.



Figure 1 – NTU-MD500P use case

3.3 Technical specifications

The main technical parameters of the terminal are given in Table 1:

Table 1 – Technical specifications

Parameters of LAN Ethernet interfaces			
Number of interfaces	4		
Electrical connector	RJ-45		
Data rate	Auto-detection, 10/100/1000 Mbps, duplex/half duplex		
Supported standards	IEEE 802.3i 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3x Flow Control IEEE 802.3 NWay auto-negotiation IEEE 802.3af IEEE 802.3at		
PON interface parameters			
Number of interfaces	1		
Supported standards	ITU-T G.984.x Gigabit-capable passive optical networks (GPON) ITU-T G.988 ONU management and control interface (OMCI) specification IEEE 802.1Q Tagged VLAN IEEE 802.1P Priority Queues IEEE 802.1D Spanning Tree Protocol		
Connector type	SC/APC corresponds to ITU-T G.984.2, ITU-T G.984.5 Filter, FSAN Class B+, SFF-8472		
Transmission medium	Fiber optic cable SMF – 9/125, G.652		
Split ratio	Up to 1:128		

Maximum distance	20 km
Transmitter:	1310 nm
Upstream data rate	1244 Mbps
Transmitter power	From +0.5 dBm to +5 dBm
• Spectrum width (RMS)	1 nm
Receiver:	1490 nm
Downstream data rate	2488 Mbps
Receiver sensitivity	From -8 to -28, BER≤1.0x10 ⁻¹⁰
Optical overload of the receiver	-8 dBm
Management	
Local management	Web, CLI
Remote control	TR-069, OMCI
Firmware update	OMCI, TR-069, HTTP, TFTP
Access restriction	By password
General parameters	
Power supply	110-250 V AC, 50-60 Hz
Maximum power consumption	80 W
Operating temperature range	From 0 to +40 °C
Relative humidity	No more than 80%
Dimensions ($W \times H \times D$)	267 × 44 × 178 mm
Form factor	19", size 1U
Weight	1.56 kg

3.4 Design

This section describes design and indicators layout of the device. Images of the front, back and side panels of the device are shown in the section, connectors, LED indicators and controls are described.

NTU-MD500P is enclosed in a metal case suitable for 19" rack, the height of the case is 1U.

3.4.1 Front panel layout

The device front panel layout is shown in Figure 2.



Figure 2 – NTU-MD500P front panel

Table 2 – Description	of connectors and	d front panel controls
-----------------------	-------------------	------------------------

N⁰	Front panel element	Description
1	Power	Device power indicator
	Status	Device operation indicator
	Alarm	Indicator of optical signal absence
	Link	Indicator of optical interface operation
	PoE 1-4	Status indicators of PoE ports
2	F	Functional button to restart the device and reset to factory settings:
		- pressing the button for less than 10 seconds restarts the device;
		- pressing the button for more than 10 seconds resets the device to the factory settings.
3	LAN 10/100/1000 14	4 RJ-45 ports for connecting network devices
4	PON	PON SC port (socket) of the GPON optical interface
5	110-250 V AC 50-60 Hz	Connector for AC power source

3.4.2 Side and back panels of the device





Nº	Back panel element
1	Earth bonding point



Figure 4 – NTU-MD500P left-side panel

There are ventilation grilles on the side and back panels of the device, which serve to remove heat. Do not cover the ventilation grilles, it can lead to overheating of the device components and cause malfunctioning. See recommendations for device installation in the Installing and connecting NTU-MD500P section.

3.5 Light indication

System indicators (Power, Status, Alarm, Link) are used to determine the operation status of the device nodes.

Table 3 –	Light	indication	of device	status
-----------	-------	------------	-----------	--------

Indicator name	Indicator status	Device status
Power	Solid green	The power is on, the device is operating normally
	Off	The power is off
Status	Solid red	The moment the drivers are lauching
	Solid green	The device has a configuration which differs from the default one
	Green, flashing slowly	The default configuration is set on the device
РоЕ 1-4	Solid green	The PoE consumer is connected, the power supply is in on (the indicator corresponds to a port).
	Solid red	PoE error on port
	Off	PoE consumer is not connected
Alarm	Off	Normal operation of the device
	Solid red	There is no optical signal
Link	Off	The device is loading
	Green, flashing fast	Getting settings via OMCI
	Solid green	The device has been successfully configured via OMCI.
	Green, flashing slowly	Configuration is absent (authorization)
	Red, flashing slowly	No signal from OLT
LAN P1P4	Green	10/100 Mbps connection has been established
	Orange	1000 Mbps connection has been established
	Flashing	The process of packet data transmission

3.6 Delivery package

The basic delivery package of NTU-MD500P device includes:

- Subscriber terminal NTU-MD500P;
- Power cord with euro plug C-13, 1.8 m;
- Mounting kit for installing into 19" rack;
- Technical passport.

4 Installing and connecting NTU-MD500P

4.1 Operating conditions and installation procedure

This chapter describes procedure of installation into 19" rack and connection to a power supply.

4.1.1 Safety requirements

General requirements

When working with the device, it is necessary to comply with safety regulations for the operation with electrical installations.

- It is forbidden to work with the device to persons who are not allowed to operation in accordance with the safety requirements.
- 1. The operation of the device must be carried out by engineering and technical personnel who have received special training.
- 2. Connect only fault-free auxiliary equipment to the terminal.
- 3. The terminal is designed for twenty-four-hour operation under the following conditions:
 - ambient temperature from 0 to +40 ° C;
 - relative humidity up to 80 % at 25 °C;
 - atmospheric pressure from 6.0×10^4 Pa to 10.7×10^4 Pa (from 450 to 800 mm Hg).
- 4. Do not expose the device to mechanical shocks and vibrations, as well as smoke, dust, water, chemicals.
- 5. In order to avoid overheating of the device components and disruption of its operation, it is forbidden to cover the ventilation grilles and place objects on the surface of the device.

Electrical safety requirements

- Before connecting the terminal to a power source, it is necessary to ground the device case using the earth bonding point (Figure 3). A grounding wire must be securely fixed to the earth bonding point. The resistance value between the earth bonding point and ground bus must not exceed 0.1 Ohm. Before connecting measuring instruments and a PC to the device, they must be previously grounded. The potential difference between the device case and measuring instruments should not exceed 1 V.
- 2. Before turning on the device, make sure that the cables are intact and securely attached to the connectors.
- 3. When installing or removing the case, make sure that the power supply of the device is switched off.

4.1.2 Installation procedure

Before installing and switching on, it is necessary to check the device for visible mechanical damage. In case of damage, stop installing the device, draw up an appropriate report and contact the supplier. If the device has been exposed to low temperature for a long period of time, it should be kept at room temperature for two hours before operation. After a long stay of the device in high humidity conditions, it is necessary to keep it under normal conditions for at least 12 hours before switching on.

Mounting

The terminal package includes brackets for installation in a rack and screws for fixing brackets to the device case. To install the brackets:

- Step 1. Align the four screw holes on the bracket with the same holes on the side panel of the device.
- Step 2. Using a screwdriver, attach the bracket with screws to the case.
- Step 3. Repeat steps 1 and 2 for the second bracket.





Installing into a rack

To install the device in a rack:

- Step 1. Attach the device to the vertical rails of the rack.
- Step 2. Align the holes of the brackets with the holes on the rack rails. Use the holes in the rails at the same level on both sides of the rack so that the device will be positioned strictly horizontally.
- Step 3. Use a screwdriver to attach the device to the rack with screws.



Figure 6 – Mounting brackets

The device has horizontal ventilation. Ventilation grilles are located on the side panels of the device. Do not cover the ventilation grilles to avoid overheating of the device components and malfunctioning.

▲ To avoid overheating and provide the necessary ventilation, the device must be placed so that there is at least 10 cm of free space above and below it.

4.2 Connecting the device

1. Connect LAN port of NTU-MD500P and Ethernet port of your PC using an Ethernet cable.



Figure 7 – Connecting the device to the computer

2. Connect the optical cable provided by the Internet service provider to the PON connector of the device.





3. Connect the terminal to 220 V power supply network using the power adapter included into the delivery package. Wait until the device is fully loaded.



Figure 9 – Connecting the device to the power supply

5 Device architecture

PON gpondef WANConnectionDevice br0 Filter 3	eth0
Marking 3	eth1
Filter 5	eth2
Ipinterface1	eth3

Figure 10 – Logical architecture of the device with the factory configuration

The main elements of the device:

- · Optical transceiver (SFF module) is designed to convert an optical signal into an electrical one;
- Processor (PON chip) is a converter of Ethernet and GPON interfaces.

In the factory configuration, the following logic blocks are present (Figure 10):

- Br0;
- eth0...3;
- IPInterface1.

The **br0** block in this case is intended for combining LAN ports into one group.

The **eth0..3** blocks are physically Ethernet ports with an RJ-45 connector for connecting a PC, STB or other network devices. Logically included in the **br0** block.

The **Filter** and **Marking** blocks are designed to put local interfaces in one group (in the **br0** block). These blocks are responsible for the traffic transmission rules, the **Filter** blocks are responsible for incoming traffic on the interface, the **Marking** blocks are responsible for outgoing traffic.

The **ipinterface1** block is a logical object where IP address for access to the local network is stored, as well as a DHCP server that distributes addresses to clients.

6 Configuring the device via web interface. Admin access.

Getting started

To configure the device, you need to connect the device via a web browser:

- 1. Open a web browser (web page viewer), for example, Firefox, Google Chrome.
- 2. Type the device IP address in the browser's address bar

The default IP address: 192.168.0.1, subnet mask: 255.255.255.0

If the connection is successful, a page with the authorization request will be displayed in the browser window:

Aeltex	NTU-MD500P	
	Authorization	
	User name Password	
	Login	

3. Enter username and password

Default user name – admin, password – password.

4. Click the "Login" button. The starting page of the device's web interface will be displayed in the browser window.

Changing the password

In order to avoid unauthorized access, it is recommended to change the password for further operation. To change the password in the menu *Admin*, section "*Password*", in the field "*Old Password*" enter the current password in the fields "*New Password*" and "*Confirm new password*" enter a new password. To save changes, click the **Apply Changes** button.

Password Configuration	Password Configuration				
This page is used to set the account to access the web server of your Device. Empty user name and password will disable the protection.					
UserName:	admin 💌				
Old Password:					
New Password:					
Confirmed Password:					
Apply Changes Res	et				

Elements of the web interface

General view of the device configuration window is shown below.

Sertex			NTU-M	D500P			3	admi Logo
Status	Device Status							
WAN	This page shows the curren	it status and son	ne basic setting:	of the device	D.			
Services					_			
Advance	System							
Diagnostics	Board Type		NTU-MD500P					
Admin Statistics	Serial Number		GP51000024					
otototteo	PON Serial		454C545882	000003				
	Base WAN MAC		E4:5A:D4:ED	:E2:1F				
	Hardware Version		1v1					
	Uptime		1:29					
	Date/Time		Thu Jan 101	:29:39 1970				
	Image 1 Firmware Vers	ion (Active)	2.4.1.323					
	Image 2 Firmware Vers	ion						
	CPU Usage		1%					
	Memory Usage		11%					
	Name Servers							
	IPv4 Default Gateway				_			
	IPv6 Default Gateway							
	LAN Configuration			_				
	IP Address	192.168.0.1						
	Subnet Mask	255.255.255.0						
	DHCP Server	Enabled						
	MAC Address	e4:5a:d4:ed:e2	:1f					
	WANConfiguration							
	Interface VLAN ID MAC C	onnection Type Pro	tocol IP Address	Subnet Mask Ga	teway NAPT	Firewall IG	MP 802.1p Sta	atus
	L2TP Configuration							
	Interface Protocol	Local IP Add	ress Remote	IP Address	Status			
	Refresh							

The user interface can be divided into 3 parts :

- The navigation tree of the device settings menu.
 The main window of selected section settings.
- 3. Change user button.

6.1 Status menu. Device information

6.1.1 Device submenu. General information on the device

The section displays general information on the device, the main parameters of LAN and WAN interfaces.

EAN	Device Status This page shows the current	status and some bas	ic settings of the d	evice.		
Services						
Advance	System					
Admin	Board Type		NTU-MD500P:re	ev.B		
Statistics	Serial Number		GP5F000024			
	PON Serial		454C54588F000	0003		
	Base WAN MAC		CC:9D:A2:DC:D	C:0C		
	Hardware Version		2v0			
	Uptime		6 days, 8 min			
	Date/Time		Wed Jan 7 00:0	08:32 1970		
	Image 1 Firmware Versi	ion (Active)	2.4.7.52			
	Image 2 Firmware Versi	ion	2.4.7.52			
	CPU Usage		1%			
	Memory Usage		11%			
	Name Servers					
	IPv4 Default Gateway					
	IPv6 Default Gateway					
	LAN Configuration					
	IP Address	192.168.0.1]		
	Subnet Mask	255.255.255.0]		
	DHCP Server	Enabled]		
	MAC Address	cc:9d:a2:dc:dc:0	c]		
	WANConfiguration					
	Interface VLAN MAC	onnection Type	IP Subne Address Mask	et Gateway NAR	PT Firewall IG	MP 802.1p Status
	1 2TP Configuration					
	Interface Protocol	Local IP Add	ess Remote	IP Address	Status	
	Refresh					I

Status → Device

System

- Board Type hardware model;
- Serial Number serial number of the device;
- PON Serial serial number of the device in PON network;
- Base WAN MAC WAN MAC address of the device;
- Hardware Version hardware version of the device;
- Uptime device operation time;
- Date/Time the current time on the device;
- Image 1 Firmware Version (Active) current firmware version;
- Image 2 Firmware Version backup software version;
- CPU Usage percentage of CPU usage;
- Memory Usage percentage of memory usage;
- Name Servers name of DNS server;
- IPv4 Default Gateway;
- IPv6 Default Gateway.

LAN Configuration

- IP Address IP address of the device;
- Subnet Mask network mask of the device;
- DHCP Server status of DHCP server;
- MAC Address MAC address of the device.

WAN Configuration

- Interface interface name;
- VLAN ID VLAN ID of the interface;
- MAC MAC address of the interface;
- Connection Type;
- Protocol the protocol used;
- IP Address IP address of the interface;
- Subnet Mask;
- Gateway;
- NAPT NAPT state;
- Firewall firewall status;
- IGMP Proxy IGMP Proxy status;
- 802.1p 802.1p mark;
- Status interface status.

L2TP Configuration

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

To update the data on the page, click **Refresh**.

6.1.2 IPv6 Status submenu. IPv6 System Information

The section displays the current status of the IPv6 system.

Status \rightarrow IPv6

Status Device IPv6 PON LAN	IPv6 Status This page shor	ws the current	t system status of :	IPv6.				
	LANConfigu	LANConfiguration						
WAN	IPv6 Addres	s						
Services	IPv6 Link-Lo	IPv6 Link-Local Address			fe80::ce9d:a2ff:fedc:dc0c/128			
Advance Diagnostics Admin Statistics	Prefix Deleg Prefix	ation						
	WANConfigu	Iration						
	Interface	VLAN ID	Connection Type	Protocol	IP Address	Status		
	Refresh							

LAN Configuration

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

Prefix Delegation

• Prefix – prefix of IPv6 address.

WAN Configuration

- Interface interface name;
- VLAN ID VLAN ID of the interface;
- Connection Type;

- Protocol the protocol used;
- IP Address IP address of the interface;
- Status interface status.

To update the data on the page, click **Refresh**.

6.1.3 PON submenu. Optical module status

The section shows the current state of the PON interface.

Status Device IPv6 PON LAN LAN WAN Services Advance Diagnostics	PON Status This page shows t	PON Status This page shows the current system status of PON.				
	PON Status	PON Status				
	Vendor Name					
	Part Number					
	Temperature		45.148438 C			
	Voltage		3.352300 V			
Admin Ctatics	Tx Power		4.185333 dBm			
Statistics	Rx Power		-inf dBm			
	Bias Current		6.250000 mA			
	GPON Status ONU State ONU ID LOID Status	01 255 Initial Stat	us			

Status \rightarrow PON

PON Status

- Vendor Name PON chipset vendor's name;
- Part Number part number of PON chipset;
- *Temperature* current temperature;
- Voltage;
- Tx Power transmission power;
- Rx Power signal power at reception;
- Bias Current.

GPON Status

- ONU State a status of authorization on OLT (01 -> 02 -> 03 -> 04 -> 05);
- ONU ID device ID on OLT;
- LOID Status authorization status on OLT (Initial -> Standby -> Serial Number -> Ranging Operation).

To update the data on the page, click **Refresh**.

6.1.4 LAN submenu. Information on the status of LAN interface

In this section, you can view the main parameters of LAN interfaces.

Status \rightarrow LAN

Exatus Device IPv6 PON	LAN Port S This page sl	tatus hows the current LAN Port status.	
	LAN1	Up; 1000M, Full Mode	
WAN	LAN2	Down	
Services	LAN3	Down	
Advance	LAN4	Down	
Admin Statistics	Refresh		

To update information in the table, click **Refresh**.

6.2 LAN menu. Configuring LAN interface

In this section, you can configure the main characteristics of wired and wireless LAN interfaces.

Status	LAN Interface Set	LAN Interface Settings				
WAN Services	This page is used to you may change the	configure the LAN interface of your Device. Here setting for IP addresses, subnet mask, etc				
Advance	InterfaceName:	LANIPInterface				
Admin Statistics	IP Address:	192.168.0.1				
	Subnet Mask:	255.255.255.0				
	IPv6 Address:	fe80::1				
	IPv6 DNS Mode:	HGWProxy V				
	Prefix Mode:	WANDelegated V				
	WAN Interface:	▼				
	Firewall:	Disabled C Enabled				
	IGMP Snooping:	O Disabled Enabled				

LAN

- InterfaceName interface name;
- IP Address IP address of the interface;
- Subnet Mask interface subnet mask;
- IPv6 Address;
- IPv6 DNS Mode configure the mode of domain names usage:
 - HGWProxy configure DNS mode for IPv6;
 - WANConnection use the WAN interface to get the DNS server address;
 - Static specify a static DNS server address (IPv6 DNS1, IPv6 DNS2).
- Prefix Mode configure prefix reception mode (from WAN interface or statically):
 - WANDelegated the option of delegating prefixes received from the provider;
 - Static specify prefix statically.
- WAN Interface select WAN interface to be used when WANDelegated.
- Firewall (Enabled/Disabled) enable/disable firewall for LAN interface;
- IGMP Snooping (Enabled/Disabled) enable/disable IGMP Snooping.

6.3 WAN menu. Configuring WAN interface

6.3.1 PON WAN submenu

In this section, you can configure the PON WAN parameters.

Status	PON WAN This page is used to configure the parameters for PONWAN
PON WAN	new link 🗸
Services	Enable VLAN:
Advance	VLAN ID: 802.1p_Mark V
Diagnostics	Channel Mode: Bridged 🗸
Admin Statistics	Interface Grouping: Create New Group 🗸
	Group Name: Group_1
	Enable NAPT:
	Admin Status: Enable Disable
	Enable firewall:
	Connection Type: Other 🗸
	Default Route: Disable Enable
	Enable IGMP-Proxy:
	Apply Changes Delete

WAN → PON WAN

- Enable VLAN;
- VLAN ID VLAN identification number;
- 802.1p_Mark 802.1p priority;
- · Channel Mode VLAN interface operation mode;
 - Bridged;
 - IPoE getting an address via the DHCP protocol;
 - *PPPoE* installing a point-to-point tunnel over Ethernet.
- Interface Grouping select a group of interfaces;
- Group name name of the interface group;
- Enable NAPT enable NAPT (Network address port translation) function;
- Admin Status (Enable/Disable) enable/disable administrative status;
- Enable Firewall;
- Connection Type type of service provided on the WAN;
- Default Route (Enable/Disable) enable/disable the use of the selected interface as a default gateway;
- Enable IGMP-Proxy enable interception and forwarding of IGMP messages.

To save changes, click Apply Changes, to delete – Delete.

6.3.2 VPN submenu

6.3.2.1 L2TP submenu. Setting up an L2TP VPN

In this section, you can configure the virtual connection parameters L2TP VPN. The L2TP protocol is used to create a secure connection channel over the Internet between a remote user's computer and a local computer.

)PON WAN VPN	L2TP VPN: Oisable O Ena	ble				
	Server:					
rvices	Tunnel Authentication:					
lvance	Tunnel Authentication Secret	t:				
agnostics	PPP Authentication:	Auto 🗸				
lmin	PPP Encryption:	NONE 🗸				
ausucs	UserName:					
	Password:					
	PPP Connection Type:	Persistent 🗸				
	Idle Time (min):					
	MTU:	1458				
	Default Gateway:					
	Apply Changes					
	L2TP Table:					
	Coloct Interface Cor	Tunnel	РРР	MTH	Default	Action

 $WAN \rightarrow VPN \rightarrow L2TP$

L2TP VPN is a mode in which access to the Internet is carried out through a tunnel using the L2TP protocol. When **Enable** is selected, the following parameters will be available for editing:

- Server L2TP server address (domain name or IP address in IPv4 format);
- Tunnel Authentication enable authentication;
- Tunnel Authentication Secret authentication key;
- PPP Authentication select authentication protocol used on L2TP server to validate connections;
- PPP Encryption select data encryption protocol to be used (only for the CHAPMSv2 authentication method);
- UserName the username for authorization on L2TP server;
- Password password for authorization on L2TP server;
- PPP Connection Type;
- Idle Time (min) idle time in seconds, breaks an inactive connection after a specified time (only for establishing a connection on demand (dial-on-demand));
- MTU the maximum size of the data block transmitted over the network (the recommended value is 1462);
- Default Gateway select whether the created tunnel will be a default L2TP gateway.

To save changes, click Apply Changes.

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

6.3.2.2 IPsec submenu. Configuring IP Security

This page is used to configure settings for VPN in IPsec mode.

Status	IPsec VPN Configuration
WAN	This page is used to configure the parameters for IPsec mode VPN.
PON WAN	Negotiation Type Automatic Manual Auto Configure:
IPsec	Mode Transport Mode 🗸
Advance Diagnostics	Remote: Tunnel Addr. 0.0.0.0
Admin	Local: Tunnel Addr. 0.0.0.0
	Security Option: Encapsulation Type ESP V
	IKE Auth Method Pre Shared Key Pre shared key
	Advanced Option Add/Save
	IPsec Information List: Enable State Type RemoteGW RemoteIP Interface LocalIP EncapMode filterProtocol filterPort Delete Selected Enable Disable FilterPort FilterPort
	Certificate Management:
	privKey.pem Choose File No file chosen Upload

 $WAN \rightarrow VPN \rightarrow IPsec$

- Negotiation Type select the type of negotiation: automatic or manual one;
 Negotiation Type Automatic:
 - Mode IPsec operation mode (only transport mode is supported);
 - *Remote Tunnel Addr.* server IP address;
 - Local Tunnel Addr. local IP address;
 - Security Option:
 - Encapsulation Type;
 - IKE Auth Method IKE authentication method (Pre-shared key or Certificate);
 - Pre shared key set shared key (if using Pre-shared key method);
 - Advanced Option set up advanced security options:
 - Filter Option:
 - Protocol;
 - Port.
 - *IKE Phase 1* setting up the first phase:
 - Negotiation Mode negotiation mode: main or aggressive;
 - Keepalive Time session uptime in seconds;
 - *IKE Algorithm 1-4* select key exchange algorithms.
 - *IKE Phase 2* setting up the second phase:
 - pfs_group mode select PFS(DH) group;
 - Encrypt Algorithm encryption algorithm;
 - Auth Algorithm authentication algorithm;
 - Keepalive Time session uptime in seconds;
 - Keepalive Byte bytes to keep session active, KB.

- Negotiation Type Manual:
 - Mode IPsec operation mode (only transport mode is supported);
 - Remote Tunnel Addr. server IP address;
 - Local Tunnel Addr. local IP address;
 - Security Option:
 - Encapsulation Type;
 - Encapsulation Type ESP:
 - ESP Encrypt Algorithm ESP encryption algorithm;
 - ESP Encrypt Key ESP encryption key;
 - ESP Auth Algorithm ESP authentication algorithm;
 - ESP Auth Key ESP authentication key.
 - Encapsulation Type AH:
 - AH Auth Algorithm AH authentication algorithm (md5 or sha1);
 - AH Auth AH authentication key.
 - Encapsulation Type ESP+AH:
 - ESP Encrypt Algorithm ESP encryption algorithm;
 - ESP Encrypt Key ESP encryption key;
 - ESP Auth Algorithm ESP authentication algorithm;
 - ESP Auth Key ESP authentication key;
 - AH Auth Algorithm AH authentication algorithm;
 - AH Auth AH authentication key.
 - Advanced Option set up advanced security options;
 - Filter Option:
 - Protocol;
 - Port.
- Certificate Management select and download a management certificate. Click Select File to select the certificate then click Upload.

To save changes, click Add/Save.

In the table **IPsec Information List**, you can view, enable, disable and delete (**Delete Selected**) the created rules.

6.4 Services menu. Configuring services

6.4.1 DHCP Settings submenu. Configuring DHCP

In this section, a DHCP server or a DHCP repeater is configured.

- DHCP Mode select operation mode:
 - NONE DHCP is disabled;
 - DHCP Server operation in the DHCP server mode;
 - DHCP Relay operation in the DHCP relay mode.

Services \rightarrow DHCP (DHCP Server is selected)

Status LAN WAN	DHCP Settings This page is used to configure	DHCP Server and DHCP Relay.
Services	DHCP Mode: ONONE O	HCP Relay OHCP Server
DNS Firewall UPnP RIP Advance	Enable the DHCP Server if you LAN. The device distributes nu LAN IP Address: 192.168.0	are using this device as a DHCP server. This page lists the IP address pools available to hosts on your nbers in the pool to hosts on your network as they request Internet access.
Diagnostics	IP Pool Range:	.168.0.10 - 192.168.0.254 ow Client
Statistics	Subnet Mask: 25	.255.255.0
	Max Lease Time:	00 seconds (-1 indicates an infinite se)
	DomainName: Ho	ne
	Gateway Address: 19	.168.0.1
	DNS option: (Apply Changes) Port-Base	Jse DNS Proxy O Set Manually Filter MAC-Based Assignment

- IP Pool Range the range of addresses issued to clients;
- Show Client a button for viewing clients who have leased addresses. When enabled, a table with information about the DHCP clients leased addresses is displayed;
- Subnet Mask subnet mask;
- Max Lease Time maximum lease time, -1 for timeless lease;
- *DomainName* domain name;
- Gateway Address gateway address;
- DNS option defines DNS operation:
 - Use DNS relay the ONT address will be issued as DNS and all requests will be relayed via ONT;
 - Set manually set DNS manually.

Port-Based Filter configures filtering according to ports, **MAC-Based Assignment** – according to MAC addresses.

Services \rightarrow DHCF	P (DHCP Relay is selected)
-----------------------------	----------------------------

 Status LAN WAN Services DHCP DNS Firewall UPnP RIP Advance Diagnostics 	DHCP Settings This page is used to configure DHCP Server and DHCP Relay. DHCP Mode: O NONE O DHCP Relay O DHCP Server This page is used to configure the DHCP Server IP Address for DHCP Relay. DHCP Server IP Address: 172.19.31.4 Apply Changes
Diagnostics Admin Statistics	

• DHCP Server IP Address – IP address of remote DHCP server, which will be used for DHCP Relay.

To save changes, click **Apply Changes**.

6.4.2 DNS submenu

6.4.2.1 Dynamic DNS submenu. Dynamic Domain Name System Settings

Dynamic DNS (dynamic domain name system) allows updating information on DNS server in real time and (optionally) in automatic mode. It is used to assign a permanent domain name to a device (computer, router, for example NTU-RG) having dynamic IP address. IP address might be obtained via IPCP in PPP connections or via DHCP.

Dynamic DNS is often used in local networks, where clients receive an IP address via DHCP, and then register their names in the local DNS server.

Etatus LAN WAN Services	Dynamic DNS Configuration This page is used to configure the Dynamic DNS address from DynDNS.org or TZO or No-IP. Here you can Add/Remove to configure Dynamic DNS.
DHCP	Enable:
Dvnamic DNS	DDNS Provider: DynDNS.org 🗸
Firewall	Hostname:
UPnP	Interface 🗸
	DynDns/No-IP Settings:
Advance Diagnostics Admin Statistics	UserName: Password:
	Add Modify Remove Dynamic DNS Table: Image: Comparison of the second sec
	Select State Hostname UserName Service Status

Services \rightarrow DNS \rightarrow Dynamic DNS

- Enable when selected, DHCP server is used (network devices will receive IP addresses dynamically, from the range below);
- D-DNS Provider select the type of D-DNS service (provider): DynDNS.org, No-IP.com;

• *Hostname/Intereface* – if you use another provider, you should specify the name (*Hostname*) and address (*Interface*) of the provider manually.

DynDns/No-IP Settings:

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

The section displays **Dynamic DNS Table** with a list of available DNS and its parameters. To add an entry, click **Add**. To change/delete a position, select it and click **Modify** or **Remove**.

6.4.3 Firewall submenu. Configuring the firewall

6.4.3.1 ALG On-Off Configuration submenu. Enabling disabling ALG services.

In this section, you can enable or disable ALG and Pass Through services.



Services → Firewall → ALG

Please, do not forget to click Apply changes, to save changes made.

6.4.3.2 IP/Port Filtering submenu. Configuring address filtering

Address filtering settings are available in this menu. The IP filtering function allows you to filter traffic passing through the router according to IP addresses and ports. The use of such filters can be useful to protect or put restrictions on the local network.

Status LAN WAN Services	IP/Port Filtering Entries in this table are used to restrict certain types of data packets through the Gateway. Use of such filters can be helpful in securing or restricting your local network.
DHCP	Outgoing Default Action Openy OAllow
DNS Firewall ALG IP/Port Filtering	Incoming Default Action C Deny Allow Apply Changes
MAC Filtering	Direction: Outgoing 🗸 Protocol: TCP 🗸 Rule Action 🖲 Deny 🔿 Allow
Port Forwarding	Source IP Address: Subnet Mask: Port: -
Domain Blocking	Destination IP Address: Subnet Mask: Port: -
	WAN Interface: Any 🗸
	Add
Advance	Current Filter Table:
Admin	Select Direction Protocol Source IP Address Source Port Destination IP Address Destination WAN Rule
Statistics	Delete Selected Delete All

Services \rightarrow Firewall \rightarrow IP/Port Filtering

Default settings

- Outgoing Default Action Deny/Allow filtering of outgoing packets;
- Incoming Default Action Deny/Allow filtering of incoming packets.

To save changes made, click Apply Changes.

To add a filter, complete the appropriate fields and click Add:

- Direction direction of packet transmission (outgoing/incoming);
- Protocol filtering protocol;
- Rule Action packet processing policy (Deny/Allow);
- Source IP Address;
 - Subnet mask;
 - Port.
- · Destination IP Address;
 - Subnet mask;
 - Port.
- WAN Interface incoming interface.

The added filters are displayed in **Current Filter Table**. The entries in this table are used to restrict certain types of data packets through the gateway. To delete a certain filter, select an entry and click the **Delete selected** button, to delete all filters – **Delete All**.

6.4.3.3 MAC Filtering submenu. MAC address filtering settings

The section helps to configure filtration based on MAC addresses, which allows you to forward or block traffic according to MAC address of the source and recipient.

Status LAN WAN Services	MAC Filtering for bridge mode Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.
	Dutgoing Default Action ODeny OAllow
Firewall ALG IP/Port Filtering	Incoming Default Action Openy Allow Apply Changes
MAC Filtering	Direction: Outgoing 🗸
Port Forwarding	Source MAC Address: 00:00:00:00:00:00
URL Blocking	Destination MAC Address: 00:00:00:00:00:00
Domain Blocking	Rule Action Deny O Allow
	Add
Advance	Current Filter Table:
Diagnostics	Select Direction Source MAC Address Destination MAC Address Interface Rule Action
Admin Statistics	Delete Selected Delete All

Services \rightarrow Firewall \rightarrow MAC Filtering

- Outgoing Default Action default packet processing policy for outgoing traffic (Deny (drop out) / Allow (transmit));
- Incoming Default Action default packet processing policy for incoming traffic (Deny (drop out) / Allow (transmit)).

To save changes, click Apply Changes.

To add a filter, complete the appropriate fields and click Add button:

- Direction direction of packet transmission (outgoing/incoming);
- Source MAC Address add source MAC address for which you want to set restriction/access.
- Destination MAC Address add destination MAC address for which you want to set restriction/access.
- Rule Action packet processing policy (Deny (drop out) / Allow (transmit));
- WAN Interface incoming interface.

The added filters are displayed in the filter table below – **Current Filter Table**. The *Rule action* field displays the type of rule created (**Allow** or **Deny** traffic transmission). To delete a certain rule in the list, select it and click **Delete Selected**, to delete the entire list, click **Delete All**.

6.4.3.4 Port Forwarding submenu. Configuring port forwarding

This section contains **Current Port Forwarding Table** displaying information on port forwarding. Entries in this table allow you to automatically redirect shared network services to a specific computer behind the NAT firewall. These settings are only necessary if you want to deploy a host, such as a web server or mail server, on a private LAN behind the NAT firewall of the router you are using. To save changes, click **Apply Changes**.

	Port Forwarding: 🔘 I	Disable CEnable App	ily Changes						
 	Enable 🔽 Application	n: Active Worlds		~					
Filtering tering	Comment	Local IP	Local Port from	Local Port to	Protocol Remote IP	Remote Port from	Remote Port to	Interface	NAT loopbac
					Both 🗸			~	
					Both 🛩			~	
					Both 🛩			~	
					Both 🗸			~	
					Both 🗸			~	
					Both 🗸			~	
					Both 🗸			~	
					Both 🗸			~	
					Both 🗸			~	
					Both 🗸			~	
					Both 🖌			~	
					Both				

Services \rightarrow Firewall \rightarrow Port Forwarding

To add an entry to Current Port Forwarding Table, select Enable and complete the appropriate fields:

- Application there are presets in the menu for port forwarding of different applications;
- Comment write comment for the entry;
- Local IP the local IP address to which the forwarding will be performed;
- · Local port from/to specify range of the local device ports for forwarding;
- Protocol select protocol (TCP, UDP or both);
- Remote port from/to specify initial port of the incoming connection. The field "Remote port to" will be filled in automatically;
- Interface select interface;
- NAT-loopback NAT loop allows you to transfer requests from the local network to the router, so, for example, you can check the operation of the created rules.

After completing the fields to add an entry, click **Add**. To delete a certain entry, select it and click the **Delete Selected** button, to delete the entire table – **Delete All**.

6.4.3.5 URL Blocking submenu. Configuring the Internet access restriction

The URL filter performs full analysis and control for access to certain Internet resources. In this section you may set and view a list of prohibited/allowed URLs to visit. Here you can add a prohibited/permitted FQDN (Fully Qualified Domain Name) with the **Add** button, keyword filtering is also possible. The added restrictions are displayed in **URL Blocking Table** and **Keyword Filtering Table**, to delete a specific URL or keyword from the table, click on it, and then on the **Delete Selected** button. To remove all restrictions, click **Delete All**.

Status LAN WAN Services DHCP DNS Firewall ALG	URL Blocking This page is used to configure the Blocked FQDN (Such as tw.ya URL Blocking: Disable OEnable Apply Changes FQDN: Add URL Blocking Table:	ahoo.com) and filtered keyword. Here you can add/delete FQDN and filtered keyword.
	Select	FQDN
Port Forwarding URL Blocking Domain Blocking DMZ UPnP	Delete Selected Delete All	
RIP	Keyword Filtering Table:	Citizen Verwand
Advance	Select	Hiterea Keywora
Diagnostics Admin Statistics	Delete Selected Delete All	

Services → Firewall → URL Blocking

- URL Blocking (Enable/Disable) enabling/disabling URL-Blocking;
- FQDN (Fully Qualified Domain Name) full domain name;
- Keyword keyword.

To save changes, click Apply Changes.

6.4.3.6 Domain Blocking submenu. Setting up Domain Blocking

This section is used to specify domain blocking.

Services → Firewall → Domain blocking

Status LAN	Domain Blocking Configuration This page is used to configure the Blocked domain. Here you can add/delete the blocked domain.
Services	Domain Blocking: OEnable Apply Changes
Firewall	Domain: Add
	Domain Blocking Configuration:
Port Forwarding	Select Domain
URL Blocking	
Domain Blocking	
Advance	
Diagnostics	
🚞 Admin	
Statistics	

To block a domain, select **Enable**, complete the **Domain** field and click the **Add** button.

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

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

6.4.3.7 DMZ submenu. Configuring demilitarized zone

When setting IP address in the *DMZ Host IP Address* field, all requests from the external network that do not meet the *Port Forwarding* rules will be sent to the DMZ host (a trusted host with the specified address located in the local network).



Services \rightarrow Firewall \rightarrow DMZ

- DMZ Host (Enable/Disable) enabling/disabling the host;
- DMZ Host IP Address IP address.

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

6.4.4 UPnP submenu. Automatic configuration of network devices

In this section, you may configure the Universal Plug and Play (UPnP) function. UPnP provides compatibility with network equipment, software, and peripherals.



Services → UPnP

To use UPnP, you need to configure NAT on the active WAN interface.

- UPnP (Enable/Disable) enable/disable UPnP function;
- WAN Interface WAN interface on which the UPnP function will be enabled.

To save settings, click Apply Changes.

6.4.5 RIP submenu. Configuring dynamic routing

In this section you may select interfaces on devices that will use RIP and its version. Enable RIP if you are using this device as a RIP-enabled device to communicate with other users using the RIP Dynamic Routing protocol.

Services	\rightarrow	RIP
----------	---------------	-----

Status LAN WAN Services OHCP DNS Firewall LIP/Port Filtering MAC Filtering URL Blocking DMZ UPNP	RIP Configuration Enable the RIP if Routing Informative version of the pro- RIP: Disable Interface: Receive Mode: Send Mode: Add RIP Config Table	you are using this device a on Protocol. This page is u otocol used. O Enable Apply Chan br0 V NONE V NONE V	is a RIP-enabled Device to commun ised to select the interfaces on you ges	icate with others using the r device is that use RIP, and the
RIP	Select	Interface	Receive Mode	Send Mode
Advance				
Diagnostics	Delete Selected	Delete All		
admin				
Statistics				

• RIP (Enable/Disable) - enabling/disabling the use of the RIP dynamic routing protocol;

To accept and save settings, click **Apply Changes**.

- Interface the interface on which RIP will be launched;
- Receive Mode incoming packet processing mode (NONE, RIP1, RIP2, both);
- Send Mode transmission mode (NONE, RIP1, RIP2, RIP1 COMPAT).

RIP-enabled interfaces are displayed in **RIP Config Table**. To delete all entries in the table, click **Delete All**, to delete a certain entry from the list, select it and click **Delete Selected**.

6.5 Advance menu. Advanced settings

6.5.1 ARP Table submenu. Viewing the ARP protocol cache

The section displays a table of learned MAC addresses. The efficiency of ARP operation largely depends on the ARP cache, which is present on each host. The cache contains Internet addresses and their corresponding hardware addresses. The lifetime of each entry in the cache is 5 minutes from the moment the entry was created.

Status LAN	User List This table shows a list of lea	arned MAC addresses.	
Services	IP Address	MAC Address	
Advance	192.168.0.10	a0:a3:f0:d0:f5:0f	
Bridging Routing Interface Grouping POE Settings Link Mode Others IPv6 Diagnostics Admin Statistics	Refresh		

Advance \rightarrow ARP table

- IP Address the client's IP address;
- MAC Address the MAC address of the client.

To update information in the table, click **Refresh**.

6.5.2 Bridging submenu. Configuring Bridging parameters

In this section, you may configure bridge parameters. Here you can configure the lifetime of addresses in the MAC table, as well as enable/disable the 802.1d Spanning Tree protocol.

	Advance - Druging
Status LAN WAN Services	BridgingConfiguration This page is used to configure the bridge parameters. Here you can change the settings or view some information on the bridge and its attached ports.
Advance ARP Table Bridging Routing Interface Grouping IP QoS PoE Settings Link Mode Others IPv6 Diagnostics Admin Statistics	Ageing Time: 7200 (seconds) 802.1d Spanning Tree: Image: Disabled Image: Disabled Apply Changes Show MACs

Advance → Bridging

- Aging Time lifetime of addresses (sec);
- 802.1d Spanning Tree (Enable/Disable) enabling/disabling 802.1d Spanning Tree protocol.

To save changes, click **Apply Changes**.

To view information on the bridge and its connected ports, click **Show MACs**.

Advance \rightarrow Bridging \rightarrow Show MACs

Port	MAC Address	Is Local?	Ageing Timer
1	-02.f0.d0.f5.0f	no	0.01

- Port port number;
- MAC Address MAC address;
- Is Local local address;
- Aging Timer address lifetime.

To update information in the table, click **Refresh**, to close – **Close**.

6.5.3 Routing submenu. Configuring routing

The section is used to configure static routing.

Advance → Routing

Status LAN WAN Services Advance	RoutingConfiguration This page is used to configure the routing information. Here you can add/delete IP routes.
	Enable:
ARP Table	Destination:
Bridging	Subnet Mask:
	Next Hop:
IP QoS	Metric:
PoE Settings	Interface: Any 🗸
Link Mode	Add Route Update Delete Selected Show Routes
IPv6	Static Route Table:
Diagnostics Admin Statistics	Select State Destination Subnet Mask Next Hop Metric Interface

To add a static route, select **Enable**, complete the appropriate fields and click **Add Route**.

- Enable add a route;
- Destination destination address;
- Subnet Mask subnet mask;
- *Next Hop* next node;
- Metric metric;
- Interface interface.

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

To view the routes that the device frequently accesses, click **Show Routes**, then *IP Route Table* will be displayed.

s table shows a l	list of destination routs	es commonly ad	cessed by yo	our network.
Destination	Subnet Mask	Next Hop	Metric	Interface
127.0.0.0	255.255.255.0	*	0	lo
192.168.0.0	255.255.255.0		0	brO

Advance \rightarrow Routing \rightarrow Show Routes

To update information in the table, click **Refresh**, to close it, click **Close**.

6.5.4 Interface grouping submenu. Combining interfaces into groups

In this section, you can combine interfaces into different groups. By default, all interfaces are in the same group. To transfer the interface to a new group, you should:

- 1. Select a new group from the list below;
- 2. Select interfaces from the list of Available interfaces;
- 3. Press the arrow \leftarrow to move the interfaces to the group;
- 4. Apply actions by clicking Apply Changes.

Advance \rightarrow Interface grouping

Status	Interface Grouping Confi	guration		
LAN	17			7.0
WAN				
Services	Select:	New Group 🗸		
🚞 Advance	Enable:	 Image: A set of the set of the		
ARP Table	Name:			
Bridging				
Routing	Grouned Interface	as and a second s	Available Interfaces	
Interface Grouping	di super interriet	7	LANI	
📄 IP QoS				
PoE Settings			LANS	
Link Mode		->	LAN4	
Others			LANIPInterface	
IPv6		<-		
Diagnostics				
Admin		-	-	
Statistics		_		
	Annly Changes			
	Nomo	Ptatus	Interfaces	Action
	Name	Status	Interfaces	ACTION
	detault	Enable	LANI,LANZ,LAN3,LAN4,LANIPINTERTACE	

6.5.5 IP QoS submenu. Configuring the quality of services provided (QoS)

6.5.5.1 QoS Policy submenu. Setting up QoS Queues

In this section, you can configure QoS queue policies for traffic processing.

Status	IP QoS Configuration
WAN	
Services	IP QoS Obisable enable
Advance	QoS Queue Config
Bridging	This page is used to configure the QoS policy and Queue. If select PRIO of policy, the lower numbers imply greater precedence. If select WRR of policy, please input the weight of this queue. Default is 40:30:20:10. After configration, please click 'Apply Changes'
Interface Grouping	Policy: Owr
Doos Policy	Queue Policy Priority Weight Enable
Dos Classification	Q1 PRIO 1 🗌
Dec Cottings	
Duels Mede	
Conters Conters	
	QoS Bandwidth Config
Diagnostics	This part is used to capitalize the bandwidth of different two of WAN. If color: Dicable, CDE will color: the appropriate bandwidth baced on WAN.
Statistics	If select Enable, User is allowed to configure specific bandwidth of WAN.
	User Defined Bandwidth: O Disable O Enable
	Total Bandwidth Limit: 100000 Kb
	Apply Changes

Advance \rightarrow IP QoS \rightarrow QoS Policy

- IP QoS (Enable/Disable) enable/disable configuration of QoS queues;
- *Policy* select policy:
 - PRIO strict queue processing is used when selecting the PRIO policy. The smaller queue corresponds to the highest priority;
 - WRR weighted queue processing will be used when selecting the WRR policy. By default, weight
 for queues is distributed as 40:30:20:10.

QoS Bandwidth Config

Is used to configure the bandwidth of individual services.

- User defined Bandwidth (Enable/Disable) enable restriction;
- Total Bandwidth Limit, (kb) bandwidth limit, kbit.

To save changes, click Apply Changes.

6.5.5.2 QoS Classification submenu. Configuring traffic classification rules

On this page, you can specify according to which fields and their values the packet will be classified, as well as which hardware queue it will eventually belong to.

Status LAN WAN Services	QoS Classification This page is used to add or delete classicification rule. (After add a new rule, please click 'Apply Changes' to take eff -
Advance	Mark Classification Rules
ARP Table	ID Name Order DSCP Mark 802.1p Queue WanIf Rule Detail Delete Edit
Routing	Add Apply Changes
IP QoS	
QoS Policy	
Traffic Shaping	
Link Mode	
Others	
IPv6	
Diagnostics	
Statistics	

Advance \rightarrow IP QoS \rightarrow QoS Classification

To add a rule, click **Add** and complete the appropriate fields.

Status LAN WAN Services	Add QoS Classification Rules This page is used to add a IP QoS classification rule.
Advance ARP Table Bridging Routing	RuleName: rule RuleOrder:
Interface Grouping Qos Policy Qos Classification Traffic Shaping PoE Settings	Assign IP Precedence/DSCP/802.1p Precedence: Queue 1 DSCP: 802.1p:
Cink Mode	Specify Traffic Classification Rules
Admin Statistics	IP QoS Rule by type: OPort OEthery Type OIP/Protocol OMAC Address Apply Changes

Advance \rightarrow IP QoS \rightarrow QoS Classification \rightarrow Add

- RuleName rule name;
- *RuleOrder* sequence number.

Assing IP Precedence/DSCP/802.1p – setting up the assignment of IP fields.

- Precedence queue selection;
- DSCP priority in the IP packet header;
- 802.1p priority label in 802.1Q.

Specify Traffic Classification Rules - select traffic classification rule.

- IP QoS Rule by type select classification rule according to the type:
 - Port according to port;
 - *Physiacl Port* select physical port.
 - Ethery Type according to Ethertype;
 - *IP/Protocol* via IP protocol;
 - *IPv4*:
 - Protocol select protocol;
 - Source IP source IP address;
 - Source Mask source mask;
 - Destination IP Destination IP address;
 - Destination Mask destination mask;
 - Source Port source port;
 - Destination Port destination port.
 - IPv6:
 - Protocol select protocol;
 - Source IP source IP address;
 - Source Prefix Length the length of the source prefix;
 - Destination IP Destination IP address;
 - Destination Prefix Length the length of the destination prefix;
 - Source Port source port;
 - Destination Port destination port.
 - MAC Address according to MAC address.
 - Source MAC Source MAC address;
 - Destination MAC destination MAC address.

6.5.5.3 Traffic Shaping submenu. Configuring traffic

In this section, you can specify traffic restrictions according to certain rules.

Advance \rightarrow IP QoS \rightarrow Traffic Shaping

Status	IP QoS Traffic Shaping
LAN	
WAN	
Services	Total Developidth Limits (199999)
🚞 Advance	
ARP Table	
Bridging	ID Protocol Source Port Destination Port Source IP Destination IP Rate(kb/s) Delete IP Version Direction
Routing	
Interface Grouping	Add Apply Changes Apply Total Bandwidth Limit
🚞 IP QoS	
QoS Policy	
QoS Classification	
Traffic Shaping	
PoE Settings	
Link Mode	
Others	
iii IPv6	
Diagnostics	
admin	
Statistics	

• Total Bandwidth Limit (kb) - total bandwidth limit, kbit.

To add, click Add and complete the appropriate fields.

Advance \rightarrow IP QoS \rightarrow Traffic Shaping \rightarrow Add

Status	Add IP QoS Traffic Shaping Rule
WAN	
Services	IP Version: IPv4 🗸
Advance	Direction: Upstream 🗸
Bridging	Protocol: NONE V
Routing	Source IP:
Interface Grouping	Source Mask:
QoS Policy	Destination IP:
QoS Classification	Destination Mask:
Traffic Shaping PoE Settings	Source Port:
Link Mode	Destination Port:
Others	Rate Limit: kb/s
IPv6 Diagnostics Admin Statistics	Close Apply Changes

- IP Version select the IP version;
- Direction selection of the flow type, descending or ascending;
- Protocol protocol;
- Source IP source IP address;
- Source Mask/Prefix Length mask/prefix length of the source subnet;
- Destination IP destination IP address;
- Destination Mask/Prefix Length mask/prefix length of the destination subnet;
- Source Port source port;
- Destination Port destination port;
- Rate Limit (kb/s) speed limit, kbps.

To save the changes, click **Apply Changes**, to cancel, click **Close**.

6.5.6 PoE Settings submenu. Configuring PoE ports

This page is used to configure PoE settings. Here, you can enable/disable PoE on LAN ports; to do this, you need to select **Enable** or **Disable**.

Status	PoE S	ettings						
WAN	This p	age is used to	configure	e PoE setti	ngs. Here you ca	an enable/disable PoB	E on LAN ports.	
Services		<u> </u>						
🔤 Advance	PoE	⊙Disable ∪E	nable					
ARP Table								
Bridging	Port	PsE enabled	Power	Voltage	Temperature	Detection Status	Power Classification	Error Type
Routing	1	Disabled						
Interface Grouping	2	Disabled						
IP QoS	3	Disabled						
QoS Policy	4	Disabled						
Traffic Shaping								
PoE Settings	Apply changes							
Link Mode								
Others								
IPv6								
Diagnostics								
Admin								
Statistics								

Advance → PoE Settings

- Port LAN port number (1-4);
- PsE enabled:
 - Enabled PoE is enabled;
 - Disabled PoE is disabled.
- *Power* power consumption, W;
- Voltage voltage, V;
- Temperature temperature, °C;
- Detection Status PoE port status;
- Power Classification the power class of the connected PoE device;
- *Error Type* type of error.

6.5.7 Link mode submenu. Configuring LAN ports

In this section, you can set the mode of LAN ports operation. **LAN1/2/3/4** fields are used to set up the operation mode. Available modes are *10M Half Mode*, *10M Full Mode*, *100M Half Mode*, *100M Full Mode* and *Auto Mode* (auto detection mode).

		0.47.20.22.0
Status	Ethernet Link Speed/Duplex	Mode
LAN	Set the Ethernet link speed/dup	lex mode.
WAN		
Services	LANI	Auto Mode
Advance	LANT.	
ARP Table	LAN2:	Auto Mode 🗸
Bridging	LAN3:	Auto Mode 🗸 🗸
Routing	LAN4:	Auto Mode 🗸 🗸
Interface Grouping		
🚞 IP QoS	Apply Changes	
QoS Policy		
QoS Classification		
Traffic Shaping		
PoE Settings		
Link Mode		
Others		
iii IPv6		
Diagnostics		
admin		
Statistics		

Advance \rightarrow Link mode

To save changes, click Apply Changes.

6.5.8 Others submenu. Additional settings

In this section, you can configure end-to-end IP transmission for WAN interfaces, as well as enable/disable JumboFrame transmission.

ELAN WAN	Other Advanced Configuration Here you can set some other advanced settings.	
Services	IP PassThrough: NONE V Lease Time: 600 second	ds.
ARP Table	Allow LAN access	
Bridging	JumboFrame: Oisable OiEnable	
Routing Interface Grouping IP QoS QoS Policy QoS Classification Traffic Shaping PoE Settings Link Mode Others IPv6 Diagnostics Admin Statistics	Apply Changes	

Advance \rightarrow Others

6.5.9 IPv6 submenu. Configuring IPv6 protocol

In this section, you can enable/disable IPv6; to do this, select Enable or Disable.

Advance → IPv6



6.5.9.1 RADVD submenu. Configuring RADVD

The section is used to configure RADVD (Router Advertisement Daemon).

Advance \rightarrow IPv6 \rightarrow RADVD

Status	RADVD Configuration		
	This page is used to set	up the RADVD's cont	figuration of your Dev
WAN			
Services	MaxRtrAdvInterval:	600	
Advance			
ARP lable	MinRtrAdvInterval:	198	
Bridging	AdvManagedFlag:	⊙off ○on	
Routing	AdvOtherConfigFlag:	⊖off ⊙on	
Interface Grouping			
IP QoS			
PoE Settings	Apply Changes		
Link Mode			
Others			
IPv6			
IPv6			
DHCPv6			
MLD Proxy			
MLD Snooping			
IPv6 Routing			
IP/Port Filtering			
Diagnostics			
Admin			
Statistics			

- MaxRtrAdvInterval maximum interval for sending RA (Router Advertisement);
- *MinRtrAdvInterval* minimum interval for sending RA;
- AdvManagedFlag enable/disable sending Managed flag to RA;
- AdvOtherFlag enable/disable sending Other RA flag.

6.5.9.2 DHCPv6 submenu. Configuring DHCPv6 Server

The section is used to configure DHCPv6 server. By default, it works in auto-configuration mode (DHCPServer(Auto)) via prefix delegation.

📄 Status	DHCPv6 Settings
LAN	
WAN	This page is used to configure DHCPv6 Server and DHCPv6 Relay.
Services	
Advance	
ARP Table	DHCPv6 Mode: ODisable 🔍 Enable;
	Auto Config by Prefix Delegation for DHCPv6 Server. Show Client Apply Changes
Interface Grouping	
	NTP Server IP: Add
PoE Settings	
Link Mode	NTP Server Table
Others	Soloct NTD Server
IPv6	
IPv6	
RADVD	
DHCPv6	
MLD Proxy	
MLD Snooping	Add
IPv6 Routing	MAC Address:
IP/Port Filtering	IP Address:
Diagnostics	
	MAC Dividing Table
Statistics	MAC Binuny Table
Statistics	Select Host Name MAC Address IP Address
	Delete Selected

Advance \rightarrow IPv6 \rightarrow DHCPv6

- DHCPv6 Mode enable/disable the operation of DHCPv6 server;
- NTP Server IP specify the IP address of NTP server for time synchronization;
- Hostname specify the hostname;
- MAC Address specify client's MAC address to bind the IP address;
- IP Address specify client's IP address to bind to the MAC address.

To save changes, click **Apply Changes**. **Show Client** button is used to view a table of active IP addresses of DHCPv6 server.

Advance \rightarrow IPv6 \rightarrow DHCPv6 \rightarrow Show Client

Active DHCPv6 Clients
This table shows the assigned IP address, DUID and time expired for each DHCP leased client.
IP Address DUID Expired Time (sec) NONE
Refresh Close

6.5.9.3 MLD proxy submenu. Configuring MLD proxy function

In this section, you can enable/disable the operation of the MLD-proxy; to do this, you need to select **Enable** or **Disable**.

Status	MLD ProxyConfigura	tion	
LAN			
WAN	This page be used	to configure	MLD Proxy.
Services		60.58 (0.00)	
Advance	MLD Proxy:	Disable	🔘 Enable
🗋 ARP Table	WAN Interface:	~	
Bridging			
Routing			
Interface Grouping	Apply Changes		
📄 IP QoS			
PoE Settings			
Link Mode			
Others			
IPv6			
IPv6			
RADVD			
DHCPv6			
MLD Proxy			
MLD Snooping			
IPv6 Routing			
IP/Port Filtering			
Diagnostics			
Admin			
Statistics			

Advance \rightarrow IPv6 \rightarrow MLD proxy

6.5.9.4 MLD snooping submenu. Setting up the MLD snooping function

In this section, you can enable/disable MLD-snooping; to do this, you need to select Enable or Disable.

Advance \rightarrow IPv6 \rightarrow MLD snooping



6.5.9.5 IPv6 routing submenu. Configuring IPv6 routes

Static IPv6 routes are configured in this section.

Advance \rightarrow	IPv6 →	IPv6	routing
-----------------------	--------	------	---------

i∎Status DLAN	IPv6 Static R	outingCon	figuration			
WAN	This page is us routes.	ed to confi	gure the IPv6 static rol	uting information. Here	e you can add/	'delete static IP
Advance	Enable:		✓			
ARP Table	Destination:					
Routing	Next Hop:					
Interface Grouping	Metric:					
PoE Settings	Interface:		Any 🗸	Dalata All Chaw B	Poutoc	
Link Mode						
IPv6	Static IPv6 R	oute Table	e:			
	Select	State	Destination	Next Hop	Metric	Interface
DHCPv6						
MLD Proxy						
MLD Snooping						
IPv6 Routing						
IP/Port Filtering						
Diagnostics						
Admin						
Statistics						

- Enable add a route;
- Destination destination address;
- Next Hop next node;
- Metric metric;
- Interface interface.

To add IPv6 routing, complete the appropriate fields and click **Add Route**. The added routes are displayed in **Static IPv6 Route Table**, to update the information, click **Update**. To delete the entire table, click **Delete All**, to delete one route, select it and click **Delete Selected**. The **Show Routes** button displays a table of static IPv6 routes that the network usually accesses.

IP Route Table						
This table shows a list of destination routes commonly accessed by your network.						
Destination	Next Hop	Flags	Metric	Ref	Use	Interface
fe80::/64	::	U	256	0	0	br0
fe80::/128	::	U	0	1	0	lo
fe80::ce9d:a2ff:fedc:dc0c/128	::	U	0	1	0	lo
ff00::/8	::	U	256	2	25010	br0
Refresh Close						

Advance \rightarrow IPv6 \rightarrow IPv6 routing \rightarrow Show Routes

- Destination network destination;
- Next Hop next node;
- Flags flags;
- · Metric metric;
- Ref route source;

- Use route usage;
- Interface the interface through which the specified route is accessible.

To update the table, click **Refresh**, to close the window – **Close**.

6.5.9.6 IPv6 IP/Port filtering submenu. Configuring packet filtering

The page is used to configure filtering of data packets transmitted through the gateway.

Advance \rightarrow	IPv6 →	IP/Port filtering
-----------------------	--------	-------------------

Status	IPv6 IP/Port Filtering
LAN WAN	Entries in this table are used to restrict certain types of data packets through the Gateway. Use of such filters can be helpful in securing or restricting your local network.
Advance ARP Table Bridging Routing Interface Grouping	Outgoing Default Action O Deny Incoming Default Action Incoming Default Action Image: O Deny O Allow Apply Changes Image: O Deny Image: O Deny
IP QoS PoE Settings Link Mode Others IPv6 IPv6 RADVD DHCPv6	Direction: Outgoing V Protocol: TCP V Rule Action O Deny Allow Source Interface ID: Destination Interface ID: Source Port:
MLD Proxy MLD Snooping IPv6 Routing IP/Port Filtering Diagnostics Admin Statistics	Current Filter Table: Select Direction Protocol Source IP Address Interface ID Source Port Destination IP Address Interface ID Delete Selected Delete All Enterface ID Delete All Enterface ID Enterface ID

- Outgoing Default Action Deny/Allow filtering of outgoing packets;
- Incoming Default Action Deny/Allow filtering of incoming packets.

To save changes, click Apply Changes.

- Direction direction of packet transmission (outgoing/incoming);
- Protocol select protocol;
- Rule Action packet processing policy (Deny drop out; Allow transmit);
- Source Interface ID source interface;
- Destination Interface ID destination interface;
- · Source Port;
- Destination Port.

To add a filter, complete the appropriate fields and click **Add**. The added filters are displayed in **Current Filter Table**. To delete the entire table, click the **Delete All** button; to delete one filter, select it and click **Delete Selected**.

6.6 Diagnostics menu

The section is for diagnostics of access to various network nodes.

6.6.1 Ping submenu. Checking the availability of network devices

The section is designed to check the availability of network devices using the Ping utility.

$Diagnostios \rightarrow 1 mg$	Diag	nostics	\rightarrow	Ping
--------------------------------	------	---------	---------------	------

Status	Ping Diagnostics
LAN	This page is used to send ICMP ECHO REOUEST packets to network host. The diagnostic result will then be displayed.
WAN	
Services	
📄 Advance	Hust Aduress:
Diagnostics	
Ping	Go
Traceroute	
System Log	
admin	
Statistics	

To check the availability of the connected device, enter its IP address in the Host Address field and click Go.

6.6.2 Traceroute submenu. Network diagnostics

The section is intended for network diagnostics by sending UDP packets and receiving a message about port availability/unavailability.

Diagnostics -	 Traceroute
---------------	--------------------------------

Status	Traceroute Diagnostics
LILAN WAN	This page is used to diagnose the network by sending UDP-packets and receiving a message about port reach/unreachability.
Services	
🚞 Advance	Host Address:
Diagnostics	Max number of hops:
Ping	
Traceroute	Go
System Log	
admin	
Statistics	

To diagnose a network, you should enter an IP address of the connected device in the **Host address** field and the maximum number of hops for a packet.

6.6.3 System Log submenu. Logging system events

The section is intended for configuring/saving/viewing logging of system events. Logging can be disabled/ enabled by selected **Disable** or **Enable**.

Status	System Log		
LAN			
WAN	System Log :	Disable OEnable	
Services	Log Level :	Emergency 🗸	
Advance	Display Level :	Emergency 🛩	
Ping	Apply Changes		
Traceroute		Save	
System Log	Clear Log:	Reset	
Admin	_		
Statistics	System Log	Refres	;h

Diagnostics → System Log

- Log Level logging level;
- Display Level log display level;
- Clear log clear the log.

To save the log to the local storage, click the Save button.

6.7 Admin menu

Device management section. In this menu, passwords, time, configurations and other settings are configured.

6.7.1 Settings submenu. Restore and reset settings

Admin → Settings → Backup Settings



In the section, you can copy the current settings to a file (Backup Settings) by clicking Backup Settings to File.

Admin \rightarrow Settings \rightarrow Update Settings

Status LAN WAN Services Advance Diagnostics Admin Settings Update Restore Default OPON Settings Commit/Reboot Logout Firmware Upgrade Remote Access Time Zone Statistics	Update Settings This page allows you to restore settings from file Restore Settings from File: Choose File No file chosen Restore
--	--

In the section, you can restore settings from a file that was saved earlier (update settings). Click **Choose File** to select a file, then click **Restore**.

Status	Restore Default
LAN	
WAN	This page allows you to restore factory default settings
Services	
🔚 Advance	Reset Settings to Default
Diagnostics	
admin	
Settings	
Backup	
Update	
Restore Default	
GPON Settings	
Commit/Reboot	
Logout	
Password	
🗋 Firmware Upgrade	
Remote Access	
Time Zone	
TR-069	
Statistics	

Admin \rightarrow Settings \rightarrow Restore Default

In this section, you can reset the current settings to the factory default settings (*Restore Default*), to do this, click **Reset Settings to Default**.

6.7.2 GPON Setting submenu. Configuring access to GPON

In this section, you can specify a password to activate the device on OLT.

Admin → GPON Setting



• PLOAM Password – password to activate the terminal on OLT.

6.7.3 Commit/Reboot submenu. Saving changes and restarting the device

Click **Commit and Reboot** to reboot the device or to save changes to the system memory. It may take several minutes to restart the device.

Status	Commit and Reboot
	Click the button below to reboot the router
Services	
Advance	Commit and Pohoot
Diagnostics	Commit and Repoor
admin	
E Settings	
Backup	
Update	
Commit/Reboot	
Logout	
Password	
Firmware Upgrade	
Remote Access	
Time Zone	
Ctatiotica	
Staustics	



6.7.4 Logout submenu. Log out the account

In the section it is possible to log out the account by clicking Logout.



Admin → Logout

6.7.5 Password submenu. Setting up access control (setting passwords)

In this section, you may change the password for access to the device.

Admin →	Password
---------	----------

Status	Password Configuration
	This page is used to set the account to access the web server of your Device. Empty user name and password will disable the protection.
Advance	UserName: admin 🗸
Admin	Old Password:
Settings	New Password:
DUpdate Restore Default GPON Settings Commit/Rehoot	Apply Changes Reset
Logout Password	
⊢irmware ∪pgrade Remote Access Time Zone	
TR-069	

To change the password, enter the current password to the **Old Password** field, then the new password to **New Password** and to **Confirmed Password**.

To save changes, click Apply Changes; to reset the value, click Reset.

6.7.6 Firmware upgrade submenu. Software Update

To update the software, select the software file using the **Choose File** button and click **Upgrade**. To reset the value, use **Reset**.

Status	Firmware Upgrade
WAN	Step 1: Obtain an updated software image file from your ISP.
Advance	Step 2: Click the "Choose File" button to locate the image file.
Diagnostics Admin	Step 3: Click the "Upgrade" button once to upload the new image file.
Settings	NOTE: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.
Update	
Restore Default	Choose File No file chosen
GPON Settings	[Ingrade] Reset
Password	
Firmware Upgrade	
Remote Access	
Time Zone	
TR-069	
Statistics	

Admin → Firmware upgrade

During the update process, it is not allowed to turn off the device's power or restart it. The update process may take several minutes, after which the device automatically reboots.

6.7.7 Remote Access submenu. Configuring remote access rules

In the section it is possible to configure remote access rules using HTTP/Telnet/ICMP protocols.

Admin → Remote Access

Estatus	Remote Acces	s Configuration				
	This page is used to configure the Remote Access rules.					
Services						
🚞 Advance	Enable:					
Diagnostics	Service:					
Admin	Interface:					
Settings	interface.					
Backup	IP Address:	0.0.0.0				
Destars Default	Subnet Mask:	0.0.0.0				
GPON Settings	Port:					
Commit/Reboot						
Loqout	Add					
Password						
Firmware Upgrade	RA Table:					
Remote Access	Select	State	Interface	IP Address	Service	Port
Time Zone		Enable	LAN	0.0.0/0	ICMP	
TR-069		Enable	LAN	0.0.0/0	HTTP	80
Statistics						
	Delete Selected	d 🛛 🗌 Toggle Selec	ited			

- Enable add a rule;
- Service select protocol;
- Interface an interface to which the rule applies;
- *IP Address* source IP address;
- Subnet Mask subnet mask;
- Port destination port.

To add a rule, complete the appropriate fields and click **Add**. The added rules are displayed in **RA Table**. To activate/deactivate the selected rule, click the **Toggle selected** button. To delete one rule, select it in the column **Select** and click **Delete Selected**.

6.7.8 Time zone submenu. Configuring system time

In this section you may configure system time, synchronization with Internet servers of the exact time is also available.

Status	Time ZoneConfiguration
LAN	Martin and the first and a strategic strategic and a strategic st
WAN	You can maintain the system time by synchronizing with a public time server over the internet.
Services	
Advance	Year[2022 Mon[1 Day]7
Diagnostics	Current lime :
admin	
🚞 Settings	Time Zone Select : Europe/Moscow (UTC+03:00)
Backup	
Update	Enable Daylight Saving Time
Restore Default	Enable SNTP Client Update
GPON Settings	WAN Interface: Any 🗸
Commit/Reboot	SNTP Server : 💿 clock.fmt.he.net 🗸
Logout	O clock fmt he net (Manual Setting)
Password	Cockennation of Charleshoe
Firmware Upgrade	Apply Changes Refresh
Remote Access	
Time Zone	
TR-069	
Statistics	

Admin → Time zone

- Current time current time;
- Time Zone Select time zone;

- Enable Daylight Saving Time daylight saving time;
- Enable SNTP Client Update enable SNTP time synchronization;
- WAN Interface the interface through which the time is updated;
- SNTP Server is the preferred time server.

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

6.7.9 TR-069 submenu. Configuring TR-069

The section is used to specify the data for configuring the device via TR-069.

Status LAN WAN	TR-069 Configuration	re the TR-069 CPE. Here you may change the setting for the ACS's parameters.
Services Advance Diagnostics	TR069 Daemon: EnableCWMPParamete:	Enabled Olisabled Olisabled
Admin Settings Backup Update Restore Default GPON Settings Commit/Reboot Logout Password Firmware Upgrade Remote Access Time Zone TR-069 Statistics	ACS: URL: UserName: Password: Periodic Inform: Periodic Inform Interval: Connection Request: UserName: admin Password: admin Path: Port: 30005	http:// username password O Disabled ③Enabled
	Apply Undo Certificate Management: CPE Certificate Password CPE Certificate: CA Certificate:	: client Apply Undo Choose File No file chosen Upload Choose File No file chosen Upload

Admin \rightarrow TR-069

- TR069 Daemon enable/disable TR-069 daemon;
- EnableCWMPParamete (Enabled/Disabled) permission/prohibition of CWMP settings;
- ACS configuring the ACS server;
- URL URL for connection;
- UserName the name of the user to access the server;
- Password the user's password to access the server;
- Periodic Inform enabling/disabling the frequency of sending messages;
- Periodic Inform Interval the time interval of sending messages.

Connection Request – authorization data for connecting the server to ONT.

- UserName user name;
- Password password for connection;
- Path connection path;
- *Port* port to connect to.

Certificate Management – certificate management.

- CPE Certificate Password certificate password;
- CPE Certificate select certificate for CPE;
- CA Certificate select certificate for CA.

To save changes, click Apply, to reset – Undo.

To upload a file, click **Choose File** to select a file, then click **Upload**.

6.8 Statistics menu. Information about the traffic on the device ports

6.8.1 Interface submenu. Information about counters and errors

The section displays counters/errors in packets for each interface:

Statistics \rightarrow Ir	nterface
-----------------------------	----------

Status LAN WAN	Interface Statisit This page shows th	cs e packet statistics fo	r transmission an	d reception regard	ing to network interfa		
Services	Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
Diagnostics	LAN 1	523836	0	0	69055	0	0
Admin	LAN 2	0	0	0	0	0	0
Platini	LAN 3	0	0	0	0	0	0
	LAN 4	0	0	0	0	0	0
	Refresh Reset 9	Statistics					

- Interface interface;
- *Rx pkt* received packets;
- *RX err* reception errors;
- Rx drop dropped on reception;
- Tx pkt packets sent;
- *Tx err* sending error;
- *Tx drop* dropped during transmission.

To update the data on the page, click Refresh.

6.8.2 PON submenu

The section displays counters for the optical interface:

Statistics	→ PON
------------	-------

PON Statistics		
Bytes Sent	58932	
Bytes Received	196338	
Packets Sent	330	
Packets Received	1309	
Unicast Packets Sent	324	
Unicast Packets Received	445	
Multicast Packets Sent	0	
Multicast Packets Received	549	
Broadcast Packets Sent	6	
Broadcast Packets Received	315	
FEC Errors	0	
HEC Errors	0	
Packets Dropped	0	
Pause Packets Sent	0	
Pause Packets Received	0	

The following statistics are available:

- Bytes Sent;
- Bytes Received;
- Packets Sent;
- · Packets Received;
- Unicast Packet Sent;
- Unicast Packet Received;
- Multicast Packets Sent;
- Multicast Packets Received;
- Broadcast Packet Sent;
- Broadcast Packet Received;
- FEC Errors;
- HEC Errors;
- Packets Dropped;
- Pause Packets Sent;
- Pause Packets Received.

TECHNICAL SUPPORT

For technical assistance in issues related to handling Eltex Ltd. equipment, please, address to Service Center of the company: https://eltex-co.com/support/

You are welcome to visit Eltex official website to get the relevant technical documentation and software.

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

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