



Оптический сетевой терминал

## **NTU-MD500P**

Руководство по эксплуатации, Версия ПО 2.4.7

## Содержание

<b>1</b>	<b>Список изменений</b> .....	<b>5</b>
<b>2</b>	<b>Введение</b> .....	<b>6</b>
<b>3</b>	<b>Описание изделия</b> .....	<b>7</b>
3.1	Назначение .....	7
3.2	Характеристики устройств.....	7
3.3	Основные технические параметры .....	8
3.4	Конструктивное исполнение.....	10
3.4.1	Внешний вид и описание передней панели устройства.....	10
3.4.2	Боковая и задняя панели устройства .....	11
3.5	Световая индикация .....	12
3.6	Комплект поставки.....	13
<b>4</b>	<b>Порядок установки и подключения</b> .....	<b>14</b>
4.1	Условия эксплуатации и порядок установки.....	14
4.1.1	Требования техники безопасности.....	14
4.1.2	Порядок установки терминала.....	14
4.2	Подключение устройства.....	17
<b>5</b>	<b>Архитектура устройства</b> .....	<b>18</b>
<b>6</b>	<b>Настройка устройства через Web-интерфейс. Доступ администратора.</b> .....	<b>19</b>
6.1	Меню «Status». Информация об устройстве.....	21
6.1.1	Подменю «Device status». Общая информация об устройстве.....	21
6.1.2	Подменю «IPv6 Status». Информация о системе IPv6 .....	22
6.1.3	Подменю «PON». Информация о статусе оптического модуля.....	23
6.1.4	Подменю «LAN». Информация о статусе интерфейса LAN.....	24
6.2	Меню «LAN». Настройка интерфейса LAN .....	24
6.3	Меню «WAN». Настройка интерфейса WAN .....	25
6.3.1	Подменю «PON WAN» .....	25
6.3.2	Подменю «VPN» .....	26
6.3.2.1	Подменю «L2TP». Настройка L2TP VPN.....	26
6.3.2.2	Подменю «IPsec». Настройка IP Security .....	27
6.4	Меню «Services». Настройка сервисов .....	29
6.4.1	Подменю «DHCP Setting». Настройка DHCP .....	29
6.4.2	Подменю «DNS» .....	30
6.4.2.1	Подменю «Dynamic DNS». Настройки динамической системы доменных имен .....	30
6.4.3	Подменю «Firewall». Настройка брандмауэра .....	31
6.4.3.1	Подменю «ALG On-Off Configuration». Включение отключение сервисов ALG. ....	31

6.4.3.2	Подменю «IP/Port Filtering». Настройки фильтрации адресов.....	31
6.4.3.3	Подменю «MAC Filtering». Настройки фильтрации по MAC-адресам.....	32
6.4.3.4	Подменю «Port Forwarding». Настройка проброса портов.....	33
6.4.3.5	Подменю «URL Blocking». Настройки ограничения доступа в интернет.....	34
6.4.3.6	Подменю «Domain Blocking». Настройка блокировки доменов.....	34
6.4.3.7	Подменю «DMZ». Настройки демилитаризованной зоны.....	35
6.4.4	Подменю «UPnP». Автоматическая настройка сетевых устройств.....	35
6.4.5	Подменю «RIP». Настройка динамической маршрутизации.....	36
6.5	Меню «Advance». Расширенные настройки.....	36
6.5.1	Подменю «ARP Table». Просмотр кэша протокола ARP.....	36
6.5.2	Подменю «Bridging». Настройка параметров Bridging.....	37
6.5.3	Подменю «Routing». Настройка маршрутизации.....	38
6.5.4	Подменю «Interface grouping». Объединение интерфейсов в группы.....	38
6.5.5	Подменю «IP QoS». Настройка качества предоставляемых услуг (QoS).....	39
6.5.5.1	Подменю «QoS Policy». Настройка QoS-очередей.....	39
6.5.5.2	Подменю «QoS Classification». Настройка правил классификации трафика.....	40
6.5.5.3	Подменю «Traffic Shaping». Настройка трафика.....	41
6.5.6	Подменю «PoE Settings». Конфигурирование PoE-портов.....	42
6.5.7	Подменю «Link mode». Настройка LAN-портов.....	43
6.5.8	Подменю «Others». Дополнительные настройки.....	43
6.5.9	Подменю «IPv6». Настройка протокола IPv6.....	44
6.5.9.1	Подменю «RADVD». Настройка RADVD.....	44
6.5.9.2	Подменю «DHCPv6». Настройка DHCPv6-сервера.....	45
6.5.9.3	Подменю «MLD proxy». Настройка функции MLD proxy.....	46
6.5.9.4	Подменю «MLD snooping». Настройка функции MLD snooping.....	46
6.5.9.5	Подменю «IPv6 routing». Настройка IPv6-маршрутов.....	46
6.5.9.6	Подменю «IPv6 IP/Port filtering». Настройка фильтрации пакетов.....	47
6.6	Меню «Diagnostics».....	48
6.6.1	Подменю «Ping». Проверка доступности сетевых устройств.....	48
6.6.2	Подменю «Traceroute». Диагностика сети.....	48
6.6.3	Подменю «System Log». Логирование системных событий.....	49
6.7	Меню «Admin».....	49
6.7.1	Подменю «Settings». Восстановление и сброс настроек.....	49
6.7.2	Подменю «GPON Setting». Настройка доступа к GPON.....	50
6.7.3	Подменю «Commit/Reboot». Сохранение изменений и перезагрузка устройства.....	50
6.7.4	Подменю «Logout». Выход из учетной записи.....	50
6.7.5	Подменю «Password». Настройка контроля доступа (установление паролей).....	51
6.7.6	Подменю «Firmware upgrade». Обновление ПО.....	51

6.7.7	Подменю «Remote Access». Настройка правил удалённого доступа .....	52
6.7.8	Подменю «Time zone». Настройки системного времени.....	52
6.7.9	Подменю «TR-069». Настройка TR-069.....	53
6.8	Меню «Statistics». Информация о прохождении трафика на портах устройства .....	54
6.8.1	Подменю «Interface». Информация о счетчиках и ошибках.....	54
6.8.2	Подменю «PON».....	55

# 1 Список изменений

<b>Версия документа</b>	<b>Актуальность для ПО</b>	<b>Дата выпуска</b>	<b>Содержание изменений</b>
Версия 1.1	2.4.7	09.2022	Вторая публикация
Версия 1.0	1.0.1	04.2021	Первая публикация




## 2 Введение

Сеть GPON относится к одной из разновидностей пассивных оптических сетей PON. Это одно из самых современных и эффективных решений задач «последней мили», позволяющее существенно экономить на кабельной инфраструктуре и обеспечивающее скорость передачи информации до 2,5 Гбит/с в направлении downlink и 1,25 Гбит/с в направлении uplink. Использование в сетях доступа решений на базе технологии GPON дает возможность предоставлять конечному пользователю доступ к новым услугам на базе протокола IP совместно с традиционными сервисами.

Основным преимуществом GPON является использование одного станционного терминала (OLT) для нескольких абонентских устройств (ONT). OLT является конвертером интерфейсов Gigabit Ethernet и GPON, служащим для связи сети PON с сетями передачи данных более высокого уровня. Устройство ONT предназначено для подключения к услугам широкополосного доступа оконечного оборудования клиентов. Может применяться в жилых комплексах и бизнес-центрах.

В настоящем руководстве по эксплуатации изложены назначение, основные технические характеристики, правила конфигурирования, мониторинга оптического сетевого терминала NTU-MD500P.

### Примечания и предупреждения

-  Примечания содержат важную информацию, советы или рекомендации по использованию и настройке устройства.
-  Примечания содержат дополнительную информацию по использованию и настройке устройства.
-  Предупреждения информируют пользователя о ситуациях, которые могут нанести вред устройству или человеку, привести к некорректной работе устройства или потере данных.

## 3 Описание изделия

### 3.1 Назначение

NTU-MD500P – оптический сетевой терминал, который имеют 4 порта 10/100/1000BASE-T с поддержкой стандарта IEEE 802.3at PoE+. Терминал NTU-MD500P обеспечивает мощность до 30 Вт на портах 10/100/1000BASE-T с бюджетом мощности PoE – 65 Вт.

Поддержка технологии PoE позволяет подать электропитание от NTU-MD500P по кабелю UTP к IP-телефонам, беспроводным точкам доступа, IP-камерам и другим устройствам с поддержкой технологии PoE.

Преимуществом технологии GPON является оптимальное использование полосы пропускания. Эта технология является следующим шагом для обеспечения новых высокоскоростных интернет-приложений дома и в офисе. Разработанные для развертывания сети внутри дома или здания, данные устройства ONT обеспечивают надежное соединение с высокой пропускной способностью на дальние расстояния для пользователей, живущих и работающих в удаленных многоквартирных зданиях и бизнес-центрах.

### 3.2 Характеристики устройств

**Устройство имеет следующие интерфейсы:**

- 1 порт PON SC/APC для подключения к сети оператора (WAN);
- Порты Ethernet RJ-45 LAN для подключения сетевых устройств (LAN):
  - 4 порта RJ-45 10/100/1000BASE-T.

**Устройство поддерживает следующие функции:**

- *Управление и мониторинг PoE через 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.
- *Сетевые функции:*
  - поддержка TR-069;
  - работа в режиме «моста» или «маршрутизатора»;
  - поддержка PPPoE (auto, PAP-, CHAP-, MSCHAP-авторизация);
  - поддержка IPoE (DHCP-client и static);
  - поддержка DNS (Domain Name System);
  - поддержка DynDNS (Dynamic DNS);
  - поддержка UPnP (Universal Plug and Play);
  - поддержка VPN в режиме L2TP;
  - поддержка L2TP over IPSec;
  - поддержка IPSec (transport mode);
  - поддержка NAT (Network Address Translation);
  - поддержка NTP (Network Time Protocol);
  - поддержка механизмов качества обслуживания QoS;
  - поддержка IGMP-snooping;
  - поддержка IGMP-proxy;
  - VLAN в соответствии с IEEE 802.1Q.

- Обновление ПО через TR-069, OMCI, HTTP, TFTP;
- Удаленный мониторинг, конфигурирование и настройка:
  - SNMP-agent OLT;
  - CLI OLT.

На рисунках ниже приведена схема применения оборудования NTU-MD500P.

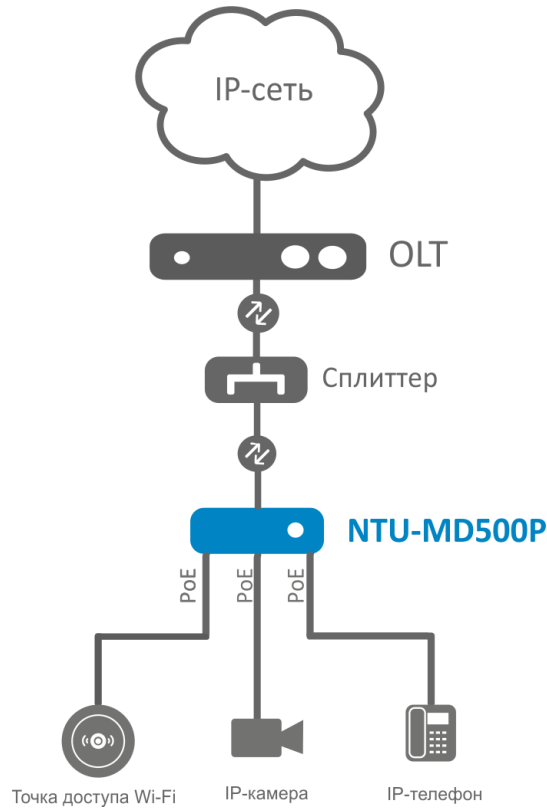


Рисунок 1 – Схема применения NTU-MD500P

### 3.3 Основные технические параметры

Основные технические параметры терминала приведены в [таблице 1](#):

Таблица 1 – Основные технические параметры

#### Параметры интерфейсов Ethernet LAN

Количество интерфейсов	4
Электрический разъем	RJ-45
Скорость передачи	Автоопределение, 10/100/1000 Мбит/с, дуплекс/полудуплекс



Поддержка стандартов	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
----------------------	---

### Параметры интерфейса PON

Количество интерфейсов	1
Поддержка стандартов	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
Тип разъема	SC/APC соответствует ITU-T G.984.2, ITU-T G.984.5 Filter, FSAN Class B+, SFF-8472
Среда передачи	Оптоволоконный кабель SMF – 9/125, G.652
Коэффициент разветвления	До 1:128
Максимальная дальность действия	20 км
Передатчик:	1310 нм
<ul style="list-style-type: none"> <li>Скорость соединения upstream</li> </ul>	1244 Мбит/с
<ul style="list-style-type: none"> <li>Мощность передатчика</li> </ul>	+0,5 дБм до +5 дБм
<ul style="list-style-type: none"> <li>Ширина спектра оптического излучения (RMS)</li> </ul>	1 нм
Приемник:	1490 нм
<ul style="list-style-type: none"> <li>Скорость соединения downstream</li> </ul>	2488 Мбит/с
<ul style="list-style-type: none"> <li>Чувствительность приемника</li> </ul>	от -8 до -28, BER $\leq$ 1.0x10 <sup>-10</sup>
Оптическая перегрузка приемника	-8 дБм

### Управление

Локальное управление	Web/CLI
Удалённое управление	TR-069, OMCI
Обновление программного обеспечения	OMCI, TR-069, HTTP, TFTP
Ограничение доступа	По паролю

## Общие параметры

Питание	110-250 В AC, 50-60 Гц
Потребляемая мощность	Не более 80 Вт
Рабочий диапазон температур	От 0 °С до +40 °С
Относительная влажность	Не более 80 %
Габариты (Ш × В × Г)	267 × 44 × 178 мм
Исполнение	19", типоразмер 1U
Масса	1,56 кг

### 3.4 Конструктивное исполнение

В данном разделе описано конструктивное исполнение устройства. Представлены изображения передней, задней и боковых панелей устройства, описаны разъемы, светодиодные индикаторы и органы управления.

Терминал NTU-MD500P выполнен в металлическом корпусе с возможностью установки в 19" каркас, высота корпуса 1U.

#### 3.4.1 Внешний вид и описание передней панели устройства

Внешний вид передней панели устройства приведен на рисунке 2.

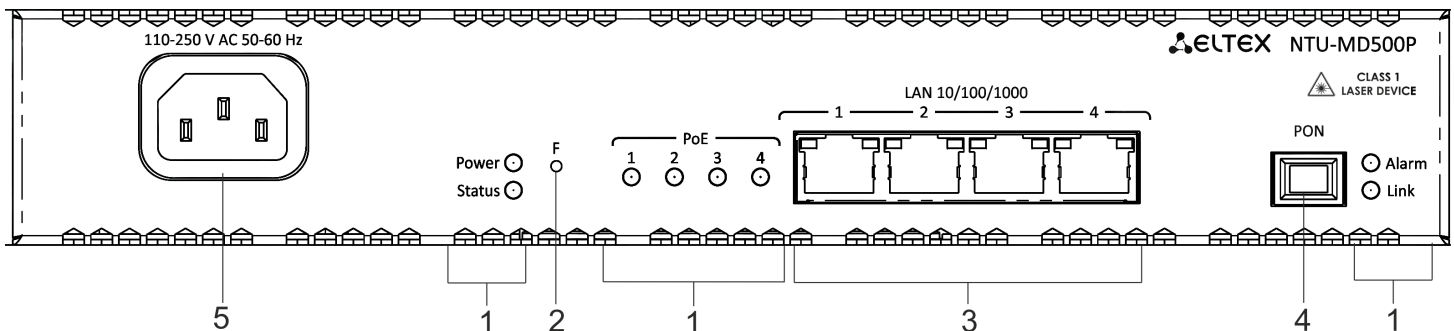


Рисунок 2 – Внешний вид передней панели NTU-MD500P

Таблица 2 – Описание разъемов и органов управления передней панели

№	Элемент передней панели	Описание
1	Power	Индикатор питания устройства.
	Status	Индикатор работы устройства.
	Alarm	Индикатор отсутствия оптического сигнала.

№	Элемент передней панели	Описание
	Link	Индикатор работы оптического интерфейса.
	PoE 1-4	Индикаторы состояния PoE-портов.
2	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам:  - при нажатии на кнопку длительностью менее 10 секунд происходит перезагрузка устройства;  - при нажатии на кнопку длительностью более 10 секунд происходит сброс настроек устройства до заводской конфигурации.
3	LAN 10/100/1000 1..4	4 разъема RJ-45 для подключения сетевых устройств.
4	PON	Разъем SC (розетка) PON оптического интерфейса GPON.
5	110-250 V AC 50-60 Hz	Разъем для подключения к источнику электропитания переменного тока.

### 3.4.2 Боковая и задняя панели устройства

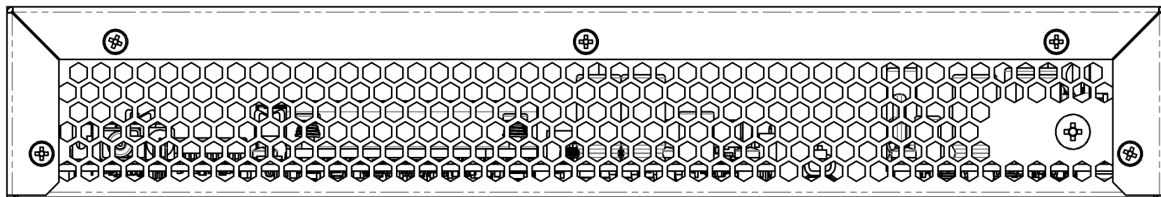


Рисунок 3 – Задняя панель NTU-MD500P

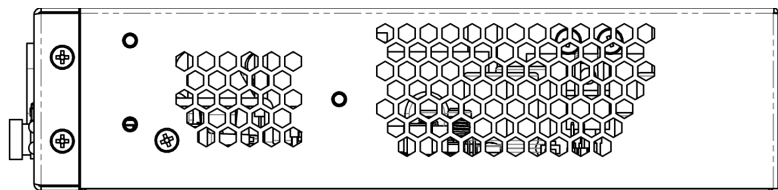


Рисунок 4 – Левая боковая панель NTU-MD500P

На боковой и задней панелях устройства расположены вентиляционные решетки, которые служат для отвода тепла. Не закрывайте вентиляционные отверстия посторонними предметами. Это может привести к перегреву компонентов устройства и вызвать нарушения в его работе. Рекомендации по установке устройства расположены в разделе «Порядок установки и подключения».

### 3.5 Световая индикация

Системные индикаторы (Power, Status, Alarm, Link) служат для определения состояния работы узлов терминала.

Таблица 3 – Световая индикация состояния терминала

Название индикатора	Состояние индикатора	Состояние устройства
<b>Power</b>	Зелёный, горит постоянно	Питание включено, нормальная работа устройства.
	Не горит	Питание выключено.
<b>Status</b>	Красный, горит постоянно	Момент запуска драйверов.
	Зелёный, горит постоянно	На устройстве установлена конфигурация, отличная от конфигурации по умолчанию.
	Зелёный, медленно мигает	На устройстве установлена конфигурация по умолчанию.
<b>PoE 1-4</b>	Зелёный, горит постоянно	Подключен потребитель PoE, подача питания осуществляется (горит индикатор, соответствующий порту).
	Красный, горит постоянно	Ошибка PoE на порту.
	Выключен	Потребитель PoE не подключен.
<b>Alarm</b>	Не горит	Нормальная работа устройства.
	Красный, горит постоянно	Оптический сигнал отсутствует.
<b>Link</b>	Не горит	Процесс загрузки устройства.
	Зелёный, быстро мигает	Получение настроек через OMCI.
	Зелёный, горит постоянно	Устройство успешно сконфигурировано по OMCI.
	Зелёный, медленно мигает	Отсутствует конфигурация (авторизация).
	Красным, медленно мигает	Нет сигнала от OLT.
<b>LAN P1..P4</b>	Зелёный	Установлено соединение 10/100 Мбит/с.
	Оранжевый	Установлено соединение 1000 Мбит/с.
	Мигает	Процесс пакетной передачи данных.

### 3.6 Комплект поставки

В базовый комплект поставки устройства NTU-MD500P входят:

- Оптический сетевой терминал NTU-MD500P;
- Шнур питания Евровилка-C13, 1.8м;
- Комплект крепления в 19" стойку;
- Руководство по эксплуатации (опционально);
- Паспорт;
- Декларация соответствия;
- Памятка о документации.

## 4 Порядок установки и подключения


### 4.1 Условия эксплуатации и порядок установки

В данной главе описаны процедуры установки терминала в стойку и подключения к питающей сети.

#### 4.1.1 Требования техники безопасности

##### Общие требования

При работе с терминалом необходимо соблюдение требований «Правил техники безопасности при эксплуатации электроустановок потребителей».

 Запрещается работать с терминалом лицам, не допущенным к работе в соответствии с требованиями техники безопасности в установленном порядке.

1. Эксплуатация терминала должна производиться инженерно-техническим персоналом, прошедшим специальную подготовку.
2. Подключать к терминалу только годное к применению вспомогательное оборудование.
3. Терминал предназначен для круглосуточной эксплуатации при следующих условиях:
  - температура окружающей среды от 0 °С до +40 °С;
  - относительная влажность воздуха до 80 % при температуре 25 °С;
  - атмосферное давление от  $6,0 \times 10^4$  Па до  $10,7 \times 10^4$  Па (от 450 до 800 мм рт.ст.).
4. Не подвергать терминал воздействию механических ударов и колебаний, а также дыма, пыли, воды, химических реагентов.
5. Во избежание перегрева компонентов терминала и нарушения его работы запрещается закрывать вентиляционные отверстия посторонними предметами и размещать предметы на поверхности терминала.

##### Требования электробезопасности

1. Перед подключением терминала к источнику питания необходимо предварительно заземлить корпус терминала, используя клемму заземления. Крепление заземляющего провода к клемме заземления должно быть надежно зафиксировано. Величина сопротивления между клеммой защитного заземления и земляной шиной не должна превышать 0,1 Ом. Перед подключением к терминалу измерительных приборов и компьютера, их необходимо предварительно заземлить. Разность потенциалов между корпусами терминала и измерительных приборов не должна превышать 1 В.
2. Перед включением терминала убедиться в целостности кабелей и их надежном креплении к разъемам.
3. При установке или снятии кожуха необходимо убедиться, что электропитание устройства отключено.

#### 4.1.2 Порядок установки терминала

Перед установкой и включением необходимо проверить терминал на наличие видимых механических повреждений. В случае наличия повреждений следует прекратить установку устройства, составить соответствующий акт и обратиться к поставщику. Если терминал находился длительное время при низкой температуре, перед началом работы следует выдержать его в течение двух часов при комнатной температуре. После длительного пребывания терминала в условиях повышенной влажности перед включением необходимо выдержать его в нормальных условиях не менее 12 часов.

##### Крепление кронштейнов

В комплект поставки терминала входят кронштейны для установки в стойку и винты для крепления кронштейнов к корпусу терминала. Для установки кронштейнов:

- **Шаг 1.** Совместите четыре отверстия для винтов на кронштейне с такими же отверстиями на боковой панели устройства.
- **Шаг 2.** С помощью отвертки прикрепите кронштейн винтами к корпусу.
- **Шаг 3.** Повторите шаги 1 и 2 для второго кронштейна.

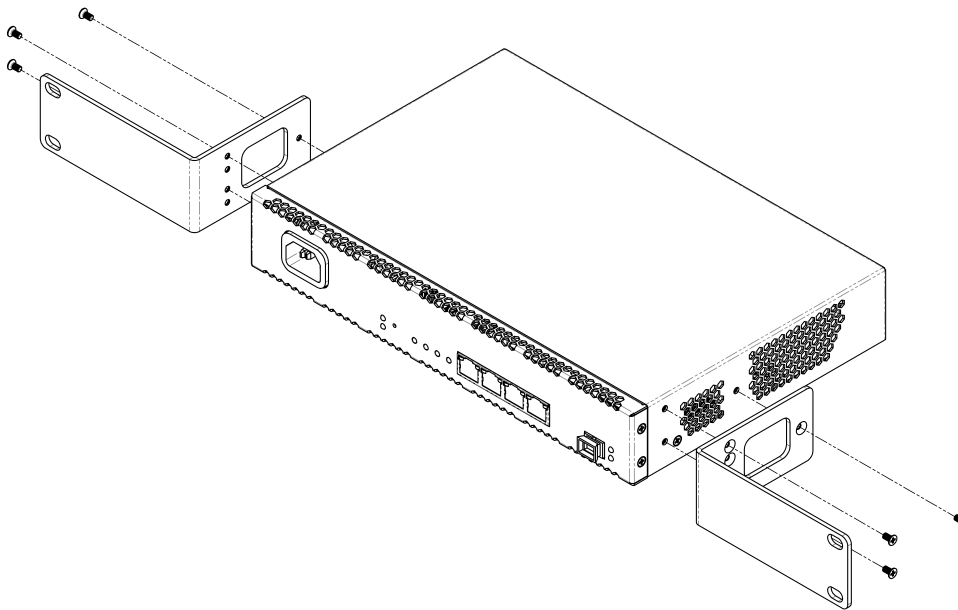


Рисунок 5 – Крепление кронштейнов

##### Установка терминала в стойку

Для установки терминала в стойку:

- **Шаг 1.** Приложите терминал к вертикальным направляющим стойки.
- **Шаг 2.** Совместите отверстия кронштейнов с отверстиями на направляющих стойки. Используйте отверстия в направляющих на одном уровне с обеих сторон стойки, для того чтобы терминал располагался строго горизонтально.
- **Шаг 3.** С помощью отвертки прикрепите терминал к стойке винтами.

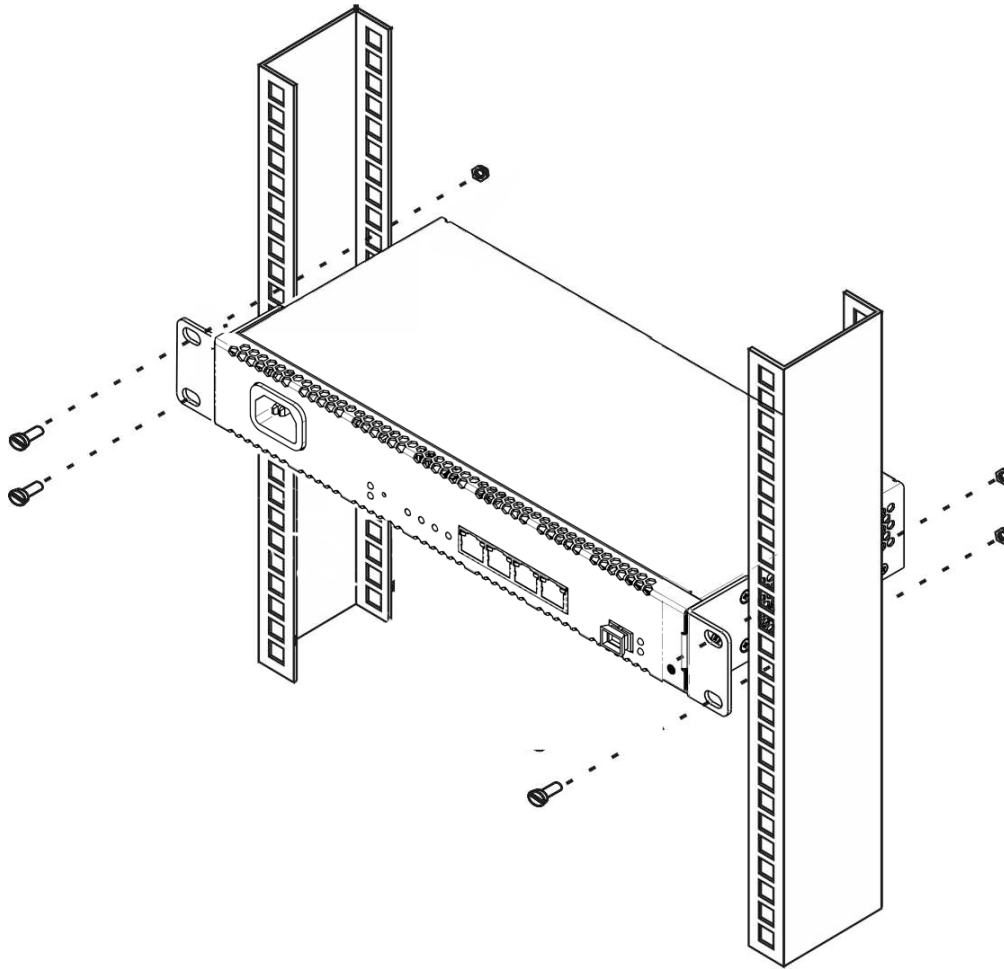


Рисунок 6 – Крепление кронштейнов

Терминал имеет горизонтальную вентиляцию. На боковых панелях терминала расположены вентиляционные отверстия. Не закрывайте вентиляционные отверстия посторонними предметами во избежание перегрева компонентов терминала и нарушения его работы.

**⚠** Для исключения перегрева и обеспечения необходимой вентиляции терминал необходимо разместить так, чтобы над и под ним оставалось свободное пространство не менее 10 см.



## 4.2 Подключение устройства

1. С помощью сетевого Ethernet-кабеля соедините LAN-порт оптического сетевого терминала NTU-MD500P и порт Ethernet компьютера.

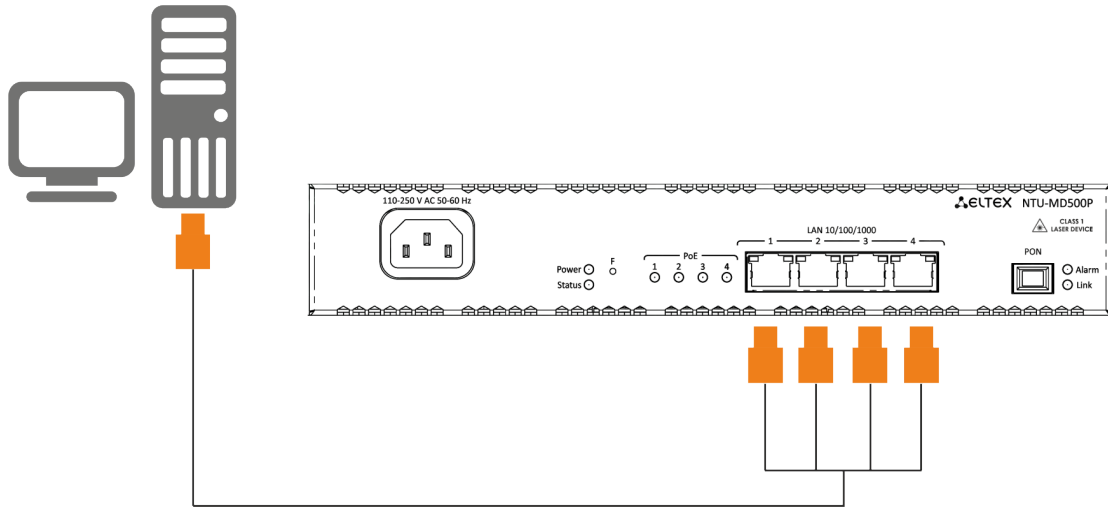


Рисунок 7 – Подключение устройства к компьютеру

2. Подключите оптический кабель, проведенный интернет-провайдером, к разъему PON терминала.

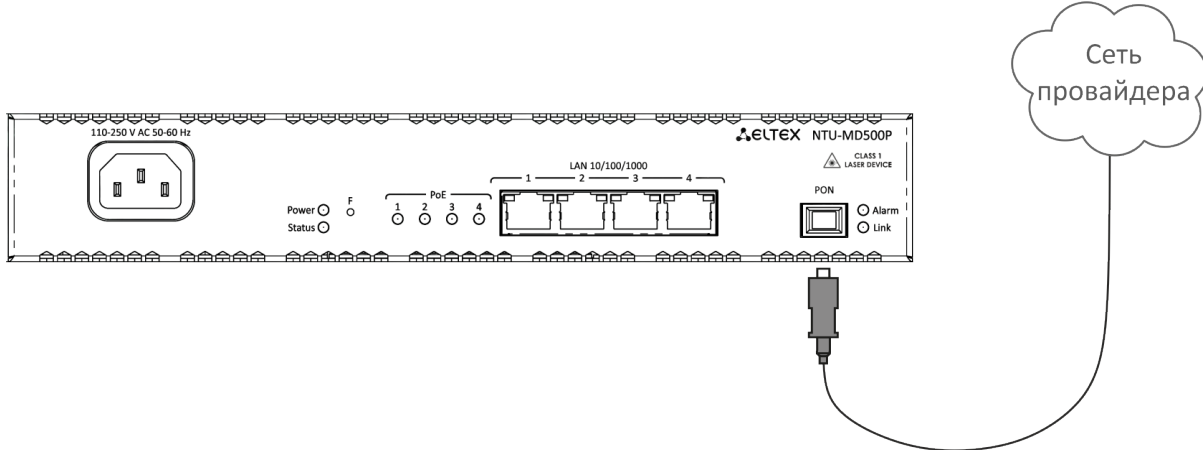


Рисунок 8 – Подключение устройства к интернет-провайдеру

3. Подключите терминал к сети 220 В через адаптер питания. Дождитесь полной загрузки устройства.

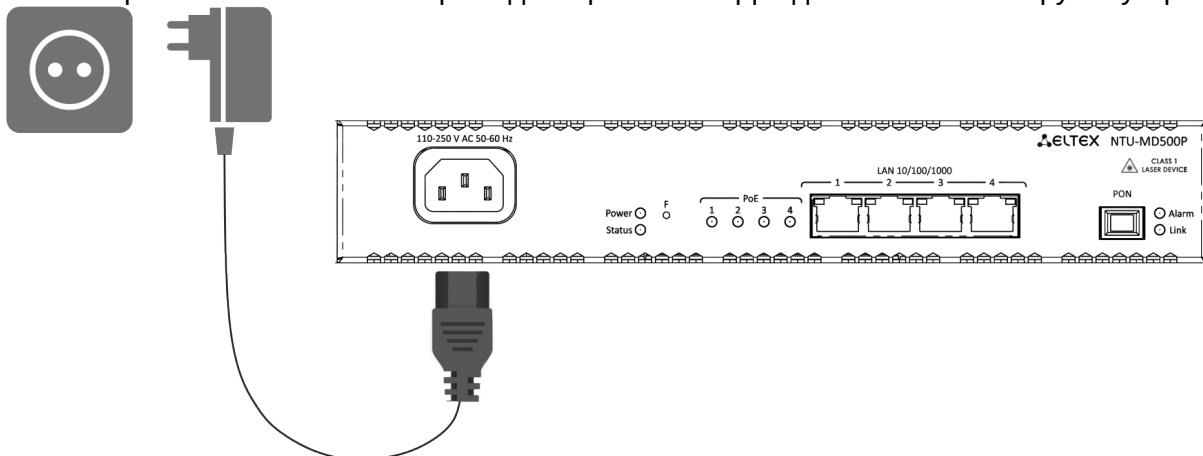


Рисунок 9 – Подключение устройства к сети питания

## 5 Архитектура устройства

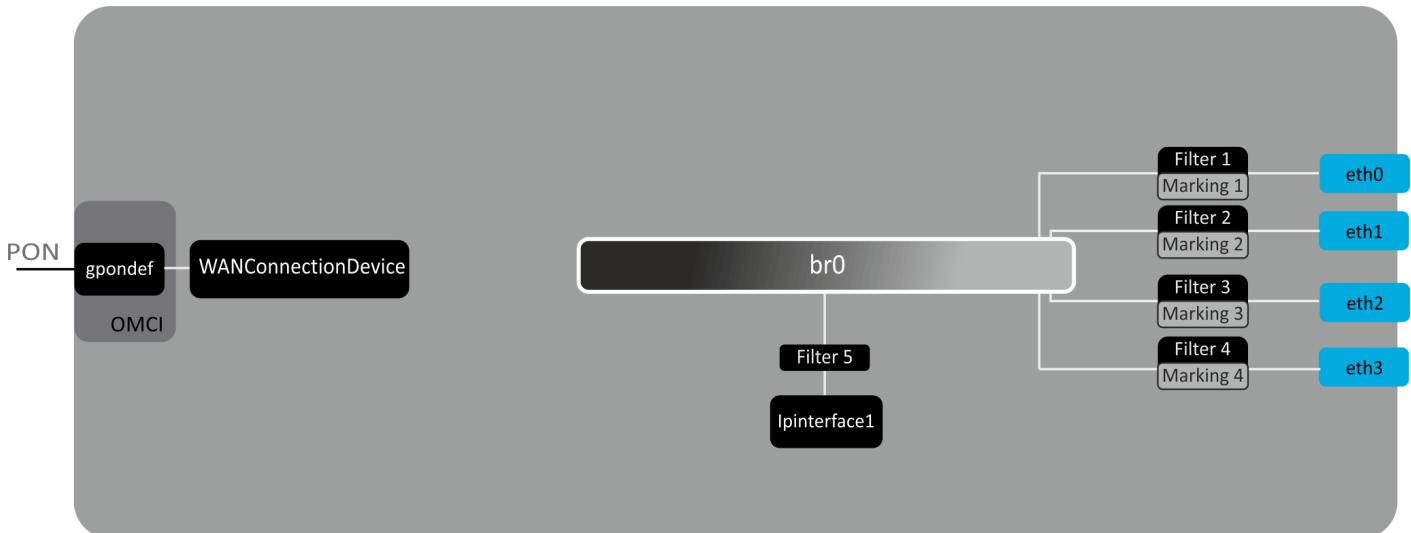


Рисунок 10 – Логическая архитектура устройства с заводской конфигурацией

### Основные элементы устройства:

- **Оптический приемо-передатчик (SFF-модуль)** – предназначен для преобразования оптического сигнала в электрический;
- **Процессор (PON-чип)** – является конвертером интерфейсов Ethernet и GPON.

При заводской (первоначальной) конфигурации в устройстве присутствуют следующие логические блоки (рис. 10):

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

**Блок br0** в данном случае предназначен для объединения портов LAN в одну группу.

**Блоки eth0..3** физически являются Ethernet-портами с разъемом RJ-45 для подключения ПК, STB или других сетевых устройств. Логически включены в блок **br0**.

**Блоки Filter и Marking** предназначены для включения локальных интерфейсов в одну группу (в блок **br0**). Отвечают за правила прохождения трафика, блоки **Filter** отвечают за входящий трафик на интерфейсе, блоки **Marking** – за исходящий.

**Блок IPInterface1** представляет собой некий логический объект, на котором располагается IP-адрес для доступа в локальной сети, а также сервер DHCP, раздающий адреса клиентам.

## 6 Настройка устройства через Web-интерфейс. Доступ администратора.

### Начало работы

Для конфигурирования устройства, необходимо подключиться к нему через Web-браузер:

1. Откройте Web-браузер (программу-просмотрщик web-страниц), например, Firefox, Google Chrome.
2. Введите в адресной строке браузера IP-адрес устройства

✔ Заводской IP-адрес устройства: *192.168.0.1* , маска подсети: *255.255.255.0*

При успешном подключении в окне браузера отобразится страница с запросом имени пользователя и пароля:

3. Введите имя пользователя в строке «User Name» и пароль в строке «Password».

✔ Имя пользователя *admin*, пароль *password*.

4. Нажмите кнопку «Login». В окне браузера откроется начальная страница web-интерфейса устройства.

### Смена пароля

Во избежание несанкционированного доступа при дальнейшей работе с устройством рекомендуется изменить пароль. Для смены пароля в меню *Admin*, раздел «Password», в поле «Old Password» введите текущий пароль, в полях «New Password» и «Confirm new password» введите новый пароль. Для сохранения изменений нажмите кнопку «Apply Changes».

## Элементы Web-интерфейса

Ниже представлен общий вид окна конфигурирования устройства.

The screenshot shows the web interface for the ELTEX NTU-MD500P device. The top header includes the ELTEX logo, the device model name 'NTU-MD500P', and a user management area with the number '3', the username 'admin', and a 'Logout' button. On the left side, there is a navigation menu labeled '1' with options: Status, LAN, WAN, Services, Advance, Diagnostics, Admin, and Statistics. The main content area, labeled '2', is titled 'Device Status' and contains the following information:

This page shows the current status and some basic settings of the device.

**System**

Board Type	NTU-MD500P
Serial Number	GP51000024
PON Serial	454C545882000003
Base WAN MAC	E4:5A:D4:ED:E2:1F
Hardware Version	1v1
Uptime	1:29
Date/Time	Thu Jan 1 01:29:39 1970
Image 1 Firmware Version (Active)	2.4.1.323
Image 2 Firmware Version	
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

**WAN Configuration**

Interface	VLAN ID	MAC	Connection Type	Protocol	IP Address	Subnet Mask	Gateway	NAPT	Firewall	IGMP Proxy	802.1p	Status

**L2TP Configuration**

Interface	Protocol	Local IP Address	Remote IP Address	Status

At the bottom of the main content area, there is a 'Refresh' button and a large number '2'.

Окно пользовательского интерфейса можно условно разделить на 3 части:

1. Дерево навигации по меню настроек устройства.
2. Основное окно настроек выбранного раздела.
3. Кнопка смены пользователя.

## 6.1 Меню «Status». Информация об устройстве

### 6.1.1 Подменю «Device status». Общая информация об устройстве

В разделе отображается общая информация об устройстве, основные параметры LAN- и WAN-интерфейсов.

*Status* → *Device status*

**Device Status**

This page shows the current status and some basic settings of the device.

---

**System**

Board Type	NTU-MD500P
Serial Number	GP51000024
PON Serial	454C545882000003
Base WAN MAC	E4:5A:D4:ED:E2:1F
Hardware Version	1v1
Uptime	1:32
Date/Time	Thu Jan 1 01:32:00 1970
Image 1 Firmware Version (Active)	2.4.1.323
Image 2 Firmware Version	
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

**WAN Configuration**

Interface	VLAN ID	MAC	Connection Type	Protocol	IP Address	Subnet Mask	Gateway	NAPT	Firewall	IGMP Proxy	802.1p	Status
nas_0	41	e4:5a:d4:ed:e2:20	Other	Bridged								down

**L2TP Configuration**

Interface	Protocol	Local IP Address	Remote IP Address	Status

### System

- *Board Type* – модель устройства;
- *Serial Number* – серийный номер устройства;
- *PON Serial* – серийный номер устройства в сети PON;
- *Base WAN MAC* – WAN MAC-адрес устройства;
- *Hardware Version* – версия аппаратного обеспечения;
- *Uptime* – время работы устройства;
- *Date/Time* – текущее время на устройстве;
- *Image 1 Firmware Version (Active)* – текущая версия ПО;
- *Image 2 Firmware Version* – версия резервного ПО;
- *CPU Usage* – процент использования CPU;
- *Memory Usage* – процент использования памяти;
- *Name Servers* – наименование сервера DNS;
- *IPv4 Default Gateway* – шлюз по умолчанию IPv4;
- *IPv6 Default Gateway* – шлюз по умолчанию IPv6.

**LAN Configuration**

- *IP Address* – IP-адрес устройства;
- *Subnet Mask* – маска сети устройства;
- *DHCP Server* – состояние DHCP-сервера;
- *MAC Address* – MAC-адрес устройства.

**WAN Configuration**

- *Interface* – название интерфейса;
- *VLAN ID* – VLAN ID интерфейса;
- *MAC* – MAC-адрес интерфейса;
- *Connection Type* – тип соединения;
- *Protocol* – используемый протокол;
- *IP Address* – IP-адрес интерфейса;
- *Subnet Mask* – маска подсети;
- *Gateway* – шлюз;
- *NAPT* – состояние NAPT;
- *Firewall* – состояние Firewall;
- *IGMP Proxy* – состояние IGMP Proxy;
- *802.1p* – метка 802.1p;
- *Status* – статус интерфейса.

**L2TP Configuration**

- *Interface* – название интерфейса;
- *Protocol* – используемый протокол;
- *Local IP Address* – IP-адрес интерфейса L2TP;
- *Remote IP Address* – IP-адрес сервера;
- *Status* – статус интерфейса.

Для обновления данных на странице нажмите кнопку «Refresh».

## 6.1.2 Подменю «IPv6 Status». Информация о системе IPv6

В разделе отображается текущий статус системы IPv6.

*Status* → *IPv6*

**IPv6 Status**

This page shows the current system status of IPv6.

LANConfiguration	
IPv6 Address	
IPv6 Link-Local Address	fe80::1/64

Prefix Delegation	
Prefix	

WANConfiguration					
Interface	VLAN ID	Connection Type	Protocol	IP Address	Status

**LAN Configuration**

- *IPv6 Address* – IPv6-адрес;
- *IPv6 Link-Local Address* – локальный IPv6-адрес.

**Prefix Delegation**

- *Prefix* – префикс IPv6-адреса.

**WAN Configuration**

- *Interface* – название интерфейса;
- *VLAN ID* – VLAN ID интерфейса;
- *Connection Type* – тип соединения;
- *Protocol* – используемый протокол;
- *IP Address* – IP-адрес интерфейса;
- *Status* – статус интерфейса.

Для обновления данных на странице нажмите кнопку «Refresh».

### 6.1.3 Подменю «PON». Информация о статусе оптического модуля

В разделе показано текущее состояние PON-интерфейса.

*Status* → *PON*

<b>PON Status</b>	
This page shows the current system status of PON.	
<hr/>	
<b>PON Status</b>	
<b>Temperature</b>	48.691406 C
<b>Voltage</b>	3.342300 V
<b>Tx Power</b>	1.228869 dBm
<b>Rx Power</b>	-15.951663 dBm
<b>Bias Current</b>	19.848000 mA
<b>GPON Status</b>	
<b>ONU State</b>	05
<b>ONU ID</b>	1
<b>LOID Status</b>	Initial Status
<input type="button" value="Refresh"/>	

**PON Status**

- *Temperature* – текущая температура;
- *Voltage* – напряжение;
- *Tx Power* – мощность сигнала на передаче;
- *Rx Power* – мощность сигнала на приеме;
- *Bias Current* – ток смещения.

**GPON Status**

- *ONU State* – статус авторизации на OLT (01 -> 02 -> 03 -> 04 -> 05);
- *ONU ID* – идентификатор устройства на OLT;
- *LOID Status* – статус авторизации на OLT (Initial -> Standby -> Serial Number -> Ranging -> Operation).

Для обновления данных на странице нажмите кнопку «Refresh».

#### 6.1.4 Подменю «LAN». Информация о статусе интерфейса LAN

В разделе доступен просмотр основных характеристик интерфейсов LAN.

*Status* → *LAN*

**LAN Port Status**

This page shows the current LAN Port status.

---

<b>LAN1</b>	Down
<b>LAN2</b>	Down
<b>LAN3</b>	Up; 1000M, Full Mode
<b>LAN4</b>	Down

Для обновления информации в таблице нажмите кнопку «Refresh».

#### 6.2 Меню «LAN». Настройка интерфейса LAN

В разделе доступна настройка основных характеристик проводных и беспроводных интерфейсов LAN.

*LAN*

**LAN Interface Settings**

This page is used to configure the LAN interface of your Device. Here you may change the setting for IP addresses, subnet mask, etc..

---

<b>InterfaceName:</b>	LANIPInterface
<b>IP Address:</b>	<input type="text" value="192.168.1.1"/>
<b>Subnet Mask:</b>	<input type="text" value="255.255.255.0"/>
<b>IPv6 Address:</b>	<input type="text" value="fe80::1"/>
<b>IPv6 DNS Mode:</b>	<input type="text" value="HGWProxy"/> ▼
<b>Prefix Mode:</b>	<input type="text" value="WANDelegated"/> ▼
<b>WAN Interface:</b>	▼
<b>Firewall:</b>	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
<b>IGMP Snooping:</b>	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
<b>Ethernet to Wireless Blocking:</b>	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled

- *InterfaceName* – название интерфейса;
- *IP Address* – IP-адрес интерфейса;
- *Subnet Mask* – маска подсети интерфейса;
- *IPv6 Address* – IPv6-адрес;
- *IPv6 DNS Mode* – настроить режим использования доменных имён:
  - *HGWProxy* – настроить режим DNS для IPv6;
  - *WANConnection* – использовать WAN-интерфейс для получения адреса DNS-сервера;
  - *Static* – указать статический адрес DNS-сервера (IPv6 DNS1, IPv6 DNS2).



- *Prefix Mode* – настроить режим получения Prefix (с WAN-интерфейса или статически):
  - *WANDelegated* – включается опция делегирования префиксов, полученных от провайдера;
  - *Static* – указать статический Prefix.
- *WAN Interface* – выбор WAN-интерфейса, который будет использоваться при WANDelegated.
- *Firewall (Enabled/Disabled)* – включение/выключение брандмауэра для интерфейса LAN;
- *IGMP Snooping (Enabled/Disabled)* – включение/выключение IGMP Snooping.

Для сохранения изменений нажмите кнопку «Apply Changes».

## 6.3 Меню «WAN». Настройка интерфейса WAN

### 6.3.1 Подменю «PON WAN»

В разделе можно настроить параметры PON WAN.

WAN → PON WAN

**PON WAN**

This page is used to configure the parameters for PONWAN

---

new link ▼

Enable VLAN:

VLAN ID:  802.1p\_Mark ▼

Channel Mode:  ▼

Interface Grouping:  ▼

Group Name:

Enable NAPT:

Admin Status:  Enable  Disable

Enable firewall:

Connection Type:  ▼

Default Route:  Disable  Enable

Enable IGMP-Proxy:

Apply Changes

- *Enable VLAN* – включение использования VLAN;
- *VLAN ID* – идентификационный номер VLAN;
- *802.1p\_Mark* – приоритет 802.1p;
- *Channel Mode* – режим работы интерфейса VLAN;
  - *Bridged* – мост;
  - *IPoE* – получение адреса по протоколу DHCP;
  - *PPPoE* – установка point-to-point туннеля через Ethernet.
- *Interface Grouping* – выбор группы интерфейсов;
- *Group name* – имя группы интерфейсов;
- *Enable NAPT* – включение функции NAPT;
- *Admin Status (Enable/Disable)* – включение/выключение административного статуса;
- *Enable Firewall* – включение брандмауэра;
- *Connection Type* – тип сервиса, предоставляемого на данном WAN;
- *Default Route (Enable/Disable)* – включение/выключение использования выбранного интерфейса как шлюза по умолчанию;
- *Enable IGMP-Proxy* – включение перехвата и пересылки сообщений IGMP.

Для сохранения изменений нажмите кнопку «Apply Changes», для удаления – «Delete».

## 6.3.2 Подменю «VPN»

### 6.3.2.1 Подменю «L2TP». Настройка L2TP VPN

В разделе можно настроить параметры виртуального соединения L2TP VPN. Протокол L2TP используется для создания защищенного канала связи через Internet между компьютером удаленного пользователя и локальным компьютером.

WAN → VPN → L2TP

**L2TP VPN Configuration**  
This page is used to configure the parameters for L2TP mode VPN.

L2TP VPN:  Disable  Enable

Server:

Tunnel Authentication:

Tunnel Authentication Secret:

PPP Authentication:

PPP Encryption:

UserName:

Password:

PPP Connection Type:

Idle Time (min):

MTU:

Default Gateway:

**L2TP Table:**

Select	Interface	Server	Tunnel Authentication	PPP Authentication	MTU	Default Gateway	Action
<input type="button" value="Delete Selected"/>							

- *L2TP VPN* – режим, при котором выход в Интернет осуществляется через специальный канал, туннель с использованием протокола L2TP. При включении «Enable» для редактирования станут доступны следующие параметры:
- *Server* – адрес сервера L2TP (доменное имя или IP-адрес в формате IPv4);
- *Tunnel Authentication* – включение аутентификации;
- *Tunnel Authentication Secret* – ключ аутентификации;
- *PPP Authentication* – выбор протокола проверки подлинности соединений, используемый на L2TP-сервере;
- *PPP Encryption* – выбор протокола шифрования данных, который будет использоваться (только для метода CHAPMSv2);
- *UserName* – имя пользователя для авторизации на L2TP-сервере;
- *Password* – пароль для авторизации на L2TP-сервере;
- *PPP Connection Type* – тип соединения;
- *Idle Time (min)* – время простоя в секундах, разрывает неактивное соединение через указанное время (только для установления соединения по требованию (dial-on-demand));
- *MTU* – максимальный размер блока данных, передаваемых по сети (рекомендуемое значение – 1462);
- *Default Gateway* – выбор того, будет ли созданный туннель L2TP-шлюзом по умолчанию.

Для сохранения изменений нажмите кнопку «Apply Changes».

В таблице «L2TP Table» осуществляется просмотр состояния виртуального соединения L2TP VPN. Для удаления определённой записи, выделите позицию и нажмите кнопку «Delete Selected».

### 6.3.2.2 Подменю «IPsec». Настройка IP Security

Эта страница используется для настройки параметров для VPN в режиме IPsec.

WAN → IPsec

#### IPsec VPN Configuration

This page is used to configure the parameters for IPsec mode VPN.

---

Negotiation Type  Automatic  Manual

**Auto Configure:**

Mode

---

**Remote:**

Tunnel Addr.

---

**Local:**

Tunnel Addr.

---

**Security Option:**

Encapsulation Type

IKE Auth Method

Pre shared key

Advanced Option

**Filter Option:**

Protocol

Port

**IKE Phase 1:**

Negotiation Mode

Keepalive Time  seconds

IKE Algorithm 1

IKE Algorithm 2

IKE Algorithm 3

IKE Algorithm 4

**IKE Phase 2:**

pfs\_group mode

Encrypt Algorithm  null\_enc  des  3des  aes

Auth Algorithm  non\_auth  md5  sha1

Keepalive Time  seconds

Keepalive Byte  KB

**IPsec Information List:**

Enable	State	Type	RemoteGW	RemoteIP	Interface	LocalIP	EncapMode	FilterProtocol	FilterPort
<input type="button" value="Delete Selected"/> <input type="button" value="Enable"/> <input type="button" value="Disable"/>									

**Certificate Management:**

cert.pem  Файл не выбран

privKey.pem  Файл не выбран

- *Negotiation Type* – выбор типа согласования;
- *Negotiation Type* – Automatic:
  - *Mode* – режим работы IPsec (поддержка только транспортного режима);
  - *Remote Tunnel Addr.* – IP-адрес сервера;
  - *Local Tunnel Addr.* – локальный IP-адрес;
  - *Security Option:*
    - *Encapsulation Type* – тип инкапсуляции;

- *IKE Auth Method* – метод аутентификации IKE;
- *Pre shared key* – общий ключ;
- *Advanced Option* – включение расширенного варианта настройки.
- *Filter Option*:
  - *Protocol* – протокол;
  - *Port* – порт.
- *IKE Phase 1* – настройка первой фазы:
  - *Negotiation Mode* – режим согласования;
  - *Keepalive Time* – время активности сессии, секунды;
  - *IKE Algorithm 1-4* – выбор алгоритмов обмена ключами.
- *IKE Phase 2* – настройка второй фазы:
  - *pfs\_group mode* – выбор PFS(DH) группы;
  - *Encrypt Algorithm* – алгоритм шифрования;
  - *Auth Algorithm* – алгоритм аутентификации;
  - *Keepalive Time* – время активности сессии, секунды;
  - *Keepalive Byte* – байт поддержки активности, Кбайт.
- *Negotiation Type* – Manual:
  - *Mode* – режим работы IPSec (поддержка только транспортного режима);
  - *Remote Tunnel Addr.* – IP-адрес сервера;
  - *Local Tunnel Addr.* – локальный IP-адрес;
  - *Security Option*:
    - *Encapsulation Type* – тип инкапсуляции;
    - *Encapsulation Type* – ESP:
      - *ESP Encrypt Algorithm* – алгоритм шифрования ESP;
      - *ESP Encrypt Key* – ключ шифрования ESP;
      - *ESP Auth Algorithm* – алгоритм аутентификации ESP;
      - *ESP Auth Key* – ключ аутентификации ESP.
    - *Encapsulation Type* – AH:
      - *AH Auth Algorithm* – алгоритм аутентификации AH;
      - *AH Auth* – ключ аутентификации AH.
    - *Encapsulation Type* – ESP+AH:
      - *ESP Encrypt Algorithm* – алгоритм шифрования ESP;
      - *ESP Encrypt Key* – ключ шифрования ESP;
      - *ESP Auth Algorithm* – алгоритм аутентификации ESP;
      - *ESP Auth Key* – ключ аутентификации ESP;
      - *AH Auth Algorithm* – алгоритм аутентификации AH;
      - *AH Auth* – ключ аутентификации AH.
  - *Advanced Option* – включение расширенного варианта настройки;
  - *Filter Option*:
    - *Protocol* – протокол;
    - *Port* – порт.
- *Certificate Management* – выбор и загрузка сертификата управления. Нажмите кнопку «Выберите файл» для выбора сертификата и кнопку «Upload» для его загрузки.

Для сохранения изменений нажмите кнопку «Add/Save».

В таблице «*IPsec Information List*» осуществляется просмотр, активация («Enable»), деактивация («Disable») и удаление созданных правил («Delete Selected»).

## 6.4 Меню «Services». Настройка сервисов

### 6.4.1 Подменю «DHCP Setting». Настройка DHCP

В разделе происходит настройка DHCP-сервера или DHCP-ретранслятора.

#### Services → DHCP (Server)

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

**DHCP Mode:**  NONE  DHCP Relay  DHCP Server

---

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

---

**LAN IP Address:** 192.168.1.1    **Subnet Mask:** 255.255.255.0

**IP Pool Range:**  -

**Subnet Mask:**

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

**DomainName:**

**Gateway Address:**

**DNS option:**  Use DNS Relay  Set Manually

- *DHCP Mode* – выбор режима работы:
  - *NONE* – DHCP отключен;
  - *DHCP Server* – работа в режиме DHCP-сервера;
  - *DHCP Relay* – работа в режиме DHCP-ретранслятора.
- *IP Pool Range* – диапазон адресов, выдаваемых клиентам;
- *Show Client* – кнопка для просмотра клиентов, арендовавших адреса. По нажатию выводится таблица с информацией о клиентах DHCP, арендуемых DHCP-сервер;
- *Subnet Mask* – маска подсети;
- *Max Lease Time* – максимальное время аренды, -1 для бесконечной аренды;
- *DomainName* – наименование домена;
- *Gateway Address* – адрес шлюза;
- *DNS option* – определяет работу DNS:
  - *Use DNS relay* – в качестве DNS будет выдан адрес ONT и все запросы будут ретранслироваться через ONT;
  - *Set manually* – установить DNS вручную.

#### Services → DHCP (Relay)

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

**DHCP Mode:**  NONE  DHCP Relay  DHCP Server

---

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

---

**DHCP Server IP Address:**

- *DHCP Server IP Address* – IP-адрес удалённого сервера DHCP.

Для сохранения изменений нажмите кнопку «Apply Changes». Кнопки «Port-Based Filter» и «MAC-Based Assignment» позволяют настроить фильтрацию по портам и MAC, соответственно.

## 6.4.2 Подменю «DNS»

### 6.4.2.1 Подменю «Dynamic DNS». Настройки динамической системы доменных имен

Динамическая DNS (динамическая система доменных имен) позволяет информации на DNS-сервере обновляться в реальном времени и (по желанию) в автоматическом режиме. Применяется для назначения постоянного доменного имени устройству (компьютеру, маршрутизатору, например NTU-RG) с динамическим IP-адресом. Это может быть IP-адрес, полученный по IPCP в PPP-соединениях или по DHCP.

Динамическая DNS часто применяется в локальных сетях, где клиенты получают IP-адрес по DHCP, а потом регистрируют свои имена в локальном DNS-сервере.

Services → DNS → Dynamic DNS

**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.

---

**Enable:**

**DDNS Provider:** DynDNS.org ▼

**Hostname:**

**Interface:** ▼

**DynDns/No-IP Settings:**

---

**UserName:**

**Password:**

**TZO Settings:**

**Dynamic DNS Table:**

Select	State	Hostname	UserName	Service	Status
--------	-------	----------	----------	---------	--------

- *Enable* – при установленном флаге использовать DHCP-сервер (сетевые устройства будут получать IP-адреса динамически, из нижеприведенного диапазона);
- *D-DNS Provider* – выбор типа службы D-DNS (провайдера): DynDNS.org, No-IP.com;
- *Custom* – иной провайдер, выбранный пользователем. В данном случае необходимо самостоятельно указать имя (*Hostname*) и адрес (*Interface*) провайдера.

#### DynDns/No-IP Settings:

- *UserName* – имя пользователя;
- *Password* – пароль авторизации на сервисе, выбранном для работы с D-DNS.

В разделе отображается таблица «Dynamic DNS Table» со списком имеющихся DNS и его параметрами. Для добавления записи нажмите кнопку «Add». Чтобы изменить/удалить позицию, выберите её и нажмите «Modify»/«Remove» напротив выбранной записи.

### 6.4.3 Подменю «Firewall». Настройка брандмауэра

#### 6.4.3.1 Подменю «ALG On-Off Configuration». Включение/отключение сервисов ALG.

В разделе можно включить или отключить сервисы ALG.

Services → Firewall → ALG

**NAT ALG and Pass Through Configuration**

This page is used to enable/disable ALG and Pass Through services.

---

ALG Type:

FTP  Enable  Disable

TFTP  Enable  Disable

H323  Enable  Disable

L2TP  Enable  Disable

IPSec  Enable  Disable

SIP  Enable  Disable

PPTP  Enable  Disable

#### 6.4.3.2 Подменю «IP/Port Filtering». Настройки фильтрации адресов

В разделе осуществляется настройка фильтрации адресов. Функция IP-фильтрация позволяет фильтровать проходящий через маршрутизатор трафик по IP-адресам и портам. Использование таких фильтров может быть полезно для защиты или ограничения локальной сети.

Services → Firewall → IP/Port Filtering

**IP/Port Filtering**

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

---

**Outgoing Default Action**  Deny  Allow

**Incoming Default Action**  Deny  Allow

---

Direction:  Protocol:  Rule Action  Deny  Allow

Source IP Address:  Subnet Mask:  Port:  -

Destination IP Address:  Subnet Mask:  Port:  -

WAN Interface:

---

**Current Filter Table:**

Select	Direction	Protocol	Source IP Address	Source Port	Destination IP Address	Destination Port	WAN Interface	Rule Action
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>								

#### Настройки по умолчанию

- *Outgoing Default Action Deny/Allow* – фильтрация для исходящих пакетов;
- *Incoming Default Action Deny/Allow* – фильтрация для входящих извне пакетов.

Для сохранения изменений нажмите кнопку «Apply Changes».

Для добавления фильтра заполните соответствующие поля и нажмите кнопку «Add»:

- *Direction Outgoing/Incoming* – направление передачи пакетов (исходящие/входящие);
- *Protocol* – протокол фильтрации;
- *Rule Action Deny/Allow* – политика обработки пакета (отбросить/пропустить);
- *Source IP Address* – IP-адрес источника;
  - *Subnet mask* – маска подсети;
  - *Port* – порт.
- *Destination IP Address* – IP-адрес назначения;
  - *Subnet mask* – маска подсети;
  - *Port* – порт.
- *WAN Interface* – входящий интерфейс.

Добавленные фильтры отображаются в нижерасположенной таблице фильтров «*Current Filter Table*». Записи в этой таблице используются для ограничения определенных типов пакетов данных через шлюз. Для удаления определённого фильтра, выделите позицию и нажмите кнопку «Delete selected», для удаления всех фильтров – кнопку «Delete All».

#### 6.4.3.3 Подменю «MAC Filtering». Настройки фильтрации по MAC-адресам

В разделе производится фильтрация на основе MAC-адресов, которая позволяет пересылать или блокировать трафик с учетом MAC-адреса источника и получателя. Для смены режима нажмите кнопку «Apply Changes».

#### Services → Firewall → MAC Filtering

**MAC Filtering for bridge mode**

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

---

**Outgoing Default Action**  Deny  Allow

**Incoming Default Action**  Deny  Allow Apply Changes

---

**Direction:** Outgoing ▼

**Source MAC Address:**

**Destination MAC Address:**

**Rule Action**  Deny  Allow

Add

---

**Current Filter Table:**

Select	Direction	Source MAC Address	Destination MAC Address	Interface	Rule Action

Delete Selected Delete All

- *Outgoing Default Action Deny/Allow* – фильтрация для исходящих пакетов;
- *Incoming Default Action Deny/Allow* – фильтрация для входящих извне пакетов.

Для сохранения изменений нажмите кнопку «Apply Changes».

Для добавления фильтра заполните соответствующие поля и нажмите кнопку «Add»:

- *Direction Outgoing/Incoming* – направление передачи пакетов (исходящие/входящие);
- *Source MAC Address* – поле для добавления исходного MAC-адреса, для которого вводится ограничение/доступ.
- *Destination MAC Address* – поле для добавления получаемого MAC-адреса, для которого вводится ограничение/доступ.
- *Rule Action Deny/Allow* – политика обработки пакета (отбросить/пропустить);
- *WAN Interface* – входящий интерфейс.



Добавленные фильтры отображаются в ниже расположенной таблице фильтров «*Current Filter Table*». Поле «*Rule*» отображает тип созданного правила («*Allow*», разрешающее или «*Deny*», запрещающее). Для удаления определённой позиции в списке, выделите её и нажмите «*Delete Selected*», чтобы удалить весь список, нажмите «*Delete All*».

#### 6.4.3.4 Подменю «*Port Forwarding*». Настройка проброса портов

В данном разделе отображается таблица «*Current Port Forwarding Table*» с информацией о пробросе портов. Записи в этой таблице позволяют автоматически перенаправлять общие сетевые службы на конкретный компьютер за брандмауэром NAT. Эти настройки необходимы только в том случае, если вы хотите разместить какой-либо хост, например веб-сервер или почтовый сервер, в частной локальной сети за брандмауэром NAT используемого маршрутизатора. Для сохранения изменений нажмите кнопку «*Apply Changes*».

#### Services → Firewall → Port Forwarding

**Port Forwarding**

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Port Forwarding:  Disable  Enable

Enable  Application: Active Worlds

Comment	Local IP	Local Port from	Local Port to	Protocol	Remote Port from	Remote Port to	Interface	NAT loopback
				Both ▾			Any ▾	<input type="checkbox"/>
				Both ▾			Any ▾	<input type="checkbox"/>
				Both ▾			Any ▾	<input type="checkbox"/>
				Both ▾			Any ▾	<input type="checkbox"/>
				Both ▾			Any ▾	<input type="checkbox"/>
				Both ▾			Any ▾	<input type="checkbox"/>
				Both ▾			Any ▾	<input type="checkbox"/>
				Both ▾			Any ▾	<input type="checkbox"/>
				Both ▾			Any ▾	<input type="checkbox"/>
				Both ▾			Any ▾	<input type="checkbox"/>
				Both ▾			Any ▾	<input type="checkbox"/>
				Both ▾			Any ▾	<input type="checkbox"/>
				Both ▾			Any ▾	<input type="checkbox"/>
				Both ▾			Any ▾	<input type="checkbox"/>
				Both ▾			Any ▾	<input type="checkbox"/>
				Both ▾			Any ▾	<input type="checkbox"/>
				Both ▾			Any ▾	<input type="checkbox"/>
				Both ▾			Any ▾	<input type="checkbox"/>
				Both ▾			Any ▾	<input type="checkbox"/>
				Both ▾			Any ▾	<input type="checkbox"/>

**Current Port Forwarding Table:**

Select	Comment	Local	IP Address	Protocol	Local Port	Enable	Remote Host	Public Port	Interface	NAT loopback
<input type="checkbox"/>										

Для добавления записи в таблицу «*Current Port Forwarding Table*» установите флаг *Enable* и заполните соответствующие поля:

- *Port Forwarding (Enable/Disable)* – включение/выключение функции проброса портов;
- *Application* – в меню имеются предустановки для проброса портов различных приложений;
- *Comment* – комментарий;
- *Local IP* – локальный IP-адрес, на который производится проброс;
- *Local port from/to* – укажите диапазон портов локального устройства для проброса;
- *Protocol* – выбор протокола (TCP, UDP или оба);
- *Remote port from/to* – укажите начальный порт входящего соединения. Поле «*Remote port to*» заполнится автоматически;
- *Interface* – выбор интерфейса;
- *NAT-loopback* – петля NAT позволяет "заворачивать" запросы из локальной сети на маршрутизатор, таким образом, например, можно проверить работу созданных правил.

После заполнения полей для добавления записи нажмите кнопку «Add». Для удаления определённой позиции выделите её и нажмите кнопку «Delete Selected», для удаления всей таблицы – кнопку «Delete All».

#### 6.4.3.5 Подменю «URL Blocking». Настройки ограничения доступа в интернет

Фильтр URL осуществляет полноценный анализ и контроль доступа к определённым ресурсам сети интернет. В данном разделе задается и отображается список запрещенных/разрешенных URL-адресов для посещения. Здесь вы можете добавить запрещенное/разрешенное FQDN (Fully Qualified Domain Name) кнопкой «Add», также возможна фильтрация по ключевым словам. Добавленные ограничения отображаются в таблицах «URL Blocking Table» и «Keyword Filtering Table», для удаления определённого URL-адреса или ключевого слова из таблицы нажмите на него, а затем на кнопку «Delete Selected». Для удаления всех ограничений нажмите «Delete All».

Services → Firewall → URL Blocking

- *URL Blocking (Enable/Disable)* – включение/выключение работы URL-Blocking;
- *FQDN (Fully Qualified Domain Name)* – полное доменное имя;
- *Keyword* – ключевое слово.

Для сохранения изменений нажмите кнопку «Apply Changes».

#### 6.4.3.6 Подменю «Domain Blocking». Настройка блокировки доменов

Этот раздел используется для задания блокировки доменов.

Services → Firewall → Domain blocking

Чтобы заблокировать домен, поставьте флаг «Enable», заполните поле «Domain» и нажмите кнопку «Add».

- *Domain Blocking (Enable/Disable)* – включение/выключение блокировки;
- *Domain* – наименование домена.

Для сохранения изменений используйте кнопку «Apply Changes». Все заблокированные домены приведены в таблице «*Domain Blocking Configuration*», чтобы удалить блокировку для одного домена, выделите его и нажмите кнопку «Delete Selected», для удаления всех ограничений нажмите кнопку «Delete All».

#### 6.4.3.7 Подменю «DMZ». Настройки демилитаризованной зоны

При установке IP-адреса в поле «DMZ Host IP Address» все запросы из внешней сети, не попадающие под правила *Port Forwarding*, будут направляться на DMZ-хост (доверительный хост с указанным адресом, расположенный в локальной сети).

Services → Firewall → DMZ

**DMZ Configuration**

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

---

**DMZ Host:**  Disable  Enable

**DMZ Host IP Address:**

- *DMZ Host (Enable/Disable)* – включение/выключение хоста;
- *DMZ Host IP Address* – IP-адрес.

Для сохранения изменений нажмите кнопку «Apply Changes».

#### 6.4.4 Подменю «UPnP». Автоматическая настройка сетевых устройств

В разделе производится настройка функции Universal Plug and Play (UPnP™). UPnP обеспечивает совместимость с сетевым оборудованием, программным обеспечением и периферийными устройствами.

Services → UPnP

**UPnP Configuration**

This page is used to configure UPnP. The system acts as a daemon when you enable it and select WAN interface (upstream) that will use UPnP.

---

**UPnP:**  Disable  Enable

✔ Для использования UPnP необходимо настроить NAT на активном WAN-интерфейсе.

- *UPnP (Enable/Disable)* – включение/выключение функции UPnP;
- *WAN Interface* – WAN-интерфейс, на котором будет работать функция UPnP.

Для сохранения настроек нажмите кнопку «Apply Changes».

### 6.4.5 Подменю «RIP». Настройка динамической маршрутизации

В разделе осуществляется выбор интерфейсов на устройствах, которые используют RIP и версию используемого протокола. Включите RIP, если вы используете это устройство в качестве устройства с поддержкой RIP для связи с другими пользователями с использованием протокола динамической маршрутизации RIP.

Services → RIP

**RIP Configuration**

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

---

**RIP:**  Disable  Enable

**Interface:**

**Receive Mode:**

**Send Mode:**

---

**RIP Config Table:**

Select	Interface	Receive Mode	Send Mode
<input type="checkbox"/>			

- *RIP (Enable/Disable)* – включение/выключение использования протокола динамической маршрутизации RIP;

Для принятия и сохранения настроек необходимо нажать кнопку «Apply Changes».

- *Interface* – интерфейс, на котором будет запускаться RIP;
- *Receive Mode* – режим обработки входящих пакетов (NONE, RIP1, RIP2, both);
- *Send Mode* – режим отправки (NONE, RIP1, RIP2, RIP1 COMPAT).

Интерфейсы с поддержкой RIP отображаются в таблице «RIP Config Table». Для удаления всех записей в таблице нажмите кнопку «Delete All», чтобы удалить одну позицию из списка, выделите её и нажмите кнопку «Delete Selected».

## 6.5 Меню «Advance». Расширенные настройки

### 6.5.1 Подменю «ARP Table». Просмотр кэша протокола ARP

В разделе отображается таблица изученных MAC-адресов. Эффективность функционирования ARP во многом зависит от ARP-кэша, который присутствует на каждом хосте. В кэше содержатся Internet-адреса и соответствующие им аппаратные адреса. Время жизни каждой записи в кэше – 5 минут с момента создания записи.

Advance → ARP table

**User List**

This table shows a list of learned MAC addresses.

---

IP Address	MAC Address
192.168.1.15	ec-08-6b-05-c5-33

- *IP Address* – IP-адрес клиента;
- *MAC Address* – MAC-адрес клиента.

Для обновления информации в таблице нажмите кнопку «Refresh».

### 6.5.2 Подменю «Bridging». Настройка параметров Bridging

В разделе осуществляется настройка параметров моста. Здесь можно настроить время жизни адресов в MAC-таблице, а также включить/выключить протокол 802.1d Spanning Tree.

*Advance* → *Bridging*

**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.

---

**Ageing Time:**  (seconds)

**802.1d Spanning Tree:**  Disabled  Enabled

- *Ageing Time* – время жизни адресов (сек);
- *802.1d Spanning Tree (Enable/Disable)* – включение/выключение протокола 802.1d Spanning Tree.

Для сохранения изменений нажмите кнопку «Apply Changes».

Для просмотра информации о мосте и его подключенных портах, нажмите кнопку «Show MACs».

*Advance* → *Bridging* → *Show MACs*

**Bridge Forwarding Database**

This table shows a list of learned MAC addresses.

Port	MAC Address	Is Local?	Ageing Timer
2	ec-08-6b-05-c5-33	no	0.01
7	e0-d9-e3-9d-f7-b6	yes	---

- *Port* – номер порта;
- *MAC Address* – MAC-адрес;
- *Is Local* – локальный адрес;
- *Ageing Timer* – время жизни адреса.

Для обновления информации в таблице нажмите кнопку «Refresh», для закрытия – кнопку «Close».

### 6.5.3 Подменю «Routing». Настройка маршрутизации

В разделе осуществляется настройка статической маршрутизации.

*Advance* → *Routing*

**RoutingConfiguration**

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

---

**Enable:**

**Destination:**

**Subnet Mask:**

**Next Hop:**

**Metric:**

**Interface:** Any ▾

---

**Static Route Table:**

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

Для добавления статического маршрута поставьте флаг «Enable», заполните соответствующие поля и нажмите на кнопку «Add Route».

- *Enable* – флаг для добавления маршрута;
- *Destination* – адрес назначения;
- *Subnet Mask* – маска подсети;
- *Next Hop* – следующий узел;
- *Metric* – метрика;
- *Interface* – интерфейс.

Добавленные статические маршруты отображаются в таблице «*Static Route Table*». Для обновления информации в таблице нажмите кнопку «Update», для удаления позиции из таблицы выделите её и нажмите кнопку «Delete Selected».

Для просмотра маршрутов, к которым часто обращается устройство, нажмите кнопку «Show Routes», после выведется таблица «*IP Route Table*».

*Advance* → *Routing* → *Show Routes*

**IP Route Table**

This table shows a list of destination routes commonly accessed by your network.

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

Для обновления информации в таблице нажмите кнопку «Refresh», для закрытия – кнопку «Close».

### 6.5.4 Подменю «Interface grouping». Объединение интерфейсов в группы

В разделе можно объединять интерфейсы в разные группы. По умолчанию все интерфейсы находятся в одной группе. Для переноса интерфейса в новую группу необходимо:

1. Выбрать новую группу из списка ниже;
2. Выбрать интерфейсы в списке доступных интерфейсов (*Available Interface*);
3. Нажать стрелку ← для переноса интерфейсов в группу;
4. Применить действия, нажав кнопку «Apply Changes».

## Advance → Interface grouping

### Interface Grouping Configuration

Select:  ▼

Enable:

Name:

Grouped Interfaces	Available Interfaces
nas0_0	LAN1 LAN2 LAN3 LAN4 LANIPInterface

Apply Changes

Name	Status	Interfaces	Action
default	Enable	LAN1,LAN2,LAN3,LAN4,LANIPInterface	
Group_1	Enable	nas0_0	

## 6.5.5 Подменю «IP QoS». Настройка качества предоставляемых услуг (QoS)

## 6.5.5.1 Подменю «QoS Policy». Настройка QoS-очередей

В разделе можно настроить политики QoS-очереди обработки трафика.

## Advance → IP QoS → QoS Policy

### IP QoS Configuration

IP QoS  Disable  Enable

#### QoS Queue Config

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 configuration, please click 'Apply Changes'

Policy:  PRIO  WRR

Queue	Policy	Priority	Weight	Enable
Q1	PRIO	1	--	<input type="checkbox"/>
Q2	PRIO	2	--	<input type="checkbox"/>
Q3	PRIO	3	--	<input type="checkbox"/>
Q4	PRIO	4	--	<input type="checkbox"/>

#### QoS Bandwidth Config

This part is used to configure the bandwidth of different type of WAN. If select Disable, CPE will select the appropriate bandwidth based on WAN. If select Enable, User is allowed to configure specific bandwidth of WAN.

User Defined Bandwidth:  Disable  Enable

Total Bandwidth Limit:  Kb

Apply Changes

- *IP QoS (Enable/Disable)* – включение/выключение конфигурирования QoS-очереди;
- *Policy* – выбор политики:
  - *PRIO* – при выборе политики PRIO используется строгая обработка очередей. Меньшей очереди соответствует наивысший приоритет;
  - *WRR* – при выборе политики WRR будет использоваться взвешенная обработка очередей. По умолчанию вес для очередей распределён как 40:30:20:10.

### QoS Bandwidth Config

Используется для настройки полосы пропускания отдельных сервисов.

- *User defined Bandwidth (Enable/Disable)* – включить ограничение;
- *Total Bandwidth Limit, (kb)* – ограничение полосы, кбит.

Для сохранения изменений нажмите кнопку «Apply Changes».

#### 6.5.5.2 Подменю «QoS Classification». Настройка правил классификации трафика

На данной странице можно указать по каким полям и их значениям будет классифицироваться пакет, а также в какую аппаратную очередь он в итоге попадет.

*Advance* → *IP QoS* → *QoS Classification*

**QoS Classification**

This page is used to add or delete classification rule. (After add a new rule, please click 'Apply Changes' to take effect.)

		Mark		Classification Rules					
ID	Name	Order	DSCP Mark	802.1p	Queue	WanIf	Rule Detail	Delete	Edit

Для добавления правила нажмите кнопку «Add» и заполните соответствующие поля.

*Advance* → *IP QoS* → *QoS Classification* → *Add*

**Add QoS Classification Rules**

This page is used to add a IP QoS classification rule.

---

RuleName:

RuleOrder:

**Assign IP Precedence/DSCP/802.1p**

Precedence:

DSCP:

802.1p:

**Specify Traffic Classification Rules**

IP QoS Rule by type:  Port  Ethery Type  IP/Protocol  MAC Address

---

- *RuleName* – имя правила;
- *RuleOrder* – порядковый номер.

**Assing IP Precedence/DSCP/802.1p** – настройка назначения полей IP.

- *Precedence* – выбор очереди;
- *DSCP* – приоритет в заголовке IP-пакета;
- *802.1p* – метка приоритета в 802.1Q.



**Specify Traffic Classification Rules** – выбор правила классификации трафика.

- *IP QoS Rule by type* – выбор правила классификации по типу:
  - *Port* – по порту;
    - *Physiact Port* – выбор физического порта.
  - *Ethery Type* – по Ether type;
  - *IP/Protocol* – по протоколу IP;
    - *IPv4*:
      - *Protocol* – выбор протокола;
      - *Source IP* – IP-адрес источника;
      - *Source Mask* – маска источника;
      - *Destination IP* – IP-адрес назначения;
      - *Destination Mask* – маска назначения;
      - *Source Port* – порт источника;
      - *Destination Port* – порт назначения.
    - *IPv6*:
      - *Protocol* – выбор протокола;
      - *Source IP* – IP-адрес источника;
      - *Source Prefix Length* – длина префикса источника;
      - *Destination IP* – IP-адрес назначения;
      - *Destination Prefix Length* – длина префикса назначения;
      - *Source Port* – порт источника;
      - *Destination Port* – порт назначения.
  - *MAC Address* – по MAC-адресу.
    - *Source MAC* – MAC-адрес источника;
    - *Destination MAC* – MAC-адрес назначения.

Для сохранения изменений нажмите кнопку «Apply Changes».

### 6.5.5.3 Подменю «Traffic Shaping». Настройка трафика

В данном разделе можно указать ограничения трафика по определенным правилам.

*Advance* → *IP QoS* → *Traffic Shaping*

**IP QoS Traffic Shaping**

---

**Total Bandwidth Limit:**  kb

ID	Protocol	Source Port	Destination Port	Source IP	Destination IP	Rate(kb/s)	Delete	IP Version	Direction
<div style="display: flex; justify-content: space-between; padding: 5px;"> <span>Add</span> <span>Apply Changes</span> <span>Apply Total Bandwidth Limit</span> </div>									

- *Total Bandwidth Limit (kb)* – общее ограничение полосы, кбит.

Для добавления нажмите кнопку «Add» и заполните соответствующие поля.  
*Advance* → *IP QoS* → *Traffic Shaping* → *Add*

**Add IP QoS Traffic Shaping Rule**

IP Version:  IPv4 ▼

Direction:  Upstream ▼

Protocol:  NONE ▼

Source IP:

Source Mask:

Destination IP:

Destination Mask:

Source Port:

Destination Port:

Rate Limit:  kb/s

- *IP Version* – выбор IP-версии;
- *Direction* – выбор типа потока, нисходящий или восходящий;
- *Protocol* – протокол;
- *Source IP* – IP-адрес источника;
- *Source Mask/Prefix Length* – маска/длина префикса подсети источника;
- *Destination IP* – IP-адрес назначения;
- *Destination Mask/Prefix Length* – маска/длина префикса подсети назначения;
- *Source Port* – порт источника;
- *Destination Port* – порт назначения;
- *Rate Limit (kb/s)* – ограничение по скорости, кбит/с.

Для сохранения изменений нажмите кнопку «Apply Changes», для отмены нажмите кнопку «Close».

#### 6.5.6 Подменю «PoE Settings». Конфигурирование PoE-портов

Эта страница используется для настройки параметров PoE. Здесь вы можете включить/отключить PoE на портах LAN, для этого необходимо установить флаг «Enable»/«Disable».

*Advance* → *PoE Settings*

**PoE Settings**

This page is used to configure PoE settings. Here you can enable/disable PoE on LAN ports.

**PoE**  Disable  Enable

**LAN1:**  **LAN2:**  **LAN3:**  **LAN4:**

Port	PoE enabled	Power	Voltage	Temperature	Detection Status	Power Classification	Error Type
1	Enabled	1.7 W	48 V	22 C	Delivering Power	Class 3	
2	Enabled	0.0 W	0 V	21 C	Searching		
3	Disabled						
4	Disabled						

- *Port* – номер LAN порта (1-4);
- *PoE enabled:*
  - *Enabled* – включена поддержка PoE на порту;

- *Disabled* – отключена поддержка PoE на порту.
- *Power* – потребляемая мощность, Вт;
- *Voltage* – напряжение, В;
- *Temperature* – температура, С;
- *Detection Status* – статус PoE-порта;
- *Power Classification* – класс мощности подключенного устройства PoE;
- *Error Type* – тип ошибки.

Для сохранения изменений нажмите кнопку «Apply Changes».

### 6.5.7 Подменю «Link mode». Настройка LAN-портов

В разделе можно задать режим работы LAN-портов. LAN1/2/3/4 – настройка режима работы, доступны режимы *10M Half Mode*, *10M Full Mode*, *100M Half Mode*, *100M Full Mode* и *Auto Mode* (режим автоопределения).

Advance → Link mode

**Ethernet Link Speed/Duplex Mode**

Set the Ethernet link speed/duplex mode.

---

LAN1: Auto Mode ▼

LAN2: Auto Mode ▼

LAN3: Auto Mode ▼

LAN4: Auto Mode ▼

Apply Changes

Для сохранения изменений нажмите кнопку «Apply Changes».

### 6.5.8 Подменю «Others». Дополнительные настройки

В разделе можно настроить сквозное прохождение IP для WAN-интерфейсов, а также включить/отключить прохождение JumboFrame.

**Other Advanced Configuration**

Here you can set some other advanced settings.

---

**IP PassThrough:** NONE ▼ Lease Time: 600 seconds

Allow LAN access

**JumboFrame:**  Disable  Enable

Apply Changes

Для сохранения изменений нажмите кнопку «Apply Changes».

### 6.5.9 Подменю «IPv6». Настройка протокола IPv6

В разделе можно включить/отключить работу IPv6-протокола, для этого необходимо установить флаг «Enable»/«Disable».

*Advance → IPv6*

Для сохранения изменений нажмите кнопку «Apply Changes».

#### 6.5.9.1 Подменю «RADVD». Настройка RADVD

В разделе осуществляется настройка RADVD (Router Advertisement Daemon).

*Advance → IPv6 → RADVD*

- *MaxRtrAdvInterval* – максимальный интервал отправки RA (Router Advertisement);
- *MinRtrAdvInterval* – минимальный интервал отправки RA;
- *AdvManagedFlag* – включение/выключение отправки флага Managed в RA;
- *AdvOtherFlag* – включение/выключение отправки флага Other RA.

Для сохранения изменений нажмите кнопку «Apply Changes».

### 6.5.9.2 Подменю «DHCPv6». Настройка DHCPv6-сервера

В разделе осуществляется настройка DHCPv6-сервера. По умолчанию работает в режиме автоконфигурации (DHCPv6Server(Auto)) через делегацию префикса.

*Advance* → *IPv6* → *DHCPv6*

**DHCPv6 Settings**

This page is used to configure DHCPv6 Server and DHCPv6 Relay.

---

**DHCPv6 Mode:**  Disable  Enable;

---

Auto Config by Prefix Delegation for DHCPv6 Server.

---

**NTP Server IP:**

**NTP Server Table**

Select	NTP Server
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>	

---

**Hostname:**

**MAC Address:**

**IP Address:**

**MAC Binding Table**

Select	Host Name	MAC Address	IP Address
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>			

- *DHCPv6 Mode* – включить/выключить работу сервера DHCPv6;
- *NTP Server IP* – настроить IP-адрес NTP-сервера для синхронизации времени;
- *Hostname* – указать имя хоста;
- *MAC Address* – указать MAC-адрес клиента для привязки IP-адреса;
- *IP Address* – указать IP-адрес клиента для привязки к MAC-адресу.

Для сохранения изменений нажмите кнопку «Apply Changes». По нажатию на кнопку «Show Client» выводится таблица активных IP-адресов DHCPv6-сервера.

*Advance* → *IPv6* → *DHCPv6* → *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	----	----

### 6.5.9.3 Подменю «MLD proxy». Настройка функции MLD proxy

В разделе можно включить/отключить работу MLD-proxy, для этого необходимо установить флаг «Enable»/«Disable».

Advance → IPv6 → MLD proxy

**MLD ProxyConfiguration**

This page be used to configure MLD Proxy.

**MLD Proxy:**  Disable  Enable

**WAN Interface:**

Для сохранения изменений нажмите кнопку «Apply Changes».

### 6.5.9.4 Подменю «MLD snooping». Настройка функции MLD snooping

В разделе можно включить/отключить работу MLD-snooping, для этого необходимо установить флаг «Enable»/«Disable».

Advance → IPv6 → MLD snooping

**MLD SnoopingConfiguration**

This page be used to configure MLD Snooping.

**MLD Snooping:**  Disable  Enable

Для сохранения изменений нажмите кнопку «Apply Changes».

### 6.5.9.5 Подменю «IPv6 routing». Настройка IPv6-маршрутов

В разделе осуществляется настройка статических IPv6-маршрутов.

Advance → IPv6 → IPv6 routing

**IPv6 Static RoutingConfiguration**

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

**Enable:**

**Destination:**

**Next Hop:**

**Metric:**

**Interface:**

**Static IPv6 Route Table:**

Select	State	Destination	Next Hop	Metric	Interface

- *Enable* – флаг для добавления маршрута;
- *Destination* – адрес назначения;
- *Next Hop* – следующий узел;
- *Metric* – метрика;
- *Interface* – интерфейс.

Для добавления IPv6 routing заполните соответствующие поля и нажмите кнопку «Add Route». Добавленные маршруты отображаются в таблице «Static IPv6 Route Table», для обновления информации нажмите кнопку «Update». Для удаления всей таблицы нажмите на кнопку «Delete All», чтобы удалить один маршрут, выберите его и нажмите кнопку «Delete Selected». Кнопка «Show Routes» выводит таблицу статических IPv6-маршрутов, к которым обычно обращается сеть.

Advance → IPv6 → IPv6 routing → Show Routes

**IP Route Table**

This table shows a list of destination routes commonly accessed by your network.

Destination	Next Hop	Flags	Metric	Ref	Use	Interface
fe80::e2d9:e3ff:fe9d:f7b2/128	::	U	0	1	0	lo
fe80::e2d9:e3ff:fe9d:f7b2/128	::	U	0	1	0	lo
fe80::e2d9:e3ff:fe9d:f7b2/128	::	U	0	1	0	lo
fe80::e2d9:e3ff:fe9d:f7b2/128	::	U	0	1	0	lo
fe80::e2d9:e3ff:fe9d:f7b2/128	::	U	0	1	0	lo
fe80::e2d9:e3ff:fe9d:f7b6/128	::	U	0	1	0	lo
ff02::1:2/128	::	UC	0	0	7	br0
ff00::/8	::	U	256	1	0	br0
ff00::/8	::	U	256	0	0	eth0
ff00::/8	::	U	256	0	0	nas0
ff00::/8	::	U	256	0	0	wlan0
ff00::/8	::	U	256	0	0	wlan1
ff00::/8	::	U	256	0	0	eth0.3

Refresh Close

- *Destination* — сеть назначение;
- *Next Hop* — следующий узел;
- *Flags* — флаги;
- *Metric* — метрика;
- *Ref* — источник маршрута;
- *Use* — использование маршрута;
- *Interface* — интерфейс, через который доступен указанный маршрут.

Для обновления таблице нажмите «Refresh», для закрытия окна — «Close».

#### 6.5.9.6 Подменю «IPv6 IP/Port filtering». Настройка фильтрации пакетов

На странице осуществляется настройка фильтрации пакетов данных, передаваемых через шлюз.

Advance → IPv6 → IP/Port filtering

**IPv6 IP/Port Filtering**

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

Outgoing Default Action  Deny  Allow

Incoming Default Action  Deny  Allow

Apply Changes

Direction:  Protocol:  Rule Action  Deny  Allow

Source Interface ID:

Destination Interface ID:

Source Port:  -

Destination Port:  -

Add

Current Filter Table:

Select	Direction	Protocol	Source IP Address	Interface ID	Source Port Destination	IP Address	Interface ID
--------	-----------	----------	-------------------	--------------	-------------------------	------------	--------------

Delete Selected Delete All

- *Outgoing Default Action Deny/Allow* – фильтрация для исходящих пакетов;
- *Incoming Default Action Deny/Allow* – фильтрация для входящих извне пакетов.

Для сохранения изменений нажмите кнопку «Apply Changes».

- *Direction Outgoing/Incoming* – направление передачи пакетов (исходящие/входящие);
- *Protocol* – выбор протокол;
- *Rule Action Deny/Allow* – политика обработки пакета (отбросить/пропустить);
- *Source Interface ID* – интерфейс источника;
- *Destination Interface ID* – интерфейс назначения;
- *Source Port* – порт источника;
- *Destination Port* – порт назначения.

Чтобы добавить фильтр, заполните соответствующие поля и нажмите кнопку «Add». Добавленные фильтры отображаются в таблице «*Current Filter Table*». Для удаления всей таблицы нажмите на кнопку «Delete All», чтобы удалить один фильтр, выберите его и нажмите кнопку «Delete Selected».

## 6.6 Меню «Diagnostics»

Раздел диагностики доступа к различным сетевым узлам.

### 6.6.1 Подменю «Ping». Проверка доступности сетевых устройств

Раздел предназначен для проверки доступности сетевых устройств при помощи утилиты Ping.

*Diagnostics → Ping*

**Ping Diagnostics**

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

---

**Host Address:**

Для проверки доступности подключенного устройства необходимо ввести его IP-адрес в поле «*Host Address*» и нажать кнопку «Go».

### 6.6.2 Подменю «Traceroute». Диагностика сети

Раздел предназначен для диагностики сети путем отправки UDP-пакетов и получения сообщения о доступности/недоступности порта.

*Diagnostics → Traceroute*

**Traceroute Diagnostics**

This page is used to diagnose the network by sending UDP-packets and receiving a message about port reach/unreachability.

---

**Host Address:**

**Max number of hops:**

Для диагностики сети необходимо ввести IP-адрес подключенного устройства в поле «*Host address*» и максимальное количество Hop для пакета.



### 6.6.3 Подменю «System Log». Логирование системных событий

Раздел предназначен для настройки/сохранения/просмотра логирования системных событий. Логирование можно выключить/включить путем установки флага «Disable/Enable» соответственно.

- *Log Level* – уровень логирования;
- *Display Level* – уровень отображения логов;
- *Clear log* – очистить журнал.

Для того чтобы сохранить журнал логов в локальное хранилище, нажмите на кнопку «Save».

## 6.7 Меню «Admin»

Раздел управления устройством. В данном меню производится настройка паролей, времени, конфигураций и прочего.

### 6.7.1 Подменю «Settings». Восстановление и сброс настроек

*Admin* → *Settings* → *Backup Settings*

В разделе можно скопировать текущие настройки в файл (*Backup Settings*) нажатием на кнопку «Backup Settings to File».

*Admin* → *Settings* → *Update Settings*

В разделе можно восстанавливать настройки из файла, который был сохранен ранее (*Update Settings*) кнопкой «Restore».

*Admin → Settings → Restore Default*

**Restore Default**

This page allows you to restore factory default settings

[Reset Settings to Default](#)

В разделе можно сбросить текущие настройки до заводских настроек по умолчанию (*Restore Default*), для этого нажмите кнопку «Reset Settings to Default».

## 6.7.2 Подменю «GPON Setting». Настройка доступа к GPON

В разделе можно указать пароль для активации терминала на OLT.

*Admin → GPON Setting*

**GPON Settings**

This page is used to configure the parameters for your GPON network access.

**PLOAM Password:**

[Apply Changes](#)

- *PLOAM Password* – пароль для активации терминала на OLT.

Для сохранения изменений нажмите кнопку «Apply Changes».

## 6.7.3 Подменю «Commit/Reboot». Сохранение изменений и перезагрузка устройства

Нажмите кнопку «Commit and Reboot» для перезагрузки устройства или для сохранения изменений в системной памяти. Перезагрузка устройства может занять несколько минут.

*Admin → Commit/Reboot*

**Commit and Reboot**

Click the button below to reboot the router

[Commit and Reboot](#)

## 6.7.4 Подменю «Logout». Выход из учетной записи

В разделе возможно выйти из учетной записи нажатием на кнопку «Logout».

*Admin → Logout*

**Logout**

This page is used to logout from the Device.

[Logout](#)

### 6.7.5 Подменю «Password». Настройка контроля доступа (установка паролей)

В разделе осуществляется смена пароля для доступа к устройству.

*Admin → Password*

**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:**

**Old Password:**

**New Password:**

**Confirmed Password:**

Для смены пароля необходимо ввести существующий пароль в поле «*Old Password*», затем новый пароль в «*New Password*» и подтвердить его «*Confirmed Password*».

Для принятия изменений и сохранения нажмите кнопку «Apply Changes», для сброса значения — кнопку «Reset».

### 6.7.6 Подменю «Firmware upgrade». Обновление ПО

Для обновления ПО выберите файл ПО, используя кнопку «Выберите файл», и нажмите «Upgrade». Для сброса значения используйте кнопку «Reset».

*Admin → Firmware upgrade*

**Firmware Upgrade**

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

**Step 2:** Click the "Choose File" button to locate the image file.

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

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

---

No file selected.

- ✓ В процессе обновления не допускается отключение питания устройства либо его перезагрузка. Процесс обновления может занимать несколько минут, после чего устройство автоматически перезагружается.

### 6.7.7 Подменю «Remote Access». Настройка правил удалённого доступа

В разделе возможно настроить правила удалённого доступа по протоколам HTTP/Telnet/ICMP.

*Admin → Remote Access*

**Remote Access Configuration**  
This page is used to configure the Remote Access rules.

Enable:

Service: HTTP ▾

Interface: Default ▾

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Port:

**RA Table:**

Select	State	Interface	IP Address	Service	Port
<input type="checkbox"/>	Enable	br0	0.0.0.0/0	HTTP	80
<input type="checkbox"/>	Enable	br0	0.0.0.0/0	ICMP	--

- *Enable* – включение правила для добавления;
- *Service* – выбор используемого протокола;
- *Interface* – интерфейс, к которому применяется правило;
- *IP Address* – IP-адрес источника;
- *Subnet Mask* – маска подсети;
- *Port* – порт назначения.

Чтобы добавить правило, заполните соответствующие поля и нажмите кнопку «Add». Добавленные правила отображаются в таблице «RA Table». Чтобы активировать/деактивировать выделенное правило, нажмите кнопку «Toggle selected». Для удаления одного правила выберите его флагом в столбце *Select* и нажмите кнопку «Delete Selected».

### 6.7.8 Подменю «Time zone». Настройки системного времени

В разделе настраивается системное время на устройстве, возможна синхронизация с интернет-серверами точного времени.

*Admin → Time zone*

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

Current Time : Year  Mon  Day

Hour  Min  Sec

Time Zone Select : Europe/Moscow (UTC+03:00) ▾

Enable Daylight Saving Time

Enable SNTP Client Update

WAN Interface: Any ▾

SNTP Server :  clock.fmt.he.net ▾

220.130.158.52 (Manual Setting)

- *Current time* – текущее время;
- *Time Zone Select* – временная зона;
- *Enable Daylight Saving Time* – переход на летнее время;
- *Enable SNTP Client Update* – включить синхронизацию времени по SNTP;
- *WAN Interface* – интерфейс, через который производится обновление времени;
- *SNTP Server* – предпочитаемый сервер времени.

Для сохранения изменений нажмите кнопку «Apply Changes», для обновления информации – кнопку «Refresh».

### 6.7.9 Подменю «TR-069». Настройка TR-069

В разделе указываются данные для управления устройством посредством TR-069.

*Admin* → *TR-069*

**TR-069 Configuration**

This page is used to configure the TR-069 CPE. Here you may change the setting for the ACS's parameters.

---

**TR069 Daemon:**  Enabled  Disabled

**EnableCWMPParamete:**  Enabled  Disabled

---

**ACS:**

**URL:**

**UserName:**

**Password:**

**Periodic Inform:**  Disabled  Enabled

**Periodic Inform Interval:**

---

**Connection Request:**

**UserName:**

**Password:**

**Path:**

**Port:**

---

**Certificate Management:**

**CPE Certificate Password:**

**CPE Certificate:**  Файл не выбран

**CA Certificate:**  Файл не выбран

- *TR069 Daemon (Enable/Disabled)* – включение/выключение демона TR-069;
- *EnableCWMPParamete (Enable/Disabled)* – разрешение/запрещение настройки по CWMP;
- *ACS* – настройка ACS-сервера;
- *URL* – URL для соединения;
- *UserName* – имя пользователя для доступа к серверу;
- *Password* – пароль пользователя для доступа к серверу;
- *Periodic Inform* – включение/выключение периодичности отправки сообщений;
- *Periodic Inform Interval* – период отправки сообщений.

**Connection Request** – данные для авторизации для подключения сервера к ONT.

- *UserName* – имя пользователя;
- *Password* – пароль для подключения;
- *Path* – путь подключения;
- *Port* – порт для подключения.

**Certificate Management** – управление сертификатами.

- *CPE Certificate Password* – пароль от сертификата;
- *CPE Certificate* – выбор сертификата для CPE;
- *CA Certificate* – выбор сертификата для CA.

Для сохранения изменений нажмите кнопку «Apply», для сброса «Undo». Чтобы загрузить выбранный файл, нажмите кнопку «Upload».

## 6.8 Меню «Statistics». Информация о прохождении трафика на портах устройства

### 6.8.1 Подменю «Interface». Информация о счетчиках и ошибках

В разделе отображаются счетчики/ошибки по пакетам для каждого интерфейса:

#### Statistics → Interface

Interface Statistics							
This page shows the packet statistics for transmission and reception regarding to network interface.							
Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop	
LAN 1	1893	0	2	3174	0	0	
LAN 2	0	0	0	0	0	0	
LAN 3	0	0	0	0	0	0	
LAN 4	0	0	0	0	0	0	
Wi-Fi 2.4GHz	682	0	0	0	0	0	
Wi-Fi 5GHz	2111	0	0	277	0	0	
ppp0_nas0_0	366	0	0	266	0	0	
nas0_1	59	0	0	15	0	0	
nas0_2	10	0	0	0	0	0	

Refresh    Reset Statistics

- *Interface* – интерфейс;
- *Rx pkt* – получено пакетов;
- *Rx err* – ошибки на приеме;
- *Rx drop* – отброшено на приеме;
- *Tx pkt* – отправлено пакетов;
- *Tx err* – ошибка отправки;
- *Tx drop* – отброшено при передаче.

Для обновления данных на странице нажмите кнопку «Refresh».

## 6.8.2 Подменю «PON»

В разделе отображаются счетчики для оптического интерфейса:

*Statistics* → *PON*

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

- *Bytes Sent* – отправлено байт;
- *Bytes Received* – байт получено;
- *Packets Sent* – пакетов отправлено;
- *Packets Received* – пакетов получено;
- *Unicast Packet Sent* – Unicast-пакетов отправлено;
- *Unicast Packet Received* – Unicast-пакетов получено;
- *Multicast Packets Sent* – Multicast-пакетов отправлено;
- *Multicast Packets Received* – Multicast-пакетов получено;
- *Broadcast Packet Sent* – широковещательных пакетов отправлено;
- *Broadcast Packet Received* – широковещательных пакетов получено;
- *FEC Errors* – ошибки FEC;
- *HEC Errors* – ошибки HEC;
- *Packets Dropped* – пакетов отброшено;
- *Pause Packets Sent* – Pause-пакетов получено;
- *Pause Packets Received* – Pause-пакетов отправлено;

## Техническая поддержка

Для получения технической консультации по вопросам эксплуатации оборудования ООО «Предприятие «ЭЛТЕКС» Вы можете обратиться в Сервисный центр компании:

Форма обратной связи на сайте: <https://eltex-co.ru/support/>

Servicedesk: <https://servicedesk.eltex-co.ru>

На официальном сайте компании Вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «ЭЛТЕКС», обратиться к базе знаний, оставить интерактивную заявку или проконсультироваться у инженеров Сервисного центра на техническом форуме:

Официальный сайт компании: <https://eltex-co.ru/>

Технический форум: <https://eltex-co.ru/forum>

База знаний: <https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base>

Центр загрузок: <https://eltex-co.ru/support/downloads>