Оптические сетевые терминалы

NTU-MD500P

Руководство по эксплуатации, Версия ПО 2.4.1

Содержание

1 Введение 5
2 Описание изделия 6
2.1 Назначение 6
2.2 Характеристики устройств 6
2.3 Основные технические параметры 7
2.4 Конструктивное исполнение 9
2.4.1 Внешний вид и описание передней панели устройства 9
2.4.2 Боковая и задняя панели устройства 10
2.5 Световая индикация 11
2.6 Комплект поставки 12
2.7 Меры безопасности и порядок установки 12
2.7.1 Введение 12
2.7.2 Требования техники безопасности 12
2.7.3 Порядок установки терминала 12
3 Архитектура устройства 15
4 Настройка устройств через Web-интерфейс. Доступ администратора. 16
4.1 Меню «Status». Информация об устройстве 18
4.1.1 Подменю «Device status». Общая информация об устройстве 18
4.1.2 Подменю «IPv6 Status». Информация о системе IPv6 19
4.1.3 Подменю «PON». Информация о статусе оптического модуля 20
4.1.4 Подменю «LAN». Информация о статусе интерфейса LAN 21
4.2 Меню «LAN». Настройка интерфейса LAN 21
4.3 Меню «WAN». Настройка интерфейса WAN 22
4.3.1 Подменю «IPsec». Настройка IP Security 22
4.3.2 Подменю «PON WAN» 23
4.3.3 Подменю «L2TP». Настройка L2TP VPN 24
4.4 Меню «Services». Настройка сервисов 25
4.4.1 Подменю «DHCP Setting». Настройка DHCP 25
4.4.2 Подменю «Dynamic DNS». Настройки динамической системы доменных имен 26
4.4.3 Подменю «Firewall». Настройка брандмауэра 27
4.4.3.1 Подменю «ALG On-Off Configuration». Включение отключение сервисов ALG. 27
4.4.3.2 Подменю «IP/Port Filtering». Настройки фильтрации адресов 27
4.4.3.3 Подменю «MAC Filtering». Настройки фильтрации по MAC-адресам 28

4.4.3.4 Подменю «Port Forwarding». Настройка проброса портов 28
4.4.3.5 Подменю «URL Blocking». Настройки ограничения доступа в интернет 29
4.4.3.6 Подменю «Domain Blocking». Настройка блокировки доменов 30
4.4.3.7 Подменю «DMZ». Настройки демилитаризованной зоны 31
4.4.4 Подменю «UPnP». Автоматическая настройка сетевых устройств 31
4.4.5 Подменю «RIP». Настройка динамической маршрутизации 31
4.5 Меню «Advance». Расширенные настройки 32
4.5.1 Подменю «ARP Table». Просмотр кэша протокола ARP 32
4.5.2 Подменю «Bridging». Настройка параметров Bridging 33
4.5.3 Подменю «Routing». Настройка маршрутизации 34
4.5.4 Подменю «Interface grouping». Объединение интерфейсов в группы 34
4.5.5 Подменю «PoE Settings». Конфигурирование PoE портов 35
4.5.6 Подменю «IP QoS». Настройка качества предоставляемых услуг (QoS) 36
4.5.6.1 Подменю «QoS Policy». Настройка QoS очередей 36
4.5.6.2 Подменю «QoS Classification». Настройка правил классификации трафика 37
4.5.6.3 Подменю «Traffic Shaping». Настройка трафика 38
4.5.7 Подменю «Link mode». Настройка LAN-портов 38
4.5.8 Подменю «IPv6». Настройка протокола IPv6 39
4.5.8.1 Подменю «RADVD». Настройка RADVD 39
4.5.8.2 Подменю «DHCPv6». Настройка DHCPv6-сервера 40
4.5.8.3 Подменю «MLD proxy». Настройка функции MLD proxy 41
4.5.8.4 Подменю «MLD snooping». Настройка функции MLD snooping 41
4.5.8.5 Подменю «IPv6 routing». Настройка IPv6 маршрутов 41
4.5.8.6 Подменю «IPv6 IP/ Port filtering». Настройка фильтрации пакетов 43
4.6 Подменю «Diagnostics» 43
4.6.1 Подменю «Ping». Проверка доступности сетевых устройств 43
4.6.2 Подменю «Traceroute» 44
4.7 Подменю «Admin» 44
4.7.1 Подменю «Settings». Восстановление и сброс настроек 44
4.7.2 Подменю «GPON Setting». Настройка доступа к GPON 45
4.7.3 Подменю «Commit/Reboot». Сохранение изменений и перезагрузка устройства 45
4.7.4 Подменю «Logout». Выход из учетной записи 45

4.7.5 Подменю «Password». Настройка контроля доступа (установление паролей) 46
4.7.6 Подменю «Firmware upgrade». Обновление ПО 46
4.7.7 Подменю «Remote Access». Настройка правил удалённого доступа 47
4.7.8 Подменю «Time zone». Настройки системного времени 47
4.7.9 Подменю «TR-069». Настройка TR-069 48
4.8 Меню «Statistics». Информация о прохождении трафика на портах устройства 49
4.8.1 Подменю «Interface». Информация о счетчиках и ошибках 49
4.8.2 Подменю «PON» 50
5 Список изменений 51

1 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.

Сетевое оборудование NTU-MD500P производства «ЭЛТЕКС» представлена терминалами, которые рассчитаны на четыре UNI интерфейса 10/100/1000BASE-T.

В настоящем руководстве по эксплуатации изложены назначение, основные технические характеристики, правила конфигурирования, мониторинга оптических сетевых терминалов NTU-MD500P.

Примечания и предупреждения

Примечания содержат важную информацию, советы или рекомендации 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.

2 Описание изделия

2.1 Назначение

NTU-MD500P — оптические сетевые терминалы, которые имеют 4 порта 10/100/1000BASE-T с поддержкой стандарта IEEE 802.3at PoE+. Терминалы NTU-MD500P обеспечивают мощность до 30 Вт на портах 10/100/1000BASE-T с бюджетом мощности PoE — 65 Вт.

Поддержка технологии PoE позволяет подать электро-питание 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.

2.2 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 (trasport 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.

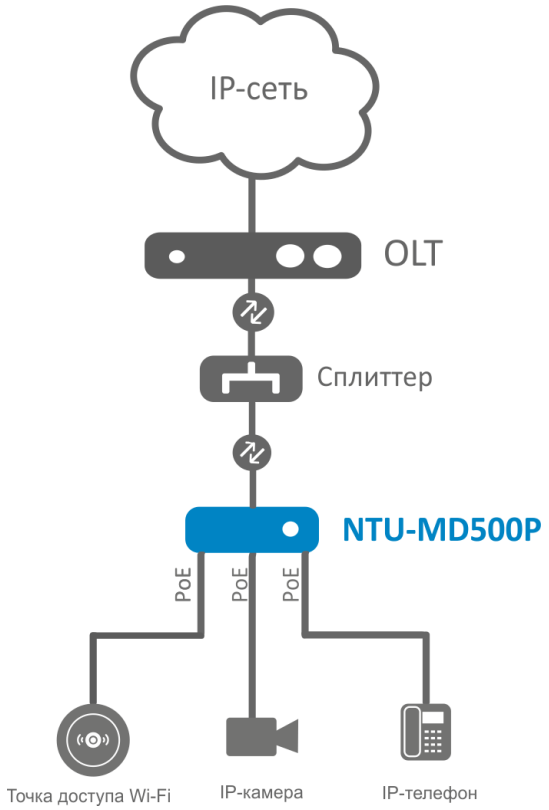


Рисунок 1 — Схема применения NTU-MD500P

2.3 Основные технические параметры

Основные технические параметры терминалов приведены в таблице 1:

Таблица 1 — Основные технические параметры

Параметры интерфейсов Ethernet LAN

Количество интерфейсов	4
Электрический разъем	RJ-45
Скорость передачи, Мбит/с	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
• Скорость соединения upstream	1244 Мбит/с
• Мощность передатчика	+0,5 дБм до +5 дБм
• Ширина спектра оптического излучения (RMS)	1 нм
Приемник:	1490 нм
• Скорость соединения downstream	2488 Мбит/с
• Чувствительность приемника	от -8 до -28, BER≤1.0×10^{-10}
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 до +40°C
Относительная влажность	Не более 80%
Габариты (ШхВхГ)	267x44x178 мм
Исполнение	19", типоразмер 1U
Масса	1,56 кг

2.4 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.

2.4.1 Внешний вид и описание передней панели устройства

Внешний вид передней панели устройства приведен на рисунке 2.

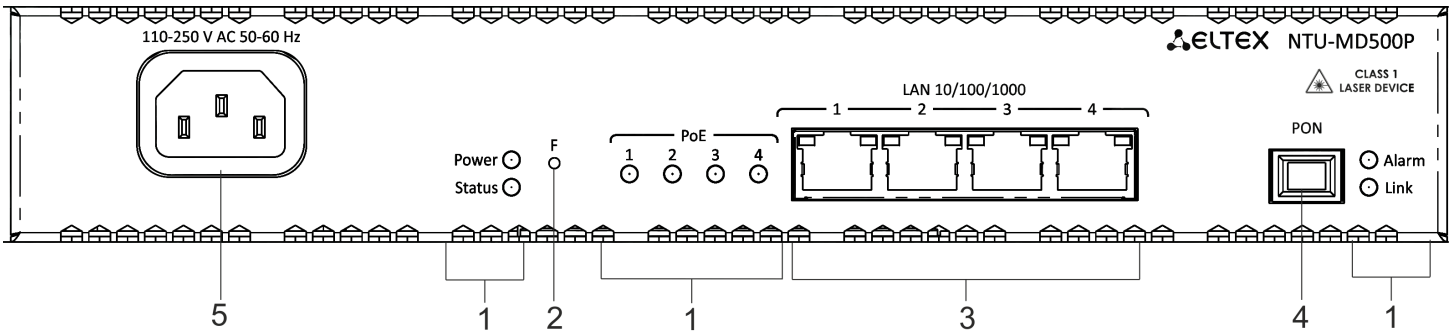


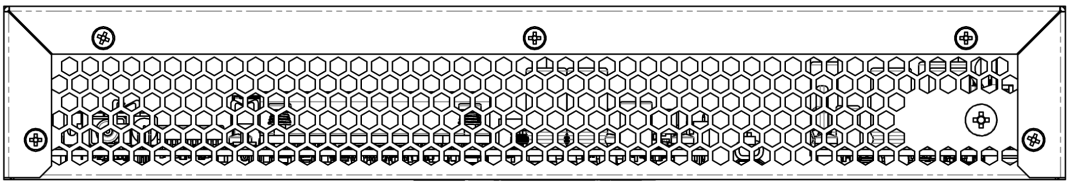
Рисунок 2 — Внешний вид задней панели NTU-MD500P

Таблица 2 — Описание разъемов, и органов управления передней панели

№	Элемент передней панели	Описание
1	Power	Индикатор питания устройства.
	Status	Индикатор работы устройства.

№	Элемент передней панели	Описание
	Alarm	Индикатор отсутствия оптического сигнала.
	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 с происходит перезагрузка устройства; - при нажатии на кнопку длительностью более 10 с 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.

2.4.2 Боковая и задняя панели устройства



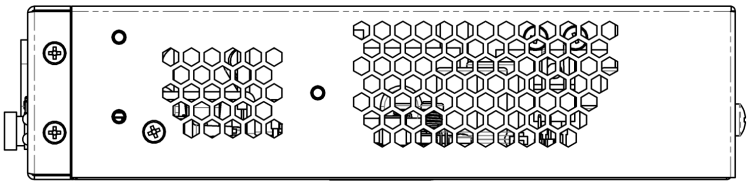


Рисунок 3 — Левая боковая панель NTU-MD500P

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 «Установка и подключение».

2.5 Световая индикация

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

Таблица 3 — Световая индикация состояния терминала

Название индикатора	Состояние индикатора	Состояние устройства
Power	Зеленый, горит постоянно	Питание включено, нормальная работа устройства.
	Не горит	Питание выключено.
Status	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.
PoE 1-4	Зеленый, горит постоянно	Подключен потребитель PoE, подача питания осуществляется (горит индикатор, соответствующий порту).
	Красный, горит постоянно	Ошибка PoE на порту.
	Выключен	Потребитель PoE не подключен.
Alarm	Не горит	Нормальная работа устройства.
	Красный, горит постоянно	Оптический сигнал отсутствует.
Link	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.
LAN P1..P4	Зелёный	Установлено соединение 10/100 Мбит/с.
	Оранжевый	Установлено соединение 1000 Мбит/с.
	Мигает	Процесс пакетной передачи данных.

2.6 Комплект поставки

В базовый комплект поставки устройства NTU-MD500P входят:

- Абонентский оптический терминал NTU-MD500P;
- Шнур питания евровилка-C13-F-1.8м;
- Памятка о документации;
- Сертификат соответствия;
- Руководство по эксплуатации.

2.7 Меры безопасности и порядок установки

2.7.1 Введение

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

2.7.2 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 6,0x10*4 до 10,7x10*4 Па (от 450 до 800 мм рт.ст.).
4. Не подвергать терминал воздействию механических ударов и колебаний, а так же 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 1В.
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.

2.7.3 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.

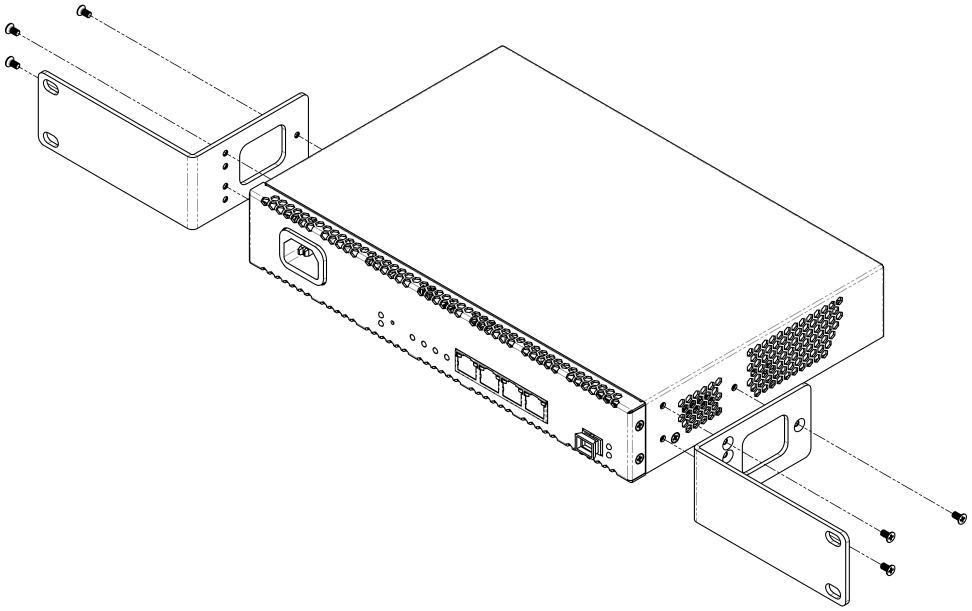


Рисунок 4 — Крепление кронштейнов

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.

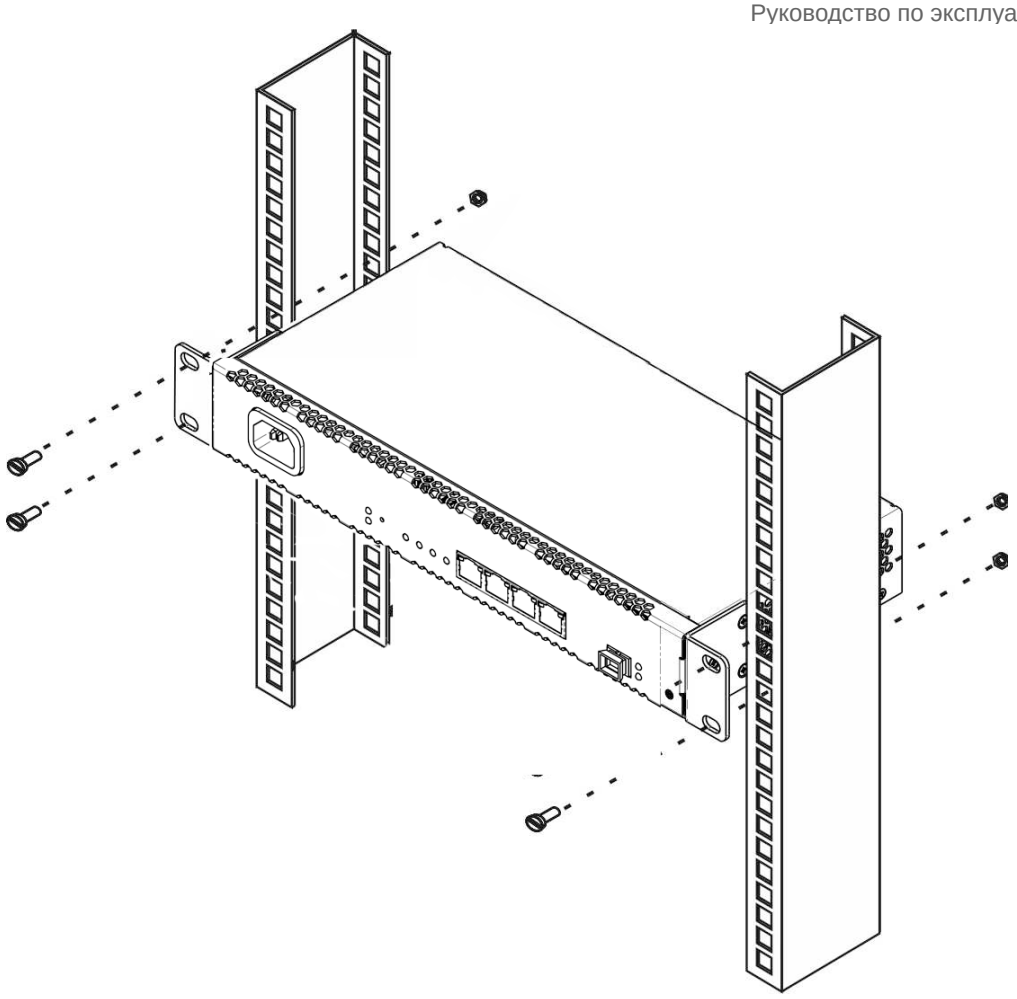


Рисунок 5 — Крепление кронштейнов

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.

3 Архитектура устройства

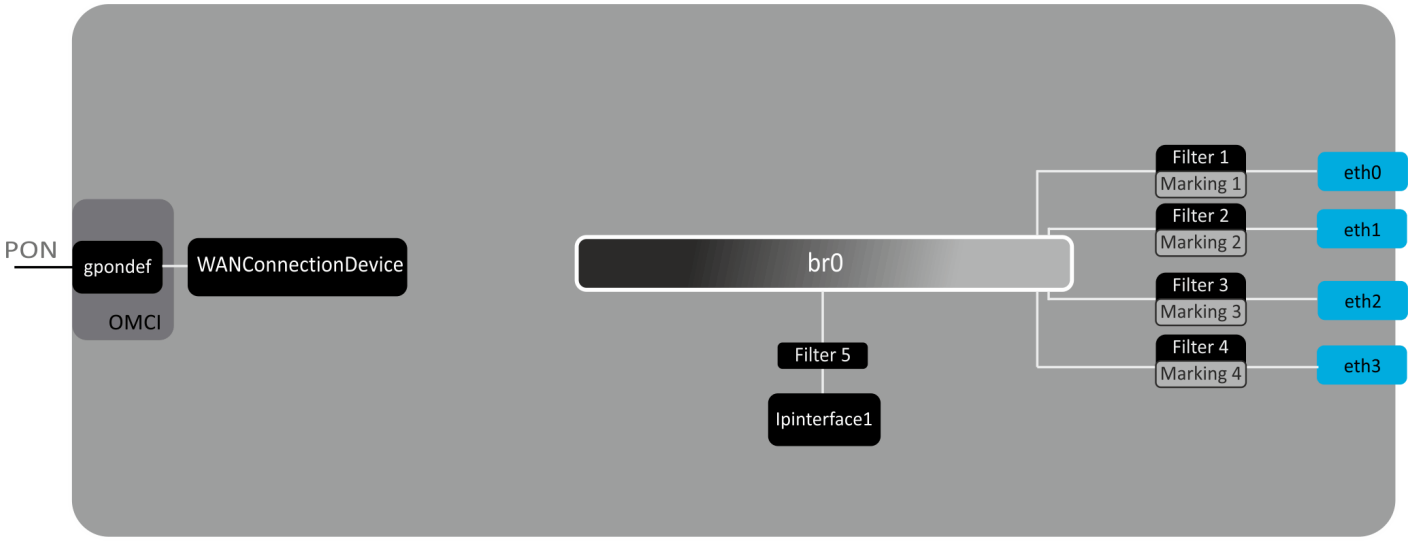


Рисунок 6 — Логическая архитектура устройства с заводской конфигурацией

Основные элементы устройства:

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

При заводской (начальной) конфигурации в устройстве присутствуют следующие логические блоки (рис. 6):

- 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.

4 Настройка устройств через Web-интерфейс. Доступ администратора.

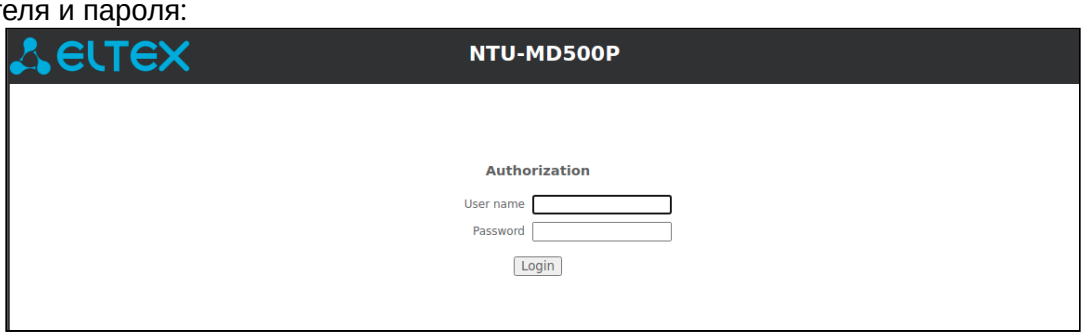
Начало работы

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:



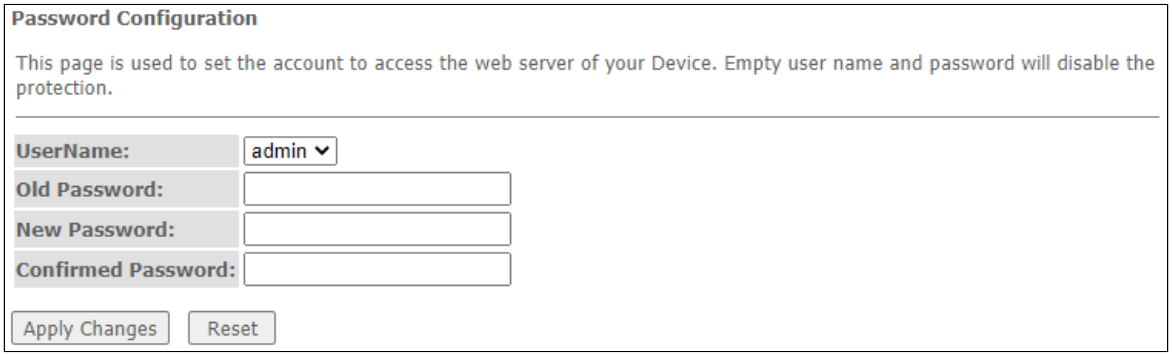
3. Введите имя пользователя в строке «User Name» и пароль в строке «Password».

   Имя пользователя *admin*, пароль *password*.

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

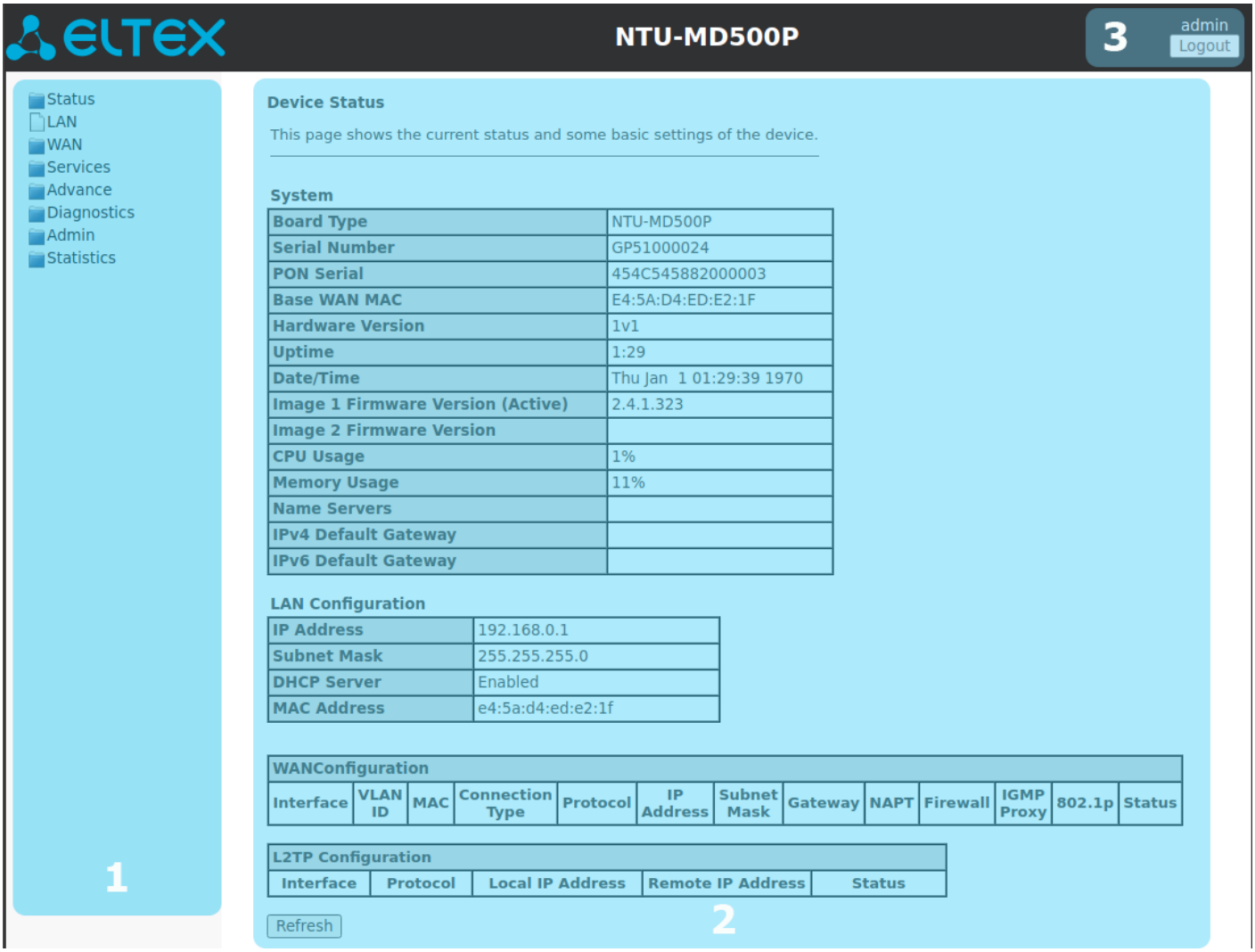
Смена пароля

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.



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.

4.1 Меню «Status». Информация об устройстве

4.1.1 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

WANConfiguration

Interface	VLAN ID	MAC	Connection Type	Protocol	IP Address	Subnet Mask	Gateway	NAPT	Firewall	IGMP Proxy	802.1p	Status
nas0_0	41	e4:5a:d4:ed:e2:20	Other	Bridged								down

L2TP Configuration

Interface	Protocol	Local IP Address	Remote IP Address	Status

Refresh

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 DHCH-сервера;
- *MAC Address* — MAC-адрес устройства.

WAN Configuration

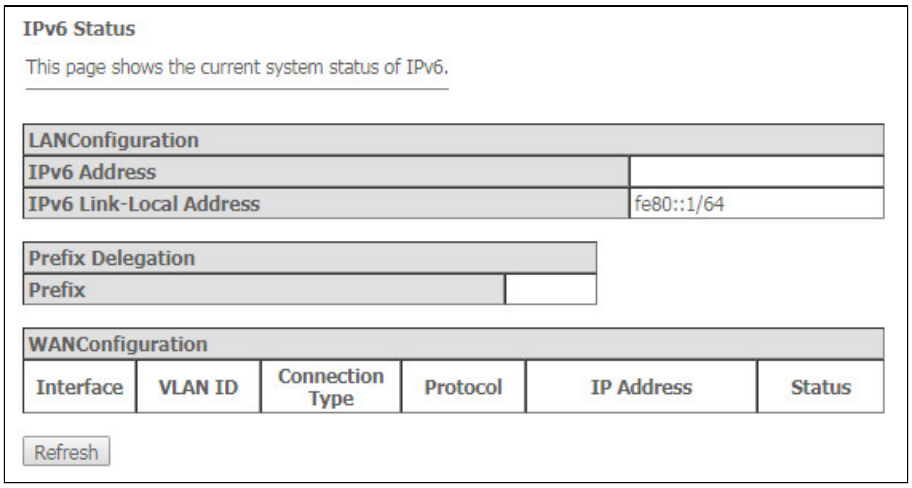
- *Interface* — название интерфейса;
- *VLAN ID* — VLAN ID интерфейса;
- *MAC* — MAC-адрес интерфейса;
- *Connection Type* — тип соединения;
- Protocol — используемый протокол;
- *IP Address* — IP-адрес интерфейса;
- *Gateway* — шлюз;
- *Status* — статус интерфейса.

Для обновления данных на странице нажмите кнопку «Refresh».

4.1.2 Подменю «IPv6 Status». Информация о системе IPv6

В разделе отображается текущий статус системы IPv6.

Status → IPv6



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».

4.1.3 Подменю «PON». Информация о статусе оптического модуля

В разделе показано текущее состояние PON-интерфейса.

Status → PON

PON Status

This page shows the current system status of PON.

PON Status	
Vendor Name	REALTEK
Part Number	RTL8290
Temperature	48.691406 C
Voltage	3.342300 V
Tx Power	1.228869 dBm
Rx Power	-15.951663 dBm
Bias Current	19.848000 mA

GPON Status	
ONU State	O5
ONU ID	1
LOID Status	Initial Status

Refresh

PON Status

- *Vendor Name* — наименование производителя;
- *Part Number* — номер партии;
- *Temperature* — текущая температура;
- *Voltage* — напряжение;
- *Tx Power* — мощность сигнала на передаче;
- *Rx Power* — мощность сигнала на приеме;
- *Bias Current* — ток смещения.

PON Status

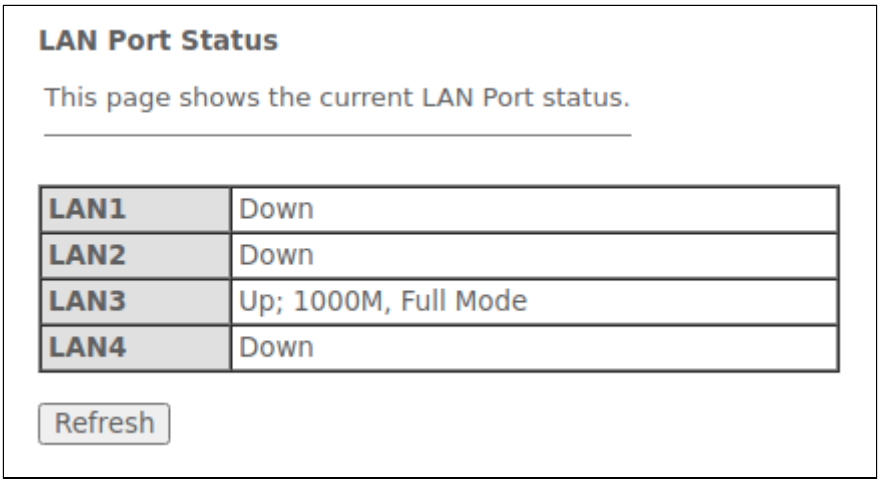
- *ONU State* — статус авторизации на OLT (O1 -> O2 -> O3 -> O4 -> O5);
- *ONU ID* — идентификатор устройства на OLT;
- *LOID Status* — статус авторизации на OLT (Initial -> Standby -> Serial Number -> Ranging -> Operation)

Для обновления данных на странице нажмите кнопку «Refresh».

4.1.4 Подменю «LAN». Информация о статусе интерфейса LAN

В разделе доступен просмотр основных характеристик интерфейсов LAN.

Status → LAN

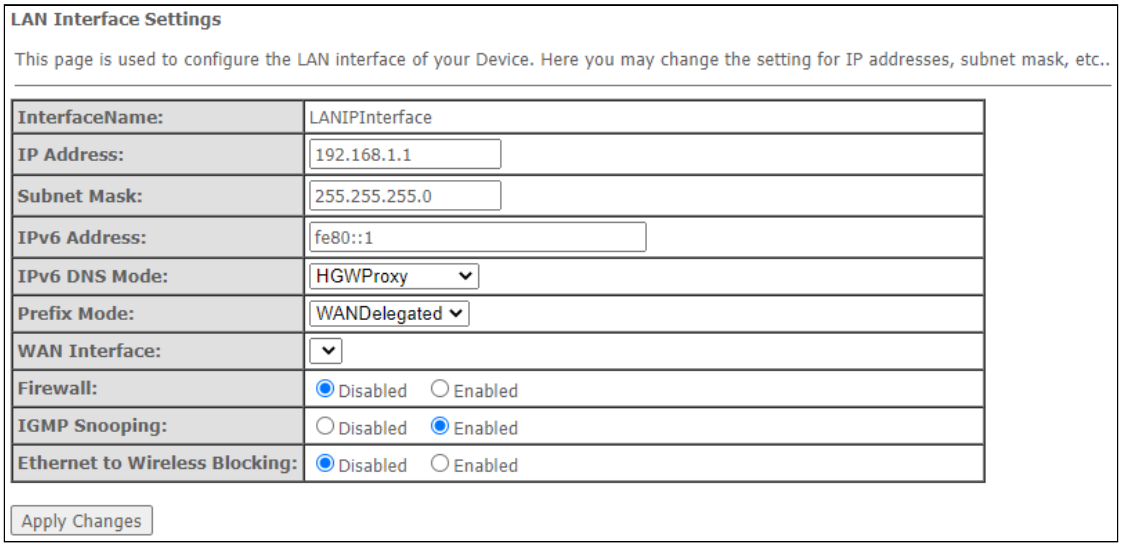


Для обновления информации в таблице нажмите кнопку «Refresh».

4.2 Меню «LAN». Настройка интерфейса LAN

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

LAN



- *Interface name* — название интерфейса;
- *IP Address* — IP-адрес интерфейса;
- *Subnet Mask* — маска подсети интерфейса;
- *IPv6 Address* — IPv6-адрес;
- *IPv6 DNS Mode* — настроить режим использования доменных имён:
  - *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.
- *IPv6 DNS* — указать статический адрес DNS-сервера (IPv6 DNS1, IPv6 DNS2);
- *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.

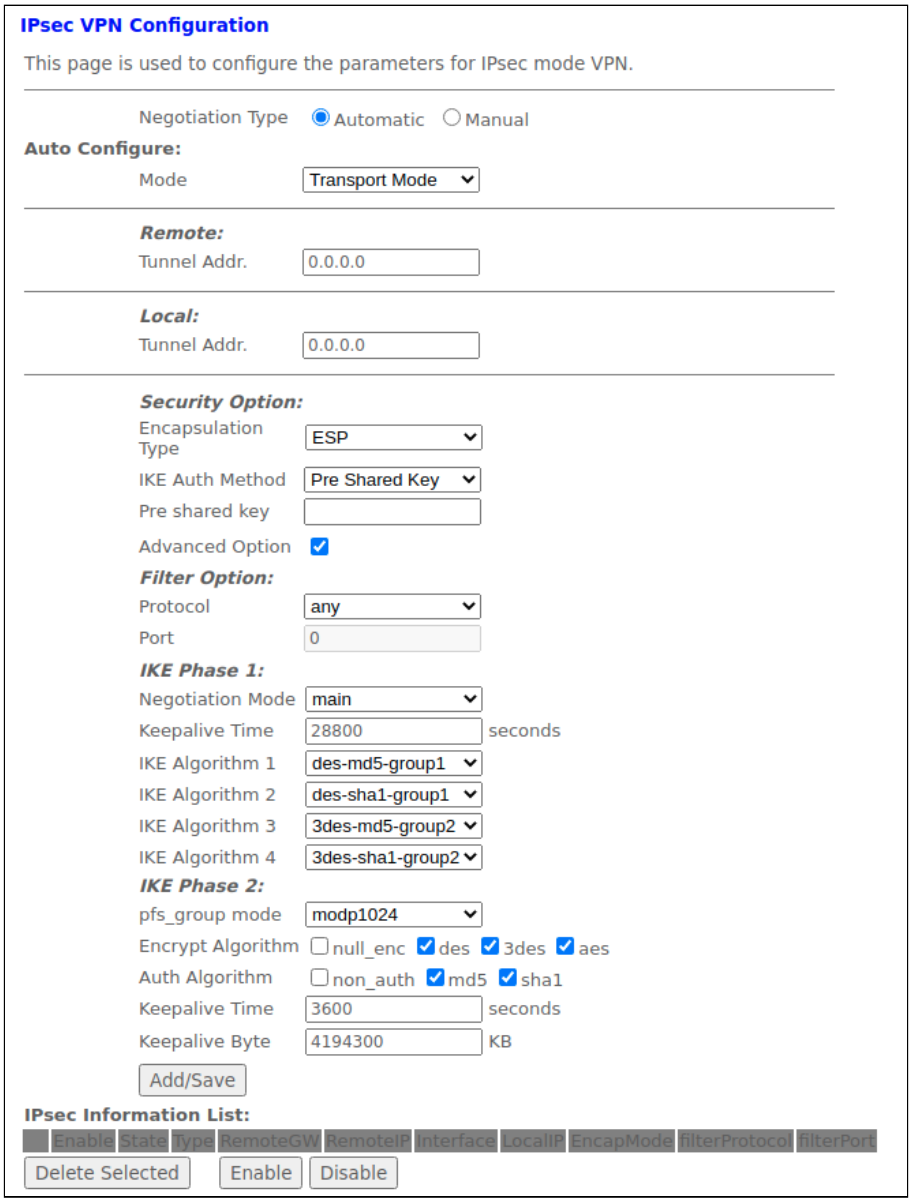
Для сохранения изменений нажмите кнопку «Apply Changes».

4.3 Меню «WAN». Настройка интерфейса WAN

4.3.1 Подменю «IPsec». Настройка IP Security

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

WAN → IPsec



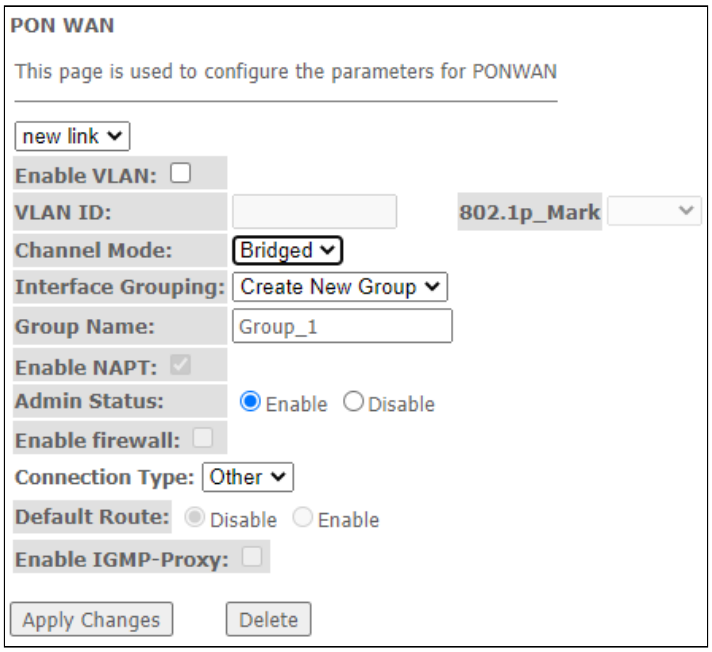
- Negotiation Type — выбор типа согласования;
- Negotiation Type — Automatic;

- 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.

4.3.2 Подменю «PON WAN»

В разделе можно настроить параметры PON WAN.

WAN → PON WAN



- *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;

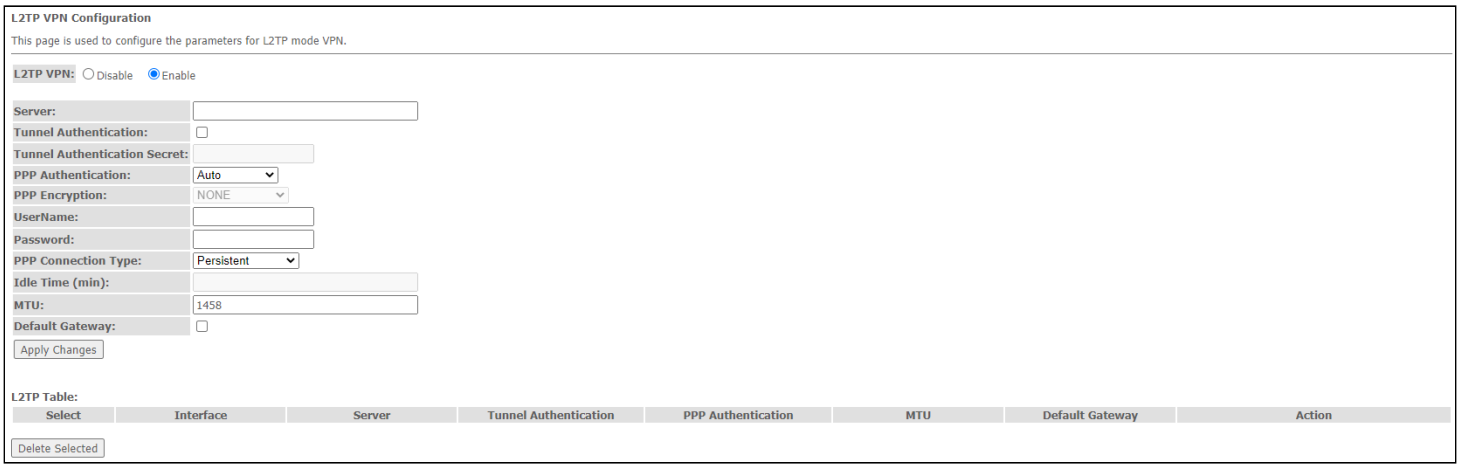
- *PPPoE* — установка point-to-point туннеля через Ethernet.
- *Enable NAPT* — включение функции NAPT;
- *Admin Status (Enable/Disable)* — включение/выключение административного статуса;
- *Enable RIPv2* — включение маршрутизации по протоколу RIPv2;
- *Enable Firewall* — включение брандмауэра;
- *Connection 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 пересылку сообщений IGMP.

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

4.3.3 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* — 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».

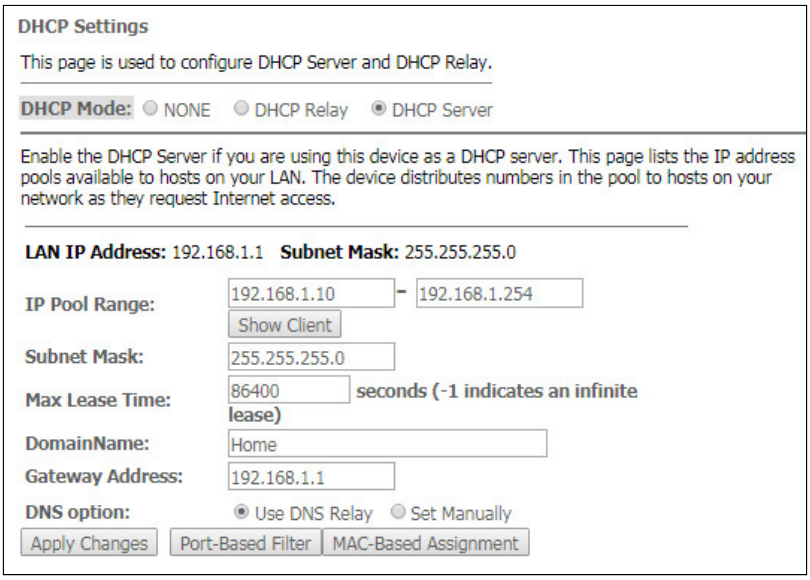
В таблице «L2TP Table» осуществляется просмотр состояния виртуального соединения L2TP VPN. Для удаления определённой записи, выделите позицию и нажмите кнопку «Delete Selected».

4.4 Меню «Services». Настройка сервисов

4.4.1 Подменю «DHCP Setting». Настройка DHCP

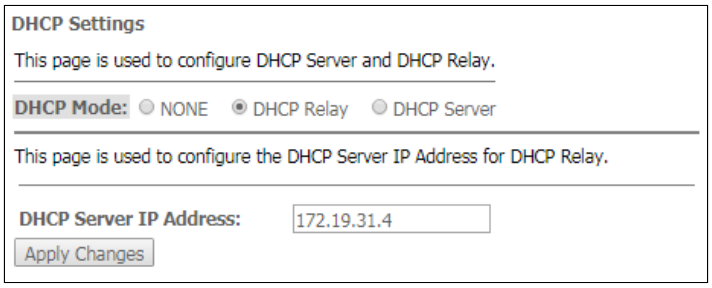
В разделе происходит настройка DHCP сервера или DHCP ретранслятора.

Services → DHCP (Server)



- *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 посети;
- *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 Server IP Address* — IP-адрес удалённого сервера DHCP.

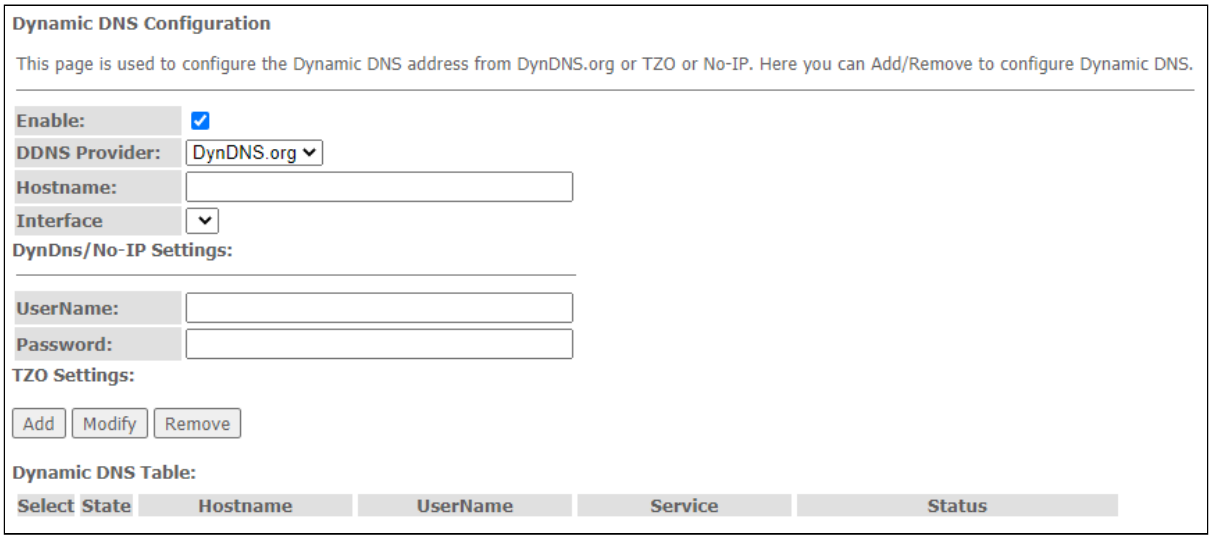
Для сохранения изменений нажмите кнопку «Apply Changes». Кнопки «Port-Based Filter» и «MAC-Based Assignment» позволяют настроить фильтрацию по портам и MAC, соответственно.

4.4.2 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



- *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, TZO.com, 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.

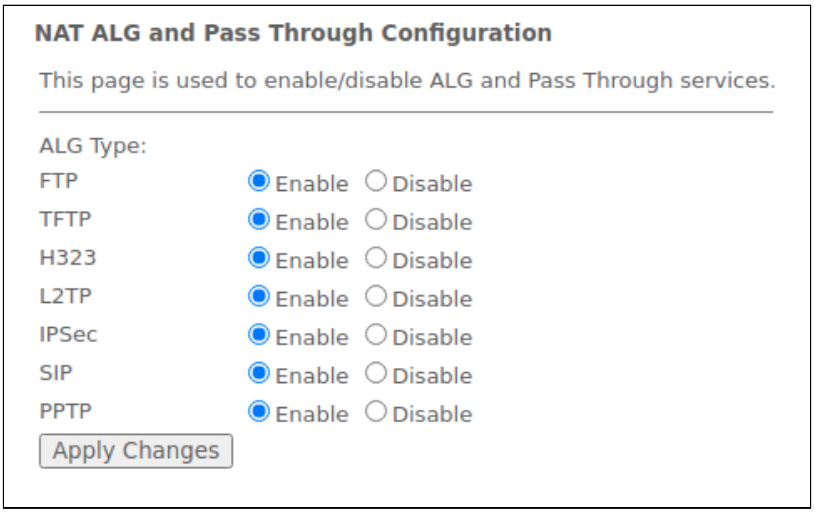
В разделе отображается таблица *« Dynamic DNS Table»* со списком имеющихся DNS и его параметрами. Для добавления записи нажмите кнопку «Add». Чтобы изменить / удалить позицию позицию, выберите её и нажмите «Modify» / «Remove» напротив выбранной записи.

4.4.3 Подменю «Firewall». Настройка брандмауэра

4.4.3.1 Подменю «ALG On-Off Configuration». Включение отключение сервисов ALG.

В разделе можно включить или отключить сервисы ALG.

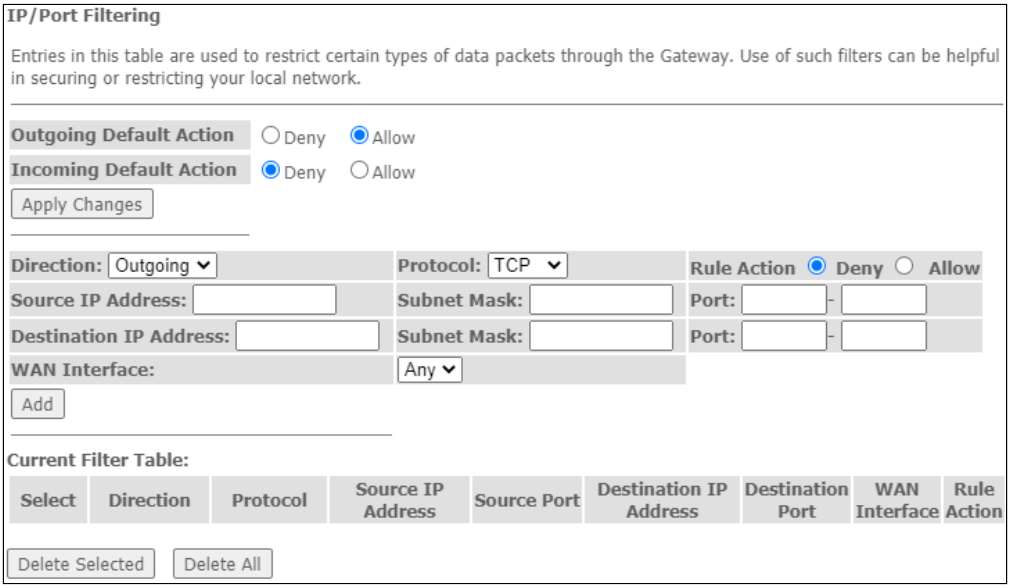
Services → Firewall → ALG



4.4.3.2 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



Настройки по умолчанию

- *Incoming Default Action Deny / Allow* — фильтрация для входящих из-вне пакетов;
- *Outgoing Default Action Deny / Allow* — фильтрация для исходящих пакетов.

Для сохранения изменений нажмите кнопку «Apply Changes».

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

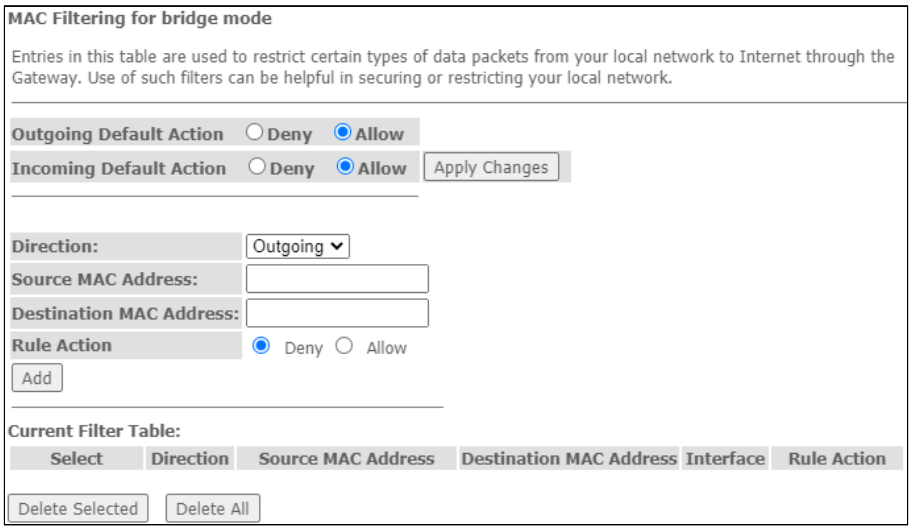
- *Protocol* — протокол фильтрации;
- *Rule Action Deny / Allow* — политика обработки пакета (отбросить/пропустить);
- *Source IP Address* — IP-адрес источника;
- *Destination IP Address* — IP-адрес назначения;
    - *Subnet mask* — маска подсети;
    - *Port* — порт.
- *Ingress Interface* — входящий интерфейс.

Добавленные фильтры отображаются в ниже расположенной 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».

4.4.3.3 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



- *Default Action* — настройки по умолчанию:
    - *Deny* — при установке флага прохождение трафика по умолчанию запрещено;
    - *Allow* — при установке флага прохождение трафика по умолчанию разрешено;
- *MAC Address* — поле для добавления MAC-адреса для которого вводится ограничение/доступ.

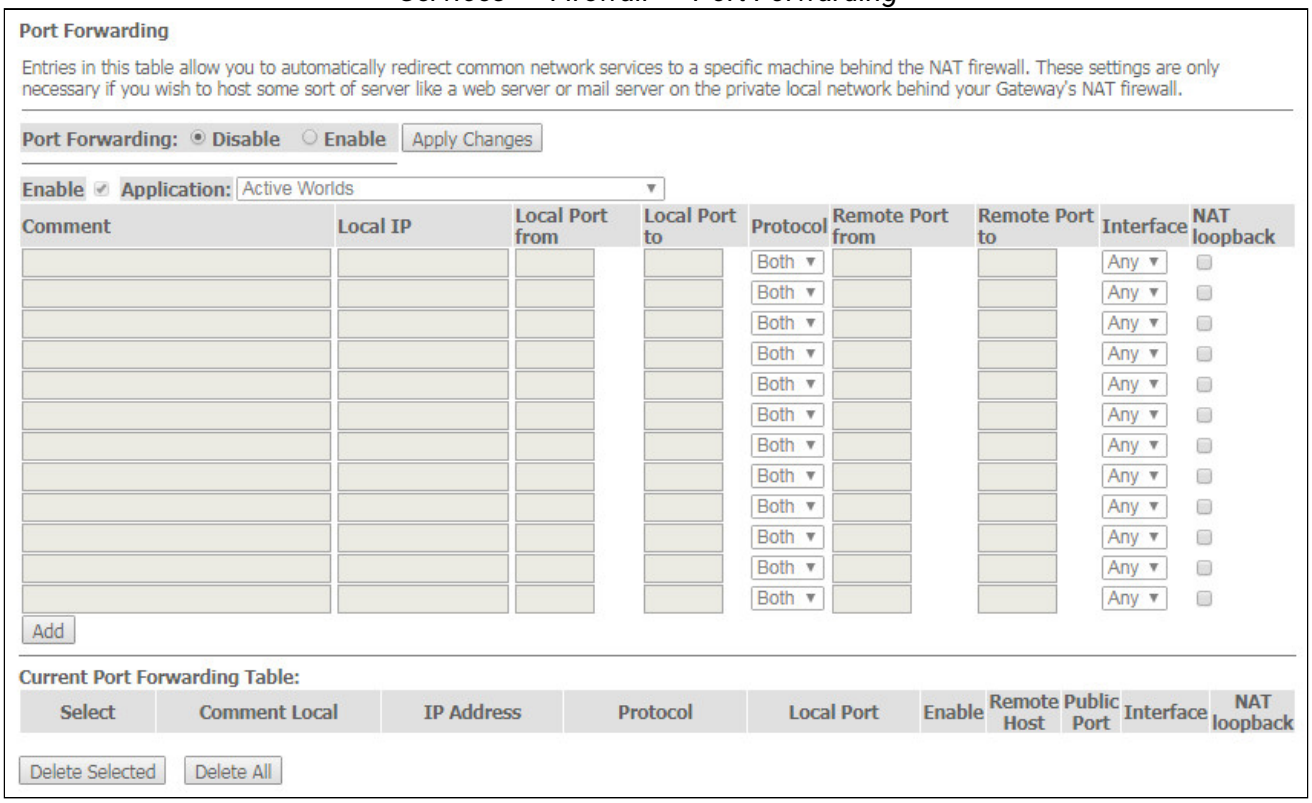
Добавленные фильтры отображаются в ниже расположенной таблице фильтров *«Current Filter Table»*. Поле *«Rule»* отображает тип созданного правила (*«Allow », разрешающее* или *«Deny», запрещающее)* . Для удаления определённой позиции в списке, выделите её и нажмите «Delete Selected», чтобы удалить весь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

4.4.3.4 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



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

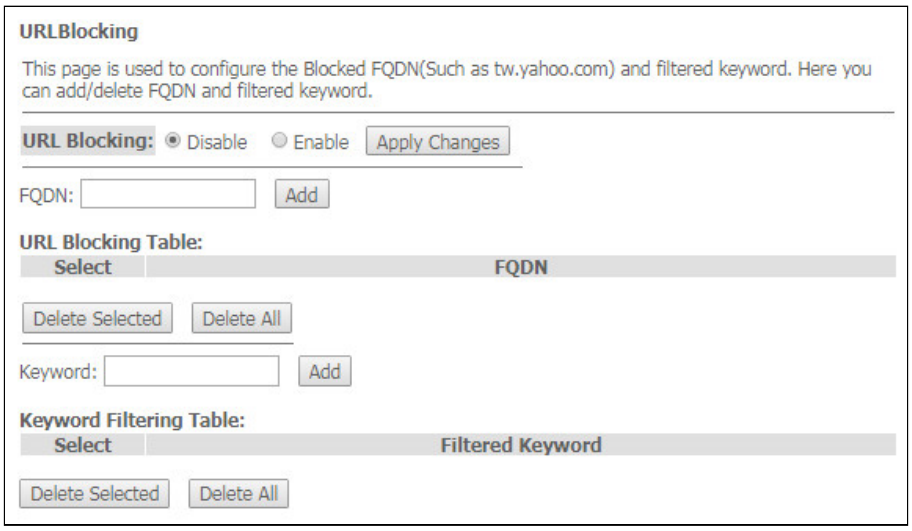
- *Port Forwarding (Enable/Disable)* — включение/выключение функции проброса портов;
- *Application* — в меню имеются предустановки для проброса портов различных приложений;
- *Comment* — комментарий;
- *Local IP* — локальный IP-адрес, на который производится проброс;
- *Local port from / to* — укажите 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».

4.4.3.5 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



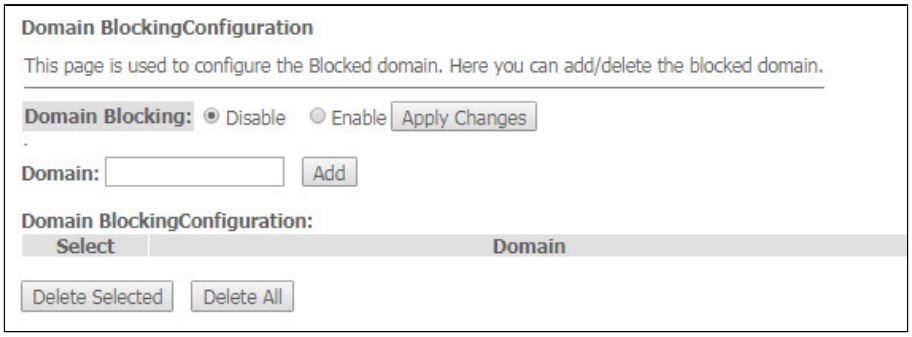
- *URL Blocking (Enable/Disable)* — включение/выключение работы URL-Blocking;
- *FQDN (Fully Qualified Domain Name)* — полное доменное имя;
- *Keyword* — ключевое слово.

Для сохранения изменений нажмите кнопку «Apply Changes».

4.4.3.6 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»

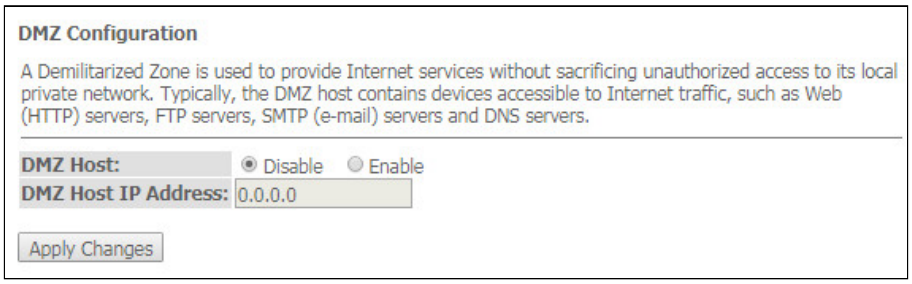
- *Domain Blocking (Enable/Disable)* — включение/выключение блокировки;
- *Domain* — наименование домена.

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

4.4.3.7 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



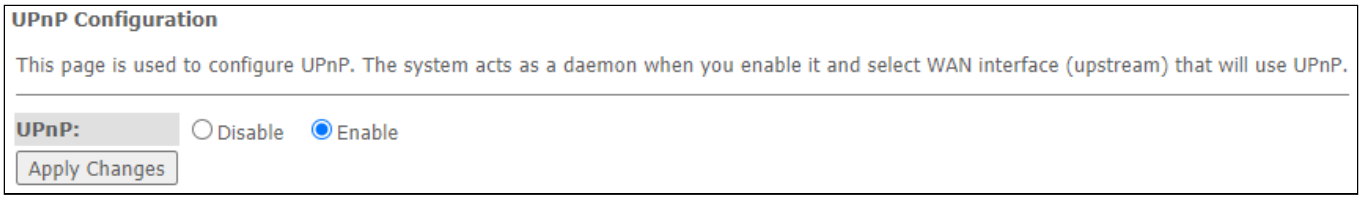
- *DMZ Host (Enable/Disable)* — включение/выключение хоста;
- *DMZ Host IP Address* — IP-адрес.

Для сохранения изменений нажмите кнопку «Apply Changes».

4.4.4 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



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

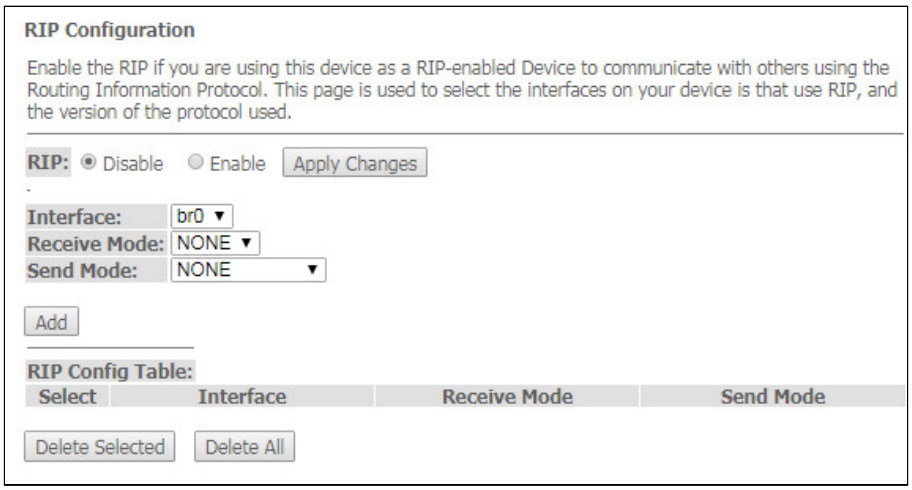
- *UPnP (Enable/Disable)* — включение/выключение функции UPnP;
- *WAN Interface* — WAN интерфейс, на котором будет работать функция UPnP;

Для сохранения настроек нажмите кнопку «Apply Changes».

4.4.5 Подменю «RIP». Настройка динамической маршрутизации

В разделе осуществляется выбор интерфейсов на устройстве, 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 (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).

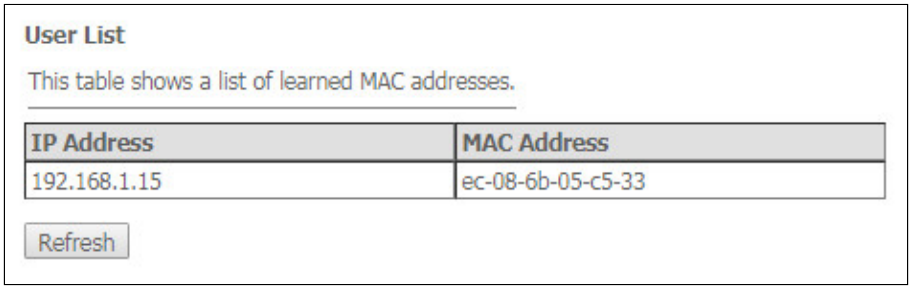
Интерфейсы с поддержкой RIP отображаются в таблице *«RIP Config Table»*. Для удаления всех записей в таблице нажмите кнопку «Delete All», чтобы удалить одну позицию из списка, выделите её и нажмите кнопку «Delete Selected».

4.5 Меню «Advance». Расширенные настройки

4.5.1 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



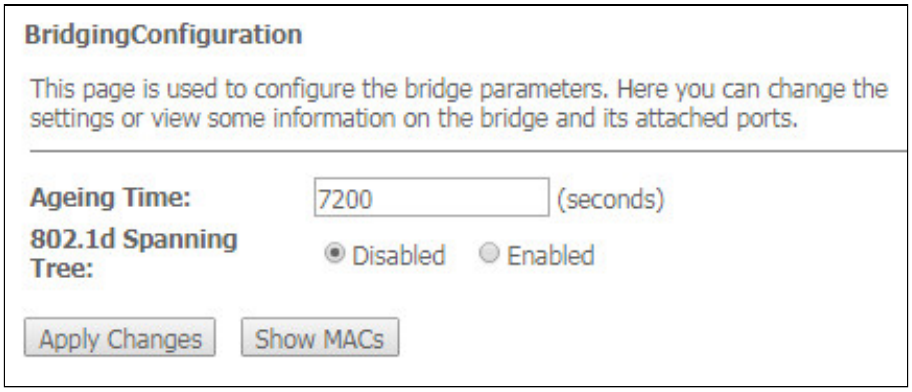
- *IP Address* — IP-адрес клиента;
- *MAC Address* — MAC-адрес клиента.

Для обновления информации в таблице нажмите кнопку «Refresh».

4.5.2 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

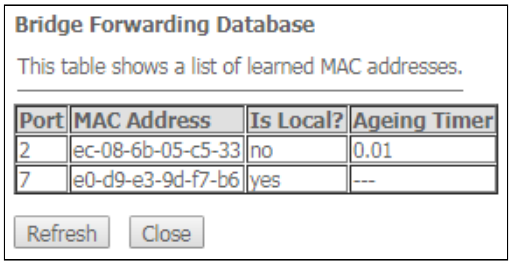


- *Ageing Time* — время жизни адресов (сек);
- *802.1d Spanning Tree (Enable/Disable)* — включение/выключение протокола 802.1d Spanning Tree.

Для сохранения изменений нажмите кнопку «Apply Changes».

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

Advance → Bridging → Show MACs



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	---

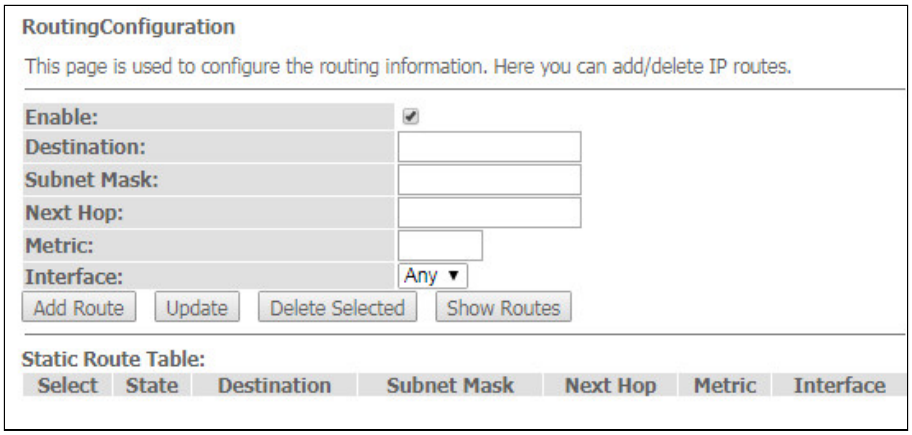
- *Port* — номер порта;
- *MAC Address* — MAC-адрес;
- *Is Local* — локальный адрес;
- *Ageing Timer* — время жизни адреса.

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

4.5.3 Подменю «Routing». Настройка маршрутизации

В разделе осуществляется настройка статической маршрутизации.

Advance → Routing



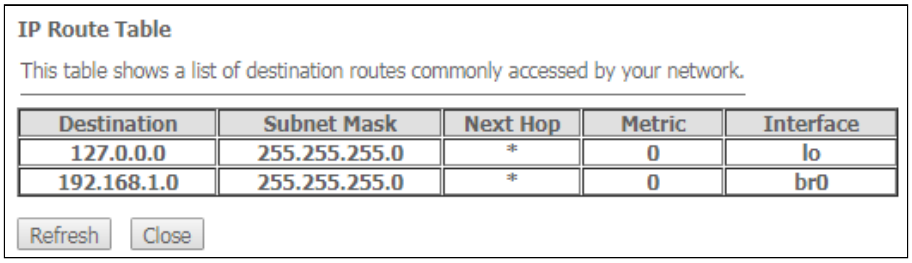
Для добавления статического маршрута поставьте флаг *«Enable»,* заполните соответствующие поля и нажмите на кнопку «Add Route».

- *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



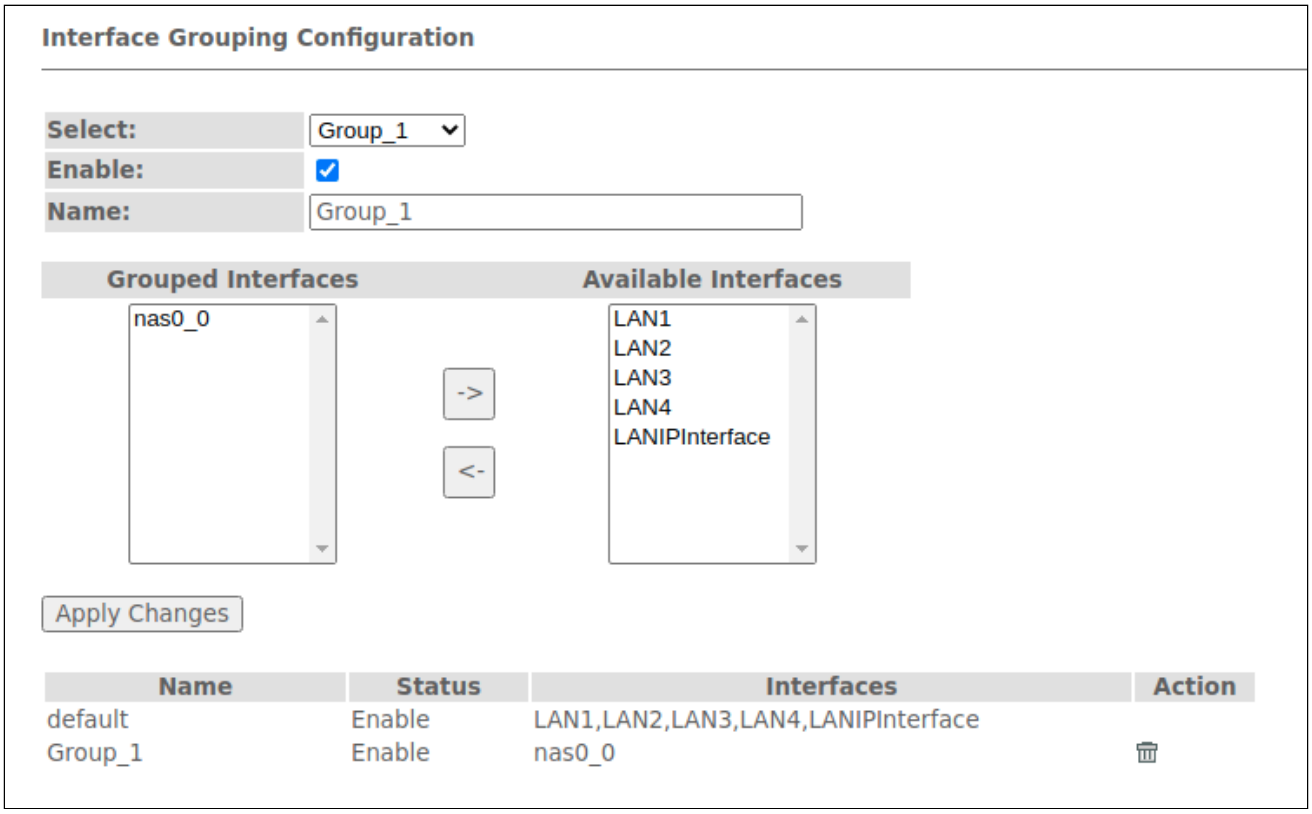
Для обновления информации в таблице нажмите кнопку «Refresh», для закрытия кнопку «Close».

4.5.4 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 группы 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».

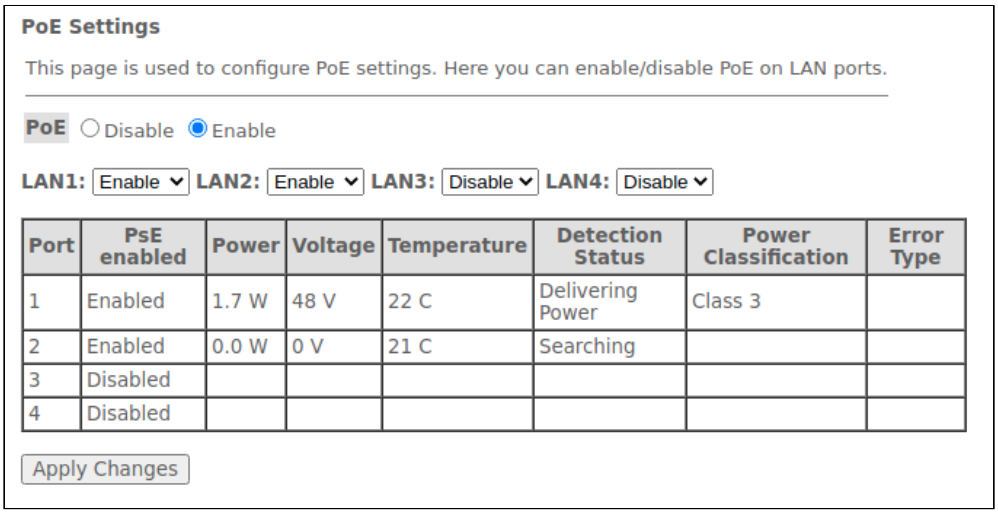
Advance → Interface grouping



4.5.5 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



Для сохранения изменений нажмите кнопку «Apply Changes».

- Port — номер LAN порта (1-4);
- PsE enabled:
  - Enabled — включена поддержка PoE на порту;
  - Disbled — отключена поддержка PoE на порту.
- Power — потребляемая мощность, Вт;

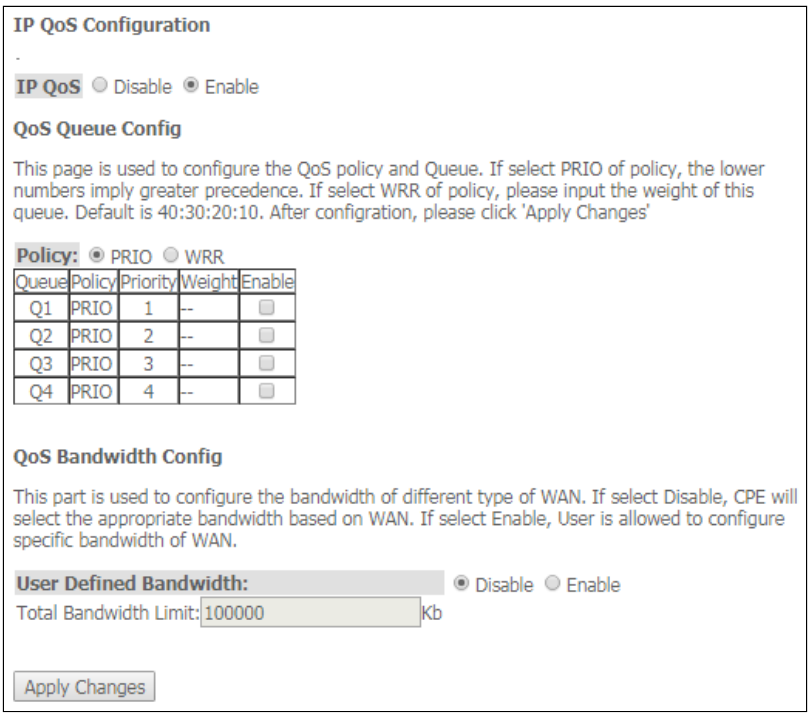
- Voltage — напряжение, В;
- Temperature — температура, С;
- Detection Status — статус PoE порта;
- Power Classification — класс мощности подключенного устройства PoE;
- Error Type — тип ошибки.

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

4.5.6.1 Подменю «QoS Policy». Настройка QoS очередей

В разделе можно настроить политики QoS очереди обработки трафика.

Advance → IP QoS → QoS Policy



- *IP QoS (Enable/Disable)* — включение/выключение конфигурирования QoS очередей;
- *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.

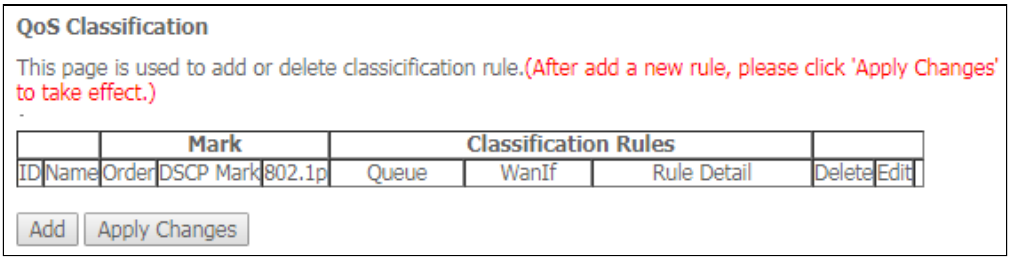
- *User defined Bandwidth (Enable/Disable)* — включить ограничение;
- *Total Bandwidth Limit, (kb)* — ограничение полосы, кб.

Для сохранения изменений нажмите кнопку «Apply Changes».

4.5.6.2 Подменю «QoS Classification». Настройка правил классификации трафика

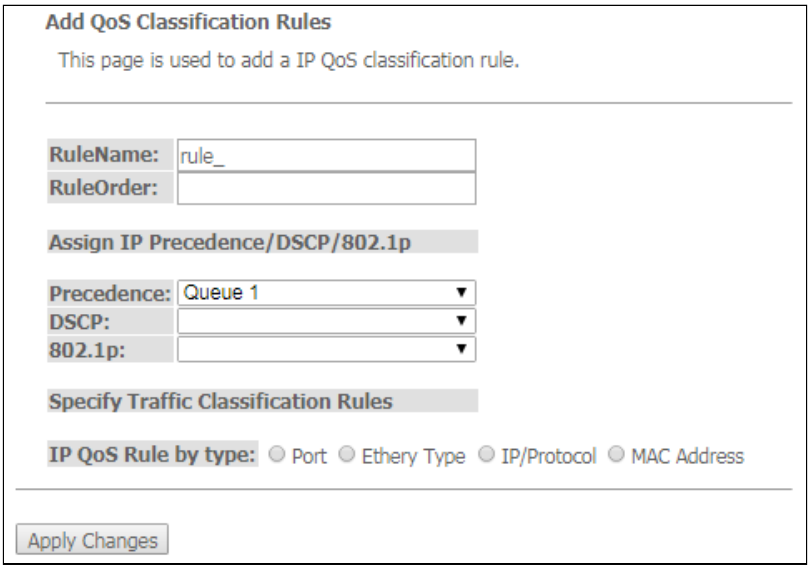
На данной странице можно указать по каким полям и их значениям будет классифицироваться пакет, а так же в какую аппаратную очередь он в итоге попадет.

Advance → IP QoS → QoS Classification



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

Advance → IP QoS → QoS Classification → Add



- *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.

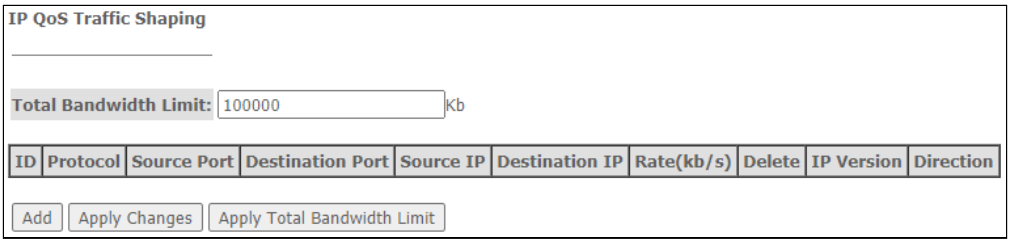
- *IP QoS Rule by type* — выбор правила классификации по типу:
  - *Port* — по порту;
  - *Ethery Type* — по Ethertype;
  - *IP/Protocol* — по протоколу IP;
  - *MAC Address* — по MAC-адресу.

Для сохранения изменений нажмите кнопку «Apply Changes».

4.5.6.3 Подменю «Traffic Shaping». Настройка трафика

В данном разделе можно указать ограничения трафика по определенным правилам.

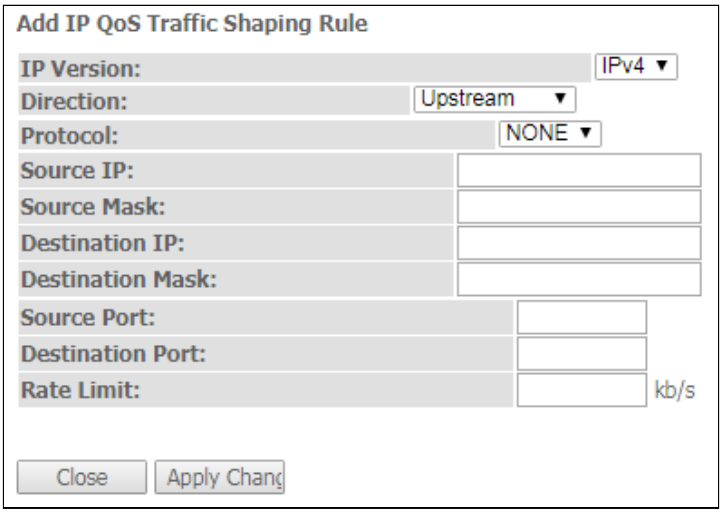
Advance → IP QoS → Traffic Shaping



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

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

Advance → IP QoS → Traffic Shaping → Add



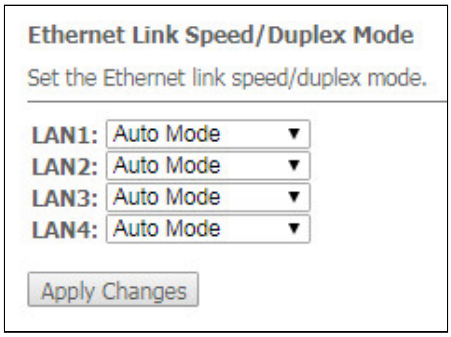
- *IP Version* — выбор IP-версии;
- *Direction* — выбор типа потока, нисходящий или восходящий;
- *Protocol* — протокол;
- *Source IP* — IP-адрес источника;
- *Source Mask* — маска подсети источника;
- *Destination IP* — IP-адрес назначения;
- *Destination Mask* — маска подсети назначения;
- *Source 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 «Close».

4.5.7 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

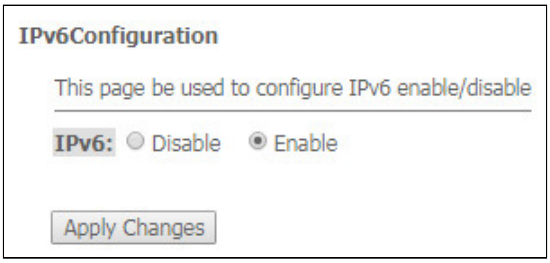


Для сохранения изменений нажмите кнопку «Apply Changes»

4.5.8 Подменю «IPv6». Настройка протокола IPv6

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

Advance → IPv6

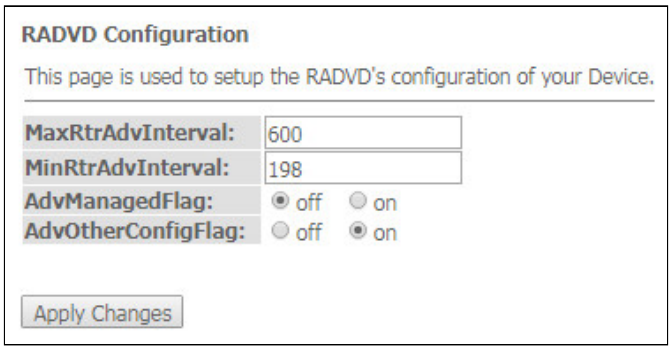


Для сохранения изменений нажмите кнопку «Apply Changes».

4.5.8.1 Подменю «RADVD». Настройка RADVD

В разделе осуществляется настройка RADVD (Router Advertisement Daemon).

Advance → IPv6 → RADVD



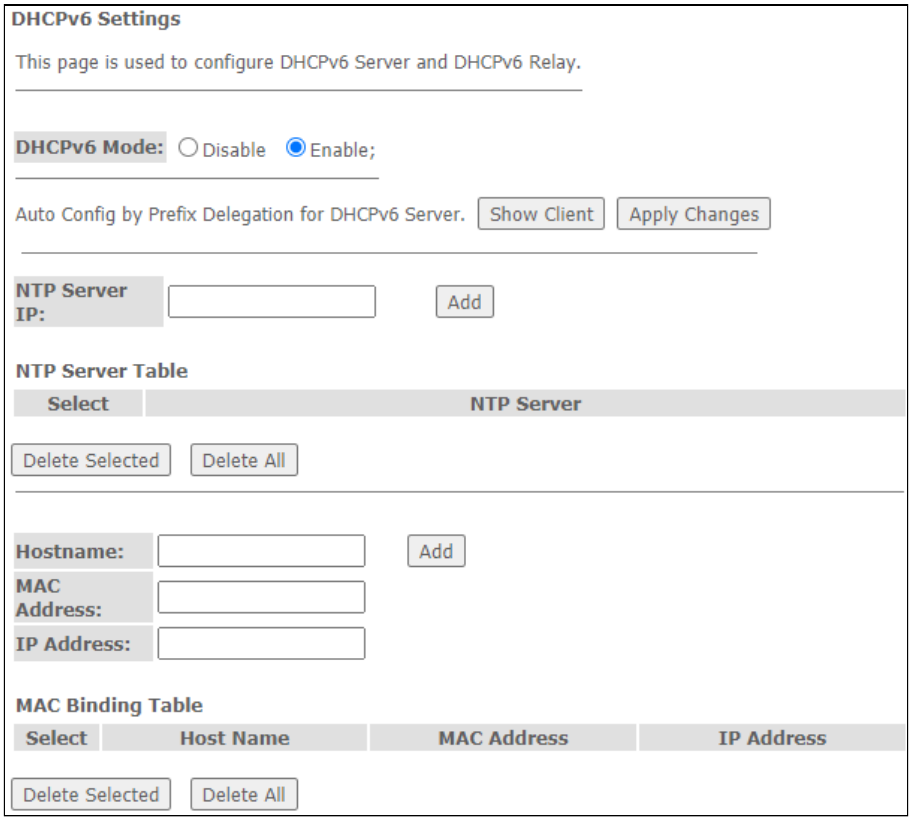
- *MaxRtrAdvInterval* — максимальный интервал отправки RA (Router Advertisement);
- *MinRtrAdvInterval* — минимальный интервал отправки RA;
- *AdvManagedFlag* — включение/выключение отправки флага Managed в RA;
- *AdvOtherFlag* — включение/выключение отправки флага Other RA.

Для сохранения изменений нажмите кнопку «Apply Changes».

4.5.8.2 Подменю «DHCPv6». Настройка DHCPv6-сервера

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

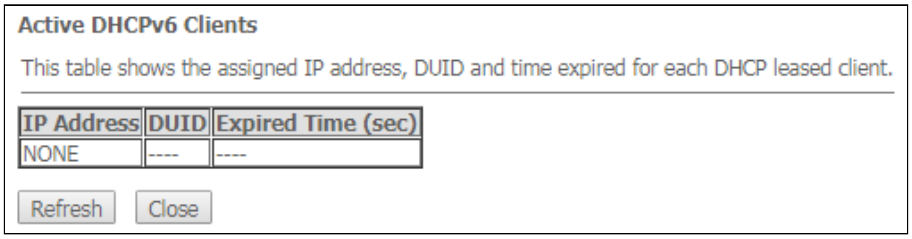
Advance → IPv6 → DHCPv6



- *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.

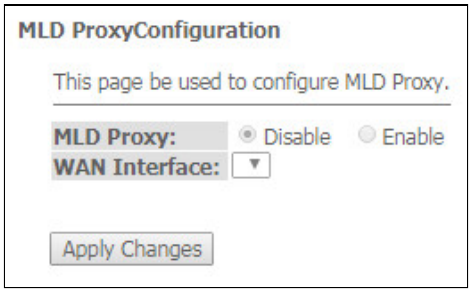
Advance → IPv6 → DHCPv6 → Show Client



4.5.8.3 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

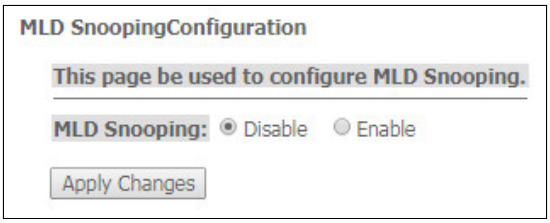


Для сохранения изменений нажмите кнопку «Apply Changes».

4.5.8.4 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

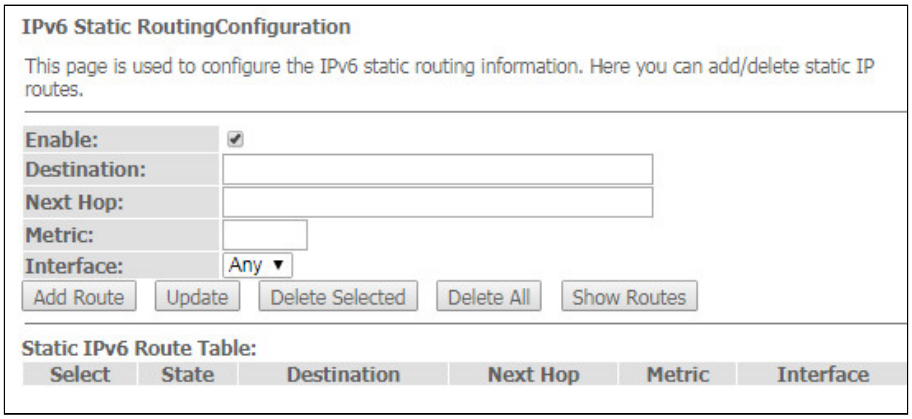


Для сохранения изменений нажмите кнопку «Apply Changes».

4.5.8.5 Подменю «IPv6 routing». Настройка IPv6 маршрутов

В разделе осуществляется настройка статических IPv6 маршрутов.

Advance → IPv6 → IPv6 routing



- *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 выберете 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

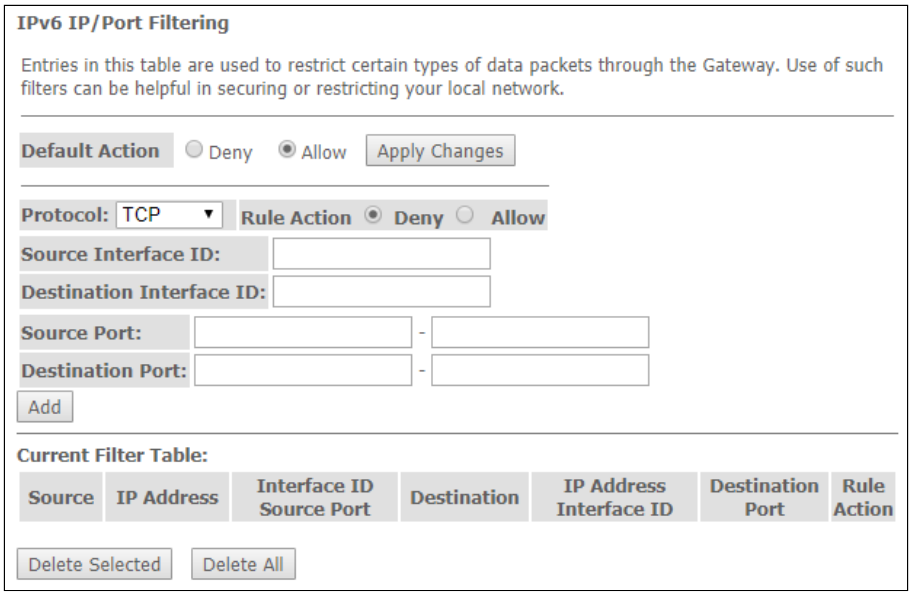
- *Destination* — сеть назначение;
- *Next Hop* — следующий узел;
- *Flags* — флаги;
- *Metric* — метрика;
- *Ref* — источник маршрута;
- *Use* — использование маршрута;
- *Interface* — интерфейс, через который доступен указанный маршрут.

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

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

На странице осуществляется настройка фильтрации пакетов данных передаваемых через шлюз.

Advance → IPv6 → IP/Port filtering



- *Default Action* — действие по умолчанию:
  - *Deny* — при установке флага прохождение трафика по-умолчанию запрещено;
  - *Allow* — при установке флага прохождение трафика по-умолчанию разрешено;
- *Protocol* — выбор протокол;
- *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 выберете его и нажмите кнопку «Delete Selected».

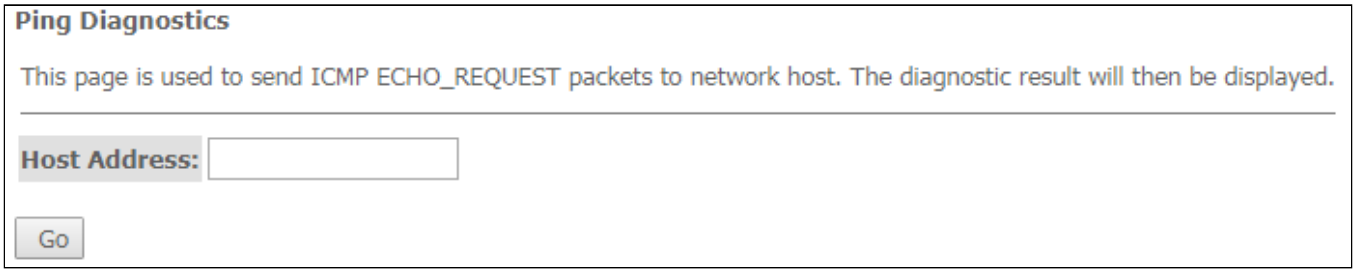
4.6 Подменю «Diagnostics»

Раздел диагностики доступа к различным сетевым узлам.

4.6.1 Подменю «Ping». Проверка доступности сетевых устройств

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

Diagnostics → Ping

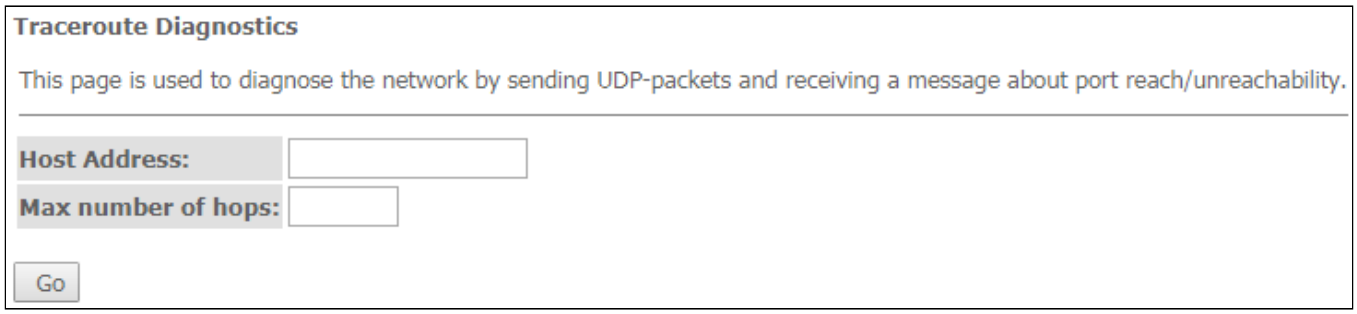


Для проверки доступности подключенного устройства необходимо ввести его IP-адрес в поле *«Host Address»* и нажать кнопку «Go».

4.6.2 Подменю «Traceroute»

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

Diagnostics → Traceroute

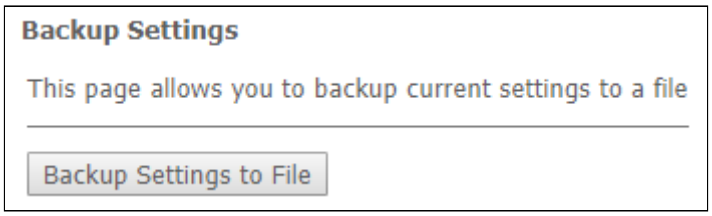


4.7 Подменю «Admin»

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

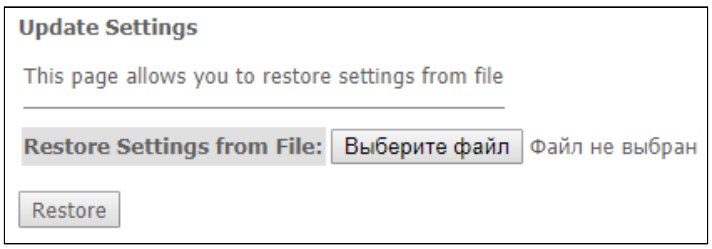
4.7.1 Подменю «Settings». Восстановление и сброс настроек

Admin → Settings → Backup Settings



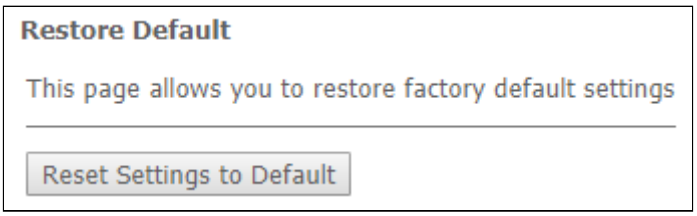
В разделе можно скопировать текущие настройки в файл (*Backup Settings)* нажатием на кнопку «Backup Settings to File».

Admin → Settings → Update Settings



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

Admin → Settings → Restore Default

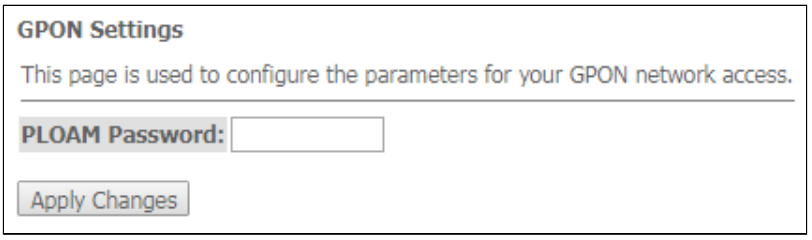


В разделе можно сбросить текущие настройки до заводских настроек по умолчанию (*Restore Default)* нажмите кнопку «Reset Settings to Default».

4.7.2 Подменю «GPON Setting». Настройка доступа к GPON

В разделе можно указать пароль для активации терминала на OLT.

Admin → GPON Setting



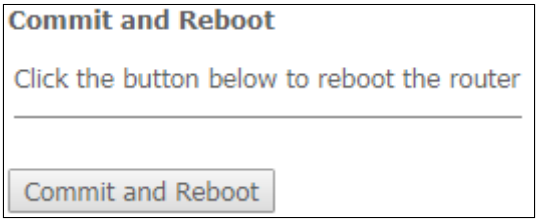
- *PLOAM Password* — пароль для активации терминала на OLT.

Для сохранения изменений нажмите кнопку «Apply Changes».

4.7.3 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.

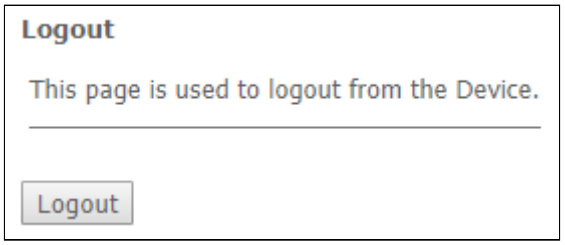
Admin → Commit/Reboot



4.7.4 Подменю «Logout». Выход из учетной записи

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

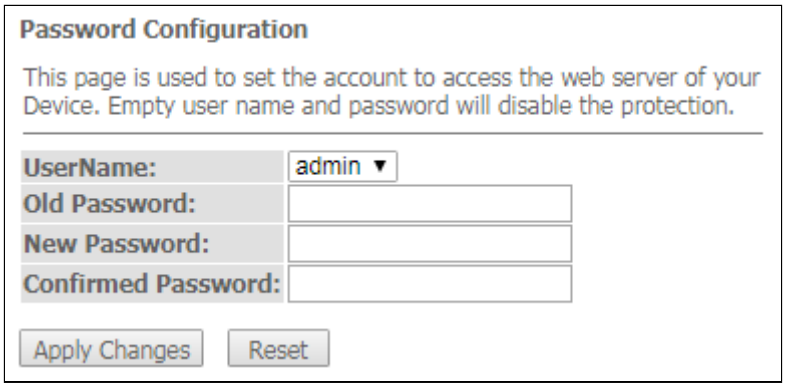
Admin → Logout



4.7.5 Подменю «Password». Настройка контроля доступа (установление паролей)

В разделе осуществляется смена пароля для доступа к устройству.

Admin → Password



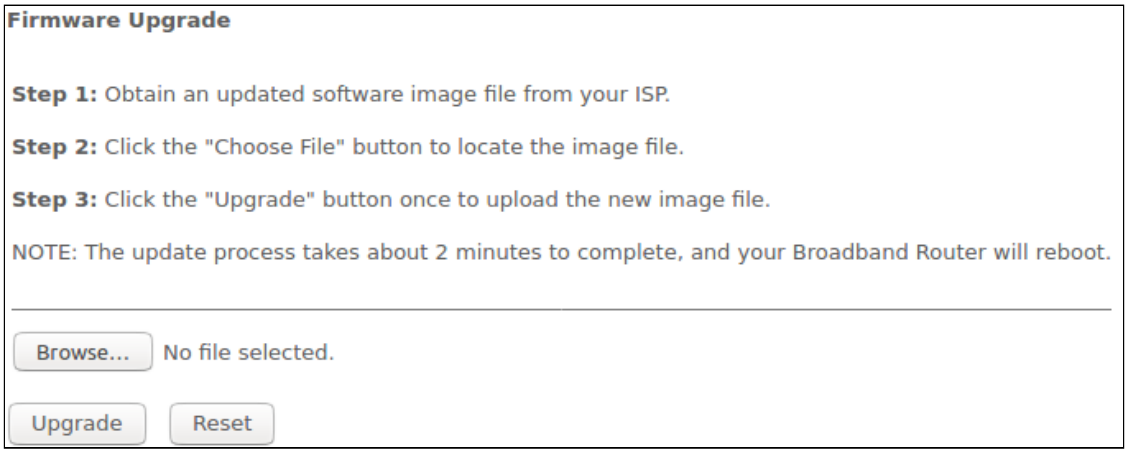
Для смены пароля необходимо ввести существующий пароль в поле *Old Password*, затем новый пароль в *New Password* и подтвердить его *Confirmed Password*.

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

4.7.6 Подменю «Firmware upgrade». Обновление ПО

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

Admin → Firmware upgrade

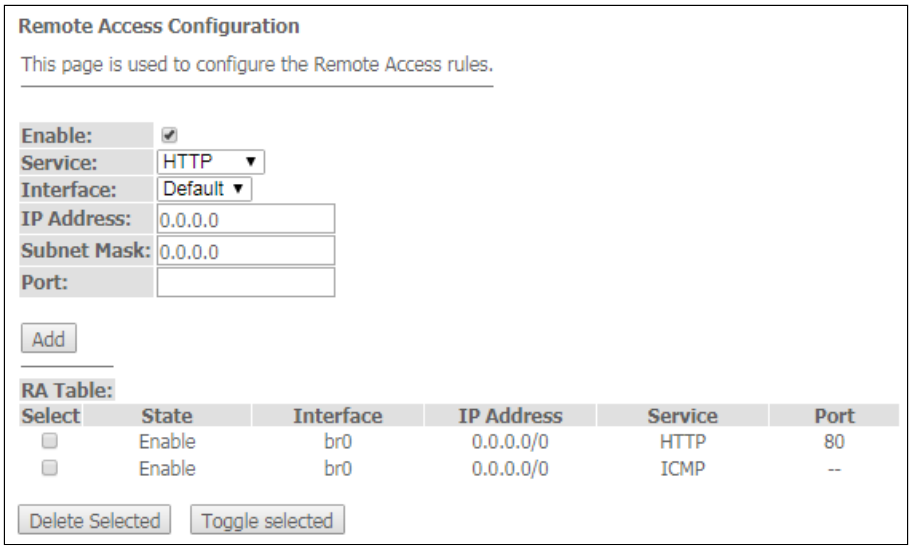


В процессе обновления не допускается отключение питания устройства, либо его перезагрузка. Процесс обновления может занимать несколько минут, после чего устройство автоматически перезагружается.

4.7.7 Подменю «Remote Access». Настройка правил удалённого доступа

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

Admin → Remote Access



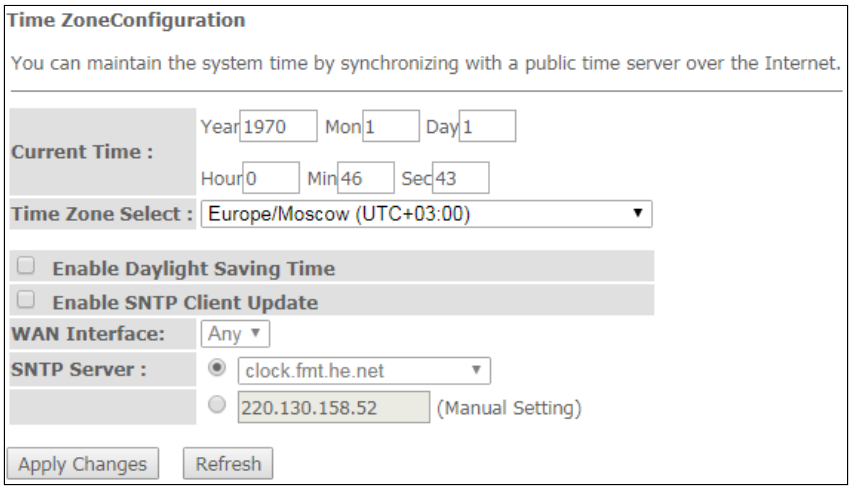
- Enable — включение правила для добавления;
- Service — выбор используемого протокола;
- Interface — интерфейс, к которому применяется правило;
- IP Address — IP-адрес источника;
- Subnet Mask — маска подсети;
- Port — порт назначения.

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 выберете его флагом в столбце *Select* и нажмите кнопку «Delete Selected».

4.7.8 Подменю «Time zone». Настройки системного времени

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

Admin → Time zone



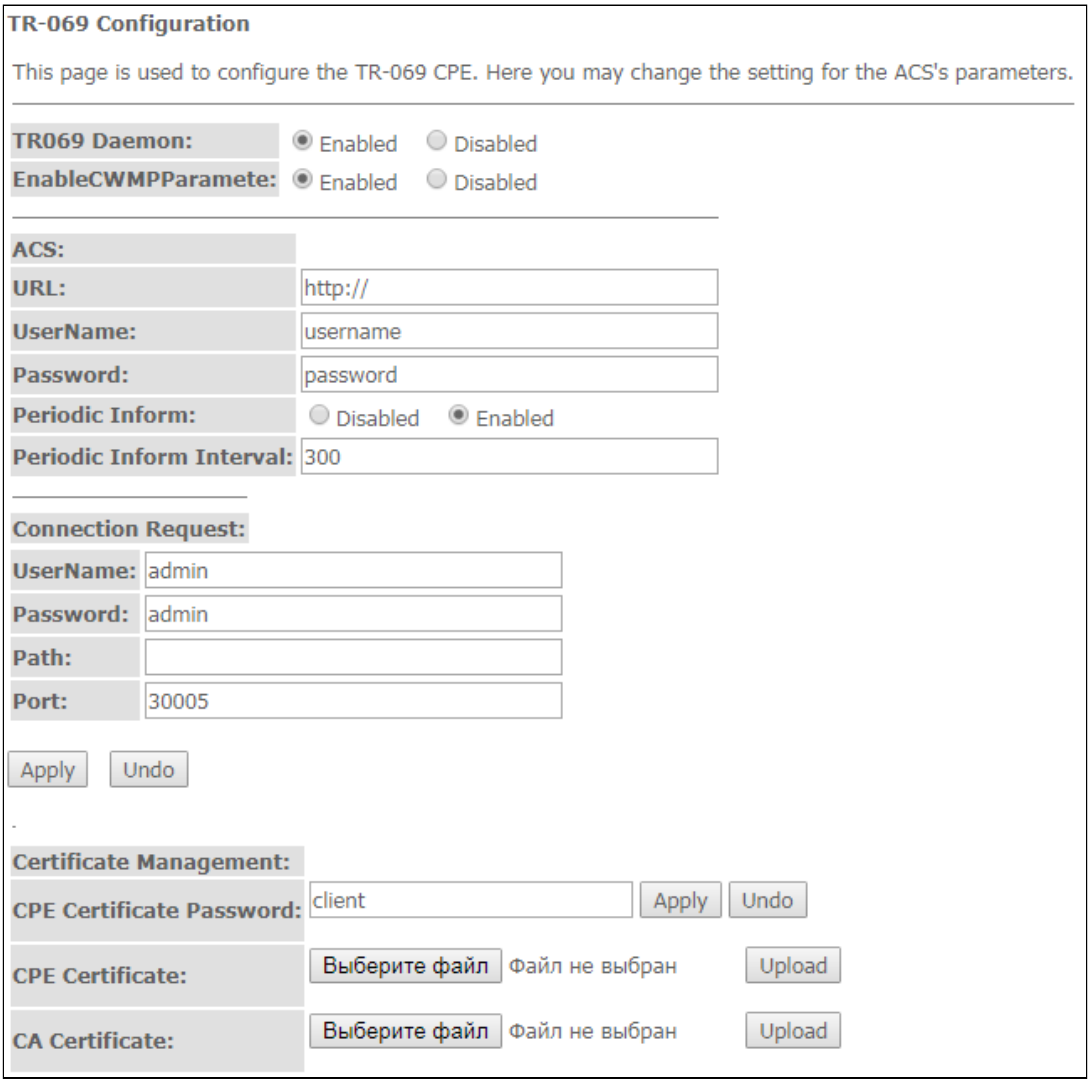
- *Current time* — текущее время;
- *Time Zone Select* — временная зона;
- *Enable Daylight Saving Time* — переход на летнее время;
- *Enable SNTP Client Update* — включить синхронизацию времени по SNTP;
- *WAN Interface* — интерфейс, через который производится обновление времени;
- *SNTP Server* — предпочитаемый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

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

4.7.9 Подменю «TR-069». Настройка TR-069

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

Admin → TR-069



- *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;
- *Enable CWMP WAN ACL* — при установленном флаге *Desable* WAN ACL будет убран в релизе;
- *IP Adress* — IP-адрес;
- *Subnet Mask* — маска подсети.

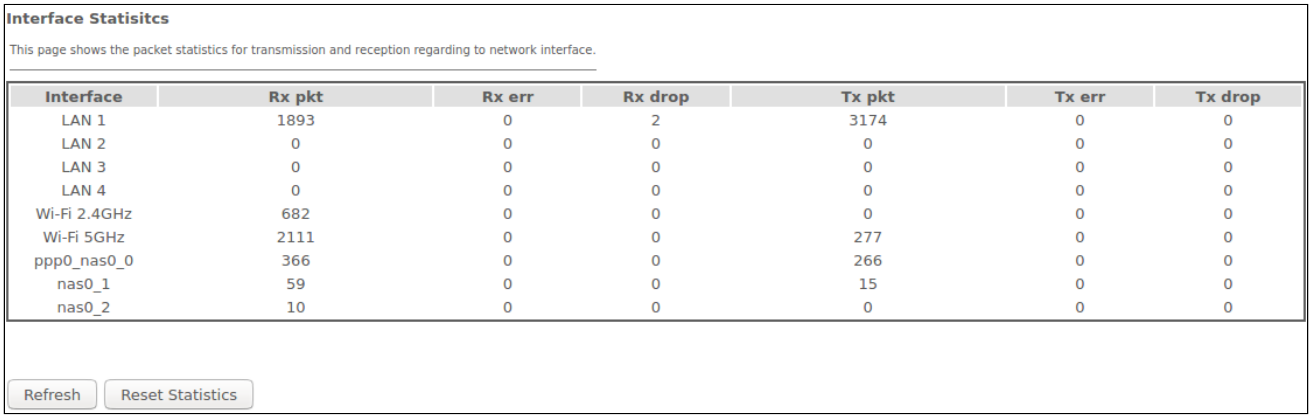
Для сохранения изменений нажмите кнопку «Apply», для сброса «Undo». Чтобы загрузить выбранный файл нажмите кнопку «Upload».

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

4.8.1 Подменю «Interface». Информация о счетчиках и ошибках

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

Statistics → Interface



Interface Statisitcs

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.

4.8.2 Подменю «PON»

В разделе отображается счетчики для оптического интерфейса:

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

- *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
- *Packets Dropped* — пакетов отброшено.

5 Список изменений

Версия документа	Актуальность для ПО	Дата выпуска	Содержание изменений
Версия 1.0	1.0.1	04.2021	Первая публикация