Абонентский оптический терминал

NTU-52W

Руководство по эксплуатации
Версия ПО 3.0.3

IP-адрес: 192.168.1.1

Username: user

Password: user

Содержание

1 Введение

Технология PON — одна из самых современных и высокоэффективных технологий «последней мили», позволяющая существенно экономить на кабельной инфраструктуре и обеспечивающая скорость передачи данных до 2,5 Гбит/с в направлении downlink и 1,25 Гбит/с в направлении uplink. Использование в сетях доступа решений на базе технологии PON дает возможность предоставлять конечному пользователю доступ к набору услуг на базе протокола IP.

Преимуществом технологии GPON является оптимальное использование полосы пропускания. Эта технология является следующим шагом для обеспечения новых высокоскоростных, интернет-приложений в доме и 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.

В настоящем руководстве по эксплуатации изложены назначение, основные технические характеристики, правила конфигурирования, мониторинга и смены программного обеспечения абонентского терминала NTU-52W.

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, принести к некорректной работе устройства или потере данных.

2 Описание изделия

2.1 Назначение

Устройство NTU-52W — высокопроизводительный многофункциональный абонентский терминал. Благодаря встроенному маршрутизатору терминал обеспечивает возможность подключения оборудования локальной сети к вышестоящему оборудованию пассивных оптических сетей и предоставление услуг широкополосного доступа конечному пользователю. Связь с сетями GPON реализуется посредством PON-интерфейса, для подключения оконечного оборудования клиентов служат интерфейсы Ethernet.

Терминал NTU-52W дает операторам возможность предоставлять клиентам доступ к IPTV, OTT и высокоскоростному Интернету. NTU-52W позволяет подключать клиентов Wi-Fi по стандарту IEEE 802.11b/g/n.

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):
  - 1 порт RJ-45 10/100BASE-T (подробнее смотрите в разделе Конструктивное исполнение);
  - 1 порт RJ-45 10/100/1000BASE-T (подробнее смотрите в разделе Конструктивное исполнение).
- Приемопередатчик Wi-Fi 802.11b/g/n.

Питание терминала осуществляется через внешний адаптер от сети 220 В/12 В.

Устройство поддерживает следующие функции:

- *сетевые функции:*
  - поддержка TR-069;
  - поддержка работы в режиме «моста» или «маршрутизатора», в том числе виртуального;
  - поддержка PPPoE (auto, PAP-, CHAP-, MSCHAP-авторизация);
  - поддержка IPoE (DHCP-client и static);
  - поддержка статического адреса и DHCP (DHCP-клиент на стороне WAN, DHCP-сервер на стороне LAN);
  - поддержка передачи Multicast-трафика по Wi-Fi;
  - поддержка DNS (Domain Name System);
  - поддержка DynDNS (Dynamic DNS);
  - поддержка UPnP (Universal Plug and Play);
  - поддержка NAT (Network Address Translation);
  - поддержка NTP (Network Time Protocol);
  - поддержка механизмов качества обслуживания QoS;
  - поддержка IGMP-snooping;
  - поддержка IGMP-proxy;
  - поддержка Firewall;
  - VLAN в соответствии с IEEE 802.1Q.
- *Wi-Fi:*
  - поддержка стандартов 802.11b/g/n.
- *обновление ПО через web-интерфейс, TR-069, OMCI;*

- *удаленный мониторинг, конфигурирование и настройка*:
  - TR-069;
  - web-интерфейс;
  - CLI;
  - OMCI.

На рисунке ниже приведена схема применения оборудования NTU-52W.

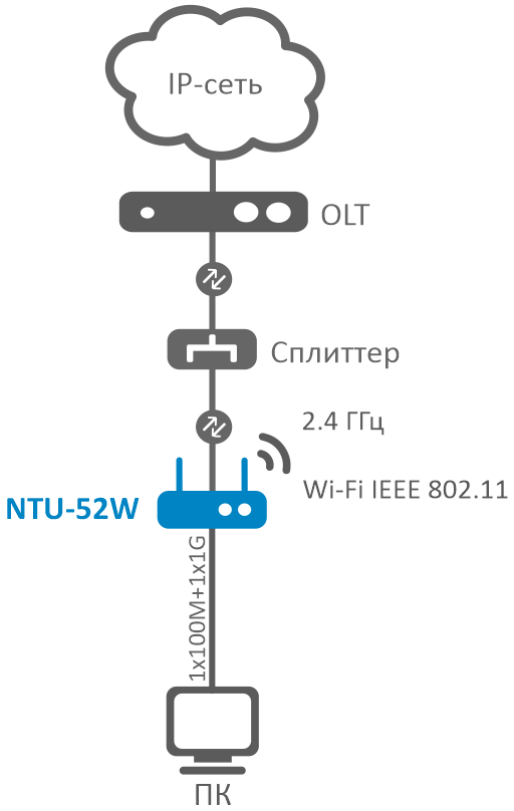


Рисунок 1 − Схема применения NTU-52W

2.3 Основные технические параметры

Основные технические параметры терминалов приведены в таблице 1.

Таблица 1 – Основные технические параметры

Параметры интерфейсов Ethernet LAN

Количество интерфейсов	2
Электрический разъем	1 порт 10/100BASE-T (RJ-45) 1 порт 10/100/1000BASE-T (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

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) IEEE 802.1Q Tagged VLAN (следующие VLAN используются для внутренней работы устройства и не могут быть использованы для создания WAN-сервисов: 0, 4032, 4022, 4023, 4024, 4027, 4026, 4000~4005, 4095) 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 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≤1.0x10^{-10}
Оптическая перегрузка приемника	-8 дБм

Параметры беспроводного интерфейса Wi-Fi

Стандарт	IEEE 802.11b/g/n
Частотный диапазон	2,400 ~ 2.483,5 МГц
Модуляция	DQPSK, DBPSK, CCK, BPSK, QPSK, 16QAM, 64QAM, OFDM
Скорость беспроводного соединения	**802.11b**: 1, 2, 5.5 и 11 Мбит/с **802.11g:** 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с **802.11n**: от 6,5 до 300 Мбит/с (от MCS0 до MCS15)
Максимальная выходная мощность передатчика	**802.11b (11 Мбит/с)**: 18 дБм **802.11g (54 Мбит/с)**: 16 дБм **802.11n (MCS7)**: 16 дБм **802.11n (MCS0)**: 18 дБм
MAC-протокол	CSMA/CA-модель ACK 32 MAC
Безопасность	64/128-битное WEP-шифрование данных; WPA, WPA2, WPA3, WPA3 Mixed; 802.1x; AES &TKIP
Количество антенн	2
Коэффициент усиления антенны	5 дБи

Управление

Локальное управление	web-интерфейс
Удаленное управление	Telnet, TR-069, CLI, OMCI
Обновление программного обеспечения	OMCI, TR-069, HTTP
Ограничение доступа	по паролю

Общие параметры

Питание	адаптер питания 12 В, 0,5 А
Потребляемая мощность	не более 6 Вт
Рабочий диапазон температур	от +5 до +40 °C
Относительная влажность	до 80 %
Габариты (Ш × В × Г)	147 × 24 × 110 мм
Масса	0,25 кг
Срок службы	не менее 5 лет

3 Конструктивное исполнение

Абонентский терминал выполнен в виде настольного изделия в пластиковом корпусе, размеры которого соответствуют 147 × 24 × 110 мм.

Внешний вид задней панели устройства NTU-52W приведен на рисунке 2.

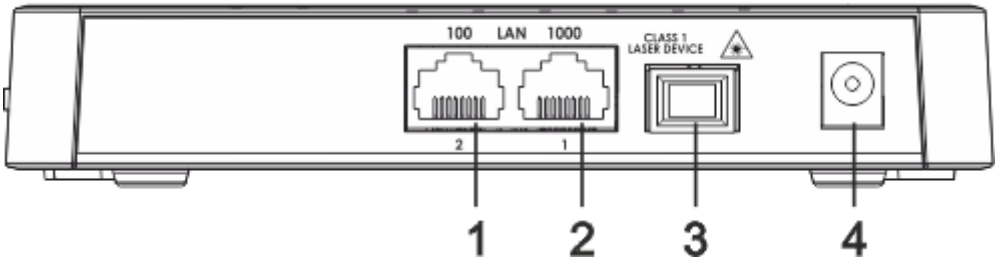


Рисунок 2 – Внешний вид задней панели NTU-52W

На задней панели NTU-52W расположены следующие разъемы и органы управления, таблица 2.

Таблица 2 – Описание разъемов и органов управления задней панели NTU-52W

№	Элемент задней панели	Описание
1	***LAN 10/100***	Разъем RJ-45 10/100BASE-T для подключения сетевых устройств
2	***LAN 10/100/1000***	Разъем RJ-45 10/100/1000BASE-T для подключения сетевых устройств
3	***PON***	Разъем SC (розетка) PON оптического интерфейса GPON
4	***12V***	Разъем для подключения адаптера питания

Внешний вид боковой панели NTU-52W приведен на рисунке 3.

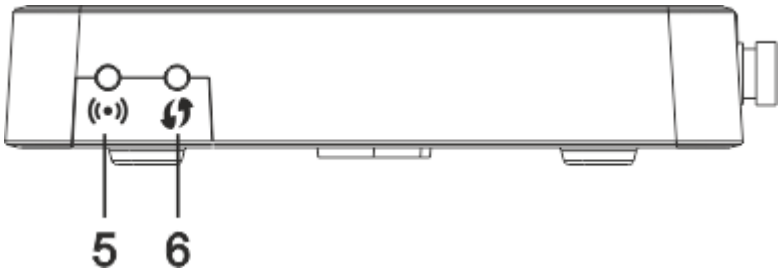


Рисунок 3 – Внешний вид боковой панели NTU-52W

На боковой панели устройства расположены следующие кнопки, таблица 3.

Таблица 3 – Описание кнопок боковой панели NTU-52W

№	Элемент боковой панели	Описание
5		Кнопка включения/выключения Wi-Fi

№	Элемент боковой панели	Описание
6		Кнопка для автоматического защищенного подключения к сети Wi-Fi на устройстве

3.1 Световая индикация

Внешний вид передней панели NTU-52W на рисунке 4.

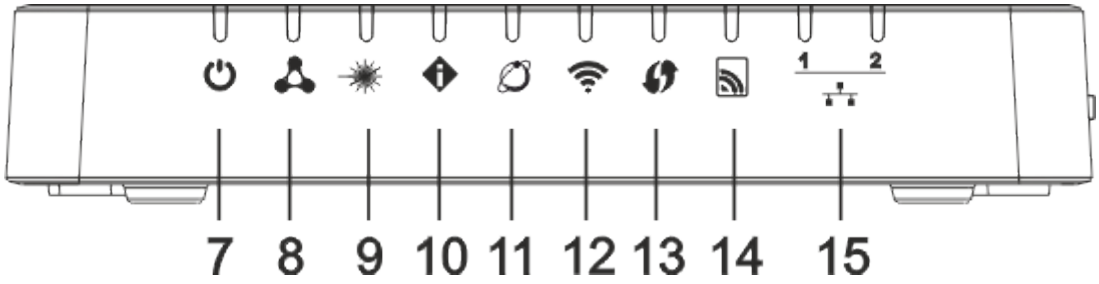


Рисунок 4 – Внешний вид передней панели NTU-52W

Текущее состояние устройства отображается при помощи индикаторов, расположенных на верхней панели. Перечень состояний индикаторов приведен в таблице 4.

Таблица 4 – Описание индикаторов передней и верхней панели NTU-52W

№	Элемент передней и верхней панелей	Состояние индикатора	Описание
7	***– индикатор питания***	не горит	Устройство отключено от сети питания или неисправно
		зеленый	Питание подключено
8	***– индикатор статуса конфигурации и ПО устройства***	оранжевый	Установлена конфигурация по умолчанию
		зеленый	Конфигурация, отличная от конфигурации по умолчанию
		мигает зеленый	Идет процесс обновления ПО
9	***– индикатор работы оптического интерфейса***	не горит	Не подключена оптика/лазер отключен со стороны OLT
		зеленый	Устройство подключено и зарегистрировано на OLT
		мигает зеленый	Устройство в процессе регистрации на OLT
10	***– индикатор ошибок оптического интерфейса***	не горит	Устройство подключено и зарегистрировано на OLT
		красный	Оптика не подключена
		мигает красный	Лазер отключен со стороны OLT

№	Элемент передней и верхней панелей	Состояние индикатора	Описание
11	***– индикатор подключения к сети Интернет***	не горит	Отсутствует IP-адрес на WAN-соединении
		зеленый	Получен IP-адрес на WAN-соединении
		мигает зеленый	Устройство в процессе подключения
12	***– индикатор активности Wi-Fi***	не горит	Wi-Fi отключен
		зеленый	Wi-Fi включен
		мигает зеленый	Идет передача данных по Wi-Fi
13	***– индикатор работы WPS***	мигает зеленый	Устройство ожидает подключения по WPS
14	***– индикатор наличия клиентов Wi-Fi***	не горит	Нет подключенных клиентов
		горит	Подключен хотя бы один клиент
15	***– 1..2 – индикаторы работы Ethernet-портов***	не горит	Кабель не подключен
		зеленый	Установлено соединение 10/100 Мбит/с
		оранжевый	Установлено соединение 1000 Мбит/с
		мигает зеленый/ оранжевый	Процесс пакетной передачи данных

Перезагрузка/сброс к заводским настройкам

Для перезагрузки устройства нужно однократно нажать кнопку *«F»* на нижней панели устройства. Для загрузки устройства с заводскими настройками необходимо нажать и удерживать кнопку *«F»* в течение 5 секунд, затем отпустить. Устройство перезагрузится. При заводских установках IP-адрес: *LAN – 192.168.1.1,* маска подсети – *255.255.255.0.* Доступ возможен с портов LAN 1 и LAN 2.

3.2 Комплект поставки

В базовый комплект поставки устройства NTU-52W входят:

- Абонентский терминал NTU-52W;
- Адаптер питания 220/12 В 0,5 А;
- Руководство по установке и первичной настройке;
- Памятка о документации.

4 Архитектура устройства

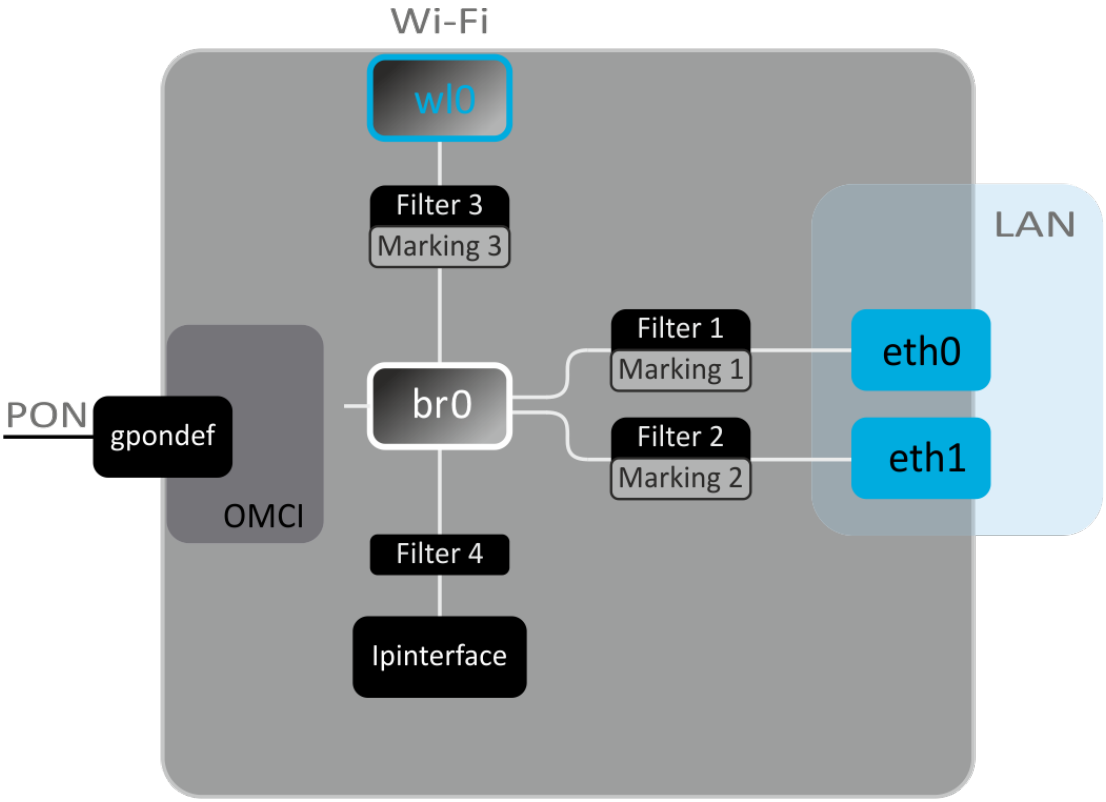


Рисунок 5 – Логическая архитектура устройства с заводской конфигурацией

Основные элементы устройства:

- **Оптический приемо-передатчик (SFF-модуль)** – предназначен для преобразования оптического сигнала в электрический;
- **Процессор (PON-чип)** – является конвертором интерфейсов Ethernet и GPON;
- **Модуль Wi-Fi** – предназначен для организации беспроводных интерфейсов на устройстве.

При заводской (начальной) конфигурации в устройстве присутствуют следующие логические блоки (рисунок 5):

- Br0;
- eth0…1;
- wl0;
- IPInterface1.

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

Блоки eth0..1 физически являются Ethernet-портами с разъемом RJ-45 для подключения ПК, STB или других сетевых устройств. Логически включены в блок **br0**.

Блок wl0 – интерфейс для подключения модуля Wi-Fi в диапазоне 2.4 ГГц.

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

5 Настройка устройств через web-интерфейс. Доступ пользователя

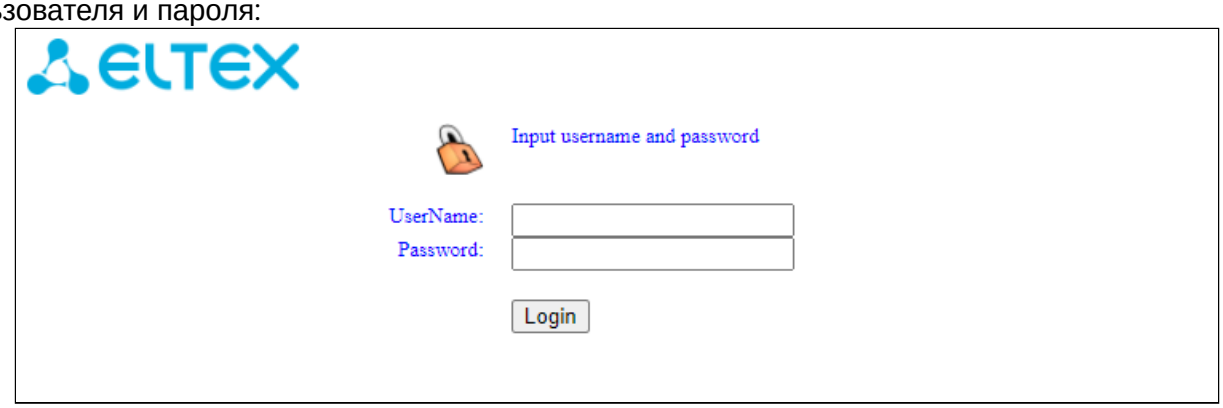
Начало работы

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: *192.168.1.1*, маска подсети: *255.255.255.0*

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



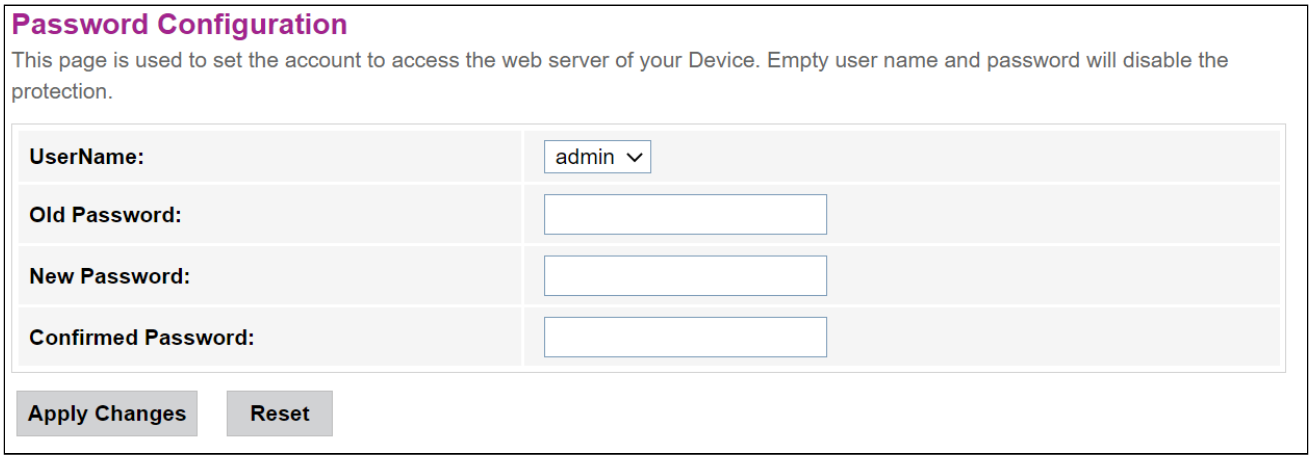
3. Введите имя пользователя в строке «UserName» и пароль в строке «Password».

   Имя пользователя *user*, пароль *user*.

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 полях «New Password» и «Confirmed password» введите новый пароль.



Элементы web-интерфейса

Ниже представлен общий вид окна конфигурирования устройства.

Окно пользовательского интерфейса можно условно разделить на 3 части:

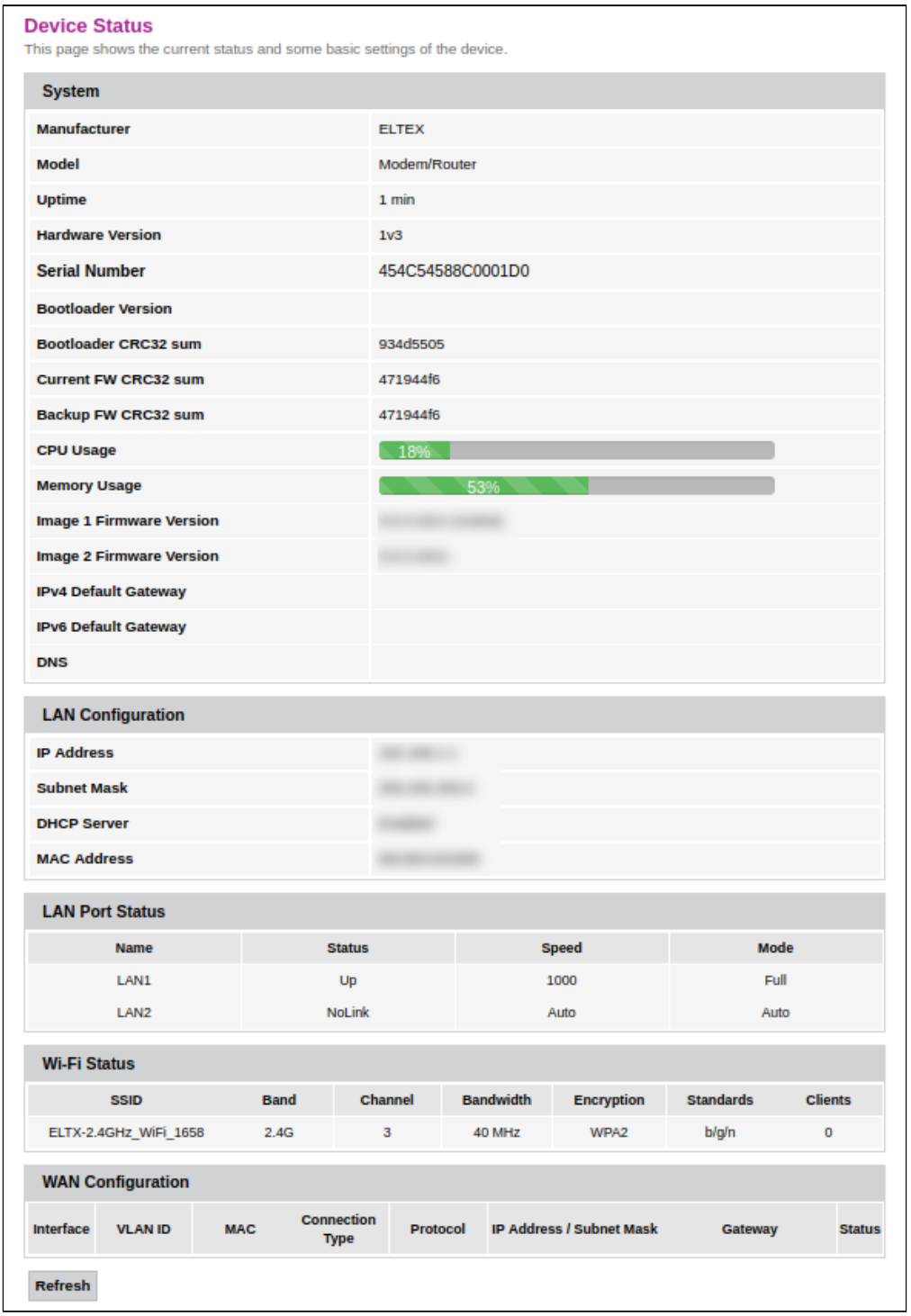
1. Дерево навигации по меню настроек устройства.
2. Основное окно настроек выбранного раздела.
3. Кнопка смены пользователя.

5.1 Меню «Status». Информация об устройстве

5.1.1 Подменю «Device status». Общая информация об устройстве

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

Status → Device status



System

- *Manufacturer* – производитель;
- *Model* – модель устройства;

- *Uptime* – время работы устройства;
- *Hardware Version* – версия аппаратного обеспечения;
- *Serial Number* – серийный номер устройства;
- *Bootloader Version* – версия загрузчика ПО;
- *Bootloader CRC32 sum* – контрольная сумма загрузчика ПО;
- *Current FW CRC32 sum* – контрольная сумма активного образа ПО;
- *Backup FW CRC32 sum* – контрольная сумма резервного образа ПО;
- *CPU Usage* – процент использования CPU;
- *Memory Usage* – процент использования памяти;
- *Image 1 Firmware Version (Active)* – текущая версия ПО;
- *Image 2 Firmware Version* – версия резервного ПО;
- *IPv4 Default Gateway* – шлюз по умолчанию IPv4;
- *IPv6 Default Gateway* – шлюз по умолчанию IPv6;
- *DNS* – адрес DNS-сервера.

LAN Configuration

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

LAN Port Status

- *Name* – название LAN-порта;
- *Status* – состояние LAN-порта;
- *Speed* – скорость подключения внешнего сетевого устройства к порту;
- *Mode* – режим работы порта (half-duplex/full-duplex/auto).

Wi-Fi Status

- *SSID* – название сети точки доступа;
- *Band* – диапазон, полоса, стандарты;
- *Channel* – номер канала;
- *Bandwidth* – ширина канала;
- *Encryption* – метод шифрования;
- *Standarts* – стандарты сети;
- *Clients* – количество подключенных клиентов.

WAN Configuration

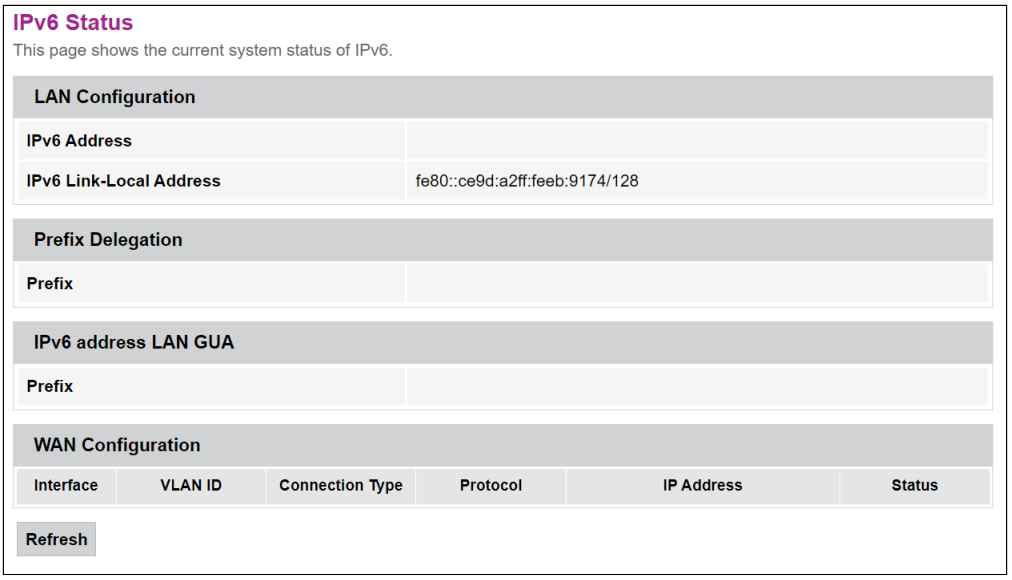
- *Interface* – название интерфейса;
- *VLAN ID* – VLAN ID интерфейса;
- *MAC* – MAC-адрес интерфейса;
- *Connection Type* – тип соединения;
- *Protocol* – используемый протокол;
- *IP Address/Subnet Mask* – IP-адрес/маска подсети интерфейса;
- *Gateway* – шлюз;
- *Status* – статус интерфейса.

Для обновления данных на странице нажмите кнопку «Refresh».

5.1.2 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.

IPv6 address LAN GUA

- *Prefix* – префикс.

WAN Configuration

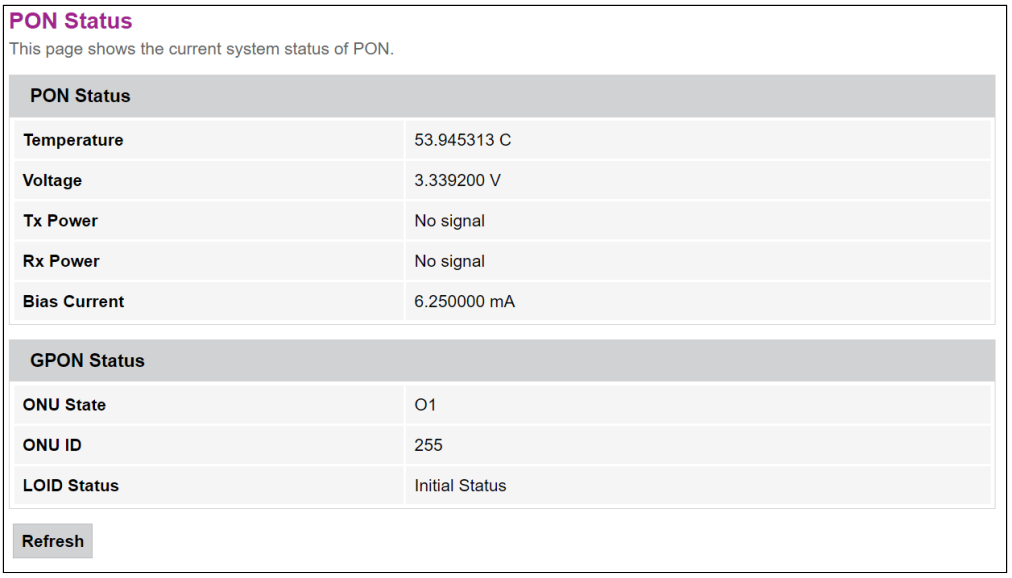
- *Interface* – название интерфейса;
- *VLAN ID* – VLAN ID интерфейса;
- *Connection Type* – тип соединения;
- *Protocol* – используемый протокол;
- *IP Address* – IP-адрес интерфейса;
- *Status* – статус интерфейса.

Для обновления данных на странице нажмите кнопку «Refresh».

5.1.3 Подменю «PON». Информация о статусе оптического модуля

В разделе показано текущее состояние PON-интерфейса.

Status → PON



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

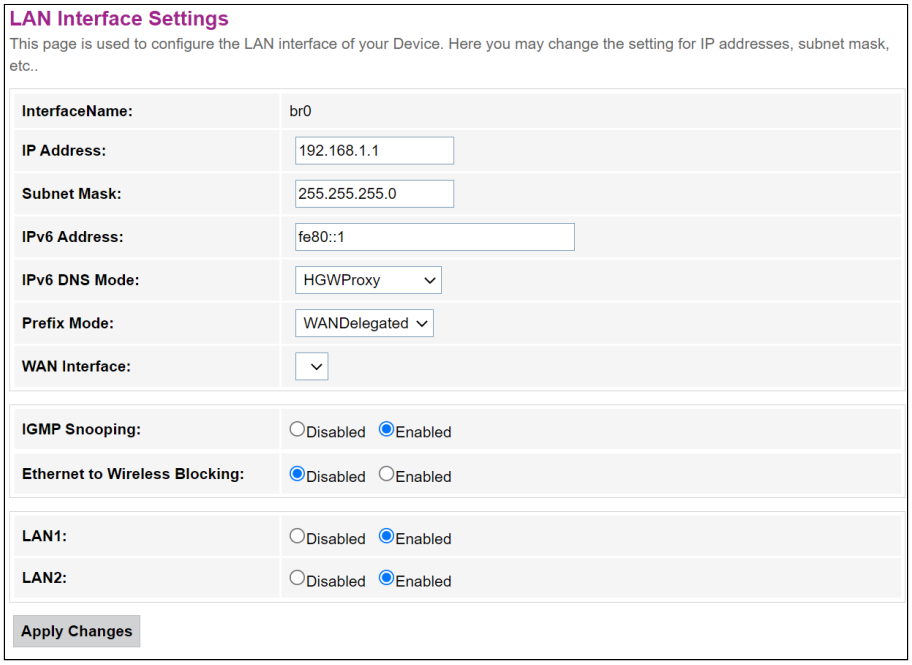
- *ONU State* – статус ONU;
- *ONU ID* – ONU ID;
- *LOID Status* – статус LOID.

Для обновления данных на странице нажмите кнопку «Refresh».

5.2 Меню «LAN». Настройка интерфейса LAN

В разделе доступна настройка основных характеристик 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:
  - *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.
- *IGMP Snooping (Enabled/Disabled)* – включение/выключение IGMP Snooping;
- *Ethernet to Wireless Blocking (Enabled/Disabled)* – включение/выключение изоляции проводных и беспроводных клиентов;
- *LAN1/LAN2 (Enabled/Disabled)* – состояние LAN-портов.

Для сохранения изменений нажмите кнопку «Apply Changes».

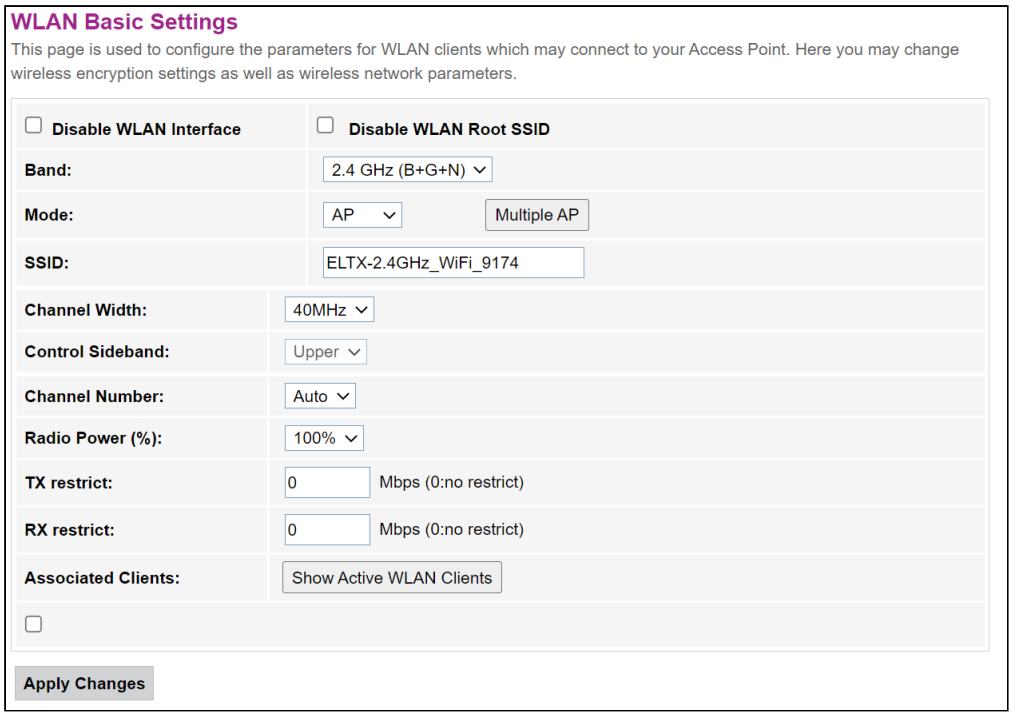
5.3 Меню «WLAN». Настройка беспроводной сети

В данном меню производятся настройки беспроводной сети.

5.3.1 Подменю «Basic settings». Основные настройки

В разделе производятся основные настройки параметров беспроводного интерфейса WLAN.

WLAN → Basic Settings



- *Disable WLAN Interface* – отключение радиоинтерфейса;
- *Disable WLAN Root SSID* – отключение основной точки доступа;
- *Band* – выбор стандарта работы Wi-Fi;
- *Mode* – режим работы точки доступа (AP/Client);
- *SSID (Service Set Identifier)* – назначить имя беспроводной сети (ввод с учетом регистра клавиатуры);

  По умолчанию на устройстве установлено имя беспроводной сети (SSID) ELTX-2.4GHz_WiFi-aaaa, где aaaa – это 4 последние цифры WAN MAC. WAN MAC указан в наклейке на корпусе устройства. В имени сети фигурирует частотный диапазон (2.4 ГГц).

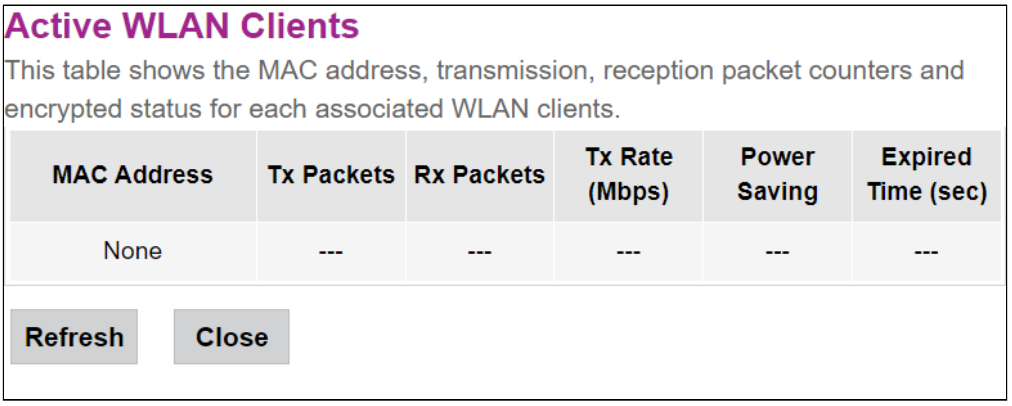
- *Channel Width* – установка ширины полосы 20, 40 МГц (для стандартов работы Wi-Fi: 2.4 ГГц (N), 2.4 ГГц (G+N), 2.4 ГГц (B+G+N));
- *Control Sideband* – боковая полоса управления, выбор второго канала (Lower или Upper) (для стандартов работы Wi-Fi: 2.4 ГГц (N), 2.4 ГГц (G+N), 2.4 ГГц (B+G+N));
- *Channel Number* – выбор используемого канала:
  - *Auto* – автоматический выбор канала.
- *Radio Power (%)* – установка мощности передатчика;
- *TX restrict* – ограничение скорости передачи;
- *RX restrict* – ограничение скорости приема;
- *Associated Clients* – число подключенных клиентов.

Для сохранения изменений нажмите кнопку «Apply Changes».

По умолчанию ключ WPA2-PSK сгенерирован уникальным для устройства, и указан на корпусной наклейке. При изменении пароля необходимо задать комбинацию от 8 до 63 символов ASCII. Пароль должен содержать цифры и латинские буквы в верхнем и нижнем регистрах.

Кнопка «Show Active WLAN Client» выводит таблицу активных клиентов WLAN.

WLAN → Basic settings → Show Active WLAN Client



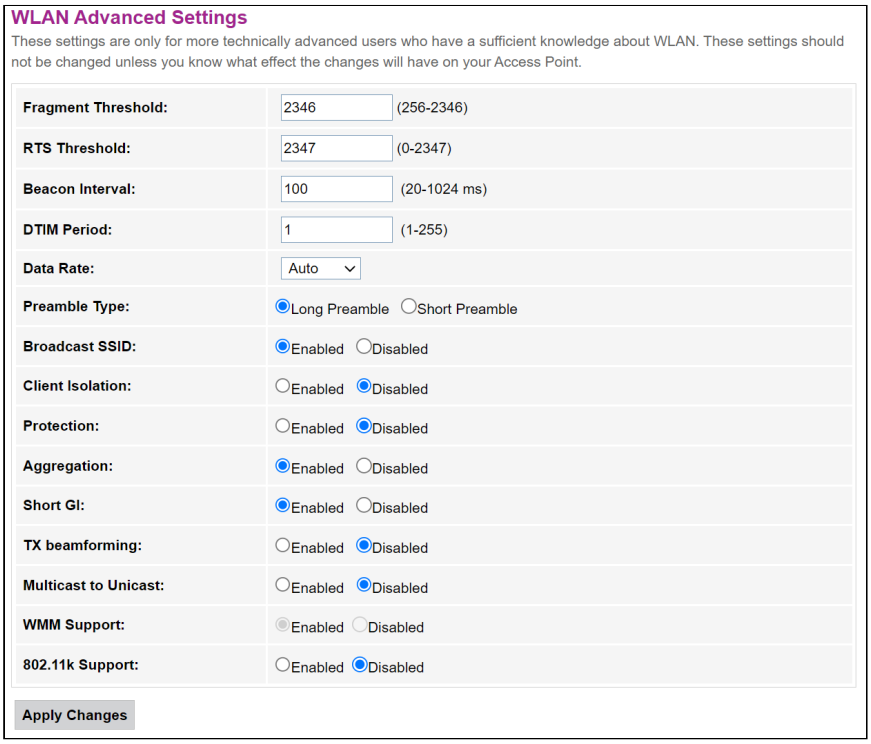
- *MAC Address* – MAC-адрес клиента;
- *Tx Packets* – количество переданных пакетов клиенту;
- *Rx Packets* – количество принятых пакетов от клиента;
- *Tx Rate (Mbps)* – канальная скорость передачи, Мбит/с;
- *Power Saving* – режим энергосбережения;
- *Expired Time (sec)* – время истечения аренды адреса, с.

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

5.3.2 Подменю «Advanced settings». Расширенные настройки

В разделе производятся расширенные настройки беспроводной сети.

WLAN → Advanced settings



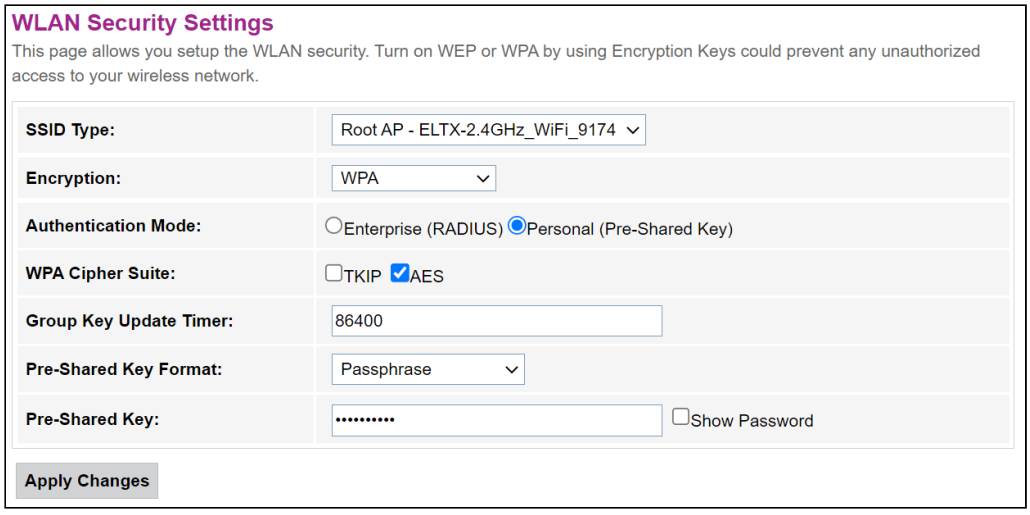
- *Fragment Threshold* – установка порога фрагментации в байтах. Если размер пакета будет превышать заданное значение, он будет фрагментирован на части подходящего размера;
- *RTS Threshold* – если сетевой пакет меньше, чем установленное пороговое значение RTS, механизм RTS/CTS (механизм соединения по каналу с использованием сигналов готовности к передаче/готовности к приему) задействован не будет;
- *Beacon Interval* – период отправки информационного пакета в беспроводную сеть, сигнализирующего о том, что точка доступа активна;
- *DTIM Period* – интервал между отправкой пакетов из буфера;
- *Data rate* – скорость передачи;
- *Preamble Type* – выбор преамбулы: длинная (*Long Preamble*)/короткая (*Short Preamble*);
- *Broadcast SSID (Enable/Disabled)* – вещание SSID в сеть (в случае Disabled SSID будет скрыт);
- *Client Isolation* (*Enable/Disabled)* – включение/выключение изоляции клиентов;
- *Protection (Enable/Disabled)* – включение/выключение 802.11n protection;
- *Aggregation (Enable/Disabled)* – включение/выключение агрегации кадров для повышения пропускной способности;
- *Short GI* (*Enable/Disabled)* – включение/выключение короткого защитного интервала;
- *TX beamforming* (*Enable/Disabled)* – включение/выключение адаптивного формирования диаграммы направленности;
- *Multicast to Unicast* (*Enable/Disabled)* – включение/выключение перекладывания всего multicast трафика в unicast;
- *WMM Support* (*Enable/Disabled)* – включение/выключение поддержки Wi-Fi Multimedia;
- *802.11k Support (Enable/Disabled)* – включение/выключение опции Radio Resource managment для передачи клиентам информации о соседних точках доступа.

Для сохранения изменений нажмите кнопку «Apply Changes».

5.3.3 Подменю «Security». Настройка параметров безопасности

В разделе осуществляются основные настройки шифрования данных в беспроводной сети.
Здесь можно настроить клиентское оборудование беспроводного доступа вручную или автоматически, используя WPS.

WLAN → Security



- *SSID Type* – текущий SSID;
- *Encryption* – установка режима шифрования:
  - *NONE (открытый)* – защита беспроводной сети отсутствует;
  - *WEP* – защита беспроводной сети по алгоритму WEP;
  - *WPA/WPA2/WPA2 Mixed/WPA3/WPA3 Mixed* – защита беспроводной сети по алгоритму WPA/WPA2/WPA2 Mixed/WPA3/WPA3 Mixed.

При выборе режима шифрования *WEP* доступны следующие настройки:

- *802.1x Authentication* – включение стандарта 802.1x (позволяет пользователям аутентифицироваться с использованием сервера аутентификации RADIUS, для шифрования данных используется WEP-ключ);
- *Authentication* – выбор режима аутентификации:
  - *Open system* – без аутентификации;
  - *Shared Key* – аутентификация по предусмотренному ключу;
  - *Auto* – автоматическая аутентификация.
- *Key Length (степень шифрования)* – использование ключей длиной 64 или 128 бит;
- *Key Format (формат ключа)* – использовать формат ASCII или HEX;
- *Encryption Key (сетевой ключ)* – ключ из 10 символов в 16-ричной системе счисления либо 5 символов ASCII1 для 64-х битного шифрования. Также возможно 26 символов в 16-ричной системе счисления, либо 13 символов ASCII для 128-х битного шифрования.

При выборе режима шифрования *WPA/WPA2/WPA2 Mixed*, доступны следующие настройки:

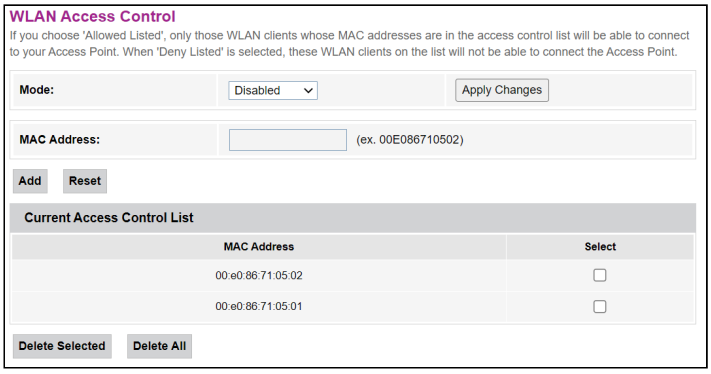
- *Authentication Mode* – режим аутентификации Enterprise (RADIUS) или Personal (Pre-Shared Key). В режиме Enterprise (RADIUS) нужно настроить:
  - *RADIUS Server IP Address* – IP-адрес RADIUS-сервера;
  - *RADIUS Server Port* – номер порта RADIUS-сервера. По умолчанию установлен порт 1812;
  - *RADIUS Server Password* – секретный ключ для доступа к RADIUS-серверу;
- *IEEE 802.11w* – включить шифрование служебных кадров;
  - *None* – шифрование служебных кадров отсутствует;
  - *Capable* – режим совместимости шифрования;
  - *Required* – требуется шифрование.
- *SHA256 (Enable/Disable)* – включение/выключение использования SHA256.
- *WPA Cipher Suite* – набор шифров WPA *TKIP* или *AES*;
- *Group Key Update Timer* – интервал обновления ключа;
- *Pre-Shared Key Format* – формат ключа ASCII или HEX;
- *Pre-Shared Key* – ключ доступа.

Для демонстрации зашифрованного ключа доступа активируйте «Show Password». Для сохранения изменений нажмите кнопку «Apply Changes».

5.3.4 Подменю «Access control». Настройка доступа

В разделе производится настройка фильтрации MAC-адресов. Все добавленные MAC-адреса будут отображаться в *Current Access Control List* – текущий список контроля доступа. При выборе режима *«Allowed Listed»,* подключиться к точке доступа смогут только те MAC-адреса, которые находятся в *Current Access Control List.* При выборе режима *«Deny Listed»* доступ будут иметь все MAC-адреса, кроме тех, которые указаны в *Current Access Control List.* Для смены режима нажмите кнопку «Apply Changes».

WLAN → Access control



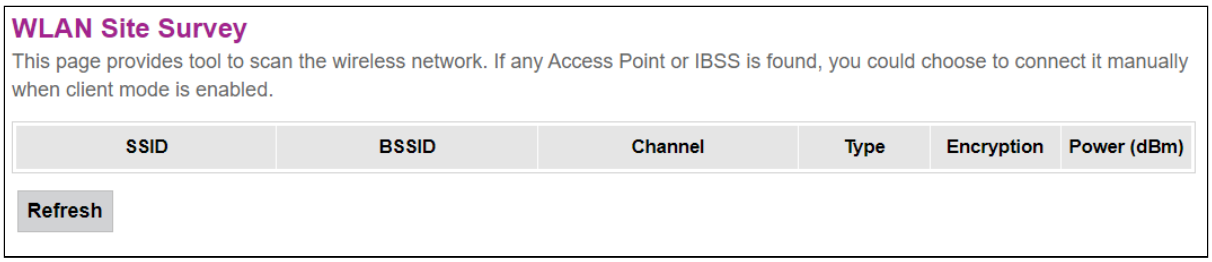
- *Mode* – выбор режима фильтрации по MAC-адресам:
  - *Disabled* – фильтр не используется;
  - *Allowed Listed* – фильтр по разрешенным адресам (белый список);
  - *Deny Listed* – фильтр по запрещенным адресам (черный список).
- *MAC Address* – поле для добавления MAC-адреса в таблицу фильтрации. Чтобы внести значение, нажмите кнопку «Add», для сброса значения — кнопку «Reset».

Для удаления определённой позиции в списке, выделите её и нажмите «Delete Selected», чтобы удалить весь список, нажмите «Delete All».

5.3.5 Подменю «WiFi radar». Сканирование беспроводной сети

В разделе осуществляется сканирование беспроводной сети, тем самым происходит обнаружение ближайших точек доступа или IBSS.

WLAN → WiFi radar



В таблице отображается следующая информация:

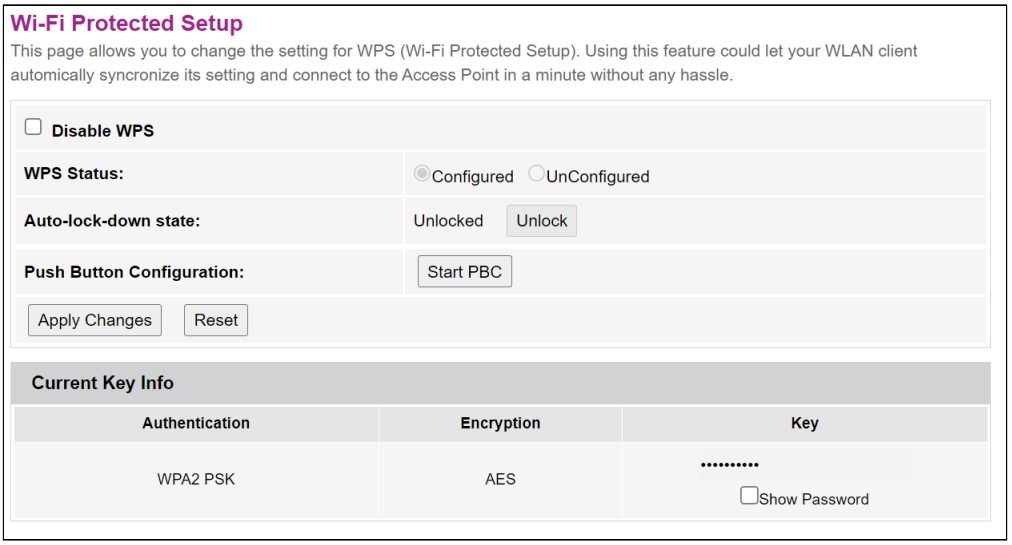
- *SSID* – имя беспроводной точки доступа;
- *BSSID* – MAC-адрес точки доступа;
- *Channel* – канал;
- *Type* – тип (AP, Client – точка доступа, клиент);
- *Encryption* – режим шифрования;
- *Power (dBm)* – мощность принимаемого сигнала.

Для сканирования эфира нажмите кнопку «Refresh».

5.3.6 Подменю «WPS». Возможность упрощенного подключения к сети Wi-Fi

В разделе осуществляется настройка для подключения по технологии WPS (Wi-Fi Protected Setup, защищенная настройка Wi-Fi).

WLAN → WPS



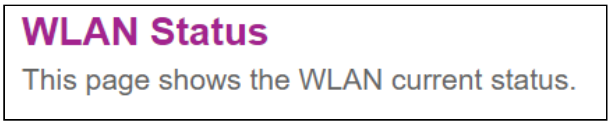
- *Disable WPS* – выключить возможность подключения к роутеру по технологии WPS;
- *Push Button Configuration* – активировать функцию WPS на роутере для подключения клиентов.

Для демонстрации зашифрованного ключа доступа активируйте «Show Password». Для сохранения изменений нажмите кнопку «Apply Changes».

5.3.7 Подменю «Status». Текущее состояние WLAN

В данном подменю отображается текущее состояние WLAN.

WLAN → Status



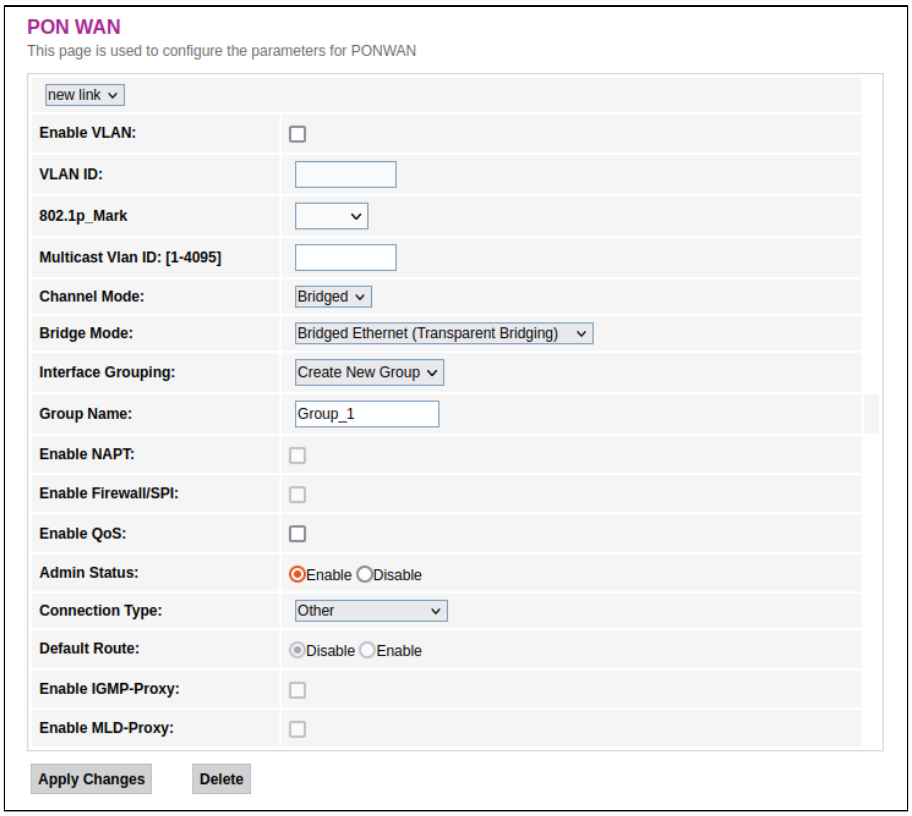
- *Mode* – AP-точка доступа;
- *Band* – диапазон, полоса, стандарты;
- *SSID* – название сети точки доступа;
- *Channel Number* – номер канала;
- *Channel Width* – ширина канала;
- *Encryption* – метод шифрования;
- *BSSID* – MAC-адрес точки доступа;
- *Associated Clients* – количество подключенных клиентов.

5.4 Меню «WAN». Настройка сервисов

5.4.1 Подменю «PON WAN». Настройка 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.
- *Interface Grouping* – выбор группы интерфейсов;
- *Group name* – имя группы интерфейсов;
- *Enable NAPT* – включение функции NAPT;
- *Enable QoS* – статус приоритизации трафика;
- *Admin Status (Enable/Disable)* – включение/выключение административного статуса;
- *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;
- *Enable MLD-Proxy* – включение перехвата и пересылку сообщений MLD.

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

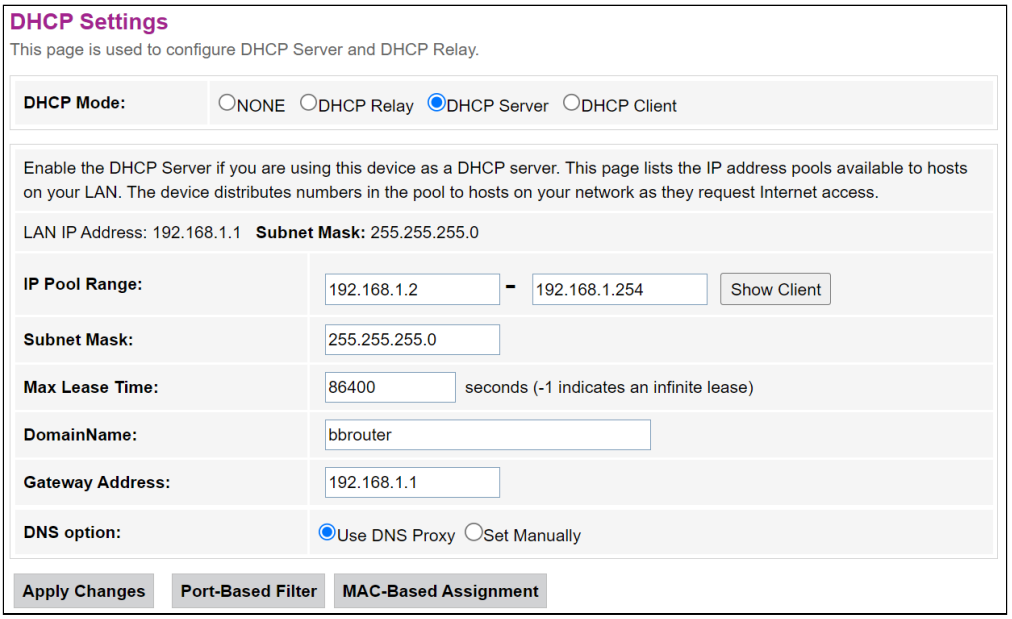
5.5 Меню «Services». Настройка сервисов

5.5.1 Подменю «Service»

5.5.1.1 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 Relay* – работа в режиме DHCP-ретранслятора;
  - *DHCP Server* – работа в режиме DHCP-сервера;
  - *DHCP Client* – работа в режиме DHCP-клиента.
- *IP Pool Range* – диапазон адресов, выдаваемых клиентам;

- *Show Client* – кнопка для просмотра клиентов, арендовавших адреса. По нажатию выводится таблица с информацией о клиентах DHCP, арендовавших DHCP-сервер;
- *Subnet Mask* – маска посети;
- *Max Leas 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.
- *DHCP Server IP Address* – IP-адрес удалённого сервера DHCP.

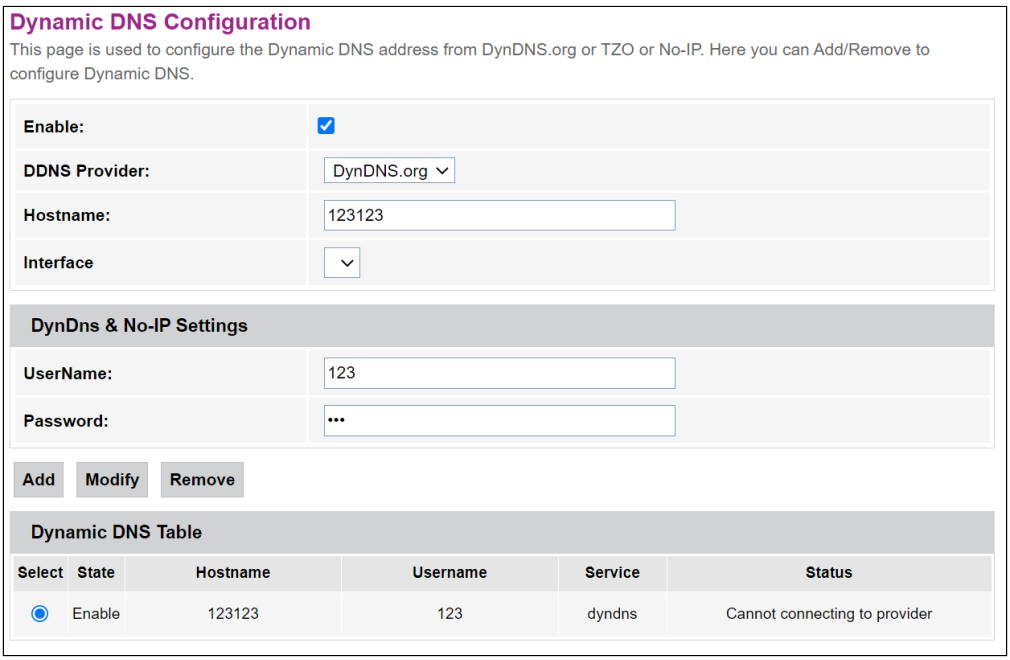
Для сохранения изменений нажмите кнопку «Apply Changes». Кнопки «Port-Based Filter» и «MAC-Based Assignment» позволяют настроить фильтрацию по портам и MAC соответственно.

5.5.1.2 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-52W) 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 → 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, No-IP.com;
- *Custom* – иной провайдер, выбранный пользователем. В данном случае необходимо самостоятельно указать имя (*Hostname*) и адрес (*Interface*) провайдера.

DynDns/No-IP Settings:

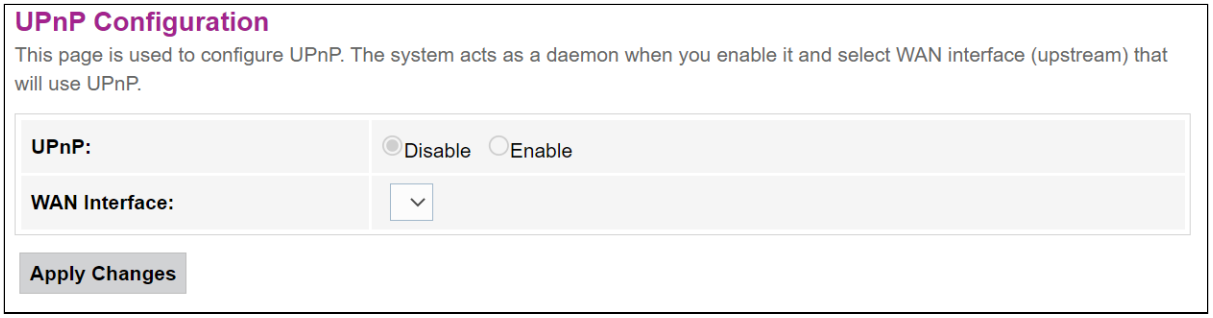
- *UserName* – имя пользователя;
- *Password* – пароль авторизации на сервисе, выбранном для работы с D-DNS.

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.

5.5.1.3 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.

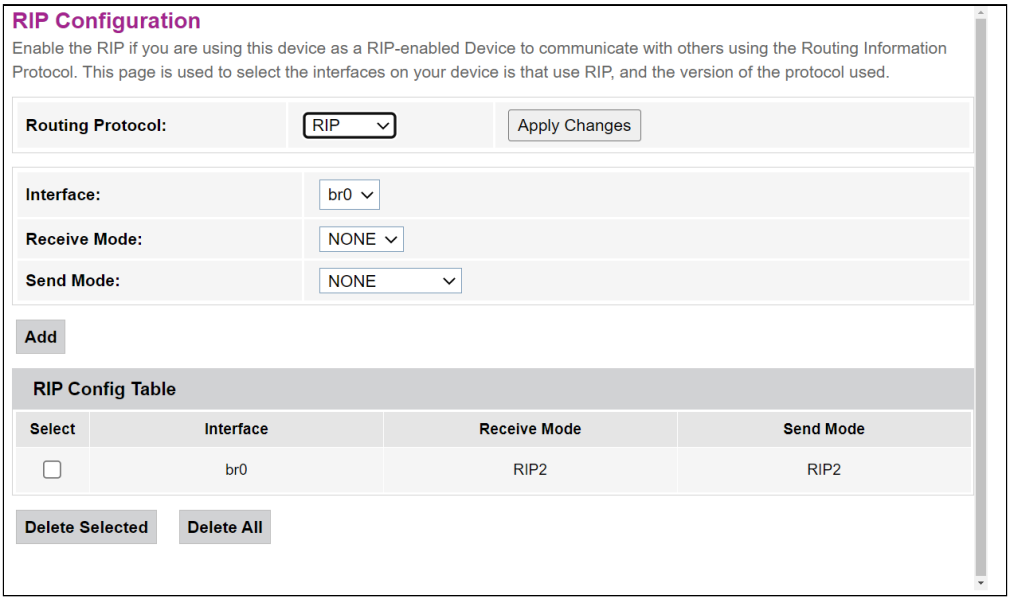
- *UPnP (Enable/Disable)* – включение/выключение функции UPnP;
- *WAN Interface* – WAN-интерфейс, на котором будет работать функция UPnP.

Для сохранения настроек нажмите кнопку «Apply Changes».

5.5.1.4 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).

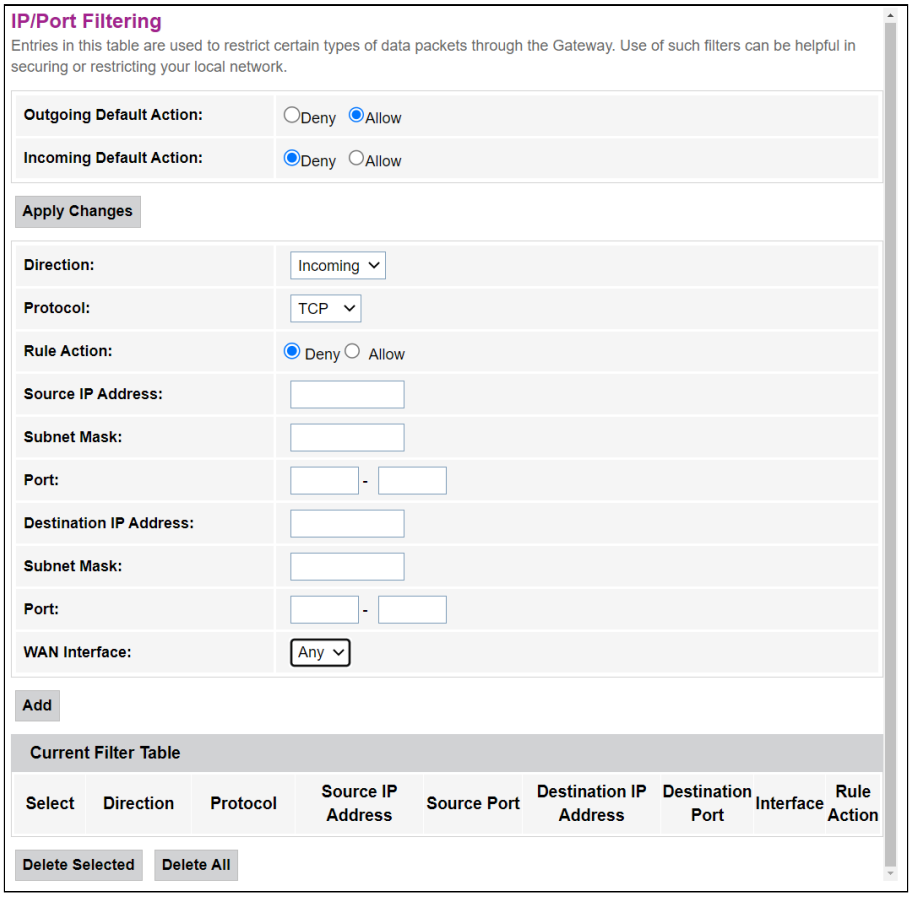
Интерфейсы с поддержкой RIP отображаются в таблице *«RIP Config Table»*. Для удаления всех записей в таблице нажмите кнопку «Delete All», чтобы удалить одну позицию из списка, выделите её и нажмите кнопку «Delete Selected».

5.5.2 Подменю «Firewall». Настройка брандмауэра

5.5.2.1 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

- *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»:

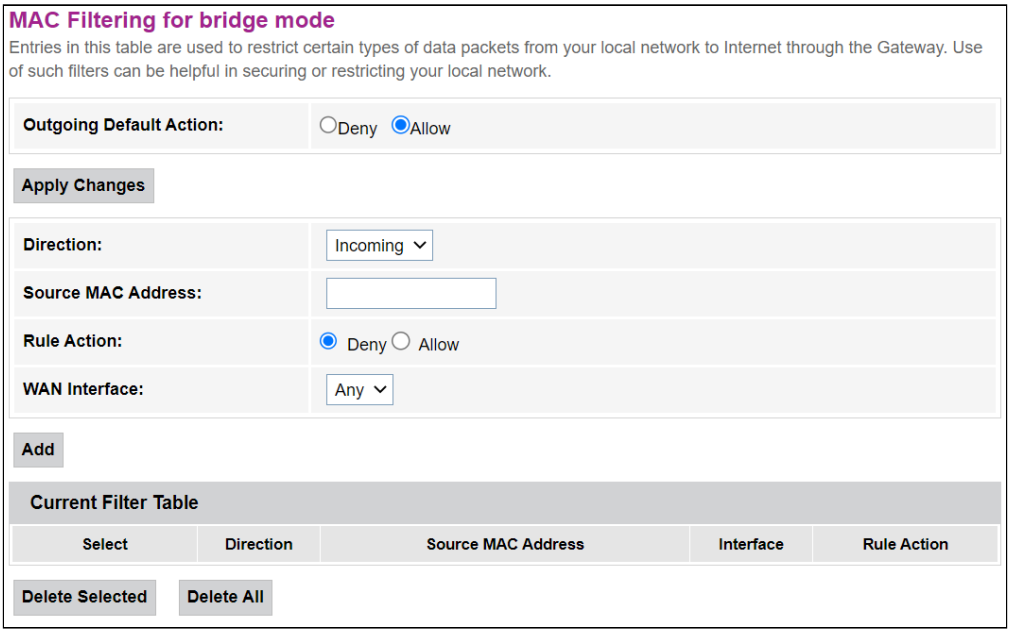
- *Protocol* – протокол фильтрации;
- *Rule Action (Deny/Allow)* – политика обработки пакета (отбросить/пропустить);
- *Source IP Address* – IP-адрес источника;
- *Subnet Mask* – маска подсети источника;
- *Port* – порт;
- *Destination IP Address* – IP-адрес назначения;
  - *Subnet Mask* – маска подсети;
  - *Port* – порт.
- *WAN 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».

5.5.2.2 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 смена режима нажмите кнопку «Apply Changes».

Services → Firewall → MAC Filtering



Настройки по умолчанию

- *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»:

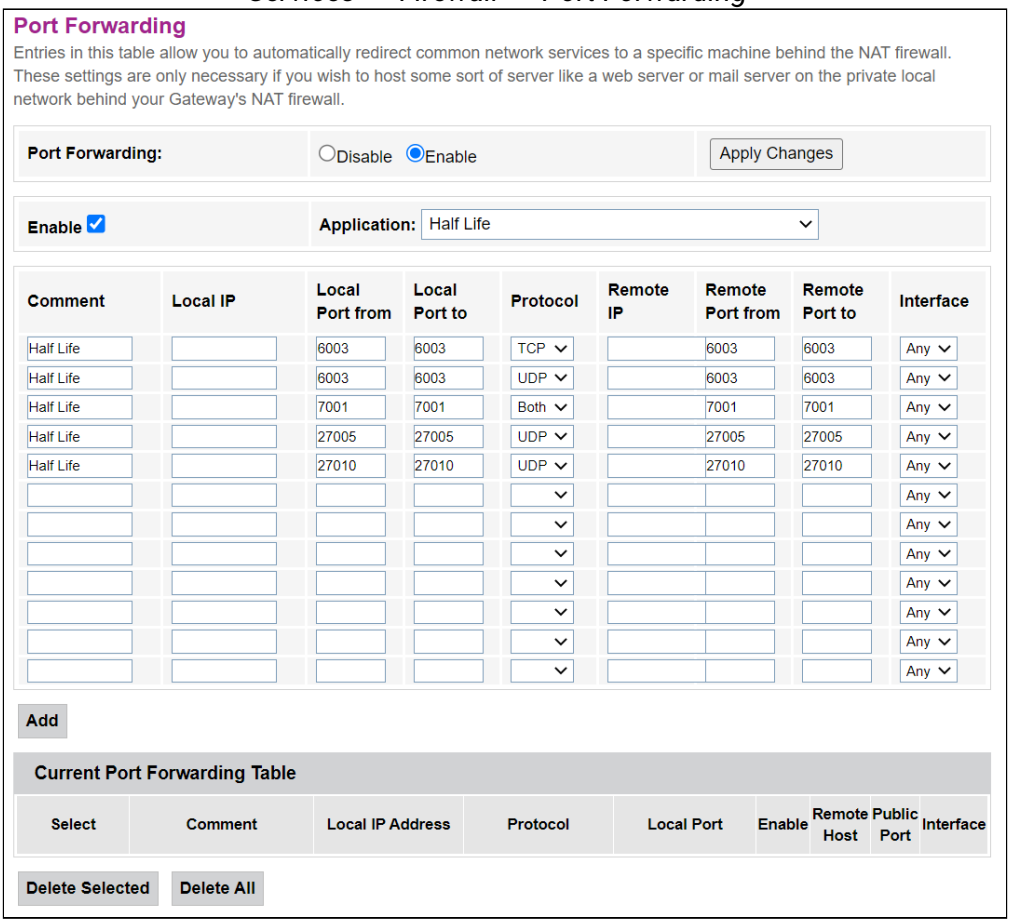
- *Source MAC Address* – поле для добавления исходного MAC-адреса, для которого вводится ограничение/доступ;
- *WAN Interface* – входящий интерфейс.

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».

5.5.2.3 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;

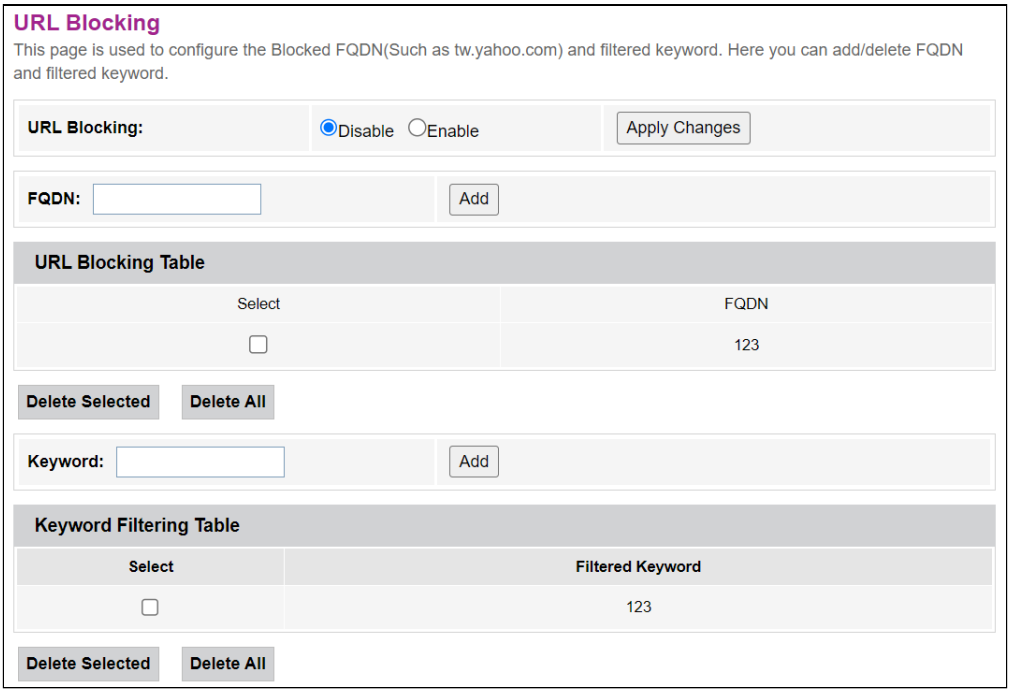
- *Comment* – комментарий;
- *Local IP* – локальный IP-адрес, на который производится проброс;
- *Local port from/to* – укажите диапазон портов локального устройства для проброса;
- *Protocol* – выбор протокола (TCP, UDP или оба);
- *Remote port from/to* – укажите начальный порт входящего соединения. Поле *Remote port to* заполнится автоматически;
- *Interface* – выбор интерфейса.

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».

5.5.2.4 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



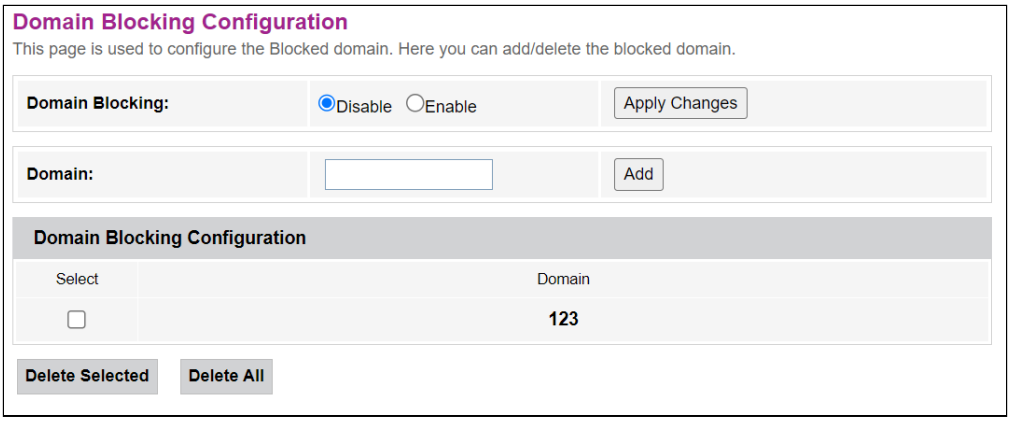
- *URL Blocking (Enable/Disable)* – включение/выключение работы URL-Blocking;
- *FQDN (Fully Qualified Domain Name)* – полное доменное имя;
- *Keyword* – ключевое слово.

Для сохранения изменений нажмите кнопку «Apply Changes».

5.5.2.5 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».

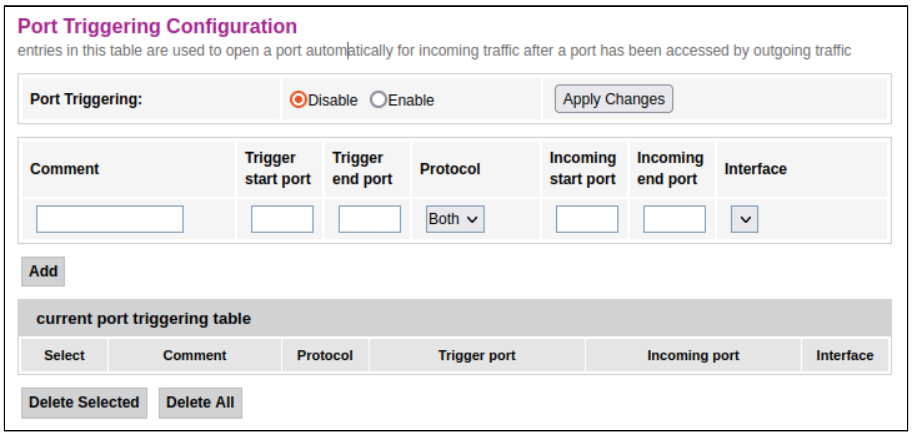
- *Domain Blocking (Enable/Disable)* − включение/выключение блокировки;
- *Domain* − наименование домена.

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».

5.5.2.6 Подменю «Port Triggering». Настройка динамического открытия портов

При появлении определенного события динамически открываются порты на своем внешнем интерфейсе, которые привязаны к соответствующим портам компьютера в локальной сети.

Services → Firewall → Port Triggering



Для добавления записи в таблицу *«current port triggering table»* установите флаг «Enable» и заполните соответствующие поля:

- *Comment* − комментарий к записи таблицы;
- *Trigger start port* − первый порт из диапазона, после обращения на который будет открыт порт из диапазона Incoming;
- *Trigger end port* − последний порт из диапазона, после обращения на который будет открыт порт из диапазона Incoming;
- *Protocol* − выбор протокола;

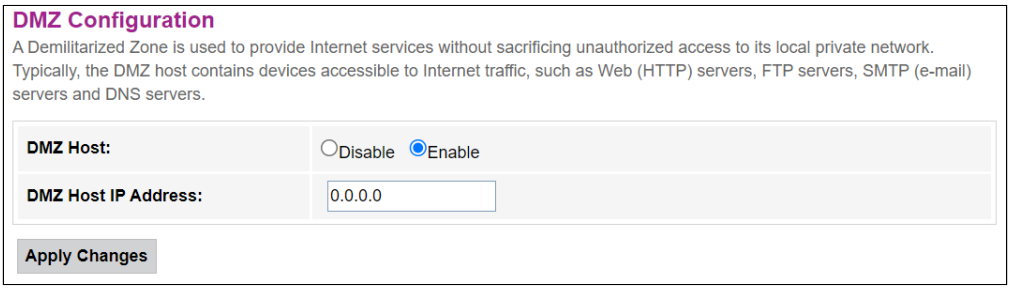
- *Incoming start port* – первый порт из диапазона, который будет открыт при обращении к порту из диапазона Trigger;
- *Incoming end port* – последний порт из диапазона, который будет открыт при обращении к порту из диапазона Trigger;
- *Interface* – выбор интерфейса.

Для сохранения изменений используйте кнопку «Apply Changes». 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».

5.5.2.7 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».

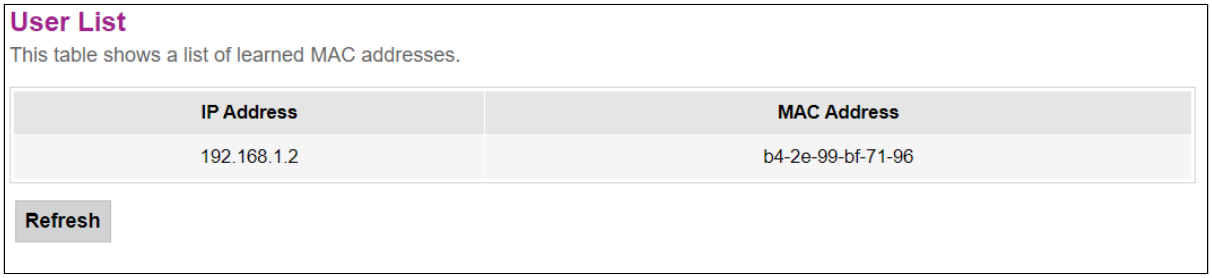
5.6 Меню «Advance». Расширенные настройки

5.6.1 Подменю «Advance»

5.6.1.1 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 → Advance → ARP table



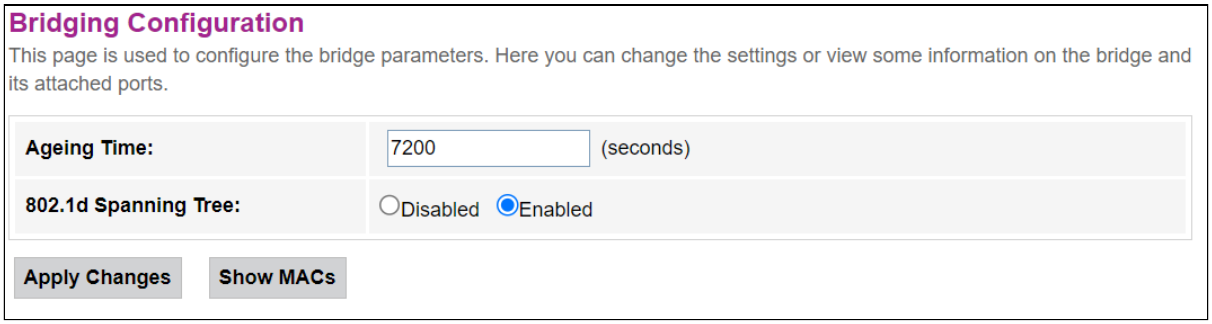
- *IP Address* – IP-адрес клиента;
- *MAC Address* – MAC-адрес клиента.

Для обновления информации в таблице нажмите кнопку «Refresh».

5.6.1.2 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 → Advance → Bridging

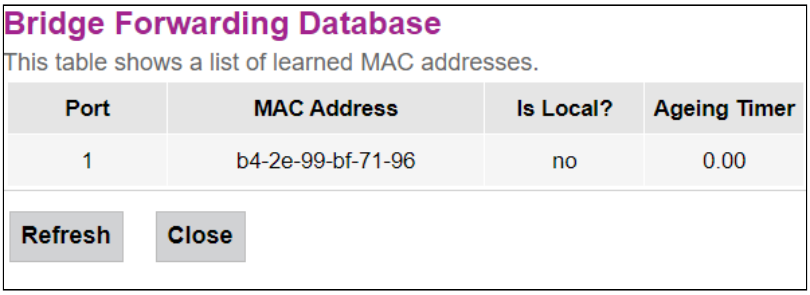


- *Ageing Time* – время жизни адресов (секунды);
- *802.1d Spanning Tree (Enable/Disable)* – включение/выключение протокола 802.1d Spanning Tree.

Для сохранения изменений нажмите кнопку «Apply Changes».

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

Advance → Advance → Bridging → Show MACs



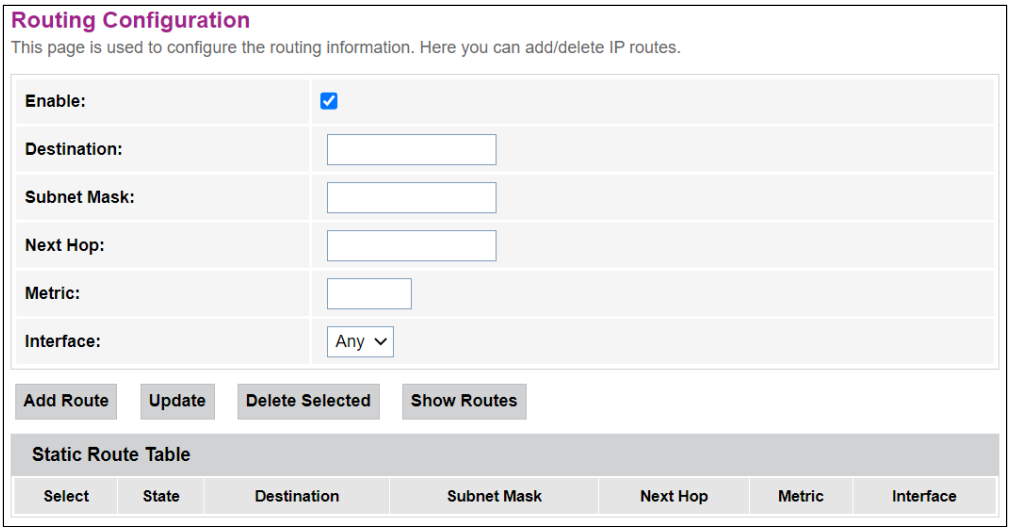
- *Port* – номер порта;
- *MAC Address* – MAC-адрес;
- *Is Local?* – локальный адрес;
- *Ageing Timer* – время жизни адреса.

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

5.6.1.3 Подменю «Routing». Настройка маршрутизации

В разделе осуществляется настройка статической маршрутизации.

Advance → Advance → Routing



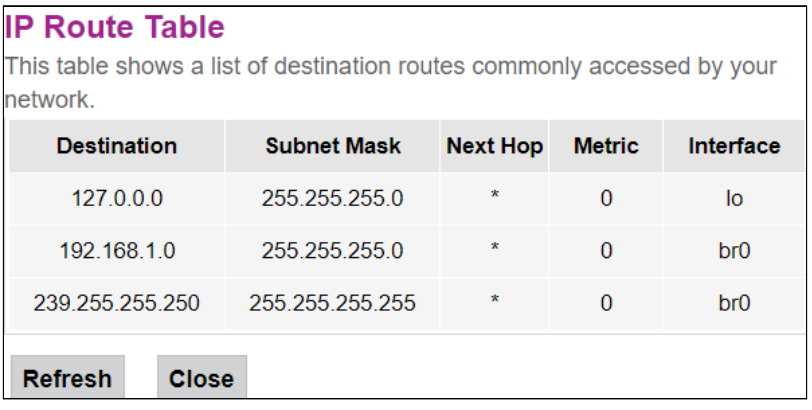
Для добавления статического маршрута поставьте флаг «*Enable*», заполните соответствующие поля и нажмите на кнопку «Add Route».

- *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 → Advance → Routing → Show Routes



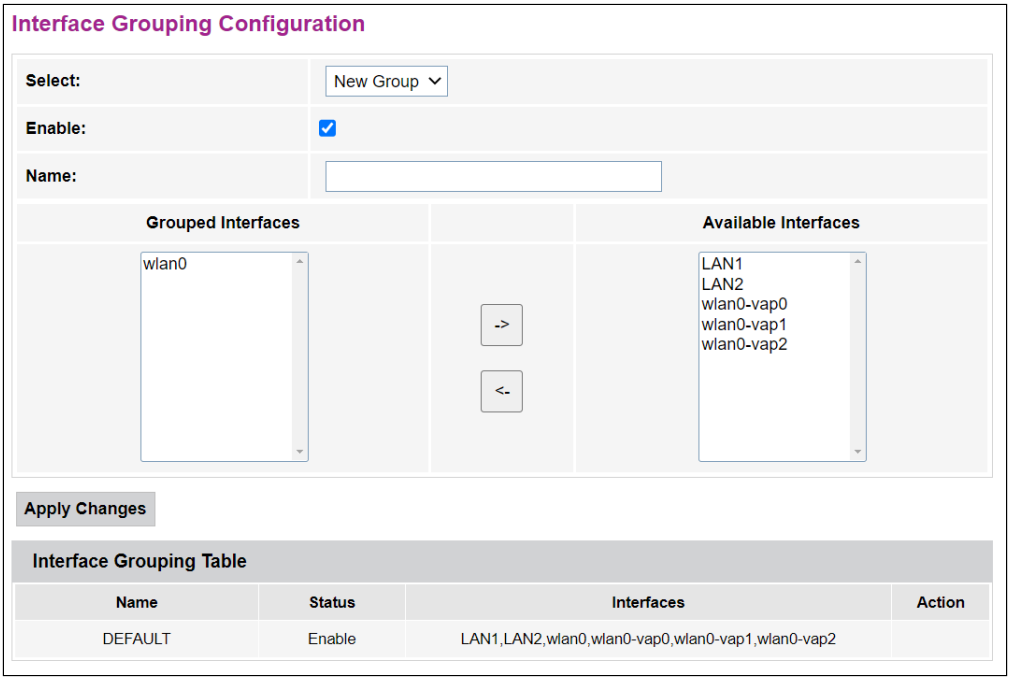
Для обновления информации в таблице нажмите кнопку «Refresh», для закрытия – кнопку «Close».

5.6.1.4 Подменю «Interface Grouping». Объединение интерфейсов в группы

В разделе можно создавать группы и переносить в них интерфейсы. По умолчанию все интерфейсы находятся в одной группе. Для переноса интерфейса в новую группу необходимо:

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

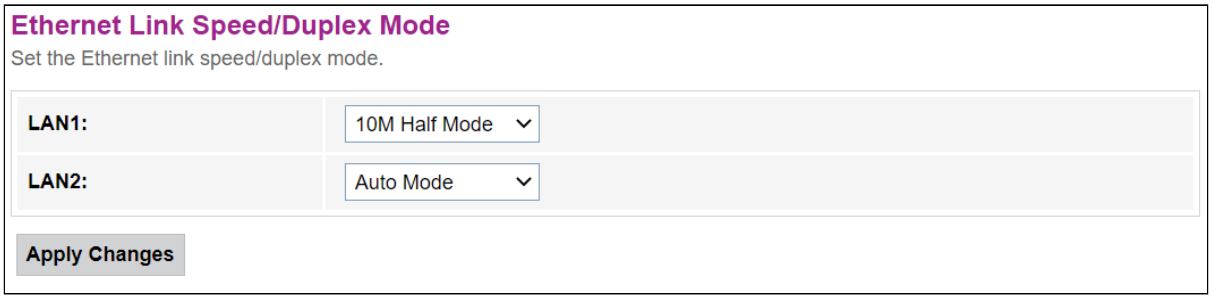
Advance → Advance → Interface Grouping



5.6.1.5 Подменю «Link mode». Настройка LAN-портов

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

Advance → Advance → Link mode



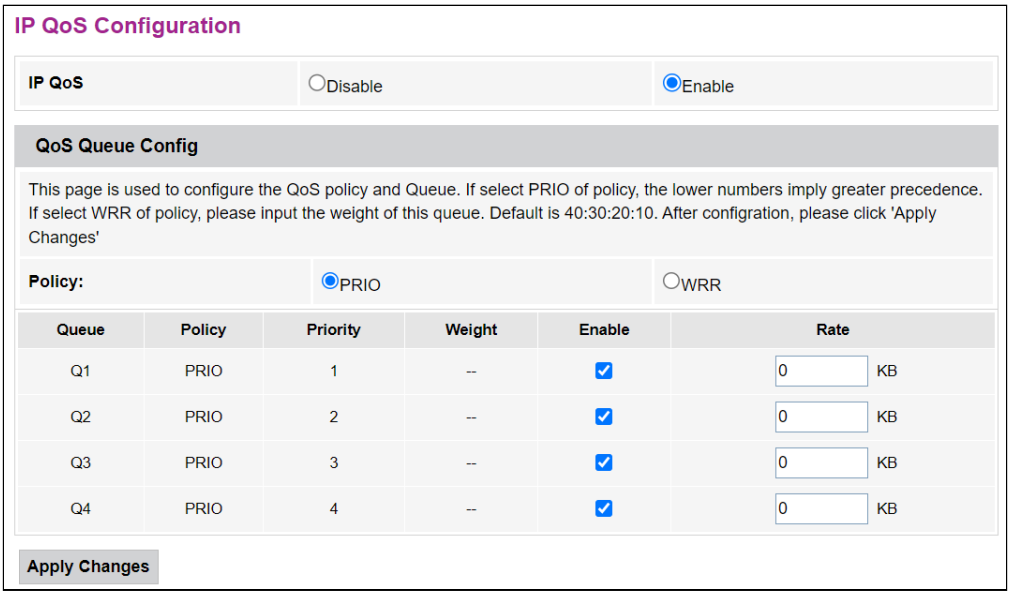
Для сохранения изменений нажмите кнопку «Apply Changes».

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

5.6.2.1 Подменю «QoS Policy». Настройка QoS-очередей

В разделе можно настроить политики QoS-очереди обработки трафика.

Advance → IP QoS → QoS Policy



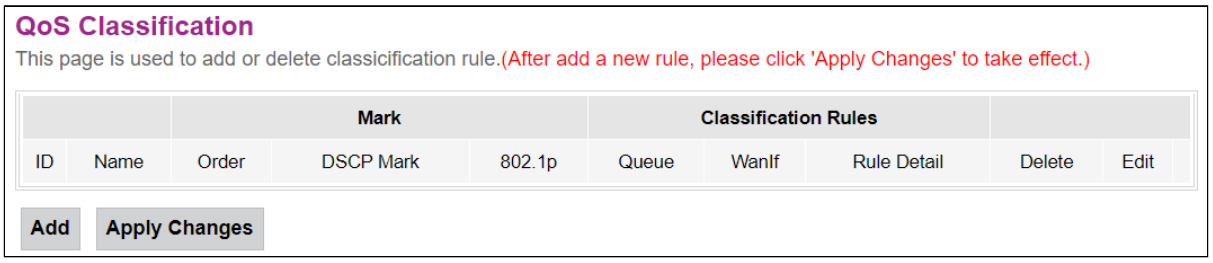
- *IP QoS (Enable/Disable)* – включение/выключение конфигурирования QoS-очередей;
- *Policy* – выбор политики:
  - *PRIO* – при выборе политики PRIO используется строгая обработка очередей. Меньшей очереди соответствует наивысший приоритет;
  - *WRR* – при выборе политики WRR будет использоваться взвешенная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

Для сохранения изменений нажмите кнопку «Apply Changes».

5.6.2.2 Подменю «QoS Classification». Настройка правил классификации трафика

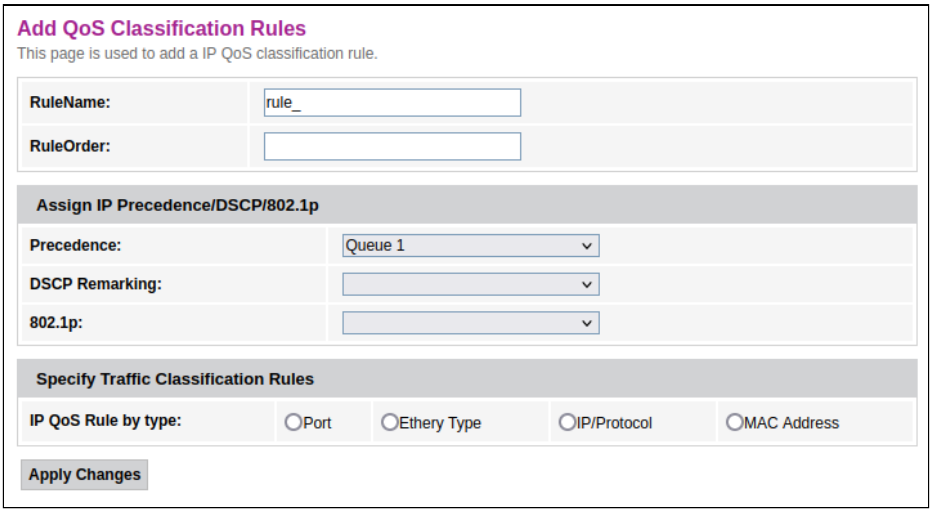
На данной странице можно указать по каким полям и их значениям будет классифицироваться пакет, а также в какую аппаратную очередь он в итоге попадет.

Advance → IP QoS → QoS Classification



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.

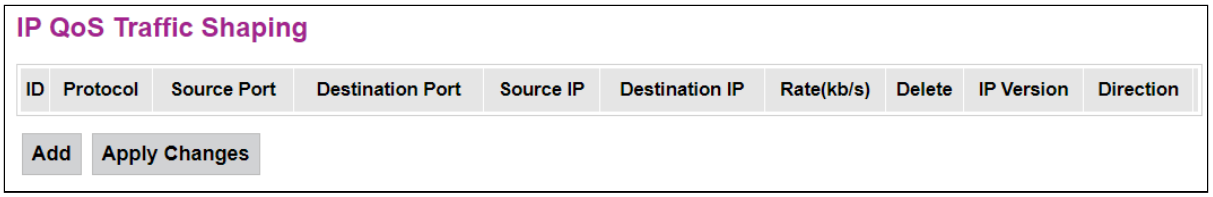
- *IP QoS Rule by type* – выбор правила классификации по типу:
  - *Port* – по порту;
  - *Ethery Type* – по Ethertype;
  - *IP/Protocol* – по протоколу IP;
  - *MAC Address* – по MAC-адресу.

Для сохранения изменений нажмите кнопку «Apply Changes».

5.6.2.3 Подменю «Traffic Shaping». Настройка трафика

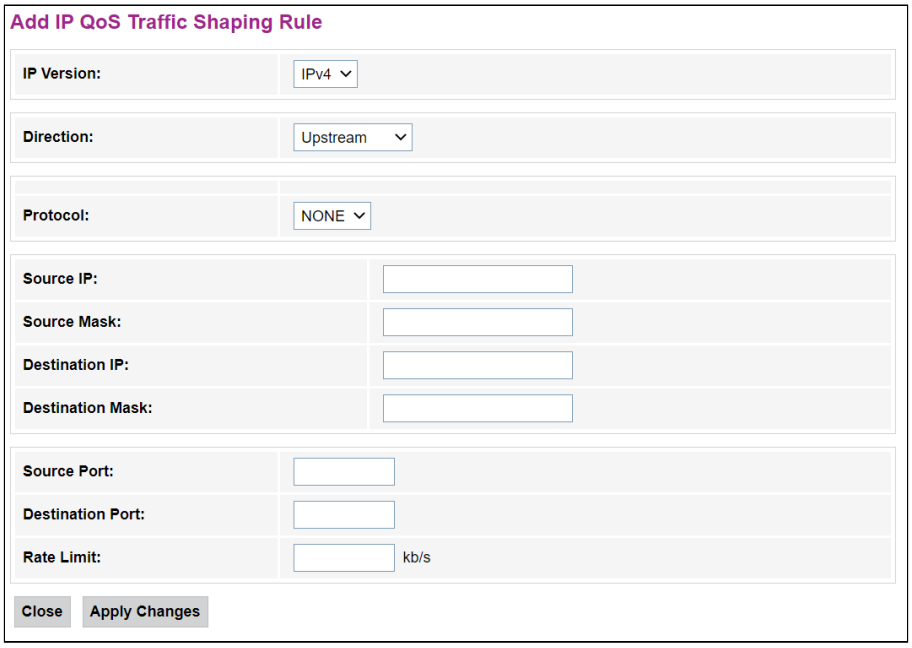
В данном разделе можно указать ограничения трафика по определенным правилам.

Advance → IP QoS → Traffic Shaping



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.

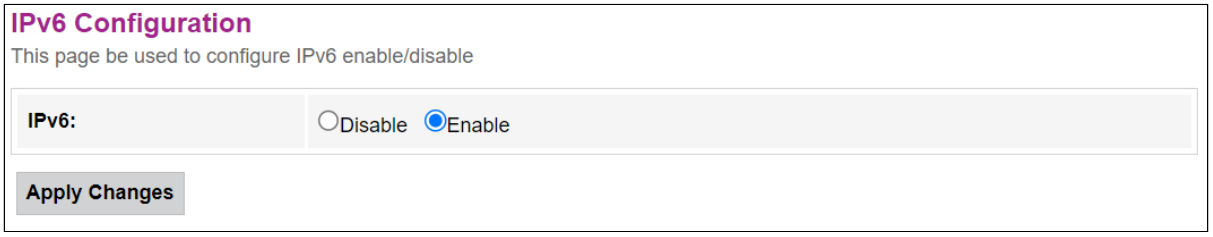
Для сохранения изменений нажмите кнопку «Apply Changes», для отмены нажмите «Close».

5.6.3 Подменю «IPv6». Настройка протокола IPv6

5.6.3.1 Подменю «IPv6 Enable/Disable». Настройка IPv6

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

Advance → IPv6 → IPv6 Enable/Disable

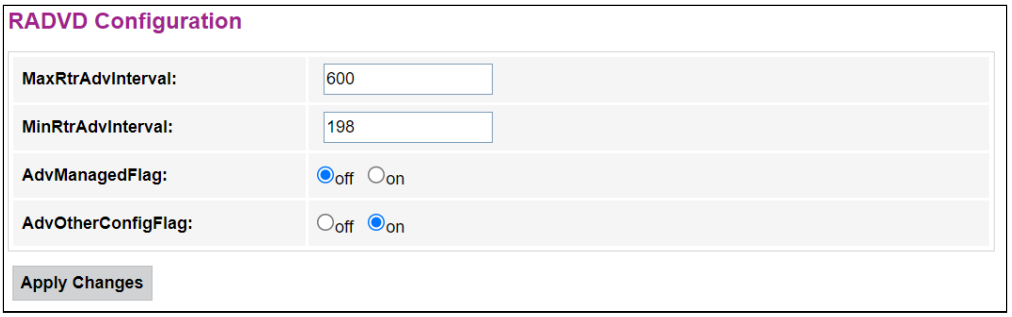


Для сохранения изменений нажмите кнопку «Apply Changes».

5.6.3.2 Подменю «RADVD». Настройка RADVD

В разделе осуществляется настройка RADVD (Router Advertisement Daemon).

Advance → IPv6 → RADVD



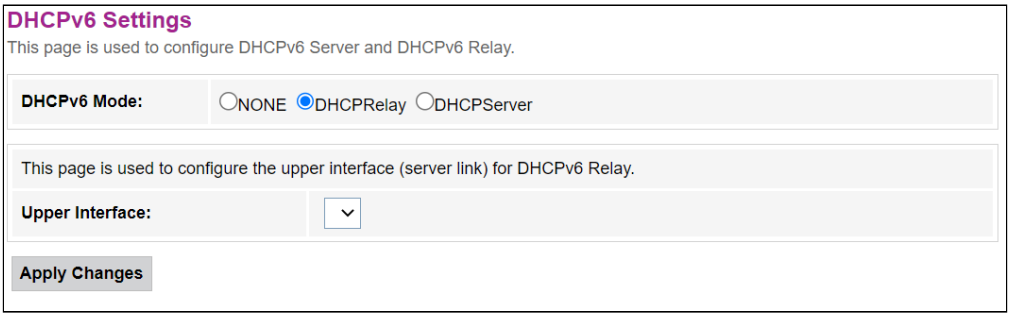
- *MaxRtrAdvInterval* – максимальный интервал отправки RA (Router Advertisement);
- *MinRtrAdvInterval* – минимальный интервал отправки RA;
- *AdvManagedFlag* – включение/выключение отправки флага Managed в RA;
- *AdvOtherConfigFlag* – включение/выключение отправки флага Other RA.

Для сохранения изменений нажмите кнопку «Apply Changes».

5.6.3.3 Подменю «DHCPv6». Настройка DHCPv6-сервера

В разделе осуществляется настройка DHCPv6-сервера.

Advance → IPv6 → DHCPv6



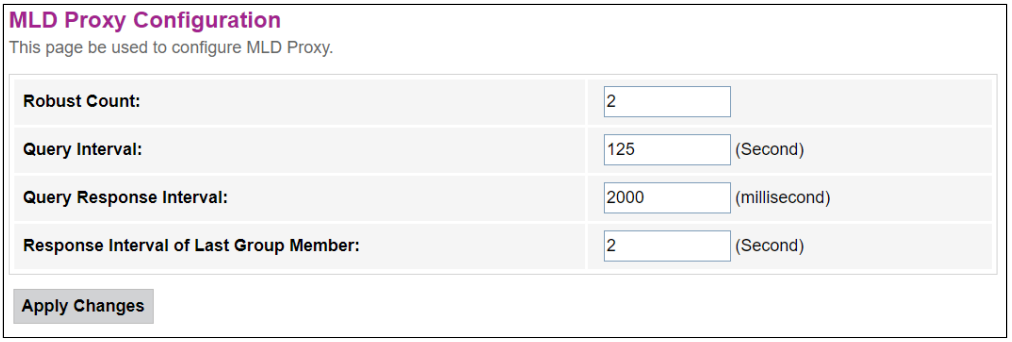
- *DHCPv6 Mode* – выбор режима:
  - *NONE* – работа без DHCP-сервера;
  - *DHCPRelay* – работа в режиме DHCP-ретранслятора;
  - *DHCPServer* – настройка DHCP-сервера.

Для сохранения изменений нажмите кнопку «Apply Changes».

5.6.3.4 Подменю «MLD proxy». Настройка функции MLD proxy

В разделе можно настроить работу MLD proxy.

Advance → IPv6 → MLD proxy



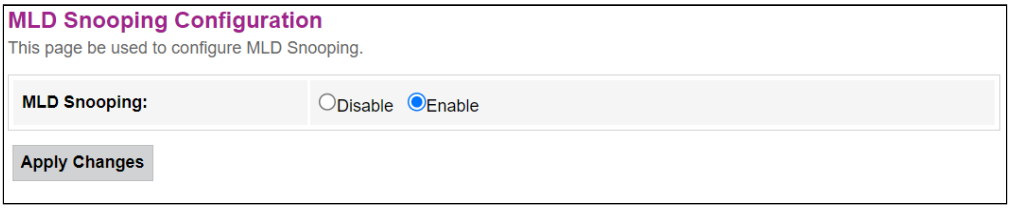
- *Robust Count* – количество попыток отправки сообщения MLD в случае потери пакета;
- *Query Interval* – интервал времени, указывающий частоту отправки сообщений Query;
- *Query Response Interval* – интервал времени, указывающий задержку ответа на сообщение Query от клиента;
- *Response Interval of Last Group Member* – количество отправляемых сообщений Group-Specific после выхода последнего клиента из группы.

Для сохранения изменений нажмите кнопку «Apply Changes».

5.6.3.5 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

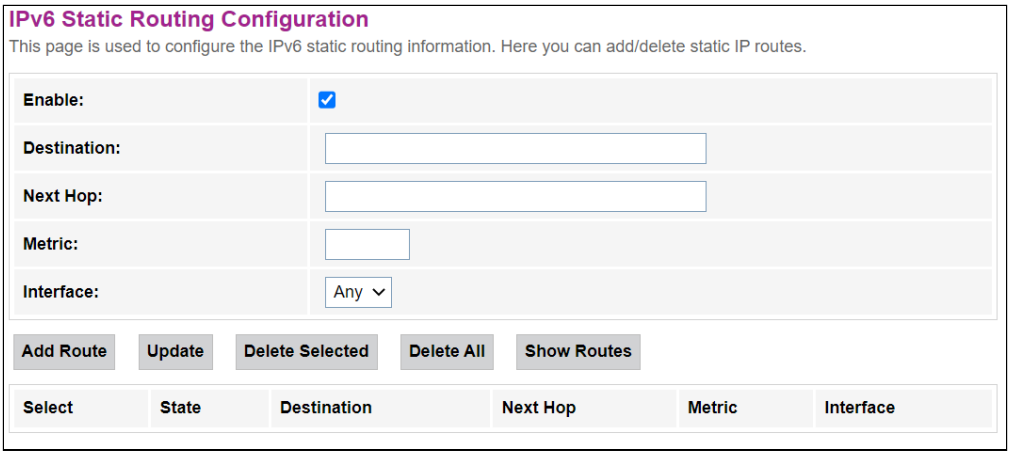


Для сохранения изменений нажмите кнопку «Apply Changes».

5.6.3.6 Подменю «IPv6 routing». Настройка IPv6-маршрутов

В разделе осуществляется настройка статических IPv6-маршрутов.

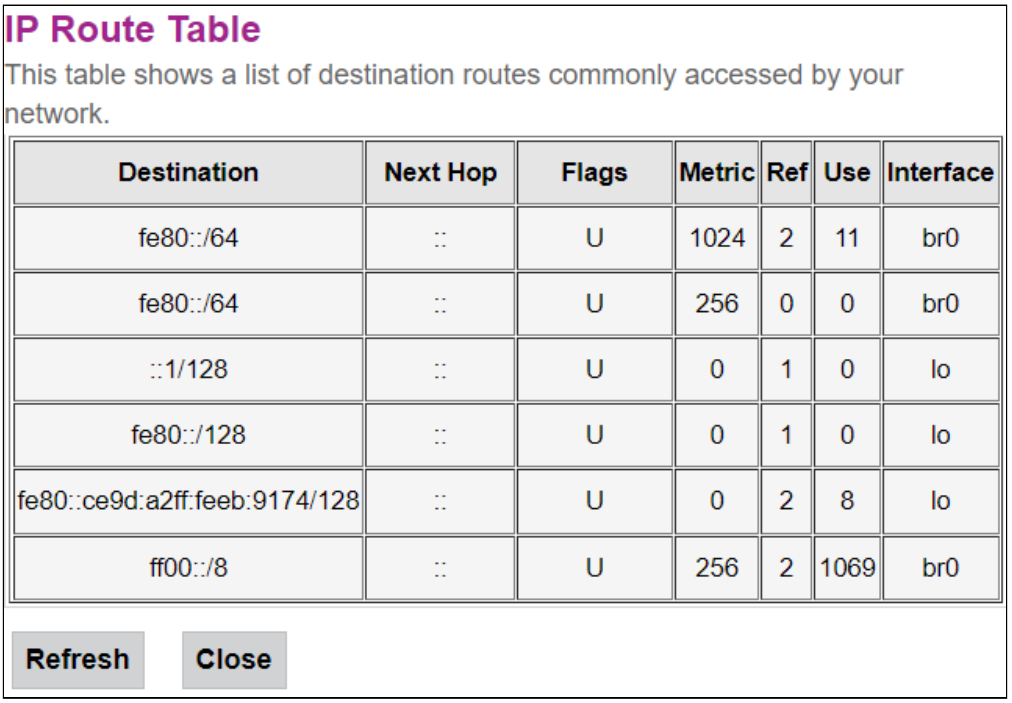
Advance → IPv6 → IPv6 routing



- *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 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



- *Destination* − сеть назначения;
- *Next Hop* − следующий узел;
- *Flags* − флаги;

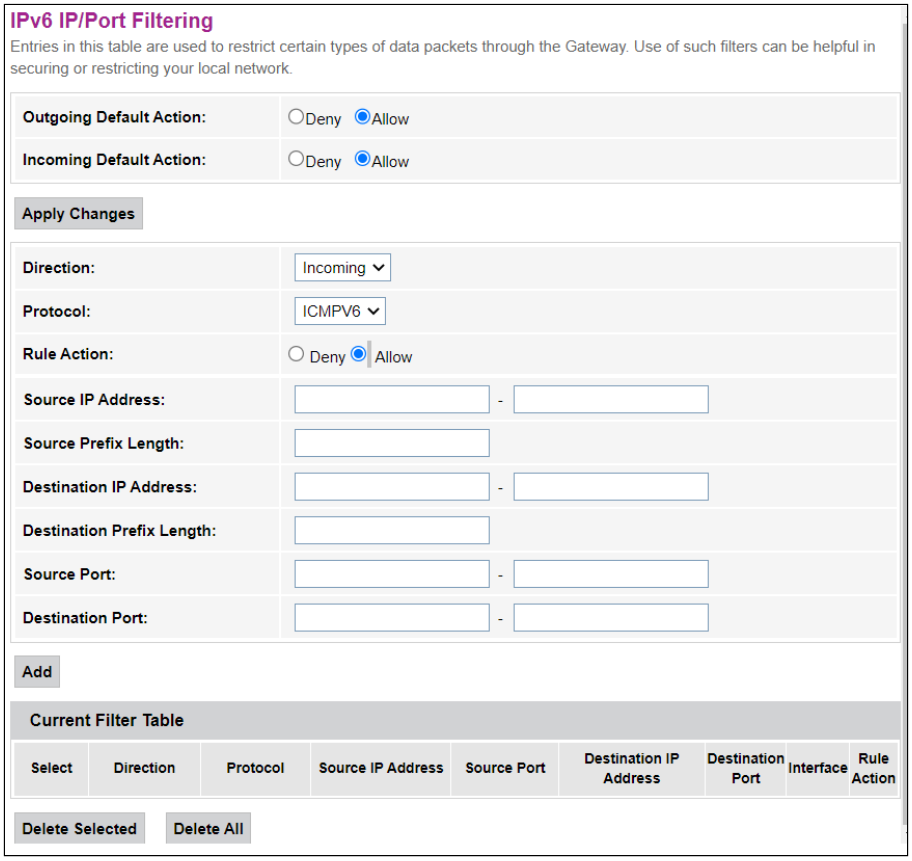
- *Metric* – метрика;
- *Ref* – источник маршрута;
- *Use* – использование маршрута;
- *Interface* – интерфейс, через который доступен указанный маршрут.

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

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

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

Advance → IPv6 → IP/Port filtering



- *Outgoing Default Action* – исходящее действие по умолчанию:
  - *Deny* – при установке флага прохождение трафика по умолчанию запрещено;
  - *Allow* – при установке флага прохождение трафика по умолчанию разрешено.
- *Incoming Default Action* – входящее действие по умолчанию:
  - *Deny* – при установке флага прохождение трафика по умолчанию запрещено;
  - *Allow* – при установке флага прохождение трафика по умолчанию разрешено.
- *Direction* – направление прохождения трафика:
  - *Outgoing* – исходящее направление;
  - *Incoming* – входящее направление.
- *Protocol* – выбор протокол;
- *Rule Action (Deny/Allow)* – политика обработки пакета (отбросить/пропустить);
- *Source IP Address* – IP-адрес источника;
- *Source Prefix Length* – длина префикса источника;
- *Destination IP Address* – IP-адрес назначения;
- *Destination Prefix Lenght* – длина префикса назначения;
- *Source Port* – порт источника;
- *Destination Port* – порт назначения.

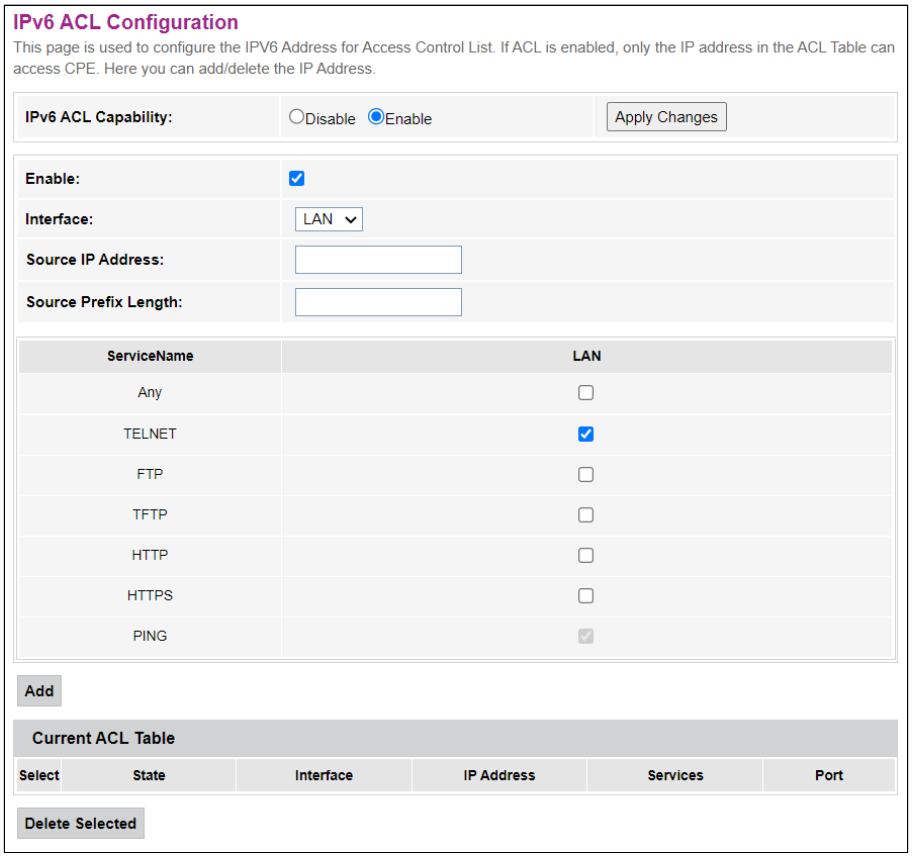
Чтобы добавить фильтр, заполните соответствующие поля и нажмите кнопку «Add». Добавленные фильтры отображаются в таблице *«Current Filter Table»*. Для удаления всей таблицы нажмите на кнопку «Delete All», чтобы удалить один фильтр, выберите его и нажмите кнопку «Delete Selected».

5.6.3.8 Подменю «IPv6 ACL». Настройка конфигурации IPv6 ACL

На странице осуществляется настройка доступа к устройству по протоколу IPv6,

Управление доступом может быть настроено как со стороны WAN, так и со стороны LAN.

Advance → IPv6 → IPv6 ACL



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

- *IPv6 ACL Capabillity* – включение функционала управления доступа к устройству;
- *Enable* – активация правила IPv6 ACL;
- *Interface* – выбор интерфейса для правила IPv6 ACL;
- *Source IP Address/Source Prefix Lenght* – настройка хостов, которым будет разрешён доступ к устройству;
- *Services* – настройка сервисов, по которым будет разрешён доступ к устройству. Доступ может быть настроен по протоколам ICMP, Telnet, HTTP. При настройке доступа со стороны LAN возможна настройка доступа без ограничений.

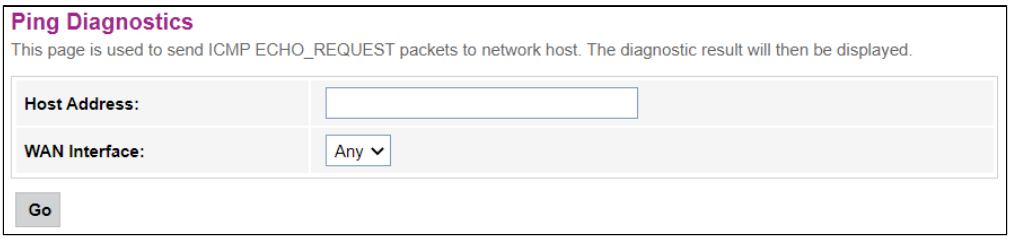
После заполнения полей для добавления записи нажмите кнопку «Add». Для удаления определённой позиции выделите её и нажмите кнопку «Delete Selected».

5.7 Меню «Diagnostics»

5.7.1 Подменю «Ping». Проверка доступности сетевых устройств

Раздел предназначен для проверки доступности сетевых устройств при помощи утилиты Ping, используя протокол ICMP.

Diagnostics → Ping



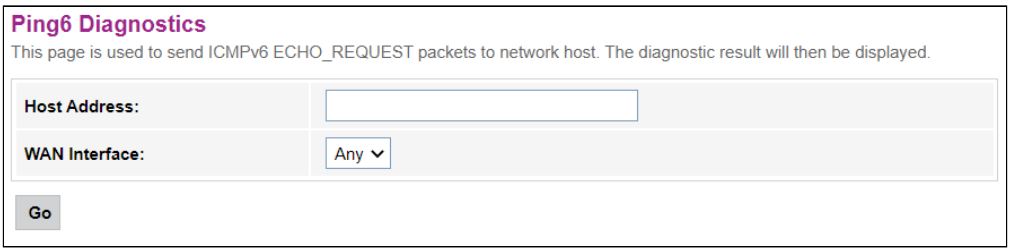
- *WAN Interface* – интерфейс, через который будет производится проверка доступности.

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

Подменю «Ping6». Проверка доступности сетевых устройств

Раздел предназначен для проверки доступности сетевых устройств при помощи утилиты Ping, используя протокол ICMPv6.

Diagnostics → Ping6



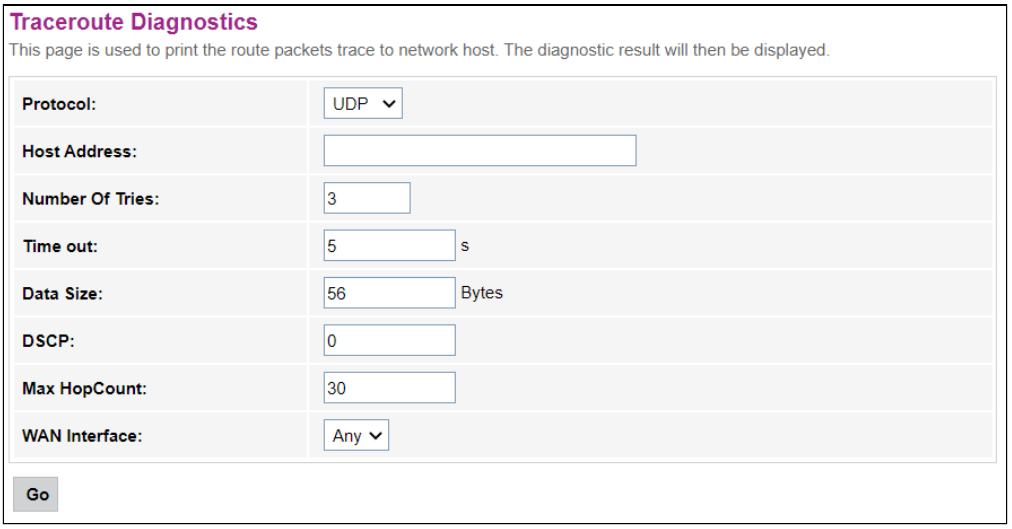
- *WAN Interface* – интерфейс, через который будет производится проверка доступности.

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

5.7.2 Подменю «Traceroute». Настройка трассировки пакетов IPv4

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

Diagnostics → Traceroute



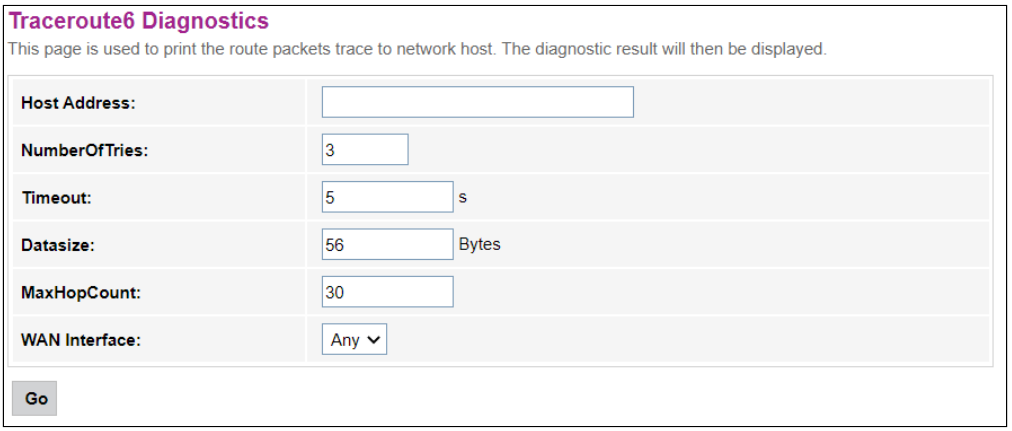
- *Protocol* – протокол, используемый при трассировке;
- *Host Address* – адрес устройства, до которого будет производится трассировка;
- *Number Of Tries* – количество попыток трассировки;
- *Time out* – время ожидания ответа на пакет;
- *Data Size* – размер данных пакета в байтах;
- *DSCP* – значение Differentiated services codepoint в отправляемых пакетах;
- *Max HopCount* – максимальное количество узлов для маршрутизации пакета;
- *WAN Interface* – интерфейс, через который будет производится трассировка.

Для диагностики сети заполните поля и нажмите кнопку «Go».

5.7.3 Подменю «Traceroute6». Настройка трассировки пакетов IPv6

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

Diagnostics → Traceroute6



- *Host Address* – адрес устройства, до которого будет производится трассировка;
- *Number Of Tries* – количество попыток трассировки;
- *Time out* – время ожидания ответа на пакет;
- *Data Size* – размер данных пакета в байтах;

- *Max HopCount* – максимальное количество узлов для маршрутизации пакета;
- *WAN Interface* – интерфейс, через который будет производится трассировка.

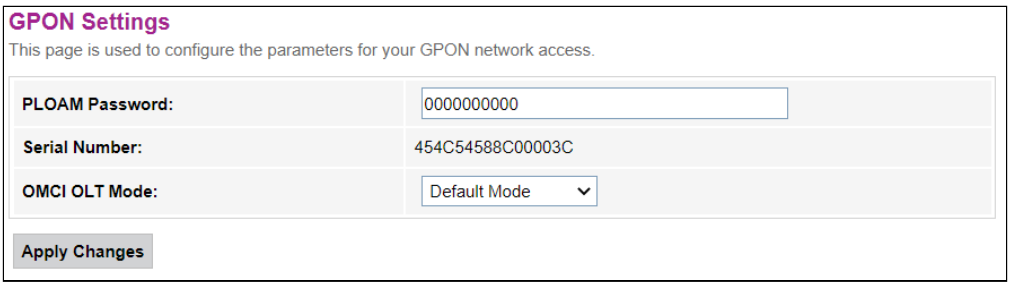
Для диагностики сети заполните поля и нажмите кнопку «Go».

5.8 Меню «Admin»

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

5.8.1 Подменю «GPON Settings». Настройка доступа к GPON

Admin → GPON Settings

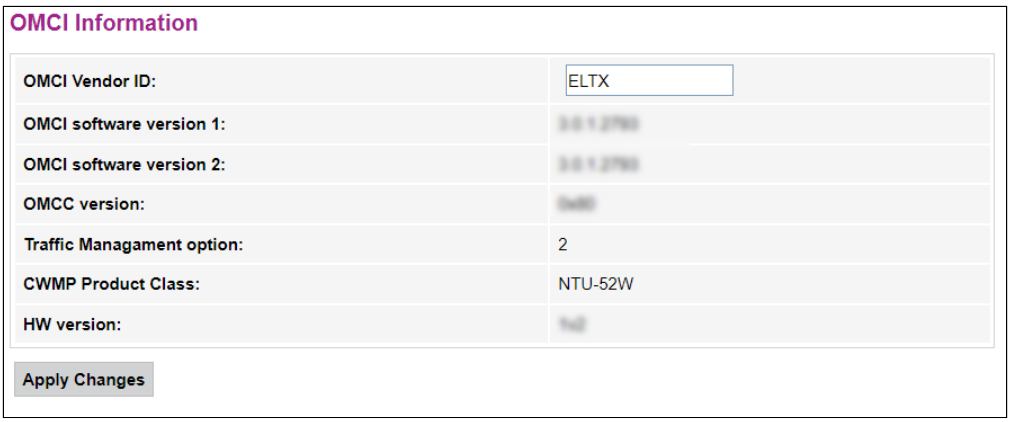


- *PLOAM Password* – пароль для активации терминала на OLT;
- *Serial Number* – PON серийный номер CPE.

Для сохранения изменений нажмите кнопку «Apply Changes».

5.8.2 Подменю «OMCI Information»

Admin → OMCI Information



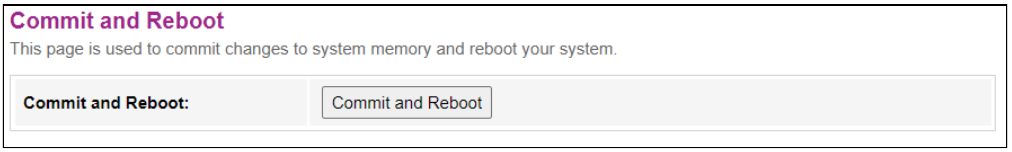
- *OMCI Vendor ID* – наименование производителя;
- *OMCI software version 1* – версия ПО в первой области;
- *OMCI software version 2* – версия ПО во второй области;
- *OMCC version* – версия канала управления OMCI;
- *Traffic Managment option* – значение приоритета трафика;
- *CWMP Product Class* – наименование модели устройства;
- *HW version* – версия аппаратного обеспечения.

Для сохранения изменений нажмите кнопку «Apply Changes».

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

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

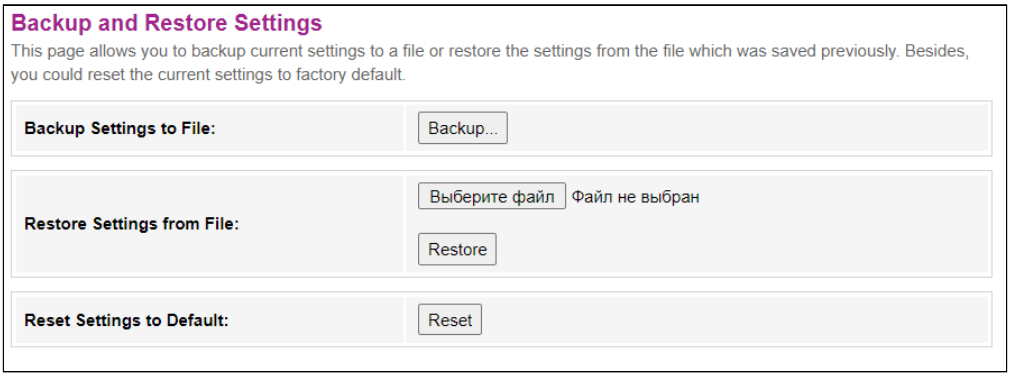
Admin → Commit/Reboot



5.8.4 Подменю «Backup/Restore». Восстановление и сброс настроек

В разделе можно скопировать текущие настройки в файл (*Backup Settings)* нажатием на кнопку «Backup Settings to File», восстановить настройки из файла, который был сохранен ранее (*Update Settings)* кнопкой «Restore» и сбросить текущие настройки до заводских настроек по умолчанию (*Restore Default),* для этого нажмите кнопку «Reset Settings to Default».

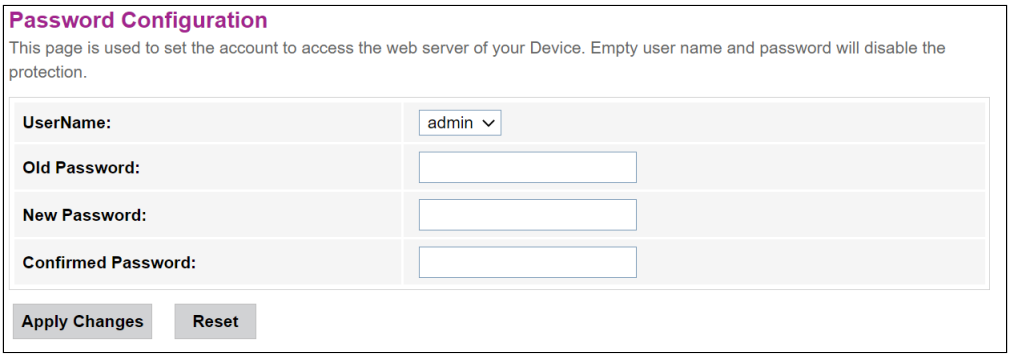
Admin → Backup/Restore



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

В разделе осуществляется смена пароля для доступа к устройству.

Admin → Password



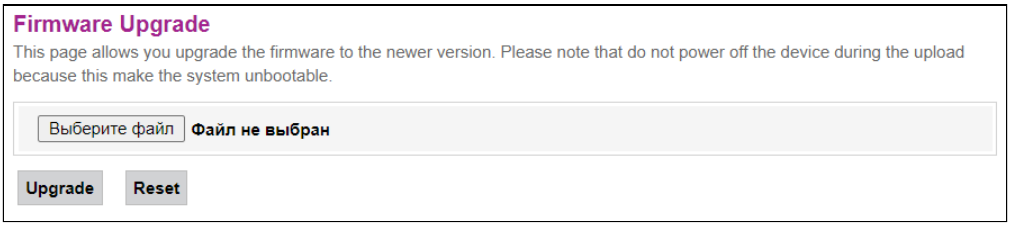
Для смены пароля необходимо ввести существующий пароль в поле *Old Password*, затем новый пароль в *New Password* и подтвердить его *Confirmed Password*.

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

5.8.6 Подменю «Firmware upgrade». Обновление ПО

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

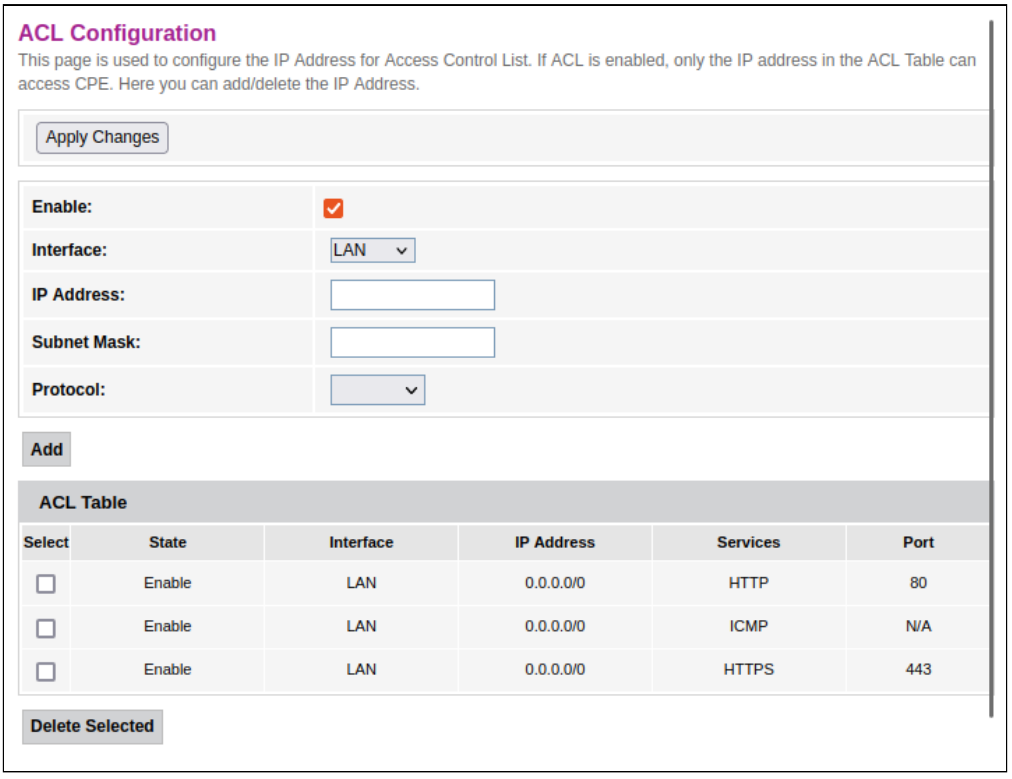
Admin → Firmware upgrade



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

5.8.7 Подменю «ACL»

Admin → Firmware upgrade



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

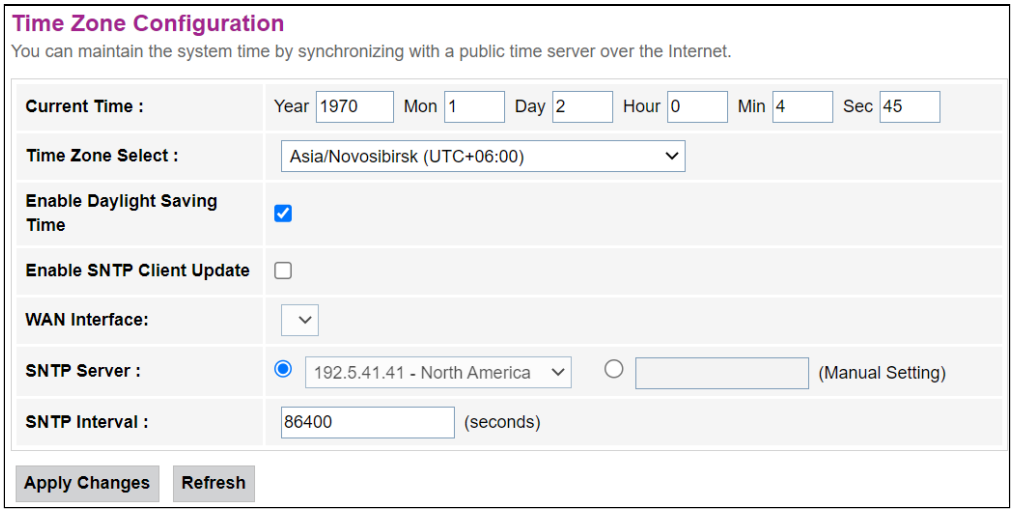
- *Interface* – выбор интерфейса;
- *IP Address* – IP-адрес источника;
- *Subnet Mask* – маска подсети;
- *Protocol* – используемый протокол.

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

5.8.8 Подменю «Time zone». Настройки системного времени

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

Admin → Time zone



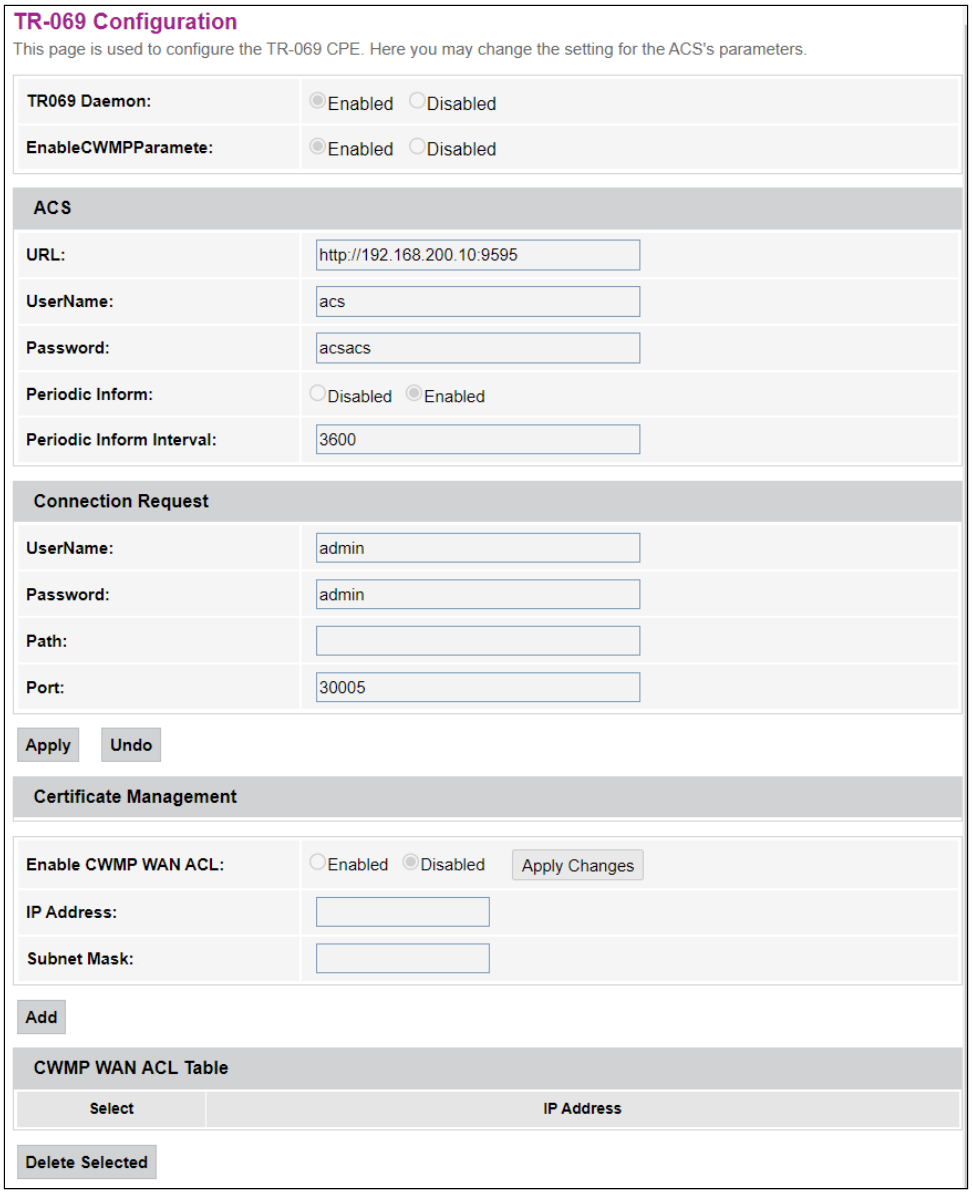
- *Current time* – текущее время;
- *Time Zone Select* – временная зона;
- *Enable Daylight Saving Time* – переход на летнее время;
- *Enable SNTP Client Update* – включить синхронизацию времени по SNTP;
- *WAN Interface* – интерфейс, через который производится обновление времени;
- *SNTP Server* – предпочитаемый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

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

5.8.9 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.

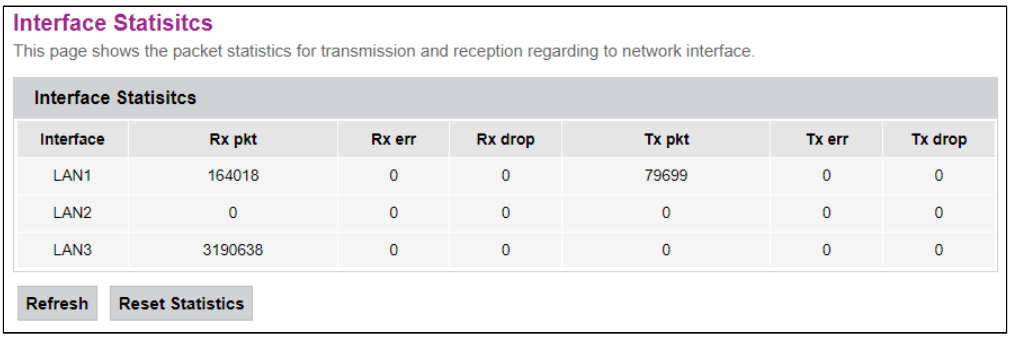
Для сохранения изменений нажмите кнопку «Apply», для сброса – «Undo». Чтобы загрузить выбранный файл, нажмите кнопку «Upload». После заполнения полей для добавления записи нажмите кнопку «Add». Хтобы удалить одну позицию из списка, выделите её и нажмите кнопку «Delete Selected».

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

5.9.1 Подменю «Interface». Информация о счетчиках и ошибках

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

Statistics → Interface

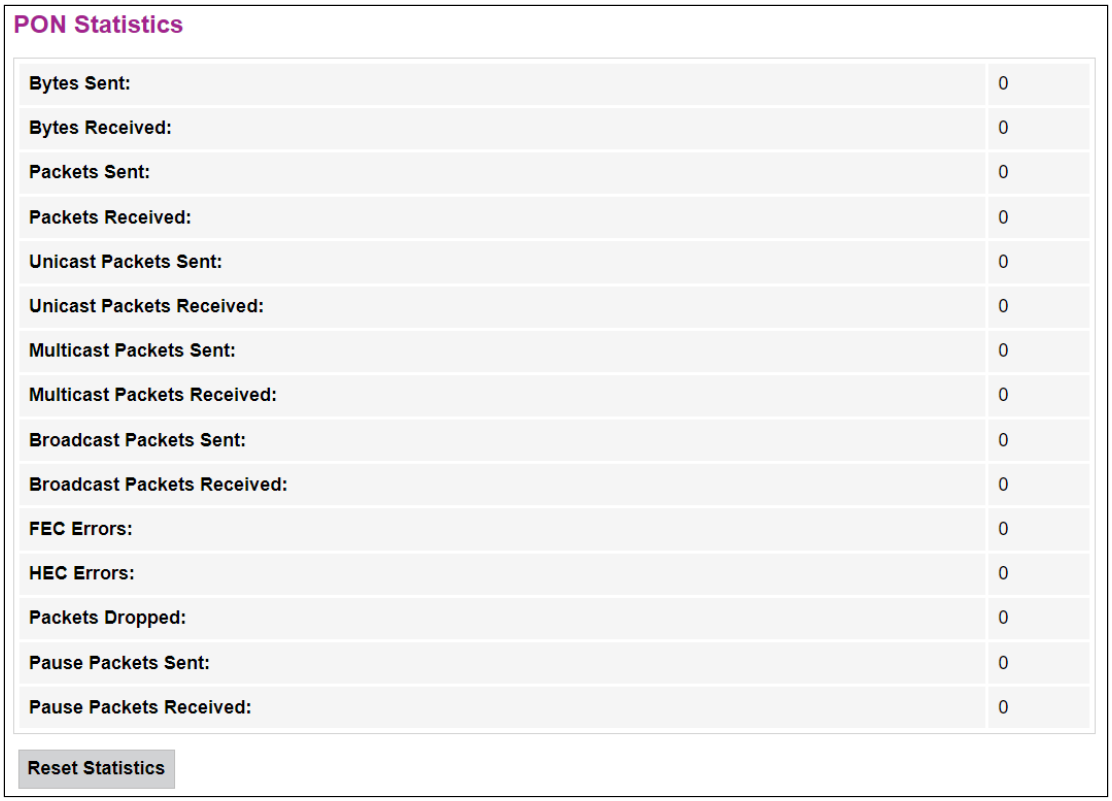


- *Interface* – интерфейс;
- *Rx pkt* – получено пакетов;
- *RX err* – ошибки на приеме;
- *Rx drop* – отброшено на приеме;
- *Tx pkt* – отправлено пакетов;
- *Tx err* – ошибка отправки;
- *Tx drop* – отброшено при передаче.

5.9.2 Подменю «PON». Информация о счетчиках для оптического интерфейса

В разделе отображается счетчики для оптического интерфейса.

Statistics → PON



- *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* – остановленных пакетов отправлено;
- *Pause Packets Received* – остановленных пакетов получено.

6 Список изменений

Версия документа	Актуальность для ПО	Дата выпуска	Содержание изменений
Версия 1.2	3.0.3	07.2023	Третья публикация
Версия 1.1	3.0.2	03.2023	Вторая публикация
Версия 1.0	3.0.1	02.2023	Первая публикация

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: http://eltex-co.ru/support/

E-mail: techsupp@eltex.nsk.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: http://eltex-co.ru

Технический форум: http://eltex-co.ru/forum

База знаний: http://eltex-co.ru/support/knowledge

Центр загрузок: http://eltex-co.ru/support/downloads