Комплексные решения для построения сетей

NTU-2V
NTU-RG-1402G-W

Руководство по эксплуатации, версия 1.2 (14.07.2016)

Абонентские оптические терминалы

IP-адрес: 192.168.1.1
имя пользователя: user
пароль: user

http://eltex.nsk.ru/support/downloads

Версия документа	Дата выпуска	Содержание изменений
Версия 1.2	14.07.2016	Третья публикация
Версия 1.1	16.11.2015	Вторая публикация
Версия 1.0	21.05.2014	Первая публикация
Версия ПО **NTU-RG 2.14.2.348** **NTU-2V 2.14.2.349**		

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.

СОДЕРЖАНИЕ

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 Gbps в направлении downlink и 1.25 Gbps 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 конвертором интерфейсов Gigabit Ethernet и GPON, служащим для связи сети PON с сетями передачи данных более высокого уровня. ONT предназначено для подключения к услугам широкополосного доступа оконечного оборудования клиентов. Может применяться в жилых комплексах и бизнес-центрах.

Линейка оборудования ONT NTU производства «Элтекс» представлена терминалами:

- NTU-2V , имеющим два UNI интерфейса (*user network interfaces* – абонентские сетевые интерфейсы) Ethernet: **1 порт Ethernet 100 Base-TX, 1 порт Ethernet 10/100/1000 Base-T** и один порт FXS;

- NTU-RG-1402G-W, которые рассчитаны на четыре UNI интерфейса 10/100/1000Base-T и поддержку интерфейсов FXS, Wi-Fi, USB.

В настоящем руководстве по эксплуатации изложены назначение, основные технические характеристики, правила конфигурирования, мониторинга и смены программного обеспечения оптических терминалов серии *NTU-RG* и устройств серии *NTU-2.*

2 ОПИСАНИЕ ИЗДЕЛИЯ

2.1 Назначение

Устройства *NTU-2V, NTU-RG* GPON ONT (Gigabit Ethernet Passive Optical Network) – высокопроизводительные абонентские терминалы, предназначенные для связи с вышестоящим оборудованием пассивных оптических сетей и предоставления услуг широкополосного доступа конечному пользователю. Связь с сетями GPON реализуется посредством PON интерфейса, для подключения оконечного оборудования клиентов служат интерфейсы Ethernet.

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.

Благодаря встроенному маршрутизатору, устройства обеспечивают возможность подключения оборудования локальной сети к сети широкополосного доступа. Терминалы обеспечивают защиту межсетевым экраном для компьютеров в сети от атак DoS и вирусных атак, осуществляют фильтрацию пакетов для осуществления управления доступом на основе портов и MAC/IP-адресов источника/назначения. Пользователи могут настроить домашний или офисный Web-сайт, добавив один из LAN-портов в зону DMZ. Функция Родительский контроль обеспечивает фильтрацию Web-сайтов с нежелательным содержимым, блокировку доменов и позволяет задавать расписание использования Интернета. Виртуальная частная сеть (VPN) предоставляет мобильным пользователям и филиалам защищенный канал связи для подключения к корпоративной сети.

Порты FXS позволяют пользоваться услугами IP-телефонии, предоставляя множество полезных функций, таких как отображение идентификатора звонящего, трехстороннюю конференцию, телефонную книгу, ускоренный набор. Все это обеспечивает удобство пользователя при наборе номера и приеме телефонных звонков.

Порт USB может использоваться для подключения USB-устройств (USB-флеш-накопитель, внешний HDD).

Абонентский маршрутизатор NTU-RG-1402G-W позволяет подключать клиентов Wi-Fi по стандарту IEEE 802.11b/g/n. Абонентский маршрутизатор NTU-RG-1402G-Wac поддерживает стандарт 802.11ac, что обеспечивает рекордную скорость передачи данных до 1Гбит/с и позволяет доставлять современные высокоскоростные сервисы клиентскому оборудованию по беспроводной сети.

2.2 Варианты исполнения

Устройства серий *NTU-2V* и *NTU-RG* отличаются набором интерфейсов и функциональными возможностями (см. табл. 1).

Таблица 1 – Варианты исполнения

Наименование модели	WAN	LAN	FXS	Wi-Fi	USB
NTU-2V	1xGPON	1x1Gigabit 1x100Megabit	1	-	-
NTU-RG-1402G-W	1xGPON	4x1Gigabit	2	+	2
NTU-RG-1402G-Wac	1xGPON	4x1Gigabit	2	+	2

2.3 Характеристика устройства

Устройство имеет следующие интерфейсы:

- Порты RJ-11 для подключения аналоговых телефонных аппаратов:
  - Для моделей NTU-RG: 2 порта RJ-11;
  - Для моделей NTU-2: 1 порт RJ-11;
- 1 порт PON SC/APC для подключения к сети оператора;
- Порты Ethernet RJ-45 LAN для подключения сетевых устройств:
  - Для моделей NTU-RG: 4 порта RJ-45 10/100/1000Base-T;
  - Для моделей NTU-2: 1 порт RJ-45 100 Base-TX, 1 порт RJ-45 10/100/1000Base-T;
- Приемопередатчик Wi-Fi[1] 802.11ac[2], 802.11n, 802.11b, 802.11g;
- 2 порта USB2.0[1] - для подключения внешних накопителей USB или HDD.

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

Устройство поддерживает следующие функции:

- *сетевые функции:*
  - работа в режиме «моста» или «маршрутизатора»;
  - поддержка PPPoE (PAP, CHAP, MSCHAP авторизация);
  - поддержка статического адреса и DHCP (DHCP-клиент на стороне WAN, DHCP-сервер на стороне LAN);
  - поддержка UPNP;
  - поддержка IPSec;
  - поддержка NAT;
  - поддержка Firewall;
  - поддержка NTP;
  - поддержка механизмов качества обслуживания QoS;
  - поддержка IGMP-snooping;
  - поддержка IGMP-proxy;
  - поддержка функции Parental Control;
  - поддержка функции Storage service.
- *IP-телефония:*
  - поддержка протокола SIP;
  - аудиокодеки: G.729 (A), G.711(A/U), G.723.1;
  - ToS для пакетов RTP;
  - ToS для пакетов SIP;
  - эхо компенсация (рекомендации G.164, G.165);
  - детектор тишины (VAD);
  - генератор комфортного шума;
  - обнаружение и генерирование сигналов DTMF;
  - передача DTMF (INBAND, RFC2833, SIP INFO);
  - передача факса: upspeed/pass-through. G.711, T.38;
- *функции ДВО:*
  - удержание вызова – Call Hold;
  - передача вызова – Call Transfer;
  - уведомление о поступлении нового вызова – Call Waiting;
  - безусловная переадресация - Forward unconditionally;

[1] Только для NTU-RG

[2] Только для NTU-RG-1402G-Wac

- переадресация по неответу - Forward on "no answer";
- переадресация по занятости – Forward on “busy”;
- определитель номера Caller ID по ETSI FSK;
- запрет выдачи Caller ID (анонимный звонок) - Anonymous calling;
- теплая линия - Warmline;
- гибкий план нумерации;
- индикация о наличии сообщений на голосовой почте - MWI;
- блокировка анонимных звонков - Anonymous call blocking;
- запрет на исходящие вызовы - Call Barring;
- "не беспокоить" – DND.

- обновление ПО через Web-интерфейс, TR-069, OMCI;

- удаленный мониторинг, конфигурирование и настройка:
  - TR-069;
  - Web-интерфейс;
  - OMCI;
  - Telnet.

На рисунке 1 приведена схема применения оборудования NTU.

Схема применения

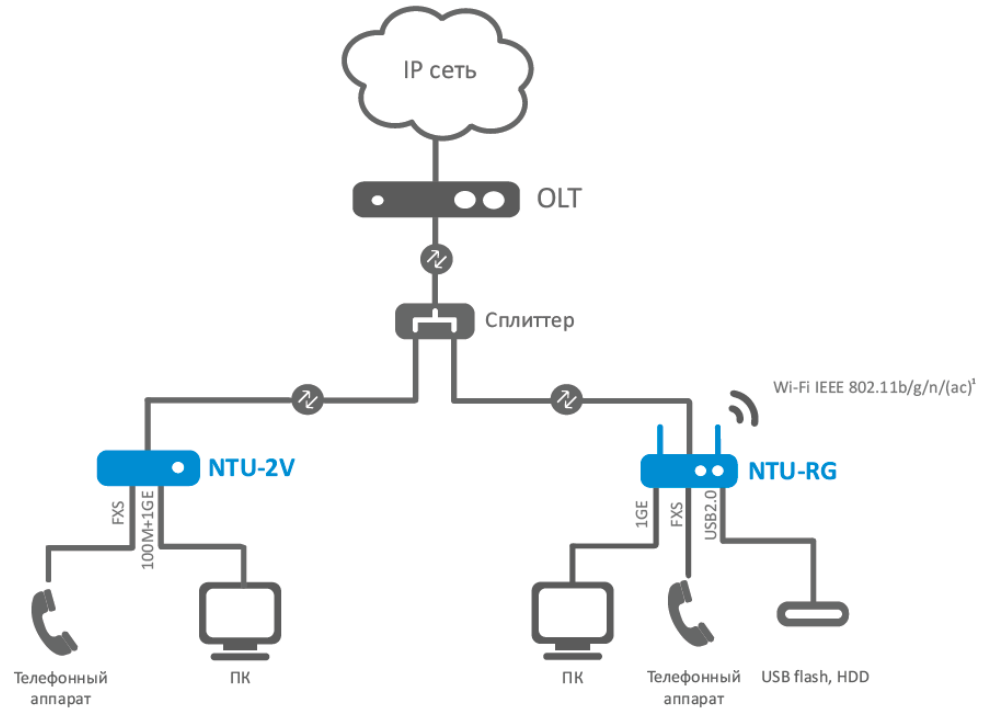


Рисунок 1– Схема применения NTU-2, NTU-RG-1402G-W

2.4 Основные технические параметры

Основные технические параметры терминалов приведены в таблице 2.

Таблица 2. Основные технические параметры

Протоколы VoIP

Поддерживаемые протоколы	SIP

Аудиокодеки

Кодеки	G.729, annex A G.711(A/μ) G.723.1 (5,3 Kbps) Передача факса: G.711, T.38

Параметры интерфейсов Ethernet LAN

Количество интерфейсов	Серия NTU-2	2
	Серия NTU-RG	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

Параметры интерфейса PON

Количество интерфейсов PON	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 FSAN Class B+ SFF-8472 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
Среда передачи	оптоволоконный кабель SMF - 9/125, G.652
Коэффициент разветвления	до 1:64
Максимальная дальность действия	20 км
Передатчик:	1310Нм
Скорость соединения upstream	1244Mb/s
Мощность передатчика	+0,5 до +5 dBm
Ширина спектра опт. излучения (-20дБ)	1 nm
Приемник	1490Нм
Скорость соединения downstream	2488Mb/s
Чувствительность приемника	от -8 до -28 dBm

Параметры аналоговых абонентских портов

количество портов	NTU-2	1
	NTU-RG	2
сопротивление шлейфа		до 2 кОм
прием набора		импульсный/частотный (DTMF)
выдача Caller ID		есть

Параметры беспроводного интерфейса Wi-Fi

Модель	**NTU-RG-1402G-W**	**NTU-RG-1402G-Wac**
Стандарт	IEEE 802.11b/g/n	802.11a/b/g/n, 802.11a/an/ac
Частотный диапазон	2.400 ~ 2.497 ГГц	2400 ~ 2483,5 МГц, 4900-5850 МГц
Модуляция	PSK/CCK, DQPSK, DBPSK, OFDM	BPSK, QPSK, 16 QAM, 64 QAM, 256 QAM, CCK
Скорость передачи данных, Мбит/с	**802.11b**: 11, 5.5, 2, 1 **802.11g**: 54, 48, 36, 24, 18,12, 9, 6 **802.11n 20MHz BW:** 130, 117, 104, 78, 52, 39, 26, 13 **802.11n 40MHz BW:** 270, 243, 216, 162, 108, 81, 54, 27	**802.11b/g/gn:** 1-13 (2412-2472 МГц) **802.11a/ac:** 36-64(5180 - 5320 МГц), 100-140 (5500 - 5700 МГц), 149-165 (5745 - 5825 МГц) **20&40 МГц:** 6, 9, 12 , 18, 24, 36, 48, 54, MCS0-MCS23, MCS0-8 NSS1, MCS0-9 NSS3 **802.11n 20MHz BW:** 216,7 **802.11n 40MHz BW:** 450 **802.11ac:** 1299 Мбит/с (80 МГц)
Максимальная выходная мощность передатчика	**802.11b:** 17dBm +/-1.5dBm **802.11g:** 15dBm +/-1.5dBm **802.11n:** 14.75dBm +/-1.5dBm	
MAC-протокол	CSMA/CA модель ACK 32 MAC	
Безопасность	64/128-битное WEP-шифрование данных; WPA, WPA2	
Поддержка операционной системы	Windows XP 32/64, Windows Vista 32/64, Windows 2000, Windows 7 32/64 Linux, VxWorks	
Количество антенн	NTU-RG-1402G-W	2
	NTU-RG-1402G-Wac	3
Коэффициентом усиления антенны	5 dBi	
Рабочий диапазон температур	от 0 до +70°C	

Управление

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

Общие параметры

Питание		адаптер питания 12V DC /220 AC
Потребляемая мощность	NTU-2V	не более 5 Вт
	NTU-RG-1402G-W	не более 15 Вт
	NTU-RG-1402G-Wac	не более 15 Вт
Рабочий диапазон температур		от +5 до +40°C
Относительная влажность		до 80%
Габариты	NTU-2V	122×96×32 мм
	NTU-RG	187x120x32 мм
Масса	NTU-2V	0,25 кг
	NTU-RG	0,3 кг

2.5 Конструктивное исполнение

2.5.1 NTU-2V

Устройства серии NTU-2V выполнены в виде настольного изделия в пластиковом корпусе размерами 122×96×32 мм.

Внешний вид задней панели устройства NTU-2(V) приведен на рисунке 2.

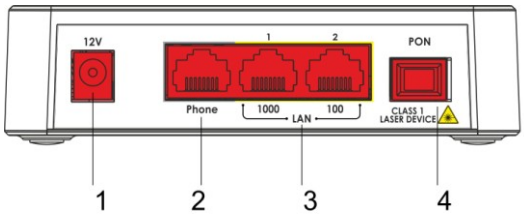


Рисунок 2 – Внешний вид задней панели NTU-2V

На задней панели устройства NTU-2V расположены следующие разъемы и органы управления, таблица 3.

Таблица 3 – Описание индикаторов и органов управления задней панели

Элемент задней панели		**Описание**
1	***12V***	разъем для подключения адаптера питания
2	***Phone***	разъем RJ-11 для подключения аналогового телефонного аппарата
3	***LAN 1000***	разъем RJ-45 10/100/1000Base-T для подключения сетевых устройств
	LAN 100	разъем RJ-45 100Base-TX для подключения сетевых устройств
4	***PON***	разъем SC (розетка) PON оптического интерфейса GPON для подключения к сети PON

Внешний вид боковой и верхней панели устройства NTU-2V приведен на рисунке 3.

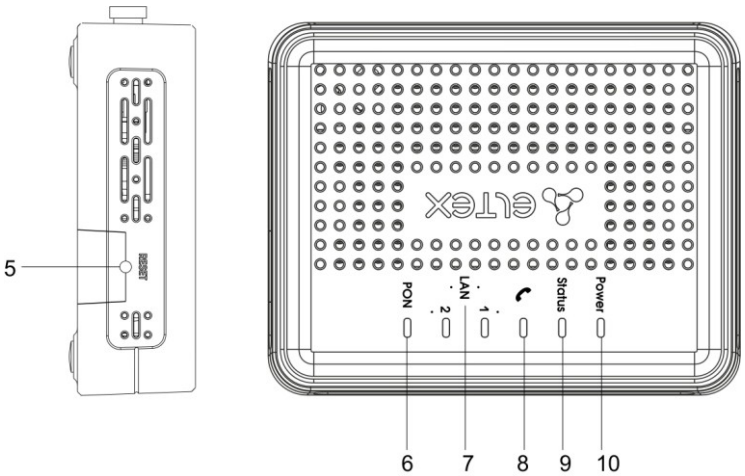


Рисунок 3 – Внешний вид верхней панели NTU-2V

На боковой и верхней панели устройства NTU-2V расположены следующие органы управления и световые индикаторы, таблица 4.

Таблица 4 – Описание индикаторов и органов управления боковой и верхней панели

Элемент панелей		Описание
5	***Reset***	функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам
6	***PON***	индикатор работы оптического интерфейса
7	***LAN***	индикаторы работы Ethernet-портов
8		индикатор работы аналогового телефонного аппарата
9	***Status***	индикатор сигнализации прохождения авторизации устройства
10	***Power***	индикатор питания и статуса работы устройства

2.5.1.1 **NTU-RG**

Абонентский терминал NTU-RG-1402G-W выполнен в виде настольного изделия в пластиковом корпусе.

Внешний вид задней панели устройства NTU-RG-1402G-W приведен на рисунке 4.

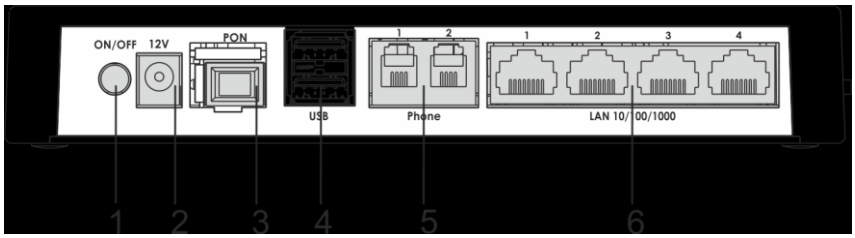


Рисунок 4 – Внешний вид задней панели NTU-RG-1402G-W

На задней панели устройства расположены следующие разъемы и органы управления, таблица 5.

Таблица 5 – Описание разъемов, и органов управления задней панели

№	Элемент задней панели	Описание
1	***On/Off***	кнопка питания
2	***12V***	разъем подключения адаптера питания
3	***PON***	разъем SC (розетка) *PON* оптического интерфейса GPON
4	***USB***	2 разъема для подключения внешних накопителей и других USB-устройств
5	***Phone 1, Phone 1***	2 разъема RJ-11 для подключения аналоговых телефонных аппаратов
6	**LAN 10/100/1000 1..4**	4 разъема RJ-45 для подключения сетевых устройств

Внешний вид боковой и верхней панелей устройства NTU-RG-1402G-Wприведен на Рисунке 5.

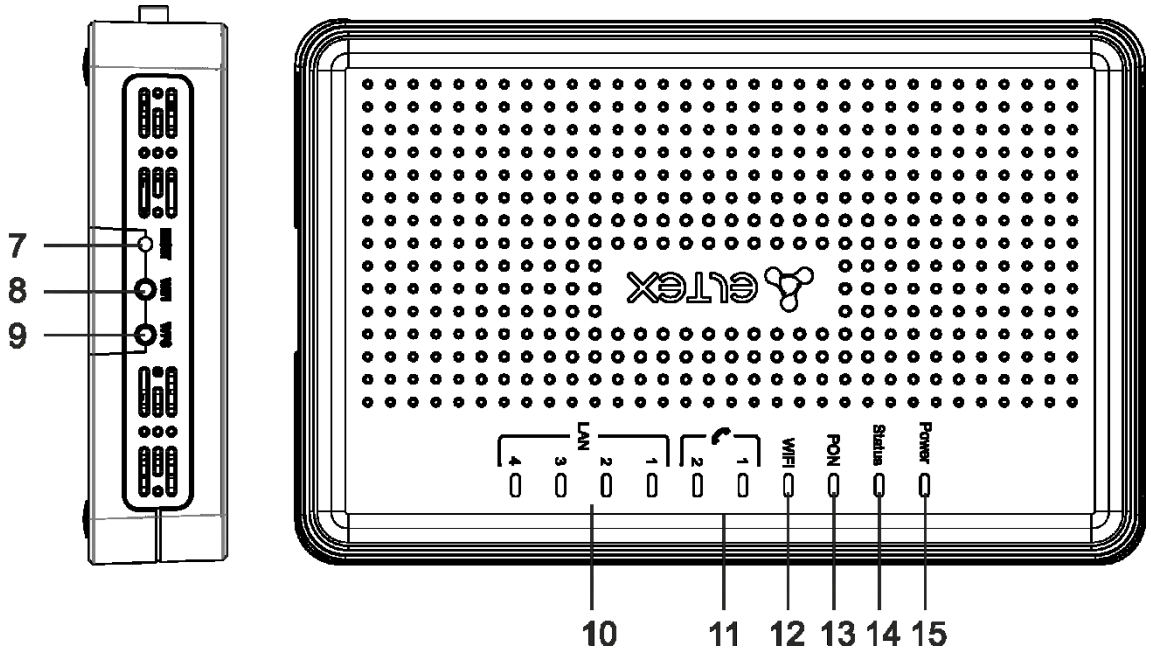


Рисунок 5 – Внешний вид боковой и верхней панели NTU-RG-1402G-W

На боковой панели устройства расположены следующие кнопки, таблица 6.

Таблица 6 – Описание кнопок боковой панели

№	Элемент боковой панели	Описание
7	***Reset***	функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам
8	***Wi-Fi***	кнопка включения/выключения Wi-Fi
9	***WPS***	кнопка для автоматического защищенного подключения к сети Wi-Fi на устройстве

На верхней панели устройства расположены следующие световые индикаторы, таблица 7.

Таблица 7 – Описание индикаторов верхней панели

№	Элемент верхней панели	Описание
10	***LAN 1..4***	индикаторы работы Ethernet-портов
11	***1..2***	индикатор активности портов FXS
12	***Wi-Fi***	индикатор активности Wi-Fi
13	***PON***	индикатор работы оптического интерфейса
14	***Status***	индикатор сигнализации прохождения авторизации устройства
15	***Power***	индикатор питания и статуса работы

2.6 Световая индикация

2.6.1 NTU-2V

Текущее состояние устройства отображается при помощи индикаторов ***PON, LAN 1..2, Phone 1, Status, Power,*** расположенных на передней панели.

Перечень состояний индикаторов приведен в таблице 8.

Таблица 8 – Световая индикация состояния устройства

Индикатор	Состояние индикатора	Состояние устройства
PON	не горит	процесс загрузки устройства
	зеленый	установлено соединение между станционным оптическим терминалом и устройством
	мигает красным	нет сигнала от станционного оптического терминала
LAN 1..2	зеленый	установлено соединение 10/100 Мбит/с
	оранжевый	установлено соединение 1000 Мбит/с
	мигает	процесс пакетной передачи данных
Phone	горит	телефонная трубка снята
	мигает	порт не зарегистрирован или не пройдена авторизация на SIP-сервере
	медленно мигает	прием сигнала вызова
Status	не горит	установлен режим работы static или bridge для интерфейса wan, PPP-клиент не запущен
	зеленый	устройство успешно прошло авторизацию на станционном терминале (поднята PPP сессия на интерфейсе WAN)
	оранжевый	устройство не прошло авторизацию (PPP сессия не поднята на интерфейсе WAN)
Power	не горит	устройство отключено от сети питания или неисправно
	зеленый	текущая конфигурация устройства отличается от конфигурации по умолчанию
	оранжевый	установлена конфигурация по умолчанию
	красный	устройство находится в процессе загрузки

2.6.2 NTU-RG

Текущее состояние устройства отображается при помощи индикаторов ***LAN 1..4, Phone 1..2, Wi-Fi, PON, Status, Power,*** расположенных на передней панели.

Перечень состояний индикаторов приведен в таблице 9.

Таблица 9 – Световая индикация устройства

Индикатор	Состояние индикатора	Состояние устройства
LAN 1..4	зеленый	установлено соединение 10/100 Мбит/с
	оранжевый	установлено соединение 1000 Мбит/с
	мигает	процесс пакетной передачи данных
Phone 1..2	горит	телефонная трубка снята
	мигает	порт не зарегистрирован или не пройдена авторизация на SIP-сервере

	медленно мигает	прием сигнала вызова
Wi-Fi	зеленый	сеть Wi-Fi активна
	мигает	процесс передачи данных по Wi-Fi
	не горит	сеть Wi-Fi не активна
PON	не горит	процесс загрузки устройства
	зеленый	установлено соединение между станционным оптическим терминалом и устройством
	мигает красным	нет сигнала от станционного оптического терминала
Status	не горит	установлен режим работы static или bridge для интерфейса wan, PPP-клиент не запущен
	зеленый	устройство успешно прошло авторизацию на станционном терминале (поднята PPP сессия на интерфейсе WAN)
	оранжевый	устройство не прошло авторизацию (PPP сессия не поднята на интерфейсе WAN)
Power	не горит	устройство отключено от сети питания или неисправно
	зеленый	текущая конфигурация устройства отличается от конфигурации по умолчанию
	оранжевый	установлена конфигурация по умолчанию
	красный	устройство находится в процессе загрузки

2.6.3 Индикация интерфейсов LAN

Режимы работы, отображаемые индикаторами на портах LAN на задней панели устройства, приведены в Таблице 10.

Таблица 10 – Световая индикация интерфейсов LAN

Режимы работы	**Желтый индикатор**	**Зеленый индикатор**
Порт работает в режиме 1000Base-T, нет передачи данных	горит постоянно	горит постоянно
Порт работает в режиме 1000Base-T, есть передача данных	горит постоянно	мигает
Порт работает в режиме 10/100Base-TX, нет передачи данных	не горит	горит постоянно
Порт работает в режиме 10/100Base-TX, есть передача данных	не горит	мигает

2.7 Перезагрузка/сброс к заводским настройкам

Для перезагрузки устройства нужно однократно нажать кнопку «Reset» на боковой панели изделия. Для загрузки устройства с заводскими настройками необходимо нажать и удерживать кнопку «Reset» 7-10 секунд, пока индикатор POWER не загорится красным светом. 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.

2.8 Комплект поставки

В базовый комплект поставки устройства *NTU-2V, NTU-RG-1402G-W* входят:

- абонентский оптический терминал *NTU-2V, NTU-RG-1402G-W*;
- адаптер питания 220/12;
- руководство по эксплуатации.

3 АРХИТЕКТУРА NTU-RG-1402G-W

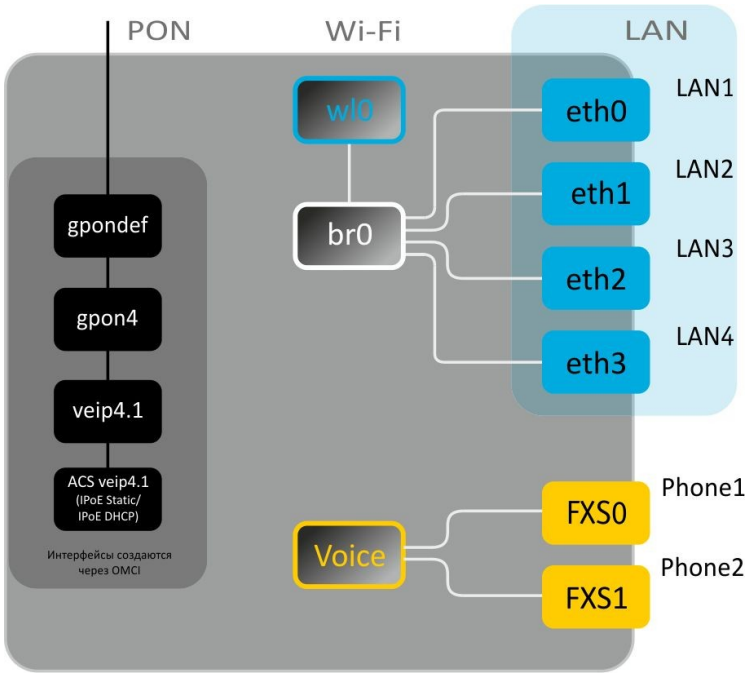


Рисунок 6 – Архитектура устройства с заводской конфигурацией

Основные элементы устройства

- **оптический приемо-передатчик (SFF-модуль)** - предназначен для преобразования оптического сигнала в электрический;
- **процессор (PON-чип) –** является конвертором интерфейсов Ethernet и GPON**;**
- **Wi-Fi модуль** – предназначен для организации беспроводного интерфейса на устройстве.

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

- br0;
- Voice (блок IP телефонии);
- eth0…3;
- FXS0…1;
- wl0.

Блок br0 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 FXS0..1 физически являются портами с разъемом RJ-11 для подключения аналоговых телефонных аппаратов. Логически включены в блок Voice. Управление блоком Voice может осуществляться через WEB-интерфейс, а также удаленно с помощью сервера ACS по протоколу TR-069. В данном блоке задаются параметры сервиса VoIP (адрес SIP сервера, номера телефонных аппаратов, услуги ДВО и т. д).

Блок wl0 является интерфейсом для подключения Wi-Fi-модуля.

При подключении к устройству ОВ (установлении успешного соединения со станционным оптическим устройством OLT) дополнительно создаются блоки **gpondef, gpon4, veip4, veip4.1 (ACS)** при помощи протокола OMCI (ONT Management and Control Interface).

Блок ACS может работать в 2-х режимах: IPoE Static (задание статического адреса для интерфейса veip4.1) и IPoE DHCP (получение адреса автоматически по протоколу DHCP). Блок используется для удаленного управления устройством с помощью сервера ACS (Auto Configuration Server – сервер автоконфигурации абонентских устройств). При помощи данного блока организуется взаимодействие с абонентским оборудованием, осуществляется обработка запросов от устройств ONT и подключаются сервисы.

На рисунке 7 представлена архитектура устройства, сконфигурированного для предоставления услуг Triple Play.

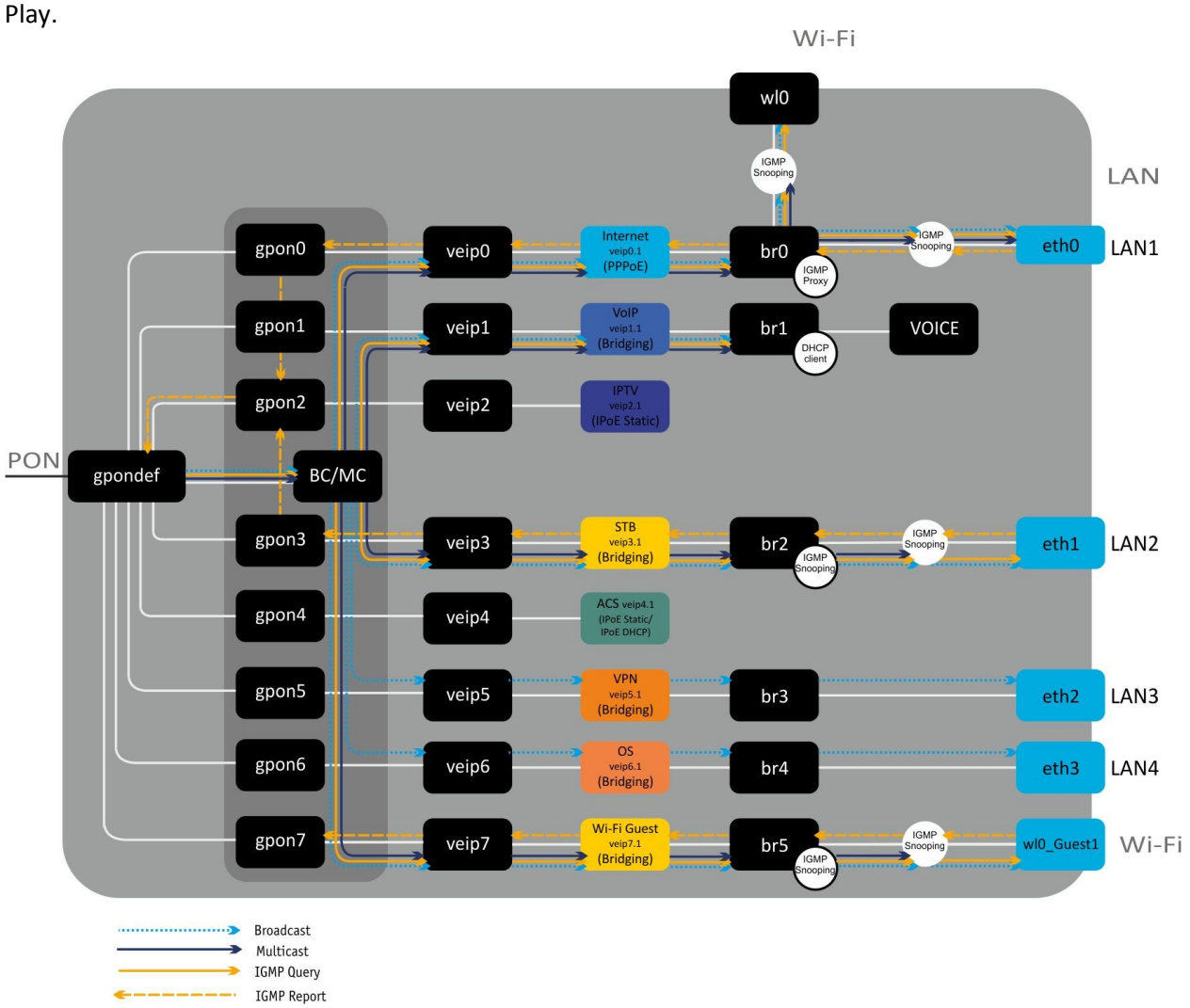


Рисунок 7 –Архитектура устройства, сконфигурированного для предоставления услуг Triple Play

Блоки gpon i (где i=0..7) представляют собой логическое окончание gem-портов, по которым передается трафик различных услуг. Весь unicast-трафик, проходящий через блоки *gpon i* (*gpon0* – *gpon5*) передается на соответствующие *veip*-интерфейсы.

Блок BC/MC является логическим окончанием GEM-портов широковещательной (broadcast) и групповой (multicast) передачи. Через него передается multicast/broadcast-трафик в нисходящем потоке (downstream).

Veip-интерфейсы обеспечивают стык интерфейсов *gpon* (OMCI часть) и *Linux*-интерфейсов. Через *veip I* интерфейсы (где i=0…7) передается тегированный трафик, полученный с соответствующих *veip i.n*-интерфейсов.

Multicast/broadcast-трафик, полученный с блока *MC/BC*, попадает на все *veip*-интерфейсы.

Блоки veip i.n являются WAN-интерфейсами роутера устройства, каждый из которых служит для предоставления определенного вида услуг. В приведенном примере:

- veip0.1 служит для предоставления услуги Internet;
- veip1.1 – для предоставления услуги VoIP;
- veip2.1 – для управления multicast-трафиком;
- veip3.1 – для предоставления услуг VoD, IPTV на STB;
- veip4.1 – для удаленного управления и мониторинга по протоколу TR-069;
- veip5.1 – для предоставления услуги VPN на отдельном порту;
- veip6.1 – для предоставления других услуг (например, охранной сигнализации);
- veip7.1 – для организации гостевой Wi-Fi-сети.
-

Любой из WAN-интерфейсов может работать в следующих режимах:

- PPPoE – запускается PPP client;
- IPoE DHCP – запускается DHCP client;
- IPoE Static – используется статический адрес;
- Bridging – работа в режиме моста.

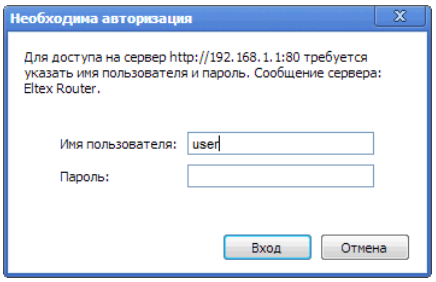
Блоки eth0..3 являются LAN-интерфейсами (LAN1…4) для подключения клиентского оборудования.

Логическими блоками, которые объединяют интерфейсы LAN и WAN, являются **br0..5**. *Br0* подключен к интерфейсу veip0.1, который работает в режиме PPPoE и к портам *eth0*, *eth1*, *wl0.* Блок *br1* работает в режиме bridge + DHCP, что позволяет использовать адрес этого интерфейса для SIP клиента (блок VOICE). Блоки *br2*, *br3, br4, br5* работают в режиме моста, который позволяет прозрачно пропускать трафик на LAN порты маршрутизатора.

4 НАСТРОЙКА NTU-RG-1402G-W ЧЕРЕЗ WEB-ИНТЕРФЕЙС. ДОСТУП ПОЛЬЗОВАТЕЛЯ

Для того чтобы произвести конфигурирование устройства, необходимо подключиться к нему через web browser (программу для просмотра гипертекстовых документов), например, Firefox, Google Chrome. Для этого необходимо ввести в адресной строке браузера IP-адрес устройства (при заводских установках адрес: - *192.168.1.1,* маска подсети – *255.255.255.0)*.

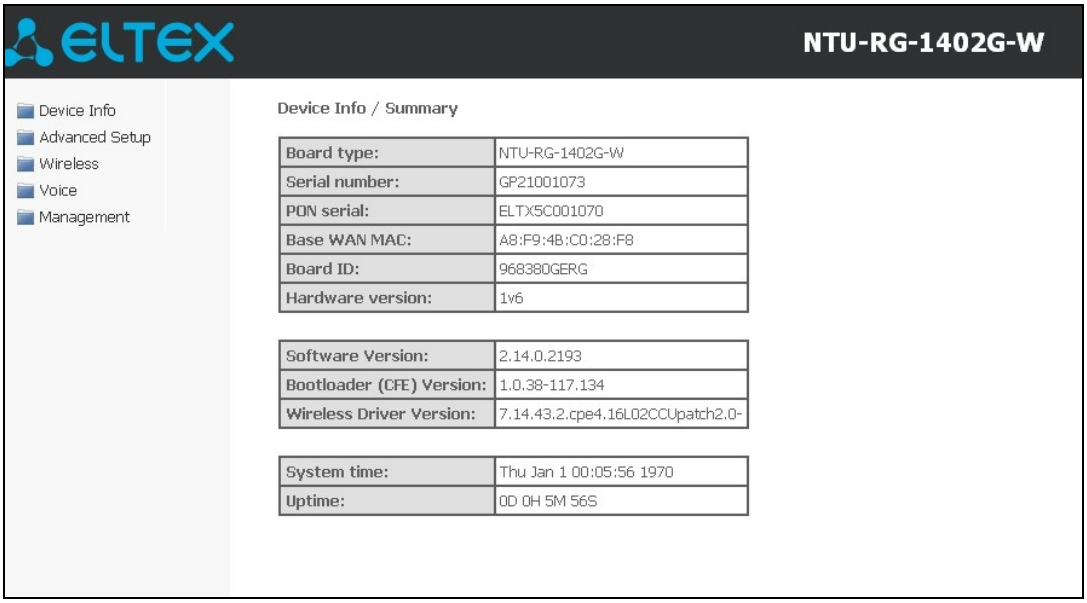
После введения IP-адреса устройство запросит имя пользователя и пароль.



Имя пользователя ***user***, пароль ***user*.**

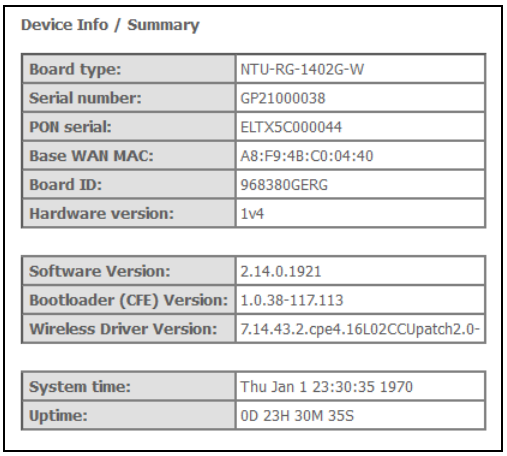
Во избежание несанкционированного доступа при дальнейшей работе с устройством рекомендуется изменить пароль (**раздел *4.6.5).***

Ниже представлен общий вид окна конфигурирования устройства. Слева расположено дерево навигации по меню настроек объектов, справа – область редактирования параметров.



4.1 Меню «*Device Info*» . Информация об устройстве

4.1.1 Подменю ***Summary.*** **Общая информация об устройстве**



- *Board type* –модель устройства*;*
- *Serial number* – серийный номер устройства;
- *PON serial* – серийный номер устройства в сети PON;
- *Base WAN MAC* – WAN MAC-адрес устройства;*Board ID* – идентификатор платы;
- *Hardware Version* – версия аппаратного обеспечения;

- *Software Version* – версия ПО;
- *Bootloader (CFE) Version* – версия начального загрузчика;
- *Wireless Driver Version* – версия адаптера Wi-Fi;

- *System time* – текущее время на устройстве;
- *Uptime*– время работы устройства с момента последней перезагрузки.

4.1.2 Подменю ***WAN.*** **Информация о состоянии сервисов**

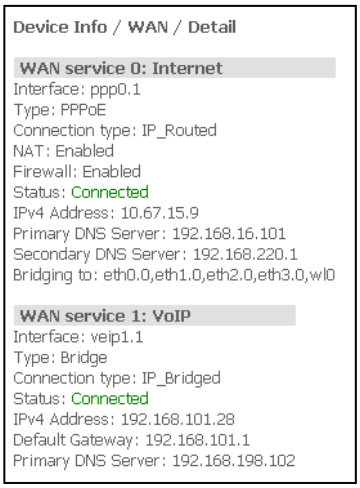
4.1.2.1 Подменю ***General.*** **Общая информация**

В данной вкладке выводится общая информация существующих конфигурациях интерфейса WAN.

4.1.2.2 Подменю ***Detail.*** **Подробная информация**

В данной вкладке выводится подробная информация о существующих конфигурациях интерфейса WAN.

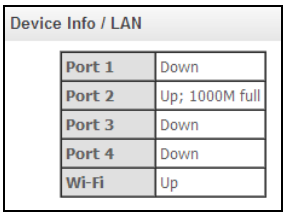
Для просмотра доступна следующая информация о сервисах:



- *Interface* – имя интерфейса;
- *Type* – режим работы интерфейса;
- *Connection Type* – тип подключения;
- *NAT* – статус NAT;
- *Firewall* – статус Firewall;
- *Status* –статус соединения;
- *IPv4 Address* – адрес для доступа;
- *Default Gateway* – шлюз по умолчанию;
- *Primary DNS Server*[1]– адрес первичного DNS сервера, используемого для работы;
- *Secondary DNS Server*[1] – адрес вторичного DNS сервера, используемого для работы;
- *Bridging to* – список связанных LAN-интерфейсов.

4.1.3 Подменю ***LAN.*** **Мониторинг состояния портов LAN. Мониторинг статуса Wi-Fi интерфейса**

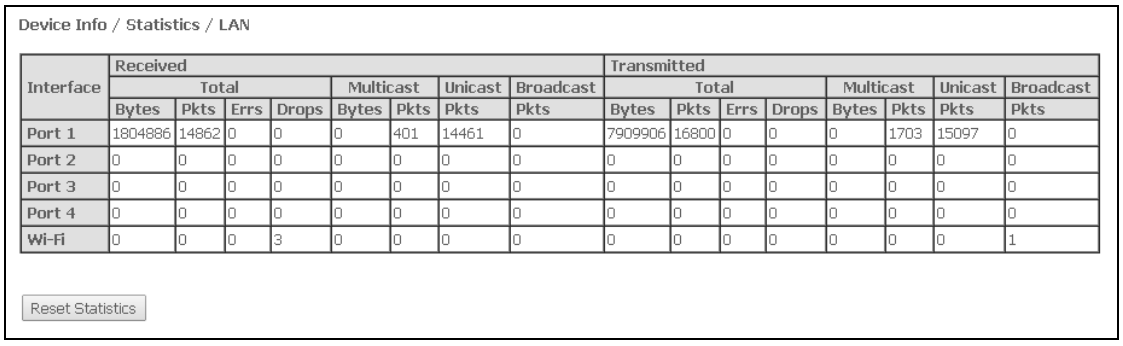
В данном меню доступен просмотр статусов и характеристик проводных и беспроводных интерфейсов LAN. Для проводных соединений указан статус, скорость соединения, режим работы (дуплекс/полудуплекс).



4.1.4 Подменю ***Statistics.*** **Информация о прохождении трафика на портах устройства**

В меню осуществляется просмотр статистики принятых и переданных пакетов для WAN Service, LAN и оптического интерфейса.

Интерфейс LAN:



Interface	Received								Transmitted							
	Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
Port 1	1804886	14862	0	0	0	401	14461	0	7909906	16800	0	0	0	1703	15097	0
Port 2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Port 3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Port 4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Wi-Fi	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	1

[1] Только для сервиса **INTERNET, VoIP**

WAN Service:

Device Info / WAN / General

Interface	Description	Type	VlanMuxId	Igmp Pxy	Igmp Src Enbl	NAT	Firewall	Status	IPv4 Address
veip1.1	veip1	Bridge	3149	Disabled	Disabled	Disabled	Disabled	Connected	192.168.2.1
veip2.1	veip2	IPoE	30	Enabled	Disabled	Disabled	Disabled	Connected	192.168.21.21
veip3.1	veip3	Bridge	0	Disabled	Disabled	Disabled	Disabled	Connected	0.0.0.0
veip4.1	ipoe_veip4	IPoE	4000	Disabled	Disabled	Disabled	Disabled	Connected	192.168.200.5
ppp0.1	veip0	PPPoE	2149	Disabled	Disabled	Enabled	Enabled	Connected	10.154.8.135

Интерфейс Optical:

Для устройств с возможностью измерения параметров оптического сигнала[1] данное меню имеет дополнительную таблицу:

- *Link Status* – статус оптического линка,
- *Optical Signal Level* – уровень принимаемого сигнала (1490нм),
- *Transmit Optical Level* – уровень передаваемого сигнала (1310нм),
- *Temperature* – температура SFF-модуля;
- *Vcc Voltage* – напряжение питания;
- *Bias Current* – ток смещения.

Device Info / Statistics / Optical

Received				Transmitted			
Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
0	0	0	0	0	0	0	0

Reset Statistics

Link Status	Optical Signal Level	Transmit Optical Level	Temperature	Vcc Voltage	Bias Current
Down	No signal	2.38 dBm	46.7 C	3.41 V	7.90 mA

Для обнуления данных и возобновления накопления статистики необходимо нажать *«Reset Statistic».*

4.1.5 Подменю ***Route.*** **Просмотр таблицы маршрутизации**

В меню осуществляется просмотр таблицы маршрутизации.

Device Info / Route

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
0.0.0.0	0.0.0.0	0.0.0.0	U	0	Internet	ppp0.1
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
192.168.21.0	0.0.0.0	255.255.255.0	U	0	MC	veip2.1
192.168.101.0	0.0.0.0	255.255.255.0	U	0		br1
192.168.111.9	0.0.0.0	255.255.255.255	UH	0	Internet	ppp0.1
192.168.198.102	192.168.101.1	255.255.255.255	UGH	0		br1
192.168.203.0	0.0.0.0	255.255.255.0	U	0	ipoe_veip4	veip4.1

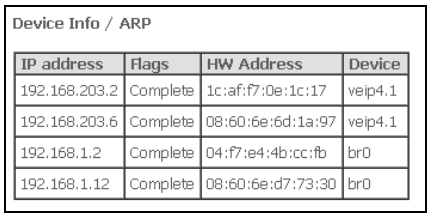
Flags:
U - up,
G - gateway,
H - host,
R - reinstate,
D - dynamic (redirect),
M - modified (redirect).
! - reject

[1] Опционально

- *Destination* – IP-адрес назначения;
- *Gateway* – IP-адрес шлюза;
- *Subnet mask* – маска подсети(Genmask);
- *Flag* – флаг маршрута:
  - *U* – маршрут активен;
  - *!* – нерабочий маршрут, пакеты будут отброшены;
  - *G* – маршрут использует шлюз (gateway);
  - *H* – адресом назначения является отдельный хост;
  - *R* - восстановленный маршрут;
  - *D* – устанавливается, если маршрут был создан по приходу перенаправляемого сообщения ICMP;
  - *M* – устанавливается, если маршрут был модифицирован перенаправляемым сообщением ICMP;
- *Metric* – приоритет маршрута;
- *Service* – сервис, к которому относится маршрут;
- *Interface* – сетевой интерфейс, к которому относится маршрут.

4.1.6 Подменю ***ARP.*** **Просмотр кэша протокола ARP**

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.

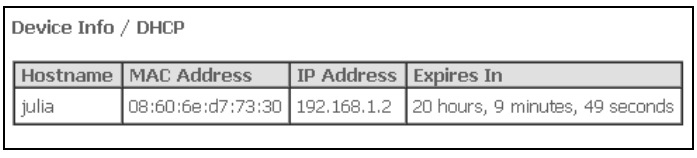

Device Info / ARP

IP address	Flags	HW Address	Device
192.168.203.2	Complete	1c:af:f7:0e:1c:17	veip4.1
192.168.203.6	Complete	08:60:6e:6d:1a:97	veip4.1
192.168.1.2	Complete	04:f7:e4:4b:cc:fb	br0
192.168.1.12	Complete	08:60:6e:d7:73:30	br0

- *IP-address* – IP-адрес клиента
- *Flags* – флаги состояния:
  - *Complete* – клиент активен;
  - *Incomplete* – клиент не отвечает на ARP-запросы;
- *HW-Address*–MAC-адрес клиента;
- *Device* – интерфейс, на котором находится клиент.

4.1.7 Подменю ***DHCP.*** **Активные аренды DHCP**

В таблице DHCP можно посмотреть список активных аренд DHCP сервера и срок их истечения.

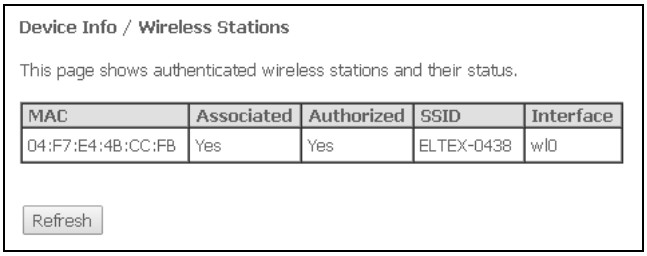

Device Info / DHCP

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

- *Hostname* – имя хоста(сетевого устройства);
- *MAC Address* – MAC адрес устройства;
- *IP Address* – адрес устройства в локальной сети, выданный маршрутизатором из пула IP-адресов;
- *Expires In* – время, через которое истекает аренда данного адреса.

4.1.8 Подменю *Wireless Stations*. Подключенные беспроводные устройства

В данном меню доступен просмотр перечня аутентифицированных беспроводных устройств и их статус.



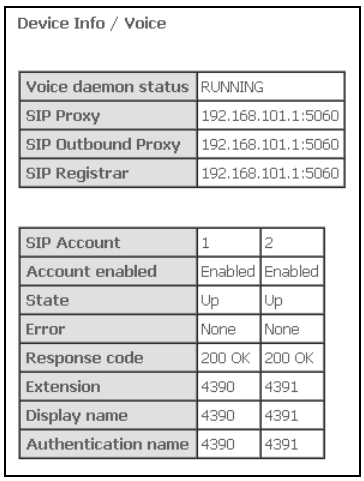
Данные об устройствах выводятся в таблице, содержащей следующие параметры:

- *MAC* – MAC-адрес устройства;
- *Associated* – статус связи с SSID;
- *Authorized* – статус авторизации;
- *SSID* – идентификатор сети, с которой связан клиент;
- *Interface* – интерфейс доступа.

Для обновления данных необходимо нажать кнопку *«Refresh»*.

4.1.9 Подменю *Voice*. Мониторинг состояния телефонных портов

В данном меню доступен просмотр статуса FXS портов и параметры SIP-аккаунтов.



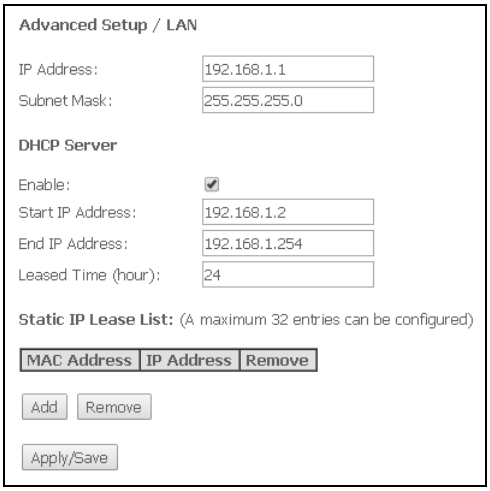
- *Voice daemon status* – состояние работы голосового демона;
- *SIP Proxy* – адрес и порт SIP Proxy;
- *SIP Outbound Proxy* – адрес и порт SIP proxy, через который будет осуществляться передача всех запросов (запросы на SIP Proxy и SIP Registrar будут маршрутизироваться через этот сервер);
- *SIP Registrar* – адрес и порт SIP сервера;
- *SIP Account* – аккаунт SIP (номер порта FXS);
- *Account enabled* – состояние порта FXS в конфигурации;
- *State* – статус аутентификации;
- *Error* – ошибка, выдаваемая сервером SIP;
- *Response code* – код ответа сервера SIP;
- *Extension* – номер телефона;
- *Display name* – отображаемое имя пользователя;
- *Authentication name* – имя пользователя для аутентификации.

4.2 Меню *«Advanced Setup»*. Расширенные настройки конфигурации

4.2.1 Подменю *LAN.* Настройки интерфейса LAN

4.2.1.1 Подменю *General Settings.* Настройка основных параметров

В данном меню производится настройка основных параметров для LAN интерфейса.



- *IP address* – адрес устройства в локальной сети;
- *Subnet Mask* – маска подсети;

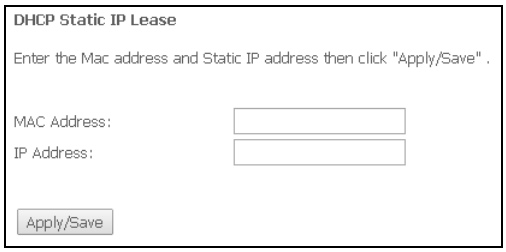
DHCP Server:

DHCP-сервер (Dynamic Host Configuration Protocol, протокол динамической настройки хостов) позволяет провести автоматическую настройку локальных компьютеров для работы в сети. Он назначает IP каждому компьютеру внутри сети. Эта дополнительная функция позволяет уйти от необходимости назначать IP-адреса вручную.

- *Enable* – при установленном флаге использовать DHCP сервер (сетевые устройства будут получать IP-адреса динамически, из нижеприведенного диапазона);
- *Start IP Address* – начальный адрес диапазона;
- *End IP Address* – конечный адрес диапазона;
- *Leased Time (hour)* – время аренды адреса (в часах);

Static IP Lease List:

В данной таблице производится привязка выдаваемых IP-адресов MAC-адресам устройств. Для добавления записи в таблицу необходимо нажать «*Add».* Может быть установлено до 32 соответствий.

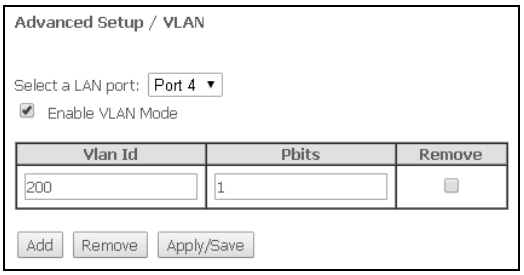


- *Mac Address* – MAC-адрес устройства;
- *IP Address* –IP-адрес устройства.

Для принятия и сохранения изменений необходимо нажать кнопку *«Apply/Save».*

4.2.1.2 Подменю ***VLAN Setting*[1]. Настройка параметров VLAN**

В данном меню производится настройка параметров виртуальных локальных сетей.



- *Select a LAN port* – выбор Ethernet-порта;
- *Enable VLAN Mode* – при установленном флаге разрешено использование VLAN.

Для добавления новой VLAN необходимо нажать кнопку *«Add»* и заполнить следующие поля*:*

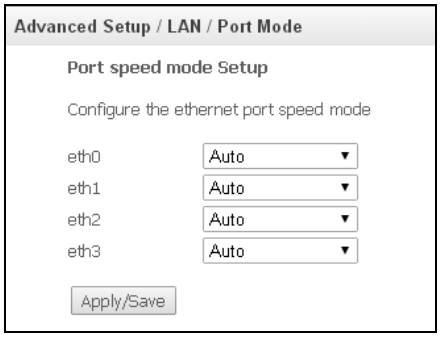
- *VLAN Id* – номер VLAN из диапазона от 1 до 4094;
- *Pbits* – номер приоритета VLAN из диапазона от 0 до 7 (0 - максимальный приоритет, 7 - минимальный).

Для принятия и сохранения изменений необходимо нажать кнопку *«Apply/Save».*

Для удаления необходимо установить флаг *«Remove»* в выбранной строке, нажать кнопки «*Remove*» и *«Apply/Save».*

4.2.1.3 Подменю ***Port Mode*[2]. Настройка скорости и режима работы портов LAN**

В меню производится настройка скорости и дуплекса Ethernet-портов.

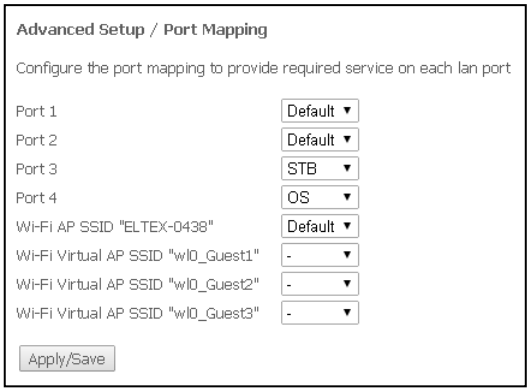


Для смены режима работы порта необходимо выбрать требуемый режим в выпадающем списке и нажать кнопку *«Apply/Save».*

[1] При отсутствии меню в конфигураторе данные настройки уже выполнены Вашим оператором связи
[2] При отсутствии меню в конфигураторе данные настройки уже выполнены Вашим оператором связи

4.2.2 Подменю *Port Mapping*[1]. Настройки распределения портов и услуг

Меню предназначено для настройки Ethernet-портов на предоставление конкретной услуги оператора, что позволяет разграничить различные типы трафика. Данная функция используется преимущественно в сетях Triple Play.



В меню возможно изменить текущие раскладки портов по услугам, например настроить 4 порта для пользования INTERNET или 3 порта для STB, в отличие от конфигурации по умолчанию, приведенной на рисунке выше.

Для принятия изменений и сохранения необходимо нажать кнопку *«Apply/Save»*.

4.2.3 Подменю *PPPoE.* Настройки PPP[2]

Для включения услуги установите флаг в поле «Enable Service».

Для сервиса Internet доступны 2 режима работы:

- IP_Routed – режим, в котором сессия PPPoE поднимается на абонентском устройстве;
- PPPoE_Bridged – режим, в котором сессия PPPoE поднимается на ПК пользователя.

- *Username* – логин пользователя для доступа к сети Интернет;
- *Password* – пароль пользователя для доступа к сети Интернет;

При выборе режима работы PPPoE_Bridged поля *Username и Password* недоступны, логин и пароль вводятся на ПК пользователя.

Для принятия и сохранения изменений необходимо нажать кнопку *«Apply/Save»*.

[1] При отсутствии меню в конфигураторе данные настройки уже выполнены Вашим оператором связи

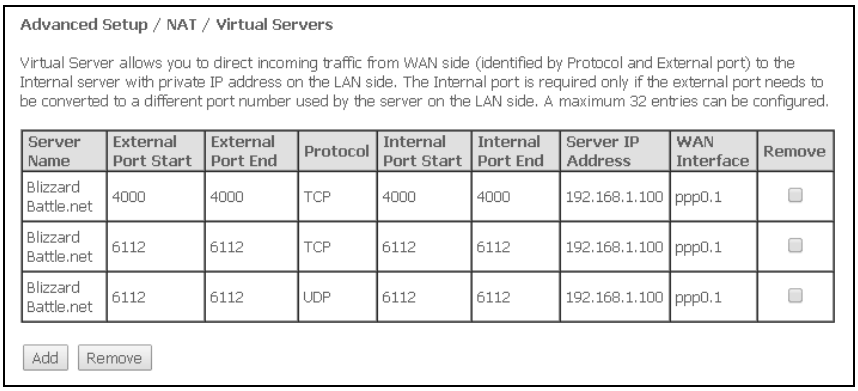
[2] При отсутствии меню в конфигураторе данные настройки уже выполнены Вашим оператором связи.

4.2.4 Подменю *NAT*. Настройки NAT

Настройки NAT могут быть эффективны при работе устройства в режиме маршрутизатора.

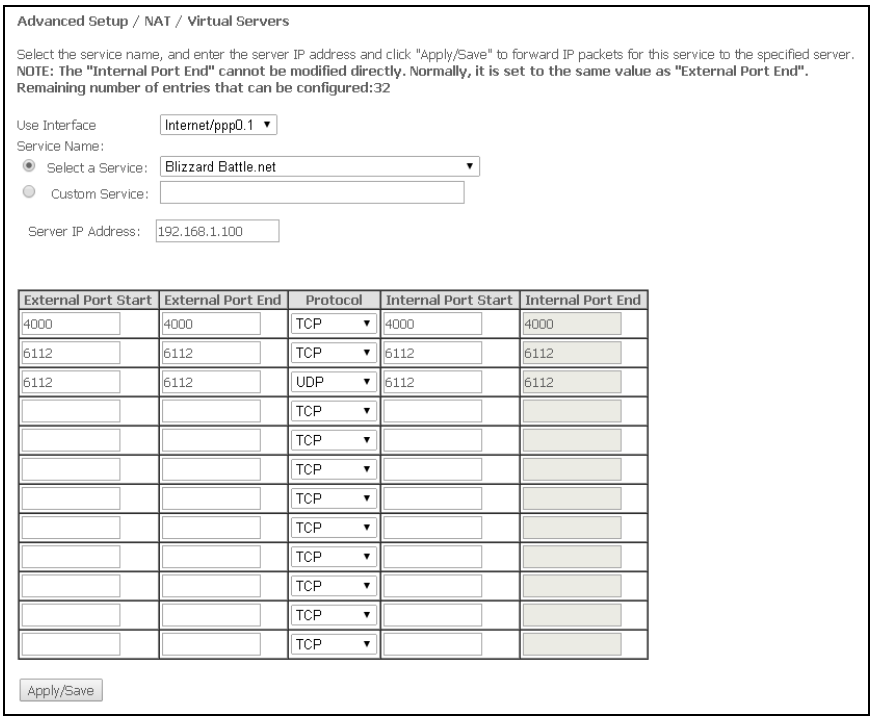
4.2.4.1 Подменю *Virtual Servers.* Настройки виртуальных серверов

Virtual Server – это функция маршрутизаторов, предназначенная для предоставления доступа пользователям через сеть Интернет к серверам, находящимся в Вашей локальной сети, например к почтовым серверам, WWW, FTP. На устройстве может быть создано до 32 записей.



Правило Virtual Server не будет работать в том случае, если запрос на IP-адрес WAN интерфейса устройства пришел из локальной сети, так как устройство не поддерживает функцию NAT Loopback. Тестирование созданных правил Virtual Server должно осуществляться только из интернета.

Для добавления записи в таблицу фильтрации необходимо нажать *«Add»* и заполнить поля в открывшемся меню:



– *Use Interface* – используемый интерфейс;

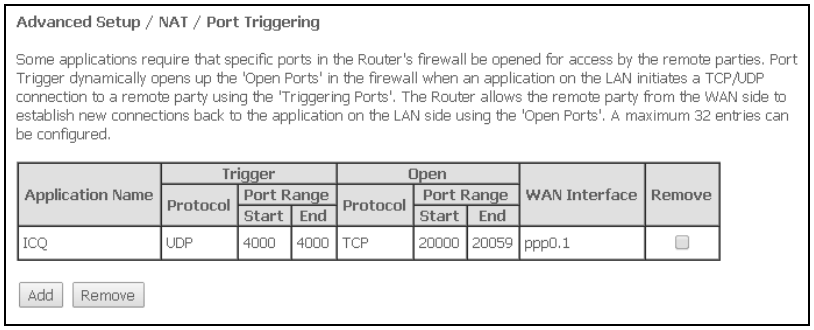
Для использования доступны только интерфейсы, настроенные на работу в режиме маршрутизатора с разрешенной трансляцией сетевых адресов.

- *Service Name* – настройки сервиса:
  - *Select a Service* – выбор преднастроенного правила;
  - *Custom Service* – создать свои, не указанные в списке *Select a Service*, правила;
- *Server IP Address* – IP-адрес сервера, находящегося в локальной сети;
- *External Port Start* – начальный внешний порт диапазона портов, на которые осуществляется обращение из Интернета;
- *External Port End* – конечный внешний порт диапазона портов, на которые осуществляется обращение из Интернета;
- *Protocol* – выбор сетевого протокола;
- *Internal Port Start* – начальный внутренний порт диапазона портов, на который будет переадресовываться трафик с внешнего порта маршрутизатора;
- *Internal Port End* – конечный внутренний порт диапазона портов, на который будет переадресовываться трафик с внешнего порта маршрутизатора.

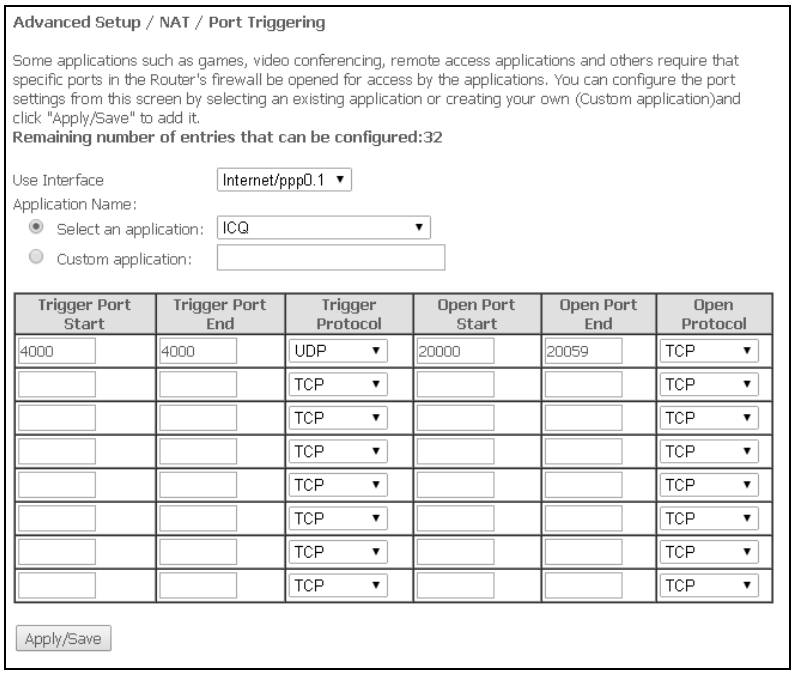
Для принятия и сохранения изменений необходимо нажать кнопку *«Apply/Save»*.

4.2.4.2 Подменю ***Port Triggering.*** **Настройки запуска портов**

Маршрутизатор по умолчанию блокирует все входящие запросы на установку соединения. Механизм работы функции *Port Triggering* заключается в том, чтобы при появлении определенного события динамически открывать порты на своем внешнем интерфейсе и привязывать их к соответствующим портам компьютера в локальной сети.



Для добавления правил в таблицу необходимо нажать кнопку *«Add»,* удаление происходит нажатием кнопки *«Remove»* напротив выбранного правила.



– *Use Interface* – используемый интерфейс.

Для использования доступны только интерфейсы, настроенные на работу в режиме маршрутизатора с разрешенной трансляцией сетевых адресов.

– *Application Name* – настройки приложения:
  – *Select an application* – выбор преднастроенного правила.
  – *Custom an application* – создать свои, не указанные в списке Select an application, правила.

В отличие от функции *Virtual Server,* здесь нет необходимости фиксировано задавать IP-адрес компьютера в LAN.

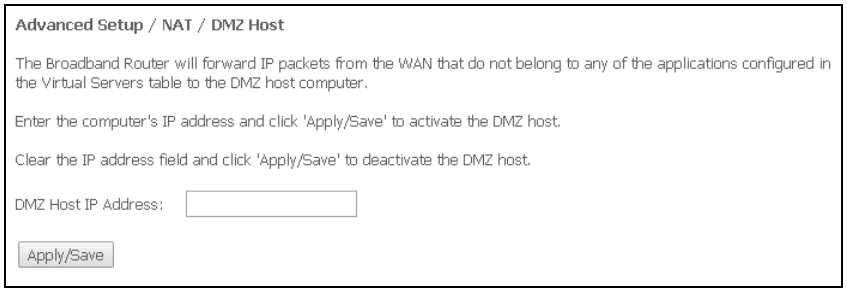
– *Trigger Port Start* – начальный порт диапазона портов, которые осуществляют функцию триггера;
– *Trigger Port End* – конечный порт диапазона портов, которые осуществляют функцию триггера;
– *Trigger Protocol* – протокол, используемый для триггера;
– *Open Port Start* – начальный порт диапазона портов, которые маршрутизатор будет открывать;
– *Open Port End* – конечный порт диапазона портов, которые маршрутизатор будет открывать;
– *Open Protocol* – используемый протокол для открываемых портов.

Для принятия и сохранения изменений необходимо нажать кнопку *«Apply/Save»*.

4.2.4.3 Подменю ***DMZ Host.*** **Настройки демилитаризованной зоны**

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

Для отключения данной настройки необходимо стереть IP-адрес из поля ввода.



Для принятия и сохранения изменений необходимо нажать кнопку *«Apply/Save»*.

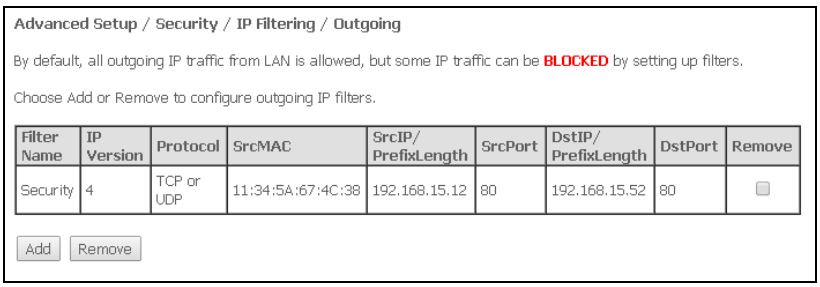
4.2.5 Подменю ***Security*****. Настройки безопасности**

В данном разделе проводится настройка параметров безопасности устройства.

4.2.5.1 Подменю ***IP Filtering.*** **Настройки фильтрации адресов**

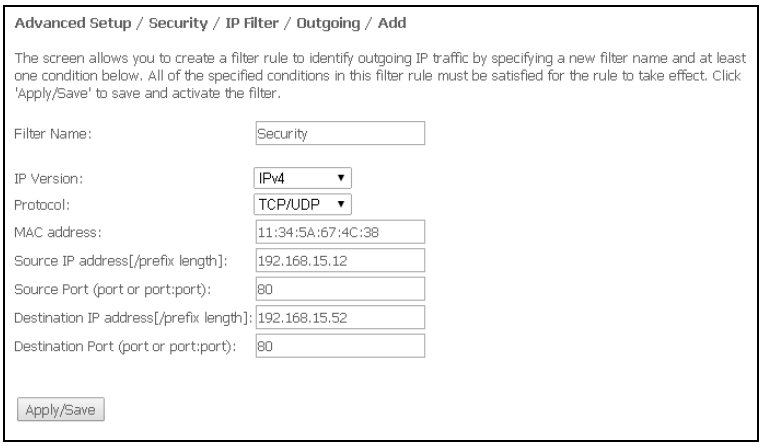
Функция *IP Filtering* позволяет фильтровать проходящий через маршрутизатор трафик по IP-адресам и портам.

Настройки фильтрации исходящего трафика (Outgoing):



По умолчанию весь исходящий трафик будет пропускаться, правила, созданные в этом меню, позволят блокировать нежелательный трафик.

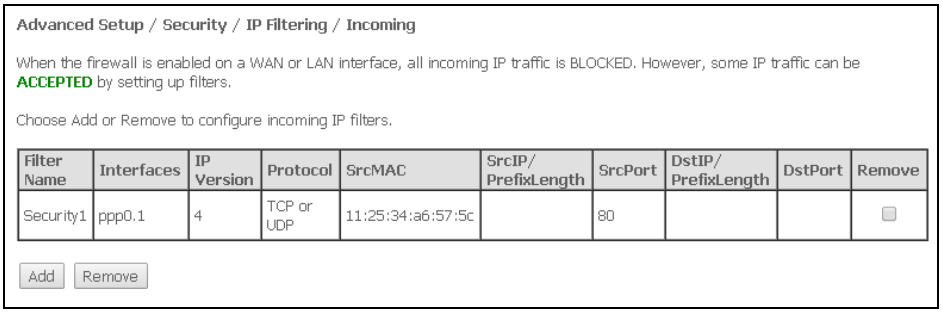
Для добавления нового правила фильтрации необходимо нажать кнопку *«Add»***.**



- *Filter Name* – текстовое описание фильтра;
- *IP Version* – выбор версии протокола IP;
- *Protocol* – выбор протокола(TCP/UDP, TCP, UDP, ICMP);
- *MAC address* – MAC-адрес источника;
- *Source IP address[/prefix length]* – IP-адрес источника (через слэш возможно указать длину префикса);
- *Source Port (port or port:port)* – порт источника или диапазон портов через двоеточие;
- *Destination IP address[/prefix length]* – IP-адрес места назначения (через слэш возможно указать длину префикса);
- *Destination Port (port or port:port)* – порт места назначения или диапазон портов через двоеточие.

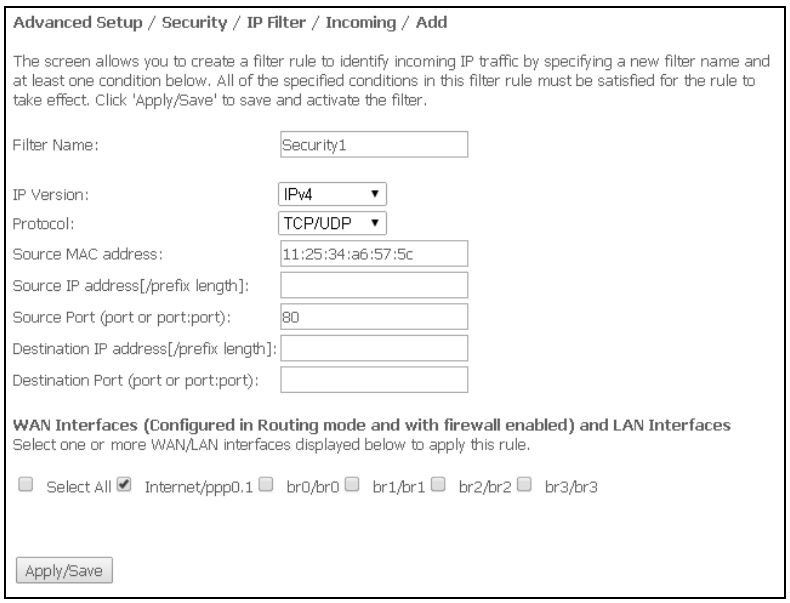
Для принятия и сохранения настроек необходимо нажать кнопку *«Apply/Save»*.

Настройки фильтрации входящего трафика (Incoming):



При включении брандмауэра на интерфейсе WAN или LAN весь входящий трафик, не попадающий под установленные правила, будет заблокирован.

Для добавления нового правила фильтрации необходимо нажать кнопку *«Add»*.



- *Filter Name* – текстовое описание фильтра;
- *IP Version* – выбор версии протокола IP;
- *Protocol* – выбор сетевого протокола;
- *Source MAC address* – MAC-адрес источника;
- *Source IP address[/prefix length]* – IP-адрес источника (через слэш возможно указать длину префикса);
- *Source Port (port or port:port)* – порт/порты источника;
- *Destination IP address[/prefix length]* – IP-адрес места назначения (через слэш возможно указать длину префикса);
- *Destination Port (port or port:port)* – порт/порты места назначения;

Интерфейсы WAN (сконфигурированные в режиме маршрутизатора и с включенным брандмауэром) и интерфейсы LAN:

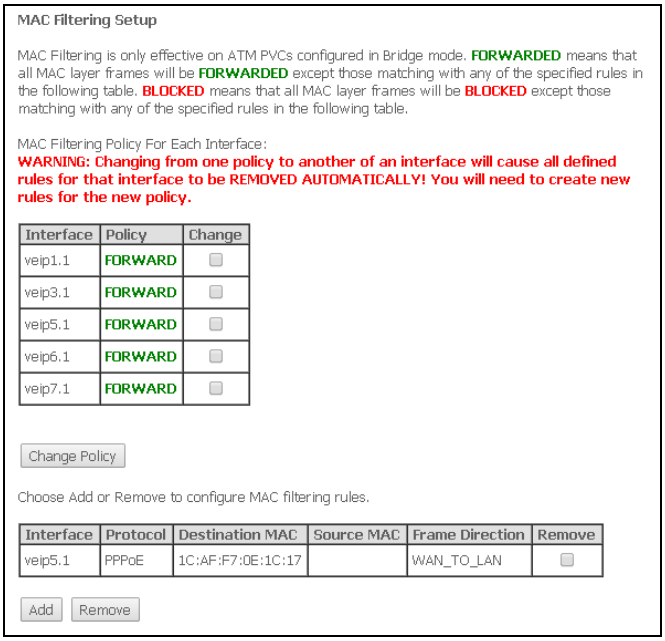
- *Select All – при установленном флаге выбрать все возможные интерфейсы.*

Либо выбрать интерфейс из приведенного списка, установив флаг напротив.

Для принятия и сохранения настроек необходимо нажать кнопку *«Apply/Save»*.

4.2.5.2 Подменю ***MAC Filtering.*** **Настройки фильтрации по MAC-адресам**

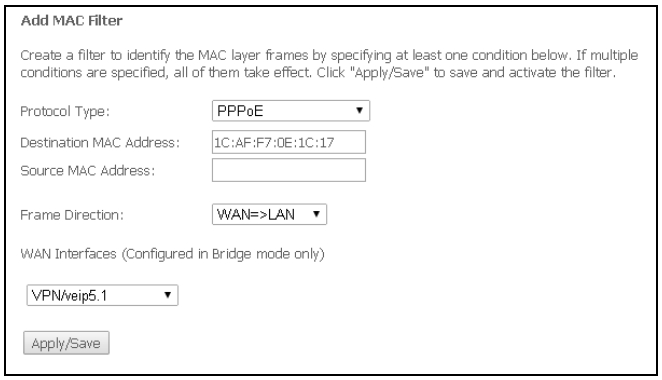
Фильтрация на основе MAC-адресов позволяет пересылать или блокировать трафик с учетом MAC-адреса источника и получателя.



Фильтрация на основе MAC-адресов работает только для интерфейсов, находящихся в режиме моста (Bridge).

Для изменения глобальной политики установите флаг напротив необходимого интерфейса и нажмите кнопку «*Change Policy*» (изменить политику). Доступно два варианта: FORWARDED и BLOCKED.

В режиме FORWARDED созданные правила будут запрещать прохождение трафика с указанными MAC-адресами источника/получателя, в режиме BLOCKED – разрешать.



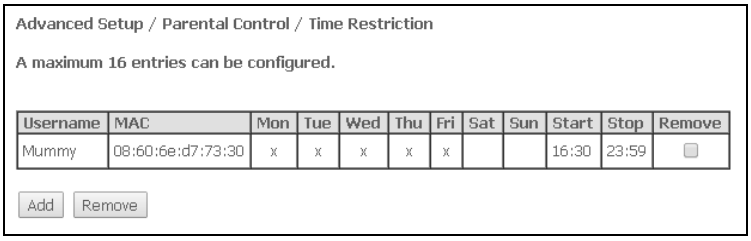
- *Protocol type* – выбор протокола (PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP);
- *Destination MAC Address* – MAC-адрес получателя;
- *Source MAC Address* – MAC-адрес отправителя;
- *Frame Direction* – направление передачи (LAN<=>WAN, LAN=>WAN, WAN=>LAN);
- *WAN Interfaces (Configured in Bridge mode only)* – выбор WAN интерфейса из выпадающего списка (доступны только интерфейсы, работающие в режиме моста).

Для принятия и сохранения настроек необходимо нажать кнопку *«Apply/Save».*

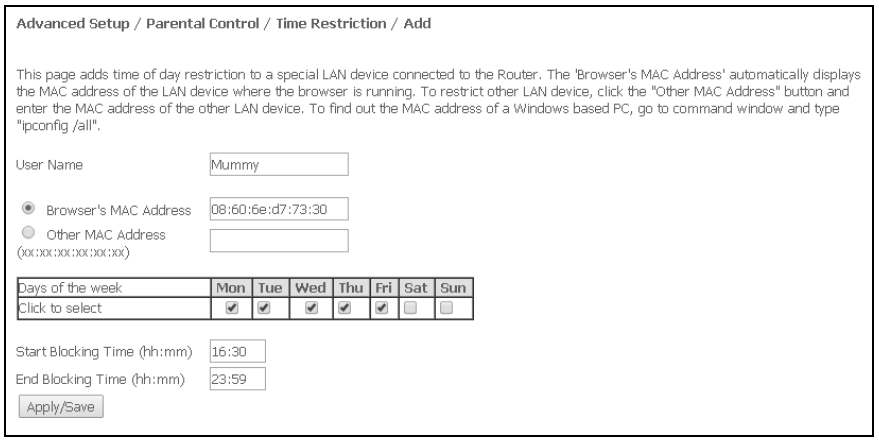
4.2.6 Подменю *Parental control*. «Родительский контроль» – настройки ограничения

4.2.6.1 Подменю *Time Restriction.* Настройки ограничения продолжительности сеансов

В данном разделе производится конфигурирование расписания работы компьютеров с использованием дней недели и часов, по которым определенному компьютеру в локальной сети будет запрещен доступ в Интернет.



Для создания нового расписания необходимо нажать кнопку *«Add»,* всего может быть добавлено *не более 16* записей*.*



– *User Name* – имя пользователя;

– *Browser's MAC Address* – автоматически определенный MAC-адрес компьютера, для которого задается расписание;

– *Other MAC Address (xx:xx:xx:xx:xx:xx)* – заданный вручную MAC-адрес компьютера, для которого определяется расписание;

– *Days of the week* – дни недели, запрещенные для доступа в интернет;

– *Start Blocking Time (hh:mm)* – время начала блокировки в формате ЧЧ:ММ;

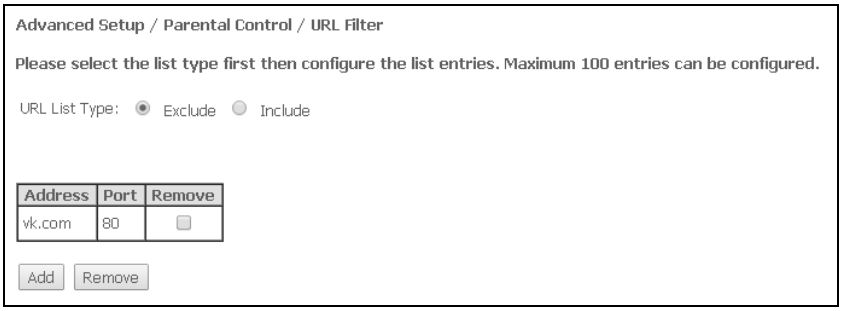
– *End Blocking Time (hh:mm)* – время окончания блокировки в формате ЧЧ:ММ;

Ограничения будут действовать, если на устройстве установлено корректное системное время.

Для добавления настроек в таблицу необходимо нажать кнопку *«Apply/Save»*.

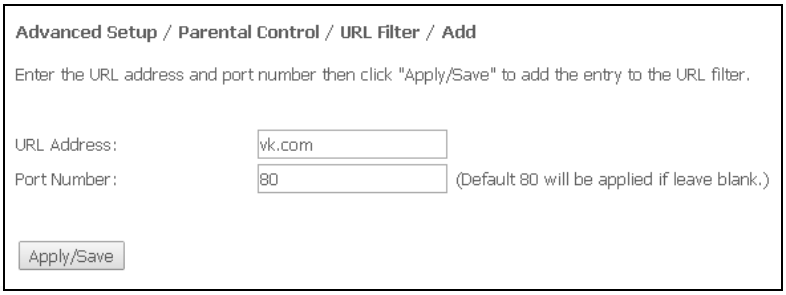
4.2.6.2 Подменю ***Url Filter.*** **Настройки ограничения доступа в интернет**

Url Filter – функция полноценного анализа и контроля доступа к определённым ресурсам сети интернет. В данном разделе задается список запрещенных/разрешенных *Url*-адресов для посещения.



- *URL List Type* – тип списка:
  - *Exclude* – запрещенные адреса;
  - *Include* – разрешенные адреса.

Для добавления нового адреса в список необходимо установить флаг напротив требуемого типа списка (*URL List Type*) и нажать кнопку *«Add»* .



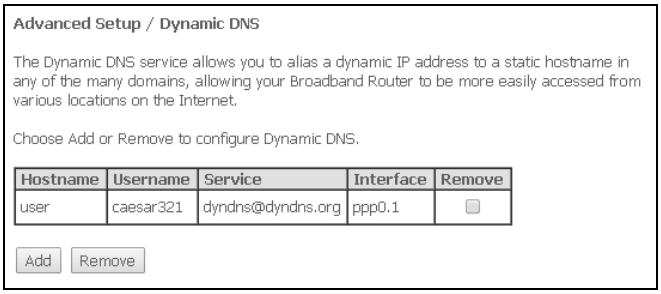
- *URL Address* – URL-адрес;
- *Port Number* – номер порта (если оставить поле пустым, будет использоваться 80 порт).

Для добавления настроек в таблицу необходимо нажать кнопку *«Apply/Save».*

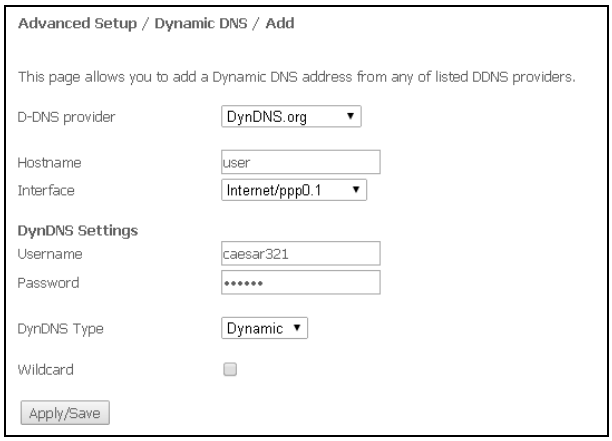
4.2.7 Подменю ***Dynamic DNS*****. Настройки динамической системы доменных имен**

Dynamic 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, роутеру, например NTU-RG) с динамическим IP-адресом. Это может быть IP-адрес, полученный по IPCP в PPP-соединениях или по DHCP.

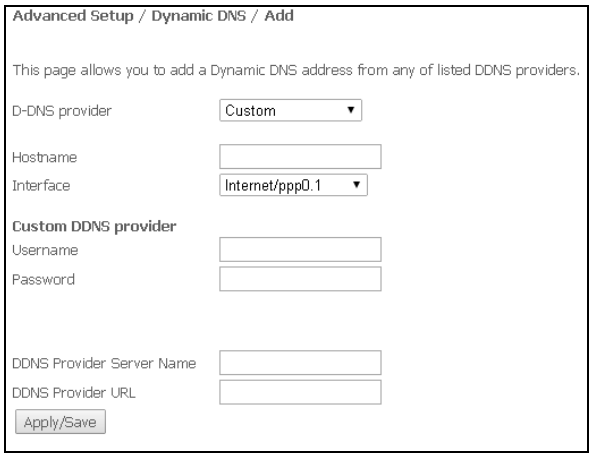
Динамическая DNS часто применяется в локальных сетях, где клиенты получают IP-адрес по DHCP, а потом регистрируют свои имена в локальном DNS-сервере.



Для добавления записи необходимо нажать кнопку *«Add»,* удаление происходит нажатием кнопки *«Remove»* напротив выбранной записи.



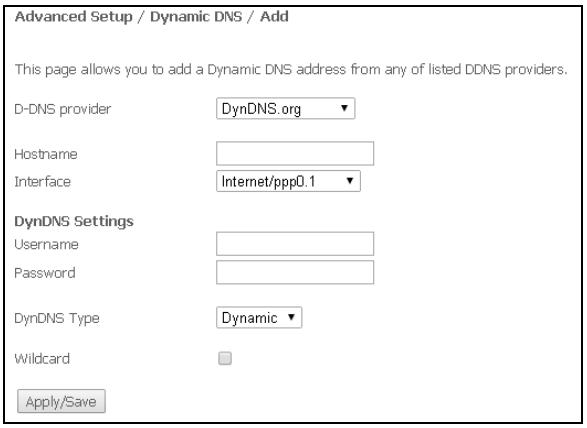
- *D-DNS provider* – выбор типа службы D-DNS (провайдера): *DynDNS.org, TZO.com, ZoneEdit.com, freedns.afraid.org, easyDNS.com, 3322.org, DynSIP.org, No-IP.com, dnsomatic.com, sitelutions.com;*
- *Custom* – иной провайдер, выбранный пользователем. В данном случае необходимо самостоятельно указать имя и адрес провайдера:

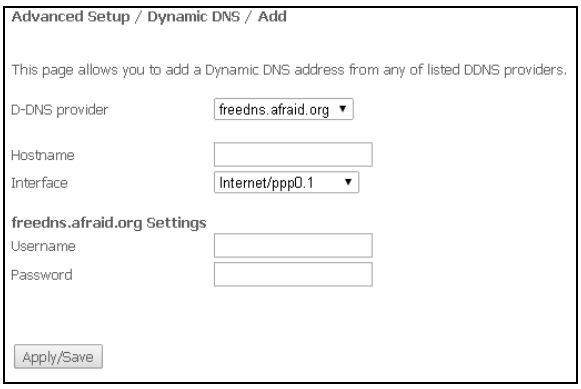


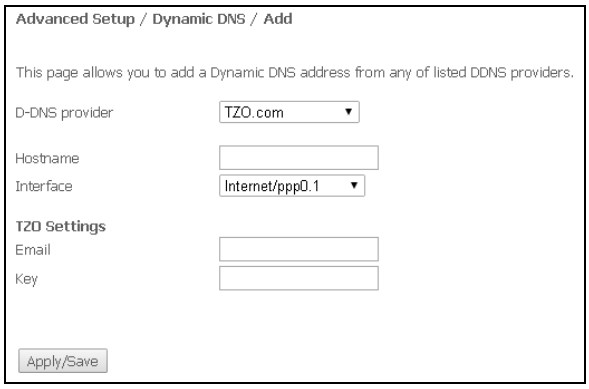
  - *Username* – имя пользователя для учетной записи DDNS;
  - *Password* – установка пароля для учетной записи DDNS;
  - *DDNS Provider Server Name* –имя провайдера услуг DDNS;
  - *DDNS Provider URL* – адрес провайдера услуг DDNS

- *Hostname* – имя хоста, зарегистрированное у провайдера DDNS;
- *Interface* – интерфейс доступа;

В зависимости от выбранного провайдера возможны следующие поля для заполнения:





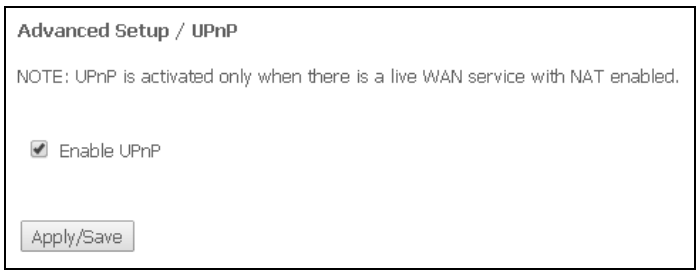


- *Username* – имя пользователя для учетной записи DDNS;
- *Password* – установка пароля для учетной записи DDNS;
- *DynDNS Type* – выбор типа услуги, зарегистрированной Вами у провайдера:
  - *Dynamic* – зарегистрирована услуга Динамический DNS (Dynamic DNS);
  - *Static* – зарегистрирована услуга Статический DNS (Static DNS);
  - *Custom* – зарегистрирована услуга Пользовательский DNS (Custom DNS);
- *Wildcard* – при установленном флаге использовать специальную запись DNS, отвечающую за все поддомены, которая будет соответствовать любому запросу к несуществующему поддомену. Она указывается в виде * в качестве поддомена, например *.domain.tld.
- *Email* – электронный адрес для аутентификации;
- *Key* – ключ для учетной записи DDNS.

Для принятия и сохранения изменений необходимо нажать кнопку *«Apply/Save».*

4.2.8 Подменю ***UPnP*. Автоматическая настройка сетевых устройств**

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



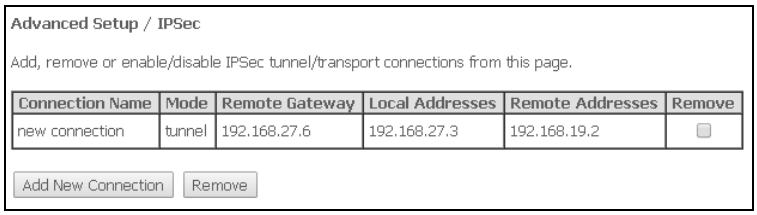
Для использования UPnP необходимо настроить NAT на активном WAN интерфейсе.

Для включения UPnP необходимо установить флаг *«Enable UPnP»***.**

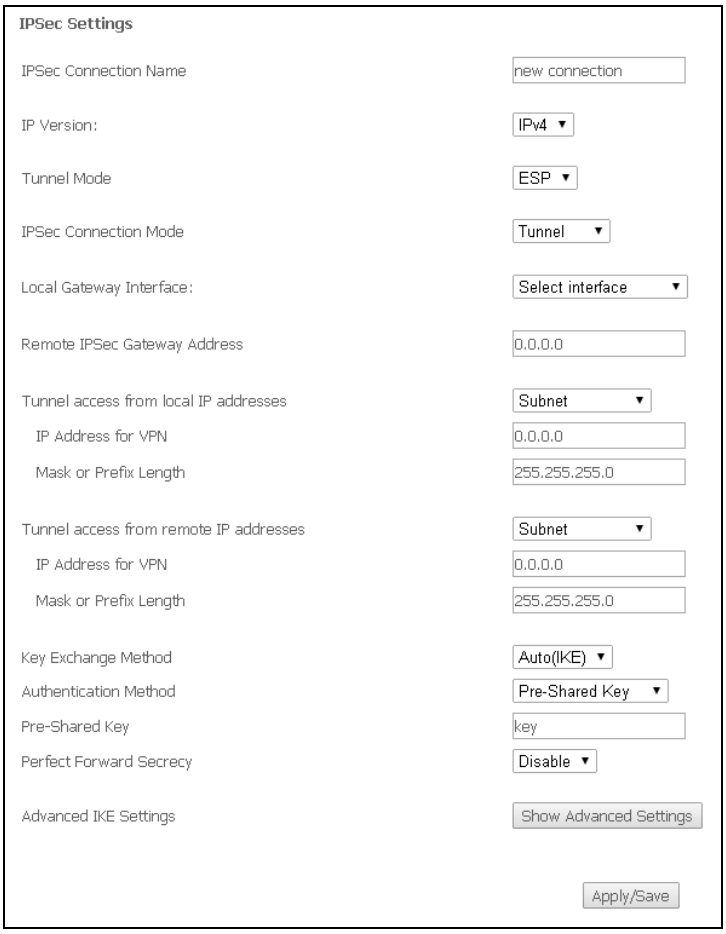
Для принятия и сохранения настроек необходимо нажать кнопку *«Apply/Save»*.

4.2.9 Подменю *IPSec*. Настройка защиты данных по протоколу IP

IP Security — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, позволяет осуществлять подтверждение подлинности. IPsec также включает в себя протоколы для защищённого обмена ключами в сети Интернет.



Для добавления записи необходимо нажать кнопку *«Add new connection».* Для удаления - установить флаг напротив требуемой записи в колонке Remove и нажать кнопку *«Remove»*.



- *IPSec Connection Name* – имя подключения;
- *IP Version* – версия протокола IP;
- *Tunnel Mode* – режим туннелирования(ESP/AH);
- *IPSec Connection Mode* – режим подключения (Tunnel/Transport);
- *Local Gateway Interface* – выбор интерфейса, используемого в качестве локального шлюза IPSec;
- *Remote IPSec Gateway Address (IPv4 address in dotted decimal)* – установка адреса удаленного шлюза IPSec;
- *Key Exchange Method* – режим смены ключа (авто/вручную (AUTO(IKE)/Manual));
- *Authentication Method* – выбор метода аутентификации:
  - *Pre-Shared Key* – установка пароля WPA-PSK (один пароль для каждого отдельного узла беспроводной сети);

- *Certificates* – выбор сертификата открытых ключей;

– *Perfect Forward Secrecy* – установка режима секретности. Данный режим добавит ещё один уровень безопасности на уровне шифрования данных, однако приведёт к увеличению нагрузки на CPU (enable – режим включен);

При выборе режима подключения *Tunnel* станут доступны следующие настройки:

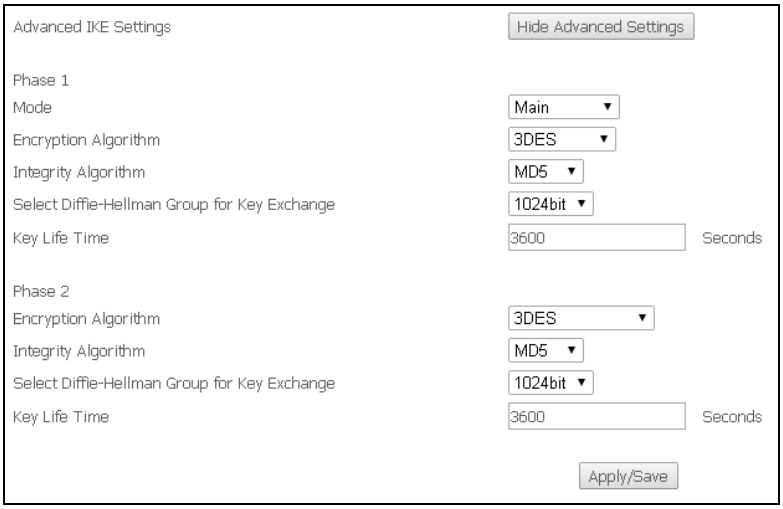
– *Tunnel access from local IP addresses* – режим туннельного доступа с локального адреса(подсеть/одиночный адрес (Subnet/Single Address));

- *IP Address for VPN* – адрес для VPN;
- *Mask or Prefix Length* – маска подсети;

– *Tunnel access from remote IP addresses* – режим туннельного доступа с удаленного адреса(подсеть/одиночный адрес (Subnet/Single Address));

- *IP Address for VPN* – адрес для VPN;
- *Mask or Prefix Length* – маска подсети;

При нажатии на кнопку *«Show Advanced Settings»* станут доступны расширенные настройки туннеля IKE:



Концепция управления и обмена ключами, управления и установления SA:

– *Phase 1 –фаза 1,* создание IKE SA для защиты фазы 2:

– *Mode* – выбор режима проведения фазы:

- *Main* – конфигурация стандартных параметров определения 1 фазы IKE VPN-туннеля (основной режим);
- *Aggressive* – конфигурация параметров определения 1 фазы IKE VPN-туннеля за минимальное время (превосходит по скорости основной, но не обеспечивает защиту подлинности);

– *Encryption Algorithm* – выбор алгоритма шифрования:

- *DES* – симметричный алгоритм шифрования, имеет блоки по 64 бита и 16 цикловую структуру сети Фейстеля, для шифрования использует ключ с длиной 56 бит;
- *3DES* – симметричный блочный шифр с увеличенной длиной ключа, созданный на основе алгоритма DES. При намного более высокой криптостойкости, скорость работы 3DES в 3 раза ниже, чем у DES;

– *Integrity Algorithm* – выбор алгоритма вычисления поля *Integrity Check Value* в заголовке пакета аутентификации (MD5, SHA1*);*

– *Select Diffie-Hellman Group for Key Exchange* – выбор размерности группы MODP для разделяемого (двойного) ключа в небезопасной среде;

– *Key Life Time* – установка времени жизни ключа, в секундах;

– *Phase 2* –фаза 2, создание SA для IPsec:

– *Encryption Algorithm* – выбор алгоритма шифрования:

- *DES* – симметричный алгоритм шифрования, имеет блоки по 64 бита и 16 цикловую структуру сети Фейстеля, для шифрования использует ключ с длиной 56 бит;

– *3DES* – симметричный блочный шифр с увеличенной длиной ключа, созданный на основе алгоритма DES. При намного более высокой криптостойкости, скорость работы 3DES всего в 3 раза ниже, чем у DES;

– *Integrity Algorithm* – выбор алгоритма вычисления поля Integrity Check Value в заголовке пакета аутентификации (MD5, SHA1*);*

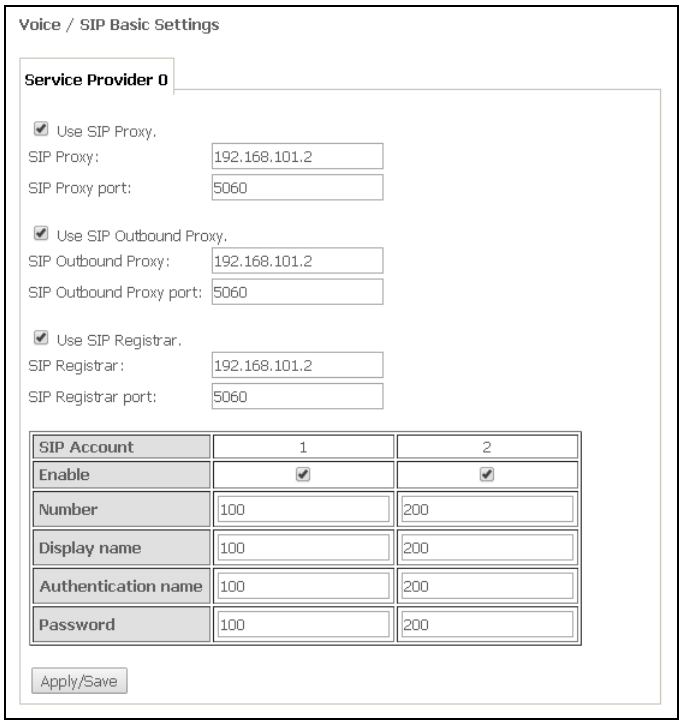
– *Select Diffie-Hellman Group for Key Exchange* – выбор длины группы MODP для разделяемого (двойного) ключа в небезопасной среде;

– *Key Life Time* – установка времени жизни ключа, в секундах.

Для принятия и сохранения настроек необходимо нажать кнопку *«Apply/Save».*

4.3 Меню «*Voice».* Настройки телефонии SIP[1]

4.3.1 Подменю *SIP Basic Setting.* Общие настройки SIP



– *SIP proxy* – адрес SIP proxy сервера для регистрации абонентов;

– *Use SIP Proxy* – при установленном флаге использовать SIP Proxy сервер:
  – *SIP Proxy* – адрес SIP Proxy;
  – *SIP Proxy port* – порт для SIP Proxy;

– *Use SIP Outbound Proxy* – при установленном флаге использовать SIP Outbound-proxy для передачи всех запросов, иначе – не использовать:
  – *SIP Outbound Proxy* – адрес SIP proxy, через который будет осуществляться передача всех запросов (запросы на SIP Proxy и SIP Registrar будут маршрутизироваться через этот сервер);
  – *SIP Outbound Proxy port* – порт для SIP proxy, через который будет осуществляться передача всех запросов;

– *Use SIP Registrar* – при установленном флаге использовать сервер регистрации SIP:
  – *SIP Registrar* – адрес сервера;
  – *SIP Registrar port* – порт сервера;

В таблице приведены общие параметры SIP для обоих портов FXS.

– *SIP Account* – аккаунт SIP (номер порта FXS);
– *Enable* – при установленном флаге данный порт включен в работу;

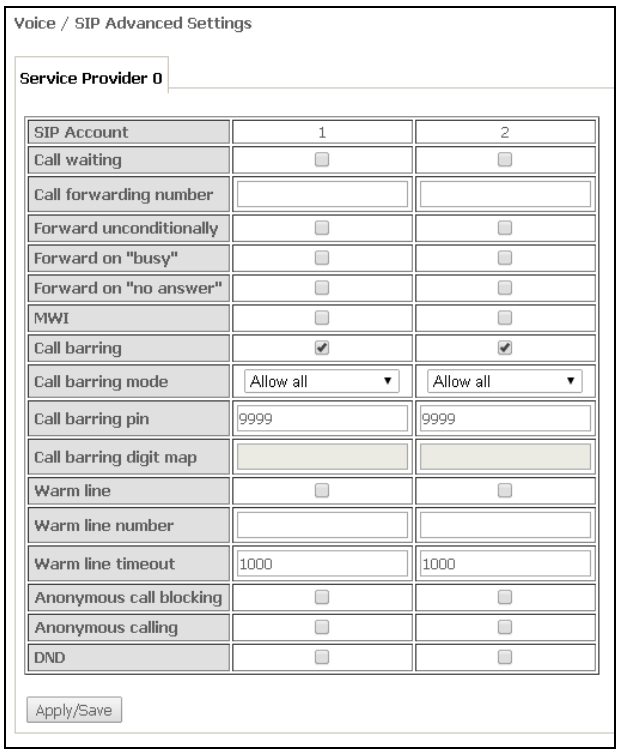
[1] При отсутствии меню в конфигураторе данные настройки уже выполнены Вашим оператором связи.

- *Number* – номер телефона;
- *Display name* – отображаемое имя пользователя;
- *Authentication name* – имя пользователя для аутентификации;
- *Password* – пароль для аутентификации;

Для принятия и сохранения изменений необходимо нажать кнопку *«Apply/Save».*

4.3.2 Подменю *SIP Advanced Setting.* Дополнительные настройки SIP

В данном меню производится настройка услуг ДВО *(*подробное описание доступно в ПРИЛОЖЕНИИ Б. ИСПОЛЬЗОВАНИЕ ДОПОЛНИТЕЛЬНЫХ УСЛУГ*)*.



- *SIP Account* – аккаунт SIP (номер порта FXS);
- *Call waiting* – при установленном флаге разрешено уведомление о поступлении нового вызова;
- *Call forwarding number*–номер для переадресации вызова;
- *Forward unconditionally*– при установленном флаге разрешена безусловная переадресация;
- *Forward on "busy"* – при установленном флаге разрешена переадресация вызова по занятости;
- *Forward on "no answer"*– при установленном флаге разрешена переадресация вызова по неответу абонента;
- *MWI* – при установленном флаге поддерживается индикация о наличии сообщений на голосовой почте;
- *Call barring* – при установленном флаге абонент может установить запрет на исходящие вызовы;
- *Call barring mode* –режим ограничения исходящих вызовов:
  - *Allow all* – все исходящие звонки разрешены;
  - *Deny all* – все исходящие звонки запрещены;
  - *Deny by digit map* – исходящие звонки запрещены только на номер, указанный в поле «Call barring digit map»;
- *Call barring pin* – пароль, по которому разрешено совершать вызовы;
- *Call barring digit map* – план нумерации, по которому разрешено/запрещено совершать вызовы*;*
- *Warm line* – при установленном флаге разрешена услуга «теплая линия», иначе – не разрешена. Услуга позволяет автоматически установить исходящее соединение без набора номера сразу после подъема трубки – *«горячая линия»*, либо с задержкой - *«теплая линия»;*
- *Warm line number* – номер *«теплой линии»;*

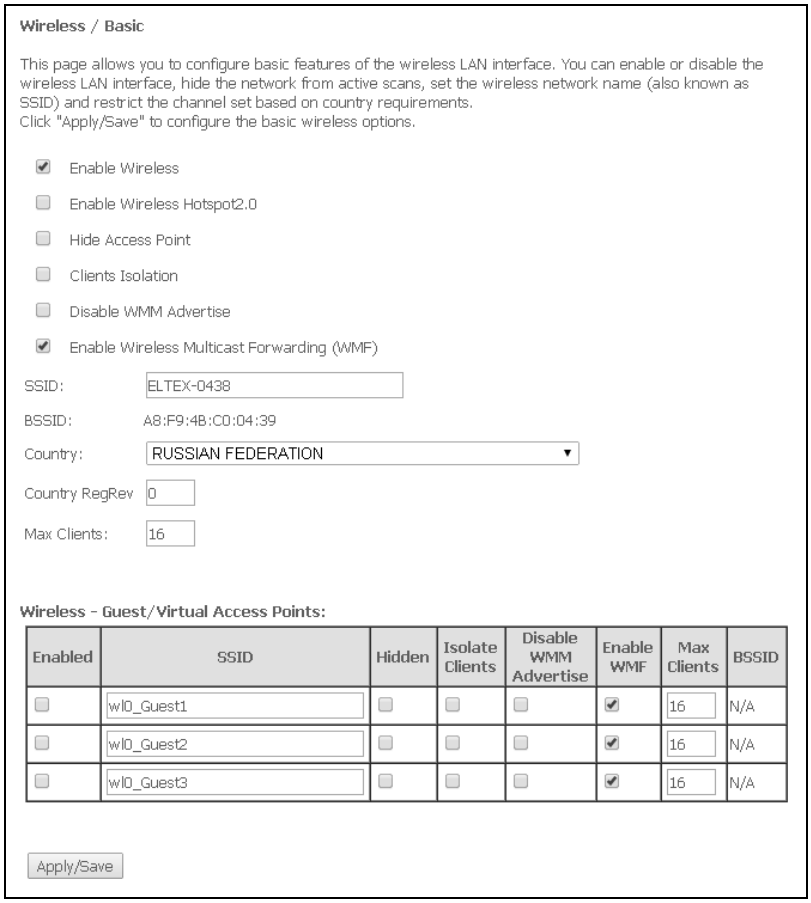
- *Warm line timeout* – таймаут до начала набора номера *«теплой линии»;*
- *Anonymous call blocking* – при установленном флаге разрешена блокировка вызовов от абонентов, номер которых не определен;
- *Anonymous calling* – при установленном флаге вызовы с порта совершаются анонимно (услуга Анти-АОН);
- *DND* – при установленном флаге включена услуга «Не беспокоить».

Для принятия и сохранения изменений необходимо нажать кнопку *«Apply/Save».*

4.4 Меню «*Wireless*». Настройка беспроводной сети

4.4.1 Подменю *Basic.* Общая информация

В данном меню производятся основные настройки беспроводного интерфейса LAN, а также возможно задать до трех виртуальных точек беспроводного доступа.



- *Enable Wireless* – включить Wi-Fi на устройстве;
- *Enable Wireless Hotspot2.0* - включить поддержку Hotspot2.0 на устройстве;
- *Hide Access Point* – скрытый режим работы точки доступа (в данном режиме SSID беспроводной сети не будет широковещательно распространяться маршрутизатором);
- *Clients Isolation* – при установленном флаге беспроводные клиенты не смогут взаимодействовать друг с другом;
- *Disable WMM Advertise* – отключить WMM (Wi-Fi Multimedia – QoS для беспроводных сетей);
- *Enable Wireless Multicast Forwarding (WMF)* – включить WMF;
- *SSID – Service Set Identifier* – назначить имя беспроводной сети(ввод с учетом регистра клавиатуры);

По умолчанию на устройстве установлено имя беспроводной сети (SSID) ELTEX-аааа, где аааа - это 4 последние цифры WAN MAC. WAN MAC указан в наклейке на корпусе устройства.

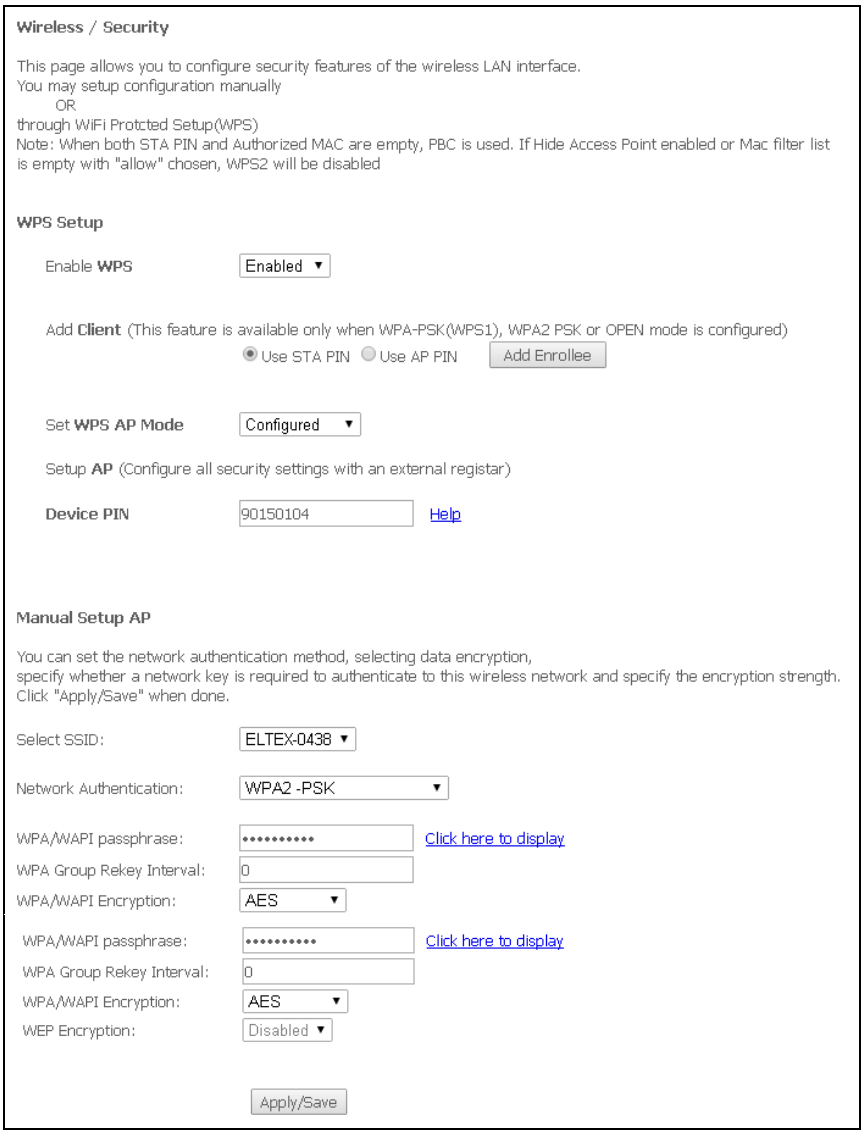
- *BSSID* – MAC-адрес точки доступа;

– *Country* – установить местоположение (страну);
– *Country RegRev* - установить идентификатор региона (для России: 0-34);
– *Max Clients* – установить максимально возможное количество одновременных беспроводных подключений.

Для принятия изменений необходимо нажать кнопку *«Apply/Save».*

4.4.2 Подменю ***Security.*** **Настройка параметров безопасности**

В данном меню производятся основные настройки шифрования данных в беспроводной сети. Возможно настроить клиентское оборудование беспроводного доступа вручную или автоматически, используя WPS.



WPS (Wi-Fi Protected Setup) – стандарт, разработанный альянсом производителей беспроводного оборудования Wi-Fi с целью упрощения процесса настройки беспроводной сети. Данная технология позволяет пользователю быстро, просто и безопасно настроить беспроводную сеть, не вникая в тонкости работы WI-FI и протоколов шифрования. WPS автоматически задает имя сети и шифрование для защиты от несанкционированного доступа, что в иных случаях приходилось делать вручную.

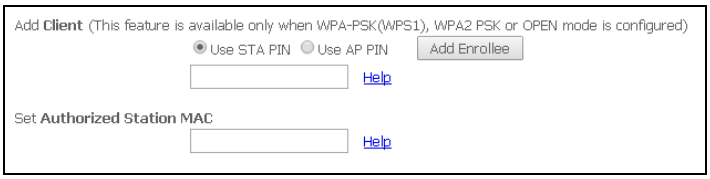
Для того чтобы подключиться, достаточно нажать на кнопку WPS, расположенную на боковой панели устройства, или же ввести PIN-код, используя веб-конфигуратор.

WPS setup:

– *Enable WPS* – для разрешения доступа по WPS в выпадающем списке выберите *«Enable»,* если сетевой адаптер WI-FI Вашего устройства поддерживает данный режим настройки;

– *Add Client*– выбор метода авторизации клиента (настройки применимы только в режимах *WPA-PSK, WPA2-PSK*). Для начала процесса авторизации необходимо нажать кнопку *«Add Enrollee»:*

– *Use STA PIN* – авторизация с помощью PIN кода, выданного клиентом;



– *Set Authorized Station MAC* – установить MAC-адрес клиентского устройства, запись в формате XX: XX: XX: XX: XX: XX;

– *Use AP PIN* – авторизация с использованием собственного PIN кода;

– *Set WPS AP Mode*– установить режим точки доступа WPS;

– *Device PIN* – собственный PIN код (восьмизначный цифровой код, генерируемый устройством).

Недостатки метода WPS

В Wi-Fi роутерах с поддержкой технологии WPS существует уязвимость относительно безопасности сети. Используя эту уязвимость, возможно подобрать пароли к протоколам шифрования WPA и WPA2. Уязвимость заключается в том, что можно методом подбора узнать используемый восьмизначный ключ сети (PIN-код).

Manual Setup AP:

– *Select SSID*– выбрать имя беспроводной сети из списка;

– *Network Authentication*– установить режим сетевой аутентификации из перечня в выпадающем списке:

– *open* – открытый – защита беспроводной сети отсутствует (в этом режиме может использоваться только WEP-ключ);

– *Shared* – общий (режим позволяет пользователям получать аутентификацию по их SSID или WEP-ключу);

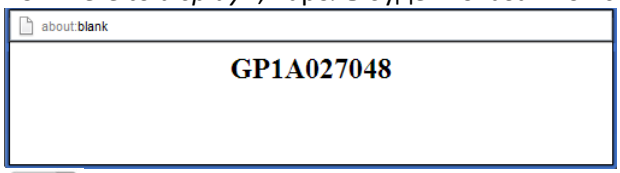
– *802.*1x – включает стандарт 802.1x(позволяет пользователям аутентифицироваться с использованием сервера аутентификации RADIUS, для шифрования данных используется WEP-ключ);

- *RADIUS Server IP Address* – IP-адрес RADIUS-сервера;
- *RADIUS Port* – номер порта RADIUS-сервера. По умолчанию установлен порт 1812;
- *RADIUS Key* – секретный ключ для доступа к RADIUS-серверу;

– *WPA2* – включает WPA2 (режим использует протокол WPA2 и требует использования сервера аутентификации RADIUS);

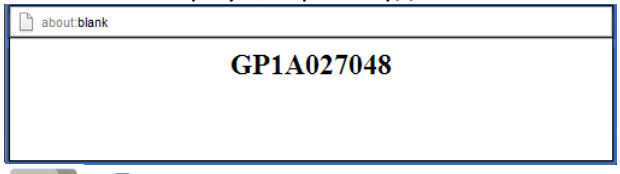
- WPA2 Preauthentication;
- Network Re-auth Interval;
- *WPA Group Rekey Interval* – интервал в секундах между сменой ключей шифрования WPA, используется для повышения уровня безопасности беспроводной сети. Если в смене ключей нет необходимости, оставьте в поле нулевое значение;
- *RADIUS Server IP Address* – IP-адрес RADIUS-сервера;
- *RADIUS Port* – номер порта RADIUS-сервера. По умолчанию установлен порт 1812;
- *RADIUS Key* – секретный ключ для доступа к RADIUS-серверу;
- *WPA/WAPI Encryption* – выбор метода шифрования данных WPA/WAPI;

- *WPA2-PSK* – включает WPA2-PSK (режим использует протокол WPA2, но не требует использования сервера аутентификации RADIUS);
  - *WPA/WAPI passphrase* – секретная фраза. Установка пароля, строка 8-63 символа ASCII. Для просмотра секретной фразы необходимо нажать на ссылку *«Clik here to display»*, пароль будет показан во всплывающем окне.



По умолчанию ключ сети соответствует серийному номеру устройства. Серийный номер указан в наклейке на корпусе устройства. При изменении пароля необходимо задать комбинацию из 10-ти символов. Пароль должен содержать цифры и латинские буквы в верхнем и нижнем регистрах.

  - *WPA Group Rekey Interval* – интервал в секундах между сменой ключей шифрования WPA, используется для повышения уровня безопасности беспроводной сети. Если в смене ключей нет необходимости, оставьте в поле нулевое значение;
  - *WPA/WAPI Encryption* – выбор метода шифрования данных WPA/WAP;
- *Mixed WPA2/WPA* – включает комбинацию WPA2/WPA (данный режим шифрования использует протоколы WPA2 и WPA, требует использования сервера аутентификации RADIUS);
  - *WPA2 Preauthentication* – предварительная проверка подлинности беспроводного клиента на других беспроводных точках доступа в используемом диапазоне. В течение проверки связь осуществляется через текущую беспроводную точку доступа;
  - *Network Re-auth Interval* – период повторной проверки подлинности. Определяет, как часто точка доступа посылает сообщение и требует от клиентов ответа, содержащего правильные данные безопасности;
  - *WPA Group Rekey Interval* – интервал в секундах между сменой ключей шифрования WPA, используется для повышения уровня безопасности беспроводной сети. Если в смене ключей нет необходимости, оставьте в поле нулевое значение;
  - *RADIUS Server IP Address* – IP-адрес RADIUS-сервера;
  - *RADIUS Port* – номер порта RADIUS-сервера. По умолчанию установлен порт 1812;
  - *RADIUS Key* – секретный ключ для доступа к RADIUS-серверу;
  - *WPA/WAPI Encryption* – выбор метода шифрования данных WPA/WAPI;
- *Mixed WPA2/WPA-PSK* – включает комбинацию WPA2/WPA-PSK (этот режим шифрования использует протоколы WPA2-PSK и WPA-PSK, не требует использования сервера аутентификации RADIUS).
  - *WPA/WAPI passphrase* – секретная фраза. Установка пароля, строка 8-63 символа ASCII. Для просмотра секретной фразы необходимо нажать на ссылку *«Clik here to display»*, пароль будет показан во всплывающем окне.



По умолчанию ключ сети соответствует серийному номеру устройства. Серийный номер указан в наклейке на корпусе устройства. При изменении пароля необходимо задать комбинацию из 10-ти символов. Пароль должен содержать цифры и латинские буквы в верхнем и нижнем регистрах.

- *WPA Group Rekey Interval* – интервал в секундах между сменой ключей шифрования WPA, используется для повышения уровня безопасности беспроводной сети. Если в смене ключей нет необходимости, оставьте в поле нулевое значение;
- *WPA/WAPI Encryption* – выбор метода шифрования данных WPA/WAPI;

Убедитесь, что беспроводной адаптер компьютера поддерживает выбранный тип шифрования.

Наиболее стойкую защиту беспроводного канала даёт совместная работа точки доступа и RADIUS сервера (для аутентификации беспроводных клиентов).

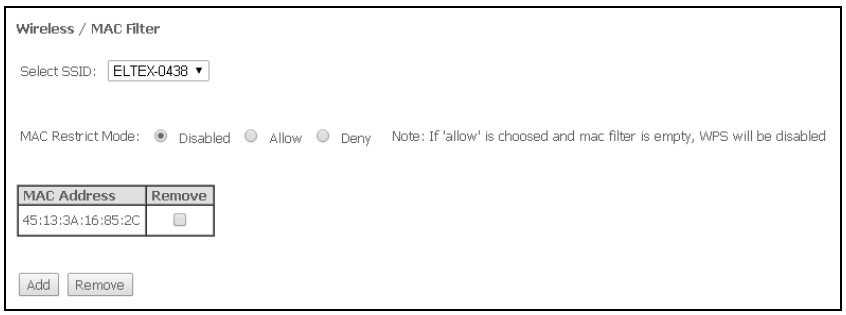
– *WEP Encryption*– для включения шифрования WEP выберите *Enable* в выпадающем списке;
  – *Encryption Strength* – 64- или 128-битное шифрование ключа*;*
  – *Current Network Key* – выбор ключа, который будет использоваться для установления соединения;
  – *Network Key 1..4* - возможно задать до четырех различных ключей из 10 символов в 16-ричной системе счисления либо 5 символов ASCII[1] для 64-х битного шифрования. Или 26 символов в 16-ричной системе счисления либо 13 символов ASCII для 128-х битного шифрования.

Для принятия изменений необходимо нажать кнопку *«Apply/Save».*

[1] ASCII - набор из 128 символов для машинного представления прописных и строчных букв латинского алфавита, чисел, знаков препинания и специальных символов.

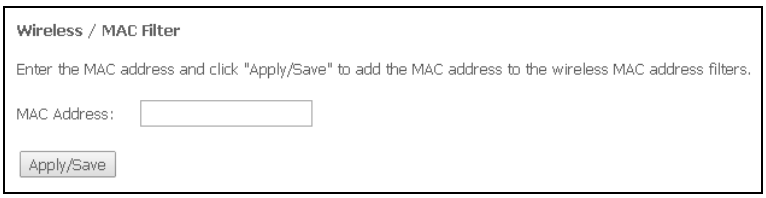
4.4.3 Подменю *MAC Filter.* Настройки фильтрации MAC-адресов

В данном меню производится настройка фильтрации MAC-адресов



- *Select SSID* – выбрать идентификатор беспроводной сети, для которой будет создано правило;
- *MAC Restrict Mode* – выбор режима фильтрации по MAC-адресам:
  - *Disabled* –не использовать фильтр;
  - *Allow* – фильтр по разрешенным адресам;
  - *Deny* – фильтр по запрещенным адресам.

Для добавления MAC-адреса в таблицу фильтрации необходимо нажать *«Add»* и ввести его значение в поле «MAC address» в открывшемся меню:

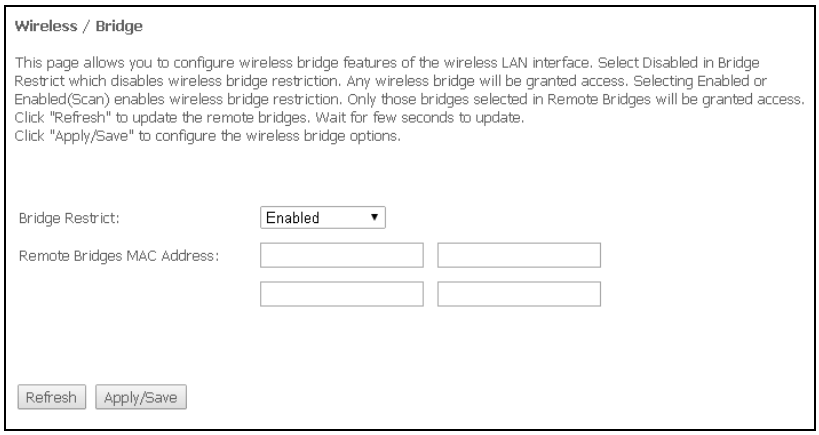


Для принятия изменений необходимо нажать кнопку *«Apply/Save».*

4.4.4 Подменю *Wireless Bridge.* Настройки беспроводного соединения в режиме моста

В данном меню задается режим работы точки доступа: в качестве точки доступа или беспроводного моста.

При использовании режима моста необходимо ввести MAC-адреса удаленных мостов. Данный режим используется для установки беспроводного соединения между двумя отдельными сетями.



В режиме «Wireless Bridge» возможно задать следующие настройки:

- *Bridge Restrict* – выбор режима работы моста:
  - *Enabled* – включить фильтр по MAC-адресам(разрешены только заданные адреса);
  - *Enable(Scan)* – поиск удаленных мостов;
  - *Disable* – ограничения по MAC-адресам отсутствуют;
- *Remote Bridges MAC Address* – адреса удаленных мостов.

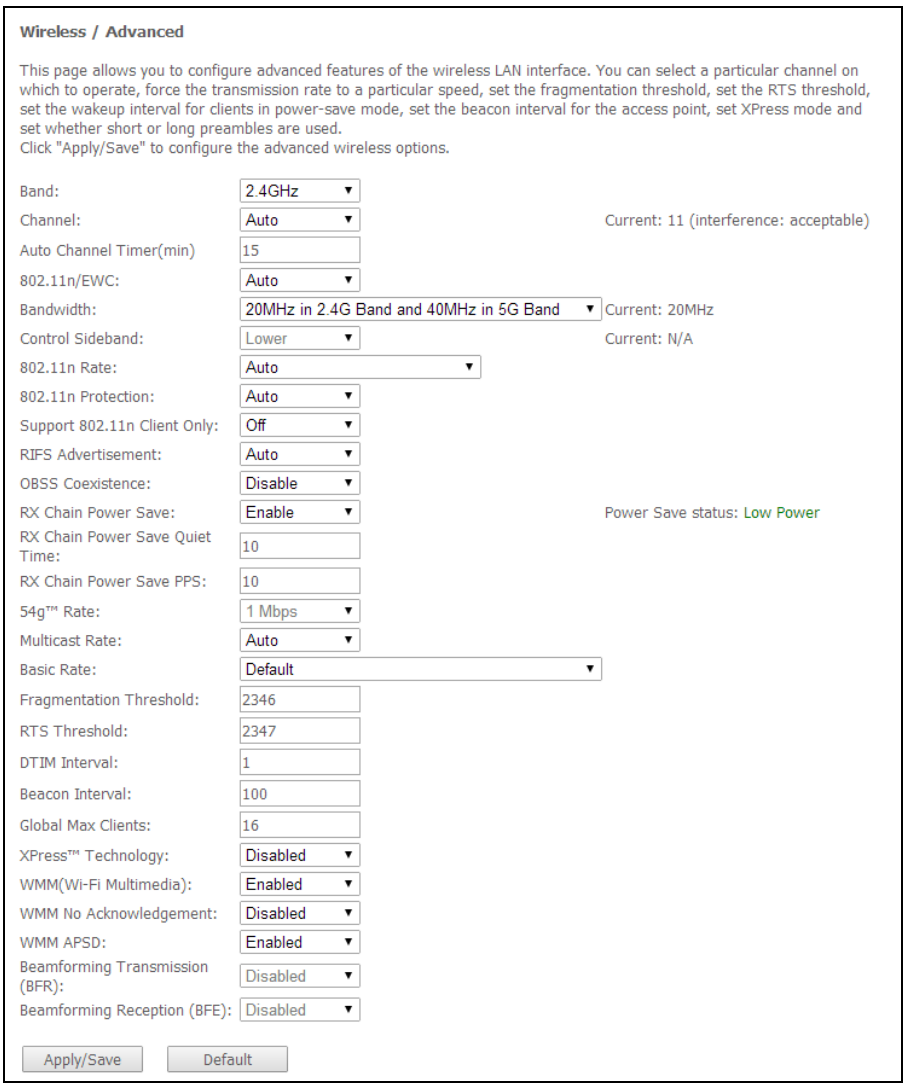
В режиме моста маршрутизатор не поддерживает функцию Wi-Fi Multimedia (WMM).

Для обновления доступных удаленных мостов необходимо нажать *«Refresh».*

Для принятия и сохранения изменений необходимо нажать кнопку *«Apply/Save».*

4.4.5 Подменю ***Advanced.*** **Расширенные настройки**

В данном меню производится расширенные настройки беспроводной сети.



- *Band* – установка частотного диапазона;
- *Channel* – устанавливает рабочий канал для маршрутизатора. При наличии помех или проблем в работе беспроводной сети изменение канала может способствовать их устранению. Рекомендуется установить значение "Auto" во избежание помех, вызываемых работой смежных сетей;
- *Auto Channel Timer (min)* – время в минутах, через которое маршрутизатор будет искать более оптимальный беспроводный канал. Параметр доступен, если установлен Auto выбор канала (0 – выключить);

- *802.11n/EWC* – режим совместимости с оборудованием 802.11n Draft2.0 и EWC(Enhanced Wireless Consortium);
- *Bandwidth* – установка полосы пропускания 20ГГц или 40 ГГц. В режиме 40 МГц используются две смежные полосы по 20 МГц для увеличения пропускной способности канала;
- *Control Sideband* – выбор второго канала(Lower или Upper) в режиме 40 МГц;
- *802.11n Rate* – установка скорости соединения;
- *802.11n Protection* – при включении увеличится безопасность, но уменьшится пропускная способность;
- *Support 802.11n Client Only* – при включении клиентам 802.11b/g будет запрещен доступ к устройству;
- *RIFS Advertisemen* – (Reduced Interframe Space) уменьшение интервала между блоками данных (PDUs), повышает эффективность Wi-Fi;
- *OBSS Co-Existance* – настройка толерантности при выборе режима работы (20Мгц или 40Мгц). Если параметр в состоянии *«Enable»* – будет выбран оптимальный режим работы устройства, учитывая *«Bandwidth*», иначе режим работы будет зависеть только от параметра *«Bandwidth»;*
- *RX Chain Power Save* – отключение приема на одной из антенн устройства в целях энергосбережения;
- *RX Chain Power Save Quiet Time* – период времени, в течении которого интенсивность трафика должна быть ниже PPS, для включения режима энергосбережения;
- *RX Chain Power Save PPS* – верхняя граница параметра PPS (packet per second). Если в течение времени, определенного параметром *«RX Chain Power Save Quiet Time»,* интенсивность пакетов на интерфейсе WLAN не превышает данную величину, включается режим энергосбережения;
- *54g™ Rate* – установка скорости в режиме совместимости с устройствами 54g™;
- *Multicast Rate* – установка скорости трафика при многоадресной передаче;
- *Basic Rate* –базовая скорость передачи;
- *Fragmentation 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;
- *DTIM Interval* – временной интервал, по истечении которого широковещательные и многоадресные пакеты, помещенные в буфер, будут доставлены беспроводным клиентам;
- *Beacon Interval* – период отправки информационного пакета в беспроводную сеть, сигнализирующего о том что точка доступа активна;
- *Global Max Clients* – максимальное количество беспроводных клиентов;
- *XPress™ Technology* – использование позволяет повысить пропускную способность до 27% в сетях стандарта 802.11g. А в смешанных сетях 802.11g и 802.11b использование XPress™ Technology может повысить пропускную способность до 75%;
- *WMM (Wi-Fi Multimedia)* – установка режима Wi-Fi Multimedia (WMM). Данный режим позволяет быстро и качественно передавать аудио- и видеоконтент одновременно с передачей данных;
- *WMM No Acknowledgement* – при использовании данного режима приёмная сторона не подтверждает принятые пакеты. В среде с малым количеством помех это позволит увеличить эффективность передачи, в среде с большим количеством помех эффективность передачи снизится;
- *WMM APSD* – установить автоматический переход в режим экономии энергии (enabled – автоматический переход разрешен);

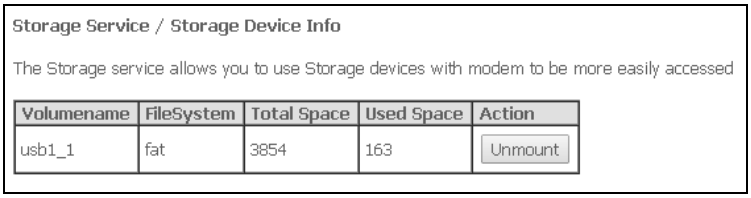
- *Beamforming Transmission (BFR)*[1] – функция формирование луча позволяет уменьшить интерференцию при передаче беспроводного сигнала и улучшить качество Wi-Fi соединения;
- *Beamforming Reception (BFE)*[2] – функция концентрации при приеме сигнала позволяет улучшить качество Wi-Fi соединения.

Для принятия и сохранения изменений необходимо нажать кнопку *«Apply/Save»*.

4.5 Меню «Storage Service». Службы файловых хранилищ

4.5.1 Подменю *Storage Device Info.* Информация о подключенных USB-устройствах

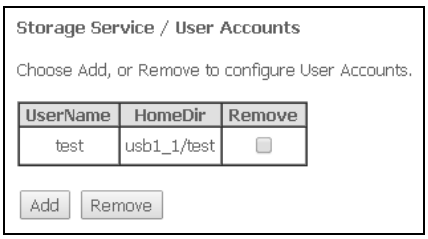
В данном меню доступен список всех подключенных запоминающих устройств. Предоставляется следующая информация:



- *Volumename* – имя устройства;
- *FileSystem* – тип файловой системы;
- *Total Space* – общий объем;
- *Used Space* – используемый объем;
- *Unmount* – для безопасного извлечения устройства необходимо предварительно нажать данную кнопку.

4.5.2 Подменю *User Accounts.* Настройка пользователей Samba

В данном меню происходит настройка учетных записей пользователей Samba.



Для добавления записи необходимо нажать кнопку *«Add»*. Для удаления - установить флаг напротив требуемой записи в колонке Remove и нажать кнопку *«Remove»*.

- *Username* –логин для доступа к сетевому ресурсу;
- *Password* – пароль для доступа к сетевому ресурсу;
- *Confirm Password* – подтверждение пароля для доступа;
- *volumeName* – путь к сетевому ресурсу (имя подключенного запоминающего устройства отображается на странице *«Storage Device Info»).*

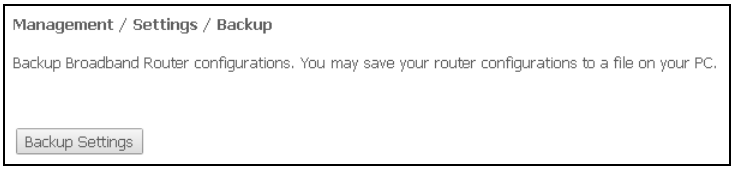
[1] В текущей версии не поддерживается
[2] В текущей версии не поддерживается

4.6 Меню «*Management*». Управление устройством

4.6.1 Подменю *Settings.* Настройки

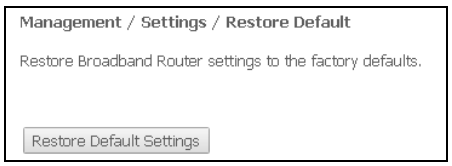
4.6.1.1 Подменю *Backup*. Резервное копирование

Меню позволяет по нажатию кнопки *«Backup Settings»* выгрузить конфигурацию на ПК.



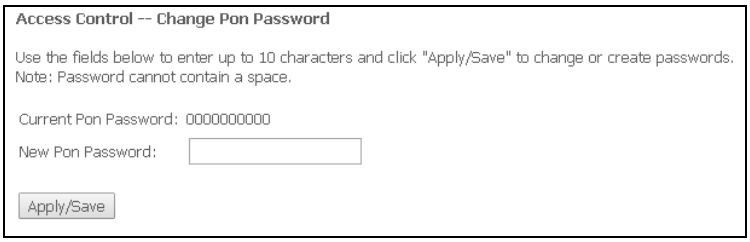
4.6.1.2 Подменю *Restore Default.* Возврат к настройкам по умолчанию

Меню позволяет вернуться к настройкам устройства, установленным по умолчанию. Устройство при этом будет перезагружено.



4.6.2 Подменю *Pon Password*. Смена пароля для доступа к сети PON

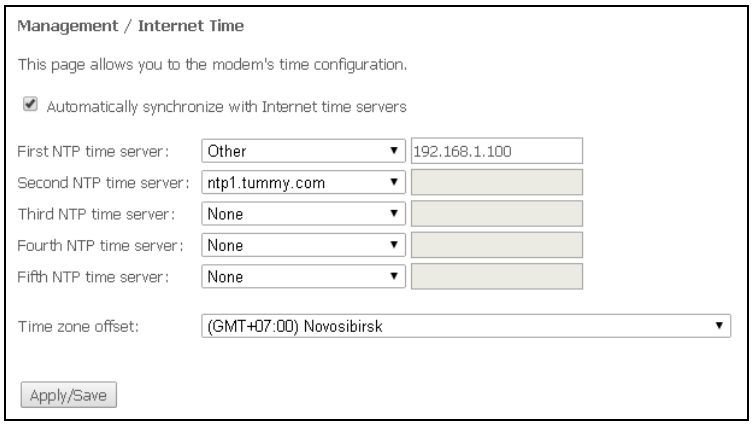
Данное меню позволяет изменить пароль для авторизации NTU-RG на станционном устройстве пассивной оптической сети.



Для смены пароля необходимо ввести 10 символов в поле *«New Pon Password»* . Для принятия и сохранения изменений необходимо нажать кнопку *«Apply/Save».* Применение настроек произойдет после перезагрузки устройства.

Настоятельно не рекомендуется изменять пароль самостоятельно – это может привести к потере связи со станционным устройством.

4.6.3 Подменю *Internet Time.* Настройки системного времени



Во вкладке настраивается системное время на устройстве.

– *Automatically synchronize with Internet time servers* – при установленном флаге производить автоматическую синхронизацию с интернет-серверами точного времени;

– *First NTP time server* –выбор основного сервера точного времени;

– *Second NTP time server* – выбор второго сервера точного времени, none – не использовать дополнительные сервера;

– *Third NTP time server* – выбор третьего сервера точного времени, none – не использовать дополнительные сервера;

– *Fourth NTP time server* – выбор четвертого сервера точного времени, none – не использовать дополнительные сервера;

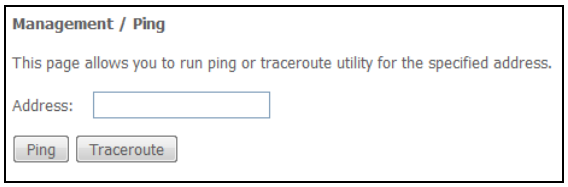
– *Fifth NTP time server* – выбор пятого сервера точного времени, none – не использовать дополнительные сервера;

– *Time zone offset* – установка часового пояса в соответствии с всемирным координационным временем (UTC).

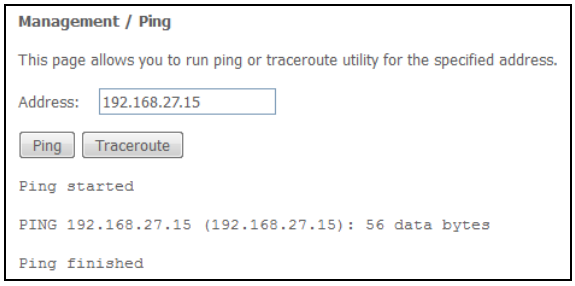
При выборе в выпадающем списке серверов значения *Other* справа станет активным окно для заполнения, куда следует вручную ввести адрес сервера точного времени.

4.6.4 Подменю *Ping*. Проверка доступности сетевых устройств

Данное меню предназначено для проверки доступности подключенных к маршрутизатору сетевых устройств при помощи утилиты Ping.

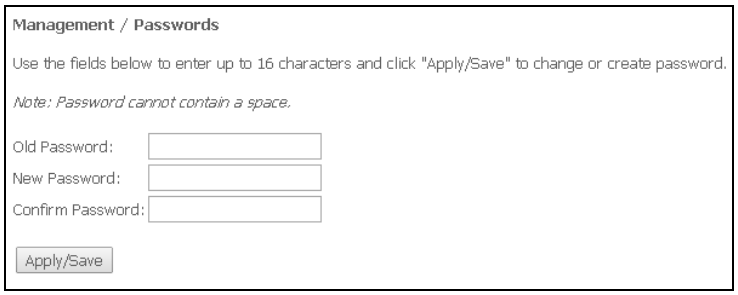


Для проверки доступности подключенного устройства необходимо ввести его IP-адрес в поле и нажать кнопку «Ping». Для просмотра трассировки маршрута нажмите кнопку *«TraceRoute».* Вывод будет осуществлен на данной странице web-конфигуратора.



4.6.5 Подменю ***Passwords***. **Настройка контроля доступа (установление паролей)**

В данном меню осуществляется смена пароля для доступа к устройству.



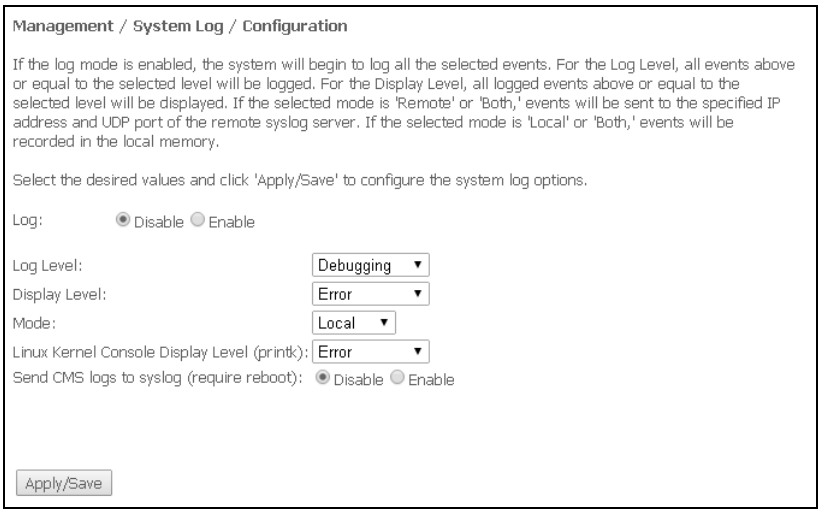
Для смены пароля необходимо ввести существующий пароль, затем новый пароль и подтвердить его.

Для принятия изменений и сохранения необходимо нажать кнопку *«Apply/Save».*

4.6.6 Подменю ***System Log.*** **Просмотр и настройка системного журнала**

4.6.6.1 Подменю ***Configuration.*** **Настройка системного журнала**

Меню используется для настройки событий, происходящих на маршрутизаторе.



- *Log* – включение/выключение системного журнала(enable/disable);
- *Log Level* – установка уровня детализации журнала событий. Классификация уровней важности в порядке снижения значимости:
  - *Emergency* – аварийный случай;
  - *Alert* – тревога;
  - *Critical* – критическое событие;
  - *Error* – ошибка;
  - *Warning* – предупреждение;
  - *Notice* – уведомление;
  - *Informational* – информация;
  - *Debugging* – устранение неполадок;
- *Display Level* – установка уровня отображения выводимых сообщений журнала событий;
- *Mode* – режим работы журнала:
  - *Local* – местный (все события возвращаются на маршрутизатор через буферную память);
  - *Remote* – удаленный (все события возвращаются на сервер Syslog);
  - *Both* – работают оба режима;

– *Flash* – отправка на USB-накопитель;

– *Linux Level Console Display Level (printk)* – установка уровня сообщений, выводимых в консоль Linux;

– *Send CMS logs to syslog (require reboot)* – включение/выключение отправки сообщений от CMS в системный журнал.

При выборе удаленного режима (Remote) доступны следующие настройки:

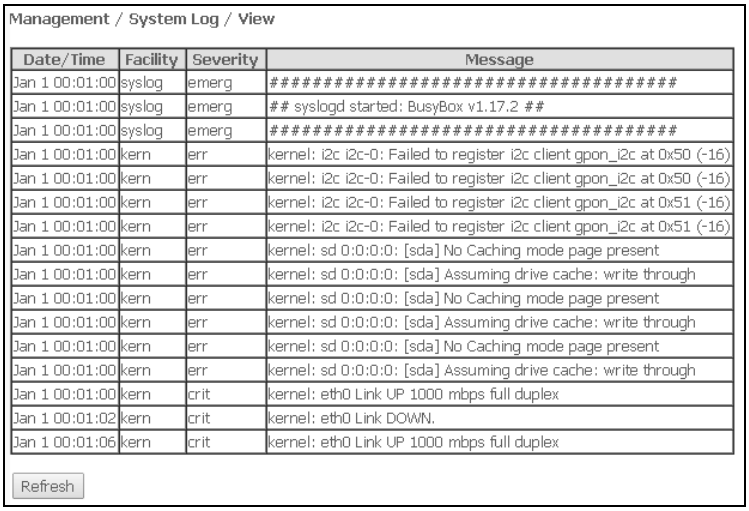
– *Server IP address* – IP-адрес сервера Syslog, на котором сохраняются все события;

– *Server IP Port* – номер порта сервера Syslog.

Для принятия изменений и сохранения необходимо нажать кнопку *«Apply/Save».*

4.6.6.2 Подменю ***View.*** **Просмотр системного журнала**

Меню служит для просмотра событий, происходящих на маршрутизаторе.

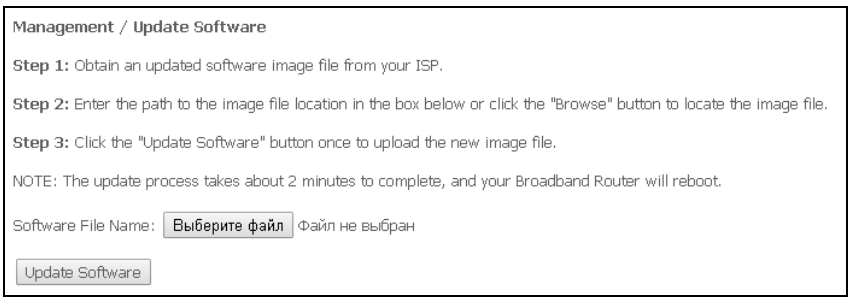


Чтобы закрыть окно просмотра журнала, нажмите *«Close».* Обновить информацию можно кнопкой *«Refresh».*

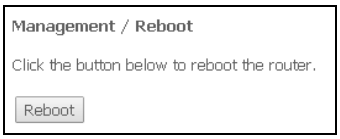
4.6.7 Подменю ***Update Software.*** **Обновление ПО**

Для обновления ПО необходимо выбрать файл ПО в строке *«Software File name*» (используя кнопку *«Выберите файл»* или *«Обзор..»*) и нажать «*Update Software*».

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

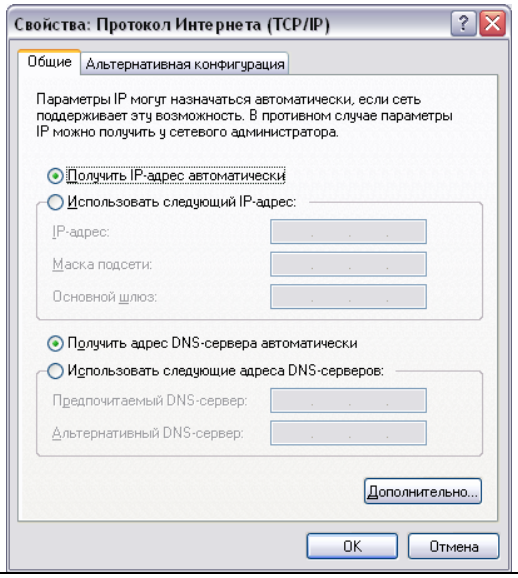


4.6.8 Подменю *Reboot.* Перезагрузка устройства



Для перезагрузки устройства необходимо нажать на кнопку *«Reboot»*. Перезагрузка устройства может занять несколько минут.

ПРИЛОЖЕНИЕ А ВОЗМОЖНЫЕ ПРОБЛЕМЫ И ВАРИАТЫ ИХ РЕШЕНИЯ

Проблема	Возможная причина	Решение
При вводе IP-адреса маршрутизатора (например, 192.168.1.1) не удается получить доступ к Web-интерфейсу	компьютер не принадлежит к данной IP-подсети для подключения к Web-интерфейсу.	В свойствах подключения к интернету на Вашем компьютере установите параметр «Получать IP-адрес автоматически». 
	на компьютере установлен Web-браузер с выключенной опцией Java-script	включите опцию Java-script в Вашем браузере или воспользуйтесь другим Web-браузером
	неисправный кабель	проверьте физическое соединение по статусу индикаторов (они должны гореть). Если индикаторы не горят, попробуйте использовать другой кабель или подключитесь к другому порту устройства, если это возможно. Если компьютер выключен, индикатор может не гореть.
	доступ запрещен программным обеспечением интернет-безопасности Вашего компьютера	отключите программное обеспечение интернет-безопасности на компьютере (брэндмауэры)
Воспроизводится сигнал ошибки в телефоне, подключенном к порту FXS	Неверные настройки порта	проверьте корректность настроек в меню *«VoIP»* (см. 4.3 Меню «*Voice*». Настройки телефонии SIP)
Утерян/не подходит пароль доступа к WEB-интерфейсу устройства	_____	Необходимо сбросить маршрутизатор к настройкам по умолчанию с помощью кнопки F на задней панели устройства. К сожалению, при этом все выполненные настройки будут утрачены.

ПРИЛОЖЕНИЕ Б. ИСПОЛЬЗОВАНИЕ ДОПОЛНИТЕЛЬНЫХ УСЛУГ

1. Уведомление о поступлении нового вызова – Call Waiting

Услуга позволяет пользователю при занятости его телефонным разговором с помощью определенного сигнала получить оповещение о новом входящем вызове.

Пользователь при получении оповещения о новом вызове может принять ожидающий вызов.

Доступ к услуге устанавливается через меню настроек абонентского порта на странице *«Voice/SIP Advanced Setting» (**раздел 4.3.2 Подменю SIP Advanced Setting. Дополнительные настройки SIP**)* путем установки флага «*Call waiting*».

Использование услуги:

Находясь в состоянии разговора и при получении индикации о поступлении нового вызова, нажав R, возможно принять ожидающий вызов с установкой текущего соединения на удержание. Последующие нажатия R обрабатываются в соответствии с алгоритмами, описанными в разделе ***2* Передача вызова – Calltransfer** и **3 Конференция – Conference.**

– R – короткий отбой (flash).

2. Передача вызова – Calltransfer

Услуга *«Calltransfer»* позволяет временно разорвать соединение с абонентом, находящимся на связи (абонент А), установить соединение с другим абонентом (абонент С) и передать вызов с отключением абонента В (абонента выполняющего услугу).

Использование услуги:

Находясь в состоянии разговора с абонентом А, установить его на удержание с помощью короткого отбоя flash (R), дождаться сигнала «ответ станции» и набрать номер абонента С. После ответа абонента С положить трубку.

3. Конференция – Conference

Конференция – услуга, обеспечивающая возможность одновременного телефонного общения трех и более абонентов.

Использование услуги:

Находясь в состоянии разговора с абонентом А, установить его на удержание с помощью короткого отбоя flash (R), дождаться сигнала «ответ станции» и набрать номер абонента С. После ответа абонента С, нажав R, перейти в режим конференцсвязи.

Абонент, собравший конференцию, является ее инициатором, другие два абонента – ее участниками. В режиме конференции нажатие короткого отбоя flash инициатором приводит к отключению абонента, вызов которому был совершен последним. Участник конференции, имеет возможность поставить на удержание остальных членов конференции.

Конференция разрушается, если ее покидает инициатор, обоим участникам при этом будет передано сообщение отбоя. Если конференцию покидает любой из участников, то ее инициатор и второй участник переключатся в состояние обычного двустороннего разговора.

4. **Message Waiting Indication (MWI) - индикация о наличии голосовых сообщений в почтовом ящике**

Если абоненту оставлено на сервере голосовое сообщение, то включение данной услуги предоставит возможность своевременно узнать об этом. При включенной услуге MWI, если на сервере имеется новое сообщение, абонент при поднятии трубки услышит прерывистый зуммер.

Для включения услуги MWI необходимо на странице *«Voice/SIP Advanced Setting» (**раздел 4.3.2 Подменю SIP Advanced Setting. Дополнительные настройки SIP**)* установить флаг в поле *«MWI»* для требуемого порта.

5. **Запрет на исходящие вызовы – Call Barring**

Услуга позволяет установить ограничение на доступ с телефонного аппарата абонента к определенным видам исходящей связи.

Доступ к услуге осуществляется через меню настроек абонентского порта на странице «*Voice/SIP Advanced Setting*» *(**раздел 4.3.2*** **Подменю *SIP Advanced Setting.* Дополнительные настройки SIP***)* путем установки флага «*Call barring*» и задания необходимых параметров в полях *«Call barring mode»* и *«Call barring digit map».*

Возможно 3 варианта ограничения вызовов в зависимости от параметра, указанного в поле «Call barring mode»:

- *Allow all* – все исходящие звонки разрешены
- *Deny all* – все исходящие звонки запрещены
- *Deny by digit map* – исходящие звонки запрещены только на номер, указанный в поле «Call barring digit map»

Использование услуги:

Значение *«Call barring digit map»* - 1150. Для ограничения всех исходящих вызовов в поле *«Call barring mode»* необходимо выбрать значение «*Deny all*». Для того, чтобы разрешить все исходящие вызовы, требуется выбрать «*Allow all*». Для запрета исходящих звонков на номер 1150 необходимо задать «*Deny by digit map*» в поле *«Call barring mode».*

СВИДЕТЕЛЬСТВО О ПРИЕМКЕ И ГАРАНТИИ ИЗГОТОВИТЕЛЯ NTU-2V

Абонентский оптический терминал NTU-2V зав. № _____ соответствует требованиям технических условий ТУ6650-100-33433783-2013 и признан годным для эксплуатации.

Транспортирование оборудования должно производиться по условиям 5 , хранение – по условиям 1 по ГОСТ 15150.

Предприятие-изготовитель ООО «Предприятие «Элтекс» гарантирует соответствие абонентского шлюза требованиям технических условий ТУ6650-100-33433783-2013 при соблюдении потребителем условий эксплуатации, установленных в настоящем руководстве.

Гарантийный срок 1 год. Дата изготовления указана на упаковке.

Изделие не содержит драгоценных материалов.

Директор предприятия _____ Черников А. Н.
подпись Ф.И.О.

Начальник ОТК предприятия _____ Игонин С.И.
подпись Ф.И.О.

Изготовитель:
ООО «Предприятие «Элтекс»
630020 г. Новосибирск,
ул. Окружная, 29В
E-mail: eltex@eltex.nsk.ru

Сделано в России

СВИДЕТЕЛЬСТВО О ПРИЕМКЕ И ГАРАНТИИ ИЗГОТОВИТЕЛЯ NTU-RG-1402G-W

Абонентский оптический терминал NTU-RG-1402G-W зав. № _____ соответствует требованиям технических условий ТУ6650-101-33433783-2013, ТУ 6650-108-33433783-2014 и признан годным для эксплуатации.

Транспортирование оборудования должно производиться по условиям 5 , хранение – по условиям 1 по ГОСТ 15150.

Предприятие-изготовитель ООО «Предприятие «Элтекс» гарантирует соответствие абонентского шлюза требованиям технических условий ТУ6650-101-33433783-2013, ТУ6650-108-33433783-2014при соблюдении потребителем условий эксплуатации, установленных в настоящем руководстве.

Гарантийный срок 1 год. Дата изготовления указана на упаковке.

Изделие не содержит драгоценных материалов.

Директор предприятия _____ Черников А. Н.

подпись Ф.И.О.

Начальник ОТК предприятия _____ Игонин С.И.

подпись Ф.И.О.

Изготовитель:
ООО «Предприятие «Элтекс»
630020 г. Новосибирск,
ул. Окружная, 29В
E-mail: eltex@eltex.nsk.ru

Сделано в России