Абонентский маршрутизатор

RG-35-WZ

Руководство по эксплуатации, версия ПО 1.7.0 (02.2018)

IP-адрес: http://192.168.1.1

имя пользователя: admin

пароль: password

Версия документа	Дата выпуска	Содержание изменений
Версия 1.0	03.08.2017	Первая публикация
Версия программного обеспечения	Версия ПО**: 1.7.0** Версия web-интерфейса: **1.0.1**	

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

1.1 Аннотация

Современные тенденции развития связи диктуют операторам необходимость поиска наиболее оптимальных технологий, позволяющих удовлетворить стремительно возрастающие потребности абонентов, сохраняя при этом преемственность бизнес-процессов, гибкость развития и сокращение затрат на предоставление различных сервисов. Беспроводные технологии набирают обороты и уже за короткое время прошли огромный путь от нестабильных низкоскоростных сетей связи малого радиуса до сетей широкополосного доступа, сопоставимых по скорости с проводными сетями с высокими критериями к качеству предоставления услуг.

Устройство RG-35-WZ является точкой доступа Wi-Fi с интегрированным маршрутизатором. Основное предназначение RG-35-WZ: установка внутри зданий в качестве точки доступа к различным ресурсам по проводным и беспроводным сетям передачи данных.

Устройство ориентировано на домашних пользователей и небольшие офисы.

В настоящем руководстве по эксплуатации изложены назначение, основные технические характеристики, конструктивное исполнение, порядок установки, правила конфигурирования, мониторинга и смены программного обеспечения точки доступа RG-35-WZ.

1.2 Условные обозначения

Обозначение	Описание
Полужирный шрифт	Полужирным шрифтом выделены примечания и предупреждения, название глав, заголовков, заголовков таблиц.
Курсивом	Курсивом указывается информация, требующая особого внимания.

Примечания и предупреждения

Примечания содержат важную информацию, советы или рекомендации по использованию и настройке устройства.

Предупреждения информируют пользователя о ситуациях, которые могут нанести вред устройству или человеку, привести к некорректной работе устройства или потере данных.

2 ОПИСАНИЕ ИЗДЕЛИЯ

2.1 Назначение

Для возможности предоставления пользователям доступа к высокоскоростной безопасной сети передачи данных разработан абонентский маршрутизатор RG-35-WZ (далее «устройство»).

Устройство RG-35-WZ – единая точка доступа к современным интерактивным сервисам по проводным и беспроводным сетям передачи данных: Интернет и Full HD IPTV. RG-35-WZ имеет встроенный контроллер «Умного дома» для подключения и взаимодействия с датчиками и устройствами системы «Умный дом» по радиоканалу Z-Wave и управления ими через платформу Eltex Smart Control.

Маршрутизатор RG-35-WZ предназначен для подключения устройств к беспроводной сети, поддерживающей стандарты IEEE 802.11a/b/g/n/ac. RG-35-WZ подключается к проводной сети с помощью 10/100/1000M Ethernet-интерфейса, и с помощью радиоинтерфейса создает беспроводной высокоскоростной доступ для устройств, поддерживающих технологию Wi-Fi в диапазоне 2,4 и 5 ГГц. К RG-35-WZ можно подключить до четырех устройств проводной сети. USB-разъем используется для подключения внешних накопителей или 3G/4G USB-модема.

RG-35-WZ поддерживает современные требования к качеству сервисов и позволяет передавать наиболее важный трафик в более приоритетных очередях по сравнению с обычным. Обеспечение приоритизации происходит при помощи основных технологий QoS.

В устройстве реализован расширенный функционал для стабильной работы IP-телевидения по беспроводной сети: плавность и непрерывность воспроизведения видео обеспечиваются специальным программным функционалом. Устройство позволяет работать на частотах 2,4 и 5 ГГц, а также предоставляет возможность одновременной трансляции видеопотоков и передачи данных.

2.2 Характеристика устройства

Интерфейсы:

- LAN: 4 порта Ethernet RJ-45 10/100BASE-T;
- WAN: 1 порт Ethernet RJ-45 10/100/1000BASE-T;
- WLAN: IEEE 802.11b/g/n 2,4 ГГц и 802.11a/n/ac 5 ГГц;
- USB: 1 порт USB2.0.

Питание устройства осуществляется через внешний адаптер 5 В от сети 220 В.

Функции:

- *сетевые функции:*
  - работа в режиме «моста» , «маршрутизатора» или "WISP";
  - поддержка PPPoE (PAP, SPAP и CHAP авторизация, PPPoE компрессия);
  - поддержка PPTP;
  - поддержка L2TP;
  - поддержка статического адреса и DHCP (DHCP-клиент на стороне WAN, DHCP-сервер на стороне LAN);
  - поддержка DNS;
  - поддержка NAT;

  - поддержка UPnP;
  - сетевой экран (Firewall);
  - клонирование MAC-адреса на WAN-интерфейсе;
  - поддержка NTP;
  - поддержка механизмов качества обслуживания QoS;
  - «проброс» портов (Port forwarding);
  - статическая и динамическая маршрутизация;
  - ограничение доступа к устройству через WAN и LAN.

- поддержка функций IPTV (IGMP-proxy, UDP-to-HTTP proxy);
- обновление ПО через web-интерфейс;
- TR-069;
- удаленный мониторинг, конфигурирование и настройка: web-интерфейс, Telnet.

На рисунке 1 приведена схема применения оборудования RG-35-WZ.

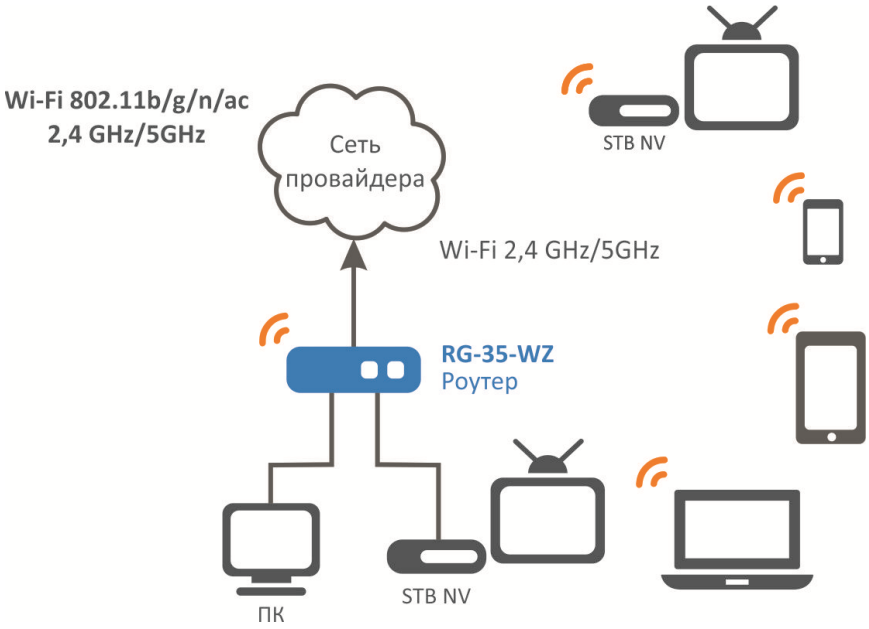


Рисунок 1 - Функциональная схема использования RG-35-WZ

2.3 Основные технические параметры

Основные технические параметры устройства приведены в Таблица 1.

Таблица 1 – Основные технические параметры

Общие параметры

Процессор	RTL8197F
Тактовая частота	1000 МГц
RAM DDR (оперативная память)	128 Мб
ROM eMMC flash (системная память)	16 Мб
Операционная система	Linux

Параметры WAN-интерфейса Ethernet

Количество портов	1
Электрический разъем	RJ-45
Скорость передачи, Мбит/с	10/100/1000, автоопределение
Поддержка стандартов	BASE-T

Параметры LAN-интерфейса Ethernet

Количество интерфейсов	4
Электрический разъем	RJ-45
Скорость передачи, Мбит/с	10/100, автоопределение
Поддержка стандартов	BASE-T

Параметры беспроводного интерфейса

Стандарты	802.11 a/b/g/n/ac
Частотный диапазон, МГц	2.4 ~ 2.4835 ГГц, 5.15 ~ 5.35 ГГц, 5.65 ~ 5.73 ГГц, 5.735 ~ 5.835 ГГц
MIMO	2x2 2,4 ГГц; 2x2 5 ГГц
Модуляция	BPSK, QPSK, 16 QAM, 64 QAM, 256QAM, DBPSK, DQPSK, CCK
Скорость передачи данных, Мбит/с	**802.11a до 54 Мбит/с** 802.11b до 11 Мбит/с 802.11a/g до 54 Мбит/с **802.11n (HT20) до 144 Мбит/с** 802.11n (HT40) до 300 Мбит/с 802.11ac (HT80) до 866 Мбит/с
Максимальная выходная мощность передатчика	**2,4 ГГц (802.11 b/g/n): до 15 дБм** **5 ГГц (802.11 a/n/ac): до 17 дБм**
Чувствительность приемника	2,4 ГГц: **802.11n(MCS0):** -90 дБм **802.11n(MCS4):** -79 дБм **802.11n(MCS7):** -72 дБм 5 ГГц: **802.11ac (MCS0):** -92 дБм **802.11ac (MCS4):** -82 дБм **802.11ac (MCS7):** -76 дБм
Безопасность	64/128/152-битное WEP-шифрование данных; WEP, TKIP и AES

Управление

Удаленное управление	Web-интерфейс, Telnet, TR-069
Ограничение доступа	по паролю, по IP-адресам (белый список)

Общие параметры

Питание	адаптер питания 5 В DC, 2,5 А.
Потребляемая мощность	не более 4 Вт
Рабочий диапазон температур	от +5 до +40°С
Относительная влажность при температуре 25°С	до 80%
Габариты	430x159x43,6 мм
Масса	не более 0,2 кг.

2.4 Конструктивное исполнение

Точка доступа RG-35-WZ выполнена в пластиковом корпусе размерами 430x159x43,6 мм.

2.4.1 Передняя панель устройства

Внешний вид передней панели устройства RG-35-WZ приведен на рисунке 2.

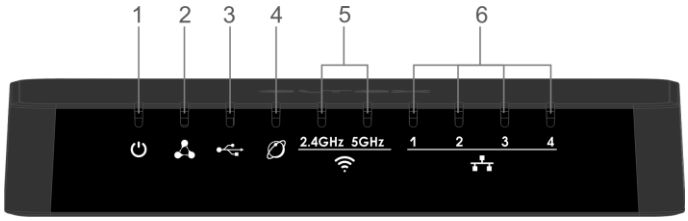


Рисунок 2 – Внешний вид передней панели RG-35-WZ

На верхней панели устройства *RG-35-WZ* расположены следующие световые индикаторы, таблица 2.

Таблица 2 – Описание индикаторов верхней панели

Элемент передней панели		Описание
1		индикатор питания
2		индикатор статуса работы устройства
3		индикатор работы внешнего USB-устройства (USB flash, внешний жесткий диск)
4		индикатор работы WAN-интерфейса
5		индикатор работы беспроводной сети на частоте 2,4 ГГц и 5 ГГц
6		индикаторы работы портов LAN-интерфейса

2.4.2 Задняя панель устройства

Внешний вид задней панели устройства RG-35-WZ приведен на рисунке 3.

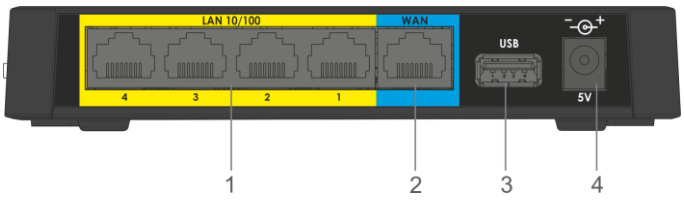


Рисунок 3 – Внешний вид задней панели RG-35-WZ

На задней панели устройства RG-35-WZ расположены следующие разъемы и органы управления, таблица 3.

Таблица 3 – Описание индикаторов и органов управления задней панели RG-35-WZ

Элемент задней панели		Описание
1	LAN 10/100	4 порта 10/100BASE-T Ethernet (разъем RJ-45) для подключения сетевых устройств
2	WAN	порт 10/100/1000BASE-T (разъем RJ-45) для подключения к внешней сети
3	USB	разъем USB для подключения внешнего USB-устройства (USB flash, жесткий диск)
4	5V	разъем для подключения адаптера питания

2.4.3 Боковая панель устройства

Внешний вид боковой панели устройства RG-35-WZ приведен на рисунке 4.

Рисунок 4 – Внешний вид боковой панели RG-35-WZ

На боковой панели устройства RG-35-WZ расположены следующие органы управления:

Таблица 4 – Описание органов управления боковой панели RG-35-WZ

Элемент боковой панели		Описание
1		Кнопка включения/отключения Wi-Fi
2		Кнопка для подключения клиента по протоколу WPS

2.5 Световая индикация

Текущее состояние устройства отображается при помощи индикаторов, расположенных на верхней панели. Перечень состояний индикаторов приведен в Таблица 5.

Таблица 5 – Световая индикация состояния устройства RG-35-WZ

Индикатор		Состояние индикатора	Состояние устройства
	WLAN	зеленый, горит постоянно	сеть Wi-Fi активна в данном диапазоне: 2,4 ГГц и/или 5 ГГц
		зеленый, мигает	процесс передачи данных по беспроводной сети в данном диапазоне: 2,4 ГГц и/или 5 ГГц
	WAN	горит зеленым (10, 100Mbps)/ оранжевым (1000 Mbps)	установлено соединение между станционным терминалом и абонентским устройством
		мигает	процесс пакетной передачи данных по WAN-интерфейсу
	LAN	зеленый, горит	установлено соединение с подключенным сетевым устройством
		мигает	процесс пакетной передачи данных по LAN-интерфейсу
	USB	зеленый, горит	USB-устройство подключено
		не горит	USB-устройство отключено
	Power	зеленый, горит постоянно	включено питание устройства, нормальная работа
	Status	зеленый, мигает	Запущена функция WPS
		не горит	отсутствует доступ в интернет
		зеленый, горит постоянно	нормальная работа

2.6 Перезагрузка устройства и сброс к заводским настройкам

На нижней панели устройства находится функциональная кнопка «F», которая позволяет перезагрузить устройство и сбросить настройки к заводским. Использовать кнопку «F» нужно, когда маршрутизатор включен и готов к работе: индикатор «Power» горит зеленым, индикатор «Status» горит/мигает зеленым или желтым светом.

Для перезагрузки устройства нажмите и сразу отпустите кнопку «F».

Для запуска устройства с заводскими настройками нажмите и удерживайте кнопку «F» более 5-ти секунд, пока индикатор «Status» не начнет мигать красным/зеленым цветом. Произойдет автоматическая перезагрузка устройства. При заводских установках на WAN-интерфейсе запущен DHCP-клиент, адрес интерфейса LAN - *192.168.1.1,* маска подсети – *255.255.255.0*; имя пользователя/пароль для доступа через web-интерфейс: admin/password.

2.7 Управление кнопкой WPS

Устройство поддерживает функцию подключения клиентов к Wi-Fi сети по стандарту WPS. Для настройки подключения выберите на клиентском устройстве способ подключения WPS и на правой боковой панели устройства нажмите и удерживайте в течение 3-х секунд кнопку WPS . После этого клиент подключится к маршрутизатору автоматически.

По умолчанию функция WPS включена. Отключить функцию можно на странице настройки WPS. Ее описание приведено в разделе 0 Подменю «WPS».

2.8 Комплект поставки

В базовый комплект поставки устройства RG-35-WZ входят:

- Абонентский маршрутизатор RG-35-WZ;
- Адаптер питания 220/5В 2,0 А;
- Руководство по установке и настройке.

3 ПОРЯДОК УСТАНОВКИ

3.1 Инструкции по технике безопасности

1. Не устанавливайте устройство рядом с источниками тепла и в помещениях с температурой ниже 5°C или выше 40°C.
2. Не используйте устройство в помещениях с высокой влажностью. Не подвергайте устройство воздействию дыма, пыли, воды, механических колебаний или ударов.
3. Не вскрывайте корпус устройства. Внутри устройства нет элементов, предназначенных для обслуживания пользователем.

Во избежание перегрева компонентов устройства и нарушения его работы запрещается размещать предметы на поверхности оборудования.

3.2 Рекомендации по установке

1. Перед установкой и включением устройства необходимо проверить устройство на наличие видимых механических повреждений. В случае наличия повреждений следует прекратить установку устройства, составить соответствующий акт и обратиться к поставщику.
2. Если устройство находилось длительное время при низкой температуре, перед началом работы следует выдержать его в течение двух часов при комнатной температуре. После длительного пребывания устройства в условиях повышенной влажности перед включением выдержать в нормальных условиях не менее 12 часов.
3. Устройство устанавливается в горизонтальном положении, соблюдая инструкции по технике безопасности.
4. При размещении устройства для обеспечения зоны покрытия сети Wi-Fi с наилучшими характеристиками учитывайте следующие правила:
    a. Устанавливайте устройство в центре беспроводной сети;
    b. Минимизируйте число преград (стены, потолки, мебель и другое) между RG-35-WZ и другими беспроводными сетевыми устройствами;
    c. Не устанавливайте устройство вблизи (порядка 2 м.) электрических, радио устройств;
    d. Не рекомендуется использовать радиотелефоны и другое оборудование, работающее на частоте 2,4 ГГц, 5 ГГц, в радиусе действия беспроводной сети Wi-Fi;
    e. Препятствия в виде стеклянных/металлических конструкций, кирпичных/бетонных стен, а также емкости с водой и зеркала могут значительно уменьшить радиус действия Wi-Fi сети.

3.3 Порядок включения

1. Подключите сетевой Ethernet-кабель, проведённый вашим интернет-провайдером, к разъему WAN RG-35-WZ, рисунок 3.
2. Если RG-35-WZ будет использоваться в качестве домашнего проводного маршрутизатора, то подключите сетевой Ethernet-кабель к разъемам **LAN** RG-35-WZ маршрутизатора и вашего сетевого устройства (компьютер, принтер, телевизионная приставка и другое).
3. Подключите шнур адаптера питания к разъему питания устройства **5V**. Далее подключите адаптер к источнику питания, рисунок 3.
4. После подключения точки доступа к сети питания дождитесь полной загрузки устройства (это может занять около минуты).

4 УПРАВЛЕНИЕ УСТРОЙСТВОМ ЧЕРЕЗ WEB-КОНФИГУРАТОР

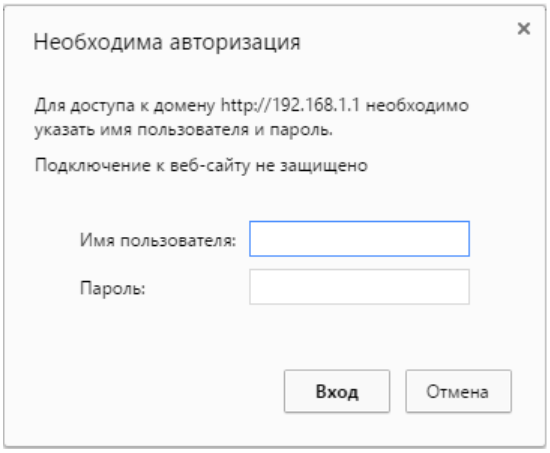
4.1 Начало работы

Для начала работы нужно подключиться к устройству по интерфейсу LAN через Web-браузер:

1. Откройте Web-браузер (программу-просмотрщик гипертекстовых документов), например, Firefox, Opera, Chrome.
2. Введите в адресной строке браузера IP-адрес устройства.

Заводской IP-адрес устройства: 192.168.1.1, маска подсети: 255.255.255.0

При успешном обнаружении устройства в окне браузера отобразится страница с запросом имени пользователя и пароля.



3. Введите имя пользователя в строке «Имя пользователя» и пароль в строке «Пароль».

Заводские установки: имя - *admin*, пароль - *password*.

4. Нажмите кнопку «Войти». В окне браузера откроется страница *«Об устройстве»*.

4.2 Применение конфигурации и отмена изменений

1. Применение конфигурации

По нажатию на кнопку «Сохранить» происходит сохранение конфигурации во flash-память устройства. Чтобы настройки вступили в силу нажмите на кнопку «Сохранить и Применить». Некоторые настройки вступят в силу только после перезагрузки устройства. Система предупредит об этом при нажатии на кнопку.

2. Отмена изменений

Отмена изменений производится только до нажатия на кнопку «Применить». В этом случае изменённые на странице параметры обновятся текущими значениями, записанными в памяти устройства. После нажатия на кнопку «Применить изменения» возврат к предыдущим настройкам будет невозможен.

4.3 Панель управления устройством

Все изменения настроек устройства выполняются при помощи вкладок «*Панели управления*», расположенной на левой стороне Web-интерфейса.

4.3.1 Основные элементы Web-интерфейса

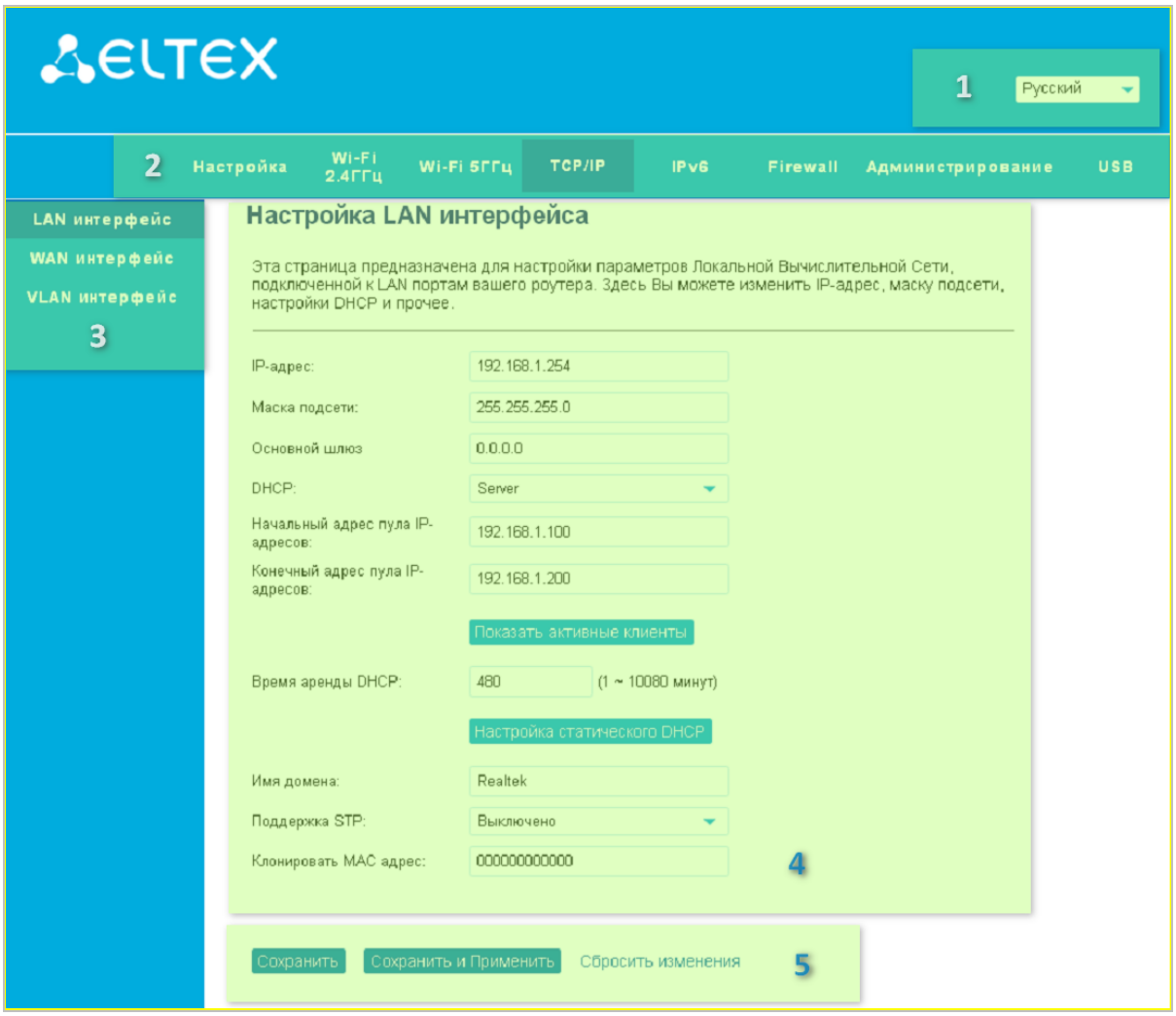


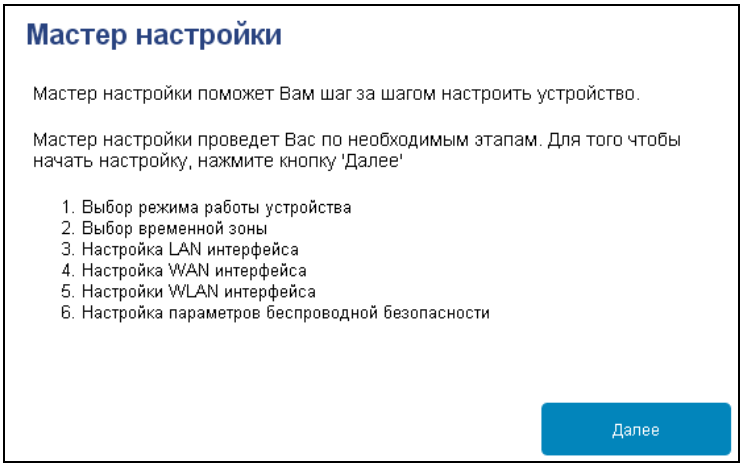
Рисунок 5 - Элементы навигации Web-конфигуратора

1. Кнопка смены языка Web-интерфейса.
2. Верхнее горизонтальное меню вкладок.
3. Левое вертикальное меню вкладок для выполнения настроек.
4. Основное поле настроек устройства, соответствующее выбранной вкладке из поля 3.
5. Кнопки сохранения изменений конфигурации и сброса до последних сохраненных значений.

4.3.2 Меню «Настройка»

В меню Настройка можно выбрать Мастер Настройки для установки основных параметров работы, или выбрать режим работы в соответствующем подменю "Режим работы".

4.3.2.1 Меню «Мастер настройки»



При первом включении устройства воспользуйтесь мастером настройки для выставления основных параметров работы устройства. Мастер позволяет шаг за шагом настроить:

- Режим работы;
- Синхронизацию времени;
- Параметры LAN-интерфейса;
- Параметры WAN-интерфейса (Интернет);
- Параметры Wi-Fi сетей диапазонов 2.4 ГГц и 5 ГГц.

После выполнения всех настроек в мастере устройство будет перезагружено для применения новой конфигурации.

4.3.2.2 Меню «Режим работы»

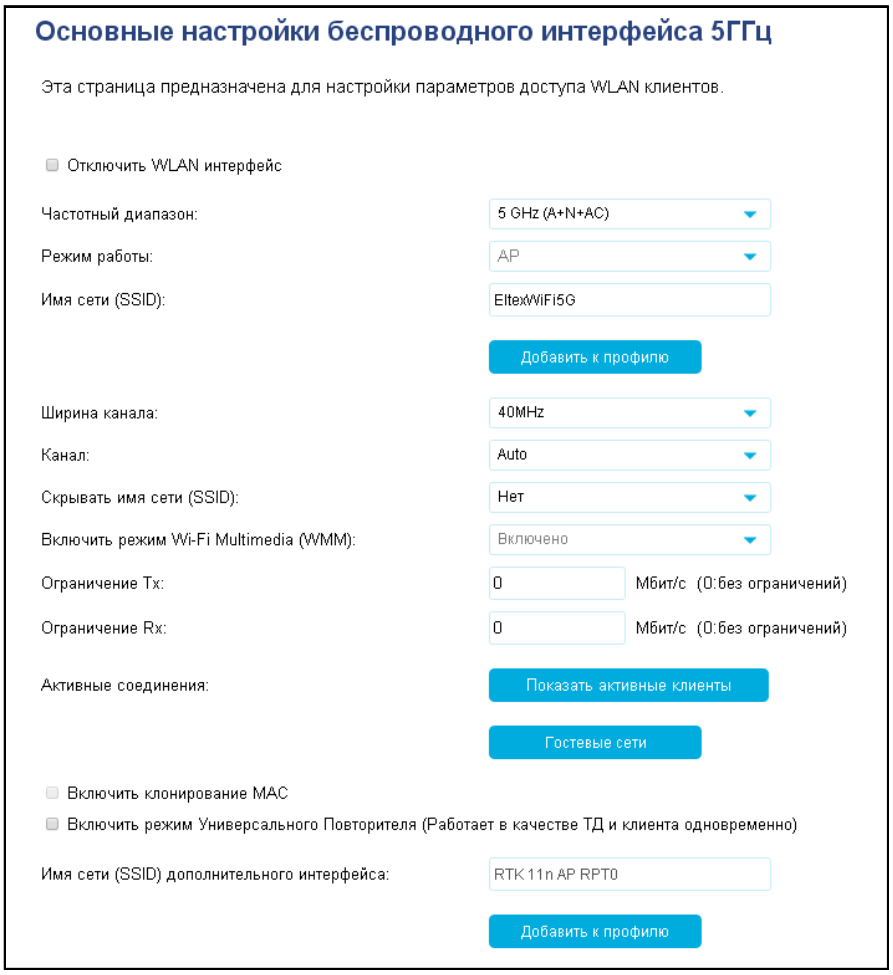
Устройство поддерживает 3 основных режима работы:

- Шлюз – устройство работает как обычный домашний маршрутизатор с включенной функцией NAT (Network Address Translation), все устройства подключенные к LAN сети выходят через один IP адрес, назначенный на WAN порт. Доступны режимы: DHCP клиент, Static IP, PPPoE, PPTP, L2TP.
- Мост – в этом режиме все Ethernet порты и беспроводные интерфейсы работают в одной сети, функция NAT выключена. Настройки WAN порта и Firewall недоступны. Есть возможность задать статические настройки для интерфейса или получение по DHCP.
- Подключение к провайдеру по беспроводной сети (WISP) – в этом режиме один из модулей Wi-Fi (2,4 ГГц или 5 ГГц) переходит в режим клиента, подключается к беспроводной сети провайдера и работает в качестве WAN порта.

4.3.3 Меню «Wi-Fi 2.4 ГГц» и «Wi-Fi 5 ГГц»

В меню «Wi-Fi 2.4 ГГц» и «Wi-Fi 5 ГГц» выполняются настройки беспроводной Wi-Fi сети. Настройки выполняются для сети Wi-Fi на частоте 2.4 ГГц или 5 ГГц. Устройство поддерживает работу одновременно в двух диапазонах частот.

Подменю «Основные настройки»



— *Отключить WLAN интерфейс* – при установленном флаге сеть Wi-Fi для частоты 2.4 ГГц или 5 ГГц выключена.

— *Частотный диапазон* – позволяет выбрать режим работы для беспроводного интерфейса в соответствии с серией стандартов Wi-Fi 802.11.

Для 2.4 ГГц:

- *2.4 GHz (B)* – если все беспроводные клиенты поддерживают стандарт 802.11b, по данному стандарту максимальная скорость составляет 11 Мбит/с;
- *2.4 GHz (G)* – по стандарту 802.11g максимальная скорость составляет 54 Мбит/с;
- *2.4 GHz (N)* – стандарт 802.11n предусматривает максимальную скорость до 300 Мбит/с;
- *2.4 GHz (B+G)* – если в сети присутствуют беспроводные клиенты с поддержкой 802.11b и 802.11g, по стандарту 802.11g максимальная скорость составляет 54 Мбит/с;
- *2.4 GHz (G+N)* – если в сети присутствуют беспроводные клиенты с поддержкой 802.11g и 802.11n, то максимальная скорость составляет 300 Мбит/с;

- *2.4 GHz (B+G+N)* – если в сети присутствуют беспроводные клиенты с поддержкой 802.11b, 802.11g и 802.11n, то максимальная скорость составляет 300 Мбит/с.

Для 5 ГГц:

- *5 GHz (A)* – максимальная скорость составляет 54 Мбит/с;
- *5 GHz (N)* – данный стандарт предусматривает максимальную скорость до 150 Мбит/с;
- *5 GHz (A+N)* – стандарт поддерживает работу устройств с 802.11a и 802.11n;
- *5 GHz (AC)* - данный стандарт предусматривает максимальную скорость до 433 Мбит/с;
- *5 GHz (N+AC)* - стандарт поддерживает работу устройств с 802.11n и 802.11ac;
- *5 GHz (A+N+AC)* - стандарт поддерживает работу устройств с 802.11a, 802.11n и 802.11ac с максимальной скоростью 433 Мбит/с.

— Режим работы – позволяет выбрать в каком режиме будет работать радиомодуль:
  - AP – режим точки доступа;
  - WDS – режим беспроводного моста для соединения нескольких точек доступа, дополнительные настройки содержатся в подменю «Беспроводной мост»;
  - AP+WDS – режим работы одновременно в качестве точки доступа и беспроводного моста;

— *Гостевые сети* – позволяет настроить до 4-х SSID на каждый диапазон с различными настройками безопасности.

— *Имя сети (SSID)* - имя беспроводной сети, используется для подключения к устройству. Максимальная длина имени – 32 символа, ввод с учетом регистра клавиатуры. Данный параметр может состоять из цифр, латинских букв, пробелов, а также символов “-“, “_”, “.”, “!”, “;”, “#”, при этом символы “!”, “;” , “#” и пробел не могут стоять первыми.

— *Ширина канала* - ширина полосы частот канала, на котором работает беспроводная точка доступа, принимает значения 20, 40 МГц на частоте 2,4 ГГц или 20, 40, 80 МГц на частоте 5 ГГц.

— *Канал* - номер канала для работы беспроводной сети. При выборе значения «auto» автоматически определяется канал с меньшим уровнем помех.

— *Скрывать имя сети (SSID)* - при установленном флаге точка доступа будет скрыта в эфире. Подключиться к ней можно заранее зная её SSID.

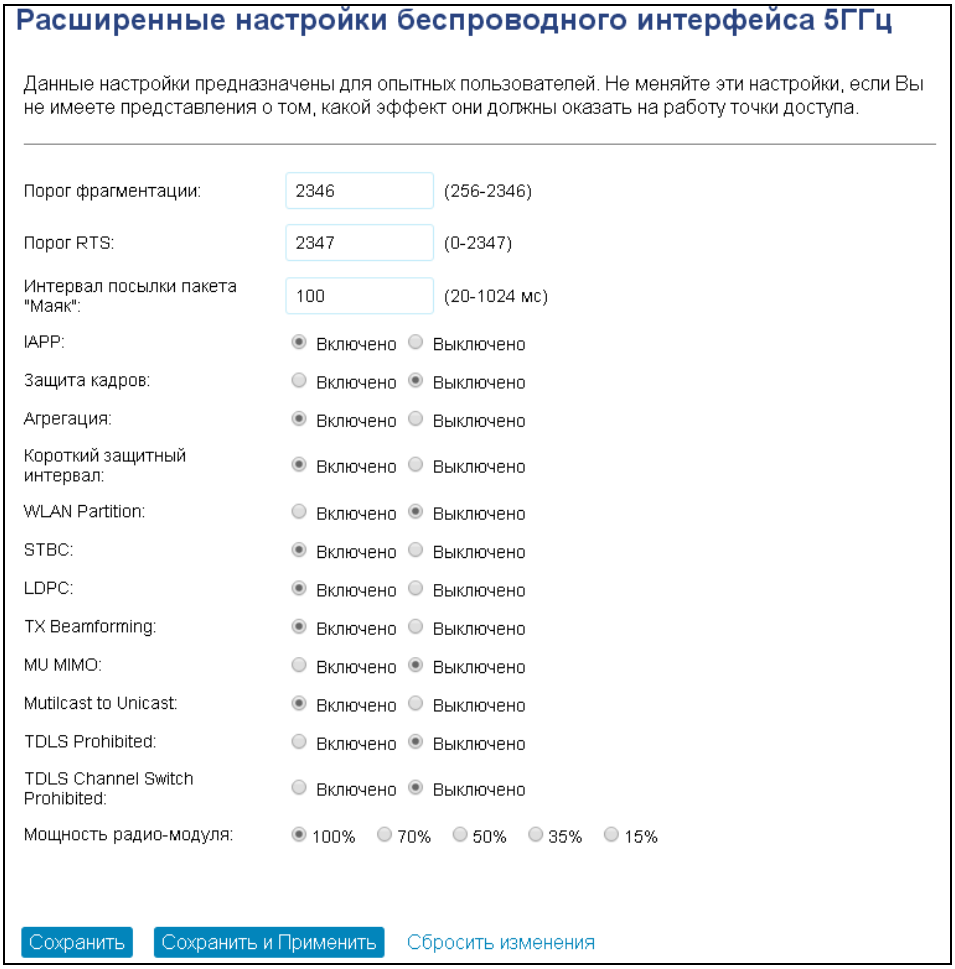
— *Включить режим Wi-Fi Multimedia (WMM)* - при установленном флаге включена функция Wi-Fi Multimedia, которая позволяет оптимизировать передачу мультимедийного трафика по беспроводной среде.

— *Ограничение Tx* – позволяет задать ограничение по передаче трафика Wi-Fi клиентам.

— *Активные соединения* – открывает в новом окне таблицу со списком всех подключенных к Wi-Fi сети клиентов.

— *Максимальное количество клиентов* – позволяет задать количество Wi-Fi устройств, которые одновременно могут быть подключены к точке доступа. Чтобы снять ограничение выставите значение 0.

Подменю «Расширенные»



— *Порог фрагментации (Fragment Threshold)* - максимальный размер непрерывного блока данных для передачи по беспроводной сети. Данные большего размера будут разбиты на части — фрагментированы; принимает значения от 256 до 2346.

— *Порог RTS (RTS Threshold)* - максимальный запрашиваемый размер блока данных для передачи. В технологии CSMA/CA пакеты RTS (request to send) посылаются базовой станции до передачи реальных данных. При наличии свободного окна база отвечает пакетом CTS (clear to send) и клиент отсылает пакет запрошенного размера. Чем меньше размер RTS, тем больше вероятность получить разрешение от базовой станции, тем быстрее восстанавливается сеть после коллизий, но тем меньше производительность сети в целом. Принимает значения от 0 до 2347.

— *Интервал посылки пакета "Маяк" (Beacon Interval)* - промежуток времени между служебными сообщениями (маяками) в беспроводной сети. Служебные сообщения передают параметры частот, протоколов, безопасности, мощности передатчиков, задержек и т. д. Принимает значения от 20 до 1024.

— *Тип преамбулы (Preample Length)* – размер преамбулы показывает длину служебного поля в каждом пакете. Длинная преамбула состоит из 128 бит, короткая – из 56 бит. Короткий размер преамбулы повышает общее быстродействие системы, используется для мультимедийных приложений.

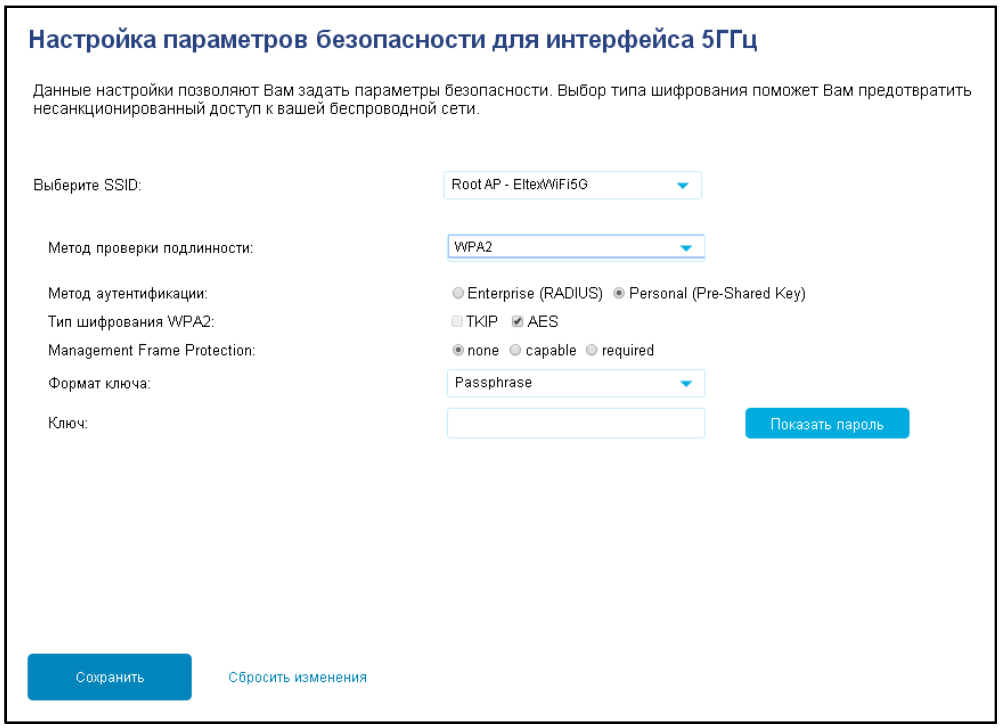
— *IAPP* – протокол IAPP (Inter-Access Point Protocol) позволяет использовать роуминг клиентов между несколькими точками доступа внутри одного сегмента сети.

— *Защита кадров (Protection)* – это специальный механизм для сетей 802.11b/g. Включение механизма гарантирует возможность работы медленных устройств стандарта b в среде с большим количеством высокоскоростных устройств стандарта g. Это достигается

увеличением времени обслуживания старых клиентов, заданием для них меньшего размера окна RTS, снижением общего быстродействия сети.

- *Агрегация (Aggregation)* – включает возможность объединения нескольких маленьких пакетов для передачи в одном большом.
- *Короткий защитный интервал (Short GI)* – средство снижения ошибок при взаимодействии радио устройств — пустой промежуток между передаваемыми шестнадцатеричными символами (0,1,...E,F). Стандартный длинный защитный интервал (Long GI) имеет продолжительность 800нс. Считается, что за это время сигнал полностью доходит до приемника с учетом всех задержек и отражений. По истечении этого интервала, передается следующий символ. Short GI длится 400нс. Использование Short GI повышает общую производительность беспроводной сети примерно на 11%, но иногда ведет к увеличению ошибок приема/передачи.
- *WLAN Partition* – включение запрета взаимодействия беспроводных клиентов между собой.
- *STBC* – включение механизма Space Time Block Coding (STBC), используется в беспроводных сетях для передачи копий потока данных через несколько антенн и для обеспечения приёма разных версий блока данных в целях повышения надежности обмена данными. Известно, что радиосигнал распространяется в среде по достаточно сложным траекториям и подвержен влиянию отражения, рефракции, рассеивания, а также искажается воздействием теплового шума приёмника, что в конечном счете приводит к тому, что одни копии переданного сигнала могут оказаться значительно лучше других (менее искажены). Эта избыточность повышает вероятность корректно декодировать сигнал из нескольких его копий на приёмной стороне. Технология STBC объединяет все копии принятого блока данных оптимальным образом для извлечения максимального количества информации из каждой из них.
- *LDPC* – использование корректирующего кода с малой плотностью проверки на четность Low-density parity-check code (LDPC), который позволяет более эффективно обнаруживать и исправлять возможные ошибки при передаче сигнала через беспроводной интерфейс.
- *TX Beamforming* – технология, подразумевающая формирование электромагнитного поля антенны базовой станции в дальней зоне в виде узконаправленного главного лепестка, ориентированного в сторону абонентского устройства с возможностью изменения направленных свойств при изменении положения этого оборудования.
- *MU MIMO* – позволяет передавать отдельный поток каждому подключенному устройству, что обеспечивает более высокую скорость при подключении одновременно нескольких устройств.
- *Multicast to Unicast* – позволяет передавать беспроводным устройствам Multicast поток в виде Unicast, при условии что включена опция UDP2HTTP в настройках WAN интерфейса.

Подменю «Безопасность»



— *Выберите SSID* – выбор сети, для которой будет выполняться конфигурирование.

— *Метод проверки подлинности* – выбор режима безопасности беспроводной сети:

- *Отключено* – шифрование беспроводной сети отсутствует, низкий уровень безопасности;
- *WEP* – шифрование WEP. WEP-ключ должен состоять из шестнадцатеричных цифр и иметь длину 10 или 26 символов, либо должен быть строкой (символы a-z, A-Z, 0-9, ~!@#$%^&*()_-+=) и иметь длину 5 или 13 символов;
- *WPA2* – шифрование WPA2. Длина ключа составляет от 8 до 63 символов. Разрешается использовать только символы: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>”`’ или пробел. Шифрование WPA2 обладает гораздо большим уровнем защиты по сравнению с WEP;
- *WPA-Mixed* - шифрование WPA и WPA2. Длина ключа составляет от 8 до 63 символов. Разрешается использовать только символы: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>”`’ или пробел.

Рекомендуется использовать режимы безопасности WPA-Mixed и WPA2 как наиболее безопасные.

— *Аутентификация 802.1x* – при установленном флаге точка доступа будет авторизовывать клиентов по 802.1x (WPA/WPA2-Enterprise) с использованием RADIUS-сервера.

— *RADIUS Server IP Address* – адрес RADIUS-сервера.

— *RADIUS Server Port* – номер UDP-порта для обмена данными между устройством и RADIUS-сервером (по умолчанию 1812).

— *RADIUS Server Password* – пароль доступа к RADIUS-серверу.

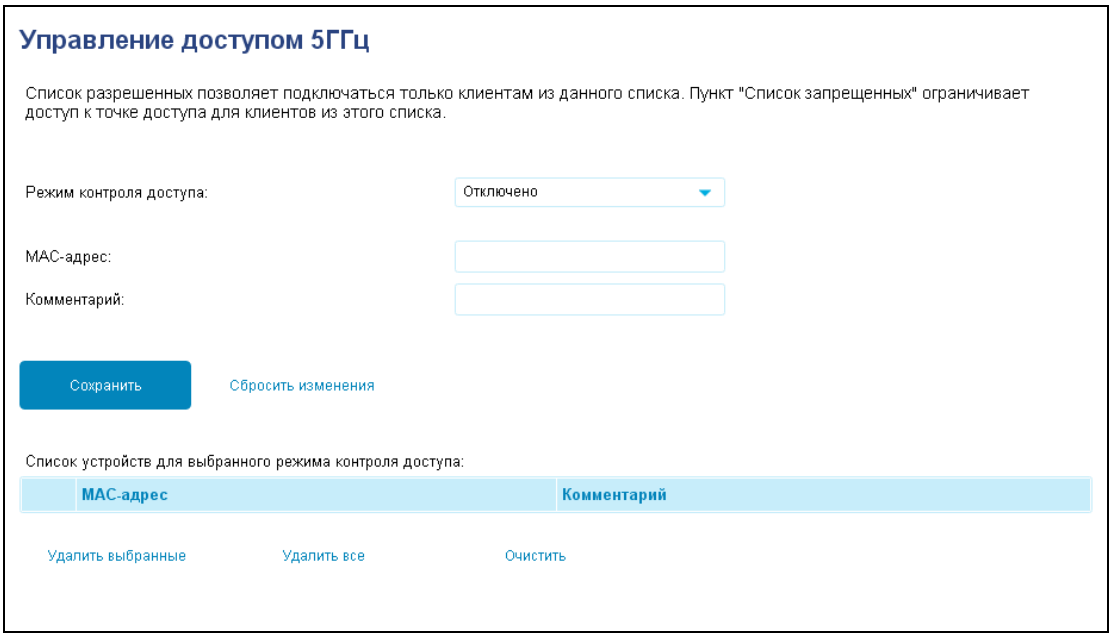
— *Метод аутентификации* – выбор способа аутентификации при подключении устройства. Варианты зависят от выбора метода проверки подлинности:

- *Open System* – аутентификация в режиме открытой системы не требует пароля, обладает низким уровнем защиты;
- *Shared Key* – аутентификация с использованием общего ключа к сети для шифрования WEP;
- *Auto* – автоматический выбор подходящего способа аутентификации;
- *Enterprise (RADUIS Key)* – аутентификация с использованием RADIUS сервера;
- *Personal (Pre-Shared Key)* – аутентификация с использованием общего пароля к сети.

— *Длина ключа* – выбор длины ключа при шифровании WEP: 64-bit или 128-bit.
— *Формат ключа* – выбор формата ключа шифрования: Hex или ASCII для шифрования WEP, а также Passphrase («секретная фраза») или HEX64 (64 символа) для WPA2 и WPA-Mixed.
— *Ключ* – поле для ввода ключа шифрования, по которому будет обеспечиваться доступ к сети.
— *Management Frame Protection* – включение защиты фреймов управления. Варианты: none (отключено), capable (выборочно) и required (обязательно). При выборе варианта capable доступен пункт с включением функции хэрширования по алгоритму SHA256.

Подменю «Управление доступом»

В подменю «Управление доступом» выполняются настройка фильтрации доступа по Wi-Fi и MAC-адресу клиента.



— *Режим контроля доступа* – позволяет задать один из трех режимов работы с беспроводными устройствами:

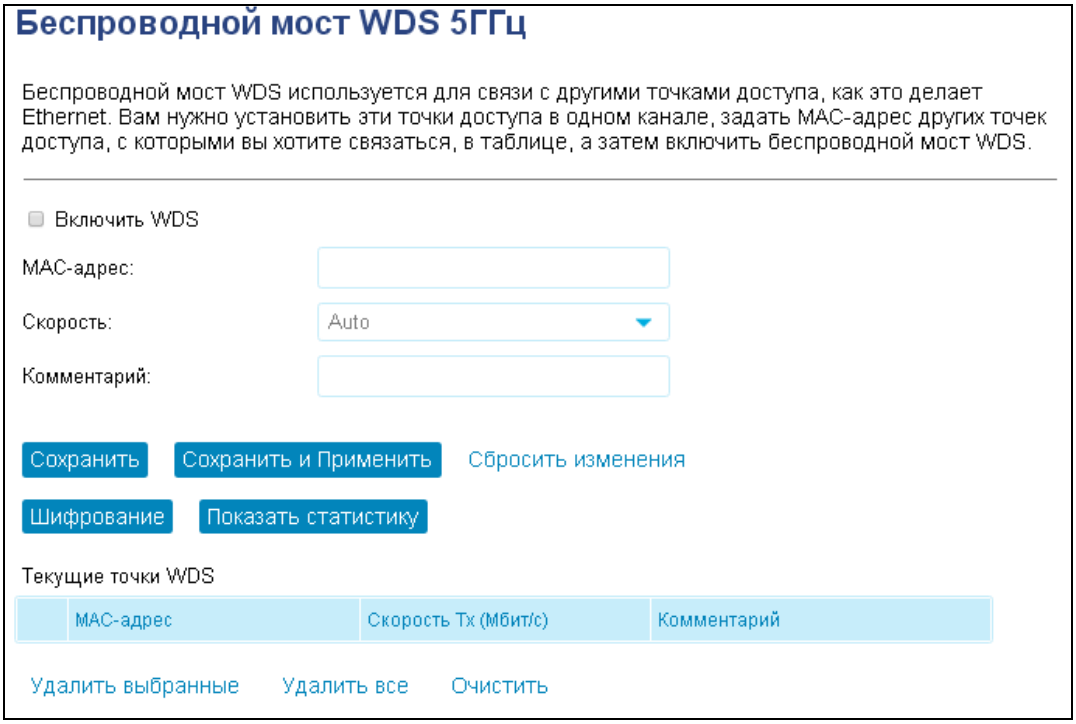
- *Отключено – нет ограничений по подключению устройств;*
- *Белый список – к Wi-Fi сети могут подключиться только устройства с MAC-адресами из списка разрешенных;*
- *Черный список – к Wi-Fi сети могут подключаться все устройства, за исключением перечисленных в списке.*

— *MAC-адрес* – поле для ввода MAC-адреса устройства. Адрес вводится сплошным текстом без разделителей, например a8f94b214fa0.

— *Комментарий* – поле для комментария к данному MAC-адресу. Не обязательно для заполнения. Для удобства рекомендуется записывать название устройства, для которого заводится запись в список.

Подменю «Беспроводной мост»

В подменю "Беспроводной мост" можно установить соединение с другими точками доступа через беспроводной мост WDS, используя их MAC-адреса.



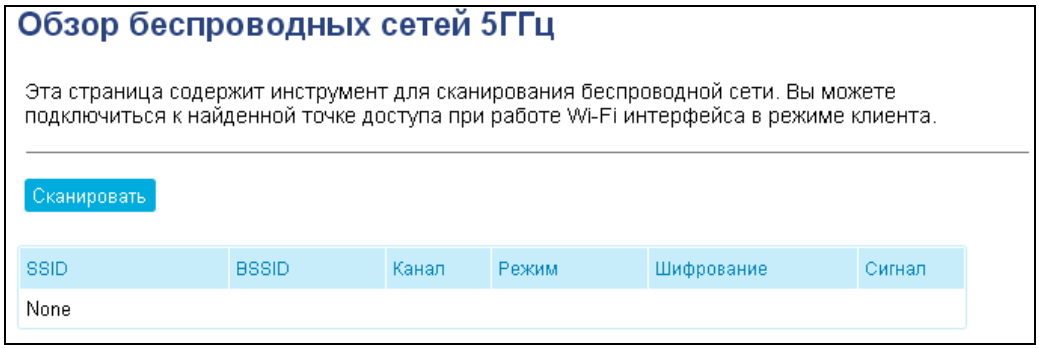
Функция WDS может использоваться отдельно для каждого диапазона частот.

— *MAC-адрес* – поле для ввода MAC-адреса устройства. Адрес вводится сплошным текстом без разделителей, например a8f94b214fa0.

— *Комментарий* – поле для комментария к данному MAC-адресу. Не обязательно для заполнения. Для удобства рекомендуется записывать название устройства, для которого заводится запись в список.

Подменю «Обзор сетей»

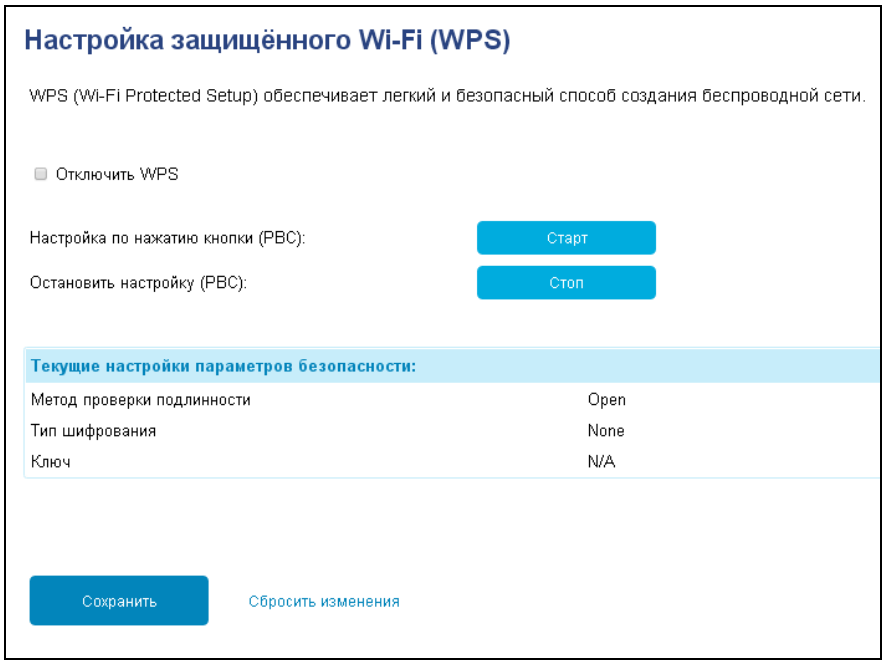
В подменю «Обзор сетей» можно запустить поиск других Wi-Fi сетей в заданном частотном диапазоне с целью определения минимально загруженного канала при тонкой настройке сети. Также через это подменю выполняется подключение к беспроводной сети провайдера в режиме работы WISP.



Подменю «WPS»

В подменю «WPS» выполняется настройка протокола WPS (Wi-Fi Protected Setup).

WPS – стандарт полуавтоматического создания беспроводной сети Wi-Fi. Целью протокола WPS является упрощение процесса настройки беспроводной сети. WPS автоматически обозначает имя сети и задает шифрование для защиты от несанкционированного доступа в сеть, при этом нет необходимости вручную задавать все параметры.



Функция WPS может использоваться отдельно для каждого диапазона частот.

Используя терминологию WPS, устройство может находиться в двух состояниях:

— *Configured* – точка доступа (хотя бы в одном диапазоне частот) сконфигурирована – это значит, что настроены имя сети, параметры шифрования и другие параметры;

— *Unconfigured* – точка доступа в обоих диапазонах частот не сконфигурирована – это значит, что все параметры Wi-Fi имеют настройки по умолчанию.

В зависимости от состояния точки доступа некоторые функции WPS могут быть заблокированы.

— *Отключить WPS* – при выставленном флаге функция WPS будет отключена на выбранном диапазоне;

— *Настройка по нажатию кнопки (PBC)* – выполняет функции кнопки WPS на корпусе устройства. Подключение клиента происходит автоматически после нажатия на данную кнопку. Подключение клиента по кнопке PBC возможно как из состояния «Unconfigured» (точка доступа не сконфигурирована), так и из состояния «Configured» (точка доступа сконфигурирована). При подключении из состояния «Configured» клиент получает настроенные на устройстве имя сети и параметры шифрования. При подключении из состояния «Unconfigured» устройство автоматически генерирует и назначает клиенту имя сети и параметры шифрования. После нажатия на кнопку PBC функция WPS активна в течение двух минут;
— *Остановить настройку (PBC)* – принудительно прекращает процесс создания нового подключения по WPS. Также процесс прекращается автоматически если в течение двух минут не удалось создать соединения.

Подменю «Расписание»

В этом меню задаются интервалы работы беспроводного интерфейса в различные часы и дни недели. При включенной функции беспроводная сеть будет недоступна во время не входящее в расписание. По умолчанию функция расписания выключена.

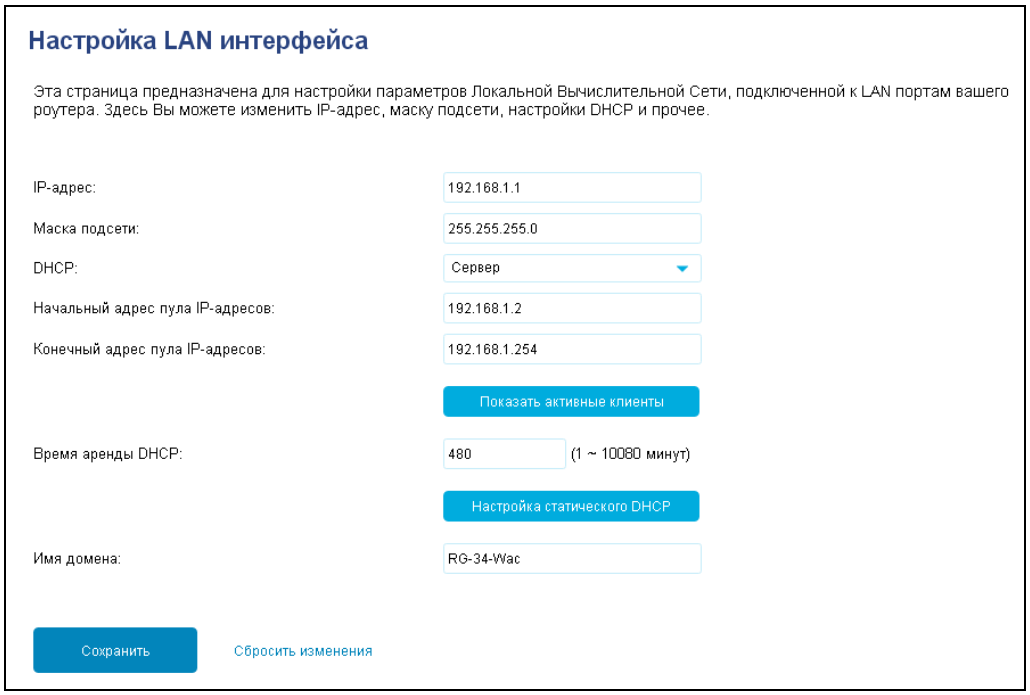
– *Включить работу по расписанию* – при выставленном флаге Wi-Fi сеть в выбранном диапазоне работает в соответствии с указанным расписанием.

4.3.4 Меню «Настройки TCP/IP»

В этом меню доступны для конфигурирования параметры LAN и WAN интерфейсов устройства, а также параметры соединений с использованием VLAN.

Подменю «LAN Интерфейс»

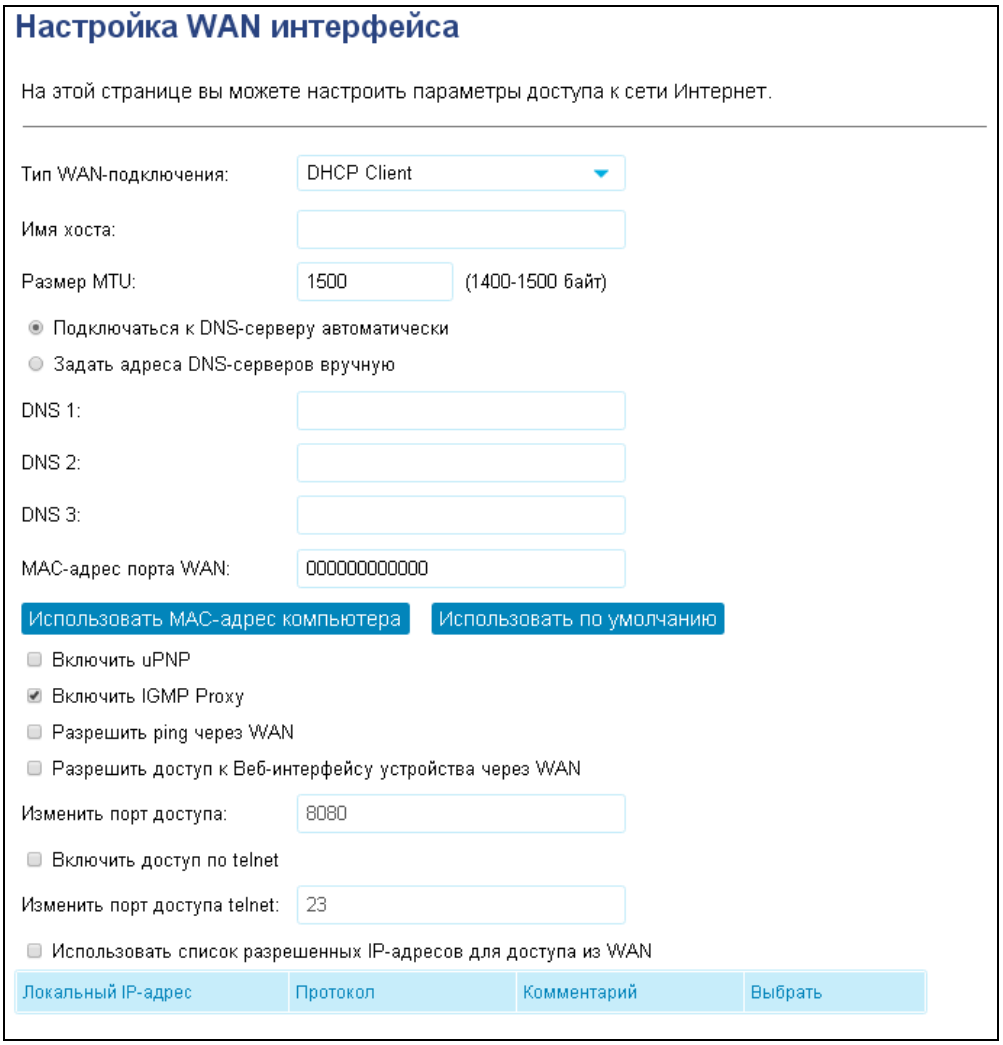
В подменю «LAN Интерфейс» находятся параметры локальных интерфейсов устройства и DHCP-сервера.



- *IP-адрес* – локальный IP-адрес устройства. Для подключенных клиентов это будет адрес основного шлюза. По умолчанию 192.168.1.1.
- *Маска подсети* – значение маски LAN сети. По умолчанию 255.255.255.0.
- *DHCP* – включение или отключение внутреннего DHCP сервера устройства для подключения LAN клиентов по этому протоколу.
- *Начальный адрес пула IP-адресов* – значение начального IP-адреса, начиная с которого будут выдаваться адреса клиентам. Адрес должен попадать в диапазон выбранной сети.
- *Конечный адрес пула IP-адресов* – последний IP-адрес, который устройство может выдать клиенту. По его достижению пул считается исчерпанным до момента освобождения уже занятого адреса. Адрес должен попадать в диапазон выбранной сети.
- *Показать активные клиенты* – отобразить список подключенных к устройству клиентов.
- *Статический DHCP* – позволяет задать статические IP-адреса подключенным клиентам.
- *Время аренды DHCP* – время аренды в минутах по истечению которого клиент должен либо освободить адрес, либо продлить на такой же промежуток.
- *Имя домена* – имя домена DHCP-сервера.

Подменю «WAN Интерфейс»

В подменю «WAN Интерфейс» выполняется настройка подключения к внешней сети через порт WAN и изменение параметров взаимодействия клиентов LAN сети и WAN порта.



— *Тип WAN-подключения* – выбор протокола, по которому будет осуществляться подключение WAN-интерфейса устройства к сети предоставления услуг провайдера:

• *Static IP* – режим работы, при котором IP-адрес и все необходимые параметры на WAN-интерфейс назначаются статически. При выборе типа «Static IP» для редактирования станут доступны следующие параметры:

– *IP-адрес* – установка IP-адреса WAN-интерфейса устройства в сети провайдера;
– *Маска подсети* – маска внешней подсети;
– *Основной шлюз* – адрес, на который отправляется пакет, если для него не найден маршрут в таблице маршрутизации.

• *DHCP Client* – режим работы, при котором IP-адрес, маска подсети, адрес DNS-сервера, шлюз по умолчанию и другие параметры, необходимые для работы в сети, будут получены от DHCP-сервера автоматически.

• *PPPoE* – режим работы, при котором на WAN-интерфейсе поднимается PPPoE-сессия. При выборе «PPPoE» для редактирования станут доступны следующие параметры:

– *Имя пользователя* – имя пользователя для авторизации на PPPoE-сервере;
– *Пароль* – пароль для авторизации;

- *Service Name* – имя услуги – значение тэга Service Name в сообщении PADI (поле не обязательно для заполнения);
- *Тип подключения* – позволяет выбрать тип подключения PPPoE: постоянное, по требованию, вручную.

• *PPTP* – режим, при котором выход в Интернет осуществляется через специальный канал, туннель, используя протокол PPTP. При выборе «PPTP» для редактирования станут доступны следующие параметры:

- *Способ сетевого подключения* – динамический IP (DHCP) или статический IP. В первом случае параметры сети (IP-адрес, маска и шлюз) будут получены автоматически. Во втором – потребуется ввести их вручную;
- *Способ подключения к серверу PPTP* – выбор способа между: по доменному имени или по IP-адресу;
- *Доменное имя* – адрес сервера будет определяться по его доменному имени. Пункт активен только при выборе способа подключения по доменному имени;
- *IP-адрес сервера* – при статическом доступе с этого адреса осуществляется доступ до PPTP-сервера;
- *Имя пользователя* – имя пользователя для авторизации на PPTP-сервере;
- *Пароль* – пароль для авторизации на PPTP-сервере;
- *Тип подключения* – позволяет выбрать тип подключения PPTP: постоянное, по требованию, вручную.

• *L2TP* – режим, при котором выход в Интернет осуществляется через специальный канал, туннель, используя протокол L2TP. При выборе «L2TP» для редактирования станут доступны следующие параметры:

- *Способ сетевого подключения* – динамический IP (DHCP) или статический IP. В первом случае параметры сети (IP-адрес, маска и шлюз) будут получены автоматически. Во втором – потребуется ввести их вручную;
- *Способ подключения к серверу L2TP* – выбор способа между: по доменному имени или по IP-адресу;
- *Доменное имя* – адрес сервера будет определяться по его доменному имени. Пункт активен только при выборе способа подключения по доменному имени;
- *IP-адрес сервера* – при статическом доступе с этого адреса осуществляется доступ до L2TP-сервера;
- *Имя пользователя* – имя пользователя для авторизации на L2TP-сервере;
- *Пароль* – пароль для авторизации на L2TP-сервере;
- *Тип подключения* – позволяет выбрать тип подключения L2TP: постоянное, по требованию, вручную.

— *Имя хоста* – сетевое имя устройства.

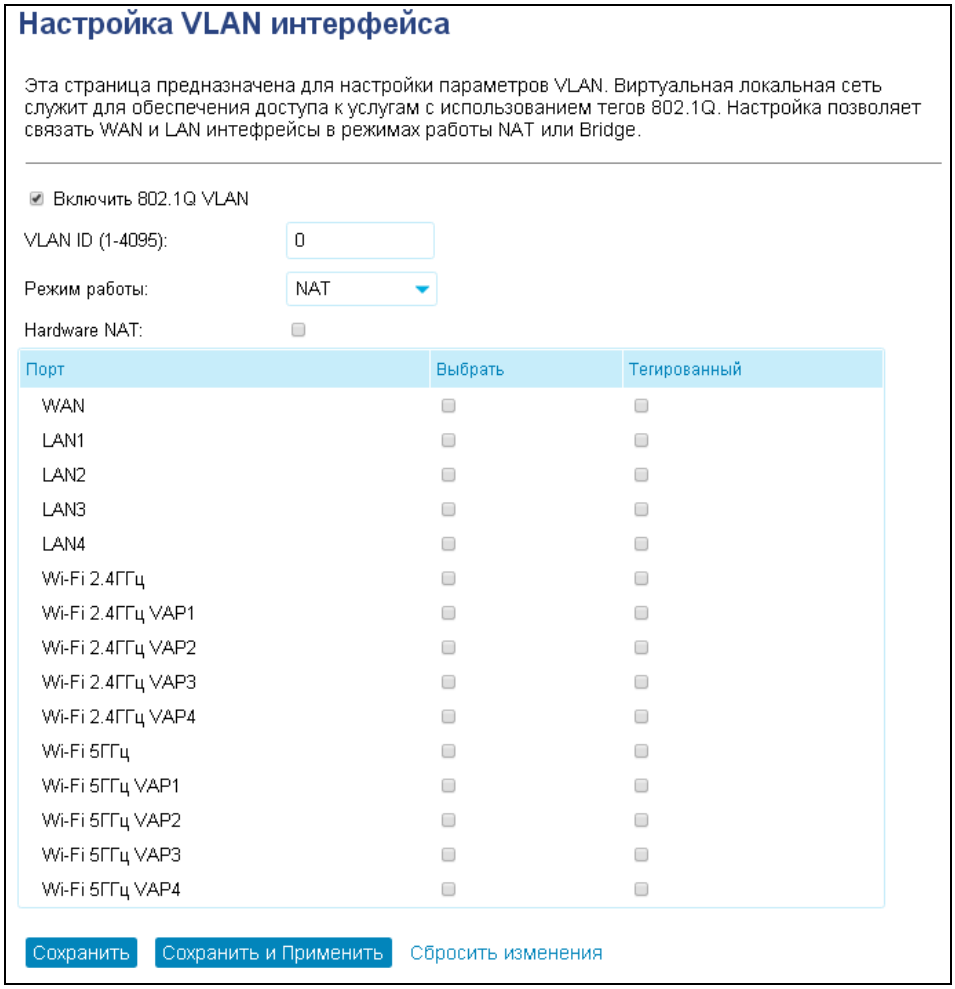
— *Размер MTU* – определяет размер кадров Ethernet передаваемых через WAN-порт.
— *Настройка DNS* – адреса используемых DNS-серверов можно как получить автоматически по DHCP, так и указать вручную.
— *MAC-адрес порта WAN* – позволяет изменить MAC-адрес WAN-порта с заводского на сторонний, если со стороны провайдера реализована проверка MAC-адресов абонентских устройств.
— *Включить uPNP* – протокол UPnP используется некоторыми приложениями (например, DC-клиентами, такими как FlylinkDC++) для автоматического создания правил проброса TCP/UDP-портов, используемыми этими приложениями, на вышестоящем маршрутизаторе. Рекомендуется включить UPnP для обеспечения работы сервисов обмена файлами в сети.
— *Включить IGMP Proxy* – при выставленном флаге устройство обрабатывает запросы IGMP, которые необходимы для работы IPTV.
— *Разрешить ping через WAN* – при выставленном флаге устройство будет отвечать на приходящие из WAN запросы ICMP.

- *Разрешить доступ к Web-интерфейсу устройства через WAN* – открывает доступ к web-интерфейсу устройства из WAN сети.
- *Изменить порт доступа* — изменение порта доступа к web-интерфейсу из WAN и LAN сети. По умолчанию используется порт 80.
- *Включить доступ по telnet* – открывает доступ до устройства по соединению telnet.
- *Изменить порт доступа telnet* – позволяет менять порт для соединения по telnet.
- *Использовать список разрешенных IP*-адресов для доступа из WAN – содержит список IP-адресов, которым разрешено подключаться к web-интерфейсу и telnet из WAN-сети.
- *Включить NAT Passthrough для разрешения пакетам (VPN) проходить через роутер к сетевым клиентам* – эта функция используется при настройки VPN подключения типа IPSec, PPTP, L2TP и IPv6.

Протоколы PPTP и L2TP используются для создания защищенного канала связи через Internet между компьютером удаленного пользователя и частной сетью его организации. PPTP и L2TP основываются на протоколе Point-to-Point Protocol over Ethernet (PPPoE) и являются его расширениями. Данные верхних уровней модели OSI сначала инкапсулируются в PPP, а затем в PPTP или L2TP для туннельной передачи через сети общего доступа. Функциональные возможности PPTP и L2TP различны. L2TP может использоваться не только в IP-сетях, служебные сообщения для создания туннеля и пересылки по нему данных используют одинаковый формат и протоколы. PPTP может применяться только в IP-сетях, и ему необходимо отдельное соединение TCP для создания и использования туннеля.

Подменю «VLAN Интерфейс»

Подменю "VLAN интерфейс" позволяет связывать порты в режиме NAT или Bridge и объединять их во VLAN с использованием тегов стандарта 802.1Q.



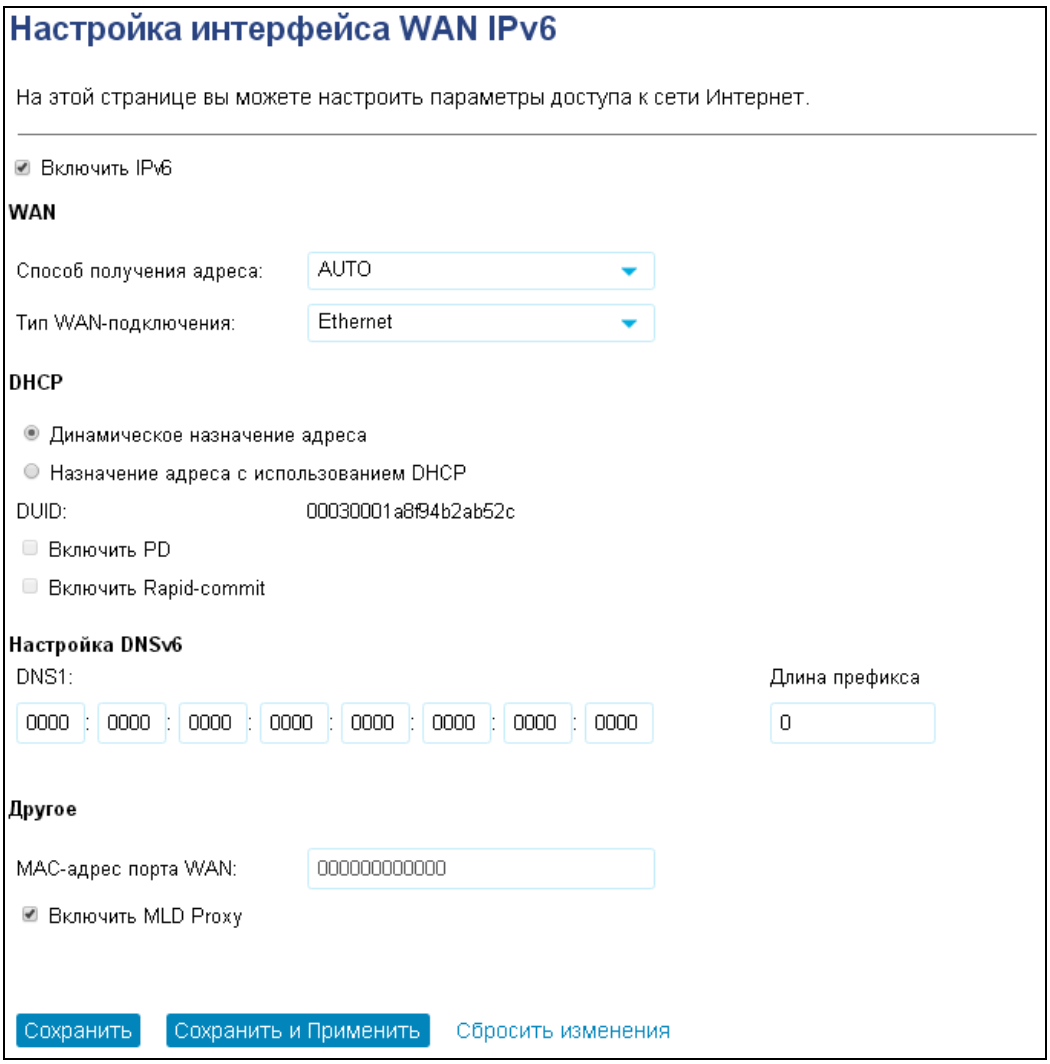
- *VLAN ID* – позволяет выбрать номер VLAN, который будет использоваться на выбранных портах.
- *Режим работы* NAT – позволяет всем портам установленной VLAN получать доступ к сети с одного адреса.
- *Режим работы Bridge* – связывает друг с другом порты одной VLAN. Трафик через порты передается с тегом 802.1Q или без него в зависимости от выставленного параметра.
- *Hardware NAT* – включение аппаратного NAT.

4.3.5 Меню «IPv6»

Позволяет настроить параметры WAN и LAN интерфейсов при использовании IPv6

Подменю «IPv6 WAN интерфейс»

В подменю «IPv6» выполняется конфигурирование подключения к внешней сети и локальной сети по протоколу IPv6.



При выборе режима «Static» будут доступны следующие настройки:

- *Внешний IPv6-адрес устройства* – статический IPv6-адрес устройства, с которым будет осуществляться доступ к сети Интернет.

- *Длина префикса* – аналог маски подсети в IPv4. Определяет какая часть адреса определяет подсеть, а какая - хост. Максимальное значение длины префикса – 128.
- *Основной шлюз* – IPv6-адрес шлюза, используемого по умолчанию.
- *Настройка DNSv6* – IPv6-адрес DNS-сервера.

При выборе режима «AUTO» будут доступны следующие настройки:

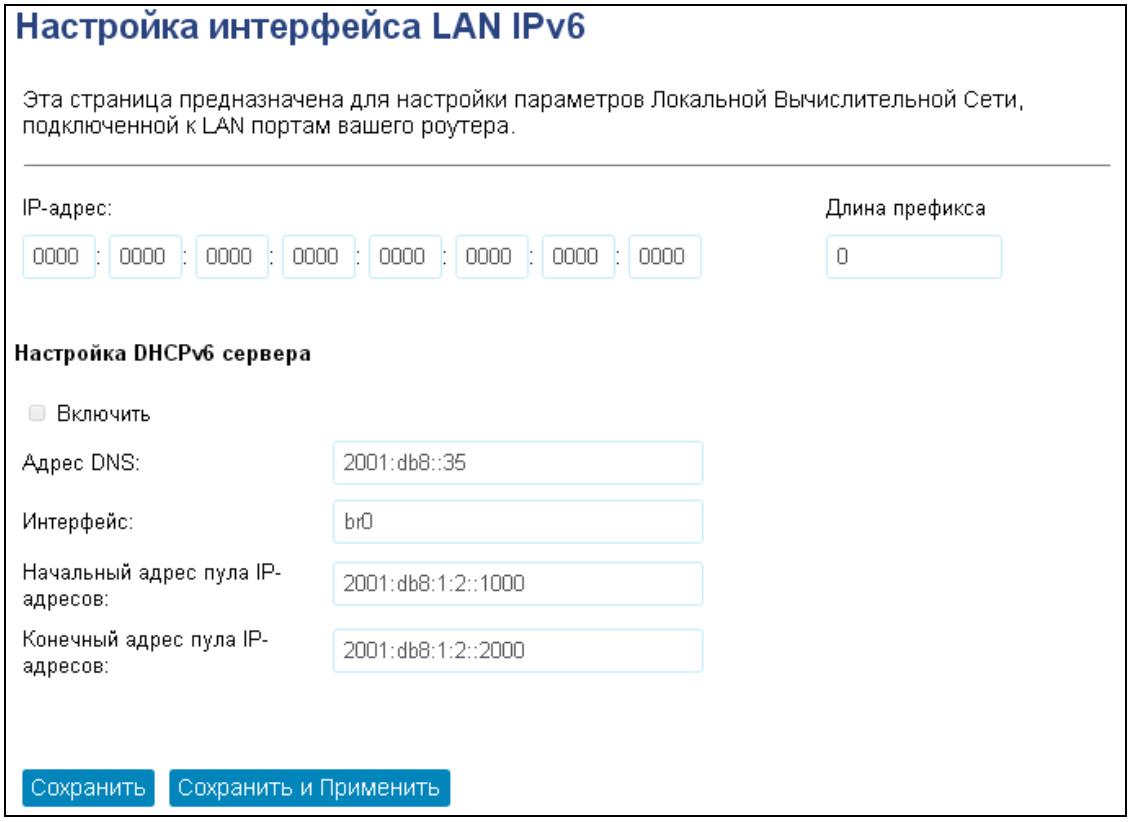
- *Получить адреса DNS-серверов автоматически* – способ получения адреса DNS-серверов: автоматически или ввести самостоятельно как при выбранном режиме «Static».
- *Включить PD* – позволяет автоматически получить IPv6 префикс.
- *Включить Rapid-commit* – режим, позволяющий получить адрес в ходе обмена 2 сообщениями, а не 4 как при обычном подключении.

При выборе типа WAN-подключения «PPPoE» настройки аналогичны режиму «AUTO». Также нужно указать параметры PPPoE-соединения:

- *Имя пользователя* – имя пользователя на сервере PPPoE.
- *Пароль* – установленный пароль.
- *Service Name* – опционально, указывается название запрашиваемого сервиса.
- *AC Name* – MAC-адрес концентратора доступа (если известен).

Подменю «IPv6 LAN интерфейс»

Позволяет настроить параметры IPv6 для локальной сети.

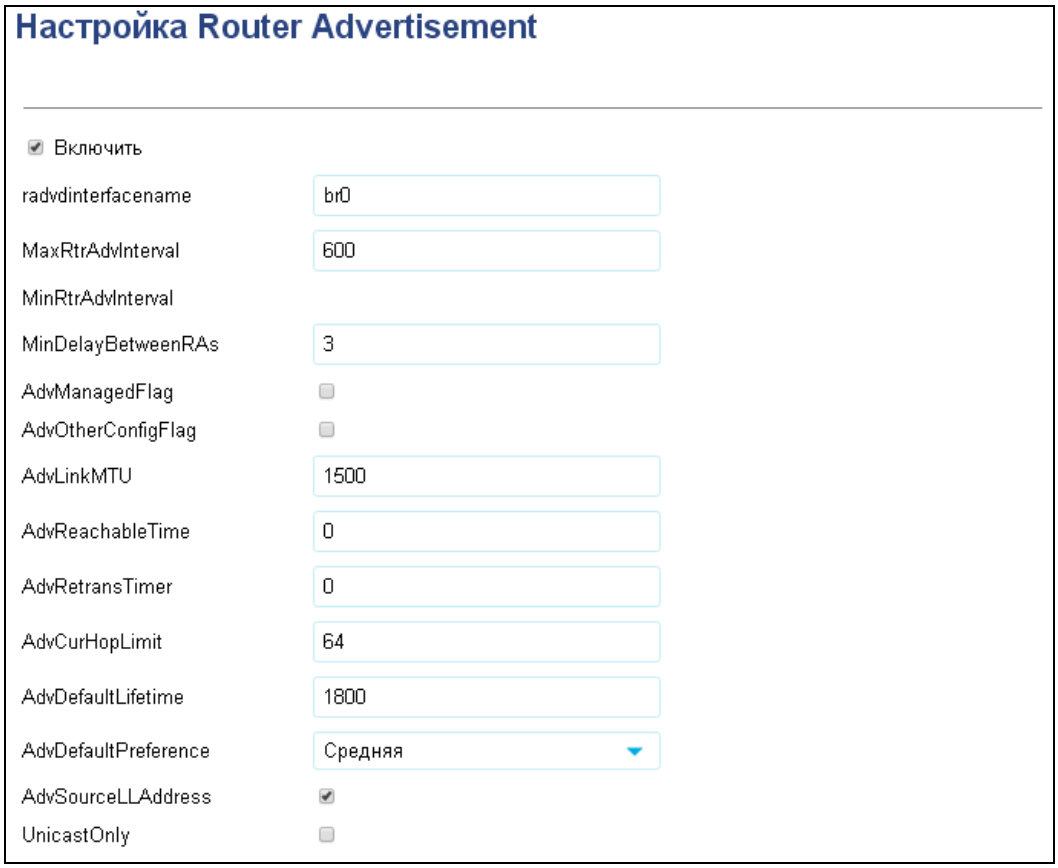


- *IPv6-адрес устройства* – статический IPv6-адрес устройства, который будет присвоен LAN интерфейсу.

- *Длина префикса* – аналог маски подсети в IPv4. Определяет какая часть адреса определяет подсеть, а какая - хост. Максимальное значение длины префикса – 128.
- *Включить DHCPv6 сервер* - позволит динамически получить параметры для интерфейса.
- *Адрес DNS* – IPv6 адрес DNS сервера.
- *Интерфейс* – название интерфейса, для которого производится настройка.
- *Начальный адрес пула IP-адресов* – значение начального IP-адреса, начиная с которого будут выдаваться адреса клиентам. Адрес должен попадать в диапазон выбранной сети.
- *Конечный адрес пула IP-адресов* – последний IP-адрес, который устройство может выдать клиенту. По его достижению пул считается исчерпанным до момента освобождения уже занятого адреса. Адрес должен попадать в диапазон выбранной сети.

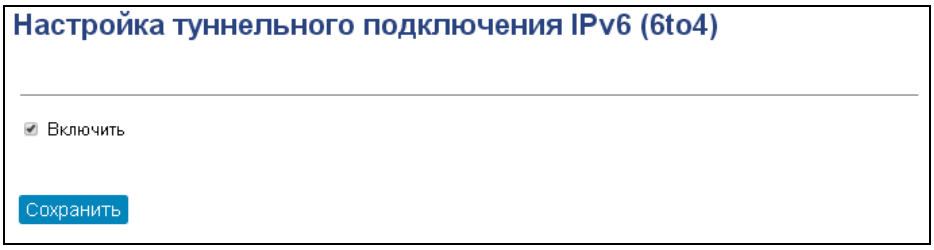
Подменю «Radvd»

Подменю "Radvd" позволяет настроить параметры рассылки сообщений Router Advertisement для выполнения автоматической настройки в режиме SLAAC.



Подменю «Tunnel (6to4)»

Позволяет создать IPv6/48 подсеть с одним IPv4 адресом.

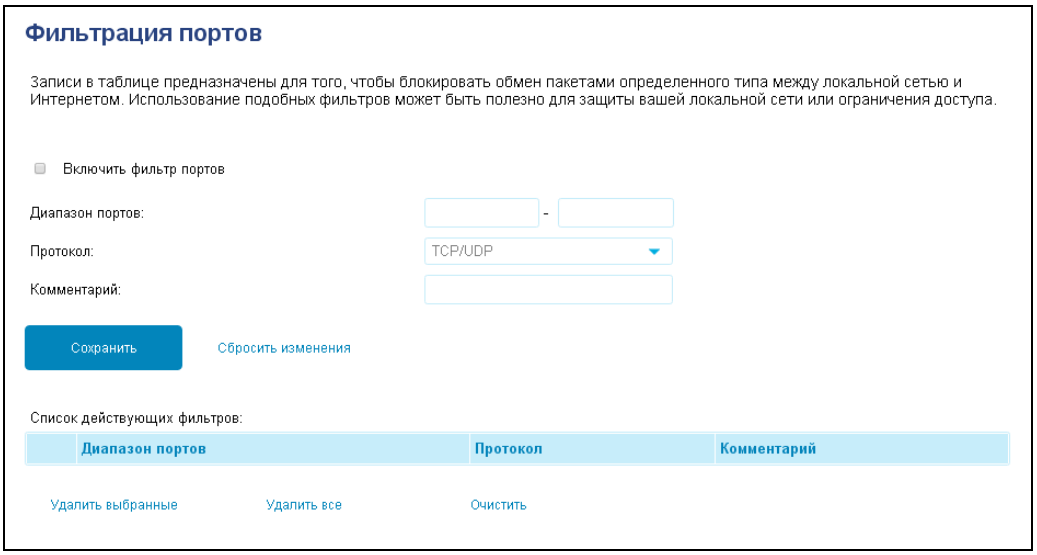


4.3.6 Меню «Firewall»

В этом меню доступны функции, позволяющие управлять доступом между LAN и WAN интерфейсами.

Подменю «Фильтрация портов»

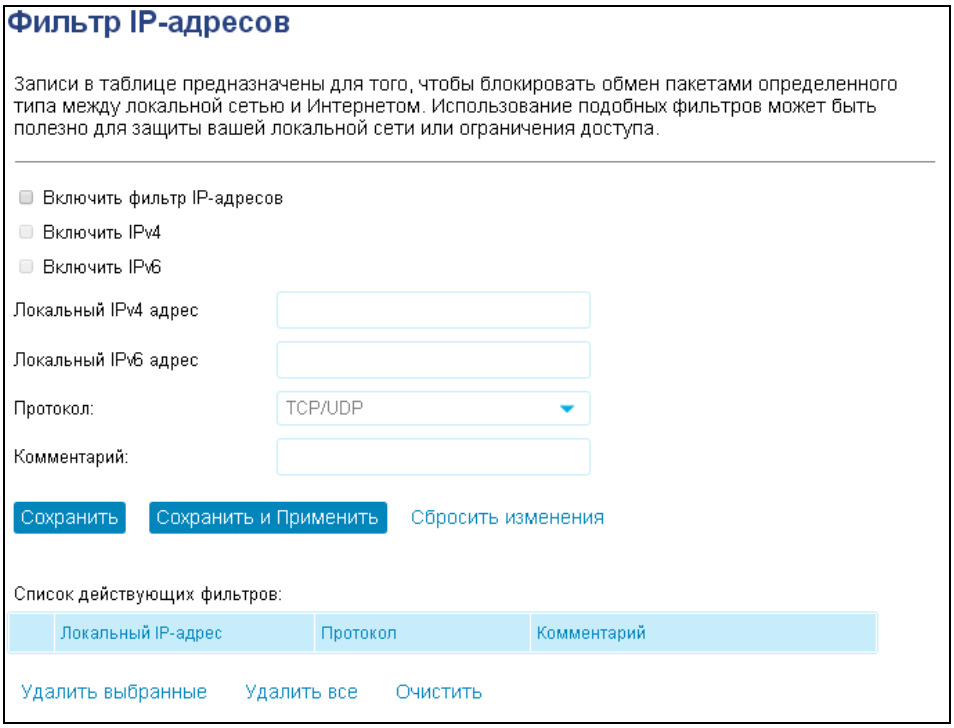
Фильтрация портов позволяет запретить трафик между LAN и WAN на заданных диапазонах портов. Использование фильтра может быть полезно для защиты LAN-сети или ограничения доступа.



- *Включить фильтр портов* – при выставленном флаге фильтр включен. При включении можно выбрать тип списка:
  - Чёрный список – доступ через порты, внесенные в список, будет запрещен.
  - *Белый список* – доступ будет разрешен только через порты, внесенные в список, и запрещен по всем остальным.
- *Включить IPv4* – фильтрация осуществляется по правилам с использованием адресов IPv4.
- *Включить IPv6* - фильтрация осуществляется по правилам с использованием адресов IPv6.
- *Диапазон портов* – вводятся номера портов, трафик с которых Вы хотите запретить.
- *Протокол* – выбор типа протокола трафика TCP, UDP или оба.
- *Комментарий* – поле для оставления заметок для фильтров.

Подменю «Фильтрация IP»

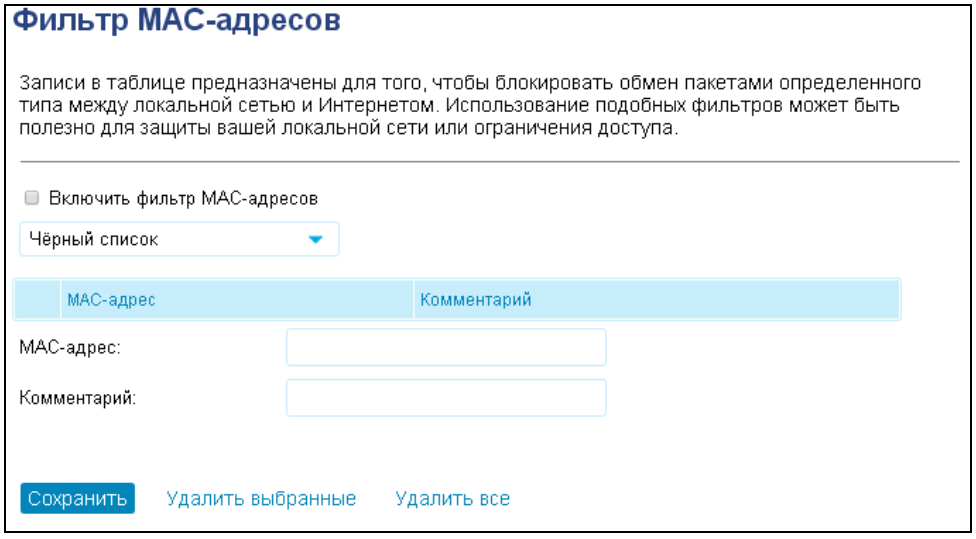
Функция «Фильтрация IP» позволяет ограничить доступ для определенных устройств в WAN-сеть (Интернет), при этом ресурсы внутри LAN-сети остаются доступны.



- *Включить фильтр IP-адресов* – при выставленном флаге фильтр включен.
- *Включить IPv4* – фильтрация осуществляется с использованием адресов IPv4.
- *Включить IPv6* – фильтрация осуществляется с использованием адресов IPv6.
- *Локальный IP-адрес* – вводятся IP-адрес устройства, которому нужно ограничить доступ.
- *Протокол* – выбор типа протокола трафика TCP, UDP или оба.
- *Комментарий* – поле для оставления заметок для фильтров.

Подменю «Фильтрация MAC»

В подменю «Фильтрация MAC» выполняются настройка фильтрации доступа по MAC-адресу клиента, подключенного в один из LAN-портов.



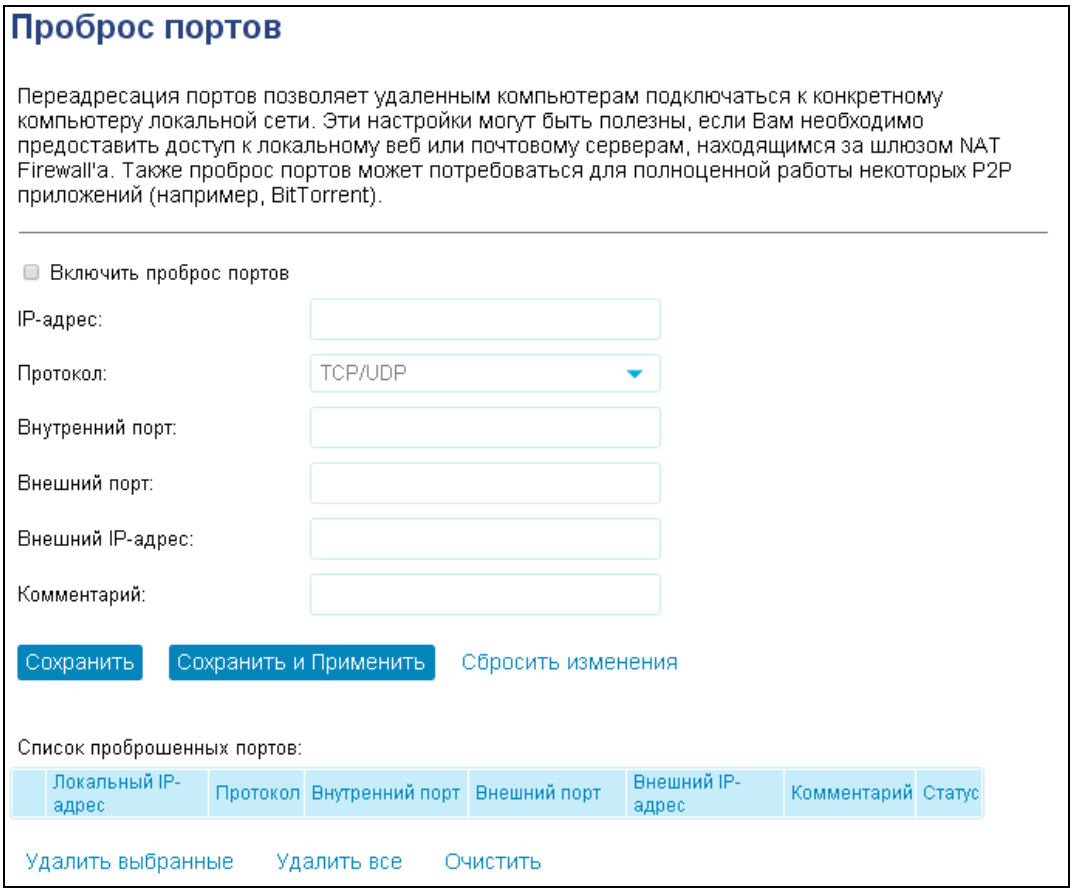
— *Включить фильтр MAC-адресов* – при выставленном флаге фильтр включен. При включении нужно выбрать тип фильтра:

  - Чёрный список – доступ будет запрещен устройствам с MAC-адресами, внесенными в список;
  - Белый список – доступ будет разрешен только устройствам, внесенным в список, и запрещен всем остальным.

— *MAC-адрес* – вводится MAC-адрес устройства, которому нужно ограничить доступ.
— *Протокол* – выбор типа протокола трафика TCP, UDP или оба.
— *Комментарий* – поле для оставления заметок для фильтров.

Подменю «Проброс портов»

Проброс сетевых портов необходим, когда TCP/UDP-соединение с локальным (подключенным к LAN-интерфейсу) компьютером устанавливается из внешней сети. Данное меню настроек позволяет задать правила, разрешающие прохождение пакетов из внешней сети на указанный адрес в локальной сети, тем самым делая возможным установление соединения. Проброс портов главным образом необходим при использовании *torrent*- и *p2p*-сервисов. Для этого в настройках *torrent*- или *p2p*-клиента нужно посмотреть используемые им TCP/UDP-порты и задать для этих портов соответствующие правила проброса на IP-адрес Вашего компьютера.

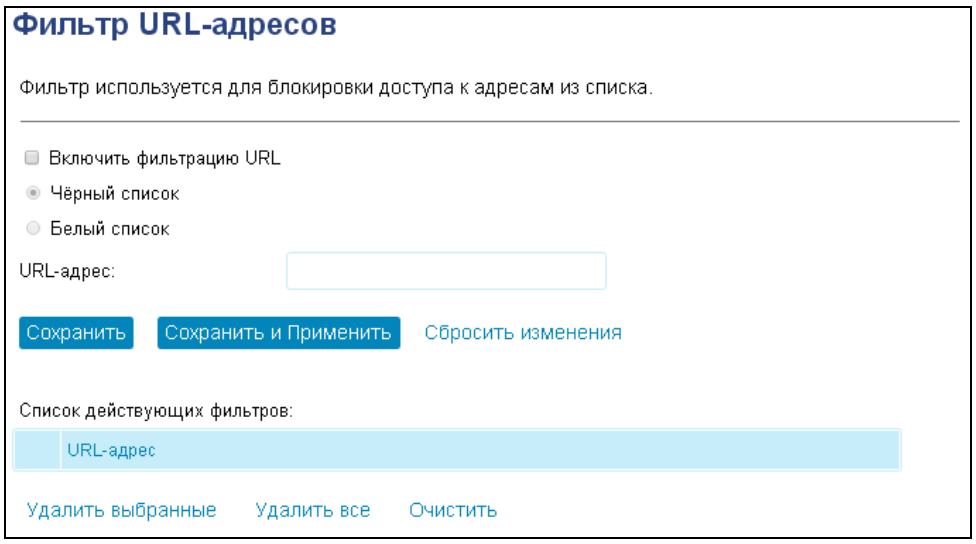


— *Включить проброс портов* – при выставленном флаге проброс портов выполняется.
— *IP-адрес* – вводится IP-адрес устройства LAN-сети, которое будет получать трафик.
— *Протокол* – выбор типа протокола трафика TCP, UDP или оба.
— *Внутренний порт* – указывается пробрасываемый порт со стороны LAN.
— *Внешний порт* — порт со стороны WAN интерфейса, может совпадать или отличаться от номера порта со стороны LAN.

— *Внешний IP*-адрес – вводится IP-адрес устройства в сети WAN, для которого будет действовать правило проброса.
— *Комментарий* – поле для оставления заметок для фильтров.

Подменю «Фильтрация URL»

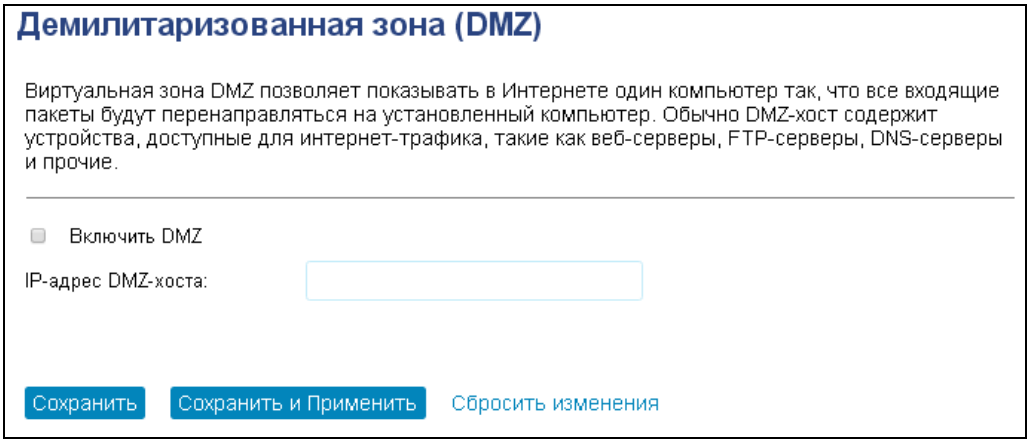
Фильтр URL позволяет ограничить доступ к ресурсам в Интернете по их доменным адресам (URL).



— *Включить фильтрацию URL* – при выставленном флаге фильтр включен. При включении укажите тип фильтра:
  - *Чёрный список* – доступ будет запрещен на сайты, адреса которых внесены в список;
  - *Белый список* – доступ будет разрешен по адресам, внесенным в список, и запрещен по всем остальным.
— *URL-адрес* – вводятся URL-адрес ресурса, доступ к которому вы хотите заблокировать.

Подменю «DMZ»

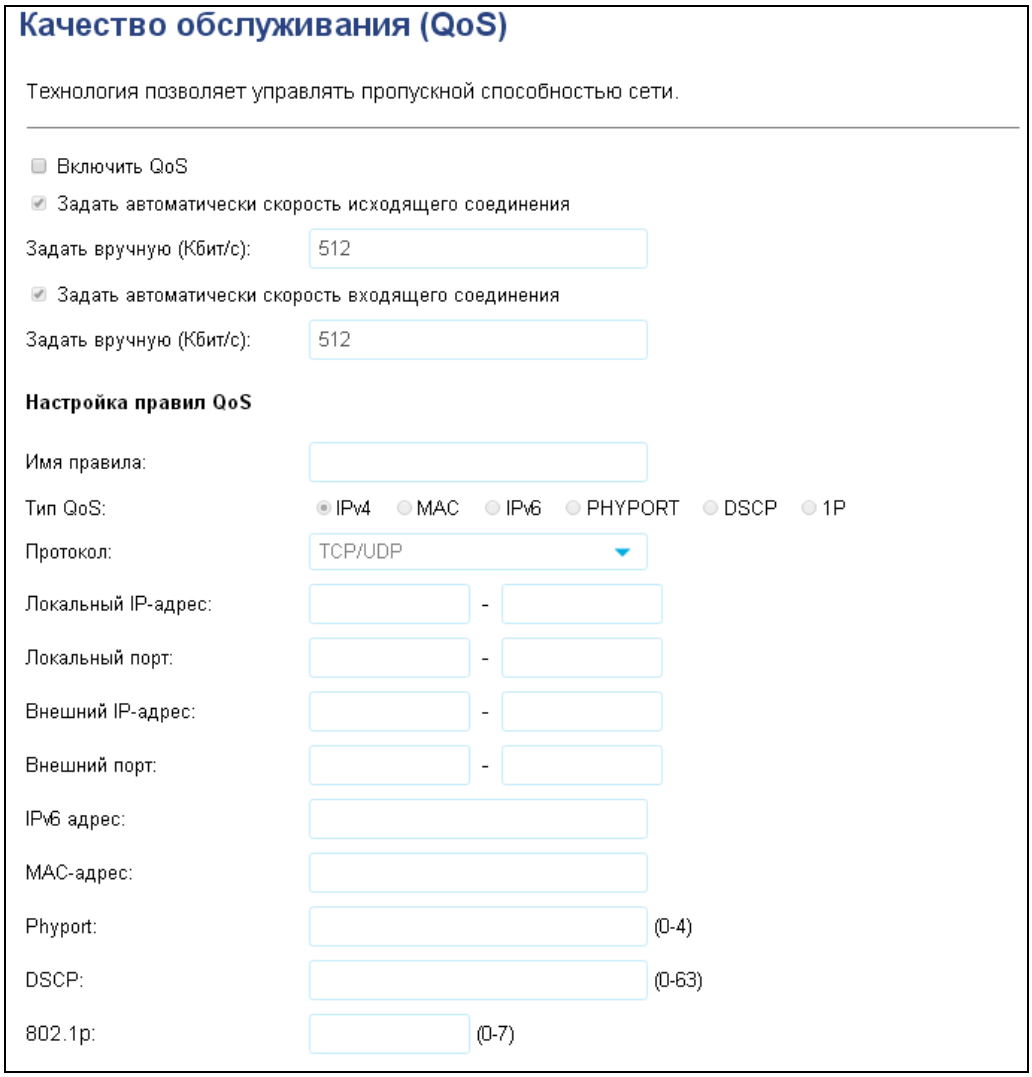
Демилитаризованная зона (DMZ) позволяет выделить одного клиента в LAN таким образом, чтобы все входящие пакеты перенаправлялись на него. Обычно DMZ-хост содержит сервисы типа web-сервер, FTP-сервер, DNS-сервер и прочие.



— *Включить DMZ* – при выставленном флаге DMZ включен;
— *IP-адрес DMZ-хоста* – вводится IP-адрес клиента в LAN-сети, которого нужно переместить в зону DMZ.

4.3.7 Меню «Quality of Service (QoS)»

Технология обеспечения качества обслуживания (QoS) позволяет распределять пропускную способность между всеми клиентами, подключенными как к проводным LAN-портам, так и по Wi-Fi.



— *Включить QoS* – при выставленном флаге функция QoS включена;

— *Скорость исходящего/входящего соединения* –позволяет задать скорость соединения для каждого клиента автоматически или выставить вручную.

Настройка правил QoS

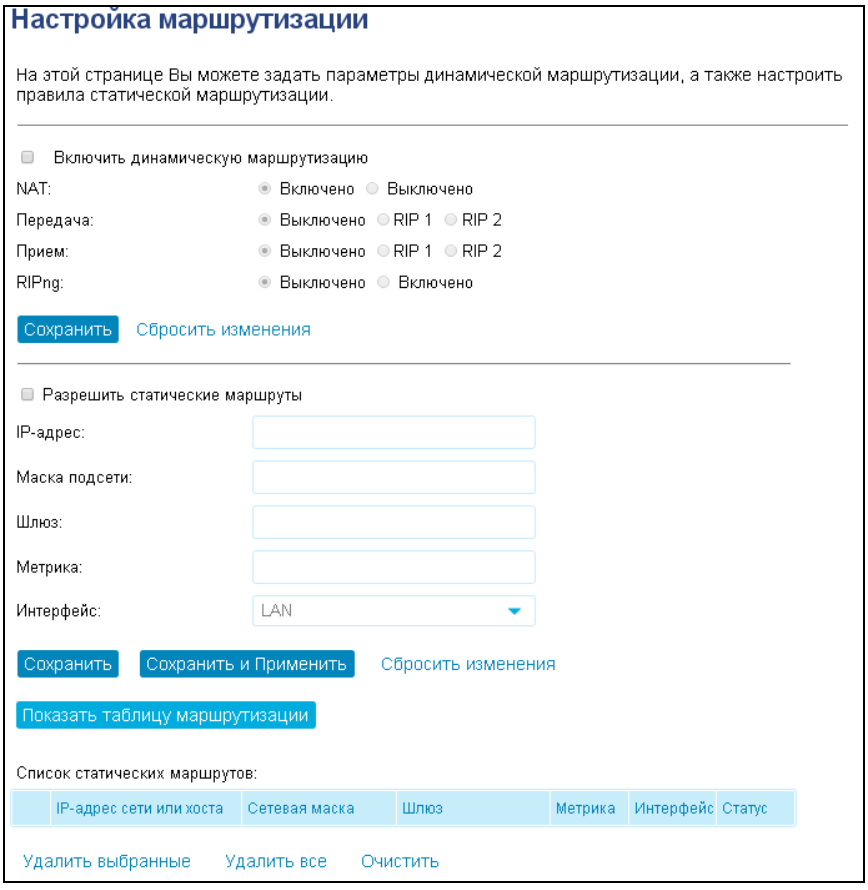
— *Тип QoS* – выберите тип параметра, для которого задается правило;

— *Протокол* – задается протокол, для которого будет работать правило;
— *Локальный IP-адрес* – задается при выбранном типе адреса IP клиента;
— *Локальный порт* – задается порт TCP/UDP со стороны LAN, для которого будет выполняться правило;
— *Внешний IP-адрес* – задается IP-адрес устройства со стороны WAN для данного правила;
— *Внешний порт* – задается порт TCP/UDP со стороны WAN;
— *IPv6 адрес* – задается адрес IPv6 для правила QoS;
— *MAC-адрес* – задается MAC-адрес клиента;
— *Phyport* – задается адрес физического интерфейса Ethernet;
— *DSCP* – задается метка заголовка QoS, по которой будет выполняться правило;

- 802.1p – задается метка приоритета для правила;
- *Режим* – позволяет выбрать между двух вариантов:
  - Гарантировать минимальную скорость;
  - Ограничивать максимальную скорость.
- *Скорость входящего/исходящего соединения* – введите требуемое значение в зависимости от выбранного режима;
- *Тип приоритета* – позволяет задать используемый тип PRIO или WRR;
- *Смена метки DSCP* – задается замена метки в заголовке QoS при прохождении LAN-WAN и наоборот;
- *Смена метки 802.1p* – задается замена метки приоритета в заголовке при прохождении LAN-WAN и наоборот;
- *Комментарий* – позволяет оставить заметку о текущем правиле QoS.

4.3.8 Меню «Настройка маршрутизации»

В меню «Настройка маршрутизации» устанавливаются динамические и статические маршруты устройства.



Динамическая маршрутизация

- *Включить динамическую маршрутизацию* – при выставленном флаге работает функция динамической маршрутизации;
- *NAT* – использовать при динамической маршрутизации;
- *Прием/Передача* – выбор используемого протокола динамической маршрутизации RIP1 или RIP2 для соответствующего направления;
- *RIPng* – при выставленном флаге включается протокол динамической маршрутизации для сети IPv6.

Статическая маршрутизация

- *Включить статические маршруты* – при выставленном флаге статические маршруты будут добавлены в таблицу маршрутизации;
- *IP-адрес* – адрес сети назначения или хоста, до которой указывается маршрут;
- *Маска подсети* – сетевая маска. Для хоста маска подсети устанавливается в значение 255.255.255.255, для подсети – в зависимости от её размера;
- *Шлюз* – IP-адрес шлюза, через который осуществляется выход на «IP-адрес»;
- *Метрика* – «стоимость» маршрута;
- *Интерфейс* – тип выходного интерфейса устройства (LAN или WAN) через который доступна целевая сеть;
- *Показать таблицу маршрутизации* – открывает в новом окне текущую таблицу маршрутизации устройства.

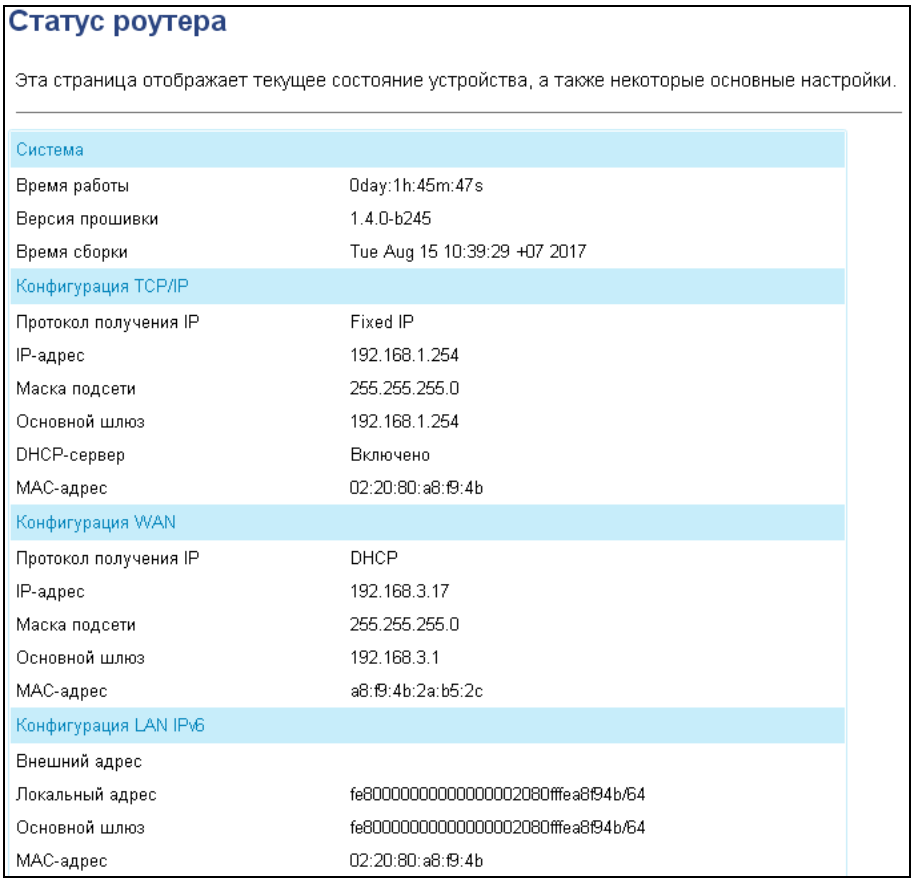
4.3.9 Меню «Администрирование»

В этом меню находится информация об устройстве, его состоянии, а также параметры конфигурации и обновления ПО.

Подменю «Статус»

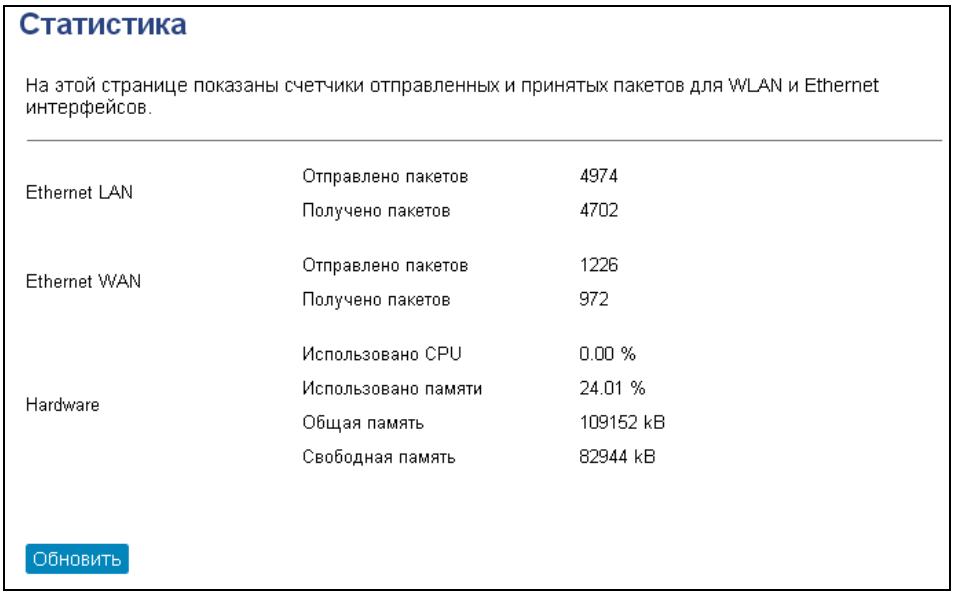
В этом подменю отображается информация об устройстве и основные настройки, такие как:

- Системные параметры (время и версия прошивки);
- Параметры беспроводных интерфейсов;
- Настройки LAN-сети;
- Настройки WAN-порта.



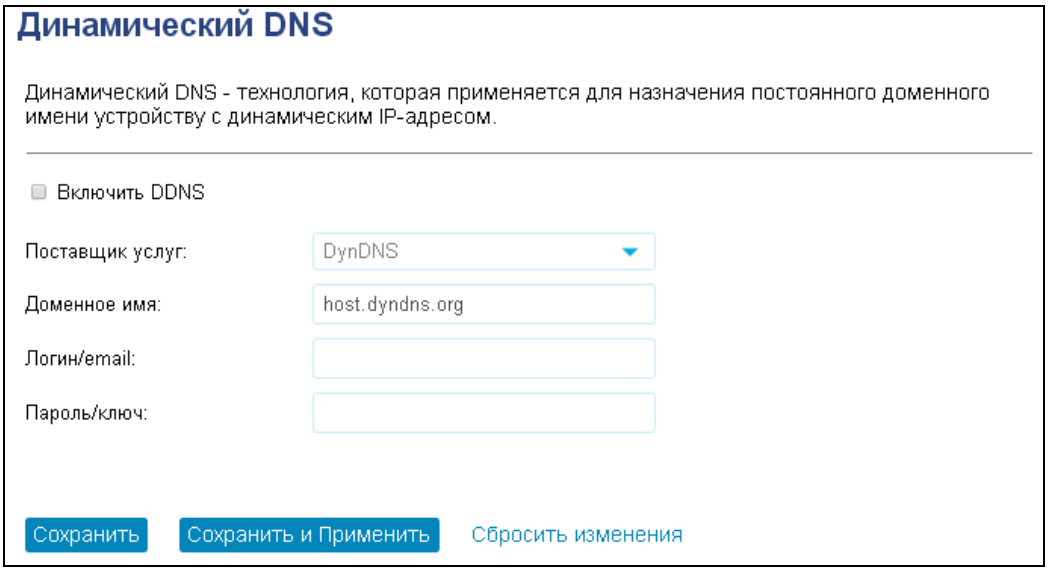
Подменю «Статистика»

В этом подменю находятся данные о переданных и принятых пакетах по каждому интерфейсу, а также информация о состоянии устройства: загрузке ЦПУ и памяти.



Подменю «DDNS»

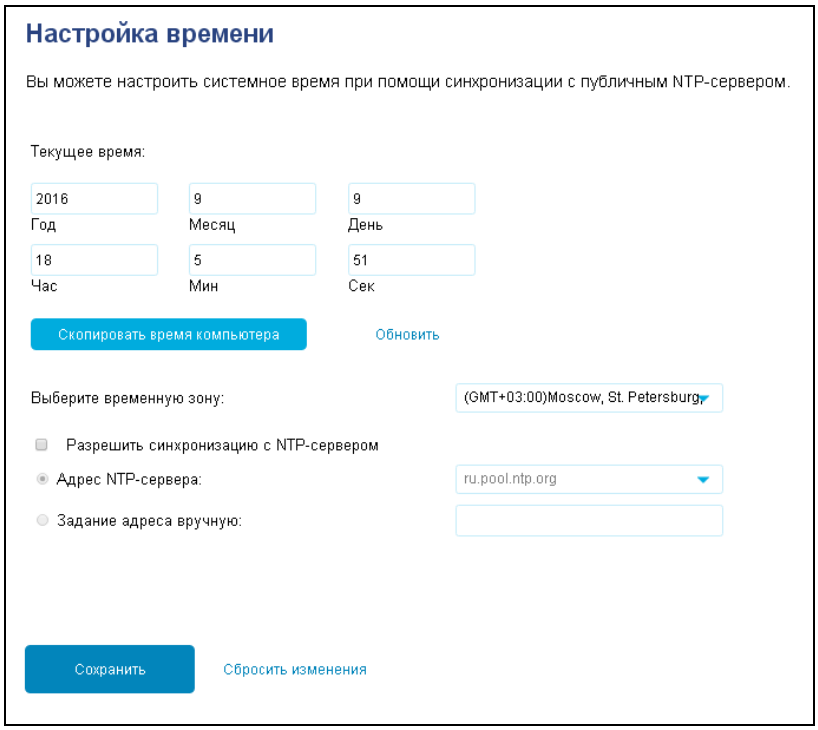
В этом подменю можно активировать услугу предоставления постоянного доменного имени устройству с динамическим IP-адресом.



- *Поставщик услуг* – выбор поставщика услуги DDNS;
- *Доменное имя* – здесь указывается доменное имя поставщика услуг;
- *Логин/email* – здесь указывается логин пользователя на сайте поставщика услуги;
- *Пароль/ключ* – здесь указывается пароль;

Подменю «Настройка даты и времени»

В этом подменю настраивается дата и системное время устройства при помощи синхронизации с NTP-сервером.

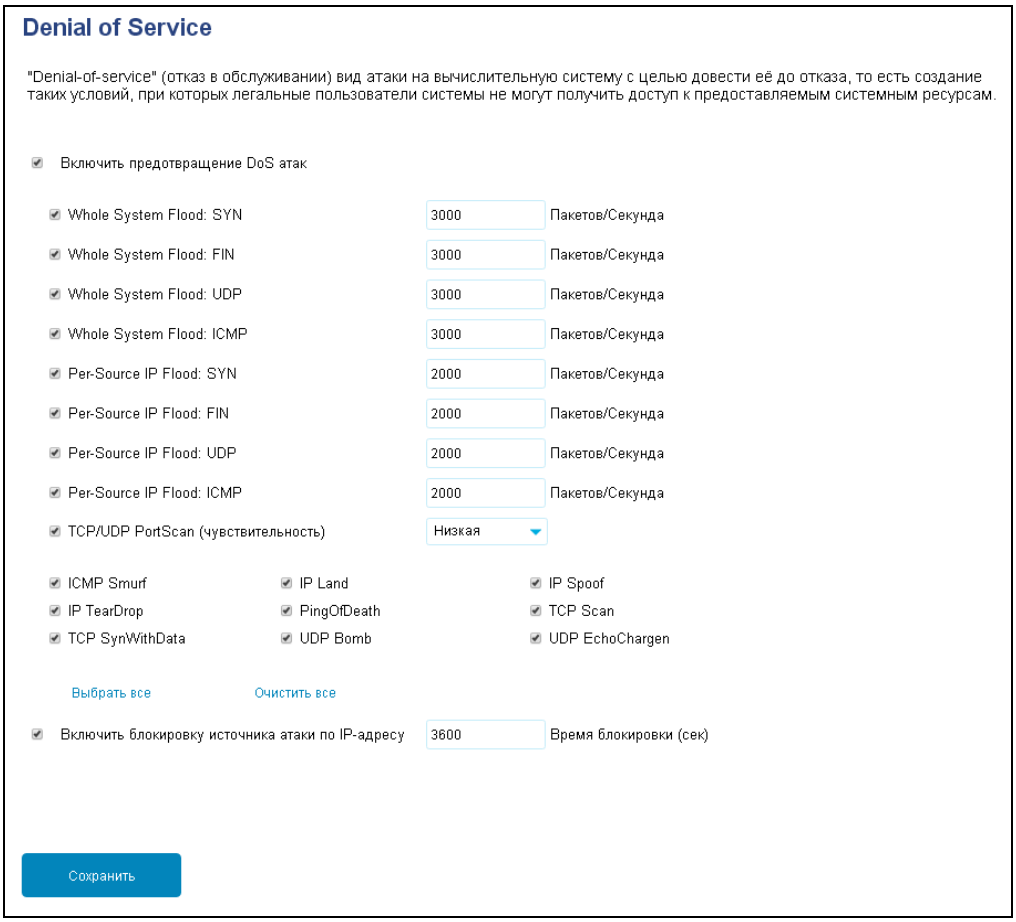


- *Текущее время* – указывается значение текущей даты и времени. Есть возможность вместо ввода скопировать эти данные из компьютера.
- *Временная зона* – часовой пояс в котором находится устройство. В зависимости от этого будет выполняться подстройка времени.
- *Разрешить синхронизацию с NTP-сервером* – при выставленном флаге происходит синхронизация с сервером точного времени.
- *Адрес NTP-сервера* – можно выбрать сервер из предложенного списка или ввести его вручную.

Подменю «Защита DoS»

Denial of Service (DoS) – группа сетевых атак, направленных на сбои в работе устройства путем отправки большого числа различных пакетов с целью вызвать 100% загрузку процессора. Со стороны пользователя это может наблюдаться в проблемах со скоростью передачи данных или их полное прекращение без видимых на то причин.

Для предотвращения DoS-атак в устройстве по умолчанию включены алгоритмы распознавания подозрительной активности пакетов, поступающих на WAN-порт, различных видов трафика и, при необходимости, производят запрет на обработку пакетов от конкретного источника или определенный (подозрительный) тип пакетов который может поступать с разных адресов.



— *Включить предотвращение DoS атак* – при выставленном флаге защита от DoS атак включена.

— *Whole System Flood* – группа счетчиков, определяющих интенсивность пакетов определенного типа, которые проходят через устройство за одну систему. В случае превышения лимита на Syslog сервер отправляется соответствующее уведомление. Счетчики задаются отдельно для пакетов SYN, FIN, UDP, ICMP.

— *Per-Source IP Flood* – группа счетчиков определяющих интенсивность трафика по каждому источнику. В случае превышения порогового значения отправляется сообщение на Syslog сервер, а также выполняется блокировка по IP-адресу источника на заданное время. Счетчики задаются отдельно для пакетов SYN, FIN, UDP, ICMP.

— *TCP/UDP Port Scan* – функция определяет подозрительную активность сканирования портов устройства и отправляет сообщение об этом на Syslog сервер.

Сканирование портов происходит с целью выявления слабого места в защите, куда может быть проведена атака. В случае появления такого сообщения на Syslog сервере рекомендуется отключить в подменю «WAN Интерфейс» опции «Разрешить ping через WAN» и «Разрешить доступ к Web-интерфейсу устройства через WAN».

— *ICMP Smurf* – функция выполняет защиту от ICMP-ответов, поступающих на WAN-интерфейс от подозрительных источников.

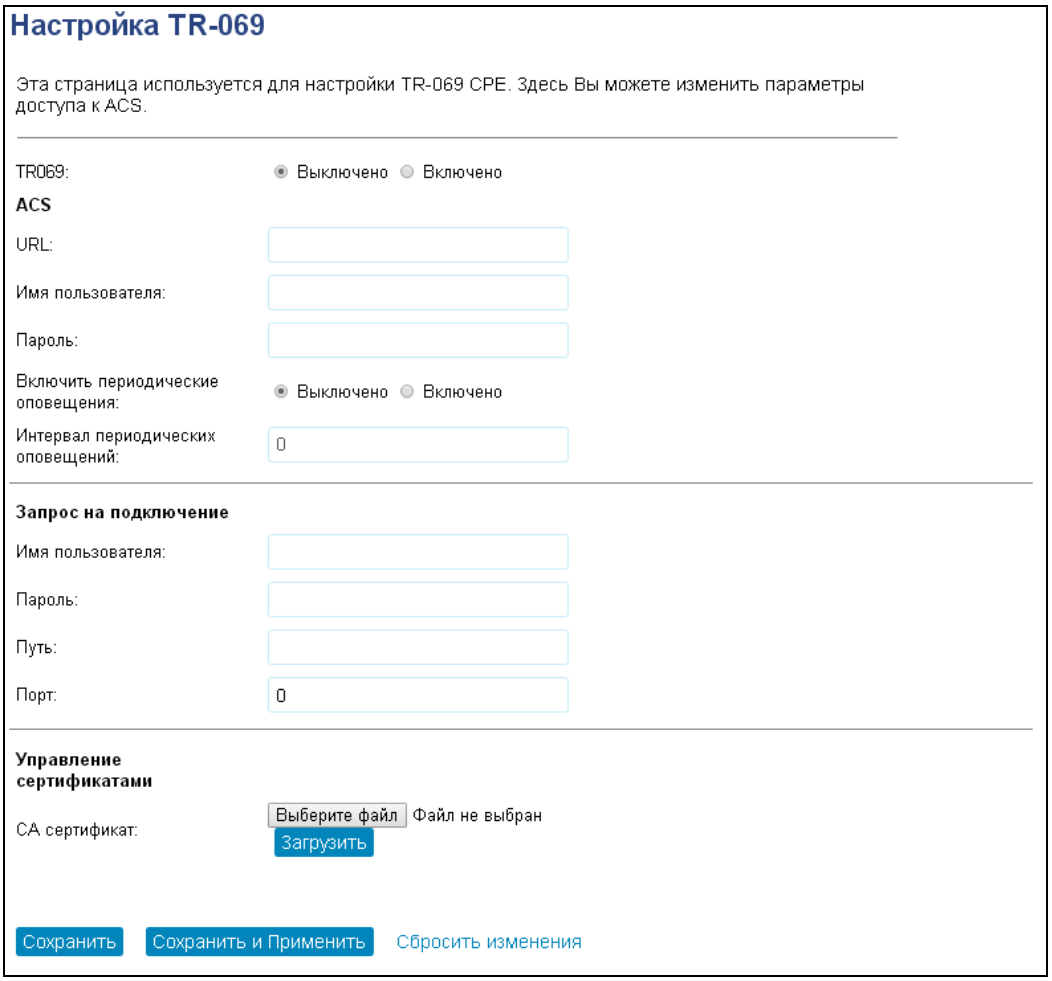
— *IP Land* – функция выполняет защиту от пакетов, у которых поля адреса отправителя и получателя в заголовке IP совпадают, что может привести к бесконечному циклу пересылки пакета самому себе и перегрузке устройства.

— *IP Spoof* – функция выполняет защиту от пакетов, которые могут быть отправлены из недостоверного источника с подменой IP-адресов для сокрытия этого факта.

- *IP TearDrop* – функция выполняет защиту от пакетов с неверно выставленным смещением данных, что при его обработке может привести к сбою определения начала и конца фрагмента данных.
- PingOfDeath – функция выполняет защиту от ICMP-пакетов с недопустимым размером (более 65 535 байт).
- *TCP SynWithData* – функция выполняет защиту от TCP-пакетов с выставленным флагом SYN, но имеющих в своем составе данные, которых быть не должно.
- *UDP Bomb* – функция выполняет защиту от UDP-пакетов в составе которых нарушен формат служебных полей.
- *UDP EchoChargen* – функция выполняет защиту от атак на сервис Chargen.
- *Включить блокировку источника атаки по IP-адресу* – при выставленном флаге в случае выявления источника атаки будет произведена его блокировка на указанное время. По окончанию таймера блокировка снимается, но может быть выполнена снова, если атака не прекратится.

Подменю «Настройка TR-069»

В подменю «Настройка TR-069» выполняется настройка протокола автоматического конфигурирования абонентских устройств TR-069.



Общие:

– *TR-069* – при установленном флаге разрешена работа встроенного клиента протокола TR-069, иначе – запрещена.

– *URL* – адрес сервера автоконфигурирования. Адрес необходимо вводить в формате http://<address>:<port> или https://<address>:<port> (<address> – IP-адрес или доменное имя ACS-

сервера, <port> – порт сервера ACS, по умолчанию порт 10301). Во втором случае клиент будет использовать безопасный протокол HTTPS для обмена информацией с сервером ACS.

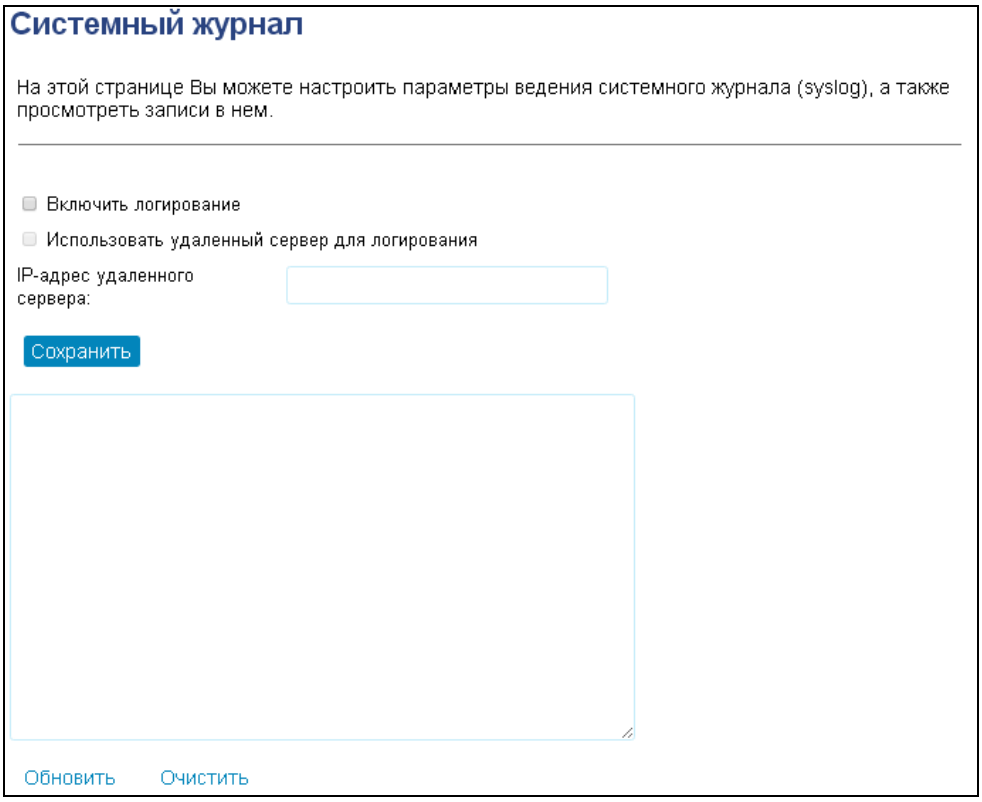
- *Включить периодический опрос* – при установленном флаге встроенный клиент TR-069 осуществляет периодический опрос сервера ACS с интервалом, равным «Интервалу периодических оповещений», в секундах. Цель опроса - обнаружить возможные изменения в конфигурации устройства.
- *Имя пользователя, Пароль* – имя пользователя и пароль для доступа клиента к ACS-серверу.

Запрос на подключение:

- *Имя пользователя, Пароль* – имя пользователя и пароль для доступа ACS-сервера к клиенту TR-069;
- *Путь* – путь в файловой системе сервера;
- *Порт* – используемый порт для подключения.

Подменю «Системный журнал»

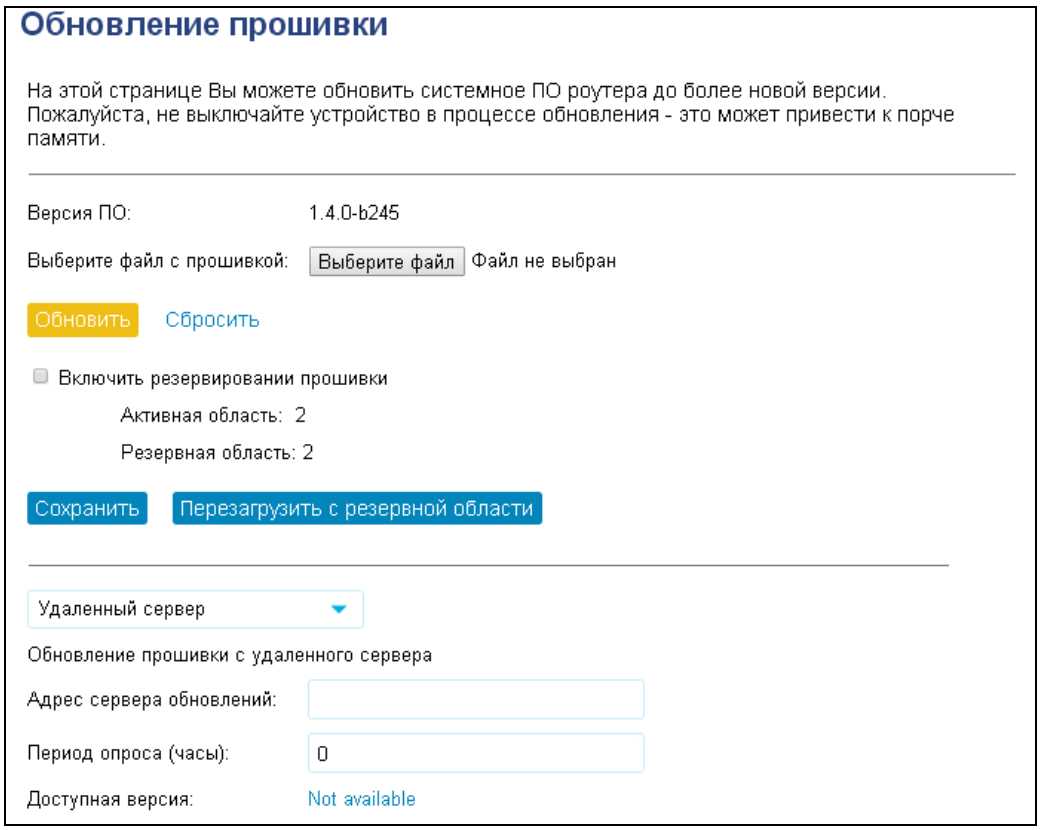
Подменю «Системный журнал» предназначено для настройки вывода разного рода отладочных сообщений системы в целях обнаружения причин проблем в работе устройства. Отладочную информацию возможно получить по событиям в беспроводной сети (например, подключение нового клиента) и защите от DoS-атак.



- *Включить логирование* – при выставленном флаге функция журнала активна;
- *Использовать удаленный сервер для логирования* – при выставленном флаге отладочная информация будет отправляться на удаленный сервер по протоколу syslog. Его адрес задается в поле «IP-адрес удаленного сервера».

Подменю «Обновление прошивки»

Подменю «Обновление ПО» предназначено для обновления управляющей микропрограммы устройства. Устройство позволяет использовать две прошивки: основную и резервную, на случай если основная повреждена. Переключение между прошивками осуществляется в этом подменю.



- *Версия ПО* – версия программного обеспечения, установленного на устройстве.
- *Выберите файл с прошивкой* – при наличии локального файла с прошивкой можно обновить ПО, указав путь к этому файлу и нажав кнопку «Обновить». Актуальную прошивку можно скачать на сайте *http://eltex-co.ru/downloads*.
- Включить резервирование прошивки – активирует запись второй прошивки в память устройства. Загрузиться со второй прошивки можно по кнопке «Перезагрузить с резервной области».

В случае когда основная прошивка повреждена, резервная будет загружена автоматически

Обновление прошивки по сети

Устройство поддерживает возможность обновления прошивки путем скачивания ее из сети. В качестве источника обновления может быть удаленный сервер или прямые ссылки на прошивку в виде HTTP, FTP, TFTP адреса.

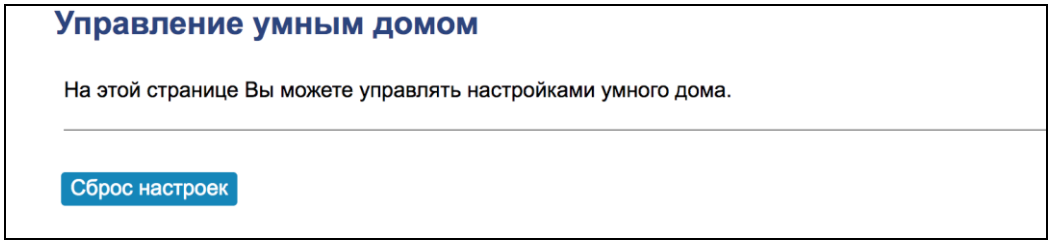
- *Адрес сервера обновлений* – в этом поле указывается адрес сервера на котором находится файл прошивки. По умолчанию это download.eltex-media.ru.
- *Период опроса* – интервал времени, по которому устройство будет обращаться к серверу за новой прошивкой.
- *Доступная версия* – версия программного обеспечения доступная для обновления на сервере.

Для работы функции проверки обновления необходимо наличие выхода в Интернет.

Не отключайте питание устройства, не выполняйте его перезагрузку в процессе обновления ПО.

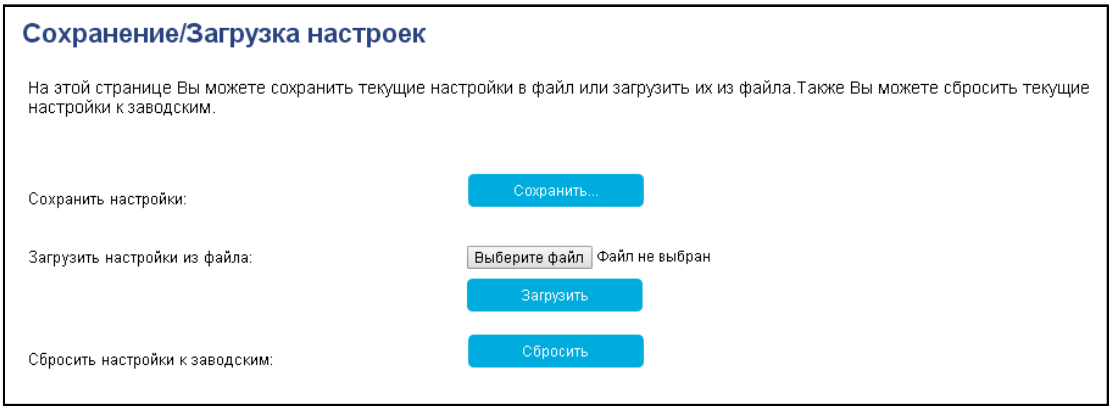
Подменю «Умный дом»

В данном подменю выполняется настройка контроллера умного дома. Кнопка «Сброс настроек» выполняет перезапуск контроллера и удаление всех подключенных по Z-Wave устройств.



Подменю «Сохранение/Загрузка настроек»

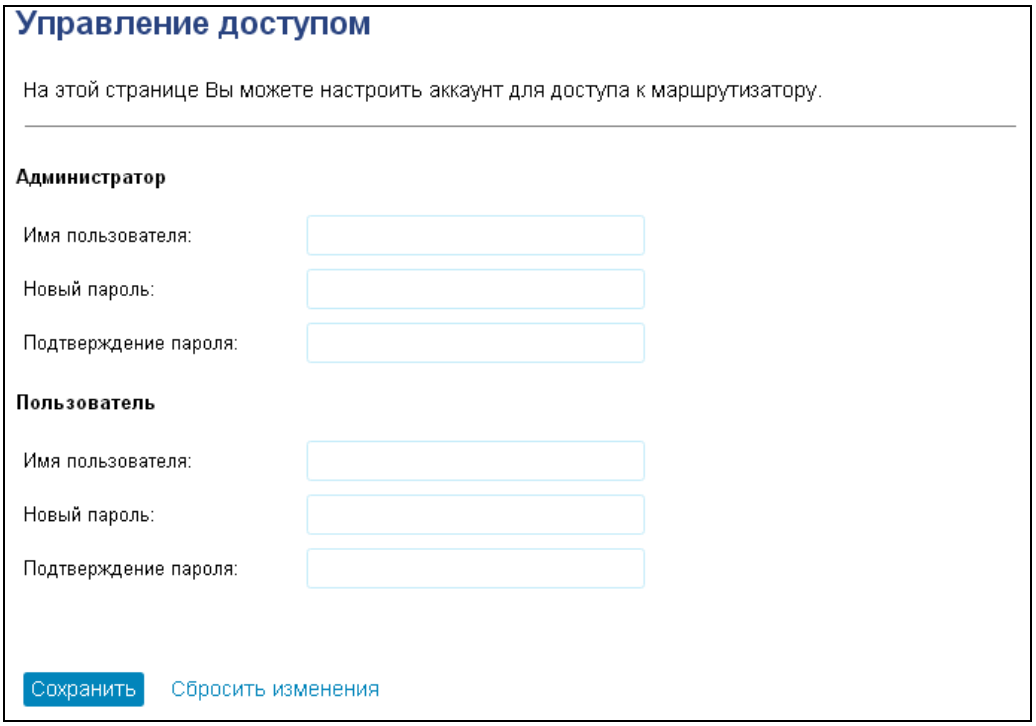
В подменю *«Сохранение/Загрузка настроек»* выполняется сохранение и обновление текущей конфигурации.



- *Сохранить настройки* - для сохранения текущей конфигурации устройства на локальный компьютер нажмите кнопку «Сохранить…».
- *Загрузить настройки* – выбор сохраненного на локальном компьютере файла конфигурации. Для обновления конфигурации устройства нажмите кнопку «Выберите файл», укажите файл (в формате .dat) и нажмите кнопку «Загрузить». Загруженная конфигурация применяется автоматически без перезагрузки устройства.
- *Сброс устройства на заводские настройки* - для сброса всех настроек устройства на стандартные заводские установки, нажмите кнопку «Сброс».

Подменю «Управление доступом»

В подменю «Управление доступом» устанавливаются логин и пароль доступа к Web-интерфейсу устройства для Администратора и Пользователя.



- *Имя пользователя* – поле для изменения имени пользователя. По умолчанию: **admin**.
- *Новый пароль* – поле для ввода нового пароля к устройству. По умолчанию: **password**.
- *Подтверждение пароля* – поле для повторного ввода нового пароля с целью его подтверждения.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку «Сохранить изменения». Для отмены изменений покиньте страницу без сохранения изменений. Для восстановления значений по умолчанию нажмите кнопку «Сбросить изменения».

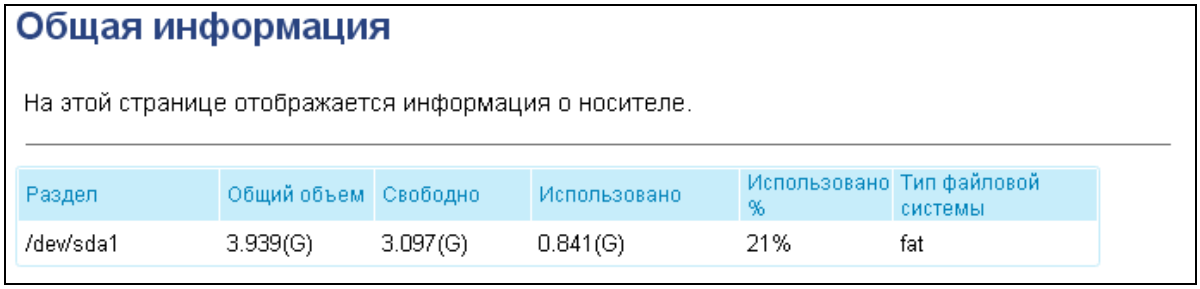
В целях обеспечения безопасности при настройке устройства рекомендуется изменить логин и пароль.

4.3.10 USB Настройки

В меню «USB Настройки» можно управлять файлами на подключенном USB накопителе, а также предоставлять к ним доступ по протоколу SMB, FTP и сервису DLNA.

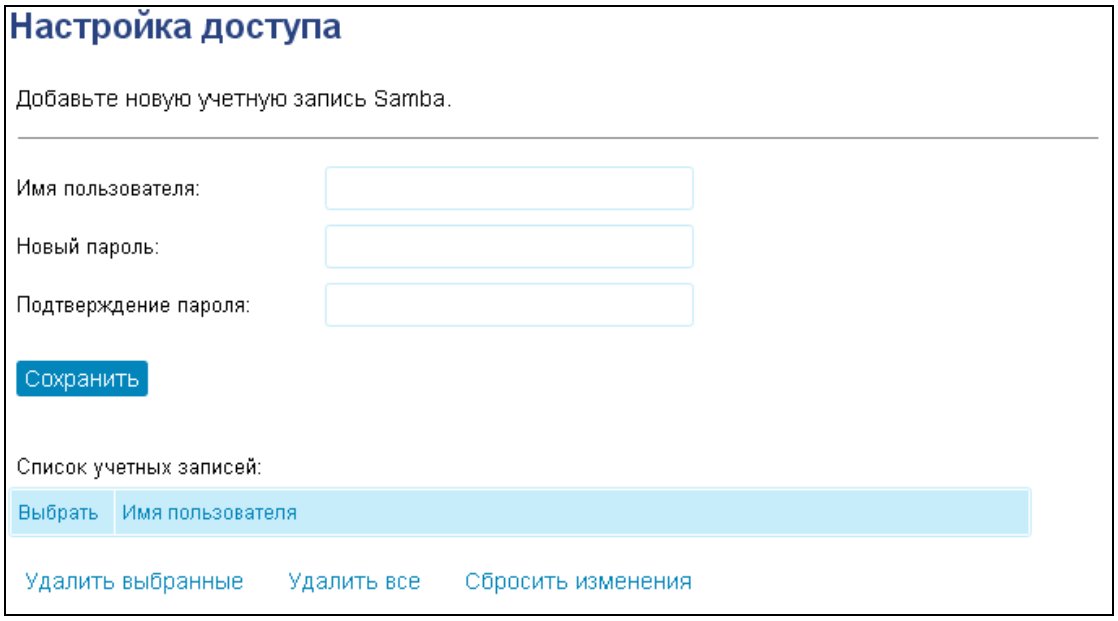
Подменю «Общая информация»

В этом подменю отображается информация о носителе.



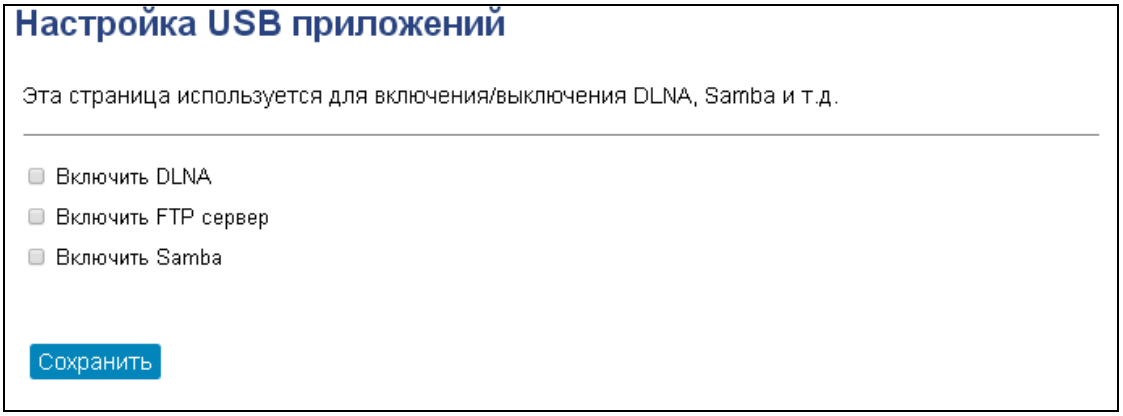
Подменю «Настройка доступа»

В этом подменю можно добавить и удалить учетные записи Samba.



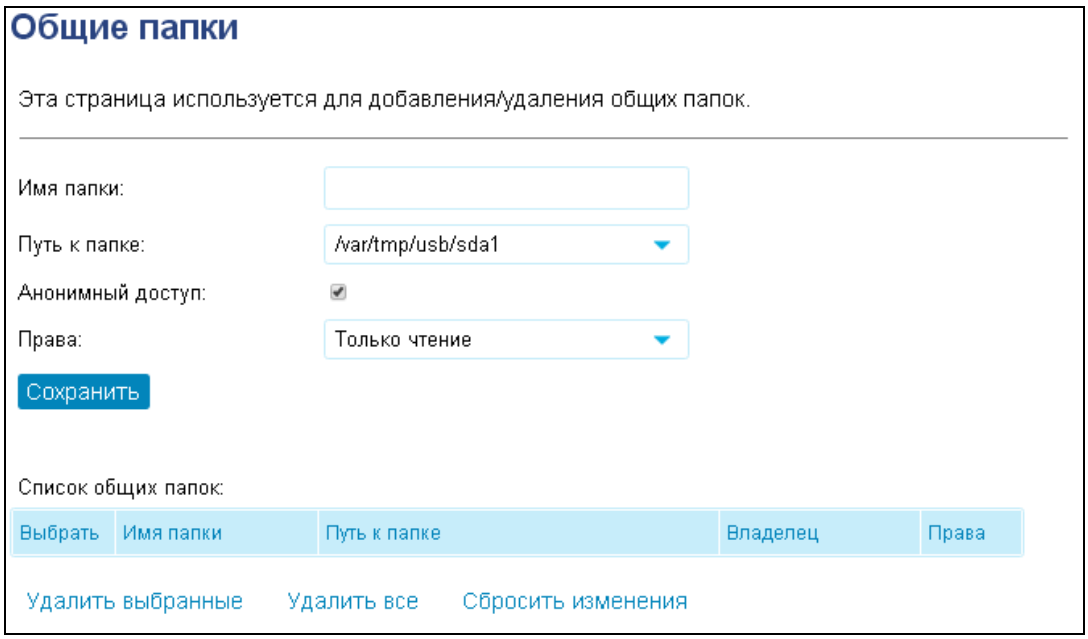
Подменю «Настройка USB приложений»

В этом подменю можно включить/выключить DLNA, FTP-server, Samba.



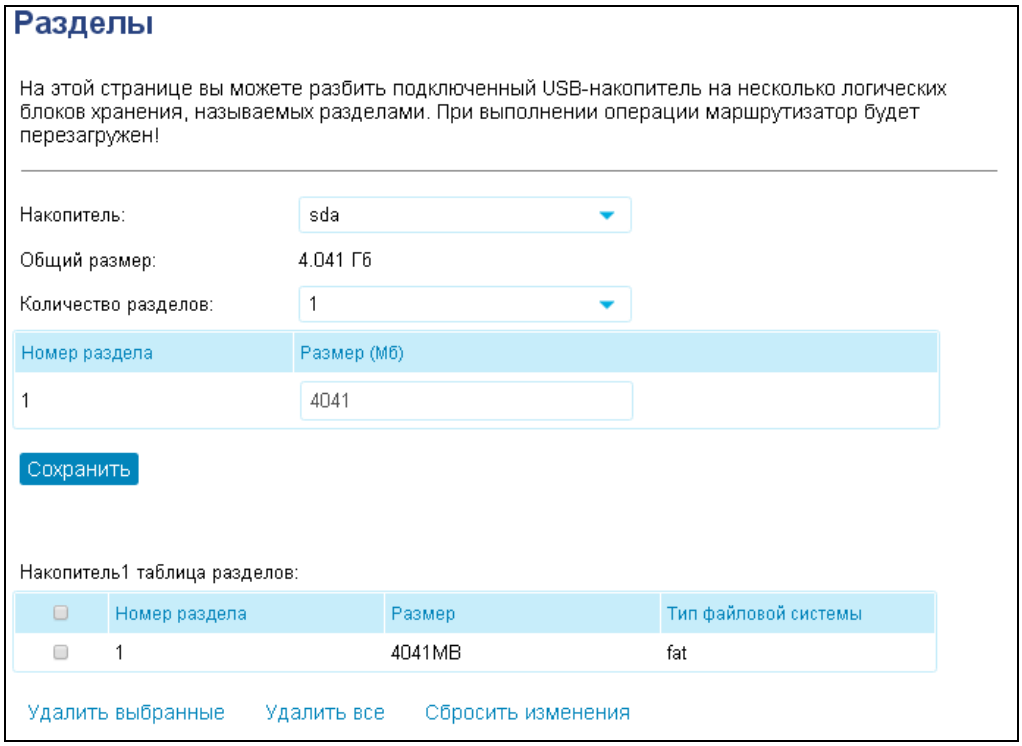
Подменю «Общие папки»

В этом подменю можно разрешить доступ устройств, подключенных к маршрутизатору к папкам на включенном в маршрутизатор USB-устройстве.



Подменю «Разделы»

В этом подменю можно управлять разделами памяти USB-устройства.



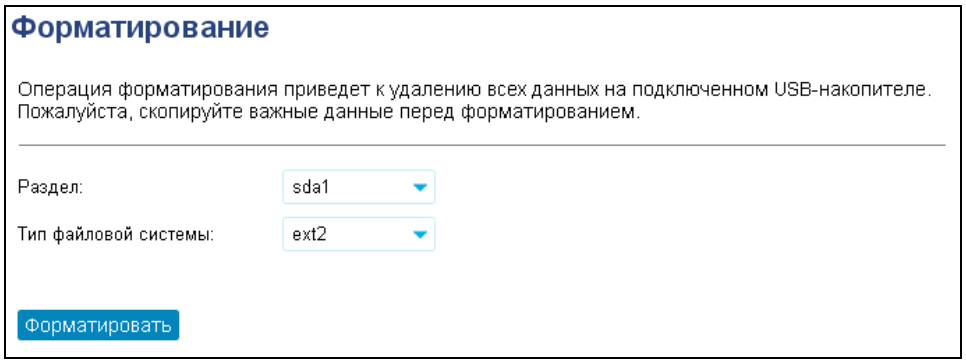
— *Накопитель* – выбор подключенного устройства.

— *Общий размер* – размер памяти устройства.

— *Количество разделов* – выбор количества разделов памяти устройства. Ниже указывается размер каждого раздела.
— *Таблица разделов* — информация о всех разделах устройства. Здесь также можно удалить несколько или все разделы.

Подменю «Форматирование»

В этом подменю можно отформатировать память. При форматировании все данные удаляются.



— *Раздел* – выбор раздела для форматирования.
— *Тип файловой системы* — выбор типа файловый системы в который будет переформатирован раздел.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации оборудования ТОО «ЭлтексАлатау» Вы можете обратиться в Сервисный центр компании:

050032, Республика Казахстан, г. Алматы, мкр-н. Алатау, ул. Ибрагимова 9
Телефон:
+7(727) 220-76-10, +7 (727) 220-76-07

E-mail: post@eltexalatau.kz

На официальном сайте компании Вы можете найти техническую документацию и программное обеспечение для продукции ТОО «ЭлтексАлатау», обратиться к базе знаний, проконсультироваться у инженеров Сервисного центра на техническом форуме.

Официальный сайт компании: http://eltexalatau.kz