Абонентский терминал

RG-35-Wac
RG-35-WZ

Руководство по эксплуатации
Версия ПО 2.1.1

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	2.1.1	

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Аннотация

Устройства RG-35-Wac и RG-35-WZ являются точками доступа Wi-Fi с интегрированным маршрутизатором. Основное предназначение RG-35-Wac и RG-35-WZ: установка внутри зданий в качестве точки доступа к различным интерактивным сервисам 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 абонентских терминалов RG-35-Wac и RG-35-WZ.

Условные обозначения

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.

1 ОПИСАНИЕ ИЗДЕЛИЯ

1.1 Назначение

Абонентские терминалы RG-35-Wac и RG-35-WZ (далее «устройство») — единые точки доступа к современным интерактивным сервисам по проводным и беспроводным сетям передачи данных: Интернет и Full HD IPTV. RG-35-Wac и RG-35-WZ подключается к проводной сети с помощью 10/100M Ethernet-интерфейса, и с помощью радиоинтерфейса создают беспроводной доступ для устройств, поддерживающих технологию Wi-Fi (IEEE 802.11a/b/g/n/ac) в диапазоне 2.4 и 5 ГГц.

К RG-35-Wac и RG-35-WZ можно подключить до четырех устройств проводной сети. USB-разъем используется для подключения внешних накопителей.

В устройствах также реализован расширенный функционал для стабильной работы IP-телевидения по беспроводной сети: программными средствами обеспечиваются плавность и непрерывность воспроизведения видео. RG-35-Wac и RG-35-WZ имеют возможность одновременной трансляции видеопотоков и передачи данных.

Устройства поддерживают современные требования к качеству сервисов и позволяют передавать наиболее важный трафик в более приоритетных очередях по сравнению с обычным. Обеспечение приоритизации происходит при помощи основных технологий QoS.

RG-35-WZ имеет встроенный контроллер «Умного дома» совместимый с Z-Wave устройствами для взаимодействия с датчиками и устройствами системы «Умный дом» и управления ими через платформу Eltex Smart Control (Eltex SC).

1.2 Характеристика устройства

Интерфейсы:

- LAN: 4 порта Ethernet 10/100BASE-T (RJ-45);
- WAN: 1 порт Ethernet 10/100BASE-T (RJ-45);
- 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 5,3 В от сети переменного тока 110-240 В.

Функции:

- сетевые функции:
  - работа в режиме «моста» , «маршрутизатора»;
  - поддержка PPPoE (PAP, SPAP и CHAP-авторизация, PPPoE-компрессия);
  - 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;
- управление Z-Wave совместимыми устройствами[1].

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

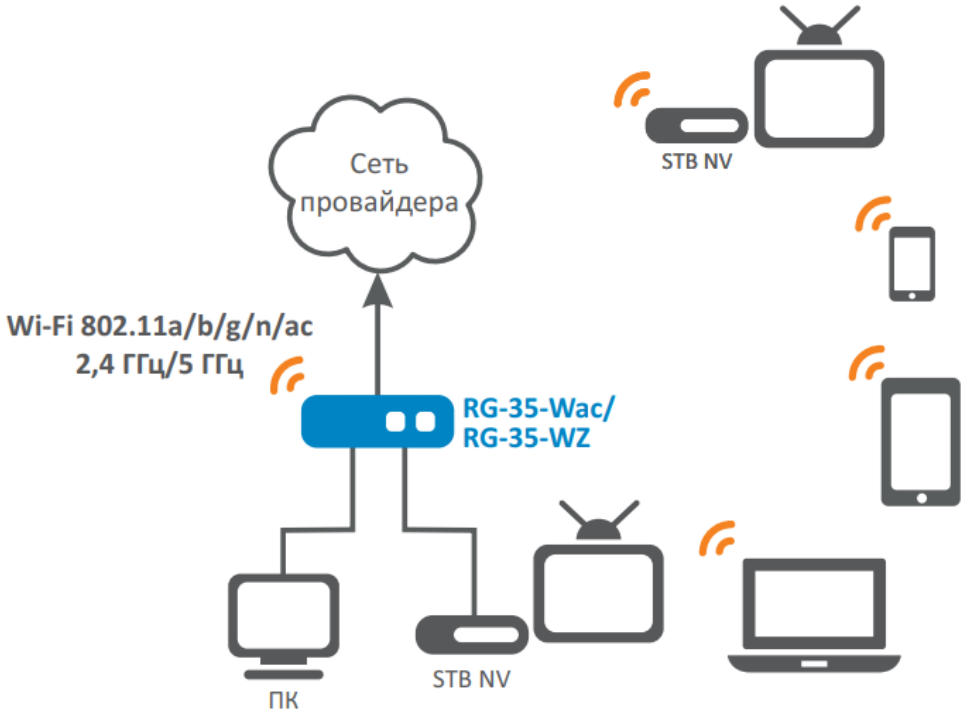


Рисунок 1 — Функциональная схема использования RG-35-WZ/Wac

[1] Доступно только для RG-35-WZ

1.3 Основные технические параметры

Основные технические параметры устройства приведены в таблице 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 (RG-35-WZ, 32 МБ)
Операционная система	Linux

Параметры WAN-интерфейса Ethernet

Количество портов	1
Электрический разъем	RJ-45
Скорость передачи, Мбит/с	10/100, 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	802.11a/b/g/n/ac
Частотный диапазон, МГц	2412–2472 МГц, 5180–5320 МГц, 5660–5805 МГц
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 867 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

Умный дом

Сигнал Z-Wave модуля на частоте[2]	869 МГц

Управление

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

Общие параметры

Питание	адаптер питания 5,3 В DC, 2 А.
Потребляемая мощность	не более 4 Вт
Рабочий диапазон температур	от +5 до +40°С
Относительная влажность при температуре 25°С	до 80%
Габариты	150x110x27 мм
Масса	не более 0,2 кг

[2] Z-Wave модуль размещается только на RG-35-WZ

1.4 Конструктивное исполнение

Абонентский терминал RG-35-Wac/RG-35-WZ выполнен в пластиковом корпусе размерами 150x110x27 мм.

1.4.1 Передняя панель устройства. Световая индикация

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

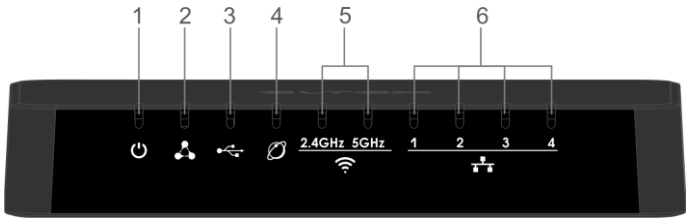


Рисунок 2 — Внешний вид передней панели RG-35-Wac/RG-35-WZ

На верхней панели устройства *RG-35-Wac/RG-35-WZ* расположены световые индикаторы. Описание работы световых индикаторов представлено в таблице 2.

Таблица 2 — Описание индикаторов верхней панели

Индикатор			Состояние индикатора	Состояние устройства
1		Power	зеленый, горит постоянно	включено питание устройства, нормальная работа
2		Status	зеленый, мигает (1 такт в секунду)	запущена функция WPS/запущен процесс обновления программного обеспечения устройства
			зеленый, мигает (5 тактов в секунду)	идет процесс загрузки CPE и установки соединения с сетью провайдера
			зеленый, горит постоянно	нормальная работа
3		USB	зеленый, горит	USB-устройство подключено
			не горит	USB-устройство не подключено
4		WAN	зеленый, горит постоянно	установлено соединение между станционным терминалом и абонентским устройством
			мигает	процесс пакетной передачи данных по WAN-интерфейсу
			не горит	WAN-кабель не подключен
5		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
			не горит	точка доступа Wi-Fi данного диапазона отключена: 2,4 ГГц и/или 5 ГГц
6		LAN	зеленый, горит	установлено соединение с подключенным сетевым устройством
			мигает	процесс пакетной передачи данных по LAN-интерфейсу
			не горит	LAN-кабель не подключен

1.4.2 Задняя панель устройства. Описание разъемов

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

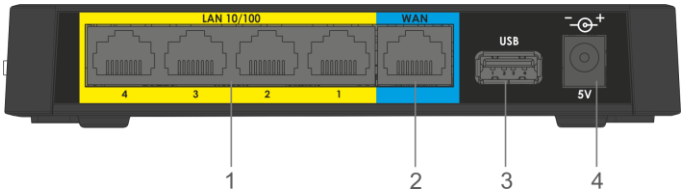


Рисунок 3 – Внешний вид задней панели RG-35-Wac/RG-35-WZ

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

Таблица 3 — Описание индикаторов и органов управления задней панели RG-35-Wac/RG-35-WZ

Элемент задней панели		Описание
1	LAN	4 порта 10/100BASE-T Ethernet (разъем RJ-45) для подключения сетевых устройств
2	WAN	порт 10/100BASE-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

1.4.3 Описание кнопок боковой панели

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

Рисунок 4 — Внешний вид боковой панели RG-35-Wac/RG-35-WZ

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

Таблица 4 — Описание органов управления боковой панели RG-35-Wac/RG-35-WZ

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

1.5 Подключение по WPS

Устройство поддерживает функцию подключения клиентов к Wi-Fi сети по стандарту WPS.

Порядок подключения:

1. Выберите на клиентском устройстве способ подключения WPS.
2. На правой боковой панели RG-35-Wac/RG-35-WZ нажмите и удерживайте в течение 3-х секунд кнопку WPS.

Клиент подключится к маршрутизатору (RG-35-Wac/RG-35-WZ) автоматически.

Подключение клиентского устройства к маршрутизатору занимает не более 2-х минут. Если не удалось подключить устройство с первого раза, повторите попытку и убедитесь, что функция WPS на клиентском устройстве была включена не позднее чем через 2 минуты после включения функции WPS на маршрутизаторе.

По умолчанию функция WPS включена. Отключить функцию можно на странице настройки WPS. Ее описание приведено в разделе 3.3.3.7 Подменю «WPS».

1.6 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.

1. Для перезагрузки устройства нажмите и удерживайте кнопку «F» в течение 2-х секунд, а затем отпустите.

2. Для запуска устройства с заводскими настройками нажмите и удерживайте кнопку «F» более 5-ти секунд, пока индикатор «Status» не начнет мигать 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;
   логин/пароль пользователя с повышенными привилегиями: superadmin/password.

1.7 Комплект поставки

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

- Абонентский маршрутизатор RG-35-Wac/RG-35-WZ;
- Адаптер питания 220–5.3В, 2.0 А;
- Руководство по установке и настройке.

2 ПОРЯДОК УСТАНОВКИ

2.1 Правила безопасной эксплуатации

1. Не устанавливайте устройство рядом с источниками тепла и в помещениях с температурой ниже 5°С или выше 40°С.
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.

2.2 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 длительное время находилось при низкой температуре, перед началом работы следует выдержать его в течение двух часов при комнатной температуре.
3. Если устройство длительное время находилось в условиях повышенной влажности, перед началом работы следует выдержать его в нормальных условиях не менее 12 часов.
4. Устройство устанавливается в горизонтальном положении, соблюдая инструкции по технике безопасности.
5. 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-Wac/RG-35-WZ и другими беспроводными сетевыми устройствами;
    c. Не устанавливайте устройство вблизи (порядка 2 м) электрических устройств и радиоустройств;
    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.

2.3 Порядок включения

1. Подключите сетевой Ethernet-кабель, проведенный вашим интернет-провайдером, к разъему WAN RG-35-Wac/RG-35-WZ (Рисунок 3).
2. Если RG-35-Wac/RG-35-WZ будет использоваться в качестве домашнего проводного маршрутизатора, то подключите сетевой Ethernet-кабель к разъемам **LAN** RG-35-Wac/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 несколько минут).

3 УПРАВЛЕНИЕ УСТРОЙСТВОМ ЧЕРЕЗ WEB-КОНФИГУРАТОР

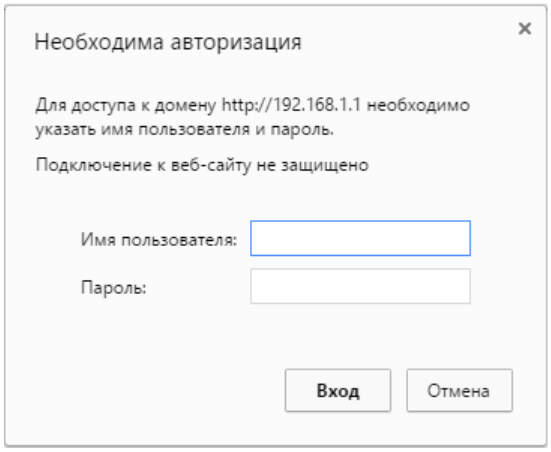
3.1 Начало работы

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

1. Откройте web-браузер, 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».

Учетная запись пользователя: имя - *admin*, пароль - *password*.

(Некоторые пункты меню в данной учетной записи скрыты)

Учетная запись администратора: имя — superadmin, пароль - password

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

3.2 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.

3.3 Панель управления устройством

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

3.3.1 Основные элементы web-интерфейса

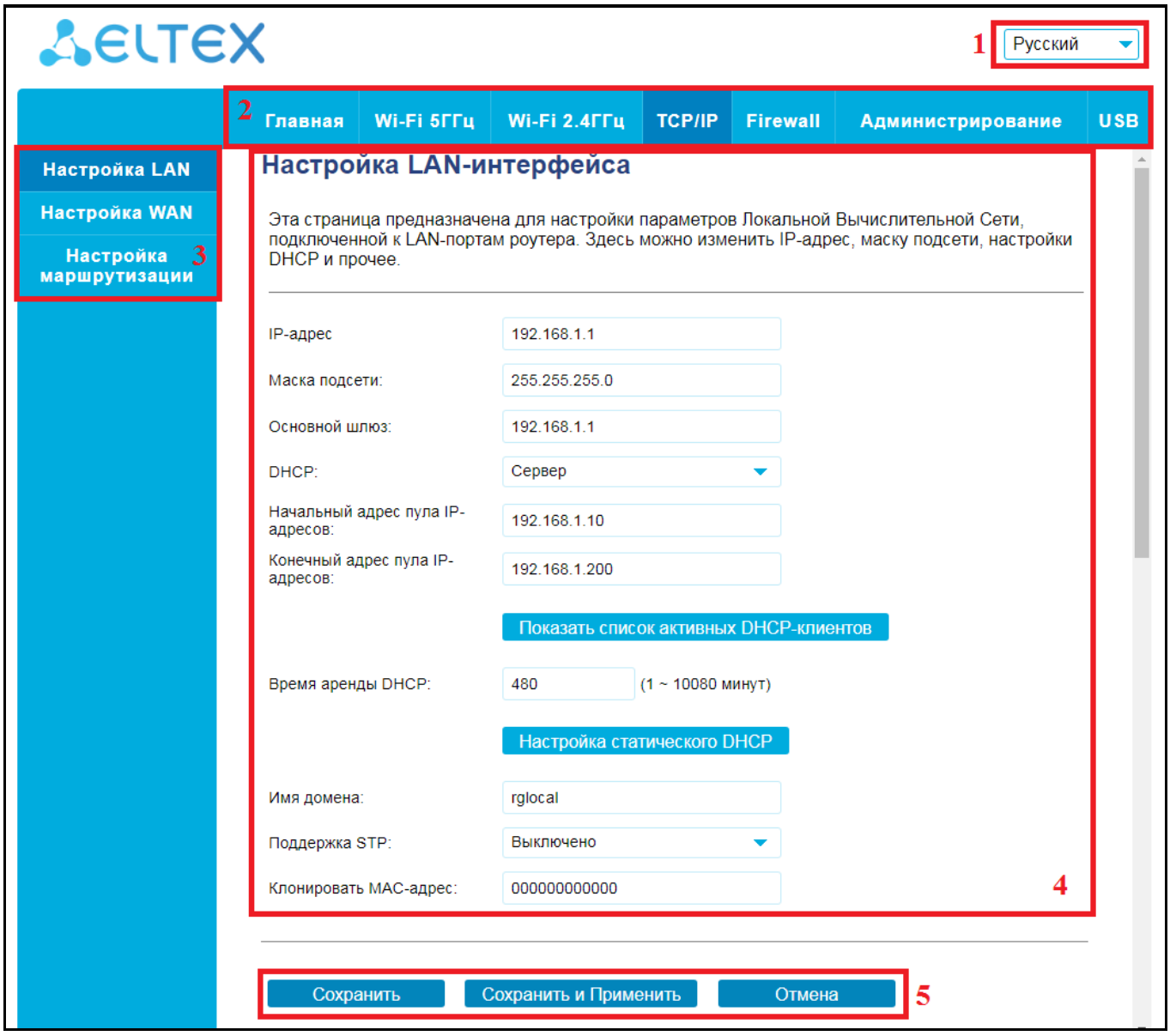


Рисунок 5 — Элементы навигации web-конфигуратора

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.

3.3.2 Меню «Главная»

В меню «Главная» можно посмотреть статус устройства, а также всех его интерфейсов.

3.3.2.1 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.

Статус роутера

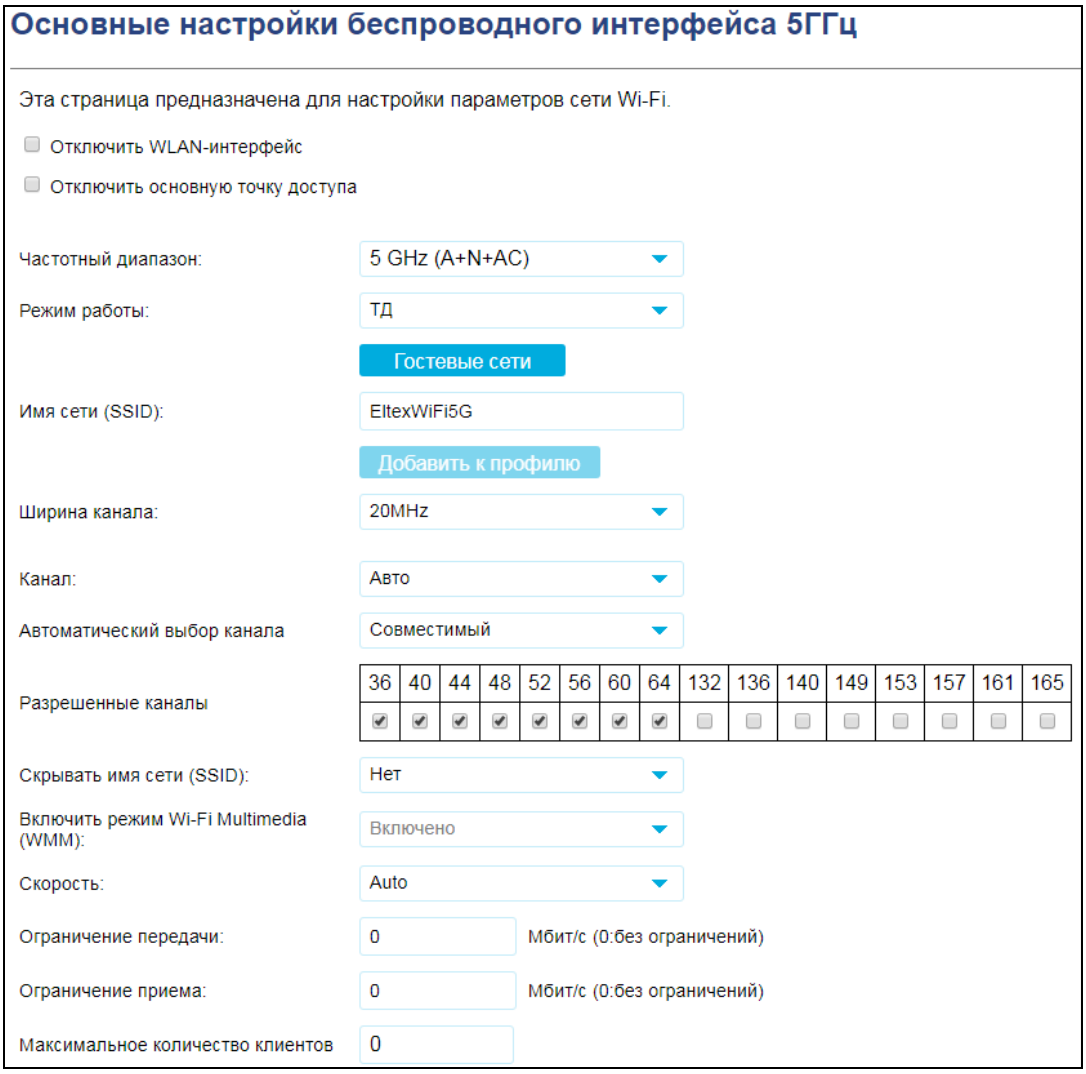
Эта страница отображает текущее состояние устройства, а также некоторые основные настройки.

Система	
Время работы	0day:4h:31m:46s
Время сборки	Tue Oct 22 15:40:04 +07 2019
Модель устройства	RG-35-WZ
H/W версия	1v7
Производитель	ELTEX
Серийный номер	VI57001732
Версия ПО	2.0.1-b15
Конфигурация беспроводного интерфейса 1	
Режим	ТД
Частотный диапазон	5 GHz (A+N)
SSID	EltexWiFi5G
Канал	36
Шифрование	WPA2 Mixed
BSSID	e2:d9:e3:98:3f:b1
Клиенты	0

3.3.3 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.

3.3.3.1 Подменю «Основные настройки»



- *Отключить WLAN интерфейс* — при установленном флаге сеть Wi-Fi в диапазоне 2.4 ГГц или 5 ГГц выключена.
- *Отключить основную точку доступа* — при установленном флаге основная точка доступа будет отключена.
- *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)* — по стандарту 802.11n максимальная скорость составляет 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 867 Мбит/с.

- *Режим работы* — позволяет выбрать в каком режиме будет работать радиомодуль:

  - *ТД* — режим точки доступа;
  - *WDS* — режим беспроводного моста для соединения нескольких точек доступа, дополнительные настройки содержатся в подменю «Беспроводной мост»;
  - *ТД+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 «Авто» автоматически определяется канал с наименьшим уровнем помех.

- *Автоматический выбор канала* — выпадающий список с возможностью выбрать режим автоматического определения канала:

  - *Совместимый* — включается с 1 по 11 канал для 2.4 ГГц, с 36 по 64 канал для 5 ГГц;
  - *Пользовательский* — право выбора включаемого канала предоставляется пользователю;
  - *Полный* — включаются все доступные каналы.

- *Разрешенные каналы* — выбор каналов, на которых будет работать точка доступа.

- *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.

- *Скорость* — выпадающий список, позволяющий выбрать значение канальной скорости.

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

- *Ограничение приема* — позволяет задать ограничение по приема трафика Wi-Fi клиентам.

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

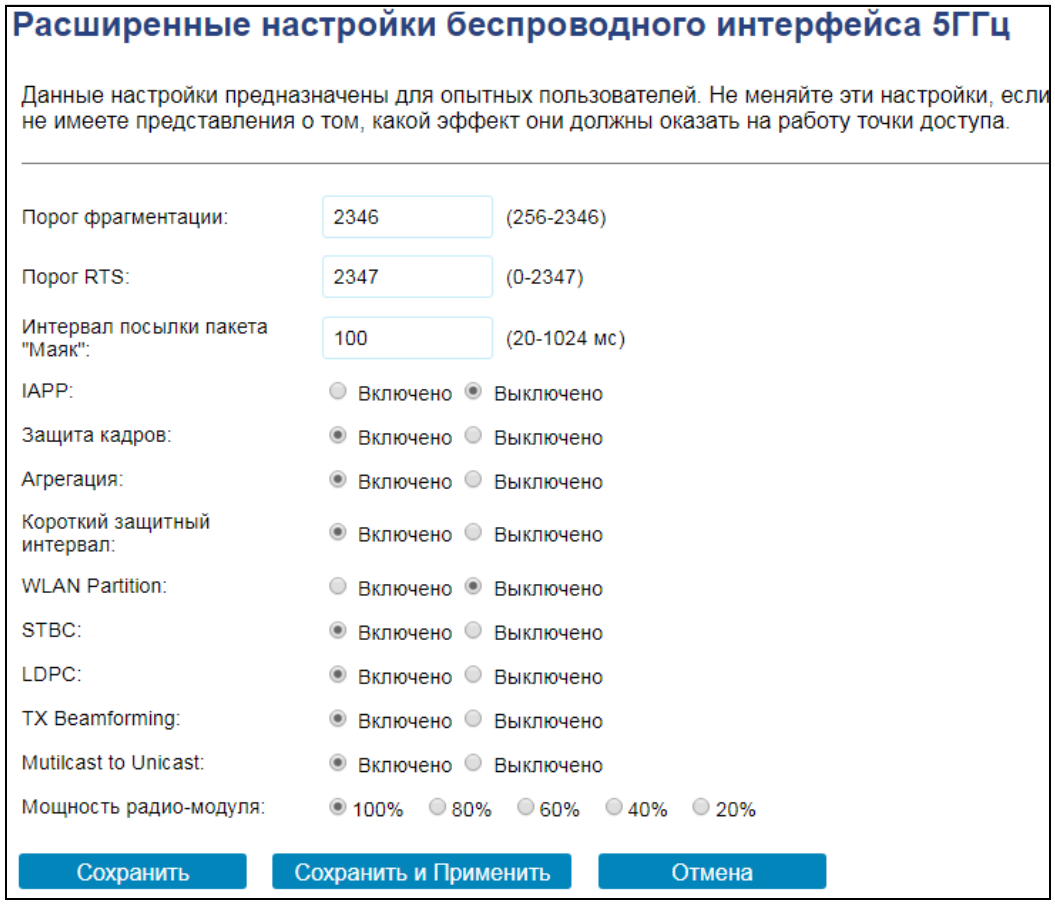
- *Активные соединения* — открывает в новом окне таблицу со списком всех подключенных к Wi-Fi сети клиентов.

- Включить клонирование MAC — при установленном флаге выполняется клонирование MAC-адреса для текущего интерфейса.

- *Включить режим универсального повторителя* — перевод устройства в режим работы «репитер» (работа в качестве точки доступа и клиента одновременно), что позволит расширить площадь покрытия сети Wi-Fi:

  – *Имя сети (SSID) дополнительного интерфейса* — имя расширенного интерфейса, к которому будут подключаться пользователи;
  – *Включения профиля беспроводного устройства* — при установленном флаге позволяет сохранять профили подключения к другим точкам доступа;
  – *Список профилей* — профили подключения к другим точкам доступа с соответствующими именами сетей (SSID) и типами шифрования.

3.3.3.2 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.

- *IAPP* — протокол IAPP (Inter-Access Point Protocol) позволяет клиентам, находящимся в роуминге маршрутизатора, взаимодействовать внутри одного сегмента сети, посредством переподключения к другому маршрутизатору. Информация о клиенте передается от одной точке доступа к другой и на её основании осуществляется переподключение клиента.

- *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 путем увеличения времени обслуживания старых клиентов, задания для них меньшего размера окна RTS и снижения 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 800 нс. 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 400 нс. 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 приема 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 приемника, 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 приемной 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.

- *Multicast to Unicast* — позволяет передавать беспроводным устройствам Multicast поток в виде Unicast, при условии что включена опция UDP2HTTP в настройках WAN-интерфейса.

- *Мощность радио-модуля* — выбор значения мощности Wi-Fi модуля.

3.3.3.3 Подменю «Безопасность»

- *Выберите SSID* — выбор сети, для которой будет выполняться конфигурирование.
- *Метод проверки подлинности* — выбор режима безопасности беспроводной сети:

  – *Выключено* — 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, ~!@#$%^&*()_-+=) и иметь длину 5 или 13 символов;
  – *WPA* — шифрование WPA. Длина ключа составляет от 8 до 63 символов. Разрешается использовать только символы: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>”`’ или пробел.
  – *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.

- *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;

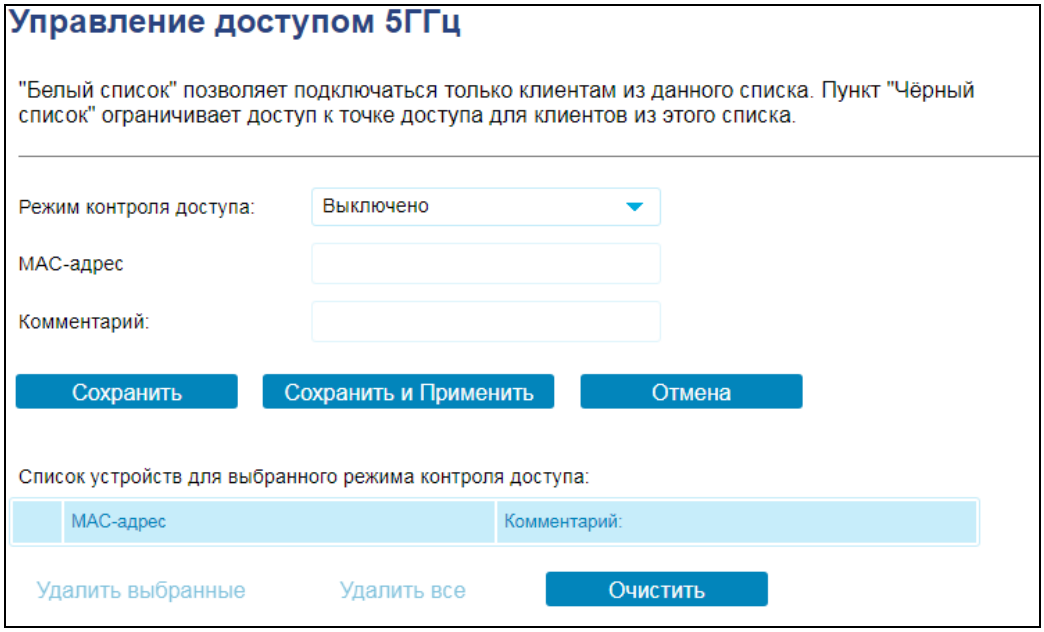
- *Enterprise (RADIUS)* — протокол, предназначенный для обеспечения централизованной аутентификации, авторизации и учета пользователей.
- *Personal (Pre-Shared Key)* — аутентификация с использованием общего пароля к сети.

- *Тип шифрования WPA/WPA2* — выбор типа шифрования TKIP или AES.
  Примечание: служба WPS будет деактивирована, если выбран метод проверки подлинности WPA или выбран тип шифрования TKIP.

- *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.
- *Защита управляющих кадров* — включение защиты фреймов управления. При выборе варианта опционально доступен пункт с включением функции хэширования по алгоритму SHA256.

3.3.3.4 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:

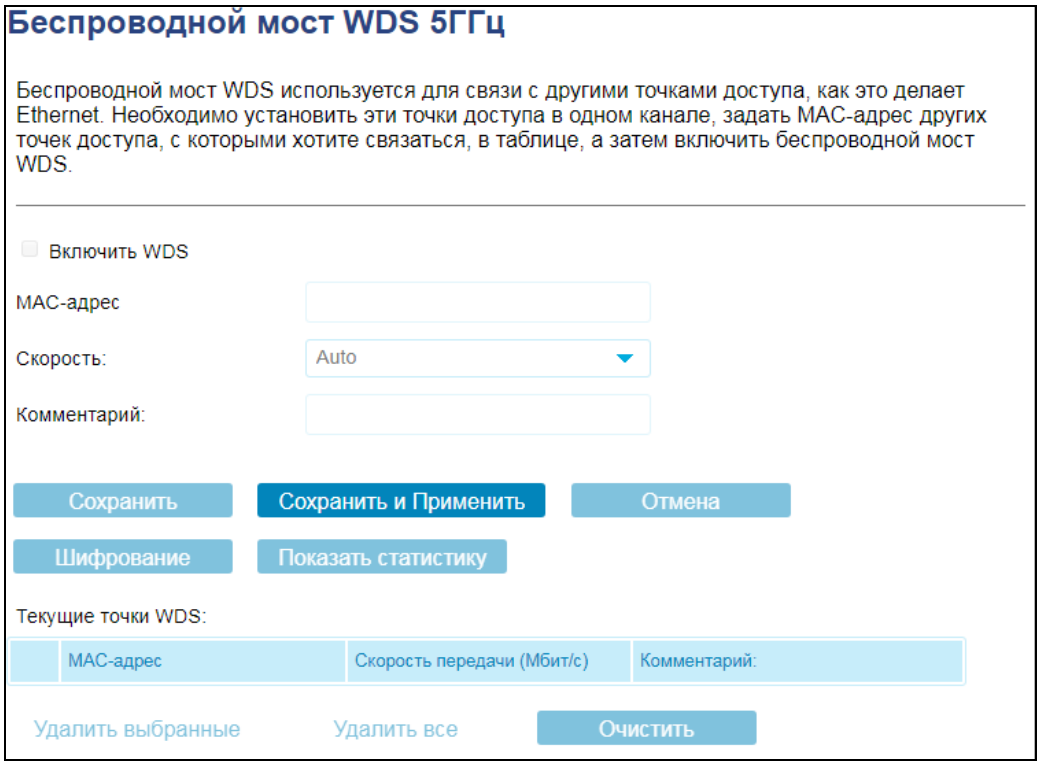
  - *Выключено* — нет ограничений по подключению устройств;
  - *Белый список* — к Wi-Fi сети могут подключиться только устройства с MAC-адресами из списка разрешенных;
  - *Черный список* — к Wi-Fi сети могут подключаться все устройства, за исключением перечисленных в списке.

- *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.

3.3.3.5 Подменю «Беспроводной мост»

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

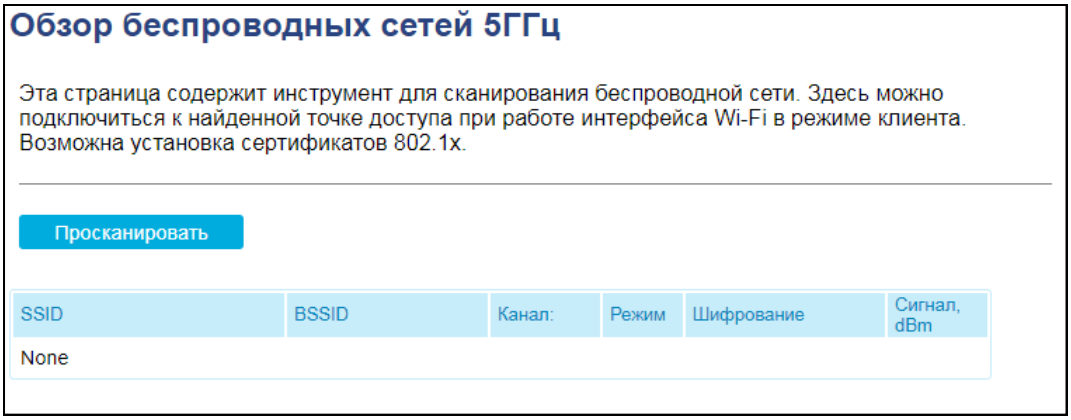


Функция WDS может использоваться отдельно для каждого диапазона частот.

- *MAC-адрес* — поле для ввода MAC-адреса устройства. Адрес вводится сплошным текстом без разделителей, например: a8f94b214fa0.
- *Скорость* — выпадающий список позволяет выбрать значение канальной скорости.
- *Комментарий* — поле для комментария к данному MAC-адресу. Не обязательно для заполнения. Для удобства рекомендуется записывать название устройства, для которого заводится запись в список.

3.3.3.6 Подменю «Обзор сетей»

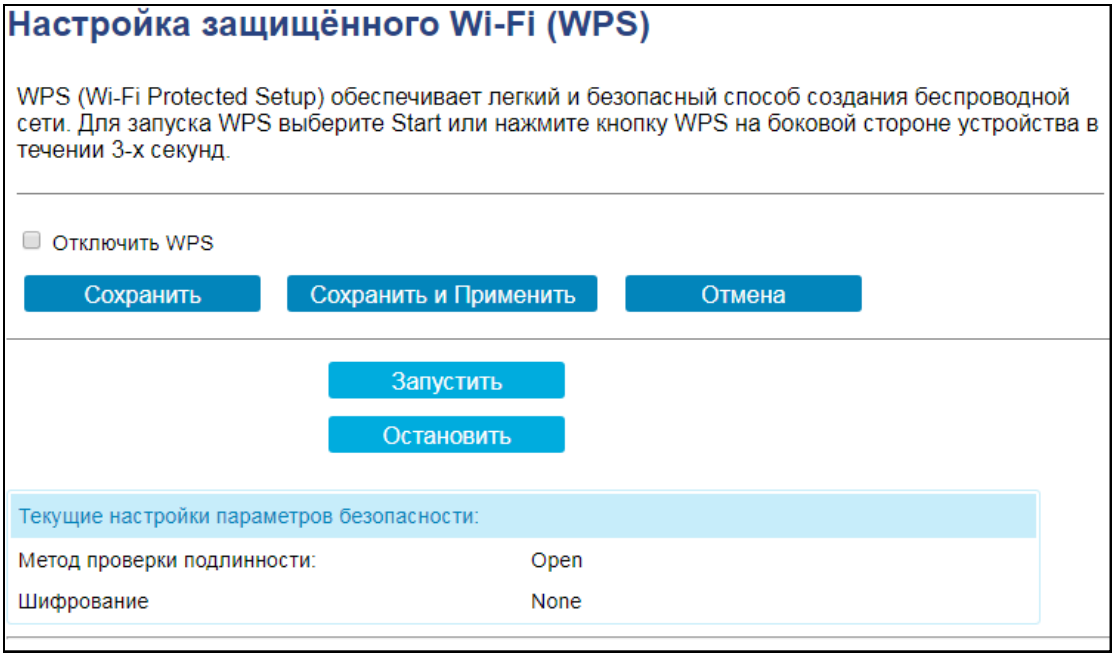
В подменю «Обзор сетей» можно запустить поиск других Wi-Fi сетей в заданном частотном диапазоне с целью определения минимально загруженного канала при тонкой настройке сети.



3.3.3.7 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;
- *Запустить* — 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* — принудительно прекращает процесс создания нового подключения по WPS. Также процесс прекращается автоматически если в течение двух минут не удалось создать соединения.

3.3.3.8 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.

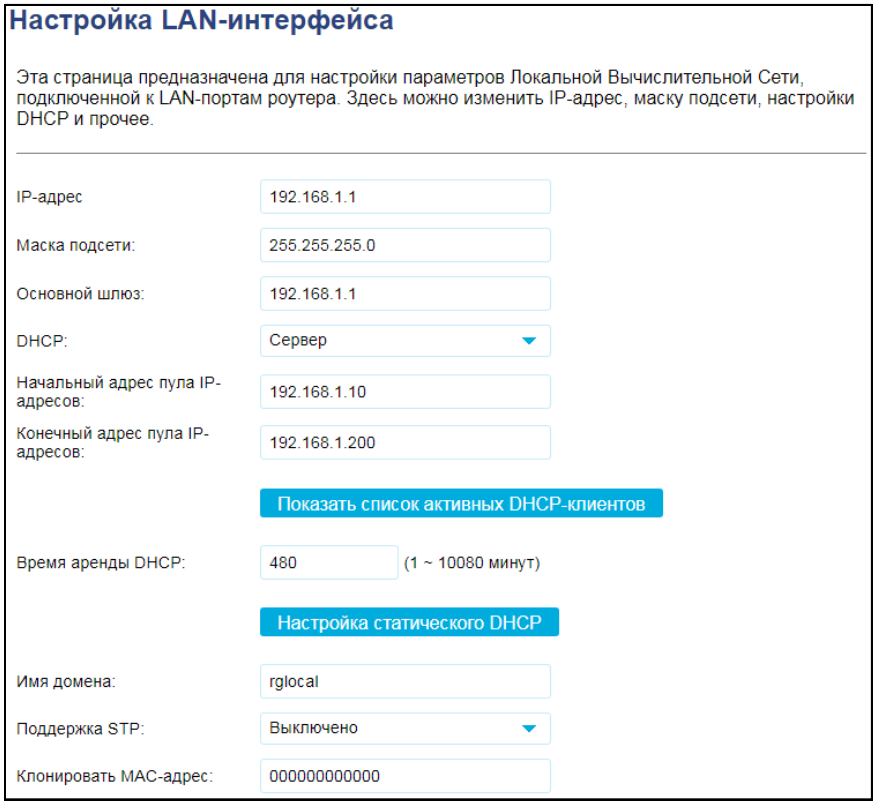
- *Включить работу по расписанию* — при выставленном флаге Wi-Fi сеть в выбранном диапазоне работает в соответствии с указанным расписанием.

3.3.4 Меню «TCP/IP»

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

3.3.4.1 Подменю «Настройка LAN»

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

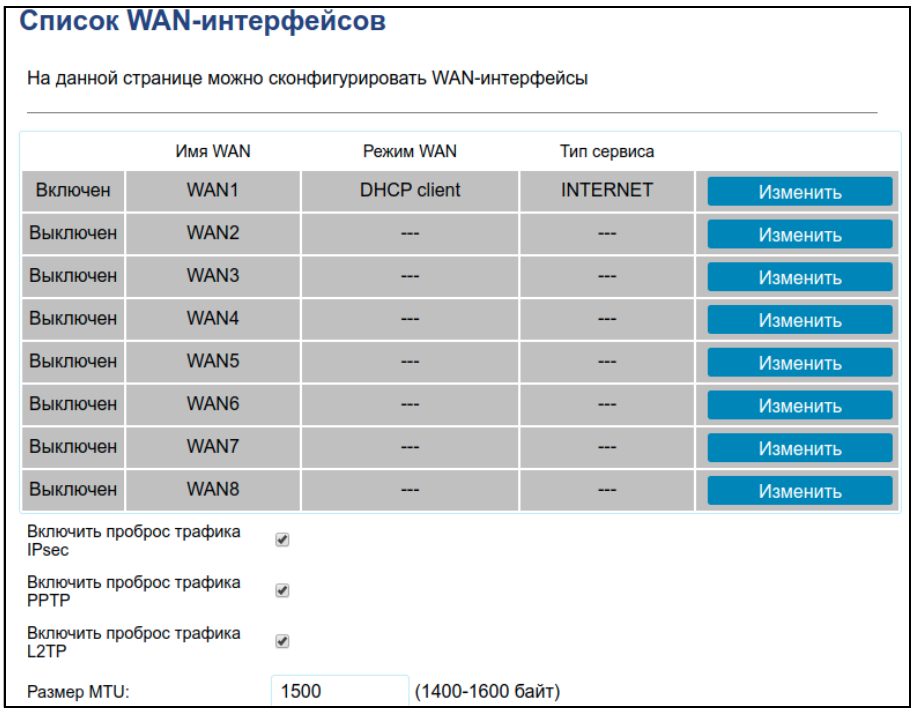


- *IP-адрес* — локальный IP-адрес устройства. Для подключенных клиентов это будет адрес основного шлюза. По умолчанию 192.168.1.1.
- *Маска подсети* — значение маски LAN-сети. По умолчанию 255.255.255.0.
- *Основной шлюз* — адрес шлюза, на который отправляется пакет, когда маршрут к сети назначения пакета неизвестен.
- *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 список активных DHCP-клиентов* — отобразить список подключенных к устройству клиентов.
- *Время аренды DHCP* — время аренды в минутах по истечению которого клиент должен либо освободить адрес, либо продлить на такой же промежуток.

- *Настройка статического DHCP* — позволяет задать статические IP-адреса подключенным клиентам.
- *Имя домена* — имя домена DHCP-сервера.
- *Поддержка STP* — протокол STP необходим для устранения петель в топологии произвольной сети Ethernet, в которой есть один или более сетевых мостов, связанных избыточными соединениями (препятствует образованию сетевых колец).
- *Клонировать MAC-адрес* — позволяет изменить MAC-адрес LAN-портов с заводского на сторонний.

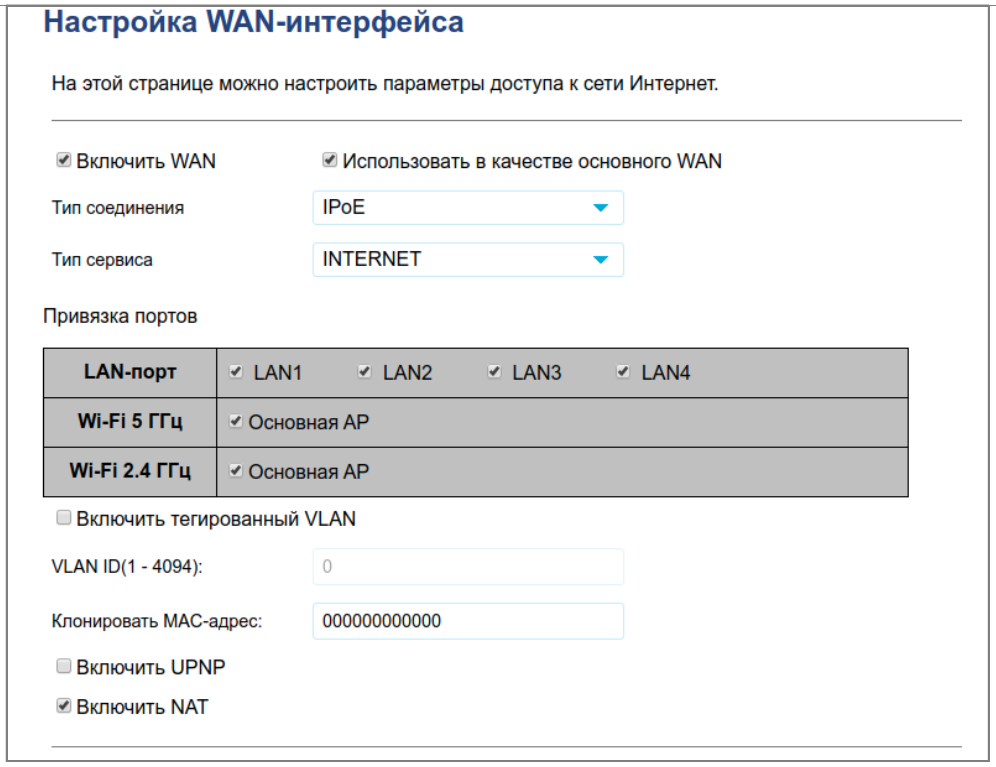
3.3.4.2 Подменю «Настройка WAN»

В подменю «Настройка WAN» можно сконфигурировать несколько WAN-интерфейсов.



Размер MTU — определяет размер кадров Ethernet передаваемых через WAN-порт.

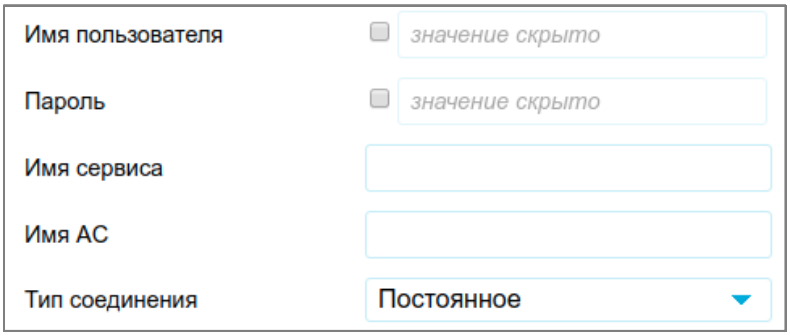
Для редактирования WAN-подключения необходимо нажать «Изменить».



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

  – *IPoE* — 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.

PPPoE

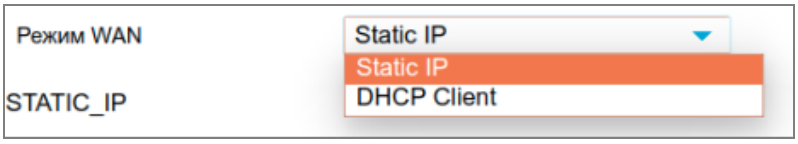


При выборе «PPPoE» для редактирования станут доступны следующие параметры:

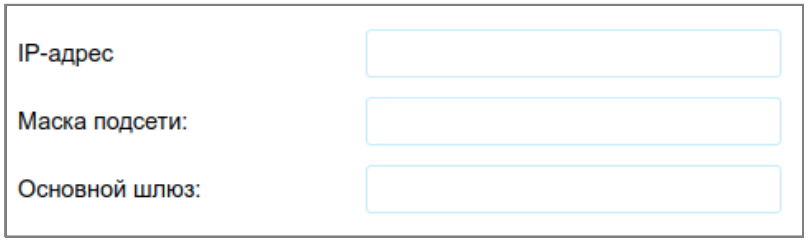
- *Имя пользователя* — имя пользователя для авторизации на PPPoE-сервере;
- *Пароль* — пароль для авторизации;
- *Service Name* — имя услуги — значение тэга Service Name в сообщении PADI (поле не обязательно для заполнения);
- *Тип соединения* — позволяет выбрать тип подключения PPPoE: постоянное, по требованию, вручную.

IPoE

При выборе IPoE соединения доступно несколько режимов работы:

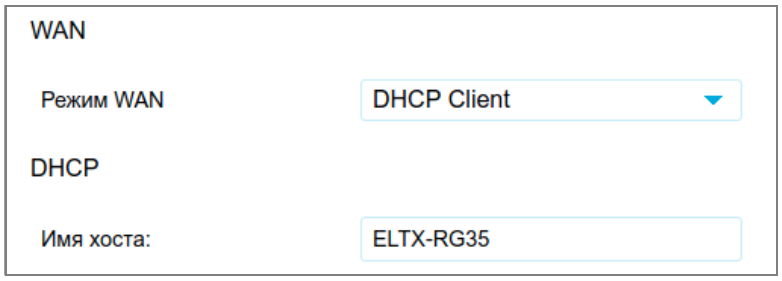


- *Static IP* — режим работы, при котором IP-адрес и все необходимые параметры на WAN-интерфейс назначаются статически. При выборе типа «Static IP» для редактирования станут доступны следующие параметры:



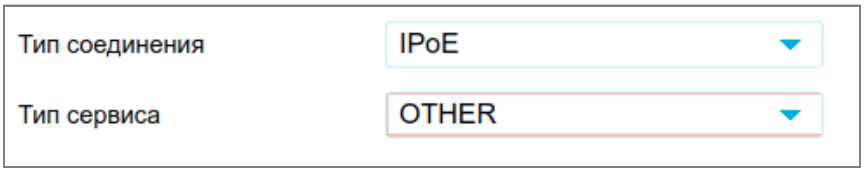
  – *IP-адрес* — установка IP-адреса WAN-интерфейса устройства в сети провайдера;
  – *Маска подсети* — маска внешней подсети;
  – *Основной шлюз* — адрес шлюза, на который отправляется пакет, если для него не найден маршрут в таблице маршрутизации.

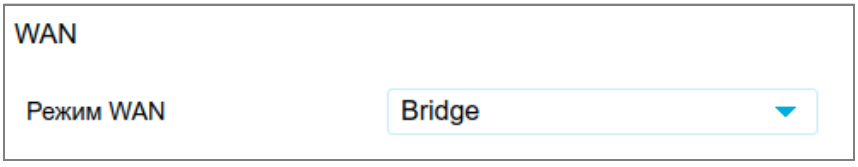
- *DHCP Client* — получение настроек роутером от DHCP-сервера.



  – *Имя хоста* — сетевое имя устройства.

- *Bridge* — подключение роутера в режиме «моста». (Для того, чтобы был доступен данный режим, необходимо выбрать «тип сервиса»- OTHER (см. тип сервиса ниже))





Общие настройки:

- Тип сервиса:
  - INTERNET — предоставляет доступ в интернет.
  - TR069 — запускает TR069-клиент на интерфейсе.
  - TR069_INTERNET — предоставляет доступ в интернет и запускает TR069-клиент на интерфейсе.
  - IPTV — конфигурирует IPoE-соединение со статическим IP-адресом 0.0.0.0 и IGMP Proxy для вещания потокового мультикаст-контента;
  - OTHER — позволяет выбрать режим WAN «Bridge».

- *Включить тегированный VLAN* — 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.

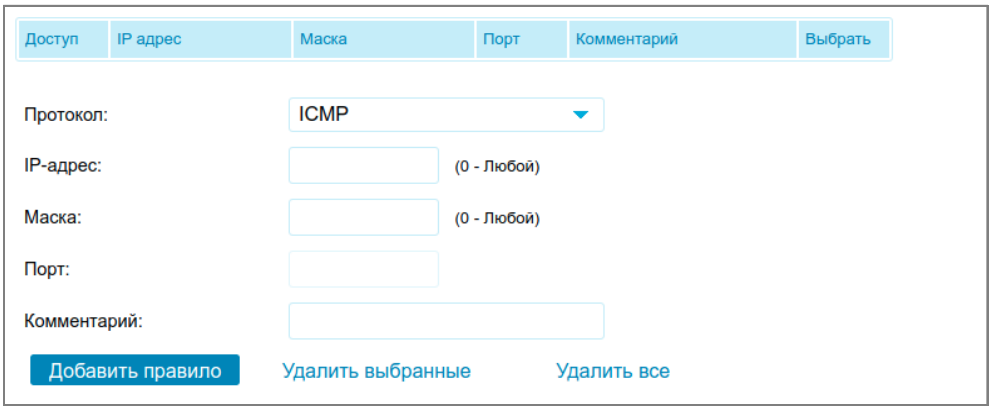
- *Клонировать MAC-адрес* — позволяет изменить MAC-адрес WAN-порта с заводского на сторонний, если со стороны провайдера реализована проверка MAC-адресов абонентских устройств.

- *Включить UPNP* — протокол UPnP используется приложениями 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 NAT* — включение трансляции сетевых адресов (отключение NAT возможно только на не основном WAN).

Удаленный доступ:

В данном пункте можно настроить удаленный доступ (WEB/TELNET) на устройство, а также разрешить PING запросы на WAN интерфейс (настройка правил из данного пункта работает только для IPv4).



- *Протокол:*
  - ICMP — при настроенном правиле устройство будет отвечать на ICMP запросы, приходящие на WAN-интерфейс.
  - HTTP — открывает доступ к web-интерфейсу устройства из WAN сети по протоколу HTTP
  - HTTPS — открывает доступ к web-интерфейсу устройства из WAN сети по протоколу HTTPS
  - TELNET — открывает доступ к устройству из WAN сети по протоколу TELNET

- *IP-адрес* — разрешает входящие запросы только для определенного адреса или сети.

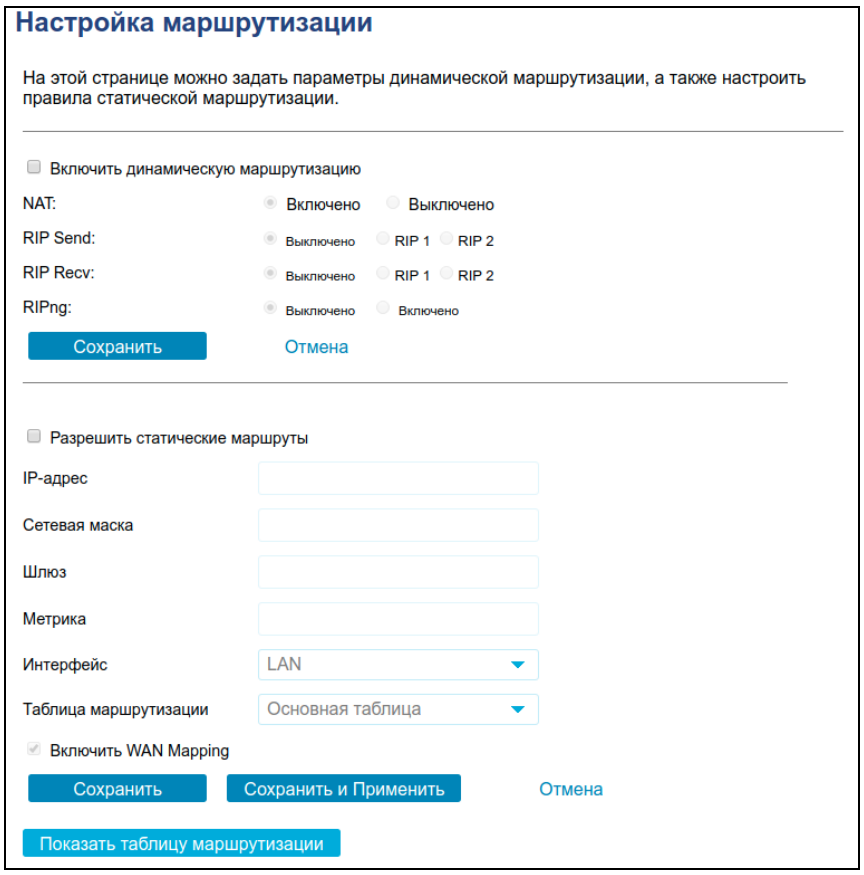
- *Маска* — маска IP-адреса сети
- *Порт* — изменение порта доступа к web-интерфейсу или TELNET из WAN сети. Для протокола ICMP поле не используется.

Для применения правила необходимо нажать «Добавить правило», а затем «Сохранить и Применить».

- *Настройка DNS* — адреса используемых DNS-серверов можно как получить автоматически по DHCP, так и указать вручную.
- *Включить IGMP Proxy* — при выставленном флаге устройство обрабатывает запросы IGMP, которые необходимы для работы IPTV.

3.3.4.3 Подменю «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;
- *RIP Send/RIP Recv (Передача/Прием)* — выбор используемого протокола динамической маршрутизации RIP1 или RIP2 для соответствующего направления;
- *RIPng* — при выставленном флаге включается протокол динамической маршрутизации для сети IPv6.

Статическая маршрутизация

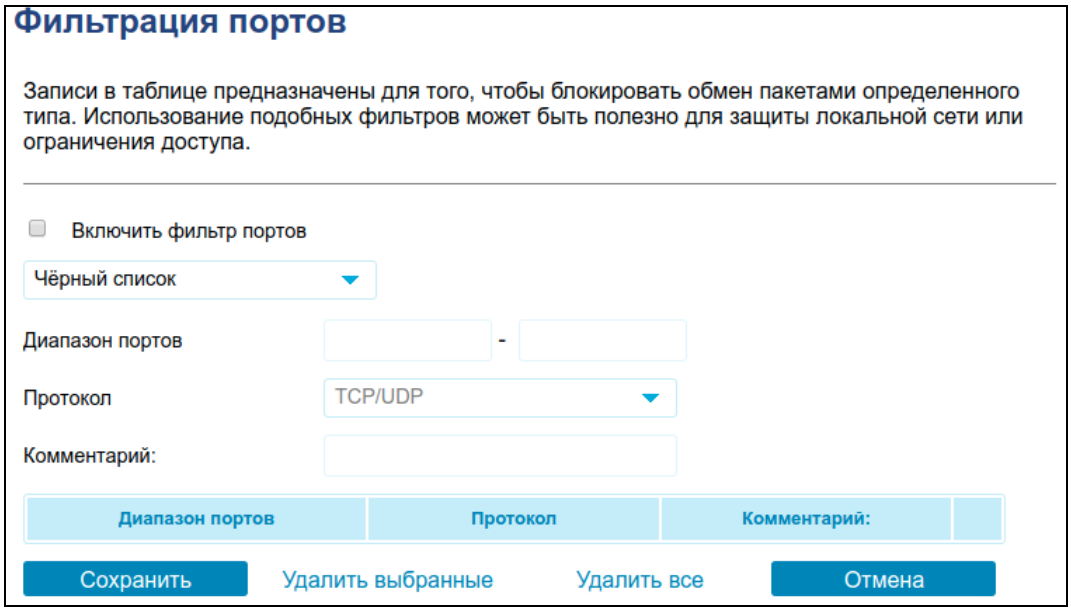
- *Разрешить статические маршруты* — при выставленном флаге статические маршруты будут добавлены в таблицу маршрутизации;
- *IP-адрес* — адрес сети назначения или хоста, до которой указывается маршрут;
- *Сетевая маска* — маска подсети. Для хоста маска подсети устанавливается в значение 255.255.255.255, для подсети – в зависимости от её размера;
- *Шлюз* —IP-адрес шлюза, через который осуществляется выход на «IP-адрес»;
- *Метрика* — числовой показатель, задающий предпочтительность маршрута. Чем меньше число, тем более предпочтителен маршрут;
- *Интерфейс* — тип выходного интерфейса устройства (LAN или WAN) через который доступна целевая сеть;
- *Таблица маршрутизации* — открывает в новом окне текущую таблицу маршрутизации устройства.

3.3.5 Меню «Firewall»

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

3.3.5.1 Подменю «Фильтрация по портам»

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.

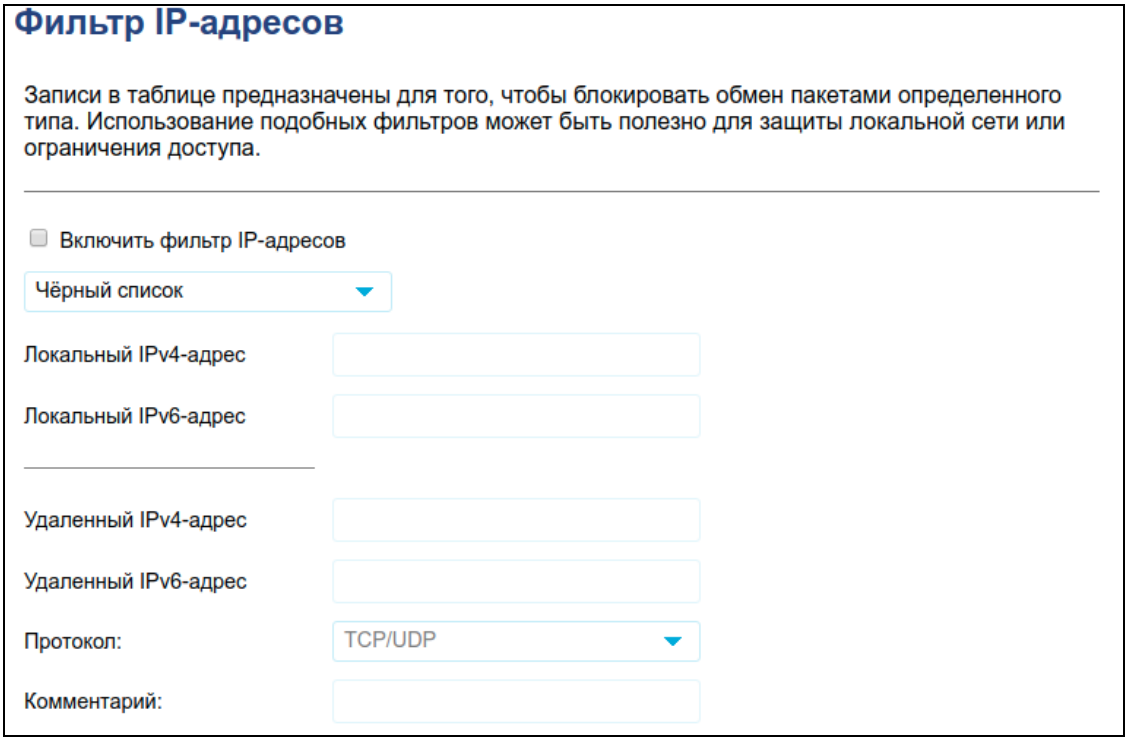


- *Включить фильтр портов* — при выставленном флаге фильтр включен. При включении можно выбрать тип списка:
  - *Чёрный список* — доступ через порты, внесенные в список, будет запрещен.
  - *Белый список* — доступ будет разрешен только через порты, внесенные в список, и запрещен по всем остальным.
- *Диапазон портов* — введите номера портов, трафик с которых Вы хотите запретить.

- *Протокол* — выбор типа протокола трафика TCP, UDP или оба.
- *Комментарий*—поле для оставления заметок для фильтров.

3.3.5.2 Подменю «Фильтрация по IP»

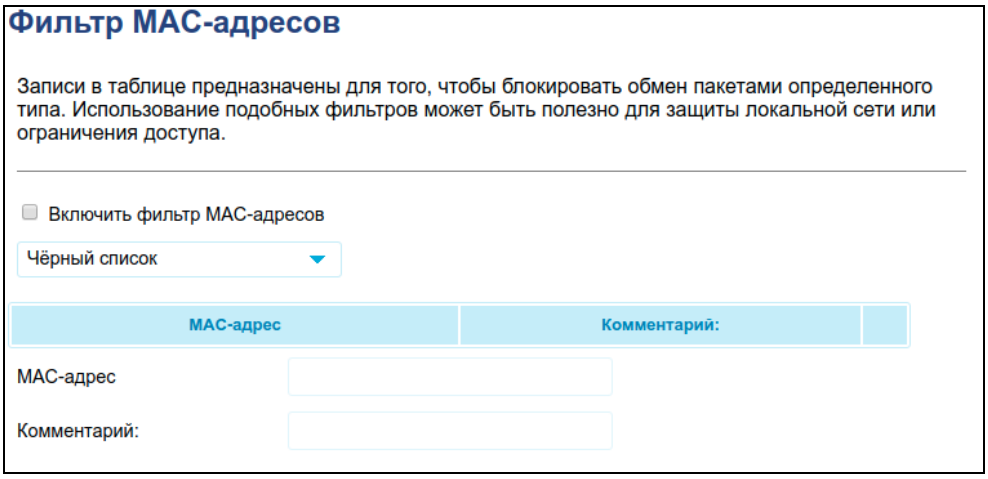
Функция «Фильтрация IP» позволяет ограничить доступ для определенных устройств в WAN-сеть (Интернет), при этом ресурсы внутри LAN-сети остаются доступны.



- *Включить фильтр IP-адресов* — при выставленном флаге фильтр включен.
- *Локальный IP-адрес* — поле ввода IP-адреса источника.
- *Удаленный IP-адрес* — поле ввода IP-адреса назначения.
- *Протокол* — выбор типа протокола трафика TCP, UDP или оба.
- *Комментарий* — поле для оставления заметок для фильтров.

3.3.5.3 Подменю «Фильтрация по MAC»

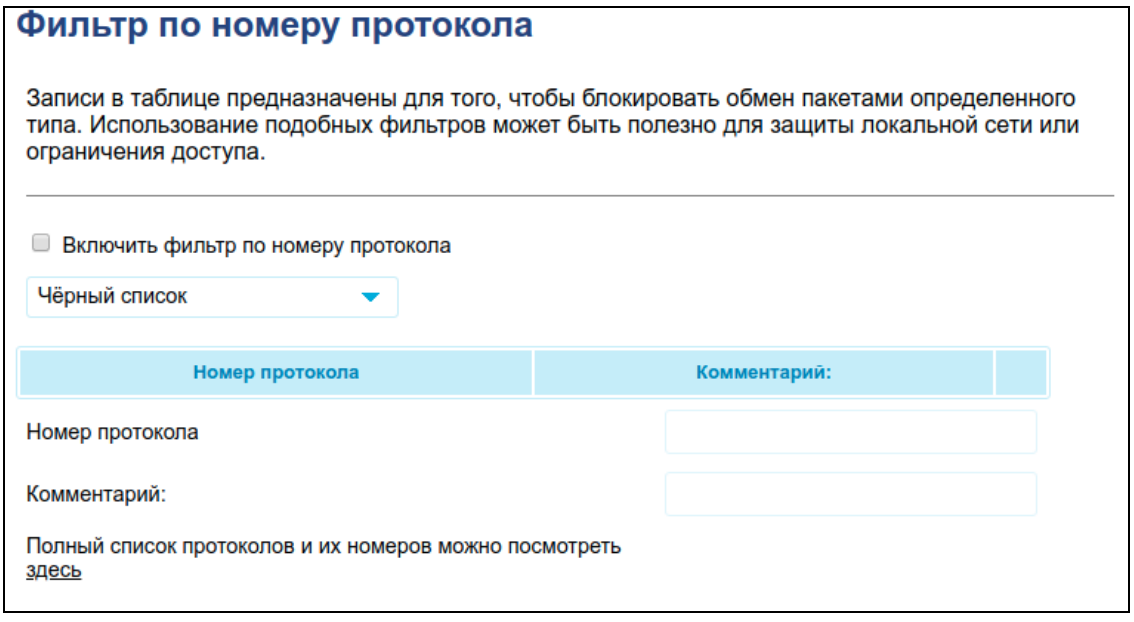
В подменю «Фильтрация MAC» выполняется настройка фильтрации доступа по MAC-адресу клиента, подключенного в один из LAN-портов.



- *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.
- *Комментарий* — поле для оставления заметок для фильтров.

3.3.5.4 Подменю «Фильтрация по номеру протокола»

В подменю «Фильтрация по номеру протокола» выполняется настройка фильтрации доступа по номеру протокола.



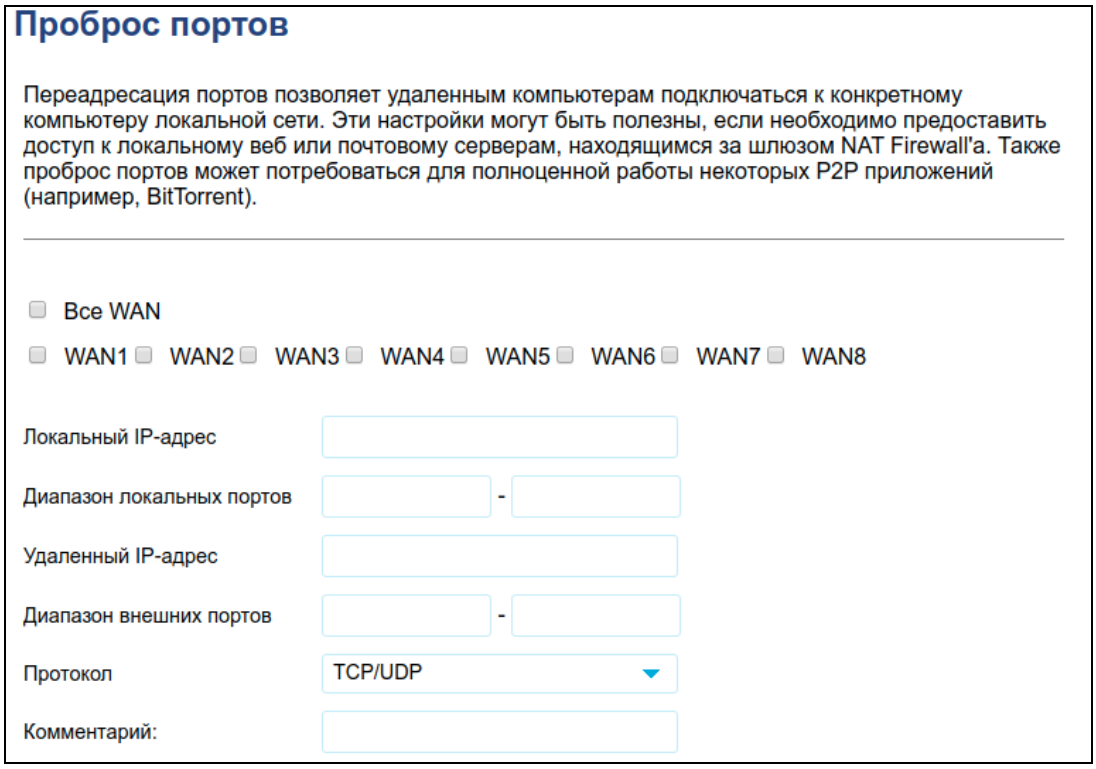
- *Включить фильтр по номеру протокола* — при выставленном флаге фильтр включен. При включении нужно выбрать тип фильтра:

- *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.

- *Номер протокола* — вводится номер протокола, которому нужно ограничить доступ.
- *Комментарий* — поле для оставления заметок для фильтров.

3.3.5.5 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.

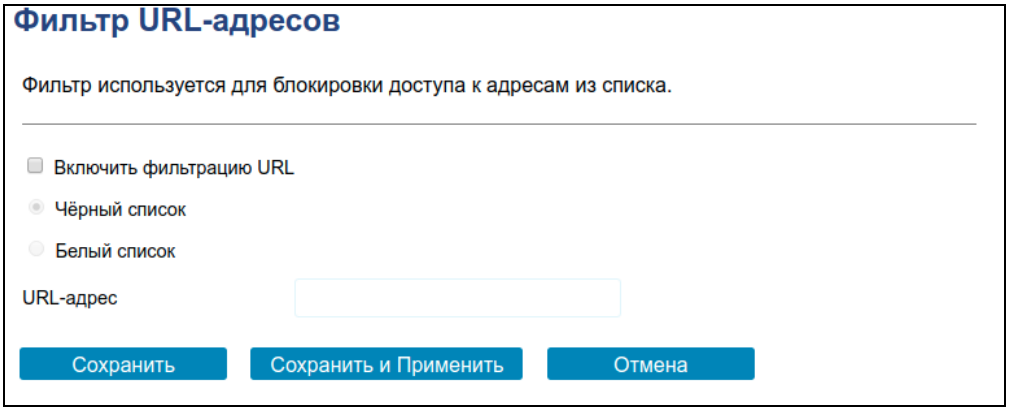


Выберите необходимые WAN-подключения для индивидуального создания правила проброса портов, установив рядом флажок или выберите «Все WAN».

- *Локальный IP-адрес* — поле ввода IP-адреса источника.
- *Диапазон локальных портов* — выбор диапазона пробрасываемых портов со стороны LAN.
- *Удаленный IP-адрес* — поле ввода IP-адреса назначения.
- *Диапазон внешних портов* — выбор диапазона портов со стороны WAN-интерфейса, он может совпадать или отличаться от номера порта со стороны LAN.
- *Протокол* — выбор типа протокола трафика TCP, UDP или оба.
- *Комментарий* — поле для оставления заметок для фильтров.

3.3.5.6 Подменю «Фильтрация URL»

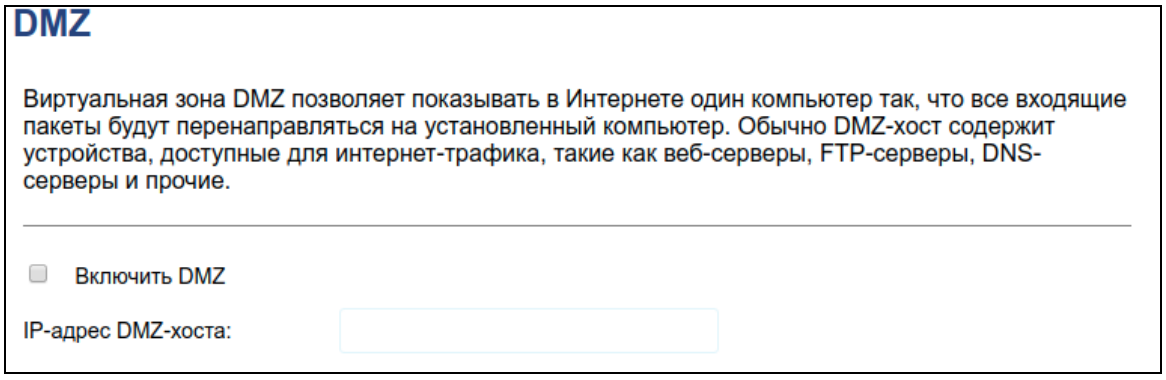
Фильтр URL позволяет ограничить доступ к ресурсам в Интернете по их доменным адресам (URL).



- *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.

3.3.5.7 Подменю «DMZ»

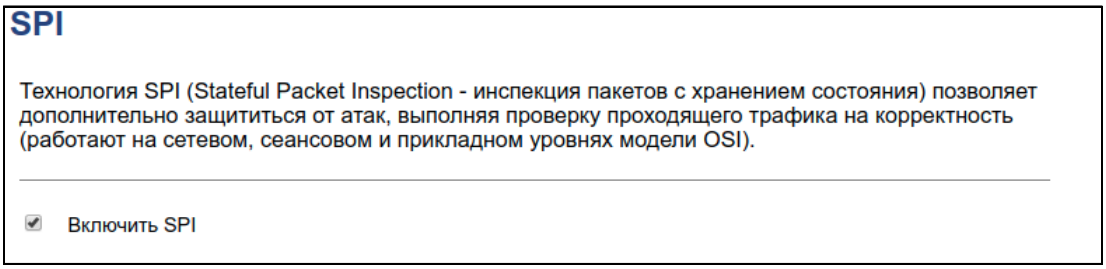
Демилитаризованная зона (DMZ) позволяет выделить одного клиента в LAN таким образом, чтобы все входящие пакеты перенаправлялись на него. Обычно DMZ-хост содержит сервисы типа web-сервер, FTP-сервер, DNS-сервер и прочие.



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

3.3.5.8 Подменю «SPI»

Описание технологии приведено на рисунке ниже.



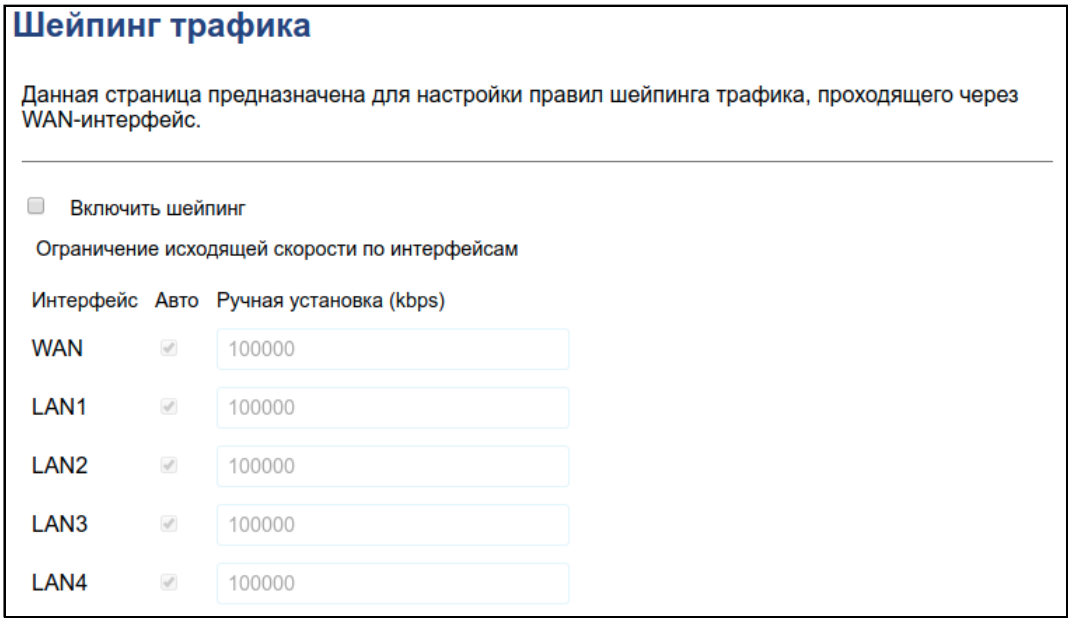
- *Включить SPI* – при выставленном флаге SPI включен.

3.3.6 Меню «Quality of Service (QoS)»[3]

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

3.3.6.1 Подменю «Шейпинг трафика»

Шейпинг трафика необходим для ограничения пропускной способности на WAN/LAN.

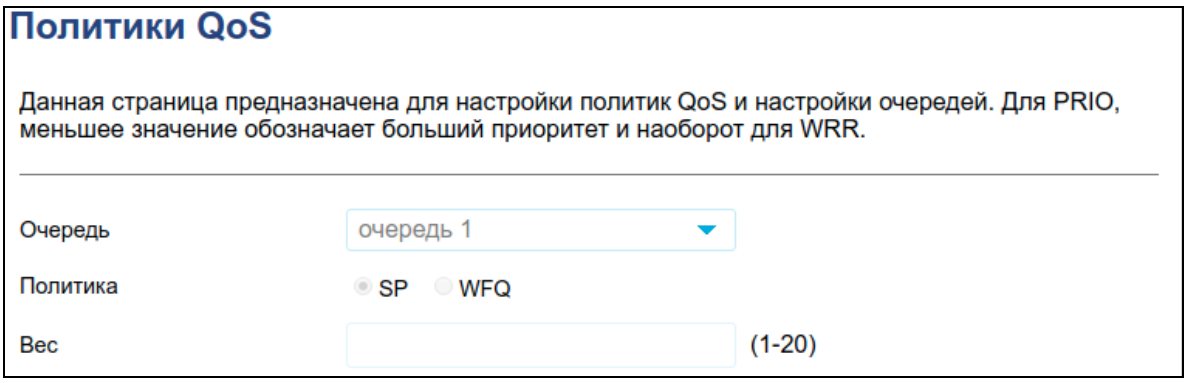


Для активации шейпинга установите флажок «Включить шейпинг», а затем статически или автоматически ограничьте полосу пропускания, используя поля и флажки, приведенные на рисунке выше.

[3] *Меню доступно только под учетной записью Admin*

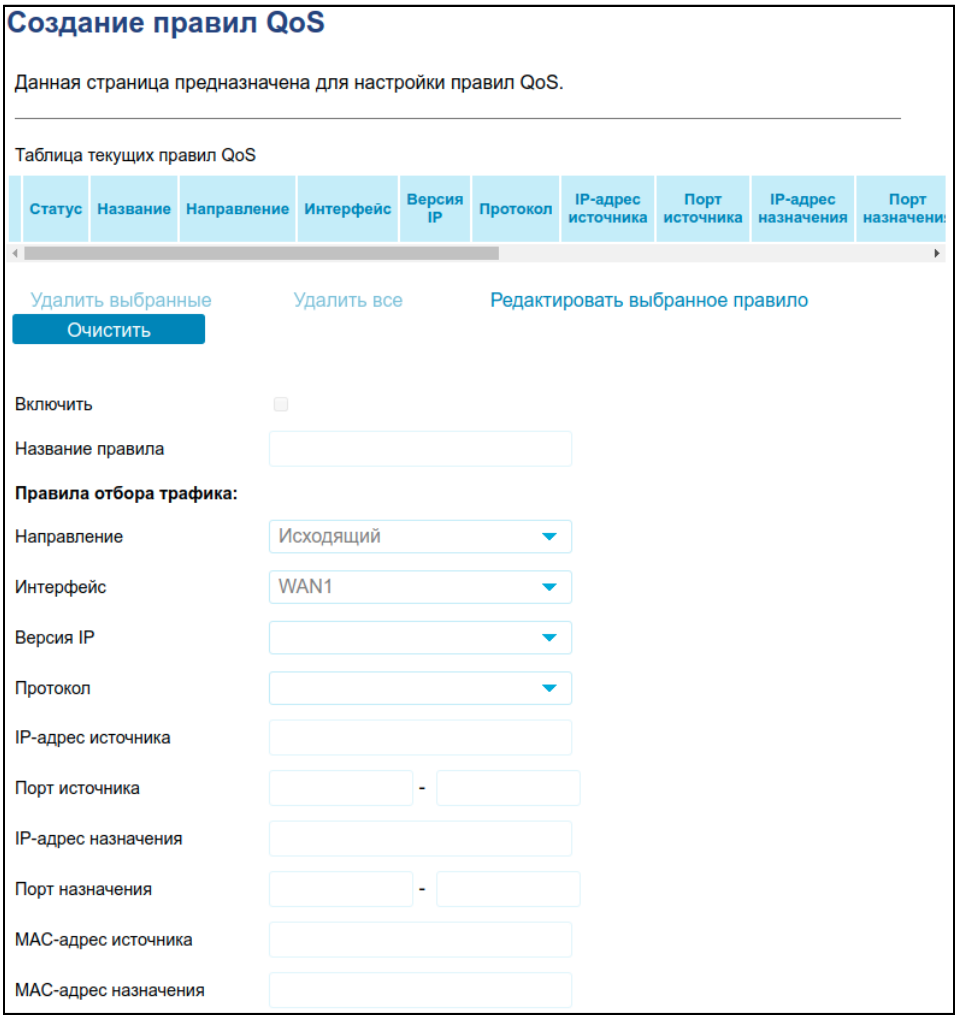
3.3.6.2 Подменю «Политики QoS»

Описание подменю приведено на рисунке ниже.



3.3.6.3 Подменю «Создание правил QoS»

Данная страница предназначена для настройки правил QoS.



- *Включить* — при выставленном флаге функция QoS включена;
- *Название правила* — понятное имя правила.

Правило отбора трафика:

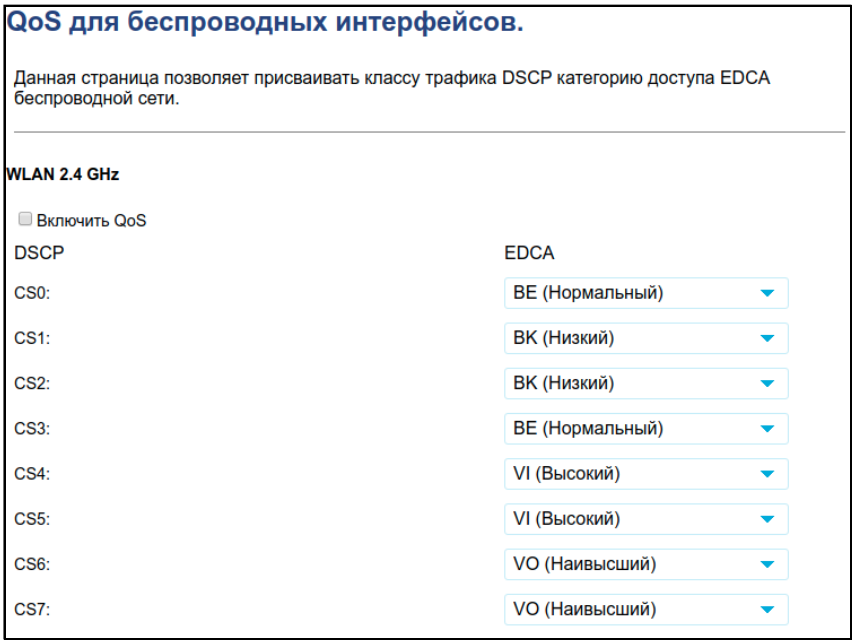
- *Направление* — выбор направления трафика для приоритизации;
- *Интерфейс* — выбор WAN-интерфейса из WAN-таблицы (WAN1-8);
- *Версия IP* — выбор версии IP-протокола;
- *Протокол* — выбор протокола, для которого будет работать правило;
- *IP-адрес источника* — задается при выбранном типе адреса IP клиента;
- *Порт источника* — задается порт TCP/UDP со стороны LAN, для которого будет выполняться правило;
- *IP-адрес назначения* — задается IP-адрес устройства со стороны WAN для данного правила;
- *Порт назначения* — задается порт TCP/UDP со стороны WAN;
- *MAC-адрес источника* — поле ввода MAC-адреса источника для данного правила;
- *MAC-адрес назначения* — поле ввода MAC-адреса назначения для данного правила;
- *Физический порт* — адрес физического интерфейса Ethernet;
- *DSCP* —метка заголовка QoS, по которой будет выполняться правило;
- VLAN ID — поле ввода идентификатора VLAN (1-4095);
- Hostname — поле ввода имени хоста.

Действия над трафиком:

- *Очередь* —метка приоритета для правила;
- *Смена метки DSCP (Remark DSCP)* — замена метки в заголовке QoS при прохождении LAN-WAN и наоборот;
- *Смена метки 802.1p (Remark 802.1p)* — замена метки приоритета в заголовке при прохождении LAN-WAN и наоборот;
- *Режим*:
  - Гарантировать минимальную скорость;
  - Ограничивать максимальную скорость.
- *Скорость шейпинга (входящего/исходящего соединения)* — введите требуемое значение в зависимости от выбранного режима.

3.3.6.4 Подменю «Wi-Fi QoS»

Данная страница позволяет включить и настроить приоритизацию трафика Wi-Fi сети, путем присваивания классу трафика DSCP категории доступа EDCA беспроводной сети.



- *Включить QoS* — при установленном флаге приоритизация трафика точки доступа будет включена.
- *DSCP* — поле в IP-пакете, позволяющее назначить сетевому трафику различные уровни обслуживания. Наивысший приоритет присваивается для CS7, наименьший для CS0.
- *EDCA* (Enhanced Distributed Channel Access) позволяет создать 4 очереди для приоритизации трафика — BE (Best Effort), BK (Background), VI (Video), VO (Voice).

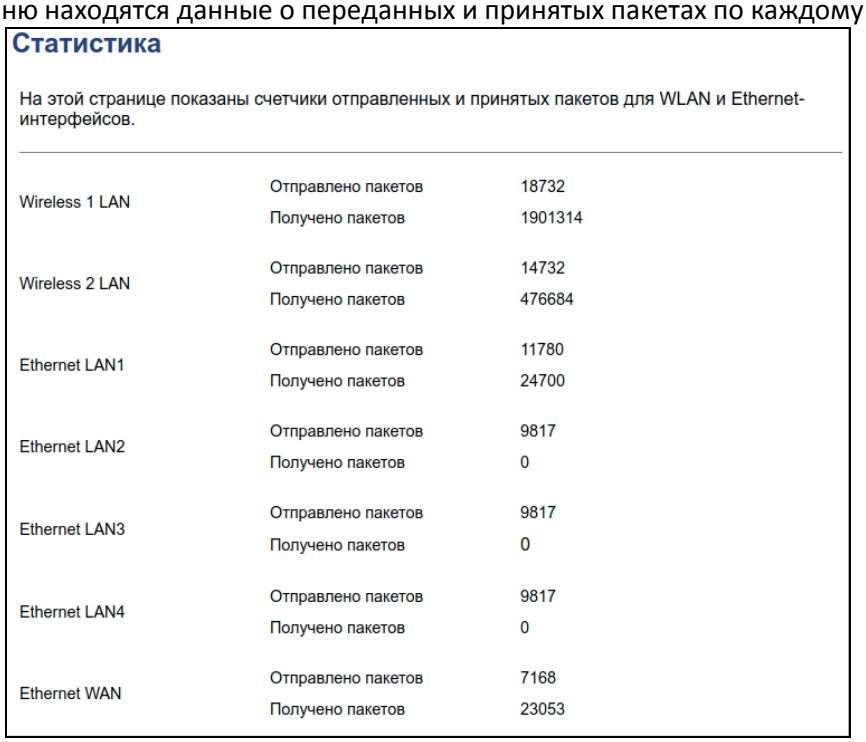
Настройка приоритизации выполняется путем сопоставления CS (Class Selector) и EDCA.

3.3.7 Меню «Администрирование»

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

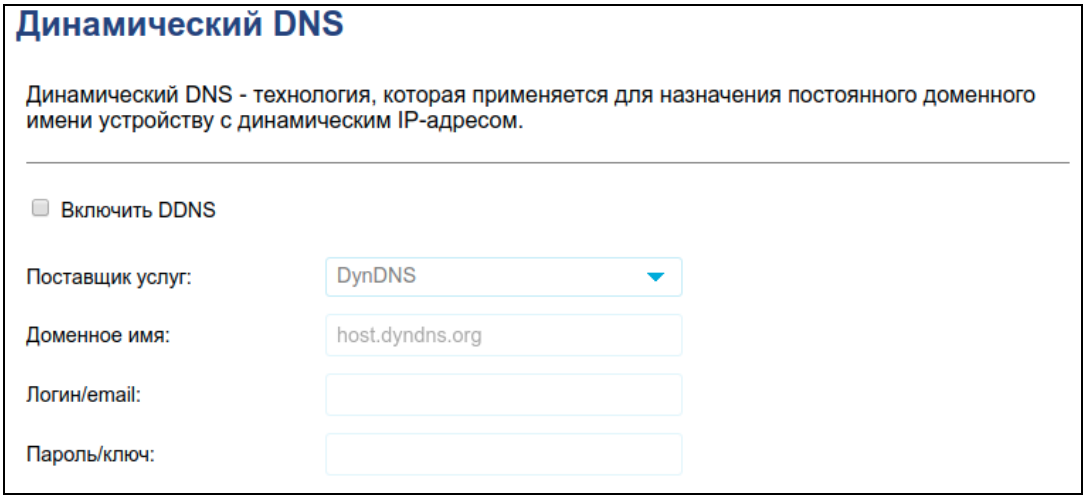
3.3.7.1 Подменю «Статистика»

В этом подменю находятся данные о переданных и принятых пакетах по каждому интерфейсу.



3.3.7.2 Подменю «DDNS»

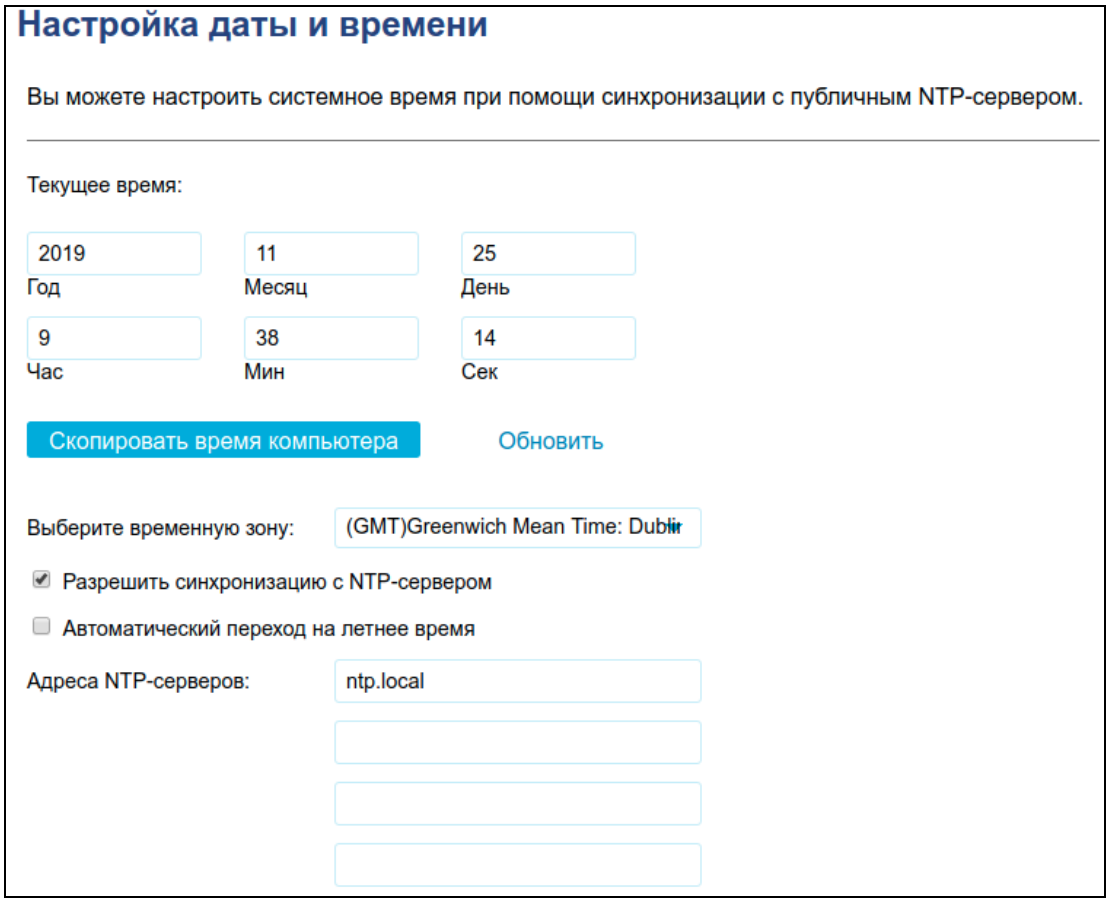
В этом подменю можно активировать услугу предоставления постоянного доменного имени устройству с динамическим IP-адресом.



- *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;

3.3.7.3 Подменю «Настройка даты и времени»

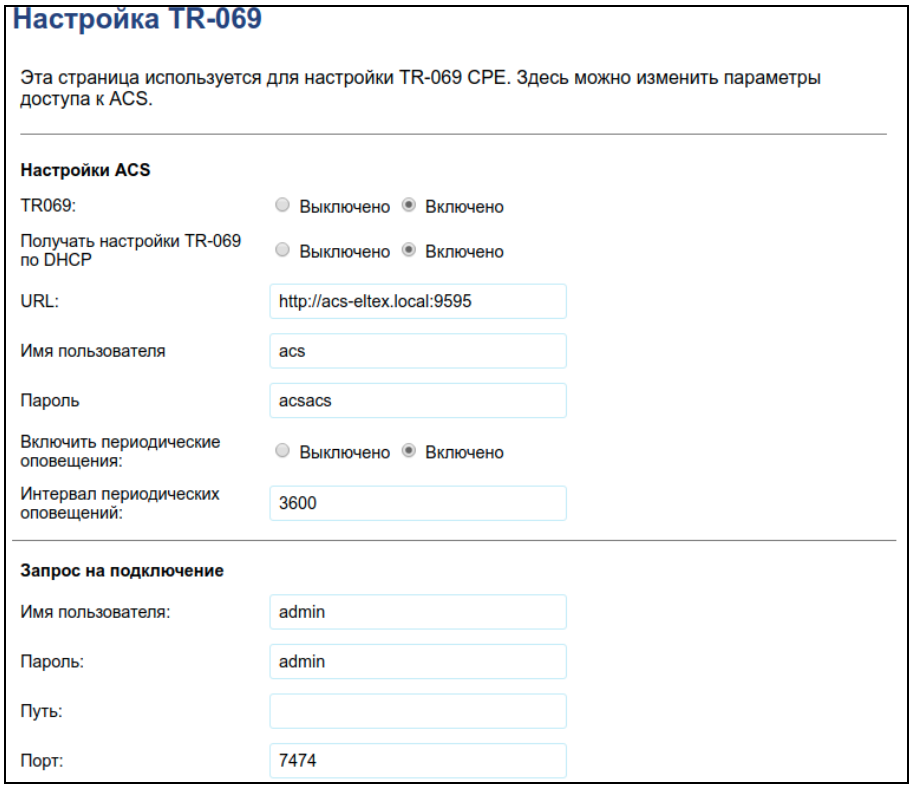
В этом подменю настраивается дата и системное время устройства при помощи синхронизации с NTP-сервером.



- *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.
- *Автоматический переход на летнее время* —при установленном флаге, переход на летнее время выполняется автоматически.
- *Адрес NTP-сервера* — можно выбрать сервер из предложенного списка или ввести его вручную.

3.3.7.4 Подменю «Настройка TR-069»[4]

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.
- *Получать настройки TR-069 по DHCP* — при включении, TR-069 клиент будет использовать параметры, полученные в 43 опции DHCP (поля ниже при этом останутся неизменными, но будут игнорироваться клиентом)
- *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.
- *Имя пользователя, Пароль* — имя пользователя и пароль для доступа клиента к ACS-серверу.
- *Включить периодические оповещения* — 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.

Запрос на подключение:

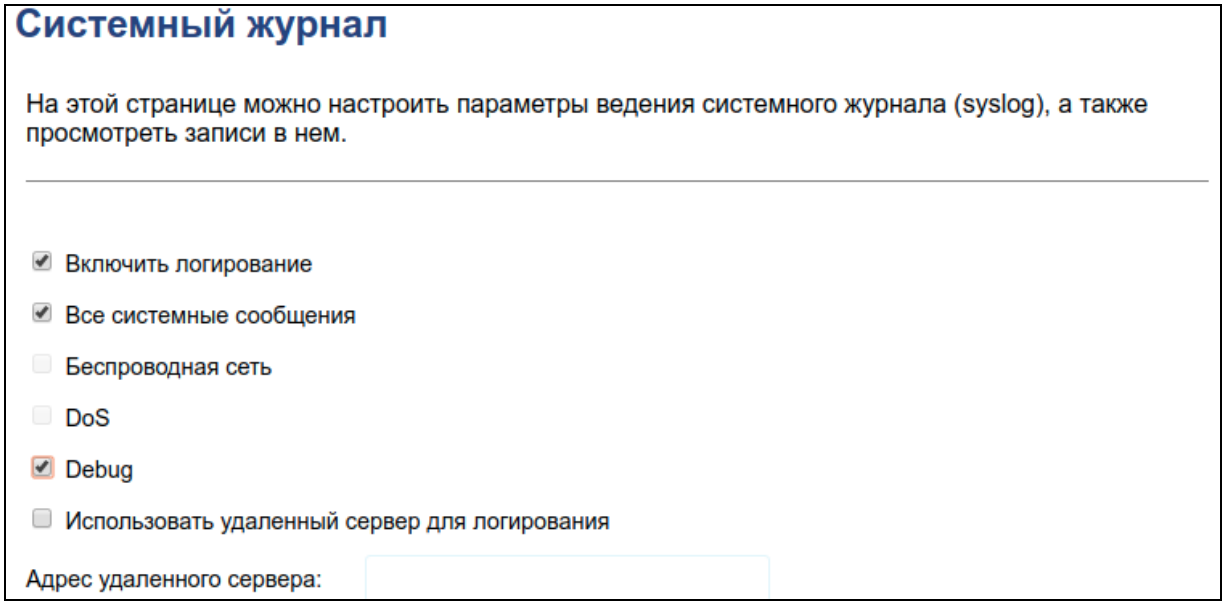
- *Имя пользователя, Пароль* — имя пользователя и пароль для доступа ACS-сервера к клиенту TR-069;
- *Путь* — адрес инициализации для запроса;

[4] *Подменю доступно только под учетной записью Admin*

- *Порт* — используемый порт для подключения.

3.3.7.5 Подменю «Системный журнал»

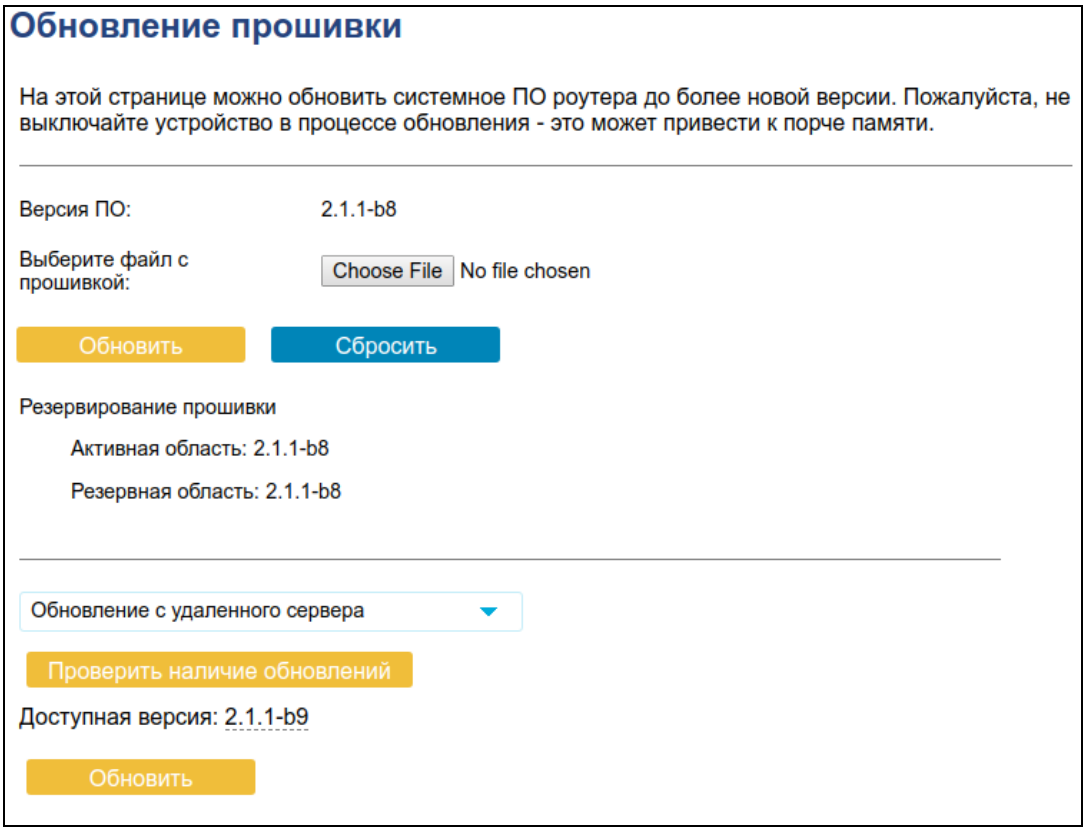
Подменю «Системный журнал» предназначено для настройки вывода разного рода отладочных сообщений системы в целях обнаружения проблем в работе устройства.



- *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».

3.3.7.6 Подменю «Обновление прошивки»

Подменю «Обновление ПО» предназначено для обновления управляющей микропрограммы устройства.



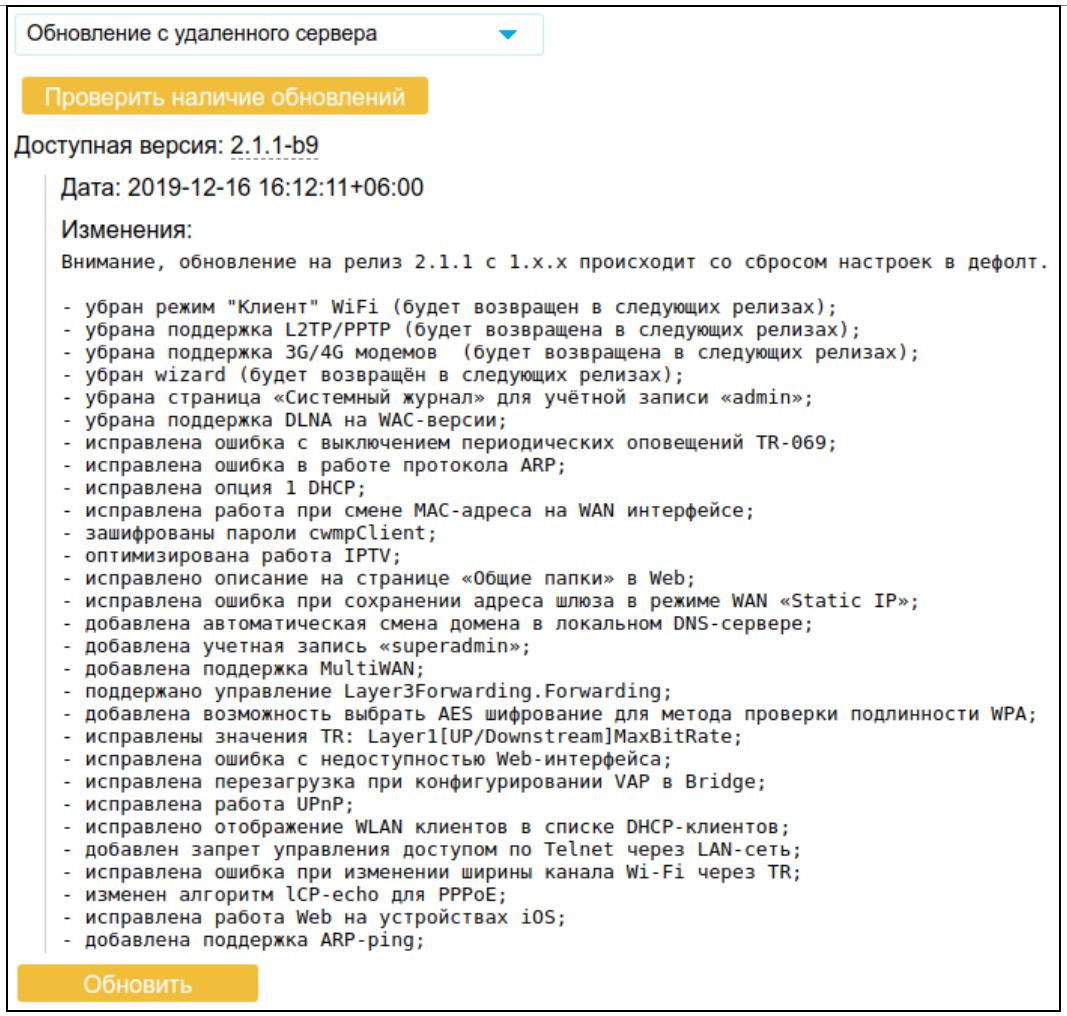
- *Версия ПО* — версия программного обеспечения, установленного на устройстве.
- *Выберите файл с прошивкой* — при наличии локального файла с прошивкой можно обновить ПО, указав путь к этому файлу и нажав кнопку «Обновить».

Когда основная прошивка повреждена, автоматически загружается резервная.

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.

Для обновления с использованием удаленного сервера, в выпадающем списке выберите «Обновление с удаленного сервера», затем нажмите «Проверить наличие обновлений». В случае, если имеются доступные обновления, будет отображено сообщение с доступной версией и кнопкой «Обновить». Для просмотра списка изменений, нажмите на подчеркнутое наименование версии программного обеспечения.



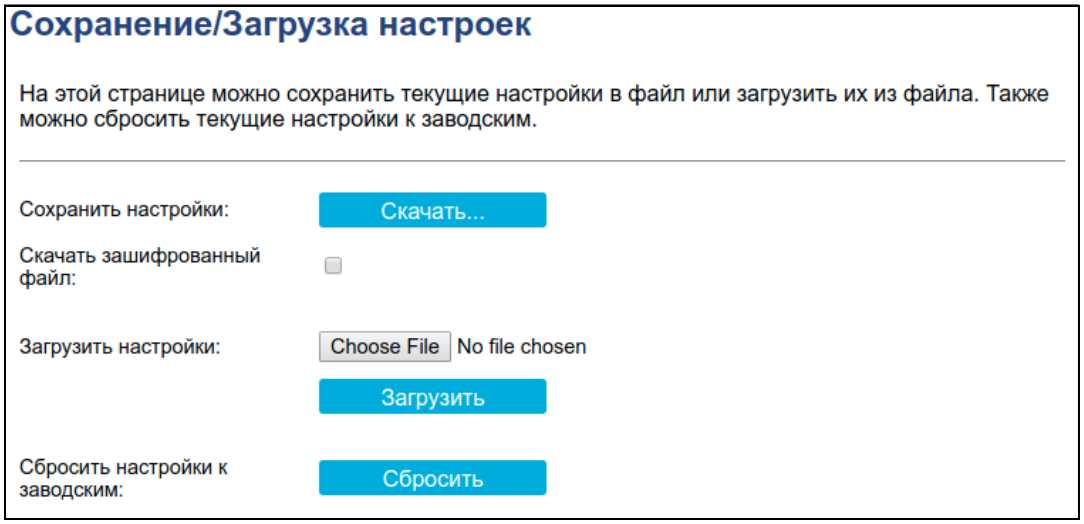
Для запуска процесса обновления программного обеспечения, нажмите кнопку «Обновить».

Для работы функции проверки обновления необходимо наличие выхода в Интернет.

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

3.3.7.7 Подменю «Сохранение/Загрузка настроек»

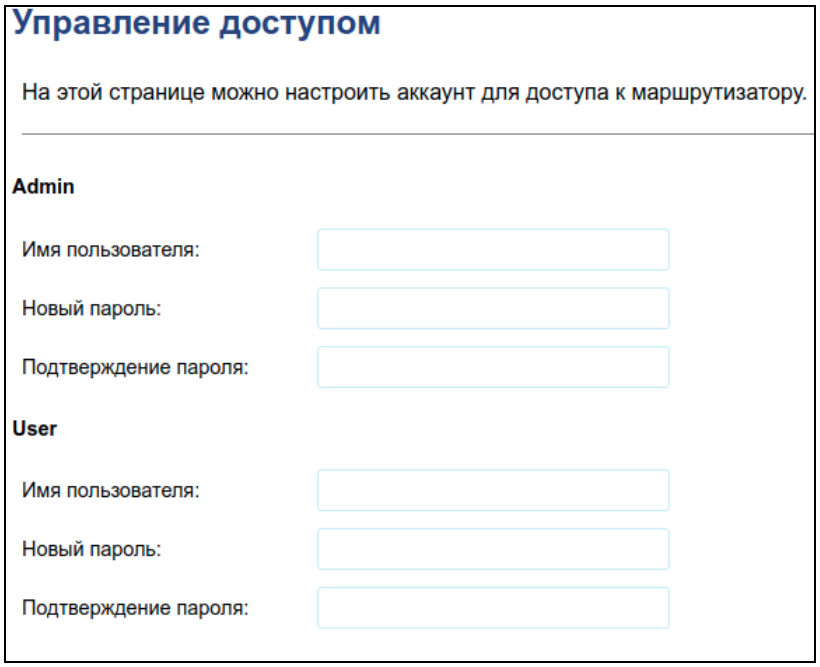
В подменю *«Сохранение/Загрузка настроек»* выполняется сохранение и обновление текущей конфигурации.



- *Сохранить настройки* — для сохранения текущей конфигурации устройства на локальный компьютер нажмите кнопку «Сохранить…».
- *Скачать зашифрованный файл* — при установленном флаге будет скачиваться зашифрованный файл.
- *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».

3.3.7.8 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.
- *Новый пароль* — поле для ввода нового пароля к устройству.
- *Подтверждение пароля* — поле для повторного ввода нового пароля с целью его подтверждения.

По умолчанию для Admin используются: superadmin/password,
для User: admin/password.

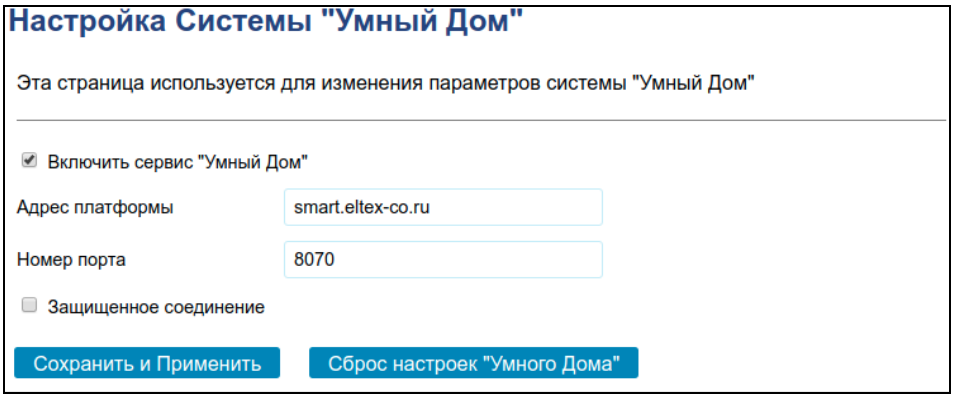
Изменение данных учетной записи Admin под учетной записью User недоступно.

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.

3.3.7.9 Подменю «Умный дом»[5]

В данном подменю выполняется настройка контроллера умного дома.



- *Включить сервис «Умный дом»* — при выставленном флаге функция контроллера «умного дома» включена;
- *Адрес платформы* — адрес сервера Eltex Smart Control (Eltex SC). Адрес необходимо вводить в формате <address>;
- *Номер порта* — порт для связи с платформой умного дома «Eltex Smart Control», по умолчанию порт 8070;
- *Защищенное соединение* — при выставленном флаге используется протокол шифрования SSL. При использовании защищенного соединения в поле «Номер порта:» укажите порт 8072;
- *Сохранить и Применить* — для сохранения внесенных изменений нажмите на кнопку;
- *Сброс настроек «Умного дома»* —перезапуск контроллера и удаление всех подключенных по протоколу Z-Wave устройств.

Альтернативная настройка «Умного дома» через telnet

1. Включите питание устройства и подключите компьютер с помощью Ethernet-кабеля к WAN-порту маршрутизатора.
2. Откройте доступ к устройству по Telnet, для этого:
   2.1. Перейдите в меню «TCP/IP»;
   2.2. Откройте вкладку «Настройка WAN»;
   2.3. Рядом с WAN1 нажмите «Изменить»;
   2.4. В выпадающем списке «Протокол» выберите «TELNET»;
   2.5. В поле «Порт» введите порт, по которому будет осуществляться доступ к устройству;
   2.6. Нажмите кнопку «Добавить правило»;
   2.7. Нажмите кнопку «Сохранить и Применить»;
3. После загрузки устройства установите telnet-соединение между компьютером и устройством, используя WAN IP-адрес устройства, логин «superadmin» и пароль «password».
4. Для просмотра текущих параметров соединения с платформой выполните команду:

   ```
   flash all | grep ZWAY
   ```

5. Настройте параметры соединения с платформой:

[5] Работа с системой «Умный дом» доступна только для RG-35-WZ. Система умный дом присутствует только в роутере RG-35-WZ. Подменю управления умным домом доступно только под учетной записью superadmin.

```
flash set ZWAY_REGISTERED [1 или 0] – установка соединения с платформой: 1–вкл, 0–выкл;
flash set ZWAY_CLOUD_HOST [адрес платформы] – настройка адреса платформы;
flash set ZWAY_CLOUD_PORT [порт] – установка номера порта платформы, по  умолчанию 8070;
flash set ZWAY_UNSECURE [0 или 1] – включить или выключить шифрование трафика при
соединении с платформой.
```

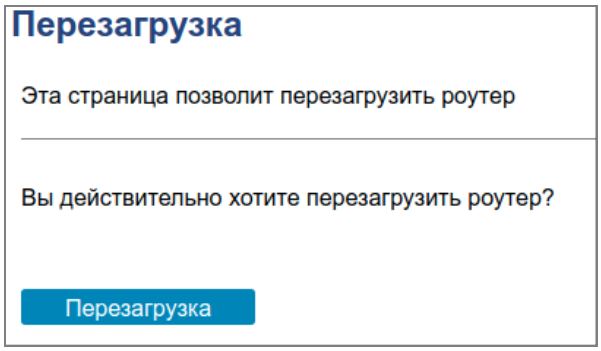
6. Перезагрузите устройство по питанию. После перезагрузки новые параметры вступят в силу и устройство будет готово к монтажу на объекте.

Пример настроек:

```
flash set ZWAY_REGISTERED 1
flash set ZWAY_CLOUD_HOST smart.eltex-co.ru
flash set ZWAY_CLOUD_PORT 8070
flash set ZWAY_UNSECURE 0
```

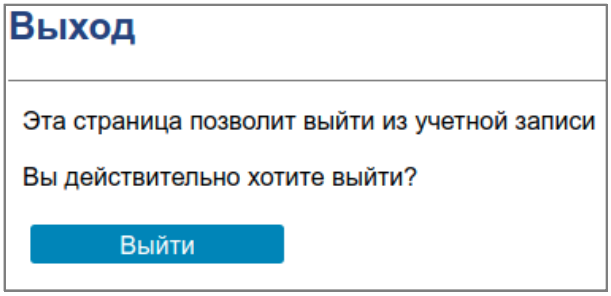
3.3.7.10 Подменю «Перезагрузка»

Описание содержимого страницы приведено на рисунке ниже.



3.3.7.11 Подменю «Выход»

Описание содержимого страницы приведено на рисунке ниже.

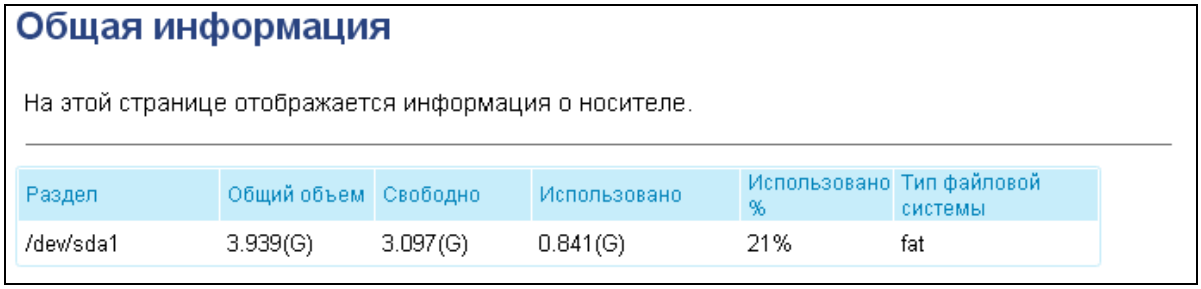


3.3.8 Меню «USB»

В меню «USB Настройки» можно предоставлять доступ к файлам на подключенном USB-накопителе по протоколу SMB и сервису DLNA[6].

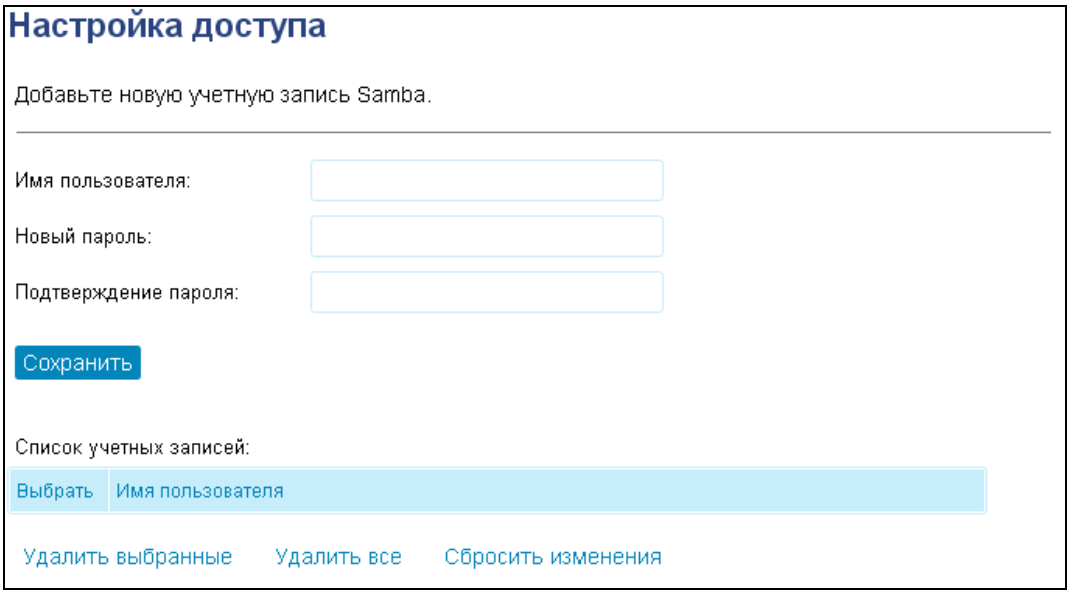
3.3.8.1 Подменю «Общая информация»

В этом подменю отображается информация о носителе: общий объем памяти, доступное свободное место на носителе, занятый объем памяти, а также тип файловой системы.



3.3.8.2 Подменю «Настройка доступа»

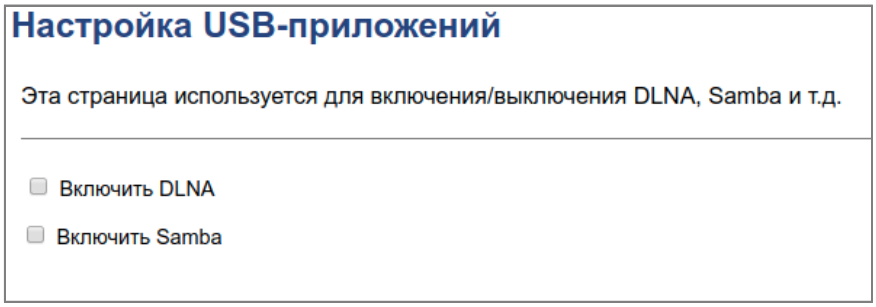
В этом подменю можно добавить и удалить учетные записи Samba, с которых будет возможен доступ к USB-носителю.



[6] *DLNA доступен только на RG-35-WZ*

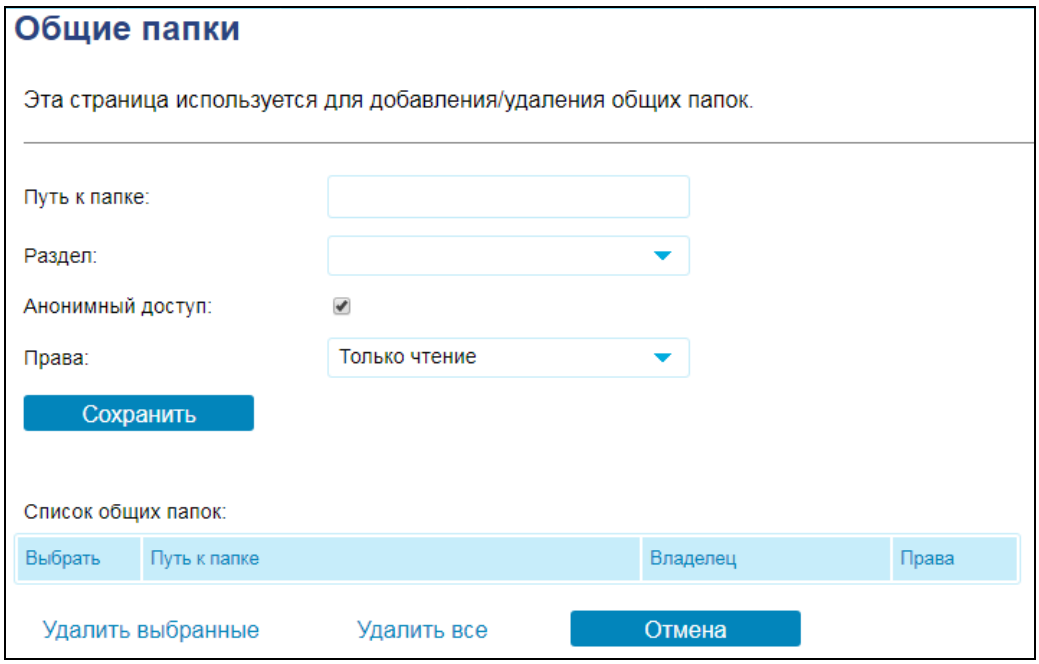
3.3.8.3 Подменю «Настройка USB приложений»

В этом подменю можно включить/выключить сервисы DLNA[7], Samba.



3.3.8.4 Подменю «Общие папки»

В этом подменю можно изменить права доступа к папкам на включенном в маршрутизатор USB-устройстве для неавторизованных пользователей.



- *Имя папки* — имя папки, которое будет отображаться в сети.
- *Раздел* — локальный раздел, к которому будет предоставлен доступ по сети.
- *Анонимный доступ* — при установленном флаге доступ к папке может быть осуществлен без авторизации.
- *Права* — выбор прав доступа к сетевой папке (Только чтение/Чтение и запись).

[7] DLNA доступен только на RG-35-WZ

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