

Абонентский маршрутизатор

RG-34-Wac

Руководство по эксплуатации, версия 1.6 (02.2017)

IP-адрес: <http://192.168.1.1>

имя пользователя: admin

пароль: password

Версия документа	Дата выпуска	Содержание изменений
Версия 1.6	16.02.2017	Изменено: 4.3.5.2 Подменю «WAN Интерфейс» Добавлено: 4.3.10.5 Подменю «Управление доступом»
Версия 1.5	23.12.2016	Изменено: 4.3.5.2 Подменю «WAN Интерфейс» 4.3.6.4 Подменю «Проброс портов» Добавлено: 4.3.10.4 Подменю «Настройка портов»
Версия 1.4	13.09.2016	Изменено: 4.3. Панель управления устройством
Версия 1.3	16.05.2016	Изменено: 4.3.5.1 Подменю «WAN Интерфейс»
Версия 1.2	13.04.2016	Изменено: 4.3.4.1 Подменю «WAN Интерфейс»
Версия 1.1	17.03.2016	Изменено: 2.2 Характеристика устройства 2.6 Перезагрузка устройства и сброс к заводским настройкам Добавлено: 4.2 Применение конфигурации и отмена изменений 4.3 Панель управления устройством
Версия 1.0	28.10.2015	Первая публикация
Версия программного обеспечения	Версия ПО: 1.10.0-b8 Версия веб-интерфейса: 1.0.3	

СОДЕРЖАНИЕ

1	Введение.....	5
1.1	Аннотация.....	5
1.2	Условные обозначения.....	5
2	Описание изделия.....	6
2.1	Назначение.....	6
2.2	Характеристика устройства.....	6
2.3	Основные технические параметры.....	8
2.4	Конструктивное исполнение.....	9
2.4.1	Передняя панель устройства.....	9
2.4.2	Задняя панель устройства.....	10
2.4.3	Боковая панель устройства.....	10
2.5	Световая индикация.....	11
2.6	Перезагрузка устройства и сброс к заводским настройкам.....	11
2.7	Управление кнопкой WPS.....	12
2.8	Комплект поставки.....	12
3	Порядок установки.....	13
3.1	Инструкции по технике безопасности.....	13
3.2	Рекомендации по установке.....	13
3.3	Порядок включения.....	13
4	Управление устройством через WEB-конфигуратор.....	14
4.1	Начало работы.....	14
4.2	Применение конфигурации и отмена изменений.....	14
4.3	Панель управления устройством.....	15
4.3.1	Основные элементы WEB-интерфейса.....	15
4.3.2	Меню «Мастер настройки».....	16
4.3.3	Меню «Режим работы».....	16
4.3.4	Меню «Беспроводная сеть».....	17
4.3.4.1	Подменю «Основные настройки».....	17
4.3.4.2	Подменю «Расширенные».....	19
4.3.4.3	Подменю «Безопасность».....	21
4.3.4.4	Подменю «Управление доступом. Wi-Fi».....	22
4.3.4.5	Подменю «Обзор сетей».....	23
4.3.4.6	Подменю «WPS».....	23
4.3.4.7	Подменю «Расписание».....	24
4.3.4.8	Подменю «Air time Fairness».....	25
4.3.5	Меню «Настройки TCP/IP».....	26
4.3.5.1	Подменю «LAN Интерфейс».....	26
4.3.5.2	Подменю «WAN Интерфейс».....	27
4.3.6	Меню «Firewall».....	30
4.3.6.1	Подменю «Фильтрация портов».....	30
4.3.6.2	Подменю «Фильтрация IP».....	31
4.3.6.3	Подменю «Фильтрация MAC».....	31
4.3.6.4	Подменю «Проброс портов».....	32
4.3.6.5	Подменю «Фильтрация URL».....	33
4.3.6.6	Подменю «DMZ».....	33
4.3.7	Меню «Quality of Service (QoS)».....	34
4.3.8	Меню «Настройка маршрутизации».....	35
4.3.9	USB Настройки.....	36
4.3.9.1	USB накопитель.....	36
4.3.9.2	FTP сервер.....	36
4.3.10	Меню «Администрирование».....	37

4.3.10.1	Подменю «Статус»	37
4.3.10.2	Подменю «Статистика»	38
4.3.10.3	Подменю «Настройка временных зон»	38
4.3.10.4	Подменю «Настройка портов»	39
4.3.10.5	Подменю «Управление доступом»	39
4.3.10.6	Подменю «Denial-of-Service»	41
4.3.10.7	Подменю «Системный журнал»	43
4.3.10.8	Подменю «Обновление прошивки»	44
4.3.10.9	Подменю «Сохранение/Загрузка настроек»	45
4.3.10.10	Подменю «Настройка TR-069»	46

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 все больше набирают обороты и к данному моменту в короткое время прошли огромный путь от нестабильных низкоскоростных сетей связи малого радиуса до сетей ШПД, сопоставимых по скорости с проводными сетями с высокими критериями к качеству предоставления услуг.

Устройство RG-34-Wac является точкой доступа Wi-Fi с интегрированным маршрутизатором. Основное предназначение RG-34-Wac: 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-34-Wac.

1.2 Условные обозначения

Обозначение	Описание
Полужирный шрифт	Полужирным шрифтом выделены примечания и предупреждения, название глав, заголовков, заголовков таблиц.
<i>Курсивом</i>	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 доступа пользователей к высокоскоростной, безопасной сети передачи данных разработан абонентский маршрутизатор RG-34-Wac (далее «устройство»).

Устройство RG-34-Wac – единая точка доступа к современным интерактивным сервисам по проводным и беспроводным сетям передачи данных: Интернет и Full HD IPTV.

Маршрутизатор RG-34-Wac предназначен для подключения устройств к беспроводной сети стандартов 802.11 a/b/g/n/ac. RG-34-Wac подключается к проводной сети с помощью 10/100/1000M Ethernet-интерфейса, и с помощью радиointерфейса создает беспроводной высокоскоростной доступ для устройств, поддерживающих технологию Wi-Fi в диапазоне 2,4 и 5 ГГц. К устройству можно подключить до четырех устройств проводной сети. USB-разъем используется для подключения внешних накопителей или 3G/4G USB-модема.

RG-34-Wac поддерживает современные требования к качеству сервисов и позволяет передавать наиболее важный трафик в более приоритетных очередях по сравнению с обычным. Обеспечение приоритезации происходит на основе 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 5В от сети 220 В.

Функции:

- *сетевые функции:*
 - работа в режиме «моста» или «маршрутизатора»;
 - 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-34-Wac.

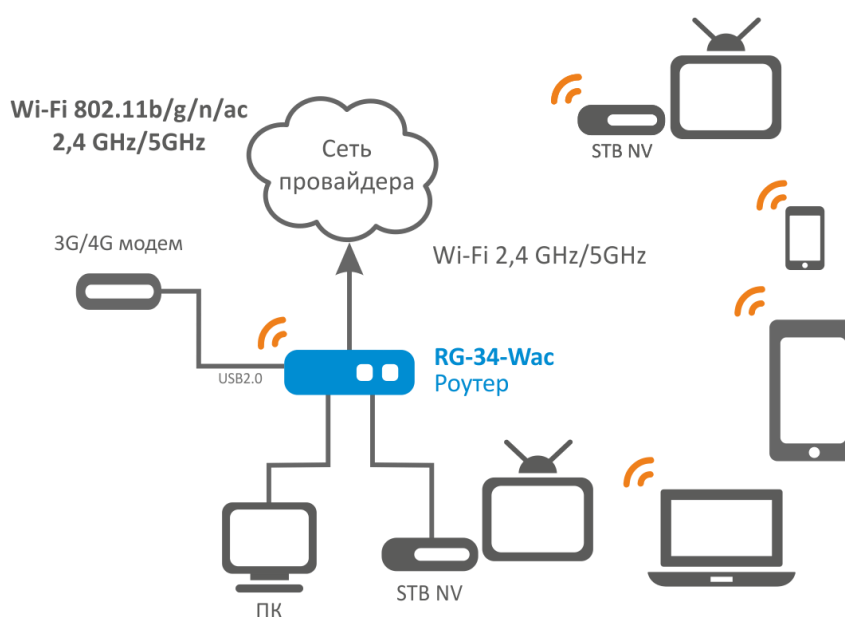


Рисунок 1 – Функциональная схема использования RG-34-Wac

2.3 Основные технические параметры

Основные технические параметры устройства приведены в Таблица 1.

Таблица 1 – Основные технические параметры

Общие параметры

Процессор	Realtek 520 МГц
RAM DDR (оперативная память)	128 Мб
ROM eMMC flash (системная память)	8 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
Модуляция	BPSK, QPSK, 16 QAM, 64 QAM, DBPSK, DQPSK, CCK
Скорость передачи данных, Мбит/с	802.11b(CCK): 1, 2, 5.5, 11 802.11g(OFDM): 6, 9, 12, 18, 24, 36, 48, 54 811n (HT20, 800ns GI): 13, 26, 39, 78, 104, 117, 130 802.11n (HT40, 400ns GI): 30, 60, 90, 120, 180, 240, 270, 300 802.11n (HT40, 800ns GI): 27, 54, 81, 108, 162, 216, 243, 270
Максимальная выходная мощность передатчика	2,4 ГГц (802.11 b/g/n): до 15 dBm 5 ГГц (802.11 a/n/ac): до 17 dBm
Чувствительность приемника	2,4 ГГц: 802.11n(MCS0): -90 dBm 802.11n(MCS4): -79 dBm 802.11n(MCS7): -72 dBm 5 ГГц: 802.11ac (MCS0): -92 dBm 802.11ac (MCS4): -82 dBm 802.11ac (MCS7): -76 dBm
Безопасность	64/128/152-битное WEP-шифрование данных; WEP, TKIP и AES

Управление

Удаленное управление	Web-интерфейс, Telnet
Ограничение доступа	по паролю

Общие параметры

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

2.4 Конструктивное исполнение

Точка доступа RG-34-Wac выполнена в пластиковом корпусе размерами 430x159x43,6 мм.

2.4.1 Передняя панель устройства

Внешний вид передней панели устройства RG-34-Wac приведен на рисунке 2.

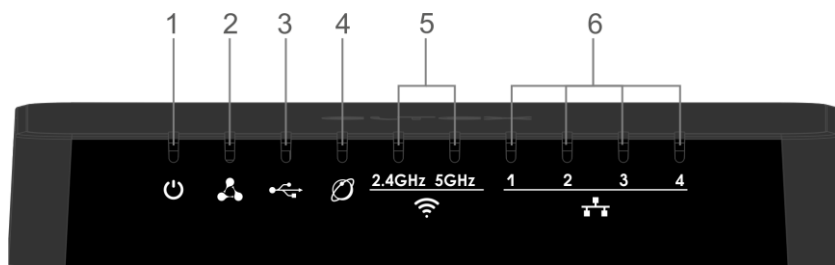








Рисунок 2 – Внешний вид передней панели RG-34-Wac

На верхней панели устройства *RG-34-Wac* 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-34-Wac приведен на рисунке 3.

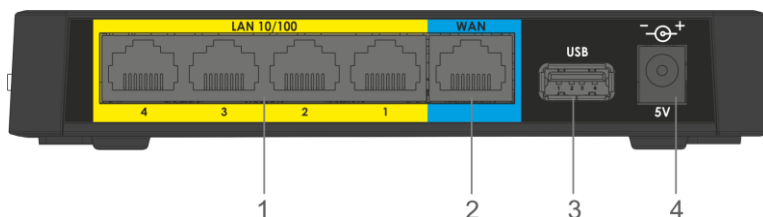


Рисунок 3 – Внешний вид задней панели RG-34-Wac

На задней панели устройства RG-34-Wac расположены следующие разъемы и органы управления, таблица 3.

Таблица 3 – Описание индикаторов и органов управления задней панели RG2400

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-34-Wac приведен на рисунке 4.



Рисунок 4 – Внешний вид боковой панели RG-34-Wac

На боковой панели устройства RG-34-Wac расположены следующие органы управления, Таблица 4







Таблица 4 – Описание органов управления боковой панели RG-34-Wac

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-34-Wac

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	красный, горит постоянно	ПО не загружено, режим начального загрузчика
		красный, мигает	загрузка ПО устройства
		красный и зеленый, мигают попеременно	сброс к заводским настройкам
		красный, желтый и зеленый, мигают попеременно	обновление ПО
		зеленый, мигает	обнаружена новая версия ПО
		желтый, горит постоянно	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 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 [4.3.3.5 Подменю «WPS»](#).

2.8 Комплект поставки

В базовый комплект поставки устройства RG-34-Wac входят:

- абонентский маршрутизатор;
- адаптер питания 220/5В 2,5 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-34-Wac 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, 5ГГц, 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-34-Wac, рисунок 3.
2. Если RG-34-Wac будет использоваться в качестве домашнего проводного маршрутизатора, то подключите сетевой Ethernet-кабель к разъемам **LAN** RG-34-Wac 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

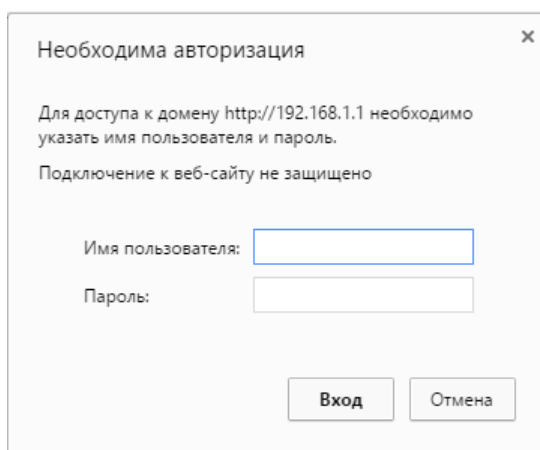
Для начала работы нужно подключиться к устройству по интерфейсу LAN через Web-браузер:

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 «Применить изменения» происходит сохранение конфигурации во flash-память устройства и применение новых настроек. 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 в левой стороне WEB-интерфейса.

4.3.1 Основные элементы WEB-интерфейса

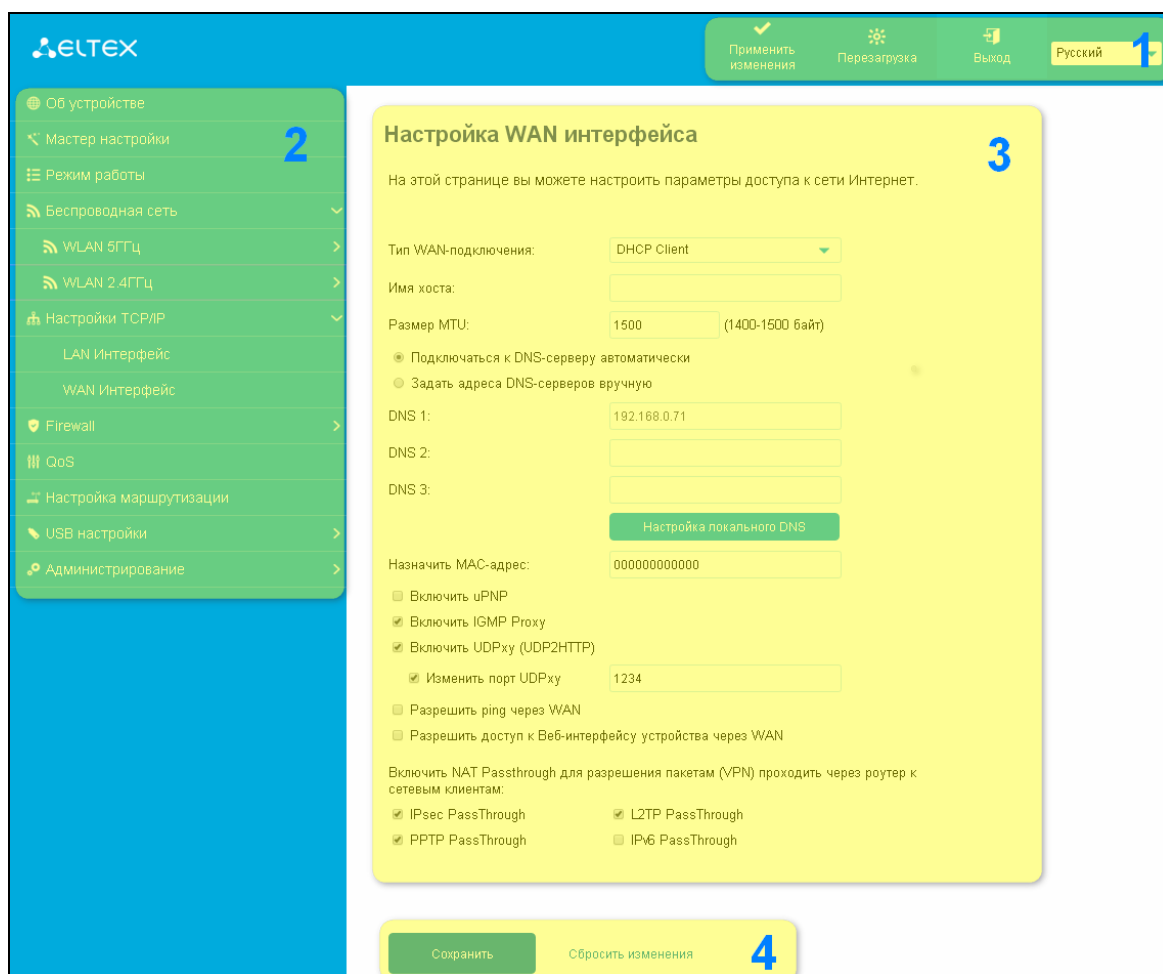
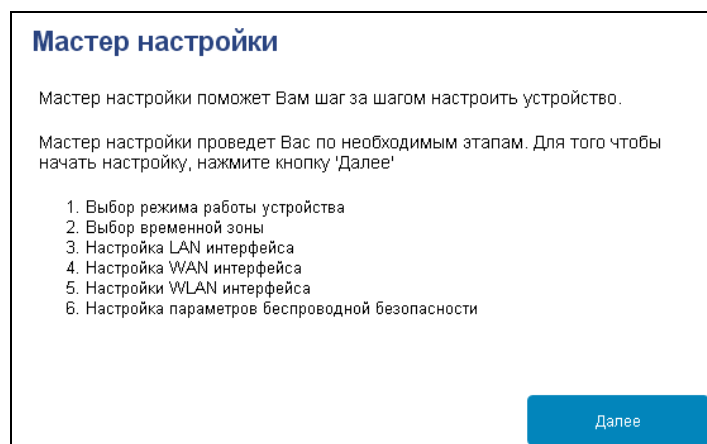


Рисунок 5 – Элементы навигации Web-конфигуратора

1. Кнопки применения конфигурации, перезагрузки устройства и смена языка WEB-интерфейса.
2. Дерево вкладок для выполнения настроек.
3. Основное поле настроек устройства, соответствующее выбранной вкладке из поля 2.
4. Кнопки сохранения изменений конфигурации и сброса до последних не сохраненных значений.

4.3.2 Меню «Мастер настройки»



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

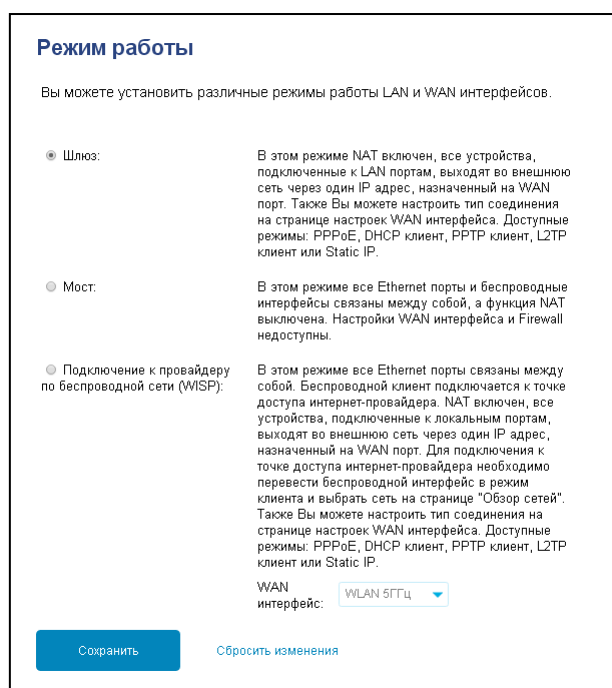
- Режим работы;
- Синхронизацию времени;
- Параметры LAN-интерфейса;
- Параметры WAN-интерфейса (Интернет);
- Параметры Wi-Fi сетей диапазонов 2.4 ГГц и 5 ГГц.

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

4.3.3 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.
- Подключение к провайдеру по беспроводной сети (WISP) – в этом режиме один из модулей Wi-Fi (2,4ГГц или 5ГГц) переходит в режим клиента, подключается к беспроводной сети провайдера и работает в качестве WAN порта.



4.3.4 Меню «Беспроводная сеть»

В меню «Беспроводная сеть» 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.

4.3.4.1 Подменю «Основные настройки»

Основные настройки беспроводного интерфейса 5ГГц

Эта страница предназначена для настройки параметров доступа WLAN клиентов.

Отключить WLAN интерфейс

Частотный диапазон: 5 GHz (A+N+AC) ▼

Режим работы: AP ▼

Имя сети (SSID): EltexWiFi5G

Добавить к профилю

Ширина канала: 40MHz ▼

Канал: Auto ▼

Скрывать имя сети (SSID): Нет ▼

Включить режим Wi-Fi Multimedia (WMM): Включено ▼

Ограничение Tx: 0 Мбит/с (0: без ограничений)

Ограничение Rx: 0 Мбит/с (0: без ограничений)

Активные соединения: Показать активные клиенты

Гостевые сети

Включить клонирование MAC

Включить режим Универсального Повторителя (Работает в качестве ТД и клиента одновременно)

Имя сети (SSID) дополнительного интерфейса: RTK 11n AP RPT0

Добавить к профилю

- *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 150 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 150 Мбит/с;
- 2.4 GHz (B+G+N) – если в сети присутствуют беспроводные клиенты с поддержкой 802.11b, 802.11g и 802.11n.

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.

— *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 WiFi Multimedia, которая позволяет оптимизировать передачу мультимедийного трафика по беспроводной среде;

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

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

4.3.4.2 Подменю «Расширенные»

Расширенный настройки беспроводного интерфейса 5ГГц

Данные настройки предназначены для опытных пользователей. Не меняйте эти настройки, если Вы не имеете представления о том, какой эффект они должны оказать на работу точки доступа.

Fragment Threshold:	<input type="text" value="2346"/>	(256-2346)
RTS Threshold:	<input type="text" value="2347"/>	(0-2347)
Beacon Interval:	<input type="text" value="100"/>	(20-1024 ms)
IAPP:	<input checked="" type="radio"/> Включено <input type="radio"/> Выключено	
Protection:	<input type="radio"/> Включено <input checked="" type="radio"/> Выключено	
Aggregation:	<input checked="" type="radio"/> Включено <input type="radio"/> Выключено	
Short GI:	<input checked="" type="radio"/> Включено <input type="radio"/> Выключено	
WLAN Partition:	<input type="radio"/> Включено <input checked="" type="radio"/> Выключено	
STBC:	<input checked="" type="radio"/> Включено <input type="radio"/> Выключено	
LDPC:	<input checked="" type="radio"/> Включено <input type="radio"/> Выключено	
TX Beamforming:	<input checked="" type="radio"/> Включено <input type="radio"/> Выключено	
Multicast to Unicast:	<input checked="" type="radio"/> Включено <input type="radio"/> Выключено	
RF Output Power:	<input checked="" type="radio"/> 100% <input type="radio"/> 60% <input type="radio"/> 50% <input type="radio"/> 35% <input type="radio"/> 15%	

Сохранить
Сбросить изменения

- *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;
- *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 отправляет 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;
- *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;
- *Preable Type* – размер преамбулы показывает длину служебного поля в каждом пакете. Длинная (Long) преамбула состоит из 128 бит, короткая (Short) – из 56 бит. Короткий размер преамбулы повышает общее быстродействие системы, используется для мультимедиа-приложений;
- *IAPP* – протокол IAPP (Inter-Access Point Protocol) позволяет использовать роуминг клиентов между несколькими точками доступа внутри одного сегмента сети;
- *Protection* – это специальный механизм для сетей 802.11 b/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;

- *Aggregation* – включает возможность объединения нескольких маленьких пакетов для передачи в одном большом;
- *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 (менее искажены) других. 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;
- *20/40MHz Coexist* – включенная опция приводит к тому, что если в радиусе действия нашей точки доступа будут обнаружены другие точки на аналогичных частотных каналах или все каналы будут сильно загружены – наша точка доступа отключит использование частотного диапазона 40МГц, чтобы не мешать соседям;
- *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;
- *RF Output Power* – регулировка мощности сигнала точки доступа в процентах от максимального уровня.

4.3.4.3 Подменю «Безопасность»

Настройка параметров безопасности для интерфейса 5ГГц

Данные настройки позволяют Вам задать параметры безопасности. Выбор типа шифрования поможет Вам предотвратить несанкционированный доступ к вашей беспроводной сети.

Выберите SSID:	<input type="text" value="Root AP - EltexWiFi5G"/>	
Метод проверки подлинности:	<input type="text" value="WPA2"/>	
Метод аутентификации:	<input type="radio"/> Enterprise (RADIUS) <input checked="" type="radio"/> Personal (Pre-Shared Key)	
Тип шифрования WPA2:	<input type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES	
Management Frame Protection:	<input checked="" type="radio"/> none <input type="radio"/> capable <input type="radio"/> required	
Формат ключа:	<input type="text" value="Passphrase"/>	
Ключ:	<input type="text"/>	<input type="button" value="Показать пароль"/>

- *Выберите SSID* – выбор SSID 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 шифрования WPA и WPA2 как наиболее безопасные на данный момент.



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 (RADIUS 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), sutable (выборочно) и required (обязательно). При выборе варианта sutable доступен пункт с включением функции хэширования по алгоритму SHA256.

4.3.4.4 Подменю «Управление Wi-Fi доступом»

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

Управление доступом 5ГГц

Список разрешенных позволяет подключаться только клиентам из данного списка. Пункт "Список запрещенных" ограничивает доступ к точке доступа для клиентов из этого списка.

Режим контроля доступа: Отключено ▾

MAC-адрес:

Комментарий:

Сохранить Сбросить изменения

Список устройств для выбранного режима контроля доступа:

MAC-адрес	Комментарий

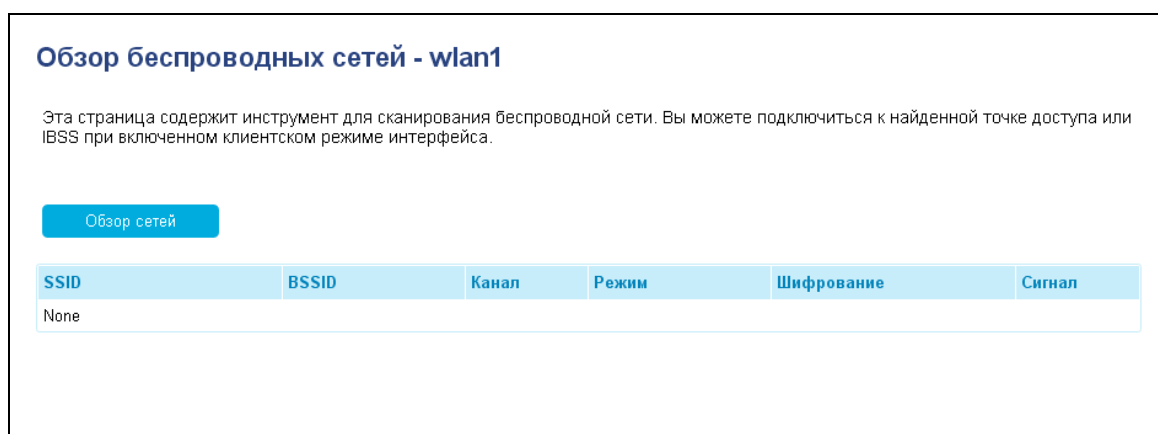
Удалить выбранные Удалить все Очистить

- *Режим контроля доступа* – позволяет задать один из трех режимов работы с беспроводными устройствами:
 - *Отключено* – нет ограничений по подключению устройств;
 - *Список разрешенных* – к Wi-Fi сети могут подключиться только устройства с MAC-адресами из списка разрешенных;

- *Список запрещенных* – 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 в него писать название устройства, для которого заводится запись в список.

4.3.4.5 Подменю «Обзор сетей»

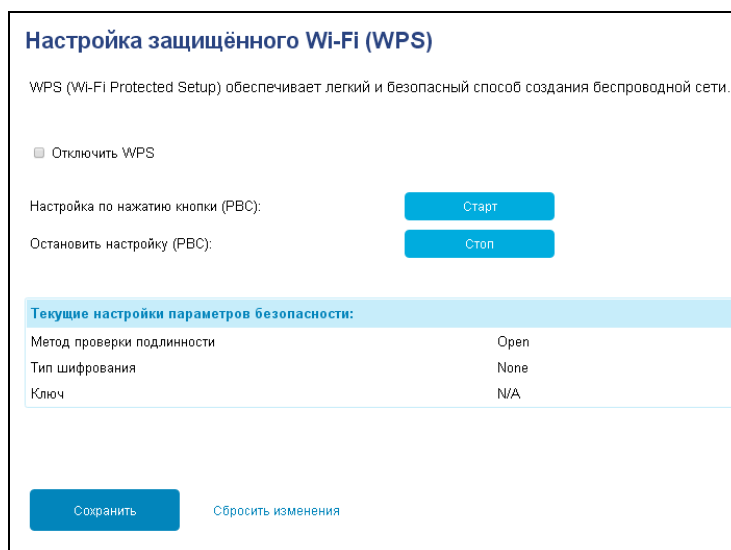
В подменю «Обзор сетей» можно запустить поиск других Wi-Fi сетей в заданном частотном диапазоне с целью определения минимально загруженного канала при тонкой настройке сети. Также через это подменю выполняется подключение к беспроводной сети провайдера в режиме работы WISP.



4.3.4.6 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 деактивироваться 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.

4.3.4.7 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.

Расписание работы беспроводного интерфейса

Эта страница позволит Вам задать расписание работы беспроводного интерфейса. Пожалуйста, не забудьте настроить системное время перед включением данной опции.

Включить работу по расписанию

День	От	До
<input type="checkbox"/> Воскресенье	00 час. 00 мин.	00 час. 00 мин.
<input type="checkbox"/> Воскресенье	00 час. 00 мин.	00 час. 00 мин.
<input type="checkbox"/> Воскресенье	00 час. 00 мин.	00 час. 00 мин.
<input type="checkbox"/> Воскресенье	00 час. 00 мин.	00 час. 00 мин.
<input type="checkbox"/> Воскресенье	00 час. 00 мин.	00 час. 00 мин.
<input type="checkbox"/> Воскресенье	00 час. 00 мин.	00 час. 00 мин.
<input type="checkbox"/> Воскресенье	00 час. 00 мин.	00 час. 00 мин.
<input type="checkbox"/> Воскресенье	00 час. 00 мин.	00 час. 00 мин.
<input type="checkbox"/> Воскресенье	00 час. 00 мин.	00 час. 00 мин.
<input type="checkbox"/> Воскресенье	00 час. 00 мин.	00 час. 00 мин.
<input type="checkbox"/> Воскресенье	00 час. 00 мин.	00 час. 00 мин.

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

4.3.4.8 Подменю «Air time Fairness»

Функция Air time Fairness позволяет распределять временные интервалы передачи данных между подключенными Wi-Fi клиентами, тем самым управляя пропускной способностью каждого клиента в отдельности.

Air Time Fairness 5ГГц

Airtime Management, также называют Airtime Fairness (эфирная равнодоступность). Эта функция позволяет управлять распределением эфирного времени. Вы можете распределить эфирное время равномерно или выделить определенный отрезок времени для конкретных устройств (используя IP/MAC-адрес). Благодаря данной функции, можно увеличить общую пропускную способность сети в ущерб скорости работы с медленными устройствами.

Режим работы: Режим работы с устройствами ▼

Распределение времени между устройствами:
 Равномерное распределение между всеми устройствами: Включено Выключено

IP MAC:

Процент эфирного времени:

Комментарий:

Добавить устройство

Изменения вступят в силу только после нажатия кнопки 'Применить изменения'.

Список устройств с настроенными приоритетами:

IP/MAC-адрес	Процент эфирного времени	Комментарий
Сумма эфирного времени не должна быть больше 100. Осталось для распределения: 100.		

Удалить выбранные
Удалить все
Обновить значения в таблице

Сохранить

- *Режим работы* – есть два основных режима:
 - *Отключено* – функция не используется, время распределяется в соответствии с внутренней логикой работы устройства;
 - *Режим работы с устройствами* – функция Airtime Fairness включена.
- *Равномерное распределение между всеми устройствами* – позволяет распределять одинаковые интервалы между всеми подключенными клиентами или использовать ручные параметры для отдельных клиентов, выделяя им необходимое число временных ресурсов;
- *IP/MAC* – в это поле вводится IP или MAC-адрес устройства которому необходимо задать определенный временной промежуток от общей длительности передачи сигналов;
- *Процент эфирного времени* – в поле указывается сколько процентов общей длительности отведено данному клиенту, может принимать значения от 0 до 100%. Для остальных клиентов оставшееся время будет распределено равномерно;
- *Комментарий* – поле для ввода комментария к записи в список, например, имя Wi-Fi клиента.

4.3.5 Меню «Настройки TCP/IP»

В этом меню доступны для конфигурирования параметры LAN и WAN интерфейсов устройства.

4.3.5.1 Подменю «LAN Интерфейс»

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

Настройка LAN интерфейса

Эта страница предназначена для настройки параметров Локальной Вычислительной Сети, подключенной к LAN портам вашего роутера. Здесь Вы можете изменить IP-адрес, маску подсети, настройки DHCP и прочее.

IP-адрес:	<input type="text" value="192.168.1.1"/>
Маска подсети:	<input type="text" value="255.255.255.0"/>
DHCP:	<input type="text" value="Сервер"/>
Начальный адрес пула IP-адресов:	<input type="text" value="192.168.1.2"/>
Конечный адрес пула IP-адресов:	<input type="text" value="192.168.1.254"/>
	<input type="button" value="Показать активные клиенты"/>
Время аренды DHCP:	<input type="text" value="480"/> (1 ~ 10080 минут)
	<input type="button" value="Настройка статического DHCP"/>
Имя домена:	<input type="text" value="RG-34-Wac"/>

[Сбросить изменения](#)

- *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.

4.3.5.2 Подменю «WAN Интерфейс»

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

Настройка WAN интерфейса

На этой странице вы можете настроить параметры доступа к сети Интернет.

Тип WAN-подключения: DHCP Client ▼

Имя хоста:

Размер MTU: (1400-1500 байт)

Подключаться к DNS-серверу автоматически
 Задать адреса DNS-серверов вручную

DNS 1:

DNS 2:

DNS 3:

[Настройка локального DNS](#)

Назначить MAC-адрес:

Включить uPNP
 Включить IGMP Проху
 Включить UDPху (UDP2HTTP)
 Изменить порт UDPху
 Разрешить ping через WAN

Включить NAT Passthrough для разрешения пакетам (VPN) проходить через роутер к сетевым клиентам:

IPsec PassThrough L2TP PassThrough
 PPTP PassThrough IPv6 PassThrough

— **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.
- *USB3G* – доступ к Интернет будет осуществляться через подключенный к устройству USB 3G модем. Доступные параметры:
 - *Имя пользователя* – имя пользователя для идентификации при подключении к беспроводной сети;
 - *Пароль* – пароль для идентификации при подключении к беспроводной сети;
 - *PIN* – поле для ввода PIN-кода используемой в модеме SIM-карты;
 - *APN* – идентификатор точки доступа в сеть оператора;
 - *Номер для доступа* – номер дозвона;
 - *Тип подключения* – тип подключения позволяет выбрать тип подключения L2TP: постоянное, по требованию, вручную.
- *LTE4G* – доступ к Интернет будет осуществляться через подключенный к устройству LTE модем. Настройка соединения производится в полностью автоматическом режиме.

— *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;
- *Локальный DNS* – позволяет назначить доменное имя для определенного IP адреса в пределах локальной сети;
- *Назначить 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 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;
- *Включить UDPху (UDP2HTTP)* – эта функция позволяет менять тип приходящего из WAN-порта трафик Multicast в LAN-сети на Unicast. Функция необходима для работы IPTV на устройствах, которые не поддерживают Multicast-трафик, а также при просмотре IPTV через беспроводной интерфейс;
- *Изменить порт UDPху* - номер порта UDPху, с которого будет осуществляться транслирование видео-потока. Используйте этот порт для подключения к транслируемым устройством потокам IPTV;
- *Разрешить ping через WAN* – при выставленном флаге устройство будет отвечать на приходящие из WAN запросы ICMP;
- *Включить NAT Passthrough для разрешения пакетам (VPN) проходить через роутер к сетевым клиентам* – эта функция используется при настройке 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.

4.3.6 Меню «Firewall»

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

4.3.6.1 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.

Фильтрация портов

Записи в таблице предназначены для того, чтобы блокировать обмен пакетами определенного типа между локальной сетью и Интернетом. Использование подобных фильтров может быть полезно для защиты вашей локальной сети или ограничения доступа.

Включить фильтр портов

Диапазон портов: -

Протокол:

Комментарий:

Список действующих фильтров:

Диапазон портов	Протокол	Комментарий
Удалить выбранные	Удалить все	Очистить

- *Включить фильтр портов* – при выставленном флаге фильтр включен;
- *Диапазон портов* – вводятся номера портов трафик с которых вы ходите запретить;
- *Протокол* – выбор типа протокола трафика TCP, UDP или оба;
- *Комментарий* – поле для оставления заметок для фильтров.

4.3.6.2 Подменю «Фильтрация IP»

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

Фильтр IP-адресов

Записи в таблице предназначены для того, чтобы блокировать обмен пакетами определенного типа между локальной сетью и Интернетом. Использование подобных фильтров может быть полезно для защиты вашей локальной сети или ограничения доступа.

Включить фильтр IP-адресов

Локальный IP-адрес:

Протокол:

Комментарий:

Список действующих фильтров:

Локальный IP-адрес	Протокол	Комментарий
<input type="button" value="Удалить выбранные"/>	<input type="button" value="Удалить все"/>	<input type="button" value="Очистить"/>

- *Включить фильтр IP-адресов* – при выставленном флаге фильтр включен;
- *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.

4.3.6.3 Подменю «Фильтрация MAC»

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

Фильтр MAC-адресов

Записи в таблице предназначены для того, чтобы блокировать обмен пакетами определенного типа между локальной сетью и Интернетом. Использование подобных фильтров может быть полезно для защиты вашей локальной сети или ограничения доступа.

Включить фильтр MAC-адресов

MAC-адрес:

Комментарий:

Список действующих фильтров:

MAC-адрес	Комментарий	
<input type="button" value="Удалить выбранные"/>	<input type="button" value="Удалить все"/>	<input type="button" value="Очистить"/>

- *Включить фильтр MAC-адресов* – при выставленном флаге фильтр включен;
- *MAC-адрес* – вводятся MAC-адрес устройства которому нужно ограничить доступ;
- *Протокол* – выбор типа протокола трафика TCP, UDP или оба;
- *Комментарий* – поле для оставления заметок для фильтров.

4.3.6.4 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.

Проброс портов

Переадресация портов позволяет удаленным компьютерам подключаться к конкретному компьютеру локальной сети. Эти настройки могут быть полезны, если Вам необходимо предоставить доступ к локальному веб или почтовому серверам, находящимся за шлюзом NAT Firewall'a. Также проброс портов может потребоваться для полноценной работы некоторых P2P приложений (например, BitTorrent).

Включить проброс портов

IP-адрес:

Протокол: TCP/UDP

Диапазон входящих портов: -

Исходящий порт:

Комментарий:

Сохранить Сбросить изменения

Список проброшенных портов:

	Локальный IP-адрес	Протокол	Исходящий порт	Диапазон входящих портов	Комментарий	
Удалить выбранные Удалить все Очистить						

- *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;
- *Диапазон входящих портов* – указывается диапазон пробрасываемых портов на WAN-интерфейсе;
- *Исходящий порт* – порт назначения устройства в LAN сети, которое будет получать трафик;
- *Комментарий* – поле для оставления заметок для фильтров.

4.3.6.5 Подменю «Фильтрация URL»

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

Фильтр URL-адресов

Фильтр используется для блокировки доступа к адресам из списка.

Включить фильтрацию URL

URL-адрес:

Список действующих фильтров:

	URL-адрес
<input type="button" value="Удалить выбранные"/> <input type="button" value="Удалить все"/> <input type="button" value="Очистить"/>	

- *Включить фильтрацию URL* – при выставленном флаге фильтр включен;
- *URL-адрес* – вводятся URL-адрес ресурса, доступ к которому вы хотите заблокировать.

4.3.6.6 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 веб-сервер, FTP-сервер, DNS-сервер и прочие.

Демилитаризованная зона (DMZ)

Виртуальная зона DMZ позволяет показывать в Интернете один компьютер так, что все входящие пакеты будут перенаправляться на установленный компьютер. Обычно DMZ-хост содержит устройства, доступные для интернет-трафика, такие как веб-серверы, FTP-серверы, DNS-серверы и прочие.

Включить DMZ

IP-адрес DMZ-хоста:

- *Включить DMZ* – при выставленном флаге DMZ включен;
- *IP-адрес DMZ-хоста* – вводятся 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.

Качество обслуживания (QoS)

Технология позволяет управлять пропускной способностью сети.

Включить QoS

Скорость исходящего соединения:

Автоматически

Задать вручную (Кбит/с):

Скорость входящего соединения:

Автоматически

Задать вручную (Кбит/с):

Настройка правил QoS:

Тип адреса: IP MAC

Локальный IP-адрес: -

MAC-адрес:

Режим:

Скорость исходящего соединения (Кбит/с):

Скорость входящего соединения (Кбит/с):

Комментарий:

Список действующих правил QoS:

Локальный IP-адрес	MAC-адрес	Режим	Скорость исходящего соединения	Скорость входящего соединения	Комментарий

- *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 адреса* – выберите тип адреса для которого задается правило: IP или MAC;
- *Локальный IP-адрес* – задается при выбранном типе адреса IP клиента;
- *Локальный MAC-адрес* – задается при выбранном типе адреса MAC клиента;
- *Режим* – позволяет выбрать между двух вариантов:
 - Гарантировать минимальную скорость;
 - Ограничивать максимальную скорость.
- *Скорость входящего/исходящего соединения* – введите требуемое значение в зависимости от выбранного режима;
- *Комментарий* – позволяет оставить заметку об текущем правиле QoS.

4.3.8 Меню «Настройка маршрутизации»

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

Настройка маршрутизации

На этой странице Вы можете задать параметры динамической маршрутизации, а также настроить правила статической маршрутизации.

Включить динамическую маршрутизацию

NAT: Включено Выключено

Передача: Выключено RIP 1 RIP 2

Прием: Выключено RIP 1 RIP 2

Разрешить статические маршруты

IP-адрес:

Маска подсети:

Шлюз:

Метрика:

Интерфейс:

Список статических маршрутов:

IP-адрес сети или хоста	Сетевая маска	Шлюз	Метрика	Интерфейс
<input type="button" value="Удалить выбранные"/> <input type="button" value="Удалить все"/> <input type="button" value="Очистить"/>				

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.

Статическая маршрутизация

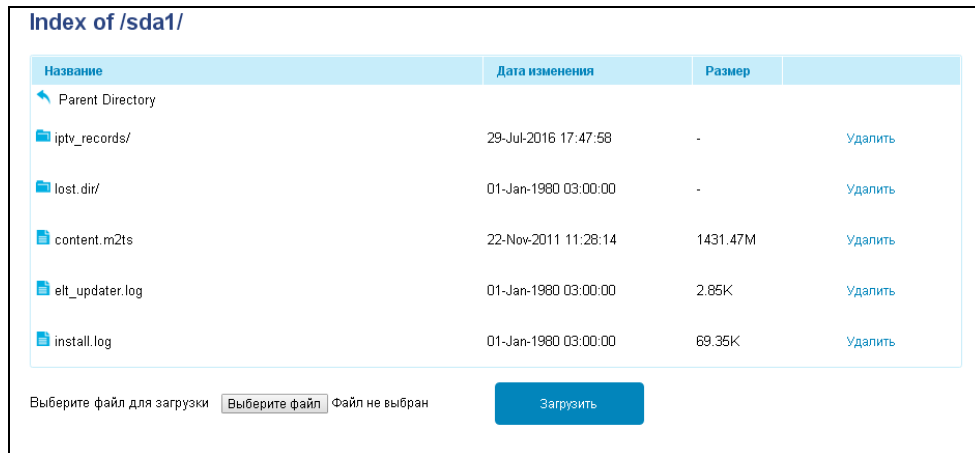
- *Включить статические маршруты* – при выставленном флаге статические маршруты будут добавлены в таблицу маршрутизации;
- *IP-адрес* – адрес сети назначения или хоста, до которой указывается маршрут;
- *Маска подсети* – сетевая маска. Для хоста маска подсети устанавливается в значение 255.255.255.255, 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 USB Настройки

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

4.3.9.1 USB накопитель

В этом подменю отображается файловая система подключенного USB накопителя.



Через подменю можно выполнять действия с файлами:

- Загружать файлы на USB накопитель;
- Скачивать файлы в память компьютера;
- Удалять файлы с USB накопителя.

4.3.9.2 FTP сервер

В этом подменю отображаются параметры встроенного в устройство FTP сервера.

FTP сервер

FTP - стандартный протокол, предназначенный для передачи файлов по TCP-сетям.

Включить передачу данных

Логин:

Пароль:

Права на запись:

Список пользователей:

Логин	Права на запись

- *Включить передачу данных* – при установленном флаге FTP сервер переходит в активное состояние, сервер готов к подключению клиентов;
- *Логин* – в поле указывается имя пользователя для подключения к серверу;

- *Пароль* – поле для ввода пароля да выбранного пользователя;
- *Права на запись* – предоставляет данному пользователю право выполнять запись файлов на FTP сервер.

4.3.10 Меню «Администрирование»

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

4.3.10.1 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:1h:4m:12s
Версия прошивки	1.8.0-b6
Время сборки	Fri Sep 9 17:01:21 NOV 2016
Конфигурация беспроводного интерфейса 1	
Режим	AP
Частотный диапазон	5 GHz (A+N+AC)
SSID	EltexWiFi5G
Канал:	64
Шифрование	Disabled
BSSID	a8:f9:4b:0e:f1:34
Клиенты	0
Конфигурация TCP/IP	
Протокол получения IP	Fixed IP
IP-адрес	192.168.1.1
Маска подсети	255.255.255.0
Основной шлюз	192.168.1.1
DHCP-сервер	Включено
MAC-адрес	02:20:80:a8:f9:4b
Конфигурация WAN	
Протокол получения IP	DHCP
IP-адрес	192.168.0.215
Маска подсети	255.255.255.0
Основной шлюз	192.168.0.1
MAC-адрес	a8:f9:4b:0e:f1:33

4.3.10.2 Подменю «Статистика»

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

Статистика

На этой странице показаны счетчики отправленных и принятых пакетов для WLAN и Ethernet интерфейсов.

Wireless 1 LAN	Отправлено пакетов	52
	Получено пакетов	6017
Ethernet LAN	Отправлено пакетов	2410
	Получено пакетов	1402
Ethernet WAN	Отправлено пакетов	1392
	Получено пакетов	8931

4.3.10.3 Подменю «Настройка временных зон»

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

Настройка времени

Вы можете настроить системное время при помощи синхронизации с публичным NTP-сервером.

Текущее время:

<input type="text" value="2016"/>	<input type="text" value="9"/>	<input type="text" value="9"/>
Год	Месяц	День
<input type="text" value="18"/>	<input type="text" value="5"/>	<input type="text" value="51"/>
Час	Мин	Сек

Выберите временную зону:

Разрешить синхронизацию с NTP-сервером
 Адрес NTP-сервера:
 Задание адреса вручную:

- *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.

4.3.10.4 Подменю «Настройка портов»

Эта страница позволяет настроить параметры LAN портов. По умолчанию, задается значение Auto, изменять можно параметры только активных интерфейсов.

Настройка портов

Эта страница позволяет настроить параметры LAN портов.

LAN порт 1:

LAN порт 2:

LAN порт 3:

LAN порт 4:

Настройка портов

Эта страница позволяет настроить параметры LAN портов.

LAN порт 1:

LAN порт 2:

LAN порт 3:

LAN порт 4:

4.3.10.5 Подменю «Управление доступом»

В подменю «Управление доступом» устанавливаются логин и пароль доступа к WEB-интерфейсу устройства.

Управление доступом

На этой странице Вы можете настроить аккаунт для доступа к маршрутизатору и включить доступ по telnet.

Сменить имя пользователя и(или) пароль

Имя пользователя:

Новый пароль:

Подтверждение пароля:

Включить доступ по telnet

Логин:

Пароль:

Разрешить доступ к Веб-интерфейсу устройства через WAN

Изменить порт доступа

Включить доступ к Веб-интерфейсу только для списка IP-адресов

Добавить IP-адрес

Список IP-адресов

<input type="button" value="Добавить IP-адрес"/>
--

- *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.



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

- *Включить доступ по telnet* – открывает доступ к устройству по службе telnet из LAN-сети;
- *Логин* – поле для ввода логина для доступа по telnet;
- *Пароль* – поле для ввода пароля для доступа по telnet;
- *Разрешить доступ к Веб-интерфейсу устройства через WAN* – открывает доступ к веб-интерфейсу устройствам из WAN сети;
- *Изменить порт доступа* – изменение порта доступа к веб-интерфейсу из WAN и LAN сети. По умолчанию используется порт 80;
- *Включить доступ к Веб-интерфейсу только для списка IP-адресов* – позволяет настроить доступ к веб-интерфейсу за WAN только для устройств с IP-адресами из списка;
- *Добавить IP-адрес* – поле для ввода IP-адреса.



В список разрешено вносить до пяти IP-адресов.

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

4.3.10.6 Подменю «Denial-of-Service»

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.

Denial of Service

"Denial-of-service" (отказ в обслуживании) вид атаки на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам.

Включить предотвращение DoS атак

<input checked="" type="checkbox"/> Whole System Flood: SYN	<input type="text" value="3000"/>	Пакетов/Секунда
<input checked="" type="checkbox"/> Whole System Flood: FIN	<input type="text" value="3000"/>	Пакетов/Секунда
<input checked="" type="checkbox"/> Whole System Flood: UDP	<input type="text" value="3000"/>	Пакетов/Секунда
<input checked="" type="checkbox"/> Whole System Flood: ICMP	<input type="text" value="3000"/>	Пакетов/Секунда
<input checked="" type="checkbox"/> Per-Source IP Flood: SYN	<input type="text" value="2000"/>	Пакетов/Секунда
<input checked="" type="checkbox"/> Per-Source IP Flood: FIN	<input type="text" value="2000"/>	Пакетов/Секунда
<input checked="" type="checkbox"/> Per-Source IP Flood: UDP	<input type="text" value="2000"/>	Пакетов/Секунда
<input checked="" type="checkbox"/> Per-Source IP Flood: ICMP	<input type="text" value="2000"/>	Пакетов/Секунда
<input checked="" type="checkbox"/> TCP/UDP PortScan (чувствительность)	<input type="text" value="Низкая"/>	

<input checked="" type="checkbox"/> ICMP Smurf	<input checked="" type="checkbox"/> IP Land	<input checked="" type="checkbox"/> IP Spoof
<input checked="" type="checkbox"/> IP TearDrop	<input checked="" type="checkbox"/> PingOfDeath	<input checked="" type="checkbox"/> TCP Scan
<input checked="" type="checkbox"/> TCP SynWithData	<input checked="" type="checkbox"/> UDP Bomb	<input checked="" type="checkbox"/> UDP EchoChargen

[Выбрать все](#) [Очистить все](#)

Включить блокировку источника атаки по IP-адресу Время блокировки (сек)

[Сохранить](#)

- *Включить предотвращение DoS атак* – при выставленном флаге защита от DoS атак включена;
- *Whole System Flood* – группа счетчиков определяющие 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 Веб-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 окончании таймера блокировка снимается, но может быть выполнена снова, если атака не прекратится.

4.3.10.7 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.

The screenshot shows the 'Системный журнал' (System Log) configuration page. At the top, there is a title and a brief instruction: 'На этой странице Вы можете настроить параметры ведения системного журнала, а также просмотреть записи в нем.' Below this, there are several configuration options:

- Включить логирование
- Все системные сообщения
- Беспроводная сеть
- DoS
- Использовать удаленный сервер для логирования

Below the options, there is a text label 'IP-адрес удаленного сервера:' followed by a text input field containing the value '192.168.0.56'. Underneath the input field is a large, empty rectangular area, likely for displaying log entries. At the bottom of the form, there are three buttons: 'Обновить' (Refresh), 'Очистить' (Clear), and 'Сохранить' (Save).

- *Включить логирование* – при выставленном флаге функция журнала активна. Логирование имеет три уровня:
 - *Все системные сообщения* – включает в себя сообщения про беспроводную сеть и DoS;
 - *Беспроводная сеть* – сообщения о состоянии беспроводной сети устройства;
 - *DoS* – информация о работе защиты от DoS-атак.
- *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».

4.3.10.8 Подменю «Обновление прошивки»

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

Обновление прошивки

На этой странице Вы можете обновить системное ПО роутера до более новой версии. Пожалуйста, не выключайте устройство в процессе обновления - это может привести к порче памяти.

Версия ПО: 1.8.0-b6

Выберите файл с прошивкой: Файл не выбран

Обновление прошивки с удаленного сервера

Адрес сервера обновлений:

Период опроса (часы):

Доступная версия: Версия недоступна

- *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.nsk.ru/downloads>;

Обновление приставки с удаленного сервера

- *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.

Чтобы проверить наличие актуальной версии прошивки на сервере нажмите на кнопку «Проверить наличие обновлений».



Для работы функции проверки обновления необходимо наличие выхода в Интернет.



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

4.3.10.9 Подменю «Сохранение/Загрузка настроек»

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

Сохранение/Загрузка настроек

На этой странице Вы можете сохранить текущие настройки в файл или загрузить их из файла. Также Вы можете сбросить текущие настройки к заводским.

Сохранить настройки:

Загрузить настройки из файла: Файл не выбран

Сбросить настройки к заводским:

- *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».

4.3.10.10 Подменю «Настройка TR-069»

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

Настройка TR-069

Эта страница используется для настройки TR-069 CPE. Здесь Вы можете изменить параметры доступа к ACS.

TR069: Выключено Включено

ACS

URL:

Имя пользователя:

Пароль:

Включить периодические оповещения: Выключено Включено

Интервал периодических оповещений:

Запрос на подключение

Имя пользователя:

Пароль:

Путь:

Порт:

Управление сертификатами

CA Certificate: Файл не выбран

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.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации оборудования ООО «Предприятие «ЭЛТЕКС» Вы можете обратиться в Сервисный центр компании:

Российская Федерация, 630020, г. Новосибирск, ул. Окружная, дом 29В.

Телефоны центра технической поддержки:

+7(383) 274-47-87,

+7(383) 272-83-31,

E-mail: techsupp@eltex.nsk.ru

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

Официальный сайт компании: <http://eltex.nsk.ru>

Технический форум: <http://eltex.nsk.ru/forum>

База знаний: <http://eltex.nsk.ru/support/knowledge>

Центр загрузок: <http://eltex.nsk.ru/support/downloads>