

Абонентский оптический терминал RFT-620

Руководство по эксплуатации

IP-адрес: <http://192.168.1.1>
имя пользователя: user
пароль: user

СОДЕРЖАНИЕ

1.	ВВЕДЕНИЕ	3
2.	ОПИСАНИЕ ИЗДЕЛИЯ.....	4
2.1	Назначение.....	4
2.2	Характеристика устройства	5
2.3	Основные технические параметры	6
2.4	Конструктивное исполнение.....	9
2.4.1	Внешний вид.....	9
2.4.2	Передняя панель	9
2.4.3	Задняя панель	10
2.5	Световая индикация	11
2.6	Перезагрузка/сброс к заводским настройкам.....	12
2.7	Комплект поставки	12
3	НАСТРОЙКА RFT-619 ЧЕРЕЗ WEB-ИНТЕРФЕЙС. ДОСТУП ПОЛЬЗОВАТЕЛЯ	13
3.1	Меню «Информация»	14
3.1.1	Подменю «Информация». Общая информация об устройстве	14
3.1.2	Подменю «WAN». Информация о состоянии WAN интерфейса.....	14
3.1.3	Подменю «Статистика». Информация о прохождении трафика на портах устройства	15
3.1.4	Подменю «Маршруты». Просмотр таблицы маршрутизации.....	16
3.1.5	Подменю «ARP». Просмотр кэша протокола ARP	16
3.1.6	Подменю «DHCP». Активные аренды DHCP	17
3.1.7	Подменю «VoIP». Мониторинг состояния SIP.....	17
3.2	Меню «Настройки»	19
3.2.1	Меню «Настройки PPPoE»	19
3.2.2	Меню «LAN». Настройки локальной сети	20
3.2.3	Меню «NAT». Настройки NAT	21
3.2.3.1	Подменю «Виртуальные серверы». Настройки виртуальных серверов	21
3.2.3.2	Подменю «Триггер портов». Настройки запуска портов	22
3.2.3.3	Подменю «DMZ-хост». Настройки демилитаризованной зоны.....	23
3.2.4	Меню «Безопасность». Настройки безопасности	24
3.2.4.1	Подменю «Фильтрация IP». Настройки фильтрации адресов	24
3.2.4.2	Подменю «Фильтрация MAC». Настройки фильтрации по MAC- адресам	26
3.2.5.2	Подменю «Фильтрация Url». Настройки ограничения доступа к адресам в интернет ..	27
3.3	Меню «Настройка WLAN». Настройки беспроводного соединения.....	29
3.3.1	Подменю «Основные настройки». Общая информация	29
3.3.2	Подменю «Безопасность». Настройка параметров безопасности.....	30
3.3.3	Подменю «Фильтрация по MAC». Настройки фильтрации MAC-адресов.....	32
3.3.4	Подменю «Беспроводной мост». Настройки беспроводного соединения в режиме моста ..	33
3.3.5	Подменю «Дополнительно». Расширенные настройки	34
	ПРИЛОЖЕНИЕ А ВОЗМОЖНЫЕ ПРОБЛЕМЫ И ВАРИАНТЫ ИХ РЕШЕНИЯ	36

1. ВВЕДЕНИЕ

Сеть GPON относится к одной из разновидностей пассивных оптических сетей PON. Это одно из самых современных и эффективных решений задач «последней мили», позволяющее существенно экономить на кабельной инфраструктуре и обеспечивающее скорость передачи информации до 2.5 Гбит/с в направлении к абоненту и 1.25 Гбит/с в направлении от абонента. Использование в сетях доступа решений на базе технологии GPON дает возможность предоставлять конечному пользователю доступ к новым услугам на базе протокола IP совместно с традиционными сервисами.

Основным преимуществом GPON является использование одного станционного терминала (OLT) для нескольких абонентских устройств (ONT). OLT является конвертором интерфейсов Gigabit Ethernet и GPON, служащим для связи сети PON с сетями передачи данных более высокого уровня. ONT предназначен для подключения к услугам широкополосного доступа оконечного оборудования клиентов. Может применяться в жилых комплексах и бизнес-центрах.

Абонентские оптические терминалы RFT-620 рассчитаны на четыре абонентских интерфейса 10/100/1000Base-TX и поддержку интерфейсов FXS, Wi-Fi, USB.

RFT-620 ориентированы на домашних пользователей и небольшие офисы. Являются идеальным решением для обеспечения телефонной связью малонаселенных объектов.

В настоящем руководстве по эксплуатации изложены назначение, основные технические характеристики, правила конфигурирования, мониторинга и смены программного обеспечения оптических абонентских терминалов RFT-620.

2. ОПИСАНИЕ ИЗДЕЛИЯ

2.1 Назначение

RFT-620 – высокопроизводительные абонентские терминалы, предназначенные для связи с вышестоящим оборудованием пассивных оптических сетей и предоставления услуг широкополосного доступа конечному пользователю. Связь с сетями GPON реализуется посредством GPON интерфейса, для подключения оконечного оборудования клиентов служат интерфейсы Ethernet, FXS, USB, WiFi.

Оптические терминалы GPON ONT (Gigabit Ethernet Passive Optical Network) обеспечивают соединение по оптическому каналу с устройством GPON класса OLT (оптический линейный терминал) и соединение до 10/100/1000 Мбит/с с конечным пользователем LAN. Преимуществом технологии GPON является оптимальное использование полосы пропускания. Эта технология является следующим шагом для обеспечения новых высокоскоростных интернет-приложений дома и в офисе. Разработанные для развертывания сети внутри дома или здания, данные устройства ONT обеспечивают надежное соединение с высокой пропускной способностью на дальние расстояния для пользователей, живущих и работающих в удаленных многоквартирных зданиях и бизнес-центрах.

Благодаря встроенному маршрутизатору, устройства обеспечивают возможность подключения оборудования локальной сети к сети широкополосного доступа. К RFT-620 можно подключить до четырех компьютеров, доступ в интернет для которых возможен с помощью встроенных функций NAT/DHCP – сервера.

RFT-620 имеет встроенный адаптер Wi-Fi, который поддерживает технологию 802.11n, что позволяет предоставлять услуги передачи данных беспроводной сети с более высоким качеством сервиса по сравнению с устройствами, поддерживающими стандарт 802.11g, оставаясь при этом обратно совместимым с устройствами с поддержкой 802.11g и 802.11b.

2.2 Характеристика устройства

Устройство имеет следующие интерфейсы:

- 2 порта RJ-11 для подключения аналоговых телефонных аппаратов;
- 1 порт PON SC/APC для подключения к сети оператора;
- 4 порта Ethernet RJ-45 10/100/1000BASE-T LAN;
- Приемопередатчик Wi-Fi 802.11b/g/n;
- Порт USB2.0 для подключения внешних накопителей, сетевого принтера.

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

Устройство поддерживает следующие функции:

- *сетевые функции:*
 - работа в режиме «моста» или «маршрутизатора»;
 - поддержка PPPoE (PAP, CHAP и MSCHAP авторизация);
 - поддержка статического адреса и DHCP (DHCP-клиент на стороне WAN, DHCP-сервер на стороне LAN);
 - поддержка DNS proxy;
 - поддержка DynDNS;
 - поддержка IPSec;
 - поддержка NAT;
 - поддержка NTP;
 - поддержка механизмов качества обслуживания QoS;
 - поддержка IGMP-snooping;
 - поддержка IGMP-proxy;
 - поддержка функции Parental Control.
- *IP-телефония:*
 - Поддержка протокола SIP;
 - Аудиокодеки: G.729 (A/ B),G.711(A/μ), G.723.1 (5,3 Kbps),G.726-24, G.726-32;
 - передача факса: upspeed/pass-through, T.38;
 - эхо компенсация;
 - детектор тишины (VAD) и генератор комфортного шума;
 - обнаружение и генерирование сигналов DTMF;
 - передача DTMF (INBAND, rfc2833, SIP INFO);
- *Дополнительные телефонные сервисы:*
 - обнаружение и генерирование сигналов DTMF;
 - удержание вызова Call Hold;
 - передача вызова – Call Transfer;
 - уведомление о поступлении нового вызова Call Waiting;
 - безусловная переадресация - Forward unconditionally;
 - переадресация по неответу - Forward on "no answer";
 - переадресация по занятости – Forward on Busy;

- определитель номера Caller ID по ETSI FSK;
 - запрет выдачи Caller ID (анонимный звонок) - Anonymous calling;
 - теплая линия - Warmline;
 - гибкий план нумерации;
 - блокировка анонимных звонков - Anonymous call blocking;
 - "не беспокоить" - DND.
- обновление ПО через web-интерфейс;
 - удаленный мониторинг, конфигурирование и настройка:
 - TR-069, web-интерфейс, Telnet.

На рисунке 1 приведена схема применения RFT-620

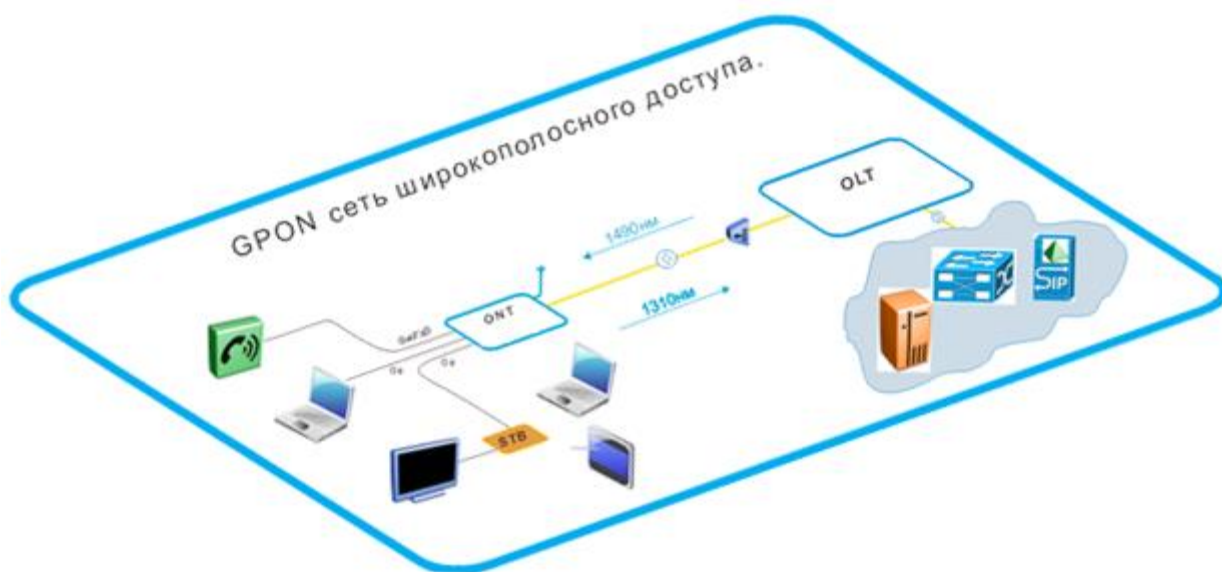


Рисунок 1 – Схема применения RFT-620

2.3 Основные технические параметры

Основные технические параметры терминалов RFT-620 приведены в таблице 2:

Таблица 2. Основные технические параметры

Протоколы VoIP

Поддерживаемые протоколы	SIP
--------------------------	-----

Аудиокодеки

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

Параметры интерфейсов Ethernet LAN

Количество интерфейсов	4
Электрический разъем	RJ-45
Скорость передачи, Мбит/с	Автоопределение, 10/100/1000 Мбит/с, дуплекс/ полудуплекс
Поддержка стандартов	IEEE 802.3i 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3x Flow Control IEEE 802.3 NWay auto-negotiation

Параметры аналоговых абонентских портов

количество портов:	2
прием набора	импульсный/частотный (DTMF)
выдача Caller ID	Есть

Параметры интерфейса PON

Количество интерфейсов PON	1
Поддержка стандартов	ITU-T G.984.x Gigabit-capable passive optical networks (GPON) ITU-T G.988 ONU management and control interface (OMCI) specification IEEE 802.1Q Tagged VLAN IEEE 802.1p Priority Queues IEEE 802.1D Spanning Tree Protocol
Тип разъема	SC/APC соответствует ITUT G.984.2
Среда передачи	оптоволоконный кабель SMF - 9/125, G.652
Коэффициент разветвления	до 1:64
Максимальная дальность действия	до 20 км
Передатчик:	1310Нм
Скорость соединения upstream	1244Mb/s
Мощность передатчика	-2..+3 dBm
Ширина спектра опт. излучения (RMS)	3 nm
Приемник	1490Нм
Скорость соединения downstream	2488Mb/s
Чувствительность приемника	от -3 до -23 dBm

Параметры беспроводного интерфейса Wi-Fi q

Стандарт	IEEE 802.11b/g/n
Частотный диапазон	2.400 ~ 2.497 ГГц

Модуляция	PSK/CCK, DQPSK, DBPSK, OFDM
Скорость передачи данных, Мбит/с	802.11b: 11, 5.5, 2, 1 802.11g: 54, 48, 36, 24, 18,12, 9, 6 802.11n 20MHz BW: 130, 117, 104, 78, 52, 39, 26, 13 802.11n 40MHz BW: 270, 243, 216, 162, 108, 81, 54, 27
Максимальная выходная мощность передатчика	802.11b: 17dBm +/-1.5dBm 802.11g: 15dBm +/-1.5dBm 802.11n: 14.75dBm +/-1.5dBm
MAC-протокол	CSMA/CA модель ACK 32 MAC
Безопасность	64/128-битное WEP-шифрование данных; WPA, WPA2 802.1x AES & TKIP
Поддержка операционной системы	Windows XP 32/64, Windows Vista 32/64, Windows 2000, Windows 7 32/64 Linux, VxWorks
Количество антенн	2 антенны (встроенные)
Коэффициентом усиления антенны	3 dBi
Рабочий диапазон температур	от 0 до +70°C

Управление

Локальное управление	web-интерфейс
Удаленное управление	по протоколу Telnet, TR-069
Ограничение доступа	по паролю

Общие параметры

Питание	адаптер питания 12V DC /220 AC
Потребляемая мощность	не более 18 Вт
Рабочий диапазон температур	от +5 до +40°C
Относительная влажность	до 80%
Габариты	244x142x35мм
Масса	480г

2.4 Конструктивное исполнение

2.4.1 Внешний вид

Устройства RFT-620 выполнены в виде настольного изделия в пластиковом корпусе размерами 244x142x35мм.

Внешний вид RFT-620 приведен на рисунке 2.



Рисунок 2 – Внешний вид RFT-620

2.4.2 Передняя панель

На рисунке 3 представлено конструктивное исполнение передней панели RFT-620

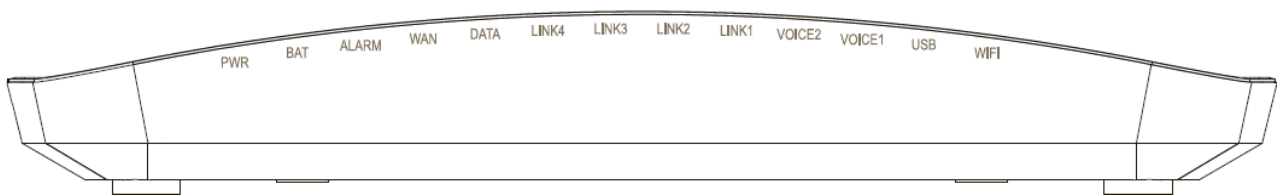


Рисунок 3 – Передняя панель RFT-620

На передней панели RFT-620 расположены следующие световые индикаторы, таблица 1.

Таблица 1 – Описание индикаторов передней панели

Элемент передней панели	Описание
<i>LINK 0...4</i>	Индикаторы работы Ethernet-портов
<i>Alarm</i>	Индикатор неисправностей устройства
<i>WAN</i>	Индикатор подключения к internet
<i>Wi-Fi</i>	Индикатор активности Wi-Fi
<i>VOICE1-2</i>	Индикатор активности портов FXS
<i>USB</i>	Индикатор активности порта USB
<i>PWR</i>	Индикатор питания
<i>BAT</i>	Индикатор подключения UPS

2.4.3 Задняя панель

Конструктивное исполнение задней панели RFT-620 приведено на рисунке 4.

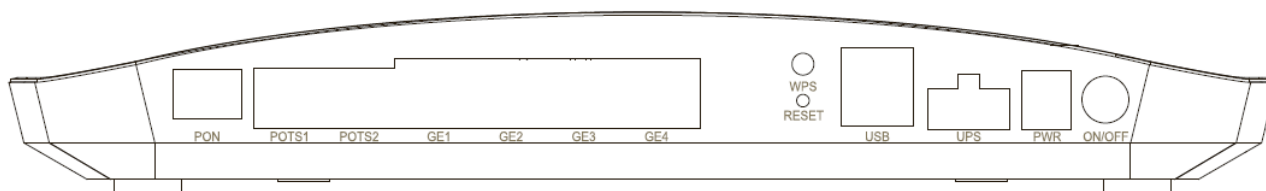


Рисунок 4 – Задняя панель абонентского терминала RFT-620

На задней панели устройства расположены следующие разъемы, таблица 2.

Таблица 2 - Описание разъемов задней панели

Элемент задней панели	Описание
<i>On/Off</i>	Кнопка питания
<i>разъем PWR</i>	Разъем для подключения питания
<i>Reset</i>	Кнопка перезагрузки и сброса на заводские настройки
<i>GE1...GE4</i>	Разъемы RJ45 10/100/1000 Base-T
<i>POTS1, POTS2</i>	Разъемы RJ-11 для подключения аналоговых телефонных аппаратов
<i>USB</i>	Разъем для подключения внешних USB-устройств
<i>WPS</i>	Кнопка активации WPS регистрации
<i>PON</i>	Разъем SC/APC (розетка) оптического интерфейса GPON

2.5 Световая индикация

Текущее состояние устройства отображается при помощи индикаторов **LINK**, **WAN**, **VOICE**, **PWR**, расположенных на передней панели.

Перечень состояний индикаторов приведен в таблице 3.

Таблица 3 – Световая индикация состояния устройства

Индикатор	Состояние индикатора	Состояние устройства
Индикаторы LAN/WAN		
LINK1... 4 (зеленый)	горит	установлено соединение 10/100/1000 Мбит/с
	не горит	нет соединения
	мигает	процесс пакетной передачи данных
WAN	мигает зеленый	установление соединения PPP/DHCP
	горит постоянно зеленый	устройство успешно прошло авторизацию (поднята PPP сессия на интерфейсе wan)
	мигает часто зеленый	идет процесс передачи данных
	горит постоянно красный	ошибка аутентификации
Индикаторы Wi-Fi		
Wi-Fi	не горит	Wi-Fi выключен
	горит постоянно зеленый	Wi-Fi включен
	мигает зеленый	установление соединения Wi-Fi или передача данных по сети Wi-Fi
	мигает красный	включено WPS, идет регистрация устройства или передача данных по сети Wi-Fi
USB	не горит	нет соединения к USB порту
	горит постоянно зеленый	наличие подключения к USB порту
	мигает зеленый	идет процесс передачи данных по USB
PWR (зеленый)	не горит	устройство отключено от сети питания или неисправно
	горит постоянно	питание включено
	мигает	устройство находится в процессе загрузки
VOICE1,VOICE2	горит постоянно зеленый	устройство зарегистрировалось на SIP-сервере
	мигает зеленый	установление соединения или активный разговор
	горит постоянно красный	ошибка конфигурации VoIP
	не горит	порт не сконфигурирован

2.6 Перегрузка/сброс к заводским настройкам

Для перезагрузки устройства нужно однократно нажать кнопку «Reset» на задней панели изделия. Для загрузки устройства с заводскими настройками необходимо нажать и удерживать кнопку «Reset» более 5 сек. При заводских установках IP адрес: LAN - 192.168.1.1, маска подсети – 255.255.255.0.

2.7 Комплект поставки

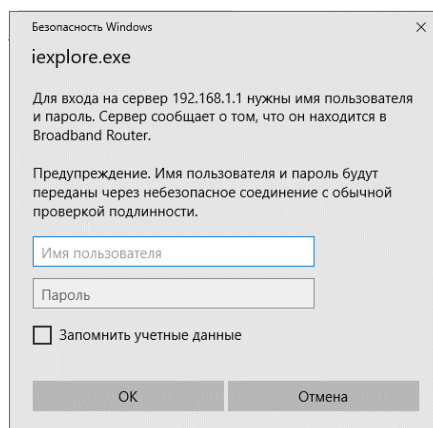
В базовый комплект поставки устройства входят:

- абонентский оптический терминал RFT-620;
- адаптер питания 220/12 В;
- руководство по эксплуатации и гарантийный талон.

3 НАСТРОЙКА RFT-620 ЧЕРЕЗ WEB-ИНТЕРФЕЙС. ДОСТУП ПОЛЬЗОВАТЕЛЯ

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

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



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

3.1 Меню «Информация»

3.1.1 Подменю «Информация». Общая информация об устройстве

Аппаратная версия:	RTO-E682-001
Серийный номер:	48575443A8EA3C97
Количество потоков процессора:	2
Время создания:	190221_1716
Версия программного обеспечения:	2.2.11
Версия загрузчика:	1.0.38-116.232
Версия голосового сервиса:	Voice
Время работы:	0D 0H 6M 59S

Эта информация отражает текущее состояние оптического сигнала.

Состояние:	Нет сигнала (O1)
Уровень приема:	-40.00 дБм
Уровень передачи:	-40.00 дБм

- *Модель* – идентификатор устройства;
- *Серийный номер* – серийный номер устройства;
- *Время создания* – отметка о времени создания программного обеспечения;
- *Версия программного обеспечения* – версия программного обеспечения;
- *Версия загрузчика* – версия начального загрузчика;
- *Версия голосового сервиса* – тип сервиса;
- *Время работы* – время работы устройства с момента последней перезагрузки.

3.1.2 Подменю «WAN». Информация о состоянии WAN интерфейса

В данном меню выводится информация о настройках и состоянии WAN интерфейса.

Информация WAN														
Интерфейс	Описание	Тип	VLAN	IPv6	IGMP прокси	IGMP источник	MLD прокси	MLD источник	NAT	Межсетевой экран	Состояние	IPv4-адрес	IPv6-адрес	MAC Address
ppp0.1	HSI	PPPoE	30	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	Unconfigured			1c:bb:a8:ea:3c:9a

Для просмотра доступна следующая информация о сервисах:

- *Интерфейс* – имя интерфейса;
- *Описание* – описание соединения
- *Тип* – режим работы интерфейса;
- *VLAN* – номер используемого Vlan;
- *MLD прокси* – состояние функции MLD proxy
- *IPv6* – состояние протокола IPv6;
- *Igmp прокси* – состояние функции IGMP proxy;
- *Igmp источник* – состояние функции IGMP Source;
- *NAT* – состояние настроек NAT;
- *Межсетевой экран* – состояние брандмауэра на интерфейсе;

- *Состояние* – текущее состояние WAN интерфейса;
- *IPv4 Address* – адрес, назначенный по протоколу IPv4;
- *IPv6 Address* – адрес, назначенный по протоколу IPv6;

3.1.3 Подменю «Статистика». Информация о прохождении трафика на портах устройства

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

Интерфейс LAN:

Статистика > LAN

Интерфейс	Получено								Передано							
	Общее количество				Мультикаст		Юникаст	Бродкаст	Общее количество				Мультикаст		Юникаст	Бродкаст
	Байты	Пакеты	Ошибки	Потери	Байты	Пакеты	Пакеты	Пакеты	Байты	Пакеты	Ошибки	Потери	Байты	Пакеты	Пакеты	Пакеты
eth0	3938	29	0	0	0	4	25	0	4056	15	0	0	0	0	15	0
eth1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Сбросить статистику

Интерфейс WAN:

Статистика > WAN сервис

Интерфейс	Описание	Получено								Передано							
		Общее количество				Мультикаст		Юникаст	Бродкаст	Общее количество				Мультикаст		Юникаст	Бродкаст
		Байты	Пакеты	Ошибки	Потери	Байты	Пакеты	Пакеты	Пакеты	Байты	Пакеты	Ошибки	Потери	Байты	Пакеты	Пакеты	Пакеты
ppp0.1	HSI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Сбросить статистику

Для обнуления данных и возобновления накопления статистики необходимо нажать «Сбросить статистику».

3.1.4 Подменю «Маршруты». Просмотр таблицы маршрутизации

В меню осуществляется просмотр таблицы маршрутизации.

Информация > Маршруты						
Флаги: U - активен, ! - отбрасывающий, G - шлюз, H - хост, R - динамический восстанавливаемый D - динамический (перенаправление), M - изменённый (перенаправление).						
Назначение	Шлюз	Сетевая маска	Флаг	Метрика	Сервис	Интерфейс
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

- *Назначение* – IP-адрес назначения;
- *Шлюз* – IP-адрес шлюза;
- *Сетевая маска* – маска подсети(Genmask);
- *Флаг* – флаг маршрута:
 - *U* – маршрут активен;
 - *!* – нерабочий маршрут, пакеты будут отброшены;
 - *G* – маршрут использует шлюз (gateway);
 - *H* – адресом назначения является отдельный хост;
 - *R* - восстановленный маршрут;
 - *D* – устанавливается, если маршрут был создан по приходу перенаправляемого сообщения ICMP;
 - *M* – устанавливается, если маршрут был модифицирован перенаправляемым сообщением ICMP;
- *Метрика* – приоритет маршрута;
- *Сервис* – сервис, к которому относится маршрут;
- *Интерфейс* – сетевой интерфейс, к которому относится маршрут.

3.1.5 Подменю «ARP». Просмотр кэша протокола ARP

Эффективность функционирования ARP во многом зависит от ARP-кэша, который присутствует на каждом хосте. В кэше содержатся Internet-адреса и соответствующие им аппаратные адреса. Время жизни каждой записи в кэше 5 минут с момента создания записи.

Информация > ARP			
IP-адрес	Флаги	MAC-адрес	Интерфейс
192.168.1.2	Просмотр завершен	b0:5a:da:9a:3d:6e	br0

- *IP-адрес* – IP-адрес клиента
- *Флаги* – флаги состояния:
 - *Просмотр завершен* – клиент активен;
 - *Просмотр не завершен* – клиент не отвечает на ARP-запросы;
- *MAC-адрес* – MAC-адрес клиента;
- *Интерфейс* – интерфейс, на котором находится клиент.

3.1.6 Подменю «DHCP». Активные аренды DHCP

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

Информация > DHCP

Имя хоста	MAC-адрес	IP-адрес	Истекает через
Vuka	b0:5a:da:9a:3d:6e	192.168.1.2	23 часов, 26 минут, 16 секунд

- *Имя хоста* – имя хоста(сетового устройства);
- *MAC-адрес* – MAC адрес устройства;
- *IP адрес* – адрес устройства в локальной сети, выданный маршрутизатором из пула IP-адресов;
- *Истекает через* – время, через которое истекает аренда данного адреса.

3.1.7 Подменю «VoIP». Мониторинг состояния SIP

Информация > VoIP

Статус	Запущен	
Интерфейс	Loopback	
IP-адрес	127.0.0.1	
Домен	(null)	
Сервер регистрации	0.0.0.0	
Прокси сервер	0.0.0.0	
Исходящий прокси сервер	0.0.0.0	

Аккаунт	0	1
Статус	Disabled	Disabled
Состояние	Disabled	Disabled
Номер	1001	2001
Отображаемое имя	(null)	(null)

- *Статус* – состояние работы голосового демона;
 - *Сервер регистрации* – адрес SIP сервера;
 - *Прокси сервер* – адрес SIP Proxu;
 - *Исходящий прокси сервер* – адрес SIP proxu, через который будет осуществляться передача всех запросов (запросы на SIP Proxu и SIP Registrar будут маршрутизироваться через этот сервер);
-
- *Аккаунт* – номер аккаунта SIP;
 - *Статус* – статус аутентификации;
 - *Состояние* – состояние порта FXS;
 - *Номер* – номер телефона;
 - *Отображаемое имя* – отображаемое имя пользователя при звонках;

3.2 Меню «Настройки»

3.2.1 Меню «Настройки PPPoE»

В меню осуществляется установка имени пользователя и пароля, для подключения по протоколу PPPoE. Имя пользователя и пароль выдаются провайдером, предоставляющим этот сервис.

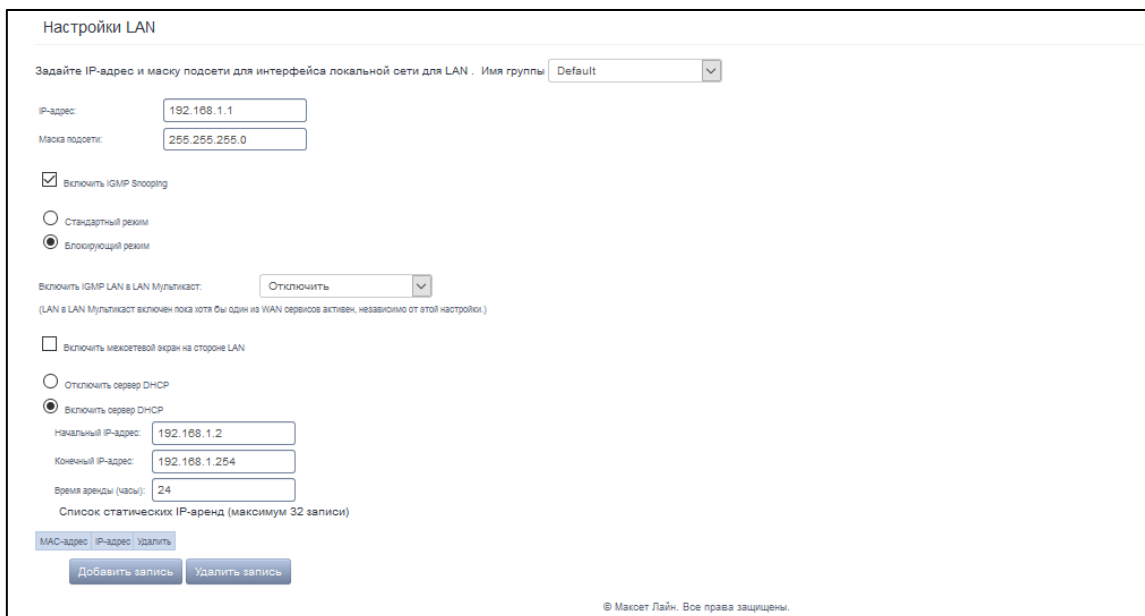
PPP Имя пользователя и Пароль

PPP имя пользователя

PPP пароль

3.2.2 Меню «LAN». Настройки локальной сети

В данном меню производится настройка основных параметров для LAN интерфейса.



- *IP-Адрес* – адрес устройства в локальной сети;
- *Маска подсети* – маска подсети;
- *Включить IGMP Snooping* – при установленном флаге происходит процесс отслеживания сетевого трафика IGMP;
- *Стандартный режим/Блокирующий режим* – режим работы IGMP Snooping: пассивный (Standard) – мультикаст трафик рассылается на все порты; активный (Blocking) – мультикаст трафик посылается только на тот порт, с которого поступил запрос на подключение к мультикаст группе;
- *Включить межсетевой экран на стороне LAN* – при установленном флаге включается брандмауер для локальной сети;

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

- *Включить DHCP Server* – при установленном флаге использовать DHCP сервер (сетевые устройства будут получать IP-адреса динамически, из нижеприведенного диапазона);
- *Начальный IP адрес* – начальный адрес диапазона;
- *Конечный IP Address* – конечный адрес диапазона;
- *Время аренды (часы)* – время аренды адреса (в часах);
- *Список статических IP аренд* – установка соответствия выдаваемых IP-адресов MAC-адресам устройств (привязка). Для добавления записи в таблицу необходимо нажать «Add». Может быть установлено до 32 соответствий.
 - *IP-адрес* – IP-адрес устройства;
 - *MAC-адрес* – MAC-адрес устройства.

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

3.2.3 Меню «NAT». Настройки NAT

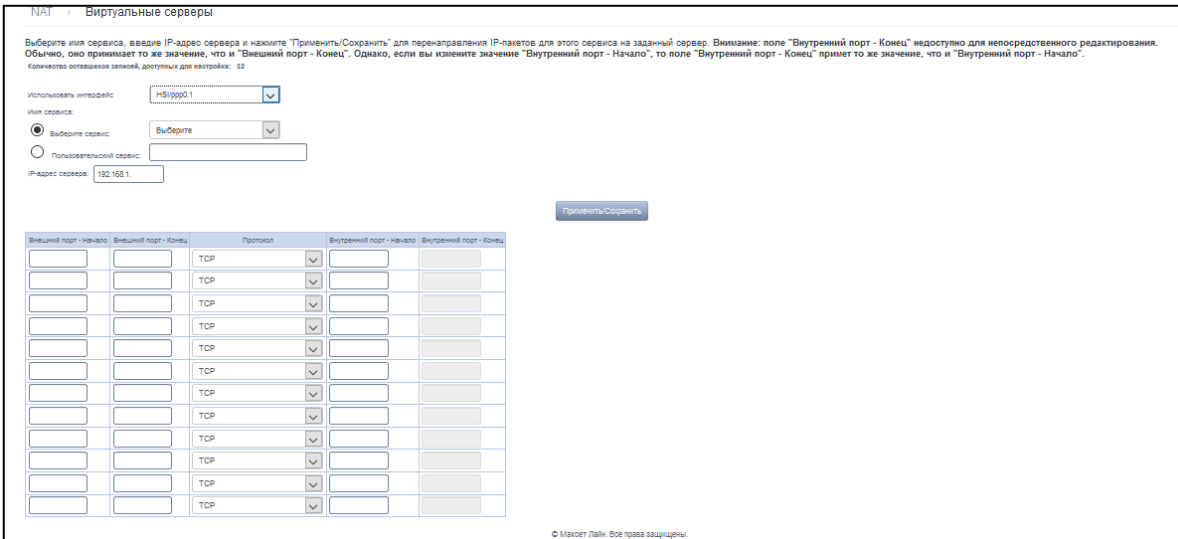
Данные настройки эффективны только при работе устройства в режиме маршрутизатора.

3.2.3.1 Подменю «Виртуальные серверы». Настройки виртуальных серверов

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

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

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



- *Использовать интерфейс* – выбор используемого интерфейса. Для использования доступны только интерфейсы, настроенные на работу в режиме маршрутизатора с разрешенной трансляцией сетевых адресов;
- *Имя сервиса* – настройки сервиса:
 - *Выберите сервис* – выбор преднастроенного правила.
 - *Пользовательский сервис* – создать свои, не указанные в списке «*Выберите сервис*», правила.
- *IP-адрес сервера* – IP-адрес сервера, находящегося в локальной сети;
- *Внешний порт-начало* – начальный внешний порт диапазона портов, на которые осуществляется обращение из Интернета;
- *Внешний порт-конец* – конечный внешний порт диапазона портов, на которые осуществляется обращение из Интернета;
- *Протокол* – выбор сетевого протокола;

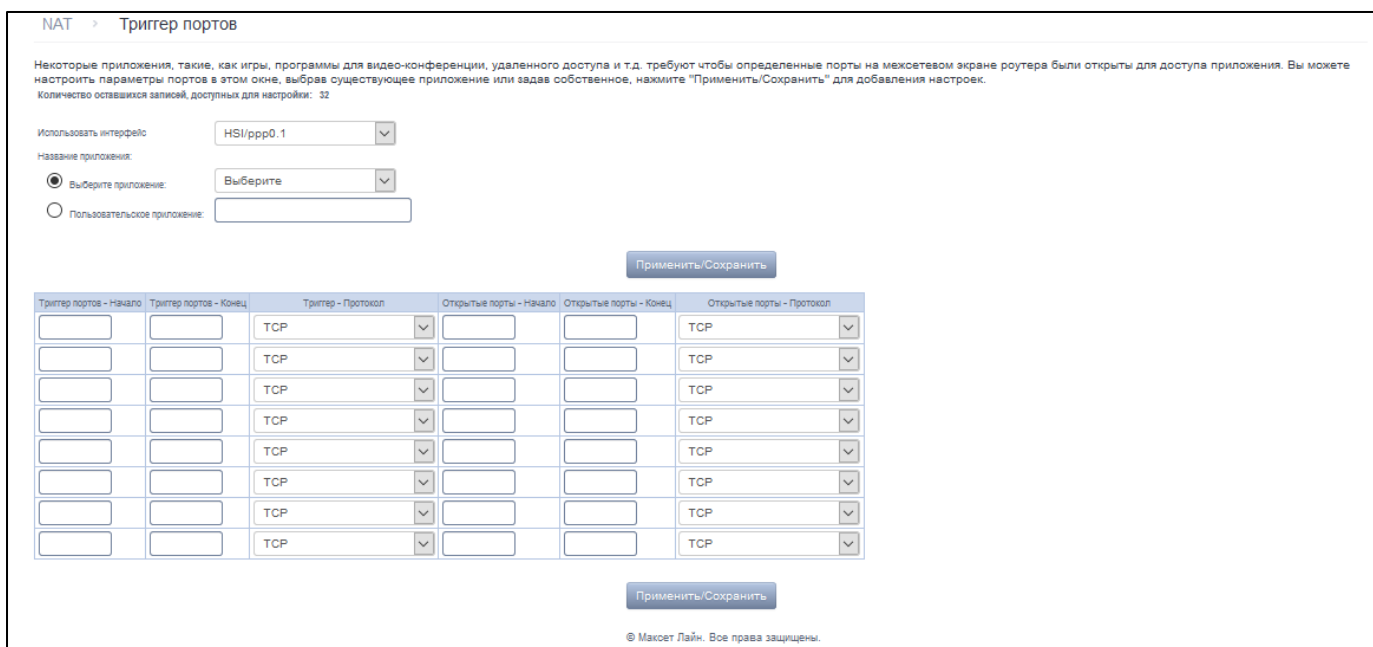
- *Внутренний порт-начало* – начальный внутренний порт диапазона портов, на который будет переадресовываться трафик с внешнего порта маршрутизатора;
- *Внутренний порт-конец* – конечный внутренний порт диапазона портов, на который будет переадресовываться трафик с внешнего порта маршрутизатора;

Для принятия и сохранения изменений необходимо нажать кнопку «*Применить/Сохранить*».

3.2.3.2 Подменю «*Триггер портов*». Настройки запуска портов

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

Для добавления правил в таблицу необходимо нажать кнопку «*Добавить*», удаление происходит нажатием кнопки «*Удалить*» при установленном одноименном флаге напротив выбранного правила.



NAT > Триггер портов

Некоторые приложения, такие, как игры, программы для видео-конференции, удаленного доступа и т.д. требуют чтобы определенные порты на межсетевом экране роутера были открыты для доступа приложения. Вы можете настроить параметры портов в этом окне, выбрав существующее приложение или задав собственное, нажмите "Применить/Сохранить" для добавления настроек.
Количество оставшихся записей, доступных для настройки: 32

Использовать интерфейс:

Название приложения:

Выберите приложение:

Пользовательское приложение:

Триггер портов - Начало	Триггер портов - Конец	Триггер - Протокол	Открытые порты - Начало	Открытые порты - Конец	Открытые порты - Протокол
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP

© Махсет Лайн. Все права защищены.

- *Использовать интерфейс* – выбор используемого интерфейса. Для использования доступны только интерфейсы, настроенные на работу в режиме маршрутизатора с разрешенной трансляцией сетевых адресов;
- *Название приложения* – настройки приложения:
 - *Выберите приложение* – выбор преднастроенного правила.
 - *Пользовательское приложение* – создать свои, не указанные в списке «*Выберите приложение*», правила.

В отличие от функции «*Виртуальный сервер*» здесь нет необходимости фиксировано задавать IP-адрес компьютера в LAN.

- *Триггер портов-начало* – начальный порт диапазона портов, которые осуществляют функцию триггера;
- *Триггер портов-конец* – конечный порт диапазона портов, которые осуществляют функцию триггера;
- *Триггер-Протокол* – протокол, используемый для триггера;

- *Открытые порты-начало* – начальный порт диапазона портов, которые маршрутизатор будет открывать;
- *Открытые порты-конец* – конечный порт диапазона портов, которые маршрутизатор будет открывать;
- *Открытые порты-Протокол* – используемый протокол для открываемых портов.

Для принятия и сохранения изменений необходимо нажать кнопку «*Применить/Сохранить*».

3.2.3.3 Подменю «DMZ-хост». Настройки демилитаризованной зоны

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

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

NAT > Хост DMZ

Роутер будет перенаправлять IP-пакеты, не принадлежащие ни одному приложению, настроенному на Виртуальных серверах, с интерфейса WAN на хост DMZ.

Введите IP-адрес компьютера и нажмите "Применить" для активации хоста DMZ.

Очистите поле IP-адреса и нажмите "Применить" для деактивации хоста DMZ.

IP-адрес хоста DMZ:

Для принятия и сохранения изменений необходимо нажать кнопку «*Применить/Сохранить*».

3.2.4 Меню «Безопасность». Настройки безопасности

В данном разделе проводится настройка параметров безопасности устройства.

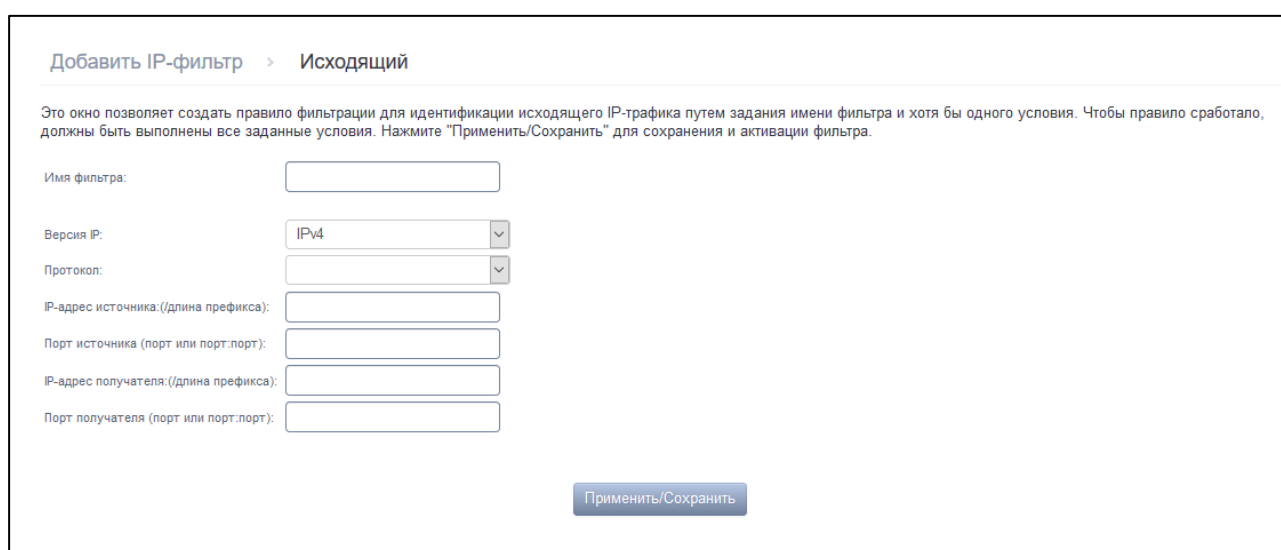
3.2.4.1 Подменю «Фильтрация IP». Настройки фильтрации адресов

Функция «Фильтрация IP» позволяет фильтровать проходящий через маршрутизатор трафик по IP-адресам и портам.

Настройки фильтрации исходящего трафика:

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

Для добавления нового правила фильтрации необходимо нажать кнопку «Добавить».



Добавить IP-фильтр > Исходящий

Это окно позволяет создать правило фильтрации для идентификации исходящего IP-трафика путем задания имени фильтра и хотя бы одного условия. Чтобы правило сработало, должны быть выполнены все заданные условия. Нажмите "Применить/Сохранить" для сохранения и активации фильтра.

Имя фильтра:

Версия IP:

Протокол:

IP-адрес источника: (/длина префикса):

Порт источника (порт или порт:порт):

IP-адрес получателя: (/длина префикса):

Порт получателя (порт или порт:порт):

- *Имя фильтра* – текстовое описание фильтра;
- *Версия IP* – выбор версии протокола IP;
- *Протокол* – выбор протокола (TCP/UDP, TCP, UDP, ICMP);
- *IP-адрес источника [/длина префикса]* – IP-адрес источника (через слэш возможно указать длину префикса);
- *Порт источника (порт или порт:порт)* – порт источника или диапазон портов через двоеточие;
- *IP-адрес получателя [/длина префикса]* – IP-адрес места назначения (через слэш возможно указать длину префикса);
- *Порт получателя (порт или порт:порт)* – порт места назначения или диапазон портов через двоеточие;

Для принятия и сохранения настроек необходимо нажать кнопку «Применить/Сохранить».

Настройки фильтрации входящего трафика (Incoming):

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

Для добавления нового правила фильтрации необходимо нажать кнопку «Добавить».

Добавить IP-фильтр > Входящий

Это окно позволяет создать правило фильтрации для идентификации входящего IP-трафика путем задания имени фильтра и хотя бы одного условия. Чтобы правило сработало, должны быть выполнены все заданные условия. Нажмите "Применить/Сохранить" для сохранения и активации фильтра.

Имя фильтра:

Версия IP:

Протокол:

IP-адрес источника [/длина префикса]:

Порт источника (порт или порт:порт):

IP-адрес получателя [/длина префикса]:

Порт получателя (порт или порт:порт):

WAN Интерфейсы (настроенные в режиме маршрутизатора с включенным межсетевым экраном) и LAN-интерфейсы
Для применения правила выберите один или несколько интерфейсов WAN/LAN, отображенных ниже.

Выбрать все br0/br0

- *Имя фильтра* – текстовое описание фильтра;
- *Версия IP* – выбор версии протокола IP;
- *Протокол* – выбор сетевого протокола;
- *IP-адрес источника [/длина префикса]* – IP-адрес источника (через слэш возможно указать длину префикса);
- *Порт источника (порт или порт:порт)* – порт/порты источника;
- *IP-адрес получателя [/длина префикса]* – IP-адрес места назначения (через слэш возможно указать длину префикса);
- *Порт получателя (порт или порт:порт)* – порт/порты места назначения;

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

- *Выбрать все* – при установленном флаге выбрать все возможные интерфейсы. Либо выбрать интерфейс из приведенного списка, установив флаг напротив.

Для принятия и сохранения настроек необходимо нажать кнопку «*Применить/Сохранить*».

3.2.4.2 Подменю «Фильтрация MAC». Настройки фильтрации по MAC- адресам

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

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

Фильтрация MAC

Фильтрация MAC действует только для ATM PVC настроенных в режиме Моста. **ОТПРАВЛЕНЫ** означает что все фреймы на уровне MAC будут **ОТПРАВЛЕНЫ** исключая любые совпадения указанных правил в следующей таблице. **БЛОКИРОВАННЫ** означает что все фреймы на уровне MAC будут **БЛОКИРОВАННЫ** исключая любые совпадения указанных правил в следующей таблице.

Ограничения фильтрации MAC для каждого интерфейса:
Внимание: изменение одного ограничения для одного из интерфейсов приведет к тому, что все другие ограничения для этого интерфейса, будут УДАЛЕНЫ АВТОМАТИЧЕСКИ! Вы должны будете снова создать новые правила ограничений.

Интерфейс	Ограничение	Изменить
veip0.1	FORWARD	<input type="checkbox"/>

Выберите Добавить или Удалить для настройки правил фильтрации MAC.

Интерфейс	Протокол	MAC назначения	MAC источника	Направление фреймов	Удалить
<input type="button" value="Добавить"/> <input type="button" value="Удалить"/>					

Для изменения режима (политики) работы, установите флаг на против необходимого интерфейса и нажмите кнопку «Изменить». Доступно два варианта работы: FORWARDED и BLOCKED.

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

Добавить MAC-фильтр

Создайте фильтр для идентификации кадров MAC-уровня путем указания хотя бы одного условия. Если указаны несколько условий, они все будут проверяться. Нажмите "Применить" для сохранения и активации фильтра.

Тип протокола:

MAC-адрес получателя:

MAC-адрес источника:

Направление кадра:

WAN -интерфейсы (только настроенные в режим "Моста")

- *Тип протокола* – выбор протокола (PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP);
- *MAC-адрес получателя* – MAC-адрес получателя;
- *MAC-адрес источника* – MAC-адрес отправителя;
- *Направление кадра* – направление передачи (LAN<=>WAN, LAN=>WAN, WAN=>LAN);
- *WAN интерфейсы (только настроенные в режиме моста)* – выбор WAN интерфейса из выпадающего списка (доступны только интерфейсы, работающие в режиме моста).

Для принятия и сохранения настроек необходимо нажать кнопку «Применить/Сохранить».

3.2.5 Меню «Родительский контроль». «Родительский контроль» – настройки ограничения

3.2.5.1 Подменю «Ограничение по времени». Настройки ограничения продолжительности сеансов

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

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

Ограничение доступа по времени

Эта страница позволяет добавить ограничение по времени дня для определенных устройств в Локальной сети, подключенных к роутеру. Для ограничения введите MAC-адрес устройства в LAN. Чтобы найти MAC-адрес компьютера, работающего под ОС Windows, наберите в командной строке команду "ipconfig /all".

Имя пользователя

MAC-адрес
 MAC-адрес (хх:хх:хх:хх:хх:хх)

Дни недели	Пнд	Втр	Срд	Чтв	Птн	Сбт	Вск
Нажмите для выбора	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Начало времени блокировки (чч:мм)

Окончание времени блокировки (чч:мм)

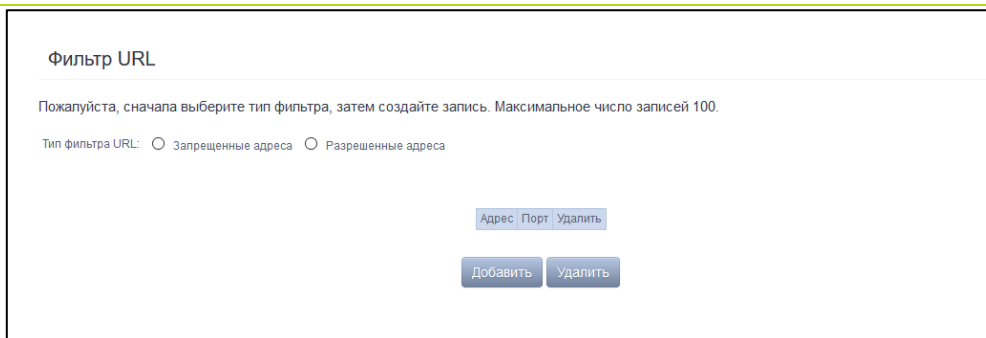
- *Имя пользователя* – имя пользователя;
- *MAC-адрес* – автоматически определенный MAC-адрес компьютера, для которого задается расписание;
- *MAC-адрес (хх:хх:хх:хх:хх:хх)* – заданный вручную MAC-адрес компьютера, для которого определяется расписание;
- *Дни недели* – дни недели, запрещенные для доступа в интернет;
- *Начало времени блокировки (чч:мм)* – время начала блокировки в формате ЧЧ:ММ;
- *Окончание времени блокировки (чч:мм)* – время окончания блокировки в формате ЧЧ:ММ;

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

Для добавления настроек в таблицу необходимо нажать кнопку «Применить/Сохранить».

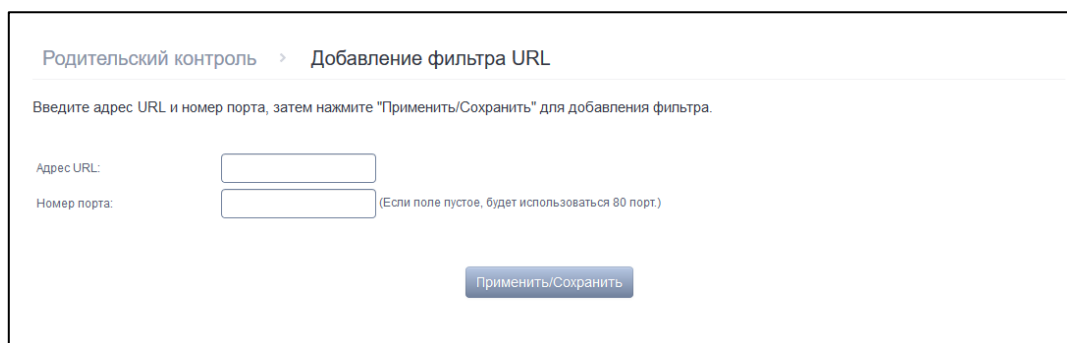
3.2.5.2 Подменю «Фильтрация Url». Настройки ограничения доступа к адресам в интернет

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



- *Тип фильтра URL* – тип списка:
 - *Запрещенные адреса* – адреса, доступ к которым запрещен;
 - *Разрешенные адреса* – адреса, доступ к которым разрешен.

Для добавления нового адреса в список необходимо установить флаг напротив требуемого типа списка (*Тип фильтра URL*) и нажать кнопку «*Добавить*».



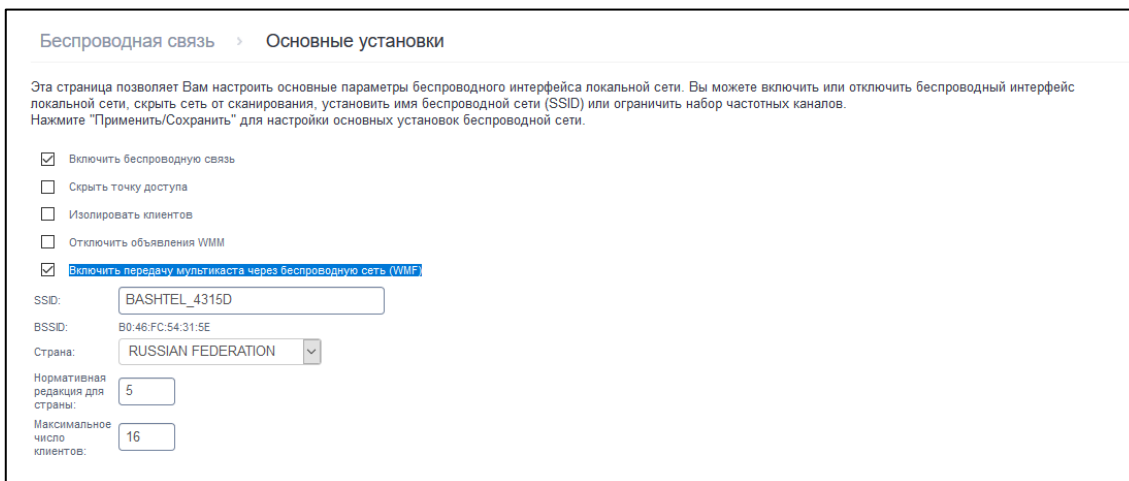
- *Адрес URL* – URL адрес, к которому необходимо применить правило фильтрации;
- *Номер порта* – номер порта (если оставить поле пустым, будет использоваться 80 порт).

Для добавления настроек в таблицу необходимо нажать кнопку «*Применить/Сохранить*».

3.3 Меню «*Настройка WLAN*». Настройки беспроводного соединения

3.3.1 Подменю «*Основные настройки*». Общая информация

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



- *Включить беспроводную связь* – включить Wi-Fi на устройстве;
- *Скрыть точку доступа* – скрытый режим работы точки доступа (в данном режиме SSID беспроводной сети не будет широкоэвещательно распространяться маршрутизатором);
- *Изолировать клиентов* – при установленном флаге беспроводные клиенты не смогут взаимодействовать друг с другом;
- *Отключить объявления WMM* – отключить WMM (Wi-Fi Multimedia – QoS для беспроводных сетей). Стоит включить, если подключаются какие-либо мультимедийные устройства по Wi-Fi (по умолчанию включена), позволяет повысить мультимедийный трафик;
- *Включить передачу мультимедиа через беспроводную сеть (WMM)* – включить WMM;
- *SSID – Service Set Identifier* – назначить имя беспроводной сети (ввод с учетом регистра клавиатуры). SSID является эквивалентом имени беспроводной сети и он задан с префиксом и имеет уникальный номер\имя. Вы можете либо оставить значение SSID по умолчанию или изменить его, введя имя в свободной форме (до 32 символов). По умолчанию на устройстве установлено имя беспроводной сети (SSID) ROSTELECOM-aaaaa, где aaaaa - 5 последних цифр серийного номера устройства. Серийный номер указан в наклейке на корпусе устройства;
- *BSSID* – MAC-адрес точки доступа;
- *Страна* – задать местоположение (страну);
- *Максимальное количество клиентов* – установить максимально возможное количество одновременных беспроводных подключений;

Беспроводная связь – гостевые/виртуальные точки доступа:

Включено	SSID	Скрытая	Изолировать клиентов	Отключить объявления WMM	Включить WMMF	Максимальное число клиентов	BSSID
<input type="checkbox"/>	wl0_Guest1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	16	N/A
<input type="checkbox"/>	wl0_Guest2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	16	N/A
<input type="checkbox"/>	wl0_Guest3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	16	N/A

© Максет Лайн. Все права защищены.

Установите флажок «Включено», чтобы включить гостевую SSID. Гостевая SSID должна отличаться от основного SSID и остальных гостевых SSID. Установите флажок «Скрытая», чтобы ваша гостевая беспроводная сеть стала невидимой.

Для принятия и сохранения изменений необходимо нажать кнопку «*Применить/Сохранить*».

3.3.2 Подменю «Безопасность». Настройка параметров безопасности

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

Беспроводная связь > Безопасность

Эта страница позволяет Вам настроить параметры безопасности беспроводного интерфейса локальной сети. Вы можете задать конфигурацию вручную или с помощью "Защищенной установки Wi-Fi" (WPS).
Внимание: когда STA PIN и авторизованные MAC пусты, будет использоваться PBC. Если включено Скрыть точку доступа или MAC-фильтр пуст и активирован, WPS2 будет отключен.

Настройка WPS

Включить WPS:

Ручная настройка точки доступа

Вы можете установить способ аутентификации, выбрать алгоритм шифрования, установить стойкость шифрования и задать ключи к беспроводной сети. Когда закончите нажмите "Применить/Сохранить".

Выберите SSID:

Аутентификация:

Защищенные управляющие кадры:

WPA/WPA2 пароль: [Чтобы отобразить, нажмите здесь](#)

Интервал групповой системы ключа WPA:

Шифрование WPA:

Шифрование WEP:

Ручная настройка точки доступа:

- *Выберите SSID*– идентификатор беспроводной сети, для которой производится настройка параметров безопасности;
- *Аутентификация* – установить режим сетевой аутентификации из перечня в выпадающем списке:
 - **Открытая** – защита беспроводной сети отсутствует (в этом режиме может использоваться только WEP-ключ);
 - **Разделенная** – общий (режим позволяет пользователям получать аутентификацию по их SSID или WEP-ключу);
 - **802.1x** – включает стандарт 802.1x(позволяет пользователям аутентифицироваться с использованием сервера аутентификации RADIUS, для шифрования данных используется WEP-ключ);

- *IP-адрес сервера RADIUS* – IP-адрес RADIUS-сервера;
 - *Порт RADIUS* – номер порта RADIUS-сервера. По умолчанию установлен порт 1812;
 - *Ключ RADIUS* – секретный ключ для доступа к RADIUS-серверу;
- **WPA2** – включает стандарт WPA (режим использует протокол WPA и требует использования сервера аутентификации RADIUS);
- *Предварительная аутентификация WPA2* – предварительная проверка подлинности беспроводного клиента на других беспроводных точках доступа в используемом диапазоне. В течение проверки связь осуществляется через текущую беспроводную точку доступа;
 - *Интервал повторной аутентификации* – период повторной проверки подлинности. Определяет, как часто точка доступа посылает сообщение и требует от клиентов ответа, содержащего правильные данные безопасности;
 - *Интервал групповой смены ключа WPA* – интервал в секундах между сменой ключей шифрования WPA, используется для повышения уровня безопасности беспроводной сети. Если в смене ключей нет необходимости, оставьте в поле нулевое значение;
 - *IP-адрес сервера RADIUS* – IP-адрес RADIUS-сервера;
 - *Порт RADIUS* – номер порта RADIUS-сервера. По умолчанию установлен порт 1812;
 - *Ключ RADIUS* – секретный ключ для доступа к RADIUS-серверу;
 - *Шифрование WPA* – выбор метода шифрования данных WPA/WAPI: TKIP+AES, AES;
 - *TKIP* – протокол шифрования, используемый для WPA. Обладает более эффективным механизмом управления ключами по сравнению с WEP;
 - *AES* – алгоритм 128 битного блочного шифрование с ключом 128/192/256 бит, используется обычно для WPA2);
- **WPA2-PSK** – включает стандарт WPA-PSK (режим использует протокол WPA, но не требует использования сервера аутентификации RADIUS). Рекомендуется как самый безопасный вариант защиты беспроводного подключения;
- *WPA/WAPI пароль* – секретная фраза. Установка пароля, строка 8-63 символа ASCII или 64 Нех символа (0-F), ключ сети чувствителен к регистру вводимых символов. Для просмотра секретной фразы необходимо нажать на ссылку «*Чтобы отобразить, нажмите здесь*», пароль будет показан во всплывающем окне;
 - *Интервал групповой смены ключа WPA* – интервал в секундах между сменой ключей шифрования WPA, используется для повышения уровня безопасности беспроводной сети. Если в смене ключей нет необходимости, оставьте в поле нулевое значение.
- **Смешанная WPA2/WPA** – включает комбинацию WPA2/WPA (данный режим шифрования использует протоколы WPA2 и WPA, требует использования сервера аутентификации RADIUS);
- *Предварительная аутентификация WPA2* – предварительная проверка подлинности беспроводного клиента на других беспроводных точках доступа в используемом диапазоне. В течение проверки связь осуществляется через текущую беспроводную точку доступа;
 - *Интервал повторной аутентификации* – период повторной проверки подлинности. Определяет, как часто точка доступа посылает сообщение и требует от клиентов ответа, содержащего правильные данные безопасности;
 - *Интервал групповой смены ключа WPA* – интервал в секундах между сменой ключей шифрования WPA, используется для повышения уровня безопасности беспроводной сети. Если в смене ключей нет необходимости, оставьте в поле нулевое значение;
 - *IP-адрес сервера RADIUS* – IP-адрес RADIUS-сервера;
 - *Порт RADIUS* – номер порта RADIUS-сервера. По умолчанию установлен порт 1812;
 - *Ключ RADIUS* – секретный ключ для доступа к RADIUS-серверу;
 - *Шифрование WPA* – выбор метода шифрования данных WPA/WAPI: TKIP+AES, AES;

- **Смешанная WPA2/WPA-PSK** – включает комбинацию WPA2/WPA-PSK (этот режим шифрования использует протоколы WPA2-PSK и WPA-PSK, не требует использования сервера аутентификации RADIUS)
 - *WPA/WAPI пароль* – секретная фраза. Установка пароля, строка 8-63 символа ASCII. Для просмотра секретной фразы необходимо нажать на ссылку «*Чтобы отобразить, нажмите здесь*», пароль будет показан во всплывающем окне.
 - *Интервал групповой смены ключа WPA* – интервал в секундах между сменой ключей шифрования WPA, используется для повышения уровня безопасности беспроводной сети. Если в смене ключей нет необходимости, оставьте в поле нулевое значение;
 - *Шифрование WPA* – выбор метода шифрования данных WPA/WAPI: TKIP+AES, AES:

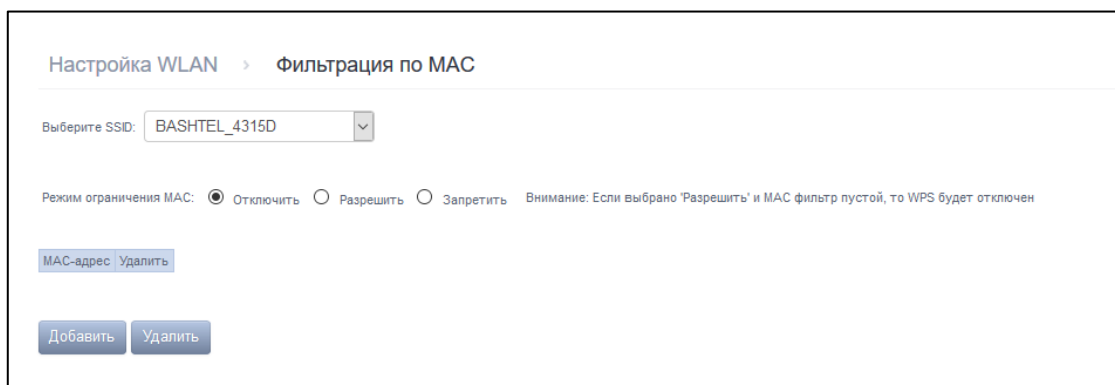
Убедитесь, что беспроводной адаптер компьютера поддерживает выбранный тип шифрования.

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

Для принятия и сохранения изменений необходимо нажать кнопку «*Применить/Сохранить*».

3.3.3 Подменю «*Фильтрация по MAC*». Настройки фильтрации MAC-адресов

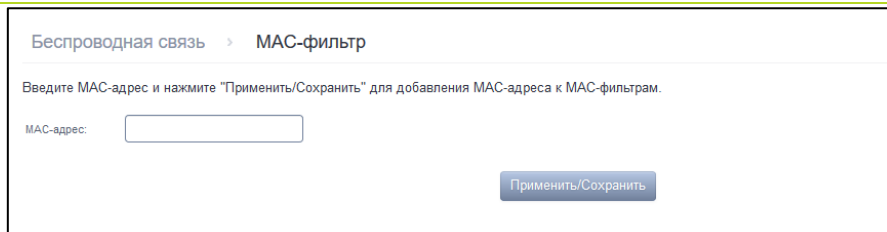
Функция «*Фильтрация по MAC*» позволяет разрешить или запретить доступ беспроводных клиентов к беспроводной сети на базе их MAC-адресов.



The screenshot shows the 'Настройка WLAN > Фильтрация по MAC' (WLAN Settings > MAC Filtering) page. At the top, there is a dropdown menu for 'Выберите SSID:' with 'BASHTEL_4315D' selected. Below this, there are three radio buttons for 'Режим ограничения MAC:': 'Отключить' (selected), 'Разрешить', and 'Запретить'. A note reads: 'Внимание: Если выбрано 'Разрешить' и MAC фильтр пустой, то WPS будет отключен'. Below the radio buttons is a table with one row containing a 'MAC-адрес' and a 'Удалить' button. At the bottom of the page are two buttons: 'Добавить' and 'Удалить'.

- *Выберите SSID* – выбрать идентификатор беспроводной сети, для которой будет создано правило;
- *Режим ограничения MAC* – выбор режима фильтрации по MAC-адресам:
 - *Отключить* – не использовать фильтр;
 - *Разрешить* – фильтр по разрешенным адресам;
 - *Запретить* – фильтр по запрещенным адресам;

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

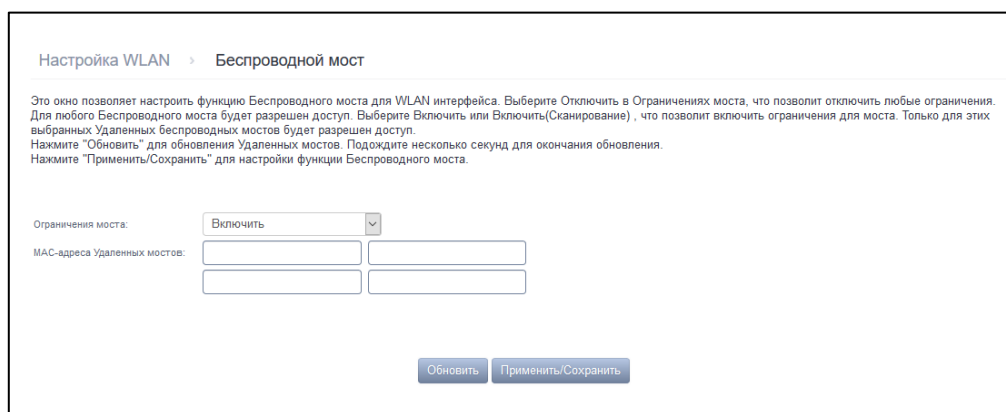


Для принятия изменений необходимо нажать кнопку «*Применить/Сохранить*».

3.3.4 Подменю «Беспроводной мост». Настройки беспроводного соединения в режиме моста

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

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



- *Ограничения моста* – выбор режима работы моста:
 - *Включить* – включить фильтр по MAC-адресам(разрешены только заданные адреса);
 - *Включить (Сканирование)* – поиск удаленных мостов;
 - *Отключить* – ограничения по MAC-адресам отсутствуют;
- *MAC-адреса удаленных мостов* – адреса удаленных мостов.

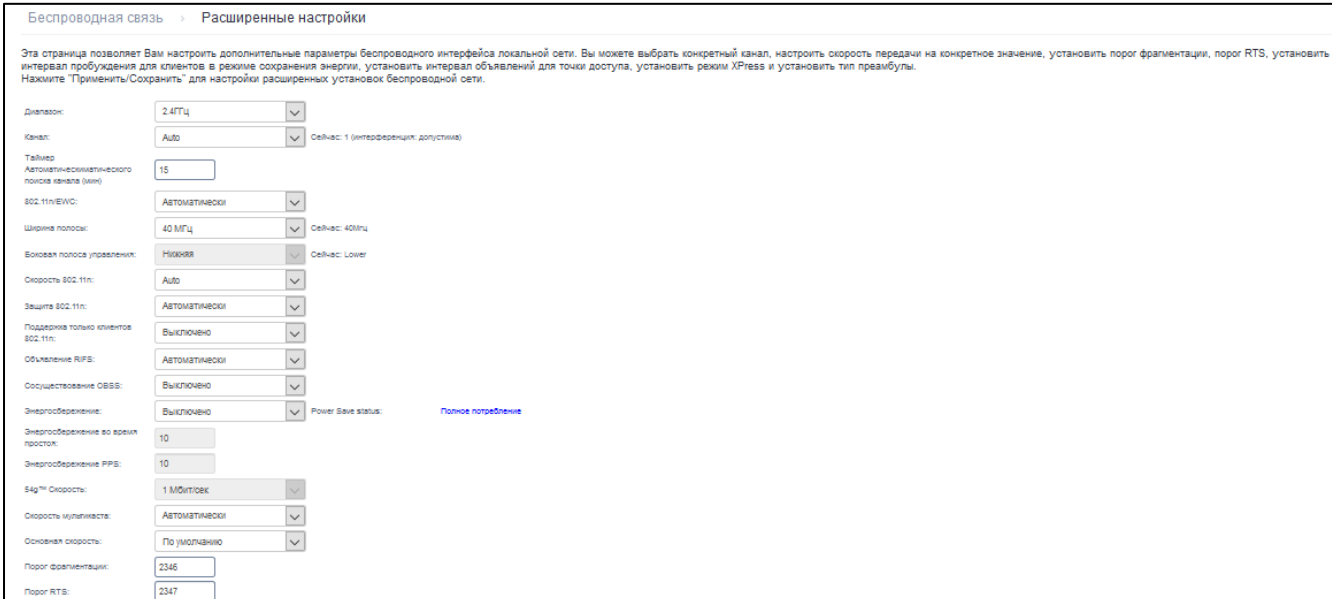
В режиме моста маршрутизатор не поддерживает функцию Wi-Fi Multimedia (WMM).

Для обновления списка доступных удаленных мостов необходимо нажать «*Обновить*».

Для принятия и сохранения изменений необходимо нажать кнопку «*Применить/Сохранить*».

3.3.5 Подменю «Дополнительно». Расширенные настройки

В данном меню производится расширенные настройки беспроводной сети:



Беспроводная связь > Расширенные настройки

Эта страница позволяет Вам настроить дополнительные параметры беспроводного интерфейса локальной сети. Вы можете выбрать конкретный канал, настроить скорость передачи на конкретное значение, установить порог фрагментации, порог RTS, установить интервал пробуждения для клиентов в режиме сохранения энергии, установить интервал объявлений для точки доступа, установить режим XPress и установить тип прамбулы. Нажмите "Применить/Сохранить" для настройки расширенных установок беспроводной сети.

Диапазон: 2.4ГГц

Канал: Авто (Интерференция: допустима) Сейчас: 1 (Интерференция: допустима)

Таймер Автоматического поиска канала (мин): 15

802.11n/EWC: Автоматически

Ширина полосы: 40 МГц (Сейчас: 40МГц)

Боковая полоса управления: Низкая (Сейчас: Lower)

Скорость 802.11n: Авто

Защита 802.11n: Автоматически

Поддержка только клиентов 802.11n: Выключено

Объявление RIFS: Автоматически

Сосуществование OBSS: Выключено

Энергосбережение: Выключено (Power Save status: Полное потребление)

Энергосбережение во время простоя: 10

Энергосбережение PPS: 10

54g™ Скорость: 1 Мбит/сек

Скорость мультиплекса: Автоматически

Основная скорость: По умолчанию

Порог фрагментации: 2346

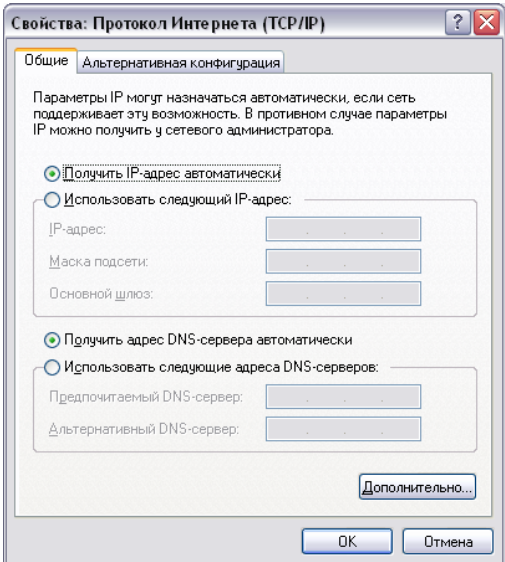
Порог RTS: 2347

- *Диапазон* – установка частотного диапазона;
- *Канал* – устанавливает рабочий канал для маршрутизатора. При наличии помех или проблем в работе беспроводной сети изменение канала может способствовать их устранению. Рекомендуется установить значение "Auto" во избежание помех, вызываемых работой смежных сетей;
- *Таймер автоматического поиска канала (мин)* – время в минутах, через которое маршрутизатор будет искать более оптимальный беспроводный канал. Параметр доступен, если установлен Auto выбор канала (0 – выключить);
- *802.11n/EWC* – режим совместимости с оборудованием 802.11n Draft2.0 и EWC (Enhanced Wireless Consortium);
- *Ширина полосы* – установка полосы пропускания 20МГц или 40 МГц. В режиме 40 МГц используются две смежные полосы по 20 МГц для увеличения пропускной способности канала;
- *Боковая полоса управления* – выбор второго канала (Lower или Upper) в режиме 40 МГц;
- *Скорость 802.11n* – установка скорости соединения;
- *Защита 802.11n* – при включении увеличится безопасность, но уменьшится пропускная способность;
- *Поддержка только клиентов 802.11n* – при включении клиентам 802.11b/g будет запрещен доступ к устройству;
- *Объявление RIFS* – (Reduced Interframe Space) уменьшение интервала между блоками данных (PDUs), повышает эффективность Wi-Fi ;
- *Сосуществование OBSS* – настройка толерантности при выборе режима работы (20МГц или 40МГц). Если параметр в состоянии "Включено" – будет выбран оптимальный режим работы устройства, учитывая "Ширину полосы", иначе режим работы будет зависеть только от параметра "Ширина полосы";
- *Энергосбережение* – отключение приема на одной из антенн устройства в целях энергосбережения;
- *Энергосбережение во время простоя* – период времени, в течении которого интенсивность трафика должна быть ниже PPS, для включения режима энергосбережения;
- *Энергосбережение PPS* – верхняя граница параметра PPS (packet per second). Если в течение времени, определенного параметром «Энергосбережение во время простоя», интенсивность пакетов на интерфейсе WLAN не превышает данную величину, включается режим энергосбережения;
- *54g™ скорость* – установка скорости в режиме совместимости с устройствами 54g™;

- *Скорость мультикаста* – установка скорости трафика при многоадресной передаче;
- *Основная скорость* – базовая скорость передачи;
- *Порог фрагментации* – установка порога фрагментации в байтах. Если размер пакета будет превышать заданное значение, он будет фрагментирован на части подходящего размера;
- *Порог RTS* – если сетевой пакет меньше, чем установленное пороговое значение RTS, механизм RTS/CTS (механизм соединения по каналу с использованием сигналов готовности к передаче/готовности к приему) задействован не будет;
- *Интервал DTIM* – временной интервал, по истечении которого широковещательные и многоадресные пакеты, помещенные в буфер, будут доставлены беспроводным клиентам;
- *Интервал объявлений* – период отправки информационного пакета в беспроводную сеть, сигнализирующего о том, что точка доступа активна;
- *Общее максимальное число клиентов* – максимальное количество беспроводных клиентов;
- *XPress™ технология* – использование позволяет повысить пропускную способность до 27% в сетях стандарта 802.11g. А в смешанных сетях 802.11g и 802.11b использование XPress™ Technology может повысить пропускную способность до 75%;
- *Мощность передачи* – определяется мощность сигнала точки доступа;
- *WMM (Wi-Fi мультимедиа)* – установка режима Wi-Fi Multimedia (WMM). Данный режим позволяет быстро и качественно передавать аудио- и видеоконтент одновременно с передачей данных;
- *WMM без подтверждения* – при использовании данного режима приёмная сторона не подтверждает принятые пакеты. В среде с малым количеством помех это позволит увеличить эффективность передачи, в среде с большим количеством помех эффективность передачи снизится;
- *WMM APSD* – установить автоматический переход в режим экономии энергии (включено – автоматический переход разрешен);

Для принятия и сохранения изменений необходимо нажать кнопку «*Применить/Сохранить*».

ПРИЛОЖЕНИЕ А ВОЗМОЖНЫЕ ПРОБЛЕМЫ И ВАРИАНТЫ ИХ РЕШЕНИЯ

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