TOTOLINK

ИНСТРУКЦИЯ ПО БЫСТРОЙ НАСТРОЙКЕ

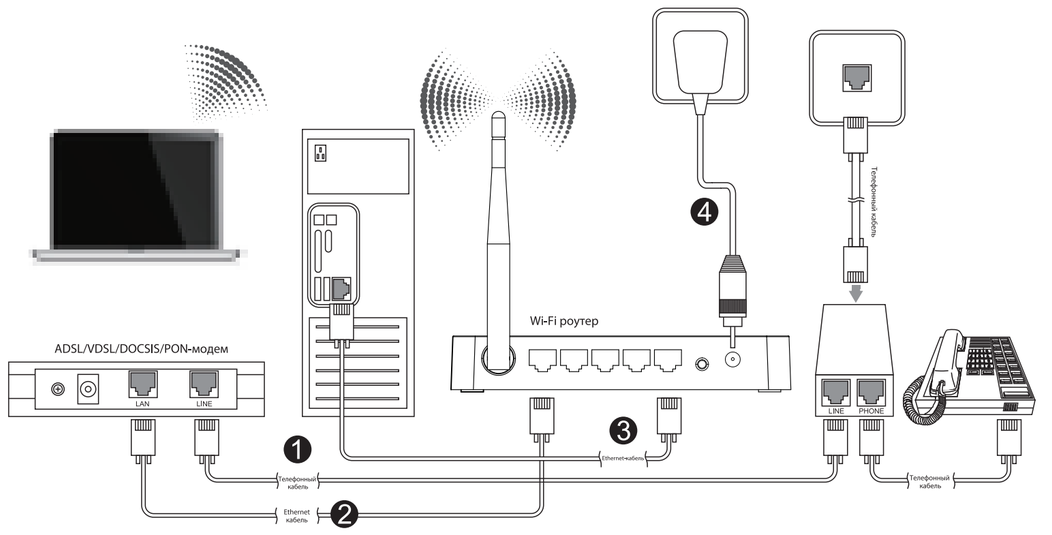
WiFi N роутер

Актуально для моделей: **N150RH, N300RH, N150RT, N151RT, N300RT**

134023640

1 Как подключить WiFi роутер

В том случае, если Ваш Интернет-провайдер предоставляет доступ в Интернет по технологии ADSL/VDSL/DOCSIS/PON, то выполните подключение Wi-Fi роутера по порядку, описанным в пунктах 1, 2, 3 и 4. В том случае, если Ваш Интернет-провайдер предоставляет доступ в Интернет по технологии Ethernet и Инженеры провели сетевой кабель к вам, то подключите кабель к порту WAN устройства, обозначенный как порт Интернет (см. изображение на задней стороне картонной коробки устройства) и следуйте порядку действий, описанному в пунктах 2, 3 и 4.



После того как Вы убедились, что все правильно подключено, проверьте состояние светодиодных индикаторов устройства.

Светодиод	Описание	
POWER	Светодиодный индикатор светится синим цветом, когда роутер подключен по питанию к электросети, во всех остальных случаях он не горит.	
CPU	Светодиодный индикатор мигает синим цветом, когда роутер включен.	
Сеть Wi-Fi	Светодиодный индикатор мигает синим цветом, когда к роутеру подключены клиенты Wi-Fi и происходит процесс передачи данных.	
WAN	Вкл.	Когда к порту WAN подключен кабель Интернет-провайдера, светодиодный индикатор светится синим цветом.
	Мигает	В процессе передачи и приема данных через порт WAN светодиодный индикатор мигает синим цветом.
	Выкл.	Когда кабель Интернет-провайдера не подключен к порту WAN.
1/2/3/4 LAN	Вкл.	Когда к порту LAN подключено клиентское устройство, соответствующий светодиодный индикатор светится синим цветом.
	Мигает	В процессе передачи и приема данных через порт LAN, соответствующий светодиодный индикатор мигает синим цветом.
	Выкл.	К соответствующему порту LAN ничего не подключено.

ВАЖНЫЕ ПРИМЕЧАНИЯ:

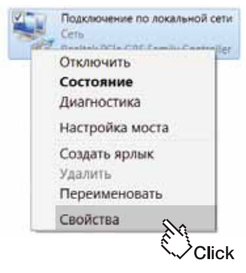
1. Отключайте адаптер питания от сети и все сетевые кабели от устройства в грозу.
2. Обеспечивайте хорошую вентиляцию и изолируйте от источников тепла.
3. Не допускайте попадания жидкостей в процессе работы и транспортировки.
4. Электросеть должна соответствовать параметрам на блоке питания.
5. Размещайте устройство на твердых горизонтальных поверхностях.

2 Как настроить компьютер для подключения роутера

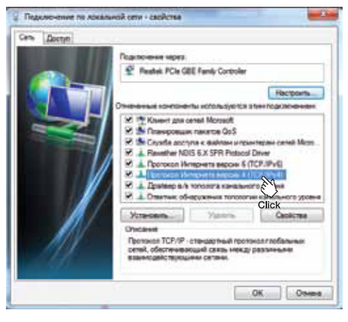
Windows Vista/7

1. Нажмите кнопку “Пуск” (левый нижний угол рабочего стола операционной системы Windows). В появившемся меню нажмите правой кнопкой мыши надпись “Сеть” и выберите “Свойства”.

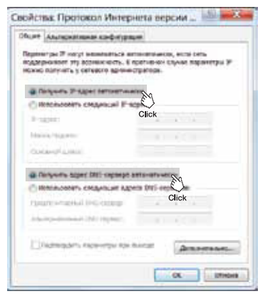
2. В появившемся окне выберите “Изменение параметров адаптера ”, в открывшемся окне кнопкой мыши на ярлыке “Подключение по локальной сети”. Выберите “Свойства”.



3. В появившемся окне выберите “Протокол Интерна версии 4 (TCP/IPv4)” и нажмите кнопку “Свойства”.



4. Выставите “Получить IP-адрес автоматически”и “Получить адрес DNS-сервера автоматически”.



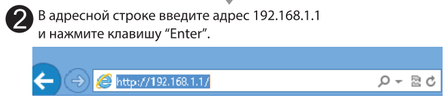
Важное примечание:
Если в данном окне имеются какие-либо сетевые реквизиты (IP-адрес, Маска подсети и т.д.), рекомендуем Вам их переписать. Они Вам обязательно пригодятся при настройке Вашего устройства.

TOTOLINK

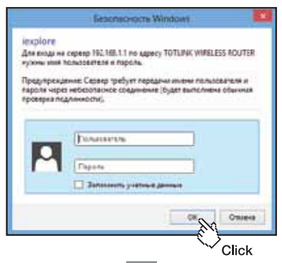
3 Как настроить подключение и авторизацию роутера для работы с интернет-провайдером

1. Запустите программу Интернет-браузер.

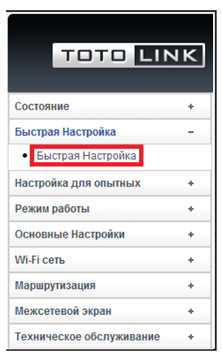
2. В адресной строке введите адрес 192.168.1.1 и нажмите клавишу “Enter”.



3. В появившемся окне введите Имя пользователя (admin) и Пароль (admin) , затем нажмите кнопку “OK”.



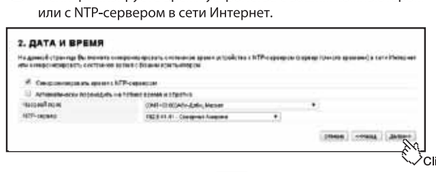
4. На открывшейся странице, в Вашем браузере, выберите “Быстрая настройка”.



5. Нажмите кнопку “Далее”.

6. Режим работы устройства по умолчанию - Режим Wi-Fi роутера / Точки доступа. Если Вы хотите выбрать другой режим, нажмите кнопку “Изменить режим работы устройства”.

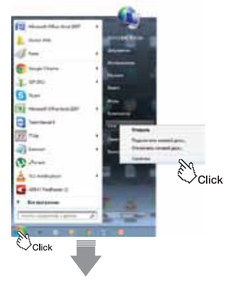
7. Задайте часовой пояс текущего местоположения устройства и синхронизируете время устройства с Вашим компьютером или с NTP-сервером в сети Интернет.



8. На Данной странице Вы можете поменять IP-адрес роутера (Вы его вводили в адресной строке браузера), а также Маску подсети.

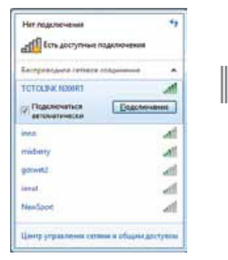
4 Как подключиться по Wi-Fi к сети Wi-Fi Вашего роутера

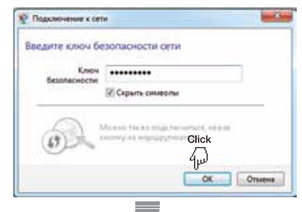
1. Нажмите кнопку “Пуск” (левый нижний угол рабочего стола операционной системы Windows). В появившемся меню нажмите правой кнопкой мыши надпись “Сеть” и выберите “Свойства”.



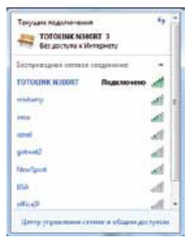
2. В появившемся окне выберите “Изменение параметров адаптера ”, в открывшемся окне кнопкой мыши на ярлыке “Беспроводное сетевое соединение”. Выберите “Подключение / Отключение”.

3. Выберите SSID (Название сети Wi-Fi), к которой необходимо подключиться, и нажмите кнопку “Подключение”.



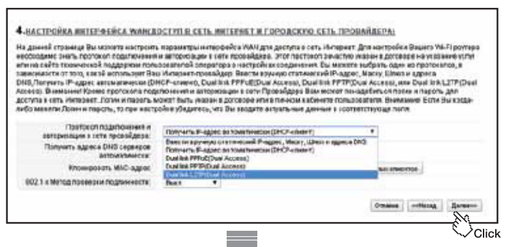


4. Введите ключ безопасности.

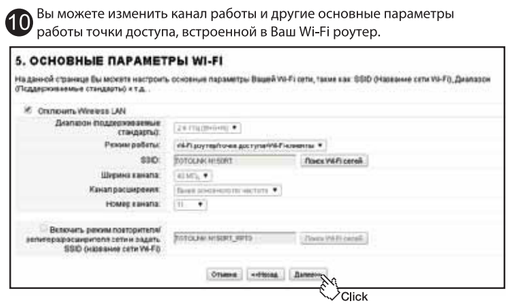


5. Если Вы подключились к сети Wi-Fi и устройство, к которому Вы подключились, настроено надлежащим образом, то Вы можете получить доступ в сеть Интернет.

9. Выберите протокол подключения и авторизации в сети Вашего оператора. Следуйте подсказкам на экране.



10. Вы можете изменить канал работы и другие основные параметры работы точки доступа, встроенной в Ваш Wi-Fi роутер.



11. Для наилучшей безопасности и производительности рекомендуем использовать WPA2-AES. Введите ключ безопасности сети Wi-Fi в соотвествующее поле (при вводе на английской раскладке клавиатуры, включая буквы и цифры, его длина может составлять от 8 до 63 символов). Нажмите кнопку “Готово” для завершения быстрой настройки.

ВАЖНЫЕ ПРИМЕЧАНИЯ:

Рекомендуем Вам запомнить Имя сети Wi-Fi (SSID) и ключ безопасности – эти параметры необходимо знать для подключения по Wi-Fi к Вашему Wi-Fi роутеру.

RST / WPS

Нажмите и удерживайте кнопку RST – WPS в течение 2-3 секунд для активации технологии WPS (Светодиодный индикатор будет при этом гореть). Для сброса всех настроек устройства в заводские – нажмите и удерживайте данную кнопку более 10 секунд (все светодиодные индикаторы будут быстро мигать, что будет свидетельствовать о начале процесса аппаратного сброса настроек).

Техническая поддержка
осуществляется по телефону: **+7 (495) 707-26-05**
Бесплатные звонки из регионов: **8-800-555-98-94**

Изготовитель:
ЗИОНКОМ ЭЛЕКТРОНИКС (ШЕНЬЧЖЕНЬ) ЛИМИТЕД
Адрес:Ком: 3D, 3-ий этаж, А-3 Диджитал Технолоджи Парк,
Роуд 7 Саутх, Хай-Тек Парк, район Нан Шан, Шеньчжень, Китай

ИСТРУКЦИИ ПО НАСТРОЙКЕ И ЭКСПЛУАТАЦИИ

TOTOLINK Wireless-N Router

TOTOLINK

СОДЕРЖАНИЕ

1. О ИСТРУКЦИИ ПО НАСТРОЙКЕ И ЭКСПЛУАТАЦИИ

Компания TOTOLINK выражает свою признательность за приобретение нашего роутера. Инструкция познакомит вас с его возможностями и поможет настроить подключение и авторизацию для обеспечения доступа в Интернет. Пожалуйста, следуйте рекомендациям и советам, приведенным в данной инструкции по настройке и эксплуатации роутера для получения максимальной скорости работы вашей сети.

1.1 Описание инструкции по настройке и эксплуатации

Обзор устройства:
Глава описывает функционал роутера и его технические характеристики.

Как подключить роутер:
Глава описывает процесс подключения роутера и настройки на компьютере.

Как настроить подключение и авторизацию роутера для работы с Интернет-провайдером:
Глава описывает, как настроить подключение и авторизацию роутера для работы с Интернет-провайдером.

Продвинутые настройки:
Глава описывает, как корректно настроить продвинутые функции устройства, включая сеть Wi-Fi, TCP/IP, межсетевой экран и т.д.

2. ОБЗОР УСТРОЙСТВА

2.1 Введение

Данная модель роутера поддерживает ряд продвинутых функций: одновременный доступ в сеть Интернет до 253 пользователей, подключенных к устройству, четырехпортовый коммутатор и межсетевой экран. Роутер позволяет подключаться к Интернет, ИСПОЛЬЗУЯ протоколы DHCP/Static IP, IP/PPPoE (Dual Access), PPTP (Dual Access) /L2TP (Dual Access), и способен обеспечить высокую скорость передачи данных. Высокая мощность передатчика наряду с эффективными антеннами обеспечивают качественное и стабильное соединение по Wi-Fi. Роутер поддерживает множество современных алгоритмов шифрования данных, передаваемых по Wi-Fi: 64/128-бит WEP, WPA/WPA2 и WPA-mixed, и позволяет использовать функции фильтров по IP-адресам, номерам портов, по URL и MAC-адресам, что делает устройство удобным в тонкой настройке и управлении. Модель совместима практически с любым оператором на территории РФ и СНГ, что делает ее идеально подходящим роутером для любого пользователя. Перед вами качественное технологичное решение для Wi-Fi, IPTV, P2P, дома или офиса!

2.2 Особенности

► Устройство полностью совместимо и соответствует стандартам IEEE 802.11n и IEEE 802.11g/b для частотного диапазона 2,4 ГГц сетей Wi-Fi.

► Устройство поддерживает алгоритмы подключения и авторизации в сети Интернет-провайдера: DHCP, статический IP-адрес, Dual Link PPPoE (Dual Access), Dual Link PPTP (Dual Access) и Dual Link L2TP (Dual Access).

► Устройство поддерживает три режима работы: Wi-Fi роутер/Точка доступа, Режим моста и Режим роутера-клиента Wi-Fi-оператора.

► Поддержка одновременной работы с городской сетью провайдера и доступ в Интернет

при авторизации по протоколам PPPoE, PPTP и L2TP на интерфейсе WAN.

► Устройство поддерживает множество современных алгоритмов шифрования данных, передаваемых по Wi-Fi: 64/128 бит WEP, WPA/WPA2 и WPA-Mixed.

► Меню «Быстрая Настройка» для конфигурирования роутера без звонков в службу технической поддержки.

► Устройство поддерживает функции фильтрации по IP-адресам, номерам портов, MAC-адресам и URL, а также перенаправление портов.

► Поддержка приоритезации полосы пропускания (технология QoS) по IP/MAC-адресам и номерам портов.

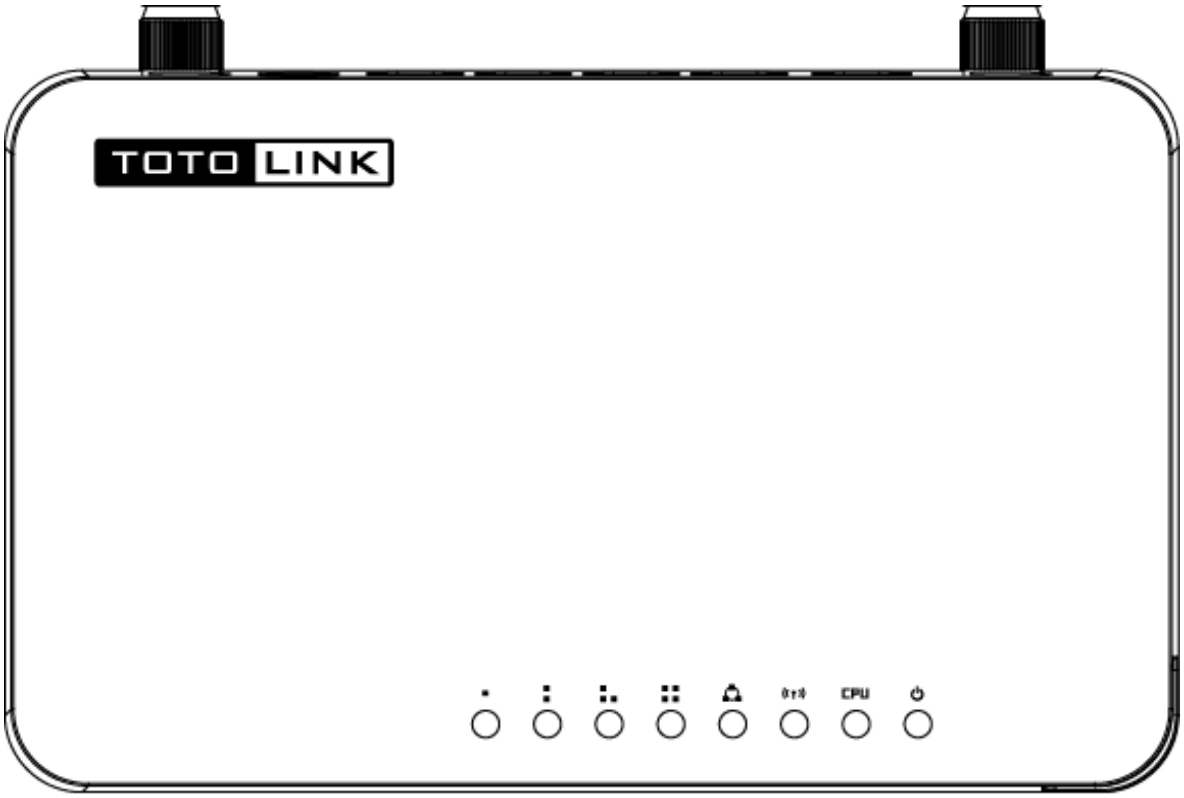
► Telnet-сервер устройства обеспечивает безопасное удаленное управление и администрирование.

► Поддержка технологии VLAN для просмотра IPTV и реализации дополнительных услуг, предоставляемых Интернет-провайдером (Tripple play)

2.3 Внешний вид

2.3.1 Передняя панель

На передней панели роутера расположено 8 светодиодных индикаторов, которые отображают текущее состояние устройства.

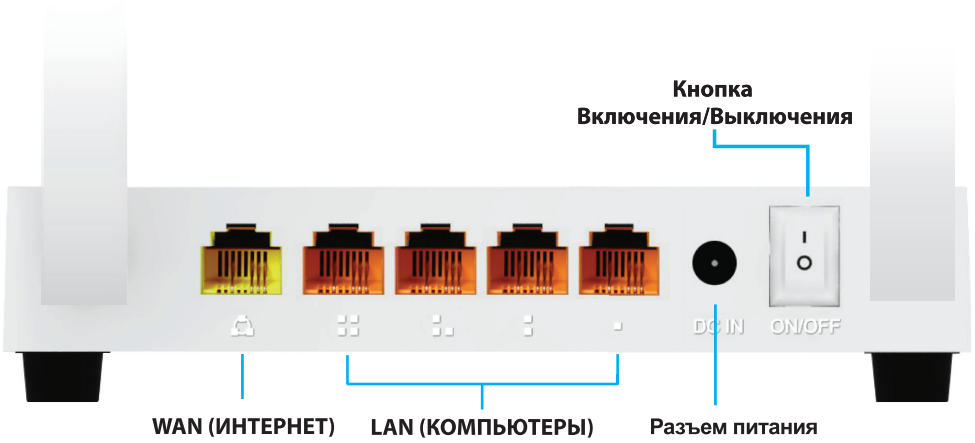


(Внешний вид корпуса, его дизайн, наименования интерфейсов могут быть изменены в зависимости от модели)

POWER	Светодиодный индикатор светится синим цветом, когда роутер подключен по питанию к электросети, во всех остальных случаях он не горит.	
CPU	Светодиодный индикатор мигает синим цветом, когда роутер включен.	
Сеть Wi-Fi	Светодиодный индикатор мигает синим цветом, когда к роутеру подключены клиенты Wi-Fi и происходит процесс передачи данных.	
WAN	**Вкл.**	Когда к порту WAN подключен кабель Интернет-провайдера, светодиодный индикатор светится синим цветом.
	Мигает	В процессе передачи и приема данных через порт WAN светодиодный индикатор мигает синим цветом.
	Выкл.	Когда кабель Интернет-провайдера не подключен к порту WAN.
1/2/3/4 LAN	**Вкл.**	Когда к порту LAN подключено клиентское устройство, соответствующий светодиодный индикатор светится синим цветом.
	Мигает	В процессе передачи и приема данных через порт LAN, соответствующий светодиодный индикатор мигает синим цветом.
	Выкл.	К соответствующему порту LAN ничего не подключено.

2.3.2 Задняя панель

На задней панели роутера расположены Ethernet-интерфейсы (RJ-45), разъем питания, кнопка RST/WPS и опциональная кнопка Включения/Выключения (зависит от модели).



DC IN	Разъем питания служит для подключения адаптера питания.
WAN	Порт служит для подключения кабеля Интернет-провайдера.
1/2/3/4 LAN	Порты служат для подключения к роутеру клиентских сетевых устройств.
RST/WPS кнопка	Нажмите и удерживайте кнопку 2-3 секунды, после чего светодиодный индикатор System будет постоянно светится. Это будет означать, что технология WPS работает корректно. Нажмите и удерживайте кнопку 10 секунд, после чего все светодиодные индикаторы устройства начнут быстро мигать, что будет означать, что устройство ушло в перезагрузку, после которой примет настройки по умолчанию.

3. КАК ПОДКЛЮЧИТЬ РОУТЕР

3.1 Как подключить роутер

Чтобы правильно подключить компьютер и другие устройства и предоставить им одновременный доступ в сеть Интернет через роутер, каждое устройство должно быть настроено надлежащим образом и подключено к роутеру Ethernet-кабелем или через Wi-Fi.

1. Отключите кабель Интернет-провайдера от компьютера, на котором был настроен доступ в сеть Интернет до приобретения роутера.

2. Подключите Ethernet-кабель, который провели инженеры вашего Интернет-провайдера в квартиру в порт WAN, обозначенный как порт Интернет (см. изображение на задней стороне картонной коробки устройства)

3. Подключите сетевой кабель из комплекта поставки устройства (Ethernet UTP LAN) одним разъемом в любой из LAN-портов роутера.

4. Подключите другой разъем сетевого кабель из комплекта поставки устройства (Ethernet UTP LAN) к сетевой плате компьютера, на котором был настроен доступ в сеть Интернет до приобретения роутера.

5. Подключите адаптер питания к разъему питания вашего роутера, затем к электросети.

6. Включите компьютер.

7. Убедитесь, что светодиодные индикаторы Power и соответствующие индикаторы LAN и WAN отображают текущее состояние роутера.

3.2 Как проверить правильность подключения роутера

Понимание сигналов светодиодной индикации роутера поможет оценить текущее состояние, а также состояние локальной сети:

1. Если адаптер питания подключен к роутеру и электросети, а само устройство подключено к сети Интернет-провайдера, должны гореть следующие светодиодные индикаторы, свидетельствующие о нормальной работе устройства: Power, WPS, LAN, Wi-Fi, WAN.

2. В том случае, когда порт WAN подключен к сети Интернет, авторизация (если таковая требуется) произведена успешно, светодиодный индикатор WAN должен мигать.

3. В том случае, когда к LAN-порту подключен компьютер или другое клиентское Ethernet-устройство, соответствующий светодиодный индикатор LAN должен мигать.

3.3 Как настроить компьютер для подключения роутера

Заводской IP-адрес роутера: 192.168.1.1, заводская маска подсети: 255.255.255.0. Оба параметра можно при необходимости изменить. В данной инструкции по настройке и эксплуатации мы будем использовать значения по умолчанию.

Проверьте подключение между компьютером и LAN-портом роутера. Существует 2 способа установить IP-связь между компьютером и роутером:

► Установка IP-адреса вручную

Зайдите в папку сетевых подключений компьютера (Пуск>Панель управления> Сеть и Интернет>Центр управления сетями и общим доступом>Изменение параметров адаптера). Нажмите правой кнопкой мыши по иконке “Подключение по локальной сети” и выберите “Свойства”. В открывшемся окне нажмите на “Протокол Интернета версии 4 (TCP/IPv4)” и нажмите кнопку “Свойства”. В открывшемся окне выберите “Использовать следующий IP-

адрес". Введите IP-адрес в активное поле: 192.168.1.xxx (где xxx – любое число от 2 до 254). Маска подсети: 255.255.255.0, основной шлюз: 192.168.1.1 (IP-адрес роутера по умолчанию).

► Автоматическое получение IP-адреса

Проверьте, настроена ли сетевая плата вашего компьютера на автоматическое получение IP-адресов. Для этого зайдите в папку сетевых подключений компьютера (Пуск>Панель управления>Сеть и Интернет>Центр управления сетями и общим доступом>Изменение параметров адаптера). Нажмите правой кнопкой мыши по иконке "Подключение по локальной сети" и выберите "Свойства". В открывшемся окне нажмите на "Протокол Интернета версии 4 (TCP/IPv4)" и нажмите кнопку "Свойства". В открывшемся окне выберите **"Получить IP-адрес автоматически".**

Теперь необходимо выполнить команду CMD из командной строки, для того что бы проверить сетевое соединение между компьютером и роутером. Откройте командную строку (Пуск> Выполнить. В открывшемся окне необходимо написать на английской раскладке клавиатуры буквы CMD и нажать клавишу Enter на клавиатуре). После описанных действий вы увидите окно командной строки. В окне командной строки введете команду **ping 192.168.1.1 –t**, затем нажмите клавишу Enter.

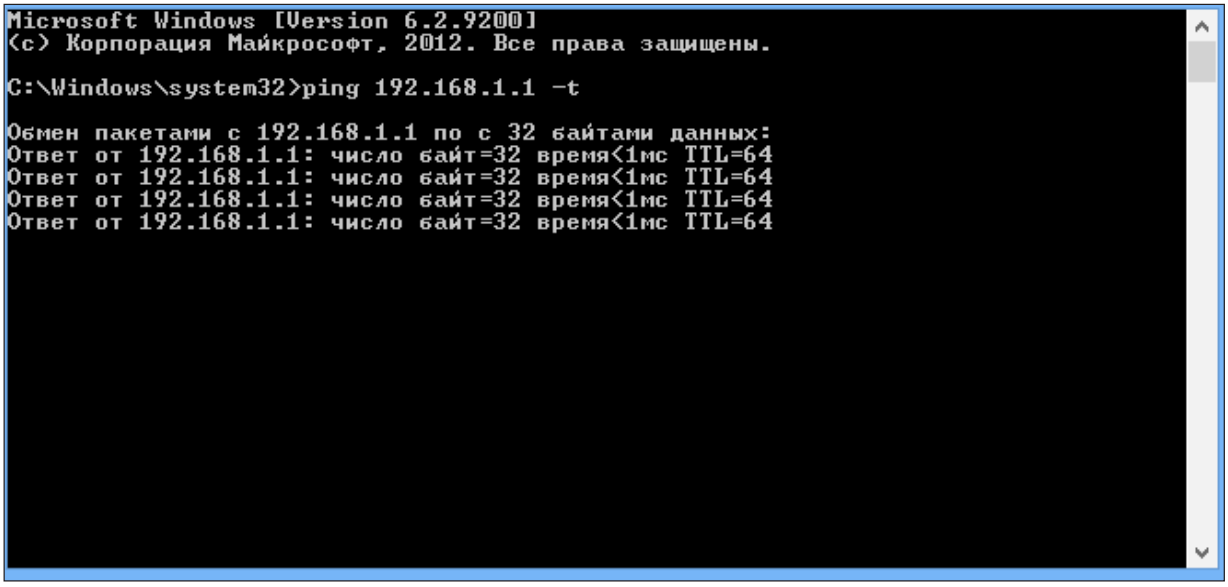


Рис. 3-1 Команда Ping прошла успешно

Если полученные вами результаты сходны с тем, что вы видите на Рис. 3-1, соединение между компьютером и роутером успешно установлено.

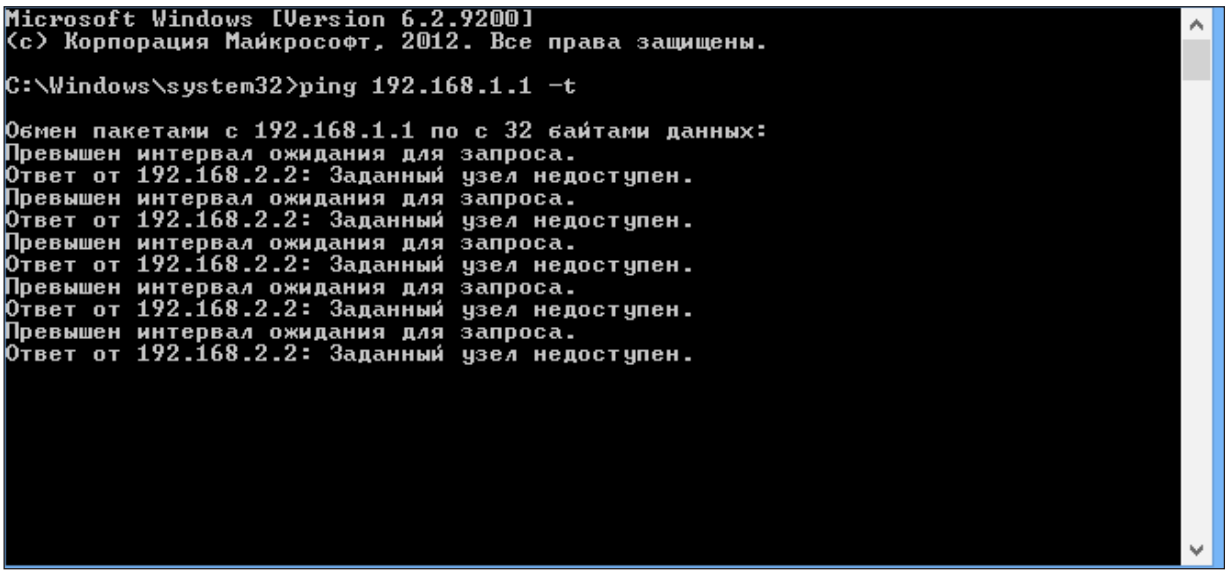


Рис. 3-2 Команда Ping не прошла

Если полученные вами результаты сходны с тем, что вы видите на Рис. 3-2, соединение между компьютером и роутером не было установлено. Пожалуйста, следуйте шагам, описанным ниже:

1. Как проверить физическое соединение между компьютером и роутером?

Если соединение между компьютером и роутером имеется, соответствующий LAN-порт роутера и соответствующий светодиодный индикатор на сетевой плате компьютера (если таковой имеется на сетевом адаптере компьютера) должны мигать.

2. Как проверить IP-связь между компьютером и роутером?

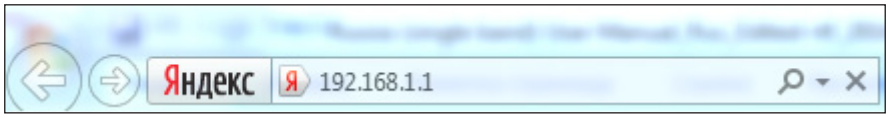
Так как IP-адрес роутера по умолчанию 192.168.1.1, IP-адрес компьютера должен иметь любое значение в диапазоне от 192.168.1.2 до 192.168.1.254. IP-адресом основного шлюза должно быть значение: 192.168.1.1

4. КАК НАСТРОИТЬ ПОДКЛЮЧЕНИЕ И АВТОРИЗАЦИЮ РОУТЕРА ДЛЯ РАБОТЫ С ИНТЕРНЕТ-ПРОВАЙДЕРОМ

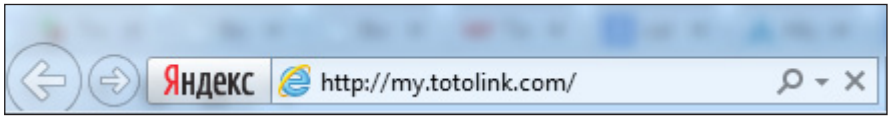
Глава описывает процесс настройки основных функций подключения и авторизации роутера для работы с Интернет-провайдером.

4.1 Как зайти в WEB-интерфейс настройки Wi-Fi роутера

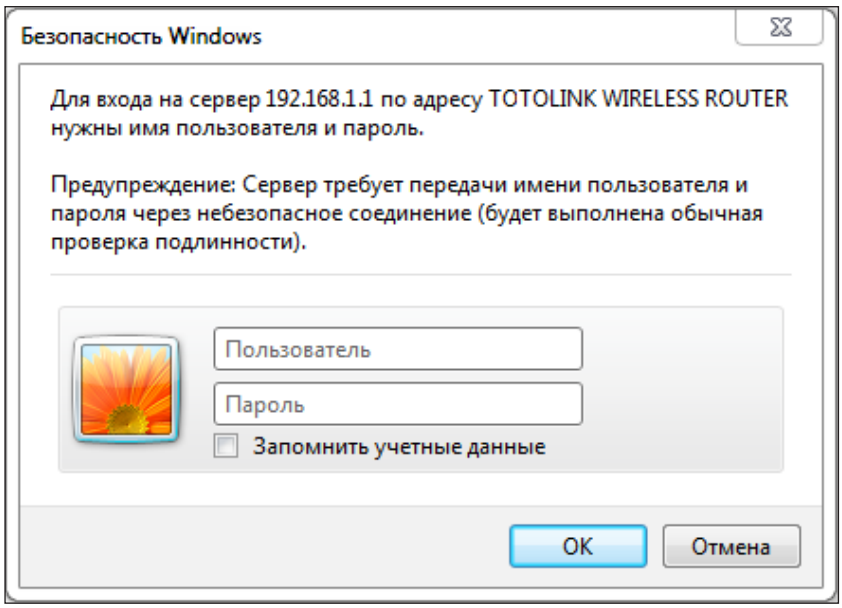
Подключитесь к роутеру, как это было описано ранее в инструкции. Запустите Интернет-браузер на компьютере. В адресной строке Интернет-браузера введите IP-адрес роутера 192.168.1.1 или адрес my.totolink.com (по умолчанию), затем нажмите клавишу Enter.



или



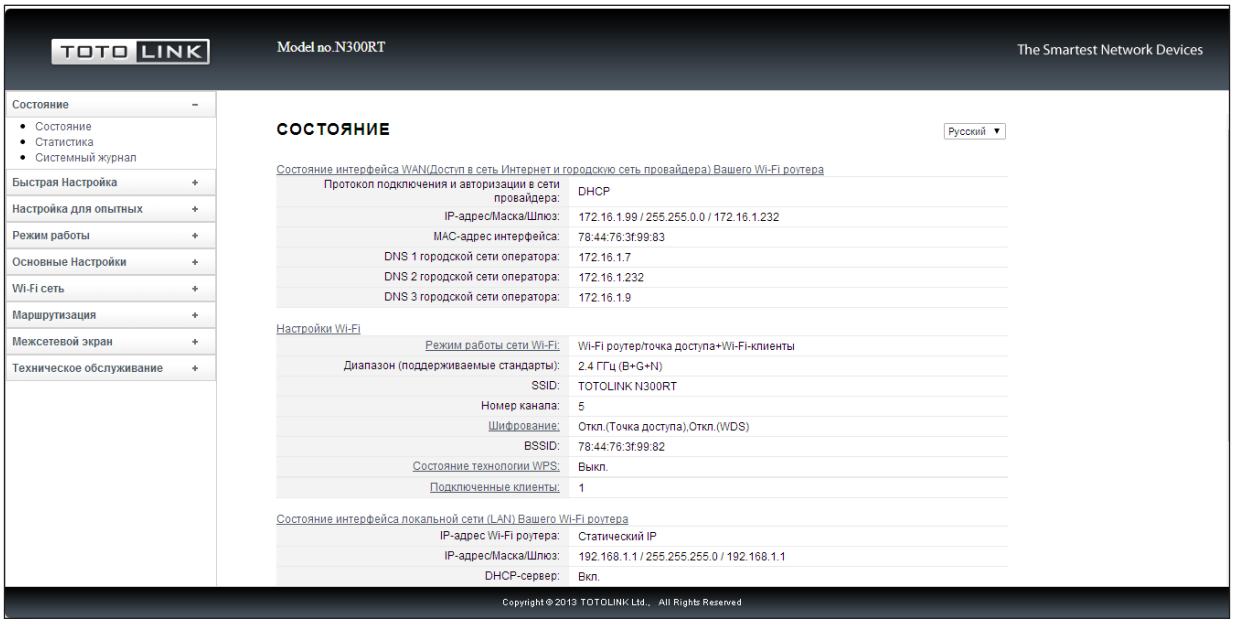
Затем вы увидите окно, запрашивающее имя пользователя и пароль:



Введите на английской раскладке клавиатуры слово admin в поле “Пользователь”, в поле “Пароль” введите на английской раскладке клавиатуры слово admin. Чтобы продолжить процесс настройки, нажмите кнопку OK или клавишу Enter.

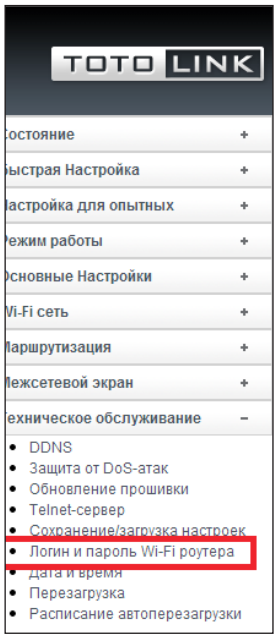
> ***Важное примечание:*** *В случае, если окно запрашивающее имя пользователя и пароль не появилось, скорее всего, в настройках Интернет-браузера настроена работа через прокси-сервер. Зайдите в настройки Интернет-браузера (Сервис > Свойства обозревателя > Вкладка “Подключения”), измените режим работы Интернет-браузера (отключите работу Интернет-браузера через прокси-сервер) и нажмите кнопку OK.*

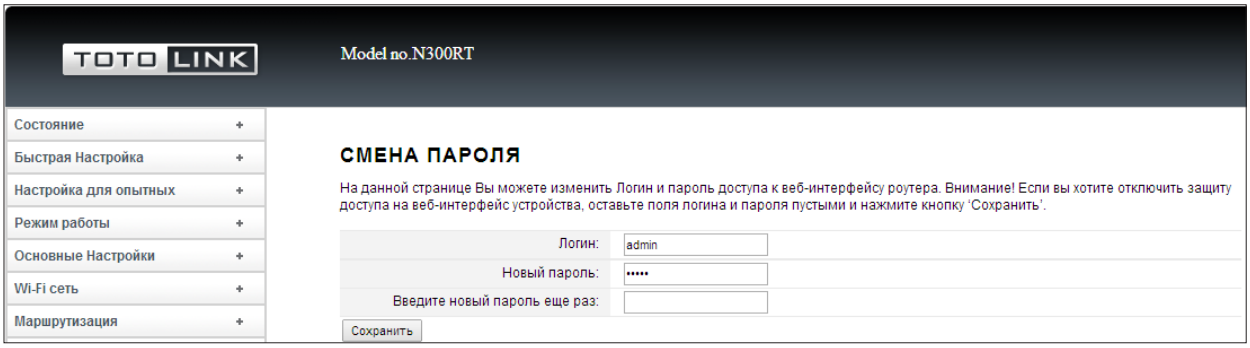
Поздравляем, вы авторизовались в WEB-интерфейсе роутера. После авторизации вы увидите данное окно в браузере.



4.2 Логин и пароль роутера

В первую очередь рекомендуем изменить логин и пароль учетной записи администратора роутера, чтобы повысить уровень конфиденциальность и защищенности доступа в WEB-интерфейс роутера. Пожалуйста, обратитесь к пункту левого меню WEB-интерфейса: “Техническое обслуживание” – “Логин и пароль Wi-Fi роутера” и прочтите соответствующую главу в данной инструкции.





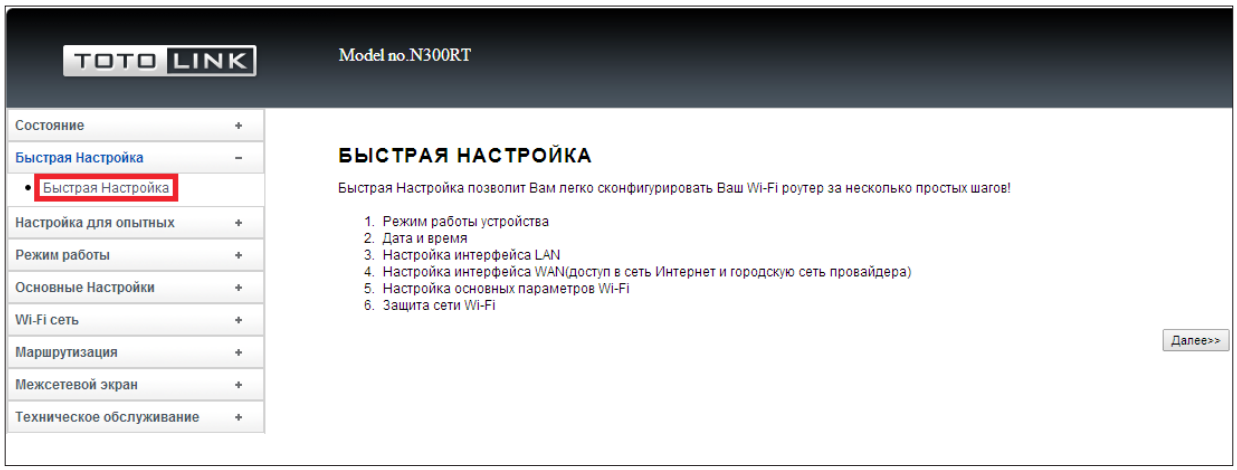
Логин: Введите в поле желаемое имя пользователя (логин) для авторизации в WEB-интерфейсе устройства.

Новый пароль: Введите в поле новый пароль для управления устройством под учетной записью администратора.

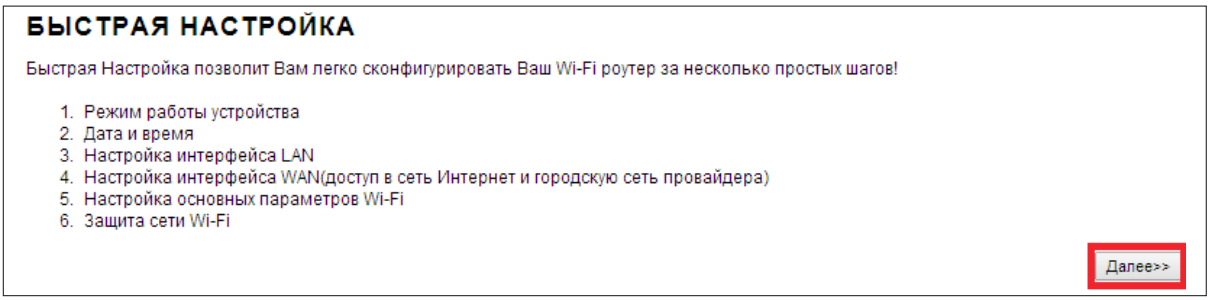
Введите новый пароль еще раз: Введите в поле новый пароль, чтобы убедится в том, что не допущена ошибка или опечатка при вводе.

4.3 Быстрая настройка

“Быстрая настройка” позволяет самостоятельно сконфигурировать роутер за считанные секунды без звонков в службу технической поддержки.



Нажмите “Быстрая настройка” в левом меню WEB-интерфейса, затем нажмите кнопку “Далее>>“, чтобы продолжить настройку.



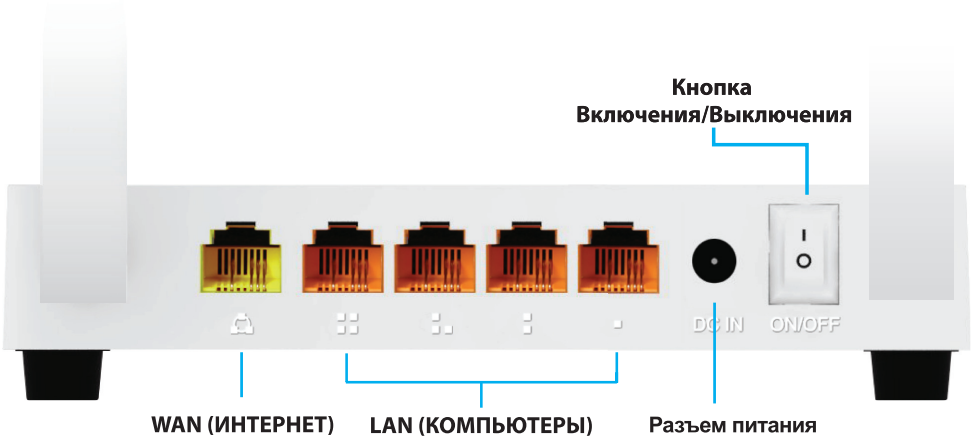
4.3.1 Режим работы устройства

Параметр определяет и описывает функционал и назначение работы устройства. Роутер поддерживает следующие режимы работы: Режим Wi-Fi роутера/Точки доступа, Режим Моста и Режим Wi-Fi Роутера-клиента Wi-Fi-оператора и Режим Повторителя/

Репитера /Расширителя сети*.Переключение между режимами работы производится при помощи кнопки “Изменить режим работы устройства”. Выберите подходящий режим работы, прочитав описание каждого в WEB-интерфейсе устройства. Чтобы продолжить процесс настройки нажмите кнопку “Далее>>“.

4.3.1.1 Режим Wi-Fi роутера/Точки доступа

Если инженеры Интернет-провайдера провели Ethernet-кабель в квартиру, выберите данный режим работы устройства. Ethernet-кабель провайдера необходимо подключить в порт WAN, который обозначен как порт “Интернет” (см. изображение на задней стороне картонной коробки от устройства). В данном режиме работы функция NAT включена. Все клиентские Wi-Fi и Ethernet-устройства, подключенные к роутеру, будут получать доступ в сеть Интернет через один IP-адрес присвоенный интерфейсу WAN Интернет-провайдером.



4.3.1.2 Режим Моста

Режим позволяет объединить две локальные Ethernet-сети через соединение Wi-Fi двух одинаковых устройств в режиме моста. Например, если у вас стоит задача объединить два офиса через дорогу в одну сеть.

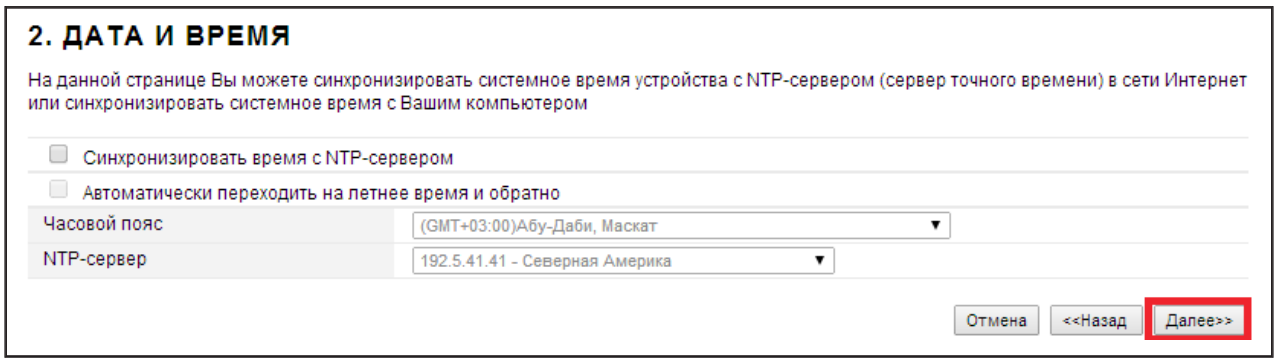
4.3.1.3 Режим Wi-Fi Роутера-клиента Wi-Fi-оператора

В этом режиме работы все LAN-порты объединены в общий интерфейс, подключение к сети Интернет осуществляется через интерфейс Wi-Fi. Функция NAT включена. Все клиентские устройства, подключенные к роутеру, будут получать доступ в сеть Интернет через один IP-адрес, присвоенный интерфейсу WAN Wi-Fi-провайдером. Необходимо перевести Wi-Fi интерфейс роутера в режим “Wi-Fi-клиент” и установить соединение с точкой доступа Wi-Fi-провайдера на странице “Поиск Wi-Fi сетей”. Доступные типы подключения в данном режиме работы устройства: Статический IP-адрес, Динамический IP-адрес (DHCP-клиент), Dual Link PPPoE (Dual Access), Dual Link PPTP (Dual Access) или Dual Link L2TP (Dual Access).

**** – Количество режимов работы устройства и их стабильность зависит от версии микропрограммного обеспечения (прошивки).***

4.3.2 Дата и время

На странице можно синхронизировать системное время устройства с NTP-сервером (сервер точного времени) в сети Интернет или синхронизировать системное время с компьютером. Для того чтобы продолжить процесс настройки нажмите кнопку “Далее>>“.



Синхронизировать время с NTP-сервером: NTP (Network Time protocol) – протокол точного времени, синхронизирующийся с сервером точного времени в сети Интернет (NTP-сервером). После синхронизации с сервером на устройстве (роутере) будет такое же время, как и у NTP-сервера в сети Интернет. Кроме этого можно синхронизировать и время всех клиентских устройств, подключенных к роутеру, чтобы избавить пользователей от возможных проблем при работе с общими сетевыми ресурсами локальной сети. Поставьте галочку в окне, чтобы включить функцию синхронизации с NTP-сервером.

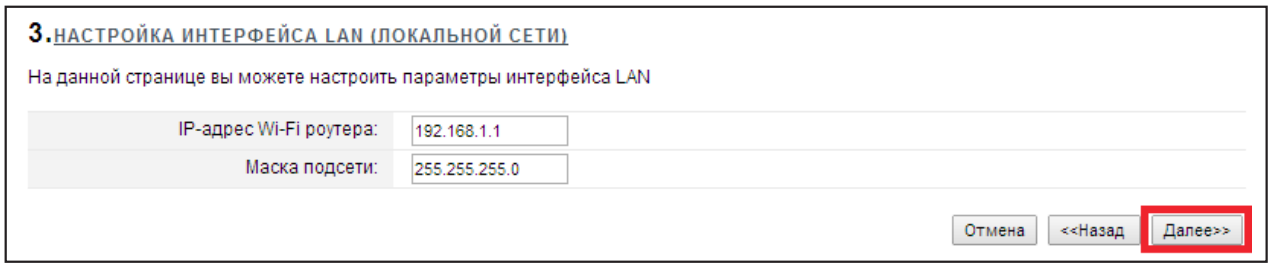
Автоматически переходить на летнее время и обратно: Поставьте галочку в окне, чтобы включить функцию.

Часовой пояс: Выберите часовой пояс текущего местоположения роутера.

NTP-сервер: Выберите NTP-сервер из списка доступных, с которым вы хотели бы синхронизировать системное время вашего устройства и его сети.

4.3.3 Настройка LAN

На этой странице можно настроить параметры интерфейса LAN.

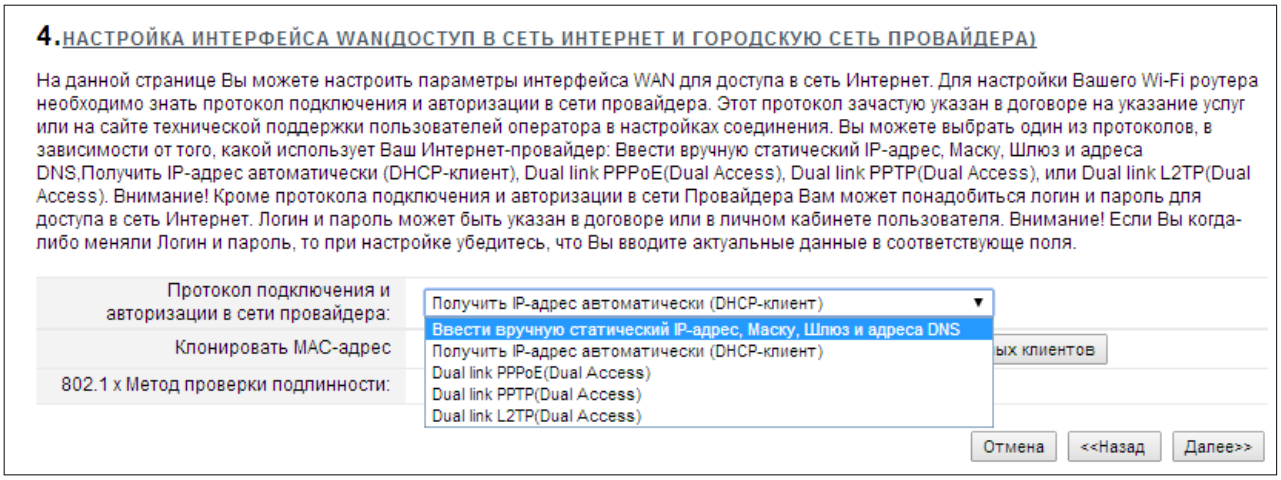


IP-адрес Wi-Fi роутера: Это IP-адрес по которому доступен WEB-интерфейс устройства для клиентов локальной сети LAN (включая сеть Wi-Fi). Помимо этой функции, данный IP- адрес будет использоваться устройством для правил маршрутизации (IP-адрес шлюза по-умолчанию).

Маска подсети: Данный параметр используется для определения классификации IP-сетей для выбранного диапазона IP-адресов. Например, 255.255.255.0 – типовое значение маски подсети для сетей класса. C, который поддерживает IP-адресацию от 192.0.0.x до 223.255.255.x. IP-сети класса C используют маски подсети длиной в 24 бита для определения адреса сети, и 8 бит для определения адреса конкретного конечного клиентского устройства (узла).

4.3.4 Настройка интерфейса WAN (Интернет)

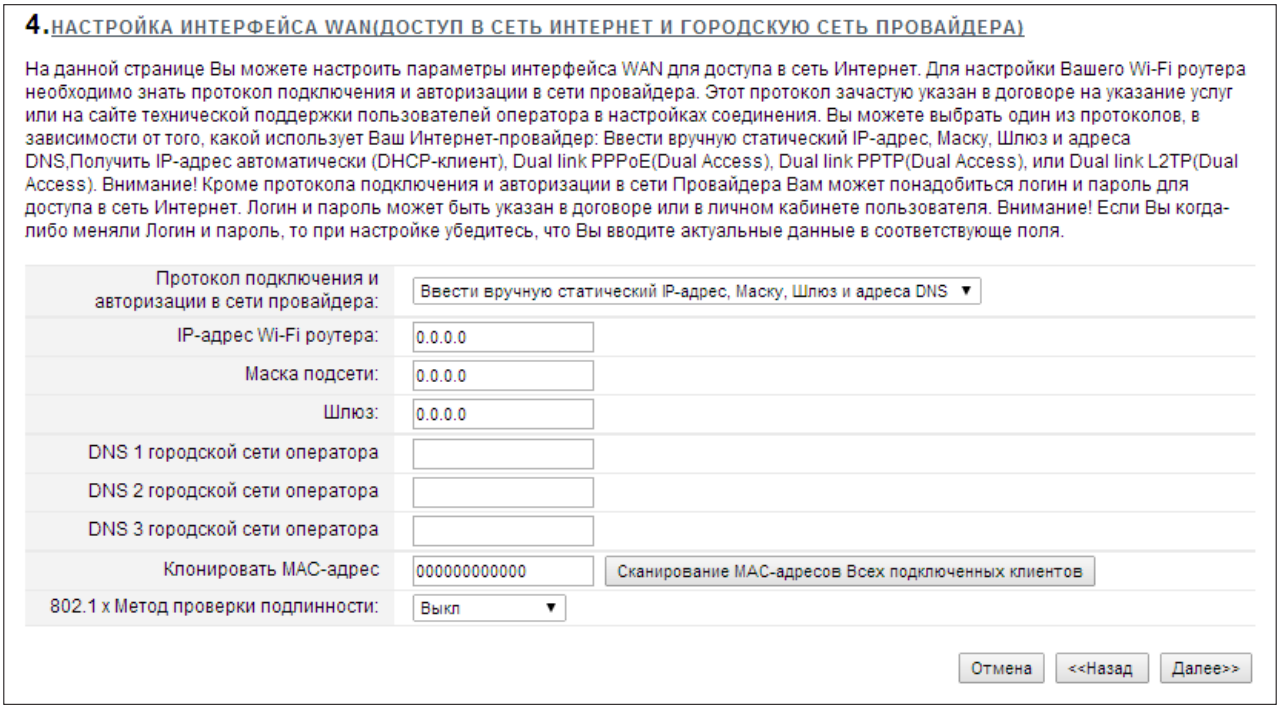
На данной странице можно настроить параметры интерфейса WAN для доступа в сеть Интернет. Для настройки роутера необходимо знать протокол подключения и авторизации в сети провайдера. Используемый протокол зачастую указан в договоре на оказание услуг или на сайте технической поддержки пользователей оператора в настройках соединения. Можете выбрать один из протоколов в зависимости от того, какой использует ваш Интернет-провайдер: 802.1 x, ввести вручную статический IP-адрес, маску, шлюз и адреса DNS, получить IP-адрес автоматически (DHCP-клиент), Dual Link PPPoE (Dual Access), Dual Link PPTP (Dual Access) или Dual Link L2TP (Dual Access). Внимание! Кроме протокола подключения и авторизации в сети провайдера может понадобиться логин и пароль для доступа в сеть Интернет. Логин и пароль могут быть указаны в договоре или в личном кабинете пользователя. Внимание! Если вы когда-либо меняли логин и/или пароль, при настройке убедитесь, что вводите актуальные данные в соответствующие поля.



Протокол подключения и авторизации в сети провайдера: Вы можете выбрать один из протоколов в зависимости от того, какой использует Интернет-провайдер.

4.3.4.1 Ввести вручную статический IP-адрес, маску, шлюз и адреса DNS

Если Интернет-провайдер указал в договоре на оказание услуг связи статический IP-адрес, маску, шлюз и адреса DNS, инженер оператора ввел эти реквизиты в свойствах сетевой платы компьютера при настройке соединения, тогда выберите именно этот протокол подключения и авторизации в сети провайдера, предварительно сбросив параметры сетевой платы компьютера на автоматическое получение IP-адресов.



IP-адрес роутера: IP-адрес, присвоенный Интернет-провайдером (данный параметр обычно указан в договоре на оказание услуг связи). Данный IP-адрес был введен в свойствах сетевой платы компьютера, на котором был настроен доступ в Интернет инженером провайдера до приобретения роутера.

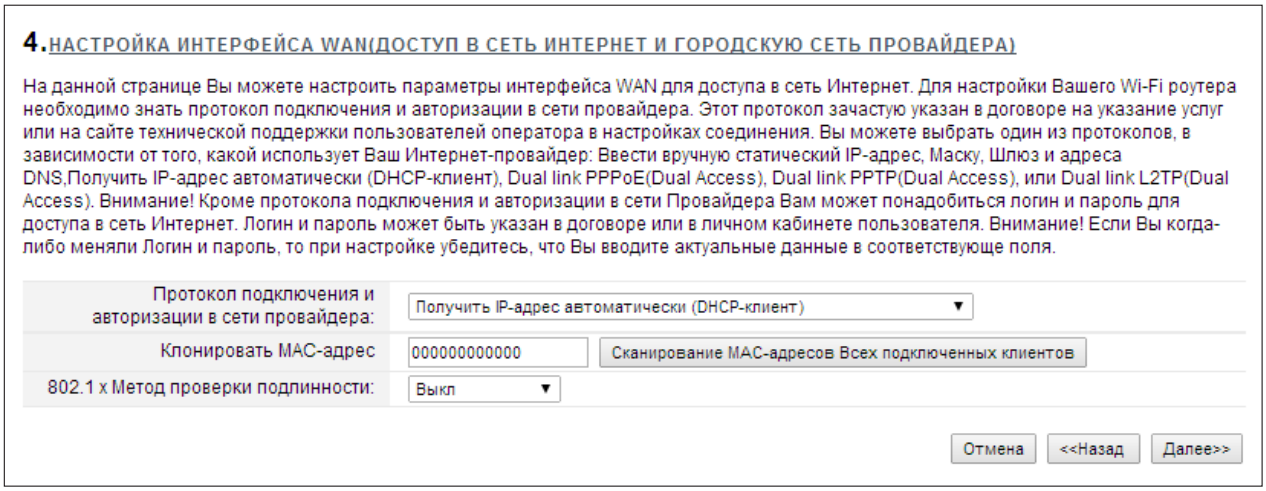
Маска подсети: Параметр используется для определения классификации IP-сетей для выбранного диапазона IP-адресов. Например, 255.255.255.0 – типовое значение маски подсети для сетей класса C, который поддерживает IP-адресацию от 192.0.0.x до 223.255.255.x. IP-сети класса C используют маски подсети длиной 24 бита для определения адреса сети и 8 бит для определения адреса конкретного конечного клиентского устройства (хоста). Данный параметр обычно указан в договоре на оказание услуг связи.

Шлюз: IP-адрес другого роутера или сервера, расположенного в городской сети Интернет-провайдера, который перенаправляет и выстраивает маршруты продвижения данных для доступа во внешнюю сеть Интернет (по соотношению к масштабам Интернет-провайдера) в какую-либо внешнюю, более высокоразвитую и высокоорганизованную сеть (от роутера до сети Интернет). Помимо этого шлюз в любой компьютерной сети должен самостоятельно выстраивать маршруты до более высокостоящего шлюза и так далее. Доступ в сеть в Интернет и вся сеть Интернет – объединение интеллектуальных устройств (шлюзов, таких как роутеры или серверы), выбирающих динамически или на основании заданных администраторами этих устройств правил. передвижения данных, работающих по протоколу IP (параметр шлюза или адрес основного шлюза обычно указан в договоре на оказание услуг связи).

DNS: Сервер в сети Интернет-провайдера DNS (Domain Name System), который работает по принципу телефонной книги для сети Интернет, сопоставляющий то, что вы видите в адресной строке Интернет-браузера в качестве названия Интернет-сайта с IP-адресом сервера, где этот сайт непосредственно находится (параметр обычно DNS указан в договоре на оказание услуг связи).

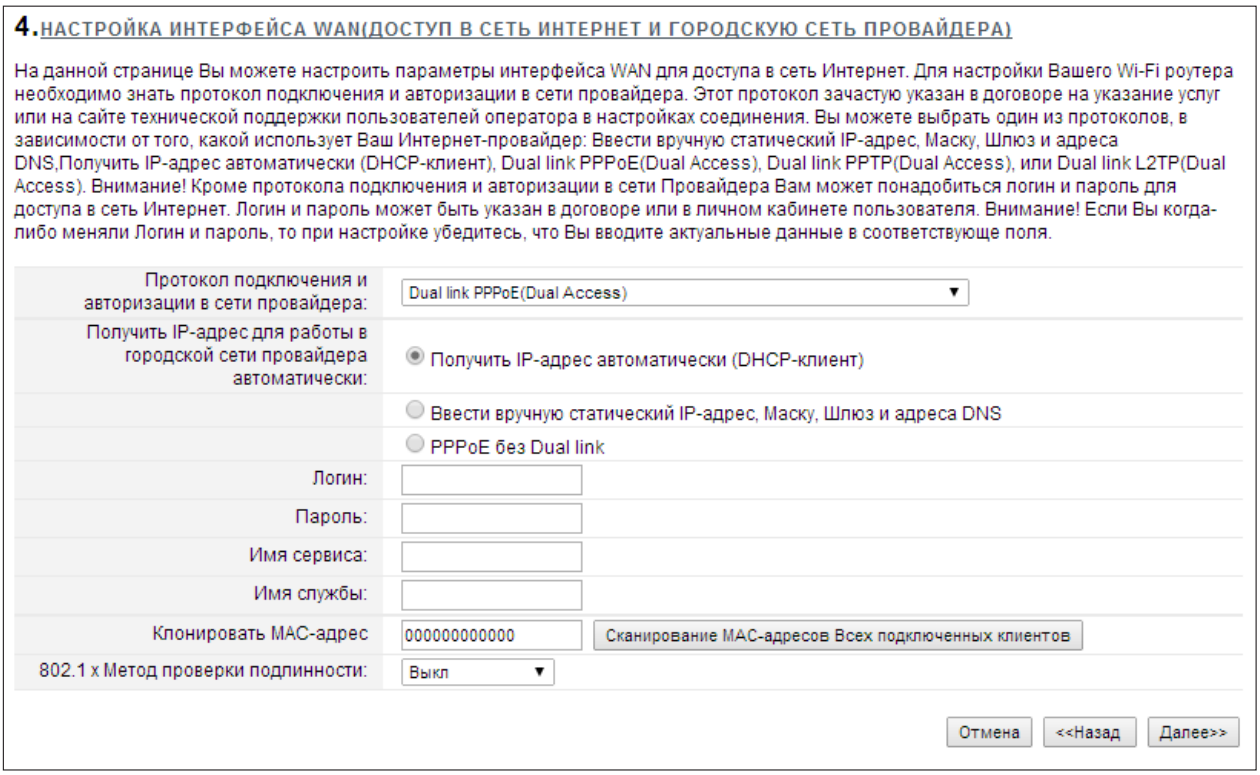
4.3.4.2 Получить IP-адрес автоматически (DHCP-клиент)

DHCP (Dynamic Host Configuration Protocol) – протокол локальных сетей (LAN). Если провайдер не указал никаких сетевых реквизитов (таких как логин, пароль, IP-адрес, маска подсети и т.д.), скорее всего, Интернет-провайдер использует этот протокол для предоставления доступа в сеть Интернет своим клиентам. Если выберите данный протокол подключения и авторизации в сети провайдера, интерфейс WAN (порт, отвечающий за доступ в сеть Интернет) получит IP-адрес и другие сетевые реквизиты автоматически от сети оператора.



4.3.4.3 Dual Link PPPoE (Dual Access)

PPPoE (Point-to-Point Protocol over Ethernet) – часто используемый протокол инкапсуляции данных для доступа в сеть Интернет, использующий защищенное соединение между двумя сетевыми интерфейсами (например, интерфейс WAN роутера и сервер авторизации Интернет-провайдера). Если инженер провайдера при настройке соединения на компьютере создавал в папке сетевых подключений “Высокоскоростное подключение”, выберите именно этот протокол подключения и авторизации в сети провайдера, предварительно удалив “Высокоскоростное подключение” из папки сетевых подключений вашего компьютера.

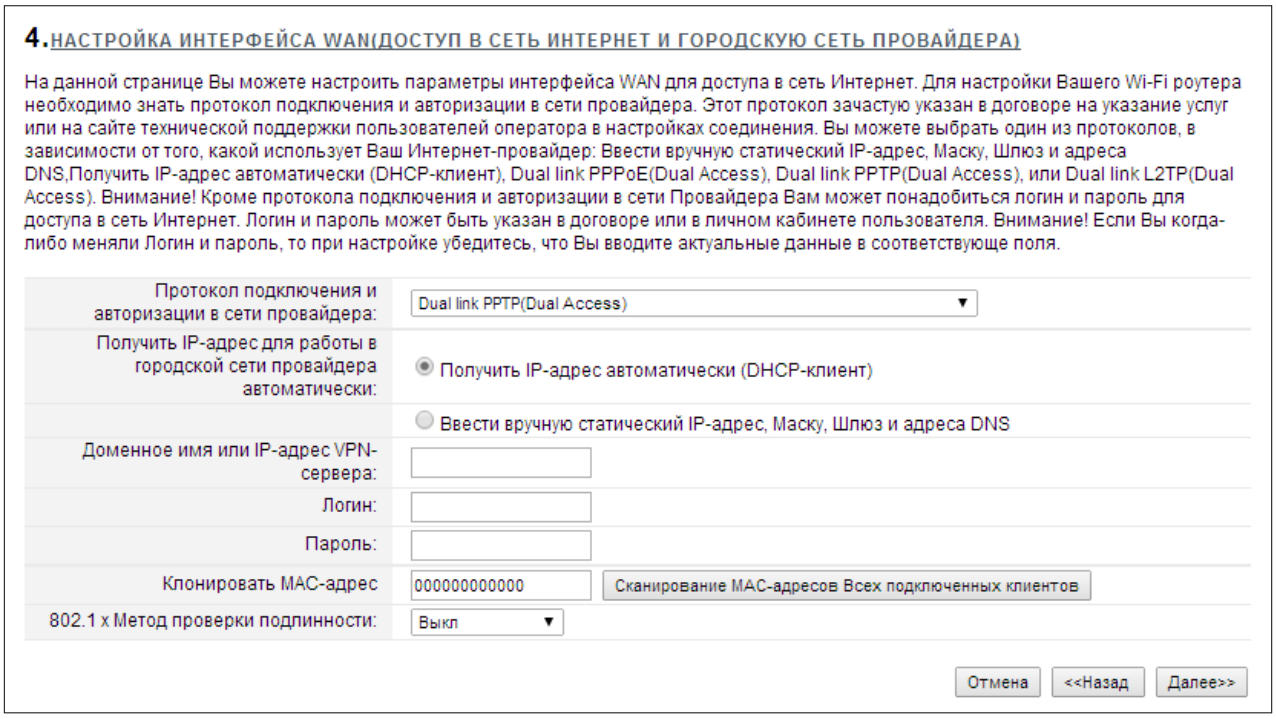


Логин: Введите в данное поле логин, присвоенный Интернет-провайдером (данный параметр обычно указан в договоре на оказание услуг связи).

Пароль: Введите в поле пароль, присвоенный Интернет-провайдером (данный параметр обычно указан в договоре на оказание услуг связи).

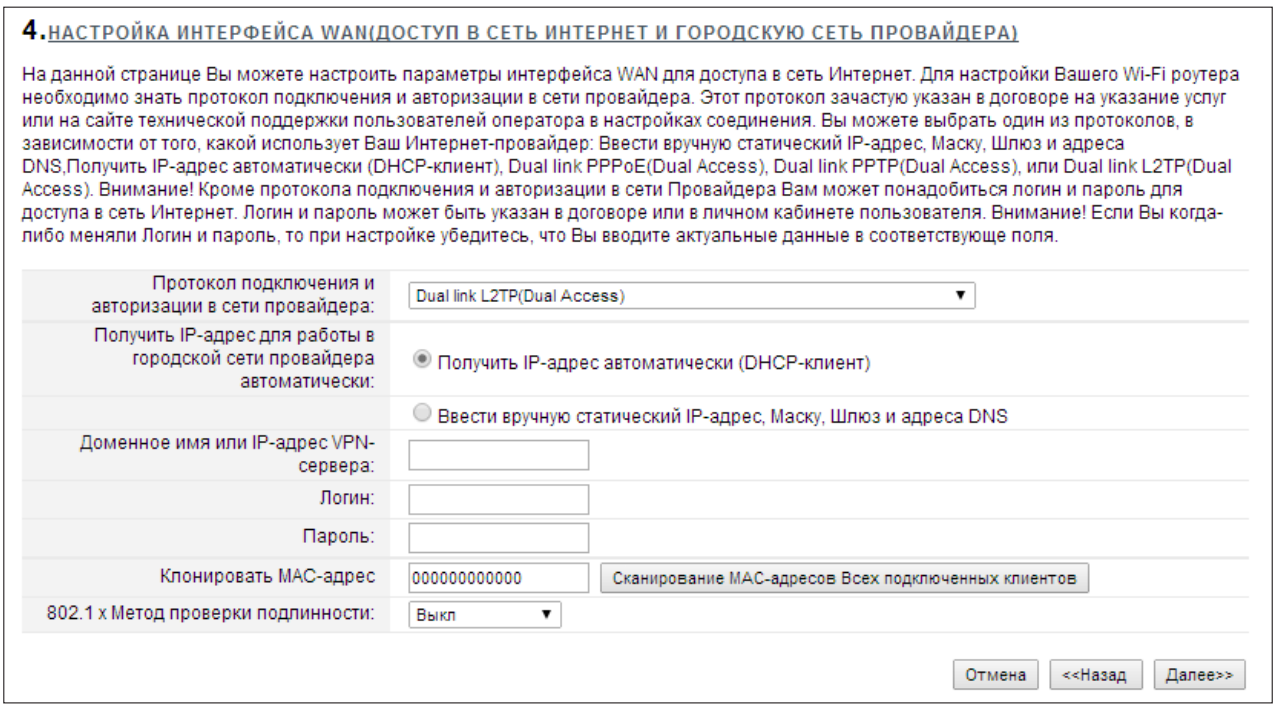
4.3.4.4 Dual Link PPTP (Dual Access)

Dual Link PPTP (Dual Access) – протокол технологии VPN (Point to Point Tunneling Protocol). Для настройки протокола подключения и авторизации в сети провайдера необходимо ввести логин и пароль для доступа в сеть Интернет в соответствующие поля, а также доменное имя VPN-сервера или его IP-адрес. Логин и пароль могут быть указаны в договоре или в личном кабинете пользователя. Если инженер провайдера при настройке соединения на компьютере создавал в папке сетевых подключений “Подключение удаленного доступа” или ярлык, имеющий такое же название как и ваш Интернет-провайдер, удалите его из папки сетевых подключений компьютера, чтобы избежать сетевых ошибок или двойной авторизации. Внимание! Если вы когда-либо меняли логин и пароль, при настройке убедитесь, что вводите актуальные данные в соответствующе пункты:



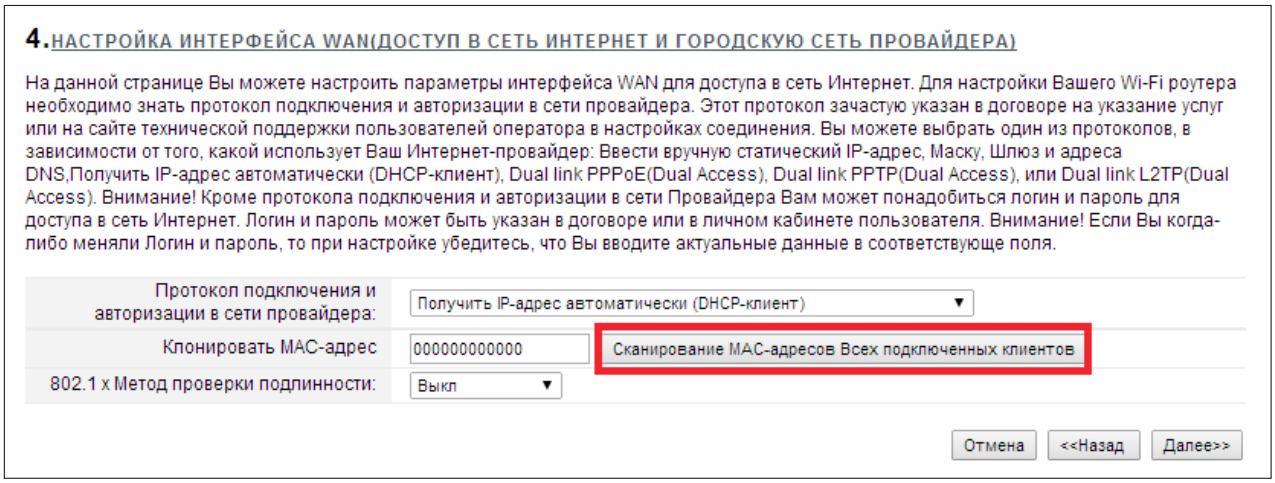
4.3.4.5 Dual Link L2TP (Dual Access)

Dual Link L2TP (Dual Access) – протокол технологии VPN (Layer 2 Tunneling Protocol). Для настройки протокола подключения и авторизации в сети провайдера необходимо ввести логин и пароль для доступа в сеть Интернет в соответствующие поля, а также доменное имя VPN-сервера или его IP-адрес. Логин и пароль могут быть указаны в договоре или в личном кабинете пользователя. Если инженер провайдера при настройке соединения на компьютере создавал в папке сетевых подключений “Подключение удаленного доступа” или ярлык, имеющий такое же название как ваш Интернет-провайдер, удалите его из папки сетевых подключений компьютера, чтобы избежать возможности сетевых ошибок или двойной авторизации. Внимание! Если вы когда-либо меняли логин и пароль, при настройке убедитесь, что вводите актуальные данные в соответствующе пункты:

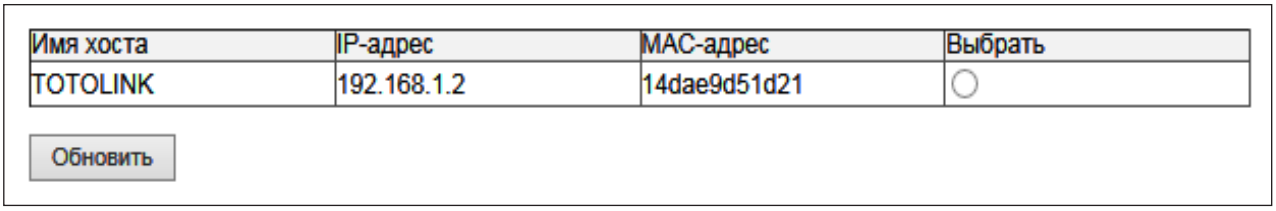


4.3.4.6 Функция ‘Клонировать MAC-адрес’

Данная функция доступна для любого протокола подключения и авторизации в сети провайдера. Если ваш Интернет-провайдер использует фильтр и авторизацию своих клиентов по MAC-адресам, и адрес компьютера, на котором был настроен доступ в Интернет до приобретения Wi-Fi роутера известен оператору, то нажмите кнопку ‘Сканирование MAC-адресов Всех подключенных клиентов’, а сам компьютер с MAC-адресом подключен к интерфейсу LAN, вам необходимо:

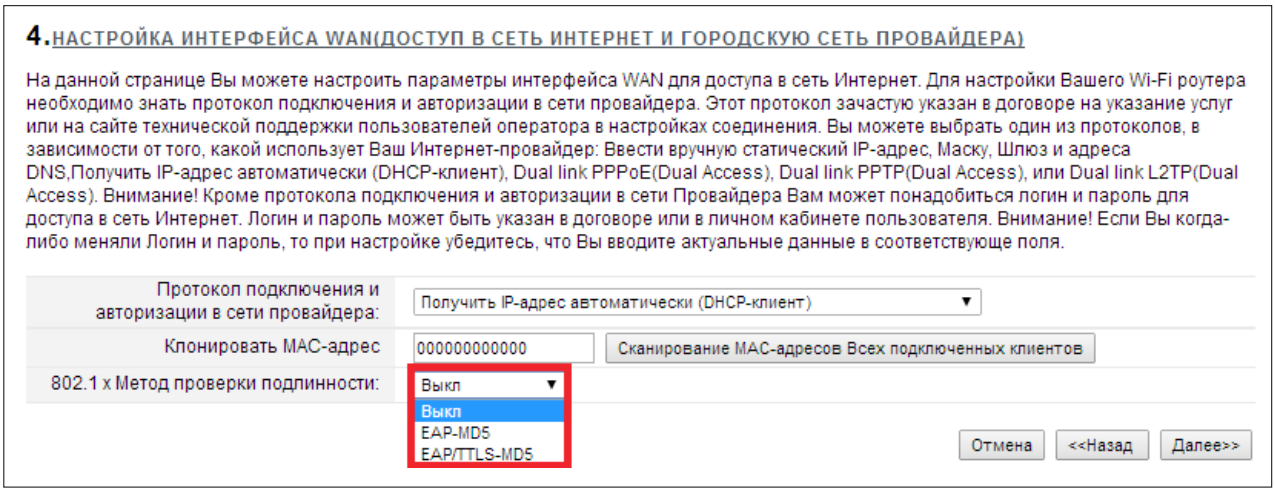


Откроется новое окно, где вы можете выбрать из списка всех подключенных клиентов именно то устройство, MAC-адрес которого известен вашему оператору, что избавит вас от звонков в службу технической поддержки Интернет-провайдера с целью прописать MAC-адрес интерфейса WAN вашего Wi-Fi роутера.

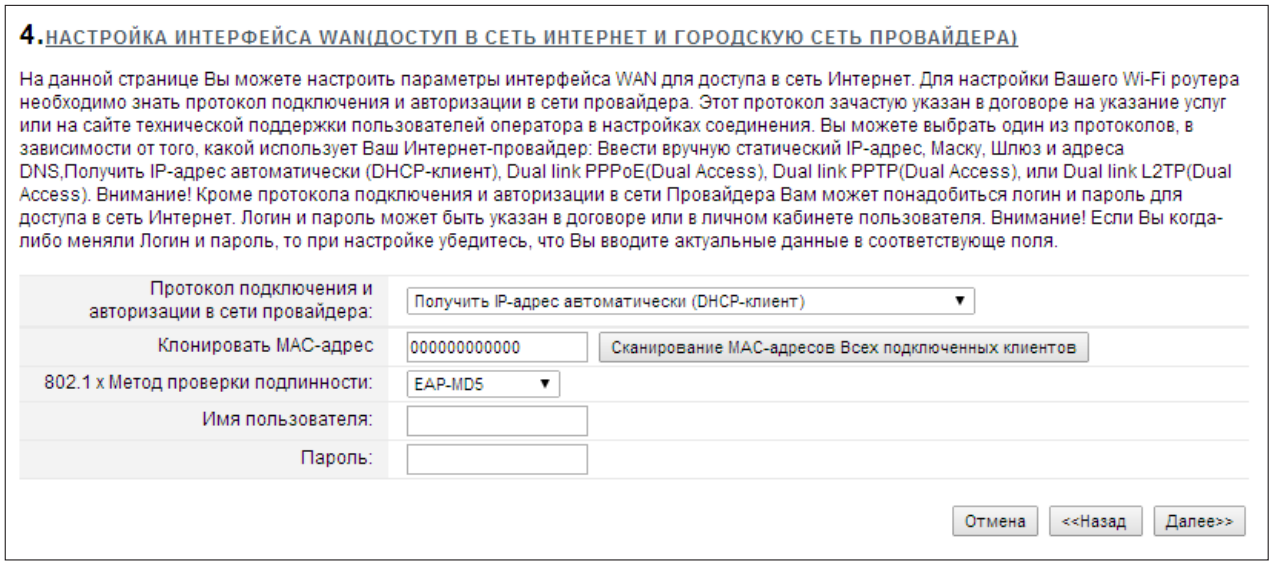


4.3.4.7 802.1 x Метод проверки подлинности

Данный метод доступен для любого протокола подключения и авторизации в сети провайдера.

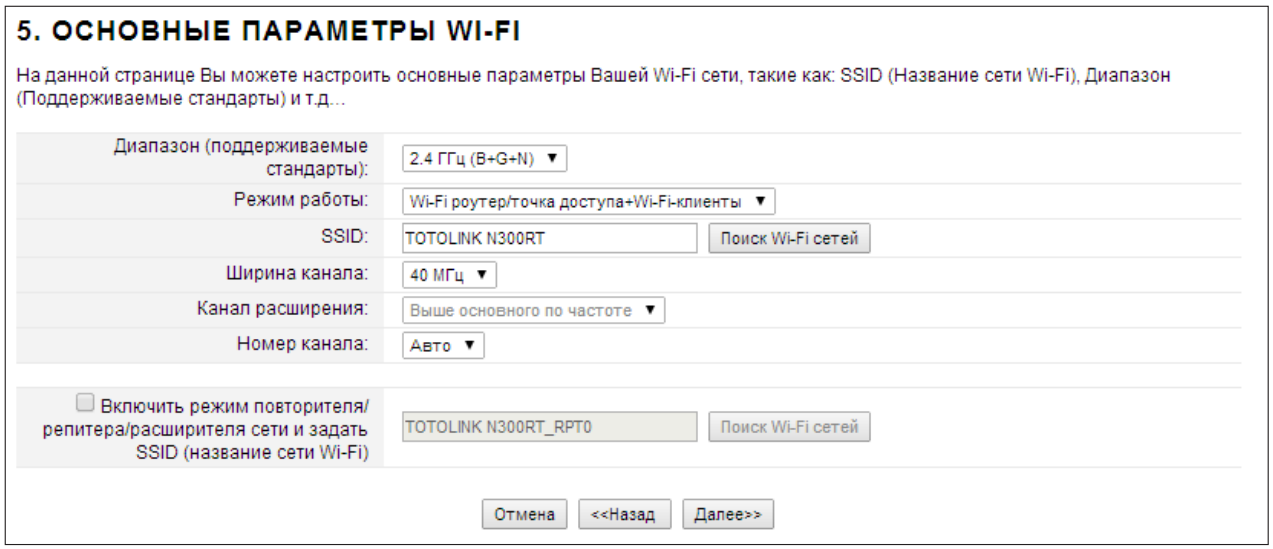


После выбора одного из методов появятся поля для ввода имени пользователя и пароля:



4.3.5 Основные параметры Wi-Fi

На данной странице можно настроить основные параметры Wi-Fi сети, такие как SSID (Название сети Wi-Fi), диапазон (поддерживаемые стандарты) и т.д.



Диапазон (поддерживаемые стандарты): Селектором можно выбрать частотный диапазон и поддерживаемые стандарты работы сети роутера. Стандарты сети Wi-Fi 802.11b и 802.11g более ранние и имеют меньшую пропускную способность, нежели стандарт 802.11n, который использует более совершенный тип модуляции сигнала (OFDM-метод). Рекомендуем выбрать 2,4 ГГц (B+G+N), так как эта настройка избавит от проблем возможной несовместимости устройства с оборудованием более ранних стандартов Wi-Fi.

Режим работы: Селектором можно выбрать режим работы точки доступа, встроенный в роутер. **

Выберите режим работы точки доступа, встроенной в роутер, исходя из соображений требуемой сетевой топологии вашей сети Wi-Fi.

Поддерживаемые режимы работы сети Wi-Fi, точкой доступа, встроенной в роутер:

► **Wi-Fi роутер/точка доступа+Wi-Fi-клиенты:** Режим работы позволяет пользователям обладающим мобильными устройствами (смартфоны, планшеты, ноутбуки) и не мобильным клиентам, оснащенными Wi-Fi адаптерами, подключиться к сети Wi-Fi и выйти в сеть Интернет. Данный режим идеально подходит для организации Wi-Fi сети с доступом в Интернет, а само устройство является технологичным решением для Wi-Fi, IPTV, P2P для дома или офиса.

► **Клиент:** В данном режиме устройство работает как обычный Wi-Fi адаптер, но оснащенный несколькими Ethernet-портами. Устройство в данном режиме позволяет подключить к сети Wi-Fi оборудование, оснащенное Ethernet-портами, но не имеющее встроенного Wi-Fi адаптера. Например, телевизоры, игровые приставки, телевизионные приставки, медиа плееры и т.д. В данном режиме работы сети Wi-Fi нельзя изменить параметры номера канала и его ширину, так как они будут взяты из той сети, подключение к которой было произведено в качестве клиента.

► **WDS:** Wireless Distribution System позволяет объединить множество устройств одной и той же модели, поддерживающих данный режим, в одну большую Wi-Fi сеть, но при этом не работать в режиме точки доступа. Устройства, объединенные в одну Wi-Fi сеть в режиме WDS, используют один и тот же частотный канал, что позволяет увеличить ее охват, но при этом будет наблюдаться деградация максимальной пропускной способности Wi-Fi при добавлении каждого нового устройства ввиду ограниченности разделяемого радиочастотного ресурса. Данный режим работы часто используется для организации крупно- и средне размерных сетей Wi-Fi, объединяя устройства “по воздуху” для нужд корпоративного сегмента, школ, университетов, аэропортов и т.д.

► **AP+WDS:** Режим позволяет объединить множество устройств одной и той же модели, поддерживающих данный режим, в одну большую Wi-Fi сеть и при этом работать в режиме точки доступа, предоставляя пользователям обладающим мобильными устройствами (смартфоны, планшеты, ноутбуки) и не мобильным клиентам, оснащенными Wi-Fi адаптерами, подключиться к сети Wi-Fi и выходить в сеть Интернет.

Важное примечание: *Если вы выбрали режим работы WDS, изменить SSID (название сети Wi-Fi) невозможно.*

** - Количество режимов работы точки доступа, встроенной в роутер, и их стабильность зависит от версии микропрограммного обеспечения (прошивки).

SSID (название сети Wi-Fi) или Service Set Identifier используется чтобы идентифицировать сеть Wi-Fi другими совместимыми с 802.11-устройствами, работающими в режиме **Wi-Fi роутер/точка доступа+Wi-Fi-клиенты** или в режиме AP+WDS.

Пояснение: Все клиентские Wi-Fi устройства, находящиеся в зоне покрытия роутера, будут получать широковещательные сообщения от точки доступа, встроенной в роутер с информацией о текущем SSID (названии сети Wi-Fi).

Ширина канала – ширина частотного канала Wi-Fi. Устройство поддерживает следующие значения ширины частотного канала технологии Wi-Fi:

20 МГц – стандартная ширина частотного канала Wi-Fi для 802.11b и 802.11g.

40 МГц – ширина частотного канала Wi-Fi, поддерживаемая 802.11n, значительно увеличивающая пропускную способность (значение выбрано по умолчанию).

Канал расширения – функция отвечает за добавление дополнительного частотного канала шириной 20 МГц к основному.

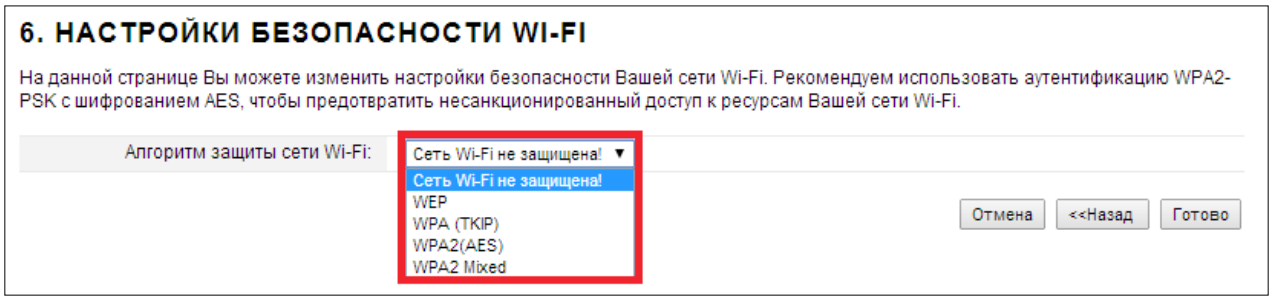
Выше основного по частоте: Значение по умолчанию – “Выше основного по частоте”, количество каналов работы технологии Wi-Fi составляет 11.

Ниже основного по частоте: Если выберите “Ниже основного по частоте”, количество каналов работы технологии Wi-Fi изменится на значение Auto, а параметр “Канал расширения” станет не активным. Изменив параметр на значение “Ниже основного по частоте”, количество каналов работы технологии Wi-Fi будет доступно для выбора селектором от 1 до 9. Лишь после того как вы выберите один из доступных каналов, параметр канала расширения будет снова активным для изменения. Если выберите “Выше основного по частоте”, количество каналов работы технологии Wi-Fi будет доступно для выбора селектором от 5 до 13.

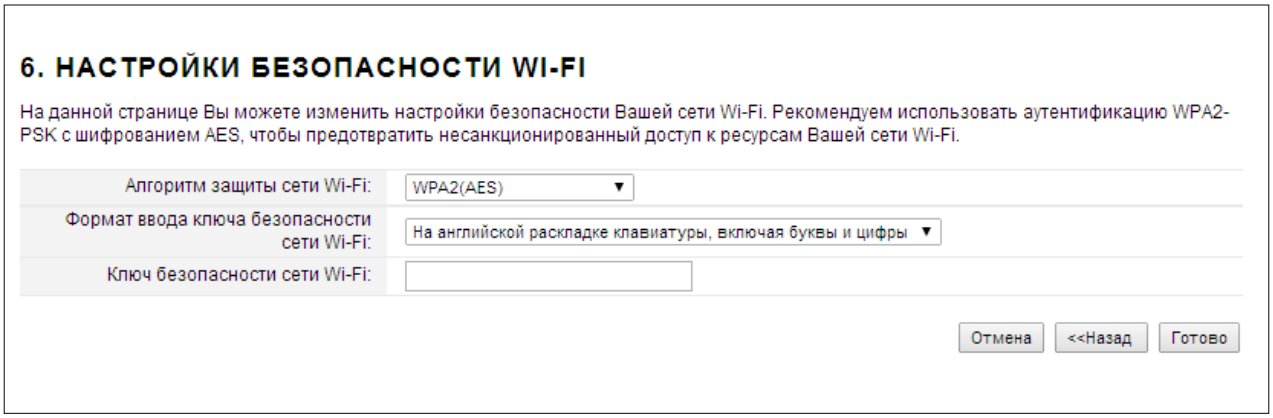
Номер канала – Селектор позволяет вручную выбрать номер частотного канала работы сети Wi-Fi.

Важное примечание: *Рекомендуем выбирать наименее загруженные частотные каналы для достижения наивысшей производительности сети Wi-Fi. На практике самыми загруженными оказываются частотные каналы с номерами 1, 6 и 11. Если вы решили выставить частотный канал с номерами 12, 13 или 14, не рекомендуем этого делать, значительная часть Wi-Fi оборудования на территории РФ и СНГ их не поддерживает. Придерживайтесь данной рекомендации и при выборе параметра канала расширения.*

4.3.6 Защита сети Wi-Fi

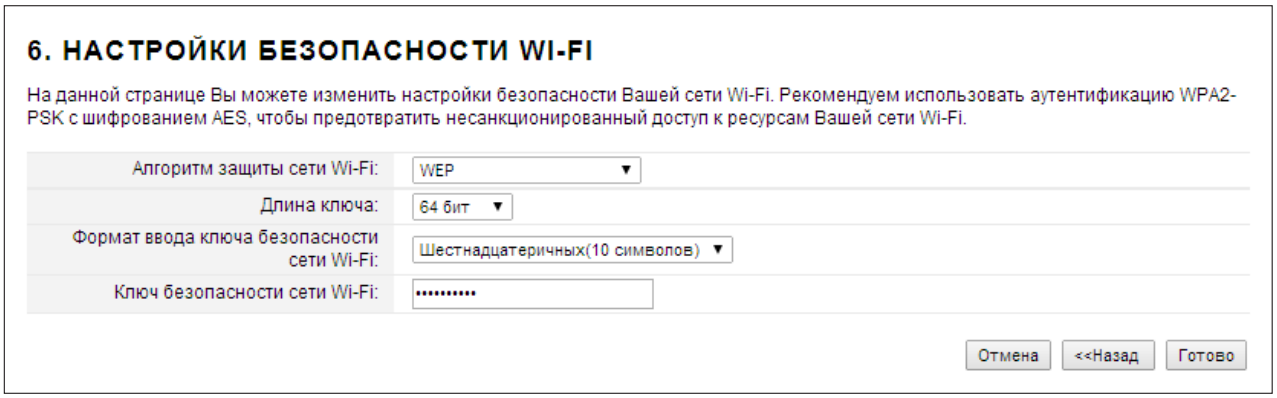


Алгоритм защиты сети Wi-Fi: Селектором можно выбрать один из поддерживаемых алгоритмов защиты сети Wi-Fi, поддерживаемых устройством: сеть Wi-Fi не защищена, WEP, WPA (TKIP), WPA2 (AES), WPA-Mixed. Выберите один из алгоритмов защиты сети Wi-Fi исходя из описания приведенного ниже и ваших потребностей:



1. WEP

WEP (Wired Equivalent Privacy) – стандартный алгоритм защиты сети Wi-Fi для группы стандартов IEEE 802.11, использующий алгоритм шифрования RC4. Выбирая алгоритм защиты сети Wi-Fi WEP стоит иметь ввиду, что все данные, передаваемые в сети Wi-Fi будут защищены шифрованием. WEP – самый старый алгоритм защиты сети Wi-Fi из всех поддерживаемых устройством. **Внимание!** Существует несколько программ, которые могут расшифровать и, как следствие, получить доступ к вашим данным, передаваемым по Wi-Fi, менее чем за 10 минут. Мы не рекомендуем использовать данный алгоритм.



Длина ключа: Селектором можно выбрать длину ключа шифрования алгоритма WEP 64 или 128 бит. Значение по умолчанию – 64 бита.

64 бита – Для длины ключа шифрования алгоритма WEP в 64 бита поддерживается два формата ввода ключа безопасности сети Wi-Fi:

• ASCII (на английской раскладке клавиатуры, включая буквы и цифры) длиной 5 символов.

• Если вы выбрали “Шестнадцатеричный (10 символов)” формат, ключ безопасности сети Wi-Fi необходимо вводить, начиная с обязательных символов 0x, например: 0x414234445.

128 бит – Для длины ключа шифрования алгоритма WEP в 128 бит поддерживается два формата ввода ключа безопасности сети Wi-Fi:

• ASCII (на английской раскладке клавиатуры, включая буквы и цифры) длиной в 13 символов.

• Если вы выбрали “Шестнадцатеричный (26 символов)” формат, ключ безопасности сети Wi-Fi необходимо вводить, начиная с обязательных символов 0x, например: 0x41424344454647484 94A4B4C4D

Формат ввода ключа безопасности сети Wi-Fi + Ключ безопасности сети Wi-Fi:

Данные параметры отвечают за длину и формат ввода ключа безопасности сети Wi-Fi, который необходимо будет вводить каждому новому Wi-Fi клиенту для подключения к устройству и последующего обмена зашифрованными данными.

Вашим устройством поддерживается два формата ввода ключа безопасности сети Wi-Fi (на английской раскладке клавиатуры, включая буквы и цифры) и шестнадцатеричный ключ.

Если вы выбрали параметр **“Длина ключа”** в 64 бита, при выборе формата ввода ключа безопасности сети Wi-Fi **“на английской раскладке клавиатуры, включая буквы и цифры”**, длина ключа безопасности сети Wi-Fi будет составлять 5 символов. Если при той же длине ключа – 64 бита вы выбрали “Шестнадцатеричный ключ”, длина ключа безопасности сети Wi-Fi будет составлять 10 символов.

Если вы выбрали параметр “Длина ключа” 128 бит, при выборе формата ввода ключа безопасности сети Wi-Fi “на английской раскладке клавиатуры, включая буквы и цифры”, длина ключа безопасности сети Wi-Fi будет составлять 13 символов. Если при той же длине ключа 128 бит вы выбрали “Шестнадцатеричный ключ”, длина ключа безопасности сети Wi-Fi будет составлять 26 символов.

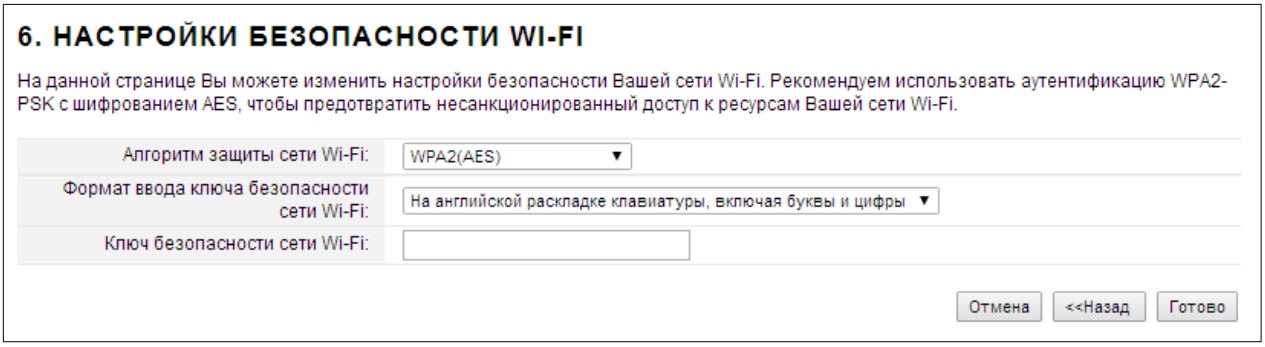
Ключ безопасности сети Wi-Fi: Пожалуйста, обратитесь к пункту “Длина ключа” для ввода ключа правильного формата и длины.

2. WPA/WPA2

WPA (Wi-Fi Protected Access) – рекомендуемый Wi-Fi Alliance алгоритм защиты сети Wi-Fi. Существует два подтипа данного алгоритма защиты сети Wi-Fi: WPA-personal, иногда именуемый как WPA Pre-Share Key (WPA/PSK), и WPA-Enterprise, иногда именуемый как WPA/802.1x. WPA2 (Wi-Fi Protected Access 2) – более криптографически стойкая ко взлому и более совершенная версия алгоритма защиты сети Wi-Fi, нежели WPA. Первый алгоритм рекомендован Wi-Fi Alliance как наилучший вариант защиты сети Wi-Fi, не приводящий к снижению скорости из-за шифрования и как наиболее надежный протокол для сетей стандарта IEEE 802.11n.

TKIP – протокол шифрования данных в сетях Wi-Fi, отвечающий за целостность ключа шифрования, который изменяется во времени и присваивается каждому пакету. Данный криптографический алгоритм является обязательным для алгоритмов защиты сети Wi-Fi WPA и WPA2.

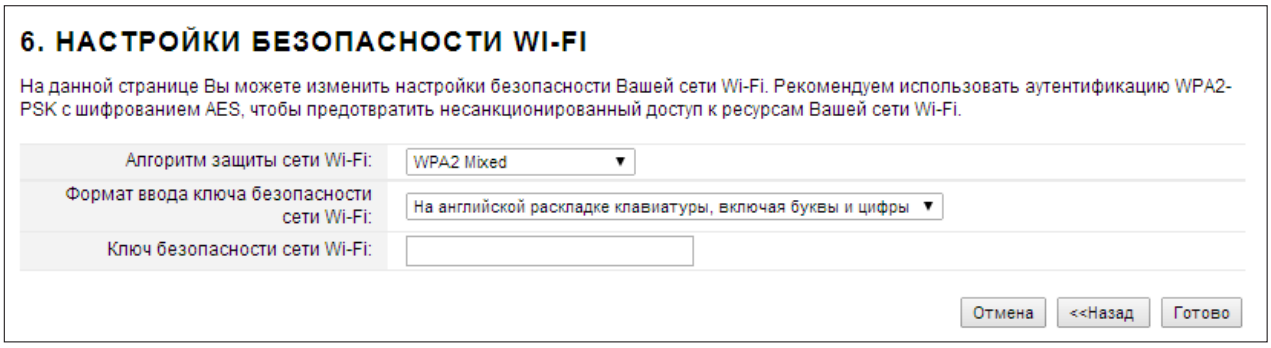
AES – протокол шифрования данных в сетях Wi-Fi, рекомендуемый для защиты сетей стандарта IEEE 802.11n совместно с аутентификацией WPA2. Данный криптографический алгоритм является обязательным для алгоритмов защиты сети Wi-Fi WPA и WPA2.



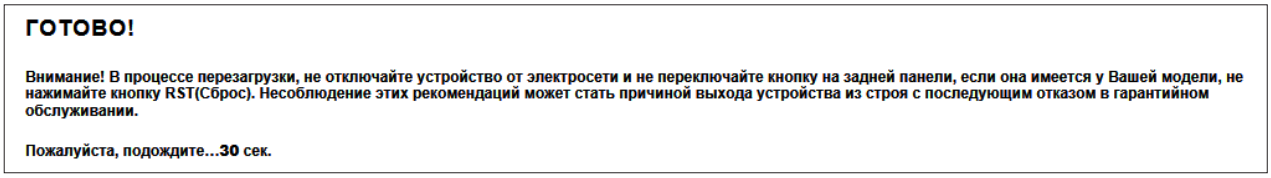
Формат ввода ключа безопасности сети Wi-Fi + Ключ безопасности сети Wi-Fi: Данные параметры отвечают за длину и формат ввода ключа безопасности сети Wi-Fi, который необходимо вводить каждому новому Wi-Fi клиенту для подключения к устройству и последующему обмену зашифрованными данными. Вашим устройством поддерживается два формата ввода ключа безопасности сети Wi-Fi: (на английской раскладке клавиатуры, включая буквы и цифры) и шестнадцатеричный ключ (64 символа). Затем необходимо ввести ключ безопасности сети Wi-Fi в поле напротив. Если вы выбрали формат ввода ключа безопасности сети Wi-Fi “на английской раскладке клавиатуры, включая буквы и цифры”, длина ключа безопасности сети Wi-Fi должна составлять от 8 до 63 символов. В том случае, если вы выбрали “Шестнадцатеричный ключ (64 символа)”, ключ безопасности сети Wi-Fi необходимо вводить, начиная с обязательных символов 0x, например: “0x321253abcde…”.

3. WPA-Mixed

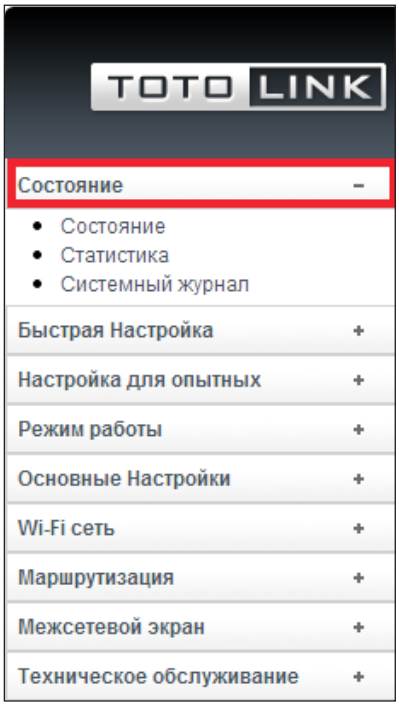
Опция позволяет использовать алгоритмы защиты сети Wi-Fi WPA и WPA2 совместно, сочетая преимущества каждого. Использование данного алгоритма защиты сети Wi-Fi обеспечивает наилучшую защиту сети Wi-Fi роутера и хороший уровень совместимости оборудования.



После того как вы завершили вышеописанные шаги, нажмите кнопку “Готово”, чтобы завершить работу мастера “Быстрой настройки”, после чего устройство выполнит перезагрузку и применить новые настройки:

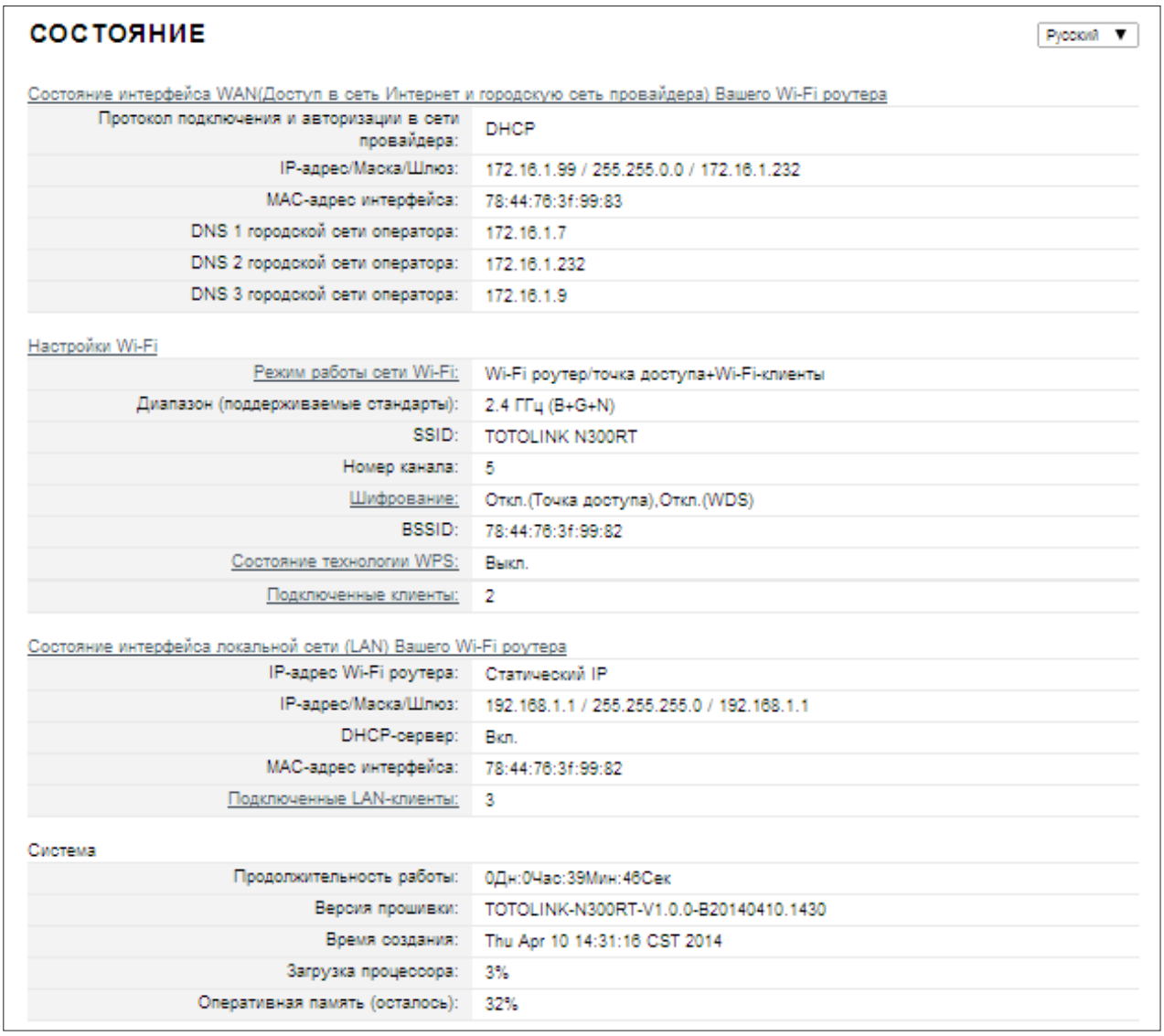


4.4 Состояние



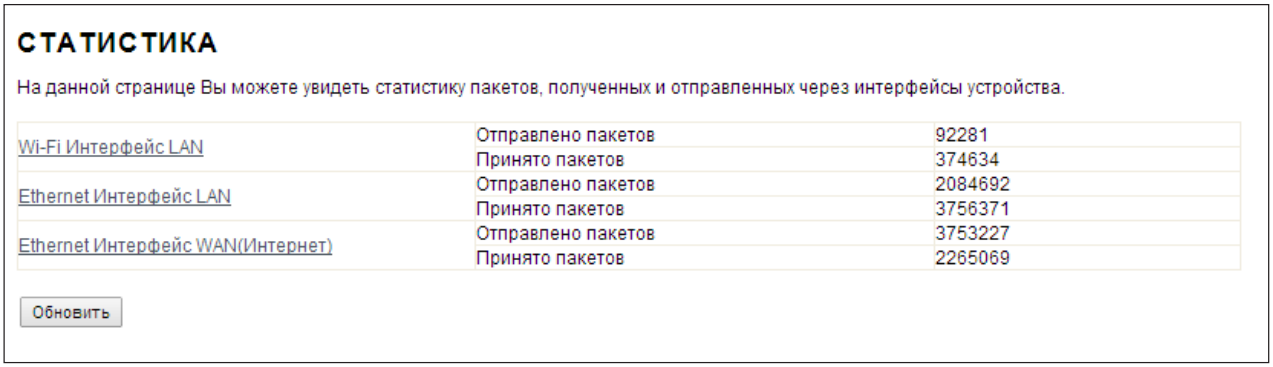
4.4.1 Состояние

Страница отображает текущее состояние всех интерфейсов роутера: WAN, LAN и сеть Wi-Fi. Помимо состояния интерфейсов устройства вы можете увидеть их текущие настройки и важную системную информацию об устройстве: продолжительность работы, версию прошивки и т.д.



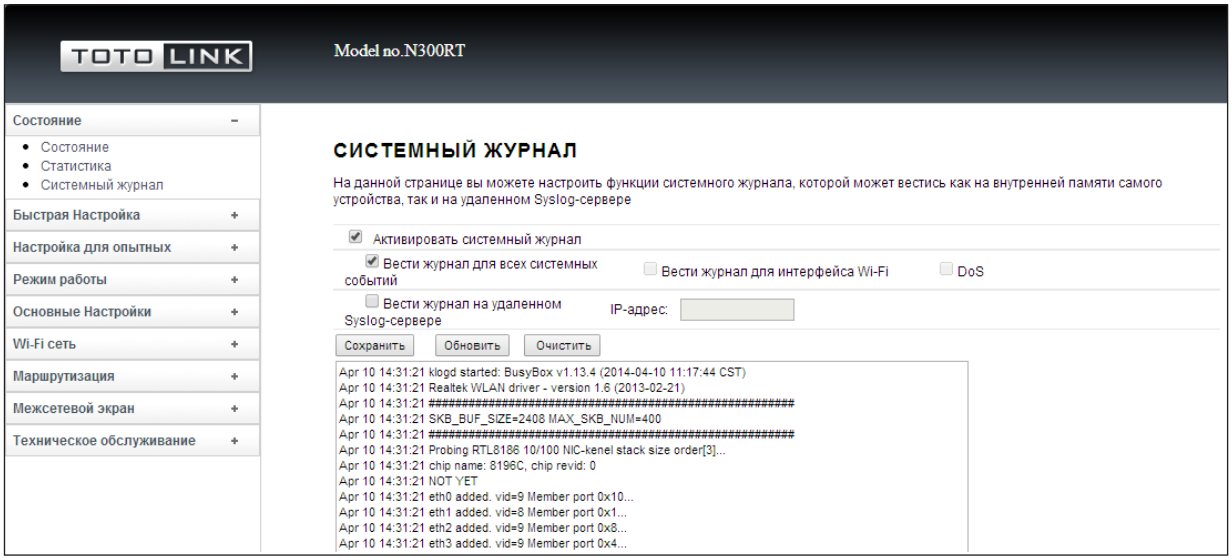
4.4.2 Статистика

На странице можно увидеть статистику пакетов, полученных и отправленных через интерфейсы устройства.



4.4.3 Системный журнал

На странице можно настроить функции системного журнала, который может быть записан как на внутренней памяти устройства, так и на удаленном Syslog-сервере.



Активировать системный журнал: Поставьте галочку в окне, чтобы включить функцию “Системный журнал”. Функция ведения системного журнала по умолчанию отключена. Ниже можно выбрать и конкретизировать тип ведения системного журнала: для всех системных событий, вести журнал для интерфейса Wi-Fi, DoS.

Вести журнал на удаленном Syslog-сервере: Поставьте галочку в окне, чтобы включить функцию отсылки сообщений функции “Системный журнал” на удаленный Syslog-сервер.

IP-адрес: Введите IP-адрес Syslog-сервера, на который будут отсылаться сообщения функции “Системный журнал”.

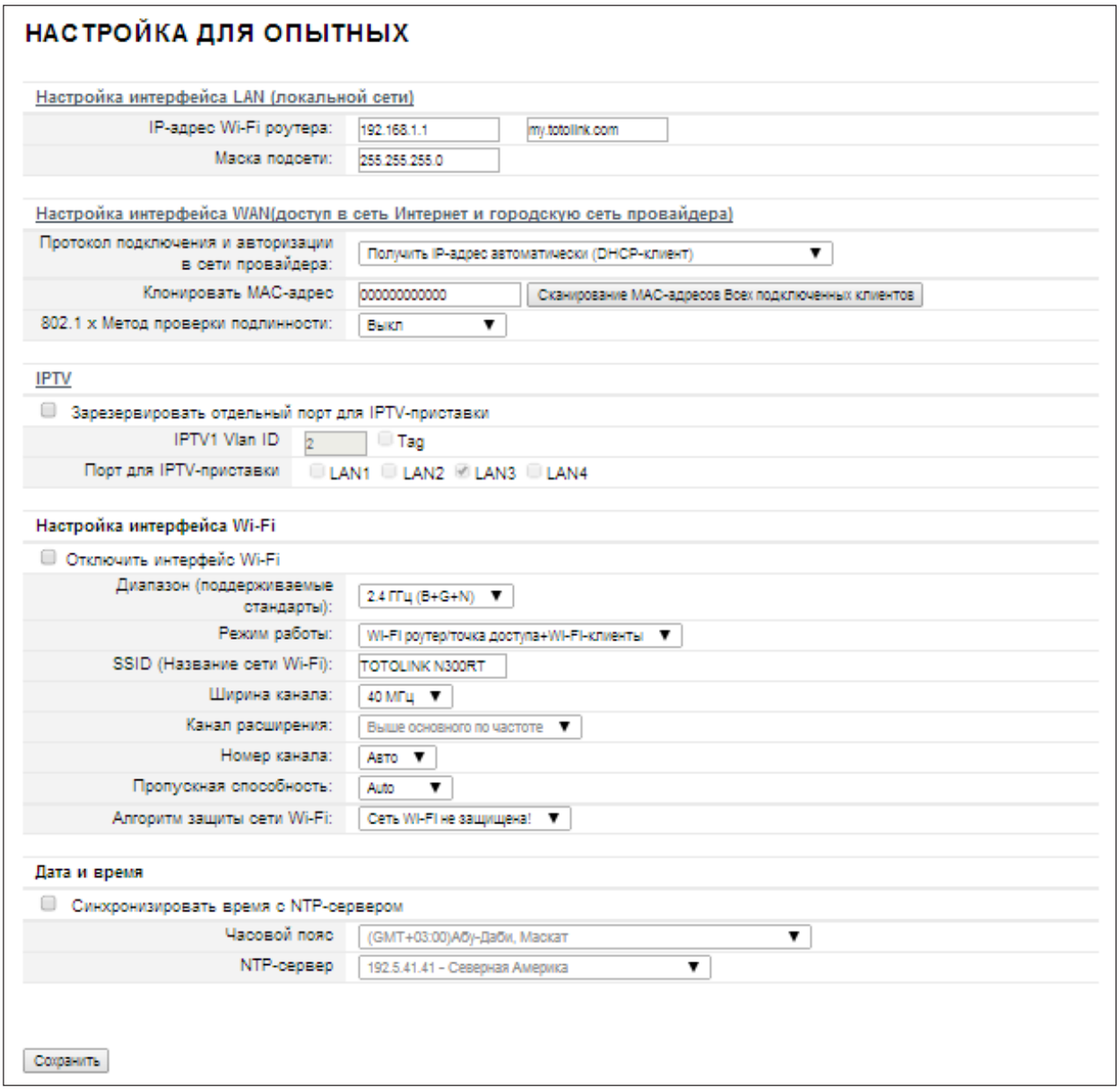
Нажмите кнопку “Сохранить” для сохранения выполненных изменений в настройках устройства.

5. ПРОДВИНУТЫЕ НАСТРОЙКИ

Глава описывает полный функционал, доступный для продвинутых пользователей, способных самостоятельно настроить роутер. Данный раздел включает в себя описание разделов: “Основные настройки”, “Wi-Fi сеть”, “Маршрутизация”, “Межсетевой экран” и “Техническое обслуживание”. Изменять данные настройки рекомендуется технически подготовленным пользователям.

5.1 Настройка для опытных

На данной странице опытные пользователи могут настроить Wi-Fi роутер полностью. На одной странице сразу можно настроить параметры интерфейса LAN (локальной сети), интерфейса WAN (доступ в сеть Интернет и городскую сеть провайдера), зарезервировать отдельный порт для работы IPTV-приставки или несколько, Настроить сеть Wi-Fi и защитить ее, синхронизировать системное время с NTP-сервером в сети Интернет.



Для получения справочной информации по пункту «Настройка интерфейса LAN» – обратитесь к пункту 4.3.3 данной инструкции.

В данном меню помимо настроек, описанных в пункте 4.3.3 данной инструкции, вы можете сменить доменное имя присвоенное вашему Wi-Fi роутеру в заводских настройках (my.totolink.com).

Для получения справочной информации по пункту «Настройка интерфейса WAN (доступ в сеть Интернет и городскую сеть провайдера)» обратитесь к пункту 4.3.4 данной инструкции.

Для получения справочной информации по функции ‘Клонировать MAC-адрес’ обратитесь к пункту 4.3.4.6 данной инструкции.

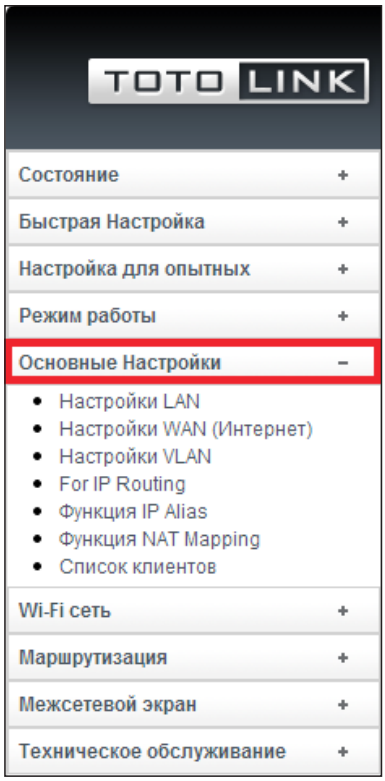
Для получения справочной информации по функции «802.1 x Метод проверки подлинности» обратитесь к пункту 4.3.4.7 данной инструкции.

IPTV: Поставьте галочку зарезервировать отдельный порт для IPTV-приставки для активации данной функции и выбора порта или нескольких портов для подключения телевизионных IPTV-приставок к соответствующим интерфейсам. Если ваш Интернет-провайдер предоставляет дополнительные сервисы по технологии Triple Play или VLAN, то предварительно уточнив параметры VLAN ID, введите их в соответствующие поля для каждого конкретного типа сервиса.

Для получения справочной информации по пункту «Настройка интерфейса Wi-Fi» обратитесь к пунктам 4.3.5 и 4.3.6 данной инструкции.

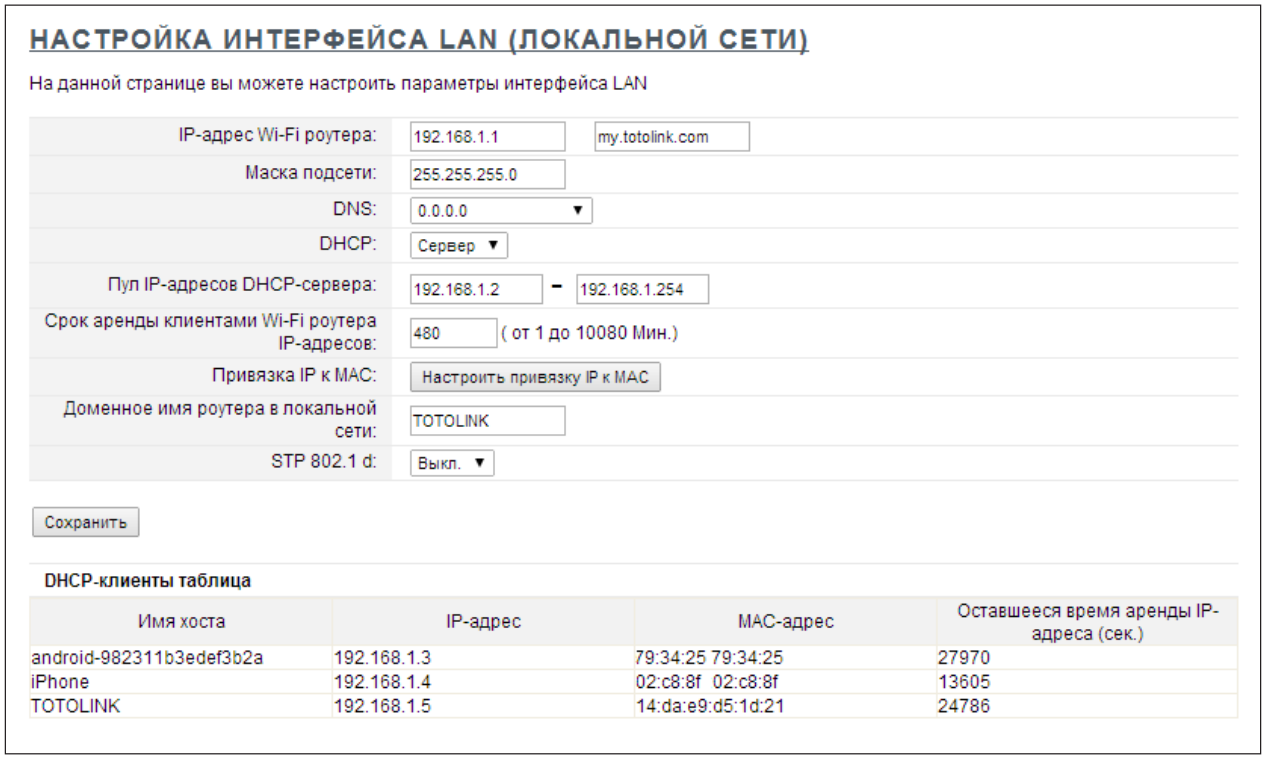
Для получения справочной информации по пункту «Дата и время» обратитесь к пункту 4.3.2 данной инструкции.

5.2 Основные настройки



5.2.1 Настройки LAN

На данной странице вы можете настроить параметры интерфейса LAN.

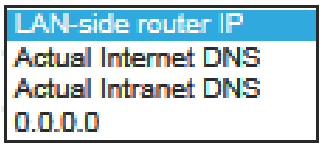


IP-адрес Wi-Fi роутера: Это IP-адрес по которому доступен WEB-интерфейс устройства для клиентов локальной сети LAN (включая сеть Wi-Fi). Помимо этой функции данный IP-адрес будет использоваться устройством для правил маршрутизации (использоваться в качестве IP-адреса основного шлюза).

В данном меню помимо настроек, описанных в пункте 4.3.3 данной инструкции, вы можете сменить доменное имя присвоенное вашему Wi-Fi роутеру в заводских настройках (my.totolink.com).

> ***Важное примечание:*** *Если вы изменяете данный IP-адрес, после его смены, для доступа к WEB-интерфейсу роутера, необходимо вводить в адресную строку браузера новый IP-адрес, а не адрес по умолчанию. Помимо этого, если вы изменяете подсеть работы устройства, изменяя его IP-адрес соответствующим образом, все правила касающиеся IP-адресов роутера и клиентских устройств, таких как перенаправление портов, DMZ и т.д. работать не будут! Необходимо заново сконфигурировать все правила.*

Маска подсети: Параметр используется для определения классификации IP-сетей для выбранного диапазона IP-адресов. Например, 255.255.255.0 – типовое значение маски подсети для сетей класса C, который поддерживает IP-адресацию от 192.0.0.x до 223.255.255.x. IP-сети класса C используют маски подсети длиной в 24 бита для определения адреса сети и 8 бит для определения адреса конкретного конечного клиентского устройства (хоста).



DNS: Селектором можно выбрать алгоритм работы устройства с DNS-серверами.

LAN-side router IP (DNS-сервером локальной сети LAN выступает IP-адрес Wi-Fi роутера и работает механизм DNS-proxy)

Actual Internet DNS (DNS-сервером локальной сети LAN выступают только IP-адреса полученные на интерфейсе WAN для работы в сети Интернет)

Actual Intranet DNS (DNS-сервером локальной сети LAN только IP-адреса полученные на интерфейсе WAN для работы в Городской сети провайдера) адрес 0.0.0.0 (round robin-алгоритм работы).

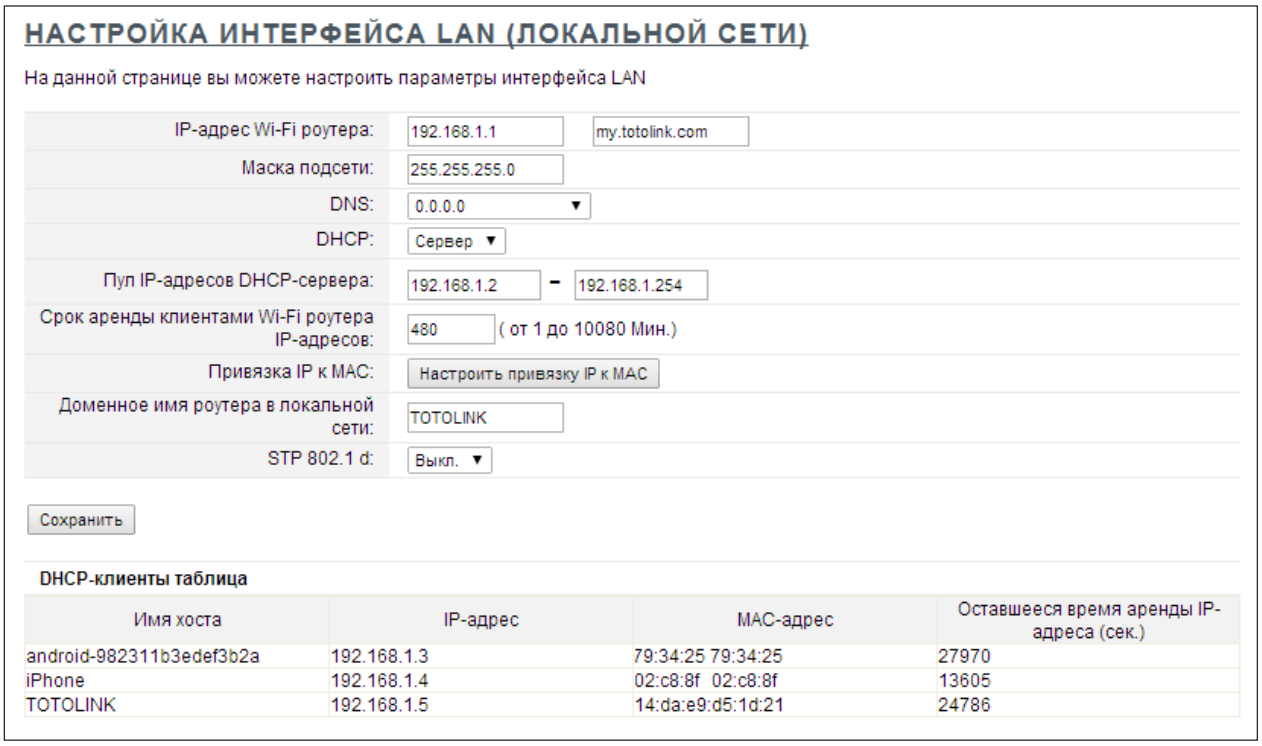
DHCP: Селектором можно выбрать Сервер – Вкл. или Выкл. DHCP-сервер устройства, автоматически назначающий подключенным клиентам IP-адреса, включая клиентов сети Wi-Fi.

Пул IP-адресов DHCP-сервера: В данных двух полях можно задать диапазон IP-адресов, доступных к автоматическому присвоению клиентским устройствам, подключенных к роутеру, как через интерфейсы LAN, так Wi-Fi.

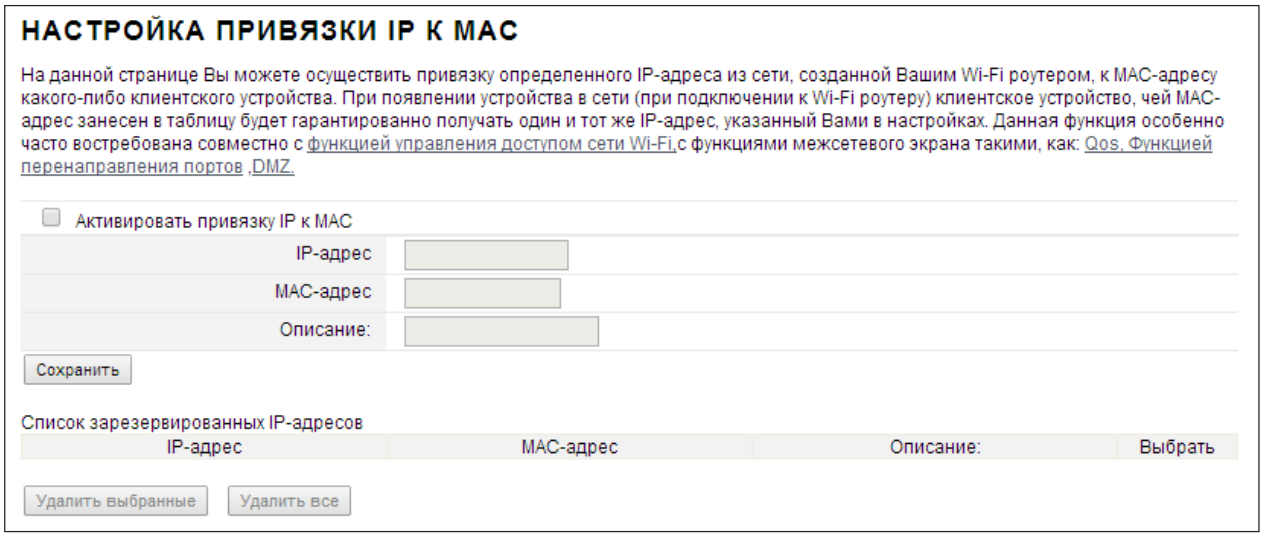
Срок аренды клиентами Wi-Fi роутера IP-адресов: IP-адреса, назначенные клиентским устройствам DHCP-сервером роутера, будут действительными в течение установленного времени. Увеличение времени аренды IP-адреса клиентами устройства чревато потенциальными конфликтами IP-адресов. Уменьшение времени приводит к понижению вероятности возникновения конфликтов IP-адресов, но может стать причиной периодичного кратковременного отсутствия соединения во время получения нового IP-адреса клиентским устройством от DHCP-сервера роутера. Оставшееся время аренды IP-адреса клиентским устройством отображается в секундах.

Доменное имя роутера в локальной сети: Введите в поле желаемое доменное имя роутера.

STP 802.1 d: Протокол IEEE 802.1d Spanning Tree Protocol (STP) разработан для поиска самого короткого пути в сети, чтобы избежать петлей в топологии сети. При включении протокола STP роутер будет посылать и передавать служебные пакеты по Bridge Protocol Data Units (BPDU) на другие сетевые устройства. Если протокол STP выключен (по умолчанию выключен), роутер будет работать как обычный шлюз и в сетевой топологии не будет петли.



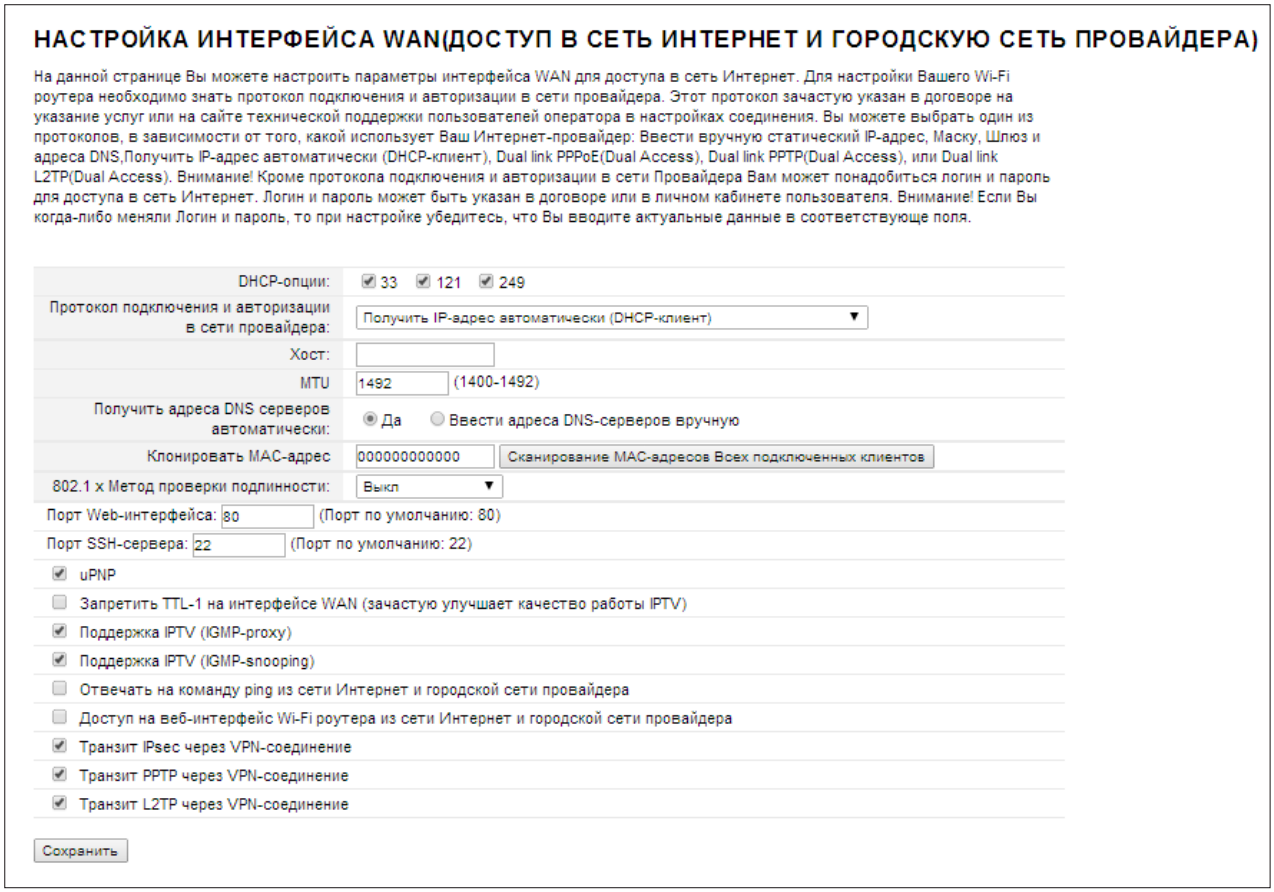
Привязка IP к MAC: Нажмите на кнопку “Настроить привязку IP к MAC”, чтобы осуществить статическую привязку MAC-адреса клиентского устройства к статическому IP-адресу из той же подсети, что и его DHCP-сервер, благодаря которой устройство всегда будет иметь один и тот же, заранее известный устройству IP.



5.2.2 Настройки WAN (Интернет)

На данной странице можно настроить параметры интерфейса WAN для доступа в сеть Интернет. Для настройки роутера необходимо знать протокол подключения и авторизации в сети провайдера. Этот протокол обычно указан в договоре на указание услуг или на сайте технической поддержки пользователей оператора в настройках соединения. Вы можете выбрать один из протоколов в зависимости от того, какой использует Интернет-провайдер: 802.1 x, ввести вручную статический IP-адрес, маску, шлюз и адреса DNS, получить

IP-адрес автоматически (DHCP-клиент), Dual Link PPPoE (Dual Access), Dual Link PPTP (Dual Access) или Dual Link L2TP (Dual Access). Внимание! Кроме протокола подключения и авторизации в сети провайдера может понадобиться логин и пароль для доступа в сеть Интернет. Логин и пароль могут быть указаны в договоре или в личном кабинете пользователя. **Внимание!** Если вы когда-либо меняли логин и пароль, при настройке убедитесь, что вводите актуальные данные в соответствующе поля.



Для получения справочной информации по пункту **«Настройка интерфейса WAN (доступ в сеть Интернет и городскую сеть провайдера)»** обратитесь к пункту 4.3.4 данной инструкции.

Для получения справочной информации по функции **«Клонировать MAC-адрес»** обратитесь к пункту 4.3.4.6 данной инструкции.

Для получения справочной информации по функции «**802.1x Метод проверки подлинности»** обратитесь к пункту 4.3.4.7 данной инструкции.

MTU: Это максимальный размер поля payload пакета данных в байтах (Maximum Transmission Unit). Изменять данный параметр не рекомендуется, кроме случаев, когда есть рекомендации Интернет-провайдера.

DNS: Сервер в сети Интернет-провайдера DNS (Domain Name System), который работает по принципу телефонной книги для сети Интернет, сопоставляющий то, что вы видите в адресной строке Интернет-браузера в качестве названия Интернет-сайта с IP-адресом сервера, где этот сайт непосредственно находится (параметр обычно указан в договоре на оказание услуг связи).

Клонировать MAC-адрес: MAC-адрес – уникальный адрес интеллектуального сетевого интерфейса, такого как интерфейс WAN, LAN, Wi-Fi. Помимо интерфейсов самого роутера, MAC-адреса есть у сетевого адаптера компьютера, Wi-Fi адаптера и т.д. Некоторые провайдеры используют фильтрацию клиентов по MAC-адресам, храня их в специальной базе, закрывая неизвестным клиентским устройствам несанкционированный доступ к сети. MAC-адрес интерфейса WAN (порт, куда подключается кабель Интернет-провайдера) не содер-

жится в базе вашего Интернет-провайдера, ему известен лишь MAC-адрес сетевой платы вашего компьютера, который должен быть подключен к порту LAN устройства. Данная функция позволяет ввести вручную MAC-адрес устройства, известного вашему Интернет-провайдеру и заменить им текущий MAC-адрес интерфейса WAN роутера. Таким образом оператор не заметит изменений. Данная функция избавляет от необходимости звонить в службу технической поддержки оператора и просить инженеров ввести MAC-адрес нового устройства в базу.

Порт Web-интерфейса: В данном поле можно изменить номер порта для доступа на Web-интерфейс устройства.

Порт SSH-сервера: В данном поле можно изменить номер порта для доступа на SSH-сервер устройства.

Запретить TTL-1 на интерфейсе WAN (зачастую улучшает качество работы IPTV): Опция отменяет вычитание значение единицы от параметра TTL (Time To Live) для всех пакетов, приходящих на интерфейс WAN.

uPNP: протокол Universal Plug and Play (UPnP). Функция автоматически определяет номер порта роутера, который необходимо открыть для устройства или приложения, чтобы обойтись без его настройки в процессе эксплуатации.

Поддержка IPTV (IGMP-proxy)/ Поддержка IPTV (IGMP-snooping): сетевой протокол (Internet Group Management Protocol), используемый для управления подпиской к multicast-группам. Протокол зачастую используется Интернет-провайдерами для предоставления дополнительных услуг, например, IPTV. Если вы поставите галочку в окне, multicast-потоки будут проходить через WAN порт устройства. Функция доступна только при включенной опции NAT.

Отвечать на команду ping из сети Интернет и городской сети провайдера: Если вы поставите галочку в окне, пользователи внешней сети будут получать ответ на команду Ping от интерфейса WAN вашего роутера.

Доступ на веб-интерфейс Wi-Fi роутера из сети Интернет и городской сети провайдера: Данный параметр разрешает доступ на веб-интерфейс извне.

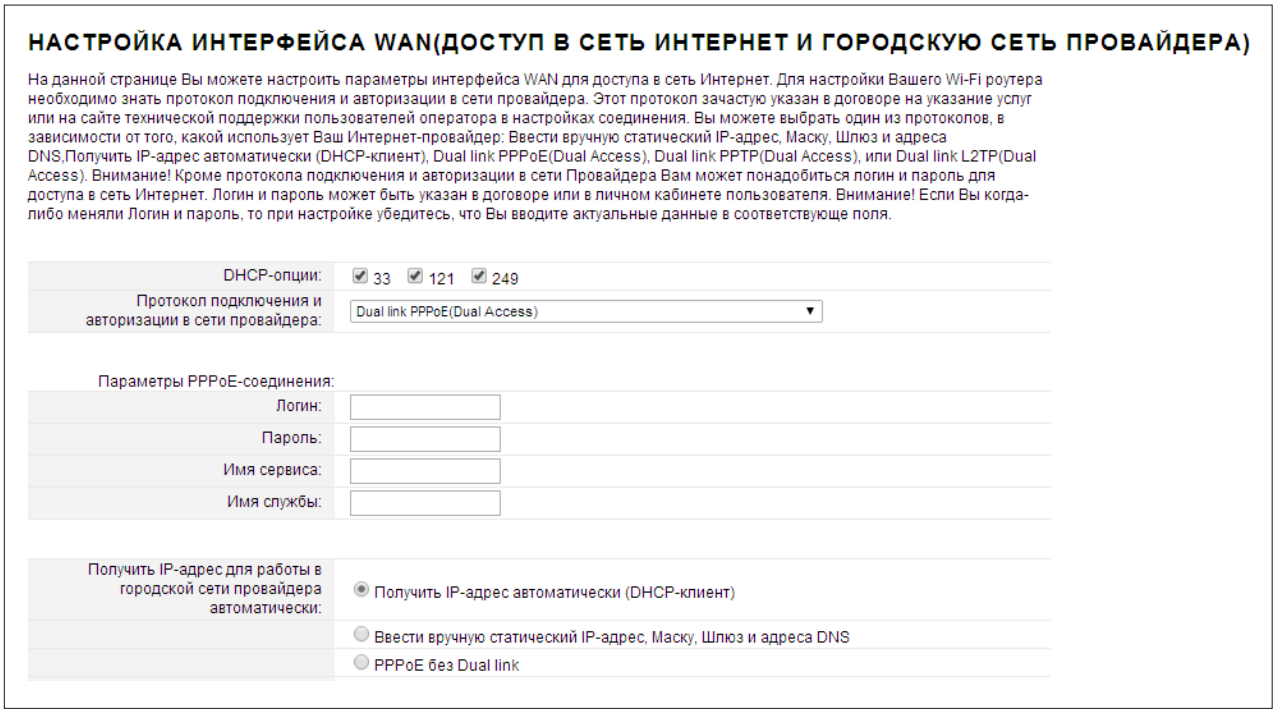
Транзит IPsec через VPN-соединение: параметр разрешает установить соединение из локальной сети вашего роутера внутри существующего VPN-соединения на интерфейсе WAN.

Транзит PPTP через VPN-соединение: параметр разрешает установить соединение из локальной сети вашего роутера внутри существующего VPN-соединения на интерфейсе WAN.

Транзит L2TP через VPN-соединение: параметр разрешает установить соединение из локальной сети вашего роутера внутри существующего VPN-соединения на интерфейсе WAN.

5.2.2.1 Dual Link PPPoE (Dual Access)

PPPoE (Point-to-Point Protocol over Ethernet) – часто используемый протокол инкапсуляции данных для доступа в сеть Интернет, использующий защищенное соединение между двумя сетевыми интерфейсами (например, интерфейс WAN роутера и сервер авторизации Интернет-провайдера). Если инженер провайдера при настройке соединения на компьютере создавал в папке сетевых подключений “Высокоскоростное подключение”, выберите именно этот протокол подключения и авторизации в сети провайдера, предварительно удалив “Высокоскоростное подключение” из папки сетевых подключений вашего компьютера.



Логин: Введите в данное поле логин, присвоенный Интернет-провайдером (данный параметр обычно указан в договоре на оказание услуг связи).

Пароль: Введите в поле пароль, присвоенный Интернет-провайдером (данный параметр обычно указан в договоре на оказание услуг связи).

Получить IP-адрес для работы в городской сети провайдера автоматически: Параметр характерен только для протоколов подключения и авторизации в сети провайдера с поддержкой технологии Dual Link: Dual Link PPPoE (Dual Access), Dual Link PPTP (Dual Access) или Dual Link L2TP (Dual Access). Если Интернет-провайдер помимо услуги доступа в сеть Интернет предоставляет дополнительные сервисы (например, IPTV, игровые локальные серверы, локальные торрент-трекеры, расположенные в локальной сети масштаба города или района присутствия оператора), необходимо выбрать один из способов получения IP-адреса для работы в сети вашего Интернет-провайдера: получить IP-адрес автоматически (DHCP-клиент) / ввести вручную статический IP-адрес, маску, шлюз и адреса DNS / PPPoE без Dual Link.

Алгоритм работы подключения: роутер поддерживает три алгоритма работы подключения.

- **Всегда подключено к сети Интернет:** При выборе данного алгоритма работы подключения, в случае потери соединения с сетью Интернет, оно будет восстановлено автоматически.

- **Подключаться к сети Интернет по запросу:** При выборе данного алгоритма работы подключения, соединение с сетью Интернет будет разорвано автоматически через заданный интервал времени и автоматически восстановлено в случае, когда понадобится доступ в сеть Интернет.

• **Подключаться к Интернет вручную:** Выбрав данный алгоритм работы подключения, можно нажать кнопку “Подключить” или “Отключить”, чтобы установить или прервать соединение с сетью Интернет.

Имя службы (AC name): Необязательный параметр. Вводите значение в данное поле только в случае, если параметр указан в договоре на оказание услуг связи с вашим Интернет-провайдером.

Имя сервиса (Service name): Необязательный параметр. Вводите значение в данное поле только в случае, если параметр указан в договоре на оказание услуг связи с вашим Интернет-провайдером.

MTU: Это максимальный размер поля payload пакета данных в байтах (Maximum Transmission Unit). Изменять данный параметр не рекомендуется кроме случаев, когда есть рекомендации Интернет-провайдера.

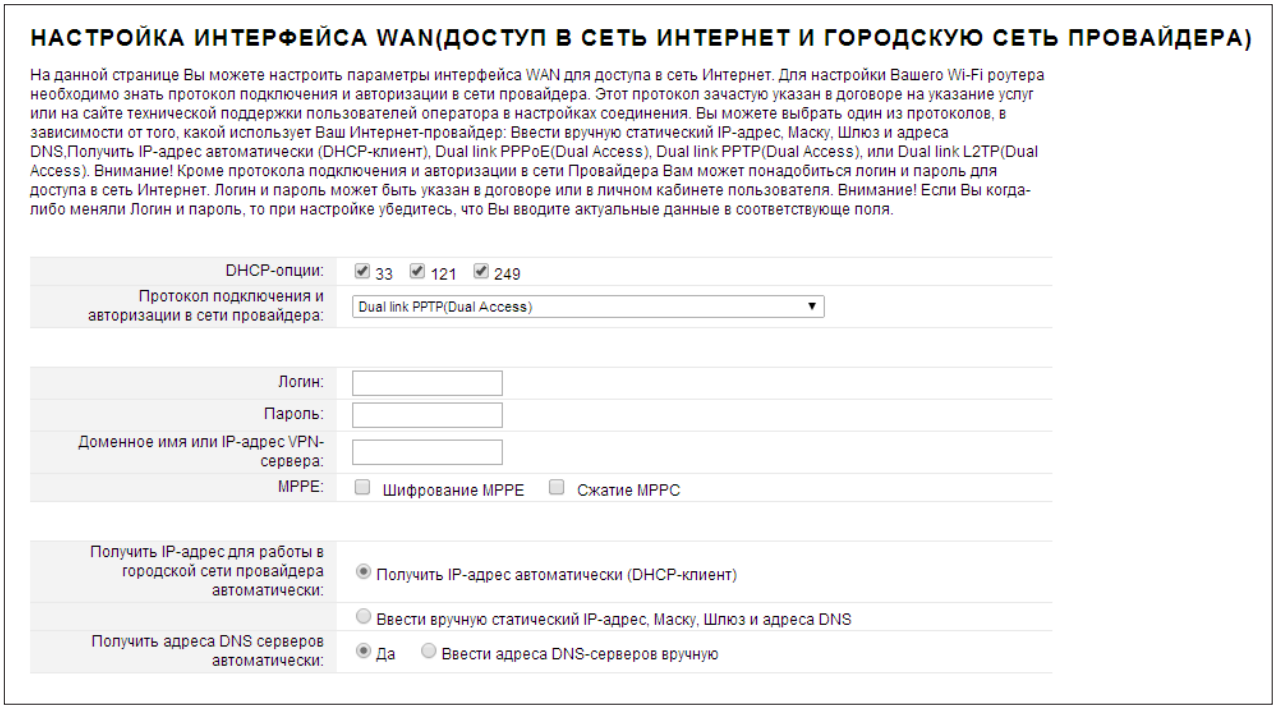
DNS: Сервер в сети Интернет-провайдера DNS (Domain Name System), который работает по принципу телефонной книги для сети Интернет, сопоставляющий то, что вы видите в адресной строке Интернет-браузера в качестве названия Интернет-сайта с IP-адресом сервера, где этот сайт непосредственно находится (параметр обычно указан в договоре на оказание услуг связи).

Клонировать MAC-адрес: MAC-адрес – уникальный адрес интеллектуального сетевого интерфейса, такого как интерфейс WAN, LAN, Wi-Fi. Помимо интерфейсов самого роутера, MAC-адреса есть у сетевого адаптера компьютера, Wi-Fi адаптера и т.д. Некоторые провайдеры используют фильтрацию клиентов по MAC-адресам, храня их в специальной базе, закрывая неизвестным клиентским устройствам несанкционированный доступ к сети. MAC-адрес интерфейса WAN (порт, куда подключается кабель Интернет-провайдера) не содержится в базе вашего Интернет-провайдера, ему известен лишь MAC-адрес сетевой платы вашего компьютера, который должен быть подключен к порту LAN устройства. Данная функция позволяет ввести вручную MAC-адрес устройства, известного вашему Интернет-провайдеру и заменить им текущий MAC-адрес интерфейса WAN роутера. Таким образом, оператор не заметит изменений. Данная функция избавляет от необходимости звонить в службу технической поддержки оператора и просить инженеров ввести MAC-адрес нового устройства в базу.

Обратитесь к пункту 5.2.2 данной инструкции для получения справочной информации по функциям и элементам не проиллюстрированных на изображении веб-интерфейса.

5.2.2.2 Dual Link PPTP (Dual Access)

Dual Link PPTP (Dual Access) – протокол технологии VPN (Point to Point Tunneling Protocol). Для настройки протокола подключения и авторизации в сети провайдера необходимо ввести логин и пароль для доступа в сеть Интернет в соответствующие поля, а также доменное имя VPN-сервера или его IP-адрес. Логин и пароль могут быть указаны в договоре или в личном кабинете пользователя. Если инженер провайдера при настройке соединения на компьютере создавал в папке сетевых подключений “Подключение удаленного доступа” или ярлык, имеющий такое же название как и ваш Интернет-провайдер, удалите его из папки сетевых подключений компьютера, чтобы избежать сетевых ошибок или двойной авторизации. Внимание! Если вы когда-либо меняли логин и пароль, при настройке убедитесь, что вводите актуальные данные в соответствующе пункты:



Получить IP-адрес для работы в городской сети провайдера автоматически: Параметр характерен только для протоколов подключения и авторизации в сети провайдера с поддержкой технологии Dual Link: Dual Link PPPoE (Dual Access), Dual Link PPTP (Dual Access) или Dual Link L2TP (Dual Access). Если Интернет-провайдер помимо услуги доступа в сеть Интернет предоставляет дополнительные сервисы (например, IPTV, игровые локальные серверы, локальные торрент-трекеры), которые расположены в локальной сети масштаба города или района присутствия оператора, необходимо выбрать один из способов получения IP-адреса для работы в сети Интернет-провайдера: получить IP-адрес автоматически (DHCP-клиент) / ввести вручную статический IP-адрес, маску, шлюз и адреса DNS.

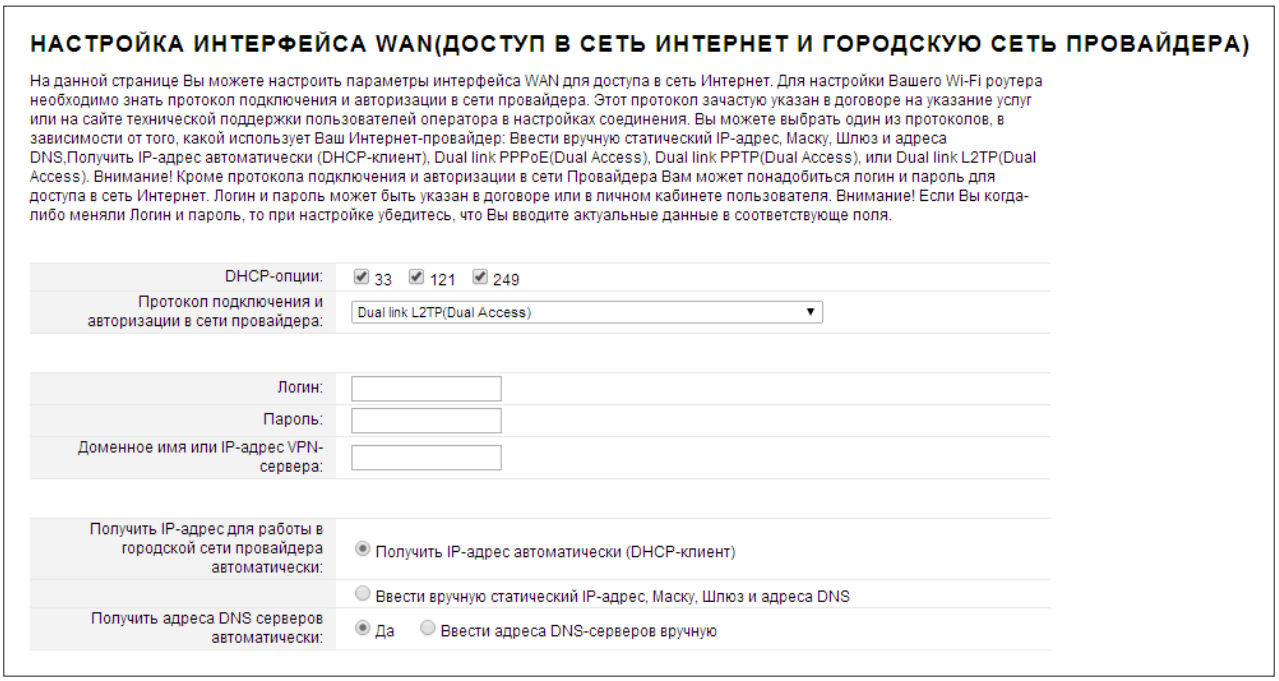
MPPE: Поставив галочки в данных окнах вы можете включить шифрование MPPE или сжатие MPPC.

Получить адреса DNS-серверов автоматически: Если выберите “Ввести адреса DNS-серверов вручную”, будет необходимо ввести адреса DNS-серверов в поля, ставшими активными. Значение данного параметра по умолчанию “Получить IP-адрес автоматически (DHCP-клиент)”, если интерфейс WAN роутера настроен на режим работы DHCP-клиент, Dual Link PPPoE (Dual Access), Dual Link PPTP (Dual Access) или Dual Link L2TP (Dual Access). Если по каким-либо причинам необходимо ввести адреса DNS-серверов, отличающихся от назначаемых устройству автоматически по протоколу DHCP, можно выбрать “Ввести вручную статический IP-адрес, маску, шлюз и адреса DNS”.

Обратитесь к пункту 5.2.2 данной инструкции для получения справочной информации по функциям и элементам не проиллюстрированных на изображении веб-интерфейса.

5.2.2.3 Dual Link L2TP (Dual Access)

Dual Link L2TP (Dual Access) – протокол технологии VPN (Layer 2 Tunneling Protocol). Для настройки протокола подключения и авторизации в сети провайдера необходимо ввести логин и пароль для доступа в сеть Интернет в соответствующие поля, а также доменное имя VPN-сервера или его IP-адрес. Логин и пароль могут быть указаны в договоре или в личном кабинете пользователя. Если инженер провайдера при настройке соединения на компьютере создавал в папке сетевых подключений “Подключение удаленного доступа” или ярлык, имеющий такое же название как ваш Интернет-провайдер, удалите его из папки сетевых подключений компьютера, чтобы избежать возможности сетевых ошибок или двойной авторизации. Внимание! Если вы когда-либо меняли логин и пароль, при настройке убедитесь, что вводите актуальные данные в соответствующе пункты:



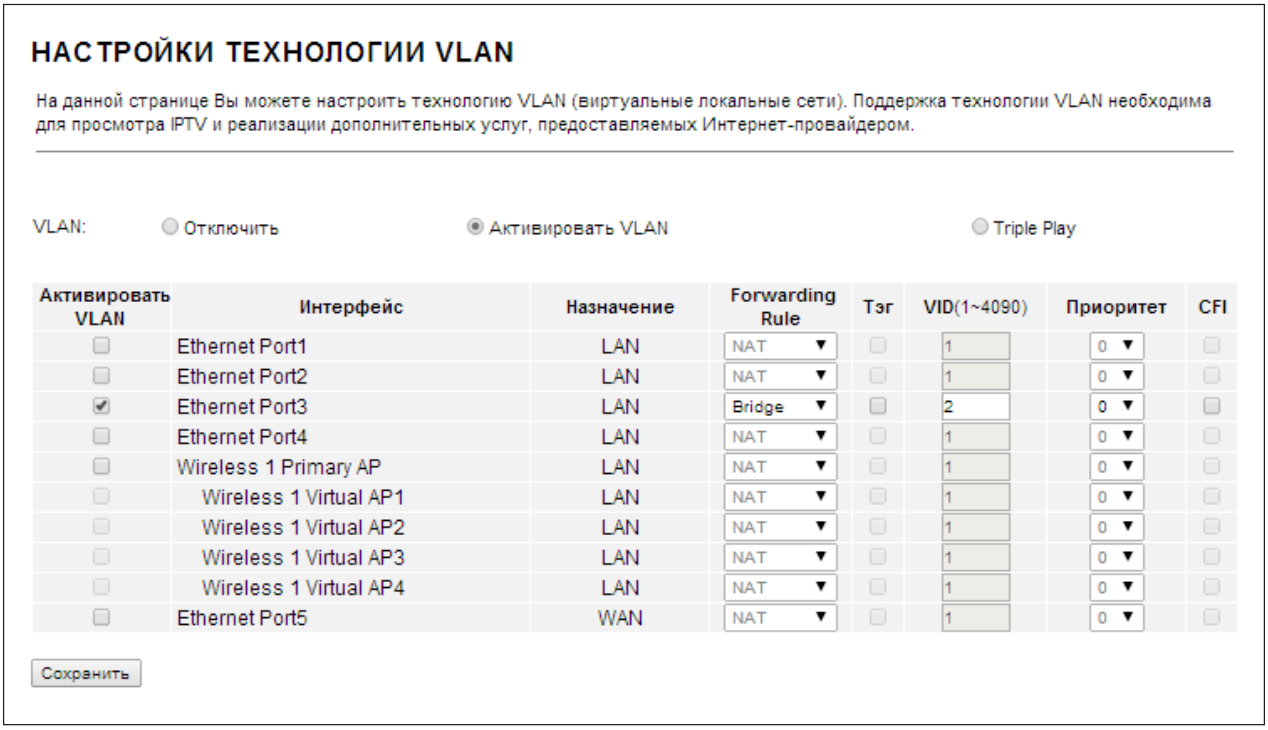
Получить IP-адрес для работы в городской сети провайдера автоматически: Параметр характерен только для протоколов подключения и авторизации в сети провайдера с поддержкой технологии Dual Link, таких как: Dual Link PPPoE (Dual Access), Dual Link PPTP (Dual Access) или Dual Link L2TP (Dual Access) L2TP соединение. Если Интернет-провайдер помимо услуги доступа в сеть Интернет предоставляет дополнительные сервисы (например, IPTV, игровые локальные серверы, локальные торрент-трекеры, расположенные в локальной сети масштаба города или района присутствия оператора), необходимо выбрать один из способов получения IP-адреса для работы в сети Интернет-провайдера: получить IP-адрес автоматически (DHCP-клиент) / ввести вручную статический IP-адрес, маску, шлюз и адреса DNS.

Обратитесь к пункту 5.2.2 данной инструкции для получения справочной информации по функциям и элементам не проиллюстрированных на изображении веб-интерфейса.

Нажмите кнопку “Сохранить” для сохранения выполненных изменений в настройках устройства.

5.2.3 Настройки VLAN

На данной странице можно настроить технологию VLAN (виртуальные локальные сети). Поддержка технологии VLAN необходима для просмотра IPTV и реализации дополнительных услуг, предоставляемых Интернет-провайдером. Устройство поддерживает 2 варианта реализации интерфейса VLAN:



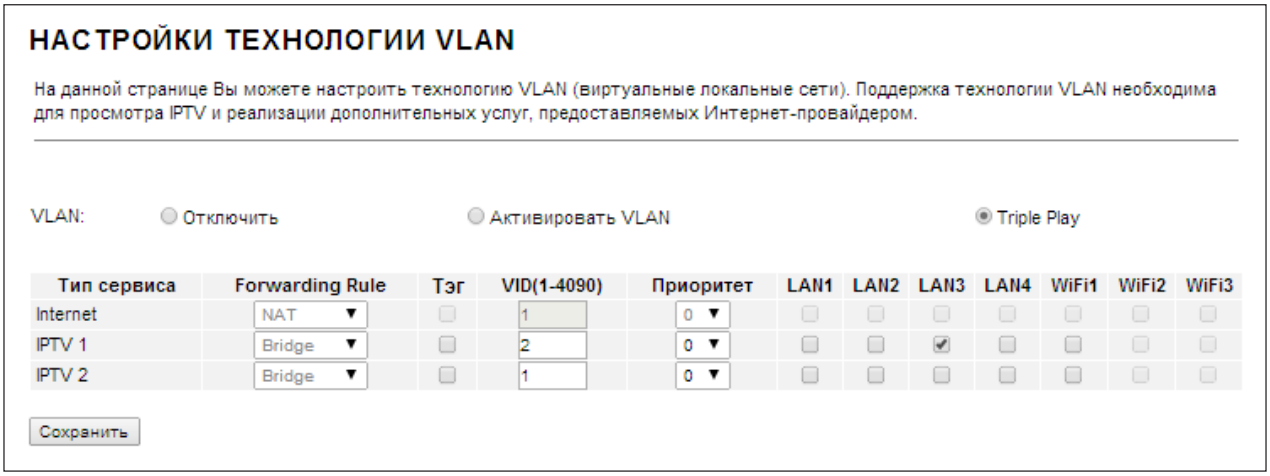
НАСТРОЙКИ ТЕХНОЛОГИИ VLAN

На данной странице Вы можете настроить технологию VLAN (виртуальные локальные сети). Поддержка технологии VLAN необходима для просмотра IPTV и реализации дополнительных услуг, предоставляемых Интернет-провайдером.

VLAN: Отключить Активировать VLAN Triple Play

Активировать VLAN	Интерфейс	Назначение	Forwarding Rule	Тэг	VID(1~4090)	Приоритет	CFI
☐	Ethernet Port1	LAN	NAT	☐	1	0	☐
☐	Ethernet Port2	LAN	NAT	☐	1	0	☐
☑	Ethernet Port3	LAN	Bridge	☐	2	0	☐
☐	Ethernet Port4	LAN	NAT	☐	1	0	☐
☐	Wireless 1 Primary AP	LAN	NAT	☐	1	0	☐
☐	Wireless 1 Virtual AP1	LAN	NAT	☐	1	0	☐
☐	Wireless 1 Virtual AP2	LAN	NAT	☐	1	0	☐
☐	Wireless 1 Virtual AP3	LAN	NAT	☐	1	0	☐
☐	Wireless 1 Virtual AP4	LAN	NAT	☐	1	0	☐
☐	Ethernet Port5	WAN	NAT	☐	1	0	☐

Сохранить



НАСТРОЙКИ ТЕХНОЛОГИИ VLAN

На данной странице Вы можете настроить технологию VLAN (виртуальные локальные сети). Поддержка технологии VLAN необходима для просмотра IPTV и реализации дополнительных услуг, предоставляемых Интернет-провайдером.

VLAN: Отключить Активировать VLAN Triple Play

Тип сервиса	Forwarding Rule	Тэг	VID(1-4090)	Приоритет	LAN1	LAN2	LAN3	LAN4	WiFi1	WiFi2	WiFi3
Internet	NAT	☐	1	0	☐	☐	☐	☐	☐	☐	☐
IPTV 1	Bridge	☐	2	0	☐	☐	☑	☐	☐	☐	☐
IPTV 2	Bridge	☐	1	0	☐	☐	☐	☐	☐	☐	☐

Сохранить

VLAN (Virtual Local Area Network) – функция дает возможность управлять группами клиентских устройств на основании физических и виртуальных интерфейсов роутера.

Активировать VLAN: Поставьте галочку в окне, чтобы включить функцию VLAN для всех интерфейсов, включая физические и виртуальные или для какого-либо отдельного физического или виртуального интерфейса.

Интерфейс: Данный столбец таблицы технологии VLAN описывает назначение интерфейса, например: Ethernet Port2, Wireless 1 Primary AP, Wireless 1 Virtual AP3 и т.д.

Назначение: Данный столбец таблицы технологии VLAN описывает принадлежность того или иного интерфейса и его пригодность в использовании в качестве WAN или LAN-интерфейса устройства.

Forwarding Rule: Данный столбец таблицы технологии VLAN имеет селектор напротив каждого активного физического и виртуального интерфейса устройства и позволяет выбрать правило коммуникации между WAN и LAN-интерфейсами, которые он объединяет: Disabled, Bridge или NAT.

Тэг: Поставьте галочку в данном окне, чтобы включить функцию тегирования VLAN. При включении функции роутер будет добавлять VLAN-маркер (тэг) к каждому пришедшему с LAN-интерфейса пакета (включая сеть Wi-Fi) перед пересылкой их на интерфейс WAN. Пожалуйста, не забудьте выставить приоритетность пересылки пакетов с LAN-интерфейса на интерфейс WAN для тегированных интерфейсов.

VID(1~4090): параметр носит название VLAN ID. Диапазон допустимых значений этого параметра – от 1 до 4090. Обычно Интернет-провайдеры, предоставляющие дополнительные сервисы помимо доступа в сеть Интернет, используют различные VID для разных сервисов. Заранее уточните у провайдера, используется ли технология VLAN (Triple play). Узнайте, какой VID за какой тип услуг отвечает, нужен ли тэг и параметр CFI.

Приоритет: Выставите приоритет для каждого VLAN. Диапазон допустимых значений этого параметра от 0 до 7.

CFI: Параметр отвечает за сосуществование технологии Ethernet и Token Ring, указывая какой формат (канонический или не канонический) MAC-адресов стоит использовать устройству в передаваемых фреймах (кадрах).

Нажмите кнопку “Сохранить” для сохранения выполненных изменений в настройках устройства.

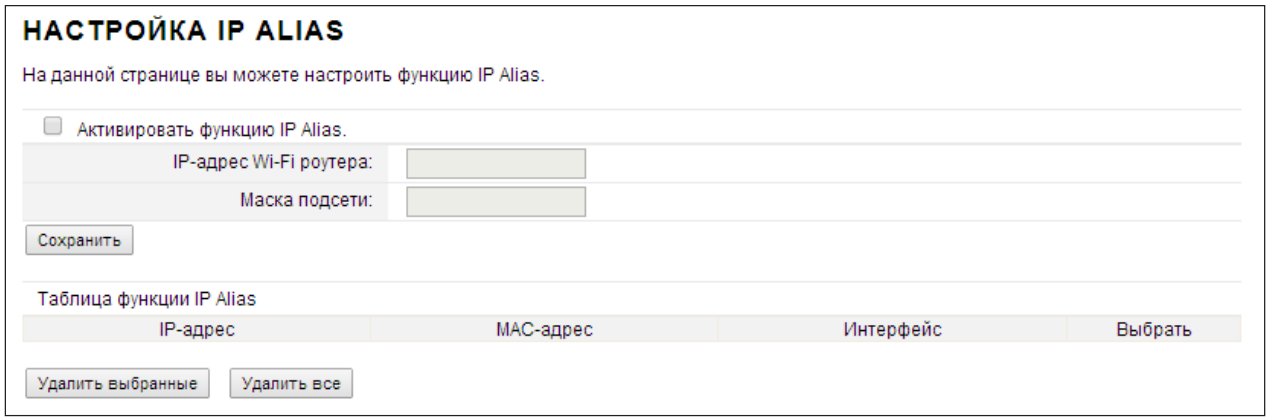
5.2.4 For IP Routing

На данной странице вы можете настроить функцию For IP Routing. Функция применит правила маршрутизации для внешнего IP-адреса введенного в данное поле.

Нажмите кнопку “Сохранить” для сохранения выполненных изменений в настройках устройства.

5.2.5 Функция IP Alias

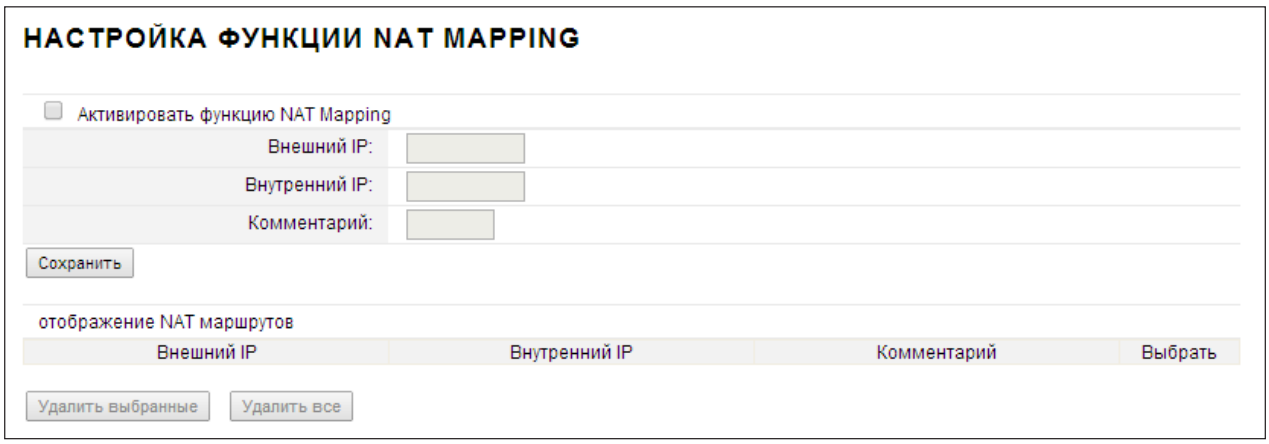
На данной странице вы можете настроить функцию IP Alias. Она позволяет назначить дополнительный виртуальный IP-адрес интерфейсу LAN.



Нажмите кнопку “Сохранить” для сохранения выполненных изменений в настройках устройства.

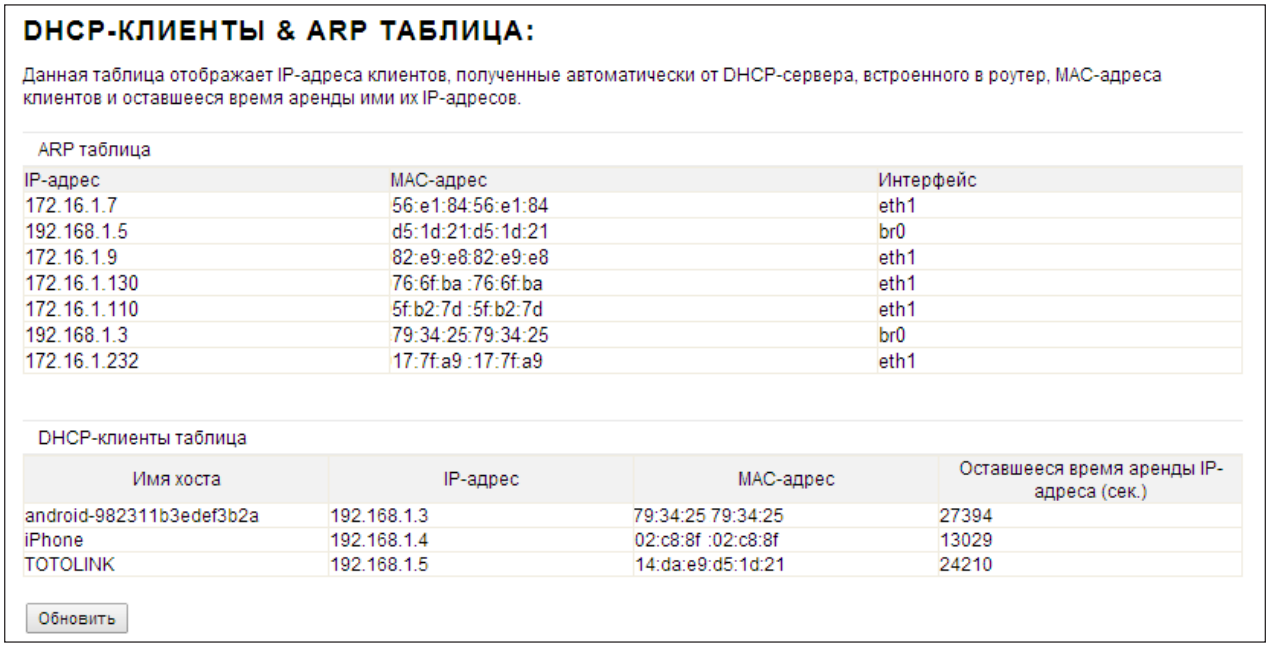
5.2.6 Функция NAT Mapping

На данной странице вы можете настроить функцию NAT Mapping. Данная функция позволяет транслировать один внешний IP-адрес на один внутренний IP-адрес.



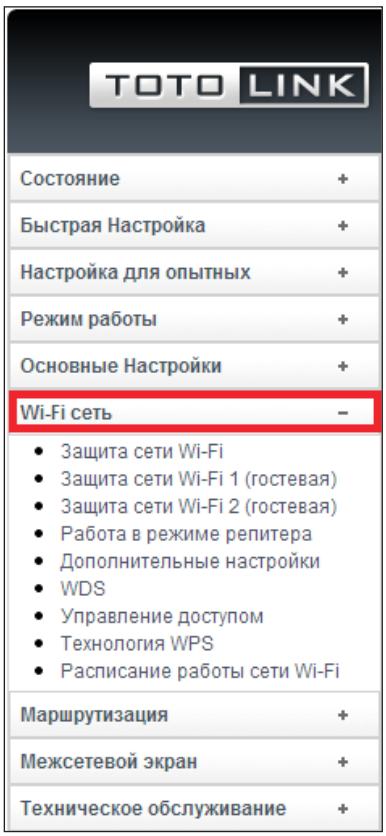
Нажмите кнопку “Сохранить” для сохранения выполненных изменений в настройках устройства.

5.2.7 Список клиентов



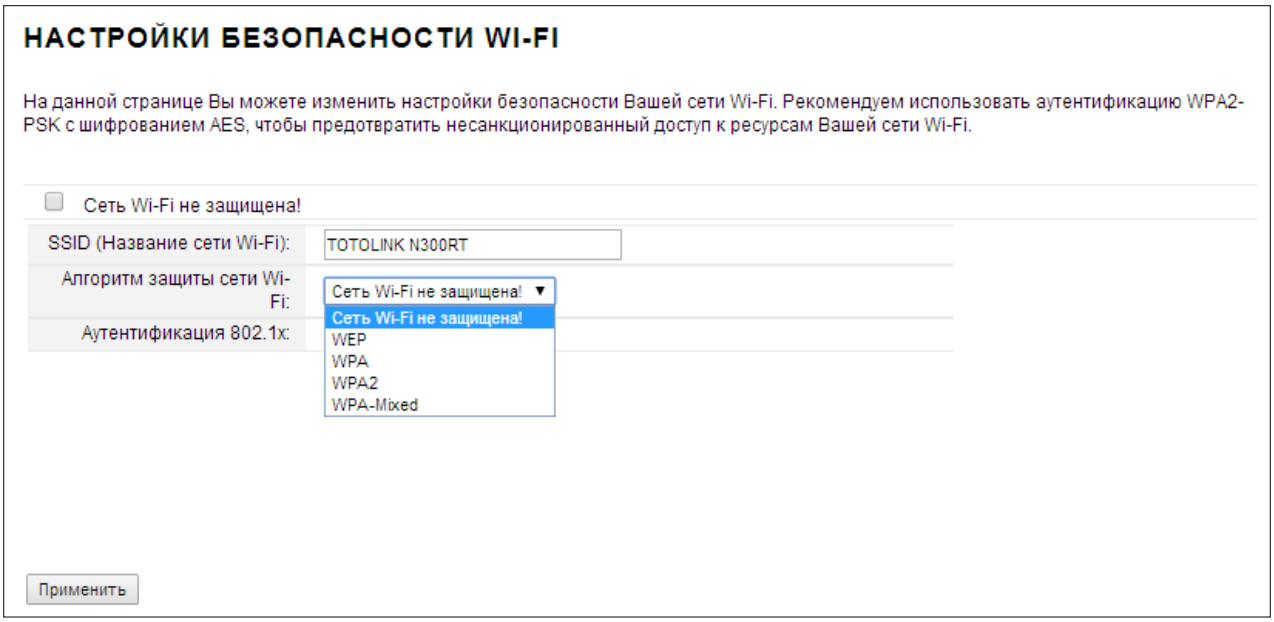
5.3 Wi-Fi сеть

На данной странице можно настроить основные параметры сети Wi-Fi точки доступа, встроенной в роутер, защитить основную сеть Wi-Fi, гостевые сети или выбрать режим работы репитера. Большинство основных параметров Wi-Fi были описаны в главе “Быстрая настойка”, здесь мы рассмотрим остальные функции более детально.



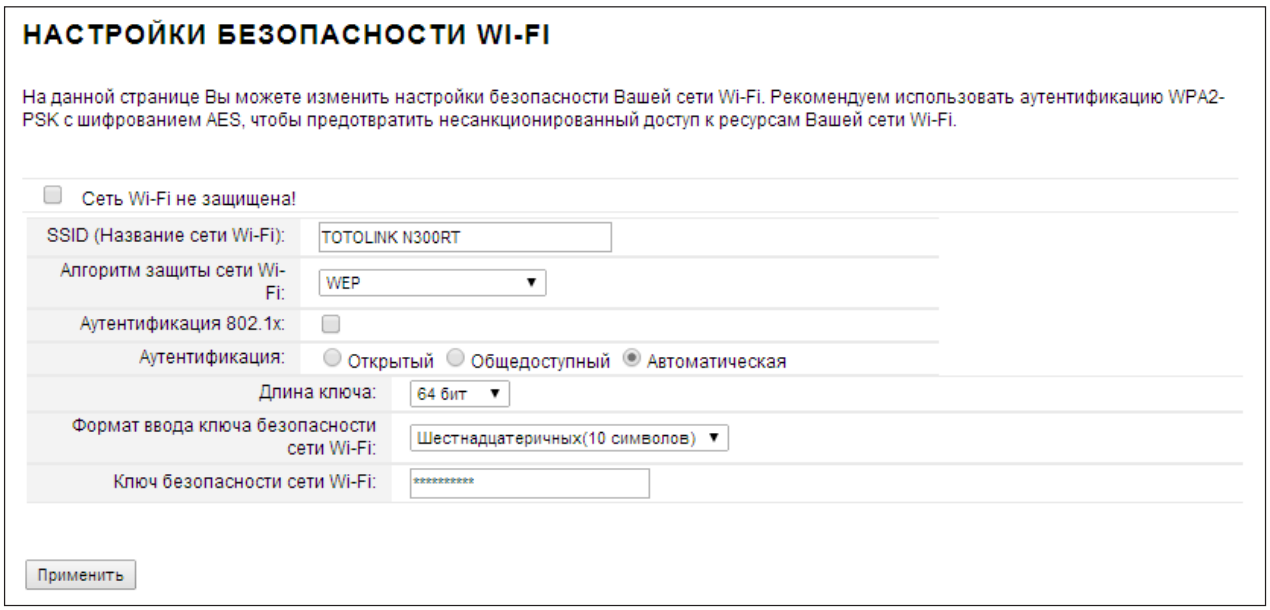
5.3.1 Защита сети Wi-Fi / Защита сети Wi-Fi 1 (гостевая) / Защита сети Wi-Fi 2 (гостевая)

Алгоритм защиты сети Wi-Fi: Селектором можно выбрать один из поддерживаемых алгоритмов защиты сети Wi-Fi, поддерживаемых устройством: сеть Wi-Fi не защищена, WEP, WPA (TKIP), WPA2 (AES), WPA-Mixed. Выберите один из алгоритмов защиты сети Wi-Fi исходя из описания приведенного ниже и ваших потребностей:



1. WEP

WEP (Wired Equivalent Privacy) – стандартный алгоритм защиты сети Wi-Fi для группы стандартов IEEE 802.11, использующий алгоритм шифрования RC4. Выбирая алгоритм защиты сети Wi-Fi WEP, стоит иметь ввиду, что все данные, передаваемые в сети Wi-Fi будут защищены шифрованием. WEP – самый старый алгоритм защиты сети Wi-Fi из всех поддерживаемых устройством. Внимание! Существо несколько программ, которые могут расшифровать и, как следствие, получить доступ к вашим данным, передаваемым по Wi-Fi, менее чем за 10 минут. Мы не рекомендуем использовать данный алгоритм.



Длина ключа: Селектором можно выбрать длину ключа шифрования алгоритма WEP 64 или 128 бит. Значение по умолчанию – 64 бита.

64 бита – Для длины ключа шифрования алгоритма WEP в 64 бита поддерживается два формата ввода ключа безопасности сети Wi-Fi:

• ASCII (на английской раскладке клавиатуры, включая буквы и цифры) длиной 5 символов.

• Если вы выбрали “Шестнадцатеричный (10 символов)” формат, ключ безопасности сети Wi-Fi необходимо вводить, начиная с обязательных символов 0x, например: 0x414234445).

128 бит – Для длины ключа шифрования алгоритма WEP в 128 бит поддерживается два формата ввода ключа безопасности сети Wi-Fi:

• ASCII (на английской раскладке клавиатуры, включая буквы и цифры) длиной в 13 символов.

• Если вы выбрали “Шестнадцатеричный (26 символов)” формат, ключ безопасности сети Wi-Fi необходимо вводить, начиная с обязательных символов 0x, например: 0x41424344454647484 94A4B4C4D).

Формат ввода ключа безопасности сети Wi-Fi + Ключ безопасности сети Wi-Fi:

Данные параметры отвечают за длину и формат ввода ключа безопасности сети Wi-Fi, который необходимо будет вводить каждому новому Wi-Fi клиенту для подключения к устройству и последующего обмена зашифрованными данными.

Вашим устройством поддерживается два формата ввода ключа безопасности сети Wi-Fi (на английской раскладке клавиатуры, включая буквы и цифры) и шестнадцатеричный ключ.

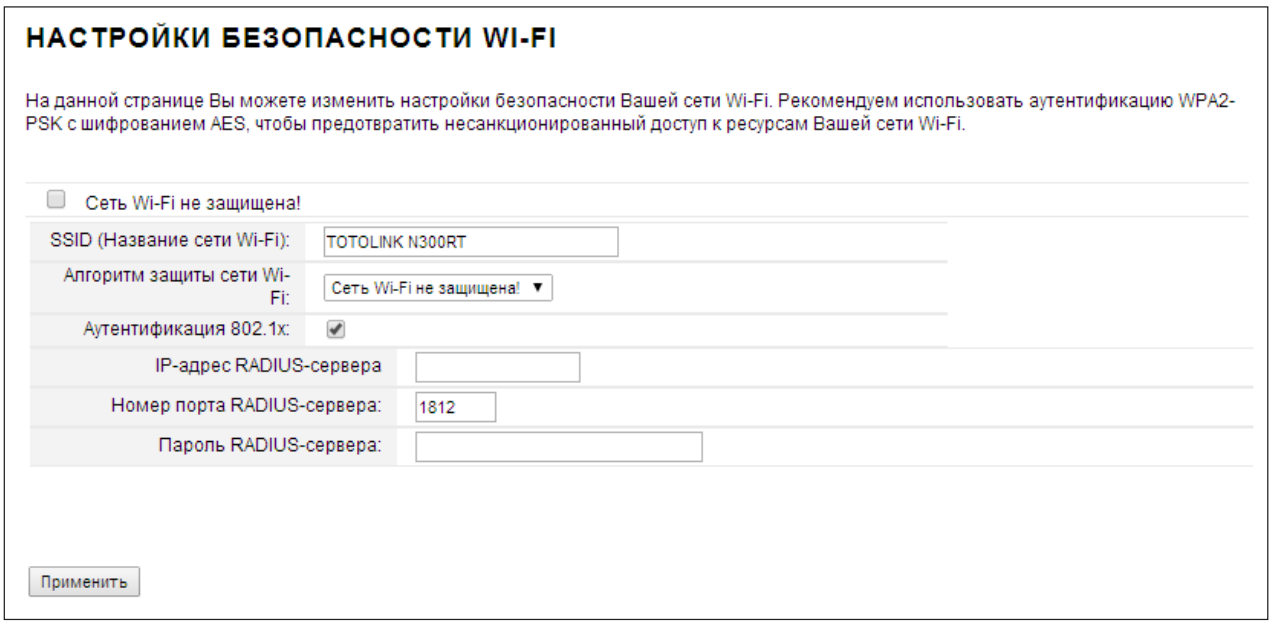
Если вы выбрали параметр **“Длина ключа”** в 64 бита, при выборе формата ввода ключа безопасности сети Wi-Fi **“на английской раскладке клавиатуры, включая буквы и цифры”,** длина ключа безопасности сети Wi-Fi будет составлять 5 символов. Если при той же длине ключа – 64 бита – вы выбрали “Шестнадцатеричный ключ”, длина ключа безопасности сети Wi-Fi будет составлять 10 символов.

Если вы выбрали параметр **“Длина ключа”** 128 бит, при выборе формата ввода ключа безопасности сети Wi-Fi **“на английской раскладке клавиатуры, включая буквы и цифры”,** длина ключа безопасности сети Wi-Fi будет составлять 13 символов. Если при той же длине ключа 128 бит вы выбрали **“Шестнадцатеричный ключ”**, длина ключа безопасности сети Wi-Fi будет составлять 26 символов.

Ключ безопасности сети Wi-Fi: Пожалуйста, обратитесь к пункту “Длина ключа” для ввода ключа правильного формата и длины.

2. Аутентификация 802.1x

Протокол WPA (Wi-Fi Protected Access) подразделяется на две реализации: WPA/PSK и WPA/802.1x. Если выбрать Аутентификация 802.1x, будет необходимо ввести IP-адрес RADIUS-сервера, номер порта RADIUS-сервера и пароль. При использовании Аутентификации 802.1x ключ шифрования сети будет получен автоматически от отдельного устройства (RADIUS-сервера).



IP-адрес RADIUS-сервера: Введите IP-адрес RADIUS-сервера в данное поле.

Номер порта RADIUS-сервера: Введите номер порта протокола UDP, который используется RADIUS-сервером для аутентификации клиентов.

Пароль RADIUS-сервера: Введите пароль в данное поле.

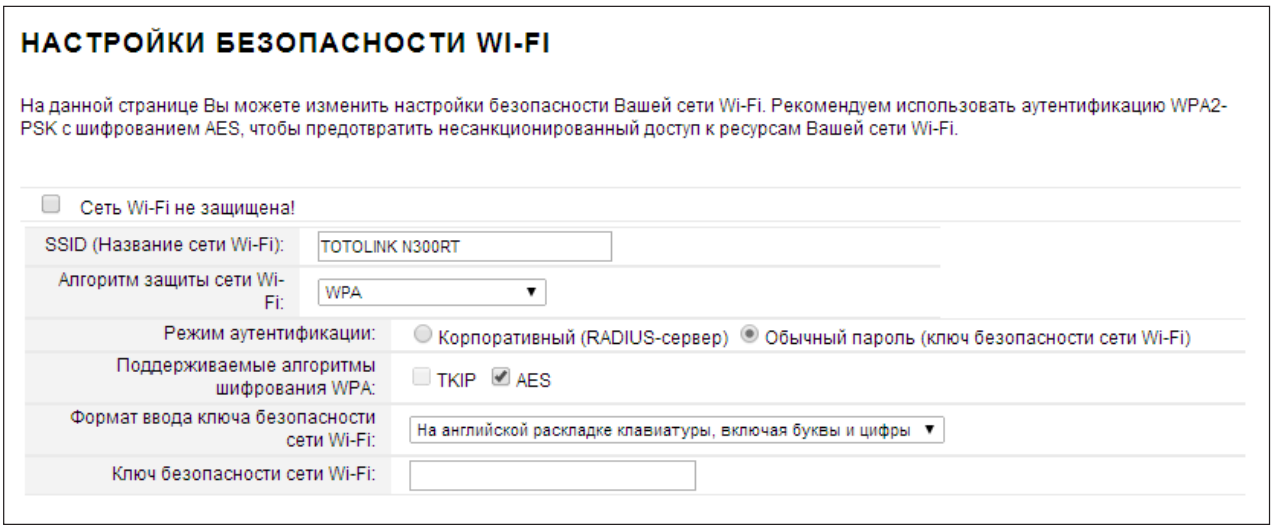
> **RADIUS**: сокращение от Remote Authentication Dial-In User’s Service (сервер удаленной аутентификации пользователей). RADIUS – защищенный алгоритм аутентификации клиент-серверной архитектуры отвечающий за аутентификацию, авторизацию и аккаунтинг, иногда используемый Интернет-провайдерами.

3. WPA/WPA2

WPA (Wi-Fi Protected Access) – рекомендуемый Wi-Fi Alliance алгоритм защиты сети Wi-Fi. Существует два подтипа данного алгоритма защиты сети Wi-Fi: WPA-personal, иногда именуемый как WPA Pre-Share Key (WPA/PSK), и WPA-Enterprise, иногда именуемый как WPA/802.1x. WPA2 (Wi-Fi Protected Access 2) – более криптографически стойкий ко взлому и более совершенная версия алгоритма защиты сети Wi-Fi, нежели WPA. Первый алгоритм рекомендован Wi-Fi Alliance как наилучший вариант защиты сети Wi-Fi, не приводящий к снижению скорости из-за шифрования и как наиболее надежный протокол для сетей стандарта IEEE 802.11n.

TKIP – протокол шифрования данных в сетях Wi-Fi, отвечающий за целостность ключа шифрования, который изменяется во времени и присваивается каждому пакету. Данный криптографический алгоритм является обязательным для алгоритмов защиты сети Wi-Fi WPA и WPA2.

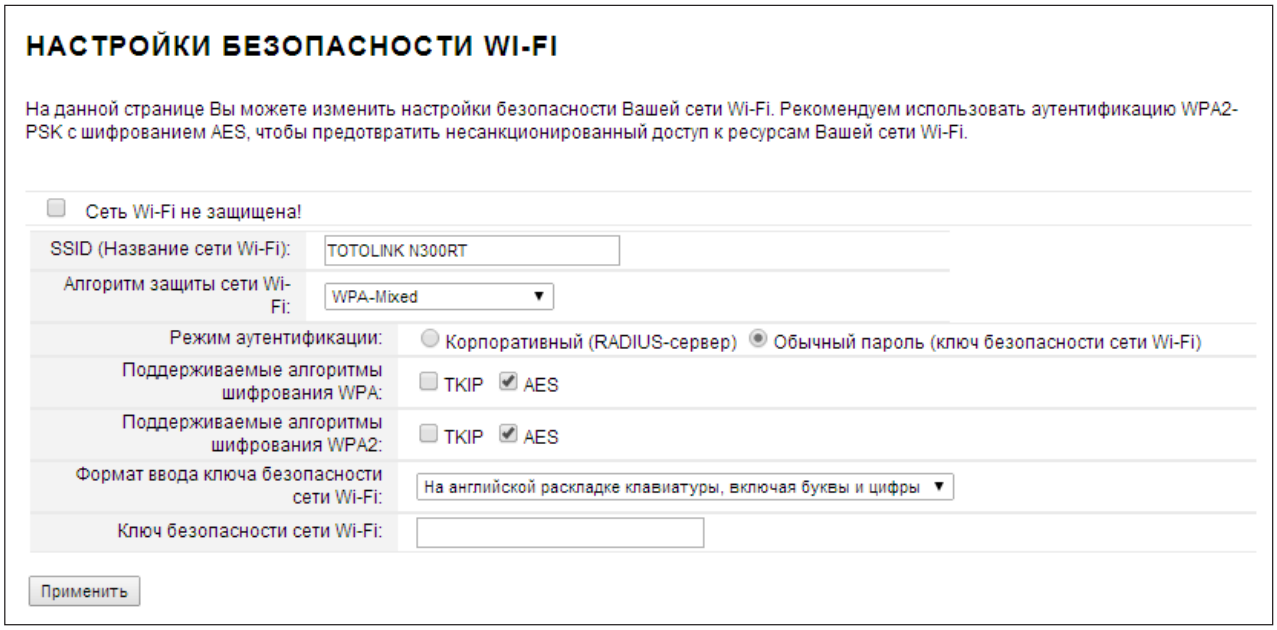
AES – протокол шифрования данных в сетях Wi-Fi, рекомендуемый для защиты сетей стандарта IEEE 802.11n совместно с аутентификацией WPA2. Данный криптографический алгоритм является обязательным для алгоритмов защиты сети Wi-Fi WPA и WPA2.



Формат ввода ключа безопасности сети Wi-Fi + Ключ безопасности сети Wi-Fi: Данные параметры отвечают за длину и формат ввода ключа безопасности сети Wi-Fi, который необходимо вводить каждому новому Wi-Fi клиенту для подключения к устройству и последующему обмену зашифрованными данными. Вашим устройством поддерживается два формата ввода ключа безопасности сети Wi-Fi: (на английской раскладке клавиатуры, включая буквы и цифры) и шестнадцатеричный ключ (64 символа). Затем необходимо ввести ключ безопасности сети Wi-Fi в поле напротив. Если вы выбрали формат ввода ключа безопасности сети Wi-Fi “на английской раскладке клавиатуры, включая буквы и цифры”, длина ключа безопасности сети Wi-Fi должна составлять от 8 до 63 символов. В том случае, если вы выбрали “Шестнадцатеричный ключ (64 символа)”, ключ безопасности сети Wi-Fi необходимо вводить, начиная с обязательных символов 0x, например: “0x321253abcde…”.

4. WPA-Mixed

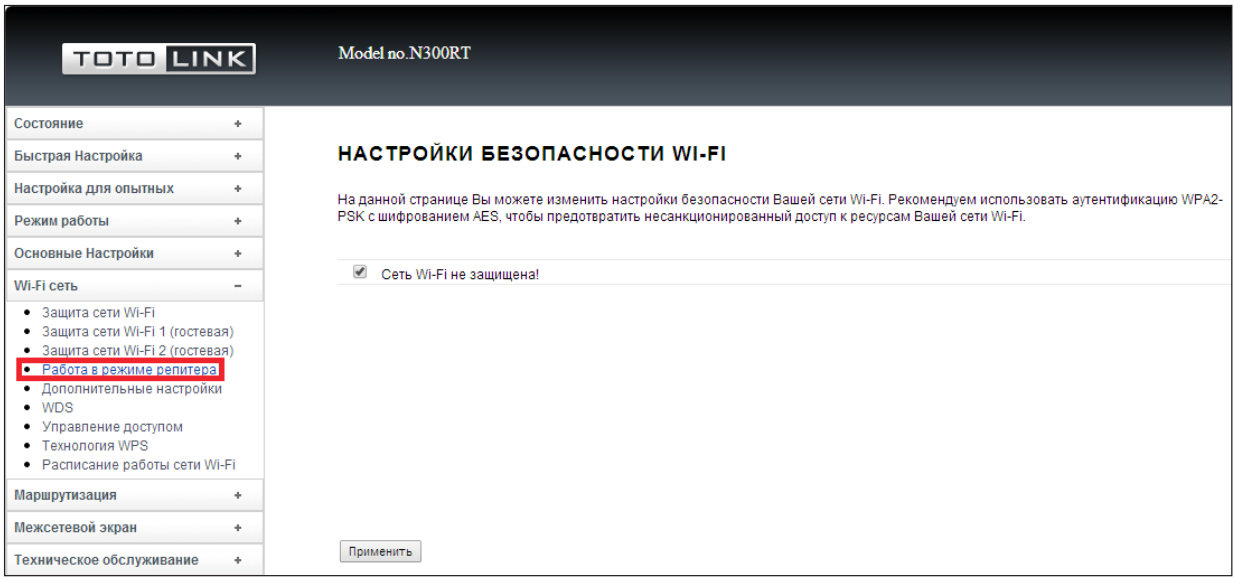
Опция позволяет использовать алгоритмы защиты сети Wi-Fi WPA и WPA2 совместно, сочетая преимущества каждого. Использование данного алгоритма защиты сети Wi-Fi обеспечивает наилучшую защиту сети Wi-Fi роутера и хороший уровень совместимости оборудования.

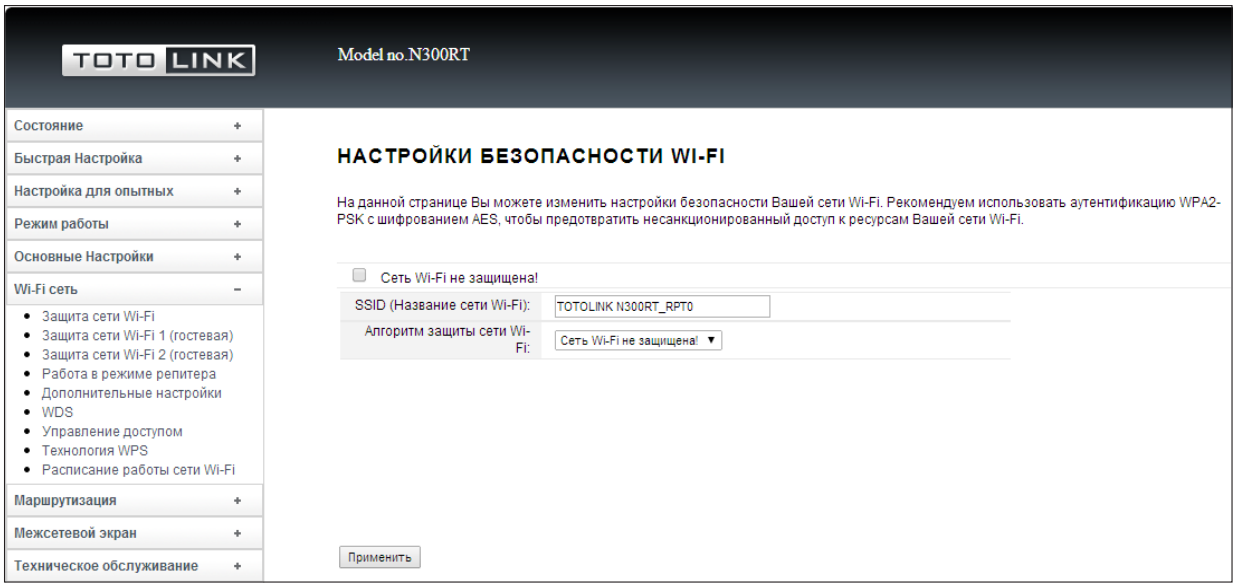


Примечание: *Используйте WEP в тех случаях, когда нет альтернативы защиты более совершенным алгоритмом или когда у вас стоит задача подключения к сети Wi-Fi устаревшего оборудования 802.11b или 802.11 b/g. Данная рекомендация связана с недостаточной криптографической стойкостью к взлому алгоритма шифрования, использованного в основе WEP. В остальных случаях рекомендуем алгоритм WPA2 с шифрованием AES.*

5.3.2 Работа в режиме репитера

Для активации режима репитера необходимо снять галочку «Сеть Wi-Fi не защищена!»





Введите в поле **SSID (название сети Wi-Fi)** необходимо ввести имя сети, находящейся в зоне покрытия устройства, сигнал которой необходимо усилить. Селектором **Алгоритм защиты сети Wi-Fi** выбирете необходимый алгоритм и введите ключ безопасности сети Wi-Fi в соответствующем поле.

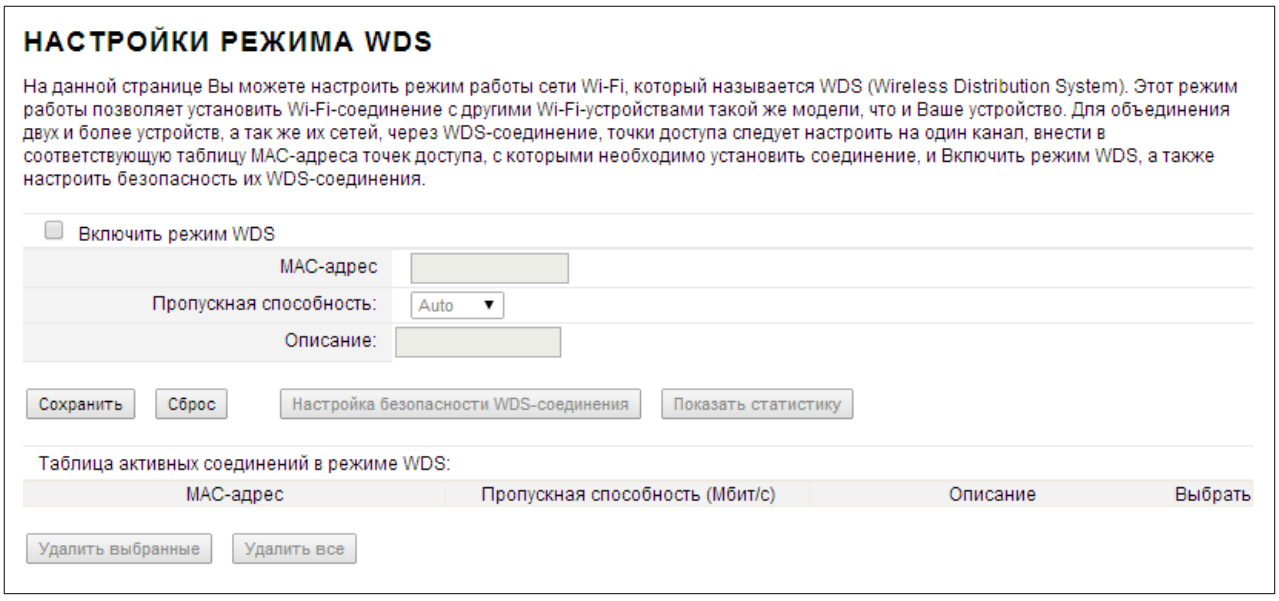
5.3.3 WDS

На данной странице можно настроить режим работы сети Wi-Fi, называемый WDS (Wireless Distribution System). Этот режим позволяет установить Wi-Fi соединение с другими Wi-Fi устройствами такой же модели, что и ваше устройство. Для объединения двух и более устройств, а так же их сетей через WDS-соединение, точки доступа следует настроить на один канал, внести в соответствующую таблицу MAC-адреса точек доступа, с которыми необходимо установить соединение и включить режим WDS, а также настроить безопасность их WDS-соединения.

Обычно, у технологии WDS следующие сферы применения:

1. Создание соединения типа «мост» по технологии Wi-Fi между двумя проводными сегментами Ethernet-сетей.

2. Увеличение покрытия уже существующей сети Wi-Fi.



Включить режим WDS: Поставьте галочку в окне, чтобы включить режим WDS.

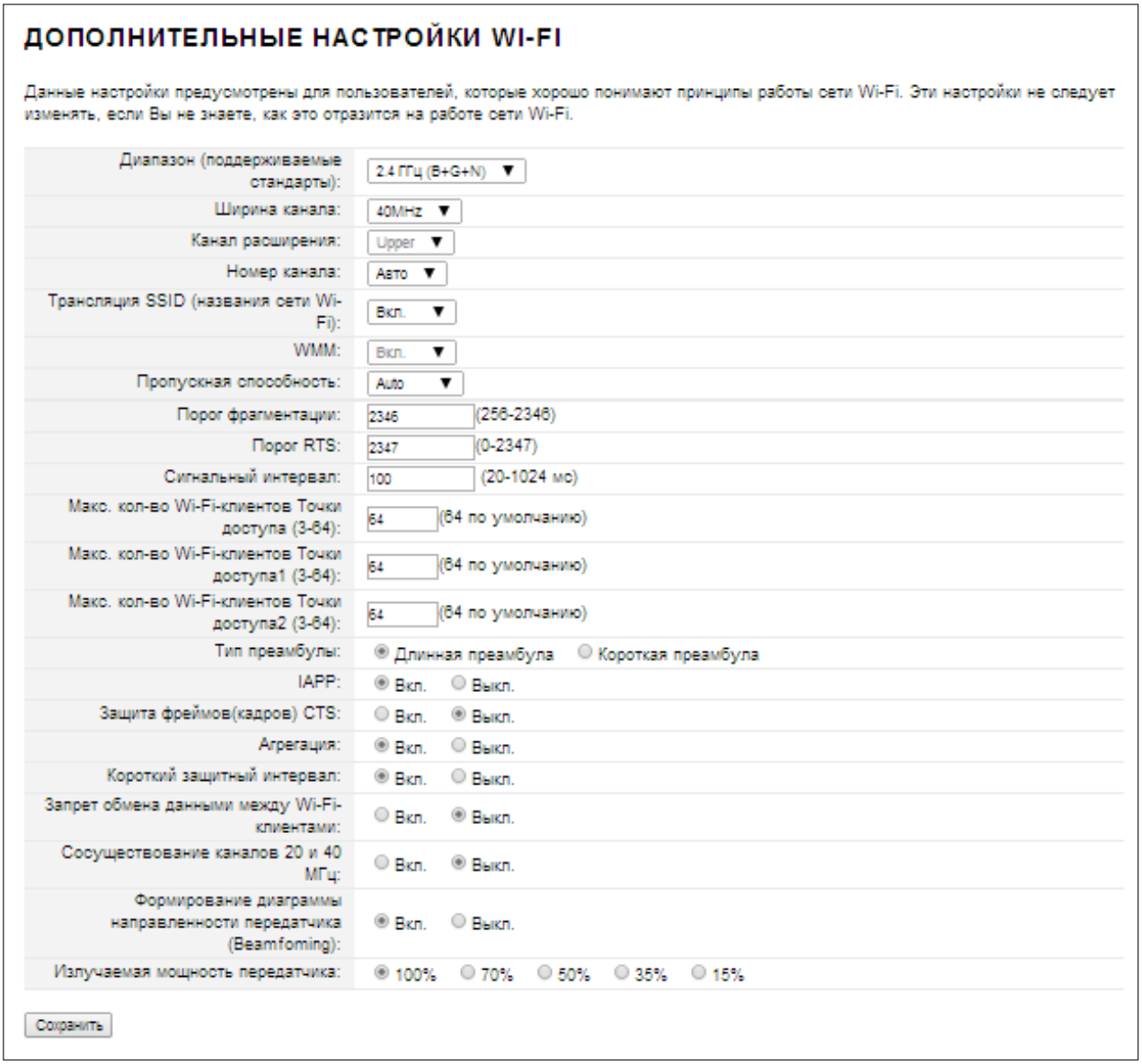
MAC-адрес: Введите MAC-адрес точки доступа с которой бы хотели установить WDS-соединение.

Пропускная способность: Выберите селектором необходимую пропускную способность между соединяющимися устройствами в режиме WDS.

Описание: Введите в поле причину, по которой хотите применить данное правило для установления WDS-соединения с другим подобным устройством. Кнопка настройка безопасности WDS-соединения позволяет сконфигурировать защиту WDS-соединения. В данном режиме поддерживается два алгоритма защиты сети Wi-Fi: WEP 64 бит и WEP 128 бит. Обратитесь к главе 4.3.6 “Защита сети Wi-Fi” данной инструкции для получения детальной информации. Нажмите кнопку “Сохранить” для сохранения выполненных изменений в настройках устройства.

5.3.4 Дополнительные настройки

Данные настройки предусмотрены для продвинутых пользователей, понимающих принципы работы сети Wi-Fi. Эти настройки не следует изменять, если вы не знаете, как это отразится на работе сети Wi-Fi.



Диапазон (поддерживаемые стандарты): Селектором можно выбрать частотный диапазон и поддерживаемые стандарты работы сети роутера. Стандарты сети Wi-Fi 802.11b и 802.11g более ранние и имеют меньшую пропускную способность, нежели стандарт 802.11n, который использует более совершенный тип модуляции сигнала (OFDM-метод). Рекомендуем выбрать 2,4 ГГц (B+G+N), так как эта настройка избавит от проблем возможной несовместимости устройства с оборудованием более ранних стандартов Wi-Fi.

Ширина канала – ширина частотного канала Wi-Fi. Устройство поддерживает следующие значения ширины частотного канала технологии Wi-Fi:

20 МГц – стандартная ширина частотного канала Wi-Fi для 802.11b и 802.11g.

40 МГц – ширина частотного канала Wi-Fi, поддерживаемая 802.11n, значительно увеличивающая пропускную способность (значение выбрано по умолчанию).

Канал расширения – функция отвечает за добавление дополнительного частотного канала шириной 20 МГц к основному.

Выше основного по частоте: Значение по умолчанию – “Выше основного по частоте”, количество каналов работы технологии Wi-Fi составляет 11.

Ниже основного по частоте: Если выберите “Ниже основного по частоте”, количество каналов работы технологии Wi-Fi изменится на значение Auto, а параметр “Канал расширения” станет не активным. Изменив параметр на значение “Ниже основного по частоте”, количество каналов работы технологии Wi-Fi будет доступно для выбора селектором от 1 до 9. Лишь после того как вы выберите один из доступных каналов, параметр канала расширения будет снова активным для изменения. Если выберите “Выше основного по частоте”, количество каналов работы технологии Wi-Fi будет доступно для выбора селектором от 5 до 13.

Номер канала – Селектор позволяет вручную выбрать номер частотного канала работы сети Wi-Fi.

Важное примечание: *Рекомендуем выбирать наименее загруженные частотные каналы для достижения наивысшей производительности сети Wi-Fi. На практике самыми загруженными оказываются частотные каналы с номерами 1, 6 и 11. Если вы решили выставить частотный канал с номерами 12, 13 или 14, не рекомендуем этого делать, значительная часть Wi-Fi оборудования на территории РФ и СНГ их не поддерживает. Придерживайтесь данной рекомендации и при выборе параметра канала расширения.*

Трансляция SSID (название сети Wi-Fi): Селектором можно выбрать включить/отключить параметр. Service Set Identifier используется чтобы идентифицировать сеть Wi-Fi другими совместимыми с 802.11-устройствами, работающими в режиме **Wi-Fi роутер/точка доступа+Wi-Fi-клиенты** или в режиме AP+WDS.

Пояснение: Все клиентские Wi-Fi устройства, находящиеся в зоне покрытия роутера, будут получать широковещательные сообщения от точки доступа, встроенной в роутер с информацией о текущем SSID (названии сети Wi-Fi).

WMM – сокращение от Wireless Multimedia. Протокол определяет уровень приоритезации трафика для четырех категорий доступа согласно таблицам приоритезации стандарта IEEE 802.1d. Категории доступа специально разработаны для обеспечения наилучшего качества обслуживания клиентов в зависимости от типа передаваемого трафика: голос, видео, трафик негарантированной доставки типа «best effort» и низкоприоритетные данные.

Примечание: *Параметр включен по умолчанию и не может быть изменен пользователем.*

Пропускная способность

Параметр определяет пропускную способность (Мбит/с) на которой устройство должно передавать данные по Wi-Fi. Помимо выбора фиксированной пропускной способности в Мбит/с можно выбрать любое значение данного параметра от MCS 0 до MCS 7. Рекомендуется не изменять значение параметра и использовать значение по умолчанию «Auto»!

MCS – сокращение от Modulation Coding Scheme (Схема используемой модуляции и кодирования сигнала). До появления стандарта IEEE 802.11n большинство точек доступа, встраиваемых в роутеры, соответствовали стандартам IEEE 802.11a/b/g и поддерживали пропускную способность от 1 Мбит/с до 54 Мбит/с (поддерживая 12 возможных вариаций пропускных способностей по Wi-Fi). С появлением стандарта IEEE 802.11n пропускная способность Wi-Fi начала зависеть от множества факторов, таких как тип используемой модуляции, скорость сверхточного кодирования, ширина канала и т.д. Чтобы не перечислять все возможные сочетания, инженеры представили единую таблицу и ввели понятие MSC, подробнее о которой можно узнать в сети Интернет.

Примечание: *Примечание: Если выбрать параметр “Ширина канала” 20 МГц, максимально возможное значение параметра “Пропускная способность” составит 65 Мбит/. Если выбрать параметр “Ширина канала” 40 МГц, максимально возможное значение параметра “Пропускная способность” составит 150 Мбит/с*

Порог фрагментации: Параметр задает максимальный размер фрейма (кадра) до процесса его фрагментации во множество фреймов (кадров). Диапазон допустимых значений – от 256 до 2346 Байт. Если установить слишком малое значение порога фрагментации, это негативно скажется на производительности сети Wi-Fi. Использование фрагментации увеличивает надежность доставки фреймов (кадров) в процессе передачи данных. Фрагментация больших фреймов на более малые значения снижает вероятность появления коллизий в процессе передачи данных. Слишком малое значение параметра уменьшит пропускную способность Wi-Fi сети, так как данные будут передаваться меньшими «порциями». Рекомендуем не изменять значение по умолчанию (2346), оно оптимально подобрано производителем чипсета Wi-Fi радиомодуля (точки доступа встроенной в роутер).

Порог RTS: Параметр задает максимальный размер фрейма (кадра) RTS (Request to Send), который высылается устройством-инициатором передачи данных всем устройствам в зоне покрытия сети роутера. Диапазон допустимых значений – от 0 до 2347 Байт. Значение по умолчанию – 2347.

RTS/CTS (Request to Send/Clear to Send) – механизм, используемый в сетях группы стандартов 802.11 для снижения вероятности возникновения коллизий, попутно решающий проблему «скрытого терминала». Размер фрейма (кадра) RTS/CTS может принимать значения от 0 до 2347 Байт. Если размер фрейма (кадра) больше порогового значения RTS/CTS, сеть Wi-Fi воспринимает его не как служебный запрос на передачу/прием данных и запускает механизм handshake, после чего начинается передача служебных фреймов (кадров). В тех случаях, когда размер фрейма (кадра) меньше или равен пороговому значению RTS/CTS, сеть Wi-Fi воспринимает его не как служебный запрос на передачу/прием данных, называемый RTS/CTS-фреймом, а как информационных кадр. Wi-Fi сеть использует Request to Send/Clear to Send фреймы (кадры) для снижения вероятности возникновения коллизий, запрашивая и инициируя процесс handshake между передающим и принимающим устройством до процесса передачи данных. Таким образом, служебный фрейм RTS, в котором содержится информация о времени, на которое будет зарезервирован канал для передачи данных передается не только на «нужное устройство», но и на все устройства сети Wi-Fi, решая проблему «скрытого терминала». Устройства сети Wi-Fi, инициирующие передачу данных, отсылают в первую очередь RTS фреймы (кадры), дождавшись handshake начинают отрав-

лять сами данные. Устройство сети Wi-Fi, ответившее CTS-фреймом на полученный RTS фрейм, свидетельствует о том, что среда свободна для передачи данных и запрашивает их передачу у устройства-инициатора. Алгоритм избегания коллизий посредством CTS-фреймов сообщает всем устройствам сети Wi-Fi информацию о доступности среды передачи данных, поэтому все устройства сети не предпринимают попытки передачи до тех пор, пока все данные не будут переданы.

Сигнальный интервал: Значение по умолчанию составляет 100 мс. Большее значение длины сигнального интервала улучшит дальность связи по Wi-Fi и повысит уровень энергосбережения на стороне клиентов сети. Если установить значение меньше чем 100 мс, это увеличит скорость подключения к устройству.

Макс. кол-во Wi-Fi клиентов Точки доступа: Опция задает максимальное количество Wi-Fi клиентов для основной сети Wi-Fi.

Макс. кол-во Wi-Fi клиентов Точки доступа 1: Опция задает максимальное количество Wi-Fi клиентов для сети Wi-Fi 1 (гостевая).

Макс. кол-во Wi-Fi клиентов Точки доступа 2: Опция задает максимальное количество Wi-Fi клиентов для сети Wi-Fi 2 (гостевая).

Тип преамбулы: Опция задает длину поля синхронизации, идущего перед каждым IEEE 802.11 фреймом (кадром). Большинство современных сетей Wi-Fi используют короткую преамбулу с полем синхронизации в 56-бит вместо длинной преамбулы с полем синхронизации в 128-бит. Некоторые устаревшие устройства, например, стандарта 802.11b поддерживают только работу с длинной преамбулой. Длинная преамбула выбрана в настройках по умолчанию.

IAPP: Протокол разработан для защищенного обмена служебной информацией через ESS (Extended Service Set) между вашим устройством и другой точкой доступа при осуществлении перехода клиента из одного Wi-Fi покрытия в другое (во время handoff) в роуминговых сетях Wi-Fi. Данный протокол включен по умолчанию.

Защита фреймов (кадров) CTS: Функция отключена по умолчанию.

Агрегация: Часть стандарта 802.11n. Данная опция позволяет за один цикл передачи отослать множество фреймов (кадров) за один раз. Технология объединяет более мелкие фреймы в один большой. У всех фреймов, которые «переупаковываются» в новые большие фреймы должны совпадать MAC-заголовки, класс трафика (QoS) и т.д.

Фреймы (кадры) – Параметр определяет количество малых фреймов (кадров), которые необходимо «переупаковывать» в новый большой фрейм (кадр).

Байт – Параметр определяет размер (в Байтах) в новых больших фреймах (кадрах).

Короткий защитный интервал: Параметр обеспечивает наилучшее качество соединения, распространения и огибания сигналов для передачи данных, чувствительных к помехам и задержкам.

Запрет обмена данными между Wi-Fi-клиентами: Функция запрещает обмен данными между Wi-Fi клиентами вашего роутера, подключенных к его точке доступа.

Сосуществование каналов 20 и 40 МГц: Функция автоматически выбирает наилучшую ширину канала исходя из спектральных условий эксплуатации устройства. Функция отключена по умолчанию.

Формирование диаграммы направленности передатчика (Beamforming): Функция позволяет улучшить зону покрытия Wi-Fi точки доступа встроенной в роутер.

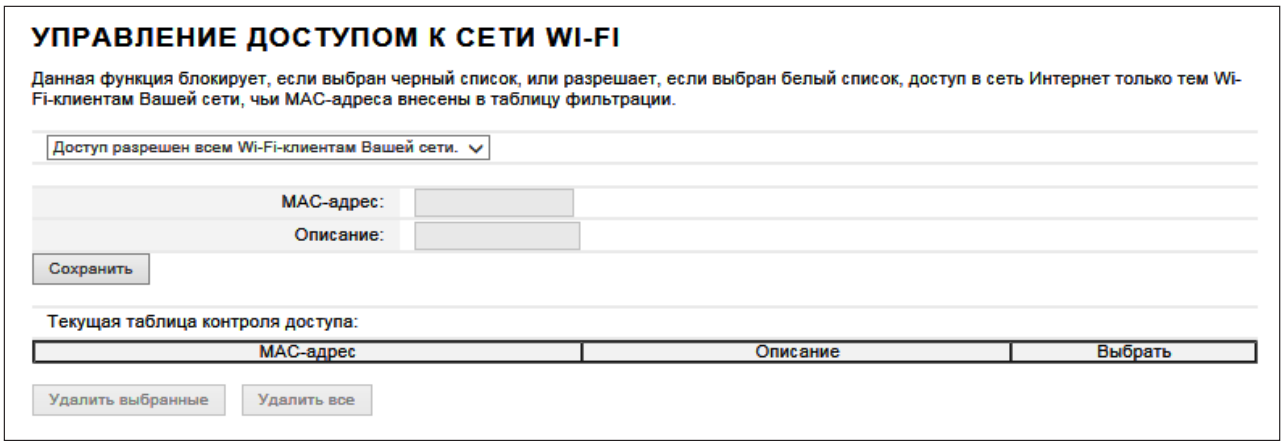
Излучаемая мощность передатчика: Селектором можно выбрать излучаемую мощность передатчика устройства. Значение по умолчанию – 100%.

Нажмите кнопку “Сохранить” для сохранения выполненных изменений в настройках устройства.

> ***Примечание:*** *Некоторые функции данного раздела могут быть дополнены/удалены в зависимости от версии микропрограммного обеспечения (прошивки)устройства.*

5.3.5 Управление доступом

Функция блокирует, если выбран черный список или разрешает, если выбран белый список доступ в сеть Интернет только тем Wi-Fi клиентам сети, чьи MAC-адреса внесены в таблицу фильтрации.



Внимание, доступ разрешен всем Wi-Fi клиентам сети по умолчанию.

Управление доступом может быть настроено двумя способами:

1. Если выбрать “Белый список” и ввести в данное поле MAC-адрес клиента сети Wi-Fi роутера, доступ для клиента с данным MAC-адресом к сети Wi-Fi будет полностью разрешен, в то время как доступ для всех остальных клиентов сети Wi-Fi будет запрещен.

2. Если выбрать “Черный список” и ввести в данное поле MAC-адрес клиента сети Wi-Fi роутера, доступ для клиента с данным MAC-адресом к сети Wi-Fi будет полностью запрещен, в то время как доступ для всех остальных клиентов сети Wi-Fi будет разрешен.

MAC-адрес: Введите в поле MAC-адрес клиентского устройства для которого необходимо применить правило управления доступом.

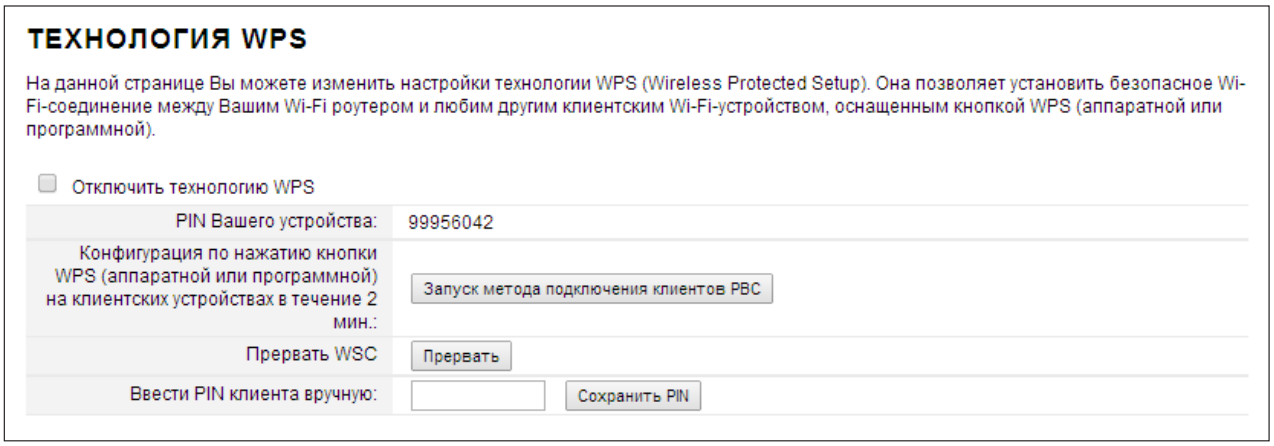
Описание: Введите в поле причину, по которой вы хотите занести в черный или белый список MAC-адрес данного клиентского устройства.

Нажмите на кнопку “Сохранить” для сохранения внесенных изменений в настройках устройства.

Текущая таблица контроля доступа: Таблица детально отображает информацию об управлении доступом. Используя кнопки, вы можете удалить выбранные или удалить все записи в таблице.

5.3.6 Технология WPS

На данной странице можно изменить настройки технологии WPS (Wireless Protected Setup). Она позволяет установить безопасное Wi-Fi соединение между роутером и любим другим клиентским Wi-Fi устройством, оснащенным кнопкой WPS (аппаратной или программной).



PIN вашего устройства: Поле отображает текущий PIN вашего Wi-Fi роутера.

Конфигурация по нажатию кнопки WPS (аппаратной или программной) на клиентских устройствах в течение 2 мин.: нажмите кнопку “Запуск метода подключения клиентов PBC” (Push-Button-To-Connect). После ее нажатия роутер будет ожидать запрос на подключение по технологии WPS от Wi-Fi клиентов в течение двух минут. Светодиодный индикатор WPS на передней панели роутера будет часто мигать. Это означает, что технология WPS роутера работает. Светодиодный индикатор вернется в свое нормальное состояние через две минуты.

Внимание! Необходимо успеть выполнить все описанные действия за интервал времени в две минуты.

Прервать WSC: Нажмите кнопку “Прервать”, чтобы отключить технологию WPS.

Ввести PIN клиента вручную: Введите PIN клиентского устройства в поле и нажмите на кнопку “Сохранить PIN”. Светодиодный индикатор WPS на передней панели вашего роутера будет часто мигать, это означает, что технология WPS вашего роутера работает. Светодиодный индикатор вернется в свое нормальное состояние через две минуты (помните, что необходимо успеть выполнить все описанные действия за интервал времени в две минуты).

Текущая информация о сети Wi-Fi: Таблица детально отображает информацию об алгоритме защиты сети Wi-Fi, аутентификации, шифровании и ключе безопасности сети Wi-Fi.

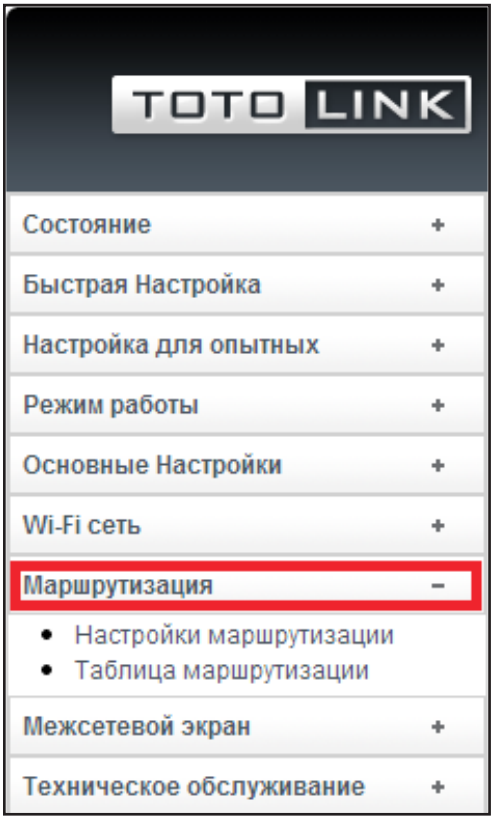
5.3.7 Расписание работы сети Wi-Fi

На данной странице Вы можете сформировать расписание работы сети Wi-Fi устройства. Внимание! Настройте соответствующие параметры в разделе ‘Дата и время’, прежде чем активировать эту функцию.

Сконфигурируйте расписание работы сети Wi-Fi согласно вашим потребностям. Нажмите кнопку “Сохранить” для сохранения выполненных изменений в настройках устройства.

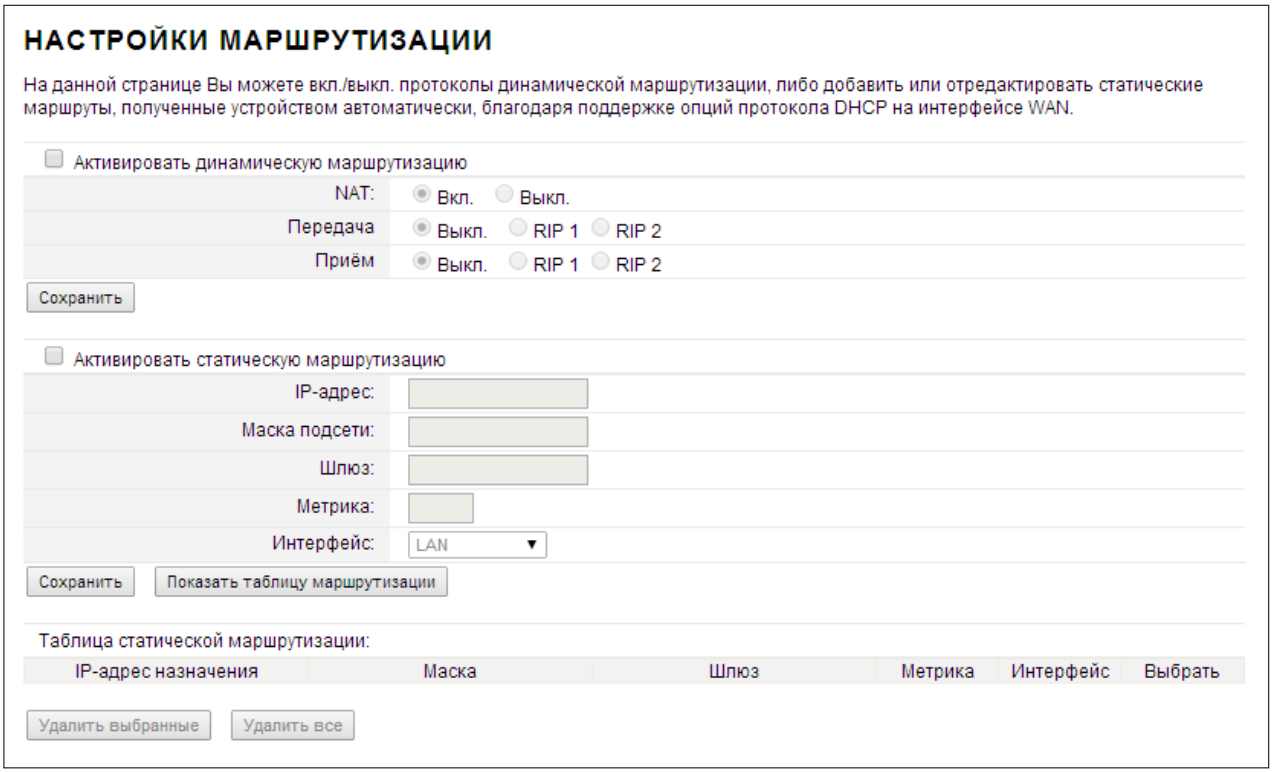
5.4 Маршрутизация

На данной странице можно настроить основные параметры маршрутизации.



5.4.1 Настройки маршрутизации

На данной странице можно вкл./выкл. протоколы динамической маршрутизации либо добавить или отредактировать статические маршруты, полученные устройством автоматически благодаря поддержке опций протокола DHCP на интерфейсе WAN.



Активировать динамическую маршрутизацию

В данном меню можно задать или настроить правила маршрутизации роутера. Если роутеры в сети Интернет-провайдера поддерживают, настроены и работают по протоколу динамической маршрутизации, позволяющей вашему роутеру отсылать и принимать информацию о сети и ее топологии (о том, как она построена) к/от роутера в сети Интернет-провайдера автоматически, то необходимо выставить корректные настройки в данном меню, предварительно удостоверившихся в них. Поставьте галочку в окне, чтобы включить функцию динамической маршрутизации.

> ***Внимание!*** *Прежде чем настраивать параметры в данном разделе убедитесь в том, что обладаете достаточным уровнем знаний в сфере маршрутизации и сетевых технологий IP-сетей.*

NAT: Опция включена по умолчанию. Более детальную информацию о параметре вы можете прочитать выше в данной инструкции.

Передача – Позволяет роутеру отсылать информацию о сети и ее топологии (о том как она построена) к роутеру в сети Интернет-провайдера таким образом, что сам роутер автоматически прокладывает маршруты.

- **Выкл.** – Отключение возможности получения информации о сети и ее топологии (о том как она построена) от роутера в сети Интернет-провайдера.

- **RIP1** – Протокол позволяет роутеру отослать информацию о маршрутах другим сетевым устройствам Интернет-провайдера по RIP версии 1.

- **RIP2** – Протокол позволяет роутеру отослать информацию о маршрутах другим сетевым устройствам Интернет-провайдера по RIP версии 2.

Прием – Позволяет роутеру получать информацию о сети и ее топологии (о том, как она построена) от роутера в сети Интернет-провайдера таким образом, что сам роутер автоматически прокладывает маршруты.

- **Выкл.** – Отключение возможности получения информации о сети и ее топологии (о том, как она построена) от роутера в сети Интернет-провайдера.

- **RIP1** – Протокол позволяет автоматически получить информацию от вышестоящего роутера в сети Интернет-провайдера по протоколу RIP версии 1.

- **RIP2** – Протокол позволяет автоматически получить информацию от вышестоящего роутера в сети Интернет-провайдера по протоколу RIP версии 2.

Активировать статическую маршрутизацию: Поставьте галочку в окне, чтобы включить функцию статической маршрутизации. Функция позволяет вручную задать маршрут продвижения пакетов через определенную IP-сеть и ее шлюз.

IP-адрес: Введите в поле IP-адрес для сети назначения маршрута IP-сети.

Маска подсети: Введите в поле маску подсети маршрута.

Шлюз: Введите в поле шлюз для сети назначения маршрута IP-сети.

Метрика: Введите в поле значение метрики маршрута IP-сети. Диапазон допустимых значений – от 1 до 15. Помните, что наименьшее значение метрики маршрута 1 обозначает наивысший приоритет.

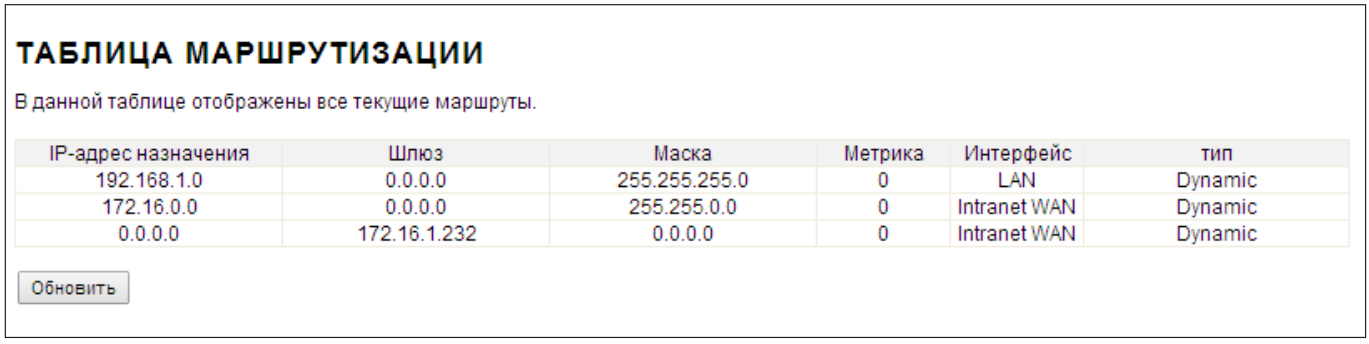
Интерфейс: Селектором можно выбрать интерфейс для IP-маршрута: Intranet WAN, Internet WAN или LAN.

Таблица статической маршрутизации: Таблица детально отображает информацию об IP-адресах сети назначения маршрутов.

Нажмите кнопку “Сохранить” для сохранения выполненных изменений в настройках устройства.

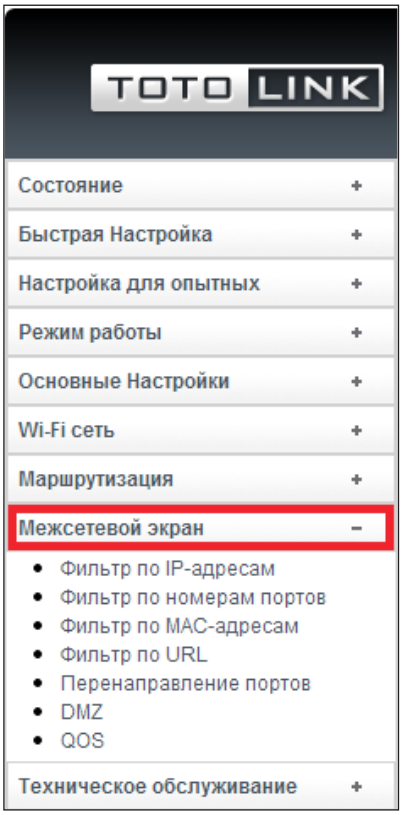
5.4.2 Таблица маршрутизации

В таблице отображены все текущие маршруты.



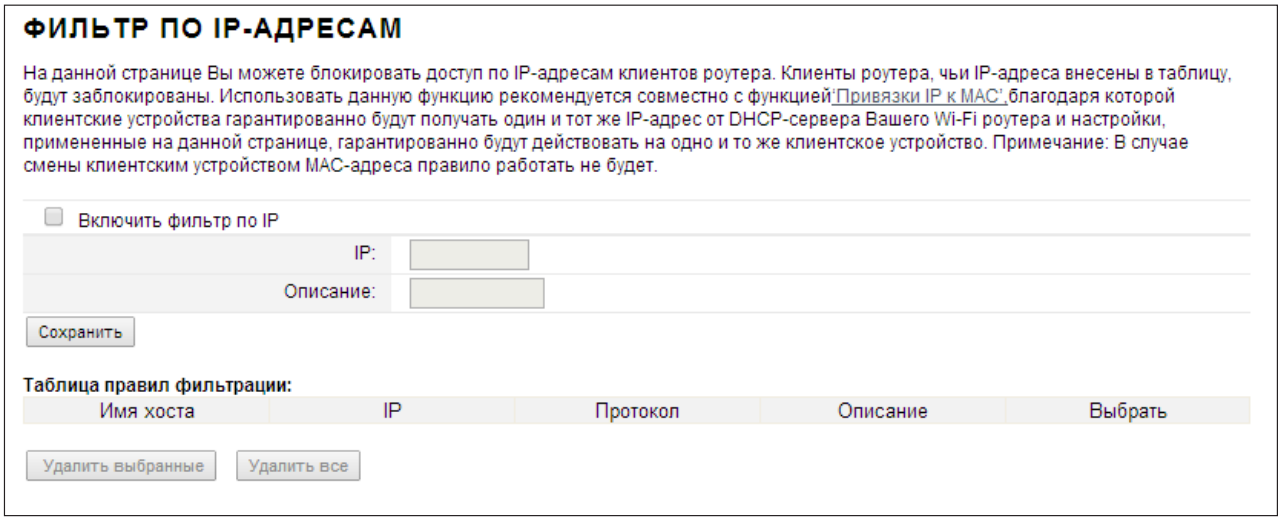
5.5 Межсетевой экран

С ростом количества клиентских устройств, подключенных к роутеру, требуется все больше скорости и производительности для обеспечения хорошего и стабильного покрытия сети Wi-Fi, передачи IPTV, работы P2P-приложений. Помимо этого роутер поддерживает функцию межсетевого экрана, который обеспечит высокий уровень безопасности сети и защитит ее от несанкционированного доступа в случае правильной настройки, корректной и внимательной эксплуатации устройства.



5.5.1 Фильтр по IP-адресам

На данной странице можно блокировать доступ по IP-адресам клиентов роутера. Клиенты роутера, чьи IP-адреса внесены в таблицу, будут заблокированы. Использовать данную функцию рекомендуется совместно с функцией “Привязки IP к MAC”, благодаря которой клиентские устройства гарантированно будут получать один и тот же IP-адрес от DHCP-сервера вашего роутера и настройки, примененные на данной странице будут действовать на одно и то же клиентское устройство. **Примечание:** В случае смены клиентским устройством MAC-адреса правило работать не будет.



Включить фильтр по IP: Поставьте галочку в окне, чтобы включить функцию фильтра по IP-адресам.

IP: Введите в поле IP-адрес клиентского устройства, доступ которому хотите запретить.

Протокол: Уточните заранее протокол работы для применяемого правила. Данным селектором можно выбрать: Оба/UDP/TCP.

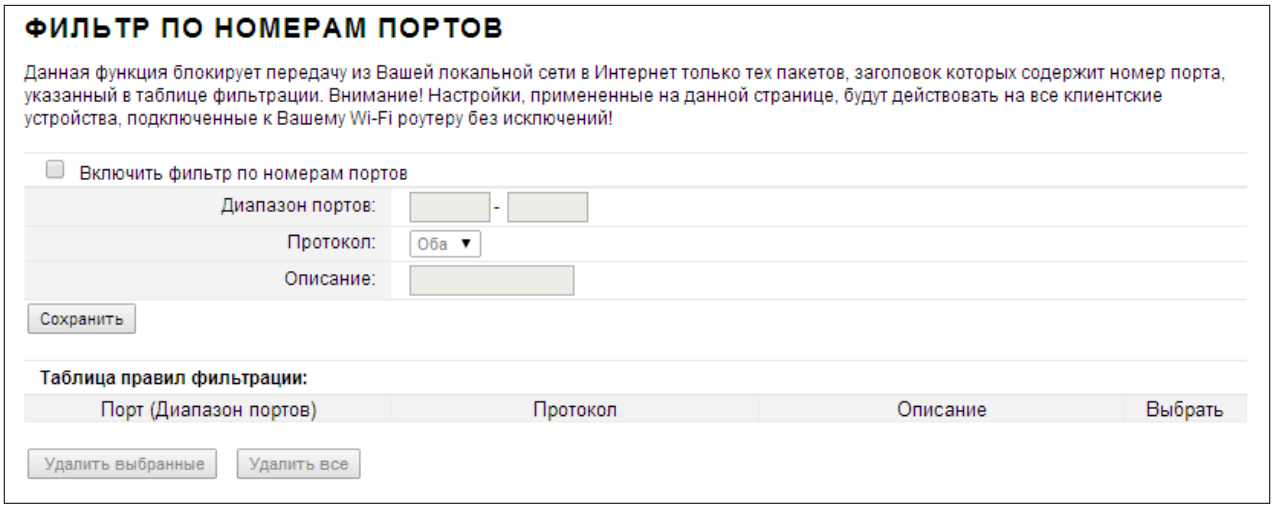
Описание: Введите в поле причину по которой хотите применить данное правило для конкретного IP-адреса. Обычно хватает пары слов для описания. Например: Торрент или сетевая атака.

Таблица правил фильтрации: Таблица детально отображает информацию об IP-адресах клиентских устройств, на которые действуют правила фильтрации.

Нажмите кнопку “Сохранить” для сохранения выполненных изменений в настройках устройства.

5.5.2 Фильтр по номерам портов

Функция блокирует передачу из вашей локальной сети в Интернет только тех пакетов, заголовок которых содержит номер порта, указанный в таблице фильтрации. **Внимание!** Настройки, примененные на странице будут действовать на все клиентские устройства, подключенные к роутеру!



Включить фильтр по номерам портов: Поставьте галочку в окне, чтобы включить функцию фильтр по номерам портов.

Диапазон портов: Введите значение номера порта в оба поля или диапазон для данного правила фильтра.

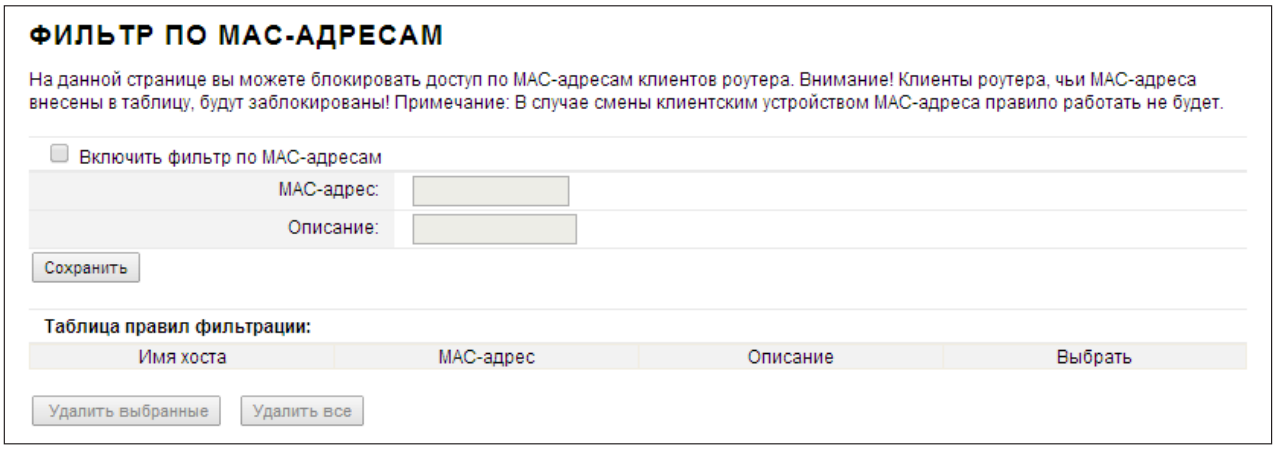
Протокол: Уточните заранее протокол работы для применяемого правила фильтра по номерам портов. Селектором можно выбрать: Оба/UDP/TCP.

Описание: Введите в поле причину, по которой хотите применить данное правило для конкретного номера порта. Обычно хватает пары слов для описания. Например: Торрент или сетевая атака.

Таблица правил фильтрации: Таблица детально отображает информацию о номерах портов, на которые действуют правила фильтрации. Нажмите кнопку “Сохранить” для сохранения выполненных изменений в настройках устройства.

5.5.3 Фильтр по MAC-адресам

На странице можно блокировать доступ по MAC-адресам клиентов роутера. Внимание! Клиенты роутера, чьи MAC-адреса внесены в таблицу, будут заблокированы! Примечание: В случае смены клиентским устройством MAC-адреса правило работать не будет.



Включить фильтр по MAC-адресам: Поставьте галочку в окне, чтобы включить функцию фильтра по MAC-адресам.

MAC-адрес: Введите в поле MAC-адрес клиентского устройства, доступ которому вы бы хотели запретить.

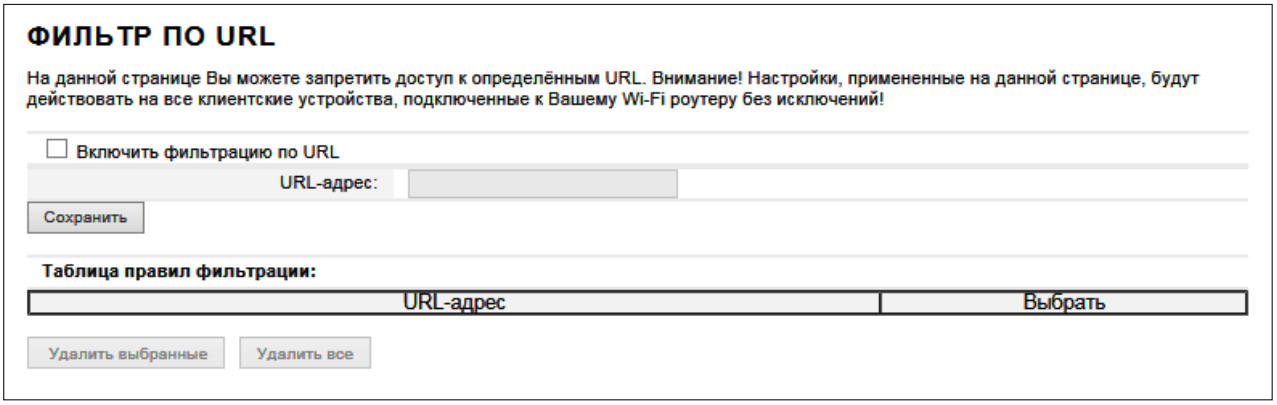
Описание: Введите в поле причину, по которой хотите применить данное правило для конкретного клиентского устройства, с данным MAC-адресом. Обычно хватает пары слов для описания. Например: Торрент или сетевая атака, неисправное оборудование и т.д.

Таблица правил фильтрации: Таблица детально отображает информацию о MAC-адресах клиентских устройств, на которые действуют правила фильтрации.

Нажмите кнопку “Сохранить” для сохранения выполненных изменений в настройках устройства.

5.5.4 Фильтр по URL

На данной странице можно запретить доступ к определенным URL. Внимание! Примененные настройки будут действовать на все клиентские устройства, подключенные к роутеру!



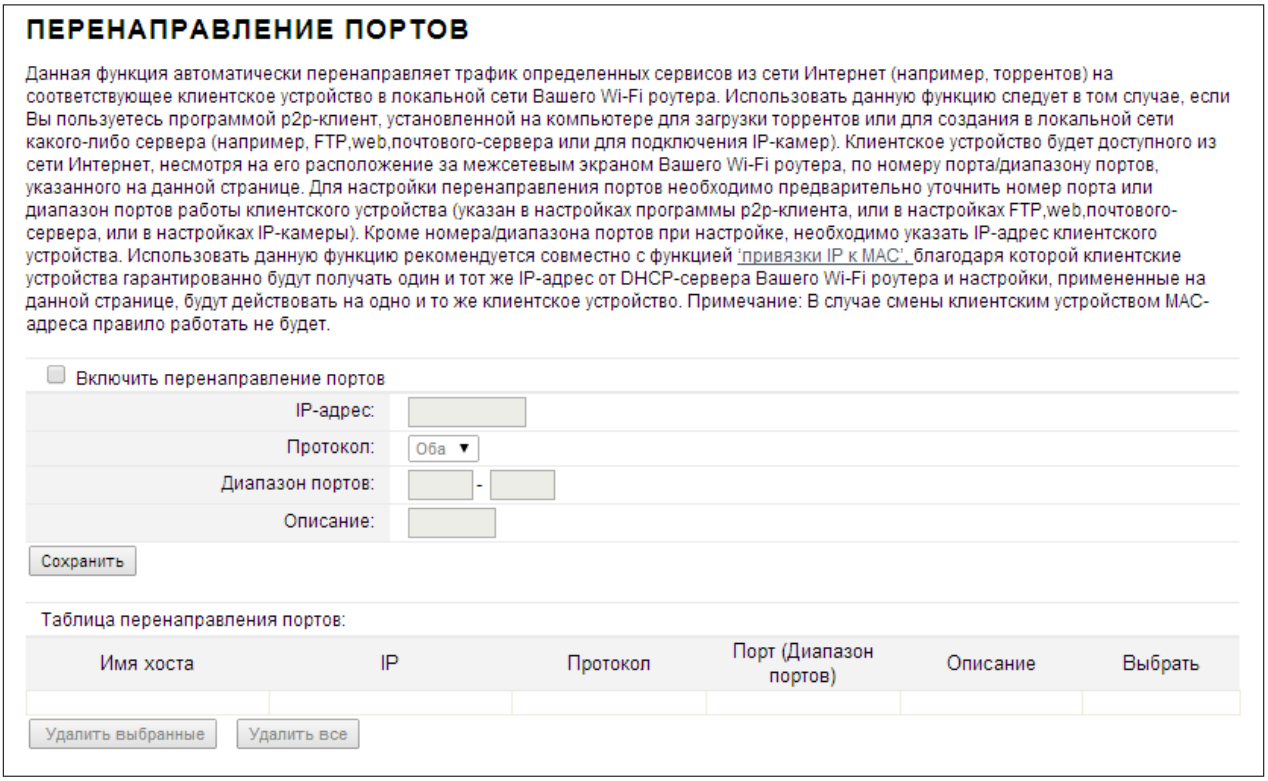
Включить фильтрацию по URL: Поставьте галочку в окне, чтобы включить функцию фильтрации по URL.

URL-адрес: Введите в поле ключевые слова, которые могут содержаться в названиях сайтов (URL), доступ к которым запрещен всем клиентским устройствам, подключенных к роутеру.

Таблица правил фильтрации: Таблица детально отображает информацию о тех ключевых словах, которые могут содержаться в названиях сайтов (URL), доступ к которым запрещен, например, по вопросам этики.

Нажмите кнопку “Сохранить” для сохранения выполненных изменений в настройках устройства.

5.5.5 Перенаправление портов



Функция автоматически перенаправляет трафик определенных сервисов из сети Интернет (например, трафик торрент-трекеров) на соответствующее клиентское устройство в локальной сети роутера. Использовать функцию следует в случае, если вы пользуетесь P2P-клиентом, установленным на компьютере для загрузки торрентов или для создания в локальной сети какого-либо сервера (например, FTP, WEB, почтового сервера или для подключения IP-камер). Клиентское устройство будет доступно из сети Интернет несмотря на его расположение за межсетевым экраном роутера, по номеру порта/диапазону портов, указанного/указанных на странице. Для настройки перенаправления портов необходимо предварительно уточнить номер порта или диапазон портов работы клиентского устройства (указан в настройках программы P2P-клиента или в настройках FTP, WEB, почтового сервера или IP-камеры). Кроме номера/диапазона портов при настройке необходимо указать IP-адрес клиентского устройства. Использовать функцию рекомендуется совместно с функцией привязки IP к MAC, благодаря которой клиентские устройства гарантированно будут получать один и тот же IP-адрес от DHCP-сервера вашего роутера и настройки, примененные на данной странице, будут действовать на одно и то же клиентское устройство. **Примечание:** В случае смены клиентским устройством MAC-адреса правило работать не будет.

Включить перенаправление портов: Поставьте галочку в окне, чтобы включить функцию перенаправления портов.

IP-адрес: Введите в поле IP-адрес устройства для которого хотите применить правило перенаправления портов.

Протокол: Уточните заранее протокол работы для применяемого правила перенаправления портов. Селектором можно выбрать: Оба/UDP/TCP.

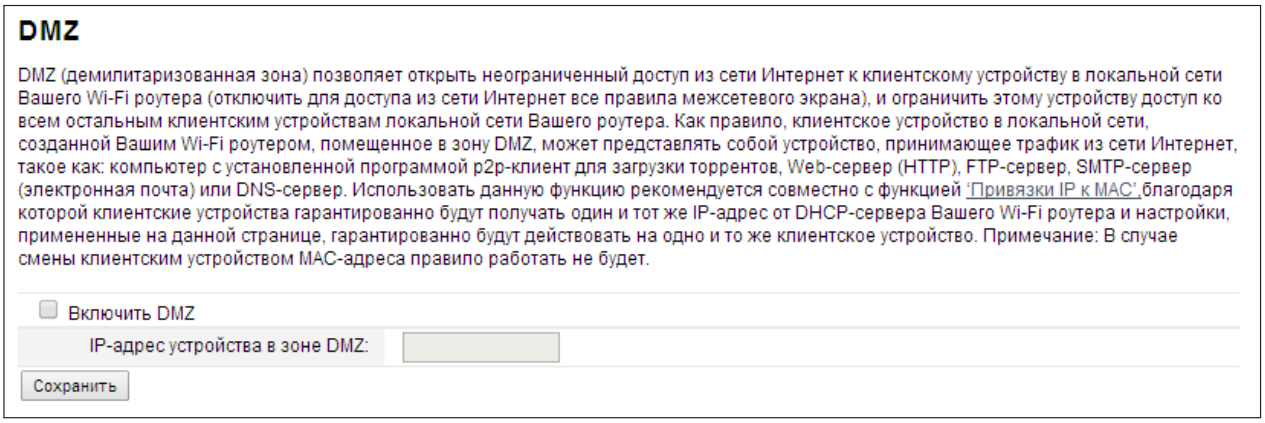
Диапазон портов: Введите значение номера порта в оба поля или диапазон.

Описание: Введите в поле причину по которой хотите применить данное правило для конкретного номера порта. Обычно хватает пары слов для описания. Например: Торрент или IP-камера.

Таблица перенаправления портов: Таблица детально отображает информацию о номерах портов, на которых действует правила перенаправления.

Нажмите кнопку “Сохранить” для сохранения выполненных изменений в настройках устройства.

5.5.6 DMZ



DMZ (демилитаризованная зона) позволяет открыть неограниченный доступ из сети Интернет к клиентскому устройству в локальной сети роутера (отключить для доступа из сети Интернет все правила межсетевого экрана) и ограничить этому устройству доступ ко всем остальным клиентским устройствам локальной сети роутера. Как правило клиентское устройство в локальной сети, созданным роутером, помещенное в зону DMZ, может представлять собой устройство, принимающее трафик из сети Интернет, например, компьютер с установленной программой P2P-клиента для загрузки торрентов, WEB-сервер (HTTP), FTP-сервер, SMTP-сервер (электронная почта) или DNS-сервер. Использовать данную функцию рекомендуется совместно с функцией привязки IP к MAC, благодаря которой клиентские устройства гарантированно будут получать один и тот же IP-адрес от DHCP-сервера вашего роутера и настройки, примененные на данной странице, гарантированно будут действовать на одно и то же клиентское устройство. Примечание: В случае смены клиентским устройством MAC-адреса правило работать не будет.

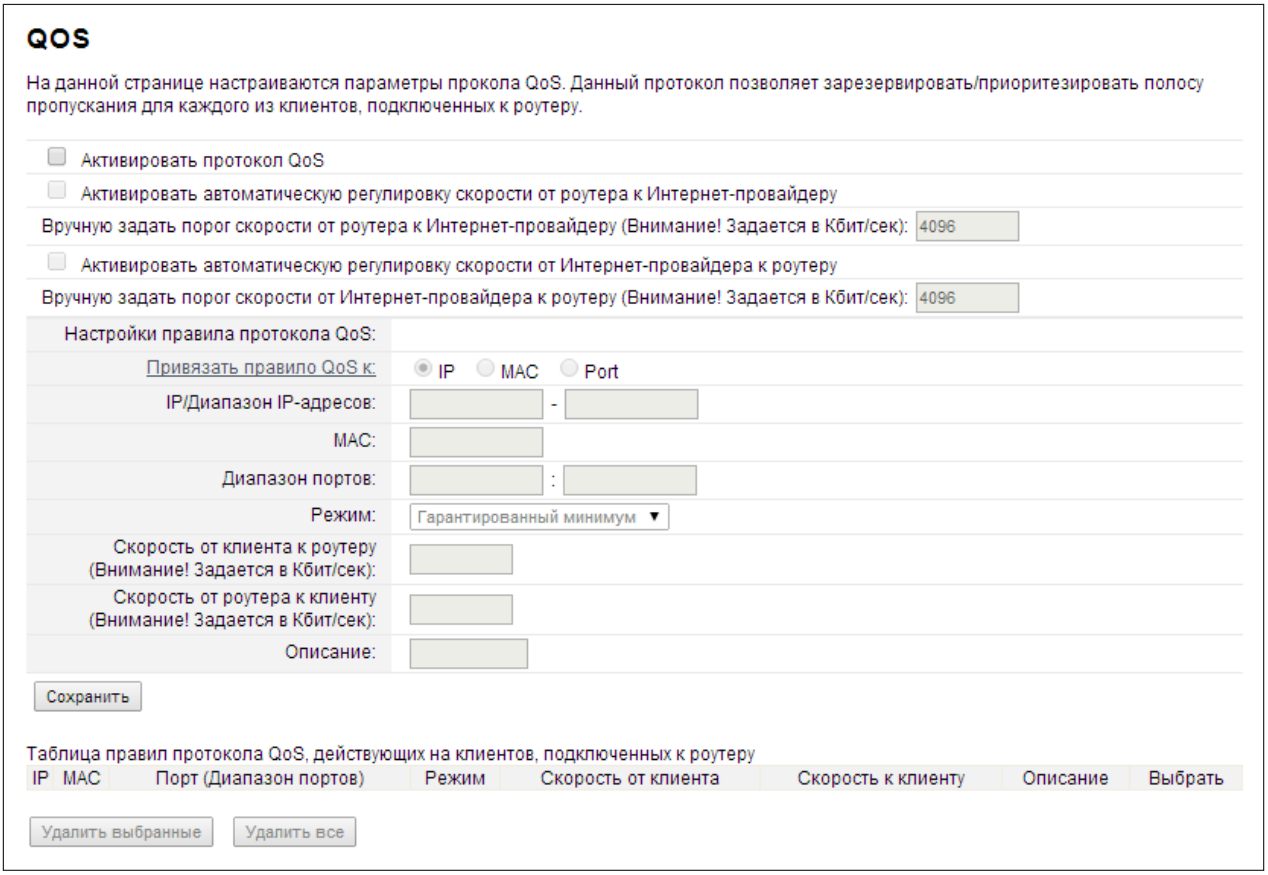
Включить DMZ: Поставьте галочку в окне, чтобы включить функцию DMZ.

IP-адрес устройства в зоне DMZ: Введите в поле IP-адрес хоста DMZ.

Нажмите кнопку “Сохранить” для сохранения выполненных изменений в настройках устройства.

5.5.7 QOS

На данной странице настраиваются параметры прокола QoS. Данный протокол позволяет зарезервировать/приоритезировать полосу пропускания для каждого из клиентов, подключенных к роутеру.



Активировать протокол QoS: Поставьте галочку в окне, чтобы включить функцию QoS.

Активировать автоматическую регулировку скорости от роутера к Интернет-провайдеру: Поставьте галочку в окне, чтобы включить автоматическую регулировку QoS.

Вручную задать порог скорости от роутера к Интернет-провайдеру (Внимание! Задается в Кбит/сек): Введите числовое значение в поле.

Активировать автоматическую регулировку скорости от Интернет-провайдера к роутеру: Поставьте галочку в окне, чтобы включить автоматическую регулировку QoS.

Вручную задать порог скорости от Интернет-провайдера к роутеру (Внимание! Задается в Кбит/сек): Введите числовое значение в поле.

Привязать правило QoS к: выберите по какому признаку будет работать правило. Вы можете выбрать: IP,MAC или Port. Нажав на саму надпись вы перейдете в раздел привязки IP к MAC.

Режим: селектором можно выбрать возможный максимум или гарантированный минимум для правила работы протокола QoS.

Скорость от клиента к роутеру (Внимание! Задается в Кбит/сек): Введите значение в данное поле.

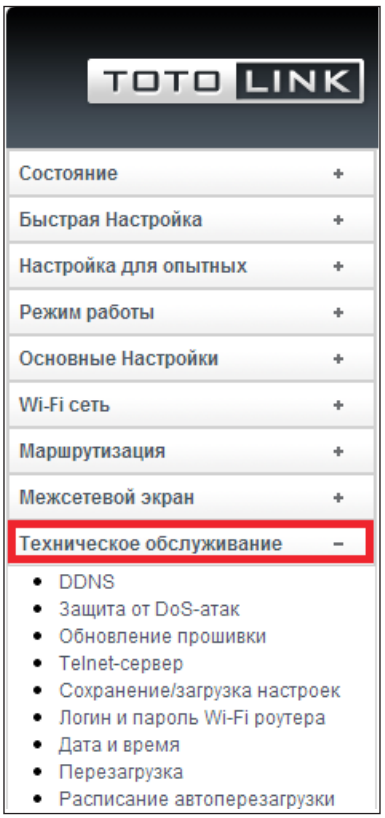
Скорость от роутера к клиенту (Внимание! Задается в Кбит/сек): Введите значение в данное поле.

Описание: Введите в поле причину по которой хотите применить данное правило для конкретного правила протокола QoS. Обычно хватает пары слов для описания. Например: Торрент или IP-камера.

Таблица правил протокола QoS, действующих на клиентов, подключенных к роутеру: Таблица детально отображает информацию о правилах. Нажмите кнопку “Сохранить” для сохранения выполненных изменений в настройках устройства.

> ***Примечание: Внимание!*** *Устройство сконфигурировано в настройках по умолчанию таким образом, что количество активных соединений не превышает 2048! Для комфортной работы p2p-клиента с одновременным просмотром IP-TV и Web-серфингом, рекомендация производителя – использовать в настройках p2p-клиентов не более 500 активных одновременных соединений наряду с ограничением полосы пропускания на уровне 7 - 7,5 МБайт/с.*

5.6 Техническое обслуживание



5.6.1 DDNS

Сервис Dynamic DNS (Domain Name Service) позволяет присвоить доменное имя к динамическому реальному IP-адресу в сети Интернет, что очень удобно для конечных пользователей. Благодаря поддержке и настройке данной функции на устройстве, Ваш Wi-Fi роутер всегда будет доступен удаленно из сети Интернет, но не по IP-адресу, который может измениться со временем, а по доменному имени, которые Вам присвоил один из поддерживаемых поставщиков сервиса Dynamic DNS. Для настройки данной функции необходимо предварительно зарегистрироваться на сайте одного из поддерживаемых устройством поставщиков сервиса Dynamic DNS, ввести логин и пароль, а также доменное имя присвоенное Вам. Внимание! Некоторые Интернет-провайдеры могут некорректно работать с данным типом сервиса ввиду топологии их сети и настройкам сервисной модели!

Активировать DDNS: Поставьте галочку в окне, чтобы включить функцию DDNS.

Сервис: селектором можно выбрать DynDNS, TZO или NOIP. Выберите одного из поставщиков сервиса DDNS для которого у вас есть зарегистрированный и работающий аккаунт.

Auto-Update interval: Введите значение в данное поле.

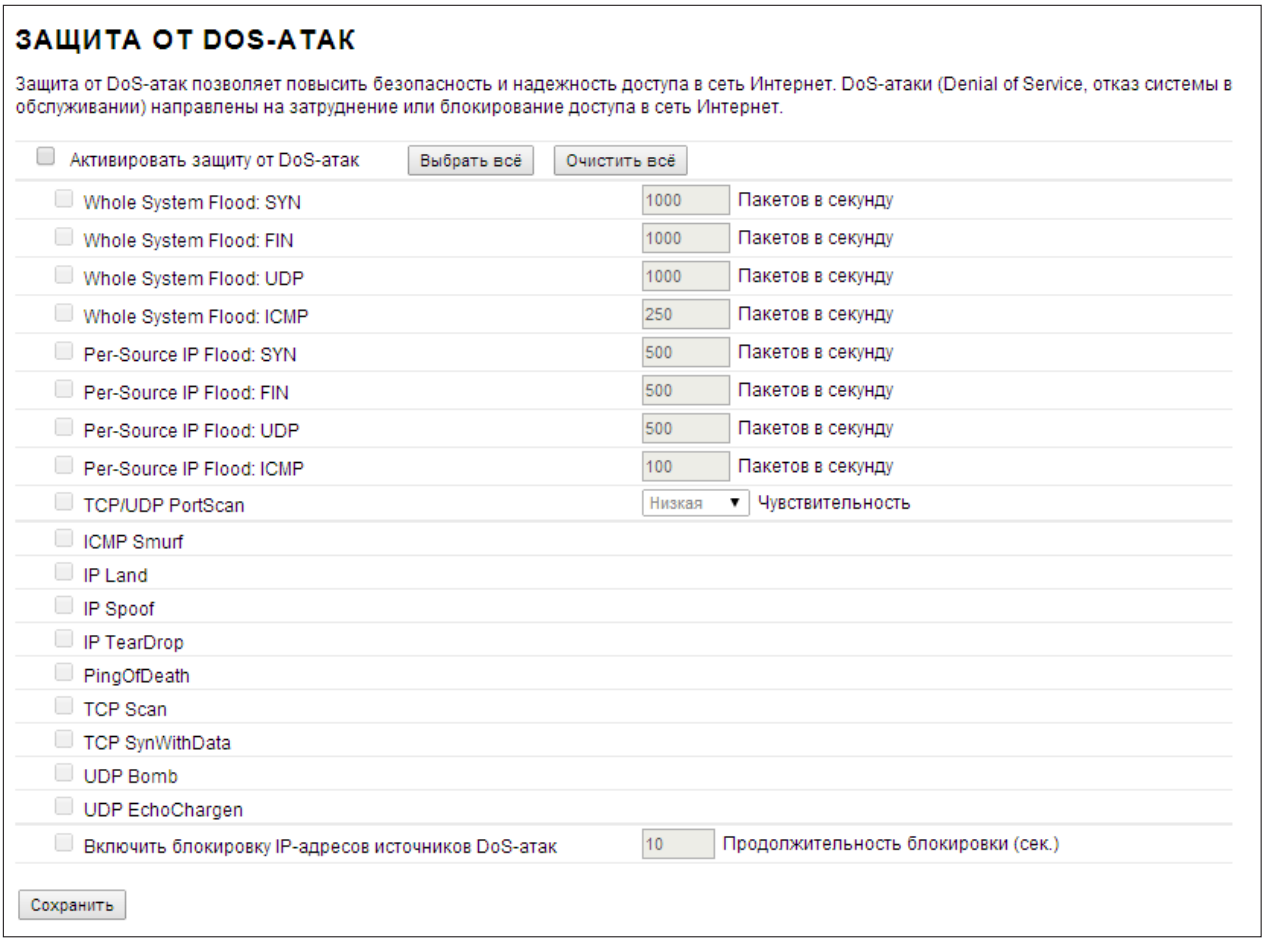
Доменное имя: Введите в поле доменное имя, которые вам присвоил поставщик сервиса DDNS в процессе регистрации и создания аккаунта.

Логин/Email: Введите в поле логин или Email, которые вам присвоил поставщик сервиса DDNS в процессе регистрации и создания аккаунта.

Пароль: Введите в поле пароль или ключ для вашего DDNS аккаунта. Нажмите кнопку “Сохранить” для сохранения выполненных изменений в настройках устройства.

5.6.2 Защита от DoS-атак

Защита от DoS-атак позволяет повысить безопасность и надежность доступа в сеть Интернет. DoS-атаки (Denial of Service, отказ системы в обслуживании) направлены на затруднение или блокирование доступа в сеть Интернет.



Активировать защиту от DoS-атак: Поставьте галочку в окне, чтобы включить функцию защиты от DoS-атак.

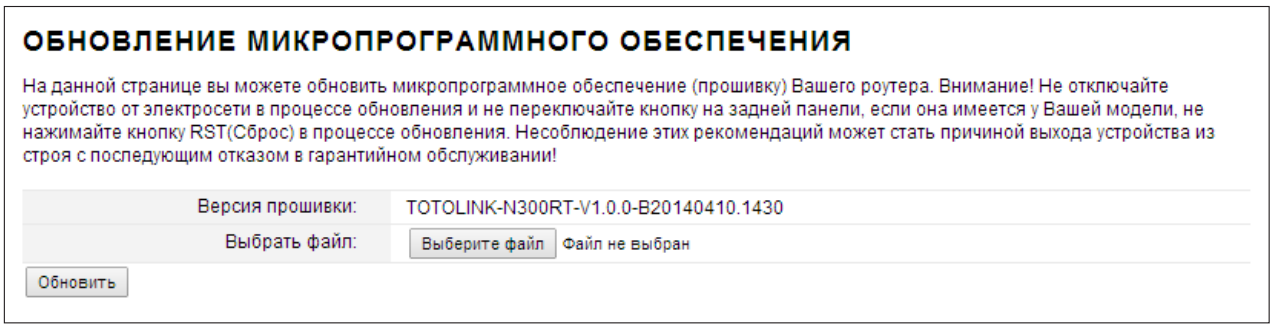
Страница отображает типы защиты от DoS-атак, которые роутер способен распознать:

Whole System Flood: SYN	ICMP Smurf
Whole System Flood: FIN	IP Land
Whole System Flood: UDP	IP Spoof
Whole System Flood: ICMP	IP TearDrop
Per-Source IP Flood: SYN	Ping of Death
Per-Source IP Flood: FIN	TCP Scan
Per-Source IP Flood: UDP	TCP SynWithData
Per-Source IP Flood: ICMP	UDP Bomb
TCP/UDP PortScan	UDP EchoChargen

Чувствительность: Селектором можно выбрать низкую или высокую чувствительность. Нажмите кнопку “Выбрать все” или “Очистить все” для выбора алгоритма защиты сети.

5.6.3 Обновление прошивки

На странице можно обновить микропрограммное обеспечение (прошивку) роутера. Внимание! Не отключайте устройство от электросети в процессе обновления и не переключайте кнопку на задней панели, если она имеется у вашей модели, не нажимайте кнопку RST (Сброс) в процессе обновления. Несоблюдение этих рекомендаций может стать причиной выхода устройства из строя с последующим отказом в гарантийном обслуживании!



Версия прошивки: Поле отображает текущую версию микропрограммного обеспечения (прошивки), установленного на устройстве.

Выбрать файл: В поле будет указан путь к новому файлу микропрограммного обеспечения (прошивки), который должен быть заранее загружен с сайта производителя устройства или каким-либо другим образом сохранен и доступен на вашем компьютере.

Нажмите кнопку “Выберите файл”, чтобы выбрать новый файл микропрограммного обеспечения (прошивки) для его установки на роутер.

5.6.4 Telnet-сервер

Включить Telnet: Функция активирует протокол Telnet для удаленного управления устройством.

Логин: Введите в поле логин для доступа по протоколу Telnet.

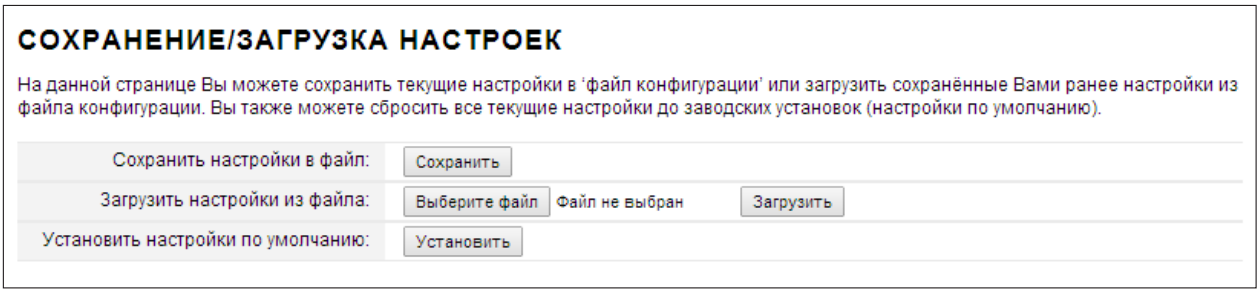
Пароль: Введите в поле пароль для доступа по протоколу Telnet.

Логин и пароль для протокола Telnet по умолчанию: root.

Нажмите кнопку “Сохранить” для сохранения выполненных изменений в настройках устройства.

5.6.5 Сохранение/загрузка настроек

На странице можно сохранить текущие настройки в “файл конфигурации” или загрузить сохраненные ранее настройки из файла конфигурации. Также можно сбросить текущие настройки до заводских установок (настройки по умолчанию).



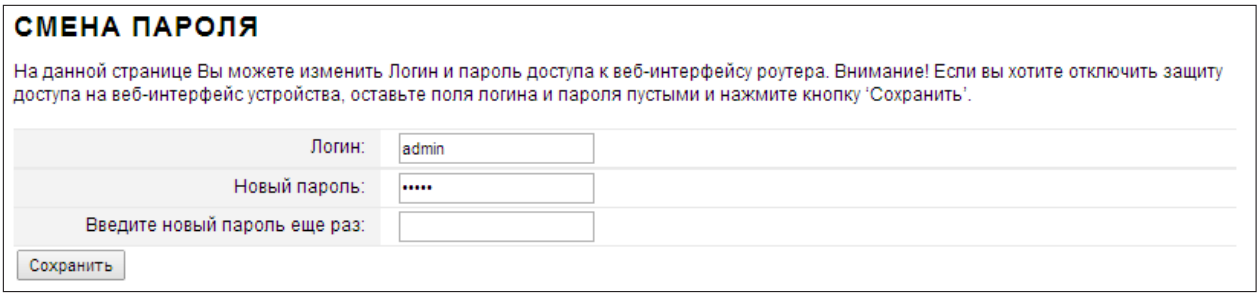
Сохранить настройки в файл: Нажмите кнопку “Сохранить”, чтобы загрузить на компьютер текущий файл конфигурации роутера, где будут сохранены все текущие настройки.

Загрузить настройки из файла: Если хотите загрузить настройки из файла конфигурации, который был сохранен на компьютере ранее и применить их, нажмите на “Выберите файл” и выберите необходимый файл конфигурации, сохраненный ранее, затем нажмите кнопку “Загрузить”.

Установить настройки по умолчанию: После нажатия кнопки “Установить” устройство уйдет в перезагрузку, после которой обретет настройки по умолчанию.

5.6.6 Логин и пароль Wi-Fi роутера

На данной странице можно изменить логин и пароль доступа к WEB-интерфейсу роутера. **Внимание!** Если хотите отключить защиту доступа к WEB-интерфейсу устройства, оставьте поля логина и пароля пустыми и нажмите кнопку “Сохранить”.



Логин: Введите в поле желаемое имя пользователя (логин) для авторизации в WEB-интерфейсе устройства.

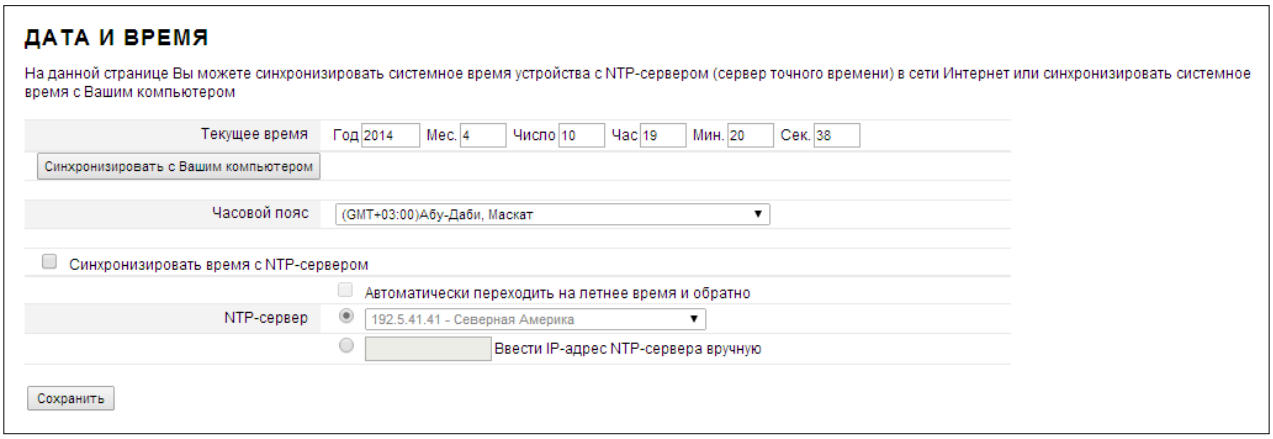
Новый пароль: Введите в поле новый пароль для управления устройством под учетной записью администратора.

Введите новый пароль еще раз: Введите в поле новый пароль, чтобы убедится в том, что не допущена ошибка или опечатка при вводе.

Нажмите кнопку “Сохранить” для сохранения выполненных изменений в настройках устройства.

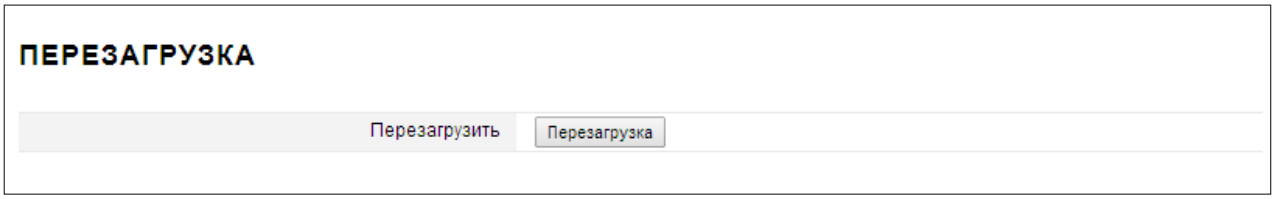
5.6.7 Дата и время

Для получения справочной информации по пункту ‘Дата и время’ обратитесь к пункту 4.3.2 данной инструкции.



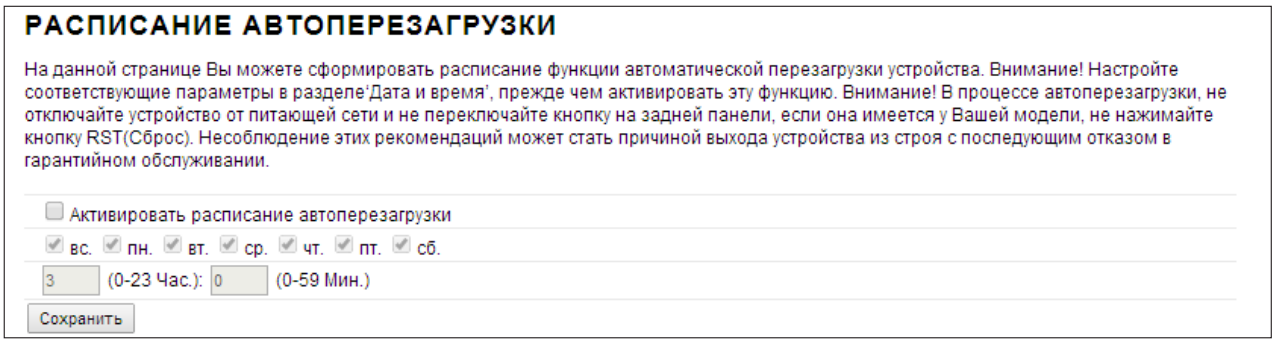
5.6.8 Перезагрузка

Нажмите кнопку “Перезагрузка” соответствующего меню для перезагрузки устройства.



5.6.9 Расписание автоперезагрузки

На данной странице Вы можете сформировать расписание функции автоматической перезагрузки устройства. Внимание! Настройте соответствующие параметры в разделе ‘Дата и время’, прежде чем активировать эту функцию. **Внимание!** В процессе автоперезагрузки, не отключайте устройство от питающей сети и не переключайте кнопку на задней панели, если она имеется у Вашей модели, не нажимайте кнопку RST(Сброс). Несоблюдение этих рекомендаций может стать причиной выхода устройства из строя с последующим отказом в гарантийном обслуживании.



Активировать расписание автоперезагрузки: Поставьте галочку в окне, чтобы включить функцию. Нажмите кнопку “Сохранить” для сохранения выполненных изменений в настройках устройства.