

TP-LINK®

Руководство пользователя

TD-W8950N

TD-W8960N

Беспроводной маршрутизатор серии N со встроенным модемом
ADSL2+



Rev: 1.0.0

1910011116

АВТОРСКОЕ ПРАВО И ТОРГОВЫЕ МАРКИ

Спецификации могут меняться без уведомления. **TP-LINK®** является зарегистрированной торговой маркой компании «TP-LINK TECHNOLOGIES CO., LTD». Прочие бренды и наименования продукции являются торговыми марками или зарегистрированными торговыми марками их владельцев.

Спецификации не могут быть воспроизведены в какой-либо форме или посредством каких-либо средств или использованы для составления производных материалов с помощью перевода, трансформации или переработки настоящей публикации при отсутствии разрешения от компании «TP-LINK TECHNOLOGIES CO., LTD». Copyright © 2015 TP-LINK TECHNOLOGIES CO., LTD. Все права защищены.

<http://www.tp-link.com>



Продукт сертифіковано згідно с правилами системи УкрСЕПРО на відповідність вимогам нормативних документів та вимогам, що передбачені чинними законодавчими актами України.

EAC

Правила безопасности

- Если устройство имеет кнопку включения/выключения питания, то с её помощью можно быстро отключить питание устройства. Если кнопки питания на устройстве нет, единственный способ полностью обесточить устройство - отключить адаптер питания от электросети.
- Не разбирайте устройство и не производите его ремонт самостоятельно, в этом случае компания вправе снять с себя гарантийные обязательства, кроме того, вы подвергаетесь риску поражения электрическим током.
- Не допускайте попадания влаги внутрь устройства.

Устройство предназначено для использования в следующих странах:

AT	BG	BY	CA	CZ	DE	DK	EE
ES	FI	FR	GB	GR	HU	IE	IT
LT	LV	MT	NL	NO	PL	PT	RO
RU	SE	SK	TR	UA	US		

Содержание

Комплект поставки	1
Глава 1. Введение	2
1.1 Обзор устройства	2
1.2 Основные характеристики	2
1.3 Описание панелей.....	4
1.3.1 Передняя панель	4
1.3.2 Задняя панель.....	5
Глава 2. Подключение маршрутизатора	7
2.1 Системные требования.....	7
2.2 Требования к среде установки	7
2.3 Подключение маршрутизатора	8
Глава 3. Руководство по быстрой настройке	9
3.1 Настройка TCP/IP	9
3.2 Руководство по быстрой настройке	10
Глава 4. Настройка маршрутизатора	15
4.1 Вход	15
4.2 Состояние.....	15
4.3 Быстрая настройка.....	16
4.4 Дополнительные настройки.....	16
4.4.1 Интерфейс уровня 2	17
4.4.2 WAN	20
4.4.3 Клонирование MAC-адреса	30
4.4.4 LAN.....	30
4.4.5 NAT.....	35
4.4.6 Защита	40
4.4.7 Родительский контроль	42
4.4.8 Приоритезация данных	44
4.4.9 Контроль пропускной способности.....	48
4.4.10 Маршрутизация.....	50
4.4.11 DNS	53
4.4.12 DSL.....	55
4.4.13 UPnP	56
4.4.14 Группировка портов	57
4.4.15 IP-туннель.....	59
4.4.16 IPSec	61

4.4.17 Multicast	64
4.5 IPTV	64
4.6 Беспроводной режим	65
4.6.1 Основные настройки	66
4.6.2 Защита	67
4.6.3 Расписание Wi-Fi	84
4.6.4 Фильтрация MAC-адресов	85
4.6.5 Беспроводной мост	87
4.6.6 Дополнительные настройки	89
4.6.7 Состояние станций	91
4.7 Гостевая Сеть	91
4.7.1 Основные настройки	92
4.7.2 Список станций	93
4.8 Диагностика	93
4.9 Управление	94
4.9.1 Настройки	94
4.9.2 Системный журнал	97
4.9.3 SNMP	98
4.9.4 Клиент TR-069	100
4.9.5 Время	101
4.9.6 Контроль доступа	102
4.9.7 Обновление встроенного ПО	103
4.9.8 Перезагрузка	104
4.10 Выход	105
Приложение А: Спецификации	106
Приложение В: Настройки ПК	107
Приложение С: Устранение неисправностей	111
Приложение D: Техническая поддержка	114

Данное руководство пользователя подходит для моделей TD-W8950N(RU)_1.0 и TD-W8960N(RU)_6.0. Для примера используется TD-W8950N(RU)_1.0. В случае несоответствия между описанием и самим устройством, пожалуйста, ориентируйтесь по устройству.

Комплект поставки

В комплект поставки входят:

- Один беспроводной маршрутизатор серии N со встроенным модемом ADSL2+ модели TD-W8950N или TD-W8960N
- Один адаптер питания для маршрутизатора
- Руководство по быстрой установке
- Один кабель с разъёмом RJ45
- Два кабеля с разъёмом RJ11
- Один ADSL-сплиттер
- Один компакт-диск с материалами, включая:
 - Руководство пользователя
 - Другую полезную информацию



Примечание:

Убедитесь в том, что комплект содержит все указанные выше наименования. Если что-либо повреждено или отсутствует, обратитесь к своему продавцу.

Глава 1. Введение

Благодарим Вас за выбор нашего беспроводного маршрутизатора серии N со встроенным модемом ADSL2+ модели **TD-W8950N**, со скоростью передачи данных до 150 Мбит/с.

1.1 Обзор устройства

Беспроводной маршрутизатор модели **TD-W8950N** – это надёжное устройство класса «всё в одном», которое объединяет в себе функции 4-х портового коммутатора, межсетевое экрана, маршрутизатора NAT и беспроводной точки доступа. Благодаря технологии 802.11n, маршрутизатор обеспечивает отличную зону покрытия сети и скорость передачи данных до 150 Мбит/с, что полностью отвечает требованиям сетей сегмента SOHO (для небольшого или домашнего офиса), а также требованиям пользователей, нуждающихся в более высокой производительности сети.

Беспроводной маршрутизатор модели **TD-W8950N** имеет встроенный трансивер ADSL2+ и высокоскоростной процессор MIPS. Устройство поддерживает полноскоростное подключение ADSL2+ в соответствии с техническими требованиями ITU и ANSI.

Помимо базовой функции физического DMT-уровня, протокол физического уровня ADSL2+ поддерживает двойной режим синхронизации dual latency ADSL2+ framing (быстрый и чередующийся) и физический уровень I.432 ATM.

Скорость беспроводной передачи данных достигает 150 Мбит/с для беспроводных клиентов стандарта 802.11n. Благодаря высокой скорости подключения устройство отлично подходит для одновременной обработки нескольких потоков данных, что способствует стабильности и высокой производительности сети. Стандарт 802.11n позволяет передавать данные по беспроводному соединению на 300% быстрее, чем по более старому стандарту 802.11g, кроме того, устройство поддерживает стандарты IEEE 802.11g и IEEE 802.11b.

Беспроводной маршрутизатор модели **TD-W8950N** обеспечивает полную конфиденциальность ваших данных с помощью нескольких функций защиты, которые включают в себя контроль широковещания SSID, 64/128-битное WEP-шифрование беспроводной локальной сети, защищённый доступ Wi-Fi (WPA2-PSK, WPA-PSK), а также дополнительную защиту с помощью меж сетевого экрана.

Гибкий контроль доступа позволяет родителям или сетевым администраторам устанавливать политику ограничения доступа для детей или сотрудников. Благодаря таким функциям переадресации как виртуальный сервер и узел DMZ можно управлять сетью и осуществлять её мониторинг в реальном времени как локально, так и удалённо.

Поскольку устройство поддерживает все наиболее популярные операционные системы, им легко и просто управлять. Можно воспользоваться Мастером быстрой настройки, кроме того, данное руководство содержит подробные пошаговые инструкции по настройке устройства. Перед установкой маршрутизатора рекомендуется ознакомиться с данным руководством, чтобы узнать обо всех его функциях.

1.2 Основные характеристики

- Поддержка стандарта IEEE 802.11n обеспечивает скорость беспроводной передачи данных до 150 Мбит/с

- Один порт LINE (RJ11), четыре порта LAN 10/100 Мбит/с (RJ45) с автосогласованием и с поддержкой авто-MDI/MDIX
- Надёжная и быстро реагирующая система защиты от скачков напряжения с помощью полупроводниковых элементов, установленных на основной схеме устройства.
- AFE для поддержки стандартов Annex A и L
- Внешний сплиттер в комплекте
- Совместный высокоскоростной доступ к Интернет для нескольких пользователей
- Подключение к Интернет по требованию и отключение после определённого времени простоя при использовании PPPoE-подключения
- Аутентификация WPA/WPA2, WPA-PSK/WPA2-PSK, шифрование TKIP/AES
- Защита с помощью 64/128/152-битного WEP-шифрования, список контроля доступа для беспроводной локальной сети
- Использование новейшей технологии DMT-модуляции и демодуляции
- Применяется технология передачи беспроводных данных до 150 Мбит/с
- Поддержка контроля доступа: родители и сетевые администраторы могут настраивать политику ограничения доступа по времени для детей или сотрудников
- Поддержка функций виртуального сервера, Port Triggering и узла DMZ
- Поддержка UPnP, динамического DNS, статической маршрутизации
- Поддержка режимов «мост» и «маршрутизатор»
- Настройка с помощью веб-утилиты через браузер
- Поддержка обновления встроенного ПО
- Поддержка статистики по потокам
- Встроенный межсетевой экран поддерживает фильтрацию IP-адресов, MAC-адресов и родительский контроль
- Встроенный DHCP-сервер
- Поддерживает Протокол IPv6
- Поддерживает Гостевую Сеть
- Поддерживает WPS
- Поддерживает IPTV

1.3 Описание панелей






1.3.1 Передняя панель


Светодиодные индикаторы расположены на передней панели (слева направо).



Рисунок 1-1

Обозначение индикаторов:

Название	Статус	Обозначение
 (Питание)	Горит	Питание маршрутизатора включено.
	Не горит	Питание отключено. Удостоверьтесь, что адаптер питания подключен правильным образом.
 (ADSL)	Горит	ADSL-линия синхронизирована и готова к работе.
	Мигает	Согласование ADSL в процессе.
	Не горит	Сбой ADSL синхронизации. Пожалуйста, обратитесь к Примечанию 1 для устранения неполадок.
 (Internet)	Горит	Подключение к Интернет успешно настроено.
	Мигает	Через Интернет происходит приём/отправка данных.
	Не горит	Подключение к Интернет не настроено либо маршрутизатор работает в режиме моста. Смотрите Примечание 2 для решения этой проблемы.
 (WLAN)	Горит	Беспроводное вещание включено, но передачи/приёма данных не происходит.
	Мигает	Происходит передача/приём данных по беспроводной сети.
	Не горит	Беспроводное вещание отключено.
 (WPS)	Горит	Беспроводное устройство было успешно подключено к сети посредством функции WPS.
	Медленно Мигает	Беспроводное устройство производит подключение к сети через функцию WPS этот процесс занимает примерно две минуты. Нажмите кнопку WPS на другом беспроводном устройстве, которое вы хотите добавить в сеть, пока мигает этот индикатор.
	Быстро Мигает	Не удалось подключить беспроводное устройство к сети посредством функции WPS. Более подробную информацию смотрите в разделе Настройки WPS .

 (LAN1-4)	Горит	К данному порту LAN подключено устройство, но оно неактивно.
	Мигает	Через данный порт LAN происходит приём/отправка данных.
	Не горит	К данному порту LAN не подключено устройство.

Примечание:

1. Если индикатор ADSL не горит, сначала проверьте ваше подключение к Интернет. Смотрите раздел [2.3 Подключение модем-маршрутизатора](#) для более подробной информации о том, как правильно подключиться к Интернет. Если вы уже настроили подключение к Интернет правильным образом, свяжитесь с вашим поставщиком Интернет-услуг и уточните, доступно ли подключение к Интернет данный момент.
2. Если не горит индикатор Internet, сначала проверьте, как работает индикатор ADSL. Если он тоже не горит, смотрите Примечание 1. Если индикатор ADSL горит, проверьте настройки подключения к Интернет. Возможно, что вам потребуется помощь вашего поставщика Интернет-услуг, чтобы проверить настройки Интернет и уточнить, что все параметры указаны правильно. Более подробная информация указана в разделе [4.2 Информации об установке](#).

1.3.2 Задняя панель

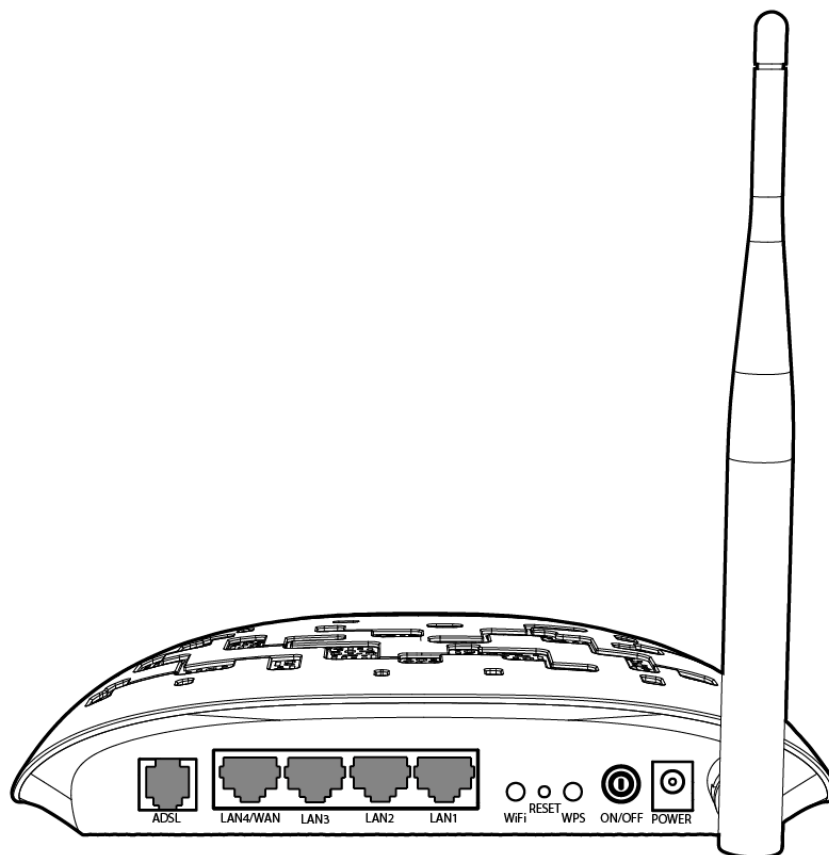


Рисунок 1-2

- **ADSL:** Подключается к порту Modem (Модем) сплиттера или к телефонной линии.

- **LAN4/WAN, LAN3, LAN2, LAN1:** Через эти порты маршрутизатор подключается к компьютеру или к иным сетевым Ethernet-устройствам. Включив функцию EWAN, вы сможете подключать кабельные/FTTH/VDSL/ADSL-устройства.
- **WiFi:** Включение беспроводного вещания.
- **RESET:** Есть два способа сброса параметров маршрутизатора и восстановления заводских настроек.
 - 1) Воспользуйтесь функцией восстановления заводских настроек в веб-утилите настройки маршрутизатора на странице **Управление – Настройки – Заводские настройки**.
 - 2) Воспользуйтесь кнопкой **RESET** на корпусе устройства: не отключая питания маршрутизатора, с помощью булавки нажмите кнопку **RESET** и удерживайте её нажатой не менее 5 секунд. Маршрутизатор перезагрузится и восстановит заводские настройки.
- **WPS:** Кнопка функции WPS. Более подробная информация указана в разделе [4.6.2.1 Настройки WPS](#).
- **ON/OFF:** Включение питания.
- **POWER:** Разъём для подключения адаптера питания.
- **Беспроводная антенна:** Служит для беспроводного получения и передачи данных.

Глава 2. Подключение маршрутизатора

2.1 Системные требования

- Широкополосный доступ в интернет (DSL/Cable/Ethernet).
- Компьютеры с работающими сетевыми адаптерами и сетевой кабель с разъемом RJ45.
- Поддержка протокола TCP/IP на каждом компьютере.
- Веб-браузер – Microsoft Internet Explorer, Mozilla Firefox или Apple Safari.

2.2 Требования к среде установки

- Маршрутизатор не должен подвергаться воздействию влаги или высоких температур.
- Размещайте маршрутизатор так, чтобы его можно было легко и удобно подключить к другим устройствам и к источнику питания.
- Следите за тем, чтобы кабели и шнур питания не находились под ногами и не создавали препятствия во избежание травмоопасных ситуаций.
- Устройство можно разместить на полке или на столе.
- Не размещайте устройство вблизи источников сильного электромагнитного излучения и вблизи устройств, чувствительных к электромагнитному излучению.

Как правило, TD-W8950N помещается на горизонтальной поверхности. . Устройство может быть размещено на стене (см Рисунок 2-1: Настенная установка).

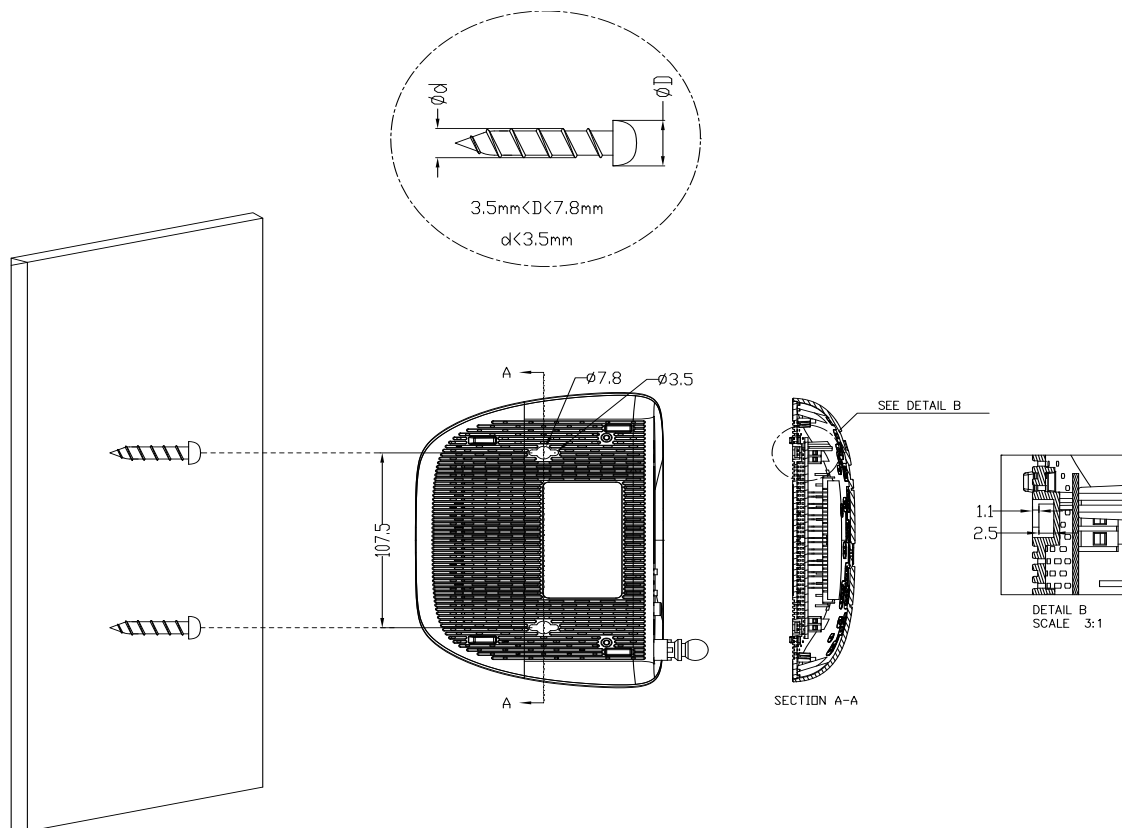


Рисунок 2-1: Настенная установка

☞ Примечание:

Диаметр шурупа: не более 4,1 мм, диаметр шляпки шурупа: не более 7,8 мм, расстояние между шурупами: 107,5 мм. Шуруп должен выступать из стены на 4 мм, длина самого шурупа должна быть не менее 20 мм, чтобы выдержать вес устройства.

2.3 Подключение маршрутизатора

Перед установкой маршрутизатора следует убедиться, что ваш компьютер имеет доступ к Интернет через широкополосное подключение. При возникновении проблем обратитесь к вашему поставщику Интернет-услуг. Перед подключением через кабель не забудьте отключить питание маршрутизатора со встроенным модемом, производите данные действия сухими руками. Следуйте изложенным ниже инструкциям.

Шаг 1: Подключите линию ADSL.

Способ первый: Один конец ADSL-кабеля подключите к порту ADSL на задней панели маршрутизатора **TD-W8950N**, другой конец подключите к соответствующему разъёму в стене.

Способ второй: Можно использовать отдельный сплиттер. Внешний сплиттер может разделять данные и голосовой трафик, то есть вы сможете иметь доступ к Интернет и одновременно с этим совершать телефонные звонки. У внешнего сплиттера есть три порта:

- **LINE:** подключается к разъёму в стене
- **PHONE:** подключается к телефонному аппарату
- **MODEM:** подключается к порту ADSL маршрутизатора **TD-W8950N**

Один конец ADSL-кабеля подключите к порту ADSL на задней панели маршрутизатора **TD-W8950N**, другой конец подключите к порту MODEM сплиттера.

Шаг 2: Подключите кабель Ethernet. Один конец сетевого кабеля подключите к порту Ethernet компьютера или к обычному порту концентратора/коммутатора, а другой конец – к порту LAN маршрутизатора **TD-W8950N**.

Шаг 3: Включите питание компьютеров или устройств локальной сети.

Подключите адаптер питания к разъёму питания (POWER) на задней панели устройства, затем подключите сам адаптер питания к электророзетке. Следите, чтобы электророзетка находилась рядом с устройством и была легкодоступна.

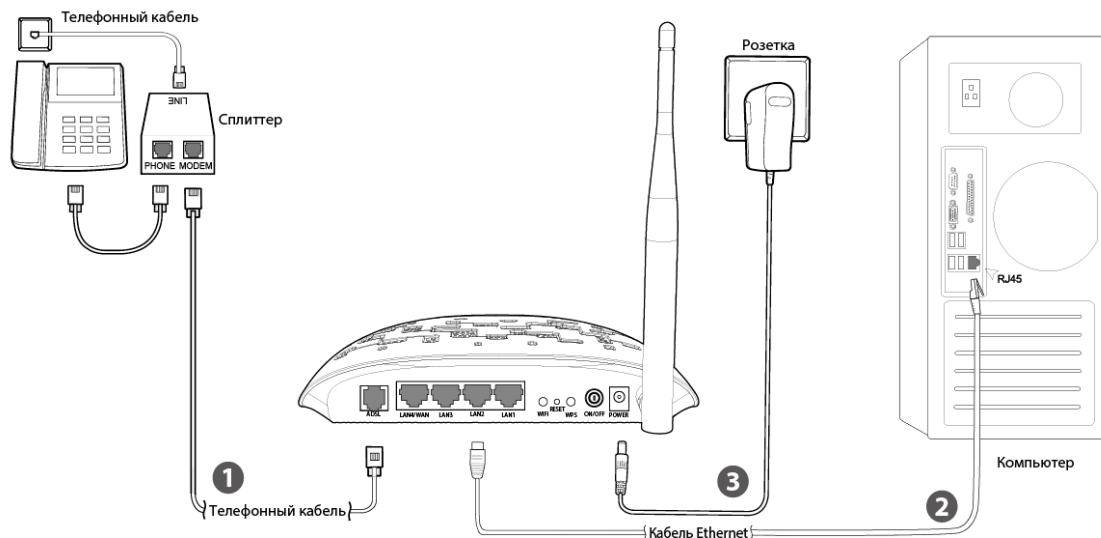


Рисунок 2-2

Глава 3. Руководство по быстрой настройке

В этой главе указаны инструкции о быстрой настройке основных параметров маршрутизатора **TD-W8950N** при помощи мастера быстрой настройки.

3.1 Настройка TCP/IP

IP-адресом по умолчанию для входа в веб-утилиту настройки **TD-W8950N** является 192.168.1.1. Маска подсети по умолчанию – 255.255.255.0. Эти параметры можно изменить на ваше усмотрение. В настоящем руководстве везде используются только значения по умолчанию.

Подключите компьютер локальной сети к одному из портов LAN/WAN маршрутизатора. После этого вы можете настроить IP-адрес для вашего компьютера следующим способом:

- Получить IP-адрес автоматически
 - 1) В настройках протокола TCP/IP вашего компьютера выберите **Получить IP-адрес автоматически**. Если вам необходимы инструкции, как это сделать, смотрите вопрос 3 в [Приложении В: Настройка компьютера](#).
 - 2) Встроенный DHCP-сервер назначит компьютеру IP-адрес.

Для проверки сетевого подключения между компьютером и маршрутизатором можно в командной строке ввести команду Ping. В меню **Пуск** выберите вкладку **Выполнить**, введите в строке **cmd** или **command** и нажмите **Enter**. В появившемся окне введите **ping 192.168.1.1**, затем нажмите **Enter**.

Если у вас результат как на рисунке ниже, это означает, что подключение между компьютером и маршрутизатором было установлено успешно.

```
Microsoft Windows [Version 6.1.7601]
(C) Copyright 2009 Microsoft Corporation.
C:\Documents and Settings\tplink>ping 192.168.1.1
Обмен пакетами с 192.168.1.1 по 32 байт:
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64
Статистика Ping для 192.168.1.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
    Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

Рисунок 3-1

Если у вас результат как на рисунке ниже, это означает, что подключение между компьютером и маршрутизатором отсутствует.

```

Microsoft Windows [Version 6.1.7601]
(C) Copyright 2009 Microsoft Corporation.

C:\Documents and Settings\tplink>ping 192.168.1.1

Обмен пакетами с 192.168.1.1 по 32 байт:

Аппаратный сбой.
Аппаратный сбой.
Заданный узел недоступен.
Заданный узел недоступен.

Статистика Ping для 192.168.1.1:
    Пакетов: отправлено = 4, получено = 0, потеряно = 4 (100% потерь),
    
```

Рисунок 3-2

Проверьте подключение следующим образом:

- 1) **Правильно ли подключен маршрутизатор к компьютеру?**
Индикаторы портов LAN, которые вы подключили к маршрутизатору и индикаторы адаптера компьютера должны гореть.
- 2) **Является ли правильной настройка TCP/IP на компьютере?**
Если IP-адрес маршрутизатора 192.168.1.1, то IP-адреса компьютеров должны лежать в диапазоне 192.168.1.2 – 192.168.1.254

3.2 Руководство по быстрой настройке

Маршрутизатор **TD-W8950N** легко настраивается и управляется с помощью веб-утилиты настройки. Веб-утилита может использоваться в любой ОС Windows, Macintosh или UNIX OS через веб-браузер (Microsoft Internet Explorer, Mozilla Firefox или Apple Safari).

Шаг 1: Чтобы войти в веб-утилиту настройки, откройте веб-браузер и введите адрес по умолчанию <http://tplinkmodem.net> в адресной строке браузера.



Рисунок 3-3

Появится окно входа в систему, аналогичное тому, как представлено на Рис. 3-4. В поле Пользователь и Пароль введите **admin**, используя нижний регистр. Затем нажмите кнопку **OK** или клавишу **Enter**.

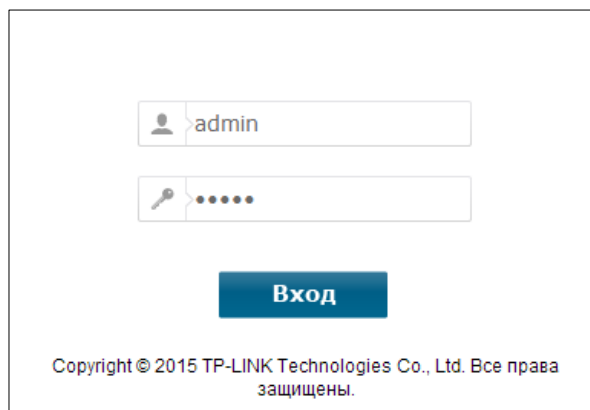


Рисунок 3-4

Примечание:

- 1) Не путайте имя доступа/пароль для входа в маршрутизатор с именем пользователя/паролем учётной записи ADSL для PPP-подключения.

- 2) Если данное окно не появилось, это означает, что ваш веб-браузер настроен на работу в режиме прокси. Зайдите в раздел **Свойства обозревателя – Подключения – Настройка параметров локальной сети**. В появившемся окне уберите галочку с ячейки **Использовать прокси-сервер для локальных подключений** и нажмите **ОК**.

Шаг 2: После успешного входа в систему, вы увидите страницу как на Рис. 3-5. Выберите в меню **Быстрая настройка** для доступа к **Мастеру быстрой настройки**.

Состояние	Устройство	
• Общая информация		
• WAN		
+ Статистика		
• Маршрутизация		
• ARP		
• DHCP		
Быстрая настройка		
Дополнительные настройки		
IPTV		
Беспроводной режим		
Гостевая сеть		
Диагностика		
Управление		
Выход		

Версия	
Версия встроенного ПО:	1.0.2 Build 150805 Rel.61680
Версия оборудования:	TD-W8950N V1 0x00000001
Время работы:	0Day(s) 00:21:42

LAN		
IPv4	LAN IP-адрес:	192.168.1.1
	LAN MAC-адрес:	02:10:18:63:18:08
IPv6	Длина префикса/IPv6-адреса:	NULL
	Автонастройка:	RADVD&DHCPv6

ADSL	
Состояние линии:	Низ
Исх. скорость линии (Кбит/с):	0
Вход. скорость линии (Кбит/с):	0

Интернет	
Примечание:	Интерфейс маршрута не задан.
Ярлык:	Нажмите здесь для быстрой настройки. Нажмите здесь для просмотра статусов всех интерфейсов WAN и информации по устранению неисправностей.

Рисунок 3-5

Шаг 3: Выберите **Тип WAN** для доступа в интернет, и нажмите **Далее**.

Быстрая настройка – Настройки WAN

Выберите тип подключения WAN для доступа к Интернет.

Выбран тип подключения WAN: ADSL WAN ADSL (телефонная линия/RJ11)

Ethernet WAN Ethernet (RJ45)

Включить IPv6 для данного подключения

Пропустить WAN
Далее

Рисунок 3-6

Примечание:

- 1) Мастер быстрой настройки поможет вам настроить службу WAN через ATM интерфейс.
- 2) Если у вас нет желания настраивать подключение WAN сейчас, можно нажать кнопку **Пропустить WAN**. Настройка подключения WAN указана в разделе [4.4.1 Интерфейс уровня 2](#).

Шаг 4: Если выбран **Режим маршрутизатора со встроенным ADSL-модемом**, необходимо выбрать **Страну** и **Поставщика Интернет-услуг** из выпадающего списка, а затем ввести соответствующие параметры, предоставленные вам вашим поставщиком Интернет-услуг. Затем нажмите **Далее**. Для примера используется PPPoE-подключение.

Быстрая настройка – Настройки WAN

Страна:	<input type="text" value="Russia"/>	▼	
Поставщик Интернет-услуг:	<input type="text" value="Other"/>	▼	
VPI/VCI:	<input type="text" value="0"/> / <input type="text" value="35"/>	([0-255] / [32-65535])	
Метод инкапсуляции:	<input type="text" value="LLC/SNAP-BRIDGING"/>	▼	(необязательно)

Тип подключения WAN:	<input type="text" value="PPPoE(PPP over Ethernet)"/>	▼	
PPP имя пользователя:	<input type="text"/>		
PPP пароль:	<input type="text"/>		
Имя PPPoE-сервиса:	<input type="text"/>		(необязательно)
Размер MTU (байт):	<input type="text" value="1480"/>		(необязательно)

Рисунок 3-7

Примечание:

Если в списке нет вашей страны или поставщика Интернет-услуг, выберите **Другое**. Затем вручную введите параметры VPI/VCI и выберите **Метод инкапсуляции**. Эти параметры указываются вашим поставщиком Интернет-услуг.

Если выбран **Режим беспроводного маршрутизатора**, вам необходимо выбрать **Тип подключения WAN**, предоставляемый вам вашим поставщиком Интернет-услуг, ввести необходимые параметры и нажать **Далее**. Для примера используется PPPoE-подключение.

Быстрая настройка – Настройки WAN

Ethernet WAN-порт: LAN4/WAN

Тип подключения WAN:

PPP имя пользователя:

PPP пароль:

Имя PPPoE-сервиса: (необязательно)

Размер MTU (байт): (необязательно)

Вторичное подключение: Отключено Динамический IP-адрес Статический IP-адрес (Для Dual Access)

Рисунок 3-8

Шаг 5: Функция беспроводного вещания включена по умолчанию. На этой странице вы можете указать новое имя беспроводной сети и создать свой собственный пароль. Имя беспроводной сети по умолчанию: TP-LINK_XXXX, а пароль беспроводной сети по умолчанию совпадает с PIN-кодом, эти данные указаны на нижней панели устройства. Нажмите **Далее** для продолжения .

Быстрая настройка – Беспроводной режим

Включить беспроводное вещание:

Вы можете указать SSID и тип аутентификации для беспроводной локальной сети.

Имя беспроводной сети: (Также называется SSID)

В целях защиты сети от хакеров и неавторизованных пользователей настоятельно рекомендуется выбрать один из указанных ниже типов защиты беспроводной сети.

Сетевая аутентификация:

Рисунок 3-9

6. Вы увидите экран **Завершение** ниже, нажмите кнопку **Подтвердить**, чтобы ваши настройки вступили в силу.

Быстрая настройка – Завершение

Настройки WAN

Тип подключения WAN:	ADSL WAN
Информация 2 уровня:	0/35 LLC/SNAP-BRIDGING
Тип подключения WAN:	PPPoE
PPP Имя пользователя:	123
PPP Пароль:	123
PPP размер MTU:	1480

Примечание 1: Некоторые WAN-соединения или интерфейсы 2 уровня могут быть заменены!

Примечание 2: Правила виртуального сервера некоторых WAN-соединений могут быть удалены!

Беспроводной режим

Имя беспроводной сети:	TP-LINK_1808
Сетевая аутентификация:	Открытая система (без защиты)

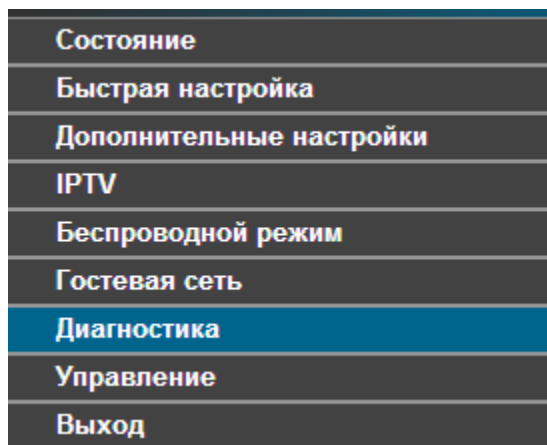
Рисунок 3-10

Глава 4. Настройка маршрутизатора

В этой главе рассказывается обо всех функциях веб-утилиты и способах настройки.

4.1 Вход

После успешного входа в маршрутизатор, вы увидите основное меню из 9 разделов, находящееся с левой стороны экрана. В правой части экрана содержится справочная информация и настройки.



Состояние
Быстрая настройка
Дополнительные настройки
IPTV
Беспроводной режим
Гостевая сеть
Диагностика
Управление
Выход

Ниже приводится подробная информация по всем основным функциям веб-утилиты.

4.2 Состояние

Меню **Состояние** содержит шесть разделов: **Общая информация**, **WAN**, **Статистика**, **Маршрутизация**, **ARP** и **DHCP**. В этом разделе содержится основная информация об устройстве и его текущих настройках. Выбрав какой-либо из подпунктов, можно посмотреть соответствующие настройки и информацию о работе устройства.

Выбрав в меню **Состояние – Общая информация**, вы увидите страницу как на Рисунок 4-1. В первой таблице указана информация о версии встроенного ПО и версии устройства. Во второй таблице отображается текущее состояние Интернет-подключения. Информация, отображаемая на данной странице, будет меняться в зависимости от параметров устройства, настроенных на странице **Дополнительные настройки**.

Устройство

Версия

Версия встроенного ПО:	1.0.2 Build 150805 Rel.61680
Версия оборудования:	TD-W8950N V1 0x00000001
Время работы:	0Day(s) 00:27:01

LAN

IPv4	LAN IP-адрес:	192.168.1.1
	LAN MAC-адрес:	02:10:18:63:18:08
IPv6	Длина префикса/IPv6-адреса:	NULL
	Автонастройка:	RADVD&DHCPv6

ADSL

Состояние линии:	Вниз
Исх. скорость линии (Кбит/с):	0
Вход. скорость линии (Кбит/с):	0

Интернет

Примечание:	Интерфейс маршрута не задан.
Ярлык:	Нажмите здесь для быстрой настройки. Нажмите здесь для просмотра статусов всех интерфейсов WAN и информации по устранению неисправностей.

Рисунок 4-1

👉 Примечание:

Выбрав другие разделы в меню **Состояние**, вы сможете посмотреть соответствующую информацию о **WAN**, статистике, маршрутизации, **ARP** и **DHCP**.

4.3 Быстрая настройка

Смотрите раздел [3.2 Руководство быстрой настройки](#).

4.4 Дополнительные настройки

Выберите меню **Дополнительные настройки**, которое содержит несколько разделов. Выбрав нужный вам раздел, можно настроить соответствующую функцию.

Дополнительные настройки
+ Интерфейс уровня 2
• WAN
• Клонирование MAC-адреса
+ LAN
+ NAT
+ Защита
+ Родительский контроль
+ Приоритезация данных
+ Контроль пропускной способности
+ Маршрутизация
+ DNS
• DSL
• UPnP
• Группировка портов
+ IP-туннель
• IPSec
• Multicast

Раздел **Дополнительные настройки** содержит вводную информацию о детальной настройке для наиболее рационального использования вашего маршрутизатора со встроенным модемом. Далее по тексту указаны подробные инструкции по каждому разделу меню **Дополнительные настройки**.

Примечание:

Чтобы полностью настроить WAN-интерфейс, вам сначала нужно выбрать **Интерфейс уровня 2** ([4.4.1 Интерфейс уровня 2](#)) в соответствии с типом подключения, который предоставлен вам вашим поставщиком Интернет-услуг, а затем вам необходимо выбрать тип подключения ([4.4.2 WAN](#)) для дальнейшей настройки.

4.4.1 Интерфейс уровня 2

Выберите **Дополнительные настройки – Интерфейс уровня 2**, и вы сможете выбрать интерфейс службы WAN (интерфейс уровня 2):

- **АТМ Интерфейс:** Настройка маршрутизатора для доступа в Интернет через ADSL. Интернет провайдер предоставляет вам VPI (Virtual Path Identifier), VCI (Virtual Channel Identifier) параметры и DSL кабель с разъемом RJ11. (Рисунок 4-2)
- **ЕТН Интерфейс:** Настройка маршрутизатора для доступа в Интернет через Ethernet. Интернет провайдер предоставляет вам услугу широкополосного доступа в интернет и Ethernet кабель с разъемом RJ45.

4.4.1.1 АТМ-Интерфейс

В меню **Дополнительные настройки – Интерфейс уровня 2 – АТМ Интерфейс** вы можете настроить АТМ интерфейсы (см. Рис. ниже).

Настройка интерфейса DSL ATM

Для настройки интерфейсов DSL ATM воспользуйтесь кнопками **Добавить** или **Удалить**.

Интерфейс	VPI	VCI	Тип подключения	Инкапсуляция	Категория	Пиковая скорость	Средняя скорость	Макс. Burst Size	Режим подключения	Приоритизация данных по IP-адресу	Установка очередности алгоритмически	Весовой коэффициент очереди	Приоритет группы	Удалить
atm0	8	35	EoA	LLC	UBR				FullSubcode	Включено	WRR	1	8	<input type="checkbox"/>

Рисунок 4-2

- **Удалить:** Отметьте данное поле в таблице (см. Рис. выше), затем нажмите кнопку **Удалить**. Соответствующий интерфейс будет удалён из таблицы.

Примечание:

Если данный интерфейс используется службой WAN, настройки которой указаны в разделе [4.4.2 WAN](#), то сначала необходимо отключить запись соответствующей службы WAN, а затем удалить интерфейс на данной странице.

- **Добавить:** После нажатия этой кнопки откроется страница (см. Рис. ниже), на которой можно добавить новый интерфейс.

Настройка ATM PVC

На данной странице вы можете настроить идентификатор ATM PVC (VPI и VCI), выбрать задержку DSL-линии и выбрать категорию обслуживания. В ином случае выберите существующий интерфейс, отметив соответствующее поле.

VPI: [0-255]

VCI: [32-65535]

Выберите Тип DSL-соединения (EoA для PPPoE, IPoE, и Мост)

EoA
 PPPoA
 IPoA

Метод инкапсуляции:

Категория обслуживания:

Выберите алгоритм планирования приоритизации данных по IP-адресу

Взвешенный циклический алгоритм
 Взвешенная справедливая очередь

Весовой коэффициент очереди по умолчанию: [1-63]

Приоритет MPAAL Group:

Рисунок 4-3

- **VPI/VCI:** Параметры VPI и VCI указываются вам вашим поставщиком Интернет-услуг. Эти параметры нельзя изменять, за исключением тех случаев, когда это требуется вашим поставщиком Интернет-услуг.
- **Тип DSL-соединения:** Выберите тип DSL-соединения, который вам предоставляется вашим поставщиком Интернет-услуг. Нужно выбрать либо **EoA** (для PPPoE, IPoE, и моста), либо **PPPoA** (PPP over ATM) или **IPoA** (IP over ATM).
- **Метод инкапсуляции:** Метод обработки данных через используемый вами тип соединения. Если вы не уверены, оставьте значение по умолчанию.
- **Категория обслуживания:** Выберите из выпадающего списка тип обслуживания, предоставленный вам вашим поставщиком Интернет-услуг. По умолчанию указано значение: **UBR без PCR**.

👉 Примечание:

Если включить приоритезацию данных уровня пакетов для постоянного виртуального канала (PVC), улучшится производительность выбранных классов приложений. Поскольку функция приоритезации данных потребляет системные ресурсы, количество постоянных виртуальных каналов будет уменьшено. Данная функция не может быть включена для типа подключения CBR и VBR в реальном времени. Если вы выберете функцию приоритезации данных, в веб-утилите настройки появится меню Приоритезация данных. Подробная настройка описана в разделе [4.4.8 Приоритезация данных](#).

4.4.1.2 ETH-Интерфейс

В меню **Дополнительные настройки – Интерфейс уровня 2 – Интерфейс ETH**, вы можете настроить интерфейсы ETH WAN интерфейсы (см. Рис. ниже).

Настройка ETH WAN-интерфейса

Для настройки ETH WAN-интерфейсов воспользуйтесь кнопками **Добавить** или **Удалить**.
Разрешить один ETH в качестве WAN-интерфейса уровня 2.

Интерфейс/(Имя)	Режим подключения	Удалить

Рисунок 4-4

👉 Примечание:

Чтобы убедиться, что порт ETH доступен, вы должны сперва выбрать **Дополнительные настройки – Порты LAN** чтобы включить свойство портов Virtual LAN.

- **Добавить:** Нажмите кнопку **Добавить**, и вы можете добавить новый интерфейс в следующем окне.

Настройка ETH WAN

На этой странице вы сможете настроить порт ETH.

Выберите порт ETH:

Рисунок 4-5

- **Выберите порт ETH:** Выберите порт ETH для настройки в качестве порта WAN.

Нажмите кнопку **Сохранить/Принять**, чтобы сохранить настройки, и затем вы увидите окно аналогичное Рисунок 4-6.



Рисунок 4-6

- **Удалить:** Отметьте данное поле в таблице (см. Рис. выше), затем нажмите кнопку **Удалить**. Соответствующий интерфейс будет удален из таблицы.

Примечание:

Один порт ETH разрешен для настройки как интерфейс WAN уровня 2.

4.4.2 WAN

Выберите **Дополнительные настройки – WAN**. На этой странице вы увидите информацию про порт WAN в таблице (см. Рисунок 4-7), в которой указаны настройки WAN и соответствующие действия для каждого интерфейса. После того как вы добавите новый интерфейс уровня 2, следуйте указанным ниже инструкциям, чтобы завершить полную настройку WAN-интерфейса. Для типов подключения имеется пять разных настроек (PPPoE, IPoE, Мост, PPPoA и IPoA). Выберите нужный вам вариант.



Рисунок 4-7

Примечание:

В следующем разделе используются другие значения VPI/VCI для того, чтобы показать настройку для разных типов подключения. Если вам нужно изменить настройки ATM PVC (VPI/VCI), вам следует перейти в предыдущий раздел ([4.4.1 Интерфейс уровня 2](#)), чтобы снова их настроить.

4.4.2.1 ATM-EoA-PPPoE

Если ваш поставщик Интернет-услуг предоставляет вам **PPPoE**-подключение и вам необходимо использовать ATM-интерфейс, следуйте нижеуказанным инструкциям для добавления WAN-сервиса поверх выбранного ATM-интерфейса:

1. Добавьте **новый** ATM-интерфейс и выберите параметр **EoA** для Типа DSL-соединения ([4.4.1.1 Интерфейс ATM](#)).
2. Нажмите **Добавить** (см. Рисунок 4-7), вы попадёте на страницу как на Рисунок 4-8. Нажмите **Далее**.

Настройка интерфейса подключения WAN

Выберите интерфейс уровня 2 для данного устройства

Примечание: Для вывода параметров ATM-интерфейса используется команда: portId_vpi_vci

Интерфейс уровня 2:

Назад

Рисунок 4-8

3. Выберите **Тип подключения WAN** (см. Рисунок 4-9). Если поставщик Интернет-услуг предоставляет вам PPPoE-подключение, выберите **PPPoE**. Вы можете указать имя сервиса в поле **Описание подключения** либо оставить значение по умолчанию. Нажмите **Далее**.

Настройка подключения WAN

Выберите тип подключения WAN:

PPP over Ethernet (PPPoE)

IP over Ethernet

Мост

Укажите описание подключения:

Для тегированного подключения введите правильный приоритет 802.1P и 802.1Q VLAN ID.
Для не тегированного подключения укажите -1 для 802.1P и для 802.1Q VLAN ID.

Введите приоритет 802.1P [0-7]:

Введите 802.1Q VLAN ID [0-4094]:

Выбор сетевого протокола:

Назад

Рисунок 4-9

4. Укажите следующие параметры и нажмите **Далее**.

PPP имя пользователя и пароль

Для PPP-соединения необходимо указать имя пользователя и пароль. В полях ниже укажите имя пользователя и пароль от вашего поставщика Интернет-услуг.

PPP имя пользователя:	<input style="width: 60%;" type="text" value="1234567890"/>
PPP пароль:	<input style="width: 60%;" type="password" value="••••••"/>
Имя PPPoE-сервиса:	<input style="width: 60%;" type="text"/>
Метод аутентификации:	<input style="width: 60%;" type="text" value="АВТО"/>
Размер MTU (байт):	<input style="width: 60%;" type="text" value="1480"/> (Значение по умолчанию: 1480. Не изменять без необходимости.)

- Включить NAT
- Включить Full Cone NAT
- Подключить по требованию (используя счётчик времени простоя)
- PPP IP-расширение
- Использовать статический IPv4-адрес
- Включить режим отладки PPP
- Объединять в мост кадры PPPoE между портами WAN и LAN

Multicast Proxy

- Включить IGMP Multicast Proxy

Рисунок 4-10

- **PPP имя пользователя/пароль:** Введите имя пользователя и пароль, предоставленные вам вашим поставщиком Интернет-услуг. Эти поля чувствительны к регистру.
- **Имя PPPoE-сервиса:** Введите имя сервиса, если оно было предоставлено вашим поставщиком Интернет-услуг. Если оставить это поле незаполненным, то по умолчанию там будет указано то же самое имя, которое было введено в поле **Описание подключения** на предыдущей странице.
- **Метод аутентификации:** Выберите **Метод аутентификации** из выпадающего списка, по умолчанию указано **АВТО**, можно оставить по умолчанию.

👉 **Примечание:**

Если вы не уверены насчёт параметров **PPP IP-расширение** и **Режим отладки PPP** и прочих, указанных ниже настроек, не трогайте их.

- **Размер MTU:** Максимальный размер пакета передаваемых данных. Отметьте это поле, и вы сможете изменять данный параметр. Размер **MTU** по умолчанию составляет 1480 байт. Не рекомендуется изменять это значение за исключением случаев, когда это требуется вашим поставщиком Интернет-услуг.
- **Включить Full cone NAT:** Это тип NAT, если данный параметр не выбран, будет работать NAT по умолчанию.
- **Подключить по требованию (используя счётчик времени простоя):** Маршрутизатор со встроенным модемом разорвёт соединение с Интернет после определённого периода неактивности (время простоя) и автоматически восстановит подключение сразу, как только вы снова попытаетесь выйти в Интернет. Эту опцию можно выбрать, если у вас не безлимитный доступ к Интернет, и вы хотите сэкономить деньги.
- **PPP IP-расширение:** Выберите эту опцию, чтобы ваш компьютер получил публичный IP-адрес от PPP-сервера, а NAT и межсетевой экран SPI были закрыты. Это похоже на мост с PPP-подключением через ваш маршрутизатор со встроенным модемом. Это особая функция, которая используется некоторыми поставщиками Интернет-услуг. Не

выбирайте эту опцию, если ваш поставщик Интернет-услуг не требует этого от вас.

- **Использовать статический адрес IPv4:** Если ваш поставщик Интернет-услуг предоставляет вам статический **IP-адрес WAN, Шлюза и DNS-сервера**, выберите эту опцию для ручного ввода указанных параметров.
 - **Включить режим отладки PPP:** Выберите данную опцию для отладки функции PPP и вы увидите информацию журнала PPP в Системном журнале. Режим отладки есть только для PPP-подключения.
 - **Объединять в мост кадры PPPoE между портами WAN и LAN:** Выберите эту опцию, чтобы начать PPP-подключение на локальном компьютере.
 - **Включить IGMP Multicast Proxy:** IGMP (протокол управления группами Интернета) используется для управления multicast-передачей данных по сетям TCP/IP. Некоторые поставщики Интернет-услуг используют IGMP для удалённой настройки удалённых клиентов, например, маршрутизаторов. По умолчанию эта функция отключена. Если вы не разбираетесь в настройках данной функции, оставьте значение по умолчанию или свяжитесь с вашим поставщиком Интернет-услуг.
5. Выберите предпочтительный WAN-интерфейс в качестве основного шлюза системы (см. Рис. 4-11) и нажмите **Далее**.

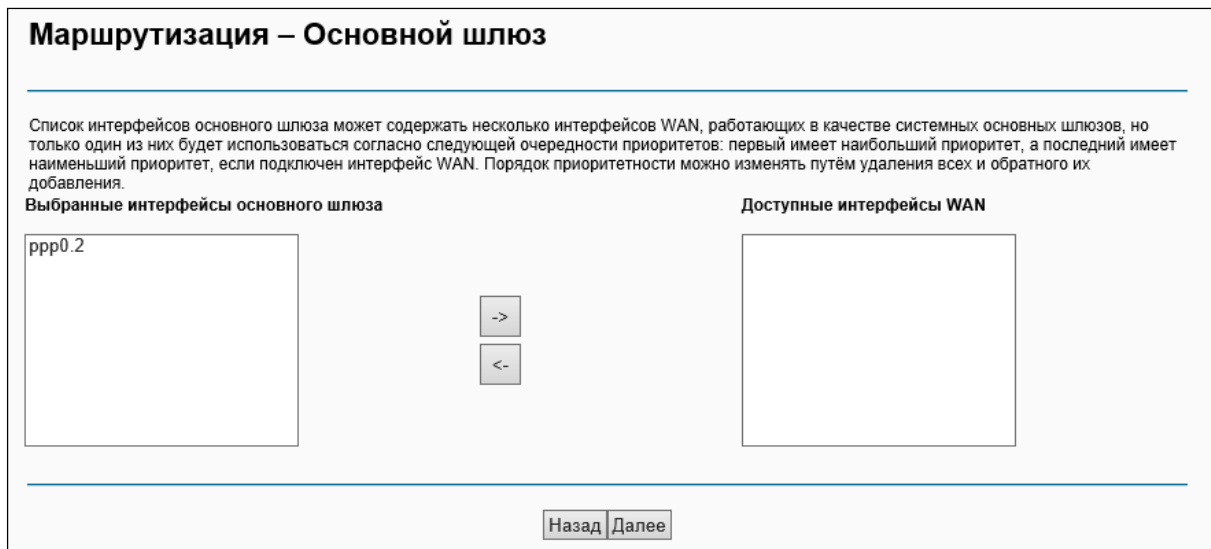


Рисунок 4-11

6. Настройте адреса DNS-серверов на странице, которая указана ниже, и нажмите **Далее**.

Настройка DNS-сервера

Выберите интерфейс DNS-сервера из доступных интерфейсов WAN или введите статический IP-адрес DNS-сервера для системы. Если в режиме ATM (асинхронный способ передачи данных) настроен только один постоянный виртуальный канал с IPoA или статический IPoE-протокол, необходимо указать статический IP-адрес DNS-сервера.
Интерфейсы DNS-сервера могут иметь несколько интерфейсов WAN , работающих в качестве системных DNS-серверов, но только один из них будет использоваться из расчёта, что первый имеет наибольший приоритет, а последний имеет наименьший приоритет, если подключен интерфейс WAN. Порядок приоритетности можно изменять путём удаления всех и обратного их добавления.

Выбрать интерфейс DNS-сервера из доступных интерфейсов WAN:

Выберите интерфейсы DNS-серверов Доступные WAN-интерфейсы

ppp0.2

Использовать следующий статический IP-адрес DNS-сервера:

Предпочитаемый DNS-сервер:

Альтернативный DNS-сервер:

Рисунок 4-12

- **Выбрать интерфейс DNS-сервера из доступных WAN-интерфейсов:** Выберите эту опцию для автоматического получения информации о DNS-серверах от выбранного WAN-интерфейса.
- **Использовать следующий статический IP-адрес DNS-сервера:** Выберите данную опцию, чтобы ввести вручную IP-адреса предпочитаемого и альтернативного DNS-серверов, предоставленных вашим поставщиком Интернет-услуг.

👉 Примечание:

Если настроен только один постоянный канал (PVC) с IPoA, необходимо ввести статический IP-адрес DNS-сервера.

7. На следующей странице будут подробно указаны сделанные вами настройки. Нажмите **Сохранить/Применить** для сохранения этих настроек.

Настройка WAN – Завершение

Убедитесь, что настройки соответствуют параметрам, предоставленным вашим поставщиком Интернет-услуг.

Тип подключения:	PPPoE
NAT:	Включено
Full Cone NAT:	Отключить
Межсетевой экран:	Включено
IGMP Multicast:	Включено
Приоритезация данных:	Включено

Нажмите "Сохранить/Применить", чтобы данный интерфейс использовался. Нажмите "Назад", чтобы вернуться назад и указать параметры настроек.

Рисунок 4-13

8. На следующей странице вы увидите таблицу с информацией о настройках порта WAN.

Настройка WAN

Для настройки подключения WAN на выбранном интерфейсе воспользуйтесь кнопками **Добавить**, **Изменить** или **Удалить**.

Интерфейс	Описание	vТип	Vlan8021p	VlanMuxId	Igmp	NAT	Межсетевой экран	IPv6	Mld	Удалить	Изменить
atm0.1	br_0_8_35	Bridge	N/A	N/A	включено	отключено	отключено	отключено	отключено	<input type="checkbox"/>	<input type="button" value="Изменить"/>
ppp0.2	pppoe_0_8_35	PPPoE	N/A	N/A	включено	включено	включено	отключено	отключено	<input type="checkbox"/>	<input type="button" value="Изменить"/>

Рисунок 4-14

- **Удалить все:** Нажмите **Удалить все** для удаления всех интерфейсов из таблицы.
- **Удалить:** Отметьте данное поле, затем нажмите кнопку **Удалить** для удаления соответствующего интерфейса из таблицы.

4.4.2.2 ATM-EoA-IPoE

Если ваш поставщик Интернет-услуг предоставляет вам **IPoE**-подключение и вам надо использовать ATM-интерфейс, следуйте указанным ниже инструкциям для добавления WAN-сервиса поверх выбранного ATM-интерфейса:

1. Добавьте **новый** ATM-интерфейс и выберите параметр **EoA** для типа DSL-соединения ([4.4.1.1 Интерфейс ATM](#)).
2. Нажмите кнопку **Добавить** на странице, как на Рисунке 4-7. Выберите интерфейс WAN-сервиса поверх ATM PVC (см. 12).
3. Если ваш поставщик Интернет-услуг предоставляет вам IPoE-подключение, выберите **IPoE** для **Типа подключения WAN** (см. Рисунок 4-9), нажмите **Далее** для продолжения.
4. Введите параметры в указанные ниже поля для настройки WAN IP-адреса и нажмите **Далее**.

WAN IP-адрес

Введите параметры, предоставленные вам вашим поставщиком Интернет-услуг для настройки WAN IP-адреса.
 Примечание: Если выбрано "Получить IP-адрес автоматически", будет включен DHCP для постоянного виртуального канала в режиме IPoE. Если выбрано "Использовать следующий статический IP-адрес", необходимо ввести WAN IP-адрес, маску подсети и шлюз интерфейса.

Получить IP-адрес автоматически

ID изготовителя (опция 60):

IAID опция 61: (8 шестнадцатеричных чисел)

DUID опция 61: (8 шестнадцатеричных чисел)

Опция 125: Отключить Включить

Использовать следующий статический IP-адрес:

WAN IP-адрес:

Маска подсети WAN:

IP-адрес шлюза WAN:

Размер MTU (байт): (необязательно)

Рисунок 4-15

- **Получить IP-адрес автоматически:** Если выбрать данную опцию, то маршрутизатор сможет получить IP-параметры сети динамически от DHCP-сервера от поставщика Интернет-услуг.

 **Примечание:**

- 1) Ответное сообщение от DHCP-сервера, как правило, содержит ряд параметров настройки (опция DHCP) для маршрутизатора. Опция DHCP включает IP-параметры сети и конкретные параметры изготовителя. В некоторых случаях маршрутизатор со встроенным модемом выполняет операции, настроенные пользователем (как показано ниже). Вы сами можете решать, как те или иные опции будут работать.
 - 2) Если маршрутизатор работает как DHCP-клиент, то он должен определить сам себя в опции 61 (клиент-идентификатор) в каждом сообщении от DHCP-сервера. DUID/IAID – это часть опции 61.
 - **Опция ID изготовителя (опция 60):** Опция с кодом 60, используемая для определения класса изготовителя.
 - **IAID опция 61:** IAID (Identity Association ID – опознавательный идентификатор) назначает опознавательный идентификатор каждому интерфейсу в отдельности. Если устройство работает с одним идентификатором DHCP-клиента, необходимо использовать значение 1 для IAID для всех DHCP-взаимодействий. Если устройство работает с несколькими идентификаторами DHCP-клиента, значение параметра IAID начинаются с 1 для первого идентификатора и возрастает для последующих идентификаторов. Например, устройство использует IAID со значением 1 для первого физического интерфейса и 2 – для второго. В дополнение к вышесказанному, устройство может использовать IAID со значением 1 для виртуального маршрута, что будет соответствовать первому объекту в модели данных, с которым будет происходить соединение, а значение 2 будет соответствовать второму объекту в модели данных, с которым будет происходить соединение.
 - **DUID опция 61:** Указывает имя интерфейса, адрес канального уровня (link-layer address) которой используется сервером в качестве её DUID (уникальный идентификатор DHCP). Необходимо указать значение для этого параметра, иначе сервер не начнёт работать. Когда сервер начнёт работать, DUID будет занесён в системный журнал.
 - **Опция 125:** Опция 125 позволяет обеспечивать предварительную настройку DHCP-сервера с такой политикой для управляющих классов, что можно обойтись без DHCP-сервера, чтобы прочитать уникальный формат, используемый в опции клиент-идентификатор.
- **Использовать следующий статический IP-адрес:** Если вам предоставили статический IP-адрес/шлюз, выберите эту опцию, а затем вручную введите **WAN IP-адрес, Маску подсети WAN и IP-адрес шлюза WAN**.
5. Далее вы попадёте на страницу как на Рис. ниже. Можно включить **NAT, Межсетевой экран SPI и IGMP Multicast**. Если вы не разбираетесь в данных настройках, оставьте параметры по умолчанию. Нажмите **Далее**.

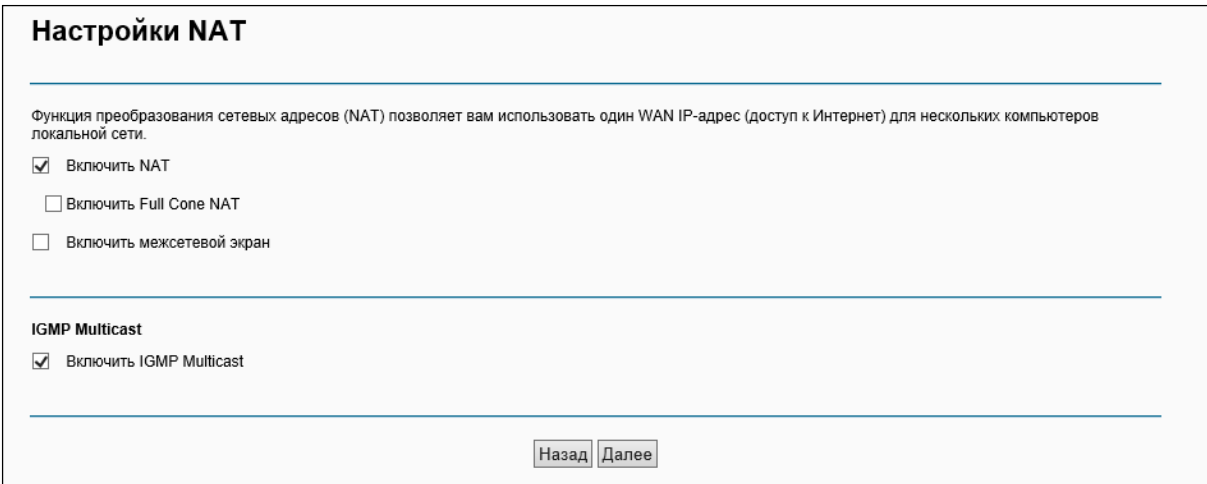


Рисунок 4-16

- **Включить NAT:** Данная технология транслирует IP-адреса локальной сети в другие IP-адреса для выхода в Интернет. Если ваш маршрутизатор осуществляет подключение вашей локальной сети к Интернет, нужно выбрать эту опцию. Если в вашей сети имеется ещё один маршрутизатор, вам не нужно выбирать эту опцию.
- **Включить межсетевой экран:** Межсетевой экран SPI увеличивает защиту сети. Выберите эту опцию для использования меж сетевого экрана.
- **Включить IGMP Multicast:** По умолчанию данная опция отключена. Эта опция не позволяет перенаправлять IGMP-пакеты (IGMP – протокол управления группами Интернета) в локальную сеть. IGMP используется, чтобы управлять multicast-передачей данных по сетям TCP/IP. Большинству пользователей эта настройка не нужна. Некоторые поставщики Интернет-услуг используют IGMP для удалённой настройки клиентских устройств (например, маршрутизаторов). Если вы не уверены, как настраивать эту опцию, свяжитесь с вашим поставщиком Интернет-услуг.

👉 Примечание:

Если отметить строку **Включить NAT**, в веб-утилите настройки появится меню **NAT**. Подробная настройка NAT указана в разделе [4.4.5 NAT](#).

6. Выберите предпочитаемый **WAN**-интерфейс в качестве основного шлюза системы и нажмите **Далее**.

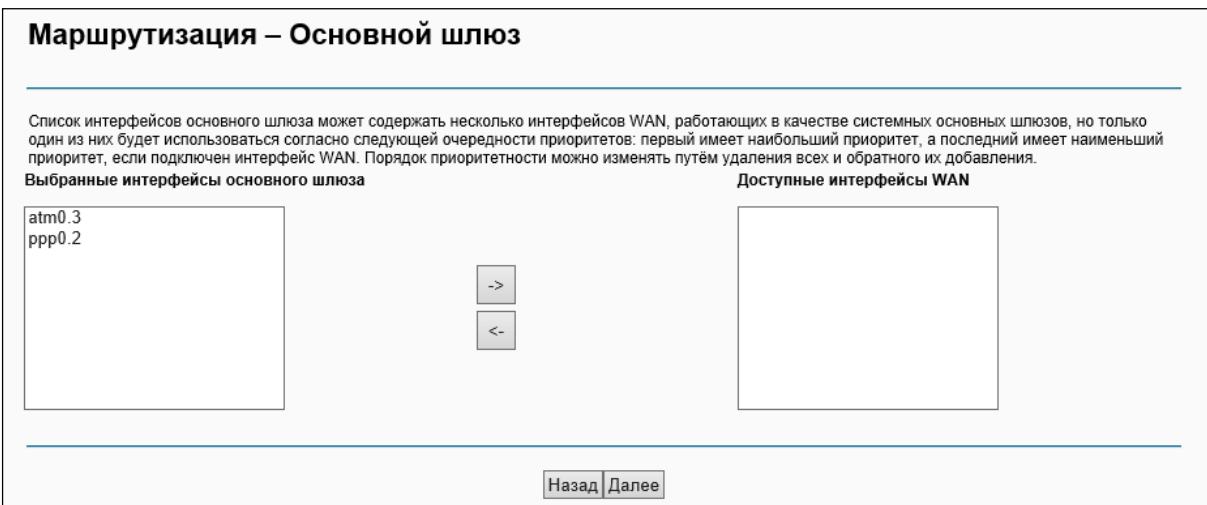


Рисунок 4-17

7. На странице, которая показана ниже, введите адреса DNS-серверов.

Настройка DNS-сервера

Выберите интерфейс DNS-сервера из доступных интерфейсов WAN или введите статический IP-адрес DNS-сервера для системы. Если в режиме ATM (асинхронный способ передачи данных) настроен только один постоянный виртуальный канал с IPoA или статический IPoE-протокол, необходимо указать статический IP-адрес DNS-сервера.
Интерфейсы DNS-сервера могут иметь несколько интерфейсов WAN, работающих в качестве системных DNS-серверов, но только один из них будет использоваться из расчёта, что первый имеет наибольший приоритет, а последний имеет наименьший приоритет, если подключен интерфейс WAN. Порядок приоритетности можно изменять путём удаления всех и обратного их добавления.

Выбрать интерфейс DNS-сервера из доступных интерфейсов WAN:

Выберите интерфейсы DNS-серверов Доступные WAN-интерфейсы

atm0.3
ppp0.2

->

<-

Использовать следующий статический IP-адрес DNS-сервера:

Предпочитаемый DNS-сервер:

Альтернативный DNS-сервер:

Рисунок 4-18

Примечание:

Если настроен только один постоянный канал (PVC) с IPoA, необходимо ввести статический IP-адрес DNS-сервера.

8. На следующей странице (Рисунок 4-19) вы увидите подробную информацию о сделанных вами настройках. Нажмите **Применить/Сохранить** для сохранения этих настроек.

Настройка WAN – Завершение

Убедитесь, что настройки соответствуют параметрам, предоставленным вашим поставщиком Интернет-услуг.

Тип подключения:	IPoE
NAT:	Включено
Full Cone NAT:	Отключить
Межсетевой экран:	Отключить
IGMP Multicast:	Включено
Приоритезация данных:	Отключить

Нажмите "Сохранить/Применить", чтобы данный интерфейс использовался. Нажмите "Назад", чтобы вернуться назад и указать параметры настроек.

Рисунок 4-19

4.4.2.3 ATM-EoA-Мост

Если вы хотите использовать тип подключения **Мост** и вам нужно использовать ATM-интерфейс, следуйте указанным ниже инструкциям для добавления WAN-сервиса поверх ATM-интерфейса:

1. Добавьте новый ATM-интерфейс и выберите **ЕоА** для типа DSL-соединения (см. раздел [4.4.1.1 ATM Интерфейс](#)).
2. Нажмите кнопку **Добавить** (см. Рисунок 4-7). Выберите WAN-интерфейс поверх ATM PVC (см. Рисунок 4-8).
3. Выберите **Мост** в качестве **Типа подключения WAN** (см. Рисунок 4-9), затем нажмите **Далее** для продолжения.
4. На странице, которая показана на Рисунке 4-13, вы увидите подробную информацию о сделанных вами настройках. Нажмите **Применить/Сохранить** для сохранения этих настроек.

4.4.2.4 ATM-PPPoA

Если ваш поставщик Интернет-услуг предоставляет **PPPoA**-подключение и вам нужно использовать ATM-интерфейс, следуйте указанным ниже инструкциям для добавления WAN-интерфейса поверх выбранного ATM-интерфейса:

1. Добавьте новый ATM-интерфейс и выберите вариант **PPPoA** для типа DSL-соединения (см. раздел [4.4.1.1 ATM Интерфейс](#)).
2. Нажмите кнопку **Добавить** на странице, как на Рисунке 4-7. Дальнейшая настройка точно такая же как для **PPPoE** (см. раздел [4.4.2.1 ATM-ЕоА-PPPoE](#)). Разница в том, что вам не нужно указывать **Имя PPPoE-сервиса** и **Объединять в мост кадры PPPoE между портами WAN и LAN** на странице, как на Рисунке 4-10.

4.4.2.5 ATM-IPoA

Если ваш поставщик Интернет-услуг предоставляет вам **IPoA**-подключение и вам надо использовать ATM-интерфейс, следуйте указанным ниже инструкциям для добавления WAN-сервиса поверх выбранного ATM-интерфейса:

1. Добавьте новый ATM-интерфейс и выберите параметр **IPoA** для типа DSL-соединения (см. раздел [4.4.1.1 ATM Интерфейс](#)).
2. Нажмите кнопку **Добавить** на странице, как на Рисунке 4-7. Дальнейшая настройка точно такая же как для **IPoE** (см. раздел [4.4.2.2 ATM-ЕоА-IPoE](#)). Разница в том, что вам нужно вручную указать статический IP-адрес на странице, как на Рисунке 4-15, а также статический IP-адрес DNS-сервера на странице, как на Рисунке 4-18.

Примечание:

ETH- и ATM-сервисы нельзя использовать одновременно. Если ATM-интерфейс был настроен, вы не сможете настроить другой WAN-сервис поверх ETH-интерфейса, пока не удалён ATM-интерфейс.

4.4.2.6 ETH-PPPoE

Если ваш поставщик Интернет-услуг предоставляет вам **PPPoE**-подключение и вам надо использовать ETH-интерфейс, следуйте указанным ниже инструкциям для добавления WAN-сервиса поверх выбранного ETH-интерфейса:

1. Добавьте новый ETH-интерфейс на экране [4.4.1.2 ETH-Интерфейс](#).
2. Нажмите кнопку **Добавить** (см. Рисунок 4-7). Дальнейшая настройка точно такая же как для **PPPoE поверх ATM-интерфейса** (см. раздел [4.4.2.1 ATM-ЕоА-PPPoE](#)).

4.4.2.7 ETH-IPoE

Если ваш поставщик Интернет-услуг предоставляет вам **PPPoE**-подключение и вам надо использовать ETH-интерфейс, следуйте указанным ниже инструкциям для добавления WAN-сервиса поверх выбранного ETH-интерфейса:

1. Добавьте новый ЕТН-интерфейс на экране [4.4.1.2 ЕТН-Интерфейс](#).
2. Нажмите кнопку **Добавить** (см. Рисунок 4-7). Дальнейшая настройка точно такая же как для **IPoE поверх** АТМ-интерфейса (см. раздел [4.4.2.2 АТМ-ЕоА-IPoE](#)).

4.4.3 Клонирование MAC-адреса

В меню на странице **Дополнительные настройки – Клонирование MAC-адреса** доступны настройки MAC-адреса для WAN-интерфейса (см. Рис. ниже).

В списке WAN-интерфейсов находятся интерфейсы уровня 2, настройка которых указана в разделе [4.4.1 Интерфейс уровня 2](#), и их MAC-адрес по умолчанию. Если вы не настроили соответствующий WAN-сервис в разделе [4.4.2 WAN](#), в поле MAC-адреса будет указано “Необходим соответствующий WAN-сервис”.

Текущий адрес вашего компьютера указывается последним в списке WAN-интерфейсов.

Клонировать MAC-адрес

Укажите MAC-адрес для выбранного WAN-сервиса.

Клонировать MAC-адрес для ppp0.2:	Не настроен	Восстановить MAC-адрес
Текущий MAC-адрес компьютера:	74:d4:35:9f:d8:b0	Клонировать в ppp0.2 ▾

Примечание: Использовать функцию клонирования MAC-адреса можно только для портов WAN. Клонированные MAC-адреса НЕ ДОЛЖНЫ совпадать!

Рисунок 4-20

Введите новое значение для WAN-интерфейса, MAC-адрес которого вы хотите изменить.

Можно выбрать соответствующий WAN-интерфейс из выпадающего списка и нажать кнопку **Клонировать** для клонирования текущего MAC-адреса вашего компьютера.

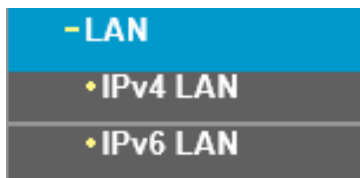
Кнопка **Восстановить MAC-адрес** служит для восстановления MAC-адреса WAN-интерфейса по умолчанию.

Примечание:

Функция клонирования MAC-адреса применима только к порту WAN маршрутизатора. Клонированные MAC-адреса не должны совпадать.

4.4.4 LAN

В меню на странице **Дополнительные настройки – LAN** можно настроить параметры локальной сети, а также настроить **LAN IPv4-адрес** и **LAN IPv6-адрес**.



4.4.4.1 Настройка IPv4 LAN

В меню на странице **Дополнительные настройки – LAN – IPv4 LAN** доступны настройки локальной сети (см. Рисунок 4-21), здесь можно настроить LAN IPv4-интерфейс вашего маршрутизатора со встроенным модемом.

Локальная сеть (LAN)/Настройка Настройка

Настройте IP-адрес маршрутизатора с модемом DSL и маску подсети для интерфейса. Имя группы

IP-адрес:
Маска подсети:

Включить IGMP Snooping

Стандартный режим
 Режим блокировки

Отключить DHCP-сервер
 Включить DHCP-сервер

Начальный IP-адрес:
Конечный IP-адрес:
Время аренды (часы): (1~48)

Список арендуемых IP-адресов:: (Можно указать не более 32 записей)

MAC-адрес	IP-адрес	Состояние	Включить/Отключить	Изменить	Удалить
<input type="button" value="Добавить"/> <input type="button" value="Включить все"/> <input type="button" value="Выбрать все"/> <input type="button" value="Удалить"/>					

Включить ретрансляцию DHCP-сервера
IP-адрес DHCP-сервера:

Примечание: Необходимо отключить NAT для WAN-соединений, иначе ретрансляция DHCP-сервера не будет работать!

Настройте второй IP-адрес и маску подсети для интерфейса LAN

Рисунок 4-21

- **IP-адрес:** Вы можете указать IP-адрес и маску подсети LAN-интерфейса вашего маршрутизатора.
 - **IP-адрес:** Введите локальный IP-адрес маршрутизатора, после чего вы сможете заходить в веб-утилиту настройки маршрутизатора с помощью этого IP-адреса, по умолчанию указано 192.168.1.1
 - **Маска подсети:** Введите маску подсети вашего маршрутизатора, по умолчанию указано 255.255.255.0
- **Включить IGMP Snooping:** Если вы выберете эту опцию, необходимо будет выбрать режим IGMP: Стандартный режим или Режим блокировки.
- **DHCP-сервер:** Вы можете настроить параметры работы DHCP-сервера маршрутизатора (DHCP – протокол динамической настройки узла). DHCP-сервер маршрутизатора включен по умолчанию и предоставляет службу DHCP-сервера через порт LAN. DHCP-сервер предоставляет параметры IP компьютерам, которые подключены к маршрутизатору через Ethernet-порт и в настройках которых указано, чтобы они получали IP-адреса автоматически. Если маршрутизатор настроен как DHCP-сервер, он становится основным шлюзом для подключённого к нему DHCP-клиента. Имейте в виду, что, если вы измените IP-адрес маршрутизатора, вам необходимо изменить диапазон IP-адресов в пуле адресов, используемых DHCP-сервером для LAN.

- **Начальный IP-адрес:** Укажите значение, начиная с которого DHCP-сервер будет предоставлять IP-адреса. Поскольку IP-адрес маршрутизатора по умолчанию 192.168.1.1, то Начальный IP-адрес по умолчанию будет **192.168.1.2**, соответственно для параметра Начальный IP-адрес необходимо указать 192.168.1.2 или больше, не меньше, чем 192.168.1.254
 - **Конечный IP-адрес:** Укажите значение, далее которого DHCP-сервер не будет предоставлять IP-адреса. Конечный IP-адрес не должен быть более 192.168.1.254. **192.168.1.254** – это конечный IP-адрес по умолчанию.
 - **Время аренды (часы):** Это срок, на который пользователю в сети будет разрешено соединение с маршрутизатором, используя текущий динамический IP-адрес. Укажите период времени в часах, на который будет "арендован" данный динамический IP-адрес. После того, как срок действия данного IP-адреса истечёт, пользователь автоматически получит новый динамический IP-адрес. Значение по умолчанию: **24** часа.
- **Список арендуемых IP-адресов:** Вы можете указать зарезервированный IP-адрес для компьютера локальной сети, компьютер всегда будет получать указанный IP-адрес каждый раз, как только он получает доступ к DHCP-серверу. Зарезервированные IP-адреса должны быть назначены серверам, которые требуют постоянных параметров IP. Нажмите кнопку **Добавить** (см. Рисунок 4-21), после чего вы сможете настроить правило на странице, как на рисунке ниже.

Аренда статического IP-адреса

Введите MAC-адрес и статический IP-адрес и затем нажмите "Сохранить/Применить" .

MAC-адрес:

IP-адрес:

Рисунок 4-22

- **MAC-адрес:** MAC-адрес компьютера локальной сети, которому вы хотите зарезервировать IP-адрес.
 - **IP-адрес:** IP-адрес, который вы резервируете за определённым компьютером.
- **Настройте второй IP-адрес и маску подсети для интерфейса LAN:** Можно настроить второй LAN IP-адрес и вторую LAN маску подсети по умолчанию для маршрутизатора, с помощью которых вы также сможете входить в веб-утилиту настройки.

4.4.4.2 Настройка IPv6 LAN

В меню на странице **Дополнительные настройки – LAN – IPv6 LAN** доступны настройки локальной сети (см. Рисунок 4-23), здесь можно настроить LAN IPv6-интерфейс вашего маршрутизатора со встроенным модемом.

Автонастройка LAN IPv6-адреса

Примечание: DHCPv6 с сохранением состояния поддерживается при длине префикса до 64. Идентификатор интерфейса НЕ ДОЛЖЕН содержать ПУСТЫЕ РАЗДЕЛЫ "::". Введите все символы. Например: введите "0:0:0:2" вместо "::2".

Настройка статического LAN IPv6-адреса

Адрес интерфейса (требуется длина префикса):

Назначение LAN IPv6-адресов

Включить DHCPv6-сервер

Без хранения состояния

С хранением состояния

Начальный идентификатор интерфейса:

Конечный идентификатор интерфейса:

Время аренды (часов):

Включить RADVD

Включить рассылку префиксов ULA

Создать в произвольном порядке

Настроить статически

Префикс:

Предпочтительно время работы (часов):

Действительно время работы (часов):

Рисунок 4-23

- **Адрес интерфейса (требуется длина префикса):** Введите здесь длину префикса адреса интерфейса.
- **Назначение LAN IPv6-адресов:** Выберите способ, каким будут назначаться IPv6-адреса компьютерам вашей локальной сети. Можно выбрать DHCPv6-сервер и RADVD.

DHCPv6-сервер:

- 1) Если выбран параметр **Без сохранения состояния**, настройка не требуется.
- 2) Если выбран параметр **С сохранением состояния**, то введите нижеследующие параметры.

<input checked="" type="checkbox"/>	Включить DHCPv6-сервер	
<input type="checkbox"/>	Без хранения состояния	
<input checked="" type="radio"/>	С хранением состояния	
	Начальный идентификатор интерфейса:	<input type="text" value="0:0:0:2"/>
	Конечный идентификатор интерфейса:	<input type="text" value="0:0:0:254"/>
	Время аренды (часов):	<input type="text" value="24"/>

- **Начальный идентификатор интерфейса:** Введите значение, начиная с которого DHCPv6-сервер будет предоставлять IPv6-адреса.
- **Конечный идентификатор интерфейса:** Введите значение, после которого DHCPv6-сервер не будет предоставлять IPv6-адреса.
- **Время аренды (часы):** Это срок, на который пользователю в сети будет разрешено соединение с маршрутизатором, используя текущий динамический IPv6-адрес. Укажите период времени в часах, на который будет "арендован" данный динамический IPv6-адрес. После того, как срок действия данного IPv6-адреса истечёт, пользователь автоматически получит новый динамический IPv6-адрес. Значение по умолчанию: 24 часа.

RADVD:

- 1) Если выбран вариант **Создать в произвольном порядке**, настройка не требуется.
- 2) Если выбран вариант **Настроить статически**, необходимо указать нижеследующие параметры.

<input checked="" type="checkbox"/>	Включить RADVD	
<input checked="" type="checkbox"/>	Включить рассылку префиксов ULA	
<input type="radio"/>	Создать в произвольном порядке	
<input checked="" type="radio"/>	Настроить статически	
	Префикс:	<input type="text"/>
	Предпочтительно время работы (часов):	<input type="text" value="-1"/>
	Действительно время работы (часов):	<input type="text" value="-1"/>

- **Префикс:** Введите значение префикса сайта.

Нажмите **Сохранить/Применить**, чтобы настройки вступили в силу.

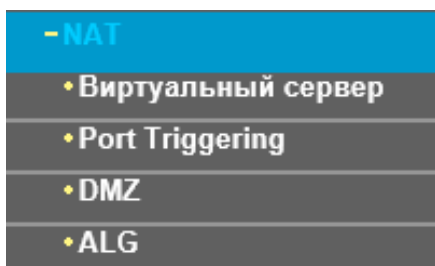
4.4.5 NAT

Функция преобразования сетевых адресов (NAT) позволяет вам использовать один WAN IP-адрес (доступ к Интернет) для нескольких компьютеров локальной сети.

Примечание:

Если в настройках WAN вы выбрали **PPPoA** или **PPPoE**, или если вы выбрали **Включить NAT** для типов подключения **IPoA** и **IPoE** ([4.4.2 WAN](#)), то в веб-утилите настройки появится меню **NAT**.

Меню **Дополнительные настройки – NAT** содержит три раздела: **Виртуальные серверы**, **Port Triggering**, **DMZ** и **ALG**. Для настройки нужной функции выберите соответствующее меню.



4.4.5.1 Виртуальные серверы

На странице **Дополнительные настройки – NAT – Виртуальный сервер** можно настроить виртуальные серверы (см. Рисунок 4-24).

Виртуальные серверы могут быть использованы для настройки сервисов общего пользования в вашей локальной сети, таких как DNS, электронная почта и FTP. Виртуальный сервер определяется как порт сервиса, и все запросы из сети Интернет на данный порт будут перенаправляться на компьютер, исходя из IP-адреса сервера. Любой компьютер, используемый в качестве виртуального сервера, должен иметь статический или зарезервированный IP-адрес, поскольку его IP-адрес может быть изменен при использовании функции DHCP.

NAT – Настройка виртуальных серверов											
<p>Виртуальный сервер позволяет вам направлять входящий трафик из сети WAN (идентифицируемый протоколом и внешним портом) на внутренний сервер с частным IP-адресом в сети LAN. Внутренний порт необходим только в том случае, если значение внешнего порта должно быть изменено на значение другого порта, используемого сервером в сети LAN. Вручную может быть добавлено не более 32 записей. Можно добавить не более 64 записей UPnP-клиентами.</p>											
Имя сервера	Начальный внешний порт	Конечный внешний порт	Протокол	Начальный внутренний порт	Конечный внутренний порт	IP-адрес сервера	WAN-интерфейс	Состояние	Включить/Выключить	Изменить	Удалить
<input type="button" value="Добавить"/> <input type="button" value="Включить все"/> <input type="button" value="Выбрать все"/> <input type="button" value="Удалить"/>											

Рисунок 4-24

➤ **Таблица виртуальных серверов:** В таблице содержатся записи виртуальных серверов.

- **Имя сервера:** Это имя **виртуального сервера**. Данное имя уникально и обязательно должно быть заполнено.
- **Начальный внешний порт:** Начальный номер внешнего порта. Вы можете ввести порт сервиса или оставить поле пустым.
- **Конечный внешний порт:** Конечный номер внешнего порта. Вы можете ввести порт сервиса или оставить поле пустым.
- **Протокол:** Протокол, используемый для данного приложения (**TCP**, **UDP**, или **TCP/UDP**).

- **Начальный внутренний порт:** Начальный номер внутреннего порта. Вы можете ввести порт сервиса или оставить поле пустым.
- **Конечный внутренний порт:** Конечный номер внутреннего порта. Вы можете ввести порт сервиса или оставить поле пустым.
- **IP-адрес сервера:** IP-адрес компьютера, предоставляющего сервис.
- **WAN-интерфейс:** Интерфейс WAN, который предоставляет сервис.

- **Добавить:** Нажмите кнопку **Добавить** для добавления записей.
- **Удалить:** Отметьте галочкой это поле в таблице (см. Рисунке 4-24), затем нажмите кнопку **Удалить**, после чего соответствующая запись будет удалена из таблицы.

Чтобы добавить запись виртуального сервера:

1. Нажмите кнопку **Добавить** на странице, как на Рисунке 4-24, после чего вы увидите новый виртуальный сервер (см. Рисунок. 4-25).

NAT – Виртуальные серверы

Выберите имя сервиса, введите IP-адрес сервера и нажмите "Сохранить/Применить" для перенаправления IP-пакетов от данного сервиса к указанному серверу.
ПРИМЕЧАНИЕ: "Конечный внутренний порт" не может изменяться напрямую. Значение данного параметра обычно совпадает с Конечным внешним портом. Тем не менее, если вы измените "Начальный внутренний порт", то "Конечный внутренний порт" примет такое же значение.
 Количество доступных для изменения записей:32

Использовать интерфейс:

Имя сервиса:

Выберите услугу:

Пользовательский сервис:

IP-адрес сервера:

Начальный внешний порт	Конечный внешний порт	Протокол	Начальный внутренний порт	Конечный внутренний порт
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		

Рисунок 4-25

2. Из выпадающего списка выберите интерфейс, который вы хотите использовать.
3. Из выпадающего списка выберите сервис, который вы хотите использовать. Если в списке нет нужного вам сервиса, введите имя сами в поле Пользовательский сервис.
4. Введите IP-адрес компьютера в поле **IP-адрес сервера**.
5. Введите Начальный внешний порт, Конечный внешний порт, Начальный внутренний порт и Конечный внутренний порт в таблице, затем выберите протокол, используемый для данного виртуального сервера (**TCP**, **UDP** или **TCP/UDP**).

- Нажмите **Сохранить/Применить** для включения виртуального сервера, после чего вы увидите ваши настройки на странице виртуальных серверов (Рисунок 4-24).

Примечание:

Если вы выберете сервис из выпадающего списка, Начальный внешний порт, Конечный внешний порт, Начальный внутренний порт, Конечный внутренний порт и Протокол будут добавлены в таблицу автоматически. Вам потребуется только указать IP-адрес для виртуального сервера.

4.4.5.2 Port Triggering

На странице **Дополнительные настройки – NAT – Port Triggering** можно настроить параметры Port Triggering (см. Рисунок 4-26).

Некоторым приложениям требуется, чтобы определённые порты межсетевого экрана маршрутизатора были открыты для доступа удалённым клиентам. Функция Port Triggering динамически открывает “Открытые порты” маршрутизатора, когда приложение в локальной сети инициирует TCP/UDP-соединение для удалённого клиента, использующего “Триггер Порты”. Маршрутизатор позволяет удалённому клиенту в сети WAN создавать новые подключения к приложениям в локальной сети, используя “Открытые порты”. Можно настроить не более 32 записей.

NAT – Port Triggering

Некоторым приложениям требуется, чтобы определённые порты межсетевого экрана маршрутизатора были открыты для доступа удалённым клиентам. Функция Port Triggering динамически открывает “Открытые порты” маршрутизатора, когда приложение в локальной сети инициирует TCP/UDP-соединение для удалённого клиента, использующего “Триггер Порты”. Маршрутизатор позволяет удалённому клиенту в сети WAN создавать новые подключения к приложениям в локальной сети, используя “Открытые порты”. Можно настроить не более 32 записей.

Имя приложения	Триггер		Открытый			WAN-интерфейс	Состояние	Включить/Отключить	Изменить	Удалить	
	Протокол	Диапазон портов		Протокол	Диапазон портов						
		Начало	Конец		Начало						Конец

Рисунок 4-26

- **Таблица Port Triggering:** В таблице содержится информация о записях функции Port Triggering.
 - **Имя приложения:** Это имя записи **Port Triggering**. Данное значение уникально и должно быть обязательно заполнено.
 - **Триггер:** Здесь указывается Протокол, а также диапазон триггер портов – начальный и конечный триггер порт.
 - **Открытый:** Здесь указывается Протокол, а также диапазон открытых портов – начальный и конечный открытый порт.
 - **WAN-интерфейс:** Интерфейс WAN-сервиса для функции Port Triggering.
- **Добавить:** Нажмите эту кнопку для добавления новой записи.
- **Удалить:** Отметьте галочкой это поле в таблице (Рисунок 4-26), затем нажмите кнопку **Удалить**, после чего соответствующая запись будет удалена из таблицы.

Чтобы добавить новую запись Port Triggering:

- Нажмите кнопку **Добавить** (см. Рисунок 4-26), после чего вы увидите новую запись Port Triggering на странице, как на Рисунке 4-27.

NAT – Port Triggering

Некоторые приложения, такие как игры, видеоконференции, приложения, которым необходим удалённый доступ, требуют, чтобы определённые порты межсетевое экрана маршрутизатора были открыты для доступа. Вы можете произвести настройки порта на данной странице, выбрав приложение или создав собственное правило для пользовательского приложения и нажав "Сохранить/Применить".

Количество доступных для изменения записей: 32

Имя приложения:

Использовать интерфейс:

Выбрать приложение:

Пользовательское приложение:

Начальный Триггер порт	Конечный Триггер порт	Триггер протокол	Начальный Открытый порт	Конечный Открытый порт	Открытый протокол
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

Рисунок 4-27

2. Выберите приложение из выпадающего списка. Если в списке нет нужного вам приложения, выберите кнопку **Пользовательское приложение** и введите имя на ваше усмотрение в поле справа.
3. Введите **Начальный Триггер порт**, **Конечный Триггер порт**, **Начальный открытый порт** и **Конечный открытый порт** в таблице, затем выберите **Триггер протокол** и **Открытый протокол (TCP, UDP или TCP/UDP)**.
4. Нажмите **Сохранить/Применить** для включения настроек, после чего вы увидите ваши настройки на странице, как на Рисунок 4-26.

👉 Примечание:

Если вы выберете приложение из выпадающего списка, **Начальный внешний порт**, **Конечный внешний порт**, **Начальный внутренний порт**, **Конечный внутренний порт** и **Протокол** будут добавлены в таблицу автоматически.

4.4.5.3 DMZ

На странице **Дополнительные настройки – NAT – DMZ** можно настроить узел DMZ (см. Рисунок 4-28).

Функция DMZ позволяет создавать особый сетевой сегмент для узла локальной сети, обращающегося к таким Интернет-ресурсам как онлайн-игры или видеоконференции..

NAT – Узел DMZ

Устройство будет пересылать IP-пакеты из Интернет, которые не принадлежат приложениям, указанным в таблице виртуальных серверов, к узлу DMZ компьютера.

Введите IP-адрес компьютера и нажмите 'Сохранить/Применить' для активации узла DMZ.

Очистите поле 'IP-адрес' и нажмите 'Сохранить/Применить' для деактивации узла DMZ.

DIP-адрес узла DMZ:

Рисунок 4-28

Чтобы добавить новый узел DMZ:

Можно ввести IP-адрес компьютера и затем нажать **Сохранить/Применить** для активации узла DMZ, настроенного на данной странице.

Примечание:

Хост DMZ переадресовывает все порты одновременно. У любого ПК, порты которого переадресовываются, функцию DHCP-клиента должна быть отключена. Также этот ПК должен иметь назначенные статический IP-адрес, так как его IP-адрес может меняться при использовании функции DHCP.

4.4.5.4 ALG

На странице **Дополнительные настройки – NAT – ALG** можно настроить основные параметры безопасности (см. Рисунок 4-29).

ALG

Выберите тип ALG ниже.

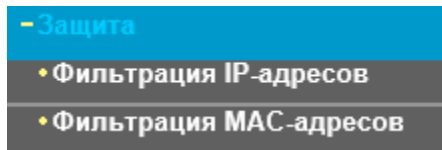
- Включить FTP
- Включить TFTP
- Включить SIP
- Включить H.323
- Включить RSTP
- Включить IRC

Рисунок 4-29

Нажмите кнопку **Сохранить/Принять** для сохранения ваших настроек.

4.4.6 Защита

Раздел меню **Дополнительные настройки – Защита** содержит параметры защиты, а также подразделы **Фильтрация IP-адресов** и **Фильтрация MAC-адресов** (доступны только в режиме моста).



4.4.6.1 Фильтрация IP-адресов

Функция фильтрации IP-адресов позволяет администраторам контролировать доступ пользователей к Интернет по IP-адресу пользователя. Под данной функцией подразумевается фильтрация **исходящих** IP-адресов. Подробные инструкции указаны ниже.

На странице **Дополнительные настройки – Защита – Фильтрация IP-адресов** можно настроить правила фильтрации исходящего трафика (см. Рисунок 4-30).

Функция фильтрации исходящих IP-адресов позволяет контролировать IP-трафик из локальной сети. По умолчанию исходящий IP-трафик из локальной сети разрешён, однако можно **ЗАБЛОКИРОВАТЬ** определённые IP-адреса, настроив правила фильтрации.

Настройка фильтра исходящих IP-адресов

По умолчанию исходящий IP-трафик из локальной сети разрешён, однако можно **ЗАБЛОКИРОВАТЬ** определённые IP-адреса, настроив правила фильтрации.

Для настройки фильтра исходящих IP-адресов воспользуйтесь кнопками **Добавить** или **Удалить**. Можно настроить не более 36 фильтров.

Имя фильтра	Версия IP-протокола	Протокол	IP ист./ Длина префикса	Порт ист	IP назн./ Длина префикса/td>	Порт назн	Удалить

Рисунок 4-30

Чтобы настроить правило фильтрации исходящих IP-адресов:

1. **Нажмите кнопку **Добавить** (см. Рисунок 4-30), после чего вы попадёте на страницу, как на Рисунке 4-32.**

Добавить фильтр исходящих IP-адресов

На данной странице можно создать правило фильтра для определения исходящего IP-трафика, указав новое имя фильтра и хотя бы одно условие. Чтобы правило фильтра вступило в силу, должны удовлетворяться все выбранные для него условия. Нажмите **Сохранить/Применить** для сохранения и включения фильтра.

Имя фильтра:

Версия IP-протокола:

Протокол:

IP-адрес источника [/длина префикса]:

Порт источника (порт или порт:порт):

IP-адрес назначения [/длина префикса]:

Порт назначения (порт или порт:порт):

Рисунок 4-31

2. Введите **Имя фильтра** для правила, это имя уникально и обязательно должно быть указано.
3. Из выпадающего списка выберите **протокол (TCP/UDP, TCP, UDP или ICMP)** для соединения между IP-адресом источника и IP-адресом назначения.
4. Введите **IP-адрес источника** в десятичном формате с разделительными точками, а затем введите **Порт источника** (порт или порт: порт) в соответствующих полях.
5. Введите **IP-адрес назначения** в десятичном формате с разделительными точками, затем введите **Порт назначения** (порт или порт: порт) в соответствующих полях.
6. Нажмите **Сохранить/Применить** для сохранения записи.

 **Примечание:**

Когда вы добавляете запись фильтрации исходящих IP-адресов, вам необходимо настроить хотя бы одно условие на предыдущей странице за исключением Имени фильтра. Если поле Протокол оставить пустым, это будет означать, что правило применяется ко всем протоколам. Если вы оставите пустыми поля IP-адрес источника и/или IP-адрес назначения, это будет означать, что правило применяется ко всем IP-адресам источника и/или IP-адресам назначения. Если оставить пустыми поля Порт источника и/или Порт назначения, то правило применяется ко всем Портам источника и/или Портам назначения.

4.4.6.2 Фильтрация MAC-адресов

На странице **Дополнительные настройки – Защита – Фильтрация MAC-адресов** можно настроить правила фильтрации MAC-адресов (см. Рисунок 4-32). Данный раздел меню позволяет контролировать доступ к Интернет пользователей вашей локальной сети по их MAC-адресам.

 **Примечание:**

Фильтрация MAC-адресов может использоваться только для постоянных виртуальных каналов ATM, настроенных в режиме моста.

Настройка фильтрации MAC-адресов

Фильтрация MAC-адресов работает только для постоянных виртуальных каналов ATM, настроенных в режиме моста. **ПЕРЕНАПРАВЛЕНО** означает, что все кадры MAC-уровня будут **ПЕРЕНАПРАВЛЕНЫ**, за исключением тех, которые соответствуют настройкам правил в таблице ниже. **ЗАБЛОКИРОВАНО** означает, что все кадры MAC-уровня будут **ЗАБЛОКИРОВАНЫ**, за исключением тех, которые соответствуют настройкам правил в таблице ниже.

Политика фильтрации MAC-адресов для каждого интерфейса:
ВНИМАНИЕ: Изменение глобальной политики приведёт к тому, что все настроенные правила БУДУТ УДАЛЕНЫ АВТОМАТИЧЕСКИ! Вам потребуется создать новые правила в отношении новой политики.

Интерфейс	Политика	Изменить
atm0.1	ПЕРЕНАПРАВЛЕНО	<input type="checkbox"/>

Для настройки правил фильтрации MAC-адресов воспользуйтесь кнопками Добавить или Удалить. Можно настроить не более 36 фильтров.

Интерфейс	Протокол	MAC-адрес назначения	MAC-адрес источника	Удалить

Рисунок 4-32

- **Изменить политику:** Для фильтрации MAC-адресов можно использовать два вида политик: **ПЕРЕНАПРАВЛЕНО** или **ЗАБЛОКИРОВАНО**. Поставьте галочку в столбце **Изменить**, затем нажмите кнопку **Изменить политику** для изменения политики. Если вы выбрали опцию **ПЕРЕНАПРАВЛЕНО**, то все кадры MAC-уровня будут пропущены маршрутизатором, за исключением тех, которые были указаны в правилах в таблице

(см. Рисунок 4-32). Если выбрать опцию **ЗАБЛОКИРОВАНО**, маршрутизатор будет **блокировать** все кадры MAC-уровня за исключением тех, которые были указаны в правилах фильтрации MAC-адресов.

- **Добавить:** Нажмите кнопку **Добавить**, после чего вы попадёте на следующую страницу (Рисунок 4-32), где можно настроить фильтр MAC-адресов.
- **Удалить:** Отметьте галочкой это поле в таблице (Рисунок 4-32), затем нажмите кнопку **Удалить**, после чего соответствующая запись будет удалена из таблицы.

Чтобы добавить правило фильтрации MAC-адресов:

1. Нажмите кнопку **Добавить** (Рисунок 4-32), вы попадёте на следующую страницу (Рисунок 4-33).

Добавить фильтр MAC-адресов

Создайте фильтр, чтобы определить кадры MAC-уровня, выбрав хотя бы одно условие. Если выбрано несколько условий, все они будут применяться. Нажмите "Сохранить/Применить" для сохранения и включения фильтра.

Тип протокола:

MAC-адрес назначения:

MAC-адрес источника:

WAN-интерфейсы (настроенные только в режиме моста):

Рисунок 4-33

2. Выберите из выпадающего списка **Тип протокола** для правила.
3. Введите **MAC-адрес назначения** и **MAC-адрес источника**.
4. Из выпадающего списка выберите **Направление кадра** для правила.
5. Из выпадающего списка выберите **WAN-интерфейс**.
6. Нажмите **Сохранить/Применить** для сохранения записи фильтра, после чего вы увидите ваши настройки на странице, как на Рисунке 4-32.

4.4.7 Родительский контроль

В меню на странице **Дополнительные настройки – Родительский контроль** находятся настройки родительского контроля, здесь же находятся разделы **Ограничение по времени** и **Фильтрация URL**. **Ограничение по времени** позволяет вам контролировать активность пользователей в Интернет путём ограничения доступа к Интернет по времени. **Фильтрация URL** запрещает компьютерам, подключённым к маршрутизатору, доступ к определённым веб-сайтам. Обе эти функции работают независимо друг от друга.

4.4.7.1 Ограничение по времени

Данная функция позволяет настроить время, в течение которого определённому устройству локальной сети, подключённому к маршрутизатору, будет запрещён доступ к Интернет.

Время запрета доступа

Можно настроить не более 16 записей.

Имя пользователя	MAC-адрес	Дней							Время		Состояние	Включить/Отключить	Изменить	Удалить	
		Пн	Вт	Ср	Чт	Пт	Сб	Вск	Начало	Конец					

Рисунок 4-34

Чтобы добавить запись ограничения доступа по времени:

1. Нажмите кнопку **Добавить** (Рисунок 4-34), далее вы увидите страницу, как на Рисунке 4-35.

Время запрета доступа

На этой странице можно добавить время, когда будет запрещён доступ устройств локальной сети к маршрутизатору. В поле "MAC-адрес браузера" автоматически отображается MAC-адрес устройства локальной сети, на котором запущен браузер. Для запрета доступа другим устройствам нажмите "Другие MAC-адреса" и введите MAC-адрес другого устройства локальной сети. Чтобы найти MAC-адрес компьютера с Windows, откройте командную строку и введите "ipconfig /all".

Имя пользователя:

MAC-адрес браузера:

Другой MAC-адрес (XX:XX:XX:XX:XX:XX):

Дней недели:	Пн	Вт	Ср	Чт	Пт	Сб	Вск
Нажмите для выбора:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Начальное время блокировки (ЧЧ:ММ):

Конечное время блокировки (ЧЧ:ММ):

Рисунок 4-35

2. Введите **Имя пользователя** устройства локальной сети, подключённого к маршрутизатору.
3. Чтобы запретить доступ устройству, на котором запущен веб-браузер, отметьте строку **MAC-адрес браузера**. В поле рядом будет автоматически указан MAC-адрес. Чтобы запретить доступ прочим устройствам локальной сети, отметьте строку **Другой MAC-адрес (XX:XX:XX:XX:XX:XX)** и введите MAC-адрес другого устройства локальной сети.
4. Выберите день, когда будет работать правило.
5. Введите **Начальное время блокировки** и **Конечное время блокировки** по отдельности в соответствующих полях внизу, чтобы контролируемое устройство не могло подключиться к Интернет в течение указанного периода времени.
6. Нажмите **Сохранить/Применить** для сохранения данной записи, после чего вы увидите ваши настройки в таблице (см. Рисунок 4-34).

👉 Примечание:

Функция ограничения доступа по времени будет работать только после того, как вы настроите время на маршрутизаторе в меню **Управление – Время**.

4.4.7.2 Фильтрация URL

Данная функция позволяет настраивать правила фильтрации по URL-адресам для того, чтобы контролировать доступ компьютеров локальной сети к определённому порту. Данная функция работает независимо от ограничения доступа по времени.

Фильтр URL-адресов

Сначала выберите тип списка, затем настройте записи в списке. Можно настроить не более 200 URL-адресов.

Тип списка URL-адресов: Отключить Разрешить Запретить

LAN IP-адрес	Порт	Адрес	Состояние	Включить/Отключить	Изменить	Удалить

Рисунок 4-36

Маршрутизатор располагает тремя политиками для функции фильтрации URL-адресов.

- **Отключить:** Функция фильтрации URL-адресов не будет работать.
- **Разрешить:** Разрешить компьютерам доступ к указанным URL-адресам.
- **Запретить:** Запретить доступ компьютерам к указанным URL.

Чтобы добавить запись фильтрации URL:

1. Выберите кнопку **Запретить** или **Разрешить**. Для примера выбрано **Запретить**.
2. Нажмите кнопку **Добавить** (см. Рисунок 4-36), после чего вы увидите страницу, как на Рисунке 4-37. Введите URL-адрес и Номер порта.

Родительский контроль – Фильтр URL-адресов Добавить

Введите адрес, затем нажмите "Сохранить/Применить" для добавления записи фильтрации URL-адресов. По желанию можно указать LAN IP-адрес, если вы хотите сделать настройку для конкретного компьютера локальной сети.

Диапазон LAN IP-адресов: - (необязательно)

Номер порта: (Если это поле оставить пустым, то по умолчанию будет использоваться порт 80.)

Адрес:

Рисунок 4-37

3. Нажмите **Сохранить/Применить** для сохранения данной записи, после чего вы увидите ваши настройки на странице, как на Рисунок 4-36. Каждый компьютер, подключённый к маршрутизатору, не сможет зайти на данный URL-адрес через указанный порт.

4.4.8 Приоритезация данных

На странице **Дополнительные настройки – Приоритезация данных** можно включить функцию приоритезации данных (см. Рисунок 4-38). Данная функция позволяет установить очерёдность обработки различного трафика, входящего через ваш маршрутизатор. Функция приоритезации данных прикрепляет специальные определительные метки или заголовки входящим пакетам, что позволяет направить пакеты в ту или иную приоритетную очередь.

Это полезно, когда вы хотите указать более высокий приоритет некоторому типу данных, например, пакеты голосового трафика будут иметь более высокий приоритет, чем пакеты web-трафика. Данная опция позволяет более качественно обрабатывать указанный сетевой трафик с помощью различных технологий.

Приоритезация данных – Настройка управления очередями

Если отмечена строка 'Включить функцию приоритезации данных', необходимо выбрать DSCP-маркер по умолчанию для автоматической маркировки входящего трафика без использования отдельного классификатора. Нажмите 'Сохранить/Применить'.

Примечание: если строка 'Включить функцию приоритезации данных' не выбрана, то данная функция будет отключена для всех портов.

Примечание: DSCP-маркер по умолчанию используется для маркировки всех исходящих пакетов, которые не подходят под правила классификации.

Включить функцию приоритезации данных

Выбрать DSCP-маркер по умолчанию

Рисунок 4-38

Отметьте строку **Включить функцию приоритезации данных**, чтобы включить данную функцию для всех интерфейсов.

Из выпадающего списка необходимо **Выбрать DSCP-маркер по умолчанию** для автоматической маркировки входящего трафика без использования отдельного классификатора.

Нажмите **Сохранить/Применить** для сохранения текущих настроек.

👉 Примечание:

DSCP-маркер по умолчанию помечает все исходящие пакеты, которые не подходят ни под одно правило классификации.

4.4.8.1 Настройка очередей

На странице **Дополнительные настройки – Приоритезация данных – Настройка очередей** можно настроить виртуальные серверы.

Настройка очереди приоритезации данных

Для режима ATM (асинхронный режим передачи данных) можно настроить не более 8 записей.
 Для режима PTM (пакетный режим передачи) можно настроить не более 8 записей.
 Для каждого Ethernet-интерфейса можно настроить не более 4 записей.
 Для каждого Ethernet WAN-интерфейса можно настроить не более 4 записей.
 Для добавления очереди воспользуйтесь кнопкой **Добавить**.
 Для удаления очереди отметьте соответствующие поля 'Удалить', затем нажмите кнопку **Удалить**.
 После нажатия кнопки **Включить** устройство проанализирует все очереди в таблице. Очереди, у которых стоит галочка в поле 'Включить', будут включены. Те очереди, у которых нет отметки в поле 'Включить', не будут активированы.
 После обновления страницы поле 'Включить' информирует о состоянии очереди.
 Если вы отключили функцию WMM на странице 'Беспроводной режим', очереди, относящиеся к беспроводному режиму, не будут использоваться.

Имя	Ключ	Интерфейс	ID очереди	Приор/Alrt/Bes	Задержка DSL-линии	Приоритет PTM	Мин. скорость (Бит/с)	Скорость шейпинга (Бит/с)	Burst Size (байт)	Включить	Удалить
WMM Voice Priority	1	w0	1	1/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
WMM Voice Priority	2	w0	2	2/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
WMM Video Priority	3	w0	3	3/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
WMM Video Priority	4	w0	4	4/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
WMM Best Effort	5	w0	5	5/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
WMM Background	6	w0	6	6/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
WMM Background	7	w0	7	7/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
WMM Best Effort	8	w0	8	8/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
Default Queue	33	atm0	1	8/WRR/1	Path0					<input checked="" type="checkbox"/>	<input type="checkbox"/>
TCP ACK Queue	34	atm0	2	7/WRR/1	Path0					<input checked="" type="checkbox"/>	<input type="checkbox"/>

Рисунок 4-39

Нажмите кнопку **Добавить** (см. Рисунок 4-39) для настройки записи очереди на следующей странице (см.Рисунок 4-40).

Настройка очередей приоритезации трафика

На данной странице можно настроить очередь приоритезации трафика и добавить её к выбранному интерфейсу 2 уровня.

Имя:

Включить: ▾

Интерфейс: ▾

Приоритет очередей: ▾ (ниже значение, выше приоритет)

- В списке приоритетов очередей отображается алгоритм расписания для каждого уровня приоритетности.
 - Очереди с одинаковыми приоритетами располагаются согласно алгоритму.
 - Очереди с разными приоритетами располагаются на основании строгой приоритетности.

Алгоритм расписания

Взвешенный циклический алгоритм
 Взвешенная справедливая очередь

Весовой коэффициент очереди: [1-63]

Задержка DSL-линии: ▾

Рисунок 4-40

- **Имя:** Укажите имя записи.
- **Включить:** Выбрав эту опцию, вы включите данную запись.
- **Интерфейс:** Конкретный WAN-сервис, назначенный для данной записи приоритезации данных.
- **Приоритет очередей:** Уровень приоритетности для данной очереди приоритезации данных.
- **Задержка DSL-линии:** Выберите параметр задержки для данного типа передачи данных, для настоящего маршрутизатора доступен только вариант Path0.

Завершив настройку параметров приоритезации данных, нажмите **Сохранить/Применить** для её сохранения, после чего вы увидите ваши настройки на странице, как на Рисунке 4-39.

👉 Примечание:

- 1) Меньшее число для обозначения приоритетности означает более высокий приоритет данной очереди по отношению к другим.
- 2) Запись очереди, настроенная на данной странице, будет использоваться классификатором для правильной сортировки входящих пакетов.

4.4.8.2 Классификация

В данном разделе указано, как создать правило классификации исходящего трафика, назначить очередь приоритетности, интерфейс и (по выбору) переписать DSCP-байт заголовка IP-пакета.

Правило состоит из имени класса и как минимум из одно из указанных ниже условий. Для того чтобы правило вступило в силу, должны выполняться все условия, указанные для данного правила.

Настройка функции приоритезации данных – можно настроить не более – можно настроить не более 32 правил.

Чтобы добавить правило, нажмите кнопку **Добавить**.
 Чтобы удалить правило, поставьте галочку напротив ненужного вам правила в столбце **Удалить** и нажмите кнопку **Удалить**.
 После нажатия кнопки **Включить**, устройство просканирует все записи в таблице. Правила, у которых стоит галочка в столбце **Включить**, будут включены. Те правила, у которых нет отметки в столбце **Включить**, не будут активированы.
 После обновления страницы столбец **Включить** информирует о состоянии записей.
 Если вы отключили функцию WMM на странице **Беспроводной режим**, критерии классификации, относящиеся к беспроводному режиму, не будут использоваться.

Имя класса	Порядок	КРИТЕРИЙ КЛАССИФИКАЦИИ										РЕЗУЛЬТАТЫ КЛАССИФИКАЦИИ			Удалить			
		Class	Intf	Ether Type	MAC/маска ист	MAC/маска назн	Ид/длина преф. ист	Ид/длина преф. назн	Протокол	Порт ист	Порт назн	Проверка DSCP	Проверка 802.1P	Ключ очереди		DSCP-маркер	802.1P-маркер	Включить

Рисунок 4-41

Нажмите кнопку **Добавить** (см. Рис. 4-41) для настройки правила классификации приоритезации данных на следующей странице.

Добавить правило класса сетевого трафика

На этой странице можно создать правила классов трафика для классификации входящего трафика на основе приоритетной очереди и дополнительно указать DSCP или Ethernet-приоритетность пакетов.
 Нажмите **сохранить/Применить** для сохранения и активации правила.

Имя класса трафика:

Порядок правила:

Состояние правила:

Указать критерии классификации (Если не указан, это означает, что критерий не используется)

Интерфейс класса:

Ether Type:

MAC-адрес источника:

Маска MAC-адреса источника:

MAC-назначения:

Маска MAC-адреса назначения:

Указать результаты классификации (Если значение не указано, то данный параметр не используется)

Указать очередь класса (обязательная настройка):

Маркировка точки кода дифференцированных услуг (DSCP):

Маркировка приоритетности 802.1p:

- Пакеты без VLAN, выходящие через интерфейс без VLAN, будут тэгироваться VID 0 и P-BITS на основе правила класса.
- У пакетов с VLAN, выходящих через интерфейс с VLAN, P-BITS пакета будут заново маркироваться P-BITS правилом класса. Дополнительный тэг VLAN не будет добавлен.
- Пакеты без VLAN, выходящие через интерфейс с VLAN, будут тэгироваться VID интерфейса and и P-BITS правила класса.
- Пакеты с VLAN, выходящие через интерфейс с VLAN, будут дополнительно тэгированы VID пакета и P-BITS правила класса.

Рисунок 4-42

Указав условия, нажмите **Сохранить/Применить** для сохранения записи.

4.4.9 Контроль пропускной способности

На странице **Дополнительные настройки – Контроль пропускной способности** (см. Рисунок 4-43) можно включить данную функцию и настроить параметры общей исходящей/входящей пропускной способности.

Контроль пропускной способности

На этой странице можно включить/отключить контроль пропускной способности. Настройки применяются только, если отмечена строка "Включить контроль пропускной способности".
Нажмите "Сохранить/Применить" для сохранения настроек.

Примечание:
Если данная строка не отмечена, все правила контроля доступа будут отключены.
Если вы используете ADSL-подключение, убедитесь, что общая исходящая/входящая пропускная способность не превышает входящую/исходящую скорость подключения, иначе контроль пропускной способности не будет работать.

Включить контроль пропускной способности

Тип линии: ADSL Другое

Общая исходящая пропускная способность: Кбит/с

Общая входящая пропускная способность: Кбит/с

Рисунок 4-43

- **Включить контроль пропускной способности:** Отметьте эту строку для включения функции контроля пропускной способности.
- **Общая исходящая пропускная способность (Кбит/с):** Введите скорость исходящего потока данных через порт WAN.
- **Общая входящая пропускная способность (Кбит/с):** Введите скорость входящего потока данных через порт WAN.
- **Сохранить/Применить:** Нажмите эту кнопку, чтобы ваши настройки вступили в силу.

Примечание:

Параметры общей исходящей пропускной способности и общей входящей пропускной способности должны быть настроены обязательно.

4.4.9.1 Список правил

На странице **Дополнительные настройки – Контроль пропускной способности – Список правил** (см. Рис. 4-44) можно просматривать и настраивать параметры контроля трафика.

Список правил контроля пропускной способности

На этой странице отображены правила контроля пропускной способности. Для настройки правил воспользуйтесь соответствующими кнопками. Можно настроить не более 16 записей.
Если *максимальная* пропускная способность не указана или её значение превышает значение общей пропускной способности, то максимальная пропускная способность по умолчанию будет равна общей.
Следите за тем, чтобы *минимальная* пропускная способность не превышала общую, иначе функция контроля пропускной способности не будет работать.

Описание	Приоритет	Исходящая пропускная способность (Кбит/с)		Входящая пропускная способность (Кбит/с)		Состояние	Изменить	<input type="checkbox"/>
		Мин	Макс	Мин	Макс			
<input type="button" value="Добавить"/> <input type="button" value="Включить"/> <input type="button" value="Отключить"/> <input type="button" value="Удалить"/>								

Рисунок 4-44

Чтобы добавить правило контроля трафика, нажмите кнопку **Добавить**, правило можно будет настроить на следующей странице (см. Рис. 4-45).

Настройка правил контроля пропускной способности

На этой странице можно настроить правило контроля пропускной способности. Для каждого правила можно указать определённый приоритет. Правило будет использоваться для контроля скорости исходящих и входящих пакетов
Нажмите "Сохранить/Применить" для сохранения правила.

Состояние правила: Включить Отключить

Диапазон IP-адресов: -

Диапазон портов: -

Протокол:

Протокол:

Мин. скорость Макс. скорость

Скорость исходящего трафика: - Кбит/с

Скорость входящего трафика: - Кбит/с

Рисунок 4-45

- **Состояние правила:** Выберите состояние правила из выпадающего списка для включения/отключения правила.
- **Диапазон IP-адресов:** Введите один IP-адрес или диапазон IP-адресов.
- **Диапазон портов:** Введите один порт или диапазон портов.
- **Протокол:** Выберите тип протокола из выпадающего списка (TCP, UDP или TCP/UDP).
- **Приоритет:** Из выпадающего списка выберите приоритет. Доступно пять вариантов: Самый высокий, 1, 2, 3, 4, 5, 6 и Самый низкий. По умолчанию очередь приоритетности для правила: 4.
- **Скорость исходящего трафика:** Укажите мин. и макс. значения скорости исходящего потока данных через порт WAN.
- **Скорость входящего трафика:** Укажите мин. и макс. значения скорости входящего потока данных через порт WAN.

После того как все параметры настроены, нажмите **Сохранить/Применить**, чтобы ваши настройки вступили в силу, после чего вы увидите список, как на Рисунке 4-46. Если вы хотите изменить правило, нажмите кнопку **Изменить**. Если вы хотите удалить правило, сначала поставьте галочку в столбце **Удалить**, затем нажмите кнопку **Удалить**.

Список правил контроля пропускной способности

На этой странице отображены правила контроля пропускной способности. Для настройки правил воспользуйтесь соответствующими кнопками. Можно настроить не более 16 записей.
 Если *максимальная* пропускная способность не указана или её значение превышает значение общей пропускной способности, то *максимальная* пропускная способность по умолчанию будет равна общей.
 Следите за тем, чтобы *минимальная* пропускная способность не превышала общую, иначе функция контроля пропускной способности не будет работать.

Описание	Приоритет	Исходящая пропускная способность (Кбит/с)		Входящая пропускная способность (Кбит/с)		Состояние	Изменить	<input type="checkbox"/>
		Мин	Макс	Мин	Макс			
192.168.1.101-192.168.1.103, 80, TCP/UDP	4	100	200	400	800	Включено	Изменить	<input type="checkbox"/>

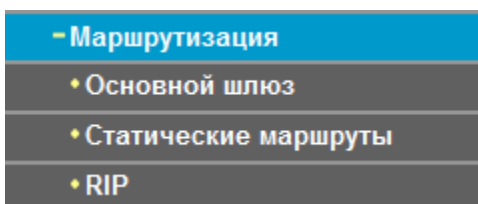
Рисунок 4-46

👉 Примечание:

Макс. скорость исходящего/входящего трафика и мин. скорость исходящего/входящего трафика определяются за счёт выделения излишка исходящей/входящей пропускной способности согласно приоритету. Если правила с разными приоритетами, то излишек пропускной способности используется сначала для правила с наибольшим приоритетом согласно макс. скорости исходящего/входящего трафика, настроенного для такого правила. Если после этого всё ещё остаётся какой-то излишек пропускной способности, он используется для правила с менее высоким приоритетом. Если правила имеют одинаковый приоритет, излишек пропускной способности расходуется для этих правил исходя из мин. скорости исходящего/входящего трафика, настроенной для таких правил. Чем больше скорость исходящего/входящего трафика, которая указана для правила, тем более пропускной способности будет выделено для него.

4.4.10 Маршрутизация

В меню **Дополнительные настройки – Маршрутизация** содержится три раздела: **Основной шлюз**, **Статические маршруты** и **RIP**. Подробное описание настроек указано ниже.

**4.4.10.1 Основной шлюз**

Если вы зайдёте в меню **Дополнительные настройки – Маршрутизация – Основной шлюз**, вы увидите следующую страницу.

Настройки маршрутизации – Основной шлюз

Список интерфейсов основного шлюза может содержать несколько интерфейсов WAN, работающих в качестве системных основных шлюзов, но только один из них будет использоваться согласно следующей очередности приоритетов: первый имеет наибольший приоритет, а последний имеет наименьший приоритет, если подключен интерфейс WAN. Порядок приоритетности можно изменять путём удаления всех и обратного их добавления..

Выбранные интерфейсы основного шлюза

atm0.3
ppp0.2

->

<-

Доступные интерфейсы WAN

Выберите предпочтительный интерфейс WAN в качестве системного IPv6 основного шлюза.

Выбранный интерфейс WAN НЕТ НАСТРОЕННЫХ ИНТЕРФЕЙСОВ ▾

Сохранить/Применить

Рисунок 4-47

4.4.10.2 Статическая маршрутизация

На странице **Дополнительные настройки – Маршрутизация – Статическая маршрутизация** можно настроить статические маршруты (см. Рисунок 4-48). Статический маршрут – это заранее установленный маршрут, по которому сетевые данные перемещаются к конкретному узлу или сети.

Маршрутизация – Статические маршруты

Максимальное количество записей, которое можно настроить: 32.

Версия IP-адреса	DstIP/Длина префикса	Шлюз	Интерфейс	Метрика	Состояние	Включить/Отключить	Изменить	Удалить

Добавить
Включить все
Выбрать все
Удалить

Рисунок 4-48

Чтобы добавить запись статического маршрута:

1. **Нажмите кнопку Добавить (см. Рисунок 4-48), вы увидите страницу, как на Рисунке 4-49.**

Маршрутизация – Статические маршруты Добавить

Введите адрес, маску подсети, шлюз сети назначения И/ИЛИ доступный WAN-интерфейс, затем нажмите "Сохранить/Применить" для добавления записи в таблице.

Версия IP-адреса:

IP-адрес назначения/длина префикса:

Интерфейс:

IP-адрес шлюза:

(по выбору: значение метрики должно быть 0 или выше)

Метрика:

Рисунок 4-49

2. Введите следующие данные:
 - **Версия IP-адреса:** Выберите версию IP-протокола.
 - **IP-адрес назначения/длина префикса:** IP-адрес назначения является адресом сети или узла, которому вы хотите назначить статический маршрут.
 - **Интерфейс:** Выберите имя интерфейса иначе для статического маршрута будет использовано имя интерфейса по умолчанию.
 - **IP-адрес шлюза:** Если вы выбрали IPoE или IPoA для **Интерфейса**, то на странице появится данный параметр. Следите, чтобы адрес шлюза был введён правильно. Параметр **Интерфейс** будет использовать адрес шлюза по умолчанию для статического маршрута.
3. Нажмите **Сохранить/Применить** для сохранения ваших настроек, после чего вы увидите ваши настройки на странице, как на Рисунок 4-48.

Чтобы удалить запись статического маршрута:

1. Отметьте галочкой это поле в таблице (Рисунок 4-48).
2. Нажмите кнопку **Удалить**, после чего соответствующая запись будет удалена из таблицы.

Примечание:

Следите, чтобы IP-адрес шлюза был указан без ошибок, если был выбран интерфейс на базе IP-адреса (IPoE, IPoA).

4.4.10.3 RIP

Выбрав меню **Дополнительные настройки – Маршрутизация – RIP**, вы увидите следующую страницу (см. Рисунок 4-50).

Маршрутизация – Настройка RIP

ПРИМЕЧАНИЕ: НЕВОЗМОЖНО НАСТРОИТЬ ПРОТОКОЛ RIP на WAN-интерфейсе со включенным NAT (например, PPPoE).

Для включения RIP на WAN-интерфейсе выберите нужную версию RIP и режим , затем отметьте поле 'Включить'. Для остановки RIP на WAN-интерфейсе, снимите галочку с поля 'Включено'. Нажмите кнопку 'Сохранить/Применить' для начала/остановки RIP и сохранения параметров.

Интерфейс	Версия	Режим	Включить
atm0.1	2 ▾	Passive ▾	<input type="checkbox"/>

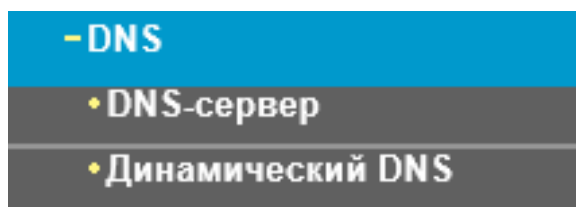
Рисунок 4-50

👉 Примечание:

Нельзя настроить RIP на WAN-интерфейсе со включённым NAT (например, PPPoE).

4.4.11 DNS

Если вы выбрали тип подключения **PPPoE**, **PPPoA** или **IPoA** в настройках WAN, вам будет доступно меню **DNS**, которое содержит разделы **DNS-сервер** и **Динамический DNS**.

**4.4.11.1 DNS-сервер**

На странице **Дополнительные настройки – DNS – DNS-сервер** доступны настройки **DNS-сервера** (см. Рисунок 4-51).

Настройка DNS-сервера

Выберите интерфейс DNS-сервера из доступных интерфейсов WAN или введите статический IP-адрес DNS-сервера для системы. Если в режиме ATM (асинхронный способ передачи данных) настроен только один постоянный виртуальный канал с IPoA или статический IPoE-протокол, необходимо указать IP-адрес DNS сервера.

Интерфейсы DNS-сервера могут иметь несколько интерфейсов WAN, работающих в качестве системных DNS-серверов, но только один из них будет использован согласно приоритету: первый имеет наибольший приоритет, а последний имеет наименьший приоритет, если подключен интерфейс WAN. Порядок приоритетности можно изменять путём удаления всех и обратного их добавления.

- Выбрать интерфейс DNS-сервера из доступных WAN-интерфейсов:**

Выберите интерфейсы DNS-серверов

atm0.3
ppp0.2



Доступные WAN-интерфейсы

- Использовать следующий статический IP-адрес DNS-сервера:**

Предпочитаемый DNS-сервер:

Альтернативный DNS-сервер:

Выберите настроенный WAN-интерфейс для вывода информации по IPv6-адресам DNS-серверов или введите статические IPv6-адреса DNS-серверов. Имейте в виду, что выбор WAN-интерфейса для IPv6-адреса DNS-серверов включит DHCPv6 клиент на этом интерфейсе.

- Получить информацию о IPv6-адресе DNS-сервера от WAN-интерфейса:**

Выбранный WAN-интерфейс:

- Использовать следующий статический IPv6-адрес DNS-сервера:**

Предпочитаемый IPv6-адрес DNS-сервера:

Альтернативный IPv6-адрес DNS-сервера:

Сохранить/Применить

Рисунок 4-51

Для постоянных виртуальных каналов (PVC), настроенных как PPPoA, PPPoE, отметьте строку **Выбрать интерфейс DNS-сервера из доступных интерфейсов WAN**, маршрутизатор автоматически примет первый полученный адрес DNS-сервера от выбранного настроенного WAN-интерфейса во время установки подключения.

Для одного постоянного виртуального канала (PVC), настроенного как IPoA, статический IPoE-протокол выберите **Использовать следующий статический IP-адрес DNS-сервера** и введите IP-адреса предпочитаемого и/или альтернативного (по выбору) DNS-сервера, предоставленные вашим поставщиком Интернет-услуг.

Здесь также можно выбрать настроенный WAN-интерфейс для IPv6 DNS-сервера или ввести статические IPv6-адреса DNS-серверов, предоставленные вашим поставщиком Интернет-услуг.

Нажмите кнопку **Сохранить/Применить** для сохранения проделанных вами настроек.

4.4.11.2 Динамический DNS

На странице **Дополнительные настройки – DNS – Динамический DNS** вам доступны настройки параметров динамического DNS (см. Рисунок 4-52).

Маршрутизатор поддерживает функцию динамической системы доменных имён (**DDNS**), которая позволяет назначить фиксированный узел или доменное имя динамическому IP-адресу Интернет. С помощью динамического DNS можно назначить динамический IP-адрес статическому имени узла в любом из нескольких доменов, что облегчит доступ к маршрутизатору из Интернет.

Dynamic DNS

Функция динамического DNS позволяет задавать динамический IP-адрес статическому узлу в любом из нескольких доменов, облегчая доступ к вашему маршрутизатору с DSL-модемом с разных мест через Интернет.

Для настройки динамического DNS выберите **Добавить** или **Удалить**.

Имя узла	Имя пользователя	Сервис	Интерфейс	Удалить
<input type="button" value="Добавить"/> <input type="button" value="Удалить"/>				

Рисунок 4-52

Чтобы добавить запись DDNS:

1. Нажмите кнопку **Добавить** (см. Рисунок 4-52), после чего вы сможете настроить параметры DDNS на следующей странице (см. Рисунок 4-53).

Добавить Динамический DNS

На данной странице вы сможете добавить адрес Динамического DNS от служб DynDNS.org, TZO или NO-IP.

Поставщик D-DNS:

Имя узла:

Интерфейс:

Настройки No-IP

Имя пользователя:

Пароль:

Рисунок 4-53

2. Выберите **Поставщика D-DNS** из выпадающего списка.
3. Введите **Имя узла** DNS-сервера, затем выберите соответствующий **Интерфейс** для DDNS, можно оставить значение по умолчанию.
4. Введите **Имя пользователя** и **Пароль** для учётной записи DDNS.

Нажмите **Сохранить/Применить** для сохранения ваших настроек.

4.4.12 DSL

На странице **Дополнительные настройки – DSL** вам доступна настройка параметров DSL (см. Рисунок 4-54).

Настройки DSL

Выберите режим модуляции ниже.

- Включить G.Dmt
- Включить G.lite
- Включить T1.413
- Включить ADSL2
- Включить AnnexL
- Включить ADSL2+
- Включить AnnexM

Выберите пару телефонного провода.

- Внутренняя пара
- Внешняя пара

Пропускная способность

- Включить Bitswap
- Включить SRA

Рисунок 4-54

Можно выбрать режим модуляции, пару телефонного провода и пропускную способность Bitswap или SRA. После того, как вы настроили данные параметры, нажмите **Сохранить/Применить** для сохранения настроек.

4.4.13 UPnP

На странице **Дополнительные настройки – UPnP** можно включить или отключить поддержку UPnP (универсальная автоматическая настройка сетевых устройств).

UPnP (Universal Plug and Play) – набор сетевых протоколов, который строится на основе стандартов и технологий интернета, таких как TCP/IP, обеспечивающий быстрый обмен данными между любыми двумя устройствами, находящимися под контролем какого-либо управляющего устройства сети (peer-to-peer). UPnP-устройство может динамически подключиться к сети, получить IP-адрес, передать информацию о себе и получить информацию о других устройствах сети. Кроме того, устройство может легко покинуть сеть и выйти из сети автоматически, если оно больше не используется. Широковещание UPnP возможно только в локальной сети.

UPnP

ПРИМЕЧАНИЕ: Функция UPnP работает только при наличии активного WAN-сервиса со включённым NAT.

Включить UPnP

Рисунок 4-55

Поставьте галочку и нажмите **Сохранить/Применить** для включения функции UPnP.

4.4.14 Группировка портов

На странице **Дополнительные настройки – Группировка портов** можно привязывать постоянные виртуальные каналы (PVC) к определённым портам LAN и соединять группы через мост, каждая группа будет действовать как отдельная сеть.

Группировка портов

Группировка портов позволяет привязывать постоянные виртуальные каналы (PVC) к определённым портам LAN и соединять группы через мост. Каждая группа действует как отдельная сеть. Для этой функции надо с помощью кнопки **Добавить** создать группировку с соответствующими интерфейсами LAN и WAN. Кнопка **Удалить** служит для удаления группировки и добавления не сгруппированных интерфейсов к Основной группе. IP-адрес имеет только основная группа. Можно настроить не более 16 записей.

Имя группы	Удалить	WAN-интерфейс	LAN-интерфейсы	ID DHCP изготовителя
Default	<input type="checkbox"/>	atm0.1 ppp0.2	LAN1 LAN2 LAN3 WLAN1	

Рисунок 4-56

Чтобы данная функция работала, с помощью кнопки **Добавить** необходимо создать группировку с соответствующими интерфейсами LAN и WAN. Кнопка **Удалить** служит для удаления группировки и добавления не сгруппированных интерфейсов к Основной группе. IP-адрес имеет только основная группа.

Чтобы создать новую группировку портов:

1. Нажмите кнопку **Добавить**, затем добавьте новую группировку портов на следующей странице.

Настройка группировки портов

Чтобы создать новую группу интерфейсов:

1. Введите Имя группы. Имя группы должно быть уникальным, выберите 2. (динамический) или 3. (статический):

2. Если вы хотите автоматически добавлять LAN-клиенты к WAN-интерфейсу в новой группе, добавьте DHCP ID изготовителя. Если вы укажете ID DHCP изготовителя, любому запросу DHCP-клиента с указанным ID изготовителя (DHCP опция 60) будет отказано в предоставлении IP-адреса от локального DHCP-сервера.

3. Чтобы создать группировку портов, выберите интерфейсы из списка доступных интерфейсов и добавьте их к списку группируемых интерфейсов с помощью кнопок-стрелок.

Имейте в виду, что эти клиенты могут получать публичный IP-адрес

4. Нажмите Применить/Сохранить, чтобы сделанные вами изменения немедленно вступили в силу

ВНИМАНИЕ: Если ID изготовителя указан для конкретного клиентского устройства, нужно ПЕРЕЗАГРУЗИТЬ клиентское устройство, подключенное к модему, чтобы оно могло получить необходимый IP-адрес.

Имя группы:

WAN-интерфейс, используемый в группировке

Группированные LAN-интерфейсы

LAN1
 LAN2
 LAN3
 WLAN1

Автоматически добавлять клиенты со следующими ID DHCP изготовителя

Рисунок 4-57

2. Введите уникальное имя группы.
3. Из выпадающего списка выберите интерфейс, который вы хотите использовать.

👉 Примечание:

Если вы хотите автоматически добавлять LAN-клиенты к WAN-интерфейсу в новой группе, укажите ID DHCP изготовителя, тогда на запрос DHCP-клиента с указанным ID изготовителя (DHCP опция 60) локальный DHCP-сервер откажет в предоставлении IP-адреса.

4. Выберите интерфейсы из списка доступных интерфейсов и добавьте в список группируемых интерфейсов с помощью кнопок-стрелок для создания группировки портов.

👉 Примечание:

Данные клиенты могут получить публичные IP-адреса.

5. Нажмите **Сохранить/Применить**, чтобы запись вступила в силу немедленно.

👉 Примечание:

Если ID изготовителя указан для конкретного клиентского устройства, нужно ПЕРЕЗАГРУЗИТЬ клиентское устройство, подключенное к модему, чтобы оно могло получить необходимый IP-адрес.

4.4.15 IP-туннель

IPv6-туннель представляет собой переходный механизм, позволяющий передавать IPv6-пакеты через IPv4-сети и обеспечивающий сообщение между изолированными IPv6-узлами и сетями по IPv4-инфраструктуре до того, как IPv6 полностью заменит IPv4. Это временное решение для сетей, которые не поддерживают параллельное использование двух стеков протоколов — IPv6 и IPv4 (dual stack).

Меню **Дополнительные настройки – IP-туннель** содержит два раздела: **IPv6inIPv4** и **IPv4inIPv6**, далее идёт подробное описание этих разделов.

4.4.15.1 IPv6inIPv4

На странице **Дополнительные настройки – IP-туннель – IPv6inIPv4** находятся настройки туннеля 6in4. На данной странице можно настроить статические маршруты (см. Рисунок 4-58).

IP-туннели – Настройка туннеля 6in4

Имя	WAN	LAN	Динамически	Длина маски IPv4	Префикс 6rd	Адрес граничного ретранслятора	Удалить
<input type="button" value="Добавить"/> <input type="button" value="Удалить все"/> <input type="button" value="Удалить"/>							

Рисунок 4-58

Нажмите кнопку **Добавить** (см. Рисунок 4-58) для настройки туннеля 6in4 на следующей странице (см. Рисунок 4-59).

IP-туннелирование – Настройка туннеля 6in4

В настоящий момент возможна настройка только 6rd.

имя туннеля:

Механизм: 6RD

Соответствующий WAN-интерфейс:

Соответствующий LAN-интерфейс: LAN/br0

В ручную Автоматически

Длина маски IPv4:

Префикс 6rd с длиной префикса:

IPv4-адрес граничного ретранслятора:

Рисунок 4-59

- **Механизм: 6RD** – этот тип используется, если у вас подключение WAN использует IPv4-адреса, а в локальной сети используются IPv6-адреса.
- **Соответствующий WAN-интерфейс:** Выберите подключение WAN из выпадающего списка. В выпадающем списке указаны только установленные подключения WAN.
- **Соответствующий LAN-интерфейс:** Выберите подключение LAN из выпадающего списка. В выпадающем списке указаны только активные подключения LAN.
- **Длина маски IPv4:** Длина маски IPv4 выбранного подключения WAN.
- **Префикс 6rd с длиной префикса:** Длина 6rd префикса.

- **IPv4-адрес граничного ретранслятора:** IPv4-адрес граничного маршрутизатора туннеля 6RD, ретранслирующего IPv6-адреса в IPv4-адреса.

Нажмите **Сохранить/Применить** для вступления настроек в силу.

 **Примечание:**

В этом случае не должно быть IPv6 WAN-подключений, если таковые имеются, появится уведомление с требованием удалить их.

4.4.15.2 IPv4inIPv6

На странице **Дополнительные настройки – IP-туннель – IPv4inIPv6** находятся настройки туннеля 4in6. На данной странице можно настроить статические маршруты (см. Рисунок 4-60).

IP-туннели – Настройка туннеля 4in6

Имя	WAN	LAN	Динамически	AFTR	Удалить

Рисунок 4-60

Нажмите кнопку **Добавить** (см. Рисунок 4-60) для настройки туннеля 4in6 на следующей странице (см. Рисунок 4-61).

IP-туннелирование – Настройка туннеля 4in6

В настоящий момент возможна настройка только DS-Lite.

Имя туннеля:

Механизм: DS-Lite ▼

Соответствующий WAN-интерфейс: ▼

Соответствующий LAN-интерфейс: LAN/br0 ▼

В ручную Автоматически

AFTR:

Рисунок 4-61

- **Механизм:** DS-Lite – этот тип используется, если у вас подключение WAN использует IPv6-адреса, а в локальной сети используются IPv4-адреса
- **Соответствующий WAN-интерфейс:** Выберите подключение WAN из выпадающего списка. В выпадающем списке указаны только установленные подключения WAN
- **Соответствующий LAN-интерфейс:** Выберите подключение LAN из выпадающего списка. В выпадающем списке указаны только активные подключения LAN.
- **AFTR:** Укажите IPv6-адрес удалённого узла.

Нажмите **Сохранить/Применить** для вступления настроек в силу.

Примечание:

В этом случае не должно быть IPv4 WAN-подключений, если таковые имеются, появится уведомление с требованием удалить их.

4.4.16 IPSec

На странице **Дополнительные настройки – IPSec** можно **Добавить/Удалить** или **Включить/Отключить** соединения IPSec-туннель на следующей странице (см. Рисунок 4-62).

Соединения в режиме IPSec-туннеля

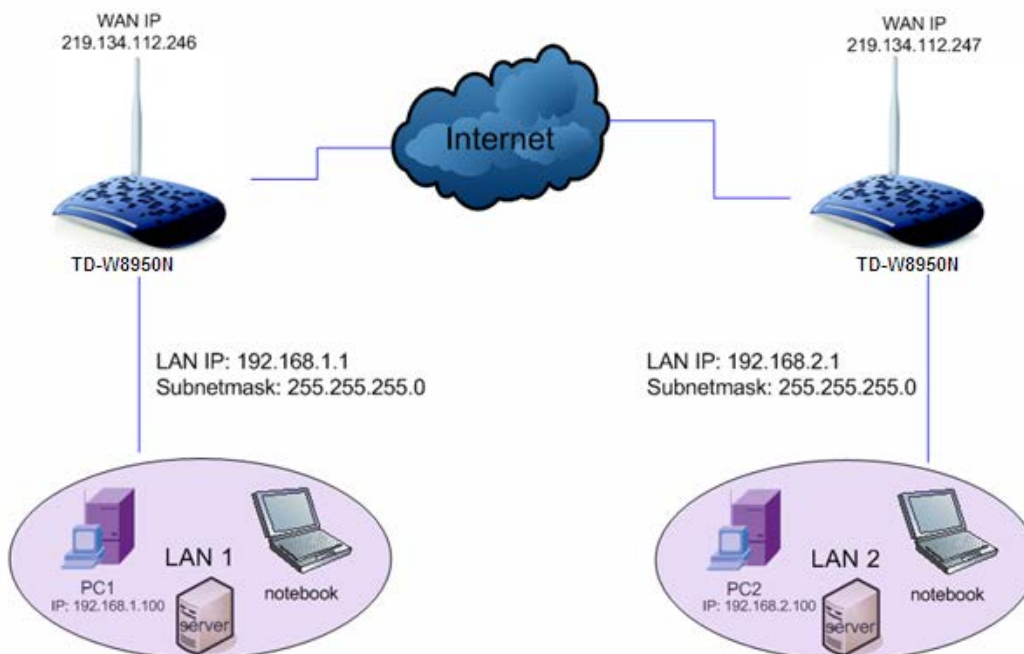
Добавить, удалить или включить/отключить соединения через IPSec-туннель с этой страницы.

DPD - Обнаружение мёртвого узла **(Внимание! Может негативно влиять на стабильность соединения)**

Имя соединения	Удалённый шлюз	Локальный адрес	Удалённый адрес	Состояние	Включить/Отключить	Изменить	Удалить

Рисунок 4-62

В данном разделе показано, как настроить VPN-туннель между двумя маршрутизаторами **TD-W8950N**. Схема показана ниже.



Примечание:

Можно использовать другие VPN-маршрутизаторы для настройки VPN-туннелей с **TD-W8950N**. **TD-W8950N** поддерживает до 10 VPN-туннелей одновременно.

Нажмите **Добавить новое соединение** (см. Рисунок 4-62), после чего откроется следующая страница (см. Рисунок 4-63).

Настройки IPSec

Имя IPSec-соединения:	<input type="text" value="new connection"/>
Адрес (URL/IPv4) удалённого IPSec-шлюза:	<input type="text" value="0.0.0.0"/>
Туннельный доступ с локального IP-адреса:	<input type="text" value="Подсеть"/> ▼
IP-адрес для VPN:	<input type="text" value="0.0.0.0"/>
Маска подсети IP-адреса:	<input type="text" value="255.255.255.0"/>
Туннельный доступ с удалённого IP-адреса:	<input type="text" value="Подсеть"/> ▼
IP-адрес для VPN:	<input type="text" value="0.0.0.0"/>
Маска подсети IP-адреса:	<input type="text" value="255.255.255.0"/>
Метод обмена ключами:	<input type="text" value="Автоматически (IKE)"/> ▼
Метод аутентификации:	<input type="text" value="Пароль беспроводной"/> ▼
Пароль беспроводной сети:	<input type="text" value="key"/>
Совершенная прямая секретность:	<input type="text" value="Отключить"/> ▼
Дополнительные настройки IKE:	<input type="text" value="Дополнительные настройки"/>

Рисунок 4-63

- **Имя IPSec-соединения:** Укажите имя VPN-соединения.
- **Адрес удалённого IPSec-шлюза (IP или доменное имя):** Укажите IP-адрес шлюза назначения, которым является публичный WAN IP-адрес или доменное имя конечного удалённого VPN-сервера (Например, введите **219.134.112.247** для **первого устройства 1**, введите **219.134.112.246** для **второго устройства**).
- **Туннельный доступ с локального IP-адреса:** Выберите Подсеть, если вы хотите подключить всю локальную сеть к VPN-сети или выберите Одиночный адрес, если вы хотите, чтобы только один IP-адрес подключался к VPN-сети.
- **IP-адрес для VPN:** Введите IP-адрес вашей локальной сети (Например: **192.168.1.1** для **первого устройства** и **192.168.2.1** для **второго устройства**).
- **Маска подсети IP-адреса:** Укажите маску подсети вашей локальной сети (Например, введите **255.255.255.0** для **первого устройства** и для **второго устройства**).
- **Туннельный доступ с удалённого IP-адреса:** Выберите Подсеть, если вы хотите подключить всю удалённую локальную сеть к VPN-сети или выберите Одиночный адрес, если вы хотите, чтобы только один IP-адрес подключался к VPN-сети.
- **IP-адрес для VPN:** Введите IP-адрес удалённой локальной сети (Например, **192.168.2.1** для **первого устройства** и **192.168.1.1** для **второго устройства**).
- **Маска подсети IP-адреса:** Введите маску подсети удалённой локальной сети (Например, **255.255.255.0** для **первого устройства** и для **второго устройства**).
- **Метод обмена ключами:** Выберите Авто (IKE) или Вручную.
- **Метод аутентификации:** Выберите Пароль беспроводной сети (рекомендуется).

- **Pre-Shared Key:** Для аутентификации введите Pre-Shared Key (Например: 12345678).
- **Совершенная прямая секретность:** PFS (Совершенная прямая секретность) представляет собой дополнительный протокол защиты.

Рекомендуется оставить значения по умолчанию в дополнительных настройках.

После того, как основные настройки завершены, и кнопка **Сохранить/Применить** для **первого** и для **второго устройства** была нажата, компьютеры первой локальной сети смогут обмениваться данными с компьютерами второй удалённой локальной сети (например: можно отправить запрос ping на IP-адрес второго компьютера – 192.168.2.100 – с первого компьютера).

 **Примечание:**

Обе конечные точки VPN-серверов должны использовать одинаковый пароль беспроводной сети и одинаковые настройки совершенной прямой секретности.

Нажмите кнопку **Дополнительные настройки**, после чего будут показаны дополнительные.

Дополнительные настройки IKE: Скрыть дополнительные настройки

Фаза 1

Режим:

Тип моего идентификатора:

Мой идентификатор:

Тип удалённого идентификатора:

Удалённый идентификатор:

Алгоритм шифрования:

Алгоритм проверки целостности:

Выберите группу Диффи-Хеллмана для обмена ключами:

Срок действия ключа: Секунд

Фаза 2

Алгоритм шифрования:

Алгоритм проверки целостности:

Срок действия ключа: Секунд

Рисунок 4-64

- **Основной режим:** Выберите Основной режим для настройки параметров стандартного обмена данными для IKE фаза 1.
- **Агрессивный режим:** Выберите этот режим для настройки параметров IKE фаза 1 VPN-туннеля для осуществления более быстрого обмена данными (этот вариант не рекомендуется из-за менее надёжной защиты).

 **Примечание:**

Разница между этими режимами заключается в том, что агрессивный режим пропускает больше данных в меньшем количестве пакетов, преимущество в том, что соединение устанавливается немного быстрее в агрессивном режиме, поскольку защитные маркеры межсетевого экрана передаются в открытую. При использовании агрессивного режима информация о некоторых параметрах (например, группы Диффи-Хеллмана, и PFS) не может быть передана, поэтому в этом случае очень важно, чтобы настройки совпадали на обоих «концах» сети.

➤ **Срок действия ключа:**

Введите количество секунд для срока действия IPsec. Это период времени, который должен пройти перед тем, как будет установлено новое сопоставление безопасности (SA) IPsec с удалённой конечной точкой. Значение по умолчанию: 3600.

 **Примечание:**

Если вы хотите изменить настройки по умолчанию в **Дополнительных настройках**, убедитесь, что обе конечные точки VPN-серверов используют одинаковый Алгоритм шифрования, Алгоритм проверки целостности, группу Диффи-Хеллмана и Срок действия ключа в **Фазе 1** и **Фазе 2**.

4.4.17 Multicast

На странице **Дополнительные настройки – Multicast** можно настроить протокол **IGMP**.

Настройка IGMP

Введите параметры протокола IGMP в нижеследующих полях, если вы хотите изменить настройки по умолчанию.

Версия по умолчанию:	3
Интервал запросов:	125
Интервал ожидания ответа на запросы:	10
Интервал запроса для последнего участника:	10
Переменная надёжности:	2
Максимальное кол-во multicast-групп:	25
Максимальное кол-во multicast-источников (для IGMP версии 3 : (1 - 24)):	10
Максимальное кол-во участников multicast-групп:	25
Включить Fast Leave:	<input checked="" type="checkbox"/>
Включить LAN-LAN Multicast (внутри LAN):	<input type="checkbox"/>

Рисунок 4-65

Нажмите **Применить/Сохранить** для сохранения ваших настроек.

4.5 IPTV

При выборе **IPTV** откроется страница, как указано на Рисунок 4-66.

IPTV

Включить IPTV

Выберите порт LAN, который будет использоваться для IPTV, и подключите ТВ-приставку к этому порту.

LAN1 LAN2 LAN3

Включить беспроводное соединение для IPTV

Примечание: Когда порт WLAN настроен для IPTV-соединения, функция беспроводного вещания доступна только для IPTV-соединения.

WLAN2 WLAN3

Укажите параметры постоянного виртуального канала (PVC) для IPTV.

VPI:	<input type="text" value="0"/>	(0-255)
VCI:	<input type="text" value="35"/>	(1-65535)

Включить Гарантированную пропускную способность для IPTV

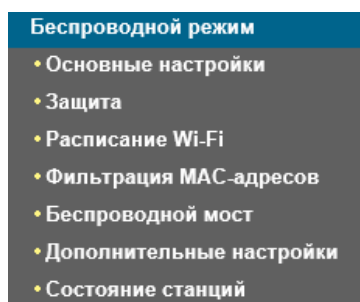
Функция контроля пропускной способности устройства отключена, нажмите [здесь](#), чтобы включить её.

Рисунок 4-66

- **Включить IPTV:** Отметьте данное поле, чтобы включить IPTV. Если данное поле отмечено, укажите настройки, указанные на изображении. Убедитесь, что вы указали верные значения.
- **VPI (0-255):** Определяет виртуальный путь между конечными точками в сети ATM. Допустимый диапазон: от 0 до 255. Пожалуйста, укажите значения, предоставленные вашим поставщиком Интернет-услуг.
- **VCI (1-65535):** Определяет конечные точки виртуального канала в сети ATM. Допустимый диапазон: от 1 до 65535 (Диапазон от 1 до 31 зарезервирован под различные известные протоколы). Пожалуйста, укажите значения, предоставленные вашим поставщиком Интернет-услуг.
- Нажмите кнопку **Сохранить/Применить** для сохранения настроек.

4.6 Беспроводной режим

Раздел меню **Беспроводной режим** содержит 7 подменю настройки параметров беспроводной сети. При выборе соответствующего подменю вы сможете настроить соответствующую функцию. Подробное описание каждого пункта представлено ниже.



4.6.1 Основные настройки

При выборе **Беспроводной режим – Основные настройки** откроется окно, как указано на рисунке ниже. Основные настройки беспроводной сети указаны на данном рисунке.

Беспроводной режим – Основные настройки

На данной странице можно настроить основные параметры беспроводного режима LAN-интерфейса. Вы можете включить/отключить беспроводное вещание, скрыть сеть от активного сканирования, указать имя беспроводной сети (также называется SSID) и запретить настройку каналов согласно региональным требованиям. Нажмите "Сохранить/Применить", чтобы настройки базовых параметров беспроводного режима вступили в силу.

Включить беспроводное вещание
 Скрыть широковещание SSID
 Изолирование клиентов

SSID1:
 SSID2: Включить
 SSID3: Включить
 BSSID: 02:10:18:63:18:08
 Страна:

Рисунок 4-67

На данной странице вы сможете настроить основные параметры беспроводного режима LAN-интерфейса. Вы можете включить/отключить беспроводное вещание, скрыть сеть от активного сканирования, указать имя беспроводной сети (SSID) и запретить настройку каналов согласно региональным требованиям.

- **Включить беспроводное вещание:** Если вы хотите использовать функцию беспроводного вещания, вам необходимо отметить данное поле. Если вы снимете отметку с данного поля, все нижеуказанные настройки беспроводного вещания будут отключены.
- **Скрыть широковещание SSID:** Вы можете выбрать данную настройку, чтобы ваша сеть не появлялась в результатах при поиске беспроводных сетей пользователями беспроводных устройств.
- **Изолирование клиентов:** Отметьте данное поле для включения функции изолирования точки доступа, чтобы станции, подключаемые к точке доступа, не могли взаимодействовать друг с другом.
- **Имя беспроводной сети:** Имя беспроводной сети, используемое всеми точками в беспроводной сети. Имя беспроводной сети (SSID) должно быть одинаковым для всех устройств в беспроводной сети. Данное поле является чувствительным к регистру и не должно превышать 32 знака (могут быть использованы любые знаки на клавиатуре). Убедитесь, что данные настройки являются одинаковыми для всех станций в вашей

беспроводной сети. Укажите необходимое значение имени беспроводной сети (SSID) в данном поле.

- **BSSID:** Отображает MAC-адрес модема со встроенным маршрутизатором
- **Страна:** Разные страны могут иметь определённые ограничения на настройку канала и мощность передатчика.

Нажмите **Сохранить/Применить** для сохранения ваших настроек.

4.6.2 Защита

При выборе **Беспроводной режим – Защита** перед вами откроется страница, как указано ниже. На данной странице вы сможете настроить параметры безопасности беспроводного режима LAN-интерфейса, вручную указав метод сетевой аутентификации или с помощью функции **WPS** (Настройка защищённого Wi-Fi).

Беспроводной режим – Защита

На этой странице можно настроить параметры защиты беспроводной локальной сети. Вы можете настроить параметры вручную или с помощью функции WPS (Настройка защищённого Wi-Fi)

WPS

Включить WPS:

Добавить клиента (Данная функция доступна только, если были выбраны режимы защиты WPA-PSK, WPA2-PSK или Открытая система)

Кнопка WPS
 PIN-код

[Справка](#)

PIN-код устройства:

[Справка](#)

Настроить точку доступа вручную

В целях защиты сети от хакеров и неавторизованных пользователей настоятельно рекомендуется выбрать один из указанных ниже типов защиты беспроводной сети. Вы можете настроить метод сетевой аутентификации, выбрать шифрование, указать, нужно ли вводить пароль для входа в беспроводную сеть, а также выбрать степень надёжности шифрования.

Внимание: Не рекомендуется выбирать шифрование WEP, если устройство работает в режиме 11n. Если выбран WEP, то максимальная скорость передачи данных составляет до 54 Мбит/с.

Примечание: Режим "только 11n" не поддерживается при использовании шифрования WEP или если тип шифрования WPA выбран "TKIP".

Примечание: Нельзя выбирать "TKIP" для "шифрования WPA", если устройство работает в режиме "только 11n". Когда укажете необходимые настройки, нажмите "Сохранить/Применить".

Выберите SSID:

Сетевая аутентификация:

WEP Encryption:

Рисунок 4-68

4.6.2.1 настройки WPS

Этом раздел поможет вам быстро добавить новое беспроводного устройство к существующей сети с помощью функции WPS (или QSS).

Примечание:

- 1) Данная функция возможна только при выборе режима Открытая система, WPA-PSK, WPA2-PSK или Смешанная WPA2/WPA-PSK.
- 2) Для осуществления успешного соединения с помощью WPS вам также потребуется произвести соответствующие настройки нового устройства для функции WPS.

I. С помощью кнопки WPS

Если беспроводной маршрутизатор поддерживает функцию WPS и возможность подключения нажатием кнопки, вы можете добавить его к сети при помощи двух следующих способов. При выборе поля **Кнопка WPS** перед вами появится страница, как указано ниже.

Беспроводной режим – Защита

На этой странице можно настроить параметры защиты беспроводной локальной сети. Вы можете настроить параметры вручную или с помощью функции WPS (Настройка защищённого Wi-Fi)

WPS

Включить WPS:

Добавить клиента (Данная функция доступна только, если были выбраны режимы защиты WPA-PSK, WPA2-PSK или Открытая система)

Кнопка WPS
 PIN-код

код [Справка](#)

[Справка](#)

Настроить точку доступа вручную

В целях защиты сети от хакеров и неавторизованных пользователей настоятельно рекомендуется выбрать один из указанных ниже типов защиты беспроводной сети. Вы можете настроить метод сетевой аутентификации, выбрать шифрование, указать, нужно ли вводить пароль для входа в беспроводную сеть, а также выбрать степень надёжности шифрования. **Внимание: Не рекомендуется выбирать шифрование WEP, если устройство работает в режиме 11n. Если выбран WEP, то максимальная скорость передачи данных составляет до 54 Мбит/с.**

Примечание: Режим "только 11n" не поддерживается при использовании шифрования WEP или если тип шифрования WPA выбран "TKIP".
 Примечание: Нельзя выбирать "TKIP" для шифрования WPA, если устройство работает в режиме "только 11n".
 Когда укажете необходимые настройки, нажмите "Сохранить/Применить".

Выберите SSID:

Сетевая аутентификация:

Пароль беспроводной сети: (Также называется Общий ключ WPA)
[Показать пароль](#)
 (Введите значение длиной от 8 до 63 символов в кодировке ASCII или от 8 до 64 шестнадцатеричных чисел.)

Период обновления пароля беспроводной сети: (не обязательно)

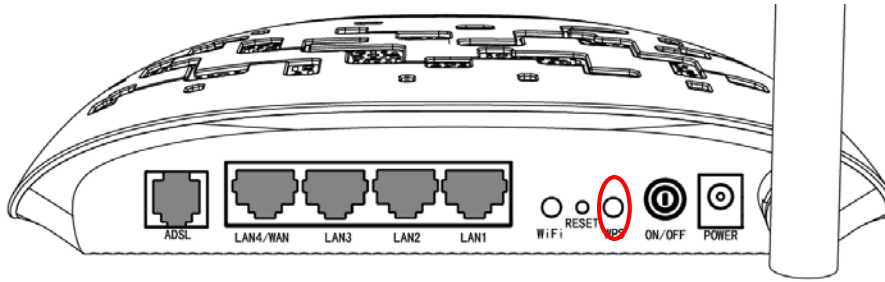
Шифрование WPA:

WEP Encryption:

Рисунок 4-69

Первый способ: Нажатием кнопки.

Шаг 1: Нажмите кнопку WPS на задней панели маршрутизатора.



Шаг 2: Нажмите и удерживайте кнопку WPS на адаптере в течение 2-3 секунд.



Шаг 3: Подождите некоторое время, пока на мониторе не появится окно адаптера. Нажмите **Завершить** для завершения настройки **WPS**.

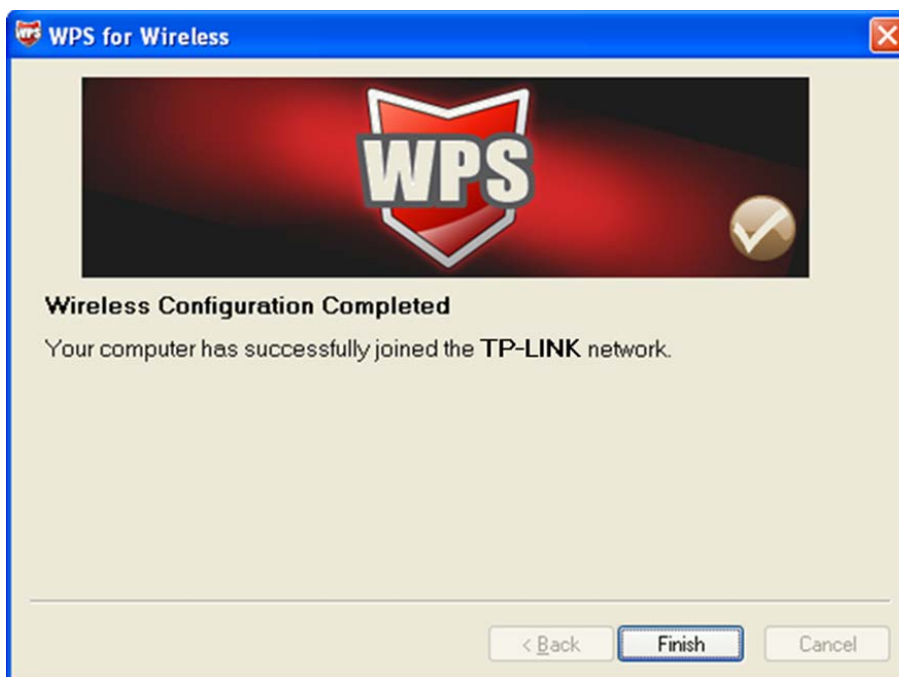
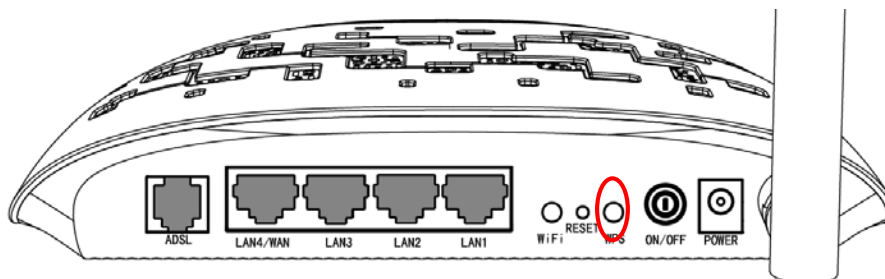


Рисунок 4-70

Второй способ:

Шаг 1: Нажмите кнопку WPS на задней панели маршрутизатора.



Шаг 2: Для настройки беспроводного адаптера выберите **“Нажать кнопку на моей точке доступа”** в утилите настройки WPS как показано ниже, затем нажмите **Далее**.

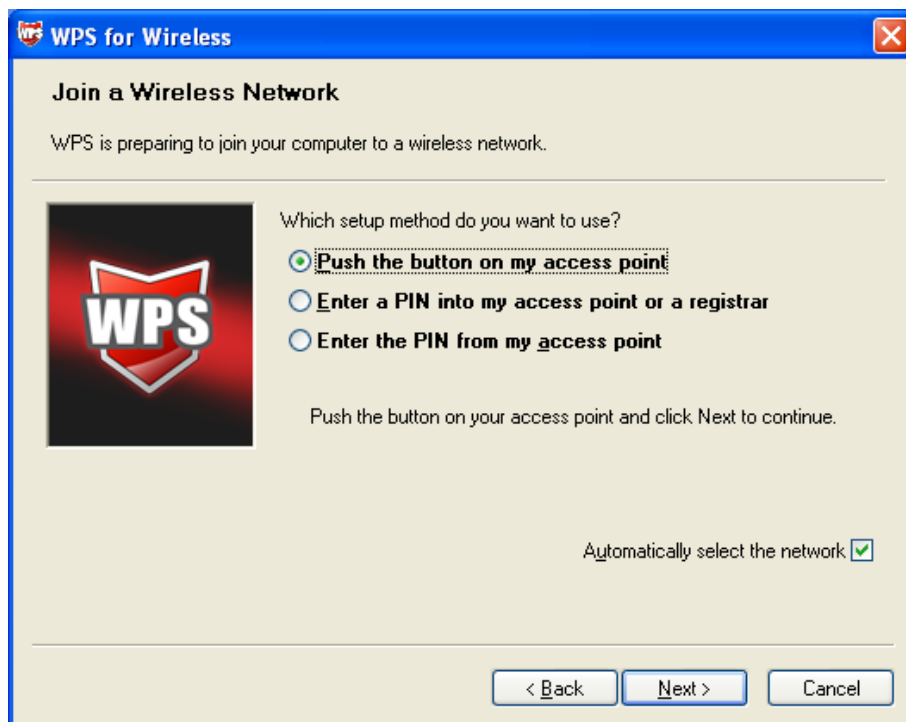


Рисунок 4-71

Шаг 3: Подождите некоторое время, пока на мониторе не появится следующее окно. Нажмите **Завершить** для завершения настройки **WPS**.

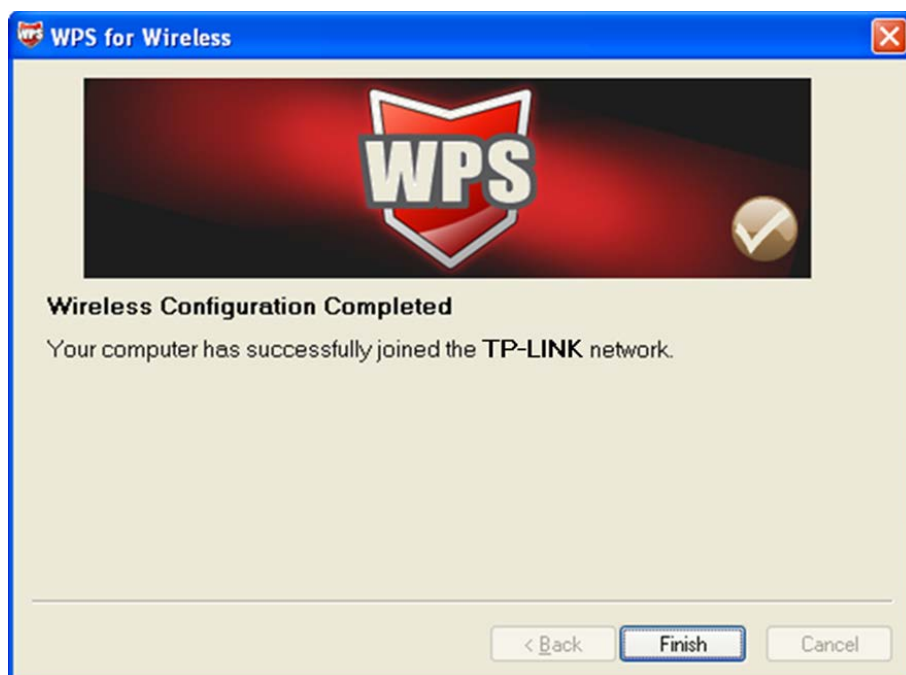


Рисунок 4-72

II. Через PIN

Если добавляемое новое устройство поддерживает функцию WPS и аутентификацию через PIN-код, вы можете добавить его в сеть с помощью PIN-кода двумя следующими способами.

Первый способ: Введите PIN-код беспроводного адаптера на маршрутизаторе.

Шаг 1: Отметьте поле **PIN-код** и введите PIN-код беспроводного адаптера в поле, указанном на изображении ниже. Затем нажмите **Добавить устройство**.

Беспроводной режим – Защита

На этой странице можно настроить параметры защиты беспроводной локальной сети. Вы можете настроить параметры вручную или с помощью функции WPS (Настройка защищённого Wi-Fi)

WPS

Включить WPS:

Добавить клиента (Данная функция доступна только, если были выбраны режимы защиты WPA-PSK, WPA2-PSK или Открытая система)

Кнопка WPS
 PIN-

код [Справка](#)

[Справка](#)

Настроить точку доступа вручную

В целях защиты сети от хакеров и неавторизованных пользователей настоятельно рекомендуется выбрать один из указанных ниже типов защиты беспроводной сети. Вы можете настроить метод сетевой аутентификации, выбрать шифрование, указать, нужно ли вводить пароль для входа в беспроводную сеть, а также выбрать степень надёжности шифрования. **Внимание: Не рекомендуется выбирать шифрование WEP, если устройство работает в режиме 11n. Если выбран WEP, то максимальная скорость передачи данных составляет до 54 Мбит/с.**
 Примечание: Режим "только 11n" не поддерживается при использовании шифрования WEP или если тип шифрования WPA выбран "TKIP".
 Примечание: Нельзя выбирать "TKIP" для шифрования WPA, если устройство работает в режиме "только 11n".
 Когда укажете необходимые настройки, нажмите "Сохранить/Применить".

Выберите SSID:

Сетевая аутентификация:

Пароль беспроводной сети: (Также называется Общий ключ WPA)
[Показать пароль](#)
 (Введите значение длиной от 8 до 63 символов в кодировке ASCII или от 8 до 64 шестнадцатеричных чисел.)

Период обновления пароля беспроводной сети: (не обязательно)

Шифрование WPA:

WEP Encryption:

Рисунок 4-73

Примечание:

PIN-код адаптера всегда отображается на странице настройки WPS.

Шаг 2: Для настройки беспроводного адаптера выберите **“Ввести PIN-код на моей точке доступа/маршрутизаторе”** в окне утилиты WPS, как показано ниже, затем нажмите **Далее**.



Рисунок 4-74

Примечание:

В данном примере PIN-кодом по умолчанию является 16952898, как указано на изображении выше.

Метод второй: Ввести PIN-код маршрутизатора на беспроводном адаптере.

Шаг 1: Получить PIN-код, сгенерированный маршрутизатором, как указано ниже. Нажмите **Создать новый PIN**, чтобы получить новый PIN-код для вашего маршрутизатора.

Беспроводной режим – Защита

На этой странице можно настроить параметры защиты беспроводной локальной сети. Вы можете настроить параметры вручную или с помощью функции WPS (Настройка защищённого Wi-Fi)

WPS

Включить WPS:

Добавить клиента (Данная функция доступна только, если были выбраны режимы защиты WPA-PSK, WPA2-PSK или Открытая система)

Кнопка WPS PIN-код

[Справка](#)

PIN-код устройства: [Справка](#)

Настроить точку доступа вручную

В целях защиты сети от хакеров и неавторизованных пользователей настоятельно рекомендуется выбрать один из указанных ниже типов защиты беспроводной сети. Вы можете настроить метод сетевой аутентификации, выбрать шифрование, указать, нужно ли вводить пароль для входа в беспроводную сеть, а также выбрать степень надёжности шифрования. **Внимание: Не рекомендуется выбирать шифрование WEP, если устройство работает в режиме 11n. Если выбран WEP, то максимальная скорость передачи данных составляет до 54 Мбит/с.**

Примечание: Режим "только 11n" не поддерживается при использовании шифрования WEP или если тип шифрования WPA выбран "TKIP".
 Примечание: Нельзя выбирать "TKIP" для "шифрования WPA", если устройство работает в режиме "только 11n".
 Когда укажете необходимые настройки, нажмите "Сохранить/Применить".

Выберите SSID:

Сетевая аутентификация:

Пароль беспроводной сети: (Также называется Общий ключ WPA)

[Показать пароль](#)
 (Введите значение длиной от 8 до 63 символов в кодировке ASCII или от 8 до 64 шестнадцатеричных чисел.)

Период обновления пароля беспроводной сети: (не обязательно)

Шифрование WPA:

WEP Encryption:

Рисунок 4-75

Шаг 2: Для настройки беспроводного адаптера, пожалуйста, выберите **“Ввести PIN-код моей точки доступа/маршрутизатора”** в утилите настройки WPS, как указано ниже, после чего введите PIN-код маршрутизатора в поле **PIN-код точки доступа**, затем нажмите **Далее**.

Рисунок 4-76

4.6.2.2 Настроить точку доступа вручную

Следуйте нижеуказанным инструкциям для ручной настройки параметров безопасности беспроводного режима LAN-интерфейса. Вы можете выбрать режим сетевой аутентификации, выбрать способ шифрования данных, указать необходимость использования сетевого ключа для аутентификации в данной беспроводной сети и выбрать уровень шифрования.

Беспроводной режим – Защита

На этой странице можно настроить параметры защиты беспроводной локальной сети. Вы можете настроить параметры вручную или с помощью функции WPS (Настройка защищённого Wi-Fi)

WPS

Включить WPS:

Добавить клиента (Данная функция доступна только, если были выбраны режимы защиты WPA-PSK, WPA2-PSK или Открытая система)

Кнопка WPS PIN-код

[Справка](#)

PIN-код устройства: [Справка](#)

Настроить точку доступа вручную

В целях защиты сети от хакеров и неавторизованных пользователей настоятельно рекомендуется выбрать один из указанных ниже типов защиты беспроводной сети. Вы можете настроить метод сетевой аутентификации, выбрать шифрование, указать, нужно ли вводить пароль для входа в беспроводную сеть, а также выбрать степень надёжности шифрования. **Внимание: Не рекомендуется выбирать шифрование WEP, если устройство работает в режиме 11n. Если выбран WEP, то максимальная скорость передачи данных составляет до 54 Мбит/с.**

Примечание: Режим "только 11n" не поддерживается при использовании шифрования WEP или если тип шифрования WPA выбран "TKIP".
Примечание: Нельзя выбирать "TKIP" для "шифрования WPA", если устройство работает в режиме "только 11n".
Когда укажете необходимые настройки, нажмите "Сохранить/Применить".

Выберите SSID:

Сетевая аутентификация:

Пароль беспроводной сети: (Также называется Общий ключ WPA)

[Показать пароль](#)
(Введите значение длиной от 8 до 63 символов в кодировке ASCII или от 8 до 64 шестнадцатеричных чисел.)

Период обновления пароля беспроводной сети: (не обязательно)

Шифрование WPA:

WEP Encryption:

Рисунок 4-77

Сетевая аутентификация: Выберите тип аутентификации из выпадающего списка. Возможные варианты: Open, Shared, WPA, WPA-PSK, WPA2, WPA2-PSK, Смешанная WPA2/WPA и Смешанная WPA2/WPA-PSK.

Примечание:

Для большинства пользователей рекомендуется использовать настройки беспроводного режима LAN-интерфейса по умолчанию. Изменения, применяемые к данным настройкам, могут негативно повлиять на производительность вашей беспроводной сети. При некоторых обстоятельствах настройки могут улучшить работу беспроводной сети. Прежде чем вносить изменения в настройки, внимательно подумайте и оцените их возможные последствия.

1. WEP

WEP – это базовый способ шифрования, обеспечивающий два уровня шифрования: 64-битный и 128-битный. Чтобы настроить шифрование WEP, есть два пути.

- Выберете тип Сетевой аутентификации **Открытая система (без защиты)** и выберите **Включено** из выпадающего списка шифрования WEP, как указано на Рис. 4-83. Тип Сетевой аутентификации **Открытая система (без защиты)** с

отключённым шифрованием WEP позволит любой беспроводной станции подключаться к точке доступа.

- Выберите **Общая система (с защитой)** из выпадающего списка шифрования WEP, как указано на Рис. 4-84. **Общая система (с защитой)** должна обеспечивать шифрование WEP. Сеть, использующая Открытую или Общую систему аутентификации с шифрованием WEP, позволит станциям использовать один ключ шифрования для подключения. Следуйте нижеуказанной инструкции для настройки Общих ключей.

Беспроводной режим – Защита

На этой странице можно настроить параметры защиты беспроводной локальной сети. Вы можете настроить параметры вручную или с помощью функции WPS (Настройка защищённого Wi-Fi)

WPS

Включить WPS:

Настроить точку доступа вручную

В целях защиты сети от хакеров и неавторизованных пользователей настоятельно рекомендуется выбрать один из указанных ниже типов защиты беспроводной сети. Вы можете настроить метод сетевой аутентификации, выбрать шифрование, указать, нужно ли вводить пароль для входа в беспроводную сеть, а также выбрать степень надёжности шифрования. **Внимание: Не рекомендуется выбирать шифрование WEP, если устройство работает в режиме 11n. Если выбран WEP, то максимальная скорость передачи данных составляет до 54 Мбит/с.** Примечание: Режим "только 11n" не поддерживается при использовании шифрования WEP или если тип шифрования WPA выбран "TKIP". Примечание: Нельзя выбирать "TKIP" для шифрования WPA, если устройство работает в режиме "только 11n". Когда укажете необходимые настройки, нажмите "Сохранить/Применить".

Выберите SSID:

Сетевая аутентификация:

WEP Енспуртион:

Шифрование WEP:

Текущий пароль сети:

Сетевой пароль 1:

Сетевой пароль 2:

Сетевой пароль 3:

Сетевой пароль 4:

Введите 13 символов в кодировке ASCII или 26 шестнадцатеричных числа для 128-битных ключей шифрования
Введите 5 символов в кодировке ASCII или 10 шестнадцатеричных чисел для 64-битных ключей шифрования

Рисунок 4-78

Беспроводной режим – Защита

На этой странице можно настроить параметры защиты беспроводной локальной сети. Вы можете настроить параметры вручную или с помощью функции WPS (Настройка защищённого Wi-Fi)

WPS

Включить WPS:

Настроить точку доступа вручную

В целях защиты сети от хакеров и неавторизованных пользователей настоятельно рекомендуется выбрать один из указанных ниже типов защиты беспроводной сети. Вы можете настроить метод сетевой аутентификации, выбрать шифрование, указать, нужно ли вводить пароль для входа в беспроводную сеть, а также выбрать степень надёжности шифрования. **Внимание: Не рекомендуется выбирать шифрование WEP, если устройство работает в режиме 11n. Если выбран WEP, то максимальная скорость передачи данных составляет до 54 Мбит/с.**

Примечание: Режим "только 11n" не поддерживается при использовании шифрования WEP или если тип шифрования WPA выбран "TKIP".
Примечание: Нельзя выбирать "TKIP" для "шифрования WPA", если устройство работает в режиме "только 11n".
Когда укажете необходимые настройки, нажмите "Сохранить/Применить".

Выберите SSID:

Сетевая аутентификация:

WEP Енсгуртион:

Шифрование WEP:

Текущий пароль сети:

Сетевой пароль 1:

Сетевой пароль 2:

Сетевой пароль 3:

Сетевой пароль 4:

Введите 13 символов в кодировке ASCII или 26 шестнадцатеричных числа для 128-битных ключей шифрования
Введите 5 символов в кодировке ASCII или 10 шестнадцатеричных чисел для 64-битных ключей шифрования

Рисунок 4-79

- **Шифрование WEP:** Выберите соответствующий уровень защиты, 64-битный или 128-битный.
- **Текущий пароль сети:** Чтобы указать, какой ключ использовать, выберите номер ключа передачи.
- **Сетевой пароль 1-4:** Если вы хотите вручную указать ключи WEP, введите их в полях Сетевой пароль 1-4.

Настройка параметров WEP

1. Выберите **Общая система (с защитой)**
2. Выберите **Общая система (с защитой)** из выпадающего списка **Сетевая аутентификация**, после чего в меню появятся новые разделы для соответствующих настроек.
3. Выберите **64-бит** из выпадающего списка **Шифрование WEP**.
4. Выберите **“1”** из выпадающего списка **Текущий пароль сети**.
5. Введите пароль в поле **Сетевой пароль 1**.
6. Нажмите **Сохранить/Применить** для сохранения новых настроек.

Беспроводной режим – Защита

На этой странице можно настроить параметры защиты беспроводной локальной сети. Вы можете настроить параметры вручную или с помощью функции WPS (Настройка защищённого Wi-Fi)

WPS

Включить WPS:

Настроить точку доступа вручную

В целях защиты сети от хакеров и неавторизованных пользователей настоятельно рекомендуется выбрать один из указанных ниже типов защиты беспроводной сети. Вы можете настроить метод сетевой аутентификации, выбрать шифрование, указать, нужно ли вводить пароль для входа в беспроводную сеть, а также выбрать степень надёжности шифрования. **Внимание: Не рекомендуется выбирать шифрование WEP, если устройство работает в режиме 11n. Если выбран WEP, то максимальная скорость передачи данных составляет до 54 Мбит/с.** Примечание: Режим "только 11n" не поддерживается при использовании шифрования WEP или если тип шифрования WPA выбран "TKIP". Примечание: Нельзя выбирать "TKIP" для шифрования WPA, если устройство работает в режиме "только 11n". Когда укажете необходимые настройки, нажмите "Сохранить/Применить".

Выберите SSID:

Сетевая аутентификация:

WEP Енскрипцион:

Шифрование WEP:

Текущий пароль сети:

Сетевой пароль 1:

Сетевой пароль 2:

Сетевой пароль 3:

Сетевой пароль 4:

Введите 13 символов в кодировке ASCII или 26 шестнадцатеричных числа для 128-битных ключей шифрования
Введите 5 символов в кодировке ASCII или 10 шестнадцатеричных чисел для 64-битных ключей шифрования

Рисунок 4-80

Примечание:

В данном руководстве для примера используется следующий вариант настроек: **Сетевая аутентификация** - **Общая система (с защитой)**, **Степень надёжности** - **64-бит**, **Текущий пароль сети** - **“1”** и **Сетевой пароль 1** из 10 шестнадцатеричных чисел “1234567890” (см. Рисунок 4-80).

2. WPA-Enterprise

Защита WPA для беспроводного соединения разработана с целью устранить недостатки технологии WEP. WPA сочетает генерирование пароля вместе с аутентификацией через RADIUS-сервер.

Беспроводной режим – Защита

На этой странице можно настроить параметры защиты беспроводной локальной сети.
Вы можете настроить параметры вручную или с помощью функции WPS (Настройка защищенного Wi-Fi)

WPS

Включить WPS:

Настроить точку доступа вручную

В целях защиты сети от хакеров и неавторизованных пользователей настоятельно рекомендуется выбрать один из указанных ниже типов защиты беспроводной сети. Вы можете настроить метод сетевой аутентификации, выбрать шифрование, указать, нужно ли вводить пароль для входа в беспроводную сеть, а также выбрать степень надёжности шифрования. **Внимание: Не рекомендуется выбирать шифрование WEP, если устройство работает в режиме 11n. Если выбран WEP, то максимальная скорость передачи данных составляет до 54 Мбит/с.**

Примечание: Режим "только 11n" не поддерживается при использовании шифрования WEP или если тип шифрования WPA выбран "TKIP".
Примечание: Нельзя выбирать "TKIP" для "шифрования WPA", если устройство работает в режиме "только 11n".
Когда укажете необходимые настройки, нажмите "Сохранить/Применить".

Выберите SSID:	<input type="text" value="TP-LINK_1808"/>	
Сетевая аутентификация:	<input type="text" value="WPA-Enterprise (хорошо)"/>	
Период обновления пароля беспроводной сети:	<input type="text" value="0"/>	(не обязательно)
IP-адрес RADIUS-сервера:	<input type="text" value="0.0.0.0"/>	
Порт RADIUS-сервера:	<input type="text" value="1812"/>	(1-65535)
Пароль RADIUS-сервера:	<input type="text"/>	(не обязательно)
Шифрование WPA:	<input type="text" value="AES"/>	
WEP Encryption:	<input type="text" value="Отключено"/>	

Рисунок 4-81

- **Период обновления пароля беспроводной сети:** Введите период обновления пароля беспроводной сети, который определяет, как часто маршрутизатор должен менять его.
- **IP-адрес RADIUS-сервера:** IP-адрес RADIUS-сервера аутентификации.
- **Порт RADIUS-сервера:** Порт RADIUS-сервера аутентификации. Номер по умолчанию: 1812.
- **Пароль RADIUS-сервера:** Пароль RADIUS-сервера аутентификации.
- **Шифрование WPA:** Выберите шифрование, которые вы собираетесь использовать: TKIP+ AES или AES (метод шифрования AES более надёжен, чем TKIP).

Настройка WPA-Enterprise

1. Выберите **WPA-Enterprise** из выпадающего списка **Сетевая аутентификация**. Меню изменится, в нём появятся новые разделы с соответствующими настройками.
2. Измените **Период обновления пароля беспроводной сети** по желанию.
3. Укажите IP-адрес RADIUS-сервера в поле **IP-адрес RADIUS-сервера**.
4. При необходимости измените **Порт RADIUS-сервера**.
5. Введите пароль в поле **Пароль RADIUS-сервера**.
6. Выберите **AES** в качестве Шифрования WPA.
7. Нажмите **Сохранить/Применить** для сохранения ваших настроек.

Беспроводной режим – Защита	
<p>На этой странице можно настроить параметры защиты беспроводной локальной сети. Вы можете настроить параметры вручную или с помощью функции WPS (Настройка защищённого Wi-Fi)</p>	
<p>WPS</p> <p>Включить WPS: <input type="button" value="Отключено"/></p>	
<p>Настроить точку доступа вручную</p> <p>В целях защиты сети от хакеров и неавторизованных пользователей настоятельно рекомендуется выбрать один из указанных ниже типов защиты беспроводной сети. Вы можете настроить метод сетевой аутентификации, выбрать шифрование, указать, нужно ли вводить пароль для входа в беспроводную сеть, а также выбрать степень надёжности шифрования. Внимание: Не рекомендуется выбирать шифрование WEP, если устройство работает в режиме 11n. Если выбран WEP, то максимальная скорость передачи данных составляет до 54 Мбит/с. Примечание: Режим "только 11n" не поддерживается при использовании шифрования WEP или если тип шифрования WPA выбран "TKIP". Примечание: Нельзя выбирать "TKIP" для шифрования WPA, если устройство работает в режиме "только 11n". Когда укажете необходимые настройки, нажмите "Сохранить/Применить".</p>	
Выберите SSID:	<input type="button" value="TP-LINK_1808"/>
Сетевая аутентификация:	<input type="button" value="WPA-Enterprise (хорошо)"/>
Период обновления пароля беспроводной сети:	<input type="text" value="0"/> (не обязательно)
IP-адрес RADIUS-сервера:	<input type="text" value="0.0.0.0"/>
Порт RADIUS-сервера:	<input type="text" value="1812"/> (1-65535)
Пароль RADIUS-сервера:	<input type="text" value="....."/> (не обязательно) (Введите значение длиной от 8 до 63 символов в кодировке ASCII или от 8 до 64 шестнадцатеричных чисел.)
Шифрование WPA:	<input type="button" value="AES"/>
WEP Encryption:	<input type="button" value="Отключено"/>
<input type="button" value="Сохранить/Применить"/>	

Рисунок 4-82

3. WPA-Personal

В шифровании WPA-Personal используется общий ключ и не требуется использование отдельного сервера аутентификации. Пароли могут быть указаны в кодировке ASCII или шестнадцатеричными числами.

Беспроводной режим – Защита

На этой странице можно настроить параметры защиты беспроводной локальной сети. Вы можете настроить параметры вручную или с помощью функции WPS (Настройка защищённого Wi-Fi)

WPS

Включить WPS:

Добавить клиента (Данная функция доступна только, если были выбраны режимы защиты WPA-PSK, WPA2-PSK или Открытая система)

Кнопка WPS PIN-код

[Справка](#)

PIN-код устройства: [Справка](#)

Настроить точку доступа вручную

В целях защиты сети от хакеров и неавторизованных пользователей настоятельно рекомендуется выбрать один из указанных ниже типов защиты беспроводной сети. Вы можете настроить метод сетевой аутентификации, выбрать шифрование, указать, нужно ли вводить пароль для входа в беспроводную сеть, а также выбрать степень надёжности шифрования. **Внимание: Не рекомендуется выбирать шифрование WEP, если устройство работает в режиме 11n. Если выбран WEP, то максимальная скорость передачи данных составляет до 54 Мбит/с.**

Примечание: Режим "только 11n" не поддерживается при использовании шифрования WEP или если тип шифрования WPA выбран "TKIP".
 Примечание: Нельзя выбирать "TKIP" для "шифрования WPA", если устройство работает в режиме "только 11n".
 Когда укажете необходимые настройки, нажмите "Сохранить/Применить".

Выберите SSID:

Сетевая аутентификация:

Пароль беспроводной сети: (Также называется Общий ключ WPA)

[Показать пароль](#)
 (Введите значение длиной от 8 до 63 символов в кодировке ASCII или от 8 до 64 шестнадцатеричных чисел.)

Период обновления пароля беспроводной сети: (не обязательно)

Шифрование WPA:

WEP Encryption:

Рисунок 4-83

- **Пароль беспроводной сети:** Укажите пароль, общий для вашего маршрутизатора и прочих сетевых устройств (8-63 символов в кодировке ASCII или 8-64 шестнадцатеричных числа).
- **Показать пароль:** Нажмите здесь, чтобы отобразить Пароль беспроводной сети.

Настройка WPA-Personal

1. Выберите **WPA-Personal**. Меню изменится, в нём появятся новые разделы с соответствующими настройками.
2. Защита WPA-Personal использует общий ключ. Введите пароль в поле рядом (в кодировке ASCII или шестнадцатеричными числами).
3. Измените Период обновления пароля беспроводной сети по желанию или оставьте значение по умолчанию.
4. Нажмите **Сохранить/Применить** для сохранения новых настроек.

Беспроводной режим – Защита

На этой странице можно настроить параметры защиты беспроводной локальной сети. Вы можете настроить параметры вручную или с помощью функции WPS (Настройка защищённого Wi-Fi)

WPS

Включить WPS:

Добавить клиента (Данная функция доступна только, если были выбраны режимы защиты WPA-PSK, WPA2-PSK или Открытая система)

Кнопка WPS
 PIN-код

код [Справка](#)

PIN-код устройства: [Справка](#)

Настроить точку доступа вручную

В целях защиты сети от хакеров и неавторизованных пользователей настоятельно рекомендуется выбрать один из указанных ниже типов защиты беспроводной сети. Вы можете настроить метод сетевой аутентификации, выбрать шифрование, указать, нужно ли вводить пароль для входа в беспроводную сеть, а также выбрать степень надёжности шифрования. **Внимание: Не рекомендуется выбирать шифрование WEP, если устройство работает в режиме 11n. Если выбран WEP, то максимальная скорость передачи данных составляет до 54 Мбит/с.**

Примечание: Режим "только 11n" не поддерживается при использовании шифрования WEP или если тип шифрования WPA выбран "TKIP".
 Примечание: Нельзя выбирать "TKIP" для "шифрования WPA", если устройство работает в режиме "только 11n".
 Когда укажете необходимые настройки, нажмите "Сохранить/Применить".

Выберите SSID:

Сетевая аутентификация:

Пароль беспроводной сети: (Также называется Общий ключ WPA)
[Показать пароль](#)
 (Введите значение длиной от 8 до 63 символов в кодировке ASCII или от 8 до 64 шестнадцатеричных чисел.)

Период обновления пароля беспроводной сети: (не обязательно)

Шифрование WPA:

WEP Encryption:

Рисунок 4-84

Примечание:

Если вы нажмёте “Показать пароль”, появится окно (см. Рисунок 4-85), в котором будет виден указанный вами пароль. Кроме того, не будут показаны пустые символы на концах пароля.

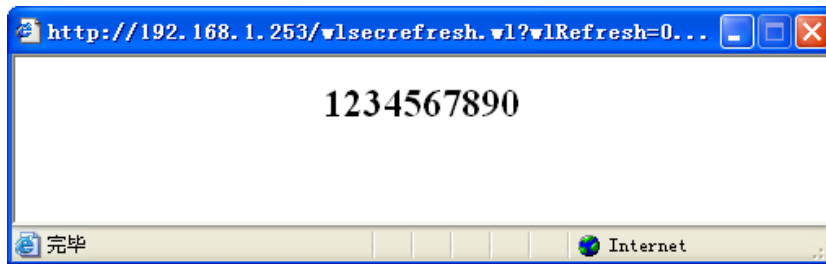


Рисунок 4-85

4. WPA2-Enterprise

Выберите WPA2-Enterprise из выпадающего списка для настройки защиты WPA2-Enterprise, после чего в меню появятся новые разделы для соответствующих настроек. Настройка аналогична настройкам WPA.

Беспроводной режим – Защита

На этой странице можно настроить параметры защиты беспроводной локальной сети. Вы можете настроить параметры вручную или с помощью функции WPS (Настройка защищённого Wi-Fi)

WPS

Включить WPS:

Настроить точку доступа вручную

В целях защиты сети от хакеров и неавторизованных пользователей настоятельно рекомендуется выбрать один из указанных ниже типов защиты беспроводной сети. Вы можете настроить метод сетевой аутентификации, выбрать шифрование, указать, нужно ли вводить пароль для входа в беспроводную сеть, а также выбрать степень надёжности шифрования. **Внимание: Не рекомендуется выбирать шифрование WEP, если устройство работает в режиме 11n. Если выбран WEP, то максимальная скорость передачи данных составляет до 54 Мбит/с.**
 Примечание: Режим "только 11n" не поддерживается при использовании шифрования WEP или если тип шифрования WPA выбран "TKIP".
 Примечание: Нельзя выбирать "TKIP" для "шифрования WPA", если устройство работает в режиме "только 11n".
 Когда укажете необходимые настройки, нажмите "Сохранить/Применить".

Выберите SSID:

Сетевая аутентификация:

Предварительная аутентификация WPA2:

Период повтора сетевой аутентификации: (не обязательно)

Период обновления пароля беспроводной сети: (не обязательно)

IP-адрес RADIUS-сервера:

Порт RADIUS-сервера: (1-65535)

Пароль RADIUS-сервера:

(Введите значение длиной от 8 до 63 символов в кодировке ASCII или от 8 до 64 шестнадцатеричных чисел.)

Шифрование WPA:

WEP Encryption:

Рисунок 4-86

- **Предварительная аутентификация WPA2:** Выберите Включить из выпадающего списка, тогда станции будут проходить аутентификацию с точкой доступа в ходе сканирования, поскольку необходимо сопоставление защиты, станция уже будет аутентифицирована.
- **Период повтора сетевой аутентификации:** Введите значение в секундах – это период, через который будет повторяться сетевая аутентификация, данная функция не будет работать, если указать "0" или оставить поле пустым.

5. WPA2-Personal

Если вы хотите настроить защиту WPA2-Personal, выберите WPA2-Personal из выпадающего списка, после чего в меню появятся новые разделы для соответствующих настроек. Для защиты WPA2-Personal используется общий ключ и не требуется использование отдельного сервера аутентификации. Пароли указываются символами в кодировке ASCII или с помощью шестнадцатеричных чисел.

Настроить точку доступа вручную

В целях защиты сети от хакеров и неавторизованных пользователей настоятельно рекомендуется выбрать один из указанных ниже типов защиты беспроводной сети. Вы можете настроить метод сетевой аутентификации, выбрать шифрование, указать, нужно ли вводить пароль для входа в беспроводную сеть, а также выбрать степень надёжности шифрования. **Внимание: Не рекомендуется выбирать шифрование WEP, если устройство работает в режиме 11n. Если выбран WEP, то максимальная скорость передачи данных составляет до 54 Мбит/с.**
 Примечание: Режим "только 11n" не поддерживается при использовании шифрования WEP или если тип шифрования WPA выбран "TKIP".
 Примечание: Нельзя выбирать "TKIP" для "шифрования WPA", если устройство работает в режиме "только 11n".
 Когда укажете необходимые настройки, нажмите "Сохранить/Применить".

Выберите SSID:

Сетевая аутентификация:

Пароль беспроводной сети: (Также называется Общий ключ WPA)
[Показать пароль](#)
 (Введите значение длиной от 8 до 63 символов в кодировке ASCII или от 8 до 64 шестнадцатеричных чисел.)

Период обновления пароля беспроводной сети: (не обязательно)

Шифрование WPA:

WEP Encryption:

Рисунок 4-87

6. Mixed WPA2/WPA Enterprise

Выберите из выпадающего списка Смешанная WPA2/WPA Enterprise, после чего в меню появятся новые разделы для соответствующих настроек. Настройка такая же, как и для WPA-PSK.

Беспроводной режим – Защита

На этой странице можно настроить параметры защиты беспроводной локальной сети.
Вы можете настроить параметры вручную или с помощью функции WPS (Настройка защищённого Wi-Fi)

WPS

Включить WPS:

Настроить точку доступа вручную

В целях защиты сети от хакеров и неавторизованных пользователей настоятельно рекомендуется выбрать один из указанных ниже типов защиты беспроводной сети.
Вы можете настроить метод сетевой аутентификации, выбрать шифрование, указать, нужно ли вводить пароль для входа в беспроводную сеть, а также выбрать степень надёжности шифрования.
Внимание: Не рекомендуется выбирать шифрование WEP, если устройство работает в режиме 11n. Если выбран WEP, то максимальная скорость передачи данных составляет до 54 Мбит/с.
Примечание: Режим только 11n не поддерживается при использовании шифрования WEP или если тип шифрования WPA выбран TKIP.
Примечание: Нельзя выбирать TKIP для шифрования WPA, если устройство работает в режиме только 11n.
Когда укажете необходимые настройки, нажмите "Сохранить/Применить".

Выберите SSID:	<input type="text" value="TP-LINK_1808"/>	
Сетевая аутентификация:	<input type="text" value="Mixed WPA2/WPA Enterprise (адаптивная защита)"/>	
Предварительная аутентификация WPA2:	<input type="text" value="Отключено"/>	
Период повтора сетевой аутентификации:	<input type="text" value="36000"/>	(не обязательно)
Период обновления пароля беспроводной сети:	<input type="text" value="0"/>	(не обязательно)
IP-адрес RADIUS-сервера:	<input type="text" value="0.0.0.0"/>	
Порт RADIUS-сервера:	<input type="text" value="1812"/>	(1-65535)
Пароль RADIUS-сервера:	<input type="text"/>	(не обязательно)
(Введите значение длиной от 8 до 63 символов в кодировке ASCII или от 8 до 64 шестнадцатеричных чисел.)		
Шифрование WPA:	<input type="text" value="AES"/>	
WEP Encryption:	<input type="text" value="Отключено"/>	

Рисунок 4-88

7. Mixed WPA2/WPA-Personal

Выберите из выпадающего списка Смешанная WPA2/WPA-Personal, после чего в меню появятся новые разделы для соответствующих настроек. Настройка такая же, как и для WPA-PSK.

Беспроводной режим – Защита

На этой странице можно настроить параметры защиты беспроводной локальной сети.
Вы можете настроить параметры вручную или с помощью функции WPS (Настройка защищённого Wi-Fi)

WPS

Включить WPS: ▾

Добавить клиента (Данная функция доступна только, если были выбраны режимы защиты WPA-PSK, WPA2-PSK или Открытая система)

Кнопка WPS PIN-код

[Справка](#)

PIN-код устройства: [Справка](#)

Настроить точку доступа вручную

В целях защиты сети от хакеров и неавторизованных пользователей настоятельно рекомендуется выбрать один из указанных ниже типов защиты беспроводной сети. Вы можете настроить метод сетевой аутентификации, выбрать шифрование, указать, нужно ли вводить пароль для входа в беспроводную сеть, а также выбрать степень надёжности шифрования.
Внимание: Не рекомендуется выбирать шифрование WEP, если устройство работает в режиме 11n. Если выбран WEP, то максимальная скорость передачи данных составляет до 54 Мбит/с.
Примечание: Режим "только 11n" не поддерживается при использовании шифрования WEP или если тип шифрования WPA выбран "TKIP".
Примечание: Нельзя выбирать "TKIP" для шифрования WPA, если устройство работает в режиме "только 11n".
Когда укажете необходимые настройки, нажмите "Сохранить/Применить".

Выберите SSID: ▾

Сетевая аутентификация: ▾

Пароль беспроводной сети: (Также называется Общий ключ WPA)
[Показать пароль](#)
(Введите значение длиной от 8 до 63 символов в кодировке ASCII или от 8 до 64 шестнадцатеричных чисел.)

Период обновления пароля беспроводной сети: (не обязательно)

Шифрование WPA: ▾

WEP Encryption: ▾

Рисунок 4-89

4.6.3 Расписание Wi-Fi

В меню на странице **Беспроводной режим – Расписание Wi-Fi** можно настроить планировщик задач. Для использования данной функции сначала необходимо настроить системное время маршрутизатора.

Беспроводной режим – Расписание

На данной странице можно настроить расписание.

Нажмите на таблицу или используйте кнопку 'Добавить', чтобы указать период, когда беспроводное вещание будет отключено автоматически!

Расписание не будет работать, если вы не настроили системное время. Чтобы настроить системное время, нажмите [здесь](#).

Расписание беспроводного режима: Включить Отключить

Применить к: Начало: Конец:

Время	0:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00
Вск.															
Пн.															
Вт.															
Ср.															
Чт.															
Пт.															
Сб.															

Рисунок 4-90

👉 Примечание:

Время, которое вы указываете, это тот период, когда беспроводное вещание не будет работать.

Перед настройкой расписания работы беспроводного режима настройте системное время (см. раздел [4.9.5 Время](#)), после чего вы сможете включать или отключать беспроводное вещание.

- **Применить к:** Выберите день или дни, в которые беспроводное вещание не будет работать.
- **Начало/Конец:** Можно выбрать все дни – 24 часа или указать конкретное время **Начала** и **Конца** в соответствующем поле.
- **Добавить:** Нажмите эту кнопку, чтобы добавить выбранное вами время в таблицу.

Нажмите **Очистить расписание**, чтобы удалить настройки из таблицы.

Нажмите **Сохранить/Применить** для завершения настройки.

4.6.4 Фильтрация MAC-адресов

Выбрав в меню раздел **Беспроводной режим – Фильтрация MAC-адресов**, вы попадёте на страницу настройки фильтрации MAC-адресов (см. Рис. ниже).

Беспроводной режим – Фильтрация MAC-адресов

Можно настроить не более 64 записей.

Выберите SSID:

Режим запрета MAC-адресов: Отключено Разрешить Запретить

Примечание: Если выбран вариант 'Разрешить', но MAC-адреса не указаны для правил фильтрации, то функция WPS будет отключена.

MAC-адрес	Удалить

Рисунок 4-91

Можно ограничить беспроводной доступ, настроив фильтр MAC-адресов беспроводных устройств, работающих в пределах вашей сети и закреплённых за вашим RADIUS-сервером. Можно блокировать или разрешать доступ пользователям по их MAC-адресам. Если вы не хотите фильтровать пользователей по MAC-адресам, выберите Отключено.

- **Отключено:** Выберите эту опцию для отключения функции фильтрации MAC-адресов.
- **Разрешить:** Выберите эту опцию, чтобы функция фильтрации MAC-адресов разрешила беспроводной доступ устройствам, занесённым вами в таблицу.
- **Запретить:** Выберите эту опцию, чтобы функция фильтрации MAC-адресов запретила беспроводной доступ устройствам, занесённым вами в таблицу.
- **Добавить:** Нажмите эту кнопку, чтобы добавить MAC-адрес.
- **Удалить:** Отметьте эту опцию для MAC-адреса, затем нажмите кнопку Удалить для удаления MAC-адреса из таблицы.

После нажатия кнопки **Добавить** открывается страница как на рисунке ниже, где вы можете ввести MAC-адрес в поле **MAC-адрес**.

 **Примечание:**

Формат MAC-адреса должен быть **“xx:xx:xx:xx:xx:xx”**, например **“00:13:0A:55:FF:09”**.

Беспроводное вещание – Фильтрация MAC-адресов

Введите MAC-адрес и нажмите "Сохранить/Применить", чтобы добавить его в список фильтрации MAC-адресов.

MAC-адрес:

Рисунок 4-92

Заполнив MAC-адрес, нажмите **Сохранить/Применить** для сохранения настроек.

4.6.5 Беспроводной мост

На странице **Беспроводной режим – Беспроводной мост** вам доступны настройки параметров **беспроводного моста** LAN-интерфейса (см. Рис. ниже). Для сохранения текущих настроек нажмите **Применить/Сохранить**.

Беспроводной режим – Мост

На этой странице можно настроить функцию беспроводного моста для беспроводной сети. Можно выбрать "Беспроводной мост" (также называется WDS - Система распределения беспроводных сетей), тогда будет отключена функция точки доступа, чтобы включить её, выберите режим "Точка доступа". Функция беспроводного моста будет работать и в этом режиме, и беспроводные станции смогут подключаться к точке доступа. Если вы выберете "Отключено" в строке "Ограничение моста", ограничений связи шлюза с мостами не будет, то есть можно будет установить соединение с любыми беспроводными мостами. Параметры "Включено" или "Вкл. (Сканирование)" устанавливают ограничение связи шлюза с мостами. Доступ будет разрешён только для тех мостов, которые указаны в полях "MAC-адреса удалённых мостов".

Нажмите "Обновить" для обновления удалённых мостов. Обновление займёт несколько секунд.

Нажмите "Сохранить/Применить", чтобы настройки беспроводного моста вступили в силу.

Примечание 1: Беспроводной мост доступен только, если используются типы сетевой аутентификации: "Открытая система" или "Общая система".

Если вы хотите, чтобы удалённые беспроводные устройства подключались к данному маршрутизатору через мост, сначала укажите в настройках сетевой аутентификации "Открытая система" или "Общая система"!

Примечание 2: Другие точки доступа могут подключаться через мост к данному маршрутизатору только в том случае, если в их настройках параметр канала настроен так же, как на данном маршрутизаторе.

Режим:

Ограничение моста:

Рисунок 4-93

- **Режим** Выберите режим точки доступа из выпадающего списка. Доступны опции: Точка доступа и Беспроводной мост.
 - **Точка доступа:** Выберите эту опцию, чтобы разрешить доступ беспроводным станциям, включая клиентов точки доступа.
 - **Беспроводной мост:** Эта функция также называется WDS (Wireless Distribution System – беспроводная система распределения), она позволяет беспроводным

станциям (которые тоже работают в режиме моста) подключиться к двум или более удалённым локальным сетям.

➤ **Ограничение моста:**

- **Отключено:** Если вы выберете эту опцию, ограничений связи шлюза с мостами не будет, то есть можно будет установить соединение с любыми беспроводными мостами.
- **Включено:** Если вы выберете эту опцию (как показано ниже), то будут установлены ограничения связи шлюза с мостами. Введите MAC-адреса удалённых мостов, с которыми вы хотите разрешить соединение. Можно будет установить соединение только с указанными удалёнными мостами.

Режим:	<input type="text" value="Точка доступа"/>	<input type="button" value="v"/>
Ограничение моста:	<input type="text" value="Включено"/>	<input type="button" value="v"/>
MAC-адреса удалённых мостов:	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>
<input type="button" value="Обновить"/> <input type="button" value="Сохранить/Применить"/>		

Рисунок 4-94

- **Вкл. (сканирование):** Если вы выберете эту опцию, то будут установлены ограничения связи шлюза с мостами. Устройство будет сканировать всё вокруг для поиска доступных точек доступа. Можно будет установить соединение только с выбранными точками доступа.
- **Обновить:** Нажмите эту кнопку для сканирования и отображения точек доступа.

Беспроводной режим – Мост

На этой странице можно настроить функцию беспроводного моста для беспроводной сети. Можно выбрать "Беспроводной мост" (также называется WDS - Система распределения беспроводных сетей), тогда будет отключена функции точки доступа, чтобы включить её, выберите режим "Точка доступа". Функция беспроводного моста будет работать и в этом режиме, и беспроводные станции смогут подключаться к точке доступа. Если вы выберете "Отключено" в строке "Ограничение моста", ограничений связи шлюза с мостами не будет, то есть можно будет установить соединение с любыми беспроводными мостами. Параметры "Включено" или "Вкл. (Сканирование)" устанавливают ограничение связи шлюза с мостами. Доступ будет разрешён только для тех мостов, которые указаны в полях "MAC-адреса удалённых мостов".
 Нажмите "Обновить" для обновления удалённых мостов. Обновление займёт несколько секунд.
 Нажмите "Сохранить/Применить", чтобы настройки беспроводного моста вступили в силу.

Примечание 1: Беспроводной мост доступен только, если используются типы сетевой аутентификации: "Открытая система" или "Общая система".

Если вы хотите, чтобы удалённые беспроводные устройства подключались к данному маршрутизатору через мост, сначала укажите в настройках сетевой аутентификации "Открытая система" или "Общая система"!

Примечание 2: Другие точки доступа могут подключаться через мост к данному маршрутизатору только в том случае, если в их настройках параметр канала настроен так же, как на данном маршрутизаторе.

Режим:

Ограничение моста:

MAC-адреса удалённых мостов:

	SSID	BSSID	КАНАЛ
<input type="checkbox"/>	TP-LINK_796F	60:E3:27:44:79:6F	7
<input type="checkbox"/>	TP-LINK_RE_9B0A	22:19:66:CA:9B:0A	1
<input type="checkbox"/>	TP-LINK_0E99	CC:34:29:8A:39:C8	6
<input type="checkbox"/>	TP-LINK_0E99	FC:D7:33:10:0E:99	6
<input type="checkbox"/>	MEGuest_8B07	12:19:66:CA:8B:07	11

Рисунок 4-95

Примечание:

Беспроводной мост возможен только в случае использования способов аутентификации: **Открытая** или **Общая система**. Сначала войдите в меню в раздел **Беспроводной режим – Защита** и выберите метод аутентификации **Открытая система**, **Общая система**.

4.6.6 Дополнительные настройки

В меню **Беспроводной режим – Дополнительные настройки** вам доступны более детальные настройки параметров беспроводного режима (см. рисунок ниже).

Беспроводной режим – Дополнительные настройки

На данной странице можно указать дополнительные настройки беспроводного режима. Можно выбрать конкретный канал, на котором будет работать маршрутизатор, указать порог фрагментации, порог RTS, интервал проверки готовности клиентов выйти из энергосберегающего режима, интервал маяка для точки доступа.

Примечание: Если вы выбрали режим "только 11n", вы не сможете выбрать тип шифрования беспроводного режима: "WEP" или "TKIP".
Нажмите "Сохранить/Применить", чтобы параметры дополнительных настроек вступили в силу.

Канал:	Auto ▾
Режим:	11bgn ▾
Пропускная способность:	20/40 МГц ▾
Контроль боковой полосы частот:	Нижняя ▾
Порог фрагментации:	2346
Порог RTS:	2347
Интервал DTIM:	1
Интервал маяка:	100
Мощность передатчика:	100% ▾
WMM(Wi-Fi Multimedia):	Включено ▾

Сохранить/Применить

Рисунок 4-96

- **Канал:** Из выпадающего списка выберите канал, который вы хотите использовать. Здесь указано, какая рабочая частота будет использоваться. Изменять канал беспроводной связи не стоит, если у вас не наблюдаются проблемы, вызванные помехами с другой точкой доступа, расположенной неподалёку.
- **Режим:** Из выпадающего списка можно выбрать 11b, 11bg, 11bgn и только 11n. Режим 11bgn позволяет всем устройствам стандартов 802.11b, 802.11g и 802.11n подключаться к маршрутизатору.
- **Пропускная способность:** Выберите пропускную способность, которую вы хотите использовать из выпадающего списка. Если вы выбрали более высокую пропускную способность, устройство будет отправлять и принимать данные с большей скоростью.
- **Контроль боковой полосы частот:** Если указать большее значение для пропускной способности, то можно будет выбрать любое значение для данного параметра.
- **Порог фрагментации:** Данная величина представляет собой максимальный размер пакета, после которого пакет данных будет фрагментирован в несколько пакетов. Если у вас наблюдается высокий процент пакетных ошибок, вы можете немного повысить значение данного параметра. Если указать слишком низкое значение, то производительность сети упадёт. Если вы уменьшаете значение по умолчанию, то рекомендуется проводить лишь совсем незначительное уменьшение, но в большинстве случаев лучше использовать значение по умолчанию: 2346.
- **Порог RTS:** Если вы столкнулись с проблемой неустойчивой передачи данных, рекомендуется незначительно уменьшить настройку по умолчанию, которое составляет 2347. Если сетевой пакет меньше, чем размер порога RTS, то механизм RTS/CTS не будет включен. Маршрутизатор посылает запрос на отправку (RTS) конкретной принимающей станции и согласовывает с ней отправку данных. После получения RTS (запроса на отправку) беспроводная станция отвечает с помощью разрешения на отправку (CTS) для подтверждения, что в данный момент можно начать передачу данных. Данный механизм предоставляет вам свободный канал передачи данных, уведомляя остальные станции не отправлять пакеты в течение определённого времени. В большинстве случаев данный параметр остаётся без изменений: 2347.
- **Интервал DTIM:** Данный параметр может быть настроен в пределах от 1 до 255 и определяет интервал отправки Сообщения о Доставке Трафика (DTIM). DTIM – временной интервал, по истечении которого широковещательные (broadcast) и

многоадресные (multicast) пакеты, помещенные в буфер, будут доставлены беспроводным клиентам. Этот параметр измеряется количеством полученных кадров-маяков. Когда маршрутизатор поместил в буфер широковещательные и многоадресные пакеты для отправки их соответствующим клиентам, он отправляет следующее DTIM-сообщение через интервал DTIM. Клиенты слышат маяк и выходят из режима ожидания для получения широковещательных и многоадресных пакетов. Значение по умолчанию: 1.

- **Интервал маяка:** Введите значение от 20 до 1000 миллисекунд. Интервал маяка означает частоту интервала маяка. Маяк – это пакет, широковещаемый маршрутизатором с целью синхронизации беспроводной сети. Значение по умолчанию: 100.
- **Мощность передатчика:** Здесь можно указать мощность передачи беспроводного сигнала маршрутизатором. Высокая мощность увеличит расстояние, на которое маршрутизатор отправляет беспроводной сигнал, а также улучшит приём сигнала. Выбрав низкую мощность сигнала, вы уменьшите расстояние, на которое передается беспроводной сигнал, но снизите вероятность того, что сигнал будет страдать от воздействия помех других беспроводных устройств.
- **WMM (Wi-Fi Multimedia):** Функция WMM обеспечивает первоочередную отправку сообщений с высоким приоритетом. Настоятельно рекомендуется включить данную функцию.

4.6.7 Состояние станций

В меню на странице **Беспроводной режим – Состояние станций** находится список аутентифицированных беспроводных станций (см. рисунок ниже).

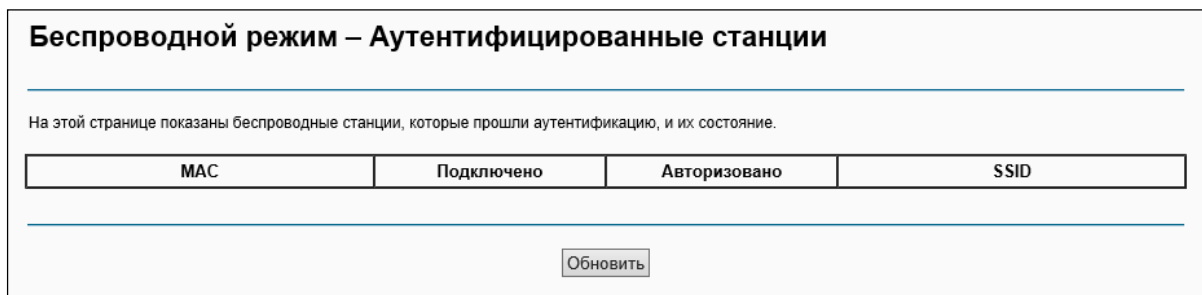


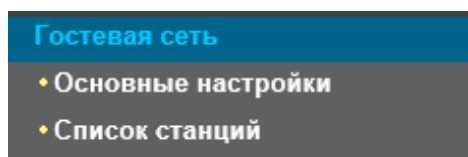
Рисунок 4-97

На данной странице отображены аутентифицированные беспроводные станции и их состояние.

- **MAC-адрес:** Здесь показан MAC-адрес подключённой беспроводной станции.
- **Подключено:** Здесь указано, подключена ли беспроводная станция к точке доступа.
- **Авторизовано:** Здесь указана информация об аутентификации.
- **SSID:** Здесь указан SSID подключенной беспроводной станции.

На данной странице нельзя изменять данные. Для обновления информации в таблице о текущих подключенных беспроводных станциях нажмите кнопку **Обновить**.

4.7 Гостевая Сеть



Меню **Гостевая сеть** содержит два раздела: **Основные настройки** и **Список станций**. Выберите нужный вам раздел для просмотра или настройки соответствующих функций. Подробное описание по каждому разделу приведено далее.

4.7.1 Основные настройки

На странице **Гостевая сеть – Основные настройки** (см. Рисунок 4-98) можно создать отдельную сеть для гостей пользователей без доступа к вашей основной сети и подключённым к ней компьютерам.

Беспроводной режим – Гостевая сеть

На этой странице можно настроить гостевую сеть.

Гостевая сеть: Включить Отключить

SSID гостевой сети:

Тип аутентификации:

Шифрование:

Пароль беспроводной сети: (Введите значение длиной от 8 до 63 символов в кодировке ASCII или от 8 до 64 шестнадцатеричных чисел.)

[Показать пароль](#)

Период обновления пароля беспроводной сети: (секунд; минимальное значение: 30; 0 означает, что обновление не производится.)

Разрешить гостевым пользователям доступ к локальной сети:

Изоляция гостевой сети:

Контроль пропускной способности гостевой сети: Функция контроля пропускной способности устройства отключена, нажмите [здесь](#) чтобы включить её.

Рисунок 4-98

Вы можете включить или отключить гостевую сеть. Включив данную функцию, можно настроить параметры беспроводного режима для гостевой сети.

- **SSID Гостевой сети:** Имя гостевой сети. Если вы решили создать гостевую сеть, настоятельно рекомендуется использовать такое имя сети, которое легко отличает её от вашей основной сети.
- **Тип аутентификации:** Выберите тип аутентификации из выпадающего списка.
- **Шифрование:** Можно выбрать либо **AES**, либо **AES+TKIP**.
- **Пароль беспроводной сети:** Здесь указан беспроводной пароль по умолчанию, можно нажать **Показать пароль**, чтобы увидеть его. Можно создать свой пароль длиной от 8 до 63 символов в кодировке ASCII или от 8 до 64 шестнадцатеричных чисел.
- **Период обновления пароля:** Укажите интервал обновления пароля беспроводной сети в секундах. Для данного параметра можно указать «30» или больше. Если указать «0», то обновление производится не будет.
- **Разрешить гостевым пользователям доступ к локальной сети:** Гости будут иметь доступ к вашей локальной сети, но не смогут зайти в веб-утилиту настройки маршрутизатора.
- **Изоляция гостевой сети:** Данная функция позволяет изолировать беспроводных клиентов друг от друга в вашей гостевой сети. Данная функция отключена по умолчанию.

- **Контроль пропускной способности гостевой сети:** Данная функция позволяет настроить исходящую и входящую пропускную способность для гостевой сети.

Для сохранения настроек нажмите **Сохранить/Применить**.

4.7.2 Список станций

На странице **Гостевая сеть – Список станций** можно увидеть следующую информацию о подключенных беспроводных станциях: MAC-адрес, подключено или нет, авторизовано или нет, SSID и интерфейс.

Беспроводной режим – Аутентифицированные станции

На этой странице показаны беспроводные станции, которые прошли аутентификацию, и их состояние.

MAC	Подключено	Авторизовано	SSID

Рисунок 4-99

- **MAC-адрес:** Здесь показан MAC-адрес подключённой беспроводной станции.
- **Подключено:** Здесь указано, подключена ли беспроводная станция к точке доступа.
- **Авторизовано:** Здесь указана информация об аутентификации.
- **SSID:** Здесь указан SSID подключенной беспроводной станции.

На данной странице нельзя изменять данные. Для обновления информации в таблице о текущих подключенных беспроводных станциях нажмите кнопку **Обновить**.

4.8 Диагностика

На странице **“Диагностика”** указаны результаты тесте ENET (Ethernet) подключения, беспроводного соединения и синхронизации ADSL-линии. Можно посмотреть дополнительную информацию в разделе **Справка** для более подробной информации по данному тесту.

br_0_8_35 Диагностика

Ваш модем может протестировать DSL-подключение. Отдельные тесты перечислены ниже. Если в результате теста указана ошибка, нажмите "Запустить тесты повторно" внизу станицы и пройдите тест ещё раз, чтобы убедиться, что данная ошибка повторяется. Если тест всё же не удаётся пройти, нажмите "Справка" и следуйте инструкциям.

Тест подключения к вашей локальной сети

Тест подключения LAN1:	ОШИБКА	Справка
Тест подключения LAN2:	ОШИБКА	Справка
Тест подключения LAN3:	УСПЕШНО	Справка
Тест беспроводного подключения:	УСПЕШНО	Справка

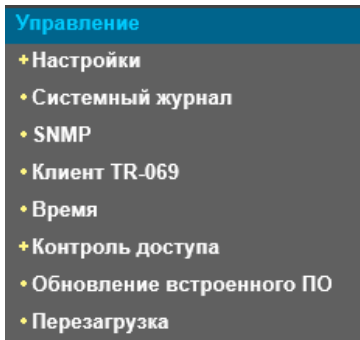
Тест подключения к вашему поставщику услуг DSL

Тест синхронизации xDSL-линии:	ОШИБКА	Справка
Тест ping сегмента F5 ATM OAM:	ОТКЛЮЧЕНО	Справка
Тест ping из конца в конец ATM OAM F5:	ОТКЛЮЧЕНО	Справка

Рисунок 4-100

4.9 Управление

Меню **Управление** содержит восемь разделов: **Настройки**, **Системный журнал**, **SNMP**, **Клиент TR-069**, **Время**, **Контроль доступа**, **Обновление встроенного ПО** и **Перезагрузка**. Выберите нужный вам раздел для настройки соответствующей функции.



4.9.1 Настройки

В данном разделе находятся три важные функции для управления маршрутизатором: **Экспорт** (резервное сохранение настроек), **Импорт** (обновление настроек) и **Восстановление заводских настроек**. Подробная информация по разделам указана ниже.

4.9.1.1 Экспорт

На странице **Управление – Настройки – Экспорт** (см. Рисунок 4-101) можно сохранить текущие настройки маршрутизатора в резервный файл.

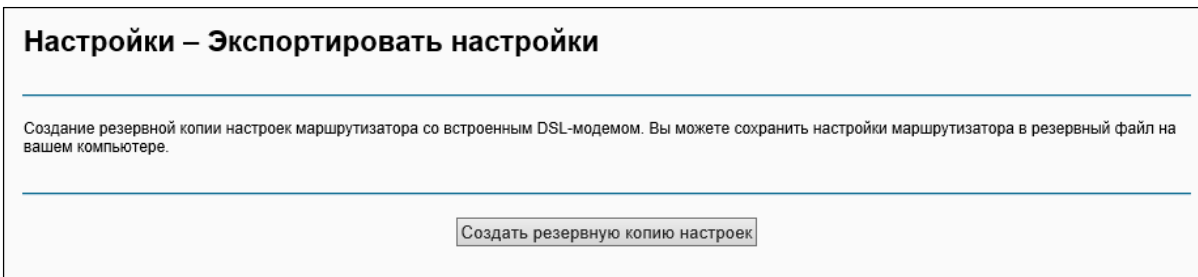


Рисунок 4-101

Для сохранения настроек в резервный файл:

1. Нажмите **Создать резервную копию** настроек (см. Рисунок 4-101), после чего появится окно, как на Рисунке 4-102.

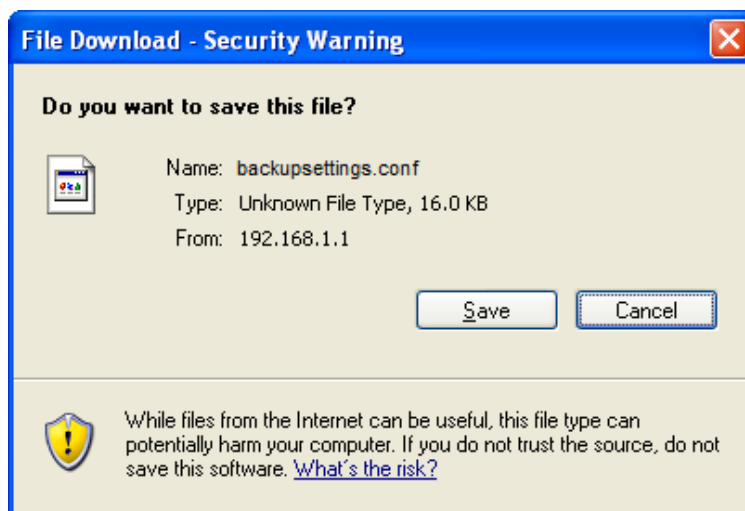


Рисунок 4-102

2. Нажмите кнопку **Сохранить** и сохраните файл, куда вам удобно (см. Рисунок 4-103).

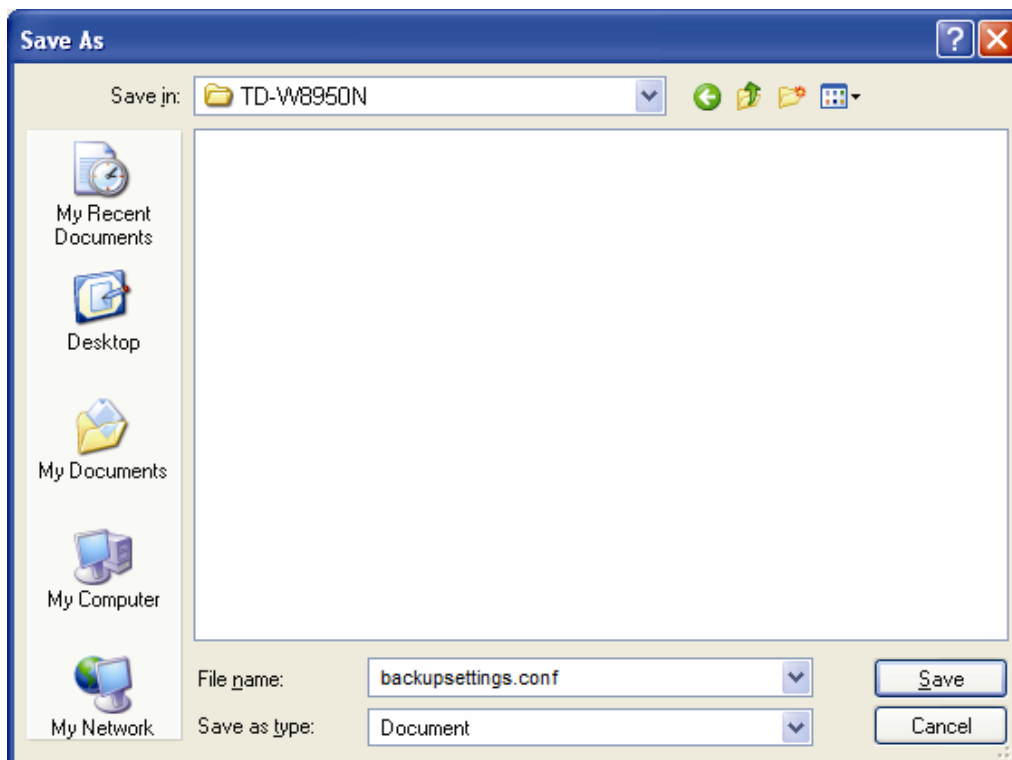


Рисунок 4-103

4.9.1.2 Импорт

На странице **Управление – Настройки – Импорт** (см. Рисунок 4-104) можно обновить настройки маршрутизатора.

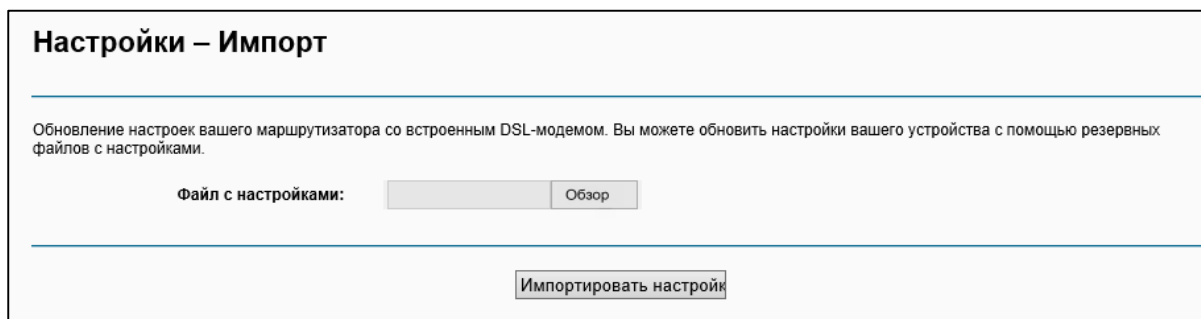


Рисунок 4-104

Для обновления настроек маршрутизатора:

1. Нажмите кнопку **Обзор** и выберите файл с настройками, также путь можно ввести вручную в поле имени файла с настройками.
2. **Когда вы выбрали файл с настройками, нажмите Импортировать настройки.**

Примечание:

По завершении настройки маршрутизатор будет перезагружен. Этот процесс займёт какое-то время, не выключайте питания маршрутизатора и не нажимайте кнопку **Reset** на устройстве, пока идёт процесс обновления настроек.

4.9.1.3 Восстановление настроек

На странице **Управление – Настройки – Восстановление настроек** (см. Рисунок 4-105) можно восстановить настройки маршрутизатора по умолчанию.

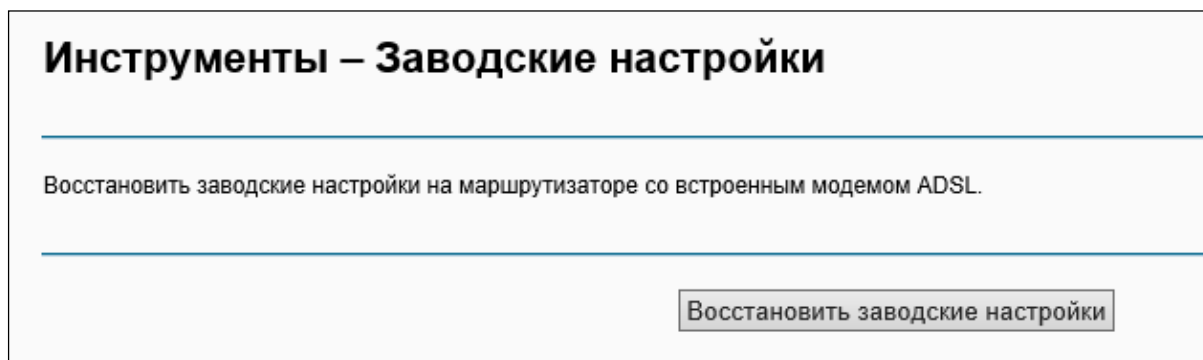


Рисунок 4-105

- **Восстановить заводские настройки:** Нажмите эту кнопку для восстановления заводских настроек маршрутизатора, затем следуйте инструкциям, указанным на мониторе компьютера.
- **Учётная запись и пароль:** По умолчанию **имя пользователя/пароль: admin/admin**.
- **IP-адрес** по умолчанию: 192.168.1.1
- **Маска подсети** по умолчанию: 255.255.255.0.

4.9.2 Системный журнал

На странице **Управление – Системный журнал** (см. Рисунок 4-106) можно просматривать системный журнал и настроить параметры системного журнала.

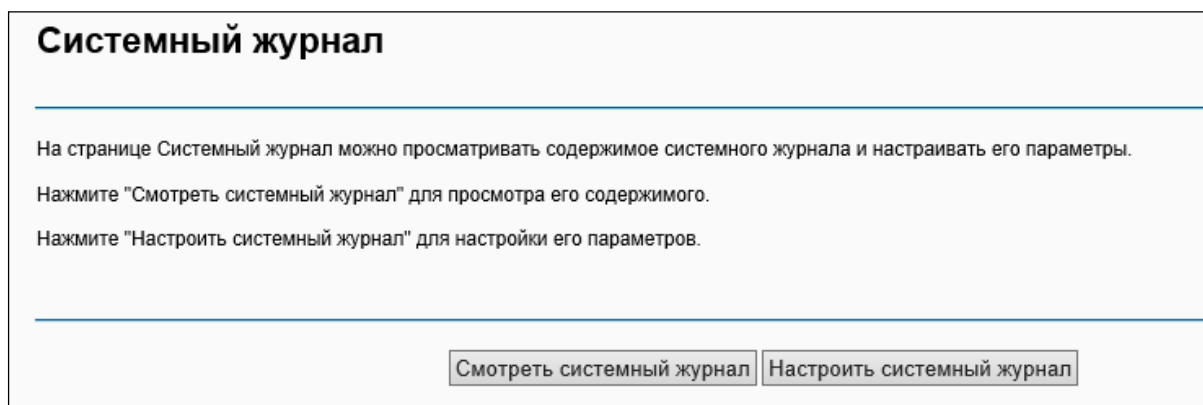


Рисунок 4-106

Чтобы посмотреть системный журнал:

Нажмите **Смотреть системный журнал**, вы попадёте на страницу (см. Рисунок 4-107), где находятся текущие журналы маршрутизатора.

Системный журнал			
Время	Facility	Важность	Уведомление
<input type="button" value="Обновить"/> <input type="button" value="Назад"/>			

Рисунок 4-107

- **Обновить:** Для обновления информации в таблице нажмите эту кнопку.
- **Назад:** Нажмите эту кнопку для возврата на предыдущую страницу.

Для настройки системного журнала:

Нажмите кнопку **Настроить системный журнал** (см. Рисунок 4-106), после чего вы попадёте на страницу, как на Рисунок 4-108.

Системный журнал – Настройка	
<p>Если включить журнал, система начнёт сохранять информацию о всех выбранных событиях. В списке 'Уровень журнала' можно выбрать события, которые будут заноситься в журнал. В списке 'Уровень отображения' выбираются отображаемые в журнале события (выбранное событие и те, что находятся выше по списку). Если выбрать 'Удалённо' или 'Оба', события будут заноситься в журнал на удалённом сервере по указанному IP-адресу и UDP-порту. Если выбрать 'Локально' или 'Оба', события будут храниться в локальной памяти.</p> <p>Настройте параметры и нажмите 'Сохранить/Применить' для настройки системного журнала.</p>	
Журнал:	<input checked="" type="radio"/> Отключить <input type="radio"/> Включить
Уровень журнала:	<input type="text" value="Исправление"/>
Уровень отображения:	<input type="text" value="Ошибка"/>
Режим:	<input type="text" value="Локально"/>
<input type="button" value="Сохранить/Применить"/>	

Рисунок 4-108

- **Отключить/Включить:** Выберите Включить, чтобы события записывались в журнал, если вы не хотите, чтобы данные события заносились в журнал, нажмите Отключить.
- **Уровень журнала:** Из выпадающего списка выберите уровень журнала. Будут заноситься в журнал все события, которые находятся в списке выше выбранного вами варианта, включая выбранный.
- **Уровень отображения:** Выберите уровень отображения из выпадающего списка. Будут отображены все события, которые находятся в списке выше выбранного вами варианта, включая выбранный.
- **Режим:** Выберите режим записи событий. Если выбрать **Локально**, события будут занесены в локальную память. Если выбрать **Удалённо**, будут заноситься в журнал на удалённом сервере по указанному IP-адресу и UDP-порту. Если выбрать Оба, то события будут заноситься в локальную память и отправляться на удалённый сервер.

4.9.3 SNMP

На странице **Управление – SNMP** (см. Рисунок 4-109), можно настраивать параметры SNMP.

SNMP (Простой протокол сетевого управления) в настоящий момент широко применяется в компьютерных сетях, его назначение – обеспечивать передачу управляющей информации между двумя узлами. Сетевые администраторы могут легко найти и изменить параметры

любого узла в сети, быстро локализовать проблему и определить её причину, распределить потребление ресурсов сети и настроить отчётность.

SNMP-агент – это приложение, запущенное на маршрутизаторе, которое выполняет функцию получения и обработки SNMP-сообщений и последующего отправления ответов SNMP-менеджеру. Кроме этого, SNMP-агент помогает локализовать то или иное событие, отправив информацию о его местонахождении в сети. Если на маршрутизаторе запущен SNMP-агент, то его можно отслеживать и/или управлять его работой с помощью SNMP-менеджера через SNMP-сообщения.

SNMP-менеджер – это приложение (другими словами, служба SNMP), которое генерирует SNMP-сообщения/запросы для изменения и доставки управляющей информации, также оно получает запрашиваемую информацию и отчёты о событиях/местонахождении событий, которые посылаются SNMP-агентом. SNMP-менеджер представляет собой стороннюю систему управления. Функцию мониторинга сети осуществляет SNMP-менеджер.

SNMP – Настройка

Протокол SNMP (Простой протокол сетевого управления) позволяет программе управления извлекать статистику и состояние от SNMP-агента данного устройства.

Выберите необходимые значения и нажмите "Сохранить/Применить" для настройки параметров SNMP.

SNMP-агент:	<input checked="" type="radio"/> Отключить <input type="radio"/> Включить
Сообщество чтения:	<input type="text" value="public"/>
Сообщество записи:	<input type="text" value="private"/>
Имя системы:	<input type="text" value="TP-LINK"/>
Расположение системы:	<input type="text" value="unknown"/>
Контакт системы:	<input type="text" value="unknown"/>
IP-адрес SNMP-менеджера:	<input type="text" value="0.0.0.0"/>

Рисунок 4-109

- **SNMP-агент:** Можно включить или отключить данную функцию, отметив нужный вам вариант.

👉 Примечание:

Сообщество SNMP обеспечивает простой метод аутентификации между маршрутизатором (SNMP-агент) и удалённым сетевым менеджером (SNMP-менеджером). Можно указать значение для параметра «Сообщество» как пароль для аутентификации станции управления маршрутизатором.

- **Сообщество чтения:** В этом поле можно указать параметр сообщества SNMP, который предоставляет доступ к маршрутизатору только для чтения, то есть данное сообщество сможет только просматривать настройки маршрутизатора. Значение по умолчанию «публично».
- **Сообщество записи:** В этом поле можно указать параметр сообщества SNMP, который предоставляет доступ к маршрутизатору для чтения и записи, то есть данное сообщество сможет просматривать настройки маршрутизатора и изменять их. Значение по умолчанию «частно».
- **Имя системы:** Укажите имя (буквы и/или числа) сообщества SNMP. Ваш маршрутизатор (SNMP-агенты) будут показывать управляющие данные на управляемых системах как указанное вами "имя системы".
- **Расположение системы:** Тот, кто будет получать уведомление в случае обнаружения проблем.

- **Контакт системы:** Где находится лицо, которое будет получать уведомления.
- **IP-адрес SNMP-менеджера:** IP-адрес SNMP-менеджера, куда SNMP-агент передаёт уведомления о появлении проблем.

Выберите нужные вам значения и нажмите **Сохранить/Применить**, чтобы настройки SNMP вступили в силу.

4.9.4 Клиент TR-069

На странице **Управление – Клиент TR-069** доступны настройки параметров клиента TR-069. **TR-069** (протокол управления WAN) позволяет серверу автонастройки (ACS) автоматически производить настройку, предоставление/сбор информации об устройстве в сети и диагностику устройства.

Клиент TR-069 – Настройка

Протокол управления через глобальную сеть (TR-069) позволяет серверу автонастройки осуществлять автонастройку, предоставление параметров, сбор данных и диагностику данного устройства.

Выберите нужные параметры и нажмите "Сохранить/Применить" для настройки клиента TR-069.

Уведомить Отключить Включить

Период уведомления:

URL-адрес сервера автонастройки:

Имя пользователя сервера автонастройки:

Пароль сервера автонастройки:

WAN-интерфейс, используемый клиентом TR-069t:

Отобразить сообщения SOAP на серийной консоли Отключить Включить

Аутентификация запроса на подключение

Имя пользователя запроса на подключение:

Пароль запроса на подключение:

URL запроса на подключение:

Рисунок 4-110

- **Уведомлять:** Отметьте это поле для включения/отключения **Период уведомления**.
- **Период уведомления:** Промежуток времени, через который вам маршрутизатор будет соединяться с **сервером автонастройки (ACS)**.
- **URL-адрес сервера автонастройки:** Эту информацию необходимо получить от вашего поставщика Интернет-услуг. Сервер автонастройки поможет автоматически производить настройку, предоставление/сбор информации об устройстве в сети и диагностику устройства.
- **Имя пользователя сервера автонастройки:** Эту информацию необходимо получить от вашего поставщика Интернет-услуг.
- **Пароль сервера автонастройки:** Эту информацию необходимо получить от вашего поставщика Интернет-услуг.

Примечание:

Если вы хотите зайти на сервер автонастройки, вам необходимо узнать **Имя пользователя** и **Пароль сервера автонастройки**.

- **WAN-интерфейс, используемый клиентом TR-069:** Выберите WAN-интерфейс из выпадающего списка для того, чтобы данная функция работала.
- **Имя пользователя запроса на подключение:** Укажите значение на ваше усмотрение.
- **Пароль запроса на подключение:** Укажите значение на ваше усмотрение.

 **Примечание:**

Имя пользователя запроса на подключение и Пароль запроса на подключение используется для входа на сервер автонастройки через маршрутизатор для управления им.

Выберите подходящие значения и нажмите **Сохранить/Применить**, чтобы настройка клиента TR-069 вступила в силу.

4.9.5 Время

На странице **Управление – Время** доступны настройки времени на маршрутизаторе.

Настройки времени

На данной странице можно указать настройки времени для устройства.

Дата/время : Thu Jan 1 00:13:16 1970
Дата/время на вашем компьютере : Mon Aug 17 09:36:54 2015

Указать дату/время маршрутизатора со встроенным модемом ADSL

Дата (Y/M/D) :
Время (H:M:S) :

Включить DST

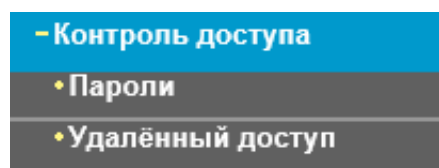
Начало: 1970
Конец: 1970

Автоматически синхронизировать с серверами мирового времени

Укажите первый NTP-сервер времени:
Укажите второй NTP-сервер времени:
Укажите третий NTP-сервер времени:
Укажите четвертый NTP-сервер времени:
Укажите пятый NTP-сервер времени:
Смещение часового пояса:

Рисунок 4-111

4.9.6 Контроль доступа



Меню **Контроль доступа** содержит два раздела: **Пароли** и **Удалённый доступ**. Далее представлено подробное описание по каждому разделу.

4.9.6.1 Пароли

На странице **Управление – Контроль доступа – Пароли** (см. Рисунок 4-112) можно изменить пароль маршрутизатора по умолчанию. Пароль по умолчанию совпадает с именем пользователя по умолчанию: admin/admin, support/support и user/user соответственно категории пользователя.

Контроль доступа – Пароль

Доступ к вашему маршрутизатору с DSL-модемом возможен через три учётных записи: admin, support и user.

Учётная запись "admin" предоставляет неограниченный доступ с возможностью изменения и просмотра настроек устройства.

Учётная запись "support" используется техническими специалистами поставщика Интернет-услуг для проведения диагностики и обслуживания устройства.

Учётная запись "user" предоставляет доступ к устройству с правом просмотра настроек и статистики, а также с возможностью обновления встроенного ПО.

В полях ниже можно ввести пароль длиной до 16 символов. Нажмите "Сохранить/Применить", чтобы изменить/создать пароль. Примечание: пароль не может содержать пробелы.

Имя пользователя:	<input type="text" value="admin"/>
Старый пароль:	<input type="password"/>
Новый пароль:	<input type="password"/>
Подтвердить пароль:	<input type="password"/>

Рисунок 4-112

Чтобы изменить пароль:

1. Выберите **Имя пользователя**, для которого вы хотите изменить пароль.
2. В поле **Старый пароль** введите текущий используемый пароль.
3. В полях **Новый пароль** и **Подтвердить пароль** укажите новый пароль.
4. Нажмите **Сохранить/Применить**, чтобы ваши настройки вступили в силу.

Примечание:

- 1) Доступ к вашему маршрутизатору с DSL-модемом возможен через три учётных записи: admin, support и user. Учётная запись "admin" предоставляет неограниченный доступ с возможностью изменения и просмотра настроек устройства. Учётная запись "support" используется техническими специалистами поставщика Интернет-услуг для проведения диагностики и обслуживания устройства. Учётная запись "user" предоставляет доступ к устройству с правом просмотра настроек и статистики, а также с возможностью обновления встроенного ПО.
- 2) Можно осуществлять удалённое управление через учётные записи "admin" и "support". Если вы включили функцию удалённого доступа, настоятельно рекомендуется изменить пароли по умолчанию для этих двух учётных записей.

- 3) Пароль не может содержать пробел, максимальная длина пароля составляет 16 символов.

4.9.6.2 Удалённый доступ

На странице **Управление – Контроль доступа – Удалённый доступ** (см. Рисунок 4-113) можно изменять пароль для доступа на маршрутизатор по умолчанию.

Контроль доступа – Удалённый доступ

Доступ к вашему устройству через WAN-интерфейс с помощью учётных записей user (**support** и **admin**).

Выберите WAN-интерфейс:

Web:

Telnet:

ICMP(ping):

Рисунок 4-113

- **Web:** Отметьте эту опцию, чтобы заходить на маршрутизатор через web-браузер.
- **Telnet:** Отметьте эту строку, чтобы заходить на маршрутизатор через командную строку.
- **ICMP (ping):** Отметьте эту строку, чтобы компьютер в публичной сети мог отправлять ping-запрос на WAN-адрес маршрутизатора.

Нажмите **Сохранить/Применить** для вступления ваших настроек в силу.

4.9.7 Обновление встроенного ПО

На странице **Управление – Обновление встроенного ПО** (см. Рисунок 4-114) можно обновить встроенное ПО маршрутизатора до последней версии.

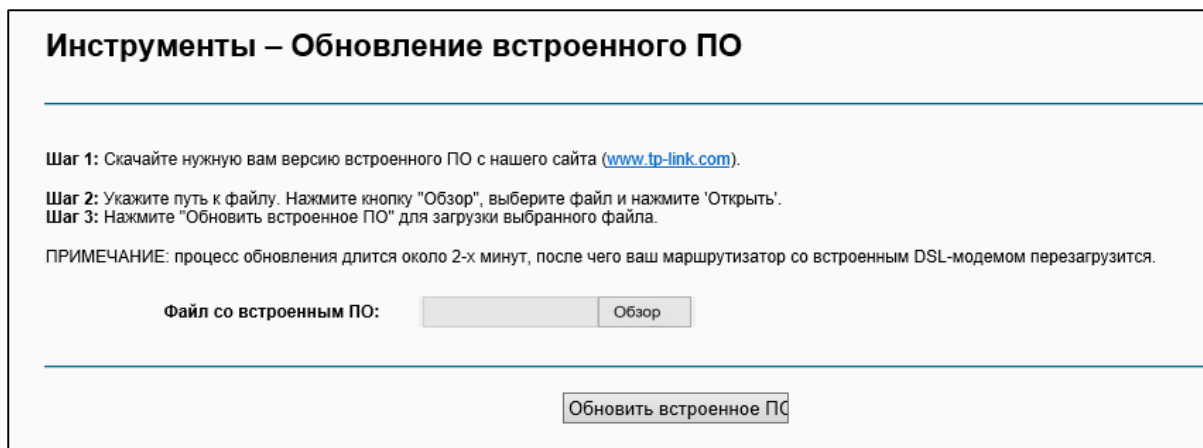


Рисунок 4-114

- **Обзор:** Нажмите эту кнопку, чтобы выбрать файл со встроенным ПО маршрутизатора.
- **Обновить встроенное ПО:** Нажмите эту кнопку после того, как вы выбрали файл.

Чтобы обновить встроенное ПО маршрутизатора:

1. Скачайте последнюю версию встроенного ПО с сайта **TP-LINK** (<http://www.tp-link.com>).
2. Нажмите кнопку **Обзор** и выберите со встроенным ПО либо укажите путь к файлу вручную.
3. Нажмите кнопку **Обновить встроенное ПО**.

Примечание:

- 1) Нет необходимости обновлять программное обеспечение, если оно не содержит необходимую вам новую функцию. Тем не менее, при возникновении проблем, связанных непосредственно с маршрутизатором, а не с его настройками, следует произвести обновление встроенного ПО.
- 2) Перед обновлением встроенного ПО маршрутизатора запишите настройки наиболее важных параметров, которые вы сами настраивали ранее, чтобы не забыть их.
- 3) При обновлении встроенного ПО не выключайте питание маршрутизатора и не нажимайте кнопку RESET на маршрутизаторе.
- 4) По завершении обновления устройство автоматически выполнит перезагрузку.

4.9.8 Перезагрузка

На странице **Управление – Перезагрузка** (см. Рисунок 4-115) можно осуществить перезагрузку маршрутизатора.

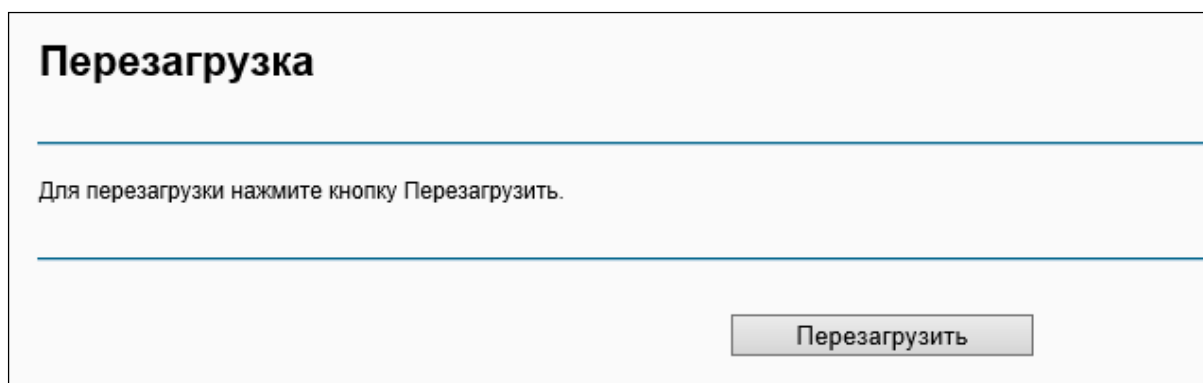


Рисунок 4-115

 **Примечание:**

- 5) После того как вы нажали кнопку **Перезагрузить**, подождите немного прежде чем снова открывать веб-браузер.
- 6) Во время процесса перезагрузки не выключайте питание и не нажимайте кнопку RESET на маршрутизаторе.
- 7) При необходимости перенастройте IP-адрес компьютера, чтобы он подходил новым настройкам маршрутизатора.

4.10 Выход

Выбрав в меню **Выход**, вы вернётесь на страницу авторизации для входа в маршрутизатор (см. Рисунок 4-116).

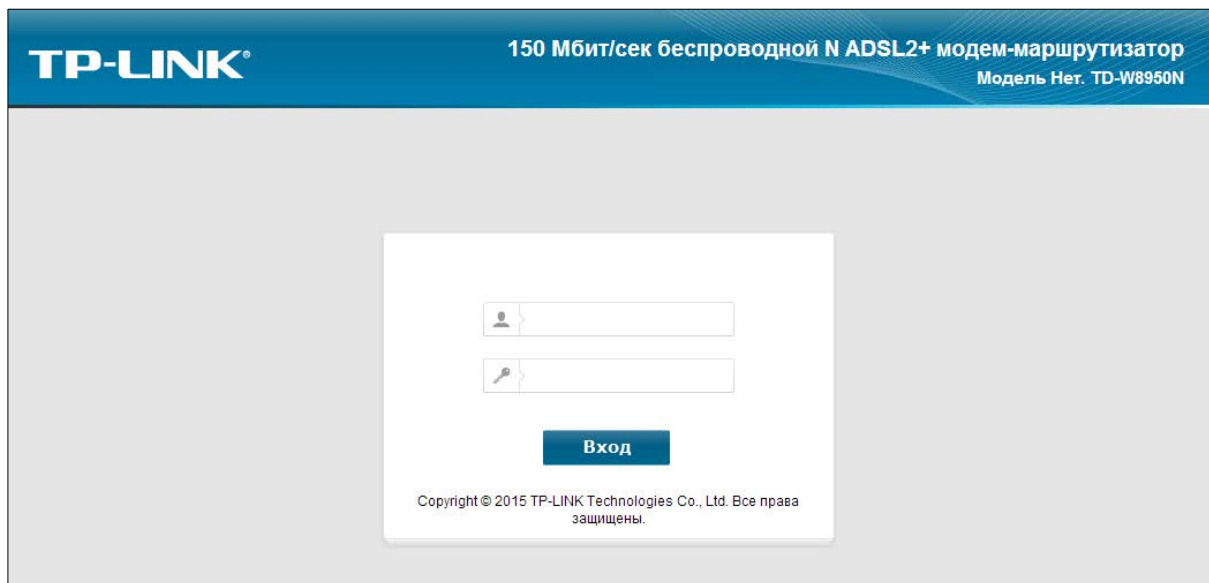


Рисунок 4-116

Приложение А: Спецификации

Общие параметры	
Стандарты	ANSI T1.413, ITU G.992.1, ITU G.992.2, ITU G.992.3, ITU G.992.5, IEEE 802.3, IEEE 802.3u, IEEE 802.11b , IEEE 802.11g , 802.11n
Протоколы	TCP/IP, IPoA , PPPoA , PPPoE, SNTP, HTTP, DHCP, ICMP, NAT
Порты	Четыре порта RJ45 10/100 Мбит/с с автосогласованием (Авто-MDI/MDIX)
	Один порт RJ11
Тип кабеля	10BASE-T: неэкранированная витая пара кат. 3, 4, 5 EIA/TIA-568 100Ω STP (максимум 100m)
	100BASE-TX: неэкранированная витая пара кат. 5, 5e EIA/TIA-568 100Ω STP (максимум 100m)
Светодиодные индикаторы	Ⓜ Power (Питание), Ⓜ ADSL, Ⓜ Internet (Интернет), Ⓜ WLAN, Ⓜ WPS, Ⓜ 1,2,3,4 (LAN) – Локальная сеть
Сертификация	FCC, CE

Беспроводной	
Диапазон частот	2.4~2.4835GHz
Скорость передачи данных	11n: TD-W8950N до 150 Мбит/с (Авто) TD-W8960N до 300 Мбит/с (Авто) 11g: 54/48/36/24/18/12/9/6 Мбит/с (Авто) 11b: 11/5.5/2/1 Мбит/с (Авто)
Расширение частот	DSSS(Direct Sequence Spread Spectrum)
Модуляция	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
Безопасность	WEP/WPA/WPA2/WPA2-PSK/WPA-PSK
Чувствительность @PER	130M: -64дБм@10% PER (процент пакетов с ошибками); 54M: -68дБм@10% PER 11M: -85дБм@8% PER 6M: -88дБм@10% PER 1M: -90дБм@8% PER

Физическая и окружающая среда	
Температура	Рабочая: 0°C~40°C (32°F~104°F)
	Хранения: -40°C~70°C(-40°F~158°F)
Влажность	Рабочая: 10% ~ 90% RH, без образования конденсата
	Хранения: 5% ~ 90% RH, без образования конденсата

Приложение В: Настройки ПК

В этом разделе мы расскажем, как установить и настроить правильно TCP/IP в Windows7. Сначала убедитесь, работает ли ваш Ethernet адаптер, обратитесь к ручным настройкам адаптера если необходимо.

1. Настройки компонента TCP/IP

- 1) На панели задач Windows, нажмите кнопку **Старт**, и затем нажмите **Панель управления**.
- 2) Нажмите значок **Сеть и интернет**, и затем нажмите вкладку **Сетевые подключения** в появившемся окне.
- 3) Щелкните правой мышкой по значку, показанному ниже, выберите свойства в диалоговом окне.

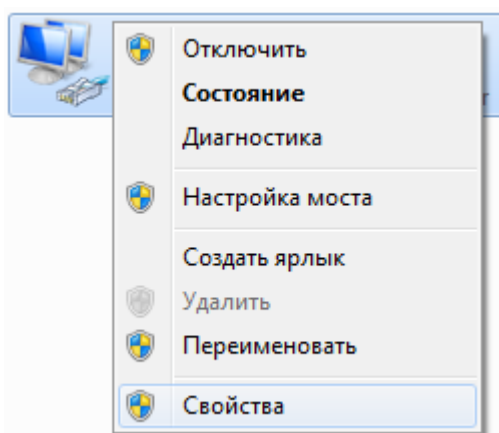


Рисунок В-1

- 4) В диалоговом окне, которое показано ниже, дважды щелкните на **Интернет протокол (TCP/IP)**.

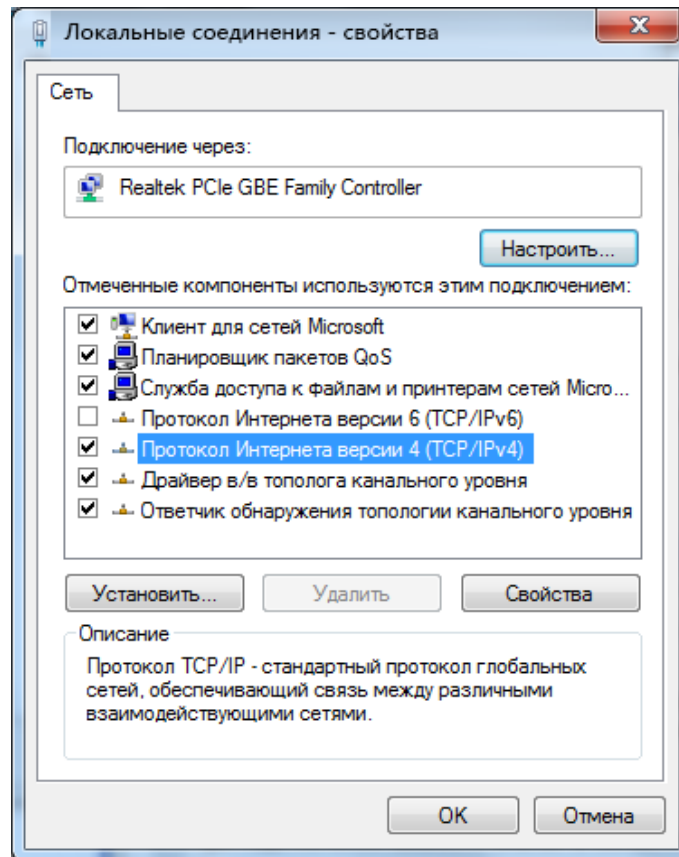


Рисунок В-2

- 5) Появится следующее окно **Свойства TCP/IP** и вкладка **IP-адрес** откроется в этом окне по умолчанию.

Теперь у вас есть два способа настройки протокола **TCP/IP** ниже:

➤ **Настроить IP адрес автоматически**

Выберите **Получить IP адрес автоматически**, выберите **Получить DNS сервер автоматически**, как показано на Рисунке ниже:

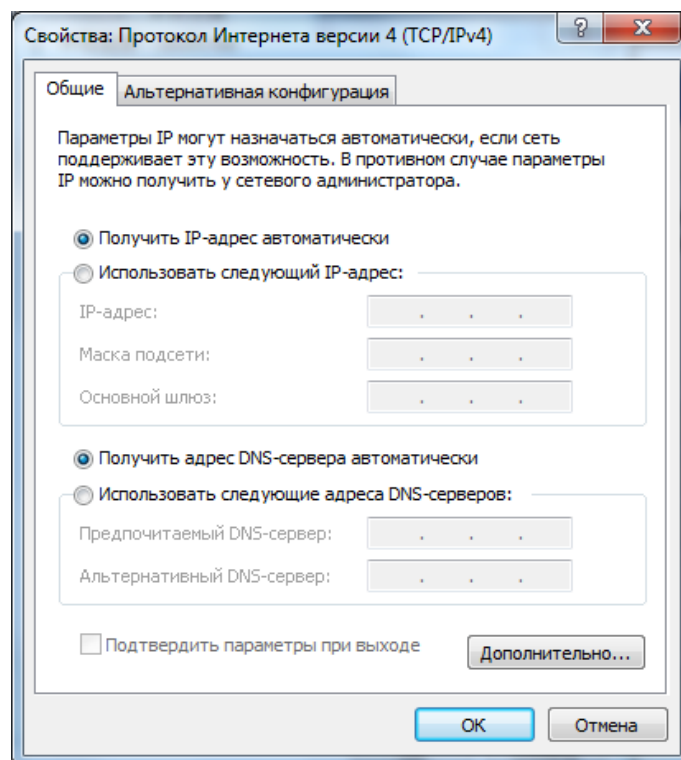


Рисунок В-3

👉 Примечание:

Для ОС Windows 98 или раньше, ПКИ маршрутизатору может потребоваться перезагрузка.

➤ **Настройка IP адреса вручную**

- 1 Выберите переключатель **Использовать следующий IP адрес**. Исследуемые элементы будут доступны
- 2 Если LAN IP адрес маршрутизатора 192.168.1.1, укажите **IP адрес** – 192.168.1.x (где x от 2 до 254) и **Маску подсети** – 255.255.255.0.
- 3 Введите LAN IP адреса маршрутизатора (по умолчанию IP 192.168.1.1) в поле **Основной шлюз**.
- 4 Выберите **Использовать следующие DNS сервер адреса**. В поле **Предпочитаемый DNS сервер** вы можете ввести такое же значение, как **Основной шлюз** или введите локальный DNS сервер IP адрес.

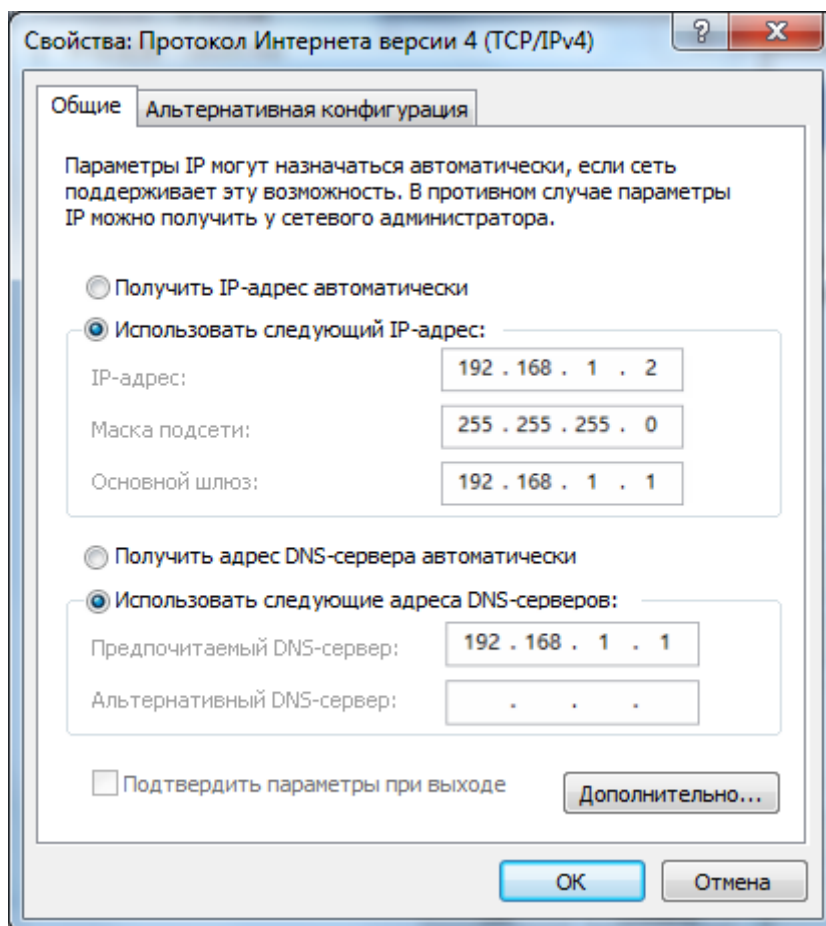


Рисунок В-4

Затем:

Нажмите **ОК**, чтобы сохранить ваши настройки.

Приложение С: Устранение неисправностей

T1. Что делать, если я не знаю или забыл пароль?

1) Пароль беспроводной сети по умолчанию: Пароль беспроводной сети по умолчанию указан на соответствующей наклейке (“Пароль беспроводной сети/PIN”) на нижней панели устройства.

2) Пароль для входа в веб-утилиту настройки: Сначала восстановите заводские настройки. Имя пользователя и пароль по умолчанию: admin/admin.

T2. Как восстановить заводские настройки маршрутизатора?

Не отключая питания маршрутизатора, с помощью булавки нажмите и удерживайте нажатой 8-10 секунд кнопку **RESET**, расположенную на задней панели устройства.

Примечание:

После сброса настроек текущие настройки будут утеряны, поэтому вам придётся перенастраивать маршрутизатор заново.

T3. Что делать, если я не могу зайти в веб-утилиту настройки маршрутизатора?

1) Настройте IP-адрес компьютера.

Для Mac OS X

- Нажмите на значок **Apple** на панели задач вашего компьютера.
- Перейдите в раздел **Системные настройки – Сеть**.
- Выберите **Ethernet** в меню слева, после чего нажмите **Дополнительно** для настройки проводного подключения или выберите **AirPort** для настройки беспроводного подключения.
- Откройте вкладку **TCP/IP**, затем ниже выберите значение **Использовать DHCP** из выпадающего списка **Конфигурировать IPv4**.
- Нажмите **Применить** для сохранения настроек.

Для Windows 7

- Откройте меню **Пуск – Панель управления – Сеть и Интернет – Просмотр состояния сети и задач – Изменение параметров адаптера**.
- Правой кнопкой мыши нажмите на **Беспроводное сетевое соединение (или Подключение по локальной сети)**, затем нажмите **Свойства**.
- Выберите **Протокол Интернета версии 4(TCP/IPv4)** и нажмите **Свойства**.
- Выберите **Получить IP-адрес автоматически** и **Получить адрес DNS-сервера автоматически**, после чего нажмите **ОК**.

Для Windows XP

- Откройте меню **Пуск – Панель управления**. Выберите **Сети подключение к Интернету – Сетевые подключения**.
- Правой кнопкой мыши нажмите на **Беспроводное сетевое соединение (или Подключение по локальной сети)**, выберите **Свойства**.

- Выберите **Протокол Интернета** и нажмите **Свойства**.
- Выберите **Получить IP-адрес автоматически** и **Получить адрес DNS-сервера автоматически**, после чего нажмите **ОК**.

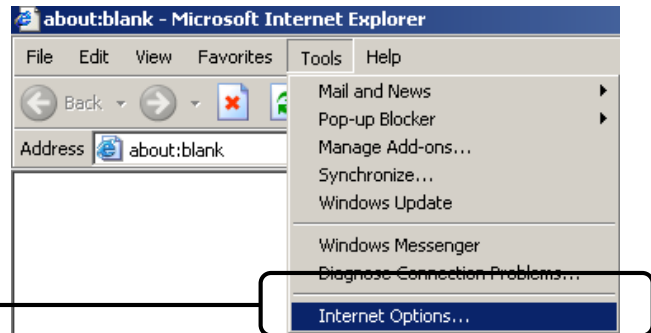
Для Windows 8

- Во всплывающем окне в нижнем правом углу экрана нажмите значок **Поиск** (🔍). Затем выберите **Приложения**, введите **Панель управления** в строке поиска и нажмите **Enter**. Вы попадёте на **Панель управления**.
- Выберите **Панель управления – Просмотр состояния сети и задач – Изменение параметров адаптера**.
- Правой кнопкой мыши нажмите на Ethernet, выберите **Свойства**.
- Далее дважды нажмите на **Протокол интернета версия 4(TCP/IPv4)**. Выберите **Получить IP-адрес автоматически** и **Получить адрес DNS-сервера автоматически**, после чего нажмите **ОК**.

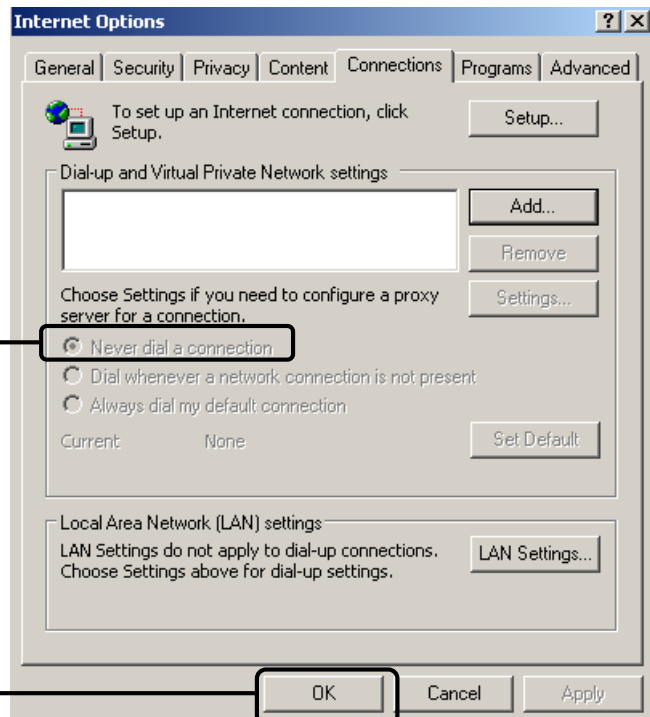
2) Настройте ваш браузер (для примера показан Internet Explorer)

Откройте браузер, в меню сверху зайдите в **Сервис**, вы увидите меню, как показано на рисунке справа.

Нажмите **Свойства обозревателя**



Выберите **Не использовать коммутируемые подключения**



Нажмите **ОК**

Теперь попробуйте снова зайти в веб-утилиту настройки после того, как были изменены указанные выше настройки. Если вы всё ещё не можете зайти в веб-утилиту настройки маршрутизатора, восстановите заводские настройки и перенастройте маршрутизатор заново согласно инструкциям раздела [3.2 Руководство по быстрой настройке](#). Если проблема не решена, свяжитесь со службой технической поддержки.

T4. Что делать, если пропал доступ к Интернет?

- 1) Проверьте, хорошо ли подключены все разъёмы, включая разъём телефонного кабеля, кабеля Ethernet и разъём адаптера питания.
- 2) Проверьте, можете ли вы зайти на страницу веб-утилиты настройки маршрутизатора. Если у вас получилось, следуйте указанным далее инструкциям. Если нет, настройте параметры TCP/IP компьютера, как указано в **пункте 3**, после чего снова проверьте, есть ли у вас доступ к веб-утилите настройки. Если проблема не решена, смотрите следующую инструкцию.
- 3) Свяжитесь с вашим поставщиком Интернет-услуг и уточните данные о VPI/VCI, типе подключения, имени пользователя и пароле для доступа к Интернет. Возможно, вами были указаны неверные данные, проверьте их и исправьте при необходимости.
- 4) Если проблема с доступом к Интернет не решена, восстановите заводские настройки вашего маршрутизатора и перенастройте модем заново согласно инструкциям раздела [3.2 Руководство по быстрой настройке](#).
- 5) Если ваша проблема осталась не решённой, пожалуйста, обратитесь в нашу службу технической поддержки.

Примечание:

Для более подробной информации по устранению неполадок и контактной информации технической поддержки, пожалуйста, зайдите на наш веб-сайт технической поддержки: <http://www.tp-link.com/ru/support>.

Приложение D: Техническая поддержка

- Для большей помощи по устранению неполадок, следуйте по ссылке:
<http://www.tp-link.com/ru/support/faq>
- Чтобы скачать последнее ПО, Драйвер, Утилиту и Руководство пользователя, следуйте по ссылке:
<http://www.tp-link.com/ru/support/download>
- По всей остальной технической поддержке, пожалуйста, свяжитесь с нами используя следующую информацию:

По всему миру

Тел.: +86 755 2650 4400
Тариф: в зависимости от тарифов различных операторов, услуги IDD (прямой набор международного номера).
E-mail: support@tp-link.com
Рабочее время: круглосуточно, без выходных

США/Канада

Тел.: +1 866 225 8139
Тариф: support.usa@tp-link.com(США)
support.ca@tp-link.com(Канада)
Рабочее время: круглосуточно, без выходных

Турция

Тел.: 0850 7244 488
Тариф: в зависимости от тарифов различных операторов
E-mail: support.tr@tp-link.com
Рабочее время: с 09:00 до 21:00, без выходных

Украина

Тел.: 0800 505 508
Тариф: бесплатно для городской связи; операторы мобильной связи: в зависимости от тарифов различных операторов
E-mail: support.ua@tp-link.com
Рабочее время: с понедельника по пятницу с 10:00 до 22:00

Бразилия

Звонок бесплатный: 0800 608 9799
E-mail: suporte.br@tp-link.com
Рабочее время: с понедельника по пятницу с 09:00 до 20:00, воскресенье: с 09:00 до 15:00

Индонезия

Тел.: (+62) 021 6386 1936
Тариф: в зависимости от тарифов различных операторов.
E-mail: support.id@tp-link.com
Рабочее время: с понедельника по пятницу с 09:00 до 12:00, и с 13:00 до 18:00
* Кроме праздничных дней

Австралия/Новая Зеландия

Тел.: NZ 0800 87 5465 (звонок бесплатный)
AU 1300 87 5465 (в зависимости от тарифов для номеров 1300)
E-mail: support.au@tp-link.com (Австралия)
support.nz@tp-link.com (Новая Зеландия)
Рабочее время: круглосуточно, без выходных

Германия/Австрия

Тел.: +49 1805 875 465
+49 1805 TPLINK
+43 820 820 360
Тариф: городская связь из Германии: 0,14 евро/мин.
городская связь из Австрии: 0,20 евро/мин.
E-mail: support.de@tp-link.com
Рабочее время: с 09:00 до 12:30 и с 13:30 до 18:00 с понедельника по пятницу. GMT+1 или GMT+2 (летнее время)
*Кроме праздничных дней в Германии

Сингапур

Тел.: +65 6284 0493
Тариф: в зависимости от тарифов различных операторов
E-mail: support.sg@tp-link.com
Рабочее время: круглосуточно, без выходных

Великобритания

Тел.: +44 (0) 845 147 0017
Тариф: городская связь: 1п-10,5п/мин., в зависимости от времени суток; операторы мобильной связи: 15п-40п/мин., в зависимости от тарифов различных операторов
E-mail: support.uk@tp-link.com
Рабочее время: круглосуточно, без выходных

Италия

Тел.: +39 023 051 9020
Тариф: в зависимости от тарифов различных операторов.
E-mail: support.it@tp-link.com
Рабочее время: с понедельника по пятницу с 09:00 до 13:00; с 14:00 до 18:00

Малайзия

Звонок бесплатный: 1300 88 875 465
Email: support.my@tp-link.com
Рабочее время: круглосуточно, без выходных

Польша

Тел.: +48 (0) 801 080 618
+48 223 606 363 (для звонков с мобильных телефонов)
Тариф: в зависимости от тарифов различных операторов
E-mail: support.pl@tp-link.com
Рабочее время: с понедельника по пятницу с 09:00 до 17:00. GMT+1 или GMT+2 (летнее время)

Франция

Тел.: 0820 800 860
Тариф: 0,118 евро/мин. из Франции
Email: support.fr@tp-link.com
Рабочее время: с понедельника по пятницу с 09:00 до 18:00
* Кроме праздничных дней во Франции

Швейцария

Тел.: +41 (0) 848 800 998
Тариф: 4-8 Rp/мин, в зависимости от тарифов различных операторов
E-mail: support.ch@tp-link.com
Рабочее время: с понедельника по пятницу с 09:00 до 12:30 и с 13:30 до 18:00. GMT+1 или GMT+2 (летнее время)

Российская Федерация

Тел.: 8 (499) 754 5560 (Москва)
8 (800) 250 5560 (звонок бесплатный из любого региона РФ)
E-mail: support.ru@tp-link.com
Форум: <http://forum.tp-link.ru/>
Рабочее время: с понедельника по субботу, с 9:00 до 21:00 (мск)
* Кроме выходных и праздничных дней в Российской Федерации