VigorFly 200

Wi-Fi маршрутизатор

Руководство пользователя

Версия 1.0

DrayTek

VigorFly 200
Wi-Fi маршрутизатор
Руководство пользователя

Версия: 1.0

от 17.03.2010

Информация о защите прав

Декларация защиты авторских прав

Торговые марки

В данном документе используются следующие торговые марки:

- Microsoft – зарегистрированная торговая марка Microsoft Corp.
- Windows, Windows 95, 98, Me, NT, 2000, XP, Vista и Explorer являются торговыми марками Microsoft Corp.
- Apple и Mac OS зарегистрированные торговые марки Apple Inc.
- Другие продукты могут быть торговыми марками или зарегистрированными торговыми марками соответствующих производителей.

Инструкции по безопасности

Инструкции по безопасности

- Перед началом эксплуатации маршрутизатора внимательно прочитайте руководство пользователя
- Маршрутизатор – сложное техническое устройство. Не пытайтесь вскрыть и отремонтировать маршрутизатор самостоятельно. Ремонт должны проводить только сертифицированные и квалифицированные специалисты.
- Не храните и не эксплуатируйте маршрутизатор в местах с повышенной влажностью, например, в ванной. Избегайте попадания влаги на корпус и внутрь устройства.
- Маршрутизатор должен использоваться в закрытых помещениях при температуре воздуха от +5°C до +40°C.
- Избегайте эксплуатации устройства под воздействием прямого солнечного света и вблизи источников тепла. Это может вызвать повреждение корпуса и электронных компонентов устройства вследствие перегрева.
- Не размещайте на улице кабель подключения к электросети и адаптер питания, это увеличивает риск поражения электрическим током.
- Храните и эксплуатируйте устройство в недосягаемом для детей месте.
- При эксплуатации маршрутизатора, учитывайте местные законы по охране природы.

Гарантия

Мы гарантируем потребителям отсутствие дефектов в наших устройствах и его материалах в течение 1 (одного) года с момента приобретения его у дилера. Пожалуйста, сохраняйте ваш чек после покупки устройства, поскольку именно он содержит информацию о дате покупки. В случае если в течение одного года с момента покупки изделия обнаружится какая-либо неисправность устройства или несовершенство его материалов, мы обязуемся, по нашему усмотрению, отремонтировать или заменить дефектную продукцию или ее компоненты без взимания платы за запасные части или работу специалистов. При этом мы полагаем необходимым доставить устройство в авторизованный сервисный центр, чтобы привести его в рабочее состояние. Любая замена будет состоять в установке нового или восстановленного продукта той же цены и будет предложена исключительно по нашему усмотрению. Эта гарантия не будет выполнена в случае, если продукт был модифицирован, неверно использован, испорчен или работал не в нормальных условиях. Гарантия не покрывает дополнительное или лицензированное программное обеспечение (ПО) других поставщиков. Устранение дефектов, существенно не влияющих на работу устройства, не покрывается гарантией. Мы сохраняем за собой право обновлять печатную и онлайн-документацию и вносить изменения в содержание без обязательств уведомления об этом.

Станьте зарегистрированным пользователем

Вы можете зарегистрировать свой маршрутизатор на нашем интернет-сайте http://www.draytek.com.

Обновление программного обеспечения (ПО)

ПО маршрутизаторов будет регулярно обновляться благодаря непрерывному развитию технологий DrayTek. Используйте сайт DrayTek **http://www.draytek.com**, чтобы найти последние версии ПО и необходимую документацию.

Декларация для Европейского Сообщества

Производитель: DrayTek Corp.

Адрес: No. 26, Fu Shing Road, HuKou County, HsinChu Industrial Park, Hsin-Chu, Taiwan 303

Продукт: VigorFly 200 Series Router

Корпорация DrayTek заявляет, что маршрутизатор VigorFly 200 соответствует важнейшим требованиям и актуальным положениям Директивы R&TTE 1999/5/EEC.

Продукт соответствует требованиям Электромагнитной Совместимости, установленной Директивой 2004/108/EC в соответствии с требованиями, изложенными в EN55022/Class B и EN55024/Class B.

Продукт соответствует требованиям директивы Low Voltage (LVD) Directive 2006/95/ в соответствии с требованиями, изложенными в EN60950-1.

Этот продукт предназначен для WLAN-сетей 2.4Гц в регионах Европейского Сообщества и Швейцарии с ограничениями по Франции. Информацию о подходящих сетях вы найдете на вашем продукте.

Содержание

1 Коротко об устройстве

VigorFly 200 – широкополосный маршрутизатор с поддержкой беспроводных сетей стандарта 802.11n. К порту Ethernet WAN можно подключать Ethernet коммутаторы и VDSL/VDSL2/GPON/G.SHDSL/ADSL2+/ADSL модемы для работы с выделенной линией. Производительность при работе в режиме трансляции сетевых адресов (NAT) позволяет обеспечить непрерывную передачу мультимедийного потока с высокой скоростью. С помощью встроенного коммутатора на 4 порта 10/100 Ethernet LAN вы можете объединить ваш персональный компьютер (ПК) с компьютерами членов вашей семьи или ваших друзей и вместе пользоваться мультимедийными приложениями и одним выходом в Интернет. Наличие съемных антенн обеспечивает возможность быстрой и надежной работы беспроводной сети (WLAN). Если у вас нет выделенной линии, вы можете использовать с нашим устройством 4G WiMAX USB-модем для работы с сетью Yota. Так же вы можете подключить 3.5G USB-модем в USB-порт устройства VigorFly 200 для работы в сетях 3.5G (будет доступно в последующих версиях ПО). Подключение с помощью 3.5G / WiMAX-модемов обеспечит приемлемые для рядового пользователя возможности приема/передачи данных. Так же к порту USB может быть подключено печатающее устройство, и маршрутизатор будет служить принт-сервером.

Поддержка работы беспроводных сетей стандарта 802.11n Draft 2.0 обеспечит пользователям стабильную и надежную беспроводную связь для высокоскоростной передачи информации с поддержкой технологии WMM (Wi-Fi Мультимедиа).

1.1 Веб-конфигурация и кнопки

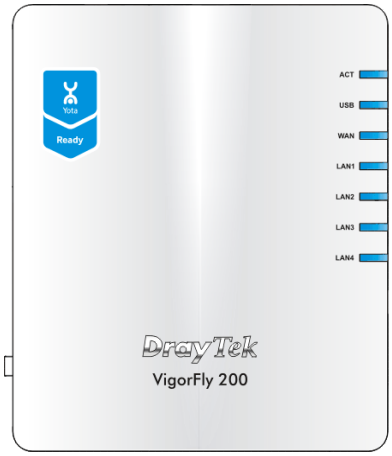
Основные кнопки управления, используемые в веб-интерфейсе для настройки:

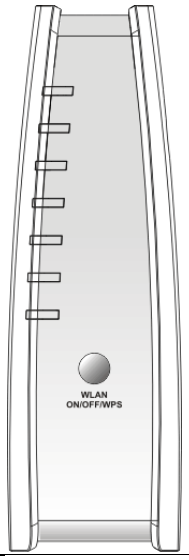
OK	Сохранить и применить настройки.
Отменить	Отменить изменения и вернуться к ранее сохраненным настройкам.
Очистить Все	Очистить все настройки параметров, включая настройки из выпадающего списка. Будут восстановлены настройки по умолчанию.
Добавить	Добавить новые настройки для выбранного пункта.
Редактировать	Редактировать настройки выбранного пункта.
Удалить	Удалить выбранный пункт вместе с соответствующими настройками.

Примечание: Описание других кнопок, используемых в веб-интерфейсе, вы найдете в соответствующих главах настоящего руководства.

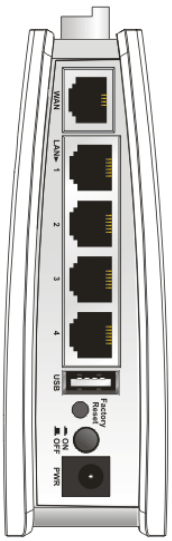
1.2 **Индикаторы и разъемы**

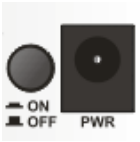
Перед использованием маршрутизатора ознакомьтесь с индикаторами и разъемами на устройстве.





Индикатор	Статус	Объяснение
ACT	Выкл	Система не готова или не работает
	Мигает	Система готова к работе и работает нормально.
USB	Вкл	USB-устройство подключено
	Мигает	Идет передача данных
WAN	Вкл	Есть подключение к WAN-порту
	Мигает	Идет передача данных
LAN 1 – 4	Вкл	Есть подключение к LAN-порту
	Выкл	Нет подключения LAN
	Мигает	Идет передача данных (прием/передача)
WLAN (синий) на кнопке WPS	Вкл	Беспроводная точка доступа готова
	Выкл	Беспроводная точка доступа не готова к работе
	Мигает (синий)	Идет передача данных по беспроводному каналу.
WPS (оранж) на кнопке WPS	Выкл	WPS отключен
	Мигает (оранж)	Мигает через каждую секунду в течение двух минут – WPS настроен и ожидает беспроводного подключения.
	Мигает (оранж)	Идет передача данных по беспроводному каналу.
WPS кнопка	Нажмите и удерживайте кнопку в течение 2-х секунд; ждите, пока устройство перейдет в режим WPS-подключения. После этого загорится оранжевый светодиод.	

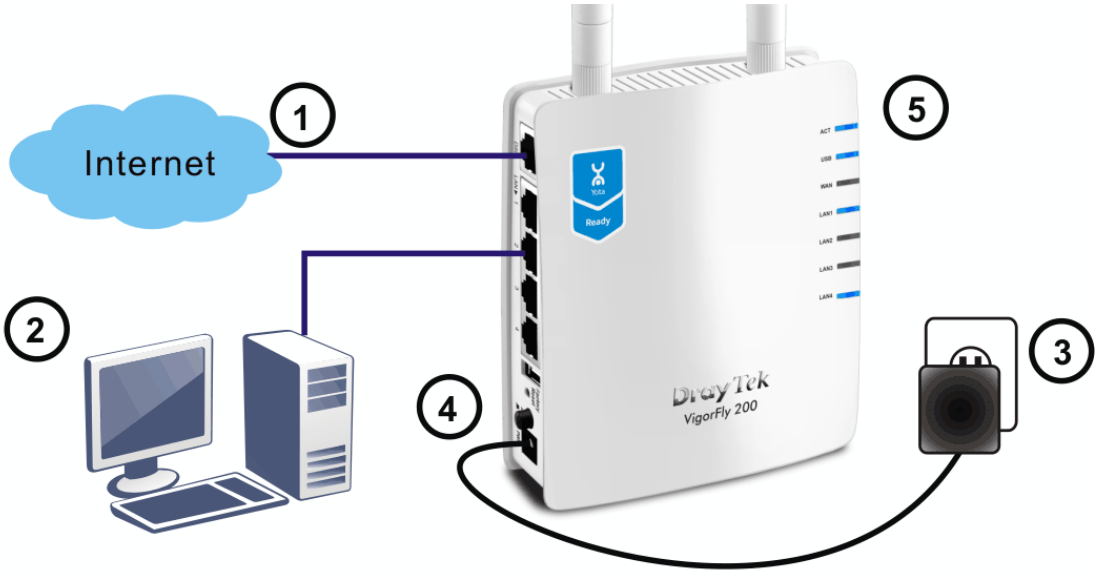


Интерфейс	Описание
WAN	Разъем для подключения к внешней сети (Интернет)
LAN (1-4)	Разъемы для подключения к локальной сети.
USB	Разъем для устройств памяти USB (Pen Driver/Mobile HD*), принтера или 3G/4G-модемов. *Будет доступно в следующих версиях ПО
	Возвращение настроек по умолчанию. **Использование**: включите маршрутизатор. Нажмите на кнопку и удерживайте более 10 секунд. Отпустите кнопку. Маршрутизатор перезагрузится, вернув настройки по умолчанию.
	ON/OFF: Кнопка включения/выключения питания. PWR: Разъем подключения питания.

1.3 Подключение оборудования

Перед настройкой маршрутизатора, вам необходимо правильно подключить устройство.

1. Подключите WAN порт устройства к модему или к другим сетевым устройствам (Ethernet коммутатор) с помощью Ethernet-кабеля.
2. Подсоедините LAN порт устройства к сетевому порту вашего ПК при помощи Ethernet-кабеля.
3. Подсоедините антенны.
4. Подключите разъем адаптера питания к соответствующему разъему на устройстве. Адаптер питания подключите к электросети 220В.
5. Включите маршрутизатор, нажав кнопку подключения питания.
6. Проверьте индикаторы **ACT, WAN** и **LAN**, чтобы убедиться в подключении к сети.



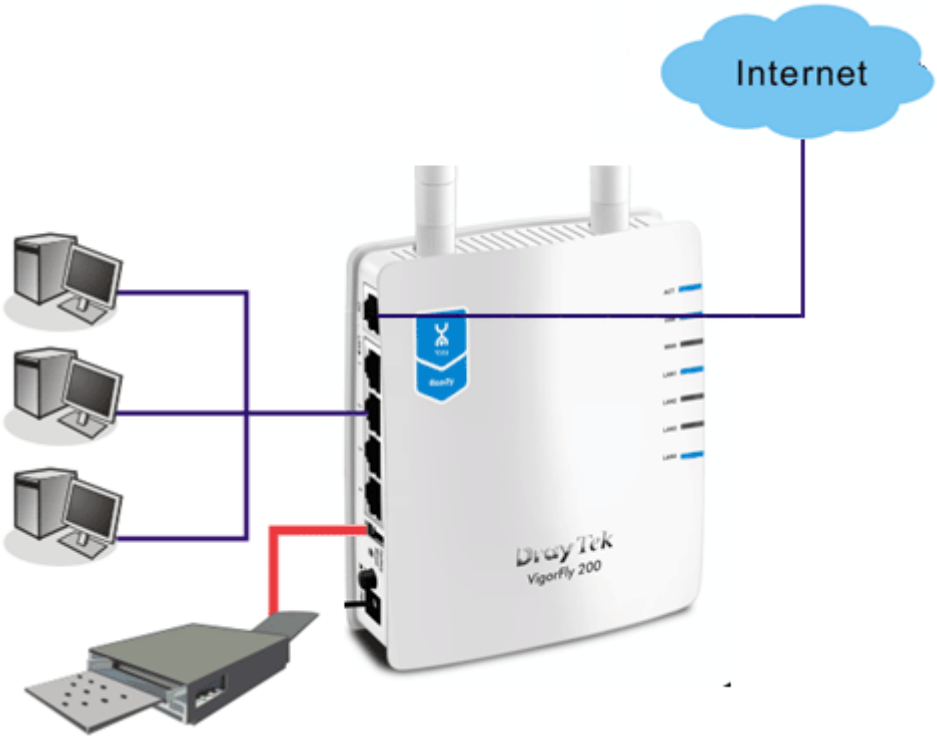
(Более подробную информацию об индикаторах см. в разделе 1.1)

1.4 Установка принтера

Вы можете использовать маршрутизатор как сервер печати. В этом случае все компьютеры, подключенные к маршрутизатору, смогут печатать документы с помощью одного принтера, подключенного к USB-порту устройства.

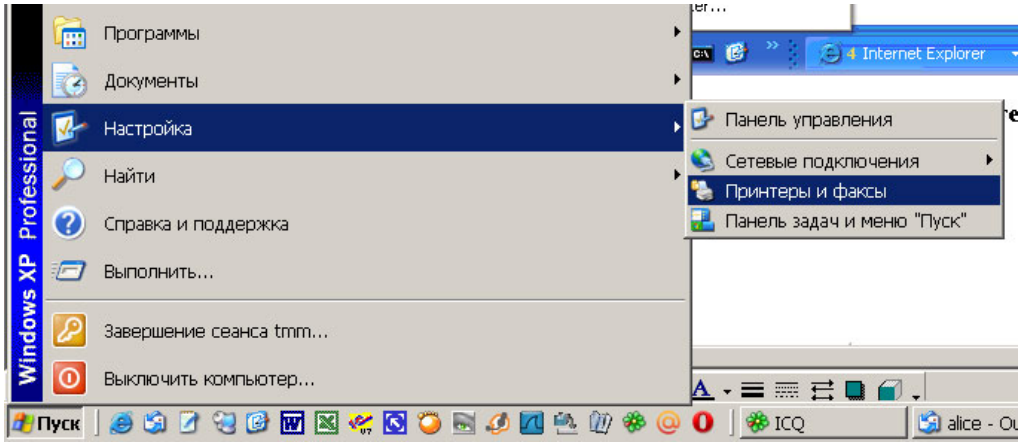
ВАЖНО: поддерживаются только принтеры с USB-портом.

В следующем примере рассмотрено подключение принтера для операционных систем Windows XP/2000. Инструкции для Windows 98/ME/Vista вы найдете на сайте **www.draytek.com**.

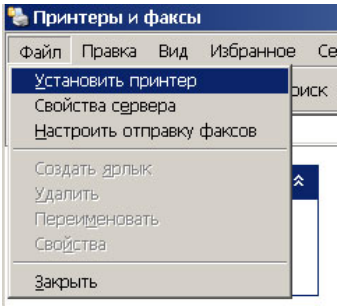


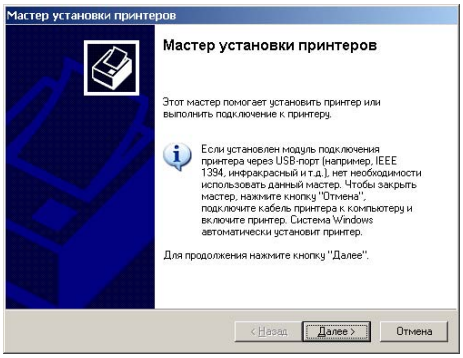
Перед использованием этой функции необходимо провести настройку вашего ПК.

1. Подключите принтер к маршрутизатору через USB порт.
2. Нажмите **Пуск -> Настройка -> Принтеры и факсы**

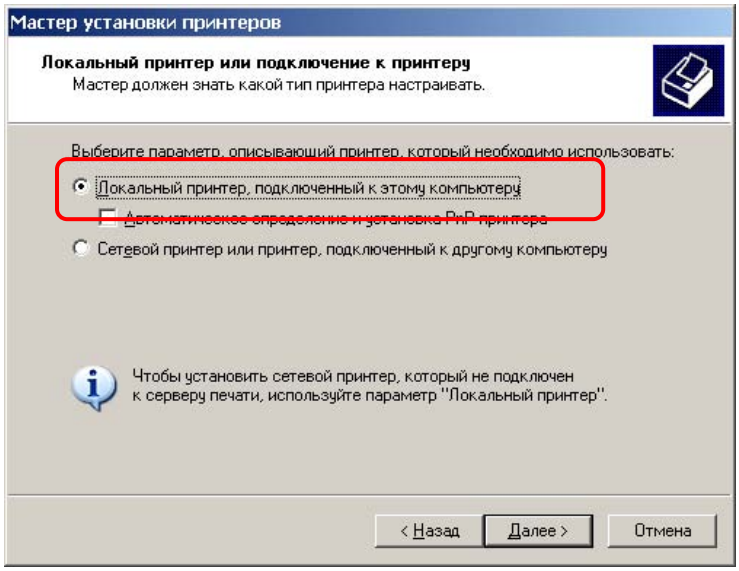


3. Откройте меню **Файл -> Установить принтер**. Появится новое диалоговое окно. Нажмите **Далее**.

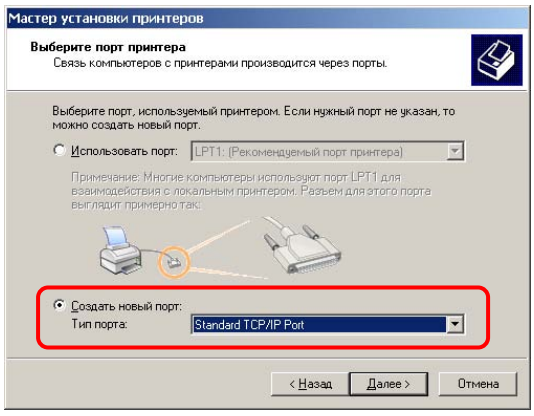


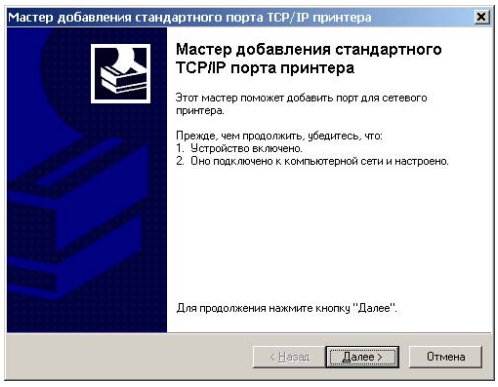


4. Выберите **Локальный принтер, подключенный к этому компьютеру** и нажмите **Далее**.

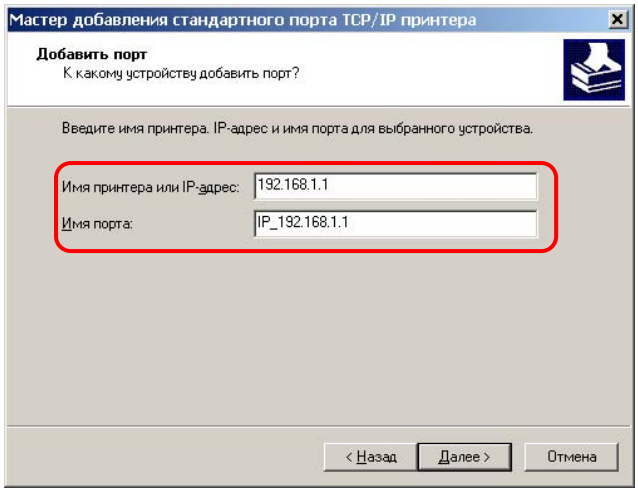


5. Выберите **Создать новый порт.** В разделе **Тип порта** используйте опцию **Standard TCP/IP Port** в выпадающем списке. Нажмите **Далее**. В следующем окне нажмите **Далее.**

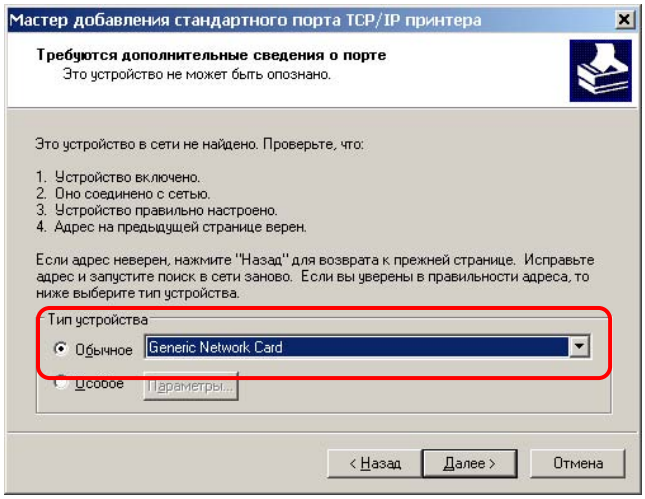




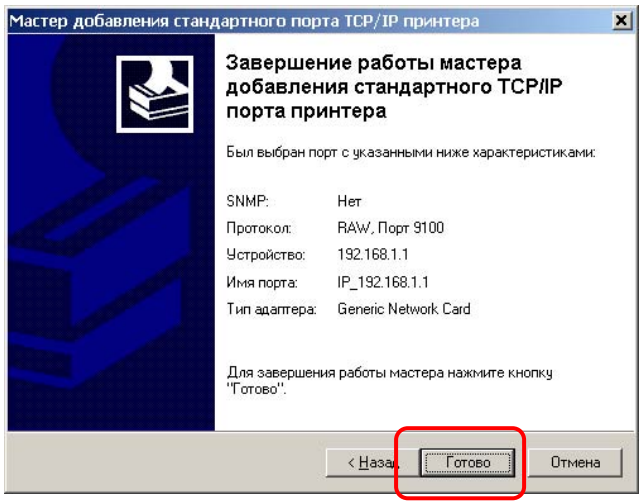
6. В новом окне введите **192.168.1.1** (IP-адрес маршрутизатора) в поле **Имя принтера или IP-адрес** и наберите **IP_192.168.1.1** в поле **Имя порта**. Нажмите **Далее**.



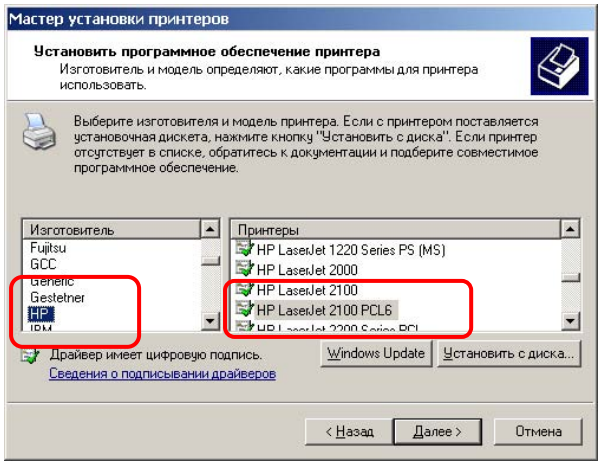
7. В меню **Тип устройства> Обычное** выберите **Generic Network Card**. Нажмите **Далее.**



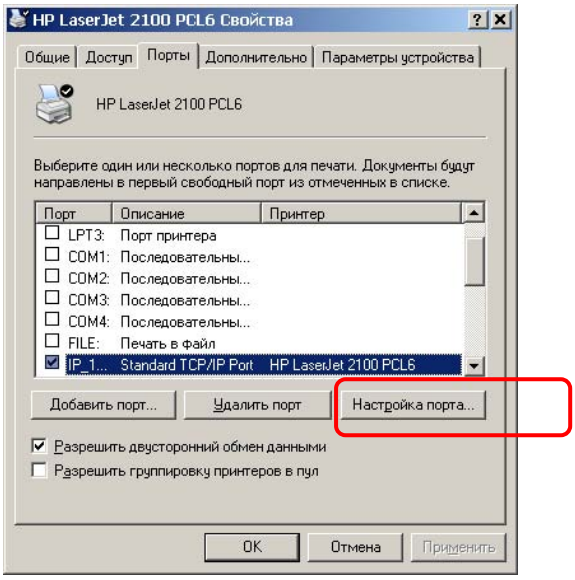
8. В следующем окне нажмите **Готово**.



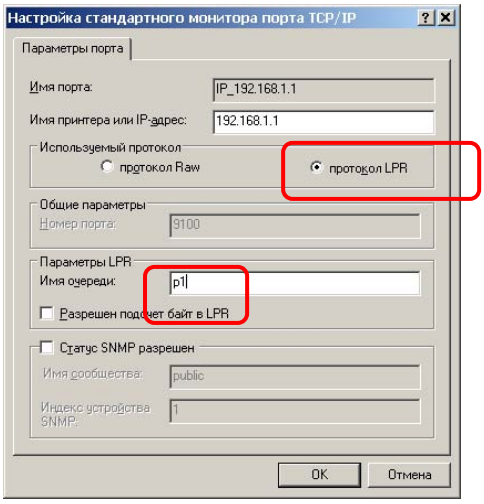
9. Теперь система попросит вас выбрать модель принтера, который вы будете использовать с маршрутизатором. Выберите производителя и модель из появившегося списка. После того как вы выберете нужную опцию, нажмите **Далее**. После этого система установит необходимые драйвера на ваш компьютер.



10. Для завершения настройки вам необходимо вернуться в меню **Панель управления -> Принтеры** и редактировать **Свойства** нового принтера. Там выберите закладку Порты, найдите строку в столбце Порт, которая отмечена галочкой и нажмите **Настройка порта…**



11. Выберите "**LPR**" в блоке **Используемый протокол**, введите **p1** в поле **Имя очереди**. Нажмите **OK.**



С маршрутизатором VigorFly 200 работают принтеры различных производителей.

Примечание 1: Некоторые принтеры, поддерживающие функции факсов и сканнеров, не поддерживаются. Если вы не знаете, поддерживается ли ваш принтер, посетите страницу www.draytek.com, где содержится список поддерживаемых принтеров. Откройте **Support >FAQ**; выберите раздел **Printer Server** и выберите вопрос **What types of printers are compatible with Vigor router**?.

Примечание 2: Маршрутизатор Vigor отвечает на запросы по печати только через LAN-порт, через WAN-порт печать не осуществляется.

2 Основные настройки

Для использования маршрутизатора необходимо поменять пароль для обеспечения безопасности и выполнить необходимые настройки. Эта часть объясняет, как установить пароль пользователя и как настроить маршрутизатор для успешного доступа в Интернет.

2.1 Двухуровневое управление

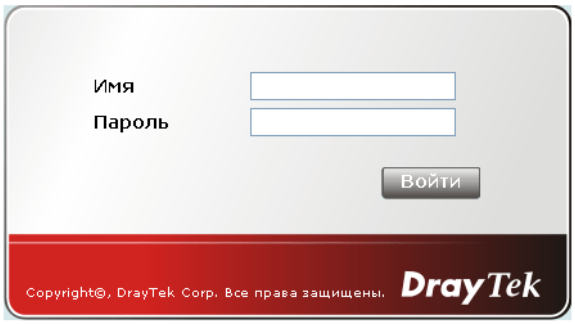
Маршрутизатор поддерживает двухуровневое управление: Режим пользователя и Режим администратора. Режимы отличаются возможностью изменения параметров системы. В режиме администратора доступно больше настроек.

2.2 Доступ к веб-интерфейсу управления

1. Убедитесь в том, что маршрутизатор подключен к компьютеру.

Примечание: вы можете настроить ваш компьютер так, чтобы он получал IP-адрес от маршрутизатора или настроить IP-адрес компьютера самостоятельно. IP-адрес ПК должен принадлежать к той же подсети, что и адрес маршрутизатора. По умолчанию адрес маршрутизатора **192.168.1.1**. Более подробную информацию вы найдете далее в разделе **Решение проблем**.

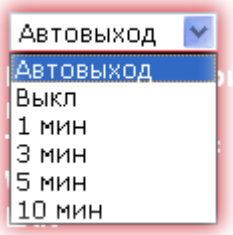
2. Откройте браузер на вашем компьютере и наберите адрес **http://192.168.1.1**. Появится следующее окно.



3. Для доступа в режиме пользователя оставьте все поля для ввода пустыми и нажмите **Войти**. Для входа в режиме администратора наберите **admin/admin** в полях **Имя /Пароль** и нажмите **Войти**. Вы получите доступ к расширенным настройкам.

Примечание: Если вы не можете получить доступ к Интернет-настройкам, откройте раздел **Решение проблем** данного руководства для определения и решения вашей проблемы.

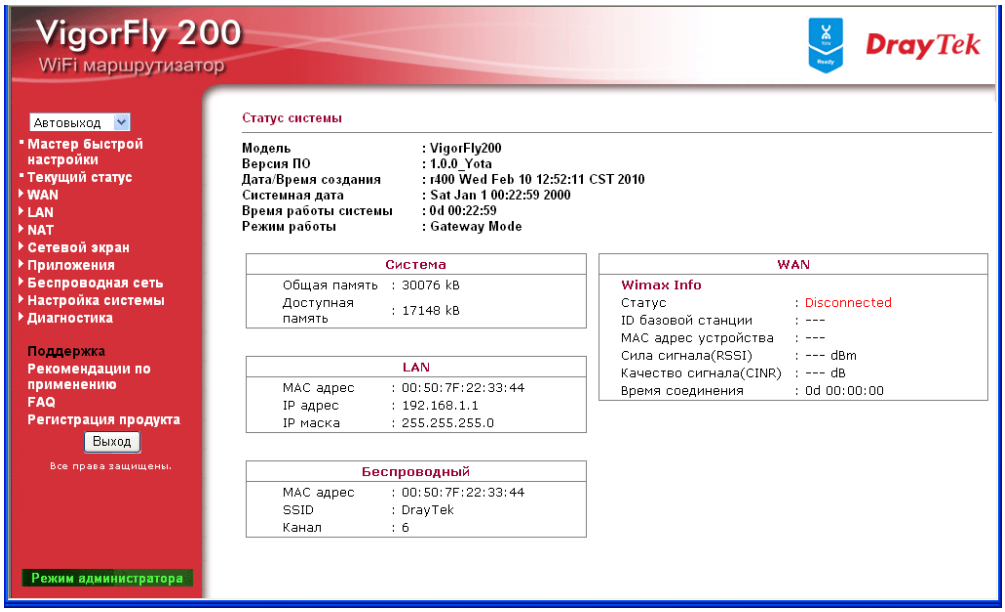
4. Вы можете установить политику длительности подключения к веб-интерфейсу. По умолчанию принята опция **Автовыход**. Это значит, что система автоматически прервет подключение через пять минут бездействия и для дальнейшей работы вам будет необходимо заново ввести данные учетной записи. Установите удобный вам режим работы.



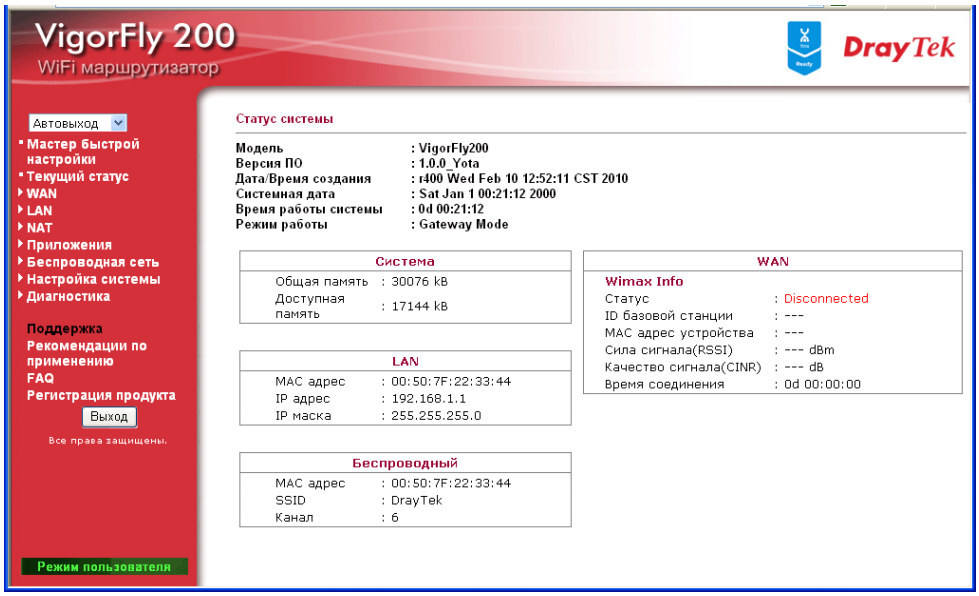
2.3 Смена пароля

Перед настройкой маршрутизатора, пожалуйста, смените пароль для надежной защиты маршрутизатора. Это можно сделать только в **Режиме администратора**.

1. Откройте браузер и наберите адрес **http://192.168.1.1.** В новом окне появится поле с именем пользователя и паролем.
2. Наберите admin/admin в полях Имя /Пароль для доступа к управлению в режиме администратора и нажмите **Войти**.



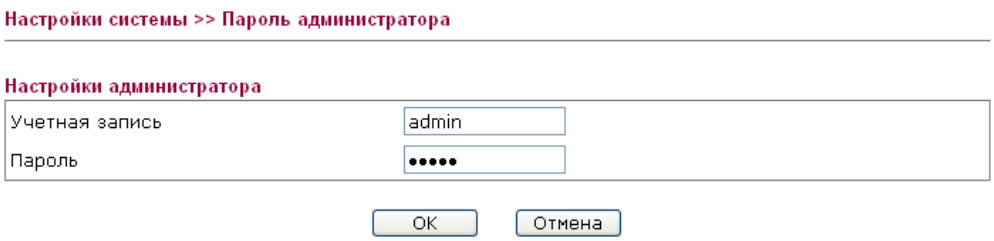
Главная страница в **Режиме администратора (полные настройки)**



Главная страница в **Режиме пользователя (базовые настройки)**

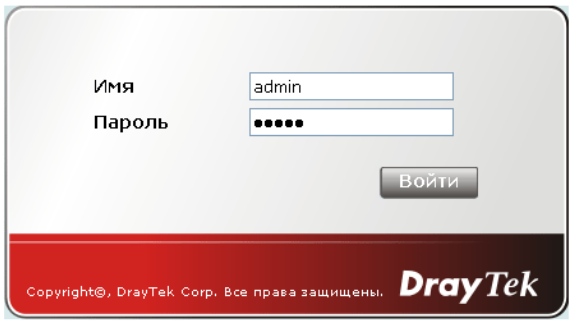
Примечание: Страница может немного различаться в зависимости от типа вашего маршрутизатора.

3. Чтобы сменить пароль, подключитесь **в Режиме администратора**. Зайдите на страницу **Настройки системы** и выберите **Пароль администратора**.



4. Введите новое имя пользователя и новый пароль. Нажмите **OK**. Вы сменили пароль.

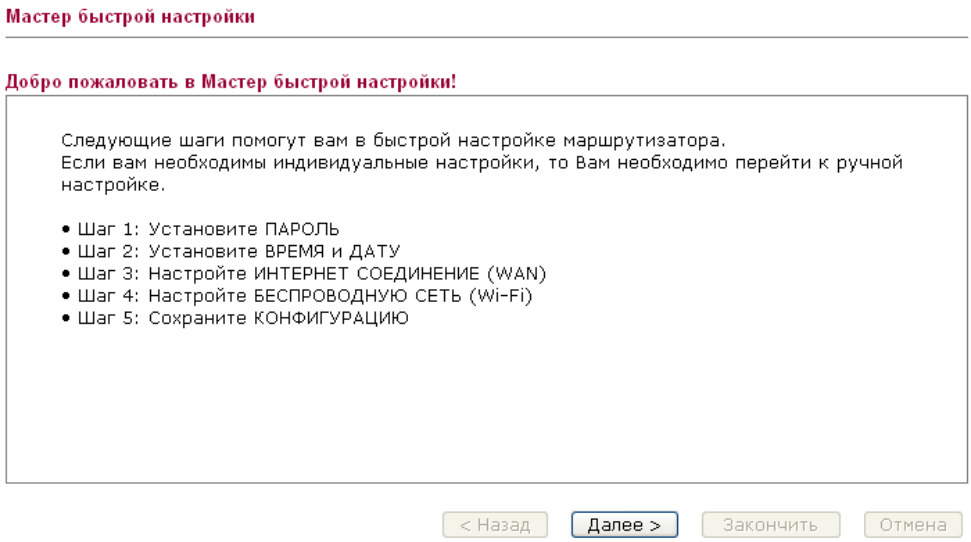
5. При следующем подключении к Интернет-странице с настройками маршрутизатора используйте новые имя пользователя и пароль.



2.4 Мастер быстрой настройки

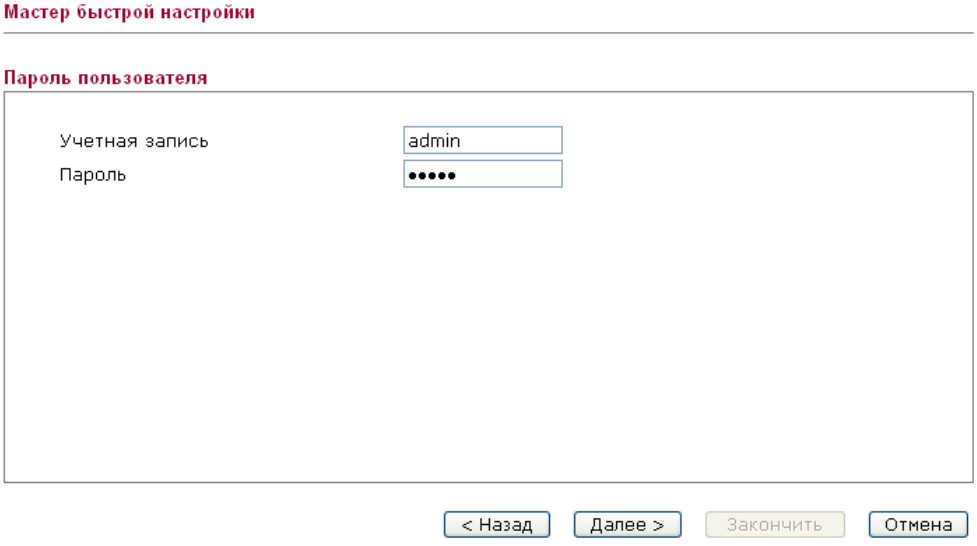
Примечание: Мастер быстрой настройки работает как в режиме пользователя, так и в режиме администратора.

Если ваш маршрутизатор поддерживает работу в режиме NAT, описанные ниже шаги помогут вам быстро настроить маршрутизатор и начать его использование. При вызове **Мастера быстрой настройки,** программа поприветствует вас. Нажмите **Далее**.



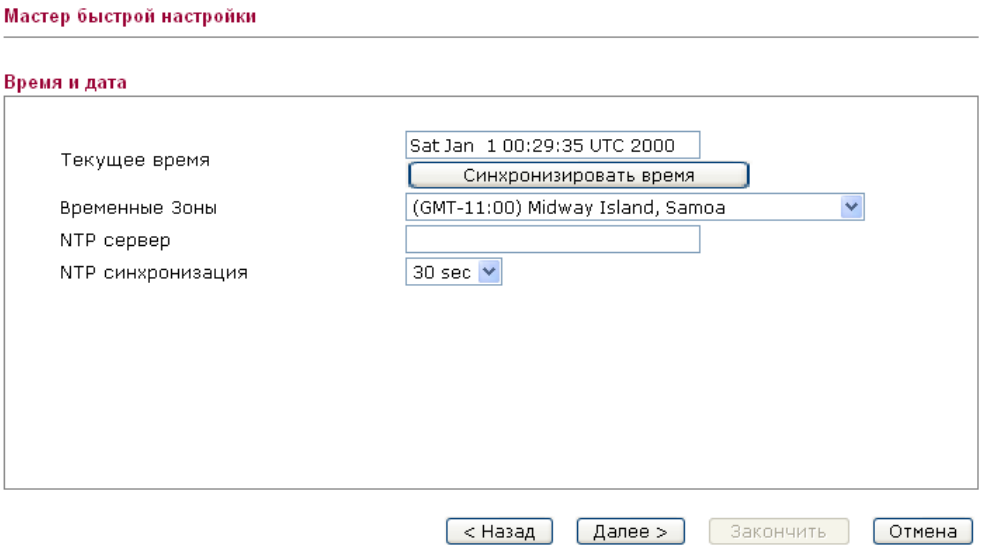
2.4.1 Ввод пароля

Введите новые имя пользователя и пароль на первой странице Мастера быстрой настройки. Нажмите **Далее**.



2.4.2 Настройка даты и времени

На следующей странице выберите необходимую Временную Зону (Часовой пояс) и введите адрес NTP-сервера. Если вы не знаете адреса, оставьте поле пустым. Нажмите **Далее**.

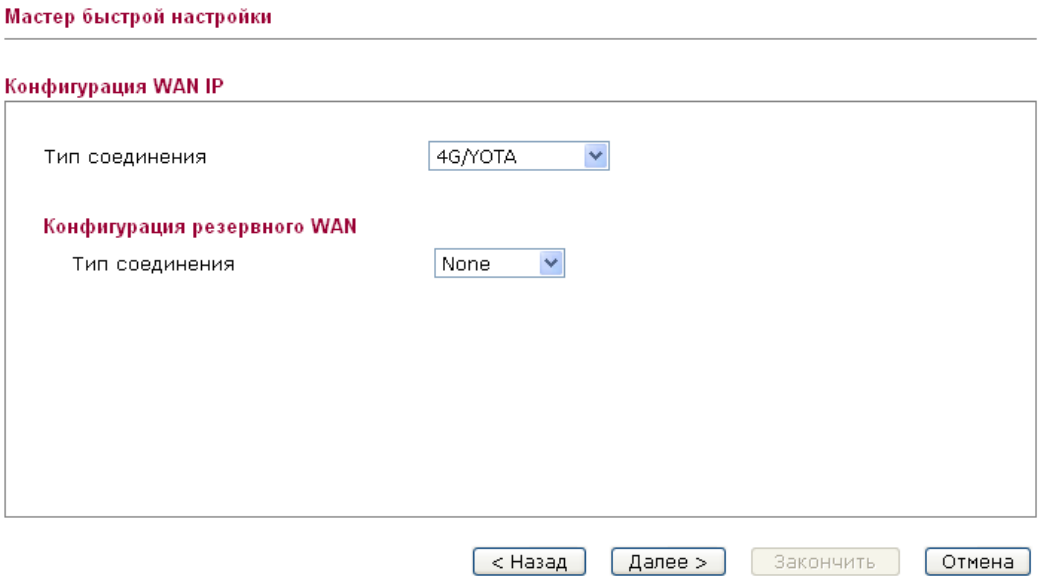


2.4.3 Настройка Интернет-подключения

На следующей странице выберите подходящий тип подключения в соответствии с услугами вашего провайдера. Существует пять вариантов подключения. Отображение следующей страницы зависит от вашего выбора.

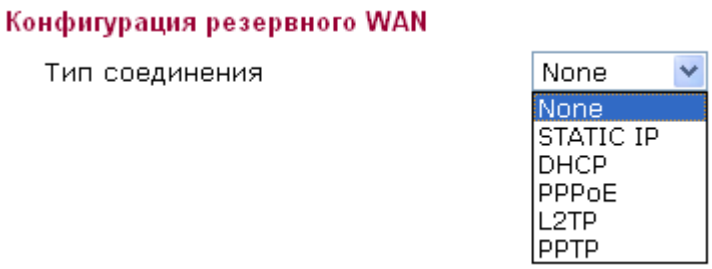
4G/YOTA

WAN-подключение по умолчанию – 4G/YOTA. Такой тип Интернет-подключения используется для работы в сети Yota WiMAX.



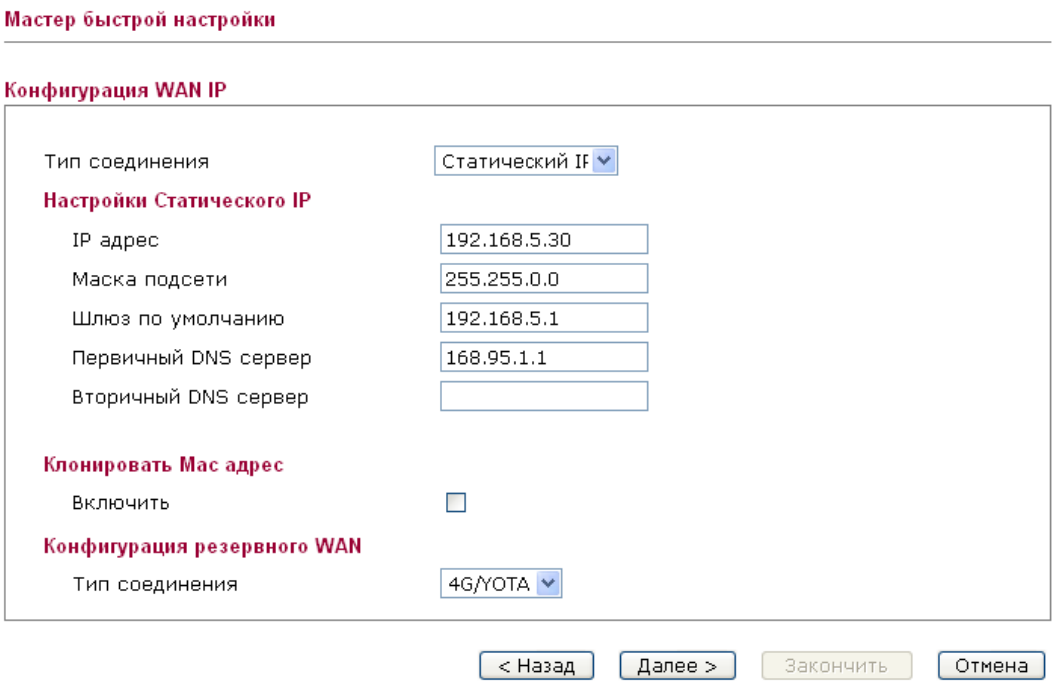
Для установки 4G-подключения не требуется никаких дополнительных настроек. Если вы не хотите настраивать резервирование WAN, просто нажмите **Далее.**

Если вы хотите настроить резервирование WAN, используйте «выпадающий список», чтобы выбрать один из других типов подключения. Соответствующие настройки появятся далее. Для подробной информации о настраиваемых параметрах, пожалуйста, обращайтесь к соответствующим разделам настоящего руководства.



Статический IP

Вы самостоятельно вводите фиксированный IP-адрес и другие IP-настройки (маска, шлюз, DNS). Все данные вы должны получить у провайдера.



IP-адрес	Введите IP-адрес.
Маска подсети	Введите маску подсети.
Шлюз по умолчанию	Введите IP-адрес шлюза по умолчанию.
Первичный DNS сервер	Введите первичный IP-адрес DNS.
Вторичный DNS сервер	Введите вторичный IP-адрес DNS.
Клонировать MAC-адрес	Доступно, если поле «Включить» активировано. Нажмите **Клонировать MAC-адрес** и маршрутизатор определит MAC-адрес вашего ПК автоматически. Результат будет отображен в поле **MAC-адрес**. Кроме того, если вы хотите сменить MAC-адрес для WAN-подключения, активируйте поле «Включить» и введите MAC-адрес самостоятельно.

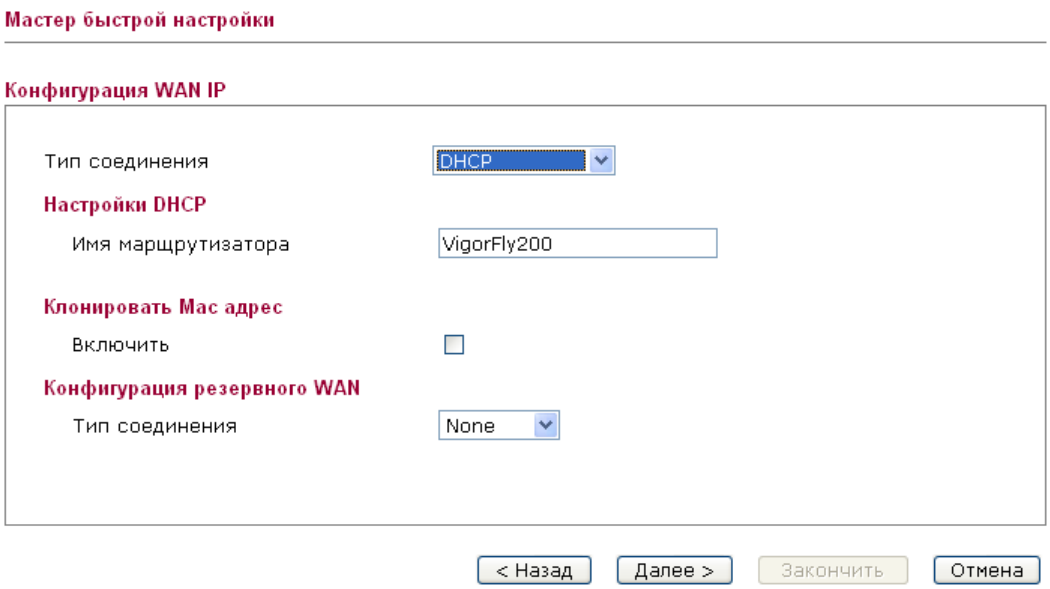
Включить Включить функцию клонирования MAC-адреса.

Конфигурация резервного WAN Если вы хотите настроить резервный WAN для каждого типа, пожалуйста, используйте выпадающий список для выбора режима подключения **4G/YOTA**.

После завершения настроек, нажмите **Далее**.

DHCP

Выберите этот тип, чтобы система автоматически получала IP-настройки от DHCP-сервера.



Настройки DHCP **Имя маршрутизатора –** по умолчанию VigorFly200.

Клонировать MAC-адрес Доступно, если поле «Включить» активировано. Нажмите **Клонировать MAC-адрес.** Маршрутизатор определит MAC-адрес автоматически. Результат будет отображен в поле **MAC-адрес**. Кроме того, если вы хотите сменить MAC-адрес для WAN-подключения, активируйте поле «Включить» и введите MAC-адрес самостоятельно.

Включить Маршрутизатор определит MAC-адрес автоматически.

Конфигурация резервного WAN

Если вы хотите настроить резервный WAN для каждого типа, пожалуйста, используйте выпадающий список для выбора режима подключения **4G/YOTA**.

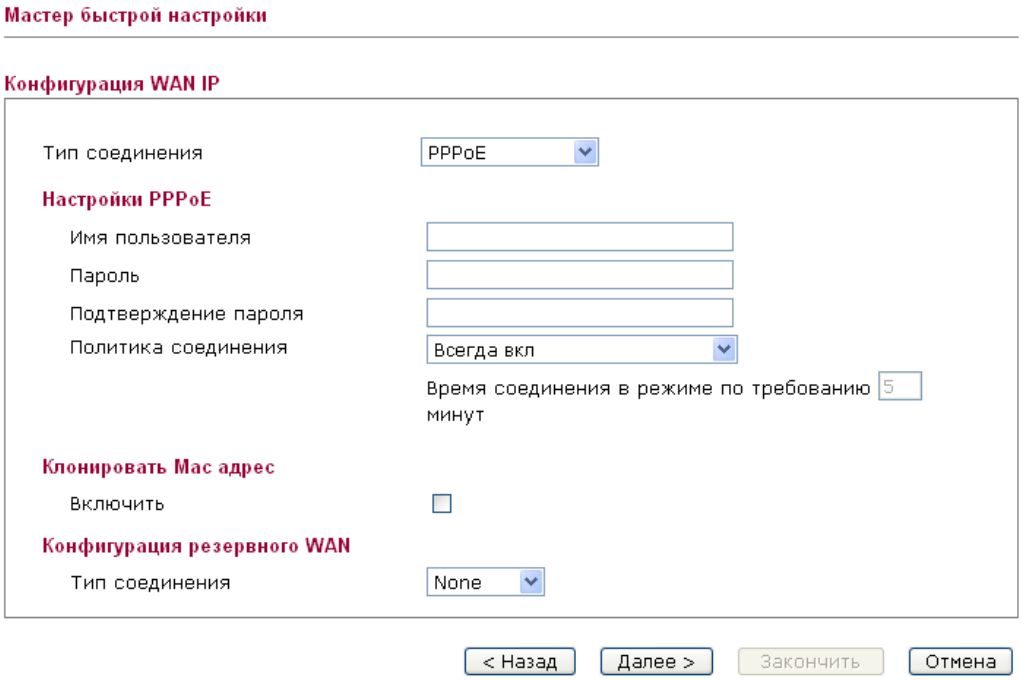
После завершения настроек, нажмите **Далее**.

PPPoE

PPPoE (от англ. **Point-to-Point Protocol over Ethernet)** это сетевой протокол передачи кадров PPP через Ethernet. С его помощью происходит подключение пользователей к Интернету посредством общего широкополосного канала, например, DSL-линии, беспроводного устройства или обычного модема. Все пользователи делят одно подключение.

PPPoE подключение часто используется xDSL-провайдерами. Локальные пользователи делят одно PPPoE подключение для доступа в Интернет. Ваш провайдер предоставит вам информацию об имени пользователя, пароле и идентификации.

Если ваш провайдер использует PPPoE подключение, выберите этот режим. Будет показана следующая страница:

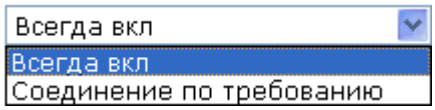


Имя Введите имя, предоставленное вашим провайдером.

Пароль Введите пароль, предоставленный вашим провайдером.

Подтверждение пароля Введите пароль повторно для подтверждения.

Политика соединения Вы можете выбрать опцию **Всегда вкл** чтобы сохранять подключение к Интернету всё время. В противном случае выберите **Соединение по требованию.**



Всегда вкл – маршрутизатор сохраняет подключение к Интернету всё время.

Соединение по требованию – маршрутизатор прервет подключение в случае длительного бездействия.

Время бездействия – установите время бездействия перед разрывом соединения. Время указывается в минутах.

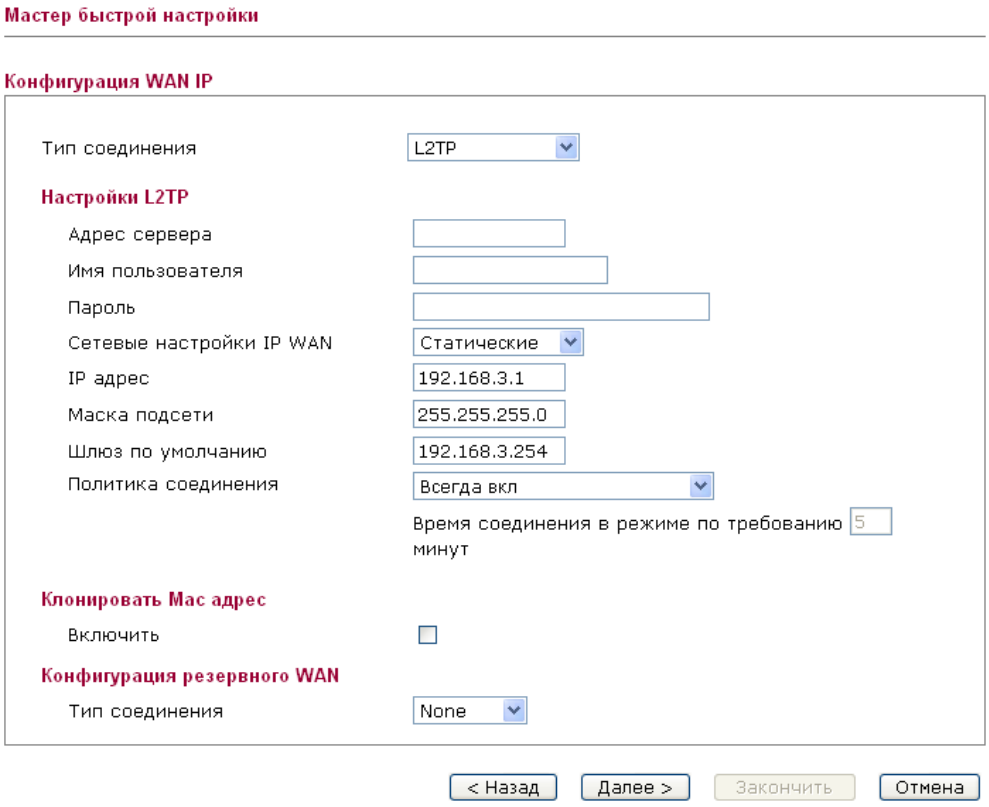
Клонировать MAC-адрес Доступно, если поле «Включить» активировано. Нажмите **Клонировать MAC-адрес.** Маршрутизатор определит MAC-адрес автоматически. Результат будет отображен в поле **MAC-адрес**. Кроме того, если вы хотите сменить MAC-адрес для WAN-подключения, активируйте поле «Включить» и введите MAC-адрес самостоятельно.

Конфигурация резервного WAN Если вы хотите настроить резервный WAN для каждого типа, пожалуйста, используйте выпадающий список для выбора режима подключения **4G/YOTA**.

После завершения настроек, нажмите **Далее**.

PPTP/L2TP

Если вы выбрали тип подключения PPTP или L2TP, введите имя пользователя, пароль и всю необходимую информацию, предоставленную вашим провайдером.



IP-адрес сервера L2TP/PPTP Введите IP-адрес сервера PPTP/L2TP.

Имя Введите имя, предоставленное провайдером.

Пароль Введите пароль, предоставленный провайдером.

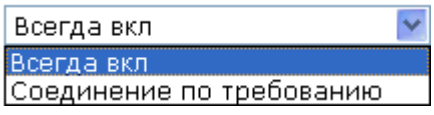
Сетевые настройки WAN IP Вы можете выбрать статический IP или DHCP.

IP-адрес Введите IP-адрес, если вы выбрали статический IP в качестве настройки WAN.

Маска подсети Введите маску подсети, если вы выбрали статический IP в качестве настройки WAN.

Шлюз по умолчанию Введите IP-адрес шлюза по умолчанию, если вы выбрали статический IP в качестве настройки WAN.

Политика соединения Вы можете выбрать опцию **Всегда вкл,** чтобы сохранять подключение к Интернету всё время. В противном случае выберите **Соединение по требованию.**



Всегда вкл – маршрутизатор сохраняет подключение к Интернету всё время.

Соединение по требованию – маршрутизатор

прервет подключение при длительном бездействии.

Время бездействия – установите время бездействия перед разрывом соединения. Время указывается в минутах.

Клонировать MAC-адрес

Доступно, если поле «Включить» активировано. Нажмите **Клонировать MAC-адрес.** Маршрутизатор определит MAC-адрес автоматически. Результат будет отображен в поле **MAC-адрес**.

Кроме того, если вы хотите сменить MAC-адрес для WAN-подключения, активируйте поле «Включить» и введите MAC-адрес самостоятельно.

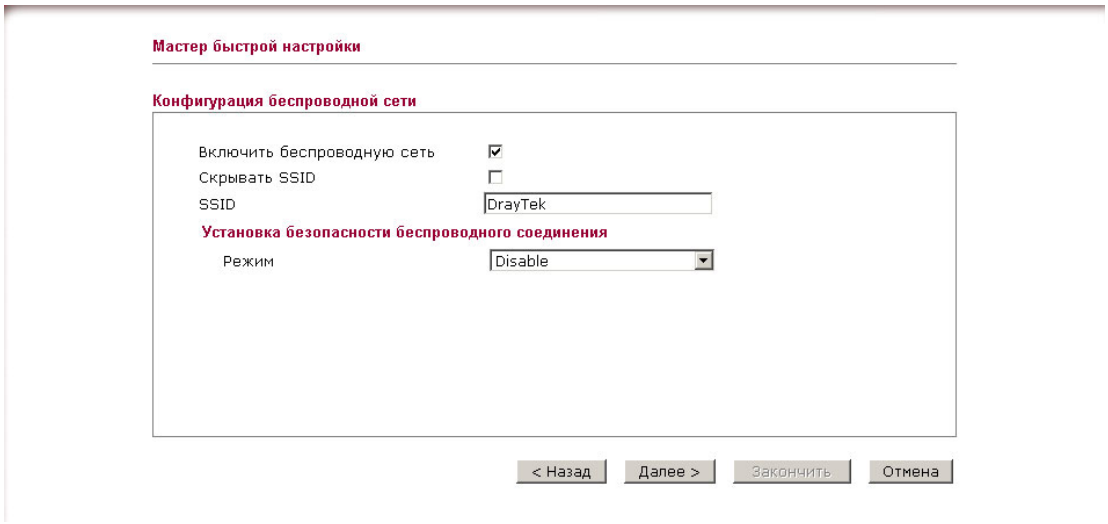
Конфигурация резервного WAN

Если вы хотите настроить резервный WAN для каждого типа, пожалуйста, используйте выпадающий список для выбора режима подключения **4G/YOTA**.

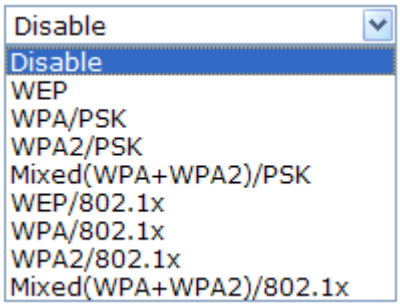
После завершения настроек, нажмите **Далее**.

2.4.4 Настройки беспроводного соединения

Теперь вам необходимо настроить беспроводное соединение.



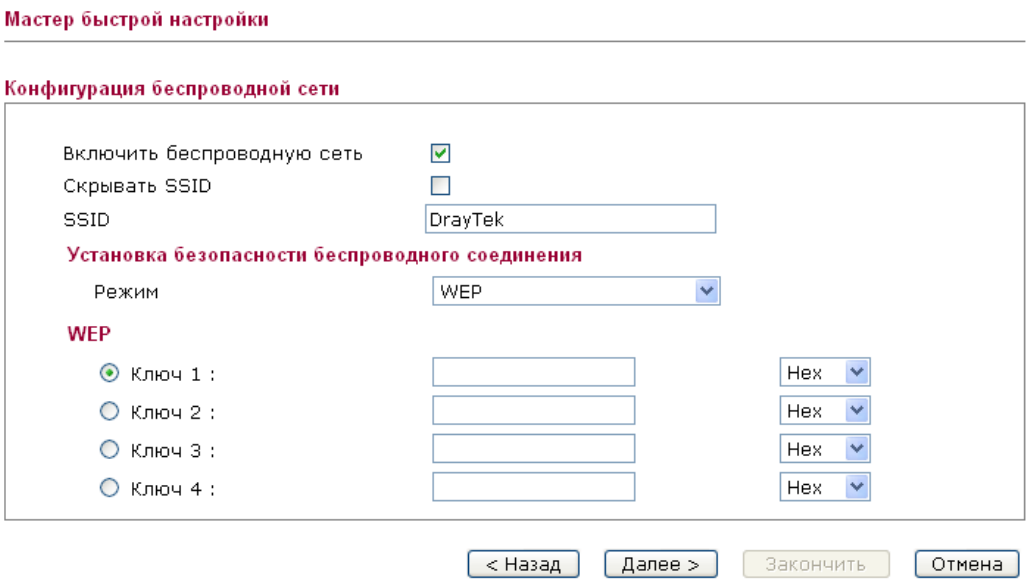
Включить беспроводную сеть	Галочка – если вы хотите активировать беспроводную сеть.
Скрывать SSID	Галочка – если вы хотите активировать эту опцию, чтобы избежать посторонних подключений неизвестных пользователей к вашей сети.
SSID	Идентификатор беспроводной сети (SSID) может быть любым набором букв и знаков. По умолчанию введено слово "DrayTek". Мы рекомендуем вам придумать свое.
Режим	Выберите необходимый режим безопасности для работы беспроводной сети.



Каждый из режимов выведет вас на новую страницу, где вам будет нужно произвести необходимые настройки.

WEP

Если вы выбрали WEP конфигурацию, вам необходимо определить ключ шифрования (Ключ 1 ~ Ключ 4) и режим идентификации (открытый или разделенный). Все беспроводные устройства должны поддерживать один и тот же бит-размер WEP шифрования и иметь одинаковый ключ.

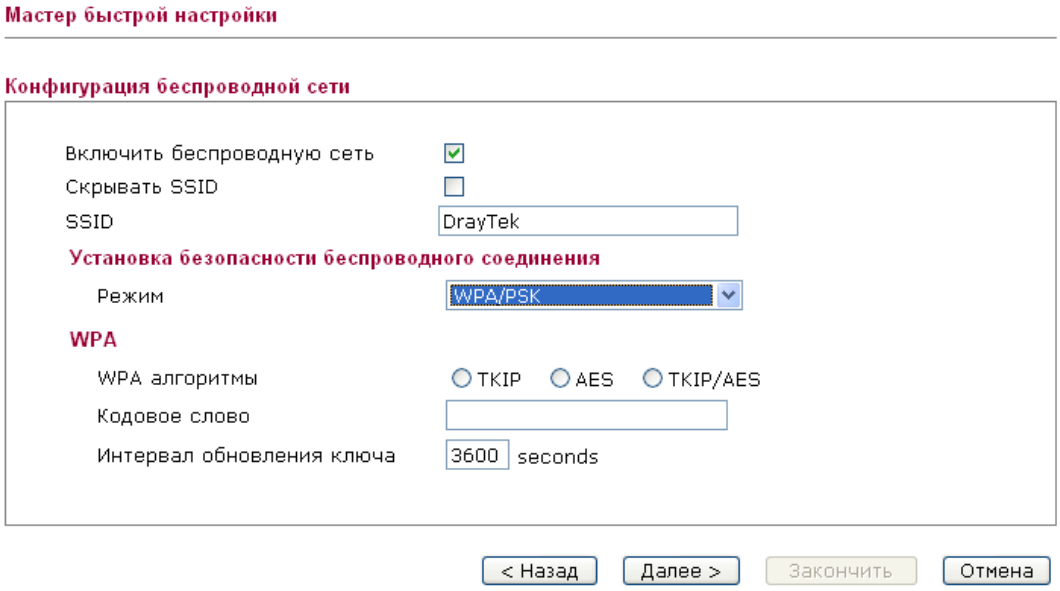


Ключ 1 ~ Ключ 4

Можно ввести четыре ключа, но использован будет только один, выбранный пользователем. Формат WEP-ключа ограничивается 5 символами ASCII или 10 шестнадцатеричными значениями 64-битного шифрования; или 13 символами ASCII или 26 шестнадцатеричными значениями 128-битного шифрования. Разрешены символы ASCII с 33(!) до 126(~) кроме '#' и ','.

WPA/PSK или WPA2/PSK или Смешанное шифрование (WPA+WPA2)/PSK

Принимает только WPA-клиентов; ключ шифрования должен быть введен с заранее заданными ключами. WPA кодирует каждый переданный пакет, используя ключи, которые вводятся в соответствующее поле или автоматически передаются посредством 802.1x авторизации.



WPA алгоритмы — Выберите WPA алгоритм: TKIP, AES или TKIP/AES.

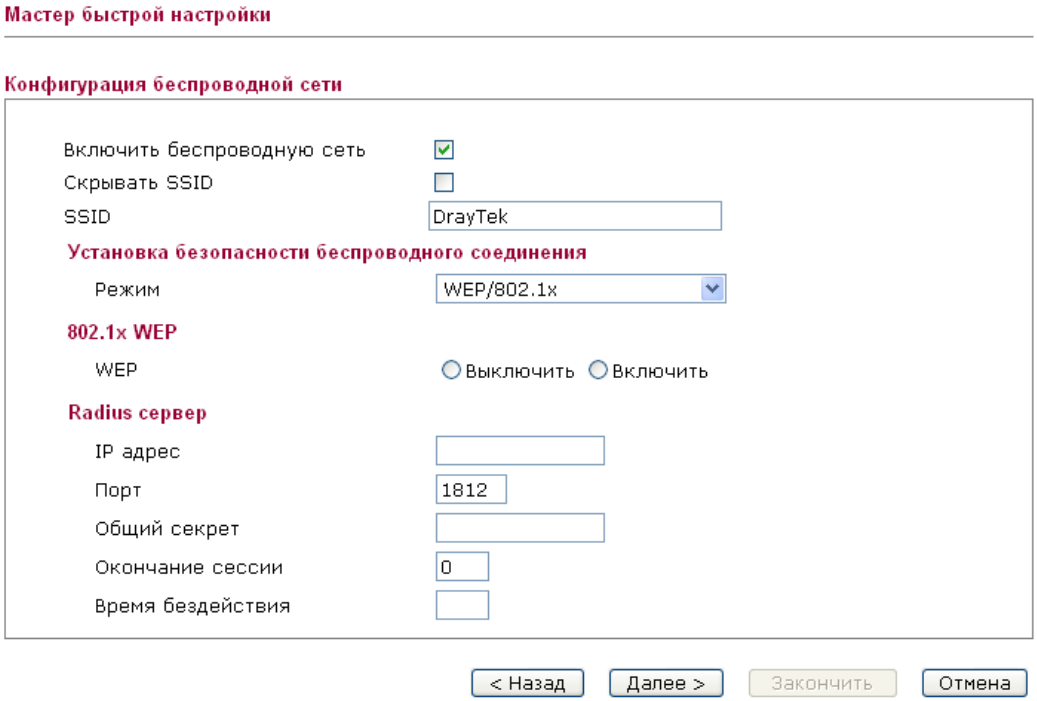
Кодовое слово — 8~63 ASCII символы, такие как 012345678..(или 64 шестнадцатеричных знака, начинающиеся с 0x, такие как "0x321253abcde...").

Интервал обновления ключа — WPA использует ключи авторизации сети. Тем не менее, нормальные сетевые операции используют различные ключи шифрования, которые генерируются произвольно. Введите в этом поле временной интервал смены ключей (в секундах). Меньший интервал увеличит безопасность, но снизит мощность. По умолчанию установлен интервал в 3600 секунд. Установите 0 для отключения генерации ключей.

WEP/802.1x

RADIUS (Remote Authentication Dial-In User Service) – это протокол службы, обеспечивающей аутентификацию, идентификацию и сбор сведений об использованных ресурсах.

Встроенная функция RADIUS-клиента позволяет маршрутизатору обеспечивать беспроводного клиента и RADIUS-сервер выполнением взаимной идентификации. Данная функция активирует централизованный удаленный доступ с идентификацией для сетевого управления. Если вы выбираете WPA-RADIUS в качестве режима работы безопасности, вам необходимо настроить режим WPA, алгоритм, RADIUS-сервер, порт RADIUS-сервера и секрет RADIUS-сервера.



WEP

Выключить – Выключить WEP шифрование. Информация, отсылаемая в точку доступа, не будет кодироваться.

Включить – Включить WEP шифрование.

IP-адрес

Введите IP-адрес RADIUS-сервера.

Порт

Номер UDP-порта, используемого RADIUS-сервером. По умолчанию установлен 1812 в соответствии с RFC 2138.

Общий секрет

RADIUS-сервер и клиент имеют общий секрет, который используется для идентификации сообщений между ними. Обе стороны должны быть настроены для использования одного и того же общего секрета.

Окончание сессии

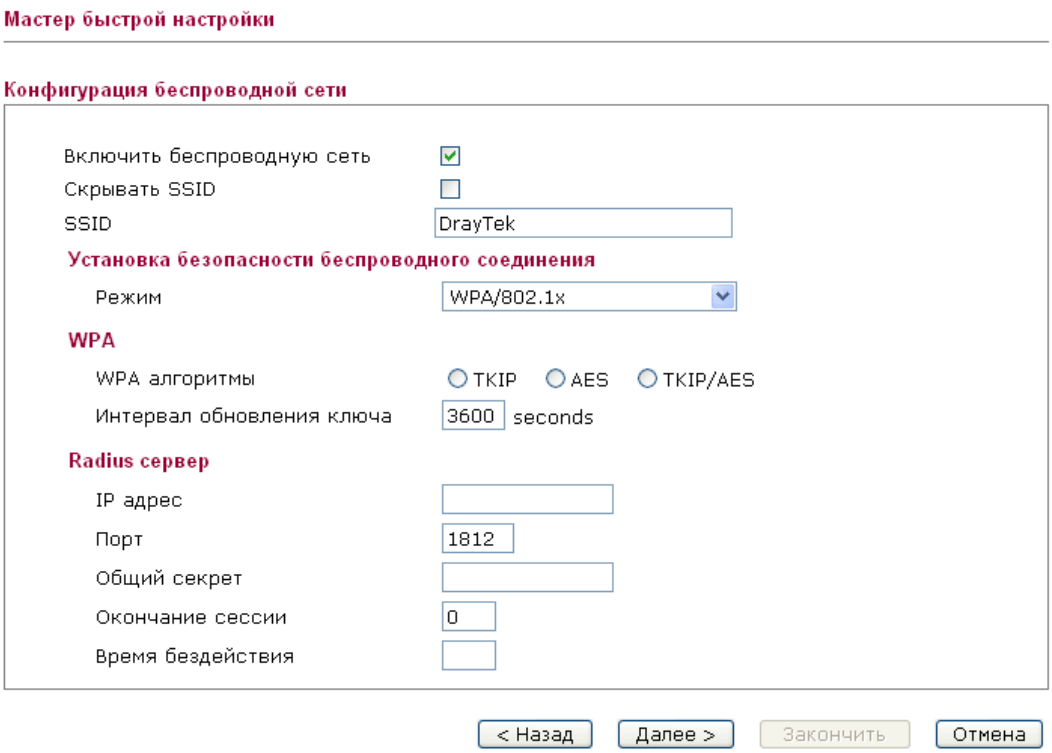
Установите временной максимум предоставления услуг перед реидентификацией. Впишите ноль, чтобы установить немедленную идентификацию сразу же после окончания сессии (указывайте время в секундах).

Время бездействия

Время бездействия – установите время бездействия перед разрывом соединения.

WPA/802.1x

WPA кодирует каждый переданный пакет, используя заранее заданные ключи (PSK), которые вводятся в соответствующее поле или автоматически передаются посредством 802.1x авторизации.



WPA алгоритмы — Выберите WPA алгоритм: TKIP, AES или TKIP/AES.

Интервал обновления ключа — WPA использует ключи авторизации сети. Тем не мене, обычные сетевые операции используют различные ключи шифрования, которые генерируются произвольно. Введите в этом поле временной интервал смены ключей (в секундах). Меньший интервал увеличит безопасность, но снизит производительность. По умолчанию установлен интервал в 3600 секунд. Установите 0 для отключения генерации ключей.

IP-адрес — Введите IP-адрес RADIUS-сервера.

Порт — Номер UDP-порта, используемого RADIUS-сервером. По умолчанию установлен 1812 на основе RFC 2138.

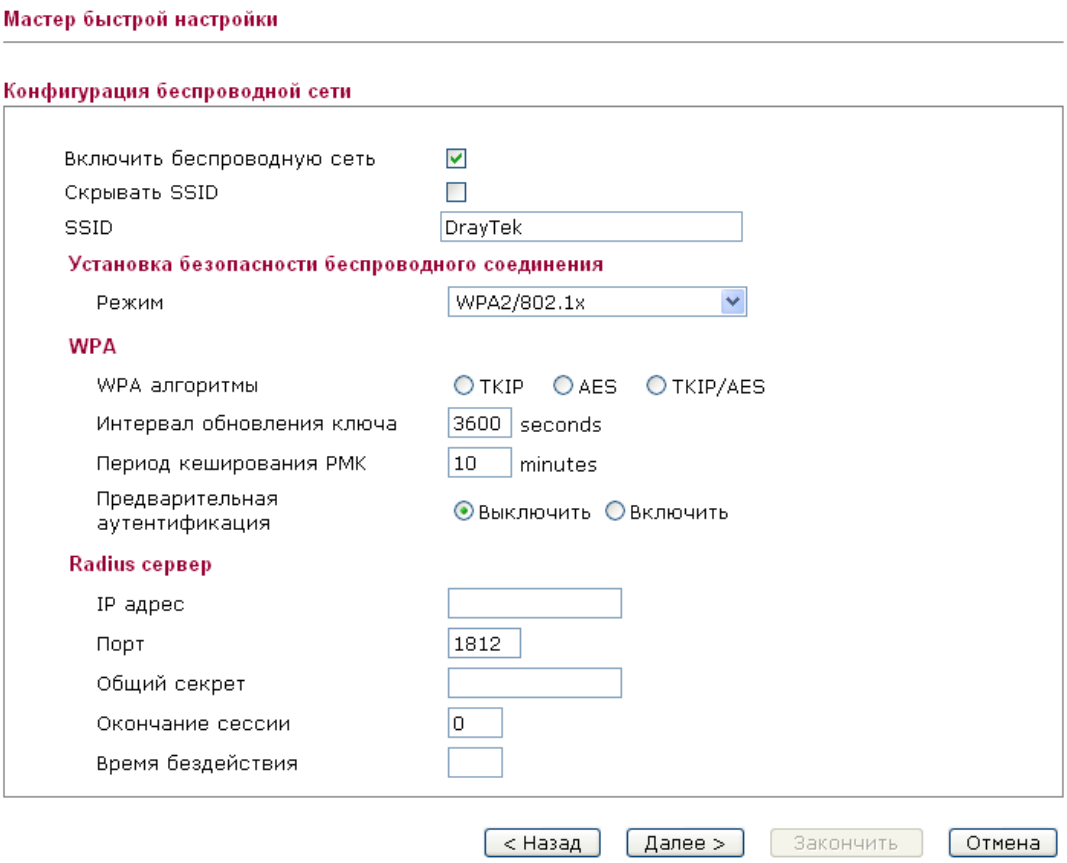
Общий секрет — RADIUS-сервер и клиент имеют общий секрет, который используется для идентификации сообщений между ними. Обе стороны должны быть настроены для использования одного и того же общего секрета.

Окончание сессии — Установите временной максимум предоставления услуг перед реидентификацией. Впишите ноль, чтобы установить немедленную идентификацию сразу же после окончания сессии (указывайте время в секундах).

Время бездействия — **Время бездействия –** установите время бездействия перед разрывом соединения.

WPA2/802.1x

WPA кодирует каждый переданный пакет, используя заранее заданные ключи (PSK), которые вводятся в соответствующее поле или автоматически передаются посредством 802.1x авторизации.



WPA алгоритмы Выберите WPA алгоритм: TKIP, AES или TKIP/AES.

Интервал обновления ключа WPA использует ключи авторизации сети. Тем не менее, нормальные сетевые операции используют различные ключи шифрования, которые генерируются произвольно. Введите в этом поле временной интервал смены ключей (в секундах). Меньший интервал увеличит безопасность, но снизит мощность. По умолчанию установлен интервал в 3600 секунд. Установите 0 для отключения генерации ключей.

PMK Cache Period Установите период хранения WPA2 PMK (парные ключи). PMK Cache управляет списком BSSID и ассоциированными SSID, с которыми устройство идентифицировалось ранее.

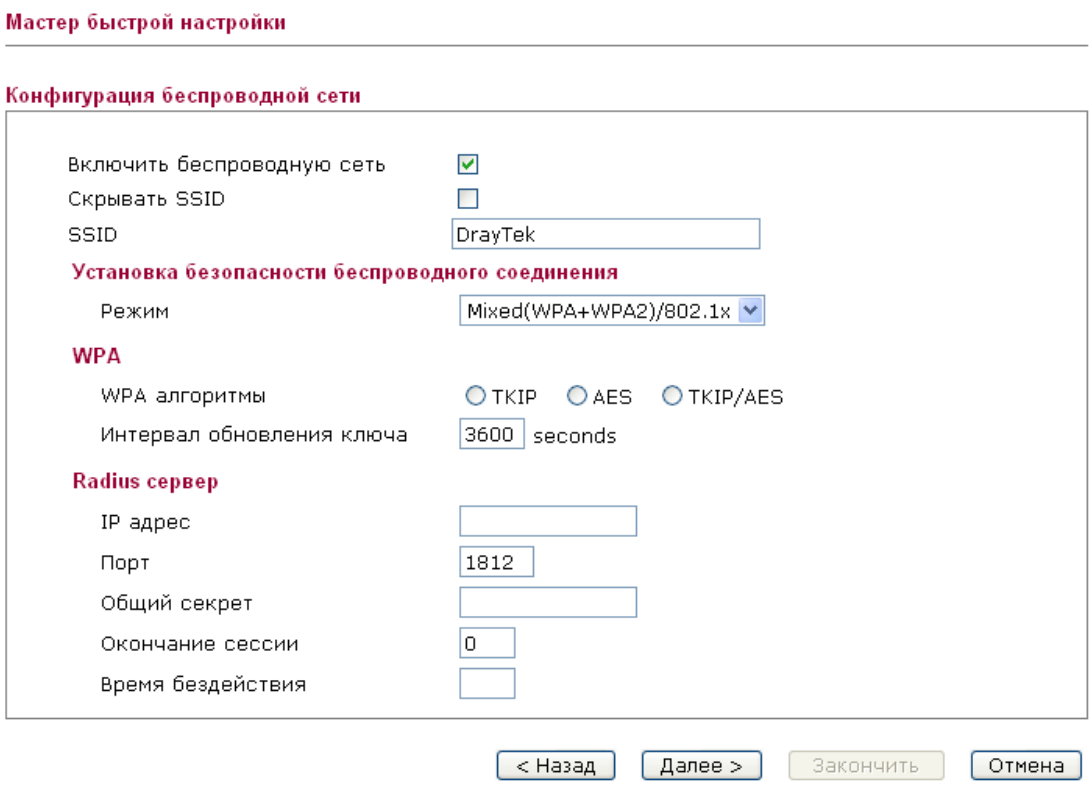
Предварительная аутентификация Активирует передатчик для идентификации и более безопасного и быстрого переключения между точками доступа. С процедурой предварительной аутентификации, определенной спецификацией IEEE 802.11i, предварительное четырехстороннее рукопожатие может уменьшить задержку передачи, воспринимаемую мобильной точкой. Это сделает переключение более безопасным и быстрым (доступно только в WPA2).

Включить – Включить предварительную

	аутентификацию IEEE 802.1X. **Выключить –** Выключить предварительную аутентификацию IEEE 802.1X.
IP-адрес	Введите IP-адрес RADIUS-сервера.
Порт	Номер UDP-порта, используемого RADIUS-сервером. По умолчанию установлен 1812 в соответствие с требованиями RFC-2138.
Общий секрет	RADIUS-сервер и клиент имеют общий секрет, который используется для идентификации сообщений между ними. Обе стороны должны быть настроены для использования одного и того же общего секрета.
Окончание сессии	Установите временной максимум предоставления услуг перед реидентификацией. Впишите ноль, чтобы установить немедленную идентификацию сразу же после окончания сессии (указывайте время в секундах).
Время бездействия	**Время бездействия –** установите время бездействия перед разрывом соединения.

Смешанное шифрование (WPA+WPA2)/802.1x

WPA кодирует каждый переданный пакет, используя заранее заданные ключи (PSK), которые вводятся в соответствующее поле или автоматически передаются посредством 802.1x авторизации.



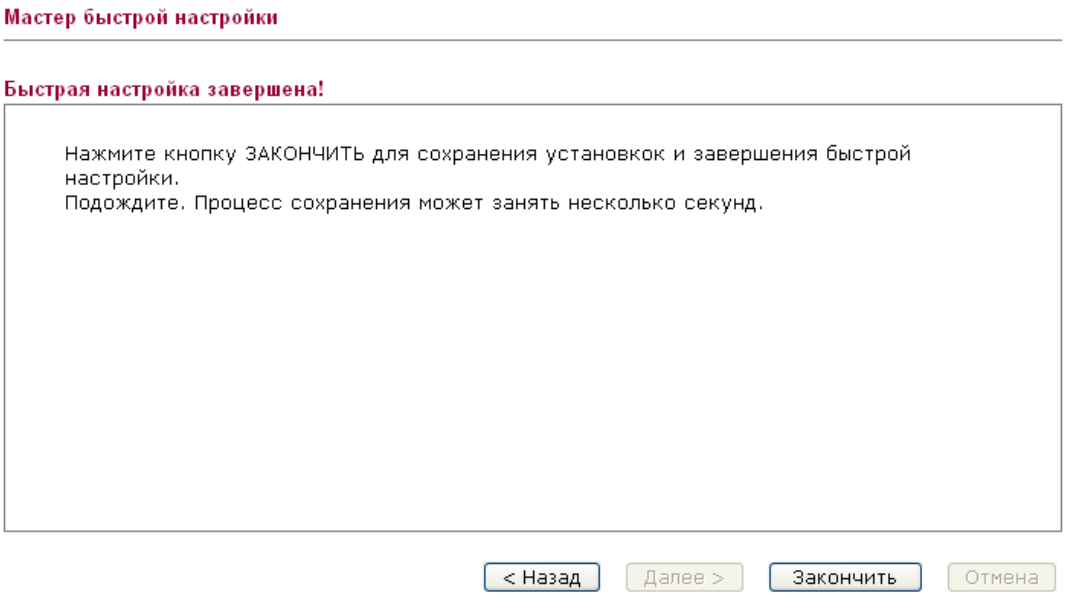
WPA алгоритмы	Выберите WPA алгоритм: TKIP, AES или TKIP/AES.
Интервал обновления ключа	WPA использует ключи авторизации сети. Тем не менее, нормальные сетевые операции используют различные ключи шифрования, которые генерируются произвольно. Введите в этом поле временной интервал смены ключей (в секундах). Меньший интервал

	увеличит безопасность, но снизит мощность. По умолчанию установлен интервал в 3600 секунд. Установите 0 для отключения генерации ключей.
IP-адрес	Введите IP-адрес RADIUS-сервера.
Порт	Номер UDP-порта, используемого RADIUS-сервером. По умолчанию установлен 1812 в соответствие с требованиями RFC 2138.
Общий секрет	RADIUS-сервер и клиент имеют общий секрет, который используется для идентификации сообщений между ними. Обе стороны должны быть настроены для использования одного и того же общего секрета.
Окончание сессии	Установите временной максимум предоставления услуг перед реидентификацией. Впишите ноль, чтобы установить немедленную идентификацию сразу же после окончания сессии (указывайте время в секундах).
Время бездействия	**Время бездействия –** установите время бездействия перед разрывом соединения.

После завершения настроек, нажмите **Далее.**

2.4.5 Сохранение настроек Мастера

Теперь вы увидите следующее окно.

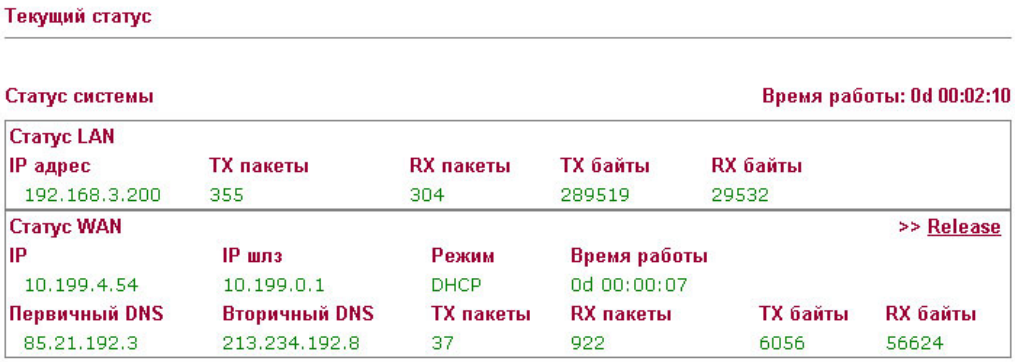


Это означает, что процедура быстрой настройки завершена. Различные типы режимов подключения будут иметь различный текст. Нажмите Закончить и перезагрузите маршрутизатор.

2.5 Текущий статус

На странице Текущий статус отображается статус системы, статус WAN-подключения и другие данные, связанные с маршрутизатором. Если вы выбрали в качестве протокола PPPoE, на странице вы найдете кнопки управления Dial (Подключить) к PPPoE или Drop (Прервать) соединение с PPPoE.

Текущий статус DHCP



Подробное объяснение:

Статус LAN

IP адрес Показывает IP-адрес на LAN-интерфейсе.

TX пакеты Показывает общее число переданных пакетов на LAN-интерфейсе.

RX пакеты Показывает общее число принятых пакетов на LAN-интерфейсе.

Статус WAN

IP Показывает IP-адрес на WAN-интерфейсе.

IP шлз Показывает IP-адрес шлюза по умолчанию.

Режим Показывает тип WAN-подключения (напр. PPPoE).

Время работы Показывает время работы.

Первичный DNS Показывает настройки первичного DNS.

Вторичный DNS Показывает настройки вторичного DNS.

TX пакеты Показывает общее число переданных пакетов на WAN-интерфейсе.

TX байты Показывает скорость передачи в байт/с на WAN-интерфейсе.

RX пакеты Показывает общее число принятых пакетов на WAN-интерфейсе.

RX байты Показывает скорость приема в байт/с на WAN-интерфейсе.

Renew Повторно запросить по DHCP IP-настройки для WAN.

Release Сбросить полученные по DHCP IP-настройки для WAN.

Примечание: Слова, высвеченные зеленым, означают, что WAN-подключение готово к доступу в Интернет; красный цвет означает, что WAN-подключение к доступу в Интернет не готово.

2.6 Сохранение настроек

Каждый раз, когда вы нажимаете **ОК** для сохранения настроек, вы можете видеть в левом нижнем углу системные сообщения, показывающие реакцию системы на ваши действия и режим работы.

Режим пользователя – означает, что доступ к системе осуществляется в режиме пользователя.

Режим администратора – означает, что доступ к системе осуществляется в режиме администратора.

Система готова – показывает, что система готова для изменения настроек.

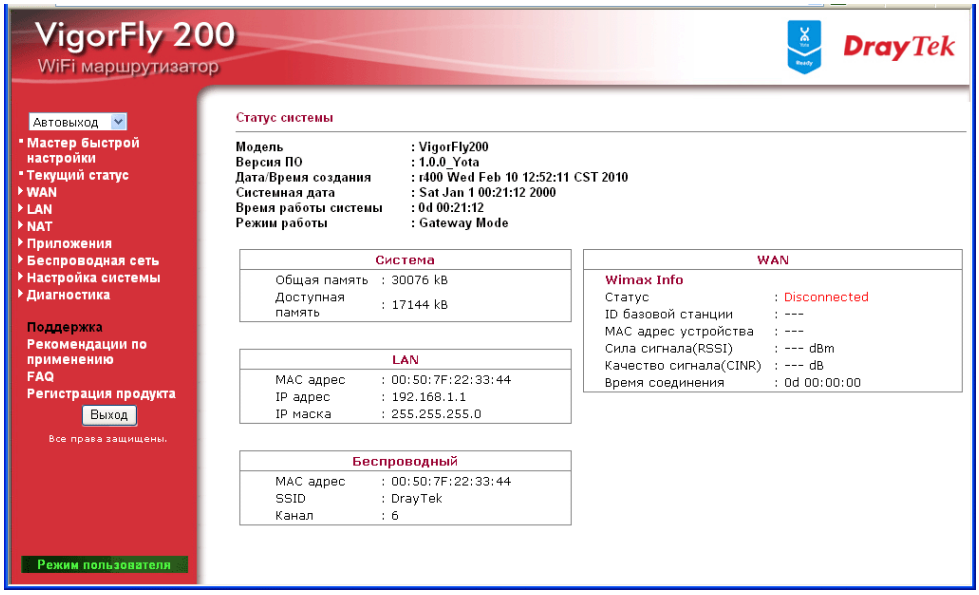
Настройки сохранены – означает, что настройки сохранены, поскольку вы нажали **Готово** или **ОК**.

3 Операции в режиме пользователя

Эта глава поможет пользователям изменить простейшие настройки маршрутизатора в режиме пользователя.

1. Откройте браузер на вашем компьютере и наберите адрес **http://192.168.1.1.** В следующем окне вас попросят ввести имя пользователя и пароль.
2. Для доступа к базовым настройкам (режим пользователя) ничего не вводите и нажмите **Войти**.

Появится следующее окно. В левом нижнем углу будет написано **Режим пользователя**.



3.1 WAN

Мастер быстрой настройки позволяет быстро настроить маршрутизатор для подключения.

Немного об IP-сетях

IP означает Internet Protocol (Интернет-протокол).

Каждое устройство – в том числе маршрутизаторы, принт-серверы, компьютеры – должно иметь свой уникальный IP-адрес для своей идентификации в сети. Чтобы избежать адресных противоречий, все IP-адреса публично зарегистрированы в Сетевом Информационном Центре (NIC). Уникальные IP-адреса обязательны для всех устройств, представленных в публичных сетях. Но в связи с тем что, количество публичных адресов ограничено, в частных TCP/IP локальных сетях (LAN) могут использоваться неуникальные адреса. Например, для связи компьютера и маршрутизатора. NIC зарезервировал определенные диапазоны адресов, которые никогда не будут публичными. И именно такие адреса рекомендуется использовать в локальных сетях. Следующие диапазоны IP-адресов не являются публичными:

10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

Совместное использование публичных и частных IP-адресов

Чаще всего маршрутизатор объединяет группы компьютеров и его главная задача – управлять локальной сетью и защищать ее. Каждому из компьютеров назначен частный IP-адрес, выданный DHCP-сервером маршрутизатора. Для связи с компьютерами в локальной сети сам маршрутизатор также использует частный IP, например, 192.168.1.1. В то же время маршрутизатор связан с другими сетевыми устройствами через Интернет, при этом он должен иметь публичный IP. Для работы в такой схеме применяют механизм, называемый Трансляция сетевых адресов (Network Address Translation – NAT). При этом маршрутизатор будет транслировать публичный адрес в частный, а также передавать пакеты информации с компьютеров из локальной сети в Интернет и обратно. Таким образом, все компьютеры в локальной сети могут делить общее Интернет-подключение через один публичный IP-адрес.

Получение публичного IP от провайдера

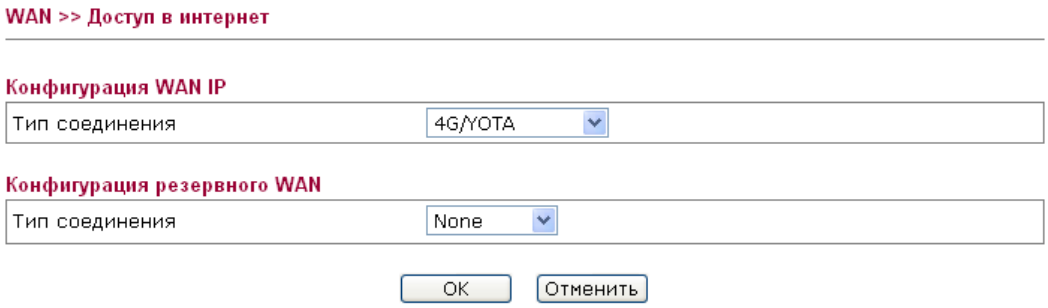
При ADSL-подключении PPP-аутентификации и авторизации используется для связывания оборудования, расположенного в помещении клиента (customer premises equipment – CPE). PPPoE подключает сеть через устройство доступа (DSLAM) к одному или нескольким концентраторам через удаленный доступ. Реализация этой возможности значительно облегчает использование Интернета. В то же время она обеспечивает контроль доступа, биллинг и типы сервиса в соответствии с пожеланиями пользователя.

Когда маршрутизатор начнет подключаться к Интернет-провайдеру, последовательность поисковых действий отправит запрос о подключении. Будет создана новая сессия. Ваш пользовательский ID и пароль пройдут аутентификацию с помощью протоколов **PAP** или **CHAP** с системой **RADIUS.** А ваш IP-адрес, DNS-сервер и пр. будут назначены автоматически.

Ниже показано меню WAN.

3.1.1 Доступ в Интернет

Эта страница поможет вам настроить конфигурацию WAN для работы в различных режимах. Выберите в выпадающем списке **Тип соединения** необходимый вам режим работы WAN.



4G/YOTA

Для активации функции WIMAX выберите соответствующий тип подключения.

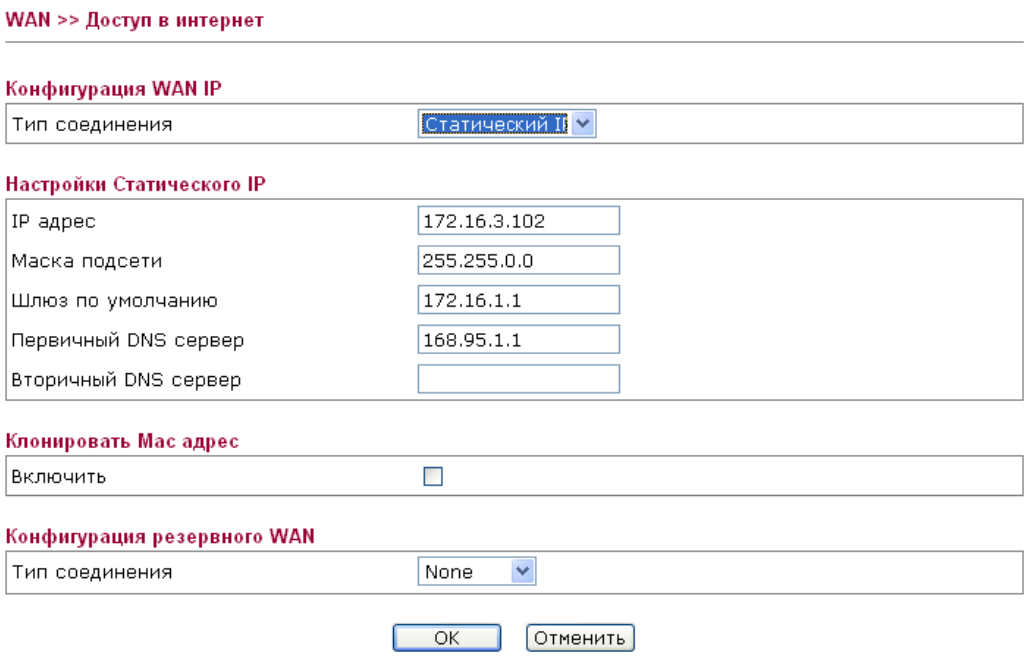
Конфигурация резервного WAN

Если вы хотите настроить резервный WAN для каждого типа, пожалуйста, используйте выпадающий список для выбора одного из режимов подключения. В зависимости от вашего выбора появятся соответствующие настройки. Детальную информацию о соответствующих настройках параметров вы найдете в соответствующих секциях ниже.

Для установки 4G-подключения не требуется никаких дополнительных настроек. Если вы не хотите настраивать WAN-резервирование, просто нажмите **Далее.**

Статический IP

Чтобы выбрать режим статического IP для доступа в Интернет, выберите **Статический IP** в списке типов подключения. Появится следующая страница.



IP-адрес Введите IP-адрес.

Маска подсети Введите маску подсети.

Шлюз по умолчанию Введите IP-адрес шлюза по умолчанию.

Первичный DNS сервер Вам необходимо назначить IP-адрес DNS-сервера. Провайдеры предлагают, как правило, сразу несколько DNS-серверов. Если ваш провайдер не предоставляет их, маршрутизатор назначит IP DNS-сервера по умолчанию –

198.95.1.1

Вторичный DNS сервер Вы можете выбрать второй IP-адрес DNS-сервера, т.к. провайдеры предлагают, как правило, сразу несколько DNS-серверов. Если ваш провайдер не предоставляет их, маршрутизатор назначит вторичный IP DNS-сервера по умолчанию.

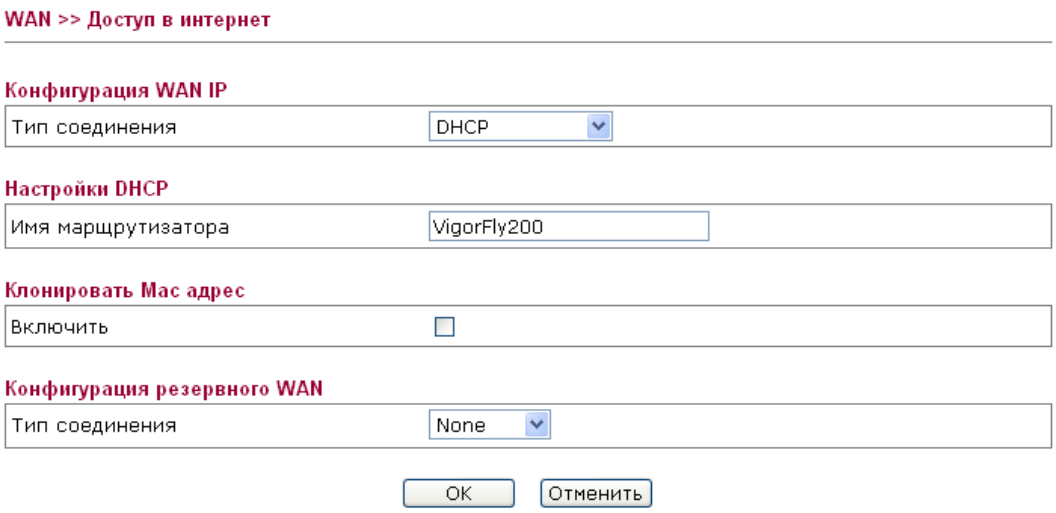
Клонировать MAC-адрес Доступно, если поле «Включить» активировано. Нажмите **Клонировать MAC-адрес.** Маршрутизатор определит MAC-адрес автоматически. Результат будет отображен в поле **MAC-адрес**.

Конфигурация резервного WAN Если вы хотите настроить резервный WAN для каждого типа, пожалуйста, используйте выпадающий список для выбора режима подключения **4G/YOTA**.

После завершения настроек, нажмите **ОК** для сохранения.

DHCP

Режим DHCP позволяет пользователю получить IP-настройки для маршрутизатора автоматически от DHCP-сервера. Т.е. если вы выбираете режим **DHCP**, DHCP-сервер вашего провайдера назначит IP-настройки для вашего маршрутизатора автоматически. Вам не нужно самостоятельно устанавливать никаких IP-настроек.



Имя маршрутизатора Введите имя маршрутизатора. По умолчанию VigorFly 200.

Клонировать MAC-адрес Доступно, если поле «Включить» активировано. Нажмите **Клонировать MAC-адрес.** Маршрутизатор определит

MAC-адрес автоматически. Результат будет отображен в поле **MAC-адрес**.

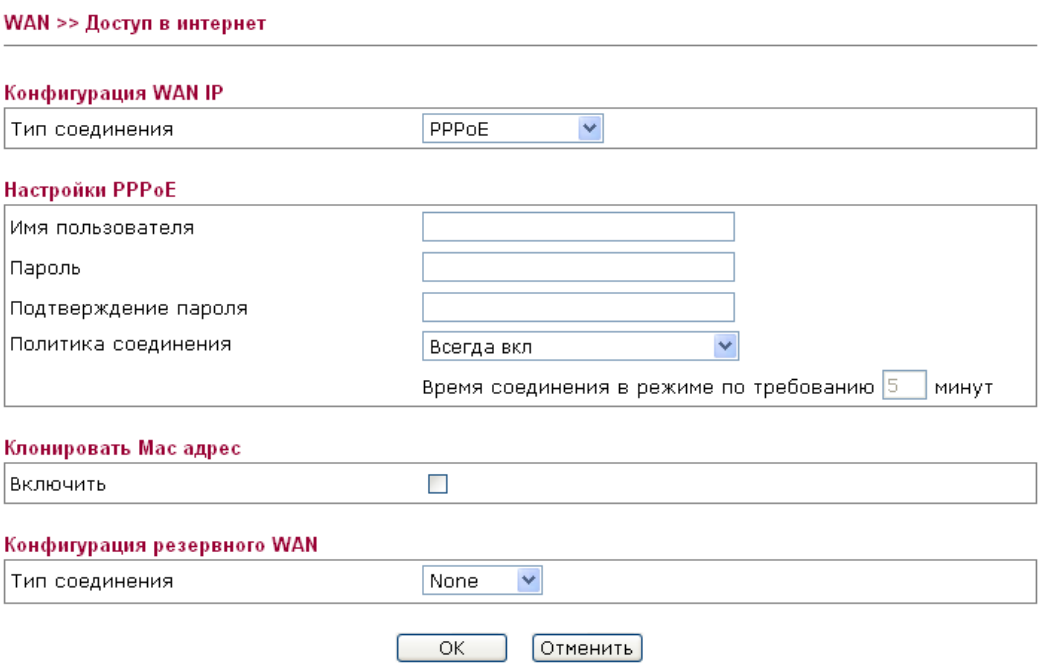
Конфигурация резервного WAN

Если вы хотите настроить резервный WAN для каждого типа, пожалуйста, используйте выпадающий список для выбора режима подключения **4G/YOTA**.

После завершения настроек, нажмите **ОК** для сохранения.

PPPoE

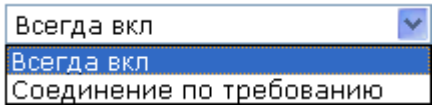
Для выбора подключения по PPPoE, пожалуйста, выберите PPPoE в меню **Доступ в Интернет.** Будет отображена следующая страница:



Имя Введите имя, предоставленное вашим провайдером.

Пароль Введите пароль, предоставленный вашим провайдером.

Политика соединения Вы можете выбрать опцию **Всегда вкл** чтобы сохранять подключение к Интернету всё время. В противном случае выберите **Соединение по требованию.**



Время бездействия – установите время бездействия перед разрывом соединения. Впишите число, если вы выбрали

Соединение по требованию.

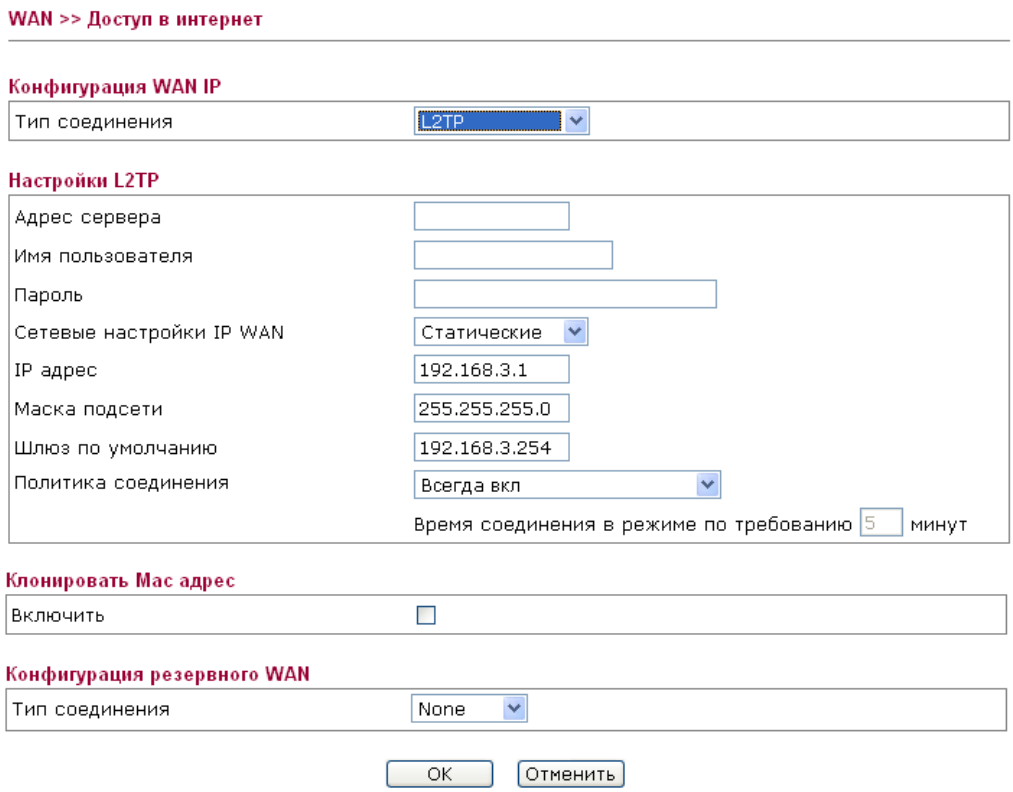
Клонировать MAC-адрес Доступно, если поле «Включить» активировано. Нажмите **Клонировать MAC-адрес.** Маршрутизатор определит MAC-адрес автоматически. Результат будет отображен в поле **MAC-адрес**.

Конфигурация резервного WAN Если вы хотите настроить резервный WAN для каждого типа, пожалуйста, используйте выпадающий список для выбора режима подключения **4G/YOTA**.

После завершения настроек, нажмите **ОК** для сохранения.

PPTP/L2TP

Для выбора протокола **PPTP/L2TP**, пожалуйста, выберите **PPTP/L2TP** в меню **Тип Подключения.** Будет показана следующая страница:



IP-адрес сервера Введите IP-адрес сервера PPTP/L2TP

Имя Введите имя, предоставленное провайдером

Пароль Введите пароль, предоставленный провайдером

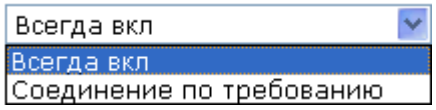
Сетевые настройки IP WAN Вы можете выбрать **Статический IP** или **DHCP** для IP настроек WAN

IP-адрес Введите IP-адрес

Маска подсети Введите маску подсети

Шлюз по умолчанию Введите адрес шлюза для этого маршрутизатора.

Политика соединения Вы можете выбрать опцию **Всегда вкл** чтобы сохранять подключение к Интернету всё время. В противном случае выберите **Соединение по требованию.**



Время бездействия – установите время бездействия перед разрывом соединения. Впишите число, если вы выбрали **Соединение по требованию.**

Клонировать MAC-адрес Доступно, если поле «Включить» активировано. Нажмите **Клонировать MAC-адрес.** Маршрутизатор определит MAC-адрес автоматически. Результат будет отображен в поле **MAC-адрес**.

Конфигурация резервного WAN

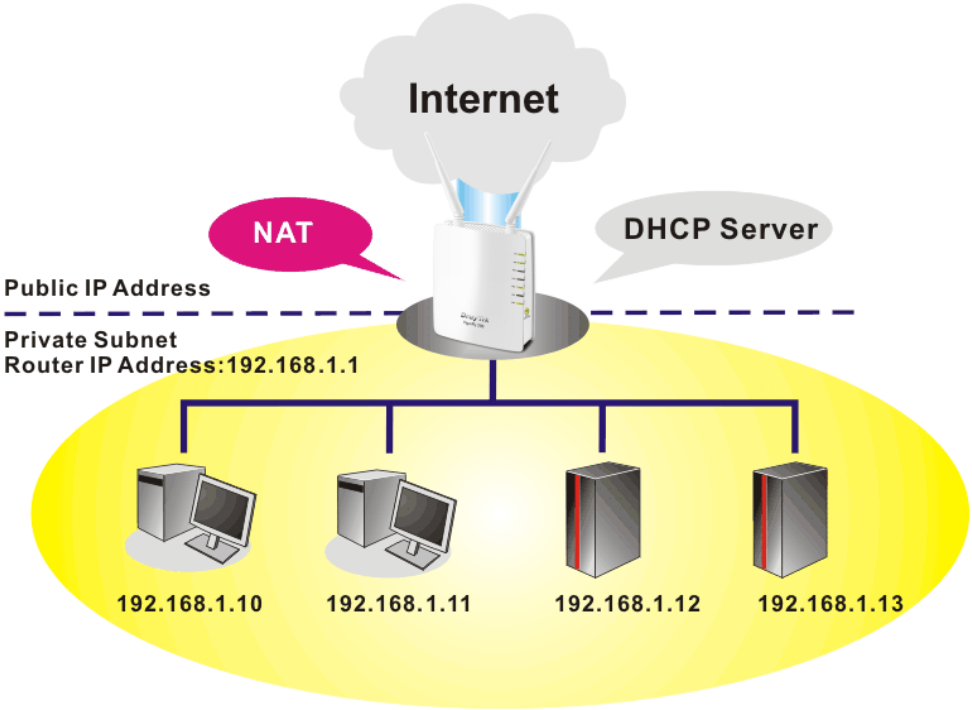
Если вы хотите настроить резервный WAN для каждого типа, пожалуйста, используйте выпадающий список для выбора режима подключения **4G/YOTA**.

После завершения настроек, нажмите **OK** для сохранения.

3.2 LAN

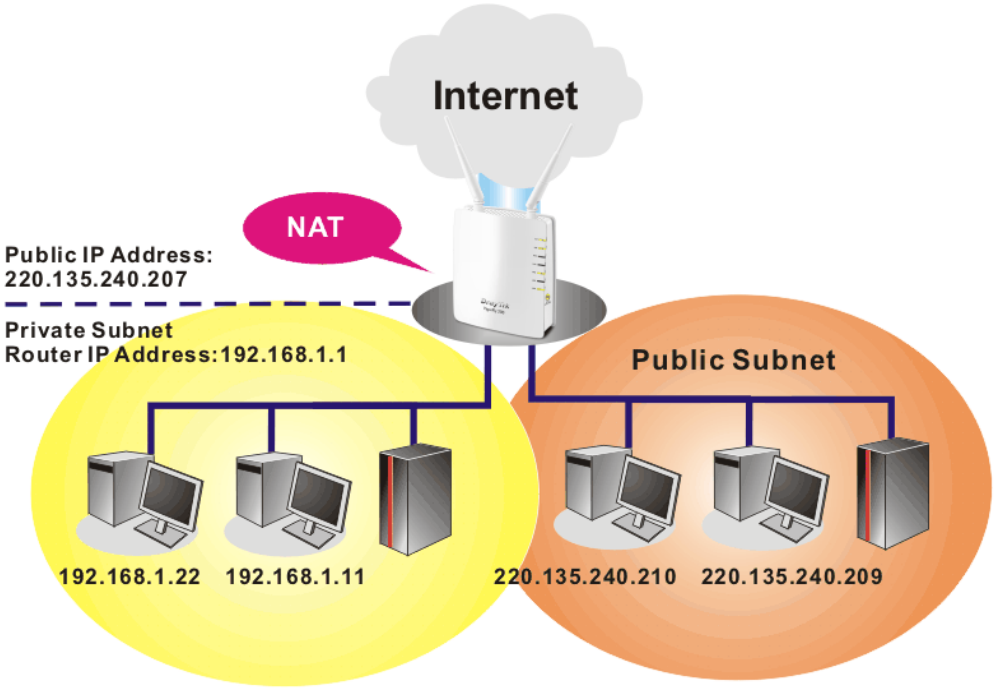
Основы LAN

Маршрутизатор VigorFly работает в режиме трансляции сетевых адресов (NAT). При этом создается ваша собственная частная сеть. Как уже было сказано, маршрутизатор использует публичные IP-адреса для связи с Интернетом и частные IP для локальных устройств. Функция NAT транслирует пакеты информации из публичных IP в частные и обратно, отправляя пакеты к нужным хостам. Кроме того, маршрутизатор имеет встроенный DHCP-сервер, который назначает частные IP-адреса для всех локальных устройств. Следующая диаграмма показывает принцип работы маршрутизатора.



В некоторых случаях, у вас может быть публичный IP-адрес подсети от вашего провайдера вида 220.135.240.0/24. Это значит, что вы можете установить публичную подсеть или обратиться ко второй подсети, где каждый хост будет иметь публичный IP-адрес. Как часть публичной подсети, маршрутизатор Vigor будет служить для маршрутизации, чтобы обеспечить хостам в публичной подсети передачу информации к

другим публичным хостам или внешним серверам. Поэтому маршрутизатор должен быть установлен как шлюз для публичных хостов.



Что такое протокол RIP?

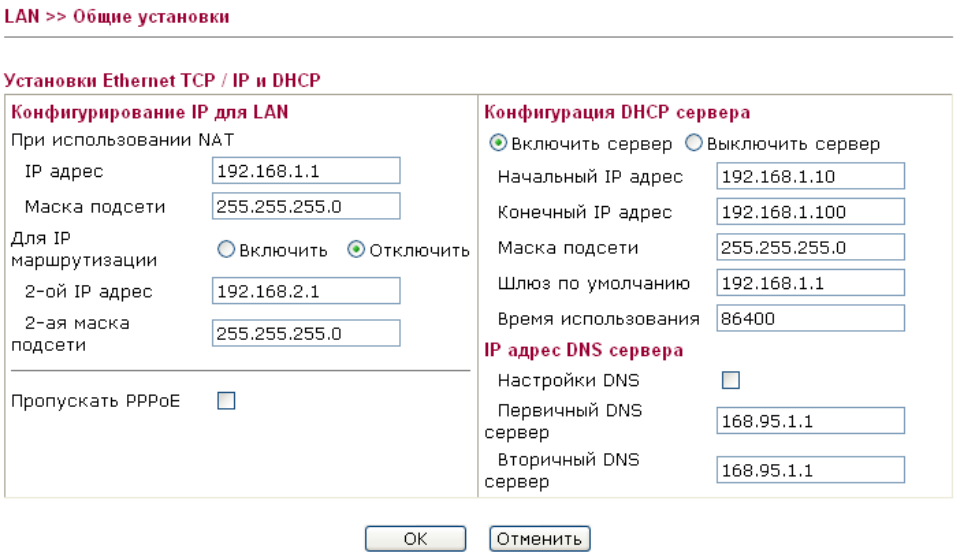
Чтобы улучшить свою работу, маршрутизатор Vigor будет обмениваться информацией о маршрутизации с соседними маршрутизаторами, используя протокол RIP (Routing Information Protocol). Это позволяет пользователям обмениваться такой информацией, как IP-адреса; маршрутизаторы будут автоматически информировать друг друга.

3.2.1 Общие настройки

Меню LAN > Общие настройки выглядит так:

Нажмите **LAN**, чтобы открыть настройки LAN и выберите **Общие настройки.**

На этой странице отображены основные настройки LAN.



IP-адрес	Введите частный IP-адрес для подключения к локальной частной сети (по умолч: 192.168.1.1).
Маска подсети	Введите маску, которая определит размеры подсети. (по умолч: 255.255.255.0)
Для IP маршрутизации	Включите, чтобы активировать функцию. По умолчанию: Отключено.
2-ой IP адрес	Введите вторичный IP-адрес для подключения к подсети (по умолч: 192.168.2.1).
2-ая маска подсети Mask	Маска, которая определит размеры сети.
Пропускать PPPoE	Если вы хотите использовать сетевой PPPoE-сервер через маршрутизатор, поставьте галочку, чтобы пропускать PPPoE-пакеты в назначенное место.
Конфигурация DHCP сервера	DHCP это протокол динамической конфигурации узла. Маршрутизатор может выполнять функции DHCP-сервера вашей сети. Он автоматически будет отправлять IP-настройки любому локальному пользователю-клиенту DHCP. Рекомендуется оставить маршрутизатор в качестве DHCP-сервера, если вы не имеете другого DHCP-сервера. Если вы хотите использовать другой DHCP-сервер в сети, Relay Agent поможет вам перенаправить DHCP-запрос в нужное место.
Включить сервер	Маршрутизатор будет автоматически раздавать IP-настройки узлам сети.
Выключить сервер	Вы можете назначить IP-адреса хостов самостоятельно.
Начальный IP адрес	Введите начальный IP-адрес. Если 1-й адрес маршрутизатора 192.168.1.1, следующий будет 192.168.1.2 или больше, но меньше, чем 192.168.1.254.
Конечный IP адрес	Введите конечный IP-адрес.
Маска подсети	Введите маску, которая определит размеры сети. (по умолч: 255.255.255.0/24)

Шлюз по умолчанию	Введите шлюз по умолчанию для DHCP-сервера. Это число всегда то же, что и 1й IP-адрес маршрутизатора, что означает, что маршрутизатор – шлюз по умолчанию.
Время использования	Вы можете установить время использования выданных IP-настроек для назначенного ПК.
Ручная настройка DNS	Если эта функция включена, сетевые компьютеры будут использовать введенные в эти поля первичный и вторичный DNS-серверы, как свои DNS-серверы. В противном случае сетевые компьютеры используют в качестве DNS-сервера маршрутизатор и маршрутизатор будет работать как DNS-прокси.
Первичный DNS сервер	Введите IP-адрес DNS-сервера. Если ваш провайдер не предоставляет их, маршрутизатор назначит IP DNS-сервера по умолчанию – 194.109.6.66.
Вторичный DNS сервер	Введите второй IP-адрес DNS-сервера. Если ваш провайдер не предоставляет их, маршрутизатор назначит вторичный IP DNS-сервера по умолчанию – 194.98.0.1. Если оставить незаполненными оба поля, маршрутизатор назначит IP-адреса локальным пользователям, как DNS-прокси сервер и будет поддерживать DNS-кэш. Если IP адрес домена уже в DNS-кэше, маршрутизатор переназначит доменное имя. В противном случае маршрутизатор перенаправляет очередь пакетов DNS на внешний DNS-сервер, установив WAN-подключение (напр. DSL/кабельное).

После завершения настроек, нажмите **ОК** для сохранения.

3.3 NAT

Обычно маршрутизатор работает в режиме устройства NAT. NAT – это механизм, с помощью которого один или несколько частных IP-адресов могут быть транслированы в один публичный. Публичный IP-адрес, как правило, назначен провайдером. Частные IP распознаются только внутренними хостами.

Когда исходящие пакеты, предназначенные для какого-либо публичного сервера, достигают NAT маршрутизатора, маршрутизатор поменяет адрес источника на публичный IP-адрес этого маршрутизатора, выберет доступный публичный порт и затем перенаправит его. При этом маршрутизатор сохранит информацию (адрес/порт), использованную при этом подключении. Когда публичный сервер отвечает, входящий трафик, разумеется, будет предназначен для публичного IP, но маршрутизатор перенаправит данные, основываясь на сохраненных ранее данных. Таким образом, внутренние и внешние хосты могут поддерживать связь без проблем.

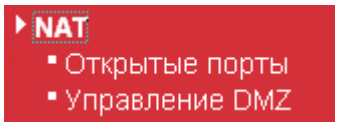
Среди преимуществ NAT:

- **Экономия на стоимости аренды публичных IP** и эффективное использование IP-адресов. NAT транслирует внутренние IP-адреса локальных хостов в публичные IP-адреса, так что множество внутренних хостов сможет работать посредством всего лишь одного IP-адреса.

- **Улучшение безопасности внутренних сетей, скрытие IP-адресов.** Есть много атак на основе прямого обращения к IP-адресу. Т.к. злоумышленнику не могут быть известны какие-либо из частных IP-адресов, функция NAT может надежно защитить внутреннюю сеть.

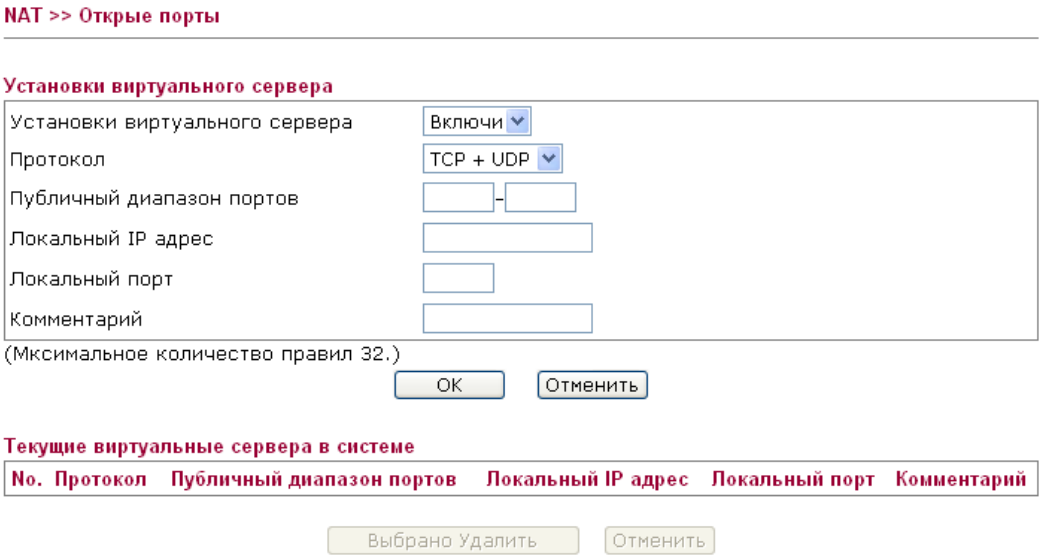
На странице NAT вы увидите частный IP-адрес, определенный в RFC-1918. Обычно по умолчанию мы используем подсети 192.168.1.0/24 для маршрутизатора. Как отмечалось ранее, функция NAT может назначить один или несколько IP-адресов и / или сервис-портов для разных сервисов. Иными словами, функция NAT также работает в случае использования метода назначения портов.

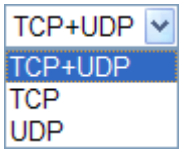
Ниже показано меню NAT.



3.3.1 Открытые порты

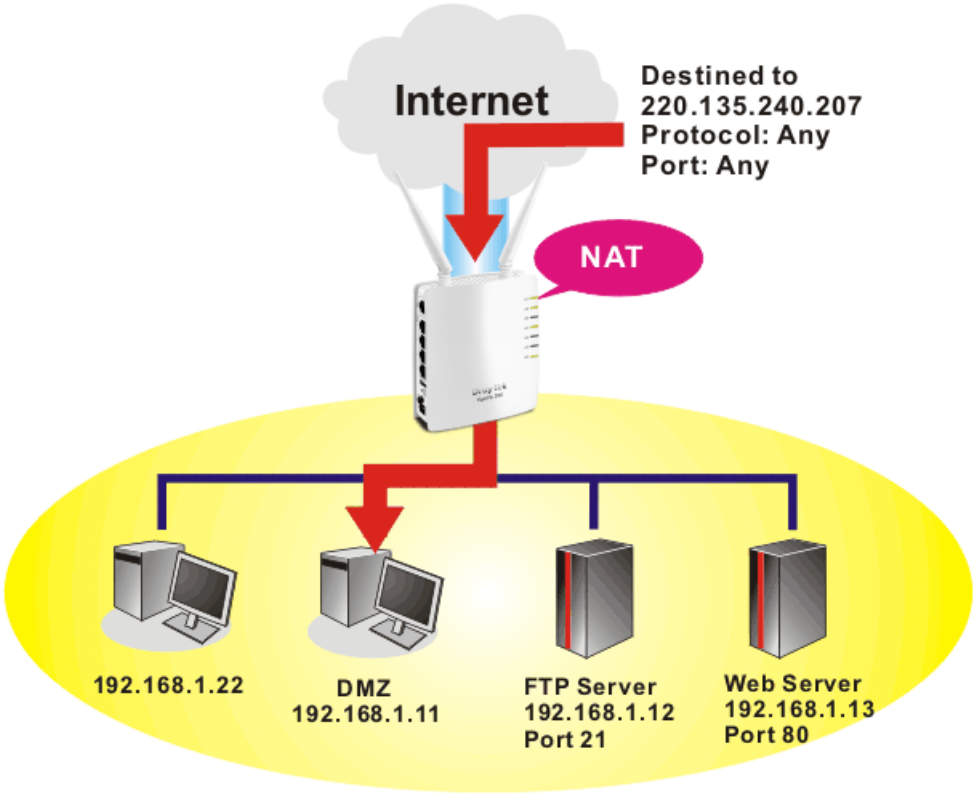
Открытые порты позволяют вам открыть несколько портов для прохождения данных специальных приложений. Обычно это P2P-приложения (напр., BT, KaZaA, Gnutella, WinMX, eMule и др.), веб-камеры и проч. Убедитесь в том, что вы используете последние версии приложений.



Установки виртуального сервера	Выберите **Включить**, чтобы включить эту настройку.
Протокол	Определите протоколы транспортного уровня: **TCP**, **UDP** или **TCP+UDP**. 
Публичный диапазон портов	Определите начальный и конечный номер портов для сервиса, предлагаемого локальным хостом.
Локальный IP адрес	Введите частный IP локального хоста.
Локальный порт	Если функция настроена, трафик будет привязан к этому порту локального хоста.
Комментарий	Введите описания данного правила для виртуального сервера.
OK	Когда вы завершите ввод настроек, нажмите на эту кнопку, чтобы сохранить изменения и отобразить поле **Текущие виртуальные сервера в системе**
Отмена	Нажмите, чтобы отменить последние настройки.
Удалить	Нажмите, чтобы удалить настройки выбранного виртуального сервера.

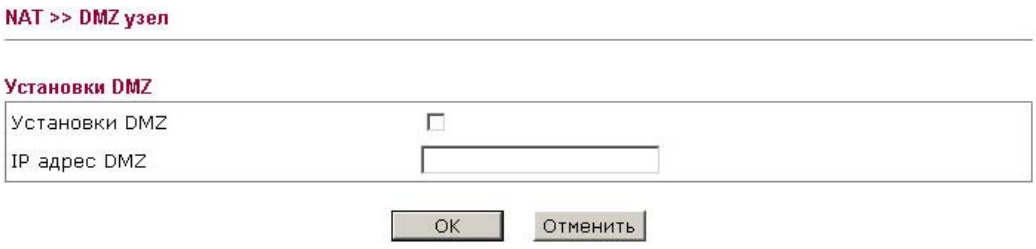
3.3.2 Управление DMZ

Маршрутизатор Vigor имеет возможность создания **Демилитаризованной зоны (DMZ)**. В этом режиме маршрутизатор будет направлять все незатребованные данные по любым протоколам на один узел в LAN. Обычные приложения других клиентов локальной сети продолжат работать без каких-либо проблем. DMZ позволяет определенному внутреннему пользователю быть полностью открытым, что бывает необходимо при работе некоторых приложений, например, Netmeeting или Интернет-игр.



Примечание: настройки безопасности NAT будут в известной степени ослаблены при настройке узла DMZ. Мы предлагаем вам добавить дополнительные фильтры или второй брандмауэр.

Нажмите **Управление DMZ**, чтобы открыть следующую страницу:



Установки DMZ	Галочка – чтобы активировать функцию узла DMZ.
IP адрес DMZ	Введите частный IP для узла DMZ.
OK	Нажмите, чтобы сохранить настройки.
Отменить	Нажмите, чтобы очистить последние настройки.

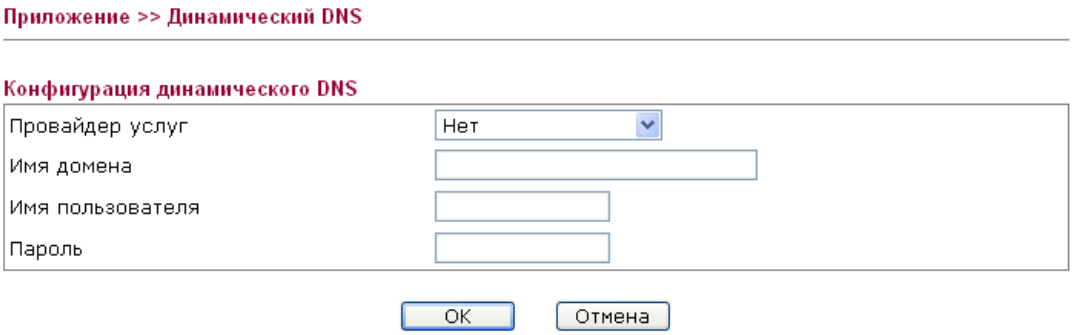
3.4 Приложения

Ниже показано меню Приложения.

3.4.1 Динамический DNS

Провайдер часто предоставляет динамический IP-адрес, когда вы подключаетесь к Интернету через провайдера. Это значит, что публичный IP, назначенный для вашего маршрутизатора, меняется каждый раз, когда вы подключаетесь к Интернету. Функция Динамического DNS позволяет вам назначить доменное имя для динамического IP WAN. Функция позволяет маршрутизатору обновлять его метки онлайн IP-адреса WAN назначенного динамического DNS-сервера. Когда маршрутизатор будет подключен к Интернету, у вас будет возможность использовать зарегистрированное доменное имя, чтобы получить доступ к маршрутизатору или внутреннему виртуальному серверу в Интернете. Это особенно полезная функция, если вы выступаете хостом веб-сервера, FTP-сервера или других серверов позади маршрутизатора.

Перед использованием функции динамического DNS, вы должны запросить свободный DDNS у провайдеров DDNS сервиса. Маршрутизатор позволяет создавать три аккаунта для трех различных провайдеров сервиса DDNS. Маршрутизатор Vigor совместим с DDNS-сервисами наиболее популярных провайдеров, таких как: **www.dyndns.org, www.no-ip.com, www.dtdns.com, www.changeip.com, www.dynamic- nameserver.com.** Вы должны посетить их веб-сайты, чтобы зарегистрировать доменное имя маршрутизатора.



Провайдер услуг	Выберите имя сервис-провайдера для DDNS-аккаунта. Если вы выбираете **Нет,** функция будет отключена.
Имя домена	Введите доменное имя, которое вы использовали ранее. Используйте «выпадающий список», чтобы выбрать нужный домен.
Имя пользователя	Введите имя, которое вы настроили для использования домена.
Пароль	Введите пароль.

После завершения настроек, нажмите **ОК** для сохранения.

3.5 **Беспроводная сеть** LAN

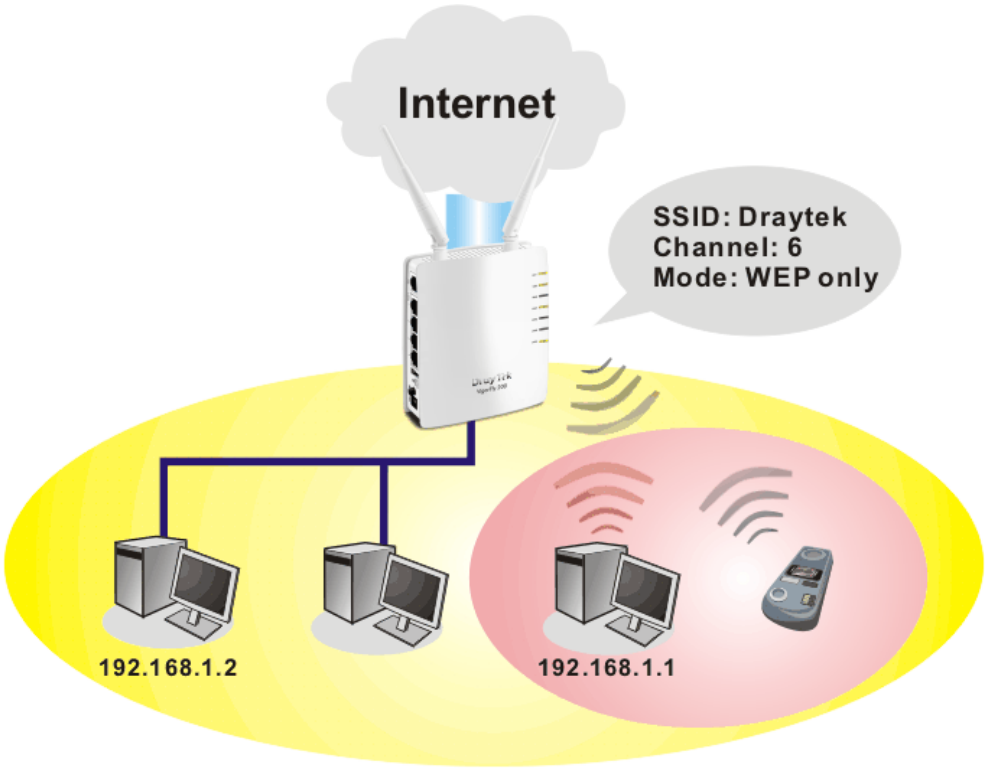
3.5.1 Основные принципы

В последние годы произошел огромный рост рынка беспроводной связи. Беспроводные технологии сейчас доступны практически в каждом уголке планеты. Сотни миллионов людей сегодня обмениваются информацией с помощью беспроводных устройств связи. Маршрутизатор Vigor создан для эффективной работы в малом офисе или дома. Теперь сотрудникам компаний достаточно принести в переговорную комнату всего лишь один ноутбук, в то время как раньше приходилось прокладывать сетевые кабели или сверлить в стенах отверстия. Беспроводная сеть обеспечивает высокую мобильность – так что пользователи WLAN могут одновременно получать доступ как к Интернету, так и к LAN (как если бы это была проводная связь).

Беспроводные маршрутизаторы VigorFly200 оснащены беспроводным LAN интерфейсом, работающим вместе по стандарту IEEE 802.11n draft 2. Маршрутизатор использует специальную беспроводную технологию, которая позволяет повысить скорость передачи данных до 300 Мбит/с*. У вас никогда не возникнет проблем с потоковой передачей музыки или видео.

Примечание: * Скорость передачи данных может отличаться в зависимости от условий сети и факторов среды, включая объем сетевого трафика, ограничение скорости провайдером и используемые материалы.

В режиме инфраструктуры маршрутизатор играет роль точки доступа, к которой подключаются беспроводные клиенты. Все клиенты будут делить одно Интернет-подключение. Раздел **Основные настройки** позволит вам настроить беспроводную сеть, включая ее SSID идентификацию, радиочастотный канал и проч.



Обзор безопасности

Шифрование в реальном времени: маршрутизатор Vigor поддерживает систему шифрования AES, что может повысить степень защиты вашей информации, не оказывая влияния на работу приложений.

Широкий выбор стандартов безопасности: чтобы вы могли быть уверенными в безопасности и секретности ваших беспроводных подключений, мы предлагаем вам несколько стандартов безопасности.

WEP (Wired Equivalent Privacy) – это унаследованный метод шифрования с использованием 64-битного или 128-битного ключа каждого передаваемого по радио пакета. Обычно точка доступа назначит набор из четырех ключей и привяжет их к каждой станции, используя только один ключ из четырех.

WPA (Wi-Fi Protected Access), наиболее доминирующий механизм безопасности в индустрии, делится на две категории: WPA-персональный или называемый WPA-Заранее заданные ключи (WPA Pre-Share Key – WPA/PSK), и WPA-предприятие или WPA/802.1x.

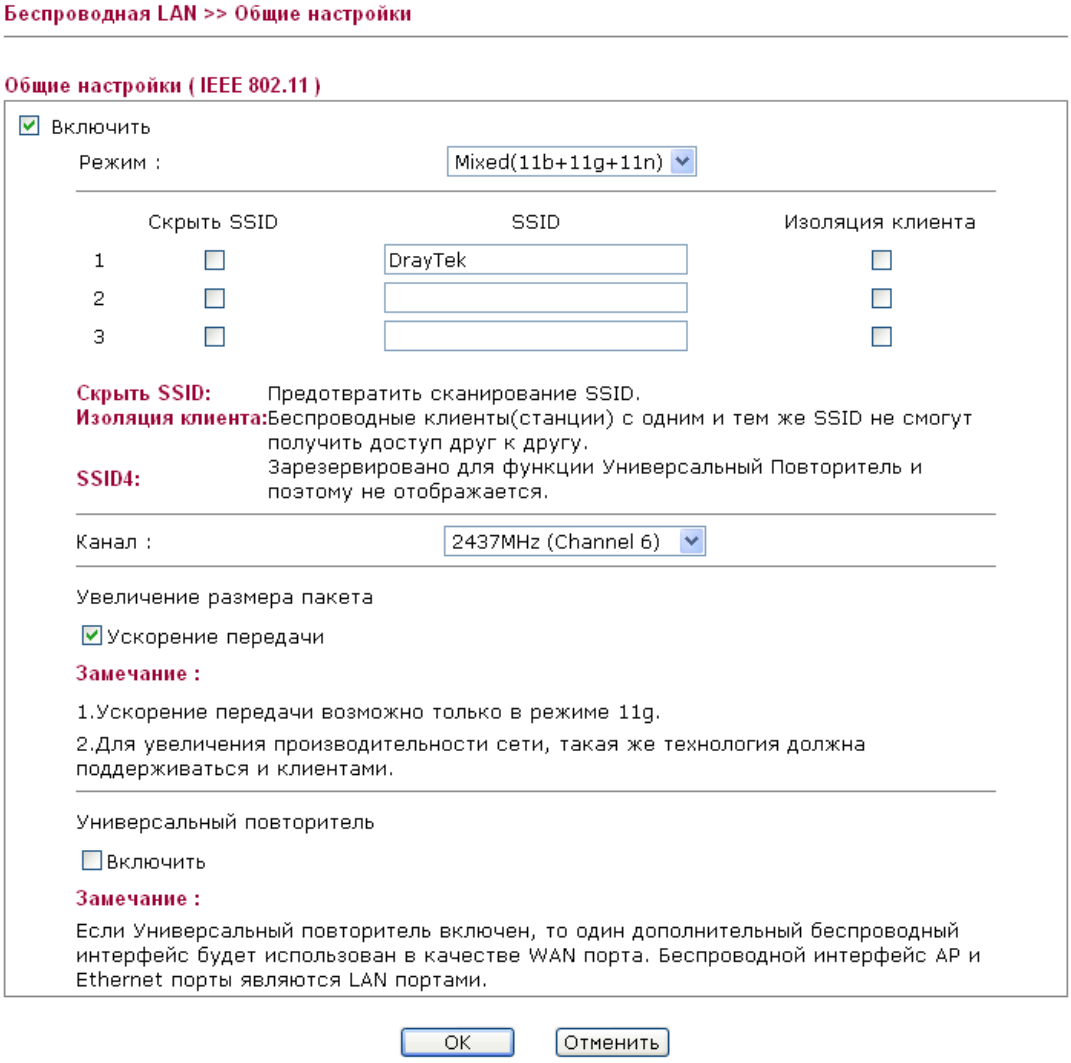
В WPA-персональном во время передачи данных для шифрования используются заранее заданные ключи. WPA запрашивает временный протокол целостности ключа (TKIP) для шифрования данных, в то время как WPA2 запрашивает AES. WPA-предприятие сочетает шифрование с аутентификацией.

Поскольку была подтверждена уязвимость системы WEP, мы советуем вам выбрать WPA для наиболее защищенного подключения. Вы должны выбрать механизм защиты по вашим потребностям. Неважно, какую систему безопасности вы выберете, все они усиливают защиту беспроводной передачи данных и/или увеличивают секретность вашей беспроводной сети. Беспроводной маршрутизатор Vigor гибок и может одновременно поддерживать множество защищенных подключений как с WEP, так и с WPA.

Ниже показано меню **Беспроводная сеть**.

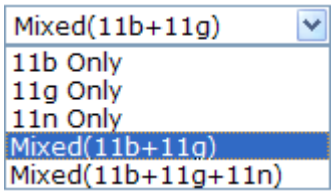
3.5.2 Общие настройки

При нажатии **Общие настройки** появится веб-страница, на которой вы сможете настроить SSID и беспроводной канал.



Включить беспроводную LAN — Галочка – чтобы активировать функцию.

Режим — В настоящий момент маршрутизатор может подключаться к Смешанной (Mixed) (11b+11g), только 11g, только 11b, только 11n и Смешанным (Mixed) (11b+11g+11n) станциям одновременно. Выберите режим Mix (11b+11g+11n).



Скрыть SSID — Отметьте, чтобы предотвратить широковещание SSID в эфире.

SSID — Введите имя для идентификации беспроводной сети маршрутизатора. Устройство поддерживает до 3

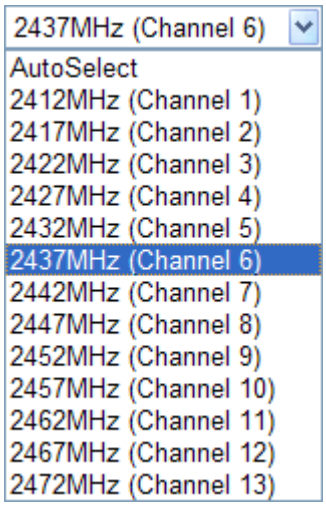
независимых SSID. Каждый беспроводной клиент, подключенный к одному SSID, не будет видеть беспроводных клиентов, подключенных к другому.

Изоляция клиента

Отметьте, чтобы беспроводные клиенты/станции с одним SSID не имели доступа друг к другу.

Канал

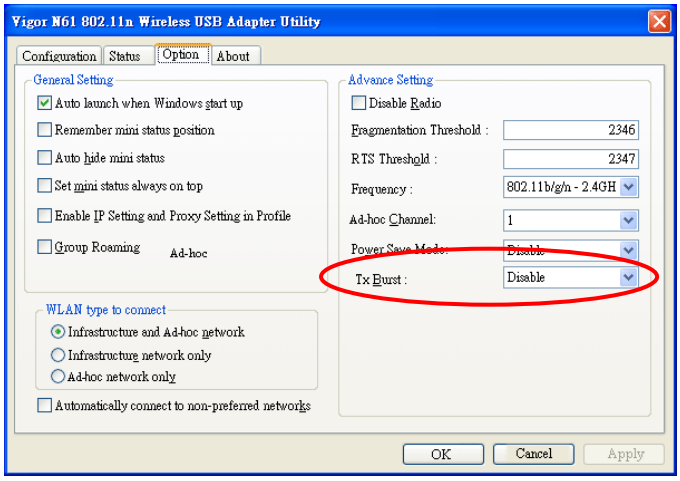
Частотный канал беспроводной LAN. По умолчанию – 6. Вы можете переключить канал, если на выбранном канале сильные помехи. Если вы не имеете понятия о частоте, выберите АвтоВыбор, чтобы система могла решить это за вас.



Увеличение размера пакета

Эта функция может увеличить скорость передачи данных на 40% (Кликните на **Ускорение передачи**). Функция активна только когда она одновременно поддерживается и точкой доступа, и станцией (беспроводным клиентом). Поэтому беспроводной клиент должен также поддерживать эту функцию.

Примечание: эту функцию поддерживает беспроводной адаптер DraytekVigor N61. Поэтому вы можете использовать и установить ее прямо на ваш компьютер для согласования с Packet-OVERDRIVE (выберите **Включить** в меню **Ускорение Передачи** во вкладке **Опции**, как на картинке).



Универсальный Повторитель

Если включен этот режим, точка доступа может работать как беспроводной повторитель, она может быть станцией и точкой доступа одновременно. Она может использовать функции станции, чтобы подсоединиться к Корневой ТД и использовать функцию ТД для обслуживания всех беспроводных станций в пределах покрытия.

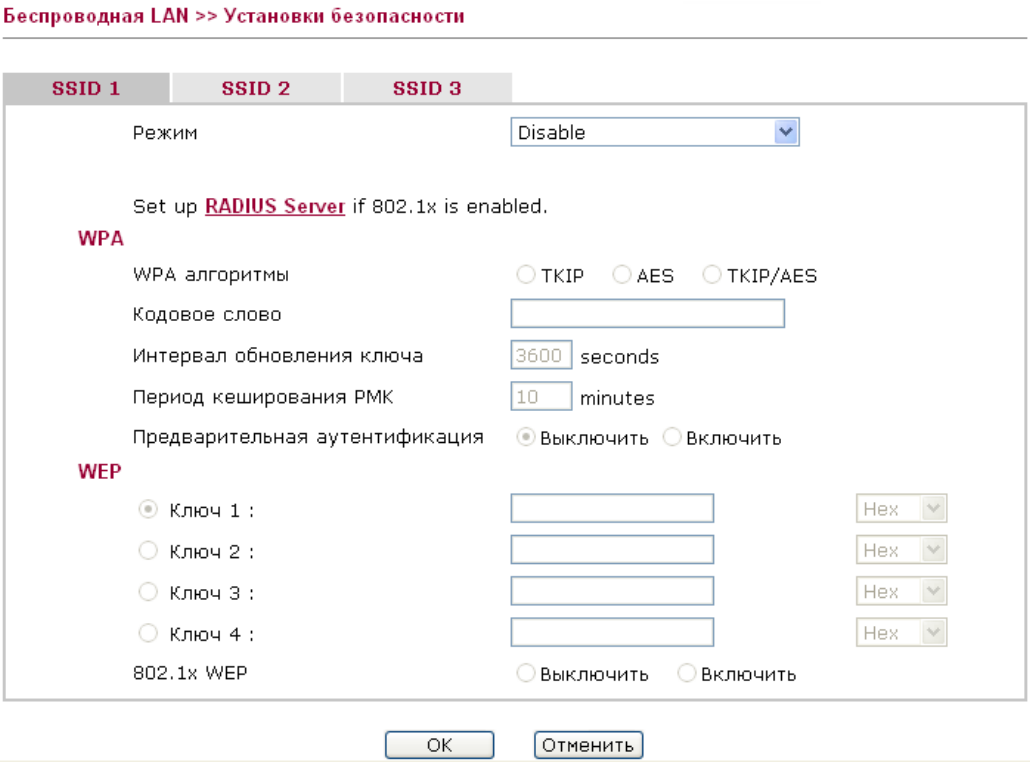
Галочка – чтобы активировать функцию. Она станет отображаться в меню **Беспроводная LAN** для ваших дальнейших настроек. Для этого нажмите Обновить в вашем браузере или нажмите F5 на клавиатуре.

Откройте **Беспроводная сеть>>Универсальный повторитель**. Более подробную информацию вы найдете в соответствующем разделе руководства.

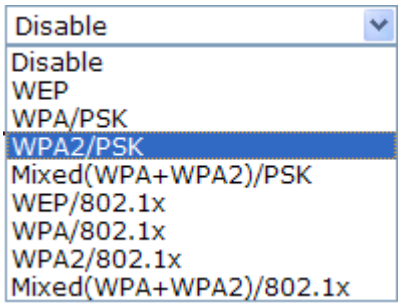
3.5.3 Безопасность

Эта страница позволяет вам настроить режимы безопасности для SSID 1, 2 и 3 соответственно. После настройки нажмите **ОК** для сохранения и активации изменений.

После выбора пункта **Безопасность** появится новое окно.



Режим Вам на выбор будет предложено несколько режимов.

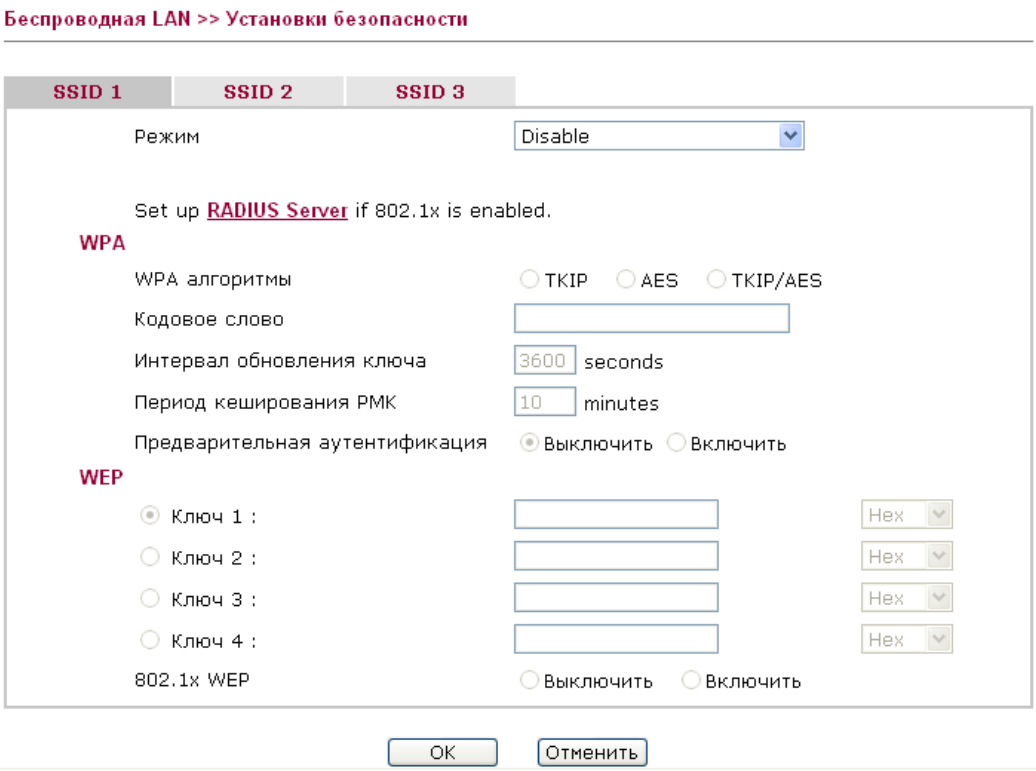


- **Отключить**

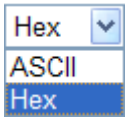
  Механизм шифрования будет отключен.

- **WEP**

  Принимает только WEP-клиентов, в поле WEP Ключ должен быть введен ключ шифрования.

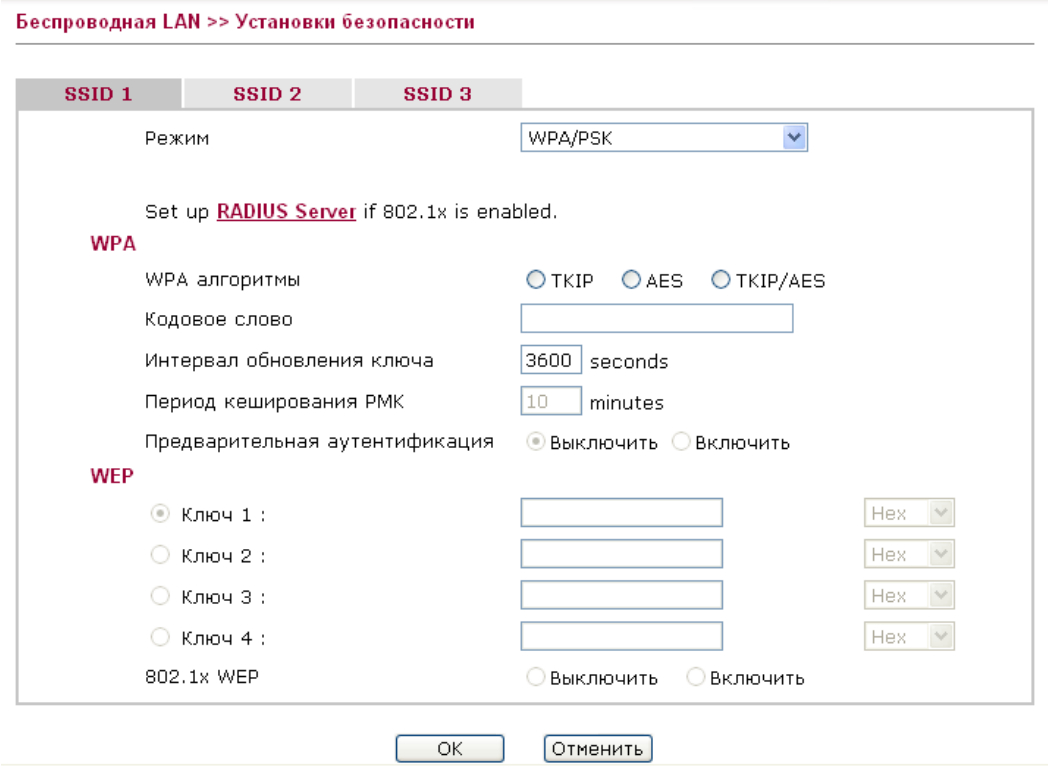


Ключ 1 ~ Ключ 4 Можно ввести четыре ключа, но использован будет только один, выбранный пользователем. Формат WEP-ключа ограничивается 5 символами ASCII или 10 шестнадцатеричными значениями 64-битного шифрования; или 13 символами ASCII или 26 шестнадцатеричными значениями 128-битного шифрования. Разрешены символы ASCII с 33(!) до 126(~) кроме '#' и ','.



- **WPA/PSK или WPA2/PSK или Смешанное шифрование (WPA+WPA2)/PSK**

  Принимает только WPA-клиентов; ключ шифрования должен быть введен с заранее заданными ключами. WPA кодирует каждый переданный пакет, используя ключи, которые вводятся в соответствующее поле или автоматически передаются посредством 802.1x авторизации.

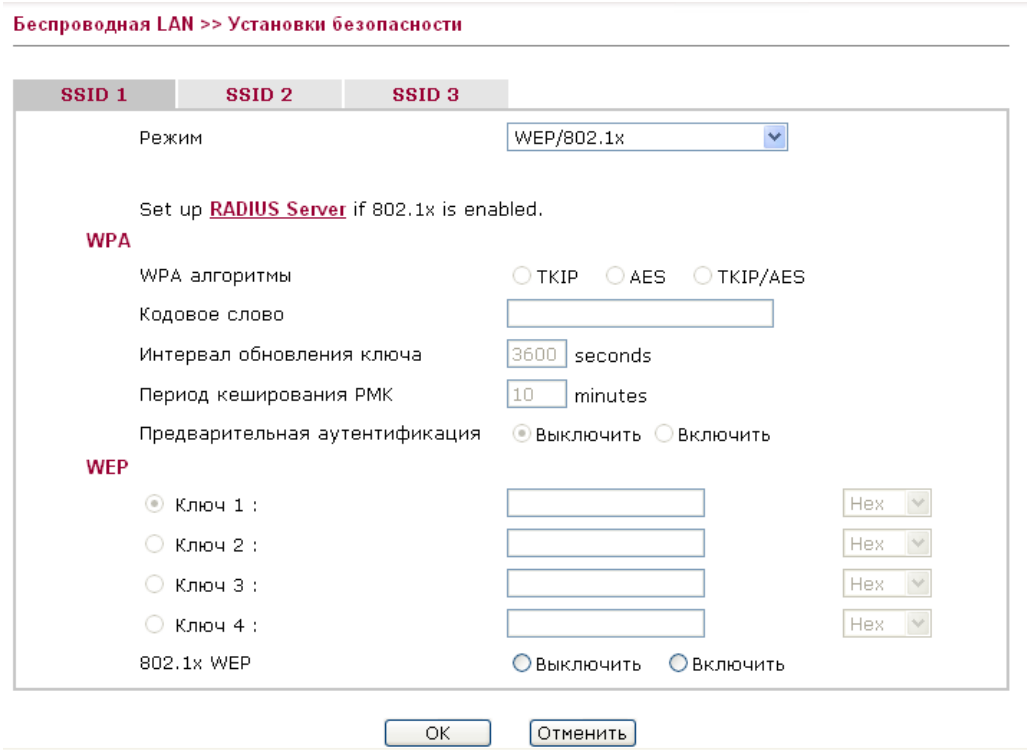


WPA алгоритмы	Выберите WPA алгоритм: TKIP, AES или TKIP/AES.
Кодовое слово	8~63 ASCII символы, такие как 012345678..(или 64 шестнадцатеричных знака, начинающиеся с 0x, такие как "0x321253abcde...").
Интервал обновления ключа	WPA использует ключи авторизации сети. Тем не менее, нормальные сетевые операции используют различные ключи шифрования, которые генерируются произвольно. Введите в этом поле временной интервал смены ключей (в секундах). Меньший интервал увеличит безопасность, но снизит мощность. По умолчанию установлен интервал в 3600 секунд. Установите 0 для отключения генерации ключей.

- **WEP/802.1x**

  Встроенная функция RADIUS-клиента позволяет маршрутизатору поддерживать удаленного пользователя или беспроводного передатчика и RADIUS-сервер в выполнении взаимной идентификации. Данная функция активирует централизованный удаленный доступ идентификации для сетевого управления.

  WPA кодирует каждый передаваемый пакет, используя ключ, который может быть заранее заданным PSK и введенным вручную в соответствующем поле или автоматически установлен в процессе 802.1x аутентификации. Выберите режим WPA, WPA2 или Auto в качестве режима WPA.

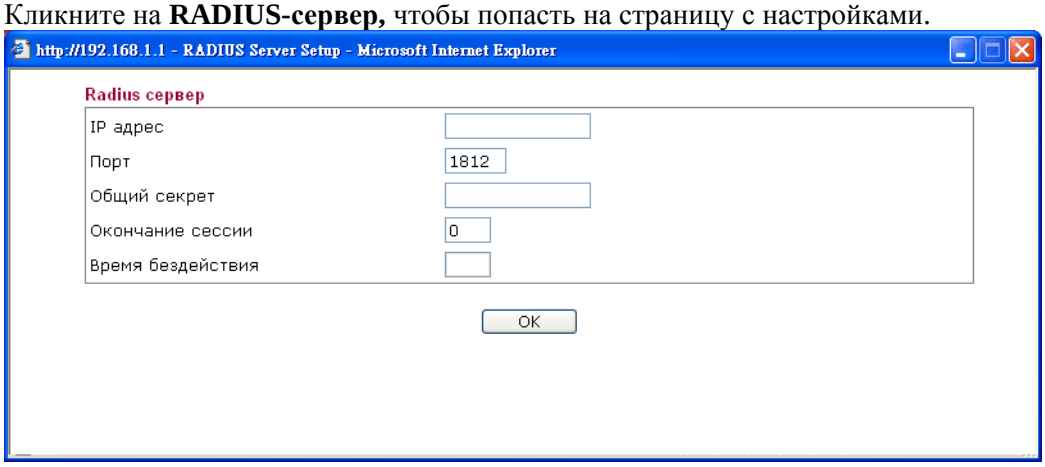


802.1x WEP

Отключить – Отключить WEP-шифрование. Информация, передаваемая в точку доступа, не будет кодироваться.

Включить – Включить WEP-шифрование.

Кликните на **RADIUS-сервер,** чтобы попасть на страницу с настройками.



IP-адрес Введите IP-адрес RADIUS-сервера.

Порт Номер UDP-порта, используемого RADIUS-сервером. По умолчанию установлен 1812 на основе RFC 2138.

Общий секрет RADIUS-сервер и клиент имеют общий секрет, который используется для идентификации сообщений между ними. Обе стороны должны быть настроены для использования одного и того же общего секрета.

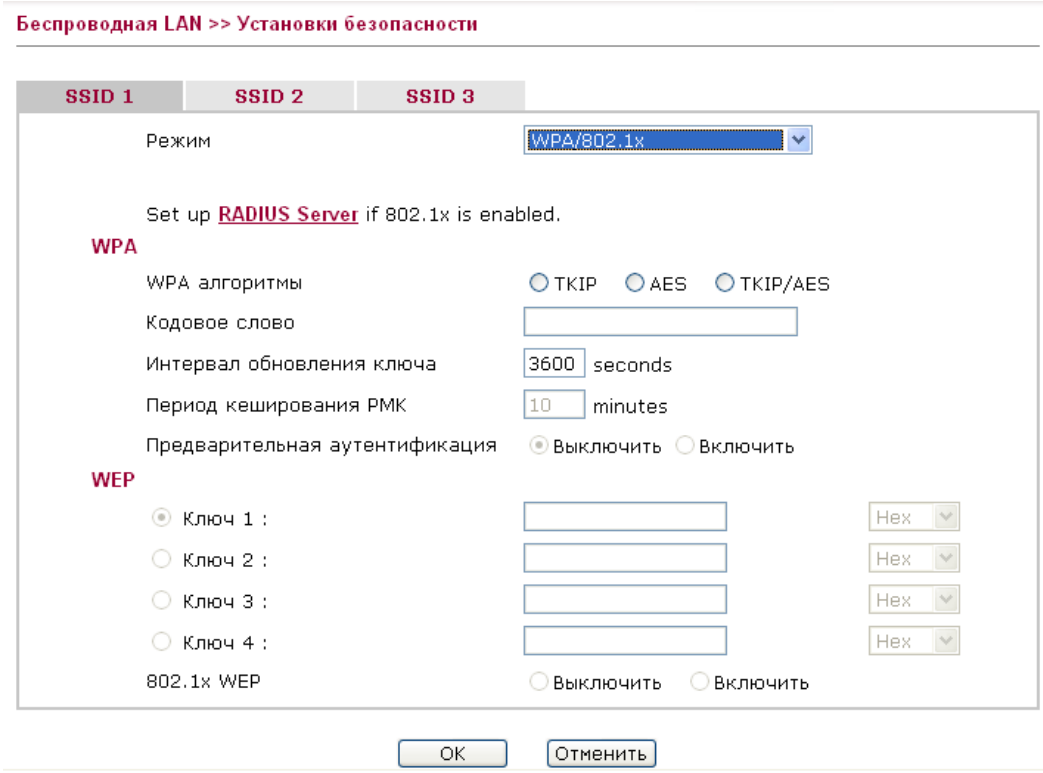
Окончание сессии Установите временной максимум предоставления услуг перед реидентификацией. Впишите ноль, чтобы

установить немедленную идентификацию сразу же после окончания сессии (указывайте время в секундах).

Время бездействия — **Время бездействия –** установите время бездействия перед разрывом соединения.

- **WPA/802.1x**

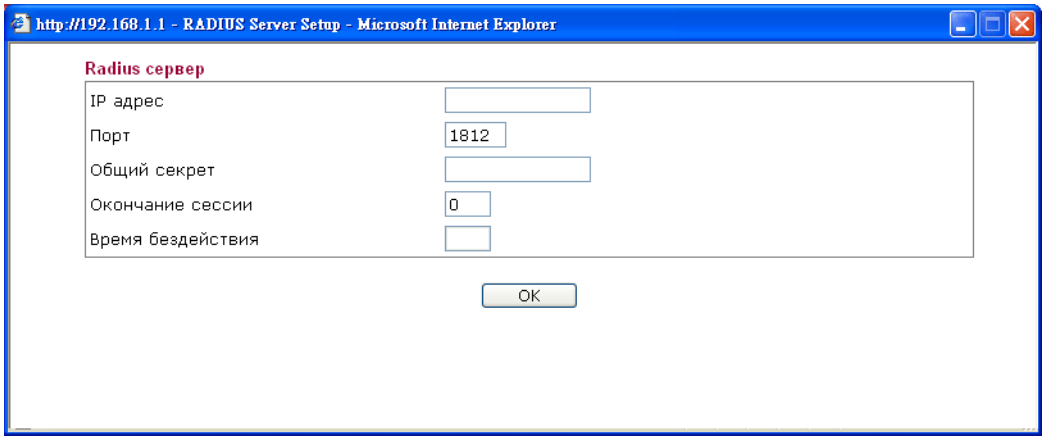
WPA кодирует каждый переданный пакет, используя заранее заданные ключи (PSK), которые вводятся в соответствующее поле или автоматически передаются посредством 802.1x авторизации.



WPA алгоритмы — Выберите WPA алгоритм: TKIP, AES или TKIP/AES.

Интервал обновления ключа — WPA использует ключи авторизации сети. Тем не менее, нормальные сетевые операции используют различные ключи шифрования, которые генерируются произвольно. Введите в этом поле временной интервал смены ключей (в секундах). Меньший интервал увеличит безопасность, но снизит мощность. По умолчанию установлен интервал в 3600 секунд. Установите 0 для отключения генерации ключей.

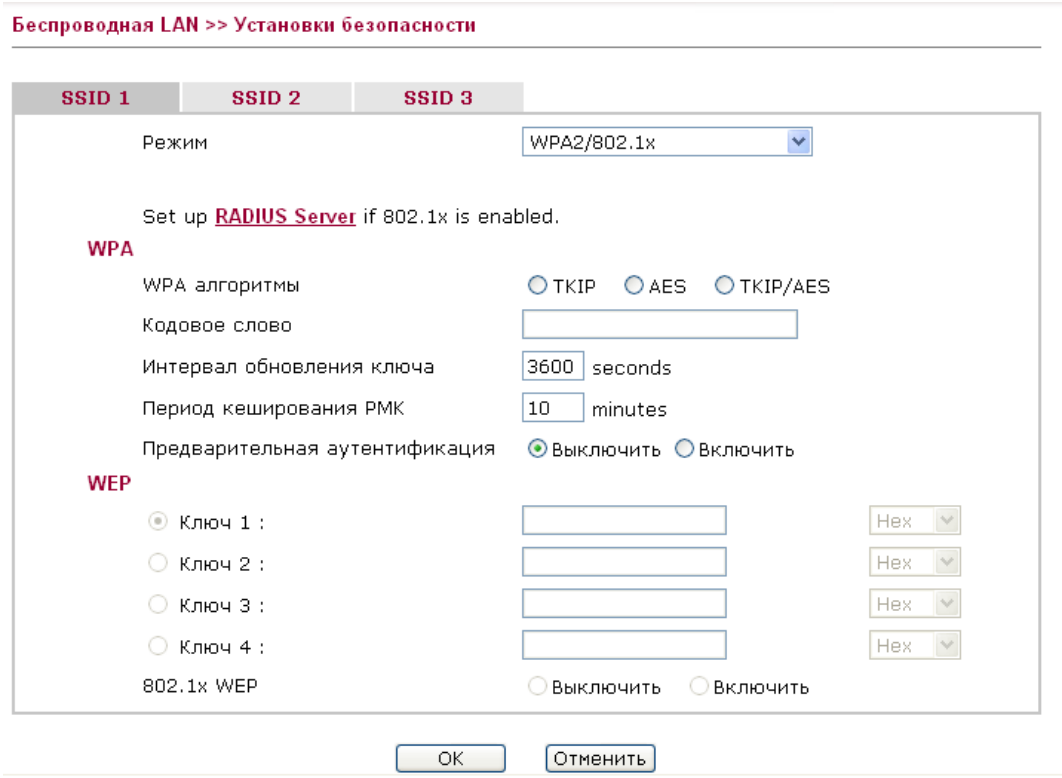
Кликните на **RADIUS-сервер,** чтобы попасть на страницу с настройками.



IP-адрес	Введите IP-адрес RADIUS-сервера.
Порт	Номер UDP-порта, используемого RADIUS-сервером. По умолчанию установлен 1812 в соответствии с RFC 2138.
Общий секрет	RADIUS-сервер и клиент имеют общий секрет, который используется для идентификации сообщений между ними. Обе стороны должны быть настроены для использования одного и того же общего секрета.
Окончание сессии	Установите временной максимум предоставления услуг перед реидентификацией. Впишите ноль, чтобы установить немедленную идентификацию сразу же после окончания сессии (указывайте время в секундах).
Время бездействия	**Время бездействия –** установите время бездействия перед разрывом соединения.

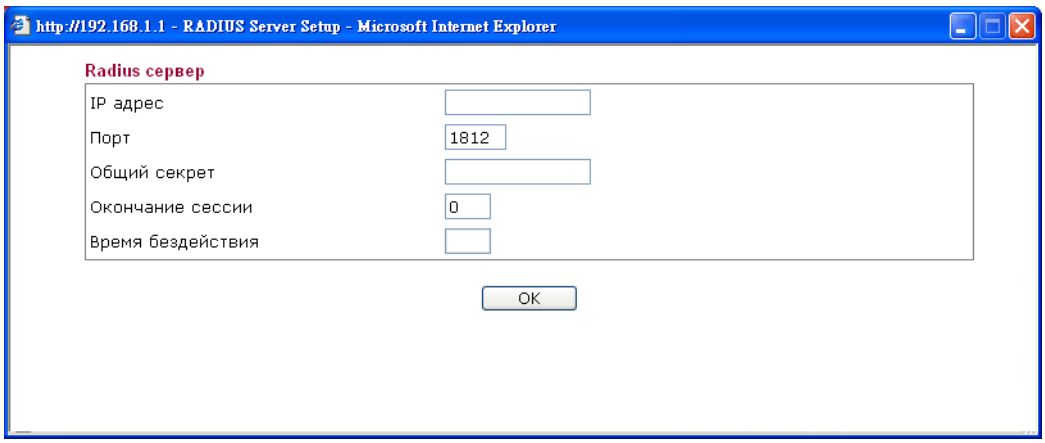
- **WPA2/802.1x**

WPA кодирует каждый переданный пакет, используя заранее заданные ключи (PSK), которые вводятся в соответствующее поле или автоматически передаются посредством 802.1x авторизации.



WPA алгоритмы	Выберите WPA алгоритм: TKIP, AES или TKIP/AES.
Интервал обновления ключа	WPA использует ключи авторизации сети. Тем не менее, нормальные сетевые операции используют различные ключи шифрования, которые генерируются произвольно. Введите в этом поле временной интервал смены ключей (в секундах). Меньший интервал увеличит безопасность, но снизит мощность. По умолчанию установлен интервал в 3600 секунд. Установите 0 для отключения генерации ключей.
PMK Cache Period	Установите период хранения WPA2 PMK (парные ключи). PMK Cache управляет списком BSSID и ассоциированными SSID, с которыми устройство идентифицировалось ранее.
Предварительная аутентификация	Активирует передатчик для идентификации и более безопасного и быстрого переключения между точками доступа. С процедурой предварительной аутентификации, определенной спецификацией IEEE 802.11i, предварительное четырехстороннее рукопожатие может уменьшить задержку передачи, воспринимаемую мобильной точкой. Это сделает переключение более безопасным и быстрым (доступно только в WPA2). **Включить –** Включить IEEE 802.1X предварительную аутентификацию. **Выключить –** Выключить IEEE 802.1X предварительную аутентификацию.

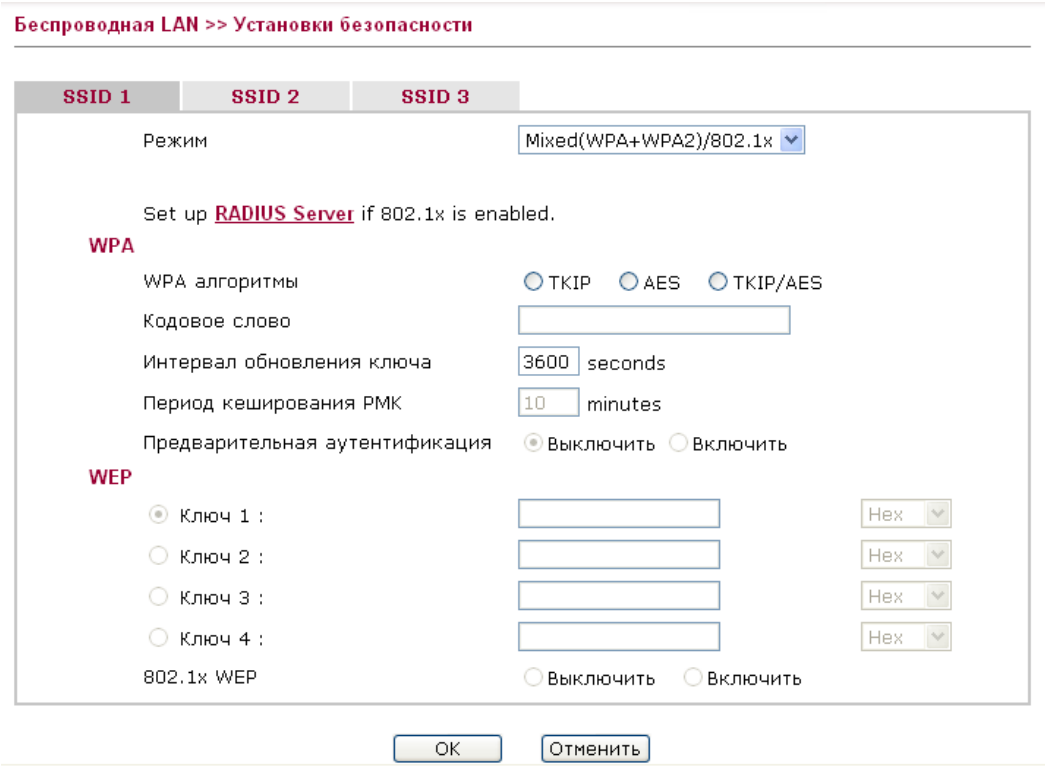
Кликните на **RADIUS-сервер,** чтобы попасть на страницу с настройками.



IP-адрес	Введите IP-адрес RADIUS-сервера.
Порт	Номер UDP-порта, используемого RADIUS-сервером. По умолчанию установлен 1812 в соответствии с RFC 2138.
Общий секрет	RADIUS-сервер и клиент имеют общий секрет, который используется для идентификации сообщений между ними. Обе стороны должны быть настроены для использования одного и того же общего секрета.
Окончание сессии	Установите временной максимум предоставления услуг перед реидентификацией. Впишите ноль, чтобы установить немедленную идентификацию сразу же после окончания сессии (указывайте время в секундах).
Время бездействия	**Время бездействия –** установите время бездействия перед разрывом соединения.

- **Смешанное шифрование (WPA+WPA2)/802.1x**

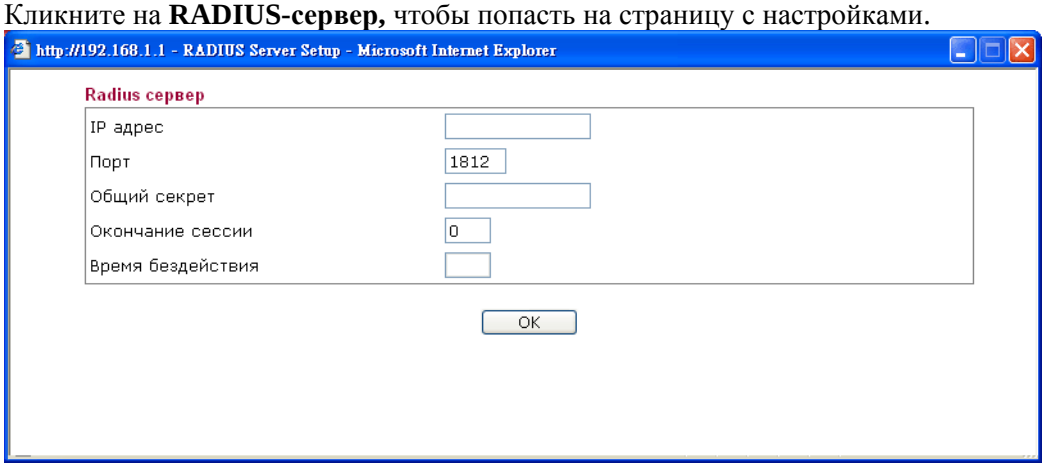
  WPA кодирует каждый переданный пакет, используя заранее заданные ключи (PSK), которые вводятся в соответствующее поле или автоматически передаются посредством 802.1x авторизации.



WPA алгоритмы Выберите WPA алгоритм: TKIP, AES или TKIP/AES.

Интервал обновления ключа WPA использует ключи авторизации сети. Тем не менее, нормальные сетевые операции используют различные ключи шифрования, которые генерируются произвольно. Введите в этом поле временной интервал смены ключей (в секундах). Меньший интервал увеличит безопасность, но снизит мощность. По умолчанию установлен интервал в 3600 секунд. Установите 0 для отключения генерации ключей.

Кликните на **RADIUS-сервер,** чтобы попасть на страницу с настройками.



IP-адрес Введите IP-адрес RADIUS-сервера.

Порт Номер UDP-порта, используемого RADIUS-сервером. По умолчанию установлен 1812 в соответствии с RFC 2138.

Общий секрет RADIUS-сервер и клиент имеют общий секрет, который используется для идентификации сообщений между

ними. Обе стороны должны быть настроены для использования одного и того же общего секрета.

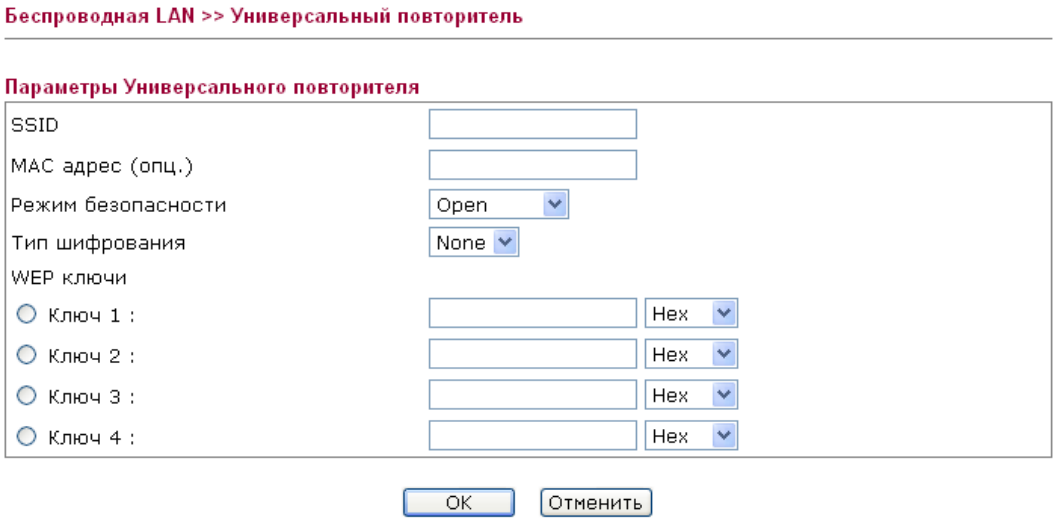
Окончание сессии — Установите временной максимум предоставления услуг перед реидентификацией. Впишите ноль, чтобы установить немедленную идентификацию сразу же после окончания сессии (указывайте время в секундах).

Время бездействия — **Время бездействия –** установите время бездействия перед разрывом соединения.

3.5.4 Универсальный повторитель

Это меню доступно только когда эта функция активирована в меню **Беспроводная сеть>>Общие настройки**. Эта функция позволяет вам назначить точки доступа, к которым может подключаться удаленный клиент. VigorFly 200 может работать как беспроводной повторитель; он может быть и клиентом и точкой доступа одновременно. Он может использовать режим клиента для подключения к корневой точке доступа и использовать режим точки доступа для управления всеми беспроводными станциями внутри зоны покрытия.

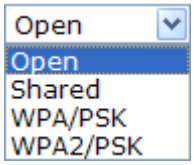
> **Примечание:** Во время использования функции Универсальный повторитель точка доступа будет демодулировать принятый сигнал. Пожалуйста, проверьте, не является ли этот сигнал шумами от другой работающей сети, нужный сигнал будет модулирован и усилен. Выходная мощность у этого режима такая же, как у WDS или обычной работы в режиме точки доступа.



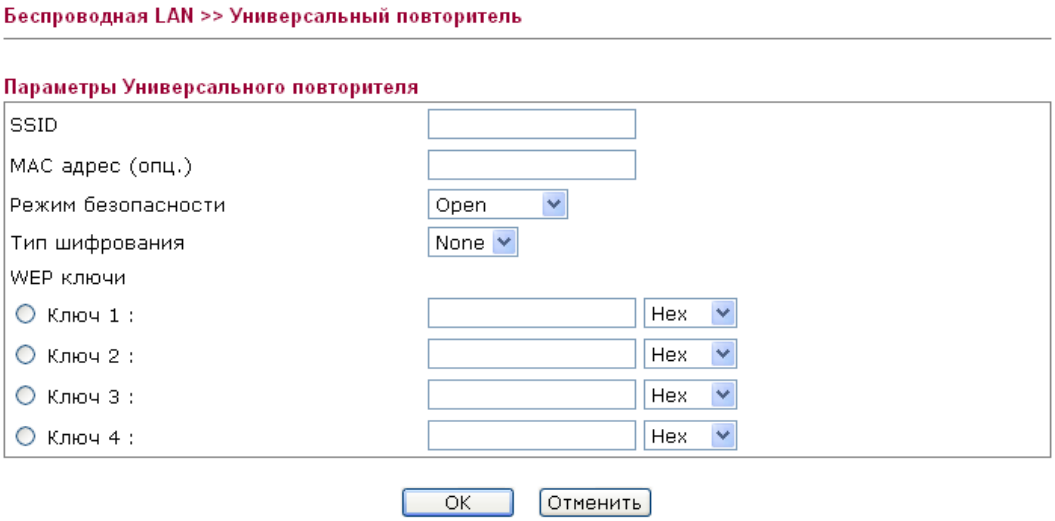
SSID — Установите имя идентификации маршрутизатора.

MAC-адрес (опционально) — Введите MAC-адрес точки доступа, к которой будет подключаться маршрутизатор.

Режим безопасности — Вам на выбор будет предложено несколько режимов с разными параметрами (напр., WEP ключи, Ключевое слово).

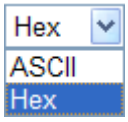


- **Открытый / Совместный режим**

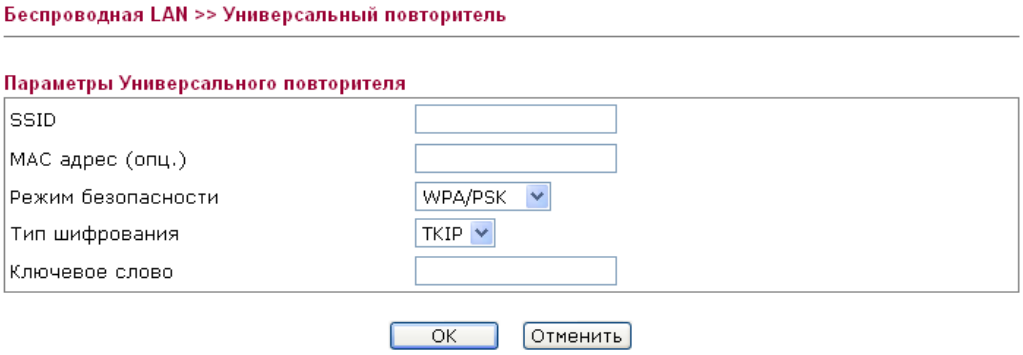


Тип шифрования — Выберите **Нет,** чтобы выключить WEP-шифрование. Информация, отправляемая в точку доступа, не будет шифрована. Чтобы включить WEP-шифрование данных, выберите **WEP.**

WEP Ключи — Можно ввести четыре ключа, но использован будет только один, выбранный пользователем. Формат WEP-ключа ограничивается 5 символами ASCII или 10 шестнадцатеричными значениями 64-битного шифрования; или 13 символами ASCII или 26 шестнадцатеричными значениями 128-битного шифрования. Разрешены символы ASCII с 33(!) до 126(~) кроме '#' и ','.



- **Режим WPA/PSK и режим WPA2/PSK**

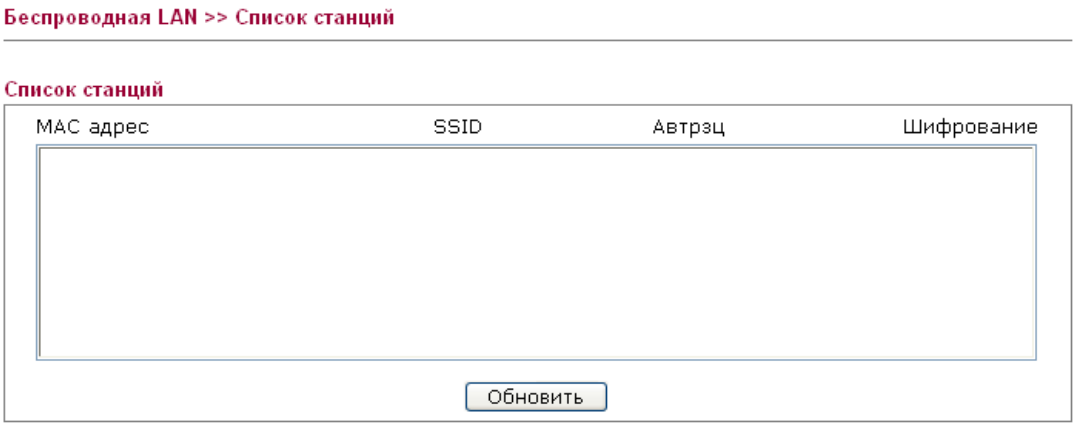


Тип шифрования — Выберите TKIP или AES в качестве алгоритма WPA.

Кодовое слово — 8~63 ASCII символы, такие как 012345678..(или 64 шестнадцатеричных знака, начинающиеся с 0x, такие как "0x321253abcde...").

3.5.5 Список беспроводных клиентов

Список беспроводных клиентов отображает информацию о подключениях беспроводных клиентов вместе с их историями подключений.

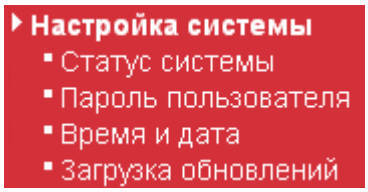


MAC-адрес	Показывает MAC-адрес подключающегося клиента
SSID	Показывает SSID подключающегося клиента
Автрзц	Показывает режим авторизации подключающегося клиента
Шифрование	Показывает метод шифрования подключающегося клиента
Обновить	Нажмите, чтобы обновить страницу

3.6 Настройка системы

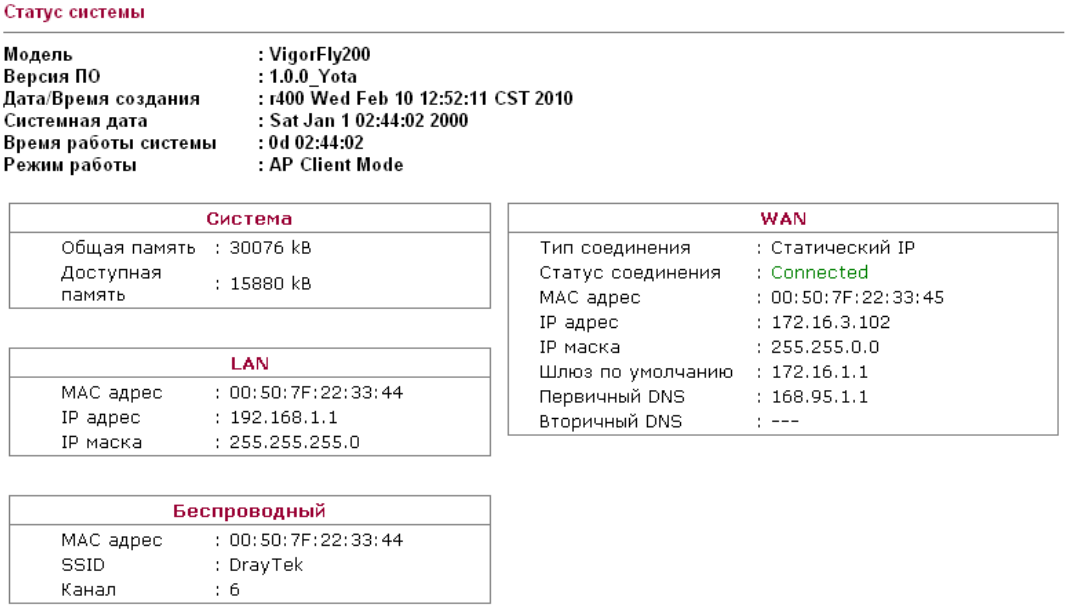
Для настройки системы вы можете использовать следующие разделы меню настроек: Статус системы, Время и дата, Загрузка обновлений.

Ниже показано меню Настройка системы.



3.6.1 Статус системы

Статус системы позволяет определить основные сетевые настройки маршрутизатора. Он также включает информацию LAN и WAN интерфейсов. Вы можете увидеть время последнего обновления и рабочую версию ПО.

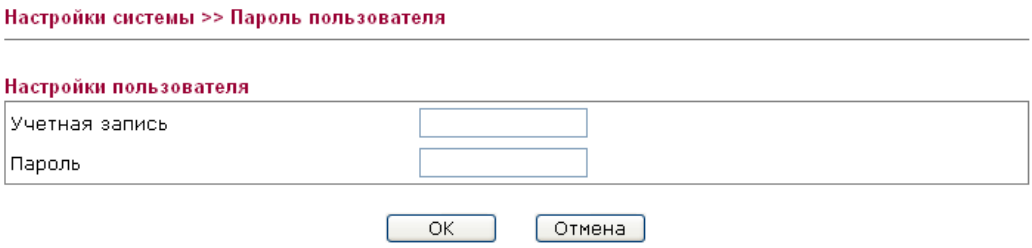


Модель	Отображает название модели маршрутизатора.
Версия ПО	Отображает версию ПО маршрутизатора.
Дата/Время создания	Отображает дату и время нынешней версии ПО маршрутизатора.
Системная дата	Отображает дату и время системного сервера.
Время работы системы	Отображает время подключения системного сервера.
Режим работы	Отображает режим работы маршрутизатора
Общая память	Отображает размер оперативной памяти системы.
Доступная память	Отображает доступную память системы.
MAC-адрес	Отображает MAC-адрес LAN/WAN/WLAN интерфейса.
IP-адрес	Отображает MAC-адрес LAN/WAN интерфейса.
IP-маска	Отображает адрес маски подсети LAN/WAN

	интерфейса.
Тип устройства	Отображает тип устройства, использованного для беспроводной LAN.
SSID	Отображает SSID этого маршрутизатора.
Канал	Отображает канал, использованный беспроводной LAN.
Тип соединения	Отображает тип сетевого соединения этого маршрутизатора.
Статус соединения	Отображает статус сети.
Шлюз по умолчанию	Отображает адрес шлюза WAN-интерфейса.
Первичный DNS	Отображает настройки назначенного первичного DNS.
Вторичный DNS	Отображает настройки назначенного вторичного DNS.

3.6.2 Пароль пользователя

Эта страница позволяет вам установить новый пароль для пользовательских операций.

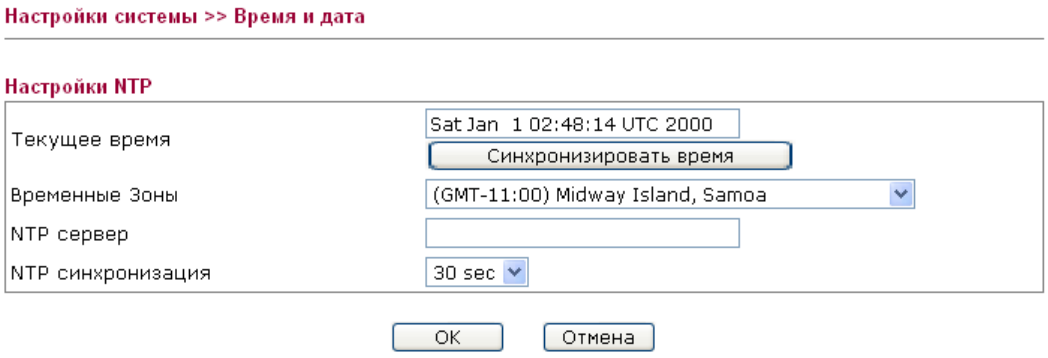


Учетная запись	Введите имя для входа.
Пароль	Введите новый пароль.

Когда вы нажмете **OK**, появится окно **Вход.** Пожалуйста, используйте новый пароль для доступа к странице настроек.

3.6.3 Время и дата

Вы можете установить время.



Текущее время	Нажмите **Синхронизировать время.**
Временные Зоны	Выберите вашу временную зону (часовой пояс).
NTP сервер	Введите адрес NTP-сервера.

NTP синхронизация Введите интервал синхронизации с NTP-сервером.

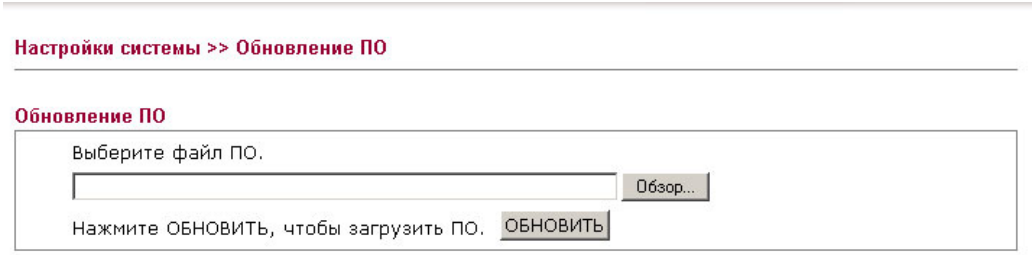
Нажмите OK для сохранения.

3.6.4 Обновление ПО

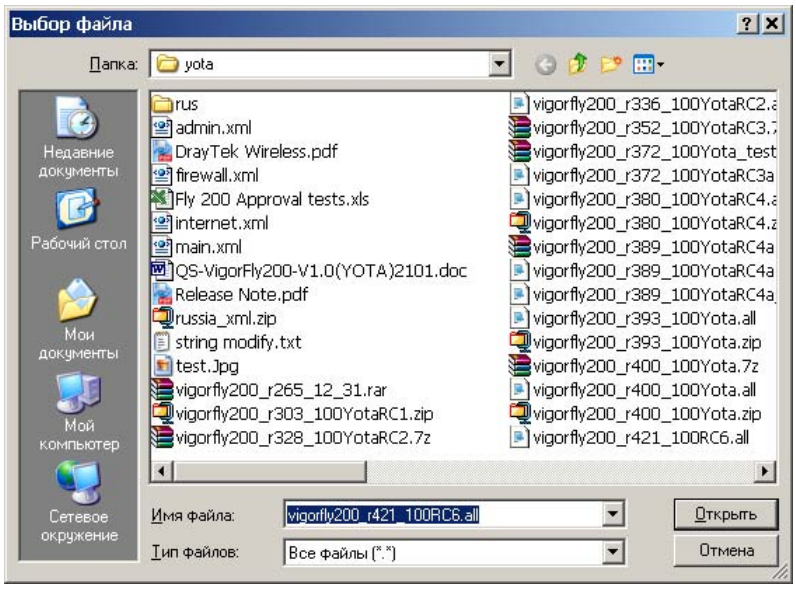
Следующая веб-страница поможет вам обновить ПО. Обратите внимание: этот пример для ОС Windows.

Скачайте новое ПО с сайта DrayTek или с FTP. Сайт DrayTek находится по адресу www.draytek.com, FTP – ftp.draytek.com.

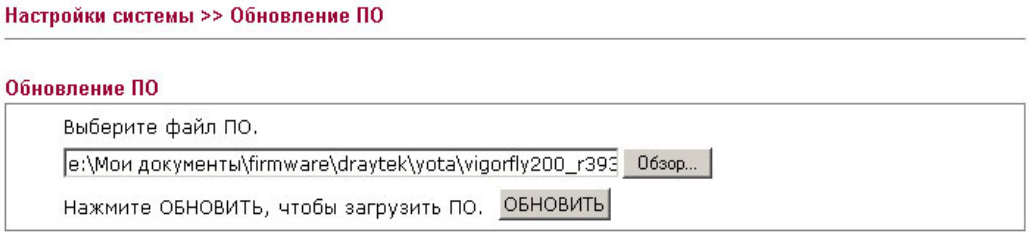
Нажмите **Настройка системы>>Обновление ПО**, чтобы выбрать обновления ПО.



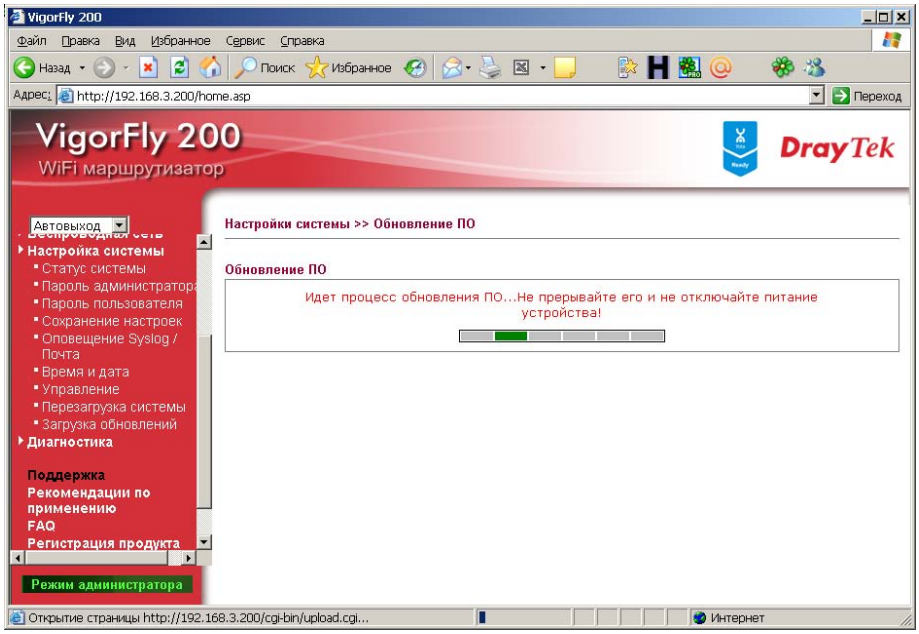
В появившемся окне введите путь к файлу с обновлением ПО и его имя или найдите ПО через файл-менеджер, нажав кнопку **Обзор.** Выберите файл с обновлением ПО и нажмите **Открыть**.



Нажмите кнопку **ОБНОВИТЬ**.

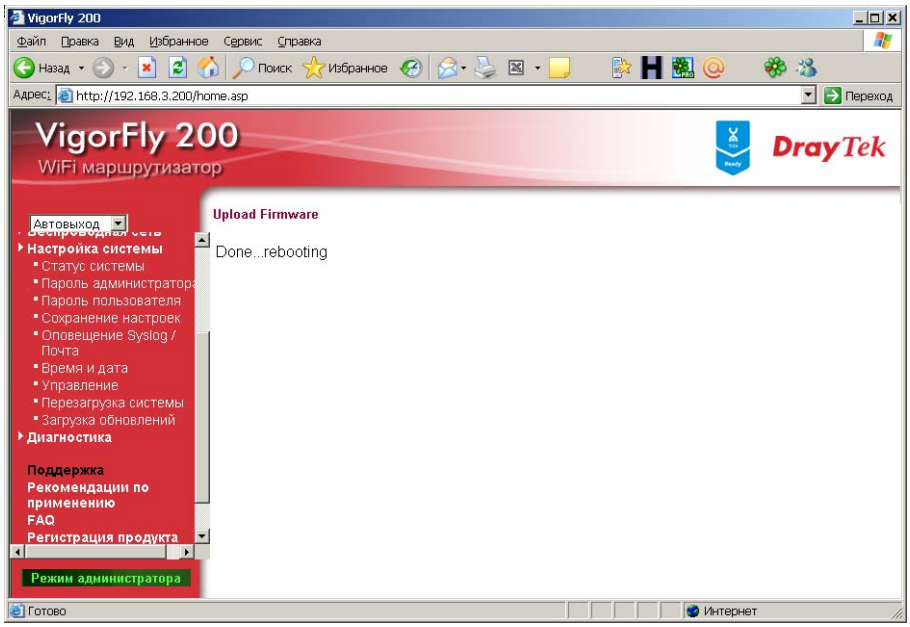


После этого появится следующее сообщение

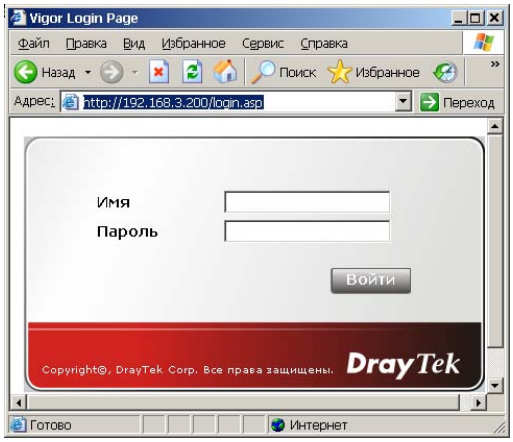


Не выключайте компьютер и маршрутизатор во время процесса обновления.

1. Подождите приблизительно 60 секунд пока происходит обновление ПО.
2. После успешного обновления ПО появится следующее сообщение.



3. Через некоторое время появится приглашение на ввод данных учетной записи. Введите их и нажмите **Войти.**

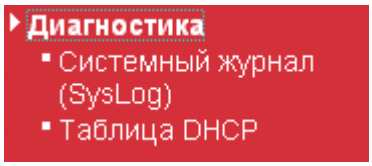


4. В случае успешной идентификации и обновления ПО появится следующее сообщение:

Нажмите OK для продолжения работы.

3.7 **Диагностика**

Функция **Диагностика** предлагает полезный способ проверить статус вашего маршрутизатора. Ниже показано меню **Диагностика.**



3.7.1 Системный журнал (Syslog)

Нажмите **Диагностика>>Системный журнал**, чтобы открыть страницу.

Очистить	Нажмите, чтобы очистить записи.
Обновить	Нажмите, чтобы обновить страницу.

3.7.2 Таблица DHCP

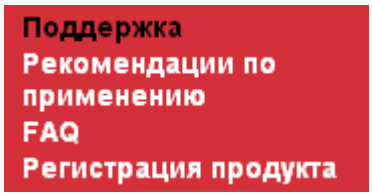
Возможность предоставляет информацию об IP-адресах задач. Эта информация может пригодиться в диагностике сетевых проблем, таких, например, как конфликты IP-адресов.

Нажмите **Диагностика>>Таблица DHCP,** чтобы открыть страницу.

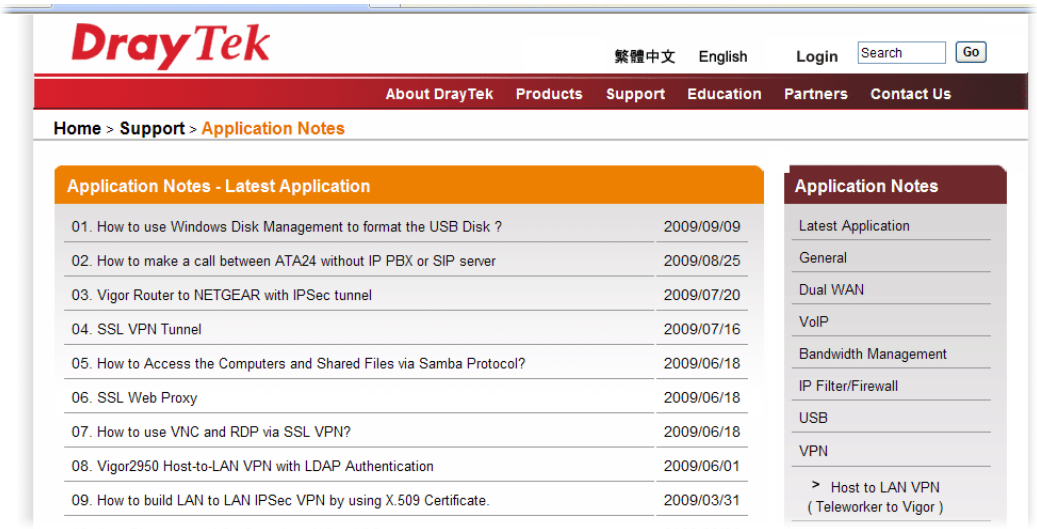
Имя хоста	Отображает имя компьютера, принимающее назначенный IP-адрес этого маршрутизатора.
IP-адрес	Отображает IP-адрес, заданный маршрутизатором для определенного ПК.
MAC-адрес	Отображает MAC-адрес для определенного ПК, которому был назначен IP-адрес DHCP.
Время окончания	Отображает время использования определенного ПК.
Обновить	Нажмите, чтобы обновить страницу.

3.8 Поддержка

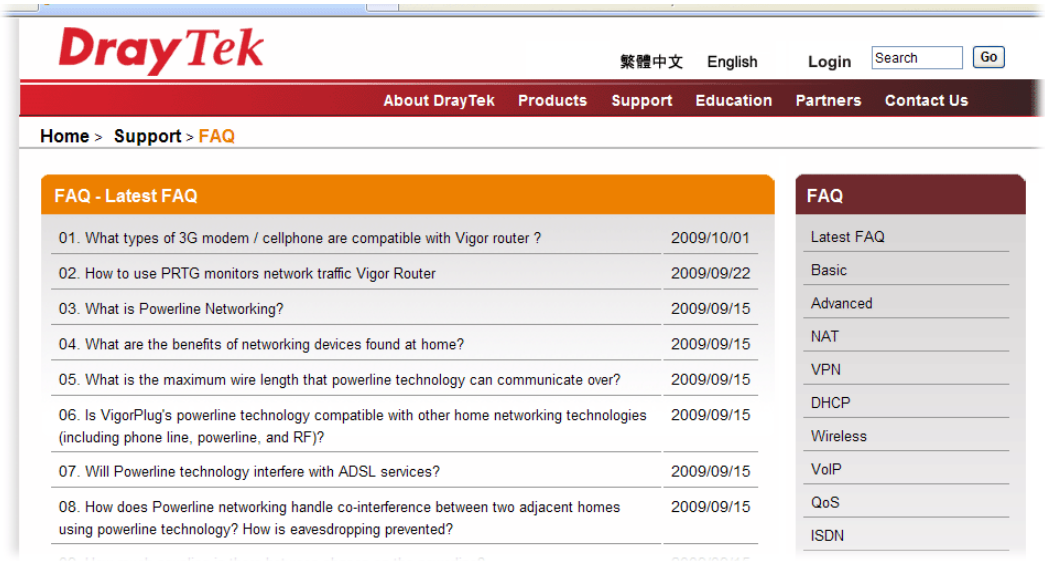
Когда вы выберете какой-либо раздел в меню **Поддержка,** вы будете перенаправлены на соответствующую страницу сайта www.draytek.com.



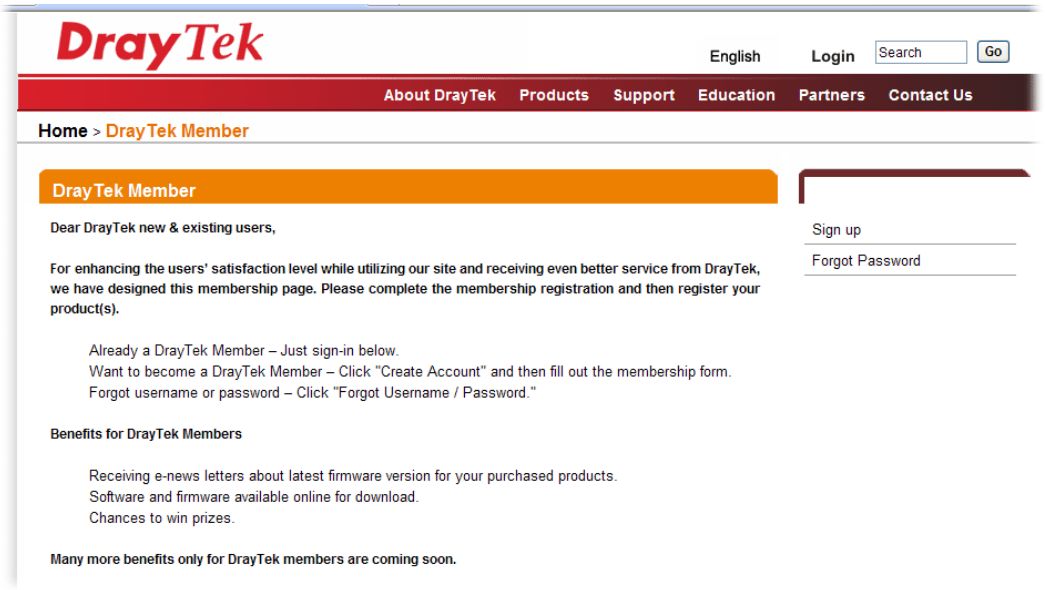
Нажмите **Поддержка>> Рекомендации по применению,** появится следующая страница.



Нажмите **Поддержка>> FAQ,** появится следующая страница.



Нажмите **Поддержка>> Регистрация продукта,** появится следующая страница.

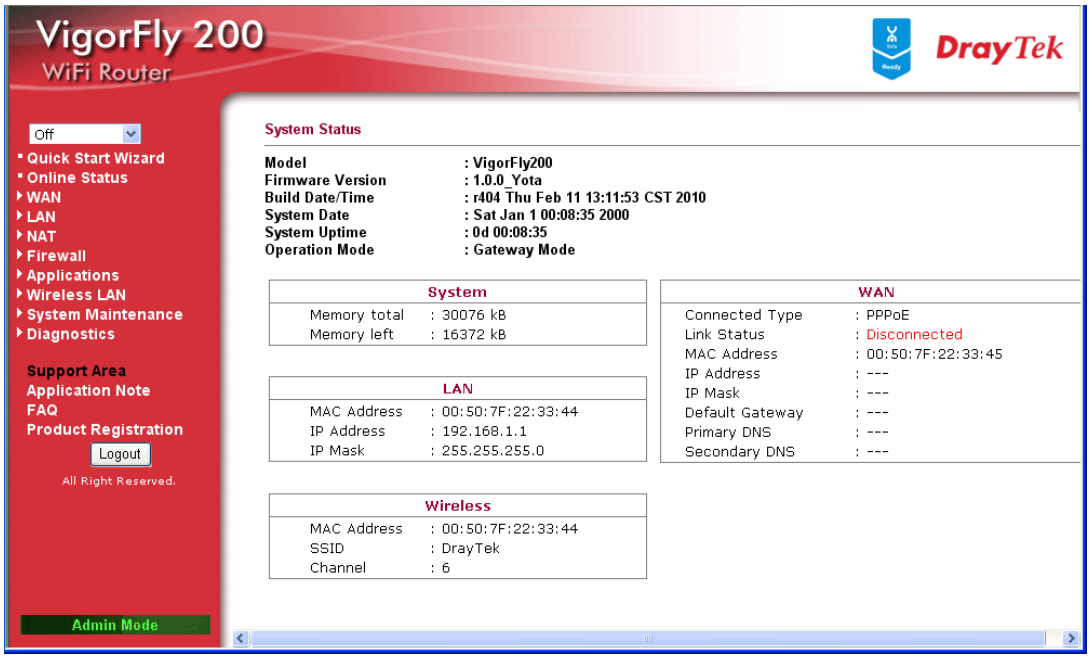


4 Операции в режиме администратора

В этой главе описано изменение сложных (полных) настроек маршрутизатора в режиме администратора.

1. Откройте браузер на вашем компьютере и наберите адрес **http://192.168.1.1**. В следующем окне вас попросят ввести имя пользователя и пароль.
2. Для доступа к режиму администратора введите admin/admin в полях **Имя пользователя/Пароль** и нажмите **Войти**.

Появится следующее окно. В левом нижнем углу будет написано **Режим администратора**.



4.1 WAN

Мастер быстрой настройки позволяет быстро настроить маршрутизатор для подключения.

Основы IP-сетей

IP означает Интернет-протокол. Каждое устройство, включая маршрутизаторы, принт-серверы, компьютеры должно иметь IP-адрес для идентификации положения в сети. Чтобы избежать конфликта адресов, все IP-адреса публично зарегистрированы в Сетевом Информационном Центре (NIC). Уникальные IP-адреса обязательны для всех устройств, представленных в публичных сетях, но не для частных TCP/IP локальных сетей (LAN) (используемых, например, для связи хоста и маршрутизатора, поскольку в данном случае нет необходимости публичного доступа к устройствам). Поэтому NIC зарезервировал определенные адреса, которые никогда не будут публичными. Следующие IP-адреса не являются публичными:

10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

Что такое публичные IP-адреса и частные IP-адреса

Маршрутизатор связывает группы компьютеров, поскольку его главная задача – управлять локальной сетью и защищать ее. Каждый из компьютеров имеет частный IP-адрес, назначенный DHCP-сервером маршрутизатора. Для связи с компьютерами сам маршрутизатор также использует частный IP – 192.168.1.1. В то же время маршрутизатор будет связан с другими сетевыми устройствами посредством публичного IP. При передаче данных функция перевода сетевых адресов (Network Address Translation – NAT) будет переводить публичные/частные адреса и передавать пакеты информации на необходимые компьютеры в локальной сети. Таким образом, все компьютеры будут делить общее Интернет-подключение.

Получение частного IP от провайдера

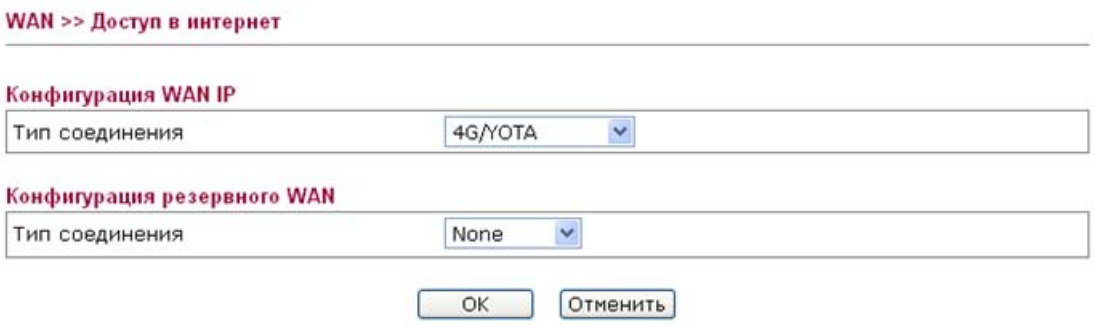
При ADSL-подключении PPP-подтип аутентификации и авторизации необходим для связывания оборудования в помещении клиента (customer premises equipment – CPE). PPPoE подключает сеть через устройство доступа к одному или нескольким концентраторам через удаленный доступ. Реализация этой возможности значительно облегчает использование. В то же время она обеспечивает контроль доступа, биллинг и типы сервиса в соответствии с пожеланиями пользователя.

Когда маршрутизатор начнет подключаться к Интернет-провайдеру, последовательность поисковых действий отправит запрос о подключении. Создастся сессия. Ваш пользовательский ID и пароль будут идентифицированы через **PAP** или **CHAP** с системой идентификации **RADIUS.** А ваш IP-адрес, DNS-сервер и прочая информация будут назначаться вашим провайдером.

Ниже показано меню WAN.

4.1.1 Доступ в Интернет

Эта страница позволит вам настроить конфигурацию WAN в различных режимах. Выберите в выпадающем списке **Тип Подключения** необходимый вам режим работы WAN. Появится следующая страница.



4G/YOTA

Для активации функции WIMAX выберите соответствующий тип подключения.

Конфигурация Если вы хотите настроить резервный WAN для каждого типа, пожалуйста, используйте выпадающий список для

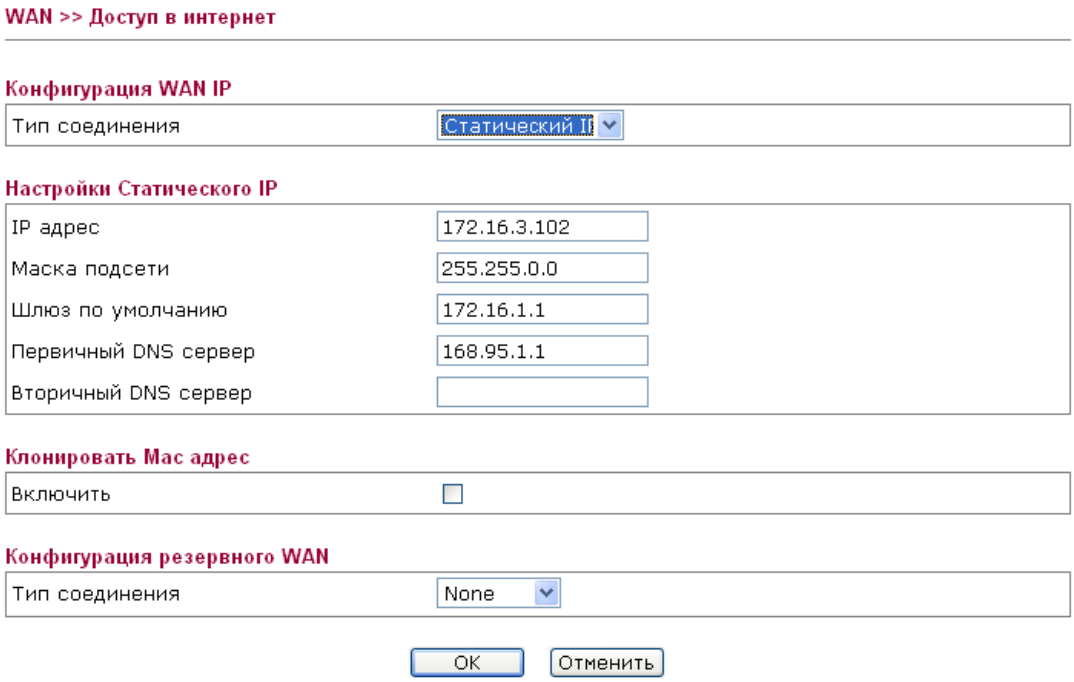
резервного WAN выбора одного из режимов подключения. В зависимости от вашего выбора появятся соответствующие настройки. Детальную информацию о соответствующих настройках параметров вы найдете в соответствующих разделах ниже.

Для установки 4G-подключения не требуется никаких дополнительных настроек. Если вы не хотите настраивать WAN-бэкап, просто нажмите **Далее.**

Статический IP

Вы получите фиксированный публичный IP-адрес или публичную подсеть, то есть набор публичных IP-адресов от вашего провайдера. В большинстве случаев провайдеры, доставляющие интернет с помощью кабеля, предлагают фиксированный адрес, в то время как DSL-провайдеры предлагают подсеть. Если вы используете подсеть, вы можете вписать в соответствующем поле как один, так и несколько IP-адресов.

Чтобы выбрать **статический режим** в качестве протокола доступа, пожалуйста, выберите **Статический IP** в списке типов подключения. Появится следующая страница.



IP-адрес Введите IP-адрес.

Маска подсети Введите маску подсети.

Шлюз по умолчанию Введите IP-адрес шлюза по умолчанию.

Первичный DNS сервер Вам необходимо назначить IP-адрес DNS-сервера. Провайдеры предлагают, как правило, сразу несколько DNS-серверов. Если ваш провайдер не предоставляет их,

маршрутизатор назначит IP DNS-сервера по умолчанию – 198.95.1.1

Вторичный DNS сервер Вы можете выбрать второй IP-адрес DNS-сервера, т.к. провайдеры предлагают, как правило, сразу несколько DNS-серверов. Если ваш провайдер не предоставляет их, маршрутизатор назначит вторичный IP DNS-сервера по умолчанию.

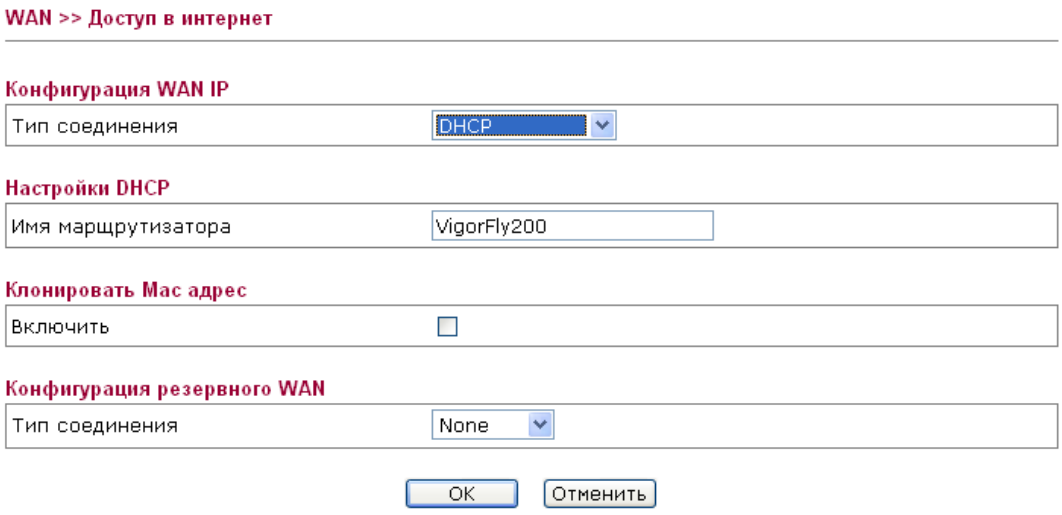
Клонировать MAC-адрес Доступно, если поле **Включить** активировано. Нажмите **Клонировать MAC-адрес.** Маршрутизатор определит MAC-адрес автоматически. Результат будет отображен в поле **MAC-адрес**.

Конфигурация резервного WAN Если вы хотите настроить резервный WAN для каждого типа, пожалуйста, используйте выпадающий список для выбора режима подключения **4G/YOTA**.

После завершения настроек, нажмите **ОК** для сохранения.

DHCP

DHCP позволяет пользователю получить IP-адрес автоматически от DNS-сервера. Если вы выбираете режим DHCP, DHCP-сервер вашего провайдера назначит IP-адрес вашего маршрутизатора автоматически. Вам не нужно устанавливать никаких настроек.



Имя маршрутизатора Введите имя маршрутизатора. Это может быть то же имя, что было использовано в Системном журнале.

Клонировать MAC-адрес Доступно, если поле «Включить» активировано. Нажмите **Клонировать MAC-адрес.** Маршрутизатор определит MAC-адрес автоматически. Результат будет отображен в

поле **MAC-адрес**.

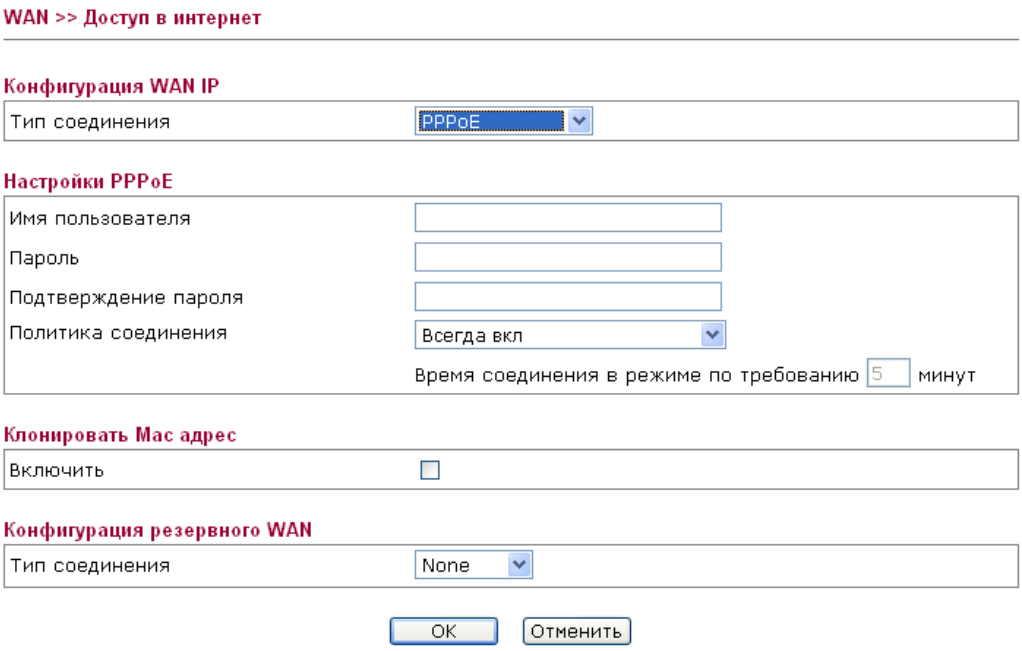
Конфигурация резервного WAN

Если вы хотите настроить резервный WAN для каждого типа, пожалуйста, используйте выпадающий список для выбора режима подключения **4G/YOTA**.

После завершения настроек, нажмите **ОК** для сохранения.

PPPoE

Для выбора протокола PPPoE, пожалуйста, выберите PPPoE в меню **Доступ в Интернет.** Будет показана следующая страница.

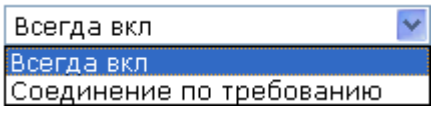


Имя Введите имя, предоставленное вашим провайдером.

Пароль Введите пароль, предоставленный вашим провайдером.

Подтвердите пароль Введите пароль для подтверждения

Политика соединения Вы можете выбрать опцию **Всегда вкл** чтобы сохранять подключение к Интернету всё время. В противном случае выберите **Соединение по требованию.**



Время бездействия – установите время бездействия перед разрывом соединения. Впишите число, если вы выбрали

Соединение по требованию.

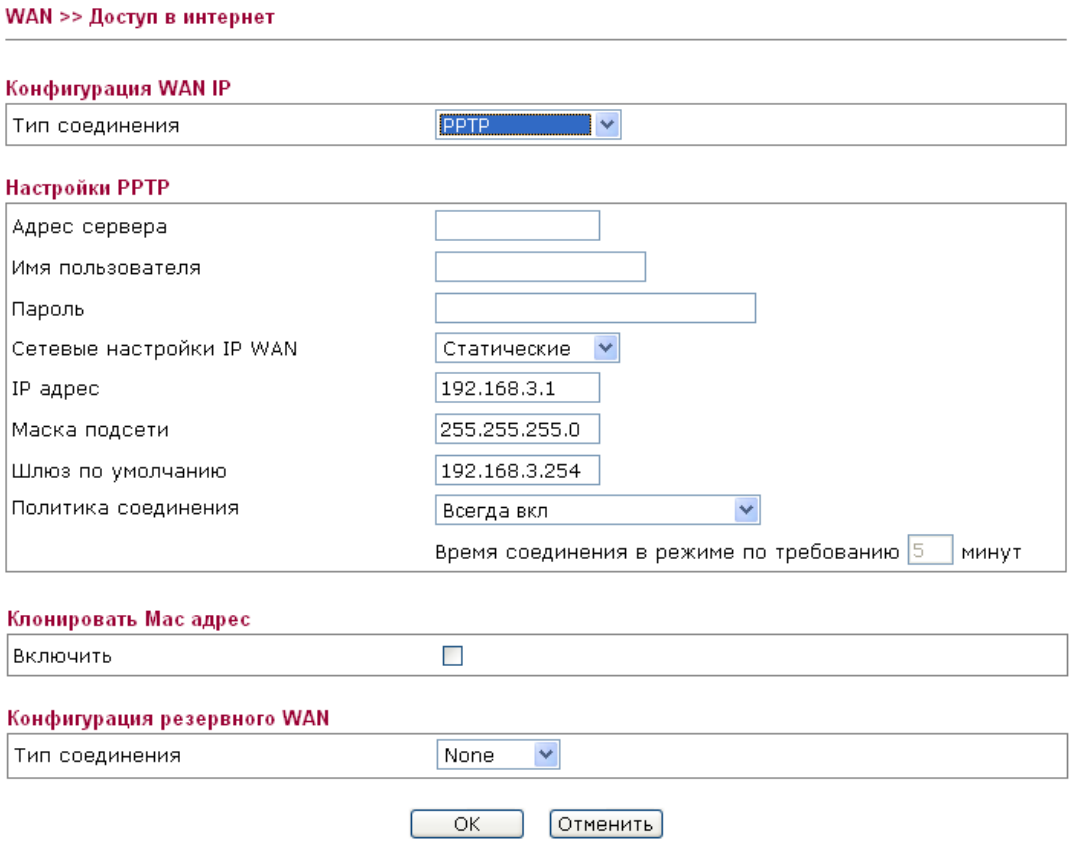
Клонировать MAC-адрес Доступно, если поле **Включить** активировано. Нажмите **Клонировать MAC-адрес.** Маршрутизатор определит MAC-адрес автоматически. Результат будет отображен в поле **MAC-адрес**.

Конфигурация резервного WAN Если вы хотите настроить резервный WAN для каждого типа, пожалуйста, используйте выпадающий список для выбора режима подключения **4G/YOTA**.

После завершения настроек, нажмите **ОК** для сохранения.

PPTP/L2TP

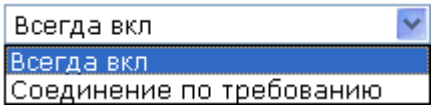
Для выбора протокола **PPTP/L2TP**, пожалуйста, выберите **PPTP/L2TP** в меню **Тип Подключения.** Будет показана следующая страница:



IP-адрес сервера Введите IP-адрес сервера PPTP/L2TP.

Имя Введите имя, предоставленное провайдером.

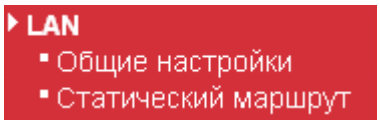
Пароль Введите пароль, предоставленный провайдером.

Адресный режим	Вы можете выбрать **Статический IP** или **DHCP** в качестве настройки IP WAN сети.
IP-адрес	Введите IP-адрес, если вы выбрали статический IP в качестве настройки WAN.
Маска подсети	Введите маску подсети, если вы выбрали статический IP в качестве настройки WAN.
Шлюз по умолчанию	Введите адрес шлюза для этого маршрутизатора.
Политика соединения	Вы можете выбрать опцию **Всегда вкл** чтобы сохранять подключение к Интернету всё время. В противном случае выберите **Соединение по требованию.**  **Время бездействия –** установите время бездействия перед разрывом соединения. Впишите число, если вы выбрали **Соединение по требованию.**
Клонировать MAC-адрес	Доступно, если поле **Включить** активировано. Нажмите **Клонировать MAC-адрес.** Маршрутизатор определит MAC-адрес автоматически. Результат будет отображен в поле **MAC-адрес**. 

После завершения настроек, нажмите **ОК** для сохранения.

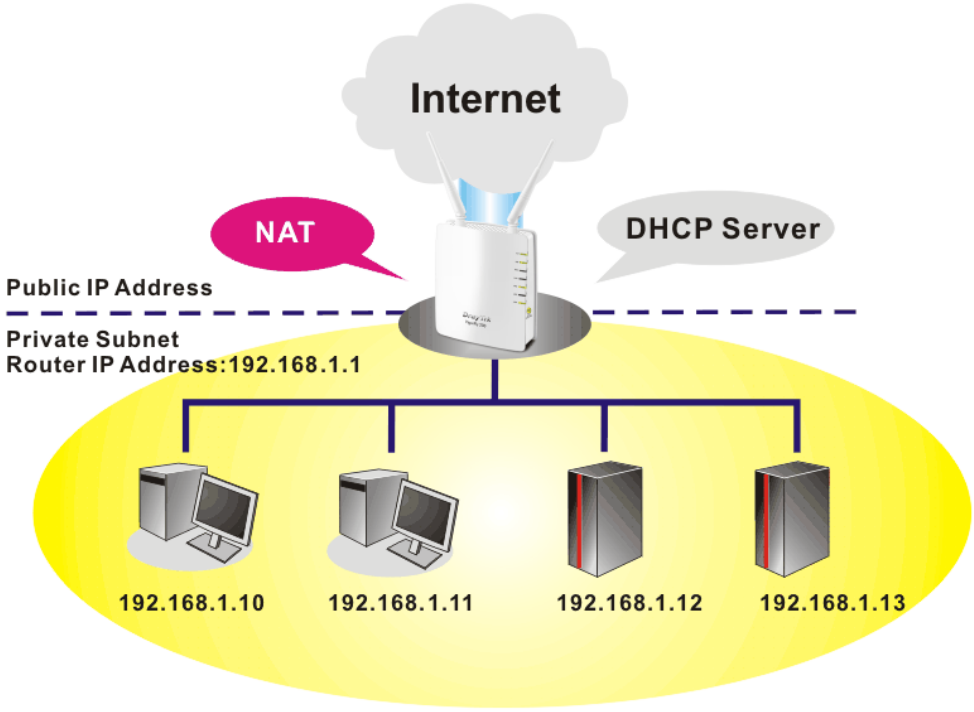
4.2 LAN

Локальная вычислительная сеть LAN (Local Area Network) – это группа подсетей, регулируемых и управляемых маршрутизатором. Структура сети зависит от типа публичного IP, предоставляемого вашим провайдером.

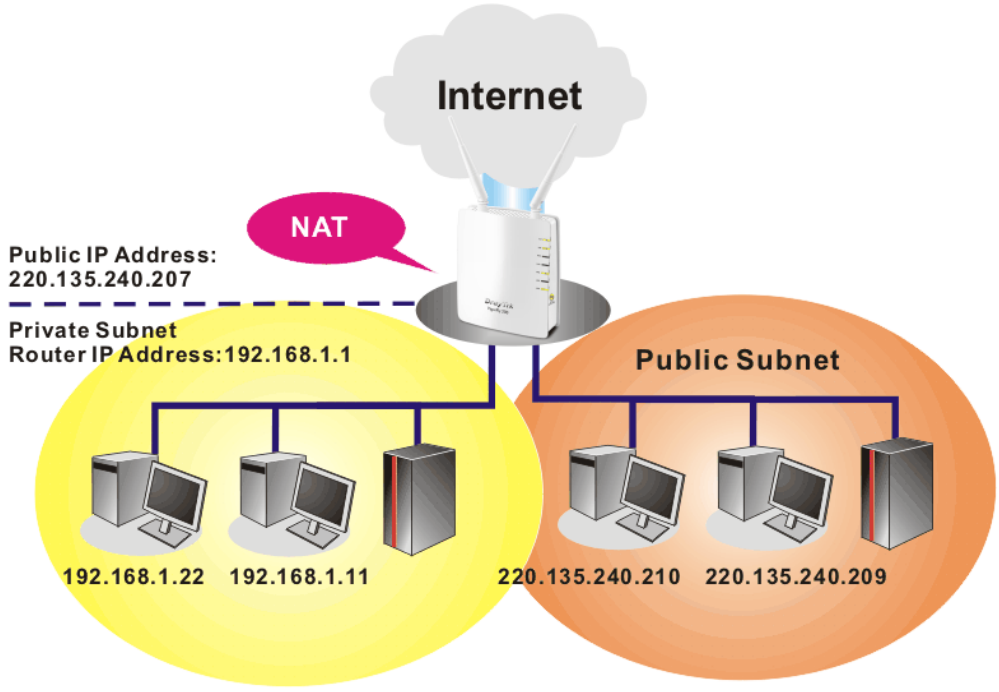


Основы LAN

Наиболее характерная функция маршрутизатора Vigor состоит в преобразовании сетевых адресов. Он создает вашу собственную частную подсеть. Как уже было сказано, маршрутизатор использует публичные IP-адреса для связи с Интернетом и частные IP для локальных устройств. Функция NAT пересылает пакеты информации из публичных IP в частные и обратно, отправляя пакеты к нужным хостам. Кроме того, маршрутизатор имеет встроенный DHCP-сервер, который назначает частные IP-адреса для всех локальных устройств. Следующая диаграмма показывает принцип работы маршрутизатора.



В некоторых случаях, у вас может быть публичный IP-адрес подсети от вашего провайдера вида 220.135.240.0/24. Это значит, что вы можете установить публичную подсеть или обратиться ко второй подсети, где каждый хост будет иметь публичный IP-адрес. Как часть публичной подсети, маршрутизатор Vigor будет служить для IP-маршрутизации, чтобы помочь хостам в публичной подсети передавать информацию другим публичным хостам или внешним серверам. Поэтому маршрутизатор должен быть установлен как шлюз для публичных хостов.



Что такое протокол RIP?

Чтобы улучшить свою работу, маршрутизатор Vigor будет обмениваться информацией о маршрутизации с соседними маршрутизаторами, используя протокол RIP (Routing

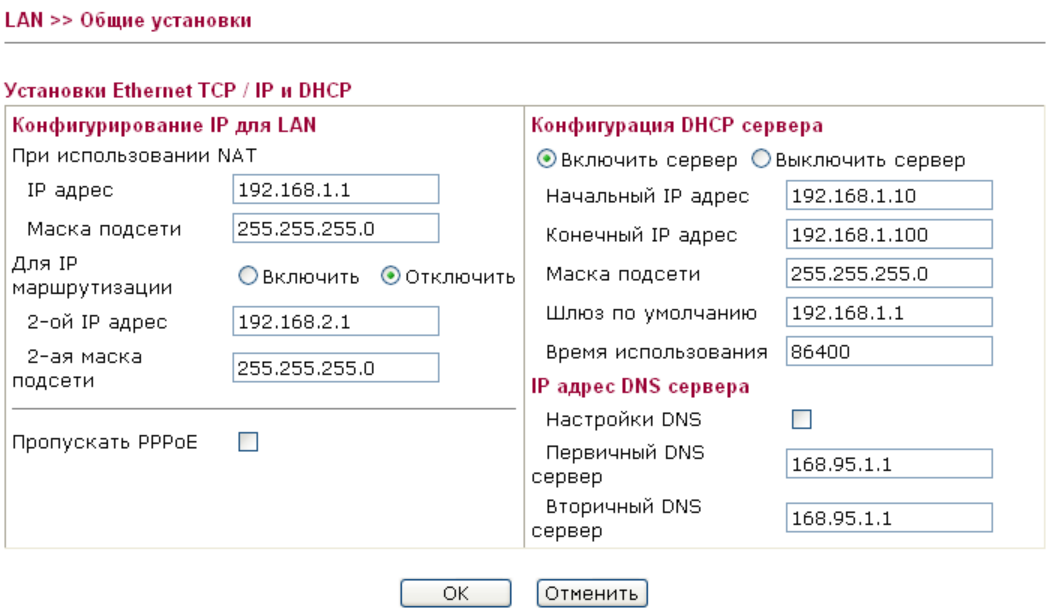
Information Protocol). Это позволяет пользователям обмениваться такой информацией, как IP-адреса; маршрутизаторы будут автоматически информировать друг друга.

Что такое статическая маршрутизация?

Когда у вас есть несколько подсетей в LAN, иногда более эффективным и быстрым способом подключения является функция **Статической маршрутизации.** Вам надо просто установить правила пересылки данных с одной назначенной подсети на другую без RIP.

4.2.1 Общие настройки

На этой странице указаны основные настройки LAN. Нажмите **LAN**, чтобы открыть настройки LAN и выберите **Общие настройки**.



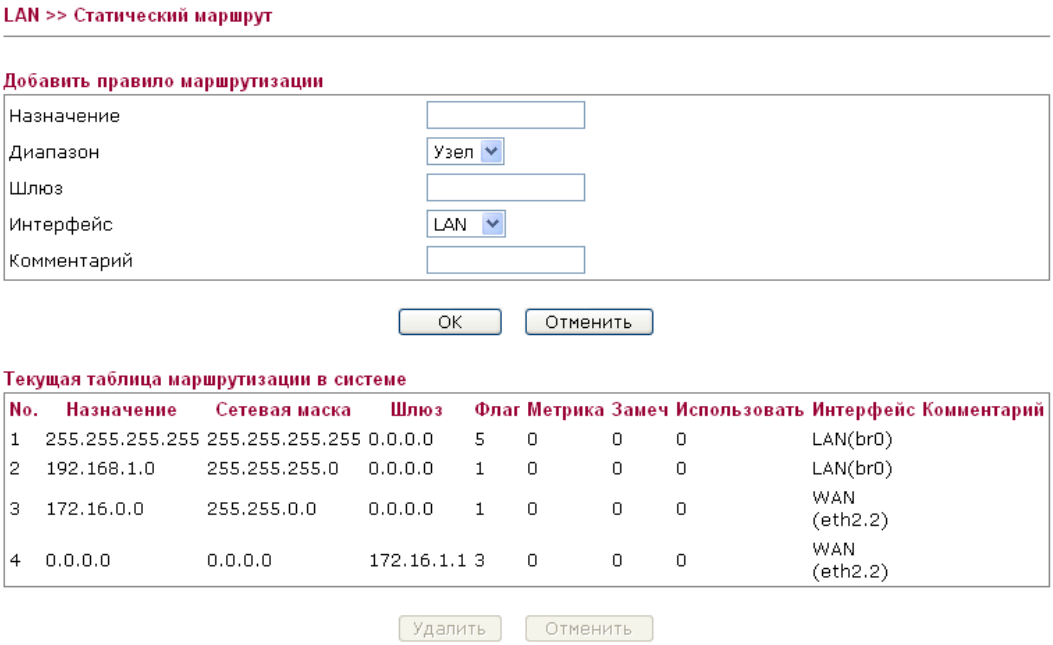
IP-адрес	Введите частный IP-адрес для подключения к локальной частной сети (по умолч: 192.168.1.1).
Маска подсети	Введите маску, которая определит размеры сети (по умолч: 255.255.255.0)
Для IP маршрутизации	Отметьте, чтобы активировать функцию. По умолчанию отключено.
2-ой IP адрес	Введите вторичный IP-адрес для подключения к подсети (по умолч: 192.168.2.1).
2-ая маска подсети	Введите маску, которая определит размеры сети.
Подключения PPPoE	Если вы хотите использовать сетевой PPPoE-сервер посредством маршрутизатора, поставьте галочку, чтобы перенаправить PPPoE-пакеты в назначенное место.
Конфигурация DHCP сервера	DHCP это протокол динамической конфигурации узла. Маршрутизатор служит DHCP-сервером вашей сети, поэтому он автоматически отправляет связанные IP-настройки любому локальному пользователю-клиенту DHCP. Рекомендуется оставить маршрутизатор в качестве DHCP-сервера, если вы не имеете другого DHCP-сервера.

	Если вы хотите использовать другой DHCP-сервер в сети, Relay Agent поможет вам перенаправить DHCP-запрос в назначенное место.
Включить сервер	Маршрутизатор автоматически раздаст IP-адреса хостам.
Выключить сервер	Вы можете назначить IP-адреса хостов самостоятельно.
Начальный IP адрес	Введите начальный IP-адрес. Если 1-й адрес маршрутизатора 192.168.1.1, следующий будет 192.168.1.2 или больше, но меньше, чем 192.168.1.254.
Конечный IP адрес	Введите конечный IP-адрес.
Маска подсети	Введите маску, которая определит размеры сети (по умолч: 255.255.255.0/24).
Шлюз по умолчанию	Введите шлюз по умолчанию для DHCP-сервера. Это число всегда то же, что и 1й IP-адрес маршрутизатора, что означает, что маршрутизатор – шлюз по умолчанию.
Время использования	Вы можете установить время использования назначенного компьютера.
Ручная настройка DNS	Если эта функция включена, сетевые компьютеры будут использовать первичный и вторичный DNS-серверы как свои DNS-серверы. В противном случае сетевые компьютеры используют в качестве DNS-сервера маршрутизатор и маршрутизатор создаст им прокси.
Первичный DNS сервер	Вам необходимо назначить IP-адрес DNS-сервера. Провайдеры предлагают, как правило, сразу несколько DNS-серверов. Если ваш провайдер не предоставляет их, маршрутизатор назначит IP DNS-сервера по умолчанию – 194.109.6.66.
Вторичный DNS сервер	Вы можете выбрать второй IP-адрес DNS-сервера, т.к. провайдеры предлагают, как правило, сразу несколько DNS-серверов. Если ваш провайдер не предоставляет их, маршрутизатор назначит вторичный IP DNS-сервера по умолчанию – 194.98.0.1. Если оставить незаполненными оба поля, маршрутизатор назначит IP-адреса локальным пользователям, как DNS-прокси сервер и будет поддерживать DNS-кэш. Если IP адрес домена уже в DNS-кэше, маршрутизатор переназначит доменное имя. В противном случае маршрутизатор перенаправляет очередь пакетов DNS на внешний DNS-сервер, установив WAN-подключение (напр. DSL/кабельное).

После завершения настроек, нажмите **OK** для сохранения.

4.2.2 Статическая маршрутизация

Зайдите в LAN, чтобы открыть страницу настроек и выберите **Статическая маршрутизация**. Это поможет маршрутизатору описать единственный способ определения пути маршрутизатора в сети.



Назначение — Введите IP-адрес для примененных правил маршрутизации.

Диапазон — Выберите **Узел** или **Сеть** для назначения шлюза или сетевой маски, установленной для данного правила маршрутизации.

Сетевая маска — Введите сетевую маску для правила маршрутизации, если вы выбираете **Сеть** в качестве настройки **Назначение**.

Шлюз — Введите адрес шлюза для данного правила маршрутизации.

Интерфейс — Выберите WAN или LAN в качестве интерфейса для данной маршрутизации.

Комментарий — Введите комментарий для напоминания о данном правиле маршрутизации.

OK — Нажмите для сохранения настроек и их отображения на таблице маршрутизатора.

Отменить — Нажмите, чтобы очистить текущие настройки.

4.3 NAT

Обычно маршрутизатор служит в качестве устройства NAT. NAT – это механизм, с помощью которого один или несколько частных IP-адресов могут быть преображены в один публичный. Публичный IP-адрес, как правило, назначен провайдером. Частные IP распознаются только внутренними хостами.

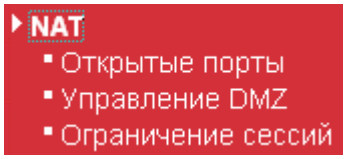
Когда исходящие пакеты, предназначенные для какого-либо публичного сервера, достигают NAT маршрутизатора, маршрутизатор поменяет адрес источника на публичный IP-адрес этого маршрутизатора, выберет доступный публичный порт и затем перенаправит его. При этом маршрутизатор сохранит информацию и адрес/порт, использованные при этом подключении. Когда публичный сервер отвечает, входящий трафик, разумеется, будет предназначен для публичного IP, но маршрутизатор перенаправит данные, основываясь на сохраненных данных. По этой причине внутренние и внешние узлы могут поддерживать связь.

Среди преимуществ NAT:

- **Экономия на стоимости аренды публичных IP** и эффективное использование IP-адресов. NAT переводит внутренние IP-адреса локальных хостов в публичные IP-адреса, так что множество внутренних хостов сможет работать посредством всего лишь одного IP-адреса.
- **Улучшение безопасности внутренних сетей, скрытие IP-адресов.** Есть много жертв атак на основе IP-адреса. Поскольку злоумышленнику не могут быть известны какие-либо из частных адресов IP, функция NAT может защитить внутреннюю сеть.

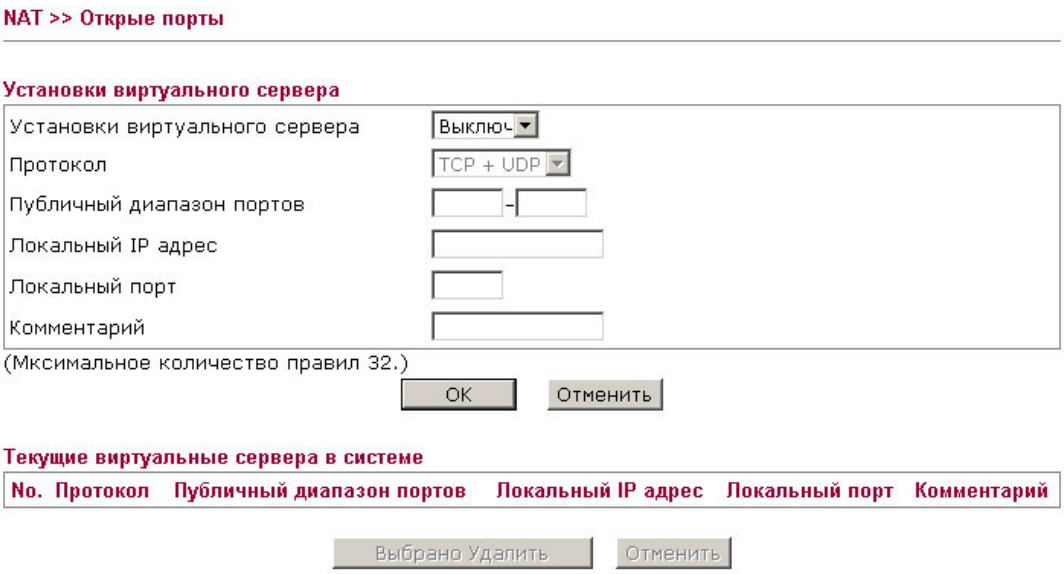
На странице NAT вы увидите частный IP-адрес, определенный в RFC-1918. Обычно мы используем подсети 192.168.1.0/24 для маршрутизатора. Как отмечалось ранее, функция NAT может назначить один или несколько IP-адресов и / или сервис-портов для разных сервисов. Иными словами, функция NAT также выполняется в случае использования метода назначения портов.

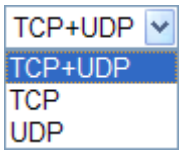
Ниже показано меню NAT.



4.3.1 Открытые порты

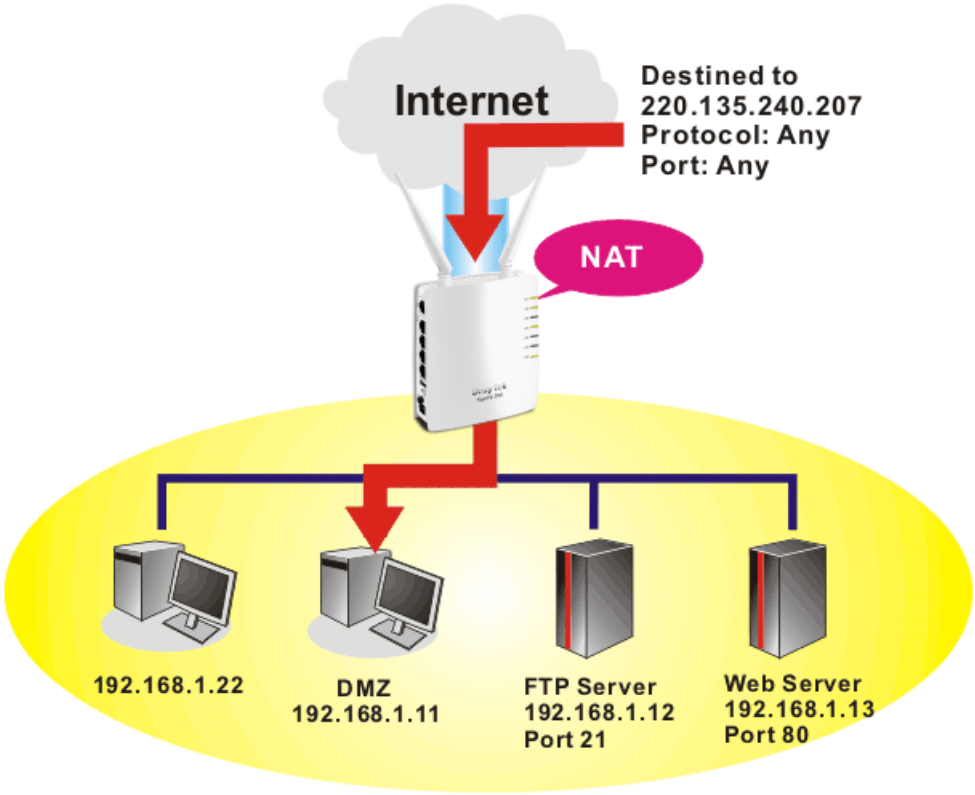
Открытые порты позволяют вам открыть несколько портов для трафика специальных приложений. Обычно их используют P2P-приложения (напр., BT, KaZaA, Gnutella, WinMX, eMule и др.), веб-камера и проч. Убедитесь в том, что вы используете последние версии приложений, чтобы у вас не возникло проблем с системой безопасности.



Установки виртуального сервера	Выберите Активировать, чтобы включить эту настройку.
Протокол	Определите протоколы транспортного уровня: **TCP**, **UDP** или **TCP+UDP**. 
Публичный диапазон портов	Определите начальный и конечный номер портов для сервиса, предлагаемого локальным хостом.
Локальный IP адрес	Введите частный IP локального хоста.
Локальный порт	Если функция настроена, трафик будет привязан в этому порту локального хоста.
Комментарий	Введите слова извещения для виртуального сервера.
OK	Когда вы завершите настройки, нажмите на эту кнопку, чтобы сохранить изменения и отобразить поле **Текущие виртуальные сервера в системе**
Отмена	Нажмите, чтобы очистить последние настройки.
Удалить	Нажмите, чтобы удалить настройки выбранного виртуального сервера.

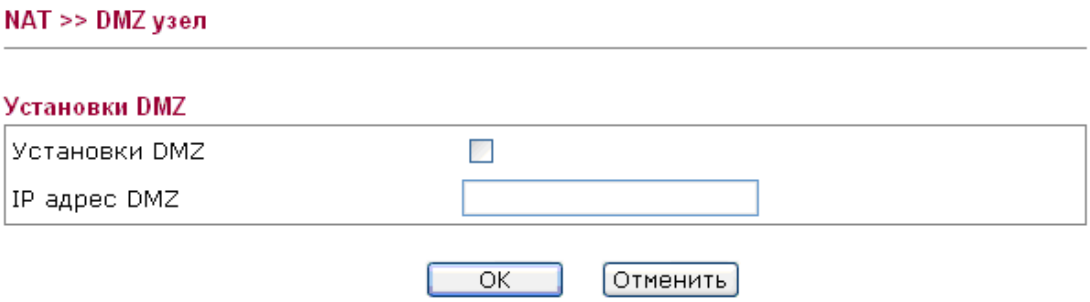
4.3.2 Узел DMZ

Как было сказано выше, **переадресация портов** может перенаправить входящий TCP/UDP или другой трафик с определенных портов на назначенный частный IP-адрес/порт узла в сети. Однако другие порты IP, например 50-й (ESP) и 51-й (AH), не могут быть перенаправлены. Маршрутизатор Vigor предлагает возможность создания узла **DMZ**, который запишет ВСЕ незатребованные данные по любым протоколам на один хост в LAN. Обычные действия других клиентов в Интернете продолжат работать без каких-либо прерываний связи. Узел DMZ позволяет определенному внутреннему пользователю быть полностью открытым, что бывает необходимо при работе некоторых приложений, напр. Netmeeting или Интернет-игр.



Примечание: настройки безопасности NAT будут в известной степени ослаблены при настройке узла DMZ. Мы предлагаем вам добавить дополнительные фильтры или второй брандмауэр.

Нажмите **Управление DMZ**, чтобы открыть следующую страницу:



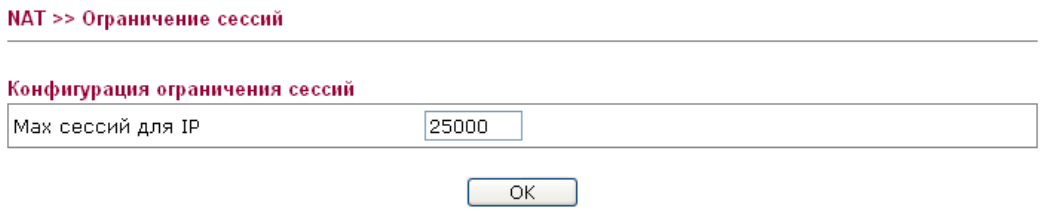
Установки DMZ Кликните, чтобы активировать функцию узла DMZ.

IP адрес DMZ Введите частный IP для узла DMZ.

OK	Нажмите, чтобы сохранить настройки.
Отмена	Нажмите, чтобы очистить последние настройки.

4.3.3 Ограничение сессий

Компьютер с частным IP-адресом получает доступ к Интернету через NAT-маршрутизатор. Маршрутизатор создает записи NAT-сессий для такого подключения. P2P (Peer to Peer) приложения (напр., BitTorrent) постоянно требуют открытия множество сессий для своей работы. При этом на каждую сессию выделяются ресурсы системы, при большом количестве сессий ресурсов может не хватать, и это будет сказываться на общей производительности системы. Чтобы решить данную проблему, используйте ограничение сессий для определенных узлов.



Пожалуйста, определите приемлемое количество сессий для маршрутизатора. Если вы ничего не введете в этом поле, система использует значение ограничения сессий по умолчанию (25000).

4.4 Сетевой экран (брандмауэр, firewall)

Основные понятия о сетевом экране

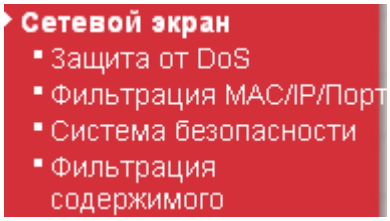
Поскольку пользователи широкополосных сетей требуют все большего количества информации для мультимедиа, интерактивных приложений и дистанционного обучения, важной задачей стало обеспечение безопасности работы в Интернете. Сетевой экран маршрутизатора предлагает средства защиты вашей локальной сети от атак неавторизованных пользователей. Он также ограничивает доступ в Интернет пользователей локальных сетей. Кроме того, он может отфильтровывать определенные пакеты, которые могут заставить маршрутизатор установить нежелательное подключение.

Защита от DoS

Защита от DoS помогает определить и смягчить последствия DoS-атак. Атаки, как правило, бывают двух типов: «переполнение» и обнаружение уязвимых мест. При атаках типа «переполнение» (flooding-type) пытаются использовать ресурсы системы целиком, в то время как при точечных ударах (vulnerability) пытаются парализовать систему, действуя на уязвимые места протокола или операционной системы.

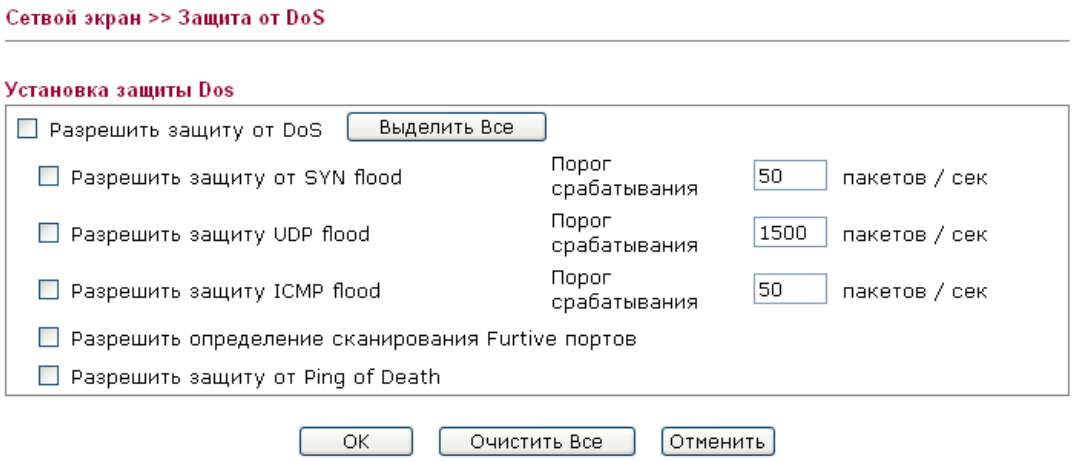
Функция **Защита от DoS** позволяет маршрутизатору проверять каждый входящий пакет, основываясь на данных базы знаний об атаках. В защищенной сети маршрутизатором будет блокироваться каждый подозрительный пакет, который будет пытаться парализовать хост с помощью непрерывного самокопирования. При этом если вы включите функцию записи в Системный журнал (SysLog), то в журнал будут записываться предупреждения о подозрительных пакетах. Маршрутизатор Vigor так же следит за трафиком. Любой подозрительный пакет данных, несоответствующий предустановленным значениям (например, превышает пороговую величину), будет расценен как признак атаки. В этом случае маршрутизатор активирует свой защитный механизм, чтобы немедленно ограничить или прервать прием подозрительных пакетов.

Ниже показано меню **Сетевой экран.**



4.4.1 Защита от DoS

Существуют 5 видов обнаружения/защиты в настройках **Защита от DoS.** По умолчанию функция выключена. Нажмите **Сетевой экран** и выберите **Защита от DoS,** чтобы открыть страницу настроек.

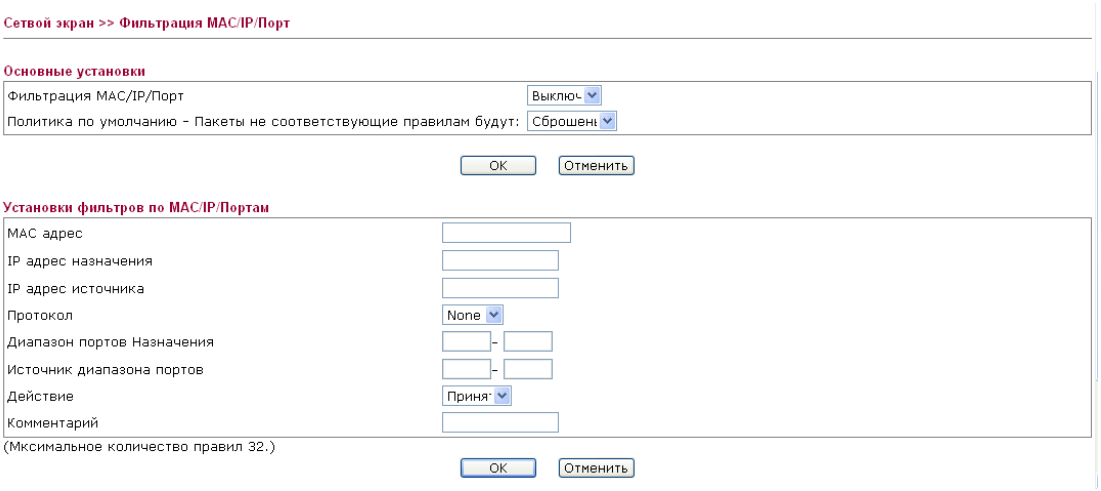


Разрешить защиту от DoS	Галочка – чтобы активировать функцию.
Разрешить защиту от SYN flood	Поставьте галочку, чтобы активировать защиту от SYN-потока. Как только маршрутизатор обнаружит поток TCP SYN пакетов из Интернета, превышающий допустимый порог, маршрутизатор будет в течение заранее определенного времени в случайном порядке отказываться от приема последующих TCP SYN пакетов. Цель состоит в том, чтобы не дать входящим пакетам исчерпать все системные ресурсы. По умолчанию допустимый порог составляет 50 пакетов в секунду, время отказа – 10 секунд.
Разрешить защиту UDP flood	Поставьте галочку, чтобы активировать защиту от UDP-потока. Как только маршрутизатор обнаружит поток UDP пакетов из Интернета, превышающий допустимый порог, маршрутизатор будет в течение заранее определенного времени в случайном порядке отказываться от приема последующих UDP пакетов. По умолчанию допустимый порог составляет 150 пакетов в секунду, время отказа – 10 секунд.
Разрешить защиту ICMP flood	Поставьте галочку, чтобы активировать защиту от ICMP-потока. Как только маршрутизатор обнаружит поток ICMP-пакетов из Интернета, превышающий допустимый порог, маршрутизатор будет в течение заранее определенного времени в случайном порядке

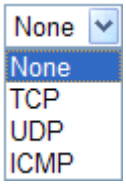
	отказываться от последующих эхо-запросов ICMP. По умолчанию допустимый порог составляет 50 пакетов в секунду, время отказа – 10 секунд.
Разрешить определение сканирования Furtive портов	Атака Port Scan атакует маршрутизатор посредством отправки большого количества пакетов на множество разных портов, чтобы обнаружить сервисы, которые ответят на запрос. Кликните, чтобы активировать определение атак Port Scan. В случае определения подобной атаки, маршрутизатор отправит предупреждение.
Разрешить защиту от Ping of Death	Поставьте галочку, чтобы активировать функцию Block Ping of Death. В случае такой атаки злоумышленник отправляет перекрывающие пакеты на определенные хосты; хосты зависают, поскольку они начинают восстанавливать свои пакеты. Маршрутизатор блокирует любые пакеты, пытающиеся осуществить этот тип атаки.
OK	Нажмите, чтобы сохранить настройки.
Очистить все	Нажмите, чтобы очистить все настройки на странице.
Отменить	Нажмите, чтобы отменить текущую операцию.

4.4.2 Фильтрация MAC/IP/Port

Эта страница позволяет вам установить до 32 правил фильтрации MAC/IP/Port. Когда вы закончите настройки, просто нажмите **OK**. Новые правила будут отображены здесь:



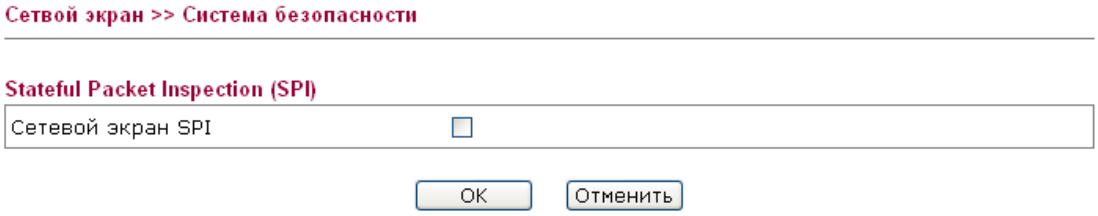
Фильтрация MAC/IP/Port	Выберите **Включить**, чтобы активировать функцию.
Политика по умолчанию	**Приняты** – все пакеты, которые не соответствуют правилу, будут приняты. **Сброшены** – все пакеты, которые не соответствуют правилу, будут блокированы.
MAC-адрес	Введите MAC-адрес узла.
IP адрес назначения	Введите IP адрес назначения для применения этого правила.

Источник IP адресов	Введите Источник IP адресов для применения этого правила.
Протокол	Определите протокол(ы), к которому(-ым) будет применяться это правило. 
Диапазон портов Назначения	Определите Диапазон портов Назначения.
Источник диапазона портов	Определите Источник диапазона портов.
Действие	**Приняты** – все пакеты, которые соответствуют правилу, будут приняты. **Сброшены** – все пакеты, которые соответствуют правилу, будут блокированы.
Комментарий	Введите описания настроек фильтров. Максимально допустимая длина – 23 знака.
OK	Нажмите, чтобы сохранить настройки.
Отменить	Нажмите, чтобы отменить текущую операцию.

4.4.3 Система безопасности

Stateful Packet Inspection (SPI) это архитектура сетевого экрана, которая работает на сетевом уровне. В отличие от статической пакетной фильтрации, которая проверяет пакеты, основываясь на информации в их заголовках, SPI создает механизм проверки подключений, которая фиксирует все подключения на сетевом экране и проверяет их работу. Полноценный сетевой экран маршрутизатора не только проверяет информацию по заголовкам, но также следит за состоянием подключения.

Поставьте галочку в следующем поле и нажмите **OK,** чтобы активизировать SPI сетевой экран для фильтрации входящих и исходящих пакетов.



4.4.4 Фильтрация содержимого

Фильтр веб-контента

Все мы знаем, что содержимое Интернета временами может быть недопустимым к просмотру для некоторых категорий лиц. Будучи ответственным родителем или работодателем, вы должны защищать своих подопечных от возможной опасности или пустого времяпровождения. С функцией веб-фильтрации маршрутизатора Vigorfly200 вы можете защитить свой бизнес от угроз, связанных с производством, юридической

ответственностью, сетями и безопасностью. Родители могут оградить своих детей от просмотра веб-страниц или чатов для взрослых.

После активации функции Веб-фильтрации маршрутизатора VigorFly 200 и составления категорий запрещенных веб-сайтов, каждый запрошенный Интернет-адрес (напр., www.bbc.co.uk) будет проверяться по базе знаний, размещенной на специализированном сервере. База знаний обновляется ежедневно международной командой энтузиастов. Сервер проверит адрес сайта и отправит категорию сайта на ваш маршрутизатор. Затем маршрутизатор, исходя из выбранных вами ограничений, решит, можно ли открыть запрашиваемую страницу. Данный процесс никак не влияет на скорость подключения и открытия Интернет-страниц, потому что каждая база знаний может выдерживать миллионы запросов о категоризации сайтов.

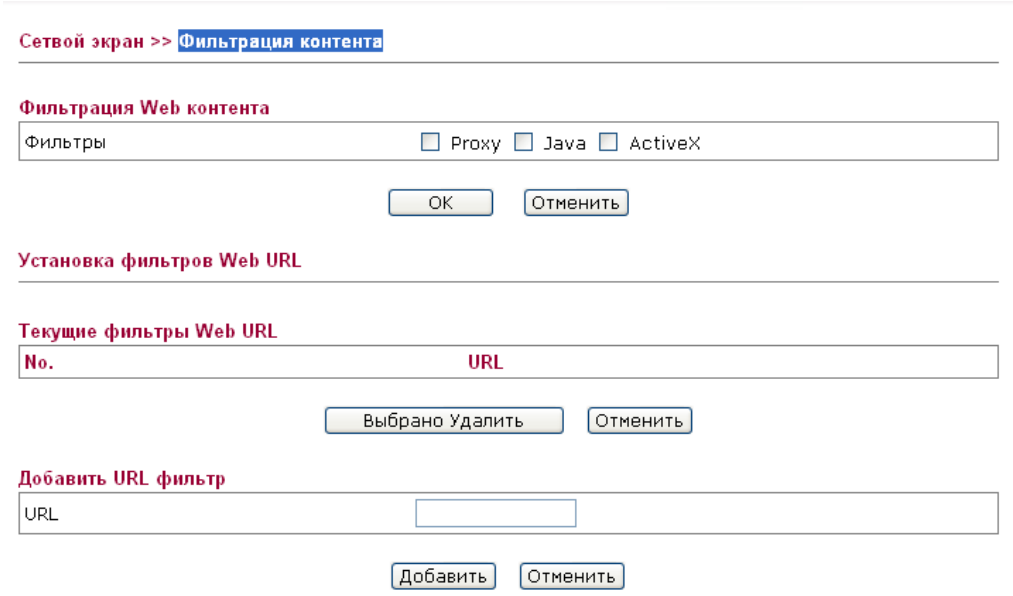
Контент-фильтр URL

Маршрутизатор VigorFly200 также оснащен контент-фильтром URL – не только для того, чтобы ограничить нелегальный входящий/исходящий трафик с недопустимых Интернет-страниц, но также и для того, чтобы запретить веб-приложения, запуск которых может вызвать исполнение вредоносного кода.

После того, как пользователь введет ссылку с нежелательными ключевыми словами (или кликнет по таковой), функция блокировки URL по ключевым словам отклонит HTTP запрос этой веб-страницы. Таким образом, можно ограничить доступ пользователя к сайту. **Фильтрация содержимого URL** работает как хорошо обученный продавец магазина, который никогда не продаст подросткам журналы для взрослых. В офисах **фильтр содержимого URL** используется для создания ориентированной на работу Интернет-среды – что позволяет увеличить эффективность работы. Почему фильтр содержимого URL работает в области фильтрации лучше, чем традиционный брандмауэр? Потому что фильтр проверяет строки URL или некоторые данные HTTP, скрывающиеся в содержании TCP пакетов, в то время как брандмауэр проверяет пакеты, основываясь исключительно на проверке заголовков TCP / IP.

С другой стороны, маршрутизатор VigorFly 200 может предотвратить случайную загрузку вредоносных программ с веб-страниц. Очень часто вредоносные коды скрываются в исполняемых объектах, таких как: ActiveX, Java Applet, в сжатых файлах и прочих исполняемых файлах. Скачав подобные типы файлов с веб-сайтов, вы рискуете навредить системе. Например, объект управления ActiveX обычно используется в интерактивных веб-приложениях. Если внутри содержится вредоносный код, он перенесется на систему пользователя.

Для настройки функции откройте **Сетевой экран>> Фильтрация содержимого** для доступа к следующей странице.

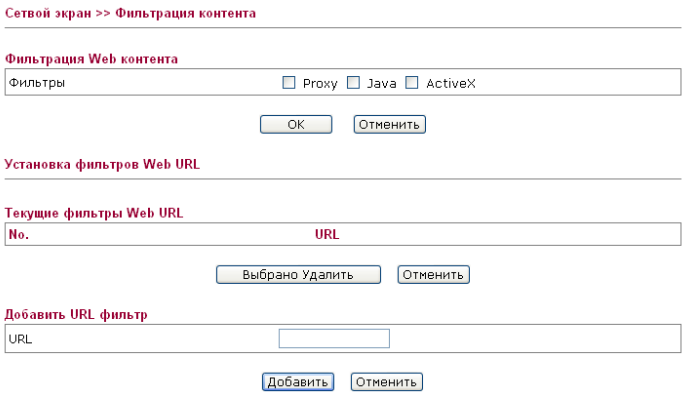


Фильтрация Web-контента

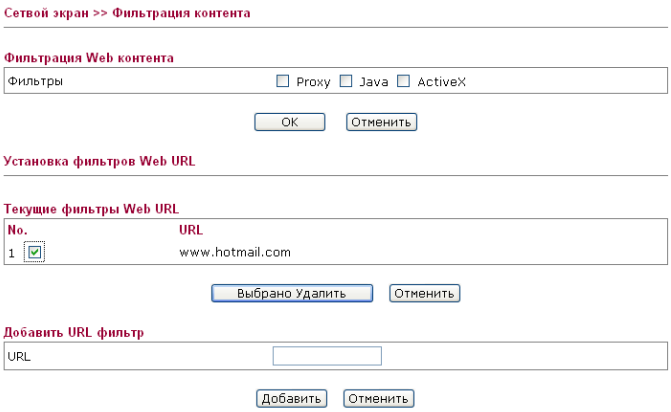
В настоящий момент вам предлагается только три типа контент-фильтров. Выберите Proxy, Java или ActiveX и нажмите **OK**. Система будет фильтровать и блокировать веб-страницы в соответствии с вашими предпочтениями.

Установка фильтров Web URL

URL – введите адрес веб-сайта в строке URL и нажмите **Добавить.** Новая ссылка с заданным URL появится на странице. Система будет фильтровать и блокировать веб-страницы в соответствии с вашими предпочтениями.

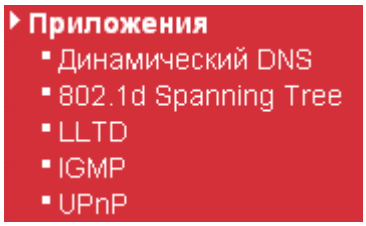


Чтобы удалить URL-настройки, просто кликните по нужной ссылке и нажмите кнопку **Удалить.**



4.5 Приложения

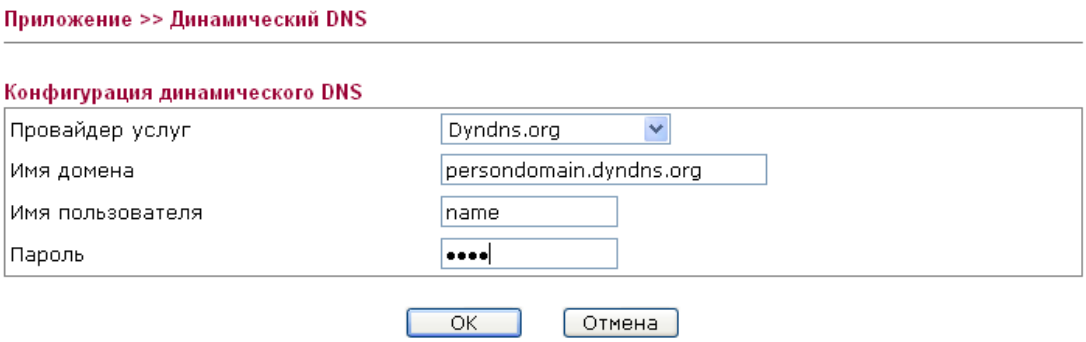
Ниже показано меню Приложения.



4.5.1 Динамический DNS

Провайдер часто предоставляет динамический IP-адрес, когда вы подключаетесь к Интернету через провайдера. Это значит, что публичный IP, назначенный для вашего маршрутизатора, меняется каждый раз, когда вы подключаетесь к Интернету. Функция **Динамического DNS** позволяет вам назначить доменное имя для динамического IP WAN. Функция позволяет маршрутизатору обновлять его метки онлайн IP-адреса WAN назначенного динамического DNS-сервера. Когда маршрутизатор будет подключен, у вас будет возможность использовать зарегистрированное доменное имя, чтобы получить доступ к маршрутизатору или внутреннему виртуальному серверу из Интернета. Это особенно полезная функция, если вы выступаете хостом веб-сервера, FTP-сервера или других серверов позади маршрутизатора.

Перед использованием функции динамического DNS вы должны зарегистрироваться у какого-либо поставщика услуг DDNS. Маршрутизатор позволяет использовать три учетных записи для трех различных провайдеров сервиса DDNS. Маршрутизатор Vigor совместим с DDNS-сервисами наиболее популярных провайдеров, таких как: **www.dyndns.org, www.no-ip.com, www.dtdns.com, www.changeip.com, www.dynamic-nameserver.com.** Вы должны посетить их веб-сайты, чтобы зарегистрировать доменное имя.

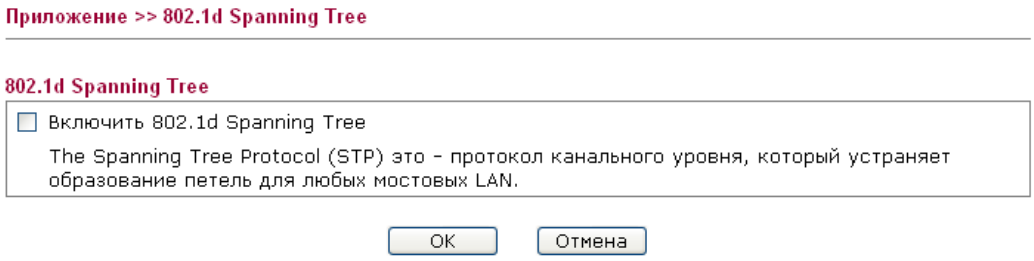


Провайдер услуг	Выберите имя сервис-провайдера для DDNS-аккаунта. Если вы выбираете **Нет,** функция будет отключена.
Имя домена	Введите доменное имя, которое вы использовали ранее. Используйте «выпадающий список», чтобы выбрать нужный домен.
Имя пользователя	Введите имя, которое вы настроили для использования домена.
Пароль	Введите пароль.
OK	Кликните, чтобы сохранить и применить настройки.

После завершения настроек, нажмите OK для их активации.

4.5.2 802.1d Spanning Tree

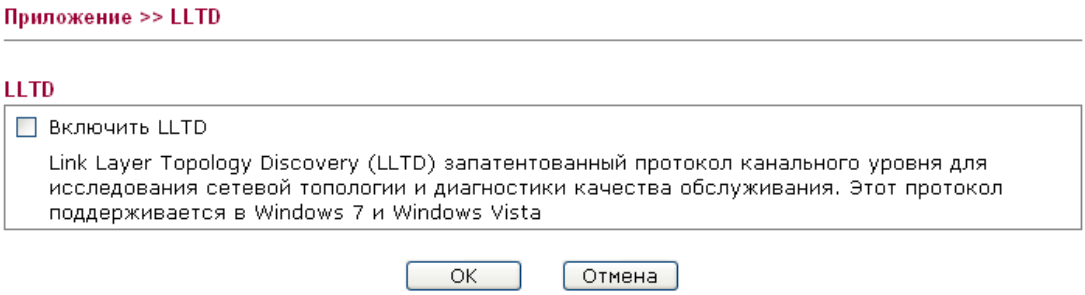
Spanning Tree Protocol (STP) – это протокол канального уровня, который устраняет образование петель для любых мостовых LAN.



Включить 802.1d Spanning Tree	Поставьте галочку, чтобы включить функцию.
OK	Кликните, чтобы сохранить и применить настройки.

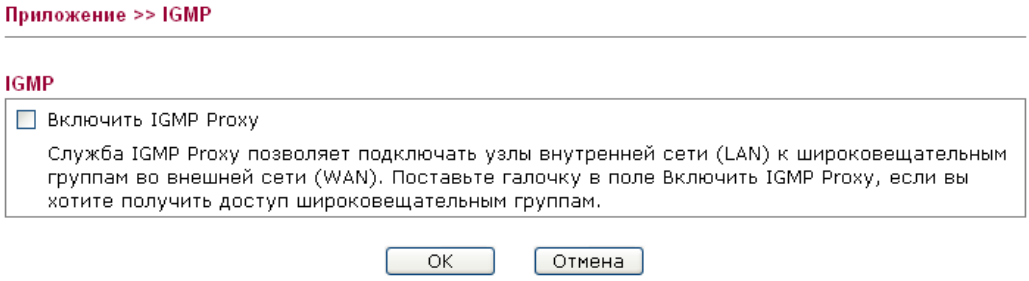
4.5.3 LLTD

Link Layer Topology Discovery (LLTD) – запатентованный протокол канального уровня для исследования сетевой топологии и диагностики качества обслуживания. Этот протокол поддерживается в Windows 7 и Windows Vista.



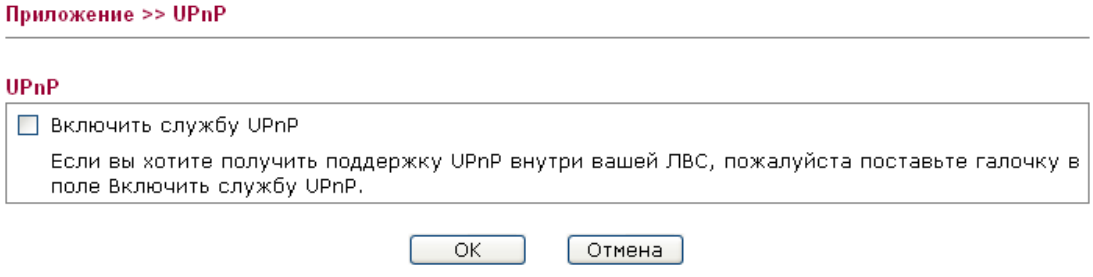
4.5.4 IGMP

IGMP это аббревиатура для *Internet Group Management Protocol*. Это связующий протокол, который в основном используется для управления в многоадресных группах.



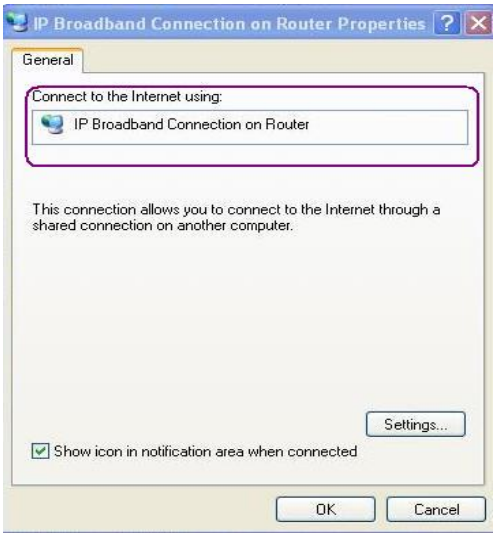
4.5.5 Конфигурация UPnP

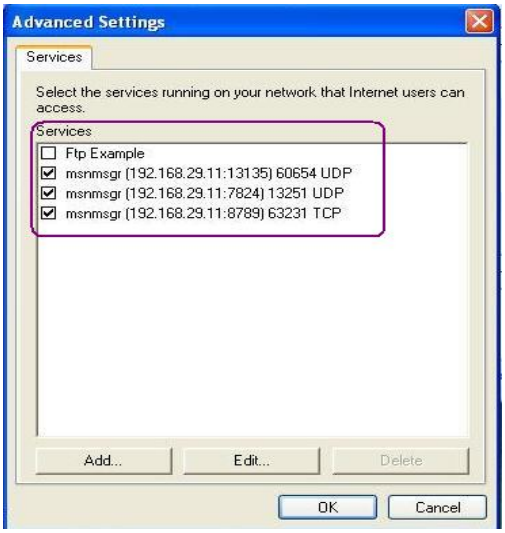
Протокол **UPnP** (Universal Plug and Play) используется, чтобы облегчить установку и настройку сетевых устройств. Легкая настройка доступна для подключенных напрямую периферийных устройств с существующей системой Windows 'Plug and Play'. Для NAT маршрутизаторов главной особенностью UpnP является функция NAT Traversal. Она позволяет приложениям внутри брандмауэра автоматически открывать порты, которые им необходимы для прохождения через маршрутизатор. Это более надежно, чем режим, в котором порты открываются маршрутизатором. Кроме того, пользователю не нужно вручную создавать список портов или DMZ. UPnP доступен в ОС Windows XP; маршрутизатор обеспечивает поддержку программы MSN Messenger, так что пользователи смогут общаться не только с помощью сообщений, но так же и с помощью голоса и видеосвязи.



После активации функции **Включить UPnP,** иконка **Широкополосное IP-подключение через Маршрутизатор** появится в разделе **Сетевые подключения**. Статус подключения и контроль статуса будут доступны для активации. NAT Traversal UPnP позволяют работать мультимедиа приложениям. Для этого нужно вручную установить список портов или использовать другие похожие методы. Скриншоты показывают эту особенность.

UpnP-возможность маршрутизатора позволяет таким UpnP приложениям как MSN Messenger обнаруживать то, что они размещены позади NAT маршрутизатора. Приложение также установит внешний IP-адрес и настроит список портов маршрутизатора. Впоследствии такой механизм перенаправит пакеты от внешних портов маршрутизатора на внутренние порты, используемые приложением.





Напоминание о брандмауэре и UPnP

Не может работать с брандмауэром

Работающие приложения брандмауэра могут стать причиной неправильной работы функции UPnP. Это происходит из-за того, что приложения будут блокировать возможность доступа к некоторым сетевым портам.

Вопросы безопасности

Из-за активированной функции UPnP в вашей сети могут возникнуть угрозы безопасности. Вы должны оценить риски, прежде чем активировать функцию.

- В некоторых операционных системах Microsoft были обнаружены недостатки UPnP, поэтому убедитесь, что вы установили все последние пакеты обновлений и исправлений.

- Непривилегированные пользователи могут контролировать некоторые функции маршрутизатора, в том числе удаление и добавление портов.

Функция UPnP динамически добавляет списки портов от имени некоторых UPnP-совместимых приложений. Если происходит аварийное завершение приложения, отметки об этих портах не могут быть удалены.

4.6 **Беспроводная** LAN

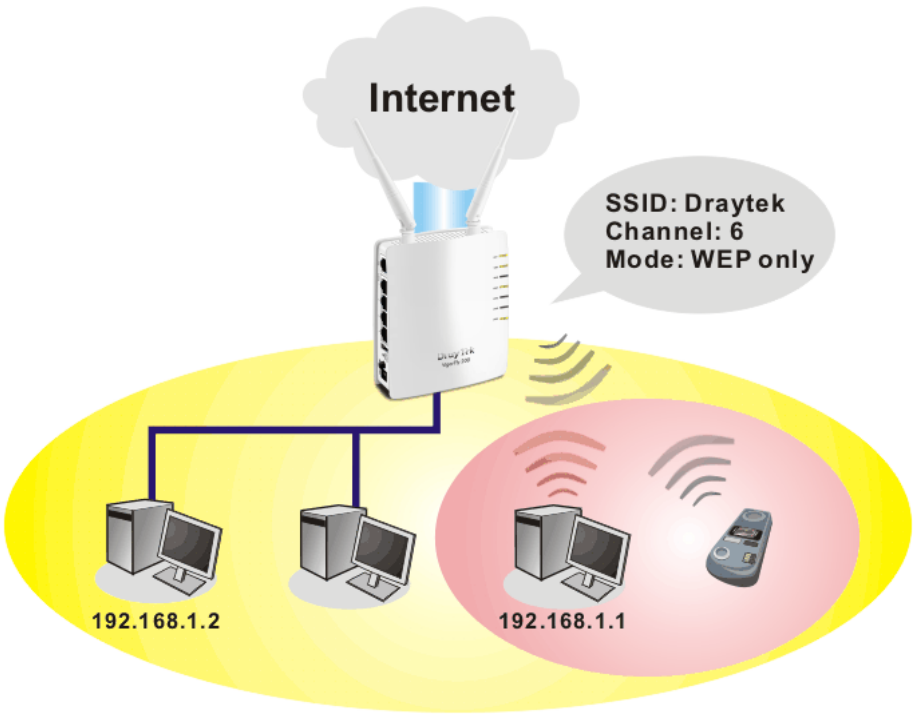
4.6.1 Основные принципы

В последние годы произошел огромный рост рынка беспроводной связи. Беспроводные технологии сейчас доступны практически в каждом уголке планеты. Сотни миллионов людей сегодня обмениваются информацией с помощью беспроводных устройств связи. Маршрутизатор Vigor создан для эффективной работы в маленьком офисе или дома. Теперь сотрудникам компаний достаточно принести в переговорную комнату всего лишь один ноутбук, в то время как раньше приходилось прокладывать сетевые кабели или сверлить в стенах отверстия. Беспроводная сеть обеспечивает высокую мобильность – так что пользователи WLAN могут одновременно получать доступ как к Интернету, так и к LAN (как если бы это была проводная связь).

Беспроводные маршрутизаторы Vigor оснащены беспроводным LAN интерфейсом, работающим вместе со стандартом IEEE 802.11n draft 2. Чтобы улучшить его мощность, маршрутизатор оснащен специальной беспроводной технологией, позволяющей повысить скорость передачи данных до 300 Мбит/с*. Поэтому у вас никогда не возникнет проблем с потоковой передачей музыки или видео.

Примечание: * Скорость передачи данных может отличаться в зависимости от условий в сети и факторов среды, включая сетевой трафик, используемые материалы перегородок.

В режиме инфраструктуры маршрутизатор играет роль точки доступа, к которой подключаются беспроводные клиенты. Все беспроводные клиенты будут делить одно Интернет-подключение. Раздел меню **Основные настройки** позволит вам настроить параметры беспроводной сети, включая ее SSID, частотный канал и проч.



Обзор безопасности

Шифрование оборудования в реальном времени: маршрутизатор Vigor оснащен системой шифрования AES, и может усилить защиту вашей информации, не оказывая влияния на пользовательские операции.

Полный выбор стандартов безопасности: чтобы вы могли быть уверенными в безопасности и в секретности ваших беспроводных подключений, мы предлагаем вам несколько стандартов безопасности.

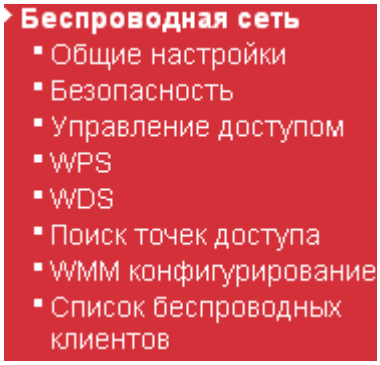
WEP (Wired Equivalent Privacy) – это унаследованный метод шифрования с использованием 64-битного или 128-битного ключа каждого передаваемого по радио пакета. Обычно точка доступа назначит набор из четырех ключей и привяжет их к каждой станции, используя только один ключ из четырех.

WPA (Wi-Fi Protected Access), наиболее доминирующий механизм безопасности в индустрии, делится на две категории: WPA-персональный или называемый WPA-Заранее заданные ключи (WPA Pre-Share Key – WPA/PSK), и WPA-предприятие или WPA/802.1x.

В WPA-персональном во время передачи данных для шифрования используются заранее заданные ключи. WPA запрашивает временный протокол целостности ключа (TKIP) для шифрования данных, в то время как WPA2 запрашивает AES. WPA-предприятие сочетает шифрование с аутентификацией.

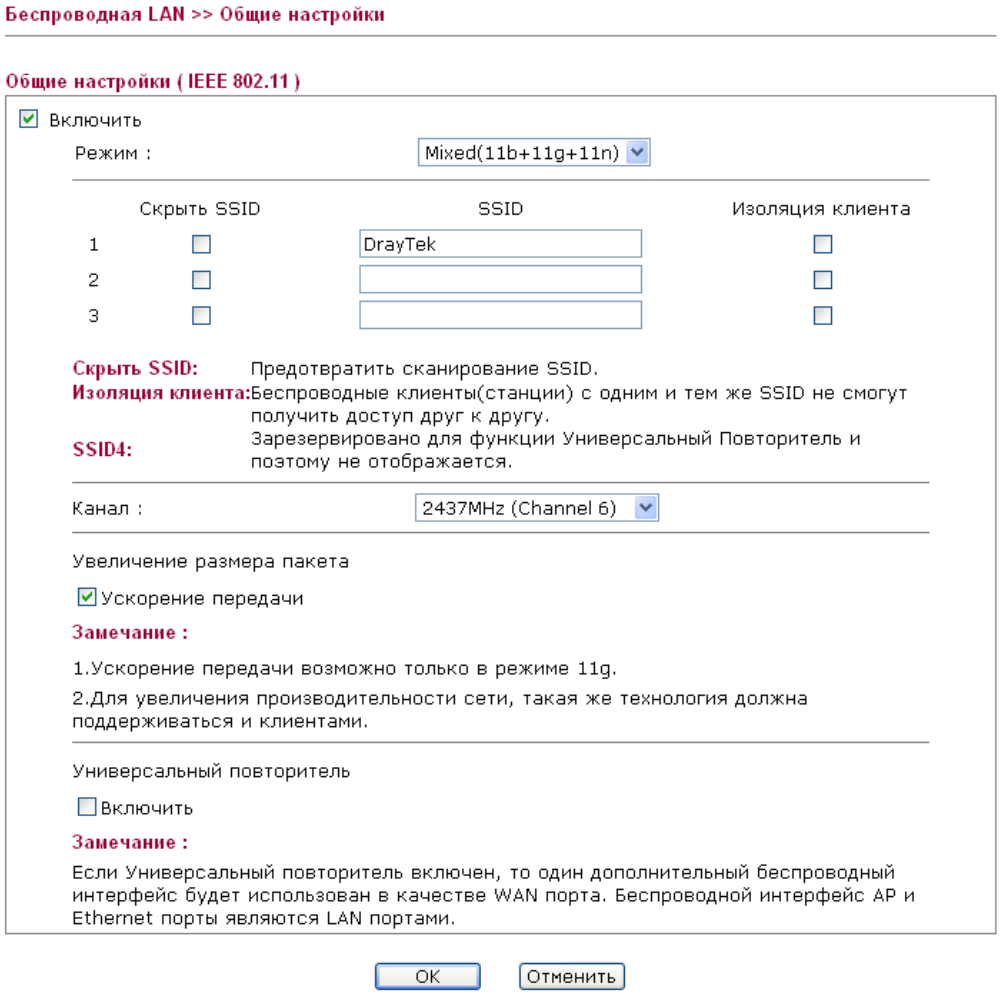
Поскольку была подтверждена уязвимость системы WEP, мы советуем вам выбрать WPA для наиболее защищенного подключения. Вы должны выбрать механизм защиты по вашим потребностям. Неважно, какую систему безопасности вы выберете, все они усиливают защиту беспроводной передачи данных и/или увеличивают секретность вашей беспроводной сети. Беспроводной маршрутизатор Vigor гибок и может одновременно поддерживать множество защищенных подключений как с WEP, так и с WPA.

Ниже показано меню **Беспроводная сеть**.



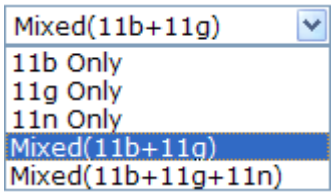
4.6.2 Общие настройки

При нажатии **Общие настройки** появится новая веб-страница, на которой вы сможете задать SSID, выбрать частотный канал и настроить другие параметры сети.



Включить — Поставьте галочку, чтобы активировать функцию.

Режим — В настоящий момент маршрутизатор может подключаться к Смешанной (Mixed) (11b+11g), только 11g, только 11b, только 11n и Смешанной (Mixed) (11b+11g+11n) станциям одновременно. Выберите режим Mixed (11b+11g+11n).



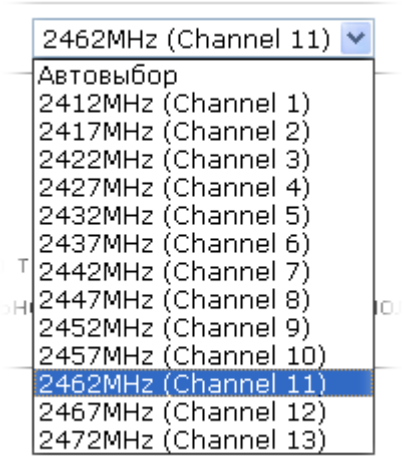
Скрывать SSID — Отметьте, чтобы предотвратить подключения неавторизованных клиентов или STA к вашей беспроводной LAN. В зависимости от маршрутизатора, пользователь может видеть всю информацию кроме SSID или вообще не может видеть информацию о маршрутизаторе во время обзора сайтов. Система позволяет вам установить три набора SSID для разных

целей.

SSID — Установите имя для идентификации маршрутизатора.

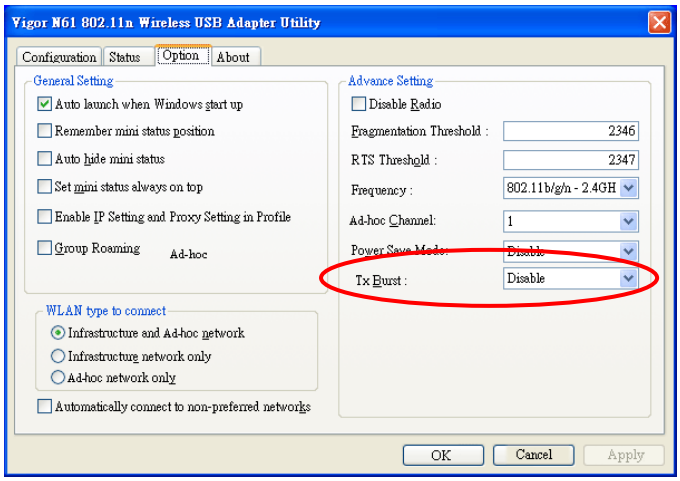
Изоляция клиента — Кликните, чтобы беспроводные клиенты/станции с одним SSID не имели доступа друг к другу.

Канал — Канал частоты беспроводной LAN. По умолчанию – 6. Вы можете переключить канал, если на выбранном канале сильны помехи. Если вы не имеете понятия о частоте, пожалуйста, выберите АвтоВыбор, чтобы система могла решить за вас.



Увеличение размера пакета — Эта функция может увеличить мощность передачи данных на 40% (Кликните на **Ускорение передачи**). Функция активна только когда она одновременно осуществляется и точкой доступа, и станцией (беспроводным клиентом). Поэтому беспроводной клиент должен также поддерживать эту функцию.

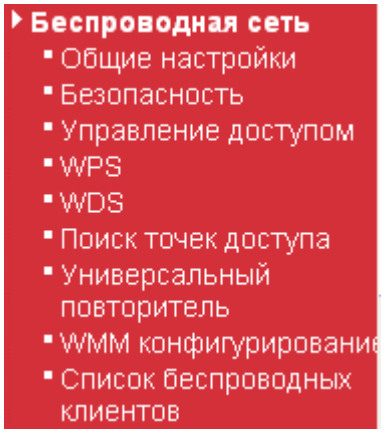
Примечание: эту функцию поддерживает беспроводной адаптер Vigor N61. Поэтому вы можете использовать и установить ее прямо на ваш компьютер для согласования с Packet-OVERDRIVE (выберите **Включить** в меню **Ускорение Передачи** во вкладке **Опции**, как на картинке).



Универсальный Повторитель

Если включен этот режим, точка доступа может работать как беспроводной повторитель, она может быть станцией и точкой доступа одновременно. Она может использовать функции станции, чтобы подсоединиться к Корневой ТД и использовать функцию ТД, для обслуживания всех беспроводных станций в пределах покрытия.

Галочка – чтобы активировать функцию. Она станет отображаться в меню **Беспроводная LAN** для ваших дальнейших настроек.

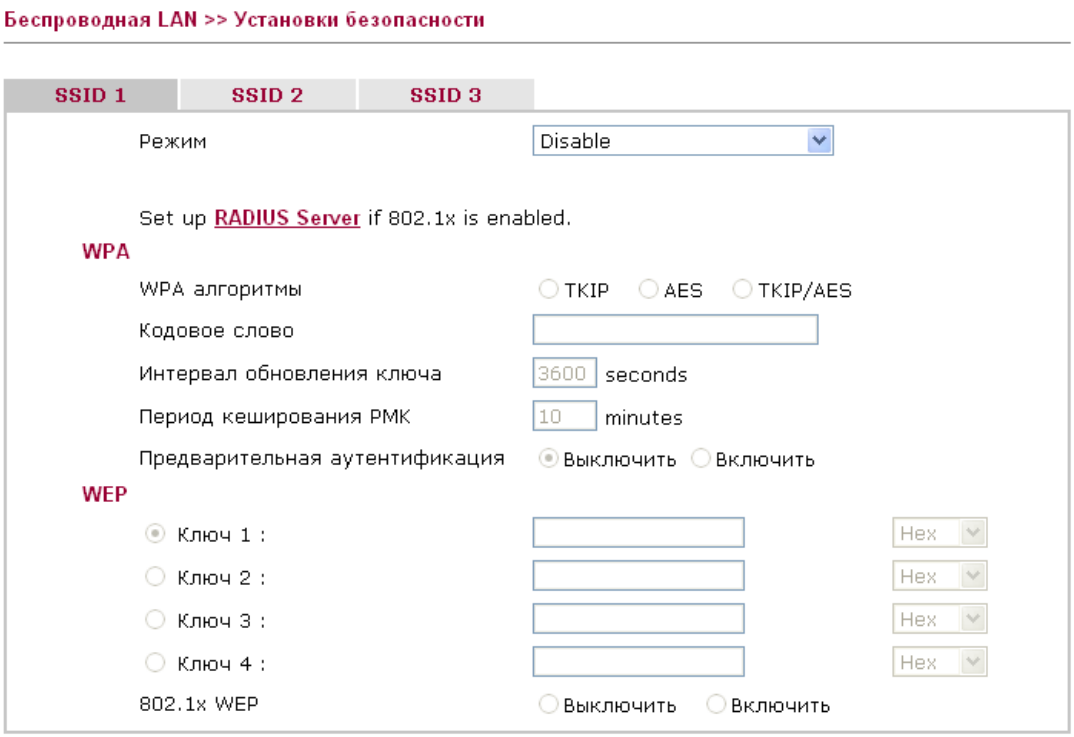


Откройте **Беспроводная сеть>>Универсальный повторитель**. Более подробную информацию вы найдете в соответствующей секции.

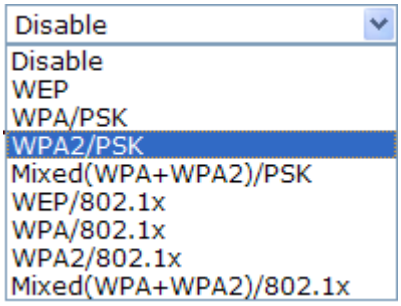
4.6.3 Безопасность

Эта страница позволяет вам настроить режимы безопасности для SSID 1, 2 и 3 соответственно. После настройки нажмите OK для сохранения и активации изменений.

После нажатия **Установки безопасности** появится новое окно.



Режим Вам на выбор будет предложено несколько режимов.

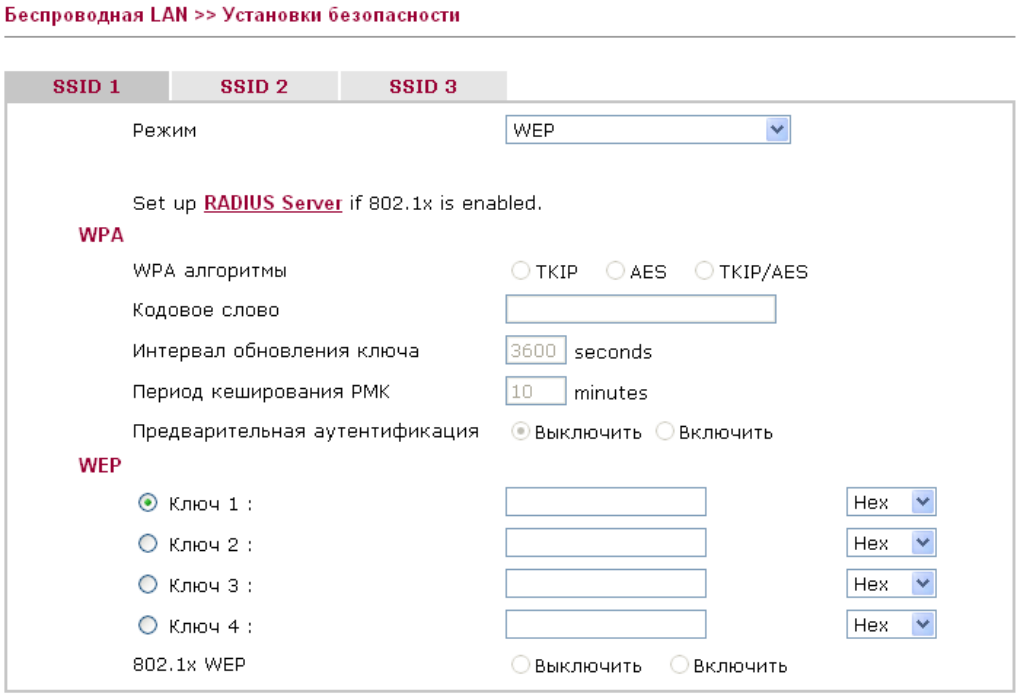


- **Отключить**

  Механизм шифрования будет отключен.

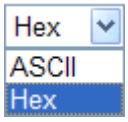
- **WEP**

  Принимает только WEP-клиентов, в поле WEP Ключ должен быть введен ключ шифрования.



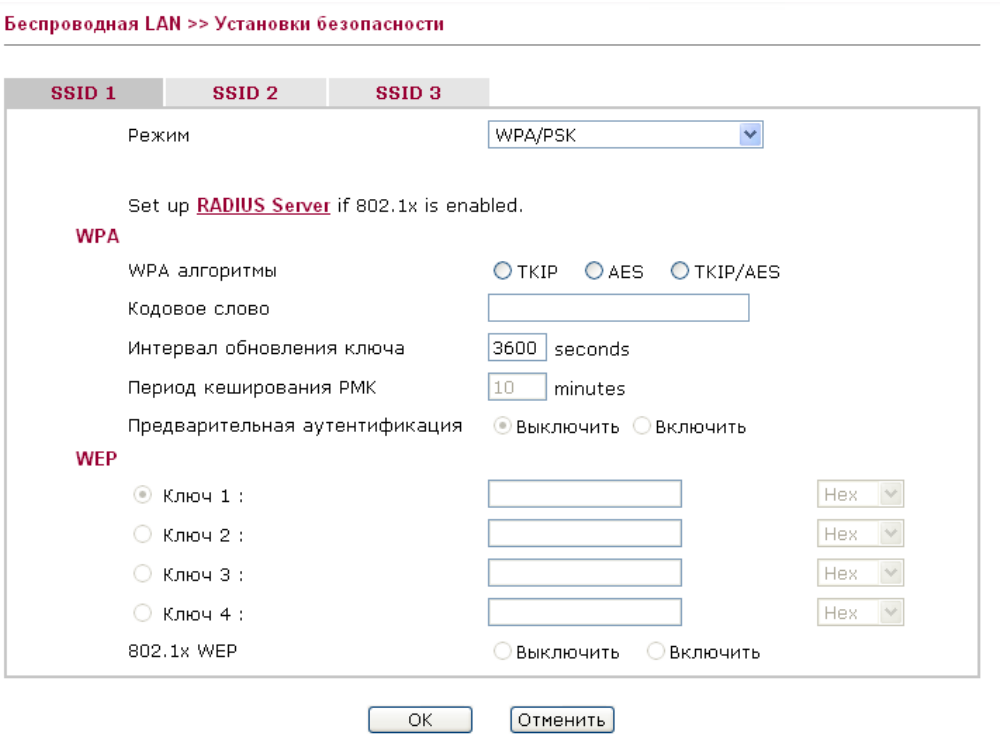
WEP Ключ 1 ~ Ключ 4

Можно ввести четыре ключа, но использован будет только один, выбранный пользователем. Формат WEP-ключа ограничивается 5 символами ASCII или 10 шестнадцатеричными значениями 64-битного шифрования; или 13 символами ASCII или 26 шестнадцатеричными значениями 128-битного шифрования. Разрешены символы ASCII с 33(!) до 126(~) кроме '#' и ','.



- **WPA/PSK или WPA2/PSK или Смешанное шифрование (WPA+WPA2)/PSK**

  Принимает только WPA-клиентов; ключ шифрования должен быть введен с заранее заданными ключами. WPA кодирует каждый переданный пакет, используя ключи, которые вводятся в соответствующее поле или автоматически передаются посредством 802.1x авторизации.



WPA алгоритмы — Выберите WPA алгоритм: TKIP, AES или TKIP/AES.

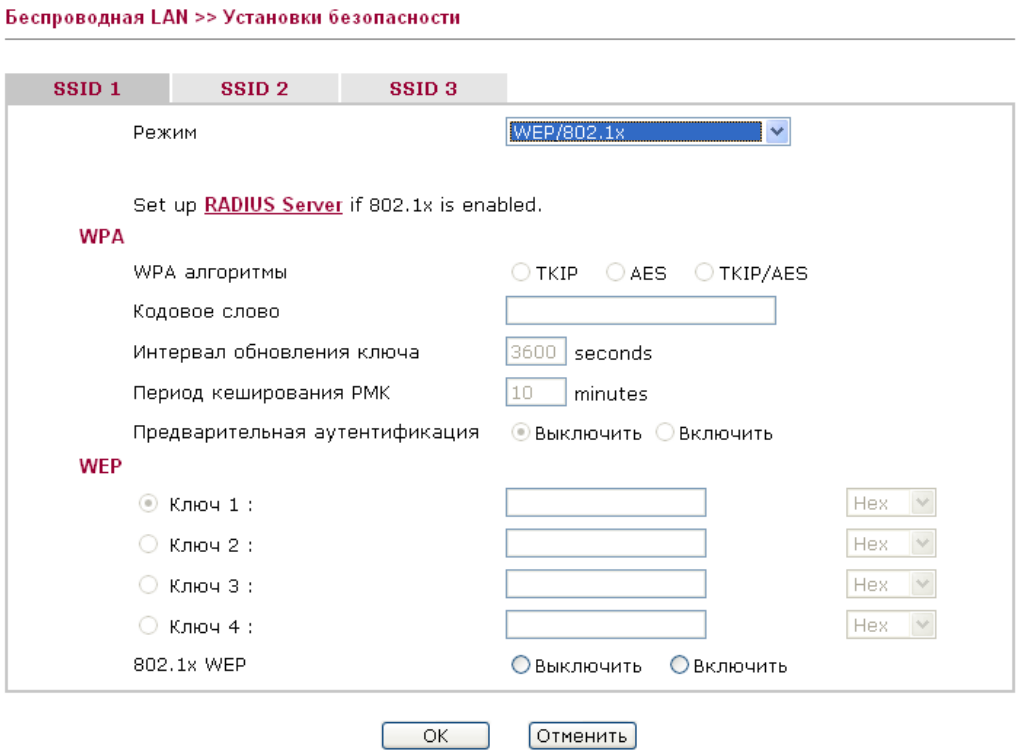
Кодовое слово — 8~63 ASCII символы, такие как 012345678..(или 64 шестнадцатеричных знака, начинающиеся с 0x, такие как "0x321253abcde...").

Интервал обновления ключа — WPA использует ключи авторизации сети. Тем не менее, нормальные сетевые операции используют различные ключи шифрования, которые генерируются произвольно. Введите в этом поле временной интервал смены ключей (в секундах). Меньший интервал увеличит безопасность, но снизит мощность. По умолчанию установлен интервал в 3600 секунд. Установите 0 для отключения генерации ключей.

- **WEP/802.1x**

  Встроенная функция RADIUS-клиента позволяет маршрутизатору поддерживать удаленного пользователя или беспроводного передатчика и RADIUS-сервер в выполнении взаимной идентификации. Данная функция активирует централизованный удаленный доступ идентификации для сетевого управления.

  WPA кодирует каждый передаваемый пакет, используя ключ, который может быть заранее заданным PSK и введенным вручную в соответствующем поле или автоматически установлен в процессе 802.1x аутентификации. Выберите режим WPA, WPA2 или Auto в качестве режима WPA.

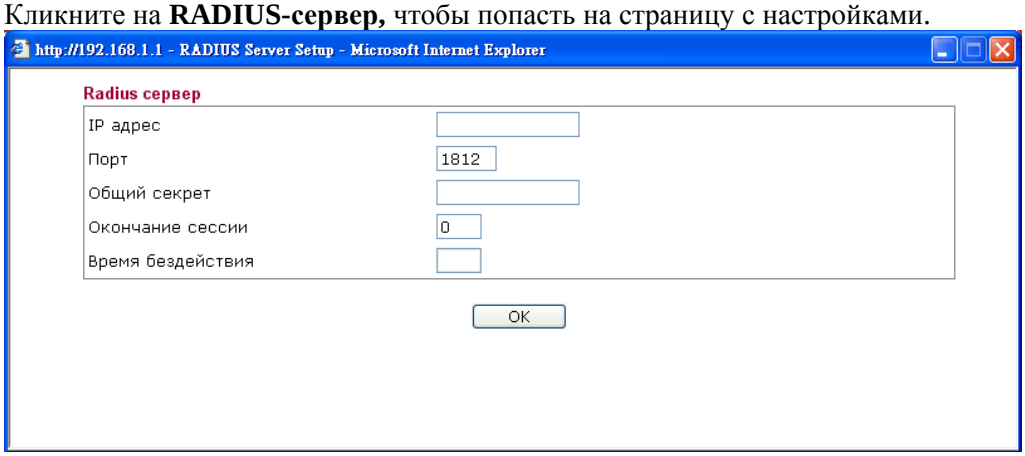


802.1x WEP

Отключить – Отключить WEP-шифрование. Информация, передаваемая в точку доступа, не будет кодироваться.

Включить – Включить WEP-шифрование.

Кликните на **RADIUS-сервер,** чтобы попасть на страницу с настройками.



IP-адрес Введите IP-адрес RADIUS-сервера.

Порт Номер UDP-порта, используемого RADIUS-сервером. По умолчанию установлен 1812 на основе RFC 2138.

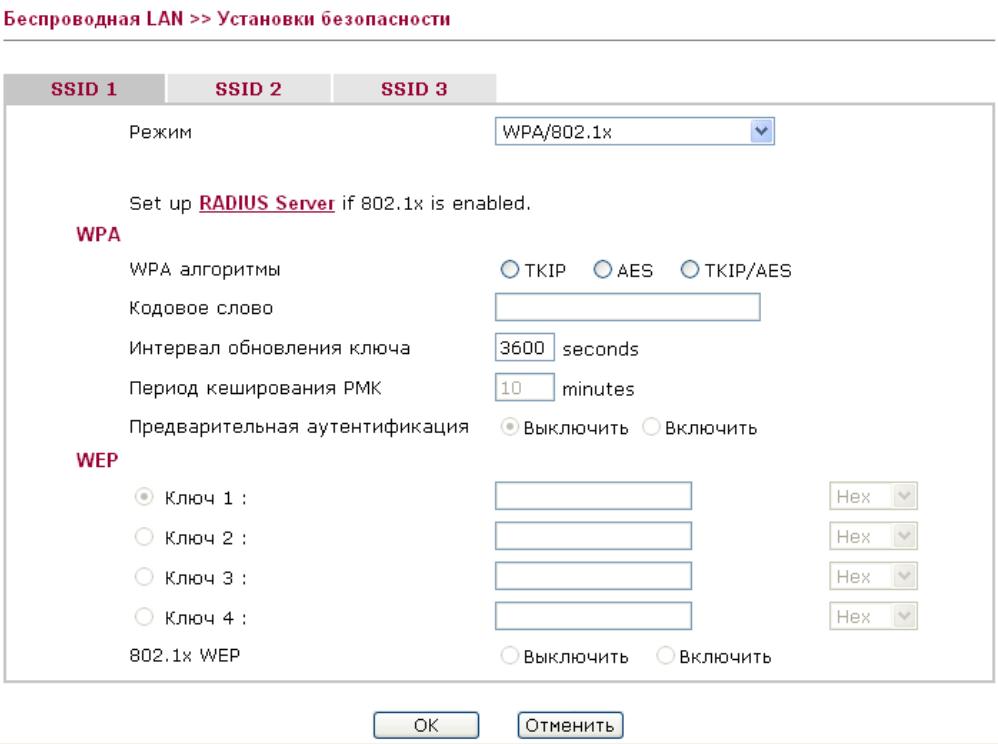
Общий секрет RADIUS-сервер и клиент имеют общий секрет, который используется для идентификации сообщений между ними. Обе стороны должны быть настроены для использования одного и того же общего секрета.

Окончание сессии Установите временной максимум предоставления услуг перед реидентификацией. Впишите ноль, чтобы установить немедленную идентификацию сразу же после окончания сессии (указывайте время в секундах).

Время бездействия — **Время бездействия –** установите время бездействия перед разрывом соединения.

- **WPA/802.1x**

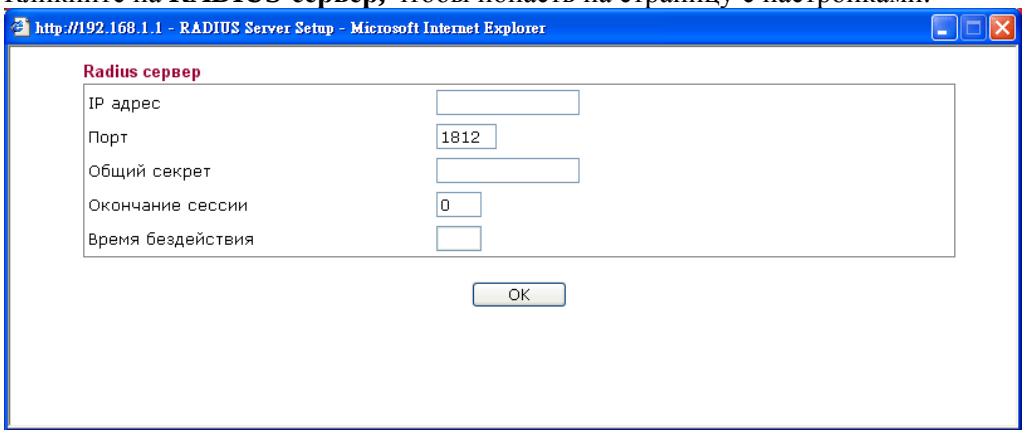
WPA кодирует каждый переданный пакет используя заранее заданные ключи (PSK), которые вводятся в соответствующее поле или автоматически передаются посредством 802.1x авторизации.



WPA алгоритмы — Выберите WPA алгоритм: TKIP, AES или TKIP/AES.

Интервал обновления ключа — WPA использует ключи авторизации сети. Тем не менее, нормальные сетевые операции используют различные ключи шифрования, которые генерируются произвольно. Введите в этом поле временной интервал смены ключей (в секундах). Меньший интервал увеличит безопасность, но снизит мощность. По умолчанию установлен интервал в 3600 секунд. Установите 0 для отключения генерации ключей.

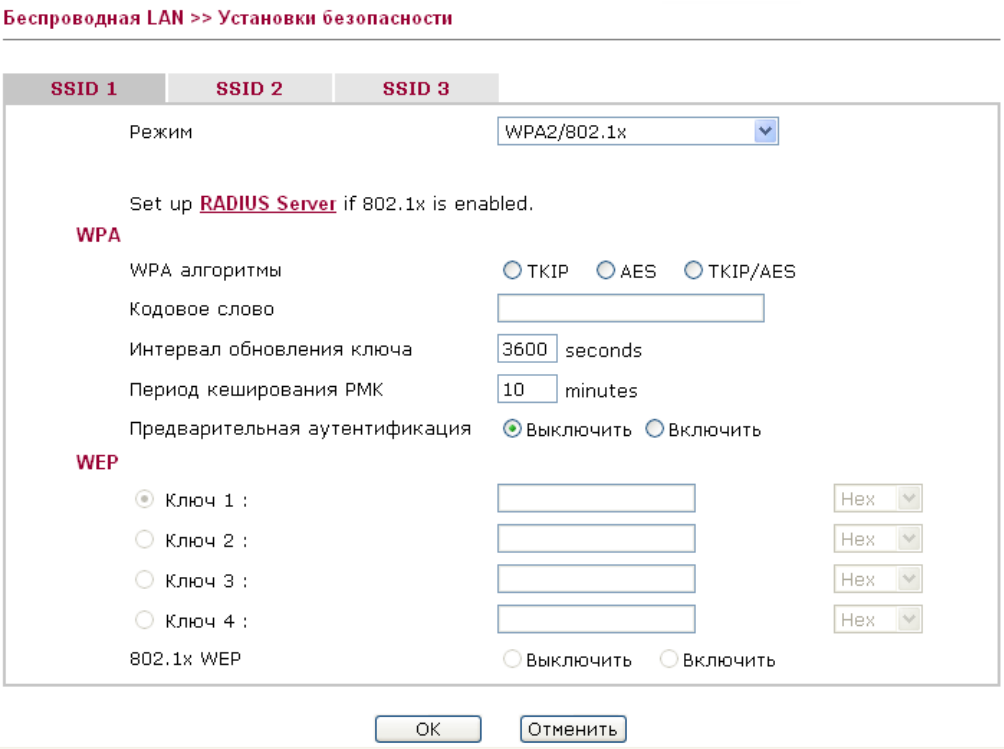
Кликните на **RADIUS-сервер,** чтобы попасть на страницу с настройками.



IP-адрес	Введите IP-адрес RADIUS-сервера.
Порт	Номер UDP-порта, используемого RADIUS-сервером. По умолчанию установлен 1812 на основе RFC 2138.
Общий секрет	RADIUS-сервер и клиент имеют общий секрет, который используется для идентификации сообщений между ними. Обе стороны должны быть настроены для использования одного и того же общего секрета.
Окончание сессии	Установите временной максимум предоставления услуг перед реидентификацией. Впишите ноль, чтобы установить немедленную идентификацию сразу же после окончания сессии (указывайте время в секундах).
Время бездействия	**Время бездействия –** установите время бездействия перед разрывом соединения.

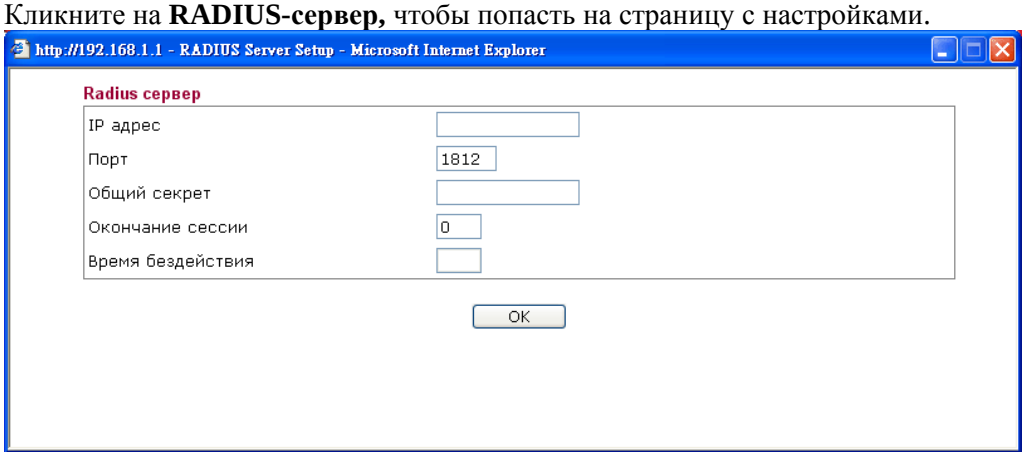
- **WPA2/802.1x**

WPA кодирует каждый переданный пакет, используя заранее заданные ключи (PSK), которые вводятся в соответствующее поле или автоматически передаются посредством 802.1x авторизации.



WPA алгоритмы	Выберите WPA алгоритм: TKIP, AES или TKIP/AES.
Интервал обновления ключа	WPA использует ключи авторизации сети. Тем не менее, нормальные сетевые операции используют различные ключи шифрования, которые генерируются произвольно. Введите в этом поле временной интервал смены ключей (в секундах). Меньший интервал увеличит безопасность, но снизит мощность. По умолчанию установлен интервал в 3600 секунд. Установите 0 для отключения генерации ключей.
PMK Cache Period	Установите период хранения WPA2 PMK (парные ключи). PMK Cache управляет списком BSSID и ассоциированными SSID, с которыми устройство идентифицировалось ранее.
Предварительная аутентификация	Активирует передатчик для идентификации и более безопасного и быстрого переключения между точками доступа. С процедурой предварительной аутентификации, определенной спецификацией IEEE 802.11i, предварительное четырехстороннее рукопожатие может уменьшить задержку передачи, воспринимаемую мобильной точкой. Это сделает переключение более безопасным и быстрым (доступно только в WPA2). **Включить –** Включить IEEE 802.1X предварительную аутентификацию. **Выключить –** Выключить IEEE 802.1X предварительную аутентификацию.

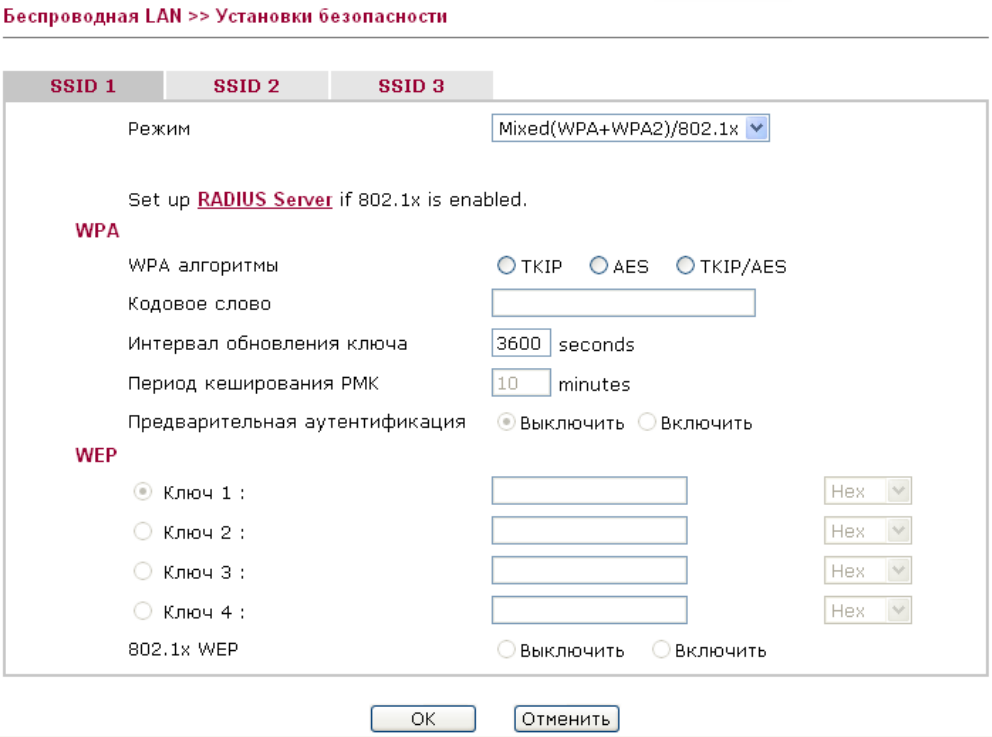
Кликните на **RADIUS-сервер,** чтобы попасть на страницу с настройками.



IP-адрес	Введите IP-адрес RADIUS-сервера.
Порт	Номер UDP-порта, используемого RADIUS-сервером. По умолчанию установлен 1812 на основе RFC 2138.
Общий секрет	RADIUS-сервер и клиент имеют общий секрет, который используется для идентификации сообщений между ними. Обе стороны должны быть настроены для использования одного и того же общего секрета.
Окончание сессии	Установите временной максимум предоставления услуг перед реидентификацией. Впишите ноль, чтобы установить немедленную идентификацию сразу же после окончания сессии (указывайте время в секундах).
Время бездействия	**Время бездействия –** установите время бездействия перед разрывом соединения.

- **Смешанное шифрование (WPA+WPA2)/802.1x**

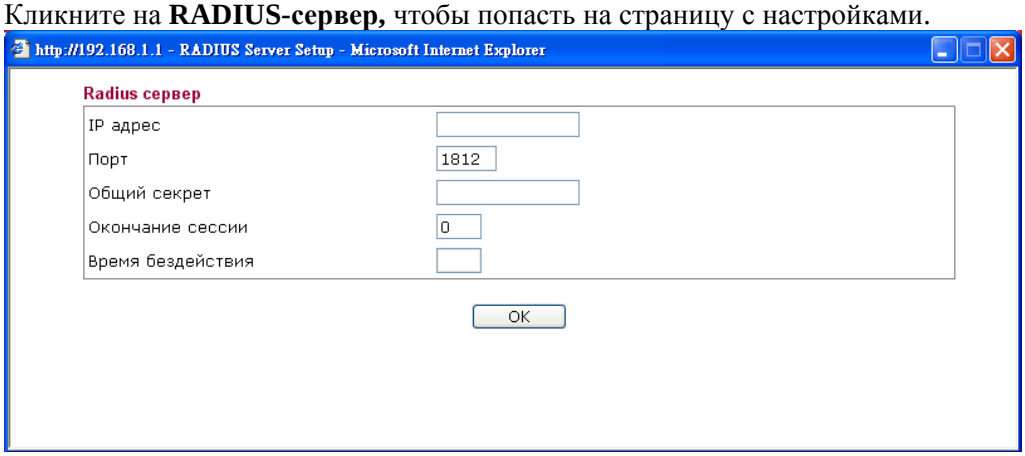
  WPA кодирует каждый переданный пакет используя заранее заданные ключи (PSK), которые вводятся в соответствующее поле или автоматически передаются посредством 802.1x авторизации.



WPA алгоритмы Выберите WPA алгоритм: TKIP, AES или TKIP/AES.

Интервал обновления ключа WPA использует ключи авторизации сети. Тем не менее, нормальные сетевые операции используют различные ключи шифрования, которые генерируются произвольно. Введите в этом поле временной интервал смены ключей (в секундах). Меньший интервал увеличит безопасность, но снизит мощность. По умолчанию установлен интервал в 3600 секунд. Установите 0 для отключения генерации ключей.

Кликните на **RADIUS-сервер,** чтобы попасть на страницу с настройками.



IP-адрес Введите IP-адрес RADIUS-сервера.

Порт Номер UDP-порта, используемого RADIUS-сервером.

По умолчанию установлен 1812 на основе RFC 2138.

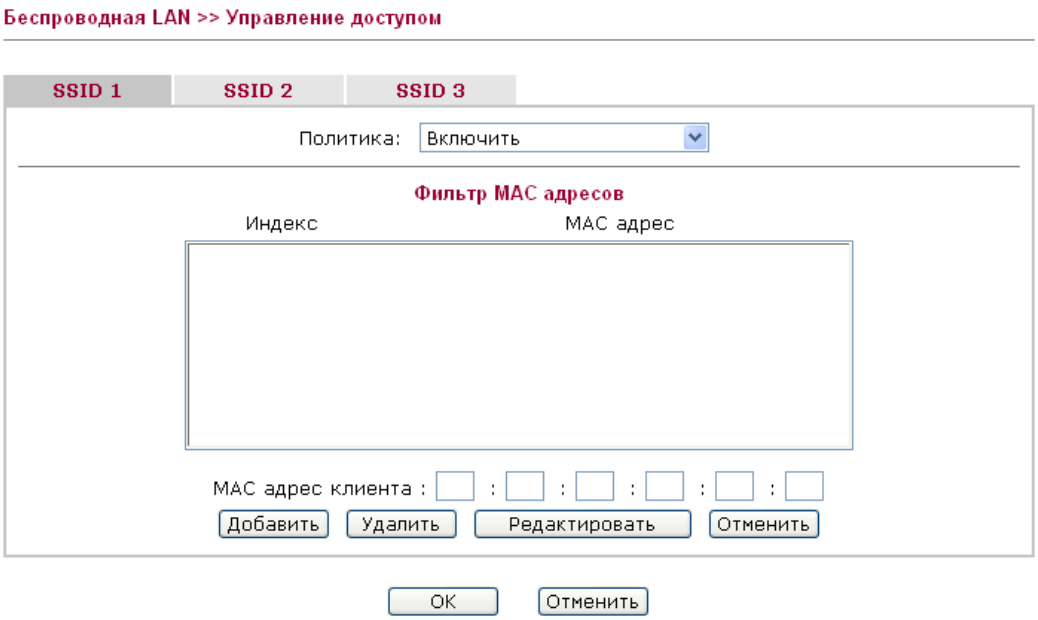
Общий секрет — RADIUS-сервер и клиент имеют общий секрет, который используется для идентификации сообщений между ними. Обе стороны должны быть настроены для использования одного и того же общего секрета.

Окончание сессии — Установите временной максимум предоставления услуг перед реидентификацией. Впишите ноль, чтобы установить немедленную идентификацию сразу же после окончания сессии (указывайте время в секундах).

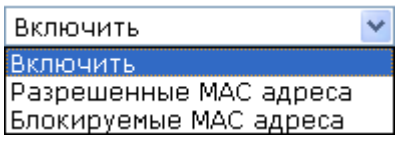
Время бездействия — **Время бездействия –** установите время бездействия перед разрывом соединения.

4.6.4 Управление доступом

(PSK)Для дополнительной защиты беспроводной сети существует функция **Управление доступом.** Она позволяет ограничить права доступа к беспроводной сети клиентов с определенным MAC-адресом. Нажмите **Управление доступом**. Здесь вы сможете редактировать MAC-адреса клиентов, чтобы настроить их права доступа (разрешить или запретить доступ).



Политика — Выберите, чтобы выбрать один из типов или отключить функцию. Выберите **Активировать фильтр MAC адресов**, чтобы вручную вписать MAC-адреса клиентов.



Фильтр MAC-адресов — Отображает все добавленные ранее MAC-адреса.

MAC-адрес клиента — Введите MAC-адрес беспроводного клиента.

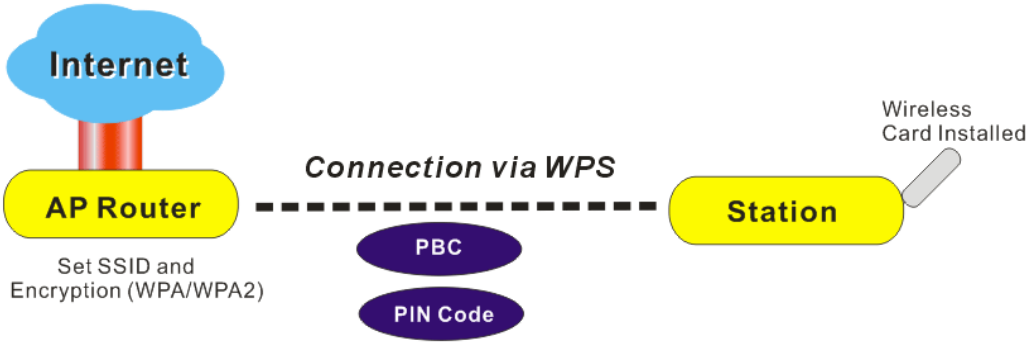
Добавить — Добавить новый MAC-адрес в список.

Удалить	Удалить выбранный MAC-адрес из списка.
Редактировать	Редактировать выбранный в списке MAC-адрес.
Отменить	Прекратить настройку контроля доступа.
OK	Нажмите, чтобы сохранить список.
Отменить	Очистить список MAC-адресов.

4.6.5 WPS

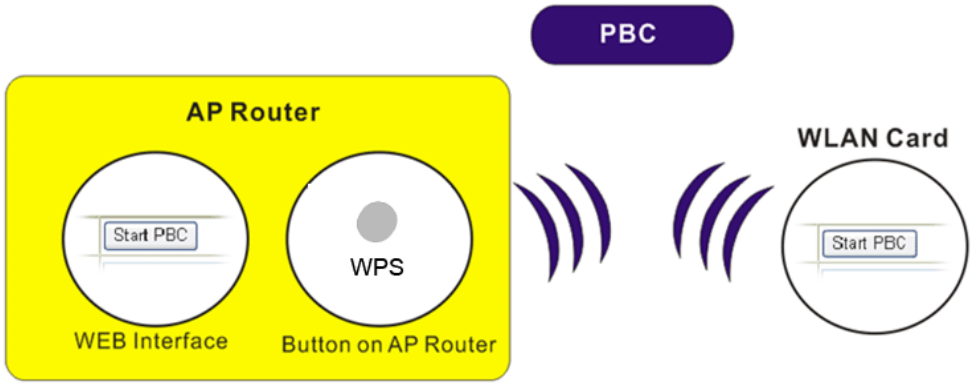
WPS (Wi-Fi Protected Setup) обеспечивает простое соединение беспроводного клиента и беспроводной точки доступа (маршрутизатор) с шифрованием WPA и WPA2.

Это простейший способ создания связи между клиентами беспроводной сети и маршрутизатором. Чтобы установить беспроводную связь, пользователям не нужно будет выбирать режим шифрования и каждый раз вводить кодовое слово; нужно только нажать на кнопку на беспроводном клиенте, и WPS позволит подключаться клиенту к маршрутизатору автоматически.



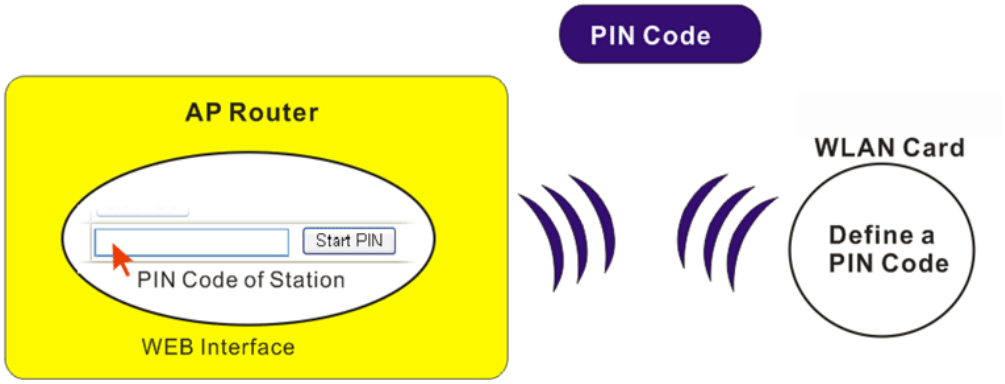
Примечание: данная функция доступна только на беспроводных станциях с поддерживаемым WPS.

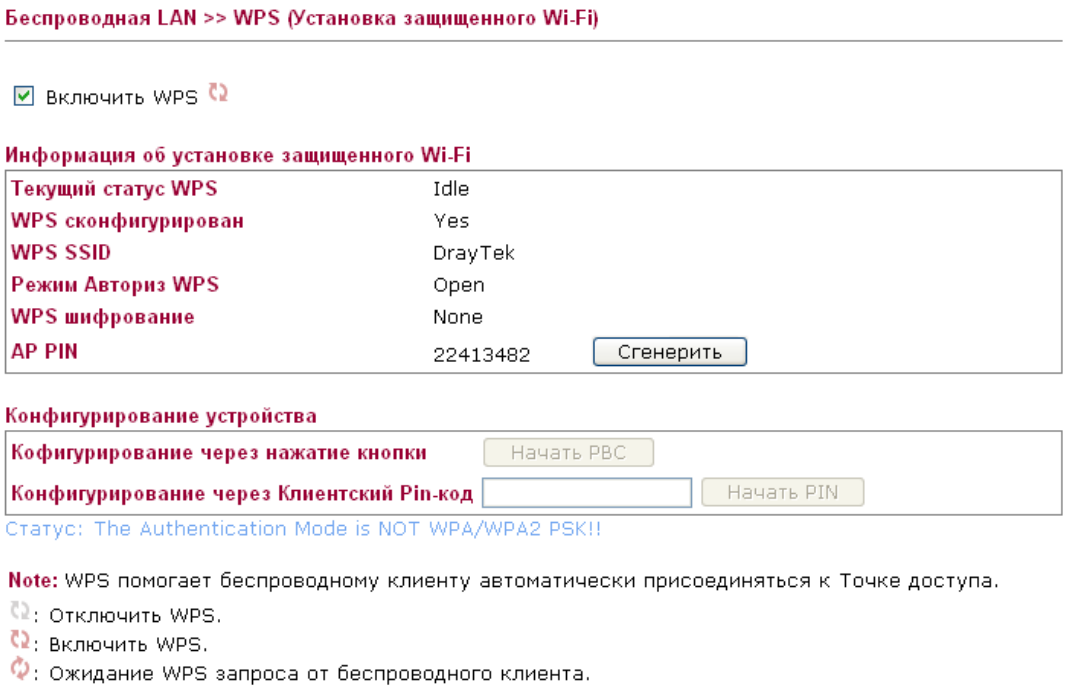
Существует два способа подключения точки доступа и станций с помощью WPS: нажать кнопку ***Начать PBC*** или используя ***PIN-код***. У маршрутизаторов серии VigorFly 200, которые служат точкой доступа, кнопка WPS находится на передней панели. Нажмите кнопку **WPS** или щелкните **Начать PBC** в интерфейсе веб-конфигурации. На той стороне станции, где установлена сетевая карта, нажмите кнопку сетевой карты **Начать PBC**.



Если вы хотите использовать PIN-код, вы должны знать PIN-код, назначенный в беспроводном клиенте. Затем обеспечьте маршрутизатор PIN-кодом беспроводного

клиента, к которому вы хотите подключиться.





Включить WPS	Кликните, чтобы активировать настройки WPS.
Текущий статус WPS	Отображает необходимую системную информацию о WPS. Если функция беспроводной безопасности (шифрование) настроена правильно, здесь будет отображено **WPS сконфигурирован.**
WPS SSID	Отображает актуальный SSID.
Режим Авториз WPS	Отображает актуальный режим аутентификации маршрутизатора. Только WPA2/PSK и WPA/PSK поддерживают WPS.
WPS шифрование	Отображает режим шифрования маршрутизатора (Нет, WEP, TKIP, AES, проч.)
AP PIN	Номер, отображенный в этом поле, будет вводиться в регистраторе удаленной станции удаленным клиентом для подключения.
Кофигурирование через нажатие кнопки	Нажмите **Начать PBC** чтобы воспользоваться первым способом настройки (см. выше). Маршрутизатор будет ожидать WPS запросов от беспроводных клиентов в

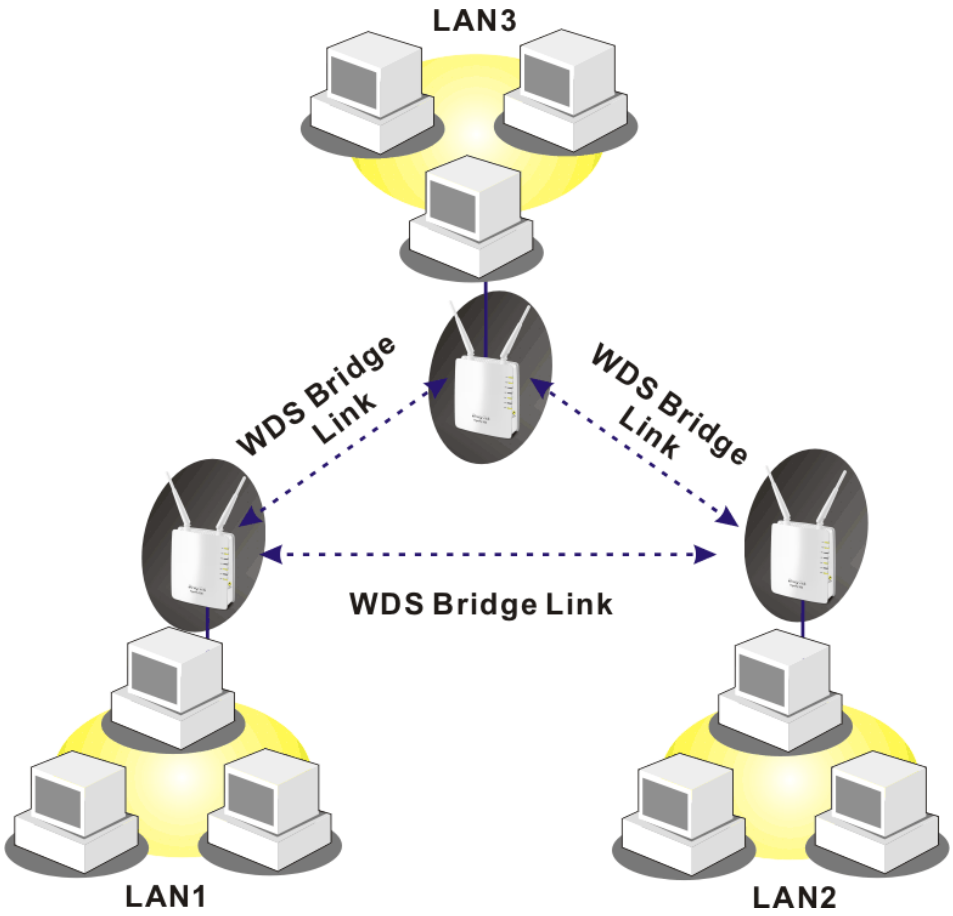
	течение двух минут. Диод WPS будет быстро мигать в процессе работы WPS. Он вернется к нормальному режиму работы через две минуты (вам нужно настроить WPS в течение двух минут).
Конфигурирование через Клиентский Pin-код	Введите PIN-код, установленный в удаленном клиенте, через который вы будете подключаться, затем нажмите кнопку **Начать PIN.** Диод WLAN будет быстро мигать в процессе работы WPS. Он вернется к нормальному режиму работы через две минуты (вам нужно настроить WPS в течение двух минут).

4.6.6 WDS

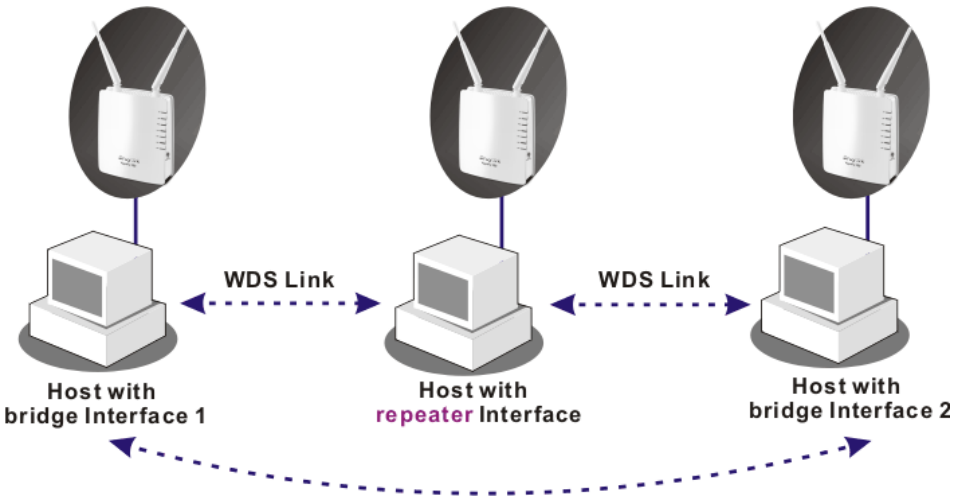
WDS (Wireless Distribution System) – протокол для беспроводного подключения двух и более точек доступа. Обычно он может быть использован для следующих приложений:

- Обеспечение моста между двумя LAN через эфир.
- Расширение площади покрытия WLAN.

Для соответствия вышеуказанным требованиям маршрутизатор поддерживает два режима WDS: мост (bridge) и повторитель (repeater). Ниже показан принцип работы функции WDS-Bridge:

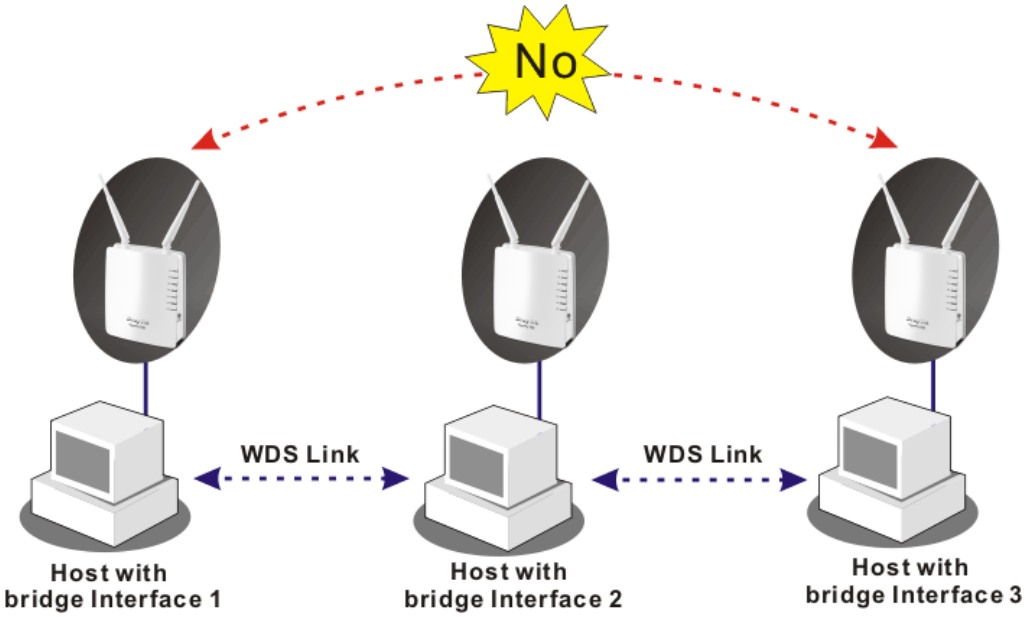


Ниже показана работа в режиме WDS-повторителя:

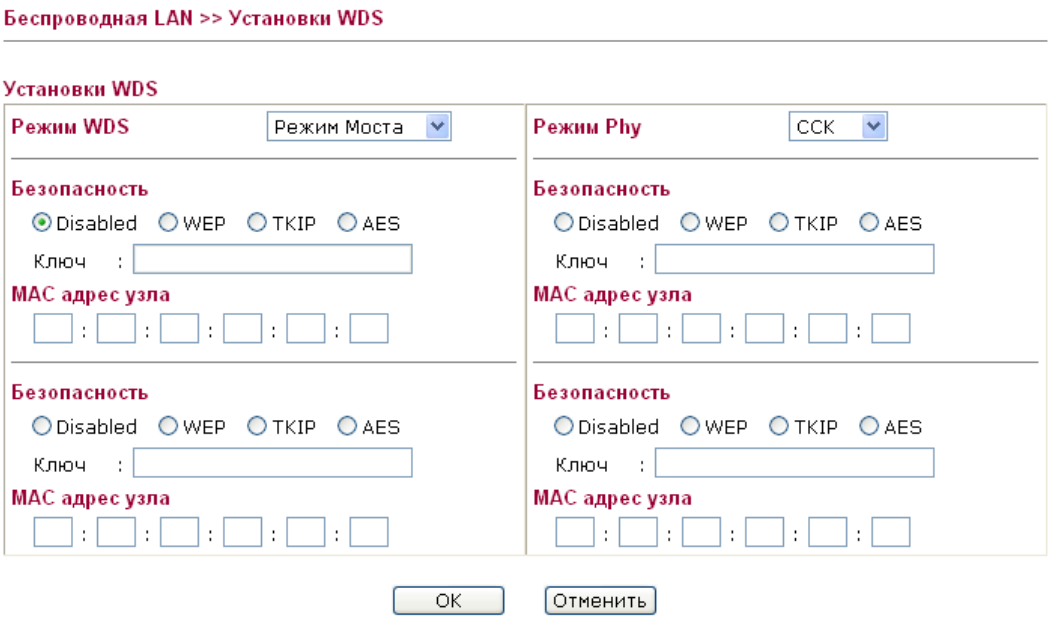


Главное различие между режимами заключается в следующем: в режиме **Повторителя** пакеты, полученные от одного узла точки доступа, могут быть переданы другому узлу через WDS; в режиме **Моста** пакеты могут быть лишь перенаправлены к локальным проводным или беспроводным хостам. Другими словами, только режим Повторитель может осуществить передачу пакетов от WDS к WDS.

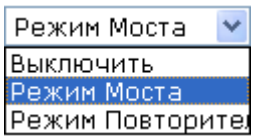
В следующих примерах хосты, подключенные к Мостам 1 и 3, могут связываться с хостами, подключенными к Мосту 2 через WDS связи. Однако хосты, подключенные к Мосту 1, НЕ могут связываться с хостами, подключенными к Мосту 3 через Мост 2.



Кликните на **WDS** в меню **Wireless LAN**. Появится следующая страница.



Режим — Выберите режим WDS. Вы можете выбрать режим **Моста** для первого варианта настроек или режим **Повторителя** для второго. Если вы выберете **Выключить,** функция будет отключена.



Безопасность — Существуют четыре типа безопасности: **Отключено, WEP, TKIP** и **Ключ** или **MAC-адрес узла**. Выберите один из типов для маршрутизатора. Пожалуйста, отключите неиспользуемую ссылку, чтобы увеличить мощность.

Ключ — Введите 8~63 ASCII символов или 64 шестнадцатеричных знака, начинающихся с «0x».

MAC-адрес узла — На странице можно ввести четыре MAC-адреса узлов.

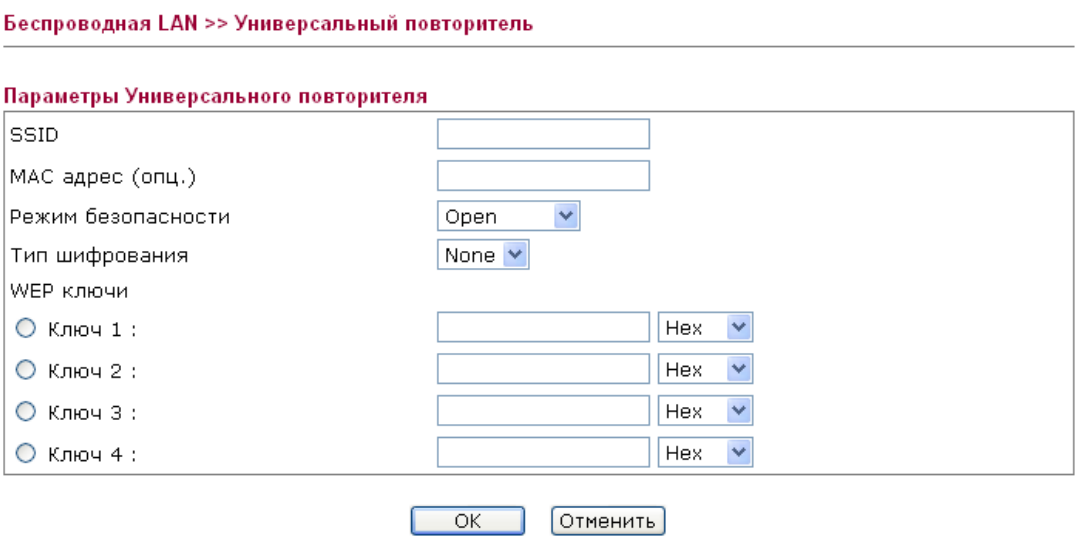
Режим Phy — Существуют три типа скорости передачи данных, разработанные различными методами для **режима Phy**. Данные будут передаваться через канал связи.

OK — Нажмите для сохранения настроек.

4.6.7 Универсальный повторитель

Это меню доступно только когда оно активировано в **Беспроводная сеть>>Общие настройки**. Эта функция позволяет вам назначить точку доступа, к которой может подключаться маршрутизатор как удаленный клиент. Маршрутизатор может работать как беспроводной повторитель; он может быть и беспроводным клиентом и точкой доступа одновременно. Он может использовать режим клиента для подключения к корневой точке доступа и использовать режим точки доступа для управления всеми беспроводными станциями внутри зоны покрытия.

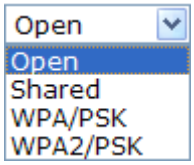
Примечание: Во время использования функции Универсальный повторитель точка доступа будет демодулировать принятый сигнал. Пожалуйста, проверьте, не является ли этот сигнал шумами от другой работающей сети, нужный сигнал будет модулирован и усилен. Выходная мощность у этого режима такая же, как у WDS или обычной работы в режиме точки доступа.



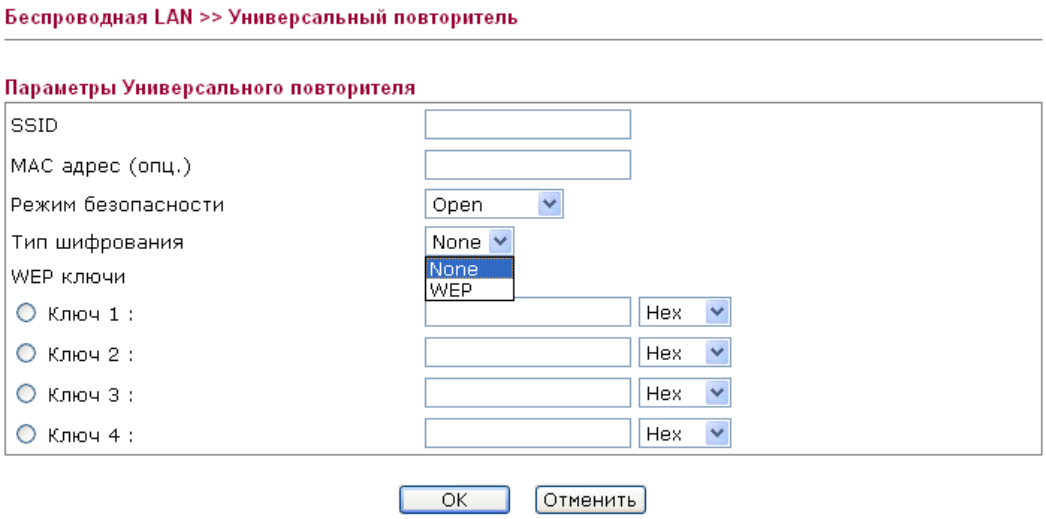
SSID — Установите имя идентификации маршрутизатора.

MAC-адрес (опционально) — Введите MAC-адрес точки доступа, к которой будет подключаться маршрутизатор.

Режим безопасности — Вам на выбор будет предложено несколько режимов с разными параметрами (напр., WEP-ключи, Ключевое слово).

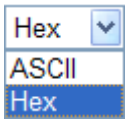


- **Открытый / Совместный режим**

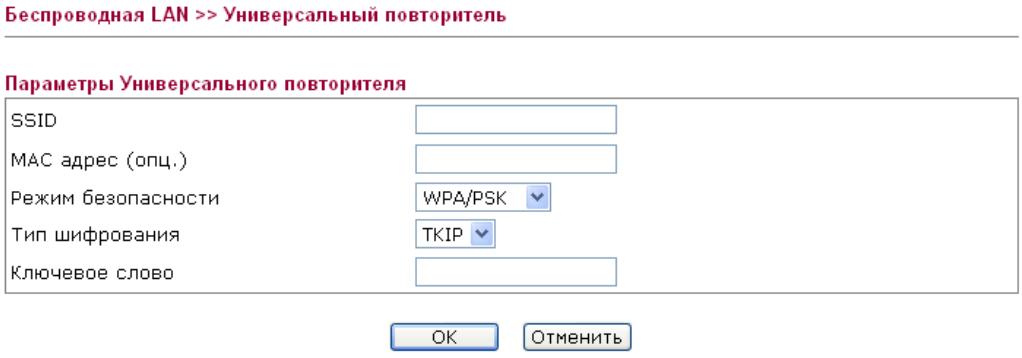


Тип шифрования — Выберите **Нет,** чтобы выключить WEP-шифрование. Информация, отправляемая в точку доступа, не будет шифрована. Чтобы включить WEP-шифрование данных, выберите **WEP.**

WEP-Ключи — Можно ввести четыре ключа, но использован будет только один, выбранный пользователем. Формат WEP-ключа ограничивается 5 символами ASCII или 10 шестнадцатеричными значениями 64-битного шифрования; или 13 символами ASCII или 26 шестнадцатеричными значениями 128-битного шифрования. Разрешены символы ASCII с 33(!) до 126(~) кроме '#' и ','.



- **Режим WPA/PSK и режим WPA2/PSK**



Тип шифрования — Выберите TKIP или AES в качестве алгоритма WPA.

Кодовое слово — 8~63 ASCII символы, такие как 012345678..(или 64 шестнадцатеричных знака, начинающихся с 0x, такие как "0x321253abcde...").

4.6.8 Поиск точек доступа

Маршрутизатор Vigor может сканировать все каналы и находить работающие в округе точки доступа. На основе результатов сканирования пользователи будут знать, какие каналы чисты для использования. Кроме того, он может быть использован для более легкого обнаружения точек доступа для WDS-связи. Обратите внимание, что в процессе сканирования (около 5 секунд), беспроводные клиенты не смогут подключиться к маршрутизатору.

Следующая страница используется для проверки наличия точек доступа в беспроводной LAN. Обнаруженными могут быть только точки доступа, работающие на том же канале, что и маршрутизатор. Пожалуйста, нажмите **Сканировать** для поиска всех подключенных точек доступа.

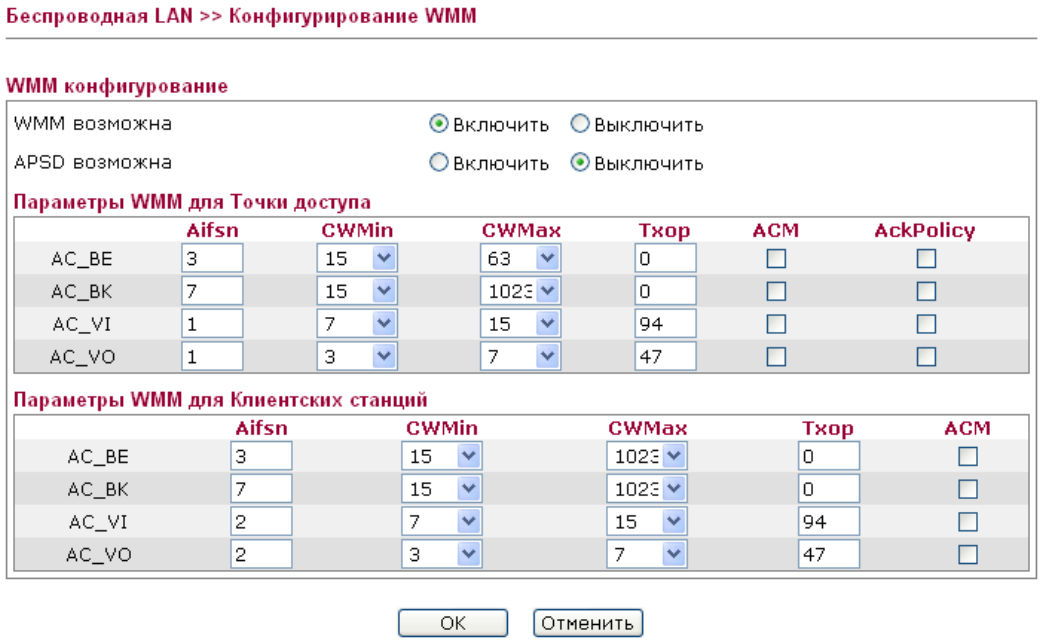
SSID	Отображает SSID точки доступа, найденной маршрутизатором.
BSSID	Отображает MAC-адрес точки доступа, найденной маршрутизатором.
RSSI	Отображает силу сигнала. RSSI – это аббревиатура от Receive Signal Strength Indication.
Канал	Отображает беспроводной канал, используемый точкой доступа, которую обнаружил маршрутизатор.
Шифрование	Отображает тип шифрования найденной точки доступа.
Аутентификация	Отображает тип аутентификации, принятой обнаруженной точкой доступа.
Сканировать	Используется для поиска всех подключенных точек доступа. Результаты будут показаны в поле над этой кнопкой.
Статистика	Отображает статистику для каналов, используемых точками доступа.
MAC-адрес точки доступа	Если вы хотите обнаружить точку доступа, применив WDS-настройки, пожалуйста, введите MAC-адрес точки доступа.
SSID Точки доступа	Для выбора точки доступа с применением WDS-настроек, вам нужно назначить MAC-адрес или SSID точки доступа. В этом поле вы можете ввести SSID точки доступа.

Добавить Выберите **Мост** или **Повторитель** для выбранной точки. Далее нажмите **Добавить**. MAC-адрес точки доступа будет введен далее и отображен на странице WDS-настроек.

4.6.9 WMM Конфигурирование

WMM (Wi-Fi Multimedia) – определяет приоритетные уровни четырех категорий доступа, полученных от 802.1D (prioritization tabs). Категории основаны на конкретных типах трафика, голоса, видео, лучшей работе и низкой приоритетности данных. Есть четыре категории доступа – AC_BE, AC_BK, AC_VI и AC_VO для WMM.

APSD (automatic power-save delivery) это усиление механизмов сбережения энергии, которые поддерживаются Wi-Fi сетями. Функция позволяет устройствам дольше работать в режиме сна и потреблять меньше энергии для увеличения производительности с помощью минимизации задержек передач. Такие функции предназначены для мобильных и беспроводных телефонов, в основном поддерживающих VoIP.



WMM возможна Нажмите **Включить,** чтобы принять WMM параметры беспроводной передачи данных.

APSD возможна По умолчанию **Выключено.** Нажмите **Включить**, чтобы активировать функцию APSD.

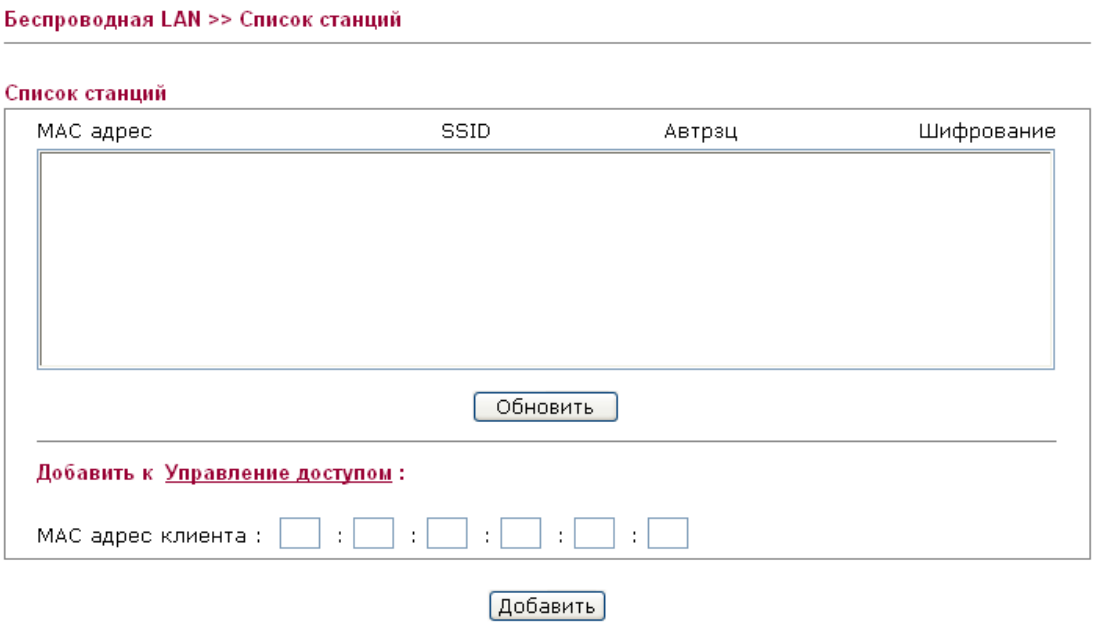
Aifsn Контроль за временем ожидания каждой передачи данных. Пожалуйста, установите число от 1 до 15. Этот параметр будет влиять на временную задержку категорий доступа WMM. Для голосовых или видео-сервисов устанавливайте небольшое число в категориях AC_VI и AC_VO. Для почты или браузеров используйте большое число в категориях AC_BE и AC_BK.

CWMin/CWMax **CWMin** означает спор Window-Min; **CWMax –** спор Window-Max. Пожалуйста, установите число от 1 до 15.

	Обратите внимание на то, что число CWMax должно быть больше, чем CWMin или равно ему. Оба числа будут влиять на временную задержку категорий доступа WMM. Разница между категориями AC_VI и AC_VO должна быть меньше; разница между AC_BE и AC_BK должна быть больше.
Txop	Возможность передачи. Для категорий AC_VI и AC_VO, которым требуется приоритет в передаче данных, установите большее число, чтобы предоставить им более широкие возможности передач. Выберите число от 0 до 65535.
ACM	Admission Control Mandatory может ограничивать станции в использовании некоторых категорий. Кликните, чтобы активировать.
AckPolicy	По умолчанию поле не отмечено. Это значит, что точка доступа маршрутизатора будет отвечать на запросы во время передачи WMM пакетов через беспроводное соединение. Устройство может удостовериться, что узел должен получать WMM пакеты.
OK	Нажмите, чтобы сохранить настройки.

4.6.10 Список беспроводных клиентов

Список беспроводных клиентов содержит информацию о подключавшихся беспроводных клиентах вместе с их статусом.



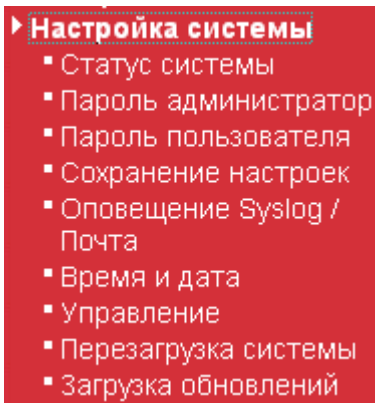
MAC-адрес	Отображает MAC-адрес подключающегося клиента.
SSID	Отображает SSID, к которому подключается клиент.
Автрз	Отображает тип аутентификации, которую беспроводной клиент использует для подключения к данной точке доступа.

Шифрование	Отображает режим шифрования, используемый беспроводным клиентом.
Обновить	Нажмите эту кнопку, чтобы обновить статус списка станций.
Добавить к Управление доступом	**MAC-адрес клиента** – Для дополнительной защиты беспроводного доступа существует возможность контроля доступа. Функция позволяет вам ограничить доступ к сети с помощью управления доступом по MAC-адресу клиента беспроводной LAN. Доступ к беспроводной LAN будет ограничен в соответствии с MAC-адресом беспроводного клиента.
Добавить	Нажмите, чтобы добавить актуальный MAC-адрес в **Контроль Доступа**.

4.7 Настройка системы

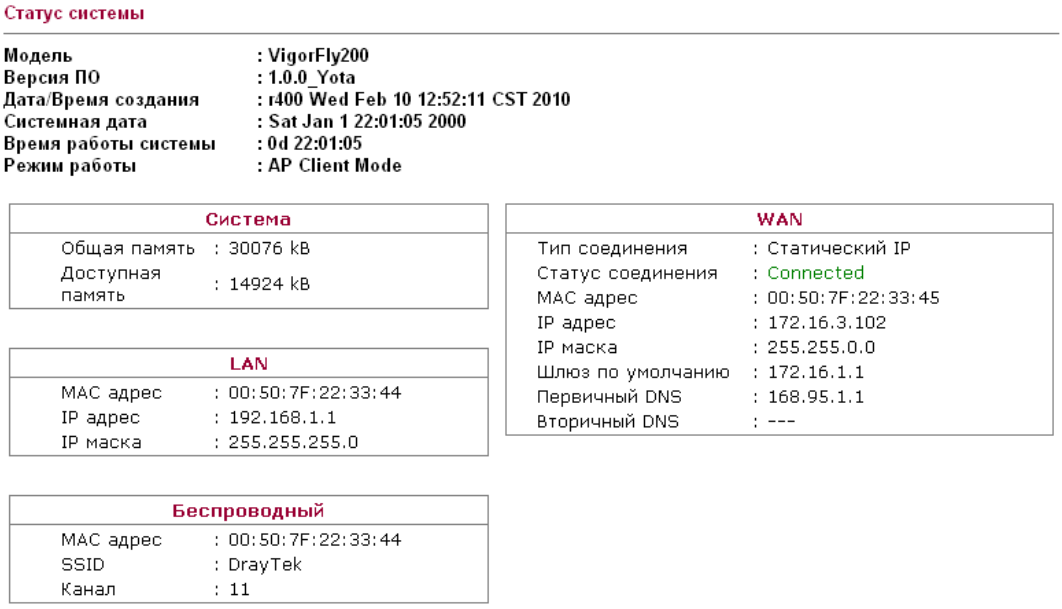
Для настройки системы вы должны знать следующие разделы меню настроек: Статус системы, Пароль администратора, Сохранение настроек, Оповещение Syslog/Почта, Время и дата, Управление, Перезагрузка системы и Загрузка обновлений.

Ниже показано меню Настройка системы.



4.7.1 Статус системы

Статус системы позволяет определить основные сетевые настройки маршрутизатора. Он также включает информацию о состоянии LAN и WAN интерфейсов. Вы можете увидеть время последнего обновления ПО и его текущую версию.

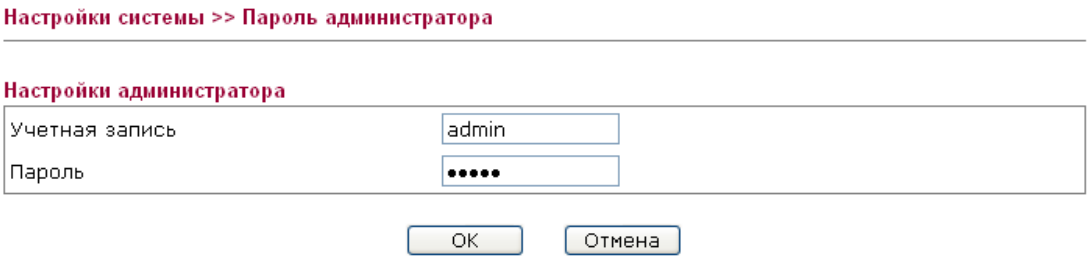


Модель	Отображает название модели маршрутизатора.
Версия ПО	Отображает версию ПО маршрутизатора.
Дата/Время создания	Отображает дату и время нынешней версии ПО маршрутизатора.
Системная дата	Отображает дату и время системного сервера.
Время работы системы	Отображает время подключения системного сервера.
Режим работы	Отображает режим работы маршрутизатора.
Общая память	Отображает размер оперативной памяти системы.
Доступная память	Отображает доступную память системы.
MAC-адрес	Отображает MAC-адрес LAN/WAN/WLAN-интерфейса.
IP-адрес	Отображает MAC-адрес LAN/WAN-интерфейса.
IP маска	Отображает адрес маски подсети LAN/WAN-интерфейса.
Тип устройства	Отображает тип устройства, использованного для беспроводной LAN.
SSID	Отображает SSID этого маршрутизатора.
Канал	Отображает канал, использованный беспроводной LAN.
Тип соединения	Отображает тип сетевого соединения этого маршрутизатора.
Статус соединения	Отображает статус сети.
Шлюз по умолчанию	Отображает адрес шлюза WAN-интерфейса.

Первичный DNS	Отображает настройки назначенного первичного DNS.
Вторичный DNS	Отображает настройки назначенного вторичного DNS.

4.7.2 Пароль администратора

Эта страница позволяет вам установить новый пароль для операций в режиме администратора.

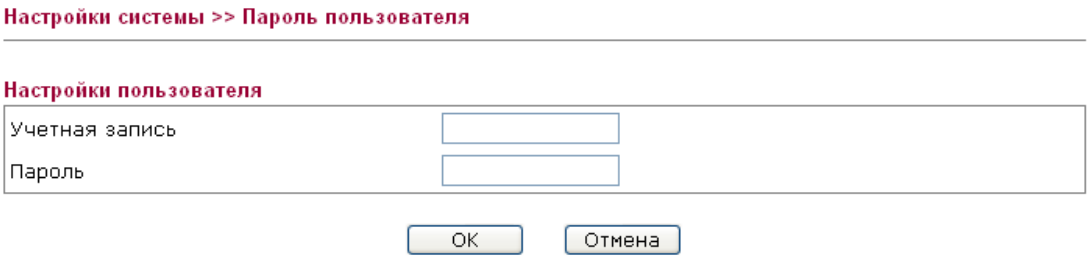


Учетная запись	Введите имя для входа.
Пароль	Введите новый пароль.

Когда вы нажмете **OK**, появится окно **Вход.** Пожалуйста, используйте новый пароль для доступа к странице настроек.

4.7.3 Пароль пользователя

Эта страница позволяет вам установить новый пароль для пользовательских операций.

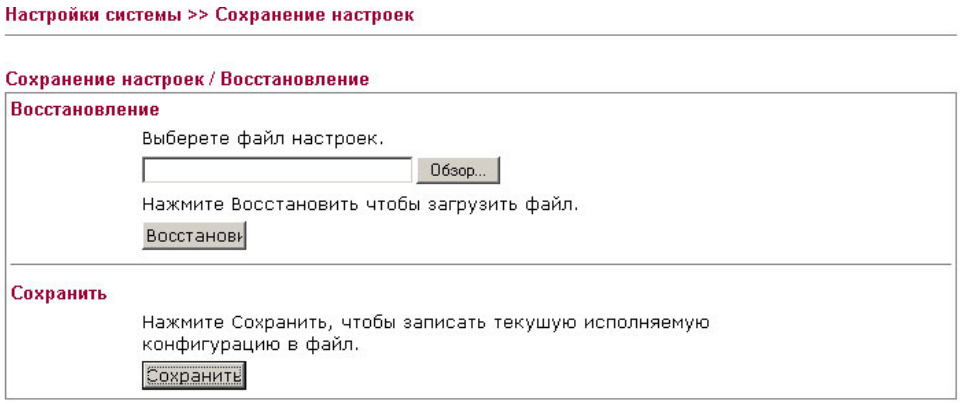


Учетная запись	Введите имя для входа.
Пароль	Введите новый пароль.

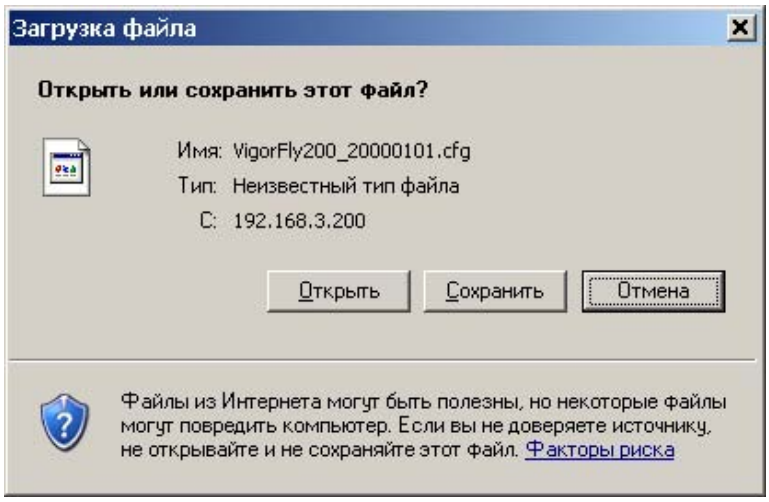
Когда вы нажмете **OK**, появится окно **Вход.** Пожалуйста, используйте новый пароль для доступа к странице настроек.

4.7.4 Сохранение настроек

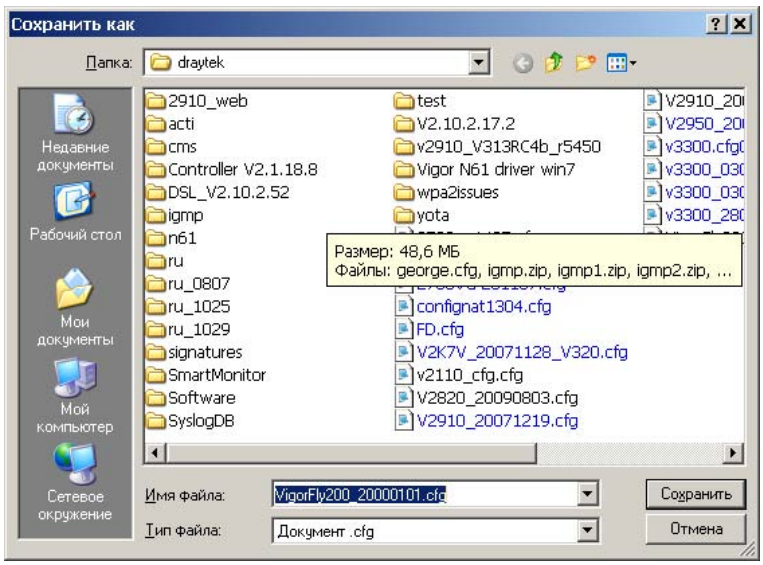
1. Выберите **Настройки системы** >> **Сохранение настроек**. Откроется дополнительное окно как показано ниже.



2. Нажмите кнопку **Сохранить**, чтобы открылось следующее диалоговое окно. Нажмите **Сохранить**, чтобы открыть другое диалоговое окно для сохранения конфигурации как файла.



3. В диалоговом окне **Сохранить как…** имя файла по умолчанию будет **config.cfg**. Вы можете придумать другое имя файла.



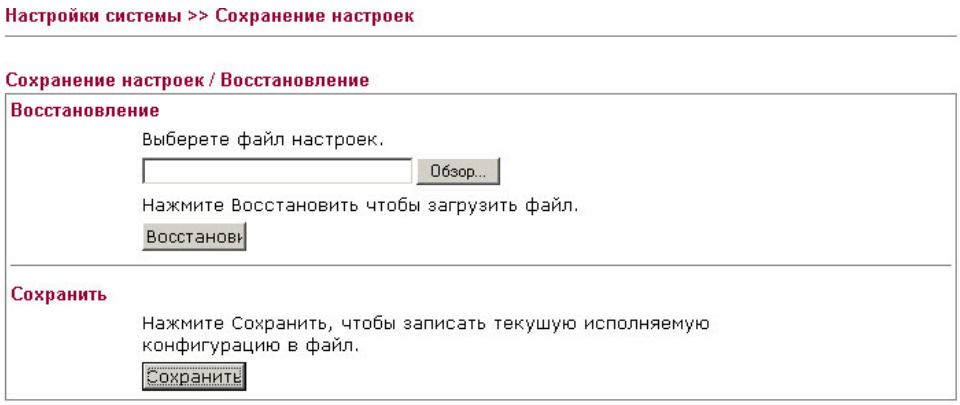
4. Нажмите **Сохранить,** конфигурация автоматически загрузится на ваш компьютер с именем **VigorFly200_20000101.cfg**.

В данном примере использована ОС Windows. В ОС Mac или Linux функция также доступна; будут различаться лишь диалоговые окна.

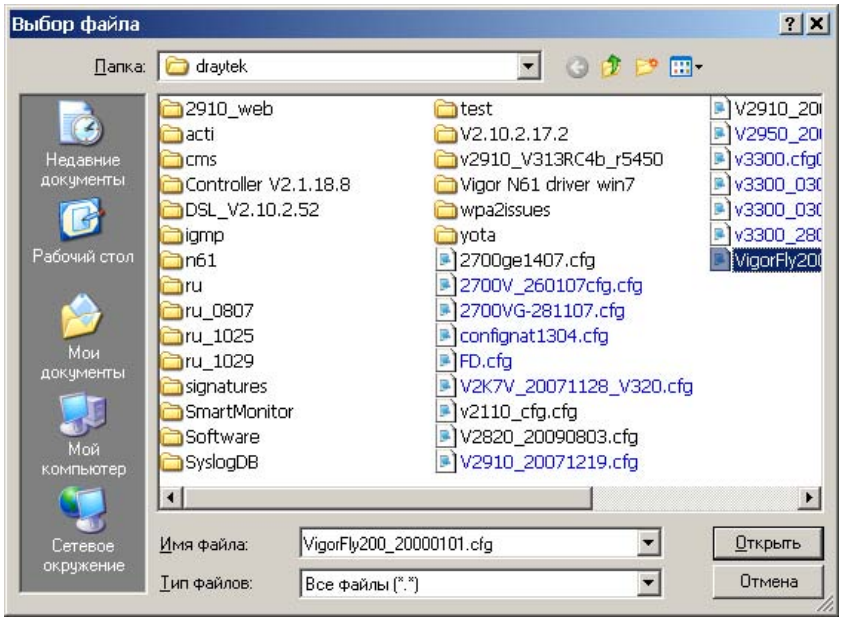
Примечание: Сохранение сертификации должно выполняться отдельно. Сохранение настроек не включает в себя сохранение информации о Сертификате.

Восстановление конфигурации

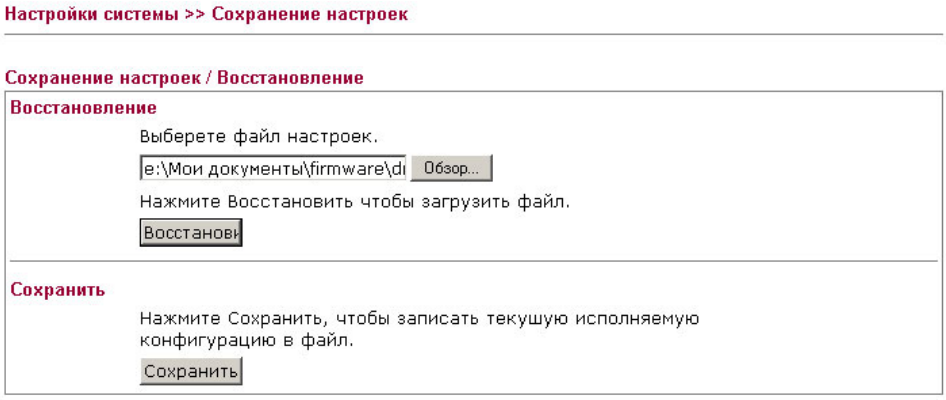
1. Выберите **Настройки системы** >> **Сохранение настроек**. Будет показана следующая страница.



2. Нажмите **Обзор…** чтобы выбрать правильный файл конфигурации для загрузки. Выберите файл с конфигурацией и нажмите **Открыть**

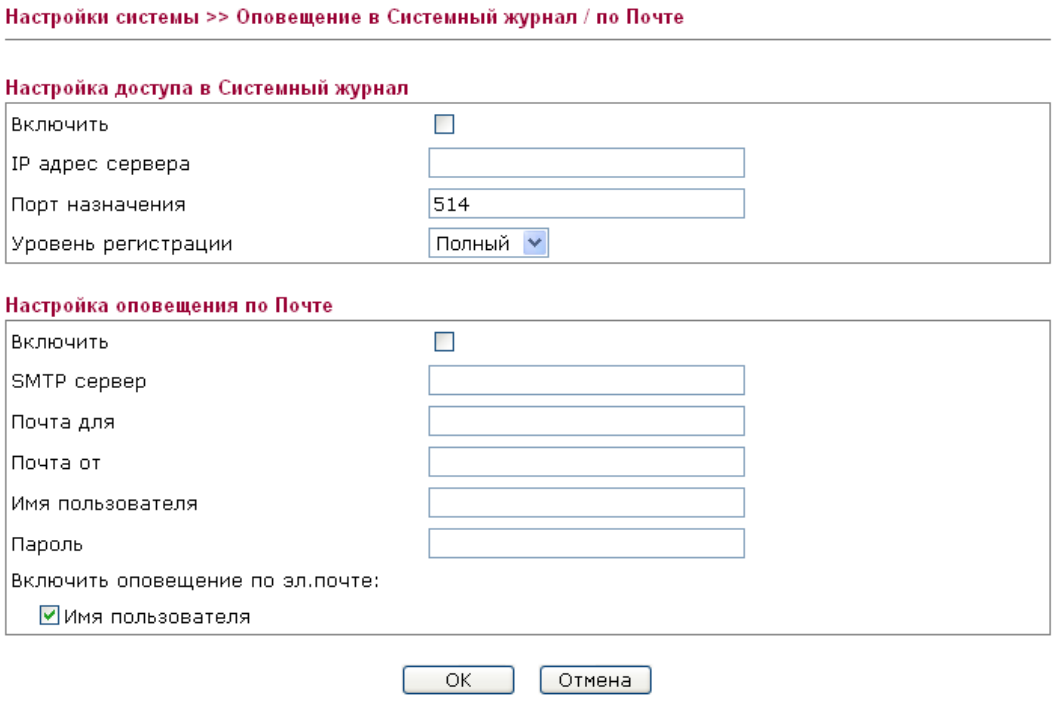


3. Нажмите **Восстановить** и подождите несколько секунд. Появится картинка, сообщающая, что процедура восстановления прошла успешно.

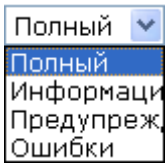


4.7.5 Оповещение Syslog/Почта

Функция **Оповещение в SysLog/Почта** предлагается пользователям для контроля работы маршрутизатора.



Разрешить (настройку доступа к Syslog)	Отметьте **Включить,** чтобы активировать функцию.
IP-адрес сервера	IP-адрес Syslog-сервера.
Порт назначения	Установите порт для протокола Syslog.
Уровень регистрации	Выберите уровни регистрации для сохранения в системный журнал.

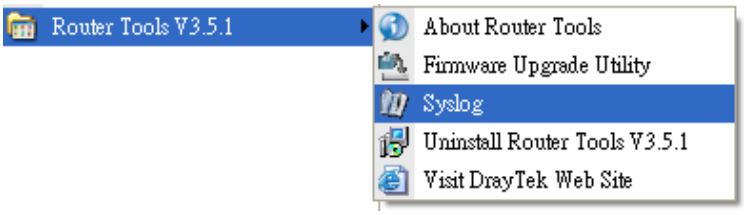


Разрешить (оповещения по почте)	Отметьте **Включить,** чтобы активировать функцию.
SMTP-сервер	IP-адрес SMTP-сервера.
Почта для	Установите почтовый адрес получателя.
Почта от	Установите путь получения отправителя.
Имя пользователя	Введите имя пользователя для идентификации.
Пароль	Введите пароль для идентификации.
Включить оповещение по эл.почте	Отметьте поле **Имя пользователя,** чтобы отправлять оповещения по e-mail в случаях, когда маршрутизатор будет обнаруживать записи, соответствующие вашему запросу.

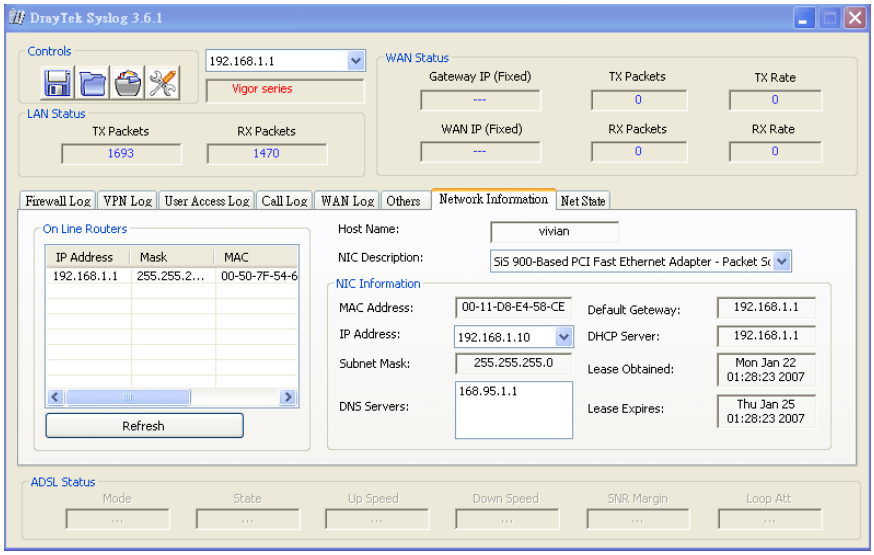
Нажмите **ОК** для сохранения.

Для просмотра Syslog нужно сделать следующее:

1. Установите IP-адрес компьютера-контролера в поле **IP-адрес сервера**.
2. Установите программу Router Tools с прилагающегося диска. После инсталляции выберите **Router Tools>>Syslog** в списке программ.

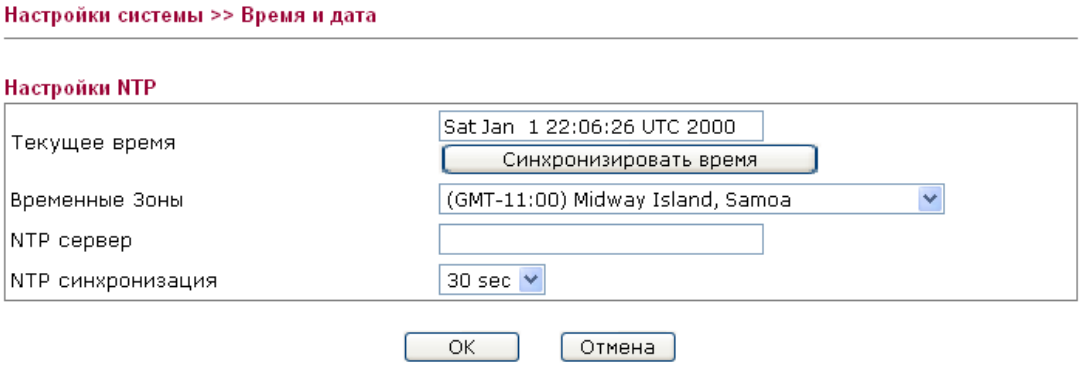


3. В окне Syslog выберите маршрутизатор, за которым вы хотите наблюдать. Во вкладке **Информация о сети** выберите подключенный к маршрутизатору сетевой адаптер. В противном случае, вам не удастся получить информацию от маршрутизатора.



4.7.6 Время и дата

Вы можете установить текущее время.

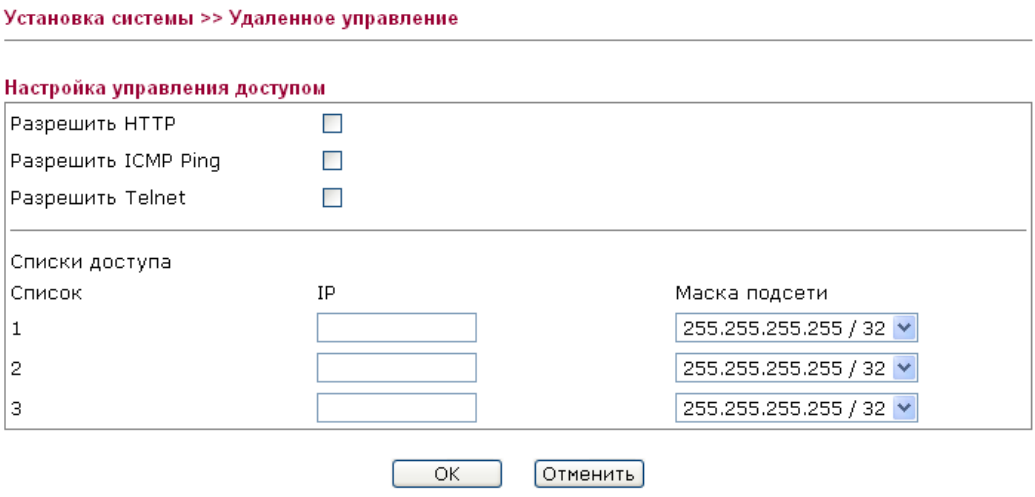


Текущее время	Нажмите **Синхронизировать время.**
Временные Зоны	Выберите ваш часовой пояс.
NTP Сервер	Введите новый NTP сервер.
NTP синхронизация	Введите временной интервал обновлений с NTP-сервера.

Нажмите OK для сохранения.

4.7.7 Управление

Эта страница позволяет вам управлять настройками контроля доступа, списка доступа, протоколами управления. Например, для управления системой контроля доступа, номер порта используется для отправки / получения сообщений сессии.



Разрешить HTTP/ICMP Ping/Telnet	Галочка – чтобы разрешить системным администраторам входить из Интернета. Системой предоставляется несколько серверов для управления маршрутизатором из Интернета. Активируйте функцию для дальнейших настроек.
Списки доступа	Вы можете настроить функцию так, что системный администратор сможет входить только с определенного хоста или из сети, определенной списком. Разрешается

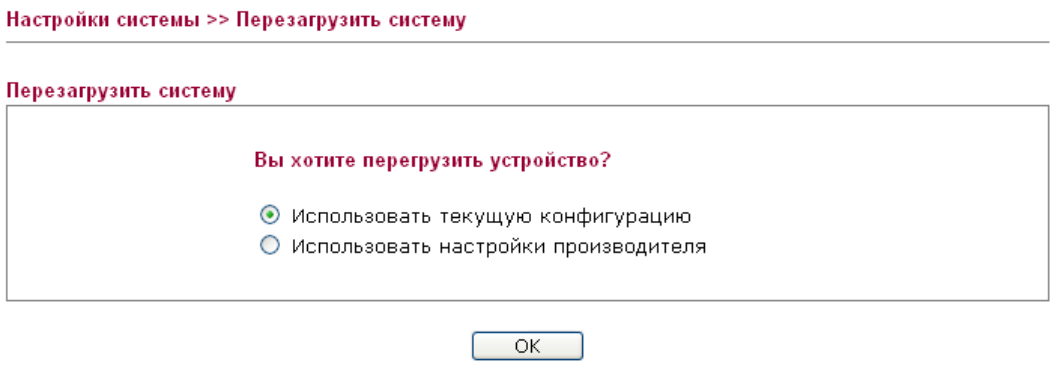
добавить 3 IP/маски подсетей.

Список IP – Показывает IP-адрес с правом доступа к маршрутизатору.

Маска подсети – Отображает маску подсети с правом доступа к маршрутизатору.

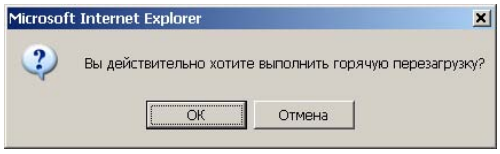
4.7.8 Перезагрузить систему

Веб-конфигуратор может также использоваться для перезагрузки маршрутизатора для начала использования актуальной конфигурации. Выберите **Перезагрузить систему** в меню **Настройка системы**, чтобы открыть следующую страницу:



Нажмите **ОК**. Через 10 секунд маршрутизатор перезагрузит систему.

Примечание: После конфигурации веб-настроек система выдаст сообщение во всплывающем окне Перезагрузить Систему.



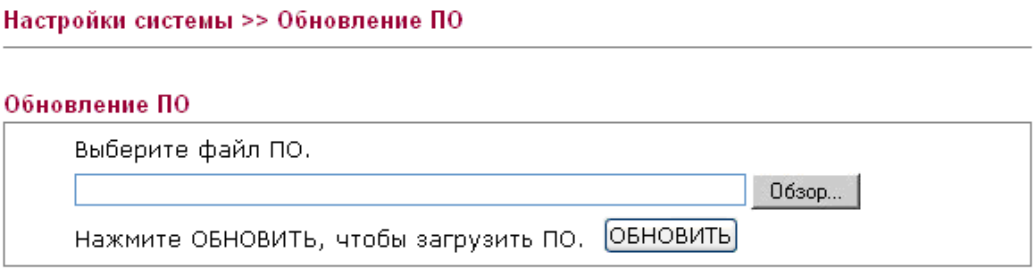
Нажмите ОК для перезагрузки маршрутизатора, чтобы убедиться в нормальной работе и предупредить неожиданные ошибки маршрутизатора в будущем.

4.7.9 Обновление ПО

Перед обновлением вашего ПО, вам необходимо установить Инструменты маршрутизатора. Утилита обновления ПО также входит в набор инструментов. Следующая Интернет-страница поможет вам обновить ПО. Обратите внимание: этот пример для ОС Windows.

Скачайте новое ПО с сайта DrayTek или с FTP. Сайт DrayTek находится по адресу www.draytek.com, FTP – ftp.draytek.com.

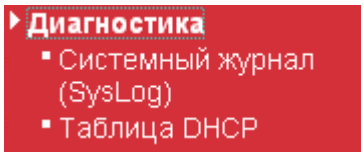
Нажмите **Настройка системы>>Обновление ПО**, чтобы загрузить утилиту обновления ПО.



Нажмите **Обзор...** чтобы определить место хранения нового ПО и нажмите **Обновить.** Не выключайте компьютер во время процесса обновления.

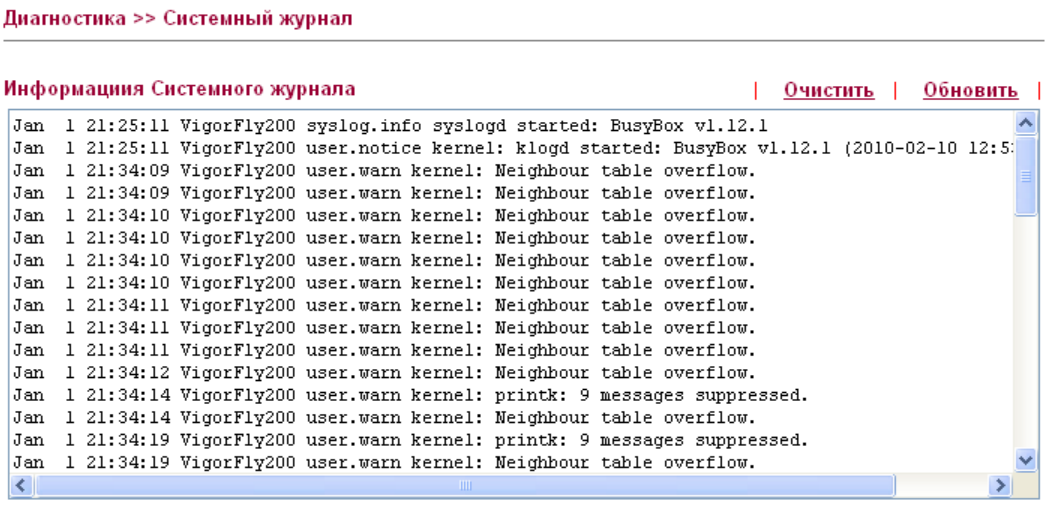
4.8 Диагностика

Функция **Диагностика** предлагает полезный способ проверить статус вашего маршрутизатора. Ниже показано меню **Диагностика**.



4.8.1 Системный журнал (SysLog)

Нажмите **Диагностика>>Системный журнал**, чтобы открыть страницу.

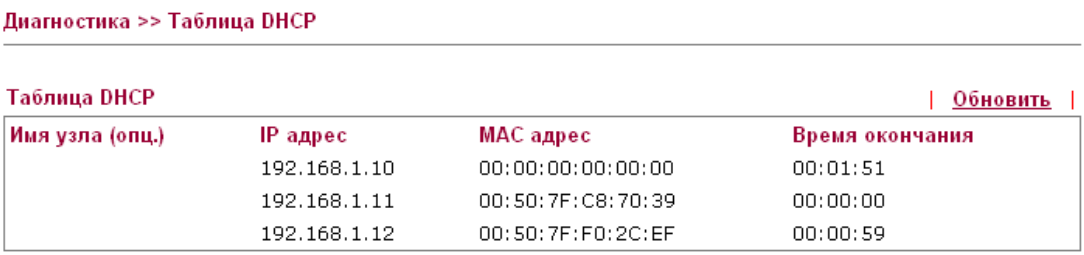


Очистить	Нажмите, чтобы очистить записи.
Обновить	Нажмите, чтобы обновить страницу.

4.8.2 Таблица DHCP

Возможность предоставляет информацию об IP-адресах задач. Эта информация может пригодиться в диагностике сетевых проблем, таких, например, как конфликты IP-адресов.

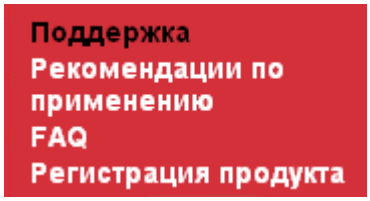
Нажмите **Диагностика>>Таблица DHCP,** чтобы открыть страницу.



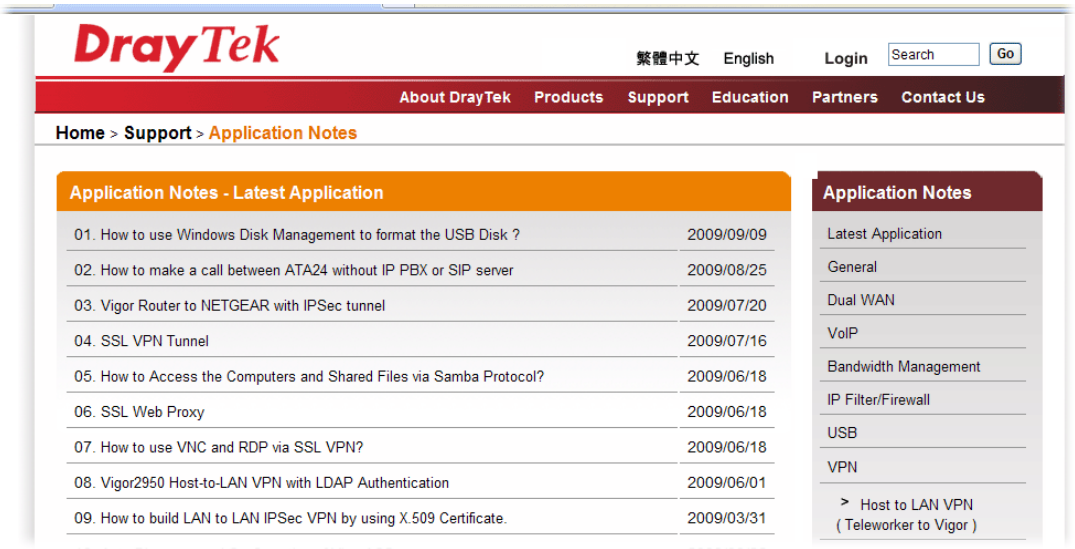
Имя узла	Отображает имя компьютера, принимающее назначенный IP-адрес этого маршрутизатора.
IP-адрес	Отображает IP-адрес, заданный маршрутизатором для определенного ПК.
MAC-адрес	Отображает MAC-адрес для определенного ПК, которому был назначен IP-адрес DHCP.
Время окончания	Отображает время использования определенного ПК.
Обновить	Нажмите, чтобы обновить страницу.

4.9 Поддержка

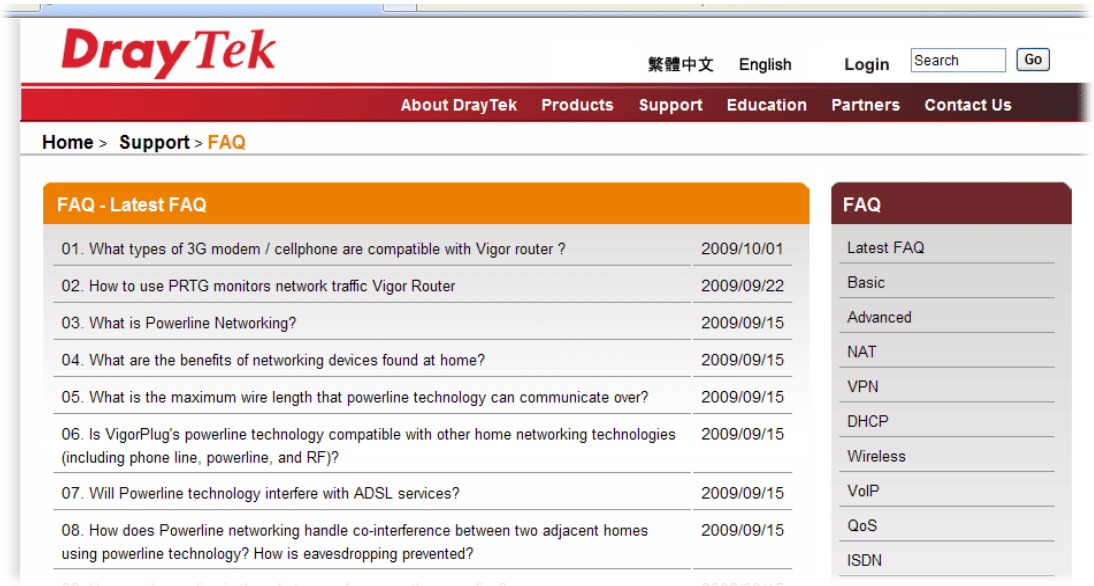
Когда вы выберете какой-либо раздел в меню **Поддержки,** вы будете перенаправлены на соответствующую страницу сайта www.draytek.com.



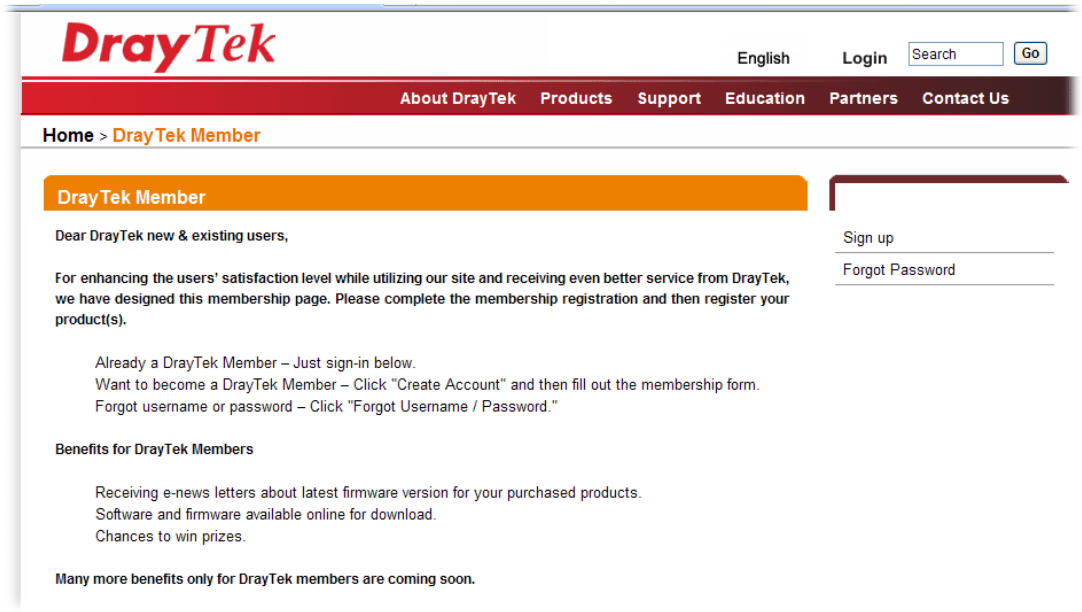
Нажмите **Поддержка>> Замечание по применению,** появится следующая страница.



Нажмите **Поддержка>> FAQ,** появится следующая страница.



Нажмите **Поддержка>> Регистрация продукта,** появится следующая страница.



5 Решение проблем

Эта глава поможет вам справиться с нетипичными ситуациями: если вы, например, не можете выйти в Интернет после установки маршрутизатора и завершения веб-конфигурации. Вам поможет последовательная проверка базового статуса инсталляции:

- Проверка статуса оборудования.
- Проверка настроек сетевых подключений компьютера.
- Проверка маршрутизатора с вашего компьютера (пингование).
- Проверка настроек провайдера.
- Восстановление заводских настроек в случае необходимости.

Если вы сделали всё это, но маршрутизатор по-прежнему не работает, обратитесь за помощью специалистов к дилеру.

5.1 Проверка статуса оборудования

Чтобы проверить статус оборудования:

1. Проверьте адаптер питания и кабели WLAN/LAN подключений. Детальное описание вы найдете в части **1.3 Установка оборудования.**
2. Включите маршрутизатор. Убедитесь в том, что раз в секунду мигает диод ACT, светится диод LAN.

3. Если этого не происходит, значит, что что-то не так со статусом оборудования. Вернитесь в **1.3 Установка оборудования**, чтобы переустановить оборудование.

5.2 Проверка настроек сетевых подключений компьютера

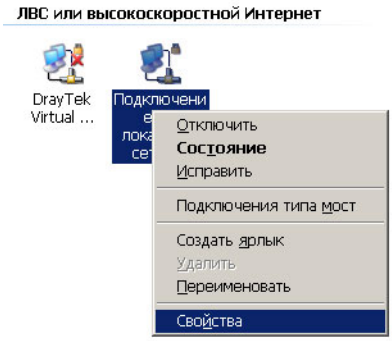
Иногда проблемы с соединением возникают из-за неправильных настроек сетевого подключения. Если проблемы со связью всё ещё не исчезли после применения советов из предыдущего раздела, пожалуйста, выполните действия, приведенные ниже, чтобы убедиться в том, что настройки сетевых подключений в порядке.

ОС Windows

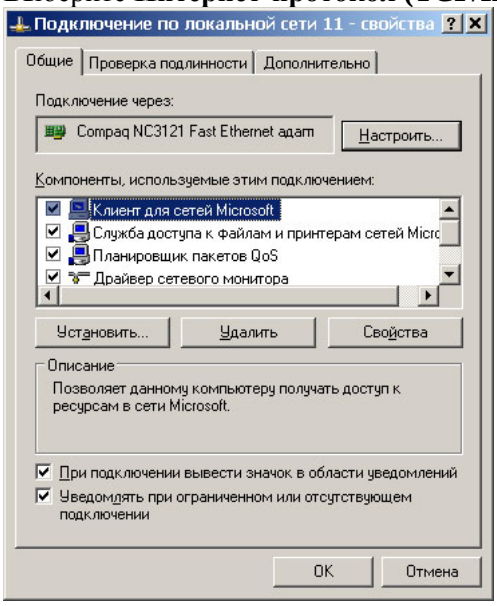
Пример для пользователей ОС Windows XP. Примеры для пользователей других ОС вы можете найти на сайте, **www.draytek.com** в разделе поддержки.

1. Откройте **Панель управления** и двойным щелчком выберите **Сетевые подключения**.

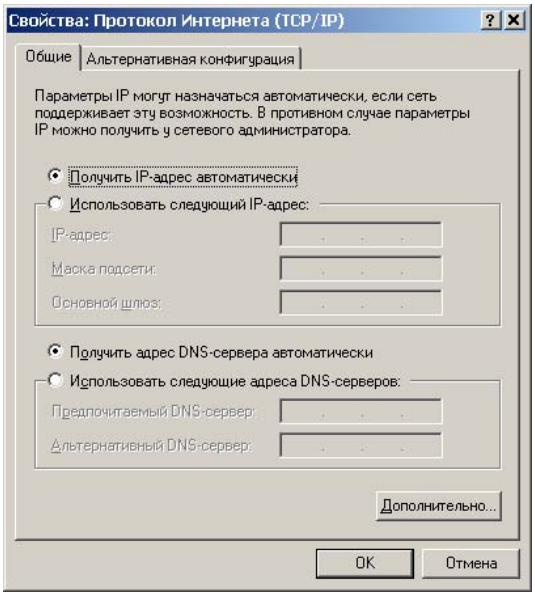
2. Щелкните правой кнопкой мыши по иконке **Подключения по локальной сети** и выберите **Свойства**.



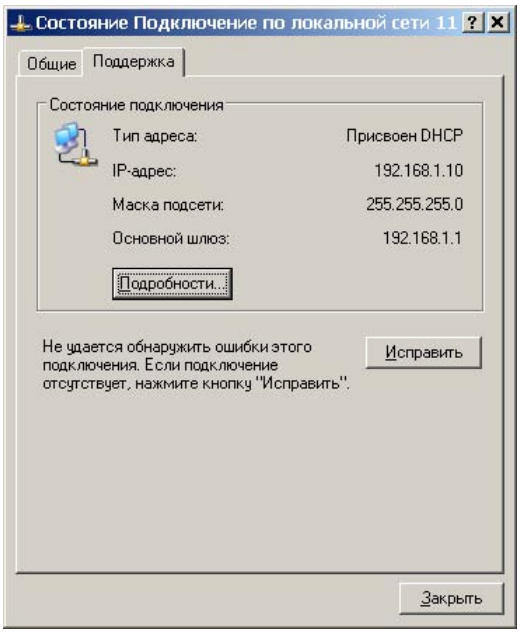
3. Выберите **Интернет-протокол (TCP/IP)** и потом нажмите на кнопку **Свойства.**

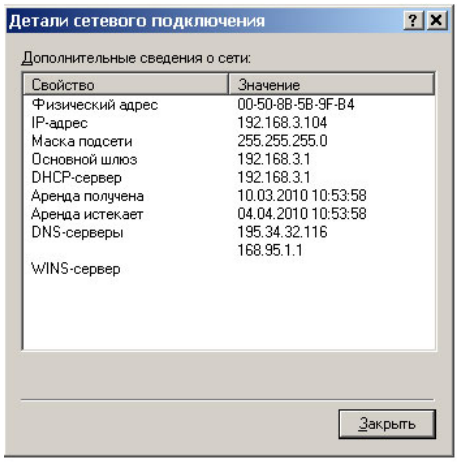


4. Выберите **Получить IP-адрес автоматически** и **Получить DNS-сервер автоматически**.



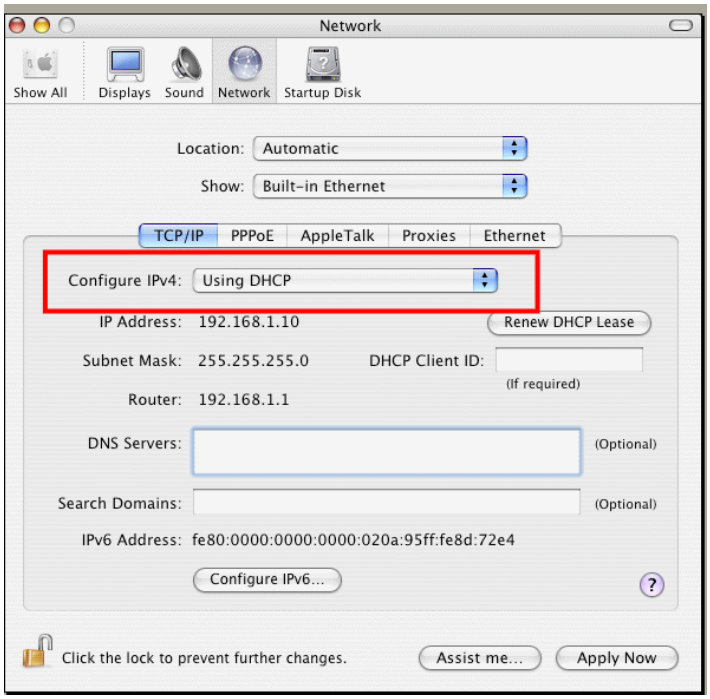
5. Убедитесь, что IP-настройки получены





ОС MacOS

1. Дважды щелкните по используемому MacOS на рабочем столе.
2. Откройте папку **Программы** и войдите в **Сеть.**
3. В окне **Сеть** выберите **Используя DHCP** в выпадающем списке Настройки IPv4.



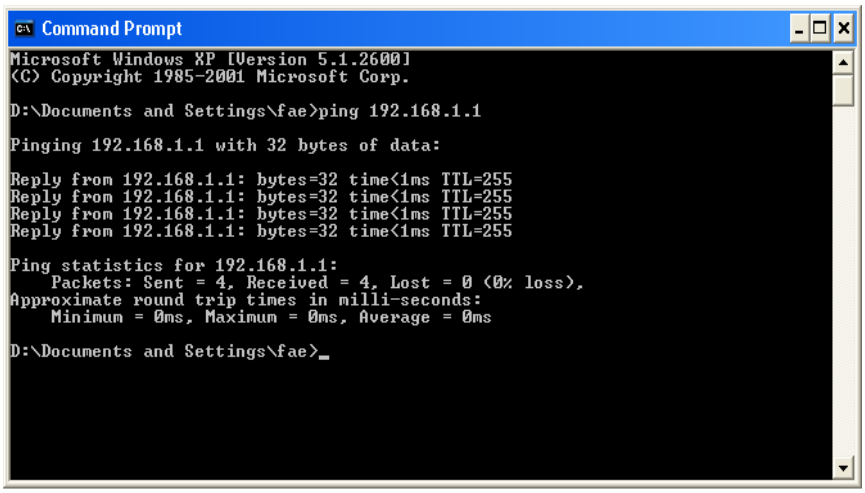
5.3 Проверка маршрутизатора с вашего компьютера (пингование)

IP-адрес шлюза по умолчанию 192.168.1.1. По некоторым причинам вам может понадобиться использование команды «ping» для проверки статуса связи маршрутизатора. **Главное, чтобы компьютер получил ответ с адреса 192.168.1.1.** Если нет, пожалуйста, проверьте IP-адрес вашего компьютера. Мы предлагаем вам установить сетевую настройку **Получить IP автоматически** (см. Главу 5.2)

Пожалуйста, следуйте описанию, чтобы правильно пинговать маршрутизатор.

ОС Windows

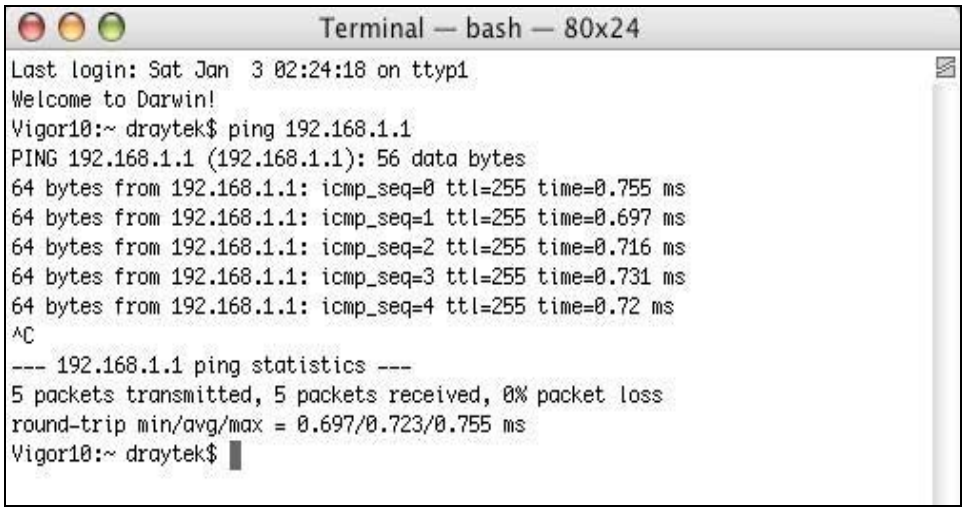
1. Откройте **окно командной строки** (из меню **Пуск>>Выполнить**)
2. Введите **command** (для Windows 95/98/ME) или **cmd** (для Windows NT / 2000/XP/Vista). Появится диалоговое окно команд DOS.



3. Введите **ping 192.168.1.1** и нажмите [Enter]. Если связь в порядке, появится строчка **“Reply from 192.168.1.1:bytes=32 time<1ms TTL=255”**.
4. Если строка не появляется, проверьте настройки IP-адреса вашего компьютера.

MacOS (Терминал)

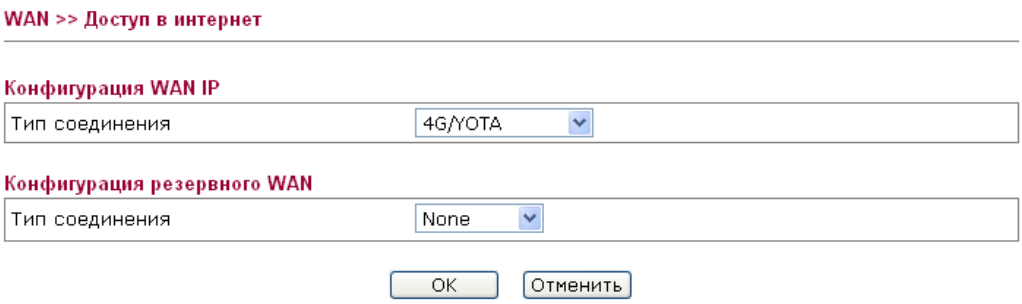
1. Дважды щелкните по используемому MacOS на рабочем столе.
2. Откройте папку **Программы** и войдите в **Служебные программы**.
3. Дважды кликните по иконке **Терминал**. Появится окно Терминал.
4. Введите **ping 192.168.1.1** и нажмите [Enter]. Если связь в порядке, появится строчка **“64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms”**.



5.4 Проверка настроек провайдера

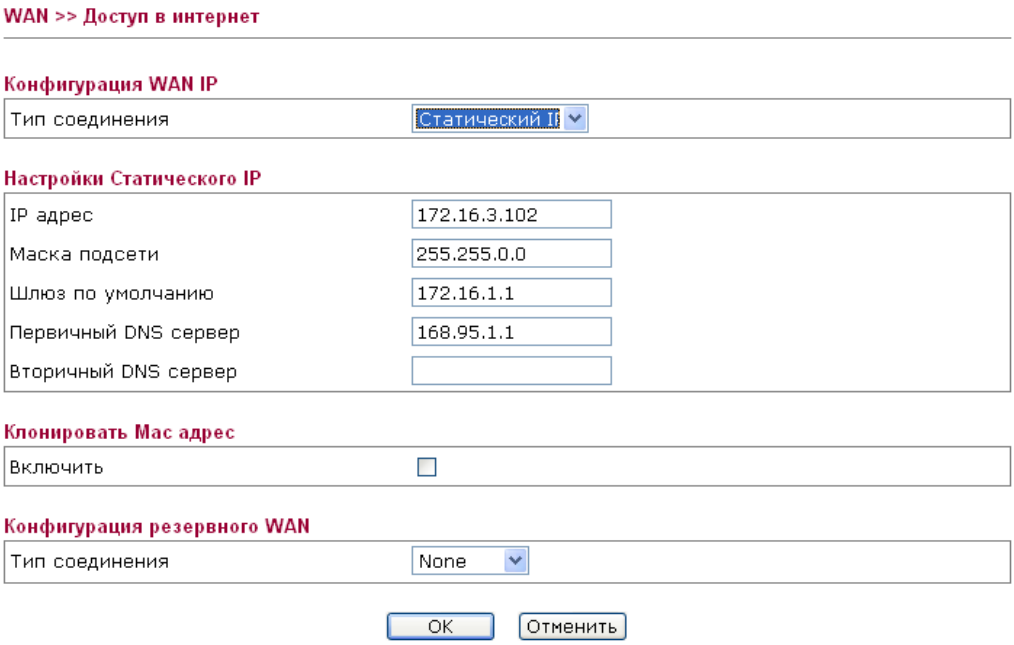
Откройте **WAN>> Доступ в интернет** и проверьте настройки провайдера. Используйте выпадающий список **Тип Подключения**, чтобы выбрать 4G/YOTA или Static IP/DHCP/PPPoE/PPTP/L2TP для проверки ранее введенных настроек.

Для 4G/YOTA



Для статических пользователей

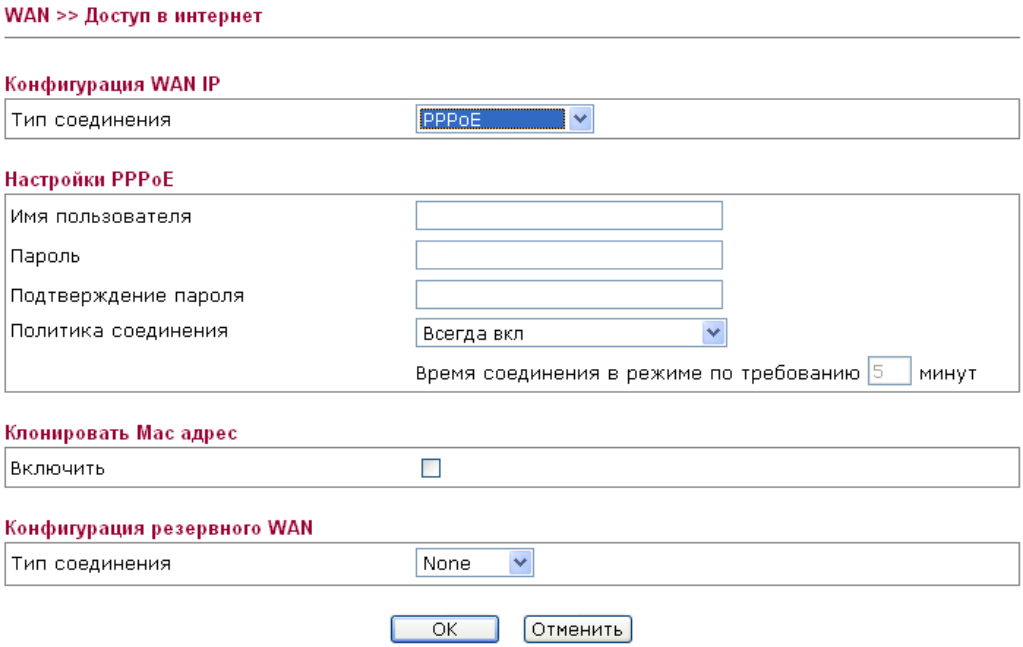
1. Выберите **Статический IP** в качестве типа подключения.



2. Проверьте **IP-адрес, IP маски** и **IP** (они должны определяться вашим провайдером).

Для пользователей PPPoE

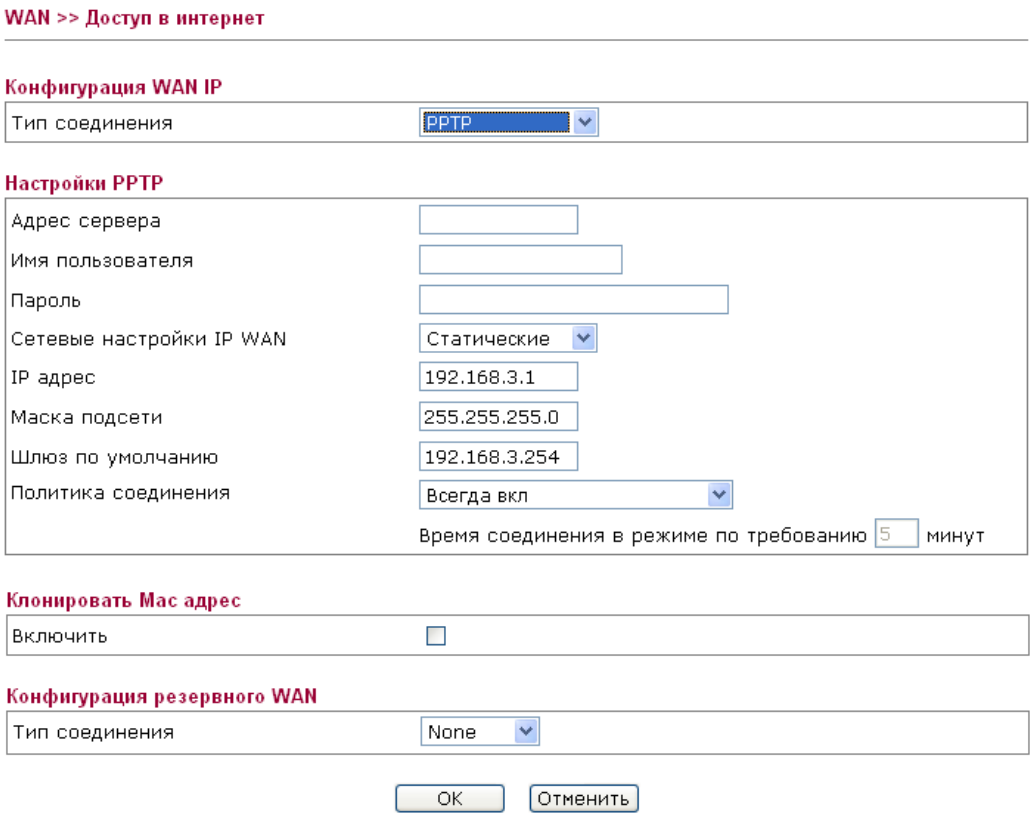
1. Используйте **PPPoE** в качестве типа подключения.



2. Проверьте **Имя пользователя** и **Пароль** (они должны определяться вашим провайдером).

Для пользователей PPTP/L2TP

1. Выберите **PPTP/L2TP** в качестве типа подключения.



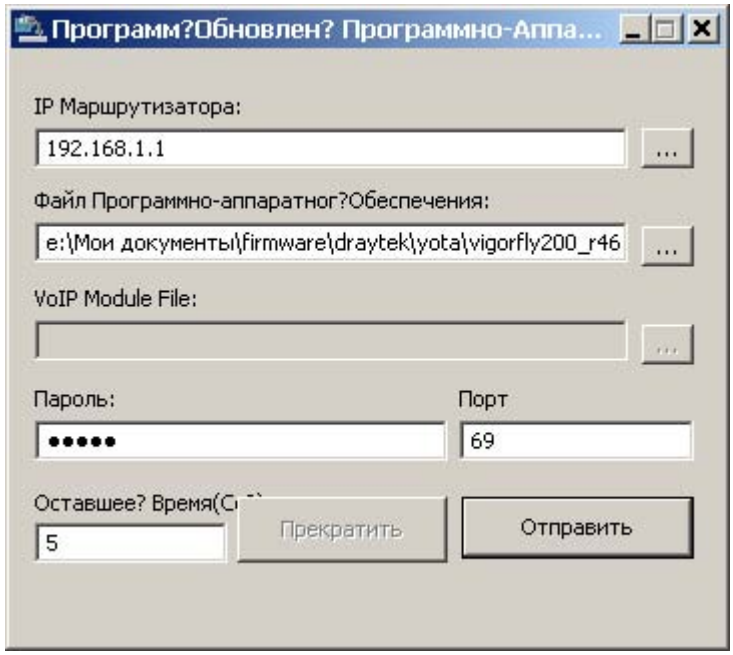
2. **Имя пользователя, Пароль, IP-адрес, Маска подсети** должны быть правильными значениями, которые вы получили от вашего провайдера.

5.5 Перевод маршрутизатора в TFTP режим для обновления ПО

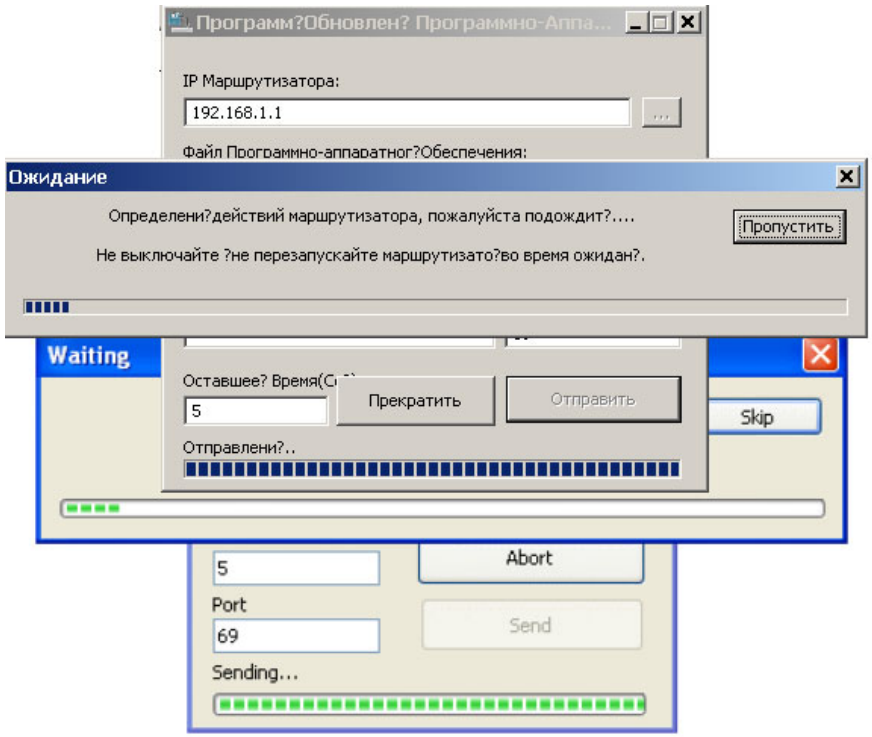
1. Смените IP-адрес вашего ПК на 192.168.1.10.
2. Откройте утилиту **Обновление ПО (Firmware upgrade utility)** и вручную введите IP маршрутизатора 192.168.1.1 (если оно не установлено установите с компакт диска прилагаемого в комплекте ПО Router Tools) .
3. Укажите размещение обновления.

> **Примечание:** Есть два типа обновлений. Формат обновлений *.rst* восстановит настройки по умолчанию после обновления ПО. Формат *.all* оставит предыдущую конфигурацию после обновления ПО.

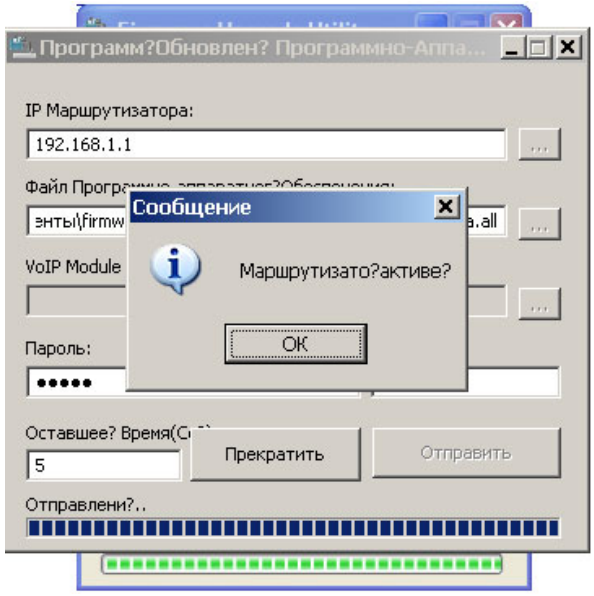
4. Введите **Пароль**, если вы устанавливали пароль ранее.
5. Нажмите и держите кнопку **Factory Reset** на маршрутизаторе. Выключите и включите питание.
6. Отпустите кнопку **Factory Reset**, когда индикатор ACT будет мигать с частотой 1 раз в 5 секунд.
7. нажмите **Отправить**.



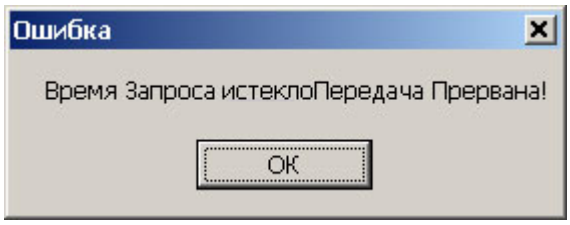
8. Так выглядит панель, показывающая процесс обновления.



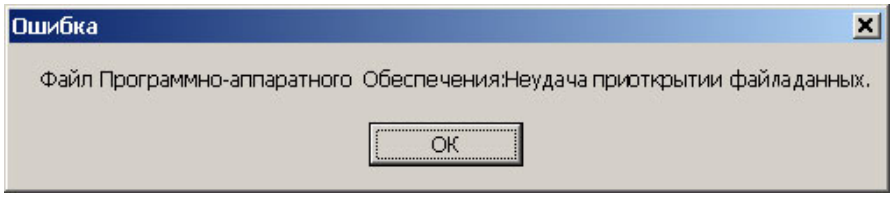
9. Когда обновление ПО успешно завершится, появится следующее окно.



Если появится сообщение «**Время запроса истекло. Передача прервана!»**, проверьте, активно ли подключение между компьютером и маршрутизатором.



Если появится сообщение об ошибке **«Файл программно-аппаратного обеспечения: Неудача при открытии файла данных»**, убедитесь, правильно ли вы указали путь файлу с ПО для вашего маршрутизатора.



Примечание: Пожалуйста, отключите брандмауэр на время обновления ПО, если вы используете ОС Windows Vista. Брандмауэр можно выключить в меню **Панель управления >> Центр безопасности >> Брандмауэр.**

5.6 Восстановление заводских настроек в случае необходимости

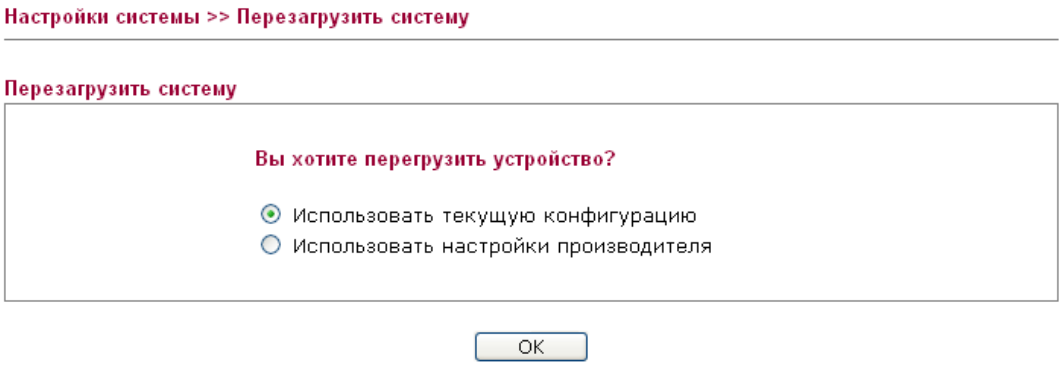
Иногда неправильное подключение можно исправить, восстановив заводские настройки. Попробуйте сбросить настройки маршрутизатора с помощью ПО или оборудования.

Предупреждение: После нажатия **Восстановить заводские настройки по умолчанию** вы потеряете все ранее введенные настройки. Убедитесь в том, что вы сохранили все необходимые настройки.

Сбросить с помощью ПО

Вы можете восстановить настройки по умолчанию с помощью веб-страницы.

Выберите **Настройки системы>>Перезагрузить систему.** Появится следующий экран. Выберите **Использовать настройки производителя** и нажмите **ОК.** Через несколько секунд маршрутизатор вернет заводские настройки.



Сброс настроек оборудования

Во время работы маршрутизатора (мигает диод ACT) нажмите кнопку **Factory Reset** и держите ее больше 10 секунд. Когда вы увидите, что диод ACT быстро мигает, отпустите кнопку. Маршрутизатор восстановит настройки по умолчанию.

После восстановления всех заводских настроек по умолчанию вы снова можете сконфигурировать настройки маршрутизатора в соответствии с вашими требованиями.

5.7 Обратитесь к дилеру

Если после использования всех вышеописанных советов маршрутизатор всё ещё не работает правильно, обратитесь к вашему дилеру за дальнейшей помощью. По любым вопросам вы можете написать на адрес support@atg.ru.