BELKIN®

Модем ADSL2+ с беспроводным маршрутизатором Wireless G

802.11g

Руководство пользователя

F5D7632ru4A

Содержание

Введение

Благодарим вас за покупку модема Belkin ADSL2+ с маршрутизатором Wireless G (далее: "маршрутизатор")! С новым маршрутизатором уже через считанные минуты у вас будет совместный доступ к Интернет-подключению и сетевая связь между компьютерами. Ниже описаны характеристики маршрутизатора, которые делают его идеальным выбором для домашних сетей и сетей малого офиса. Ознакомьтесь, пожалуйста, с данным "Руководством пользователя" и обратите особое внимание на Приложение Б "Что учесть при размещении и настройке".

Характеристики устройства

Совместимость как с ПК, так и с компьютерами Mac®

Маршрутизатор поддерживает разнообразные сетевые среды, включая Mac OS® 8.x, 9.x, X v10.x, AppleTalk®, Linux®, Windows® 95, 98SE, Me, NT®, 2000, XP, Vista и другие. Нужно иметь обозреватель Интернет и сетевой адаптер, поддерживающий TCP/IP (стандартный язык Интернет).

Индикаторы на лицевой панели

Светодиодные индикаторы на лицевой панели маршрутизатора показывают, какие его функции сейчас активны. Благодаря им можно сразу понять, подключен ли маршрутизатор к Интернет. Это избавляет от необходимости использовать специальные программы и процедуры слежения за состоянием сети.

Расширенный пользовательский Web-интерфейс

Дополнительные функции маршрутизатора легко настроить через Web-обозреватель, без необходимости устанавливать на компьютер специальные программы. Не нужны установочные диски, не нужно их хранить и, главное, есть возможность быстро и легко менять и применять функции настроек с любого компьютера сети.

Встроенный 10/100 коммутатор с 4 портами

У маршрутизатора есть встроенный 4-портовый сетевой коммутатор, обеспечивающий подключенным к сети компьютерам возможность совместного доступа к принтерам, данным и MP3-файлам, цифровым фотографиям и многим другим ресурсам. Коммутатор оснащен системой автоматического определения, то есть настройки на скорость подключенных устройств. Коммутатор обеспечивает одновременную передачу данных между компьютерами и сетью Интернет без прерываний и потребления дополнительных ресурсов.

Встроенный беспроводной узел доступа 802.11g

802.11g - удивительная новая технология беспроводной связи со скоростью передачи данных до 54 Мбит/сек, что почти в пять раз быстрее стандарта 802.11b.

Встроенный протокол динамической конфигурации сетевого узла (DHCP)

Встроенный протокол динамической конфигурации сетевого узла (Built-In Dynamic Host Configuration Protocol; DHCP) обеспечивает самое простое подключение к сети. DHCP-сервер автоматически присваивает каждому компьютеру IP-адрес, благодаря чему нет нужды в сложных сетевых настройках.

Совместное использование NAT IP-адреса

Маршрутизатор использует транслятор сетевых адресов (Network Address Translation; NAT) для совместного использования одного и того же IP-адреса, присвоенного поставщиком услуг Интернет, и тем самым избавляет от затрат на дополнительные IP-адреса учетной записи у поставщика этих услуг.

SPI-брандмауэр

Маршрутизатор оснащен брандмауэром, защищающим сеть от многих распространенных способов взлома, включая IP Spoofing, Land Attack, Ping of Death (PoD), Denial of Service (DoS), IP нулевой длины, Smurf Attack, TCP Null Scan, SYN flood, UDP flooding, Tear Drop Attack, ICMP defect, RIP defect и Fragment Flooding.

Фильтрация MAC-адресов

Для дополнительной защиты можно задавать список MAC-адресов (уникальных идентификаторов пользователей), которым разрешен доступ к сети. У каждого компьютера есть собственный MAC-адрес. Достаточно ввести эти MAC-адреса в список с помощью пользовательского Web-интерфейса – и вы сможете управлять доступом к вашей сети.

Совместимость с протоколом Universal Plug-and-Play (UPnP)

Протокол UPnP (Universal Plug-and-Play) – технология, обеспечивающая прямую работу систем речевых и видеосообщений, игр и других приложений, поддерживающих стандарт UPnP.

Поддержка сквозного доступа к VPN

При соединении с учрежденческой сетью из дома через подключение к VPN маршрутизатор обеспечит компьютеру с VPN сквозной вход через маршрутизатор в учрежденческую сеть.

Преимущества домашней сети

Руководствуясь нашими простыми указаниями по установке домашней сети Belkin, вы сможете:

- Использовать для всех домашних компьютеров одно и то же высокоскоростное подключение к Интернет
- Получать на всех соединенных домашних компьютерах совместный доступ к таким ресурсам, как файлы и жесткие диски
- Всей семьей использовать один и тот же принтер
- Использовать совместный доступ к документам, музыке, видео и цифровым изображениям
- Хранить, считывать и копировать файлы с одного компьютера на другой
- Одновременно играть в режиме онлайн, проверять электронную почту и общаться в Интернет

Преимущества беспроводной сети Belkin

Мобильность — нет нужды в специальном "компьютерном кабинете" — отныне можно работать на любом подключенном к сети ноутбуке или настольном компьютере в радиусе покрытия беспроводной связи

Простота установки — Мастер простой установки Belkin делает подключение очень легким

Гибкость — доступ к принтерам, компьютерам и другим сетевым устройствам можно настраивать из любой точки дома

Простота расширения — широкий ряд сетевой продукции компании Belkin позволяет легко расширять сеть и подключать к ней такие устройства, как принтеры или игровые приставки

Никаких кабелей — никаких затрат и неудобств, обычно возникающих при прокладке кабелей Ethernet дома или на работе

Широкая отраслевая совместимость — возможность выбора оборудования из широкого ряда взаимосовместимой сетевой продукции

Убедитесь, что есть все необходимое

Содержимое комплекта

- Модем ADSL2+ с беспроводным маршрутизатором Wireless G
- Телефонный шнур RJ11 – серый
- Сетевой кабель RJ45 Ethernet – желтый
- Микрофильтр* ADSL
- Блок питания
- Компакт-диск с Руководством пользователя и программным обеспечением Помощник при установке

*Микрофильтры ADSL различаются в зависимости от страны. Если микрофильтр не включен в комплект, его нужно приобрести.

Системные требования

- Работающее ADSL-соединение и телефонная розетка для подключения маршрутизатора
- По крайней мере один компьютер с установленными и правильно настроенными платой сетевого интерфейса и Web-обозревателем
- Сетевой протокол TCP/IP на каждом компьютере, подключенном к маршрутизатору
- Отсутствие в локальной сети других DHCP-серверов, способных назначать IP-адреса компьютерам или устройствам

Системные требования программного обеспечения Помощник при установке

- ПК под управлением Windows® 2000, XP или Vista™
- Процессор не ниже 500 МГц и не менее 128 Мб оперативной памяти
- Web-обозреватель

Параметры подключения к Интернет

Помощник при установке содержит базу данных поставщиков услуг Интернет во всех странах и помогает быстро настроить маршрутизатор. Если в списке нет вашего поставщика услуг интернет, перед настройкой маршрутизатора получите от своего поставщика услуг следующие данные:

• Протокол подключения к Интернет: (PPPoE, PPPoA, динамический IP, статический IP)

• Мультиплексирование или инкапсуляция: (LLC или VC MUX)

• Виртуальный канал: VPI (идентификатор виртуального пути) _____
(число от 0 до 255)

• VCI (идентификатор виртуального канала) _____
(число от 1 до 65535)

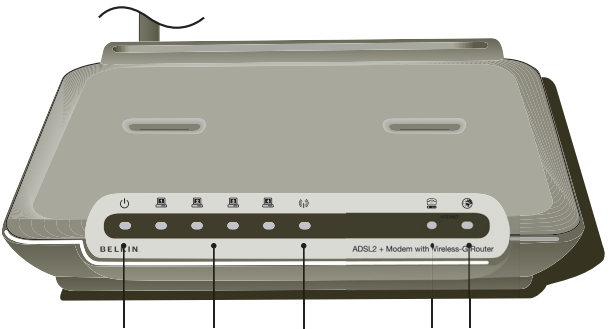
• Для пользователей PPPoE и PPPoA: Учетная запись пользователя ADSL и пароль _____

• Для пользователей со статическим IP: IP-адрес ___ . ___ . ___ . ___
Маска подсети ___ . ___ . ___ . ___
Шлюзовой сервер по умолчанию ___ . ___ . ___ .

• IP-адрес сервера доменных имён (DNS) ___ . ___ . ___ . ___
(если предоставляется поставщиком услуг)

Ознакомление с маршрутизатором

Маршрутизатор разработан для настольного размещения. Для удобства разъемы всех кабелей находятся на задней панели маршрутизатора. Наглядные индикаторы на лицевой панели маршрутизатора отображают данные о текущем состоянии и активности сети.



Индикатор питания

Индикатор состояния локальной сети (1-4)

Индикатор ADSL

Индикатор Интернет

Индикатор состояния беспроводной локальной сети

Передняя панель

На иллюстрации ниже показана лицевая панель маршрутизатора:

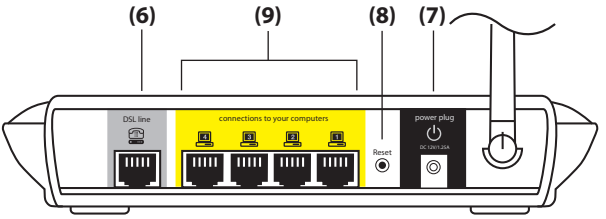
Светодиодные индикаторы

Девять индикаторов на лицевой панели маршрутизатора описаны в таблице на следующей странице (слева направо):

Светодиодные индикаторы	Цвет	Состояние	Описание
ADSL			
	Зеленый	ВЫКЛ.	Отсутствует питание или линия ADSL физически отсоединена
		Мигающий	Идет процесс установления связи или подготовка устройств
		Ровный	Подключение по линии ADSL установлено
Беспроводная связь			
	Зеленый	ВЫКЛ.	Отключено питание или отсутствует радиосигнал (отсутствует или не работает WLAN-карта)
		Мигающий	Через интерфейс беспроводной локальной сети поступает поток данных
		Ровный	Интерфейс беспроводной локальной сети готов к работе
Интернет			
	Зеленый	ВЫКЛ.	Нет подключения к Интернет
		Мигающий	Передача или прием данных
		Ровный	Есть подключение к Интернет
LAN 1-4			
Локальная сеть 1 -4	Зеленый	ВЫКЛ.	Отключено питание или отсутствует несущая Ethernet
		Мигающий	Присутствует несущая Ethernet и через Ethernet-порт поступают данные пользователя
		Ровный	Присутствует несущая Ethernet
Power			
	Зеленый	ВЫКЛ.	Питание отключено
		Ровный	Питание включено

Задняя панель

На рисунке ниже показана задняя панель маршрутизатора:



Разъем питания — К этому гнезду нужно подключить прилагаемый блок питания. Использование неподходящего блока питания может повлечь поломку маршрутизатора.

Порты Ethernet —Ethernet-порты RJ45, 10/100 с автоматическим согласованием скорости. Порты помечены числами от 1 до 4, соответствующими нумерации индикаторов на лицевой панели маршрутизатора. К этим портам подключаются компьютеры сети и другие сетевые устройства.

Линия ADSL —Этот порт предназначен для подсоединения к линии ADSL. Подключите к нему свою ADSL-линию.
Кнопка "Reset" —Кнопка "Reset" ("Сброс") используется в редких случаях, при неправильной работе маршрутизатора. Сброс установок маршрутизатора восстанавливает его нормальную работу с сохранением запрограммированных настроек. Кроме того, с помощью кнопки "Reset" ("Сброс") можно восстановить заводские настройки по умолчанию. Восстановление этих настроек можно использовать в случаях, когда забыт заданный пароль.

а) Сброс установок маршрутизатора
Прижмите кнопку "Reset" ("Сброс") на одну секунду, затем отпустите. Сброс будет завершен, когда индикатор питания/готовности вновь начнет светиться ровно.

б) Восстановление заводских настроек
Прижмите кнопку "Reset" ("Сброс") на 20 секунд, затем отпустите. Восстановление будет завершено, когда индикатор питания/готовности вновь начнет светиться ровно.

Подключение и настройка маршрутизатора

Помощник при установке

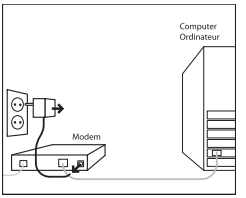
Для простой и быстрой установки маршрутизатора компания Belkin предлагает программное обеспечение Помощник при установке. С его помощью маршрутизатор начнет работу уже через считанные минуты. Для работы Помощника при установке необходимо, чтобы компьютер (под управлением Windows 2000, XP или Vista™) был подключен непосредственно к ADSL и в процессе установки было активным подключение к Интернет. В остальных случаях для настройки маршрутизатора следует использовать дополнительный способ установки (см. соответствующий раздел данного руководства пользователя). При использовании операционной системы, отличной от Windows 2000, XP или Vista либо Mac OS X, настройку маршрутизатора также следует проводить с помощью раздела “Дополнительный способ установки” данного руководства пользователя.

Шаг 1-A: Подключение оборудования – Указания Краткого руководства к установке

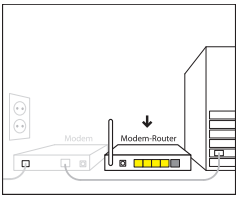
Подключение нового маршрутизатора

Следуйте данным указаниям, если НЕ ПРОВОДИТЕ замену существующего модема. При замене существующего модема перейдите к следующему разделу (“Замена существующего модема или модема-маршрутизатора”, см. стр. 9).

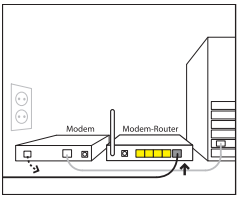
1-A.1 Извлеките новый маршрутизатор из упаковки и разместите рядом с компьютером. Поднимите антенну маршрутизатора.



1-A.2 Возьмите желтый кабель RJ45, прилагаемый к маршрутизатору. Подключите один его конец к любому желтому порту с пометкой “Wired Computers” (проводное подключение к компьютерам) на задней панели маршрутизатора. Затем подключите другой конец кабеля к сетевому порту на задней панели компьютера. [Insert Ethernet logo]

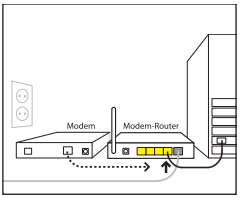


1-A.3 Возьмите прилагаемый серый телефонный шнур RJ11. Подключите один его конец к серому порту с пометкой “DSL” на задней панели маршрутизатора. Затем подсоедините другой конец шнура к ADSL-подключению (настенному гнезду или ADSL-разветвителю).



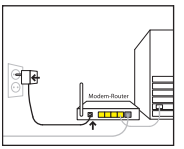
Примечание: Некоторые разъемы ADSL требуют микрофильтра. О том, нужен ли он вам, следует узнать у поставщика услуг ADSL. Компания Belkin прилагает микрофильтр при продажах в тех регионах, где он требуется. Чтобы определить, нужен ли микрофильтр, обратитесь к руководству пользователя, предоставленному поставщиком услуг ADSL.

1-А.4 Подключите блок питания маршрутизатора к черному порту с пометкой “Power” (“Питание”) на задней панели. Подождите 20 секунд, пока маршрутизатор загрузится. Проверьте индикацию на лицевой панели маршрутизатора. Убедитесь, что индикаторы “Wired” (“Проводное подключение”) и “Modem-Router” (“Модем-маршрутизатор”) светятся зеленым цветом. В противном случае проверьте соединения.

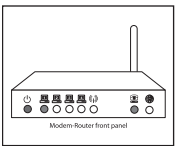


Шаг 1-Б: Замена существующего модема или модема-маршрутизатора

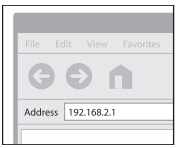
Следуйте данным указаниям, если у вас уже есть модем или модем-маршрутизатор, который предстоит заменить новым маршрутизатором.



1-Б.1 **Извлеките** новый маршрутизатор из упаковки и разместите рядом с прежним модемом. Поднимите антенну маршрутизатора. Отсоедините шнур питания старого модема.



1-Б.2 Найдите кабель, соединяющий прежний модем с компьютером. Отсоедините этот кабель от старого модема и подключите к любому желтому порту с пометкой “Wired Computers” (проводное подключение к компьютерам) на задней панели нового маршрутизатора.



1-Б.3 Найдите кабель, соединяющий прежний модем с настенным гнездом ADSL. Отсоедините его от старого модема и подключите к серому порту с пометкой “DSL” на задней панели маршрутизатора.

1-Б.4 Подключите блок питания маршрутизатора к черному порту с пометкой “Power” (“Питание”) на задней панели.

1-Б.5 **Подождите** 20 секунд, пока маршрутизатор загрузится. Проверьте индикацию на лицевой панели маршрутизатора. Убедитесь, что индикаторы “ADSL” и “LAN” (“Локальная сеть”) светятся зеленым цветом. В противном случае проверьте соединения.

Шаг 2: Настройка маршрутизатора – Запуск Помощника при установке

2.1 Закройте на компьютере все работающие программы. Отключите брандмауэр и программы совместного использования Интернет-соединения.

2.2 Вставьте компакт-диск. В течение 15 секунд на экране автоматически появится Помощник при установке (Setup Assistant). Чтобы запустить Помощник при установке, нажмите “Go” (“Пуск”). Следуйте дальнейшим указаниям.

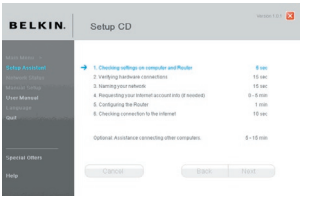
ВАЖНОЕ ЗАМЕЧАНИЕ: Запускайте Помощник при установке на компьютере, подключенном непосредственно к маршрутизатору (Шаг 1-A.2).

Примечание для пользователей Windows: Если Помощник при установке не запустился автоматически, нажмите “Мой компьютер”, перейдите на дисковод для компакт-дисков и дважды щелкните на файле “SetupAssistant”, чтобы запустить Помощник.

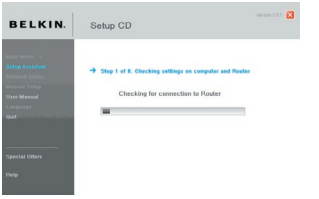
2.3 Выбор страны. В раскрывающемся списке выберите свою страну. Чтобы продолжить, нажмите “Begin” (“Начать”).

2.4 Экран подтверждения. Подтвердите, что завершили все шаги Краткого руководства к установке, установив отметку в поле справа от стрелки. Нажмите “Next” (“Далее”).

2.5 Помощник при установке показывает окно хода установки по завершении каждого ее этапа.



2.6 Проверка настроек. Теперь Помощник при установке проверит сетевые настройки компьютера и соберет данные, необходимые для подключения маршрутизатора к Интернет.



2.7 Проверка подключений оборудования
Теперь Помощник при установке проверит аппаратные подключения.

2.8 Имя беспроводной сети

Помощник при установке покажет имя беспроводной сети по умолчанию (идентификатор набора услуг, SSID). Это имя беспроводной сети, к которой будут подключаться компьютеры и другие устройства с сетевыми адаптерами беспроводной связи. Можно использовать предложенное имя по умолчанию или задать другое, уникальное имя. Запишите это имя для использования в будущем. Нажмите "Next" ("Далее"), чтобы продолжить.

2.9 Запрос данных учетной записи Интернет (если необходимо)

Если ваша учетная запись Интернет требует имени и пароля, на экране появится подобное окно (см. иллюстрацию). В раскрывающихся списках выберите свою страну или поставщика услуг Интернет.

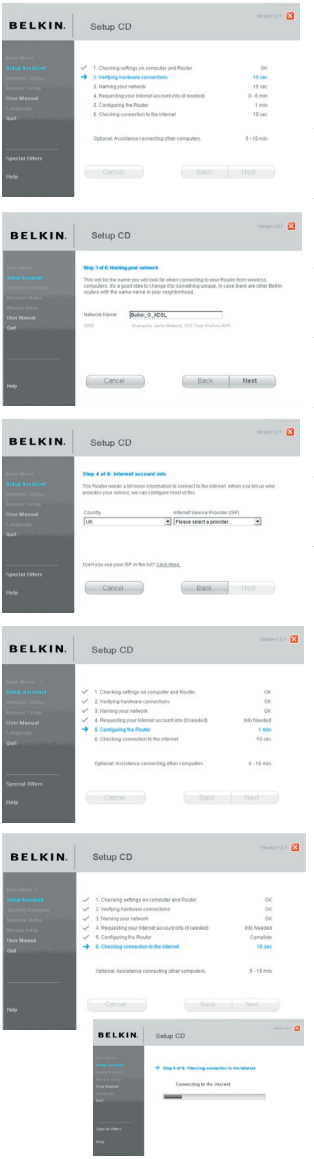
2.10 Настройка маршрутизатора

Теперь Помощник при установке настроит маршрутизатор: отправит на него данные, а затем перезапустит. Дождитесь дальнейших указаний на экране.

Примечание: Не отключайте кабели или питание маршрутизатора во время его перезапуска. Это может повлечь сбои в его работе.

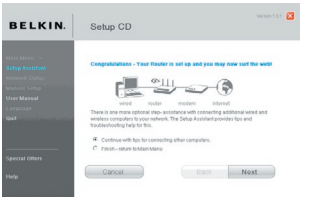
2.11 Проверка подключения к Интернет

Установка почти завершена. Теперь Помощник при установке проверит подключение к Интернет.

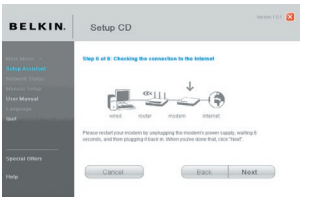


Поздравляем!

Вы завершили установку маршрутизатора Belkin! Когда маршрутизатор подключится к Интернет, на экране появится окно поздравления. Теперь можно открыть Web-обозреватель и посетить любимые Web-сайты.

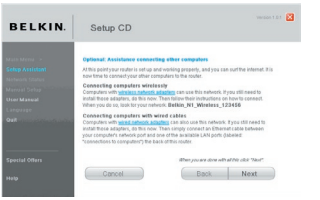


Помощник при установке можно использовать для настройки Интернет-соединения других компьютеров с проводным или беспроводным подключением; для этого нажмите “Next” (“Далее”). Если сейчас не нужно добавлять к маршрутизатору другие компьютеры, нажмите “Exit the Assistant” (“Закрыть Помощник”) и нажмите “Next” (“Далее”).



Устранение неисправностей

Если Помощник при установке не смог подключиться к Интернет, появится следующее окно. Пройдите шаги по устранению неполадок, следуя указаниям на экране.



2.12 По выбору: Помощь в подключении других компьютеров. Данный необязательный шаг поможет подключить к сети другие компьютеры с проводным или беспроводным соединением. Следуйте указаниям на экране.

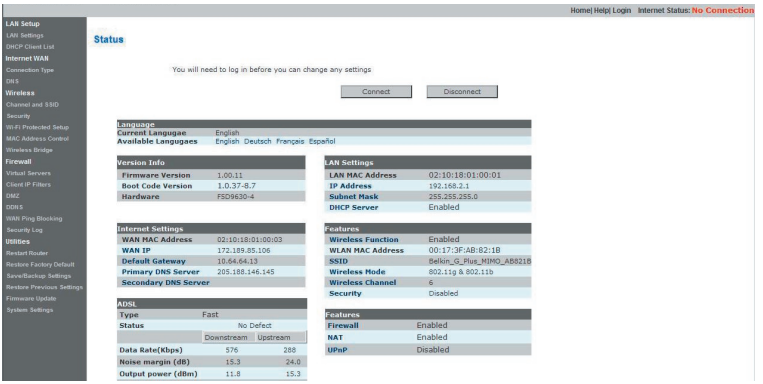
Убедитесь, что другие компьютеры с проводным или беспроводным соединением правильно подключены к сети. Теперь сеть настроена и работает. Сейчас можно перейти к работе в Интернет. Нажмите “Next” (“Далее”), чтобы вернуться к главному меню.

Ознакомление с пользовательским Web-интерфейсом

На начальной странице отображаются краткие сведения о состоянии и параметрах маршрутизатора. С этой страницы можно перейти ко всем страницам дополнительных настроек.

Использование Диспетчера с Web-интерфейсом

После того, как главный ПК правильно настроен, запустите Web-обозреватель и введите в адресную строку собственный IP-адрес маршрутизатора: “192.168.2.1”, затем нажмите “Enter” (Ввод).



1. Ссылки быстрого перехода

Щелкнув на одной из этих ссылок, можно перейти прямо на нужную страницу пользовательского интерфейса маршрутизатора. Ссылки разделены на логические категории и собраны в группы (вкладки), благодаря чему легче искать нужные параметры. Если щелкнуть на заголовке вкладки, появится краткое описание ее функций.

2. Кнопка “Home” (“В начало”)

На каждой странице пользовательского интерфейса есть кнопка “Home” (“В начало”). Она позволяет вернуться на начальную страницу.

3. Кнопка “Help” (“Справка”)

Кнопка “Help” (“Справка”) позволяет перейти на справочные страницы маршрутизатора. Справка доступна также на многих страницах - достаточно щелкнуть на опции “more info” (“Подробнее”) рядом с некоторыми разделами.

4. Кнопка “Login/Logout” (“Вход/Выход”)

Эта кнопка позволяет входить в систему маршрутизатора и покидать ее. После входа в систему маршрутизатора, надпись на кнопке меняется на “Logout” (“Выход”). При входе в систему маршрутизатора появляется окно входа, где нужно ввести пароль. Изменения в настройки можно вносить после входа в систему маршрутизатора. По окончании изменения настроек можно выйти из системы, нажав кнопку “Logout” (“Выход”). Подробнее о входе в систему маршрутизатора см. раздел “Вход в систему маршрутизатора”.

5. Индикатор состояния Интернет

Этот индикатор, отображаемый на каждой странице, показывает состояние подключенности маршрутизатора. Если на индикаторе ЗЕЛЕНЫМ цветом отображается надпись “connection OK” “(“Есть соединение”), маршрутизатор подключен к Интернет. Когда маршрутизатор не подключен к Интернет, на индикаторе КРАСНЫМ цветом отображается надпись “no connection” (“Нет соединения”). Состояние индикатора обновляется автоматически при изменении настроек маршрутизатора.

6. Параметры локальной сети

Здесь отображаются параметры локальной сети со стороны маршрутизатора. Их можно изменить, щелкнув на ссылке быстрого перехода “LAN” (“Локальная сеть”) в левой части экрана.

7. Характеристики

Здесь отображаются параметры NAT, брандмауэра, беспроводной связи и других функций маршрутизатора. Их можно изменить, щелкнув на любой из этих ссылок или на ссылках быстрого перехода в левой части экрана.

8. Параметры Интернет

Здесь отображаются параметры Интернет или внешней сети подключенного к Интернет маршрутизатора. Их можно изменить, щелкнув на ссылке быстрого перехода “Internet/WAN” (“Интернет/Внешняя сеть”) в левой части экрана.

9. Информация о версии

Здесь отображаются версии встроенного ПО, загрузочного кода и аппаратного обеспечения и серийный номер маршрутизатора.

10. Название страницы

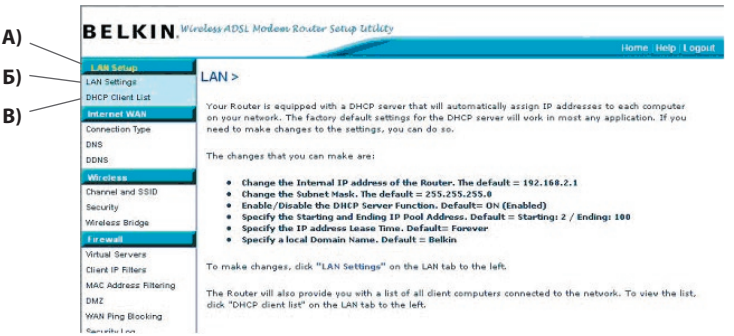
Название текущей страницы. В данном руководстве ссылки на страницы иногда приводятся по их названиям. Например, “LAN > LAN Settings” (“Локальная сеть>Настройки локальной сети”) означает страницу под названием “LAN Settings” (“Настройки локальной сети”).

Изменение параметров локальной сети

Здесь можно увидеть и изменить все параметры внутренней локальной сети маршрутизатора.

Параметры локальной сети

Чтобы выйти на соответствующую страницу, щелкните на заголовке вкладки “LAN” (A). Там приводится краткое описание существующих функций. Для просмотра или изменения любых параметров локальной сети щелкните на “LAN Settings” (“Настройки локальной сети”) (Б), а для просмотра списка подключенных компьютеров - на опции “DHCP Client List” (“Список DHCP-клиентов”) (В).



IP-адрес

“IP-адрес” - это внутренний IP-адрес маршрутизатора. IP-адрес по умолчанию – “192.168.2.1”. Для доступа к расширенному интерфейсу настроек введите этот IP-адрес в адресную строку браузера. При необходимости этот адрес можно изменить. Для изменения IP-адреса введите новый IP-адрес и нажмите “Apply Changes” (“Применить”). Выбранный IP-адрес должен быть немаршрутизируемым. Примеры немаршрутизируемых IP:

192.168.x.x (где x – любое число от 0 до 255)
10.x.x.x (где x – любое число от 0 до 255)

Маска подсети

Изменять маску подсети не нужно. Это уникальная, новая особенность маршрутизатора Belkin.

Сервер DHCP

DHCP-сервер обеспечивает очень простую настройку сети, так как автоматически присваивает IP-адрес каждому входящему в сеть компьютеру. Значение по умолчанию – “On” (“Включен”). DHCP-сервер можно, при необходимости, отключить; однако, чтобы это сделать, вам придется вручную выставить статические IP-адреса для каждого компьютера в сети. Чтобы отключить DHCP-сервер, выберите опцию “Off” (“Отключен”) и нажмите “Apply Changes” (“Применить”).

Пул IP-адресов

Это диапазон значений IP-адрес, резервируемых для динамического присваивания компьютерам сети. Для смены этого диапазона необходимо ввести начальный и конечный IP-адрес и нажать “Apply Changes” (“Применить”). Значение начального IP-адреса должно быть меньше конечного.

Срок аренды

Интервал времени, в течение которого DHCP-сервер будет резервировать IP-адрес за каждым компьютером. Рекомендуется оставить срок аренды на значении “Forever” (“Бессрочно”) Значение по умолчанию “Forever” (“Бессрочно”) означает, что после присвоения компьютеру IP-адреса DHCP-сервером этот IP-адрес для данного компьютера больше не изменится. Если выставить срок аренды на более короткие интервалы, например, один день или один час, то IP-адреса будут высвобождаться после указанного срока. Это также означает, что IP-адрес каждого компьютера может измениться с течением времени. От IP-адреса зависят некоторые дополнительные функции маршрутизатора - например, DMZ или фильтрация клиентов по IP-адресам. По этой причине изменения IP-адреса могут быть нежелательными.

Локальное доменное имя

Своей сети можно присвоить локальное доменное имя (название сети). Нет нужды менять этот параметр без веской причины. Свою сеть можно назвать как угодно, например, “MY NETWORK” (“МОЯ СЕТЬ”).

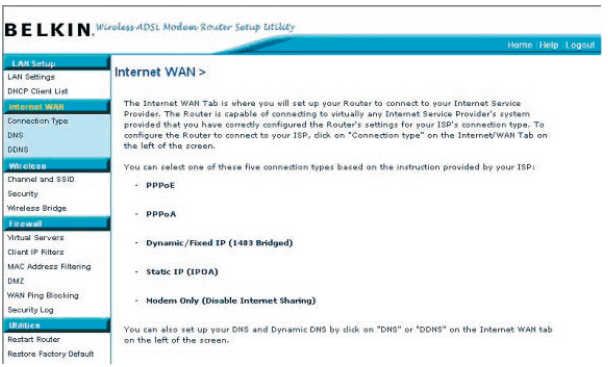
Перечень DHCP-клиентов

Можно просматривать список компьютеров, подключенных к сети. В списке отображаются IP-адрес компьютера, имя хоста (название компьютера в сети) и MAC-адрес платы сетевого интерфейса (NIC) компьютера. Для обновления списка нажмите кнопку “Refresh” (“Обновить”). После этого список будет обновлен с отображением любых изменений.

Интернет / Внешняя сеть

Подключение маршрутизатора к поставщику услуг Интернет настраивается на вкладке “Internet/WAN” (“Интернет/Внешняя сеть”). При правильной конфигурации маршрутизатора согласно типу подключения к поставщику услуг Интернет маршрутизатор можно подключить практически к любой системе услуг Интернет. Параметры подключения к Интернет предоставляет поставщик услуг Интернет.

Для настройки маршрутизатора с параметрами поставщика услуг Интернет щелкните на опции “Connection Type” (“Тип подключения”) в левой части экрана. Выберите используемый тип подключения. Если поставщик услуг предоставил вам параметры DNS, щелкните на опции “DNS” (2) и введите записи о требующих явного задания DNS-адресах поставщика услуг Интернет. Если маршрутизатор настроен правильно, то после задания этих параметров индикатор “Internet Status” (“Состояние Интернет”) будет отображать слово “Connected” (“Есть подключение”).



Тип подключения

На странице “Connection Type” (“Тип подключения”) можно выбрать один из пяти типов подключения (в соответствии с указаниями поставщика услуг Интернет):

PPPoE

PPPoA

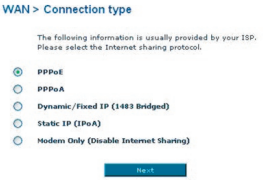
Динамический IP (1483 Bridged)

Статический IP (IPoA)

Только модем (отключение совместного использования Интернет)

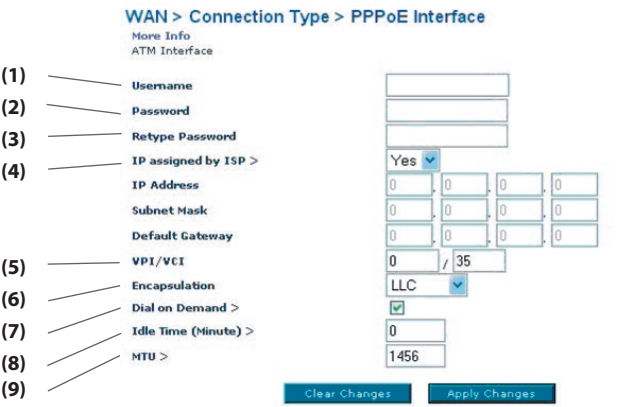
Примечание: Если вы не знаете, какой тип подключения выбрать, обратитесь к поставщику услуг Интернет.

Выберите тип подключения и щелкните на соответствующем переключателе, затем нажмите “Next” (“Далее”).



Установка типа подключения “PPPoE” или “PPPoA”

PPPoE (Point-to-Point Protocol over Ethernet) - стандартный способ соединения сетевых устройств. Для подключения к Интернет и доступа к сети поставщика услуг Интернет нужны имя пользователя и пароль. PPPoA (PPP через протокол ATM) похож на PPPoE, но чаще всего используется в Великобритании. Выберите “PPPoE” или “PPPoA” и нажмите “Next” (“Далее”). Введите информацию, предоставленную поставщиком услуг Интернет, и нажмите “Apply Changes” (“Применить”), чтобы активизировать настройки.



1. Имя пользователя — Введите имя пользователя (назначается поставщиком услуг Интернет).

2. Пароль — Введите свой пароль (назначается поставщиком услуг Интернет).

3. Подтвердите пароль — Введите пароль еще раз

(назначается поставщиком услуг).

4. IP, назначенный поставщиком услуг — Оставьте значение “Yes” (“Да”), если поставщик услуг присваивает IP-адрес автоматически. Если поставщик услуг назначает фиксированный IP-адрес, выберите “No” (“Нет”) и введите присвоенные значения.

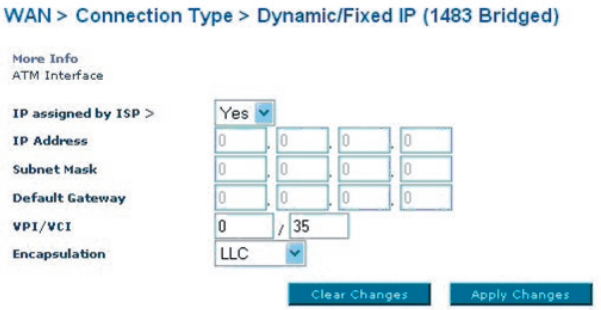
5. VPI/VCI — Введите VPI - идентификатор виртуального пути - и VCI - идентификатор виртуального канала (назначаются поставщиком услуг Интернет).

6. Инкапсуляция — Выберите тип инкапсуляции (предоставляется поставщиком услуг Интернет) , чтобы задать способ обрабатотки множественных протоколов на транспортном уровне ATM. VC-MUX: PPPoA VC-MUX (уплотнение виртуального канала) позволяет только одному протоколу работать на виртуальном канале при меньшем количестве непроизводительных затрат. LLC: PPPoA Logical Link Control (управление логическим каналом) позволяет использовать несколько протоколов на одном виртуальном канале (больше непроизводительных затрат).

7. Подключение по требованию — При выборе опции “Dial on Demand” (“Подключение по требованию”) маршрутизатор автоматически подключается к Интернет, когда пользователь открывает Web-обозреватель.

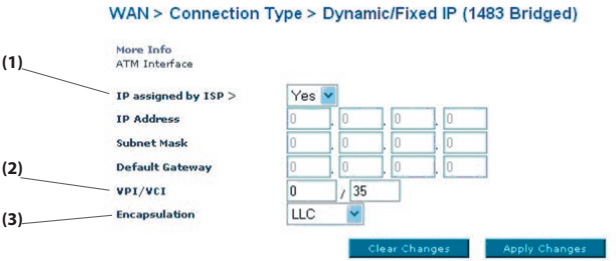
8. Ожидание (в минутах) — Введите максимальный срок бездействия при подключении к Интернет. По истечении этого срока соединение будет прервано.

9. MTU — Не меняйте настройки MTU (максимальный размер пакета данных), если поставщик услуг не требует вводить его конкретное значение. Изменение настроек MTU может вызвать проблемы с подключением к Интернет - прерывания связи, падение скорости соединения или сбои в работе Интернет-приложений.



Задание соединения через динамический IP (1483 Bridged)

Такое подключение создает мост между вашей сетью и сетью поставщика услуг Интернет. Маршрутизатор будет получать IP-адрес автоматически от DHCP-сервера поставщика услуг Интернет.



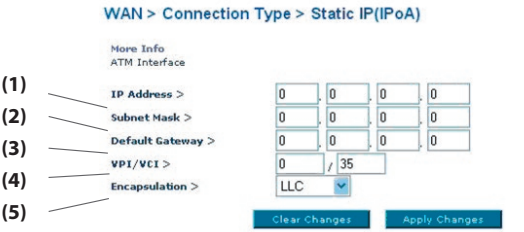
1. IP, назначенный поставщиком услуг — Оставьте значение “Yes” (“Да”), если поставщик услуг присваивает IP-адрес автоматически. Если поставщик услуг назначает фиксированный IP-адрес, выберите “No” (“Нет”) и введите присвоенные значения.

2. VPI/VCI — Введите идентификаторы виртуального пути (VPI) и виртуального канала (VCI). Эти параметры назначаются поставщиком услуг Интернет.

3. Инкапсуляция — Выберите LLC или VC MUX, которым пользуется ваш поставщик услуг Интернет.

Установка подключения через статический IP (“Static IP” - IPoA)

Этот тип соединения называют также “Классический IP через ATM” или “CLIP”; при нем поставщик услуг Интернет назначает маршрутизатору фиксированный IP для подключения к Интернет.



1. IP-адрес — Введите IP-адрес, назначенный маршрутизатору поставщиком услуг Интернет для интерфейса внешней сети.
2. Маска подсети — Введите маску подсети, назначенную поставщиком услуг Интернет.
3. Шлюз по умолчанию — Введите IP-адрес шлюза по умолчанию. Если маршрутизатор не сможет найти адресата в локальной сети, он перенаправит пакеты в шлюз по умолчанию (назначенный поставщиком услуг Интернет).
4. VPI/VCI — Введите идентификаторы виртуального пути (VPI) и виртуального канала (VCI). Эти параметры назначаются поставщиком услуг Интернет.
5. Инкапсуляция — Выберите LLC или VC MUX, которым пользуется ваш поставщик услуг Интернет.

Установка соединения только на модем (с отключением совместного доступа к Интернет)

В этом режиме маршрутизатор работает просто как мост, передающий пакеты через порт DSL. Для доступа в Интернет необходима установка на компьютерах дополнительного программного обеспечения.

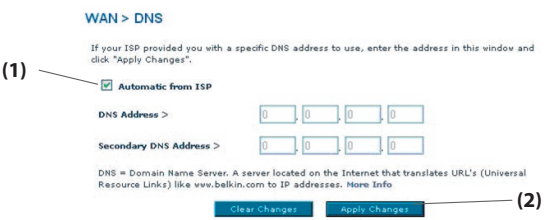
1. VPI/VCI — Введите идентификаторы виртуального пути (VPI) и виртуального канала (VCI) (назначаются поставщиком услуг Интернет).

2. Инкапсуляция — Выберите LLC или VC MUX (назначаются поставщиком услуг Интернет).

Настройки DNS (сервера доменных имен)

"Сервер доменных имен" - это сервер Интернет, преобразующий унифицированные указатели ресурса (Universal Resource Locators; URLs) - например, "www.belkin.com" - в IP-адреса. Многие поставщики услуг Интернет не требуют ввода этих данных для работы маршрутизатора. Если поставщик услуг Интернет [Designer: call this out in screenshot below] не предоставляет конкретного адреса DNS, следует поставить отметку в поле "Automatic from ISP" ("Получать автоматически") (1). При использовании подключения через статический IP-адрес для правильной работы с Интернет может понадобиться ввести первичный и вторичный адреса DNS. При соединении через динамический IP-адрес или PPPoE вводить адрес DNS, скорее всего, не потребуется.

Установите отметку рядом с опцией "Automatic from ISP" ("Получать автоматически"). Для ввода параметров DNS снимите отметку рядом с опцией "Automatic from ISP" ("Получать автоматически") и введите адреса DNS в соответствующие поля. Чтобы сохранить настройки, нажмите "Apply Changes" ("Применить") (2) .

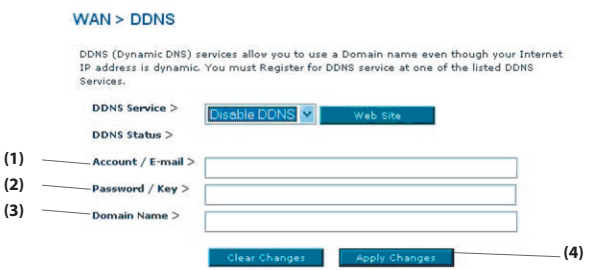


Использование DDNS (динамического DNS)

Услуга динамического DNS позволяет задавать псевдоним динамического IP-адреса как статическое имя хоста в любом из множества доменов, которые предлагает DynDNS. org, что означает упрощенный доступ к компьютерам вашей сети из различных участков Интернет. DynDNS.org предлагает эту услугу членам Интернет-сообщества бесплатно (до пяти имен хоста). Альтернативой DynDNS.org может стать TZO.com. Услуга динамического DNSSM идеально подходит для домашнего Web-сайта или файлового сервера, а также облегчает доступ с работы к домашнему ПК и хранящимся на нем файлам. Использование этой услуги гарантирует, что имя хоста всегда указывает на ваш IP-адрес, - независимо от того, насколько часто меняет его поставщик услуг Интернет. При изменении IP-адреса ваши друзья и коллеги всегда могут найти ваш компьютер, посетив сайт yourname. dyndns.org! Чтобы бесплатно зарегистрироваться и получить динамическое DNS-имя хоста, посетите сайт http://www.dyndns.org.

Настройка клиента обновления динамического DNS маршрутизатора

Прежде чем использовать эту функцию, нужно подписаться на бесплатную услугу обновления на сайте DynDNS.org. По окончании регистрации следуйте указаниям ниже.
1. Введите свое имя пользователя на DynDNS.org в поле “Account / E-mail” (“Учетная запись / Адрес электронной почты”) (1).
2. Введите свой пароль на DynDNS.org в поле “Password / Key” (“Пароль / Ключ”) (2).
3. Введите свое доменное имя на DynDNS.org (задается на сайте DynDNS.org) в поле “Domain Name” (“Имя домена”) (3).
4. Нажмите “Apply Changes” (“Применить”), чтобы обновить свой IP-адрес.
При каждом изменении IP-адреса, назначаемого поставщиком услуг Интернет, маршрутизатор автоматически обновит IP-адрес на серверах DynDNS.org. Кроме того, это можно сделать вручную, нажав кнопку “Apply Changes” (“Применить”) (4).
В раскрывающемся списке на странице “Connection Type” (“Тип подключения”) можно выбрать нужный тип подключения.



Беспроводная связь

На вкладке “Wireless” (“Беспроводная связь”) можно изменять настройки беспроводной сети. Здесь можно изменить имя беспроводной сети (SSID), рабочий канал и параметры системы защиты шифрованием.

Канал и SSID (идентификатор набора услуг)

1. Изменение имени беспроводной сети (SSID)

Для идентификации беспроводной сети используется специальное имя - SSID (идентификатор набора услуг). Его можно оставить прежним или изменить на любое другое. Если по соседству есть другие беспроводные сети, лучше удостовериться, что ваш SSID уникален, то есть не совпадает с SSID другой беспроводной сети. Чтобы изменить SSID, введите в поле “SSID” новое имя и нажмите “Apply Changes” (“Применить”). Изменения вступают в силу немедленно. После изменения SSID может также потребоваться изменить настройки компьютеров беспроводной сети с учетом ее нового имени. Подробнее об изменении этих параметров см. документацию к адаптеру беспроводной связи.

2. Использование функции трансляции SSID

В целях безопасности можно отключить широкую трансляцию SSID своей сети. Такое отключение позволит скрыть имя сети от компьютеров, разыскивающих беспроводные сети. Чтобы отключить трансляцию своего SSID, выберите “DISABLE” (“Отключить”) и нажмите “Apply Changes” (“Применить”). Изменения вступают в силу немедленно. Теперь каждый компьютер нужно настроить на конкретный SSID - опция “ANY” (“ЛЮБОЙ”) уже недопустима. Подробнее об изменении этих параметров см. документацию к адаптеру беспроводной связи.

Примечание: Эту дополнительную функцию рекомендуется задействовать только опытным пользователям.

3. Переключатель режима беспроводной связи

Маршрутизатор может работать в одном из трех режимов беспроводной связи: “Mixed (11b+11g)”, “11g Only” и “11b Only”. Ниже они описаны подробнее.

Mixed (11b+11g) (смешанный режим)

В этом режиме маршрутизатор одновременно совместим с беспроводными клиентами стандартов 802.11b и 802.11g. Этот режим устанавливается производителем по умолчанию и обеспечивает правильную работу со всеми устройствами, совместимыми с Wi-Fi®. Если сеть совмещает клиенты 802.11b и 802.11g, рекомендуется оставлять данный режим по умолчанию. Не следует менять этот параметр без веской причины.

Режим “11g-Only” (“Только 11g”)

Режим “802.11g-Only” (“Только 11g”) работает только с клиентами 802.11g. Этот режим рекомендуется использовать для предотвращения доступа к сети клиентов стандарта 802.11b. Чтобы изменить режим, выберите нужный режим в раскрывающемся меню “Wireless Mode” (“Режим беспроводной связи”) и нажмите “Apply Changes” (“Применить”).

Режим “11b-Only” (“Только 11b”)

Настоятельно рекомендуется НЕ ИСПОЛЬЗОВАТЬ этот режим без очень веской причины. Данный режим включен список с единственной целью - для решения особых проблем, которые могут возникать с адаптерами некоторых клиентов стандарта 802.11b и НЕОБЯЗАТЕЛЕН для взаимосвязи стандартов 802.11g и 802.11b.

4. Изменение канала беспроводной связи

У вас есть возможность выбора из целого ряда рабочих каналов. В Соединенных Штатов таких каналов 11. В Великобритании и большинстве стран Европы - 13. В некоторых других странах набор каналов иной. Маршрутизатор настроен на работу на каналах, используемых в вашей стране. Значение по умолчанию: “Auto” (“Автоматически”). Если нужно, канал можно изменить. Если по соседству есть другие беспроводные сети, лучше настроить свою сеть на канал, отличающийся от каналов остальных сетей. Для лучшей производительности используйте канал, отстоящий от канала другой беспроводной сети по меньшей мере на пять каналов. Если, например, другая сеть работает на канале 11, установите свою сеть на канал с номером 6 или менее. Чтобы изменить канал, выберите его в раскрывающемся списке. Нажмите “Apply Changes” (“Применить”). Изменения вступают в силу немедленно.

Шифрование и защита

Защита сети Wi-Fi

Есть несколько способов усилить защиту своей беспроводной сети и уберечь свои данные от непрошенных глаз. Данный раздел предназначен для домашних пользователей, домашних и малых офисов. К моменту публикации данного руководства использовались четыре метода шифрования.

Название	64-битный Wired Equivalent Privacy	128-битный Wired Equivalent Privacy	Wi-Fi Protected Access-TKIP	Wi-Fi Protected Access 2
Сокращение	64-битный WEP	128-битный WEP	WPA-TKIP/AES (или просто WPA)	WPA2-AES (или просто WPA2)
Безопасность	Хорошо	Лучше	Отлично	Отлично
Функции	Статические ключи	Статические ключи	Шифрование с динамическими ключами и взаимной проверкой подлинности	Шифрование с динамическими ключами и взаимной проверкой подлинности
	Ключи шифрования на основе алгоритма RC4 (обычно 40-битные ключи)	Надежнее 64-битного WEP; использует ключ длиной 104 бита плюс 24 дополнительных бита со сгенерированными системой данными	Дополнен протоколом TKIP (Temporal Key Integrity Protocol; протокол временной целостности ключей), который, благодаря ротации ключей, повышает защищенность шифрования	AES (Advanced Encryption Standard; улучшенный стандарт шифрования) не влечет никаких потерь пропускной способности

WEP (Wired Equivalent Privacy)

WEP - распространенный протокол, повышающий защищенность всех беспроводных устройств, совместимых с Wi-Fi. WEP разработан, чтобы обеспечить беспроводные сети уровнем защиты конфиденциальности, сравнимым с уровнем защищенности проводных сетей.

64-битный WEP

64-битный WEP был первым среди 64-битных методов шифрования, которые задействуют ключи длиной 40 бит плюс 24 дополнительных бит данных, сгенерированных системой (в сумме 64 бит). Некоторые производители оборудования называют 64-битное шифрование 40-битным. Вскоре после внедрения этой технологии разработчики выяснили, что 64-битное шифрование слишком легко поддается дешифровке.

128-битный WEP

Вследствие потенциальной слабости защиты по 64-битному протоколу WEP было разработано более надежное, 128-битное шифрование. 128-битное шифрование задействует ключи длиной 104 бит плюс 24 дополнительных бит данных, сгенерированных системой (в сумме 128 бит). Некоторые производители оборудования называют 128-битное шифрование 104-битным. Большая часть новейшего беспроводного оборудования на современном рынке поддерживает как 64-битный WEP, так и 128-битное шифрование, однако у вас могут быть более ранние устройства, поддерживающие только 64-битный WEP. Вся беспроводная продукция компании Belkin поддерживает как 64-битный WEP, так и 128-битное шифрование.

Шифровальные ключи

После выбора 64-битного или 128-битного WEP-шифрования очень важно сгенерировать шифровальный ключ. Если не использовать единый для всей беспроводной сети шифровальный ключ, различные устройства беспроводной сетевой связи не смогут соединяться друг с другом и не удастся обмениваться данными по сети. Можно вручную ввести шестнадцатеричный ключ в числовое поле либо ввести фразу-пароль в поле “Passphrase” (“Фраза-пароль”) и щелкнуть на кнопке “Generate” (“Сгенерировать”), чтобы создать ключ. Шестнадцатеричный ключ представляет собой сочетание букв от A до F и цифр от 0 до 9. Для 64-битного WEP нужно ввести 10 шестнадцатеричных знаков. Для 128-битного WEP нужно ввести 26 шестнадцатеричных знаков.

Пример:
AF 0F 4B C3 D4 = ключ 64-битного WEP
C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = ключ 128-битного WEP
Фраза-пароль WEP - НЕ ТО ЖЕ САМОЕ, что ключ WEP. Беспроводная карта использует фразу-пароль для генерации ключей WEP, однако производители другого оборудования могут использовать для генерации ключей иные способы. Если в сети есть устройства разных производителей, проще всего воспользоваться шестнадцатеричным WEP-ключом маршрутизатора или узла доступа и ввести его вручную в таблицу шестнадцатеричных ключей WEP в окне конфигурации беспроводной карты.

WPA (Wi-Fi Protected Access)

WPA - новый стандарт Wi-Fi, разработанный для улучшения защитных характеристик протокола WEP. Для использования защиты WPA следует модернизировать драйверы и программное обеспечение беспроводного оборудования. Такие обновления можно найти на сайте поставщика беспроводного оборудования. Существуют два типа защиты WPA: WPA-PSK (без сервера) и WPA (с RADIUS-сервером 802.1x).

WPA-PSK (без сервера)
Этот метод задействует в качестве сетевого ключа так называемый “предварительно согласованный ключ”. Сетевой ключ - это пароль длиной от 8 до 63 знаков. Он может представлять собой сочетание букв, цифр и символов. Каждый клиент использует для доступа к сети один и тот же сетевой ключ. Этот режим обычно применяется в домашних сетях.

WPA (с RADIUS-сервером 802.1x)

В этой системе RADIUS-сервер автоматически распределяет сетевой ключ среди клиентов. Такие системы обычно используются в корпоративной среде.

WPA2

Маршрутизатор поддерживает WPA2 - второе поколение стандарта 802.11i на основе WPA. Он предлагает повышенный уровень безопасности беспроводной связи благодаря сочетанию улучшенной проверки подлинности сети и усиленному методу шифрования AES.

Требования WPA2

ВАЖНОЕ ЗАМЕЧАНИЕ:Для использования защиты WPA2 все компьютеры и беспроводные карты клиентов нужно обновить исправлениями, драйверами и клиентскими служебными программами, поддерживающими WPA2. В период подготовки данного руководства пользователя компания Microsoft® уже выпустила несколько исправлений защиты, которые можно загрузить бесплатно.. Эти исправления предназначены только для операционной системы Windows XP. В настоящее время другие операционные системы не поддерживаются.

Для компьютеров под управлением Windows XP, на которых не установлен Service Pack 2 (SP2), можно бесплатно загрузить созданный Microsoft файл "Windows XP Support Patch for Wireless Protected Access (KB 826942)": http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=009D8425-CE2B-47A4-ABEC-274845DC9E91

Для Windows XP с установленным Service Pack 2 компания Microsoft выпустила обновление компонентов беспроводных клиентов с поддержкой WPA2 (KB893357). Обновление можно найти по ссылке: http://www.microsoft.com/downloads/details.aspx?FamilyID=662bb74d-e7c1-48d6-95ee-1459234f4483&DisplayLang=en.

ВАЖНОЕ ЗАМЕЧАНИЕ: Кроме того, нужно убедиться, что все беспроводные клиентские карты и адаптеры поддерживают WPA2, а также загружены и установлены новейшие драйверы. Большинство обновлений драйверов для беспроводных карт Belkin можно найти на сайте технической поддержки Belkin: www.belkin.com/networking. Чтобы увидеть список беспроводной продукции Belkin, поддерживающей WPA/WPA2, посетите наш сайт: www.belkin.com/networking.

Совместное использование одних и тех же сетевых ключей

Большинство устройств Wi-Fi поставляется с отключенной защитой. Таким образом, после установки сети нужно включить WEP или WPA и убедиться, что все устройства беспроводной сетевой связи используют один и тот же сетевой ключ.

Использование шестнадцатеричного ключа
Шестнадцатеричный ключ представляет собой сочетание букв от A до F и цифр от 0 до 9. 64-битные ключи - это пять двузначных чисел. 128-битные ключи - 13 двузначных чисел.

Пример:
AF 0F 4B C3 D4 = 64-битный ключ
C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-битный ключ

В полях ниже задайте ключ, вводя в каждое поле по два знака
от A до F и от 0 до 9. Этот ключ будет использоваться для задания
настроек шифрования на маршрутизаторе и компьютерах беспроводной сети.

Примечание для пользователей Mac: Оригинальная продукция Apple AirPort® поддерживает только 64-битное шифрование. Продукция Apple AirPort 2 может поддерживать 64- или 128-битное шифрование. Проверьте версию используемой вами продукции. Если не удается настроить сеть на 128-битное шифрование, попробуйте использовать 64-битное.

Установка WEP

1. В раскрывающемся меню выберите “WEP”.
2. Выберите 64- или 128-битный режим (“WEP Mode”).
3. После выбора режима WEP-шифрования можно ввести шестнадцатеричный ключ вручную.

Шестнадцатеричный ключ представляет собой сочетание букв от A до F и цифр от 0 до 9. Для 64-битного WEP нужно ввести 10 шестнадцатеричных знаков. Для 128-битного WEP нужно ввести 26 шестнадцатеричных знаков.
Пример:
AF 0F 4B C3 D4 = 64-битный ключ
C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-битный ключ

3. Для завершения нажмите "Apply Changes" ("Применить"). Режим шифрования маршрутизатора установлен. Теперь все компьютеры данной беспроводной сети должны быть настроены с теми же параметрами защиты.

ПРЕДУПРЕЖДЕНИЕ: Если настройка беспроводного маршрутизатора осуществляется на компьютере с клиентом беспроводной связи, убедитесь, что для этого беспроводного клиента защита включена. В противном случае беспроводное соединение прервется.

Изменение параметров защиты беспроводной связи

Маршрутизатор оснащен WPA/WPA2 - новейшим стандартом защиты беспроводной связи. Маршрутизатор также поддерживает более ранний стандарт защиты - WEP. По умолчанию, защита беспроводной связи отключена. Чтобы включить защиту, нужно сначала определить, каким стандартом лучше пользоваться. Чтобы перейти к параметрам защиты, нажмите "Security" ("Защита") на вкладке "Wireless" ("Беспроводная связь").

Установка WPA

Примечание: Для использования защиты WPA на всех клиентах сети нужно установить поддерживающие этот стандарт обновления драйверов и программ. В период подготовки данного руководства пользователя компания Microsoft уже выпустила исправление защиты, которое можно загрузить бесплатно. Исправление предназначено только для операционной системы Windows XP. Кроме того, нужно загрузить с сайта службы поддержки Belkin новейший драйвер сетевой карты для настольного ПК или ноутбука Wireless G. В настоящее время другие операционные системы не поддерживаются. Исправление, разработанное компанией Microsoft, поддерживает только устройства с WPA-драйверами - такими, как продукция стандарта 802.11g компании Belkin.

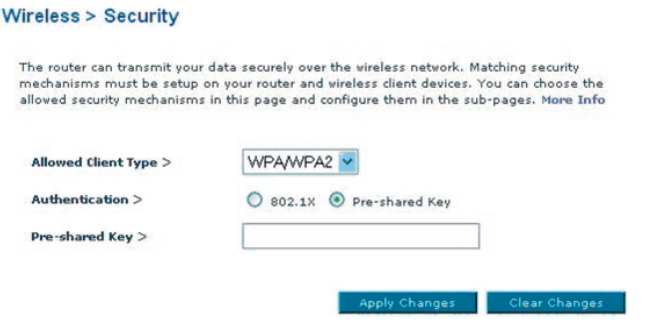
Существуют два типа защиты WPA: WPA-PSK (без сервера) и WPA (с RADIUS-сервером). В качестве защитного ключа WPA-PSK (без сервера) использует так называемый "предварительно согласованный ключ" (PSK). Предварительно согласованный ключ - это пароль длиной от 8 до 63 знаков. Он может представлять собой сочетание букв, цифр и других символов. Каждый клиент использует для доступа к сети один и тот же ключ. Этот режим обычно применяется в домашних сетях. WPA (с RADIUS-сервером) - это система, где RADIUS-сервер автоматически распределяет ключи среди клиентов. Она обычно используется в корпоративной среде. WPA2 - второе поколение WPA, предлагающее более совершенные методы шифрования через WPA.

Настройка WPA-PSK (без сервера)

1. В раскрывающемся меню "Allowed Client Type" ("Допустимый тип клиента") выберите пункт "WPA/WPA2".

2. Для обычного домашнего пользования или малого офиса в поле "Authentication" ("Проверка подлинности") выберите "Pre-shared Key" ("Предварительно согласованный ключ"). Этот параметр должен быть одинаковым для всех клиентов сети.

3. Введите предварительно согласованный ключ. Он может иметь длину от 8 до 63 знаков и состоять из букв, цифр и символов. Тот же ключ должен использоваться на всех настраиваемых клиентах. Предварительно согласованный ключ может выглядеть, например, так: "Smith family network key" ("Сетевой ключ семьи Смитов").



4. Для завершения нажмите “Apply Changes” (“Применить”). Теперь следует настроить все клиенты в соответствии с данными установками.

Задание настроек WPA/WPA2 (с RADIUS-сервером)

Используйте эту опцию, если для распределения ключей клиентам сети используется RADIUS-сервер

1. В раскрывающемся меню “Allowed Client Type” (“Допустимый тип клиента”) выберите пункт “WPA/WPA2”.

2. Для среды с RADIUS-сервером выберите в качестве “Encryption Technique” (“Метод шифрования”) значение “802.1x”. Этот параметр должен быть одинаковым для всех клиентов сети.

3. В поле “Session Idle Timeout” (“Прекращение сеанса при бездействии”) введите срок бездействия для прекращения сеанса RADIUS-сервера.

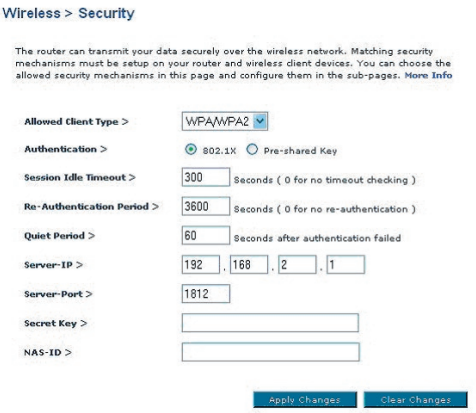
4. В поле “Re-Authentication Period” (“Период проверки подлинности”) введите интервал смены ключа — частоту распределения ключей (в пакетах).

5. В поле “Quiet Period” (“Период тишины”) введите срок ожидания, после которого проверка подлинности не подтверждается.

6. В поля “Server IP” (“IP сервера”) и “Server Port” (“Порт сервера”) введите IP-адрес и номер порта RADIUS-сервера.

7. В поле “Secret Key” (“Секретный ключ”) введите RADIUS-ключ.

8. Для завершения нажмите “Apply Changes” (“Применить”). Теперь следует настроить все клиенты в соответствии с данными установками.



Примечание: Убедитесь, что беспроводные компьютеры обновлены для работы с WPA2 и на них заданы правильные настройки подключения к маршрутизатору.

Настройка сетевых карт Belkin Wireless G для использования функций защиты

Примечание:В этом разделе описано, как настроить сетевые карты Belkin Wireless G на использование защиты. К настоящему моменту беспроводной маршрутизатор или узел доступа уже должен быть настроен на использование WPA или WEP. Для установления беспроводного соединения нужно настроить карту беспроводной связи для ноутбуков и настольных ПК на использование тех же параметров защиты.

Подключение компьютера к беспроводной сети, требующей 64- или 128-битного WEP-ключа

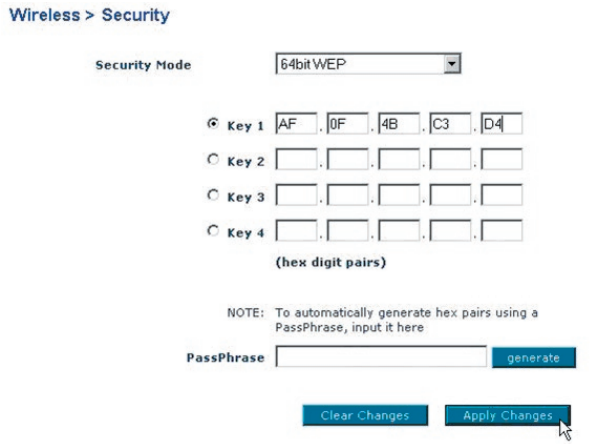
1. Дважды щелкните на значке “Signal Indicator” (“Индикатор сигнала”), чтобы открыть окно “Wireless Networks” (“Беспроводные сети”). Кнопка “Advanced” (“Дополнительно”) позволяет просматривать и настраивать дополнительные параметры беспроводной карты.

2. На вкладке “Wireless Network Properties” (“Свойства беспроводной сети”) выберите имя сети в списке “Available networks” (“Доступные сети”) и нажмите “Configure” (“Настроить”).

3. В поле “Data Encryption” (“Шифрование данных”) выберите “WEP”.

4. Не устанавливайте отметку в поле “Network key is provided for me automatically” (“Сетевой ключ предоставляется автоматически”). Если данный компьютер используется для подключения к корпоративной сети, посоветуйтесь со своим системным администратором о том, нужно ли устанавливать эту отметку.

5. Введите в поле “Network key” (“Сетевой ключ”) свой WEP-ключ.



Важное замечание: WEP-ключ представляет собой сочетание букв от A до F и цифр от 0 до 9. Для 128-битного WEP нужно ввести 26 знаков. Для 64-битного WEP нужно ввести 10 знаков. Сетевой ключ должен совпадать с ключом, выбранным для маршрутизатора.

6. Нажмите “OK”, чтобы сохранить настройки.

Подключение компьютера к беспроводной сети, требующей WPA-PSK (без сервера)

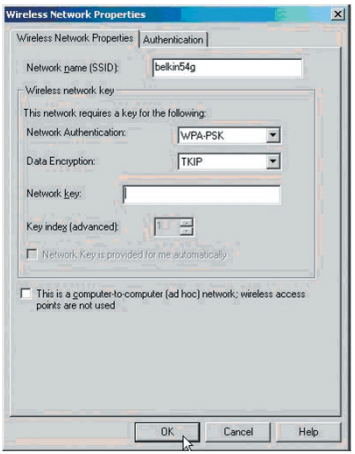
1. Дважды щелкните на значке “Signal Indicator” (“Индикатор сигнала”), чтобы открыть окно “Wireless Networks” (“Беспроводные сети”). Кнопка “Advanced” (“Дополнительно”) позволяет просматривать и настраивать дополнительные параметры беспроводной карты.

2. На вкладке “Wireless Networks” (“Беспроводные сети”) выберите имя сети в списке “Available networks” (“Доступные сети”) и нажмите “Configure” (“Настроить”).

3. В меню “Network Authentication” (“Проверка подлинности сети”) выберите “WPA-PSK (No Server)”.

4. Введите в поле “Network key” (“Сетевой ключ”) свой WPA-ключ.

Важное замечание: WPA-PSK представляет собой сочетание букв от A до Z и цифр от 0 до 9. Длина WPA-PSK может составлять от 8 до 63 знаков. Сетевой ключ должен совпадать с ключом, выбранным для маршрутизатора.



5. Нажмите “OK”, чтобы сохранить настройки.

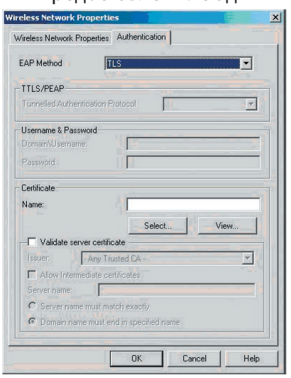
Подключение компьютера к беспроводной сети, требующей WPA (с RADIUS-сервером)

1. Дважды щелкните на значке “Signal Indicator” (“Индикатор сигнала”), чтобы открыть окно “Wireless Networks” (“Беспроводные сети”). Кнопка “Advanced” (“Дополнительно”) позволяет просматривать и настраивать дополнительные параметры беспроводной карты.

2. На вкладке “Wireless Networks” (“Беспроводные сети”) выберите имя сети в списке “Available networks” (“Доступные сети”) и нажмите “Configure” (“Настроить”).

3. В меню “Network Authentication” (“Проверка подлинности сети”) выберите “WPA”.

4. На вкладке “Authentication” (“Проверка подлинности”) выберите параметры, предоставленные администратором сети.



5. Нажмите “OK”, чтобы сохранить настройки.

Настройка WPA для беспроводных карт ДРУГИХ производителей для настольных ПК и ноутбуков

Если ваши беспроводные карты для настольных ПК или ноутбуков были произведены ДРУГОЙ компаний (не компанией Belkin) и не сопровождаются программным обеспечением WPA, можно бесплатно загрузить созданный компанией Microsoft файл “Windows XP Support Patch for Wireless Protected Access”.

Примечание: Данный файл компании Microsoft предназначен только для Windows XP. В настоящее время другие операционные системы не поддерживаются.

Важное замечание: Необходимо удостовериться, что производитель карты беспроводной связи поддерживает WPA, а также загрузить с сайта поддержки производителя и установить новейший драйвер.

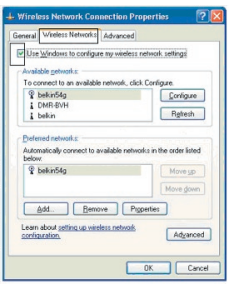
Поддерживаемые операционные системы:

• Windows XP Professional
• Windows XP Home Edition

Настройка утилиты беспроводной сетевой связи Windows XP на WPA-PSK

Чтобы использовать WPA-PSK, убедитесь, что используется утилита беспроводной сетевой связи Windows:

1. В Windows XP выберите “Start > Control Panel > Network Connections” (“Пуск>Панель управления>Сетевые подключения”).
2. Правой кнопкой щелкните на “Wireless Network Connection” (“Подключения беспроводной сети”) и выберите “Properties” (“Свойства”).
3. Щелкните на вкладке “Wireless Networks” (“Беспроводные сети”) - откроется следующее окно. Установите отметку в поле “Use Windows to configure my wireless network settings” (“Использовать Windows для конфигурации беспроводной сети”).
4. На вкладке “Wireless Networks” (“Беспроводные сети”) щелкните на кнопке “Configure” (“Настройка”), после чего откроется следующее окно.



5. Для домашнего и малого офиса выберите “WPA-PSK” в пункте “Network Administration” (“Администрирование сети”).

Примечание: Выбирайте опцию “WPA”, если используете данный компьютер для подключения к корпоративной сети, поддерживающей авторизационный сервер (например, RADIUS-server). За более подробными сведениями обращайтесь к администратору своей сети.

6. В пункте “Data Encryption” (“Шифрование данных”) выберите “TKIP” или “AES”. Этот параметр должен совпадать с настройкой маршрутизатора.

7. Введите в поле “Network key” (“Сетевой ключ”) свой шифровальный ключ.

Важное замечание: Введите предварительно согласованный ключ. Он может иметь длину от 8 до 63 знаков и состоять из букв, цифр и символов. Тот же ключ должен использоваться на всех настраиваемых клиентах.

8. Нажмите “OK”, чтобы применить настройки.

Расширение радиуса беспроводной связи и использование режима моста

Что такое беспроводной мост?

Режим моста - это рабочий “режим”, который можно использовать, чтобы расширить радиус работы беспроводной сети или создать расширение сети в другом месте дома или работы без проводных соединений.
Примечание: Нет гарантии, что данная функция будет взаимосовместима с оборудованием, изготовленным другими производителями средств беспроводной связи.

Примечание: Чтобы добиться оптимальной производительности, загрузите новейшие версии встроенного ПО для маршрутизатора на сайте: http://web.belkin.com/support

Добавление нового сегмента сети без использования проводов

Подсоединение сетевого коммутатора или концентратора к гнезду RJ45 маршрутизатора обеспечит доступ к остальной сети целому ряду компьютеров, подключенных к коммутатору.

Установка моста между маршрутизатором и вторичным узлом доступа

Для установки моста между маршрутизатором Belkin и вторичным узлом доступа необходимо войти в расширенную служебную программу установки маршрутизатора и ввести в соответствующее поле MAC-адрес узла доступа. Кроме того, нужно выполнить и другие действия.

ПОЖАЛУЙСТА, ВНИМАТЕЛЬНО СЛЕДУЙТЕ ПРИВЕДЕННЫМ НИЖЕ УКАЗАНИЯМ.

1. Установите узел доступа на тот же канал, на который настроен маршрутизатор. Подробнее об изменении каналов см. раздел “Канал и SSID” данного руководства пользователя.

2. Найдите на нижней части узла доступа его MAC-адрес. На этикетке внизу указаны два MAC-адреса. Вам нужен адрес с пометкой “WLAN MAC Address”. MAC-адрес начинается с последовательности 0030BD, за которой следуют шесть чисел или букв (т. е. 0030BD-XXXXXX). Перепишите этот MAC-адрес. Переходите к следующему шагу.

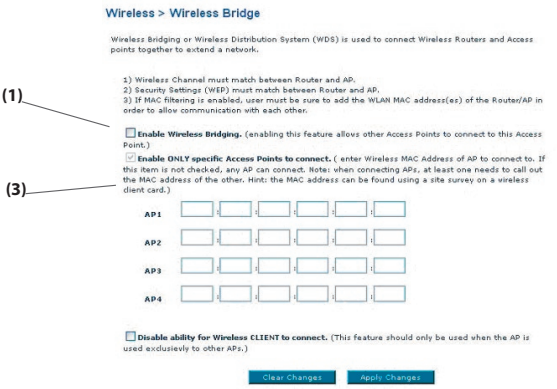
3. Разместите вторичный узел доступа в радиусе действия беспроводного маршрутизатора и на том участке, куда желаете расширить радиус связи или добавить сегмент сети. В помещении радиус покрытия составляет обычно 30-60 метров.

4. Подключите узел доступа к питанию. Убедитесь, что узел доступа включен, и переходите к следующему шагу.

5. На компьютере, уже подключенном к маршрутизатору, запустите Web-обозреватель, чтобы войти в расширенную служебную программу установки маршрутизатора. В строке адреса введите “192.168.2.1”. Не набирайте перед этим числом приставки “www” или “http://”. Примечание: Если вы меняли IP-адрес маршрутизатора, введите выбранный ранее IP-адрес.

6. В окне Web-обозревателя появится начальная страница маршрутизатора. В левой части экрана щелкните на “Wireless Bridge” (“Беспроводной мост”) (2). Появится следующее окно:

7. Установите отметку в поле “Enable ONLY specific Access Points to connect” (“Разрешить подключение ТОЛЬКО указанным узлам доступа”) (1).



8. В поле "AP1" (3) введите MAC-адрес вторичного узла доступа. После ввода адреса нажмите "Apply Changes" ("Применить").

9. Настройка функции моста завершена.

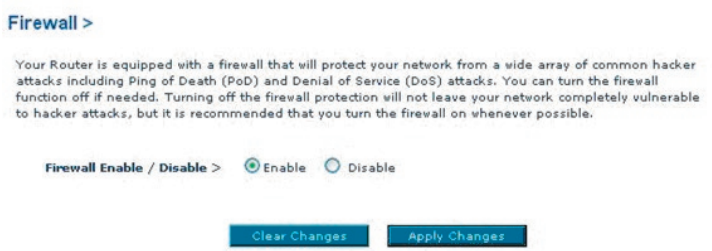
Примечание: Установка соединения через мост может занять около минуты. В некоторых случаях для активации моста нужно перезапустить узел доступа и маршрутизатор.

Брандмауэр

Маршрутизатор оснащен брандмауэром, защищающим сеть от многих распространенных способов взлома, включая:

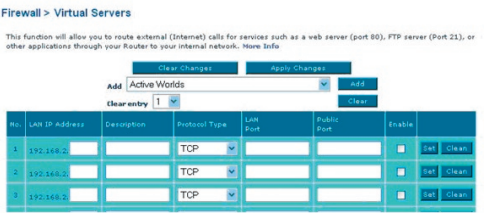
- IP Spoofing
- Land Attack
- Ping of Death (PoD)
- Denial of Service (DoS)
- IP нулевой длины
- Smurf Attack
- TCP Null Scan
- SYN flood
- UDP flooding
- Tear Drop Attack
- ICMP defect
- RIP defect
- Fragment flooding

Кроме того, брандмауэр маскирует порты, которые часто используются для взлома сети. Он превращает эти порты в "невидимки", то есть, с точки зрения потенциального взломщика, на компьютере их просто нет. При необходимости брандмауэр можно отключить; однако рекомендуется оставить его включенным. Отключение брандмауэра не сделает сеть полностью уязвимой для попыток взлома, но все же лучше включить брандмауэр.



Виртуальные серверы

Виртуальные серверы позволяют направлять внешние (Интернет) запросы на обслуживание к Web-серверу (порт 80), FTP-серверу (порт 21) или другим приложениям через маршрутизатор во внутреннюю сеть. Поскольку компьютеры внутренней сети защищены брандмауэром, компьютеры из сети Интернет не могут на них выйти, они их просто "не видят". При необходимости настроить виртуальный сервер для какого-либо приложения следует связаться с поставщиком этого приложения и выяснить, какие настройки порта нужно использовать. Данные о порте можно ввести в маршрутизатор вручную.



Выбор приложения

Выберите приложение в раскрывающемся списке. Нажмите "Add" ("Добавить"). Параметры будут скопированы в следующее доступное поле экрана. Чтобы сохранить настройки для этого приложения, нажмите "Apply Changes" ("Применить"). Чтобы удалить приложение из списка, выберите номер строки для удаления и нажмите "Clear" ("Очистить").

Ввод параметров виртуального сервера вручную

Для ввода параметров вручную введите IP-адрес в поле, отведенное для внутреннего (серверного) устройства, порт(ы) для прохождения и тип порта (TCP или UDP), затем нажмите "Apply Changes" ("Применить"). Каждая запись для входного порта состоит из двух полей длиной не более пяти символов, где задаются начальное и конечное значения диапазона порта - в формате [xxxxx]-[xxxxx]. Для каждой записи можно ввести единичное значение порта, заполнив оба поля одним и тем же значением (например, [7500]-[7500]); можно ввести и широкий диапазон портов (например, [7500]-[9000]). При необходимости ввести несколько единичных значений портов или сочетания диапазонов и единичного значения следует использовать несколько записей, но не более 20 (например, 1. [7500]-[7500], 2. [8023]-[8023], 3. [9000]-[9000]). Каждому внутреннему IP-адресу может соответствовать только один порт. Открытие портов в брандмауэре может поставить под угрозу защиту системы. Включение и отключение этих настроек осуществляется очень быстро. Когда какое-либо конкретное приложение не используется, рекомендуется эти настройки отключать.

Фильтрация клиентов по IP

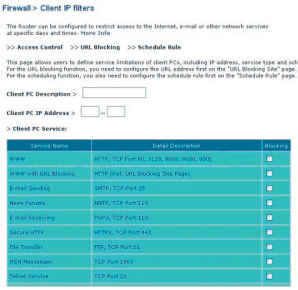
Маршрутизатор можно настроить на ограничение доступа к Интернет, электронной почте или другим сетевым службам в определенные дни и в определенное время. Ограничения можно задать для одного компьютера, группы компьютеров или множества компьютеров из разных групп.

Управление доступом

Функция управления доступом позволяет ограничивать исходящие потоки данных или отказывать в доступе через интерфейс внешней сети. По умолчанию все исходящие потоки данных разрешены. Чтобы настроить ограниченный доступ к компьютерам, проделайте следующее:

1. В окне "Access Control" ("Управление доступом") щелкните на пункте "Add PC" ("Добавить ПК").

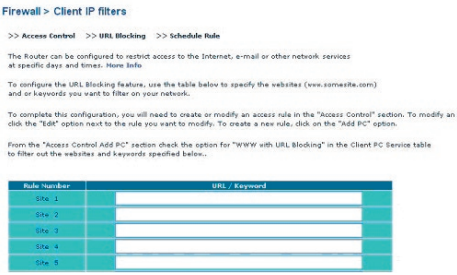
2. Задайте соответствующие настройки для клиентского ПК (как показано на следующей иллюстрации).



3. Нажмите "OK", затем "Apply Changes" ("Применить"), чтобы сохранить настройки.

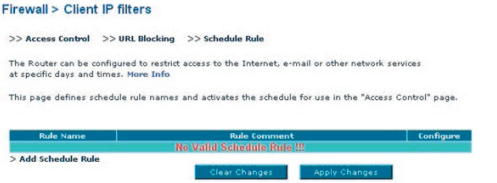
Блокировка URL

Для настройки функции блокировки URL укажите Web-сайты (www.somesite.com) или ключевые слова для использования в качестве фильтров в сети. Чтобы применить изменения, нажмите "Apply Changes" ("Применить"). Для завершения настройки необходимо создать или изменить правило доступа в разделе "Client IP filters" ("Фильтрация клиентов по IP"). Чтобы изменить существующее правило, щелкните на пункте "Edit" ("Редактировать") рядом с правилом, которое нужно изменить. Чтобы создать новое правило, щелкните на пункте "Add PC" ("Добавить ПК"). Чтобы включить фильтр для указанных Web-сайтов и ключевых слов, в разделе "Access Control > Add PC" ("Управление доступом > Добавить ПК") установите отметку в поле "WWW with URL Blocking" ("WWW с блокировкой URL") в таблице "Client PC Service" ("Услуга для клиентского ПК").



Правила доступа по расписанию

Можно организовать фильтр доступа в Интернет для локальных клиентов на основе правил. Каждое правило доступа может быть активировано в запланированное время. Задайте расписание в разделе “Schedule Rule” (“Правила доступа по расписанию”) и примените правило на странице “Access Control” (“Управление доступом”).



Чтобы добавить расписание, проделайте следующее:

1. Нажмите “Add Schedule Rule” (“Добавить правило доступа по расписанию”).

2. Появится следующее окно:

3. Чтобы настроить правило доступа по расписанию, укажите имя, комментарий, время начала и окончания работы фильтра в сети.

4. Для сохранения настроек нажмите “OK”, затем “Apply Changes” (“Применить”).

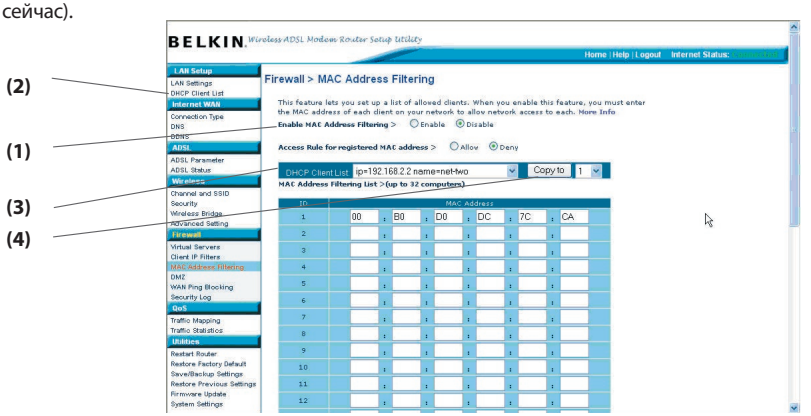
5. Для завершения настройки необходимо создать или изменить правило доступа в разделе “Client IP filters” (“Фильтрация клиентов по IP”). После этого расписание начнет использоваться на странице “Access Control” (“Управление доступом”).

Настройка фильтрации MAC-адресов

Фильтр MAC-адресов – мощное средство безопасности, позволяющее указывать компьютеры, которым разрешен доступ к сети. Ни один компьютер, не указанный в списке фильтра, не будет допущен в сеть. После включения этой функции необходимо ввести MAC-адрес каждого клиента (компьютера) сети, чтобы предоставить им право доступа к сети. Пункт "Block" ("Блокировать") позволяет включать и отключать доступ любого компьютера к сети без необходимости добавлять MAC-адрес этого компьютера в список или удалять его из списка. Чтобы включить эту функцию, выберите пункт "Enable MAC Address Filtering" ("Включить фильтрацию MAC-адресов") (1). Затем выберите правило доступа: "Allow" ("Разрешить доступ") или "Deny" ("Отказать в доступе").

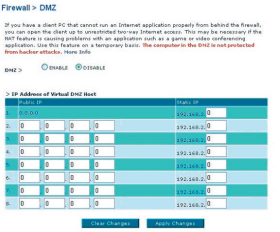
Введите MAC-адрес каждого компьютера сети, выбрав его в раскрывающемся списке "DHCP Client List" ("Перечень клиентов DHCP") (2), затем выберите идентификатор для копирования адреса (3) и нажмите "Copy to" ("Копировать в..."). Другой способ: щелкните на соответствующем поле (4) [Designer: pls callout (4) in the screenshot] и введите MAC-адрес компьютера, который нужно добавить в список. Чтобы сохранить настройки, нажмите "Apply Changes" ("Применить") (5).

Примечание: Невозможно удалить MAC-адрес компьютера, используемого для доступа к администраторским функциям маршрутизатора (компьютера, который вы используете сейчас).



DMZ (демилитаризированная зона)

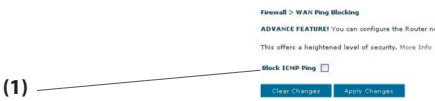
Если на одном из клиентских ПК не удается запустить какое-либо Интернет-приложение по причине работы брандмауэра, этому клиенту можно разрешить неограниченный двусторонний доступ к Интернет. Это может понадобиться, если функция NAT (трансляции сетевых адресов) создает проблемы для таких приложений, как игры или видеоконференции. Не пользуйтесь этой функцией постоянно. В режиме DMZ компьютер не защищен от попыток взлома.



Чтобы перевести компьютер в демилитаризированную зону (DMZ), введите в соответствующее поле последние цифры его IP-адреса и выберите “Enable” (“Включить”). Для применения нажмите “Apply Changes” (“Применить”). При использовании нескольких статических IP-адресов внешней сети можно выбрать, на какой из них будет направлен DMZ-хост. Введите IP-адрес во внешней сети, на который следует направить DMZ-хост, введите две последние цифры IP-адреса главного DMZ-компьютера, выберите “Enable” (“Включить”) и нажмите “Apply Changes” (“Применить”).

Блокирование ICMP-тестирования

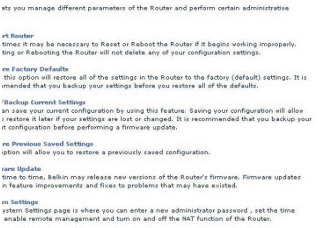
Для поиска потенциальных жертв в Интернет компьютерные взломщики пользуются так называемым “эхо-тестированием” (pinging). Эхо-тестируя конкретный IP-адрес и получая от него отклик, взломщик может определить, есть ли по адресу нечто такое, что может его заинтересовать. Маршрутизатор можно настроить так, что он не будет откликаться на ICMP-тестирование извне. Это повышает степень защищенности маршрутизатора.



Чтобы отключить отклик на эхо-тестирование, выберите опцию “Block ICMP Ping” (“Блокировать ICMP-тестирование”) (1) и нажмите “Apply Changes” (“Применить”). Теперь маршрутизатор не будет откликаться на ICMP-тестирование.

Служебные программы

В окне “Utilities” (“Служебные программы”) можно управлять различными параметрами маршрутизатора и выполнять определенные административные функции.



Перезапуск маршрутизатора

Подчас возникает необходимость перезагрузить или перезапустить маршрутизатор, если в его работе возникают сбои. Перезагрузка или перезапуск маршрутизатора НЕ УДАЛЯЮТ какие-либо настройки устройства.

Перезагрузка маршрутизатора для возврата к нормальной работе

1. Щелкните на кнопке “Restart Router” (“Перезапустить маршрутизатор”).

2. Появится следующее сообщение: Нажмите “OK”, чтобы перезапустить маршрутизатор.

Восстановление заводских настроек

Данная функция позволяет вернуть все настройки маршрутизатора к заводским значениям по умолчанию. Перед этим рекомендуется сделать резервную копию настроек.

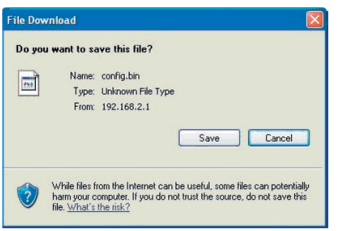
1. Щелкните на кнопке “Restore Defaults” (“Восстановить настройки по умолчанию”).

2. Появится следующее сообщение: Нажмите “OK”, чтобы восстановить заводские настройки.

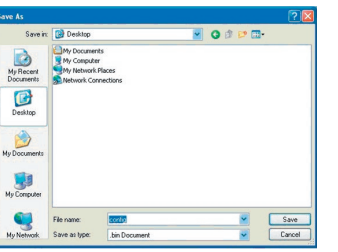
Сохранение и резервное копирование текущих настроек

Эта функция позволяет сохранить текущую конфигурацию. Сохранение конфигурации позволит восстановить ее, если настройки были утрачены или изменены. Перед обновлением встроенного ПО рекомендуется сделать резервную копию конфигурации.

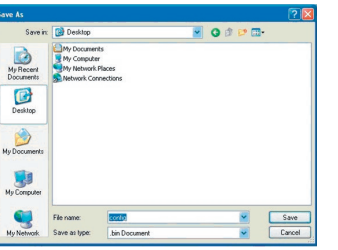
1. Нажмите “Save” (“Сохранить”). Откроется окно “File Download” (“Загрузка файла”). Нажмите “Save” (“Сохранить”).



2. Появится окно, где можно выбрать место для сохранения файла конфигурации. Выберите место для размещения файла. Файлу можно дать любое имя, однако постарайтесь назвать его так, чтобы легко найти в дальнейшем. После выбора места сохранения и имени файла нажмите “Save” (“Сохранить”).



3. По окончании сохранения появится следующее окно: Нажмите “Close” (“Закрыть”). Конфигурация сохранена.



Восстановить прежние настройки

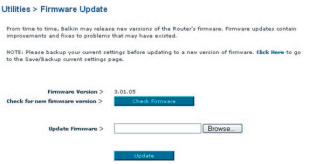
Данная функция позволяет восстановить ранее сохраненную конфигурацию.

1. Нажмите “Browse” (“Обзор”). Появится окно, где можно выбрать местонахожение файла конфигурации. Найдите файл конфигурации (“config.bin”) и дважды щелкните на нем.

2. Нажмите “Open” (“Открыть”).

Обновление встроенного ПО

Время от времени компания Belkin выпускает новые версии встроенного ПО маршрутизатора. Обновления встроенного ПО содержат улучшения прежних версий и исправления существующих проблем. После выпуска компанией Belkin новых версий встроенного ПО их можно загрузить с сайта обновления Belkin и установить новейшую версию встроенного ПО маршрутизатора.



Поиск новых версий встроенного ПО

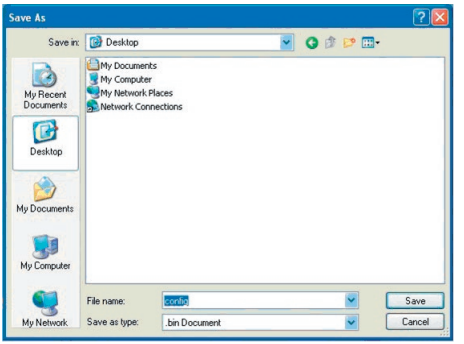
С помощью кнопки “Check Firmware” (“Найти встроенное ПО”) (1) [Designer: pls callout (1) in the screenshot] можно провести быстрый поиск новой версии встроенного ПО. При нажатии на эту кнопку появится новое окно обозревателя с сообщением о наличии или отсутствии новой версии встроенного ПО. Если она найдена, появится возможность ее загрузить.

Загрузка новой версии встроенного ПО

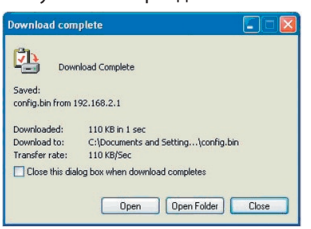
Если после нажатия на кнопку “Check Firmware” (“Поиск обновлений ПО”) найдена новая версия встроенного ПО, появится окно, схожее с показанным ниже:

1. Для загрузки новой версии встроенного ПО нажмите “Download” (“Загрузить”).

2. Появится окно, где можно выбрать место сохранения файла встроенного ПО. Выберите место для размещения файла. Файлу можно присвоить любое имя либо оставить имя по умолчанию. Необходимо сохранить файл в таком месте, чтобы вы смогли впоследствии найти его. После выбора места для размещения нажмите “Save” (“Сохранить”).

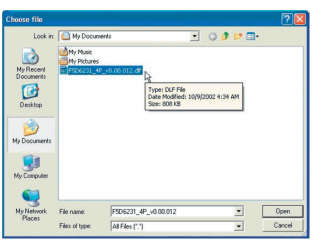


3. По окончании сохранения появится следующее окно: Нажмите “Close” (“Закрыть”). Загрузка встроенного ПО завершена. Для обновления встроенного ПО следуйте указаниям раздела “Обновление встроенного ПО маршрутизатора”.



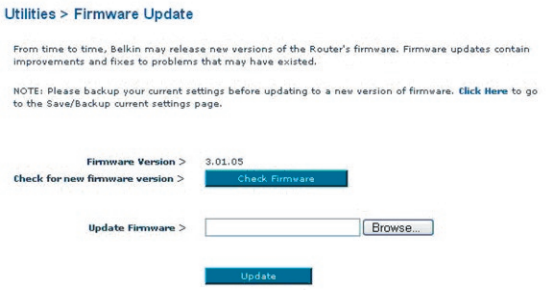
Обновление встроенного ПО маршрутизатора

1. На странице “Firmware Update” (“Обновление встроенного ПО”) нажмите “Browse” (“Обзор”) (2) [Designer: pls callout (2) in the screenshot]. Появится окно, где можно выбрать местонахождение файла обновления встроенного ПО.

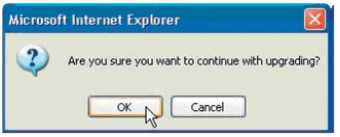


2. Перейдите к загруженному файлу обновления встроенного ПО. Дважды щелкните на имени этого файла.

3. Теперь в поле “Update Firmware” (“Обновить встроенное ПО”) будут отображаться местоположение и имя выбранного файла. Нажмите “Update” (“Обновить”).



4. Последует запрос о продолжении. Нажмите “OK”.



5. Появится еще одно сообщение. Оно предупреждает о том, что при загрузке встроенного ПО в маршрутизатор он может не откликаться в течение минуты, после чего перезагрузится. Нажмите “OK”.

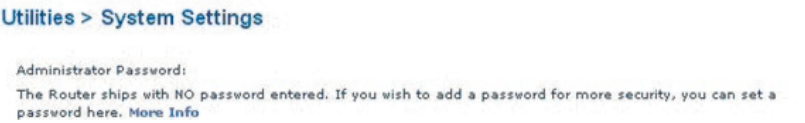
На экране появится 60-секундный обратный отсчет. По достижении нулевого значения обновление встроенного ПО маршрутизатора будет завершено. После этого должна автоматически открыться начальная страница маршрутизатора. Если этого не произойдет, введите в панель навигации Web-обозревателя адрес маршрутизатора (по умолчанию: “192.168.2.1”).

Параметры системы

На странице “System Settings” (“Параметры системы”) можно ввести новый пароль администратора, установить часовой пояс, включить возможность удаленного управления и включить или выключить функцию UPnP маршрутизатора.

Задание или изменение пароля администратора

Маршрутизатор поставляется БЕЗ заданного пароля. Чтобы использовать пароль для усиления защиты, задайте его здесь. Запишите свой пароль и храните в надежном месте, так как в дальнейшем он потребуется для входа в систему маршрутизатора. Пароль также рекомендуется задать, если вы намерены пользоваться функцией удаленного управления маршрутизатором.



Изменение срока автоматического выхода

Функция автоматического выхода позволяет настроить срок пребывания в интерфейсе дополнительных настроек маршрутизатора. Таймер влючается при отсутствии активности - например, если вы вносили какие-либо изменения в расширенном интерфейсе установки, а затем отошли от компьютера без выхода из системы. Если таймер установлен на 10 минут, то через 10 минут бездействия срок сеанса работы с системой истечет. Для внесения новых изменений вновь придется входить в систему маршрутизатора. Функция автоматического выхода предназначена для обеспечения безопасности, срок по умолчанию – 10 минут. Примечание: С расширенным интерфейсом настройки маршрутизатора не могут работать несколько компьютеров одновременно.

Установка времени и часового пояса

Маршрутизатор поддерживает внутреннее время путем подключения к серверу SNTP (Простой протокол сетевого времени). Это позволяет маршрутизатору синхронизитировать системные часы с глобальным временем Интернет. Синхронизированные часы маршрутизатора используются для ведения записей журнала защиты и управления фильтрацией клиентов. Выберите свой часовой пояс. Если в вашей местности осуществляются переходы на летнее время, установите отметку в поле “Enable Daylight Saving” (“Включить переходы на летнее время и обратно”). Для обновления системных часов может потребоваться некоторое время. Маршрутизатору может понадобиться по меньшей мере 15 минут для установления связи с серверами времени Интернет и получения ответа. Выставить часы самостоятельно невозможно. Есть возможность выбирать первичный и резервный NTP-сервер для синхронизации часов маршрутизатора с разными NTP-серверами времени через Интернет. Выберите нужный NPT-сервер в раскрывающемся списке или просто оставьте в этом поле текущий сервер.

Включение удаленного управления

Прежде чем включать эту функцию маршрутизатора Belkin, УБЕДИТЕСЬ, ЧТО ЗАДАЛИ ПАРОЛЬ АДМИНИСТРАТОРА. Удаленное управление позволяет изменять настройки маршрутизатора удаленно, через Интернет.

Есть два способа удаленного управления маршрутизатором. Первый предоставляет доступ к маршрутизатору дистанционно, через Интернет; для этого следует выбрать опцию "Any IP address can remotely manage the Router" ("Любой IP-адрес имеет право удаленного управления маршрутизатором"). Теперь если на любом компьютере, подключенном к Интернет, ввести свой IP-адрес внешней сети, появится окно входа в систему маршрутизатора, где нужно будет ввести пароль. Второй способ предоставляет право удаленного управления маршрутизатором только конкретному IP-адресу. Этот способ более безопасен, но менее удобен. Чтобы воспользоваться им, введите в соответствующее поле IP-адрес, с которого намерены получать доступ к маршрутизатору, и выберите опцию "Only this IP address can remotely manage the Router" ("Только этот IP-адрес имеет право удаленного управления маршрутизатором").

Перед включением этой функции НАСТОЯТЕЛЬНО РЕКОМЕНДУЕТСЯ задать пароль администратора. Если этот пароль не задан, маршрутизатор будет потенциально открыт для вторжения извне. По умолчанию в качестве порта доступа используется порт 8080. Чтобы изменить это значение, введите в поле "remote port "("порт удаленного доступа") номер другого порта. Нажмите "Apply Changes" ("Применить"), чтобы сохранить настройки.

Включение и отключение NAT (трансляции сетевых адресов)

Примечание: Эту дополнительную функцию рекомендуется задействовать только опытным пользователям. Прежде чем включать эту функцию, УБЕДИТЕСЬ, ЧТО ЗАДАЛИ ПАРОЛЬ АДМИНИСТРАТОРА. Трансляция сетевых адресов (NAT) - метод, с помощью которого маршрутизатор обеспечивает совместное использование одного IP-адреса, предоставленного поставщиком услуг Интернет, всеми компьютерами вашей сети. Отключать NAT следует лишь в том случае, если поставщик услуг предоставляет вам несколько IP-адресов либо если вам необходимо отключить NAT для настройки более сложной системной конфигурации. Если у вас только один IP-адрес, то при отключении NAT компьютеры вашей сети не смогут получать доступ к Интернет. Кроме того, могут возникать и другие проблемы. Отключение NAT одновременно отключает функции брандмауэра.

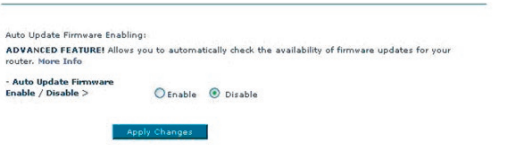
Включение и отключение UPnP (Universal Plug-and-Play).

UPnP - еще одна дополнительная функция маршрутизатора Belkin. Эта технология обеспечивает прямую работу систем речевых и видеосообщений, игр и других приложений, поддерживающих стандарт UPnP.

Для правильной работы некоторых приложений необходимо соответствующим образом настроить брандмауэр маршрутизатора. Обычно для этого требуется открыть порты TCP и UDP, а в некоторых случаях настроить триггерные порты. Приложение, поддерживающее UPnP, способно связаться с маршрутизатором и "подсказать" ему, как именно следует настроить брандмауэр. Маршрутизатор поставляется с отключенной функцией UPnP. Включите эту функцию, если используете UPnP-приложения и хотите получить максимальные преимущества от возможностей UPnP. Для этого выберите опцию "Enable" ("Включить") в разделе "UPnP Enabling" ("Включение UPnP") на странице "Utilities" ("Служебные программы"). Чтобы сохранить изменения, нажмите "Apply Changes" ("Применить").

Включение и выключение автоматического обновления встроенного ПО

Это новшество означает, что маршрутизатор оснащен встроенной возможностью автоматически искать новые версии встроенного ПО и сообщать об их выявлении. При входе в расширенный пользовательский Web-интерфейс маршрутизатор проведет поиск обновлений встроенного ПО. Он сообщит об их выявлении. После этого можно загрузить новую версию или отказаться от загрузки. Маршрутизатор поставляется с отключенной функцией автоматического поиска. Чтобы включить ее, выберите пункт "Enable" ("Включить") и нажмите "Apply Changes" ("Применить").



Настройка компьютеров

Для правильной связи компьютера с маршрутизатором необходимо изменить сетевые настройки "TCP/IP/Ethernet" компьютера на "Obtain an IP address automatically/Using DHCP" ("Получать IP-адрес автоматически / С помощью DHCP"). Для большинства домашних компьютеров это стандартная настройка.
Следуя описанным шагам, СПЕРВА настройте компьютер, подключенный к ADSL-модему. Те же этапы используются для добавления компьютеров к маршрутизатору после того, как настроено его подключение к Интернет.

Настройка сетевых адаптеров вручную

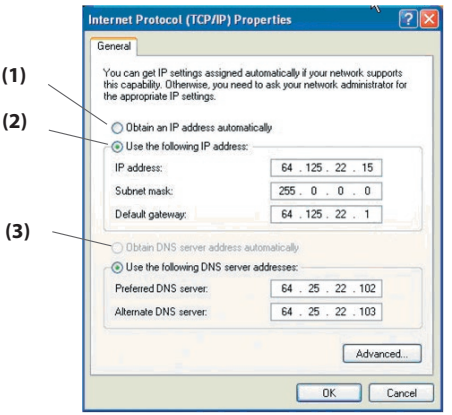
Windows XP, 2000 или NT

1. Выберите “Start > Settings > Control Panel” (“Пуск > Настройка > Панель управления”).

2. Дважды щелкните на значке “Network and dial-up connections” (“Сетевые и коммутируемые соединения”) в Windows 2000) или “Network” (“Сеть”) в Windows XP.

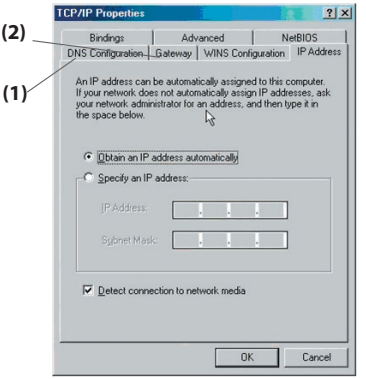
3. Щелкните правой кнопкой на пункте “Local Area Connection” (“Подключение по локальной сети”), соответствующем вашему сетевому адаптеру, и выберите в раскрывающемся меню пункт “Properties” (“Свойства”).

4. В окне “Local Area Connection Properties” (“Свойства подключения по локальной сети”) щелкните на опции “Internet Protocol (TCP/IP)” (“Протокол Интернет (TCP/IP)”), затем на кнопке “Properties” (“Свойства”). Появится следующее окно:



5. Если выбран пункт “Use the following IP address” (“Использовать следующий IP-адрес”) (2) [Designer:] pls callout (2) in the screenshot above], маршрутизатор необходимо настроить на подключение через статический IP-адрес. Введите информацию об адресах в таблицу ниже. Позднее эти данные нужно будет ввести в маршрутизатор.

6. Если эти опции еще не выбраны, выберите "Obtain an IP address automatically" ("Получать IP-адрес автоматически") (1) и "Obtain DNS server address automatically" ("Получать адрес DNS-сервера автоматически") (3). Нажмите "OK". Теперь сетевые адаптеры настроены на работу с маршрутизатором.

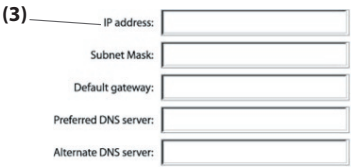


Windows 98SE или ME

1. Щелкните правой кнопкой на пункте "My Network Neighborhood" ("Сетевое окружение") и выберите в раскрывающемся меню пункт "Properties" ("Свойства").

2. Выберите "TCP/IP > Settings" ("TCP/IP > Параметры") для установленного сетевого адаптера. Появится следующее окно:

3. Если отмечен пункт "Specify an IP Address" ("Указать IP-адрес"), маршрутизатор необходимо настроить на подключение через статический IP-адрес. Введите информацию об адресах в таблицу ниже. Позднее эти данные нужно будет ввести в маршрутизатор.



4. Запишите IP-адрес и маску подсети из вкладки "IP Address" ("IP-адрес") (3).

5. Щелкните на вкладке "Gateway" ("Шлюз") (2). Впишите в таблицу адрес шлюза.

6. Щелкните на вкладке "DNS Configuration" ("Конфигурация DNS") (1). Впишите в таблицу адрес(а) DNS.

7. Если эта опция еще не выбрана, выберите "Obtain an IP address automatically" ("Получать IP-адрес автоматически") на вкладке "IP Address" ("IP-адрес"). Нажмите "OK". Перезагрузите компьютер. После перезапуска компьютера сетевой адаптер (или адаптеры) будет настроен на работу с маршрутизатором. Используя данные шаги, ПЕРВЫМ настройте компьютер, подключенный к кабельному или DSL-модему. Те же шаги можно использовать для добавления компьютеров к маршрутизатору после того, как он настроен на подключение к Интернет.

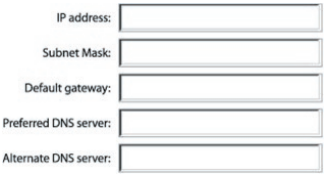
Mac OS вплоть до версии 9.x

Для правильной связи компьютера с маршрутизатором необходимо изменить настройки TCP/IP компьютера Mac TCP/IP на DHCP.

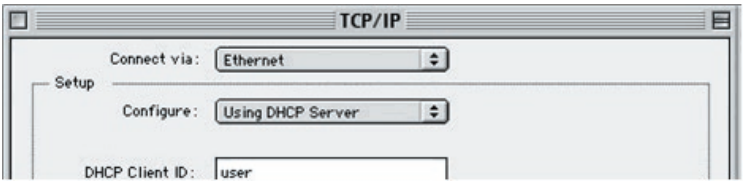
1. Откройте меню Apple. Выберите "Control Panels" ("Панели управления"), затем "TCP/IP".

2. Откроется панель управления TCP/IP. В раскрывающемся меню "Connect via:" ("Подключиться с помощью") выберите "Ethernet Built-In" или "Ethernet" (1).

3. Если ниже, в меню “Configure” (“Настроить”) (2) [Designer: pls callout (2) in the screenshot above], выбран пункт “Manually” (“Вручную”), маршрутизатор необходимо настроить на подключение через статический IP-адрес. Введите информацию об адресах в таблицу ниже. Позднее эти данные нужно будет ввести в маршрутизатор.



4. Если эта опция еще не выбрана, в меню “Configure” (“Настроить”) выберите пункт “Using DHCP Server” (“С помощью DHCP-сервера”). В этом случае компьютер получит IP-адрес от маршрутизатора.



5. Закройте окно. Если были внесены какие-либо изменения, появится следующее окно: Нажмите “Save” (“Сохранить”).

Перезапустите компьютер. После перезапуска компьютера сетевые параметры будут настроены на работу с маршрутизатором.

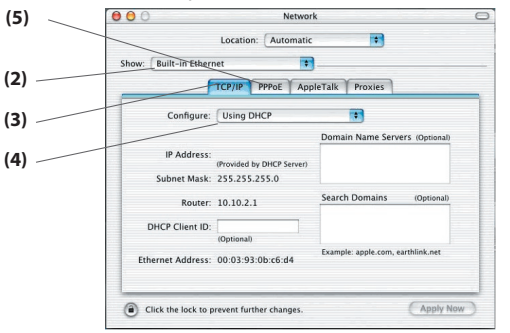
Mac OS X

1. Щелкните на значке “System Preferences” (“Системные установки”).

2. В меню “System Preferences” (“Системные установки”) выберите “Network” (“Сеть”) (1).

3. В меню “Network” (“Сеть”) выберите “Built-in Ethernet” (“Встроенный Ethernet”) (2) рядом с пунктом “Show” (“Показать”).

4. Перейдите на вкладку “TCP/IP” (3). Рядом с пунктом “Configure” (“Настроить”) (4) должен быть пункт “Manually” (“Вручную”) или “Using DHCP” (“С помощью DHCP”). Если их нет, перейдите на вкладку PPPoE (5) и убедитесь, что там НЕ выбран пункт “Connect using PPPoE” (“Подключение через PPPoE”). Если он выбран, придется настраивать маршрутизатор на соединение PPPoE с использованием имени пользователя и пароля.



5. Если выбран пункт “Manually” (“Вручную”), маршрутизатор необходимо настроить на тип подключения через статический IP-адрес. Введите информацию об адресах в таблицу ниже. Позднее эти данные нужно будет ввести в маршрутизатор.

IP address:	
Subnet Mask:	
Default gateway:	
Preferred DNS server:	
Alternate DNS server:	

6. Если этот пункт еще не выбран, рядом с опцией “Configure” (“Настроить”) выберите пункт “Using DHCP” (“С помощью DHCP”) (4) и нажмите “Apply Now” (“Применить”).

Теперь сетевые адаптеры настроены на работу с маршрутизатором.

Рекомендуемые настройки Web-обозревателя

В большинстве случаев менять настройки Web-обозревателя не придется. Если возникают проблемы с доступом к Интернет или расширенному пользовательскому Web-интерфейсу, измените настройки Web-обозревателя на рекомендуемые в данном разделе.

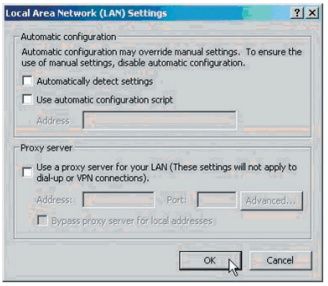
Microsoft Internet Explorer 4.0 или более поздние версии

1. Запустите Web-обозреватель. Выберите “Tools” (“Сервис”), затем “Internet Options” (“Свойства обозревателя”).

2. В окне “Internet Options” (“Свойства обозревателя”) есть три переключателя:

“Never dial a connection” (“Никогда не использовать”), “Dial whenever a network connection is not present” (“Использовать при отсутствии подключения к сети”) и “Always dial my default connection” (“Всегда использовать принятое по умолчанию подключение”). Если есть возможность выбора, включите “Never dial a connection” (“Никогда не использовать”). Если выбор невозможен, переходите к следующему шагу.

3. В окне “Internet Options” (“Свойства обозревателя”) щелкните на вкладке “Connections” (“Подключение”) и выберите “LAN Settings…” (“Настройка сети”).

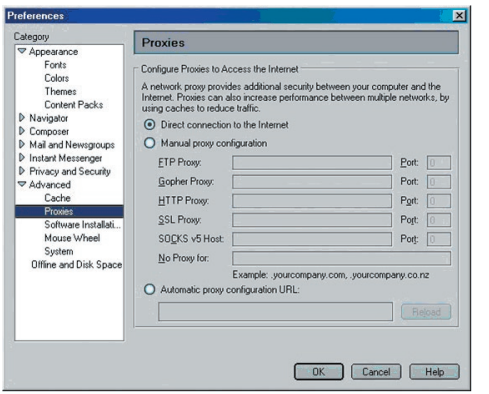


4. Убедитесь, что не отмечена ни одна из следующих опций: “Automatically detect settings” (“Автоматическое определение параметров”), “Use automatic configuration script” (“Использовать сценарий автоматической настройки”) и “Use a proxy server” (“Использовать прокси-сервер”). Нажмите “OK”. Еще раз нажмите “OK” в окне “Internet Options” (“Свойства обозревателя”).

Netscape® Navigator® 4.0 или более поздние версии

1. Запустите Netscape. Щелкните на меню “Edit”, затем на пункте “Preferences”.

2. В окне “Preferences” щелкните на “Advanced” и выберите “Proxies”. В окне “Proxies” (“Прокси”) выберите “Direct connection to the Internet” (“Прямое подключение к Интернет”).



Устранение неисправностей

Проблема:

Не светится индикатор ADSL.

Решение:

1. Проверьте аппаратное соединение между маршрутизатором и линией ADSL. Убедитесь, что кабель от ADSL-линии подсоединен к порту "DSL Line" ("Линия DSL") маршрутизатора.
2. Убедитесь, что маршрутизатор подключен к питанию. Индикатор питания [Insert: Power Icon] на лицевой панели должен светиться.

Проблема:

Не светится индикатор Интернет.

Решение:

1. Убедитесь, что кабель от ADSL-линии подсоединен к порту "DSL Line" ("Линия DSL") маршрутизатора и светится индикатор ADSL [Insert: ADSL icon].
2. Убедитесь, что поставщик услуг Интернет предоставил правильные VPI/VCI, имя пользователя и пароль.

Проблема:

Мой тип подключения - статический IP-адрес. Не удается установить подключение к Интернет.

Решение:

Поскольку используется подключение через статический IP-адрес, поставщик услуг Интернет обязан предоставить вам IP-адрес, маску подсети и адрес шлюза. Не запуская Мастер, перейдите на страницу "Connection Type" ("Тип подключения") и выберите свой тип подключения. Нажмите "Next" ("Далее"), выберите "Static IP" ("Статический IP") и введите свой IP-адрес, маску подсети и шлюз по умолчанию.

Проблема:

Я забыл или потерял свой пароль.

Решение:

Прижмите кнопку "Reset" ("Сброс") на задней панели по меньшей мере на шесть секунд для восстановления заводских настроек по умолчанию.

Проблема:

На моем ПК с беспроводным подключением нет связи с маршрутизатором.

Решение:

1. Убедитесь, что на ПК и маршрутизаторе совпадают настройки SSID и что на клиентах заданы одинаковые параметры защиты - такие, как WPA- или WEP-шифрование.
2. Убедитесь, что расстояние между маршрутизатором и ПК не слишком велико.

Проблема:

Часто прерывается беспроводная связь.

Решение:

1. Перенесите ПК с беспроводным подключением ближе к маршрутизатору, чтобы улучшить сигнал.
2. Возможно, на связь влияют помехи от микроволновой печи или беспроводных телефонов, работающих в полосе 2,4 ГГц. Перенесите маршрутизатор в другое место или измените канал беспроводной связи.

Проблема:

Не удается установить беспроводное подключение к Интернет.

Решение:

Если не удается установить подключиться к Интернет с беспроводного компьютера, проделайте следующее:

1. Посмотрите на индикаторы маршрутизатора. При использовании маршрутизатора Belkin индикация должна быть такой:

• Светится индикатор “Power” (“Питание”).
• Светится и не мигает индикатор “Connected” (“Соединение”).
• Светится или мигает индикатор “WAN” (“Внешняя сеть”).

2. Откройте служебную программу беспроводной связи, щелкнув на значке на панели задач в правом нижнем углу экрана. При использовании карты беспроводной связи Belkin этот значок выглядит следующим образом [INSERT ICON] (может быть красным или зеленым):
3. Открывшееся окно может выглядеть по-разному в зависимости от модели используемой карты беспроводной связи; тем не менее, в любой версии служебной программы должен быть виден список “Available Networks” (“Доступные сети”) - все беспроводные сети, к которым можно подключиться.

Есть ли в этом списке название вашей беспроводной сети?
Да, в списке есть название моей сети - перейдите к решению проблемы “Не удается

установить беспроводное подключение к Интернет, хотя моя сеть есть в списке". Нет, в списке нет названия моей сети – перейдите к решению проблемы "Не удается установить беспроводное подключение к Интернет, и моей сети нет в списке".

Проблема:

Не удается установить беспроводное подключение к Интернет, хотя моя сеть есть в списке.

Решение:

Если имя вашей сети есть в списке "Available Networks" ("Доступные сети"), следуйте приведенным ниже указаниям по установке беспроводного подключения:

1. Щелкните на имени нужной сети в списке "Available Networks" ("Доступные сети"). Если в сети включена система защиты (шифрования), потребуется ввести сетевой ключ. Более подробно о безопасности см. на странице под заголовком "Изменение параметров защиты беспроводной связи".
2. Через несколько секунд значок на панели задач в правом нижнем углу экрана станет зеленым, что означает успешное подключение к сети.

Проблема:

Не удается установить беспроводное подключение к Интернет, и моей сети нет в списке.

Решение:

Если имени нужной сети нет в списке "Available Networks" ("Доступные сети") служебной программы беспроводной связи, попробуйте сделать следующее:

1. Если возможно, временно разместите компьютер на расстоянии 1,5–3 метра от маршрутизатора. Закройте служебную программу беспроводной связи и вновь запустите ее. Если теперь имя нужной сети есть в списке "Available Networks" ("Доступные сети"), проблема может быть связана с расстоянием до маршрутизатора или помехами. Воспользуйтесь рекомендациями Приложения B: "Что учесть при размещении и настройке".

2. На компьютере, подключенном к маршрутизатору сетевым кабелем (в противоположность беспроводной связи), включите опцию "Broadcast SSID" ("Транслировать SSID"). Данный параметр находится на странице беспроводной конфигурации "Channel and SSID" ("Канал и SSID") маршрутизатора.

Если после этих шагов по-прежнему не удается получить доступ к сети Интернет, обратитесь в службу технической поддержки Belkin.

Проблема:

Беспроводная сеть работает неудовлетворительно.
Скорость передачи данных иногда очень низка.
Плохой уровень сигнала.
Возникают сложности с установлением и поддержкой связи с виртуальной частной сетью (VPN).

Решение:

Беспроводные технологии основаны на радиоволнах, а это означает, что качество связи и пропускная способность снижаются по мере увеличения расстояния между устройствами. Другими причинами ухудшения уровня сигнала, главной из которых обычно является металл, могут стать такие источники помех, как стены или металлические приспособления. Таким образом, обычный радиус действия беспроводных устройств в помещении составляет от 30 до 60 метров. Обратите также внимание, что скорость работы соединения может снижаться по мере удаления от маршрутизатора или узла доступа.

Чтобы определить, связана ли данная проблема беспроводной связи с расстоянием, рекомендуется, если это возможно, ненадолго перенести компьютер на расстояние 1,5-3 метра от маршрутизатора.

Изменение канала беспроводной связи – В зависимости от насыщенности локальной беспроводной связи и уровня помех переключение на другой канал может повысить качество и надежность беспроводной сетевой связи. По умолчанию маршрутизатор настроен на канал 11. В зависимости от места жительства, можно выбрать один из нескольких других каналов (указания по смене каналов см. в разделе "Изменение канала беспроводной связи" на стр. XX).

Ограничение скорости беспроводной передачи - Ограничение скорости беспроводной передачи может улучшить максимальный радиус действия беспроводной связи и повысить устойчивость соединения. Большинство карт беспроводной связи позволяет ограничивать скорость передачи. Чтобы изменить это свойство, откройте панель управления Windows, выберите "Network Connections" ("Сетевые подключения") и дважды щелкните на подключении беспроводной карты. В диалоговом окне "Свойства" нажмите кнопку "Настроить" на вкладке "Общее" (пользователям Windows 98 нужно выбрать в списке беспроводную карту и нажать кнопку "Свойства"), затем выберите вкладку "Дополнительно" и задайте скорость передачи. Беспроводные карты клиентов обычно устанавливаются на автоматическое регулирование скорости передачи, однако это может повлечь периодические прерывания соединений, когда сигнал беспроводной связи становится слишком слабым; как правило, чем ниже скорость передачи, тем устойчивее соединение. Попробуйте устанавливать разные скорости передачи до тех пор, пока не подберете значение, наиболее подходящее для ваших условий работы; обратите внимание, что все имеющиеся в списке скорости передачи являются достаточными для работы в Интернет. Подробнее см. руководство к эксплуатации карты беспроводной связи.

Проблема:

Как увеличить радиус действия беспроводной сети?

Решение:

Компания Belkin рекомендует использовать следующие изделия, увеличивающие покрытие беспроводной сети для больших домов и офисов:

- Беспроводной узел доступа: Беспроводной узел доступа может практически удвоить площадь покрытия беспроводной сети. Узел доступа обычно размещают в месте,

на которое не распространяется действие беспроводного маршрутизатора. Он подключается к маршрутизатору с помощью кабеля Ethernet или через домашнюю линию электроснабжения с помощью двух Ethernet-адаптеров связи через электросеть.

- Для беспроводных сетей 802.11g (54g) компания Belkin предлагает беспроводной расширитель радиуса / узел доступа, который можно подключить к беспроводному маршрутизатору Belkin 802.11g без использования Ethernet-кабеля или Ethernet-адаптеров связи через электросеть.

Изделия Belkin можно приобрести у местных розничных торговцев или заказать непосредственно в компании Belkin.

Чтобы подробнее узнать о расширителях радиуса и покрытия сети, посетите сайт: www.belkin.com/networking. Там можно найти сведения о:

Расширителе диапазона беспроводной связи / узле доступа Wireless G (F5D7132)

Проблема:

Возникли проблемы с настройкой WEP-защиты на маршрутизаторе или узле доступа Belkin.

Решение:

1. Войдите в систему беспроводного маршрутизатора или узла доступа.
2. Откройте Web-обозреватель и введите IP-адрес беспроводного маршрутизатора или узла доступа. (по умолчанию адрес маршрутизатора: "192.168.2.1", узла доступа: "192.168.2.254"). Войдите в систему маршрутизатора, щелкнув на кнопке "Login" в правом верхнем углу экрана. Потребуется ввести пароль. Если пароль не был задан, оставьте поле пароля пустым и нажмите "Submit" ("Отправить").
3. Щелкните на вкладке "Wireless" ("Беспроводная связь") в левой части экрана. Для перехода на страницу настроек защиты выберите вкладку "Encryption" ("Шифрование") или "Security" ("Защита").
4. В раскрывающемся меню выберите "128-bit WEP" ("128-битный WEP").
5. После выбора режима WEP-шифрования, можно вручную ввести шестнадцатеричный WEP-ключ либо ввести фразу-пароль в поле "Passphrase" ("Фраза-пароль") и нажать "Generate" ("Сгенерировать"), чтобы создать WEP-ключ на основе фразы-пароля. Для завершения нажмите "Apply Changes" ("Применить"). Теперь следует настроить все клиенты в соответствии с данными установками. Шестнадцатеричный ключ представляет собой сочетание букв от A до F и цифр от 0 до 9. Для 128-битного WEP нужно ввести 26 шестнадцатеричных знаков.

Например:

C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = 128-битный ключ

6. Для завершения нажмите "Apply Changes" ("Применить"). Режим шифрования беспроводного маршрутизатора установлен. Теперь все компьютеры данной беспроводной сети должны быть настроены с теми же параметрами защиты.

ПРЕДУПРЕЖДЕНИЕ: Если настройка беспроводного маршрутизатора или узла доступа осуществляется на компьютере с клиентом беспроводной связи,

убедитесь, что для этого беспроводного клиента защита включена. В противном случае беспроводное соединение прервется.

Примечание для пользователей Mac: Оригинальная продукция Apple AirPort поддерживает только 64-битное шифрование. Продукция Apple AirPort 2 может поддерживать 64- или 128-битное шифрование. Проверьте версию используемой вами продукции Apple AirPort. Если не удается настроить сеть на 128-битное шифрование, попробуйте использовать 64-битное.

Проблема:

Возникла проблема с настройкой WEP-защиты на беспроводной карте Belkin.

Решение:

Карта беспроводной связи должна использовать тот же ключ, который используется беспроводным маршрутизатором или узлом доступа. Например, если беспроводной маршрутизатор или узел доступа используют ключ 00112233445566 778899AABBCC, такой же ключ должна использовать и беспроводная карта.

1. Дважды щелкните на значке “Signal Indicator” (“Индикатор сигнала”), после чего появится окно “Wireless Networks” (“Беспроводные сети”).
2. Кнопка “Advanced” (“Дополнительно”) позволяет просматривать и настраивать дополнительные параметры карты.
3. После нажатия на кнопку “Advanced” (“Дополнительно”) откроется служебная программа беспроводной локальной сети Belkin. С помощью этой программы можно управлять всеми дополнительными функциями беспроводной карты Belkin.
4. На вкладке “Wireless Network Properties” (“Свойства беспроводной сети”) выберите имя сети в списке “Available networks” (“Доступные сети”) и нажмите кнопку “Properties” (“Свойства”).
5. В поле “Data Encryption” (“Шифрование данных”) выберите “WEP”.
6. Убедитесь, что НЕ установлена отметка рядом с пунктом “The key is provided for me automatically” (“Ключ предоставляется автоматически”). Если данный компьютер используется для подключения к корпоративной сети, проконсультируйтесь со своим системным администратором о том, нужно ли устанавливать эту отметку.
7. Введите в поле “Network key” (“Сетевой ключ”) свой WEP-ключ.

Важное замечание: WEP-ключ представляет собой сочетание букв от A до F и цифр от 0 до 9. Для 128-битного WEP нужно ввести 26 знаков. Сетевой ключ должен совпадать с ключом, присвоенным беспроводному маршрутизатору или узлу доступа.
Например: C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = 128-битный ключ
8. Нажмите “OK”, затем “Apply” (“Применить”), чтобы сохранить настройки.
При использовании беспроводной карты ДРУГОГО производителя (не компании Belkin) обратитесь к руководству по эксплуатации этой карты.

Проблема:

Поддерживает ли продукция компании Belkin WPA?

Решение:

Примечание: Для использования защиты WPA на всех клиентах сети нужно установить поддерживающие этот стандарт обновления драйверов и программ. В период подготовки данных "Вопросов и ответов" компания Microsoft уже выпустила исправление защиты, которое можно загрузить бесплатно. Исправление предназначено только для операционной системы Windows XP.

Загрузить исправление можно здесь:
http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&displaylang=en

Кроме того, нужно загрузить с сайта службы поддержки Belkin новейший драйвер сетевой карты Wireless 802.11g для настольного ПК или ноутбука. В настоящее время другие операционные системы не поддерживаются. Исправление, разработанное компанией Microsoft, поддерживает только устройства с WPA-драйверами - такими, как продукция стандарта 802.11g компании Belkin.

Новейший драйвер можно найти на сайте: http://www.belkin.com/uk/support/tech/index.asp

Проблема:

Возникла проблема с настройкой WPA-защиты на беспроводном маршрутизаторе или узле доступа Belkin в домашней сети.

Решение:

1. В раскрывающемся меню "Security Mode" ("Режим защиты") выберите "WPA-PSK (no server)".
2. В меню "Encryption Technique" ("Методы шифрования") выберите "TKIP" или "AES". Этот параметр должен быть одинаковым для всех клиентов сети.
3. Введите предварительно согласованный ключ. Он может иметь длину от 8 до 63 знаков и состоять из букв, цифр, символов или пробелов. Тот же ключ должен использоваться на всех настраиваемых клиентах. Например, ваш PSK может выглядеть так: "Smith family network key" ("Сетевой ключ семьи Смитов").
4. Для завершения нажмите "Apply Changes" ("Применить"). Теперь следует настроить все клиенты в соответствии с данными установками.

Проблема:

Возникла проблема с настройкой WPA-защиты на беспроводном маршрутизаторе или узле доступа Belkin в корпоративной сети.

Решение:

Используйте эту опцию, если для распределения ключей клиентам сети

используется RADIUS-сервер. Она обычно используется в корпоративной среде.
1. В раскрывающемся меню “Security Mode” (“Режим защиты”) выберите пункт “WPA (with server)”.
2. В меню “Encryption Technique” (“Методы шифрования”) выберите “TKIP” или “AES”. Этот параметр должен быть одинаковым для всех клиентов сети.
3. В поле “RADIUS Server” введите IP-адрес RADIUS-сервера.
4. В поле “Radius Key” введите RADIUS-ключ.
5. Введите интервал смены ключа. Интервал смены ключа – частота распределения ключей (в пакетах).
6. Для завершения нажмите “Apply Changes” (“Применить”). Теперь следует настроить все клиенты в соответствии с данными установками.

Проблема:

Возникла проблема с настройкой WPA-защиты на беспроводной карте Belkin в домашней сети.

Решение:

Клиенты должны использовать тот же ключ, что и беспроводной маршрутизатор или узел доступа. Например, если в беспроводном маршрутизаторе или узле доступа используется ключ “Smith family network key” (“Сетевой ключ семьи Смитов”), тот же ключ должны использовать и клиенты.

1. Дважды щелкните на значке “Signal Indicator” (“Индикатор сигнала”), после чего появится окно “Wireless Networks” (“Беспроводные сети”).
2. Кнопка “Advanced” (“Дополнительно”) позволяет просматривать и настраивать дополнительные параметры карты.

3. После нажатия на кнопку “Advanced” (“Дополнительно”) откроется служебная программа беспроводной локальной сети Belkin. С помощью этой программы можно управлять всеми дополнительными функциями беспроводной карты Belkin.
4. На вкладке “Wireless Network Properties” (“Свойства беспроводной сети”) выберите имя сети в списке “Available networks” (“Доступные сети”) и нажмите кнопку “Properties” (“Свойства”).
5. В меню “Network Authentication” (“Проверка подлинности сети”) выберите пункт “WPA-PSK (no server)”.
6. Введите в поле “Network key” (“Сетевой ключ”) свой WPA-ключ.

Важное замечание: WPA-PSK представляет собой сочетание букв от A до Z и цифр от 0 до 9. Длина WPA-PSK может составлять от 8 до 63 знаков. Сетевой ключ должен совпадать с ключом, присвоенным беспроводному маршрутизатору или узлу доступа.
7. Для сохранения настроек нажмите “OK”, затем “Apply” (“Применить”).

Проблема:

Возникла проблема с настройкой WPA-защиты на беспроводной карте Belkin в корпоративной сети.

Решение:

1. Дважды щелкните на значке "Signal Indicator" ("Индикатор сигнала"), после чего появится окно "Wireless Networks" ("Беспроводные сети").
2. Кнопка "Advanced" ("Дополнительно") позволяет просматривать и настраивать дополнительные параметры карты.
3. После нажатия на кнопку "Advanced" ("Дополнительно") откроется служебная программа беспроводной локальной сети Belkin. С помощью этой программы можно управлять всеми дополнительными функциями беспроводной карты Belkin.
4. На вкладке "Wireless Network Properties" ("Свойства беспроводной сети") выберите имя сети в списке "Available networks" ("Доступные сети") и нажмите кнопку "Properties" ("Свойства").
5. В меню "Network Authentication" ("Проверка подлинности сети") выберите пункт "WPA".
6. На вкладке "Authentication" ("Проверка подлинности") выставьте параметры, предоставленные администратором сети.
7. Для сохранения настроек нажмите "OK", затем "Apply" ("Применить").

Проблема:

Возникла проблема с настройкой WPA-защиты, и я пользуюсь в домашней сети беспроводной картой ДРУГОГО производителя (не компании Belkin).

Решение:

Если вы пользуетесь беспроводной сетевой картой для настольных ПК или ноутбуков, произведенной ДРУГИМ изготовителем (не компанией Belkin) и ваша карта не оснащена программным обеспечением WPA, можно бесплатно загрузить созданный компанией Microsoft файл "Windows XP Support Patch for Wireless Protected Access" ("Исправление для защищенного беспроводного доступа для Windows XP"). Найдите это исправление в базе знаний Microsoft по ключевым словам "Windows XP WPA" и загрузите его.

Примечание: Данный файл компании Microsoft предназначен только для Windows XP. В настоящее время другие операционные системы не поддерживаются. Необходимо удостовериться, что производитель карты беспроводной связи поддерживает WPA, а также загрузить с сайта поддержки производителя и установить новейший драйвер.

Поддерживаемые операционные системы:
• Windows XP Professional
• Windows XP Home Edition

Включение WPA-PSK (без сервера)
1. В Windows XP выберите "Start > Control Panel > Network Connections"

(“Пуск>Панель управления>Сетевые подключения”).
2. Щелкните на вкладке “Wireless Networks” (“Беспроводные сети”) - откроется следующее окно. Установите отметку в поле “Use Windows to configure my wireless network settings” (“Использовать Windows для конфигурации беспроводной сети”).
3. На вкладке “Wireless Networks” (“Беспроводные сети”) нажмите “Configure” (“Настроить”).
4. Для домашнего и малого офиса выберите опцию “WPA-PSK” в пункте “Network Administration” (“Администрирование сети”).

Примечание:Выбирайте опцию “WPA (with radius server)” (WPA с RADIUS-сервером), если используете данный компьютер для подключения к корпоративной сети, поддерживающей сервер проверки подлинности (например, RADIUS-сервер). За более подробными сведениями обращайтесь к администратору своей сети.

5. В пункте “Data Encryption” (“Шифрование данных”) выберите “TKIP” или “AES”. Этот параметр должен совпадать с аналогичным параметром беспроводного маршрутизатора или узла доступа.
6. Введите в поле “Network key” (“Сетевой ключ”) свой шифровальный ключ.

Важное замечание: Введите свой предварительно согласованный ключ (PSK). Он может иметь длину от 8 до 63 знаков и состоять из букв, цифр и символов. Тот же ключ должен использоваться на всех настраиваемых клиентах.

7. Чтобы применить настройки, нажмите “OK”.

В чем разница между 802.11b, 802.11g, 802.11a и Pre-N?
В настоящее время существуют четыре уровня стандартов беспроводной сетевой связи, которые очень отличаются друг от друга по максимально возможным скоростям передачи данных. Основой каждого из них является наименование 802.11(x), предложенное IEEE – институтом, отвечающим за сертификацию сетевых стандартов. Самый распространенный стандарт беспроводной сетевой связи - 802.11b - передает информацию со скоростью 11 Мбит/сек, стандарты 802.11a и 802.11g - со скоростью 54 Мбит/сек, а Pre-N - со скоростью 108 Мбит/сек. Pre-N, предшественник грядущего 802.11n, позволит достичь скоростей, намного превышающих скорость стандарта 802.11g, и почти вдвое увеличить площадь покрытия беспроводной связи. Подробнее см. следующую таблицу.

Сравнительная таблица стандартов беспроводной связи

Технология беспроводной связи	802.11b	G (802.11g)	G Plus (802.11g с HSM)	G Plus MIMO (802.11g с MIMO MRC)	N1 MIMO (проект стандарта 802.11n с MIMO)
Скорость	Скорость соединения / базовая скорость: 11 Мбит/сек	В 5 раз быстрее стандарта 802.11b	В 10 раз быстрее стандарта 802.11b	В 10 раз быстрее стандарта 802.11b	Скорость на уровне проводного соединения
Частота	Помехи могут создавать обычные бытовые устройства (беспроводные телефоны или микроволновые печи), работающие в нелицензируемой полосе 2,4 ГГц	Помехи могут создавать обычные бытовые устройства (беспроводные телефоны или микроволновые печи), работающие в нелицензируемой полосе 2,4 ГГц	Помехи могут создавать обычные бытовые устройства (беспроводные телефоны или микроволновые печи), работающие в нелицензируемой полосе 2,4 ГГц	Помехи могут создавать обычные бытовые устройства (беспроводные телефоны или микроволновые печи), работающие в нелицензируемой полосе 2,4 ГГц	Помехи могут создавать обычные бытовые устройства (беспроводные телефоны или микроволновые печи), работающие в нелицензируемой полосе 2,4 ГГц
Совместимость	Совместим с 802.11g	Совместим с 802.11b/g	Совместим с 802.11b/g	Совместим с 802.11b/g	Совместим с проектом стандарта 802.11n и 802.11b/g
Покрытие	Обычно 30-60 м (100-200 футов) в помещении	До 120 м (400 футов)	До 210 м (700 футов)	До 300 м (1000 футов)	До 420 м (1400 футов)
Преимущества	Надежный — проверенная временем технология	Распространенный — широко применяется для совместного доступа в Интернет	Повышенная скорость и площадь покрытия	Улучшенное покрытие с хорошей скоростью и радиусом работы	Передовой – лучшее покрытие и пропускная способность

Информация о технической поддержке

Бесплатная техническая поддержка* *Звонки могут оплачиваться по тарифам страны

www.belkin.com

Дополнительные сведения о технической поддержке можно найти на нашем сайте **www.belkin.com** в разделе технической поддержки. Чтобы связаться со службой технической поддержки по телефону, позвоните по одному из указанных ниже номеров*.

СТРАНА	НОМЕР	АДРЕС В ИНТЕРНЕТ
АВСТРИЯ	0820 200766	www.belkin.com/uk/networking/
БЕЛЬГИЯ	07 07 00 073	www.belkin.com/nl/networking/
ЧЕХИЯ	239 000 406	www.belkin.com/uk/networking/
ДАНИЯ	701 22 403	www.belkin.com/uk/networking/
ФИНЛЯНДИЯ	097 25 19 123	www.belkin.com/uk/networking/
ФРАНЦИЯ	08 - 25 54 00 26	www.belkin.com/fr/networking/
ГЕРМАНИЯ	0180 - 500 57 09	www.belkin.com/de/networking/
ГРЕЦИЯ	00800 - 44 14 23 90	www.belkin.com/uk/networking/
ВЕНГРИЯ	06 - 17 77 49 06	www.belkin.com/uk/networking/
ИСЛАНДИЯ	800 8534	www.belkin.com/uk/networking/
ИРЛАНДИЯ	0818 55 50 06	www.belkin.com/uk/networking/
ИТАЛИЯ	02 - 69 43 02 51	www.belkin.com/it/support/tech/issues_more.asp
ЛЮКСЕМБУРГ	34 20 80 85 60	www.belkin.com/uk/networking/
НИДЕРЛАНДЫ	0900 - 040 07 90 €0.10/мин	www.belkin.com/nl/networking/
НОРВЕГИЯ	81 50 0287	www.belkin.com/uk/networking/
ПОЛЬША	00800 - 441 17 37	www.belkin.com/uk/networking/
ПОРТУГАЛИЯ	707 200 676	www.belkin.com/uk/networking/
РОССИЯ	495 580 9541	www.belkin.com/networking/
ЮАР	0800 - 99 15 21	www.belkin.com/uk/networking/
ИСПАНИЯ	902 - 02 43 66	www.belkin.com/es/support/tech/networkingsupport.asp
ШВЕЦИЯ	07 - 71 40 04 53	www.belkin.com/se/support/tech/networkingsupport.asp
ШВЕЙЦАРИЯ	08 - 48 00 02 19	www.belkin.com/uk/networking/
ВЕЛИКОБРИТАНИЯ	0845 - 607 77 87	www.belkin.com/uk/networking/
ДРУГИЕ СТРАНЫ	+44 - 1933 35 20 00	

Приложение A: Глоссарий

IP-адрес

"IP-адрес" - это внутренний IP-адрес маршрутизатора. Для доступа к расширенному интерфейсу настроек введите этот IP-адрес в адресную строку обозревателя. При необходимости этот адрес можно изменить. Для изменения IP-адреса введите новый адрес и нажмите "Apply Changes" ("Применить"). Выбранный IP-адрес должен быть немаршрутизируемым. Примеры немаршрутизируемых IP:

192.168.x.x (где x – любое число от 0 до 255)
10.x.x.x (где x – любое число от 0 до 255)

Маска подсети

Некоторые сети слишком велики, чтобы позволить всему потоку данных поступать в любую их часть. Подобные сети необходимо делить на более мелкие, более управляемые сегменты, именуемые подсетями. Маска подсети - это сетевой адрес плюс данные, зарезервированные для идентификации "подсети".

DNS

DNS – это сокращение от Domain Name Server (Сервер доменных имен). "Сервер доменных имен" – это сервер Интернет, преобразующий унифицированные указатели ресурса (Universal Resource Locators; URLs) – например, "www.belkin.com" – в IP-адреса. Многие поставщики услуг Интернет не требуют ввода этих данных для работы маршрутизатора. При использовании подключения через статический IP-адрес для правильной работы может понадобиться указать первичный и вторичный адреса DNS. При соединении через динамический IP-адрес или PPPoE вводить адрес DNS, скорее всего, не потребуется.

PPPoE

Большинство поставщиков услуг по ADSL используют для подключения протокол PPPoE. Если вы подключаетесь к Интернет через ADSL-модем, ваш поставщик услуг, скорее всего, использует для допуска к услугам протокол PPPoE.

Тип вашего подключения – PPPoE, если:
1. Поставщик услуг предоставил вам имя пользователя и пароль, необходимые для подключения к Интернет.
2. Для подключения к Интернет поставщик услуг предоставил вам такое программное обеспечение, как WinPoET или Enternet300.
3. Для выхода в Интернет вам необходимо дважды щелкнуть на значке на рабочем столе, и этот значок - не Web-обозреватель.

Чтобы настроить маршрутизатор на работу с PPPoE, введите в соответствующие поля свое имя пользователя и пароль. После ввода данных нажмите "Apply Changes" ("Применить").

Если маршрутизатор настроен правильно, то после применения этих изменений индикатор "Internet Status" ("Состояние Интернет") будет отображать слова "connection OK" ("Есть соединение").

PPPoA

Введите в соответствующие поля данные о PPPoA и нажмите "Next" ("Далее"). Чтобы активировать настройки, нажмите "Apply" ("Применить").
1. Имя пользователя – Введите имя пользователя (назначается поставщиком услуг Интернет).
2. Пароль – Введите свой пароль (назначается поставщиком услуг Интернет).
3. Введите пароль еще раз – Подтвердите пароль (назначается поставщиком услуг Интернет).
4. VPI/VCI - Введите VPI - идентификатор виртуального пути - и VCI - идентификатор виртуального канала (назначаются поставщиком услуг Интернет).

Отключение через X минут...

Данная функция используется для автоматического отключения маршрутизатора от Интернет после заданного периода бездействия. Если, например, установить отметку рядом с этой опцией и ввести в поле минут значение "5", то маршрутизатор отключится от Интернет после пяти минут бездействия соединения.
Эта функция полезна при поминутной оплате услуг Интернет.

Канал и SSID (идентификатор набора услуг)

Чтобы изменить канал работы маршрутизатора, выберите нужный канал в раскрывающемся списке. Чтобы сохранить настройки, нажмите "Apply Changes" ("Применить"). Изменить можно и SSID. SSID – это эквивалент имени беспроводной сети. SSID может быть произвольным. Если по соседству есть другие беспроводные сети, следует присвоить своей беспроводной сети уникальное имя. Щелкните на поле SSID и введите новое имя. Чтобы внести изменения, нажмите "Apply Changes" ("Применить").

Трансляция ESSID

В настоящее время различные беспроводные сетевые адаптеры имеют функцию под названием "Site Survey" ("Поиск сетей"). Она просматривает эфир в поисках существующих сетей и позволяет каждому компьютеру автоматически выбирать сеть из результатов этого поиска. Это происходит, если SSID компьютера установлен на значение "ANY" ("Любая сеть"). Маршрутизатор компании Belkin может блокировать случайный поиск сети. При отключении функции "Трансляция ESSID" какой-либо компьютер сможет подключиться к вашей сети только если его SSID настроен на конкретное имя сети (например, WLAN). Перед влючением этой функции убедитесь, что вам известен SSID (имя сети). Свою беспроводную сеть можно сделать практически невидимой. При отключении трансляции SSID сеть не попадает в результаты функции "Site Survey" ("Поиск сети"). Очевидно, что отключение трансляции SSID помогает усилить защиту сети.

Шифрование

Установка режима шифрования поможет обеспечить защиту сети. Для защиты данных маршрутизатор использует два метода WEP-шифрования: 64-битный и 128-битный. Шифрование работает на системе ключей. Компьютерный ключ должен совпадать с ключем маршрутизатора. Есть два способа создания ключа. Самый простой способ – позволить маршрутизатору преобразовать в ключ заданную вами фразу-пароль. Более надежный способ - ввод ключей вручную.

Шлюзы приложений

Шлюзы приложений позволяют указать конкретные порты, которые будут открыты для конкретных приложений, чтобы обеспечить правильную работу с функцией трансляции сетевых адресов (NAT) маршрутизатора. Существует список самых распространенных приложений. Нужное приложение можно выбрать в раскрывающемся списке. Ваш выбор будет запрограммирован в маршрутизаторе. Выберите в раскрывающемся списке строку, откуда нужно скопировать настройки, и строку, куда их нужно скопировать, затем нажмите кнопку "Copy To" ("Копировать в..."). Настройки будут перенесены в указанную строку. Чтобы сохранить настройки для этого приложения, нажмите "Apply Changes" ("Применить"). Если нужного приложения нет в списке, придется связаться с его поставщиком и выяснить, какие порты необходимо настроить. Данные о порте можно ввести в маршрутизатор вручную.

Виртуальные серверы

Данная функция позволяет направлять внешние (Интернет) запросы на обслуживание к Web-серверу (порт 80), FTP-серверу (порт 21) или другим приложениям через маршрутизатор во внутреннюю сеть. Поскольку компьютеры внутренней сети защищены брандмауэром, компьютеры из сети Интернет не могут на них выйти, они их просто "не видят". При необходимости настроить виртуальный сервер для какого-либо приложения следует связаться с поставщиком этого приложения и выяснить, какие настройки порта нужно использовать.

Чтобы задать параметры вручную, введите в соответствующие поля компьютера внутренней сети IP-адрес, тип порта (TCP или UDP), а также локальные и общие порты, необходимые для входа в сеть. Затем выберите "Enable" ("Включить") и нажмите "Set" ("Задать"). Каждому внутреннему IP-адресу может соответствовать только один порт. Открытие портов в брандмауэре может поставить под угрозу защиту системы. Включение и отключение этих настроек осуществляется очень быстро. Когда какое-либо приложение не используется, рекомендуется эти настройки отключать.

Фильтрация клиентов по IP

Маршрутизатор можно настроить на ограничение доступа к Интернет, электронной почте или другим сетевым службам в определенные дни и в определенное время. Ограничения можно задать для одного компьютера, группы компьютеров или набора компьютеров из разных групп.

Блокировка URL

Для настройки функции блокировки URL укажите Web-сайты (www.somesite.com) и/или ключевые слова для использования в качестве фильтров в сети. Чтобы применить изменения, нажмите "Apply Changes" ("Применить"). Для завершения настройки необходимо создать или изменить правило доступа в разделе фильтрации клиентов по IP. Чтобы изменить существующее правило, щелкните на опции "Edit" ("Редактировать") рядом с правилом, которое нужно изменить. Чтобы создать новое правила, щелкните на опции "Add PC" ("Добавить ПК"). Чтобы включить фильтр для указанных Web-сайтов и ключевых слов, в разделе "Access Control > Add PC" ("Управление доступом > Добавить ПК") установите отметку для опции "WWW with URL Blocking" ("WWW с блокировкой URL") в таблице "Client PC Service" ("Услуга для ПК-клиента").

Правила доступа по расписанию

Чтобы настроить правило доступа по расписанию, укажите имя, комментарий, время начала и окончания работы фильтра в сети. На этой странице задаются имена правил доступа по расписанию и включается расписание, которое будет использоваться на странице "Access Control" ("Управление доступом").

Фильтрация MAC-адресов

Фильтр MAC-адресов – мощное средство безопасности, позволяющее указывать компьютеры, которым разрешен доступ к сети. Ни один компьютер, пытающийся войти в сеть, не сможет этого сделать, если это запрещено списком фильтрации. После включения этой функции необходимо ввести MAC-адрес каждого клиента (компьютера) сети, чтобы предоставить им право доступа к сети, или скопировать MAC-адрес, выбрав имя компьютера в списке "DHCP Client List" ("Перечень клиентов DHCP"). Чтобы включить эту функцию, выберите пункт "Enable" ("Включить"). Затем нажмите "Apply Changes" ("Применить"), чтобы сохранить настройки.

DMZ (демилитаризированная зона)

Если на одном из клиентских ПК не удается запустить какое-либо Интернет-приложение по причине работы брандмауэра, этому клиенту можно разрешить неограниченный двусторонний доступ к Интернет. Это может понадобиться, если функция NAT (трансляции сетевых адресов) создает проблемы для таких приложений, как игры или видеоконференции. Не пользуйтесь этой функцией постоянно. В режиме DMZ компьютер не защищен от попыток взлома. Чтобы перевести компьютер в демилитаризированную зону (DMZ), введите в поле "Static IP" ("Статический IP") последние цифры его IP-адреса локальной сети и нажмите "Apply Changes" ("Применить").
Если есть только один общий IP-адрес (адрес во внешней сети), ему можно оставить значение "0.0.0.0". При использовании нескольких общих IP-адресов во внешней сети можно выбрать, на какой из них будет направлен DMZ-хост. Введите общий IP-адрес во внешней сети, на который следует направить DMZ-хост, введите две последние цифры IP-адреса главного DMZ-компьютера и нажмите "Apply Changes" ("Применить").

Пароль администратора

Маршрутизатор поставляется БЕЗ заданного пароля. Чтобы использовать пароль для усиления защиты, его можно задать с помощью пользовательского Web-интерфейсе маршрутизатора. Храните пароль в надежном месте, поскольку в дальнейшем он потребуется для входа в систему маршрутизатора. НАСТОЯТЕЛЬНО РЕКОМЕНДУЕТСЯ задать пароль, если вы намерены пользоваться функцией удаленного управления. Функция автоматического выхода позволяет настроить срок пребывания в расширенном интерфейсе установки маршрутизатора. Таймер влючается при отсутствии активности - например, если вы вносили какие-либо изменения в расширенном интерфейсе установки, а затем отошли от компьютера без выхода из системы.

Если таймер установлен на 10 минут, то через 10 минут бездействия срок сеанса работы с системой истечет. Для внесения новых изменений придется вновь входить в систему маршрутизатора. Функция автоматического выхода предназначена для обеспечения безопасности, срок по умолчанию – 10 минут. Обратите внимание, что одновременно в расширенный интерфейс установки маршрутизатора может войти только один компьютер.

Время и часовой пояс

Маршрутизатор поддерживает внутреннее время путем подключения к серверу SNTP (Простой протокол сетевого времени). Это позволяет маршрутизатору синхронизитировать системные часы с глобальным временем Интернет. Синхронизированные часы маршрутизатора используются для ведения записей журнала защиты и управления фильтрацией клиентов. Выберите свой часовой пояс. Если вы проживаете в стране, соблюдающей переход на летнее и зимнее время, поставьте отметку в поле "Automatically Adjust Daylight Saving" ("Автоматический переход на летнее время и обратно"). Обновление системных часов может произойти не сразу. Маршрутизатору может понадобиться по меньшей мере 15 минут для установления связи с серверами времени Интернет и получения ответа. Выставить часы самостоятельно невозможно.

Удаленное управление

Прежде чем включать эту функцию, УБЕДИТЕСЬ, ЧТО ЗАДАЛИ ПАРОЛЬ АДМИНИСТРАТОРА. Удаленное управление позволяет изменять настройки маршрутизатора из любого места, где есть доступ к Интернет.

UPnP

Протокол UPnP (Universal Plug-and-Play) – технология, обеспечивающая прямую работу систем речевых и видеосообщений, игр и других приложений, поддерживающих стандарт UPnP. Для правильной работы некоторых приложений необходимо соответствующим образом настроить брандмауэр маршрутизатора. Обычно для этого требуется открыть порты TCP и UDP, а в некоторых случаях настроить триггерные порты. Приложение, поддерживающее UPnP, способно связаться с маршрутизатором и "подсказать" ему, как именно следует настроить брандмауэр. Маршрутизатор поставляется с отключенной функцией UPnP. Включите эту функцию, если используете UPnP-приложения и хотите получить максимальные преимущества от возможностей UPnP. Для этого выберите опцию "Enable" ("Включить") в разделе "UPnP Enabling" ("Включение UPnP") на странице "Utilities" ("Служебные программы"). Чтобы сохранить изменения, нажмите "Apply Changes" ("Применить").

Приложение Б: Что учесть при размещении и настройке

Примечание: Некоторые из перечисленных ниже факторов могут повлиять на качество работы беспроводной сети, однако не препятствуют самому ее функционированию. Приведенный список может помочь, если сеть работает с пониженной производительностью.

1. Размещение беспроводного маршрутизатора (или узла доступа)

Беспроводной маршрутизатор (или узел доступа) - центральный пункт подключения к сети - желательно размещать как можно ближе к пространственному центру расположения беспроводных сетевых устройств. Чтобы добиться лучшего покрытия беспроводной сети для своих "клиентов беспроводной сети" (т. е. компьютеров, оснащенных беспроводными картами для ноутбуков или настольных ПК и беспроводными USB-адаптерами компании Belkin):

- Убедитесь, что антенны беспроводного маршрутизатора (или узла доступа) параллельны друг другу и установлены вертикально (направлены к потолку). Если вертикально установлен сам беспроводной маршрутизатор (или узел доступа), установите антенны в положение, как можно более близкое к вертикальному.
- Если в доме несколько этажей, разместите беспроводной маршрутизатор (или узел доступа) как можно ближе к пространственному центру дома. Это может означать размещение беспроводного маршрутизатора (или узла доступа) выше первого этажа.
- Старайтесь не размещать беспроводной маршрутизатор (или узел доступа) вблизи беспроводных телефонов с полосой 2,4 ГГц.

2. Преграды и помехи

Не устанавливайте беспроводной маршрутизатор (или узел доступа) вблизи устройств, способных издавать радиошумы, – например, микроволновых печей. Кроме того, беспроводную связь могут ухудшать:

- Холодильники
- Моющие и сушильные аппараты
- Металлические шкафы
- Большие аквариумы
- Металлосодержащие окна с защитой от ультрафиолета

Если на каком-либо участке сигнал беспроводной связи слабый, убедитесь, что на пути сигнала (между компьютером и беспроводным маршрутизатором или узлом доступа) нет подобных преград.

3. Беспроводные телефоны

Если описанные выше проблемы решены, но качество беспроводной связи все равно низкое, то, при наличии беспроводного телефона:

- Попробуйте убрать беспроводные телефоны подальше от беспроводных маршрутизаторов (или узлов доступа) и подключенных к беспроводной сети компьютеров.
- Отключите и снимите аккумулятор всех беспроводных телефонов, работающих

в полосе 2,4 ГГц (см. документацию их производителей). Если после этого проблемы со связью исчезнут, их причиной могли быть помехи от телефонной связи.
- Если телефон поддерживает выбор каналов, переключите его на канал связи, который находится как можно дальше от канала беспроводной сети. Например, телефон можно переключить на канал 1, а беспроводной маршрутизатор (или узел доступа) – на канал 11. Подробные указания см. в руководстве к эксплуатации телефона.
- При необходимости можно перевести беспроводной телефон на полосу 900 МГц или 5 ГГц.

4. Выбор "самого тихого" канала для беспроводной сети

В тех местах, где жилые или рабочие помещения расположены достаточно тесно (например, в многоквартирных домах или офисных комплексах), рядом могут оказаться беспроводные сети, создающие помехи друг для друга.

Для выявления других беспроводных сетей воспользуйтесь функцией "Site Survey" ("Поиск сетей") служебной программы беспроводной локальной сети (см. руководство к адаптеру); если необходимо, переведите свой беспроводной маршрутизатор (или узел доступа) и компьютеры на канал, который находится как можно дальше от каналов других сетей.

Испробуйте несколько доступных каналов, чтобы добиться самой чистой связи и избежать помех от работающих по соседству беспроводных телефонов и прочих устройств.

Более подробные сведения о видах беспроводной сетевой продукции компании Belkin читайте в разделе о поиске сетей и беспроводных каналах связи в "Руководстве пользователя".

Приведенные рекомендации позволят добиться максимальной зоны покрытия беспроводного маршрутизатора (или узла доступа). Если потребуется еще большая площадь покрытия, рекомендуем воспользоваться расширителями радиуса беспроводной связи и узлами доступа компании Belkin.

5. Защищенные соединения, виртуальные частные сети (VPN) и AOL

Защищенные соединения обычно требуют имени и пароля пользователя и применяются, когда важна защита данных. К защищенным соединениям относятся:
- Подключения к виртуальным частным сетям (VPN), которые часто используются для дистанционного доступа к учрежденческим сетям
- Программа "Bring Your Own Access" компании America Online (AOL), которая позволяет использовать службы AOL через широкополосные сети, предлагаемые другими поставщиками кабельных или DSL-услуг
- Большинство сайтов дистанционного банковского обслуживания
- Многие коммерческие сайты, требующие для доступа к учетным записям имени и пароля пользователя

Защищенные соединения могут нарушаться настройками управления электропитанием, переводящими компьютер в "спящий режим". Простейший способ избежать этого - повторное соединение после перезапуска программ VPN или AOL либо повторный вход на защищенный сайт.

Другой способ – изменение настроек управления электропитанием таким образом, чтобы компьютер не переходил в “спящий режим”; это, впрочем, может быть неприемлемо для переносных компьютеров. Для изменения настроек управления электропитанием в Windows используйте пункт “Power Option” (“Электропитание”) на Панели управления.
Если сложности с защищенными соединениями, подключениями к VPN и AOL продолжаются, вернитесь к рекомендациям на предшествующих страницах и убедитесь, что соответствующие проблемы решены.

Подтверждение Федеральной комиссии связи США (FCC)

ДЕКЛАРАЦИЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ ФЕДЕРАЛЬНОЙ КОМИССИИ СВЯЗИ США К ЭЛЕКТРОМАГНИТНОЙ СОВМЕСТИМОСТИ

Мы, компания Belkin International, Inc., зарегистрированная по адресу 501 West Walnut Street, Compton, CA 90220, с полной ответственностью заявляем, что данное изделие,

F5D7632uk4A

, к которому относится данная декларация, соответствует разделу 15 Правил Федеральной комиссии связи США. Работа устройства подчиняется двум следующим условиям: (1) данное устройство не должно вызывать вредных помех; (2) данное устройство должно воспринимать любые помехи, включая помехи, способные вызвать нежелательную работу устройства.

Осторожно: радиочастотное излучение.

Выходная мощность излучения данного устройства намного ниже допускаемых Федеральной комиссией связи США пределов радиочастотного излучения. Тем не менее, желательно пользоваться устройством так, чтобы свести с минимуму потенциальное влияние на человека в обычном режиме работы.
При подключении к устройству внешней антенны следует располагать антенну так, чтобы свести к минимуму потенциальное влияние на человека в обычном режиме работы. Чтобы избежать вероятности превышения установленных Федеральной комиссией связи США пределов радиочастотного излучения, человеку не следует находиться на расстоянии ближе 20 см (8 дюймов) от антенны в обычном режиме работы.

Уведомление Федеральной комиссии связи США

Данное оборудование прошло испытания и признано соответствующим ограничениям для цифровых устройств класса B согласно разделу 15 Правил Федеральной комиссии связи США. Эти ограничения призваны обеспечить приемлемую защиту от вредных помех при установке в жилых районах.
Данное оборудование создает, использует и может излучать радиочастотную энергию. Если оборудование все же вызывает вредные помехи при телевизионном приеме или радиоприеме (это можно определить, выключив и вновь включив оборудование), пользователю рекомендуется избавиться от помех, приняв одну или несколько из перечисленных мер:

- Развернуть или переместить принимающую антенну.
- Увеличить расстояние между оборудованием и приемником.
- Подключить оборудование к выходу сети питания, отличной от той, к которой подключен приемник.
- Обратиться за помощью к поставщику либо опытному радио- или телемастеру.

Модификации

Федеральная комиссия связи США требует уведомлять пользователя о том, что любые изменения или модификации, которые не одобрены Belkin International, Inc. в явной форме, могут лишить пользователя полномочий на использование оборудования.

Канада - Industry Canada (IC)

Беспроводная радиосвязь данного устройства соответствует спецификациям RSS 139 и RSS 210 Industry Canada. Данное цифровое оборудование класса B соответствует канадским спецификациям ICES-003.
Cet appareil numérique de la classe B conforme á la norme NMB-003 du Canada.

Европа - Уведомление ЕС

Радиотовары с предупреждающей маркировкой CE 0682 или CE соответствуют Директиве о радио- и телекоммуникационном оконечном оборудовании (R&TTE; 1995/5/EC) Комиссии ЕЭС.
Соответствие данной директиве означает соблюдение следующих Европейских норм (в скобках
указаны соответствующие международные стандарты):
• EN 60950 (IEC60950) – Безопасность изделия
• EN 300 328 Технические требования к радиооборудованию
• ETS 300 826 Общие требования к электромагнитной совместимости для радиооборудования.
Для определения типа передатчика см. опознавательную этикетку на изделии Belkin.
Товары с маркировкой CE соответствуют Директиве об электромагнитной совместимости (89/336/EEC) и Директиве о низком напряжении (73/23/EEC) Комиссии ЕЭС. Соответствие данным директивам означает соблюдение следующих Европейских норм (в скобках указаны соответствующие международные стандарты):
• EN 55022 (CISPR 22) – Электромагнитные помехи
• EN 55024 (IEC61000-4-2,3,4,5,6,8,11) – Электромагнитная стойкость
• EN 61000-3-2 (IEC610000-3-2) – Гармонические колебания сетей питания
• EN 61000-3-3 (IEC610000) – Колебания в сетях питания
• EN 60950 (IEC60950) – Безопасность изделия
Товары, содержащие данное радиопередающее устройство, помечаются предупреждающей маркировкой CE 0682 или CE, а также могут быть помечены логотипом CE.

BELKIN

EC Declaration of Conformity to R&TTE Directive 1999/5/EC

Manufacturer	:	*BELKIN LTD,* *EXPRESS BUSINESS PARK,* *SHIPTON WAY* *,RUSHDEN* *NN10 6GL ENGLAND*
Representative **(residing in the EC holding the TCF)**	:	*Belkin Ltd*
Product / Apparatus	:	**ADSL Modem/Wireless G Router**
Type Number	:	**F5D7632-4**
Variants include	:	**All Country Variants**

Declaration

I declare that above product conforms to all the applicable requirements of EU Directive1999/5/EC and is CE-marked accordingly:

Article 3.1a: (*Standard(s)*) used to show compliance with LVD, 73/23/EEC:

IEC 60950-1 2001 Compliant Test Report No: LD931001H03 03 NOV 04

Article 3.1b: (*Standard(s)*) used to show compliance with EMC Directive, 89/336/EEC:

EN301 489-1 V1.4.1 (2002-08);EN 301 489-17 V1.2.1 (2002-08) Compliant Test Report No:RM931001H03

Article 3.2: *Standard(s)* used to show compliance:

…EN300 328 V1.4.1 (2003-04)….. Compliant Test Report No:RC93100H03

Signature	:	
Name	:	K Simpson
Title	:	European Regulatory Compliance Manager
Date	:	20 MAR 2006

d of c f5d7632

Belkin International, Inc., Ограниченная гарантия на срок службы изделия

Что включает эта гарантия

Belkin International, Inc. гарантирует первоначальному покупателю данного изделия Belkin отсутствия у изделия дефектов конструкции, сборочных материалов или изготовления.

Срок действия гарантии

Belkin International, Inc. предоставляет гарантию на срок службы изделия Belkin.

Что делать для решения проблем

Гарантия качества изделия
Компания Belkin, по своему усмотрению, произведет бесплатный ремонт или бесплатную замену любого дефектного изделия (за исключением затрат на доставку изделия).

Что входит в эту гарантию

Все перечисленные выше гарантийные обязательства не имеют силы, если изделие Belkin не представлено компании Belkin International Inc. для оценки по запросу компании Belkin исключительно за счет покупателя либо если Belkin International Inc. определяет, что изделие Belkin прошло неверную установку, подверглось каким-либо модификациям или несанкционированному ремонту. Гарантия качества изделия Belkin не защищает от таких форс-мажорных обстоятельств (за исключением удара молнии), как наводнение, землетрясение, война, акты вандализма, хищение, естественный износ, эрозия, истощение запасов, устаревание, злоупотребление, ущерб, вызванный перепадами низкого напряжения (т. е. исчезновение или падение напряжения в электросети), работа несанкционированных программных продуктов или модификация либо изменение системного оборудования.

Как получить обслуживание

Для получения технического обслуживания изделия Belkin нужно проделать следующее:
1. Обратиться в Belkin International, Inc. по адресу 501 W. Walnut St., Compton CA 90220, Attn: Customer Service или позвонить по телефону (800)-223-5546 в течение 15 дней после выявления дефекта. Будьте готовы предоставить следующие сведения:

а) Инвентарный номер изделия Belkin.
б) Место покупки изделия.
в) Дата покупки изделия.
г) Копия оригинала квитанции.

2. После этого представитель службы работы с клиентами компании Belkin даст указания о том, куда направить квитанцию и изделие Belkin и как будет проводится дальнейшая работа с заявкой.

Belkin International, Inc., оставляет за собой право осмотра поврежденных изделий Belkin. Все затраты на доставку изделия в Belkin International Inc. для осмотра

оплачиваются исключительно покупателем. Если компания Belkin, исключительно по ее усмотрению, решает, что доставка поврежденного оборудования в Belkin International Inc. нецелесообразна, компания Belkin может, исключительно по ее усмотрению, указать место ремонта оборудования, куда следует направить изделие для осмотра и оценки затрат на его ремонт. Стоимость доставки оборудования в такое место ремонта оборудования и обратно, а также оценки затрат на ремонт, оплачивается исключительно покупателем. Поврежденное оборудование должно оставаться доступным для осмотра вплоть до истечения срока рассмотрения заявки. При урегулировании любых претензий компания Belkin International Inc. оставляет за собой право на суброгацию по любому из имеющихся страховых договоров покупателя.

Как связано с данной гарантией государственное право
ДАННАЯ ГАРАНТИЯ СОДЕРЖИТ ИСКЛЮЧИТЕЛЬНО ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА BELKIN INTERNATIONAL, INC., И НЕТ ИНЫХ ГАРАНТИЙ, ЯВНЫХ ЛИБО, ЗА ИСКЛЮЧЕНИЕМ ПРЕДУСМОТРЕННЫХ ЗАКОНОМ СЛУЧАЕВ, КОСВЕННЫХ, ВКЛЮЧАЯ КОСВЕННЫЕ ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА, ЛЮБЫЕ ГАРАНТИИ, СВЯЗАННЫЕ С УСЛОВИЯМИ КАЧЕСТВА, НАЛИЧИЕМ РЫНОЧНЫХ КАЧЕСТВ ИЛИ ПРИГОДНОСТЬЮ ИЗДЕЛИЯ ДЛЯ КОНКРЕТНЫХ ЦЕЛЕЙ, И ТАКИЕ КОСВЕННЫЕ ГАРАНТИИ, В СЛУЧАЕ ИХ СУЩЕСТВОВАНИЯ, ОГРАНИЧИВАЮТСЯ ПО СРОКУ ДЕЙСТВИЯ УСЛОВИЯМИ ДАННОЙ ГАРАНТИИ.

В некоторых штатах не допускается ограничение срока косвенных гарантийных обязательств, поэтому вышеупомянутые ограничения могут оказаться неприменимыми к вам.

BELKIN INTERNATIONAL, INC. НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА СЛУЧАЙНЫЕ, ОСОБЫЕ, ПРЯМЫЕ, НЕПРЯМЫЕ, КОСВЕННЫЕ ИЛИ МНОЖЕСТВЕННЫЕ УБЫТКИ, ВКЛЮЧАЯ (НО НЕ ОГРАНИЧИВАЯСЬ ПЕРЕЧИСЛЕННЫМ ДАЛЕЕ) ПОТЕРЮ БИЗНЕСА ИЛИ ПРИБЫЛИ, ВЫЗВАННЫЕ ПРОДАЖЕЙ ИЛИ ИСПОЛЬЗОВАНИЕМ ЛЮБЫХ ИЗДЕЛИЙ КОМПАНИИ BELKIN, ДАЖЕ ПРИ ПРЕДУПРЕЖДЕНИИ О ВОЗМОЖНОСТИ ПОДОБНЫХ УБЫТКОВ.

Данная гарантия предоставляет вам конкретные юридические права, но, кроме того, в зависимости от законодательства штата, у вас могут быть иные права. В некоторых штатах не допускается исключение или ограничение случайного ущерба или ущерба вследствие использования товара и прочих форм ущерба, поэтому вышеупомянутые ограничения и исключения могут оказаться неприменимыми к вам.

Сведения об утилизации изделия можно найти на сайте
http://environmental.belkin.com

ДЛЯ ИСПОЛЬЗОВАНИЯ В	AT	BE	CY	CZ	DK	EE	FI	FR	DE	GR	HU	IE
IT	LV	LT	LU	MT	NL	PL	PT	SK	SI	ES	SE	GB	IS	LI
NO	CH	BG	RO	TR								

РАБОТАЕТ НА КАНАЛАХ 1-13

Ограничения на использование в некоторых странах. . . . . **.ОборудованиеКласс 2**

BELKIN®

Модем ADSL2+ с беспроводным маршрутизатором Wireless G

BELKIN®

www.belkin.com

Служба технической поддержки Belkin
Великобритания: 0845 607 77 87
Европа: www.belkin.com/support

Belkin Ltd.
Express Business Park
Shipton Way, Rushden
NN10 6GL, Великобритания
+44 (0) 1933 35 2000
Факс: +44 (0) 1933 31 2000

Belkin SAS
130 rue de Silly
92100 Boulogne-Billancourt,
France
+33 (0) 1 41 03 14 40
Факс: +33 (0) 1 41 31 01 72

Belkin GmbH
Hanebergstrasse 2
80637 Munich
Германия
+49 (0) 89 143405 0
Факс: +49 (0) 89 143405 100

Belkin Iberia
C/ Anabel Segura, 10 planta baja, Of. 2
28108, Alcobendas, Madrid
Испания
+34 91 791 23 00
Факс: +34 91 490 23 35

Belkin Italy & Greece
Via Carducci, 7
Milano 20123
Италия
+39 02 862 719
Факс: +39 02 862 719

Belkin B.V.
Boeing Avenue 333
1119 PH Schiphol-Rijk,
Netherlands
+31 (0) 20 654 7300
Факс: +31 (0) 20 654 7349

P74725ru