



1-портовый беспроводной
маршрутизатор ADSL2+,
54 Мбит/с



RT-204

РУКОВОДСТВО
ПОЛЬЗОВАТЕЛЯ

Это руководство пользователя подготовлено AirTies Wireless Networks Corporation. Все права защищены.

Краткое описание

Это руководство проведет вас по шагам, необходимым для установки и настройки вашего AirTies RT-204 - беспроводного 1-портового маршрутизатора ADSL2+, 54 Мбит/с. Пожалуйста, перед началом установки внимательно прочитайте это руководство.

Гарантия не распространяется на неисправности или повреждения, возникшие в результате нарушения инструкций в руководстве. При таких обстоятельствах компания AirTies ответственности не несет.

Руководство пользователя является важным источником, к которому вы можете обратиться с целью безопасной и правильной эксплуатации вашего устройства. Пожалуйста, сохраняйте его для будущего использования.

Эксплуатация и безопасность

- Чтобы предотвратить повреждение устройства, убедитесь, что оно находится в своей оригинальной коробке во время транспортировки.
- Используйте устройство только с оригинальным адаптером питания.
- Не подсоединяйте Ethernet порт вашего устройства к PSTN (телефонной) розетке.
- В случае возникновения каких-либо проблем, не открывайте и не разбирайте устройство. Позвоните в службу технической поддержки AirTies.
- Чтобы предупредить электрический удар, не пользуйтесь устройством в мокрых или влажных местах.
- Не используйте устройство в случае утечки газа. Не включайте и не выключайте устройство. Не подключайте и не отключайте шнур питания.
- Избегайте использования устройства в запыленной среде. Если же случается накопление пыли, используйте сухую ткань, чтобы ее вытереть.
- Чтобы очистить устройство с внешней стороны, воспользуйтесь сухой тканью. Не пробуйте очищать устройство внутри: там нет компонентов, которые пользователь может сам отремонтировать.
- Для получения информации об установке и настройке устройства прочитайте руководство пользователя до конца.
- Средний срок службы устройства 7 лет, что установлено Управлением по вопросам промышленности и торговли.

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ	5
1.1 Минимальные системные требования	5
1.2 Комплектация	5
2. ИНСТАЛЛЯЦИЯ RT-204	6
2.1 Перед началом инсталляции	6
2.2 Инсталляция и конфигурирование с использованием компакт-диска простой установки AirTies RT-204 (Easy Setup CD).....	7
2.3 Настройка ADSL-соединения при помощи Web-интерфейса AirTies RT-204	11
3. Беспроводные настройки	13
3.1 Беспроводная безопасность	13
3.2 AirTies Mesh Technology (Меш технология)	16
3.2.1 Что следует учесть при создании ячеистой сети (Mesh Network)	17
3.2.2 Mesh настройки RT-204	17
4. Настройки трансляции сетевых адресов (NAT – Network Address Translation) и переадресации протоков.	18
4.1 DMZ (демилитаризованная зона).....	20
5. Настройки брандмауэра	21
5.1 Управление доступом	22
5.2 Защита от DoS-атак (Anti-DoS)	24
6. Tools (Сервис)	24
6.1 Обновление ПО	25
7. Как пользоваться программой AirTies ADSL Utility	25
7.1 Счетчик загрузки по линии ADSL	25
7.2 Автоматическое обновление ПО	26
8. Передняя панель	27
9. Задняя панель	28
10. Часто задаваемые вопросы	28
11. Технические характеристики	29
12. Физические характеристики	29
13. Гарантийные обязательства	30

1. ВВЕДЕНИЕ

1.1 Минимальные системные требования

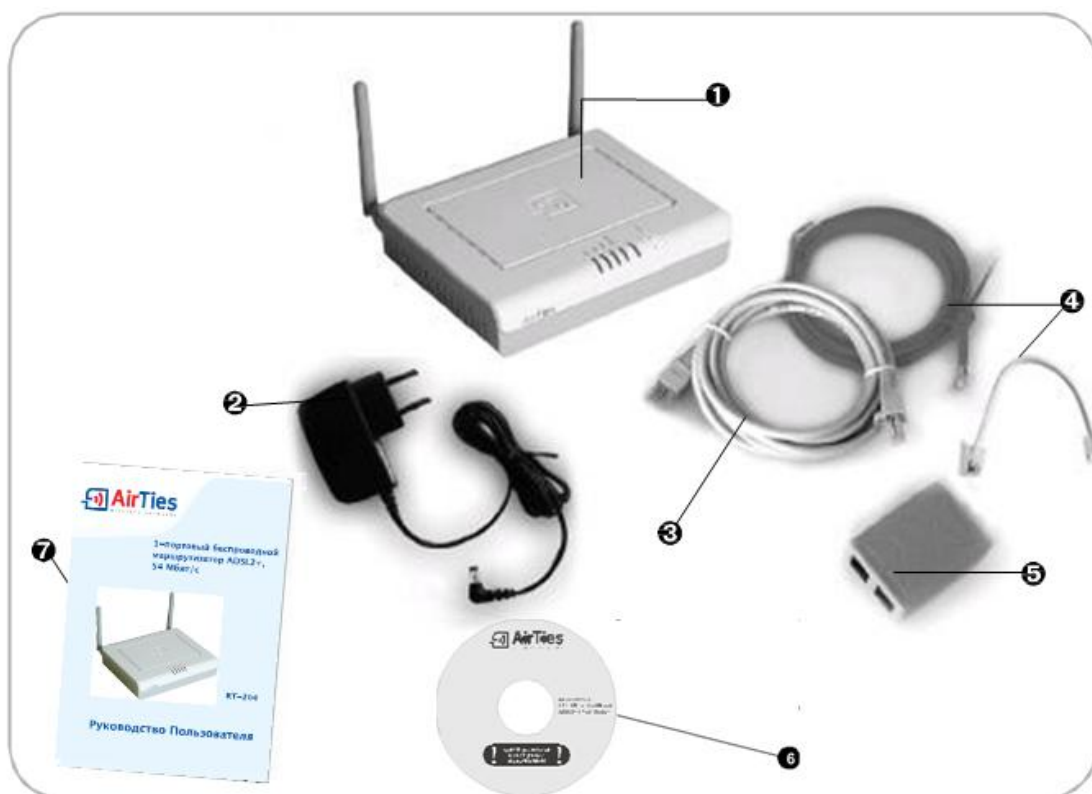
Для использования беспроводного ADSL2+ 1-портового маршрутизатора AirTies RT-204, вам понадобится как минимум:

- Для компьютеров, которые будут подключены к RT-204: Ethernet порт или 802.11b/g карта беспроводного доступа; любая версия ОС Windows или одна из операционных систем UNIX, Linux или Mac.
- Для использования программы AirTies Utility: одна из ОС Windows 98 / ME / 2000 / 2003, XP или Vista.
- При нормальной работе нет необходимости подключения маршрутизатора к ПК.

1.2 Комплектация

Пожалуйста, проверьте наличие в коробке с устройством AirTies RT-204 всех перечисленных ниже компонентов:

1. RT-204 1-портовый беспроводной маршрутизатор ADSL2+, 54 Мбит/с
2. Адаптер питания
3. Кабель Ethernet
4. Стандартные телефонные/DSL кабели (1 длинный, 1 короткий)
5. Сплиттер (разветвитель)
6. Компакт-диск простой установки (Easy Setup CD)
7. Руководство пользователя и гарантийный талон

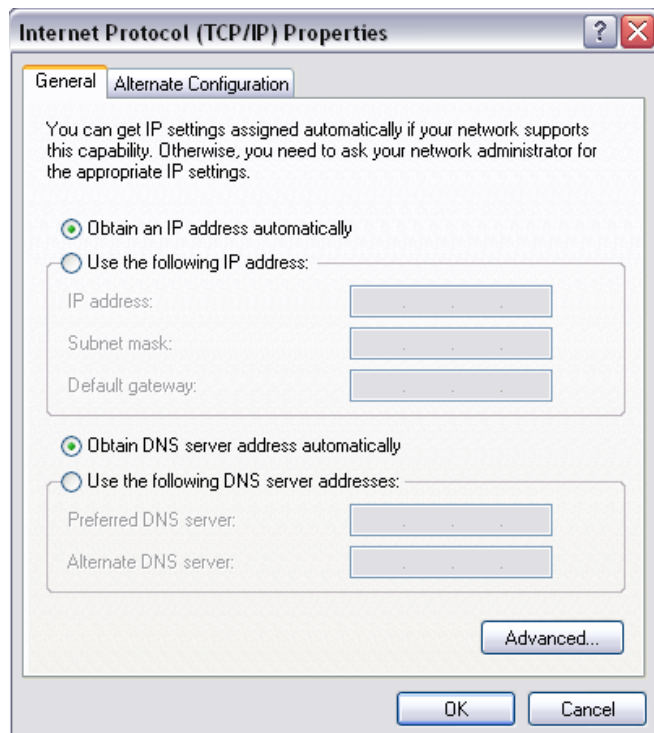


2. ИНСТАЛЛЯЦИЯ RT-204

2.1 Перед началом инсталляции

Перед началом инсталляции убедитесь, что настройки соединения по локальной сети вашего компьютера выбраны следующие пункты: **“Obtain an IP address automatically”** («Получить IP-адрес автоматически») и **“Obtain DNS server address automatically”** («Получить адрес DNS сервера автоматически»). Чтобы сделать это, следуйте следующим шагам на вашем компьютере с установленной ОС Windows:

1. Нажмите **Start – Settings – Control Panel** (Пуск – Настройки – Панель управления).
2. Двойной щелчок мышью на **“Network”** («Сетевое окружение»).
3. Выберите **“Internet Protocol (TCP/IP)”** («Интернет протокол TCP/IP») и нажмите на **“Properties”** («Свойства»).
4. В окне **“Internet Protocol (TCP/IP) Properties”** («Свойства Интернет протокола TCP/IP») выберите **“Obtain an IP address automatically”** («Получить IP-адрес автоматически») и **“Obtain DNS server address automatically”** («Получить адрес DNS сервера автоматически»).



Для инсталляции вставьте компакт-диск простой установки AirTies (AirTies Easy Setup CD) в CD-привод вашего компьютера. Анимации, показывающие, как подсоединить кабели, запустятся автоматически. После этого запустится программа простой установки, где вам необходимо будет ввести информацию о своем пользователе ADSL.

Если анимация не запустится автоматически, пожалуйста, запустите программу “installation.exe” с компакт-диска.



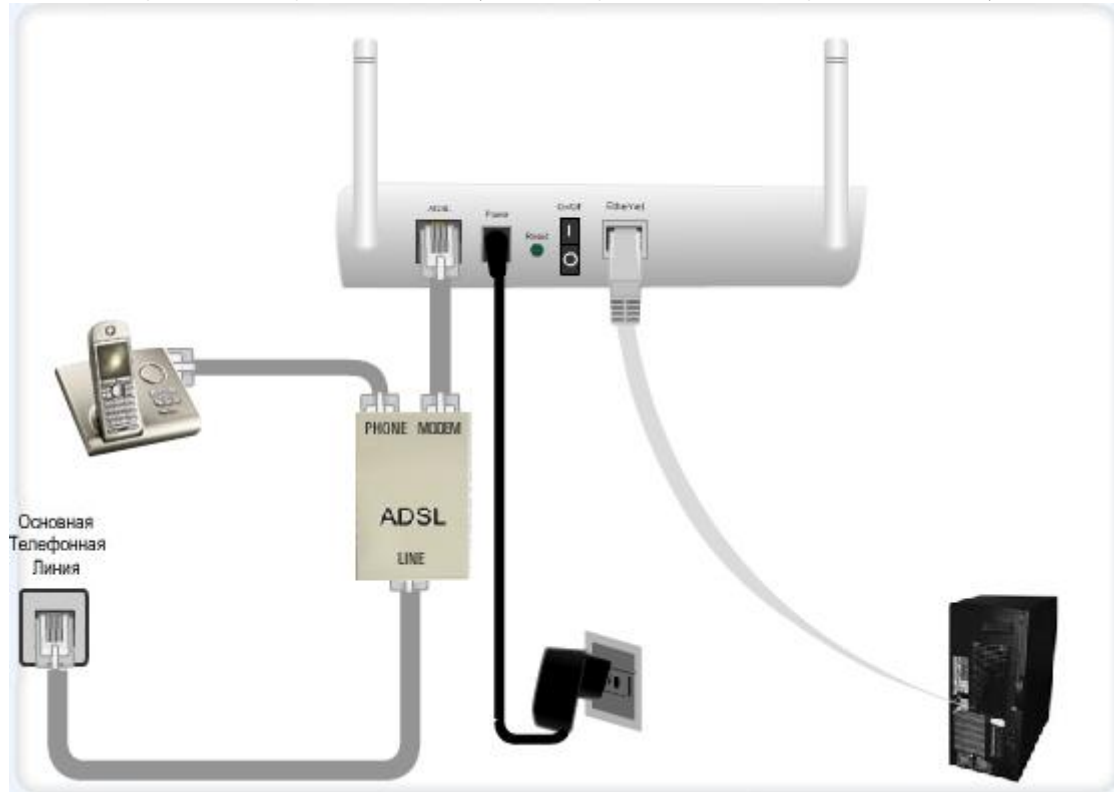
Внимание! Для установки маршрутизатора Вам необходимо вставить компакт-диск простой установки (Easy Setup CD) в CD-привод вашего компьютера..

2.2 Установка и конфигурирование с использованием компакт-диска простой установки AirTies RT-204 (Easy Setup CD)

1. После того, как вы вставили диск установки в ваш компьютер, выберите RT-204 в появившемся окне выбора продукта. Следуйте анимированным инструкциям и произведите необходимые подключения вашего маршрутизатора.



2. Когда анимация закончится, кабели должны быть подключены так, как показано на рисунке ниже.



3. Нажмите **“HARDWARE SETUP COMPLETED”** («Установка устройства завершена»).



4. Нажмите **“Next >”** (“Далее >”) в окне **“AirTies ADSL Utility Setup Wizard”** («Мастер установки AirTies ADSL Utility»).



5. Введите необходимую информацию, как показано ниже, и нажмите **“Next >”** (“Далее >”).

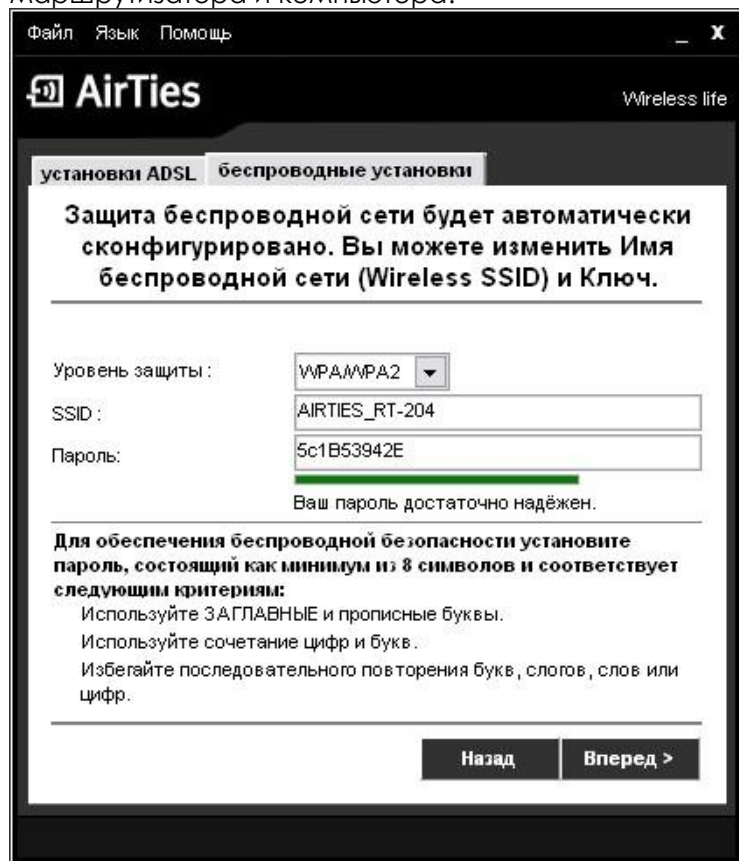
(A) - Введите имя пользователя ADSL, присвоенное вам вашим сервис-провайдером.

(B) - Введите пароль ADSL, предоставленный вам вашим сервис-провайдером.

(C) - Введите ваше имя, фамилию, номер телефонной линии (включая код города), подключенной к услуге ADSL, а также адрес вашей электронной почты.

Нажмите **“Next >”** («Далее >»).

6. В появившемся окне вы можете легко сконфигурировать беспроводные настройки вашего маршрутизатора и компьютера.



(A) Вы можете изменить тип шифрования на WPA, WPA2 либо WEP. Такие же значения должны быть установлены на каждом компьютере, который будет подключен к маршрутизатору по беспроводной сети.

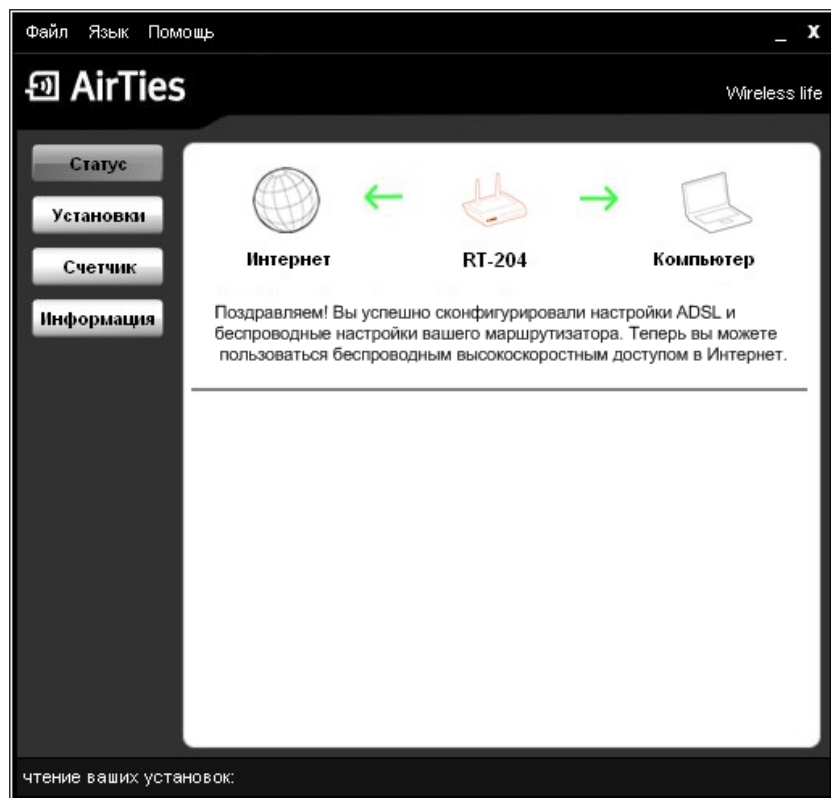
(B) Имя беспроводной сети по умолчанию установлено на AIRTIES_RT-204. Вы можете ввести имя на ваш выбор.

Например: MY_home_204

(C) Вы можете изменить пароль, который был произвольно присвоен вам программой установки. Такой же пароль должен быть установлен на каждом компьютере, который будет подключен к маршрутизатору по беспроводной сети.

Если вы закончите конфигурирование в окне **“Wireless Settings”** («Беспроводные настройки»), не установив пароль, программа установки выберет произвольный пароль и установит его на маршрутизаторе и компьютере, используемом для инсталляции. Вы можете увидеть этот пароль, нажав на вкладку **“Wireless Settings”** («Беспроводные настройки») меню **“Settings”** («Настройки») в программе AirTies ADSL Utility.

7. **Поздравляем!** Вы закончили настройку ADSL-соединения вашего маршрутизатора. Окно ниже будет отображать статус вашего Интернет-соединения. Если, после того, как вы закончили настройку, вы не можете подключиться к Интернету, пожалуйста, свяжитесь со своим сервис-провайдером.



2.3 Настройка ADSL-соединения при помощи Web-интерфейса AirTies RT-204

Как только вы соединили кабелями ваш маршрутизатор AirTies и компьютер, как показано выше, вы можете сконфигурировать настройки ADSL-соединения вашего маршрутизатора, используя любой web-браузер (например, Internet Explorer, Mozilla Firefox, Netscape). Для этого подключение к Интернету не обязательно.

- 1 - Откройте ваш web-браузер (например, Internet Explorer или Mozilla Firefox).
- 2 - В адресной строке введите **192.168.2.1** – IP-адрес вашего устройства по умолчанию. Таким образом вы запустите web-интерфейс вашего маршрутизатора AirTies.



- 3 - Появится запрос ввести пароль для входа. Изначально оставьте это поле пустым и продолжайте, нажав "ОК".

Для самого лучшего изображения рекомендуется использовать Internet Explorer 5.5+ или Firefox 1.0.6+ с минимальным разрешением 1024x768.

Авторское право © 2005-2009 AirTies Wireless Networks. Все права защищены.

4 - В появившемся окне перейдите к **“ADSL Settings”** («Настройкам ADSL») под основным меню «ADSL» в полосе меню слева. Нажмите **“Edit”** («Изменить»), чтобы продолжить конфигурирование ADSL.

Настройка Интернета (WAN)						
Название PVC	VPI/VCI	Инкапсуляция	Протокол	Шлюз по умолчанию	NAT	Брандмауэр
vc1	1/32	LLC	pppoe			

Создать

Редактировать

Сохранить Отменить

5 - В появившемся окне введите имя пользователя ADSL и пароль, предоставленные вам вашим сервис-провайдером. Нажмите **“Save”** («Сохранить»).

Настройки PVC

Для установки вашего соединения по линии ADSL выберите протокол для соединения с Интернет, после чего введите данные соединения. Эту информацию вы можете получить у своего сервис-провайдера.

Название PVC: Протокол:

Настройки PPP

Инкапсуляция: ☒ LLC ☐ VCMUX

Имя пользователя ADSL:

Пароль ADSL:

MTU: byte

По запросу: ☐

Параметры PVC

VPI:

VCI:

ATM QoS:

PCR: cps

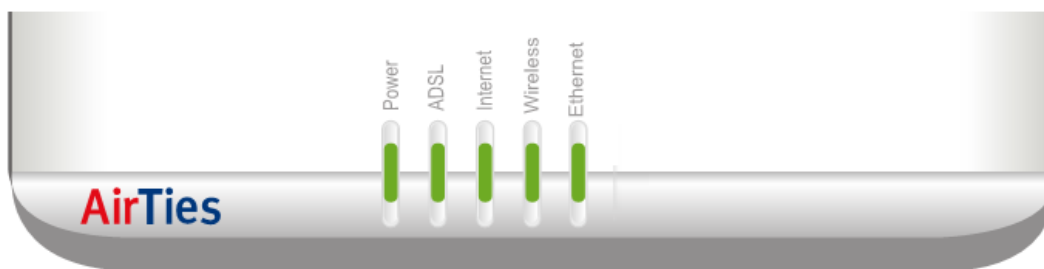
SCR: cps

MBS: cells

Сохранить Отменить

6- **Поздравляем!** Вы успешно завершили конфигурирование настроек ADSL вашего маршрутизатора. Вы

узнаете, что подключены к Интернету, когда LED-индикатор "Internet" («Интернет») на передней панели засветится постоянным зеленым. Если у вас возникнут проблемы с подключением к Интернету после того, как вы завершили настройки, пожалуйста, свяжитесь с вашим провайдером услуги ADSL.



3. Беспроводные настройки

Вы можете сконфигурировать настройки беспроводного соединения и беспроводной безопасности устройства RT-204 с помощью меню "**WIRELESS**" («Беспроводная сеть») web-интерфейса. Чтобы сконфигурировать вашу беспроводную сеть, перейдите в "**Wireless Settings**" («Настройки беспроводной сети») под меню "**WIRELESS**" («Беспроводная сеть»). Вы можете назначить имя своей беспроводной сети, введя имя в поле "**Primary SSID**" («Первичный SSID»). Вы можете выбрать канал (между 1 и 13) для беспроводного соединения.

Нажмите "**Save**" («Сохранить») для сохранения своих настроек.

Расширенная установка

Установка беспроводной сети активирована в начальной конфигурации вашего модема. Вы можете изменить имя вашей беспроводной сети (SSID) и скрыть его от других беспроводных клиентов. Вы можете выбрать канал между 1-13 для беспроводного соединения (мы рекомендуем каналы 1, 6 и 11).

Частота :	2.4 GHz
Режим :	802.11b/g
Канал :	6
Питание :	100%
Скорость (Мб/с) :	Авто

Первичный SSID:	Скрытый SSID	Отключение пользователя	Безопасность	Фраза-пароль
AIRTIES_RT-204	☐	☐	Шифрование отсутствует	

Сохранить **Отменить**

3.1 Беспроводная безопасность

Принимая во внимание важность защиты информации, рекомендуется выбрать один из протоколов безопасности, описанных ниже, который лучше всего соответствует вашим требованиям. AirTies RT-204 поддерживает новейшие методы беспроводной безопасности для обеспечения защиты данных.

Нажмите на подменю "**Wireless Security Settings**" («Настройки беспроводной безопасности») под меню "**WIRELESS**" («Беспроводная сеть»).

Беспроводная безопасность

Тип безопасности: ☒ Шифрование отсутствует ☐ WEP ☐ WPA/WPA2

Для функционирования в режиме точки доступа беспроводная безопасность не требуется и по умолчанию отключена. Если вы желаете, чтобы неавторизованные пользователи не могли подключиться к вашей точке доступа либо прослушивать информацию, пересылаемую с помощью беспроводных сигналов, рекомендуется использовать один из протоколов шифрования WEP (Wired Equivalent Privacy) или WPA (WiFi Protected Access), которые производят шифрование вашей беспроводной сети. Ваш модем поддерживает оба стандарта шифрования. WPA является самым надежным протоколом, который очень сложно сломать. Вся продукция AirTies и любой беспроводный клиент, поддерживающий протокол 802.11g, также поддерживает WPA. Если какие-либо беспроводные клиенты в вашей беспроводной сети не поддерживают WPA, тогда рекомендуется использовать WEP, который является менее надежным протоколом.

Защищенный доступ по Wi-Fi (WPA) и протокол WEP (Wired Equivalent Privacy) являются протоколами беспроводного шифрования, используемыми для шифрования потока данных в пределах беспроводной сети. AirTies RT-204 поддерживает оба протокола. На сегодняшний день WPA является одним из лучших стандартов беспроводного шифрования и обеспечивает самый лучший уровень защиты данных. Все беспроводные продукты AirTies и недавно представленные беспроводные устройства связи, работающие по стандарту 802.11g, поддерживают WPA. Если какое-либо устройство в вашей беспроводной сети не поддерживает WPA, рекомендуется выбрать шифрование WEP.

Фильтрация MAC-адресов позволяет контролировать, какие радиотерминалы могут подсоединиться к RT-204 и воспользоваться вашим доступом в Интернет.

Для обеспечения безопасности вашей беспроводной сети рекомендуется активировать как фильтрацию MAC-адресов, так и один из протоколов беспроводного шифрования WPA либо WEP.

Ваше устройство AirTies поддерживает также протокол аутентификации 802.1x. Для получения более подробной информации по установке безопасности 802.1x, пожалуйста, посетите вебсайт AirTies по адресу www.airties.com.

3.1.1 Настройки безопасности WPA

Перейдите к **"Wireless Security Settings"** («Настройки беспроводной безопасности»), находящимися под меню **"WIRELESS"** («Беспроводная сеть») web-интерфейса RT-204. Нажмите на кнопку **«WPA»** в поле **"Security Type"** («Тип защиты»). Нажмите на кнопку **"WPA/TKIP Personal (PSK)"** («WPA/TKIP персональный (PSK)») и введите сетевой ключ длиной от 8 до 63 символов (используйте комбинацию из букв и цифр, например, abcvyz_123) в поле **"Passphrase"** («Фраза-пароль»). Убедитесь, что вы выбрали шифр, который нелегко угадать. Нажмите **"Save"** («Сохранить»).

Для использования WPA2, более новой версии WPA, беспроводные приемники должны поддерживать WPA2.

Беспроводная безопасность

Тип безопасности: ☐ Шифрование отсутствует ☐ WEP ☒ WPA/WPA2

WPA является очень надежным протоколом безопасности. После установления шифрования WPA, ключ шифрования периодически обновляется, поэтому его сложно взломать. Введите фразу-пароль, длиной от 8 до 63 символов, нажмите «Сохранить». Вам также необходимо ввести эту фразу-пароль в настройках беспроводных клиентов, которые будут подключены к точке доступа.

Если вы заинтересованы в использовании аутентификации Enterprise WPA (802.1x), для получения более подробной информации посетите наш сайт <http://www.airties.com>.

Тип аутентификации:

Тип шифрования:

Фраза-пароль:

Интервал(ы) групповой ретрансляции:

Вам необходимо активировать WPA и установить одинаковый сетевой шифр на всех устройствах, которые будут подключены к RT-204 по беспроводной сети.

3.1.2 Настройки безопасности WEP

Перейдите к **"Wireless Security Settings"** («Настройки беспроводной безопасности») под меню **"WIRELESS"** («Беспроводная сеть») web-интерфейса RT-204. Нажмите на кнопку **"WEP"** в поле **"Security Type"** («Тип безопасности»). Существует три уровня шифрования WEP. В 64-битовом шифровании используется шифр из 10 шестнадцатеричных цифр (A-F и 0-9). В 128-битовом шифровании используется 26 цифр, а в 256-битовом – 58 цифр. После выбора длины шифра введите соответствующее число шестнадцатеричных цифр, любую комбинацию из (0-9, A-F), для шифра (например, ABC1234DEF для 64-битового шифрования). Поддерживается два режима аутентификации: **"Open"** («Открытый») и **"Shared"** («Общий»). Рекомендуется выбрать **"Open"** («Открытый») в поле **"Authentication Mode"** («Режим аутентификации»). Нажмите **"Save"** («Сохранить»), чтобы сохранить свои настройки в маршрутизаторе.

Беспроводная безопасность

Тип безопасности: ☐ Шифрование отсутствует ☒ WEP ☐ WPA/WPA2

Введите хотябы один пароль для шифрования WEP. Длина пароля выбирается в «Типе шифрования». Пароли типа HEX должны состоять из шестнадцатеричных знаков (цифры от 0 до 9, a, b, c, d, e, f). Это шифрование поддерживает два режима аутентификации: открытый и с общим доступом. Рекомендуется использовать открытый режим. Вы можете ввести до 4 паролей и выбрать любой из них. Вы также можете ввести этот пароль в настройках беспроводных клиентов, которые будут подключены к вашей точке доступа.

Режим аутентификации:

Тип безопасности WEP:

Активный шифр	Обзор	Шифр
1	☒	
2	☐	
3	☐	
4	☐	

3.1.3 Фильтрация MAC-адресов

Нажмите на **"MAC Address Filtering"** («Фильтрацию MAC-адресов») под меню **"WIRELESS"** («Беспроводная сеть») web-интерфейса RT-204.

В появившемся окне отметьте ячейку **"Enable MAC Filtering"** («Разрешить фильтрацию MAC-адресов»). Нажмите на кнопку **"Allow"** («Разрешить») и введите беспроводной MAC-адрес устройства, которому будет предоставлен доступ к вашей беспроводной сети, в поле слева от кнопки **"Add"** («Добавить») (например, **"00-14-38-15-60-DD"**). Нажмите **"Add"** («Добавить»).

Фильтрация MAC-адресов

С помощью этой страницы вы можете определить клиентов, которым будет предоставлен доступ к вашей беспроводной сети, а также заблокировать нежелательных клиентов. Сначала включите эту функцию, выбрав «Включить фильтрацию MAC-адресов». Для создания списка заблокированных клиентов отметьте «Только запретить MAC-адреса в списке MAC». Вы можете ввести MAC-адреса клиентов, которых следует заблокировать либо в текстовом окне «Новый MAC-адрес», либо прямо из списка «Существующие клиенты LAN». MAC-адреса необходимо вводить в формате '00-23-45-67-89'. Для сохранения настроек, нажмите «Сохранить».

Если вы хотите создать список только тех клиентов, которым будет предоставлен доступ к беспроводной сети, выберите «Только разрешить MAC-адреса в списке MAC» для введенных вами данных.

Включить фильтрацию MAC-адресов ☐

☐ Только разрешить MAC-адреса в списке MAC

☒ Только запретить MAC-адреса в списке MAC

Новый MAC-адрес Добавить >

Существующие клиенты LAN

MAC-АДРЕС

--

Добавить >
< Удалить

Blocked Client List

--

Повторите этот шаг для каждого устройства, которому будет предоставлен доступ к вашей беспроводной сети.

Если вы предпочитаете ввести MAC-адрес устройств, которым не будет предоставлен доступ к вашей сети, нажмите **“Deny”** («Запретить») вместо **“Allow”** («Разрешить»), после этого введите беспроводные MAC-адреса устройств.

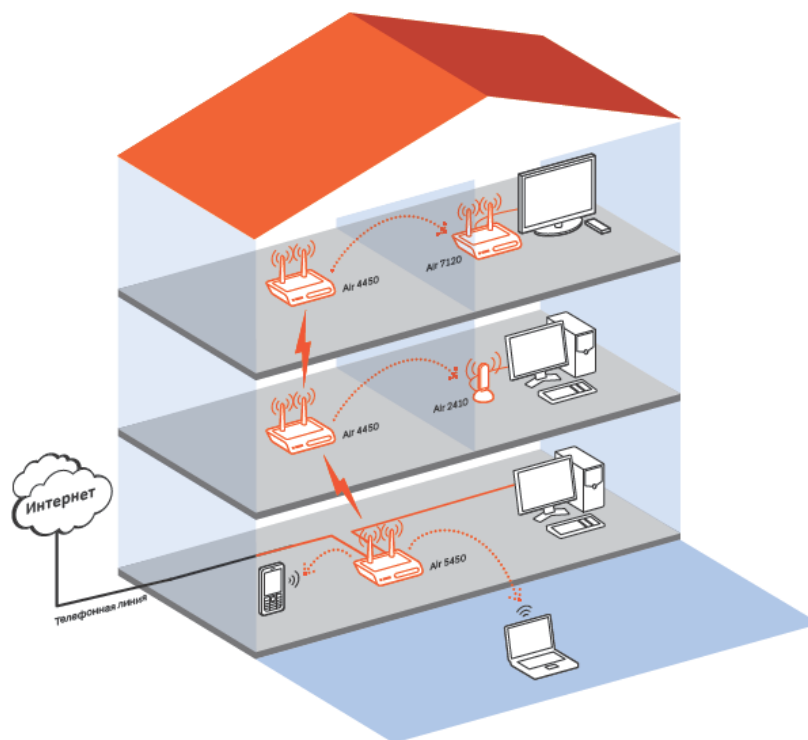
3.2 **AirTies Mesh Technology (Меш технология)**

RT-204 поддерживает AirTies Mesh Network Technology, которая решает проблемы слабого беспроводного сигнала и ограниченной зоны покрытия, которые часто встречаются в многоэтажных, бетонных зданиях и на обширных территориях.

Ячеистую сеть (Mesh Network) можно создать с помощью одного устройства RT-204 и одной или более беспроводных точек доступа AirTies AP-302, подключенных к RT-204 и соединённых между собой. Устройства AP-301 функционируют как репитеры (повторители) и соединяются между собой через специальный беспроводный протокол (MESH).

Wi-Fi сигналы, поступающие от беспроводных терминалов, автоматически достигают ближайшей точки доступа и потом, используя AirTies Mesh Technology, достигают устройства RT-204 посредством точек доступа, находящихся в этом промежутке. Таким образом, беспроводная зона покрытия может быть максимально расширена.

Схема ниже отображает структуру ячеистой сети (AirTies Mesh Network). Настройки ячеистой сети (Mesh Network) для устройства RT-204 описываются ниже. Детальную информацию о создании ячеистой сети (Mesh Network) с помощью вашего маршрутизатора и устройств AirTies AP-301 можно найти в руководстве пользователя для AP-301 либо на вебсайте <http://www.airties.com>.



3.3

Что следует учесть при создании ячеистой сети (Mesh Network)

- 1- RT-204 и все репитеры должны работать в одном канале (например, Канал 6).
- 2- Для двух любых репитеров, которые будут обмениваться данными, нужно выбрать MAC-адрес друг друга на странице MESH(настройки Mesh).
- 3- Репитеры следует размещать в местах с силой сигнала не менее «Хорошей (50%)».

3.4

Mesh настройки RT-204

- 1- Перейдите к **"MESH"** под меню **"WIRELESS"** («Беспроводная сеть») web-интерфейса RT-204. В окне **"MESH "** отметьте ячейку **"Поиск точек доступа"** .

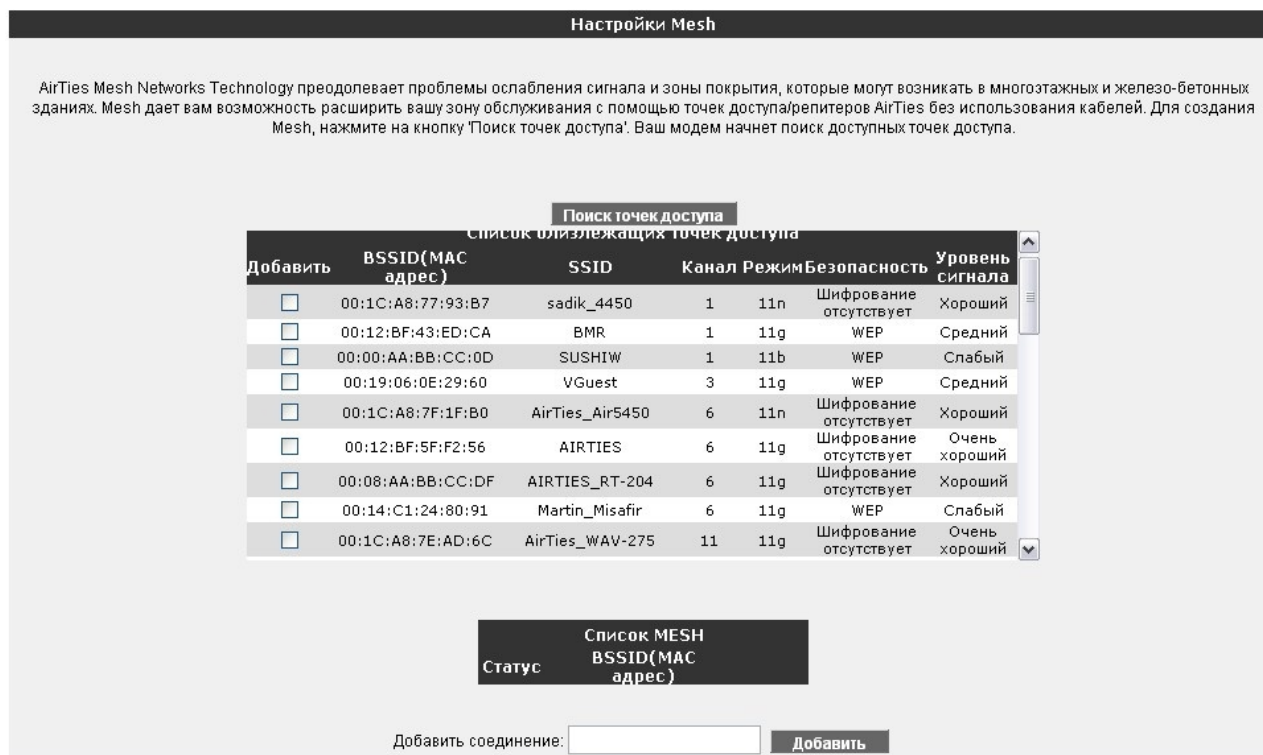
Настройки Mesh

AirTies Mesh Networks Technology преодолевает проблемы ослабления сигнала и зоны покрытия, которые могут возникать в многоэтажных и железобетонных зданиях. Mesh дает вам возможность расширить вашу зону обслуживания с помощью точек доступа/репитеров AirTies без использования кабелей. Для создания Mesh, нажмите на кнопку «Поиск точек доступа». Ваш модем начнет поиск точек доступа.

Поиск точек доступа

Статус	Список MESH BSSID(MAC адрес)
Добавить подключение: Добавить	

- 2- RT-204 начнет поиск беспроводных точек доступа, к которым он может подключиться. На экране отобразится список обнаруженных точек доступа. Отметьте ячейку той точки доступа, с которой вы хотите установить соединение Mesh для вашего устройства RT-204. Нажав **“Save”** («Сохранить»), вы определяете, что эта точка доступа будет первой получать сигналы от RT-204, и завершите настройки Mesh вашего маршрутизатора.



Точка доступа, которую вы выбрали, должна функционировать в одном канале с вашим маршрутизатором RT-204.

4. **Настройки трансляции сетевых адресов (NAT – Network Address Translation) и переадресации портов**

Network Address Translation (NAT) – это способ назначить всю сеть (или сети) на один IP-адрес. NAT дает возможность многим клиентам получать доступ в Интернет через единый глобальный IP-адрес, предоставленный вам вашим Интернет-провайдером. В то время, как вашему устройству RT-204 присвоен глобальный IP-адрес, все другие устройства в вашей локальной сети назначены на локальный IP-адрес, например, 192.168.2.23.

Обычно NAT используется вместе с **“Port Forwarding”** («Переадресацией портов»). Переадресация портов используется для того, чтобы хост за пределами вашей локальной сети имел доступ к компьютеру в вашей локальной сети. Пакеты данных, которые пересылаются на определенный порт в вашем глобальном IP-адресе, переадресовываются на один и тот же порт локального компьютера, у которого нет глобального IP-адреса. Некоторые популярные Internet приложения, требующие однорангового соединения (например, Emule, Kazaa, VPN, Remote Desktop) проходят через ваш маршрутизатор и достигают вашего компьютера с помощью переадресации портов.

Чтобы установить переадресацию портов на вашем устройстве RT-204, перейдите к **“Port Forwarding”** («Переадресации портов») под меню **NAT**, находящемуся на левой полосе меню web-интерфейса.

Нажмите **“New”** («Создать»), чтобы определить новое правило переадресации портов.

Переадресация портов

☐ Включить переадресацию портов

Создать

Имя правила	IP клиента	Активные приложения	Активировать	Конфигурация
-------------	------------	---------------------	--------------	--------------

Сохранить

Отменить

Rule Name (Имя правила): введите имя правила для создания нового правила.

SELECT CLIENT (Выбор клиента): в этом поле вы указываете LAN клиентов для переадресации портов. Для выбора клиента вы либо выбираете IP-клиента из списка "**Existing LAN Clients**" («Существующие LAN клиенты»), либо вручную введите IP-клиента в поле "**New IP Address**" («Новый IP-адрес»), после этого нажмите "**Add >**" («Добавить >»). IP появится в поле "**Selected IP Address**" («Выбранный IP-адрес»).

Маршрутизация портов

Чтобы добавить новое правило, введите имя правила. Чтобы определить клиента LAN, к которому будет применяться правило, введите IP-адрес, либо выберите их из списка существующих клиентов и нажмите 'Добавить'. Когда вы определили клиента, к которому будет применяться правило, определите приложения, к которым будет применяться переадресация портов.

Название правила

Интерфейс LAN lan-0 ▼
 Интерфейс WAN vlan1 ▼

ВЫБОР КЛИЕНТА

Новый IP-адрес

Добавить >

Выбранный IP клиента

Существующие клиенты LAN

MAC-АДРЕС	IP-АДРЕС	ИМЯ
00:1B:38:F0:53:E7	192.168.2.20	

Добавить >

Ваш модем можно сконфигурировать таким образом, чтобы он исполнял функции виртуального сервера, и чтобы клиенты в Интернете могли получить доступ к таким услугам, как web или FTP серверы в вашей LAN, используя реальные IP-адреса, которые пересылаются на локальные IP-адреса таких серверов. Так могут пересылаться входящие пакеты на IP-адрес в LAN на основе протокола и номера порта. Вы можете определить port map, используя знак '-' между двумя номерами портов. Пример Port Map: 1060-1100

В разделе в нижней части страницы необходимо ввести параметры для правила переадресации портов.

- В поле "**Application Name**" («Имя приложения») определите имя для правила переадресации портов, которое вы создаете.
- В поле "**TCP Ports**" («Порты TCP») введите номера портов TCP, которые использует приложение со стороны WAN и LAN. (Порты WAN и LAN, используемые приложением, определяются создателями приложения и обычно являются идентичными.)
- В поле "**UDP Ports**" («Порты UDP») введите номера портов UDP, которые использует приложение со стороны WAN и LAN. (Порты WAN и LAN, используемые приложением, определяются создателями приложения и обычно являются идентичными.)

Нажмите **"Add >"** («Добавить >») после того, как ввели все значения в необходимые поля. В таблице ниже вы увидите введенные вами значения для приложения.

Если приложение, для которого вы будете использовать переадресацию портов, существует в списке приложений с левой стороны страницы, вы просто можете выбрать приложение и нажать **"Add >"** («Добавить >»). Автоматически сгенерируется информация о портах.

После того, как вы завершите определять параметры приложений на ваш выбор, нажмите кнопку **"Save"** («Сохранить») в нижнем правом углу страницы.

входящие пакеты на IP-адрес в LAN на основе протокола и номера порта. Вы можете определить port map, используя знак '-' между двумя номерами портов. Пример Port Map: 1060-1100

- Введите имя для правила переадресации портов, которое вы хотите определить, в поле Приложения.
- Введите номер(а) портов, используемые приложением (приложениями) в поле Порты WAN.
- Введите номер(а) портов, которые будут использоваться приложением в локальной сети, в поле Целевые порты LAN (обычно это совпадает с настоящим портом (портами)).
- Вместо переадресации одного порта, вы можете переадресовать множество портов, обозначая их в виде интервалов, разделенных '-'. Например, чтобы переадресовать все порты от 23 до 80, введите 23:80 в этом поле.

DiabloII
Doom 3
Half Life 2 Steam
Quake 3
Remote Administrator
Remote Desktop
SMTP
SSH
gnutella
Web Server
FTP
Syslog
VNC
Telnet
POP3

Создать

Изменить

Удалить

Добавить >

Название приложения

WAN

LAN

Порты TCP

Порты UDP

Добавить >

Имя приложения

Порты WAN TCP

Порты WAN UDP

Порты LAN TCP

Порты LAN UDP

Remove

Сохранить

Отменить

После того, как вы нажали **"Save"** («Сохранить»), появится окно со списком всех ваших определений переадресации портов. Убедитесь, что вся введенная информация правильная. После этого отметьте ячейку **"Enable Port Forwarding"** («Разрешить переадресацию портов») и нажмите **"Save"** («Сохранить»).

Переадресация портов

☒ Включить переадресацию портов

Создать

Имя правила	IP клиента	Активные приложения	Активировать	Конфигурация
Example	192.168.2.2	Example	☒	Редактировать Удалить

Сохранить

Отменить

4.1 DMZ (демилитаризованная зона)

Свойство DMZ (DeMilitarized Zone - демилитаризованная зона) открывает все порты единственного хоста

локальной сети для неограниченного доступа из Интернета.

Хотя этот метод является рискованным, вы можете открыть и переадресовать все порты конкретного клиента за раз с помощью DMZ, чтобы решить проблемы доступа, возникающие в результате настроек брандмауэра или NAT.

ВНИМАНИЕ: Не рекомендуется сохранять все порты открытыми для какого-либо клиента длительное время.

Чтобы разрешить DMZ, перейдите в **“DMZ”** под меню **“NAT”** в web-интерфейсе. Отметьте ячейку **“Enable DMZ”** («Разрешить DMZ») и введите локальный IP-адрес клиента, на который вы бы хотели переадресовывать трафик, в поле **“IP Address”** («IP-адрес»). Нажмите **“Save”** («Сохранить»). Теперь все пакеты данных, отправленные на IP-адрес RT-204 WAN, ваш глобальный IP-адрес будет переадресовываться на этот локальный компьютер, независимо от порта назначения.

Настройки DMZ

Функция Demilitarized Zone (DMZ) предоставляет доступ ко всем портам клиента LAN из Интернета. Чтобы переадресовать весь Интернет трафик на конкретного клиента LAN, выберите его IP адрес из списка существующих клиентов и нажмите Сохранить. Чтобы определить нового клиента LAN, нажмите на ссылку под названием Клиенты LAN.

☒ Активировать DMZ

Интерфейс LAN lan-0 Интерфейс WAN vlan1

IP-адрес

Выберите один : 00:1B:38:F0:53:E7 192.168.2.20

Впишите :

Сохранить Отменить

5. Настройки брандмауэра

Брандмауэр предотвращает доступ к вашей локальной сети и вашему компьютеру неавторизованными пользователями Интернета.

Брандмауэр AirTies наделен функцией **Stateful Packet Inspection (SPI)**. SPI проверяет получаемые пакеты, чтобы определить, пропускать ли данные через брандмауэр к подсоединенным компьютерам. Для Интернет-адресов, являющихся источником атак, блокируется доступ к вашей сети.

С помощью меню брандмауэра вы также можете ограничить или заблокировать доступ в Интернет любому локальному пользователю, устанавливая расширенные правила для доступа в Интернет.

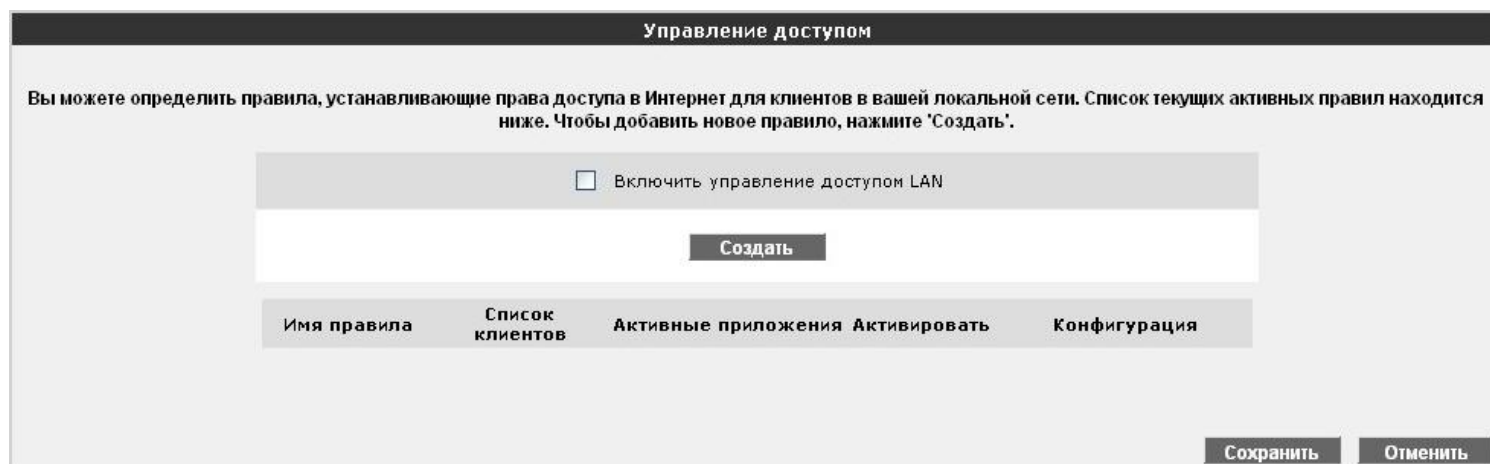
На вашем устройстве AirTies RT-204 брандмауэр активирован по умолчанию. Чтобы отключить брандмауэр, перейдите в главное меню **“FIREWALL”** («Брандмауэр»), нажмите кнопку **“Disable Firewall”** («Отключить брандмауэр»), а потом **“Save”** («Сохранить»). В следующих разделах описываются подменю, находящиеся под главным меню **“FIREWALL”** («Брандмауэр»), и соответствующие настройки.



5.1 Управление доступом

Вы можете открыть или закрыть доступ в Интернет для любого компьютера в вашей локальной сети, используя функцию "Access Control" («Управление доступом»). Эти ограничения доступа могут устанавливаться как по IP, так и по MAC-адресам.

Чтобы разрешить "**Access Control**" («Управление доступом»), отметьте ячейку "**Enable Access Control**" («Разрешить управление доступом»). Нажмите "**New**" («Создать»), чтобы определить новое правило доступа.



Чтобы создать новое правило, введите имя правила. Чтобы определить клиентов LAN, к которым будет применено правило, введите MAC-адреса клиентов LAN, либо введите диапазон IP-адресов, либо выберите их из списка существующих клиентов и нажмите «Добавить». Определив всех клиентов, к которым будет применено правило, в списке клиентов, определите приложения, которые будут ограничены.

Имя правила

LAN Interface

WAN Interface

ВЫБОР КЛИЕНТА

Новый MAC-адрес

Диапазон новых IP-адресов

Существующие клиенты LAN

MAC-АДРЕС	IP-АДРЕС	ИМЯ
00:1A:4B:5C:7A:7D	192.168.2.20	

Список ограниченных клиентов

00:1A:4B:5C:7A:7D

Выберите приложение (приложения), которые будут ограничены для клиента (клиентов) в «Списке ограниченных клиентов». Если вы хотите ограничить приложение, которого нет в списке, вы можете определить новое приложение, нажав на кнопку «Создать». Определив все необходимые приложения, нажмите «Сохранить».

ВЫБОР ПРИЛОЖЕНИЙ

Заблокировать весь трафик: ☐

Существующие приложения

DiabloII
Doom 3
Half Life 2 Steam
Quake 3
Remote Administrator
Remote Desktop
SMTP
SSH
gnutella
Web Server

Ограниченные приложения

Расписание: ☐

Начало

Окончание

День ☐ Пн ☐ Вт ☐ Ср ☐ Чт ☐ Пт ☐ Сб ☐ Вскр

В появившемся окне:

- Введите имя для правила доступа, которое вы бы хотели определить, в “Rule Name” («Имя правила»).
- Выберите легкое для запоминания имя.
- В разделе “**SELECT CLIENT**” («Выбор клиента») введите IP или MAC-адреса клиентов, чей бы доступ вы бы хотели ограничить с помощью этого правила, и нажмите “**Add >**” («Добавить >»).
- В разделе “**SELECT APPLICATIONS**” («Выбор приложений») укажите приложения, к которым вы бы хотели заблокировать доступ клиентов, которых вы ранее определили. Вы можете выбрать приложение со списка “**Existing Applications**” («Существующие приложения») и нажать “**Add >**” («Добавить >»), чтобы добавить новое приложение в список “**Existing Applications**” («Существующие приложения»).

5.2 Защита от DoS-атак (Anti-DoS)

Функция **Anti-DoS** предотвращает атаки “Denial of Service” («Отказ от обслуживания»), целью которых является вывести из строя ваш маршрутизатор, переполнив его запросами соединения. В этом окне вы можете установить максимальное количество разрешенных соединений из Интернета для определенного промежутка времени для каждого протокола.

Anti-DOS

Функция Anti-DoS блокирует атаки “Denial of Service” на ваш модем. На этой странице вы можете определить максимальное количество разрешенных соединений для отдельных протоколов в течение конкретного промежутка времени.

☒ Активировать Anti-Dos

vc1

☒ AntiDoS активирован

TCP За секунду 100 количество новых соединений

UDP За секунду 100 количество новых соединений

ICMP За секунду 1 количество новых соединений

lan-0

☒ AntiDoS активирован

TCP За секунду 1000 количество новых соединений

UDP За секунду 1000 количество новых соединений

ICMP За секунду 10 количество новых соединений

Сохранить Отменить

6. Сервис (Tools)

С этой страницы вы можете перезапустить свой маршрутизатор, вернуться к заводским настройкам, создать резервную копию конфигурации вашего маршрутизатора.

- Кнопка “**Restart**” («Рестарт») позволяет вам удаленно выключить и включить ваш маршрутизатор. В процессе этой операции соединение с маршрутизатором будет утеряно. Вы можете заново подсоединиться после того, как маршрутизатор снова включится.
- Кнопка “**Restore Factory Defaults**” («Вернуться к заводским настройкам») позволяет вам удаленно вернуть маршрутизатор к заводским настройкам. Это удалит все текущие настройки на вашем маршрутизаторе.
- “**Backup Config**” («Конфигурация резервного копирования») позволяет вам сохранять текущие настройки вашего маршрутизатора на своем компьютере.
- “**Restore Config**” («Конфигурация восстановления настроек») позволяет вам восстановить ранее сохраненную конфигурацию на вашем маршрутизаторе.

Сервис

Перезагрузка

Нажмите на эту кнопку, чтобы перезапустить систему. Ваше соединение с модемом будет разорвано и возобновлено через несколько секунд.

Вернуться к заводским на

Нажмите на эту кнопку, чтобы вернуться к заводским настройкам модема. Ваше соединение с модемом будет разорвано и возобновлено через несколько секунд.

Сохранить резервную копи

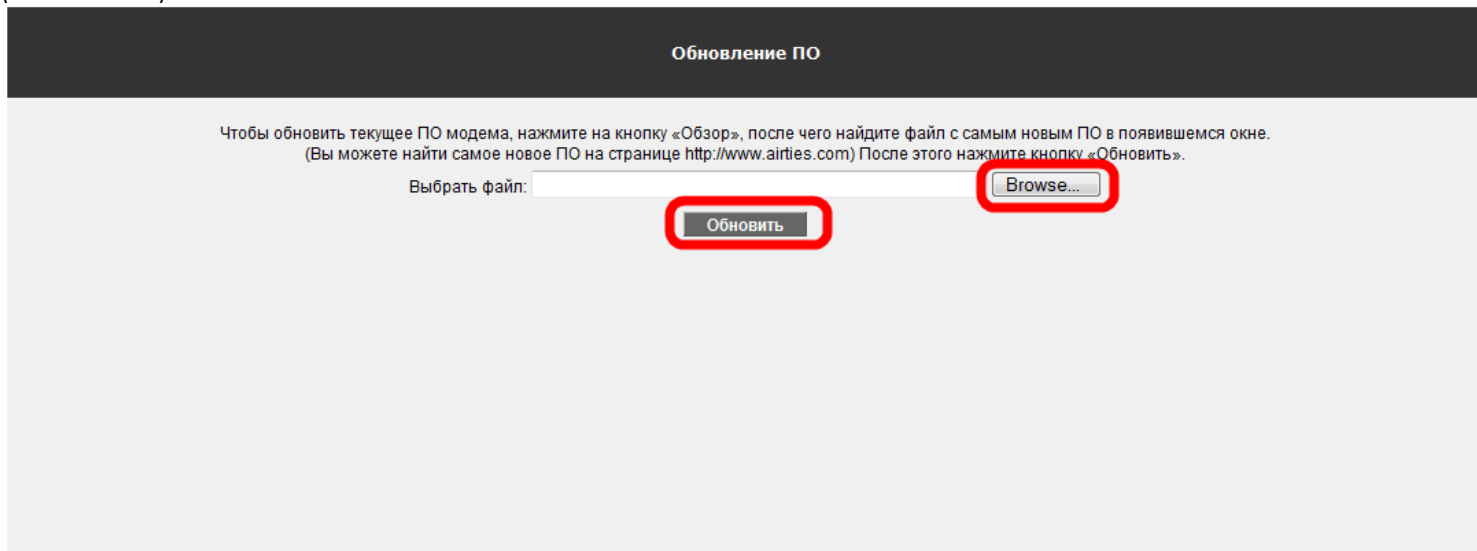
Нажмите на эту кнопку, чтобы сохранить эту конфигурацию на вашем компьютере. Позже вы можете возобновить свои текущие настройки, выбрав сохраненный файл конфигурации и нажав на кнопку ниже.

Восстановить configura

Browse...

6.1 Обновление ПО

Для того, чтобы обновить ПО, установленное на маршрутизаторе, перейдите к **"Firmware Update"** («Обновление ПО»), находящемуся под меню **"TOOLS"** («Сервис»). Нажмите **"Browse"** («Обзор») и выберите файл с самым новым ПО на вашем компьютере в появившемся временном рабочем окне. (Вы можете скачать файл с самым новым ПО с веб-сайта AirTies www.airties.com). После этого нажмите **"Upgrade"** («Обновить»).

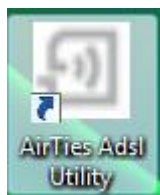


После того, как ПО успешно установлено, система перезапустится автоматически. Поэтому соединение с устройством будет потеряно. Вам понадобится заново подсоединиться к устройству, если вы захотите изменить какие-либо настройки.

7. Как пользоваться программой AirTies ADSL Utility

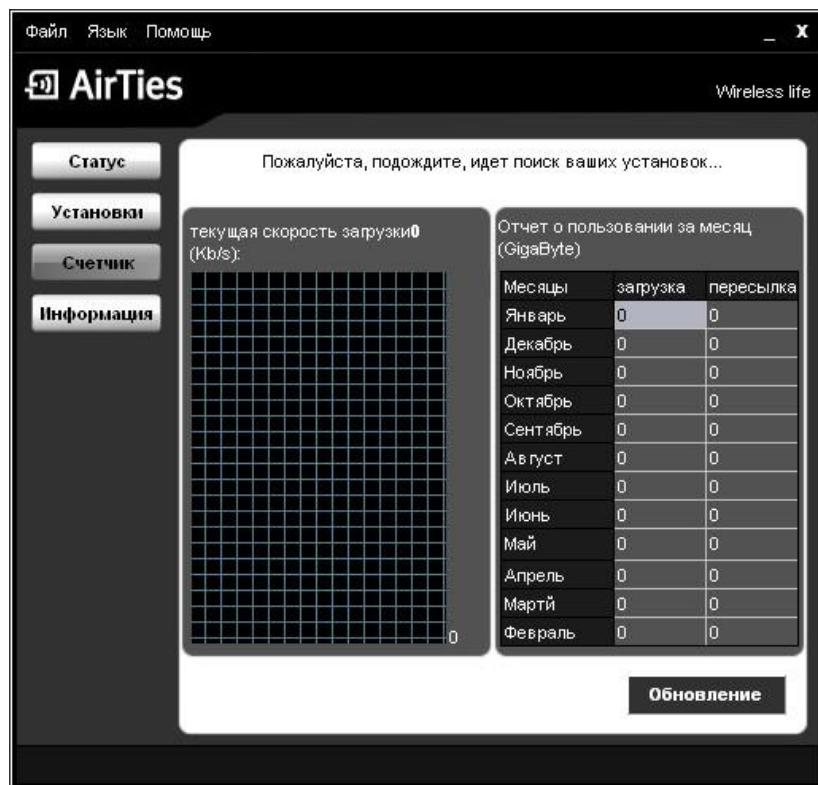
7.1

Программа AirTies ADSL Utility устанавливается на вашем компьютере с помощью компакт-диска простой установки (**Easy Setup CD**), который идет в комплекте с вашим маршрутизатором AirTies. Чтобы запустить программу ADSL Utility, нажмите на ярлык **AirTies ADSL Utility** на вашем рабочем столе после того, как установка с компакт-диска завершится.



7.2 Счетчик загрузки по линии ADSL

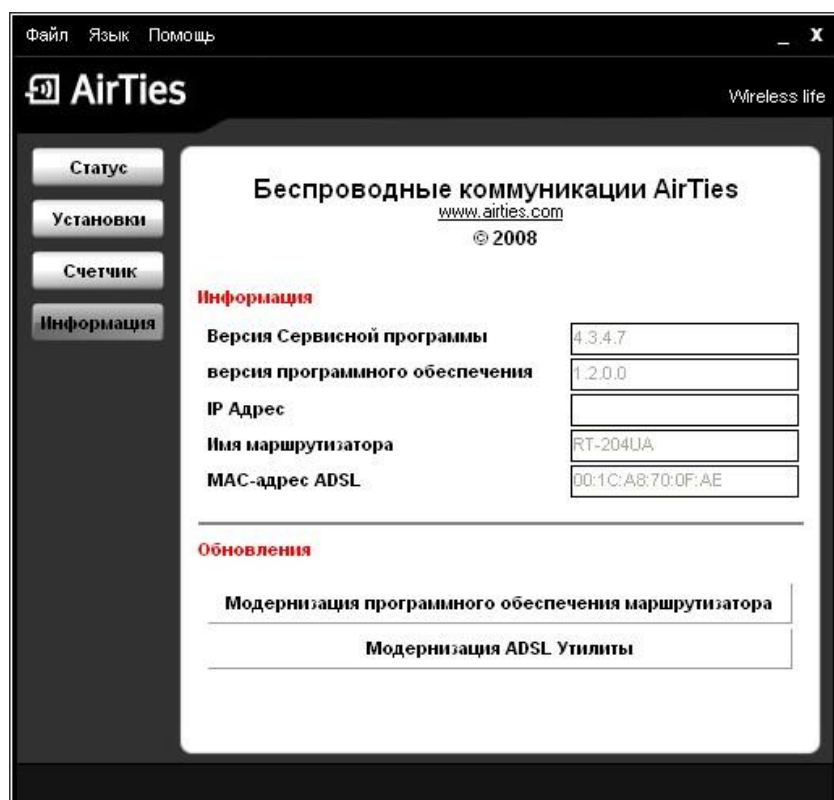
Нажав на меню **"Counter"** («Счетчик») программы AirTies ADSL Utility, вы можете просматривать информацию о ежемесячных объемах использования широкополосного канала (прием и передача данных), а также о текущей скорости приема данных. Даже если к вашему маршрутизатору подключено более одного компьютера, достаточно установить программу AirTies ADSL Utility всего на одном из этих компьютеров. Программа выводит отчет об объемах ежемесячного использования всего трафика данных, проходящего через ваш маршрутизатор. Данные хранятся в постоянной памяти устройства RT-204 и, таким образом, не будут утеряны при выключении маршрутизатора.



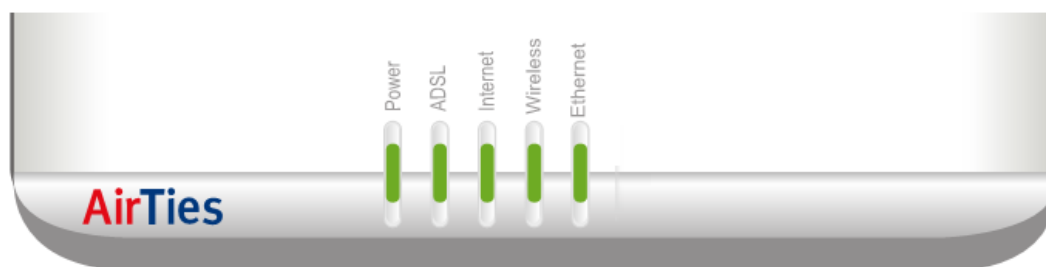
7.3 Автоматическое обновление ПО

Программа AirTies ADSL Utility сообщает вам о появлении обновленной версии ПО для вашего маршрутизатора. Если вы пожелаете, она обновит его. Используя самое новое ПО на вашем маршрутизаторе, вы не только добиваетесь максимальной эффективности работы вашего устройства, но также пользоваться преимуществами работы по новым технологиям.

Вы также можете обновить ПО, зайдя в меню **“Information”** («Информация») программы AirTies ADSL Utility и нажав на кнопки **“Upgrade Firmware”** («Обновить ПО») или **“Upgrade ADSL Utility Software”** («Обновить программу ADSL Utility»).

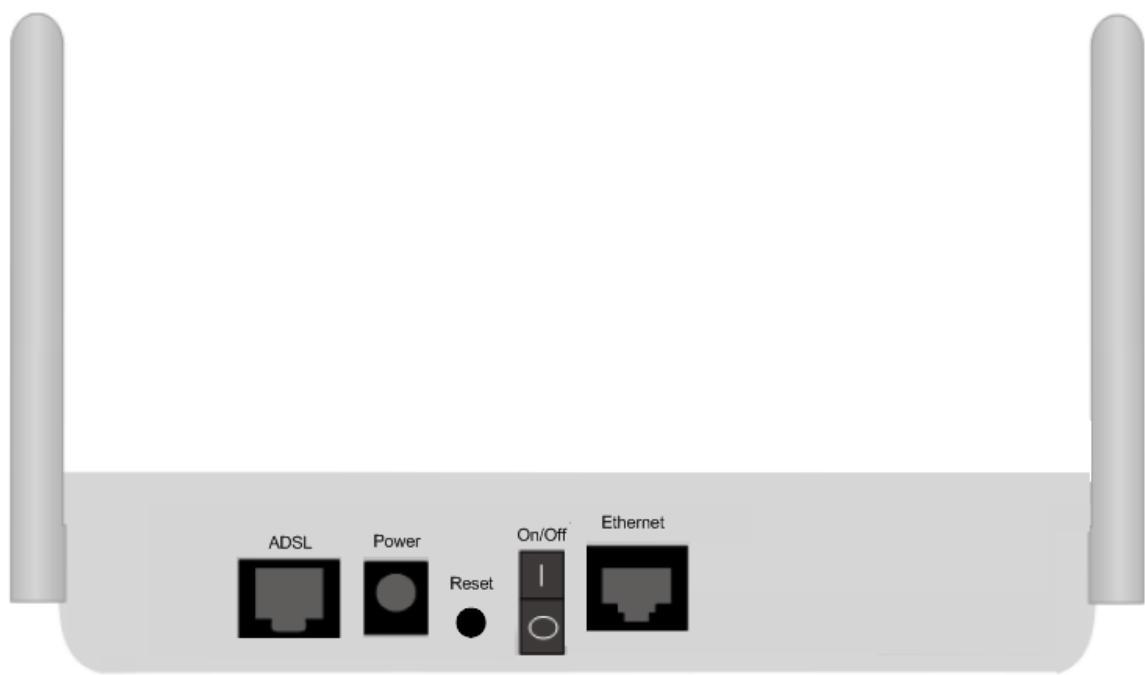


8. Передняя панель



LED	СВЕТ	СТАТУС
Power (Питание)	Зеленый	Маршрутизатор AirTies включен
	Выкл.	Маршрутизатор AirTies выключен
ADSL	Зеленый	ADSL соединение установлено и активно
	Мигающий зеленый	ADSL соединение устанавливается
	Выкл.	ADSL соединение отсутствует
Internet (Интернет)	Зеленый	Интернет-соединение установлено
	Выкл.	Интернет-соединение отсутствует
Wireless (Беспроводн.)	Зеленый	Соединение беспроводной сети активно
	Мигающий зеленый	Соединение беспроводной сети активно, происходит обмен данными
	Выкл.	Соединение беспроводной сети не активно
Ethernet	Зеленый	LAN соединение установлено
	Мигающий зеленый	LAN соединение активно, происходит обмен данными
	Выкл.	LAN соединение отсутствует

9. **Задняя панель**



ADSL	Порт линии ADSL. Подсоединяется к порту MODEM сплиттера.
Power (Питание)	Порт питания 9 В. Подсоединяется к адаптеру питания.
Reset (Сброс)	Кнопка возврата устройства к заводским настройкам.
On/Off (Вкл./Выкл.)	Кнопка для включения и выключения маршрутизатора.
Ethernet	Ethernet порт.

10. **Часто задаваемые вопросы**

Во время инсталляции с помощью компакт-диска простой установки (Easy Setup CD), происходит ошибка “Cannot access the router” («Доступ к маршрутизатору отсутствует»).

- Проверьте соединение между маршрутизатором и компьютером, на котором запущен компакт-диск простой установки (Easy Setup CD).
- Если на вашем компьютере установлен брандмауэр, например, Windows Firewall или Zone Alarm, это может запрещать доступ программы AirTies ADSL Utility к вашему маршрутизатору. Отключите брандмауэр и заново запустите инсталляцию с компакт-диска.

Интернет-соединение отсутствует, а LED-индикатор ADSL не работает.

- Проверьте правильность соединения сплиттера (разветвителя), как это описано в руководстве пользователя.
 - Узнайте у сервис-провайдера, не случился ли общий отказ по линии ADSL. Если вы только подключились к услуге ADSL, узнайте у провайдера, активирована ли уже ваша линия ADSL.
- Внимание: когда ваш маршрутизатор включается, LED-индикатор ADSL будет мигать около минуты. Убедитесь, что вы подождали одну минуту, чтобы Интернет-соединение установилось.



Что необходимо сделать, чтобы вернуть маршрутизатор к заводским настройкам?

- Пока ваш маршрутизатор включен, нажмите кнопку "Reset" («Сброс») на задней панели с помощью карандаша либо похожего предмета с тонким наконечником и удерживайте около 5 секунд. Сброс удаляет все сконфигурированные вами настройки маршрутизатора.

Вы можете позвонить в службу технической поддержки AirTies, работающую круглосуточно 7 дней в неделю, чтобы получить поддержку касательно любой проблемы, которая у вас может возникнуть с вашим устройством AirTies.

11. Технические характеристики

- Характеристики ADSL: T1.413, G.992.1 (G.DMT), G.992.2 (G.Lite), G.992.3/4 (ADSL2), G.992.3 AnnexL (RE-ADSL2), G.992.5 (ADSL2+), G.992.5 AnnexM (RE-ADSL2+), управление формой трафика UBR/CBR
- Протоколы соединения: PPPoE, PPPoA, RFC1483 Bridging, RFC1483 Routing, классический IP по ATM, PAP/CHAP
- Беспроводное соединение 802.11b/g: скорости передачи данных 1, 2, 5.5, 6, 9, 11, 12, 24, 36, 48, 54 Мбит/с
- Интервал частот: ETSI 2400 МГц (мин.)- 2483,5 МГц (макс.) (13 каналов, 3 не пересекающихся)
- Поддержка других протоколов: RFC2684, RFC2364, RFC2516, RFC1577, IEEE802.1d, RFC1631
- Маршрутизатор и брандмауэр: улучшенный брандмауэр Anti-DoS SPI; фильтрация по URL, IP и MAC-адресам; переадресация портов; DMZ; переадресация статического IP; DHCP сервер и клиент; DNS Proxy; PPP (PAP/CHAP/MSCHAP)
- UPnP: Plug & Play (универсальная технология «включай и работай»)
- Управление: SNMP, Web, TR-069
- Кнопка сброса (Reset) для возврата к заводским настройкам
- Порты: ADSL(RJ-11), Power(Питание – 9 В постоянного тока), 1 x 10/100 Ethernet(RJ-45, auto MDI/MDIX)
- LED-индикаторы: Power (Питание), ADSL, Internet, Wireless (Беспроводн.), Ethernet
- VPN pass-through
- Поддержка 8 PVC (постоянных виртуальных каналов)
- Устройство 2 класса (Class 2)

12. Физические характеристики

- Размеры: 170 мм x 130 мм x 35 мм
- Вес: 350 г
- Питание: 9 вольт постоянного тока
- Рабочее напряжение адаптера: между 100 В и 240 В переменного тока
- Рабочая температура: 0° C - 40° C
- Температура хранения: -25° C - 55° C
- Влажность: 10% - 90% без конденсации

13. **Гарантийные обязательства**

1. Производитель гарантирует отсутствие производственных дефектов и неисправностей устройства и несет ответственность по гарантийным обязательствам.
2. Если Ваше устройство AirTies вышло из строя, сначала свяжитесь с центром круглосуточной технической поддержки AirTies по номеру 8 800 507 4440.
3. В случае необходимости служба круглосуточной технической поддержки AirTies присвоит номер заказа и попросит прислать вышедшее из строя устройство в ремонтный центр AirTies. Пожалуйста, разборчиво напишите номер заказа на упаковке.
4. Гарантийный период исчисляется с момента приобретения устройства и составляет 3 года.
5. Те части, которые поставляются вместе с устройством, такие как адаптер питания и кабели, имеют гарантию 3 года.
6. Если устройство выходит из строя по любой причине в течение гарантийного срока, оно будет отремонтировано компанией AirTies или авторизованным техническим центром AirTies бесплатно.
7. Запчасти, не подлежащие ремонту, будут заменены на новые бесплатно.
8. Несмотря на то, что закон не обязывает компании осуществлять за свой счет ремонт оборудования, испорченного в результате несоблюдения правил, указанных в Руководстве пользователя, следуя принципу безусловного удовлетворения потребностей клиента, компания AirTies приложит все усилия для устранения проблемы за свой счет.
9. Устройство, отправленное в авторизованный технический центр обслуживания AirTies, будет отремонтировано или заменено и возвращено обратно его владельцу в течение 2 рабочих дней с момента доставки устройства в центр обслуживания.
10. Если замена идентичной моделью не возможна, AirTies заменит неисправное устройство более новой моделью, имеющей те же технические характеристики и свойства.
11. Центры ремонта AirTies:

В Украине: ООО «Айчепулл», ул. Воровского 22, офис 420, Киев, 01601. Телефон: +38 044 494 07 51

©2009 AirTies Wireless Networks, все права защищены. Товарные знаки или зарегистрированные товарные знаки являются собственностью их владельцев. Программное обеспечение и спецификации могут изменяться без уведомления.