



WiFi



Руководство пользователя MiFi РОУТЕР ОТ СКАЙ ЛИНК

3.1
Мбит/сек
VW310

Содержание



Технические характеристики _____ 03

1. Общая информация

Комплектация _____	05
Системные требования _____	05
Технические особенности _____	06
Описание аппаратных средств _____	07

2. Установка _____ 09

3. Конфигурация

Конфигурация на веб-базе _____	11
Базовая настройка	
Настройка соединения _____	11
Статус _____	13

Расширенная настройка

Настройка интернет-протокола IP _____	14
Настройка беспроводного соединения _____	15
Управление трафиком _____	21
Безопасность _____	24
Сервисная программа _____	27

4. Администратор _____ 35

5. Статус _____ 37

6. Приложение VW App _____ 39

7. Устранение неисправностей _____ 45

Технические характеристики



Стандарты

IEEE 802.11g
IEEE 802.11b

Скорость передачи радиосигналов

54 Мб/с 48 Мб/с
36 Мб/с 24 Мб/с
18 Мб/с 12 Мб/с
11 Мб/с 9 Мб/с
6 Мб/с 5,5 Мб/с
2 Мб/с 1 Мб/с

Безопасность

WEP 64/128 бит
WPA-PSK
WPA-PSK2

Частотный диапазон

2,4 ГГц - 2,483 ГГц

Частотный диапазон CDMA

Прием: 463 ~ 468 МГц
Передача: 453 ~ 458 МГц

Ширина полосы пропускания канала

CDMA 1,23 МГц

Тип внешней антенны

Две встроенные телескопические антенны с функцией разнесенного приема, разъем для подключения внешней антенны

Адаптер переменного тока

Переменный ток 110~240 в, 50~60 Гц
Постоянный ток 5,0 в / 2,0 А

Светодиоды

Питание Сигнал
1x/EVDO WAN
WLAN

Рабочая температура

-20 °C ~ +60 °C

Температура хранения

-30 °C ~ +70 °C

Влажность

5 ~ 95%

Габариты

115(Д)х65(Ш)х15 (В) мм

Вес

150 гр (Без батареи)

Время работы

В режиме эксплуатации: 2 часа

В режиме ожидания: 3 часа

Срок службы: 5 лет

1. Общая информация



Комплектация

- 1 Главное устройство
- 2 Адаптер переменного тока
- 3 Руководство пользователя

Системные требования

- Минимум один компьютер с установленной на нем картой интерфейса беспроводной сети или адаптером
- Сетевой протокол TCP/IP, установленный на каждом компьютере
- Интернет-браузер



Технические особенности

◆ Ускоренная беспроводная сеть

Устройство VW310 обеспечивает скорость беспроводного соединения до 54Мб/с с другими беспроводными клиентами 802.11g.

◆ Совместимость с устройствами 802.11b

Устройство VW310 полностью соответствует стандартам IEEE 802.11b, поэтому его можно подключать к существующим переходникам PCI, USB и Cardbus стандарта 802.11b.

◆ Улучшенные характеристики файервола

Пользовательский интерфейс на веб-основе отображает ряд улучшенных свойств управления сетью, в том числе:

Составление графика фильтрации

- Можно составить график активации фильтров в определенные дни или на указанное количество часов или минут.

Родительский контроль

- Удобная фильтрация контента на основе адреса MAC и/или URL.

Защищенность многократных/параллельных сеансов

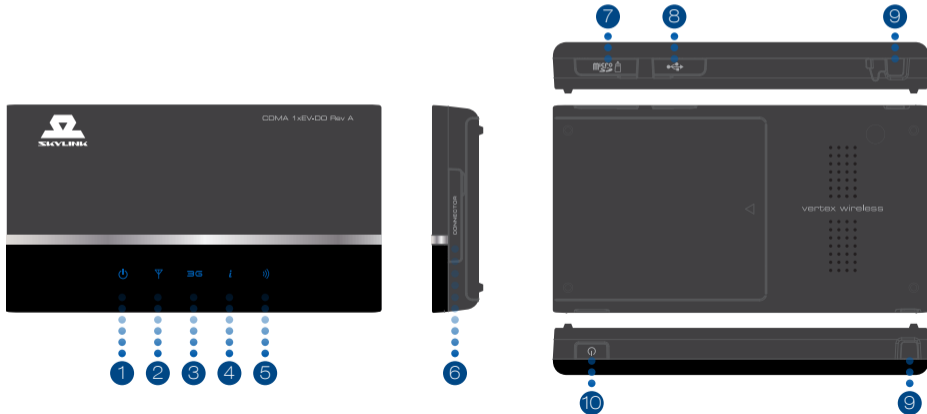
- С помощью устройства VW310 можно подключаться к сеансам VPN. Устройство поддерживает многократные и параллельные сеансы IPSec и PPTP, поэтому пользователи VW310 могут уверенно подключаться к корпоративной сети.

*Максимальная скорость беспроводного сигнала согласно техническим характеристикам стандарта IEEE. Фактическая скорость обработки данных может отличаться от этого показателя. Параметры сети CDMA и факторы среды, в т.ч. объем сетевого трафика, материалы, используемые при изготовлении, конструкция, служебные сигналы сети, низкая фактическая скорость обработки данных. Условия среды оказывают негативное воздействие на скорость беспроводного сигнала.

1. Общая информация



Описание аппаратных средств



① Питание

Состояние	Описание
ВЫКЛ	На маршрутизатор не подается питание
Непрерывный синий	Питание на маршрутизатор подается либо от адаптера, либо от аккумулятора (полная зарядка)
Непрерывный фиолетовый	Питание на маршрутизатор подается от наполовину заряженного аккумулятора
Непрерывный красный	Питание на маршрутизатор подается от почти разрядившегося аккумулятора
Мигающий синий	Аккумулятор заряжается
Мигающий красный	Ошибка при зарядке аккумулятора (неисправный аккумулятор и т.д.)

② Сигнал

Состояние	Описание
ВЫКЛ	Нет сигнала 1x или EV-DO
Непрерывный синий	Самый сильный уровень
Непрерывный фиолетовый	Средний уровень
Непрерывный красный	Низкий уровень

③ 1x/EV-DO

Состояние	Описание
ВЫКЛ	Маршрутизатор подключен к 1x
Непрерывный синий	Маршрутизатор подключен к EV-DO

④ WAN

Состояние	Описание
ВЫКЛ	Маршрутизатор отключен
Непрерывный синий	Маршрутизатор подключен к WAN

⑤ WLAN

Состояние	Описание
ВЫКЛ	Wi-Fi не используется
Непрерывный синий	Wi-Fi активирован
Мигающий синий	Через Wi-Fi прошли активные данные

⑥ Штепсельный разъем

⑦ Слот micro SD для совместного использования файлов

⑧ Слот USB (Mini-B) для зарядки аккумулятора

⑨ Антенна

2. Установка



Принципы беспроводной установки

Беспроводной маршрутизатор VW310 позволяет вашей сети осуществлять виртуальное соединение где бы вы ни находились в пределах рабочего диапазона вашей беспроводной сети. Однако диапазон может быть ограничен количеством, толщиной и расположением стен, перекрытий или других объектов, через которые должны пройти беспроводные сигналы. Обычно диапазоны варьируются в зависимости от типа материалов и фоновых радиочастотных помех в вашем доме или офисе.

1. Маршрутизатор следует размещать в точке с хорошим сигналом CDMA.
2. Старайтесь, чтобы количество стен и перекрытий между устройством VW310 и другими сетевыми устройствами было минимальным: каждая стена или перекрытие могут сократить диапазон работы вашего адаптера на 1~30 метров.
3. Имеют значение материалы, из которых изготовлены окружающие объекты. Сплошная металлическая дверь или алюминиевые стойки могут негативно влиять на диапазон. Постарайтесь разместить точки доступа, беспроводные маршрутизаторы и компьютеры таким образом, чтобы сигнал проходил через гипсокартонные

беспроводные маршрутизаторы и компьютеры таким образом, чтобы сигнал проходил через гипсокартонные перегородки или открытые дверные проемы. Такие материалы и объекты, как стекло, сталь, металл, стены с изоляцией, вода (аквариумы), зеркала, картотечные шкафы, кирпич и бетон ослабляют ваш беспроводной сигнал.

4. Хранить вдали (минимум 1~2 метра) от электрических приборов или устройств, производящих радиочастотные помехи.

5. Если вы пользуетесь радиотелефоном, работающим на частоте 2,4 ГГц или X - 10 (беспроводные устройства типа потолочных вентиляторов, осветительных приборов и домашних систем безопасности), ваше беспроводное соединение может быть существенно ослаблено или вообще прекращено. Убедитесь, что база радиотелефона, работающего на частоте 2,4 ГГц, находится как можно дальше от ваших беспроводных приборов. База передает сигнал, даже если телефон не используется.

3. Конфигурация



Конфигурация на веб-основе

Откройте интернет-браузер и введите IP-адрес маршрутизатора (192.168.200.1)

В окне браузера появится страница для входа в систему управления маршрутизатором. Введите пароль и нажмите кнопку "Login" («Войти»), чтобы войти в систему.

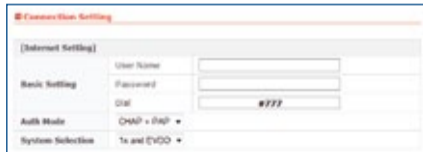


** Примечание: Маршрутизатор поставляется без пароля. При входе в систему оставьте графу для ввода пароля незаполненной и нажмите на кнопку "Login" («Войти»), чтобы войти в систему.

Базовая настройка

Настройка соединения

[Настройка интернета]



Базовые настройки

Введите имя пользователя протокола PPP, пароль и номер (предоставляются оператором. Номер по умолчанию: #777) Выберите систему CDMA из выпадающего меню: 1x и EVDO, 1x, или EVDO

Выбор системы

[Беспроводные настройки]

Беспроводной режим

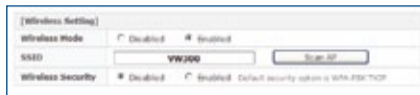
Для использования режима Wi-Fi выберите «enabled» («активизировать»), в противном случае выберите «disabled» («отключить»). Если вы выбрали «Активизировать», ниже появятся пункты SSID и Wireless Security («Безопасность беспроводного соединения»).

SSID

Идентификатор беспроводной сети – это название вашей беспроводной сети. Создайте название, используя до 32 символов.

Безопасность беспроводного соединения

Для использования режима безопасности беспроводного соединения выберите «enabled» («активизировать»), в противном случае выберите «disabled» («отключить»). Если вы выбрали «Активизировать», ниже появится пункт Wireless Code («Код беспроводного соединения»). (Параметр



3. Конфигурация



безопасности по умолчанию - WPA-PSK TKIP. Если вам нужны дополнительные параметры, войдите в меню Wireless Setup («Настройка беспроводного соединения») в «Расширенных настройках»

Код беспроводного соединения

Введите код для кодирования WPA-PSK TKIP, если хотите использовать параметр безопасности в режиме Wi-Fi.

Статус

С помощью этого меню можно проверить текущее состояние маршрутизатора.

Расширенные настройки

Данное меню предлагает различные расширенные функциональные конфигурации сети и рекомендуется для пользователей-экспертов. Нет необходимости использовать это меню всем пользователям.

The screenshot shows the 'Internet Setting' menu. It includes sections for 'Basic Setting' with fields for User Name, Password, and DSL (set to #???), and 'Auth Mode' (set to CHAP + PAP). The 'System Selection' is set to 'T1 and EVOVO'. Below this is the 'Dynamic IP' section with 'DNS Server' set to 'Auto Select', and fields for 'Primary DNS Address' and 'Secondary DNS Address'. At the bottom is the 'NATU' section with 'NATU' set to 'Auto Select'.

Настройка интернет-протокола IP

- Настройка интернета

[Настройки интернета]

Базовые настройки

Введите имя пользователя протокола PPP, пароль и номер (предоставляются оператором).
Номер по умолчанию: #777)

Выбор системы

Выберите систему CDMA из выпадающего меню: 1x и EVDO, 1x, или EVDO

[Динамический протокол IP]

Сервер DNS

Выберите ручное Manual или автоматическое Auto настраивание сервера DNS.

Первичный адрес DNS

Введите первичный IP-адрес сервера DNS, заданный вашим поставщиком интернет-услуг (интернет-провайдером).

Вторичный адрес DNS

Введите вторичный IP-адрес сервера DNS, заданный вашим интернет-провайдером (по желанию).

MTU

Максимальный размер пакета данных - вам может понадобиться изменить максимальный размер пакета, чтобы оптимизировать работу с вашим конкретным интернет-провайдером.
По умолчанию установлен автоматический размер максимального пакета.

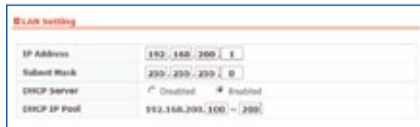
- Настройки локальной вычислительной сети LAN

IP-адрес

Это внутренний IP-адрес маршрутизатора.
По умолчанию задан IP-адрес "192.168.200.1",
при необходимости его можно изменить.

Маска подсети

Это уникальный расширенный параметр маршрутизатора. По умолчанию задан номер "255.255.255.0", при необходимости его можно изменить.



3. Конфигурация



Сервер DHCP

Сервер протокола динамического выбора конфигурации головной машины (DHCP) автоматически задает IP-адрес компьютерам локальной/частной сети. Для использования сервера DHCP выберите «Enabled» («Активизировать»), в противном случае выберите «Disabled» («Отключить»).

** Примечание: Для того, чтобы использовать сервер DHCP, убедитесь, что ваши компьютеры являются клиентами протокола DHCP. Для этого введите их параметры TCP/IP, чтобы автоматически получить IP-адрес.

IP-пул протокола DHCP

Введите начальный и конечный IP-адреса для присваивания IP-диапазона серверу DHCP. По умолчанию диапазон составляет 100-200.

Настройка беспроводного соединения

- Базовые настройки беспроводного соединения

[Режим работы беспроводного маршрутизатора]

Выберите режим работы беспроводного маршрутизатора из списка: Disabled («Отключен»)/ AP («Прикладной процессор») / WDS Master («Ведущее устройство WDS»)/ WDS Slave («Подчиненное устройство WDS»)



[Беспроводная сеть]

Беспроводной режим

Выберите режим работы беспроводного соединения из выпадающего списка:

- Смешанный режим (B+G) – Выберите этот параметр, если используете беспроводных клиентов обоих стандартов 802.11b и 802.11g.
- Режим G – Выберите этот параметр, если используете беспроводных клиентов только стандарта 802.11g.
- Режим B – Выберите этот параметр, если используете беспроводных клиентов только стандарта 802.11b.

WMM

Режим беспроводного мультимедийного расширения (WMM) – это механизм сбережения энергии на основе программы 802.11e и устаревшей 802.11 (для оборудования, работающего на аккумуляторах), и точно отрегулированного энергопотребления. Чтобы использовать режим WMM, выберите «Enabled» («Активизировать»), в противном случае выберите «Disabled» («Отключить»). Идентификатор беспроводной сети – это название вашей беспроводной сети. SSID должен быть одинаковым для всех устройств беспроводной сети. Создайте название, используя до 32 символов (можно использовать любые символы на клавиатуре, при этом учитывается регистр).

SSID

Пересылать SSID

Если вы не хотите, чтобы SSID вашей беспроводной сети пересылался маршрутизатором, выберите «Disabled» («Отключить»), в противном случае выберите «Enabled» («Активизировать»). Если выбран параметр «Отключить», SSID не будет определяться при выборе сайта, и вашим беспроводным клиентам нужно будет вводить SSID вручную, чтобы подключиться к маршрутизатору.

Канал

Можно выбрать несколько рабочих каналов. Если в вашем регионе работают другие беспроводные сети, будет установлен канал, отличающийся от канала таких других беспроводных сетей. Чтобы обеспечить лучшее качество работы, выбирайте канал, который как минимум на пять позиций отстоит от каналов другой беспроводной сети.

3. Конфигурация



Выходная мощность Можно выбрать размер выходной мощности. По умолчанию установлено 100 %. При необходимости выходную мощность можно изменить. Для лучшего качества работы используйте 100 %.

» Ведущая и подчиненная система распределения беспроводного соединения (WDS)

WDS - это система, обеспечивающая беспроводную взаимосвязь точек доступа в сети. Она обеспечивает расширение беспроводной сети с помощью множества точек доступа, при этом для их связи не требуется проводная магистраль. Для расширения зоны беспроводного покрытия необходимо более двух устройств VW310 (максимум 4). WDS может быть как ведущей, так и удаленной подчиненной. Ведущая система WDS передает данные через удаленных подчиненных WDS, беспроводных клиентов или другую передающую станцию либо главной, либо другой передающей подчиненной системе WDS. Ведущая и подчиненная системы WDS должны иметь одинаковые конфигурации SSID, канала и безопасности.

** Примечание: При настройке функции WDS отключите параметр безопасности беспроводного соединения для всех прикладных процессоров. Функция WDS для устройств серии VW310 выполняется другими прикладными процессорами, использующими чипсет Ralink, однако функция может быть ограничена для другого беспроводного чипсета.

Настройка безопасности Wi-Fi

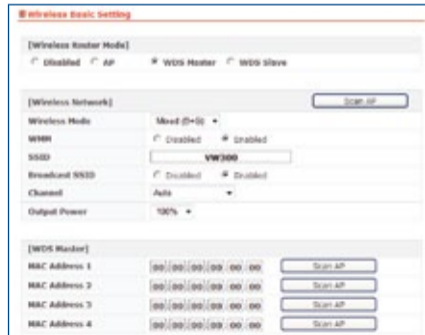
Отключите параметр безопасности Wi-Fi security в каждом устройстве. (Можно установить параметр безопасности в режиме WDS, однако рекомендуется производить настройку безопасности после выбора конфигурации WDS. Также необходимо установить одинаковый параметр безопасности в каждом ведущем и подчиненном устройстве).

Настройка ведущей системы WDS

едущий режим устанавливается в устройстве, работающем в сети EVDO для WAN. Подсоединитесь к веб-интерфейсу пользователя с помощью IP-адреса "192.168.200.1" → Перейти в меню [Расширенные настройки] → [Настройки беспроводного соединения] → [Базовые настройки] → Нажать [Ведущая WDS] → Установить нужный SSID и канал. (Эти данные SSID и канала должны быть такими же и в подчиненном устройстве WDS) → Нажать "Поиск прикладного процессора" в разделе «Ведущая WDS» → Выбрать прикладной процессор, который вы хотите использовать в качестве подчиненной системы WDS → Нажать "Применить", чтобы применить выбранную конфигурацию.

Настройка подчиненной системы WDS

Подсоединитесь с помощью IP-адреса "192.168.200.1" к пользовательскому веб-интерфейсу, который вы хотите использовать в качестве подчиненной системы WDS. Перейти в меню [Расширенные настройки] → [Настройки беспроводного соединения] → [Базовые настройки] → Нажать [Подчиненная WDS] → Установить нужный SSID и канал. (Эти данные SSID и канала должны быть такими же, как и в ведущем устройстве WDS). Установить нужный IP-адрес пользовательского веб-интерфейса. (Если устройство работает как подчиненная система WDS, можно войти в пользовательский веб-интерфейс с помощью этого адреса). → Нажать "Поиск прикладного процессора" в разделе «Подчиненная WDS» → Выбрать прикладной процессор, который вы хотите использовать в качестве ведущей системы WDS → Нажать "Применить", чтобы применить выбранную конфигурацию.



3. Конфигурация



- Настройки безопасности

Предлагается несколько способов максимального повышения безопасности вашей беспроводной сети и защиты данных от посягательств. Данный раздел предназначен для домашнего использования, домашних и небольших офисов. На момент выхода данного «руководства пользователя» существует два метода кодирования.

[Обеспечение безопасности с помощью пароля]

Тип безопасности Выберите тип безопасности из выпадающего меню.

- Нет (открытый доступ) и совместное использование

- В этом режиме для подсоединения к сети беспроводное устройство должно знать ключ WEP.

- WPA-PSK и WPA-PSK2

- В данном режиме доступ к Wi-Fi, защищенный кодированием данных с помощью предварительного ключа (WPA-PSK и WPA-PSK2), обеспечивает крайне высокую степень безопасности данных, очень эффективно блокируя случайное проникновение. Для установления подлинности вашего беспроводного соединения используется фраза-пароль или ключ. Ключ представляет собой буквенно-цифровой пароль, включающий от 8 до 63 символов. Помимо бук и цифр в пароль могут входить символьные обозначения и пробелы.

Wireless Security Setting

[Wireless Security Option]

Security using Password Security using Mac Address

[Security using Password]

Security Type: None/Open

Encryption Type: WEP

Encryption Type: 64-bit WEP 128-bit WEP

WEP Key: Auto Select Manual ASCII

WEP Passphrase:

Key1

Key2

Key3

Key4

Тип кодирования Выберите тип кодирования из выпадающего меню

- Нет (открытый доступ) и совместное использование
- WEP (защита данных на уровне проводных сетей)
 - Протокол WEP обеспечивает безопасность, кодируя данные по всей вашей беспроводной сети таким образом, что она остается защищенной при передаче данных с одного беспроводного устройства на другое. Чтобы получить доступ к сети WEP, нужно знать ключ. Ключ - это созданная вами последовательность символов. При использовании протокола WEP необходимо определить уровень кодирования. Тип кодирования определяет длину ключа. В данном режиме это общий протокол, усиливающий безопасность всех беспроводных устройств, совместимых с Wi-Fi. Протокол WEP разрабатывался с целью обеспечения беспроводных сетей уровнем защиты данных, сравнимым с защитой проводной сети.
- Протокол TKIP и стандарт шифрования AES для WPA-PSK и WPA-PSK2
 - Усовершенствованный протокол кодирования с использованием временных ключей (TKIP). TKIP кодирует ключи с помощью алгоритма хеширования и, добавляя свойство проверки целостности, исключает возможность искажения ключей. Ключ WPA2 основан на стандарте 802.11i и при кодировании вместо TKIP использует расширенный стандарт шифрования (AES).

[Обеспечение безопасности с помощью MAC-адреса]

MAC-адрес - это мощное средство защиты, позволяющее вам определять, каким компьютерам разрешать работать в сети. При использовании этого параметра необходимо ввести MAC-адрес каждого клиента (компьютера), работающего в вашей сети, чтобы каждому открыть сетевой доступ.



3. Конфигурация



Режим

Выберите один из трех предлагаемых режимов:

- Открыть - В данном режиме нет ограничений в доступе у всех устройств, подключенных к модему, будь то через порт Wi-Fi или порт Ethernet.
- Отклонить - В данном режиме сервисная таблица показывает клиента \MAC-адрес, заблокированных модемом.
- Разрешить - В данном режиме сервисная таблица показывает MAC-адрес клиента, которому модемом разрешен доступ.

** Примечание: Нельзя удалить MAC-адрес компьютера, используемого для доступа к административным функциям маршрутизатора (компьютер, используемый вами в данный момент).

Управление рабочей нагрузкой (трафиком)

- Переадресация портов

С помощью параметра переадресации портов можно направить определенные типы входящего трафика на серверы вашей локальной сети. Например, можно сделать локальный веб-сервер, FTP-сервер видимым и доступным для интернета. Эта функция позволяет направлять внешние (из интернета) вызовы сервисов, например, веб-сервера (порт 80), FTP-сервера (порт 21) или других приложений, через маршрутизатор в вашу внутреннюю сеть. Необходимо связаться с поставщиком приложений, чтобы узнать, какие настройки порта нужно задать. Для ввода настроек выберите из выпадающего меню «Протокол» и увидите список общих приложений (TCP, UDP). Выберите нужные приложения, введите IP-адрес и номер порта в окошке для внутренней машины (сервера) и нажмите «Добавить» и «Применить».

- Демилитаризованная зона (DMZ)

Целесообразность функции демилитаризованной зоны проявляется при использовании некоторых приложений WEB, FTP, Telnet, E-Mail для проведения онлайн-конференций. Модем запрограммирован на распознавание некоторых из этих приложений и на правильную работу с ними, но существуют другие приложения, работа которых может быть неудовлетворительной. Трафик, поступающий из интернета, обычно перекрывается модемом, если такой трафик не является ответом на запрос одного из ваших компьютеров. Компьютер в демилитаризованной зоне НЕ защищен от вторжения хакеров.

- Нерегулярный протокол FTP

Можно использовать эту функцию, если вы хотите подсоединиться к внешнему нерегулярному порту протокола FTP. Можно использовать максимум пять нерегулярных портов FTP.

- Резервирование канала (качество сервиса)

Параметр механизма резервирования канала способствует улучшению работы вашей сети путем назначения приоритетов среди приложений. По умолчанию механизм резервирования канала отключен, и приоритетность приложений не устанавливается автоматически. Функция гарантирует минимальную скорость при установке скорости работы компьютера или порта, а также ограничивает максимальную скорость. Эту функцию эффективно использовать при наличии большого количества пользователей. Установка настроек рассчитана только на 10 компьютеров.

Загрузка, выгрузка

Текущая скорость работы сервиса CDMA. Можно устанавливать скорость работы интернета в диапазоне от 12 кб/с до 3,1Мб/с.

ПК

При использовании сервиса ограничения скорости соединения с интернетом, если при этом к одному маршрутизатору подключено много компьютеров (ПК), скорость интернета снижается.

3. Конфигурация



Сервисный порт

Необходимо задать уникальный номер порта для обеспечения необходимой минимальной скорости.

Скорость загрузки, выгрузки

Скорость, при которой данные передаются с модема. Можно ограничить как минимальную, так и максимальную скорость.

The screenshot shows a configuration window with the following sections:

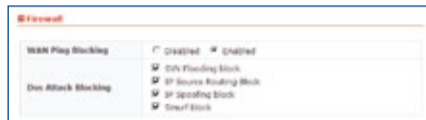
- QoS**: A section with a radio button for "Disabled" and a checked radio button for "Enabled". Below it are two rows: "Download" and "Upload", each with a dropdown menu set to "Mbps" and a plus sign.
- PC**: A section with three input fields for IP address.
- Service Port**: A radio button for "all Port" and a "TCP" dropdown menu followed by an input field.
- Download**: A radio button for "no Configuration" and two input fields for "min" and "max" with "Kbps" units.
- Upload**: A radio button for "no Configuration" and two input fields for "min" and "max" with "Kbps" units.

Below these settings is a red text label "* Maximum of 10" and an "Add" button. At the bottom, there is a table with columns: "No.", "ON/OFF", "PC", "Port", "Down", and "Up". The table is currently empty. At the very bottom are "On/Off", "Apply", and "OK" buttons.

Безопасность

- Межсетевой защитный экран Firewall (файервол)

Маршрутизатор оснащен файерволом, защищающим вашу сеть от массовых атак хакеров, в том числе: от запросов ping через WAN / синхронного засорения трафика (флудинга) / маршрутизации источника IP-адреса / спуфинга IP-адреса / атаки Smurf. При необходимости функцию файервола можно отключить. При отключении защиты с помощью файервола ваша система не становится полностью уязвимой для атак хакеров, тем не менее рекомендуется включить файервол при первой возможности.



- Фильтрация IP-/MAC-адреса

Маршрутизатор можно настроить на ограниченный доступ к интернету, электронной почте или другим сетевым сервисам в определенные дни и часы. Ограничения можно установить для отдельного компьютера или для нескольких компьютеров, указав IP- или MAC-адрес. Всего в список конфигурации можно ввести до 30 действительных адресов.

[Фильтрация IP-/MAC-адреса клиента]

Режим

Выберите режим фильтрации «Запретить» или «Разрешить»

Направление

С внутреннего на внешний источник (Internal to External)

: Выберите этот параметр, если хотите применить функцию фильтрации к исходящей связи.
(По умолчанию всем клиентам разрешена исходящая связь).

С внешнего на внутренний источник (External to Internal)

: Выберите этот параметр, если хотите применить функцию фильтрации к входящей связи. (по

3. Конфигурация



Протокол

умолчанию все клиенты ограничены в использовании исходящей связи. Таким образом, данная настройка действует при активированной демилитаризованной зоне или переадресации портов). Выберите один из параметров: TCP / UDP / ВСЕ. При выборе параметра «ВСЕ» режим фильтрации будет применяться ко всем протоколам.

Запуск интернет-протокола IP

- С внутреннего на внешний источник

IP-адрес:

Указание IP-адреса внутреннего клиента с целью ограничения его доступа путем фильтрации.

Все IP-адреса:

Применить фильтрацию ко всем клиентам.

MAC-адрес:

Указание MAC-адреса внутреннего клиента с целью ограничения его доступа путем фильтрации. Можно выбрать MAC-адрес клиента с помощью кнопки «Поиск прикладного процессора».

- С внешнего на внутренний источник

IP-адрес:

Указание внешнего IP-адреса с целью ограничения его



- Все IP-адреса: доступа путем фильтрации. Применить фильтрацию ко всем внешним IP-адресам.
- MAC-адрес: Данный параметр недоступен.

Адресат интернет-протокола IP

- С внутреннего на внешний источник
 - IP-адрес/порт: Указание внешнего IP-адреса и порта с целью ограничения его доступа.
 - Все IP-адреса: Применить фильтрацию ко всем внешним IP-адресам.
- С внешнего на внутренний источник
 - IP-адрес/порт: Указание IP-адреса и порта внутреннего клиента с целью ограничения его доступа.
 - Все IP-адреса: Применить фильтрацию ко всем внутренним IP-адресам.

- **Фильтрация уникальных сетевых адресов URL**

Можно заблокировать доступ к конкретному адресу URL интернет-сайта. При указании конкретного адреса URL клиенты не могут зайти по данному адресу. Всего можно указать до 10 адресов.

- **Удаленный доступ к маршрутизатору**

С помощью удаленного управления можно изменять настройки маршрутизатора из любой точки с выходом в интернет.

Пример. Если зарегистрированное имя домена DDNS - "vertexwireless.VW310.com" и в этом пункте меню вы указали номер порта "8888", можно получить доступ к маршрутизатору по следующему адресу: <http://vertexwireless.VW310.com:8888>.



3. Конфигурация



Сервисная программа

- Статическое присвоение IP-адресов DHCP

Используйте это меню, чтобы задать фиксированный локальный IP-адрес для MAC-адреса.

MAC-адрес

В поле "MAC-адрес" введите MAC-адрес, которому вы хотите присвоить фиксированный IP-адрес. Можно также использовать функцию поиска MAC-адреса.

При нажатии кнопки «Поиск MAC-адреса» маршрутизатор найдет MAC-адреса клиентов, подключенных в текущий момент, и выдаст их список в таблице.

IP-адрес

Выберите один MAC-адрес из списка и введите в поле "IP-адрес" IP-адрес, который вы хотите ему присвоить, затем нажмите «Добавить», чтобы добавить информацию о статическом присвоении IP-адреса в таблицу. Убедитесь, что IP-адрес находится между начальным IP-адресом сервера DHCP и максимальным количеством пользователей протокола DHCP.



Список клиентов протокола DHCP и их фиксированные локальные IP-адреса отображаются внизу экрана. Если вы хотите удалить клиента из списка, нажмите кнопку "Del" («Удалить»).

- Сервер динамических доменных имен DDNS

Сервис DDNS позволяет присваивать динамические IP-адреса статическим именам хост-узлов в любом из многих доменов DynDNS.org, обеспечивая таким образом легкий доступ к вашим сетевым компьютерам из различных мест с выходом в интернет. Домен DynDNS.org предоставляет указанный сервис максимум для пяти имен хост-узлов бесплатно с доступом в интернет-сообщество. Сервис DDNS идеально подходит для домашней интернет-страницы, файлового сервера или для легкого доступа к вашему домашнему ПК и сохраненным файлам, например, с работы.

Использование данного сервиса гарантирует, что имя вашего хост-узла всегда будет связано с вашим IP-адресом, независимо от того, как часто ваш интернет-провайдер его меняет. При изменении вашего IP-адреса ваши друзья и знакомые всегда смогут найти вас, набрав адрес vasheimya.dyndns.org.

Для бесплатной регистрации имени своего хост-узла сервера DDNS, зайдите на сайт <http://www.dyndns.org>.

Настройка обновленных данных клиента DDNS, использующего маршрутизатор Перед использованием этой функции необходимо зарегистрироваться в бесплатном сервисе обновления

DynDNS.org. После получения регистрации выполните следующие указания.

Для активации сервиса DDNS нажмите "Enabled" («Активирован»).

Для соединения с интернет-страницей DynDNS.org нажмите кнопку «Click».

В поле «Имя хост-узла» ведите имя домена DynDNS.org, под которым вы зарегистрировались

- Параметр подстановочного знака: Эта настройка позволяет или запрещает использовать подстановочные знаки для вашего хост-узла.
- Например, если ваш DDNS-адрес VW310.dyndns.org и использование

Dynamic DNS Service	
Dynamic DNS	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Service Provider	<input type="text" value="DDNS"/> www.dyndns.com
Host Name	<input type="text"/> <input type="checkbox"/> Use Wildcards
User Name	<input type="text"/>
Password	<input type="text"/>

3. Конфигурация



подстановочных знаков разрешено, тогда достаточно будет набрать x.VW310.dyndns.org («x» - подстановочный знак). Для разрешения использования подстановочных знаков выберите параметр "Use Wildcards" («Использовать подстановочные знаки»).

Введите в поле "User Name" («Имя пользователя») свое имя пользователя для DynDNS.org

Введите в поле "Password" («Пароль») свой пароль для DynDNS.org

Нажмите "APPLY" («Применить»), чтобы обновить свой IP-адрес

При изменении IP-адреса, присвоенного вашим интернет-провайдером, маршрутизатор будет автоматически обновлять ваш IP-адрес на сервере DynDNS.org. Также можно это делать и вручную, нажав кнопку "APPLY" («Применить»).

- Технология UPnP

Универсальный стандарт автоматической настройки конфигураций «включай и работай» (UPnP) – это технология, обеспечивающая комплексную работу с голосовыми сообщениями, видео сообщениями, играми и другими приложениями, совместимыми со стандартом UPnP. Для правильной работы некоторых приложений необходимо внести некоторые изменения в настройки файервола маршрутизатора. Обычно для этого требуется открыть порты TCP и UDP. Приложение, соответствующее технологии UPnP, обладает способностью «разговаривать» с маршрутизатором, сообщая ему какие именно изменения конфигурации файервола нужно произвести.

Маршрутизатор поставляется с отключенным параметром UPnP. Если вы используете приложения, соответствующие стандарту UPnP, и хотите воспользоваться преимуществами технологии UPnP, можно включить параметр UPnP. Просто

выберите "Enabled" («Активизировать») в разделе "UPnP" на странице "Utility" («Сервисная программа»). Нажмите "APPLY" («Применить»), чтобы сохранить изменения.

- Протокол NAT-T

Если вы используете сервисы VPN, VoIP или PPTP, можете активизировать или отключать их в зависимости от вашего сетевого окружения.

- Статическая маршрутизация

Тип соединения по статическому IP-адресу менее распространен по сравнению с другими типами соединения. Это предварительно определенный путь, по которому должна пройти сетевая информация, чтобы попасть в конкретный хост-узел или сеть. Если ваш интернет-провайдер использует IP-адресацию, вам понадобится ваш IP-адрес, маска подсети и адрес шлюза интернет-провайдера. Эту информацию можно получить у своего интернет-провайдера.



Адресат

Адресат - это IP-адрес локальной сети удаленной сети или хост-узел, к которому вы хотите установить статический маршрут.

Маска подсети

Определяет, какая часть IP-адреса из адресата локальной сети относится к сети, а какая - к хост-узлу.

Шлюз

Это IP-адрес устройства шлюза, обеспечивающего связь между маршрутизатором и удаленной сетью или хост-узлом. Таблица статической маршрутизации отображается внизу экрана. Если хотите удалить клиента из списка, нажмите "Del" («Удалить»)

3. Конфигурация



- Самодиагностика

Чтобы шлюз не переходил в ждущий режим во время долгого отсутствия деятельности, осуществляется проверка доступности адресатов (PING-запрос) по адресам, указанным в поле настройки.

Если какой-либо из адресов не отвечает на запрос, он запускает для себя сеанс протокола PPP об отсутствии по определенным причинам (сбой шлюза или прекращение сеанса со стороны оператора).

Диагностика

Если вы хотите использовать функцию самодиагностики, выберите параметр "Enabled" («Активизировать»).

IP- или URL-адрес

Три адреса, по которым отправляется запрос PING.

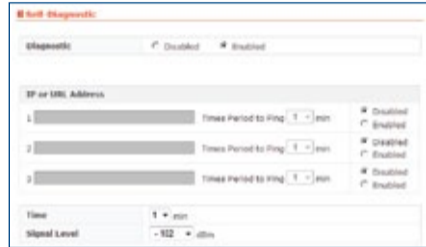
Для каждого адреса установите время посылки запроса PING от 1 до 30 минут, затем выберите параметр "Enabled" («Активизировать»).

Время

Временной интервал для перезапуска сеанса протокола PPP при отсутствии ответа на запрос PING от многих IP-адресов или URL-адресов.

Уровень сигнала

Пределы радиочастотной чувствительности шлюза. Если радиочастотная чувствительность шлюза ниже указанного предела от -102 до -104 дБм, он не будет перезапускать сеанс протокола PPP, поскольку это считается проблемой слабой зоны радиочастот.



- Диспетчер файлов

Данное устройство поддерживает карту microSD для совместного пользования файлами, а также их передачи и хранения. Слот microSD расположен на той же стороне устройства, что и разъем для USB.

1. Осторожно отодвиньте язычок с отметкой "microSD" сбоку устройства.

2. Осторожно вставьте карту microSD (надписью вниз) в слот сбоку устройства до характерного щелчка, означающего, что карта заняла рабочее положение.

**Примечание: Если карта microSD не была отформатирована или записана в формате, который компьютер не распознает, вам может быть предложено отформатировать карту microSD. Во время форматирования стираются все данные, записанные на карте microSD, и после чего файлы нельзя восстановить. Во избежание потери информации, проверьте содержимое карты microSD перед форматированием.

3. Убедитесь, что вы зашли на веб-страницу под своим логином >> Расширенные настройки >> Сервисная программа >> Диспетчер программ

Сервер Если вы хотите использовать функцию совместного использования файлов, оставьте выбранным параметр "Enabled" («Активизировать»). Если нет, выберите параметр "Disabled" («Отключить»), затем нажмите "APPLY" («Применить»).

Идентификатор пользователя Идентификатор пользователя для доступа к карте microSD.

Пароль Пароль для доступа к карте microSD.

Порт Порт для обеспечения совместного использования файлов, а также их передачи и хранения.



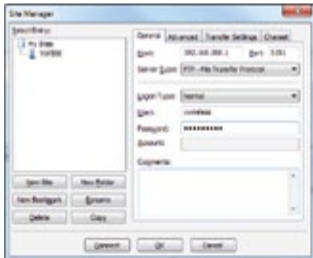
3. Конфигурация



Доступ к карте microSD

Если карта microSD вставлена и распознана диспетчером программ на веб-странице, вставленная карта отобразится в ваших приложениях FTP и приложении VW App для устройств Apple, таких как iPod, iPhone и iPad.

1. В приложении FTP введите тот же идентификатор пользователя, пароль и порт, что установлены в устройстве VW310, затем подключитесь к серверу FTP на устройстве VW310 как показано ниже.



2. В устройстве Apple, выберите пункт "6. VW App".

4. Администратор



- Пароль для входа в систему

Данное меню предназначено для настройки пароля для входа в веб-интерфейс пользователя.

Маршрутизатор поставляется БЕЗ пароля. Если вы хотите для большей безопасности добавить пароль, установите его здесь. Запишите пароль и храните в безопасном месте, поскольку он понадобится, чтобы впредь входить в маршрутизатор. Также рекомендуется установить пароль, если вы планируете использовать функцию удаленного управления маршрутизатором.

- Управление системой

Резервирование и восстановление

С помощью данной функции можно сохранить текущую конфигурацию или восстановить ранее сохраненную конфигурацию. Сохранение конфигурации дает возможность восстановить ее позже, если настройки сбились или изменились. Рекомендуется делать резервную копию текущей конфигурации перед осуществлением программного обновления.

Перезапуск маршрутизатора

Иногда может потребоваться перезапуск или перезагрузка маршрутизатора, если он начинает неправильно работать. Перезапуск или перезагрузка маршрутизатора НЕ приводит к удалению настроек конфигурации.

Восстановить заводские настройки

С помощью этой функции восстанавливаются все заводские настройки маршрутизатора (по умолчанию). Рекомендуется делать резервную копию настроек перед тем, как восстанавливать все настройки по умолчанию.

- Прошивка

Периодически ваш поставщик услуг может выпускать новые версии прошивок маршрутизатора. Прошивка содержит улучшенные функции и способы решения возможных проблем. Когда поставщик услуг выпускает новую прошивку, вы можете загрузить ее с сайта обновлений поставщика услуг и обновить прошивку своего маршрутизатора до последней версии. На странице "Firmware upgrade" («Обновление прошивки») нажмите "Browse" («Поиск»). Откроется окно, в котором можно выбрать файл обновления прошивки. В ходе обновления будет отображаться предупреждение следовать указаниям.

5. Статус



- Информация о статусе

С помощью этого меню можно проверить состояние соединения шлюза. Здесь можно увидеть подробное описание WAN / LAN / WLAN.

- Информация о распределении протокола DHCP

Можно посмотреть список компьютеров (называемых «клиенты»), подсоединенных к вашей сети. Можно посмотреть IP-адрес компьютера, имя хост-узла (если компьютеру был задан хост-узел), а также MAC-адрес карты сетевого интерфейса компьютера.

- Информация о трафике

Маршрутизатор ведет статистический учет трафика, проходящего через него. Можно посмотреть объем пакетов, проходящих через Ethernet и части беспроводного соединения сети. С помощью кнопки Refresh («Обновить») можно сбросить все данные об объеме пакетов.

- Системный журнал

В данном меню отображается системный журнал маршрутизатора, который можно сохранить как текстовый файл с помощью кнопки Save («Сохранить»). Если вы хотите обновить или сбросить данные системного журнала, нажмите кнопку Refresh («Обновить») или Delete («Удалить»).

6. Приложение VW App



1. Установка приложения VW App из интернет-магазина App Store

1 На устройстве Apple установить приложение "VW App" из интернет-магазина App Store



Нажать для начала установки

2. Подключиться к сети Wi-Fi на устройстве VW310

- 1 Включить устройство VW310 при вставленной карте microSD
- 2 Выбрать SSID для устройства VW310 на iPhone

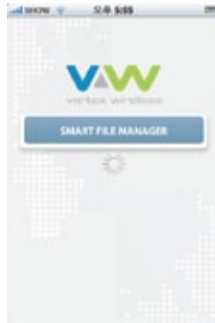


6. Приложение VW App



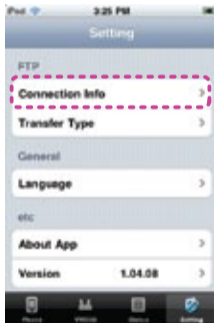
3. Запуск приложения VW App

- 1 Запустить приложение VW App



4. Настройки

- 1 Нажать «Setting» («Настройки»)
- 2 Нажать Connection Info («Информация о соединении»)
- 3 Нажать кнопку “VW310 Find” («Найти VW310»), при этом автоматически загрузится информация о доступе к протоколу ftp в устройстве VW310.Если вы изменили информацию о доступе, нажмите кнопку “Save” («Сохранить»), чтобы сохранить конфигурацию.

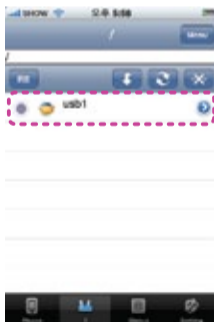
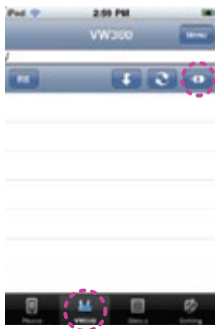


6. Приложение VW App



5. Просмотр карты microSD на устройстве VW310

- 1 Нажмите иконку VW310.
- 2 Нажмите кнопку "Access" («Доступ»).
- 3 Нажмите на папку "usb1".

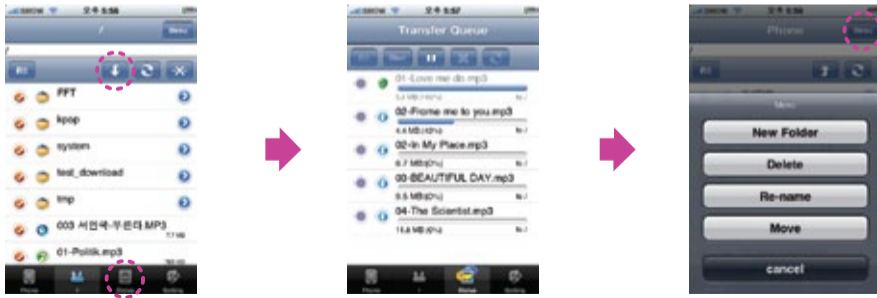


6. Передача файлов

- 1 Выбрать файл, затем нажать значок Download («Загрузка»).
- 2 Нажать значок Status («Статус») и на экране отобразится состояние процесса передачи.
- 3 выгрузка файлов осуществляется так же, как и загрузка.

7. Файлы и папки

- 1 Можно создавать любое количество папок, удалять файлы, изменять название файлов и перемещать файлы в другую папку.
- 2 Нажмите кнопку Menu («Меню») в правом верхнем углу. выберите кнопку с функцией, которую хотите выполнить.



7. Устранение неисправностей



1. Я не могу войти в сервисную программу конфигураций на веб-основе

- Удостовериться в наличии физического соединения, проверив световые индикаторы на устройстве. Если световые индикаторы мигают или не горят, попробовать подключить устройство другим кабелем.
- Отключить активизированное на компьютере программное обеспечение системы безопасности работы в интернете.
- Убедиться, что у вас обновленный веб-браузер с поддержкой языка Java. Рекомендуемые браузеры:
 - Internet Explorer 6.0 или выше
 - Firefox 1.5 или выше
 - Netscape 8 или выше
 - Mozilla 1.7.12 (5.0) или выше
 - Opera 8.5 или выше
 - Safari 1.2 или выше (с Java 1.3.1 или выше)

2. Я забыл(а) пароль.

- Необходимо сбросить все настройки маршрутизатора. К сожалению, это приведет к удалению ваших настроек восстановлению заводских по умолчанию. Чтобы сбросить настройки маршрутизатора, удерживайте кнопку сброса

в течение 10 секунд (кнопка сброса расположена на задней стенке маршрутизатора). Отпустите кнопку, произойдет перезагрузка маршрутизатора, подождите 30 секунд и войдите в маршрутизатор. IP-адрес по умолчанию - 192.168.200.1. (пароль для входа: оставьте поле пароля незаполненным)

3. Я не могу подключиться к некоторым сайтам или отправить/получить письма по электронной почте при подсоединении к маршрутизатору.

- Попробуйте уменьшать максимальный размер пакета передачи данных MTU на десяток (например, 1492, 1482, 1472 и т.д.)

4. Мне нужно обновить прошивку

- Сначала подготовьте соответствующую прошивку для загрузки в маршрутизатор (она предоставляется поставщиком услуг при необходимости), а затем перейдите на страницу "Firmware upgrade" («Обновление прошивки») под именем администратора в веб-интерфейсе пользователя.

