Novacom Wireless

3G (Wi-Fi/HSPA) роутер
GNS-UR4i VPN

[Руководство пользователя]

[02.04.2010]

Содержание

1. Введение

3G (Wi-Fi/HSPA) роутер **Novacom GNS-UR4i VPN** является высокоэффективным инструментом, который организовывает беспроводные сети дома, на работе или в общественном месте. Роутер GNS- UR4i VPN поддерживает использование USB 3G модема, либо WCDMA или EVDO и даже HSDPA, а также поддерживает беспроводную передачу данных до 300 Мбит/сек, и проводной передачи данных до 100 Мбит/с.
Роутер **Novacom GNS-UR4i VPN** отвечает всем требованиям безопасности.

1.1. Комплектация

Важно! В первую очередь проверьте комплектацию оборудования.

Комплект **Novacom GNS- UR4i VPN** должен содержать упомянутые ниже пункты. Если любой из пунктов отсутствует, пожалуйста, свяжитесь со своим торговым посредником.

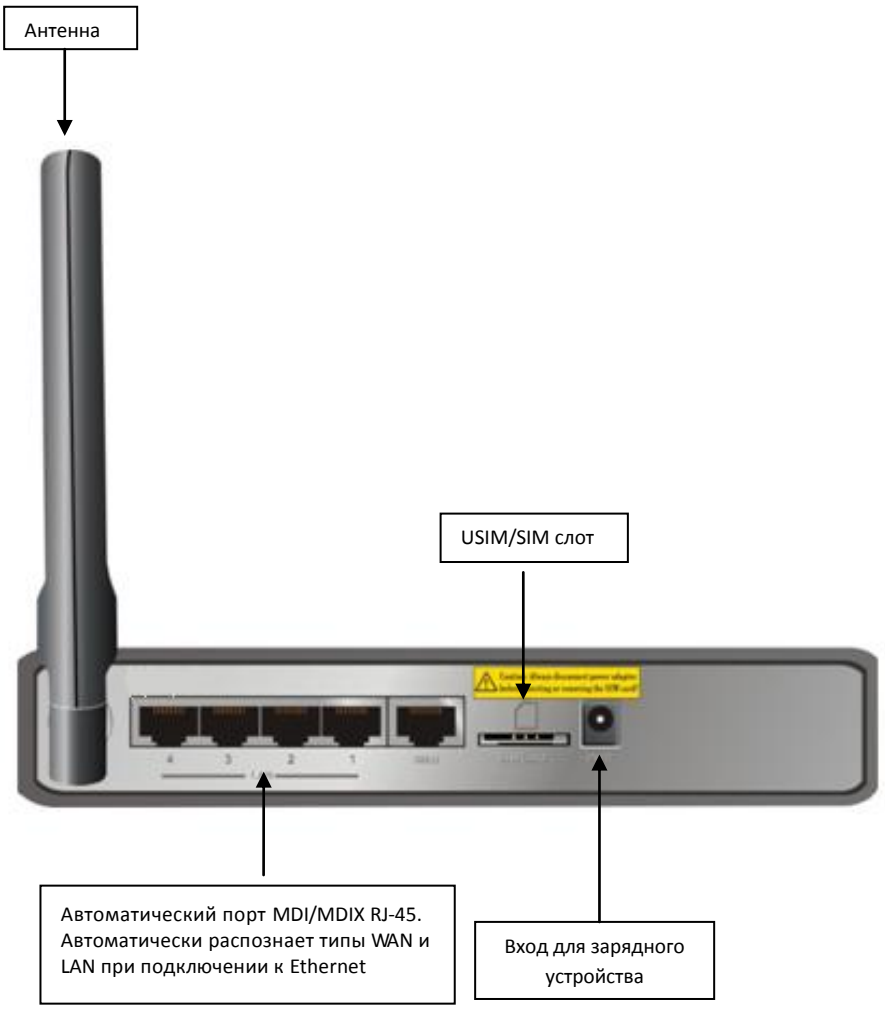
Пункт	Описание	Количество
1	Novacom GNS- UR4i VPN	1
2	Кабель RJ-45	1
3	Адаптер питания 12V 2.0A	1
4	Инструкция по установке	1
5	CD	1

Внимание! Использование источников питания с другим напряжением, кроме включенного в комплект **Novacom GNS- UR4i VPN** может нанести ущерб оборудованию и привести к аннулированию гарантии на этот прибор.

1.2. Системные требования к конфигурации

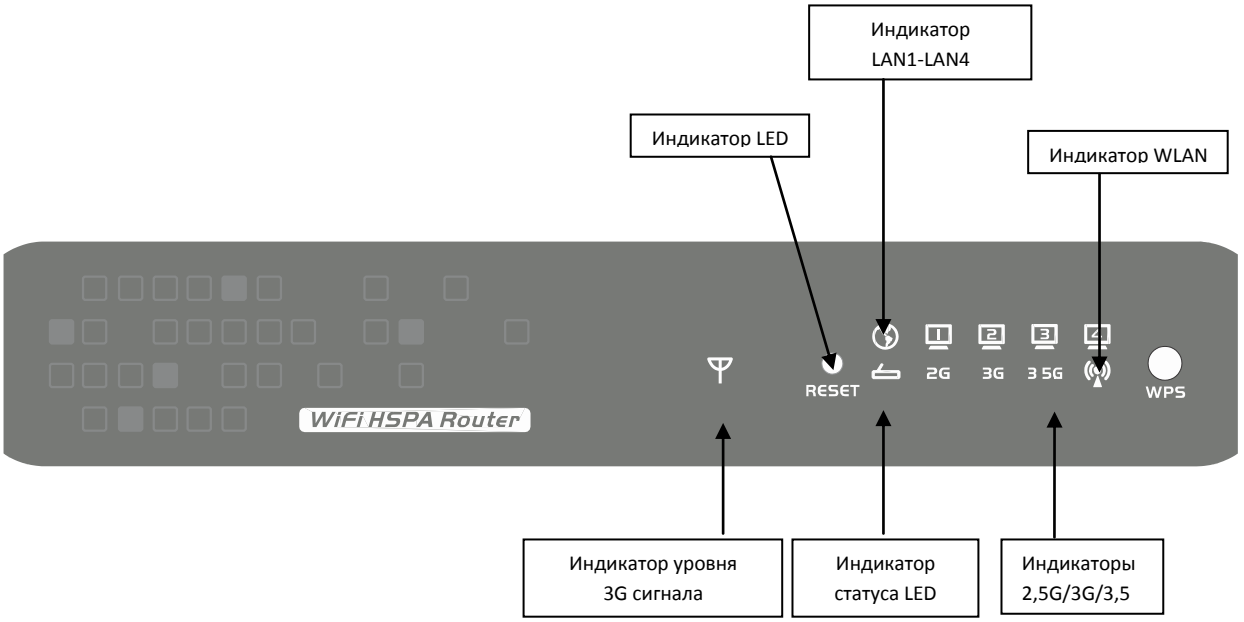
- 3G SIM-карта с подключенным пакетом услуг
  Примечание: условия подключения услуг уточняйте у Вашего оператора
- Компьютеры с операционной системой Windows, Macintosh или Linux с установленным Ethernet адаптером.
- Internet Explorer версии 6.0 или Netscape Navigator версии 7.0 и выше.
- Wi-Fi системные требования: 802.11b, 802.11g или 802.11n адаптер.

1.3. Интерфейсы: вид сзади



Примечание: содержит кнопку перезагрузки для возвращения настроек к оригинальным заводским по умолчанию, в случае, если Вы забыли установленные Вами настройки.

1.4. Индикаторы: вид спереди



Индикатор состояния (WPS):

Мигает зеленым: прибор в обычном режиме
Быстро мигает зеленым: прибор в режиме WPS PBC

A. Индикатор WAN:
Горит зеленым: установлено соединение Ethernet
Мигает зеленым: идет передача данных через Ethernet

B. Индикаторы LAN1 ~ LAN4:
Горит зеленым: установлено соединение Ethernet
Мигает зеленым: идет передача данных через Ethernet

D. Индикатор WLAN (беспроводной локальной сети):
Горит зеленым: WLAN активна и доступна
Мигает зеленым: идет передача данных через WLAN

E. Индикатор 2G/2.5G:
Горит зеленым: установлено соединение EDGE или GPRS
Мигает зеленым: идет передача данных через 2G/2.5G

F. Индикатор 3G:
Горит зеленым: установлено соединение UMTS
Мигает зеленым: идет передача данных через 3G

G. Индикатор 3.5G:
Горит зеленым: установлено соединение HSDPA/HSUPA
Мигает зеленым: идет передача данных через 3.5G

H. Индикатор уровня сигнала:
Мигает красным: нет сигнала от SIM-карты или неверный PIN-код
Горит красным: слабый уровень сигнала (1)

Горит желтым: средний уровень сигнала (2-3)
Горит зеленым: высокий уровень сигнала (4-5)

1.5. Преимущества

1. IEEE 802.11b / g. совместимый

Обратная совместимость с IEEE 802.11b стандартами
Макс. физическая скорость до 54 Мбит/с в режиме 802.11g
Поддержка защиты: WEP (64/128 бит), WPA, WPA2, WPA-PSK, WPA2-PSK, 802.1x и
Поддерживает WPS

2. Встроенный модуль HSUPA модем для 3G-доступа

Скорость закачки до 7.2Mbps
Скорость отдачи до 2.0Mbps
850/1900/2100MHz по HSUPA / UMTS
850/900/1800/1900MHz для EDGE/GPRS/GSM802.

3. 5 портов 10/100 RJ-45

4 * LAN
1 * WAN (Поддержка 3G-соединения)

4. Подключение к глобальной сети через Ethernet

Динамический IP (DHCP-клиент)
Статический IP
PPPoE
PPTP
L2TP

5. PPTP через 3G соединение с глобальной сетью

6. Встроенная функция трансляции сетевых адресов: один IP на несколько компьютеров

7. Встроенный firewall для защиты Вашей сети

8. VPN через поддерживаемые
   PPTP
   L2TP
   IPSec

9. Легкая установка обновлений
   Web интерфейс
   Windows утилита

10. Легкое управление:
    Web интерфейс
    SNMP

TR069(Опционально)
UpnP

11. Сетевые протоколы
    UDP/TCP/IP/ARP/RARP/ICMP
    DHCP/PPPoE
    DNS/TFTP/HTTP

12. Антенна
    1 x Внешняя 3G антенна
    1 x Встроенная 3G антенна
    1 x Встроенная Wi-Fi антенна

13. Подключение нескольких компьютеров к широкополосному либо WCDMA или EV-DO Интернету или даже использование HSDPA модема для общего подключения к Интернету.

2. Настройка 3G-роутера GNS- UR4i VPN

2.1. Требования по установке

3G-роутер GNS- UR4i VPN позволяет получить доступ к сети с помощью беспроводного соединения, практически из любого места в пределах его рабочего диапазона. Но следует учесть, что количество, толщина и расположение стен, потолков или других объектов, через которые должны будут проходить беспроводные сигналы, могут сузить этот диапазон. Стандартный диапазон варьируется в зависимости от типа используемых материалов, и уровня радиопомех в помещении.

Чтобы увеличить эффективность работы оборудования, пожалуйста, соблюдайте данные инструкции:

1. Ограничьте количество преград между GNS- UR4i VPN и другими сетевыми устройствами. Каждая стена или потолок может сократить диапазон работы роутера от 1 до 30 м.
   Примечание: те же свойства касаются и широкополосного соединения EVDO.
2. Держите роутер вдали от электрических устройств (таких, как микроволновые печи, кондиционеры и телевизоры), которые испускают большое количество радиопомех.

2.1.1 Инструкции по установке: настройка сети

Подключите роутер к Сети

Внимание: не подключайте роутер к питанию до того, как выполните необходимые действия по установке, указанные ниже:

1. Подсоедините антенну: рис. 2.1

Рис. 2.1

a. Извлеките антенну из пластиковой упаковки.
b. Вкрутите антенну по часовой стрелке в отверстие на задней панели устройства.
c. После этого направьте антенну вверх. Это обеспечит оптимальный прием.

2. Вставьте SIM/USIM карту в роутер одним из предложенных способов: **Рис. 2.2**

Рис. 2.2

3. Вставьте соединительный Ethernet кабель в порт LAN на задней панели шлюза и в свободный Ethernet порт на сетевом адаптере компьютера, который Вы будете использовать для настройки оборудования. **См. рис. 2.3**

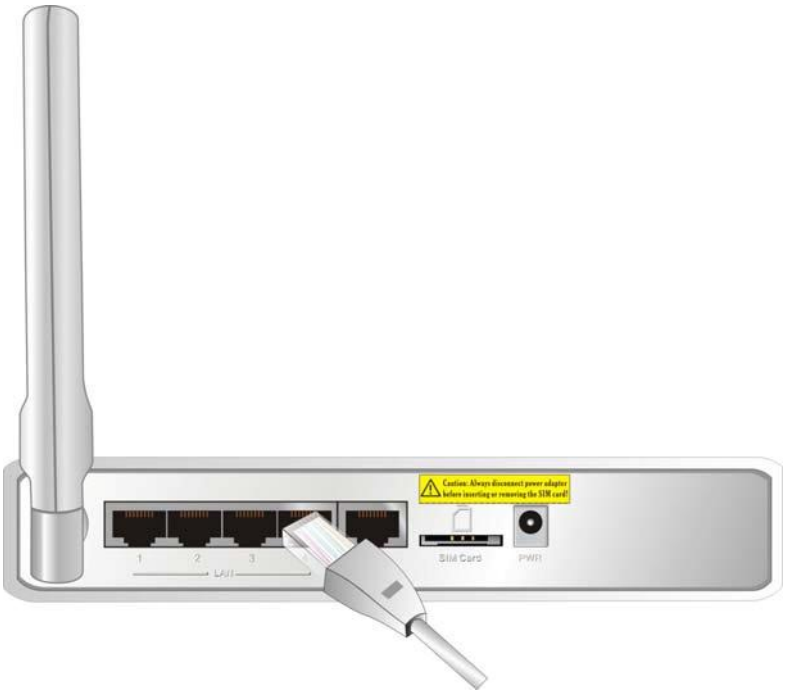


Рис. 2.3

Внимание: LAN порты Wi-Fi HSPA роутера поддерживают технологию “Auto-MDI/MDIX”, то есть он сами определяет вход и выход и допускают соединение с компьютером, свитчем и т.д. как прямым, так и перекрёстным кабелем локальной сети.

4. (Опционально), Вставьте Ethernet кабель в порт Wired WAN port на задней панели шлюза. Этого можно не делать, если Вы выбираете беспроводное 3G соединение. **См. рис. 2.4**

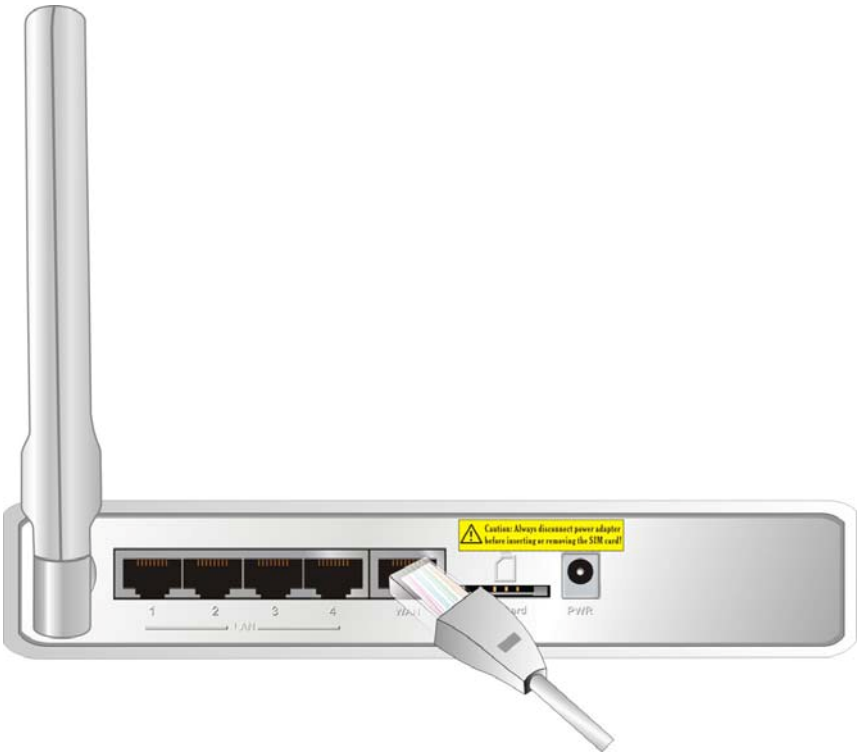


Рис. 2.4

Важно: У 3G-роутера WAN портом также является “Auto-MDI/MDIX.”. Он обеспечивает кабельное Ethernet соединение через LAN.

5. Подключите адаптер питания к разъему на задней панели 3G роутера. Затем подключите другой конец адаптера питания к розетке или удлинителю. **Рис. 2.5**

Рис. 2.5

6. Индикаторы (См.рис 2.6)
   a. Все индикаторы засветятся, сигнализируя, что питание подключено
   b. Затем индикаторы начнут мигать, сигнализируя, что шлюз выполняет инициализацию и процесс подключения к Интернету. Это займет несколько минут.
   c. Когда соединение будет установлено, начнет мигать индикатор WLAN
   d. См. Пункт 1.4 данного руководства: «Индикаторы: вид спереди».

Рис. 2.6

2.1.2 Установка соединения Wi-Fi

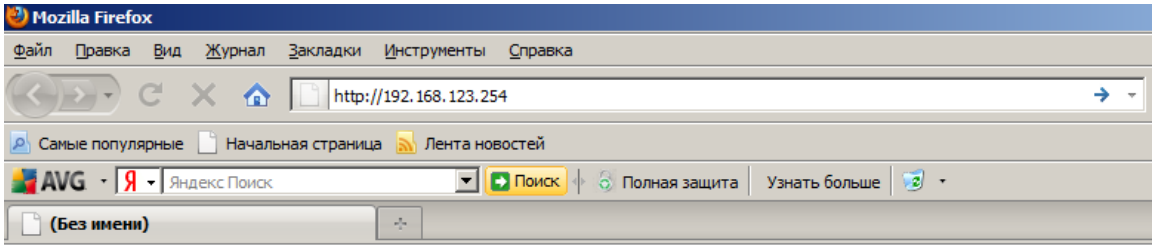
Если Вы выбрали параметры шифрования WEP или WPA-PSK, проверьте, чтобы данные настройки совпадали с настройками Вашего Wi-Fi адаптера.

Wi-Fi и параметры шифрования должны совпадать с доступом к меню конфигурации 3G-роутера и с доступом в Интернет. Пожалуйста, обратитесь к документации Wi-Fi адаптера для дополнительной информации.

3. Использование меню конфигурации

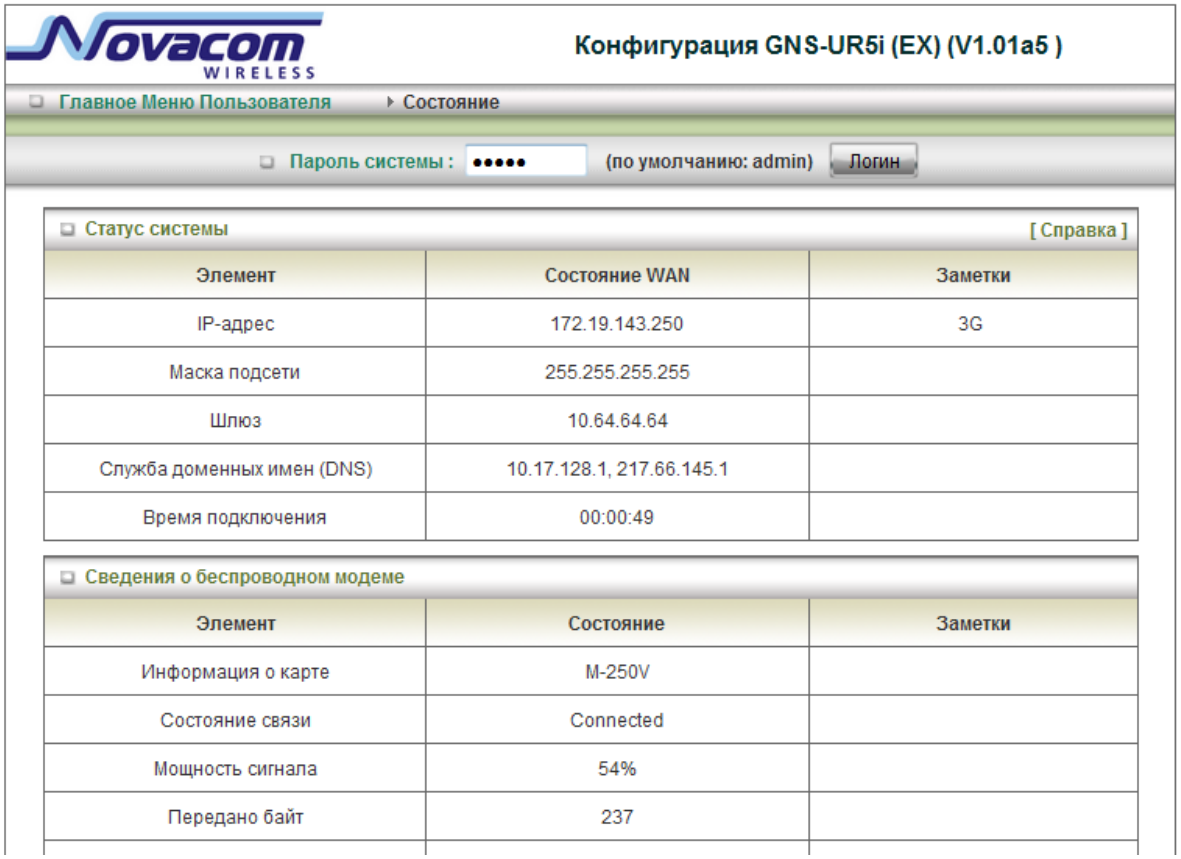
После правильной настройки GNS- UR4i VPN будет получать и присваивать IP адрес автоматически. Параметры конфигурации могут быть установлены через меню конфигурации GNS- UR4i VPN Вы можете получить доступ к этому интерфейсу, выполнив действия, перечисленные ниже:

1. Откройте веб-браузер.
2. Введите **IP Адрес** (http://192.168.123.254) 3G-роутера



Внимание: Если Вы меняли IP адрес роутера, присваиваемый по умолчанию, убедитесь, что вводите верный IP адрес.

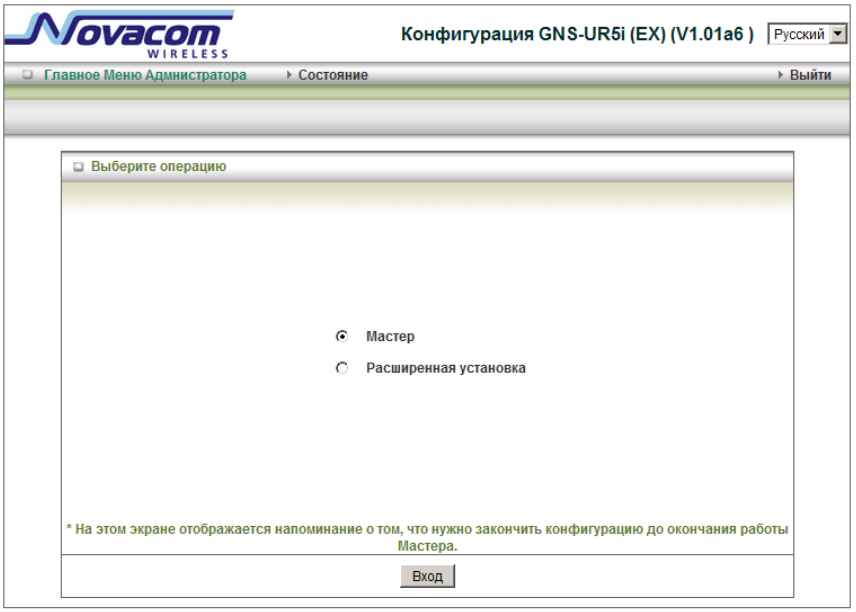
3. Наберите “**admin**” в поле для ввода пароля.



4. Нажмите кнопку Login.

3.1. Мастер настройки

- Выберите “**Мастер**” для более простого задания базовых настроек. (Сверьте с пунктом 3.1).
- Или нажмите “**Расширенная установка**” для расширенных настроек (Пожалуйста, сверьте с каждым пунктом раздела 3.2 «Меню администратора»).

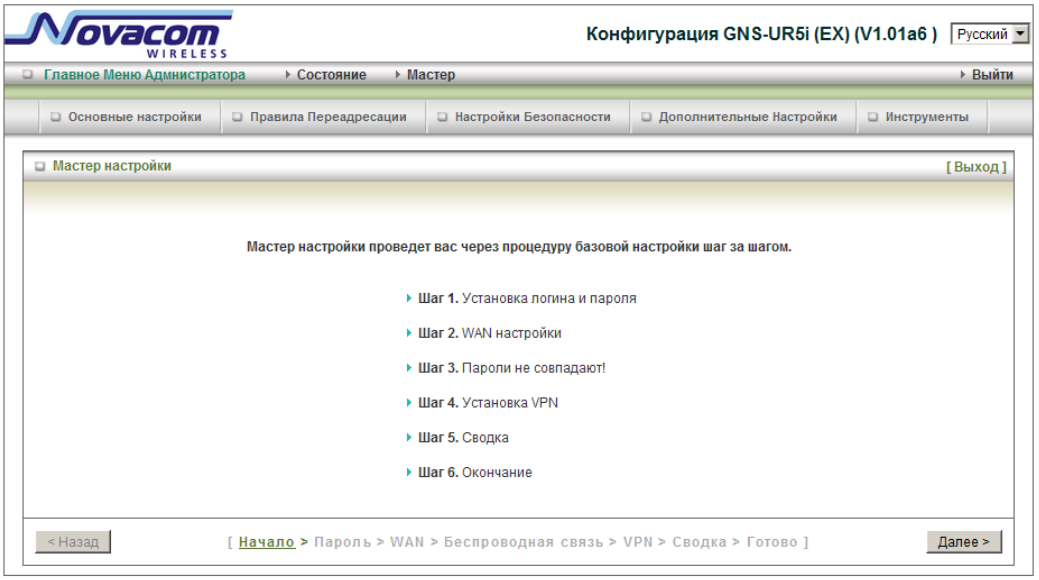

Конфигурация GNS-UR5i (EX) (V1.01a6)
Русский
Главное Меню Администратора
Состояние
Выйти
Выберите операцию
Мастер
Расширенная установка
* На этом экране отображается напоминание о том, что нужно закончить конфигурацию до окончания работы Мастера.
Вход

Нажмите «Вход» для запуска.

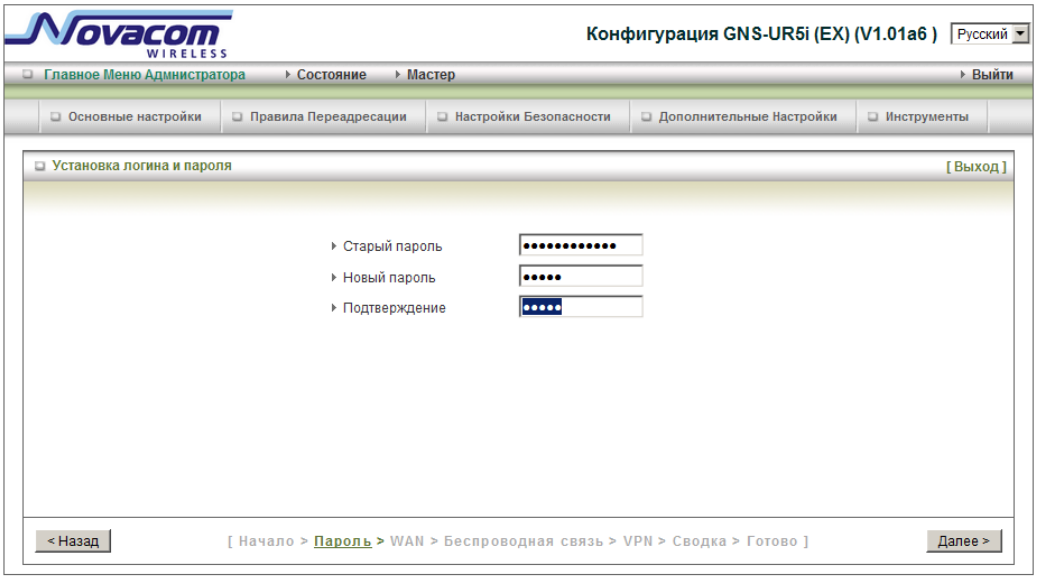
С пошаговым мастером настройки, Вы сможете легко настроить роутер. Эти настройки включают в себя настройку:

a. Логина и пароля,
b. Настройки WAN
c. Настройки беспроводного соединения,

Нажмите кнопку «Далее» для запуска конфигурации.



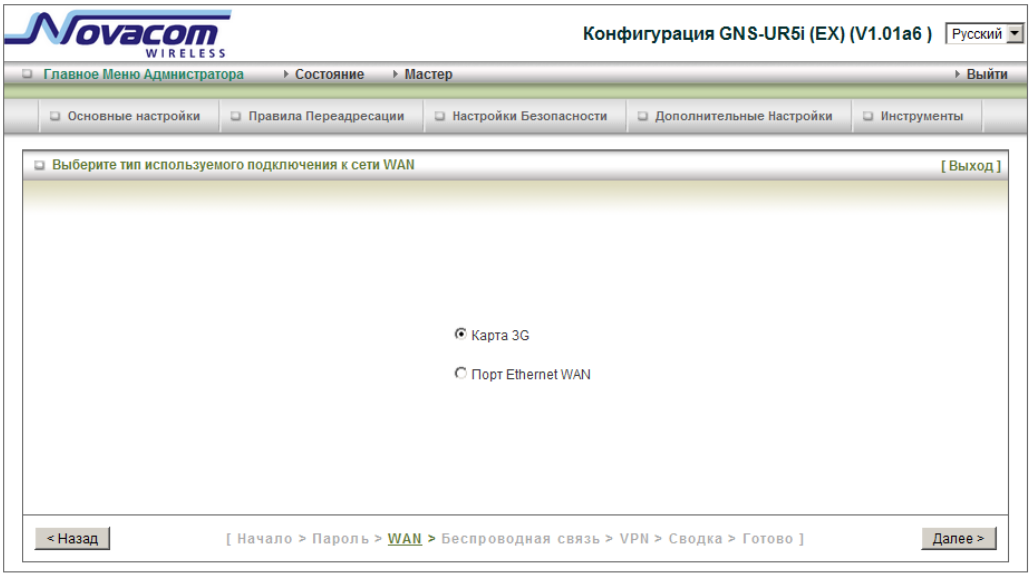
Шаг 1: Позволяет изменить системный пароль.



Вы можете изменить пароль. Рекомендуется изменить системный пароль на Ваш собственный из соображений безопасности.

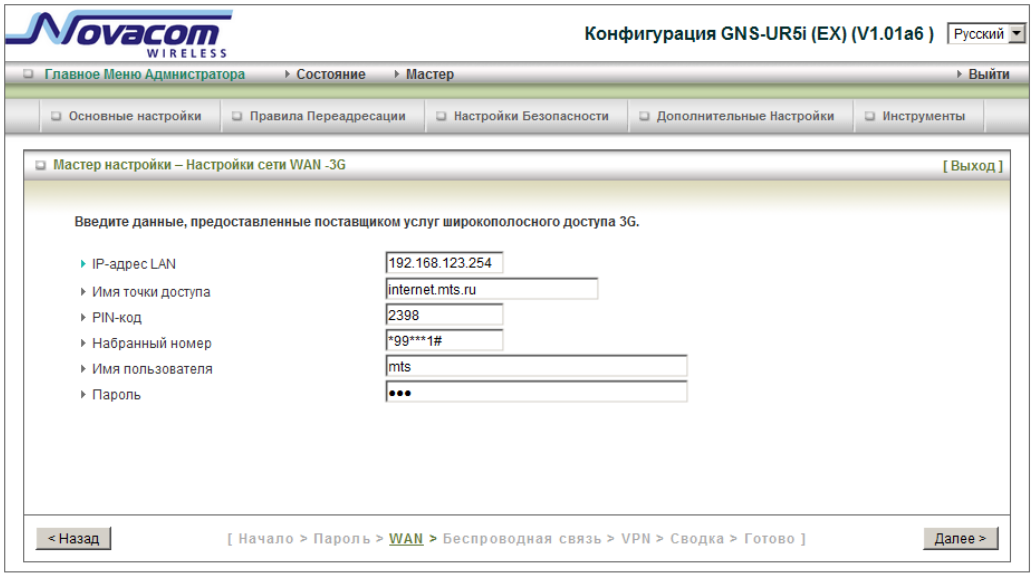
1. Введите Ваш старый пароль (если смена пароля первая, слово “admin” является паролем по умолчанию.)
2. Введите Ваш новый пароль
3. Введите этот новый пароль еще раз для подтверждения.
4. Нажмите «Далее», чтобы перейти к следующим установкам.

Шаг 2: Выбор соединения: Локальная сеть, 3G или проводной Ethernet.



.

Шаг 3: Настройка соединения 3G для выхода в Интернет.



Введите информацию, предоставленную провайдером услуг 3G.
Нажмите «Далее»

LAN это сокращение от Local Area Network (Локальная Сеть), и подразумевает Вашу внутреннюю сеть. Это IP настройки интерфейса LAN для 3G роутера, и они подразумевают Ваши собственные настройки. Вы можете изменить IP адрес LAN при необходимости. IP адрес LAN относится только к Вашей внутренней сети и не может быть отслежен через Интернет.

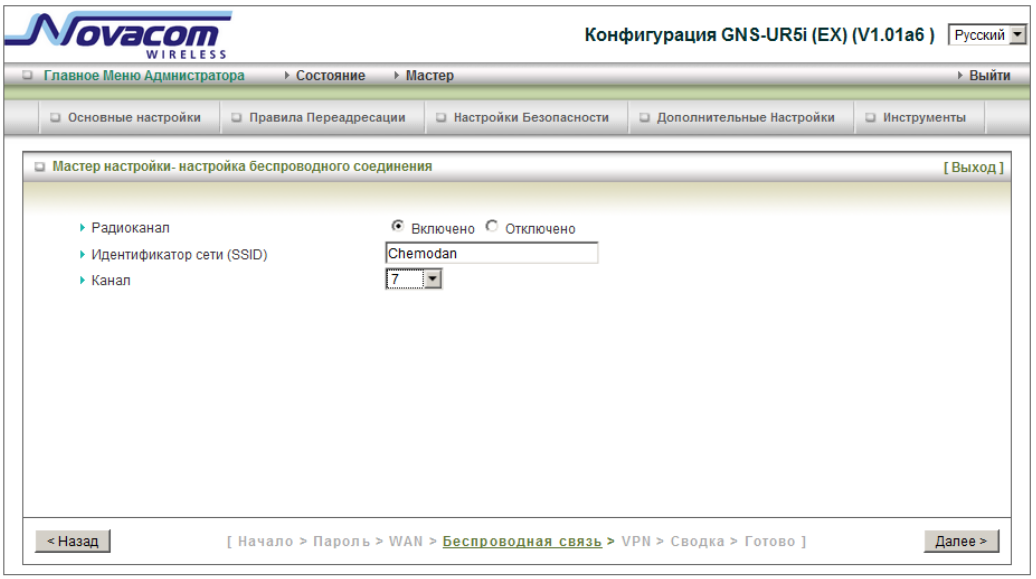
Важно: На роутере 3G при использовании подсети 255.255.255.0 (Class C) доступно 254 адреса. Например: IP адрес роутера: 192.168.123.1. Доступный разброс IP адресов клиентов от 192.168.123.2 до 192.168.123.254.

1. **IP адрес LAN -** IP адрес интерфейса LAN. По умолчанию это: **192.168.123.254**
2. Имя хоста - опционально
3. MAC адрес WAN

Если Вы нажмете кнопку Clone MAC, адрес установится автоматически

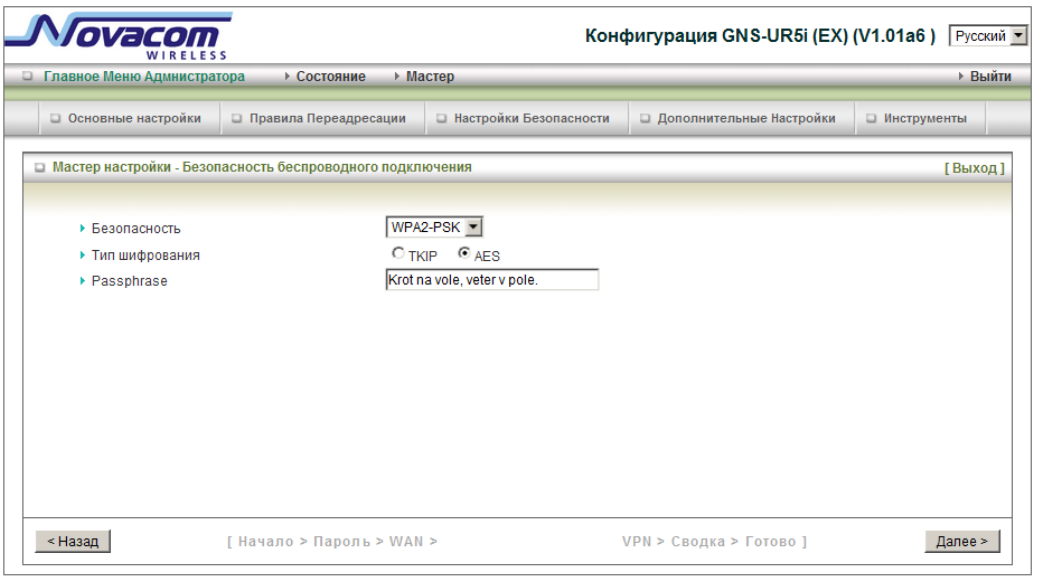
4. Нажмите «Далее», чтобы продолжить установку.

Шаг 5: Изменение настроек беспроводного соединения.



1. Выберите «Вкл.» или «Выкл.» По умолчанию установлено «Выкл.».
2. ID сети (SSID) будет установкой по умолчанию.
3. Канал: Выберите местный беспроводной канал для подключения к сети.
4. Нажмите «Далее».

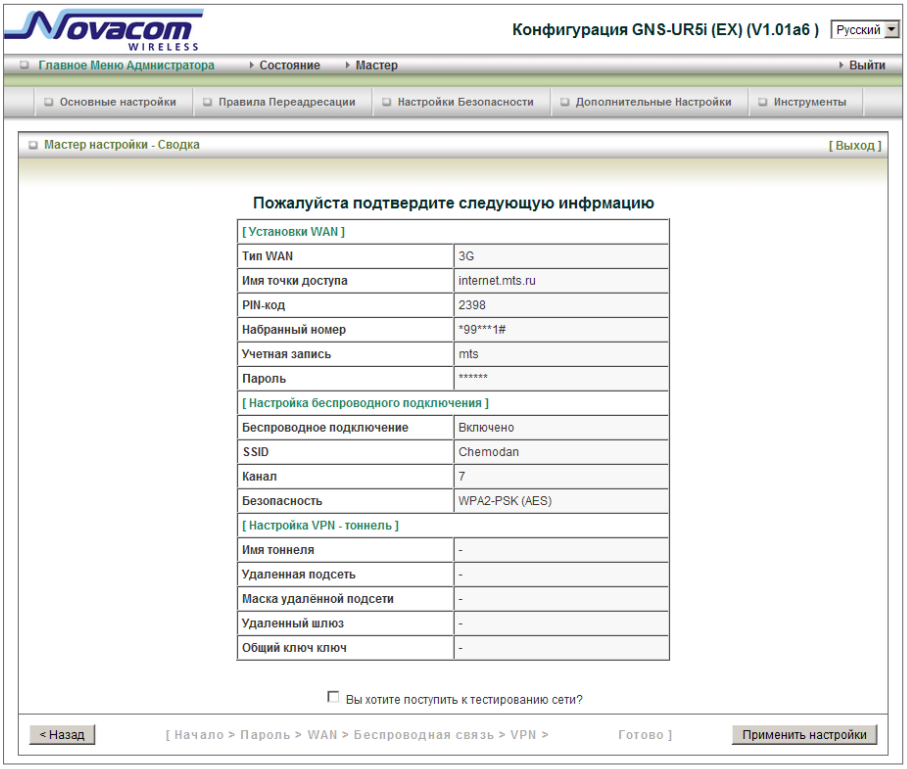
Шаг 6: Выберите метод защиты Ваших беспроводных настроек.



1. Выберите тип защиты “WPA2-PSK”, тип шифрования («AES”) и введите WPA ключ.

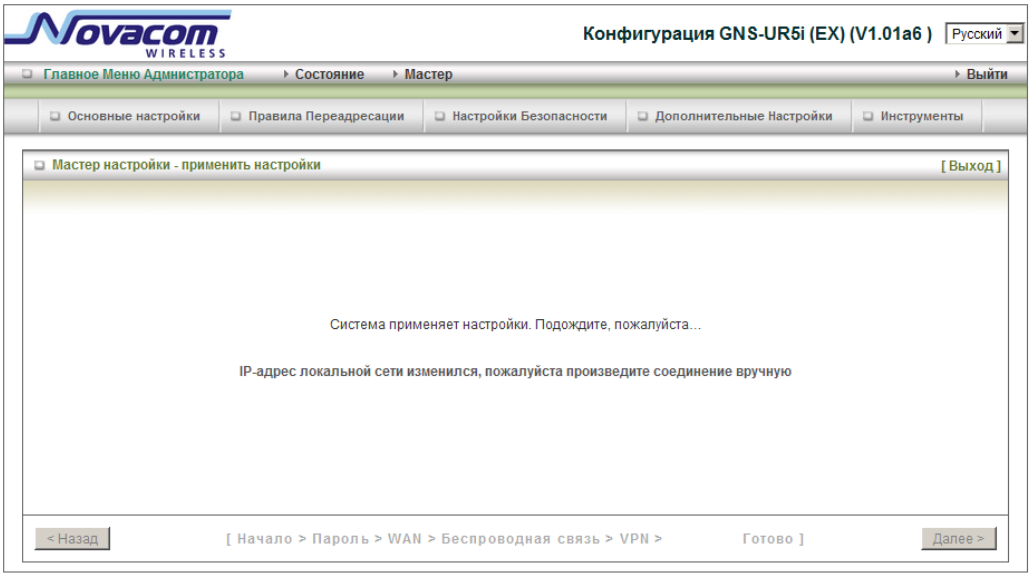
2. Нажмите «Далее»

Шаг 7: Сводка (проверка настроенных параметров).



Нажмите кнопку «Применить настройки»

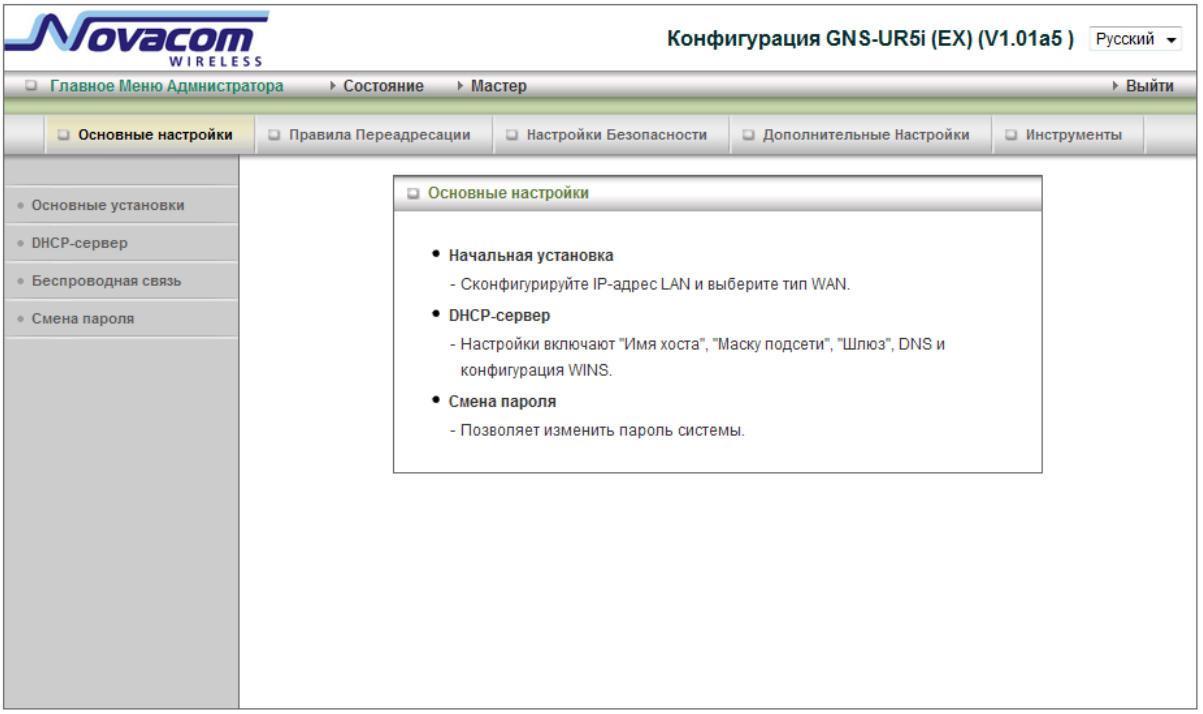
Шаг 8: Загрузка настроек



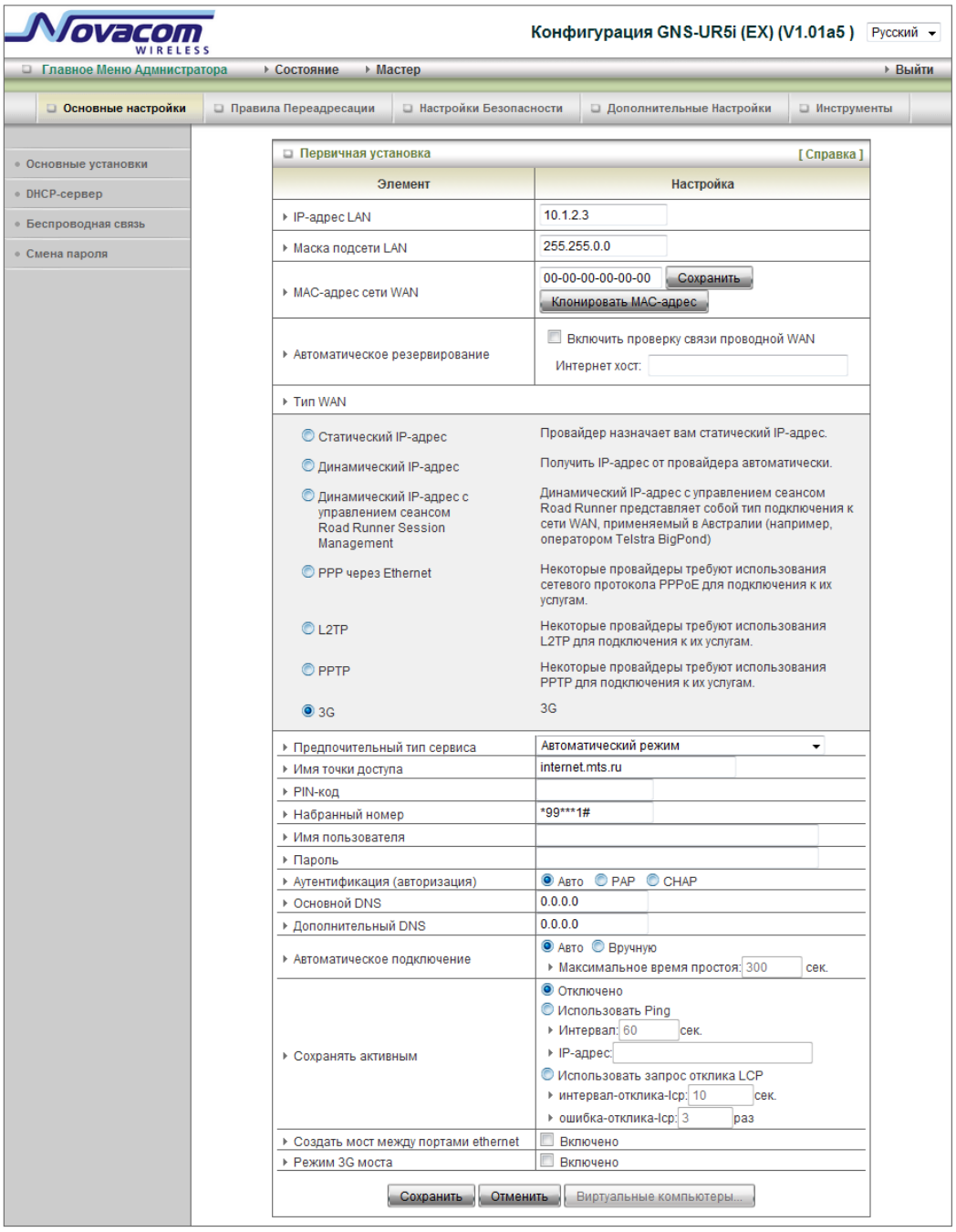
Нажмите «Далее» для возврата на страницу статуса.

3.2. Меню Администратора

3.2.1 Основные настройки



3.2.1.1 Основные установки — тип WAN, виртуальные компьютеры.



1. **IP адрес LAN:** локальный IP адрес устройства. Компьютеры Вашей сети должны использовать IP адрес локальной сети Вашего оборудования как шлюз по умолчанию. Вы можете изменить его при необходимости.
2. **MAC адрес WAN:** адресом по умолчанию является адрес WAN интерфейса роутера.
3. **Клонирование –MAC адреса WAN: Эта функция позволяет скопировать** MAC адрес Вашей сетевой карты и заменить им WAN MAC адрес роутера. MAC

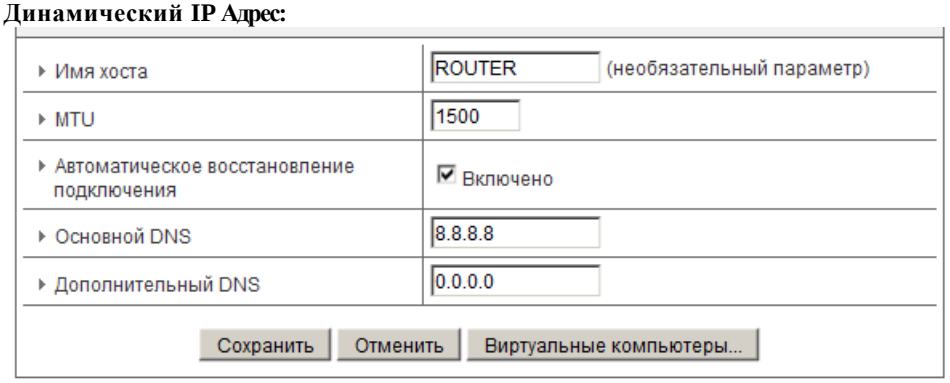
адрес, установленный по умолчанию, менять не рекомендуется, если этого не требует Ваш провайдер.

4. Тип **WAN**: Тип соединения WAN, установленный Вашим Провайдером.

Статический IP Адрес

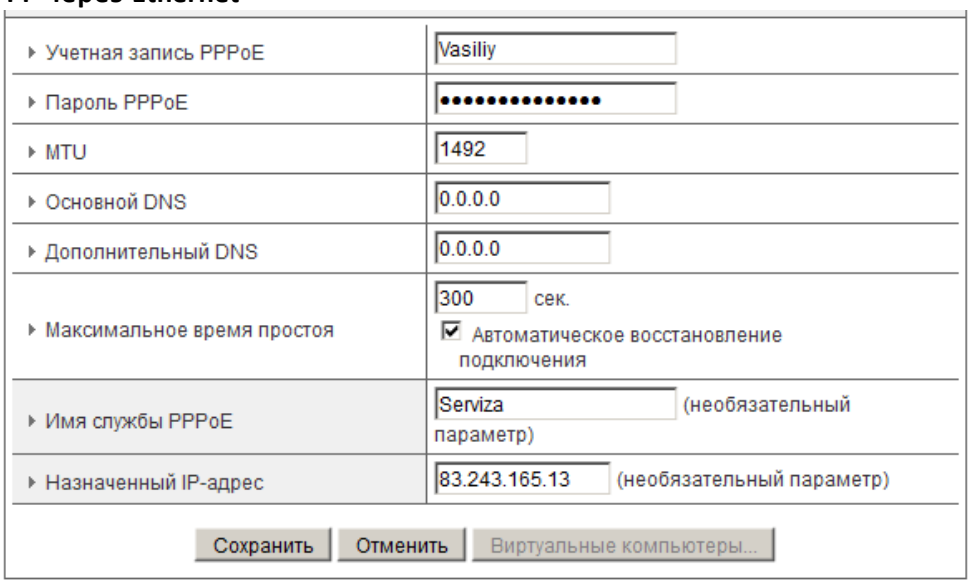
WAN IP адрес, маска подсети, роутер, первичный и вторичный DNS: введите нужные значения, установленные Провайдером.

Динамический IP Адрес:



1. Имя хоста: опционально, требуется некоторыми провайдерами, например, @Home.
2. MTU(Максимальный размер блока информации): Большинство провайдеров устанавливает значение MTU для пользователей. Наиболее распространенное значение MTU - 1492.
3. Автоматическое восстановление подлкючения: эта функция позволяет роутеру восстановить Ваш IP адрес автоматически после истечения времени аренды, даже когда система неактивна.

PPP через Ethernet

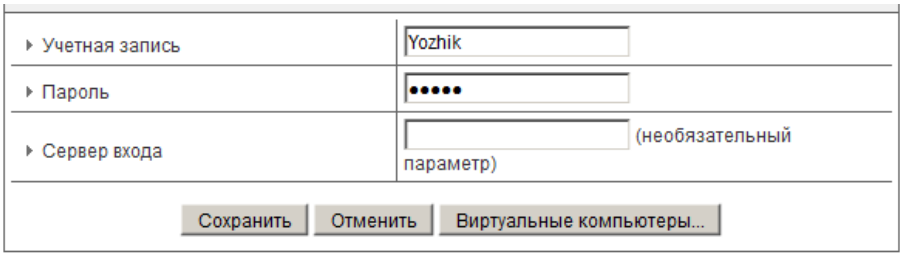


1. Учетная запись и пароль PPPoE: учетная запись и пароль, установленные провайдером. В целях обеспечения безопасности, в поле пароля ничего не отображается. Если вы не хотите менять пароль, оставьте поле пустым .
2. Максимальное время простоя: время, в течение которого компьютер остается

неактивным перед тем, как отключить сессию PPPoE. Установите это значение на ноль или подключите функцию автоповтора соединения, чтобы отключить данную функцию.

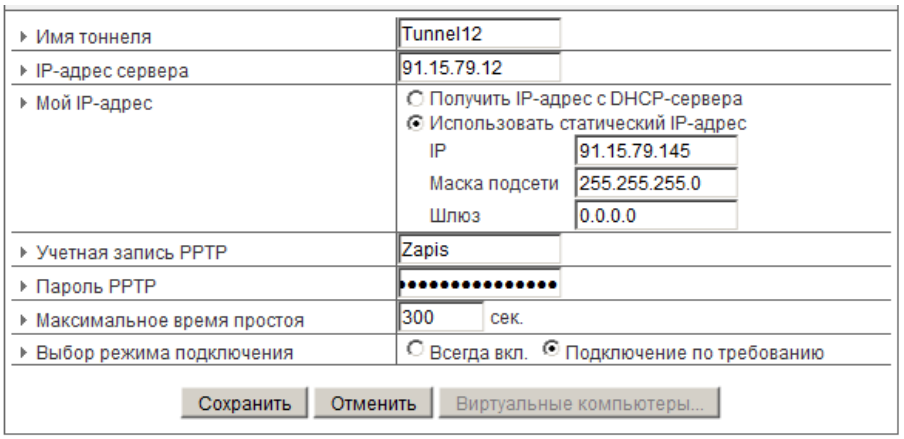
3. Автоматическое восстановление соединения (Всегда включен): Устройство будет связываться с провайдером, пока соединение не будет установлено.
4. Сервисное имя PPPoE : опционально. Введите сервисное имя, если провайдер требует этого. В ином случае, оставьте поле пустым.
5. Максимальный размер блока информации (MTU): Большинство провайдеров устанавливает значение MTU для пользователей. Наиболее распространенное значение MTU - 1492.

Динамический IP адрес с управлением сеансом Road Runner



Учетная запись и пароль: учетная запись и пароль, установленные провайдером.

PPTP



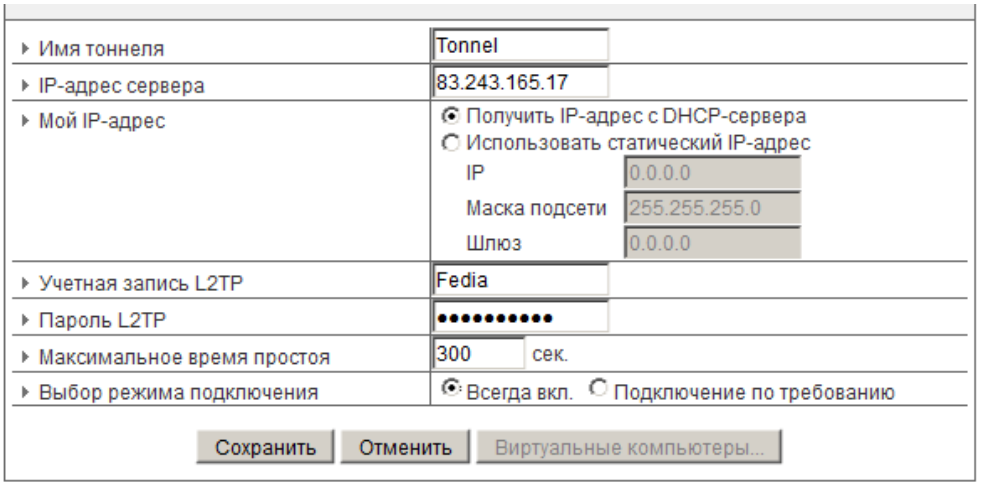
1. Прежде всего, проверьте настройки провайдера, узнайте, присвоен Вам статический или динамический IP адрес. Например: При использовании Статического адреса, провайдером предоставляется выделенный IP адрес, маска подсети и шлюз.
2. IP адрес сервера: IP адрес сервера PPTP.
3. Учетная запись и пароль PPTP: учетная запись и пароль, установленные для Вас Вашим провайдером.. В целях обеспечения безопасности, в этом поле ничего не отображается. Если вы не хотите изменить пароль, оставьте поле пустым.
4. Максимальное время простоя: время, в течение которого компьютер

остается неактивным перед тем как отключить сессию PPTP. Установите это значение на ноль или подключите функцию «всегда вкл» соединения, чтобы отключить данную функцию. Если функция «всегда вкл» соединения включена, шлюз будет автоматически соединяться с провайдером после перезагрузки системы или сброса соединения.

5. Выбор режима соединения: Существует два режима:

Соединение по запросу: Устройство будет соединяться с провайдером , если клиенты посылают исходящие пакеты.
Всегда включено: Устройство будет связываться с провайдером пока соединение не будет установлено.

L2TP



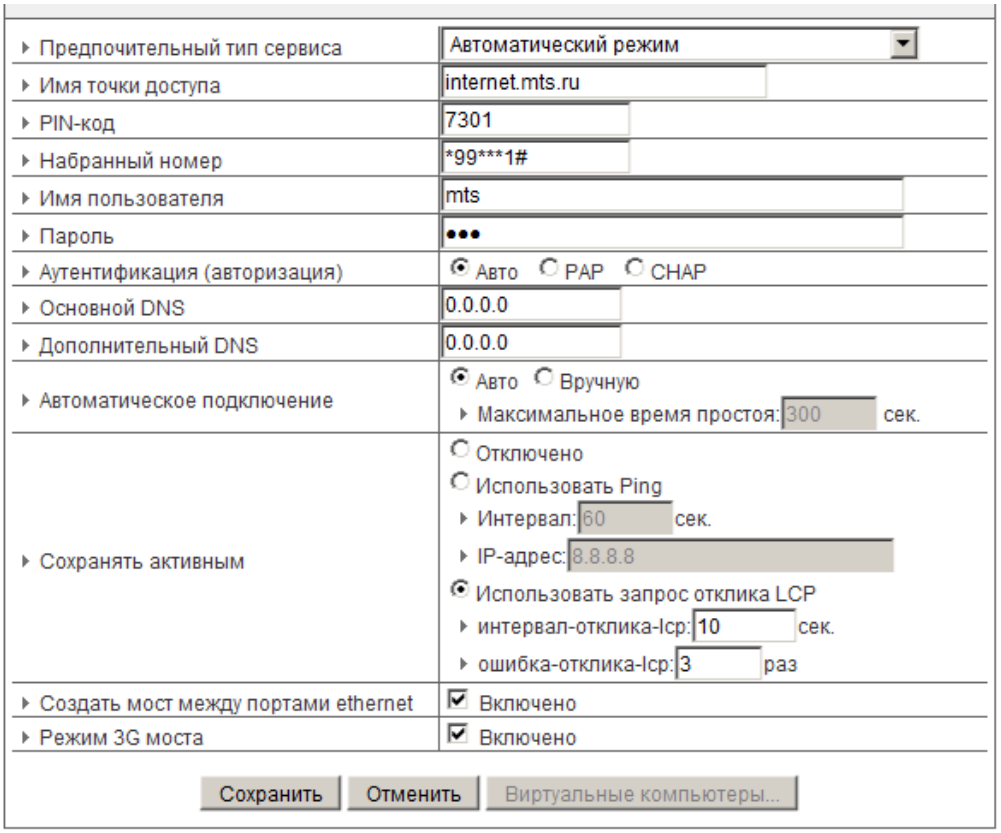
1. Прежде всего проверьте настройки Вашего провайдера, узнайте, присвоен Вам статический или динамический IP адрес.

Например: При использовании Статического адреса, провайдером предоставляется выделенный IP адрес, маска подсети и шлюз.

2. IP адрес сервера: IP адрес сервера L2TP.
3. Учетная запись и пароль PPTP: учетная запись и пароль, установленные для Вас Вашим провайдером.. В целях обеспечения безопасности, в этом поле ничего не отображается. Если вы не хотите изменить пароль, оставьте поле пустым.
4. Максимальное время простоя: время, в течение которого компьютер остается неактивным перед тем как отключить сессию L2TP. Установите это значение на ноль или подключите функцию авто-повтора соединения, чтобы отключить данную функцию. Если функция автоповтора соединения включена, шлюз будет автоматически соединяться с провайдером после перезагрузки системы или сброса соединения.
5. Выбор режима соединения: Существует два режима:

Соединение по запросу: Устройство будет соединяться с провайдером , если клиенты посылают исходящие пакеты.
Всегда включен: Устройство будет связываться с провайдером пока соединение не будет установлено.

3G



Для соединения 3G. Заполнение этих полей может быть не обязательным для установки соединения. Информация на данной странице используется только в случае требования провайдера ввести Имя пользователя и Пароль для подключения к сети 3G.
Пожалуйста, сверьтесь с документацией или службой поддержки провайдера для дополнительной информации.

1. Предпочтительный тип сервиса: Существует 5 режимов: Автоматический / Предпочтительный 3G / Только 3G / Предпочтительный 2G / Только 2G.
2. APN: Введите здесь APN Вашего компьютера.
3. Пин-код: Введите Пин-код Вашей SIM карты
4. Dial-Number: Это поле можно не заполнять, если этого не требует Ваш провайдер
5. Имя пользователя: Введите здесь новое имя пользователя для Вашего компьютера
6. Пароль: Введите новый пароль.
7. Первичный DNS: Эта функция позволяет установить первичный DNS сервер (опционально)
8. Вторичный DNS: Эта функция позволяет установить вторичный DNS сервер (опционально)

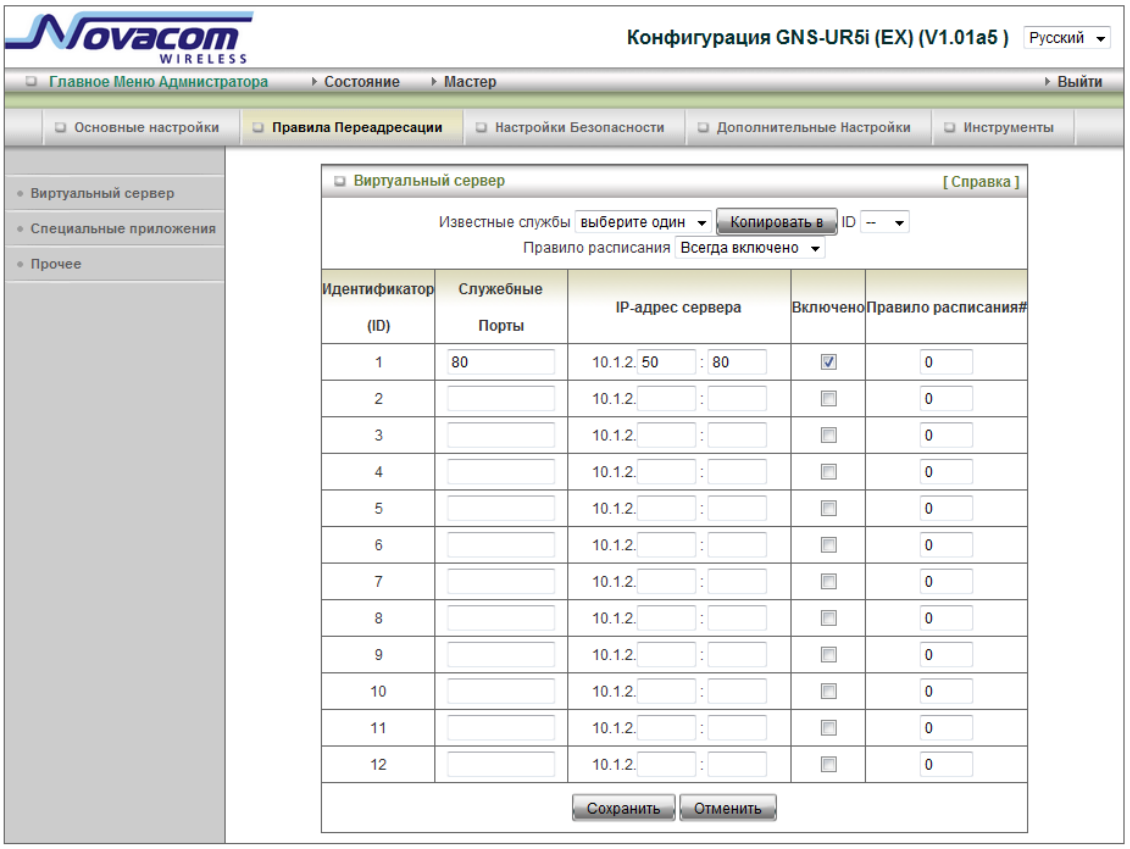
Авто-соединение: Существует 2 режима:

Автоматический: Устройство будет соединяться с провайдером , если клиенты посылают исходящие пакеты

Ручной: Вручную: Устройство не будет устанавливать соединение до тех пор, пока не нажата клавиша соединения на странице статуса.

9. Максимальное время простоя: Соединение будет разорвано при достижении этого значения времени простоя.
10. Сохранять активным (английский термин Keepalive): Существует 3 режима: Отключен / Использовать Ping /Использовать LCP Echo запрос
11. Создать мост между портами Ethernet. В этом режиме порт WAN используется как 5 порт локальной сети.

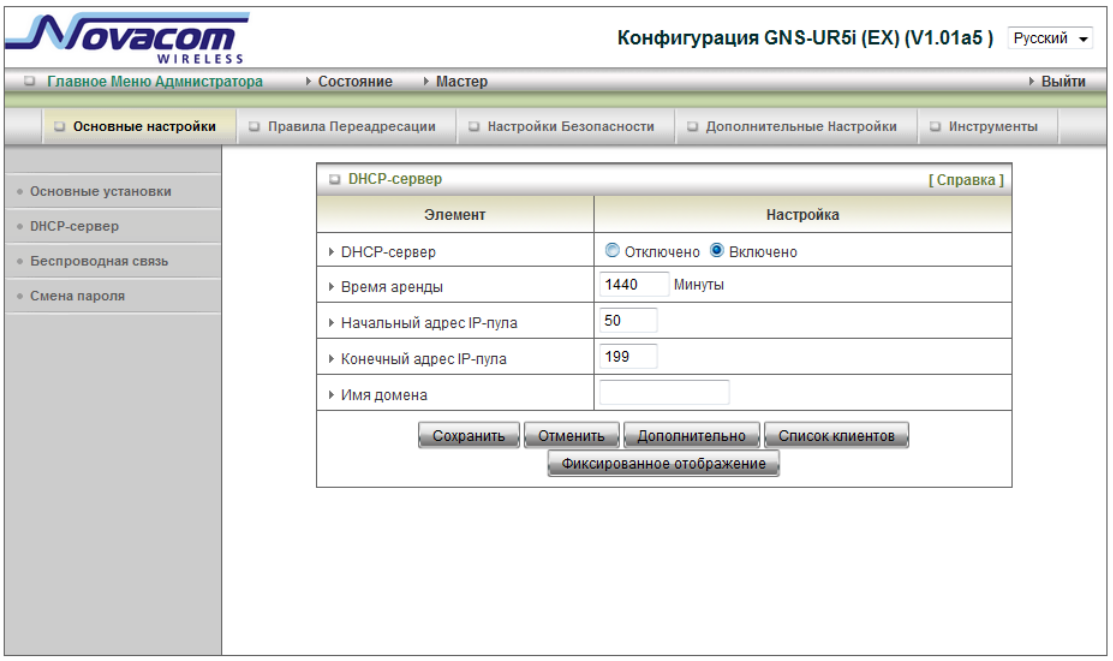
3.2.1.2 Виртуальные компьютеры Эти настройки имеют смысл в том случае, если от роутер получает внешний IP-адрес в Интернет.



Виртуальный компьютер позволяет использовать оригинальные функции NAT, а также позволяет вам настроить взаимно-однозначное отображение нескольких глобальных IP адресов и локального адреса IP.

1. Глобальный IP: Введите глобальный IP адрес, установленный Вашим провайдером.
2. Локальный IP: Введите локальный IP адрес Вашей локальной сети, связанный с глобальным IP адресом.
3. Установить: Отметьте этот пункт для включения функции Виртуального компьютера.

3.2.1.3 DHCP Сервер



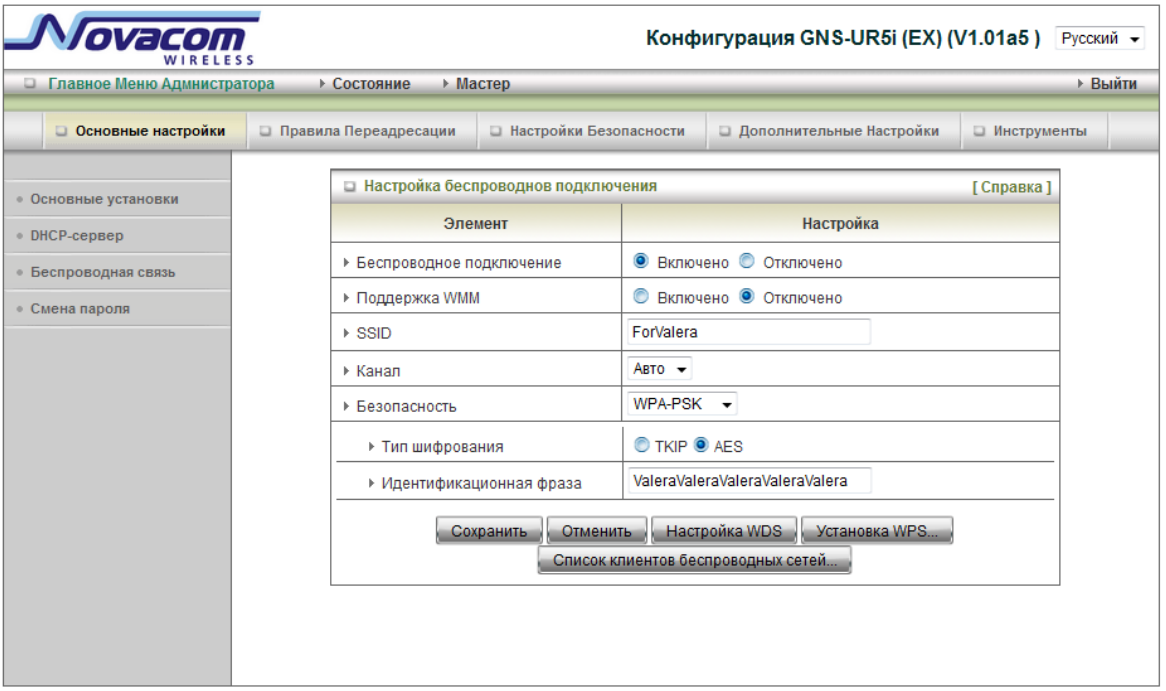
Нажмите **«More>>»,**

1. **DHCP Сервер:** Выберите **Выключен** или **Включен**
2. **Срок действия договора:** Срок действия договора DHCP для DHCP клиента
3. **Пул начальных/финальных IP адресов:** Когда бы ни поступил запрос, сервер DHCP автоматически выделит неиспользуемый IP адрес из адресного пула для запрашивающего компьютера. Вы должны определить начальный/финальный адреса для пула IP адресов.
4. **Имя домена:** Опционально. Информация будет передана клиенту.
5. **Первичный/Вторичный DNS:** Опционально, Эта функция позволяет Вам назначать DNS Сервера.
6. **Первичный/Вторичный WINS:** Опционально, Эта функция позволяет Вам назначать WINS Сервера
7. **Шлюз:** Опционально. Адресом шлюза будет IP адрес альтернативного шлюза. Эта функция позволит Вам назначить другой шлюз когда DHCP сервер определит IP Вашего компьютера.
8. **Фиксированное местоположение:** Обратитесь к странице «Контроль MAC адреса".

После окончания заполнения

Нажмите **"Сохранить"** чтобы сохранить изменения или "**Изменить"** чтобы вернуться к первоначальным настройкам.

3.2.1.4 Настройки беспроводного соединения.



Беспроводные настройки позволяют Вам сконфигурировать беспроводное соединение

1. **Беспроводной доступ:** По умолчанию включен**.** Выбор этой опции позволит Вам настроить WAP.
2. **Восприятие WMM:** По умолчанию отключен**.** Сервис WMM® представляет собой набор функций для Wi-Fi сети, улучшение качества обслуживания пользователей для аудио-, видео-и голосовых приложений за счет приоритизации трафика данных
3. **SSID:** Service Set Identifier (SSID) является именем, определяемым для определенной беспроводной локальной сети (WLAN). Фабричная установка по умолчанию SSID - «по умолчанию». SSID может быть легко изменен, чтобы установить новую беспроводную сеть. (Важно: названия SSID могут содержать до 32 знаков ASCII),
4. **Канал:** «Автоматически» является установкой по умолчанию. Устройства, подключенные к сети должны делить один канал. (Важно: Беспроводные адаптеры автоматически сканируют и приводят в соответствие друг другу беспроводные настройки. Вы также можете выбрать канал, который хотите использовать.)
5. **Безопасность:** Вы можете выбрать какой тип защиты использовать: Никакой, WEP, 802.1X, WPA-PSK, WPA, WPA2PSK, WPA2.

   Никакой:
   Параметры Wi-Fi защиты не устанавливаются для устройства.

WEP:
Когда Вы выбираете защиту 128 или 64-битным WEP ключом, пожалуйста, выберите единственный WEP ключ и введите 26 или 10 шестнадцатеричных (0, 1, 2…8, 9, A, B…F) знаков

802.1X

Флажок используется для переключения функции 802.1X. При включенной функции 802.1X, пользователь беспроводной сети должен сначала авторизовать данному маршрутизатору право использования услуг сотовой сети.

1. RADIUS Server IP: IP-адрес или доменное имя 802.1X сервера.
2. RADIUS Port: По умолчанию используется порт 1812.
3. RADIUS Shared Key: значение ключа разделяется RADIUS-сервером и этим маршрутизатором. Это ключевое значение согласуется с ключевым значением в RADIUS сервере.

WPA-PSK

1. Выберите тип шифрования, TKIP или AES
2. Пароль: Длина предварительного ключа от 8 до 63 .
3. Введите ключ, например 12345678

WPA

Флажок используется для переключения функции WPA. Если включена функция WPA,
пользователь беспроводной сети должен сначала авторизовать данному маршрутизатору право использования услуг сотовой сети, RADIUS-сервера.
1. IP-адрес или доменное имя 802.1X сервера.
2. Выберите тип шифрования и ключ в RADIUS -IP сервера / Порт / Общий ключ.
3. Значение ключа разделяется RADIUS-сервером и этим маршрутизатором. Это ключевое значение согласуется с ключевым значением на RADIUS сервере.

WPA2-PSK

1. Выберите тип шифрования, TKIP или AES.
2. Пароль: Длина предварительного ключа от 8 до 63.
3. Введите ключ, например 12345678.

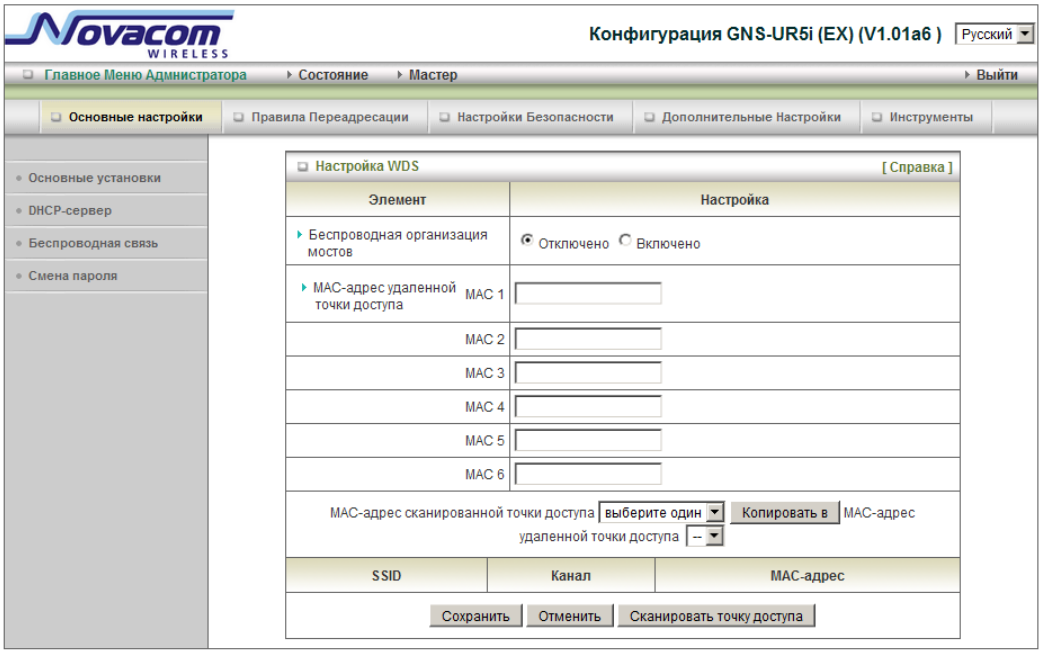
WPA2

Флажок используется для переключения функции WPA2. Если включена функция WPA2,
пользователь беспроводной сети должен сначала авторизовать данному маршрутизатору право использования услуг сотовой сети, RADIUS-сервера.
1. IP-адрес или доменное имя 802.1X сервера.
2. Выберите тип шифрования и ключ в RADIUS -IP сервера / Порт / Общий

ключ.
3. Значение ключа разделяется RADIUS-сервером и этим маршрутизатором. Это ключевое значение согласуется с ключевым значением в RADIUS сервере.

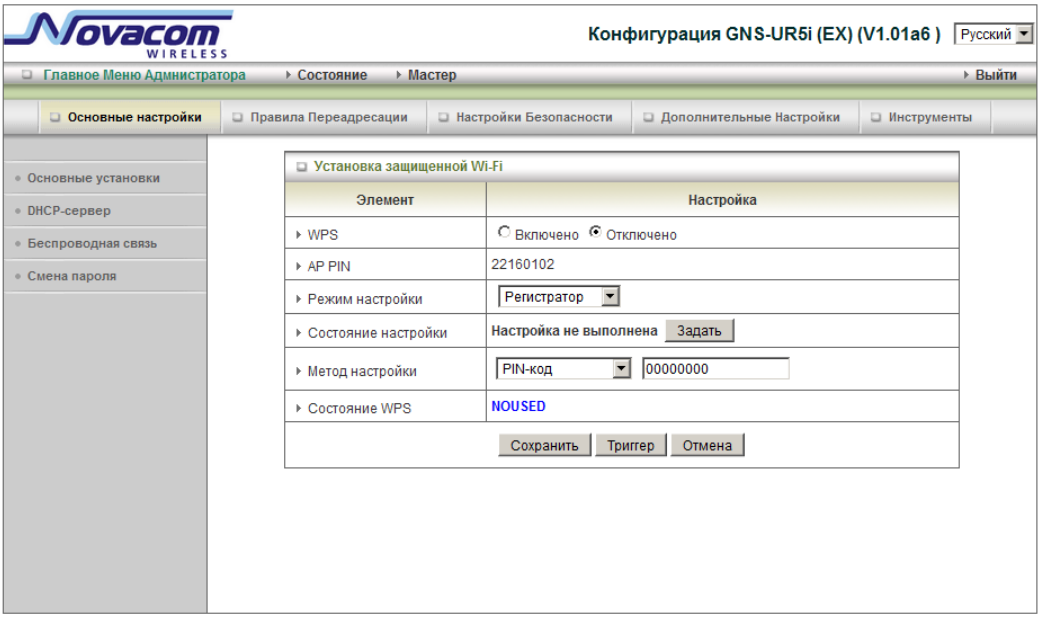
Настройка WDS (Беспроводной системы распределения)

Согласно стандартам IEEE802.11 операция WDS становится доступной. Используя WDS возможно установить беспроводное соединение с точками доступа и таким образом расширить проводную инфраструктуру до тех областей, где использование кабеля невозможно или неэффективно.



WPS(Установка защиты соединения Wi-Fi)

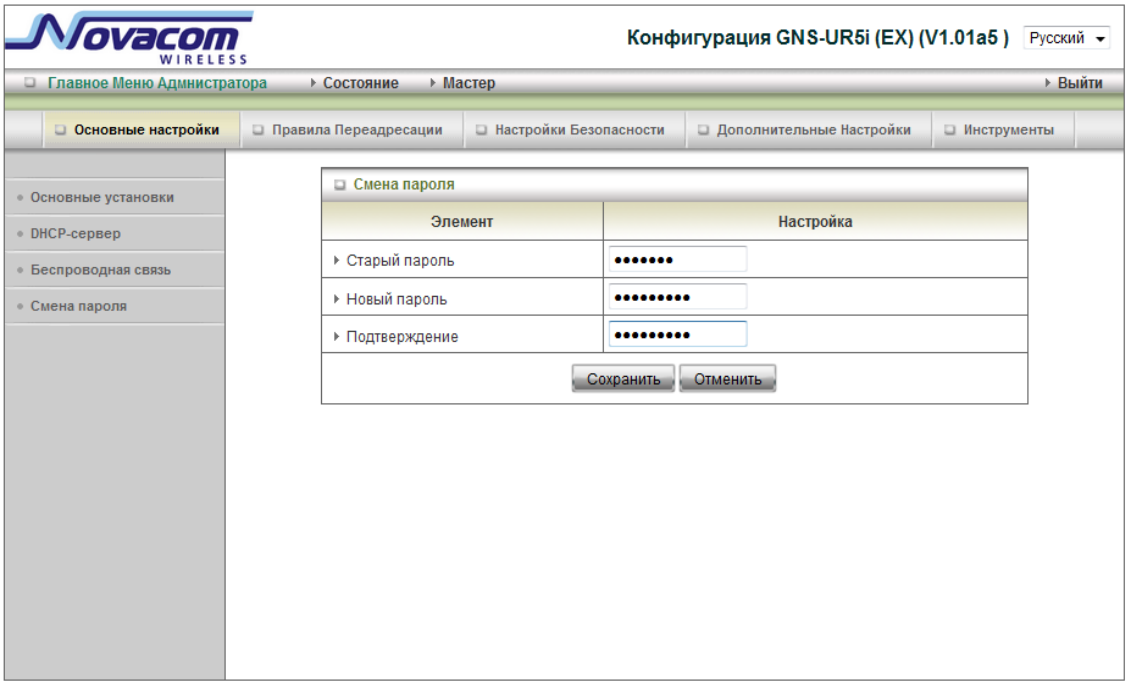
WPS расшифровывается как «Настройки защиты Wi-Fi», что значит то же самое что WCN-NET и обеспечивает безопасность беспроводного соединения.



Список клиентов беспроводного соединения

Здесь указываются все клиенты беспроводного соединения.

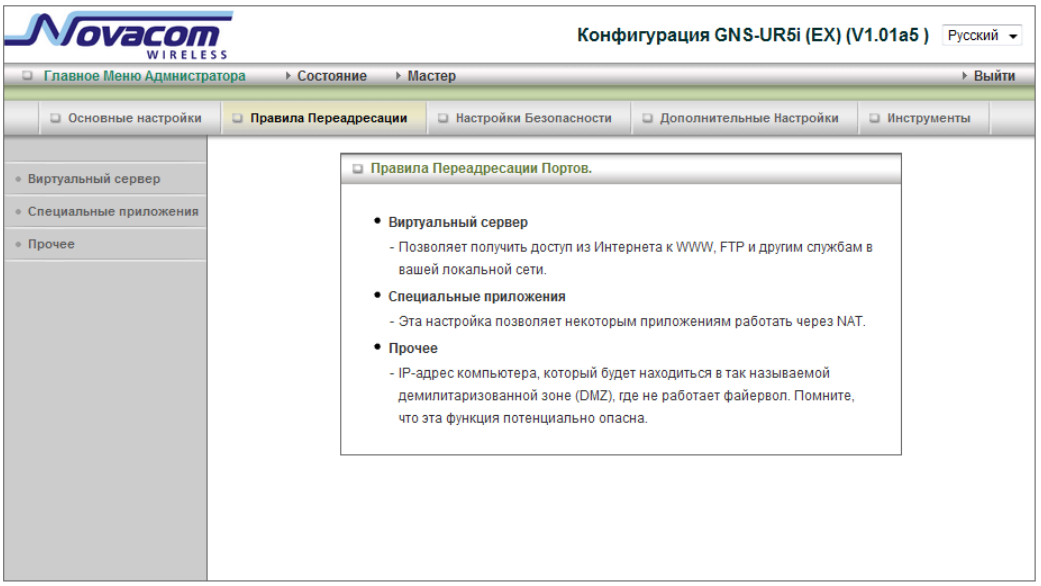
3.2.1.5 Смена пароля



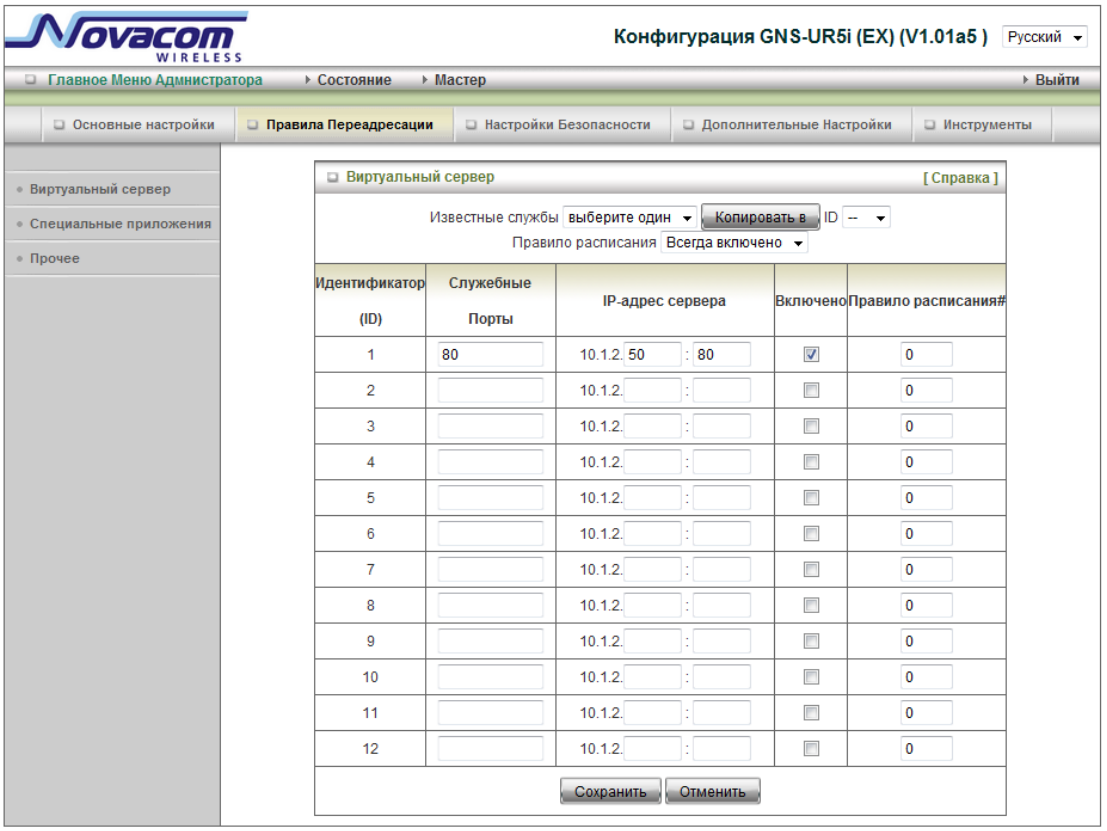
Здесь Вы можете изменить пароль. Мы **настоятельно** рекомендуем Вамсменить системный пароль из соображений безопасности.

Нажмите “Сохранить” чтобы сохранить изменения или “Изменить” чтобы вернуться к первоначальным настройкам.

3.2.2 Правила переадресации



3.2.2.1 Виртуальный сервер



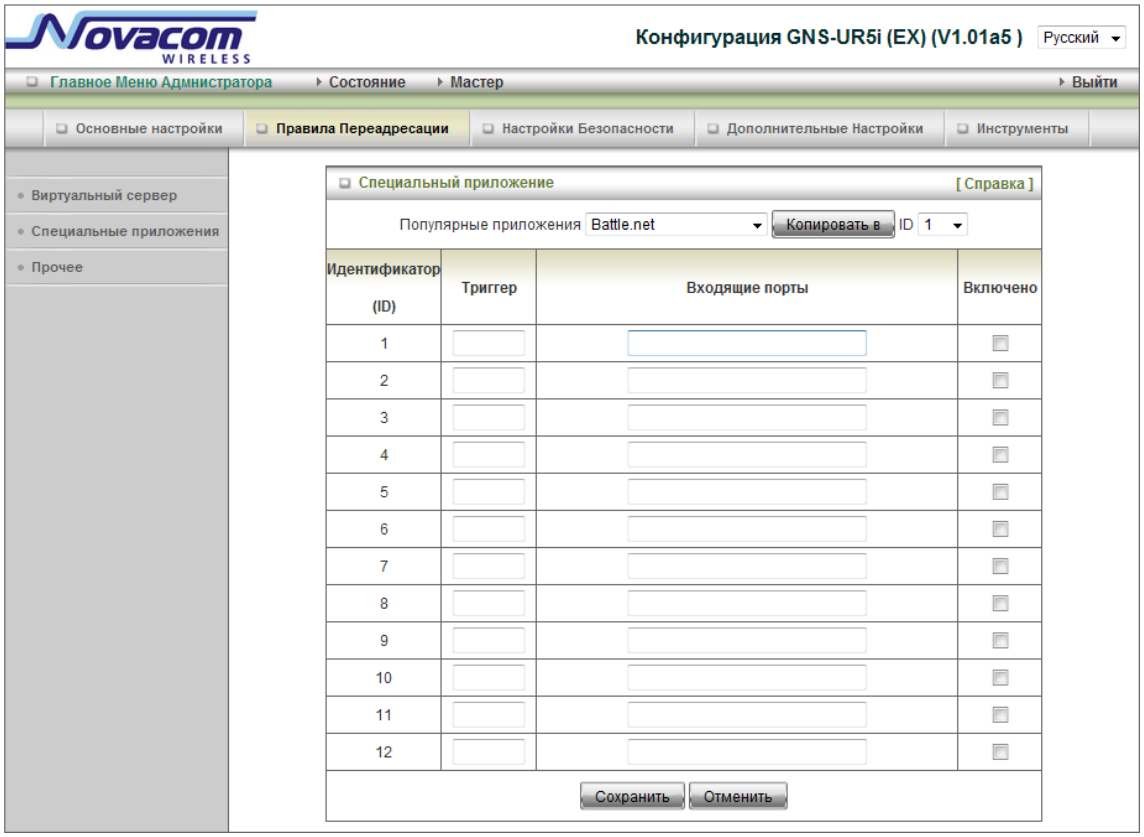
Сервис NAT firewall данного оборудования отфильтровывает неопознанные пакеты для защиты Вашей сети, поэтому все хосты, защищенные этим сервисом, остаются невидимыми для внешнего мира. При желании, Вы можете сделать некоторые из них доступными, задействуя маршрутизацию Виртуального Сервера.
Виртуальный сервер определяется как Служебный порт и все запросы на этот порт переадресовываются на компьютер, определяемый через IP адрес сервера. Virtual Server может работать по графику, и давать пользователю большую гибкость в контроле доступа. Для более полной информации обратитесь к разделу «График».

Например, если у Вас есть FTP сервер (порт 21) на 192.168.123.1, веб-сервер (порт 80) на 192.168.123.2, и VPN сервер на 192.168.123.6, Вам нужно заполнить следующую таблицу маршрутизации виртуального сервера:

Service Port	Server IP	Enable
21	192.168.123.1	V
80	192.168.123.2	V
1723	192.168.123.6	V

Нажмите **«Сохранить»,** чтобы сохранить изменения или **«Изменить»,** чтобы вернуться к первоначальным настройкам.

3.2.2.2 Специальные приложения



Некоторые приложения требуют несколько соединений, например, Интернет-игры, видеоконференции, интернет-телефония и т.д. Из-за функции firewall, эти приложения не могут работать с NAT роутера напрямую. Функция «Особые приложения» позволяет некоторым из этих приложений работать с данным оборудованием. Если данная функция не поможет настроить работу приложения, попытайтесь настроить свой компьютер как DMZ хост.

1. **Триггер:** количество исходящих портов, необходимых приложению.
2. **Входящие порты**: когда триггерный пакет определен, входящие пакеты, отправленные на определенные номера портов, могут пройти через защиту firewall.

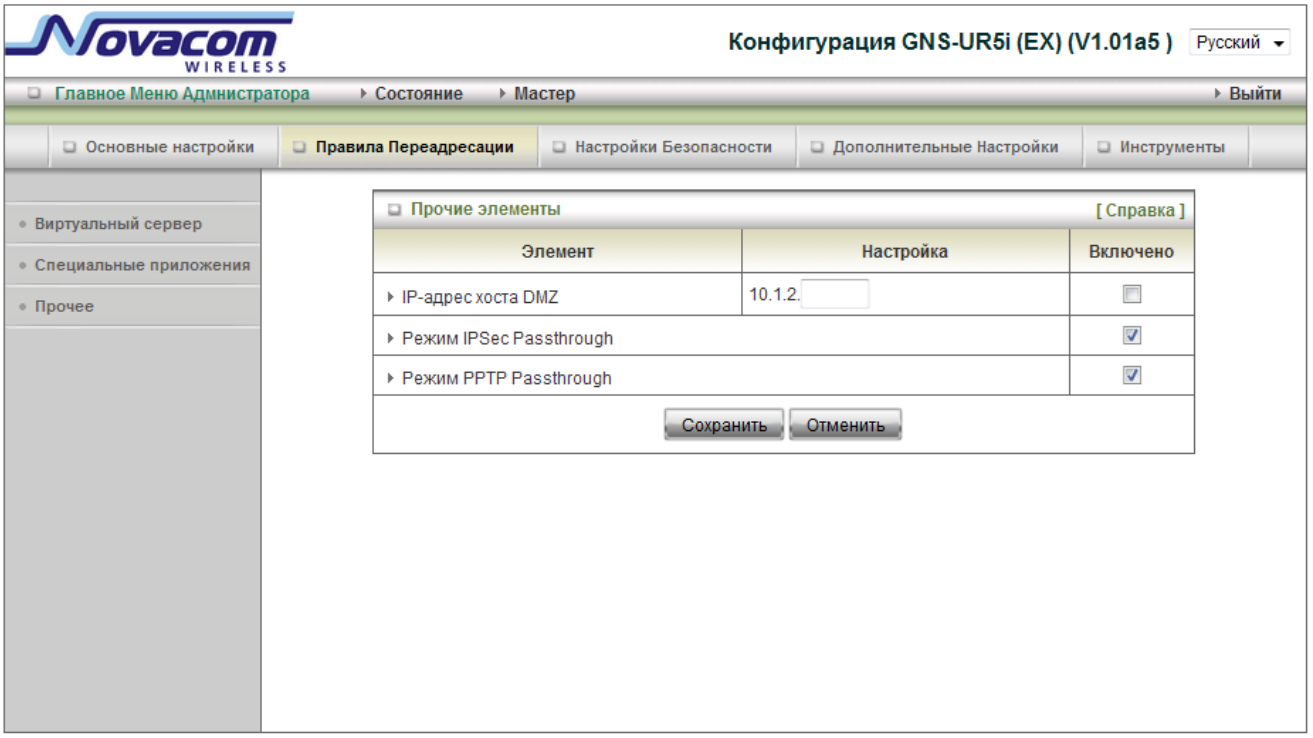
Некоторые настройки на данном оборудовании уже заданы.

1. Выберите приложение и
2. Нажмите «**Скопировать в»**, чтобы добавить настройки данного приложения в Ваш список.

Важно! В любой момент времени, коридор «Специальных приложений» может использоваться только одним компьютером.

Нажмите «Сохранить», чтобы сохранить изменения или «Изменить», чтобы вернуться к первоначальным настройкам.

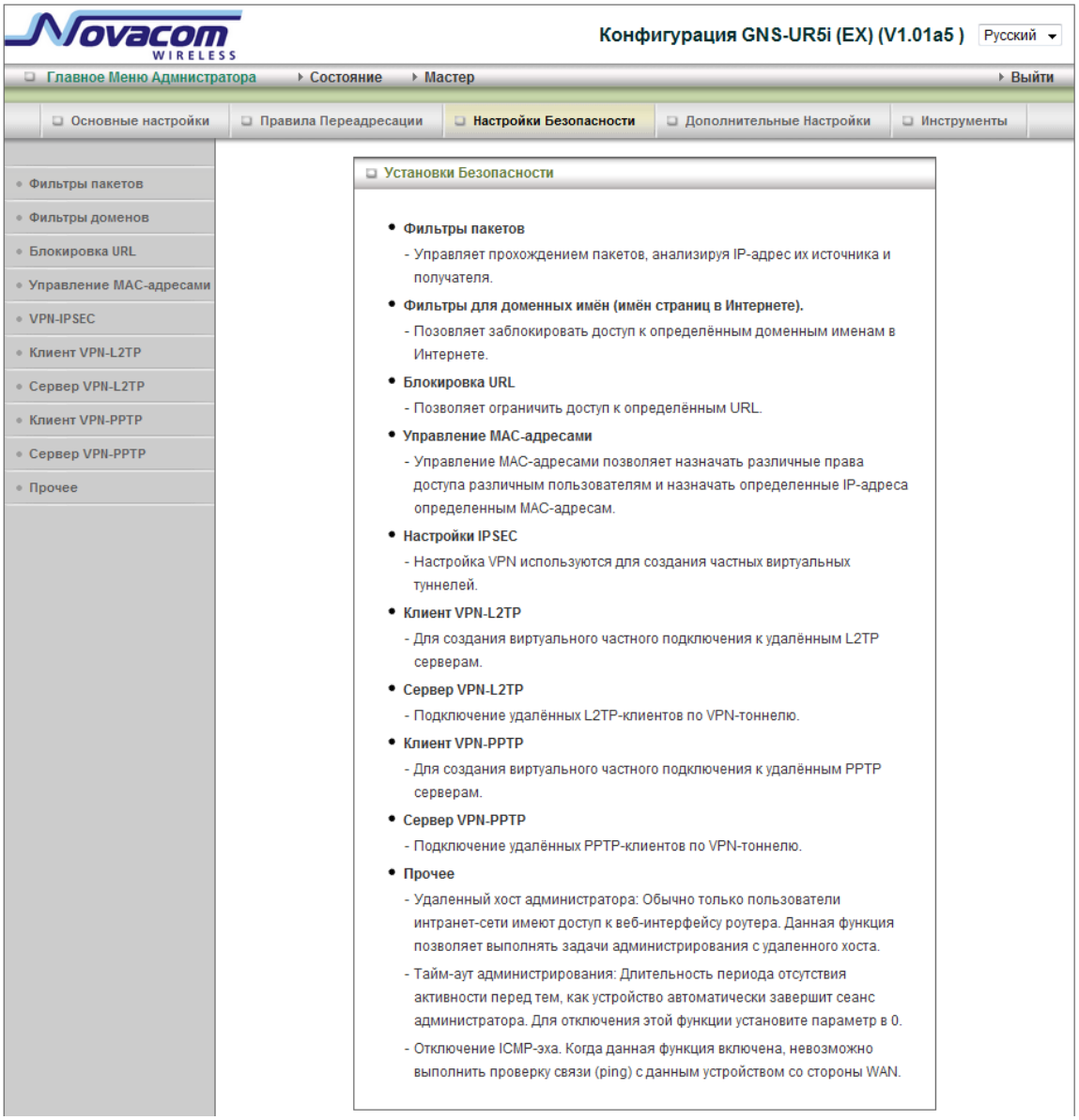
3.2.2.3 Прочее



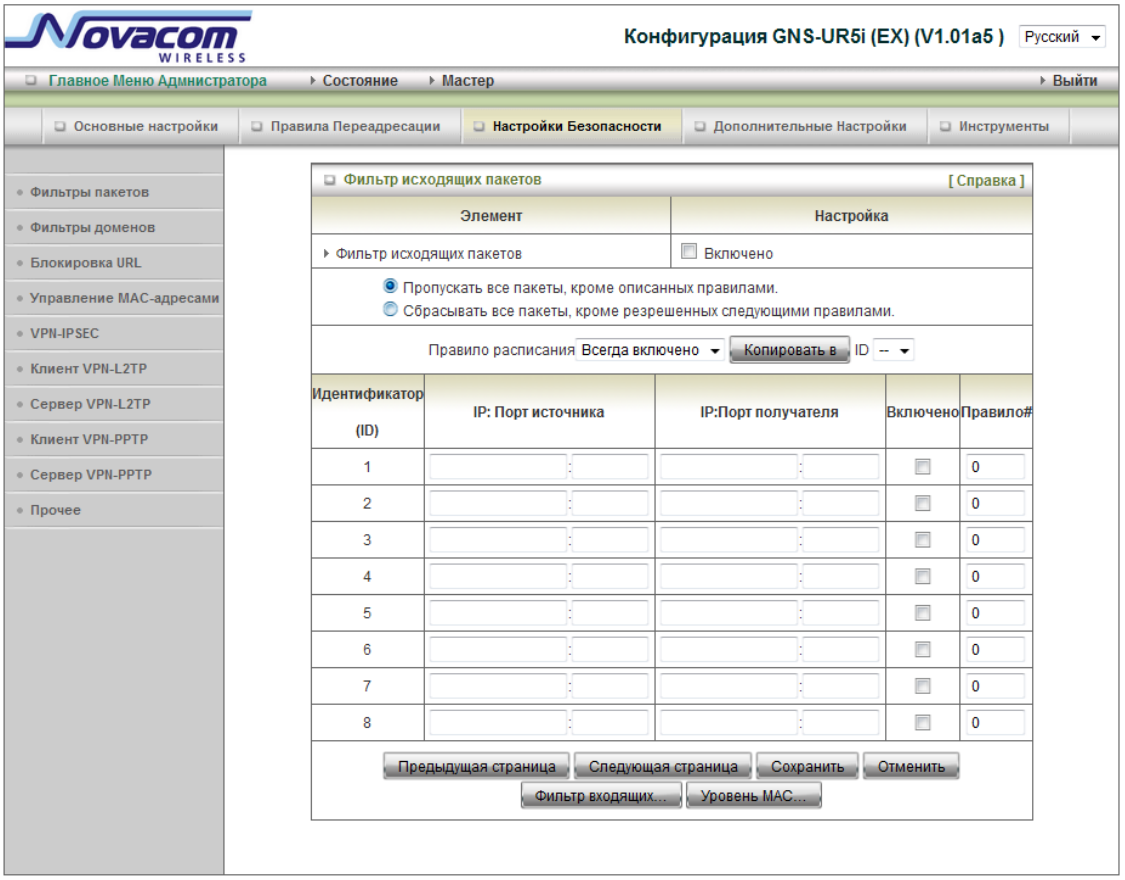
1. **IP адрес DMZ хоста**
   Хост DMZ (Демилитаризированная зона) это хост без защиты firewall. Он позволяет компьютеру устанавливать неограниченную 2-стороннюю связь для интернет-игр, видеоконференций, интернет-телефонии и других специальных приложений
2. **Коридор IPSec / PPTP**
   Устройство также поддерживает коридор IPSec / PPTP. Когда включен коридор VPN, несколько соединений VPN может быть установлено через устройство. Это полезно, когда у вас много клиентов VPN в локальной сети

Нажмите «Сохранить», чтобы сохранить изменения или «Изменить», чтобы вернуться к первоначальным настройкам.

3.2.3 Настройки безопасности



3.2.3.1 Фильтрация пакетов



Пакетный фильтр включает в себя фильтр исходящих и входящих пакетов. Они настраиваются одинаково.
Пакетный фильтр позволяет вам контролировать пакеты, пропускаемые роутером. Исходящий фильтр распространяется на все исходящие пакеты. Тем не менее, входящий фильтр распространяется только на пакеты, предназначенные для виртуальных серверов или DMZ хоста. Вы можете выбрать одну из двух политик фильтрации:

1. Пропускать все, соответствующие указанным правилам
2. Отклонять все, кроме соответствующих указанным правилам

Вы можете определить 8 правил для каждого направления: входящего и исходящего. Для каждого правила Вы можете установить следующее:

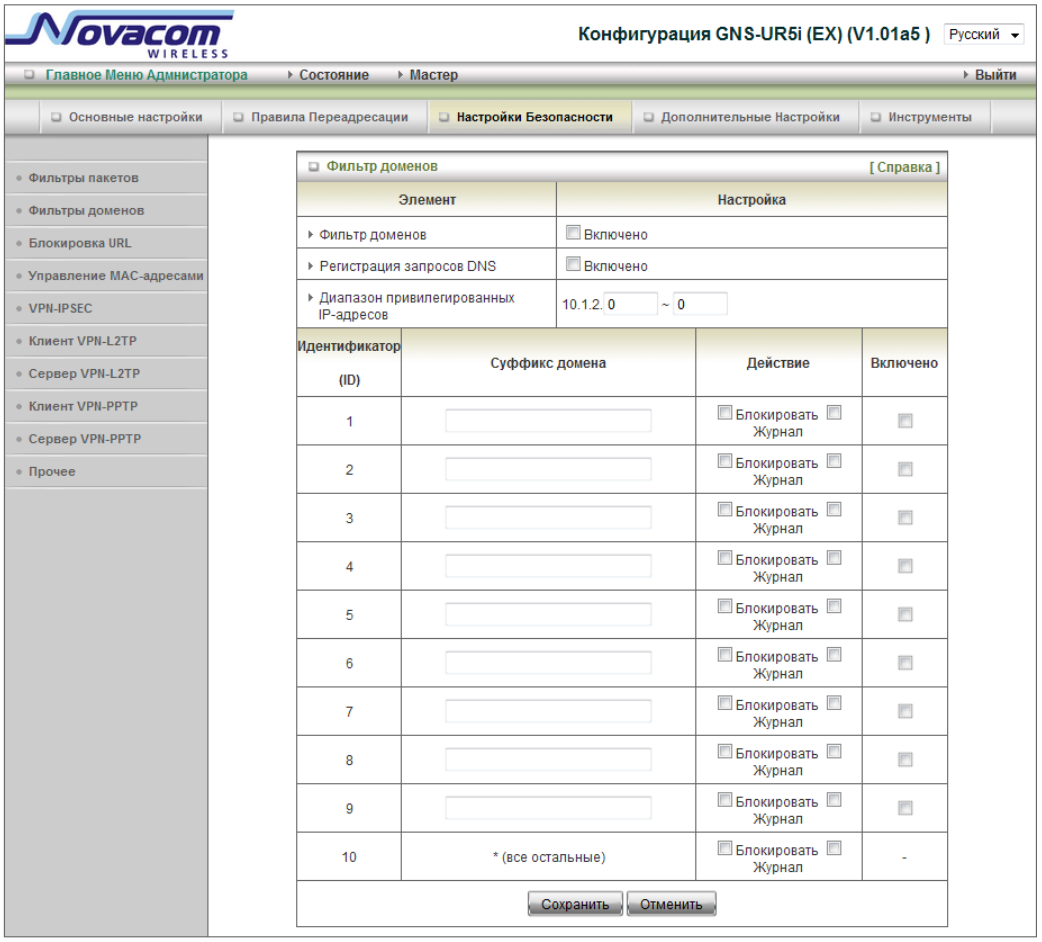
- Исходный IP-адрес
- исходный порт
- IP адрес назначения
- Порт назначения
- Протокол TCP или UDP или оба
- Использование правила #

Для исходного IP адреса или адреса назначения, Вы можете определить единственный IP адрес (4.3.2.1) или ряд IP адресов (4.3.2.1-4.3.2.254). Пустое значение подразумевает все IP адреса.
Для исходного порта или порта назначения, Вы можете определить единственный порт (80) или ряд портов (1000-1999). Добавьте префикс "T" или "U" для определения TCP или UDP протокола. Например, T80, U53, U2000-2999, Отсутствие префикса подразумевает включение обоих протоколов (TCP и UDP) are defined. Пустое значение подразумевает все адреса портов. Пакетный фильтр может работать по графику и дает пользователю большую гибкость контроля доступа. Для получения более подробной информации обратитесь к разделу «График».

Каждое из правил может быть включено и отключено по отдельности.

Нажмите «Сохранить», чтобы сохранить изменения или «Изменить», чтобы вернуться к первоначальным настройкам.

3.2.3.2 Фильтр доменов



Позволяет запретить пользователям данного устройства получить доступ к конкретным URL.

1. **Фильтр доменов включен.**

   Поставьте флажок, если Вы хотите включить фильтр.

2. **Регистрация DNS запросов**

   Отметьте, если Вы хотите отслеживать когда кто-то получает доступ к конкретным URL.

3. **Список привилегированных IP адресов**

   Настройте группу хостов и наделите эту группу полномочиями устанавливать соединение с сетью без ограничений.

4. **Доменный суффикс**

   Суффикс адреса URL может быть запрещен, например, ".com", "xxx.com".

5. **Действия**

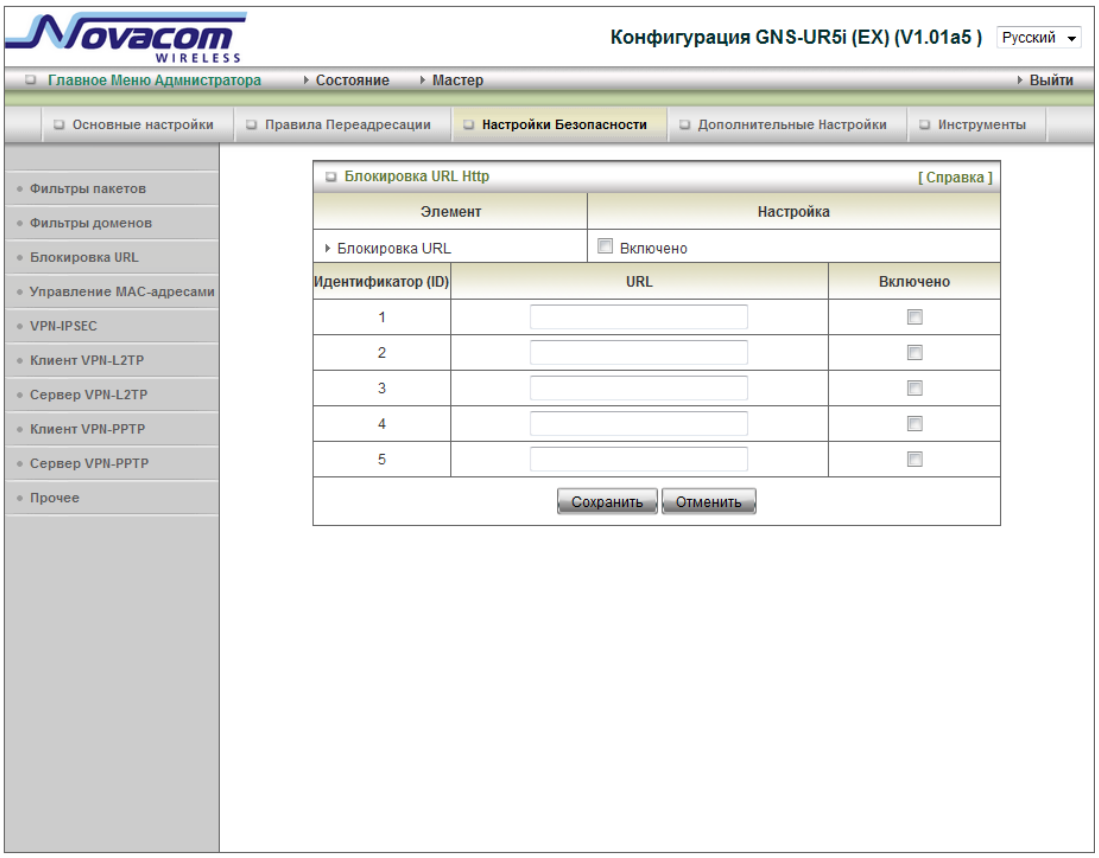
   Когда кто-либо получает доступ к адресу URL, где встречается запрещенный доменный суффикс — какое действие должна произвести система? Отметьте «прекратить», если Вы хотите блокировать доступ. Отметьте «зарегистрировать», если Вы хотите зарегистрировать этот доступ.

6. **Включить**

   Отметьте включение для каждого правила.

Нажмите «Сохранить», чтобы сохранить изменения или «Изменить», чтобы вернуться к первоначальным настройкам.

3.2.3.3 Блокирование URL



Блокирование URL будет блокировать компьютерам локальной сети доступ к определенным сайтам. Главное различие между «Фильтром доменов» и «Блокированием URL» является то, что фильтр доменов требует, чтобы пользователь ввел суффикс (как.com или.org, и т. д.), в то время как Блокирование URL требует, чтобы пользователь ввел только ключевое слово. Другими словами, фильтр доменов может заблокировать определенный вебсайт, в то время как Блокирование URL может заблокировать сотни вебсайтов с данным ключевым словом.

1. **Блокирование URL включено**

   Отметьте, если хотите включить блокирование URL.

2. **URL**

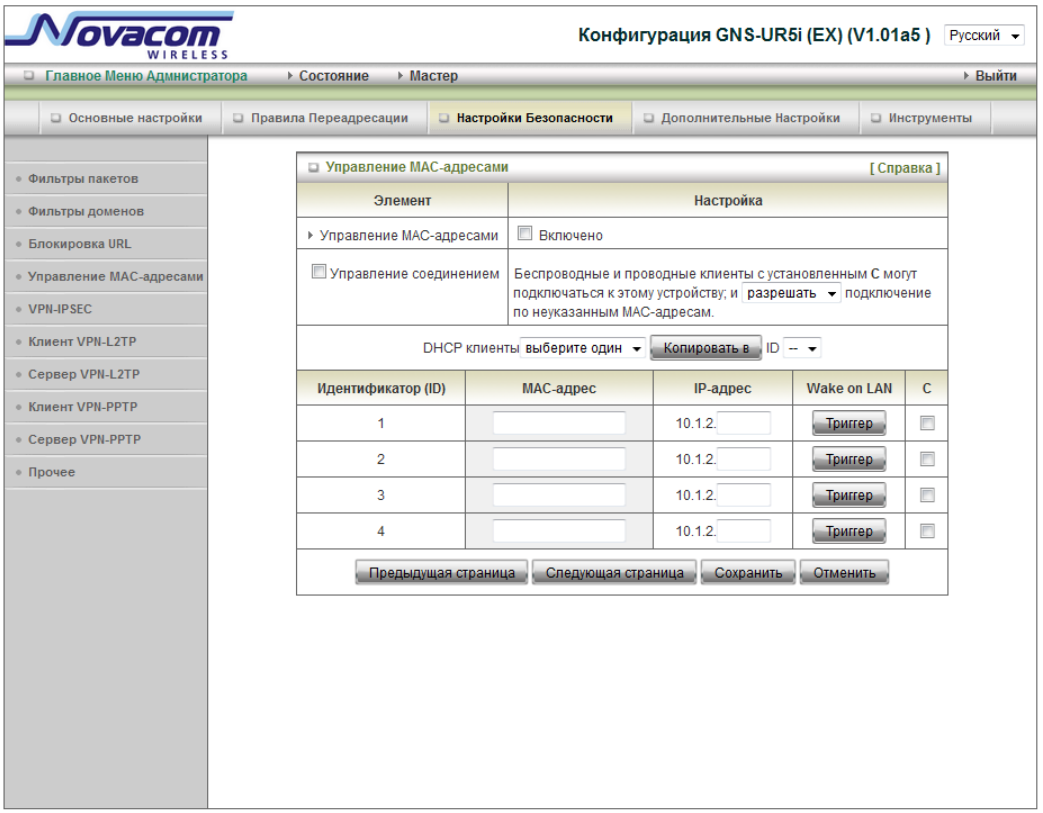
   Если какая-нибудь часть URL Вебсайта будет соответствовать ключевому слову, то связь будет заблокирована.
   Например, Вы можете использовать ключевое слово «секс», чтобы заблокировать все вебсайты, если их URL содержат ключевое слово «секс»

3. **Включить**

   Отметьте включение для каждого правила.

Нажмите «Сохранить», чтобы сохранить изменения или «Изменить», чтобы вернуться к первоначальным настройкам.

3.2.3.4 Управление MAC адресами



Контроль MAC-адресов позволяет назначить различные права доступа для разных пользователей и назначить конкретное значение IP-адреса для определенного адреса MAC.

1. **Контроль MAC адресов**

   Отметьте «Включить» для включения контроля MAC адресов. Все настройки на данной странице войдут в силу только если отмечено «Включить».

2. **Контроль соединения**

   Отметьте «Контроль соединения» для включения контроля проводного и беспроводного доступа к устройству. Если клиенту отказано в подключении к устройству, это означает, что ему также откзано в доступе в Интернет. Выберите «разрешить» или «отказать» для разрешения или отказа в доступе клиентам, чьи MAC адреса не входят в «Контрольную таблицу» (см.ниже).

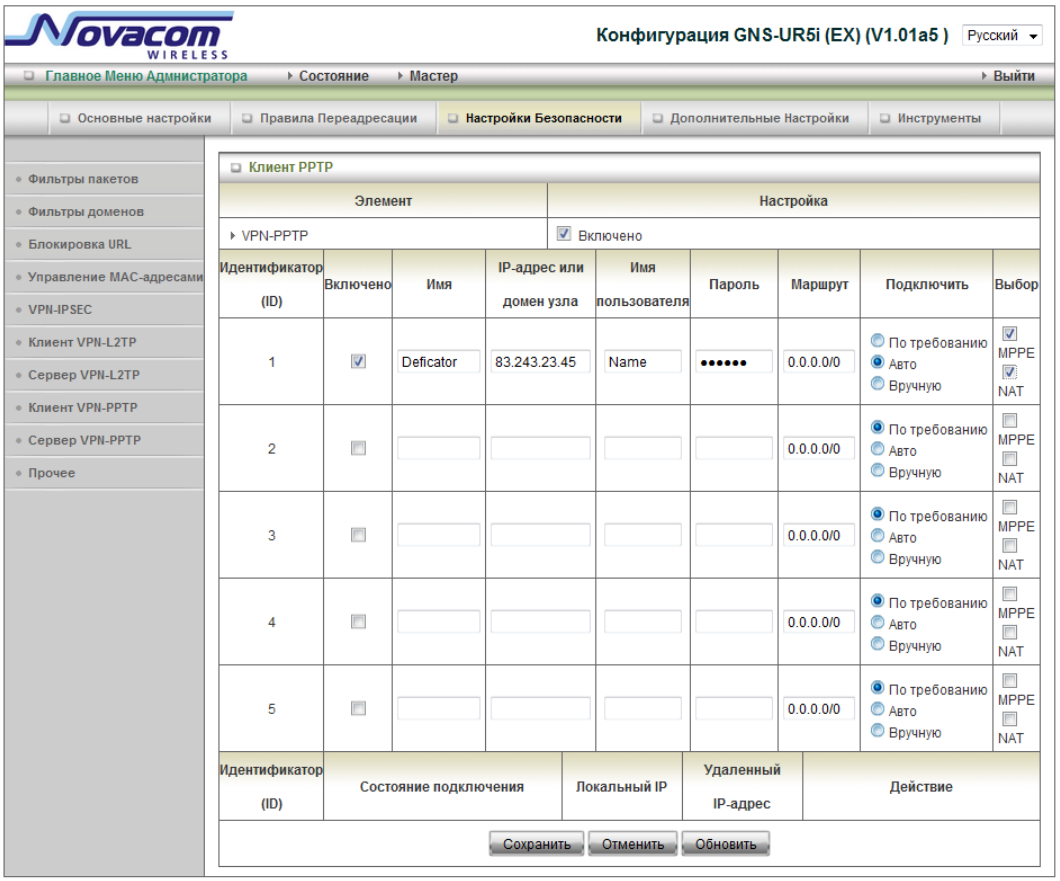
3. **Контроль подключения**

   Отметьте «Контроль подключения» для включения контроля за беспроводным подключением клиента к беспроводной локальной сети. Если клиенту отказано в подключении к беспроводной локальной сети, это означает, что клиент не может посылать или получать данные через это устройство. Выберите «разрешить» или «отказать» для разрешения или отказа в подключении к беспроводной сети

клиентам, чьи MAC адреса не входят в «Контрольную таблицу».

Нажмите «Сохранить», чтобы сохранить изменения или «Изменить», чтобы вернуться к первоначальным настройкам.
Нажмите «Следующая страница», чтобы перейти ниже по списку или «Предыдущая страница» для возврата к предыдущей странице.

3.2.3.5 VPN-PPTP клиент



1. **VPN-PPTP:** Включает или выключает PPTP клиент.
2. **Включить:** Отметьте включение для каждого правила..
3. **Название:** название пункта.
4. **Основной IP/Домен:** IP/Домен PPTP сервера
5. **PPTP учетная запись и пароль:** учетная запись и пароль, назначенные Вам Вашим провайдером. Если Вы не хотите менять пароль, оставьте поле пустым.
6. **Маршрут:** какое соединение будет использовать PPTP?
7. **Соединение**: Существует 3 режима:

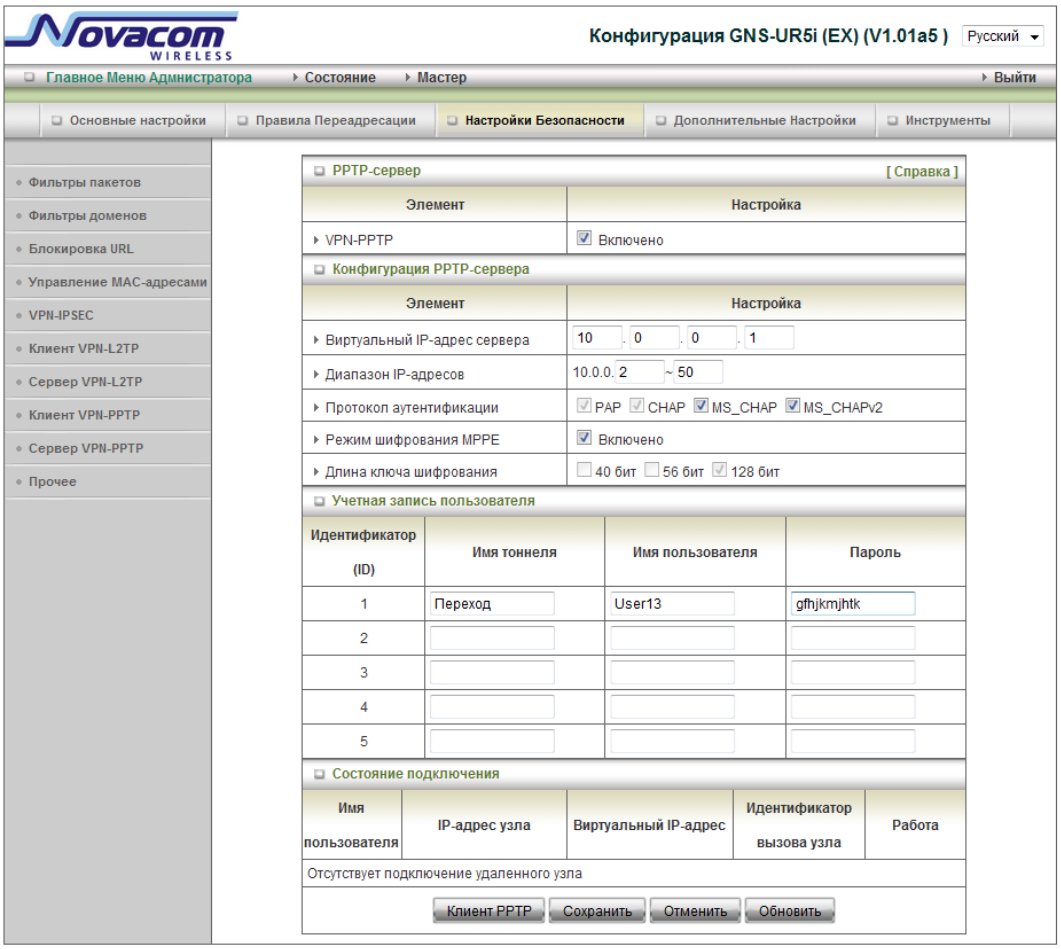
   По запросу: Устройство будет связываться с провайдером при отправлении клиентами исходящих пакетов.

   Автоматически: Устройство будет связываться с провайдером, пока соединение не будет установлено.

Вручную: Устройство не будет устанавливать соединения, пока не будет нажата клавиша соединения на странице статуса.

Нажмите «Сохранить», чтобы сохранить изменения или «Изменить», чтобы вернуться к первоначальным настройкам.

3.2.3.6 Сервер VPN-PPTP

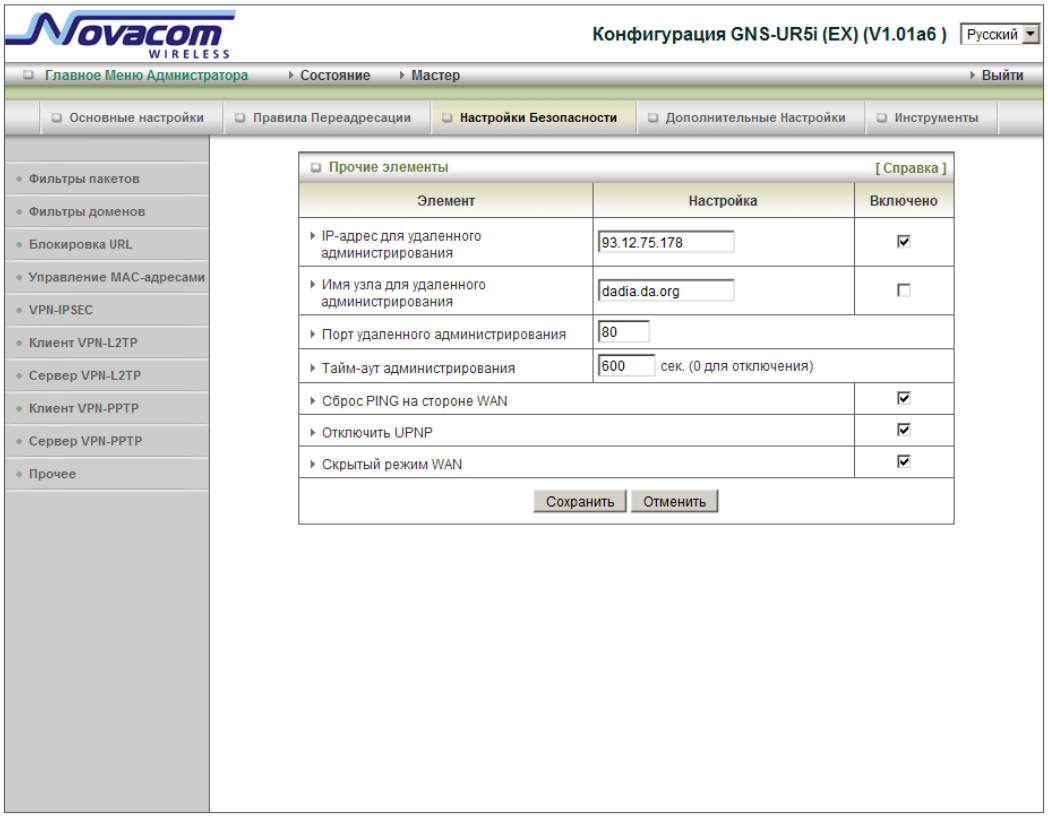


1. **VPN-PPTP:** Включает или выключает PPTP сервер.
2. **Виртуальный IP адрес сервера:** IP адрес сервера PPTP.
3. **Ряд IP адресов:** Ряд IP адресов клиентов. IP адреса этого ряда присваиваются клиентам, устанавливающим соединение.
4. **Протокол идентификации:** Можно выбрать из следующих протоколов: PAP, CHAP MS_CHAP и MS_CHAPv2.
5. **Режим шифрования MPPE:** Включает или выключает MPPE шифрование.
6. **Длина шифровального кода:** Можно выбрать из следующих режимов: 40bits, 56bits и 128bits.
7. **Имя коридора:** Опционально
8. **Имя пользователя\пароль:** Имя пользователя и пароль, используемые для регистрации на PPTP сервере, задаются

здесь. Общее количество пар: 5.

Нажмите «Сохранить», чтобы сохранить изменения или «Изменить», чтобы вернуться к первоначальным настройкам.

3.2.3.7 Прочее



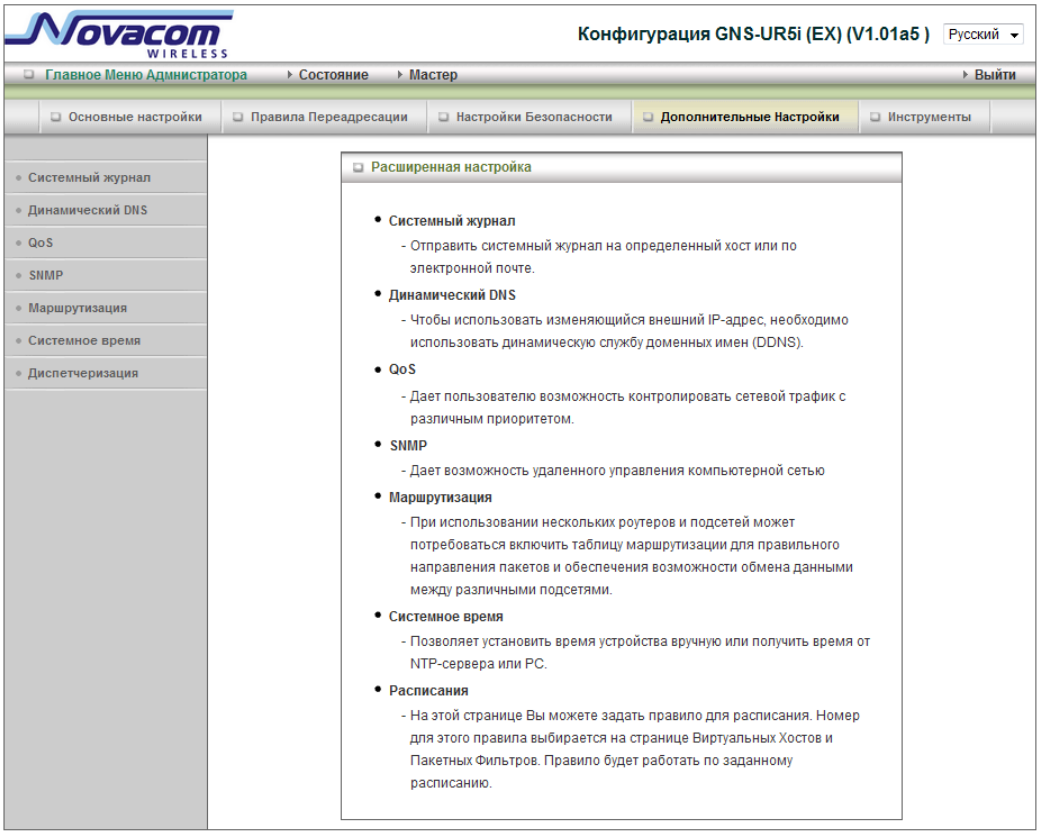
1. **Удаленное администрирование IP/Хоста/Порта**
   Обычно, только пользователь внутренней сети может просматривать встроенные веб-страницы и выполнять функции администратора.
   Эта функция позволяет Вам выполнять функции администратора с удаленного хоста. Если эта функция включена, удаленное администрирование может осуществляться только в определенного IP адреса. Если указанный IP адрес 0.0.0.0, любой хост может установить соединение с данным оборудованием и выполнить администрирование. Вы можете использовать маску подсети "/nn" для обозначения определенной группы доверенных IP адресов. Например, "10.1.2.0/24". Важно!: Когда включена функция Удаленного администрирования, порт веб сервера перемещается на 88. Вы также можете изменить порт веб-сервера на другой.
2. **Автоматическое выключение**
   Время неактивности до автоматического разлогинивания, вы можете установить это значение на 0, чтобы отключить эту функцию.
3. **Отказ запросам со стороны WAN**

Когда включена эта функция, ни один хост WAN не может послать запрос шлюзу.

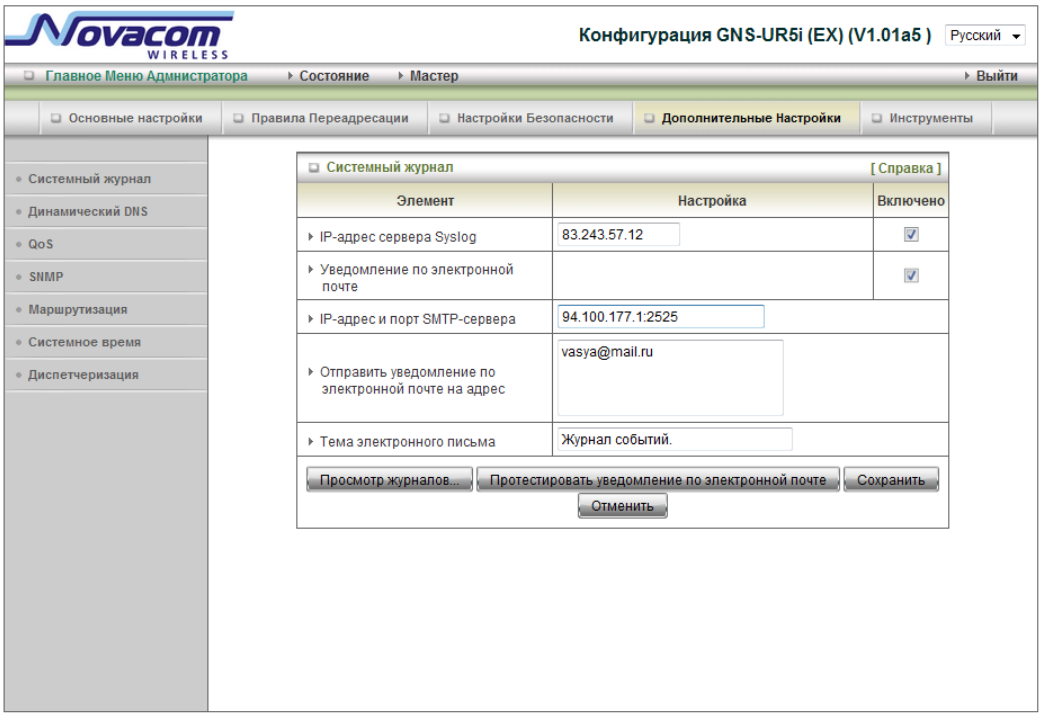
4. **Отключить UPNP**
   Устройство может отключить функцию UPNP. Если Ваша операционная система поддерживает функцию UPNP, поищите ее и она подключится, например в Windows XP. Вы можете получить IP устройства через UPNP.
5. **Держать WAN в скрытом режиме**
   Если порт закрыт, устройство игнорирует входящие попытки соединения, а не отклоняет их.

Нажмите «Сохранить», чтобы сохранить изменения или «Изменить», чтобы вернуться к первоначальным настройкам.

3.2.4 Дополнительные настройки.



3.2.4.1 Системный журнал



Эта страница поддерживает два метода передачи системных логов для определенных целей: с помощью протокола syslog (UDP) и SMTP(TCP). Вам нужно настроить следующее:

1. **IP адрес для протокола Syslog**

   IP пункта назначения, куда будет отправляться syslog.

   Отметьте «Включить», чтобы включить эту функцию.

2. **Включить извещения E-mail**

   Отметьте, если Вы хотите включить Email оповещения (пересылка syslog по электронной почте).

3. **IP и порт SMTP сервера**

   Введите IP адрес и порт SMTсервера через двоеточие ':'. Если Вы не указываете номер порта, по умолчанию его значение будет 25. Например, "mail.your_url.com" или "192.168.1.100:26".

4. **Посылать извещения E-mail на адрес**

   Адресаты, которые будут получать эти логи. Вы можете указатьа больше одногоадресата, разделив адреса точкой с запятой или запятой.

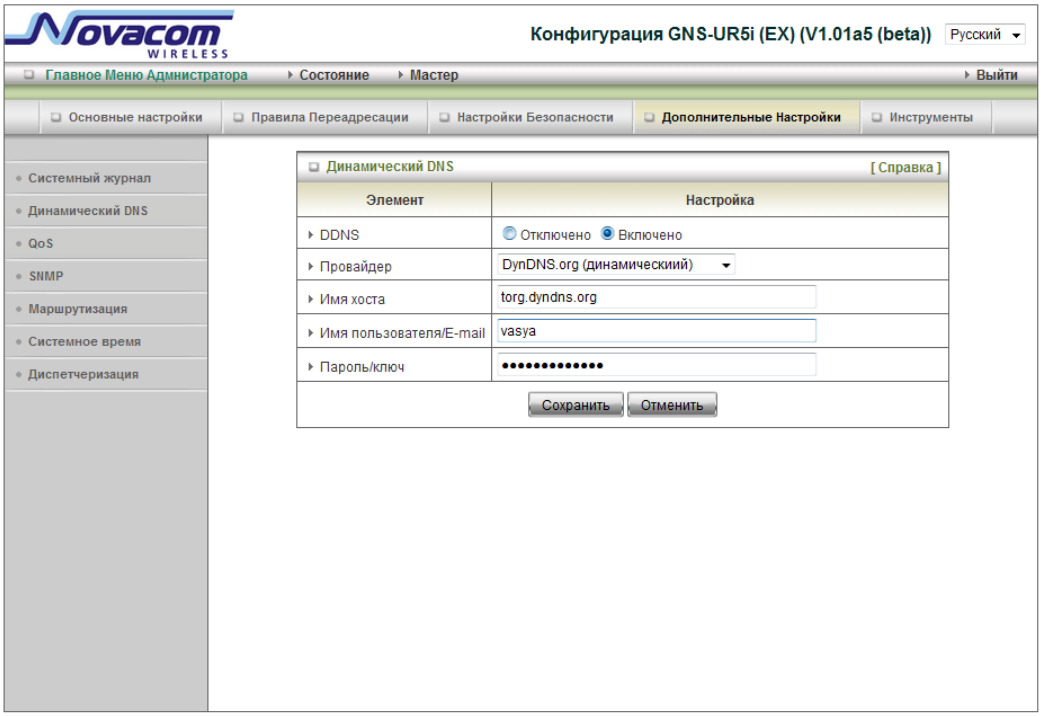
5. **Тема E-mail**

   Тема извещения. Эта настройка опциональна.

Нажмите «Сохранить», чтобы сохранить изменения или «Изменить», чтобы

вернуться к первоначальным настройкам.

3.2.4.2 Динамический DNS



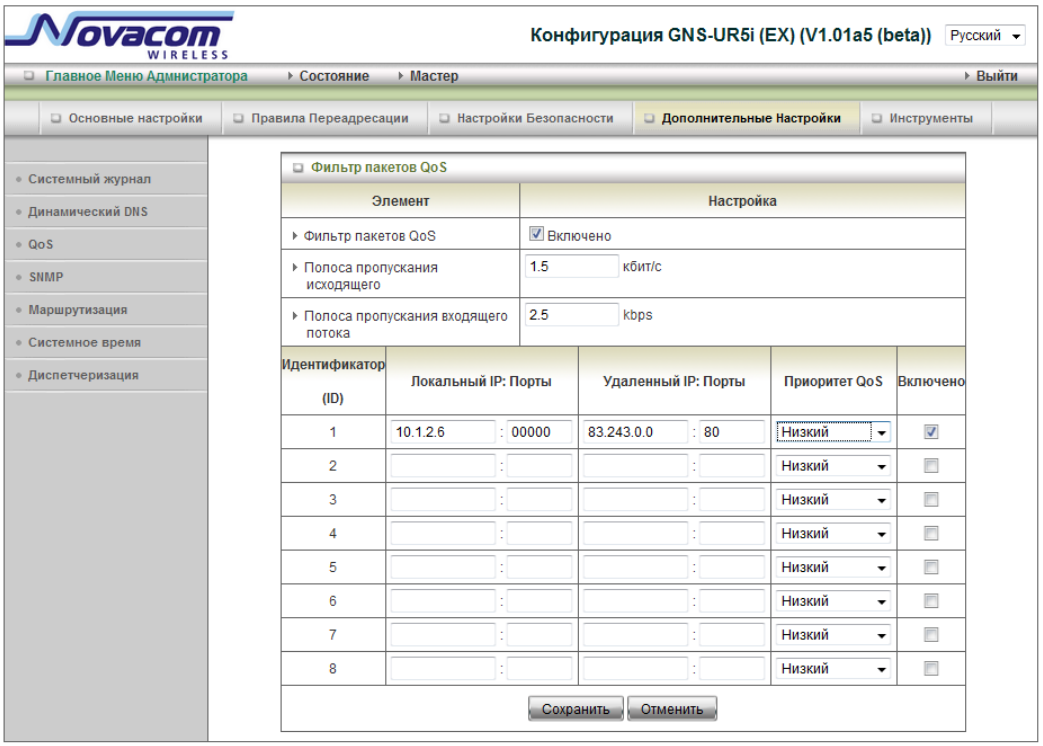
Для использования динамического IP адреса вашего сервера, Вам необходимо подключить динамическое обслуживание доменного имени (DDNS). Таким образом, каждому, желающему подключиться к Вашему хосту необходимо просто знать его имя. Динамический DNS будет связывать имя хоста с Вашим текущим IP адресом, который меняется каждый раз, когда Вы подключаетесь к Интернету через Вашего провайдера.
Перед включением динамического DNS, Вам необходимо зарегистрировать аккаунт на одном из DDNS серверов, список которых указан в поле «Провайдер».
Чтобы включить динамический DNS поставьте флажок «Включить» в поле DDNS. Дальше Вы можете ввести необходимую информацию о Вашем сервере DDNS.

Вам нужно указать:
Провайдера
Имя хоста
Имя пользователя/E-mail
Пароль/Ключ

Эту информацию Вы получите после регистрации аккаунта на DDNS сервере.

Нажмите «Сохранить», чтобы сохранить изменения или «Изменить», чтобы вернуться к первоначальным настройкам.

3.2.4.3 QOS (Качество обслуживания)



Обеспечивает различные приоритеты для различных пользователей или потоков данных, либо гарантирует определенный уровень производительности.

1. **Фильтр пакетов QoS**

   Этот пункт включает функцию QoS.

2. **Исходящий поток**

   Устанавливает ограничение скорости исходящего потока.

3. **Входящий поток**

   Устанавливает ограничение скорости входящего потока.

4. **Локальный IP**

   Установите здесь значение локального IP адреса.

5. **Локальные порты**

   Установите здесь значение локальных портов.

6. **УдаленныйIP**

   Установите здесь значение удаленного IP адреса.

7. **Удаленные порты**

Установите здесь значение удаленных портов.

8. **Приоритеты QoS**

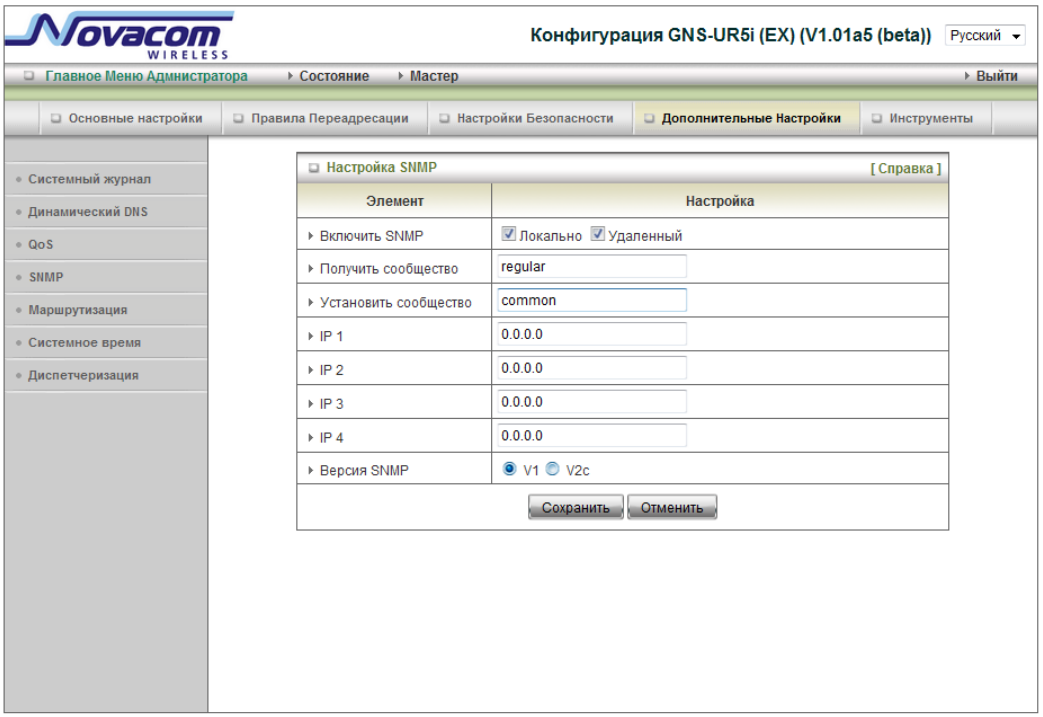
Это определяет уровень приоритета текущей политики конфигурации. Пакеты, связанные с этой политикой, будут обслуживаться на основании уровня приоритета. Для важных приложений рекомендуются Высокие или Нормальные уровни. Для необязательных приложений выберите Низкий уровень.

1. **Включить**

Отметьте включение для каждого правила.

Нажмите «Сохранить», чтобы сохранить изменения или «Изменить», чтобы вернуться к первоначальным настройкам.

3.2.4.4 SNMP



SNMP, Простой Протокол Управления Сетью, является протоколом, разработанным, чтобы дать пользователю способность утдаленно управлять компьютерной сетью, выбирая и устанавливая предельные значения и отслеживая действия в сети.

1. **Включить SNMP**

   Отметьте Локальный, Удаленный или оба, чтобы включить функцию SNMP. Если выбран Локальный, устройство будет отсечать на запросы из локальной сети (LAN).Если выбран Удаленный, устройство будет отсечать на запросы из глобальной сети (WAN).

2. **Группа запросов**

   Определение группы запросов GetRequest на которые устройство будет отвечать

3. **Группа установок**

Определение группы установок SetRequest которые устройство будет принимать.

IP 1, IP 2, IP 3, IP 4

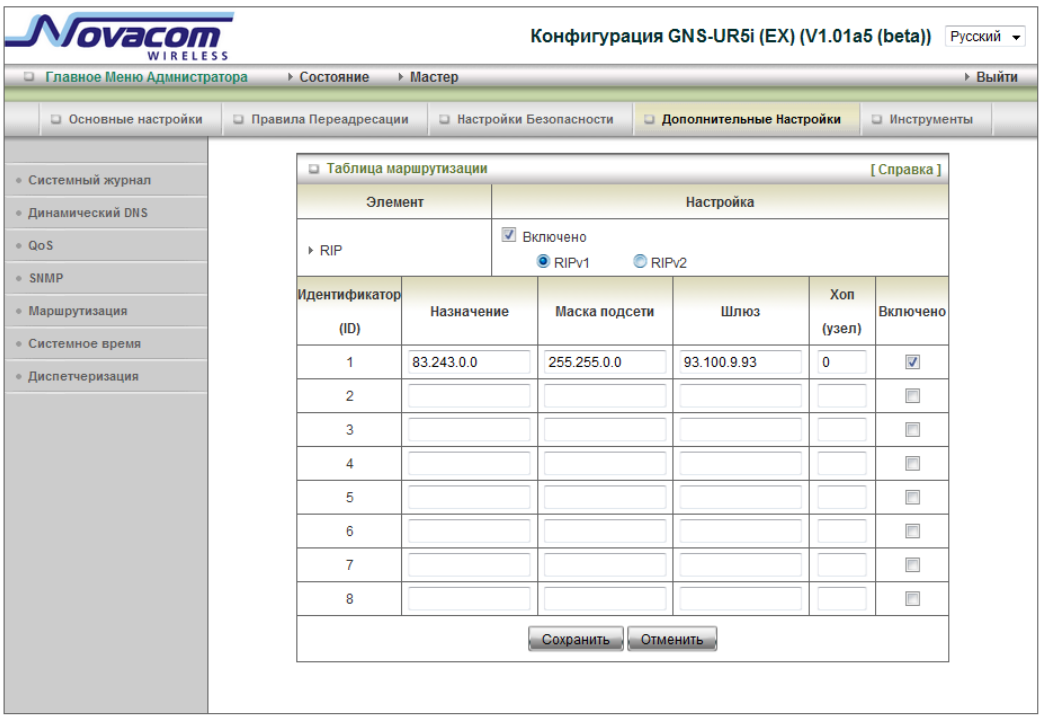
Введите здесь IP компьютеров, с которых будет осуществляться функция SNMP. Пользователь должен настроить путь, по которому устройство будет передавать SNMP сообщения.

4. **Версия SNMP**

   Пожалуйста, выберите ту версию SNMP, которую поддерживает Ваше программное обеспечение SNMP.

Нажмите «Сохранить», чтобы сохранить изменения или «Изменить», чтобы вернуться к первоначальным настройкам.

3.2.4.5 Маршрутизация



1. **Таблицы маршрутизации.**

Позволяет определить, какой физический адрес интерфейса будет использоваться для исходящих IP данных. Если у вас есть более чем один маршрутизатор и подсеть, вам необходимо включить таблицу маршрутизации, чтобы пакеты данных могли найти найти правильные пути маршрутизации и позволить различным подсетям взаимодействовать друг с другом

Настройки Таблицы маршрутизации используются для настройки функции статической и динамической маршрутизации

2. **Динамическая маршрутизация**

Информационный протокол маршрутизации (RIP) будет обмениваться информацией о назначении вычислительных маршрутов со всей сетью. Выберите RIPv2 если у Вас есть в сети альтернативная подсеть.

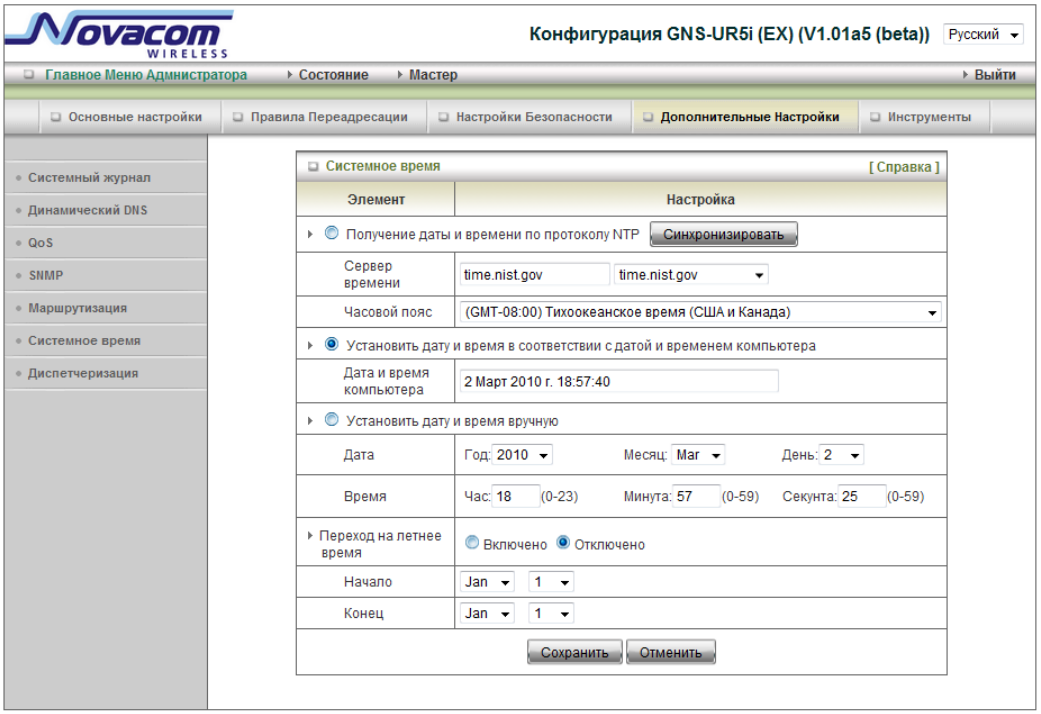
В противном случае выберите RIPv1, если Вам нужен этот протокол.

3. **Статическая маршрутизация**

Для статической маршрутизации, вы можете указать до 8 правил маршрутизации. Вы можете ввести IP-адрес назначения, маску подсети, шлюз, шаг для каждого правила маршрутизации, а затем включить или отключить правило, установив или сняв флажок Включить.

Нажмите «Сохранить», чтобы сохранить изменения или «Изменить», чтобы вернуться к первоначальным настройкам.

3.2.4.6 Системное время



1. **Установить дату и время с помощью NTP протокола**

Выберите, если Вы хотите установить дату и время с помощью NTP протокола

1. **Синхронизировать сейчас:**

   Синхронизировать системное время с сетевым сервером времени

2. **Сервер времени**

   Выберите сервер времени NTP чтобы сверяться со временем UTC (Всемирное Координированное Время)

3. **Часовой пояс**

   Выберите часовой пояс местонахождения устройства.

2. **Установка времени и даты с помощью настроек компьютера**

   Выберите, если хотите установить время и дату, установленные на компьютере.

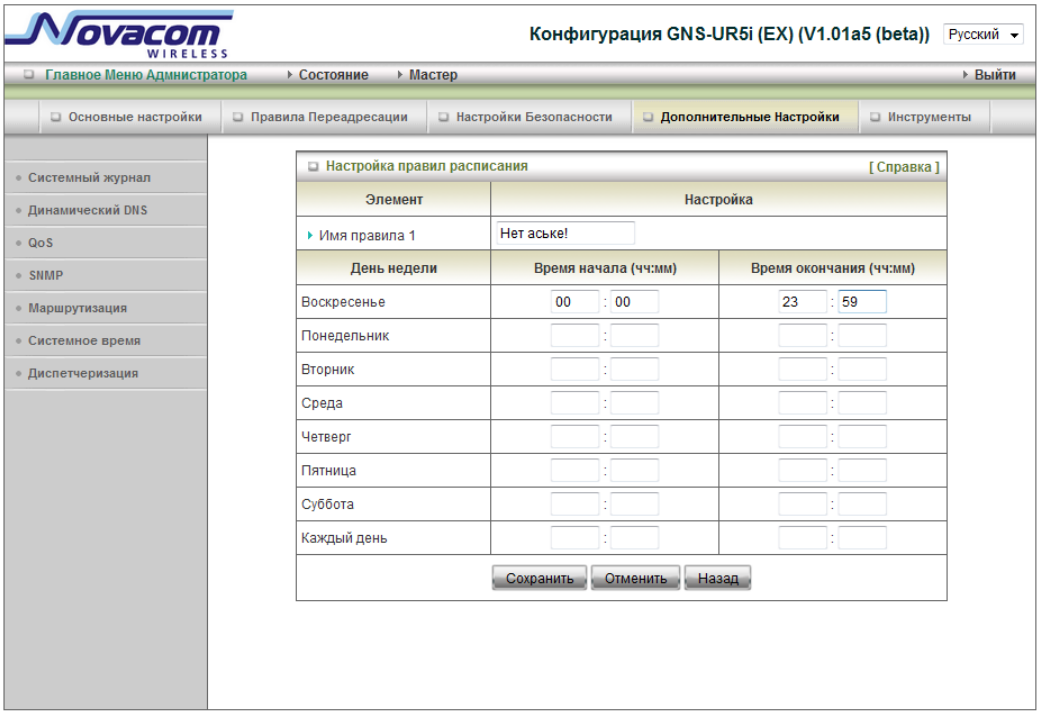
3. **Установка времени и даты вручную**

Выберите, если хотите установить время и дату вручную

4. **Летний период:** установите время летнего периода.

Нажмите «Сохранить», чтобы сохранить изменения или «Изменить», чтобы вернуться к первоначальным настройкам.

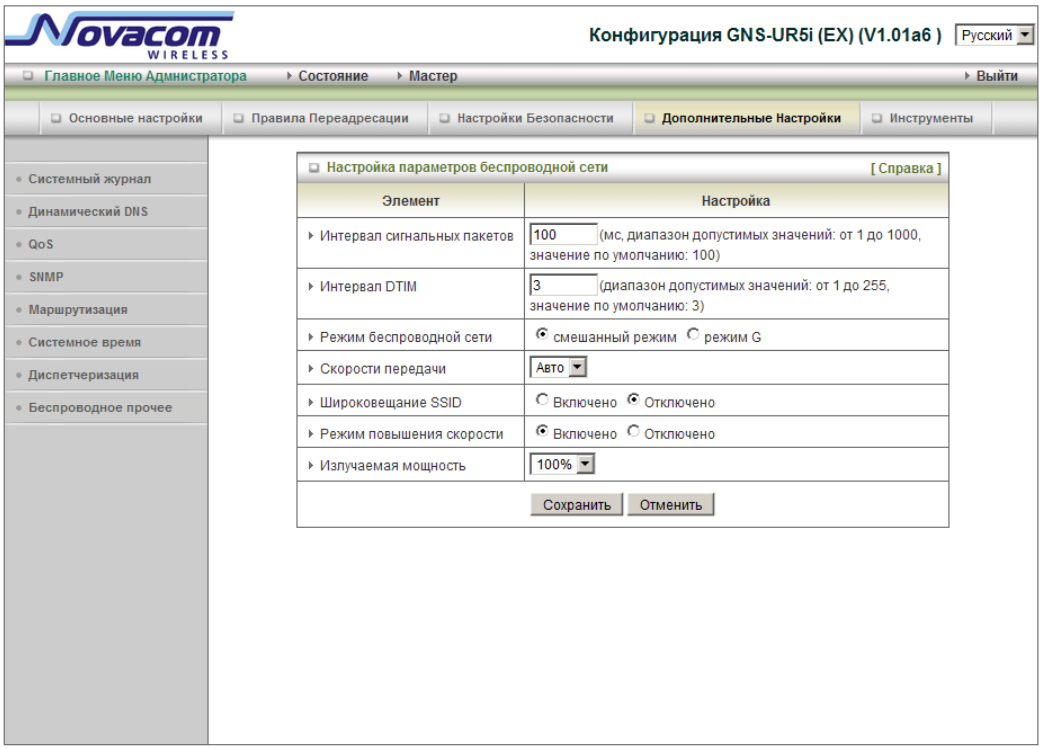
3.2.4.7 Диспетчеризация.



Вы можете установить график для автоматического включения/выключения разных функций.
Отметьте «Включить». Нажмите «Добавить новое правило». Здесь вы можете написать название правила и выбрать день и время начала и завершения его действия.
Например “ftp time” каждый день с 14:10 до 16:20

Нажмите «Сохранить», чтобы сохранить изменения

3.2.4.8 Настройки беспроводного сервиса



1. **Интервал маяка**

   Маяки — пакеты, отправляемые точкой доступа для синхронизации с сетью. Установите значение интервала маяка между 1 и 1000. По умолчанию установлено значение 100 милисекунд.

2. **Интервал DTIM**

   Введите значение от 1 до 65535 для Сообщений индикации входящего трафика (DTIM). DTIM это обратный отсчет, информирующий клиентов о следующем окне для прослушивания широковещательных и групповых сообщений. Когда точка доступа ретранслирует сообщения для подключенных клиентов, она посылает следующий DTIM со значением DTIM интервала. Клиенты точки доступа слышат маяки и включают прием широковещательных и групповых сообщений. По умолчанию значение интервала DTIM установлено 3

3. **Беспроводной режим**

   Выберите режим беспроводного соединения для беспроводного соединения

4. **Скорость передачи**

   Выберите основную скорость передачи, базирующуюся на скорости передачи беспроводных адаптеров WLAN (беспроводная локальная сеть).

5. **SSID вещание**

   Выберите, включить или выключить беспроводное SSID вещание. Выключая

трансляцию SSID, Вы делаете Вашу беспроводную сеть практически невидимой.

6. **Улучшенный режим скорости**

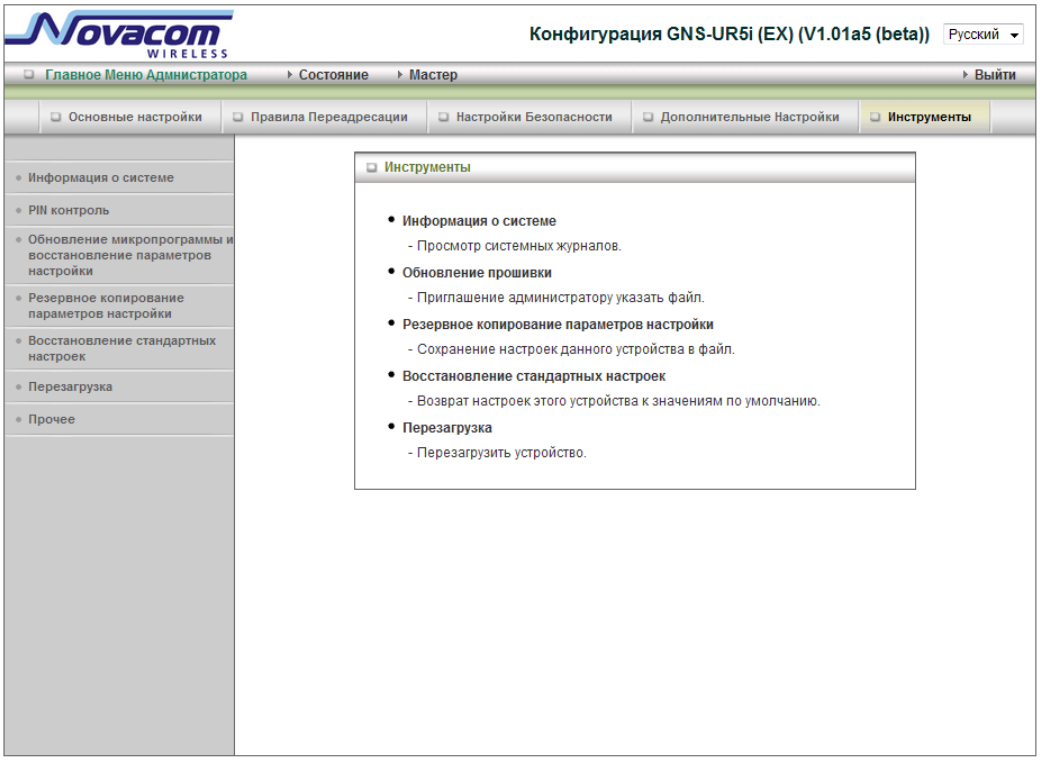
   Это функция разрыва передачи для беспроводных решений Ralink

7. **Мощность передачи антенны:**

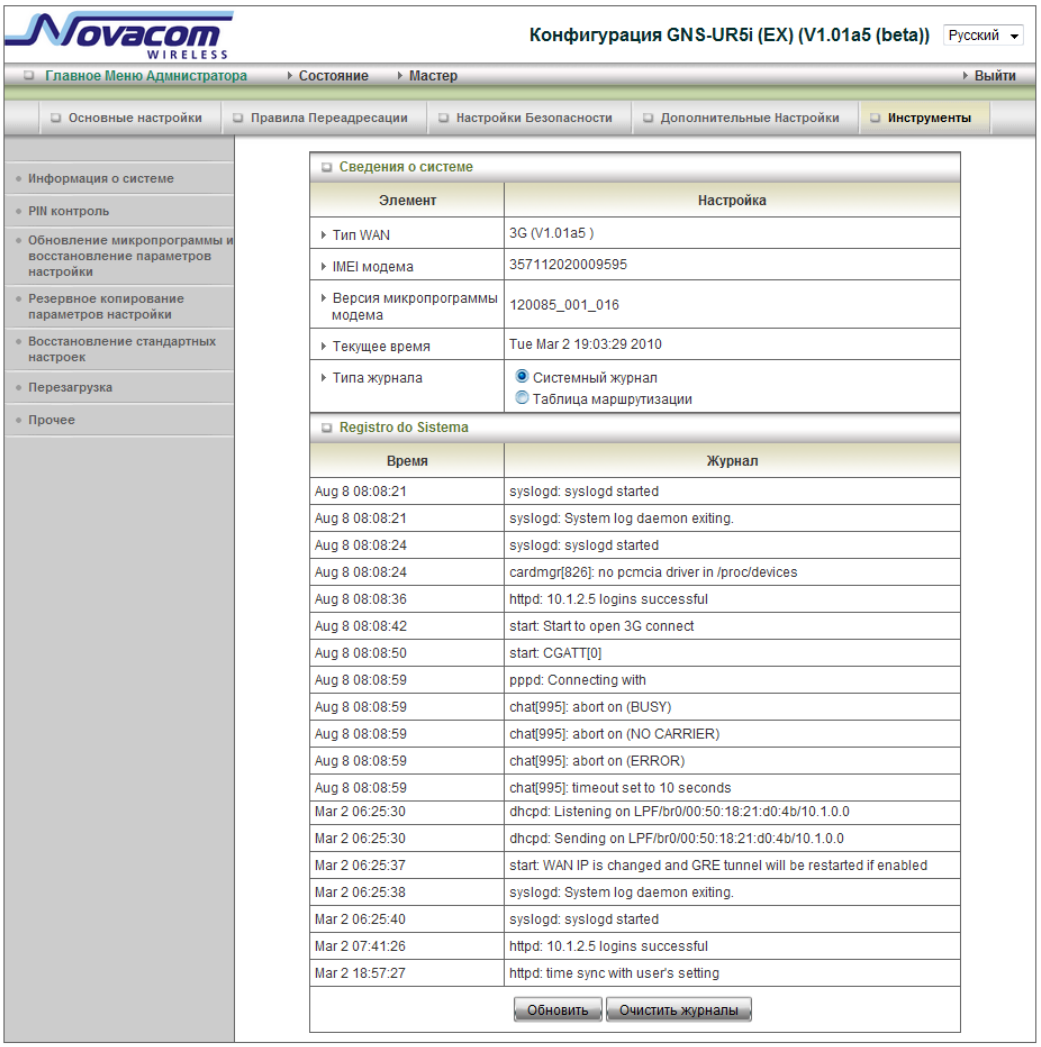
   Выберите мощность передачи антенны.

Нажмите «Сохранить», чтобы сохранить изменения или «Изменить», чтобы вернуться к первоначальным настройкам.

3.2.5 Инструменты

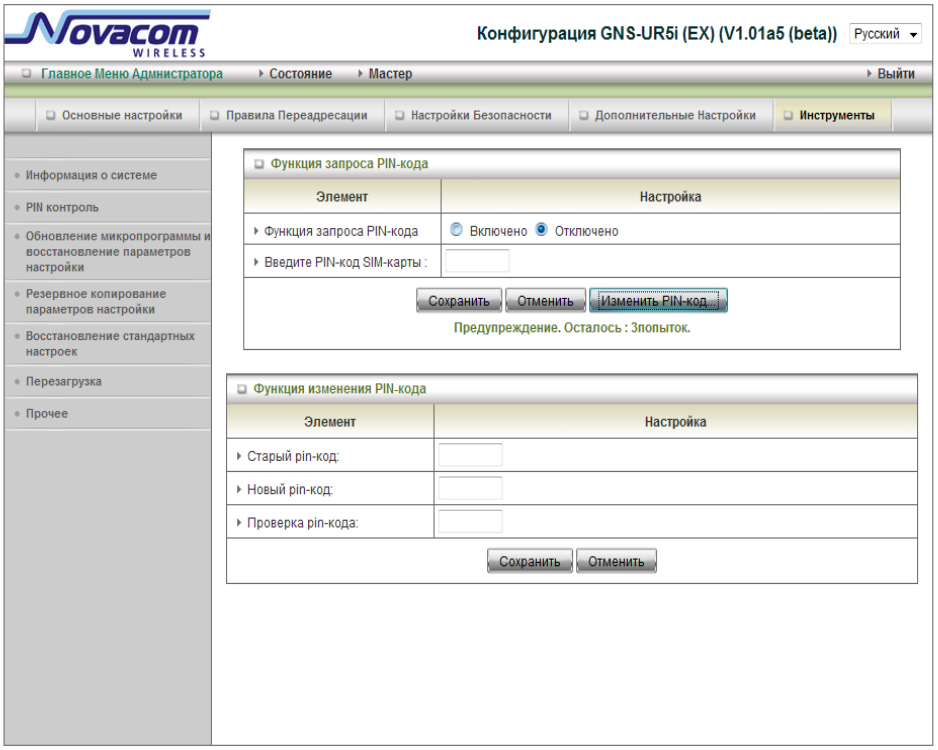


3.2.5.1 Системная информация

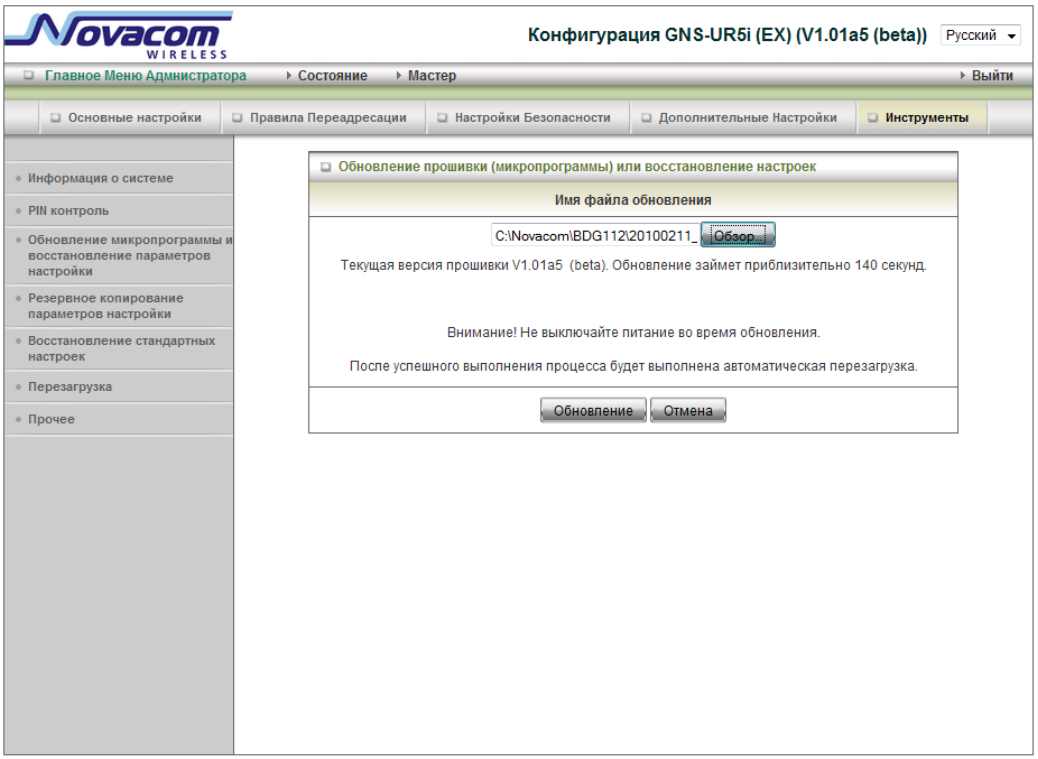


Здесь Вы можете видеть системную информацию и системный журнал. С этой страницы можно очистить системный журнал.

3.2.5.2. Управление пин-кодом.



3.2.5.2 Обновление микропрограмм и восстановление параметров настройки



Вы можете обновить микропрограмму (прошивку роутера), нажав кнопку «Upgrade».

Здесь же можно восстановить из файла настройки, сохранённые ранее в пункте «Резервное копирование настроек».

3.2.5.4 Настройки резервного копирования

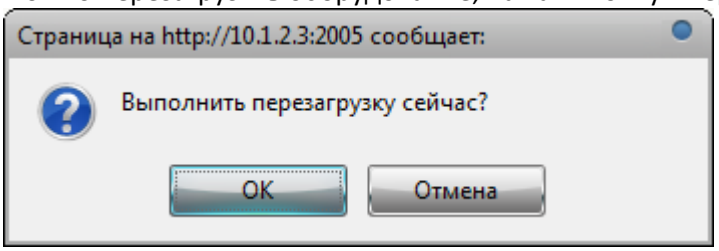
Можно сделать резервную копию своих параметров настройки, нажав кнопку «Backup Setting» и сохранить ее как бинарный файл . Как только потребуется восстановить эти параметры настройки, пожалуйста, обратитесь к разделу 3.2.5.2 « Обновление микропрограмм»

3.2.5.5 Возврат к стандартным настройкам

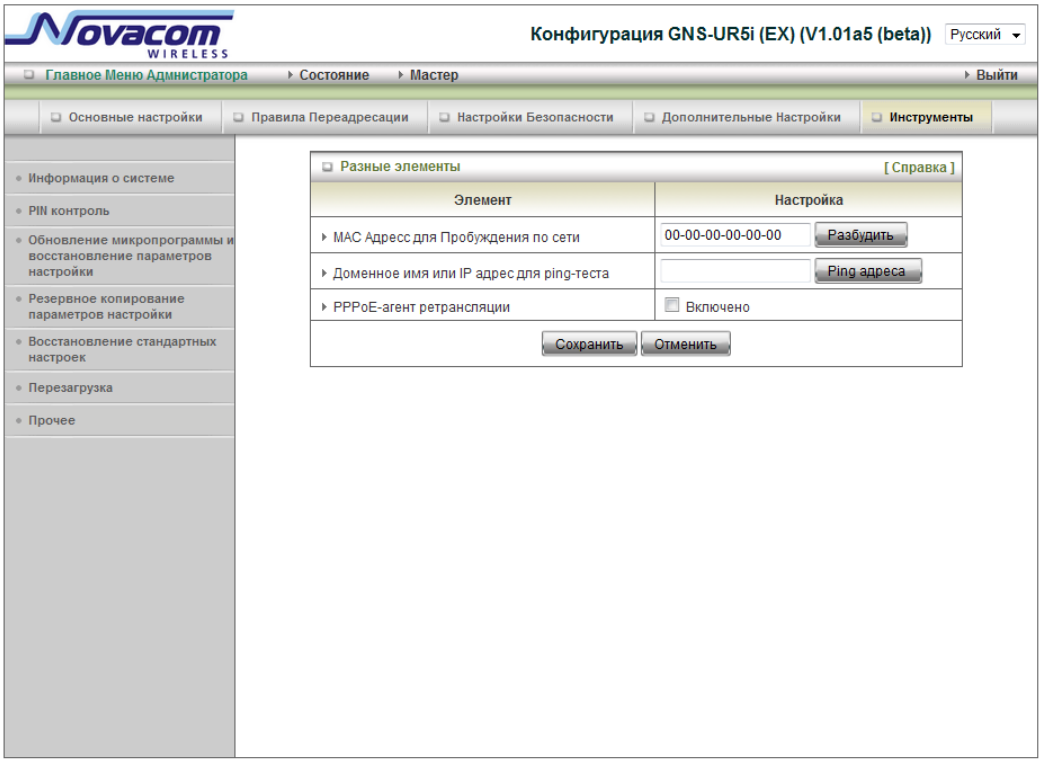
Можно перезагрузить оборудование, вернув его к настройкам производителя, нажав кнопку «Возврат к стандартным настройкам»

3.2.5.6 Перезагрузка

Можно перезагрузить оборудование, нажав кнопку «Перезагрузка».



3.2.5.7 Прочее



1. **MAC адрес для Wake-on-LAN**

   Wake-on-LAN это технология, которая позволяет Вам удаленно включить устройство, подключенное к сети. Чтобы воспользоваться этой функцией, необходимо, чтобы устройство было оборудовано функцией Wake-on-LAN и Вы должны знать MAC адрес этого устройства, например 00-11-22-33-44-55. При нажатии кнопки «Разбудить», роутер немедленно посылает устройству команду на включение.

2. **Имя домена или IP адрес для Ping теста**
   Вы можете ввести URL или IP адрес и затем нажать кнопку «Ping» для проверки работоспособности.

4. Устранение неполадок.
В этом разделе дается обзор общих вопросов, а также возможные решения по установке и эксплуатации 3G роутер.

1. Не удается получить доступ к меню конфигурации, когда я использую мой компьютер для настройки роутера. Почему?
Важно: Рекомендуется использовать соединение Ethernet для настройки роутера.

Убедитесь, что индикатор соединения **Ethernet** на 3G роутере **горит**.
Если индикатор не горит, проверьте, должным ли образом подключен Ethernet кабель

Важно: Убедитесь, что **IP-адрес** находится в том же диапазоне и подсети, что и шлюз Wi-Fi HSPA. IP адрес шлюза Wi-Fi HSPA является 192.168.123.254. Все

компьютеры в сети должны иметь уникальные IP-адреса в тех же пределах (например, 192.168.123.x). Любые компьютеры, имеющие одинаковые IP адреса, не будут видны в сети. Все компьютеры должны также иметь ту же маску подсети (например, 255.255.255.0).
Выполните Ping тест, чтобы убедиться, что Wi-Fi HSPA шлюз отвечает.

Нажмите Start > Run.

1:Наберите **cmd**.
2:Нажмите **Enter.**
3:Наберите "**ping 192.168.123.254".** Успешный пинг показывает 4 ответа.

Важно: Если Вы меняли IP-адрес по умолчанию, убедитесь, что запрашиваете верный IP Address, присвоенный 3G роутеру.

Убедитесь, что ваш Ethernet адаптер работает правильно, и что все сетевые драйверы установлены правильно.

Важно: Названия сетевых адаптеров могут варьироваться, в зависимости от Вашего конкретного адаптера. Шаги по установке, указанные ниже, подходят для всех сетевых адаптеров.

1. Нажмите **Start > Мой компьютер > Свойства**.
2. Выберите вкладку **«Оборудование»**.
3. Нажмите **«Менеджер устройств»**.
4. Двойнок клик на "**Сетевые адаптеры"**.
5. Нажмите правой кнопкой мыши на **Wireless Cardbus Adapter**, или на название Вашего сетевого адаптера.
6. Выберите **Свойства,** чтобы убедиться, что все драйвера установлены правильно.
7. Просмотрите **«Статус устройства»**, чтобы убедиться, что устройство работает правильно.
8. Нажмите «**OK»**.

2**: Почему мой беспроводной клиент не может получить доступ в Интернет?**

Важно: Установите соединение Wi-Fi. Если Вы выбрали тип шифрования **WEP** или **WPA-PSK**, убедитесь, что установки шифровки соответствуют настройкам Wi-Fi. Пожалуйста, обратитесь к документации Вашего Wi-Fi адаптера за дополнительной информацией.

Убедитесь, что беспроводной клиент связан и соединен с правильной Точкой доступа. Для проверки этого соединения, выполните следующие шаги:

1. **Нажмите правой кнопкой мыши** на иконку **Local Area Connection (Местное соединение)** на панели задач.
2. Выберите «Просмотр доступных беспроводных сетей» в «Беспроводных настройках». Появится экран **«Подключение к беспроводной сети»**. Убедитесь, что выбрана верная доступная сеть.

Убедитесь, что IP адрес, назначенный беспроводному адаптеру находится в пределах той же подсети, что и точка доступа и роутер. IP адрес 3G роутера — **192.168.123.254.** Беспроводные адаптеры должны иметь IP адрес в тех же пределах (напр.192.168.123.x). Хотя маска подсети должна быть одной и той же для всех компьютеров в сети, ни у каких двух устройств не может быть одного и того же IP-адреса. Поэтому, у каждого устройства должен быть уникальный IP- адрес

Чтобы проверить IP-адрес, присвоенный беспроводному адаптеру, выполните следующие действия:
1.Введите IPCONFIG/все в командном режиме
2.Введите Ping 192.168.123.254. чтобы проверить, можно ли получить доступ к шлюзу Wi-Fi HSPA

3.Почему качество моего беспроводного соединения продолжает падать?
Для решения проблемы попробуйте предпринять следующие действия.

• Расположение антенны.

1. Попробуйте разное расположение антенны для шлюза Wi-Fi HSPA.
2. Попытайтесь держать антенну на расстоянии не менее 70 см от стены или других объектов.

• Попытайтесь сменить канал роутера, точки доступа и беспроводного адаптера на другой, что может позволить избежать помех.
• Держите оборудование вдали (как минимум 90-180 см) от приборов, производящих радиопомехи, таких как микроволновые печи, мониторы, электромоторы, и т.д.

4. Почему мне не удается установить беспроводное соединение?

Важно: для устранения неполадок 3G роутера необходима связь Ethernet.
Если включена функция шифрования на 3G роутере, необходимо также включить шифрование на всех беспроводных клиентов, чтобы установить беспроводное соединение.

- Для 802.11g параметры настройки шифрования: 64 или 128 бит. Убедитесь, что уровень бит шифрования одинаков для 3G роутера и беспроводного клиента.
- Убедитесь, что SSID (Service Set Identifier) 3G роутера и клиента беспроводной сети один и тот же. Если нет — беспроводное соединение не будет установлено.
- Поместите 3G роутер и беспроводного клиента в одной комнате, а затем проверьте беспроводное соединение.
- Отключите все настройки безопасности, такие как **WEP**,и **MAC Address Control**.
- Выключите 3G роутер и клиент.
  Включите сначала 3G роутер, а затем оборудование клиента.
- Убедитесь, что все устройства устанавливаются в режиме Инфраструктура .
- Убедитесь, что индикаторы сигнализируют о нормальной деятельности. Если нет — проверьте, что кабели питания и Ethernet надежно подключены.
- Убедитесь, что IP-адрес, маска подсети, шлюз и настройки DNS правильно введены для подключения к сети.
- Если Вы используете беспроводные телефоны 2.4GHz, оборудование X-10, или другие системы домашней охраны, потолочные вентиляторы или светильники, качество беспроводного соединения может резко снизиться или совсем пропасть

Чтобы избежать помех, измените канал на 3G роутер и все устройства в сети.

- Держите оборудование не менее 3-6 метров от электрических устройств, которые генерируют радиопомехи. Например: микроволновые печи, мониторы, электромоторы, и так далее.

5. Я не помню моего ключа шифрования. Что я должен делать?

- Если Вы забыли свой ключ шифрования, карта Wi-Fi не сможет установить соединение. Если ключ шифрования был установлен для 3G роутера, он также должен быть установлен для Wi-Fi карты, которая будет устанавливать соединение.

Чтобы перезагрузить ключ(и) шифрования, соединитесь с 3G роутером, используя кабель. (Пожалуйста, обратитесь к разделу «Основные настройки-Беспроводное соединение (Безопасность — Без шифрования)» на стр.10 для дополнительной информации)

7. Как мне сбросить настройки 3G роутера до заводских параметров по умолчанию?

- Если другие методы устранения неисправностей не помогли, вы можете сбросить настройки 3G роутера до заводских параметров по умолчанию.
  Для сброса настроек 3G роутера до заводских настроек по умолчанию, выполните следующие действия, перечисленные ниже:
  Убедитесь, что 3G роутер включен
  Найдите кнопку Сброс на задней панели 3G роутера.
  Используйте скрепку, чтобы нажать на кнопку Сброс.
  Удерживайте 10 секунд и затем отпустите.
  После перезагрузки 3G роутера, он сбрасывается на заводские установки по умолчанию.
  Важно: обратите внимание, что этот процесс займет несколько минут.

8. Что такое VPN?

- VPN (Виртуальная частная сеть). VPN создает «туннель» через существующее подключение к интернету, используя PPTP (двухточечный протокол туннелирования) или IPSec (IP Безопасность) протоколы с различными схемами шифрования, включая Microsoft Challenge Handshake Authentication Protocol (MS-CHAP).
- Эта особенность позволяет использовать свое существующее подключение к интернет, чтобы соединиться с удаленным сайтом, используя дополнительные параметры безопасности. Если соединение VPN не функционирует, проверьте, что настройки соединения VPN верны.

Важно: эта информация должна быть предоставлена провайдером VPN. Нажатие кнопки сброса возвращает заводские настройки по умолчанию.

9. Что делать, если кабель Ethernet не работает должным образом?

- Во-первых, убедитесь, что существует прочная связь кабеля между портом Ethernet на роутере, и на вашей сетевой карте (Network Interface Card).
- Во-вторых, убедитесь, что адаптер сетевой карты «Включен» и настроен на прием IP адреса от DHCP.
- Если настройки сделаны правильно, убедитесь, что вы НЕ используете кроссоверный кабель Ethernet. Хотя 3G роутер является MDI / MDIX совместимым, не все сетевые адаптеры являются такими. Поэтому рекомендуется использовать прямой кабель, когда это возможно.

3. Техническая спецификация

3G	BandRich M250 3G встроенный модем
Стандарты	IEEE 802.11b/g IEEE 802.3 IEEE 802.3u
Беспроводное соединение	
Стандарт	IEEE 802.11 B\G
Скорость данных	54, 48, 36, 24, 18, 12, 9, и 6 Mbps на канал, Auto Fall-Back
Частота	2.4 – 2.462 GHz, CCK / OFDM модуляция
Диапазон покрытия	Tx/Rx power 18dbm/Per Cell Внутри помещения около 35-100 метров; На улице до 100-300 метров
Кол-во каналов	1-11 для Северной Америки (FCC);1-11 для Канады (DOC) 1-13 Европа (кроме Испании и Франции) (ETSI) 1-14 Япония (TELEC);
Безопасность	64-бит и 128-бит WEP шифрование; WPA шифрование
Антенна	Внешняя антенна 1.8 dBI
Firewall	IP фильтрование NAT (Передача сетевых адресов) с VPN MAC фильтрование
Поддержка WAN	3G, статичный IP, динамичный IP, PPPoE,PPTP,L2TP
Схема подключения	Соединение по запросу, авторазъединение
Функция NAT	Класс C ;One-to-Many; Макс 253 пользователя; виртуальный сервер ; DMZ Host
VPN	PPTP, L2TP и IPSec
Конфигурации и управление	IE, Навигатор браузер и SNMP
	DHCP сервер и Клиент сервер
Рабочая среда	Температура : 0 - 40^{O}C, влажность 10%-90% без конденсата
Поддерживаемые операционные системы	Windows 95/98/ME/NT/2000/XP; Linux
Питание	включение 12 В, 2.0 А