

Novacom Wireless

3G (Wi-Fi/HSPA) роутер **GNS-UR4i VPN**

[Руководство пользователя]



Содержание

1. Введение.....	3
1.1. Комплектация.....	3
1.2. Системные требования к конфигурации.....	3
1.3. Интерфейсы – вид сзади.....	4
1.4. Интерфейсы – вид спереди.....	4
1.5. Преимущества.....	6
2. Настройка 3G роутера.....	8
2.1. Требования по установке.....	8
2.2. Инструкции по установке – настройка сети.....	8
2.3. Установка соединения Wi-Fi.....	13
3. Использование меню конфигурации.....	13
3.1. Мастер настройки.....	14
3.2. Меню администратора.....	22
3.2.1. Основные настройки.....	22
3.2.2. Правила перенадресации.....	36
3.2.3. Настройки безопасности.....	40
3.2.4. Дополнительные настройки.....	49
4. Устранение неполадок.....	62
5. Технические характеристики.....	66

1. Введение

3G (Wi-Fi/HSPA) роутер **Novacom GNS-UR4i VPN** является высокоэффективным инструментом, который организывает 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.

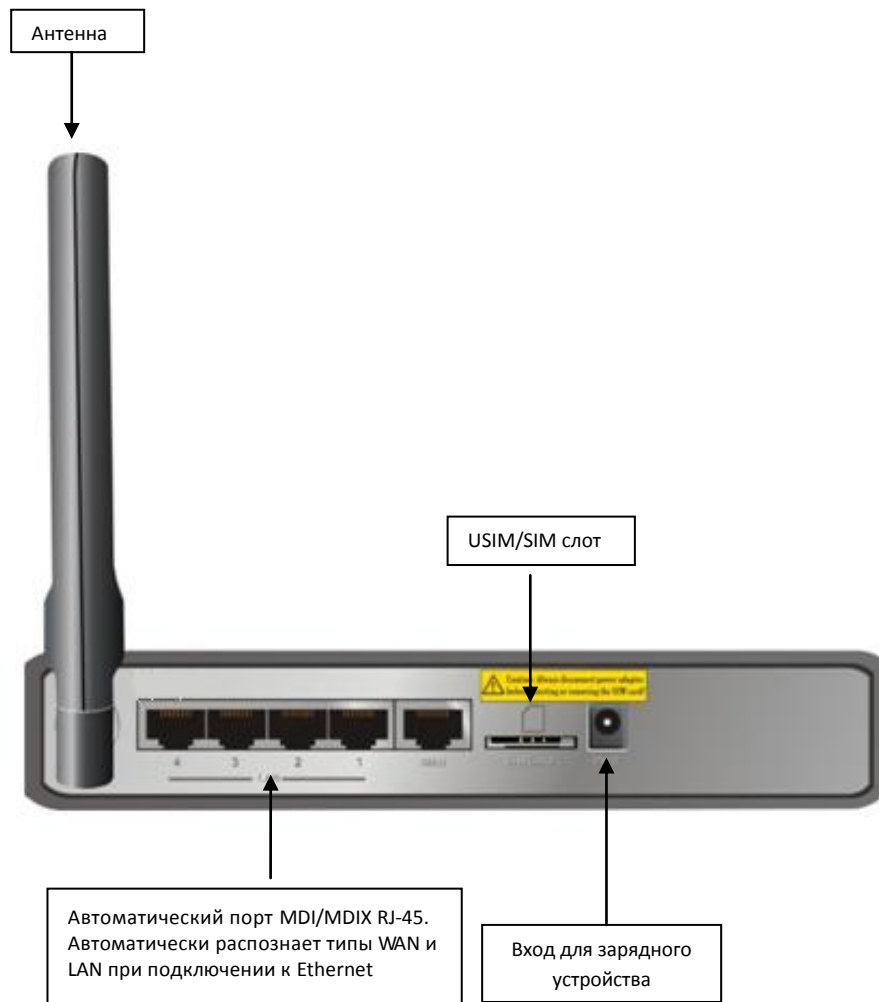
Пункт	Описание	Количество
1	Novacom GNS- UR4i VPN	1
2	Кабель RJ-45	1
3	Адаптер питания 12V 2.0A	1
4	Инструкция по установке	1
5	CD	1

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

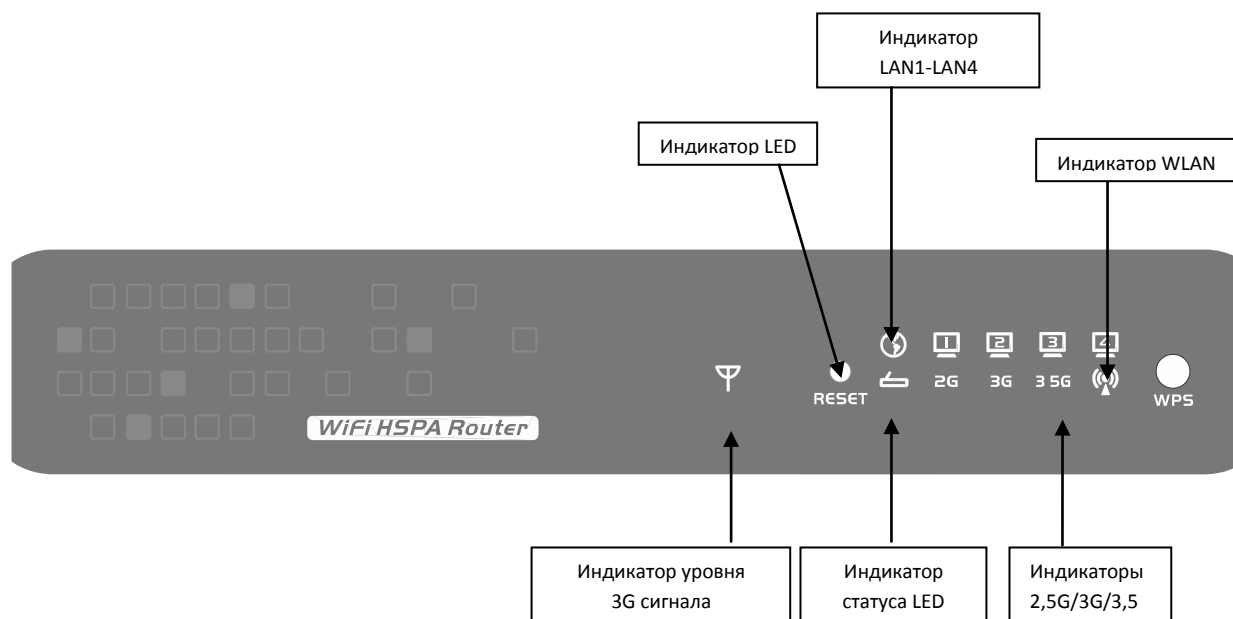
- 3G SIM-карта с подключенным пакетом услуг
Примечание: условия подключения услуг уточняйте у Вашего оператора
- Компьютеры с операционной системой Windows, Macintosh или Linux с установленным Ethernet адаптером.
- Internet Explorer версии 6.0 или Netscape Navigator версии 7.0 и выше.
- Wi-Fi системные 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 HSPA модем для 3G-доступа
Скорость загрузки до 7.2Mbps
Скорость отдачи до 2.0Mbps
850/1900/2100MHz по HSPA / 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**

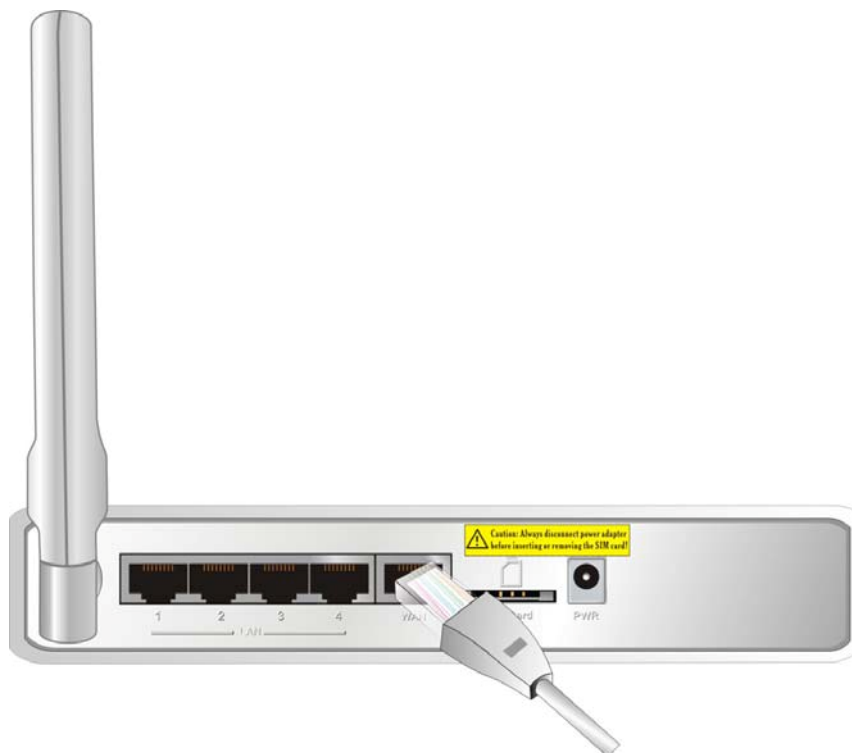


Рис. 2.4

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)

- а. Все индикаторы засветятся, сигнализируя, что питание подключено
- б. Затем индикаторы начнут мигать, сигнализируя, что шлюз выполняет инициализацию и процесс подключения к Интернету. Это займет несколько минут.
- с. Когда соединение будет установлено, начнет мигать индикатор WLAN
- д. См. Пункт 1.4 данного руководства: «Индикаторы: вид спереди».



Рис. 2.6

2.1.2 Установка соединения Wi-Fi

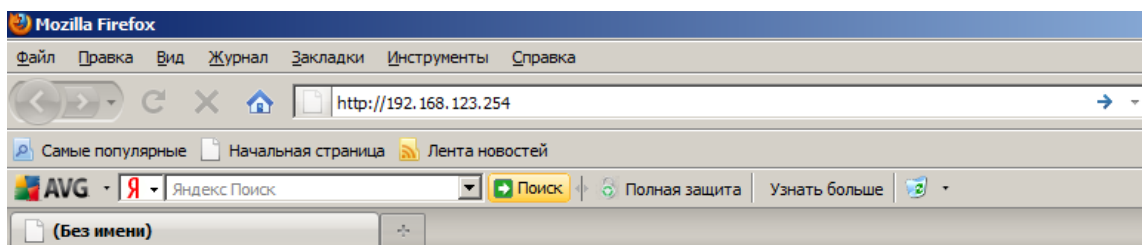
Если Вы выбрали параметры шифрования WEP или WPA-PSK, проверьте, чтобы данные настройки совпадали с настройками Вашего Wi-Fi адаптера.

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.



Конфигурация GNS-UR5i (EX) (V1.01a5)

Главное Меню Пользователя

Состояние

Пароль системы :

(по умолчанию: admin)

Логин

Статус системы

[Справка]

Элемент	Состояние WAN	Заметки
IP-адрес	172.19.143.250	3G
Маска подсети	255.255.255.255	
Шлюз	10.64.64.64	
Служба доменных имен (DNS)	10.17.128.1, 217.66.145.1	
Время подключения	00:00:49	

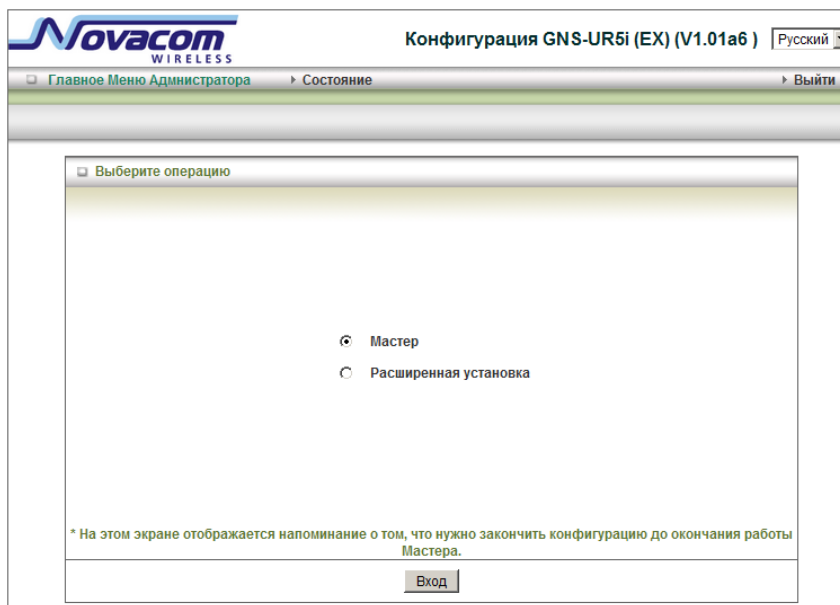
Сведения о беспроводном модеме

Элемент	Состояние	Заметки
Информация о карте	M-250V	
Состояние связи	Connected	
Мощность сигнала	54%	
Передано байт	237	

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»).



Novacom WIRELESS

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.

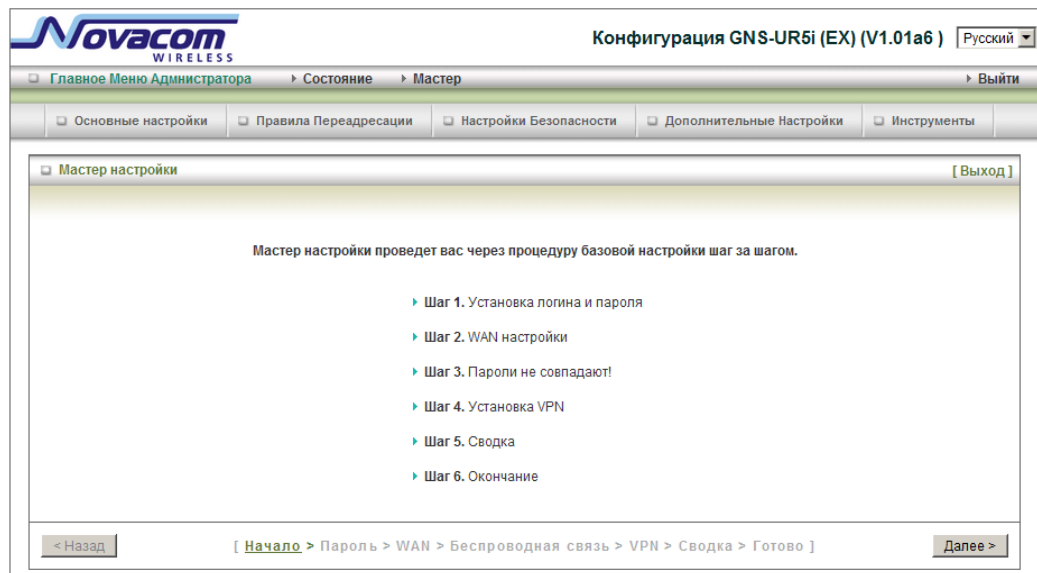
Вход

Нажмите «Вход» для запуска.

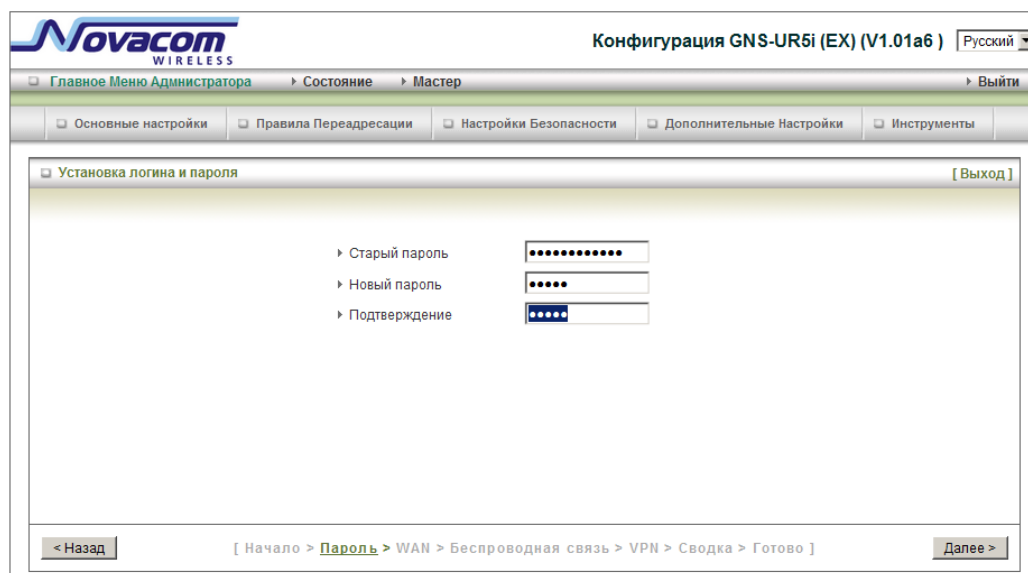
С пошаговым мастером настройки, Вы сможете легко настроить роутер. Эти настройки включают в себя настройку:

- а. Логина и пароля,
- б. Настройки WAN
- с. Настройки беспроводного соединения,

Нажмите кнопку «Далее» для запуска конфигурации.



Шаг 1: Позволяет изменить системный пароль.

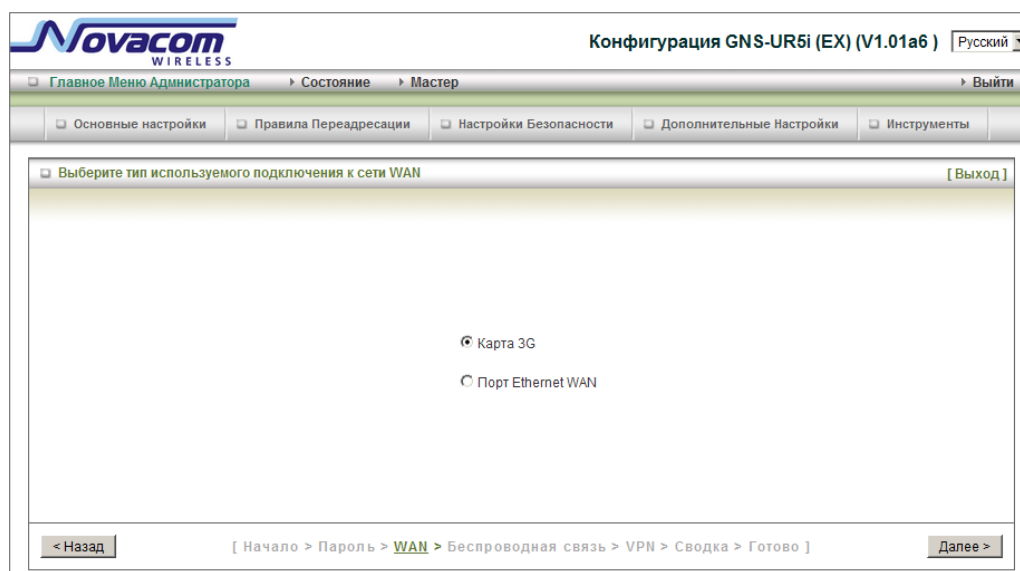


The screenshot shows the configuration page for the Novacom GNS-UR5i (EX) router. The title bar indicates the version is V1.01a6 and the language is Russian. The main menu includes 'Главное Меню Администратора', 'Состояние', 'Мастер', and 'Выйти'. The 'Мастер' (Wizard) section is active, showing a progress bar with steps: 'Основные настройки', 'Правила Переадресации', 'Настройки Безопасности', 'Дополнительные Настройки', and 'Инструменты'. The current step is 'Установка логина и пароля' (Login and password setup), with a '[Выход]' (Exit) link. The form contains three password fields: 'Старый пароль' (Old password), 'Новый пароль' (New password), and 'Подтверждение' (Confirmation). At the bottom, there is a '< Назад' (Back) button, a breadcrumb trail '[Начало > Пароль > WAN > Беспроводная связь > VPN > Сводка > Готово]', and a 'Далее >' (Next) button.

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

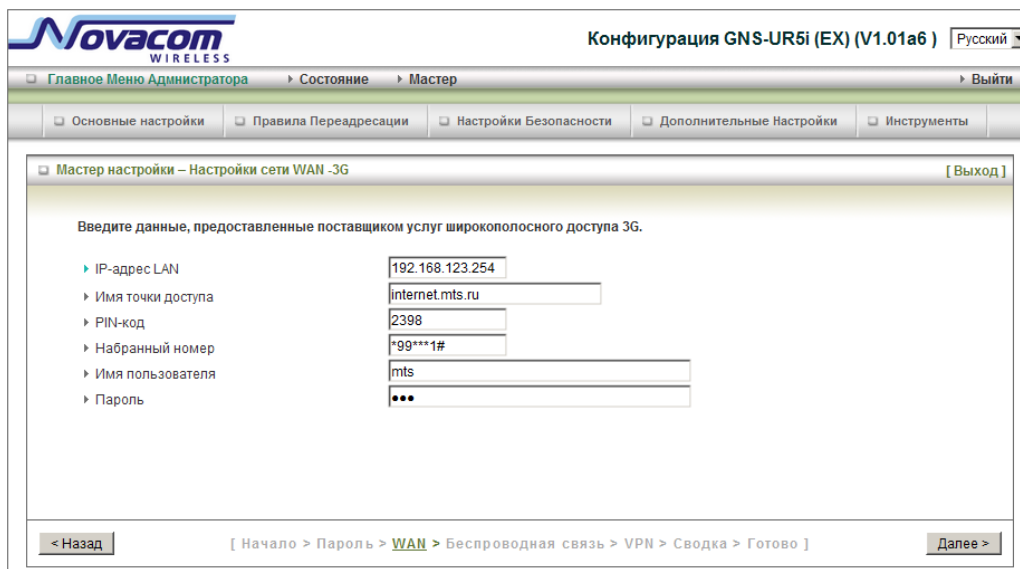
1. Введите Ваш старый пароль (если смена пароля первая, слово "admin" является паролем по умолчанию.)
2. Введите Ваш новый пароль
3. Введите этот новый пароль еще раз для подтверждения.
4. Нажмите «Далее», чтобы перейти к следующим установкам.

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



The screenshot shows the configuration page for the Novacom GNS-UR5i (EX) router, specifically the 'WAN Connection Type' selection screen. The title bar and main menu are identical to the previous screenshot. The 'Мастер' (Wizard) section shows the progress bar with the current step being 'Выберите тип используемого подключения к сети WAN' (Select the type of WAN connection to use). The form contains two radio button options: 'Карта 3G' (3G Card) and 'Порт Ethernet WAN' (Ethernet WAN Port). At the bottom, there is a '< Назад' (Back) button, a breadcrumb trail '[Начало > Пароль > WAN > Беспроводная связь > VPN > Сводка > Готово]', and a 'Далее >' (Next) button.

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.

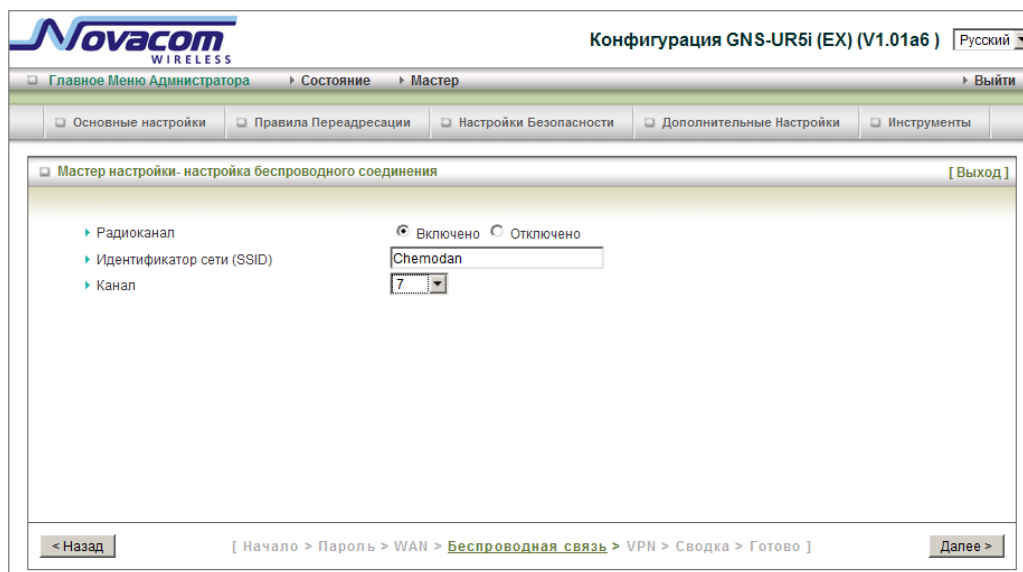
Важно: На роутере 3G при использовании подсети 255.255.255.0 (Class C) доступно 254 адреса. Например: IP адрес роутера: 192.168.123.1. Доступный разброс IP адресов клиентов от 192.168.123.2 до 192.168.123.254.

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.

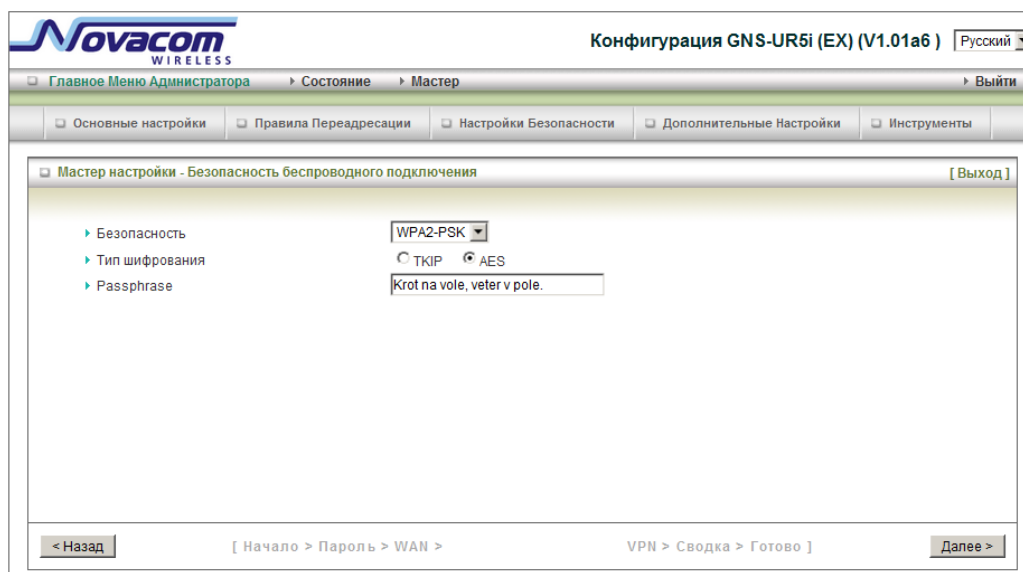
Шаг 5: Изменение настроек беспроводного соединения.



The screenshot shows the configuration page for the wireless connection. The title bar indicates 'Конфигурация GNS-UR5i (EX) (V1.01a6)' and the language is set to 'Русский'. The breadcrumb trail is 'Главное Меню Администратора > Состояние > Мастер > Выйти'. The main menu includes 'Основные настройки', 'Правила Переадресации', 'Настройки Безопасности', 'Дополнительные Настройки', and 'Инструменты'. The current page is 'Мастер настройки - настройка беспроводного соединения'. It features a 'Радиоканал' section with a 'Включено' radio button selected and an 'Отключено' radio button. Below this, the 'Идентификатор сети (SSID)' is set to 'Chemodan' and the 'Канал' is set to '7'. At the bottom, there is a navigation bar with buttons for '< Назад', '[Начало > Пароль > WAN > Беспроводная связь > VPN > Сводка > Готово]', and 'Далее >'.

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.

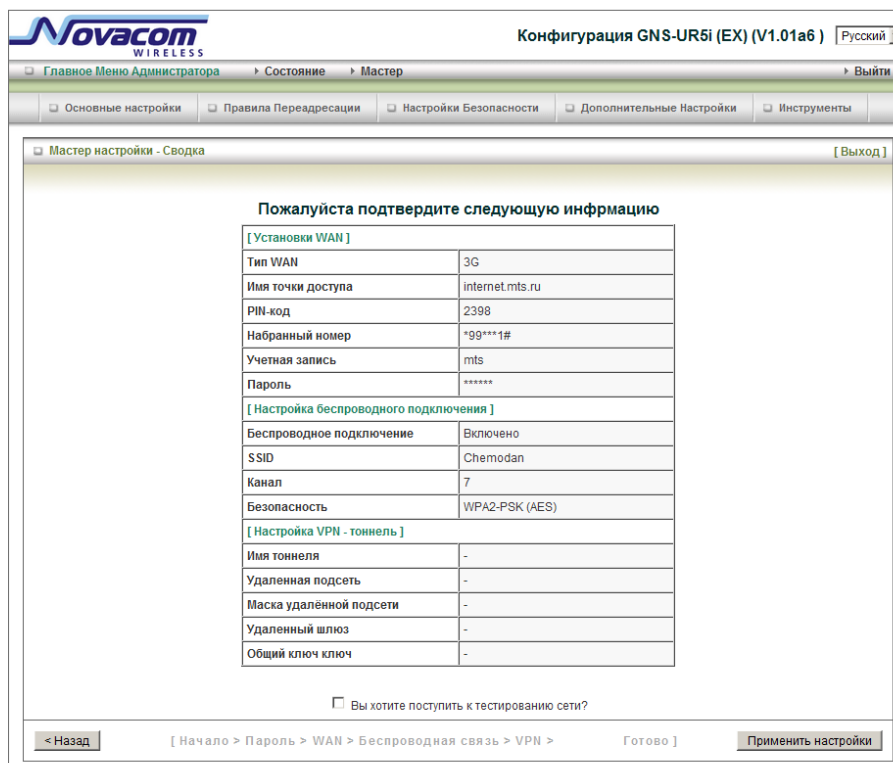


The screenshot shows the configuration page for wireless connection security. The title bar indicates 'Конфигурация GNS-UR5i (EX) (V1.01a6)' and the language is set to 'Русский'. The breadcrumb trail is 'Главное Меню Администратора > Состояние > Мастер > Выйти'. The main menu includes 'Основные настройки', 'Правила Переадресации', 'Настройки Безопасности', 'Дополнительные Настройки', and 'Инструменты'. The current page is 'Мастер настройки - Безопасность беспроводного подключения'. It features a 'Безопасность' section with a 'WPA2-PSK' dropdown menu. Below this, the 'Тип шифрования' is set to 'AES' (selected) and 'TKIP'. The 'Passphrase' is set to 'Krot na vole, veter v pole.'. At the bottom, there is a navigation bar with buttons for '< Назад', '[Начало > Пароль > WAN > VPN > Сводка > Готово]', and 'Далее >'.

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

2. Нажмите «Далее»

Шаг 7: Сводка (проверка настроенных параметров).



Конфигурация GNS-UR5i (EX) (V1.01a6) [Русский]

Главное Меню Администратора > Состояние > Мастер > Выйти

Основные настройки Правила Переадресации Настройки Безопасности Дополнительные Настройки Инструменты

Мастер настройки - Сводка [Выйти]

Пожалуйста подтвердите следующую информацию

[Установки WAN]	
Тип WAN	3G
Имя точки доступа	internet.mts.ru
PIN-код	2398
Набранный номер	*99***1#
Учетная запись	mts
Пароль	*****

[Настройка беспроводного подключения]	
Беспроводное подключение	Включено
SSID	Chemodan
Канал	7
Безопасность	WPA2-PSK (AES)

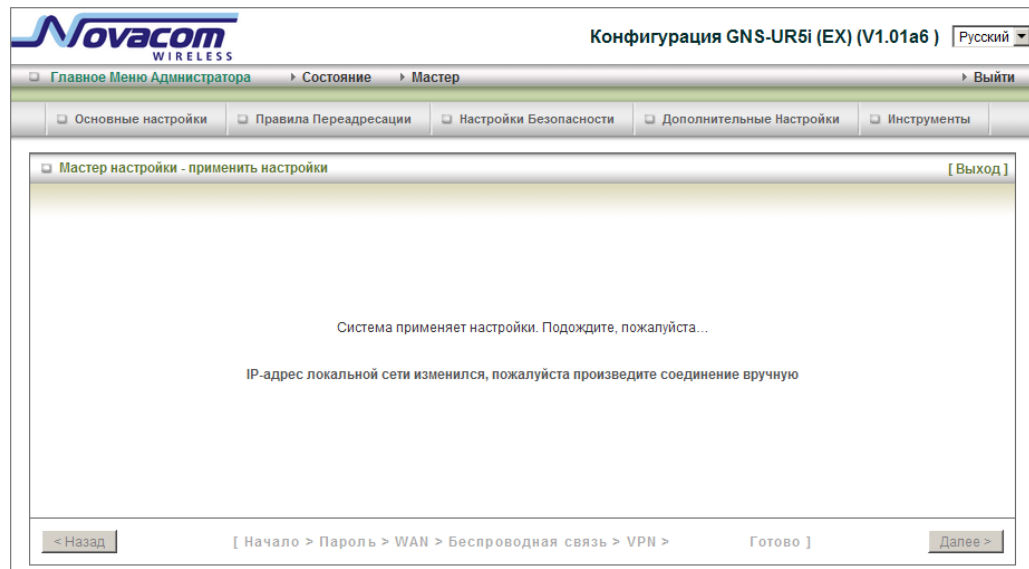
[Настройка VPN - тоннеля]	
Имя тоннеля	-
Удаленная подсеть	-
Маска удаленной подсети	-
Удаленный шлюз	-
Общий ключ ключ	-

☐ Вы хотите поступить к тестированию сети?

< Назад [Начало > Пароль > WAN > Беспроводная связь > VPN > Готово] Применить настройки

Нажмите кнопку «Применить настройки»

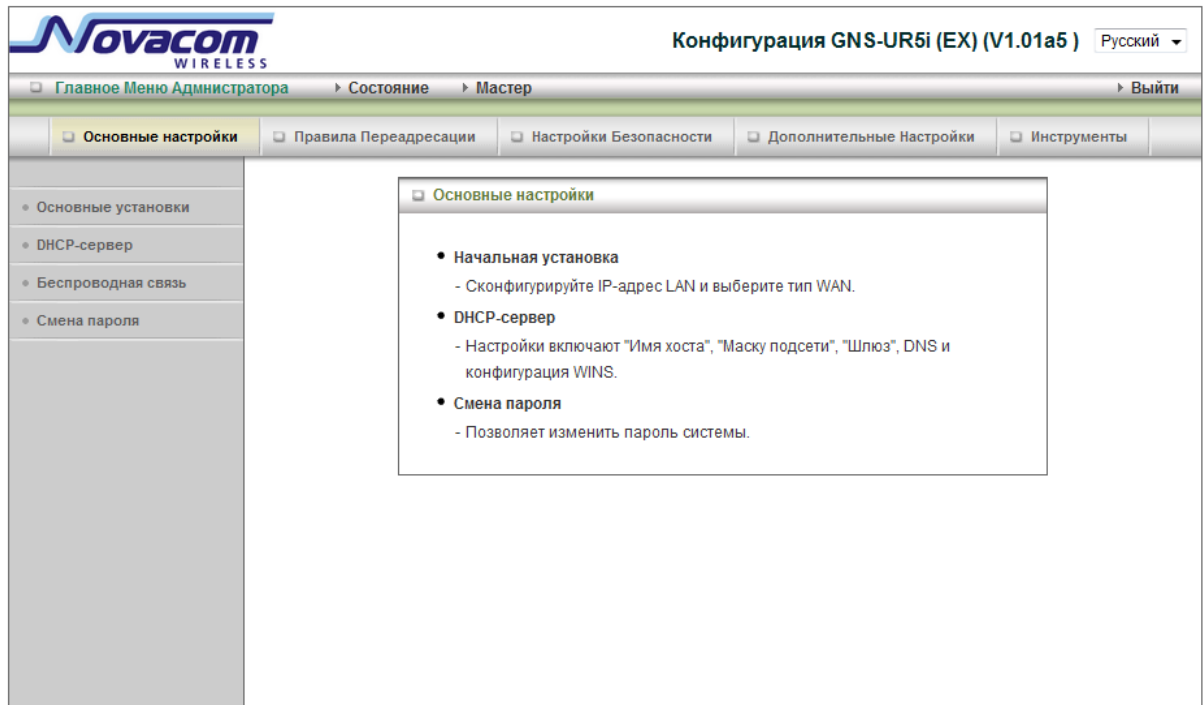
Шаг 8: Загрузка настроек



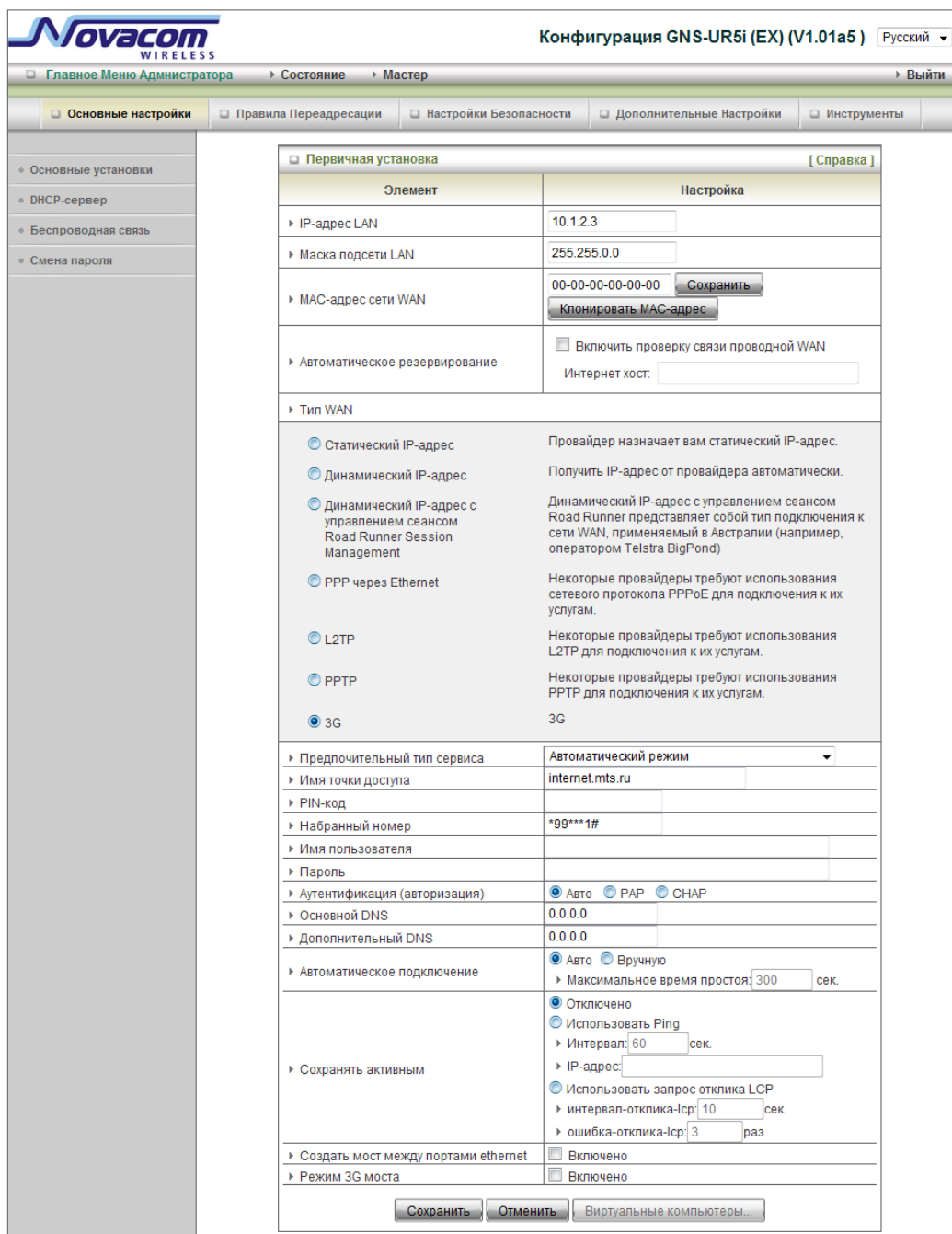
Нажмите «Далее» для возврата на страницу статуса.

3.2. Меню Администратора

3.2.1 Основные настройки



3.2.1.1 Основные установки — тип WAN, виртуальные компьютеры.



The screenshot shows the configuration interface for a Novacom GNS-UR5i (EX) router. The title bar indicates the version is V1.01a5 and the language is Russian. The main menu includes 'Основные настройки' (Basic Settings), 'Правила Переадресации' (Forwarding Rules), 'Настройки Безопасности' (Security Settings), 'Дополнительные Настройки' (Advanced Settings), and 'Инструменты' (Tools). The 'Основные настройки' section is expanded, showing 'Первичная установка' (Initial Setup) as the active tab. The 'Первичная установка' section contains a table with two columns: 'Элемент' (Element) and 'Настройка' (Setting). The table lists various settings including IP address, subnet mask, MAC address, WAN type, and connection parameters. The 'Тип WAN' (WAN Type) section is expanded, showing options for static IP, dynamic IP, PPP over Ethernet, L2TP, PPTP, and 3G. The '3G' option is selected. Below this, there are fields for service type, access point name, PIN code, phone number, username, password, authentication method, DNS servers, automatic connection settings, and connection mode. The 'Сохранить' (Save) button is visible at the bottom.

Элемент	Настройка
IP-адрес LAN	10.1.2.3
Маска подсети LAN	255.255.0.0
MAC-адрес сети WAN	00-00-00-00-00-00 Сохранить Клонировать MAC-адрес
Автоматическое резервирование	<input type="checkbox"/> Включить проверку связи проводной WAN Интернет хост: <input type="text"/>
Тип WAN	<ul style="list-style-type: none"><input type="radio"/> Статический IP-адрес: Провайдер назначает вам статический IP-адрес.<input type="radio"/> Динамический IP-адрес: Получить IP-адрес от провайдера автоматически.<input type="radio"/> Динамический IP-адрес с управлением сеансом Road Runner Session Management: Динамический IP-адрес с управлением сеансом Road Runner представляет собой тип подключения к сети WAN, применяемый в Австралии (например, оператором Telstra BigPond)<input type="radio"/> PPP через Ethernet: Некоторые провайдеры требуют использования сетевого протокола PPPoE для подключения к их услугам.<input type="radio"/> L2TP: Некоторые провайдеры требуют использования L2TP для подключения к их услугам.<input type="radio"/> PPTP: Некоторые провайдеры требуют использования PPTP для подключения к их услугам.<input checked="" type="radio"/> 3G: 3G
Предпочтительный тип сервиса	Автоматический режим
Имя точки доступа	internet.mts.ru
PIN-код	
Набранный номер	*99***1#
Имя пользователя	
Пароль	
Аутентификация (авторизация)	<input checked="" type="radio"/> Авто <input type="radio"/> PAP <input type="radio"/> CHAP
Основной DNS	0.0.0.0
Дополнительный DNS	0.0.0.0
Автоматическое подключение	<input checked="" type="radio"/> Авто <input type="radio"/> Вручную Максимальное время простоя: 300 сек.
Сохранять активным	<input checked="" type="radio"/> Отключено <input type="radio"/> Использовать Ping Интервал: 60 сек. IP-адрес: <input type="text"/> <input type="radio"/> Использовать запрос отклика LCP интервал-отклика-lcp: 10 сек. ошибка-отклика-lcp: 3 раз
Создать мост между портами ethernet	<input type="checkbox"/> Включено
Режим 3G моста	<input type="checkbox"/> Включено

[Сохранить](#) [Отменить](#) [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:

► Имя хоста	<input type="text" value="ROUTER"/> (необязательный параметр)
► MTU	<input type="text" value="1500"/>
► Автоматическое восстановление подключения	<input checked="" type="checkbox"/> Включено
► Основной DNS	<input type="text" value="8.8.8.8"/>
► Дополнительный DNS	<input type="text" value="0.0.0.0"/>
<input type="button" value="Сохранить"/> <input type="button" value="Отменить"/> <input <="" td="" type="button" value="Виртуальные компьютеры..."/>	

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 подключения: эта функция позволяет роутеру восстановить Ваш IP адрес автоматически после истечения времени аренды, даже когда система неактивна.

PPP через Ethernet

► Учетная запись PPPoE	<input type="text" value="Vasiliy"/>
► Пароль PPPoE	<input type="password" value="....."/>
► MTU	<input type="text" value="1492"/>
► Основной DNS	<input type="text" value="0.0.0.0"/>
► Дополнительный DNS	<input type="text" value="0.0.0.0"/>
► Максимальное время простоя	<input type="text" value="300"/> сек. <input checked="" type="checkbox"/> Автоматическое восстановление подключения
► Имя службы PPPoE	<input type="text" value="Serviza"/> (необязательный параметр)
► Назначенный IP-адрес	<input type="text" value="83.243.165.13"/> (необязательный параметр)
<input type="button" value="Сохранить"/> <input type="button" value="Отменить"/> <input <="" td="" type="button" value="Виртуальные компьютеры..."/>	

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	<input type="text" value="Yozhik"/>
Пароль	<input type="password" value="....."/>
Сервер входа	<input type="text"/> (необязательный параметр)
<input type="button" value="Сохранить"/> <input type="button" value="Отменить"/> <input type="button" value="Виртуальные компьютеры..."/>	

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

PPTP

Имя туннеля	<input type="text" value="Tunnel12"/>
IP-адрес сервера	<input type="text" value="91.15.79.12"/>
Мой IP-адрес	<input type="radio"/> Получить IP-адрес с DHCP-сервера <input checked="" type="radio"/> Использовать статический IP-адрес IP <input type="text" value="91.15.79.145"/> Маска подсети <input type="text" value="255.255.255.0"/> Шлюз <input type="text" value="0.0.0.0"/>
Учетная запись PPTP	<input type="text" value="Zapis"/>
Пароль PPTP	<input type="password" value="....."/>
Максимальное время простоя	<input type="text" value="300"/> сек.
Выбор режима подключения	<input type="radio"/> Всегда вкл. <input checked="" type="radio"/> Подключение по требованию
<input type="button" value="Сохранить"/> <input type="button" value="Отменить"/> <input type="button" value="Виртуальные компьютеры..."/>	

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

Имя туннеля	Tunnel
IP-адрес сервера	83.243.165.17
Мой IP-адрес	<input checked="" type="radio"/> Получить IP-адрес с DHCP-сервера <input type="radio"/> Использовать статический IP-адрес IP 0.0.0.0 Маска подсети 255.255.255.0 Шлюз 0.0.0.0
Учетная запись L2TP	Fedia
Пароль L2TP	••••••••
Максимальное время простоя	300 сек.
Выбор режима подключения	<input checked="" type="radio"/> Всегда вкл. <input type="radio"/> Подключение по требованию
<input type="button" value="Сохранить"/> <input type="button" value="Отменить"/> <input type="button" value="Виртуальные компьютеры..."/>	

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

Предпочтительный тип сервиса	Автоматический режим
Имя точки доступа	internet.mts.ru
PIN-код	7301
Набранный номер	*99***1#
Имя пользователя	mts
Пароль	...
Аутентификация (авторизация)	<input checked="" type="radio"/> Авто <input type="radio"/> PAP <input type="radio"/> CHAP
Основной DNS	0.0.0.0
Дополнительный DNS	0.0.0.0
Автоматическое подключение	<input checked="" type="radio"/> Авто <input type="radio"/> Вручную Максимальное время простоя: 300 сек.
Сохранять активным	<input type="radio"/> Отключено
	<input type="radio"/> Использовать Ping Интервал: 60 сек.
	<input type="radio"/> IP-адрес: 8.8.8.8
	<input checked="" type="radio"/> Использовать запрос отклика LCP интервал-отклика-lcp: 10 сек. ошибка-отклика-lcp: 3 раз
Создать мост между портами ethernet	<input checked="" type="checkbox"/> Включено
Режим 3G моста	<input checked="" type="checkbox"/> Включено
<div>Сохранить Отменить Виртуальные компьютеры...</div>	

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

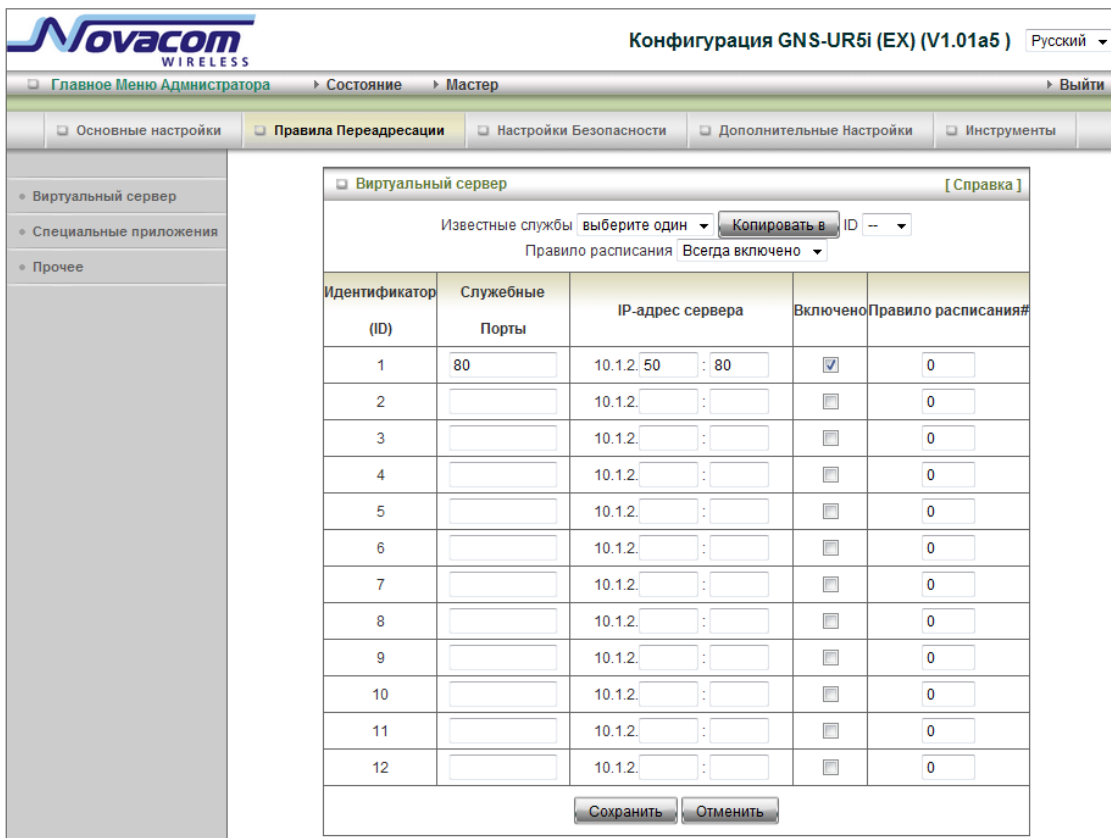
Ручной: Вручную: Устройство не будет устанавливать соединение до тех пор, пока не нажата клавиша соединения на странице статуса.

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.



The screenshot shows the configuration interface for a Novacom GNS-UR5i (EX) router. The title bar indicates the version is V1.01a5 and the language is Russian. The navigation menu includes 'Главное Меню Администратора', 'Состояние', 'Мастер', and 'Выйти'. The main menu has tabs for 'Основные настройки', 'Правила Переадресации' (selected), 'Настройки Безопасности', 'Дополнительные Настройки', and 'Инструменты'.

Under 'Правила Переадресации', there is a section for 'Виртуальный сервер' with a '[Справка]' link. It includes a dropdown for 'Известные службы' (set to 'выберите один'), a 'Копировать в' button, an 'ID' dropdown, and a 'Правило расписания' dropdown (set to 'Всегда включено').

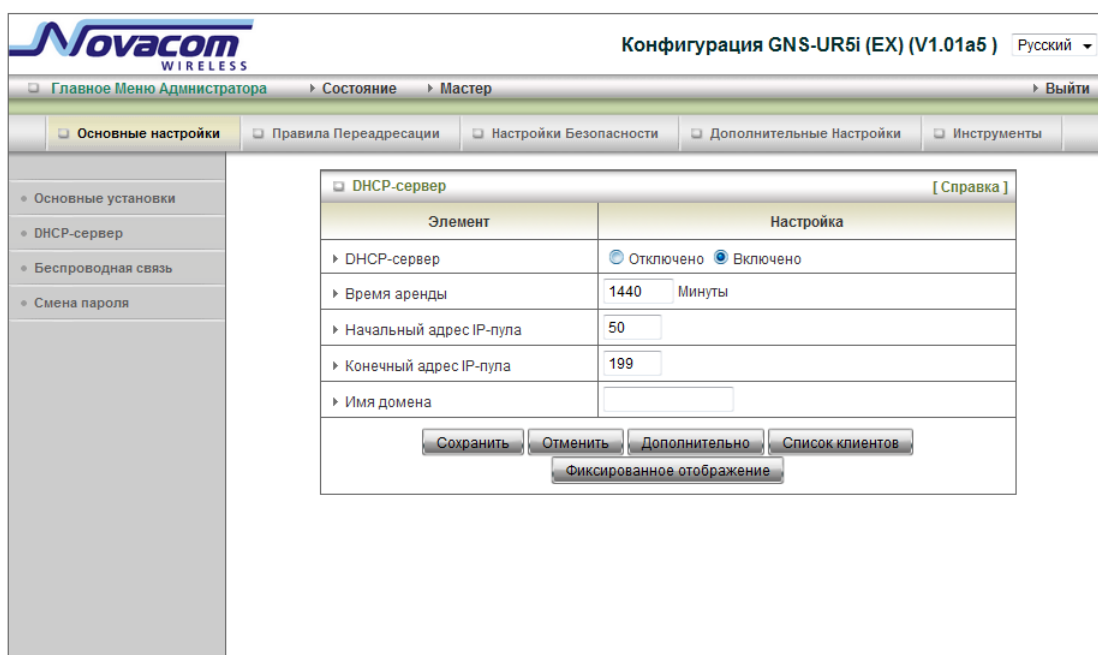
Идентификатор (ID)	Служебные Порты	IP-адрес сервера	Включено	Правило расписания#
1	80	10.1.2.50 : 80	<input checked="" type="checkbox"/>	0
2		10.1.2. :	<input type="checkbox"/>	0
3		10.1.2. :	<input type="checkbox"/>	0
4		10.1.2. :	<input type="checkbox"/>	0
5		10.1.2. :	<input type="checkbox"/>	0
6		10.1.2. :	<input type="checkbox"/>	0
7		10.1.2. :	<input type="checkbox"/>	0
8		10.1.2. :	<input type="checkbox"/>	0
9		10.1.2. :	<input type="checkbox"/>	0
10		10.1.2. :	<input type="checkbox"/>	0
11		10.1.2. :	<input type="checkbox"/>	0
12		10.1.2. :	<input type="checkbox"/>	0

At the bottom of the table are 'Сохранить' and 'Отменить' buttons.

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



The screenshot shows the configuration interface for the Novacom GNS-UR5i (EX) router. The title bar indicates the version is V1.01a5 and the language is Russian. The main menu includes options like 'Главное Меню Администратора', 'Состояние', 'Мастер', and 'Выйти'. The 'Основные настройки' (Basic Settings) tab is selected, and the 'DHCP-сервер' (DHCP Server) sub-tab is active. The left sidebar lists various settings categories. The main content area displays the DHCP server configuration table.

Элемент	Настройка
DHCP-сервер	<input type="radio"/> Отключено <input checked="" type="radio"/> Включено
Время аренды	1440 Минуты
Начальный адрес IP-пула	50
Конечный адрес IP-пула	199
Имя домена	

Buttons at the bottom: Сохранить, Отменить, Дополнительно, Список клиентов, Фиксированное отображение.

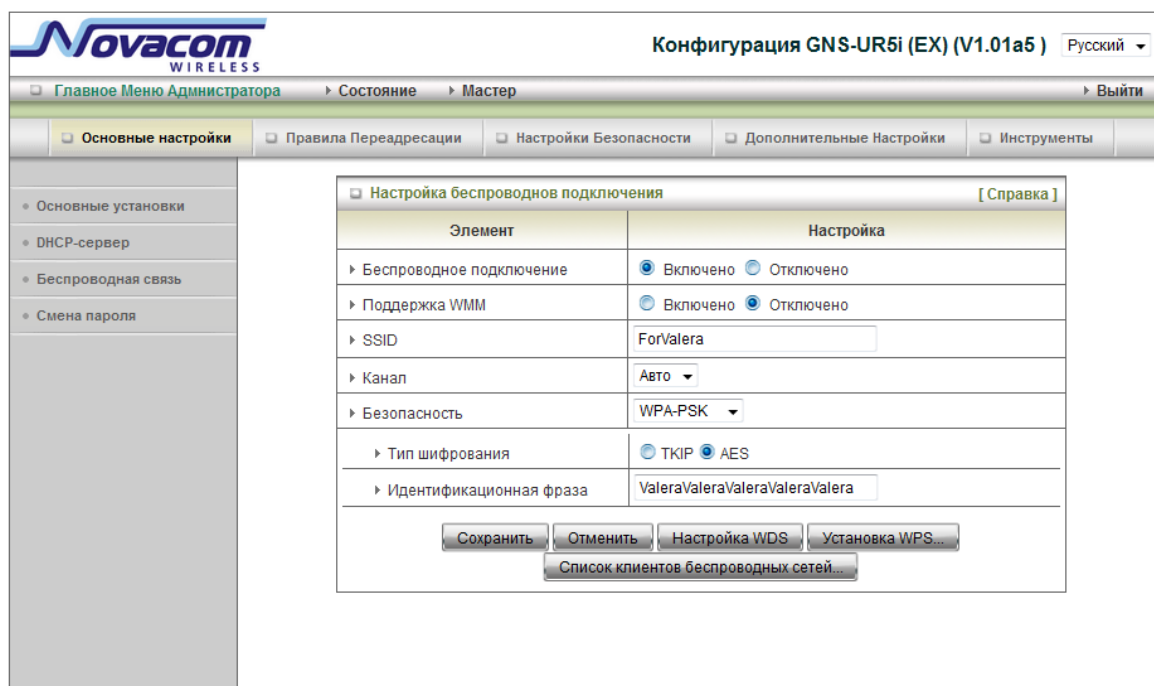
Нажмите «More>>»,

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.



Элемент	Настройка
Беспроводное подключение	<input checked="" type="radio"/> Включено <input type="radio"/> Отключено
Поддержка WMM	<input type="radio"/> Включено <input checked="" type="radio"/> Отключено
SSID	ForValera
Канал	Авто
Безопасность	WPA-PSK
Тип шифрования	<input type="radio"/> TKIP <input checked="" type="radio"/> AES
Идентификационная фраза	ValeraValeraValeraValeraValera

Сохранить Отменить Настройка WDS Установка WPS...
Список клиентов беспроводных сетей...

Беспроводные настройки позволяют Вам сконфигурировать беспроводное соединение

- Беспроводной доступ:** По умолчанию включен. Выбор этой опции позволит Вам настроить WAP.
- 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
- 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),
- 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.)
- 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.

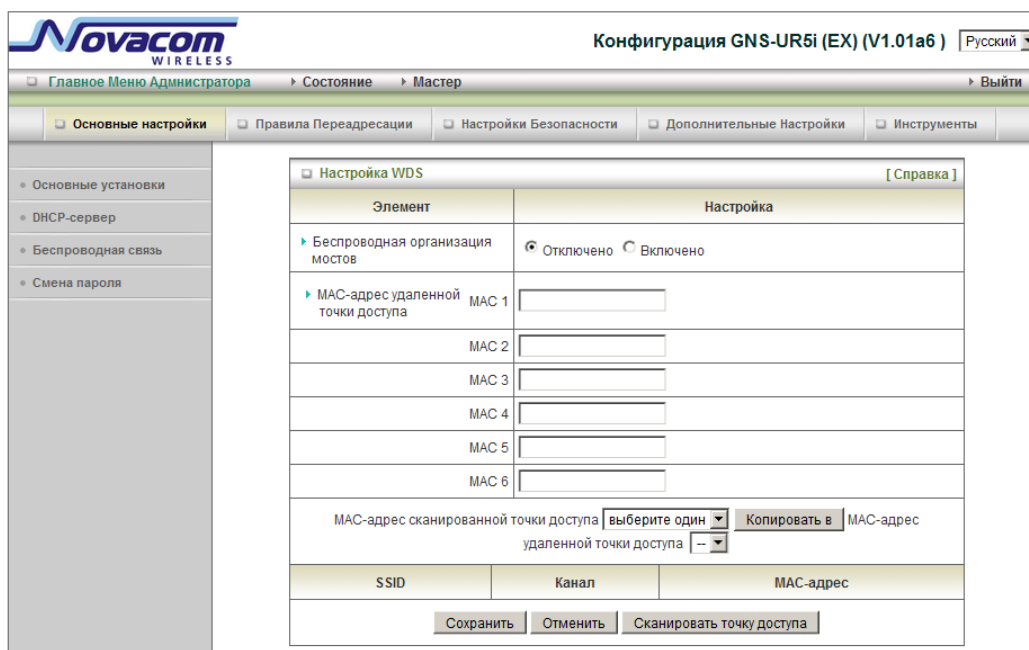
1. IP-адрес или доменное имя 802.1X сервера.
2. Выберите тип шифрования и ключ в RADIUS -IP сервера / Порт / Общий

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)

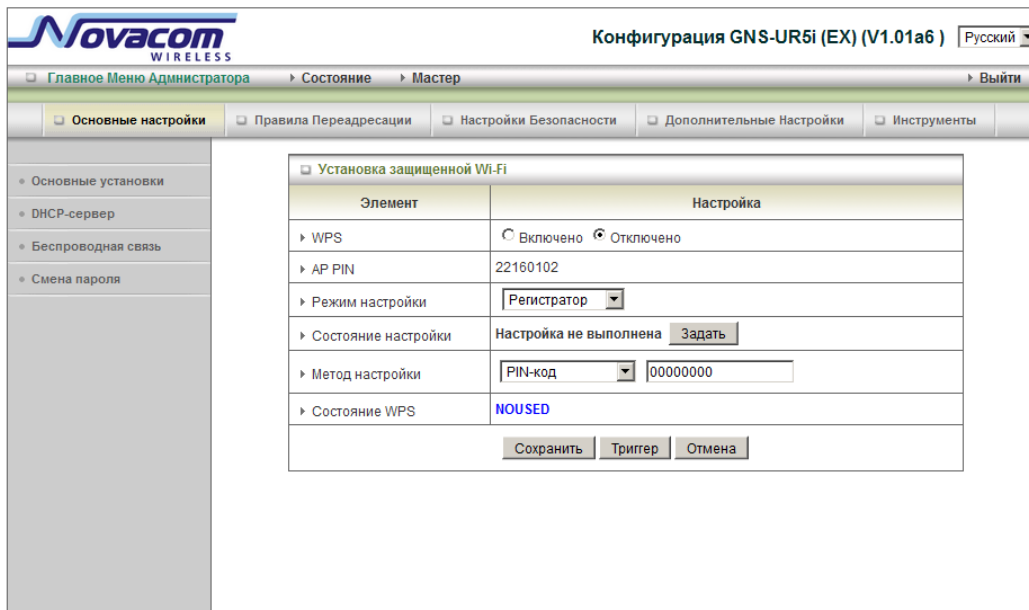
Согласно стандартам IEEE802.11 операция WDS становится доступной. Используя WDS возможно установить беспроводное соединение с точками доступа и таким образом расширить проводную инфраструктуру до тех областей, где использование кабеля невозможно или неэффективно.



Элемент	Настройка
Беспроводная организация мостов	<input checked="" type="radio"/> Отключено <input type="radio"/> Включено
MAC-адрес удаленной точки доступа	MAC 1 <input type="text"/>
	MAC 2 <input type="text"/>
	MAC 3 <input type="text"/>
	MAC 4 <input type="text"/>
	MAC 5 <input type="text"/>
	MAC 6 <input type="text"/>
MAC-адрес сканированной точки доступа <input type="text"/> <input type="button" value="выберите один"/> <input type="button" value="Копировать в"/> MAC-адрес удаленной точки доступа <input type="text"/>	
SSID	Канал
MAC-адрес	
<input type="button" value="Сохранить"/> <input type="button" value="Отменить"/> <input type="button" value="Сканировать точку доступа"/>	

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.



The screenshot shows the configuration interface for a Novacom GNS-UR5i (EX) router. The title bar indicates the version is V1.01a6 and the language is Russian. The main menu includes options like 'Главное Меню Администратора', 'Состояние', 'Мастер', and 'Выйти'. The 'Основные настройки' (Basic Settings) tab is selected, showing a sidebar with 'Основные установки', 'DHCP-сервер', 'Беспроводная связь', and 'Смена пароля'. The 'Установка защищенной Wi-Fi' (WPS Setup) section is active, displaying a table of settings.

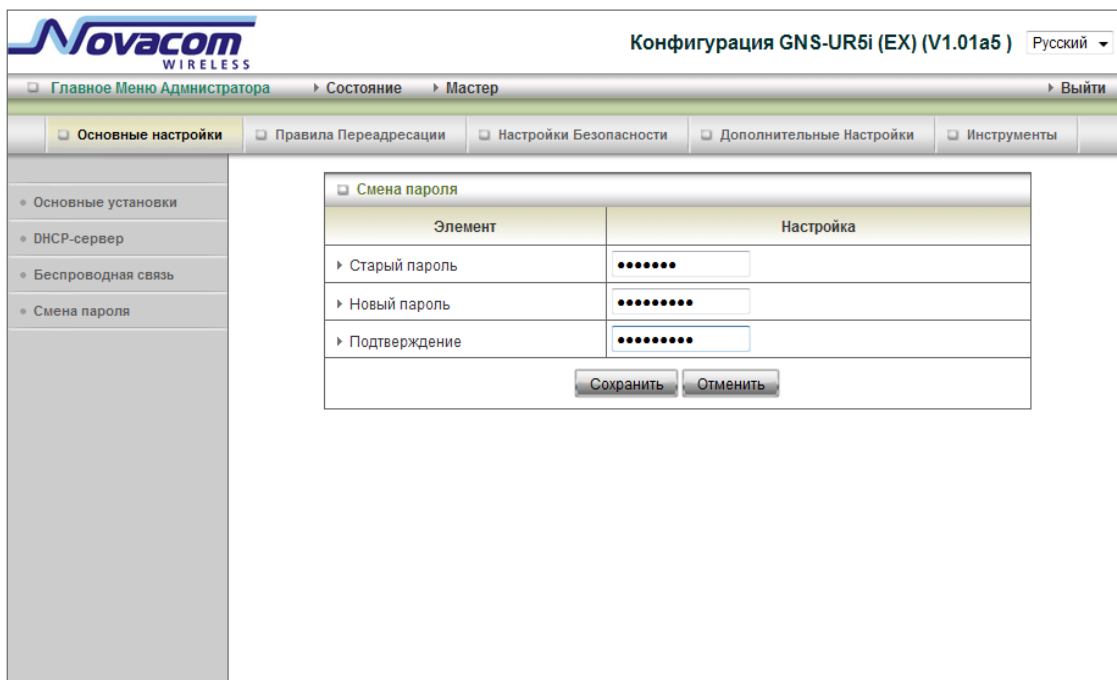
Элемент	Настройка
WPS	<input type="radio"/> Включено <input checked="" type="radio"/> Отключено
AP PIN	22160102
Режим настройки	Регистратор
Состояние настройки	Настройка не выполнена Задать
Метод настройки	PIN-код <input type="text" value="00000000"/>
Состояние WPS	NOUSED

At the bottom of the table are buttons: [Сохранить](#), [Триггер](#), and [Отмена](#).

Список клиентов беспроводного соединения

Здесь указываются все клиенты беспроводного соединения.

3.2.1.5 Смена пароля



The screenshot shows the configuration page for a Novacom GNS-UR5i (EX) router. The page title is "Конфигурация GNS-UR5i (EX) (V1.01a5)" with a language dropdown set to "Русский". The navigation menu includes "Главное Меню Администратора", "Состояние", "Мастер", and "Выйти". The main menu has tabs for "Основные настройки", "Правила Переадресации", "Настройки Безопасности", "Дополнительные Настройки", and "Инструменты". The left sidebar lists configuration categories: "Основные установки", "DHCP-сервер", "Беспроводная связь", and "Смена пароля". The "Смена пароля" section is active, displaying a table with two columns: "Элемент" and "Настройка".

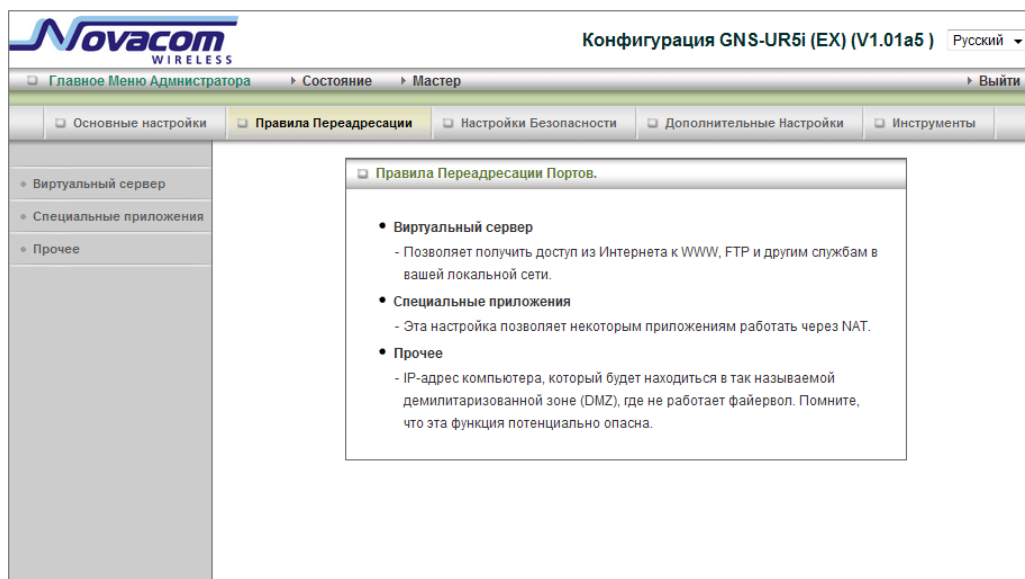
Элемент	Настройка
Старый пароль
Новый пароль
Подтверждение

At the bottom of the form are two buttons: "Сохранить" and "Отменить".

Здесь Вы можете изменить пароль. Мы **настоятельно** рекомендуем Вам сменить 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

Конфигурация GNS-UR5i (EX) (V1.01a5) Русский

Главное Меню Администратора > Состояние > Мастер > Выйти

Основные настройки Правила Переадресации Настройки Безопасности Дополнительные Настройки Инструменты

Виртуальный сервер [Справка]

Известные службы выберите один Копировать в ID --

Правило расписания Всегда включено

Идентификатор (ID)	Служебные Порты	IP-адрес сервера	Включено	Правило расписания#
1	80	10.1.2.50 : 80	<input checked="" type="checkbox"/>	0
2		10.1.2. :	<input type="checkbox"/>	0
3		10.1.2. :	<input type="checkbox"/>	0
4		10.1.2. :	<input type="checkbox"/>	0
5		10.1.2. :	<input type="checkbox"/>	0
6		10.1.2. :	<input type="checkbox"/>	0
7		10.1.2. :	<input type="checkbox"/>	0
8		10.1.2. :	<input type="checkbox"/>	0
9		10.1.2. :	<input type="checkbox"/>	0
10		10.1.2. :	<input type="checkbox"/>	0
11		10.1.2. :	<input type="checkbox"/>	0
12		10.1.2. :	<input type="checkbox"/>	0

Сохранить Отменить

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.

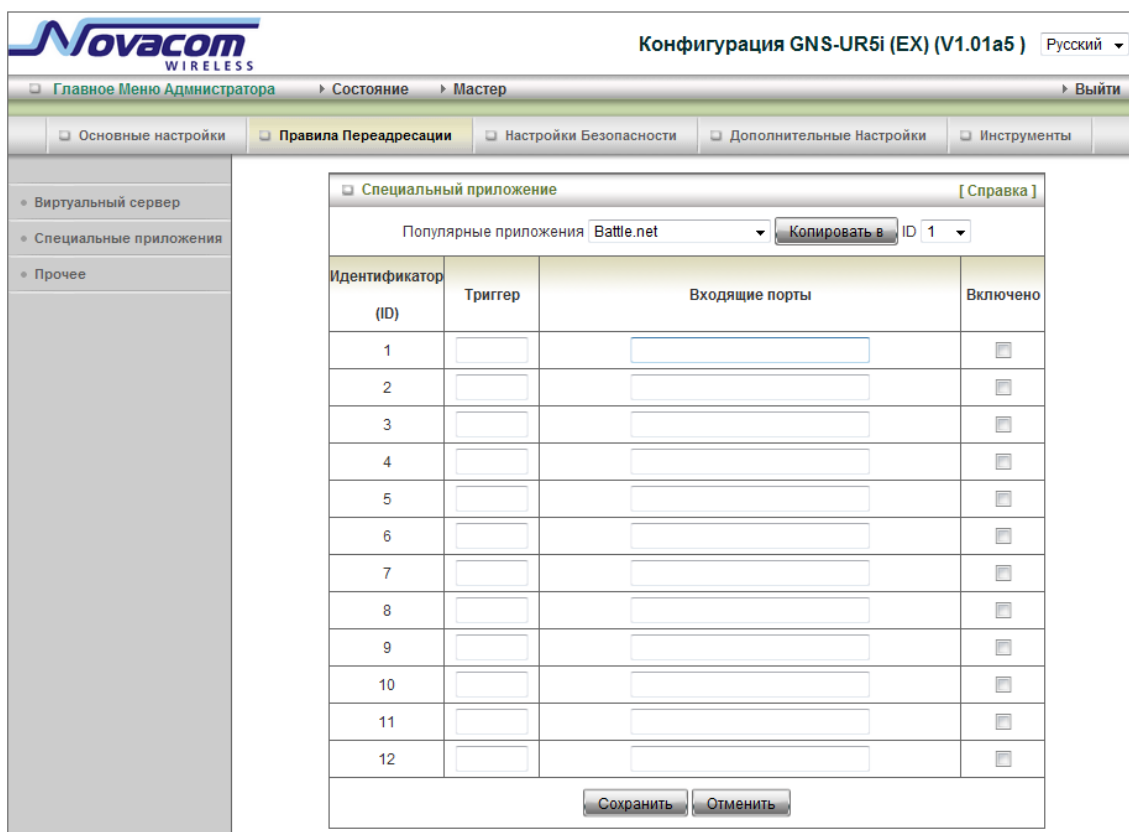
Виртуальный сервер определяется как Служебный порт и все запросы на этот порт переадресовываются на компьютер, определяемый через IP адрес сервера. Virtual Server может работать по графику, и давать пользователю большую гибкость в контроле доступа. Для более полной информации обратитесь к разделу «График».

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



Идентификатор (ID)	Триггер	Входящие порты	Включено
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
11	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
12	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

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, попробуйте 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.

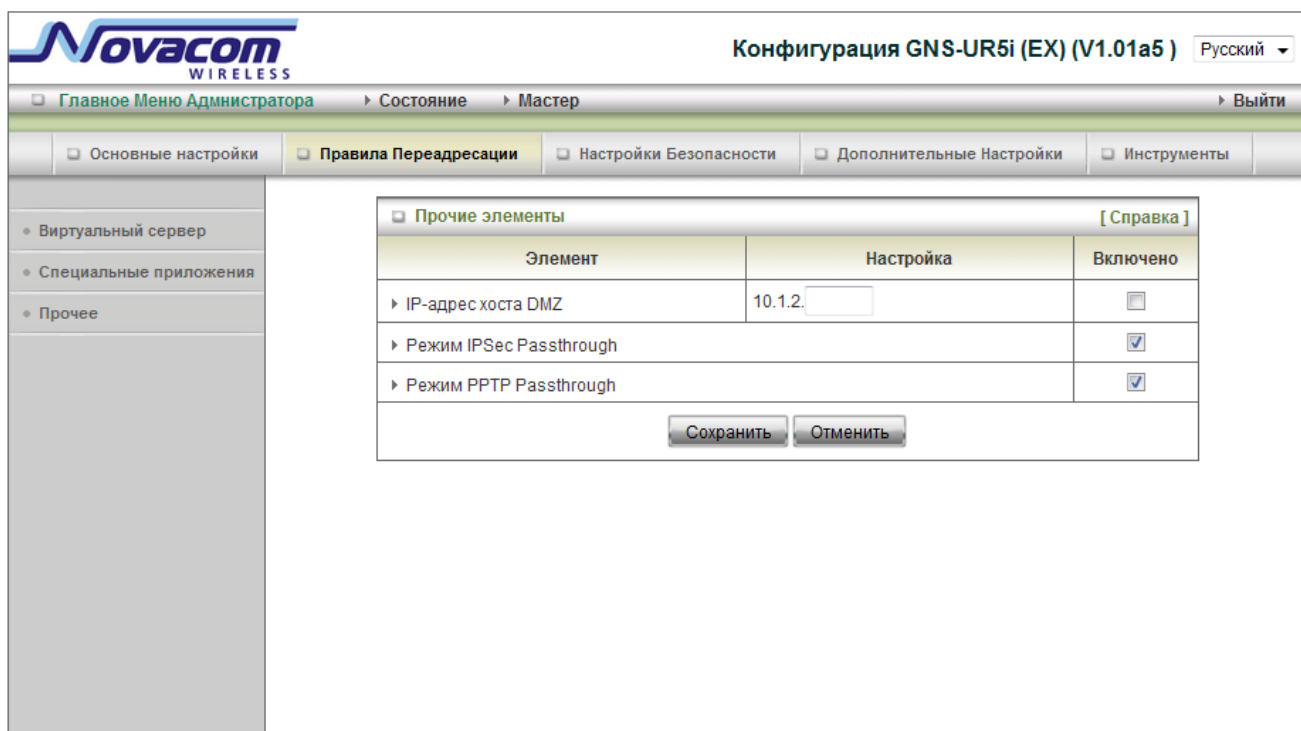
Некоторые настройки на данном оборудовании уже заданы.

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



Novacom WIRELESS

Конфигурация GNS-UR5i (EX) (V1.01a5) Русский

Главное Меню Администратора Состояние Мастер Выйти

Основные настройки Правила Переадресации Настройки Безопасности Дополнительные Настройки Инструменты

Виртуальный сервер
Специальные приложения
Прочее

Прочие элементы [Справка]

Элемент	Настройка	Включено
IP-адрес хоста DMZ	10.1.2.	<input type="checkbox"/>
Режим IPSec Passthrough		<input checked="" type="checkbox"/>
Режим PPTP Passthrough		<input checked="" type="checkbox"/>

Сохранить Отменить

1. IP адрес DMZ хоста

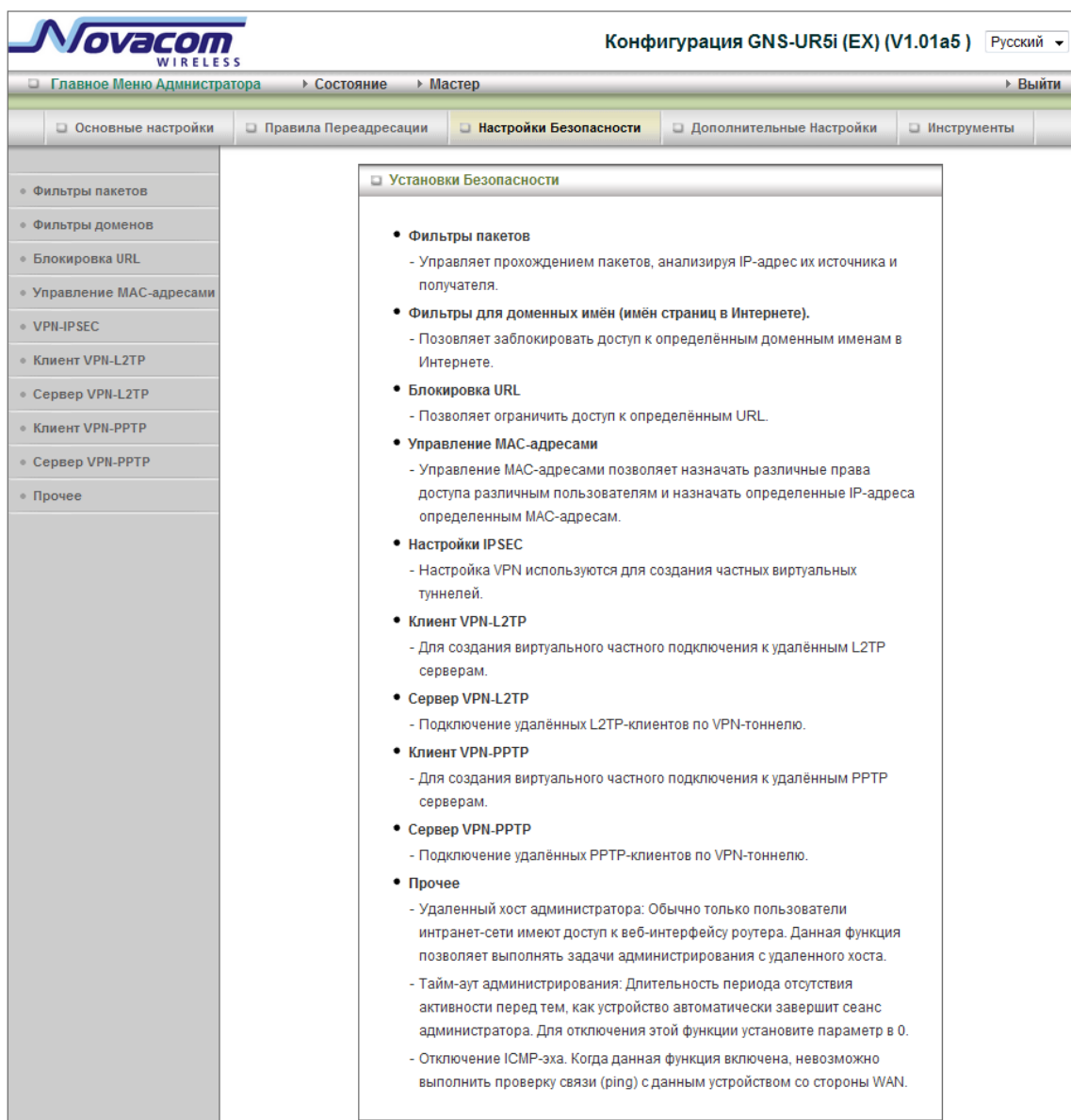
Хост DMZ (Демилитаризованная зона) это хост без защиты firewall. Он позволяет компьютеру устанавливать неограниченную 2-стороннюю связь для интернет-игр, видеоконференций, интернет-телефонии и других специальных приложений

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



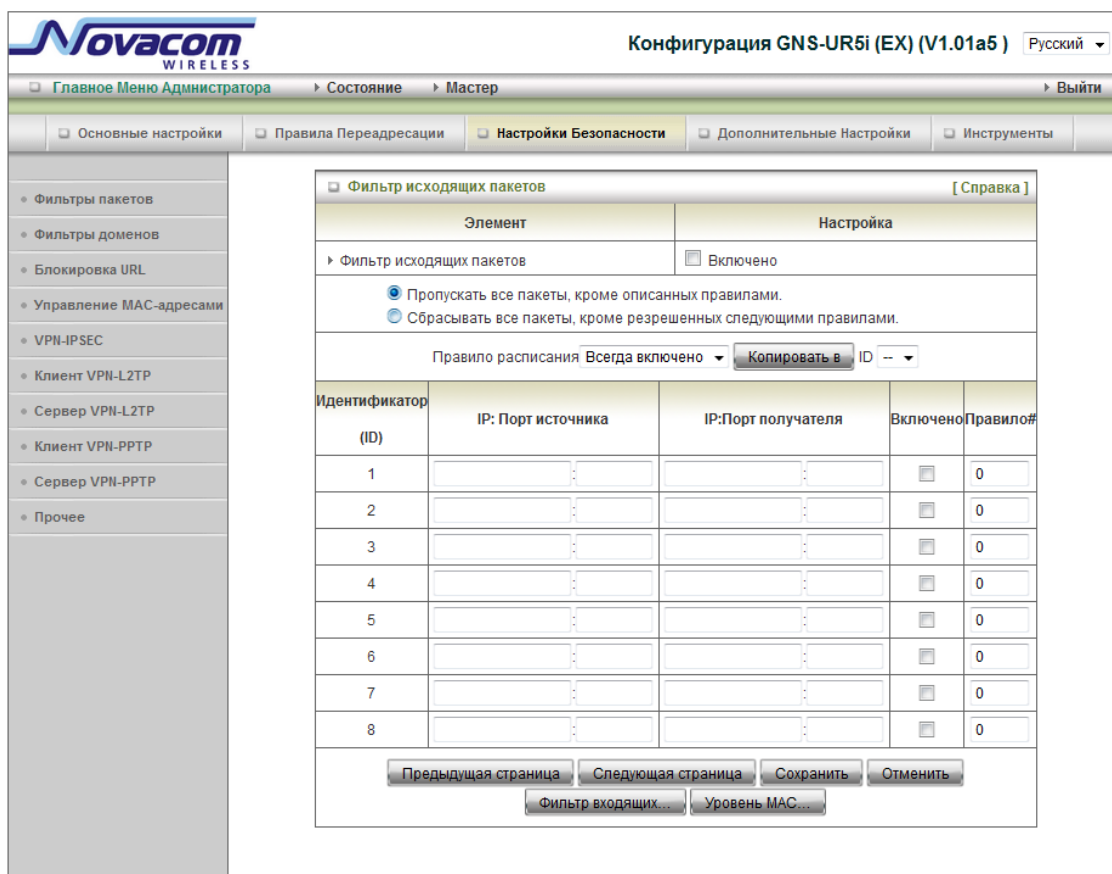
The screenshot displays the configuration web interface for a Novacom GNS-UR5i (EX) router. The page title is "Конфигурация GNS-UR5i (EX) (V1.01a5)" with a language dropdown set to "Русский". The navigation bar includes "Главное Меню Администратора", "Состояние", "Мастер", and "Выйти". The main menu has tabs for "Основные настройки", "Правила Переадресации", "Настройки Безопасности" (selected), "Дополнительные Настройки", and "Инструменты".

On the left, a sidebar lists security-related options: "Фильтры пакетов", "Фильтры доменов", "Блокировка URL", "Управление MAC-адресами", "VPN-IPSEC", "Клиент VPN-L2TP", "Сервер VPN-L2TP", "Клиент VPN-PPTP", "Сервер VPN-PPTP", and "Прочее".

The main content area is titled "Установки Безопасности" and contains a list of security features with brief descriptions:

- Фильтры пакетов**
 - Управляет прохождением пакетов, анализируя IP-адрес их источника и получателя.
- Фильтры для доменных имён (имён страниц в Интернете).**
 - Позволяет заблокировать доступ к определённым доменным именам в Интернете.
- Блокировка URL**
 - Позволяет ограничить доступ к определённым URL.
- Управление MAC-адресами**
 - Управление MAC-адресами позволяет назначать различные права доступа различным пользователям и назначать определённые IP-адреса определённым MAC-адресам.
- Настройки IPSEC**
 - Настройка VPN используются для создания частных виртуальных туннелей.
- Клиент VPN-L2TP**
 - Для создания виртуального частного подключения к удалённым L2TP серверам.
- Сервер VPN-L2TP**
 - Подключение удалённых L2TP-клиентов по VPN-туннелю.
- Клиент VPN-PPTP**
 - Для создания виртуального частного подключения к удалённым PPTP серверам.
- Сервер VPN-PPTP**
 - Подключение удалённых PPTP-клиентов по VPN-туннелю.
- Прочее**
 - Удаленный хост администратора: Обычно только пользователи интранет-сети имеют доступ к веб-интерфейсу роутера. Данная функция позволяет выполнять задачи администрирования с удаленного хоста.
 - Тайм-аут администрирования: Длительность периода отсутствия активности перед тем, как устройство автоматически завершит сеанс администратора. Для отключения этой функции установите параметр в 0.
 - Отключение ICMP-эха. Когда данная функция включена, невозможно выполнить проверку связи (ping) с данным устройством со стороны WAN.

3.2.3.1 Фильтрация пакетов



The screenshot shows the configuration page for 'Фильтр исходящих пакетов' (Outgoing packet filter). The interface includes a sidebar with navigation links and a main content area with a table for configuring rules.

Фильтр исходящих пакетов [Справка]

Элемент	Настройка
Фильтр исходящих пакетов	<input type="checkbox"/> Включено
<input checked="" type="radio"/> Пропускать все пакеты, кроме описанных правилами.	
<input type="radio"/> Сбрасывать все пакеты, кроме разрешенных следующими правилами.	
Правило расписания: Всегда включено <input type="button" value="Копировать в ID --"/>	

Идентификатор (ID)	IP: Порт источника	IP: Порт получателя	Включено	Правило#
1			<input type="checkbox"/>	0
2			<input type="checkbox"/>	0
3			<input type="checkbox"/>	0
4			<input type="checkbox"/>	0
5			<input type="checkbox"/>	0
6			<input type="checkbox"/>	0
7			<input type="checkbox"/>	0
8			<input type="checkbox"/>	0

Buttons: Предыдущая страница, Следующая страница, Сохранить, Отменить, Фильтр входящих..., Уровень MAC...

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 #

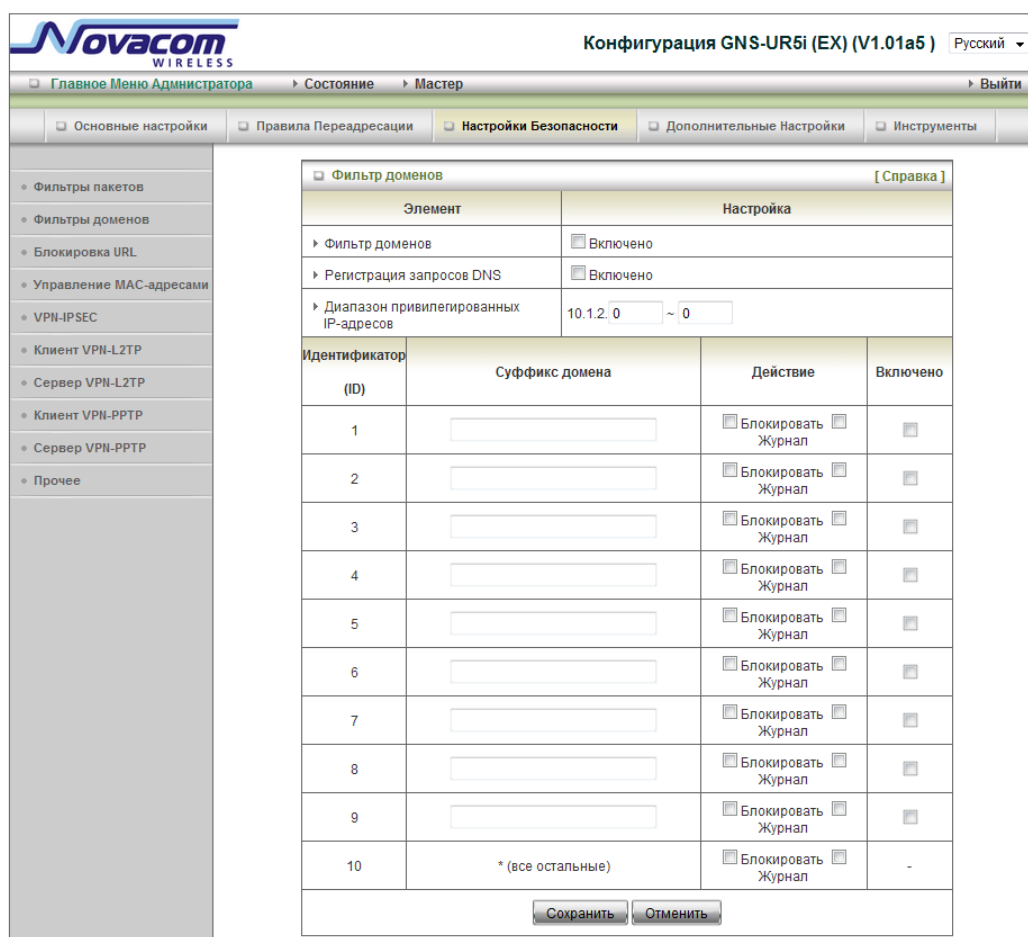
Для исходного IP адреса или адреса назначения, Вы можете определить единственный IP адрес (4.3.2.1) или ряд IP адресов (4.3.2.1-4.3.2.254). Пустое значение подразумевает все IP адреса.

Для исходного порта или порта назначения, Вы можете определить единственный порт (80) или ряд портов (1000-1999). Добавьте префикс "Т" или "U" для определения TCP или UDP протокола. Например, Т80, 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



Конфигурация GNS-UR5i (EX) (V1.01a5) Русский

Главное Меню Администратора > Состояние > Мастер > Выйти

Основные настройки > Правила Переадресации > **Настройки Безопасности** > Дополнительные Настройки > Инструменты

Фильтры пакетов
Фильтры доменов
Блокировка URL
Управление MAC-адресами
VPN-IPSEC
Клиент VPN-L2TP
Сервер VPN-L2TP
Клиент VPN-PPTP
Сервер VPN-PPTP
Прочее

Фильтр доменов [Справка]

Элемент	Настройка
Фильтр доменов	<input type="checkbox"/> Включено
Регистрация запросов DNS	<input type="checkbox"/> Включено
Диапазон привилегированных IP-адресов	10.1.2.0 ~ 0

Идентификатор (ID)	Суффикс домена	Действие	Включено
1		<input type="checkbox"/> Блокировать <input type="checkbox"/> Журнал	<input type="checkbox"/>
2		<input type="checkbox"/> Блокировать <input type="checkbox"/> Журнал	<input type="checkbox"/>
3		<input type="checkbox"/> Блокировать <input type="checkbox"/> Журнал	<input type="checkbox"/>
4		<input type="checkbox"/> Блокировать <input type="checkbox"/> Журнал	<input type="checkbox"/>
5		<input type="checkbox"/> Блокировать <input type="checkbox"/> Журнал	<input type="checkbox"/>
6		<input type="checkbox"/> Блокировать <input type="checkbox"/> Журнал	<input type="checkbox"/>
7		<input type="checkbox"/> Блокировать <input type="checkbox"/> Журнал	<input type="checkbox"/>
8		<input type="checkbox"/> Блокировать <input type="checkbox"/> Журнал	<input type="checkbox"/>
9		<input type="checkbox"/> Блокировать <input type="checkbox"/> Журнал	<input type="checkbox"/>
10	* (все остальные)	<input type="checkbox"/> Блокировать <input type="checkbox"/> Журнал	-

Сохранить Отменить

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**

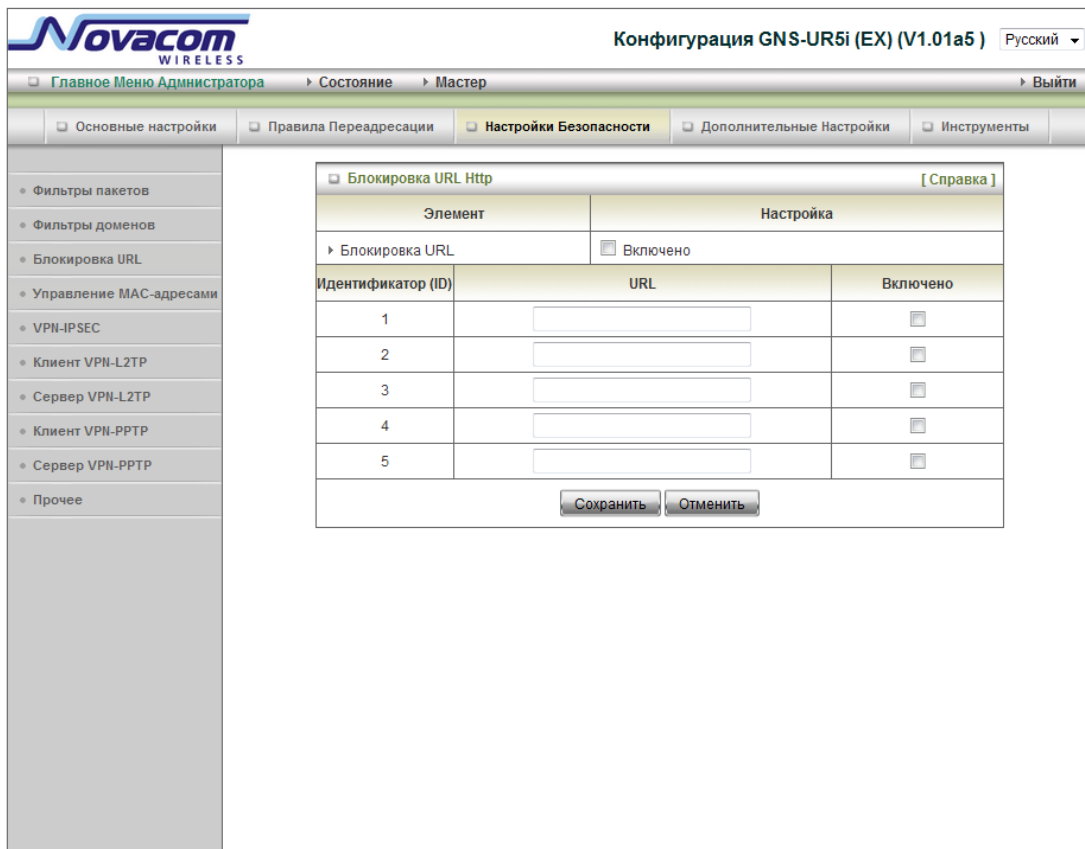
Когда кто-либо получает доступ к адресу URL, где встречается запрещенный доменный суффикс — какое действие должна произвести система? Отметьте «прекратить», если Вы хотите блокировать доступ. Отметьте «зарегистрировать», если Вы хотите зарегистрировать этот доступ.

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



The screenshot shows the configuration interface for a Novacom GNS-UR5i (EX) router. The title bar indicates the version is V1.01a5 and the language is Russian. The main menu includes 'Главное Меню Администратора', 'Состояние', 'Мастер', and 'Выйти'. The 'Настройки Безопасности' (Security Settings) tab is selected, showing options for 'Основные настройки', 'Правила Переадресации', 'Настройки Безопасности', 'Дополнительные Настройки', and 'Инструменты'. On the left, a sidebar lists various security features: 'Фильтры пакетов', 'Фильтры доменов', 'Блокировка URL', 'Управление MAC-адресами', 'VPN-IPSEC', 'Клиент VPN-L2TP', 'Сервер VPN-L2TP', 'Клиент VPN-PPTP', 'Сервер VPN-PPTP', and 'Прочее'. The 'Блокировка URL Http' section is active, displaying a table for configuring URL blocking rules. The table has columns for 'Элемент' (Element), 'Настройка' (Setting), 'Идентификатор (ID)' (Identifier), 'URL', and 'Включено' (Enabled). The 'Включено' checkbox is checked. Below the table are 'Сохранить' (Save) and 'Отменить' (Cancel) buttons.

Элемент	Настройка
Блокировка URL	<input checked="" type="checkbox"/> Включено

Идентификатор (ID)	URL	Включено
1	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>

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.

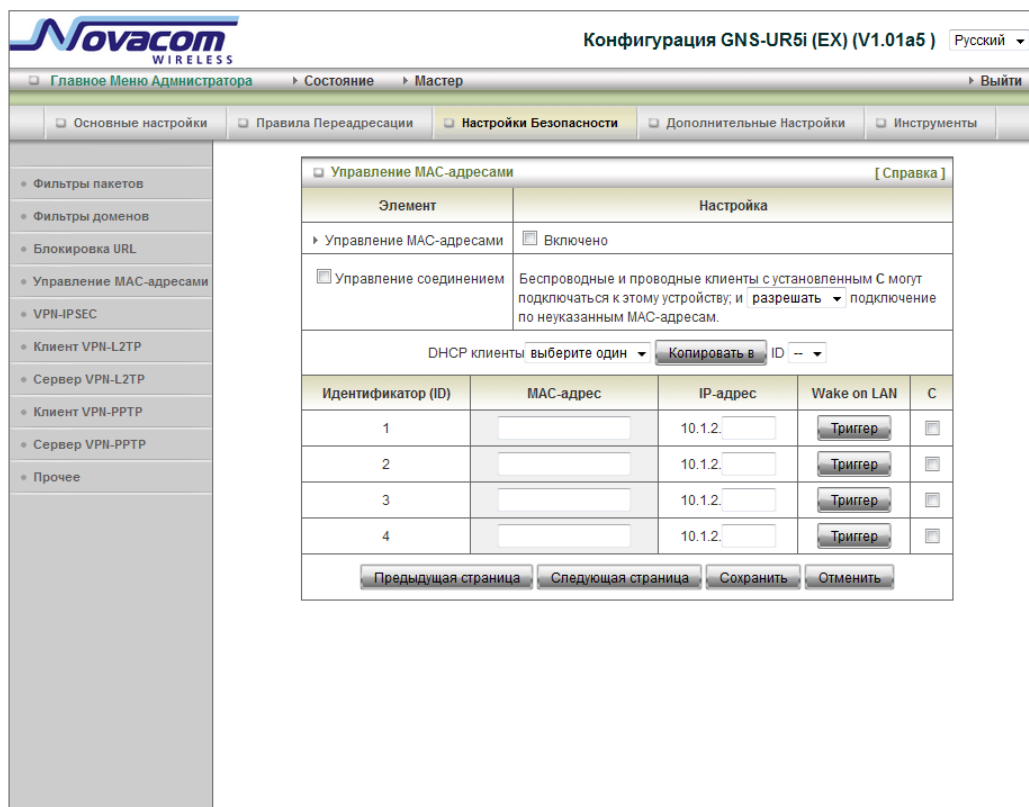
Например, Вы можете использовать ключевое слово «секс», чтобы заблокировать все вебсайты, если их URL содержат ключевое слово «секс»

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



The screenshot shows the configuration page for the Novacom GNS-UR5i (EX) router. The page title is "Конфигурация GNS-UR5i (EX) (V1.01a5)" with a language dropdown set to "Русский". The navigation menu includes "Главное Меню Администратора", "Состояние", "Мастер", and "Выйти". The main menu has tabs for "Основные настройки", "Правила Переадресации", "Настройки Безопасности", "Дополнительные Настройки", and "Инструменты". The left sidebar lists various settings like "Фильтры пакетов", "Фильтры доменов", "Блокировка URL", "Управление MAC-адресами", "VPN-IPSEC", "Клиент VPN-L2TP", "Сервер VPN-L2TP", "Клиент VPN-PPTP", "Сервер VPN-PPTP", and "Прочее". The "Управление MAC-адресами" section is active, showing a table with columns: "Элемент", "Настройка", "Идентификатор (ID)", "MAC-адрес", "IP-адрес", "Wake on LAN", and "C". The table contains 4 rows of configuration data.

Элемент	Настройка
Управление MAC-адресами	<input checked="" type="checkbox"/> Включено
Управление соединением	Беспроводные и проводные клиенты с установленным С могут подключаться к этому устройству, и разрешать подключение по неуказанным MAC-адресам.

DHCP клиенты: выберите один ID

Идентификатор (ID)	MAC-адрес	IP-адрес	Wake on LAN	C
1	<input type="text"/>	10.1.2.	<input type="button" value="Триггер"/>	<input type="checkbox"/>
2	<input type="text"/>	10.1.2.	<input type="button" value="Триггер"/>	<input type="checkbox"/>
3	<input type="text"/>	10.1.2.	<input type="button" value="Триггер"/>	<input type="checkbox"/>
4	<input type="text"/>	10.1.2.	<input type="button" value="Триггер"/>	<input type="checkbox"/>

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 отказано 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

Novacom WIRELESS Конфигурация GNS-UR5i (EX) (V1.01a5) Русский

Главное Меню Администратора > Состояние > Мастер > Выйти

Основные настройки Правила Переадресации **Настройки Безопасности** Дополнительные Настройки Инструменты

Фильтры пакетов
Фильтры доменов
Блокировка URL
Управление MAC-адресами
VPN-IPSEC
Клиент VPN-L2TP
Сервер VPN-L2TP
Клиент VPN-PPTP
Сервер VPN-PPTP
Прочее

Клиент PPTP

Элемент Настройка

VPN-PPTP ☒ Включено

Идентификатор (ID)	Включено	Имя	IP-адрес или домен узла	Имя пользователя	Пароль	Маршрут	Подключить	Выбор
1	<input checked="" type="checkbox"/>	Deficator	83.243.23.45	Name	0.0.0.0/0	<input checked="" type="radio"/> По требованию <input checked="" type="radio"/> Авто <input type="radio"/> Вручную	<input checked="" type="checkbox"/> MPPE <input checked="" type="checkbox"/> NAT
2	<input type="checkbox"/>					0.0.0.0/0	<input type="radio"/> По требованию <input type="radio"/> Авто <input type="radio"/> Вручную	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT
3	<input type="checkbox"/>					0.0.0.0/0	<input type="radio"/> По требованию <input type="radio"/> Авто <input type="radio"/> Вручную	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT
4	<input type="checkbox"/>					0.0.0.0/0	<input type="radio"/> По требованию <input type="radio"/> Авто <input type="radio"/> Вручную	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT
5	<input type="checkbox"/>					0.0.0.0/0	<input type="radio"/> По требованию <input type="radio"/> Авто <input type="radio"/> Вручную	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT
Идентификатор (ID)	Состояние подключения		Локальный IP	Удаленный IP-адрес	Действие			
<input type="button" value="Сохранить"/> <input type="button" value="Отменить"/> <input type="button" value="Обновить"/>								

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:

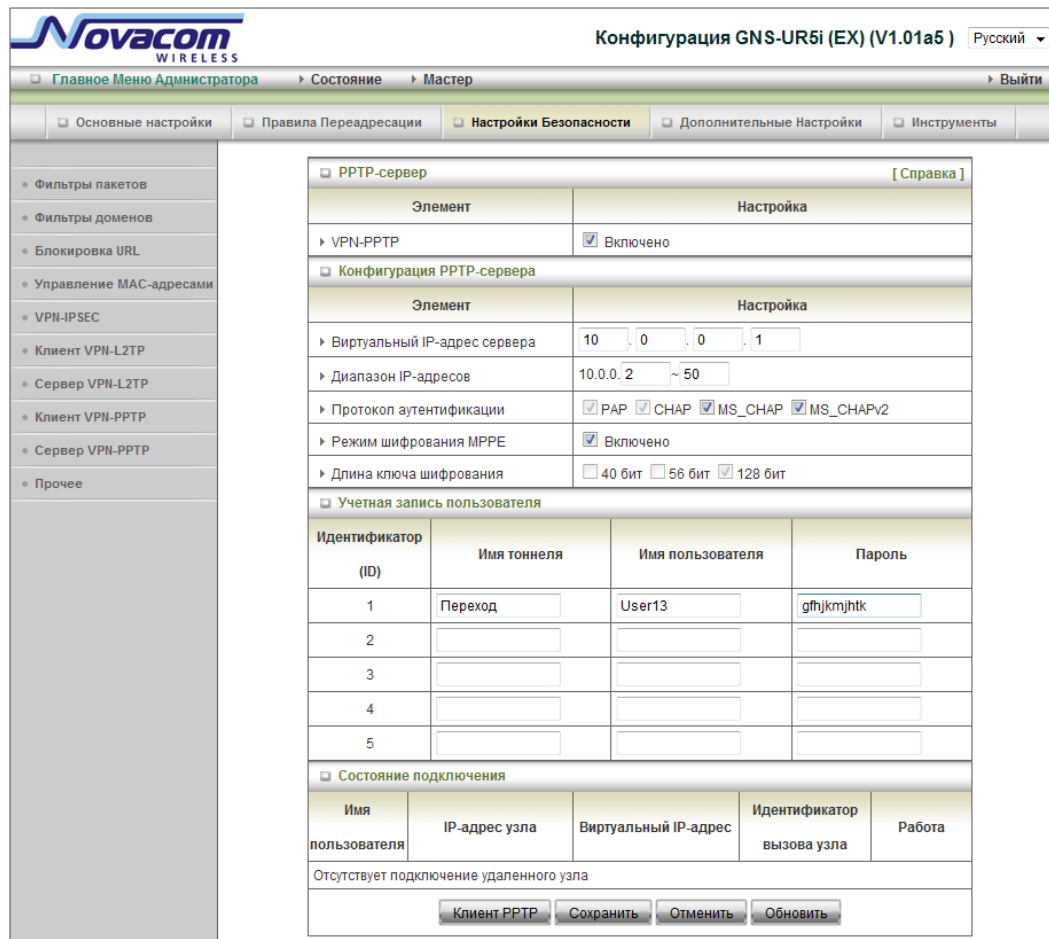
По запросу: Устройство будет связываться с провайдером при отправлении клиентами исходящих пакетов.

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



The screenshot shows the configuration page for the PPTP server. The interface includes a sidebar with navigation options and a main content area with various settings.

Панель навигации (слева):

- Фильтры пакетов
- Фильтры доменов
- Блокировка URL
- Управление MAC-адресами
- VPN-IPSEC
- Клиент VPN-L2TP
- Сервер VPN-L2TP
- Клиент VPN-PPTP
- Сервер VPN-PPTP
- Прочее

Заголовок: Конфигурация GNS-UR5i (EX) (V1.01a5) | Русский

Вкладки: Основные настройки, Правила Переадресации, **Настройки Безопасности**, Дополнительные Настройки, Инструменты

Настройка VPN-PPTP:

Элемент	Настройка
VPN-PPTP	<input checked="" type="checkbox"/> Включено

Конфигурация PPTP-сервера:

Элемент	Настройка
Виртуальный IP-адрес сервера	10 . 0 . 0 . 1
Диапазон IP-адресов	10.0.0.2 ~ 50
Протокол аутентификации	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MS_CHAP <input checked="" type="checkbox"/> MS_CHAPv2
Режим шифрования MPPE	<input checked="" type="checkbox"/> Включено
Длина ключа шифрования	<input type="checkbox"/> 40 бит <input type="checkbox"/> 56 бит <input checked="" type="checkbox"/> 128 бит

Учетная запись пользователя:

Идентификатор (ID)	Имя туннеля	Имя пользователя	Пароль
1	Переход	User13	gfhjkmjhtk
2			
3			
4			
5			

Состояние подключения:

Имя пользователя	IP-адрес узла	Виртуальный IP-адрес	Идентификатор вызова узла	Работа
Отсутствует подключение удаленного узла				

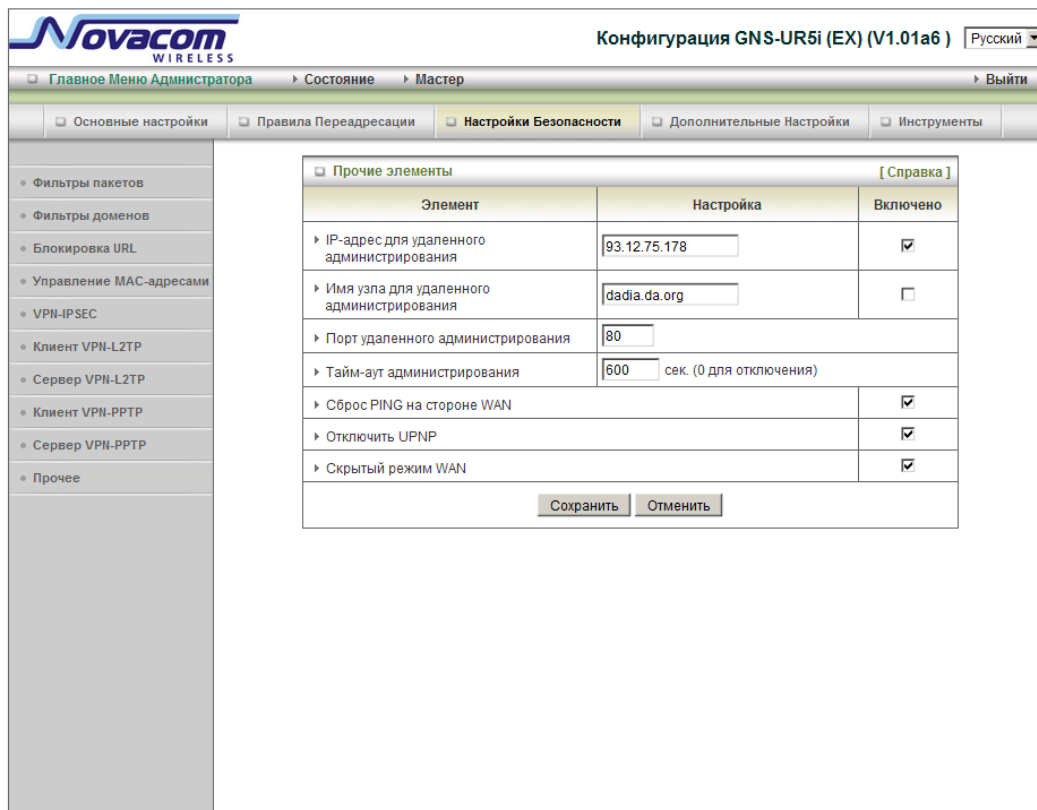
Кнопки: Клиент PPTP, Сохранить, Отменить, Обновить

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



Элемент	Настройка	Включено
IP-адрес для удаленного администрирования	93.12.75.178	<input checked="" type="checkbox"/>
Имя узла для удаленного администрирования	dadia.da.org	<input type="checkbox"/>
Порт удаленного администрирования	80	
Тайм-аут администрирования	600 сек. (0 для отключения)	
Сброс PING на стороне WAN		<input checked="" type="checkbox"/>
Отключить UPNP		<input checked="" type="checkbox"/>
Скрытый режим WAN		<input checked="" type="checkbox"/>

Сохранить Отменить

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**

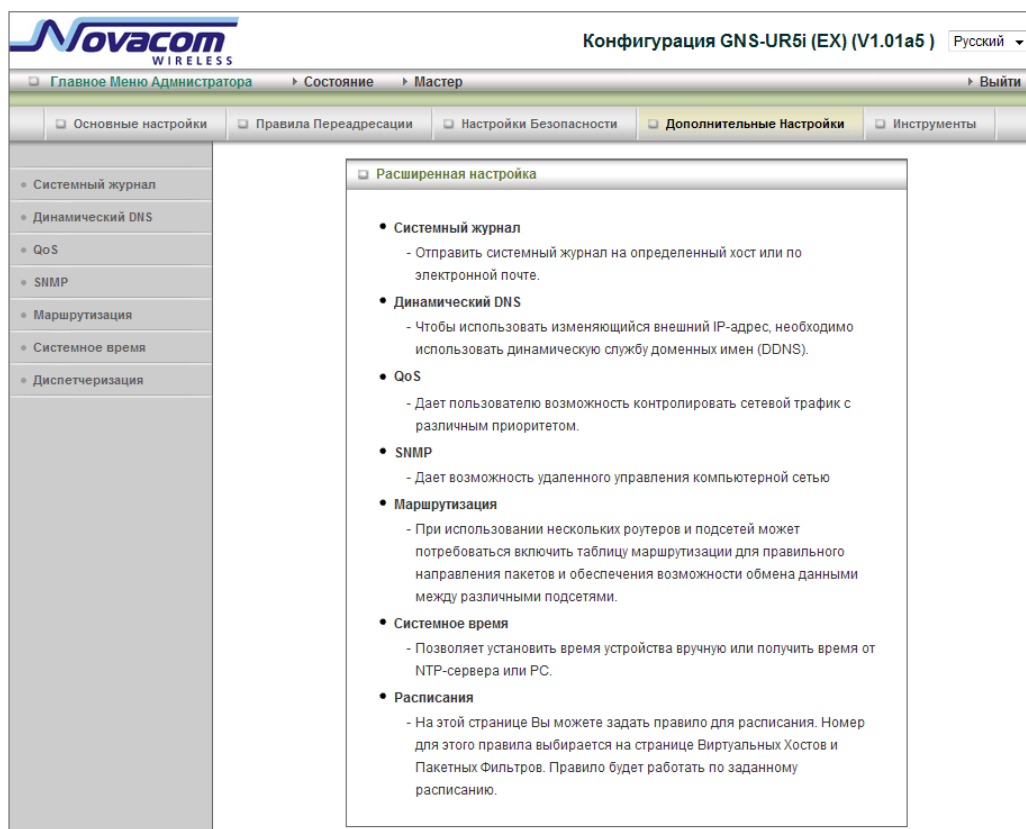
Устройство может отключить функцию UPNP. Если Ваша операционная система поддерживает функцию UPNP, поищите ее и она подключится, например в Windows XP. Вы можете получить IP устройства через UPNP.

5. **Держать WAN в скрытом режиме**

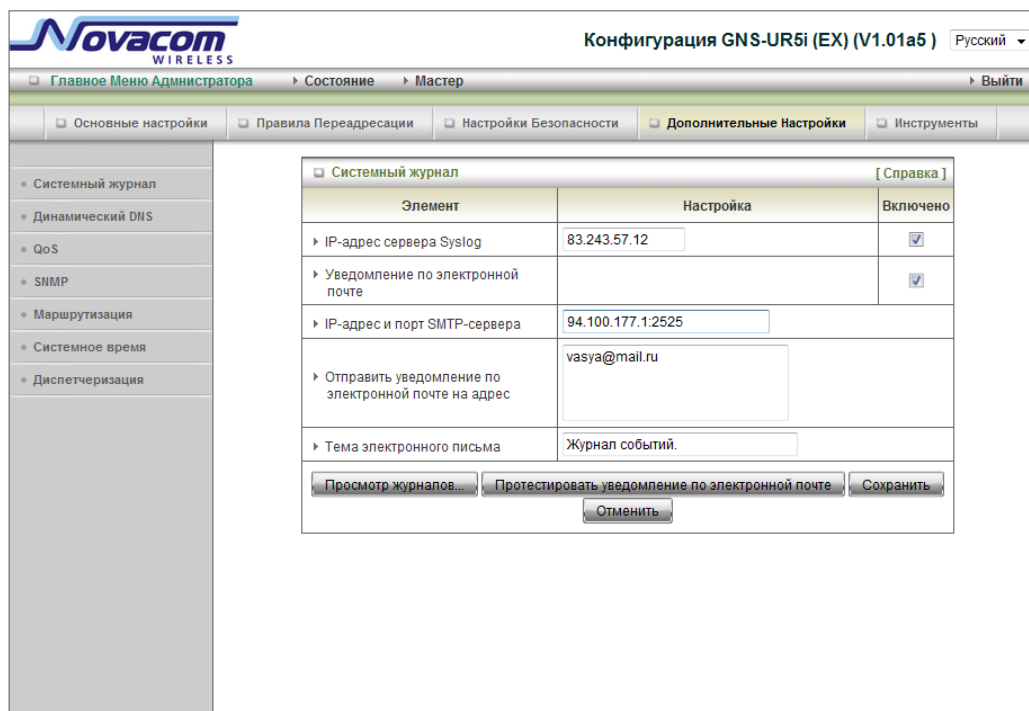
Если порт закрыт, устройство игнорирует входящие попытки соединения, а не отклоняет их.

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

3.2.4 Дополнительные настройки.



3.2.4.1 Системный журнал



Элемент	Настройка	Включено
IP-адрес сервера Syslog	83.243.57.12	<input checked="" type="checkbox"/>
Уведомление по электронной почте		<input checked="" type="checkbox"/>
IP-адрес и порт SMTP-сервера	94.100.177.1:2525	
Отправить уведомление по электронной почте на адрес	vasya@mail.ru	
Тема электронного письма	Журнал событий.	

Просмотр журналов... Протестировать уведомление по электронной почте Сохранить Отменить

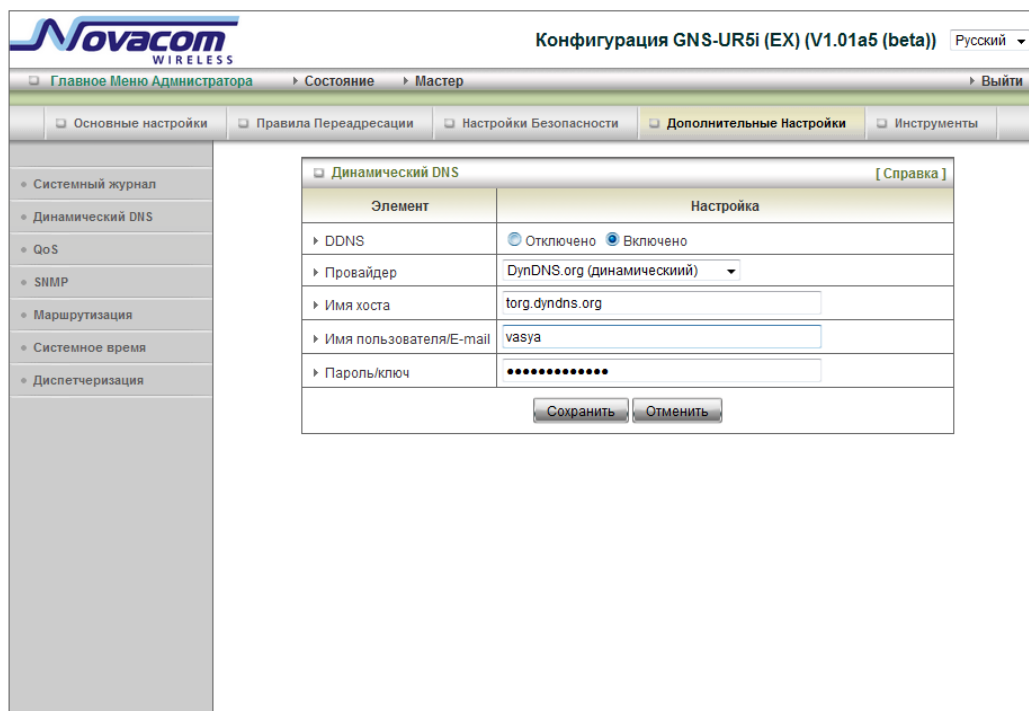
Эта страница поддерживает два метода передачи системных логов для определенных целей: с помощью протокола syslog (UDP) и SMTP(TCP). Вам нужно настроить следующее:

- IP адрес для протокола Syslog**
IP пункта назначения, куда будет отправляться syslog.
Отметьте «Включить», чтобы включить эту функцию.
- Включить извещения E-mail**
Отметьте, если Вы хотите включить Email оповещения (пересылка syslog по электронной почте).
- IP и порт SMTP сервера**
Введите IP адрес и порт SMTP-сервера 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".
- Посылать извещения E-mail на адрес**
Адресаты, которые будут получать эти логи. Вы можете указать больше одного адресата, разделив адреса точкой с запятой или запятой.
- 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



The screenshot shows the configuration page for Dynamic DNS (DDNS) in the Novacom GNS-UR5i (EX) (V1.01a5 (beta)) web interface. The page is titled "Динамический DNS" and includes a "[Справка]" link. The interface has a sidebar with navigation options: "Системный журнал", "Динамический DNS", "QoS", "SNMP", "Маршрутизация", "Системное время", and "Диспетчеризация". The main content area contains a table with two columns: "Элемент" and "Настройка".

Элемент	Настройка
DDNS	<input type="radio"/> Отключено <input checked="" type="radio"/> Включено
Провайдер	DynDNS.org (динамический)
Имя хоста	torg.dyndns.org
Имя пользователя/E-mail	vasya
Пароль/ключ

At the bottom of the table are two buttons: "Сохранить" and "Отменить".

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. Далее Вы можете ввести необходимую информацию о Вашем сервере DDNS.

Вам нужно указать:

Провайдера

Имя хоста

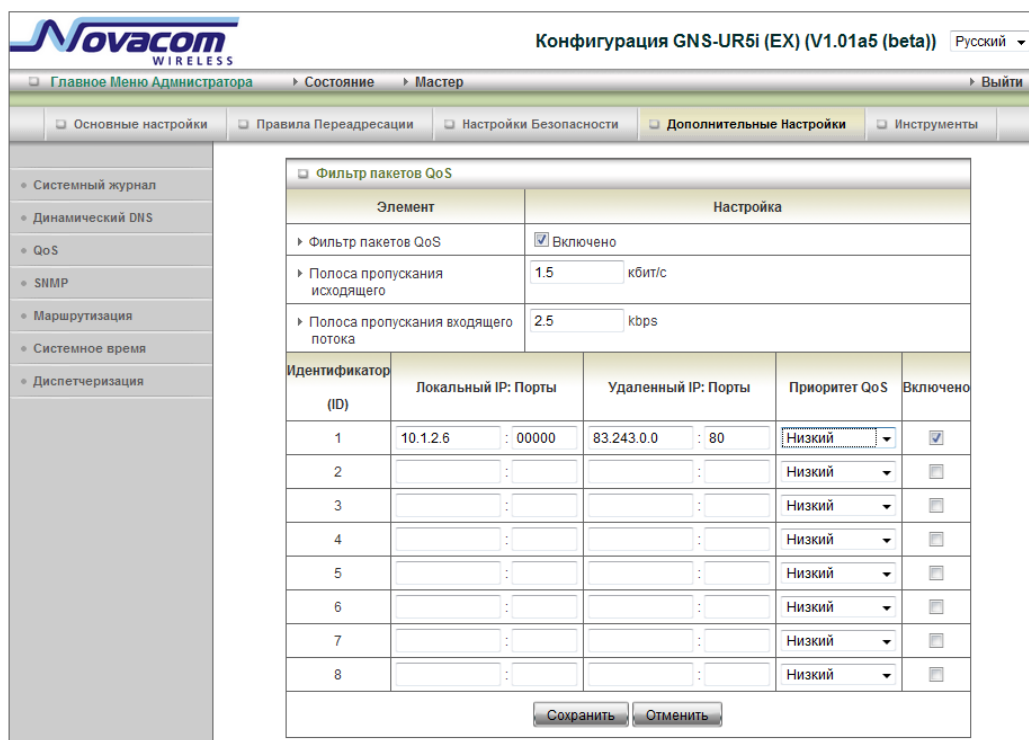
Имя пользователя/E-mail

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)



Элемент	Настройка
Фильтр пакетов QoS	<input checked="" type="checkbox"/> Включено
Полоса пропускания исходящего	1.5 кбит/с
Полоса пропускания входящего потока	2.5 kbps

Идентификатор (ID)	Локальный IP: Порты	Удаленный IP: Порты	Приоритет QoS	Включено
1	10.1.2.6 : 00000	83.243.0.0 : 80	Низкий	<input checked="" type="checkbox"/>
2			Низкий	<input type="checkbox"/>
3			Низкий	<input type="checkbox"/>
4			Низкий	<input type="checkbox"/>
5			Низкий	<input type="checkbox"/>
6			Низкий	<input type="checkbox"/>
7			Низкий	<input type="checkbox"/>
8			Низкий	<input type="checkbox"/>

Сохранить Отменить

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

- Фильтр пакетов QoS**
Этот пункт включает функцию QoS.
- Исходящий поток**
Устанавливает ограничение скорости исходящего потока.
- Входящий поток**
Устанавливает ограничение скорости входящего потока.
- Локальный IP**
Установите здесь значение локального IP адреса.
- Локальные порты**
Установите здесь значение локальных портов.
- Удаленный IP**
Установите здесь значение удаленного IP адреса.
- Удаленные порты**
Установите здесь значение удаленных портов.
- Приоритеты QoS**

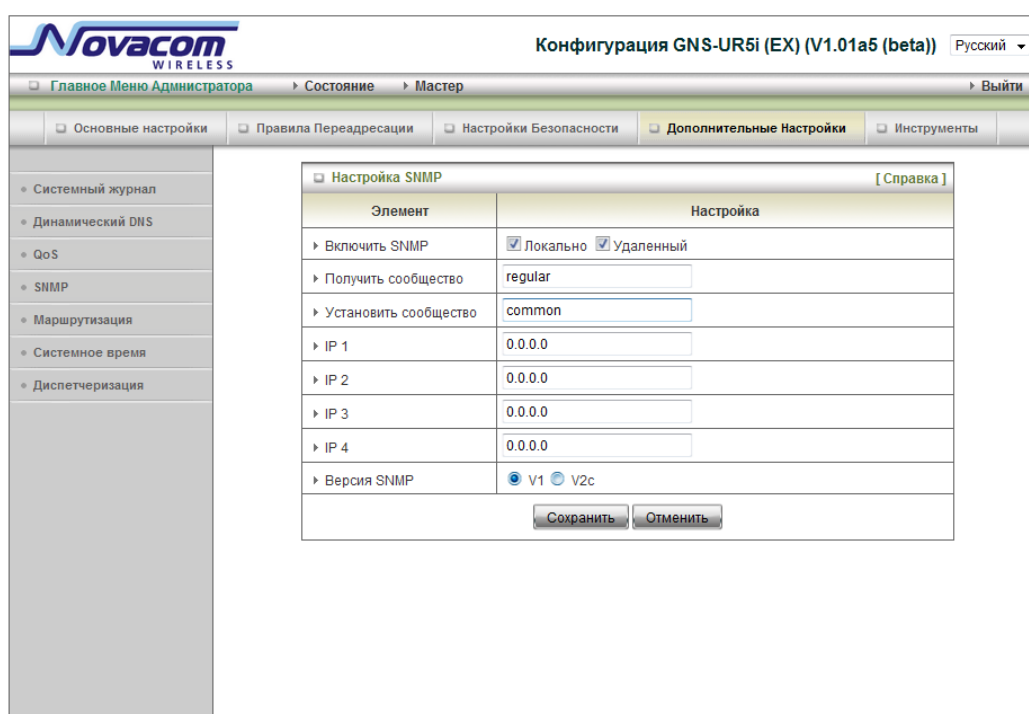
Это определяет уровень приоритета текущей политики конфигурации. Пакеты, связанные с этой политикой, будут обслуживаться на основании уровня приоритета. Для важных приложений рекомендуются Высокие или Нормальные уровни. Для необязательных приложений выберите Низкий уровень.

1. Включить

Отметьте включение для каждого правила.

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

3.2.4.4 SNMP



Элемент	Настройка
Включить SNMP	<input checked="" type="checkbox"/> Локально <input checked="" type="checkbox"/> Удаленный
Получить сообщество	regular
Установить сообщество	common
IP 1	0.0.0.0
IP 2	0.0.0.0
IP 3	0.0.0.0
IP 4	0.0.0.0
Версия SNMP	<input checked="" type="radio"/> V1 <input type="radio"/> V2c

Сохранить Отменить

SNMP, Простой Протокол Управления Сетью, является протоколом, разработанным, чтобы дать пользователю способность удаленно 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 отвечать на запросы из локальной сети (LAN). Если выбран Удаленный, устройство будет отвечать 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

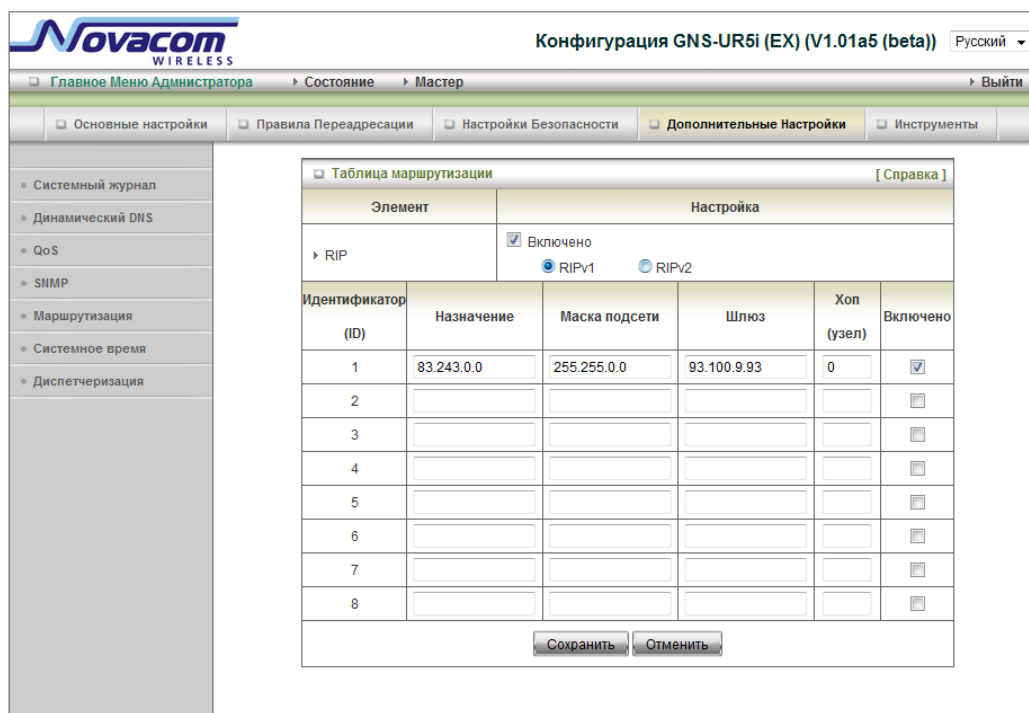
Введите здесь IP компьютеров, с которых будет осуществляться функция SNMP. Пользователь должен настроить путь, по которому устройство будет передавать SNMP сообщения.

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



The screenshot shows the configuration page for the Novacom GNS-UR5i (EX) router. The page title is "Конфигурация GNS-UR5i (EX) (V1.01a5 (beta))". The language is set to "Русский". The navigation menu includes "Главное Меню Администратора", "Состояние", "Мастер", and "Выйти". The main menu has tabs for "Основные настройки", "Правила Переадресации", "Настройки Безопасности", "Дополнительные Настройки", and "Инструменты". The left sidebar lists various settings: "Системный журнал", "Динамический DNS", "QoS", "SNMP", "Маршрутизация", "Системное время", and "Диспетчеризация". The "Маршрутизация" section is active, showing the "Таблица маршрутизации" (Routing Table) configuration. The table has columns for "Элемент" (Element), "Настройка" (Configuration), "Идентификатор (ID)", "Назначение" (Destination), "Маска подсети" (Subnet Mask), "Шлюз" (Gateway), "Хоп (узел)" (Hop (node)), and "Включено" (Enabled). The "RIP" section is expanded, showing "Включено" (Enabled) with radio buttons for "RIPv1" and "RIPv2". Below this is a table with 8 rows for routing entries. The first row is pre-filled with ID 1, Destination 83.243.0.0, Subnet Mask 255.255.0.0, Gateway 93.100.9.93, Hop 0, and Enabled checked. The other rows are empty. At the bottom are "Сохранить" (Save) and "Отменить" (Cancel) buttons.

Элемент	Настройка				
Включено	<input checked="" type="checkbox"/> Включено				
	<input type="radio"/> RIPv1 <input type="radio"/> RIPv2				
Идентификатор (ID)	Назначение	Маска подсети	Шлюз	Хоп (узел)	Включено
1	83.243.0.0	255.255.0.0	93.100.9.93	0	<input checked="" type="checkbox"/>
2					<input type="checkbox"/>
3					<input type="checkbox"/>
4					<input type="checkbox"/>
5					<input type="checkbox"/>
6					<input type="checkbox"/>
7					<input type="checkbox"/>
8					<input type="checkbox"/>

Сохранить Отменить

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 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.

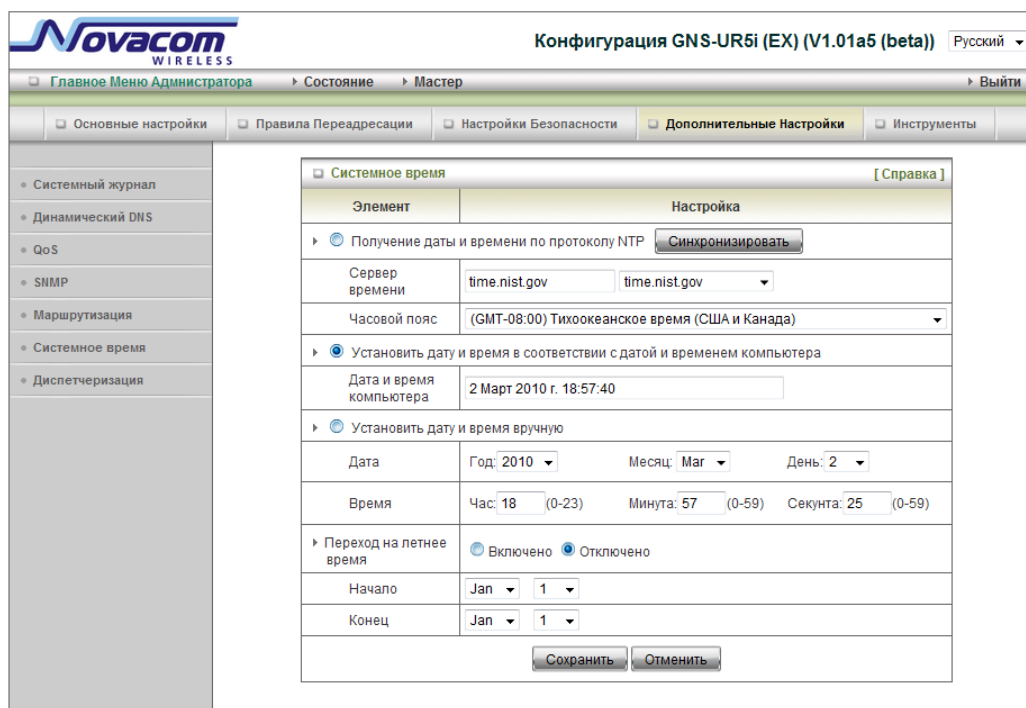
В противном случае выберите RIPv1, если Вам нужен этот протокол.

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



Конфигурация GNS-UR5i (EX) (V1.01a5 (beta)) Русский

Главное Меню Администратора > Состояние > Мастер > Выйти

Основные настройки | Правила Переадресации | Настройки Безопасности | **Дополнительные Настройки** | Инструменты

Системный журнал
Динамический DNS
QoS
SNMP
Маршрутизация
Системное время
Диспетчеризация

Системное время [Справка]

Элемент	Настройка
<input checked="" type="radio"/> Получение даты и времени по протоколу NTP <input type="button" value="Синхронизировать"/>	
Сервер времени	time.nist.gov time.nist.gov
Часовой пояс	(GMT-08:00) Тихоокеанское время (США и Канада)
<input checked="" type="radio"/> Установить дату и время в соответствии с датой и временем компьютера	
Дата и время компьютера	2 Март 2010 г. 18:57:40
<input type="radio"/> Установить дату и время вручную	
Дата	Год: 2010 Месяц: Mar День: 2
Время	Час: 18 (0-23) Минута: 57 (0-59) Секунда: 25 (0-59)
Переход на летнее время	<input type="radio"/> Включено <input checked="" type="radio"/> Отключено
Начало	Jan 1
Конец	Jan 1
<input type="button" value="Сохранить"/> <input type="button" value="Отменить"/>	

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.

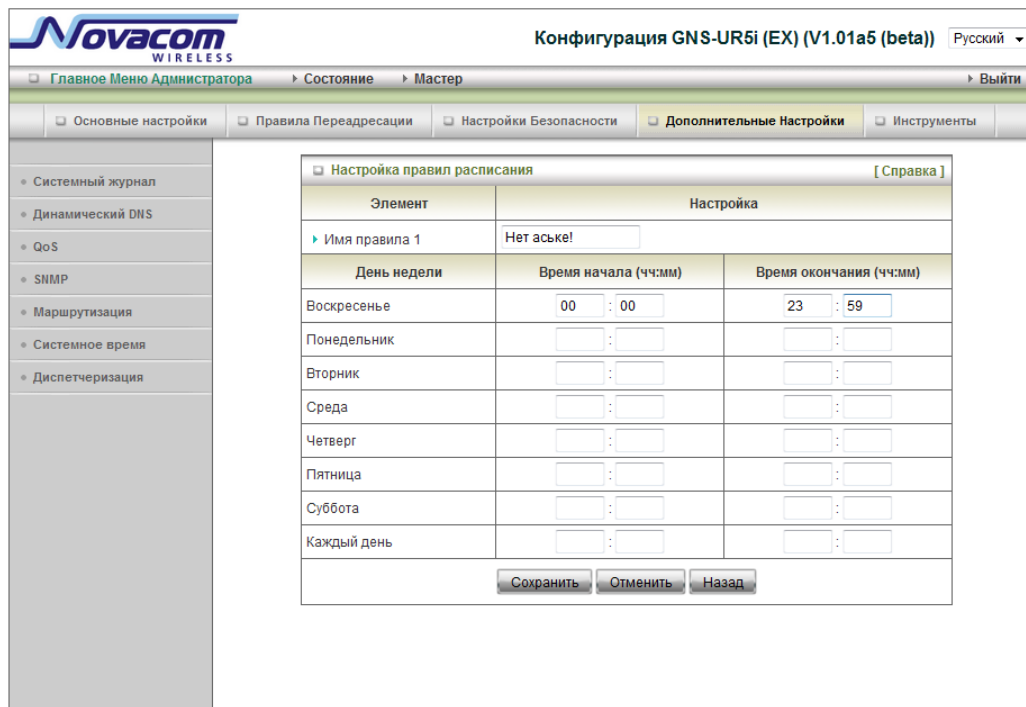
3. Установка времени и даты вручную

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.



The screenshot shows the configuration interface for a Novacom GNS-UR5i (EX) router. The main menu on the left includes options like 'Системный журнал', 'Динамический DNS', 'QoS', 'SNMP', 'Маршрутизация', 'Системное время', and 'Диспетчеризация'. The 'Диспетчеризация' (Scheduling) option is selected. The main window displays the 'Настройка правил расписания' (Schedule Rule Settings) dialog. It includes a table for defining rules with columns for 'Элемент' (Element), 'Настройка' (Setting), 'День недели' (Day of the week), 'Время начала (чч:мм)' (Start time), and 'Время окончания (чч:мм)' (End time). The table shows a rule named 'Имя правила 1' (Rule name 1) with a start time of 00:00 and an end time of 23:59. The 'Настройка' column contains the text 'Нет аське!' (Not asleep!). The dialog also includes 'Сохранить' (Save), 'Отменить' (Cancel), and 'Назад' (Back) buttons.

Элемент	Настройка
Имя правила 1	Нет аське!

День недели	Время начала (чч:мм)	Время окончания (чч:мм)
Воскресенье	00 : 00	23 : 59
Понедельник		
Вторник		
Среда		
Четверг		
Пятница		
Суббота		
Каждый день		

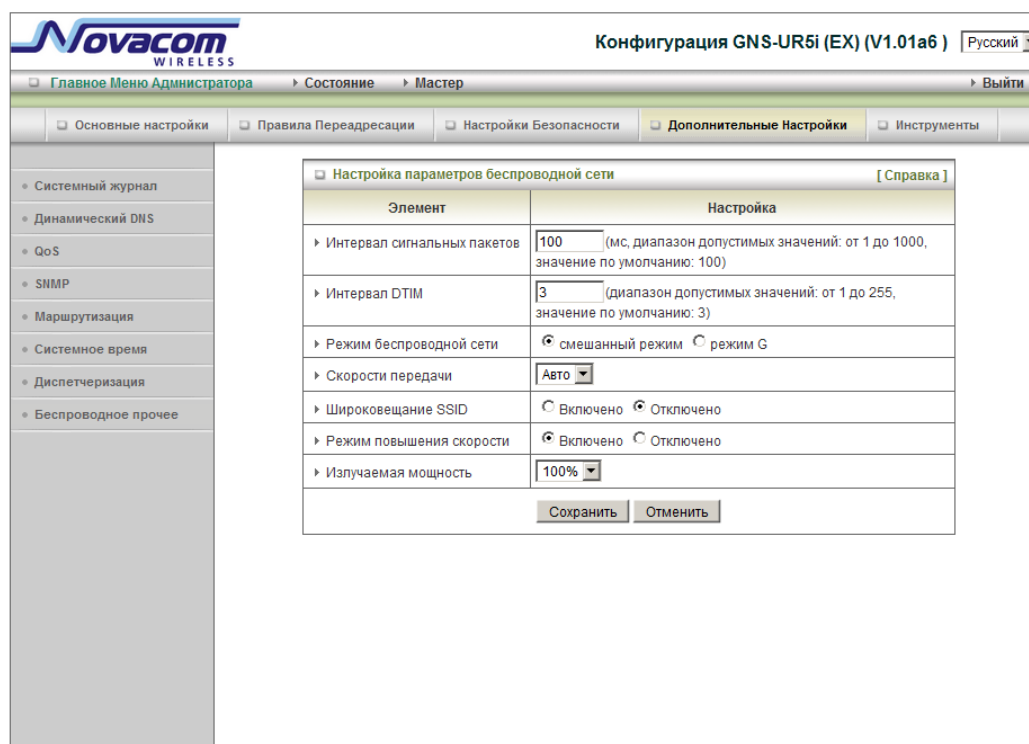
Вы можете установить график для автоматического включения/выключения разных функций.

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



The screenshot shows the configuration interface for a Novacom GNS-UR5i (EX) router. The title bar indicates 'Конфигурация GNS-UR5i (EX) (V1.01a6)' and the language is set to 'Русский'. The navigation menu includes 'Главное Меню Администратора', 'Состояние', 'Мастер', and 'Выйти'. The main menu has tabs for 'Основные настройки', 'Правила Переадресации', 'Настройки Безопасности', 'Дополнительные Настройки', and 'Инструменты'. The 'Дополнительные Настройки' tab is active, showing the 'Настройка параметров беспроводной сети' section. This section contains a table with the following settings:

Элемент	Настройка
Интервал сигнальных пакетов	100 (мс, диапазон допустимых значений: от 1 до 1000, значение по умолчанию: 100)
Интервал DTIM	3 (диапазон допустимых значений: от 1 до 255, значение по умолчанию: 3)
Режим беспроводной сети	<input checked="" type="radio"/> смешанный режим <input type="radio"/> режим G
Скорости передачи	Авто
Широковещание SSID	<input type="radio"/> Включено <input checked="" type="radio"/> Отключено
Режим повышения скорости	<input checked="" type="radio"/> Включено <input type="radio"/> Отключено
Излучаемая мощность	100%

At the bottom of the settings table are buttons for 'Сохранить' (Save) and 'Отменить' (Cancel).

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 миллисекунд.

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

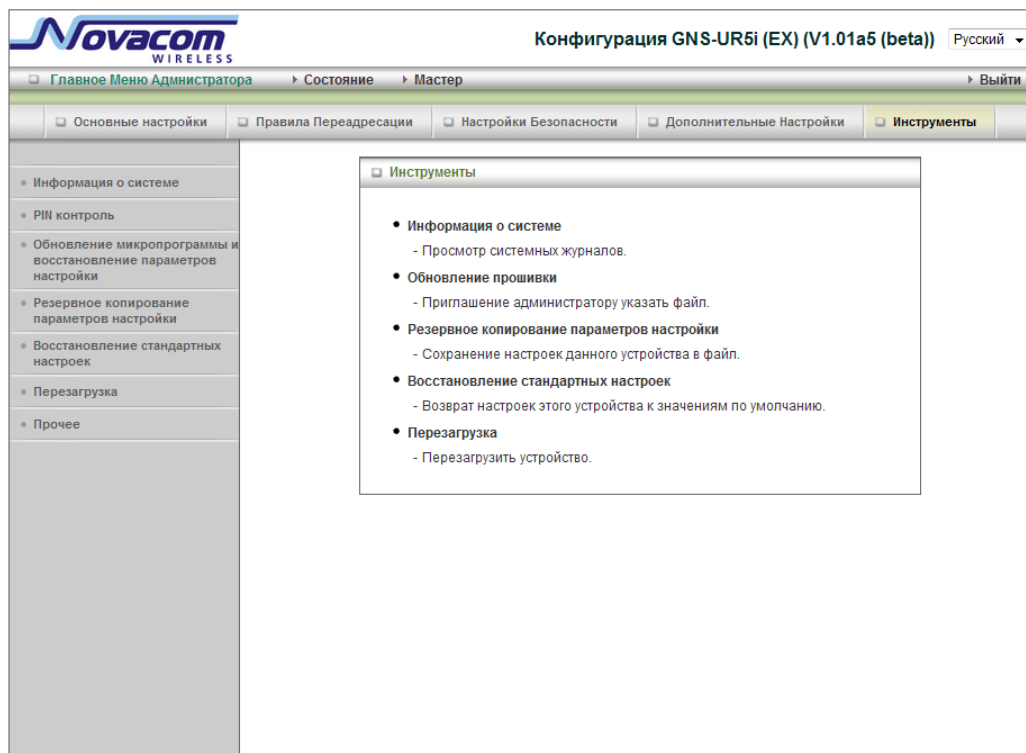
Это функция разрыва передачи для беспроводных решений Ralink

7. Мощность передачи антенны:

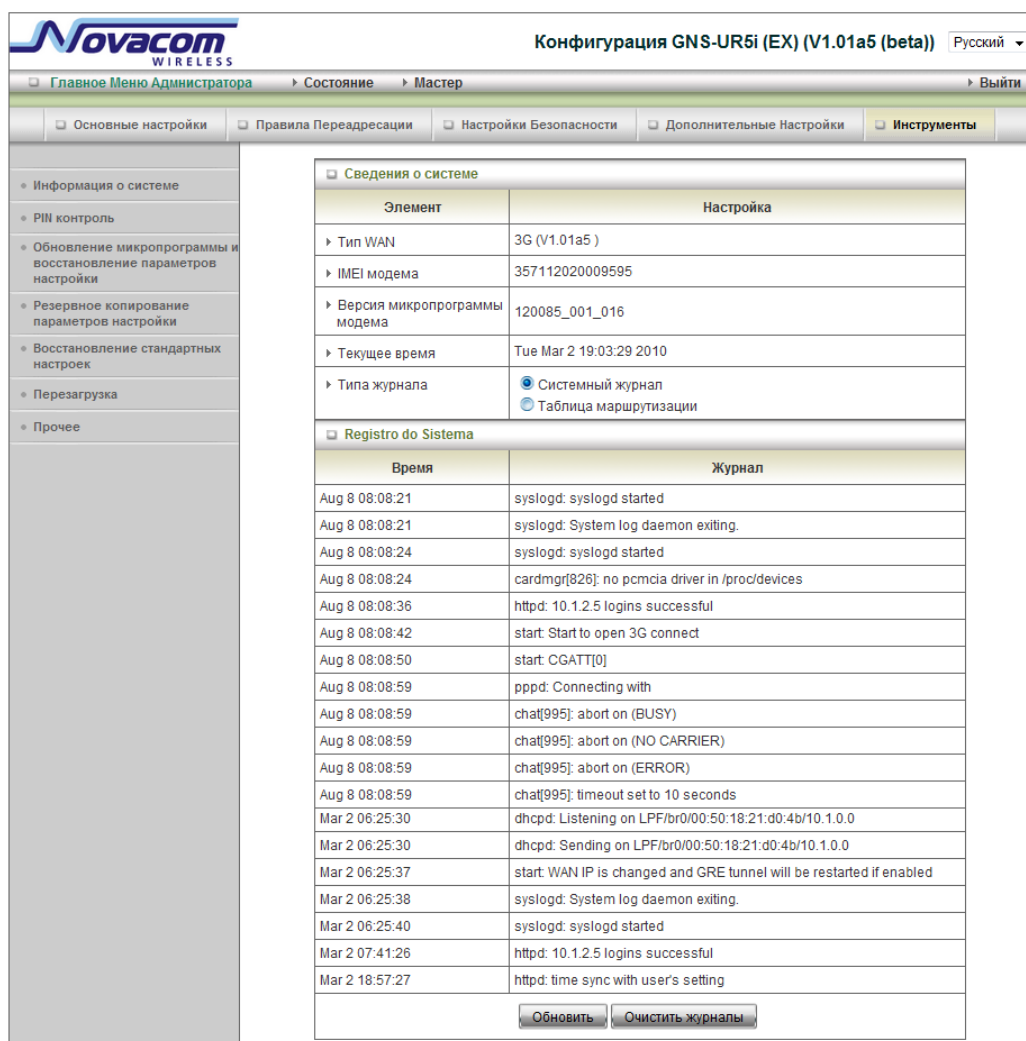
Выберите мощность передачи антенны.

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

3.2.5 Инструменты



3.2.5.1 Системная информация



The screenshot shows the configuration web interface for a Novacom GNS-UR5i (EX) router. The page title is "Конфигурация GNS-UR5i (EX) (V1.01a5 (beta))" with a language dropdown set to "Русский". The navigation menu includes "Главное Меню Администратора", "Состояние", "Мастер", and "Выйти". The main menu has tabs for "Основные настройки", "Правила Переадресации", "Настройки Безопасности", "Дополнительные Настройки", and "Инструменты".

On the left sidebar, under "Информация о системе", there are links for "PIN контроль", "Обновление микропрограммы и восстановление параметров настройки", "Резервное копирование параметров настройки", "Восстановление стандартных настроек", "Перезагрузка", and "Прочее".

The main content area displays "Сведения о системе" (System Information) and "Registro do Sistema" (System Log).

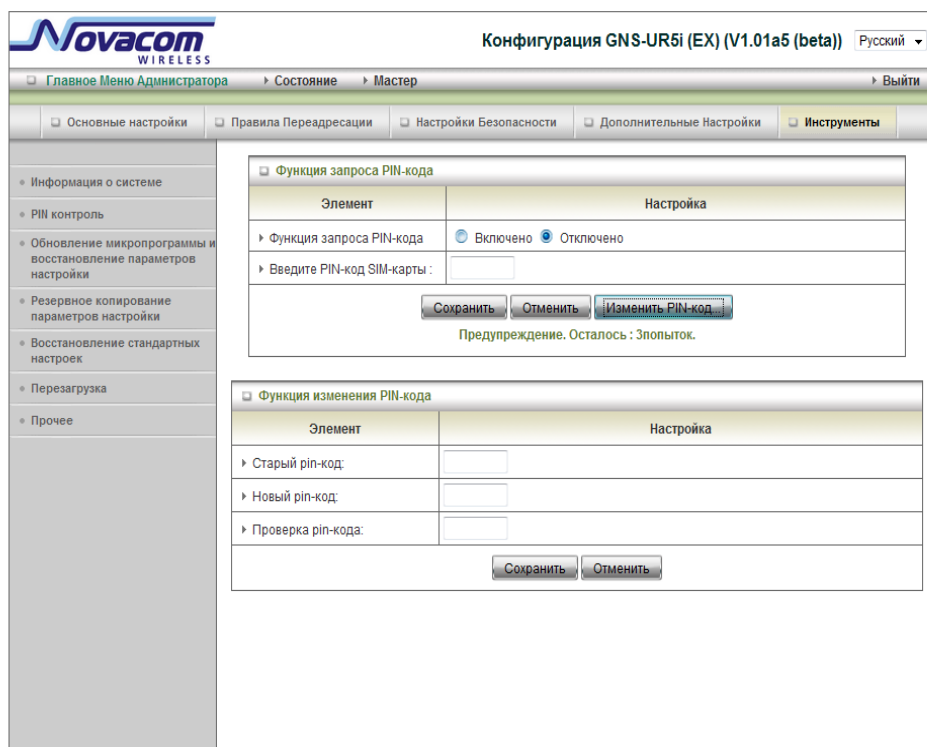
Элемент	Настройка
Тип WAN	3G (V1.01a5)
IMEI модема	357112020009595
Версия микропрограммы модема	120085_001_016
Текущее время	Tue Mar 2 19:03:29 2010
Типа журнала	<input checked="" type="radio"/> Системный журнал <input type="radio"/> Таблица маршрутизации

Время	Журнал
Aug 8 08:08:21	syslogd: syslogd started
Aug 8 08:08:21	syslogd: System log daemon exiting.
Aug 8 08:08:24	syslogd: syslogd started
Aug 8 08:08:24	cardmgr[826]: no pcmcia driver in /proc/devices
Aug 8 08:08:36	httpd: 10.1.2.5 logins successful
Aug 8 08:08:42	start: Start to open 3G connect
Aug 8 08:08:50	start: CGATT[0]
Aug 8 08:08:59	pppd: Connecting with
Aug 8 08:08:59	chat[995]: abort on (BUSY)
Aug 8 08:08:59	chat[995]: abort on (NO CARRIER)
Aug 8 08:08:59	chat[995]: abort on (ERROR)
Aug 8 08:08:59	chat[995]: timeout set to 10 seconds
Mar 2 06:25:30	dhcpcd: Listening on LPF/br0/00:50:18:21:d0:4b/10.1.0.0
Mar 2 06:25:30	dhcpcd: Sending on LPF/br0/00:50:18:21:d0:4b/10.1.0.0
Mar 2 06:25:37	start: WAN IP is changed and GRE tunnel will be restarted if enabled
Mar 2 06:25:38	syslogd: System log daemon exiting.
Mar 2 06:25:40	syslogd: syslogd started
Mar 2 07:41:26	httpd: 10.1.2.5 logins successful
Mar 2 18:57:27	httpd: time sync with user's setting

At the bottom of the log table, there are two buttons: "Обновить" (Refresh) and "Очистить журналы" (Clear logs).

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

3.2.5.2. Управление пин-кодом.



Конфигурация GNS-UR5i (EX) (V1.01a5 (beta)) Русский

Главное Меню Администратора Состояние Мастер Выйти

Основные настройки Правила Переадресации Настройки Безопасности Дополнительные Настройки Инструменты

Информация о системе
PIN контроль
Обновление микропрограммы и восстановление параметров настройки
Резервное копирование параметров настройки
Восстановление стандартных настроек
Перезагрузка
Прочее

Функция запроса PIN-кода

Элемент	Настройка
Функция запроса PIN-кода	<input type="radio"/> Включено <input checked="" type="radio"/> Отключено
Введите PIN-код SIM-карты :	<input type="text"/>

Сохранить Отменить Изменить PIN-код

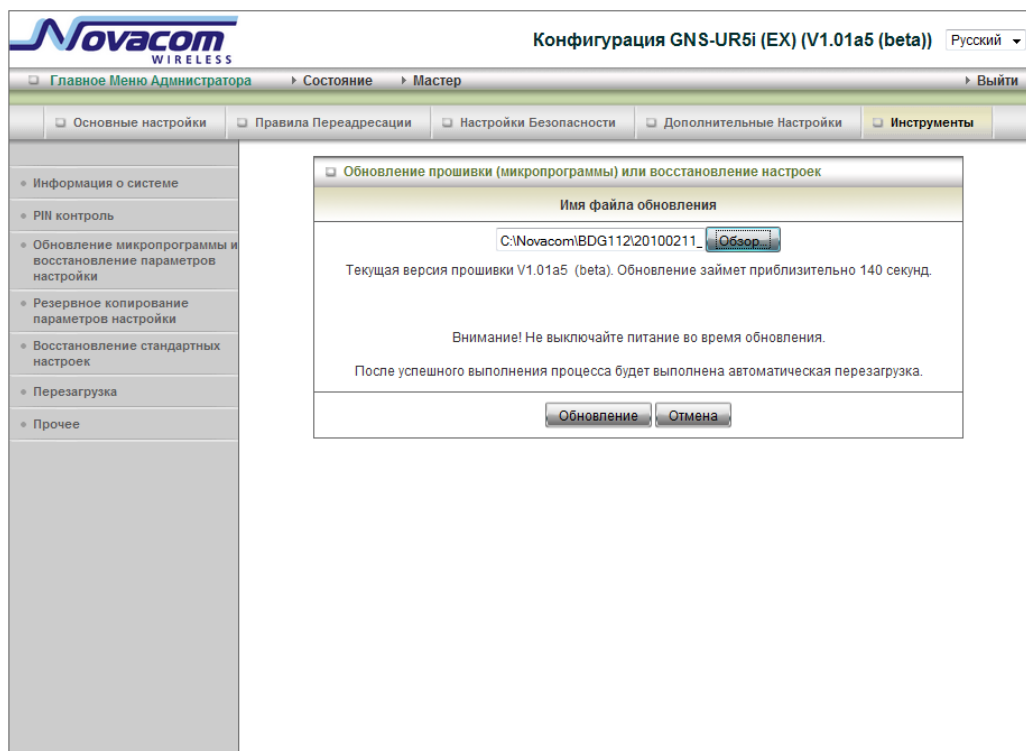
Предупреждение. Осталось : 3 попытки.

Функция изменения PIN-кода

Элемент	Настройка
Старый pin-код:	<input type="text"/>
Новый pin-код:	<input type="text"/>
Проверка pin-кода:	<input type="text"/>

Сохранить Отменить

3.2.5.2 Обновление микропрограмм и восстановление параметров настройки



Конфигурация GNS-UR5i (EX) (V1.01a5 (beta)) Русский

Главное Меню Администратора Состояние Мастер Выйти

Основные настройки Правила Переадресации Настройки Безопасности Дополнительные Настройки Инструменты

Информация о системе
PIN контроль
Обновление микропрограммы и восстановление параметров настройки
Резервное копирование параметров настройки
Восстановление стандартных настроек
Перезагрузка
Прочее

Обновление прошивки (микропрограммы) или восстановление настроек

Имя файла обновления

C:\Novacom\BDG112\20100211_ Обзор

Текущая версия прошивки V1.01a5 (beta). Обновление займет приблизительно 140 секунд.

Внимание! Не выключайте питание во время обновления.

После успешного выполнения процесса будет выполнена автоматическая перезагрузка.

Обновление Отмена

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

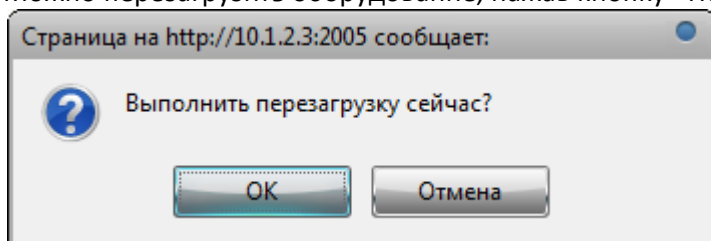
Можно сделать резервную копию своих параметров настройки, нажав кнопку «Backup Setting» и сохранить ее как бинарный файл. Как только потребуется восстановить эти параметры настройки, пожалуйста, обратитесь к разделу 3.2.5.2 «Обновление микропрограмм»

3.2.5.5 Возврат к стандартным настройкам

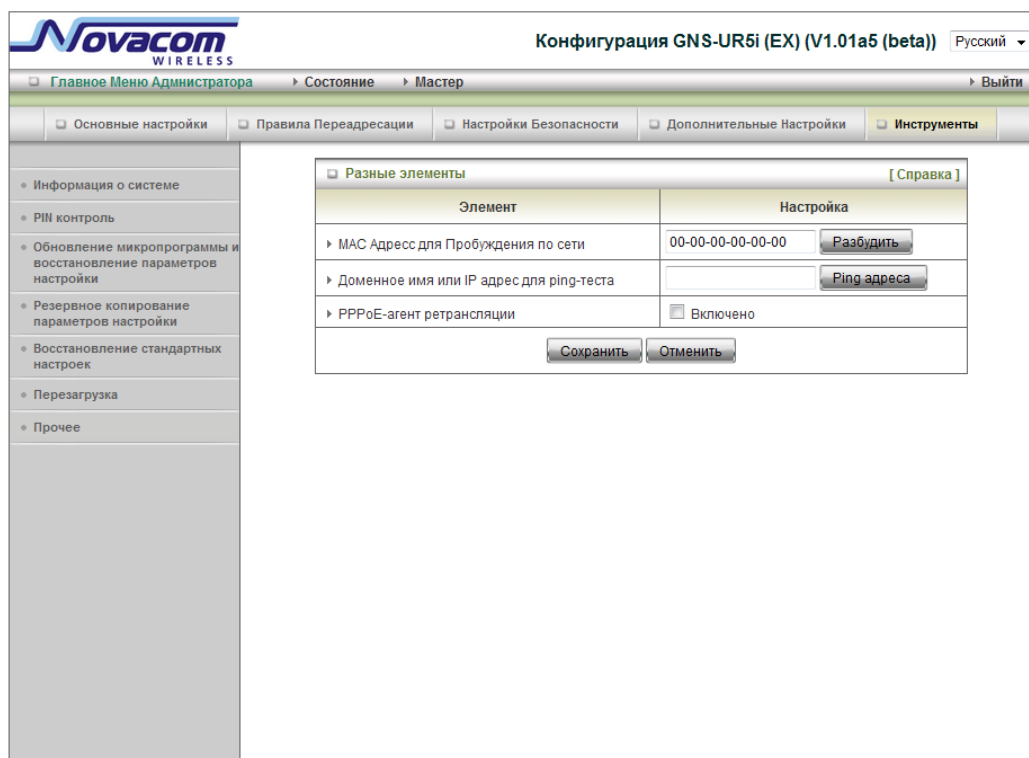
Можно перезагрузить оборудование, вернув его к настройкам производителя, нажав кнопку «Возврат к стандартным настройкам»

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 **«ОК»**.

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. Попробуйте держать антенну на расстоянии не менее 70 см от стены или других объектов.
 - Попробуйте 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 клиентах, 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 фильтрация NAT (Передача сетевых адресов) с VPN MAC фильтрация
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°C, влажность 10%-90% без конденсата
Поддерживаемые операционные системы	Windows 95/98/ME/NT/2000/XP; Linux
Питание	включение 12 В, 2.0 А