



ЭЛЕКТРОНИКА

# **РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ**

## **Средства управления и мониторинга на роутерах iRZ**



## Содержание

<b>1. Введение .....</b>	<b>7</b>
1.1. Описание документа .....	7
1.2. Предупреждение .....	7
Термины и сокращения.....	8
<b>2. Способы управления роутером iRZ .....</b>	<b>9</b>
<b>3. Быстрый доступ к устройству .....</b>	<b>10</b>
<b>4. Возвращение к заводским настройкам .....</b>	<b>11</b>
<b>5. Web-интерфейс.....</b>	<b>13</b>
5.1. Раздел «Status».....	13
5.2. Раздел «Network».....	17
5.2.1. Local Network .....	17
5.2.2. Wired Internet.....	18
5.2.3. Mobile Interfaces.....	21
5.2.4. Mobile APN Profiles.....	25
5.2.5. Loopbacks.....	26
5.2.6. Wireless Internet .....	26
5.2.7. Routes .....	30
5.2.8. Dynamic Routes(QUAGGA, только для роутеров серии R4).....	32
5.2.9. DNS Servers .....	33
5.2.10. Switch .....	34
5.3. Раздел VPN/Tunnels.....	35
5.4. Раздел «Services» .....	35
5.4.1. DHCP.....	35
5.4.2. MAC Filter .....	37
5.4.3. Firewall .....	38
5.4.4. Port Forwarding.....	44
5.4.5. VRRP.....	45
5.4.6. Time.....	46
5.4.7. SNMP .....	47
5.4.8. DynDNS.....	49
5.4.9. Crontabs .....	51



5.4.10. Command over SMS .....	51
5.4.11. RS232/RS485 over TCP.....	53
5.4.12. RS232/RS485 Server Modbus TCP to RTU.....	55
5.5. Раздел «Tools» .....	56
5.5.1. Access .....	56
5.5.2. iRZ Link Client.....	57
5.5.3. iRZ ZTP Client.....	58
5.5.4. Change Password .....	58
5.5.5. Unit Name .....	59
5.5.6. Send SMS.....	60
5.5.7. Ping .....	61
5.5.8. System Log .....	62
5.5.9. GPIO.....	63
5.5.10. Wi-Fi Clients.....	65
5.5.11. DHCP Leases .....	66
5.5.12. Reboot .....	67
5.5.13. Management .....	68
<b>6. Контакты и поддержка.....</b>	<b>70</b>
<b>Приложение 1 .....</b>	<b>71</b>
Синтаксис IP-адреса .....	71
Синтаксис IP-адреса сети .....	71
Синтаксис маски подсети.....	71
Синтаксис MAC-адреса.....	71
<b>Приложение 2 .....</b>	<b>72</b>
Доступные команды управления .....	72

## Перечень таблиц

Таблица 2.1 Сетевые службы, используемые для управления роутером.....	9
Таблица 5.1. Поля в разделе Device Info.....	13
Таблица 5.2. Поля в разделе Routing .....	13
Таблица 5.3. Поля в разделе Local Network (LAN) .....	14



Таблица 5.4. Поля раздела Mobile Internet .....	15
Таблица 5.5. Поля в разделе Wired Internet (WAN) .....	15
Таблица 5.6. Настройки Network → Local Network .....	18
Таблица 5.7. Настройки Network → Wired Internet .....	19
Таблица 5.8. Настройки Network → Mobile Interfaces–Edit .....	24
Таблица 5.9. Вкладка Mobile APN Profiles .....	25
Таблица 5.10. Настройки Network → Wireless Network (Wi-Fi Mode = Access Point) .....	27
Таблица 5.11. Настройки Network → Wireless Network (Wi-Fi Mode = Client) .....	28
Таблица 5.12. Настройки маршрутов .....	31
Таблица 5.13. Настройки маршрутов .....	34
Таблица 5.14. Настройки адресов .....	36
Таблица 5.15. Настройки правил для зон .....	39
Таблица 5.16. Настройки правил для направлений .....	40
Таблица 5.17. Настройки правил для межсетевого экрана .....	43
Таблица 5.18. Настройки правил проброса портов .....	44
Таблица 5.19. Настройки правил проброса портов .....	45
Таблица 5.20. Настройки SNMP .....	48
Таблица 5.21. Настройки DynDNS .....	50
Таблица 5.22. Настройки RS232 over TCP (C – клиент, S – сервер, M — server Modbus TCP to RTU) .....	54
Таблица 5.23. Физические характеристики для роутеров R4 .....	63
Таблица 5.24. Настройки портов GPIO .....	64
Таблица 5.25. Информация о Wi-Fi-клиентах .....	65
Таблица 5.26. Информация о DHCP Leases .....	66

## Перечень рисунков

Рис. 3.1 Ввод IP-адреса роутера в адресную строку интернет-браузера .....	10
Рис. 3.2 Ввод логина и пароля для доступа к web-интерфейсу роутера .....	10
Рис. 3.3 Страница статуса .....	11
Рис. 5.1. Пример информации в разделе Device Info .....	13
Рис. 5.2. Пример информации в разделе Routing .....	13
Рис. 5.3. Пример информации в разделе Local Network .....	14



<b>Рис. 5.4.</b> Пример информации в разделе Mobile Internet .....	14
<b>Рис. 5.5.</b> Пример информации в разделе Wired Internet (WAN) .....	15
<b>Рис. 5.6.</b> Пример информации в разделе Routing Table .....	16
<b>Рис. 5.7.</b> Вкладка Network, раздел Local Network .....	17
<b>Рис. 5.8.</b> Вкладка Network, раздел Wired Internet .....	18
<b>Рис. 5.9.</b> Типы соединения для WAN-порта .....	19
<b>Рис. 5.10.</b> WAN-порт отключен .....	20
<b>Рис. 5.11.</b> Тип соединения WAN-порта – DHCP .....	20
<b>Рис. 5.12.</b> Тип соединения WAN-порта – PPPoE .....	21
<b>Рис. 5.13</b> Вкладка Network, раздел Mobile Interfaces для одномодульного устройства .....	21
<b>Рис. 5.14</b> Вкладка Network, раздел Mobile Interfaces – Edit для одномодульного устройства .....	22
<b>Рис. 5.15.</b> Вкладка Network, раздел Mobile Interfaces для двухмодульного устройства .....	23
<b>Рис. 5.16</b> Вкладка Network, раздел Mobile Interfaces –Edit для двухмодульного устройства .....	23
<b>Рис. 5.17</b> Вкладка Mobile APN Profiles .....	25
<b>Рис. 5.18</b> Вкладка Network, раздел Loopbacks .....	26
<b>Рис. 5.19.</b> Вкладка Network, раздел Wireless Internet .....	27
<b>Рис. 5.20.</b> Режим Wi-Fi настройки Bridge with Interface .....	28
<b>Рис. 5.21.</b> Режим DHCP настройки Connection Type .....	29
<b>Рис. 5.22.</b> Режим Static, настройки Connection Type .....	29
<b>Рис. 5.23.</b> Вкладка Network, раздел Routes .....	30
<b>Рис. 5.24.</b> Настройка статических маршрутов .....	31
<b>Рис. 5.25</b> Пример настройки динамической маршрутизации по протоколам: BGP, OSPF .....	32
<b>Рис. 5.26.</b> Вкладка Network, раздел DNS Servers .....	33
<b>Рис. 5.27.</b> Вкладка Network, раздел Switch .....	34
<b>Рис. 5.28.</b> Вкладка Services, раздел DHCP .....	35
<b>Рис. 5.29.</b> Указание IP-адресов вручную .....	36
<b>Рис. 5.30.</b> Вкладка Services, раздел MAC Filter .....	37
<b>Рис. 5.31.</b> Вкладка Services, раздел Firewall .....	38
<b>Рис. 5.32</b> Вкладка Services, раздел Firewall, настройки Default Actions .....	39
<b>Рис. 5.33.</b> Вариант выбора действий для трафика .....	39
<b>Рис. 5.34</b> Вкладка Services, раздел Firewall, настройки Zones List .....	40
<b>Рис. 5.35.</b> Настройки Allowed Forwards .....	40



<b>Рис. 5.36</b> Вкладка Services, раздел Firewall, настройки User Firewall Rules.....	41
<b>Рис. 5.37.</b> Настройки Firewall .....	42
<b>Рис. 5.38.</b> Редактирование правила Firewall .....	43
<b>Рис. 5.39.</b> Вкладка Services, раздел Port Forwarding .....	44
<b>Рис. 5.40.</b> Вкладка Services, раздел VRRP .....	45
<b>Рис. 5.41.</b> Настройка времени в ручном режиме .....	46
<b>Рис. 5.42.</b> Настройка времени в автоматическом режиме .....	47
<b>Рис. 5.43.</b> Вкладка Services, раздел SNMP (v2c) .....	47
<b>Рис. 5.44.</b> Вкладка Services, раздел SNMP (v3) .....	48
<b>Рис. 5.45.</b> Вкладка Services, раздел DynDNS.....	49
<b>Рис. 5.46.</b> Сервера DNS.....	50
<b>Рис. 5.47.</b> Вкладка Services, раздел Crontabs .....	51
<b>Рис. 5.48.</b> Вкладка Services, раздел Commands over SMS .....	52
<b>Рис. 5.49.</b> Вкладка Services, раздел RS232 over TCP.....	53
<b>Рис. 5.50</b> Вкладка Services, раздел RS232 over TCP, режим Server Modbus TCP to RTU.....	55
<b>Рис. 5.51.</b> Вкладка Tools, раздел Access.....	56
<b>Рис. 5.52</b> Вкладка Tools, раздел iRZ Link Clinet .....	57
<b>Рис. 5.53.</b> Вкладка Tools, раздел Change Password.....	58
<b>Рис. 5.54.</b> Вкладка Tools, раздел Unit Name.....	59
<b>Рис. 5.55.</b> Вкладка Tools, раздел Send SMS .....	60
<b>Рис. 5.56.</b> Вкладка Tools, раздел Ping.....	61
<b>Рис. 5.57.</b> Вкладка Tools, раздел System Log.....	62
<b>Рис. 5.58.</b> Вкладка Tools, раздел GPIO .....	63
<b>Рис. 5.59.</b> Вкладка Tools, раздел Wi-Fi Clients (роутер с Wi-Fi-модулем).....	65
<b>Рис. 5.60.</b> Вкладка Tools, раздел DHCP Leases .....	66
<b>Рис. 5.61.</b> Вкладка Tools, раздел Reboot.....	67
<b>Рис. 5.62.</b> Вкладка Tools, раздел Management.....	68



## 1. Введение

### 1.1. Описание документа

Данный документ является частью набора инструкций по обслуживанию роутеров iRZ и содержит информацию только по средствам мониторинга и управления устройством. Для получения информации о работе самих устройств смотрите соответствующее руководство пользователя.

Версия документа (Дата публикации)		Изменения	
2.1 (12.03.2019)		Основной документ	
2.2 (03.06.2019)		Предупреждение о подаче напряжения на GPIO	
2.3 (20.12.2019)		Добавлен Mobile APN Profiles, Server Modbus to RTU, обновлены все разделы документа	
<b>Выполнил</b>	Колмак О., Яковлева Т.В.	<b>Проверил</b>	Колмак О.

### 1.2. Предупреждение

**Примечание.** Для каждой модели роутера существует собственный комплект документации. Пожалуйста, убедитесь, что работаете с документацией именно для вашей модели устройства.

**Внимание!** Нарушение условий эксплуатации роутера лишает Вас права на гарантийное обслуживание устройства.

Предупреждение:

- Рекомендуется уделить особое внимание разделу, посвященному предоставлению доступа к роутеру. При нарушении описанных рекомендаций возможна угроза несанкционированного доступа к роутеру, сетям и другому сетевому оборудованию со стороны третьих лиц.
- Параметры конфигурации следует вводить в полном соответствии с рекомендациями данного документа. Например, для IP-адреса:  
**Корректно:** 123.213.132.001  
**Некорректно:** 123,456.789.000, 123..456.789.000, 12 3.456.789.000
- Все поля настроек роутера необходимо заполнять только на английском языке.



## Термины и сокращения

**Техническое решение** – идея или документ, которые описывают набор технических мероприятий, направленных на реализацию конкретной задачи. Для выполнения такой задачи используются функциональные возможности компонентов решения, связанных между собой и взаимодействующих друг с другом определенным образом.

**Внешний IP-адрес** – IP-адрес в сети Интернет, предоставляемый компанией-провайдером услуг связи в пользование клиенту на своем или его оборудовании для обеспечения прямой связи с оборудованием клиента через сеть Интернет.

**Фиксированный внешний IP-адрес** – внешний IP-адрес, не изменяющийся ни при каких условиях (при смене типа оборудования клиента и т.п.) или событиях (при переподключении к сети компании-провайдера и т.д.). Единственной возможностью изменить фиксированный IP-адрес является обращение в компанию-провайдер.

**Аутентификация** – процедура проверки подлинности пользователя, клиента или узла, во время которой реквизиты, предоставленные на момент подключения, сравниваются с реквизитами в базе данных.

**Web-интерфейс роутера** – встроенное средство управления, позволяющее настраивать и контролировать работу роутера через любой стандартный интернет-браузер.

**Удаленное устройство (удаленный узел)** – устройство, территориально удаленное от рассматриваемого места, объекта или узла.





## 2. Способы управления роутером iRZ

**Внимание!** Рекомендуется уделить особое внимание настройкам доступа к устройству по протоколам HTTP, HTTPS, Telnet, SSH. От сложности паролей, разрешения удаленного доступа, используемых портов сетевых служб, настроек межсетевого экрана и других настроек сетевых служб зависит безопасность не только самого роутера, но и устройств и сетей, находящихся за ним.

**Таблица 2.1** Сетевые службы, используемые для управления роутером

Название	Описание	Требуемое ПО
HTTP/HTTPS	Веб-интерфейс, позволяющий настроить все регламентированные функции роутера. Можно использовать любой стандартный интернет-браузер.	Интернет-браузер - Opera, Firefox, Chrome, Safari и т.д. (кроме Internet Explorer)
Telnet	Командная консоль, предназначенная для более тонкой настройки устройства. Позволяет использовать стандартные команды Linux.	Telnet-клиент - присутствует во всех ОС (в Windows 7, 8, 10 требуется включить).
SSH	Аналог Telnet, в котором шифруется трафик при авторизации и работе с консолью, что снижает угрозу перехвата конфиденциальной информации третьими лицами.	SSH-клиент – присутствует по умолчанию в UNIX, требуется установить PuTTY, WinSCP, Openssh (win32) в Windows



### 3. Быстрый доступ к устройству

Откройте интернет-браузер и выполните следующие действия:

1. Введите IP-адрес роутера в адресную строку интернет-браузера.

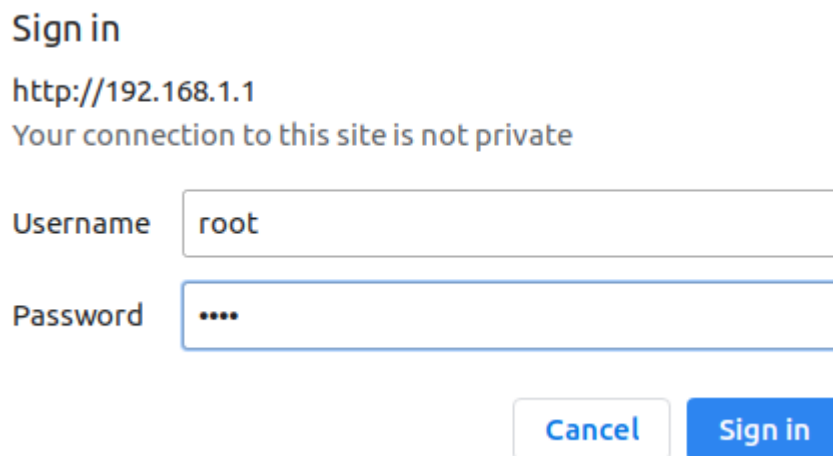


Рис. 3.1 Ввод IP-адреса роутера в адресную строку интернет-браузера

**Внимание!** Не рекомендуем использовать для работы с web-интерфейсом роутера браузер Internet Explorer

**Примечание.** IP-адрес для доступа к настройкам роутера, используемый по умолчанию, указан на наклейке на нижней стороне корпуса устройства.

2. Введите логин и пароль для доступа к веб-интерфейсу роутера  
(по умолчанию, логин – **root**, пароль – **root**)



Sign in

http://192.168.1.1

Your connection to this site is not private

Username

Password

Рис. 3.2 Ввод логина и пароля для доступа к web-интерфейсу роутера

**Примечание.** При утере пароля смотрите раздел о сбросе настроек в руководстве пользователя соответствующего устройства или общие рекомендации в разделе 4 данного руководства.



После корректно ввода логина и пароля открывается страница статуса и доступ к основному интерфейсу управления устройством.

Status	Network	VPN / Tunnels	Services	Tools
<b>Device info</b>				
Model	RL22w	Firmware	v767 (2020-01-17 13:27:16)	
Uptime	01h 39m 34s	Serial No	RDFG1000007	
Hostname	iRZ-Router	Unitname		
RAM free/total	19216 KiB / 61252 KiB			
<b>Routing</b>				
Mode	backup	Interfaces		
<b>Local Network (lan)</b>				
Status	Up	Uptime	01h 38m 56s	
Type	static	MAC	F0:81:AF:00:DE:B0	
Address	192.168.1.1/24	Rx/Tx	164.3 KiB / 2.2 MiB	
<b>Mobile Internet (sim1)</b>				
Status	Down			
<b>Routing table</b>				
192.168.1.0/24 @ lan, metric=0				

**Рис. 3.3** Страница статуса

Страница статуса содержит краткую информацию о состоянии устройства и сети:

- модель устройства;
- время работы устройства после включения (uptime);
- название оператора сотовой связи;
- тип GSM-связи, уровень GSM-сигнала;
- IP-адрес, скорость соединения;
- количество переданной и полученной информации и т.д.

## 4. Возвращение к заводским настройкам

**Внимание!** Данная операция необратима. Прежде чем выполнять сброс настроек, убедитесь, что текущие настройки устройства Вам не понадобятся (в том числе ключи и сертификаты OpenVPN, IPSec, GRE, параметры подключения к сети Интернет и т.д.).



Для того чтобы сбросить настройки роутера к заводским установкам, на роутерах iRZ имеется специальная кнопка «Reset».

Для сброса настроек зажмите кнопку и удерживайте около 20 секунд, роутер перезагрузится уже со сброшенными настройками.

Если после перезагрузки настройки роутера оказались так и не сброшены, возможно, вы удерживали кнопку не достаточно долго или на вашем устройстве сломана кнопка.

Также настройки роутера можно сбросить через веб-интерфейс, см. раздел **5.5.12** данного руководства.



## 5. Web-интерфейс

### 5.1. Раздел «Status»

На вкладке **Status** представлена информация о состоянии роутера и его сервисов, которая может быть полезна для быстрой диагностики устройства. В данном разделе приводится подробное описание полей и значений данной вкладки.

**Device Info** — информация об устройстве.

#### Device info

Model	RL41I	Firmware	v1253 (2018-04-17 15:02:14)
Uptime	01h 24m 46s	Serial No	RFAD1000046
Hostname	iRZ-Router	Unitname	
RAM free/total	74772 KiB / 124792 KiB		

Рис. 5.1. Пример информации в разделе Device Info

Таблица 5.1. Поля в разделе Device Info

Поле	Описание
Model	Выводит модель вашего роутера
Uptime	Время работы роутера с последней перезагрузки
Unitname	Имя роутера (можно задать в разделе Tools → Unit name)
Firmware	Версия установленной прошивки
Serial No	Серийный номер роутера
RAM free/total	Количество свободной оперативной памяти/общий объем оперативной памяти
Hostname	Имя хоста

**Routing** — информация о режиме работы WAN-портов.

#### Routing

Mode backup Interfaces wan

Рис. 5.2. Пример информации в разделе Routing

Таблица 5.2. Поля в разделе Routing

Поле	Описание
Mode	Указывает режим работы WAN портов: <i>balancing</i> — режим балансировки трафика между wan портами; <i>backup</i> — режим резервирования между wan портами (раздел Network → Routing).
Interfaces	Указывает интерфейсы через которые в данный момент осуществляется тот или иной режим в порядке приоритетов.



**Local Network (LAN)** — информация о состоянии локальных портов роутера. Подразделов может быть несколько, так как в настройках присутствует возможность вынести каждый Ethernet-порт в отдельный VLAN.

### Local Network (lan)

Status	Up	Uptime	21h 56m 24s
Address	192.168.1.1/24	Type	static
MAC	F0:81:AF:00:0F:6D	Rx/Tx	55.4 KiB / 1.1 MiB

**Рис. 5.3.** Пример информации в разделе Local Network

**Таблица 5.3.** Поля в разделе Local Network (LAN)

Поле	Описание
Status	Указывается есть ли физическое подключение к порту: <ul style="list-style-type: none"><li>• Up — подключение есть;</li><li>• Down — подключения нет</li></ul>
Address	IP-адрес порта с указанием маски сети
MAC	MAC-адрес порта
Uptime	Время работы порта
Type	Режим работы порта: static — статическая IP-адресация
Rx/Tx	Счетчик принятых и отправленных байт

**Mobile Internet (SIM1/SIM2/SIM3/SIM4)** — информация о состоянии подключения по каналу сотовой сети (два раздела, если устройство поддерживает две SIM-карты).

### Mobile Internet (sim1)

Status	Up	Uptime	00h 04m 18s
Network	3G	Operator	Beeline
Signal quality	26	Module name	Huawei MU709s-2
Module revision	11.652.61.00.00	Module IMEI	864881021515208
Address	10.229.29.221/32	Rx/Tx	60.0 B / 102.0 B

**Рис. 5.4.** Пример информации в разделе Mobile Internet



Таблица 5.4. Поля раздела Mobile Internet

Поле	Описание
Status	Указывается статус подключения к сотовой сети: <ul style="list-style-type: none"><li>• Up — SIM-карта зарегистрирована в сети сотового оператора и готова к работе;</li><li>• Down — SIM-карта не зарегистрирована в сети и не работает.</li></ul>
Address	IP-адрес сим карты с указанием маски сети, выдаваемый оператором сотовой сети
Operator	Выводится имя оператора сотовой сети
Module Name	Название GSM модуля, установленного в вашем роутере
Module IMEI	IMEI номер GSM модуля вашего роутера.
Uptime	Время активности с момента установки сессии
Network	Тип сотовой сети по которой в данный момент осуществляется передача данных: 2G, 3G, 4G
Signal Quality	Уровень сигнала сотовой сети в формате CSQ, минимальное значение (сигнала нет совсем) — 0, максимальное значение уровня сигнала — 31, при CSQ <b>менее</b> 12 стабильность передачи данных может варьироваться.
Module Revision	Номер версии GSM-модуля роутера
Rx/Tx	Счетчик принятых и отправленных байт

**Wired Internet (WAN)** — информация о статусе порта WAN.

### Wired Internet (wan)

Status	Up	Uptime	00h 00m 03s
Type	dhcp	MAC	F0:81:AF:00:0F:6C
Address	192.168.245.18/22	Rx/Tx	2.7 KiB / 1.3 KiB

Рис. 5.5. Пример информации в разделе Wired Internet (WAN)

Таблица 5.5. Поля в разделе Wired Internet (WAN)

Поле	Описание
Status	Состояние порта: <ul style="list-style-type: none"><li>• Up — порт активен и работает;</li><li>• Down — порт выключен.</li></ul>
Address	IP-адрес порта с указанием маски сети
MAC	MAC-адрес порта
Uptime	Время активности порта
Type	Тип работы порта: <ul style="list-style-type: none"><li>• static — на порту назначен статический IP-адрес;</li><li>• DHCP — порт получает адрес от внешнего DHCP-сервера;</li><li>• PPPoE — порт подключается к внешнему PPPoE-серверу.</li></ul>
Rx/Tx	Счетчик принятых и отправленных байт



**Tunnel** — информация о состоянии туннеля. Более подробную информацию о туннелях и их настройке можно прочитать в отдельном документе «**РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ Настройка туннелей на роутерах iRZ**» на сайте [www.radiofid.ru](http://www.radiofid.ru) .

**Routing Table** — информация по таблице маршрутизации. Выводятся все существующие на данный момент маршруты.

### Routing table

0.0.0.0/0 @ sim1, metric=3

10.64.64.64/32 @ sim1, metric=0

192.168.1.0/24 @ lan, metric=0

**Рис. 5.6.** Пример информации в разделе Routing Table





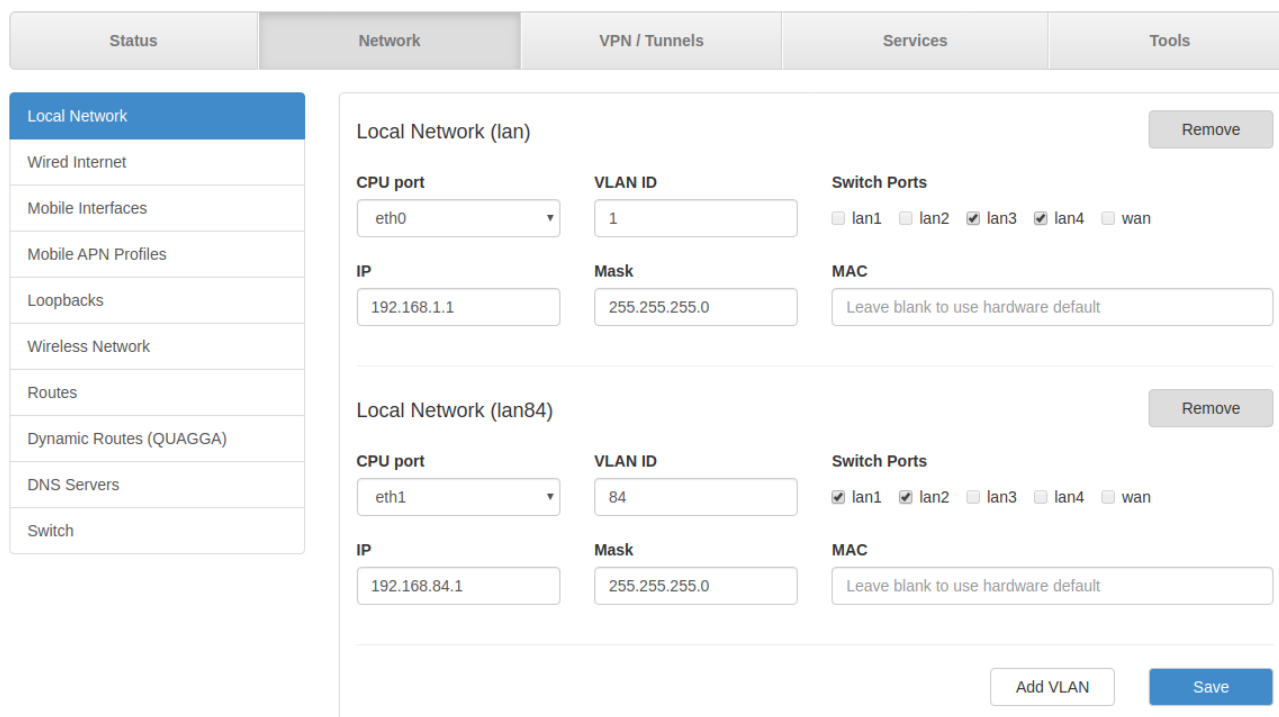
## 5.2. Раздел «Network»

### 5.2.1. Local Network

Раздел Local Network на вкладке Network предназначен для настройки локальных Ethernet-портов роутера. В роутерах iRZ имеется возможность настроить WAN-порт таким образом, чтобы он работал, как локальный Ethernet-порт и наоборот — все LAN порты превратить в WAN.

На **Рис. 5.7** представлен пример объединения Ethernet-портов в VLAN (виртуальную локальную сеть). Поскольку в данном примере настроено два VLAN, то на странице показаны две группы настроек – для виртуальных сетей «lan» и «lan84» (названия задаются автоматически или в ручную — поле VLAN ID). Чтобы добавить новый VLAN, нажмите на кнопку **Add VLAN** внизу страницы, а чтобы удалить – нажмите кнопку **Remove**, в соответствующей группе настроек.

Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!



Status	Network	VPN / Tunnels	Services	Tools
<b>Local Network</b>				
Wired Internet				
Mobile Interfaces				
Mobile APN Profiles				
Loopbacks				
Wireless Network				
Routes				
Dynamic Routes (QUAGGA)				
DNS Servers				
Switch				

#### Local Network (lan) Remove

<b>CPU port</b>	<b>VLAN ID</b>	<b>Switch Ports</b>
eth0	1	<input type="checkbox"/> lan1 <input type="checkbox"/> lan2 <input checked="" type="checkbox"/> lan3 <input checked="" type="checkbox"/> lan4 <input type="checkbox"/> wan
<b>IP</b>	<b>Mask</b>	<b>MAC</b>
192.168.1.1	255.255.255.0	Leave blank to use hardware default

---

#### Local Network (lan84) Remove

<b>CPU port</b>	<b>VLAN ID</b>	<b>Switch Ports</b>
eth1	84	<input checked="" type="checkbox"/> lan1 <input checked="" type="checkbox"/> lan2 <input type="checkbox"/> lan3 <input type="checkbox"/> lan4 <input type="checkbox"/> wan
<b>IP</b>	<b>Mask</b>	<b>MAC</b>
192.168.84.1	255.255.255.0	Leave blank to use hardware default

Add VLAN Save

**Рис. 5.7.** Вкладка Network, раздел Local Network



Таблица 5.6. Настройки Network → Local Network

Поле	Описание
CPU Port	Выбор порта процессора, который будет назначен на VLAN. Например, в роутерах серии R4 доступны два порта Ethernet 1Gbit: ETH0 и ETH1. По умолчанию, ETH0 – это четыре локальных порта, а ETH1 – один WAN-порт. Однако пользователь с помощью данной настройки может распределить порты между физическими разъемами самостоятельно.
VLAN ID	Указание номера VLAN. Изначально номер задается автоматически самим устройством, однако пользователь имеет возможность его изменить.
Switch Ports	Выбор физических портов, которые будут добавлены в VLAN
IP	IP-адрес роутера для созданного VLAN
Mask	Маска сети роутера для созданного VLAN
MAC	MAC адрес, можно задавать в ручную

### 5.2.2. Wired Internet

Раздел Wired Internet на вкладке Network предназначен для настройки WAN-порта роутера в рамках VLAN. В роутерах iRZ имеется возможность настроить локальные порты таким образом, чтобы они работали, как WAN-порты.

На **Рис. 5.8** представлен пример создания VLAN на основе WAN-порта роутера. В данном примере настроен один WAN-порт, группа настроек виртуальной сети «wan» (название задается автоматически). Чтобы добавить новый VLAN, нажмите на кнопку **Add VLAN** внизу страницы, а чтобы удалить – нажмите кнопку **Remove**, в соответствующей группе настроек.

Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!

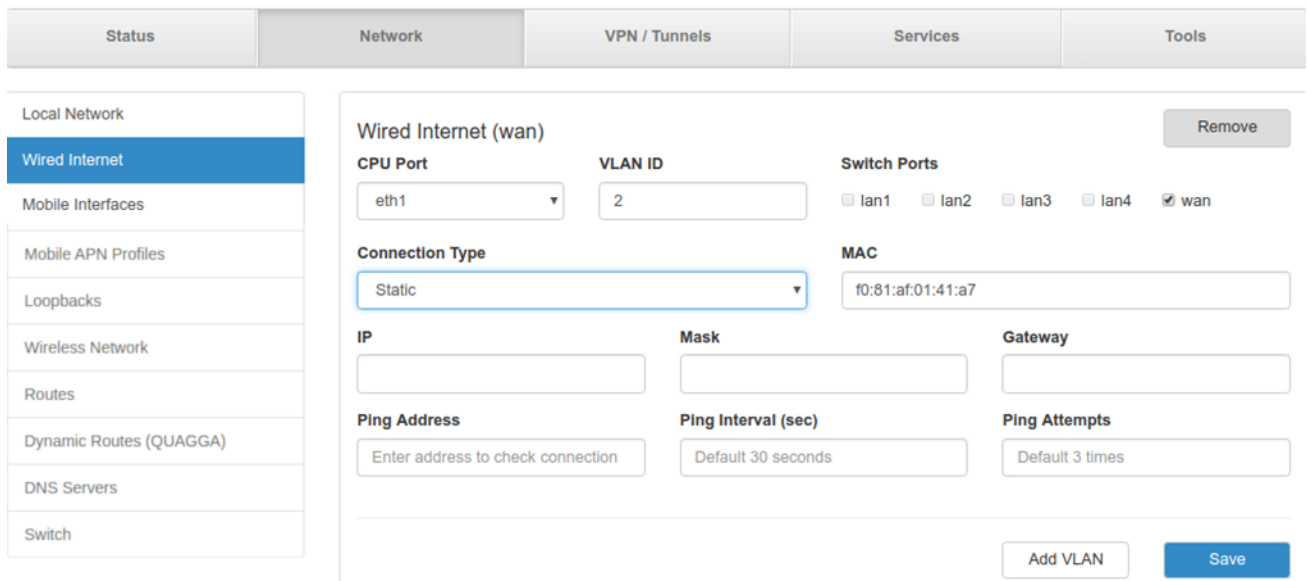


Рис. 5.8. Вкладка Network, раздел Wired Internet



Таблица 5.7. Настройки Network → Wired Internet

Поле	Описание	
CPU Port	Выбор порта процессора, который будет назначен на VLAN. Например, в роутерах серии R4 доступны два порта Ethernet 1Gbit: ETH0 и ETH1. По умолчанию, ETH0 – это четыре локальных порта, а ETH1 – один WAN-порт. Однако пользователь с помощью данной настройки может распределить порты между физическими разъемами самостоятельно.	
VLAN ID	Указание номера VLAN. Изначально номер задается автоматически самим устройством, однако пользователь имеет возможность его изменить.	
Switch Ports	Выбор физических портов, которые будут добавлены в VLAN	
Connection Type	Тип подключения к внешним сетям, через WAN-порт: <ul style="list-style-type: none"><li>• [A] <b>Disabled</b> – отключение WAN-порта;</li><li>• [B] <b>DHCP</b> – соединение с получением настроек от DHCP-сервера;</li><li>• [C] <b>Static</b> – соединение с ручными настройками;</li><li>• [D] <b>PPPoE</b> – соединение по протоколу PPPoE в роли клиента.</li></ul>	
Дополнительные настройки (в зависимости от выбранного типа соединения, поле <b>Connection Type</b> ):		
Поле	Тип	Описание
Ping Address	[A][B][C][D]	IP-адрес удаленного хоста для проверки работы соединения
Ping Interval (sec)	[A][B][C][D]	Интервал в секундах, через который будут отправляться пакеты для проверки соединения (по умолчанию, 30 секунд)
Ping Attempts	[A][B][C][D]	Количество неудачных попыток соединения, после которых роутер попытается подключиться через сотовую сеть (по умолчанию, 3)
Use Peer DNS Server	[B][D]	Включение/выключение использования внешних DNS-серверов провайдера
MAC	[B][C][D]	MAC-адрес роутера для созданного VLAN. Если поле оставить пустым, то будет использоваться MAC-адрес, установленный производителем
IP	[C]	IP-адрес роутера для созданного VLAN
Mask	[C]	Маска сети роутера для созданного VLAN
Gateway	[C]	Шлюз роутера для созданного VLAN
Login	[D]	Логин, который указывается при PPPoE-соединении
Password	[D]	Пароль, который указывается при PPPoE-соединении
AC-name	[D]	Имя концентратора доступа, который указывается при PPPoE-соединении

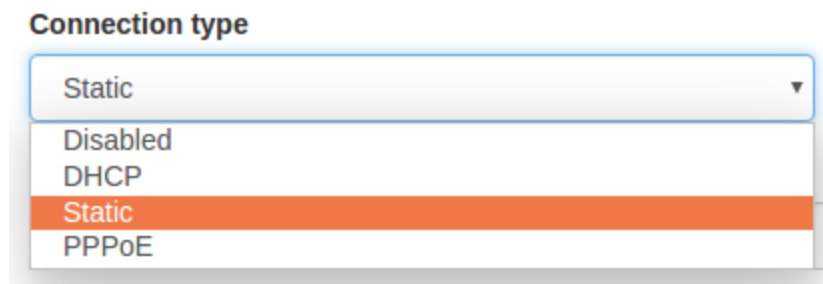
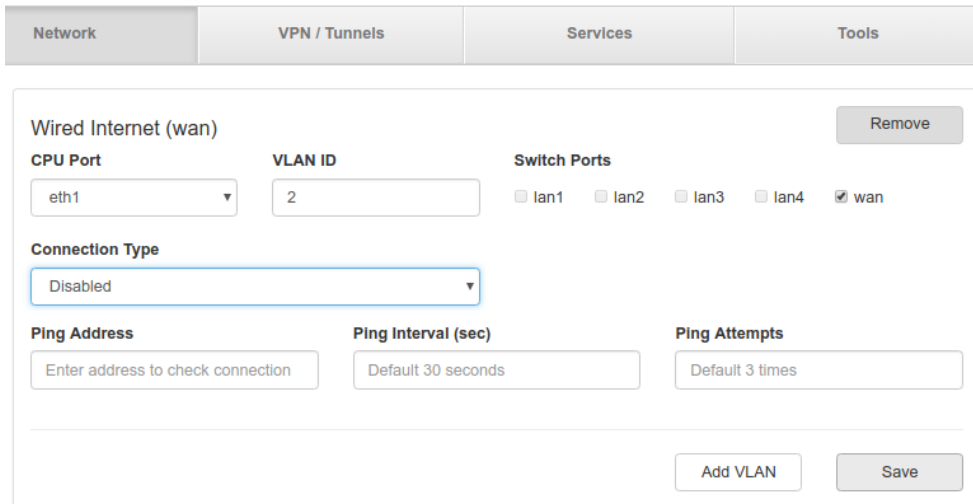


Рис. 5.9. Типы соединения для WAN-порта



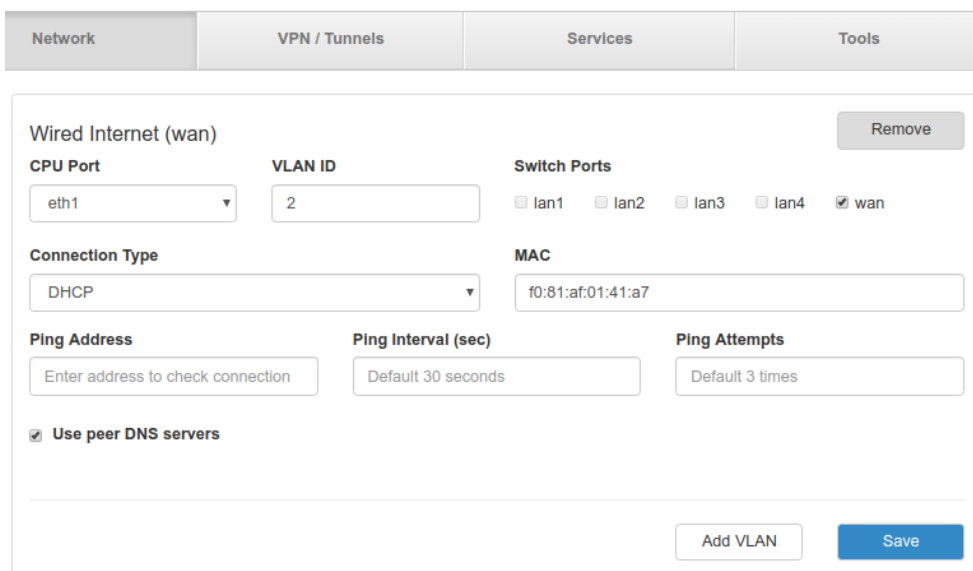
Вариант **Disabled** в поле **Connection Type** логически выключает WAN-порт, то есть физическое подключение будет присутствовать, но роутер не будет передавать по порту никаких данных. Пример настроек показан на **Рис. 5.10**, описание настроек приведено в **Таблица 5.7**.



The screenshot shows the 'Wired Internet (wan)' configuration page. At the top, there are tabs for 'Network', 'VPN / Tunnels', 'Services', and 'Tools'. The 'Network' tab is active. The configuration area includes a 'Remove' button in the top right. Below it, the 'CPU Port' is set to 'eth1', 'VLAN ID' is '2', and 'Switch Ports' has 'wan' checked. The 'Connection Type' dropdown is set to 'Disabled'. There are input fields for 'Ping Address', 'Ping Interval (sec)' (Default 30 seconds), and 'Ping Attempts' (Default 3 times). At the bottom, there are 'Add VLAN' and 'Save' buttons.

**Рис. 5.10.** WAN-порт отключен

Тип подключения **DHCP** означает, что роутер должен получить IP-адрес, маску и адреса DNS-серверов от внешнего DHCP-сервера. Пример настроек показан на **Рис. 5.11**, описание настроек приведено в **Таблица 5.7**.



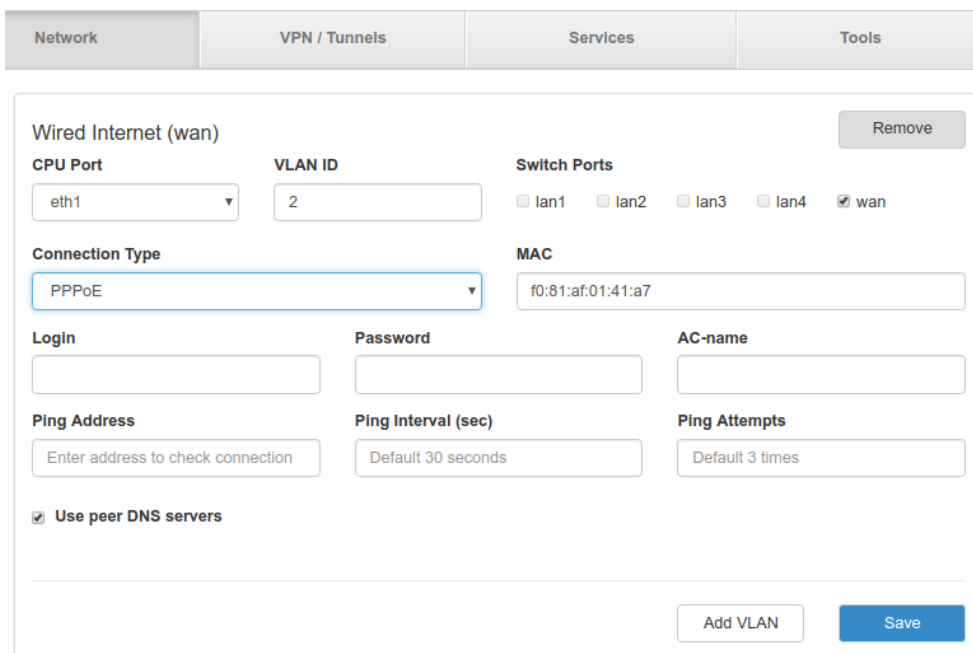
The screenshot shows the 'Wired Internet (wan)' configuration page. At the top, there are tabs for 'Network', 'VPN / Tunnels', 'Services', and 'Tools'. The 'Network' tab is active. The configuration area includes a 'Remove' button in the top right. Below it, the 'CPU Port' is set to 'eth1', 'VLAN ID' is '2', and 'Switch Ports' has 'wan' checked. The 'Connection Type' dropdown is set to 'DHCP'. There is a 'MAC' field with the value 'f0:81:af:01:41:a7'. There are input fields for 'Ping Address', 'Ping Interval (sec)' (Default 30 seconds), and 'Ping Attempts' (Default 3 times). A checkbox for 'Use peer DNS servers' is checked. At the bottom, there are 'Add VLAN' and 'Save' buttons.

**Рис. 5.11.** Тип соединения WAN-порта – DHCP

Тип подключения **Static** необходим для ручной установки сетевых настроек WAN-порта. Пример настроек показан на **Рис. 5.8**, описание настроек приведено в **Таблица 5.7**.



Тип подключения **PPPoE** необходим при использовании протокола с авторизацией на сервере PPPoE. Пример настроек показан на **Рис. 5.12**, описание настроек приведено в **Таблица 5.7**.

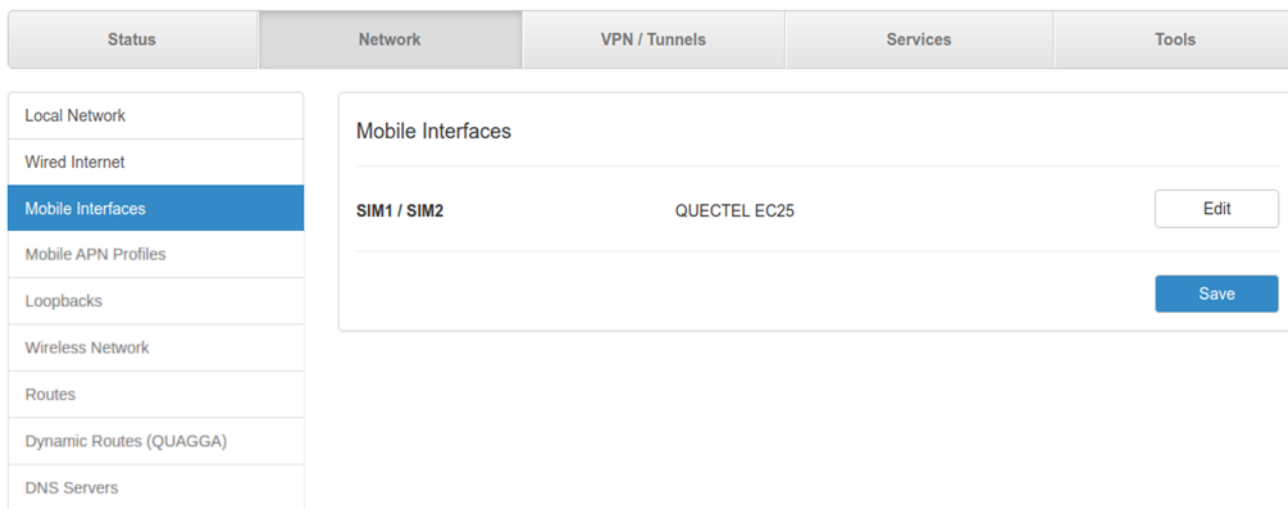


**Рис. 5.12.** Тип соединения WAN-порта – PPPoE

### 5.2.3. Mobile Interfaces

Раздел Mobile Interfaces на вкладке Network предназначен для настройки мобильного Интернета на устройстве. В зависимости от модели роутера на вкладке представлены настройки для одной или нескольких SIM-карт.

На рисунках 5.13 и 5.14 представлен раздел настроек SIM-карт для роутера с одним модулем.



**Рис. 5.13** Вкладка Network, раздел Mobile Interfaces для одномодульного устройства



Для начала редактирования настроек необходимо нажать кнопку Edit. Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!

Чтобы включать или отключать работу роутера с SIM-картой, необходимо поставить или снять галочку напротив пункта **Enable SIM1** (или **SIM2**). Нажатие на кнопку **Advanced Settings** открывает доступ ко всем возможным настройкам данного раздела.

### QUECTEL EC25

---

**Enable SIM1**

<b>APN</b> <input type="text"/>	<b>Network Access</b> Auto ▾	<b>Advanced settings</b>
<b>Username</b> <input type="text"/>	<b>Password</b> <input type="text"/>	<b>Authentication Type</b> Any ▾
<b>PIN</b> Leave blank if not needed	<b>Additional PPPD Options</b> example: debug	<b>Force MCC MNC</b> example: 25066
<b>Ping Address</b> Enter address to check connec	<b>Ping Interval (sec)</b> Default 30 seconds	<b>Ping Attempts</b> 3 by default
<input checked="" type="checkbox"/> <b>Use as defaultroute</b>	<input checked="" type="checkbox"/> <b>Use peer DNS servers</b>	<input type="checkbox"/> <b>Allow roaming</b>

---

**Enable SIM2**

<b>APN</b> <input type="text"/>	<b>Network Access</b> Auto ▾	<b>Advanced settings</b>
------------------------------------	---------------------------------	--------------------------

---

### Manage SIM

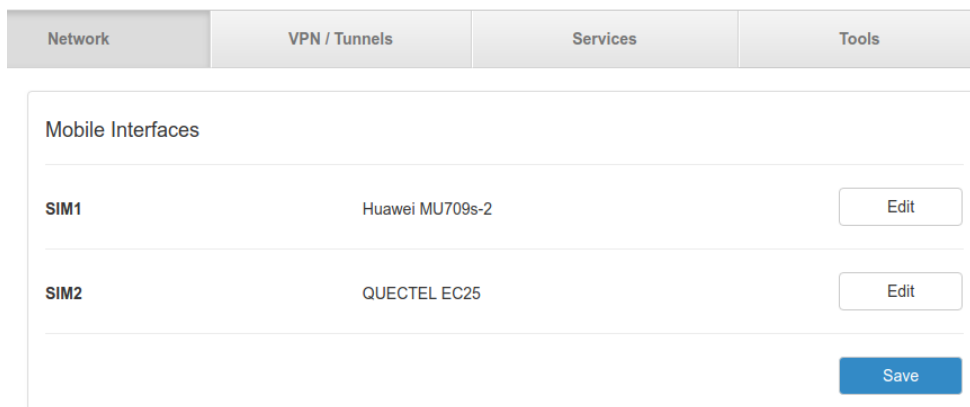
<b>Connection Timeout (sec)</b> 360	<b>Primary SIM</b> sim1 ▾	<b>Return to Primary SIM (sec)</b> 3600
--	------------------------------	--

---

**Рис. 5.14** Вкладка Network, раздел Mobile Interfaces – Edit для одномодульного устройства



На рисунках 5.15 и 5.16 представлен раздел настроек SIM-карт для роутера с двумя модулями. Для начала редактирования настроек необходимо нажать кнопку **Edit** напротив соответствующей SIM-карты или модуля. Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!

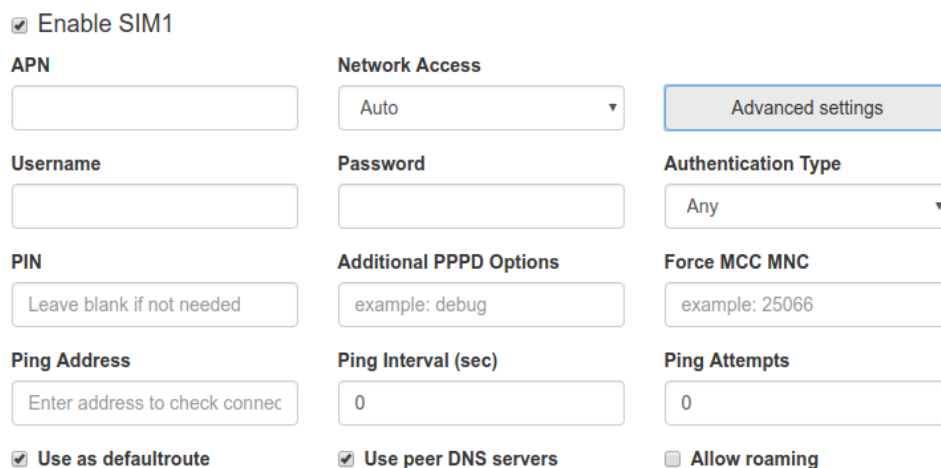


Network	VPN / Tunnels	Services	Tools
Mobile Interfaces			
SIM1	Huawei MU709s-2	<input type="button" value="Edit"/>	
SIM2	QUECTEL EC25	<input type="button" value="Edit"/>	
			<input type="button" value="Save"/>

**Рис. 5.15.** Вкладка Network, раздел Mobile Interfaces для двухмодульного устройства

Чтобы включать или отключать работу роутера с SIM-картой, необходимо поставить или снять галочку напротив пункта **Enable SIM1** (или **SIM2**). Нажатие на кнопку **Advanced Settings** открывает доступ ко всем доступным настройкам данного раздела.

Huawei MU709s-2



Enable SIM1

APN	Network Access	<input type="button" value="Advanced settings"/>
<input type="text"/>	Auto	
Username	Password	Authentication Type
<input type="text"/>	<input type="text"/>	Any
PIN	Additional PPPD Options	Force MCC MNC
Leave blank if not needed	example: debug	example: 25066
Ping Address	Ping Interval (sec)	Ping Attempts
Enter address to check connec	0	0
<input checked="" type="checkbox"/> Use as default route	<input checked="" type="checkbox"/> Use peer DNS servers	<input type="checkbox"/> Allow roaming

Manage SIM

Connection Timeout (sec)

360

**Рис. 5.16** Вкладка Network, раздел Mobile Interfaces –Edit для двухмодульного устройства



**Таблица 5.8.** Настройки Network → Mobile Interfaces–Edit

Поле	Описание
APN	Имя сотовой сети (APN). Необходимо, если у SIM-карты корпоративный тариф или выделенная сотовая сеть внутри провайдера
Authentication Type	Выбор протокола идентификации SIM-карты в сети провайдера: <ul style="list-style-type: none"><li>• Any – любой из режимов (по умолчанию);</li><li>• EAP;</li><li>• PAP;</li><li>• CHAP.</li></ul>
Network Access Mode	Выбор режима работы с сотовыми сетями: <ul style="list-style-type: none"><li>• Auto – автоматическое определение доступной сети;</li><li>• 2G Only – работа только в сети 2G;</li><li>• 3G Only – работа только в сети 3G;</li><li>• 4G Only – работа только в сети 4G.</li></ul>
Username	Имя пользователя для доступа в сотовую сеть провайдера
Password	Пароль для доступа в сотовую сеть провайдера
PIN	PIN-код SIM-карты (если установлен)
Additional PPPD Options	Указание дополнительных опций для работы протокола PPP (кроме роутеров серии R0)
Ping Address	IP-адрес удаленного хоста для проверки работы соединения
Ping Interval (sec)	Интервал в секундах, через который будут отправляться пакеты для проверки соединения (по умолчанию, 30 секунд)
Ping Attempts	Количество неудачных попыток соединения, после которых роутер попытается переподключиться к GSM оператору (по умолчанию, 3)
Allow Roaming	Разрешение/запрещение работы SIM-карты устройства в роуминге
Use Peer DNS Server	Включение/выключение использования внешних DNS-серверов провайдера
Force MCC MNC	Мобильный код страны(MCC) в комбинации с мобильным кодом сети(MNC) является уникальным идентификатором сотовой сети.
Connection Timeout (sec)	Время, которое отводится SIM-карте на подключение к сотовому оператору, по истечении данного времени роутер перезагружает сотовый модуль по питанию и дозвон начинается заново, измеряется в секундах
Primary SIM	Указывает какая из SIM карт является приоритетной (только для одномодульных роутеров)
Return to Primary SIM After (sec)	Указание промежутка времени после которого роутер произведет попытку вернуться на основную SIM карту (только для одномодульных роутеров)





### 5.2.4. Mobile APN Profiles

В данной вкладке настраиваются профили подключения к сотовой сети.

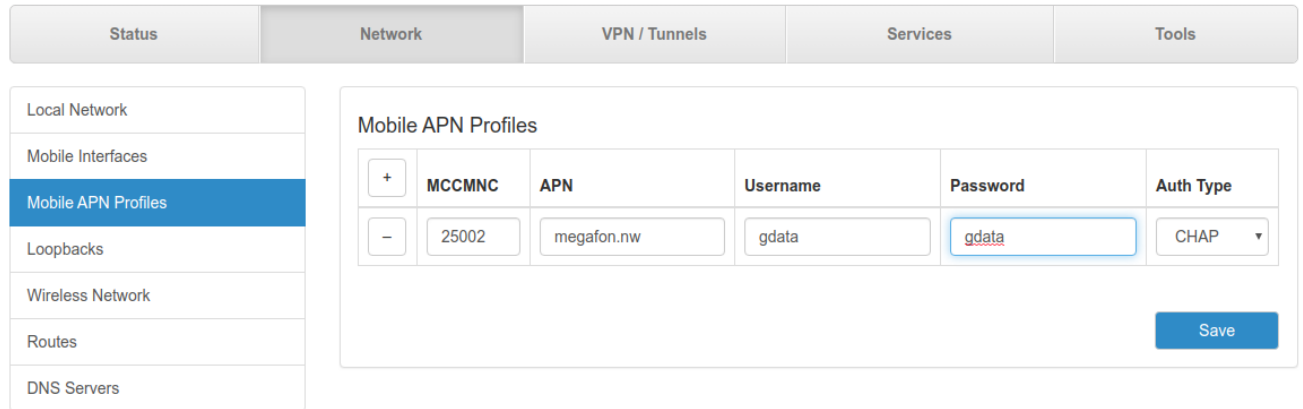


Рис. 5.17 Вкладка Mobile APN Profiles

Таблица 5.9. Вкладка Mobile APN Profiles

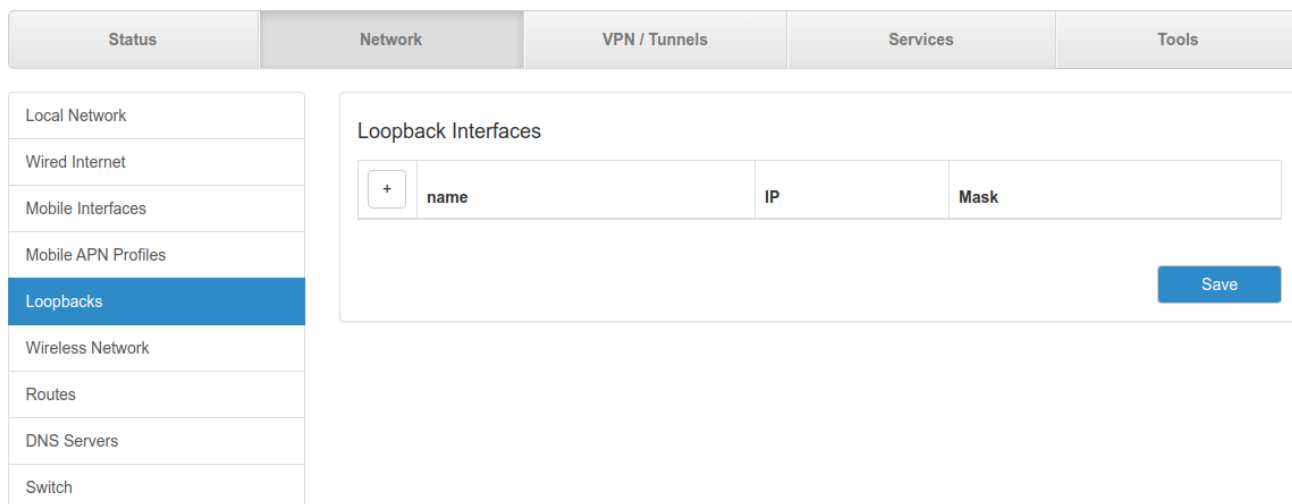
Поле	Описание
MCCMNC	Мобильный код страны(MCC) в комбинации с мобильным кодом сети(MNC) является уникальным идентификатором сотовой сети
APN	Имя сотовой сети (APN)
Username	Имя пользователя для доступа в сотовую сеть провайдера
Password	Пароль для доступа в сотовую сеть провайдера
Auth Type	Выбор протокола идентификации SIM-карты в сети провайдера: <ul style="list-style-type: none"><li>• Any – любой из режимов (по умолчанию);</li><li>• EAP;</li><li>• PAP;</li><li>• CHAP.</li></ul>



### 5.2.5. Loopbacks

В некоторых случаях необходимо назначать дополнительные IP адреса на интерфейс loopback, данный раздел предназначен для этого.

В поле name вписывается имя, в поле IP — вписывается IP-адрес, а в поле Mask — маска сети к которой принадлежит данный IP-адрес.



The screenshot shows a web interface with a top navigation bar containing tabs: Status, Network (selected), VPN / Tunnels, Services, and Tools. On the left, a sidebar menu lists various network settings: Local Network, Wired Internet, Mobile Interfaces, Mobile APN Profiles, Loopbacks (highlighted in blue), Wireless Network, Routes, DNS Servers, and Switch. The main content area is titled 'Loopback Interfaces' and contains a table with columns for '+', 'name', 'IP', and 'Mask'. Below the table is a blue 'Save' button.

Рис. 5.18 Вкладка Network, раздел Loopbacks

Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!

### 5.2.6. Wireless Internet

Раздел Wireless Network на вкладке Network предназначен для настройки параметров Wi-Fi. Данный раздел доступен в роутерах, которые поддерживают работу с Wi-Fi (см. обозначение в названии модели – «w»). На Рис. 5.19 представлен пример настроек, когда Wi-Fi выключен.

Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!



**Рис. 5.19.** Вкладка Network, раздел Wireless Internet

**Wi-Fi mode** — выбор режима работы модуля Wi-Fi:

- **Access point** — роутер работает в качестве точки доступа и ждет подключения клиентов к своей сети;
- **Client** — роутер сам подключается к внешней Wi-Fi-сети, в данном режиме интерфейс автоматически становится одним из WAN-портов;
- **Disabled** — отключение Wi-Fi-модуля.

**Access Point.**

Access Point - режим работы Wi-Fi-модуля в режиме точки доступа.

**Таблица 5.10.** Настройки Network → Wireless Network (Wi-Fi Mode = Access Point)

Поле	Описание
Bridge with Interface	Создание моста с локальным интерфейсом или создание нового интерфейса
IP	IP-адрес интерфейса роутера
Mask	Маска сети интерфейса роутера
SSID	Название Wi-Fi-сети, к которой будут подключаться клиенты
Channel	Номер канала, на котором должна работать Wi-Fi-сеть
Hide Wireless Network	Включить/отключить работу в скрытном режиме, то есть без анонсирования своего SSID
Freq	Переключение частоты работы Wi-Fi модуля
Region	Код страны (значение по умолчанию - default)
Access Mode	Тип шифрования пароля доступа к создаваемой Wi-Fi-сети: <ul style="list-style-type: none"> <li>• Open – без пароля доступа;</li> <li>• WPA;</li> <li>• WPA2-PSK.</li> </ul>
Password	Пароль для доступа к создаваемой Wi-Fi-сети



При выборе в настройке **Bridge with Interface** пункта **LAN**, Wi-Fi-интерфейс роутера будет работать в режиме моста с LAN-портами. Доступные настройки приведены на **Рис. 5.19**

При выборе в настройке **Bridge with Interface** пункта **Wi-Fi**, Wi-Fi-интерфейс будет работать, как самостоятельный интерфейс. Доступные настройки приведены на **Рис. 5.20**

WiFi mode:

- Access point
- Client
- Disabled

Bridge with interface

IP

Mask

SSID

Channel

Hide wireless network

Access mode

Password

**Рис. 5.20.** Режим Wi-Fi настройки Bridge with Interface

### Client

Client - режим работы Wi-Fi-модуля в режиме клиента при подключении к удаленной сети.

**Таблица 5.11.** Настройки Network → Wireless Network (Wi-Fi Mode = Client)

Поле	Описание
Connection Type	Выбор типа соединения: <ul style="list-style-type: none"><li>• DHCP – получение IP-адреса от сервера DHCP;</li><li>• Static – статические настройки роутера, прописываемы вручную.</li></ul>
IP	IP-адрес интерфейса роутера
Mask	Маска сети интерфейса роутера
Gateway	Шлюз роутера
Ping Address	IP-адрес удаленного хоста для проверки работы соединения
Ping Interval (sec)	Интервал в секундах, через который будут отправляться пакеты для проверки соединения (по умолчанию, 30 секунд)
Use Peer DNS Server	Включение/выключение использования внешних DNS-серверов провайдера
SSID	Название Wi-Fi-сети, к которой будут подключаться клиенты
Access Mode	Тип шифрования пароля доступа к создаваемой Wi-Fi-сети: <ul style="list-style-type: none"><li>• Open – без пароля доступа;</li><li>• WPA;</li><li>• WPA2-PSK.</li></ul>
Password	Пароль для доступа к создаваемой Wi-Fi-сети



При выборе в настройке **Connection Type** пункта **DHCP**, роутер будет получать настройки соединения от DHCP-сервера сети к которой подключается. Доступные настройки приведены на **Рис. 5.21**.

WiFi mode:

Access point  
 Client  
 Disabled

Conection Type

DHCP

Ping address

Ping interval (sec)

Use peer DNS servers

SSID

iRZ-584EDB

Access mode

WPA2-PSK

Password

\*\*\*\*\*

**Рис. 5.21.** Режим DHCP настройки Connection Type

При выборе в настройке **Connection Type** пункта **Static**, роутер будет работать со статическими настройками соединения, которые указываются в пунктах **IP**, **Mask** и **Gateway**. Доступные настройки приведены на **Рис. 5.22**.

WiFi mode:

Access point  
 Client  
 Disabled

Conection Type

Static

IP

Mask

Gateway

Ping address

Ping interval (sec)

SSID

iRZ-584EDB

Access mode

WPA2-PSK

Password

\*\*\*\*\*

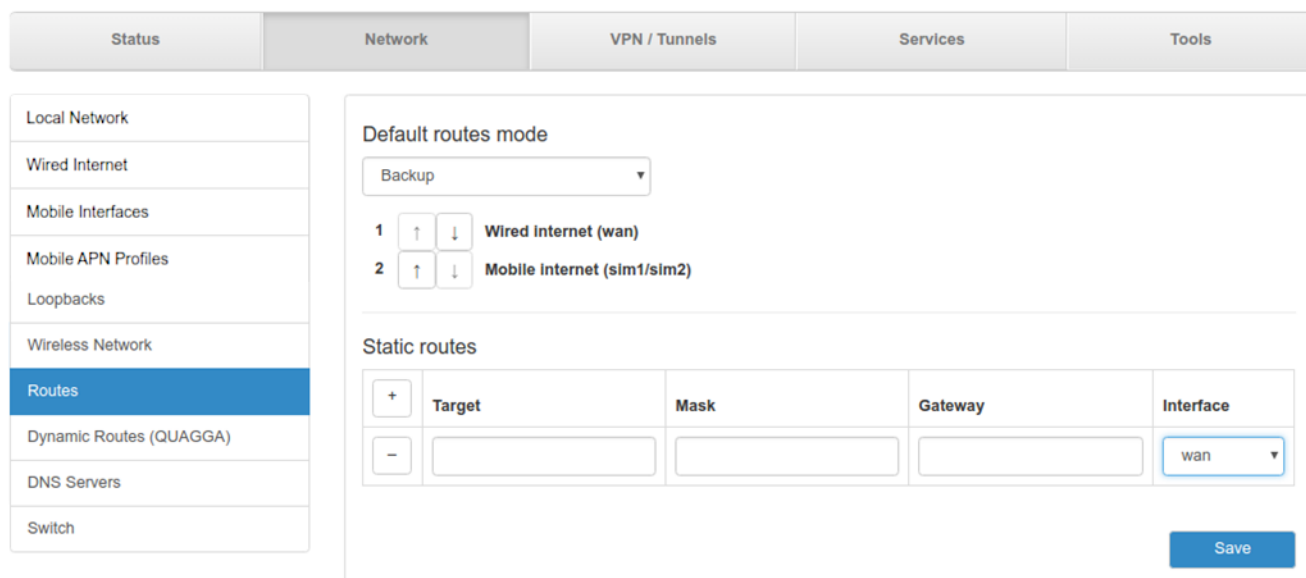
**Рис. 5.22.** Режим Static, настройки Connection Type



### 5.2.7. Routes

Раздел Routes на вкладке Network предназначен для настройки приоритетов WAN-портов, режим их работы и настройки статических маршрутов. На **Рис. 5.23** представлен пример настроек.

Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!



Status	Network	VPN / Tunnels	Services	Tools
Local Network				
Wired Internet				
Mobile Interfaces				
Mobile APN Profiles				
Loopbacks				
Wireless Network				
<b>Routes</b>				
Dynamic Routes (QUAGGA)				
DNS Servers				
Switch				

Default routes mode

Backup

1 ↑ ↓ Wired Internet (wan)

2 ↑ ↓ Mobile internet (sim1/sim2)

Static routes

	Target	Mask	Gateway	Interface
+				wan
-				

Save

**Рис. 5.23.** Вкладка Network, раздел Routes

**Default Routes Mode** — режим работы WAN-портов:

- **Balance** — режим балансировки;
- **Backup** — режим резервирования.

В режиме **Backup** роутер резервирует подключение между WAN-портами последовательно и в порядке, указанном пользователем (см. список под пунктом Backup на **Рис. 5.23**). С помощью стрелок можно перемещать выбранный WAN-порт (на рисунке «Wired Internet (WAN)») вверх ↑ или вниз ↓ в зависимости от приоритетов пользователя.

В режиме **Balance** роутер балансирует исходящий трафик между портами для увеличения пропускной способности. Данный режим доступен только при подключении роутера через два WAN-порта.

После выбора режима работы WAN портов следует подраздел настройки статических маршрутов, **Static Routes**, на **Рис. 5.24**



Default routes mode

backup ▾

1   Wired internet (wan)

2   Mobile internet (sim1)

3   Mobile internet (sim2)

---

Static routes

<input type="button" value="+"/>	Target	Mask	Gateway	Interface
<input type="button" value="-"/>	192.168.2.5	255.255.255.0	192.168.1.1	loopback ▾ loopback pptp sim1 sim2 wan ovpn gre1tun lan lan84

Рис. 5.24. Настройка статических маршрутов

Добавление нового маршрута происходит по кнопке  («плюс») в первом столбце таблицы. А удаление маршрута по кнопке  («минус»), также в первом столбце, но напротив строки ненужного маршрута. Настройки маршрутов указаны в таблице 5.12.

Таблица 5.12. Настройки маршрутов

Поле	Описание
Target	IP-адрес или подсеть назначения маршрута
Mask	Маска сети
Gateway	IP-адрес шлюза маршрута
Interface	Выбор интерфейса, через который будет работать маршрут



### 5.2.8. Dynamic Routes(QUAGGA, только для роутеров серии R4)

Данный раздел предназначен для настройки динамической маршрутизации по протоколам: BGP, OSPF. Пример настроек приведен на **Рис. 5.25**

BGPD

```
password zebra
!  
access-list vty permit 127.0.0.0/8  
access-list vty deny any  
!  
line vty  
access-class vty
```

OSPF6D

```
password zebra
!  
access-list vty permit 127.0.0.0/8  
access-list vty deny any  
!  
line vty  
access-class vty
```

OSPFD

```
password zebra
!  
access-list vty permit 127.0.0.0/8  
access-list vty deny any  
!  
line vty  
access-class vty
```

ZEBRA

```
password zebra
!  
access-list vty permit 127.0.0.0/8  
access-list vty deny any  
!  
line vty  
access-class vty
```

**Рис. 5.25** Пример настройки динамической маршрутизации по протоколам: BGP, OSPF





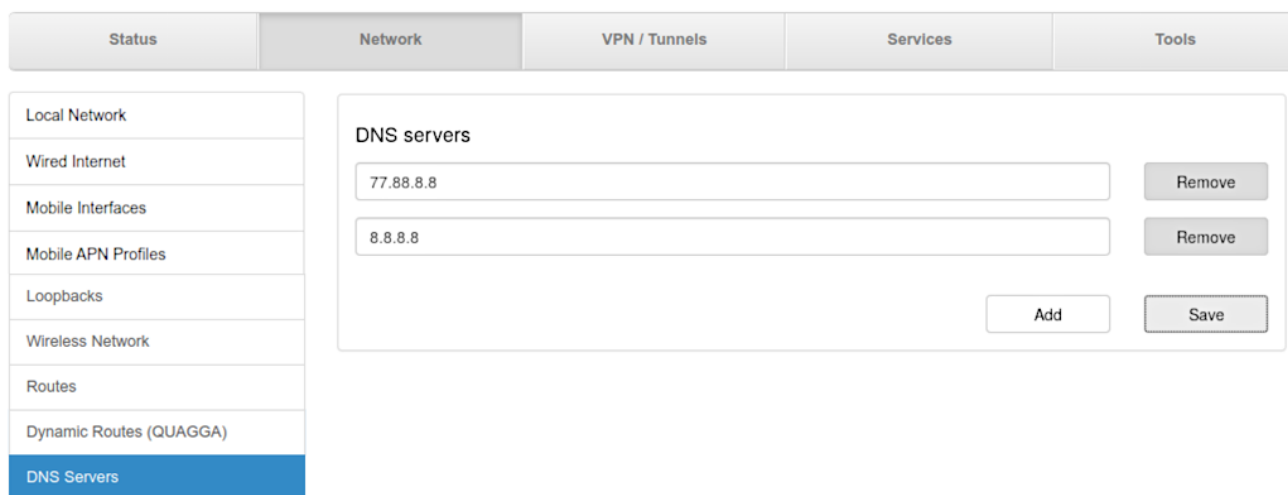
Динамическая маршрутизация в роутерах представлена пакетом Quagga для GNU/Linux систем. Процесс настройки динамической маршрутизации представляет собой заполнение текстового поля соответствующей службы соответствующего протокола в формате синтаксиса, определенного для данного пакета. Активация поля происходит по чекбоксу возле соответствующей службы.

Представлены следующие службы: BGPD – демон протокола bgp, OSPF6D – демон протокола OSPFv3 для IPv6, OSPFD – демон протокола OSPFv2. Поле ZEBRA предназначено для настройки базового ядра Zebra.

### 5.2.9. DNS Servers

Раздел DNS Servers на вкладке Network предназначен для указания адресов DNS-серверов. На **Рис. 5.26** представлен пример настроек с двумя адресами.

Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!



**Рис. 5.26.** Вкладка Network, раздел DNS Servers

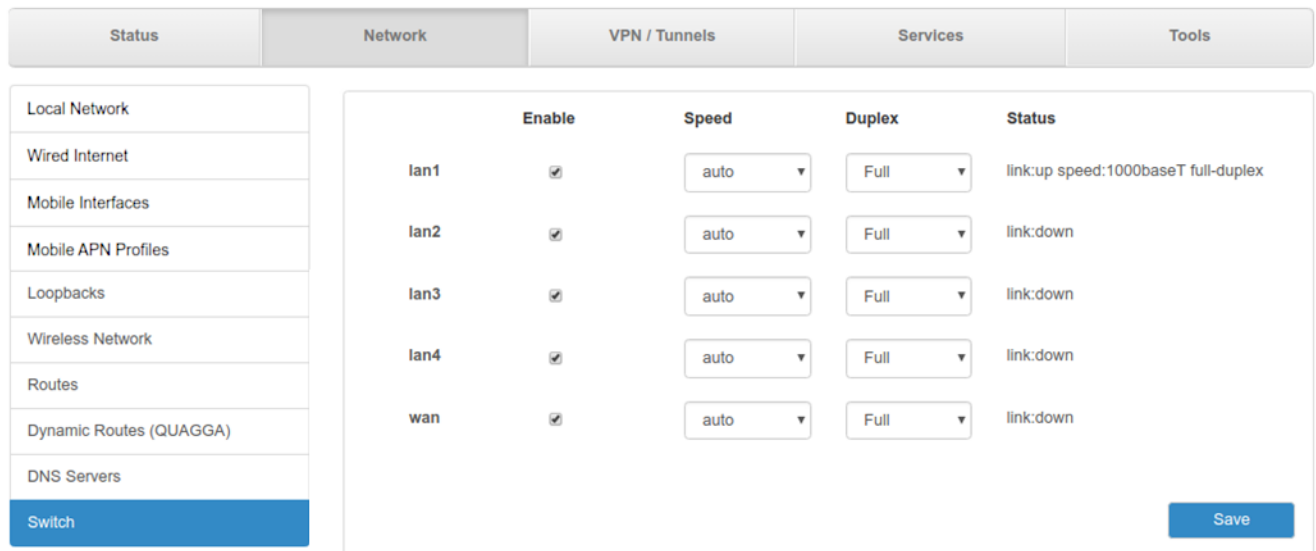
Чтобы добавить новый адрес нажмите кнопку **Add** и впишите IP-адрес DNS-сервера в появившееся поле. Чтобы удалить, один из адресов, нажмите кнопку **Remove** напротив поля адреса, который необходимо удалить.



### 5.2.10. Switch

Раздел Switch на вкладке Network предназначен для управления Ethernet-портами роутера (LAN и WAN). На **Рис. 5.27** представлен пример настройки портов роутера R4.

Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!



	Enable	Speed	Duplex	Status
lan1	<input checked="" type="checkbox"/>	auto	Full	link:up speed:1000baseT full-duplex
lan2	<input checked="" type="checkbox"/>	auto	Full	link:down
lan3	<input checked="" type="checkbox"/>	auto	Full	link:down
lan4	<input checked="" type="checkbox"/>	auto	Full	link:down
wan	<input checked="" type="checkbox"/>	auto	Full	link:down

**Рис. 5.27.** Вкладка Network, раздел Switch

**Таблица 5.13.** Настройки маршрутов

Поле	Описание
Enable	Включение/выключение работы порта
Speed	Выбор скорости работы порта: Auto (выбор скорости устройством), 10, 100, 1000 Мбит/с
Duplex	Выбор режима работы порта: <ul style="list-style-type: none"><li>• Full – передача и прием данных одновременно;</li><li>• Half – передача и прием данных по очереди.</li></ul>
Status	Информация о работе каждого порта



### 5.3. Раздел VPN/Tunnels

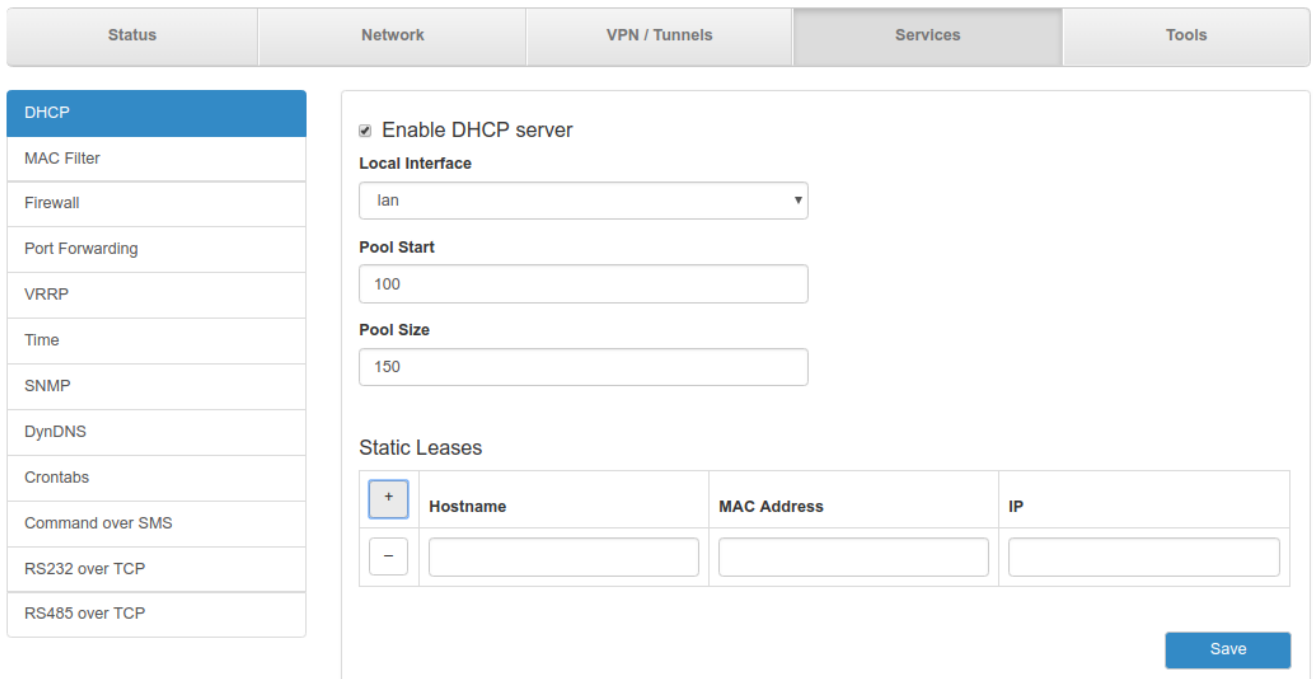
Подробную информацию о туннелях и их настройке можно прочитать в документе «**РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ Настройка туннелей на роутерах iRZ**» на сайте [www.radiofid.ru](http://www.radiofid.ru).

### 5.4. Раздел «Services»

#### 5.4.1. DHCP

Раздел DHCP на вкладке Services предназначен для управления DHCP-сервером. На **Рис. 5.28** представлен пример настройки DHCP-сервера.

Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!



The screenshot shows the DHCP configuration interface. At the top, there are navigation tabs: Status, Network, VPN / Tunnels, Services (selected), and Tools. On the left, a sidebar menu lists various services: DHCP (selected), MAC Filter, Firewall, Port Forwarding, VRRP, Time, SNMP, DynDNS, Crontabs, Command over SMS, RS232 over TCP, and RS485 over TCP. The main content area is titled 'DHCP' and contains the following settings:

- Enable DHCP server
- Local Interface:** lan (dropdown menu)
- Pool Start:** 100 (text input)
- Pool Size:** 150 (text input)
- Static Leases:** A table with columns for Hostname, MAC Address, and IP. There is a '+' button to add a new entry and a '-' button to remove one. The table currently contains one empty row.

A 'Save' button is located at the bottom right of the configuration area.

**Рис. 5.28.** Вкладка Services, раздел DHCP

Чтобы включить DHCP-сервер поставьте галочку напротив **Enable DHCP Server** и укажите настройки для его работы (см. таблицу 5.14).



Таблица 5.14. Настройки адресов

Поле	Описание
Local Interface	Выбор интерфейса на котором будет работать DHCP-сервер: LAN, LAN1, Wi-Fi (количество портов на выбор зависит от настроек локальной сети роутера и настроек Wi-Fi)
Pool Start	Адрес, с которого начнется диапазон раздаваемых адресов. Например, для указания диапазона с адреса 192.168.1. <b>100</b> (где, например, 192.168.1.0 – адрес сети, в которой работает устройство) и выше, необходимо указать значение четвертой секции (100)
Pool Size	Размер раздаваемого адресного пространства. Например, при Pool Start = 100 необходимо раздать адреса с 192.168.1.100 по 192.168.1.250 (150 адресов), тогда необходимо указать значение 150.
Static Leases – привязка IP-адреса к определенному сетевому устройству	
Hostname	Имя устройства (произвольно, на выбор пользователя)
MAC Address	MAC-адрес, по которому идентифицируется устройство и назначается IP-адрес
IP	IP-адрес, который назначается при идентификации MAC-адреса

Добавление нового адреса в подраздел Static Leases происходит по кнопке  («плюс») в первом столбце таблицы. А удаление адреса по кнопке  («минус»), также в первом столбце, но напротив строки ненужного адреса. Описания параметров указаны в таблице 5.14.

#### Static Leases

<input type="button" value="+"/> +	Hostname	MAC address	IP
<input type="button" value="-"/> -	<input type="text" value="debian"/>	<input type="text" value="FF:FF:FF:FF:FF:FF"/>	<input type="text" value="192.168.1.3"/>

Рис. 5.29. Указание IP-адресов вручную



## 5.4.2. MAC Filter

Раздел MAC Filter на вкладке Services предназначен для установки и настройки фильтра по MAC-адресам только для роутеров с модулем Wi-Fi. На **Рис. 5.30** представлен пример настройки фильтра.

Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!

Status	Network	VPN / Tunnels	Services	Tools
DHCP				
<b>MAC Filter</b>				
Firewall				
Port Forwarding				
VRRP				
Time				
SNMP				
DynDNS				
Crontabs				

Enable MAC Filter

Filter Mode

Black list  White list

MAC list

	Comment	MAC
<input type="button" value="+"/> <input type="button" value="-"/>	Notebook Acer 51	00:0c:35:1a:18:11

**Рис. 5.30.** Вкладка Services, раздел MAC Filter

Чтобы задействовать фильтр, поставьте галочку напротив **Enable MAC Filter**. Далее необходимо будет выбрать принцип, по которому будет работать фильтрация, выбрав одно из значений в подразделе **Filter Mode**:

- **Black List** – адреса, указанные в таблице MAC List будут блокироваться, со всеми остальными адресами работа будет разрешена;
- **White List** – работа с адресами, указанными в таблице MAC List будет разрешена, все остальные адреса будут блокироваться.

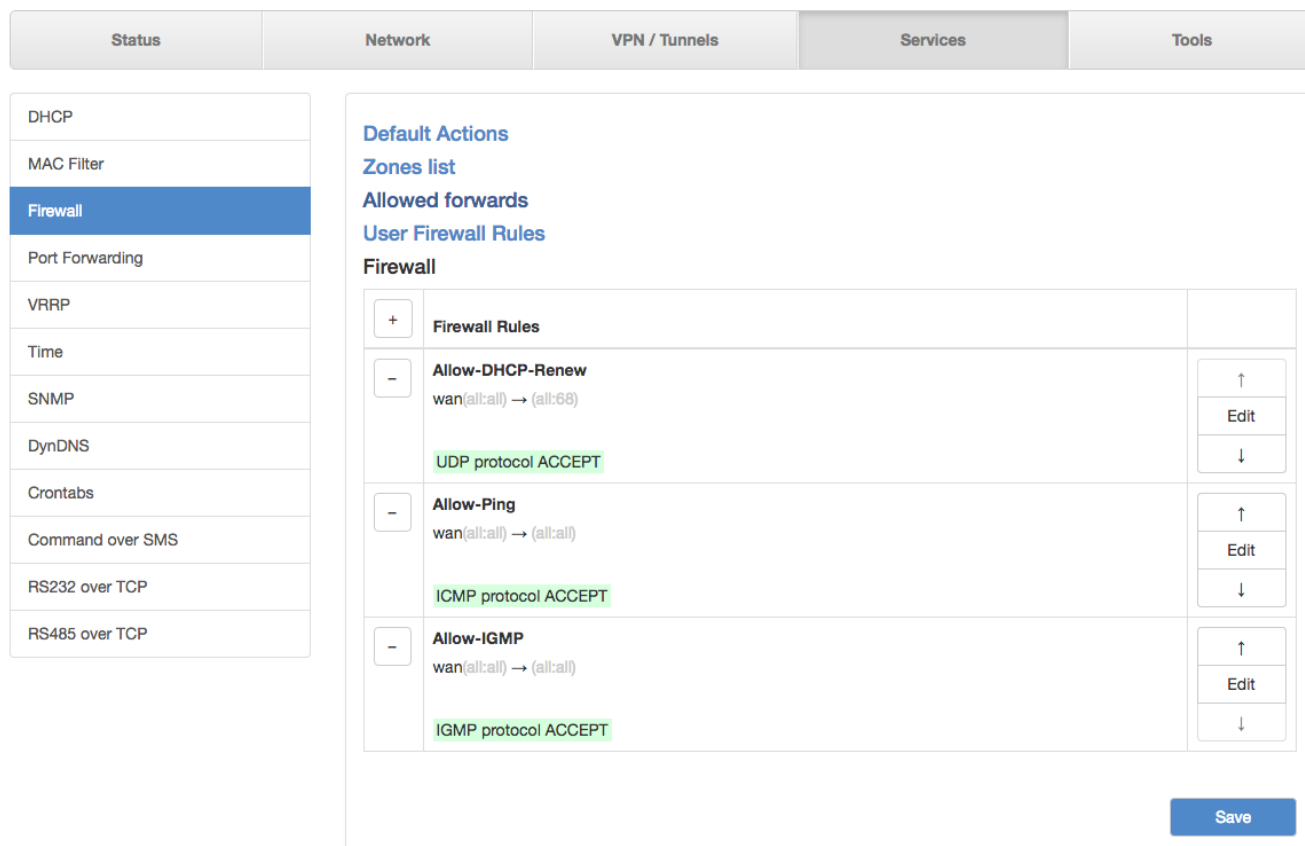
Добавление нового адреса в таблице MAC List происходит по кнопке  («плюс») в первом столбце таблицы. А удаление адреса по кнопке  («минус»), также в первом столбце, но напротив строки ненужного адреса. MAC-адрес необходимо вписывать в поле **MAC**, а поле **Comment** служит для комментариев.



### 5.4.3. Firewall

Раздел Firewall на вкладке Services предназначен для настройки межсетевого экрана (файрволла). Настройки разбиты на пять подгрупп: **Default Actions**, **Zones list**, **Allowed forwards**, **User Firewall Rules**, **Firewall**. На **Рис. 5.31** представлен пример стандартной настройки межсетевого экрана.

Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!



Status	Network	VPN / Tunnels	Services	Tools
DHCP				
MAC Filter				
<b>Firewall</b>				
Port Forwarding				
VRRP				
Time				
SNMP				
DynDNS				
Crontabs				
Command over SMS				
RS232 over TCP				
RS485 over TCP				

**Default Actions**  
**Zones list**  
**Allowed forwards**  
**User Firewall Rules**  
**Firewall**

+	Firewall Rules	
-	<b>Allow-DHCP-Renew</b> wan(all:all) → (all:68)  UDP protocol ACCEPT	↑ Edit ↓
-	<b>Allow-Ping</b> wan(all:all) → (all:all)  ICMP protocol ACCEPT	↑ Edit ↓
-	<b>Allow-IGMP</b> wan(all:all) → (all:all)  IGMP protocol ACCEPT	↑ Edit ↓

Save

**Рис. 5.31.** Вкладка Services, раздел Firewall

#### Default Actions

Подгруппа настроек Default Actions определяет глобальные установки файрвола, которые не принадлежат каким-либо конкретным зонам. Выбор глобальных установок осуществляется соответственным выбором в необходимом поле. Полей три : Input – отвечает за действия над входящим трафиком данных; Output – отвечает за действия над исходящим трафиком данных; Forward – отвечает за действия над проходящим через firewall трафиком данных.

Настройки по умолчанию данной секции представлены на **Рис. 5.32**



### Default Actions

Input	Output	Forward
REJECT	ACCEPT	REJECT

Рис. 5.32 Вкладка Services, раздел Firewall, настройки Default Actions

### Zones List

Подгруппа настроек Zones List отвечает за разбиение на зоны, в которых можно объединять интерфейсы между собой и назначать правила для входящего, исходящего и перенаправляемого трафика. Выбор нескольких интерфейсов в одной зоне осуществляется с помощью зажатой клавиши Ctrl. Добавление правил осуществляется посредством кнопки  («плюс»), а удаление — кнопкой  («минус»). Настройки зон представлены в таблице 5.15.

Таблица 5.15. Настройки правил для зон

Поле	Описание
Zone Name	Имя зоны (по умолчанию, две зоны – LAN и WAN)
Interfaces	Выбор интерфейсов роутера, которые будут входить в зону
Input	Выбор действия для входящего трафика: <b>Accept</b> – принимать, <b>Reject</b> – отклонять, <b>Drop</b> – отбрасывать, <b>Notrack</b> – не отслеживать.
Output	Выбор действия для исходящего трафика: <b>Accept</b> – принимать, <b>Reject</b> – отклонять, <b>Drop</b> – отбрасывать, <b>Notrack</b> – не отслеживать.
Forward	Выбор действия для перенаправляемого трафика: <b>Accept</b> – принимать, <b>Reject</b> – отклонять, <b>Drop</b> – отбрасывать, <b>Notrack</b> – не отслеживать.
Masquerade	Включение/выключение маскировки трафика, то есть работы службы NAT

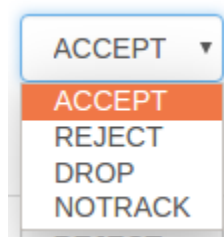


Рис. 5.33. Вариант выбора действий для трафика



### Zones list

	Zone name	Interfaces	Input	Output	Forward	Masquerade
+	lan	pppol2tp1 lan ovpn wan	ACCEPT	ACCEPT	ACCEPT	<input type="checkbox"/>
-	wan	loopback sim1 sim2 pppol2tp1	REJECT	ACCEPT	REJECT	<input checked="" type="checkbox"/>

**Рис. 5.34** Вкладка Services, раздел Firewall, настройки Zones List

### Allowed Forwards

Подгруппа настроек Allowed Forwards отвечает за контроль трафика между зонами, которые создаются в подгруппе Zone List. Можно разрешить перенаправление трафика от одного интерфейса к другому, если распределить эти интерфейсы в различные зоны. Например, в настройках на **Рис. 5.34** в зону **LAN** входят интерфейсы LAN, а в зону **WAN** – SIM1, SIM2. Правило «**LAN**→**WAN**» означает, что трафик с интерфейсов LAN (локальные порты) разрешено перенаправлять на интерфейсы SIM-карт. Это правило создано по умолчанию, и если его убрать, то передача трафика от локальных портов в зону **WAN** станет невозможной.

Добавление правил осуществляется посредством кнопки  («плюс»), а удаление — кнопкой  («минус»). Настройки правил представлены в таблице 5.16.

### Allowed forwards

	Source	Destination
-	lan	wan

**Рис. 5.35.** Настройки Allowed Forwards

**Таблица 5.16.** Настройки правил для направлений

Поле	Описание
Source	Выбор интерфейса, который будет являться источником трафика
Destination	Выбор интерфейса, который будет приемником трафика





## User Firewall Rules

Подгруппа настроек User Firewall Rules предназначена для внесения цепочек правил в формате iptables. На Рис. 5.36 представлен пример настройки правила, позволяющего открыть доступ к web интерфейсу роутера со стороны WAN зоны. Правила пишутся с клавиатуры в левое поле настроек. Данное поле можно увеличивать в размерах, потянув за нижний правый угол поля. Справа от поля настроек есть информационная табличка указаниям которой следует руководствоваться при написании собственных цепочек правил.

### User Firewall Rules

```
# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into
the
# special user chains, e.g. input_wan_rule or postrouting_lan_rule.
iptables -A input_rule -j ACCEPT -p tcp --dport 80|
```

Please use follow custom chains:

```
"nat" table:
- prerouting_rule for PREROUTING rules
- postrouting_rule for POSTROUTING rules

"filter" table:
- input_rule for INPUT rules
- output_rule for OUTPUT rules
- forward_rule for FORWARD rules
```

Рис. 5.36 Вкладка Services, раздел Firewall, настройки User Firewall Rules

## Firewall

Подгруппа настроек Firewall отвечает за создание правил для межсетевого экрана. Правила задаются для сетевых протоколов и интерфейсов. Например, указывается направление движение через интерфейсы – «wan(all:all) → (all:68)» (все адреса и порты от зоны WAN на все остальные адреса с портом 68), протокол – UDP, и действие – «Асерт» (принимать и обрабатывать).

Добавление правил осуществляется посредством кнопки  («плюс»), а удаление — кнопкой  («минус»). Для редактирования правил используется кнопка «Edit» напротив соответствующего правила. Изменение приоритета правил, то есть положение в очереди выполнения, где сначала выполняются «верхние» правила, осуществляется посредством кнопок  («вверх») и  («вниз»).



## Firewall

Firewall rules		
-	<b>Allow-DHCP-Renew</b> wan(all:all) → (all:68)  UDP protocol ACCEPT	↑ Edit ↓
-	<b>Allow-Ping</b> wan(all:all) → (all:all)  ICMP protocol ACCEPT	↑ Edit ↓
-	<b>Auto-OpenVPN-access</b> wan(all:all) → (all:1194)  UDP protocol ACCEPT	↑ Edit ↓
-	<b>Auto-GRE-access</b> wan(all:all) → (all:all)  GRE protocol ACCEPT	↑ Edit ↓

Рис. 5.37. Настройки Firewall

По умолчанию роутер все входящие подключения с WAN-интерфейсов блокирует, поэтому в разделе уже присутствует два правила «**Allow-DHCP-Renew**» и «**Allow-Ping**». Первое правило позволяет получать роутеру адреса от внешнего DHCP-сервера, а второе позволяет проверять роутер на доступность из внешней сети посредством ping-запросов.



При добавлении нового правила или редактировании уже существующего правила, настройки открываются в новом окне, см. **Рис. 5.38**

Edit firewall rule: Allow-DHCP-Renew

Name: Allow-DHCP-Renew

Source: Zone: wan, IP: 0.0.0.0/0, Port: 0

Destination: Zone: Any, IP: 0.0.0.0/0, Port: 68

Protocol: udp, Target: ACCEPT

Buttons: Close, Save changes

**Рис. 5.38.** Редактирование правила Firewall

**Таблица 5.17.** Настройки правил для межсетевого экрана

Поле	Описание
Name	Название правила (произвольное имя на выбор пользователя)
Source	Подраздел, который отвечает за настройку источника трафика
Destination	Подраздел, который отвечает за настройку приемника трафика
Zone	Выбор зоны, для которой создается правило. <b>Any</b> – любая зона
IP	Ввод диапазона IP-адресов, на которые будет распространяться правило. Адреса вводятся в формате «0.0.0.0/0», в котором, например, «192.168.0.25/150» означает, что правило распространяется на диапазон адресов от 192.168.0.25 до 192.168.0.150. Если значение не указывать, то правило распространяется на любой адрес
Port	Ввод порта, на который будет распространяться правило. Если значение не указывать, то правило распространяется на любой порт
Protocol	Выбор протокола, на который будет распространяться правило
Target	Выбор действия для трафика: <b>Accept</b> – принимать, <b>Reject</b> – отклонять, <b>Drop</b> – отбрасывать, <b>Notrack</b> – не отслеживать (подробнее см. в разделе 5.4.3, подразделе Zone List)

После выполнения настройки, чтобы сохранить внесенные изменения, нажмите кнопку **Save Changes**. Чтобы закрыть окно без сохранения изменений, нажмите кнопку **Close**.



#### 5.4.4. Port Forwarding

Раздел Port Forwarding на вкладке Services предназначен для настройки проброса портов со стороны WAN-интерфейса на локальные порты роутера. На **Рис. 5.39** представлен пример настройки.

Добавление правил проброса осуществляется посредством кнопки  («плюс»), а удаление — кнопкой  («минус»).

Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!



<input type="button" value="+"/>	Protocol	Src IP	Src Port	Dest IP	Dest Port	Comment
<input type="button" value="-"/>	TCP					

**Рис. 5.39.** Вкладка Services, раздел Port Forwarding

**Таблица 5.18.** Настройки правил проброса портов

Поле	Описание
Protocol	Выбор протокола, на который будет распространяться правило: <b>TCP</b> , <b>UDP</b> , <b>TCP/UDP</b> (оба протокола) или <b>ALL</b> (предназначен для организации DMZ зоны)
Src IP	Указывается один IP адрес, с которого будет разрешено подключение к данному порту. Если ограничивать доступ к порту необходимости нет — после следует оставить пустым
Src Port	Порт источника трафика, который «прослушивает» роутер на попытки установки соединения
Dest Port	Порт приемника трафика, на который роутер будет пересылать пакеты
Dest IP	Ввод IP-адреса приемника трафика, на который роутер будет пересылать пакеты
Comment	Поле для комментария



### 5.4.5. VRRP

Раздел VRRP на вкладке Services предназначен для настройки сетевого протокола VRRP, применяемый для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию. По сути, создается один виртуальный маршрутизатор (роутер) на базе нескольких физических роутеров, для которых назначается один общий IP-адрес, используемый, как шлюз по умолчанию для компьютеров в сети. Преимущество виртуального маршрутизатора в большей надежности узла, ведь если один из роутеров выйдет из строя, узел на базе виртуального маршрутизатора продолжит функционировать. На **Рис. 5.40** представлен пример настройки VRRP.

Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!

Enable VRRP

<b>Interface</b>	<b>Virtual MAC</b>
lan	Do not set
<b>Virtual IP Address</b>	<b>Check Interval (sec)</b>
192.168.1.200	30
<b>Virtual Server ID (1-255)</b>	<b>Priority (1-255)</b>
123	20

**Save**

**Рис. 5.40.** Вкладка Services, раздел VRRP

Чтобы включить VRRP, поставьте галочку напротив **Enable VRRP** и задайте соответствующие настройки (см. таблицу 5.19).

**Таблица 5.19.** Настройки правил проброса портов

Поле	Описание
Interface	Выбор интерфейса, через который будет работать VRRP. <b>None</b> – ничего не использовать или <b>LAN</b> — через lan порты
Virtual IP Address	IP-адрес, который будет использоваться для виртуального маршрутизатора
Check Interval (sec)	Интервал времени в секундах, через который будет проверяться доступность Master-маршрутизатора
Router ID	Цифровой идентификатор роутера, значение от «1» до «255»
Priority	Приоритет виртуального маршрутизатора, который отправляет пакет, значение от «1» до «255». Чем больше цифра, тем выше приоритет (255 – Master, 1-254 – остальные маршрутизаторы, 0 – выход Master-маршрутизатора из группы)



### 5.4.6. Time

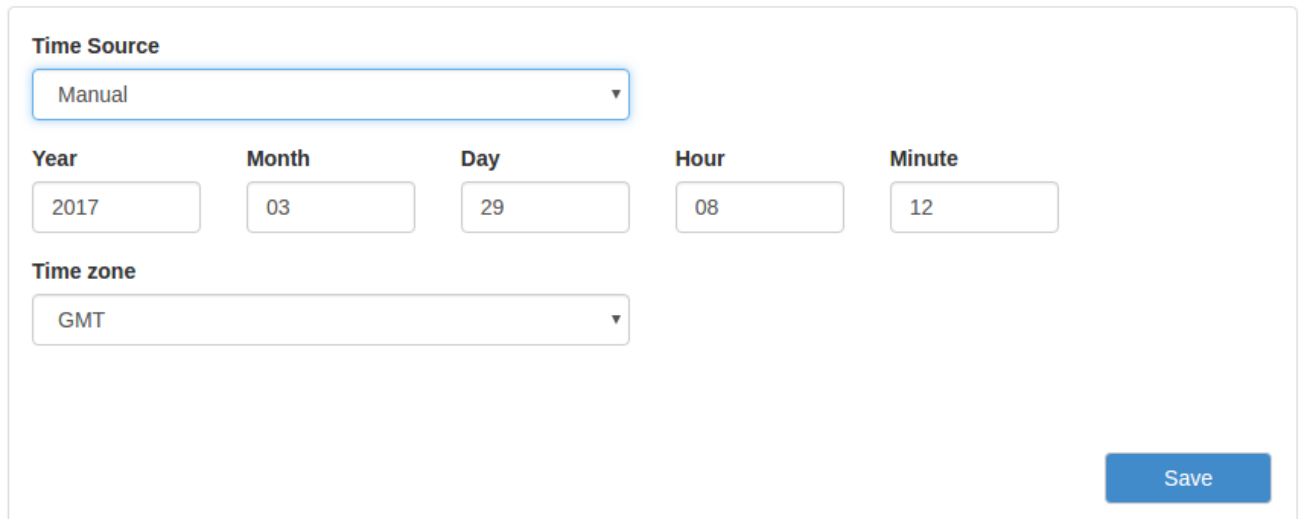
Раздел **Time** на вкладке **Services** предназначен для настройки текущего времени на устройстве. В поле **Time Source** (источник данных о времени) позволяет выбрать способ установки текущего времени:

- **NTP** – автоматический режим, в котором устройство будет получать данные о текущем времени от внешних серверов — NTP;
- **Manual** – установка времени в ручном режиме, на основе данных, внесенных пользователем.

Если в поле **Time Source** выбран режим **Manual**, то для настройки времени необходимо внести данные в соответствующие поля: год (поле **Year**), месяц (**Month**), день (**Day**), час (**Hour**), минута (**Minute**), часовой пояс (**Time Zone**).

На **Рис. 5.41** представлен пример настройки времени в ручном режиме.

Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!



The screenshot shows a configuration form for the 'Time Source' section. At the top, there is a dropdown menu labeled 'Time Source' with 'Manual' selected. Below this are five input fields: 'Year' (2017), 'Month' (03), 'Day' (29), 'Hour' (08), and 'Minute' (12). Underneath these fields is another dropdown menu labeled 'Time zone' with 'GMT' selected. A blue 'Save' button is located at the bottom right of the form.

**Рис. 5.41.** Настройка времени в ручном режиме

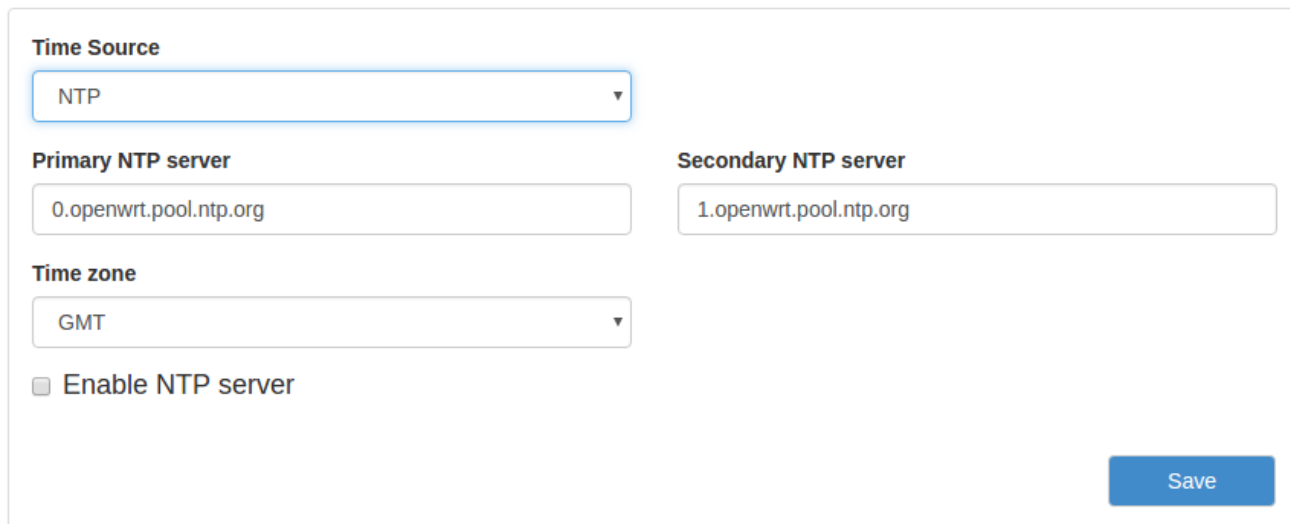
Если в поле **Time Source** выбран режим **NTP**, то для настройки времени необходимо указать IP-адреса или доменные имена для двух внешних NTP-серверов, с которых будут браться данные о текущем времени: основной сервер указывается **Primary NTP Server**, а второстепенный сервер – **Secondary NTP Server**. По умолчанию в этих полях уже указаны сервера времени, используемые в операционной системе OpenWRT по умолчанию. Дополнительно указывается часовая зона в поле **Time Zone**, если роутер находится в отличном часовом поясе от серверов.

Также на базе роутера можно создать собственный NTP-сервер. Для этого настройте параметры времени и поставьте галочку напротив **Enable NTP Server**. В этом случае клиенты локальной сети роутера, чтобы получать данные о текущем времени от этого сервера, должны указывать в настройках времени в поле с указанием сервера адреса этого роутера.

На **Рис. 5.42** представлен пример настройки времени в автоматическом режиме.



Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!



**Time Source**  
NTP

**Primary NTP server**  
0.openwrt.pool.ntp.org

**Secondary NTP server**  
1.openwrt.pool.ntp.org

**Time zone**  
GMT

Enable NTP server

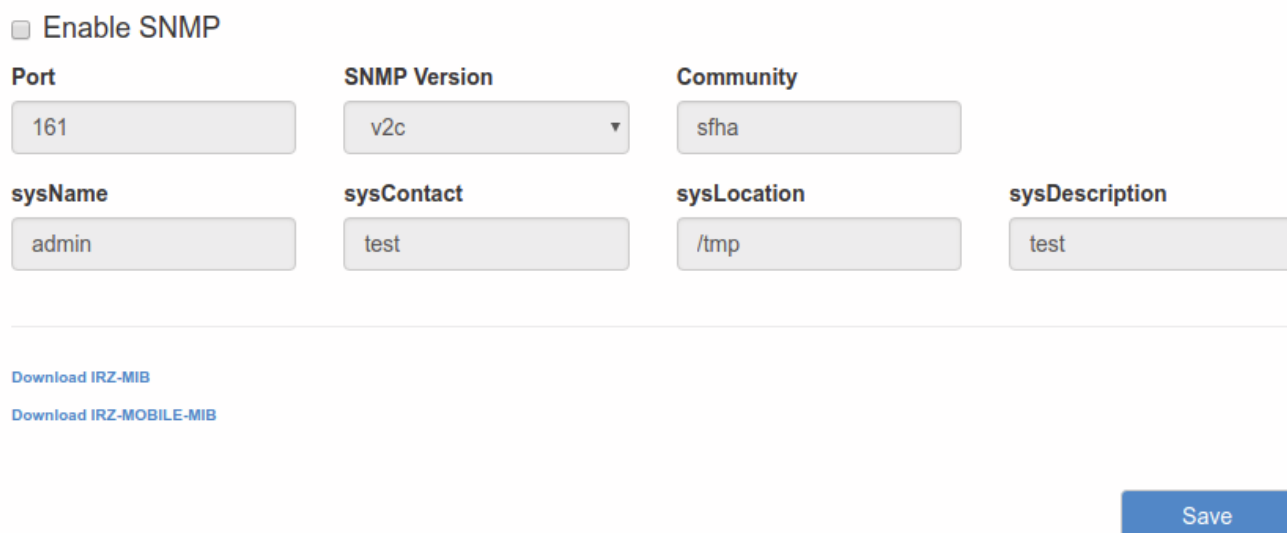
Save

Рис. 5.42. Настройка времени в автоматическом режиме

#### 5.4.7. SNMP

Раздел SNMP на вкладке Services предназначен для настройки системы мониторинга роутера по протоколу SNMP. С помощью SNMP можно контролировать (проводить мониторинг) подключенные к сети устройства. На Рис. 5.43 и Рис. 5.44 представлены примеры настройки SNMP для двух версий протокола – v2c и v3, соответственно.

Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!



Enable SNMP

**Port**  
161

**SNMP Version**  
v2c

**Community**  
sfha

**sysName**  
admin

**sysContact**  
test

**sysLocation**  
/tmp

**sysDescription**  
test

Download IRZ-MIB  
Download IRZ-MOBILE-MIB

Save

Рис. 5.43. Вкладка Services, раздел SNMP (v2c)



Чтобы включить SNMP, поставьте галочку напротив **Enable SNMP**, а затем введите соответствующие настройки (см. таблицу 5.20).

**Таблица 5.20.** Настройки SNMP

Поле	Версия	Описание
Port	v2c, v3	Порт, через который будет работать протокол SNMP. По умолчанию – «161»
SNMP Version	v2c, v3	Выбор версии протокола: <b>v2c, v3</b>
Community	v2c, v3	«Общая строка», по которой роутер предоставляет данные для системы мониторинга
sysName	v2c, v3	Имя устройства (на выбор пользователя), которое будет использоваться для идентификации данного устройства в системе мониторинга
sysContact	v2c, v3	Контактные данные (на выбор пользователя) в виде электронного адреса, телефона или другого вида
sysLocation	v2c, v3	Описание местоположения устройства (на выбор пользователя)
sysDescription	v2c, v3	Описание устройства (на выбор пользователя)
Username	v3	Имя пользователя для авторизации при контроле роутера по протоколу SNMP
Auth Passphrase (SHA)	v3	Фраза-пароль для шифрования авторизации при контроле роутера по протоколу SNMP, используется алгоритм хэширования SHA
Privacy Passphrase (AES)	v3	Фраза-пароль для шифрования передаваемого трафика от роутера к системе мониторинга, при контроле роутера по протоколу SNMP, используется алгоритм шифрования AES
Security Level	v3	Выбор уровня защиты при работу с устройством по протоколу SNMP: <ul style="list-style-type: none"><li>• Noauth – авторизация на устройстве не установлена;</li><li>• Auth – установлена авторизация;</li><li>• Priv – установлена авторизация и шифрование данных при передаче по протоколу.</li></ul>

Enable SNMP

Port

161

SNMP Version

v3

Community

public

sysName

iRZ Router

sysContact

admin@example.com

sysLocation

office

sysDescription

Username

Auth passphrase (SHA)

at least 8 characters

Privacy passphrase (AES)

at least 8 characters

Security level

noauth

[Download IRZ-MIB](#)

[Download IRZ-MOBILE-MIB](#)

Save

**Рис. 5.44.** Вкладка Services, раздел SNMP (v3)

Под настройками SNMP есть две ссылки для скачивания MIB файлов.





### 5.4.8. DynDNS

Раздел DynDNS на вкладке Services предназначен для настройки DynDNS, то есть метода автоматического обновления записей DNS-сервера. Данный метод применяется для автоматического определения IP-адреса роутера по его доменному имени, когда роутеру выделяется динамический IP-адрес. На **Рис. 5.45** представлен пример настройки DynDNS.

Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!

Enable DynDNS client

**Provider**  
custom

**Get Address From** web      **URL For Requests** http://checkip.dyndns.com/

**Username** asd      **Password** ...

**Update Interval (sec)** 300      **Hostname** example.domain.com

Force Update (use with caution)

**Remote URL**  
http://[USERNAME]:[PASSWORD]@provider.net/update\_uri?hostname=[DOMAIN]&myip=[IP]

Save

**Рис. 5.45.** Вкладка Services, раздел DynDNS

Чтобы включить DynDNS, поставьте галочку напротив **Enable DynDNS client** и настройте соответствующие параметры (см. таблицу 5.21).

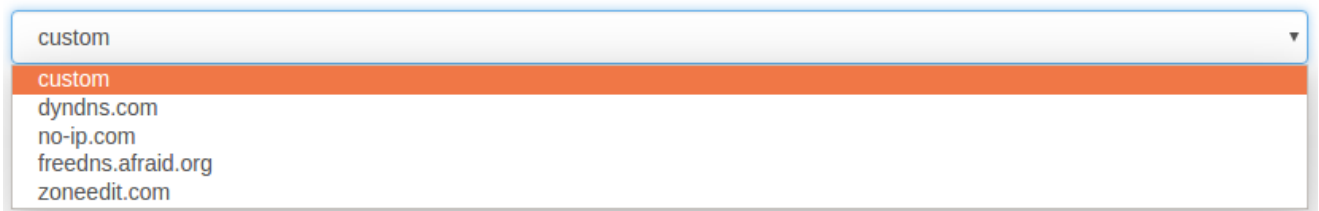


Таблица 5.21. Настройки DynDNS

Поле	Описание
Provider	Выбор провайдера услуги динамического DNS (см. <b>Рис. 5.46</b> ). В роутерах iRZ предустановлены основные настройки для нескольких распространенных провайдеров. Для настройки собственного сервера, выберите <b>Custom</b> и пропишите необходимые настройки
Get Address From	Данная настройка отвечает за определение вашего динамического IP адреса. При выборе <b>WEB</b> роутер будет получать эти данные через URL, указанные в поле URL For Requests. При выборе Network — в поле Network Interface необходимо будет указать интерфейс роутера, адрес которого будет передаваться сервису DynDNS
URL For Requests	Указывается URL сервиса определения IP адреса
Username	Имя пользователя для авторизации на сервере DynDNS
Password	Пароль для авторизации на сервере DynDNS
Hostname	Имя хоста, присвоенный вашей учетной записи в сервисе dyndns
Update Interval (sec)	Интервал в секундах, через который будет обновляться информация на сервера
Force Update	Включает или отключает обновление данных на сервисе в случае если IP адрес роутера не меняется
Remote URL	Строка URL-адреса с параметрами подключения к серверу DynDNS

В поле **Provider** указывается провайдер услуги динамического DNS. В роутерах iRZ есть возможность использовать свой собственный сервис динамического DNS или несколько предустановленных распространенных сервиса, см. **Рис. 5.46**

#### Provider



custom  
custom  
dyndns.com  
no-ip.com  
freedns.afraid.org  
zoneedit.com

Рис. 5.46. Сервера DNS



### 5.4.9. Crontabs

Раздел Crontabs на вкладке Services предназначен для настройки выполнения команд по расписанию. Для этого достаточно добавить инструкцию, указать время и саму команду.

Добавление инструкции осуществляется посредством кнопки  («плюс»), а удаление — кнопкой  («минус»). Отметка в столбце **Enable** позволяет включать, или отключать выполнение инструкции без ее удаления. Время указывается в полях: **Minute** (минута, от «0» до «59»), **Hour** (час, от «0» до «23»), **Day** (день, от «1» до «31»), **Month** (месяц, от «1» до «12»), **Weekday** (день недели, от «0» до «7», где воскресенье — это либо «0», либо «7»), а сама команда указывается в поле **Command**. На **Рис. 5.47** представлен пример поля для заполнения. В полях времени можно указать знак «\*», который означает весь диапазон значений данного поля.

Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!

<input type="button" value="+"/>	Enable	Minute	Hour	Day	Month	Weekday	Command
<input type="button" value="-"/>	<input checked="" type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="*"/>	<input type="text" value="*"/>	<input type="text" value="*"/>	<input type="text" value="*"/>	<input type="text" value="reboot"/>

**Рис. 5.47.** Вкладка Services, раздел Crontabs

### 5.4.10. Command over SMS

Раздел Command over SMS на вкладке Services предназначен для настройки выполнения команд управления роутером через SMS-сообщения. Для этого достаточно добавить инструкцию, указать команду, придумать и указать для команды ключевое слово, и, при желании ограничить доступ к управлению роутером, номер (или номера) мобильного телефона, с которого она может быть отправлена.

Добавление инструкции осуществляется посредством кнопки  («плюс»), а удаление — кнопкой  («минус»). Отметка в столбце **Enable** позволяет включать, или отключать выполнение инструкции без ее удаления. Команда, которая будет выполняться указывается в поле **Command**. В качестве команды можно использовать самописный скрипт, расположенный в энергонезависимой памяти роутера. Для таких скриптов отведен отдельный раздел в файловой системе роутера – **/opt**. Скрипт можно поместить в раздел через консоль роутера или по протоколу SCP. Скрипты могут быть написаны на языке Python версии 2.7 или на языке командного интерпретатора (shell). Для скриптов и команд необходимо указывать их полный путь, как это сделано на **Рис. 5.48**

В поле **Message** указывается ключевая фраза, которая будет содержаться в SMS-сообщении для выполнения команды из поля **Command**. Это сделано для удобства, чтобы не набирать на телефоне



настоящую длинную команду, вместо этого можно отправлять короткие ключевые фразы. Соответственно, ключевые фразы придумывает пользователь на собственное усмотрение.

В поле в столбце **From** указывается телефонный номер (если номеров несколько, они разделяются пробелами) в международном формате (например, для России это «+7[код оператора][номер]»), с которого можно выполнять команду из поля **Command**. Если данное поле оставить пустым, то команда при правильном ключевом слове будет выполняться по SMS, пришедшей с любого номера. На **Рис. 5.48** представлен пример полей для заполнения.

Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!

Если кратко описать приведенные выше шаги, то для выполнения команды, полученной по SMS необходимо:

1. Зайдите в раздел **Services** → **Command over SMS** на роутере, где должна выполняться команда;
2. Создайте инструкцию (поле должно быть активно), в которой в поле **Command** укажите команду, в поле **Message** укажите придуманную ключевую фразу (при желании ограничить доступ к управлению роутером, укажите номер мобильного телефона в поле **From**, с которого может быть отправлена команда);
3. Сохраните настройки, нажав на кнопку **Save**, внизу страницы;
4. Отправьте на телефонный номер SIM-карты роутера SMS-сообщение, содержащее ключевую фразу из поля **Message** (если поле **From** заполнено, то сообщение необходимо отправлять от номера, который там указан);
5. Если все шаги выполнены верно, на роутере выполнится команда из поля **Command**, той строки, в которой ключевые фразы из поля **Message** и SMS-сообщения совпадают.

	Enable	Message	Command	From
<input type="checkbox"/>	<input type="checkbox"/>	reboot	/sbin/reboot	
<input type="checkbox"/>	<input type="checkbox"/>	^[0-9]\ hello	/bin/false	+79211002234 +79211002233

Save

**Рис. 5.48.** Вкладка Services, раздел Commands over SMS



### 5.4.11. RS232/RS485 over TCP

Разделы RS232 over TCP и RS485 over TCP на вкладке Services предназначены для настройки работы роутера с портами RS232, и RS485, соответственно.

В роутерах iRZ работа по стандарту RS232/RS485 ограничивается приемом данных по линии Rx и передачей данных по линии Tx. Приняв данные по линии Rx роутер инкапсулирует полученные данные в IP-пакет, и в соответствии с настройками отправляет их на удаленный хост. И наоборот, получив IP-пакет, на указанный в настройках порт, роутер распаковывает IP-пакет и передает его по линии Tx на подключенное устройство.

Роутер можно настроить на два режима работы:

- **Server** — роутер ждет входящего подключения на указанный порт, устанавливается соединения и начинается передача данных;
- **Client** — роутер устанавливает соединение по указанному IP-адресу и порту, и начинает передачу данных.

Если выбран режим работы **Disabled**, то функции работы с портами RS232/485 отключены.

На **Рис. 5.49** представлен пример настройки роутера с портами RS232 в режиме Client.

The screenshot shows the 'Services' tab in the router's configuration interface. The 'RS232 over TCP' option is selected in the left sidebar. The main configuration area is titled 'Enable RS232 over TCP' and is checked. The 'Mode' is set to 'Client'. The 'Port' is 10000, 'Data Bits' is 8, 'Baudrate' is 9600, and 'Banner' is empty. The 'Remote Host' is localhost, 'Stop Bits' is 1, and 'Parity' is none. The 'Accumulation Attempts' is 3, 'Accumulation Interval (ms)' is 100, 'Peer Timeout (sec)' is 60, and 'Reconnect Delay (sec)' is 60. A 'Save' button is at the bottom right.

**Рис. 5.49.** Вкладка Services, раздел RS232 over TCP



**Таблица 5.22.** Настройки RS232 over TCP (C – клиент, S – сервер, M — server Modbus TCP to RTU)

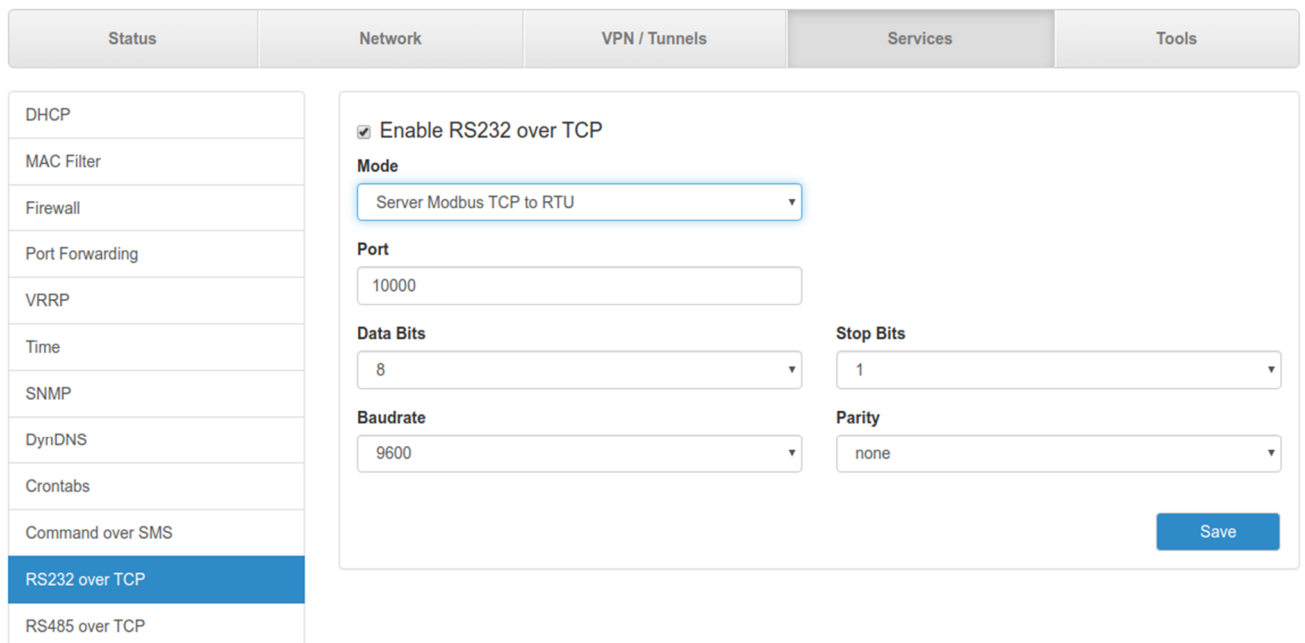
Поле	Режим	Описание
Port	C, S, M	Порт, через который будет осуществляться передача данных
Remote Host	C	IP-адрес сервера, к которому будет подключаться устройство для передачи данных
Data Bits	C, S, M	Количество бит блока, используемых при передаче данных: <b>7, 8</b>
Stop Bits	C, S, M	Количество стоп-бит блока, используемые для определения конца блока: <b>1, 2</b>
Baudrate	C, S, M	Скорость передачи данных через порт, в бод
Parity	C, S, M	Режим контроля четности бит в передаваемых блоках: <b>None</b> – без проверки, <b>Odd</b> – проверка на нечетность, <b>Even</b> – проверка на четность
Banner	C, S	Сообщение (на выбор пользователя), которое будет отображаться при работе с портом
Accumulation Attempts	C, S	Количество интервалов ожидания, после которых накопленные данные будут отправлены
Accumulation Interval (ms)	C, S	Время интервала ожидания, в мс, при получении данных
Peer Timeout (sec)	C, S	Время ожидания ответа от удаленного узла, в секундах, при установке соединения или перед отправкой данных
Reconnect Delay (sec)	C	Время задержки после неудачной попытки подключения к серверу, в секундах, после которого будет совершена еще одна попытка подключения к серверу



### 5.4.12. RS232/RS485 Server Modbus TCP to RTU

Роутеры iRZ серий R2 и R4 поддерживают функцию преобразования промышленных протоколов Modbus RTU в протокол Modbus TCP и обратно, то есть выступают в роли шлюза, обеспечивая прозрачный канал передачи данных между устройствами.

Данная функция успешно объединяет в сеть оборудование с различными протоколами и интерфейсами.



The screenshot shows the configuration page for 'RS232 over TCP' in the 'Services' tab. The interface includes a sidebar menu with options like DHCP, MAC Filter, Firewall, Port Forwarding, VRRP, Time, SNMP, DynDNS, Crontabs, Command over SMS, RS232 over TCP (selected), and RS485 over TCP. The main configuration area has the following settings:

- Enable RS232 over TCP
- Mode: Server Modbus TCP to RTU (dropdown menu)
- Port: 10000 (text input)
- Data Bits: 8 (dropdown menu)
- Stop Bits: 1 (dropdown menu)
- Baudrate: 9600 (dropdown menu)
- Parity: none (dropdown menu)
- Save button

**Рис. 5.50 Вкладка Services, раздел RS232 over TCP, режим Server Modbus TCP to RTU**

Протокол Modbus TCP предназначен для работы в сети Ethernet. Протокол Modbus RTU использует последовательные интерфейсы (RS-232, RS-485) и имеет режим передачи: RTU.

Когда роутер получает запрос Modbus TCP, он преобразует пакет в Modbus RTU и посылает его по последовательному интерфейсу. Когда роутер получает ответ от устройства Modbus RTU, он преобразует его в пакет Modbus TCP и отправляет пакет по Ethernet. При взаимодействии одно устройство Modbus всегда является ведущим (Master), а второе — ведомым (Slave). Modbus Master всегда отправляет запрос, инициируя обмен данными, а устройство Modbus Slave отправляет ответ.

Роутеры могут работать только режиме Сервера, то есть слушать входящие TCP подключения для преобразования из TCP в RTU и наоборот.



## 5.5. Раздел «Tools»

### 5.5.1. Access

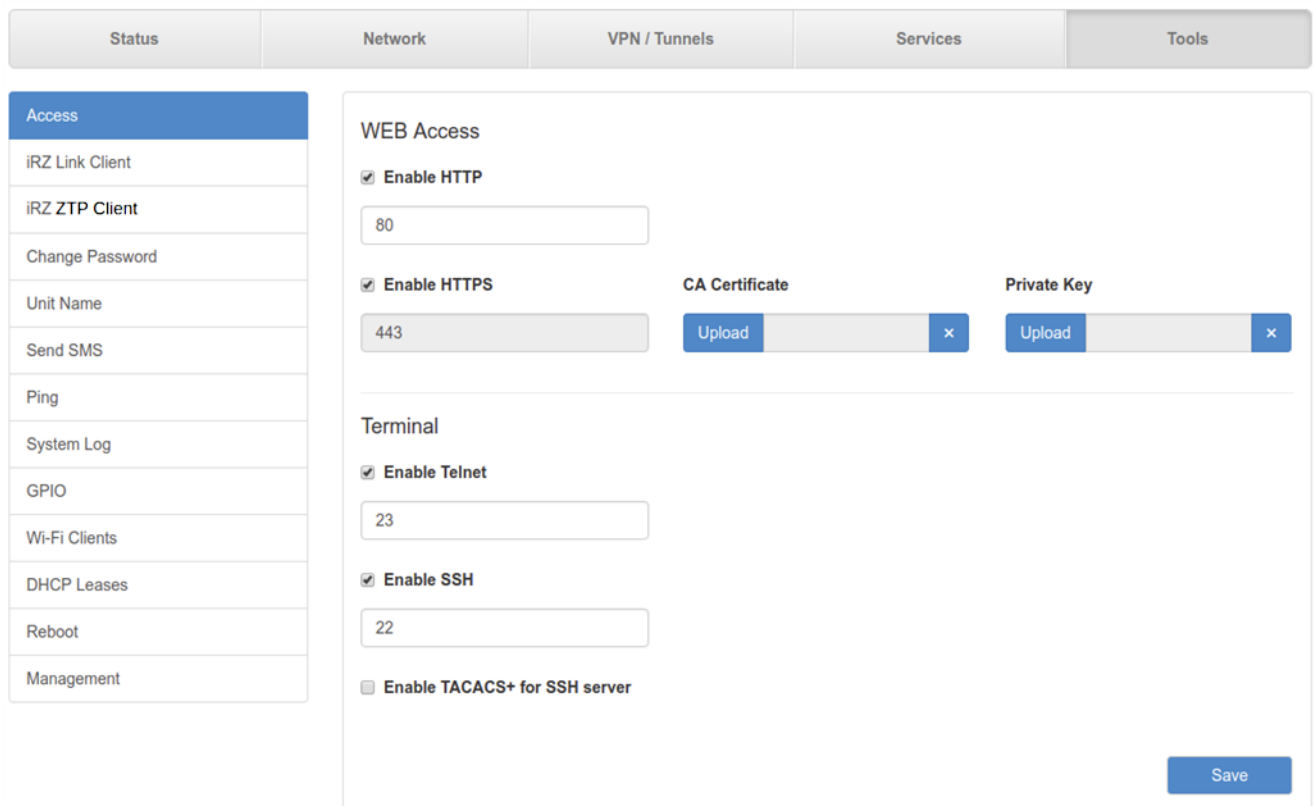
Раздел Access на вкладке Tools предназначен для настройки доступа управления роутером. Всего доступны три варианта получить доступ к роутеру. Для этого нужно поставить галочку напротив соответствующего пункта и в нижнем поле ввести порт (изначально указаны значения по умолчанию):

- **Enable HTTP server** — доступ к роутеру через веб-интерфейс;
- **Enable HTTPS server** — доступ к роутеру через веб-интерфейс с защитой через сертификат;
- **Enable Telnet server** — доступ к роутеру по протоколу telnet;
- **Enable SSH server** — доступ к роутеру по протоколу SSH.

Чтобы включить авторизацию на устройстве через сервер авторизации TACACS+ (справедливо только для роутеров серии R4), поставьте галочку напротив **Enable TACACS+ for SSH**. На **Рис. 5.51** представлен пример настройки доступа к устройству.

Чтобы подключаться к web интерфейсу роутера через защищённый протокол **HTTPS**, необходимо свои сертификаты и частный ключ загрузить на роутер в полях **CA Certificate** и **Private Key** соответственно.

Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!



Status	Network	VPN / Tunnels	Services	Tools
<b>Access</b>				
iRZ Link Client				
iRZ ZTP Client				
Change Password				
Unit Name				
Send SMS				
Ping				
System Log				
GPIO				
Wi-Fi Clients				
DHCP Leases				
Reboot				
Management				

#### WEB Access

**Enable HTTP**  
80

**Enable HTTPS**      CA Certificate      Private Key  
443      Upload      Upload

#### Terminal

**Enable Telnet**  
23

**Enable SSH**  
22

**Enable TACACS+ for SSH server**

**Save**

**Рис. 5.51.** Вкладка Tools, раздел Access





### 5.5.2. iRZ Link Client

Раздел iRZ Link Client на вкладке Tools предназначен для настройки подключения роутера к системе управления Link.

Enable Zelda (iRZ Link client)

<b>Server</b>	<b>Port</b>
<input type="text" value="link.irz.net"/>	<input type="text" value="11000"/>
<b>Force Update Information (sec.)</b>	<b>Keepalive Interval (sec.)</b>
<input type="text" value="60"/>	<input type="text" value="30"/>

Use Encryption

**Cipher Key (AES256)**

Рис. 5.52 Вкладка Tools, раздел iRZ Link Client

Отметка в строке **Enable** позволяет включать, или отключать данную оснастку. Поле **Server** необходимо для указания адреса или доменного имени сервера Link. В поле **Port** указывается порт через который работает сервер данного сервиса. В поле **Force Update Information (sec.)** указывается время через которое будет обновлена информация о роутере на сервере, а в поле **Keepalive Interval (sec.)** - время через которое роутер будет отправлять информацию на сервер что он на связи.

Поставив галочку в поле **Use Encryption** можно зашифровать данные передаваемые между роутером и сервером. Для этого необходимо будет в поле Cipher Key (AES256) указать ключ шифрования, сгенерированный по алгоритму AES 256.

Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!

Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!



### 5.5.3. iRZ ZTP Client

Данный раздел предназначен для настройки работы роутера с iRZ SD-WAN. Более подробную информацию можно прочитать в документе «**РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ iRZ SD-WAN**» на сайте [www.radiofid.ru](http://www.radiofid.ru).

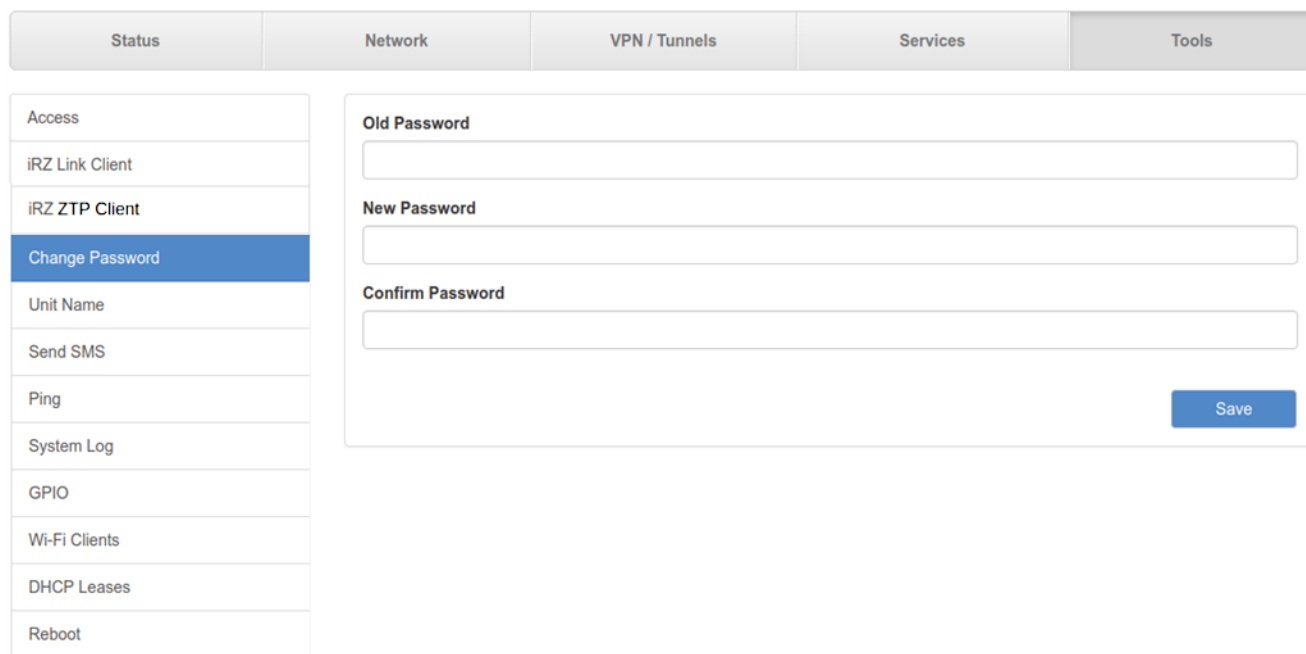
### 5.5.4. Change Password

Раздел Change Password на вкладке Tools предназначен для изменения пароля для доступа к устройству. Пароль меняется как для доступа по веб-интерфейсу, так и по Telnet и SSH.

Для изменения пароля:

1. Введите старый пароль доступа к устройству в поле **Old Password**;
2. Введите новый пароль в поле **New Password**;
3. Введите новый пароль еще раз в поле **Confirm Password**;
4. Нажмите кнопку **Save**, внизу страницы.

На **Рис. 5.53**. Вкладка Tools, раздел Change Password представлен пример полей для заполнения.



The screenshot shows the 'Tools' tab selected in the top navigation bar. On the left, a sidebar menu lists various tools, with 'Change Password' highlighted in blue. The main content area contains three input fields labeled 'Old Password', 'New Password', and 'Confirm Password'. A blue 'Save' button is located at the bottom right of the form.

**Рис. 5.53.** Вкладка Tools, раздел Change Password



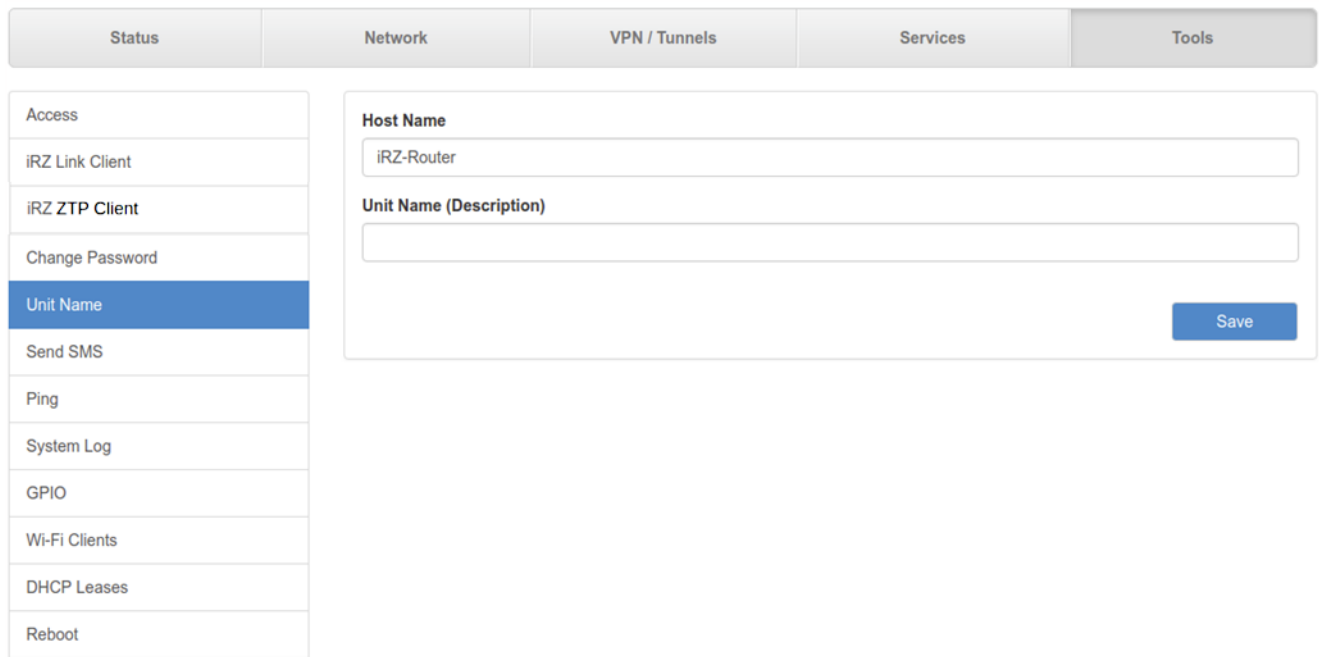
### 5.5.5. Unit Name

Раздел Unit Name на вкладке Tools предназначен для изменения названия устройства, которое отображается в веб-интерфейсе.

Для установки или изменения названия:

1. Введите новое название в поле **Unit Name**;
2. Нажмите кнопку **Save**, внизу страницы.

На **Рис. 5.54** представлен пример полей для заполнения.



Status	Network	VPN / Tunnels	Services	Tools
Access				
iRZ Link Client				
iRZ ZTP Client				
Change Password				
<b>Unit Name</b>				
Send SMS				
Ping				
System Log				
GPIO				
Wi-Fi Clients				
DHCP Leases				
Reboot				

**Host Name**

**Unit Name (Description)**

**Save**

**Рис. 5.54.** Вкладка Tools, раздел Unit Name



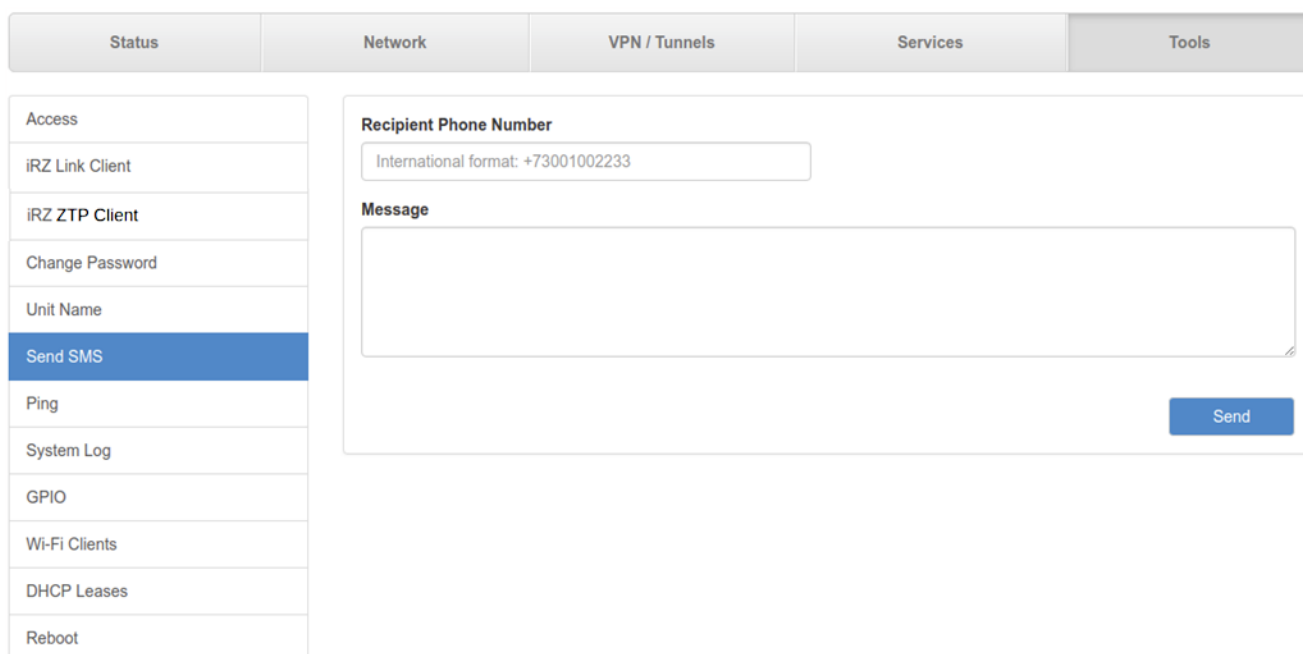
### 5.5.6. Send SMS

Раздел Send SMS на вкладке Tools предназначен для отправки SMS-сообщения на указанный номер. SMS-сообщение отправляется через активную SIM-карту, которая используется в роутере.

Для отправки сообщения (в роутере должна быть установлена SIM-карта с активной услугой, и необходимым балансом средств, а само устройство должно находиться в зоне покрытия оператора, предоставившего SIM-карту):

1. Введите номер мобильного телефона в международном формате (для России это «+7[код оператора][номер]») в поле **Recipient Phone Number**;
2. Введите сообщение в поле **Message**;
3. Нажмите кнопку **Send**, внизу страницы.

На **Рис. 5.55** представлен пример полей для заполнения.



The screenshot shows a web interface with a top navigation bar containing tabs: Status, Network, VPN / Tunnels, Services, and Tools. The 'Tools' tab is active. On the left, a sidebar menu lists various tools, with 'Send SMS' highlighted in blue. The main content area is titled 'Send SMS' and contains two input fields: 'Recipient Phone Number' with a placeholder 'International format: +73001002233' and a 'Message' text area. A blue 'Send' button is located at the bottom right of the form.

**Рис. 5.55.** Вкладка Tools, раздел Send SMS



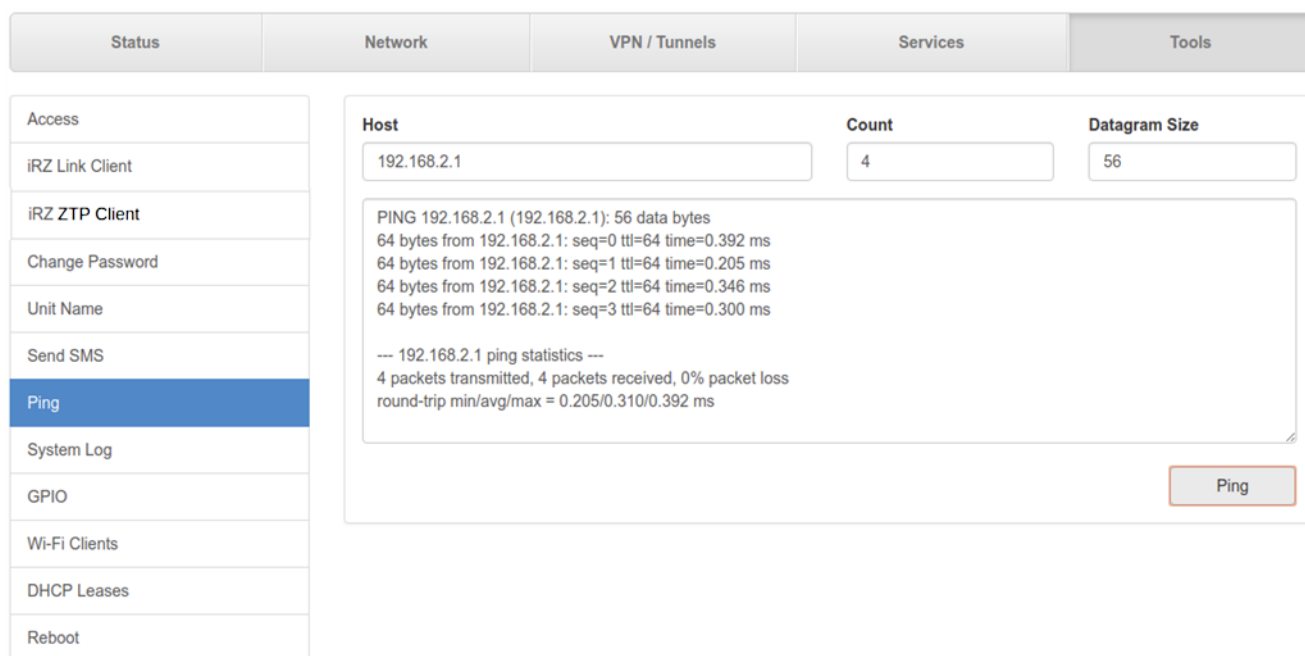
### 5.5.7. Ping

Раздел Ping на вкладке Tools предназначен для проверки соединения с удаленным узлом с помощью утилиты ping.

Чтобы проверить соединение:

1. Введите IP-адрес удаленного узла в поле **Host**;
2. Введите количество ICMP-пакетов, которые нужно отправить при проверке в поле **Count**;
3. Укажите размер ICMP-пакета в поле **Datagram Size**;
4. Нажмите кнопку **Ping**, внизу страницы, и в главном окне посередине экрана появится результат проверки.

На **Рис. 5.56** представлен пример полей для заполнения.



The screenshot shows the 'Tools' tab in the iRZ interface. On the left is a sidebar menu with items: Access, iRZ Link Client, iRZ ZTP Client, Change Password, Unit Name, Send SMS, Ping (highlighted), System Log, GPIO, Wi-Fi Clients, DHCP Leases, and Reboot. The main area is titled 'Tools' and contains the 'Ping' tool configuration. It has three input fields: 'Host' with '192.168.2.1', 'Count' with '4', and 'Datagram Size' with '56'. Below these fields is a text area showing the results of a ping command: 'PING 192.168.2.1 (192.168.2.1): 56 data bytes', followed by four lines of response data showing 64 bytes from the host with various sequence numbers and times. Below the response is a summary: '--- 192.168.2.1 ping statistics ---', '4 packets transmitted, 4 packets received, 0% packet loss', and 'round-trip min/avg/max = 0.205/0.310/0.392 ms'. At the bottom right of the main area is a 'Ping' button.

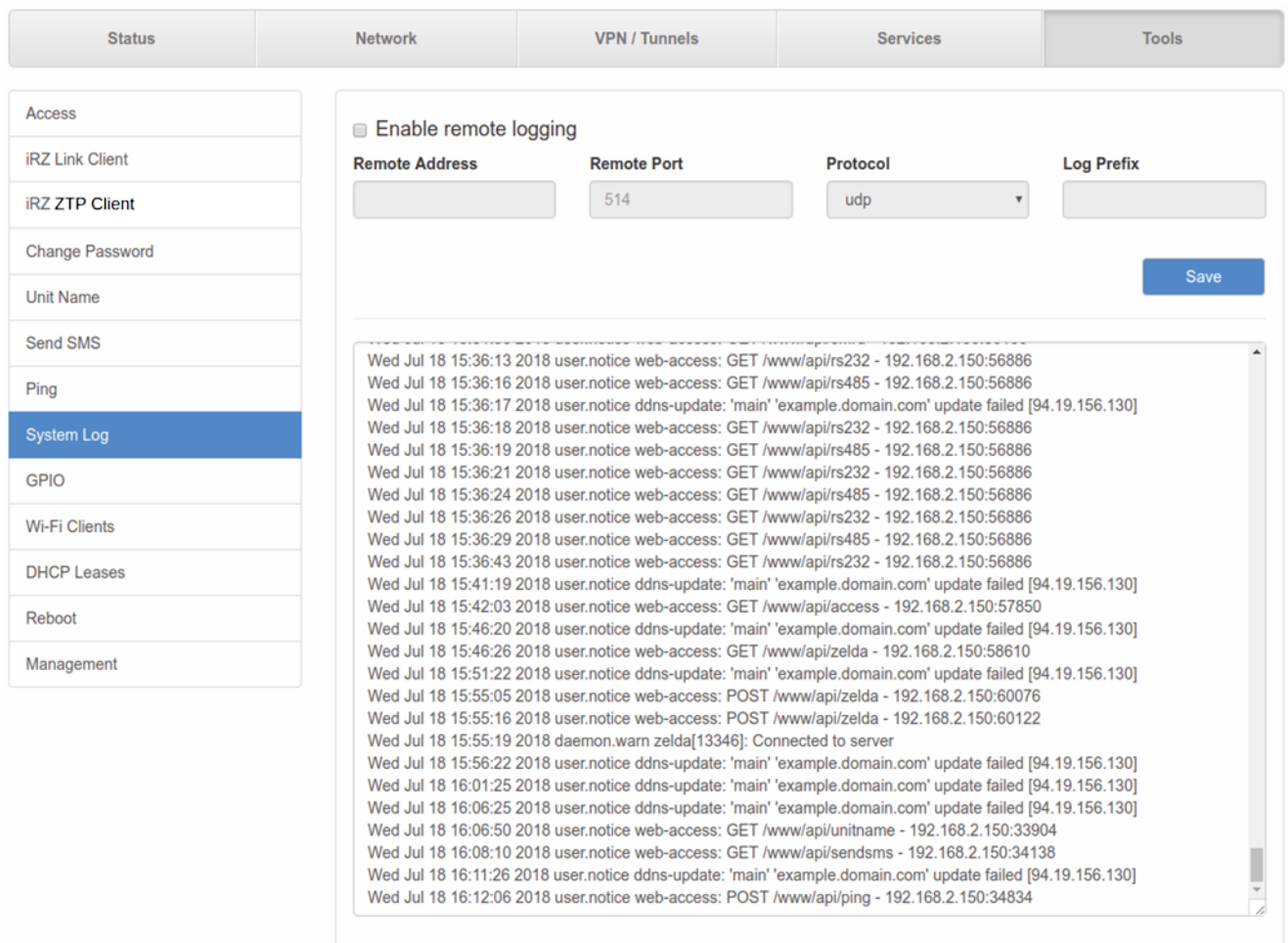
**Рис. 5.56.** Вкладка Tools, раздел Ping



### 5.5.8. System Log

Раздел System Log на вкладке Tools предназначен для работы с системным журналом устройства. Данные из системного журнала устройства можно пересылать по протоколу Syslog на удаленный адрес, для этого:

1. Поставьте галочку напротив **Enable Remote Logging**;
2. Укажите удаленный IP-адрес в поле **Remote Address**, а порт в поле **Remote Port**;
3. Выберите в поле **Protocol** протокол, по которому будут пересылаться данные;
4. В поле **Log Prefix** можно указать префикс, который будет добавляться к записям;
5. Нажмите кнопку **Save**, внизу блока.



The screenshot shows the 'Tools' tab in the iRZ interface. On the left is a sidebar menu with 'System Log' selected. The main area contains the 'Enable remote logging' configuration section. It includes a checkbox for 'Enable remote logging', which is checked. Below it are four input fields: 'Remote Address' (empty), 'Remote Port' (514), 'Protocol' (dropdown menu showing 'udp'), and 'Log Prefix' (empty). A blue 'Save' button is located at the bottom right of this section. Below the configuration fields is a scrollable log window displaying a list of system events, including web-access requests and ddns-update failures.

Status	Network	VPN / Tunnels	Services	Tools
--------	---------	---------------	----------	-------

Enable remote logging

Remote Address:  Remote Port:  Protocol:  Log Prefix:

```
Wed Jul 18 15:36:13 2018 user.notice web-access: GET /www/api/rs232 - 192.168.2.150:56886
Wed Jul 18 15:36:16 2018 user.notice web-access: GET /www/api/rs485 - 192.168.2.150:56886
Wed Jul 18 15:36:17 2018 user.notice ddns-update: 'main' 'example.domain.com' update failed [94.19.156.130]
Wed Jul 18 15:36:18 2018 user.notice web-access: GET /www/api/rs232 - 192.168.2.150:56886
Wed Jul 18 15:36:19 2018 user.notice web-access: GET /www/api/rs485 - 192.168.2.150:56886
Wed Jul 18 15:36:21 2018 user.notice web-access: GET /www/api/rs232 - 192.168.2.150:56886
Wed Jul 18 15:36:24 2018 user.notice web-access: GET /www/api/rs485 - 192.168.2.150:56886
Wed Jul 18 15:36:26 2018 user.notice web-access: GET /www/api/rs232 - 192.168.2.150:56886
Wed Jul 18 15:36:29 2018 user.notice web-access: GET /www/api/rs485 - 192.168.2.150:56886
Wed Jul 18 15:36:43 2018 user.notice web-access: GET /www/api/rs232 - 192.168.2.150:56886
Wed Jul 18 15:41:19 2018 user.notice ddns-update: 'main' 'example.domain.com' update failed [94.19.156.130]
Wed Jul 18 15:42:03 2018 user.notice web-access: GET /www/api/access - 192.168.2.150:57850
Wed Jul 18 15:46:20 2018 user.notice ddns-update: 'main' 'example.domain.com' update failed [94.19.156.130]
Wed Jul 18 15:46:26 2018 user.notice web-access: GET /www/api/zelda - 192.168.2.150:58610
Wed Jul 18 15:51:22 2018 user.notice ddns-update: 'main' 'example.domain.com' update failed [94.19.156.130]
Wed Jul 18 15:55:05 2018 user.notice web-access: POST /www/api/zelda - 192.168.2.150:60076
Wed Jul 18 15:55:16 2018 user.notice web-access: POST /www/api/zelda - 192.168.2.150:60122
Wed Jul 18 15:55:19 2018 daemon.warn zelda[13346]: Connected to server
Wed Jul 18 15:56:22 2018 user.notice ddns-update: 'main' 'example.domain.com' update failed [94.19.156.130]
Wed Jul 18 16:01:25 2018 user.notice ddns-update: 'main' 'example.domain.com' update failed [94.19.156.130]
Wed Jul 18 16:06:25 2018 user.notice ddns-update: 'main' 'example.domain.com' update failed [94.19.156.130]
Wed Jul 18 16:06:50 2018 user.notice web-access: GET /www/api/unitname - 192.168.2.150:33904
Wed Jul 18 16:08:10 2018 user.notice web-access: GET /www/api/sendsms - 192.168.2.150:34138
Wed Jul 18 16:11:26 2018 user.notice ddns-update: 'main' 'example.domain.com' update failed [94.19.156.130]
Wed Jul 18 16:12:06 2018 user.notice web-access: POST /www/api/ping - 192.168.2.150:34834
```

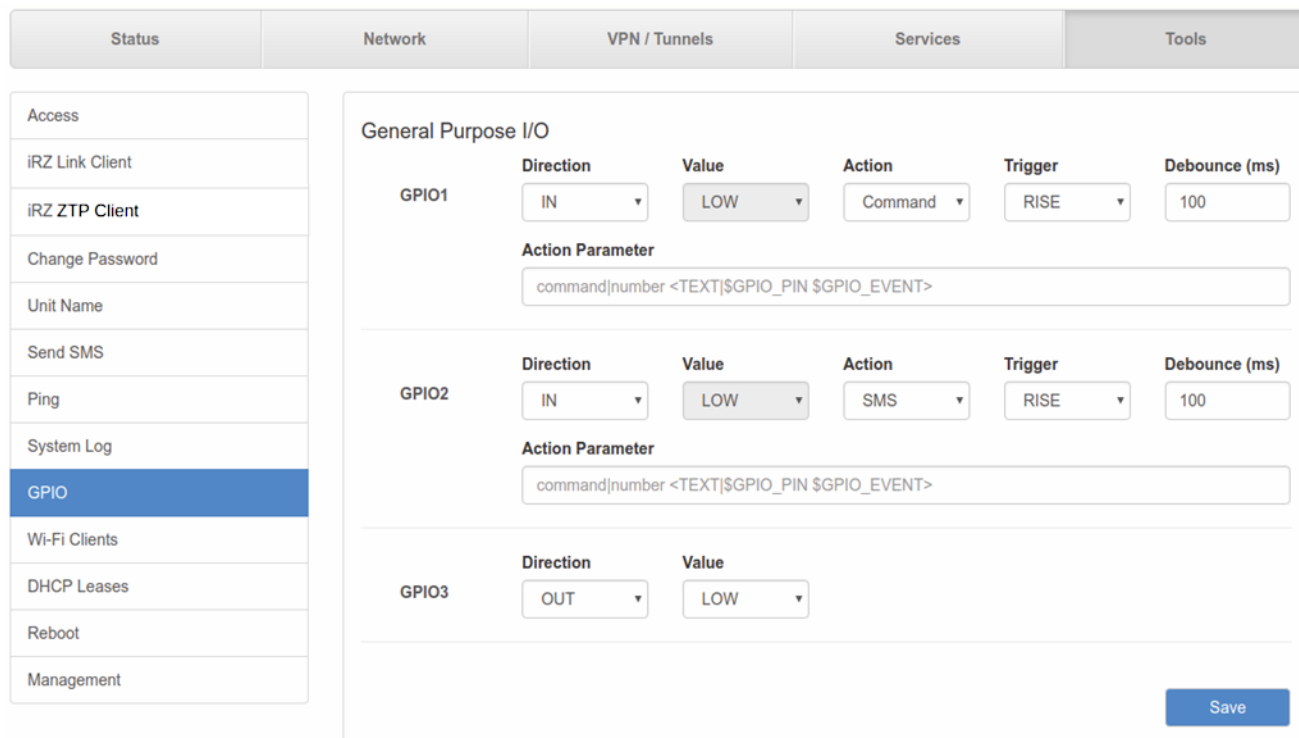
Рис. 5.57. Вкладка Tools, раздел System Log



### 5.5.9. GPIO

Раздел GPIO на вкладке Tools предназначен для настройки входов/выходов общего назначения (GPIO) роутера, если они у него есть. Количество доступных для настройки GPIO зависит от возможностей устройства. На **Рис. 5.58** представлен пример настройки GPIO для серии роутеров R4.

Для сохранения выполненных настроек используйте кнопку **Save**. При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!



**Рис. 5.58.** Вкладка Tools, раздел GPIO

У роутеров серии R4 имеется всего три GPIO-порта. Данные порты могут работать как на вход, так и на выход. Физические характеристики портов можно узнать либо в руководстве пользователя, либо на сайте производителя. Например, физические характеристики для роутеров R4:

**Таблица 5.23** Физические характеристики для роутеров R4

При режиме на вход	
Напряжение низкого уровня:	0 – 1,5 В
Напряжение высокого уровня:	3,5 – 5 В
При режиме на выход	
Напряжение:	5 В
Ток:	± 25 мА



Таблица 5.24. Настройки портов GPIO

Поле	Описание
GPIO1, GPIO2, GPIO3 ...	Имена входов/выходов
Direction	Выбор направления работы: <b>IN</b> – работает, как вход, <b>OUT</b> – выход
Value	Уровень выходного сигнала (только для выходов): <b>HIGH</b> – высокое напряжение, <b>LOW</b> – низкое
Action	Действие по триггеру (только для входов): None — ничего не делать, Command — выполнить команду по срабатыванию триггера, SMS — отправить смс на указанный номер по срабатыванию триггера
Trigger	Событие происходящее на порту: RISE – появление напряжения на порту, FALL — пропажа напряжения на порту, BOTH — оба события
Debounce (ms)	Нивелирует ложные срабатывания из-за электромагнитных наводок, измеряется в миллисекундах
Action Parameter	Поле для указания команды или номера телефона с текстом смс

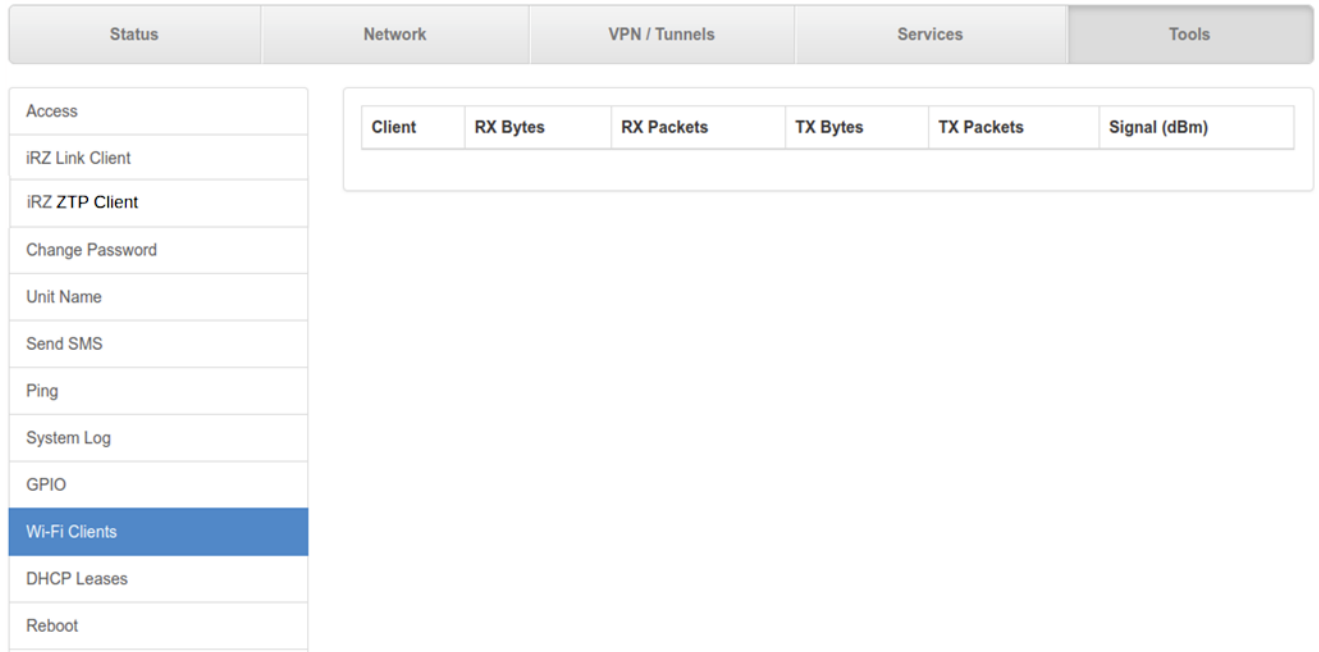
**Внимание!** Одновременная подача напряжения питания на вход роутера и на GPIO порты ЗАПРЕЩЕНА. Несоблюдение данной рекомендации ведет к выходу роутера из строя и лишает Вас права на дальнейшее гарантийное обслуживание устройства.





### 5.5.10. Wi-Fi Clients

Раздел Wi-Fi Clients на вкладке Tools предназначен для представления информации о подключенных Wi-Fi-клиентах, если устройство поддерживает работу с Wi-Fi. На **Рис. 5.59** представлен пример страницы.



**Рис. 5.59.** Вкладка Tools, раздел Wi-Fi Clients (роутер с Wi-Fi-модулем)

**Таблица 5.25.** Информация о Wi-Fi-клиентах

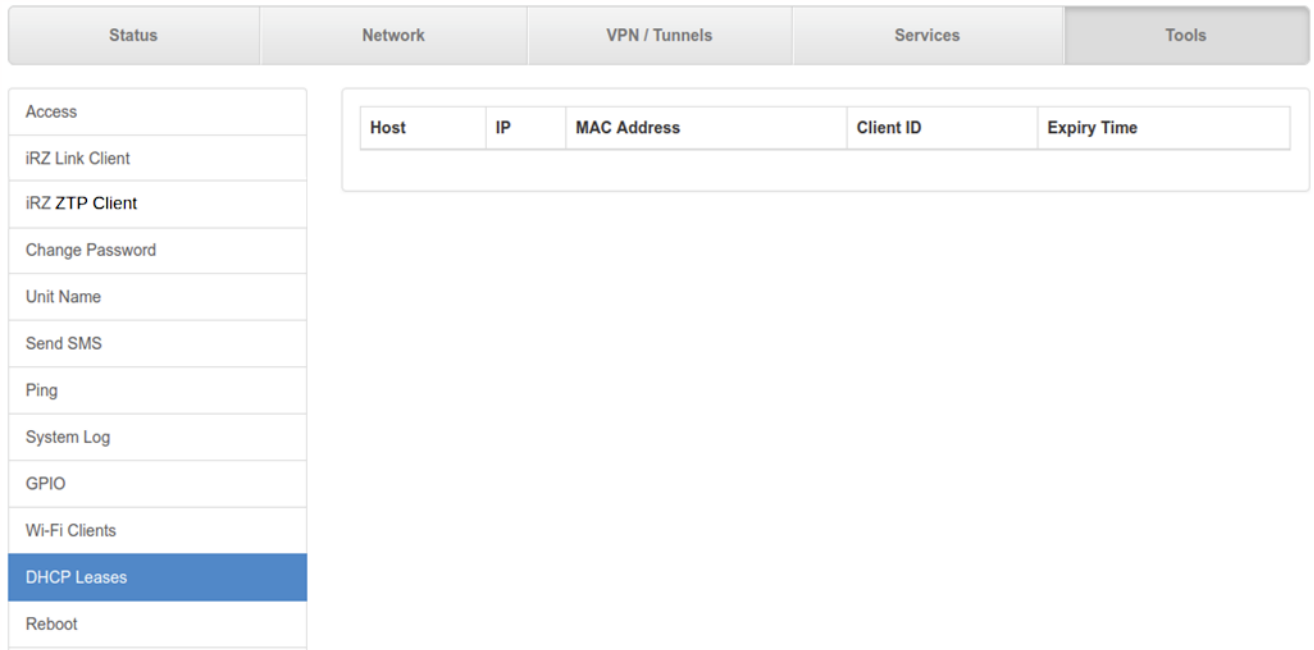
Поле	Описание
Client	MAC-адрес подключенного клиента
RX bytes	Количество принятых клиентом байт
RX packets	Количество принятых клиентом пакетов
TX bytes	Количество отправленных клиентом байт
TX packets	Количество отправленных клиентом пакетов
Signal (dBm)	Уровень сигнала для подключенного клиента в децибелах

Если роутер не поддерживает работу с Wi-Fi, то в окне будет выводиться сообщение: This router does not support this function.



### 5.5.11. DHCP Leases

Раздел DHCP Leases на вкладке Tools предназначен для представления информации о выданных IP-адресах клиентам от встроенного DHCP-сервера роутера, если он включен. На **Рис. 5.60** представлен пример страницы.



**Рис. 5.60.** Вкладка Tools, раздел DHCP Leases

**Таблица 5.26.** Информация о DHCP Leases

Поле	Описание
Host	Имя хоста
IP	Выданный IP-адрес хосту
MAC Address	MAC-адрес данного клиента
Client ID	Идентификационный номер клиента
Expiry Time	Дата и время, после которого у клиента истекает актуальность выданного сервером IP-адреса



### 5.5.12. Reboot

Раздел Reboot на вкладке Tools предназначен для перезагрузки устройства или сброса в заводские настройки. На **Рис. 5.61** представлен пример страницы.

Чтобы перезагрузить устройство, нажмите кнопку **Reboot**.

Чтобы сбросить устройство в состояние заводских настроек, поставьте галочку напротив **Perform factory reset** и нажмите кнопку **Reboot**.

Status	Network	VPN / Tunnels	Services	Tools
--------	---------	---------------	----------	-------

Access
iRZ Link Client
iRZ ZTP Client
Change Password
Unit Name
Send SMS
Ping
System Log
GPIO
Wi-Fi Clients
DHCP Leases
<b>Reboot</b>

Perform factory reset

Reboot process will take about 60 seconds to complete.

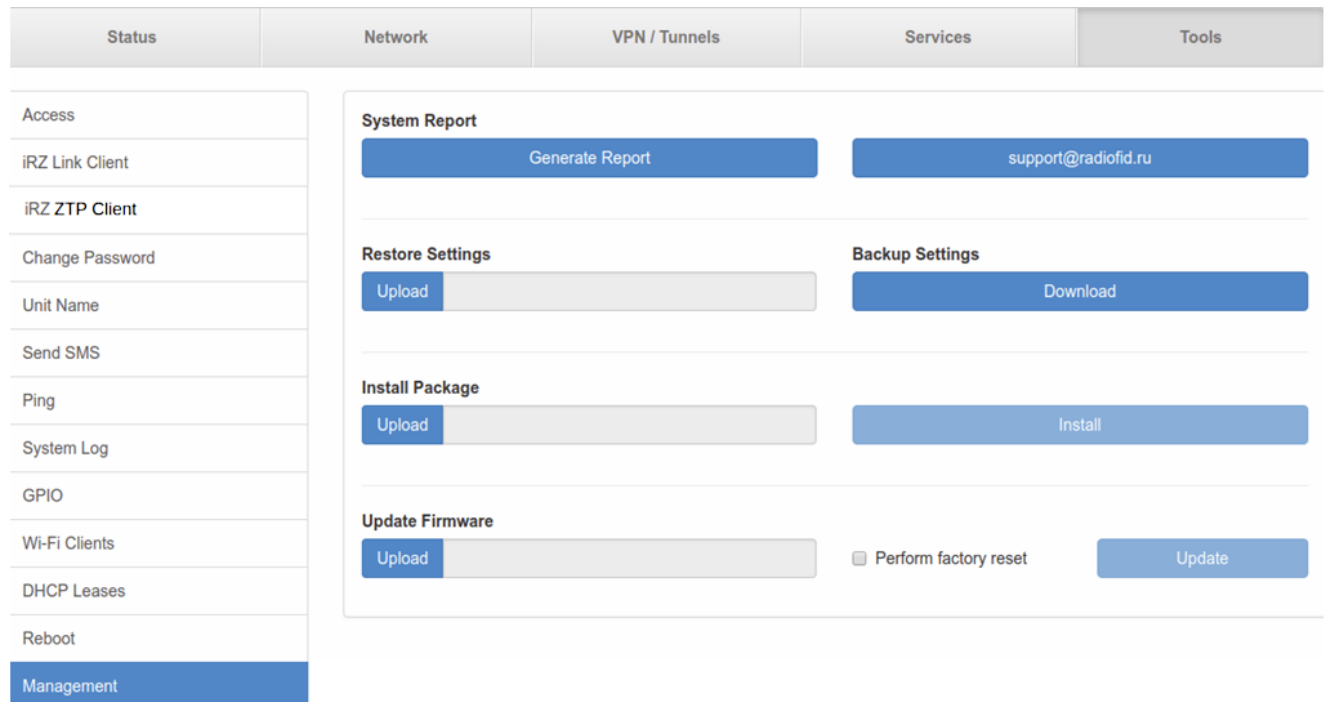
**Reboot**

**Рис. 5.61.** Вкладка Tools, раздел Reboot



### 5.5.13. Management

На данной странице настроек представлена возможность сохранения всех сделанных настроек в файл и их восстановление из файла, возможность установить дополнительный программный пакет или обновить версию прошивки роутера. Пример страницы приведён на **Рис. 5.62**



The screenshot shows the 'Tools' tab in the router's management interface. On the left is a sidebar menu with 'Management' selected. The main content area is divided into several sections:

- System Report:** Contains a 'Generate Report' button and a text input field with 'support@radiofid.ru'.
- Restore Settings:** Contains an 'Upload' button.
- Backup Settings:** Contains a 'Download' button.
- Install Package:** Contains an 'Upload' button and an 'Install' button.
- Update Firmware:** Contains an 'Upload' button, a checkbox for 'Perform factory reset', and an 'Update' button.

**Рис. 5.62.** Вкладка Tools, раздел Management

#### Получение репорт-файла.

Нажмите кнопку **Generate Report** и роутер предложит вам сохранить текстовый файл, в котором собраны логи работы роутера и его настройки. Данный файл удобен для диагностики различных проблем в настройках роутера. Соседняя кнопка предложит вам сразу написать письмо в техническую поддержку по возникшим вопросам.

#### Сохранение настроек устройства.

Нажмите кнопку **Download** в подразделе **Backup Settings** и сохраните полученный файл в компьютере.

#### Загрузка сохраненных настроек устройства.

Нажмите кнопку **Upload** в подразделе **Restore Settings** и выберите ранее сохраненный файл с настройками.

#### Установка дополнительных пакетов на устройство.

Нажмите кнопку **Upload** в подразделе **Install Package**, чтобы выбрать файл-пакет, а затем нажмите кнопку **Install**, чтобы использовать пакет в устройстве.



### **Обновление внутреннего ПО (прошивки) устройства.**

Нажмите кнопку **Upload** в подразделе **Update Firmware**, чтобы выбрать файл с прошивкой. Чтобы использовать выбранный файл в устройстве нажмите кнопку **Update**. Чтобы при обновлении прошивки сбросить настройки устройства в заводские, поставьте перед обновлением галочку напротив **Perform factory reset**.



## 6. Контакты и поддержка

Новые версии встроенного ПО, документации и сопутствующего программного обеспечения можно получить при обращении по следующим контактам.

Санкт-Петербург	
сайт компании в Интернете:	<a href="http://www.radiofid.ru">www.radiofid.ru</a>
тел. в Санкт-Петербурге:	+7 (812) 318 18 19
e-mail:	<a href="mailto:support@radiofid.ru">support@radiofid.ru</a>

Наши специалисты всегда готовы ответить на Ваши вопросы, помочь в установке, настройке и устранении проблемных ситуаций при эксплуатации оборудования iRZ.

При обращении в техническую поддержку в случае проблемных ситуаций указывайте, пожалуйста, версию используемого в роутере программного обеспечения. Кроме того, рекомендуется прикрепить к письму журналы запуска проблемных сервисов, снимки экранов настроек и любую другую полезную информацию. Чем больше информации будет предоставлено специалисту технической поддержки, тем быстрее он сможет разобраться в сложившейся ситуации.

**Примечание.** Перед обращением в техническую поддержку рекомендуется обновить программное обеспечение роутера до актуальной версии.



## Приложение 1

### Синтаксис IP-адреса

IP-адрес описывает адрес узла в IP-сети и состоит из 4х частей (октетов). Октет не может быть больше числа 254. Последний октет не может быть нулем.

**Пример: 80.70.224.2**

### Синтаксис IP-адреса сети

IP-адрес сети описывает все адресное пространство IP-сети. Состоит из 4х частей (октетов) и маски подсети. Октет не может быть больше числа 254, маска подсети не больше числа 32.

**Пример: 90.30.173.60/28**

**Пример 2: 125.24.55.219 255.255.255.0**

### Синтаксис маски подсети

Маска подсети состоит из 4х октетов, каждый из которых не может быть больше числа 255.

**Пример: 255.255.255.0**

### Синтаксис MAC-адреса

MAC-адрес состоит из 6 частей, каждая из которых не может иметь значение более FF (шестнадцатеричная система счисления).

**Пример: 00:FF:BD:69:07:4A**



## Приложение 2

### Доступные команды управления

Ниже приведен список команд, которые могут быть использованы для работы с роутером. Перед вызовом команды рекомендуется ознакомиться с ее описанием.

#### A

arp  
ash  
awk

#### B

base64  
bash  
blockdev  
brctl  
busybox  
byteconv

#### C

cat  
chat  
chmod  
chown  
chpasswd  
clear  
cont\_check  
cp  
crond  
crontab  
cryptpw  
cut

#### D

date

dbclient

decode

depmod

df

dhcpd

dmesg

dnsdomainname

dnsmasq

dropbear

dropbearconvert

dropbearkey

du

#### E

echo

egrep

encode

env

expr

#### F

false

fgrep

firmware\_update

flash\_erase

flash\_lock

flash\_unlock

flashcp

flex

ftpget

ftpput

fw\_printenv

fw\_setenv

fwload

#### G

gdbserver

genhash

genreport

getimei

getopt

getpid

getty

getusbcom

gpin

gpio

gpiod

gpspipe

grep

gsminfo

gsminfod

gunzip

gzip

#### H

halt

head

hostname

httpd

hwclock

hwinfo

#### I

id

ifconfig

ifdown

ifup

inadyn

inetd

init

ip

ip6tables

ip6tables-restore

ip6tables-save

ipaddr

ipaddress

ipcalc

iplink

iproute

iprule

ipsec\_ping

iptables

iptables-restore





iptables-save  
iptables-xml  
iptunnel

## K

keepalived  
kill  
killall  
klogd

## L

led  
less  
ln  
loaddefaults  
loadset  
lockfile-check  
lockfile-create  
lockfile-remove  
lockfile-touch  
logger  
login  
logrotate  
ls  
lsuf

## M

mail-lock  
mail-touchlock  
mail-unlock  
makedevs

md5sum  
mdev  
mesg  
migrate\_set  
mii-diag  
mini\_snmpd  
mkdir  
mkfs.jffs2  
mknod  
mkpasswd  
modem  
modinfo  
modprobe  
mount  
mv

## N

netservices  
netstat  
nohup  
nslookup  
ntpd  
ntpdate

## O

openssl  
openvpn  
opinfo  
ovpn\_ping

## P

passwd

pcregrep  
pcretest  
picocom  
pidof  
pin\_enter  
pin\_lock  
pin\_unlock  
ping  
pinger  
plainrsa-gen  
post\_decode  
poweroff  
ppp\_ping  
ppp\_watch  
pppd  
pppdump  
pppinfo  
pppstats  
printf  
ps  
pwd  
python

## R

racoon  
racoonctl  
reboot  
reserved  
rm  
rmmod  
route  
run-parts

## S

scp  
sed  
seq  
set\_gsm\_param  
setkey  
setsim  
sh  
sim  
sim\_check  
sim\_check\_pres  
sim\_check\_reg  
sim\_switch  
sleep  
sms  
sort  
ssh  
start-stop-daemon  
stat  
stty  
sync  
syslogd

## T

tail  
talk  
tar  
tcpdump  
telnet  
telnetd  
test



tftp  
tftp\_reflash  
timeconv  
top  
touch  
tr  
traceroute  
tty-lock  
tty-unlock  
ttyS1-lock  
ttyS1-unlock  
ttyS2-lock  
ttyS2-unlock

## U

umount  
uname  
uniq  
unxz  
update\_index  
uptime  
usb  
usleep  
ussd  
uudecode  
uuencode

## V

vconfig  
vi

## W

watchdog  
wc  
wget  
wget\_reflash  
which

## X

xl2tpd  
xl2tpd-control  
xtables-multi  
xz  
xzcat

## Y

yes

## Z

zcat