ЭЛЕКТРОНИКА

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Средства управления и мониторинга на роутерах iRZ

Содержание

Перечень таблиц

Перечень рисунков

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**	
1.0 (18.07.2017)		Основной документ	
Выполнил	Колмак О., Головин В. Н.	**Проверил**	Колмак О.

1.2. Предупреждение

Примечание. Для каждой модели роутера существует своя версия комплекта документации. Обращайтесь, пожалуйста, к документации для Вашего 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.

1.3. 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.

HW VSP – сокращенное название программы HW Virtual Serial Port, позволяющей добавить в операционную систему виртуальный COM-порт и перенаправлять данные с этого порта через TCP/IP-сеть на заданный IP-адрес и порт физического интерфейса.

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, 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	Веб-интерфейс, позволяющий настроить все регламентированные функции роутера. Можно использовать любой стандартный интернет-браузер.	Интернет-браузер - Opera, Firefox, IE, Chrome, Safari и т.д.
Telnet	Командная консоль, предназначенная для более тонкой настройки устройства. Позволяет использовать стандартные команды Linux.	Telnet-клиент - присутствует во всех ОС (в Windows 7 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 – native в UNIX ▪ PuTTY, WinSCP, openssh (win32) в Windows

3. Быстрый доступ к устройству

Для получения доступа к web-интерфейсу роутера можно использовать любой стандартный интернет-браузер, поддерживающий HTTP 1.0. Например, Opera, Firefox, IE или Chrome.

Откройте интернет-браузер и выполните следующие действия.

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

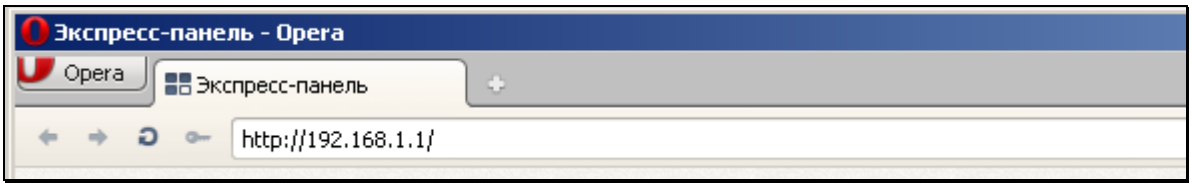

Рис. 3.1. Ввод IP-адреса роутера в адресную строку интернет-браузера

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

Если роутер включен, то после ввода IP-адреса роутера появится страница приветствия. Страница приветствия содержит краткую информацию о состоянии устройства и сети:

- имя устройства (UNIT NAME);
- 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.

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

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

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

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

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 в течении около 10 секунд (время зависит от конкретной модели), роутер перезагрузиться уже со сброшенными настройками.

Если после перезагрузки настройки роутера оказались так и не сброшены, возможно, вы удерживали кнопку не достаточно долго.

Также настройки роутера можно сбросить через веб-интерфейс, см. раздел 5.4.10 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.

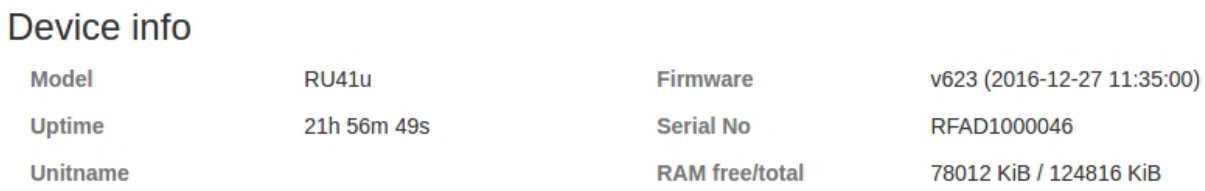

Рис. 5.1. Пример информации в разделе Device Info

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

Routing — информация о режиме работы WAN-портов.

Рис. 5.2. Пример информации в разделе Routing

Таблица 5.2. Поля в разделе Routing

Поле	Описание
Mode	Указывает режим работы WAN портов: balancing — режим балансировки трафика между wan портами; reserving — 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.

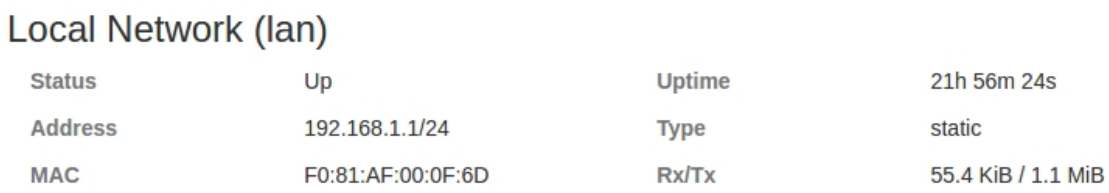

Рис. 5.3. Пример информации в разделе Local Network

Таблица 5.3. Поля в разделе Local Network (LAN)

Поле	Описание
Status	Указывается есть ли физическое подключение к порту: Up — подключение есть; Down — подключения нет
Address	IP-адрес порта с указанием макси 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) — информация о состоянии подключения по каналу сотовой сети (два раздела, если устройство поддерживает две SIM-карты).

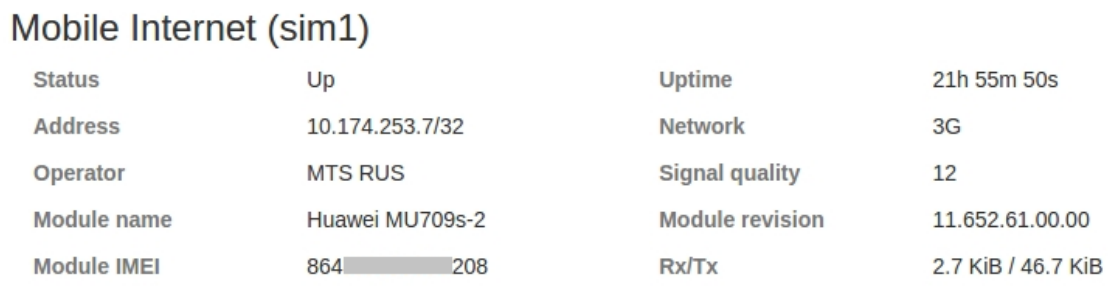

Рис. 5.4. Пример информации в разделе Mobile Internet

Таблица 5.4. Поля раздела Mobile Internet

Поле	Описание
Status	Указывается статус подключения к сотовой сети: - Up — SIM-карта зарегистрирована в сети сотового оператора и готова к работе; - Down — SIM-карта не зарегистрирована в сети и не работает.
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, когда сигнала нет совсем — 0, максимальное значение уровня сигнала — 31, стабильная работа сети начинается с уровня сигнала 12).
Module Revision	Номер версии GSM-модуля роутера
Rx/Tx	Счетчик принятых и отправленных байт

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

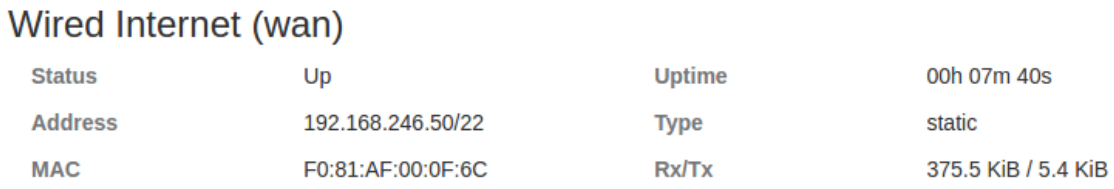

Рис. 5.5. Пример информации в разделе Wired Internet (WAN)

Таблица 5.5. Поля в разделе Wired Internet (WAN)

Поле	Описание
Status	Состояние порта: - Up — порт активен и работает; - Down — порт выключен.
Address	IP-адрес порта с указанием маски сети
MAC	MAC-адрес порта
Uptime	Время активности порта
Type	Тип работы порта: - static — на порту назначен статический IP-адрес; - DHCP — порт получает адрес от внешнего DHCP-сервера; - PPPoE — порт подключается к внешнему PPPoE-серверу.
Rx/Tx	Счетчик принятых и отправленных байт

IPsec Tunnel — информация о состоянии IPsec-тоннеля (или тоннелей, если их создано больше). В скобках указывается название тоннеля.

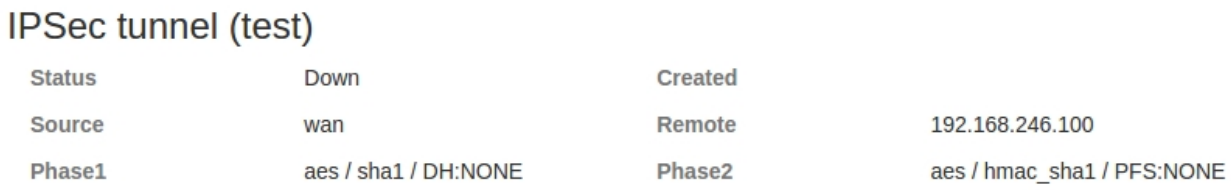

Рис. 5.6. Пример информации в разделе IPsec Tunnel

Таблица 5.6. Поля в разделе IPsec Tunnel

Поле	Описание
Status	Статус тоннеля: Up — тоннель создан и работает; Down — тоннель не создан или выключен.
Source	Имя интерфейса, с которого осуществляется работа тоннеля
Phase 1	Указываются какие алгоритмы шифрования включены, а какие выключены в Фазе 1
Created	Указывает, что туннель создан
Remote	Указывается IP-адрес внешнего интерфейса тоннеля на другой стороне
Phase 2	Указываются какие алгоритмы шифрования включены, а какие выключены в Фазе 2

OpenVPN Tunnel — информация о состоянии OpenVPN-тоннеля. В скобках указывается название тоннеля.

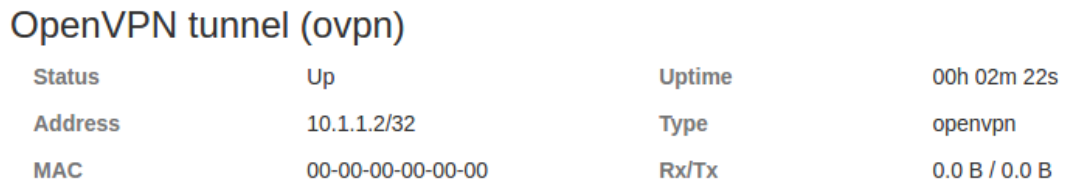

Рис. 5.7. Пример информации в разделе OpenVPN Tunnel

Таблица 5.7. Поля в разделе OpenVPN tunnel

Поле	Описание
Status	Состояние тоннеля: ▪ Up — тоннель активен и работает; ▪ Down — тоннель выключен.
Address	IP-адрес самого тоннеля этого роутера
MAC	MAC-адрес тоннеля
Uptime	Время активности тоннеля
Type	Тип работы тоннеля, единственное значение — openvpn
Rx/Tx	Счетчик принятых и отправленных байт, пройденных через тоннель

Interface — информация о состоянии GRE-тоннеля (или тоннелей, если их создано больше). В скобках указывается название тоннеля.

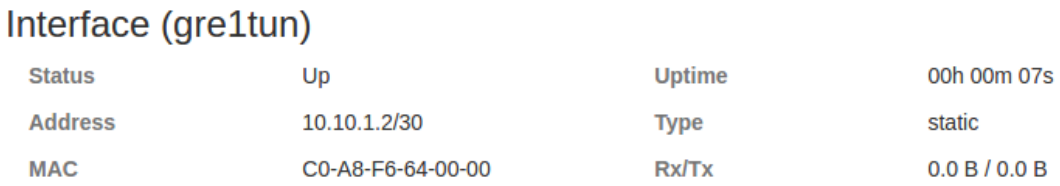

Рис. 5.8. Пример информации в разделе Interface

Таблица 5.8. Поля в разделе Interface

Поле	Описание
Status	Состояние тоннеля: ▪ Up — тоннель активен и работает; ▪ Down — тоннель выключен.
Address	IP-адрес самого тоннеля этого роутера
MAC	MAC-адрес тоннеля, совпадающий с MAC-адресом физического интерфейса от которого работает тоннель
Uptime	Время активности тоннеля
Type	Тип работы тоннеля
Rx/Tx	Счетчик принятых и отправленных байт, пройденных через тоннель

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

Рис. 5.9. Пример информации в разделе Routing Table

5.2. Раздел «Network»

Чтобы получить информацию по разделам OpenVPN Tunnel, GRE Tunnels и IPsec Tunnels смотрите «Руководство пользователя. Настройка туннелей на роутерах iRZ».

5.2.1. Local Network

Раздел Local Network на вкладке Network предназначен для настройки Ethernet-портов роутера в рамках VLAN. В роутерах iRZ имеется возможность настроить WAN-порт таким образом, чтобы он работал, как локальный Ethernet-порт.

На рисунке 5.10 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). 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!

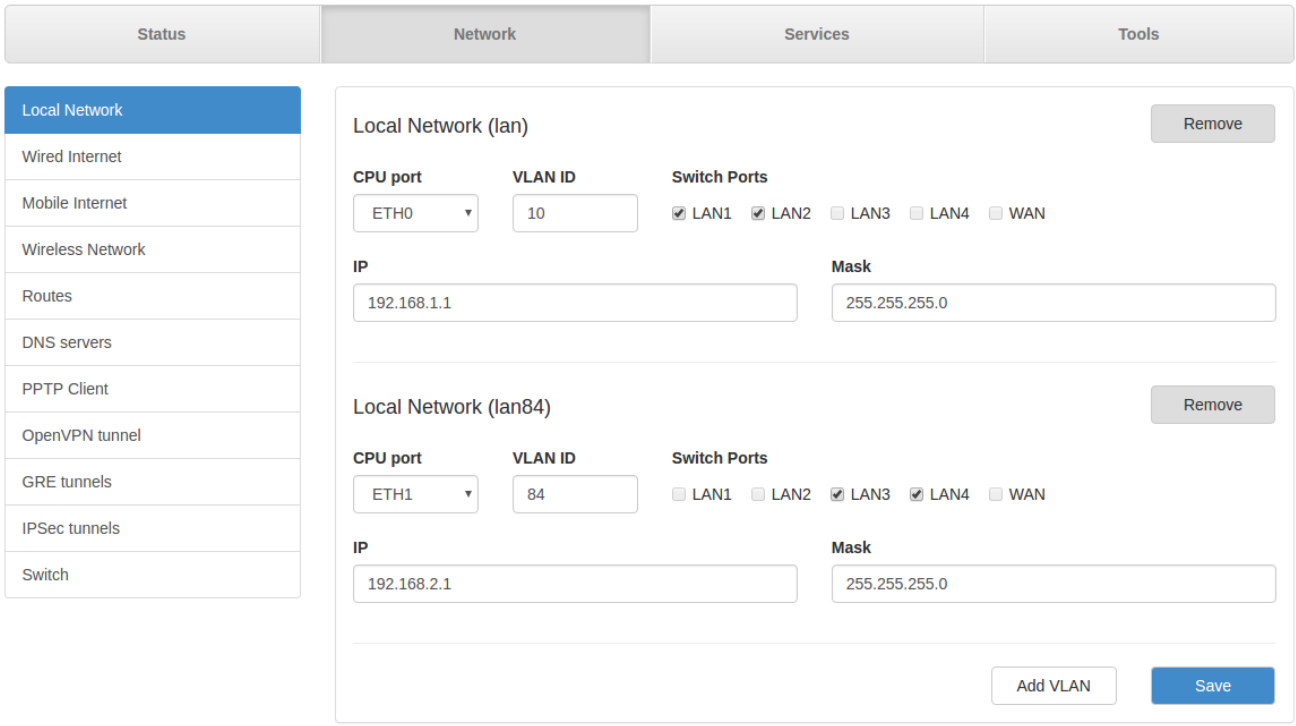

Рис. 5.10. Вкладка Network, раздел Local Network

Таблица 5.9. 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

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 рисунке 5.11 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!

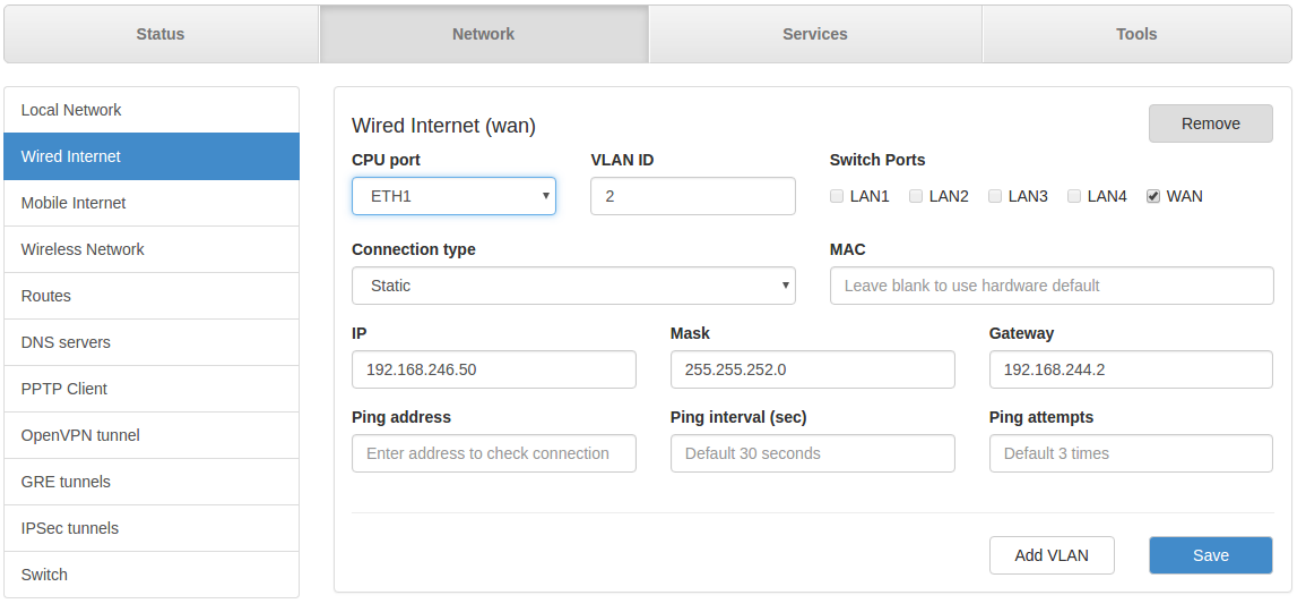

Рис. 5.11. Вкладка Network, раздел Wired Internet

Таблица 5.10. 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: [A] **Disabled** – отключение WAN-порта; [B] **DHCP** – соединение с получением настроек от DHCP-сервера; [C] **Static** – соединение с ручными настройками; [D] **PPPoE** – соединение с авторизацией на сервере PPPoE.

Дополнительные настройки (в зависимости от выбранного типа соединения, поле **Connection Type**):

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

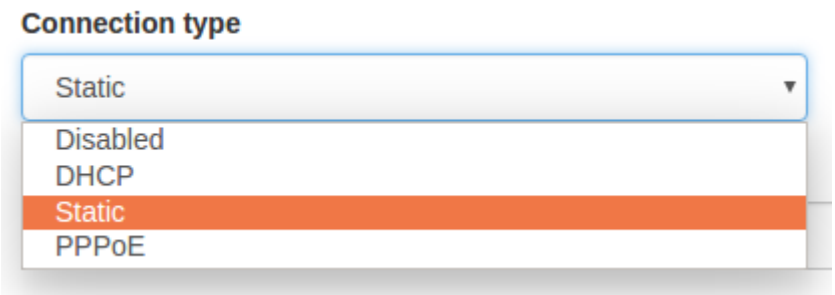

Рис. 5.12. Типы соединения для WAN-порта

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 рисунке 5.13, описание настроек приведено в таблице 5.10.

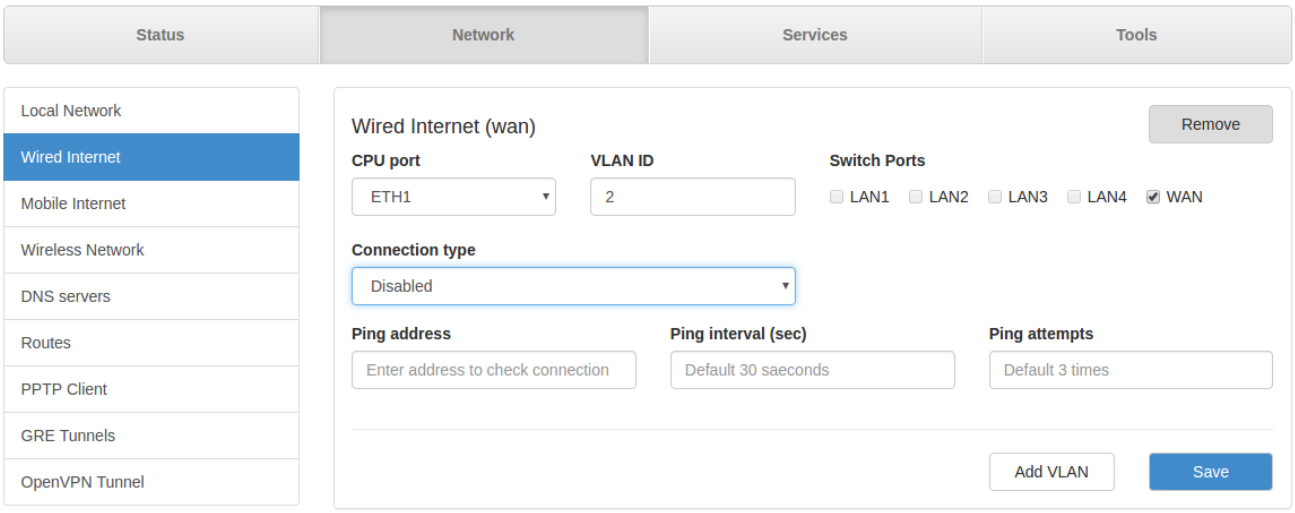

Рис. 5.13. WAN-порт отключен

Тип подключения **DHCP** означает, что роутер должен получить IP-адрес, маску и адреса DNS-серверов от внешнего DHCP-сервера. Пример настроек показан на рисунке 5.14, описание настроек приведено в таблице 5.10.

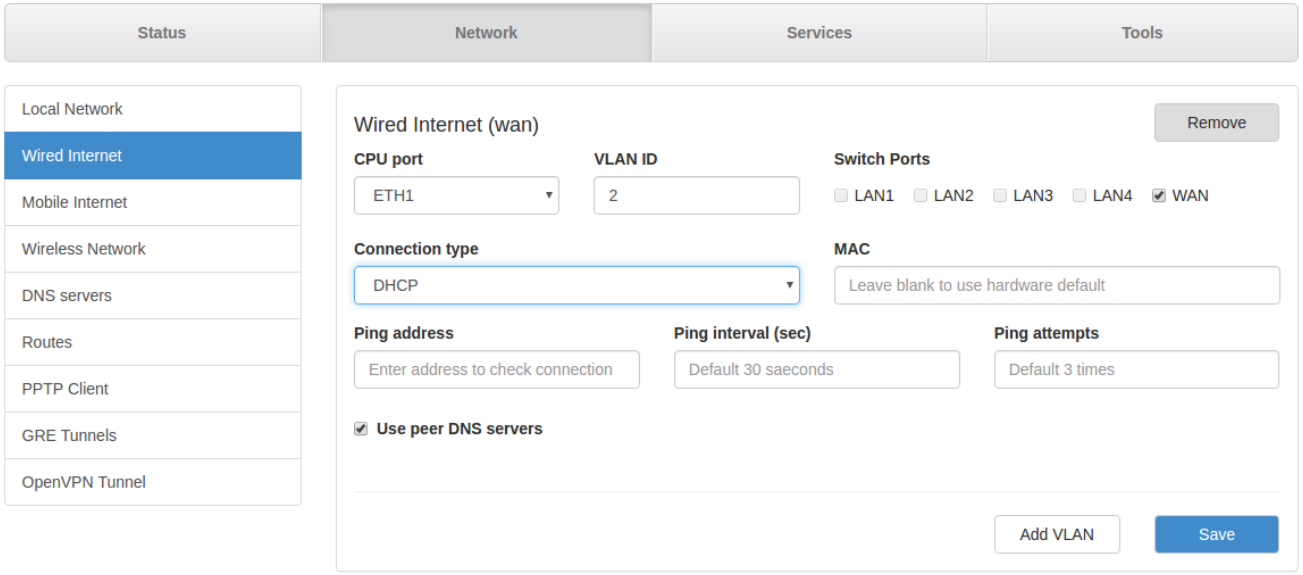

Рис. 5.14. Тип соединения WAN-порта – DHCP

Тип подключения **Static** необходим для ручной установки сетевых настроек WAN-порта. Пример настроек показан на рисунке 5.11, описание настроек приведено в таблице 5.10.

Тип подключения **PPPoE** необходим при использовании протокола с авторизацией на сервере PPPoE. Пример настроек показан на рисунке 5.15, описание настроек приведено в таблице 5.10.

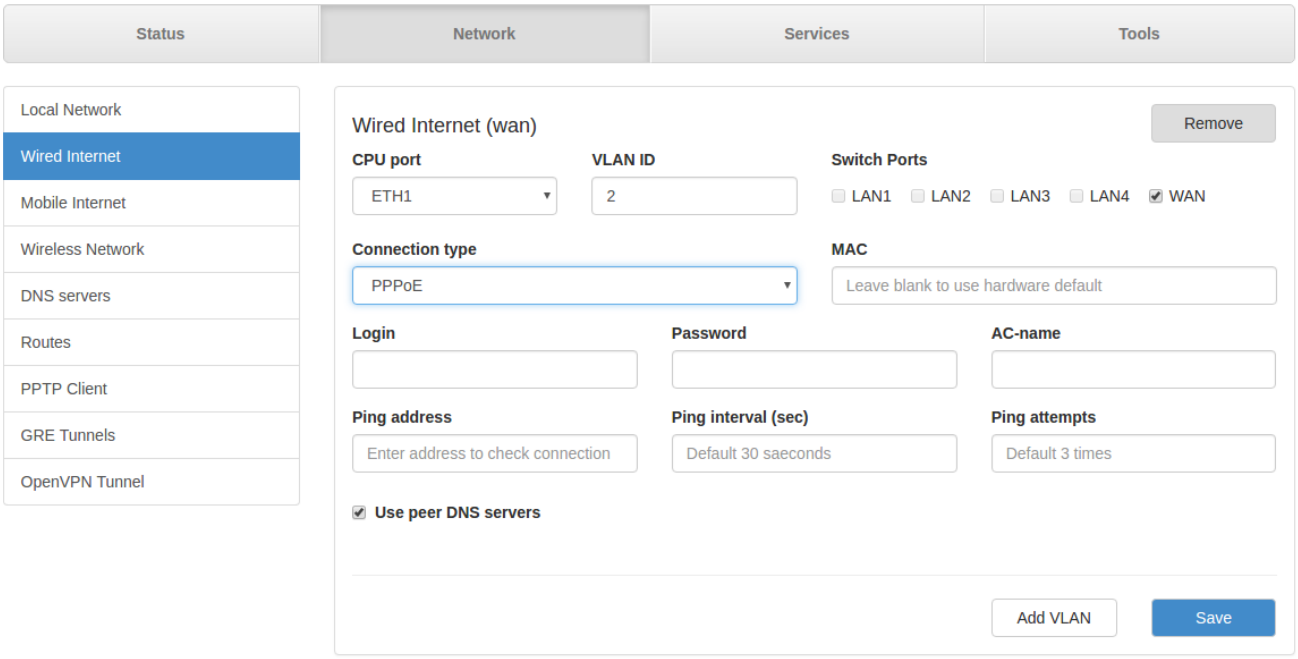

Рис. 5.15. Тип соединения WAN-порта – PPPoE

5.2.3. Mobile Internet

Раздел Mobile Internet на вкладке Network предназначен для настройки мобильного Интернета на устройстве. Если роутер поддерживает работу с двумя SIM-картами, то на страннице раздела будут представлены две группы настроек – соответственно, для SIM1 и SIM2.

На рисунке 5.16 представлен пример настроек роутера с двумя SIM-картами. Чтобы включать или отключать работу роутера с SIM-картой, необходимо поставить или снять галочку напротив пункта **Enable SIM1** (или **SIM2**). Нажатие на строку **Show Advanced Settings** открывает доступ ко всем доступным настройкам данного раздела.

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

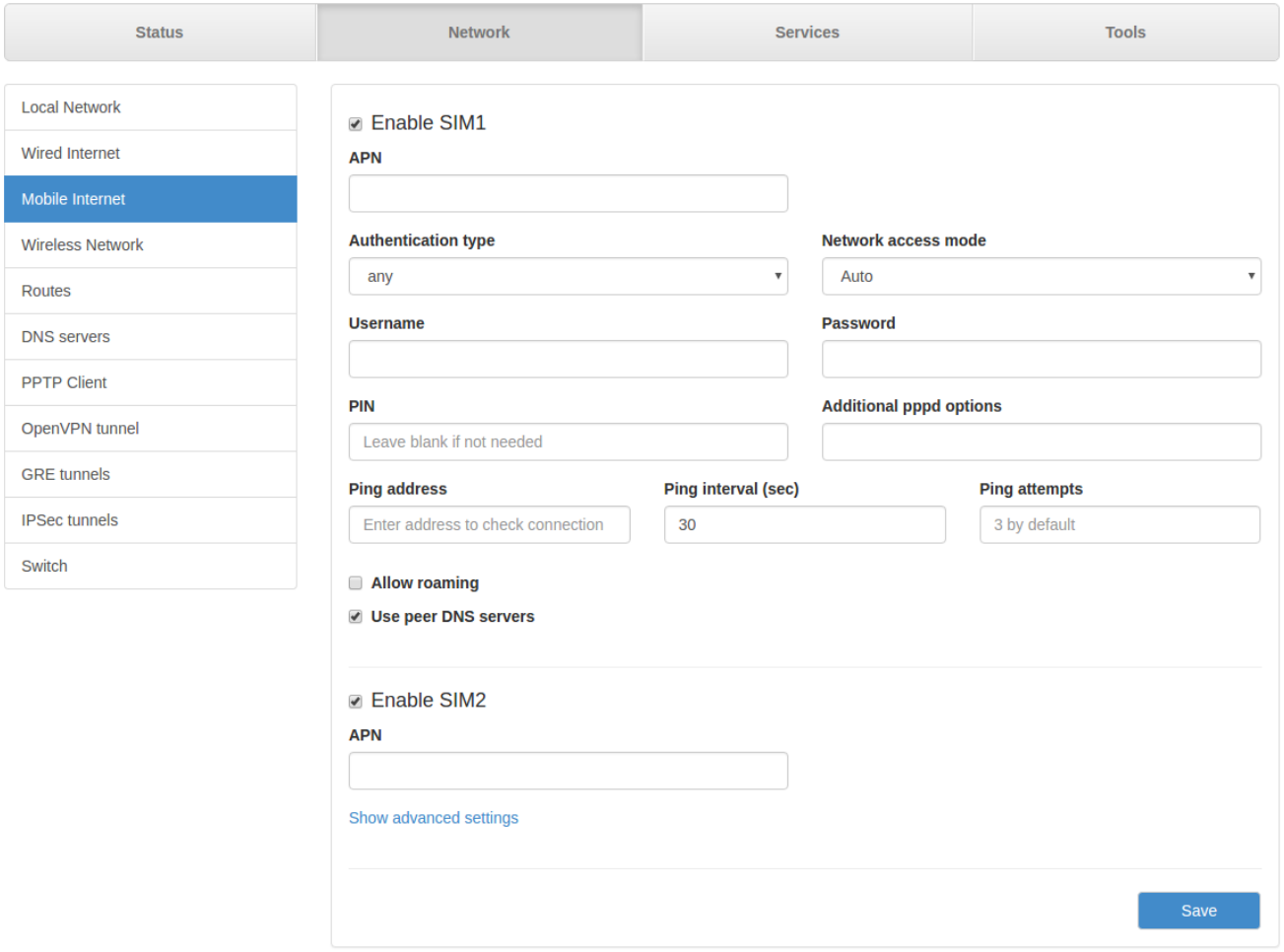

Рис. 5.16. Вкладка Network, раздел Mobile Internet

Таблица 5.11. Настройки Network → Wired Internet

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: - Any – любой из режимов (по умолчанию); - EAP; - PAP; - CHAP.
Network Access Mode	Выбор режима работы с сотовыми сетями: - Auto – автоматическое определение доступной сети; - 2G Only – работа только в сети 2G; - 3G Only – работа только в сети 3G.
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 PPPD, при работе с модулем сотовой связи
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 подключиться через сотовую сеть (по умолчанию, 3)
Allow Roaming	Разрешение/запрещение работы SIM-карты устройства в роуминге
Use Peer DNS Server	Включение/выключение использования внешних DNS-серверов провайдера

5.2.4. 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 название модели – «w»). На рисунке 5.17 представлен пример настроек Wi-Fi в режиме точки доступа.

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

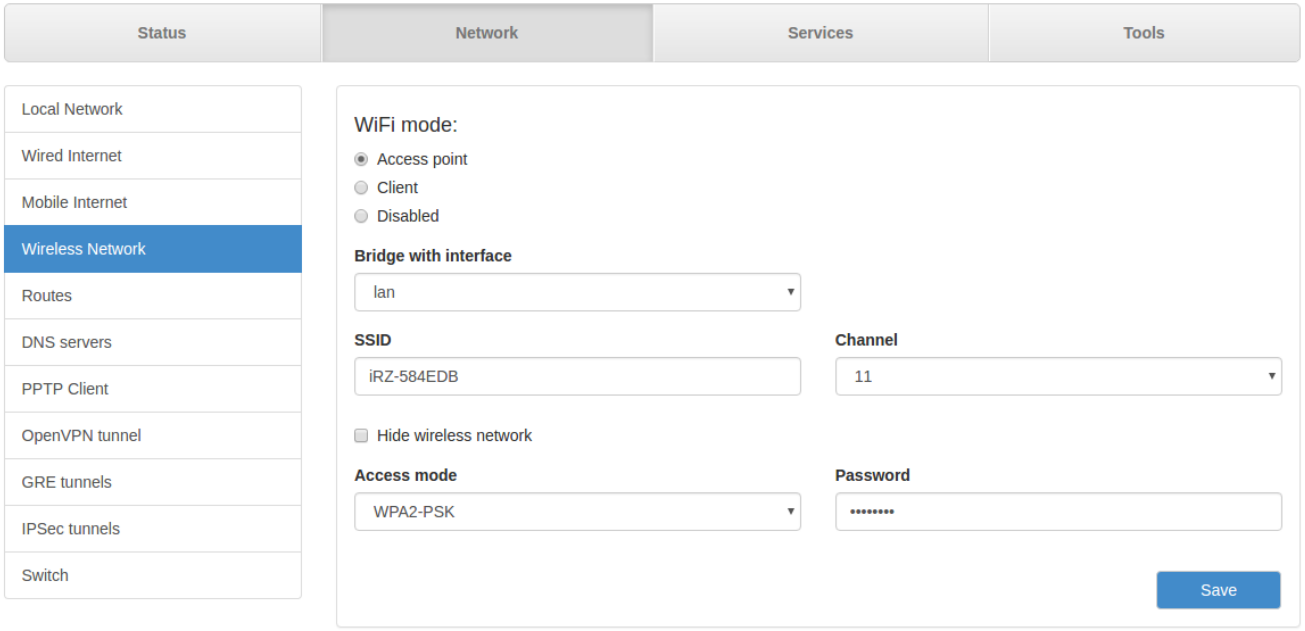

Рис. 5.17. Вкладка Network, раздел Wireless Internet

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, поэтому данный канал связи можно использовать как WAN-порт;
- **Disabled** — отключение Wi-Fi-модуля.

Access Point

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

Таблица 5.12. Настройки Network → Wireless Network (Wi-Fi Mode = Access Point)

Поле	Описание
Bridge with Interface	Создание моста с указанным интерфейсом
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
Access Mode	Тип шифрования пароля доступа к создаваемой Wi-Fi-сети: - Open – без пароля доступа; - WPA; - WPA2-PSK.
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 рисунке 5.17. При выборе в настройке **Bridge with Interface** пункта **Wi-Fi**, Wi-Fi-интерфейс будет работать, как самостоятельный интерфейс. Доступные настройки приведены на рисунке 5.18.

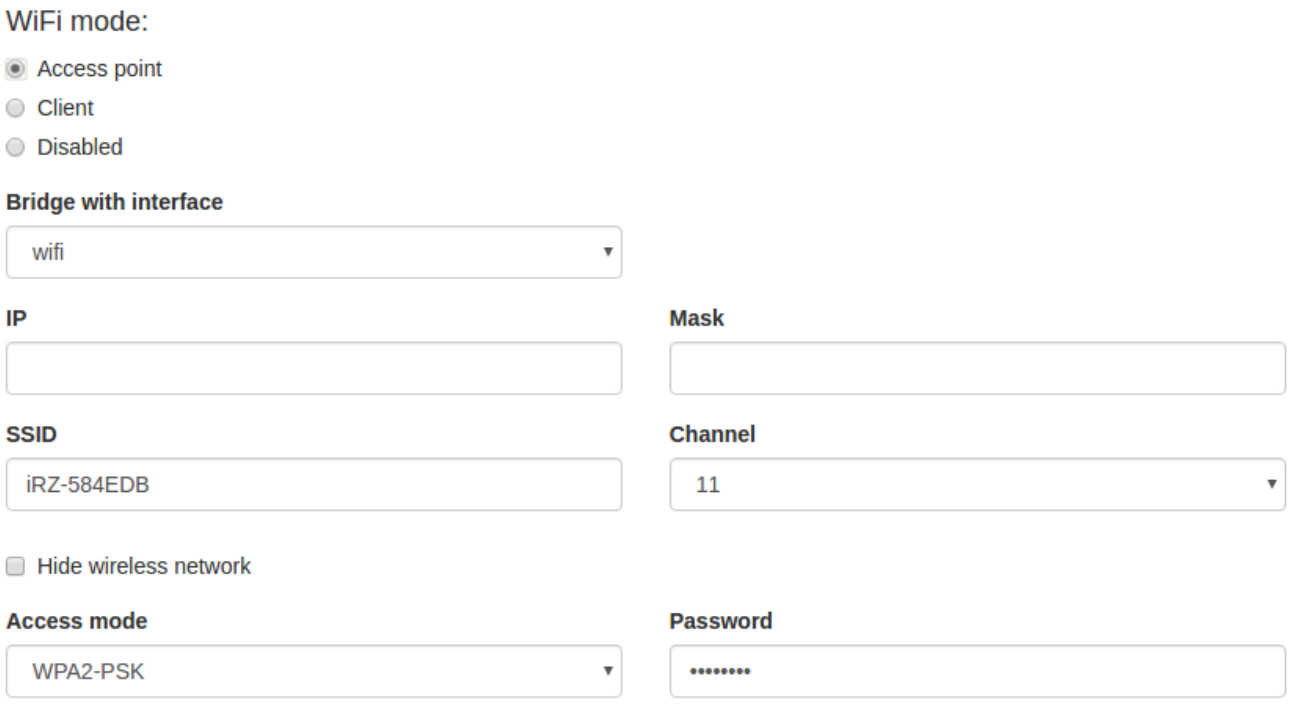

Рис. 5.18. Режим wifi настройки Bridge with Interface

Client

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

Таблица 5.13. Настройки Network → Wireless Network (Wi-Fi Mode = Client)

Поле	Описание
Connection Type	Выбор типа соединения: - DHCP – получение IP-адреса от сервера DHCP; - Static – статичные настройки роутера, прописываемы вручную.
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: - Open – без пароля доступа; - WPA; - WPA2-PSK.
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. Доступные настройки приведены на рисунке 5.19.

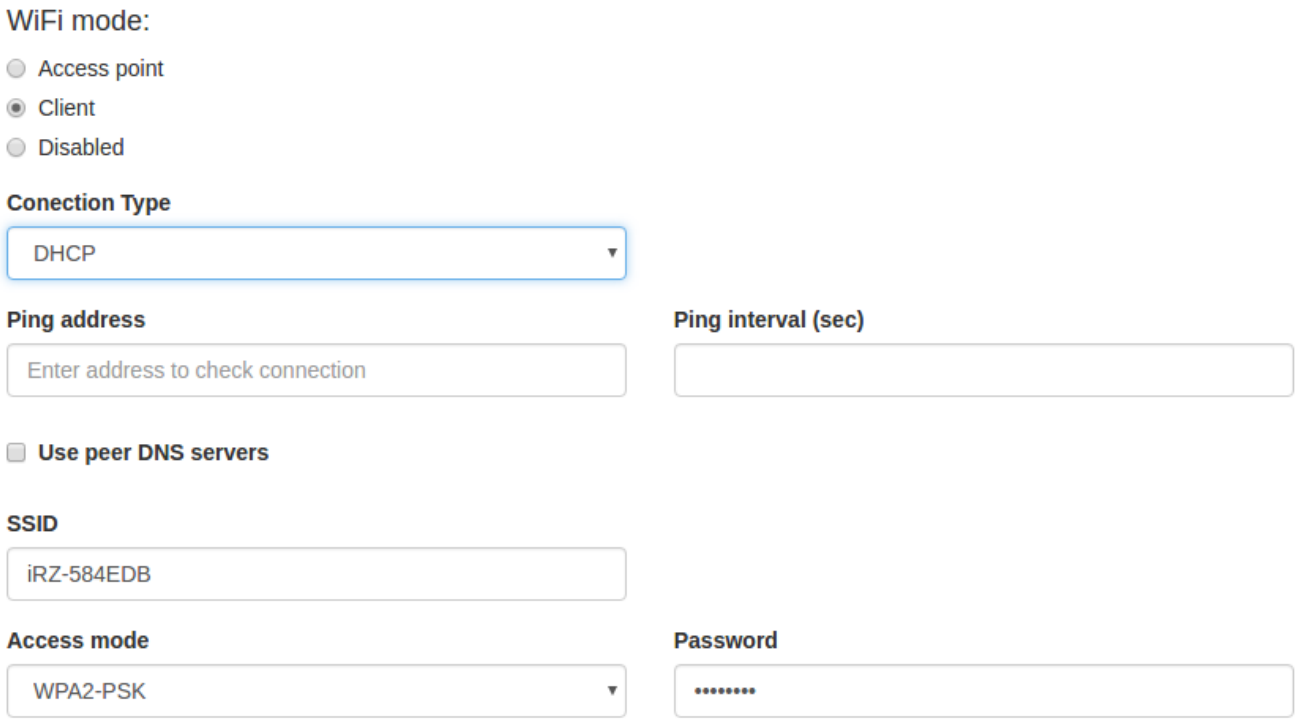

Рис. 5.19. Режим DHCP настройки Connection Type

При выборе в настройке **Connection Type** пункта **Static**, роутер будет работать со статичными настройками соединения, которые указываются в пунктах **IP**, **Mask** и **Gateway**. Доступные настройки приведены на рисунке 5.20.

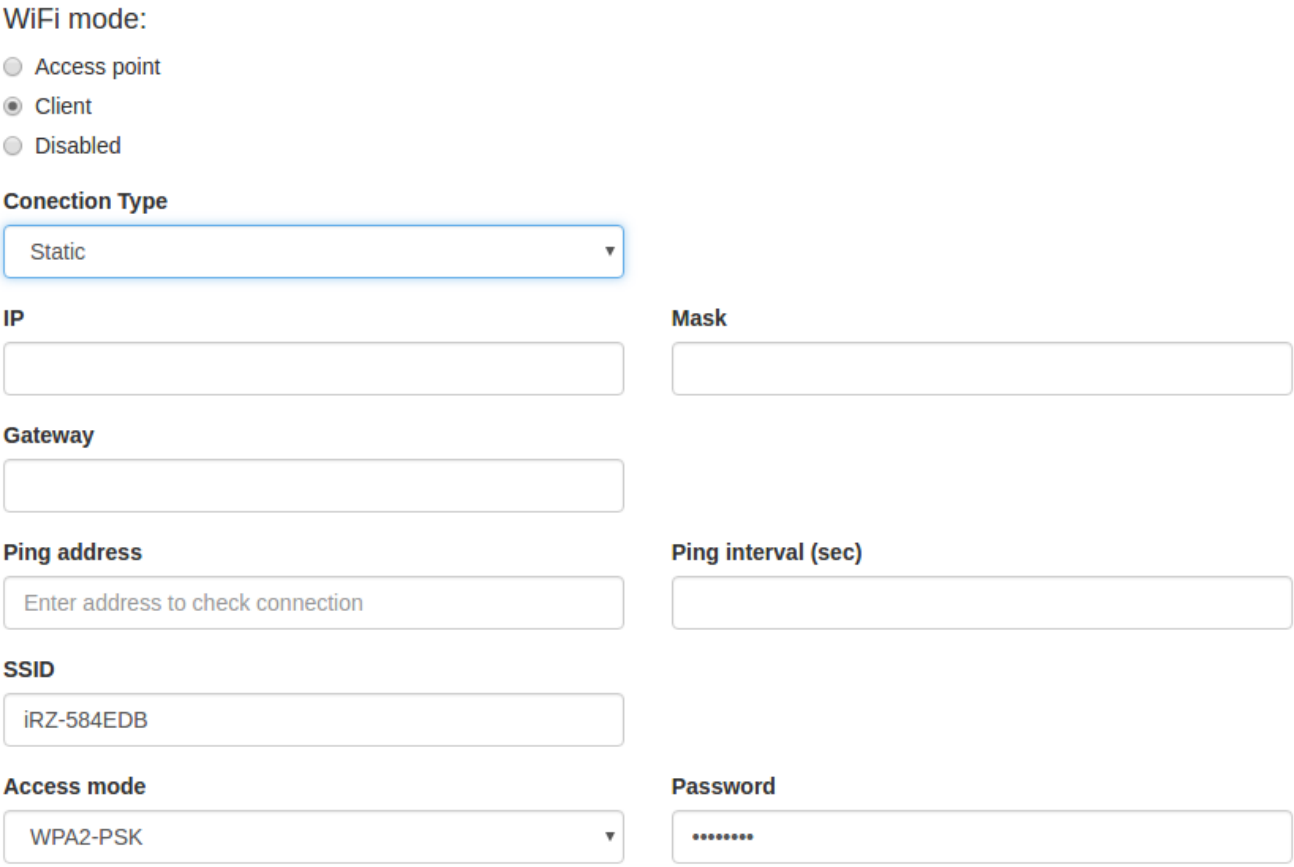

Рис. 5.20. Режим Static, настройки Connection Type

5.2.5. Routes

Раздел Routes на вкладке Network предназначен для настройки приоритетов WAN-портов, режим их работы и настройки статических маршрутов. На рисунке 5.21 представлен пример настроек Wi-Fi в режиме точки доступа.

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

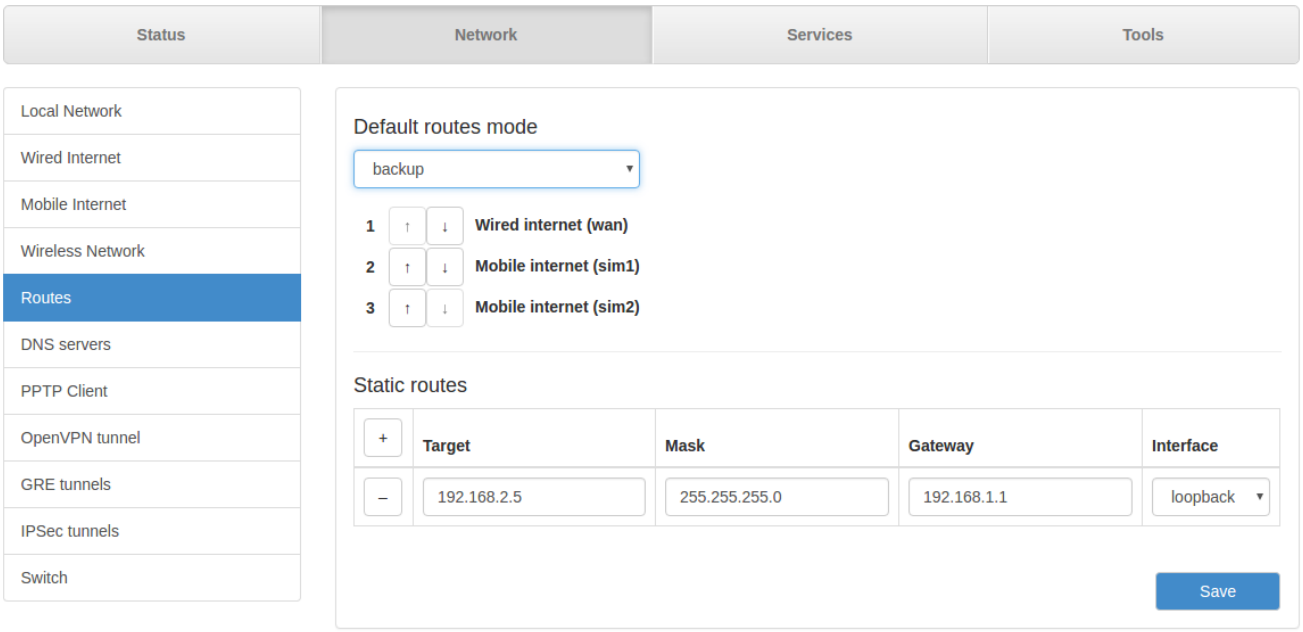

Рис. 5.21. Вкладка Network, раздел Routes

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 рисунке 5.21). 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 рисунке 5.22.

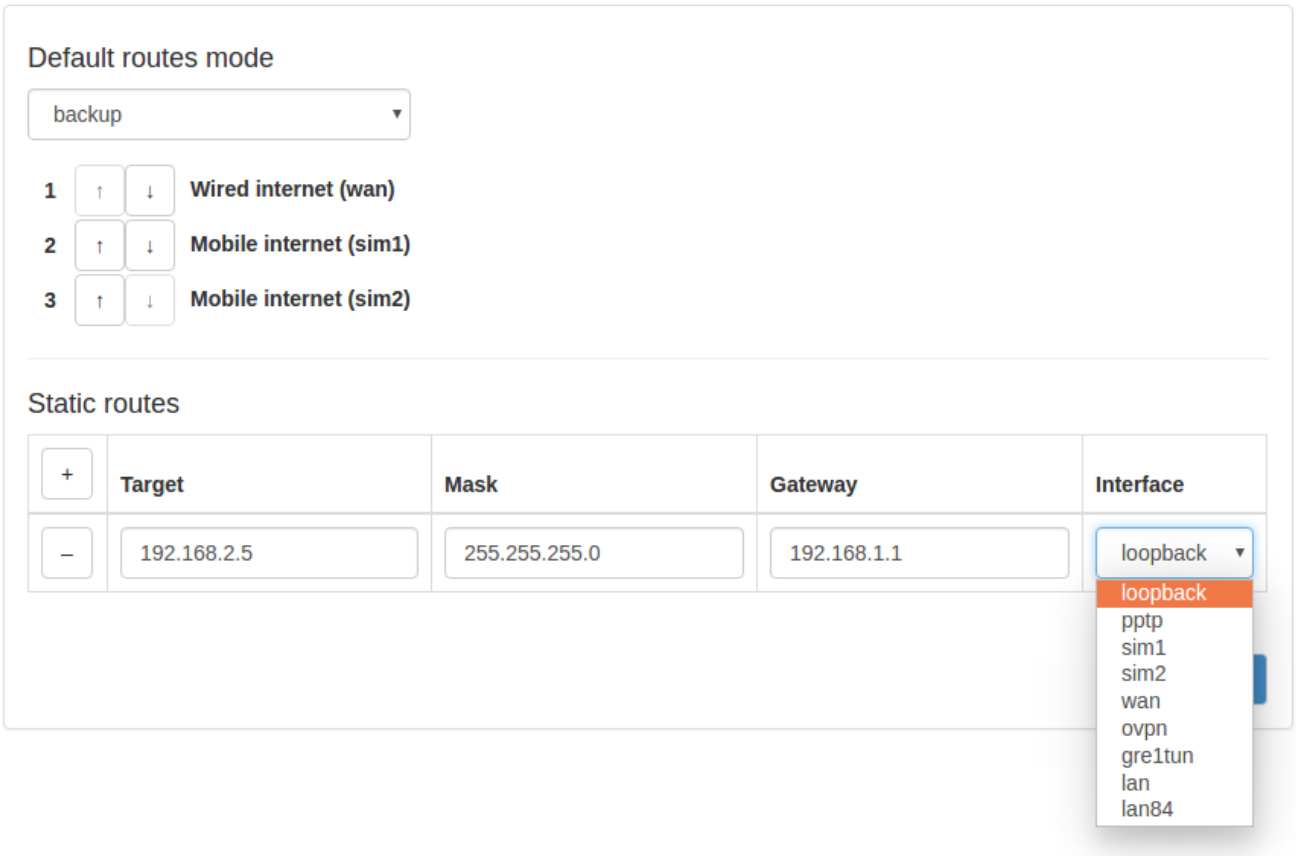

Рис. 5.22. Настройка статических маршрутов

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 5.14.

Таблица 5.14. 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

5.2.6. DNS Servers

Раздел DNS Servers на вкладке Network предназначен для указания адресов DNS-серверов. На рисунке 5.23 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!

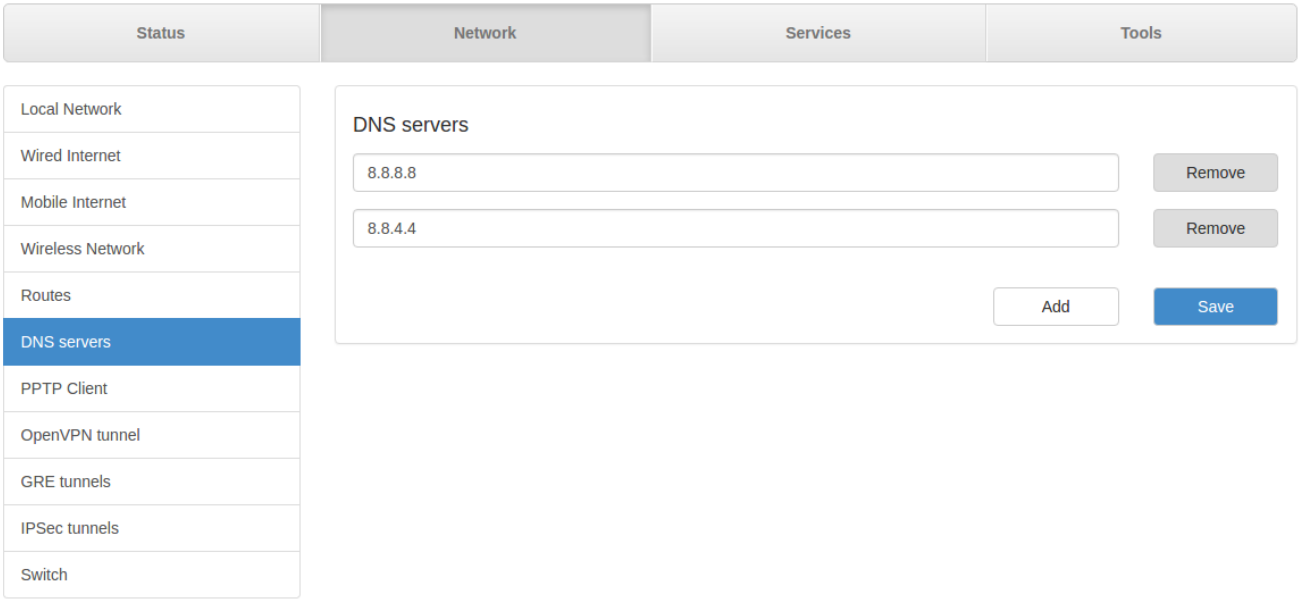

Рис. 5.23. Вкладка Network, раздел DNS Servers

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.

5.2.7. PPTP Client

Раздел PPTP Client на вкладке Network предназначен для настройки подключения по PPTP в режиме клиента. На рисунке 5.24 представлен пример настройки подключения.

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

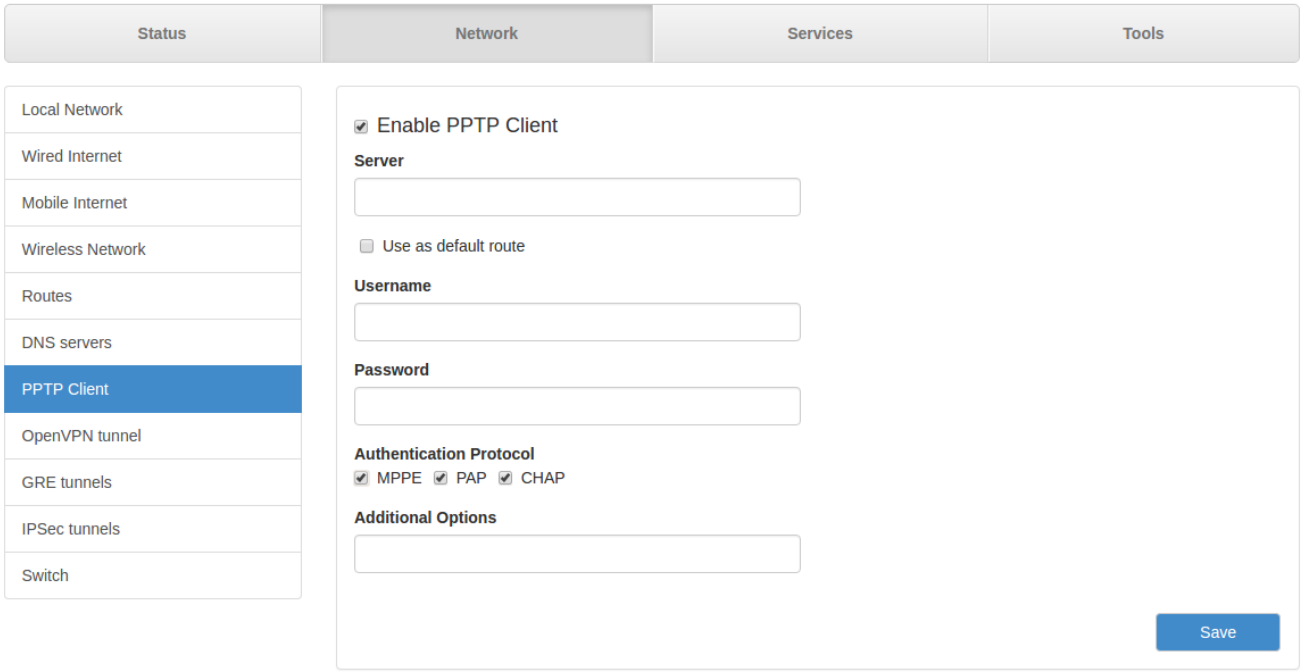

Рис. 5.24. Вкладка Network, раздел PPTP Client

Чтобы построить тоннель, поставьте галочку напротив **Enable PPTP Client** и впишите соответствующие настройки (см. таблицу 5.15). Тоннель будет работать через любой, активный на данный момент времени, WAN-порт.

Таблица 5.15. Настройки маршрутов

Поле	Описание
Server	IP-адрес сервера, к которому будет выполняться подключение
Use as Default Route	Включение/выключение установки маршрута по умолчанию через данный тоннель
Username	Имя пользователя для подключения к PPTP-серверу
Password	Пароль для подключения к PPTP-серверу
Authentication Protocol	Выбор методов шифрования трафика: - MPPE; - PAP; - CHAP.
Additional Options	Указание дополнительных опций для работы тоннеля, если необходимо

5.2.8. Switch

Раздел Switch на вкладке Network предназначен для управления Ethernet-портами роутера (LAN и WAN). На рисунке 5.25 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!

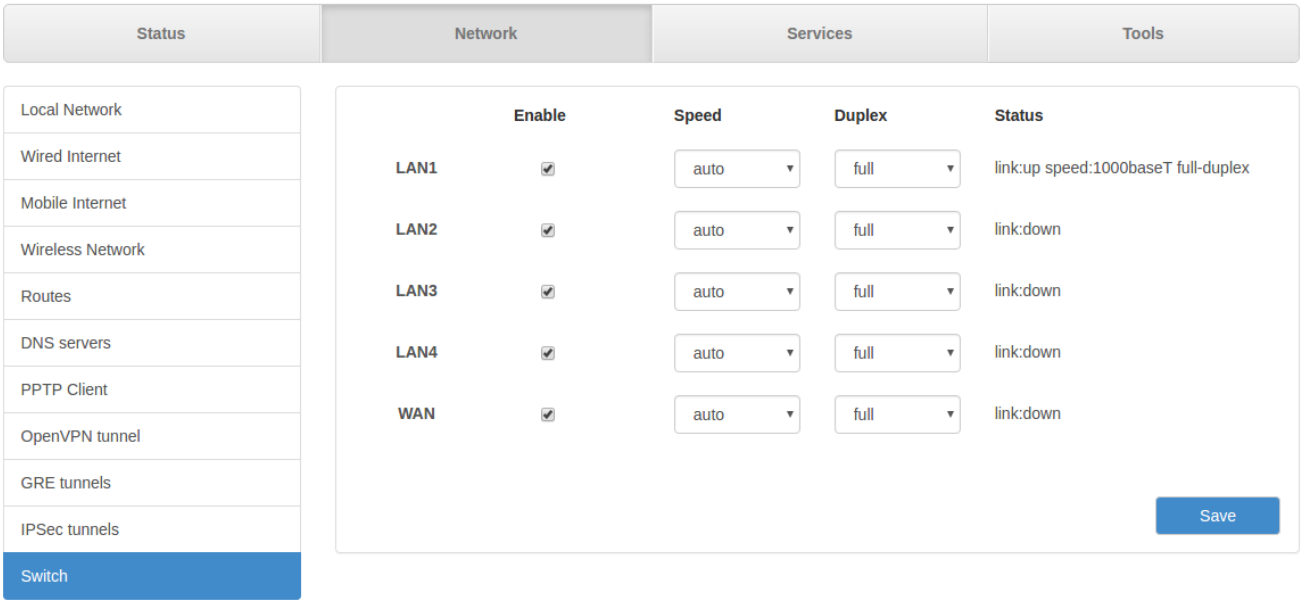

Рис. 5.25. Вкладка Network, раздел Switch

Таблица 5.16. 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: Full – передача и прием данных одновременно; Half – передача и прием данных по очереди.
Status	Информация о работе каждого порта

5.3. Раздел «Services»

5.3.1. DHCP

Раздел DHCP на вкладке Services предназначен для управления DHCP-сервером. На рисунке 5.26 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!

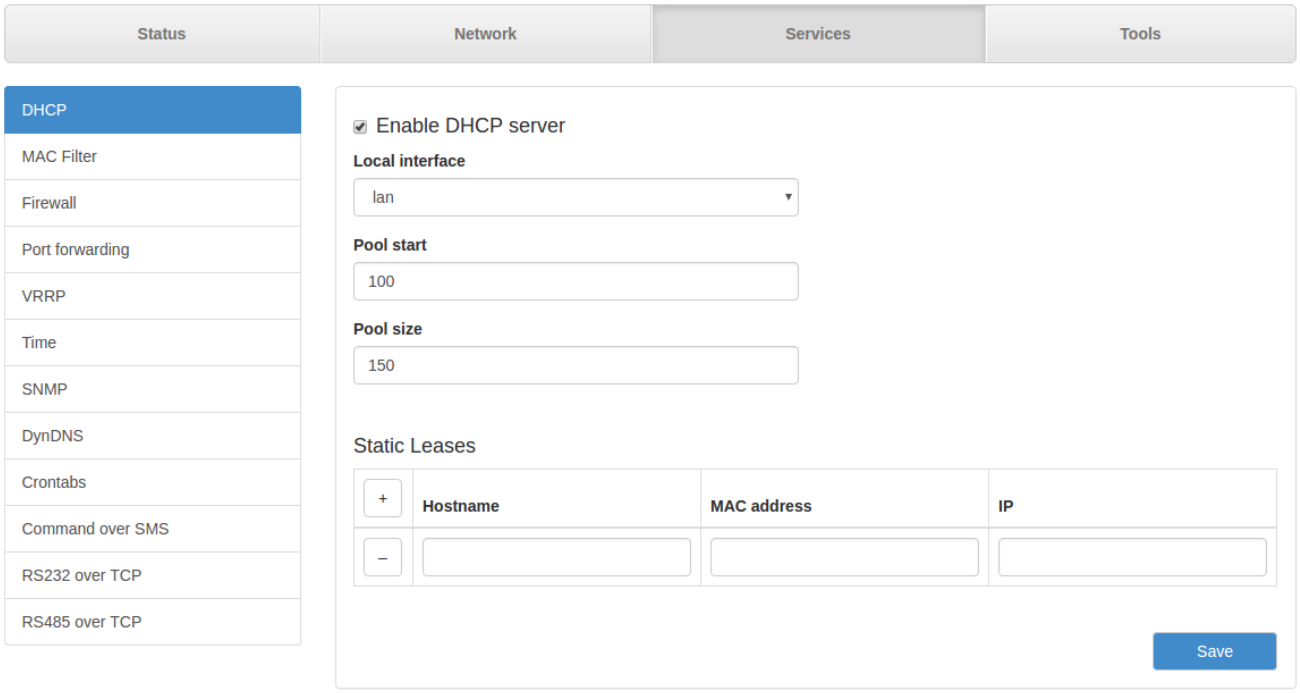

Рис. 5.26. Вкладка Services, раздел DHCP

Чтобы включить DHCP-сервер поставьте галочку напротив **Enable DHCP Server** и укажите настройки для его работы (см. таблицу 5.17).

Таблица 5.17. 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.**100** (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 значение будет «150»
Static Leases – указание IP-адресов, необходимых для сетевых устройств	
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 5.17.

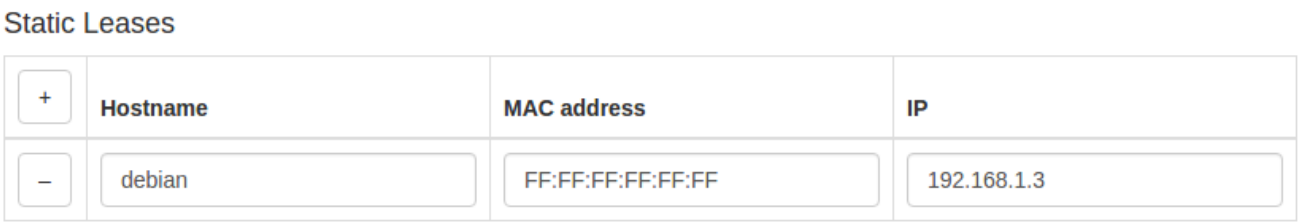

Рис. 5.27. Указание IP-адресов вручную

5.3.2. MAC Filter

Раздел MAC Filter на вкладке Services предназначен для установки и настройки фильтра по MAC-адресам. На рисунке 5.28 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!

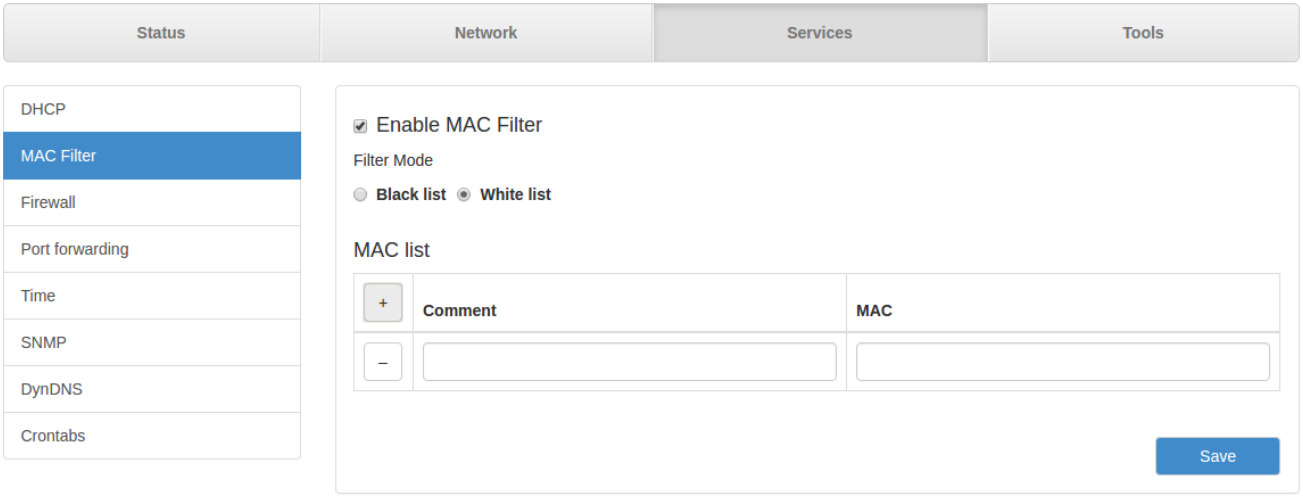

Рис. 5.28. Вкладка Services, раздел MAC Filter

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.

5.3.3. Firewall

Раздел Firewall на вкладке Services предназначен для настройки межсетевого экрана (файрволла). Настройки разбиты на три подгруппы: **Zones list**, **Allowed forwards**, **Firewall**. На рисунке 5.29 представлен пример настройки межсетевого экрана.

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

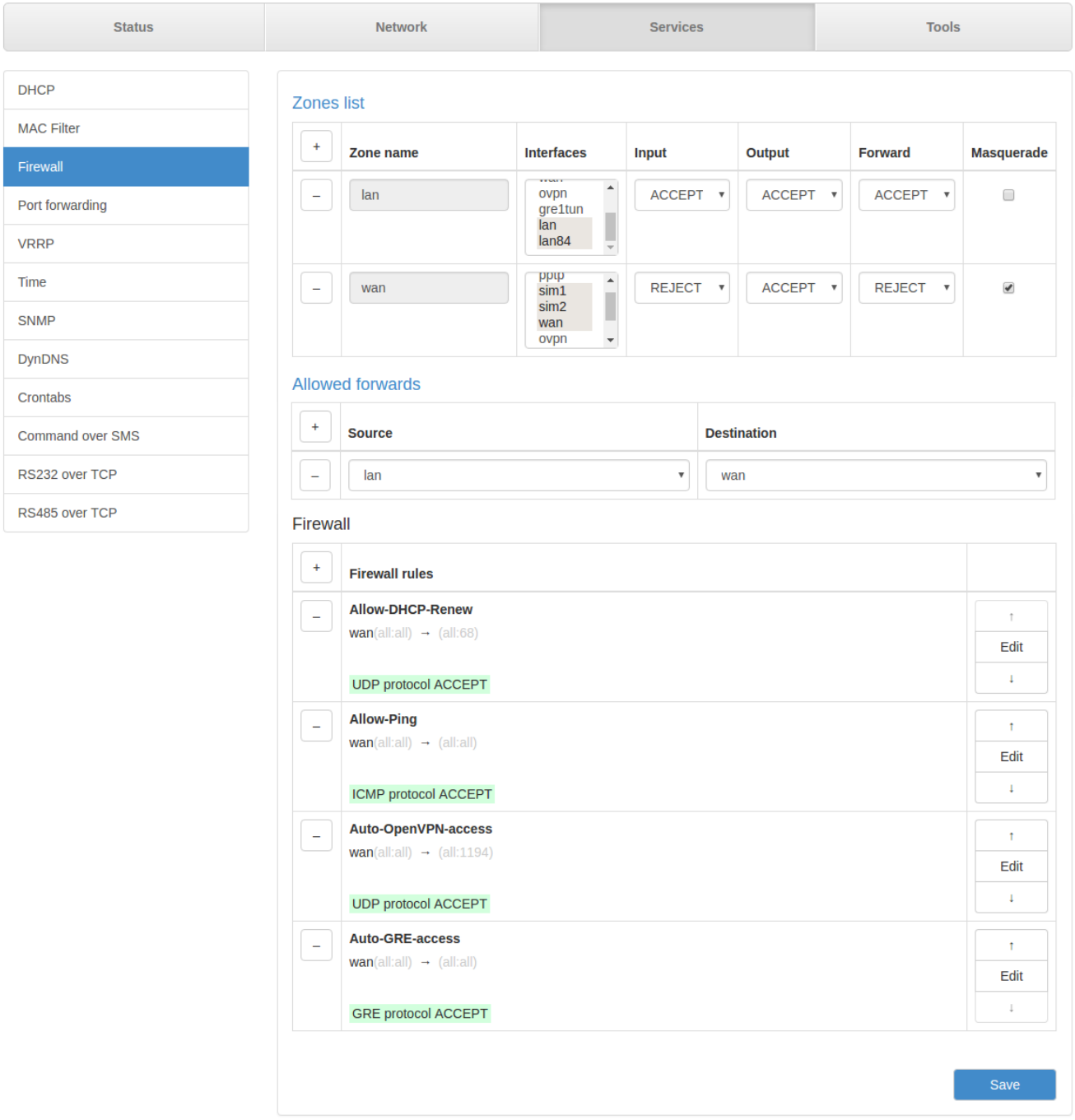

Рис. 5.29. Вкладка Services, раздел Firewall

Zone List

Подгруппа настроек Zone List отвечает за разбиение на зоны, в которых можно объединять интерфейсы между собой и назначать правила для входящего, исходящего и перенаправляемого трафика. Добавление правил осуществляется посредством кнопки + («плюс»), а удаление — кнопкой − («минус»). Настройки зон представлены в таблице 5.29.

Таблица 5.18. 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: **Accept** – принимать, **Reject** – отклонять, **Drop** – отбрасывать, **Notrack** – не отслеживать.
Output	Выбор действия для исходящего трафика: **Accept** – принимать, **Reject** – отклонять, **Drop** – отбрасывать, **Notrack** – не отслеживать.
Forward	Выбор действия для перенаправляемого трафика: **Accept** – принимать, **Reject** – отклонять, **Drop** – отбрасывать, **Notrack** – не отслеживать.
Masquerade	Включение/выключение маскировки трафика, то есть работы службы NAT

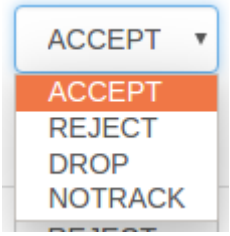

Рис. 5.30. Вариант выбора действий для трафика

Варианты действий для пакетов (поля **Input**, **Output**, **Forward**):

- **Accept** —пакеты трафика будут приниматься и обрабатываться через межсетевой экран;
- **Reject** — пакеты трафика будут отклоняться, с ответом;
- **Drop** — пакеты трафика будут отклоняться, без ответа;
- **Notrack** — пакеты трафика будут приниматься, без обработки межсетевым экраном (соединение не отслеживается).

Allowed Forwards

Подгруппа настроек Allowed Forwards отвечает за контроль трафика между зонами, которые создаются в подгруппе Zone List. Можно настроить перенаправление трафика от одного интерфейса к другому, если распределить эти интерфейсы в различные зоны. Например, в настройках на рисунке 5.30 в зону **LAN** входят интерфейсы LAN, LAN84, а в зону **WAN** – SIM1, SIM2, WAN. Правило «**LAN→WAN**» означает, что трафик с интерфейсов LAN, LAN84 (локальные порты) разрешено перенаправлять на WAN-порт и 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 5.31.

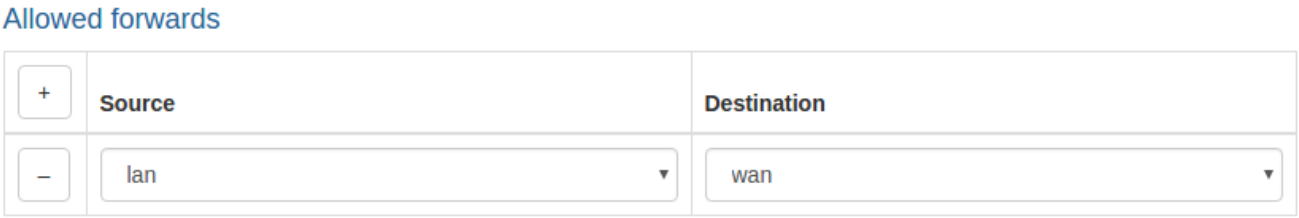

Рис. 5.31. Настройки Allowed Forwards

Таблица 5.19. Настройки правил для направлений

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

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 – «Accept» (принимать и обрабатывать).

Добавление правил осуществляется посредством кнопки + («плюс»), а удаление — кнопкой – («минус»). Для редактирования правил используется кнопка «Edit» напротив соответствующего правила (см. рисунок 5.33 и таблицу 5.20). Изменение приоритета правил, то есть положение в очереди выполнения, где сначала выполняются «верхние» правила, осуществляется посредством кнопок ↑ («вверх») и ↓ («вниз»).

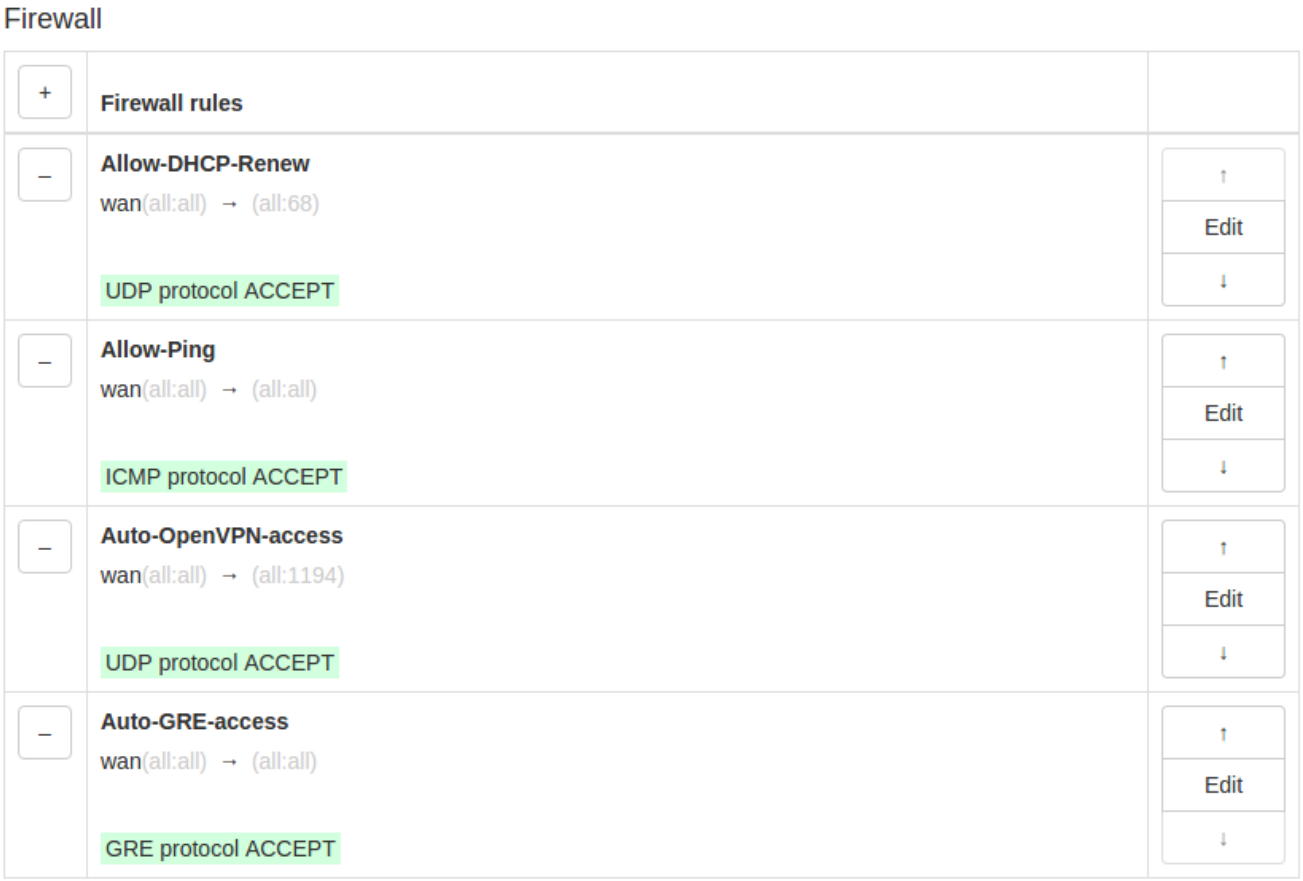

Рис. 5.32. Настройки Firewall

По умолчанию роутер R4 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. рисунок 5.33.

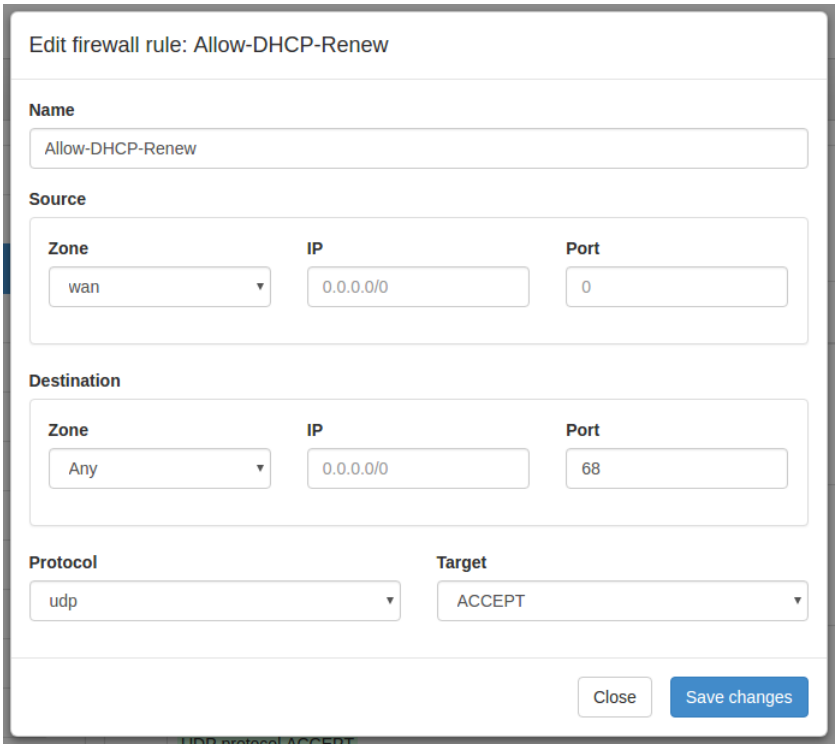

Рис. 5.33. Редактирование правила Firewall

Таблица 5.20. 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. **Any** – любая зона
IP	Ввод диапазона IP-адресов, на которые будет распространятся 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: **Accept** – принимать, **Reject** – отклонять, **Drop** – отбрасывать, **Notrack** – не отслеживать (подробнее см. в разделе 5.3.3, подразделе Zone List)

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

5.3.4. Port Forwarding

Раздел Port Forwarding на вкладке Services предназначен для настройки проброса портов со стороны WAN-интерфейса на локальные порты роутера. На рисунке 5.34 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!

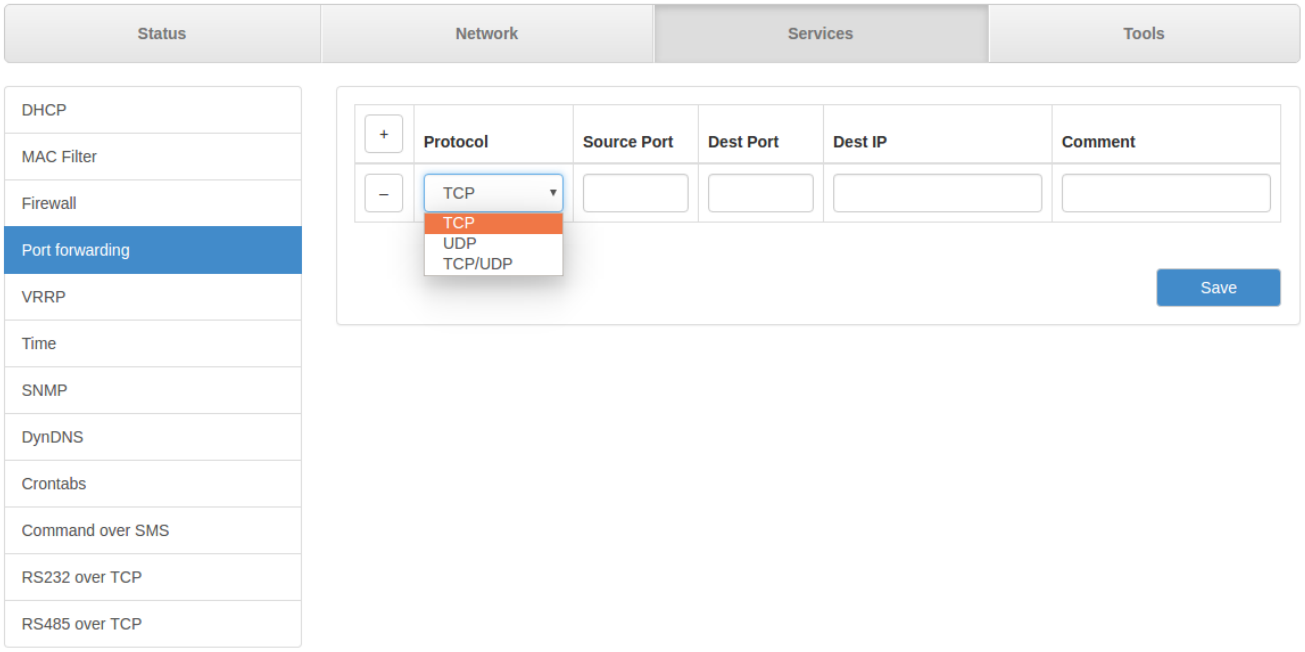

Рис. 5.34. Вкладка Services, раздел Port Forwarding

Таблица 5.21. Настройки правил проброса портов

Поле	Описание
Protocol	Выбор протокола, на который будет распространяться правило: **TCP**, **UDP** или **TCP/UDP** (оба протокола)
Source 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

5.3.5. 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 рисунке 5.35 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!

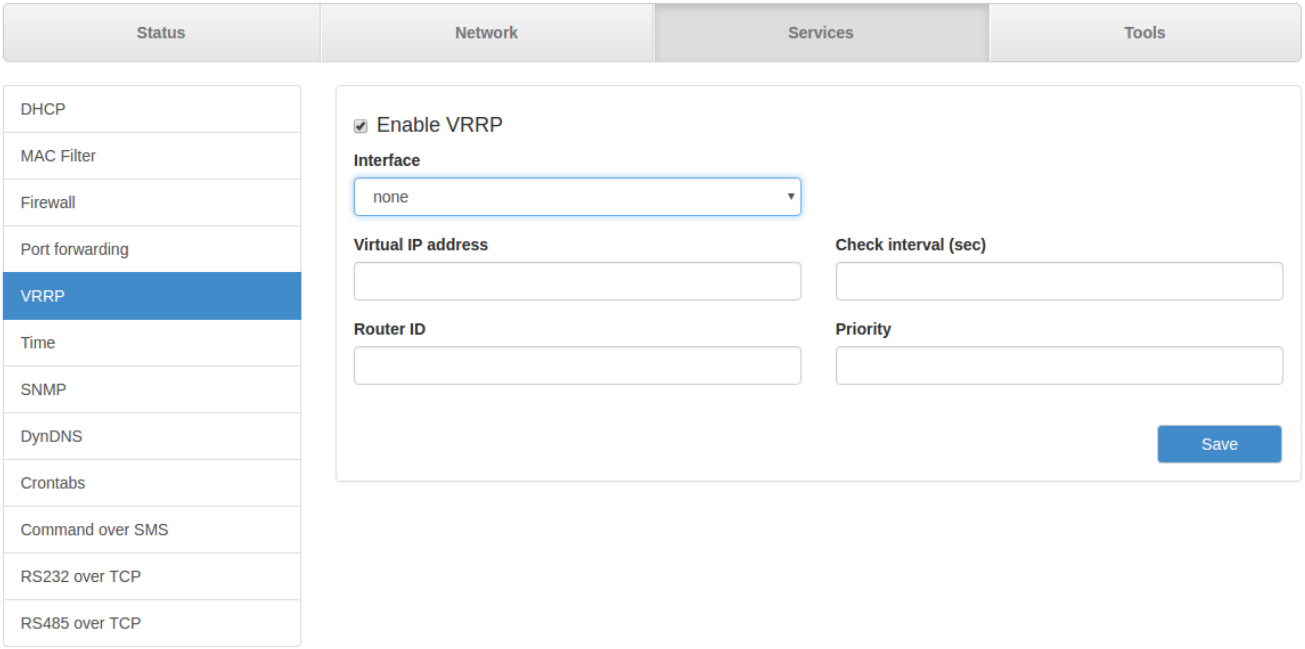

Рис. 5.35. Вкладка Services, раздел VRRP

Чтобы включить VRRP, поставьте галочку напротив **Enable VRRP** и задайте соответствующие настройки (см. таблицу 5.22).

Таблица 5.22. Настройки правил проброса портов

Поле	Описание
Interface	Выбор интерфейса, через который будет работать VRRP. **None** – ничего не использовать
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)

5.3.6. 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 рисунке 5.36 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!

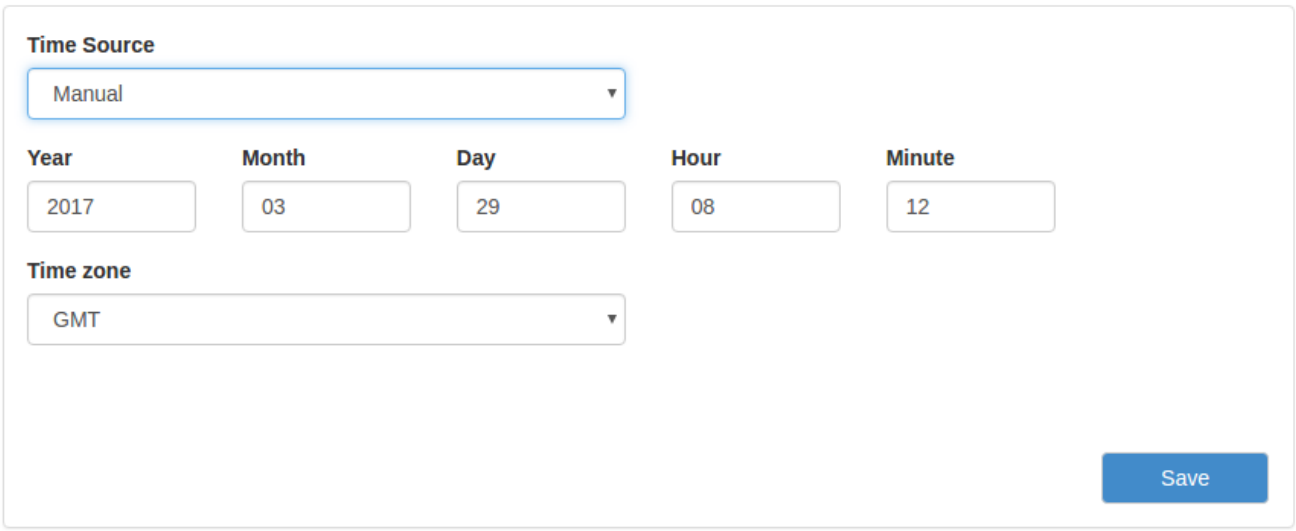

Рис. 5.36. Настройка времени в ручном режиме

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 рисунке 5.37 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!

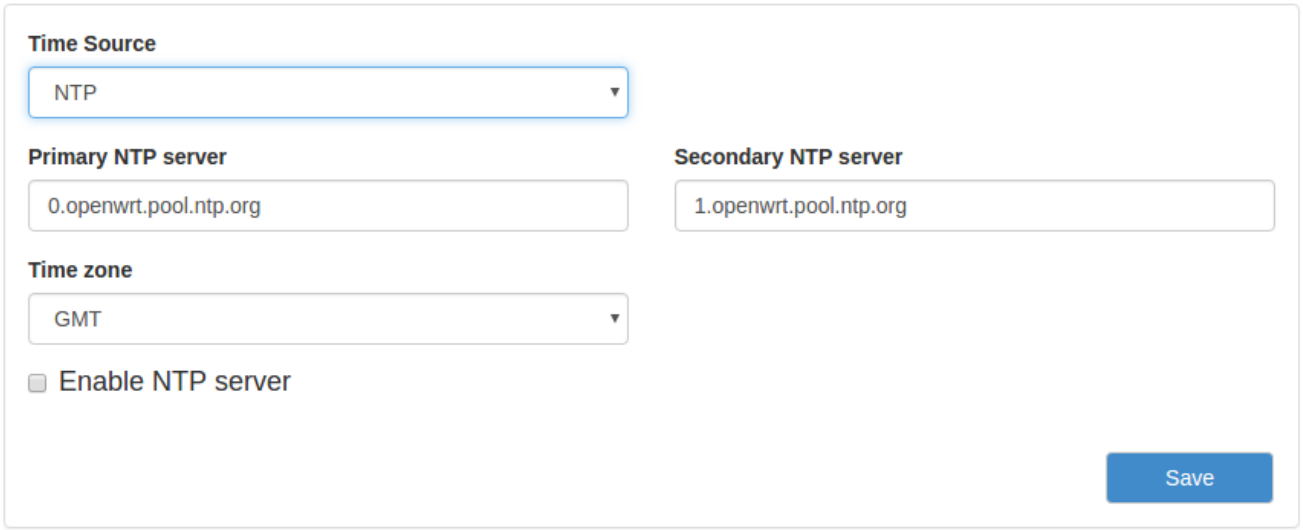

Рис. 5.37. Настройка времени в автоматическом режиме

5.3.7. 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 рисунках 5.38 и 5.39 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!

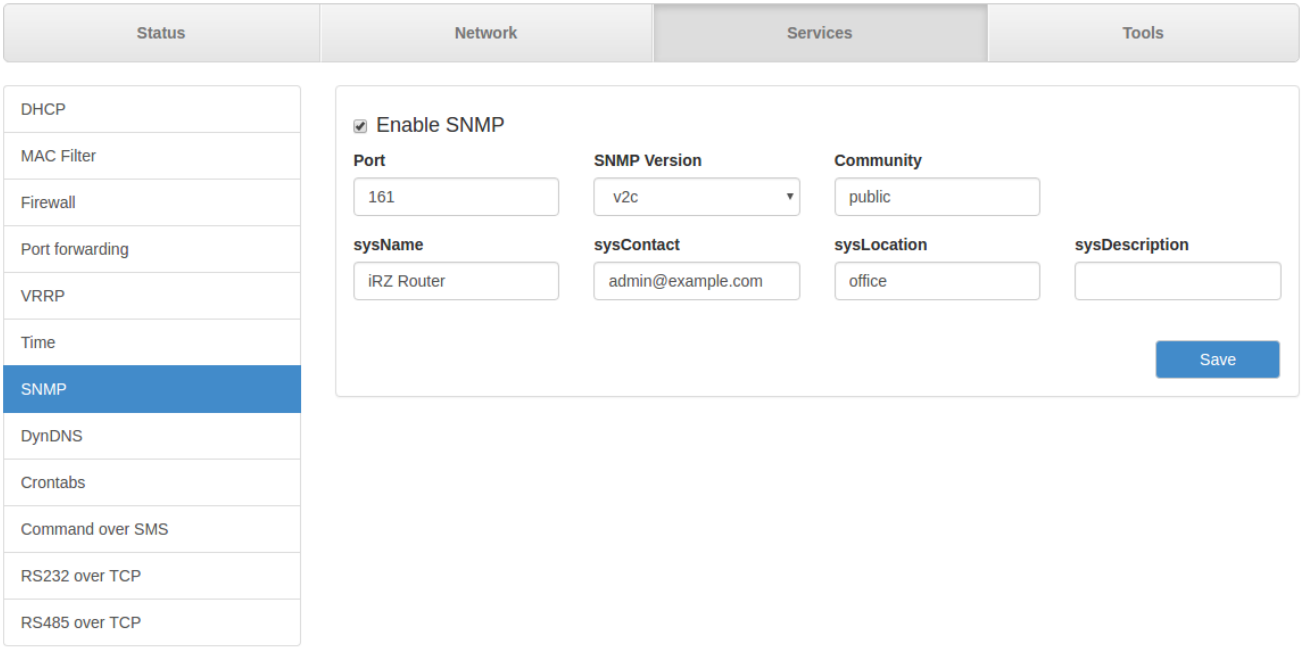

Рис. 5.38. Вкладка Services, раздел SNMP (v2c)

Чтобы включить SNMP, поставьте галочку напротив **Enable SNMP**, а затем введите соответствующие настройки (см. таблицу 5.23).

Таблица 5.23. 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: **v2c**, **v3**
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: ▪ Noauth – авторизация на устройстве не установлена; ▪ Auth – установлена авторизация; ▪ Priv – установлена авторизация и шифрование данных при передаче по протоколу.

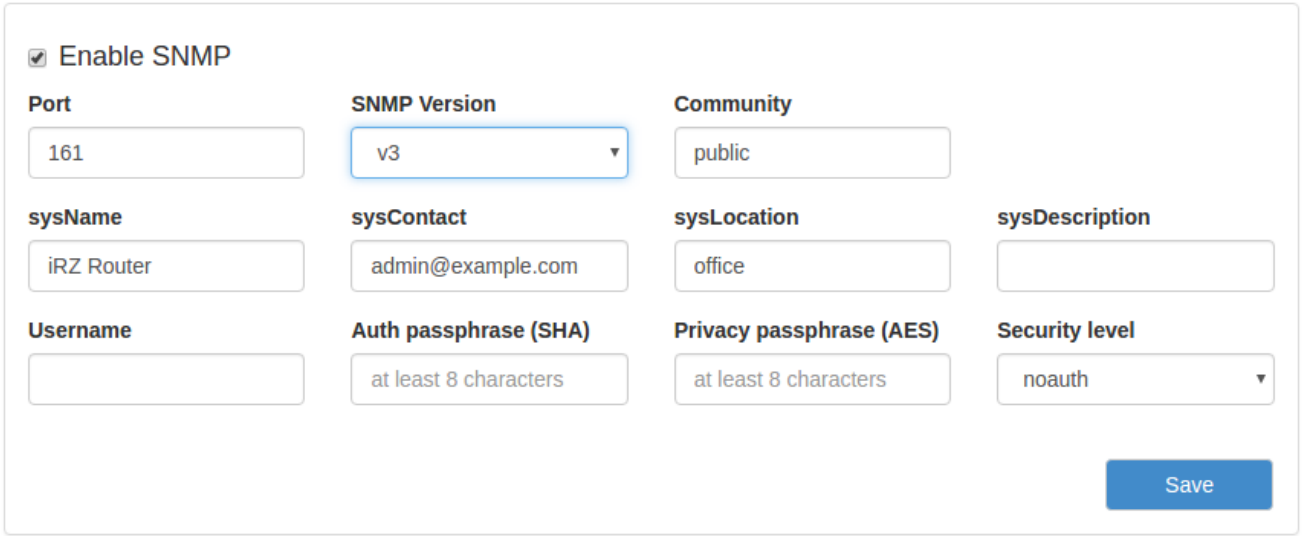

Рис. 5.39. Вкладка Services, раздел SNMP (v3)

5.3.8. 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 рисунке 5.40 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!

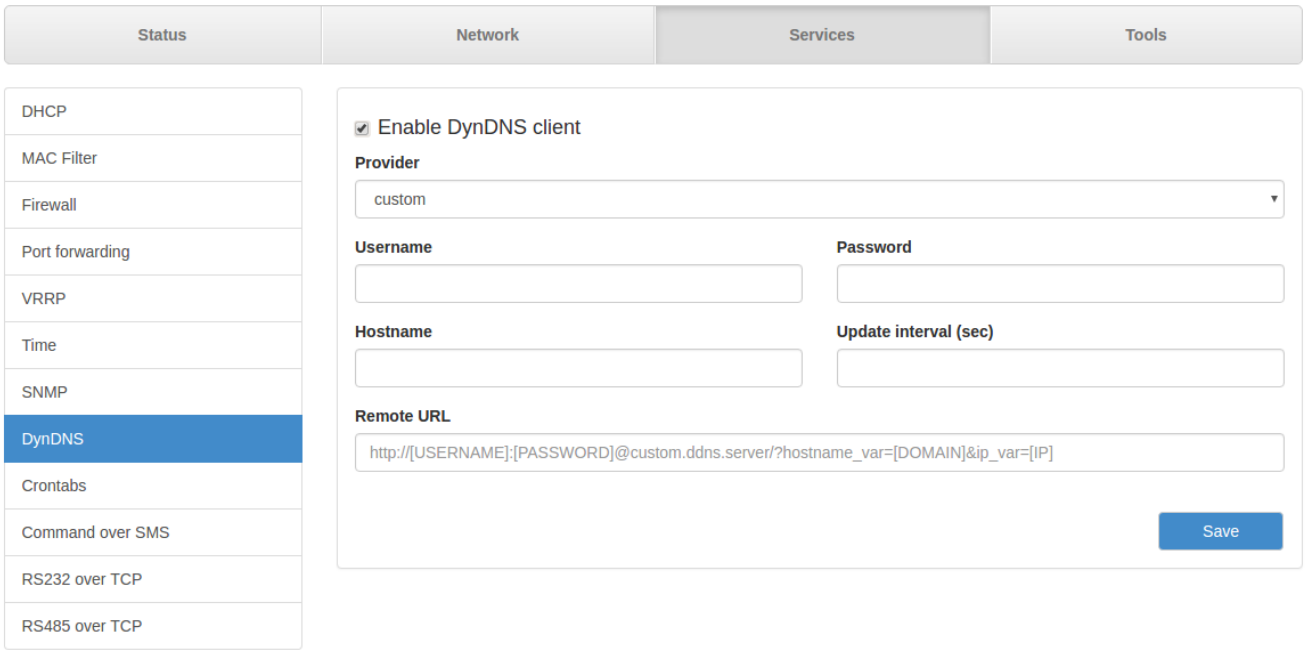

Рис. 5.40. Вкладка Services, раздел DynDNS

Чтобы включить DynDNS, поставьте галочку напротив **Enable DynDNS client** и настройте соответствующие параметры (см. таблицу 5.24).

Таблица 5.24. Настройки DynDNS

Поле	Описание
Provider	Выбор провайдера услуги динамического DNS (см. рис. 5.41). В роутерах iRZ предустановлены основные настройки для нескольких распространенных провайдеров. Для настройки собственного сервера, выберите **Custom** и пропишите необходимые настройки
Username	Имя пользователя для авторизации на сервере DynDNS
Password	Пароль для авторизации на сервере DynDNS
Hostname	Имя хоста
Update Interval (sec)	Интервал в секундах, через который будет обновляться информация на сервера
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 четыре предустановленных распространенных сервиса, см. рисунок 5.51.

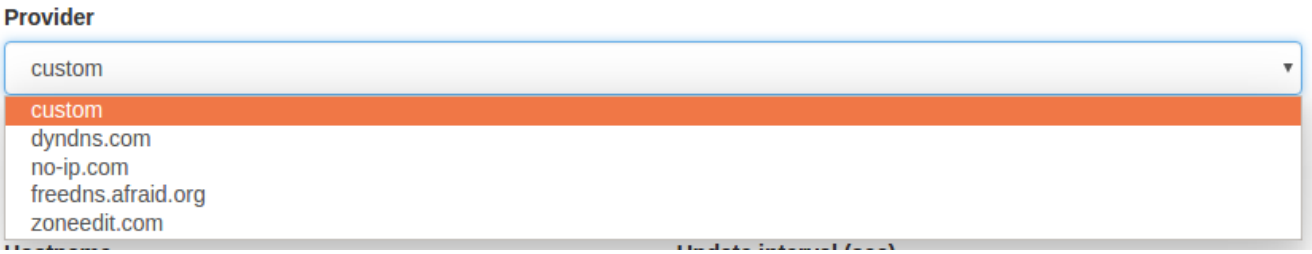

Рис. 5.41. Сервера DNS

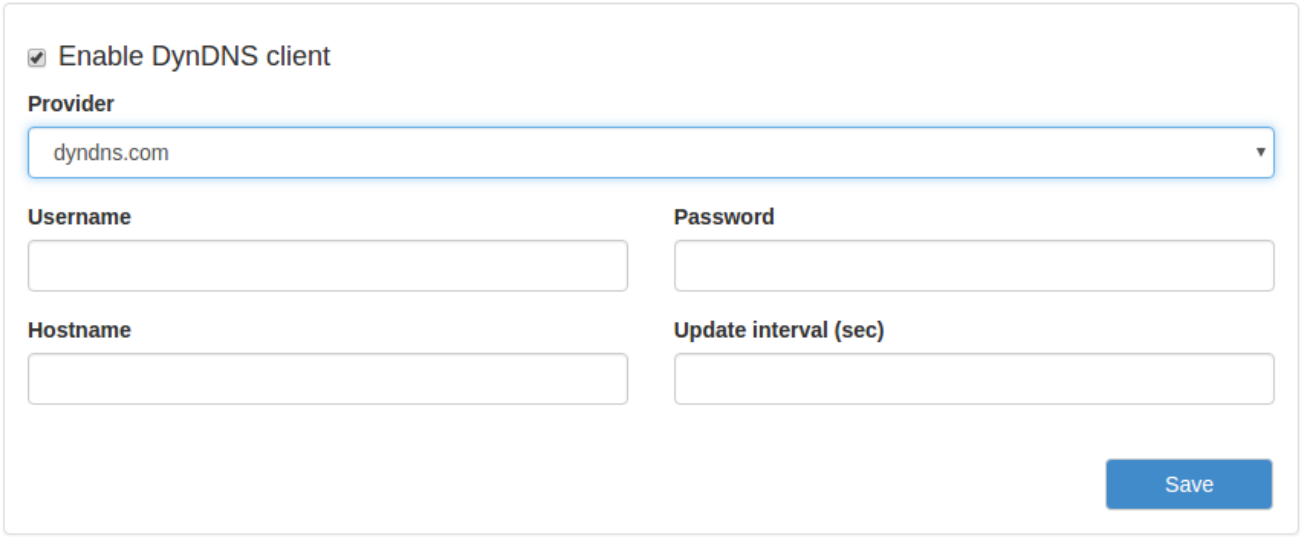

Рис. 5.42. Пример настройки DNS предустановленного провайдера

5.3.9. 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 воскресение — это либо «0», либо «7»), а сама команда указывается в поле **Command**. На рисунке 5.43 представлен пример поля для заполнения.

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

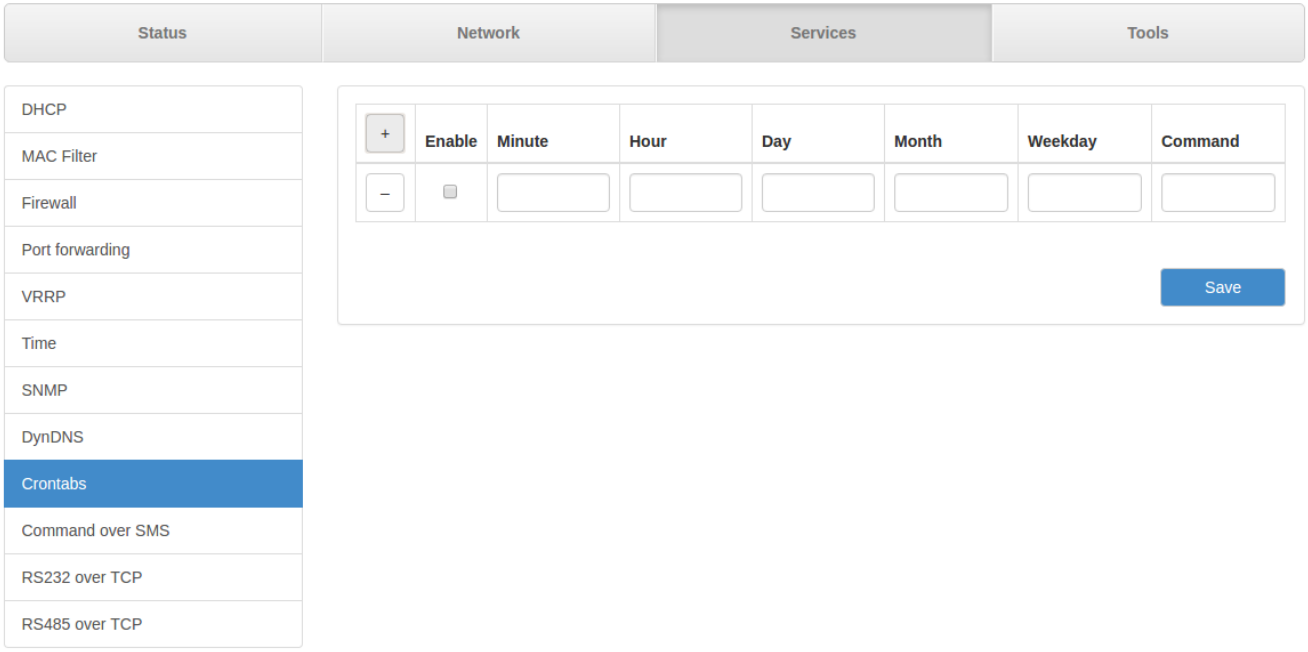

Рис. 5.43. Вкладка Services, раздел Crontabs

5.3.10. 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) ash. Для скриптов и команд необходимо указывать их полный путь, как это сделано на рисунке 5.44.

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 рисунке 5.44 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 выполниться 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 выполниться команда из поля **Command**, той строки, в которой ключевые фразы из поля **Message** и SMS-сообщения совпадают.

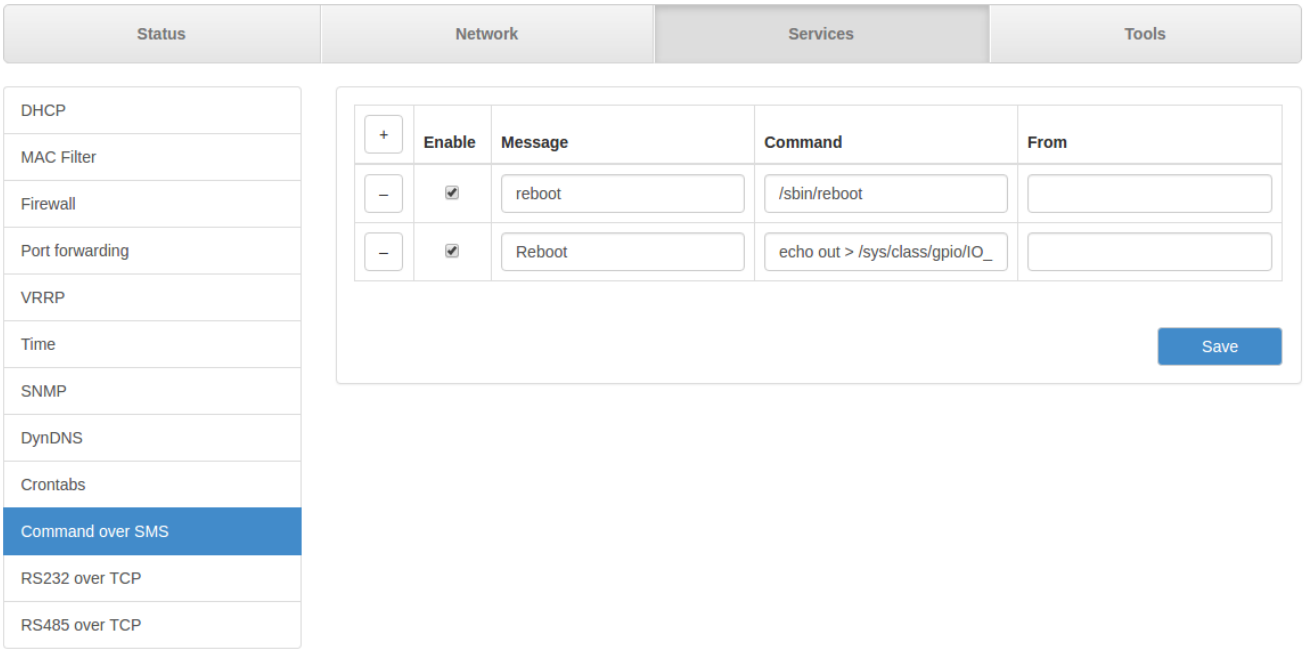

Рис. 5.44. Вкладка Services, раздел Commands over SMS

5.3.11. 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 отсылает 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 рисунке 5.45 представлен пример настройки роутера с портами RS232 в режиме сервера.

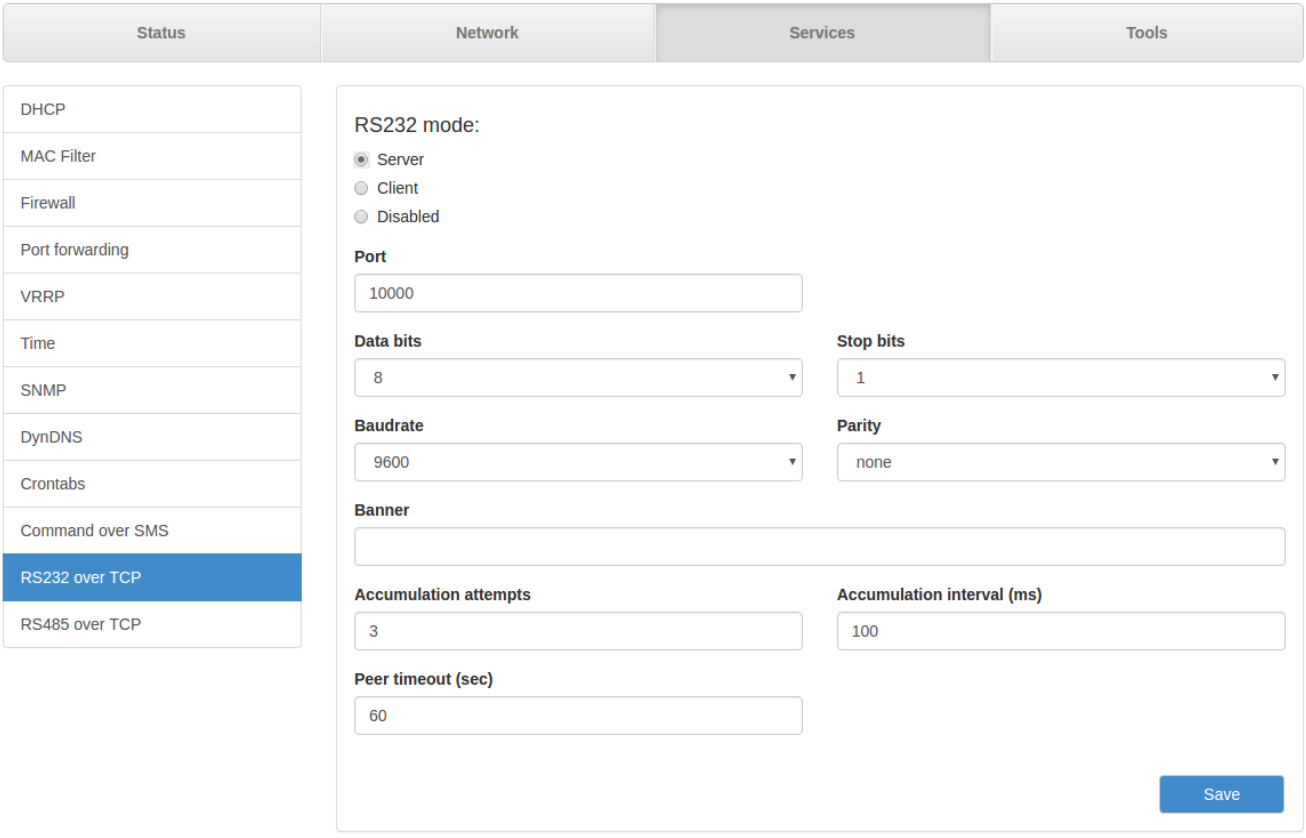

Рис. 5.45. Вкладка Services, раздел RS232 over TCP (режим сервера)

На рисунке 5.46 представлен пример настройки роутера с портами RS232 в режиме клиента.

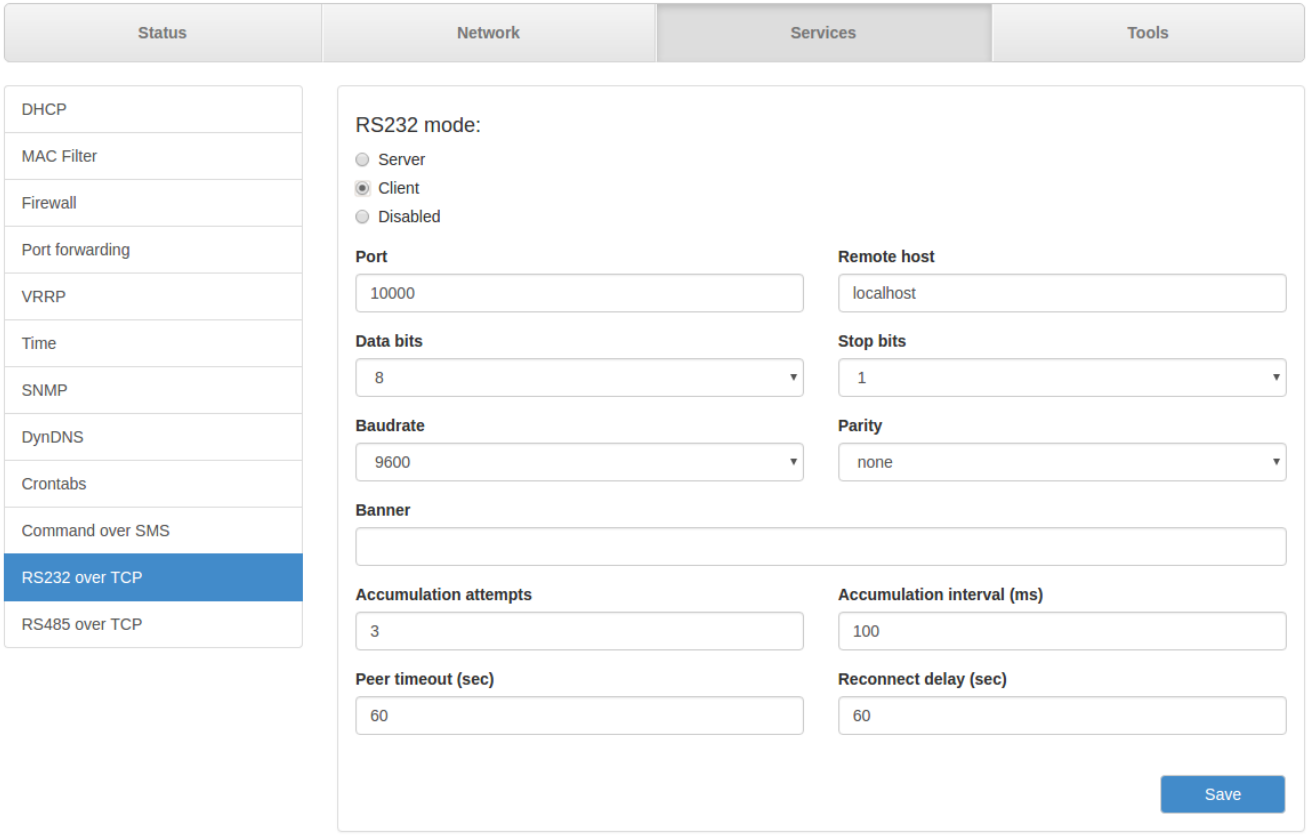

Рис. 5.46. Вкладка Services, раздел RS232 over TCP (режим клиента)

Таблица 5.25. Настройки портов через TCP (C – клиент, S – сервер)

Поле	Режим	Описание
Port	C, S	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	Количество бит блока, используемых при передаче данных: **7**, **8**
Stop Bits	C, S	Количество стоп-бит блока, используемые для определения конца блока: **1**, **2**
Baudrate	C, S	Скорость передачи данных через порт, в бод
Parity	C, S	Режим контроля четности бит в передаваемых блоках: **None** – без проверки, **Odd** – проверка на нечетность, **Even** – 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. Раздел «Tools»

5.4.1. 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 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+, поставьте галочку напротив **Enable TACACS+ for SSH**. На рисунке 5.47 представлен пример настройки доступа к устройству.

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

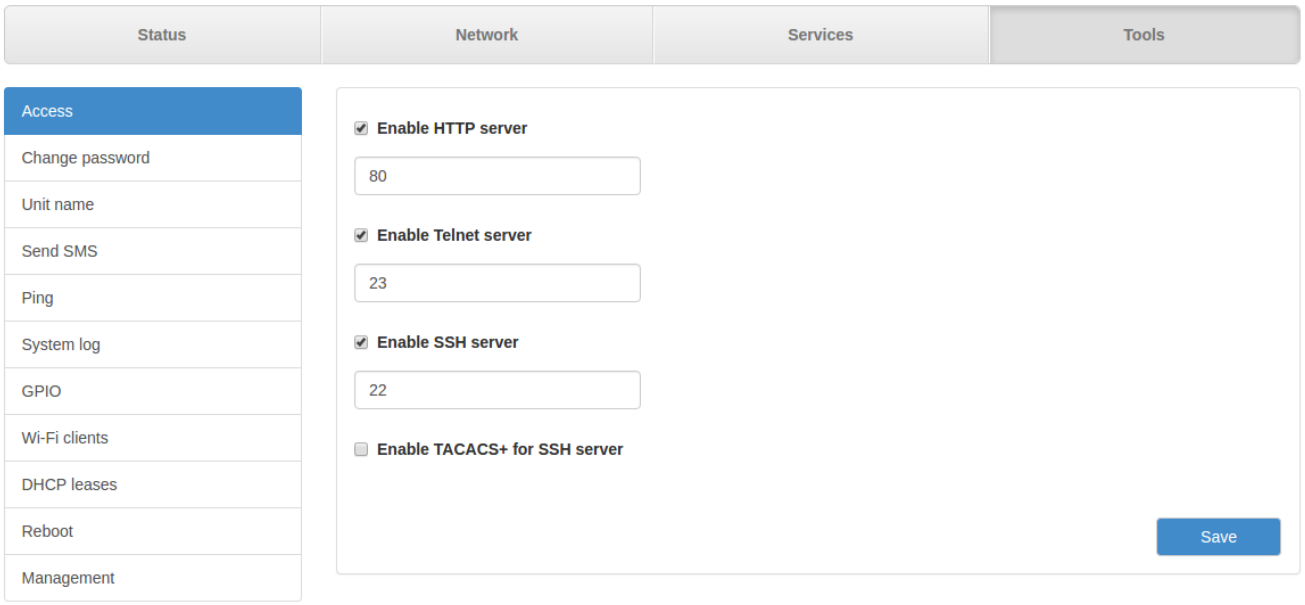

Рис. 5.47. Вкладка Tools, раздел Access

5.4.2. 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 рисунке 5.48 представлен пример полей для заполнения.

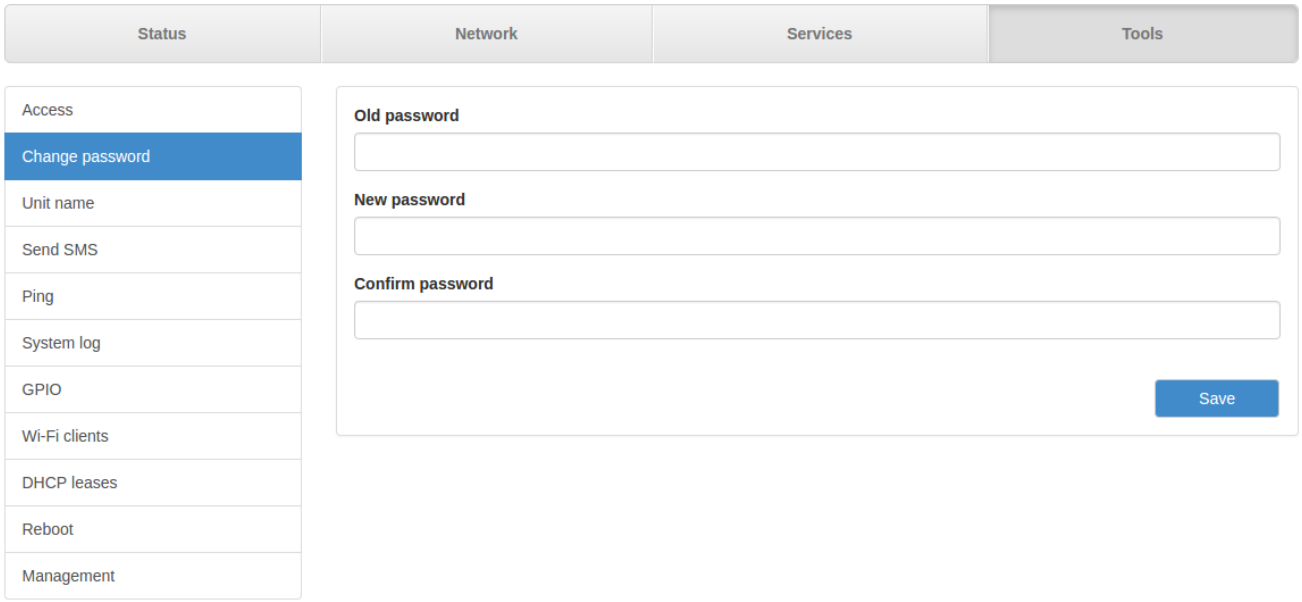

Рис. 5.48. Вкладка Tools, раздел Change Password

5.4.3. 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 рисунке 5.49 представлен пример полей для заполнения.

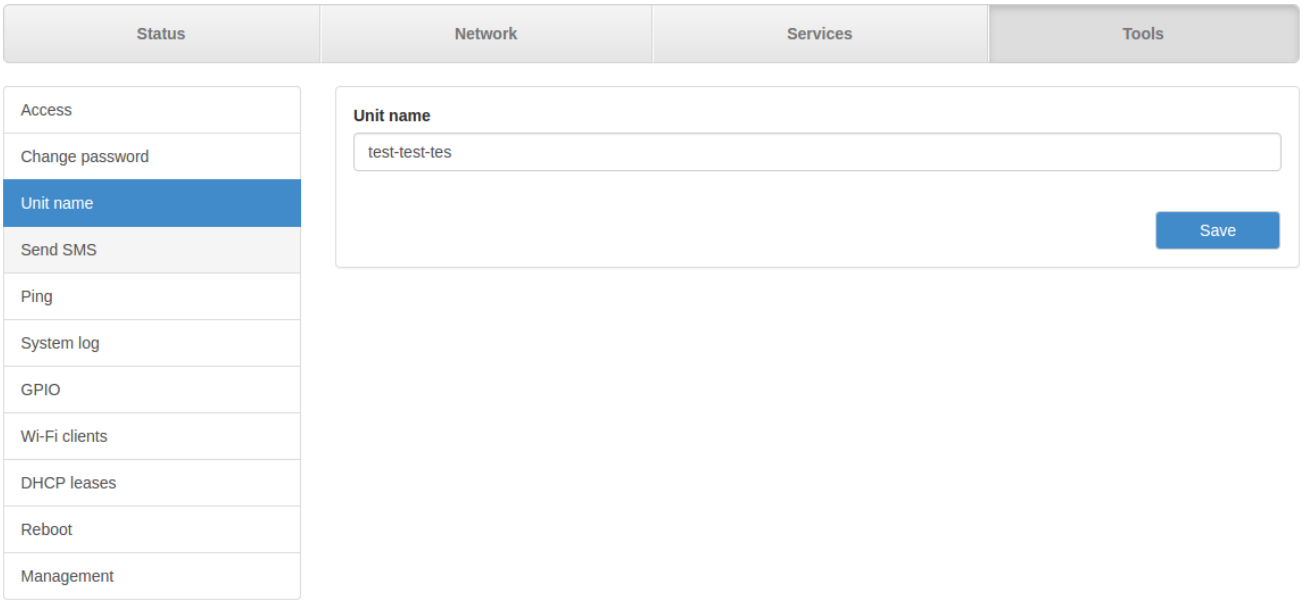

Рис. 5.49. Вкладка Tools, раздел Unit Name

5.4.4. 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 рисунке 5.50 представлен пример полей для заполнения.

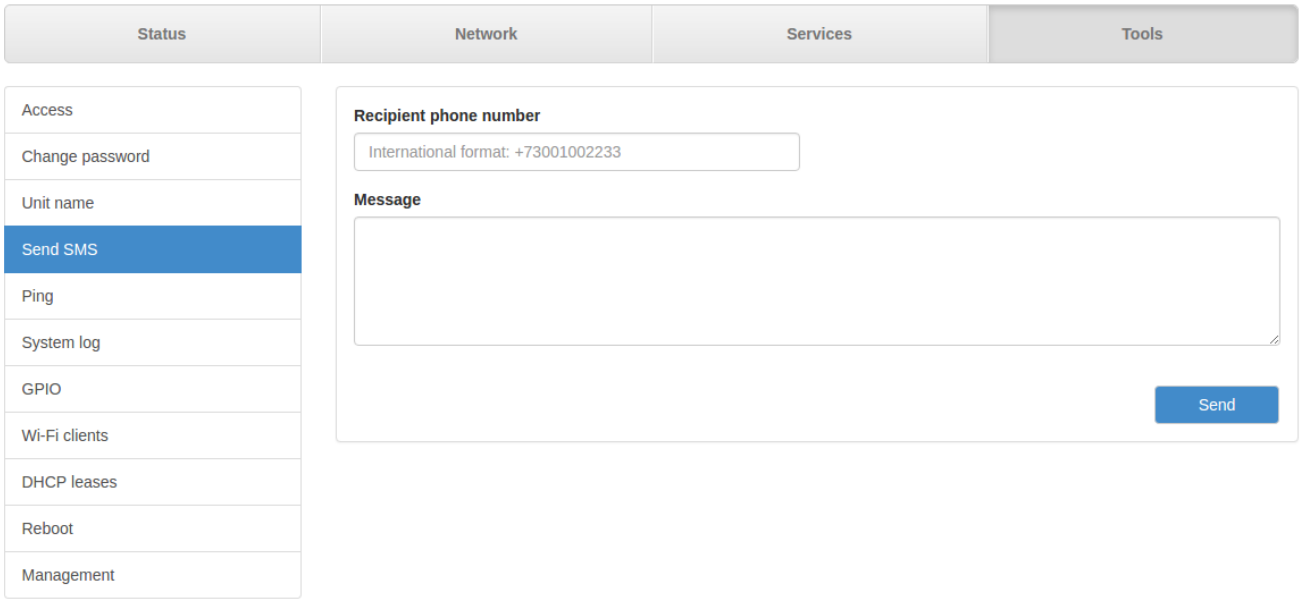

Рис. 5.50. Вкладка Tools, раздел Send SMS

5.4.5. 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 рисунке 5.51 представлен пример полей для заполнения.

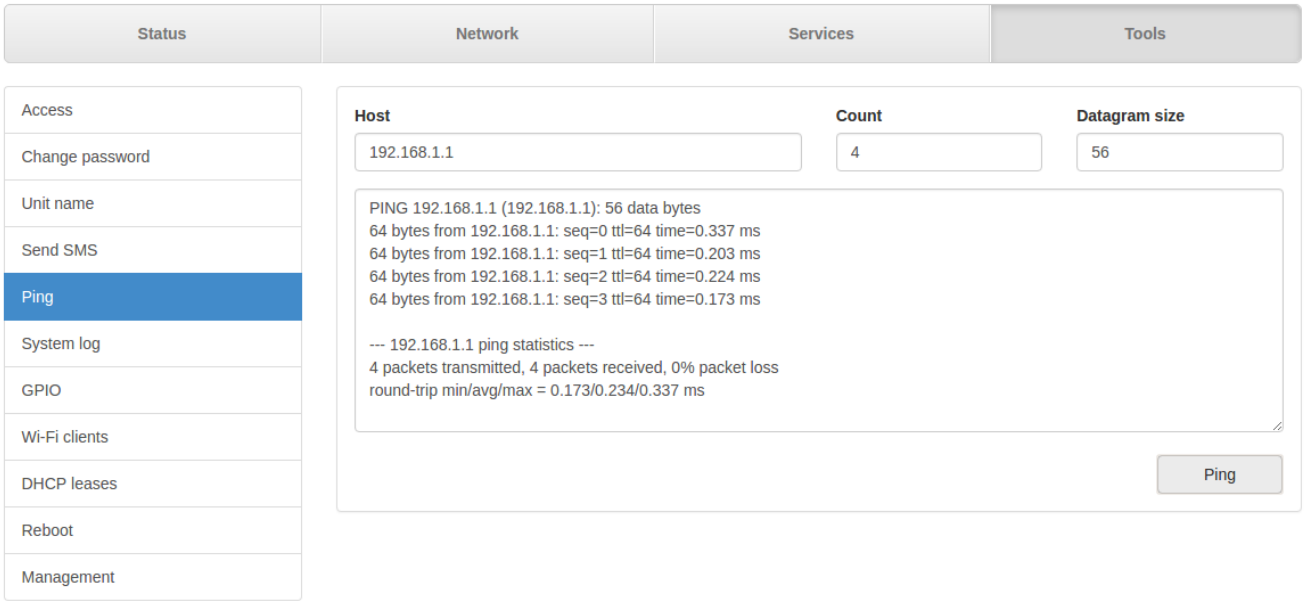

Рис. 5.51. Вкладка Tools, раздел Ping

5.4.6. 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.

Сам системный журнал устройства можно увидеть в центральном окне на рисунке 5.52. С помощью кнопки **System Report** можно получить файл с полным логом устройства, включающим в себя логи работы и все его настройки.

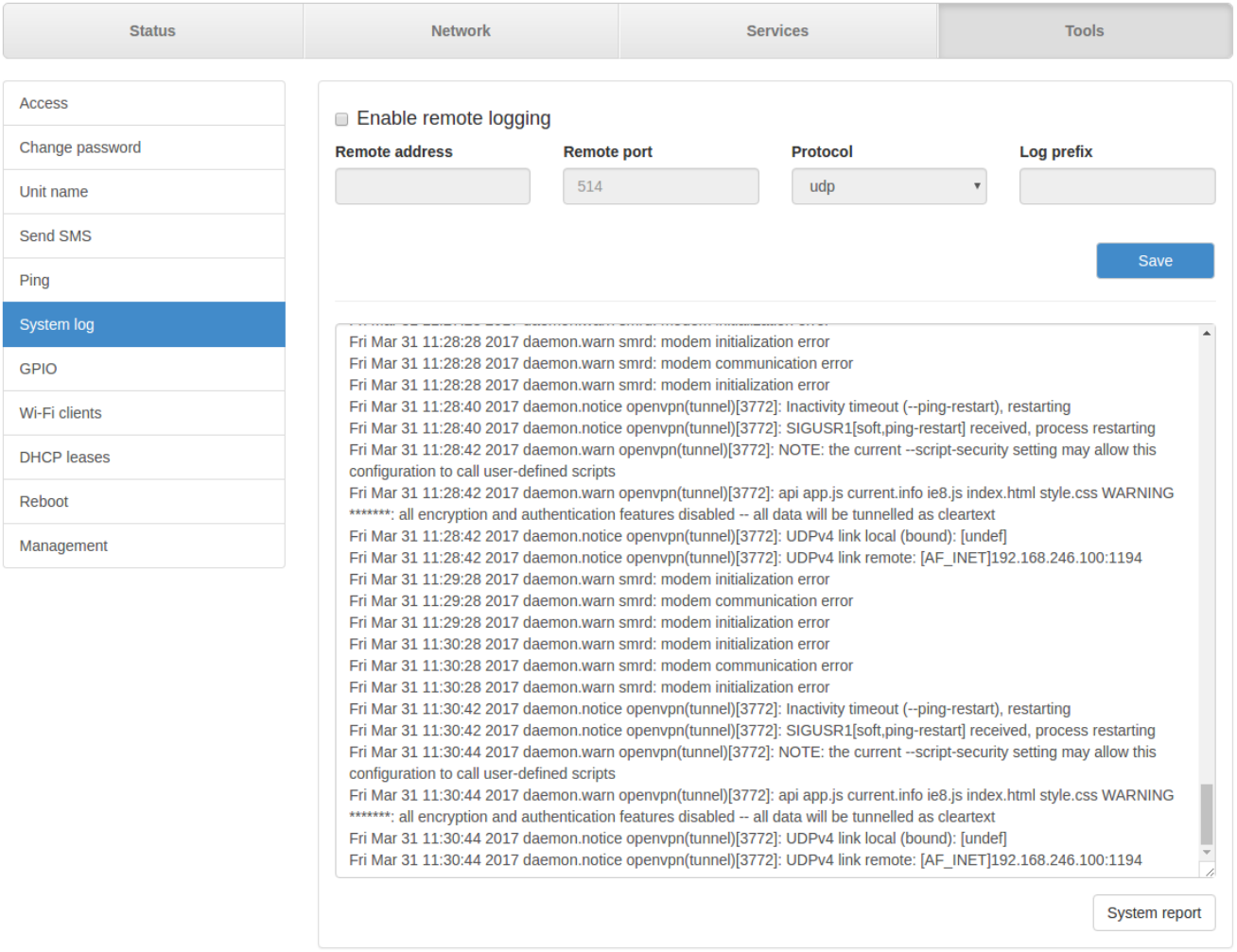

Рис. 5.52. Вкладка Tools, раздел System Log

5.4.7. 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 рисунке 5.53 представлен пример настройки GPIO.

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

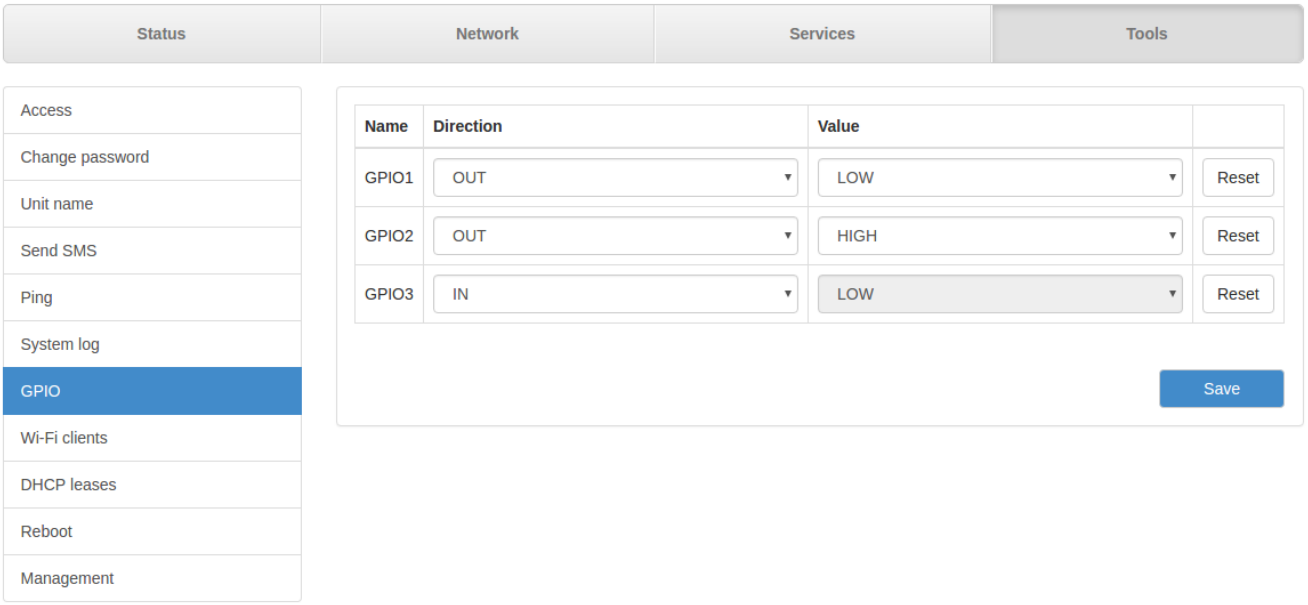

Рис. 5.53. Вкладка Tools, раздел GPIO

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:

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 5.26. Настройки портов GPIO

Поле	Описание
Name	Имена входов/выходов (также см. руководство по эксплуатации)
Direction	Выбор направления работы: **IN** – работает, как вход, **OUT** – выход
Value	Уровень выходного сигнала (только для выходов): **HIGH** – высокое напряжение, **LOW** – низкое
Reset	Сброс текущих настроек GPIO, и установка настроек по умолчанию

5.4.8. 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 рисунке 5.54 представлен пример страницы.

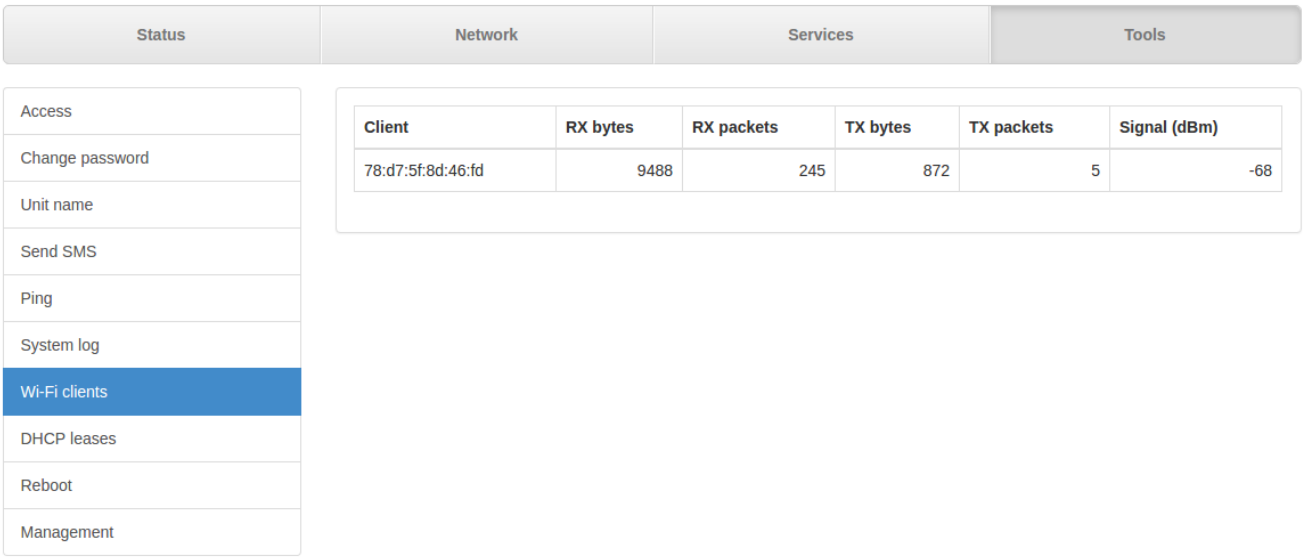

Рис. 5.54. Вкладка Tools, раздел Wi-Fi Clients (роутер с Wi-Fi-модулем)

Таблица 5.27. 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.

5.4.9. 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 рисунке 5.55 представлен пример страницы.

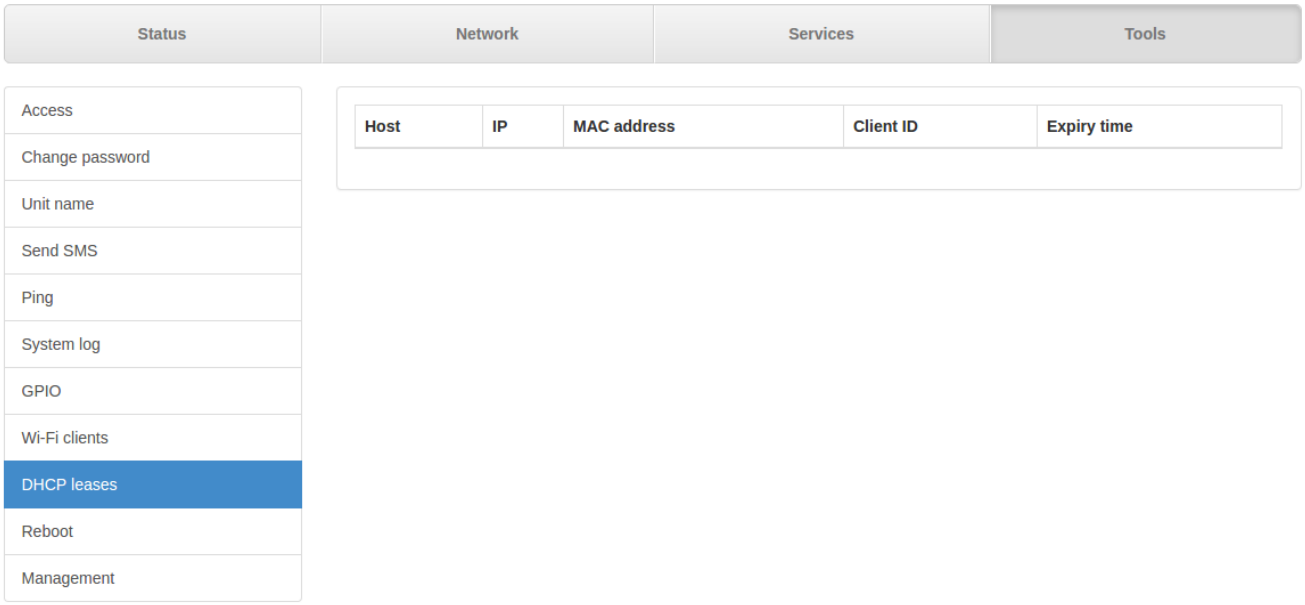

Рис. 5.55. Вкладка Tools, раздел DHCP Leases

Таблица 5.28. 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

5.4.10. Reboot

Раздел Reboot на вкладке Tools предназначен для перезагрузки устройства или сброса в заводские настройки. На рисунке 5.56 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**.

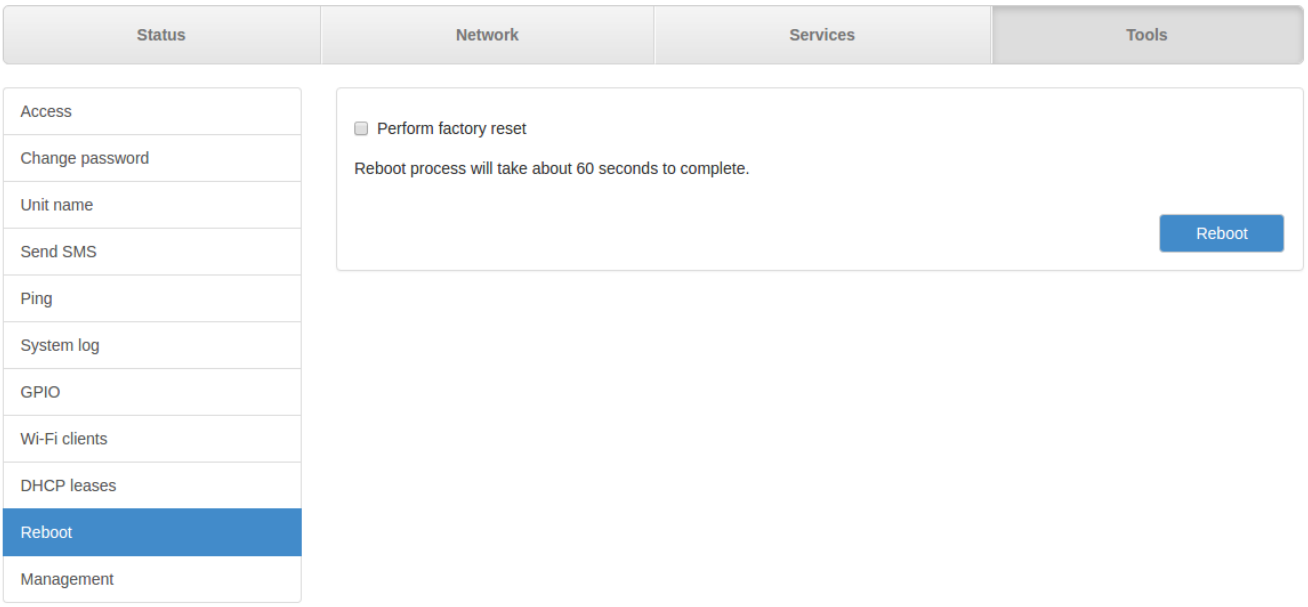

Рис. 5.56. Вкладка Tools, раздел Reboot

5.4.11. Management

Раздел Management на вкладке Tools предназначен для управления настройками роутера и обновлением внутреннего ПО (прошивок). На рисунке 5.57 представлен пример страницы.

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 рисунке 5.68.

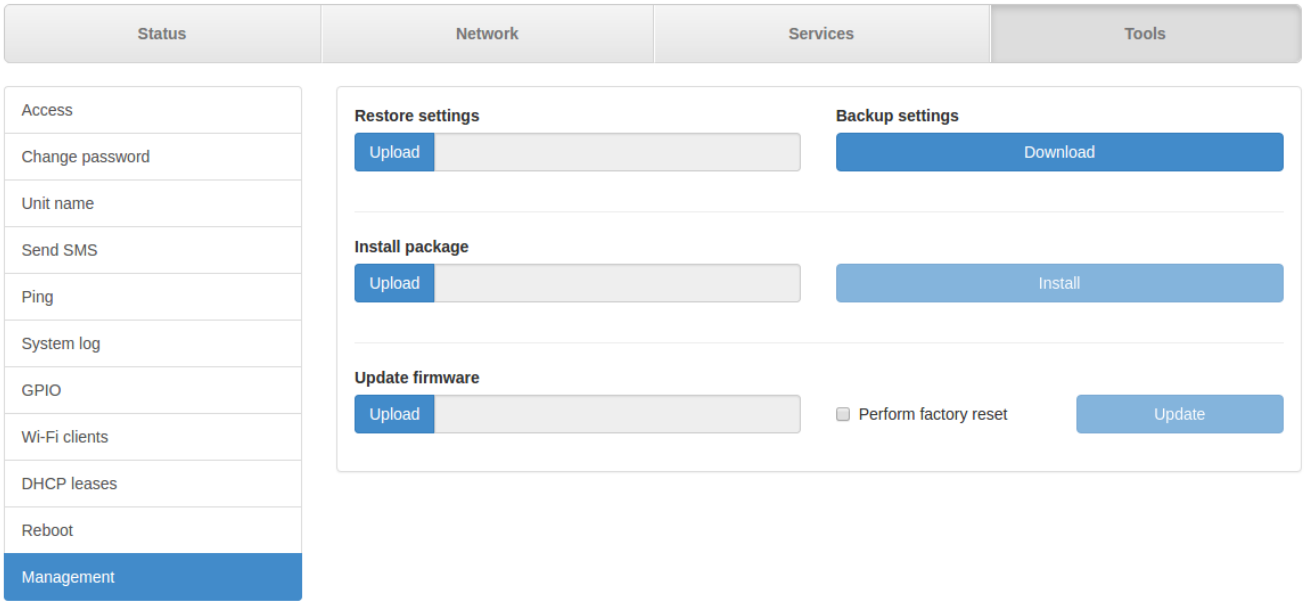

Рис. 5.57. Вкладка Tools, раздел Management

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 прошивок, документации и сопутствующего программного обеспечения можно получить при обращении по следующим контактам.

Санкт-Петербург	
сайт компании в Интернете:	www.radiofid.ru
тел. в Санкт-Петербурге:	+7 (812) 318 18 19
e-mail:	support@radiofid.ru

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
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

lsof

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