Руководство

по настройке роутеров iRZ

Содержание

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.

Дата публикации	Изменения
12.03.2019	Основной документ
03.06.2019	Предупреждение о подаче напряжения на GPIO
20.12.2019	Добавлен Mobile APN Profiles, Server Modbus to RTU, обновлены все разделы документа
06.04.2020	Изменен раздел Serial Ports
18.06.2021	Переход на встроенное ПО версии v20.1, изменения во всех разделах, переход на новое ядро, создание HTTPS сертификатов на устройстве
01.09.2021	Переход на встроенное ПО версии v20.2
27.01.2022	Переход на встроенное ПО версии v20.3, изменения в разделах **Tools**: Wireless Network, iRZ Link Client, Mobile Interfaces; **Services**: SNMP, Port Forwarding, Firewall, добавлен Application Layer Gateway
26.02.2022	Переход на встроенное ПО версии v20.3.1
14.07.2022	Переход на встроенное ПО версии v20.4
08.08.2022	Изменен раздел Network
07.10.2022	Переход на встроенное ПО версии v20.4.3
18.10.2022	Изменен раздел Temperature
29.11.2022	Переход на встроенное ПО версии v20.5, изменения в разделах **Services**: Firewall, Queues
28.02.2023	Переход на встроенное ПО версии v20.6, изменения в разделах **Status, GPIO, Network, SNMP, Serial Ports**, добавлен раздел **Zabbix Agent**
07.06.2023	Переход на встроенное ПО версии v20.7, изменения в разделе **Network** - Wireless Network
28.06.2023	Переход на встроенное ПО версии v20.7.1

1.2. Версия встроенного обеспечения

Актуальная (текущая) версия встроенного ПО

- роутеры серии R0: R0-v20.7.1 (2023-06-28)
- роутеры серии R2: R2-v20.7.1 (2023-06-28)
- роутеры серии R4: R4-v20.7.1 (2023-06-28)
- роутеры серии R50: R50-v20.7.1 (2023-06-28)

1.3. Предупреждения

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

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.

1.4. Термины и сокращения

Роутер — маршрутизатор;

2G — общее название группы стандартов сотовой связи GPRS, EDGE;

3G — общее название группы стандартов сотовой связи UMTS,HSDPA, HSUPA, HSPA+;

4G — общее название группы стандартов сотовой связи LTE;

Сервер — этот термин может быть использован в качестве обозначения для:

- серверной части программного пакета используемого в вычислительном комплексе;
- роли компонента, либо объекта в структурно-функциональной схеме технического решения, развёртываемого с использованием роутера;
- компьютера, предоставляющего те или иные сервисы (сетевые службы, службы обработки и хранения данных и прочие);

Внешний IP-адрес — IP-адрес в сети Интернет, предоставленный компанией-провайдером услуг связи в пользование клиенту на своём/его оборудовании для обеспечения возможности прямой связи с оборудованием клиента через сеть Интернет;

Фиксированный внешний IP-адрес — внешний IP-адрес, который не может измениться ни при каких условиях (смена типа оборудования клиента и др.) или событиях (переподключение к сети провайдера и др.); единственной возможностью сменить фиксированный IP-адрес является обращение в форме заявления к компании-провайдеру;

Аутентификация — процедура проверки подлинности пользователя/клиента/узла путём сравнения предоставленных им на момент подключения реквизитов с реквизитами, соотнесёнными с указанным именем пользователя/логином в базе данных;

Web-интерфейс роутера — средство управления, встроенное в роутер и обеспечивающее возможность контролировать и настраивать его функции, а также наблюдать за состоянием этих функций;

Удалённое устройство (удалённый узел) – устройство, территориально удалённое от места, либо объекта/узла, обсуждаемого в конкретно взятом контексте;

Локальная сеть — система, объединяющая несколько компьютеров в пределах одного помещения, здания или нескольких близко расположенных зданий одного предприятия. Для соединения компьютеров могут использоваться кабели, телефонные линии или беспроводные каналы;

Внешняя сеть (VLAN) — топологическая («виртуальная») локальная компьютерная сеть. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным членам группироваться вместе независимо от их физического местонахождения, даже если они не находятся в одной физической сети;

ИБП (UPS) — источник бесперебойного питания.

2. Способы управления роутером iRZ

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 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

Для доступа к настройкам роутера нужно выполнить действия, описанные ниже.

1. Откройте интернет-браузер и введите IP-адрес роутера в адресную строку.

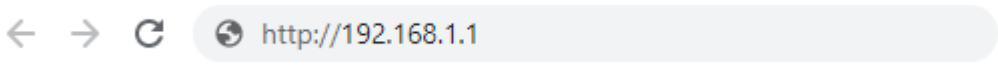


Рис. 1. Ввод IP-адреса роутера в адресную строку интернет-браузера

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

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**)

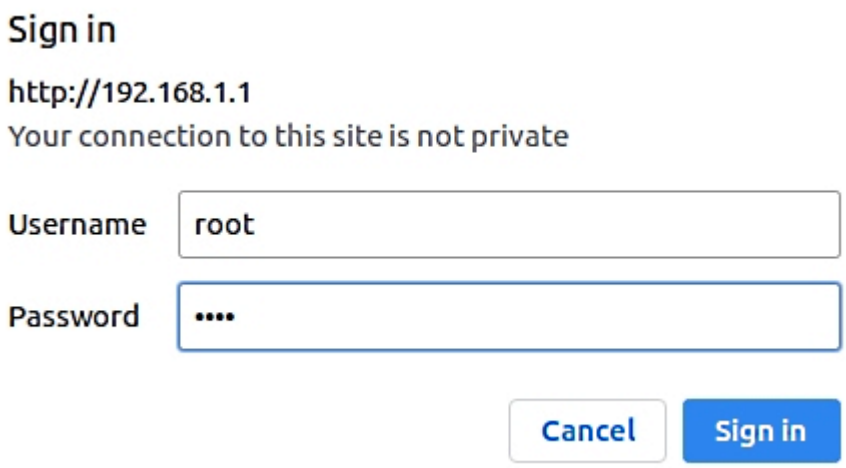


Рис. 2. Ввод логина и пароля для доступа к web-интерфейсу роутера

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.

4. Возвращение к заводским настройкам

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 **Reset** и удерживайте в течение 8 секунд. Роутер перезагрузится уже со сброшенными настройками.

Если настройки роутера после перезагрузки оказались не сброшены, возможно

1. вы удерживали кнопку не достаточно долго;
2. на вашем устройстве сломана кнопка;
3. прошивка вашего устройства давно не обновлялась - для старых версий прошивок кнопку **Reset** следует удерживать 20 секунд.

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

5. Web-интерфейс

5.1. Раздел "Status"

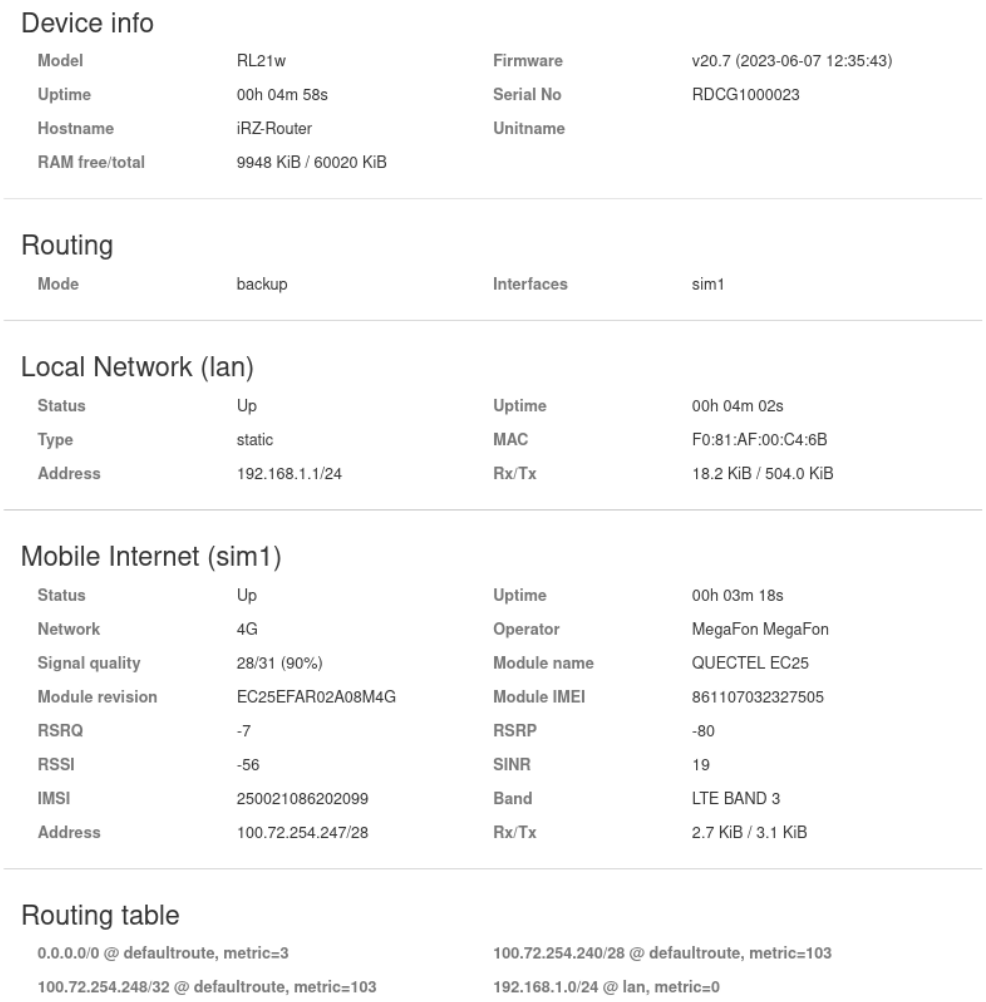


Рис. 3. Страница статуса

Страница **Status** содержит обобщённую информацию о состоянии устройства:

- модель роутера;
- время работы устройства после включения (uptime);
- тип GSM-связи, уровень GSM-сигнала;
- IP-адрес, скорость соединения и т.д.

Данная информация может быть полезна для быстрой диагностики устройства. Наличие и отсутствие отдельных полей зависит от модели и настроек роутера.

Device Info

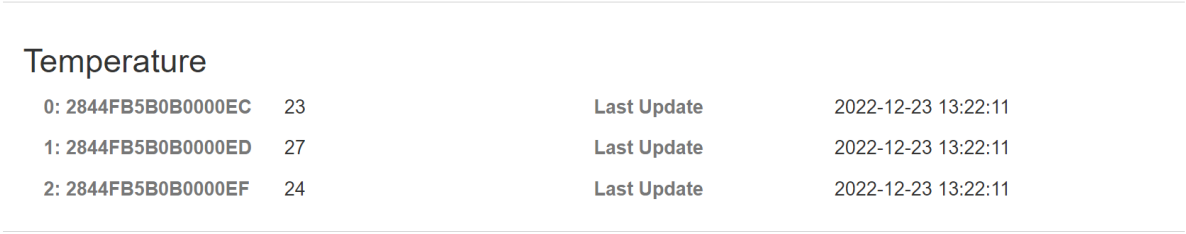
Основная информация об устройстве.

Таблица 2. Поля в разделе Device Info

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

Temperature

Информация от подключенных датчиков температуры.



Раздел содержит:

- Порядковый номер датчика
- Уникальный 16-ти значный ROM датчика
- Значение последнего измерения температуры
- Время последнего успешного измерения (Last Update)

Routing

Информация о режиме работы WAN-портов.

Таблица 3. Поля в разделе Routing

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

Таблица 4. Поля в разделе Local Network (LAN)

Поле	Описание
Status	Указывается есть ли физическое подключение к порту: Up — подключение есть, Down — подключения нет
Type	Режим работы порта: static — статическая IP-адресация
Address	IP-адрес порта с указанием макси сети
Uptime	Время работы порта
MAC	MAC-адрес порта
Rx/Tx	Счетчик принятых и отправленных байт

Mobile Internet (SIM1/SIM2/SIM3/SIM4)

Информация о состоянии подключения по каналу сотовой сети.

Число разделов соответствует числу SIM-карт, если их в устройстве установлено больше одной. В зависимости от модели роутера некоторые поля могут отсутствовать.

Таблица 5. 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
Uptime	Время активности с момента установки сессии

Таблица 5. Поля раздела Mobile Internet

Network	Тип сотовой сети по которой в данный момент осуществляется передача данных: 2G, 3G, 4G
Operator	Выводится имя оператора сотовой сети
Signal Quality	Уровень сигнала сотовой сети в формате CSQ и в процентах от максимального
Module Name	Название GSM модуля, установленного в вашем роутере
Module Revision	Номер версии GSM-модуля роутера
Module IMEI	IMEI Номер GSM модуля вашего роутера.
RSRQ	Качество сигнала, принимаемого от базовой станции
RSRP	Мощность сигнала, принимаемого от базовой станции
RSSI	Статистический показатель, уровень мощности принимаемого мобильной техникой сигнала. Отрицательное значение, и чем ближе к 0, тем сильнее сигнал
SINR	Соотношение уровня полезного сигнала к уровню шума
Bands	Частотные полосы (бэнды), которые используютя для связи в данный момент
Rx/Tx	Счетчик принятых и отправленных байт
Address	IP-адрес SIM-карты с указанием маски сети, выдаваемый оператором сотовой сети

Wired Internet (WAN)

Информация о статусе порта WAN.

Таблица 6. Поля в разделе Wired Internet (WAN)

Поле	**Описание**
Status	Состояние порта
Address	IP-адрес порта с указанием маски сети
MAC	MAC-адрес порта
Uptime	Время активности порта

Таблица 6. Поля в разделе Wired Internet (WAN)

Type	Тип работы порта
Rx/Tx	Счетчик принятых и отправленных байт

Routing Table

Информация по таблице маршрутизации.

Выводятся все существующие на данный момент маршруты.

UPS Status

Информация о состоянии источника бесперебойного питания (только для роутеров со встроенным ИБП)

Таблица 7. Поля в разделе UPS Status

Поле	**Описание**
Input Voltage	входящее напряжение
Battery Voltage	напряжение на ИБП

Если значение Input Voltage равно нулю, устройство работает от встроенного ИБП.

IPSec tunnel

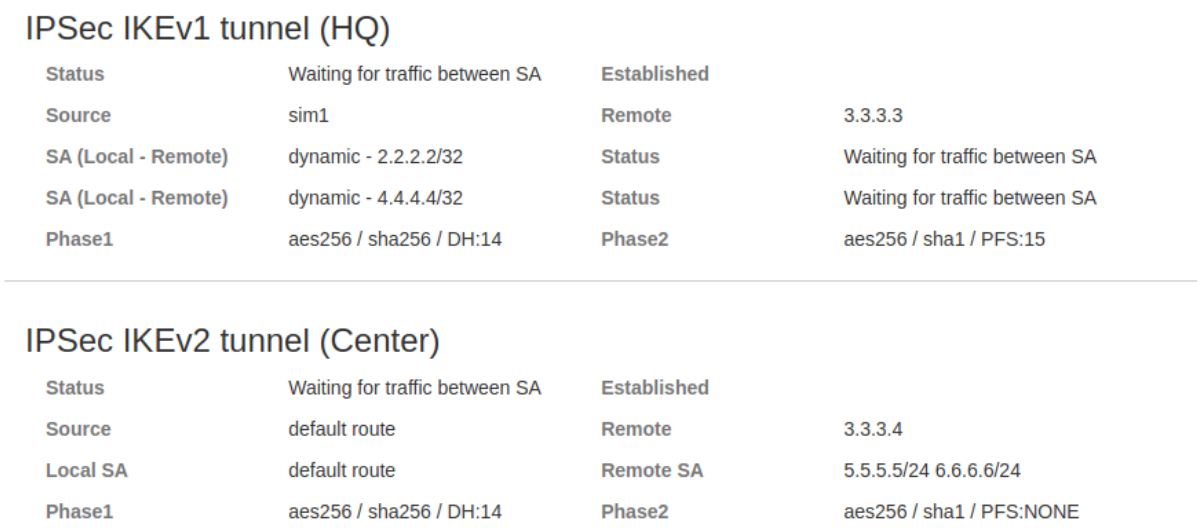


Рис. 4. Пример информации в разделе IPSec tunnel

Таблица 8. Поля в разделе Status для IPSec туннеля

Поле	**Описание**
Status	Текущий статус туннеля
Source	Локальный интерфейс, через который будет работать туннель (**Default route** – через интерфейс, являющийся на данный момент активным WAN-портом)
Remote	Доменное имя или IP-адрес порта удаленного устройства, с которым будет построен туннель
SA (Local - Remote)	Security Associations, политики безопасности
Phase 1, 2	Параметры аутентификации и шифрования для Фазы 1 и Фазы 2

Поле **Status** описывает текущее состояние туннеля. Возможные значения поля описаны в таблице ниже.

Таблица 9. Возможные значения поля Status

Поле	Описание
Network not available	Адрес источника с локальной стороны (Source Address) не доступен
Waiting for traffic between SA	Ожидание трафика между между локальной (Local subnets / Source Address) и удалённой стороной (Remote Subnets / Remote Address) чтобы инициировать обмен ключами и согласование политик
Phase 1 established	Обмен ключами прошел успешно, Phase 1 построена, Phase 2 не построена. Трафик не идёт
Installed	Туннель построен, трафик шифруется
Down	Роутер ожидает подключения клиентов (Remote Address указан как 0.0.0.0)

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 рисунке ниже 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!

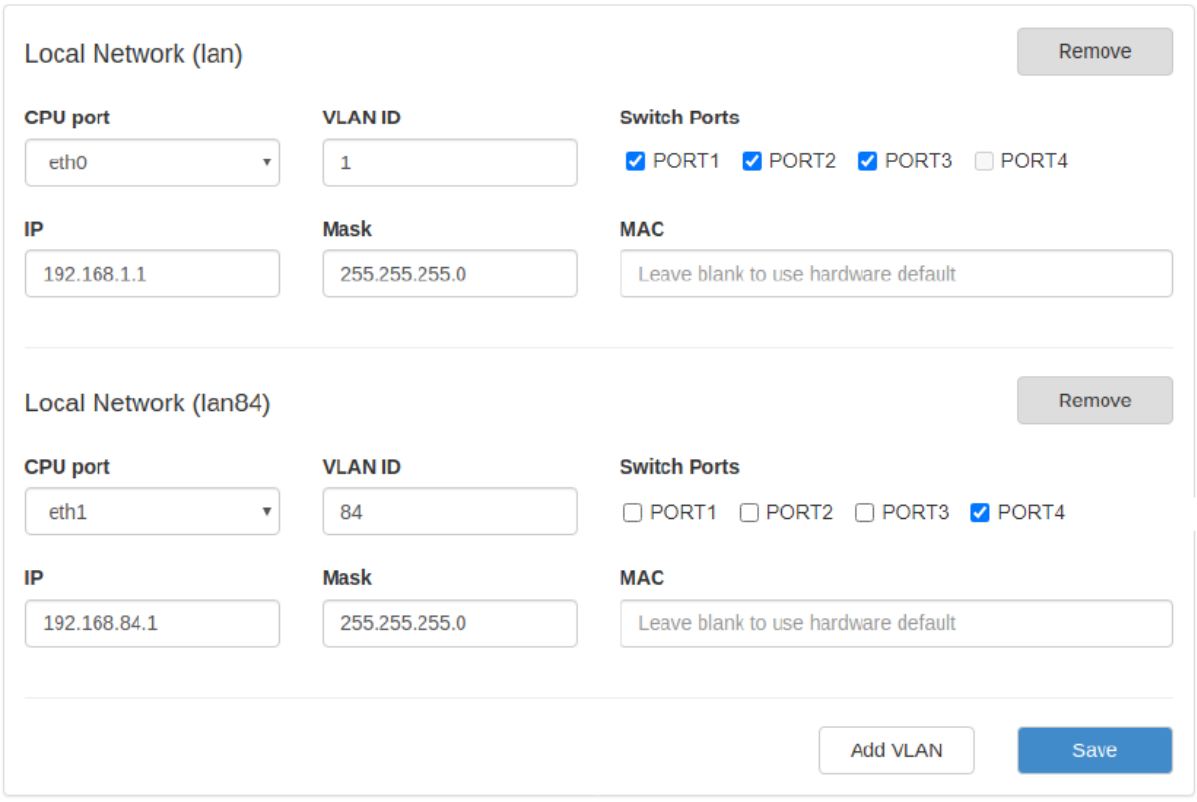


Рис. 5. Вкладка Network, раздел Local Network

Таблица 10. 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

Failover management (проверка состояния соединения)

Предусмотрена проверка состояния соединения при помощи отправки ICMP-пакетов (пинга) указанного адреса.

В поле **Ping Address** указывается IP-адрес или доменное имя сервера для проверки работы соединения. Можно указать несколько IP-адресов или доменов через **;** или через ПРОБЕЛ. В поле **Ping Interval** задается периодичность запуска пинга (в секундах). В поле **Ping Attempts** указывается количество неудачных попыток подряд.

В момент начала отслеживания соединению (маршруту) присваивается приоритет.

Управление маршрутами находится в разделе **Network** - **Routes**

- Если после отправки ICMP-пакета на сервер поступает ответ, маршрут считается работающим. Никаких дополнительных действий не происходит.
- Если после отправки ICMP-пакета на сервер ответа не поступает, попытка считается неудачной, начинает отсчитываться Ping Attempts. Маршрут переводится в резервный.
    - Если следующая попытка соединения будет удачной, маршруту возвращается исходный приоритет.
    - Если количество неудачных попыток подряд достигнет заданного, интерфейс будет перезапущен и через какое-то время маршрут стартует с приоритетом по умолчанию.

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.

Чтобы добавить новый VLAN, нажмите на кнопку **Add VLAN**, а чтобы удалить – нажмите кнопку **Remove**.

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

При создании VLAN по умолчанию в поле **Connection Type** выставлено значение **Disabled**. Это означает, что WAN-порт логически выключен - то есть физическое подключение будет присутствовать, но роутер не будет передавать по порту никаких данных.

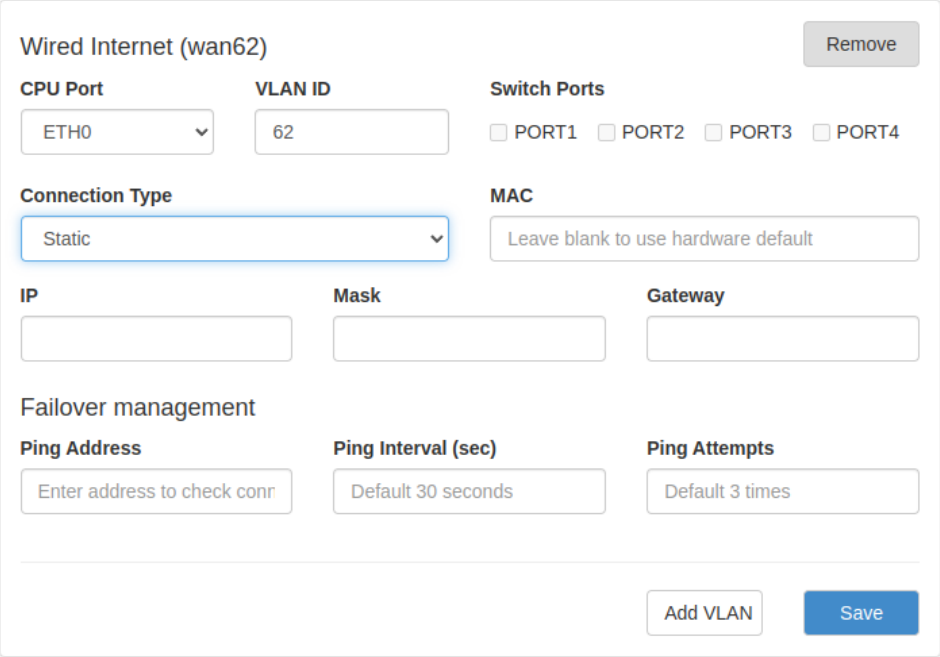


Рис. 6. Вкладка Network, раздел Wired Internet

Перечень основных настроек приведен в таблице **Network → Wired Internet**.

Таблица 11. Network → Wired Internet основные настройки

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.

Таблица 11. Network → Wired Internet основные настройки

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

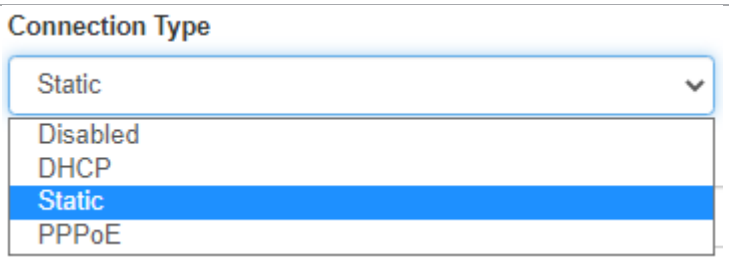


Рис. 7. Тип соединения для WAN-порта

Тип подключения **DHCP** означает, что роутер должен получить IP-адрес, маску и адреса DNS-серверов от внешнего DHCP-сервера.

Тип подключения **Static** необходим для ручной установки сетевых настроек WAN-порта.

Тип подключения **PPPoE** необходим при использовании протокола с авторизацией на сервере PPPoE.

Таблица 12. Дополнительные настройки (поле **Connection Type**)

Поле	**Описание**
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 (по умолчанию, 3)
Use Peer DNS Server	Включение/выключение использования внешних DNS-серверов провайдера
MAC	MAC-адрес роутера для созданного VLAN. Если поле оставить пустым, то будет использоваться MAC-адрес, установленный производителем
IP	IP-адрес роутера для созданного VLAN
Mask	Маска сети роутера для созданного VLAN
Gateway	Шлюз роутера для созданного VLAN
Login	Логин, который указывается при PPPoE-соединении

Таблица 12. Дополнительные настройки (поле **Connection Type**)

Password	Пароль, который указывается при PPPoE-соединении
AC-name	Имя концентратора доступа, который указывается при PPPoE-соединении

Failover management (проверка состояния соединения)

Предусмотрена проверка состояния соединения при помощи отправки ICMP-пакетов (пинга) указанного адреса.

В поле **Ping Address** указывается IP-адрес или доменное имя сервера для проверки работы соединения. Можно указать несколько IP-адресов или доменов через **;** или через ПРОБЕЛ. В поле **Ping Interval** задается периодичность запуска пинга (в секундах). В поле **Ping Attempts** указывается количество неудачных попыток подряд.

В момент начала отслеживания соединению (маршруту) присваивается приоритет.

Управление маршрутами находится в разделе **Network** - **Routes**

- Если после отправки ICMP-пакета на сервер поступает ответ, маршрут считается работающим. Никаких дополнительных действий не происходит.
- Если после отправки ICMP-пакета на сервер ответа не поступает, попытка считается неудачной, начинает отсчитываться Ping Attempts. Маршрут переводится в резервный.
    - Если следующая попытка соединения будет удачной, маршруту возвращается исходный приоритет.
    - Если количество неудачных попыток подряд достигнет заданного, интерфейс будет перезапущен и через какое-то время маршрут стартует с приоритетом по умолчанию.

Failover management доступен для типов подключения DHCP и Static (при этом должен быть указан Gateway). Для включения функции обязательно должен быть выбран параметр **Default Route**.

5.2.3. Mobile Interfaces

Раздел **Mobile Interfaces** на вкладке **Network** предназначен для настройки мобильного Интернета.

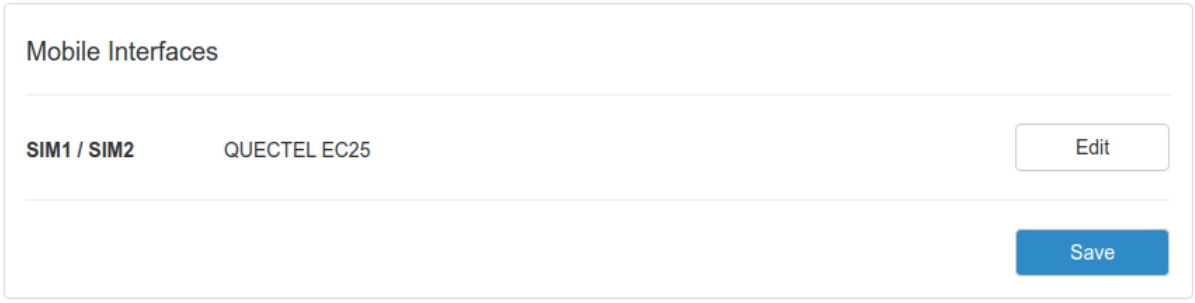


Рис. 8. Вкладка Network, раздел Mobile Interfaces для одномодульного устройства

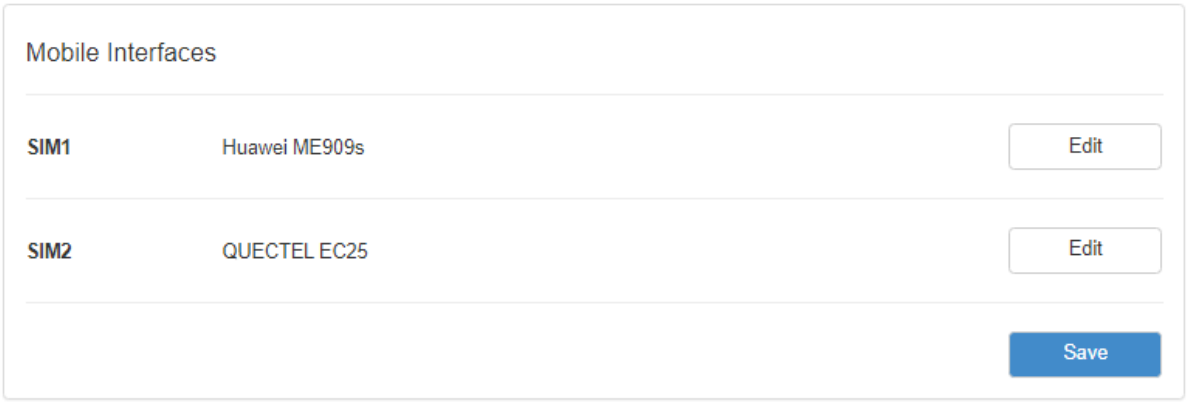


Рис. 9. Вкладка Network, раздел Mobile Interfaces для двухмодульного устройства

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.

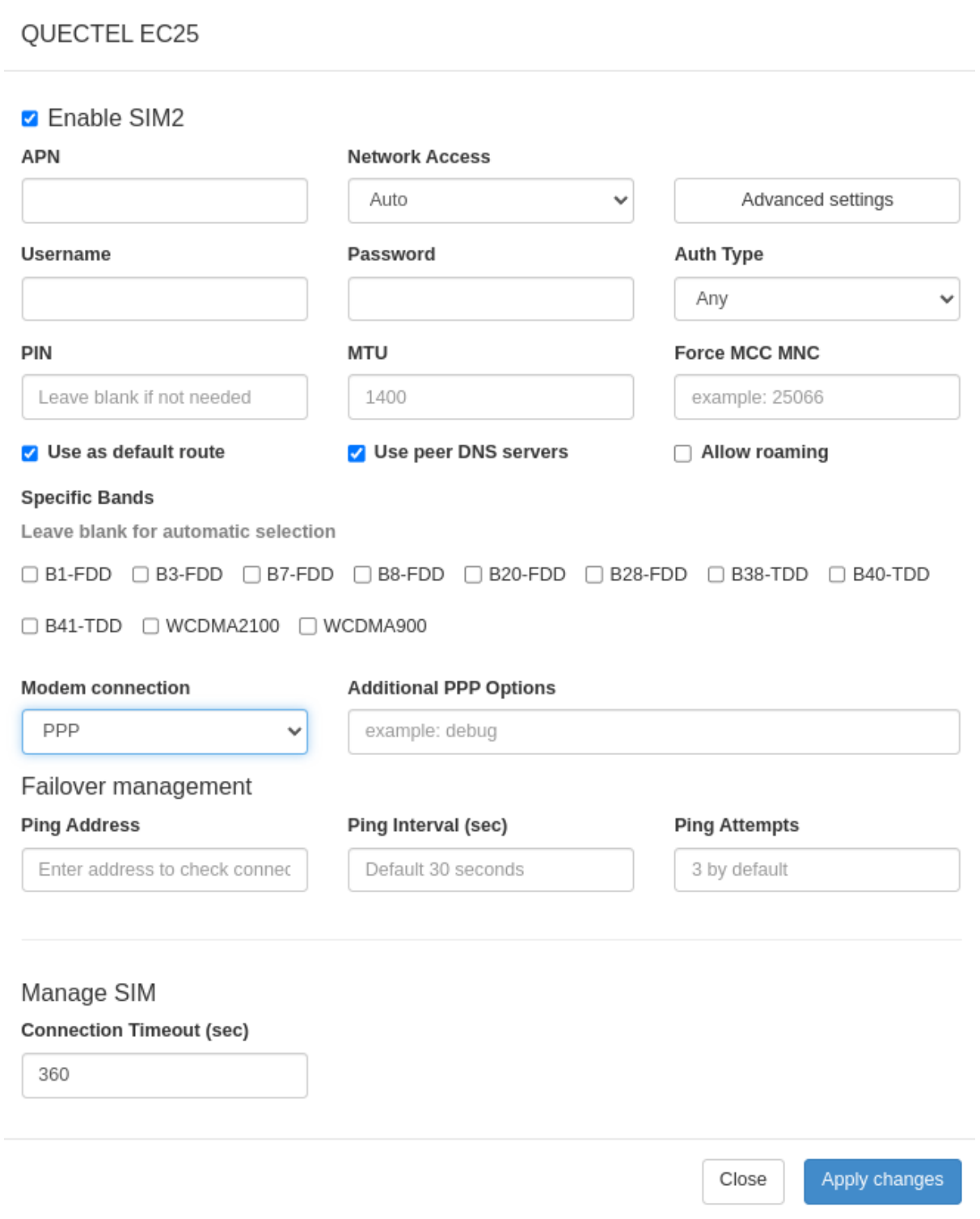


Рис. 10. Вкладка Network, раздел Mobile Interfaces − Edit

Настройки мобильного Интернета

В зависимости от модели роутера поля Specific Bands, Primary SIM, Return to Primary SIM могут отсутствовать.

Таблица 13. Настройки Network → Mobile Interfaces → Edit

Таблица 13. 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
Network Access	Выбор режима работы с сотовыми сетями 3G, 4G
Username	Имя пользователя для доступа в сотовую сеть провайдера
Password	Пароль для доступа в сотовую сеть провайдера
Authentication Type	Выбор протокола идентификации SIM-карты в сети провайдера
PIN	PIN-код SIM-карты (если установлен)
MTU	Настройка значения MTU
Force MCC MNC	Позволяет ограничить выбор сотовых операторов. Задается мобильный код страны (MCC) в комбинации с мобильным кодом сети (MNC), что является уникальным идентификатором той сети, которую требуется использовать
Use As Default Route	Использовать указанные настройки как маршрут по умолчанию
Use Peer DNS Server	Включение/выключение использования внешних DNS-серверов провайдера
Allow Roaming	Разрешение/запрет работы SIM-карты устройства в роуминге
Specific Bands	Выбор частотных полос (бэндов).
Modem Connection	Выбор протокола - **PPP** или **Auto**
Additional PPPD Options	Указание дополнительных опций при работе по протоколу PPP
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

Таблица 13. Настройки Network → Mobile Interfaces → Edit

Primary SIM	Указывает какая из SIM карт является приоритетной (только для одномодульных роутеров)
Return to Primary SIM (sec)	Указание промежутка времени, после которого роутер произведет попытку вернуться на основную SIM карту (только для одномодульных роутеров)

Выбор частотных полос (бэндов)

Функция доступна для GSM-модулей следующих ревизий:
- EP06-E - EP06ELAR04A03M4G и **выше**,
- EC25-EU - EC25EUGAR06A03M4G и **выше**,
- EC200T- EU -EC200TEUHAR05A03M16 и **выше**.

Для автоматического выбора бэндов все поля следует оставить пустыми.

Для выбора определенных бэндов нужно поставить галочки в соответствующих чекбоксах.

При этом:

- в режиме **Network Access** - **Auto** для выбора будут доступны все бэнды,
- в режиме **Network Access** - **4G only** или **3G only** - только бэнды, которые соответствуют указанным стандартам,
- в режиме **Network Access** - **2G only** выбор бэндов недоступен.

Переключение SIM-карт

Для устройств с одним GSM-модулем
Для устройств с одним GSM-модулем реализован алгоритм переключения между SIM-картами.

По приоритету SIM-карта может быть главной или второстепенной. По умолчанию главной является **SIM1**. Эту настройку можно изменить в строке **Primary SIM**.

Переключение между SIM-картами происходит в следующих случаях:

- Если главная SIM-карта отсутствует (не установлена в устройстве)
- Если через указанную SIM-карту не удалось подключиться к сети передачи данных в течении заданного интервала времени **Connection Timeout (sec)**
- Если в момент работы через второстепенную SIM-карту был достигнут интервал возвращения на главную SIM-карту **Return to Primary SIM (sec)**

Для устройств с двумя GSM-модулями

В роутерах с двумя GSM-модулями каждый модуль работает со своей SIM-картой независимо.

В разделе **Network** - **Routes** можно установить приоритет маршрутизации, согласно которому в режиме резервирования (**Backup**) передача данных будет идти в первую очередь через приоритетную SIM-карту или другой доступный канал связи (например, проводной WAN или Wi-Fi).

Если соединение через SIM-карту с более высоким приоритетом не установлено и достигнут интервал **Connection Timeout** (или в случае включенной проверки состояния соединения - количество неудачных попыток **Ping Attempts** достигло заданного), роутер инициирует перезагрузку соответствующего GSM-модуля.

В этом случае передача данных будет автоматически переключена на SIM-карту с более низким приоритетом.

После восстановления подключения приоритетной SIM-карты передача данных будет снова осуществляться через неё.

Failover management (проверка состояния соединения)

Предусмотрена проверка состояния соединения при помощи отправки ICMP-пакетов (пинга) указанного адреса.

В поле **Ping Address** указывается IP-адрес или доменное имя сервера для проверки работы соединения. Можно указать несколько IP-адресов или доменов через **;** или через ПРОБЕЛ. В поле **Ping Interval** задается периодичность запуска пинга (в секундах). В поле **Ping Attempts** указывается количество неудачных попыток подряд.

В момент начала отслеживания соединению (маршруту) присваивается приоритет.

Управление маршрутами находится в разделе **Network** - **Routes**

- Если после отправки ICMP-пакета на сервер поступает ответ, маршрут считается работающим. Никаких дополнительных действий не происходит.
- Если после отправки ICMP-пакета на сервер ответа не поступает, попытка считается неудачной, начинает отсчитываться Ping Attempts. Маршрут переводится в резервный.
    - Если следующая попытка соединения будет удачной, маршруту возвращается исходный приоритет.
    - Если количество неудачных попыток подряд достигнет заданного, интерфейс будет перезапущен и через какое-то время маршрут стартует с приоритетом по умолчанию.

Для включения функции должен быть выбран параметр **Default Route**

- Если после перезагрузки GSM-модуля соединение все еще не установлено, после достижения интервала **Connection Timeout (sec)** устройство переключится на другую SIM-карту.

Проверка состояния соединения предусмотрена для роутеров как с одним, так и с двумя GSM-модулями.

5.2.4. Mobile APN Profiles

Раздел предназначен для работы с SIM-картами виртуальных операторов.

Виртуальные операторы используют сотовые сети базовых операторов (Мегафон, МТС, Билайн, Теле2). Для подключения к каждой из базовых сетей виртуальному оператору может потребоваться отдельное значение APN и код MCCMNC.

Заполнять данные Mobile APN Profiles для работы с SIM-картами базовых операторов не требуется.

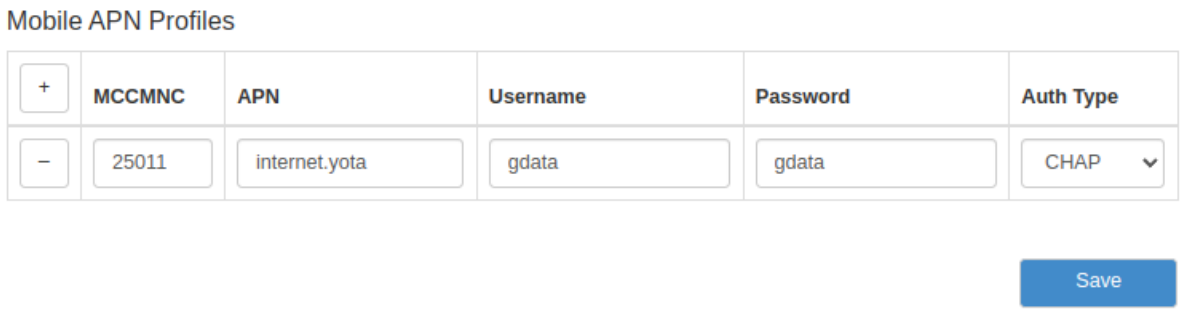


Рис. 11. Вкладка Mobile APN Profiles

Таблица 14. 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

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.

Предусмотрена валидация по имени. Имена, являющиеся системными, зарезервированы - их в поле **name** задать нельзя.

Рис. 12. 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 Network

Раздел **Wireless Network** на вкладке **Network** предназначен для настройки параметров Wi-Fi.

Данный раздел доступен только для роутеров, которые поддерживают работу с Wi-Fi (имеют индекс "w" в названии модели).

Для устройств, оборудованных двумя модулями Wi-Fi, каждый из них настраивается отдельно.

На рисунке ниже представлен пример страницы настроек.

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

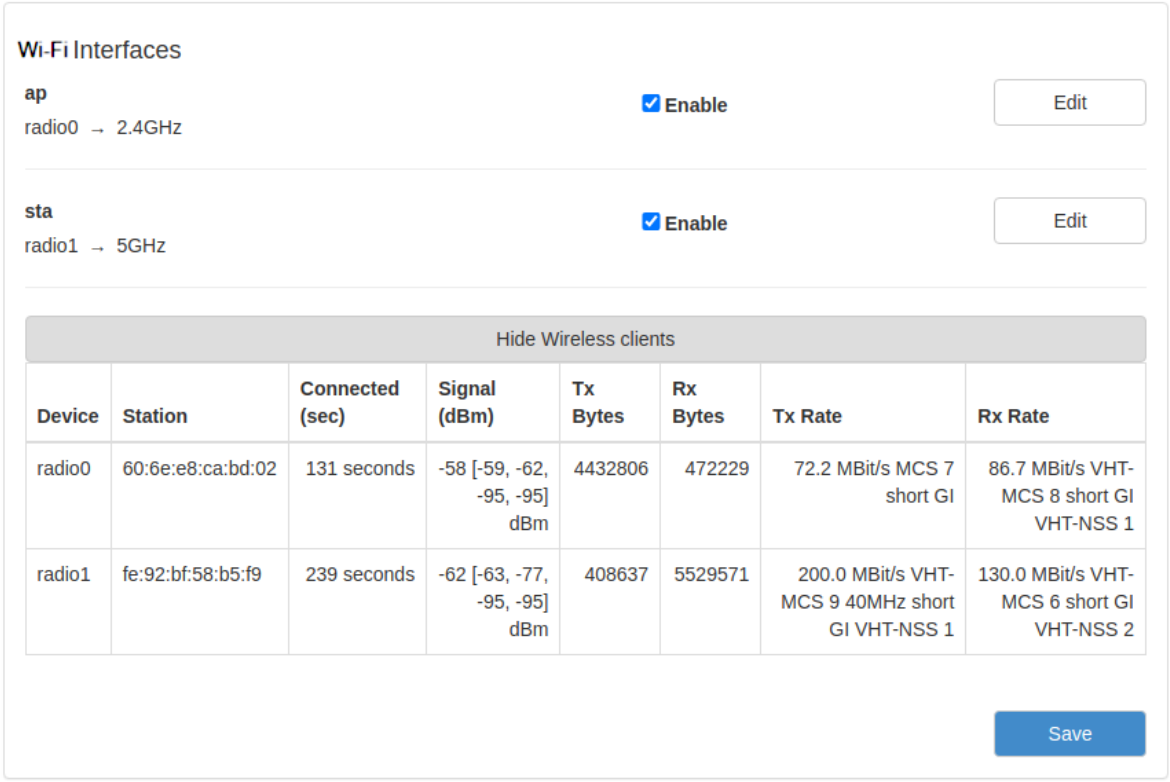


Рис. 13. Вкладка Network, раздел Wireless Internet

Чтобы включать или отключать работу роутера с Wi-Fi модулем необходимо поставить или снять галочку напротив пункта **Enable**. Для начала редактирования настроек необходимо нажать кнопку **Edit**.

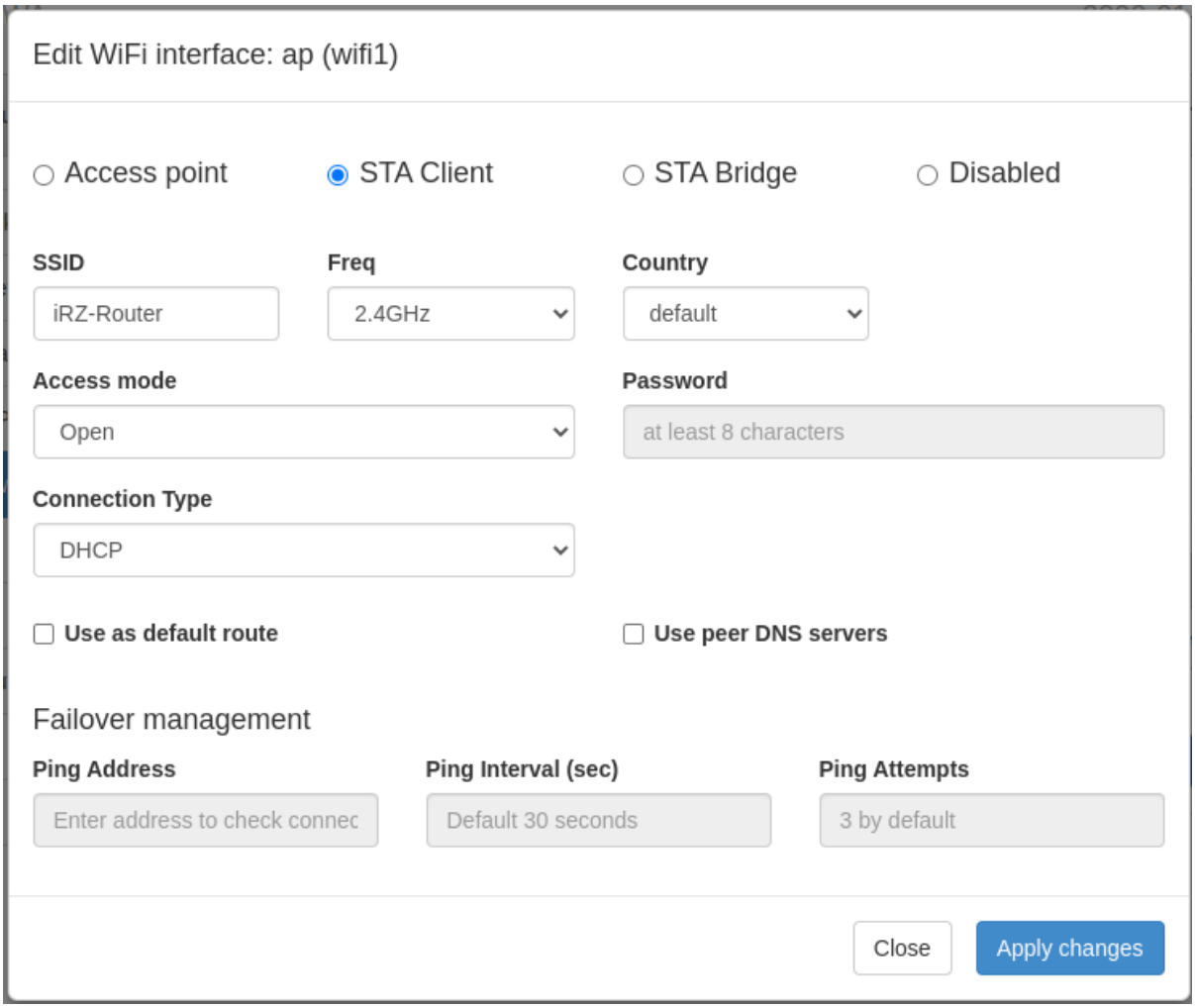


Рис. 14. Меню Edit, Вкладка Network, раздел Wireless Internet

Выбор режима работы модуля Wi-Fi:

- **Access point** — роутер работает в качестве точки доступа и ждет подключения клиентов к своей сети;
- **STA Client** — роутер работает в режиме клиентской станции и подключается к внешней Wi-Fi-сети, в данном режиме Wi-Fi-интерфейс автоматически становится одним из WAN-портов;
- **STA Bridge** — объединение локальной проводной сети с беспроводной;
- **Disabled** — отключение Wi-Fi-модуля.

Access Point

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

Таблица 15. Настройки Network → Wireless Network (Режим Access Point)

Поле	Описание
Bridge with Interface	Создание моста с локальным интерфейсом или создание нового интерфейса. • При выборе пункта **LAN** в настройке **Bridge with Interface**, Wi-Fi-интерфейс роутера будет работать в режиме моста с LAN-портами. • При выборе пункта **Wi-Fi** в настройке **Bridge with Interface**, Wi-Fi-интерфейс будет работать, как самостоятельный интерфейс. Доступные настройки приведены на рисунке.
Static IP Address	IP-адрес интерфейса роутера
Network 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
Country	Код страны
Access Mode	Тип шифрования пароля доступа к создаваемой Wi-Fi-сети
Password	Пароль для доступа к создаваемой Wi-Fi-сети
HTmode	Выбор режима производительности
Don’t scan for overlapping BSSs in HT40 mode	Включить/отключить проверку перекрытия с другими базовыми станциями в режиме HT40

STA Client

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

Таблица 16. Настройки Network → Wireless Network (Режим STA Client)

Поле	Описание
Connection Type	Выбор типа соединения. • При выборе в настройке **Connection Type** пункта **DHCP**, роутер будет получать настройки соединения от DHCP-сервера сети к которой подключается. • При выборе в настройке **Connection Type** пункта **Static**, роутер будет работать со статичными настройками соединения, которые указываются в пунктах **Static IP Address**, **Network Mask** и **Gateway**.
Static IP Address	IP-адрес интерфейса роутера
Network Mask	Маска сети интерфейса роутера
Gateway	Шлюз роутера
Use As Default Route	Использовать указанные настройки как маршрут по умолчанию
Use Peer DNS Server	Включение/выключение использования внешних DNS-серверов провайдера
SSID	Название Wi-Fi-сети, к которой будут подключаться клиенты
Freq	Переключение частоты работы Wi-Fi модуля
Country	Код страны (значение по умолчанию - default)
Access Mode	Тип шифрования пароля доступа к создаваемой Wi-Fi-сети
Password	Пароль для доступа к создаваемой Wi-Fi-сети

STA Bridge

STA Bridge - режим для объединения локальной проводной сети с беспроводной сетью.

Таблица 17. Настройки Network → Wireless Network (Режим STA Bridge)

Поле	Описание
Use As Default Route	Использовать указанные настройки как маршрут по умолчанию
Use Peer DNS Server	Включение/выключение использования внешних DNS-серверов провайдера
SSID	Название Wi-Fi-сети, к которой будут подключаться клиенты
Freq	Переключение частоты работы Wi-Fi модуля
Country	Код страны (значение по умолчанию - default)
Access Mode	Тип шифрования пароля доступа к создаваемой Wi-Fi-сети
Password	Пароль для доступа к создаваемой Wi-Fi-сети
Bridge With Interface	Выбор локальной сети с которой будет создан мост. Запрещено использование интерфейсов, которые используются как DHCP сервер.

Перед выключением DHCP не забудьте настроить статический IP адрес на устройстве, с которого собираетесь конфигурировать роутер.

Или же настройте дополнительный VLAN в секции **Local Networks**. Будет необходимо указать IP адрес интерфейса, важно указать адрес не пересекающийся с адресами из пула Wi-Fi сети.

Failover management (проверка состояния соединения)

Предусмотрена проверка состояния соединения при помощи отправки ICMP-пакетов (пинга) указанного адреса.

В поле **Ping Address** указывается IP-адрес или доменное имя сервера для проверки работы соединения. Можно указать несколько IP-адресов или доменов через **;** или через ПРОБЕЛ. В поле **Ping Interval** задается периодичность запуска пинга (в секундах). В поле **Ping Attempts** указывается количество неудачных попыток подряд.

В момент начала отслеживания соединению (маршруту) присваивается приоритет.

Управление маршрутами находится в разделе **Network** - **Routes**

- Если после отправки ICMP-пакета на сервер поступает ответ, маршрут считается работающим. Никаких дополнительных действий не происходит.

- Если после отправки ICMP-пакета на сервер ответа не поступает, попытка считается неудачной, начинает отсчитываться Ping Attempts. Маршрут переводится в резервный.
    - Если следующая попытка соединения будет удачной, маршруту возвращается исходный приоритет.
    - Если количество неудачных попыток подряд достигнет заданного, интерфейс будет перезапущен и через какое-то время маршрут стартует с приоритетом по умолчанию.

Failover management доступен в режиме STA и STA Bridge для типа соединения DHCP и Static (при этом должен быть указан Gateway). Для включения функции обязательно должен быть выбран параметр **Default Route**.

5.2.7. Routes

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

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

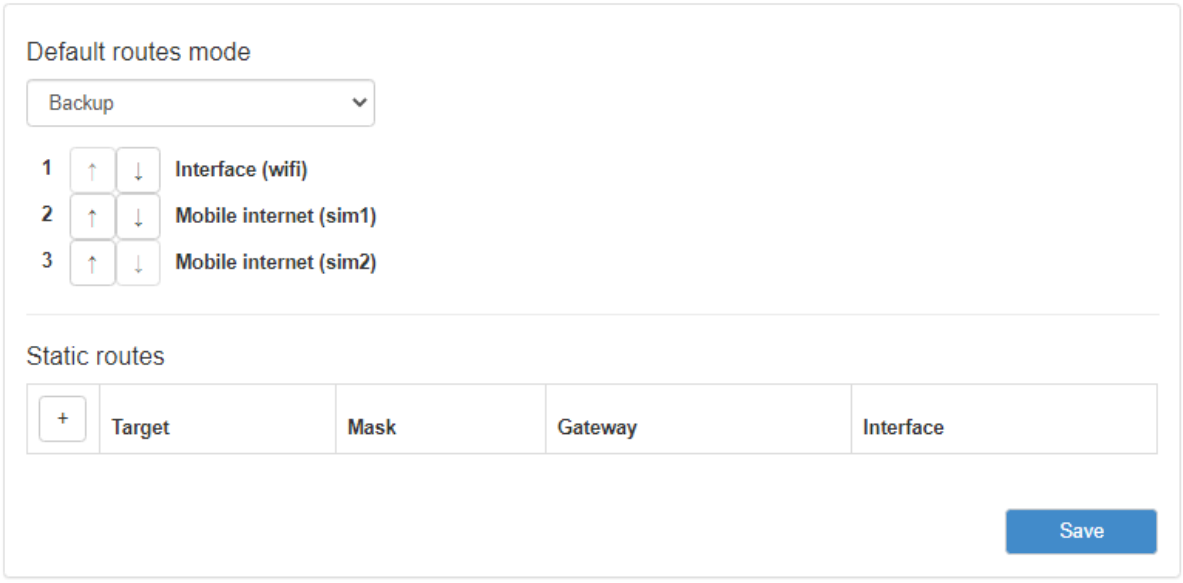


Рис. 15. Вкладка Network, раздел Routes

Default Routes Mode — режим работы интерфейсов:

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

В режиме **Backup** роутер резервирует подключение между интерфейсами в порядке, указанном пользователем (см. список под пунктом Backup на рисунке). С помощью стрелок ↑ ↓ можно перемещать выбранный интерфейс (WAN, SIM1/SIM2, туннельные интерфейсы) вверх или вниз в зависимости от приоритетов пользователя.

Для корректной работы рекомендуется настроить Failover Management на каждом из интерфейсов.

В режиме **Balance** роутер балансирует исходящий трафик между WAN-интерфейсами для увеличения пропускной способности. Данный режим для туннельных интерфейсов недоступен .

Static Routes

Подраздел для настройки статических маршрутов.

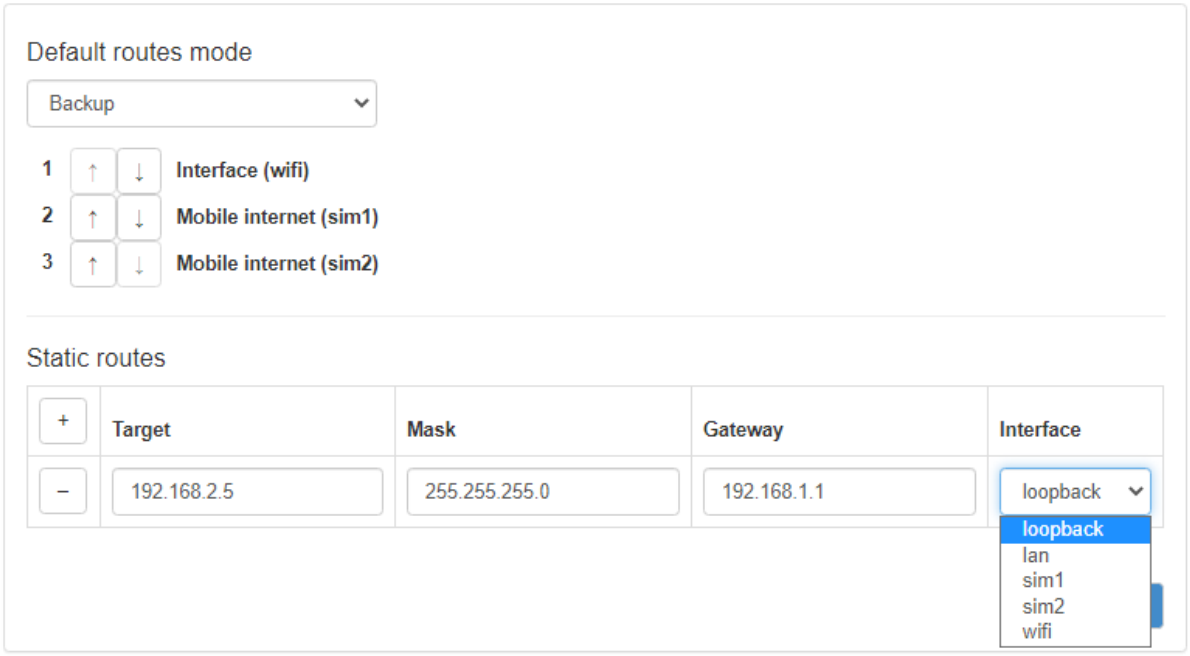


Рис. 16. Настройка статических маршрутов

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 18. 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)

Инструментом для работы с динамической маршрутизацией на роутерах iRZ является пакет **Quagga**. Поддерживаемые протоколы - **BGP**, **OSPF**.

На роутерах iRZ серии **R4** и **R50** динамическая маршрутизация доступна по умолчанию. На роутерах iRZ серии **R0** и **R2** требуется установка дополнительных пакетов.

Требуется версия прошивки 20.1 и выше.

Начиная с версии прошивки 20.6 для роутеров серии **R0** и **R2** реализована работа с динамической маршрутизацией через веб-интерфейс. На странице **Network** - **Dynamic Routes** расположена ссылка для скачивания архива пакетов, которые требуется установить.

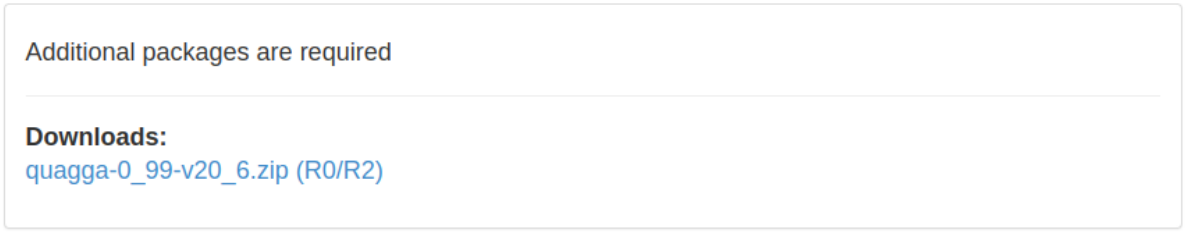


Рис. 17. Страница загрузки пакетов для роутера серии R2

Подробнее о том, как устанавливать пакеты, можно прочитать в разделе Tools - Management.

Важно устанавливать пакеты в том порядке, в котором они расположены.

После установки пользователю становится доступен веб-интерфейс, в котором представлены службы **BGPD** – демон протокола bgp, **OSPF6D** – демон протокола OSPFv3 для IPv6, **OSPFD** – демон протокола OSPFv2. Поле **ZEBRA** предназначено для настройки базового ядра Zebra.

Для настройки службы нужно отметить соответствующее текстовое поле чекбоксом и заполнить его с использованием синтаксиса файла конфигурации.

Пример настроек приведен на рисунке.

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

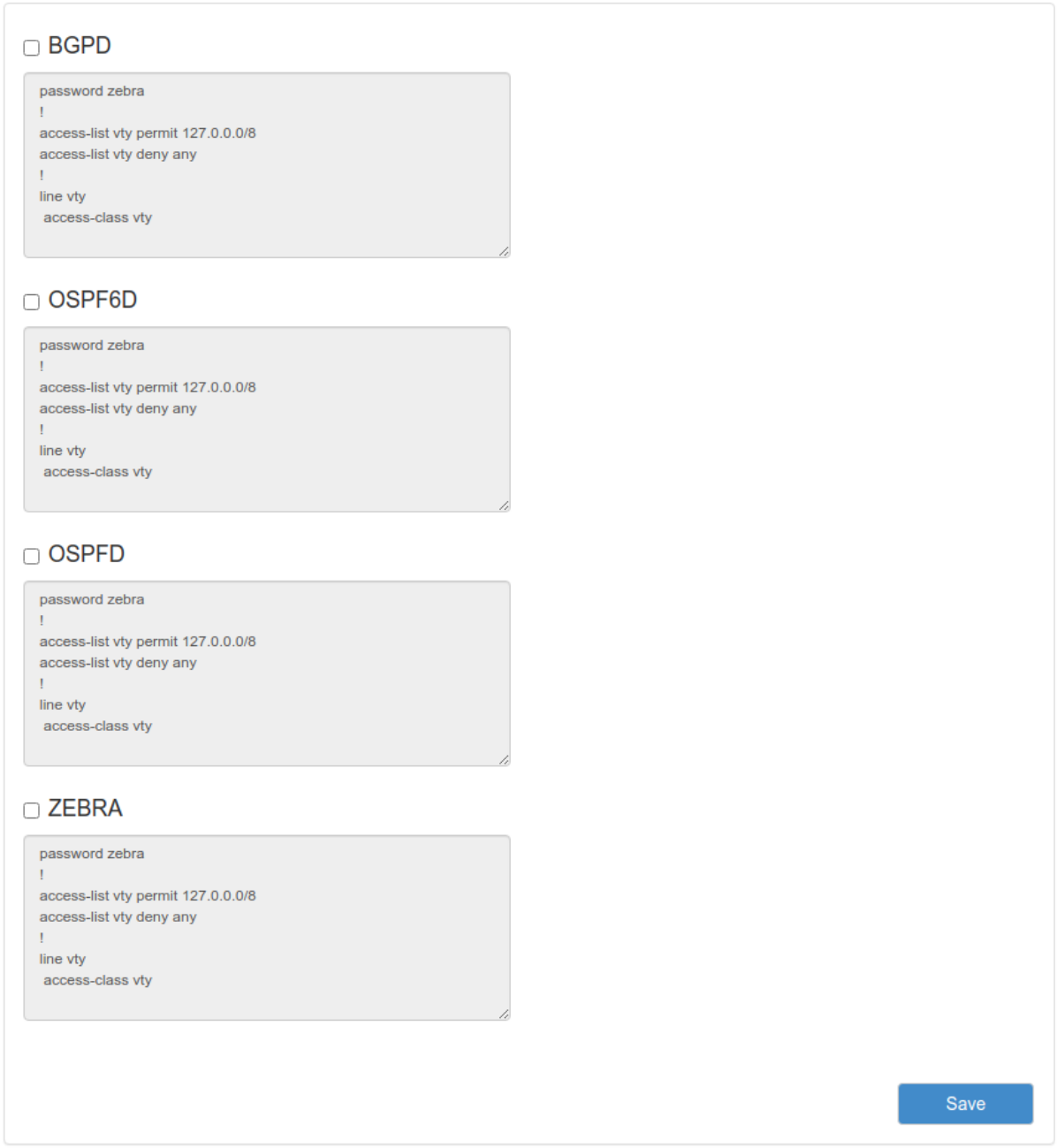


Рис. 18. Пример настройки динамической маршрутизации по протоколам: BGP, OSPF

5.2.9. DNS Servers

Раздел **DNS Servers** на вкладке **Network** предназначен для указания адресов DNS-серверов. На рисунке 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. 19. 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 рисунке представлен пример настройки портов роутера iRZ серии R4.

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

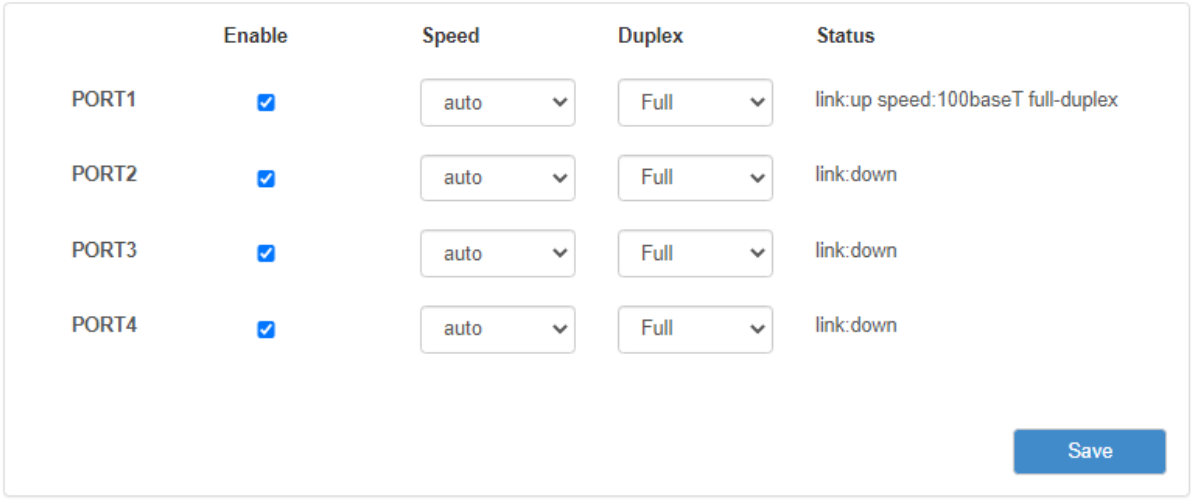


Рис. 20. Вкладка Network, раздел Switch

Таблица 19. 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 VPN/Tunnels

Подробную информацию о туннелях и их настойке можно прочитать в отдельном документе **"РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ. Настройка туннелей на роутерах iRZ"** на сайте **www.radiofid.ru**

5.4. Раздел «Services»

5.4.1. DHCP

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

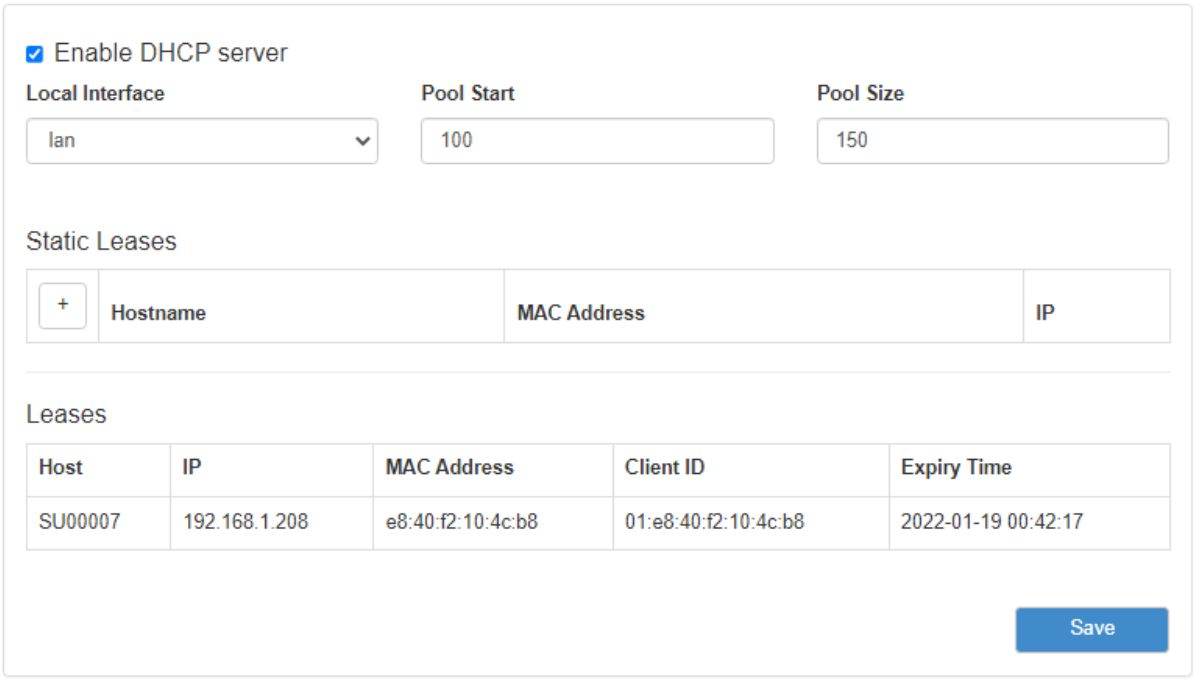


Рис. 21. Вкладка Services, раздел DHCP

Чтобы включить DHCP-сервер поставьте галочку напротив **Enable DHCP Server** и укажите настройки для его работы.

Таблица 20. Настройки DHCP

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 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 выше.

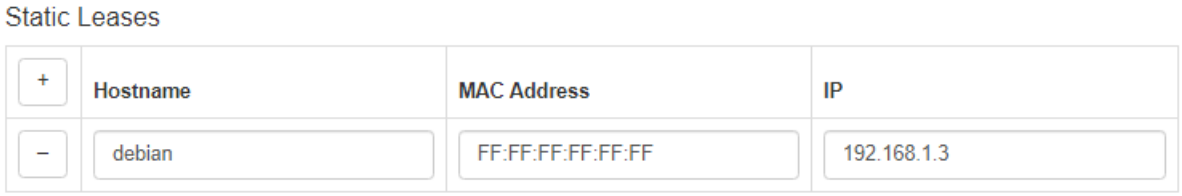


Рис. 22. Указание IP-адресов вручную

Подраздел Leases предназначен для представления информации о выданных IP-адресах клиентам от встроенного DHCP-сервера роутера, если он включен. На рисунке представлен пример страницы.

Host	IP	MAC Address	Client ID	Expiry Time
SU00007	192.168.1.208	E8:40:F2:10:4C:B8	01:e8:40:f2:10:4c:b8	

Рис. 23. Вкладка Tools, раздел DHCP Leases

Таблица 21. 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

5.4.2. 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 рисунке 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!

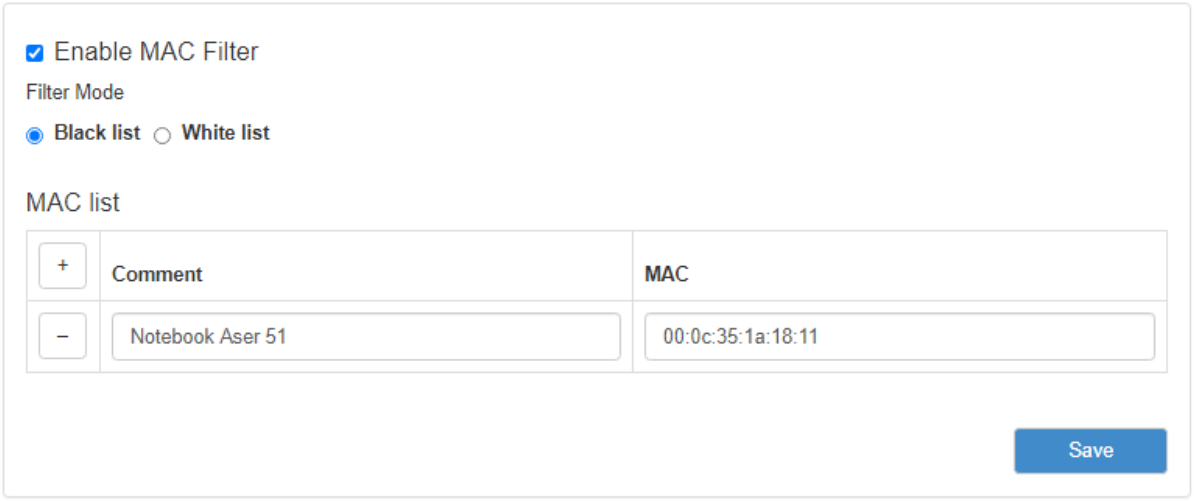


Рис. 24. Вкладка Services, раздел MAC Filter

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 рисунке ниже 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!

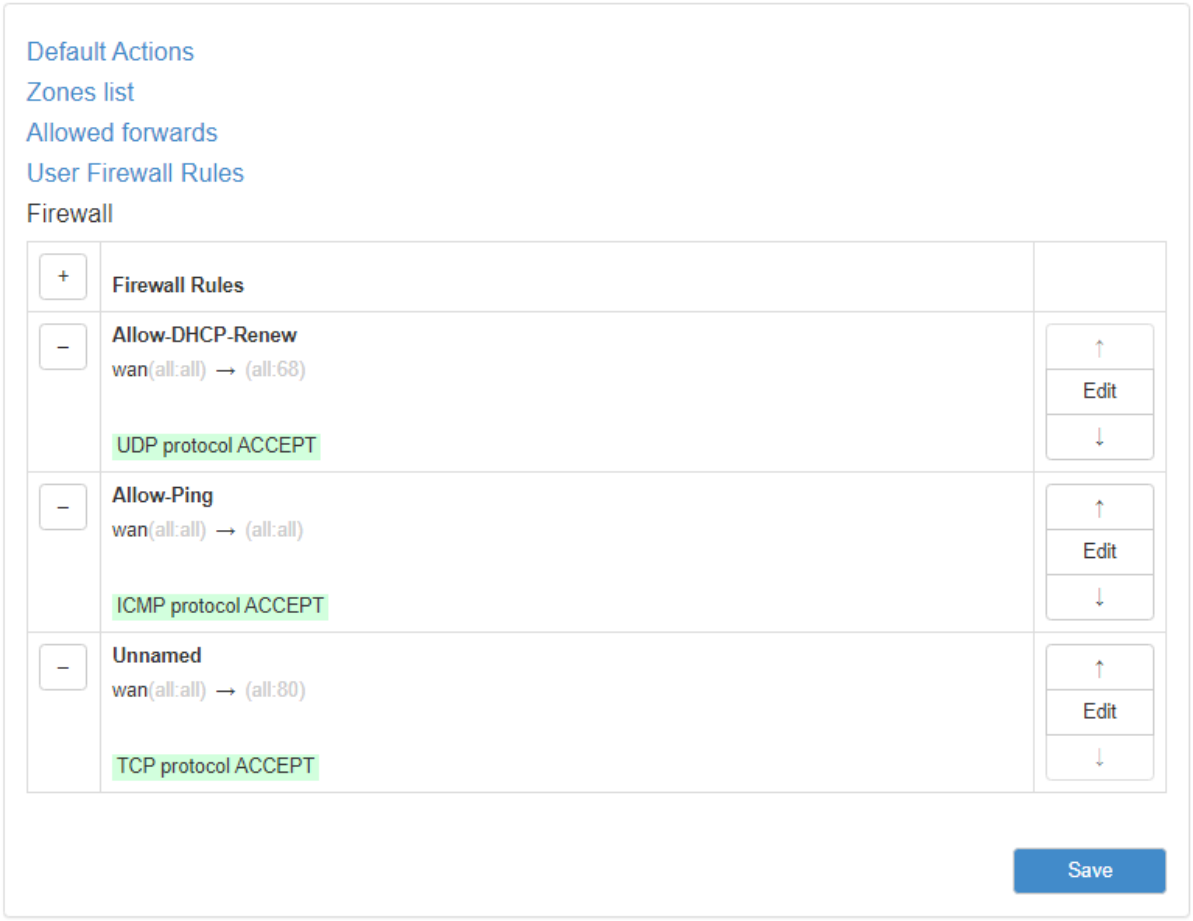


Рис. 25. Вкладка Services, раздел Firewall

Default Actions

Подгруппа настроек Default Actions определяет глобальные установки файрвола, которые не принадлежат каким-либо конкретным зонам.

Выбор глобальных установок осуществялется 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 рисунке ниже.

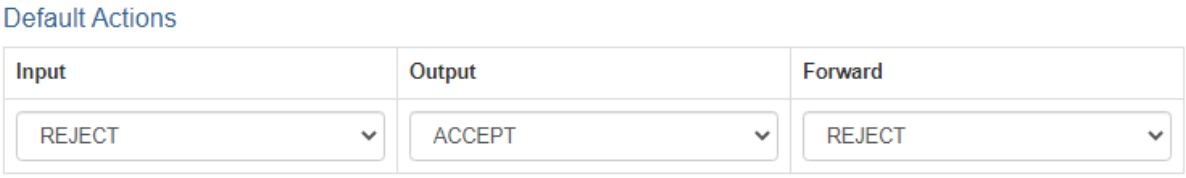


Рис. 26. Вкладка Services, раздел Firewall, настройки Default Actions

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 ниже.

Таблица 22. 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

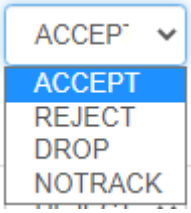


Рис. 27. Вариант выбора действий для трафика

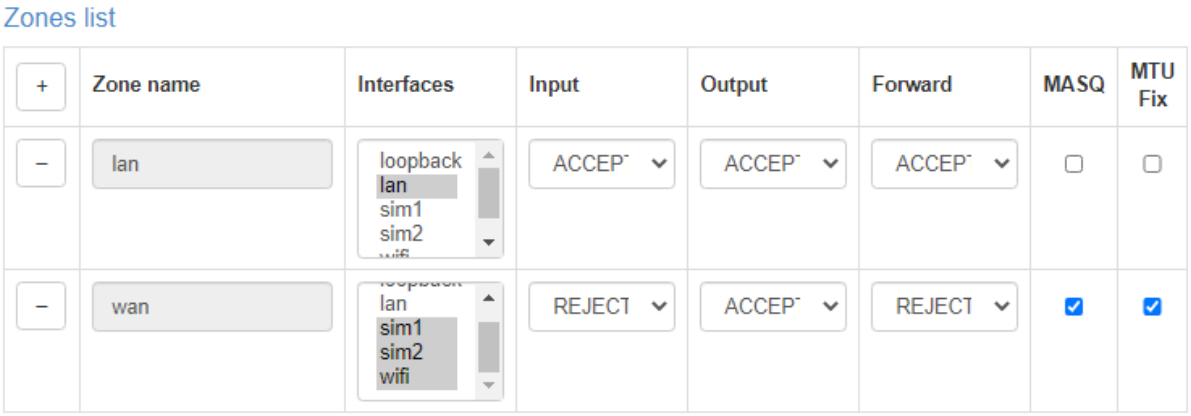


Рис. 28. Вкладка Services, раздел Firewall, настройки Zones List

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 рисунке 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 ниже.

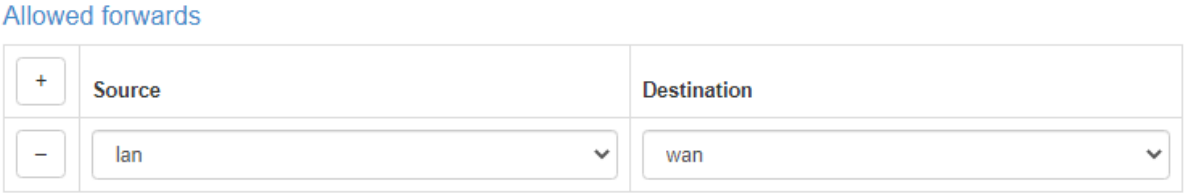


Рис. 29. Настройки Allowed Forwards

Таблица 23. 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 рисунке ниже 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.

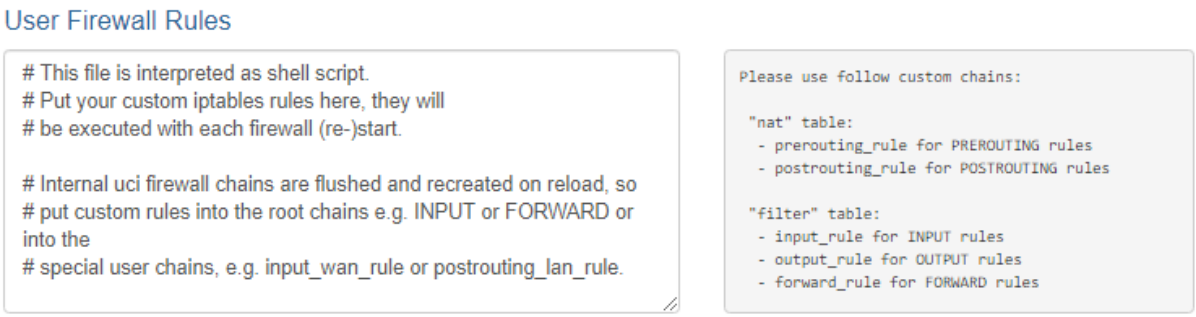


Рис. 30. Вкладка Services, раздел Firewall, настройки User Firewall Rules

Firewall

Подгруппа настроек Firewall отвечает за создание правил для межсетевого экрана. Правила задаются для сетевых протоколов и интерфейсов. Например, указывается направление движения 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. Изменение приоритета правил, то есть положение в очереди выполнения, где сначала выполняются «верхние» правила, осуществляется с помощью стрелок ↑ ↓

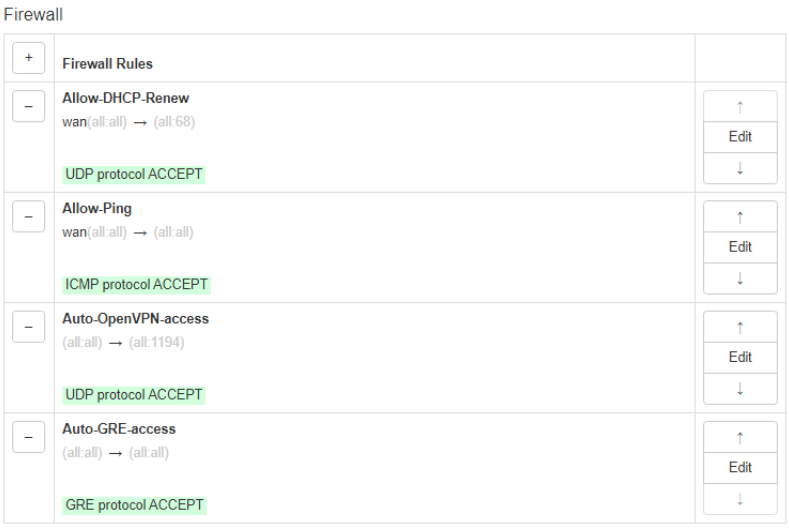


Рис. 31. Настройки Firewall

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.

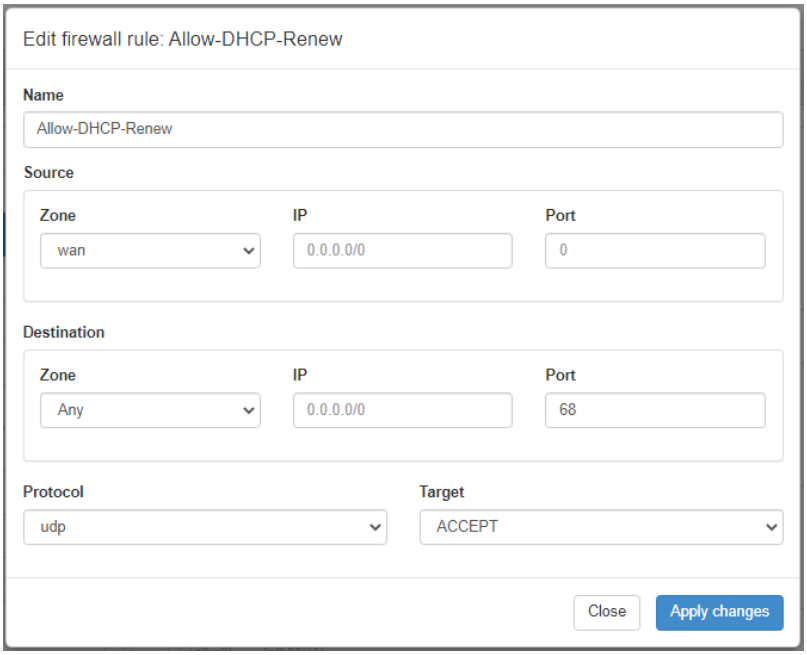


Рис. 32. Редактирование правила Firewall

Таблица 24. 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, **DSCP** – маркировать трафик для того чтобы к нему можно применять правила QoS (раздел **Services** – **Queues**)

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

Настройка QoS

Для работы с QoS в подгруппе настроек **Firewall** настраивается направление и правила маркировки трафика. Для этого после заполнения основных полей нужно в разделе **Target** выбрать **DSCP** и затем в выпадающем меню указать **DSCP Mark**

DSCP Mark

Определено три класса DSCP маркировки: по возможности (**BE** - best effort или DSCP 0), срочная доставка (**EF** - Expedited Forwarding), гарантированная доставка (**AF** - Assured Forwarding).

Для гарантированной доставки (**AF**) определено четыре класса. Они начинаются с AF и далее две цифры. Первая цифра определяет AF класс и принимает значения от 1 до 4. Вторая цифра определяет уровень вероятности сброса пакета в пределах каждого класса и принимает значения от 1 (минимальная вероятность сброса) до 3 (максимальная вероятность сброса).

В дополнение к этим трем определенным классам существуют коды селектора классов (class selector code points), которые обратно совместимы с IPP (**CS1-CS7** идентичны значениям 1-7 IPP).

Таблица 25. Коды селектора классов (class selector code points) для DSCP

Class selector name	IP Precedence name
Default / CS0	Routine
CS1	Priority
CS2	Immediate
CS3	Flash
CS4	Flash Override
CS5	Critic/Critical
CS6	Internetwork Control
CS7	Network Control

Далее в разделе **Services** – **Queues** необходимо настроить интерфейс и правило, по которому будет обрабатываться исходящий трафик с заданного интерфейса.

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 рисунке 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!

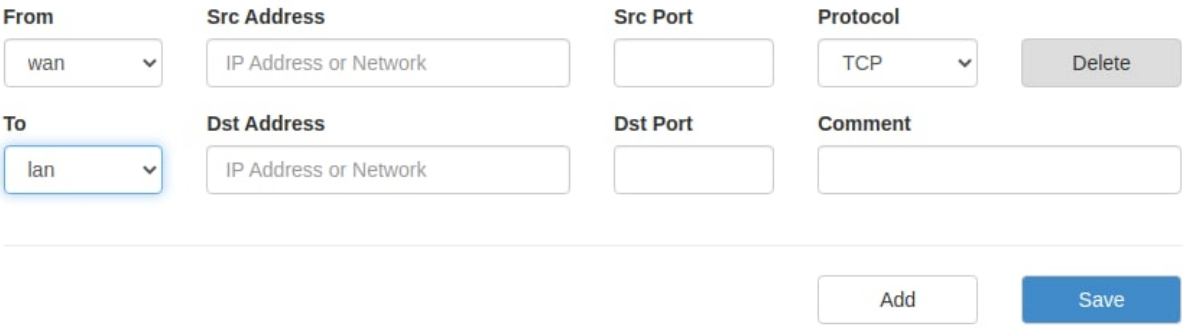


Рис. 33. Вкладка Services, раздел Port Forwarding

Таблица 26. Настройки правил проброса портов

Поле	Описание
From	Выбор из какой зоны Firewall будет осуществляться проброс
Src Address	Указывается один IP адрес, с которого будет разрешено подключение к данному порту. Если ограничивать доступ к порту необходимости нет — поле следует оставить пустым
Src Port	Порт источника трафика, который «прослушивает» роутер на попытки установки соединения
Protocol	Выбор протокола, на который будет распространяться правило: TCP, UDP, TCP/UDP (оба протокола) или ALL (предназначен для организации DMZ зоны)
To	Выбор в какую зону Firewall будет осуществляться проброс
Dst Address	Ввод IP-адреса приемника трафика, на который роутер будет пересылать пакеты
Dst Port	Порт 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 рисунке 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!

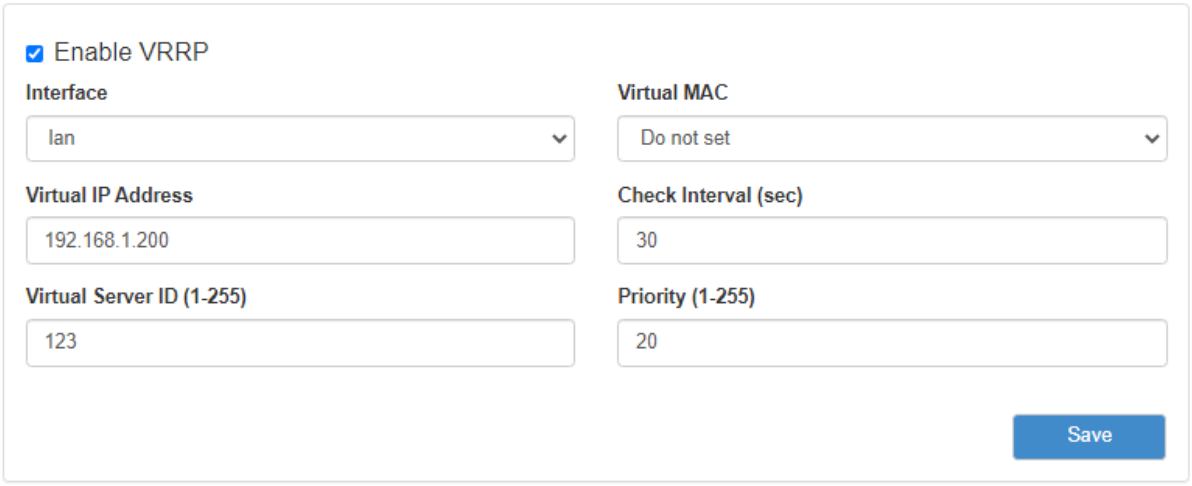


Рис. 34. Вкладка Services, раздел VRRP

Чтобы включить VRRP, поставьте галочку напротив **Enable VRRP** и задайте соответствующие настройки.

Таблица 27. Настройки правил проброса портов

Поле	Описание
Interface	Выбор интерфейса, через который будет работать VRRP. None – ничего не использовать или LAN — 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»

Таблица 27. Настройки правил проброса портов

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. Network Time Protocol

Раздел **Network Time Protocol** 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 ниже 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!

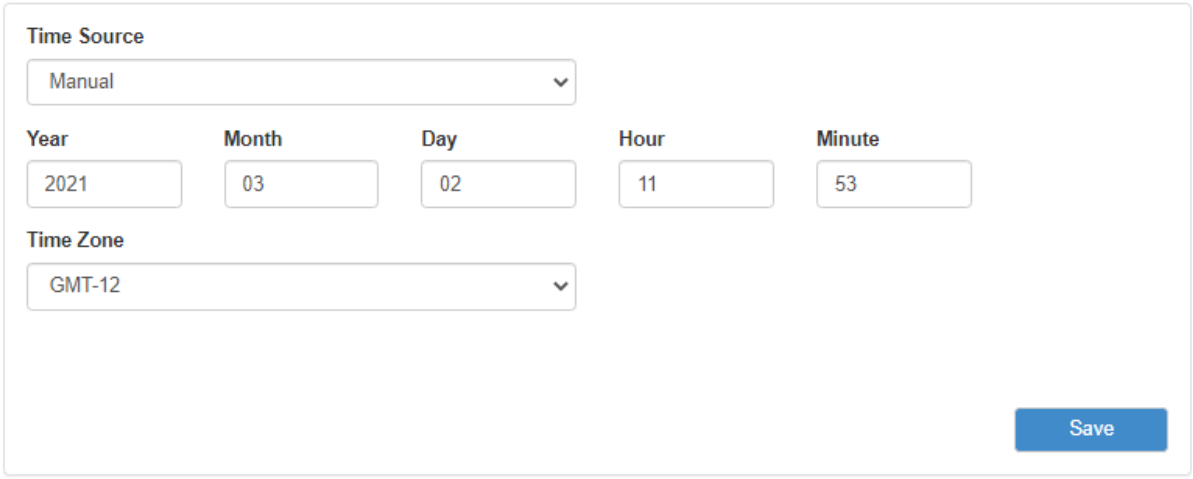


Рис. 35. Настройка времени в ручном режиме

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 ниже 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!

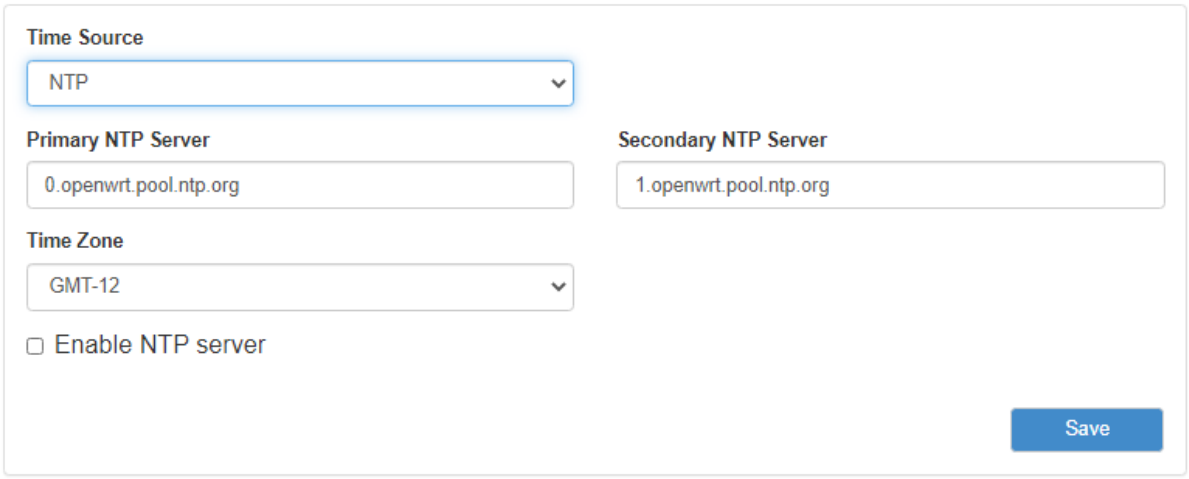


Рис. 36. Настройка времени в автоматическом режиме

5.4.7. Zabbix Agent

Раздел **Zabbix Agent** на вкладке Services предназначен для настройки мониторинга работы серверов и сетевого оборудования.

На роутерах iRZ серий R0, R2 и R4 для начала работы с агентом Zabbix требуется установить необходимые пакеты.

На роутере должна быть установлена версия прошивки 20.6 и выше.

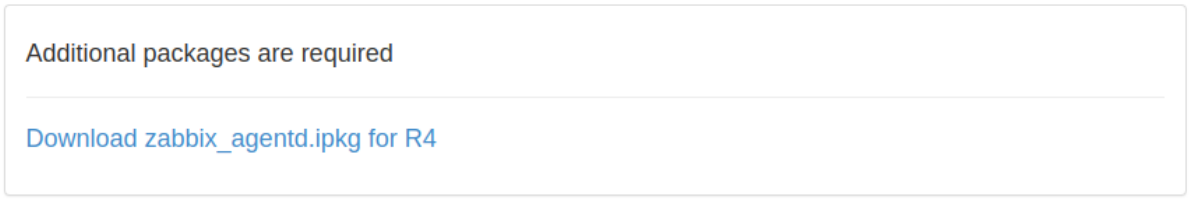


Рис. 37. Установка Zabbix Agent

Чтобы начать работу с агентом Zabbix, поставьте галочку напротив **Enable Zabbix**, а затем введите соответствующие настройки (см. таблицу).

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

На рисунке далее приведен пример настроек.

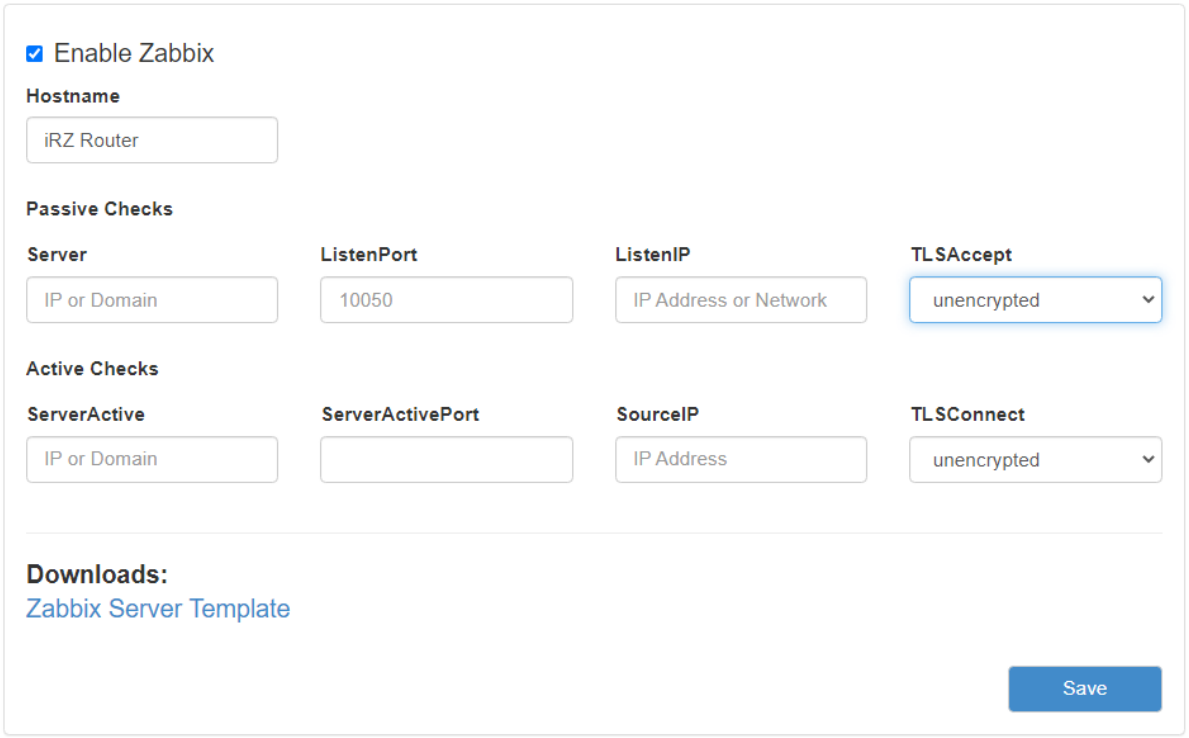


Рис. 38. Настройка Zabbix Agent

Для упрощения процесса настройки Zabbix-сервера и добавления сгруппированных элементов данных при создании узлов сети
скачайте с роутера шаблон (Download Zabbix Template).

Таблица 28. Настройка Zabbix Agent

Поле	Описание
Hostname	Уникальное, регистрозависимое имя хоста. Требуется для активных проверок и должно совпадать с именем узла сети указанном на сервере.
Passive Checks	
Server	IP адрес (или имя хоста) Zabbix-сервера. Входящие соединения будут приниматься только с хоста указанного в этом списке.
ListenPort	Агент будет слушать этот порт для подключений с сервера.
ListenIP	Агент будет слушать указанный адрес.
TLSAccept	Какие принимаются входящие подключения. Используется пассивными проверками. Можно указывать несколько значений, разделенных запятой: • unencrypted - принимать подключения без шифрования (по умолчанию) • psk - принимать подключения с TLS и pre-shared ключем (PSK) • cert - принимать подключения с TLS и сертификатом
Active Checks	
ServerActive	IP адрес (или имя хоста) Zabbix-сервера для активных проверок. Если параметр не указан, активные проверки отключены.
ServerActivePort	Порт Zabbix-сервера для активных проверок. Если порт не указывается, то используется порт по умолчанию.
SourceIP	Локальный IP адрес для исходящих подключений.
TLSConnect	Как агент должен соединяться с Zabbix-сервером или прокси. Используется активными проверками. Можно указать только одно значение: • unencrypted - подключаться без шифрования (по умолчанию) • psk - подключаться, используя TLS и pre-shared ключем (PSK) • cert - подключаться, используя TLS и сертификат

Обязательные настройки только Hostname и Server(PassiveCheck).

После выбора типа зашифрованного подключения к Zabbix-серверу появляются поля для добавления необходимых сертификатов и ключей.

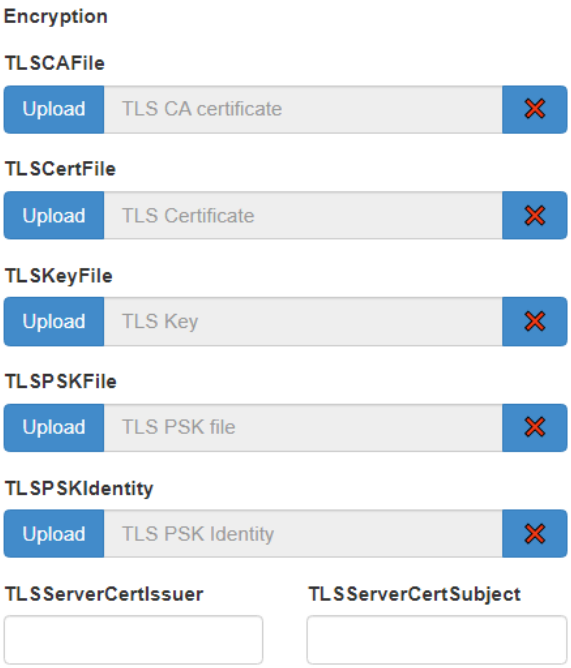


Рис. 39. Настройка Zabbix Agent, Encryption

При выборе psk заполняется только:

TLSPSKFile	Pre-shared ключ агента, используется для зашифрованных соединений с Zabbix-сервером.
TLSPSKIdentity	Строка идентификатор pre-shared ключа, используется для зашифрованных соединений с Zabbix-сервером.

При выборе cert заполняется:

TLSCAFile - обязательно	Сертификат верхнего уровня CA(и) для верификации сертификата узла, используется для зашифрованных соединений между Zabbix компонентами
TLSCertFile - обязательно	Сертификат или цепочку сертификатов, используется для зашифрованных соединений между Zabbix компонентами.
TLSKeyFile - обязательно	Приватный ключ агента, используется для зашифрованных соединений между Zabbix компонентами.
TLSServerCertIssuer - опционально	Разрешенный эмитент сертификата сервера (прокси).
TLSServerCertSubject - опционально	Разрешенная тема сертификата сервера (прокси).

5.4.8. SNMP

Раздел **SNMP** на вкладке **Services** предназначен для настройки системы мониторинга и управления роутером по протоколу SNMP.

На роутерах iRZ поддерживается две версии протокола SNMP – v2c и v3.

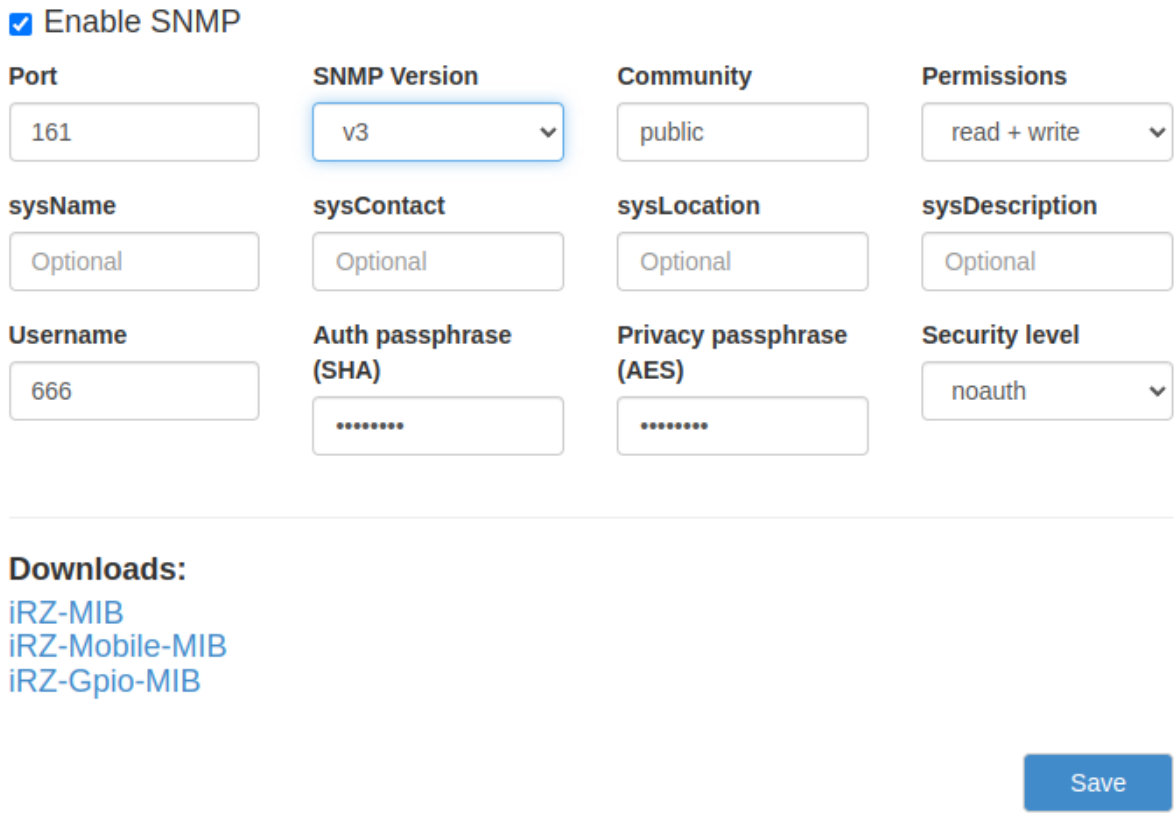


Рис. 40. Вкладка Services, раздел SNMP (v3)

Чтобы включить SNMP, поставьте галочку напротив **Enable SNMP**, а затем введите соответствующие настройки.

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

Таблица 29. 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

Таблица 29. Настройки SNMP

Permissions	v2c, v3	read - только чтение (мониторинг), read+write - мониторинг и управление GPIO
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 работе с устройством по протоколу SNMP: **Noauth** – авторизация на устройстве не установлена; **Auth** – установлена авторизация; **Priv** – установлена авторизация и шифрование данных при передаче по протоколу.

Внизу страницы в разделе **Downloads** находятся ссылки для скачивания MIB-файлов, содержащих информацию для SNMP-менеджера о том, какие параметры можно запросить или добавить.

Управление GPIO при помощи SNMP

Для начала работы в веб-интерфейсе роутера (Вкладка **Services**, раздел **SNMP**) нужно заполнить все необходимые поля и установить в разделе **Permissions** значение **read+write**.

Далее вся работа по управлению GPIO происходит **со стороны менеджера SNMP** (сервер мониторинга, компьютер - любое устройство, с которого производится запрос).

С помощью SNMP можно установить следующие параметры работы GPIO:

- направление: **IN** – работает как вход, **OUT** – выход
- уровень на выходе (для **OUT**): 0 - low, 1 - high
- debounce (для **IN**): значение в миллисекундах
- триггер (для **IN**): **RISE** – появление напряжения, **FALL** — пропажа напряжения, **BOTH** — любое из событий, **NONE** – события не отслеживаются

Событие, которое происходит при срабатывании триггера, по SNMP настроить нельзя. Его нужно настроить в веб-интерфейсе роутера во вкладке **Tools** - **GPIO**.

5.4.9. 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 ниже 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!

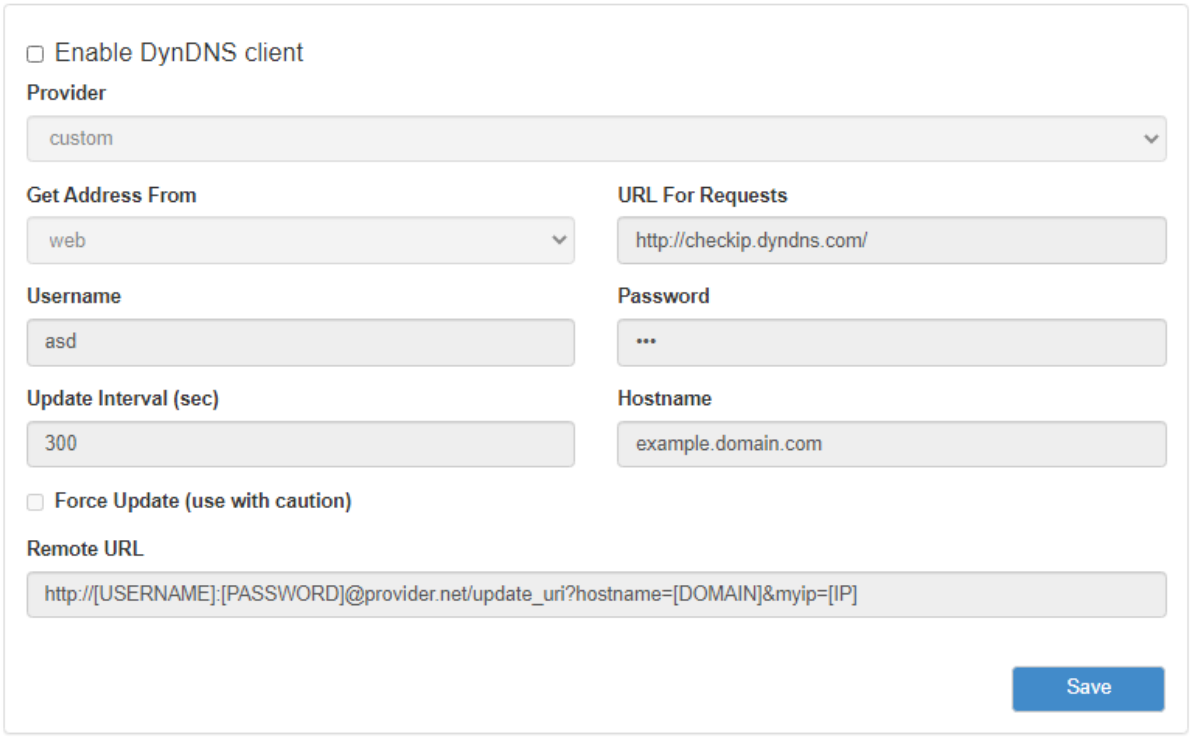


Рис. 41. Вкладка Services, раздел DynDNS

Чтобы включить DynDNS, поставьте галочку напротив **Enable DynDNS client** и настройте соответствующие параметры.

Таблица 30. Настройки DynDNS

Поле	Описание
Provider	Выбор провайдера услуги динамического DNS. В роутерах iRZ предустановлены основные настройки для нескольких распространенных провайдеров. Для настройки собственного сервера, выберите **Custom** и пропишите необходимые настройки

Таблица 30. Настройки DynDNS

Get Address From	Данная настройка отвечает за определение вашего динамического IP адреса. При выборе **WEB** 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 сервере
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. рисунок ниже.

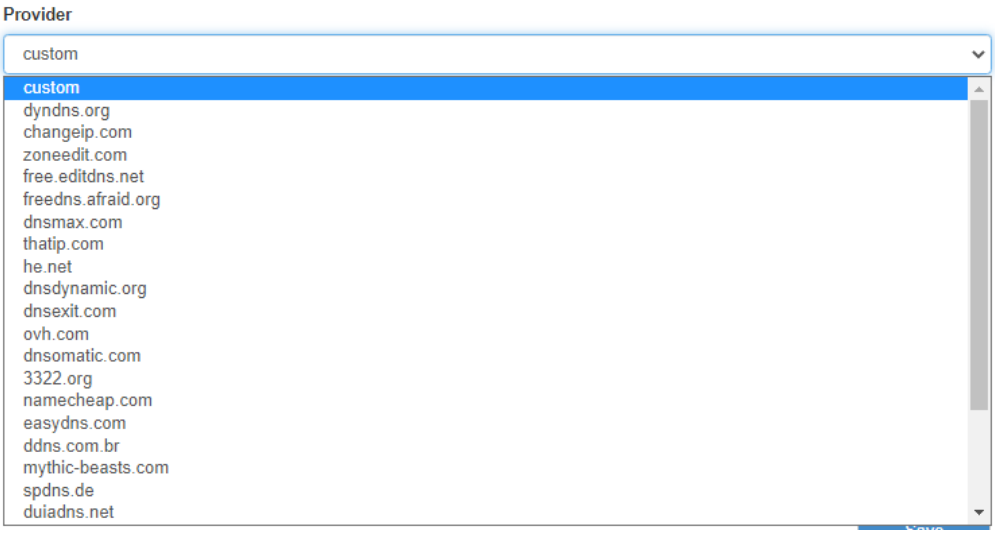


Рис. 42. Сервера DNS

5.4.10. 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 ниже 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!

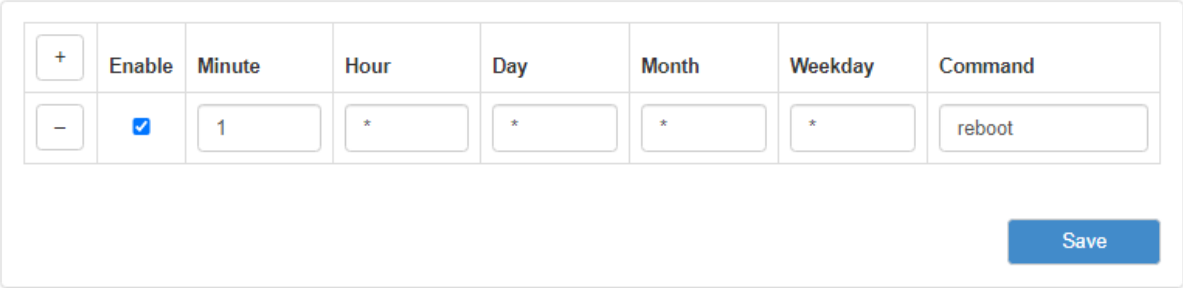


Рис. 43. Вкладка Services, раздел Crontabs

5.4.11. SMS

Раздел **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 рисунке.

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 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!

Для двухмодульных роутеров на странице отображается блок управления приоритетом модулей для отправки SMS **Priority of sending sms**. GSM-модули обозначены как **Modem 1** (GSM 1) и **Modem 2** (GSM 2). Приоритет настраивается при помощи стрелок "вверх" и "вниз", расположенных рядом с каждой строчкой.

Для отправки используется модуль с высшим приоритетом. При невозможности отправки SMS через него сообщение отправляется через модуль с меньшим приоритетом.

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

1. Зайдите в раздел **Services** → **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.

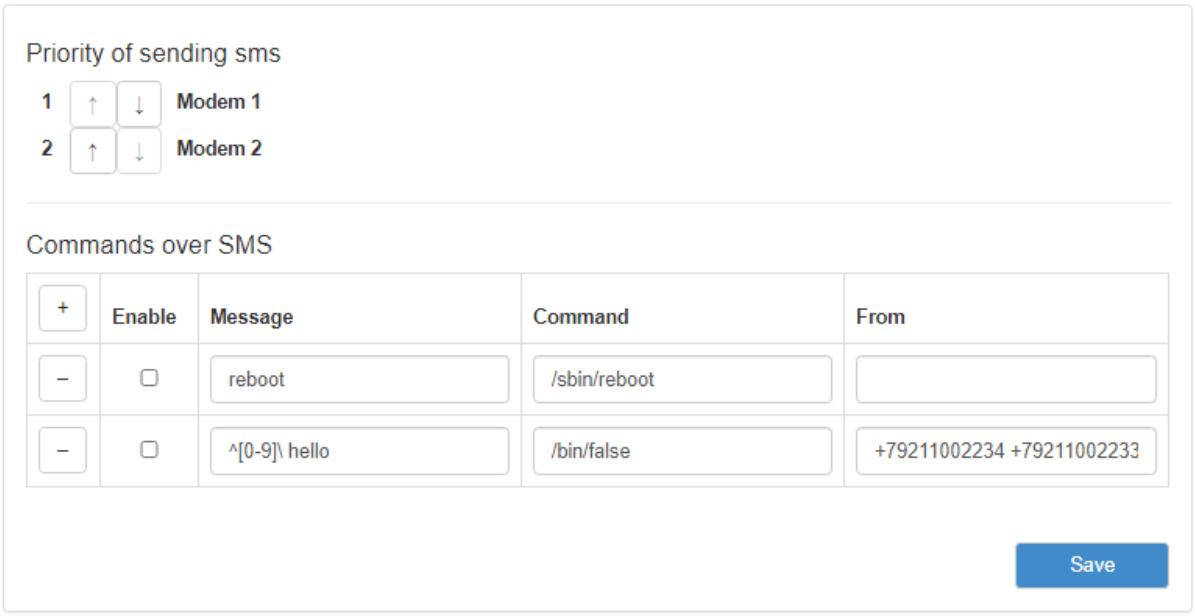


Рис. 44. Вкладка Services, раздел SMS

5.4.12. Serial ports

Раздел Serial Ports на вкладке Services предназначен для настройки работы роутера с портами RS232, и RS485.

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 следующие режимы работы:

Server

Роутер ждет входящего подключения на указанный порт, устанавливается соединение и начинается передача данных;

Client

Роутер устанавливает соединение по указанному IP-адресу и порту, и начинает передачу данных.

Server/Client Modbus TCP to RTU (для серий R2 и R4)

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. При этом роутер не выступает ни в роле ведущего, ни в роле ведомого. Он просто передаёт данные. Роли ведущего и ведомого выполняют непосредственно оконечные устройства

Роутер выполняет функцию преобразования промышленных протоколов Modbus RTU в протокол Modbus TCP и обратно, то есть выступает в роли шлюза, обеспечивая прозрачный канал передачи данных между устройствами.

Режимы Server MODBUS TCP to RTU и Client MODBUS TCP to RTU выбираются комбинацией соответствующих режимов **Local Proto** и **Remote Proto**. Выбором режима Server/Client выбирается кто устанавливает сессию, что позволяет в том числе самим устанавливать Modbus TCP to RTU соединение к удалённому узлу.

NTRIP Client

Протокол NTRIP (Networked Transport of RTCM via Internet Protocol) протокол предназначенный специально для передачи спутниковых данных через Интернет. Основан на протоколе передачи гипертекстовых файлов.

В протокол NTRIP входят следующие составные части: сервер, вещатель (кастер) и клиент. Их взаимодействие происходит следующим образом:

- NTRIP-сервер подключается к источнику поправок (базовая станция) и направляет поток корректирующей информации NTRIP-кастеру. Для соединения с кастером сервер сообщает точку доступа, через которую будет происходить обмен поправками, и пароль от нее.
- Поправки поступают на указанную точку доступа кастера.
- Ровер (подвижный приемник) обращается к NTRIP-клиенту за поправками, а клиент обращается на NTRIP-кастер, указывая его IP-адрес, порт, точку доступа (список точек доступа), логин и пароль.
- При успешном подключении клиента к кастеру происходит передача поправок с базовой станции на ровер на основании указанной точки доступа.

Чтобы включить порт, нажмите напротив него Edit, поставьте галочку Enable Port via TCP и укажите настройки для его работы (см. таблицу).

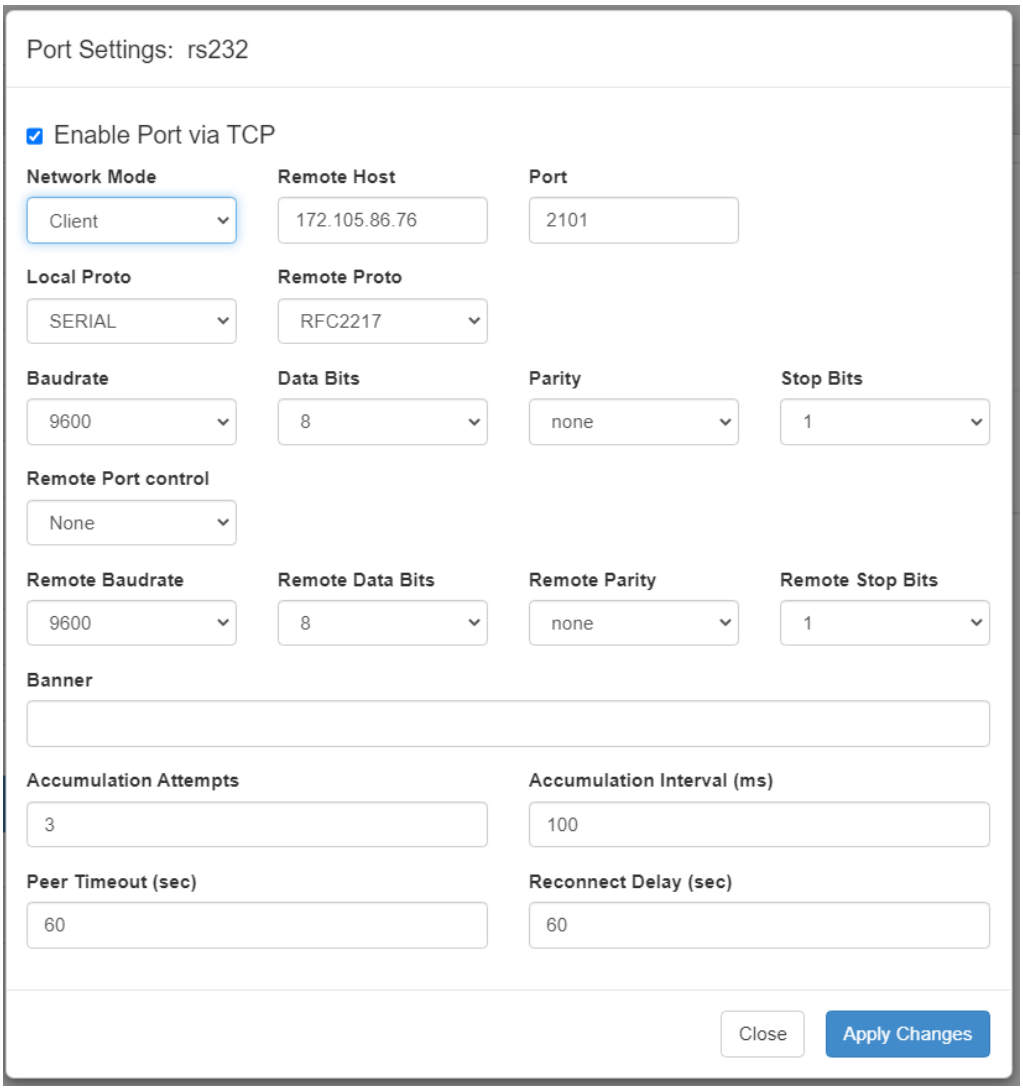


Рис. 45. Вкладка Services, раздел Serial Ports, пример настроек порта RS232

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

Таблица 31. Настройки Port via TCP

C – клиент, S – сервер, N — NTRIP Client

Поле	Режим	Описание
Network Mode	C, S, N	Режим работы порта: C – клиент, S – сервер, N — NTRIP Client
Remote Host	C, N	IP-адрес сервера, к которому будет подключаться устройство для передачи данных
Port	C, S, N	Порт, через который будет осуществляться передача данных
Local Proto	C, S	Протокол взаимодействия для локального интерфейса: SERIAL - используется как последовательный порт, MODBUS RTU - используется как Modbus RTU интерфейс
Remote Proto	C, S	Протокол взаимодействия с удаленным интерфейсом: • RAW (сокет, просто отдаёт те данные, которые получил) • RFC2217 - используется для передачи данных с возможностью управления последовательным портом • MODBUS TCP - используется как Modbus TCP интерфейс
Baudrate	C, S, N	Скорость передачи данных через порт, бод
Data Bits	C, S, N	Количество бит блока, используемых при передаче данных
Parity	C, S, N	Режим контроля четности бит в передаваемых блоках: None – без проверки, Odd – проверка на нечетность, Even – проверка на четность
Stop Bits	C, S, N	Количество стоп-бит блока, используемые для определения конца блока
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

Для работы в режиме NTRIP Client необходимо скачать и установить дополнительный пакет.

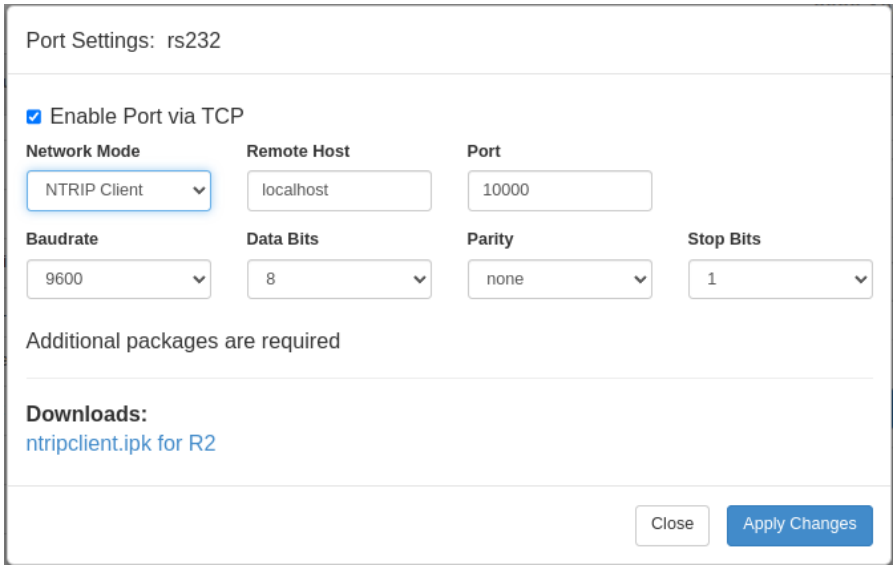


Рис. 46. Вкладка Services, раздел Serial Ports, NTRIP pack

И заполнить дополнительные настройки.

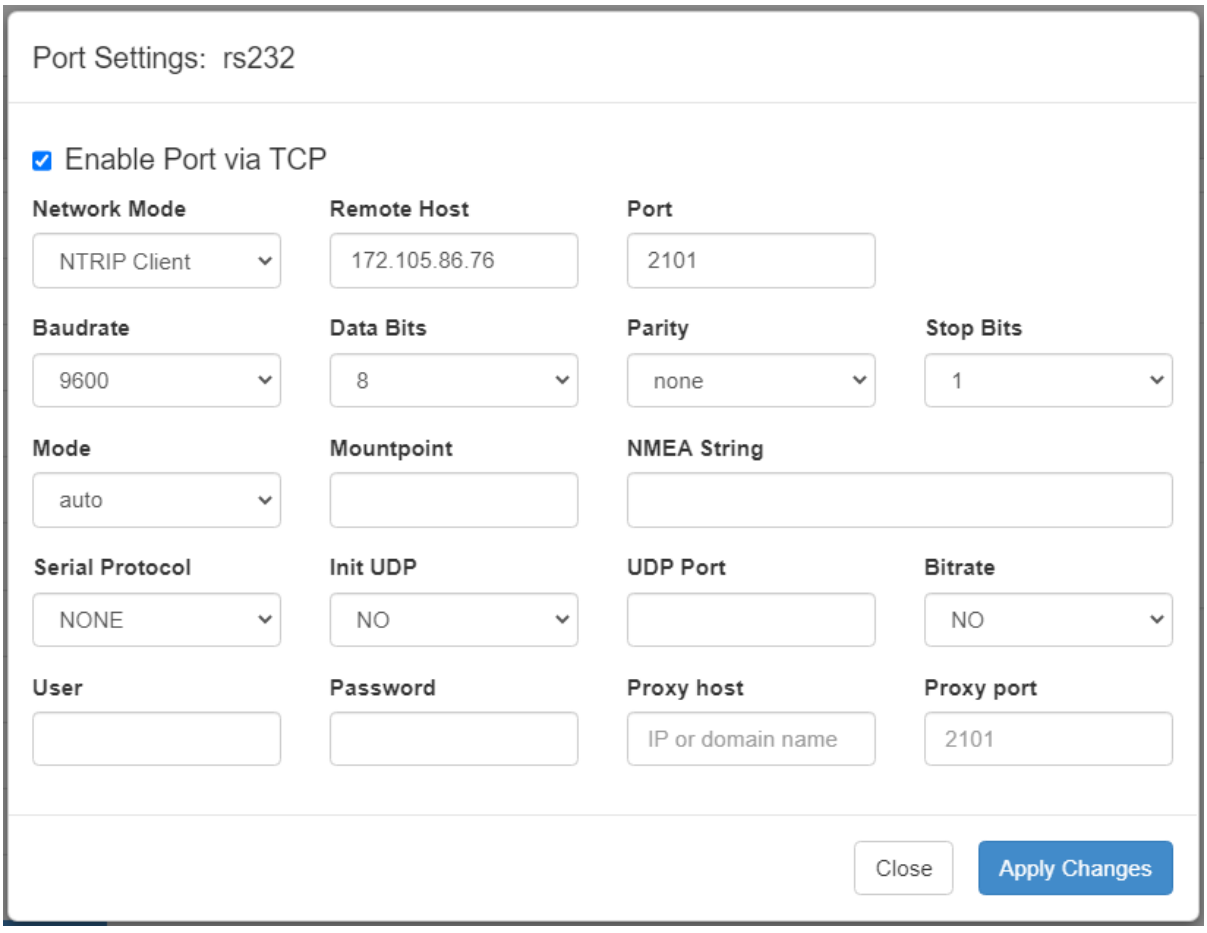


Рис. 47. Вкладка Services, раздел Serial Ports, NTRIP Client

Таблица 32. Настройки для NTRIP Client

Поле	Режим	Описание
Mode	N	Режим формата запроса данных: • auto - автоматическое определение (по умолчанию) • ntrip1 - NTRIP Version 1.0 Caster • http - NTRIP Version 2.0 Caster in TCP/IP mode • rtsp - NTRIP Version 2.0 Caster in RTSP/RTP mode • udp - NTRIP Version 2.0 Caster in UDP mode
Mountpoint	N	Точка доступа или таблица источников поправок
NMEA String	N	NMEA строка, которая содержит навигационную информацию
Serial Protocol	N	Протокол, используемый при передаче данных
Init UDP	N	Отправка начального UDP пакета для обработки файерволом
UDP Port	N	Номер локального UDP порта, используемого для входящего соединения
Bitrate	N	Вывод сообщения со значением текущего битрейта в системный лог
User	N	Имя пользователя
Password	N	Пароль
Proxy host	N	IP-адрес прокси-сервера
Proxy port	N	Порт прокси-сервера

5.4.13. Application Layer Gateway

Раздел Application Layer Gateway (ALG) на вкладке Services предназначен для настройки работы роутера со следующими протоколами, требующими ALG:

- FTP
- PPTP
- SIP
- SNMP
- TFTP
- H323
- RTSP

Для работы функционала необходимо установить нужный протокол во включенное состояние и настроить проброс соответствующего порта на вкладке Port Forwarding.

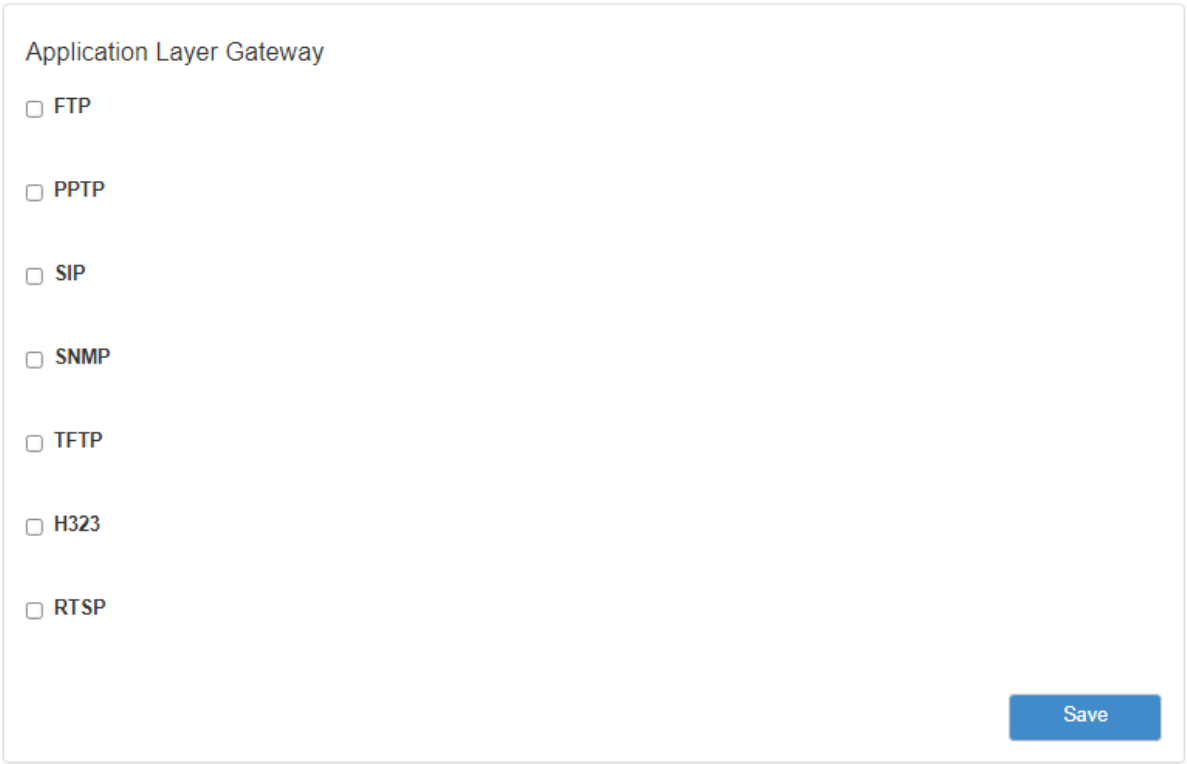


Рис. 48. Вкладка Services, раздел Application Layer Gateway

5.4.14. Queues

Раздел **Services** – **Queues** предназначен для настройки правил, по которым будет обрабатываться исходящий маркированный трафик с заданного интерфейса.

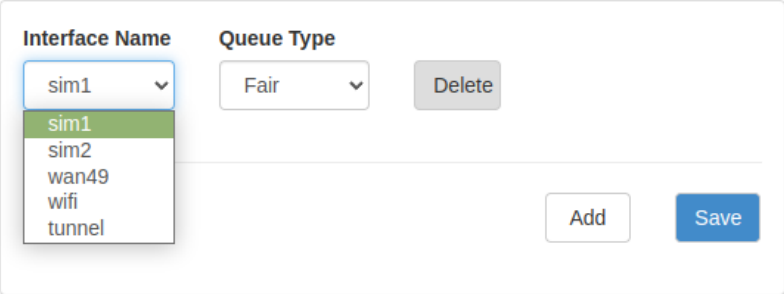


Рис. 49. Настройки Services – Queues

Таблица 33. Настройки правил для работы с QoS

Поле	Описание
Interface Name	Интерфейс, трафик с которого будет обрабатываться
Queue Type	Механизм, в соответствии с которым будет обрабатываться трафик

На данный момент реализовано два механизма:

Priority

Трафик раскладывается в несколько очередей согласно своему классу — приоритету (например, BE, AF1-4, EF, CS6-7). Алгоритм перебирает одну очередь за другой.

Сначала он пропускает все пакеты из самой приоритетной очереди, потом из менее, потом из менее. И так по кругу.

Алгоритм не начинает изымать пакеты низкого приоритета, пока не пуста высокоприоритетная очередь.

Если в момент обработки низкоприоритетных пакетов приходит пакет в более высокоприоритетную очередь, алгоритм переключаются на неё и только опустошив её, возвращается к другим.

Fair

Механизм Fair извлекает одинаковый объём данных из каждой очереди по порядку.

Порядок формирования очереди включает Fair Queuing и схему CoDel AQM (активное управление очередью с управляемой задержкой). Алгоритм использует стохастическую модель для классификации входящих пакетов в различные потоки. Каждый такой поток управляется формированием очереди с контролируемой задержкой (CoDel).

5.5. Раздел «Tools»

5.5.1. Access

Раздел **Access** на вкладке **Tools** предназначен для настройки доступа управления роутером.

По умолчанию на устройстве веб-интерфейс доступен только по HTTP.

Всего доступны три варианта получения доступа к роутеру. Для выбора одного из вариантов нужно поставить галочку напротив соответствующего пункта и в нижнем поле ввести порт (изначально указаны значения по умолчанию):

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

Чтобы включить авторизацию на устройстве через сервер авторизации TACACS+ поставьте галочку напротив **Enable TACACS+ for SSH** (только для роутеров серии R4).

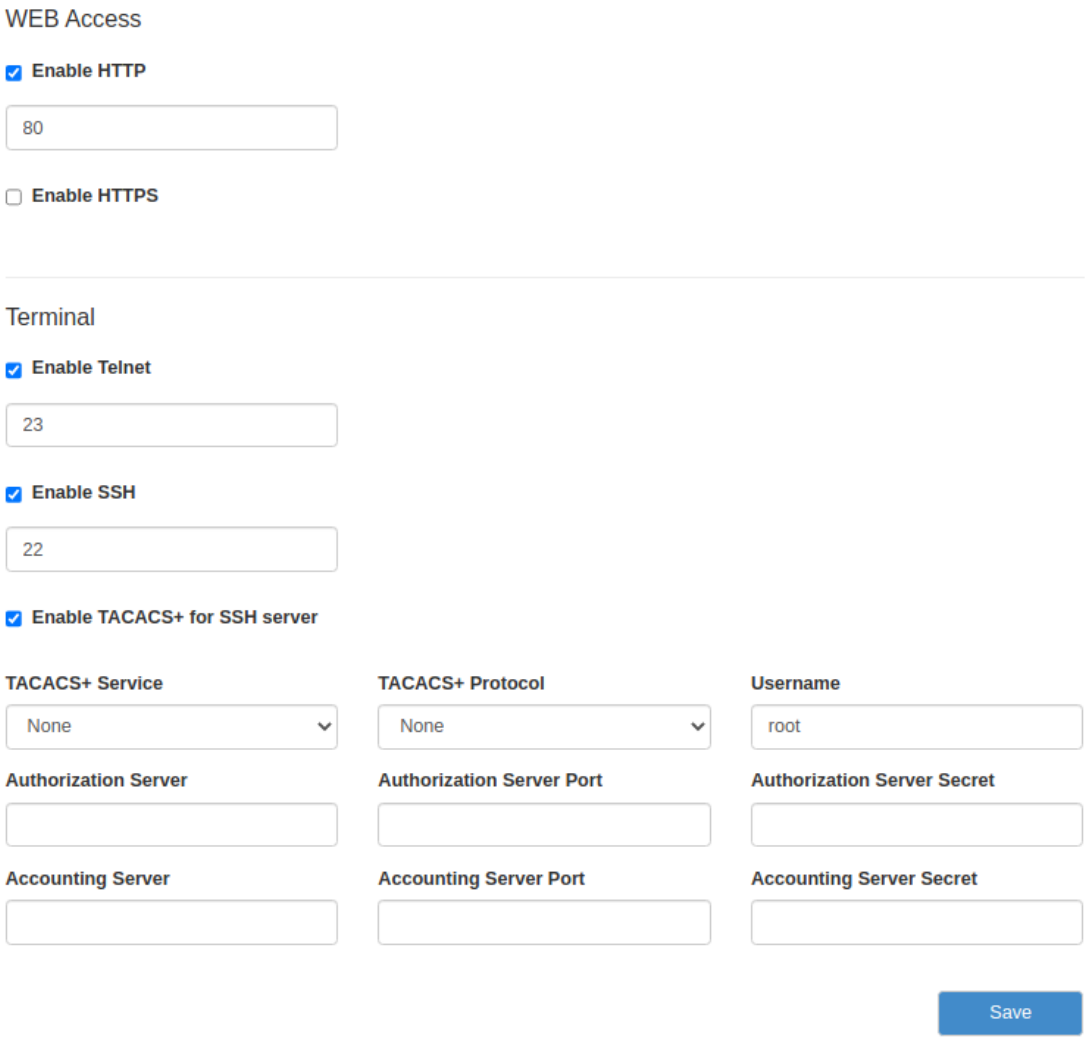


Рис. 50. Вкладка Tools, раздел Access

Чтобы подключаться к web-интерфейсу роутера через защищённый протокол **HTTPS**, необходимо загрузить на роутер свой сертификат и частный ключ. Для их загрузки используются соответственно поля **Public Key** и **Private Key**.
Если оставить поля пустыми на устройстве будет сгенерирован самоподписаный сертификат, при этом используемый вами браузер может уведомить о невозможности проверить сертификат.

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

5.5.2. iRZ Link Client

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

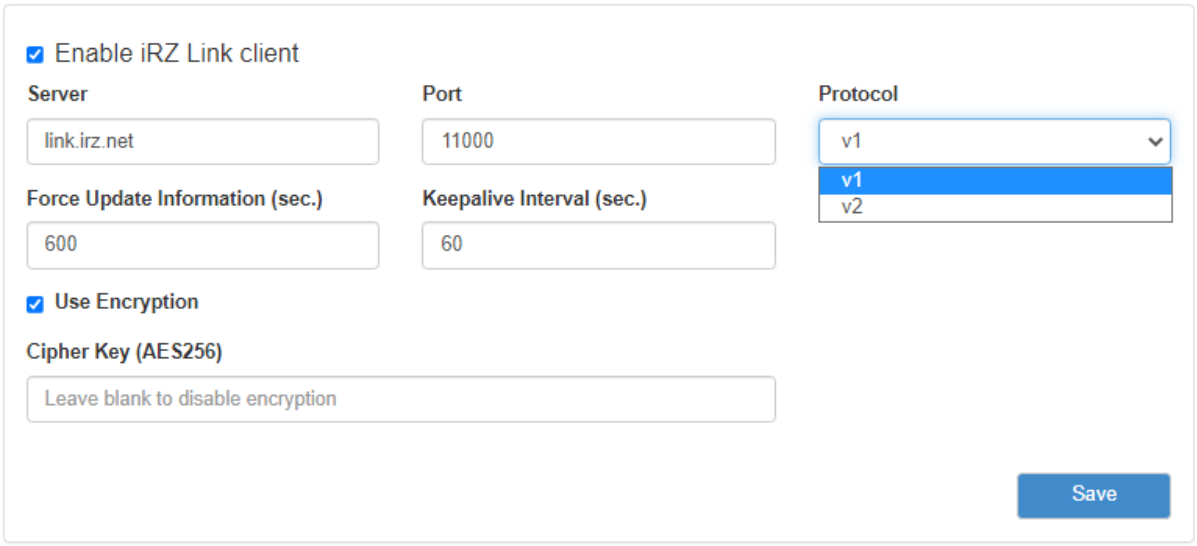


Рис. 51. Вкладка Tools, раздел iRZ Link Client

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. Поле **Protocol** необходимо для выбора протокола взаимодействия с Link/Link2 (v1 - совместим с Link и не совместим с Link2, v2 - совместим с Link2 и ограничено совместим с Link). 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!

5.5.3. Password

Раздел 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 ниже представлен пример полей для заполнения.

Рис. 52. Вкладка Tools, раздел Password

5.5.4. Hostname

Раздел **Hostname** 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 ниже представлен пример полей для заполнения.

Рис. 53. Вкладка Tools, раздел Unit Name

5.5.5. Temperature (только для роутеров серии R2)

Раздел **Temperature** предназначен для работы с подключаемыми датчиками температуры. Для того чтобы включить эту опцию, необходимо поставить галочку напротив Read Temperature Sensors и нажать кнопку Save.

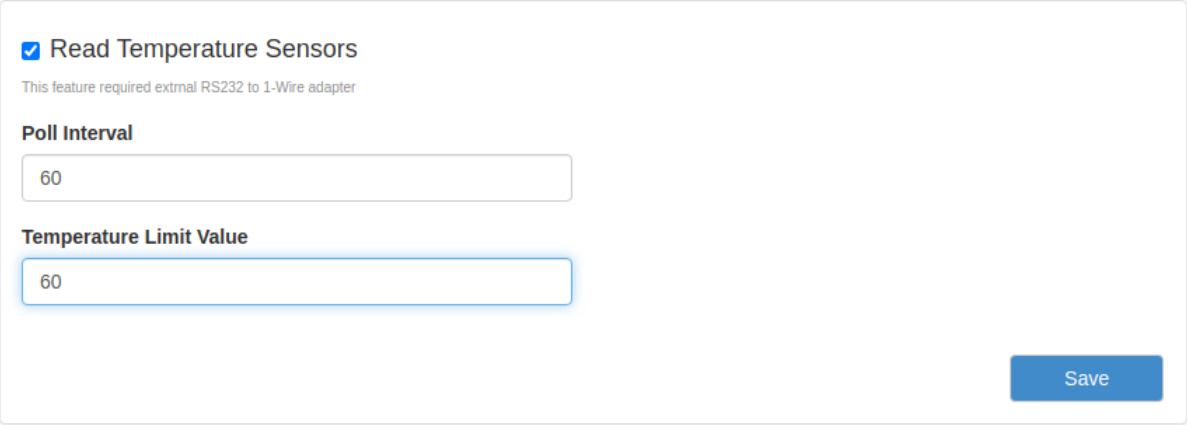


Рис. 54. Вкладка Tools, раздел Temperature

Таблица 34. Настройки Tools - Temperature

Поле	Ед. Изм.	Описание
Poll interval	сек	Интервал опроса датчиков. Опрос датчика может занимать пару секунд, поэтому рекомендуется при количестве датчиков более 5 устанавливать интервал опроса не меньше 10 сек, для 15 датчиков – не меньше 20 сек.
Temperature Limit Value	ºC	Предельное значение температуры. Используется для запуска пользовательских скриптов.

Подключение датчиков температуры (например, DS18B20) к интерфейсу RS232 роутеров iRZ серии R2 осуществляется с помощью преобразователя интерфейсов 1-Wire/RS232 производства iRZ. Подключение внешних устройств к преобразователю осуществляется через клеммную колодку, в соответствии с инструкцией на преобразователь. Одновременно возможно подключение до 30 датчиков.

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 двухмодульных роутеров предусмотрен выбор GSM-модуля, при помощи которого будет отправлено сообщение.

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. В поле **Modem to send** укажите модуль, при помощи которого должно быть отправлено SMS (только для двухмодульных роутеров);
4. Нажмите кнопку **Send**, внизу страницы.

На рисунке представлен пример полей для заполнения.

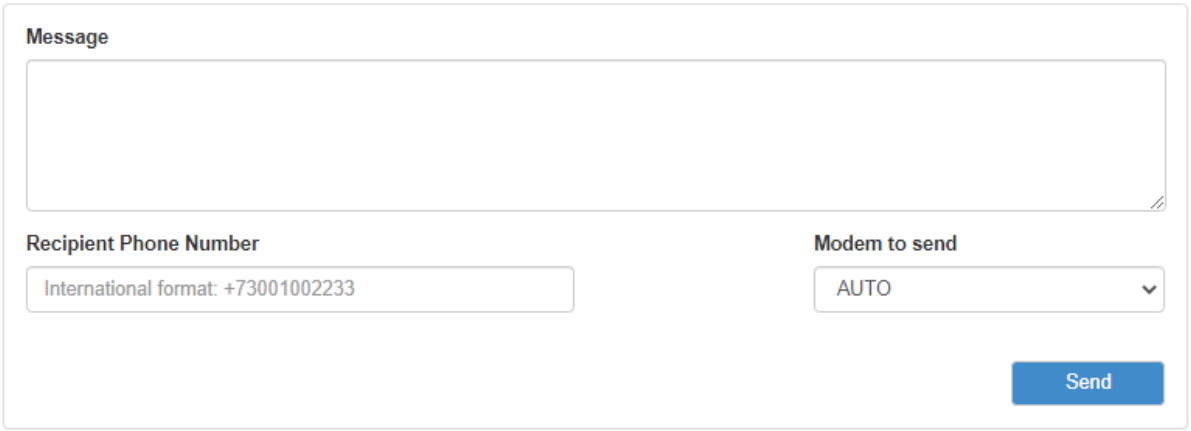


Рис. 55. Вкладка Tools, раздел Send SMS

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 рисунке представлен пример полей для заполнения.

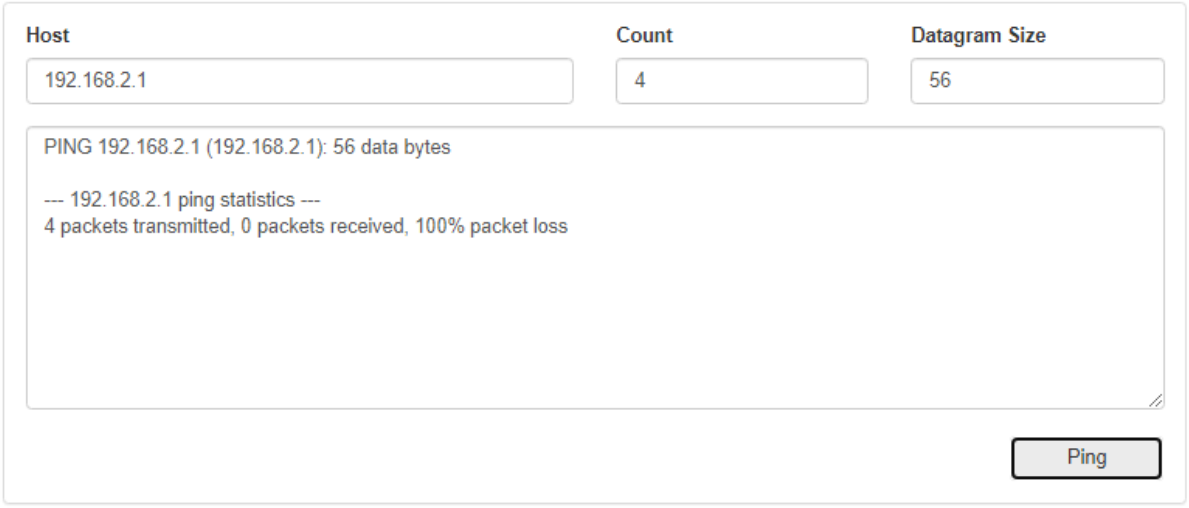


Рис. 56. Вкладка Tools, раздел Ping

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 Host**, 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.

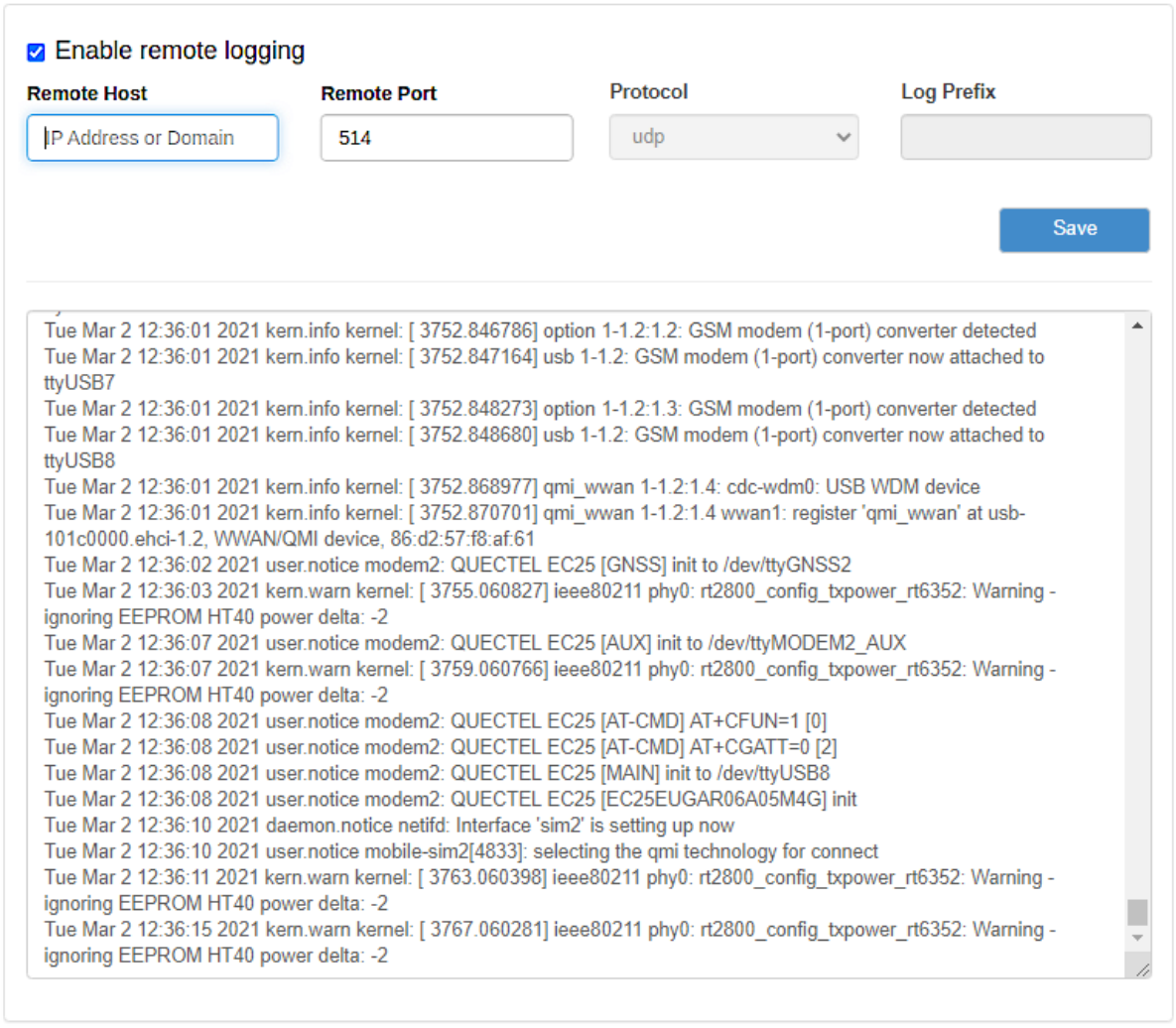


Рис. 57. Вкладка Tools, раздел System Log

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.

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

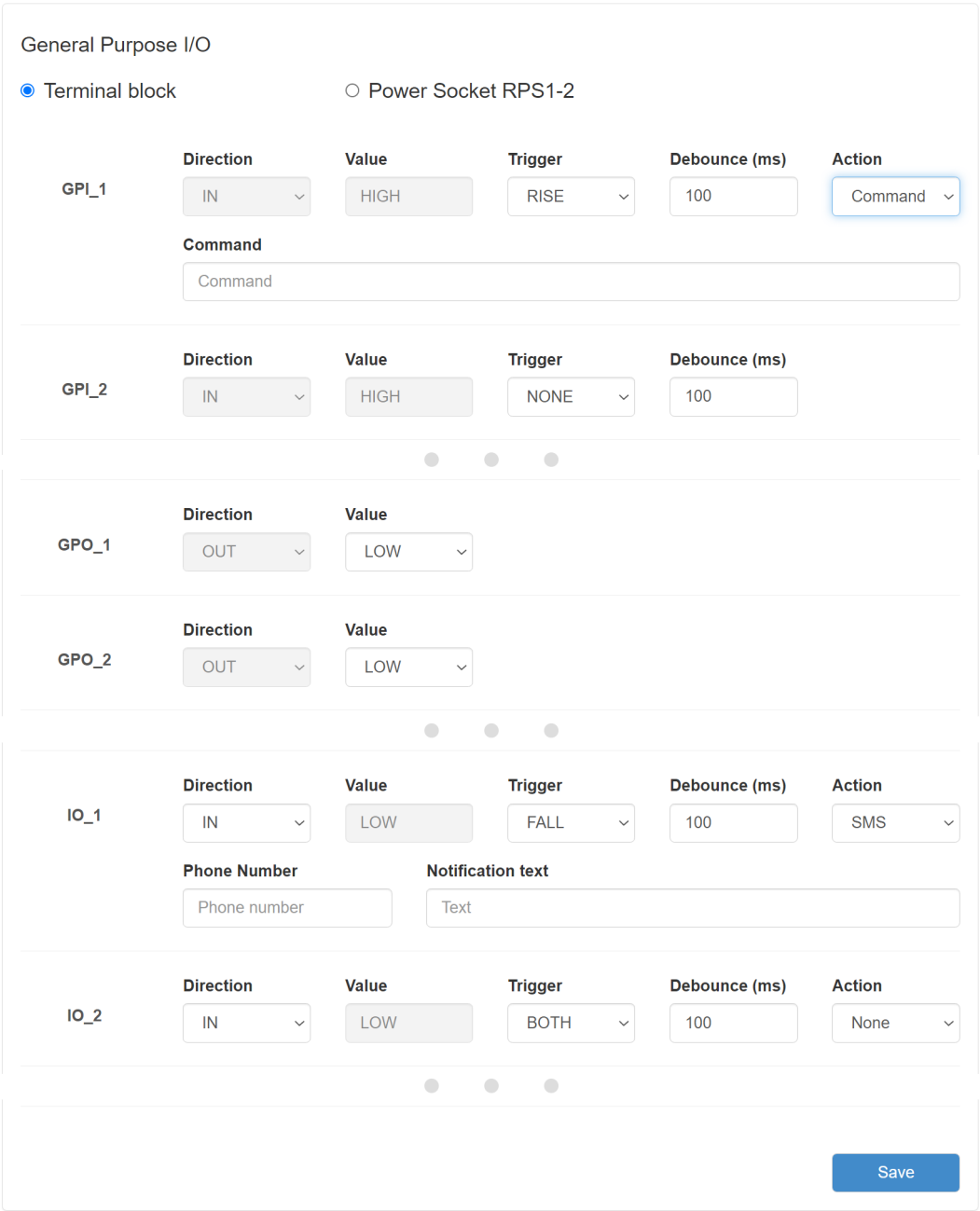


Рис. 58. Вкладка Tools, раздел GPIO

Физические характеристики и число портов GPIO для конкретного роутера можно узнать в руководстве пользователя и сайте производителя.

Подавать напряжение на вход GPIO можно **только после включения** роутера. Несоблюдение данного требования ведёт к выходу роутера из строя и лишению владельца права на гарантийное обслуживание.

На вход GPIO нельзя подавать напряжение превышающее напряжение питания роутера.

В случае если к GPIO не подключен резистор 10 кОм - нельзя допускать разности напряжения питания роутера и напряжения, подаваемого на вход GPIO. Если резистор в 10 кОм установлен, то разность напряжения питания роутера и напряжения, подаваемого на вход GPIO, допускается.

Настройки портов GPIO представлены в таблице ниже.

Таблица 35. Настройки портов GPIO

Поле	Описание
IO_1, GPI_2, GPO_4 …	Имена входов/выходов
Direction	Выбор направления работы: **IN** – работает как вход, **OUT** – выход
Value	Уровень выходного сигнала (только для выходов): **HIGH** – высокое напряжение, **LOW** – низкое
Trigger	Событие на порту (триггер): **RISE** – появление напряжения на порту, **FALL** — пропажа напряжения на порту, **BOTH** — любое из событий, **NONE** – события не отслеживаются
Debounce (ms)	Нивелирует ложные срабатывания из-за электромагнитных наводок, измеряется в миллисекундах
Action	Событие, которое происходит при срабатывании триггера (только для IN): **None** — ничего не происходит, **Command** — выполняется заданная команда, **SMS** — отправляется SMS на указанный номер
Command	Поле для указания команды (для **Action - Command**)
Phone Number	Поле для указания номера телефона, на который должно быть отправлено SMS (для **Action - SMS**)
Notification text	Текст SMS (для **Action - SMS**)

При вводе команды в поле Command можно использовать переменные, представленные в таблице ниже.

Таблица 36. Список переменных для поля Command

Поле	Описание
%%GPIO%%	имя GPIO, например IO_2
%%VALUE%%	уровень напряжения на порту, 1 или 0
%%TRIGGER%%	триггер, по которому сработало событие, RISE/FALL/BOTH
%%DEBOUNCE%%	длительность изменения состояния GPIO, превышение которой ведёт к срабатыванию события
%%TIMESTAMP%%	время в формате timestamp с момента запуска устройства
%%SERIAL%%	серийный номер устройства
%%DATE%%	дата и время на устройстве

Пример команды:

send-sms "79xxxxxxxxx" "gpio %%GPIO%% value is %%VALUE%%"

При срабатывании триггера на указанный номер телефона будет отправлено сообщение о том, что определенный порт GPIO переключился в определенное состояние. Какой именно порт - это переменная %%GPIO%% , в какое именно состояние - это переменная %%VALUE%%

Управление GPIO при помощи SNMP
Начиная с версии прошивки 20.6 доступно управление GPIO по протоколу SNMP. Для использования данной функции нужно внести соответствующие настройки в разделе **Services** - **SNMP**. Более подробная информация находится в разделе Управление GPIO при помощи SNMP.

5.5.10. Управляемый блок розеток RPS1-2

Для управления блоком розеток RPS1-2 при помощи GPIO в интерфейсе предусмотрен пункт **Power Socket RPS1-2**

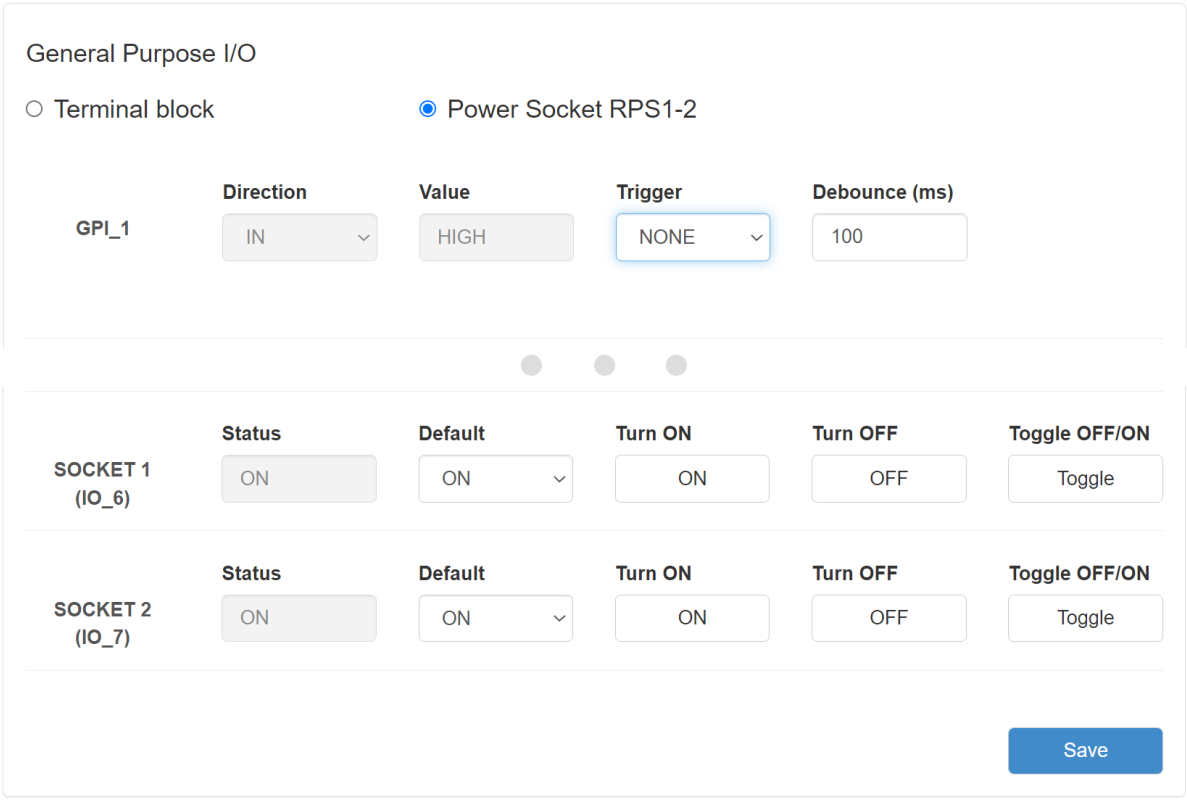


Рис. 59. Вкладка Tools, раздел GPIO, Power Socket RPS1-2

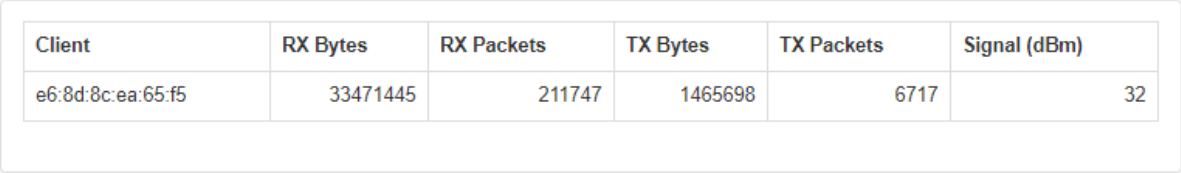
Значения полей представлены в таблице ниже.

Таблица 37. Настройки GPIO для работы с Управляемым блоком розеток RPS1-2

Поле	Описание
Status	Текущее состояние розетки
Default	Состояние, в котором розетка должна находиться по умолчанию при включении роутера
Turn ON	Включить розетку (при этом поле Status также поменяется на ON)
Turn OFF	Выключить розетку (при этом поле Status также поменяется на OFF)
Toggle OFF/ON	Выключить и включить розетку (для т.н. "перезагрузки по питанию" подключенного к розетке устройства)

5.5.11. 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 представлен пример страницы.



Client	RX Bytes	RX Packets	TX Bytes	TX Packets	Signal (dBm)
e6:8d:8c:ea:65:f5	33471445	211747	1465698	6717	32

Рис. 60. Вкладка Tools, раздел Wi-Fi Clients (роутер с Wi-Fi-модулем)

Таблица 38. 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.

5.5.12. Reboot

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

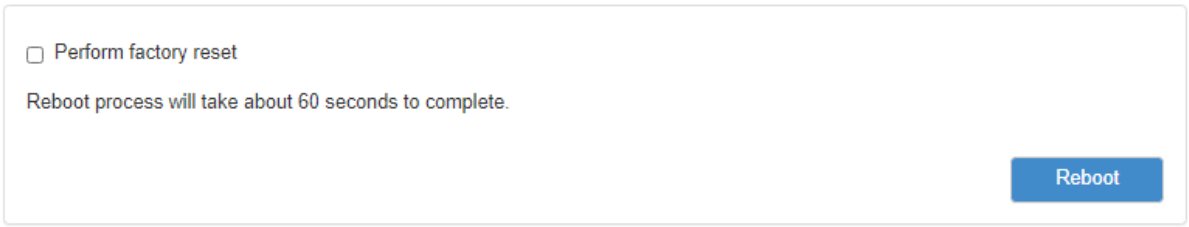


Рис. 61. Вкладка Tools, раздел Reboot

5.5.13. Management

В данном разделе пользователю предоставляется возможность сохранения всех сделанных настроек в файл, восстановление из файла, возможность установить дополнительный программный пакет или обновить версию прошивки роутера. Пример страницы приведён на рисунке.

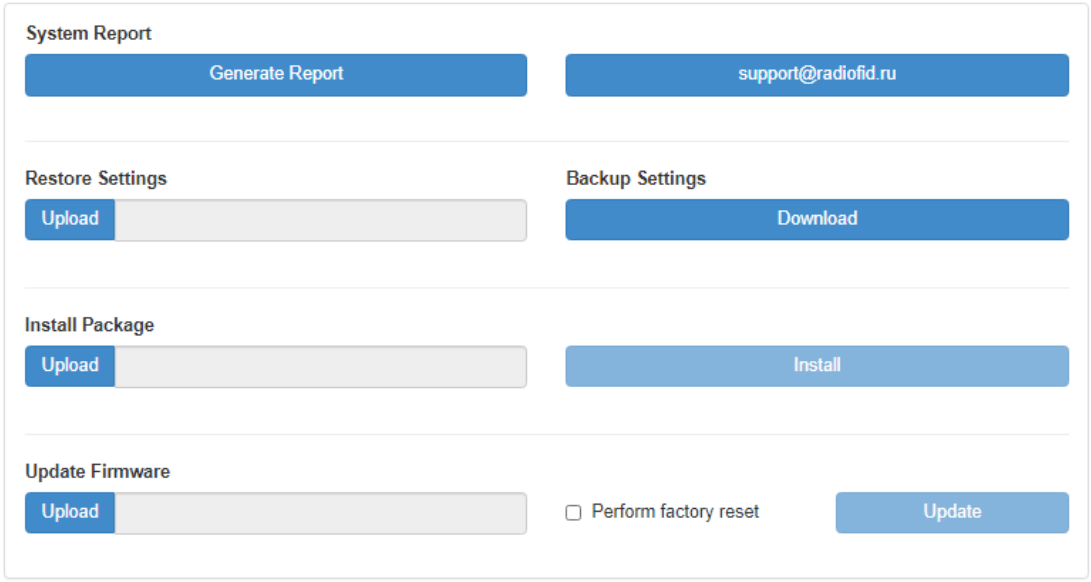


Рис. 62. Вкладка Tools, раздел Management

Получение репорт-файла.
Нажмите кнопку Generate Report и роутер предложит вам сохранить тектовый файл, в котором собраны логи работы роутера и его настроки. 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. Для удобства пользователей к имени файла добавляется серийный номер устройства и версия прошивки.

Загрузка сохраненных настроек устройства.
Нажмите кнопку **Upload** в подразделе **Restore Settings** и выберите ранее сохраненный файл с настройками. Если версия сохраненных настроек не совпадает с версией прошивки, установленной в данный момент на роутере, настройки будут применены, но пользователь получит уведомление о том что полная работоспособность всех настроек на этой версии прошивки не гарантируется.

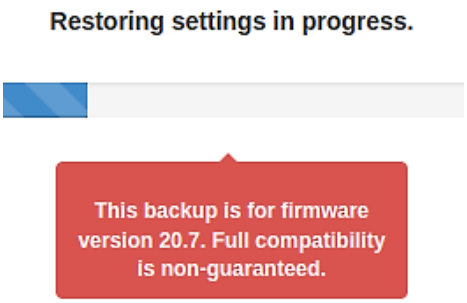


Рис. 63. Вкладка Tools, раздел Management, загрузка сохраненных настроек

Сохраняемые настройки индивидуальны для каждого роутера! При применении сохраненных настроек от одного устройства для других устройств они применяются **полностью** (включая такие индивидуальные параметры исходного устройства как MAC-адреса, SSID Wi-Fi и прочее).

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**.

Отключение питания роутера в момент обновления прошивки или сброса к заводским настройкам может привести к потере работоспособности устройства.

6. Контакты

Новые версии прошивок, документации и сопутствующего программного обеспечения можно получить, обратившись 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
Telegram	@irzhelpbot

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

В случае возникновения проблемной ситуации, при обращении в техническую поддержку, следует указывать версию программного обеспечения, используемого в роутере. Так же рекомендуется к письму прикрепить журналы запуска проблемных сервисов, снимки экранов настроек и любую другую полезную информацию. Чем больше информации будет предоставлено сотруднику технической поддержки, тем быстрее он сможет разобраться в сложившейся ситуации.

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

Нарушение условий эксплуатации (ненадлежащее использование роутера) лишает владельца устройства права на гарантийное обслуживание.

7. 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 1: 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