Руководство пользователя

по встроенному ПО роутеров

Содержание

1. Введение

1.1. Описание документа

Настоящий документ содержит исчерпывающую информацию, необходимую для эксплуатации Встроенного программного обеспечения для роутеров.

Руководство содержит описание последовательность действий, обеспечивающих работу с ПО, описание всех доступных пользователю функций, настроек и способов, с помощью которых пользователь осуществляет эксплуатацию ПО.

1.2. Версия встроенного обеспечения

Актуальная (текущая) версия встроенного ПО

- роутеры серии R0: R0-v20.4.3 (2022-09-20)
- роутеры серии R2: R2-v20.4.3 (2022-09-20)
- роутеры серии R4: R4-v20.4.3 (2022-10-07)

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.

GSM – стандарт сотовой связи («СПС-900» в РФ);

GPRS – стандарт передачи данных в сетях операторов сотовой связи «поколения 2.5G» основанный на пакетной коммутации (до 56 Кбит/с);

EDGE – преемник стандарта GPRS, представитель «поколения 2.75G», основанный на пакетной коммутации (до 180 Кбит/с);

HSPA (HSDPA, HSUPA) – технология беспроводной широкополосной радиосвязи, использующая пакетную передачу данных и являющаяся надстройкой к мобильным сетям WCDMA/UMTS, представитель «поколения 3G» (HSUPA - до 3,75 Мбит/с, HSDPA - до 7,2 Мбит/с);

WCDMA – стандарт беспроводной сотовой связи;

3G - общее описание набора стандартов, описывающих работу в широкополосных мобильных сетях UMTS и GSM: GPRS, EDGE, HSPA;

IP-сеть – компьютерная сеть, основанная на протоколе IPv4 (Internet Protocol) - межсетевой протокол 4 версии. IP-сеть позволяет объединить для взаимодействия и передачи данных различные виды устройств (роутеры, компьютеры, сервера, а так же различное узкоспециализированное оборудование);

IP-адрес – адрес узла (компьютера, роутера, сервера) в IP-сети;

Внешний IP-адрес – IP-адрес в сети Интернет, предоставленный провайдером услуг связи в пользование клиенту на своём/его оборудовании для обеспечения 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 к провайдеру;

Динамический IP-адрес – IP-адрес, который может меняться при каждом новом подключении к сети;

Динамический внешний IP-адрес – внешний IP-адрес в сети Интернет, изменяющийся, как правило, в одном из следующих случаев:

- при каждом новом подключении к Интернет;
- по истечении срока аренды клиентского локального IP-адреса;
- через заданный промежуток времени;
- в соответствии с другой политикой клиентской адресации провайдера;

Локальный IP-адрес:

- IP-адрес, назначенный локальному интерфейсу роутера, как правило локальный IP-адрес должен находиться в адресном пространстве обслуживаемой роутером сети;
- IP-адрес, присвоенный оборудованием Интернет-провайдера клиентскому устройству в момент подключения к Интернет; данный IP-адрес не может быть использован для получения доступа к клиентскому устройству из вне (через сеть Интернет), он позволяет только пользоваться доступом в Интернет;

Серый/частный/приватный IP-адрес – см. определение для термина "**локальный IP-адрес**";

Узел сети – объект сети (компьютерной/сотовой), способный получать от других узлов сети и передавать этим узлам служебную и пользовательскую информацию;

Клиент/клиентский узел/удаленный узел/удалённое устройство – устройство, территориально удалённое от места, либо объекта/узла, обсуждаемого в конкретно взятом контексте;

Сетевой экран (firewall) –программный аппаратный комплекс, призванный выполнять задачи защиты обслуживаемой роутером сети, её узлов, а так же самого роутера от: нежелательного трафика, несанкционированного доступа, нарушения их работы, а так же обеспечения целостности и конфиденциальности передаваемой информации на основе предопределённых администратором сети правил и политик обработки трафика в обоих направлениях;

(Удалённая) командная строка, (удалённая) консоль роутера – совокупность программных средств (серверная и клиентская программы Telnet/SSH), позволяющая осуществлять управление роутером посредством консольных команд при отсутствии физического доступа к устройству;

Служебный трафик – трафик, содержащий в себе служебную информацию, предназначенную для контроля работы сети, поддержания целостности передаваемых пользовательских данных и взаимодействия сетевых служб двух и более узлов между собой;

Пользовательские данные (в сети) – информация, создаваемая или используемая оборудованием в сети пользователя, для передачи, обработки и хранения которой было разработано техническое решение;

Нежелательный трафик – трафик, не несущий полезной нагрузки, который тем не менее генерируется одним или несколькими узлами сети, тем самым создавая паразитную нагрузку на сеть;

Сетевая служба – служба, обеспечивающая решения вопросов обработки, хранения и/или передачи информации в компьютерной сети;

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);

Провайдер – организация, предоставляющая доступ в сеть Интернет;

Оператор сотовой связи – организация, оказывающая услуги передачи голоса и данных, доступа в Интернет и обслуживания виртуальных частных выделенных сетей (VPN) в рамках емкости своей сотовой сети;

Относительный URL-путь – часть строки web-адреса в адресной строке браузера, находящаяся после доменного имени или IP-адреса удалённого узла, и начинающаяся с символа косой черты (символ «/»), пример:

```
Исходный web-адрес: http://192.168.1.1/index.php
```

```
Относительный путь: /index.php
```

"Crossover"-патчкорд – сетевой кабель, проводники которого обжаты таким образом, что его можно использовать для прямого подключения роутера к компьютеру без необходимости использования коммутационного оборудования;

Учётная запись, аккаунт – другое название "личного кабинета" пользователя Интернет-сайта, позволяющего вносить и редактировать его личные данные, настройки;

USB-накопитель – запоминающее устройство, подключаемое к роутеру через USB-интерфейс, и используемое для сохранения/считывания служебной информации роутера; может быть использовано для резервирования настроек роутера, их восстановления, а так же для автоматической конфигурации службы OpenVPN (не сервера OpenVPN).

Сертификат – электронный или печатный документ, выпущенный удостоверяющим центром, для подтверждения принадлежности владельцу открытого ключа или каких-либо атрибутов;

Корневой сертификат – сертификат выданный и подписанный одним и тем же центром сертификации;

Ключ сервера – блок криптографической информации, позволяющий серверу OpenVPN подтвердить свою подлинность в момент попытки получения доступа клиентом к сети, обслуживаемой данным сервером;

Ключ клиента/пользователя – блок криптографической информации, позволяющий пользователю, либо клиентскому узлу идентифицировать себя в системе, к которой он осуществляет попытку доступа;

Топология сети – термин, позволяющий описать конфигурацию сети на разных уровнях взаимодействия информационных систем. Как правило, топология сети формируется администратором/архитектором сети исходя из поставленных задач, решаемых техническим решением, основная идея которого реализуется данной сетью;

Сетевой интерфейс – данный термин имеет несколько определений:

- Аппаратная часть роутера, позволяющая осуществлять на низких уровнях взаимодействия связь с удалёнными узлами, а так же обмениваться с ними информацией;
- Программный виртуальный объект ОС, позволяющий определить правила и порядок следования и обмена информацией между узлами компьютерной сети;

OpenVPN – открытый бесплатный программный продукт, позволяющий создать защищённую виртуальную среду передачи данных внутри IP-сети. Поскольку OpenVPN представляет из себя многофункциональный программный пакет, в различном контексте термин «OpenVPN» может иметь различные значения, самые распространённые из которых: «сервер доступа к сети OpenVPN», «клиент, позволяющий подключиться к OpenVPN-сети», «сеть, либо сектор/уровень/слой сети, подразумевающий использование ПО OpenVPN»;

OpenVPN-сеть – IP-сеть, построенная на базе сети, созданной ПО OpenVPN;

(Виртуальное) адресное пространство OpenVPN-сети – адресное пространство IP-сети OpenVPN, призванное добавить сегмент в совокупность всех сетей на пути следования пользовательских данных, то есть обеспечить чёткую декомпозицию маршрута, тем самым упрощая проектирование и обслуживание всего вычислительного комплекса, построенного на базе ПО OpenVPN в целом;

OpenVPN-клиент – см. клиентский узел;

Туннель – виртуальная сущность/технология/объект, позволющая логически выделить конкретно взятый поток данных между двумя узлами, заключая его в отдельное от общего адресное пространство; Авторизация – процедура предоставления надлежащих прав субъекту (пользователю/участнику/клиенту/клиентскому узлу) системы после получения от него запроса на доступ к системе и прохождения проверки его подлинности (аутентификации);

Аутентификация – процедура проверки подлинности субъекта (пользователя/участника/клиента/клиентского узла) системы путём сравнения предоставленных им на момент подключения реквизитов с реквизитами, соотнесёнными с указанным именем пользователя/логином в базе данных.

2. Способы управления роутером

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.

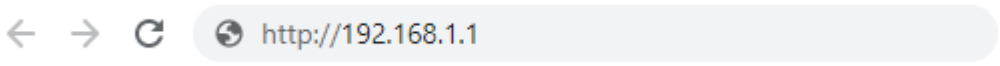


Рис. 1. Ввод IP-адреса роутера в адресную строку интернет-браузера

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**)

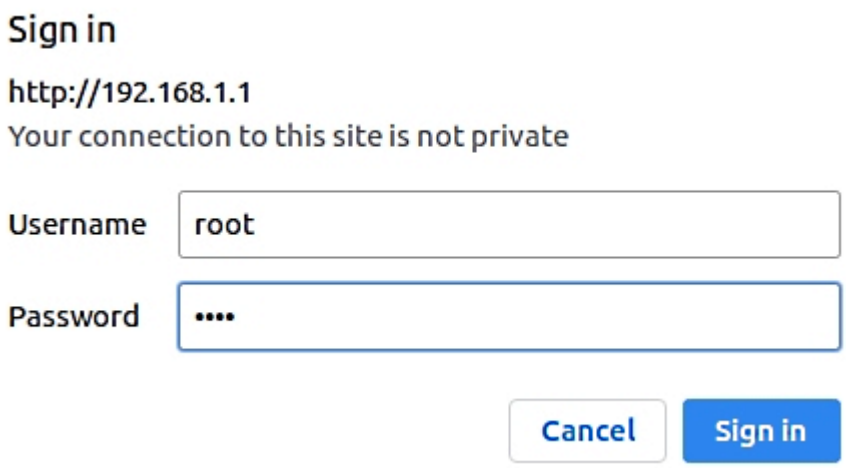


Рис. 2. Ввод логина и пароля для доступа к web-интерфейсу роутера

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 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"

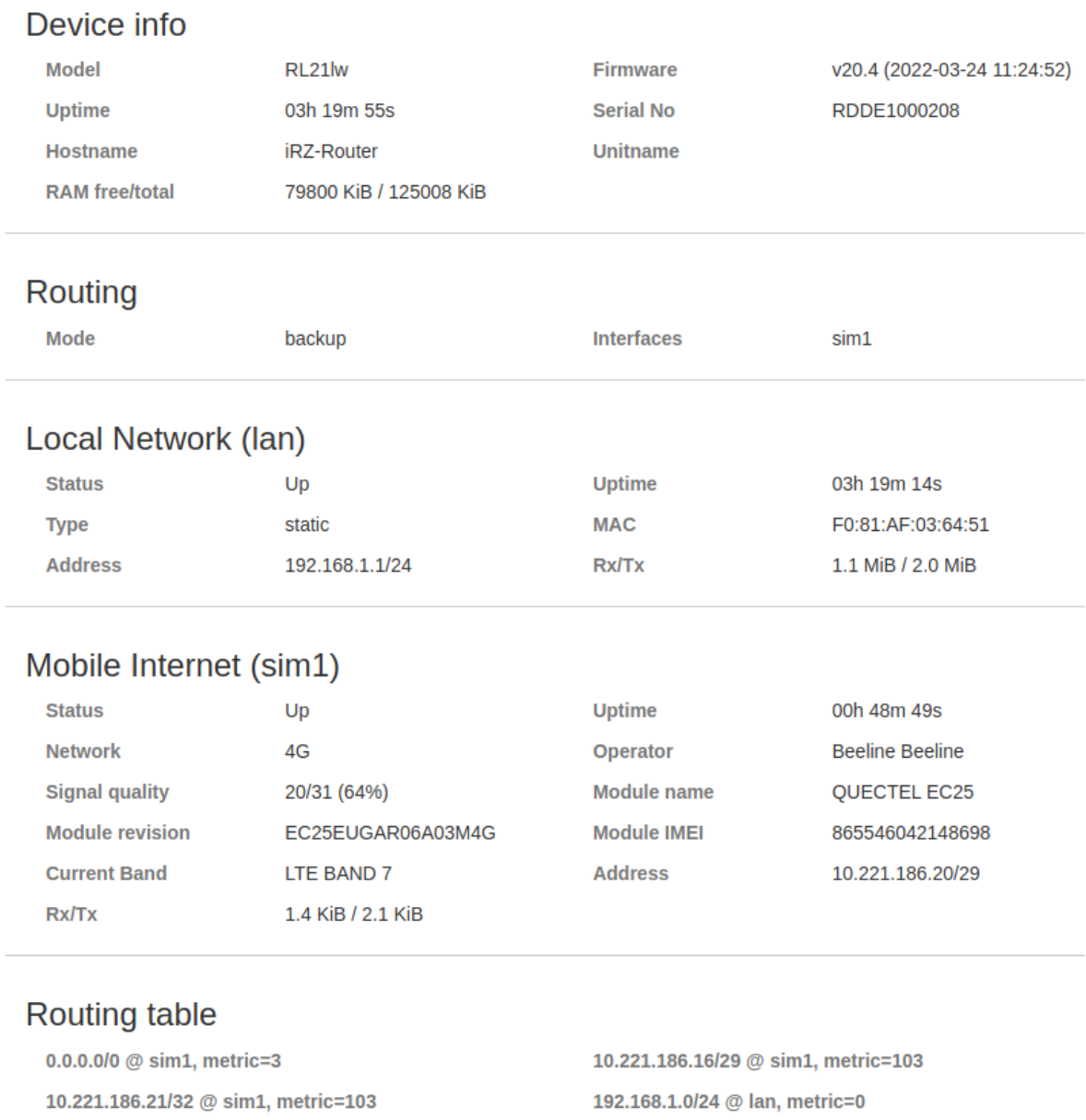


Рис. 3. Страница статуса

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 моделинастроек роутера.

5.1.1. 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)

5.1.2. 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

5.1.3. 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

5.1.4. 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
Network	Тип сотовой сети по которой в данный момент осуществляется передача данных: 2G, 3G, 4G
Signal Quality	Уровень сигнала сотовой сети в формате CSQ и в процентах от максимального
Module Revision	Номер версии GSM-модуля роутера
Band	Выбранные частотные полосы (бэнды)
Rx/Tx	Счетчик принятых и отправленных байт
Uptime	Время активности с момента установки сессии

Таблица 5. Поля раздела Mobile Internet

Operator	Выводится имя оператора сотовой сети
Module Name	Название GSM модуля, установленного в вашем роутере
Module IMEI	IMEI номер GSM модуля вашего роутера.
Address	IP-адрес сим карты с указанием маски сети, выдаваемый оператором сотовой сети

5.1.5. 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
Type	Тип работы порта
Rx/Tx	Счетчик принятых и отправленных байт

5.1.6. Routing Table

Информация по таблице маршрутизации.

Выводятся все существующие на данный момент маршруты.

5.1.7. 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.

5.1.8. IPSec tunnel

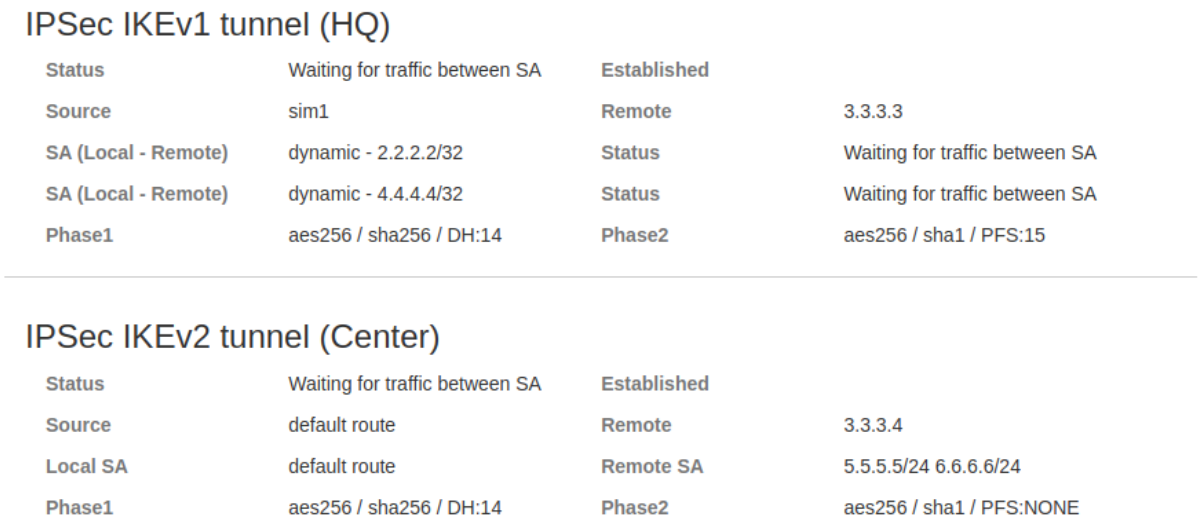


Рис. 4. Пример информации в разделе IPSec tunnel

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 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!

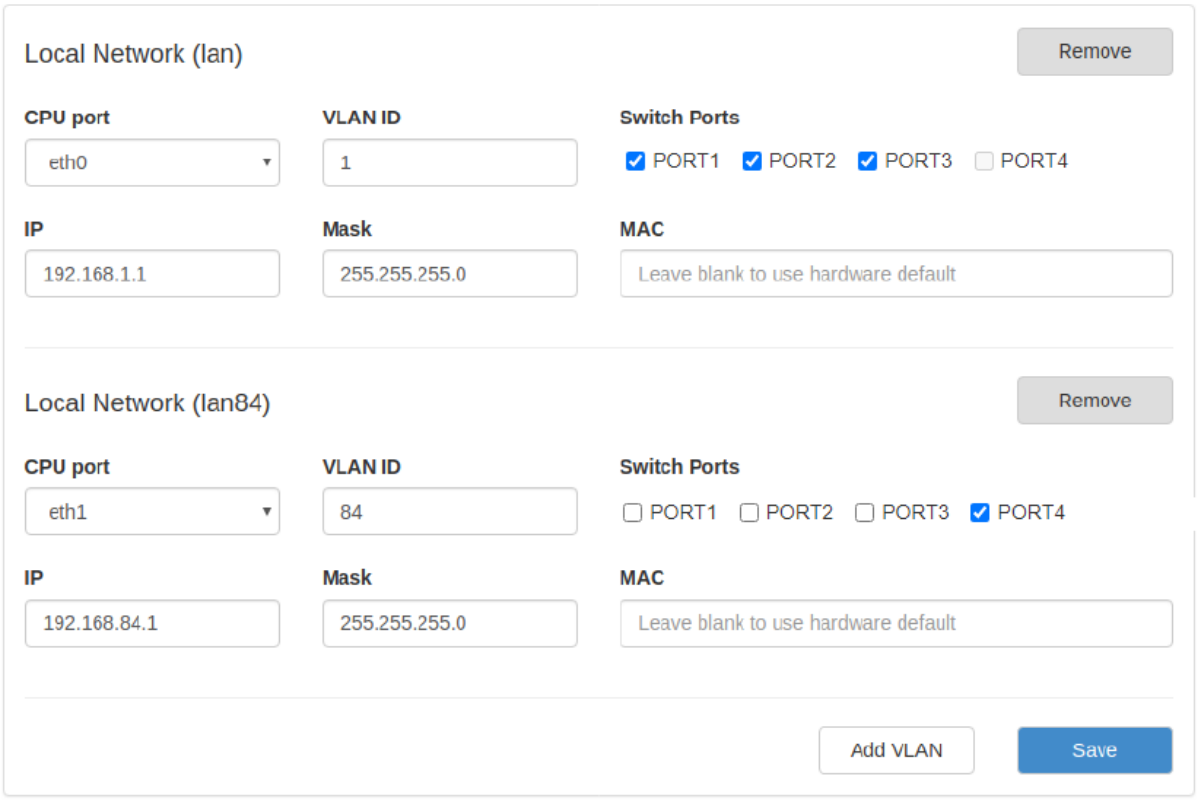


Рис. 5. Вкладка Network, раздел Local Network

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

5.2.2. Wired Internet

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

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

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

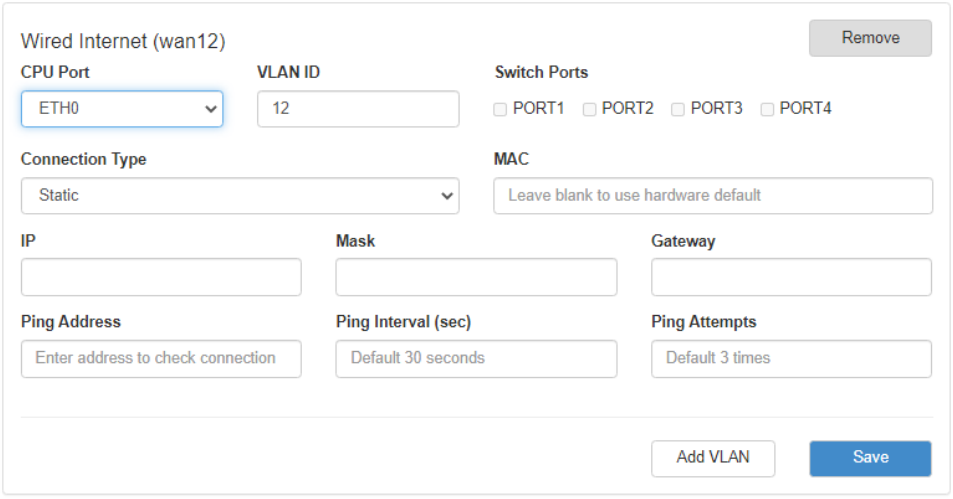


Рис. 6. Вкладка Network, раздел Wired Internet

Таблица 11. Настройки Network → Wired Internet

Поле	Описание
CPU Port	Выбор порта процессора, который будет назначен на VLAN. Например, в роутерах серии R4 доступны два порта Ethernet 1Gbit: ETH0 и ETH1. По умолчанию, ETH0 – это четыре локальных порта, а ETH1 – один WAN-порт. Однако пользователь с помощью данной настройки может распределить порты между физическими разъемами самостоятельно.
VLAN ID	Указание номера VLAN. Изначально номер задается автоматически самим устройством, однако пользователь имеет возможность его изменить.
Switch Ports	Выбор физических портов, которые будут добавлены в VLAN
Connection Type	Тип подключения к внешним сетям, через WAN-порт

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

Поле	Тип	Описание
Ping Address	Disabled, DHCP, Static, PPPoE	IP-адрес удаленного хоста для проверки работы соединения. Несколько адресов могут быть указаны через **;** или через ПРОБЕЛ
Ping Interval (sec)	Disabled, DHCP, Static, PPPoE	Интервал в секундах, через который будут отправляться пакеты для проверки соединения (по умолчанию, 30 секунд)
Ping Attempts	Disabled, DHCP, Static, PPPoE	Количество неудачных попыток соединения (по умолчанию, 3)
Use Peer DNS Server	DHCP, PPPoE	Включение/выключение использования внешних DNS-серверов провайдера
MAC	DHCP, Static, PPPoE	MAC-адрес роутера для созданного VLAN. Если поле оставить пустым, то будет использоваться MAC-адрес, установленный производителем
IP	Static	IP-адрес роутера для созданного VLAN
Mask	Static	Маска сети роутера для созданного VLAN
Gateway	PPPoE	Шлюз роутера для созданного VLAN
Login	PPPoE	Логин, который указывается при PPPoE-соединении
Password	PPPoE	Пароль, который указывается при PPPoE-соединении
AC-name	PPPoE	Имя концентратора доступа, который указывается при PPPoE-соединении

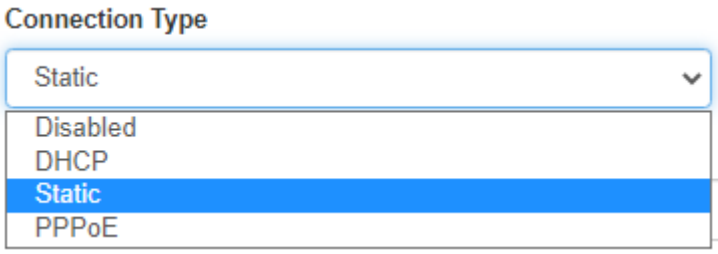


Рис. 7. Типы соединения для WAN-порта

Вариант **Disabled** в поле **Connection Type** логически выключает WAN-порт, то есть физическое подключение будет присутствовать, но роутер не будет передавать по порту никаких данных. Пример настроек показан на рисунке ниже, описание настроек приведено в таблице **Дополнительные настройки (поле Connection Type)**.

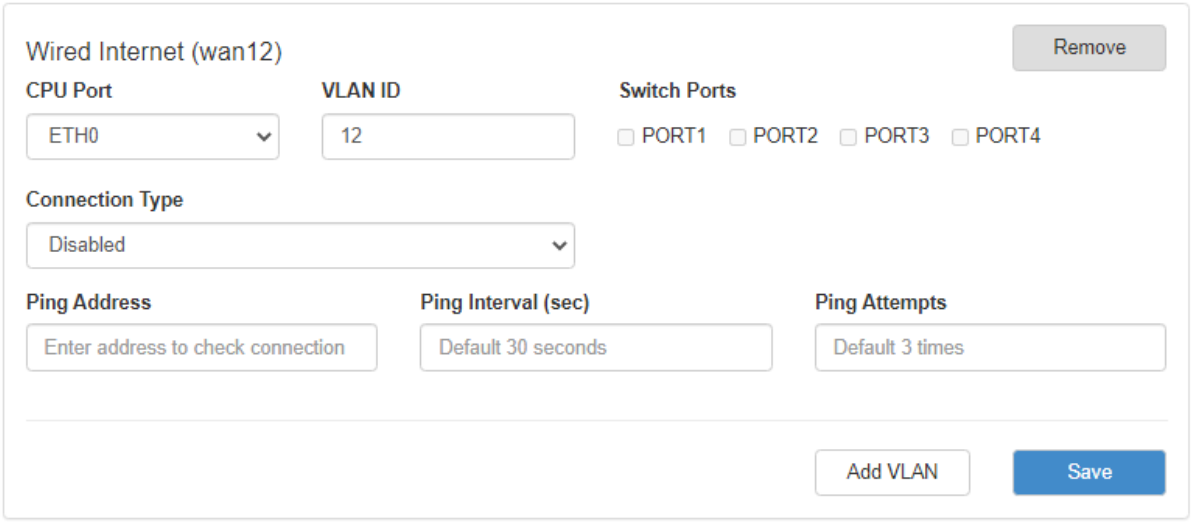


Рис. 8. WAN-порт отключен

Тип подключения **DHCP** означает, что роутер должен получить IP-адрес, маску и адреса DNS-серверов от внешнего DHCP-сервера. Пример настроек показан на рисунке ниже, описание настроек приведено в таблице **Дополнительные настройки (поле Connection Type)**

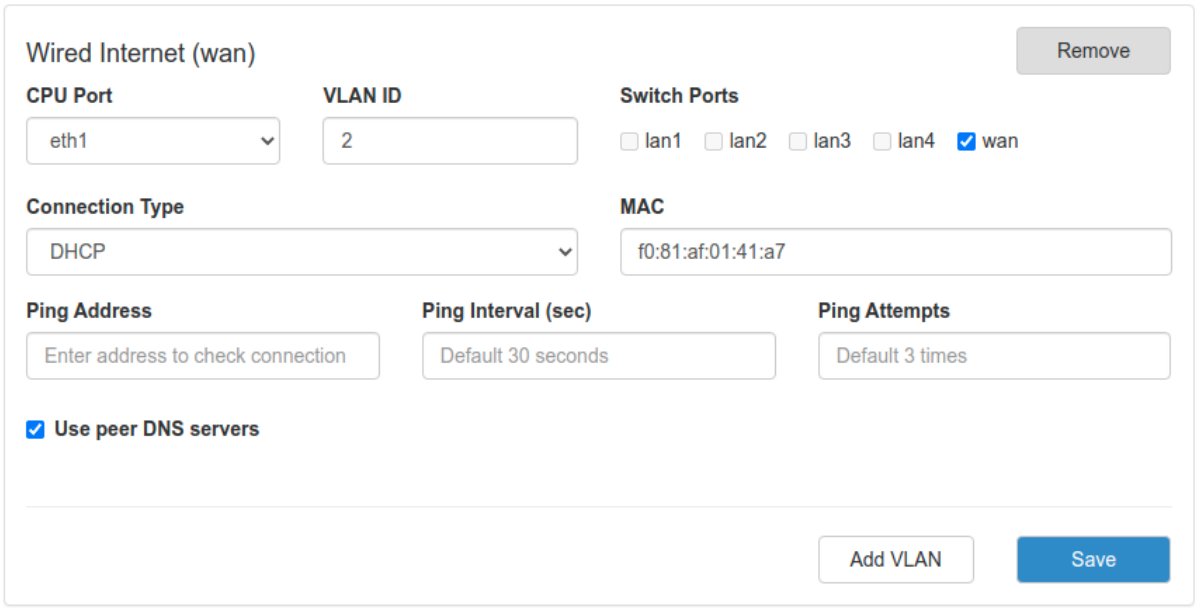


Рис. 9. Тип соединения WAN-порта – DHCP

Тип подключения **Static** необходим для ручной установки сетевых настроек WAN-порта. Пример настроек показан на рисунке ниже, описание настроек приведено в таблице **Дополнительные настройки (поле Connection Type)**

Тип подключения **PPPoE** необходим при использовании протокола с авторизацией на сервере PPPoE. Пример настроек показан на рисунке ниже, описание настроек приведено в таблице **Дополнительные настройки (поле Connection Type)**

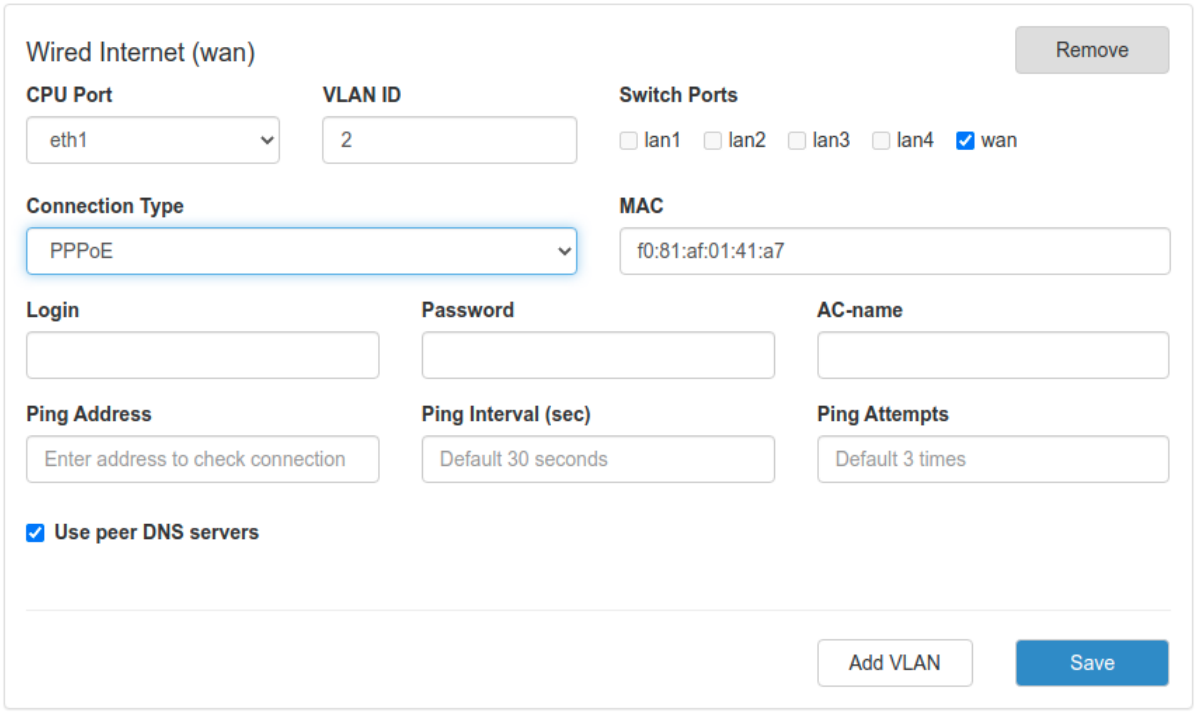


Рис. 10. Тип соединения WAN-порта – PPPoE

5.2.3. Mobile Interfaces

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

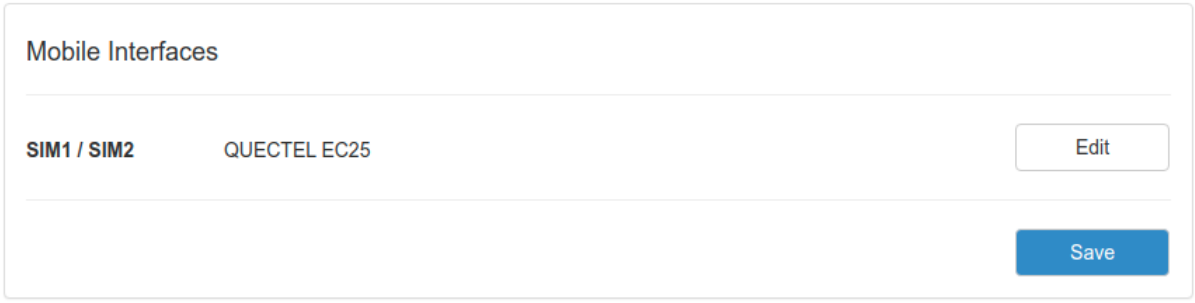


Рис. 11. Вкладка Network, раздел Mobile Interfaces для одномодульного устройства

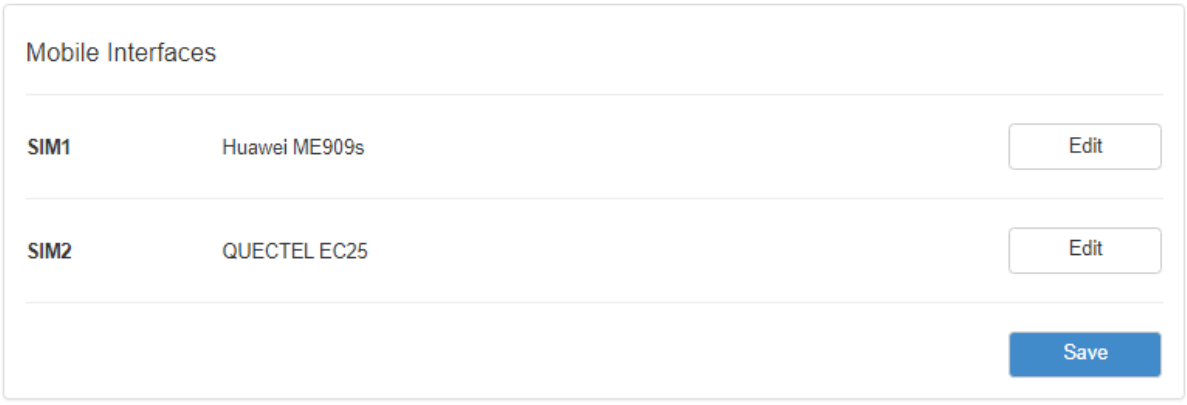


Рис. 12. Вкладка Network, раздел Mobile Interfaces для двухмодульного устройства

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.

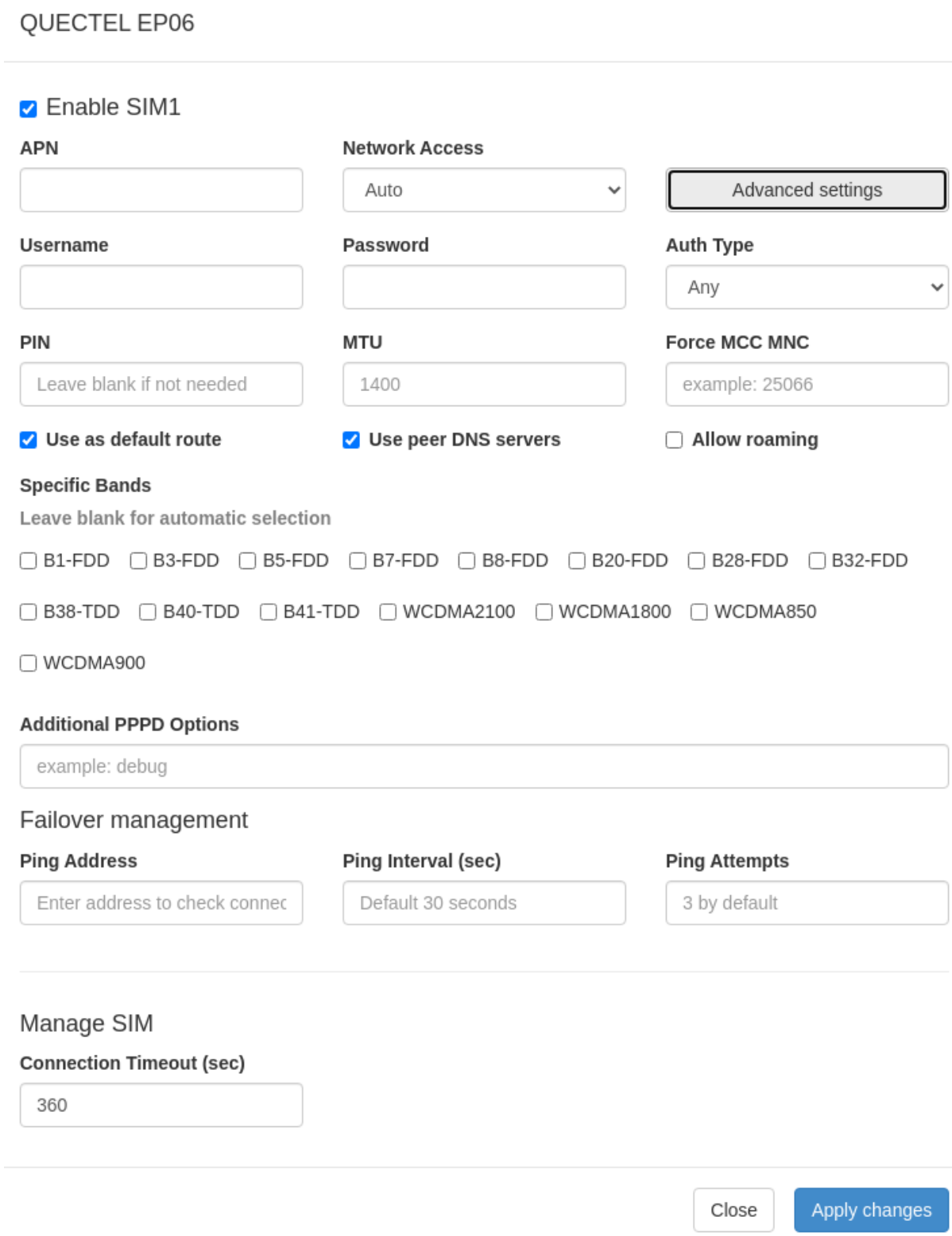


Рис. 13. Вкладка Network, раздел Mobile Interfaces − Edit

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

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).
Additional PPPD Options	Указание дополнительных опций для работы протокола PPP (кроме роутеров серии R0)
Ping Address	IP-адрес удаленного хоста для проверки работы соединения. Несколько адресов могут быть указаны через **;** или через ПРОБЕЛ
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)

Таблица 13. Настройки Network → Mobile Interfaces → Edit

Connection Timeout (sec)	Время, которое отводится SIM-карте на подключение к сотовому оператору, по истечении данного времени роутер перезагружает сотовый модуль по питанию и дозвон начинается заново, измеряется в секундах
Primary SIM	Указывает какая из SIM карт является приоритетной (только для одномодульных роутеров)
Return to Primary SIM (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 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)**

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.

Проверка состояния соединения

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

Для включения проверки состояния соединения должен быть выбран параметр **Default Route**

В поле **Ping Address** указывается IP-адрес для проверки работы соединения. Несколько адресов могут быть указаны через **;** или через ПРОБЕЛ. В поле **Ping Interval** задается периодичность запуска пинга (в секундах). В поле **Ping Attempts** указывается количество неудачных попыток соединения.

- Если соединение установлено и передача данных происходит корректно, устройство работает как обычно.
- Если соединение не установлено или количество неудачных попыток соединения достигло заданного, роутер инициирует перезагрузку GSM-модуля.
- 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.

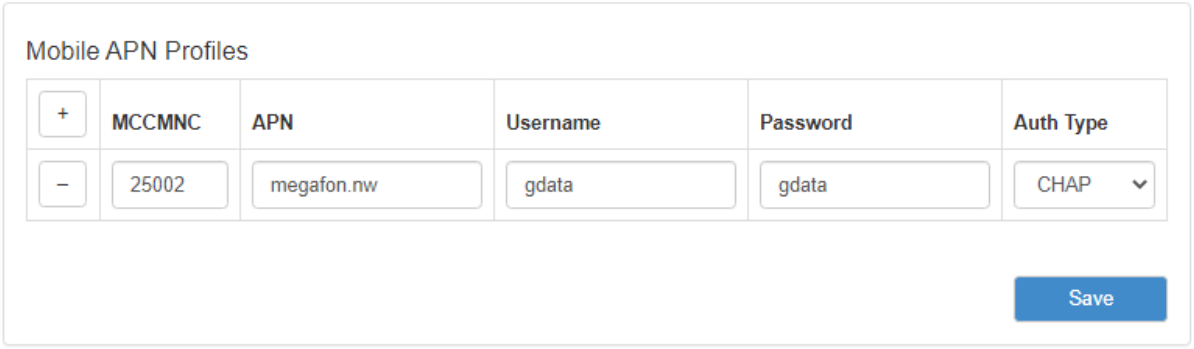


Рис. 14. Вкладка Mobile APN Profiles

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. 15. Вкладка Network, раздел Loopbacks

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

5.2.6. Wireless Internet

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

Данный раздел доступен 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!

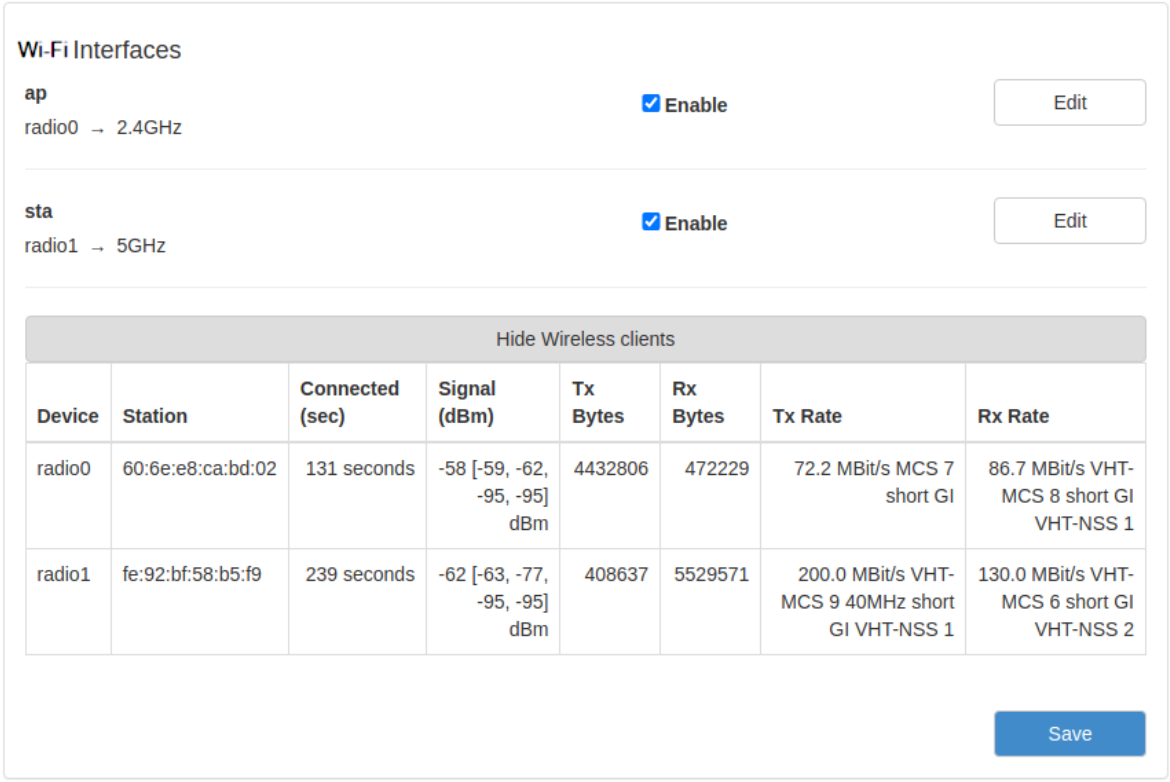


Рис. 16. Вкладка Network, раздел Wireless Internet

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**.

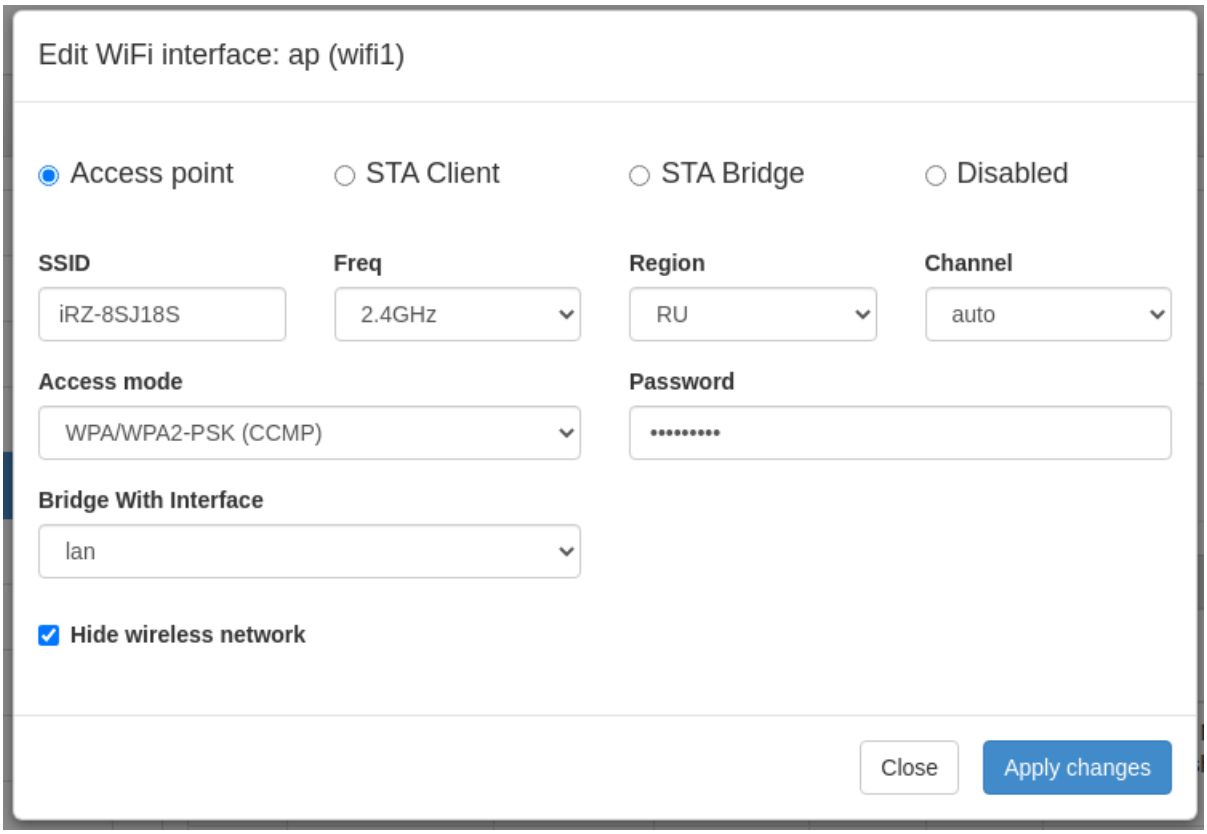


Рис. 17. Меню Edit, Вкладка Network, раздел Wireless Internet

Edit Wi-Fi interface

Выбор режима работы модуля Wi-Fi:

- **Access point** — роутер работает в качестве точки доступа и ждет подключения клиентов к своей сети;
- **STA Client** — роутер сам подключается к внешней Wi-Fi-сети, в данном режиме 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
Region	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 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
Ping Address	Несколько адресов могут быть указаны через **;** или через ПРОБЕЛ
Ping Interval (sec)	Интервал в секундах, через который будут отправляться пакеты для проверки соединения (по умолчанию, 30 секунд)
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
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
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.

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!

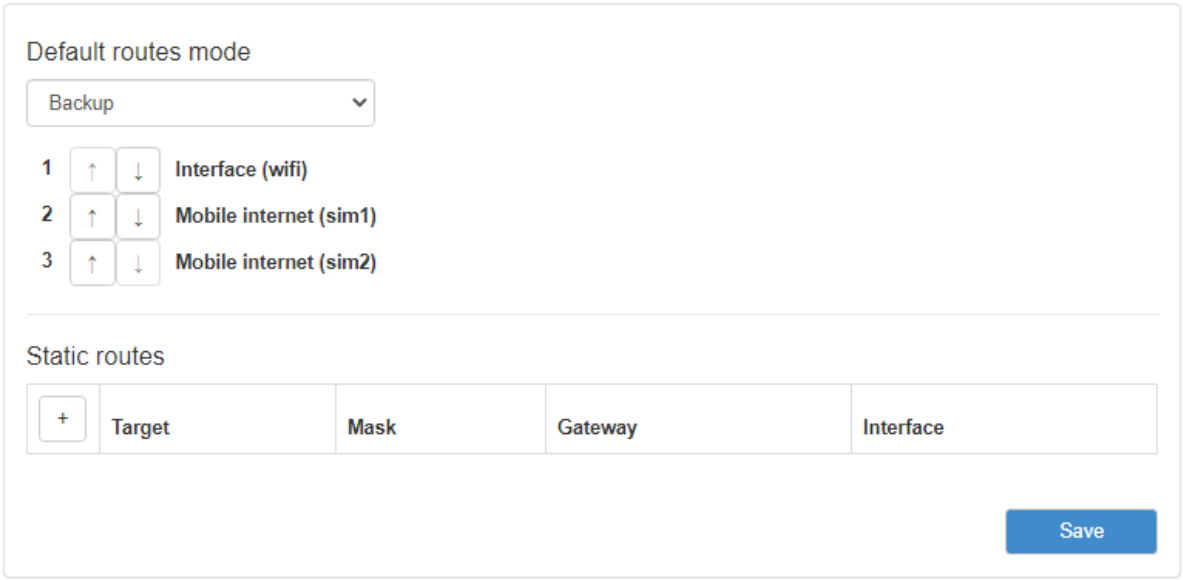


Рис. 18. Вкладка Network, раздел Routes

Default Routes Mode — режим работы WAN-портов:

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

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

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

После выбора режима работы WAN портов следует подраздел настройки статических маршрутов, Static Routes.

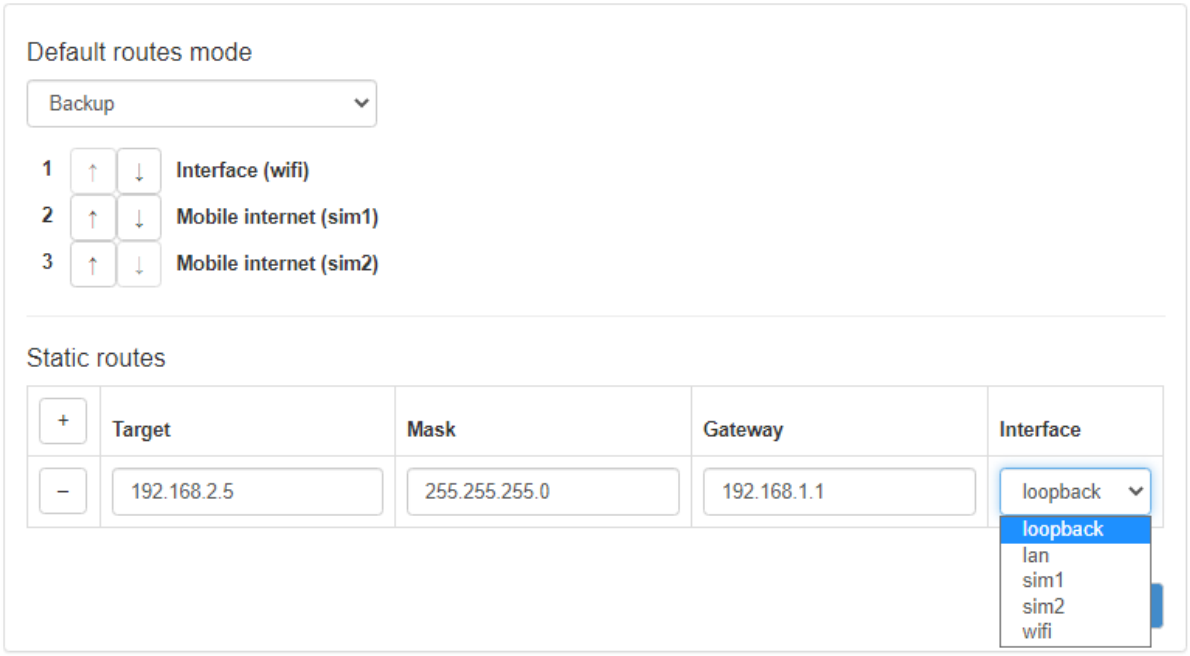


Рис. 19. Настройка статических маршрутов

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 является пакет **Quagga**. Поддерживаемые протоколы - **BGP**, **OSPF**.

На роутерах серии **R0** и **R2** для работы с динамической маршрутизацией вначале надо установить необходимые пакеты. На роутерах серии **R4** пакеты установлены по умолчанию. Требуется версия прошивки 20.1 и выше.

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!

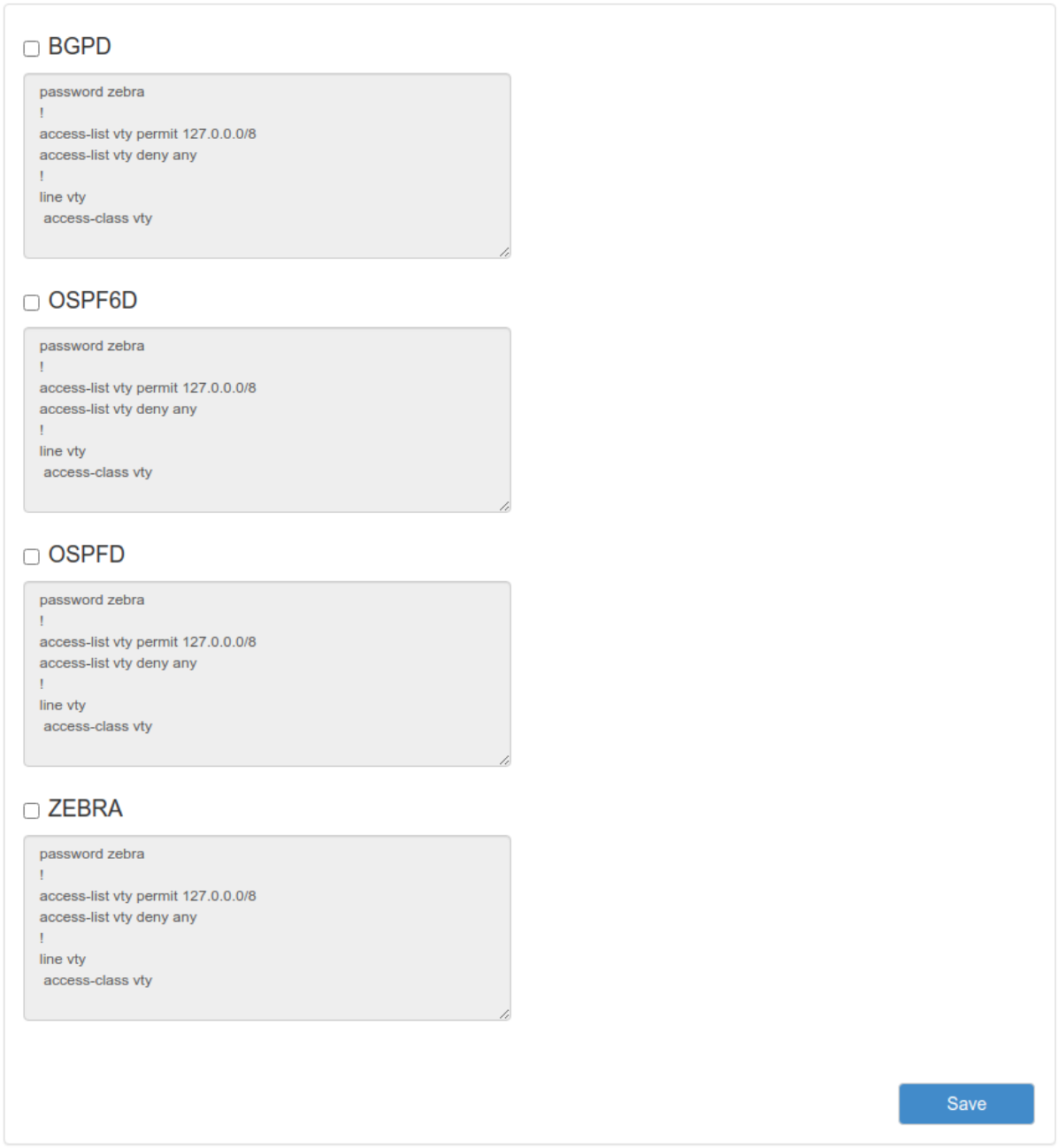


Рис. 20. Пример настройки динамической маршрутизации по протоколам: BGP, OSPF

Процесс настройки динамической маршрутизации в веб-интерфейсе представляет собой заполнение текстового поля соответствующей службы соответствующего протокола в формате синтаксиса, определнного для данного пакета.

Активация поля происходит по чекбоксу возле соответствующей службы.

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

5.2.9. DNS Servers

Раздел **DNS Servers** на вкладке **Network** предназначен для указания адресов DNS-серверов. На 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. 21. 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 серии R4.

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

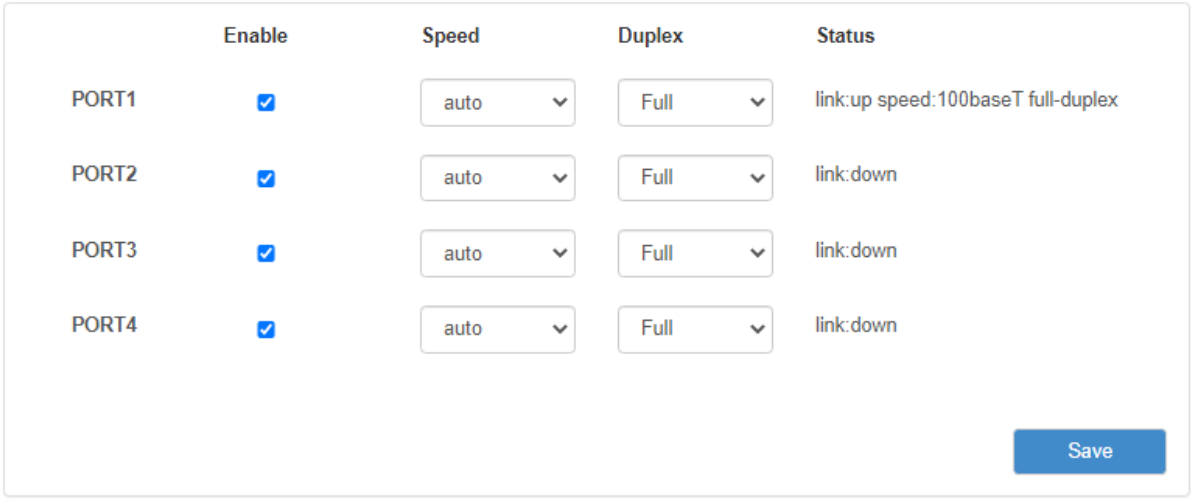


Рис. 22. Вкладка Network, раздел Switch

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

5.3.1. Предупреждения

Отклонение от рекомендованных параметров и настроек может привести к непредсказуемым последствиям и значительным издержкам как в процессе пусконаладки вычислительного комплекса, так и во время эксплуатации production-версии вычислительного комплекса в реальных условиях.

Прежде чем вносить любые изменения в настройки оборудования, устанавливаемого на объекты, настоятельно рекомендуется проверить работоспособность всех параметров новой конфигурации на тестовом стенде. Также не следует ограничиваться синтетическими тестами, а максимально реалистично воспроизвести условия, в которых будет эксплуатироваться оборудование.

5.3.2. PPTP Client

Туннель PPTP представлен в виде клиентской части. Для подключения к серверу PPTP необходимо указать адрес сервера в виде IP адреса или его доменного имени, логин и пароль клиентского доступа и выбрать тип аутентификации.

Для сохранения выполненных настроек, используйте кнопку **Save**.

При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!

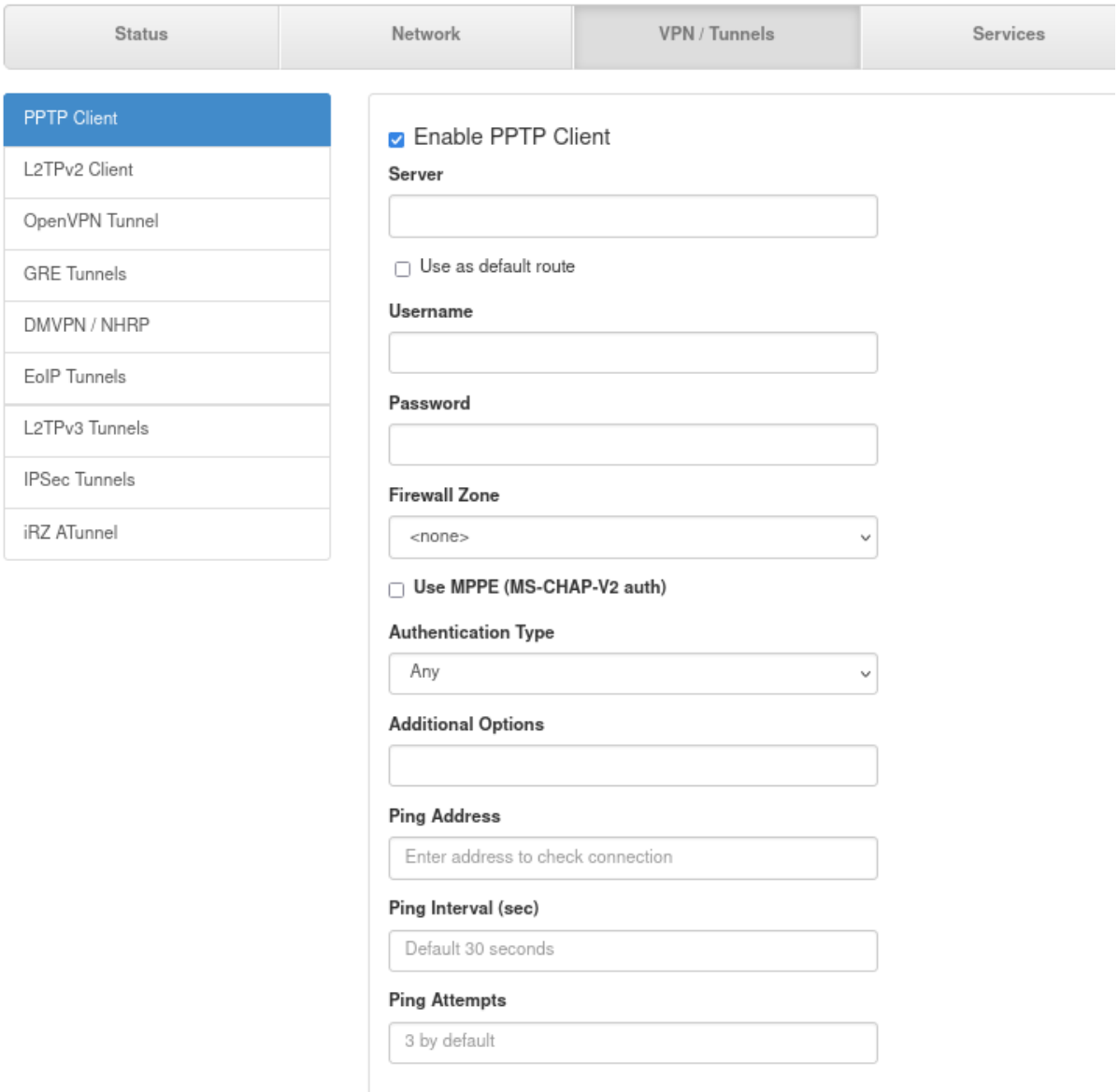


Рис. 23. Пример интерфейса PPTP Client

Для авторизации на сервере представлены следующие распространенные типы аутентификации для PPTP туннеля: EAP, PAP, CHAP и MPPE (MS-CHAP-V2). Значение Any в поле Authentication Type позволяет договариваться с сервером PPTP о методе аутентификации в автоматическом режиме.

Проверка состояния соединения

Предусмотрена проверка состояния соединения при помощи отправки пакетов (ICMP) на указанный адрес.

Для включения проверки состояния соединения должен быть выбран параметр **Default Route**

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, после чего соединение будет считаться деградировавшим.

- Если соединение установлено и передача данных происходит корректно, туннель работает как обычно.
- Если при установленном соединении количество неудачных попыток **Ping Attempts** достигло заданного, роутер инициирует перезагрузку данного интерфейса (туннель будет построен заново).

5.3.3. L2TPv2 Client

Туннель L2TP версии 2 на роутерах представлен только в виде клиентской части. Для подключения к удаленному серверу необходимо указать адрес или доменное имя сервера и логин с паролем.

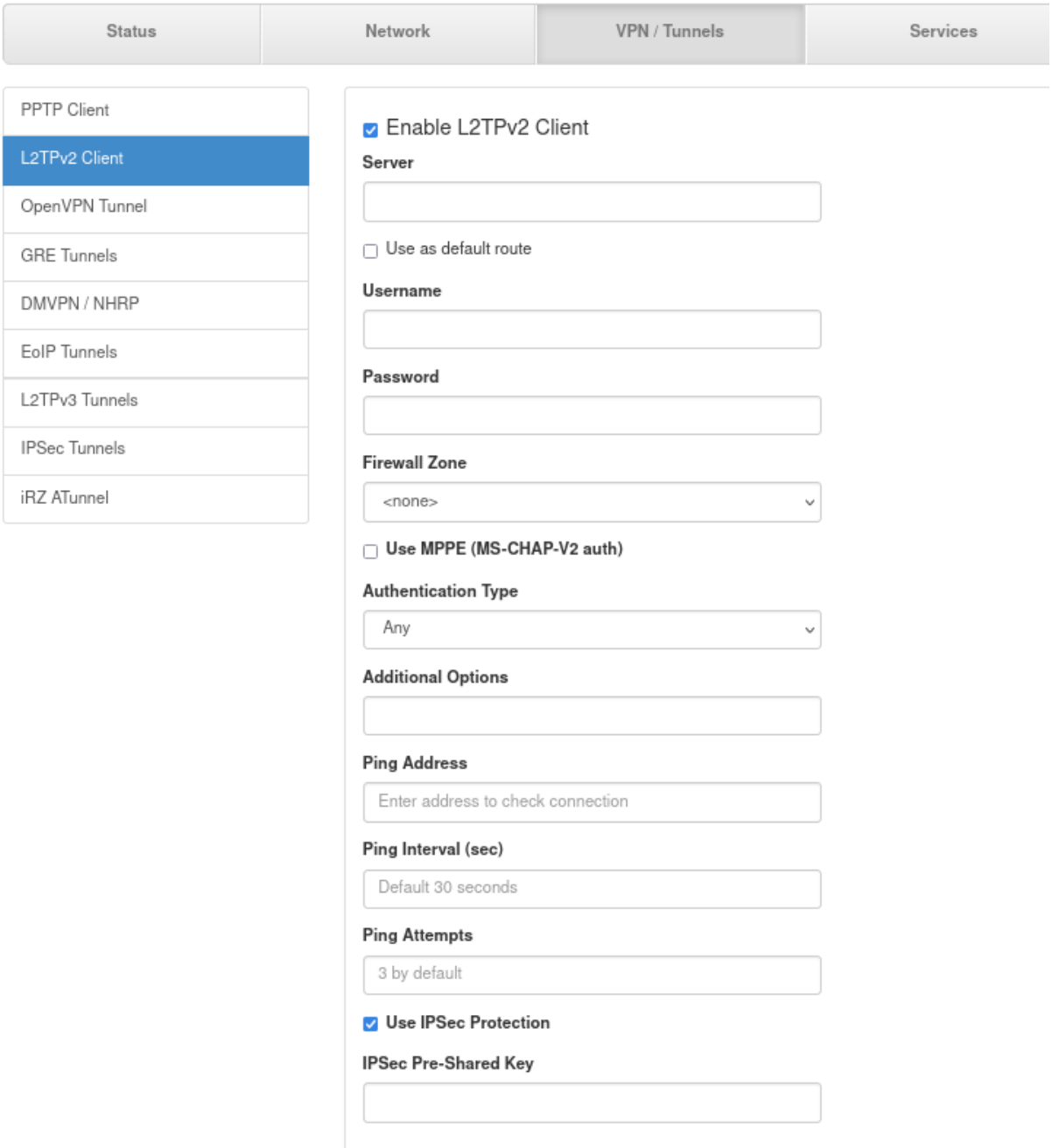


Рис. 24. Пример интерфейса L2TPv2 Client

Таблица 20. Поля в разделе L2TPv2 Client

Поле	Описание
Use as default route	Использовать как маршрут по умолчанию. В этом случае роутер будет направлять весь трафик через данный туннель, в таблице маршрутизации маршрут через данный туннель будет приоритетным. Таким образом, остальные WAN интерфейсы (такие как подключение через сотовую сеть или отдельный WAN порт) станут резервными, и переключение с одного WAN порта на другой не будет приводить к разрыву туннеля, то есть его переподключению
Use MPPE (MS-CHAP-V2)	Заставит роутер подключаться к серверу L2TP только по указанному протоколу аутентификации
Additional Options	Позволяет прописывать дополнительные опции для работы туннеля
Use IPSec Protection	Дает возможность настроить шифрование туннеля с помощью IPSec. Данный функционал разработан для взаимодействия с сетевым оборудованием Mikrotik. В поле IPSec Pre-Shared Key следует вписать ключ

Проверка состояния соединения

Предусмотрена проверка состояния соединения при помощи отправки пакетов (ICMP) на указанный адрес.

Для включения проверки состояния соединения должен быть выбран параметр **Default Route**

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, после чего соединение будет считаться деградировавшим.

- Если соединение установлено и передача данных происходит корректно, туннель работает как обычно.
- Если при установленном соединении количество неудачных попыток **Ping Attempts** достигло заданного, роутер инициирует перезагрузку данного интерфейса (туннель будет построен заново).

5.3.4. OpenVPN

OpenVPN Layer 2: dev TAP

В данном разделе рассматривается туннель OpenVPN типа Ethernet Bridging.

Этот тип туннеля OpenVPN характеризуется общим адресным пространством между устройствами, а маршрутизаторы, на которых создается OpenVPN, прозрачны для остальных сетевых устройств. Данный туннель создаётся на базе виртуального сетевого интерфейса TAP.

Всего четыре варианта настройки туннеля, различающиеся по методу аутентификации:

- без аутентификации (Authentication method: None);
- с аутентификацией по общему ключу (Authentication method: Shared secret);
- в роли сервера OpenVPN (Authentication method: TLS Server);
- в роли клиента OpenVPN (Authentication method: TLS Client).

При этом необходимо учитывать, что туннель может работать по двум сетевым протоколам: UDP и TCP. Для протокола TCP есть возможность работать по методу сервера, когда роутер ожидает подключения извне, так и по методу клиента, когда роутер инициирует подключение с другим сетевым устройством.

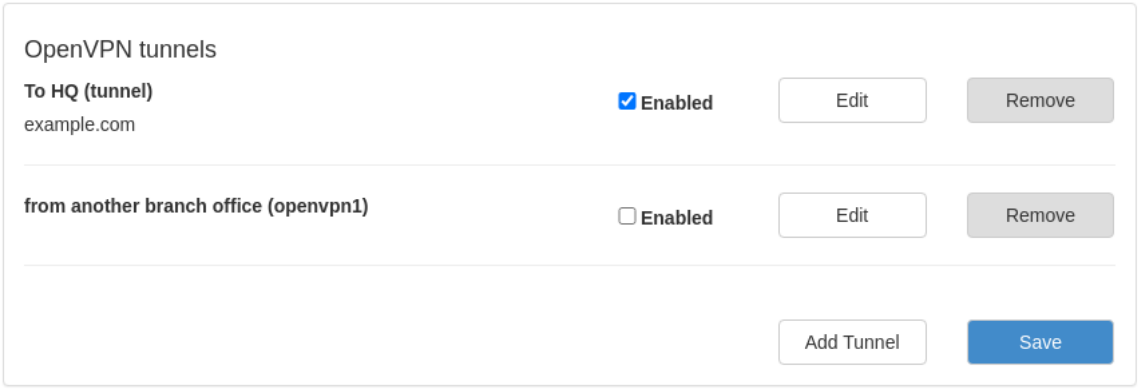


Рис. 25. Пример интерфейса раздела OpenVPN tunnels

Для настройки OpenVPN-туннеля с TAP (Layer 2), в веб-интерфейсе роутера:

1. Зайдите в раздел Network → OpenVPN Tunnel;
2. Поставьте галочку напротив пункта Enable OpenVPN tunnel;
3. Выберите в поле Device значение TAP (L2);
4. Настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. таблицы ниже).

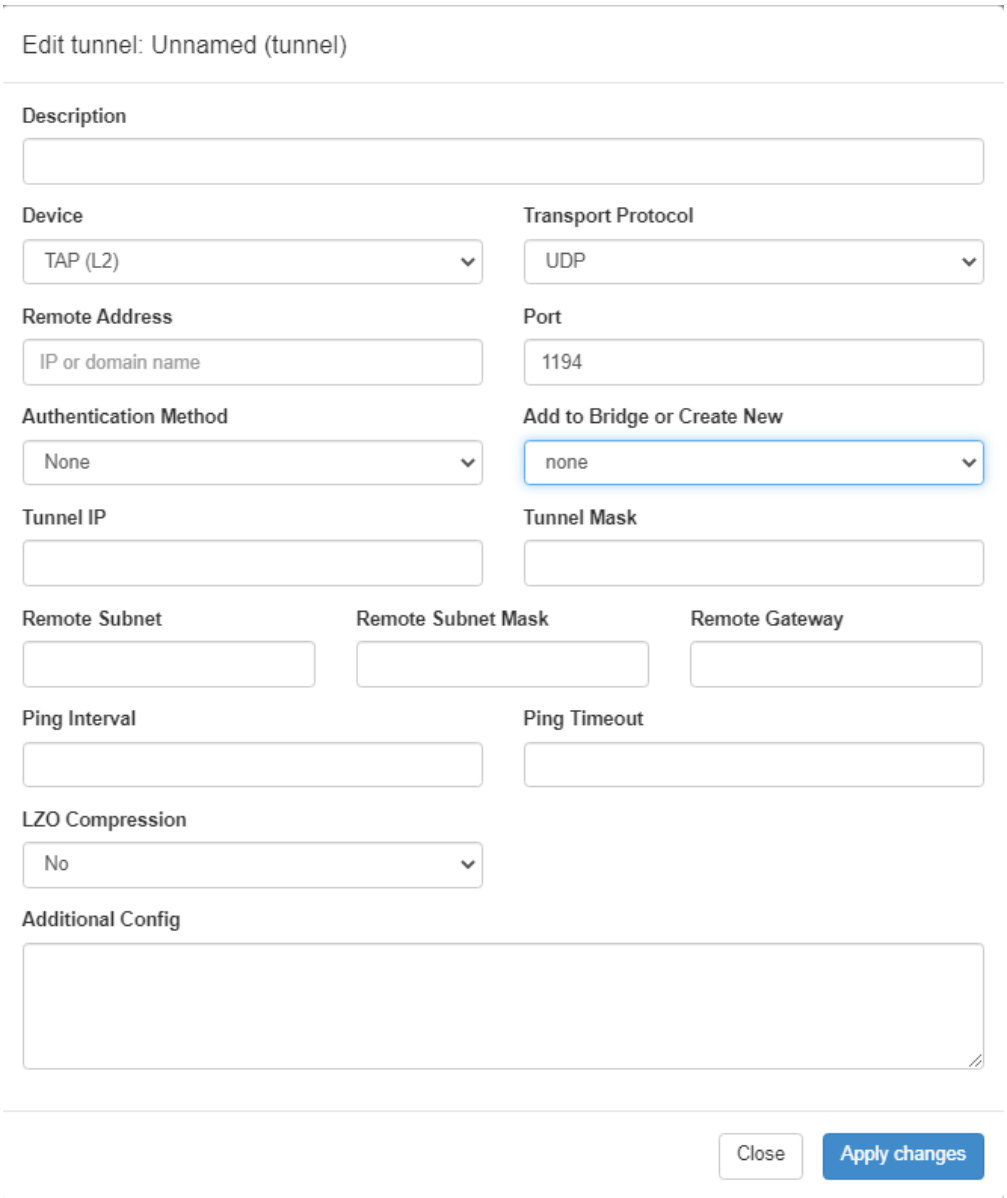


Рис. 26. Пример конфигураций OpenVPN. Настройка OpenVPN

Таблица 21. Настройки OpenVPN Tunnel → TAP (L2), основные настройки

Поля	Описание
Description	Описание и имя туннеля. Это же имя отображается во всех остальных настройках роутера (например, в разделе Firewall)
Device	Выбор виртуального интерфейса
Transport Protocol	Выбор транспортного протокола: • UDP; • TCP Server; • TCP Client.

Таблица 21. Настройки OpenVPN Tunnel → TAP (L2), основные настройки

Remote Address	IP-адрес удаленного сетевого устройства (указывается если **Transport Protocol** = **UDP** или **TCP Client**)
Port	Номер порта, через который будет работать туннель
Authentication Method	Метод авторизации
Advanced Settings:	*Нажмите на строчку Show advanced settings, чтобы открыть доступ к настройкам*
Add to Bridge or Create New	Создание моста с локальными интерфейсами роутера
Ping Interval	Время в секундах, через которое будут отсылаться ICMP-пакеты для проверки доступности удаленного сетевого устройства (и соответственно работы туннеля)
Ping Timeout	Время ожидания в секундах, через которое устройство попытается заново создать OpenVPN-туннель, если ответ от удаленного устройства не будет получен
LZO Compression	Режим сжатия данных, проходящих через туннель: • No- отсутствие сжатия данных • Always — всегда сжимать данные • Adaptive — адаптивное сжатие данных
Tunnel IP	IP-адрес туннеля на данном устройстве
Tunnel Mask	Маска IP-адреса туннеля на данном устройстве
Remote Subnet	IP-адрес удаленной сети (на другом конце туннеля), который необходим для создания маршрута в таблице маршрутизации
Remote Subnet Mask	Маска удаленной сети (на другом конце туннеля)
Remote Gateway	Шлюз удаленной сети (на другом конце туннеля)

Поле **Additional Config** позволяет указывать дополнительные параметры для создания туннеля. Пункты и их расшифровка, которые указываются в данном поле, можно посмотреть на официальном сайте OpenVPN по адресу: https://openvpn.net/index.php/open-source/documentation/howto.html#server.

OpenVPN Layer 3: dev TUN

В данном разделе рассматривается туннель OpenVPN типа Routing.

Данный тип туннеля OpenVPN характеризуется маршрутизацией пакетов между сетями на разных концах туннеля, находящимися за сетевыми устройствами, и устанавливающими туннель между собой. Данный вид туннеля создается на базе виртуального сетевого интерфейса TUN.

Всего четыре варианта настройки туннеля, различающиеся по методу аутентификации:

- без аутентификации (Authentication method: None);
- с аутентификацией по общему ключу (Authentication method: Shared secret);
- в роли сервера OpenVPN (Authentication method: TLS Server);
- в роли клиента OpenVPN (Authentication method: TLS Client).

При этом необходимо учитывать, что туннель может работать по двум сетевым протоколам: UDP и TCP. Для протокола TCP есть возможность работать по методу сервера, когда роутер ожидает подключения извне, так и по методу клиента, когда роутер инициирует подключение с другим сетевым устройством.

Для настройки OpenVPN-туннеля с TUN (Layer 3), в веб-интерфейсе роутера:

1. Зайдите в раздел Network → OpenVPN Tunnel;
2. Поставьте галочку напротив пункта Enable OpenVPN tunnel;
3. Выберите в поле Device значение TUN (L3);
4. Настройте остальные параметры на странице в зависимости от требуемой конфигурации.

5.3.5. GRE

Настройка GRE туннеля уровня L2

В примерах настройки используется следующая схема сети:

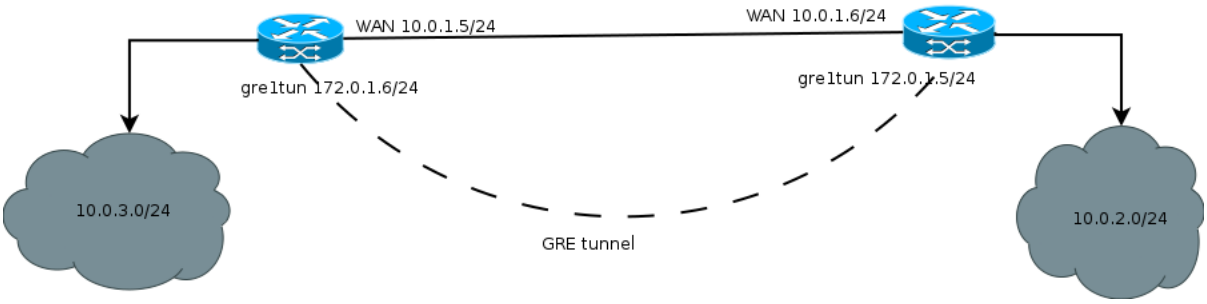


Рис. 27. Примеры конфигураций GRE. Схема сети

Для настройки GRE-туннеля уровня L2, в веб-интерфейсе роутера (см. рисунок ниже):

1. Зайдите в раздел **Network** → **Local Network**;
2. Укажите IP-адрес локального пользователя в поле **IP**;
3. Укажите маску сети в поле **Mask**;

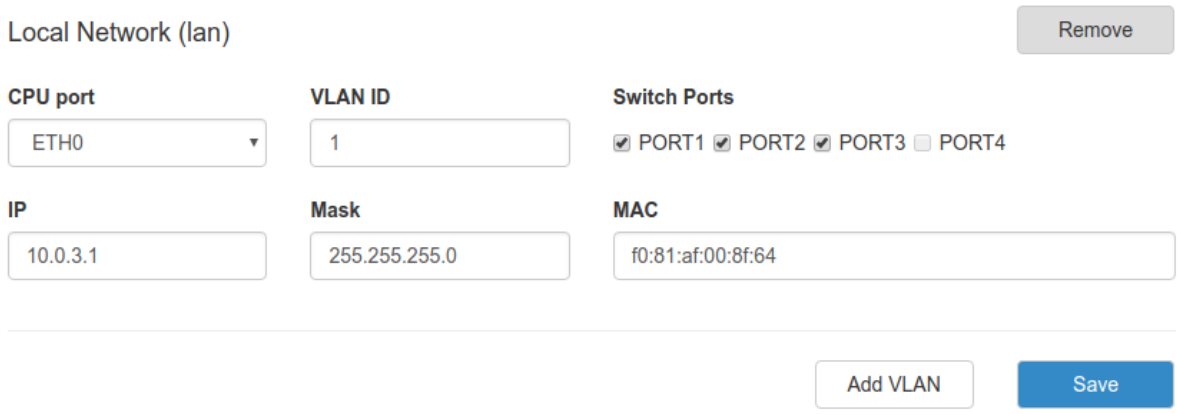


Рис. 28. Примеры конфигураций Local Network. Настройка локальной сети

Далее необходимо настроить WAN-порт роутера (см. следующий рисунок):

4. Зайдите в раздел **Network** → **Wired Internet**;

5. Укажите тип подключения в поле **Connection Type** (**Static** – статический адрес, **DHCP** – адрес

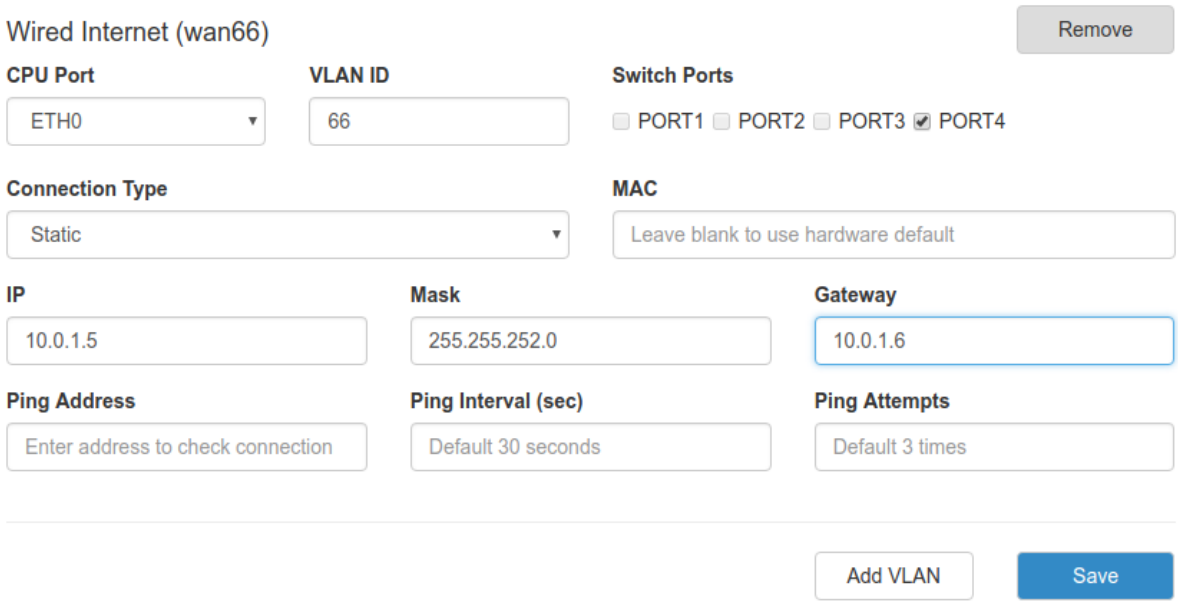


Рис. 29. Примеры конфигураций Wired Internet. Настройка WAN

Далее необходимо настроить GRE-туннель (см. следующий рисунок):

6. Зайдите в раздел **VPN/Tunnels** → **GRE Tunnels**;
7. Добавьте новый туннель, нажав на кнопку **Add Tunnel**;
8. Введите имя туннеля (на выбор пользователя) в поле **Name**;
9. Выберите локальный интерфейс, через который будет работать туннель в поле **Local Address**;
10. Укажите IP-адрес порта удаленного устройства, с которым будет построен туннель, в поле **Remote Address**;
11. Выберите на каком уровне будет работать туннель в поле **Network Type** (в данном примере рассматривается **L2**);
12. Выберите с каким **LAN** интерфейсом будет создан bridge или задайте отдельную сеть для GRE- туннеля, выбрав значение в поле **Add to Bridge or Create New** (если значение = **LAN**, то дополнительных настроек не требуется, если значение = **<new network>** , то необходимо будет указать IP-адрес пользовательского интерфейса в поле **Tunnel IP** и маску сети в поле **Tunnel Mask**);
13. Выберите к какой зоне **Firewall** необходимо отнести туннель (к зоне **Lan** или зоне **WAN**), выбрав значение в поле **Firewall Zone** (правила можно настроить вручную в разделе **Services** → **Firewall**);
14. При необходимости укажите ключ туннеля — **GRE key** (данный пункт чаще всего необходим если вы устанавливаете несколько таких туннелей с одним удаленным узлом).
15. При необходимости поставьте устройству запрет на фрагментацию (разделение) пакета на маршруте следования, поставив галочку напротив пункта **Don’t fragment**.

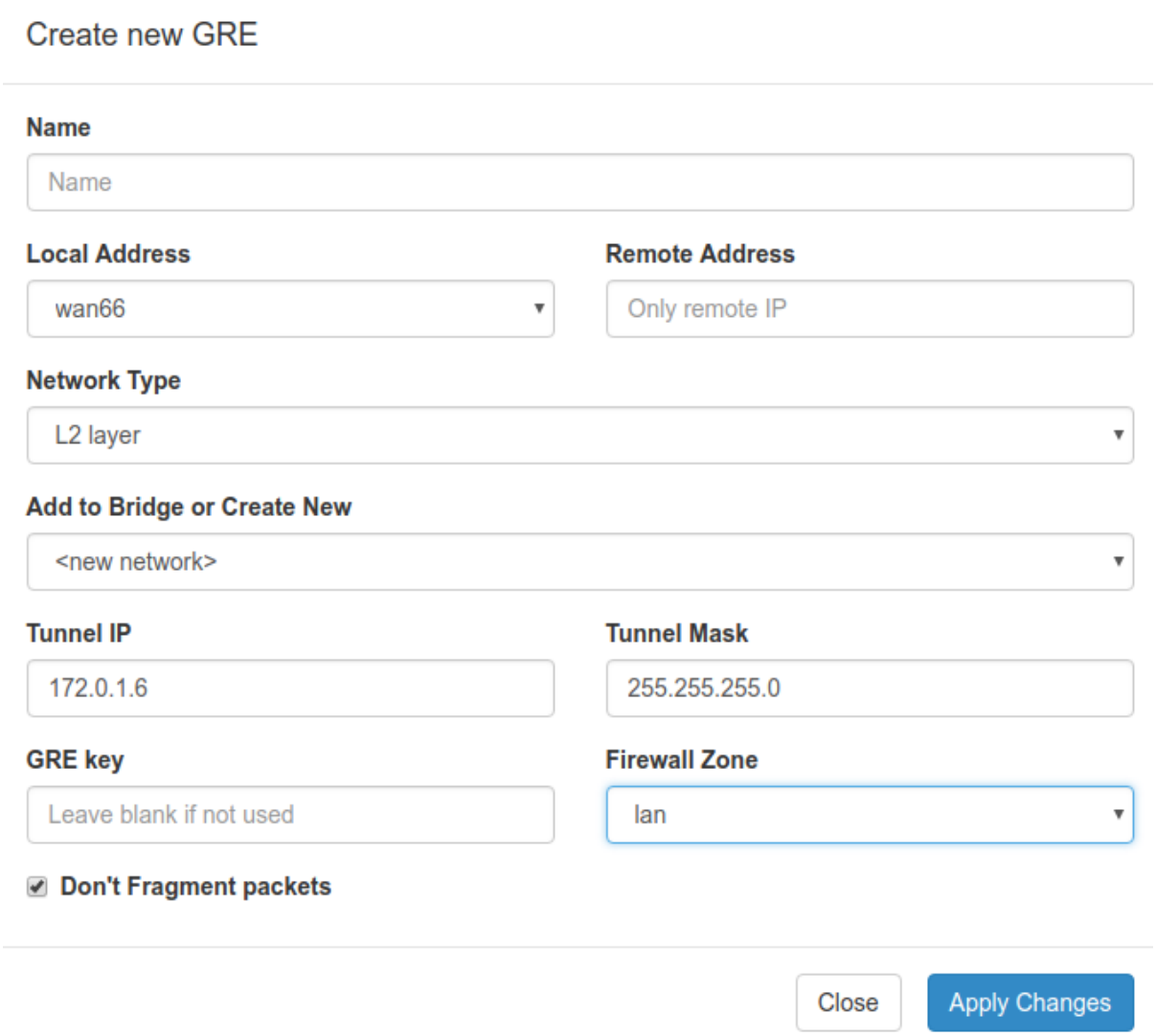


Рис. 30. Примеры конфигураций GRE. Настройка GRE-туннеля

Настройка GRE туннеля уровня L3

В примерах настройки используется следующая схема сети:

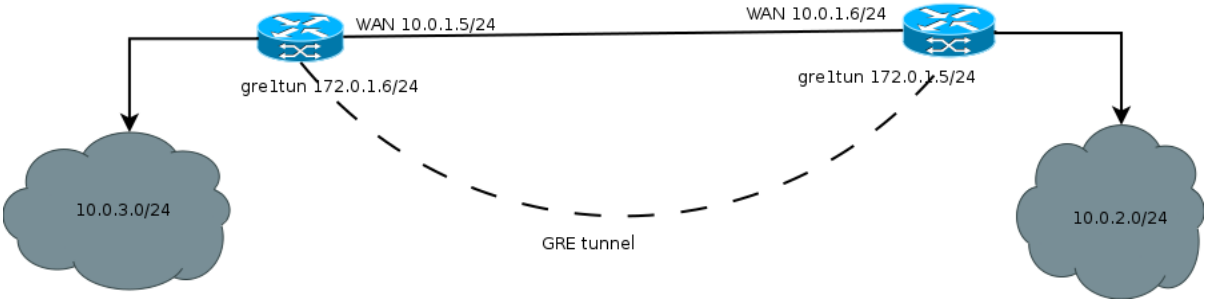


Рис. 31. Примеры конфигураций GRE. Схема сети

Для настройки GRE-туннеля уровня L3, в веб-интерфейсе роутера (см. рисунок ниже):

1. Зайдите в раздел Network → Local Network;
2. Укажите IP-адрес локального пользователя в поле IP;
3. Укажите маску сети в поле Mask;

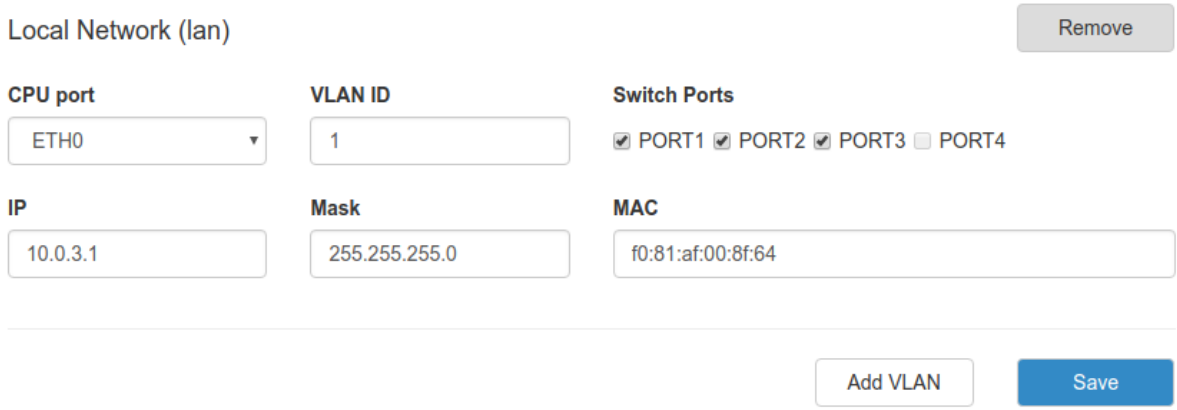


Рис. 32. Примеры конфигураций GRE. Настройка локальной сети

Далее необходимо настроить WAN-порт роутера (см. рисунок ниже):

4. Зайдите в раздел Network → Wired Internet;

5. Укажите тип подключения в поле Connection Type (Static – статический адрес, DHCP – адрес получаемый по DHCP);

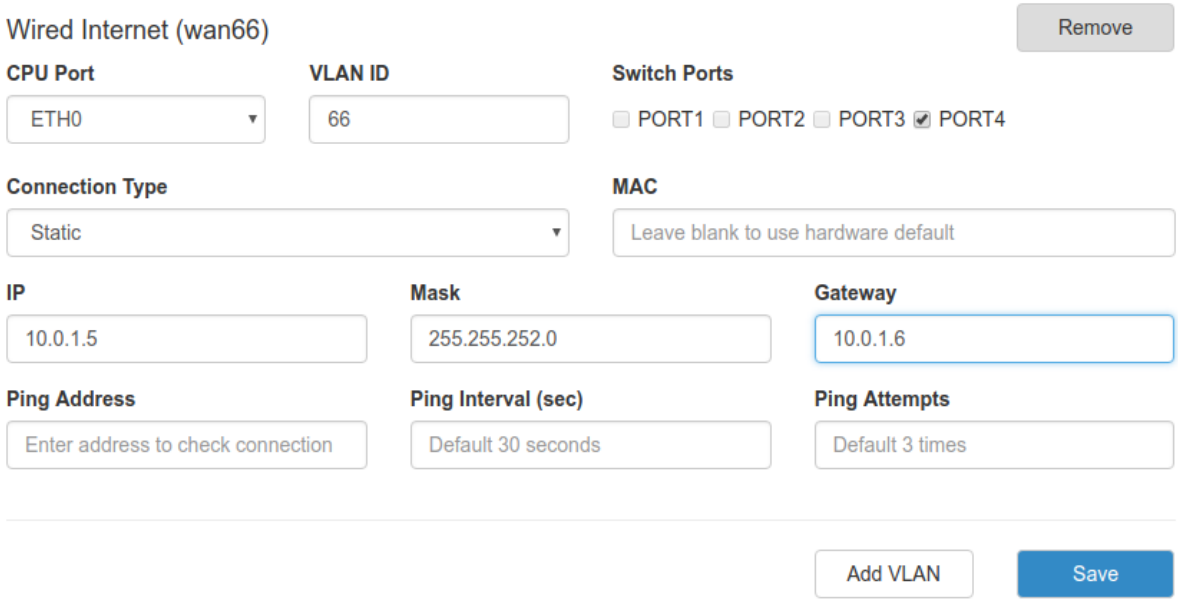


Рис. 33. Примеры конфигураций GRE. Настройка WAN

Далее необходимо настроить GRE-туннель (см. рисунок ниже):

6. Зайдите в раздел **VPN/Tunnels → GRE Tunnels**;
7. Добавьте новый туннель, нажав на кнопку **Add Tunnel**;
8. Введите имя туннеля (на выбор пользователя) в поле **Name**;
9. Выберите интерфейс, через который будет работать туннель в поле **Local Address**;
10. Укажите IP-адрес порта удаленного устройства, с которым будет построен туннель, в поле **Remote Address**;
11. Выберите на каком уровне будет работать туннель в поле **Network Type** (в данном примере рассматривается L3);
12. Укажите IP-адрес интерфейса в поле **Tunnel IP**; а также его маску в поле **Tunnel Mask** при необходимости, если не указывать — маска будет назначена автоматически и будет равна /32.
13. Выберите правило работы межсетевого экрана (firewall), если необходимо, выбрав значение в поле **Firewall Zone** (правила можно настроить вручную в разделе **Services → Firewall**);
14. При необходимости, поставьте устройству запрет на фрагментацию (разделение) пакета на маршруте следования, поставив галочку напротив пункта **Don’t fragment**.

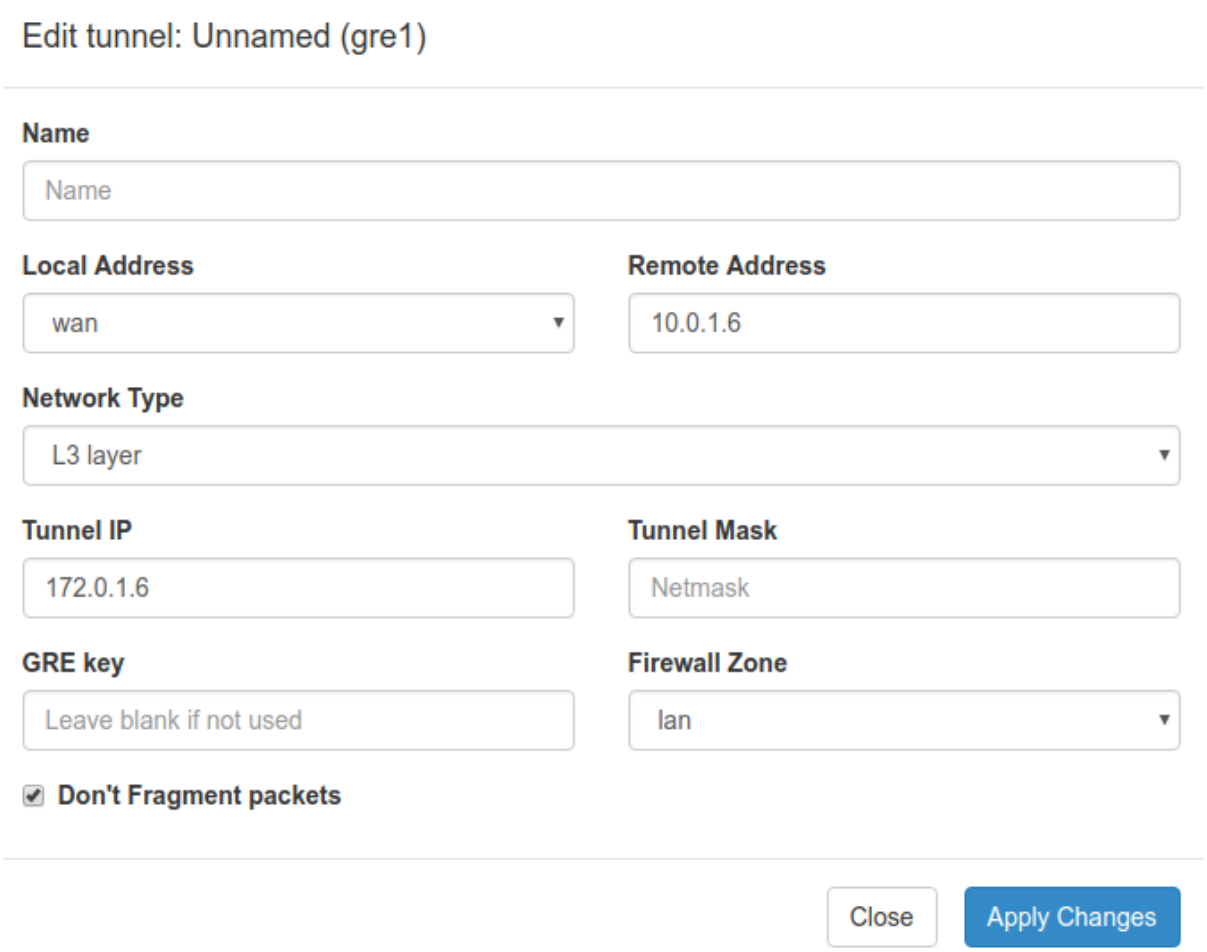


Рис. 34. Примеры конфигураций GRE. Настройка GRE-туннеля

5.3.6. IPsec

Настройка IPSec туннеля

Для создания IPsec-туннеля на роутере должна быть настроена локальная сеть и порты WAN.

Добавить новый IPsec-туннель можно, нажав на кнопку **Add Tunnel**.

Разрешить или запретить работу уже настроенного туннеля можно, поставив галочку в поле **Enable**.

Изменить параметры или удалить туннель можно с помощью кнопок **Edit** и **Remove**.

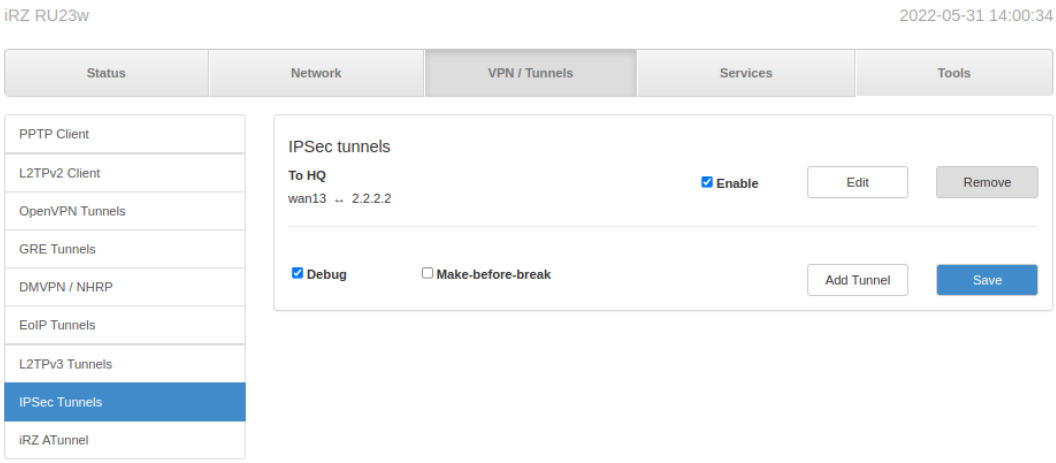


Рис. 35. Вкладка IPSec/Tunnels. Раздел IPSec tunnels

Чекбокс **Debug** увеличивает количество отладочной информации в логе.

Чекбокс **Make-before-break** включает соответствующий метод повторной аутентификации. В этом случае сначала создаются дубликаты SA (Security Associations), перекрывающиеся с существующими, а только затем удаляются старые. Это позволяет избежать разрывов соединения.

Для того чтобы метод **Make-before-break** работал, нужно чтобы оба одноранговых узла могли обрабатывать перекрывающиеся SA.

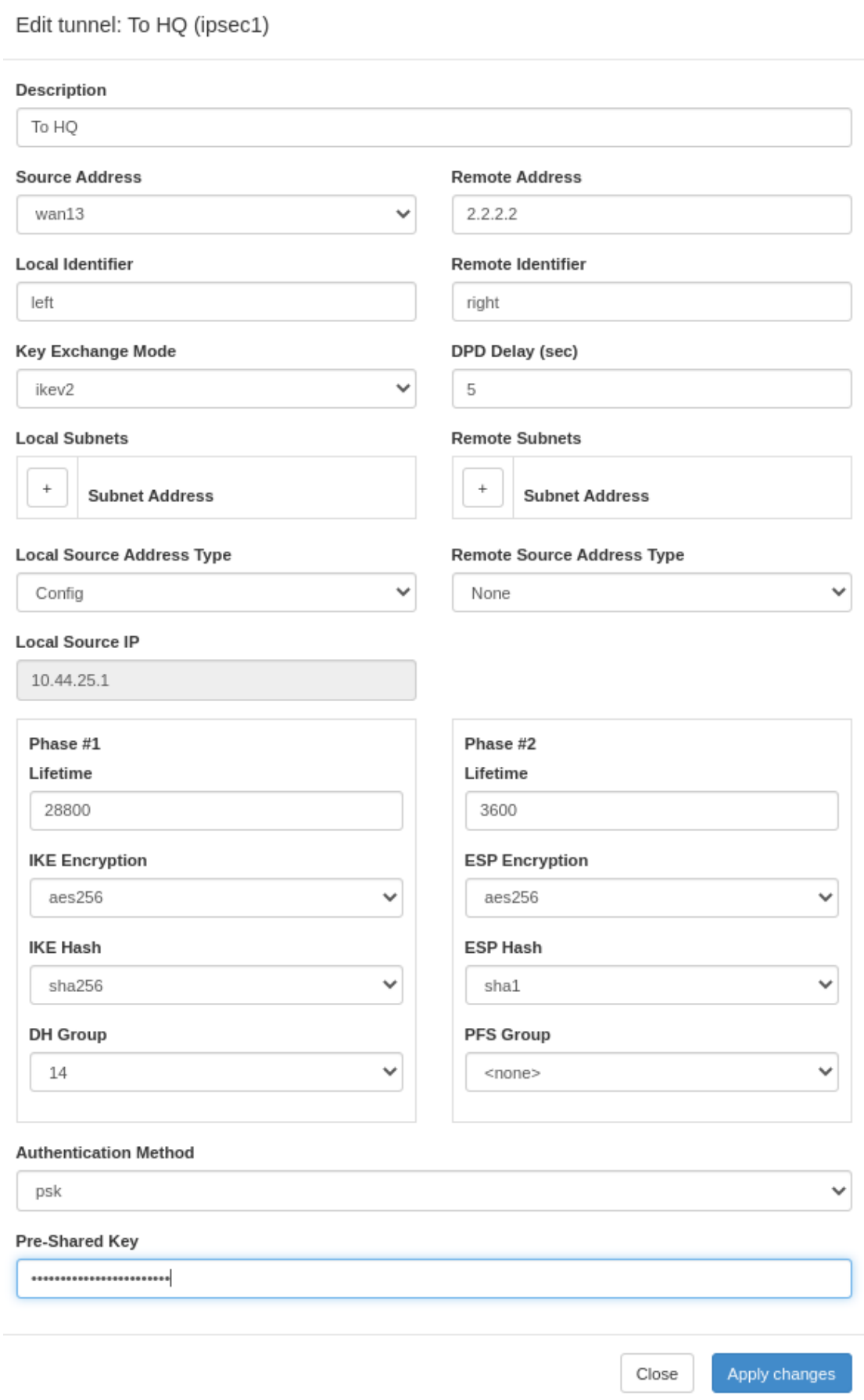


Рис. 36. Примеры конфигураций IPsec. Настройка IPsec-туннеля

Таблица 22. Параметры туннеля

Поля	Описание
Description	Описание туннеля (на выбор пользователя)
Source Address	Физический интерфейс, через который будет работать туннель **Default** – через интерфейс, являющийся на данный момент активным WAN-портом, другие варианты - **SIM1, SIM2, WAN**
Remote Address	IP-адрес порта удаленного хоста, с которым будет построен туннель. Можно указать несколько адресов через ПРОБЕЛ. IPSec выполняет попытки подключения к хостам в порядке их перечисления. Таймаут подключения 60 секунд. Если в течение этого времени подключение не произошло, происходит переключение на следующий адрес (хост) и так по кругу.
Local Identifer	Локальный идентификатор (наименование, указывается пользователем)
Remote Identifer	Идентификатор удаленной стороны (наименование, указывается пользователем)
Key Exchange Mode	Версии протокола обмена ключей при установлении туннеля - **IKEv1** или **IKEv2**
Exchange Mode	**Только** при условии **Key Exchange Mode** версии **IKEv1**. Режим установления соединения между участниками туннеля (**Main** – основной, **Aggressive** – более быстрый, но без обеспечения защиты подлинности на данном этапе).
Dead Peer Detect	Интервал в секундах, через который будет определяться доступность узла на противоположном конце туннеля (**0** – отключение данной функции)
Local Subnets	Список адресов сетей с локальной стороны, между которыми устанавливается туннель (записываются в формате CIDR)
Remote Subnets	Список адресов сетей с удаленной стороны, между которыми устанавливается туннель (записываются в формате CIDR)
Local Source Address Type	Тип получения виртуального IP адреса для локальной стороны (**None** - не настраивается, **Config** - получить автоматически, **Manual** - настроить вручную)
Remote Source Address Type	Тип получения виртуального IP адреса для удаленной стороны (**None** - не настраивается, **Config** - получить автоматически, **Manual** - настроить вручную)
Local Source IP	Виртуальный IP адрес локальной стороны, используемый туннелем
Remote Source IP	Виртуальный IP адрес удаленной стороны, используемый туннелем
Authentication Method	**psk** – по общему ключу, **pubkey** – по сертификату и ключу RSA

Таблица 23. Параметры Phase #1

Поля	Описание
Lifetime	Время жизни ключа в секундах, создаваемого на этапе фазы. Рекомендуется устанавливать значение минимум в два раза больше, чем у фазы 2 (например, 24 часа или 86400 секунд).
IKE Encryption	Выбор алгоритма шифрования: AES 128, AES 192, AES 256, 3DES.
IKE Hash	Выбор алгоритма для проверки целостности данных: SHA-1, SHA-256, SHA-512, SHA-384, MD5.
DH Group	Выбор криптографического алгоритма, который позволяет двум точкам обмениваться ключами через незащищенный канал. Числа – обозначают сложность ключа, чем выше, тем надежнее ключ.

Таблица 24. Параметры Phase #2

Поля	Описание
Lifetime	Время жизни ключа в секундах, создаваемого на этапе фазы. Рекомендуется устанавливать значение меньше, чем у фазы 1 (например, 1 час или 3600 секунд).
ESP Encryption	Выбор алгоритма шифрования: AES 128, AES 192, AES 256, 3DES.
ESP Hash	Выбор алгоритма для проверки целостности данных: SHA-1, SHA-256, SHA-384, SHA-512, MD5.
PFS Group	Выбор криптографического алгоритма, который удостоверяет, что ключи, используемые в фазе 2 не получены от фазы 1. Числа – обозначают сложность ключа, чем выше, тем надежнее ключ.

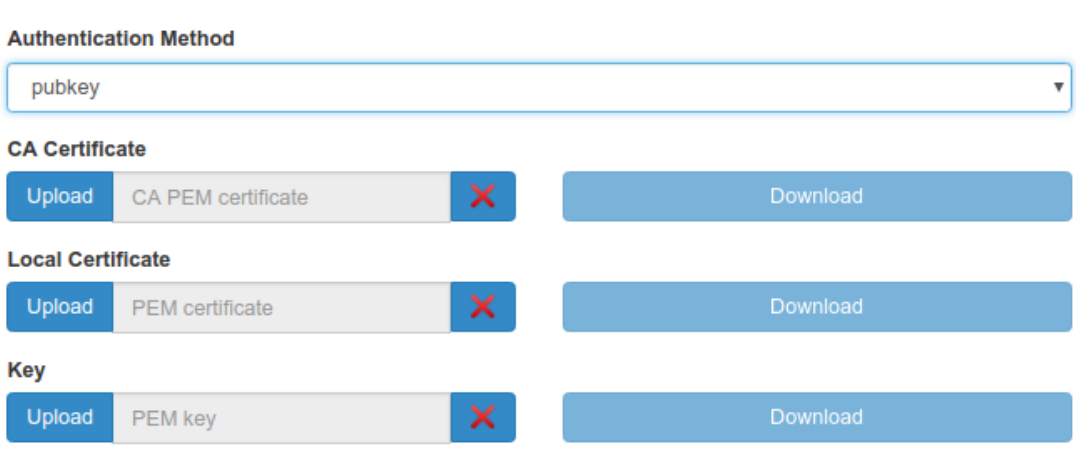


Рис. 37. Способ аутентификации pubkey

В целях безопасности для входящих подключений запрещено использование функции IPsec с параметрами: KeyExchangeMode = ikev1, Agressive mode=yes, Authentification Method = PSK.

Статус IPSec туннеля

На вкладке **Status** представлена информация о состоянии туннелей, настроенных на роутере.

IPSec tunnel — информация о работе IPSec туннеля

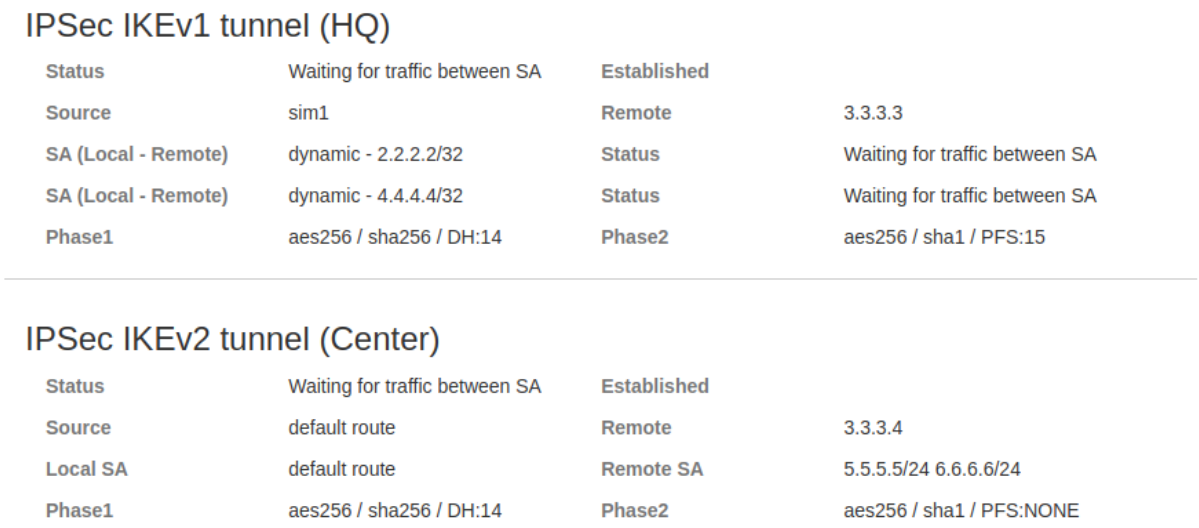


Рис. 38. Пример информации в разделе IPSec tunnel

Таблица 25. 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 26. 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)

5.3.7. DMVPN / NHRP (только для роутеров серии R4, R2)

Dynamic Multipoint VPN (DMVPN) — виртуальная частная сеть с возможностью динамического создания туннелей между узлами. Роутеры для данного туннеля могут выступать только в роли Spoke- маршрутизатора.

Для создания данного туннеля необходимо в разделе **VPN/Tunnels → DMVPN/NHRP нажать кнопку Add Tunnel** и на открывшейся странице настроек (см. рисунок ниже) заполнить поля согласно таблице приведенной далее.

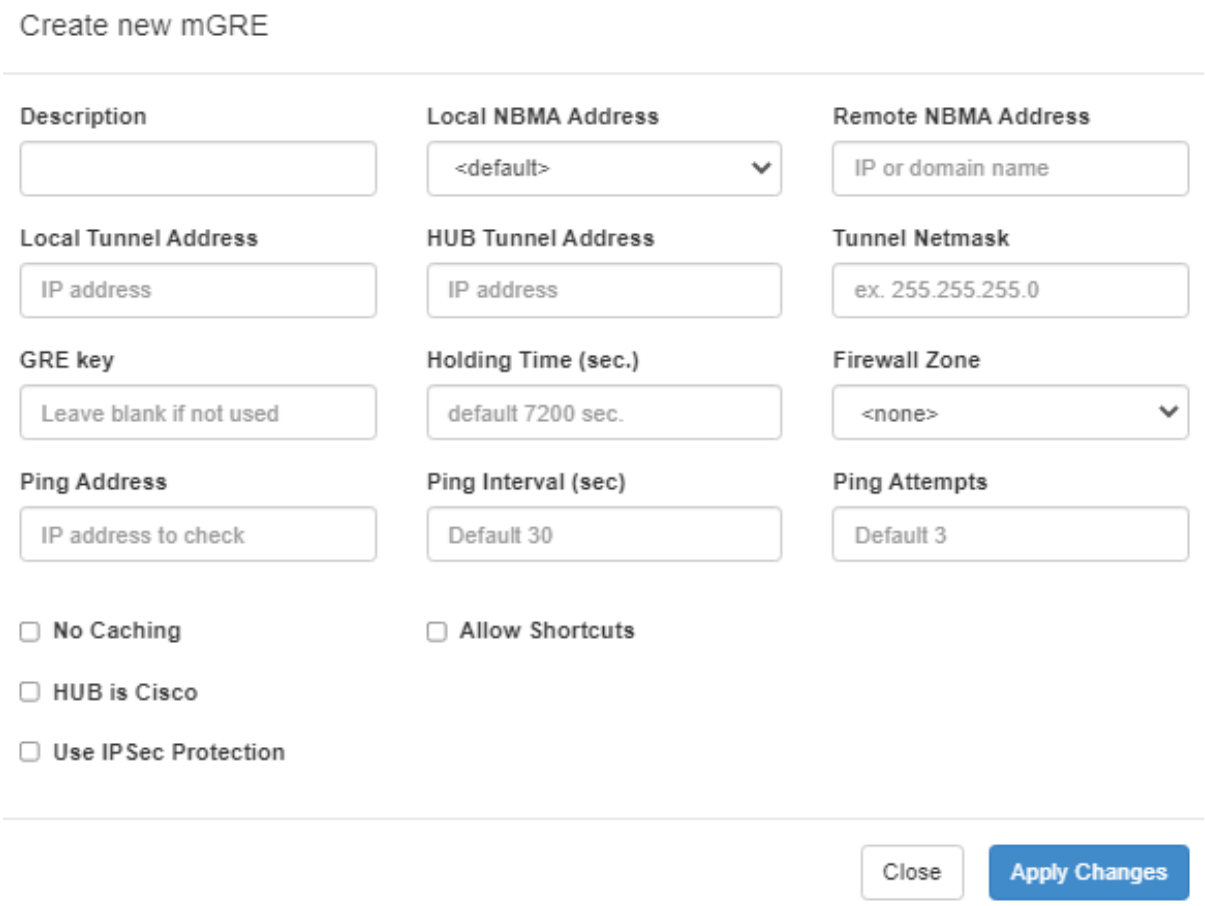


Рис. 39. Страница настроек DMVPN/NHRP

Таблица 27. Настройки DMVPN/NHRP

Поля	Описание
Description	Описание или название туннеля.
Local NBMA Address	Локальный адрес сети - NBMA(Non Broadcast Multiple Access), необходимо выбрать один из интерфейсов роутера; значение <default> означает использование интерфейса с маршрутом по умолчанию.
Remote NBMA Address	Удаленный адрес NBMA — указывается только IP адрес.
HUB Tunnel Address	Туннельный IP адрес HUBa к которому происходит подключение.
Tunnel Mask	Маска сети туннеля.
Holding Time (sec.)	Время (в секундах) в течение которого информация о соседнем NBMA хосте считается действительной.
Local Tunnel IP	Туннельный IP адрес данного роутера.
GRE key	Идентификационный ключ GRE туннеля в случае если данный функционал используется в конфигурации.
Firewall Zone	Зона, в которой будет находится туннель и соответственно политики фаервола, которые будут применяться к данному туннелю.
Ping Address	Адрес для проверки работоспособности туннеля (проверка доступности туннеля ICMP пакетами). Несколько адресов могут быть указаны через **;** или через ПРОБЕЛ
Ping Interval (sec)	Интервал проверки.
Ping Attemts	Количество попыток, по истечении которых роутер попытается переустановить туннель.
No Caching	Отключает кэширование информации о пирах из пересылаемых пакетов ответа на разрешение NHRP. Это можно использовать для уменьшения потребления памяти в больших подсетях NBMA.
Allow Shortcuts	Разрешает помещение в таблицу маршрутизации только тех префиксов, которые реально используются в данный момент времени.

Таблица 27. Настройки DMVPN/NHRP

HUB is Cisco	Данная настройка позволяет ввести ключ аутентификации в случае если хабом является оборудование компании Cisco.
No Unique	Флаг неуникальности ip-адреса туннеля в базе nhrp на hub-маршрутизаторе
Allow Redirects	Разрешает направлять трафик напрямую между spoke маршрутизаторами в обход хаба
Use IPSec Protection	Открывает дополнительное поле с возможностью настроить шифрование туннеля с помощью IPSec

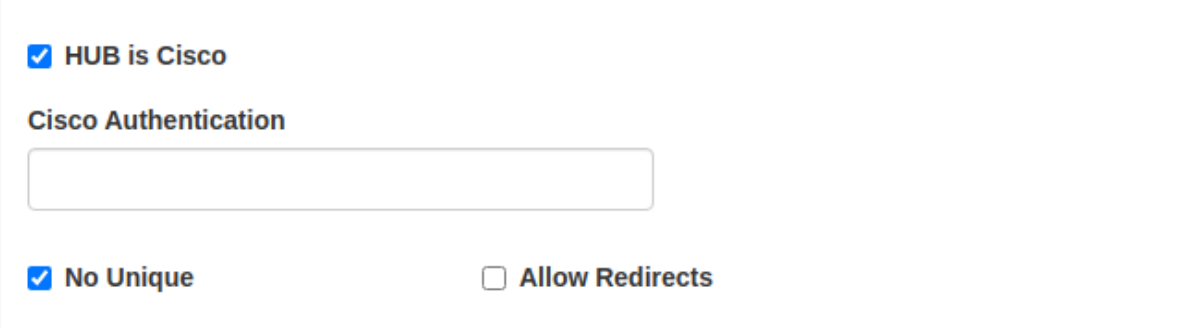


Рис. 40. Поле ввода ключа аутентификации для оборудования Cisco

Таблица 28. Настройка шифрования туннеля с помощью IPSec

Поля	**Описание**
Local Identifier	Локальный идентификатор.
Remote Identifier	Идентификатор удаленной стороны.
Key Exchange Mode	Предназначено для переключения между первой и второй версиями обмена ключей.
Authentication Method	Способ аутентификации узлов туннеля: psk – по общему ключу, rsasig – по сертификату и ключу RSA (то же что и pubkey).
DPD Delay (sec.)	Интервал отправки DPD и keepalive пакетов.
DPD Timeout (sec.)*	Интервал по которому рвётся соединение.
Agressive Mode*	Включение/отключение более активного [быстрого] режима (без обеспечения защиты подлинности).

В случае использования шифрования туннеля с помощью технологии IPSec необходимо настроить соответствующие параметры туннеля. Подробная информация о каждом параметре приведена в разделе IPsec туннели.

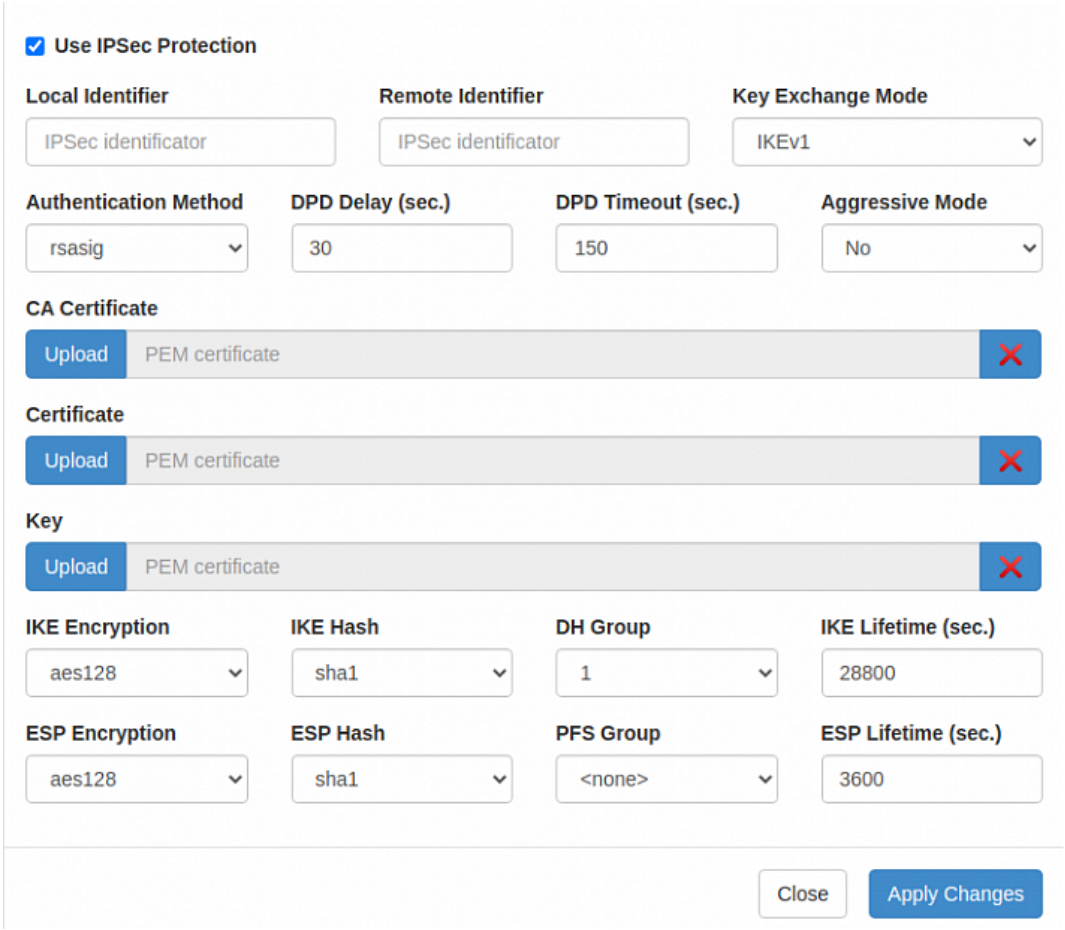


Рис. 41. Поле настройки шифрования туннеля с помощью IPSec

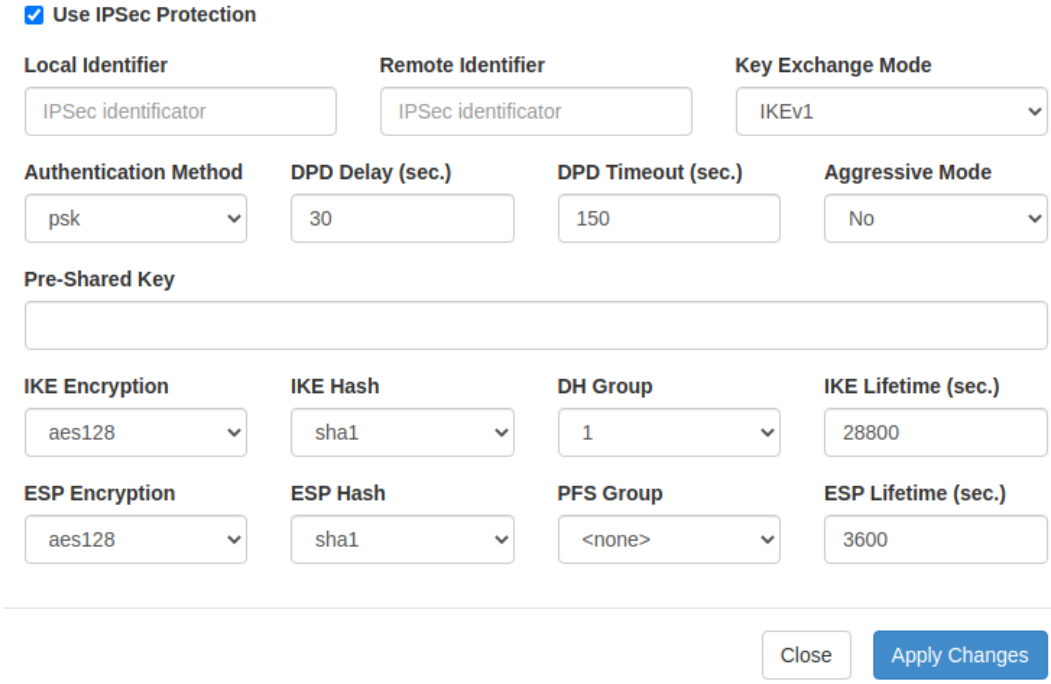


Рис. 42. Поле настройки шифрования туннеля с помощью IPSec

5.3.8. EoIP

Ethernet over IP (EoIP) — тип туннеля, разработанный компанией MikroTik, представляет собой Ethernet туннель точка-точка поверх IP подключения. Данный туннель создает мост между двумя роутерами как будто эти роутеры подключены друг к другу напрямую через физические ethernet порты. Такой туннель можно создавать поверх любого другого туннеля или подключения, умеющего транспортировать протокол IP. Пример настроек туннеля приведен на рисунке ниже.

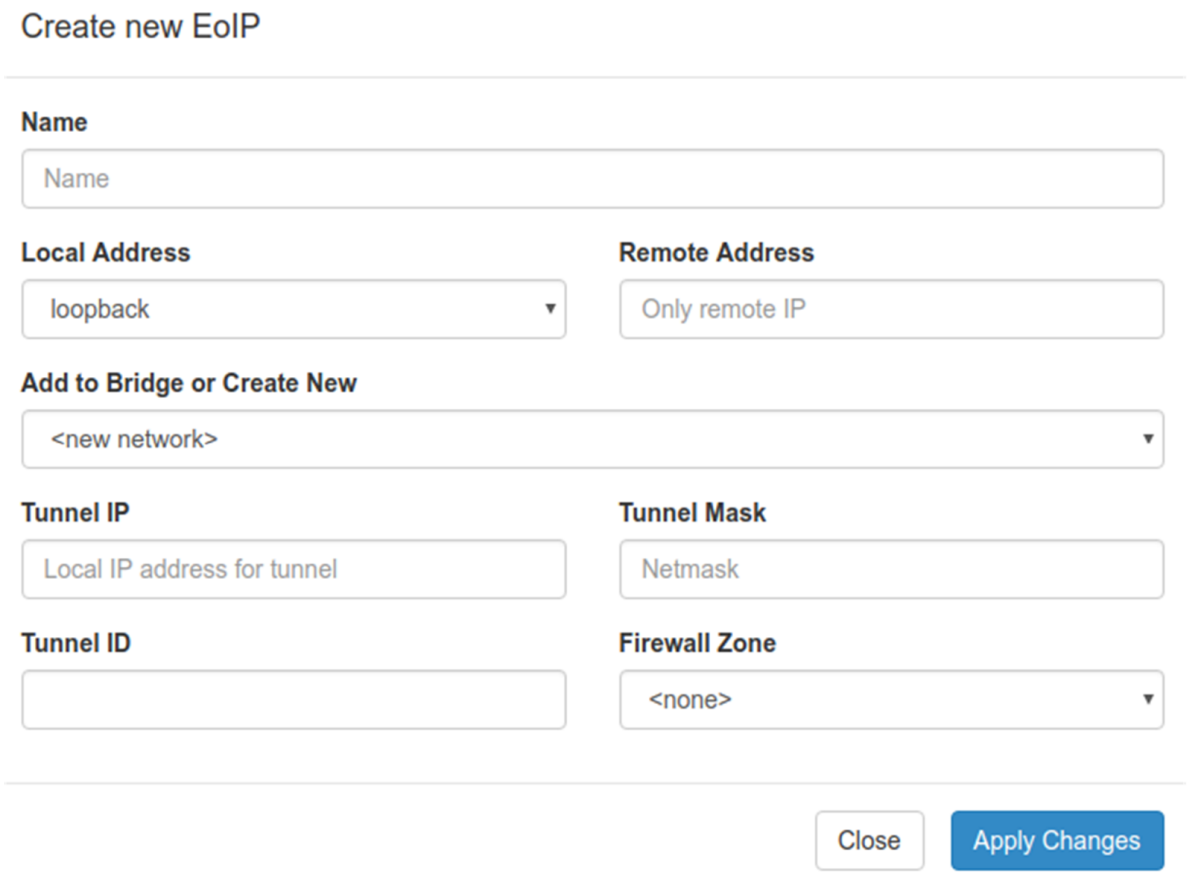


Рис. 43. Настройка EoIP-туннеля

Для создания туннеля необходимо проделать следующие шаги:

1. Зайдите в раздел **VPN / Tunnels** → **EoIP Tunnels** и создайте новый туннель кнопкой **Add Tunnel**.
2. В открывшихся настройках туннеля укажите имя туннеля в поле **Name**, если требуется.
3. В поле **Local Address** укажите интерфейс через который будет работать туннель.
4. В поле **Remote Address** необходимо указать адрес удаленной точки туннеля.
5. В поле **Add to Bridge or Create New** необходимо выбрать локальную сеть с которой будет создан мост или же задать отдельный адрес туннельного интерфейса.
6. В случае если в предыдущем пункте выбран вариант задания отдельного адреса для интерфейса туннеля необходимо в полях **Tunnel IP** и **Tunnel Mask** указать IP адрес и маску сети для интерфейса туннеля.

7. Поле **Tunnel ID** предназначено для задания идентификационного номера туннеля, в случае если создается несколько туннелей с терминированием на одной удаленной точке, для того чтобы текущий роутер и удаленный могли различать пакеты разных туннелей.

8. Поле **Firewall Zone** предназначено для ассоциации туннеля с одной из зон фаервола.

5.3.9. L2TPv3

L2TPv3 (англ. Layer 2 Tunneling Protocol — протокол туннелирования второго уровня версия 3) — в компьютерных сетях туннельный протокол, использующийся для поддержки виртуальных частных сетей.

Для настройки туннеля необходимо зайти в раздел VPN/Tunnels → L2TPv3 и добавить новый туннель по кнопке Add Tunnel.

В открывшемся окне настроек (см. рисунок ниже) заполнить поля согласно таблице приведенной далее.

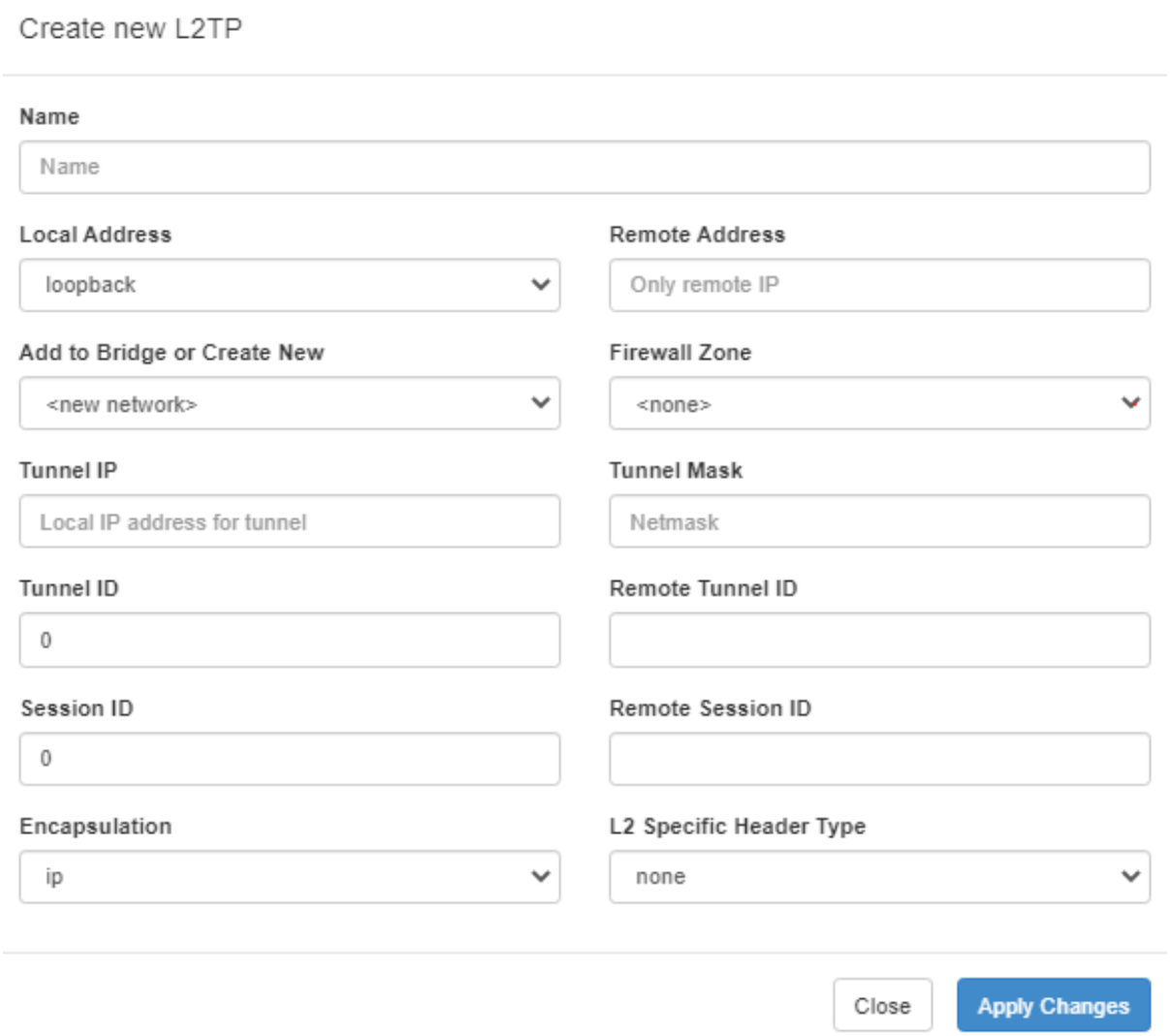


Рис. 44. Настройка L2TP3-туннеля

Таблица 29. Настройки L2TP3

Поля	Описание
Name	Название туннеля.
Local Address	Локальный интерфейс на роутере через который будет устанавливаться соединение.
Remote Address	IP-адрес удаленной сети, участвующей в туннеле.
Add to Bridge or Create New	Установление моста с каким-то из локальных интерфейсов (lan) роутера или создание отдельного интерфейса со своей подсетью - <new network>.
Tunnel IP	IP адрес туннельного интерфейса.
Tunnel Mask	Маска сети туннельного интерфейса.
Tunnel ID	ID — идентификатор туннеля на данном устройстве.
Session ID	ID — идентификатор сессии на данном устройстве.
Firewall Zone	Включение туннельного интерфейса в одну из зон фаервола.
Remote Tunnel ID	ID — идентификатор удаленного конца туннеля.
Remote Session ID	ID — идентификатор сессии на удаленном конце туннеля.
Encapsulation	Выбор способа идентификации сессии туннеля, для синхронизации настройки с двух сторон туннеля.
L2 Specific Header Type	Указывает специальное поле подуровня L2TPv3 Layer 2 для использования в заголовках пакетов данных в соответствии с RFC3931

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!

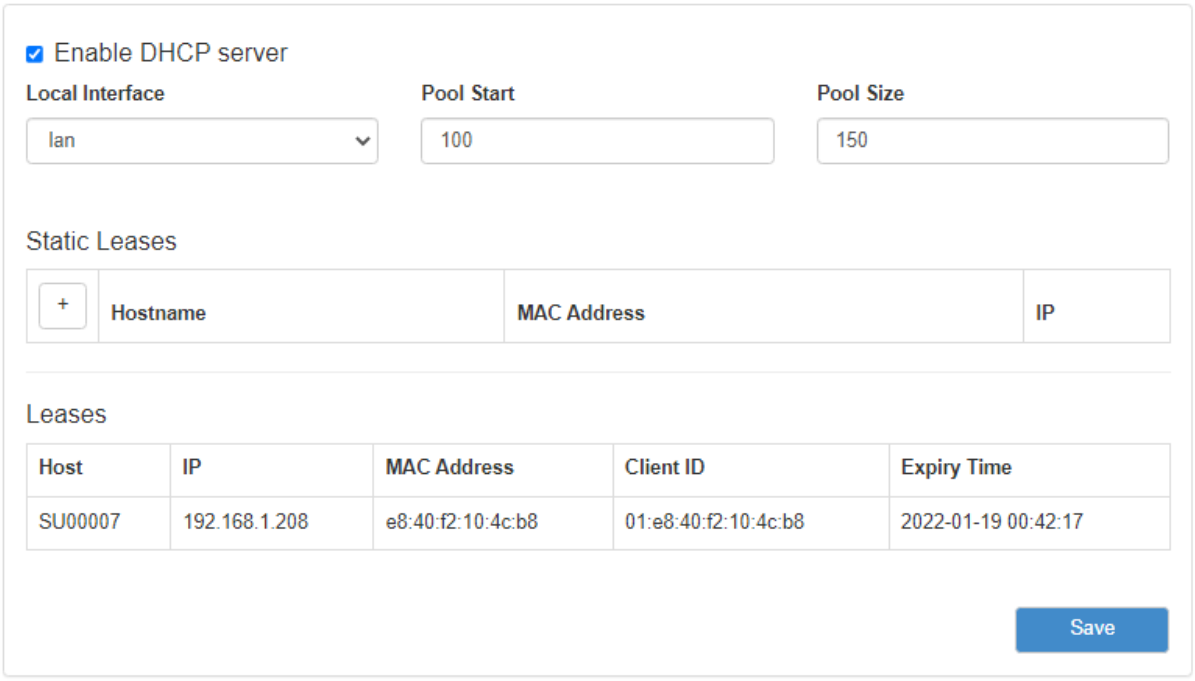


Рис. 45. Вкладка Services, раздел DHCP

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

Таблица 30. 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.

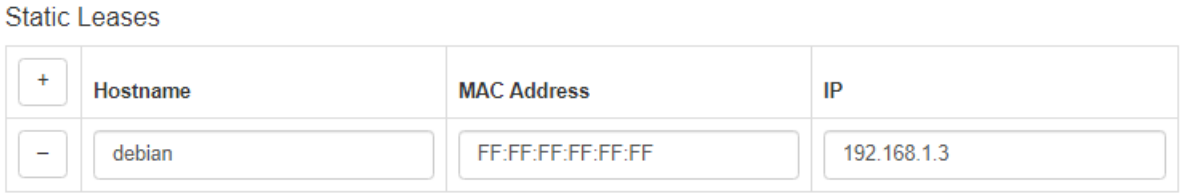


Рис. 46. Указание IP-адресов вручную

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. 47. Вкладка Tools, раздел DHCP Leases

Таблица 31. 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!

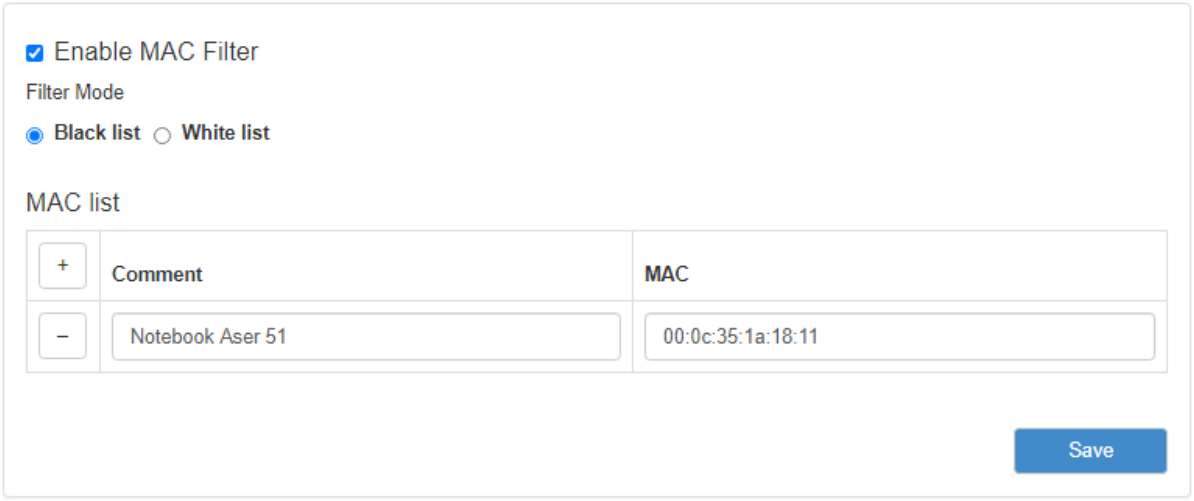


Рис. 48. Вкладка Services, раздел MAC Filter

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!

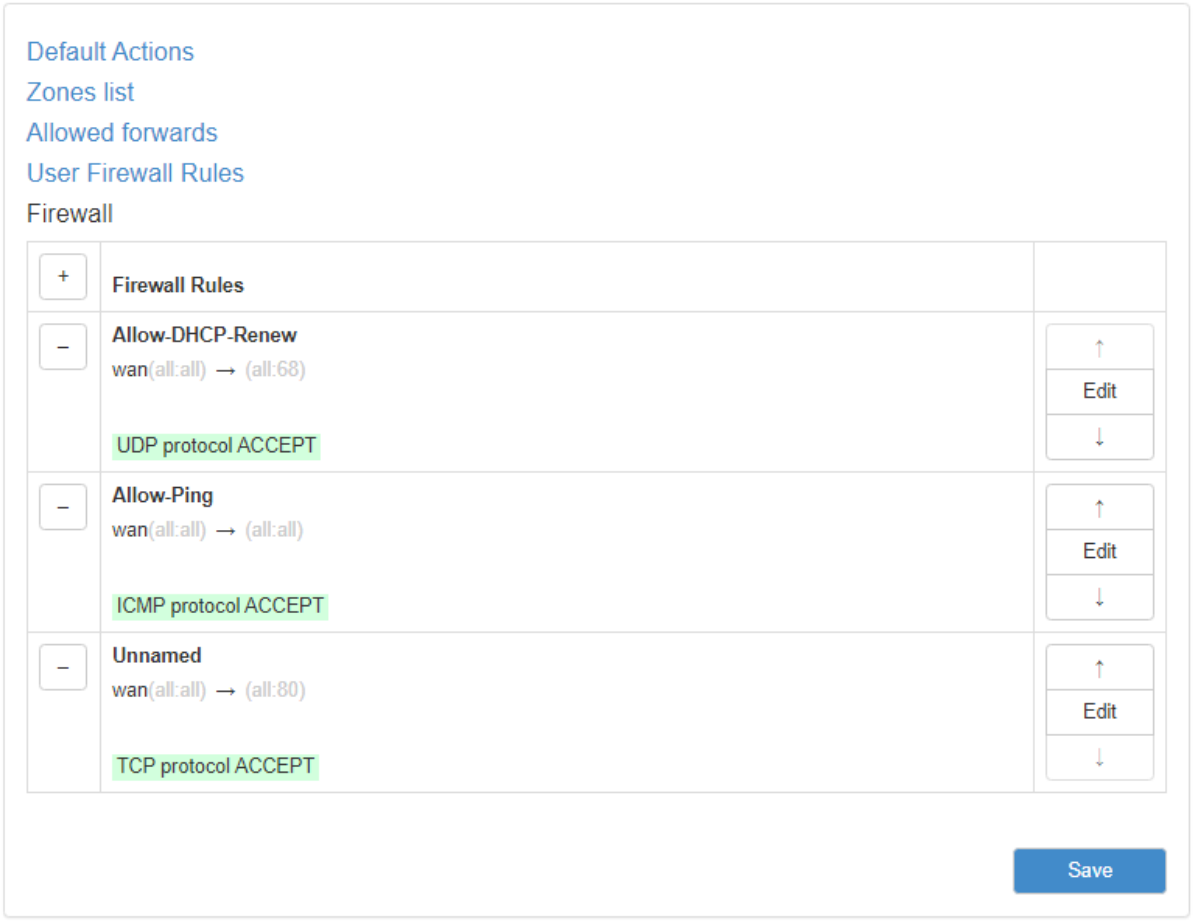


Рис. 49. Вкладка Services, раздел Firewall

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.

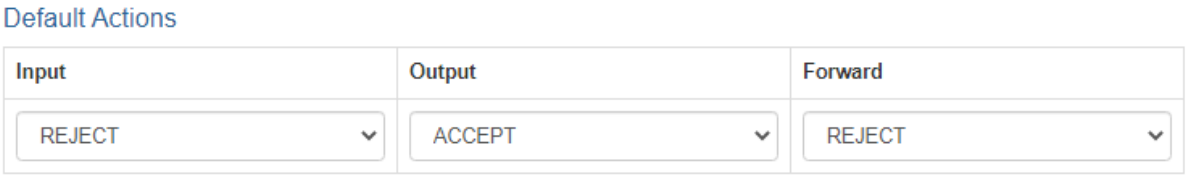


Рис. 50. Вкладка Services, раздел Firewall, настройки Default Actions

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 32. 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

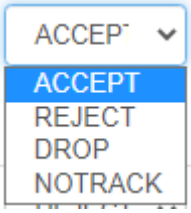


Рис. 51. Вариант выбора действий для трафика

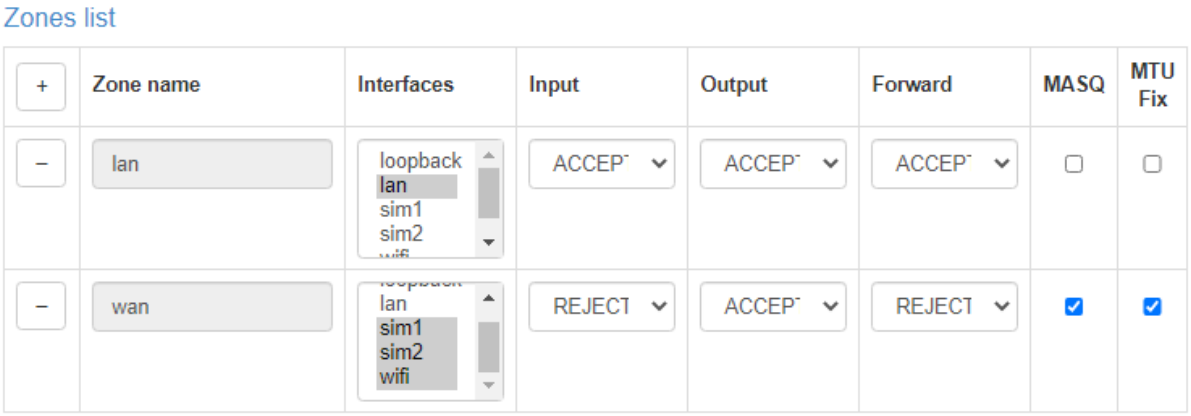


Рис. 52. Вкладка Services, раздел Firewall, настройки Zones List

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.

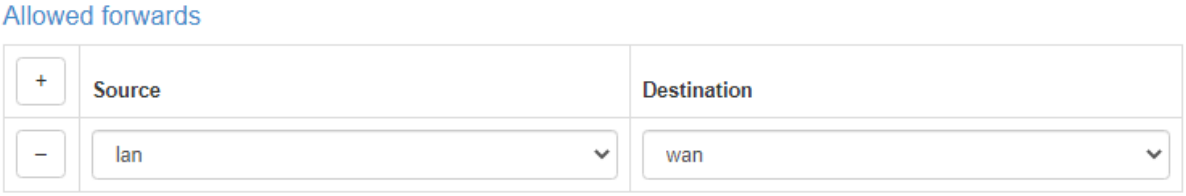


Рис. 53. Настройки Allowed Forwards

Таблица 33. 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.

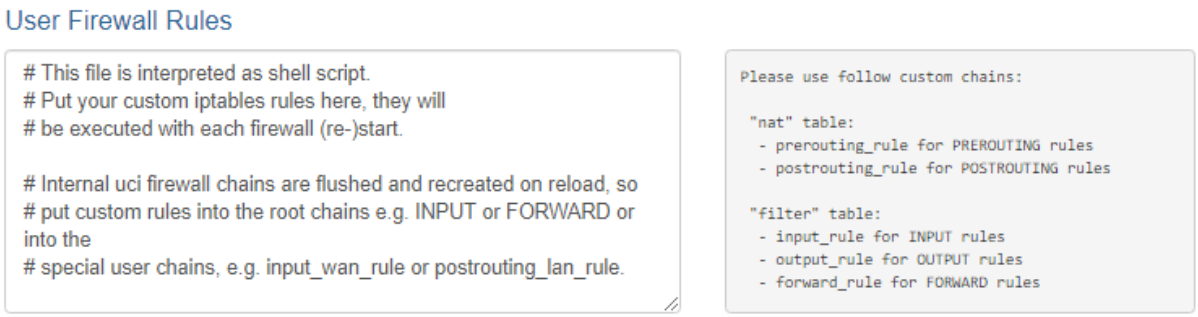


Рис. 54. Вкладка Services, раздел Firewall, настройки User Firewall Rules

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 ↑ ↓

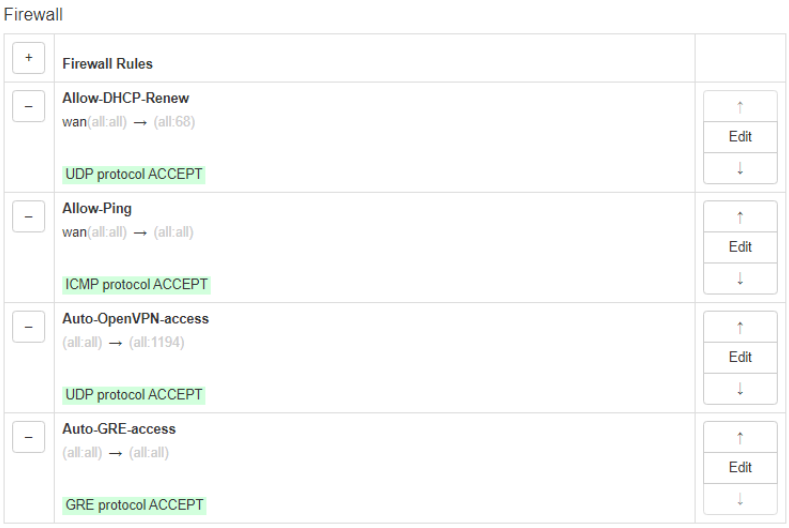


Рис. 55. Настройки Firewall

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.

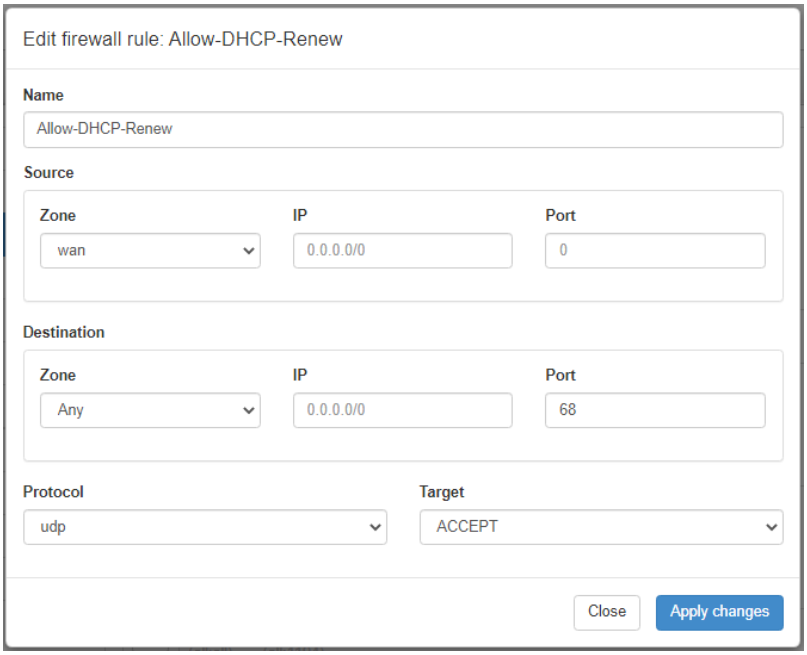


Рис. 56. Редактирование правила Firewall

Таблица 34. Настройки правил для межсетевого экрана

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

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

5.4.4. Port Forwarding

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

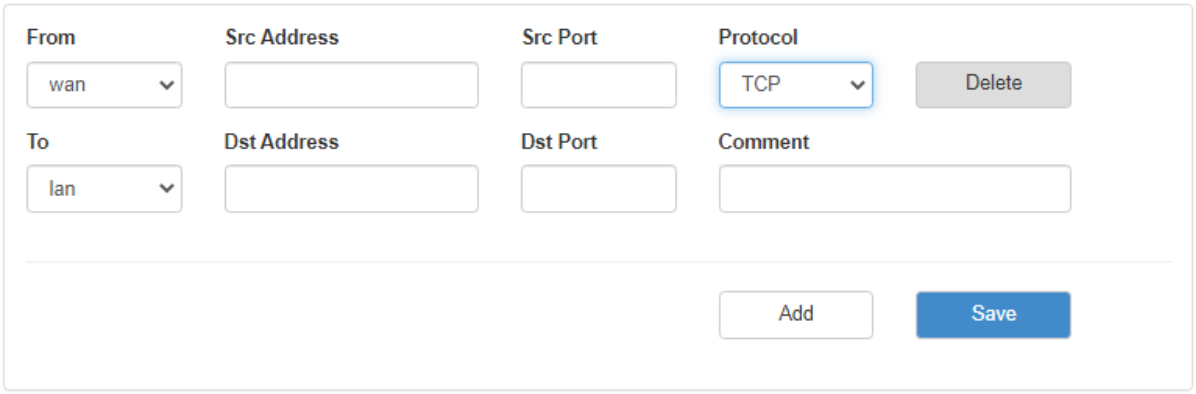


Рис. 57. Вкладка Services, раздел Port Forwarding

Таблица 35. Настройки правил проброса портов

Поле	Описание
Protocol	Выбор протокола, на который будет распространяться правило: TCP, UDP, TCP/UDP (оба протокола) или ALL (предназначен для организации DMZ зоны)
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
Dst Port	Порт приемника трафика, на который роутер будет пересылать пакеты
Dst Address	Ввод IP-адреса приемника трафика, на который роутер будет пересылать пакеты
Comment	Поле для комментария
From	Выбор от какой зоны Firewall будет осуществляться проброс
To	Выбор к какой зоне Firewall будет осуществляться проброс

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!

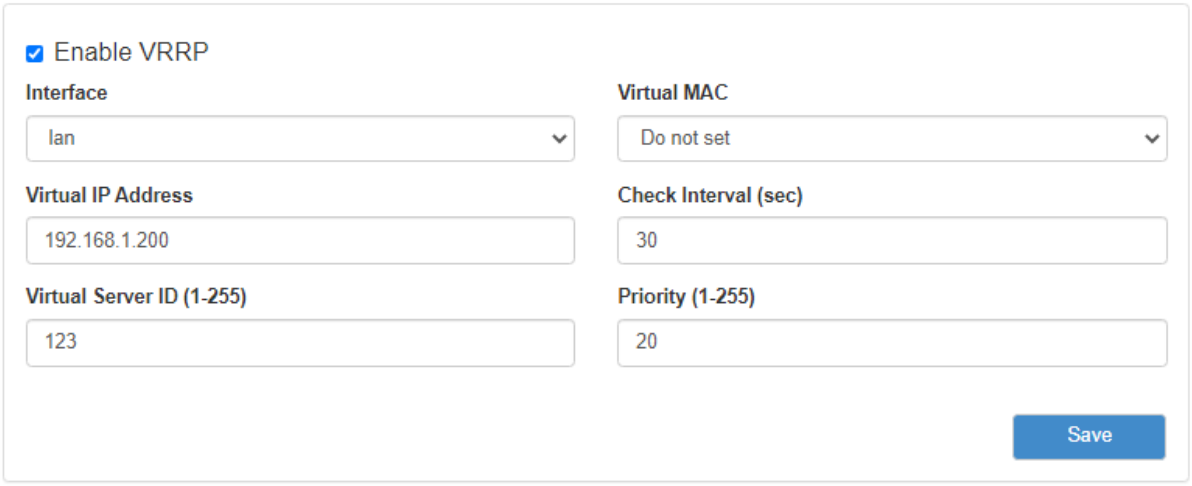


Рис. 58. Вкладка Services, раздел VRRP

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

Таблица 36. 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 36. 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!

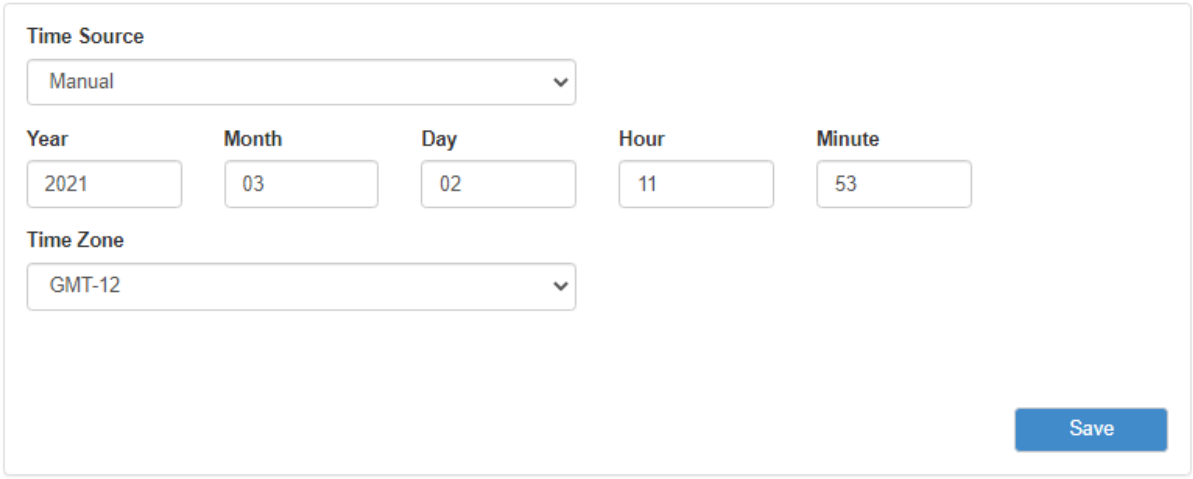


Рис. 59. Настройка времени в ручном режиме

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!

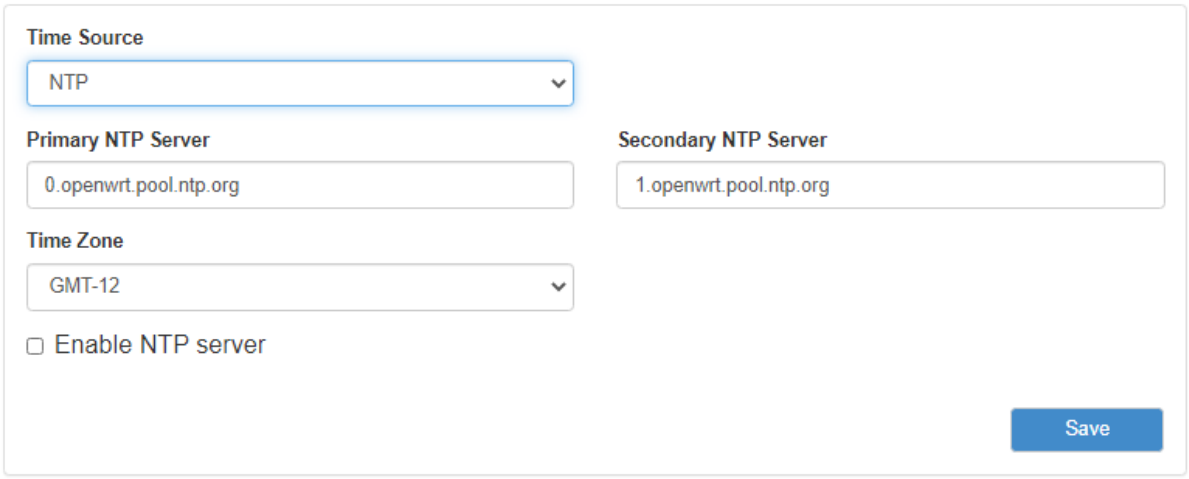


Рис. 60. Настройка времени в автоматическом режиме

5.4.7. SNMP

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

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

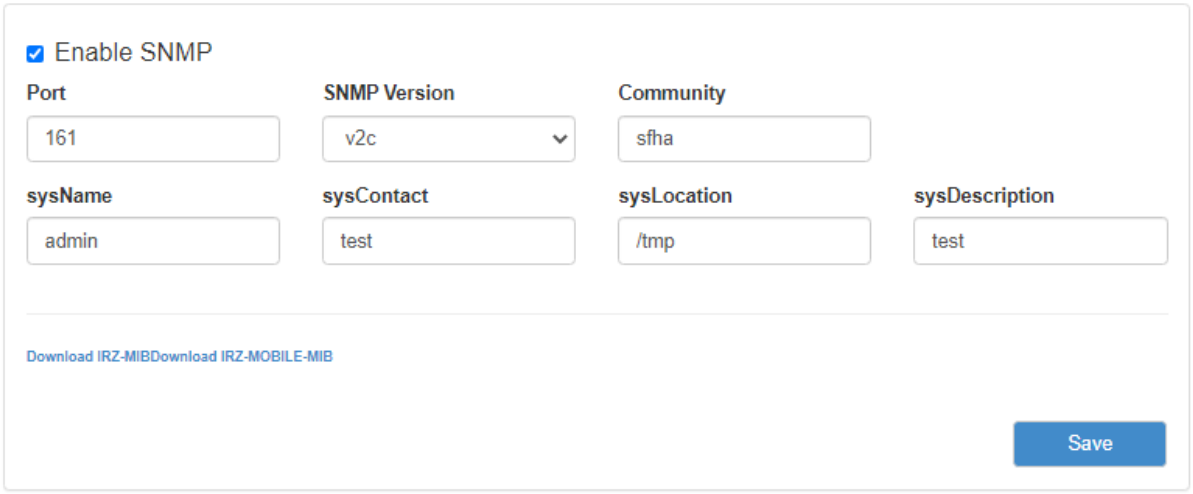


Рис. 61. Вкладка Services, раздел SNMP (v2c)

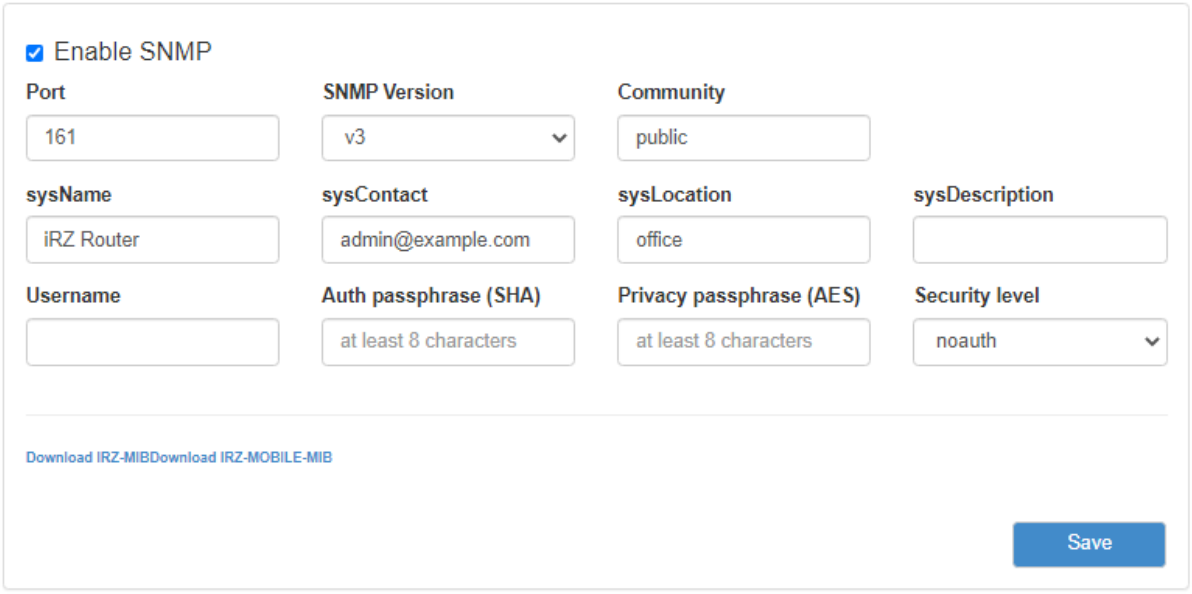


Рис. 62. Вкладка Services, раздел SNMP (v3)

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

Таблица 37. Настройки SNMP

Поле	Версия	Описание
Port	v2c, v3	Порт, через который будет работать протокол SNMP. По умолчанию – «161»
SNMP Version	v2c, v3	Выбор версии протокола: v2c, v3
Community	v2c, v3	«Общая строка», по которой роутер предоставляет данные для системы мониторинга
sysName	v2c, v3	Имя устройства (на выбор пользователя), которое будет использоваться для идентификации данного устройства в системе мониторинга
sysContact	v2c, v3	Контактные данные (на выбор пользователя) в виде электронного адреса, телефона или другого вида
sysLocation	v2c, v3	Описание местоположения устройства (на выбор пользователя)
sysDescription	v2c, v3	Описание устройства (на выбор пользователя)
Username	v3	Имя пользователя для авторизации при контроле роутера по протоколу SNMP
Auth Passphrase (SHA)	v3	Фраза-пароль для шифрования авторизации при контроле роутера по протоколу SNMP, используется алгоритм хэширования SHA
Privacy Passphrase (AES)	v3	Фраза-пароль для шифрования передаваемого трафика от роутера к системе мониторинга, при контроле роутера по протоколу SNMP, используется алгоритм шифрования AES
Security Level	v3	Выбор уровня защиты при 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.

Под настройками SNMP есть две ссылки для скачивания MIB файлов.

5.4.8. DynDNS

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

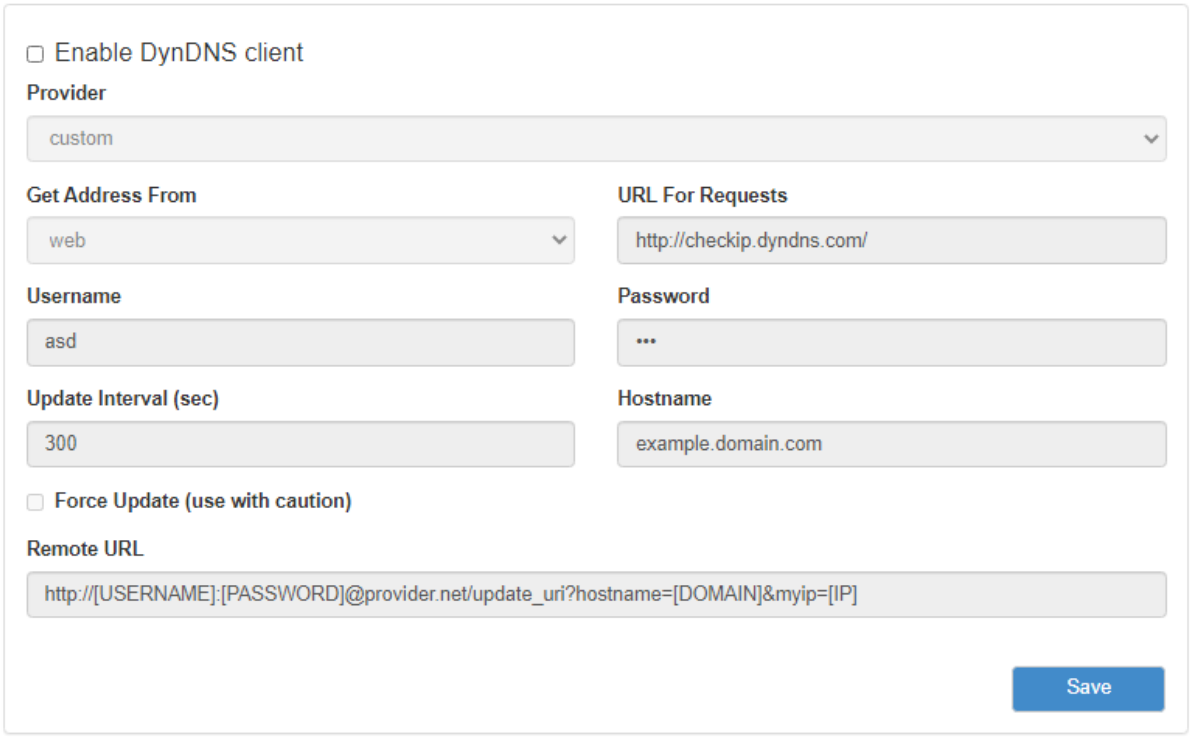


Рис. 63. Вкладка Services, раздел DynDNS

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

Таблица 38. Настройки DynDNS

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

Таблица 38. 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 есть возможность использовать свой собственный сервис динамического DNS или несколько предустановленных распространенных сервиса, см. рисунок ниже.

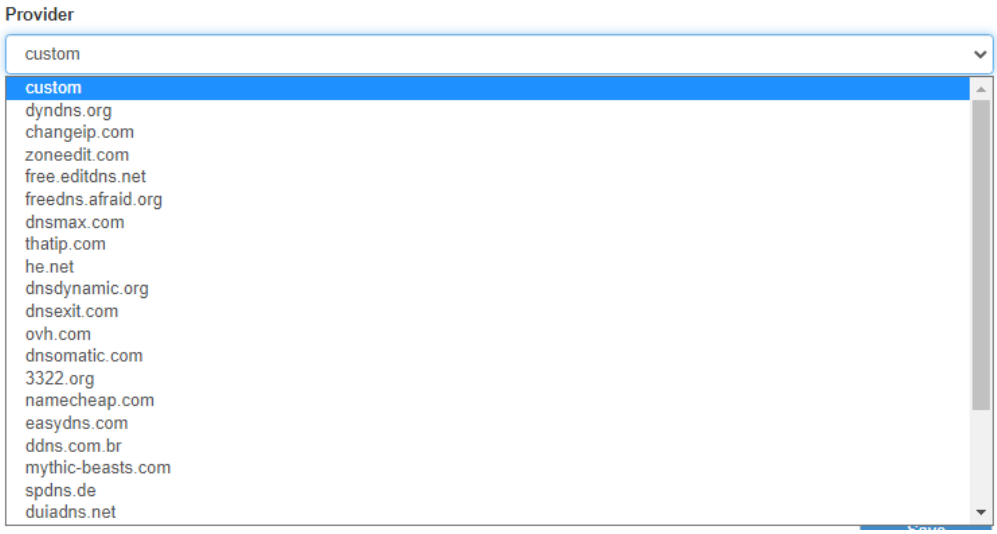


Рис. 64. Сервера DNS

5.4.9. Crontabs

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

Добавление инструкции осуществляется посредством кнопки + («плюс»), а удаление — кнопкой - («минус»). Отметка в столбце **Enable** позволяет включать, или отключать выполнение инструкции без ее удаления. Время указывается в полях: **Minute** (минута, от «0» до «59»), **Hour** (час, от «0» до «23»), **Day** (день, от «1» до «31»), **Month** (месяц, от «1» до «12»), **Weekday** (день недели, от «0» до «7», где 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!

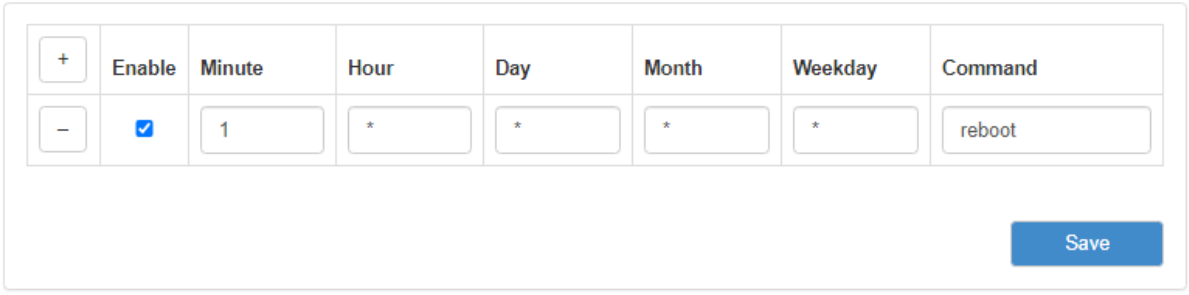


Рис. 65. Вкладка Services, раздел Crontabs

5.4.10. 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.

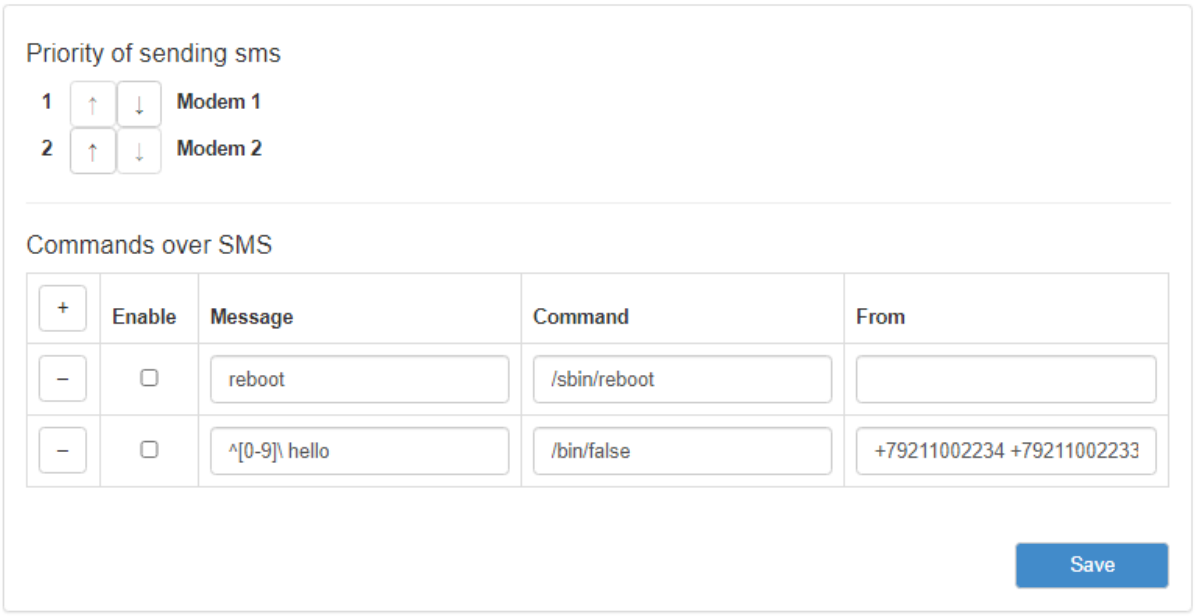


Рис. 66. Вкладка Services, раздел SMS

5.4.11. Serial ports

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

В роутерах 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.

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

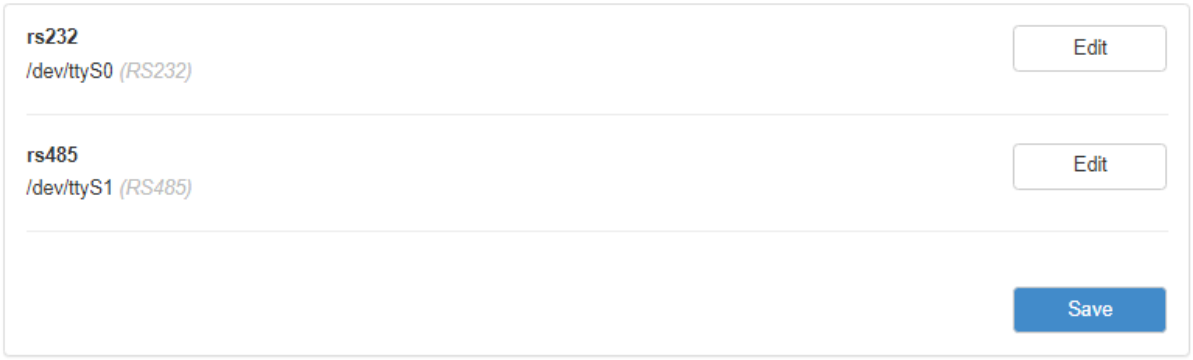


Рис. 67. Вкладка Services, раздел Serial Ports

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 Modbus TCP to RTU** (для серий R2 и R4) — 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.
Чтобы включить порт, нажмите напротив него Edit, поставьте галочку Enable Port via TCP и укажите настройки для его работы (см. таблицу).

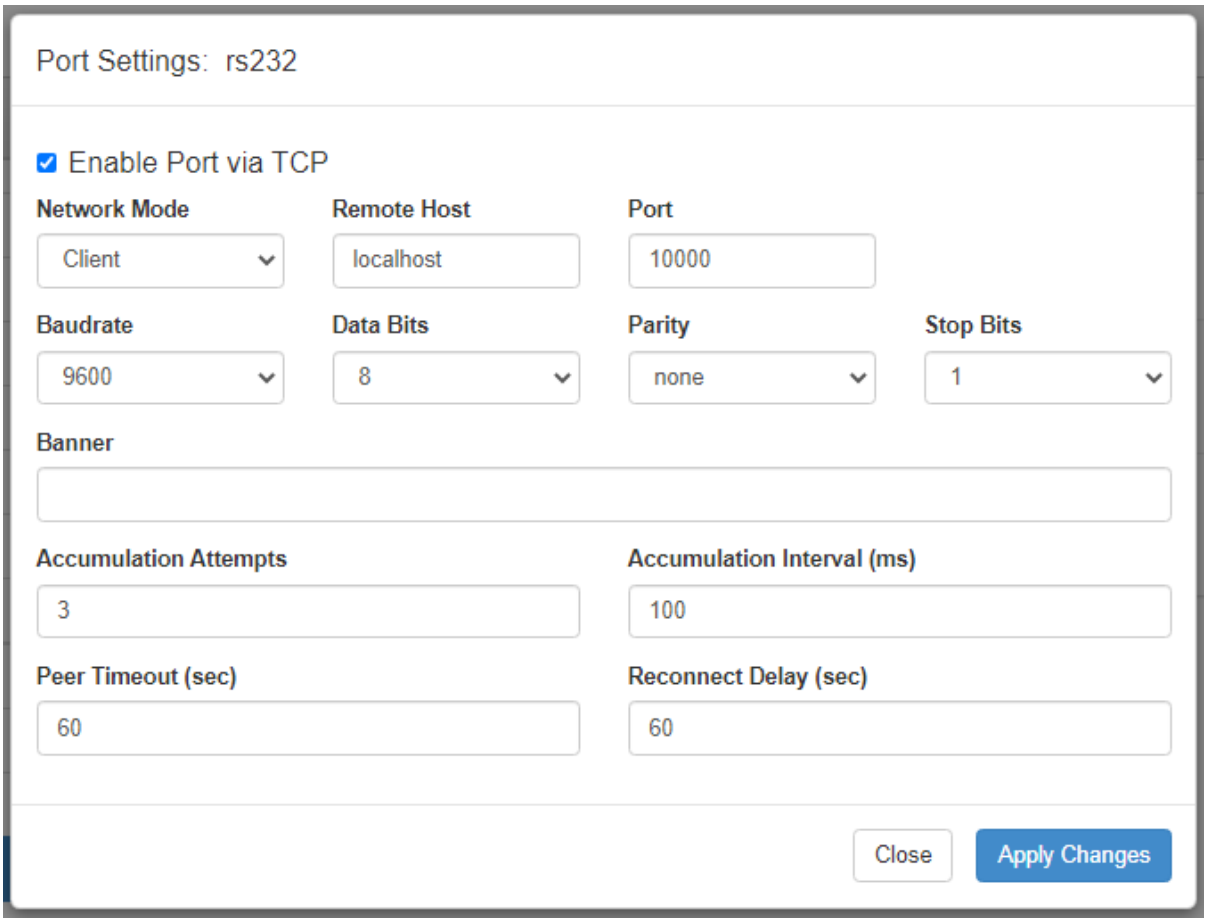


Рис. 68. Вкладка Services, раздел Serial Ports, пример настроек порта RS232

Таблица 39. Настройки Port via TCP (C – клиент, S – сервер, M — server Modbus TCP to RTU)

Поле	Режим	Описание
Network Mode	C, S, M	Режим работы порта: C – клиент, S – сервер, M — server Modbus TCP to RTU
Port	C, S, M	Порт, через который будет осуществляться передача данных
Remote Host	C	IP-адрес сервера, к которому будет подключаться устройство для передачи данных
Baudrate	C, S, M	Скорость передачи данных через порт, бод
Data Bits	C, S, M	Количество бит блока, используемых при передаче данных: 7, 8

Таблица 39. Настройки Port via TCP (C – клиент, S – сервер, M — server Modbus TCP to RTU)

Parity	C, S, M	Режим контроля четности бит в передаваемых блоках: None – без проверки, Odd – проверка на нечетность, Even – проверка на четность
Stop Bits	C, S, M	Количество стоп-бит блока, используемые для определения конца блока: 1, 2
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

О работе RS232/RS485 Server Modbus TCP to RTU

Протокол Modbus TCP предназначен для работы в сети Ethernet. Протокол Modbus RTU использует последовательные интерфейсы (RS-232, RS-485) и имеет режим передачи: RTU. Когда роутер получает запрос Modbus TCP, он преобразует пакет в Modbus RTU и посылает его по последовательному интерфейсу. Когда роутер получает ответ от устройства Modbus RTU, он преобразует его в пакет Modbus TCP и отправляет пакет по Ethernet.
При взаимодействии одно устройство Modbus всегда является ведущим (Master), а второе — ведомым (Slave). Modbus Master всегда отправляет запрос, инициируя обмен данными, а устройство Modbus Slave отправляет ответ. 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

5.4.12. 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.

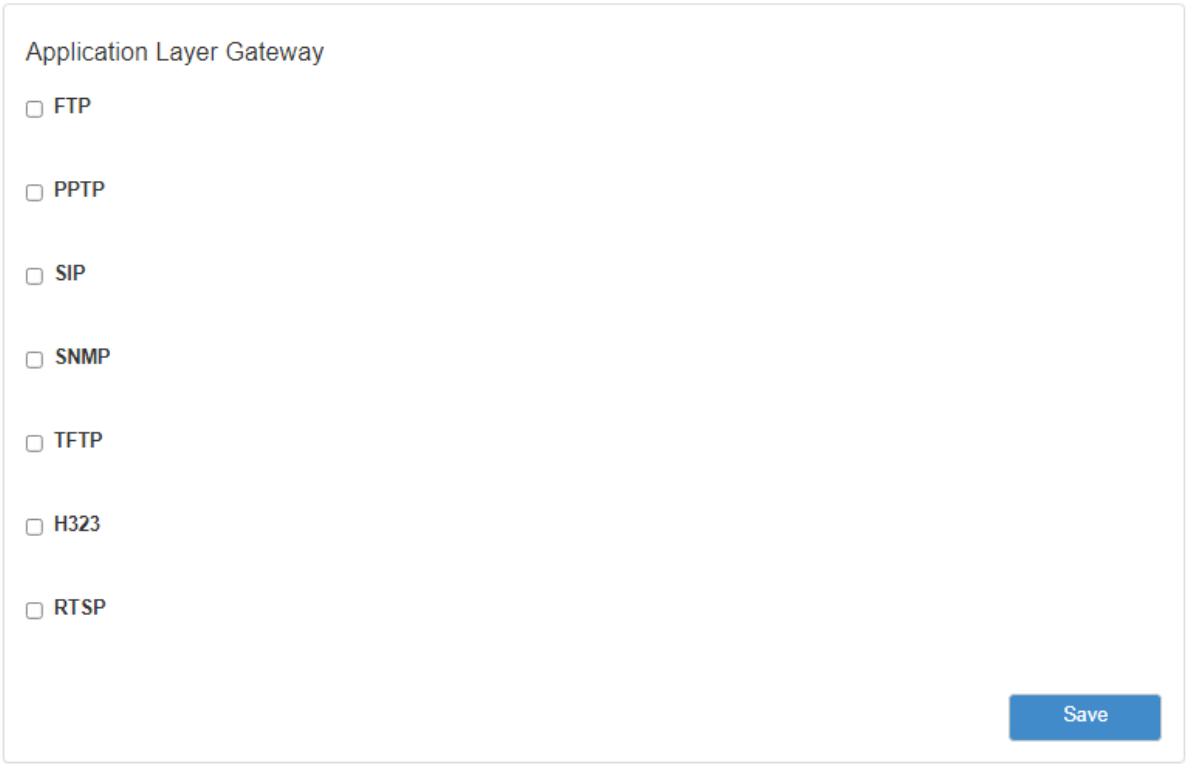


Рис. 69. Вкладка Services, раздел Application Layer Gateway

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+(справедливо только для роутеров серии R4), поставьте галочку напротив **Enable TACACS+ for SSH**. На рисунке представлен пример настройки доступа к устройству.

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!

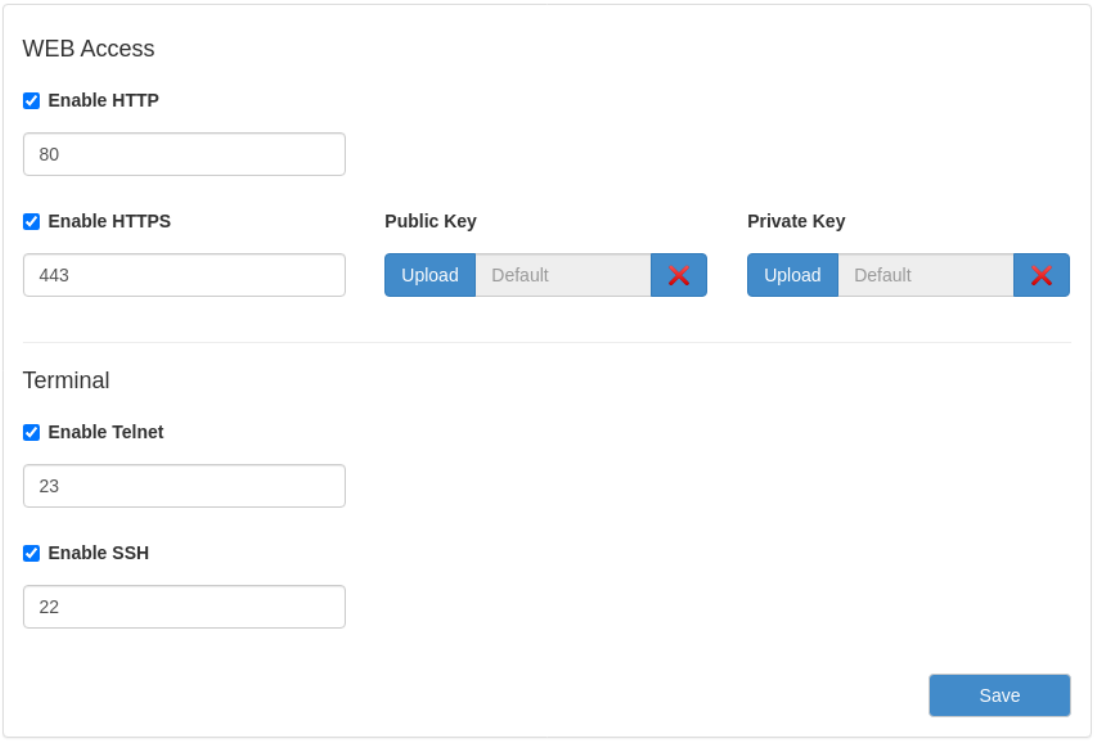


Рис. 70. Вкладка Tools, раздел Access

5.5.2. 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. 71. Вкладка Tools, раздел Password

5.5.3. 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. 72. Вкладка Tools, раздел Unit Name

5.5.4. Temperature

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.

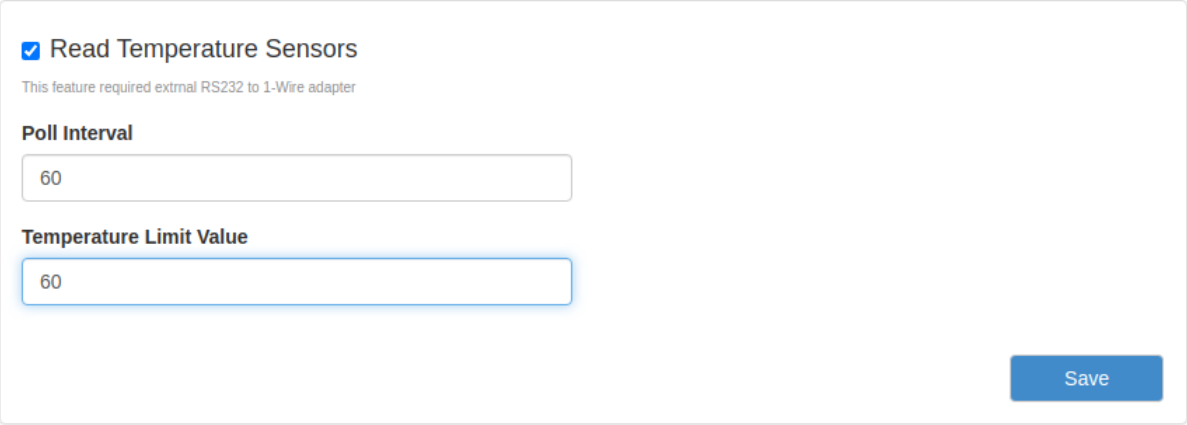


Рис. 73. Вкладка Tools, раздел Temperature

Таблица 40. 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	Значение температуры, при превышении которого пользователю отправляется уведомление

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

5.5.5. 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.

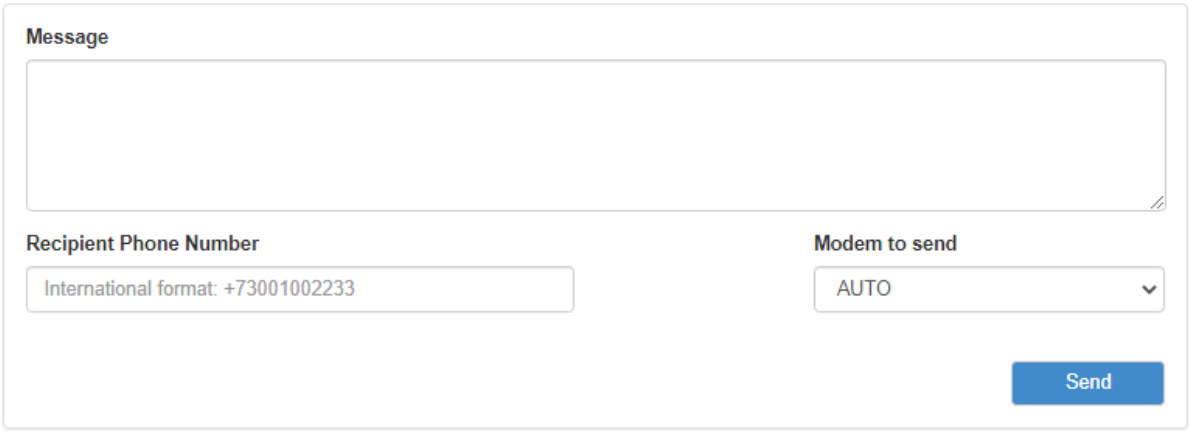


Рис. 74. Вкладка Tools, раздел Send SMS

5.5.6. 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.

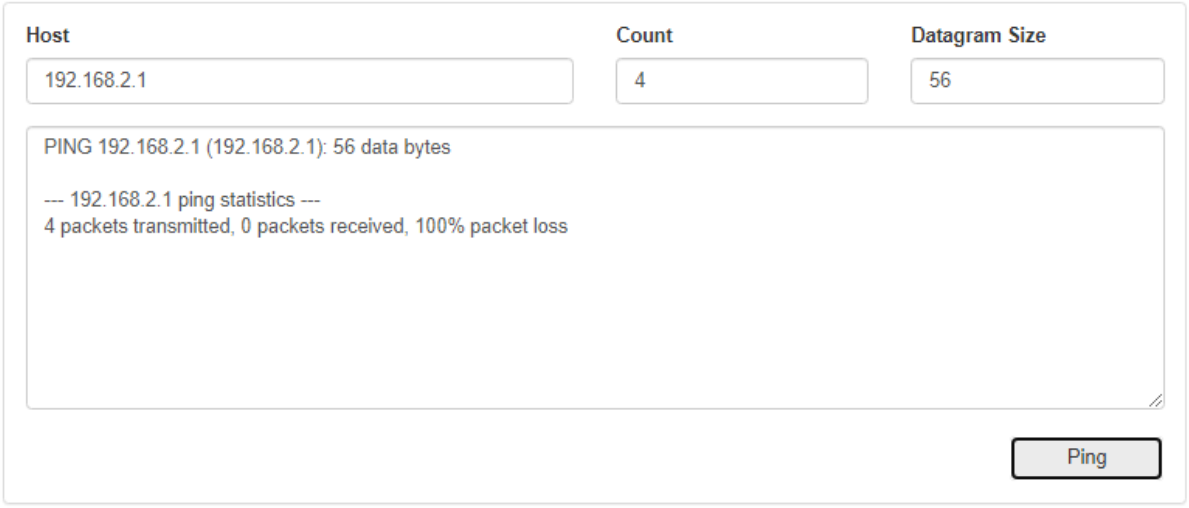


Рис. 75. Вкладка Tools, раздел Ping

5.5.7. 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.

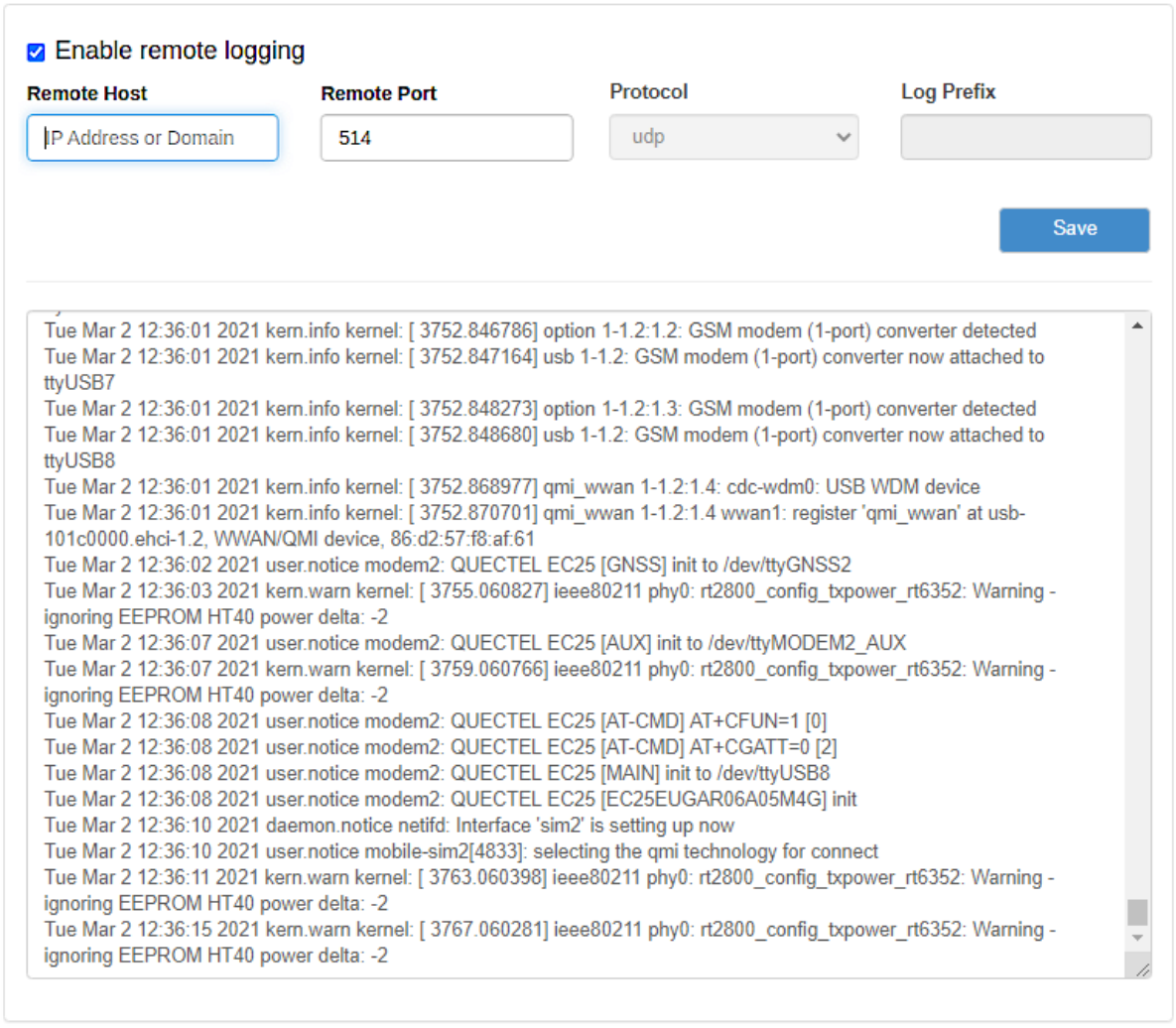


Рис. 76. Вкладка Tools, раздел System Log

5.5.8. 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!

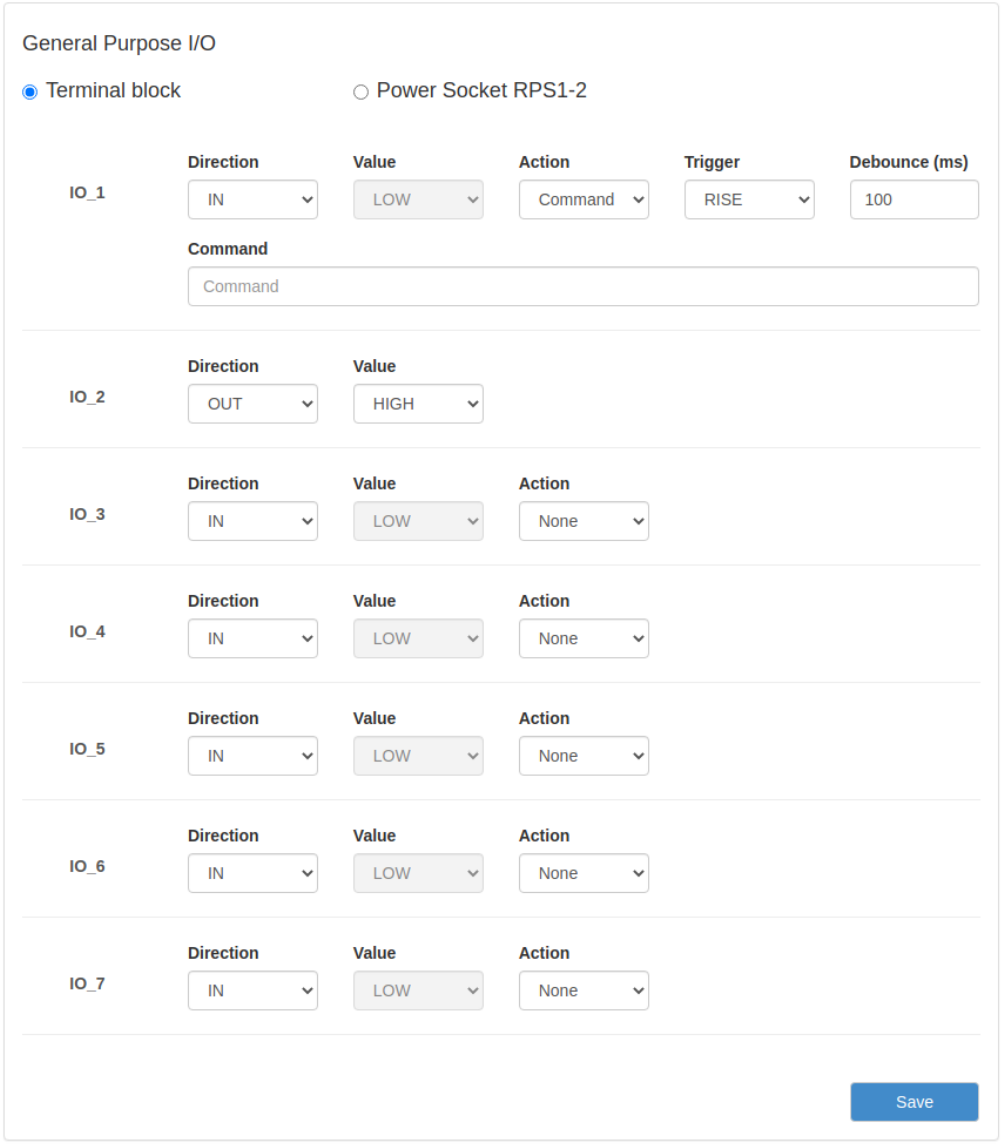


Рис. 77. Вкладка Tools, раздел GPIO

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

Настройки портов GPIO представлены в таблице ниже.

Таблица 41. Настройки портов GPIO

Поле	Описание
IO_1, IO_2, IO_3 …	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
Action	Действие по триггеру (только для входов): **None** — ничего не делать, **Command** — выполнить команду по срабатыванию триггера, **SMS** — отправить смс на указанный номер по срабатыванию триггера
Trigger	Событие происходящее на порту: **RISE** – появление напряжения на порту, **FALL** — пропажа напряжения на порту, **BOTH** — любое из событий, **NONE** – события не отслеживаются
Debounce (ms)	Нивелирует ложные срабатывания из-за электромагнитных наводок, измеряется в миллисекундах
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 42. 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%%

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.

5.5.9. Управляемый блок розеток RPS1-2

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

Значения полей представлены в таблице ниже.

Таблица 43. 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")

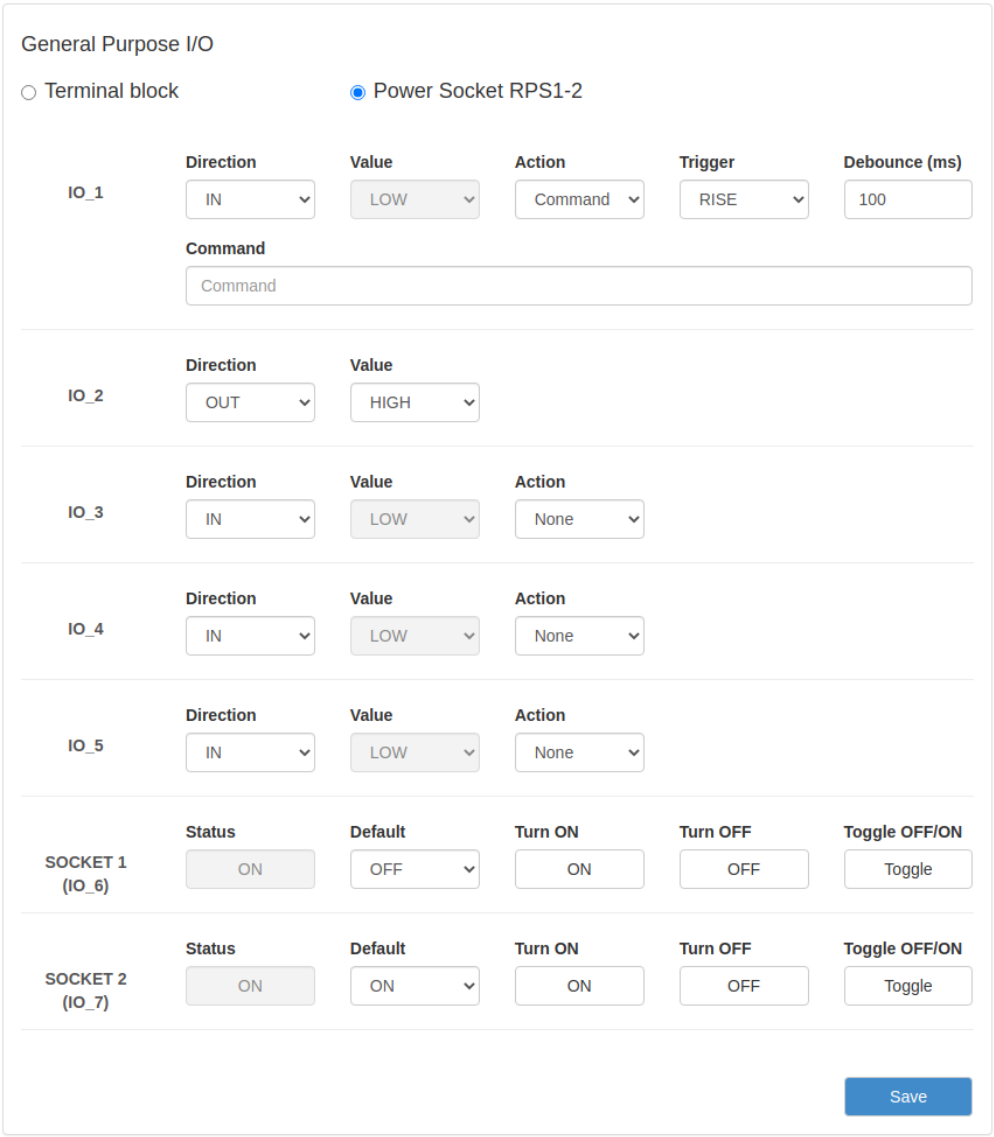
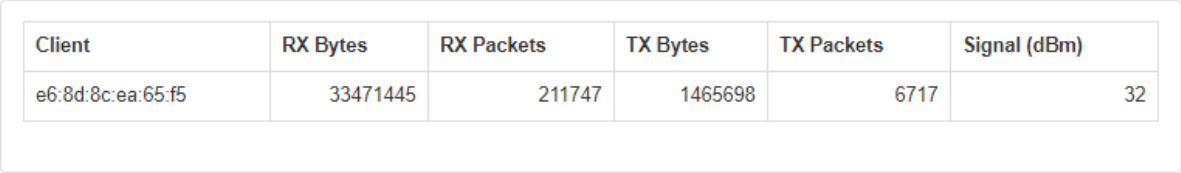


Рис. 78. Вкладка Tools, раздел GPIO, Power Socket RPS1-2

5.5.10. Wi-Fi Clients

Раздел **Wi-Fi Clients** на вкладке **Tools** предназначен для представления информации о подключенных Wi-Fi-клиентах, если устройство поддерживает работу с Wi-Fi. На 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. 79. Вкладка Tools, раздел Wi-Fi Clients (роутер с Wi-Fi-модулем)

Таблица 44. Информация о Wi-Fi-клиентах

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

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

5.5.11. 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**.

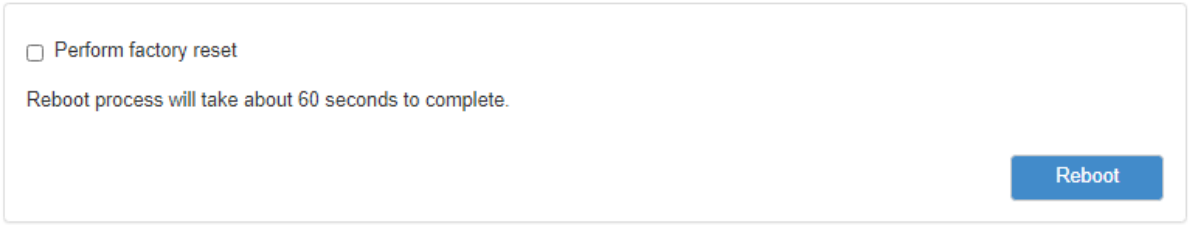


Рис. 80. Вкладка Tools, раздел Reboot

5.5.12. 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.

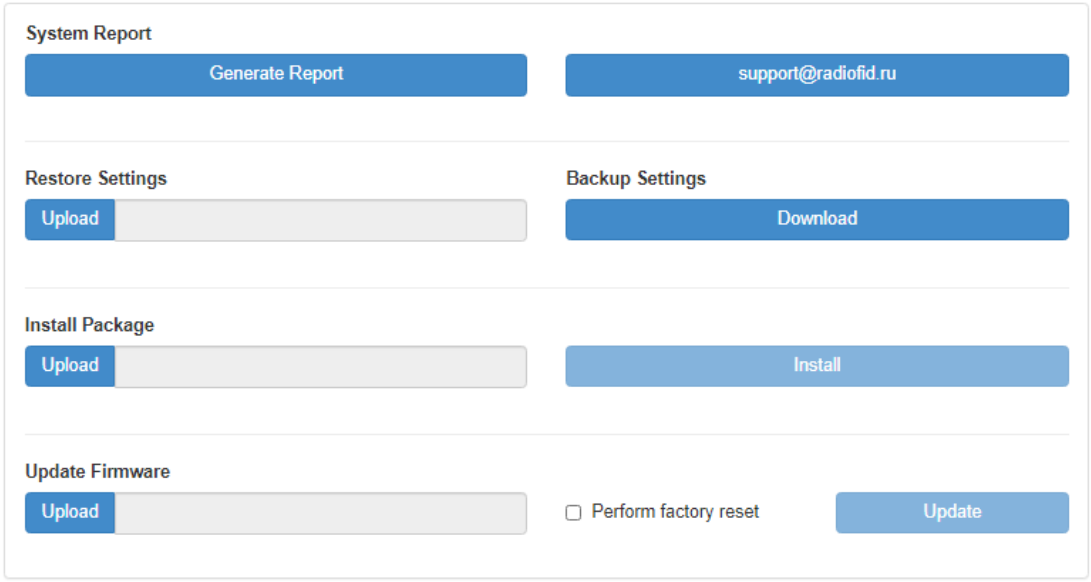


Рис. 81. Вкладка Tools, раздел Management

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.

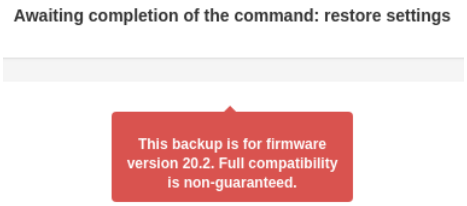


Рис. 82. Вкладка Tools, раздел Management, загрузка сохраненных настроек

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**.

6. Приложение 1

Синтаксис IP-адреса

IP-адрес описывает адрес узла в IP-сети и состоит из 4x 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 4x 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 4x 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