Руководство пользователя

Встроенного ПО для роутеров

Содержание

1. Введение

1.1. Описание документа

Руководство содержит описание последовательности действий, обеспечивающих работу со Встроенным ПО для роутеров, описание доступных пользователю функций, настроек и способов, с помощью которых пользователь осуществляет его эксплуатацию.

2. Версии Встроенного ПО для роутеров

С момента внесения в Реестр Российского ПО была выпущена обновленная версия Встроенного ПО для роутеров, которая получила новое название - **irzOS**.

Здесь и далее в документах используются следующие обозначения:

irzOS - альтернативное наименование обновленной версии Встроенного ПО для роутеров,

20.x - альтернативное наименование предыдущих версий Встроенного ПО для роутеров.

2.1. 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.

2.2. 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, позволяющая 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.

3. Доступ к веб-интерфейсу и интерфейсу командной строки

Для доступа к веб-интерфейсу ПО используется стандартный браузер (Firefox, Chrome, Opera, Safari и т.д. кроме Microsoft Edge/Internet Explorer).

Для подключения нужно ввести IP-адрес роутера в адресную строку браузера.

Адрес указан на наклейке на нижней стороне устройства (обычно **192.168.1.1**).

На странице авторизации ввести логин и пароль.

После успешной авторизации открывается статусная страница устройства.

Доступ к интерфейсу командной строки (cli), только для irzOS

Доступ к интерфейсу командной строки (CLI) осуществляется по протоколу SSH. После успешной аутентификации пользователь получает доступ в CLI с правами, соответствующими учетной записи.

Процесс доступа:

1. Установить SSH-соединения с IP-адресом роутера

Адрес указан на наклейке на нижней стороне устройства (обычно **192.168.1.1**)

1. Указать пароль, для актуальной версии ПО.
2. После этого устройство автоматически покажет интерфейс командной строки (cli)

```
user@desktop:~$ ssh admin@192.168.1.1
admin@192.168.1.1's password:
admin@Router[/]>
```

4. Настройка проводной сети

4.1. Настройка проводной сети для irzOS

Настройка проводной сети происходит в разделе **/network/bridge**

Bridge - виртуальное сетевое устройство (L2), которое объединяет физические или логические интерфейсы в единую сеть/

Bridge функционирует как виртуальный коммутатор, объединяя несколько физических (/network ethernet) или логических (/network device, /wireless network, /tunnel) сетевых интерфейсов.

По умолчанию все порты устройства объединены в **bridge0**.

4.2. Основные параметры

Disabled - отключение bridge

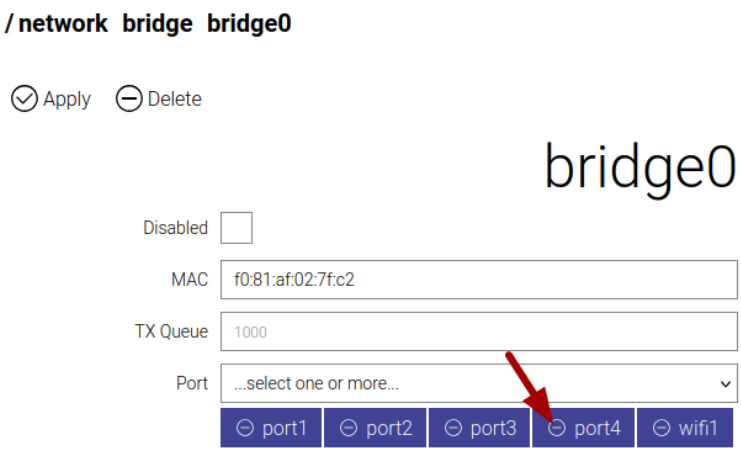
MAC - присвоение MAC-адреса. Если не указан, будет сгенерирован автоматически.

Port - настройка списка портов, объединенных в данный bridge.

4.3. Пример настройки

Задача: объединить в сеть устройства, подключенные к **port2** и **port4**.

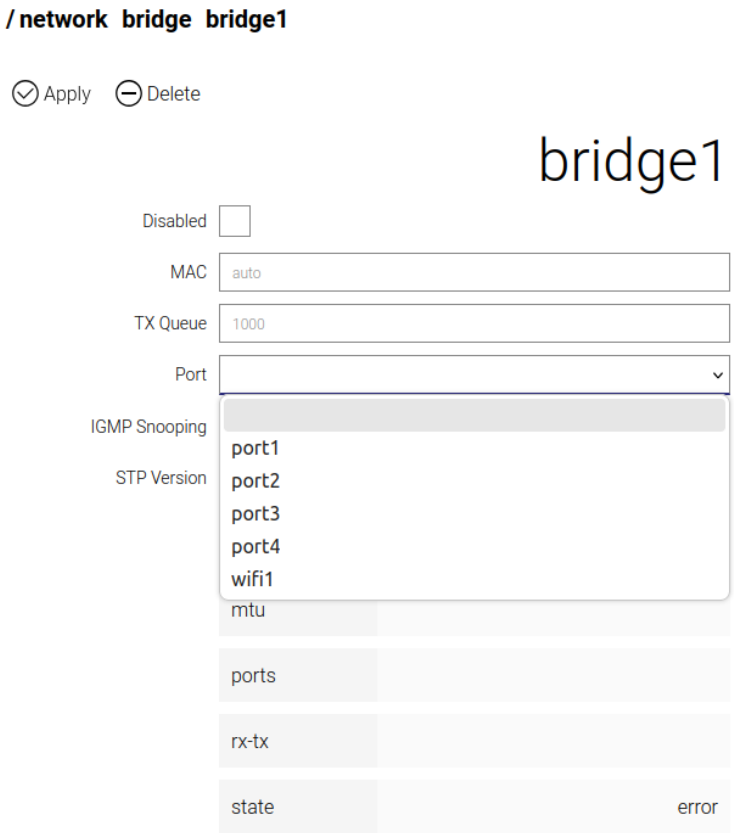
1. **Освободить порты**
   - Перейти в **/network/bridge/bridge0**
   - Удалить из списка port2, port4 нажав кнопку "минус" (-)
   - Применить настройки (apply)



Не удаляйте порт, через который роутер подключен к ПК. Это приведет к потере доступа к устройству.

2. **Создать новый bridge**

- Перейти в **/network/bridge**
- Создать новый bridge кнопкой **Add**, указать имя. Допустимы латинские буквы (A-Z, a-z), цифры (0-9), нижнее подчеркивание (_). В нашем примере **bridge1**
- Добавить порты из выпадающего меню **Port** (в нашем примере port2, port4)
- Применить настройки (apply)

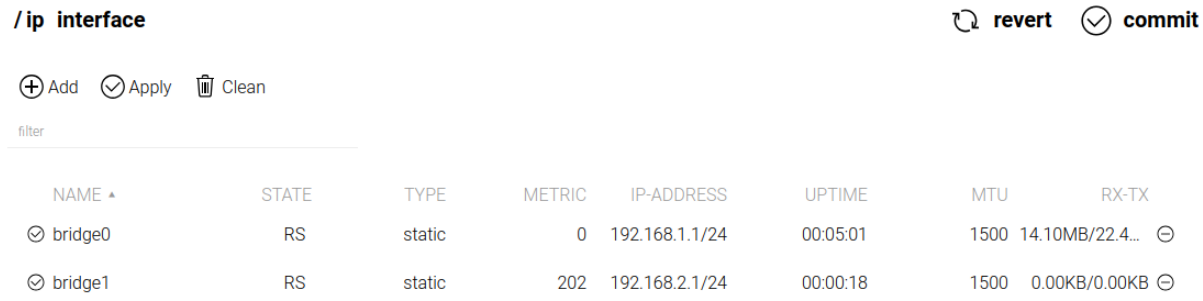


Теперь на странице **/network/bridge** видны оба виртуальных сетевых устройства и их параметры.

3. **Назначить IP**

- Перейти в **/ip/interface**
- Нажать **Add**, в выбрать из списка **bridge1**, который мы создали в п.2.
- Указать тип **static**
- Перейти в созданный интерфейс **/ip/interface/bridge1**
- Указать IP-адрес (например 192.168.2.1/24)
- Применить настройки (apply)

Теперь на странице **/ip/interface** видны оба виртуальных сетевых устройства и их параметры.



Настройка через интерфейс командной строки (cli)

Удаление портов из bridge0.

```
admin@Router[/]>network bridge bridge0
admin@Router[/network bridge bridge0]>port -port2 -port4
admin@Router[/network bridge bridge0]>..
admin@Router[/network bridge bridge0]>apply
```

Создание нового bridge, добавление портов.

```
admin@Router[/network bridge]>add name=bridge1
admin@Router[/network bridge bridge1]>port port2 port4
admin@Router[/network bridge bridge1]>apply
```

Создание интерфейса в /ip interface, назначение IP.

```
admin@Router[/]>/ip interface add device=bridge1 type=static
admin@Router[/ip interface bridge1]>ip-address 192.168.2.1/24
admin@Router[/ip interface bridge1]>apply
```

4.4. Настройка проводной сети для 20.x

Раздел Local Network на вкладке Network предназначен для настройки локальных Ethernet-портов роутера.

В роутерах iRZ имеется возможность настроить WAN-порт таким образом, чтобы он работал, как локальный Ethernet-порт и наоборот — все LAN порты превратить в WAN.

В зависимости от конкретной модели устройства количество Ethernet-портов может отличаться. Пожалуйста, сверьтесь с информацией в руководстве или осмотрите корпус устройства для уточнения.

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 вручную — 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!

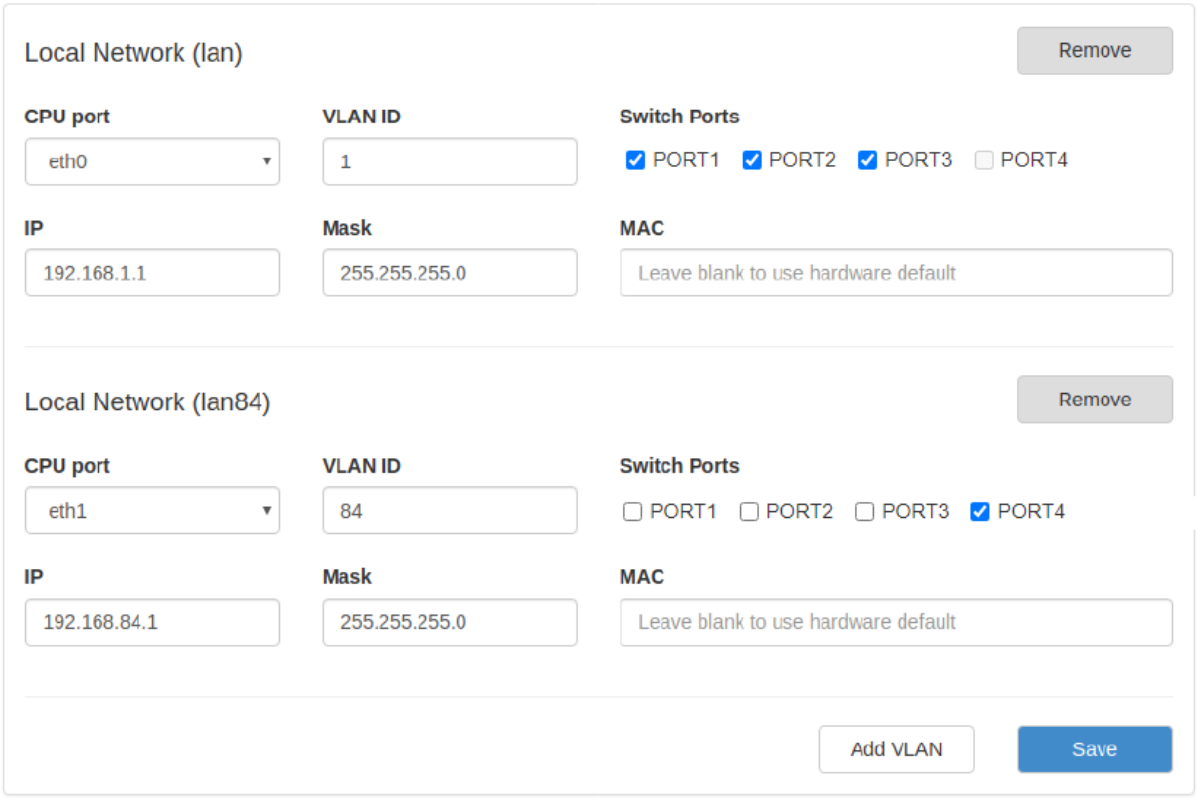


Рис. 1. Вкладка Network, раздел Local Network

Таблица 1. 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 вручную

Раздел **Wired Internet** на вкладке Network предназначен для настройки WAN-порта роутера в рамках VLAN.

В роутерах iRZ имеется возможность настроить локальные порты таким образом, чтобы они работали, как WAN-порты.

В зависимости от конкретной модели устройства количество Ethernet-портов может отличаться. Пожалуйста, сверьтесь с информацией в руководстве или осмотрите корпус устройства для уточнения.

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

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

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

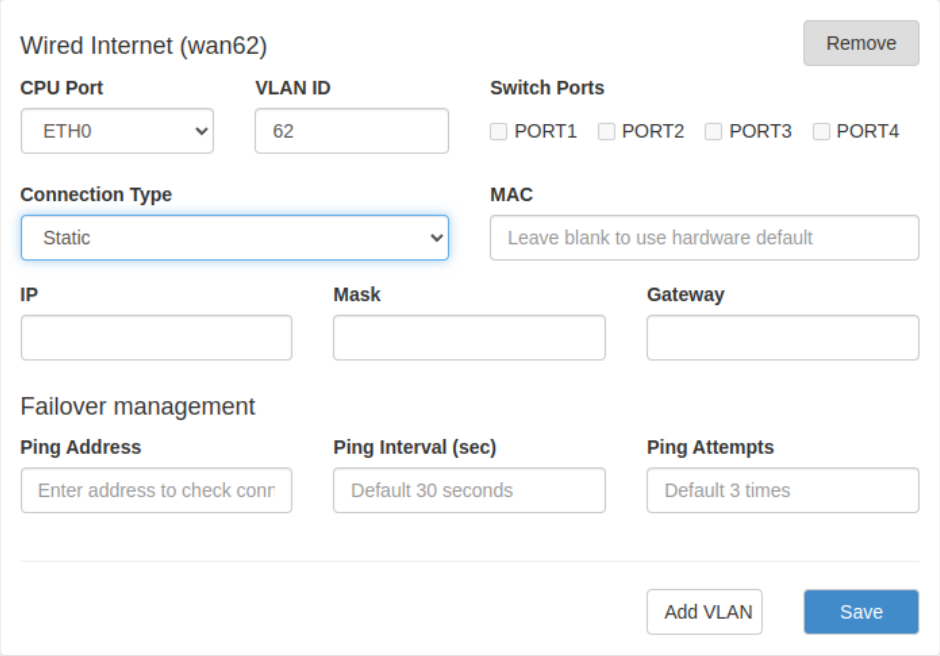


Рис. 2. Вкладка Network, раздел Wired Internet

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

Таблица 2. Network → Wired Internet основные настройки

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

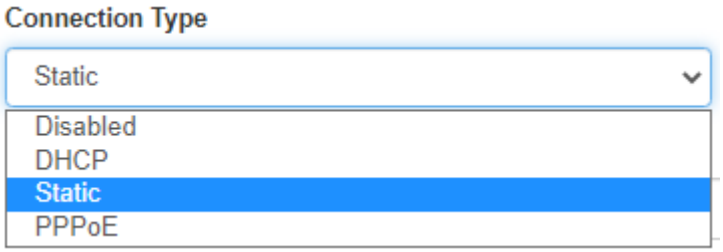


Рис. 3. Тип соединения для WAN-порта

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

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

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

Таблица 3. Дополнительные настройки (поле **Connection Type**)

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

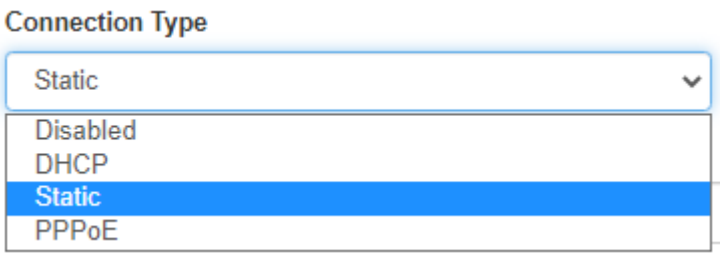


Рис. 4. Тип соединения для WAN-порта

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)**

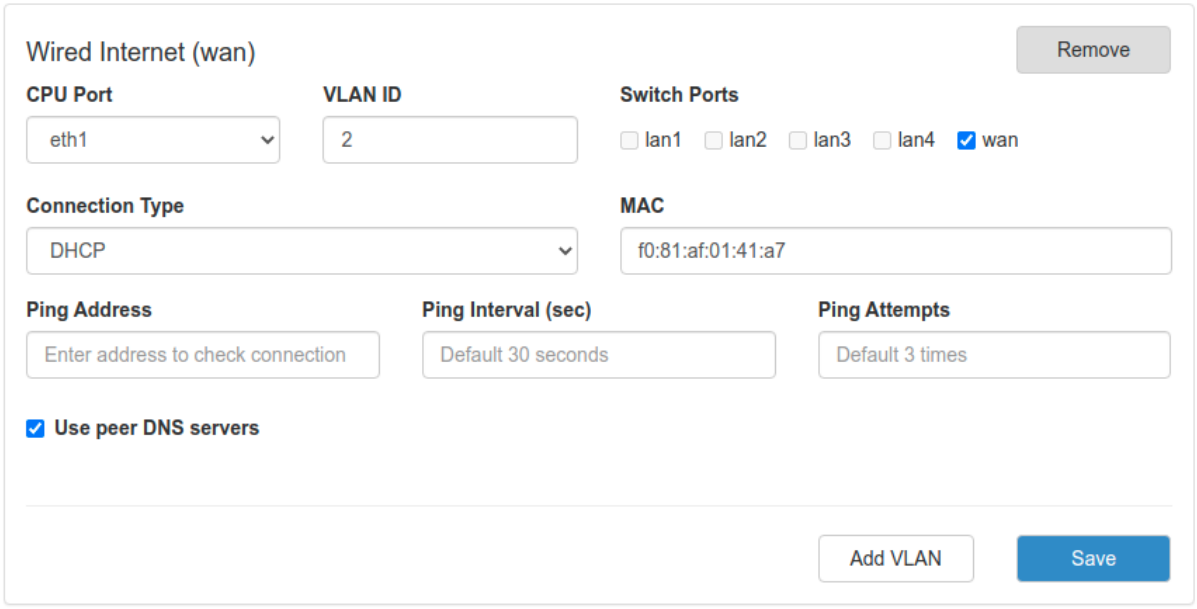


Рис. 5. WAN-порта – DHCP

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

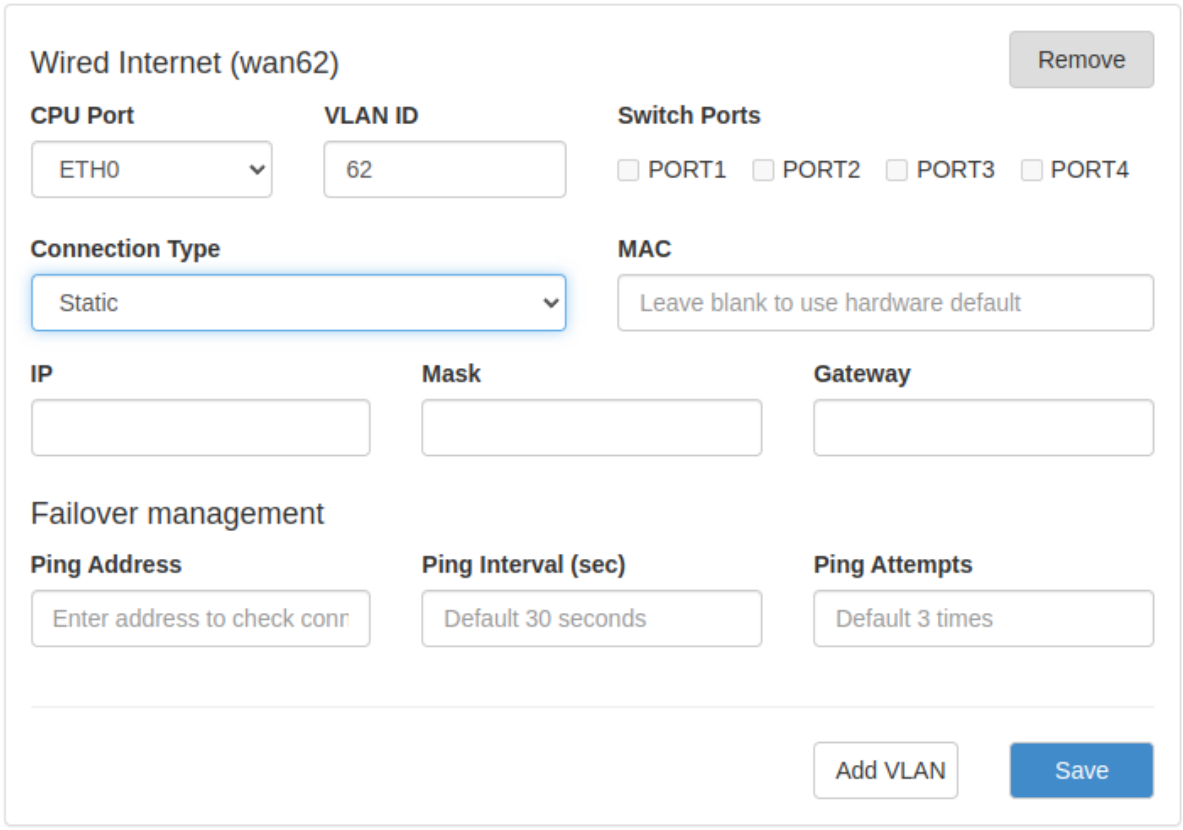


Рис. 6. WAN-порта – Static

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

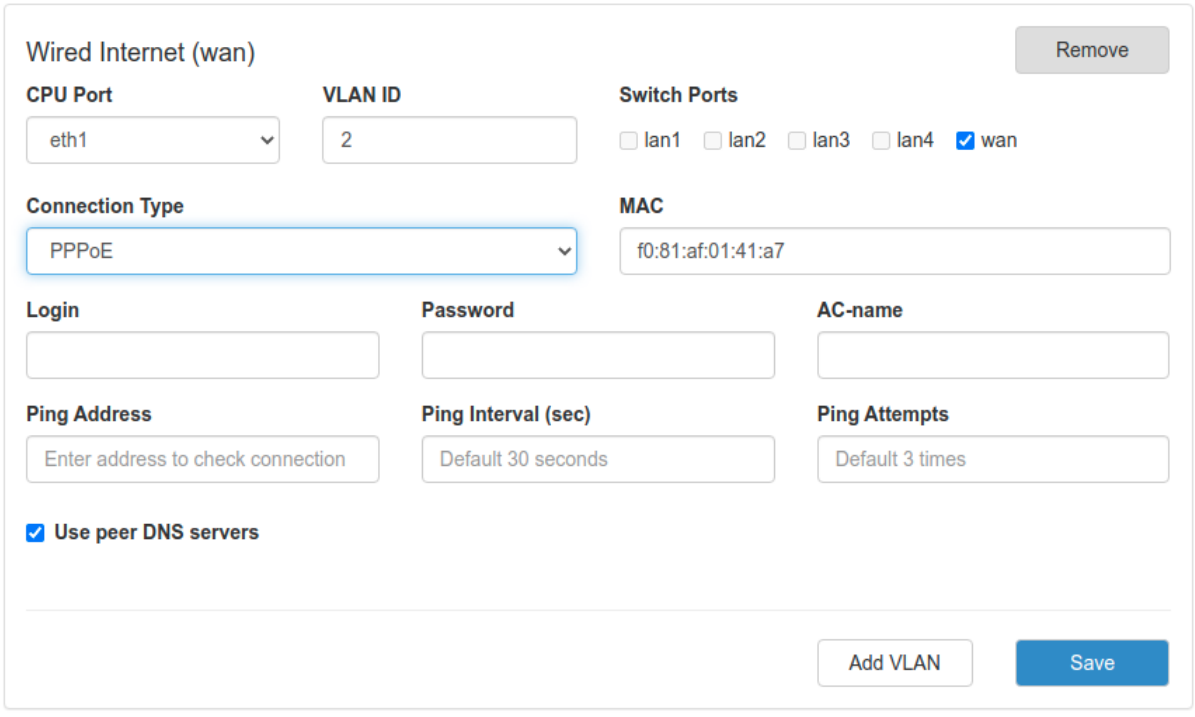


Рис. 7. Тип соединения WAN-порта – PPPoE

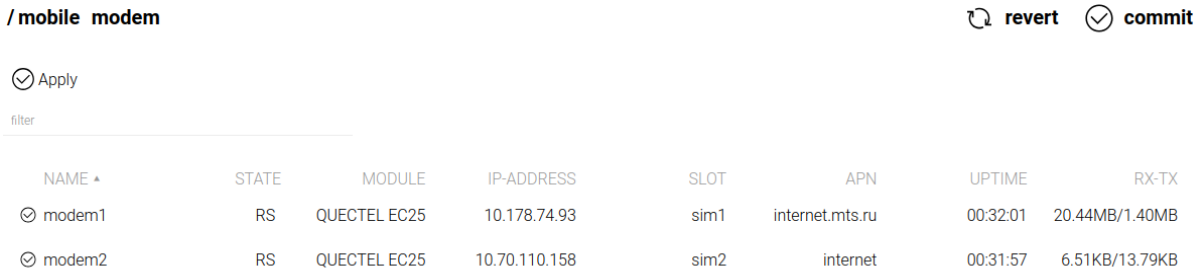
5. Настройка мобильной сети

5.1. Настройка мобильной сети для irzOS

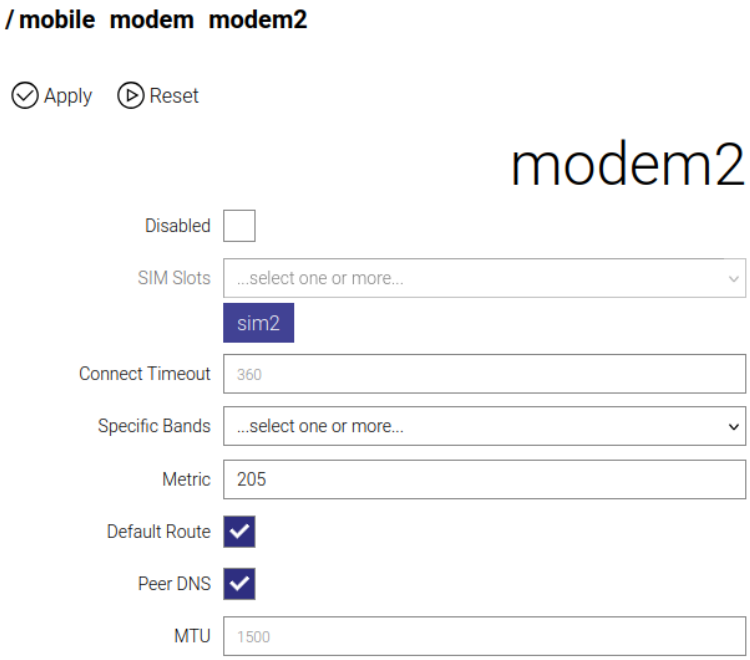
Настройка мобильной сети происходит в разделе **/mobile/modem**

Modem1…N - сотовый модуль, количество модулей зависит от модели роутера.

SIM1…N - SIM-карта, которая находится SIM-слоте с соответствующим номером.



После установки SIM-карт мобильная сеть начинает работать с настройками по умолчанию.



Текущий статус соединения отображается на главной странице устройства.

5.2. Основные параметры модема

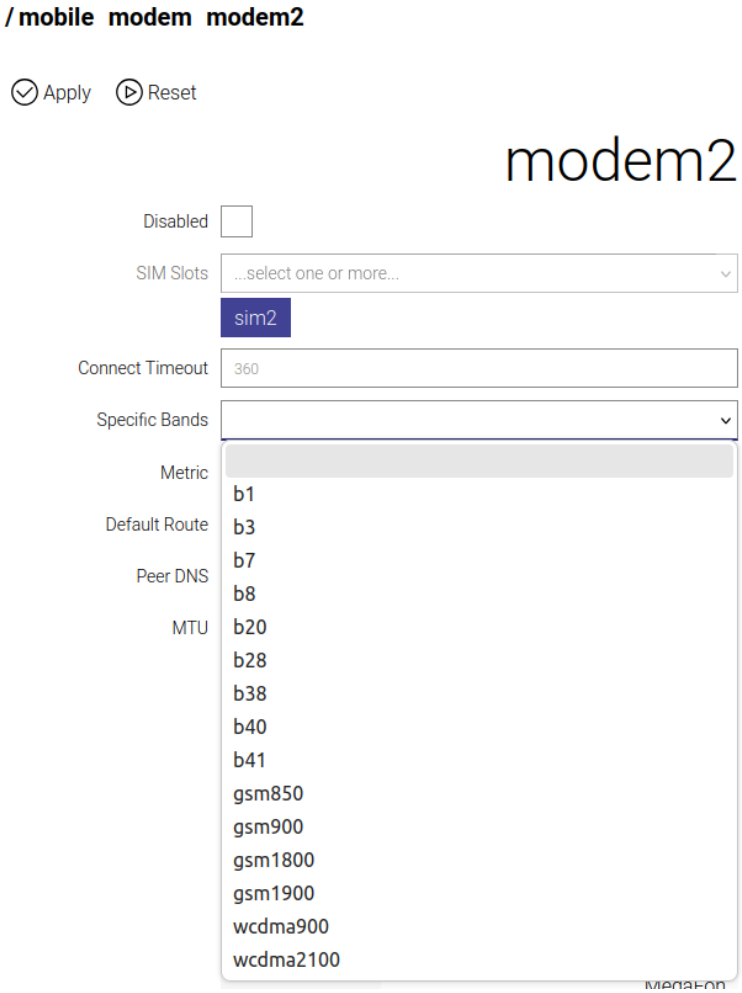
Disabled - отключение модема

Default Route - использовать канал сотовой связи как маршрут по умолчанию

Metric - численное значение, определяющее приоритет маршрута. Чем меньше значение, тем выше приоритет. Для работы **Default Route** (маршрута по умолчанию) указание метрики обязательно. Во избежание конфликтов маршрутизации, значение метрики должно быть уникальным для каждого интерфейса.

Specific Bands - выбор частотных полос (бэндов). Если сотовый модуль поддерживает выбор бэндов, в веб-интерфейсе отображается поле **specific bands** и перечень доступных бэндов.

Например:



При этом:

b<x> — 4G

wcdma<x> — 3G

gsm<x> — 2G (поддерживается не всеми модулями)

Настройка через интерфейс командной строки (cli)

Настройки по умолчанию для модема

```
admin@Router[/]>mobile modem modem2
admin@Router[/mobile modem modem2]>[TAB] - будут отображены значения, установленн
  defaultroute                  true
  disabled                      false
  metric                        205
  modem-band
  modem-connect-timeout         360
  modem-sim-slot                sim2
  mtu                           1500
  peerdns                       true
  protocol                      auto
```

Выбор бэндов

```
admin@Router[/mobile modem modem2]>modem-band
b1
b3
b7
b8
b20
b28
b38
b40
b41
gsm850
gsm900
gsm1800
gsm1900
wcdma900
wcdma2100
admin@Router[/mobile modem modem1]> modem-band b1 b20 b28 b3 b8
```

5.3. Настройка мобильной сети для 20.x

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

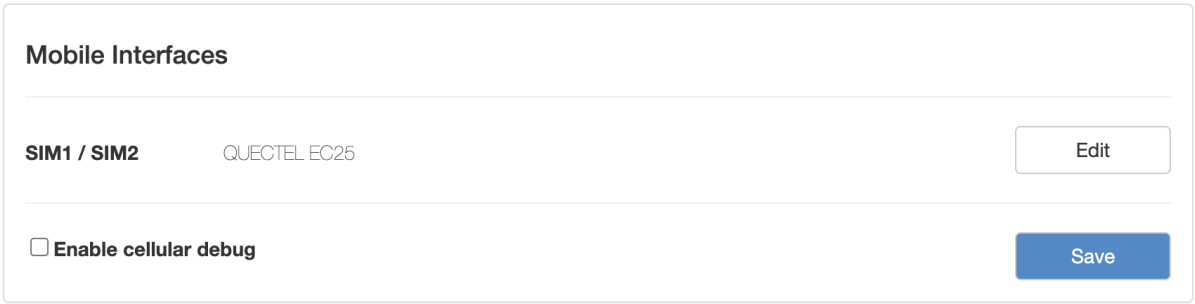


Рис. 8. Вкладка Network, раздел Mobile Interfaces для одномодульного устройства

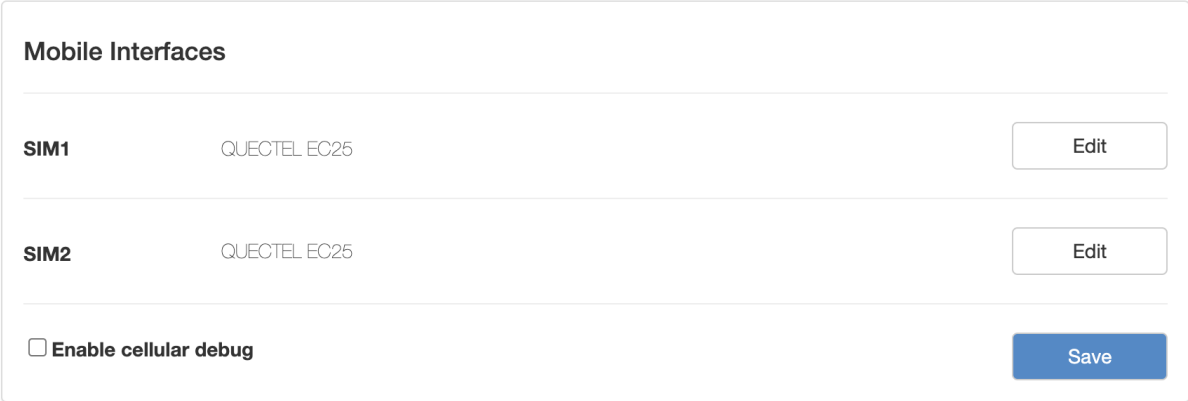


Рис. 9. Вкладка Network, раздел Mobile Interfaces для двухмодульного устройства

Чтобы увеличить количество отладочной информации в логе при работе с сотовой сетью необходимо поставит галочку в чекбоксе **Enable cellular debug**.

Для начала редактирования настроек необходимо нажать кнопку **Edit**.

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

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

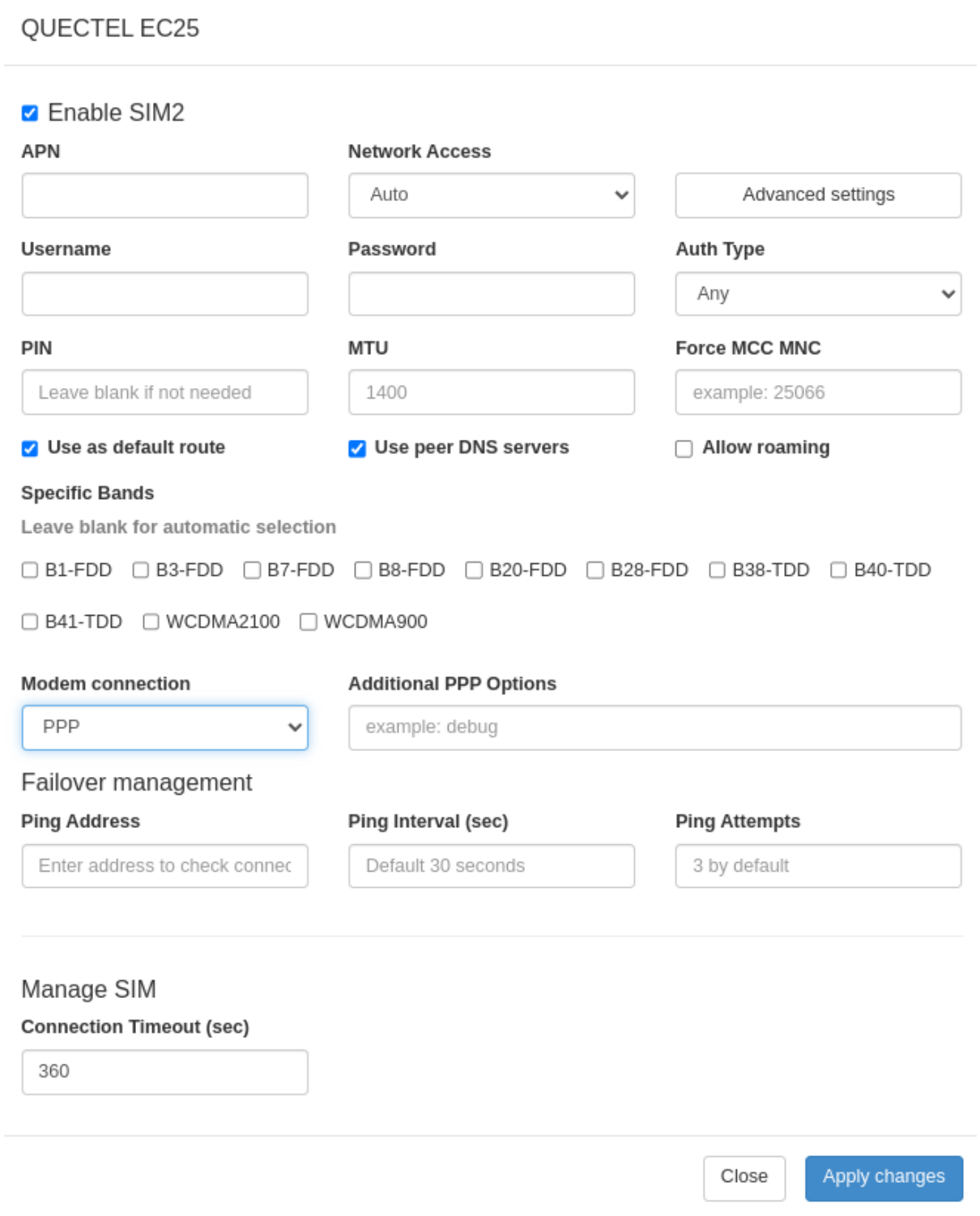


Рис. 10. Вкладка Network, раздел Mobile Interfaces − Edit

Настройки мобильного Интернета

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

Таблица 4. 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. Роутер всегда будет пытаться выходить в сеть с указанным в этом поле кодом сети, независимо от правильности кода
Use As Default Route	Использовать указанные настройки как маршрут по умолчанию
Use Peer DNS Server	Включение/выключение использования внешних DNS-серверов провайдера
Allow Roaming	Разрешение/запрет работы SIM-карты устройства в роуминге
Specific Bands	Выбор частотных полос (бэндов).
Modem Connection	Выбор протокола - **PPP** или **Auto**
Additional PPPD Options	Указание дополнительных опций при работе по протоколу PPP
Connection Timeout (sec)	Время, которое отводится SIM-карте на подключение к сотовому оператору, по истечении данного времени роутер перезагружает сотовый модуль по питанию и дозвон начинается заново, измеряется в секундах
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**;
- EC200A-EU - EC200AEUHAR01A04M16 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.

Mobile APN Profiles

Раздел предназначен для работы с SIM-картами виртуальных операторов.

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

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

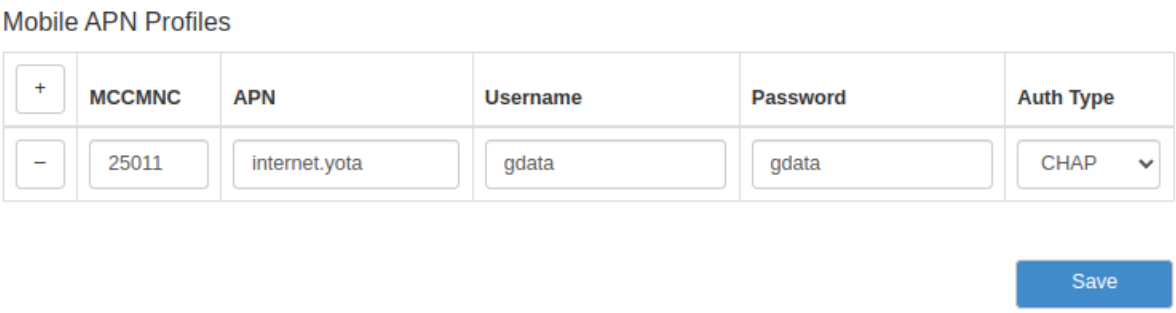


Рис. 11. Вкладка Mobile APN Profiles

Таблица 5. 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

6. Настройка Wi-Fi

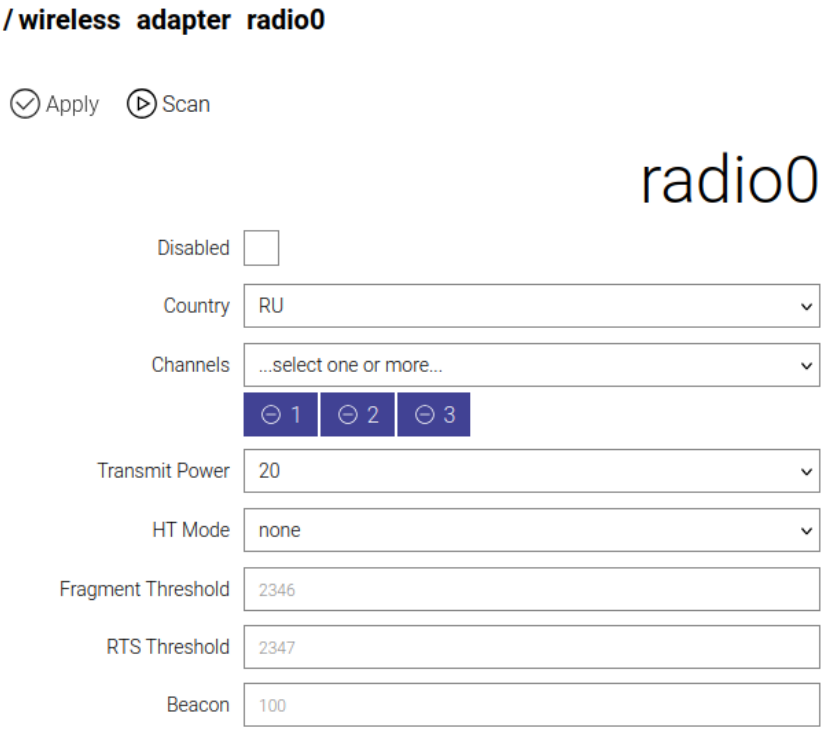
6.1. Настройка Wi-Fi для irzOS

Настройка беспроводной сети происходит в разделе **/wireless**.

6.2. Основные параметры Wi-Fi адаптера

Настройка WiFi-адаптера происходит в разделе **/wireless/adapter**

Для роутеров, оборудованных двумя Wi-Fi адаптерами, каждый из них настраивается отдельно.



Disabled - отключение адаптера

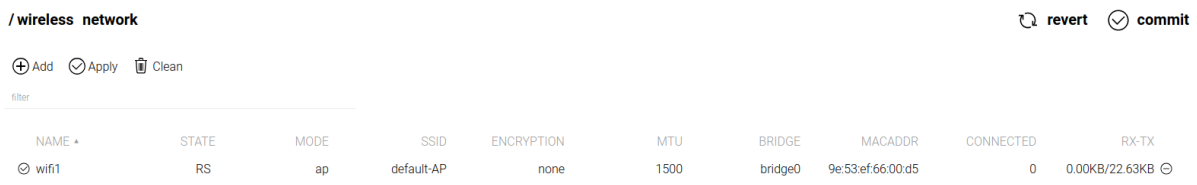
Country - регион, определяющий список разрешенных каналов

Channels - выбор каналов

- не выбрано — поиск по всем доступным каналам;
- выбрано одно значние — поиск не происходит, используется указанный канал;
- выбрано несколько значений — поиск происходит только среди них.

6.3. Основные параметры Wi-Fi сети

Настройка беспроводной происходит в разделе **/wireless/network**



Disabled - отключение беспроводной сети

Adapter - выбор физического Wi-Fi адаптера (для роутеров с одним Wi-Fi адаптером - **radio0**)

Mode - режим работы:

- **ap** (access point) — роутер работает в качестве точки доступа, ждет подключения клиентов к своей сети
- **sta** — роутер не создает собственную сеть, а подключается к заданной сети Wi-Fi

Encryption - протокол безопасности (шифрование)

SSID - имя беспроводной сети

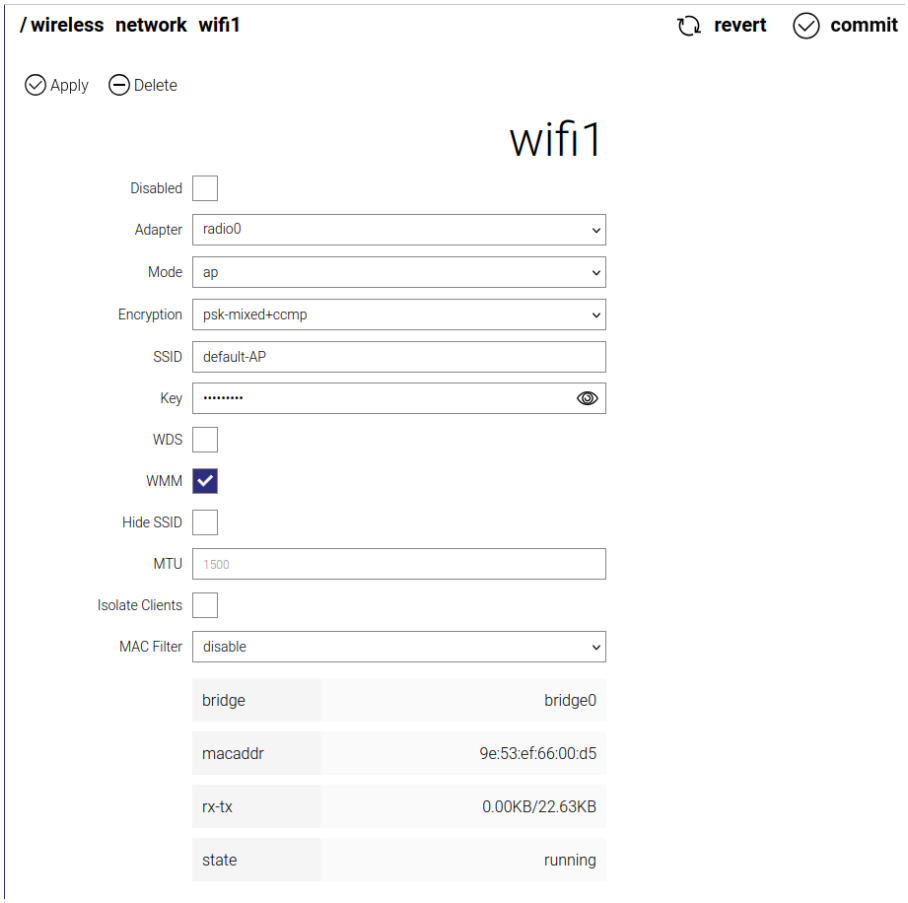
Key - пароль

Значение SSID и Key по умолчанию указаны на наклейке на нижней стороне устройства

6.4. Пример настройки

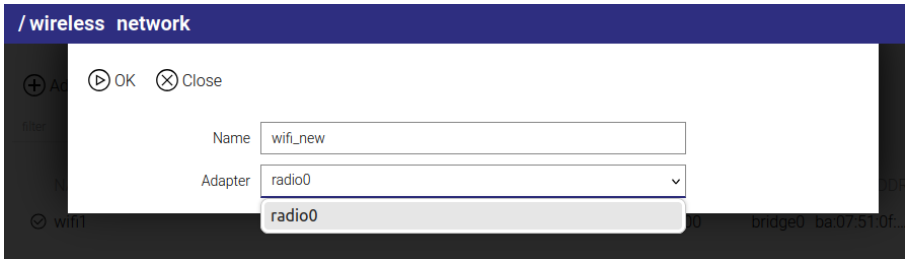
Задача: Настроить беспроводную сеть на роутере с одним Wi-Fi адаптером.

1. **Настройка адаптера**
   - Перейти в раздел **/wireless/adapter**
   - Настроить параметры для адаптера radio0 (Country, Channels)
   - Применить настройки (apply)
2. **Создание беспроводной сети**
   - Перейти в раздел **/wireless/network**

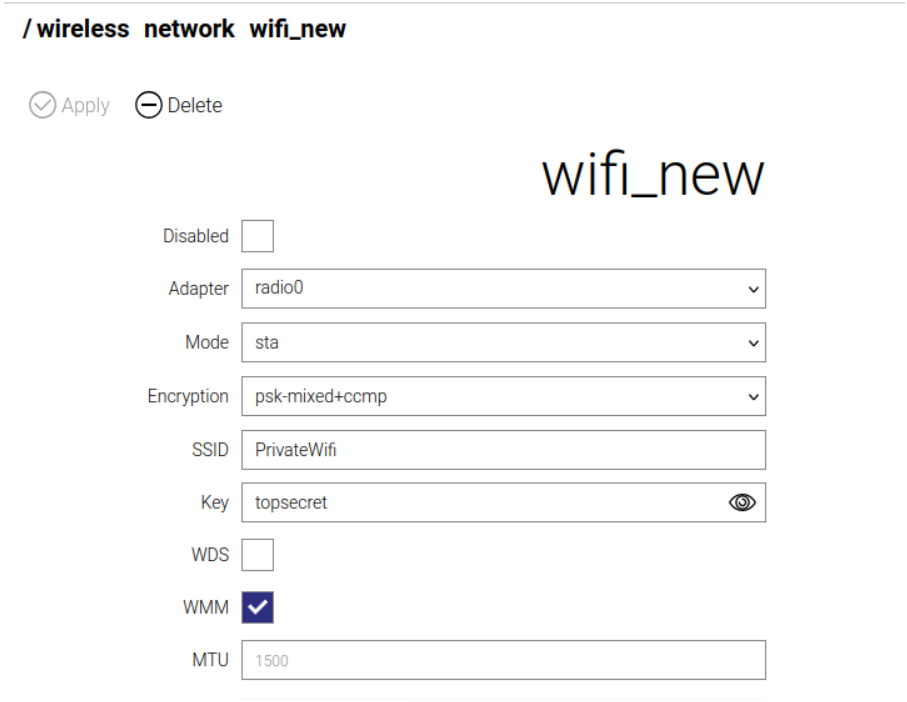


По умолчанию **wifi1** уже создан с предварительными настройками для работы в режиме **Access Point (ap)** Можно изменить настройки этой сети или создать новую.

- Нажать **Add**, указать имя. Допустимы латинские буквы (A-Z, a-z), цифры (0-9), нижнее подчеркивание (_). В нашем примере **wifi_new**.
- Из меню **Adapter** выбрать физический адаптер, в данном случае radio0
- Сохранить настройки (OK)



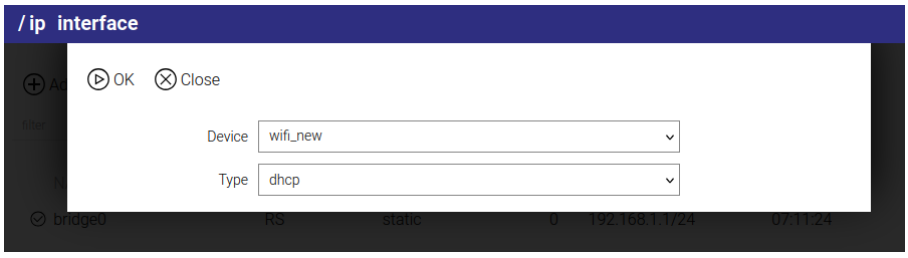
3. **Конфигурация беспроводной сети**



- **mode** (режим работы) - STA,
- **encryption** (шифрование) psk-mixed+ccmp
- **ssid** (имя сети) PrivateWifi
- **key** (пароль) topsecret
- Применить настройки (apply)

Теперь на странице /wireless/network видны обе беспроводные сети.

4. Назначить IP (для режима STA)
    - Перейти в **/ip/interface**
    - Нажать **Add**, в выбрать из списка **Wifi_new**, который мы создали в п.2.
    - Указать тип **dhcp**
    - Указать метрику (если установлен **Default Route**)
    - Применить настройки (apply)



Максимальное количество Wi-Fi сетей (AP/STA), которое можно создать на одном адаптере, зависит от серии роутера:
Серии R0, R2: до 8
Серия R10: до 4
Серия R50: до 16

Настройка через интерфейс командной строки (cli)

Настройка адаптера, выбор каналов

```
admin@Router[/]>
admin@Router[/]> wireless adapter radio0
admin@Router[/wireless adapter radio0]> channels 1,2,3
admin@Router[/wireless adapter radio0]> apply
```

Создание беспроводной сети, указание параметров

```
admin@Router[/wireless adapter radio0]> /wireless network
admin@Router[/wireless network]> add name=wifi_new adapter=radio0
admin@Router[/wireless network wifi_new]>mode sta
admin@Router[/wireless network wifi_new]>encryption psk-mixed+ccmp
admin@Router[/wireless network wifi_new]>ssid PrivateWifi
admin@Router[/wireless network wifi_new]>key topsecret
admin@Router[/wireless network wifi_new]>apply
```

Создание интерфейса в /ip interface, назначение IP

```
admin@Router[/]>/ip interface add device=wifi_new type=dhcp
admin@Router[/ip interface wifi_new]>metric 202
admin@Router[/ip interface wifi_new]>defaultroute true
admin@Router[/ip interface wifi_new]>apply
```

6.5. Настройка Wi-Fi для 20.x

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!

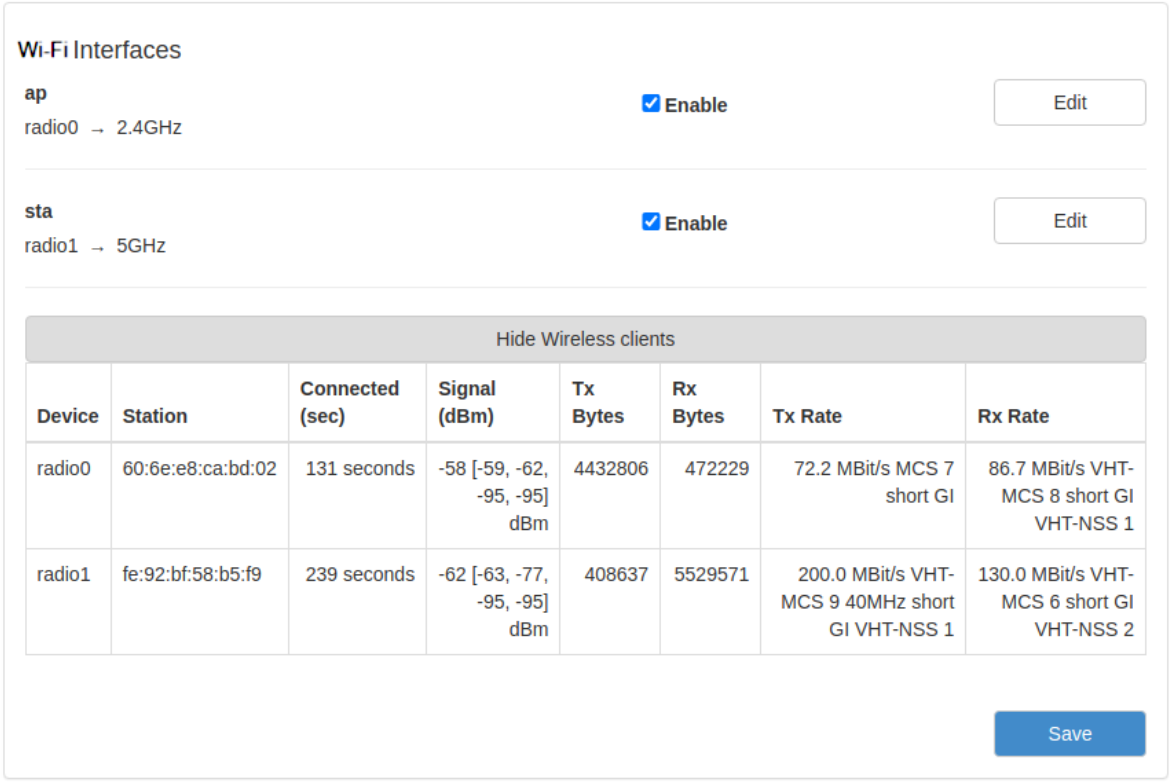


Рис. 12. Вкладка Network, раздел Wireless Internet

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**.

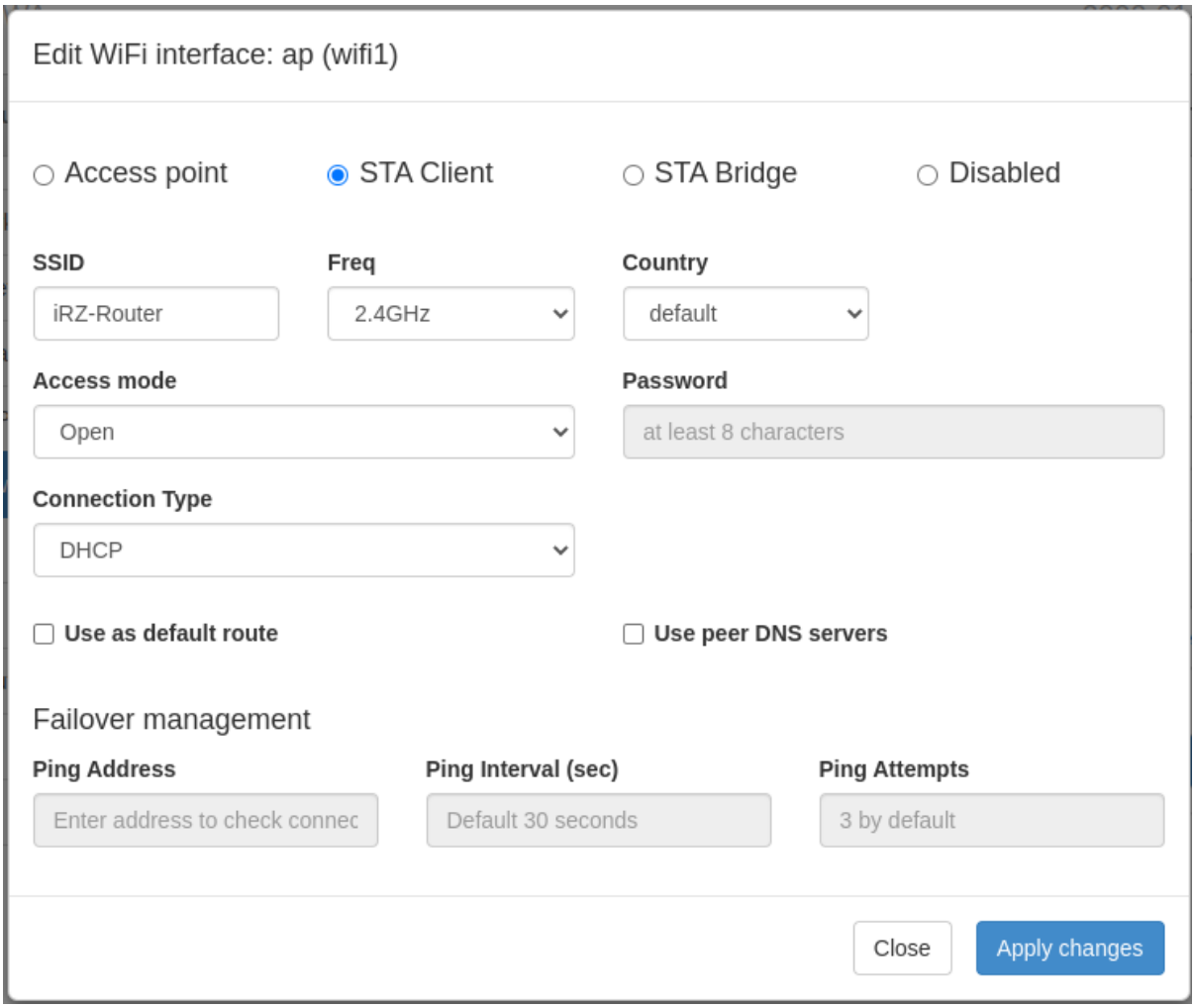


Рис. 13. Меню Edit, Вкладка Network, раздел Wireless Internet

Выбор режима работы модуля Wi-Fi:

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

Access Point

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

Таблица 6. Настройки Network → Wireless Network (Режим Access Point)

Поле	Описание
Bridge with Interface	Создание моста с локальным интерфейсом или создание нового интерфейса. • При выборе пункта **LAN** в настройке **Bridge with Interface**, Wi-Fi-интерфейс роутера будет работать в режиме моста с LAN-портами. • При выборе пункта **Wi-Fi** в настройке **Bridge with Interface**, Wi-Fi-интерфейс будет работать, как самостоятельный интерфейс. Доступные настройки приведены на рисунке.
Static IP Address	IP-адрес интерфейса роутера
Network Mask	Маска сети интерфейса роутера
SSID	Название Wi-Fi-сети, к которой будут подключаться клиенты
Channel	Номер канала, на котором должна работать Wi-Fi-сеть
Hide Wireless Network	Включить/отключить работу в скрытном режиме, то есть без анонсирования своего SSID
Freq	Переключение частоты работы Wi-Fi модуля
Country	Код страны
Access Mode	Тип шифрования пароля доступа к создаваемой Wi-Fi-сети
Password	Пароль для доступа к создаваемой Wi-Fi-сети
HTmode	Выбор режима производительности
Don’t scan for overlapping BSSs in HT40 mode	Включить/отключить проверку перекрытия с другими базовыми станциями в режиме HT40

При первом включении роутера, а так же после сброса к заводским настройкам для Wi-Fi в режиме точки доступа будет включен автоматический выбор канала.

В режиме точки доступа в разделе представлена информация о подключенных Wi-Fi-клиентах.

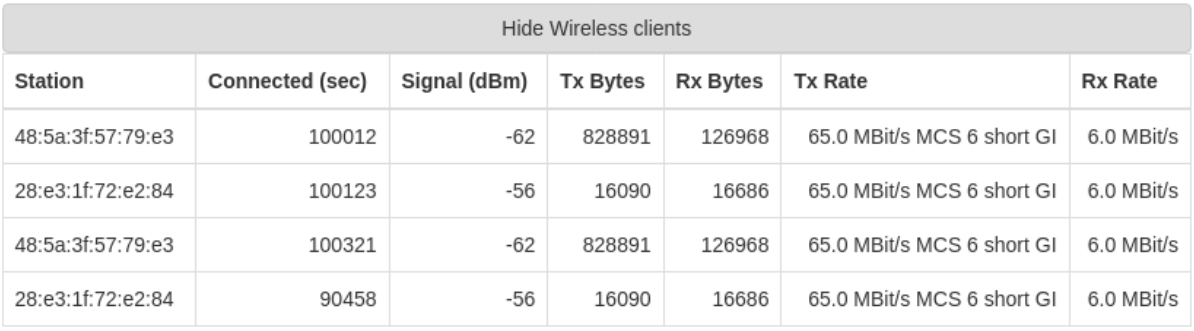


Рис. 14. Network, Wireless Network, Wi-Fi Clients

Таблица 7. Информация о Wi-Fi-клиентах

Поле	**Описание**
Station	BSSID подключенного клиента
Connected (sec)	Время, которое клиент подключен к точке доступа
Signal(dBm)	Уровень сигнала для подключенного клиента в децибелах
Tx bytes	Количество отправленных клиентом байт
Rx bytes	Количество принятых клиентом байт
Tx Rate	Скорость передачи данных
Rx Rate	Скорость приема данных

STA Client

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

Таблица 8. Настройки Network → Wireless Network (Режим STA Client)

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

STA Bridge

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

Таблица 9. Настройки Network → Wireless Network (Режим STA Bridge)

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

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

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

7. Настройка туннелей (VPN/Tunnels)

7.1. PPTP

7.1.1. Настройка PPTP для irzOS

Данный раздел настраивает роутер для работы в качестве клиента PPTP (Point-to-Point Tunneling Protocol). Это позволяет роутеру устанавливать VPN-туннель с удаленным PPTP-сервером, как правило, для удаленного доступа к частной сети.

PPTP — это широко поддерживаемый, но устаревший VPN-протокол. Его настройка проста и в основном требует указания *IP-адреса* удаленного сервера, а также *Имени пользователя* и *Пароля* для аутентификации.

Страница конфигурации позволяет выбрать *Тип аутентификации* (например, MS-CHAPv2) и включить *Шифрование* (MPPE) для обеспечения базового уровня конфиденциальности данных.

PPTP является устаревшим протоколом с известными уязвимостями в безопасности. Его использование категорически не рекомендуется для любых приложений, где важна безопасность данных. Для безопасного удаленного доступа рекомендуется использовать современные VPN-протоколы, такие как IPsec или OpenVPN.

СВОЙСТВА

disabled	Выключить конфигурацию
значения: true, false	
local-ip	Локальный адрес туннеля или интерфейс
значения: /ip interface, /mobile modem, /tunnel eoip, /tunnel gre, /tunnel l2tp, /tunnel openvpn, /tunnel pptp, /tunnel wireguard interface, /tunnel l2tp-v3, /tunnel atunnel, /defaults server, auto **пример:** bridge0	
remote-ip	Адрес удалённого хоста (FQDN ил IP адрес)
пример: localhost, sample.example.com, 8.8.8.8	
username	Имя пользователя
password	Пароль пользователя
auth	Выбор протокола для аутентификации
значения: any, chap, mschap, mschap-v2, pap, eap	**условия:** encryption = mppe
encryption	Метод защиты туннеля
значения: none, mppe	**условия:** /defaults/ipsec_installed = true
psk	Общий PSK ключ для аутентификации и обмена ключами
мин. длина: 8	**условия:** encryption = ipsec

ppp-option	Опции демона протокола Point-to-Point
значения: lcp-echo-failure, lcp-echo-interval, lcp-max-configure, lcp-max-failure, lcp-max-terminate, lcp-restart, ipcp-accept-local, ipcp-accept-remote, ipcp-max-configure, ipcp-max-failure, ipcp-max-terminate, ipcp-restart, mru, mtu	
debug	Режим подробного логгирования
значения: true, false	

7.1.2. Настройка PPTP client для 20.x

Туннель PPTP представлен на роутерах iRZ 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!

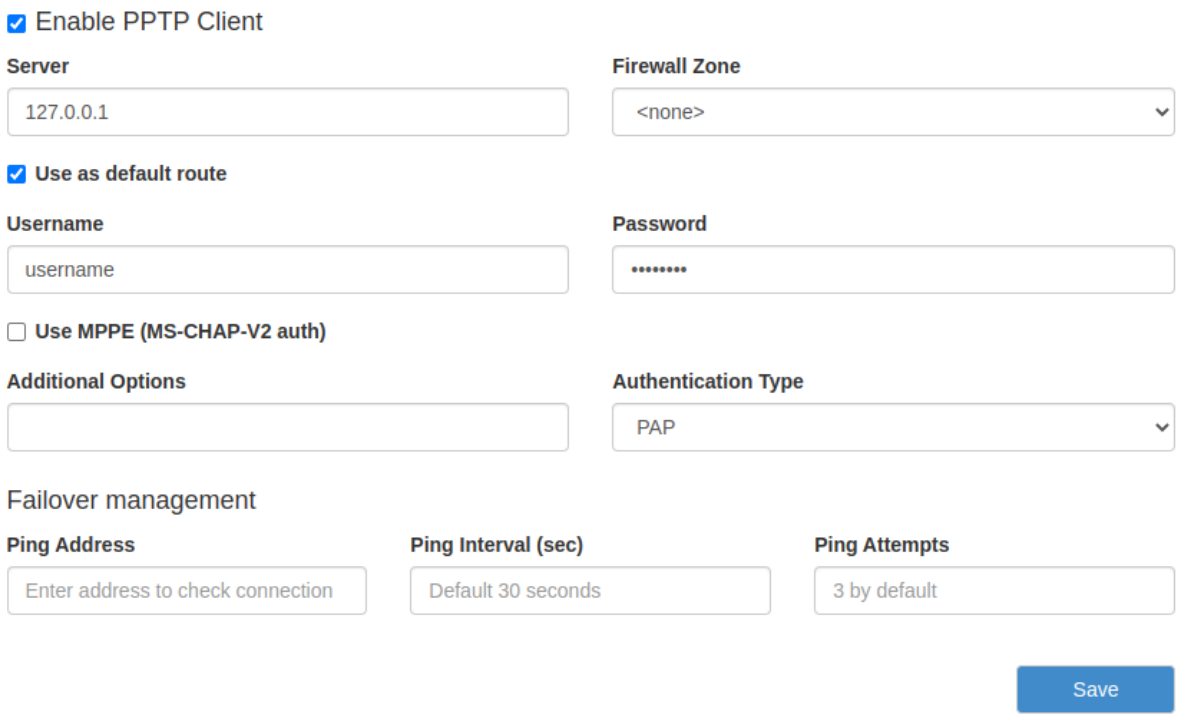


Рис. 15. Пример интерфейса PPTP Client

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).

7.2. L2TP

7.2.1. Настройка L2TP для irzOS

Данный раздел настраивает роутер для работы в качестве клиента L2TPv2, позволяя ему устанавливать безопасный туннель с удаленным L2TP-сервером. Туннель устанавливается поверх протокола PPP (Point-to-Point Protocol) и обычно используется для подключения к корпоративным сетям или сервисам удаленного доступа.

Основная настройка включает в себя указание *IP-адреса* удаленного сервера и предоставление необходимых *Имени пользователя* и *Пароля* для аутентификации. *Тип аутентификации* можно выбрать в соответствии с требованиями сервера.

Помимо базовой настройки подключения, можно включить *Шифрование* (как правило, MPPE) для защиты передаваемых данных. Поле *Метрика* позволяет управлять приоритетом маршрута в таблице маршрутизации роутера, что является важным для конфигураций с несколькими WAN-каналами или для отказоустойчивости.

СВОЙСТВА

disabled	Выключить конфигурацию
значения: true, false	
local-ip	Локальный адрес туннеля или интерфейс
значения: /ip interface, /mobile modem, /tunnel eoip, /tunnel gre, /tunnel l2tp, /tunnel openvpn, /tunnel pptp, /tunnel wireguard interface, /tunnel l2tpv3, /tunnel atunnel, /defaults server, auto **пример:** bridge0, 192.168.1.1	
remote-ip	Адрес удалённого хоста (FQDN или IP адрес)
пример: localhost, sample.example.com, 8.8.8.8	
username	Имя пользователя
password	Пароль пользователя
auth	Выбор протокола для аутентификации
значения: any, chap, mschap, mschap-v2, pap	**условия:** encryption = mppe
encryption	Метод защиты туннеля
значения: none, mppe	**условия:** /defaults/ipsec_installed = true
psk	Общий PSK ключ для аутентификации и обмена ключами
мин. длина: 8	**условия:** encryption = ipsec
ppp-option	Опции демона протокола Point-to-Point
значения: lcp-echo-failure, lcp-echo-interval, lcp-max-configure, lcp-max-failure, lcp-max-terminate, lcp-restart, ipcp-accept-local, ipcp-accept-remote, ipcp-max-configure, ipcp-max-failure, ipcp-max-terminate, ipcp-restart, mru, mtu	

debug	Режим подробного логгирования
значения: true, false	

7.2.2. Настройка L2TP v3 для irzOS

В этом разделе настраиваются туннели L2TPv3 (Layer 2 Tunneling Protocol version 3) — стандартизированный IETF протокол для создания соединений 2-го уровня "точка-точка" поверх IP-сети.

В отличие от своего предшественника L2TPv2, протокол L2TPv3 работает независимо от PPP и разработан как более универсальный и эффективный механизм транспорта L2. Его основная функция — инкапсулировать и передавать полные Ethernet-кадры, фактически создавая «псевдо-провод», который соединяет два удаленных сетевых сегмента.

Настройка требует определения конечных точек туннеля (*Local IP*, *Remote IP*) и набора уникальных идентификаторов (*Tunnel-Id*, *Session-Id*), которые должны совпадать на обеих сторонах для установки соединения.

L2TPv3 не имеет собственного встроенного шифрования, для защиты он использует нижележащий протокол безопасности транспортного уровня. Данная реализация поддерживает включение *IPsec* для шифрования всего туннеля L2TPv3.

СВОЙСТВА

disabled	Выключить конфигурацию
значения: true, false	
local-ip	Локальный адрес туннеля или интерфейс
значения: /ip interface, /mobile modem, /tunnel eoip, /tunnel gre, /tunnel l2tp, /tunnel openvpn, /tunnel pptp, /tunnel wireguard interface, /tunnel l2tpv3, /tunnel atunnel, /defaults server, auto **пример:** bridge0, 192.168.1.1	
remote-ip	Адрес удалённого хоста (FQDN ил IP адрес)
пример: localhost, sample.example.com, 8.8.8.8	
tunnel-ip	Адрес туннельного интерфейса
пример: 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	
encryption	Метод защиты туннеля
значения: none	**условия:** /defaults/ipsec_installed = true
psk	Общий PSK ключ для аутентификации и обмена ключами
мин. длина: 8	**условия:** encryption = ipsec
macaddr	MAC адрес
пример: FE:FF:FF:FF:FF:FF	
mtu	MTU интерфейса
минимум: 70, **максимум:** 65535	

l2spec-type	Тип заголовка (header) для второго уровня
значения: default, none	
tunnel-id	ID туннеля
минимум: 1, **максимум:** 4294967295	
peer-tunnel-id	ID туннеля удалённой стороны
минимум: 1, **максимум:** 4294967295	
session-id	ID сессии туннеля
минимум: 1, **максимум:** 4294967295	
peer-session-id	ID сессии удалённой стороны
минимум: 1, **максимум:** 4294967295	
encap	Тип инкапсуляции протокола
значения: ip, udp	
udp-dport	UDP порт удалённой стороны в случае UDP энкапсуляции
минимум: 1024 **пример:** 80, !80	**условия:** encap = udp
udp-sport	UDP порт для UDP энкапсуляции
минимум: 1024 **пример:** 80, !80	**условия:** encap = udp

7.2.3. Настройка L2TPv2 Client для 20.x

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.

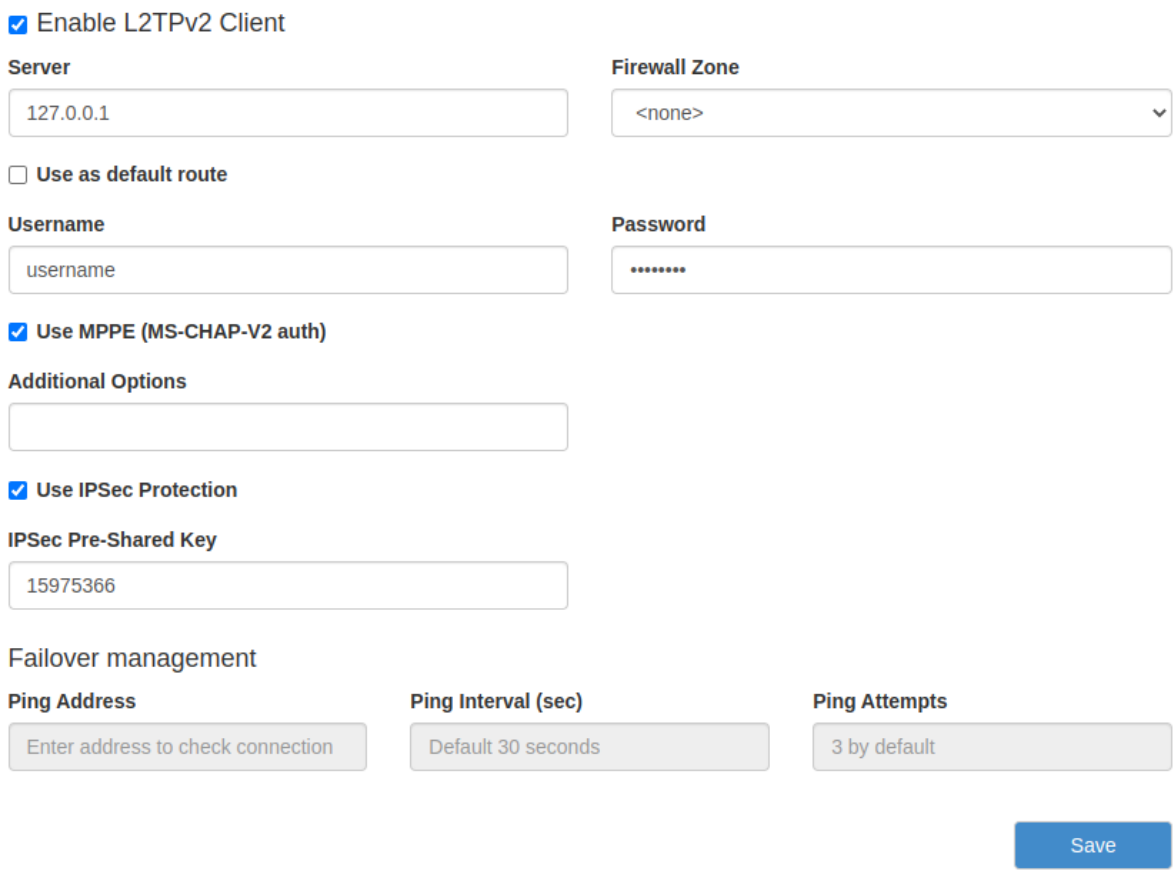


Рис. 16. Пример интерфейса L2TPv2 Client

Таблица 10. 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).

7.2.4. Настройка L2TPv3 для 20.x

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.

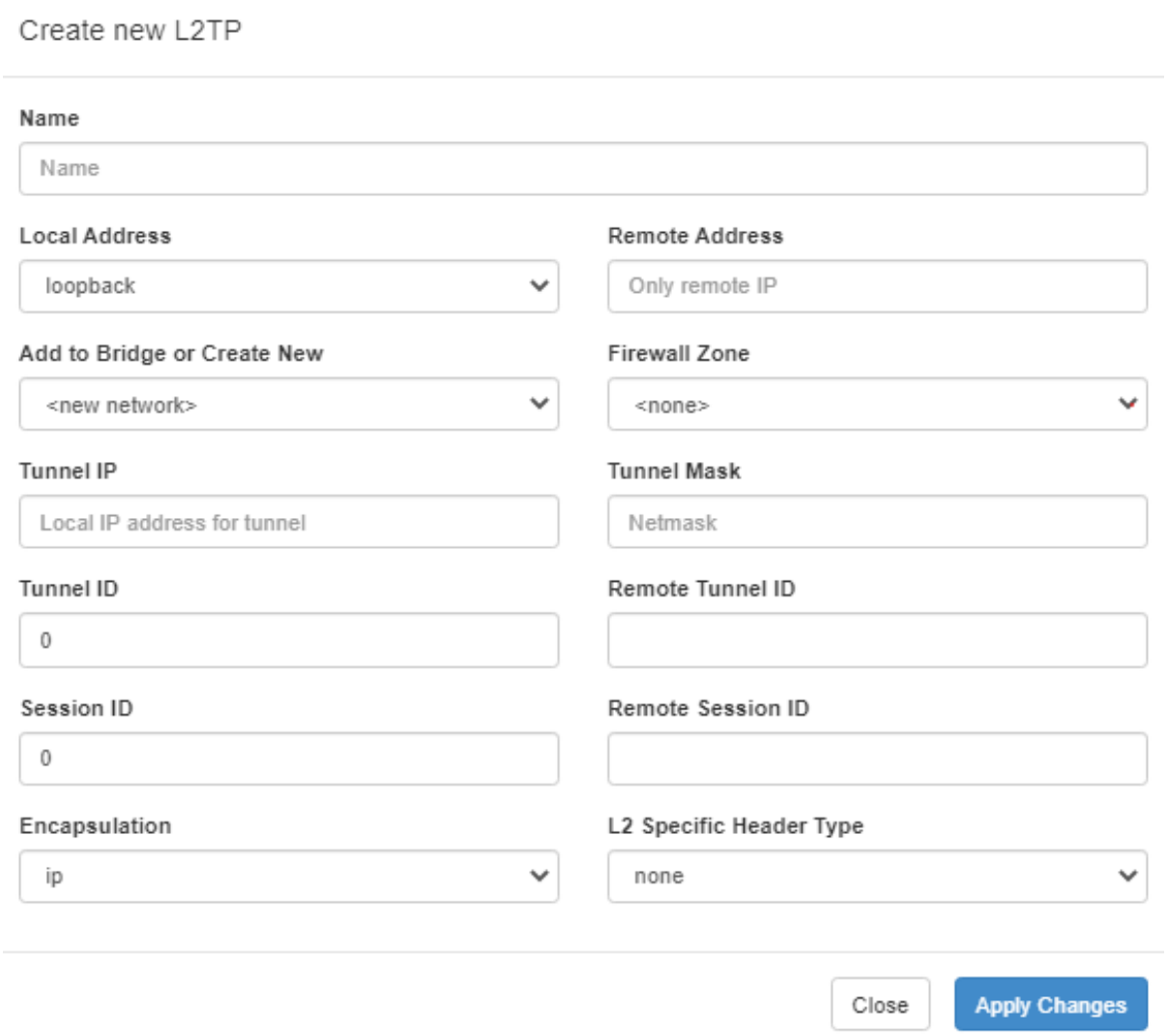


Рис. 17. Настройка L2TP3-туннеля

Таблица 11. 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
Source UDP Port	Порт источника.
Destination UDP Port	Порт назначения.

7.3. OpenVPN

7.3.1. Настройка OpenVPN для irzOS

:software:irzos_web:partial$schema-description/tunnel_OpenVPN_schema-description.adoc[]

:software:irzos:partial$cli_tables/tunnel_OpenVPN.adoc[]

7.3.2. Настройка OpenVPN Layer 2: dev TAP для 20.x

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.

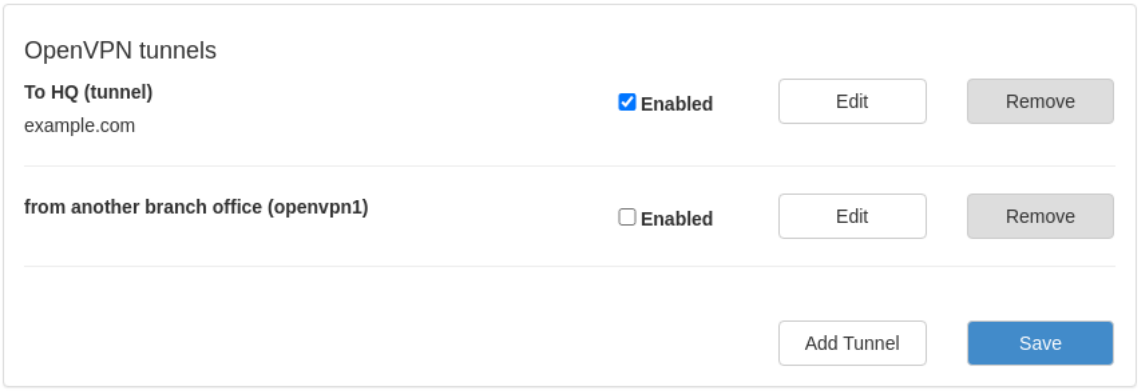


Рис. 18. Пример интерфейса раздела OpenVPN tunnels

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).

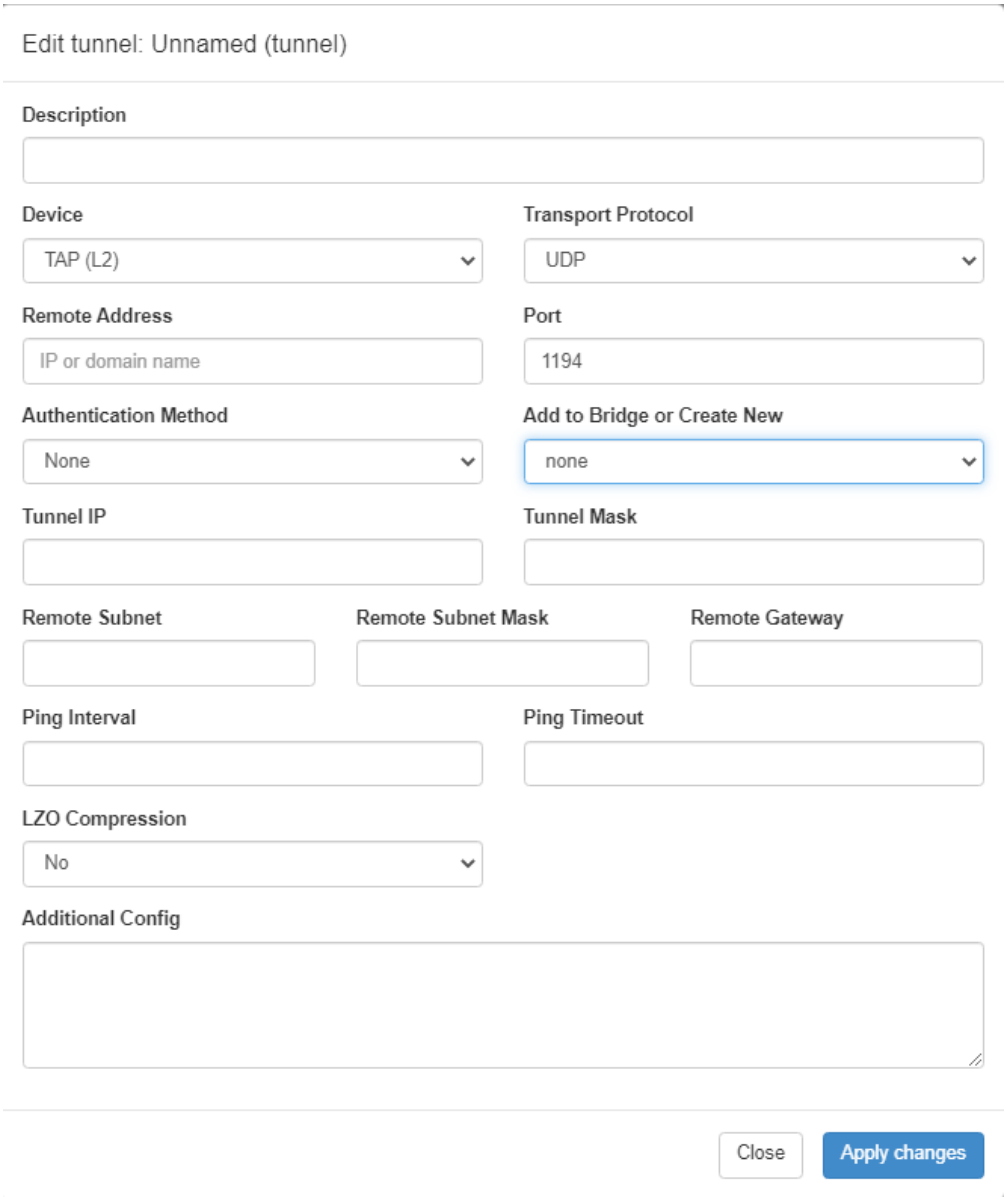


Рис. 19. Пример конфигураций OpenVPN. Настройка OpenVPN

Таблица 12. 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 12. 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, режим по умолчанию • None — не указан тип сжатия 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.

7.3.3. Настройка OpenVPN Layer 3: dev TUN для 20.x

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.

7.4. GRE

7.4.1. Настройка gre для irzOS

Данный раздел настраивает туннели GRE (Generic Routing Encapsulation) — универсальный протокол для инкапсуляции широкого спектра протоколов сетевого уровня внутрь IP-туннелей типа "точка-точка".

Основное преимущество GRE заключается в его способности транспортировать данные, которые не могут быть напрямую маршрутизированы в стандартной IP-сети, например, не-IP протоколы или multicast-трафик. Он также часто используется для создания оверлейных сетей, например, для передачи трафика IPv6 через сеть, работающую только на IPv4 (и наоборот).

Эта страница позволяет настроить все стандартные параметры GRE, включая конечные точки туннеля (*Local IP* и *Remote IP*) и опциональный *Ключ* для идентификации конкретного туннеля при наличии нескольких соединений с одним удаленным узлом. Также здесь доступны расширенные средства управления пакетами, такие как изменение *TTL* и *ToS*, и встроенный механизм *Keepalive* для мониторинга состояния туннеля и его автоматического отключения, если удаленная точка становится недоступной.

СВОЙСТВА

disabled	Выключить конфигурацию
значения: true, false	
local-ip	Локальный адрес туннеля или интерфейс
значения: /ip interface, /mobile modem, /tunnel eoip, /tunnel gre, /tunnel l2tp, /tunnel openvpn, /tunnel pptp, /tunnel wireguard interface, /tunnel l2tpv3, /tunnel atunnel, /defaults server, auto **пример:** bridge0, 192.168.1.1	
remote-ip	Адрес удалённого хоста (FQDN ил IP адрес)
пример: localhost, sample.example.com, 8.8.8.8	
tunnel-ip	Адрес туннельного интерфейса
пример: 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	
key	GRE key туннеля
минимум: 0, **максимум:** 4294967295	
encryption	Метод защиты туннеля
значения: none	
psk	Общий PSK ключ для аутентификации и обмена ключами
мин. длина: 8	**условия:** encryption = ipsec
mtu	MTU туннельного интерфейса
минимум: 70, **максимум:** 65535	
ttl	TTL туннельного интерфейса
минимум: 1, **максимум:** 255	

dscp	DSCP метка, присваемая GRE трафику
do-not-frag	Установить флаг запрета фрагментации пакета
значения: true, false	
keepalive-delay	Интервал отправки keepalive пакета в отсутствии трафика в туннеле
минимум: 0, **максимум:** 4294967	
keepalive-retries	Число попыток до перехода в состояние DOWN
минимум: 0, **максимум:** 4294967295	**условия:** keepalive-delay != "" && keepalive-delay != 0

7.4.2. Настройка GRE туннеля уровня L2 для 20.x

В примерах настройки используется следующая схема сети:

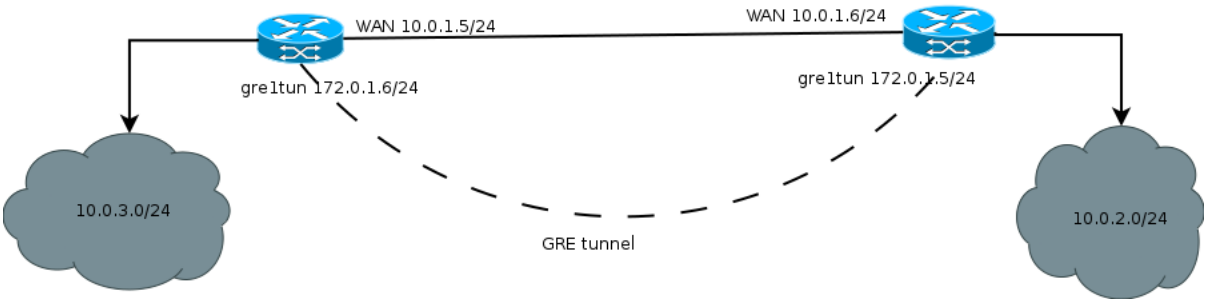


Рис. 20. Примеры конфигураций GRE. Схема сети

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**;

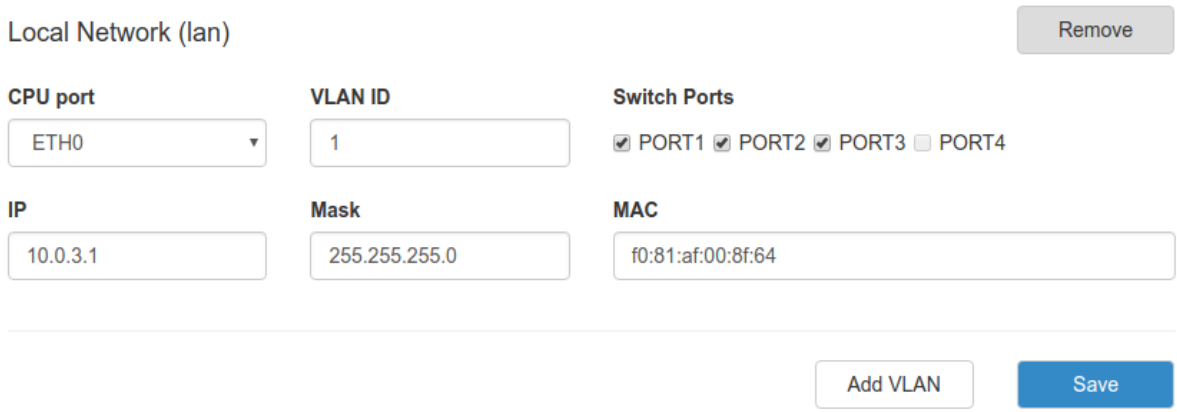


Рис. 21. Примеры конфигураций Local Network. Настройка локальной сети

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

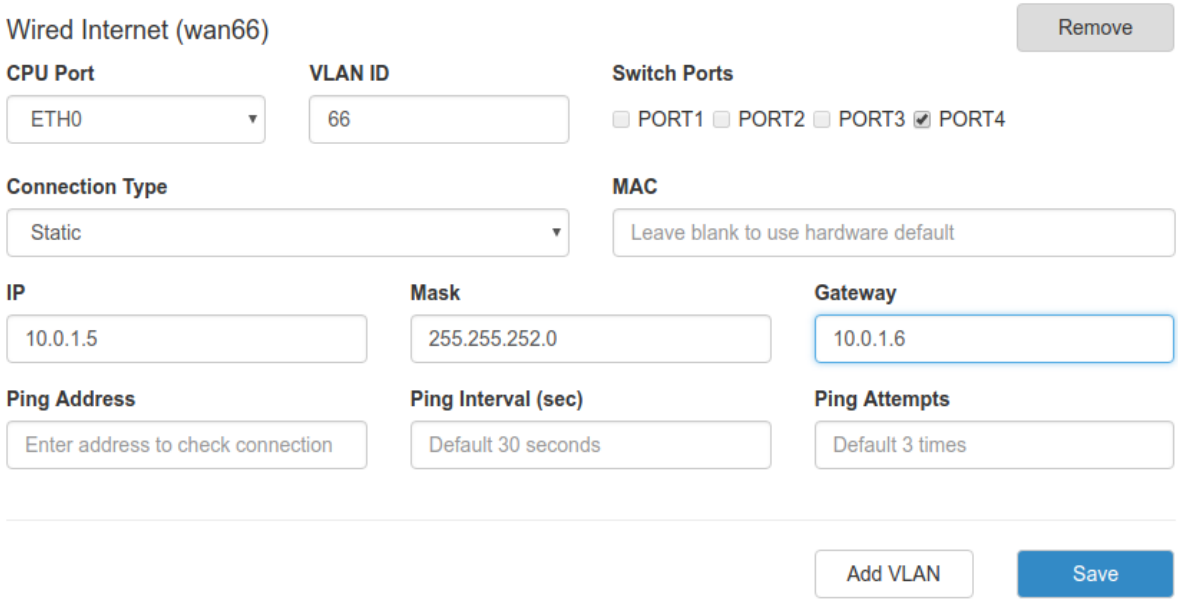


Рис. 22. Примеры конфигураций Wired Internet. Настройка WAN

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**.

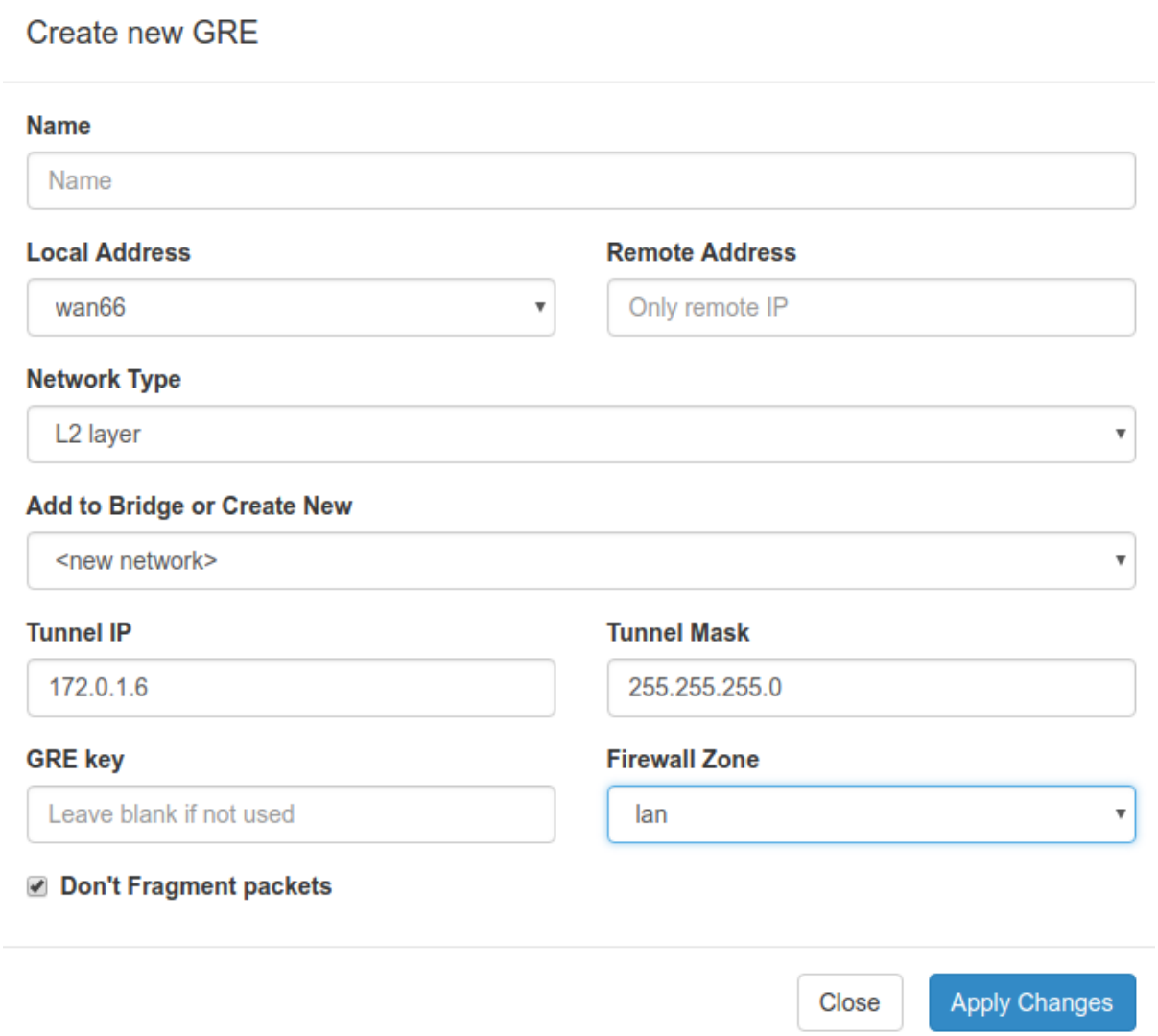


Рис. 23. Примеры конфигураций GRE. Настройка GRE-туннеля

7.4.3. Настройка GRE туннеля уровня L3 для 20.x

В примерах настройки используется следующая схема сети:

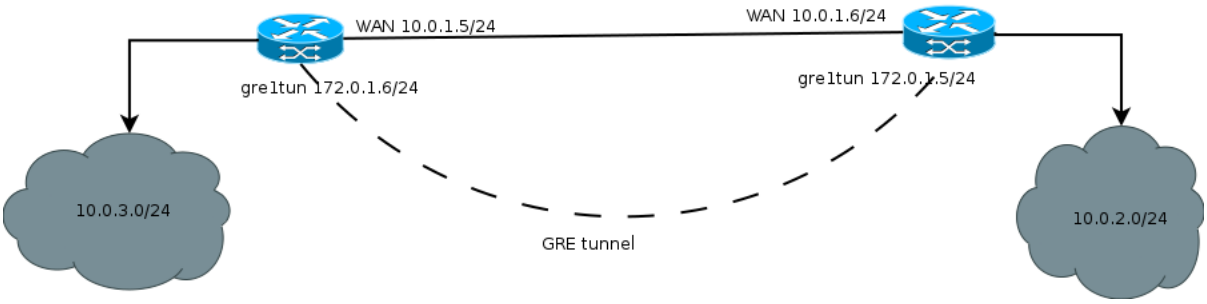


Рис. 24. Примеры конфигураций GRE. Схема сети

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;

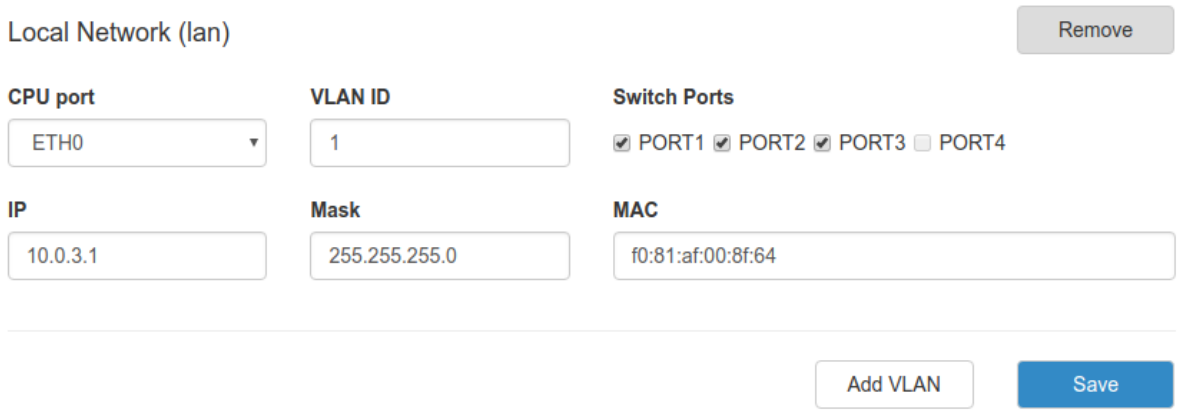


Рис. 25. Примеры конфигураций GRE. Настройка локальной сети

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);

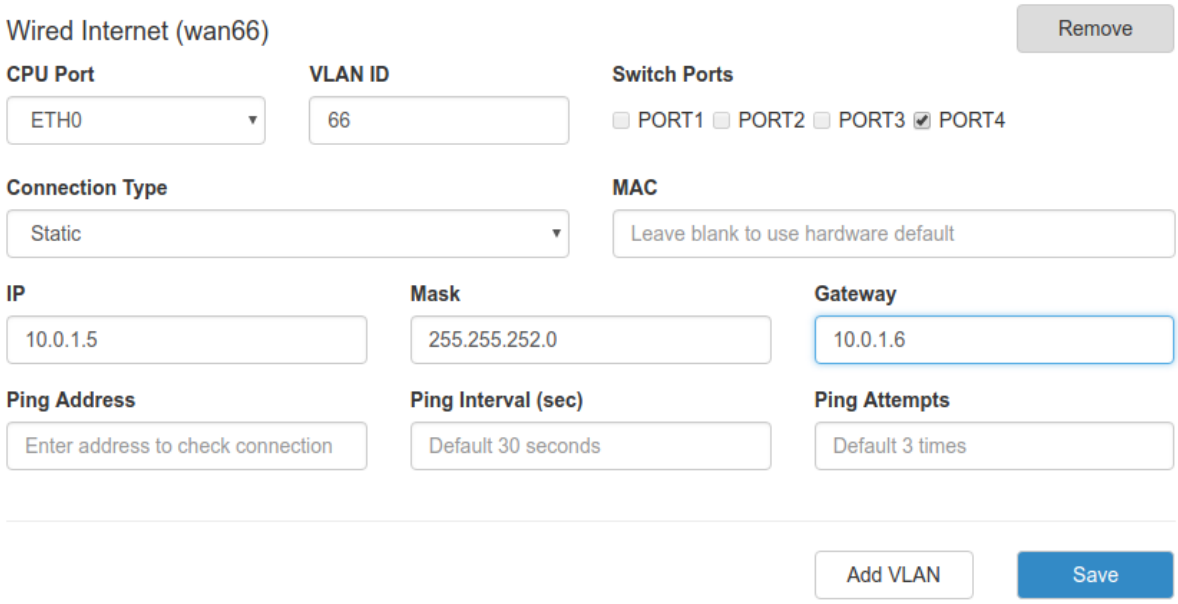


Рис. 26. Примеры конфигураций GRE. Настройка WAN

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. Укажите в поле **Keepalive Delay** временной интервал в секундах, по истечении которого идет проверка соединения со встречной стороной;
15. Укажите в поле **Keepalive Retries** количество неудачных попыток, после которых туннель GRE отключится. При получении первого ответа от встречной стороны соединение восстанавливается;
16. При необходимости, поставьте устройству запрет на фрагментацию (разделение) пакета на маршруте следования, поставив галочку напротив пункта **Don’t fragment**.

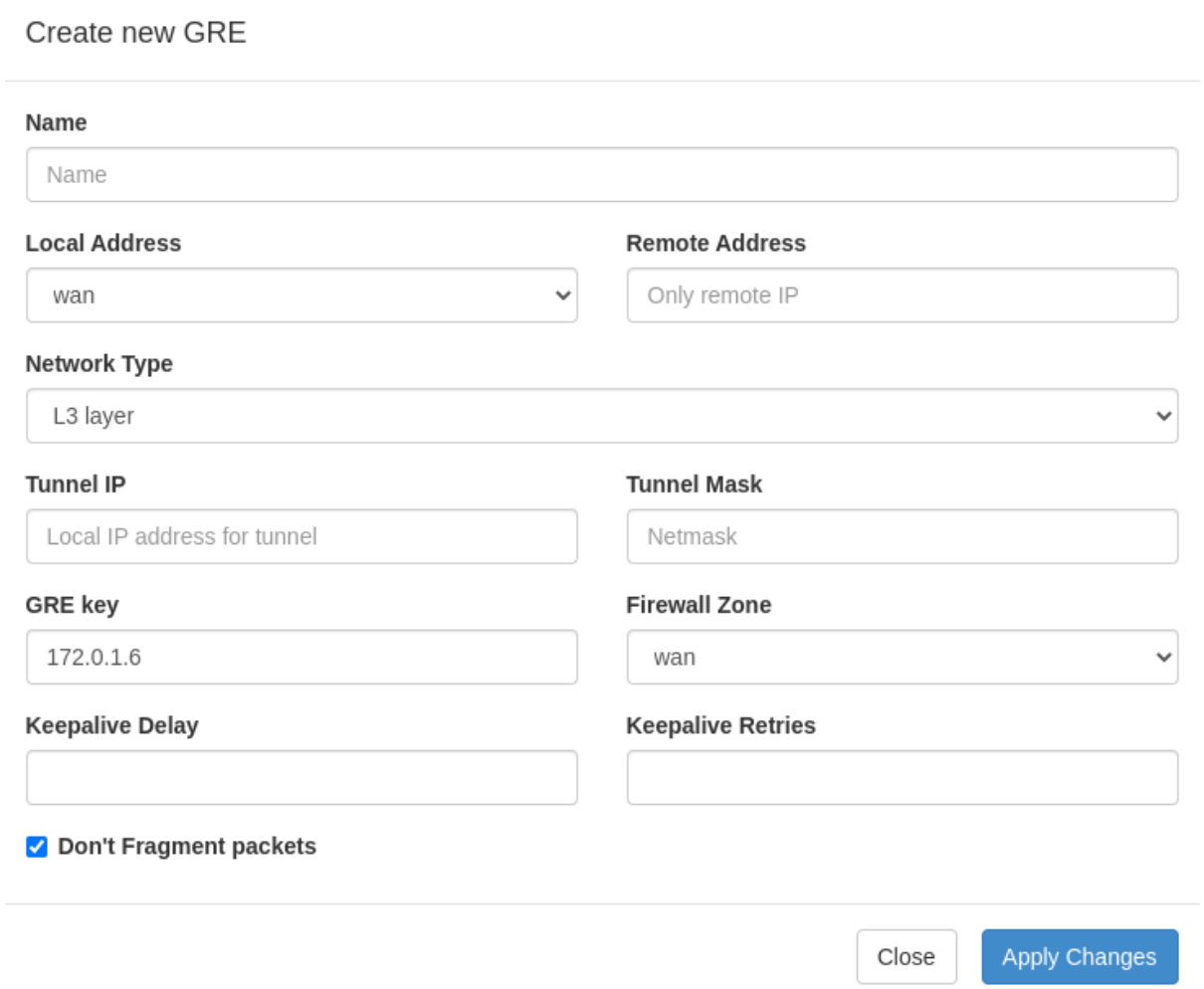


Рис. 27. Примеры конфигураций GRE. Настройка GRE-туннеля

7.5. IPsec

7.5.1. Настройка ipsec для irzOS

association

В этом разделе определяются ключевые политики безопасности IPsec. Эти политики, часто именуемые дочерними SA (Child SA) в терминологии IKEv2, являются правилами, которые точно устанавливают, какой сетевой трафик подлежит защите, как он будет защищен, и между какими узлами.

Основная функция здесь — это настройка *Локальных* и *Удаленных селекторов трафика*. Эти селекторы определяют "целевой трафик", который будет инициировать инкапсуляцию IPsec. Указывая диапазоны IP-адресов, протоколы и порты, можно создавать точные правила, соответствующие требованиям безопасности вашей сети.

Каждая политика привязывается к определенному *Соединению* (которое определяет пиры) и использует *Профиль* (который определяет алгоритмы шифрования и целостности для Фазы 2), что создает модульную и масштабируемую конфигурацию.

Функция *Apply* в этом разделе выполняет «мягкую» перезагрузку, что позволяет добавлять или изменять политики без разрыва существующих, активных безопасных ассоциаций. Для принудительного закрытия конкретной SA используйте страницу Status.

СВОЙСТВА

disabled	Выключить конфигурацию
значения: true, false	
connection	IKE соединение для согласования SA
proposal	Алгоритм шифрования и аутентификации ESP
значения: /tunnel ipsec proposal	
auto	Действие после применения конфигурации SA
значения: route, start	
type	Согласование режима работы SA
значения: tunnel, transport, passthrough, drop	
leftsubnet	Источники трафика для согласования с локальной стороны
rightsubnet	Источники трафика для согласования с удалённой стороны

connection

В этом разделе определяются соединения IKE (Internet Key Exchange). Соединение IKE устанавливает идентификационные данные и параметры безопасности для самих пиров, создавая защищенный канал управления (SA Фазы 1), который используется для согласования политик шифрования данных (дочерних SA Фазы 2).

Ключевые настройки включают:

- Определение пиров путем указания их *локального* и *удаленного* адресов шлюзов.

- Выбор версии IKE (*IKEv1* или *IKEv2*), которая будет управлять процессом согласования.
- Указание идентификаторов пиров (*Local ID*, *Remote ID*) и метода аутентификации (*Local auth*, *Remote auth*). Это ядро модели безопасности, поддерживающее такие методы, как общие ключи (Pre-Shared Keys, PSK) и аутентификацию по открытым ключам (на основе сертификатов).
- Назначение профиля IKE, который содержит конкретные алгоритмы шифрования и целостности Фазы 1, используемые для защиты канала управления.

Функция *Apply* в этом разделе выполняет «мягкую» перезагрузку, что позволяет добавлять или изменять политики без разрыва существующих, активных безопасных ассоциаций. Для принудительного закрытия конкретной SA используйте страницу Status.

СВОЙСТВА

left	Локальный адрес туннеля или интерфейс
значения: /ip interface, /mobile modem, auto	
right	Адрес удалённого хоста (FQDN ил IP адрес)
пример: localhost, sample.example.com, 8.8.8.8	
keyexchange	Версия протокола IKE для безопасного согласования SA
значения: ikev2, ikev1	
profile	IKE/ISAKMP профиль шифрования и аутентификации SA
значения: /tunnel ipsec profile	
leftid	Локальный IKE идентификатор для аутентификации
	условия: auth = pubkey
rightid	IKE идентификатор для аутентификации удалённой стороны
auth	Метод аутентификации между сторонами
значения: psk, pubkey	
psk	Общий PSK ключ для аутентификации и обмена ключами
мин. длина: 8	**условия:** auth = psk
cert	Сертификат (включая закрытый ключ)
значения: /storage certificate	**условия:** auth = pubkey
leftsourceip	Virtual IP для использования в качестве источника трафика
пример: 192.168.1.1, %config	
rightsourceip	Выделить виртуальный адрес для удалённой стороны
пример: 192.168.1.1/24, 192.168.1.1-192.168.1.100, %config	

profile

В этом разделе определяются многоразовые **Профили IKE**. Каждый профиль представляет собой именованный набор криптографических алгоритмов и параметров, который управляет процессом

установления безопасной ассоциации Фазы 1 (IKE SA).

Создание таких профилей позволяет стандартизировать и упростить конфигурацию IPsec. Вместо того чтобы повторно определять один и тот же набор алгоритмов для каждого соединения, можно создать один профиль и ссылаться на него из нескольких *Соединений* IKE.

Профиль определяет все ключевые параметры безопасности для согласования IKE, включая:

- Разрешенные алгоритмы *Шифрования*, *Хеширования* и *Псевдослучайной функции*.
- *Группу Диффи-Хеллмана (DH)*, используемую для безопасного обмена ключами.
- *Время жизни IKE*, которое определяет, как долго SA Фазы 1 остается действительной, прежде чем потребуется повторное согласование.
- Параметры Dead Peer Detection (*DPD*), которые контролируют, как роутер отслеживает доступность удаленного пира и какое *Действие* предпринимать, если пир перестает отвечать.

Функция *Apply* в этом разделе выполняет «мягкую» перезагрузку, что позволяет добавлять или изменять политики без разрыва существующих, активных безопасных ассоциаций. Для принудительного закрытия конкретной SA используйте страницу Status.

СВОЙСТВА

encryption	Алгоритм шифрования для безопасной передачи данных
значения: aes128, aes192, aes256, 3des	
hash	Хэш-функция проверки подлинности
значения: sha1, sha256, sha384, sha512, md5	
prf	Псевдослучайная хэш-функция для получения материала ключа
значения: sha1, sha256, sha384, sha512, md5	
dh	Протокол Diffie-Hellman для обмена ключами
значения: modp768, modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, modp8192	
ikelifetime	Интервал времени до пересогласования IKE/ISAKMP SA
dpddelay	Интервал отправки DPD пакета (если нет иного трафика)
dpdtimeout	Таймаут без ответа на DPD пакет, через который прервать IKEv1 соединение
dpdaction	Действие, выполняемое при разрыве соединения по таймауту
значения: hold, restart, clear, none	

proposal

В этом разделе определяются многоразовые **Профили IPsec (Proposals)**. Каждый профиль представляет собой именованный набор алгоритмов безопасности, который управляет тем, как именно будет защищаться трафик данных внутри IPsec-туннеля (SA Фазы 2, или дочерняя SA).

Аналогично Профилям IKE, эти профили обеспечивают модульный подход к управлению политиками безопасности. Определяя профиль, вы задаете набор алгоритмов *Шифрования* и *Аутентификации*, которые будут использоваться протоколом ESP (Encapsulating Security Payload) для обеспечения конфиденциальности и целостности данных.

Ключевые параметры, определяемые в профиле, включают:

- Криптографические алгоритмы для защиты данных (*Шифрование*, *Аутентификация*).
- Группу Perfect Forward Secrecy (*PFS*), которая гарантирует, что для каждого сеанса будет сгенерирован новый, независимый ключ, что повышает долгосрочную безопасность.
- *Время жизни* дочерней SA, которое определяет, как часто должны пересогласовываться ключи шифрования данных.

Эти профили затем используются в разделе "Associations", чтобы легко применять одинаковые политики защиты данных к разным туннелям.

СВОЙСТВА

encryption	Алгоритм шифрования для безопасной передачи данных
значения: aes128, aes192, aes256, 3des	
auth	HMAC алгоритм для аутентификации
значения: sha1, sha256, sha384, sha512, md5	
pfs	Алгоритм PFS, гарантирует что DH ключи не будут использованы повторно
значения: modp768, modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, modp8192, none	
lifetime	Интервал времени (сек) до пересогласования

status

Данный раздел отображает текущее рабочее состояние всех настроенных IPsec-туннелей. Он служит основным диагностическим инструментом для проверки активности настроенных туннелей и для устранения проблем с подключением.

Страница наглядно показывает результат настроек, заданных в разделах *Connections* и *Associations*. Здесь администратор может убедиться, что нужные пиры (*LOCAL-ID* и *REMOTE-ID*) и политики трафика (*LOCAL-TS* и *REMOTE-TS*) успешно согласовали и установили туннель.

Столбец *STATUS* особенно полезен для диагностики, поскольку он предоставляет конкретную информацию о состоянии туннеля, что позволяет быстро выявлять проблемы конфигурации или сети. Таблица также содержит важные операционные данные, включая время работы туннеля и счетчики трафика.

КОМАНДЫ

debug	Изменить уровень детализации логгирования
	level - Уровень детализации логирования (обязательно)

СВОЙСТВА

association	IPSec SA
	условия: association != ""
uniqueid	Уникальный идентификатор SA

status	Статус SA
local	Адрес с которого строится туннель
local-id	Локальной IKE идентификатор
remote	Адрес на который строится туннель
remote-id	IKE идентификатор удалённой стороны
uptime	Время с момента установки SA
encryption	Согласованый алгоритм шифрования
integrity	Согласованый алгоритм проверки целостности
prf	Согласованый PRF алгоритм
dh	Согласованая группа DH
local-ts	Источник трафика с локальной стороны
remote-ts	Источник трафика с удалённой стороны
expires	Время до истечения SA (rekeying/reauthentication)
reqid	Уникальный номер SA
rx-tx	Счётчик полученного / отправленного трафика

7.5.2. Настройка IPSec туннеля для 20.x

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**.

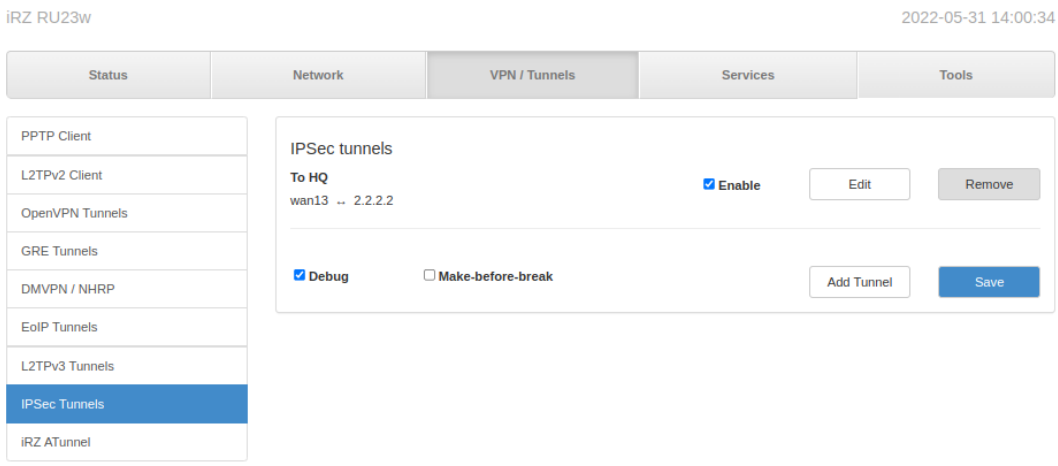


Рис. 28. Вкладка IPSec/Tunnels. Раздел IPSec tunnels

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.

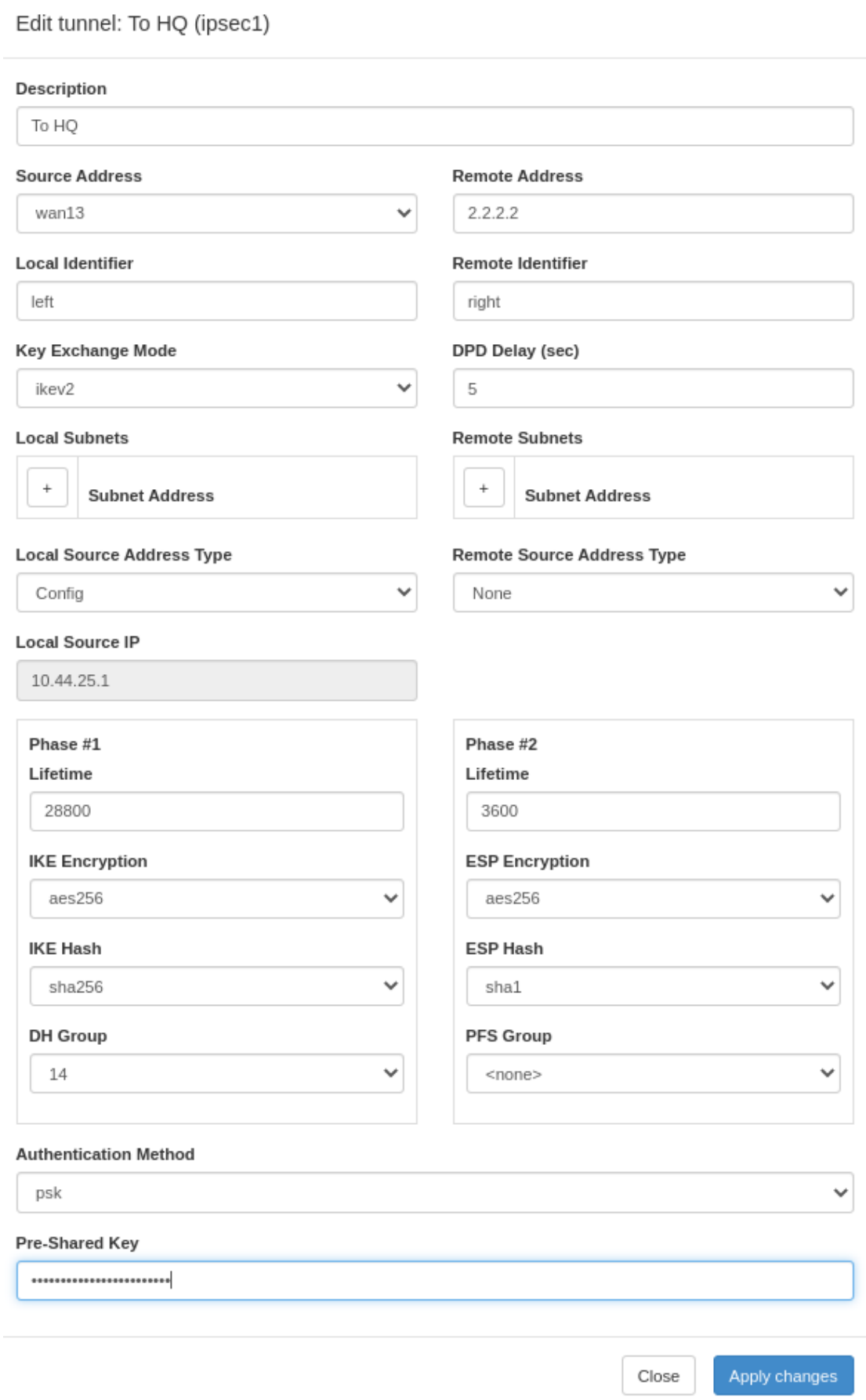


Рис. 29. Примеры конфигураций IPsec. Настройка IPsec-туннеля

Таблица 13. 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 строится туннель. Можно указать несколько адресов через ПРОБЕЛ. IPSec выполняет попытки подключения к хостам в порядке перечисления. Таймаут подключения 60 сек. Если в течение этого времени подключение не произошло, происходит переключение на следующий адрес 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** - автоматически, **Manual** - вручную)
Remote Source Address Type	Тип получения виртуального IP адреса для удаленной стороны (**None** - не настраивается, **Config** - автоматически, **Manual** - 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

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

Таблица 14. 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 15. 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

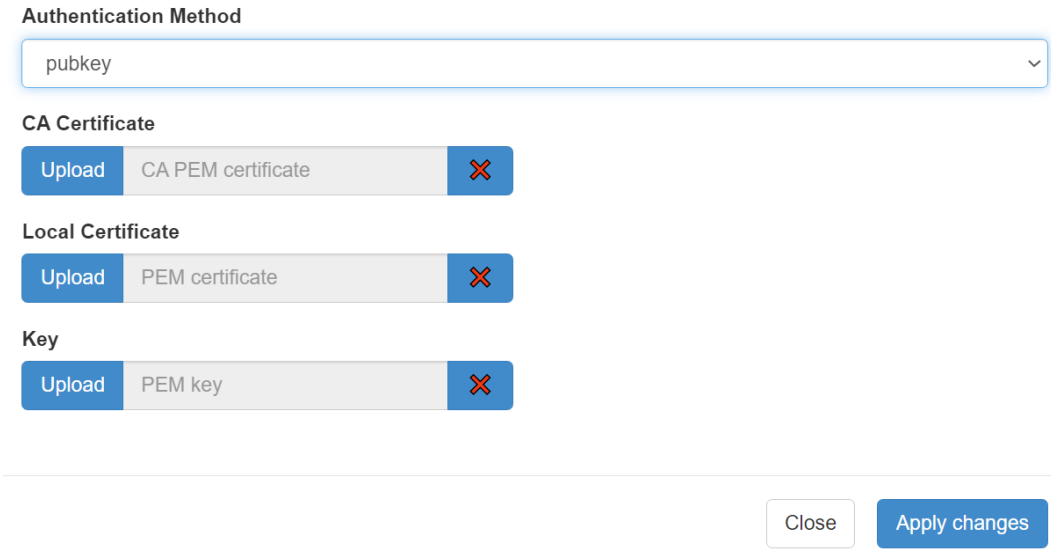


Рис. 30. Способ аутентификации pubkey

После удаления туннеля загруженные сертификаты удаляются автоматически при нажатии кнопки Save.

Статус IPSec туннеля

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

IPSec tunnel — информация о работе IPSec туннеля

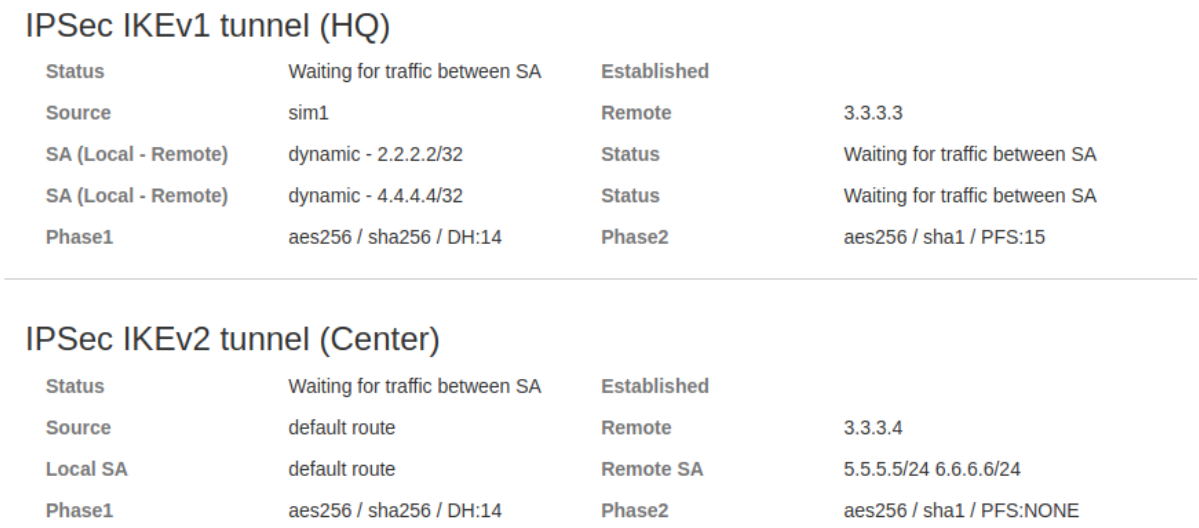


Рис. 31. Пример информации в разделе IPSec tunnel

Таблица 16. 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 17. 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)

7.6. EoIP

7.6.1. Настройка EoIP для irzOS

Данный раздел предназначен для настройки туннелей Ethernet over IP (EoIP) — протокола для создания прозрачного сетевого моста 2-го уровня между двумя удаленными точками через IP-сеть.

Туннель EoIP инкапсулирует полные Ethernet-кадры в IP-пакеты, фактически создавая виртуальное соединение "точка-точка" между двумя роутерами. Основной сценарий использования — бесшовное объединение двух раздельных сегментов LAN в единый широковещательный домен, в результате чего они ведут себя так, как будто соединены физическим Ethernet-кабелем.

Протокол EoIP, изначально разработанный компанией MikroTik, является простым и эффективным решением для расширения сетей L2. Такие туннели могут быть установлены поверх любого IP-транспорта, включая другие VPN, такие как IPsec или OpenVPN, что обеспечивает гибкий способ безопасного расширения связности на 2-м уровне.

СВОЙСТВА

disabled	Выключить конфигурацию
значения: true, false	
local-ip	Локальный адрес туннеля или интерфейс
значения: /ip interface, /mobile modem, /tunnel eoip, /tunnel gre, /tunnel l2tp, /tunnel openvpn, /tunnel pptp, /tunnel wireguard interface, /tunnel l2tpv3, /tunnel atunnel, /defaults server, auto **пример:** bridge0, 192.168.1.1	
remote-ip	Адрес удалённого хоста (FQDN ил IP адрес)
пример: localhost, sample.example.com, 8.8.8.8	
tunnel-ip	Адрес туннельного интерфейса
пример: 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	
tunnel-id	ID туннеля
минимум: 1, **максимум:** 65535	
macaddr	MAC адрес
пример: FE:FF:FF:FF:FF:FF	
mtu	MTU интерфейса
минимум: 70, **максимум:** 65535	
ttl	TTL интерфейса
минимум: 1, **максимум:** 255	
dscp	DSCP метка, присваемая GRE трафику
encryption	Метод защиты туннеля
значения: none	

psk	Общий PSK ключ для аутентификации и обмена ключами
мин. длина: 8	**условия:** encryption = ipsec

7.6.2. Настройка EoIP для 20.x

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.

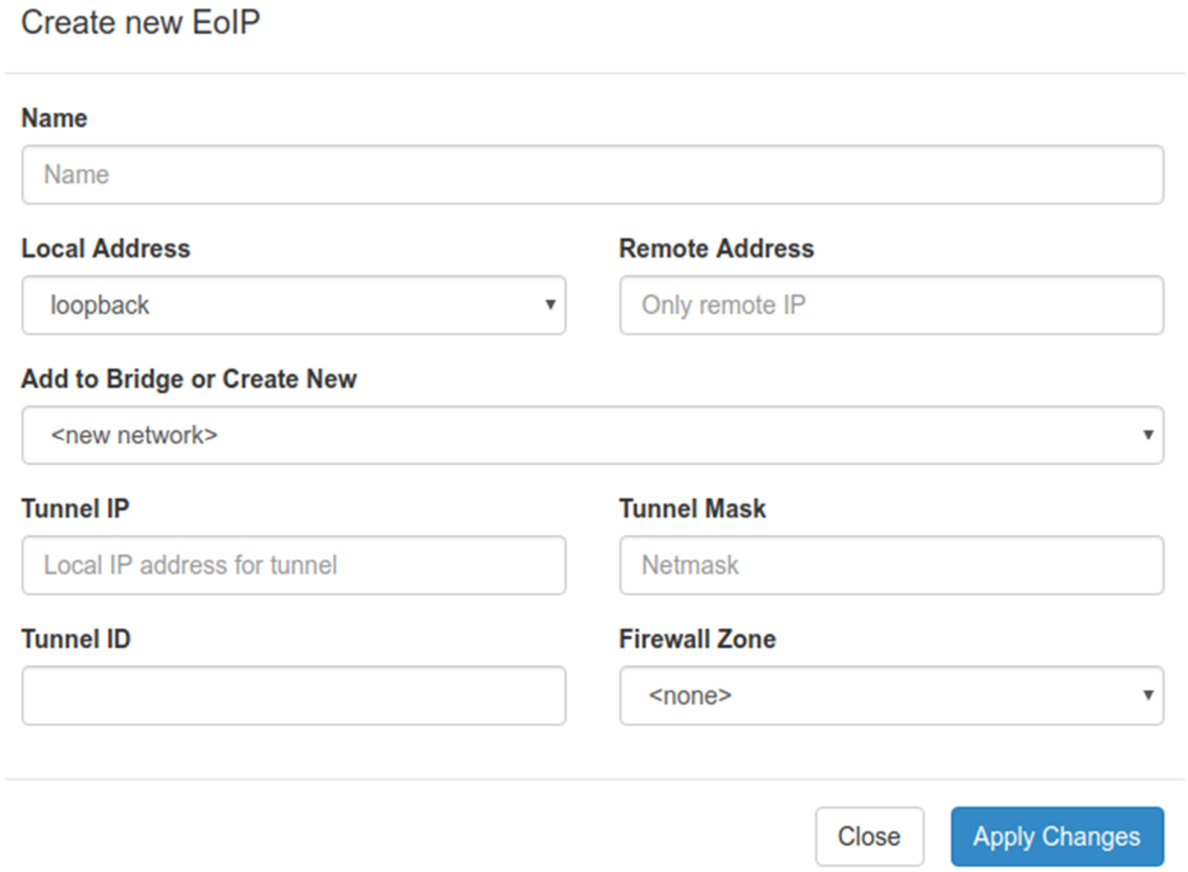


Рис. 32. Настройка EoIP-туннеля

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.

8. Сервисы

8.1. Настройка DHCP для irzOS

8.1.1. Lease

Подраздел отображает в реальном времени информацию обо всех IP-адресах, выданных встроенным DHCP-сервером роутера. Он служит центральной точкой для мониторинга подключенных к сети устройств и управления назначениями их IP-адресов.

В таблице перечислены все активные аренды с указанием MAC-адреса клиента, назначенного ему IP-адреса и времени истечения аренды.

Основная функция этой страницы — управление арендами, в частности, создание **статических аренд** (также известных как резервирования). Статическая аренда гарантирует, что определенное устройство, идентифицируемое по его MAC-адресу, всегда будет получать один и тот же IP-адрес от DHCP-сервера. Это необходимо для серверов, принтеров и любых других устройств, которым требуется постоянный и предсказуемый сетевой адрес.

Чтобы создать резервирование, вы можете просто выбрать существующую динамическую запись из списка и использовать функцию **Make Static**. Это действие преобразует временное назначение в постоянное. Кроме того, для каждой записи можно настроить интеграцию с DNS, присвоив ей полное доменное имя (FQDN).

КОМАНДЫ

make-static	Сделать динамическую запись lease постоянной

СВОЙСТВА

interface	Интерфейс, на котором может быть выдана статическая запись lease
значения: /service dhcp server, auto	
ip	IP адрес хоста
пример: 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	
mac	MAC адрес хоста
пример: FE:FF:FF:FF:FF:FF	
dns	Добавить DNS запись для разрешения IP адреса
значения: true, false	

fqdn	Указать имя хоста для разрешения IP адреса
пример: localhost, example.com, sample.example.com	

8.1.2. Server

Подраздел предназначен для определения и управления отдельными конфигурациями DHCP-сервера для каждого из ваших локальных сетевых интерфейсов. Это основная панель для настройки способа распределения IP-адресов в заданном сетевом сегменте.

Ключевым выбором на этой странице является Режим работы (**Mode**), который определяет, будет ли роутер выступать в роли DHCP-сервера или в роли агента ретрансляции DHCP.

Режим «Сервер» (Server)

При выборе режима **Server** роутер становится сервером, ответственным за выдачу IP-адресов в определенной сети. Здесь настраиваются основные параметры службы, такие как Диапазон IP-адресов (*Pool Of IP Addresses*) для аренды, Время аренды (*Leasetime*) и важную сетевую информацию, передаваемую клиентам, включая шлюз по умолчанию (*Router*) и DNS-серверы. Этот режим также позволяет выполнять расширенную настройку через пользовательские *DHCP-опции* для поддержки специализированных клиентов и сетевых сред.

Режим «Ретранслятор» (Relay)

При выборе режима **Relay** роутер не выдает IP-адреса самостоятельно. Вместо этого он прослушивает DHCP-запросы на локальном интерфейсе и пересылает их на централизованный удаленный DHCP-сервер. Этот режим обычно используется в корпоративных сетях для управления IP-адресами из единого центра. Настройка в этом режиме включает указание адреса удаленного Сервера и управление обработкой DHCP-опций (в частности, опции 82) при их ретрансляции.

СВОЙСТВА

disabled	Выключить конфигурацию
значения: true, false	
mode	Режим обработки DHCP запросов
значения: server, relay	
server	Адрес DHCP сервера для переадресации запросов
пример: 192.168.1.1, example.com, 192.168.1.1:80	**условия:** mode = relay
relay-mode	Действие над DHCP пакетом содержащим опцию 82
значения: append, replace, forward, discard	**условия:** mode = relay && suboption = true mode = relay && suboption = ""
remote-id	Option 82 Remote ID
	условия: mode = relay
hops	Максимальное количество прыжков (hop) прежде чем DHCP пакет будет отброшен
максимум: 255	**условия:** mode = relay

suboption	Send link selection suboption for directly connected clients
значения: true, false	**условия:** mode = relay
debug	Режим подробного логгирования
значения: true, false	**условия:** mode = relay
pool	Пул IP адресов для выдачи клиентам
	условия: mode = server
router	IP адрес шлюза (Опция 3)
пример: 192.168.1.1	**условия:** mode = server
dns-server	IP адрес DNS сервера (Опция 6)
	условия: mode = server
ntp-server	IP адрес NTP сервера (Опция 42)
	условия: mode = server
leasetime	Время аренды IP адреса
значения: 30m, 1h, 4h, 12h, 24h, 7d	**условия:** mode = server
flags	Параметр DHCP сервера
значения: authoritative, no-override, sequential-ip, rapid-commit	**условия:** mode = server
option	Дополнительные DHCP опции
значения: tftp-server, bootfile-name, classless-static-route	**условия:** mode = server

8.2. Настройка DHCP для 20.x

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!

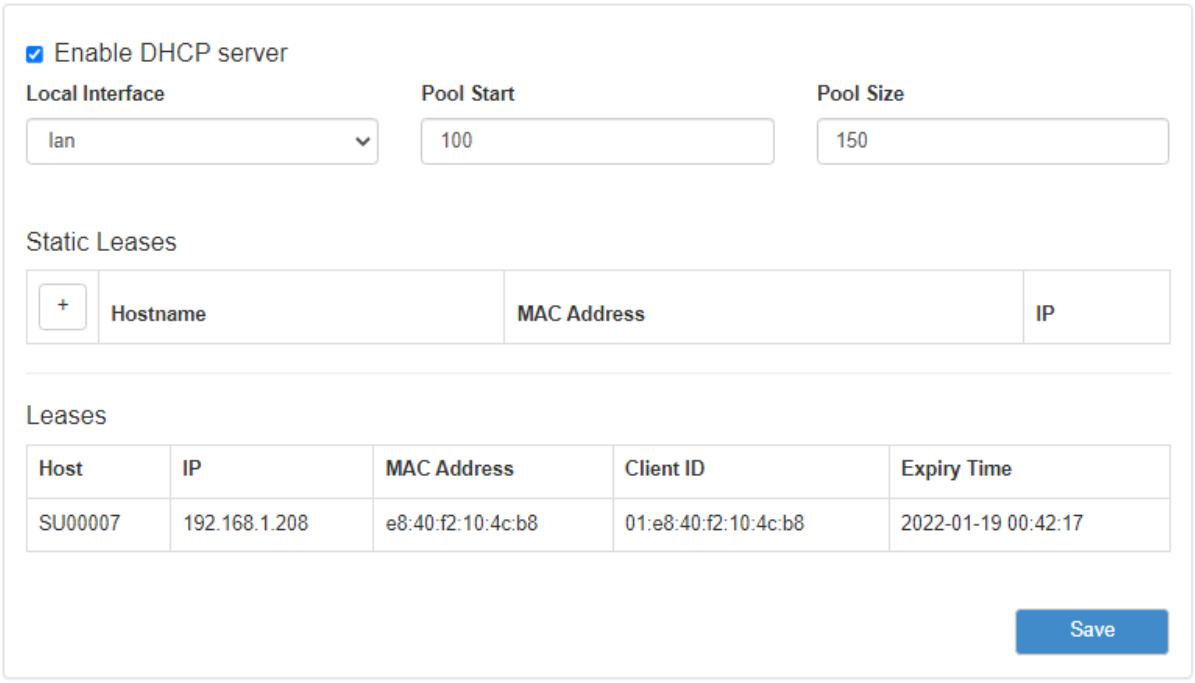


Рис. 33. Вкладка Services, раздел DHCP

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

Таблица 18. 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.

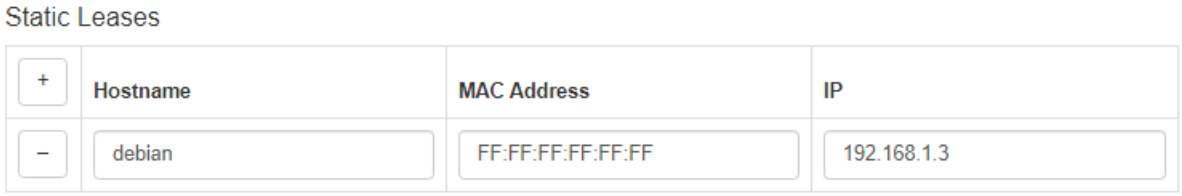


Рис. 34. Указание IP-адресов вручную

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. 35. Вкладка Tools, раздел DHCP Leases

Таблица 19. 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

8.3. Настройка DNS для irzOS

В этом разделе настраивается DNS-сервер роутера. Он служит общей точкой для обработки DNS-запросов от всех устройств в сети. Роутер пересылает эти запросы на внешние DNS-серверы и запоминает (кэширует) ответы, чтобы ускорить доступ при последующих обращениях к тем же сайтам.

Эта страница предоставляет комплексный контроль над процессом разрешения доменных имен:

- **Логика переадресации DNS:** Вы можете определить основной вышестоящий *DNS-сервер* (или серверы) для всех стандартных запросов. Кроме того, функция **DNS Forwarding** позволяет настроить условную пересылку, направляя запросы для определенных доменов (например, корпоративного домена) на другой набор DNS-серверов.
- **Разрешение локальных имен:** Функция *Static-Host* позволяет создавать собственные локальные DNS-записи, присваивая легко запоминаемые имена хостов устройствам в вашей сети (например, сопоставляя *nas.lan* с *192.168.1.10*).
- **Защита от DNS-rebinding:** Это функция безопасности, которая защищает вашу локальную сеть от соответствующих атак. Она работает, отбрасывая ответы от вышестоящих DNS-серверов, которые указывают на приватные, немаршрутизируемые IP-адреса (RFC1918). Исключения для доверенных сервисов можно настроить для определенных доменов или для DNS-черных списков, использующих localhost.
- **Привязка к интерфейсам:** Вы можете указать, на каких локальных интерфейсах DNS-сервер должен прослушивать запросы от клиентов.

СВОЙСТВА

dns-address	Адрес DNS сервера для пересылки запросов
dns-forwarding	Доменная зона и её DNS сервер для разрешения IP адресов
interface	Интерфейс для обслуживания DNS запросов
значения: /ip interface, /mobile modem, /tunnel eoip, /tunnel gre, /tunnel l2tp, /tunnel openvpn, /tunnel pptp, /tunnel wireguard interface, /tunnel l2tpv3, /tunnel atunnel, /defaults server	
static-host	Статическая A-запись DNS
rebind-protection	Защита от атаки DNS rebind (отбрасывание ответов с адресом из RFC1918)
значения: true, false	
rebind-localhost	Разрешить ответы с адресом из диапазона 127.0.0.0/8 (DNS based blacklist)
значения: true, false	**условия:** rebind-protection = true
rebind-domain	Разрешить ответы с адресом из RFC1918 для доменного имени
	условия: rebind-protection = true

8.3.1. Настройка DNS для 20.x

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. 36. 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.

8.4. Настройка Network Time Protocol (NTP) для irzOS

Раздел NTP предназначен для настройки текущего времени на устройстве.

Этот раздел настраивает сервис протокола сетевого времени (Network Time Protocol, NTP), который отвечает за поддержание точного системного времени на роутере. Точное время является обязательным требованием для корректного ведения журналов, действительной аутентификации по сертификатам и правильного функционирования многих сетевых протоколов.

Роутер может работать в двух различных ролях:

- **NTP-клиент (Синхронизация времени)** - В своей основной роли NTP-клиента роутер синхронизирует собственные часы с внешними, авторитетными серверами времени. Вы указываете эти вышестоящие серверы в списке *Pool*. Роутер будет периодически опрашивать эти серверы, чтобы обеспечить постоянную точность своих внутренних часов.
- **NTP-сервер (Источник времени для локальной сети)** - При включении опции *Server*, роутер сам становится NTP-сервером для вашей локальной сети. Клиентские устройства в локальной сети могут быть настроены на использование IP-адреса роутера в качестве источника времени. Это обеспечивает идеальную синхронизацию всех устройств в вашей локальной сети и сокращает объем NTP-трафика, направляемого в интернет.

Мониторинг статуса синхронизации

Функция **Info** предоставляет доступ к подробной таблице состояния соединений роутера с его вышестоящими NTP-серверами.

КОМАНДЫ

info	Информация о состоянии NTP клиента

СВОЙСТВА

disabled	Выключить конфигурацию
значения: true, false	
pool	Пул серверов для синхронизации
server	Разрешить обрабатывать NTP запросы клиентов
значения: true, false	

8.4.1. Настройка Network Time Protocol (NTP) для 20.x

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!

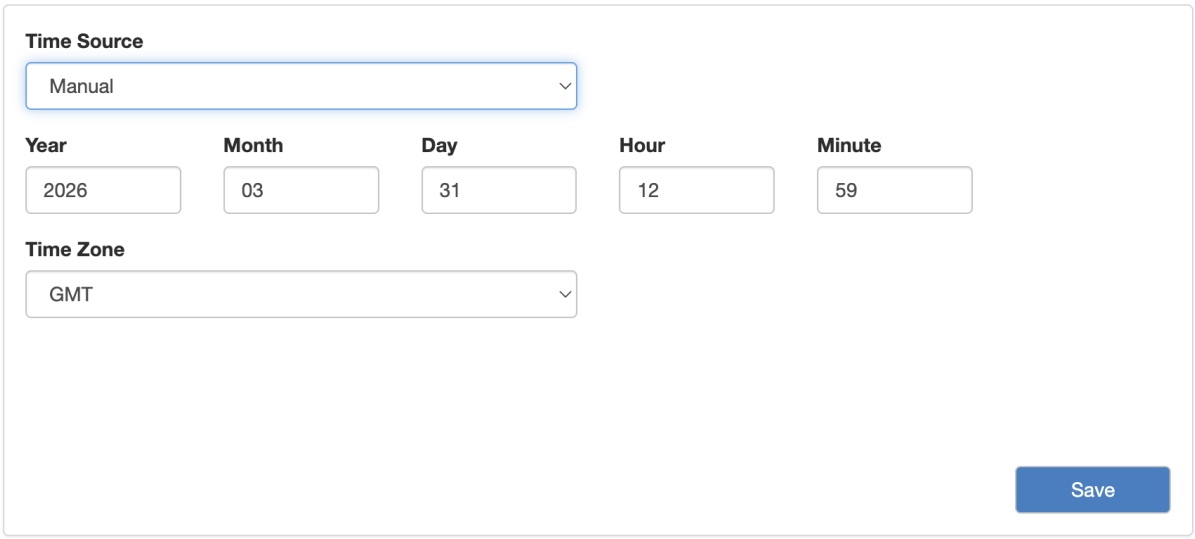


Рис. 37. Настройка времени в ручном режиме

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.

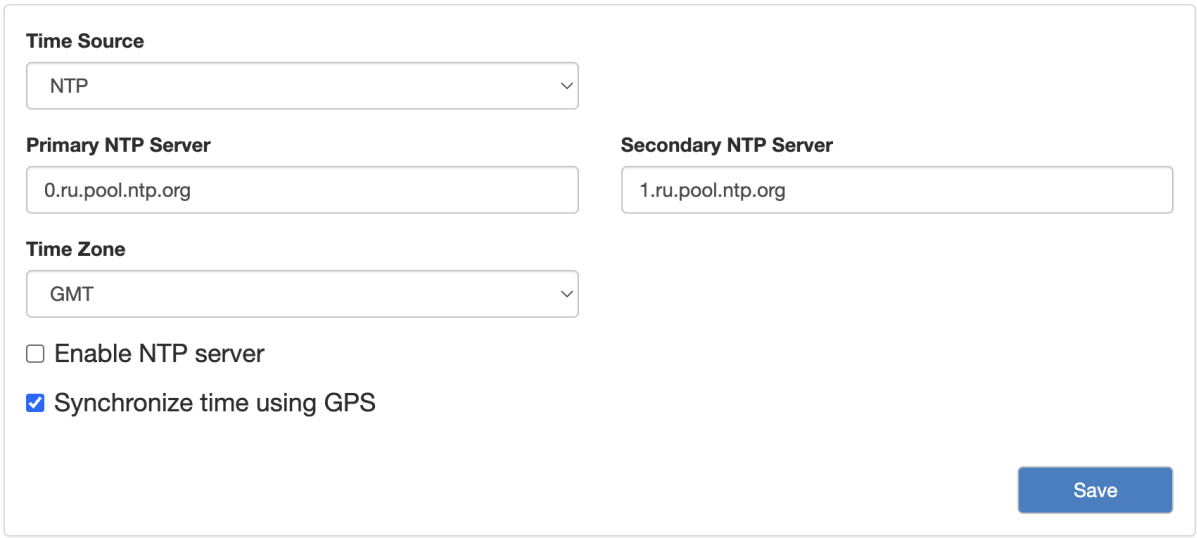


Рис. 38. Настройка времени в автоматическом режиме

Чекбокс **Synchronize time using GPS** включает/отключает синхронизацию системного времени по сигналам навигационных спутников. Данная настройка доступна только для моделей роутеров, оснащенных встроенным модулем **GPS**. Метод обеспечивает точность хода часов независимо от интернет-соединения при условии использования антенны с прямой видимостью небосвода.

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

8.5. Серверы L2TP, OpenVPN, PPTP для irzOS

8.5.1. Настройка профиля клиента (client))

Раздел предназначен для создания списка клиентов и управления учетными данными пользователей для различных VPN и туннельных сервисов, работающих на роутере (например, L2TP, OpenVPN, PPTP).

Вместо того чтобы определять пользователей в конфигурации каждой отдельной службы, эта страница позволяет создать единый профиль пользователя, который может быть связан с определенным сервисом. Это упрощает управление пользователями и обеспечивает согласованность настроек на всей платформе.

Каждый профиль клиента определяется уникальным именем пользователя (*Name*) и паролем для аутентификации. Также можно назначать атрибуты для каждого клиента, такие как определенный статический *IP-адрес туннеля* и пользовательские *Маршруты*, которые будут переданы клиенту при подключении. Это обеспечивает точный контроль доступа, позволяя определять, к каким именно сетевым ресурсам сможет получить доступ каждый удаленный пользователь.

СВОЙСТВА

disabled	Не использовать профиль пользователя
значения: true, false	
service	Сервисы, которыми пользователь может пользоваться
значения: /defaults services	
password	Пароль пользователя
tunnel-ip	IP адрес назначаемый для туннельного интерфейса удалённой стороны
пример: 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	
route	Адреса за удалённой стороной для добавления локального маршрута

8.5.2. Настройка PPTP server

Данный раздел настраивает встроенный сервер PPTP (Point-to-Point Tunneling Protocol). Он позволяет удаленным пользователям устанавливать VPN-туннель для доступа в локальную сеть.

Базовая настройка включает определение собственного IP-адреса сервера внутри туннеля и пула IP-адресов, из которого будут назначаться адреса подключающимся клиентам.

Важнейший выбор конфигурации — это метод **Шифрования**, который определяет уровень безопасности туннеля:

- **IPsec (Рекомендуется для безопасности):** Эта опция инкапсулирует трафик PPTP в защищенный IPsec-туннель. Для упрощения этой сложной настройки роутер **автоматически сгенерирует** необходимую конфигурацию при включении этого режима:
- IPsec-соединение (*pptp_server_connection*) и ассоциацию (*pptp_server_association*) в разделе *Service* / *IPsec*.
- Соответствующее правило межсетевого экрана в *Firewall* / *Filter* (*pptp_server_autogenerated*).

Для корректной работы IPsec-туннеля требуется выполнить действие вручную. После применения настроек вы **должны** перейти в раздел *Service* / *IPsec* / *Connection*, выбрать запись *pptp_server_connection* и настроить метод аутентификации (например, указать Общий ключ / Pre-Shared Key). Соединение не будет работать, пока этот шаг не будет выполнен.

- **MPPE (Microsoft Point-to-Point Encryption):** Предоставляет более простой, интегрированный метод шифрования, который автоматически работает в паре с протоколом аутентификации MS-CHAPv2.
- **None (Без шифрования):** Нешифрованный туннель PPTP. Этот вариант **категорически не рекомендуется** для использования в публичных сетях, так как он не обеспечивает конфиденциальность данных.

Аутентификация пользователей управляется централизованно в разделе *Service* / *Clients*.

При указании диапазона для полей **IP Addresses** и **IP Pool** необходимо учитывать его последующее преобразование в определенный синтаксис. Примеры:

• 1.1.1.2-1.1.1.10 → 1.1.1.2-10

• 1.1.2.3-1.1.5.10 → 1.1.2-5.10 (т.е. от 1.1.2.10 до 1.1.5.10)

СВОЙСТВА

disabled	Выключить конфигурацию
значения: true, false	
ip-addr	IP адрес туннельного интерфейса
ip-pool	Диапазон IP адресов, назначаемых клиентам
auth	Выбор протокола для аутентификации
значения: any, chap, mschap, mschap-v2, pap, eap	**условия:** encryption = mppe
encryption	Метод защиты туннеля
значения: none, mppe	**условия:** /defaults/ipsec_installed = true
psk	Общий PSK ключ для аутентификации и обмена ключами
мин. длина: 8	**условия:** encryption = ipsec
ppp-option	Опции демона протокола Point-to-Point
значения: lcp-echo-failure, lcp-echo-interval, lcp-max-configure, lcp-max-failure, lcp-max-terminate, lcp-restart, ipcp-accept-local, ipcp-accept-remote, ipcp-max-configure, ipcp-max-failure, ipcp-max-terminate, ipcp-restart, mru, mtu	

debug	Режим подробного логгирования
значения: true, false	

8.5.3. Настройка L2TP server

Данный раздел предназначен для настройки встроенного L2TPv2-сервера роутера, это позволяет удаленным пользователям устанавливать безопасные туннели в локальную сеть. Базовая настройка включает в себя определение собственного IP-адреса сервера внутри туннеля и Пула IP-адресов, из которого будут назначаться адреса подключающимся клиентам.

Важнейший выбор конфигурации — это метод шифрования (**Encryption**), который определяет уровень безопасности туннеля:

- **IPsec (Рекомендуется):** Для максимальной безопасности следует использовать L2TP поверх IPsec (*l2tp/ipsec*). При выборе этой опции роутер упрощает конфигурацию, автоматически создавая необходимые IPsec-соединение и правила межсетевого экрана.

После выбора шифрования *ipsec* и применения настроек, вы должны перейти в раздел *Service / IPsec*, чтобы установить **Общий ключ (Pre-Shared Key)** или настроить другой метод аутентификации IPsec для автоматически созданного соединения. Туннель не будет полностью функционировать, пока этот шаг не будет выполнен.

- **MPPE (Microsoft Point-to-Point Encryption):** Это более простой, интегрированный метод шифрования, который автоматически используется в паре с аутентификацией MS-CHAPv2. Он подходит для клиентов, которые не поддерживают IPsec.
- **Без шифрования (None):** Нешифрованный туннель L2TP. Этот вариант категорически не рекомендуется для использования в публичных сетях.

L2TP-сервер будет аутентифицировать клиентов по профилям пользователей, настроенным в разделе *Service / Clients*.

СВОЙСТВА

disabled	Выключить конфигурацию
значения: true, false	
ip-addr	IP адрес туннельного интерфейса
пример: 192.168.1.1	
ip-pool	Диапазон IP адресов, назначаемых клиентам
auth	Выбор протокола для аутентификации
значения: any, chap, mschap, mschap-v2, pap, eap	**условия:** encryption = mppe
encryption	Метод защиты туннеля
значения: none, mppe	**условия:** /defaults/ipsec_installed = true
psk	Общий PSK ключ для аутентификации и обмена ключами
мин. длина: 8	**условия:** encryption = ipsec

ppp-option	Опции демона протокола Point-to-Point
значения: lcp-echo-failure, lcp-echo-interval, lcp-max-configure, lcp-max-failure, lcp-max-terminate, lcp-restart, ipcp-accept-local, ipcp-accept-remote, ipcp-max-configure, ipcp-max-failure, ipcp-max-terminate, ipcp-restart, mru, mtu	
debug	Режим подробного логгирования
значения: true, false	

8.5.4. Настройка OpenVPN server

:software:irzos_web:partial$schema-description/service_OpenVPN-server_schema-description.adoc[]

:software:irzos:partial$cli_tables/service_OpenVPN-server.adoc[]

9. Настройка Firewall

9.1. Настройка Firewall для irzOS

9.1.1. Connections

Данный раздел предоставляет оперативный мониторинг и управление активными сетевыми соединениями, проходящими через роутер. Являясь центральным компонентом системы безопасности роутера, система отслеживания соединений (Connection Tracker) поддерживает информацию о состоянии (stateful) каждого соединения, что позволяет принимать обоснованные решения о разрешении или блокировке трафика.

Раздел предоставляет наглядную информацию о том, какие внутренние устройства устанавливают соединения, с какими внешними IP-адресами и портами они взаимодействуют, а также о текущем состоянии этих соединений. Эта информация позволяет роутеру более эффективно применять правила межсетевого экрана и повышать уровень сетевой безопасности.

КОМАНДЫ

flush	Очистить таблицу conntrack

СВОЙСТВА

source	Адрес источника
destination	Адрес назначения
protocol	Протокол, инкапсулированный в IP
timeout	Интервал, через который сетевое соединение будет удалёно
tcp-state	Текущее состояние TCP соединения
mark	Метка пакета
pkts	Количество пакетов переданных через соединение (исходящих/входящих)
bytes	Количество байт переданных через соединение (исходящих/входящих)

9.1.2. Defaults

В данном разделе определяются глобальные политики межсетевого экрана, действующие по умолчанию. Эти правила решают, что делать с любым сетевым пакетом, который не подошел ни под одно из более конкретных правил, созданных пользователем. Базовые политики имеют самый низкий приоритет и анализируются только после обработки всех остальных специфичных правил.

Конфигурация применяется к трем основным цепочкам:

- **INPUT:** Контролирует трафик, предназначенный для локальных процессов самого роутера, например, административный доступ (HTTPS, SSH), ответы ICMP или терминирование VPN-туннелей.
- **OUTPUT:** Контролирует трафик, генерируемый самим роутером, например, DNS-запросы, запросы NTP-клиента или трафик, инициированный утилитами мониторинга соединений.

- **FORWARD:** Контролирует транзитный трафик, проходящий через роутер между различными сетевыми интерфейсами или зонами, например, пересылку пакетов из зоны LAN в зону WAN.

СВОЙСТВА

input	Политика по умолчанию для входящего трафика
значения: accept, drop	
output	Политика по умолчанию для исходящего трафика
значения: accept, drop	
forward	Политика по умолчанию для пересылаемого (проходящего) трафика
значения: accept, drop	
drop-invalid	Откидывать неидентифицированные пакеты
значения: true, false	
syn-flood	Зашита от SYN Flood атак
значения: true, false	
syn-flood-rate	Допустимый порог количества TCP SYN пакетов в секунду
	условия: syn-flood = true
syn-flood-burst	Допустимый мгновенный всплеск количества TCP SYN пакетов
	условия: syn-flood = true
tcp-syncookies	Использовать TCP SYN cookies для противодействия TCP SYN flood
значения: true, false	
tcp-ecn	Использовать ECN (явное уведомление о перегруженности)
значения: true, false	
tcp-window-scaling	Масштабирование TCP окна
значения: true, false	
use-conntrack	Механизм отслеживания соединений (conntrack)
значения: true, false	
flow-offloading	Механизм разгрузки потока (Flow offloading)
значения: true, false	

9.1.3. Filter

Раздел предназначен для настройки основных разрешающих и блокирующих правил, т.е.фильтрации трафика.

Этот раздел предназначен для настройки основного набора правил фильтрации пакетов. Эти пользовательские правила обеспечивают точный контроль над всем трафиком — как транзитным, так и адресованным непосредственно роутеру, и составляют основу политики сетевой безопасности.

Каждое правило состоит из определенных критериев соответствия — таких как зоны источника и назначения, IP-адреса, протоколы и порты — и заданного целевого действия (**ACCEPT**, **DROP** или **REJECT**). Межсетевой экран анализирует эти правила в последовательном порядке. Действие над пакетом определяется первым правилом, которому он соответствует, после чего дальнейшая обработка этого пакета прекращается.

Пакеты, которые не соответствуют ни одному правилу в этом списке, будут обработаны общими политиками, настроенными в подразделе «Defaults». Этот механизм позволяет создавать исключения из общей политики безопасности, разрешая работу определенных служб и соединений.

КОМАНДЫ

reset-counters	Сброс счётчиков
reorder	Изменить позицию объекта

СВОЙСТВА

disabled	Отключить правило файрвола
значения: true, false	
chain	Цепочка правил таблицы
значения: input, forward, output	
src	Источник трафика (интерфейс или зона)
значения: /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	**условия:** chain = output
src-addr	IP адрес источника трафика
пример: 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	
dst	Назначение трафика (интерфейс или зона)
значения: /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	**условия:** chain = input
dst-addr	IP адрес получателя трафика
пример: 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	
protocol	Сопоставление по имени протокола
значения: dccp, ddp, egp, eigrp, encap, esp, etherip, ggp, gre, hmp, icmp, idpr-cmtp, idrp, igmp, igp, ip, ipcomp, ipencap, ipip, isis, iso-tp4, l2tp, ospf, pim, pup, rdp, rspf, rsvp, sctp, skip, st, tcp, udp, vmtp, vrrp, xns-idp, xtp, all	

icmp-type	Сопоставление по типу ICMP пакета
значения: address-mask-reply, host-redirect, pong, time-exceeded, address-mask-request, host-unknown, port-unreachable, timestamp-reply, any, host-unreachable, precedence-cutoff, timestamp-request, communication-prohibited, ip-header-bad, protocol-unreachable, TOS-host-redirect, destination-unreachable, network-prohibited, redirect, TOS-host-unreachable, echo-reply, network-redirect, required-option-missing, TOS-network-redirect, echo-request, network-unknown, router-advertisement, TOS-network-unreachable, fragmentation-needed, network-unreachable, router-solicitation, ttl-exceeded, host-precedence-violation, parameter-problem, source-quench, ttl-zero-during-reassembly, host-prohibited, ping, source-route-failed, ttl-zero-during-transit	**условия:** protocol = icmp
mark	Сравнение по метке пакета
пример: 16, !453	
action	Действие над трафиком, попавшим под правило
значения: accept, reject, drop	
policy	Сопоставление для IPSec трафика
значения: dir, pol, strict, reqid, spi, proto, mode, tunnel-src, tunnel-dst	
extra	Специальные аргументы (поддержка синтаксиса iptables)
пример: -m mac --mac-source FE:FF:FF:FF:FF:FF	

9.1.4. Mangle

Данный раздел позволяет создавать правила для изменения определенных атрибутов IP-пакетов до того, как они будут обработаны системами маршрутизации или фильтрации. Основная функция таблицы Mangle — это классификация и маркировка пакетов. Эти метки не разрешают и не блокируют трафик напрямую, а служат внутренними идентификаторами для других подсистем роутера.

Этот функционал необходим для реализации расширенных сетевых функций, таких как:

- **Маршрутизация на основе политик (PBR):** Направление маркированных пакетов через определенные WAN-интерфейсы или VPN-туннели в обход основной таблицы маршрутизации.
- **Качество обслуживания (QoS):** Приоритизация или ограничение полосы пропускания для потоков трафика на основе их меток.

Кроме того, правила Mangle могут использоваться для прямого изменения полей IP-заголовка, таких как DSCP (для классификации QoS) или TTL (Время жизни).

КОМАНДЫ

reset-counters	Сброс счётчиков
reorder	Изменить позицию объекта

СВОЙСТВА

disabled	Отключить правило файрвола
значения: true, false	

chain	Цепочка правил таблицы
значения: prerouting, input, forward, output, postrouting	
src	Источник трафика (интерфейс или зона)
значения: /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	**условия:** chain = output chain = postrouting
src-addr	IP адрес источника трафика
пример: 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	
dst	Назначение трафика (интерфейс или зона)
значения: /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	**условия:** chain = input chain = prerouting
dst-addr	IP адрес получателя трафика
пример: 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	
protocol	Сопоставление по имени протокола
значения: dccp, ddp, egp, eigrp, encap, esp, etherip, ggp, gre, hmp, icmp, idpr-cmtp, idrp, igmp, igp, ip, ipcomp, ipencap, ipip, isis, iso-tp4, l2tp, ospf, pim, pup, rdp, rspf, rsvp, sctp, skip, st, tcp, udp, vmtp, vrrp, xns-idp, xtp, all	
icmp-type	Сопоставление по типу ICMP пакета
значения: address-mask-reply, host-redirect, pong, time-exceeded, address-mask-request, host-unknown, port-unreachable, timestamp-reply, any, host-unreachable, precedence-cutoff, timestamp-request, communication-prohibited, ip-header-bad, protocol-unreachable, TOS-host-redirect, destination-unreachable, network-prohibited, redirect, TOS-host-unreachable, echo-reply, network-redirect, required-option-missing, TOS-network-redirect, echo-request, network-unknown, router-advertisement, TOS-network-unreachable, fragmentation-needed, network-unreachable, router-solicitation, ttl-exceeded, host-precedence-violation, parameter-problem, source-quench, ttl-zero-during-reassembly, host-prohibited, ping, source-route-failed, ttl-zero-during-transit	**условия:** protocol = icmp
mark	Сравнение по метке пакета
пример: 16, !453	
action	Действие над трафиком, попавшим под правило
значения: accept, dscp, mark, tcpmss, ttl	**условия:** chain = input
set-mark	Метка, которую следует установить для пакета
минимум: 0, **максимум:** 4294967295	**условия:** action = mark
set-dscp	Указать DiffServ класс в поле DSCP для приоретизации трафика
значения: cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, be, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, ef	**условия:** action = dscp
set-mss	Установить значение MSS в пакете TCP SYN
значения: clamp-mss-to-pmtu	**условия:** action = tcpmss

set-ttl	Изменить значение TTL в пакете
пример: 1, 255, +1, -1	**условия:** action = ttl
policy	Сопоставление для IPSec трафика
значения: dir, pol, strict, reqid, spi, proto, mode, tunnel-src, tunnel-dst	
extra	Специальные аргументы
пример: -m mac --mac-source FE:FF:FF:FF:FF:FF	

9.1.5. NAT

Данный раздел используется для настройки правил трансляции сетевых адресов (Network Address Translation, NAT). Эти правила модифицируют IP-адрес и/или порт источника и назначения в пакетах, проходящих через роутер. NAT является основной функцией для управления трафиком между приватными и публичными сетями.

Доступны следующие действия:

- **ACCEPT:** Явно отключает NAT для трафика, соответствующего правилу. Используется для создания исключений — например, чтобы предотвратить трансляцию адресов для трафика, направленного в определенный VPN-туннель или другую приватную сеть.
- **SNAT:** Транслирует IP-адрес источника в конкретный, статически заданный IP-адрес. Это действие обычно используется, когда WAN-интерфейс роутера имеет статический публичный IP-адрес.
- **Masquerade:** Динамически транслирует IP-адрес источника в текущий IP-адрес исходящего интерфейса. Это стандартное и рекомендуемое действие для интерфейсов с динамическими IP-адресами, например, для сотовых (LTE) или DHCP-подключений.

КОМАНДЫ

reset-counters	Сброс счётчиков
reorder	Изменить позицию объекта

СВОЙСТВА

disabled	Отключить правило файрвола
значения: true, false	
chain	Цепочка правил таблицы
значения: prerouting, postrouting, output	
src	Источник трафика (интерфейс или зона)
значения: /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	**условия:** chain = postrouting
src-addr	IP адрес источника трафика
пример: 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	

dst	Назначение трафика (интерфейс или зона)
значения: /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	**условия:** chain = prerouting
dst-addr	IP адрес получателя трафика
пример: 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	
protocol	Сопоставление по имени протокола
значения: dccp, ddp, egp, eigrp, encap, esp, etherip, ggp, gre, hmp, icmp, idpr-cmtp, idrp, igmp, igp, ip, ipcomp, ipencap, ipip, isis, iso-tp4, l2tp, ospf, pim, pup, rdp, rspf, rsvp, sctp, skip, st, tcp, udp, vmtp, vrrp, xns-idp, xtp, all	
icmp-type	Сопоставление по типу ICMP пакета
значения: address-mask-reply, host-redirect, pong, time-exceeded, address-mask-request, host-unknown, port-unreachable, timestamp-reply, any, host-unreachable, precedence-cutoff, timestamp-request, communication-prohibited, ip-header-bad, protocol-unreachable, TOS-host-redirect, destination-unreachable, network-prohibited, redirect, TOS-host-unreachable, echo-reply, network-redirect, required-option-missing, TOS-network-redirect, echo-request, network-unknown, router-advertisement, TOS-network-unreachable, fragmentation-needed, network-unreachable, router-solicitation, ttl-exceeded, host-precedence-violation, parameter-problem, source-quench, ttl-zero-during-reassembly, host-prohibited, ping, source-route-failed, ttl-zero-during-transit	**условия:** protocol = icmp
mark	Сравнение по метке пакета
пример: 16, !453	
action	Действие над трафиком, попавшим под правило
	условия: chain = output chain = prerouting chain = postrouting
nat-addr	Преобразовать адрес попавшего под правила пакета
пример: 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	**условия:** chain = output && action = dnat chain = prerouting && action = dnat chain = postrouting && action = snat
redirect-port	Транслировать попавшие под правило пакеты на указаный порт
пример: 80, !80	**условия:** chain = output && action = redirect chain = prerouting && action = redirect
policy	Сопоставление для IPSec трафика
значения: dir, pol, strict, reqid, spi, proto, mode, tunnel-src, tunnel-dst	
extra	Специальные аргументы
пример: -m mac --mac-source FE:FF:FF:FF:FF:FF	

9.1.6. RAW

В этом разделе настраиваются правила в таблице Raw — самой первой точке обработки на пути следования пакетов в межсетевом экране. Правила здесь оперируют «сырыми» пакетами до того, как они передаются в систему отслеживания соединений с состоянием (conntrack).

Основное назначение этой таблицы — находить определенные потоки трафика и применять к ним действие **NOTRACK**, которое указывает межсетевому экрану полностью пропустить инспекцию этих пакетов с отслеживанием состояния. Это может быть необходимо для:

- **Сценариев с высокой производительностью:** Чтобы снизить нагрузку на процессор и память роутера при обработке чрезвычайно высокой интенсивности трафика без отслеживания состояния.
- **Совместимости с протоколами:** Для обработки протоколов, которые по своей природе несовместимы с инспекцией состояний или с трансляцией сетевых адресов (NAT).

Пакеты, помеченные *NOTRACK*, не обрабатываются механизмом межсетевого экрана, отслеживающим состояния. Следовательно, к ним не могут применяться правила, основанные на состоянии (например, *RELATED*, *ESTABLISHED*), и они несовместимы со стандартным функционалом NAT. Эту функцию следует использовать с четким пониманием ее последствий для безопасности.

КОМАНДЫ

reset-counters	Сброс счётчиков
reorder	Изменить позицию объекта

СВОЙСТВА

disabled	Отключить правило файрвола
значения: true, false	
chain	Цепочка правил таблицы
значения: output, prerouting	
src	Источник трафика (интерфейс или зона)
значения: /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	**условия:** chain = output
src-addr	IP адрес источника трафика
пример: 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	
dst	Назначение трафика (интерфейс или зона)
значения: /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	**условия:** chain = prerouting
dst-addr	IP адрес получателя трафика
пример: 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	
protocol	Сопоставление по имени протокола
значения: dccp, ddp, egp, eigrp, encap, esp, etherip, ggp, gre, hmp, icmp, idpr-cmtp, idrp, igmp, igp, ip, ipcomp, ipencap, ipip, isis, iso-tp4, l2tp, ospf, pim, pup, rdp, rspf, rsvp, sctp, skip, st, tcp, udp, vmtp, vrrp, xns-idp, xtp, all	

icmp-type	Сопоставление по типу ICMP пакета
значения: address-mask-reply, host-redirect, pong, time-exceeded, address-mask-request, host-unknown, port-unreachable, timestamp-reply, any, host-unreachable, precedence-cutoff, timestamp-request, communication-prohibited, ip-header-bad, protocol-unreachable, TOS-host-redirect, destination-unreachable, network-prohibited, redirect, TOS-host-unreachable, echo-reply, network-redirect, required-option-missing, TOS-network-redirect, echo-request, network-unknown, router-advertisement, TOS-network-unreachable, fragmentation-needed, network-unreachable, router-solicitation, ttl-exceeded, host-precedence-violation, parameter-problem, source-quench, ttl-zero-during-reassembly, host-prohibited, ping, source-route-failed, ttl-zero-during-transit	**условия:** protocol = icmp
action	Действие над трафиком, попавшим под правило
значения: accept, drop, notrack	
extra	Специальные аргументы
пример: -m mac --mac-source FE:FF:FF:FF:FF:FF	

9.1.7. Zone

Данный раздел предназначен для создания и определения зон межсетевого экрана. Зоны — это логические контейнеры для классификации источников и назначений трафика, которые служат основными элементами для построения политик безопасности. Принадлежность к зоне определяется ее типом конфигурации:

- **Зона на основе интерфейсов:** Связывает зону с одним или несколькими сетевыми интерфейсами (например, *eth0*, *br-lan*, *tun0*). Весь трафик, входящий или исходящий через выбранный интерфейс, считается частью этой зоны. Это стандартный метод для сегментации физических или логических сетевых сегментов.
- **Зона на основе адресов:** Определяет зону по списку IP-адресов, подсетей в нотации CIDR или диапазонов IP-адресов. Трафик считается частью этой зоны, если его IP-адрес источника или назначения соответствует записи в списке, независимо от физического интерфейса, через который он проходит. Это позволяет создавать политики, независимые от топологии сети.

После создания эти зоны могут использоваться в качестве источника и назначения для построения политики безопасности.

СВОЙСТВА

type	Тип набора
значения: interface, address	
entry	Участники набора
	условия: type = interface type = address

9.2. Настройка Firewall для 20.x

9.2.1. 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!

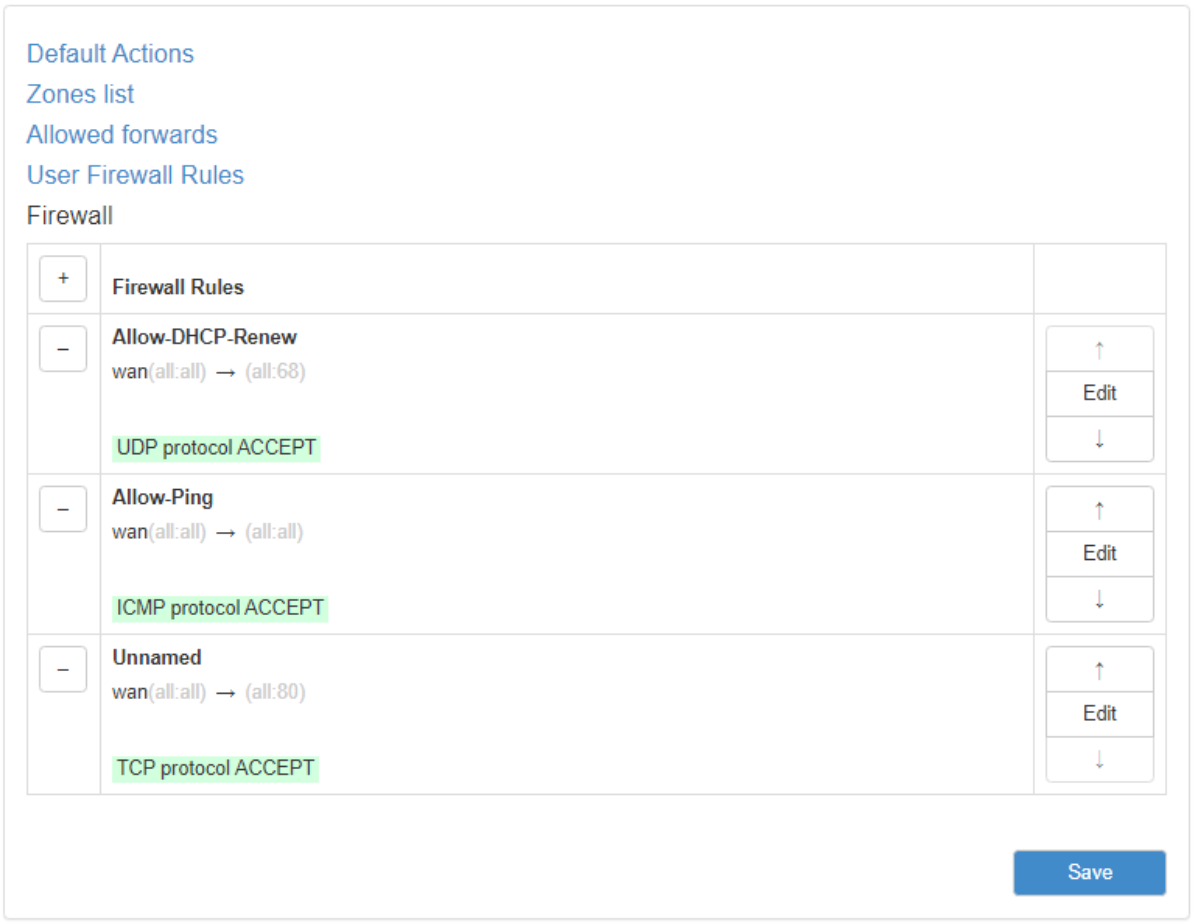


Рис. 39. Вкладка Services, раздел Firewall

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.

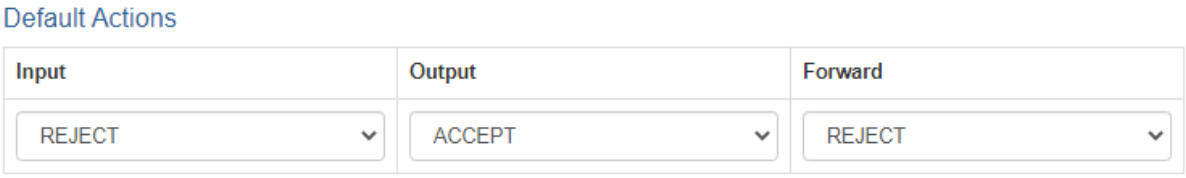


Рис. 40. Вкладка Services, раздел Firewall, настройки Default Actions

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 20. 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

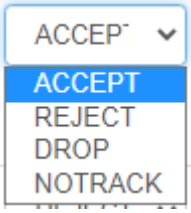


Рис. 41. Вариант выбора действий для трафика

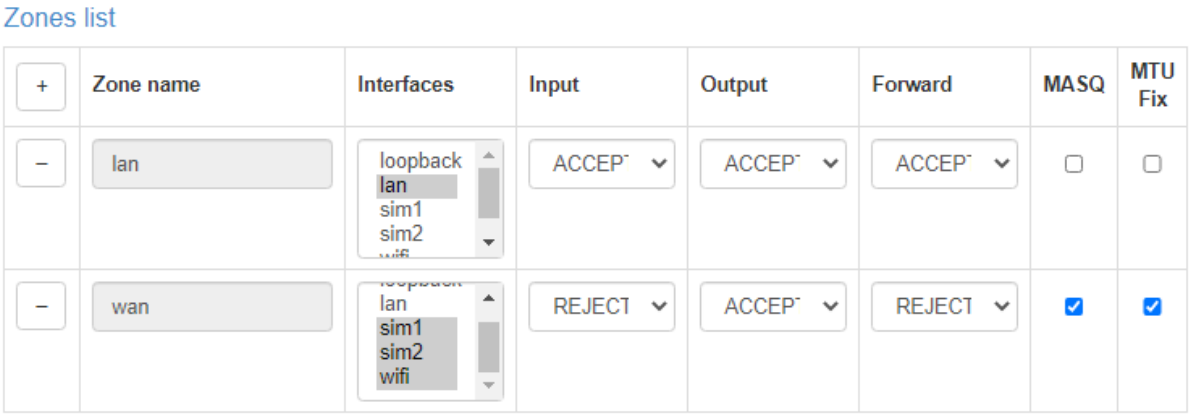


Рис. 42. Вкладка Services, раздел Firewall, настройки Zones List

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.

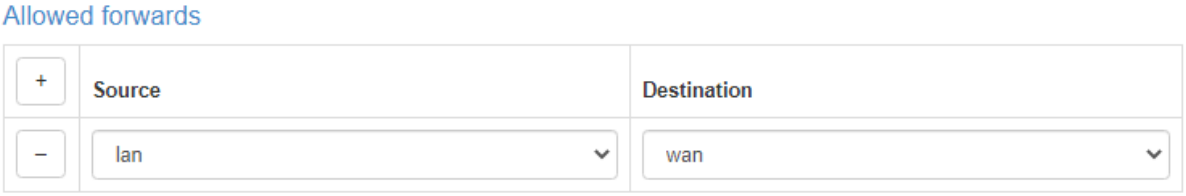


Рис. 43. Настройки Allowed Forwards

Таблица 21. 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.

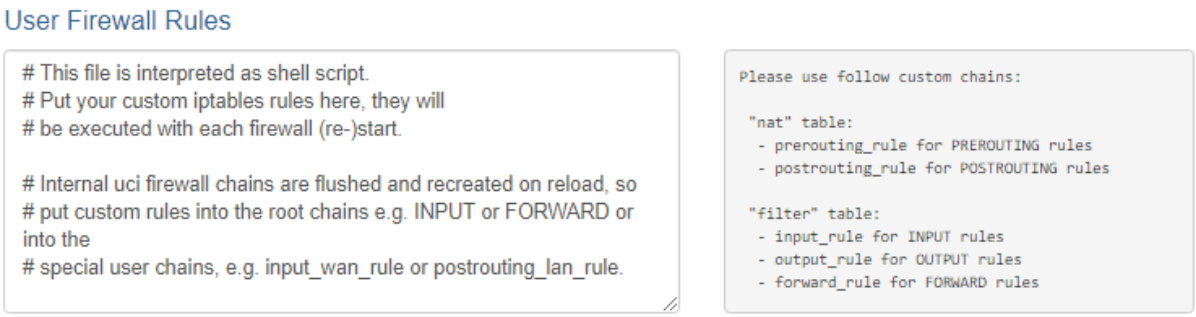


Рис. 44. Вкладка Services, раздел Firewall, настройки User Firewall Rules

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 ↑ ↓

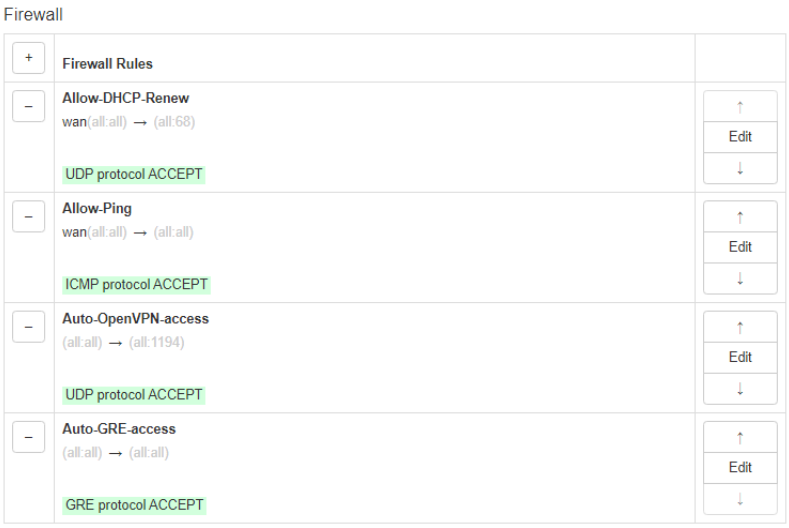


Рис. 45. Настройки Firewall

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.

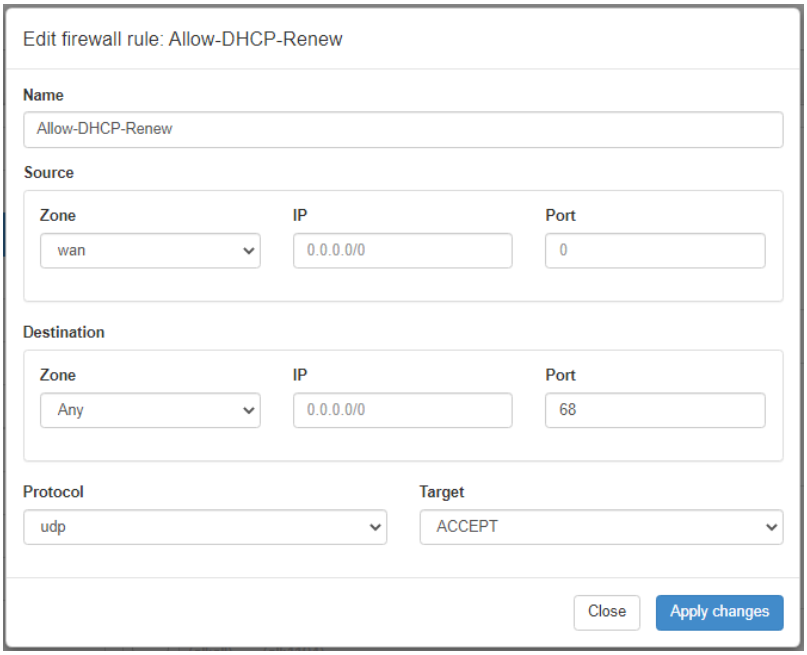


Рис. 46. Редактирование правила Firewall

Таблица 22. 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 CIDR: 0.0.0.0/0. Например, “192.168.0.25/29” означает, что правило распространяется на подсеть адресов сети с маской 29: 192.168.0.25 - 192.168.0.30. 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. В случае если выбран протокол "all" ввод номера порта блокируется
Protocol	Выбор протокола, на который будет распространяться правило
Target	Выбор действия для трафика: **Accept** – принимать, **Reject** – отклонять, **Drop** – отбрасывать, **Notrack** – не отслеживать, **DSCP** – маркировать трафик для того чтобы к нему можно применять правила QoS (раздел **Services** – **Queues**)

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

9.2.2. MAC Filter

Раздел Wireless ACL 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!

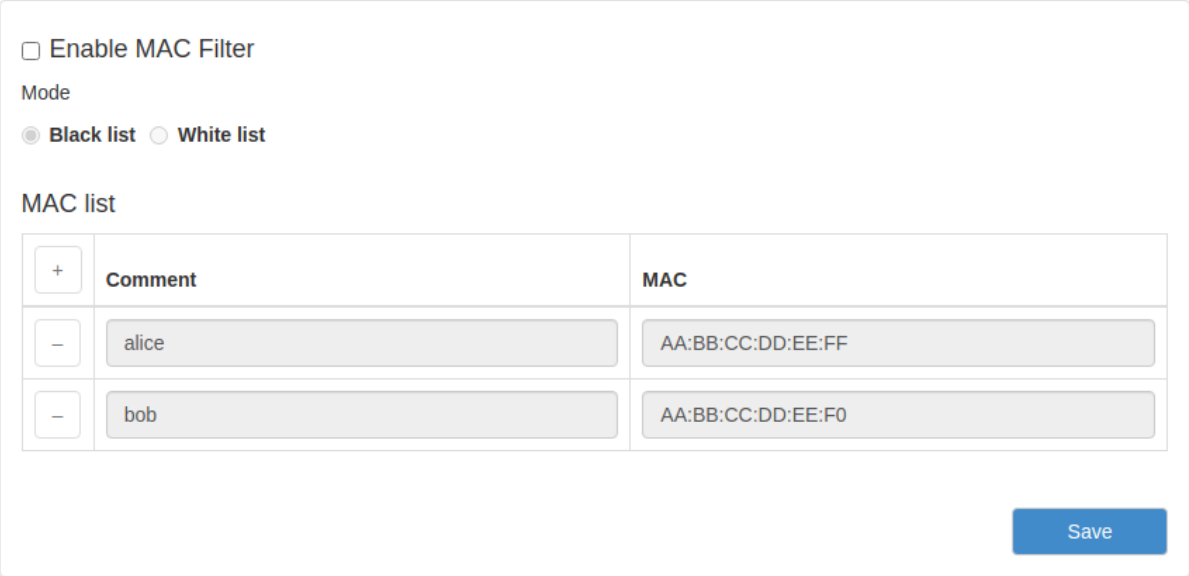


Рис. 47. Вкладка Services, раздел Wireless ACL

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 **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.

9.2.3. 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!

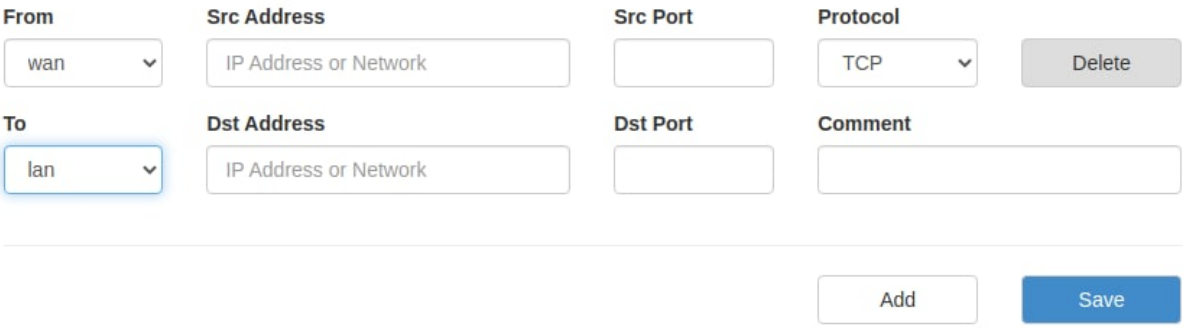


Рис. 48. Вкладка Services, раздел Port Forwarding

Таблица 23. Настройки правил проброса портов

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

10. Информационные ресурсы

Для предоставления пользователям информации об использовании ПО на официальном сайте компании выкладывается документация и ведется база знаний.

- **Официальная документация по irzOS**

Краткое руководство по настройке irzOS
https://docs.irz.net/irzos_quick_manual

Интерфейс командной строки irzOS
https://docs.irz.net/irzos_cli_manual

Руководство по установке irzOS
https://docs.irz.net/irzos_install_manual

- **Официальная документация для 20.x**

Руководство по настройке 20.x
https://docs.irz.net/controls_main

Настройка туннелей 20.x
https://docs.irz.net/tuneling

- **База Знаний для всех версий ПО**

https://faq.irz.net

Содержит разбор конкретных сценариев использования irzOS и 20.x и способах устранения часто встречающихся ошибок при их использовании.

11. Контакты технической поддержки

Новые версии прошивок, документации и сопутствующего программного обеспечения можно получить, обратившись по следующим контактам:

Санкт-Петербург

Сайт компании в Интернете	www.radiofid.ru
Тел. в Санкт-Петербурге	+7 (812) 318 18 19
e-mail	support@radiofid.ru
Telegram	@irzhelpbot

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

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

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

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