Руководство по WEB-интерфейсу
NETOS 19

Версия документа 1.1

СОДЕРЖАНИЕ

1 Введение

1.1 Описание документа

Данный документ является общим для всех роутеров MICRODRIVE и содержит информацию только по настройке и управлению устройствами посредством WEB-интерфейса. Для получения информации о работе самих устройств смотрите соответствующие руководства на эти устройства.

Таблица 1.1. История версий документа

Версия документа	Дата изменения	Изменения
1.0	20.12.2022	Первая версия
1.1	05.05.2023	Добавлено описание GRE туннелей

1.2 Подключение к WEB-интерфейсу

Для доступа к настройкам роутера через WEB-интерфейс нужно выполнить действия, описанные ниже.

Шаг 1. Установите физическое подключение с устройством – кабелем через порт Ethernet или через беспроводную сеть Wi-Fi (при наличии). Пароль от Wi-Fi сети указан на наклейке роутера.
Шаг 2. Откройте интернет-браузер и введите в адресную строку IP-адрес **«192.168.1.1»**.

Не рекомендуется использовать браузер **Internet Explorer**.

Шаг 3. Откроется форма входа в WEB-интерфейс (рис.1.2). Если пароль не установлен, нажмите **«ВОЙТИ»** (по умолчанию логин – **root**, пароль – не задан).

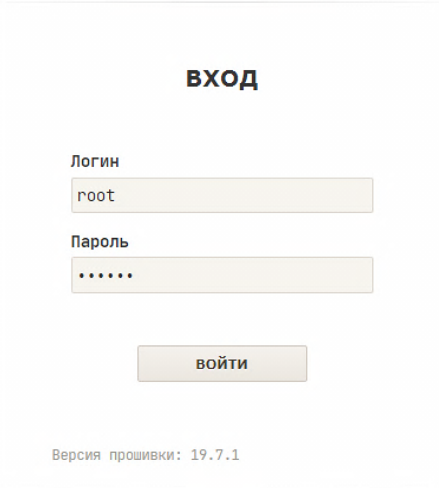


Рис.1.2. Форма входа

1.3 Сброс на заводские настройки

Для того чтобы сбросить роутер на заводские настройки, можно воспользоваться одним из трех способов.

Способ 1. Сброс кнопкой **«SET».**
Зажмите кнопку **«SET»** и удерживайте в течение 10 секунд. Роутер сбросит настройки и перезагрузится.

Способ 2. Сброс через меню в WEB-интерфейсе.
Зайдите в меню ***«Система → Прошивка»***. Нажмите кнопку **«ВЫПОЛНИТЬ СБРОС»**. Роутер сбросит настройки и перезагрузится.

Способ 3. Сброс с помощью программы **«restorer»** по проводному интерфейсу Ethernet.
Данный способ следует использовать, если нет физического доступа к кнопке «**SET»** устройства и нет подключения к WEB-интерфейсу. Запустите программу **«restorer»** и следуйте инструкции.

2 Меню «Статус»

2.1 Статус – Обзор

В меню представлены основные параметры устройства. Параметры сгруппированы в несколько подразделов (рис.2.1) – **«Система»**, **«Модем 3G/LTE»**, **«Интернет»**, **«Wi-Fi 2.4 ГГц»** и **«Ethernet»**.

Описание параметров представлено в таблице 2.1.

Система

Имя хоста	MICRODRIVE
Модель	Tandem-4GX
Время работы	1h 47m 32s
Локальное время	07:28:11 17 Aug 2022
Использовано RAM	17 MB / 58 MB
Средняя загрузка	0.09 / 0.07 / 0.03
Версия прошивки	19.7.1

Модем 3G/LTE

SIM-карта	**SIM1:** READY
Регистрация	REGISTERED, HOME
Уровень сигнала	-81 дБм / 52%
Диапазон	LTE B7 + B3
Оператор	"ROSTELECOM" / 25020
Статус соединения	Подключен: **1h 56m 29s**

Интернет

Тип	MOBILE
Интерфейс	modem
Адрес	100.79.74.132/29
Шлюз	100.79.74.133
DNS 1	95.167.167.95
DNS 2	95.167.167.96
Статус соединения	Подключен: **1h 59m 45s**

Wi-Fi 2.4 ГГц

Радио	10 канал; 20 МГц
Точка доступа 1	Активна (клиентов: 1)
Точка доступа 2	-
Wi-Fi Клиент	-

Ethernet

Порт 0	100M; Full-duplex
Порт 1	-

Рис.2.1. Меню «Статус – Обзор»

Таблица 2.1. Описание полей «Система, Модем 3G/LTE, Интернет, Wi-Fi 2G, Ethernet»

№	Название поля	Описание
Система		
1	Имя хоста	Символьное имя сетевого устройства.
2	Модель	Наименование модели устройства.
3	Время работы	Время работы устройства с момента включения. Обнуляется после перезагрузки.
4	Локальное время	Отображает текущую время и дату в соответствии с установленным часовым поясом.
5	Использовано RAM	Использовано оперативной памяти / Всего оперативной памяти.
6	Средняя загрузка	Средняя загрузка процессора за 1, 5, 15 мин.
7	Версия прошивки	Версия прошивки.
Модем 3G/LTE		
1	SIM-карта	Отображается текущий номер SIM-слота и статус SIM-карты.
2	Регистрация	Статус регистрации в сети оператора. Возможные значения: **NOT REGISTERED** – не зарегистрирован; **REGISTERED, HOME** – зарегистрирован в домашней сети; **REGISTERED, ROAMING** – зарегистрирован в сети другого оператора; **REGISTRATION DENIED** – в регистрации отказано; **NOT REGISTERED, SEARCHING...** – не зарегистрирован, поиск нового оператора.
3	Уровень сигнала	Уровень сигнала мобильной сети (параметр RSSI).
4	Диапазон	Технология доступа (2G, 3G, LTE) и частотный диапазон или частотные диапазоны, если используется агрегация.
5	Оператор	Имя мобильного оператора и код PLMN оператора.
6	Статус соединения	Статус и время подключения к Интернету по мобильной сети.
Интернет		
1	Тип	Тип интерфейса, через который доступен Интернет. Например, MOBILE, WIRELESS, ETHERNET и т.д.
2	Интерфейс	Имя интерфейса, через который доступен Интернет.
3	Адрес	IP-адрес и маска подсети на интерфейсе.
4	Шлюз	IP-адрес шлюза, через который будет проходить Интернет-трафик.
5	DNS 1	IP-адрес первого DNS сервера.
6	DNS 2	IP-адрес второго DNS сервера.
7	Статус соединения	Статус подключения к Интернету через указанный интерфейс.
Wi-Fi 2.4G *(только для устройств оснащенных Wi-Fi)*		
1	Радио	Отображается уровень выходной мощности приемопередатчика, номер частотного канала и ширина канала (20МГц или 40МГЦ).
2	Точка доступа 1	Статус первой беспроводной сети (SSID1) и количество подключенных клиентов к этой сети.
3	Точка доступа 2	Статус второй беспроводной сети (SSID2) и количество подключенных клиентов к этой сети.
4	Wi-Fi Клиент	Статус подключения к внешней точке доступа Wi-Fi в режиме клиента. См. настройку в меню ***«Сеть → Wi-Fi → Клиент».***
Ethernet		
1	Порт <номер порта>	Режим работы Ethernet-портов. Возможные значения: **10M** – 10 Мбит/сек; **100M** – 100 Мбит/сек; **1000M** – 1 Гбит/сек; **Full-duplex** – полнодуплексный режим; **Half-duplex** – полудуплексный режим.

2.1 Статус – Интерфейсы

2.2.1 Статус – Интерфейсы – Обзор

В меню ***«Статус → Интерфейсы → Обзор»*** отображается состояние активных интерфейсов (рис.2.2.1). С помощью кнопок **«СОЕДИНИТЬ»** и **«ОСТАНОВИТЬ»** можно управлять состоянием интерфейса. Интерфейс отображается, если он включен в соответствующем разделе **«Сеть»**. Описание параметров представлено в таблице 2.2.1.

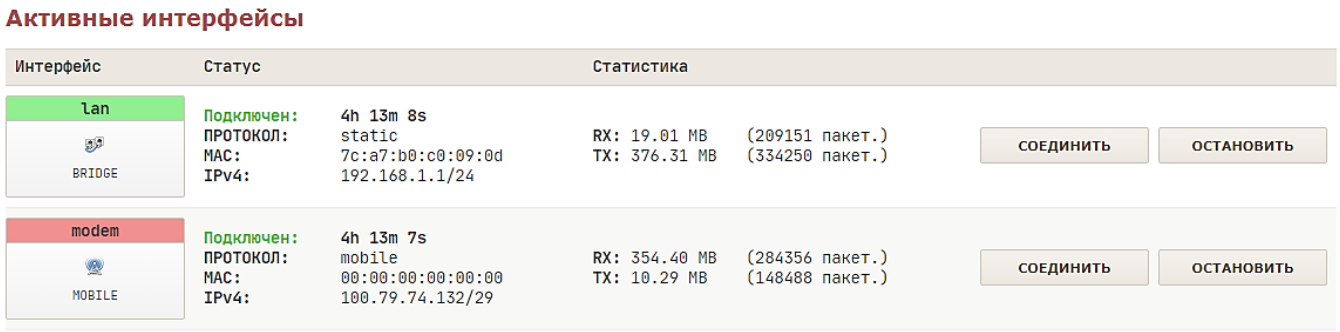


Рис.2.2.1. Меню «Статус – Интерфейсы – Обзор»

Таблица 2.2.1. Описание полей «Активные интерфейсы»

№	Название поля	Описание
Активные интерфейсы		
1	Интерфейс	Имя и тип интерфейса.
2	Статус	Статус интерфейса. Возможные значения: **Подключен** – интерфейс активен и способен передавать/принимать трафик в соответствующую сеть; **Остановлен** – интерфейс остановлен. Трафик передаваться не может; **Подключение…** - интерфейс остановлен, но идет процесс подключения. Трафик передаваться не может. Протокол – имя протокола, с помощью которого происходит управление интерфейсом, включая способ назначения IP-параметров (IP-адрес, шлюз, DNS и т.д.). Возможные значения: **static** – параметры IP будут назначены в соответствии с настройками интерфейса; **DHCP** – параметры IP будут назначены автоматически по протоколу DHCP; **mobile** – параметры IP будут назначены автоматически. Доступно только для интерфейсов, соответствующих типу MOBILE. Параметры IP выдает оператор мобильной связи в соответствии с тарифным планом; **l2tp, ovpn и другие** – параметры IP будут назначаться в соответствии с настройками VPN интерфейса. MAC – Физический адрес интерфейса. Может быть 00:00:00:00:00:00, если интерфейс работает только в сетевом режиме и не поддерживает передачу кадров 802.3. **IPv4** – IP-адрес и префикс (маска подсети) назначенный интерфейсу.
3	Статистика	RX - Объем трафика (количество пакетов) принятого через интерфейс. TX - Объем трафика (количество пакетов) переданного через интерфейс.

2.2.2 Статус – Интерфейсы – <*Имя интерфейса*>

В меню «***Статус → Интерфейсы → <Имя интерфейса>***» отображаются детальные параметры интерфейса (IP-адрес, IP-адрес шлюза, DNS, статистика) и в виде графиков текущая скорость передачи данных (рис.2.2.2).

Описание параметров представлено в таблице 2.2.2.

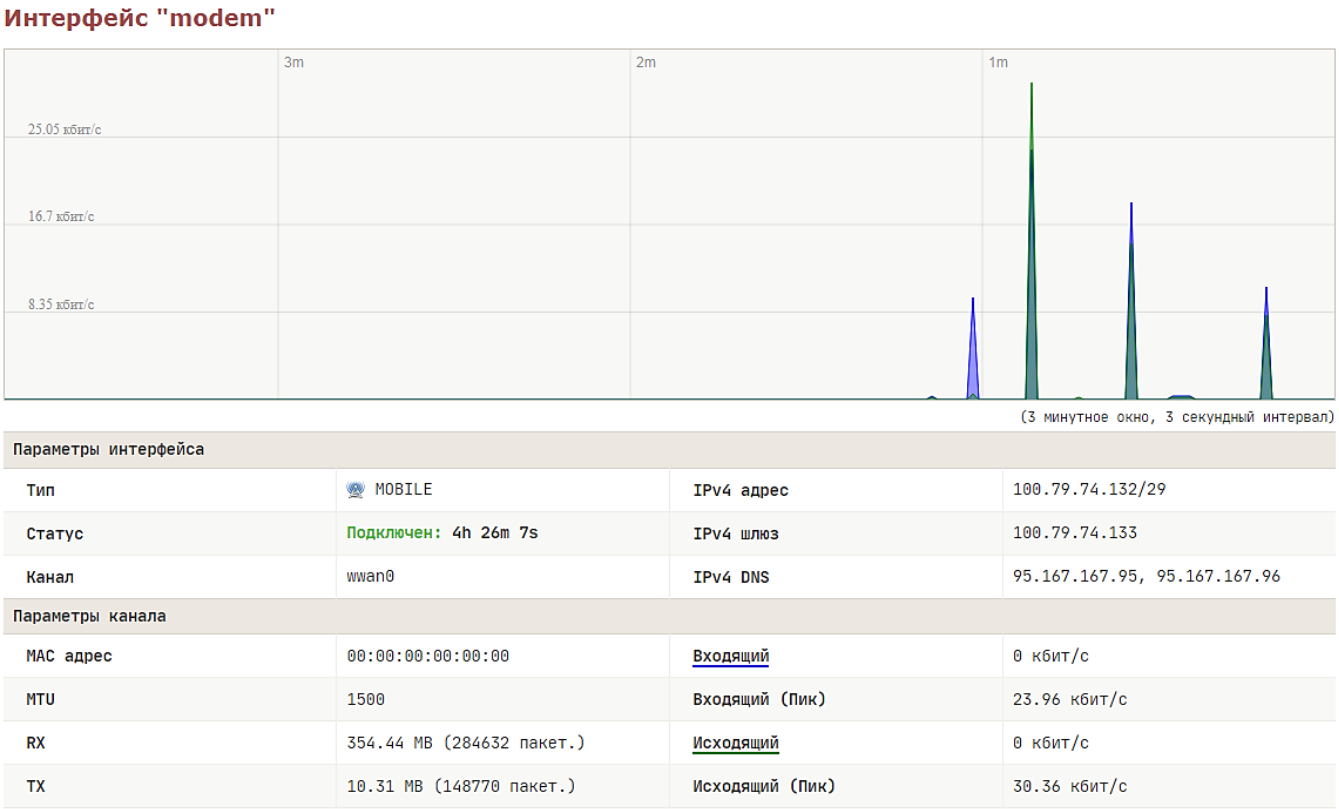


Рис.2.2.2. Меню «Статус – Интерфейсы – modem». Пример параметров интерфейса «modem»

Таблица 2.2.2. Описание полей «Интерфейс <Имя интерфейса>»

№	Название поля	Описание
Интерфейс <Имя интерфейса>		
1	Тип	Тип интерфейса. Например, MOBILE, WIRELESS, ETHERNET и т.д.
2	Статус	Статус интерфейса. Возможные значения: **Подключен** – интерфейс активен и способен передавать/принимать трафик в соответствующую сеть; **Остановлен** – интерфейс остановлен. Трафик передаваться не может; **Подключение…** - интерфейс остановлен, но идет процесс подключения. Трафик передаваться не может.
3	Канал	Имя канала (физический интерфейс).
4	IPv4 адрес	IP-адрес и маска подсети на интерфейсе. IP-адрес интерфейса может быть назначен автоматически или через соответствующие настройки.
5	IPv4 шлюз	IP-адрес шлюза, на который будет отправляться/приниматься весь трафик через указанный интерфейс. IP-адрес шлюза может быть назначен автоматически или через соответствующие настройки.
6	IPv4 DNS	IP-адрес первого и второго DNS-сервера. IP-адреса DNS-серверов могут быть назначены автоматически или через соответствующие настройки.
7	MAC адрес	Физический адрес интерфейса. Может быть 00:00:00:00:00:00, если интерфейс работает только в сетевом режиме и не поддерживает передачу кадров IEEE 802.3.
8	MTU	**M**aximum **T**ransmission **U**nit. Максимальный размер (в байтах) полезного блока данных одного пакета, который может быть передан интерфейсом без фрагментации.
9	RX	Объем трафика (количество пакетов) принятого через интерфейс.
10	TX	Объем трафика (количество пакетов) переданного через интерфейс.
11	Входящий	Скорость входящего трафика.
12	Входящий (Пик)	Пиковая скорость входящего трафика в 3-х минутном интервале.

13	Исходящий	Скорость исходящего трафика.
14	Исходящий (Пик)	Пиковая скорость исходящего трафика в 3-х минутном интервале.

2.3 Статус – Модем

2.3.1 Статус – Модем – Обзор

В меню представлены параметры 3G/LTE модема, параметры мобильной сети и статус мобильного подключения (рис. 2.3.1). Кнопки **«SIM1»** и **«SIM2»** предназначены для оперативного выбора соответствующей SIM-карты (только для моделей с 2-мя SIM-слотами). Описание параметров представлено в таблице 2.3.1.

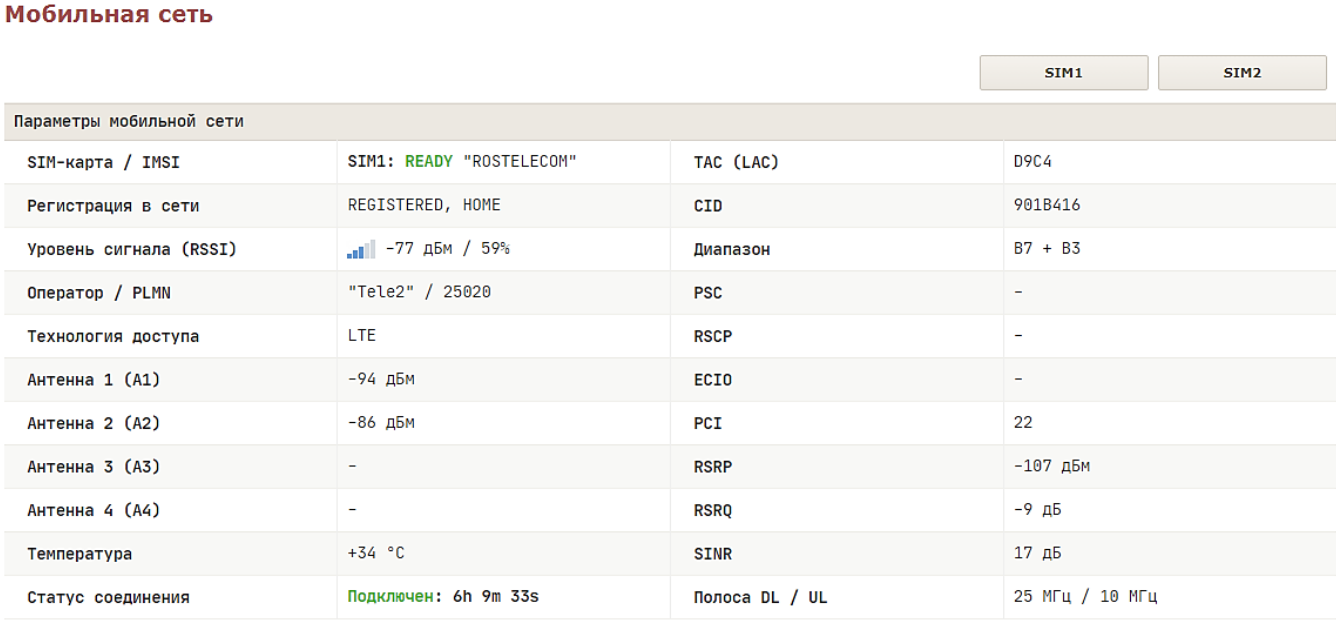


Рис.2.3.1. Меню «Статус – Модем – Обзор»

Таблица 2.3.1. Описание полей «Мобильная сеть»

№	Название поля	Описание
Мобильная сеть		
1	SIM-карта	Отображается текущий номер SIM-слота и статус SIM-карты. Дополнительно выводится имя провайдера SIM-карты.
2	Регистрация в сети	Статус регистрации в сети оператора. Возможные значения: **NOT REGISTERED** – не зарегистрирован; **REGISTERED, HOME** – зарегистрирован в домашней сети; **REGISTERED, ROAMING** – зарегистрирован в сети другого оператора; **REGISTRATION DENIED** – в регистрации отказано; **NOT REGISTERED, SEARCHING...** – не зарегистрирован, поиск нового оператора.
3	Уровень сигнала (RSSI)	Уровень сигнала мобильной сети. Для LTE, уровень сигнала в главной соте.
4	Оператор / PLMN	Имя мобильной сети, в которой зарегистрировалось устройство.
5	Технология доступа	Технология доступа к мобильной сети. Возможные значения: **LTE** – сеть четвертого поколения LTE/4G; **3G** – сеть третьего поколения WCDMA/UMTS; **2G** – сеть второго поколения EDGE/GSM/GPRS.
6	Антенна 1 (A1)	Уровень сигнала на антенном порту A1. Уровень сигнала относится к главной соте.
7	Антенна 2 (A2)	Уровень сигнала на антенном порту A2. Уровень сигнала относится к главной соте. Значение может отсутствовать, если сота или модем LTE не поддерживают режим MIMO.
8	Антенна 3 (A3)	Уровень сигнала на антенном порту A3. Уровень сигнала относится к главной соте. Значение может отсутствовать, если сота или модем LTE не поддерживают режим MIMO.
9	Антенна 4 (A4)	Уровень сигнала на антенном порту A4. Уровень сигнала относится к главной соте. Значение может отсутствовать, если сота или модем LTE не поддерживают режим MIMO.
10	Температура	Температура модуля LTE.
11	Статус соединения	Статус и время подключения по мобильной сети.
12	TAC (LAC)	Код локации БС (LAC) для сетей 3G. Код зоны отслеживания (TAC) для сетей LTE.
13	Диапазон	Частотные диапазоны главной и вспомогательных сот (если устройство поддерживает агрегацию). Используется международное обозначение диапазонов. Например, B3 – это BAND 3 или 1800 МГц. Информацию о сотах можно получить в меню ***«Статус → Модем → Соты LTE».***

14	PSC	**P**rimary **S**crambling **C**odes - код скремблирования (только для сетей 3G).
15	RSCP	Мощность принятого сигнала (только для сетей 3G) .
16	ECIO	Отношение несущая/шум (только для сетей 3G) .
17	PCI	**P**hysical **L**ayer **C**ell **I**dentifier – идентификатор соты (только для сетей LTE). Параметр относится к главной соте. Информацию о сотах можно получить в меню ***«Статус → Модем → Соты LTE».***
18	RSRP	Среднее значение мощности принятых пилотных сигналов (только для сетей LTE). Параметр относится к главной соте.
19	RSRQ	Качество принятых пилотных сигналов (только для сетей LTE) . Параметр относится к главной соте.
20	SINR	Значение сигнал/шум (только для сетей LTE). Параметр относится к главной соте.
21	Полоса DL / UL	Суммарная полоса пропускания для входящего/исходящего трафика с учетом агрегации частотных диапазонов главной и второстепенных сот (только сетей для LTE).

2.3.2 Статус – Модем – Соты LTE

В меню отображаются параметры сот LTE, доступных модулю связи. Первая сота в списке – главная сота. Пример списка сот показан на рис. 2.3.2.

Описание параметров сот представлено в таблице 2.3.2.

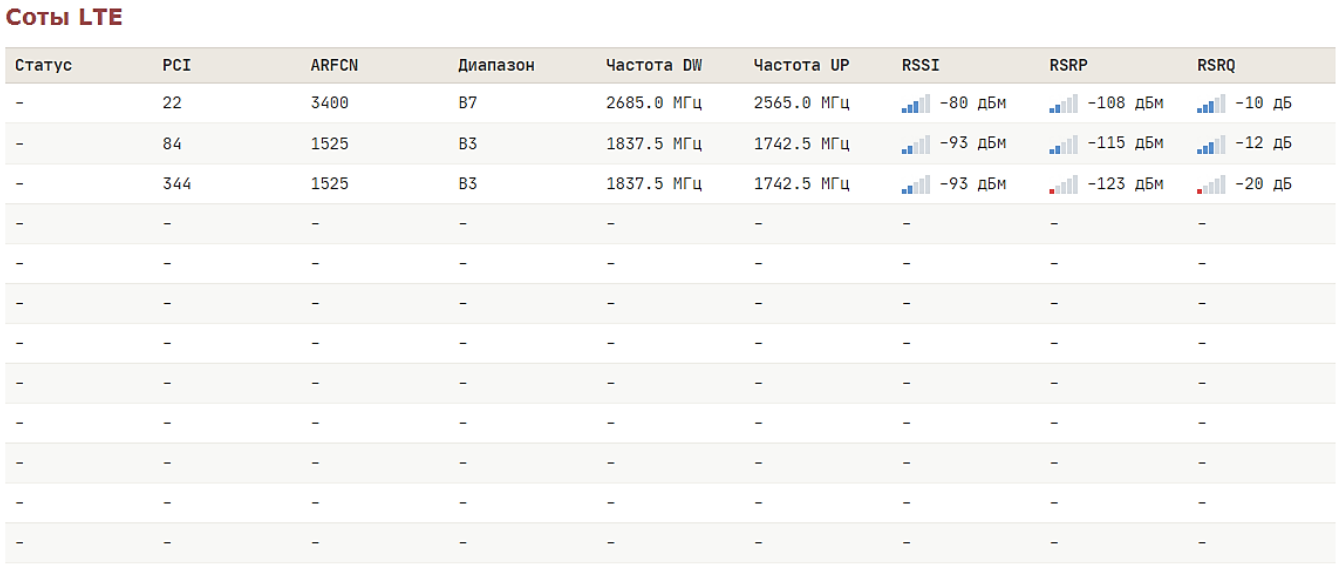


Рис.2.3.2. Меню «Статус – Модем – Соты LTE»

Таблица 2.3.2. Описание полей «Соты LTE»

№	Название поля	Описание
Соты LTE		
1	Статус	Зарезервировано.
2	PCI	**P**hysical **L**ayer **C**ell **I**dentifier – физический идентификатор соты.
3	ARFCH	Код частотного канала в соответствии с международным стандартом. Фактически обозначает частоту, на которой работает сота. Соты с одинаковым значением работают на одной частоте.
4	Диапазон	Условное обозначение частотного диапазона в соответствии с международным стандартом.
5	Частота DW	Частота, на которой передаются данные от БС к устройству. Параметр вычисляется из ARFCH.
6	Частота UP	Частота, на которой передаются данные от устройства к БС. Параметр вычисляется из ARFCH.
7	RSSI	Общий уровень сигнала в соте.
8	RSRP	Среднее значение мощности принятых пилотных сигналов в соте.
9	RSRQ	Качество принятых пилотных сигналов в соте.

2.3.3 Статус – Модем – AT-команды

В меню реализована возможность обмена AT-командами с LTE модулем. Пример обмена AT-командами показан на рис. 2.3.3.

Отправка некоторых AT-команд может привести к некорректной работе устройства.
Использовать с осторожностью!

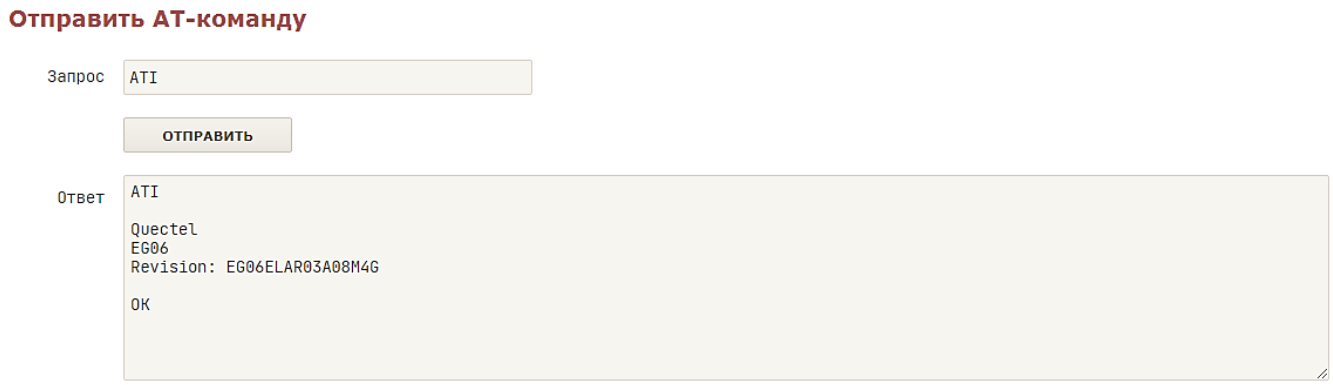


Рис.2.3.3. Меню «Статус – Модем – AT-команды». Пример обмена AT-командами

2.3.4 Статус – Модем – Отправить USSD

В меню реализована возможность обмена USSD командами. Отправка команд доступна только для LTE модулей, поддерживающих эту функцию. Список USSD команд уточняйте на сайте оператора. Для отправки запросов требуется, что бы устройство было зарегистрировано в голосовой сети. Пример обмена USSD командами показан на рис. 2.3.4.

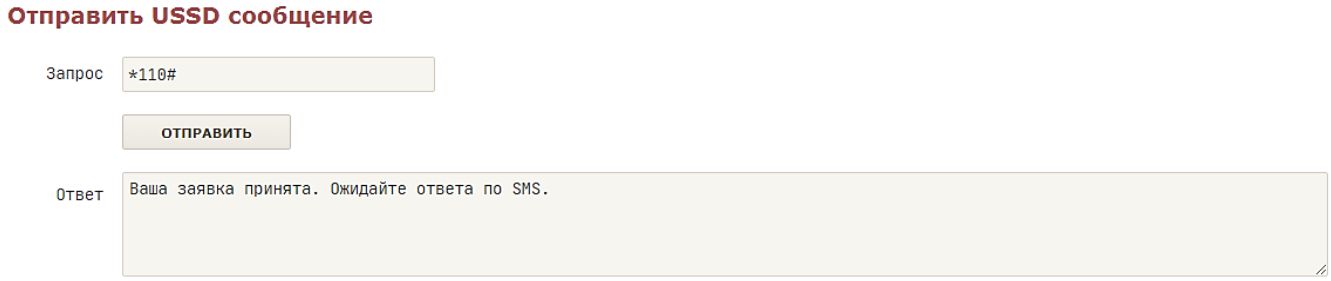


Рис.2.3.4. Меню «Статус – Модем – Отправить USSD». Пример обмена USSD

2.3.5 Статус – Модем – Отправить SMS

В меню реализована возможность отправки SMS сообщений на международные и местные мобильные номера включая короткие номера. Для отправки сообщений требуется, что бы устройство было зарегистрировано в голосовой сети, а тарифный план должен включать возможность отправки SMS. Пример отправки SMS сообщения показан на рис.2.3.5.

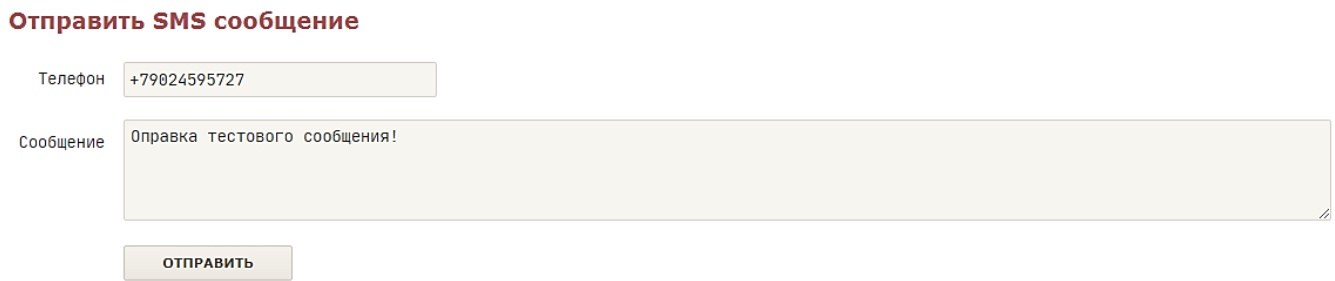


Рис.2.3.5. Меню «Статус – Модем – Отправить SMS». Пример отправки SMS

2.3.6 Статус – Модем – Читать SMS

В меню выводится список входящих SMS сообщений, полученных LTE-модемом. Во избежание переполнения памяти, более «старые» сообщения автоматически удаляются. В верхнем левом углу, параметр **«Память»** показывает свободную память, доступную память и тип памяти для хранения SMS сообщений. Значение **«ME»** указывается на то, что SMS сообщения будут сохраняться во внутренней памяти LTE-модема. Кнопка **«ОБНОВИТЬ»** предназначена для обновления списка SMS сообщений. Кнопка **«УДАЛИТЬ ВСЕ»** предназначена для удаления всех SMS сообщений. Пример чтения входящих SMS показан на рис. 2.3.6.

Рис.2.3.6. Меню «Статус – Модем – Читать SMS». Пример чтения входящих SMS сообщений

2.3.7 Статус – Модем – Поиск сетей

В меню реализована возможность выполнить поиск мобильных сетей (операторов). Поиск сетей инициируется при нажатии кнопки **«СКАНИРОВАТЬ»**. Интерфейс **«modem»** должен быть остановлен или выключен (меню ***«Статус → Интерфейсы»***). Время сканирования не более 60 секунд. На результат поиска влияют выбранные частотные диапазоны, таким образом, можно выполнить поиск сетей в необходимом частотном диапазоне. В результате работы функции будет выведена таблица с найденными мобильными сетями. Кнопки **«SIM1/SIM2»** предназначены для ручного выбора мобильной сети. При нажатии на кнопку **«SIM1»** или **«SIM2»**, устройство попытается подключиться к сети, а значение PLMN сохранится в соответствующем параметре в меню ***«Сеть → Modem → Общие → SIM1/SIM2 → PLMN».*** Для возврата в автоматический режим удалите этот параметр. Результат поиска представлен на рис. 2.3.7.

Описание параметров представлено в таблице 2.3.7.

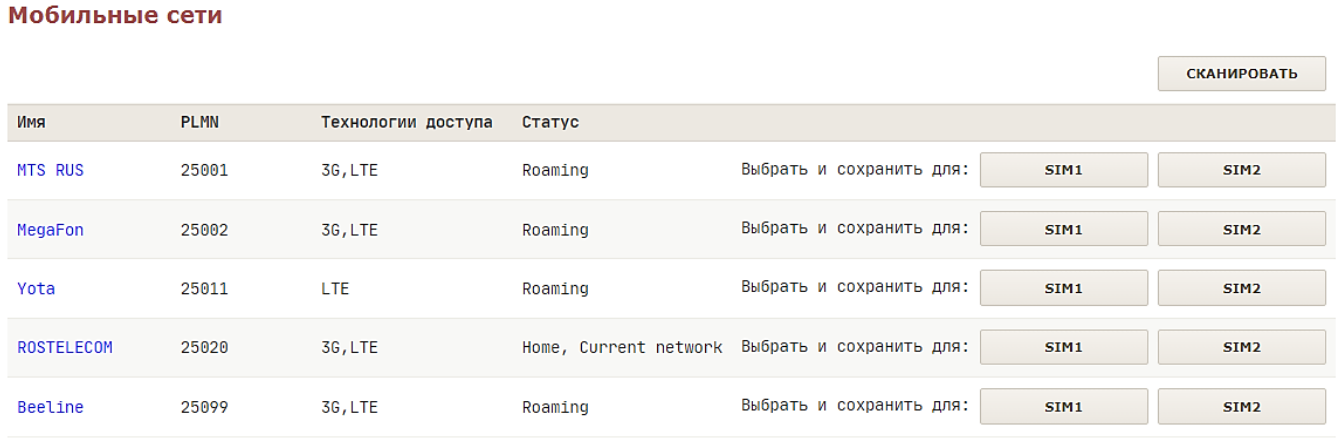


Рис.2.3.7. Меню «Статус – Модем – Поиск сетей»

Таблица 2.3.7. Описание полей «Мобильные сети»

№	Название поля	Описание
Мобильные сети		
1	Имя	Имя мобильной сети.
2	PLMN	Уникальный международный идентификатор мобильного оператора, первые 3 цифры обозначают код страны, последние 2 или 3 код оператора.
3	Технологии доступа	Поддерживаемые мобильным оператором технологии доступа.
4	Статус	Статус регистрации устройства в сети оператора.

2.3.8 Статус – Модем – Информация

В меню представлена информация о модеме и SIM-карте (рис. 2.3.8). Описание параметров представлено в таблице 2.3.8.

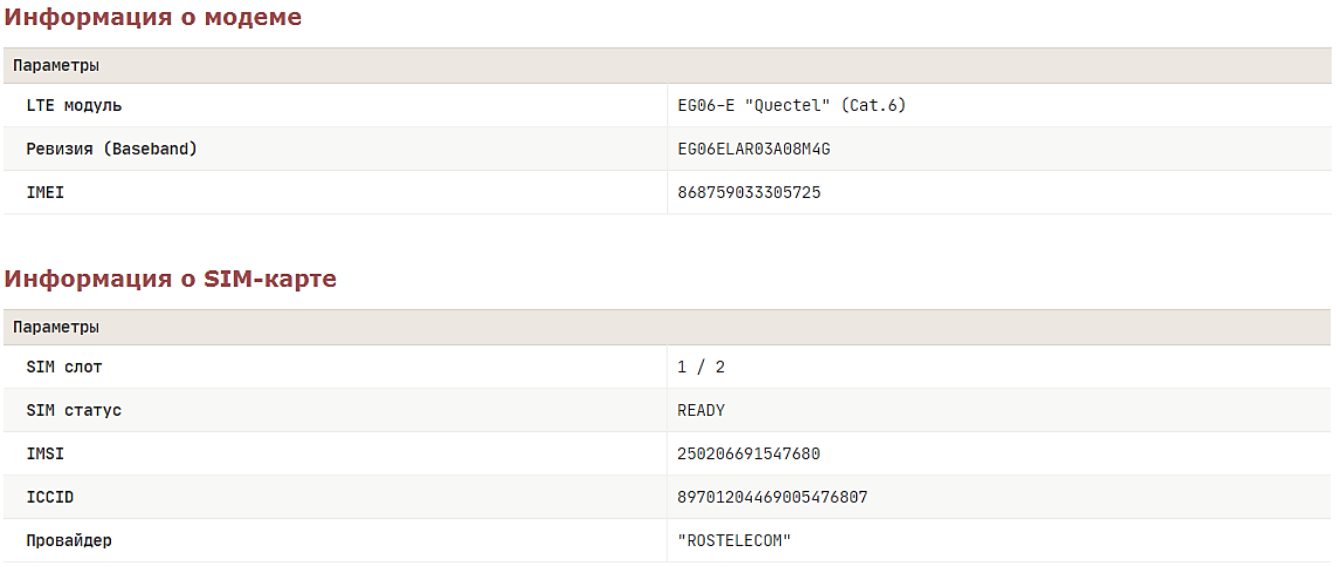


Рис.2.3.8. Меню «Статус – Модем – Информация»

Таблица 2.3.8. Описание полей «Информация о модеме, Информация о SIM-карте»

№	Название поля	Описание
Информация о модеме		
1	LTE модуль	Краткое описание используемого модуля связи.
2	Ревизия (Baseband)	Ревизия программного обеспечения модуля связи.
3	IMEI	Международный идентификатор мобильных устройств.
Информация о SIM-карте		
1	SIM слот	Текущий SIM-слот/Всего SIM-слотов.
2	SIM статус	Статус SIM-карты. Возможные значения: **READY** – инициализация SIM-карты прошла успешно; **ABSENT** – ошибка инициализации или SIM-карта отсутствует.
3	IMSI	Международный идентификатор мобильного абонента.
4	ICCID	Уникальный международный идентификатор SIM-карты.
5	Провайдер	Имя провайдера, выпустившего SIM-карту.

2.4 Статус – Wi-Fi

Меню доступно только для устройств, оснащенных Wi-Fi приемопередатчиком.

2.4.1 Статус – Wi-Fi – Обзор

В меню представлены основные параметры радиоканала 2.4 ГГц и параметры беспроводных сетей (рис.2.4.1). Большинство параметров настраиваются в меню ***«Сеть → Wi-Fi»***.

SSID1 и **SSID2** – беспроводные сети, работающие в режиме **«Wi-Fi точка доступа»**. **Wi-Fi клиент** – беспроводная сеть, работающая в режиме **«Клиент»**.

Описание параметров представлено в таблице 2.4.1.

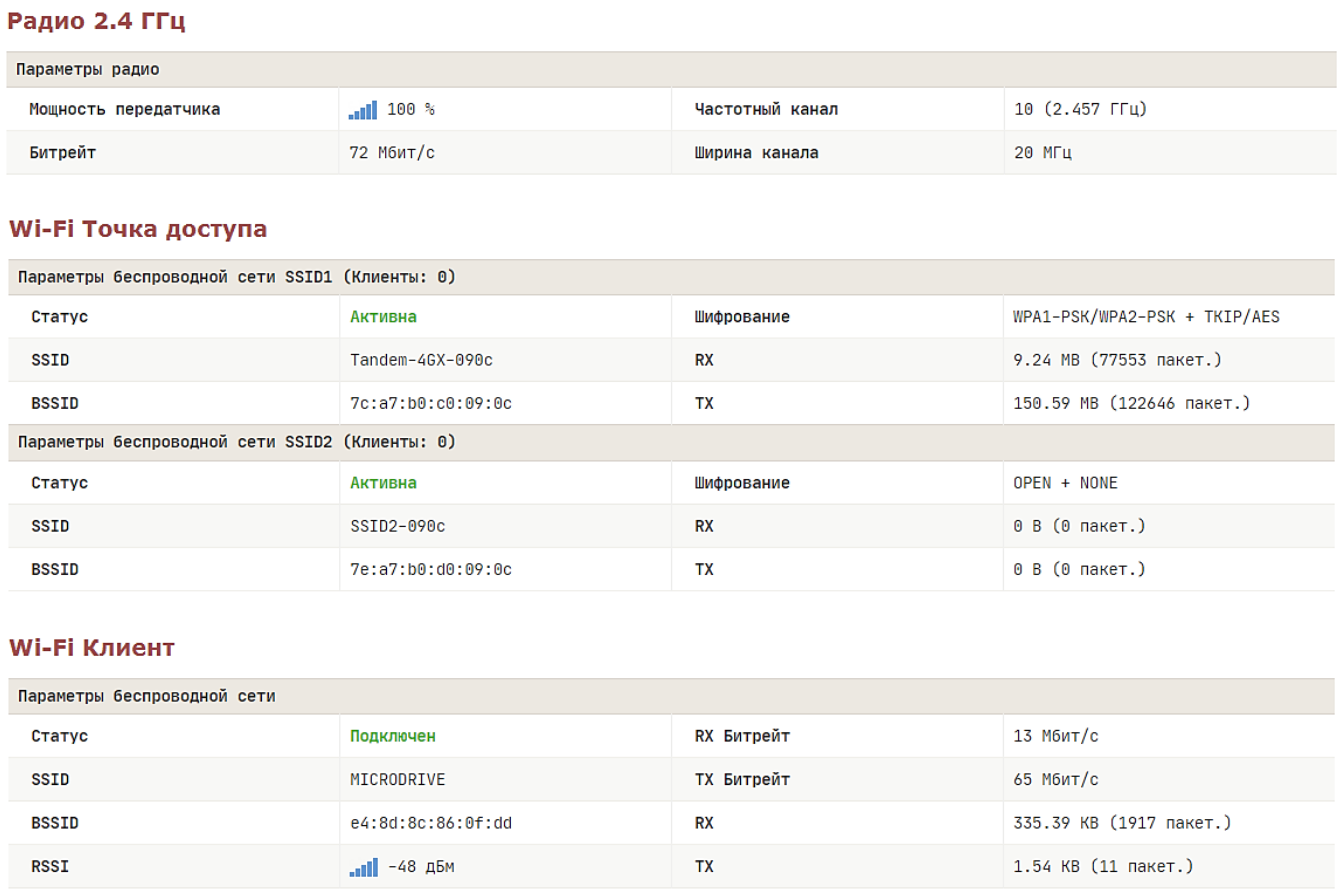


Рис.2.4.1. Меню «Статус – Wi-Fi – Обзор». Пример работы SSID1, SSID2 и режим клиента

Таблица 2.4.1. Описание полей «Радио 2.4 ГГц, Wi-Fi Точка доступа, Wi-Fi Клиент»

№	Название поля	Описание
Радио 2.4 ГГц		
1	Мощность передатчика	Выходная мощность передатчика.
2	Битрейт	Максимальная битовая скорость физического радиоканала на прием и передачу данных. Значение зависит от ширины канала, количества передающих/принимающих антенн и стандарта связи. Типовые значения: 20 МГц + одна антенна – 72 Мбит/с; 40 МГц + одна антенна – 150 Мбит/с; 20 МГц + 2 антенны – 150 Мбит/с; 40 МГц + 2 антенны – 300 Мбит/с.
3	Частотный канал	Номер частотного канала и частота.
4	Ширина канала	Полоса пропускания. Возможные значения: **20 МГц** – один частотный канал; **40 МГц** – 2 частотных канала.
Wi-Fi Точка доступа		
1	Статут	Статус беспроводной сети. Возможные значения: **Отключено** – сеть остановлена;

		Активна – сеть готова к работе.
2	SSID	Имя беспроводной сети. Задается в меню ***«Сеть → Wi-Fi → SSID1/SSID2»***.
3	BSSID	Физический адрес беспроводной сети.
4	Шифрование	Метод аутентификации и шифрования. Задается в меню ***«Сеть → Wi-Fi → SSID1/SSID2»***.
5	RX	Объем трафика, принятого через беспроводную сеть.
6	TX	Объем трафика, переданного через беспроводную сеть.
Wi-Fi Клиент		
	Статут	Статус беспроводной сети в режиме клиента. Возможные значения: **Отключено** – сеть остановлена; **Подключение** – идет подключение к внешней точке доступа; **Подключен** – установлено подключение с внешней точкой доступа.
	SSID	Имя беспроводной точки доступа, с которой установлено подключение. Задается в меню ***«Сеть → Wi-Fi → Клиент»***.
	BSSID	Физический адрес беспроводной точки доступа, с которой установлено подключение. Задается в меню ***«Сеть → Wi-Fi → Клиент»***.
	RSSI	Уровень сигнала от внешней точки доступа, по каждому антенному входу.
	RX Битрейт	Текущая битовая скорость физического радиоканала для приема данных. Скорость в основном зависит от количества приемо-передающих антенн на принимающей и передающей стороне, от мощности передатчика, от дистанции и условий приема.
	TX Битрейт	Текущая битовая скорость физического радиоканала для передачи данных. Скорость в основном зависит от количества приемо-передающих антенн на принимающей и передающей стороне, от мощности передатчика, от дистанции и условий приема.
	RX	Объем трафика, принятого через беспроводную сеть.
	TX	Объем трафика, переданного через беспроводную сеть.

2.4.2 Статус – Wi-Fi – Клиенты

В меню представлен список подключенных клиентов по Wi-Fi (рис.2.4.2). Параметр SSID указывает, к какой именно беспроводной сети подключен Wi-Fi клиент. Описание параметров представлено в таблице 2.4.2.

Подключенные клиенты

Сигнал	SSID	MAC адрес	Хост	Подключен	Битрейт (TX / RX)	Трафик (TX / RX)
-46 дБм	SSID1	8e:ec:6d:4f:da:31	-	0h 1m 30s	72 / 72	39.43 KB / 30.41 KB

Рис.2.4.2. Меню «Статус – Wi-Fi – Клиенты»

Таблица 2.4.2. Описание полей «Подключенные клиенты»

№	Название поля	Описание
Подключенные клиенты		
1	Сигнал	Уровень радиосигнала от Wi-Fi клиента.
2	SSID1	Беспроводная сеть, к которой подключился клиент SSID1 или SSID2.
3	MAC адрес	Физический адрес клиента.
4	Хост	Имя хоста (клиента).
5	Подключен	Время с момента подключения.
6	Битрейт (TX / RX)	Битовая скорость физического радиоканала на прием (RX) и на передачу (TX) данных. Значение динамически изменяется от расстояния и условий приема, а также от кол-ва приемопередающих антенн на Wi-Fi устройстве.
7	Трафик (TX / RX)	Объем трафика, переданного клиенту (TX) / принятого от клиента (RX).

2.4.3 Статус – Wi-Fi – Поиск сетей

В меню реализована возможность выполнить поиск беспроводных сетей. Поиск сетей инициируется при нажатии кнопки **«СКАНИРОВАТЬ»**. Время сканирования не более 5 секунд. В результате работы будет выведена таблица с найденными беспроводными сетями. Описание параметров представлено в таблице 2.4.3. Пример результата поиска беспроводных сетей показан на рис. 2.4.3.

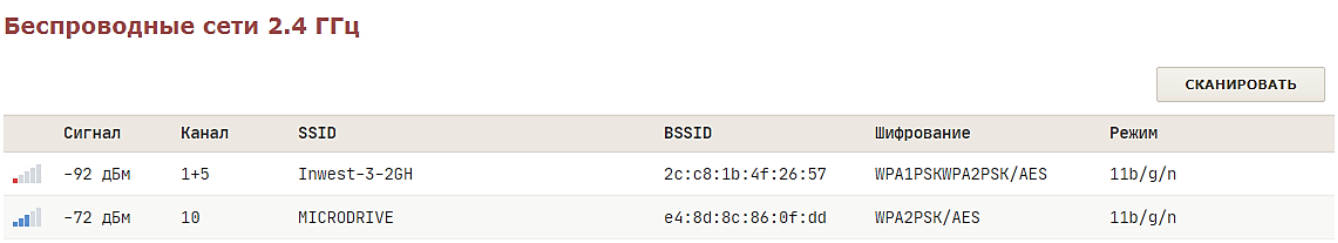


Рис.2.4.3. Меню «Статус – Wi-Fi – Поиск сетей». Пример результата поиска беспроводных сетей

Таблица 2.4.3. Описание полей «Беспроводные сети 2.4 ГГц»

№	Название поля	Описание
Беспроводные сети 2.4 ГГц		
1	Сигнал	Уровень радиосигнала от беспроводной сети.
2	Канал	Номера частотных каналов используемых беспроводной сетью. Если сеть использует 2 канала, значит полоса пропускания сети 40 МГц.
3	SSID	Имя беспроводной сети.
4	BSSID	Физический адрес беспроводной сети.
5	Шифрование	Метод шифрования и аутентификации в беспроводной сети.
6	Режим	Стандарты связи, поддерживаемые беспроводной сетью. Например, значение 11b/g/n означает, что сеть поддерживает стандарты IEEE 802.11b, IEEE 802.11g, IEEE 802.11n.

2.5 Статус – Маршруты

2.5.1 Статус – Маршруты – Маршруты IPv4

В меню представлена таблица маршрутизации (рис.2.5.1). В соответствии с этой таблицей роутер выполняет перенаправление трафика из одной сети (интерфейса) в другую сеть.

Таблица состоит из сетевых маршрутов и предназначена для определения наилучшего пути передачи сетевых пакетов. Каждая запись в таблице маршрутизации состоит из полей:

- Цель (IP-адрес и маска сети назначения);
- Шлюз (IP-адрес шлюза), если пакет необходимо передать через шлюз;
- Метрика маршрута (приоритет маршрута);
- Интерфейс.

При отправке сетевого пакета, операционная система смотрит, по какому именно маршруту он должен быть отправлен, основываясь на таблице маршрутизации. Как правило, выбирается наиболее короткий (то есть, с меньшей метрикой) маршрут из тех, которые соответствуют адресу получателя. Особый маршрут – **0.0.0.0/0** или маршрут **«По умолчанию»** именно этот маршрут используется для отправки пакетов в сеть Интернет. Если ни один из маршрутов не подходит, пакет уничтожается, а его отправителю возвращается соответствующее ICMP-сообщение. В большинстве случаев таблица маршрутизации заполняется автоматически, на основе настроек интерфейсов. Записи в таблицу могут быть добавлены вручную в меню ***«Сеть → Статические маршруты»***.

Описание параметров представлено в таблице 2.5.1.

Таблица маршрутизации

Цель	Шлюз	Метрика	Интерфейс
0.0.0.0/0	100.79.74.133	20	modem
100.79.74.128/29		20	modem
192.168.0.0/24		0	sta0
192.168.1.0/24		0	lan

Рис.2.5.1. Меню «Статус – Маршруты – Маршруты IPv4». Пример таблицы маршрутизации

Таблица 2.5.1. Описание полей «Таблица маршрутизации»

№	Название поля	Описание
Таблица маршрутизации		
1	Цель	IP-адрес и префикс сети назначения.
2	Шлюз	IP-адрес шлюза, присутствует, если сеть назначения может быть достигнута только через шлюз.
3	Метрика	Приоритет маршрута, чем меньше метрика – тем выше приоритет маршрута. 0 – максимальный приоритет.
4	Интерфейс	Имя интерфейса, через который необходимо отправлять пакеты, что бы они достигли сети, указанной в колонке **«Цель»**.

2.5.2 Статус – Маршруты – ARP

В меню представлена таблица ARP (рис.2.5.2). Таблица ARP (протокола разрешения адресов) представляет из себя кэш, в котором хранятся соответствия между адресами канального уровня (MAC) и адресами сетевого уровня (IP). Операционная система сохраняет кэш ARP в оперативной памяти, кэш может динамически обновляться с помощью протокола ARP.

Описание параметров представлено в таблице 2.5.2.

Таблица ARP

IPv4 адрес	MAC адрес	Статус	Интерфейс
192.168.1.199	8e:ec:6d:4f:da:31	stale	lan
192.168.1.2	6c:62:6d:ff:54:bc	stale	lan
192.168.1.120	f4:6d:04:ad:03:2b	reachable	lan

Рис.2.5.1. Меню «Статус – Маршруты – ARP». Пример таблицы ARP

Таблица 2.5.1. Описание полей «Таблица ARP»

№	Название поля	Описание
Таблица ARP		
1	IPv4	IP-адрес хоста.
2	MAC адрес	Физический адрес хоста.
3	Статус	Актуальность записи в таблице. Возможные значения: **stale** – запись устарела; **reachable** – запись актуальна.
4	Интерфейс	Интерфейс, на котором был обнаружен указанный хост.

2.6 Статус – DHCP

В меню находится таблица со списком выданных аренд IP-адресов (рис.2.6). Аренда IP-адреса выдается сервером DHCP по запросу от хоста в соответствии с протоколом DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol). Аренда выдается на определенное время, в зависимости от настроек сервера. Кроме IP-адреса, сервер DHCP может выдавать и другие параметры – IP-адрес шлюза, IP-адрес DNS и другие параметры. Настройки сервера DHCP находится в меню ***«Сеть → DHCP/DNS»***.

Описание параметров представлено в таблице 2.6.

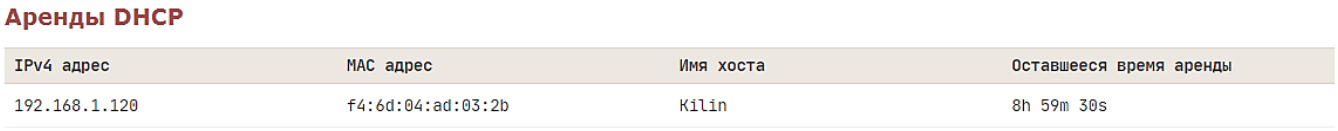


Рис.2.6. Меню «Статус – DHCP»

Таблица 2.6. Описание полей «Аренды DHCP»

№	Название поля	Описание
Аренды DHCP		
1	IPv4 адрес	IP-адрес хоста, который был назначен сервером DHCP из пула IP-адресов DHCP.
2	MAC адрес	Физический адрес хоста.
3	Имя хоста	Сетевое имя хоста.
4	Оставшееся время аренды	Время, по истечении которого, хост должен отправить повторный запрос на получение IP-адреса. Если хост не отправит запрос серверу в указанный интервал, то IP-адрес может быть назначен другому хосту в сети.

2.7 Статус – Системный журнал

В меню находится системный журнал роутера (System Log) (рис.2.7). Системный журнал – это хронологически упорядоченная совокупность записей результатов деятельности процессов и ядра операционной системы. Системный журнал используется для анализа работы операционной системы с целью выявления возможных проблем. Системный журнал хранится в оперативной памяти и после сброса питания устройства будет очищен. Размер системного журнала может быть изменен в меню ***«Система → Системный журнал».*** Параметр **«Фильтр»** позволяет выбрать режим отображения системного журнала – системные сообщения, аппаратные сообщения и все сообщения.

С помощью кнопки **«СОХРАНИТЬ В ФАЙЛ»** можно сохранить все записи журнала в текстовый файл с именем ***syslog-<модель устройства>-<версия ПО>.txt***.

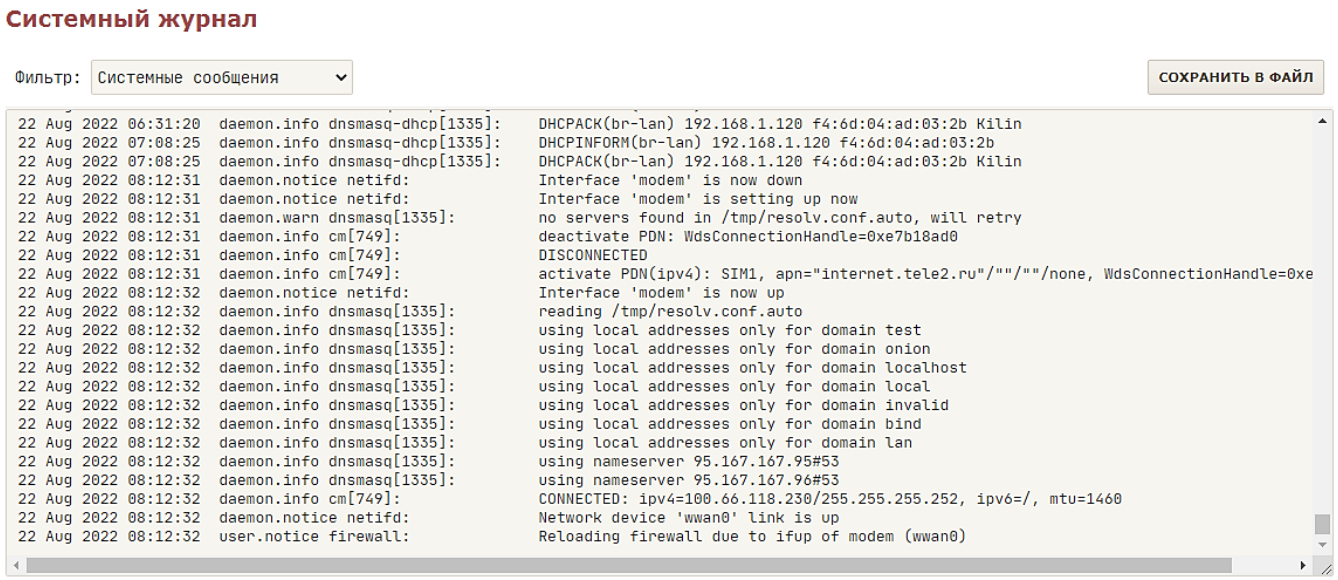


Рис.2.7. Меню «Статус – Системный журнал»

3 Меню «Система»

3.1 Система – Система

3.1.1 Система – Система – Основные настройки

В меню настраиваются основные параметры системы вашего устройства, такие как имя хоста, язык WEB-интерфейса и часовой пояс системных часов (рис.3.1.1). Кнопка **«СИНХРОНИЗИРОВАТЬ»** позволяет синхронизировать системные часы устройства с системными часами вашего ПК или смартфона.

Описание параметров представлено в таблице 3.1.1.

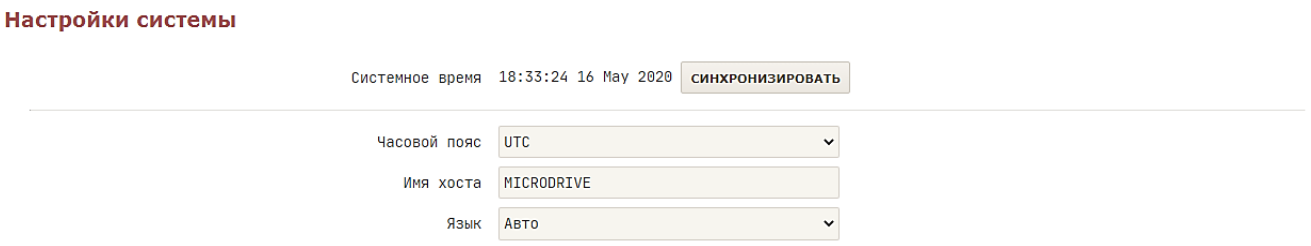


Рис.3.1.1. Меню «Система – Система – Основные настройки»

Таблица 3.1.1. Описание параметров «Настройки системы»

№	Название поля	Описание
Настройки системы		
1	Системное время	Отображается текущее системное время в операционной системе. Системное время сбрасывается при перезагрузке и может быть вновь задано вручную – с помощью кнопки **«СИНХРОНИЗИРОВАТЬ»** или автоматически через NTP протокол (см. настройки NTP-клиента).
2	Часовой пояс	Выбор часового пояса для системных часов.
3	Имя хоста	Сетевое имя хоста.
4	Язык	Выбор языка для WEB-интерфейса. Возможные значения: **Авто** – автоматическое определения языка из запросов веб-браузера; **Русский (Russian)** – русский язык; **English** – английский язык.

3.1.2 Система – Система – Системный журнал

В меню настраиваются параметры ведения системного журнала, а также параметры удаленного журналирования (рис.3.1.2). Удаленное журналирование – механизм передачи записей системного журнала на удаленный сервер по протоколу SysLog в реальном времени, в качестве транспортного протокола выступает UDP или TCP.

Описание параметров представлено в таблице 3.1.2.

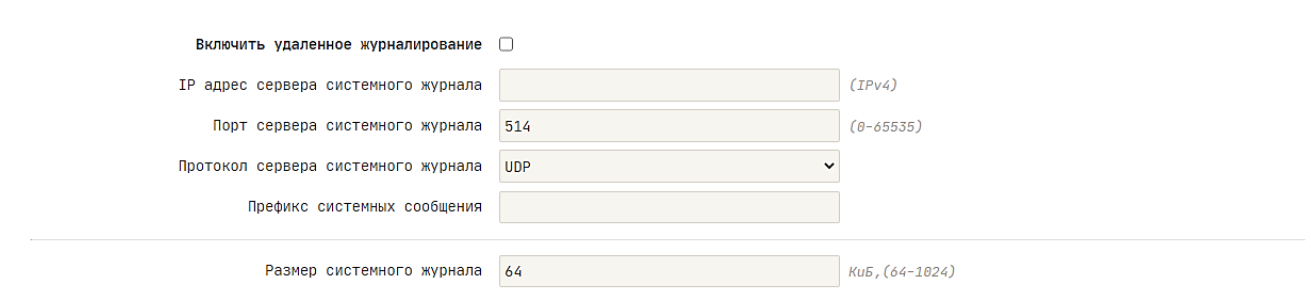


Рис.3.1.2. Меню «Система – Система – Системный журнал»

Таблица 3.1.2. Описание параметров «Системный журнал»

№	Название поля	Описание
Системный журнал		
1	Включить удаленное журналирование	Включить/Отключить отправку системных сообщений на удаленный сервер SysLog.
2	IP адрес сервера системного журнала	Задается IP-адрес сервера системного журнала.
3	Порт сервера системного журнала	Задается порт сервера системного журнала.
4	Протокол сервера системного журнала	Протокол TCP или UDP для передачи системных сообщений.
5	Префикс системных сообщений	Префикс пользовательского текста в потоковых системных сообщениях.
6	Размер системного журнала	Размер оперативной памяти (в килобайтах), выделенной для ведения системного журнала.

3.1.3 Система – Система – Синхронизация времени

В меню настраиваются параметры NTP-клиента и NTP-сервера (рис.3.1.3). NTP (**N**etwork **T**ime **P**rotocol) — сетевой протокол для синхронизации внутренних часов устройства с использованием сетей с переменной латентностью. NTP использует для своей работы протокол UDP. Синхронизация времени NTP происходит в течение определенного периода времени и включает в себя передачу пакетов NTP по сети. Пакеты NTP содержат метки времени, которые включают образец времени как от клиента, так и от сервера, участвующих в синхронизации времени.

Описание параметров представлено в таблице 3.1.3.

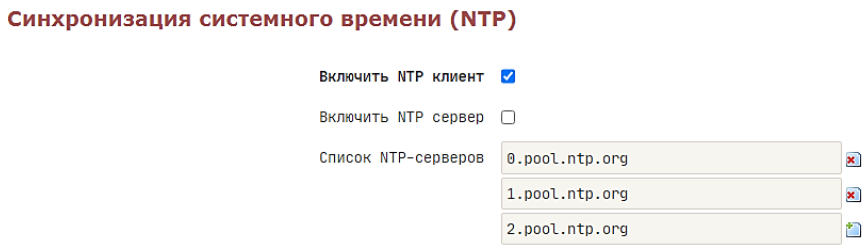


Рис.3.1.3. Меню «Система – Система – Синхронизация времени»

Таблица 3.1.3. Описание параметров «Синхронизация системного времени (NTP)»

№	Название поля	Описание
Синхронизация системного времени (NTP)		
1	Включить NTP клиент	Включить/Отключить синхронизацию внутренних системных часов с серверами точного времени по протоколу NTP.
2	Включить NTP сервер	Разрешить/Запретить устройству выступать в роли сервера точного времени.
3	Список NTP-серверов	Список IP-адресов или доменных имен серверов точного времени.

3.2 Система – Управление

3.2.1 Система – Управление – Пароль

В меню реализована возможность задать (сменить) пароль от учетной записи «***root***» (рис.3.2.1). Пароль запрашивается при подключении к устройству через WEB-интерфейс или SSH.

Для того что бы задать пароль, введите в поле **«Новый Пароль»** и **«Подтвердить Пароль»** соответствующий пароль. Для того что бы снять пароль, введите в поле **«Текущий Пароль»** установленный пароль, а поля **«Новый Пароль»** и **«Подтвердить Пароль»** оставьте пустыми. Нажмите кнопку **«СМЕНИТЬ»**.

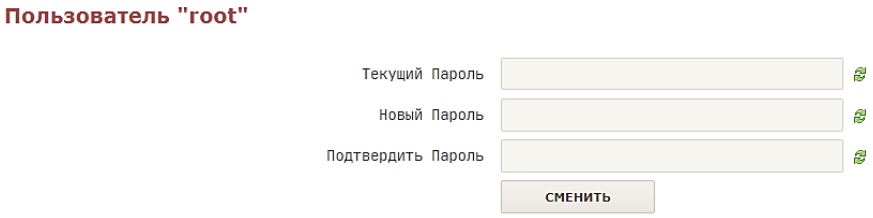


Рис.3.2.1. Меню «Система – Управление – Пароль»

3.2.2 Система – Управление – WEB Доступ (HTTP)

В меню настраиваются параметры встроенного WEB-сервера (рис.3.2.2). WEB-сервер обеспечивает доступ к устройству посредством HTTP (**H**yper **T**ext **T**ransfer **P**rotocol) протокола. **Отключение WEB-сервера приведет к потери доступа к устройству по HTTP протоколу**. При необходимости, в целях безопасности, можно сменить порт веб-сервера. WEB-сервер работает на всех IP-адресах устройства, т.е. прослушивает все интерфейсы.

Описание параметров представлено в таблице 3.2.2.

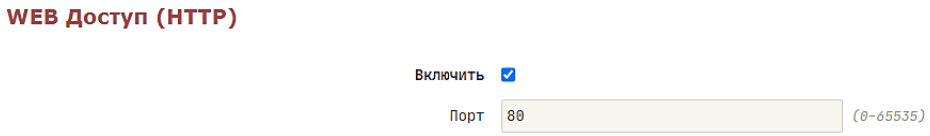


Рис.3.2.2. Меню «Система – Управление – WEB Доступ (HTTP)»

Таблица 3.2.2. Описание параметров «WEB Доступ (HTTP)»

№	Название поля	Описание
WEB доступ (HTTP)		
1	Включить	Включить/Отключить WEB-сервер.
2	Порт	TCP-порт, который прослушивает WEB-сервер.

3.2.3 Система – Управление – SSH Доступ

В меню настраиваются параметры встроенного SSH-сервера (рис.3.2.3). SSH-сервер обеспечивает доступ к устройству посредством SSH (**S**ecure **Sh**ell) протокола. В настройках можно задать порт и/или интерфейс, который будет прослушивать SSH-сервер. Для шифрования используется автоматически сгенерированный ключ, ключ будет генерироваться заново при каждом перезапуске устройства.

Описание параметров представлено в таблице 3.2.3.

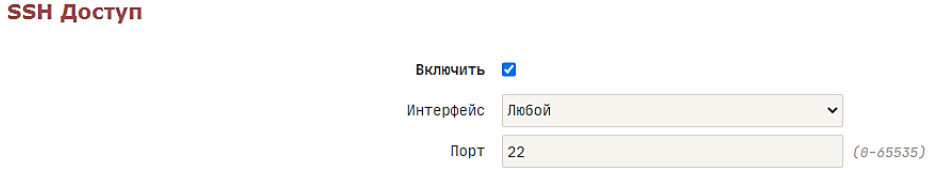


Рис.3.2.3. Меню «Система – Управление – SSH Доступ»

Таблица 3.2.3. Описание параметров «SSH Доступ»

№	Название поля	Описание
SSH Доступ		
1	Включить	Включить/Отключить SSH-сервер.
2	Интерфейс	IP-адрес интерфейса, который прослушивает SSH-сервер. Возможные значения: **Любой** – все IP-адреса в системе будут прослушиваться; **<Имя интерфейса>** – только IP-адрес указанного интерфейса будет прослушиваться.
3	Порт	TCP-порт, который прослушивает SSH-сервер.

3.2.4 Система – Управление – SMS

В меню настраиваются функции **«SMS управление»** (рис.3.2.4.1) и **«SMS-шлюз»** (рис.3.2.4.2).

3.2.4.1 Система – Управление – SMS – SMS Управление

Принцип управления устройством заключается в отправке SMS сообщений с соответствующей командой на телефонный номер активной SIM-карты. Если команда верная, роутер выполнит ее и отправит ответное сообщение, а в системном журнале будет сделана соответствующая запись. Для аутентификации сообщений, в настройках следует предварительно добавить телефонный номер отправителя. Для работы функции **«SMS-Управление»** должны быть выполнены следующие условия:

- Встроенный LTE-модем должен зарегистрироваться в голосовой сети оператора. Некоторые операторы могут использовать сети 2G/3G в качестве голосовой сети, в этом случае не следует запрещать работу модема в этих сетях;
- Тарифный план должен поддерживать голосовые вызовы, а также отправку SMS сообщений;
- Положительный баланс на лицевом счете.

Общий формат команд:

<Имя команды> [<аргументы>]

Имя команды и аргументы не должны содержать заглавных букв. Команды и аргументы разделяются пробелами.
Описание параметров представлено в таблице 3.2.4.1а.
Описание SMS-команд представлено в таблице 3.2.4.1б.

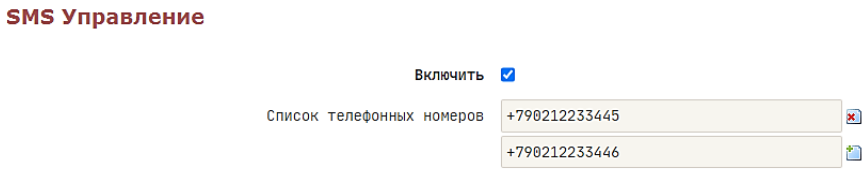


Рис.3.2.4.1. Меню «Система – Управление – SMS – SMS Управление». Пример настройки

Таблица 3.2.4.1а. Описание параметров «SMS Управление»

№	Название поля	Описание
SMS Управление		
1	Включить	Включить/Отключить управление через SMS.
2	Список телефонных номеров	Список доверенных телефонных номеров мобильных абонентов в международном формате «+7xxxxxxxxxx».

Таблица 3.2.4.1б. Описание SMS команд

№	Запрос (команда)	Пример ответа	Описание
1	**info**	**Host**=”MICRODRIVE” **Model**=”Tandem-4GX” **Ver**=17.8.14 **UpTime**=0day, 13:21 **Mem**=27/122 MB **Load**=0.02 0.14 0.09	Запросить состояние и основную информацию о системе. **Host** – имя системы; **Model** – модель роутера; **Ver** – версия ПО; **UpTime** – время работы с момента перезагрузки; **Mem** – объем занятой памяти RAM/Всего памяти RAM; **Load** – средняя загрузка системы.
2	**modem status**	**SIM1**=REGISTERED, HOME **PLMN**=25020 Tele2 **Cid**=901B4503 **Lac**=D510 **Band**=LTE BAND 3 **Rssi**=-59/89% **Rsrp**=87 **Rsrq**=-13 **Sinr**=16 **ConnectIPv4**=10.70.15.3	Запросить состояние подключения к мобильной сети. **SIM1/2** – статус регистрации в сети и текущая SIM-карта; **PLMN** – идентификатор и имя оператора; **Cid** – идентификатор соты (сектора); **Lac** – код локальной зоны (в 3G) или код зоны отслеживания (в LTE); **Band** – текущий частотный диапазон; **Rssi** – уровень сигнала в дБм и процентах; **Rsrp** – мощность пилотных сигналов в дБм (в LTE); **Rsrq** – качество пилотных сигналов в дБ (в LTE); **Sinr** – отношение сигнал/шум в дБ (в LTE); **Rscp** – мощность принятого сигнала в дБм (в 3G); **Ecio** – отношение несущая/шум дБ (в 3G); **ConnectIPv4** – IP-адрес, выданный оператором при подключении, если подключение отсутствует выводится **disconnect**. Если встроенный модем поддерживает агрегацию частот, то отправляются параметры только для основной частоты (соты).
3	**modem info**	**TYPE**=EC25 **Revision**=EC25EUGAAR06A03 **IMEI**=865544003366702 **SIM**=1/1 **IMSI**=250207792022203 “ROSTELECOM”	Запросить информацию об LTE-модеме. **TYPE** – тип LTE-модема; **Revision** – версия ПО LTE модуля; **IMEI** – международный уникальный идентификатор LTE-модема; **SIM** – текущая SIM-карта/Количество SIM-карт; **IMSI** – международный идентификатор мобильного абонента и имя провайдера.
4	**modem slot [<num>]**	**modem slot 1** **OK**	Выбрать SIM-карту. <num> – не обязательный параметр – номер SIM-карты (1 или 2). Если аргумент <num> не указан, роутер переключится на другую SIM-карту.
5	**iface <name>** **Пример:** **iface modem** **iface l2tp**	**modem**=up **Uptime**=0 day, 14:30 **IPv4**=100.71.160.50/29 **MAC**=fa:fe:1e:c0:11:2d **MTU**=1500 **Tx**=3.10 MB **Rx**=4.04 MB	Запросить статус интерфейса. <name> – имя интерфейса. **Первая строчка** – имя и статус интерфейса, возможны значения **up, down, connecting**; **Uptime** – время работы интерфейса с момента подключения; **MAC** – физический адрес интерфейса; **MTU** – размер MTU интерфейса; **Tx** – объем отправленного трафика через интерфейс; **Rx** – объем принятого трафика через интерфейс.
6	**iface <name> up**	**iface modem up** **OK**	Запустить/Перезапустить интерфейс. <name> – имя интерфейса.
7	**iface <name> down**	**iface l2tp down** **OK**	Остановить интерфейс. <name> – имя интерфейса.

8	`iface <name> enable`	`iface l2tp enable`
		
		`OK`
			Включить автозапуск интерфейса после сброса питания. <name> – имя интерфейса.

9	`iface <name> disable`	`iface lan disable`
		
		`OK`
			Отключить автозапуск интерфейса после сброса питания. <name> – имя интерфейса.

10	`wifi on`	`wifi on`
		
		`OK`
			Включить WiFi сети.

11	`wifi off`	`wifi off`
		
		`OK`
			Отключить WiFi сети.

12	`reboot`	`reboot`
		
		`OK`
			Перезагрузить роутер.

3.2.4.2 Система – Управление – SMS – SMS Шлюз

Принцип работы функции **«SMS-Шлюз»** заключается в пересылке входящих SMS сообщений на указанный номер мобильного абонента. Дополнительно возможно задать телефонные номера мобильных абонентов, SMS-сообщения от которых необходимо пересылать. Для работы функции **«SMS-Шлюз»** должны быть выполнены условия из пункта 3.2.4.1.

Описание параметров представлено в таблице 3.2.4.2.

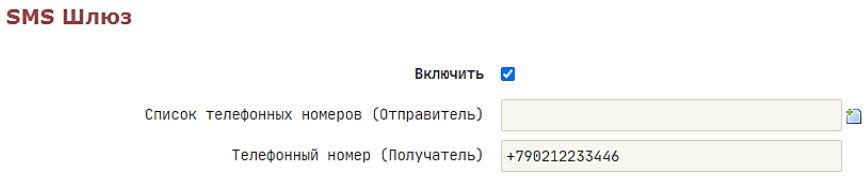


Рис.3.2.4.2. Меню «Система – Управление – SMS – SMS Шлюз». Пример настройки

Таблица 3.2.4.2. Описание параметров «SMS Шлюз»

№	Название поля	Описание
SMS Шлюз		
1	Включить	Включить/Отключить пересылку SMS-сообщений.
2	Список телефонных номеров (Отправитель)	Список телефонных номеров мобильных абонентов, SMS-сообщения от которых необходимо пересылать. Если после пустое, то пересылаются SMS-сообщения от всех абонентов.
3	Телефонный номер (Получатель)	Телефонный номер мобильного абонента, на который необходимо пересылать SMS-сообщение.

3.3 Система – Прошивка

В меню реализована возможность сброса настроек устройства на заводские значения, сохранять и загружать резервную копию файлов конфигурации (рис.3.3.1), а также возможность обновления программного обеспечения (рис.3.3.2).

3.3.1 Система – Прошивка – Резервное копирование / Восстановление

Для сброса настроек устройства нажмите кнопку **«ВЫПОЛНИТЬ СБРОС»** и дождитесь перезагрузки устройства.

Для сохранения копии конфигурации устройства нажмите кнопку **«ЗАГРУЗИТЬ АРХИВ»**, после этого Ваш интернет-браузер выполнит скачивание архива в свою рабочую папку. Сохраненный архив представляет собой файл с именем ***«backup-<модель устройства>-<версия ПО>.tar.gz».***

Для восстановления конфигурации устройства выберете соответствующий файл и нажмите кнопку **«ЗАГРУЗИТЬ»**. Система проверит архив на корректность и запустит процесс восстановления конфигурации с последующей перезагрузкой устройства. Время восстановления конфигурации не превышает 2 минут.

Конфигурации разных версий ПО не совместимы между собой.

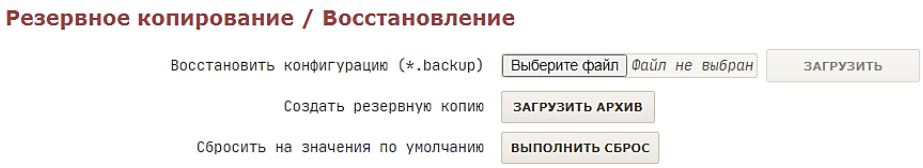


Рис.3.3.1. Меню «Система – Прошивка – Резервное копирование / Восстановление»

3.3.2 Система – Прошивка – Обновить прошивку

Для обновления программного обеспечения выберете соответствующий файл-образ и нажмите кнопку **«УСТАНОВИТЬ»** (рис.3.3.2). Далее система предложит проверить контрольную сумму файла-образа. Нажмите **«>»**.

После обновления программного обеспечения операционная система запуститься автоматически. Время обновления прошивки занимает 2-3 минуты.

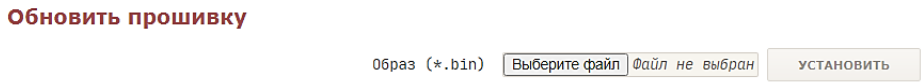


Рис.3.3.2. Меню «Система – Прошивка – Обновить прошивку»

Не отключайте питание устройства во время обновления программного обеспечения.

После обновления программного обеспечения все настройки устройства будут сброшены на заводские значения.

3.4 Система – Перезагрузка

В меню реализована возможность выполнить перезагрузку операционной системы устройства (рис.3.4). Время перезагрузки составляет 30-60 секунд.

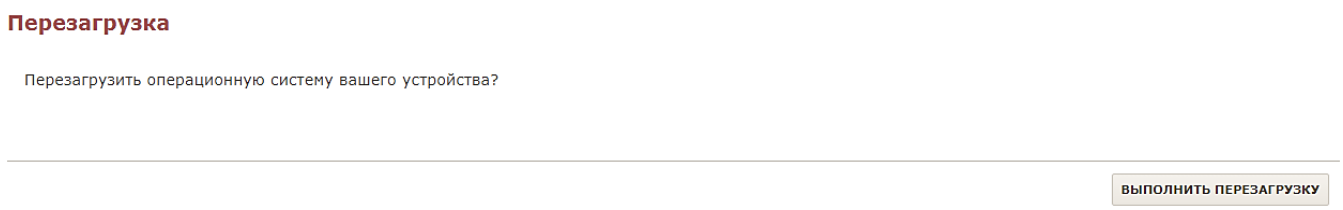


Рис.3.4. Меню «Система – Перезагрузка»

4 Меню «Сеть»

4.1 Сеть – Сетевой мост

В меню находится раздел предназначенный для настройки интерфейса сетевого моста – **«lan»**.

Сетевой мост (bridge) — сетевое устройство второго (канального) уровня модели OSI. Сетевой мост предназначен для объединения интерфейсов на канальном уровне в единую сеть. По умолчанию, мост **«lan»** объединяет каналы Wi-Fi и Ethernet.

В настройках можно сменить IP-адрес интерфейса моста и маску подсети. По IP-адресу сетевого моста будет доступен WEB-интерфейс роутера из проводной сети Ethernet и беспроводной сети Wi-Fi. Состояние интерфейса можно отслеживать в меню ***«Статус → Интерфейсы».***

> Отключение интерфейса может привести к потере доступа к устройству через Ethernet или Wi-Fi.

Раздел состоит из двух частей — **«Основные настройки»** (рис.4.1а) и **«Настройки межсетевого экрана»** (рис.4.1б). Описание параметров представлено в таблице 4.1.

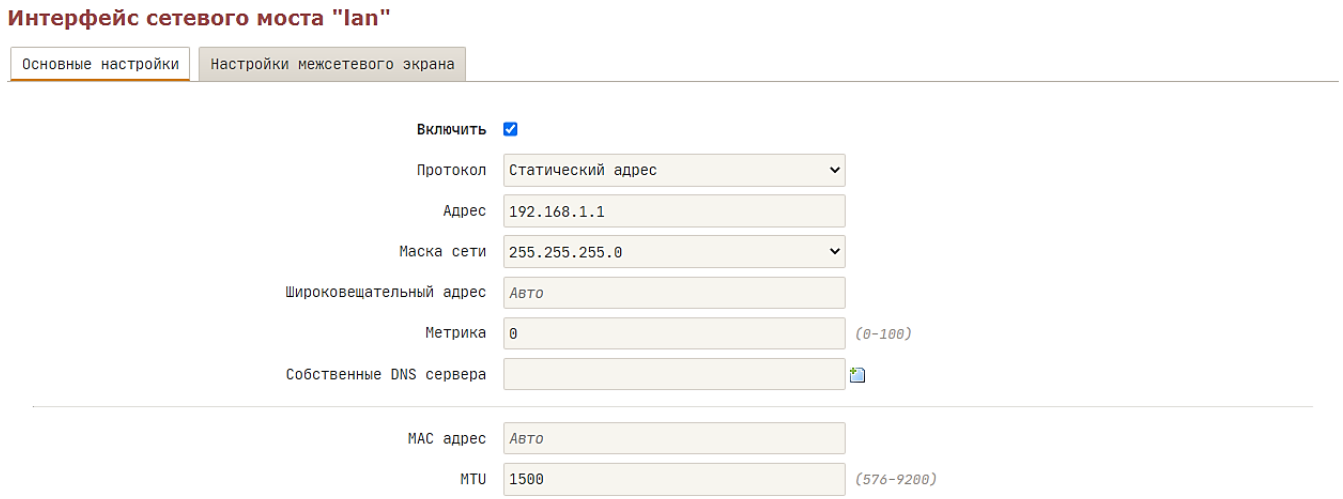


Рис.4.1а. Меню «Сеть – Сетевой мост». Вкладка «Основные настройки»

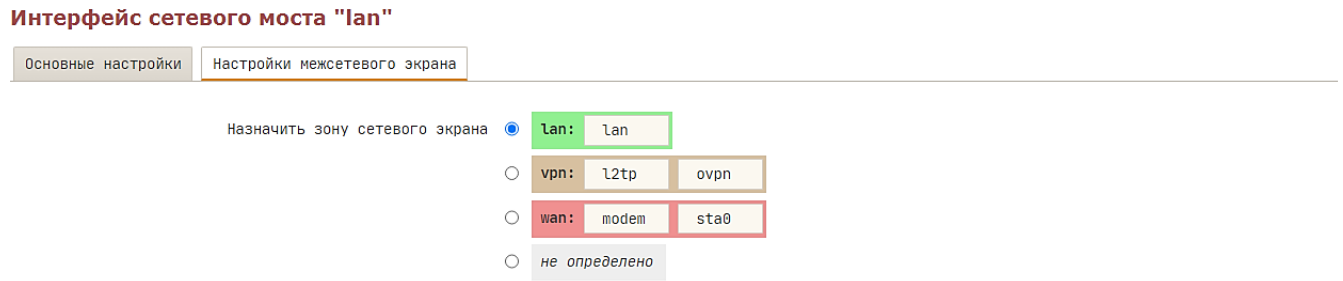


Рис.4.1б. Меню «Сеть – Сетевой мост». Вкладка «Настройки межсетевого экрана»

*Таблица 4.1. Описание параметров «Интерфейс сетевого моста **lan**»*

№	Название поля	Описание
Интерфейс сетевого моста «lan». Основные настройки		
1	Включить	Включить/Отключить интерфейс.
2	Протокол	Способ назначения интерфейсу IP-параметров. Возможные значения: **Отсутствует** – интерфейс работает без IP-адреса и функционирует только для объединения сегментов сетей; **Статический адрес** – все IP параметры задаются вручную в соответствующих полях.
3	Адрес	IP-адрес интерфейса. Должен быть задан в соответствии с общепринятыми правилами распределения сетевых адресов.
4	Маска	Битовая маска подсети. Маска предназначена для определения по IP-адресу адреса подсети и

		адреса узла.
5	Широко-вещательный адрес	IP-адрес для передачи широковещательных пакетов в сеть. Вычисляется автоматически из IP-адреса и маски подсети или задается вручную. Для адреса 192.168.1.1 и маски подсети 255.255.255.0 значение широковещательного адреса будет 192.168.1.255.
6	Метрика	Приоритет маршрутов через интерфейс в таблице маршрутизации. Значение 0 – максимальный приоритет.
7	Собственные DNS сервера	Добавить IP-адреса DNS серверов.
8	MAC адрес	Физический адрес интерфейса. Если не задан, адрес будет сгенерирован автоматически.
9	MTU	MTU (**M**aximum **T**ransmission **U**nit). Параметр определяет максимальный размер пакета данных через этот интерфейс, который будет передаваться без фрагментации.
Интерфейс сетевого моста «lan». Настройки межсетевого экрана		
1	Назначить зону сетевого экрана	Зона межсетевого экрана, к которой будет прикреплен интерфейс. Рекомендуется использовать зону **«lan»**. Настройки зон находятся в меню ***«Статус → Межсетевой экран»***.

4.2 Сеть – Wi-Fi

4.2.1 Сеть – Wi-Fi – Общие

В меню находится раздел предназначенный для настройки приемопередатчика 2.4 ГГц. Эти настройки являются общими для всех беспроводных сетей (рис.4.2.1а,б). Раздел состоит из двух частей **«Основные настройки»** (рис.4.2.1а) и **«Дополнительные настройки»** (рис.4.2.1б).

Описание параметров представлено в таблице 4.2.1.

Рис.4.2.1а. Меню «Сеть – Wi-Fi – Общие». Вкладка «Основные настройки»

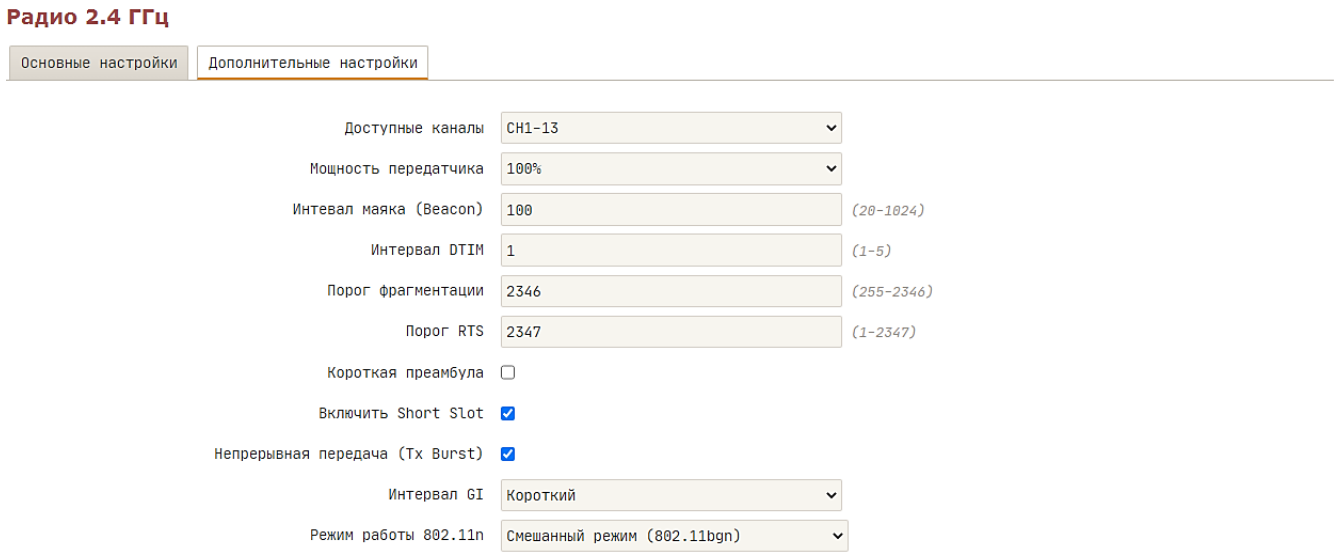


Рис.4.2.1б. Меню «Сеть – Wi-Fi – Общие». Вкладка «Дополнительные настройки»

Таблица 4.2.1. Описание параметров «Радио 2.4 ГГц»

№	Название поля	Описание
Радио 2.4 ГГц. Основные настройки		
1	Включить	Включить/Отключить приемопередатчик. Приемопередатчик должен быть включен для работы беспроводных сетей.
2	Протокол	Выбор стандарта связи. Возможные значения: **802.11bgn** – одновременная работа приемопередатчика в стандартах связи IEEE 802.11b, IEEE 802.11g, IEEE 802.11n. Стандарты IEEE 802.11b, IEEE 802.11g считаются устаревшими. Если в беспроводной сети есть устройства, работающие в этих стандартах, это приведет к снижению эффективности передачи данных в этой сети между устройствами стандарта IEEE 802.11n; **802.11b** – работа приемопередатчика в стандарте связи IEEE 802.11b, устаревший стандарт. Скорость до 11 Мбит/с; **802.11g** – работа приемопередатчика в стандарте связи IEEE 802.11g. Скорость до 54 Мбит/с. Совместим с IEEE 802.11b; **802.11n** – работа приемопередатчика в стандарте связи IEEE 802.11n. Скорость до 300 Мбит/с.
3	Канал	Выбор частотного канала. В режиме «Авто» роутер выбирает наименее загруженный частотный канал. Автоматический выбор канала работает только при запуске беспроводной сети.
4	Ширина канала	Выбор ширины канала. Возможные значения: **20МГц** – ширина канала равна 20 МГц (рекомендуется), максимальная скорость до 150 Мбит/с; **20/40МГц** – ширина канала выбирается автоматически, предпочтительно 40 МГц, максимальная

		скорость до 300 Мбит/с; При установке значения **«20/40МГц»**, беспроводная сеть занимает почти весь частотный диапазон 2.4ГГц, что может негативно сказаться на передаче данных, если в эфире работают другие беспроводные точки доступа.
5	Расширение канала	Выбор направления расширения канала. Параметр доступен, если ширина канала задана **«20/40Мгц»**. Возможные значения: **Вниз** – дополнительная полоса пропускания будет добавлена внизу частотного диапазона; **Вверх** – дополнительная полоса пропускания будет добавлена вверху частотного диапазона.
6	Изолированные SSID	Если включено, то передача пакетов между беспроводными сетями SSID1 и SSID2 будет заблокирована.
Радио 2.4 ГГц. Дополнительные настройки		
1	Доступные каналы	Выбор списка доступных частотных каналов. Возможные значения: **CH1-13** – список каналов от 1 до 13, стандартный для РФ; **CH1-14** – список каналов от 1 до 14.
2	Мощность передатчика	Настройка мощности передатчика.
3	Интевал маяка (Beacon)	Настраивается интервал рассылки пакетов Beacon, использующейся для синхронизации беспроводной сети. По умолчанию установлено значение 100 мс (рекомендуется).
4	Интервал DTIM	Задается интервал отправки уведомлений о доставке пакетов.
5	Порог фрагментации	Настраивается порог фрагментации пакетов. Пакеты больше заданного значения будут фрагментироваться.
6	Порог RTS	Настраивается время ожидания точкой доступа перед отправкой клиенту сообщения RTS (запрос на пересылку).
7	Короткая преамбула	Включить/Отключить короткую преамбулу. Короткая преамбула увеличит пропускную способность сети, однако снижает надежность доставки пакетов в плохих условиях.
8	Включить Short Slot	Включить/Отключить уменьшение времени ожидания после коллизии для повторной передачи.
9	Непрерывная передача (Tx Burst)	Включить/Отключить приоритет для исходящего трафика (от точки доступа к клиенту).
10	Интервал GI	Выбор гарантированного интервала (GI). Гарантированный интервал – это пустой промежуток между последовательно передаваемыми по беспроводной сети символами. Длинный интервал используется для снижения уровня ошибок, однако снижает скорость передачи.
11	Режим работы 802.11n	Задается режим совместимости в стандарте IEEE 802.11n. Возможные значения: **Смешанный режим (802.11bgn)** – Возможна работа устройств работающих в стандарте IEEE 802.11g, IEEE 802.11b. Снижает скорость передачи данных между устройствами стандарта IEEE 802.11n; **Чистый режим (только клиенты 802.11n)** – Работа устройств (клиентов) стандартов IEEE 802.11g, IEEE 802.11b будет не возможна.

4.2.2 Сеть – Wi-Fi – SSID1/SSID2

В меню находится раздел предназначенный для настройки беспроводных сетей, работающих в режиме **«Wi-Fi точка доступа»**. Каждая беспроводная сеть может работать в составе сетевого моста «**lan»** или как самостоятельный интерфейс со своим IP-адресом.

Раздел состоит из двух подразделов – **«Беспроводная сеть»** и **«Интерфейс wlan0/1»**.

Подраздел **«Беспроводная сеть»** предназначен для настройки параметров доступа к беспроводной сети, например имя сети или метод аутентификации. Подраздел состоит из двух частей — **«Основные настройки»** (рис.4.2.2а) и **«MAC фильтр»** (рис.4.2.2б).

Подраздел **«Интерфейс wlan0/1»** предназначен для настройки IP-параметров интерфейса, который ассоциирован с беспроводной сетью.

Параметры подраздела **«Интерфейс wlan0/1»** следует настраивать, если беспроводная сеть работает как самостоятельный интерфейс (параметр **«Мост/Интерфейс»** имеет значение **«Интерфейс: wlan0/1»**). В противном случае интерфейс «**wlan0/1»** должен быть отключен.

Подраздел состоит из двух частей — **«Основные настройки»** (рис.4.2.2в) и **«Настройки межсетевого экрана»** (рис.4.2.2г).

Описание параметров представлено в таблице 4.2.2.

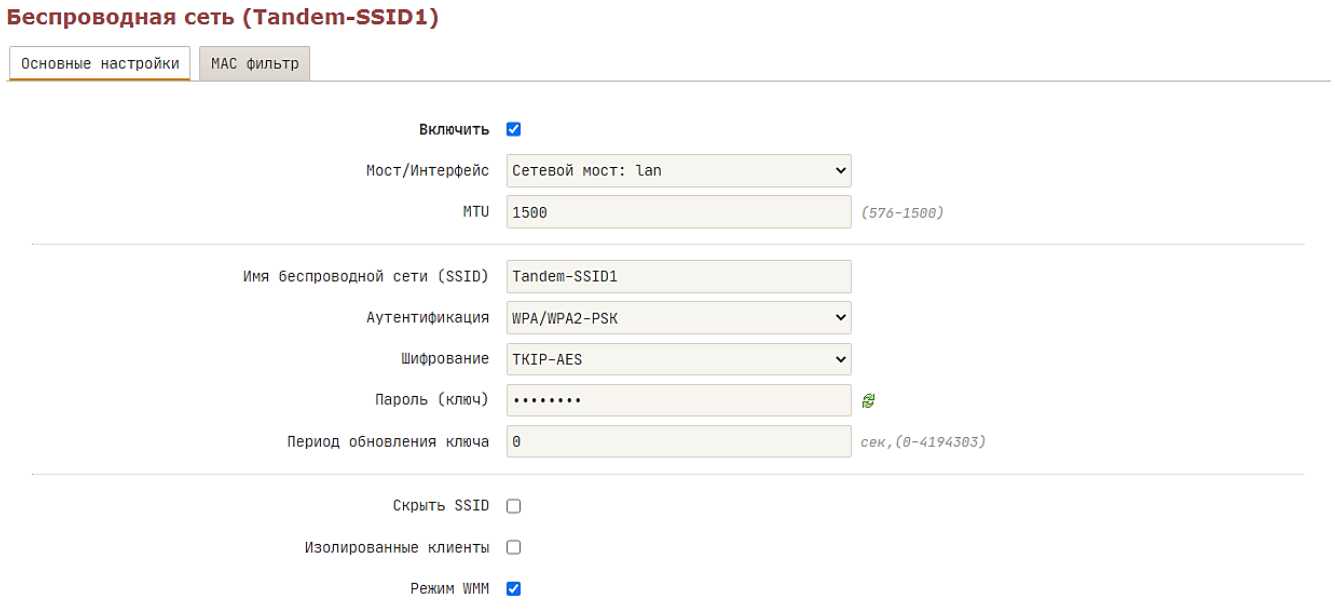


Рис.4.2.2а. Меню «Сеть – Wi-Fi – SSID1/SSID2». Подраздел «Беспроводная сеть». Вкладка «Основные настройки»

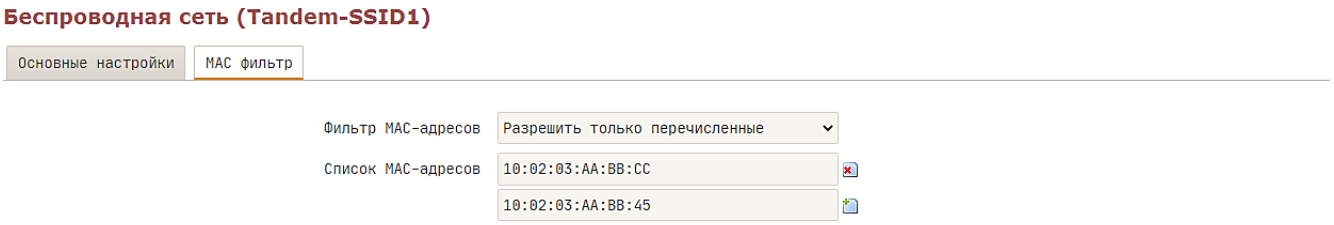


Рис.4.2.2б. Меню «Сеть – Wi-Fi – SSID1/SSID2». Подраздел «Беспроводная сеть». Вкладка «MAC фильтр»

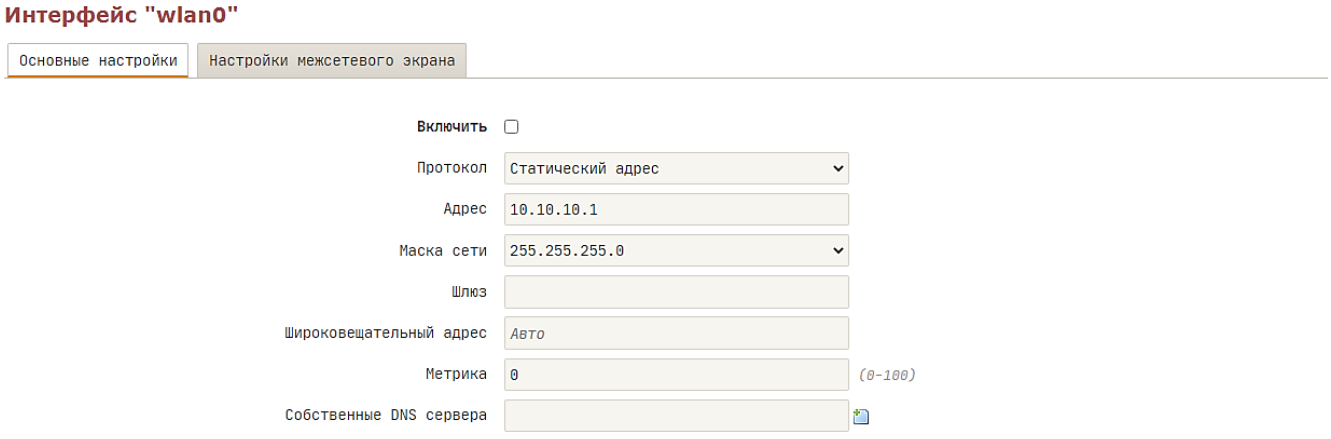


Рис.4.2.2в. Меню «Сеть – Wi-Fi – SSID1/SSID2». Подраздел «Интерфейс wlan0/wlan1». Вкладка «Основные настройки»

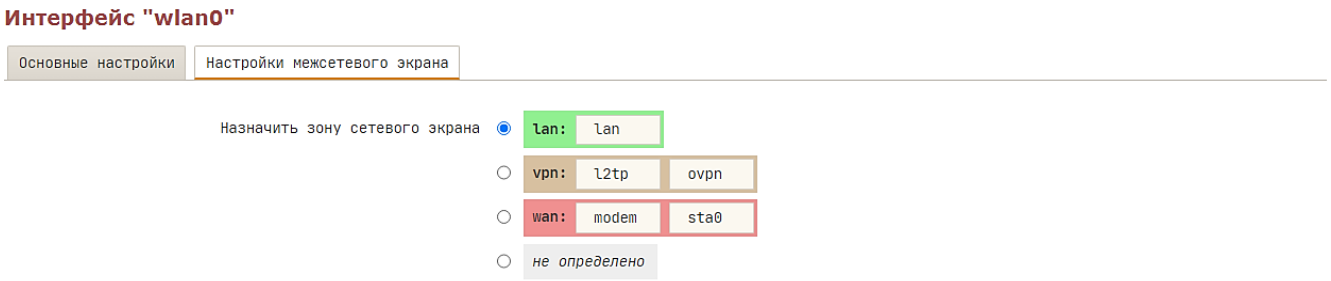


Рис.4.2.2в. Меню «Сеть – Wi-Fi – SSID1/SSID2». Подраздел «Интерфейс wlan0/wlan1». Вкладка «Настройки межсетевого экрана»

*Таблица 4.2.2. Описание параметров «Беспроводная сеть» и «Интерфейс **wlan0/1**»*

№	Название поля	Описание
Беспроводная сеть. Основные настройки		
1	Включить	Включить/Отключить беспроводную сеть.
2	Мост/Интерфейс	Выбор режима работы беспроводной сети. Возможные варианты: **Сетевой мост: lan** – в этом режиме беспроводная сеть будет частью сетевого моста. Интерфейс **«wlan0/wlan 1»** должен быть отключен; **Интерфейс: wlan0/wlan1** – в этом режиме беспроводная сеть работает как самостоятельный интерфейс со своими настройками IP. Интерфейс **«wlan0»/«wlan1»** должен быть включен.
3	MTU	MTU (**M**aximum **T**ransmission **U**nit). Параметр определяет максимальный размер пакета данных через эту сеть, который будет передаваться без фрагментации.
4	Имя беспроводной сети (SSID)	Публичное имя беспроводной сети.
5	Аутентификация	Выбор способа аутентификации клиентов. Возможные значения: **Open** – открытая сеть без аутентификации и шифрования (не рекомендуется); **WPA-PSK** – аутентификация WPA-PSK, общий ключ; **WPA2-PSK** – аутентификация WPA-PSK2, общий ключ; **WPA/WPA2-PSK** – аутентификация WPA-PSK или WPA2-PSK, общий ключ.
6	Шифрование	Выбор способа шифрования трафика. Возможные значения: **TKIP-AES** – автоматический выбор метода шифрования; **TKIP** – попакетное шифрование с проверкой целостности сообщений со скоростью передачи данных до 54 Мбит/с (не рекомендуется); **AES** – современный алгоритм шифрования для стандарта WPA/WPA2.
7	Пароль (ключ)	Пароль сети Wi-Fi, не менее 8 символов.
8	Период обновления ключа	Задается период обновления группового ключа (секунды). Значение 0 – обновление ключа отключено.
9	Скрыть SSID	Включить/Отключить маскировку имени беспроводной сети из вещания.
10	Изолированные клиенты	Включить/Отключить блокировку трафика между подключенными клиентами. Изолированные клиенты не смогут обмениваться пакетами. Блокировка трафика обеспечивается на уровне Wi-Fi драйвера.
11	Режим WMM	Включить /Отключить приоритет в передаче пакетов с мультимедийными данными.
Беспроводная сеть. MAC фильтр		
1	Фильтр MAC-адресов	Включить/Отключить фильтр по MAC-адресу. Возможные значения: **Отключить** – фильтр MAC-адресов отключен; **Разрешить только перечисленные** – разрешить подключаться к сети клиентам перечисленных в параметре **«Список MAC-адресов»**; **Разрешить все, кроме перечисленных** – разрешить подключаться к сети всем клиентам кроме перечисленных в параметре **«Список MAC-адресов»**.
2	Список MAC-адресов	Список MAC-адресов клиентов.
Интерфейс «wlan0/1». Основные настройки		
1	Включить	Включить/Отключить интерфейс.
2	Протокол	Способ назначения интерфейсу IP-параметров. Возможные значения: **Отсутствует** – интерфейс работает без IP-адреса; **Статический адрес** – все IP-параметры задаются вручную в соответствующих полях; **DHCP** – автоматический способ задания IP-параметров.
3	Адрес	IP-адрес интерфейса. Должен быть задан в соответствии с общепринятыми правилами распределения сетевых адресов. Параметр доступен только для ручного способа назначения IP-параметров.
4	Маска сети	Битовая маска подсети. Маска предназначена для определения по IP-адресу адреса подсети и адреса узла. Параметр доступен только для ручного способа назначения IP-параметров.
5	Шлюз	IP-адрес шлюза. Настраивается, если необходимо добавить маршрут «0.0.0.0/0» в таблицу маршрутизации. Параметр доступен только для ручного способа назначения IP-параметров.
6	Широковещательный адрес	IP-адрес для передачи широковещательных пакетов в сеть. Вычисляется автоматически из IP-адреса и маски подсети или задается вручную. Например, для адреса 10.10.10.1 и маски подсети 255.255.255.0 значение широковещательного адреса будет 10.10.10.255. Параметр доступен только для ручного способа назначения IP-параметров.
7	Метрика	Приоритет маршрутов через интерфейс в таблице маршрутизации. Значение 0 – максимальный приоритет.
8	Собственные DNS сервера	Добавить IP-адреса DNS серверов.

9	Добавить маршрут по умолчанию	Параметр определяет, будет ли добавлен маршрут «0.0.0.0/0» в таблицу маршрутизации. Параметр доступен только для автоматического способа назначения IP параметров (DHCP).
10	Добавить DNS объявляемые узлом	Параметр определяет, будут ли добавлены IP-адреса DNS серверов объявляемые DHCP сервером. Параметр доступен только для автоматического способа назначения IP параметров (DHCP).
Интерфейс «wlan0/1». Настройки межсетевого экрана		
1	Назначить зону сетевого экрана	Зона межсетевого экрана, к которой будет прикреплен интерфейс. Настройки зон находятся в меню ***«Статус → Межсетевой экран».*** Назначение зоны **«wan»** автоматически запрещает весь входящий трафик и включает NAT.

4.2.3 Сеть – Wi-Fi – Клиент

В меню находится раздел предназначенный для настройки беспроводной сети, работающей в режиме **«Wi-Fi Клиента»**. Беспроводная сеть может работать в составе сетевого моста «**lan»** или как самостоятельный интерфейс со своим IP-адресом.

Раздел состоит из двух подразделов – **«Беспроводная сеть»** и **«Интерфейс sta0»**.

Подраздел **«Беспроводная сеть»** предназначен для настройки параметров для подключения к внешней точке доступа, например имя сети и пароль (рис.4.2.3а).

Подраздел **«Интерфейс sta0»** предназначен для настройки IP-параметров интерфейса, который ассоциирован с беспроводной сетью.

Частотный канал внешней Wi-Fi точки доступа должен быть фиксирован. Устройство не сможет автоматически определить смену канала.

Параметры подраздела **«Интерфейс sta0»** следует настраивать, если беспроводная сеть работает как самостоятельный интерфейс (параметр **«Мост/Интерфейс»** имеет значение **«Интерфейс: sta0»**). В противном случае интерфейс «**sta0»** должен быть отключен.

Подраздел состоит из двух частей — **«Основные настройки»** (рис.4.2.3б) и **«Настройки межсетевого экрана»** (рис.4.2.3в).

Описание параметров представлено в таблице 4.2.3.

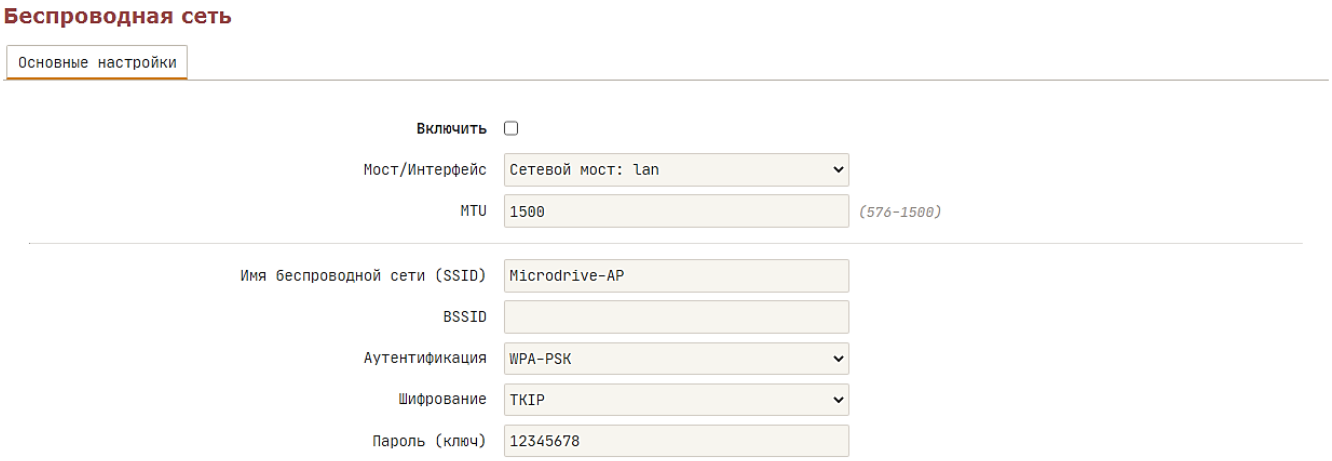


Рис.4.2.3а. Меню «Сеть – Wi-Fi – Клиент». Подраздел «Беспроводная сеть». Вкладка «Основные настройки»

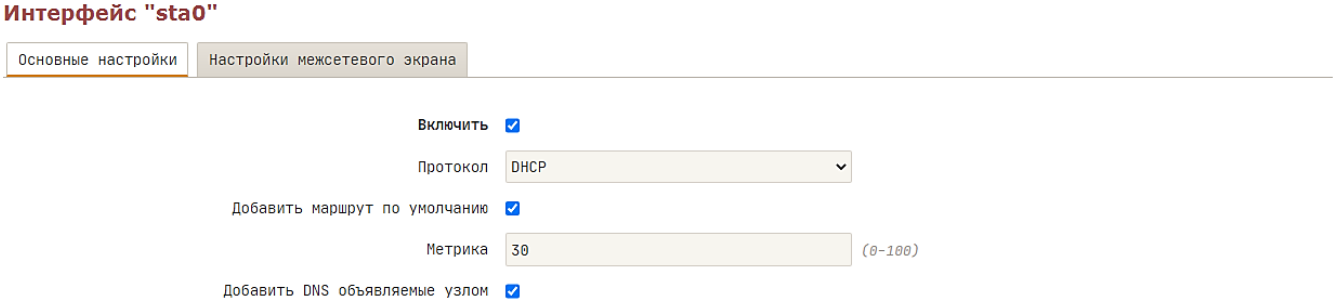


Рис.4.2.3б. Меню «Сеть – Wi-Fi – Клиент». Подраздел «Интерфейс sta0». Вкладка «Основные настройки»

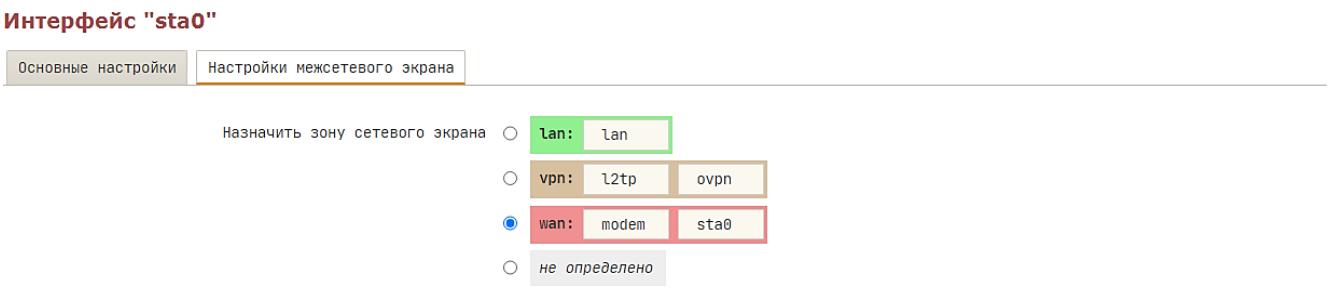


Рис.4.2.3в. Меню «Сеть – Wi-Fi – Клиент». Подраздел «Интерфейс sta0». Вкладка «Настройки межсетевого экрана»

*Таблица 4.2.3. Описание параметров «Беспроводная сеть» и «Интерфейс **sta0**»*

№	Название поля	Описание
Беспроводная сеть. Основные настройки		
1	Включить	Включить/Отключить беспроводную сеть.
2	Мост/Интерфейс	Выбор режима работы беспроводной сети. Возможные варианты: **Сетевой мост: lan** – в этом режиме беспроводная сеть будет частью сетевого моста. Интерфейс «**sta0»** должен быть отключен; **Интерфейс: sta0** – в этом режиме беспроводная сеть работает как самостоятельный интерфейс со своими настройками IP. Интерфейс «**sta0»** должен быть включен.
3	MTU	MTU (**M**aximum **T**ransmission **U**nit). Параметр определяет максимальный размер пакета данных через эту сеть, который будет передаваться без фрагментации.
4	Имя беспроводной сети (SSID)	Публичное имя беспроводной сети, к которой устанавливается подключение.
5	BSSID	MAC-адрес точки доступа. Не обязательный параметр.
6	Аутентификация	Выбор способа аутентификации клиентов. Возможные значения: **Open** – открытая сеть без аутентификации и шифрования; **WPA-PSK** – аутентификация WPA-PSK, общий ключ; **WPA2-PSK** – аутентификация WPA-PSK2, общий ключ.
7	Шифрование	Выбор способа шифрования трафика, который использует точка доступа. Возможные значения: **Отсутствует** – без шифрования; **TKIP** – попакетное шифрование с проверкой целостности сообщений; **AES** – современный алгоритм шифрования для стандарта WPA/WPA2.
8	Пароль (ключ)	Пароль сети Wi-Fi, к которой устанавливается подключение;
Интерфейс «sta0». Основные настройки		
1	Включить	Включить/Отключить интерфейс.
2	Протокол	Способ назначения интерфейсу IP-параметров. Возможные значения: **Отсутствует** – интерфейс работает без IP-адреса; **Статический адрес** – все IP параметры задаются вручную в соответствующих полях; **DHCP** – автоматический способ задания IP параметров.
3	Адрес	IP-адрес интерфейса. Должен быть задан в соответствии с общепринятыми правилами распределения сетевых адресов. Параметр доступен только для ручного способа назначения IP-параметров.
4	Маска сети	Битовая маска подсети. Маска предназначена для определения по IP-адресу адреса подсети и адреса узла. Параметр доступен только для ручного способа назначения IP-параметров.
5	Шлюз	IP-адрес шлюза. Настраивается, если необходимо добавить маршрут «по умолчанию» в таблицу маршрутизации. Параметр доступен только для ручного способа назначения IP-параметров.
6	Широковещательный адрес	IP-адрес для передачи широковещательных пакетов в сеть. Вычисляется автоматически из IP-адреса и маски подсети или задается вручную. Например, для адреса 10.10.10.1 и маски подсети 255.255.255.0 значение широковещательного адреса будет 10.10.10.255. Параметр доступен только для ручного способа назначения IP-параметров.
7	Метрика	Приоритет маршрутов через интерфейс в таблице маршрутизации. Значение 0 – максимальный приоритет.
8	Собственные DNS сервера	Добавить IP-адреса DNS серверов.
9	Добавить маршрут по умолчанию	Параметр определяет, будет ли добавлен маршрут «0.0.0.0/0» в таблицу маршрутизации. Параметр доступен только для автоматического способа назначения IP параметров (DHCP).
10	Добавить DNS объявляемые узлом	Параметр определяет, будут ли добавлены IP-адреса DNS серверов объявляемые DHCP сервером.

		Параметр доступен только для автоматического способа назначения IP параметров (DHCP).
Интерфейс «sta0». Настройки межсетевого экрана		
1	Назначить зону сетевого экрана	Зона межсетевого экрана, к которой будет прикреплен интерфейс. Настройки зон находятся в меню ***«Статус → Межсетевой экран».*** Назначение зоны **«wan»** автоматически запрещает весь входящий трафик и включает NAT.

4.3 Сеть – Модем

4.3.1 Сеть – Модем – Общие

В меню находится раздел предназначенный для настройки LTE-модема. Для каждой SIM-карты используются свои настройки.

Настройки модема разбиты на нескольких частей - **«SIM1»**, **«SIM2»**, **«Дополнительные настройки»** (рис.4.3.1а,б). Каждая часть находится на своей вкладке. Вкладки **«SIM2»** и **«Дополнительные настройки»** могут отсутствовать, если устройство не поддерживает вторую SIM-карту.

Описание параметров представлено в таблице 4.3.1.

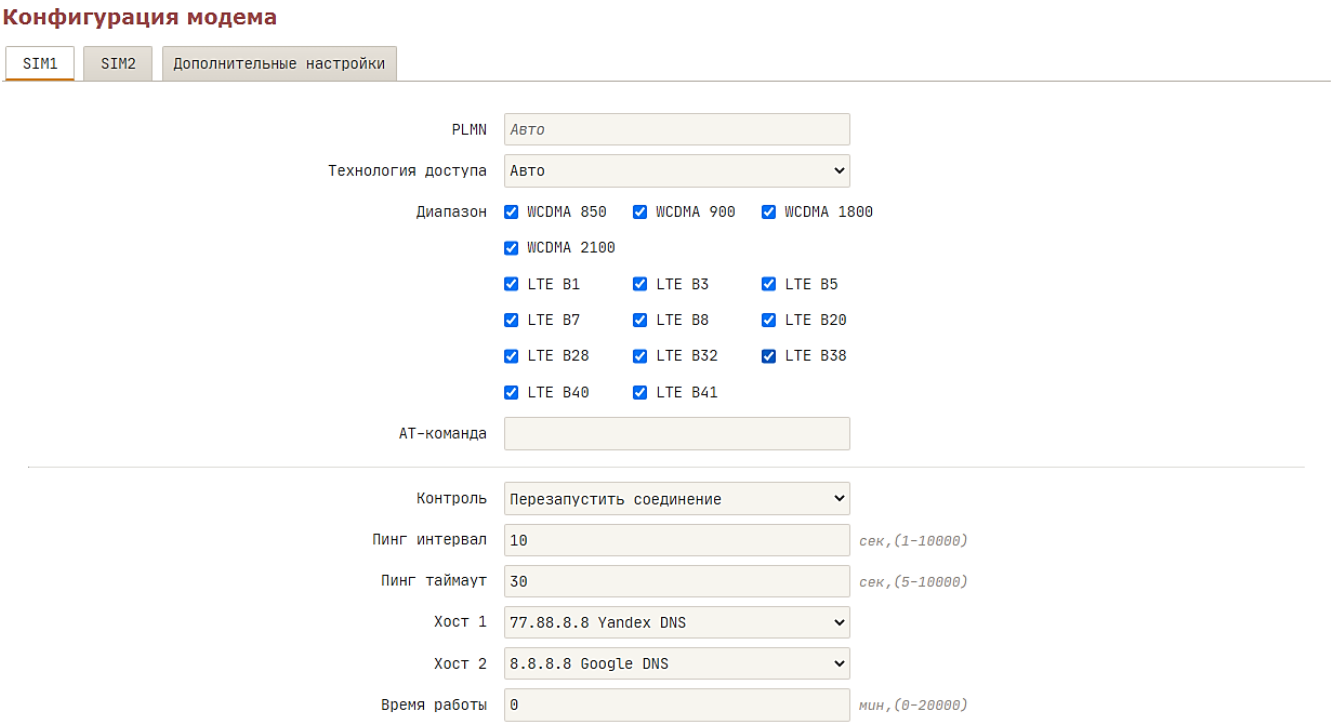


Рис.4.3.1а. Меню «Сеть – Модем – Общие». Вкладки «SIM1/SIM2»

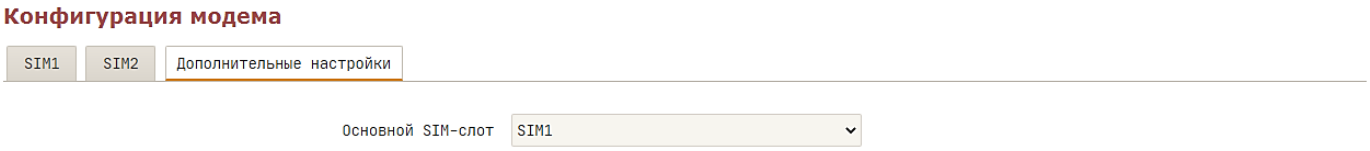


Рис.4.3.1б. Меню «Сеть – Модем – Общие». Вкладка «Дополнительные настройки»

Таблица 4.3.1. Описание параметров «Конфигурация модема»

№	Название поля	Описание
Конфигурация модема. SIM1/SIM2		
1	PLMN	Выбор предпочтительного мобильного оператора по его идентификатору PLMN. Например: 25001 (МТС) или 25020 (Tele2). Модем будет пытаться зарегистрироваться в сети в соответствии с указанным идентификатором PLMN. Если параметр пустой или 0, модем будет регистрироваться в автоматическом режиме, предпочитая домашнего оператора.
2	Технология доступа	Выбор технологии доступа. Возможные значения: **Авто** – модем будет пытаться последовательно зарегистрироваться в сетях LTE, 3G, 2G; **Только 2G** – модем будет регистрироваться только в сети 2G; **Только 3G** – модем будет регистрироваться только в сети 3G; **Только LTE** – модем будет регистрироваться только в сети LTE.
3	Диапазон	Выбор частотного диапазона. Параметр доступен, если установлен автоматический выбор технологии доступа.
4	AT-команда	Дополнительная AT-команда, которая будет автоматически выполняться сразу после применения основных настроек. Результат выполнения команды можно проконтролировать в **«Системном журнале»**.
5	Контроль	Включает/Отключает функцию **«Ping Check»**. Функция используется для автоматического

		переключения SIM-карт или контроля мобильного подключения. Для включения функции необходимо также задать IP-адрес **«Хост1»** и/или **«Хост2»**. Возможные значения: **Отключено** – функция отключена, нет контроля подключения; **Перезапустить соединение** – функция включена, при отсутствии пакетов от Хост 1 и/или Хост 2 будет выполнен перезапуск соединения; **Переключиться на SIM1/SIM2** – функция включена, при отсутствии пакетов от Хост 1 и/или Хост 2 будет выполнено переключения на другую SIM-карту. Доступно только для моделей с двумя SIM-картами.
6	Пинг интервал	Интервал (сек) отправки тестовых ICMP пакетов на Хост1, Хост2. Тестовые пакеты отправляются по очереди на Хост1 и Хост2, с половинным интервалом.
7	Пинг таймаут	Допустимый интервал (сек) ожидания ответов ICMP от Хост1, Хост2. Если по истечении интервала не было принято ни одного ответа, будет выполнено действие, заданное в параметре **«Контроль»**.
8	Хост 1	Первый IP-адрес, на который будут отправляться тестовые пакеты ICMP. Этот адрес должен быть доступен через интерфейс **«modem»**.
9	Хост 2	Второй IP-адрес, на который будут отправляться тестовые пакеты ICMP. Этот адрес должен быть доступен через интерфейс **«modem»**.
10	Время работы	Ограничение времени работы SIM-карты (минуты). Значение 0 – ограничение отключено. По истечении интервала будет выполнено действие, заданное в параметре **«Контроль»**. Параметр доступен только для моделей с двумя SIM-картами.
Конфигурация модема. Дополнительные настройки		
1	Основной SIM-слот	Задается SIM-карат после старта операционной системы роутера. Параметр доступен только для моделей с двумя SIM-картами.

4.3.1.1 Алгоритм работы функции «Ping Check»

Функция **«PingCheck»** предназначена для контроля мобильного подключения, автоматического перезапуска соединения и переключения между SIM-картами.

Роутер обеспечивает непрерывный контроль мобильного подключения путем отправки тестовых icmp пакетов до удаленных хостов. Тестовые пакеты отправляются через интерфейс **«modem»** на IP-адреса хостов 1 и 2 с постоянным интервалом, заданным в параметре **«Пинг»**. В случае если настроено 2 хоста для контроля, пакеты отправляются по очереди с половинным интервалом.

Если по истечении интервала **«Пинг таймаут»** не будет получено ни одного ответа на тестовые пакеты, роутер выполнит перезапуск мобильного соединения с физическим отключением от сотовой сети или переключение на другую SIM-карту в зависимости от настройки параметра **«Контроль»**.

После перезапуска соединения или переключения SIM-карты выдерживается фиксированный интервал 10 секунд, необходимый для повторной регистрации в сотовой сети и установки соединения, по истечении интервала начинается контроль подключения. Если после перезапуска соединения связь не восстановилась, то следующий перезапуск произойдет не раньше чем через одну минуту.

Для исключения ложных перезапусков или переключений, интервал **«Пинг таймаут»** должен быть больше интервала **«Пинг»** в 3 и более раз.

Для моделей с двумя SIM-картами, дополнительно можно задать лимит времени (параметр **«Время работы»**), по истечении которого будет выполнено действие, заданное в параметре **«Контроль»**. Если в параметре задано действие **«Переключится на SIM1/2»**, при этом SIM-карта отсутствует или не определяется, будет выполнено переключение на другую SIM-карту.

ПРИМЕР 1:

Контролировать подключение на SIM1, при отсутствии связи в течение 10 секунд, переключится на SIM2. Работать на SIM2 не более 30 минут, если нет связи в течение 20 секунд, переключится на SIM1.

Таблица 4.3.1.1а. Пример настройки функции «Ping Check»

Параметры	**Настройки для SIM1**	**Настройки для SIM2**
Контроль	Переключится на SIM2	Переключится на SIM1
Пинг	3	3
Пинг таймаут	10	20
Хост 1	8.8.8.8	8.8.8.4
Хост 2	8.8.8.8	77.88.8.8
Время работы	0	30

ПРИМЕР 2:

Контролировать подключение на SIM1, при отсутствии связи в течение 30 секунд, перезапустить соединение.

Таблица 4.3.1.1б. Пример настройки функции «Ping Check»

Параметры	Настройки для SIM1	Настройки для SIM2
Контроль	Перезапустить соединение	Отключено
Пинг	10	10
Пинг таймаут	30	30
Хост 1	8.8.8.8	
Хост 2	77.88.8.8	
Время работы	0	0

Тестирование

Для целей тестирования функции **«Ping Check»** можно воспользоваться АТ-командами:

AT+CFUN=4 - отключить радиопередатчик LTE-модема;
AT+CFUN=1 - включить радиопередатчик LTE-модема.

Ввод происходит в меню ***«Статус → Модем → АТ-команды»***. Для имитации отказа сотовой сети воспользуйтесь командой **AT+CFUN=4**.

В системном журнале регистрируются основные события, связанные с мобильной сетью, включая перезапуск соединения и переключения между SIM-картами. Служба, которая управляет мобильным подключением и управляет SIM-картами, создает записи в журнале с префиксом **«cm»**.

Пример системного журнала:

```
....
28 Nov 2022 10:37:01  daemon.info cm[748]:  Select SIM --> SIM1
28 Nov 2022 10:37:02  daemon.info cm[748]:  SIM1 detected: imsi=250206691454258 "ROSTELECOM", status=READY
28 Nov 2022 10:37:02  daemon.info cm[748]:  verification: mode=auto(24), band=w850 w900 w1800 w2100 b1 b3 b5 b7 b8 b20 b28 b32 b38 b40 b41, plmn=0
28 Nov 2022 10:37:03  daemon.info cm[748]:  SIM1, PS=detached, CS=detached, PLMN=25020, Radio=LTE, Reg=NOT REGISTERED, SEARCHING
28 Nov 2022 10:37:04  daemon.info cm[748]:  SIM1, PS=attached, CS=attached, PLMN=25020, Radio=LTE, Reg=REGISTERED
28 Nov 2022 10:37:06  daemon.info cm[748]:  activate PDN(ipv4): SIM1, apn="internet.tele2.ru"/""/""/none, WdsConnectionHandle=0x81ac4550
28 Nov 2022 10:37:07  daemon.info cm[748]:  CONNECTED: ipv4=12.140.106.220/255.255.255.248, ipv6=/, mtu=1460
....
```

4.3.2 Сеть – Модем – APN

В меню находится раздел предназначенный для настройки профиля **APN** (**A**ccess **P**oint **N**ame).

APN – это условное название точки доступа LTE/3G/2G мобильного оператора, через которую модем подключается к услуге передачи данных (Internet). От правильности настройки APN зависит стабильная работа и тарификация услуги. Профиль APN используется при регистрации модема в сети оператора и установке подключения.

Раздел состоит из двух подразделов – **«Профиль APN»** и **«Интерфейс modem»**.

Подраздел **«Профиль APN»** предназначен для настройки параметров APN и функции **«IP Passthrough»** (рис.4.3.2а). Настройки разбиты на нескольких частей - **«SIM1»**, **«SIM2»**. Вкладки **«SIM2»** может отсутствовать, если устройство не поддерживает вторую SIM-карту. При переключении SIM-карт, автоматически будут применяться настройки APN соответствующей SIM-карты. Функция **«Авто APN»** позволяет автоматически подставлять параметры APN из внутренней базы при инициализации подключения.

Подраздел **«Интерфейс modem»** предназначен для настройки IP-параметров интерфейса, который ассоциирован с профилем APN.

Подраздел состоит из двух частей — **«Основные настройки»** (рис.4.2.3б) и **«Настройки межсетевого экрана»** (рис.4.2.3в).

Описание параметров представлено в таблице 4.3.2.

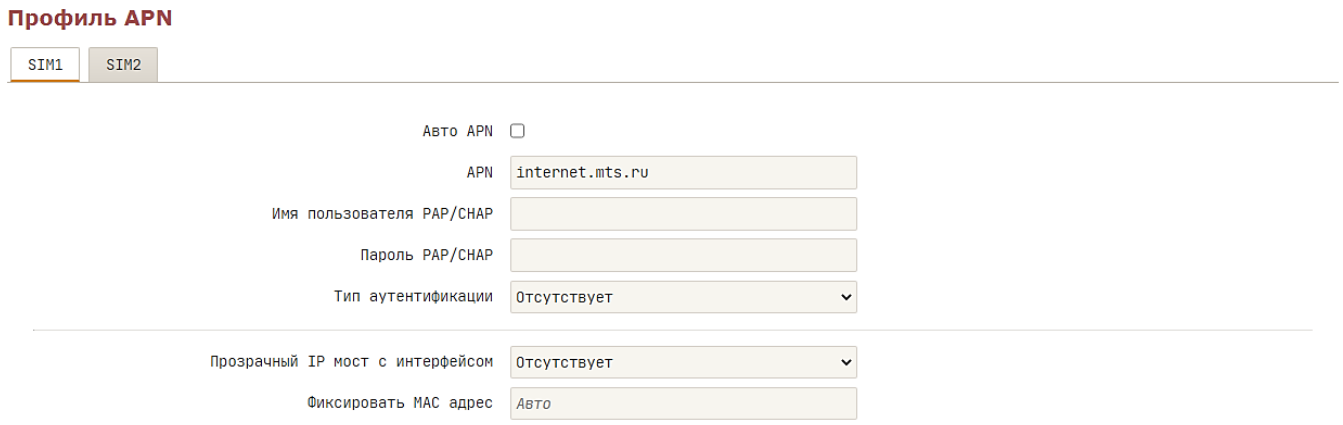


Рис.4.3.2а. Меню «Сеть – Модем – APN». Подраздел «Профиль APN». Вкладки «SIM1/SIM2»

Рис.4.3.2б. Меню «Сеть – Модем – APN. Подраздел «Интерфейс modem». Вкладка «Основные настройки»

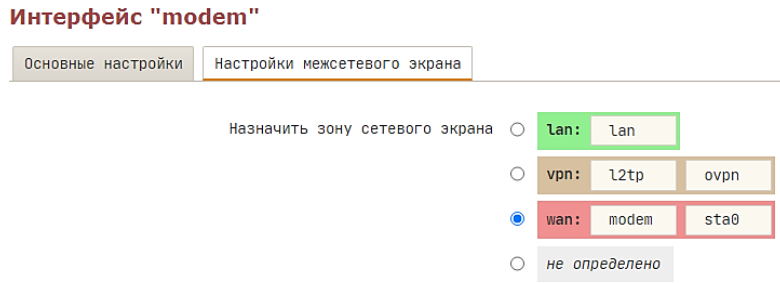


Рис.4.3.2в. Меню «Сеть – Модем – APN. Подраздел «Интерфейс modem». Вкладка «Основные настройки»

Таблица 4.3.2. Описание параметров «Профиль APN» и «Интерфейс modem»

№	Название поля	Описание
Профиль APN. SIM1/SIM2		
1	Авто APN	Включить/Отключить автоматическую подстановку настроек профиля APN (APN, имя пользователя, пароль, тип аутентификации) из внутренней базы данных. Для использования специфических услуг вроде «статический IP-адрес», требуется вручную задать эти настройки .

2	APN	Имя точки доступа оператора связи. Например: ***internet.mts.ru.***
3	Имя пользователя PAP/CHAP	Имя пользователя по протоколу аутентификации. Поле может быть пустым.
4	Пароль PAP/CHAP	Пароль по протоколу аутентификации. Поле может быть пустым.
5	Тип аутентификации	Выбор протокола аутентификации. Возможные значения: **Отсутствует** – подключение без аутентификации; **Pap** – аутентификация по протоколу Pap; **Chap** – аутентификация по протоколу Chap; **Pap и Chap** – аутентификация по протоколу Pap и Chap.
6	Прозрачный IP мост с интерфейсом	Включить/Отключить функцию **«IP Passthrough»**. Одновременно задается интерфейс для транзита трафика. Возможные значения: **Отсутствует** – функция отключена; **Lan** – функция включена, трафик с интерфейса **«modem»** перенаправляется в интерфейс **«lan»** и обратно. Интернет для роутера будет не доступен.
7	Фиксировать MAC адрес	Задается MAC-адрес узла, для которого будет выполняться перенаправление трафика в интерфейс **«modem»** и обратно. Для других узлов трафик будет обрабатываться как обычно. Если MAC-адрес узла не задан, роутер автоматически определит MAC-адрес и будет использовать его для транзита, при этом в сети **«lan»** больше не должно быть других узлов.
Интерфейс «modem». Основные настройки		
1	Включить	Включить/Отключить интерфейс. Параметр определяет, будет ли установлено подключение к сети в соответствии с настройками APN.
2	Добавить маршрут по умолчанию	Параметр определяет, будет ли добавлен маршрут **«0.0.0.0/0»** в таблицу маршрутизации.
3	Метрика	Приоритет маршрутов через интерфейс в таблице маршрутизации. Значение 0 – максимальный приоритет.
4	Добавить DNS объявляемые узлом	Параметр определяет, будут ли добавлены IP-адреса DNS серверов объявляемые мобильным оператором.
5	Собственные DNS сервера	Добавить IP-адреса DNS серверов.
Интерфейс «modem». Настройки межсетевого экрана		
1	Назначить зону сетевого экрана	Зона межсетевого экрана, к которой будет прикреплен интерфейс. Настройки зон находятся в меню ***«Статус → Межсетевой экран».*** Назначение зоны **«wan»** автоматически запрещает весь входящий трафик и включает NAT.

4.3.2.1 Алгоритм работы функции «IP Passthrough»

Функция **«IP Passthrough»** позволяет получать IP-конфигурацию (IP-адрес, шлюз, DNS) непосредственно на клиентском устройстве.

В этом случае за настройки IP отвечает прошивка LTE-модема, а роутер используется только для настройки параметров модема - APN, технология доступа, частотные диапазоны и т.д. Другими словами интерфейс **«lan»** будет объединен с интерфейсом **«modem»** специальным мостом, один конец которого будет обрабатывать кадры 802.3 (Ethernet), а другой конец – IP-кадры. Перехват и перенаправление кадров происходит до того момента как они обрабатываются межсетевым экранам, поэтому настройка межсетевого экрана не требуется. Для правильной работы мосту необходимо знать MAC-адрес хоста, который подключен со стороны **«lan»**. MAC-адрес может быть задан в параметре **«Фиксировать MAC адрес»** либо определен автоматически на основе поступающих пакетов.

Ключевые особенности:

- **«IP Passthrough»** будет работать только для одного хоста, если задан автоматический режим определения MAC-адреса хоста;
- **«IP Passthrough»** будет работать с несколькими хостами, но транзит трафика будет выполняться только для определенного MAC-адреса;
- Работает через Ethernet или Wi-Fi;
- Возможность использовать WEB-Интерфейс устройства с хоста, который используется для транзита;
- Если функция **«IP Passthrough»** активирована, роутер больше не может отправлять пакеты в интерфейс **«modem»** (кроме пакетов icmp функции **«Ping Check»**) соответственно никакие службы и утилиты, использующие этот интерфейс работать не будут;
- Транзит только IPv4 пакетов.

Не рекомендуется использовать с динамическими IP-адресами.

Вариант настройки для одного хоста, подключенного по Ethernet:

Шаг 1. Зайдите в WEB-интерфейс роутера по IP-адресу 192.168.1.1.

Шаг 2. В параметре **«Прозрачный IP мост с интерфейсом»** выберете интерфейс **«lan»**. Параметр **«Фиксировать MAC адрес»** оставьте пустым. Роутер должен быть подключен к мобильной сети, а интерфейс **«modem»** получить соответствующий IP-адрес.

Шаг 3. Отключить Wi-Fi в меню ***«Сеть → Wi-Fi → Общие»***.
Шаг 4. В настройках сетевой карты транзитного хоста задайте способ получения IP-адреса – DHCP. Сетевая карта должна автоматически получить IP-параметры (адрес, шлюз, DNS). IP-адрес, полученный сетевой картой, должен совпадать с IP-адресом интерфейса **«modem»**. На этом этапе, доступ к WEB-интерфейсу роутера будет не возможен. Для того что бы восстановить доступ к WEB-интерфейсу роутера смените IP-адрес и маску подсети сетевой карты на 192.168.1.2/255.255.255.0.

Вариант настройки для нескольких хостов, подключенных по Ethernet или Wi-Fi:

Только один хост используется для транзита трафика, другие хосты смогу получить доступ к WEB-интерфейсу роутера, но без доступа к сети Интернет.

Шаг 1. Зайдите в WEB-интерфейс роутера по IP-адресу 192.168.1.1.
Шаг 2. В параметре **«Прозрачный IP мост с интерфейсом»** выберете интерфейс **«lan»**. В параметре **«Фиксировать MAC адрес»** укажите MAC-адрес хоста для транзита. Роутер должен быть подключен к мобильной сети, а интерфейс **«modem»** получить соответствующий IP-адрес.
Шаг 3. В настройках сетевой карты транзитного хоста задайте способ получения IP-адреса – DHCP. Сетевая карта должна автоматически получить IP-параметры (адрес, шлюз, DNS). IP-адрес, полученный сетевой картой, должен совпадать с IP-адресом интерфейса **«modem»**. На этом этапе, доступ к WEB-интерфейсу роутера с транзитного хоста будет не возможен. Для того что бы восстановить доступ к WEB-интерфейсу роутера смените IP-адрес и маску подсети сетевой карты на 192.168.1.2/255.255.255.0. Остальные хосты, подключенные к роутеру через Ethernet или Wi-Fi, смогут получить доступа к WEB-Интерфейсу.

4.4 Сеть – VPN

4.4.1 Сеть – VPN – L2TP

В меню находится раздел предназначенный для настройки VPN клиента **L2TP** (**L**ayer **2** **T**unneling **P**rotocol). Настройки разбиты на две части **«Основные настройки»** и **«Настройки межсетевого экрана»** (рис.4.4.1а,б).

Описание параметров представлено в таблице 4.4.1.

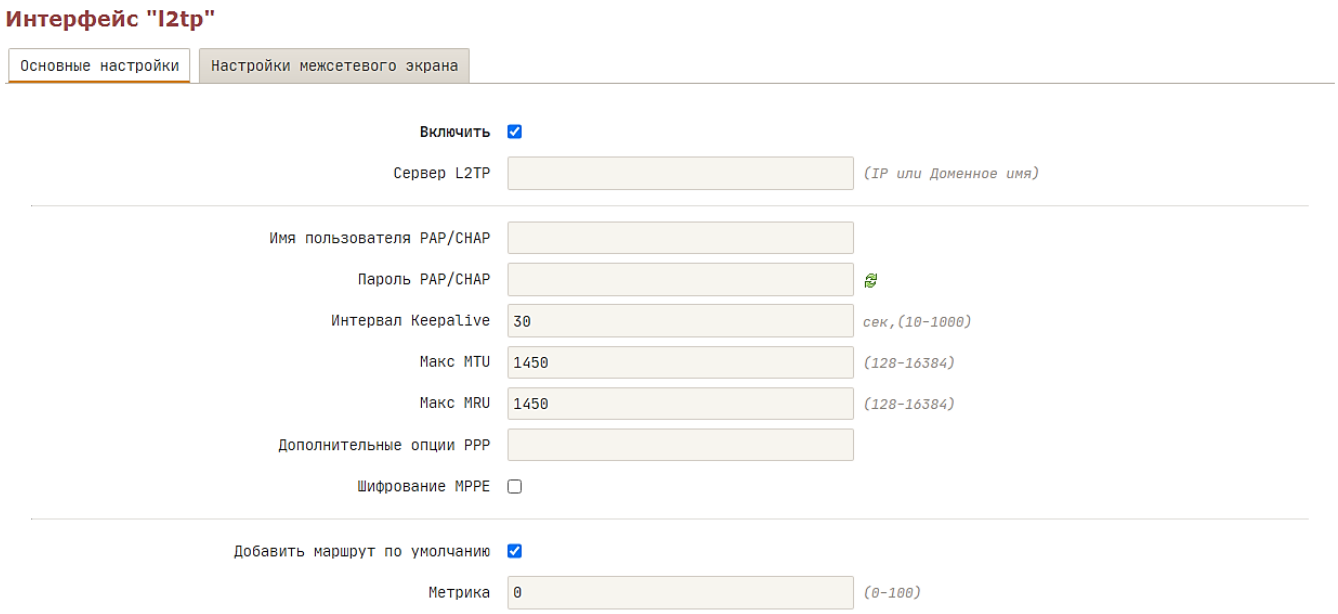


Рис.4.4.1а. Меню «Сеть – VPN – L2TP». Вкладки «Основные настройки»

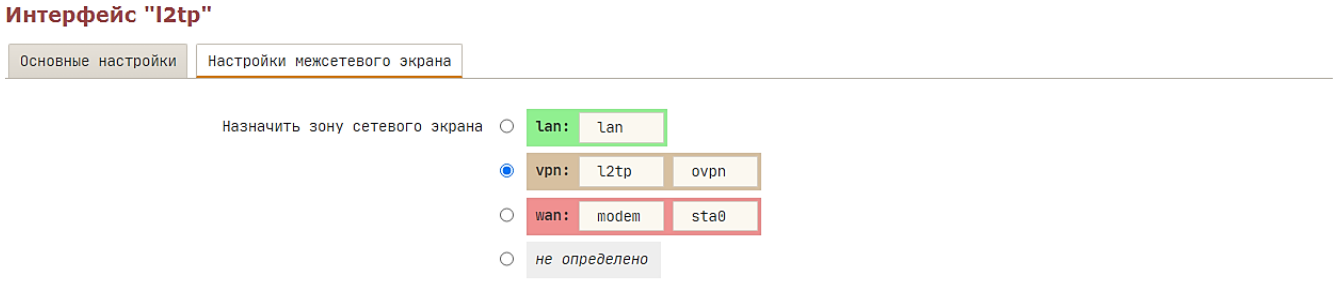


Рис.4.4.1б. Меню «Сеть – VPN – L2TP». Вкладка «Настройки межсетевого экрана»

Таблица 4.3.1. Описание параметров «Интерфейс l2tp»

№	Название поля	Описание
Интерфейс «l2tp». Основные настройки		
1	Включить	Включить/Отключить интерфейс.
2	Сервер L2TP	Доменное имя или IP-адрес удаленного узла (сервера), к которому будет подключаться L2TP клиент.
3	Имя пользователя PAP/CHAP	Имя пользователя для авторизации на сервере.
4	Пароль PAP/CHAP	Пароль для авторизации на сервере.
5	Интервал Keepalive	Параметр используется для контроля соединения с удаленной стороной, путем отправки LCP эхо запросов. Значение 0 – контроль будет отключен. Интервал Keepalive – это предельный интервал ожидания эхо запросов LCP, по истечении которого интерфейс **«l2tp»** будет перезапущен. Интервал отправки LCP эхо запросов равен Keepalive/5.
6	Макс MTU	**M**aximum **T**ransmission **U**nit. Максимальный размер пакета, который интерфейс **«l2tp»** сможет отправить без фрагментации пакета.
7	Макс MRU	**M**aximum **R**eceive **U**nit. Максимальный размер пакета, который интерфейс **«l2tp»** сможет получить без фрагментации пакета.
8	Дополнительные опции PPP	Передать дополнительные опции службе pppd.
9	Шифрование MPPE	Включить/Отключить шифрование MPPE. Настройка на клиенте должна совпадать с настройкой на сервере.

10	Добавить маршрут по умолчанию	Параметр определяет, будет ли добавлен маршрут **«0.0.0.0/0»** в таблицу маршрутизации.
11	Метрика	Приоритет маршрутов через интерфейс в таблице маршрутизации. Значение 0 – максимальный приоритет.
Интерфейс «l2tp». Настройки межсетевого экрана		
1	Назначить зону сетевого экрана	Зона межсетевого экрана, к которой вы хотите прикрепить этот интерфейс. Для этого интерфейса может быть выбрана зона **«vpn»**, если требуется разрешить маршрутизацию трафика в локальную сеть и обратно или зона **«wan»**, если VPN – туннель будет использоваться для перенаправления интернет трафика, в этом случае автоматически запрещается весь входящий трафик и включается NAT. Настройки зон находятся в меню ***«Статус → Межсетевой экран»***.

4.4.2 Сеть – VPN – OpenVPN

В меню находится раздел предназначенный для настройки VPN клиента OpenVPN (версия 2.5.3). Настройки разбиты на несколько частей – **«Основные настройки»**, **«Дополнительные настройки»**, **«Аутентификация»** и **«Настройки межсетевого экрана»**. Каждая часть находится на своей вкладке. Вкладка **«Аутентификация»** доступна, когда включена аутентификация **«Shared Secret»** или **«TLS Client»**.

Описание параметров представлено в таблице 4.4.2.

Пример конфигурации сервера и тестовые сертификаты https://github.com/Microdrive/openconfig.

Возможности:

- Создание VPN-туннеля типа «Точка-Точка» уровня L2/L3 с аутентификацией по общему секретному ключу (Shared Key), с шифрованием или без шифрования;
- Создание VPN-туннеля типа «Сеть» уровня L2/L3 с аутентификацией TLS при помощи сертификатов и закрытых ключей (TLS-клиент). Дополнительная аутентификация по логину и/или паролю. Дополнительная аутентификация и шифрование канала управления TLS при помощи общего закрытого ключа;
- Перенаправление интернет трафика через туннель. Конфигурация VPN-шлюз;
- Транспортный протокол – UDP или TCP.

Таблица 4.4.2. Описание параметров «Интерфейс ovpn»

№	Название поля	Описание	Опция OpenVPN
Интерфейс «ovpn». Основные настройки			
1	Включить	Включить/Отключить интерфейс.	**-**
2	TUN/TAP	Выбор типа кадров при инкапсуляции. TUN (L3) – инкапсулируются кадры IPv4, TAP (L2) – инкапсулируются кадры 802.3 (Ethernet).	***dev***
3	Сетевой мост	Параметр определяет, будет ли добавлен интерфейс в соответствующий сетевой мост. Параметр доступен только для режима TAP.	**-**
4	Транспортный протокол	Выбор транспортного протокола. Возможные значения: **UDP** – в качестве транспорта используется UDP протокол; **TCP** – в качестве транспорта используется TCP протокол.	***proto, tcp-client***
5	Сервер OPENVPN	Доменное имя или IP-адрес удаленного узла (сервера), к которому будет подключаться OpenVPN клиент.	***remote***
6	Порт	Порт удаленного узла (сервера)	***port***
7	Сжатие	Выбор алгоритма сжатия. Возможные значения: **По умолчанию** – клиент OpenVPN использует настройки по умолчанию (рекомендуется); **Отключено** – сжатие отключено, должно совпадать с настройкой на сервере; **LZO** – используется алгоритм сжатия LZO, должен совпадать с настройкой на сервере; **LZ4** – используется алгоритм сжатия LZ4, должен совпадать с настройкой на сервере; Если используется подключение типа «Сеть», то сервер может переопределить значение этой опции при подключении.	***compress***
8	Интервал Keepalive	Параметр используется для контроля соединения с удаленной стороной, путем отправки эхо запросов. Значение 0 – контроль будет отключен. Интервал Keepalive – это предельный интервал ожидания эхо запросов, по истечении которого интерфейс **«ovpn»** будет перезапущен. Интервал отправки эхо запросов равен Keepalive/5. Если используется подключение типа «Сеть», то сервер может переопределить	***keepalive***

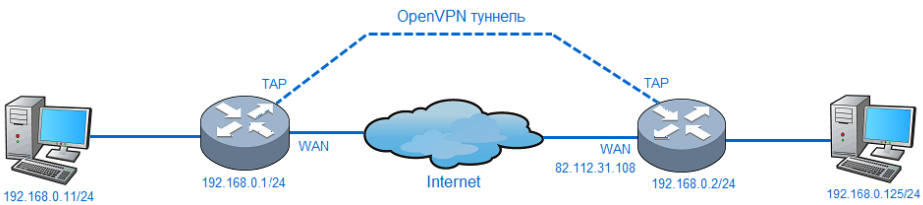
		значение этой опции при подключении.	
9	Аутентификация	Выбор метода аутентификации и топологии сети. Возможные значения: **Отключено** – подключение типа «Точка-Точка» без аутентификации и шифрования; **Shared Secret** – подключение типа «Точка-Точка», аутентификация с общим ключом; **TLS Client** – подключение типа «Сеть», аутентификация с помощью сертификатов и/или пароля.	***secret, tls-client***
10	Шифрование	Выбор алгоритма шифрования канала передачи данных. Возможные значения: **По умолчанию** – значение по умолчанию AES-128-CBC; **Отключено** – шифрование не используется; **AES-128-CBC** – алгоритм шифрования AES-128-CBC; **AES-128-CFB** – алгоритм шифрования AES-128-CFB; **AES-128-CFB1** – алгоритм шифрования AES-128-CFB1; **AES-128-CFB8** – алгоритм шифрования AES-128-CFB8; **AES-128-GCM** – алгоритм шифрования AES-128-GCM; **AES-128-OFB** – алгоритм шифрования AES-128-OFB; **AES-192-CBC** – алгоритм шифрования AES-192-CBC; **AES-192-CFB** – алгоритм шифрования AES-192-CFB; **AES-192-CFB1** – алгоритм шифрования AES-192-CFB1; **AES-192-CFB8** – алгоритм шифрования AES-192-CFB8; **AES-192-GCM** – алгоритм шифрования AES-192-GCM; **AES-192-OFB** – алгоритм шифрования AES-192-OFB; **AES-256-CBC** – алгоритм шифрования AES-256-CBC; **AES-256-CFB** – алгоритм шифрования AES-256-CFB; **AES-256-CFB1** – алгоритм шифрования AES-256-CFB1; **AES-256-CFB8** – алгоритм шифрования AES-256-CFB8; **AES-256-GCM** – алгоритм шифрования AES-256-GCM; **AES-256-OFB** – алгоритм шифрования AES-256-OFB; **CHACHA20-POLY1305** – алгоритм шифрования CHACHA20-POLY1305; **BF-CBC** – алгоритм шифрования BF-CBC. Если используется подключение типа «Сеть», то сервер может переопределить значение этой опции при подключении.	***ciphers, data-ciphers***
11	Алгоритм аутентификации	Выбор алгоритма аутентификации. Возможные значения: **По умолчанию** – значение по умолчанию SHA1; **Отключено** – аутентификация не используется; **SHA1** – метод аутентификации SHA1; **SHA256** – метод аутентификации SHA256; **SHA512** – метод аутентификации SHA512. Если используется подключение типа «Сеть», то сервер может переопределить значение этой опции при подключении.	***auth***
12	Локальный VPN адрес	IP-адрес виртуального интерфейса **«ovpn»**. Параметр доступен только для аутентификации Shared Secret.	***ifconfig_l***
13	Удаленный VPN адрес	IP-адрес удаленной стороны. Параметр доступен только для аутентификации Shared Secret в режиме TUN.	***ifconfig_r***
14	Маска сети VPN	Маска виртуального интерфейса **«ovpn»**. Параметр доступен только для аутентификации Shared Secret в режиме TAP.	***ifconfig***
Интерфейс «ovpn». Дополнительные настройки			
1	Дополнительная конфигурация	Задаются дополнительные опции клиенту OpenVPN, которые будут добавлены к основной конфигурации при запуске интерфейса. Опция **«verb 3»** задает 3-ий уровень информационных сообщений в системном журнале.	
Интерфейс «ovpn». Аутентификация			
1	Общий ключ (secret.key)	Общий ключ для шифрования соединения типа «Точка-Точка». Ключ должен включать заголовок и окончание: -----BEGIN OpenVPN Static key V1----- … -----END OpenVPN Static key V1----- Параметр доступен только для аутентификации Shared Secret.	***secret***
2	Сертификат CA (ca.crt)	Сертификат удостоверяющего центра. Сертификат должен включать заголовок и окончание: -----BEGIN CERTIFICATE-----	**ca**

		… -----END CERTIFICATE----- Параметр доступен только для аутентификации TLS Client.	
3	Сертификат клиента (client.crt)	Подписанный сертификат клиента. Содержит открытый ключ и дополнительные атрибуты: имя клиента, срок действия и др. Должен заканчиваться: -----END CERTIFICATE----- Параметр доступен только для аутентификации TLS Client.	***cert***
4	Ключ клиента (client.key)	Закрытый ключ клиента. Ключ должен включать заголовок и окончание: -----BEGIN PRIVATE KEY----- … -----END PRIVATE KEY----- Параметр доступен только для аутентификации TLS Client.	***key***
5	Логин	Дополнительная аутентификация по логину и паролю. Параметр доступен только для аутентификации TLS Client.	-
6	Пароль	Дополнительная аутентификация по логину и паролю. Параметр доступен только для аутентификации TLS Client.	-
7	TLS Аутентификация/Шифрование	Задается дополнительный уровень аутентификации или шифрования канала управления TLS. Возможные значения: **Отключено** - дополнительная аутентификация и шифрование канала управления TLS отключено; **Аутентификация** – аутентификация без шифрования, направление ключа не задано; **Аутентификация, key-direction 0** – аутентификация без шифрования, направление ключа – 0; **Аутентификация, key-direction 1** – аутентификация без шифрования, направление ключа – 1; **Шифрование** – аутентификация и шифрование. Если на сервере задано направление ключа 1 (опция **key-direction 1**), то на клиенте должно быть задано 0 и на оборот. Параметр доступен только для аутентификации TLS Client.	***tls-auth, tls-crypt keydirection***
8	Ключ (ta.key)	Общий ключ для шифрования канала управления TLS. Ключ должен включать заголовок и окончание: -----BEGIN OpenVPN Static key V1----- … -----END OpenVPN Static key V1----- Параметр доступен только для аутентификации TLS Client.	***tls-auth, tls-crypt***
Интерфейс «ovpn». Настройки межсетевого экрана			
1	Назначить зону сетевого экрана	Зона межсетевого экрана, к которой вы хотите прикрепить этот интерфейс. Для этого интерфейса может быть выбрана зона **«vpn»**, если требуется разрешить маршрутизацию трафика в локальную сеть и обратно или зона **«wan»**, если VPN – туннель будет использоваться для перенаправления интернет трафика, в этом случае автоматически запрещается весь входящий трафик и включается NAT. Настройки зон находятся в меню ***«Статус → Межсетевой экран»***.	

4.4.2.1 Настройка туннеля L2 типа «Точка-Точка» с аутентификацией по общему ключу (Shared Secret)

В конфигурации туннеля типа «Точка-Точка» одно из устройств должно выступать в роли сервера и иметь статический общедоступный IP-адрес (белый IP). Второе устройство, выполняющее роль клиента, может иметь динамический IP-адрес и работать за NAT. Кадры 802.3 (Ethernet, Wi-Fi) могут свободно проходить между хостами 192.168.0.11 и 192.168.0.125, а также другими хостами в сети 192.168.0.0/24. В настройках межсетевого экрана, на стороне сервера, необходимо отрыть соответствующий порт для приема входящего соединения от клиента.

Пример топологии показан на рис.4.4.2.1. Пример настройки приведен в таблице 4.4.2.1.



4.4.2.1. *Пример топологии «Точка-Точка»*, уровень L2

Таблица 4.4.2.1. Пример настройки для топологии «Точка-Точка»

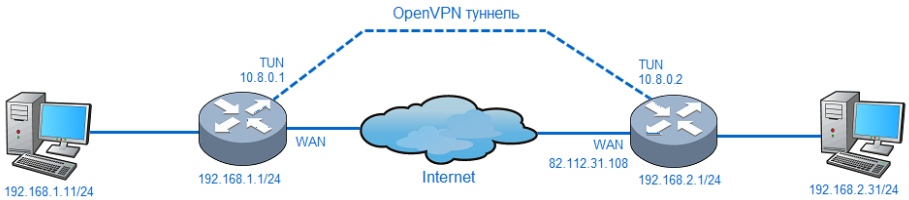
Параметры	**Клиент**	**Сервер**
TUN/TAP	TAP (L2)	TAP (L2)
Сетевой мост	**«lan»**	**«lan»**
Транспортный протокол	Может быть UDP или TCP	Может быть UDP или TCP
Сервер OPENVPN	82.112.31.108	Оставить пустым
Порт	1194	1194
Сжатие	По умолчанию	По умолчанию
Интервал Keepalive	30	30
Аутентификация	Shared Secret	Shared Secret
Шифрование	CHACHA20-POLY1305 или любой другой	CHACHA20-POLY1305 или любой другой
Алгоритм аутентификации	SHA1	SHA1
Локальный VPN IP	Оставить пустым, если интерфейс добавлен в сетевой мост	Оставить пустым, если интерфейс добавлен в сетевой мост
Маска сети VPN	Оставить пустым, если интерфейс добавлен в сетевой мост	Оставить пустым, если интерфейс добавлен в сетевой мост
Аутентификация		
Общий ключ (secret.key)	Содержимое файла с общим ключом	Содержимое файла с общим ключом
Настройки межсетевого экрана		
Назначить зону сетевого экрана	Зона **«lan»**	Зона **«lan»**

192.168.0.11/24 – IP-адрес хоста за клиентом;
192.168.0.1/24 – IP-адрес интерфейса сетевого моста **«lan»** клиента, в который добавлен TAP-интерфейс OpenVPN, IP-адрес необходим, что бы иметь доступ к устройству из сети 192.168.0.0/24;
192.168.0.125/24 – IP-адрес хоста за сервером;
192.168.0.2/24 – IP-адрес интерфейса сетевого моста **«lan»** сервера, в который добавлен TAP-интерфейс OpenVPN, IP-адрес необходим, что бы иметь доступ к устройству из сети 192.168.0.0/24;
82.112.31.108 – IP-адрес WAN интерфейса сервера.

4.4.2.2 Настройка туннеля L3 типа «Точка-Точка» с аутентификацией по общему ключу (Shared Secret)

В конфигурации туннеля типа «Точка-Точка» одно из устройств должно выступать в роли сервера и иметь статический общедоступный IP-адрес (белый IP). Второе устройство, выполняющее роль клиента, может иметь динамический IP-адрес и работать за NAT. В настройках межсетевого экрана, на стороне сервера, необходимо отрыть соответствующий порт для приема входящего соединения от клиента. Для доступа к сетям за клиентом, на стороне сервера необходимо добавить статические маршруты через интерфейс **«ovpn»**. Для доступа к сетям за сервером, на стороне клиента необходимо добавить статические маршруты через интерфейс **«ovpn»**.

Пример топологии показан на рис.4.4.2.2. Пример настройки приведен в таблице 4.4.2.2.



4.4.2.2. *Пример топологии «Точка-Точка»*, уровень L3

Таблица 4.4.2.2. Пример настройки для топологии «Точка-Точка»

Параметры	**Клиент**	**Сервер**
TUN/TAP	TUN (L3)	TUN (L3)
Транспортный протокол	Может быть UDP или TCP	Может быть UDP или TCP
Сервер OPENVPN	82.112.31.108	Оставить пустым
Порт	1194	1194
Сжатие	По умолчанию	По умолчанию

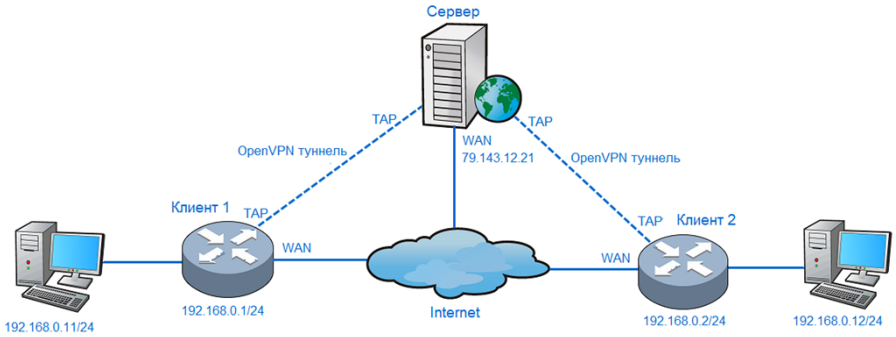
Интервал Keepalive	30	30
Аутентификация	Shared Secret	Shared Secret
Шифрование	CHACHA20-POLY1305 или любой другой	CHACHA20-POLY1305 или любой другой
Алгоритм аутентификации	SHA1	SHA1
Локальный VPN IP	10.8.0.1	10.8.0.2
Удаленный VPN адрес	10.8.0.2	10.8.0.1
Аутентификация		
Общий ключ (secret.key)	Содержимое файла с общим ключом	Содержимое файла с общим ключом
Настройки межсетевого экрана		
Назначить зону сетевого экрана	Зона **«lan»** или **«vpn»**	Зона **«lan»** или **«vpn»**

192.168.1.11/24 – IP-адрес хоста за клиентом;
192.168.1.1/24 – IP-адрес интерфейса сетевого моста **«lan»** клиента;
192.168.2.31/24 – IP-адрес хоста за сервером;
192.168.2.1/24 – IP-адрес интерфейса сетевого моста **«lan»** сервера;
10.8.0.1 – IP-адрес интерфейса **«ovpn»** клиента;
10.8.0.2 – IP-адрес интерфейса **«ovpn»** сервера;
82.112.31.108 – IP-адрес WAN интерфейса сервера.

4.4.2.3 Настройка туннеля L2 типа «Сеть» с аутентификацией TLS

В конфигурации туннеля типа «Сеть» должен присутствовать сервер со статическим общедоступным IP-адресом. К серверу будут подключаться клиенты, которые могут иметь динамический IP-адрес и работать за NAT. В настройках межсетевого экрана, на стороне сервера, необходимо отрыть соответствующий порт для приема входящих соединений от клиентов. Кадры 802.3 (Ethernet) могут свободно проходить между хостами, расположенными за клиентами, через центральный сервер (сервер выполняет функцию сетевого моста). В конфигурации сервера следуют отключить функцию присвоения IP-адресов для клиентов (опция ***server-bridge*** без параметров).

Пример топологии показан на рис.4.4.2.3. Пример настройки приведен в таблице 4.4.2.3.



4.4.2.3. *Пример топологии «Сеть»*, уровень L2

Таблица 4.4.2.3. Пример настройки клиента для топологии «Сеть»

Параметры	**Клиент**
TUN/TAP	TAP (L2)
Сетевой мост	**«lan»**
Транспортный протокол	Может быть UDP или TCP
Сервер OPENVPN	79.143.12.21
Порт	1194
Сжатие	По умолчанию
Интервал Keepalive	30, может быть переопределено сервером
Аутентификация	TLS Client
Шифрование	AES-128-CBC, может быть переопределено сервером
Алгоритм аутентификации	SHA1, может быть переопределено сервером
Аутентификация	
Сертификат CA (ca.crt)	Содержимое файла корневого сертификата

Сертификат клиента (client.crt)	Содержимое файла с сертификатом клиента
Ключ клиента (client.key)	Содержимое файла с ключом клиента
Логин	Оставить пустым, если сервер не запрашивает логин и пароль
Пароль	Оставить пустым, если сервер не запрашивает логин и пароль
TLS Аутентификация/ Шифрование	Отключено, если не требуется аутентификация и шифрование канала управления
Ключ (ta.key)	Содержимое файла с общим ключом, если включена аутентификация/шифрование TLS
Настройки межсетевого экрана	
Назначить зону сетевого экрана	Зона **«lan»** или **«vpn»**

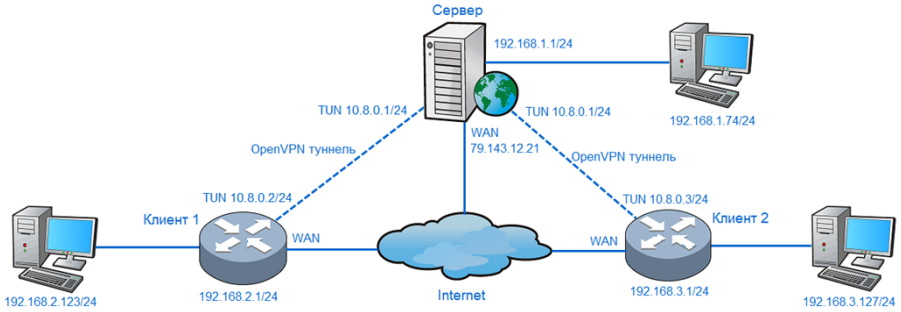
192.168.0.11/24 – IP-адрес хоста за клиентом 1;
192.168.0.12/24 – IP-адрес хоста за клиентом 2;
192.168.0.1/24 – IP-адрес интерфейса сетевого моста **«lan»** клиента 1;
192.168.0.2/24 – IP-адрес интерфейса сетевого моста **«lan»** клиента 2;
79.143.12.21 – IP-адрес WAN интерфейса сервера.

4.4.2.4 Настройка туннеля L3 типа «Сеть» с аутентификацией TLS

В конфигурации туннеля типа «Сеть» должен присутствовать сервер со статическим общедоступным IP-адресом. К серверу будут подключаться клиенты, которые могут иметь динамический IP-адрес и работать за NAT. В настройках межсетевого экрана, на стороне сервера, необходимо отрыть соответствующий порт для приема входящих соединений от клиентов.

Если требуется маршрутизировать трафик между хостами в сети за клиентами (через сервер), то в индивидуальных конфигурациях для клиентов на стороне сервера, нужно добавить соответствующие маршруты (опция ***iroute***). Опция ***iroute*** имеет двойное назначение. Опция сообщает серверу, какие сети есть за клиентами, а также выдает всем клиентам информацию о сетях за другими клиентами. Таким образом, нет необходимости вручную добавлять статические маршруты на стороне клиентов.

Пример топологии показан на рис.4.4.2.4. Пример настройки приведен в таблице 4.4.2.4.



4.4.2.4. *Пример топологии «Сеть»*, уровень L3

Таблица 4.4.2.4. Пример настройки клиента для топологии «Сеть»

Параметры	**Клиент**
TUN/TAP	TUN (L3)
Транспортный протокол	Может быть UDP или TCP
Сервер OPENVPN	79.143.12.21
Порт	1194
Сжатие	По умолчанию
Интервал Keepalive	30, может быть переопределено сервером
Аутентификация	TLS Client
Шифрование	AES-128-CBC, может быть переопределено сервером
Алгоритм аутентификации	SHA1, может быть переопределено сервером
Аутентификация	
Сертификат CA (ca.crt)	Содержимое файла корневого сертификата
Сертификат клиента (client.crt)	Содержимое файла с сертификатом клиента

Ключ клиента (client.key)	Содержимое файла с ключом клиента
Логин	Оставить пустым, если сервер не запрашивает логин и пароль
Пароль	Оставить пустым, если сервер не запрашивает логин и пароль
TLS Аутентификация/ Шифрование	Отключено, если не требуется аутентификация и шифрование канала управления
Ключ (ta.key)	Содержимое файла с общим ключом, если включена аутентификация/шифрование TLS
Настройки межсетевого экрана	
Назначить зону сетевого экрана	Зона **«lan»** или **«vpn»**

192.168.2.123/24 – IP-адрес хоста за клиентом 1;
192.168.3.127/24 – IP-адрес хоста за клиентом 2;
192.168.1.74/24 – IP-адрес хоста за сервером;
192.168.1.1/24 – IP-адрес интерфейса LAN сервера;
10.8.0.1/24 – IP-адрес интерфейса TUN OpenVPN Сервера;
10.8.0.2/24 – IP-адрес интерфейса **«ovpn»** клиента 1;
10.8.0.3/24 – IP-адрес интерфейса **«ovpn»** клиента 2;
192.168.2.1/24 – IP-адрес интерфейса сетевого моста **«lan»** клиента 1;
192.168.3.1/24 – IP-адрес интерфейса сетевого моста **«lan»** клиента 2;
79.143.12.21 – IP-адрес WAN интерфейса сервера.

IP-адреса клиентов в виртуальной сети 10.8.0.0/24 и маршруты до сетей за клиентами, должен выдавать сервер. IP-адреса сетей за клиентами и сервером должны быть уникальными.

4.4.2.5 Настройка туннеля L2/L3 типа «Сеть» с аутентификацией по логину и паролю

В этой конфигурации не требуется создание клиентских сертификатов и ключей, но все еще требуется общий корневой сертификат (CA). Настройка производится как в 4.4.2.3 или 4.4.2.4, но сертификат клиента и ключ клиента не добавляются, при этом обязательно требуется указывать логин и пароль. Логин будет использоваться сервером в качестве параметра **«Common Name»** для идентификации клиента и передачи ему соответствующих настроек.

4.4.2.6 OpenVPN шлюз

Конфигурация VPN-шлюз используется для перенаправления Интернет трафика через интерфейс **«ovpn»**. Топология сети может быть «Точка-Точка» или «Сеть».

Для топологии «Точка-Точка», следует добавить 2 статических маршрута в меню ***«Сеть → Статические маршруты»***.

1. Прямой маршрут до удаленного узла (сервера):

Параметры	**Клиент**
Интерфейс	**«modem» или другой WAN интерфейс**
Цель	IP-адрес сервера
Маска сети	255.255.255.255
Шлюз	Оставить пустым
Метрика	0

2. Маршрут «0.0.0.0/0»:

Параметры	**Клиент**
Интерфейс	**«ovpn»**
Цель	0.0.0.0
Маска сети	0.0.0.0
Шлюз	Оставить пустым, если сеть уровня L3 или указать IP-адрес шлюза, если сеть уровня L2
Метрика	0

Для топологии «Сеть», маршруты для перенаправления Интернет трафика будут добавлены автоматически, если в конфигурации сервера задана опция ***push "redirect-gateway def1"***.

Зона межсетевого экрана может быть изменена на **«wan»**, если требуется маскировать локальную сеть (NAT) и запретить входящий трафик.

4.4.3 Сеть – VPN – GRE

В меню находится раздел предназначенный для добавления/удаления интерфейсов GRE (**G**eneric **R**outing **E**ncapsulation) (рис.4.4.3а).

Для создания нового интерфейса необходимо нажать кнопку **«ДОБАВИТЬ»,** для редактирования уже созданного интерфейса необходимо нажать кнопку **«РЕДАКТИРОВАТЬ»**, далее заполнить необходимые поля (рис.4.4.3б) и сохранить изменения, нажав кнопку **«СОХРАНИТЬ»**. Для удаления интерфейса необходимо нажать кнопку **«УДАЛИТЬ»**, а потом кнопку **«СОХРАНИТЬ»**.

Описание параметров представлено в таблице 4.4.3а и 4.4.3б.

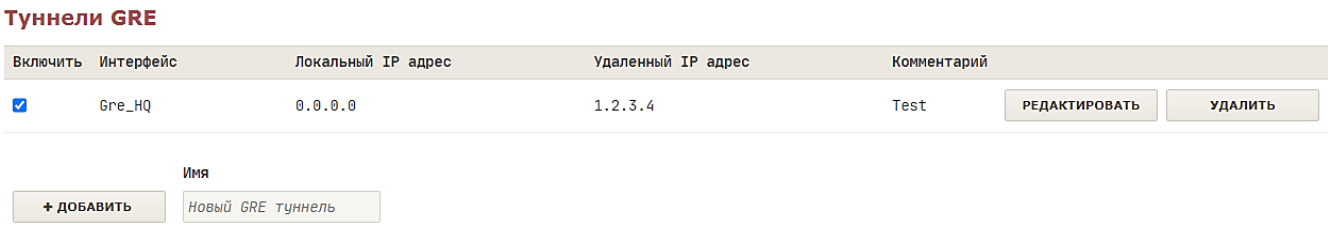


Рис.4.4.3а. Меню «Сеть – VPN – GRE». Интерфейс GRE с именем «Gre_HQ»

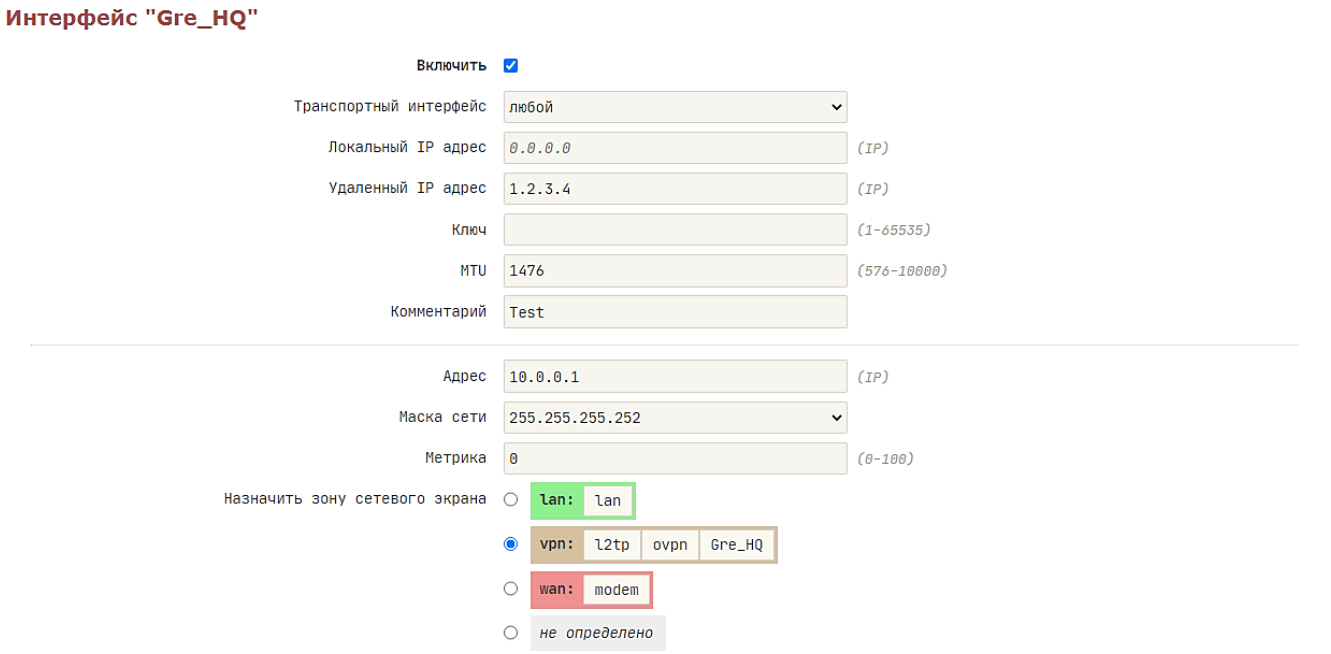


Рис.4.4.3б. Меню «Сеть – VPN – GRE». Редактирование интерфейса «Gre_HQ»

Таблица 4.4.3а. Описание параметров «Туннели GRE»

№	Название поля	Описание
Туннели GRE		
1	Включить	Включить/Отключить интерфейс.
2	Интерфейс	Имя туннельного интерфейса GRE.
3	Локальный IP адрес	IP-адрес локального конца туннеля, если задано значение 0.0.0.0, то локальный IP-адрес будет назначен автоматически.
4	Удаленный IP адрес	IP-адрес удаленного конца туннеля. Обязательный параметр.
5	Комментарий	Текстовый комментарий.

Таблица 4.4.3б. Описание параметров «Интерфейс <имя интерфейса>»

№	Название поля	Описание
Интерфейс <имя интерфейса>		
1	Включить	Включить/Отключить интерфейс.
2	Транспортный интерфейс	Выбрать интерфейс, через который будет проходить трафик GRE. Работа интерфейса GRE будет синхронизирована с работой транспортного интерфейса, если транспортный интерфейс будет остановлен, то и интерфейс GRE будет остановлен. Если **«Локальный IP адрес»** не задан или

		задано значение 0.0.0.0, то в качестве локального IP-адреса будет использоваться IP-адрес транспортного интерфейса.
3	Локальный IP адрес	IP-адрес локального конца туннеля, если задано значение 0.0.0.0, то локальный IP-адрес будет назначен автоматически.
4	Удаленный IP адрес	IP-адрес удаленного конца туннеля. Обязательный параметр.
5	Ключ	Идентификатор туннеля, используется, если через один транспортный интерфейс может проходить несколько GRE туннелей. Идентификатор туннеля должен быть одинаковым на обеих сторонах.
6	MTU	MTU (Maximum Transmission Unit) интерфейса GRE. Параметр определяет максимальный размер пакета данных через этот интерфейс. Должен быть меньше MTU транспортного интерфейса на 24 байта (заголовок IP + заголовок GRE).
7	Комментарий	Текстовый комментарий.
8	Адрес	IP-адрес, который будет назначен интерфейсу GRE. Должен быть задан в соответствии с общепринятыми правилами распределения сетевых адресов.
9	Маска сети	Битовая маска подсети интерфейса GRE.
10	Метрика	Приоритет маршрутов через интерфейс GRE в таблице маршрутизации. Значение 0 – максимальный приоритет.
11	Назначить зону сетевого экрана	Зона межсетевого экрана, к которой будет прикреплен интерфейс. Рекомендуется использовать зону **«vpn»** или **«lan»**. Настройки зон находятся в меню ***«Статус → Межсетевой экран»***.

4.5 Сеть – DHCP/DNS

В меню находится раздел предназначенный для настройки службы DHCP/DNS. Служба DHCP/DNS выполняет функции DHCP сервера и DNS сервера одновременно.

DCHP сервер предназначен для автоматического распределения IP-адресов между узлами сети. Помимо IP-адреса, DHCP сервер также может сообщать клиенту дополнительные параметры, необходимые для нормальной работы в сети (IP-адрес шлюза, IP-адрес DNS и другие параметры). Эти параметры называются опциями DHCP. Список стандартных опций можно найти в RFC 2132. IP-адреса, выданные в аренду, доступны для просмотра в меню ***«Статус → DHCP»***.

Распределение IP-адресов возможно двумя способами – динамическое распределение и статическое распределение. При динамическом распределении, каждому клиенту выделяется IP-адрес из пула свободных IP-адресов. Адрес выделяется динамически на определенный срок, это называется арендой адреса. По истечении аренды, клиенты должны снова запросить IP-адрес при этом IP-адрес может быть другим. При статическом распределении, IP-адрес строго закрепляется за определенным клиентом, при этом клиенты идентифицируются как по MAC-адресу, так и по имени (*Hostname*).

DNS сервер предназначен для преобразования доменных имен в IP-адрес узла.

Настройки службы DHCP/DNS разбиты на 3 раздела **«Общие»**, **«Постоянные аренды DHCP»** и **«Локальный DNS»**.

4.5.1 Сеть – DHCP/DNS – Общие

В меню находится раздел предназначенный для настройки основных параметров службы DHCP/DNS.

Раздел разбит на два подраздела **«Настройки DHCP/DNS сервера»** и **«DHCP Пул»** (рис.4.5.1а,б).

Описание параметров представлено в таблице 4.5.1.

Рис.4.5.1а. Меню «Сеть – DHCP/DNS – Общие». Подраздел «Настройки DHCP/DNS сервера»

Рис.4.5.1б. Меню «Сеть – DHCP/DNS – Общие». Подраздел «DHCP Пул»

Таблица 4.5.1. Описание параметров «Настройки DHCP/DNS сервера» и «DHCP Пул»

№	Название поля	Описание
Настройки DHCP/DNS сервера		
1	Включить	Включить/Отключить службу DHCP/DNS.
2	Авторитетный режим	Включить/Отключить авторитетный режим. Это ускоряет аренду DHCP. Используется, если это единственный сервер в сети.
3	Включить защиту от «DNS Rebinding»	Включить/Отключить защиту от атак повторной привязки DNS, отбрасывая восходящие ответы RFC1918.
DHCP Пул		
1	Включить	Включить/Отключить пул, для распределения IP-адресов.
2	Динамический IP	Включить/Отключить динамическое распределение IP-адресов. Если отключено, то DHCP сервер будет обслуживать запросы только от тех клиентов, которые определенны в таблице **«Постоянные аренды DHCP»**.
3	Интерфейс	Прослушиваемый интерфейс. Также используется для вычисления IP-адреса сети /24.
4	Старт	Стартовый IP-адрес узла в подсети /24. Адрес сети вычисляется из IP-адреса выбранного интерфейса. Например, если IP-адрес интерфейса **192.168.1.1**, то IP-адреса будут распределяться, начиная с **192.168.1.100**.
5	Количество	Количество IP-адресов в диапазоне.
6	Время аренды	Указывается время аренды IP-адреса. 12h – 12 часов, 2m – 2 минуты.
7	Опции DHCP	Список опций, передаваемых клиентам. Опции состоит из номера опции и значения опции. Номер опции и значение разделяются запятой. Например: 26, 1470 – опция 26 (размер MTU), значение 1470. Полный список опции определен в RFC 2132.

4.5.2 Сеть – DHCP/DNS – Постоянные аренды DHCP

В меню находится раздел предназначенный для создания статических записей DHCP. Каждая запись состоит из имени или MAC-адреса хоста и IP-адреса, который будет выделен хосту при запросе по DHCP протоколу. Если вместо IP-адреса задать значение **«Игнорировать»**, то для указанного хоста запросы на получение IP-адреса сервером DHCP обрабатываться не будут. Для создания записей необходимо нажать кнопку **«ДОБАВИТЬ»**, заполнить необходимые поля и сохранить изменения, нажав кнопку **«СОХРАНИТЬ»**. Для удаления нужной записи необходимо нажать кнопку **«УДАЛИТЬ»**, а потом кнопку **«СОХРАНИТЬ»**.

Пример настройки показан на рис 4.5.2.

Описание параметров представлено в таблице 4.5.2.

Рис.4.5.2. Меню «Сеть – DHCP/DNS – Постоянные аренды DHCP». Пример статической записи DHCP

Таблица 4.5.2. Описание параметров «Постоянные аренды DHCP»

№	Название поля	Описание
Постоянные аренды DHCP		
1	Включить	Включить/Отключить обработку записи службой DHCP/DNS.
2	Имя хоста	Указывается имя хоста. Допускается не указывать, если привязка будет происходить по MAC-адресу.
3	MAC адрес	Указывается MAC-адрес. Допускается не указывать, если привязка будет происходить по имени хоста.
4	IPv4 адрес	IP-адрес из пула IP-адресов. Если указано **«Игнорировать»**, то для этого хоста запросы DHCP обрабатываться не будут.

4.5.3 Сеть – DHCP/DNS – Локальный DNS

В меню находится раздел предназначенный для создания статических записей DNS. Каждая запись состоит из доменного имени и соответствующего ему IP-адреса. Для создания записей необходимо нажать кнопку **«ДОБАВИТЬ»**, заполнить необходимые поля и

сохранить изменения, нажав кнопку **«СОХРАНИТЬ»**. Для удаления нужной записи необходимо нажать кнопку **«УДАЛИТЬ»**, а потом кнопку **«СОХРАНИТЬ»**.

Пример добавления локальной статической записи DNS показан на рис 4.5.3.

Описание параметров представлено в таблице 4.5.3.

Рис.4.5.3. Меню «Сеть – DHCP/DNS – Локальный DNS». Пример статической записи DNS

Таблица 4.5.3. Описание параметров «Имена узлов»

№	Название поля	Описание
Имена узлов		
1	Доменное имя	Доменное имя для IP-адреса.
2	IPv4 адрес	IP-адрес.

4.6 Сеть – Статические маршруты

В меню находится раздел предназначенный для добавления статических маршрутов в таблицу маршрутизации (рис.4.6). Маршрутизация служит для определения, через какой интерфейс и шлюз можно достичь нужного хоста или сети. Для создания записей необходимо нажать кнопку **«ДОБАВИТЬ»**, заполнить необходимые поля и сохранить изменения, нажав кнопку **«СОХРАНИТЬ»**. Для удаления нужной записи необходимо нажать кнопку **«УДАЛИТЬ»**, а потом кнопку **«СОХРАНИТЬ»**.

Описание параметров представлено в таблице 4.6.

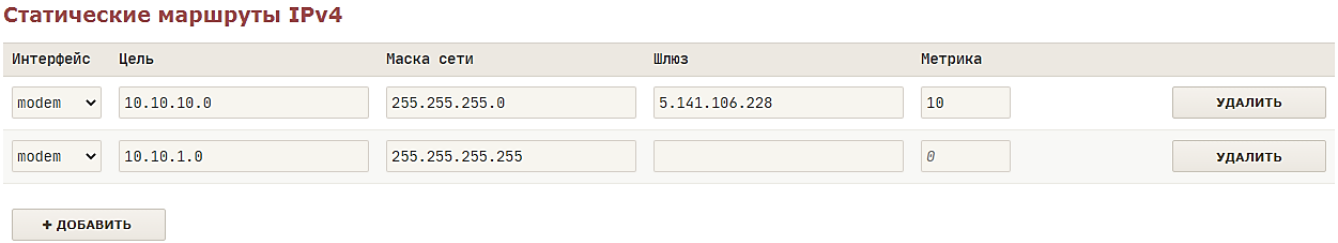


Рис.4.6. Меню «Сеть – Статические маршруты»

Таблица 4.6. Описание параметров «Статические маршруты IPv4»

№	Название поля	Описание
Статические маршруты IPv4		
1	Интерфейс	Выбор интерфейса, через который должен направляться трафик к указанному хосту или сети.
2	Цель	Целевой IP-адрес хоста или сети.
3	Маска сети	Маска целевой подсети. Для хоста должно быть указано **255.255.255.255**.
4	Шлюз	Шлюз, через который будет идти маршрут до адреса. IP-адрес шлюза должен принадлежать той же подсети что IP-адрес интерфейса.
5	Метрика	Приоритет маршрута в таблице маршрутизации, 0 – максимальный приоритет.

4.7 Сеть – Межсетевой экран

В меню выполняется конфигурация межсетевого экрана. Настройки позволяют создавать пользовательские правила для решения определенных задач, например, открыть или перенаправить порты, ограничить доступ к сети или из сети к хосту, модифицировать отдельные поля проходящих пакетов и т.д.

Настройки разбиты на пять подразделов – **«Настройка зон», «Перенаправления портов», «Правила для трафика», «Пользовательские правила»** и **«Дополнительные настройки»**. Подразделы расположены на соответствующих вкладках.

Для упрощения настройки межсетевого экрана созданы специальные группы настроек – зоны межсетевого экрана. Интерфейсы, принадлежащие к одной зоне, будут иметь общую политику фильтрации по отношению к входящему, транзитному и исходящему трафику.

Суть настройки межсетевого экрана обычно сводится к созданию пользовательских исключающих правил в соответствующих таблицах **«DNAT»**, **«SNAT»**, **«Правила для входящего трафика»**, **«Правила для транзитного трафика»** и **«Правила для исходящего трафика»**.

Каждый IP-пакет, проходящий через интерфейсы, будет проверяться на соответствие критериям правил в соответствующих таблицах (сверху вниз). Порядок правил в таблицах имеет значение. Правила расположенные выше имеют больший приоритет и будут проверяться первыми. Если IP-пакет попадает под критерии, над ним будет выполнено действие, указанное в правиле. Только одно правило в таблице может быть выполнено. Если для IP-пакета, проходящего через интерфейс, в таблице нет подходящего правила, то над таким пакетом будет выполнено действие, соответствующее политике зоны, к которой прикреплен интерфейс, либо политике **«По умолчанию»**, если интерфейс не прикреплен ни к одной из зон. Политика зон межсетевого экрана приводится в таблицах 4.7а, 4.7б. Настройка зон производится в меню ***«Сеть → Межсетевой экран → Настройка зон»***. Настройка политики **«По умолчанию»** производится в меню ***«Сеть → Межсетевой экран →*** **Дополнительные настройки»**.

Общие критерии отбора для IP-трафика это протокол (TCP, UDP, ICMP и т.д.), IP-адрес источника, порт источника, IP-адрес назначения, порт назначения.

Действия над трафиком для таблицы **«DNAT»** – подмена IP-адреса назначения и/или подмена порта назначения. Действия над трафиком для таблицы **«SNAT»** – подмена IP-адреса источника и/или подмена порта источника. Действия над трафиком для таблиц **«Правила для входящего трафика»**, **«Правила для транзитного трафика»** и **«Правила для исходящего трафика»** – ***DROP, REJECT, ACCEPT***.

Действие **DROP** – игнорировать пакеты, действие **REJECT** – отбрасывать пакеты и отправлять ответное сообщение ICMP, действие **ACCEPT** – обрабатывать пакеты.

Любой IP-трафик, проходящий через роутер, можно разделить на три категории – входящий, транзитный и исходящий трафик.

Входящий трафик – это любые IP-пакеты, поступающие через любой интерфейс, IP-адрес назначения которых совпадает с любым IP-адресом любого интерфейса роутера. Важно, что инициатором подключения является удаленный хост. Обычно входящий трафик обрабатывается какой-либо службой ОС (WEB-сервером, SSH-сервером и т.д.) или самим стеком TCP/IP.

Транзитный трафик – это любые IP-пакеты, поступающие через любой интерфейс, IP-адрес назначения которых не совпадает ни с одним из IP-адресов интерфейсов роутера и существует запись в таблице маршрутизации для IP-адреса назначения. Такой трафик будет перенаправлен в другой интерфейс (если разрешают правила межсетевого экрана). Этот процесс называется маршрутизация или перенаправление.

Исходящий трафик – это IP-пакеты, которые были отправлены через интерфейс. Важно, что инициатором подключения выступает службы ОС (OpenVPN, L2TP и т.д.) или стек TCP/IP.

Таблица 4.7а. Политика зон межсетевого экрана (настройка по умолчанию).

WAN	Входящий трафик – **DROP** (игнорировать); Исходящий трафик – **ACCEPT** (разрешен); Транзитный трафик между интерфейсами зоны – **DROP** (игнорировать); Ограничение MSS – Включено; Выполняется трансляция IP-адреса отправителя – функция NAT.
LAN	Входящий трафик – **ACCEPT** (разрешен); Исходящий трафик – **ACCEPT** (разрешен); Транзитный трафик между интерфейсами зоны – **ACCEPT** (разрешен).
VPN	Входящий трафик – **ACCEPT** (разрешен); Исходящий трафик – **ACCEPT** (разрешен); Транзитный трафик между интерфейсами зоны – **ACCEPT** (разрешен).
Не определена (политика «По умолчанию»)	Входящий трафик – **ACCEPT** (разрешен); Исходящий трафик – **ACCEPT** (разрешен); Транзитный трафик между интерфейсами зоны – **REJECT** (игнорировать).

Таблица 4.7б. Маршрутизация между зонами (настройка по умолчанию).

Зона источника	**Зона назначения**	
WAN	**любая**	Маршрутизация запрещена.
LAN	**VPN, WAN**	Маршрутизация разрешена.
VPN	**LAN**	Маршрутизация разрешена.
Не определена (политика «По умолчанию»)	**любая**	Маршрутизация запрещена.

4.7.1 Сеть – Межсетевой экран – Настройка зон

В меню находится раздел предназначенный для настройки политики зон межсетевого экрана (рис.4.7.1а). Для создания новой зоны необходимо нажать кнопку **«ДОБАВИТЬ»,** для редактирования уже созданной необходимо нажать кнопку **«РЕДАКТИРОВАТЬ»**, далее заполнить необходимые поля (рис.4.7.1б,в) и сохранить изменения, нажав кнопку **«СОХРАНИТЬ»**. Для удаления нужной зоны необходимо нажать кнопку **«УДАЛИТЬ»**, а потом кнопку **«СОХРАНИТЬ»**.

Описание параметров представлено в таблице 4.7.1а и 4.7.1б.

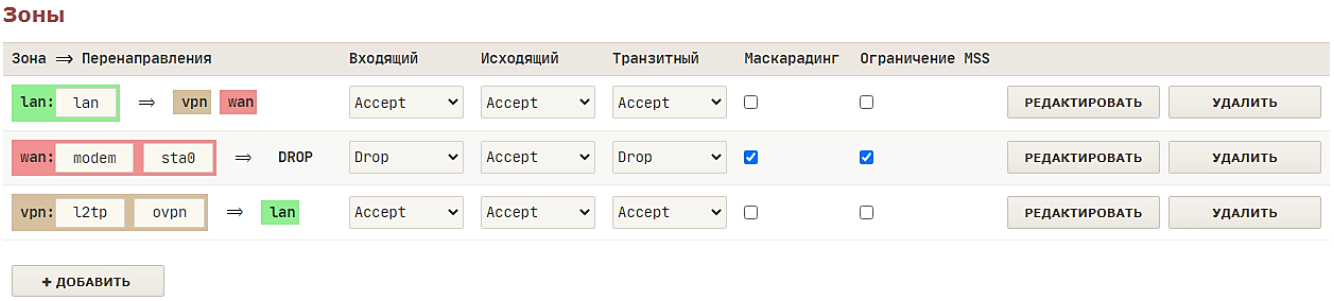


Рис.4.7.1а. Меню «Сеть – Межсетевой экран – Настройка зон»

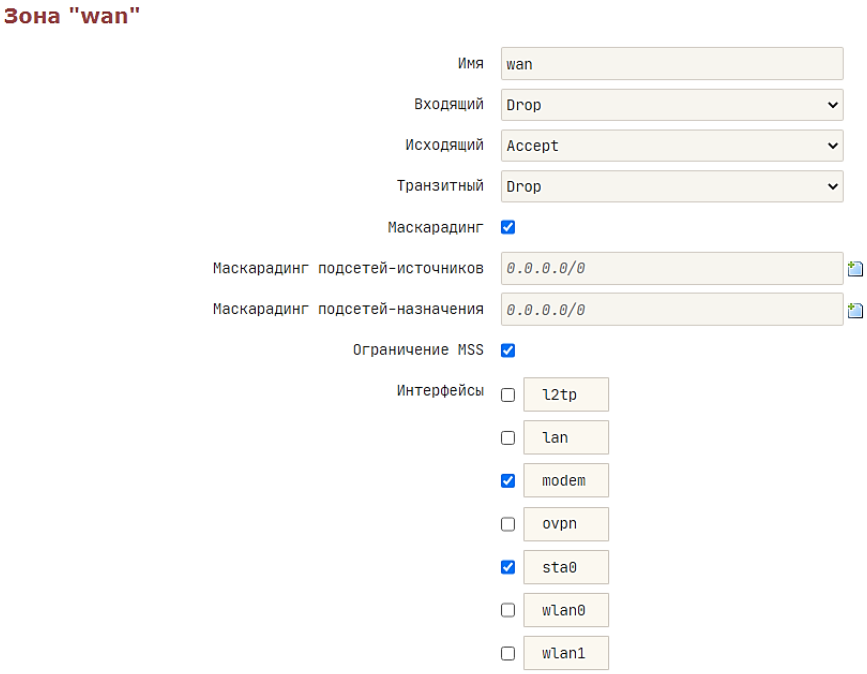


Рис.4.7.1б. Меню «Сеть – Межсетевой экран – Настройка зон». Редактирование зоны «wan»

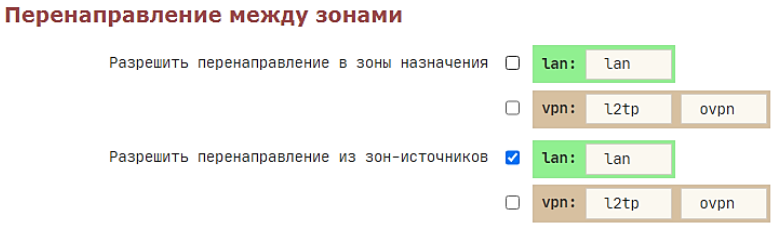


Рис.4.7.1в. Меню «Сеть – Межсетевой экран – Настройка зон». Редактирование зоны «wan»

Таблица 4.7.1а. Описание параметров «Зоны»

№	Название поля	Описание
Зоны		
1	Зона ⟹ Перенаправления	Имя зоны и действие по отношению к транзитному трафику из этой зоны. Настройки по умолчанию приведены в таблице 4.7б.
2	Входящий	Действие по отношению к входящему трафику через интерфейсы зоны.
3	Исходящий	Действие по отношению к исходящему трафику через интерфейсы зоны.

4	Транзитный	Действие по отношению к транзитному трафику между интерфейсами зоны.
5	Маскарадинг	Включает/Отключает трансляцию IP-адреса источника (функция NAT).
6	Ограничение MSS	Включает/Отключает ограничение максимального размера TCP сегмента (MSS) для предотвращения фрагментации пакетов.

Таблица 4.7.1б. Описание параметров «Зона <имя зоны>» и «Перенаправление между зонами»

№	Название поля	Описание
Зона <имя зоны>		
1	Имя	Имя зоны.
2	Входящий	Действие по отношению к входящему трафику через интерфейсы зоны.
3	Исходящий	Действие по отношению к исходящему трафику через интерфейсы зоны.
4	Транзитный	Действие по отношению к транзитному трафику между интерфейсами зоны.
5	Маскарадинг	Включает/Отключает трансляцию IP-адреса источника (NAT).
6	Маскарадинг подсетей-источника	Создать список подсетей-отправителей, для которых нужно использовать трансляцию IP-адреса.
7	Маскарадинг подсетей-назначения	Создать список подсетей-получателей, для которых нужно использовать трансляцию IP-адреса.
8	Ограничение MSS	Включает/Отключает ограничение максимального размера TCP сегмента (MSS) для предотвращения фрагментации пакетов.
9	Интерфейсы	Список интерфейсов, прикрепленных к зоне.
Перенаправление между зонами		
1	Разрешить перенаправление в зоны назначения	Разрешить маршрутизацию в указанные зоны.
2	Разрешить перенаправление из зон-источников	Разрешить маршрутизацию из указанных зон.

4.7.2 Сеть – Межсетевой экран – Перенаправления портов – DNAT

В меню находится подраздел создания пользовательских правил для подмены IP-адреса и/или порта назначения в поступающих IP-пакетах (рис.4.7.2а). Это технология известна также как **«проброс портов»** или **«перенаправление портов»** и позволяет обращаться из внешней сети (Интернет) к хостам, которые находятся в локальной сети за маршрутизатором, использующим NAT.

Для создания нового правила необходимо нажать кнопку **«ДОБАВИТЬ»,** для редактирования уже созданного правила необходимо нажать кнопку **«РЕДАКТИРОВАТЬ»**, далее заполнить необходимые поля (рис.4.7.2б) и сохранить изменения, нажав кнопку **«СОХРАНИТЬ»**. Для удаления правила необходимо нажать кнопку **«УДАЛИТЬ»**, а потом кнопку **«СОХРАНИТЬ»**. Для быстрого создания правил можно сразу заполнить необходимые поля, после чего нажать кнопки **«ДОБАВИТЬ» и «СОХРАНИТЬ»**. Правила, которые находятся в начале таблицы, будут иметь больший приоритет. Для изменения приоритета правил можно воспользоваться кнопками **«▲»** и **«▼»**, а после изменения нажать кнопку **«СОХРАНИТЬ»**.

Описание параметров представлено в таблице 4.7.2а и 4.7.2б.

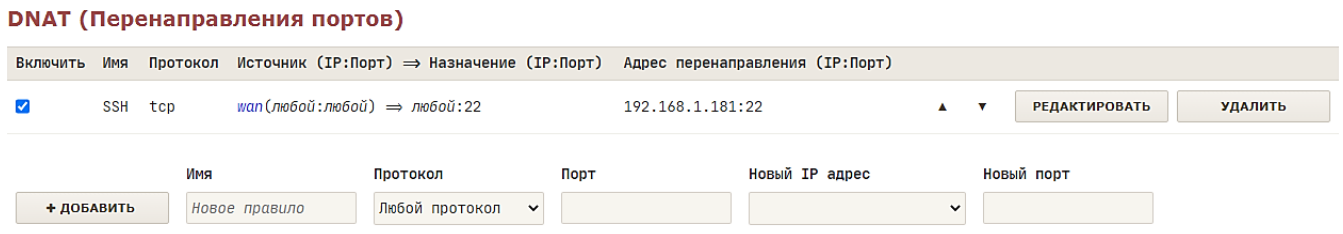


Рис.4.7.2а. Меню «Сеть – Межсетевой экран – Перенаправление портов – DNAT».
Пример правила для перенаправления порта TCP 22 на IP-адрес 192.168.1.181

Таблица 4.7.2а. Описание параметров «DNAT (Перенаправления портов)»

№	Название поля	Описание
DNAT (Перенаправления портов)		
1	Включить	Включить/Отключить правило.
2	Имя	Имя правила.
3	Протокол	Протокол поверх IP.
4	Источник (IP:Порт) ⟹	Зона источника, IP-адрес и порт источника, IP-адрес и порт назначения.

	Назначение ((IP:Порт)	
5	Адрес перенаправления (IP:Порт)	Новый IP-адрес и/или порт во входящих IP-пакетов. Замена будет выполнена, если IP-пакет будет удовлетворять критериям отбора.

Правило "SSH"

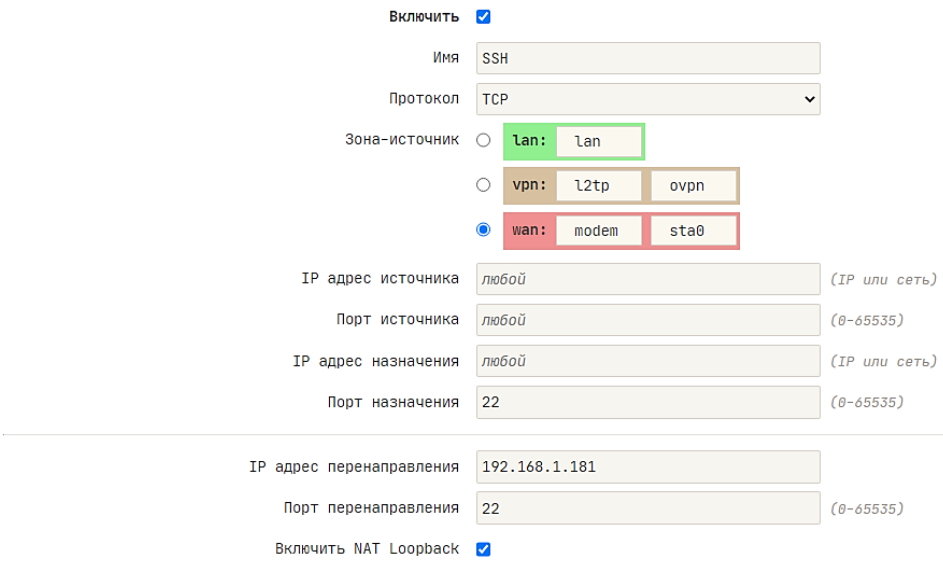


Рис.4.7.2б. Меню «Сеть – Межсетевой экран – Перенаправление портов – DNAT». Пример редактирования правила «SSH»

Таблица 4.7.2б. Описание параметров «Правило <Имя правила>»

№	Название поля	Описание
Правило <Имя правила>		
1	Включить	Включить/Отключить правило.
2	Имя	Имя правила.
3	Протокол	Протокол поверх IP.
4	Зона источника	Выбор зоны определяет интерфейсы, IP-трафик через которые будет использоваться для отбора.
5	IP адрес источника	IP-адрес источника – отправителя пакета.
6	Порт источника	Порт источника – отправителя пакета. Через символ «-» можно указывать диапазон портов. Только для протокола TCP/UDP.
7	IP адрес назначения	IP-адрес назначения – получателя пакета.
8	Порт назначения	Порт назначения – получателя пакета. Через символ «-» можно указывать диапазон портов.
9	IP адрес перенаправления	Новый IP-адрес назначения во входящих IP-пакетах. Замена будет выполнена, если IP-пакет будет удовлетворять критериям отбора.
10	Порт перенаправления	Новый порт назначения во входящих IP-пакетах. Через символ «-» можно указывать диапазон портов. Замена будет выполнена, если IP-пакет будет удовлетворять критериям отбора.
11	Включить NAT Loopback	Включить/Отключить функцию позволяющую пользователям локальной сети получить доступ к ресурсам или устройствам этой же локальной сети через внешний IP-адрес маршрутизатора (WAN IP).

В пунктах №3-8 задаются критерии отбора входящих IP-пакетов. После подмены IP-адреса и/или порта, IP-пакет может быть принят локальной службой или стеком TCP/IP, либо отправлен в другой интерфейс.

DMZ-хост

DMZ-хост – это способ предоставления доступа к внутренним серверам (таким, как почтовый, WWW, FTP) пользователям и программам из внешней сети (Интернет). Доступ предоставляется путем перенаправления определенного диапазон TCP/UDP портов на указанный хост в локальной сети. DMZ-хост это не сегмент DMZ, так как хост с открытыми портами не будет изолирован от других хостов в локальной сети.

Для создания правила DMZ нажмите кнопку **«ДОБАВИТЬ»**, предварительно выбрав в поле **«Протокол»** необходимое значение (обычно TCP и UDP), в поле **«Порт»** (внешний порт) и **«Новый порт»** (внутренний порт) укажите одинаковый диапазон портов, например 1-9999, а в поле **«Новый IP адрес»** укажите IP-адрес хоста в локальный сети, выполняющего функцию DMZ-хоста. Нажмите кнопку **«СОХРАНИТЬ»**. Рекомендуется для DMZ-хоста, зарезервировать IP-адрес, выдаваемый службой DHCP (настройка в меню ***«Сеть →***

***DHCP/DNS* → Постоянные аренды DHCP»)**.

4.7.3 Сеть – Межсетевой экран – Перенаправления портов – SNAT

В меню находится подраздел создания пользовательских правил для подмены IP-адреса и/или порта источника в IP-пакетах, уходящих через интерфейс (рис.4.7.3а). В представленном примере создано правило для подмены IP-адреса источника на **10.10.0.2** для всех IP-пакетов с протоколом TCP направляющихся в сеть **10.10.0.1/24** через любые интерфейсы зоны **«wan»**.

Для создания нового правила необходимо нажать кнопку **«ДОБАВИТЬ»,** для редактирования уже созданного правила необходимо нажать кнопку **«РЕДАКТИРОВАТЬ»**, далее заполнить необходимые поля (рис.4.7.3б) и сохранить изменения, нажав кнопку **«СОХРАНИТЬ»**. Для удаления правила необходимо нажать кнопку **«УДАЛИТЬ»**, а потом кнопку **«СОХРАНИТЬ»**. Правила, которые находятся в начале таблицы, будут иметь больший приоритет. Для изменения приоритета правил можно воспользоваться кнопками **«▲»** и **«▼»**, а после изменения нажать кнопку **«СОХРАНИТЬ»**.

Описание параметров представлено в таблице 4.7.3а и 4.7.3б.

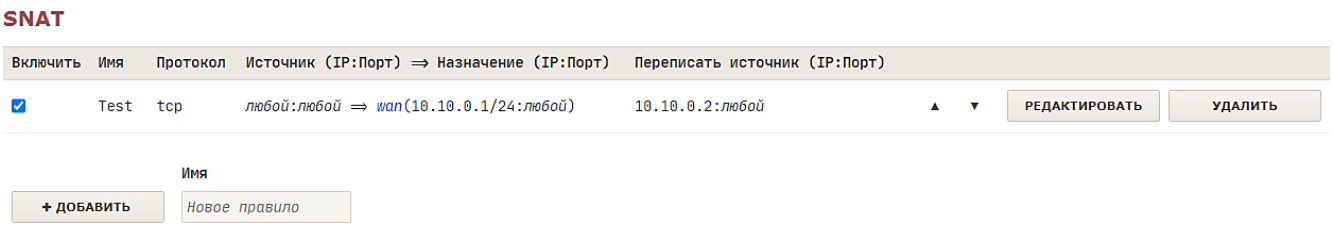


Рис.4.7.3а. Меню «Сеть – Межсетевой экран – Перенаправление портов – SNAT». Пример подмены адреса источника IP-пакета

Таблица 4.7.3а. Описание параметров «SNAT»

№	Название поля	Описание
SNAT		
1	Включить	Включить/Отключить правило.
2	Имя	Имя правила.
3	Протокол	Протокол поверх IP.
4	Источник (IP:Порт) ⟹ Назначение ((IP:Порт)	IP-адрес и порт источника, зона назначения, IP-адрес и порт назначения.
5	Переписать источник (IP:Порт)	Новый IP-адрес и/или порт источника в исходящих или транзитных IP-пакетах. Замена будет выполнена, если IP-пакет будет удовлетворять критериям отбора.

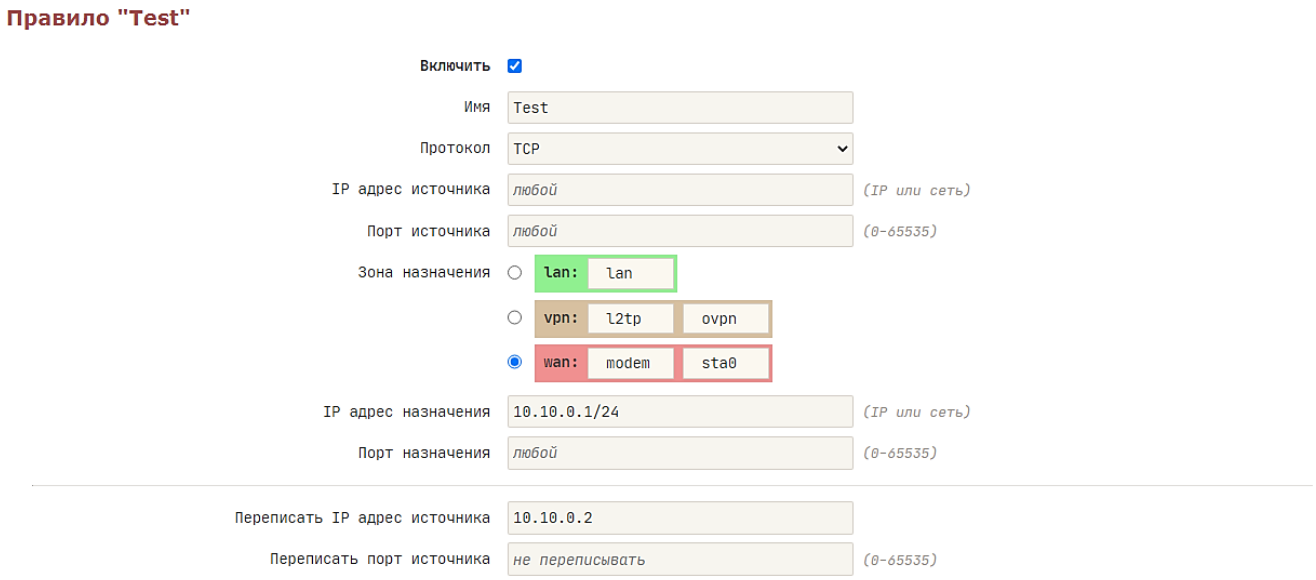


Рис.4.7.3б. Меню «Сеть – Межсетевой экран – Перенаправление портов – SNAT». Пример редактирования правила «Test»

Таблица 4.7.3б. Описание параметров «Правило <Имя правила>»

№	Название поля	Описание
Правило <Имя правила>		
1	Включить	Включить/Отключить правило.
2	Имя	Имя правила.
3	Протокол	Протокол поверх IP.
4	IP адрес источника	IP-адрес источника – отправителя пакета.
5	Порт источника	Порт источника – отправителя пакета. Через символ «-» можно указывать диапазон портов. Только для протокола TCP/UDP.
6	Зона назначения	Выбор зоны определяет интерфейсы, IP-трафик через которые будет использоваться для отбора.
7	IP адрес назначения	IP-адрес назначения – получателя пакета.
8	Порт назначения	Порт назначения – получателя пакета. Через символ «-» можно указывать диапазон портов.
9	Переписать IP адрес источника	Новый IP-адрес источника в исходящих или транзитных IP-пакетах. Замена будет выполнена, если IP-пакет будет удовлетворять критериям отбора.
10	Переписать порт источника	Новый порт источника в исходящих или транзитных IP-пакетах. Через символ «-» можно указывать диапазон портов. Замена будет выполнена, если IP-пакет будет удовлетворять критериям отбора.

В пунктах №3-8 задаются критерии отбора исходящих или транзитных IP-пакетов.

4.7.4 Сеть – Межсетевой экран – Правила для трафика – Входящий

В меню находится подраздел создания пользовательских правил для управления фильтрацией входящих IP-пакетов (подключений) (рис.4.7.4а). Чаще всего используется термин **«открыть порты»**.

По умолчанию роутер все входящие подключения с интерфейсов в зоне **«wan»** блокирует, поэтому в таблице уже присутствует два правила **«Allow-DHCP-Renew»** и **«Allow-Ping»**. Первое правило позволяет получать интерфейсу адрес от внешнего DHCP-сервера, а второе позволяет проверять на доступность IP-адреса из внешней сети посредством icmp-запросов (ping).

Для создания нового правила необходимо нажать кнопку **«ДОБАВИТЬ»,** для редактирования уже созданного правила необходимо нажать кнопку **«РЕДАКТИРОВАТЬ»**, далее заполнить необходимые поля (рис.4.7.4б) и сохранить изменения, нажав кнопку **«СОХРАНИТЬ»**. Для удаления правила необходимо нажать кнопку **«УДАЛИТЬ»**, а потом кнопку **«СОХРАНИТЬ»**. Для быстрого создания правил можно сразу заполнить необходимые поля, после чего нажать кнопки **«ДОБАВИТЬ» и «СОХРАНИТЬ»**. Правила, которые находятся в начале таблицы, будут иметь больший приоритет. Для изменения приоритета правил можно воспользоваться кнопками **«▲»** и **«▼»**, а после изменения нажать кнопку **«СОХРАНИТЬ»**.

Описание параметров представлено в таблице 4.7.4а и 4.7.4б.

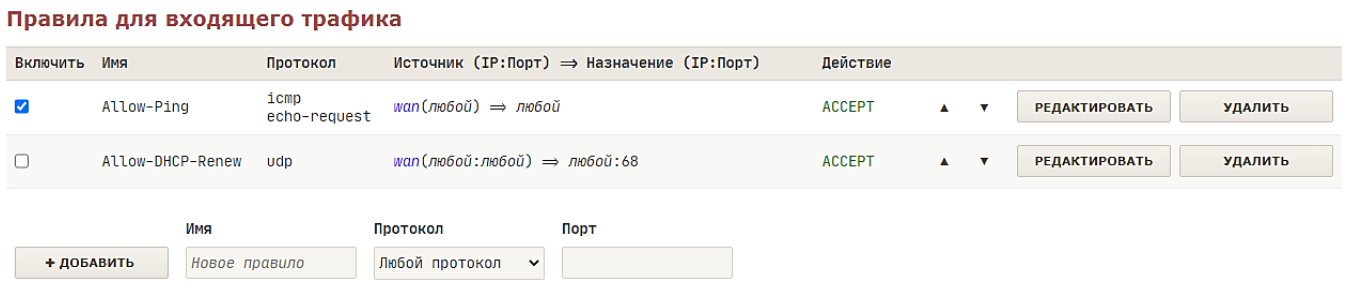


Рис.4.7.4а. Меню «Сеть – Межсетевой экран – Правила для трафика – Входящий».
*Правила **«Allow-DHCP-Renew»** и **«Allow-Ping»***

Таблица 4.7.4а. Описание параметров «Правила для входящего трафика»

№	Название поля	Описание
Правила для входящего трафика		
1	Включить	Включить/Отключить правило.
2	Имя	Имя правила.
3	Протокол	Протокол поверх IP.
4	Источник (IP:Порт) ⟹ Назначение ((IP:Порт)	Зона источника, IP-адрес и порт источника, IP-адрес и порт назначения.
5	Действие	Действие, которое будет применено к входящему подключению, если выполнится условие отбора.

		Возможные значения: **ACCEPT** – разрешить входящее подключение; **DROP** – игнорировать входящее подключение; **REJECT** – отклонить входящее подключение, при этом удаленному хосту будет отправлено соответствующее icmp-сообщение.

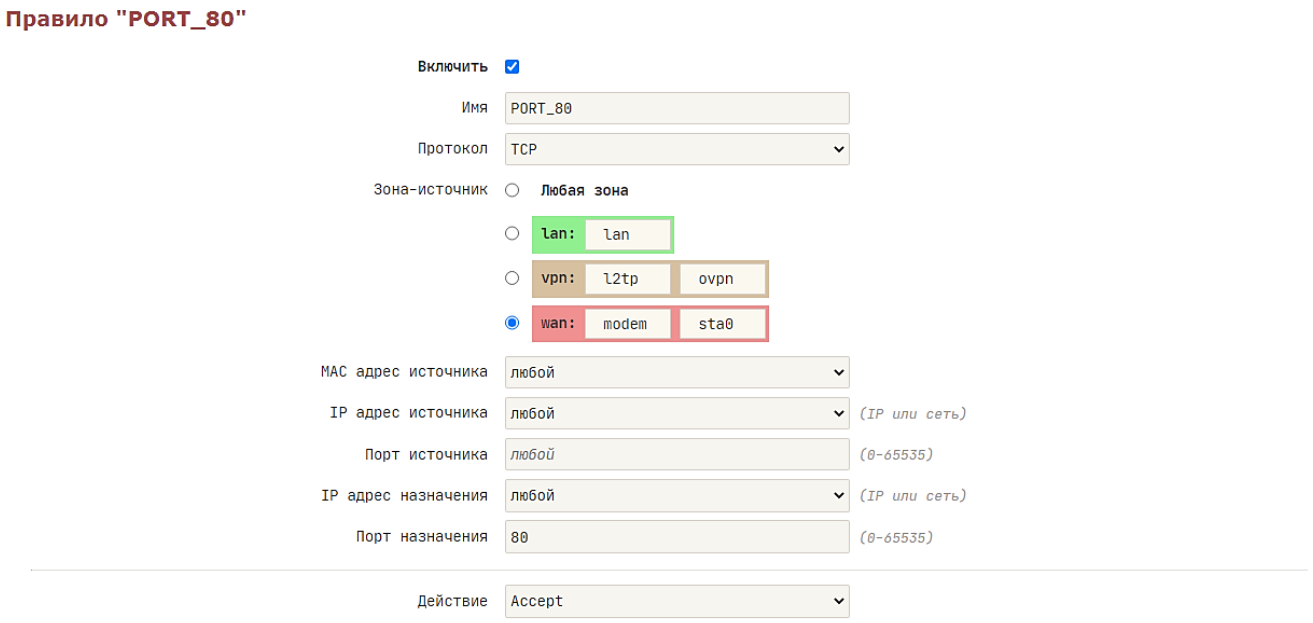


Рис.4.7.4б. Меню «Сеть – Межсетевой экран – Правила для трафика – Входящий».
Пример редактирования правила «PORT_80» (открыть порт 80)

Таблица 4.7.4б. Описание параметров «Правило <Имя правила>»

№	Название поля	Описание
Правило <Имя правила>		
1	Включить	Включить/Отключить правило.
2	Имя	Имя правила.
3	Протокол	Протокол поверх IP.
4	Зона источника	Выбор зоны определяет интерфейсы, IP-трафик через которые будет использоваться для отбора.
5	MAC адрес источника	MAC-адрес отправителя пакета. Используется только для интерфейсов поддерживающих передачу кадров 802.3 (Ethernet).
6	IP адрес источника	IP-адрес источника – отправителя пакета.
7	Порт источника	Порт источника – отправителя пакета. Через символ «-» можно указывать диапазон портов. Только для протокола TCP/UDP.
8	IP адрес назначения	IP-адрес назначения – получателя пакета.
9	Порт назначения	Порт назначения – получателя пакета. Через символ «-» можно указывать диапазон портов.
10	Действие	Действие, которое будет применено к IP-пакету, если выполнится условие отбора. Возможные значения: **ACCEPT** – разрешить входящее подключение; **DROP** – игнорировать входящее подключение; **REJECT** – отклонить входящее подключение, при этом удаленному хосту будет отправлено соответствующее icmp-сообщение.

В пунктах №3-9 задаются критерии отбора входящих IP-пакетов.

4.7.5 Сеть – Межсетевой экран – Правила для трафика – Транзитный

В меню находится подраздел создания пользовательских правил для управления транзитными IP-пакетами, то есть, пакетами, которые будут перенаправлены в другие интерфейсы (рис.4.7.5а).

Для создания нового правила необходимо нажать кнопку **«ДОБАВИТЬ»,** для редактирования уже созданного правила необходимо нажать кнопку **«РЕДАКТИРОВАТЬ»**, далее заполнить необходимые поля (рис.4.7.5б) и сохранить изменения, нажав кнопку **«СОХРАНИТЬ»**.

Для удаления правила необходимо нажать кнопку **«УДАЛИТЬ»**, а потом кнопку **«СОХРАНИТЬ»**. Правила, которые находятся в начале таблицы, будут иметь больший приоритет. Для изменения приоритета правил можно воспользоваться кнопками **«▲»** и **«▼»**, а после изменения нажать кнопку **«СОХРАНИТЬ»**.

Описание параметров представлено в таблице 4.7.5а и 4.7.5б.

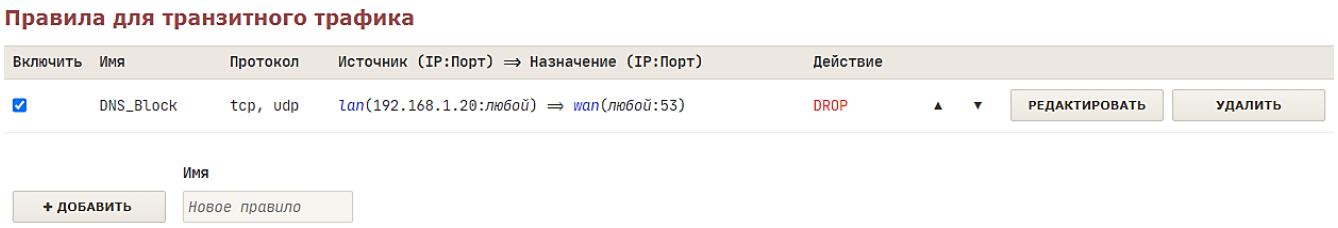


Рис.4.7.5а. Меню «Сеть – Межсетевой экран – Правила для трафика – Транзитный». Пример блокировки транзитных DNS запросов с IP 192.168.1.20

Таблица 4.7.5а. Описание параметров «Правила для транзитного трафика»

№	Название поля	Описание
Правила для транзитного трафика		
1	Включить	Включить/Отключить правило.
2	Имя	Имя правила.
3	Протокол	Протокол поверх IP.
4	Источник (IP:Порт) ⟹ Назначение ((IP:Порт)	Зона источника, IP-адрес и порт источника, зона назначения, IP-адрес и порт назначения.
5	Действие	Действие, которое будет применено к транзитному IP-пакету, если выполнится условие отбора. Возможные значения: **ACCEPT** – разрешить транзитное подключение; **DROP** – игнорировать транзитное подключения; **REJECT** – отклонить транзитное подключение, при этом удаленному хосту будет отправлено соответствующее icmp-сообщение.

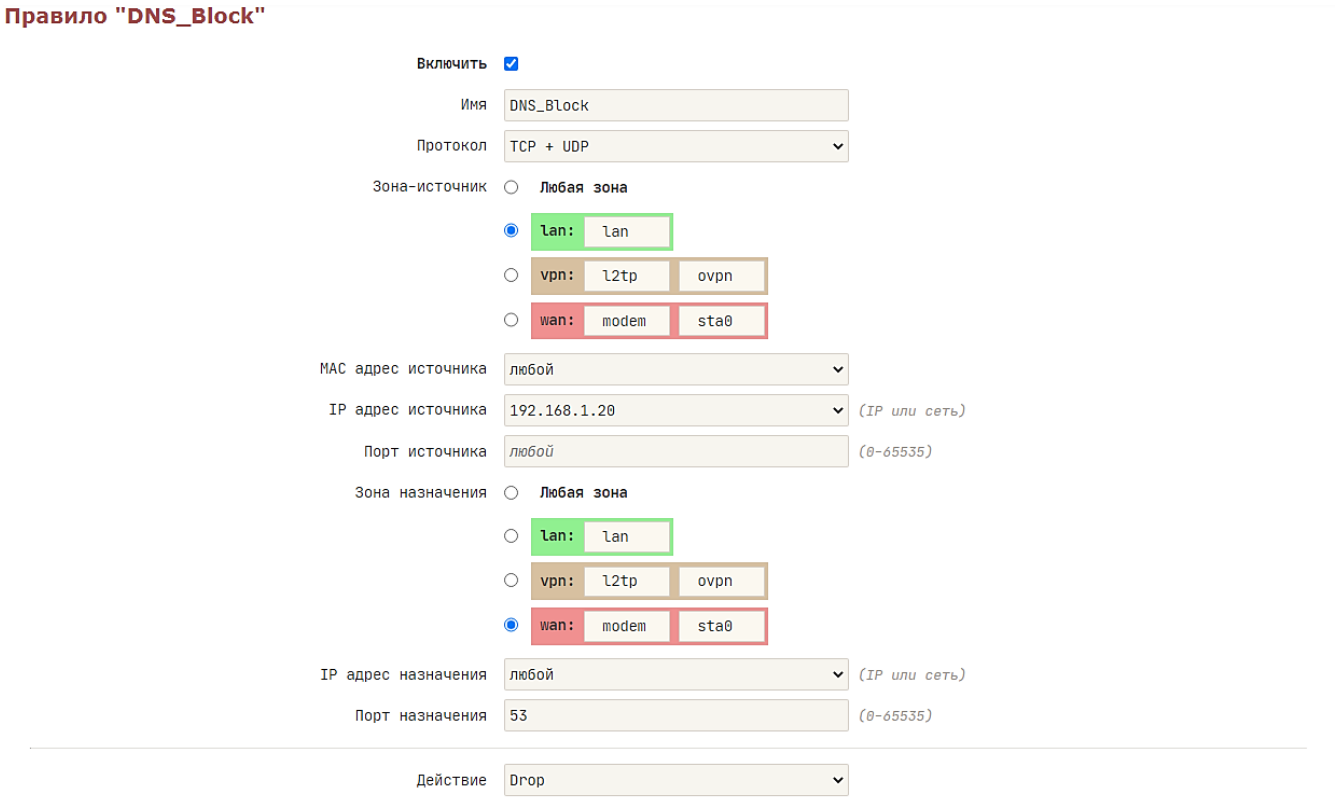


Рис.4.7.5б. Меню «Сеть – Межсетевой экран – Правила для трафика – Транзитный». Пример редактирования правила «DNS_Block»

Таблица 4.7.5б. Описание параметров «Правило <Имя правила>»

№	Название поля	Описание
Правило <Имя правила>		
1	Включить	Включить/Отключить правило.
2	Имя	Имя правила.
3	Протокол	Протокол поверх IP.
4	Зона источника	Выбор зоны определяет интерфейсы, IP-трафик через которые будет использоваться для отбора.
5	MAC адрес источника	MAC-адрес отправителя пакета. Используется только для интерфейсов поддерживающих передачу кадров 802.3 (Ethernet).
6	IP адрес источника	IP-адрес источника – отправителя пакета.
7	Порт источника	Порт источника – отправителя пакета. Через символ «-» можно указывать диапазон портов. Только для протокола TCP/UDP.
8	Зона назначения	Выбор зоны определяет интерфейсы, на которые перенаправляется транзитный трафик.
9	IP адрес назначения	IP-адрес назначения – получателя пакета.
10	Порт назначения	Порт назначения – получателя пакета. Через символ «-» можно указывать диапазон портов.
11	Действие	Действие, которое будет применено к транзитному IP-пакету, если выполнится условие отбора. Возможные значения: **ACCEPT** – разрешить транзитное подключение; **DROP** – игнорировать транзитное подключения; **REJECT** – отклонить транзитное подключение, при этом удаленному хосту будет отправлено соответствующее icmp-сообщение.

В пунктах №3-10 задаются критерии отбора транзитных IP-пакетов.

4.7.6 Сеть – Межсетевой экран – Правила для трафика – Исходящий

В меню находится подраздел создания пользовательских правил для управления исходящими IP-пакетами (подключениями) (рис.4.7.6а).

Для создания нового правила необходимо нажать кнопку **«ДОБАВИТЬ»,** для редактирования уже созданного правила необходимо нажать кнопку **«РЕДАКТИРОВАТЬ»**, далее заполнить необходимые поля (рис.4.7.6б) и сохранить изменения, нажав кнопку **«СОХРАНИТЬ»**. Для удаления правила необходимо нажать кнопку **«УДАЛИТЬ»**, а потом кнопку **«СОХРАНИТЬ»**. Правила, которые находятся в начале таблицы, будут иметь больший приоритет. Для изменения приоритета правил можно воспользоваться кнопками **«▲»** и **«▼»**, а после изменения нажать кнопку **«СОХРАНИТЬ»**.

Описание параметров представлено в таблице 4.7.6а и 4.7.6б.

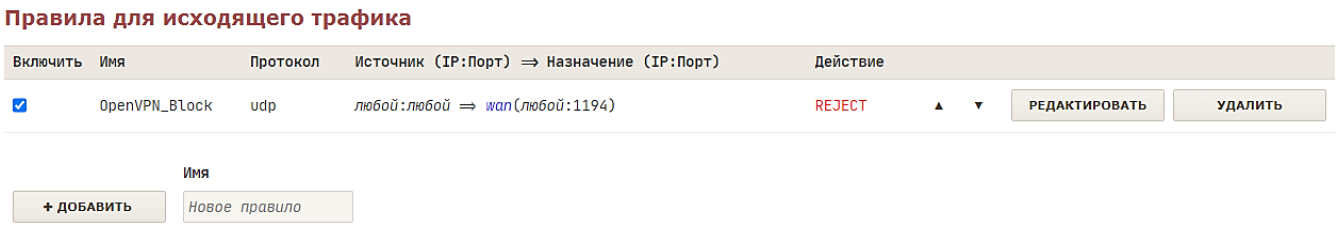


Рис.4.7.6а. Меню «Сеть – Межсетевой экран – Правила для трафика – Исходящий». Пример блокировки исходящих подключений на порт 1194

Таблица 4.7.6а. Описание параметров «Правила для исходящего трафика»

№	Название поля	Описание
Правила для исходящего трафика		
1	Включить	Включить/Отключить правило.
2	Имя	Имя правила.
3	Протокол	Протокол поверх IP.
4	Источник (IP:Порт) ⟹ Назначение ((IP:Порт)	IP-адрес и порт источника, зона назначения, IP-адрес и порт назначения.
5	Действие	Действие, которое будет применено к исходящему IP-пакету, если выполнится условие отбора. Возможные значения: **ACCEPT** – разрешить исходящее подключение; **DROP** – игнорировать исходящее подключение; **REJECT** – отклонить исходящее подключение, при этом локальному процессу будет отправлено

		соответствующее icmp-сообщение.

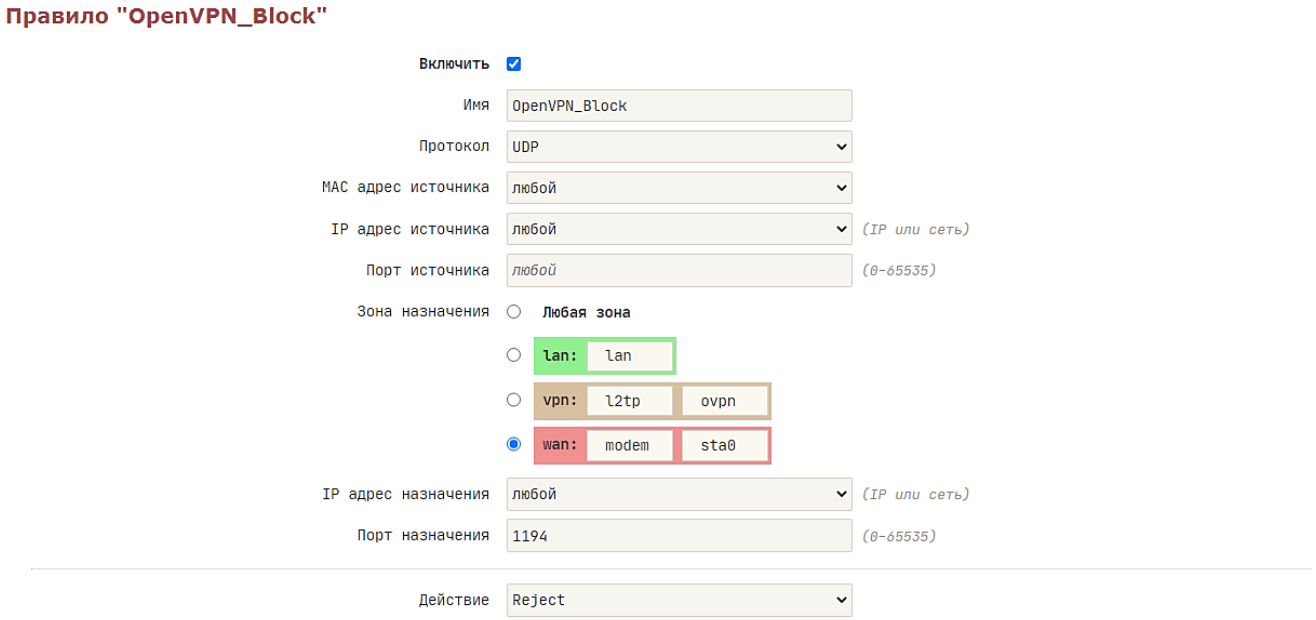


Рис.4.7.6б. Меню «Сеть – Межсетевой экран – Правила для трафика – Исходящий». Пример редактирования правила «OpenVPN_Block»

Таблица 4.7.6б. Описание параметров «Правило <Имя правила>»

№	Название поля	Описание
Правило <Имя правила>		
1	Включить	Включить/Отключить правило.
2	Имя	Имя правила.
3	Протокол	Протокол поверх IP.
4	MAC адрес источника	MAC-адрес отправителя пакета. Оставить пустым.
5	IP адрес источника	IP-адрес источника – отправителя пакета.
6	Порт источника	Порт источника – отправителя пакета. Через символ «-» можно указывать диапазон портов. Только для протокола TCP/UDP.
7	Зона назначения	Выбор зоны определяет интерфейсы, через которые отправляется исходящий трафик.
8	IP адрес назначения	IP-адрес назначения – получателя пакета.
9	Порт назначения	Порт назначения – получателя пакета. Через символ «-» можно указывать диапазон портов.
10	Действие	Действие, которое будет применено к IP-пакету, если выполнится условие отбора. Возможные значения: **ACCEPT** – разрешить исходящее подключение; **DROP** – игнорировать исходящее подключение; **REJECT** – отклонить исходящее подключение, при этом локальному процессу будет отправлено соответствующее icmp-сообщение.

В пунктах №3-9 задаются критерии отбора исходящих IP-пакетов.

4.7.7 Сеть – Межсетевой экран – Пользовательские правила

В меню находится подраздел для создания цепочек правил в формате iptables (рис.4.7.7). Правила в iptables будут добавлены после добавления основных пользовательских правил. Для сохранения изменений нажмите кнопку **«СОХРАНИТЬ»**.

Пользовательские правила

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

# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into the
# special user chains, e.g. input_wan_rule or postrouting_lan_rule.


iptables -t mangle -A POSTROUTING -j TTL --ttl-set 67 -o wwan0
```

Рис.4.7.7. Меню «Сеть – Межсетевой экран – Пользовательские правила».
*Пример правила для изменения «ttl» на интерфейсе **«modem»***

4.7.8 Сеть – Межсетевой экран – Дополнительные настройки

В меню находится подраздел с настройками политики **«По умолчанию»** для тех случаев, когда интерфейс не принадлежит ни одной из зон (рис.4.7.8).

Описание параметров представлено в таблице 4.7.8.

Дополнительные настройки

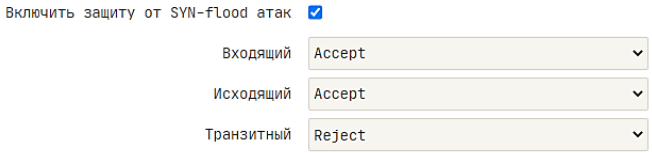


Рис.4.7.8. Меню «Сеть – Межсетевой экран – Правила для трафика – Дополнительные настройки».

Таблица 4.7.8. Описание параметров «Дополнительные настройки»

№	Название поля	Описание
Дополнительные настройки		
1	Включить защиту от SYN-flood атак	Включить/Отключить защиту от SYN-flood атак.
2	Входящий	Действие, которое будет применено к входящему подключению, если оно выполняется через интерфейс, который не принадлежит ни одной из зон. Возможные значения: **ACCEPT** – разрешить входящее подключение; **DROP** – игнорировать входящее подключение; **REJECT** – отклонить входящее подключение, при этом удаленному хосту будет отправлено соответствующее icmp-сообщение.
3	Исходящий	Действие, которое будет применено к исходящему подключению, если оно выполняется через интерфейс, который не принадлежит ни одной из зон. Возможные значения: **ACCEPT** – разрешить исходящее подключение; **DROP** – игнорировать исходящее подключение; **REJECT** – отклонить исходящее подключение, при этом локальному процессу будет отправлено соответствующее icmp-сообщение.
4	Транзитный	Действие, которое будет применено к транзитному подключению, если оно выполняется через интерфейс, который не принадлежат ни одной из зон. Возможные значения: **ACCEPT** – разрешить транзитное подключение; **DROP** – игнорировать транзитное подключение; **REJECT** – отклонить транзитное подключение, при этом удаленному хосту будет отправлено соответствующее icmp-сообщение.

5 Меню «Утилиты»

5.1 Меню Утилиты – Диагностика

В меню находятся диагностические утилиты, с их помощью можно проверить доступность удаленного хоста, проверить работу DNS сервера или измерить пропускную способность. Каждая утилита расположена на своей вкладке.

5.1.1 Утилиты – Диагностика – Эхо-запрос

В меню предоставлена возможность работы с утилитой **«ping»**. Утилита позволяет проверить доступность удаленного узла или интернет соединения, для этого введите в поле **«Хост»** соответствующий IP-адрес или доменное имя удаленного узла и нажмите кнопку **«СТАРТ»**. Роутер пошлет 5 icmp-запросов (ping) до адресата и если он доступен, то адресат вышлет ответ на этот запрос (рис.5.1.1). Поле **«Размер «байт»** позволяет задать размер icmp-пакета без учета заголовка. Размер IP-пакета = Размер icmp + 8 (заголовок icmp) + 20 (заголовок ip).

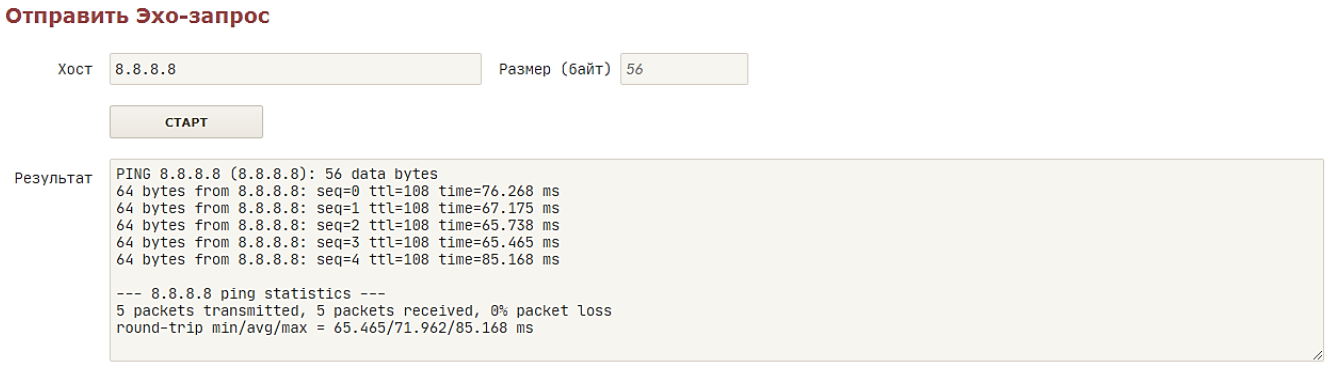


Рис.5.1.1. Меню «Утилиты – Диагностика – Эхо-запрос». Пример отправки эхо-запроса до IP-адреса 8.8.8.8

5.1.2 Утилиты – Диагностика – Трассировка

В меню предоставлена возможность работы с утилитой **«traceroute»**. Утилита позволяет узнать, по какому пути следуют пакеты данных до указанного домена или IP адреса, чтобы выявить потери пакетов или задержку в их прохождении, для этого введите в поле **«Хост»** соответствующий IP-адрес или доменное имя удаленного узла и нажмите кнопку **«СТАРТ»**. После окончания работы, утилита вернет отчет (рис.5.1.2).

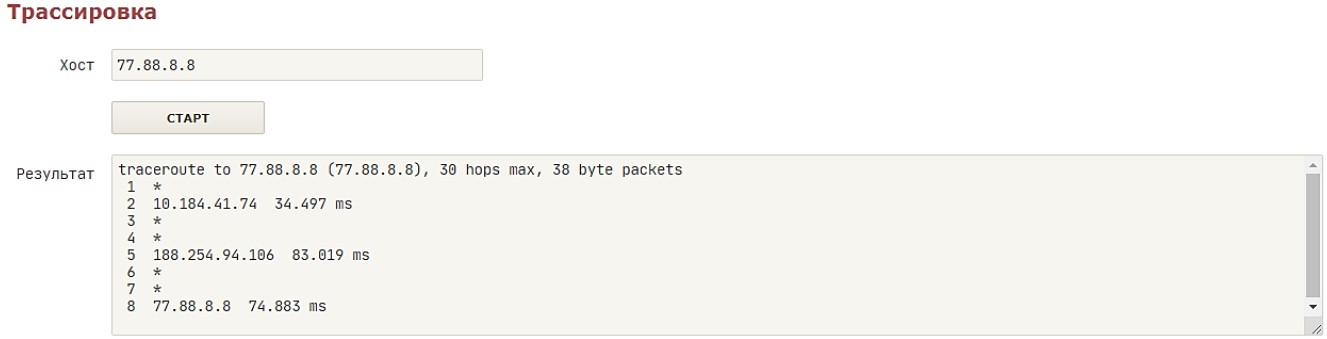


Рис.5.1.2. Меню «Утилиты – Диагностика – Трассировка». Пример отчета трассировки маршрута до IP-адреса 77.88.8.8

5.1.3 Утилиты – Диагностика – DNS

В меню предоставлена возможность работы с утилитой **«nslookup»**. Утилита позволяет узнать IP-адрес по доменному имени, для этого введите в поле **«Домен»** соответствующее доменное имя узла и нажмите кнопку **«СТАРТ»**. После окончания работы, утилита вернет отчет (рис.5.1.3). В поле **«Сервер DNS»** указывается IP-адреса DNS сервера, на который будет отправлен запрос DNS.

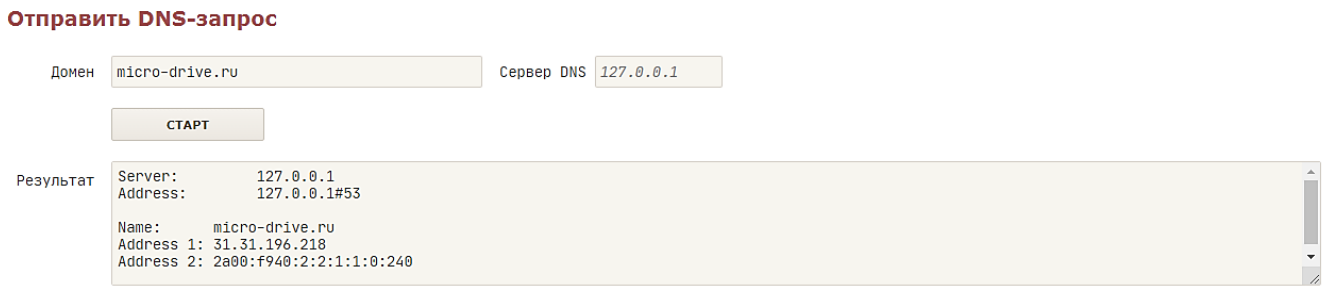


Рис.5.1.3. Меню «Утилиты – Диагностика – DNS». Запрос IP-адреса доменного имени «micro-drive.ru»

5.1.4 Утилиты – Диагностика – Тест скорости

В меню предоставлена возможность работы с утилитой **«iperf3»** в режиме клиента. **«iperf3»** – кроссплатформенная консольная клиент-серверная программа – генератор TCP и UDP трафика для тестирования пропускной способности сети. С ее помощью можно измерить максимальную пропускную способность сети между сервером и клиентом и провести нагрузочное тестирование канала связи.

Скачать **«iperf3»** можно с сайта https://iperf.fr/iperf-download. Для загрузки доступны версии утилиты для разных ОС (Windows, macOS, Ubuntu, Debian, Mint, Fedora, Red Hat, CentOS, openSUSE, Arch Linux, FreeBSD). Для мобильных устройств с ОС Android можно воспользоваться приложением **Magic iPerf**.

Для выполнения тестирования программа должна быть запущена на двух устройствах (это могут быть как компьютеры, так и смартфоны, планшеты). Одно из них будет выполнять роль сервера, а другое роль клиента. Между ними и будет происходить передача данных для измерения пропускной способности соединения.

Для запуска теста, введите в поле **«Сервер»** IP-адрес хоста, на котором будет запущен **«iperf3»** в режиме сервера, нажмите кнопку **«СТАРТ».** После окончания работы, утилита вернет отчет (рис.5.1.4). В поле **«Направление»** указывается направление передачи трафика при тестировании. В приведенном примере на хосте **192.168.1.120**, в режиме сервера, запущен **«iperf3»**. Роутер выполняет роль клиента. Физическое подключение – Ethernet 100Мбит/сек.

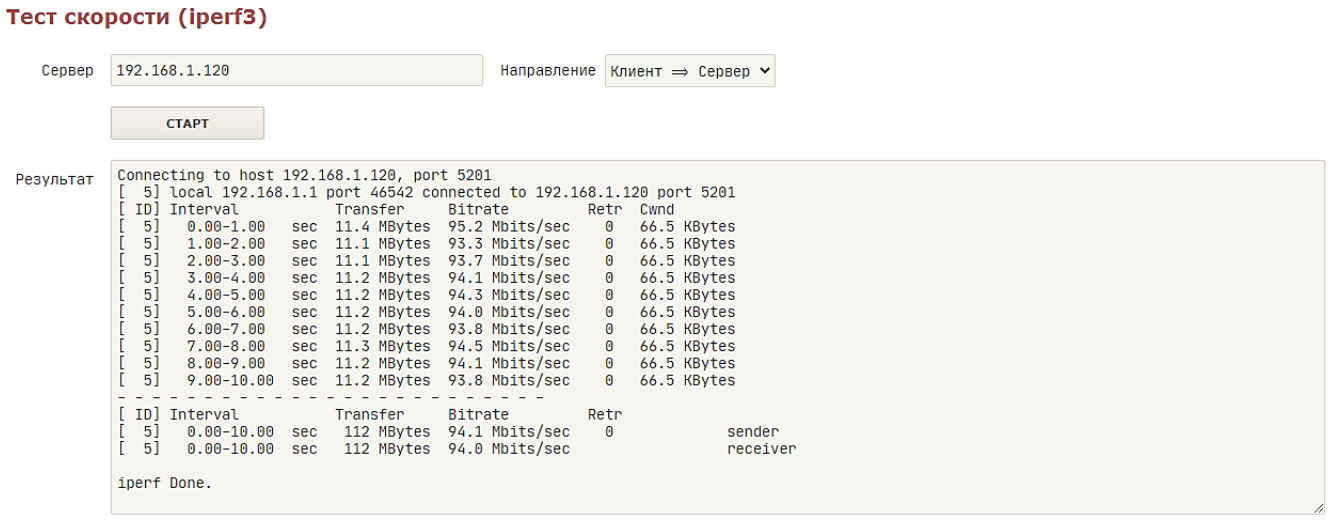


Рис.5.1.4. Меню «Утилиты – Диагностика – Тест скорости».
Тестирование пропускной способности канала связи между роутером и хостом 192.168.1.120.

Через SSH подключение можно запустить утилиту **«iperf3»** как в режиме клиента, так и в режиме сервера, с возможностью передать дополнительные опции.

Синтаксис команды iperf3

```
iperf3 [-s|-c хост] [опции]
```

Таблица 5.1.4. Опции команды «iperf3»

Опция	Описание
Общие опции для сервера и клиента	
-p #	Номер порта, на котором будет работать сервер/клиент (по умолчанию используется 5201).
-f [k|m|g|K|M|G]	Формат скорости в результатах теста: k (Кбит), K (Кбайт), m (Мбит), M (Мбайт), g (Гбит), G (Гбайт).

-I #	Интервал между выводом результата тестирования, в секундах.
-V	Более детализированный вывод информации.
-d	Вывод дополнительной информации для отладки.
-v	Показать версию.
-h	Показать справку.
Основные опции для сервера	
-s	Запустить в режиме сервера.
Основные опции для клиента	
-c <IP-адрес хоста>	Запуск клиента и подключение к серверу.
-u	Протокол UDP вместо TCP.
-b #[K|M|G]	Максимальная скорость в битах/сек (0 - отсутствует ограничение); по умолчанию отсутствует ограничение скорости для TCP, а для UDP составляет 1 Мбит/сек.
-t #	Время тестирования в секундах (по умолчанию 10 сек).
-n #[K|M|G]	Количество байт для передачи данных (вместо ключа -t).
-R	Запуск в обратном режиме (сервер отправляет трафик, клиент принимает).

ПРИМЕР 1:

Запустить в режиме сервера.

```
iperf3 –s
```

ПРИМЕР 2:

Запустить в режиме клиента и начать тест.

```
iperf3 –c 192.168.1.100
```

ПРИМЕР 3:

Запустить в режиме клиента и начать тест, передать только 100 Мбайт.

```
iperf3 –c 192.168.1.100 –n 100M
```

6 Меню «Помощь»

6.1 Помощь – Файлы

В меню предоставлена возможность скачать справочную и другую информацию, которая является частью файловой системы роутера.