Руководство по WEB-интерфейсу

Содержание

1. Подключение к WEB-интерфейсу и настройка сетевого адаптера

1.1. Подключение к WEB-интерфейсу роутера

1. Подключитесь к LAN порту роутера с помощью сетевого кабеля.
2. Откройте Ваш браузер и наберите в адресной строке браузера «**192.168.1.1**». Не используйте браузер «Internet Explorer».
3. Если не удалось зайти на роутер по указанному адресу, посмотрите настройки TCP/IP вашей сетевой карты. Компьютер должен получать IP-адрес и DNS автоматически по DHCP протоколу.

1.2. Пример настройки сетевой карты для Windows 10

1. Для этого перейдите в Центр управления сетями и общим доступом – Изменение параметров адаптера (Рис.1.1).

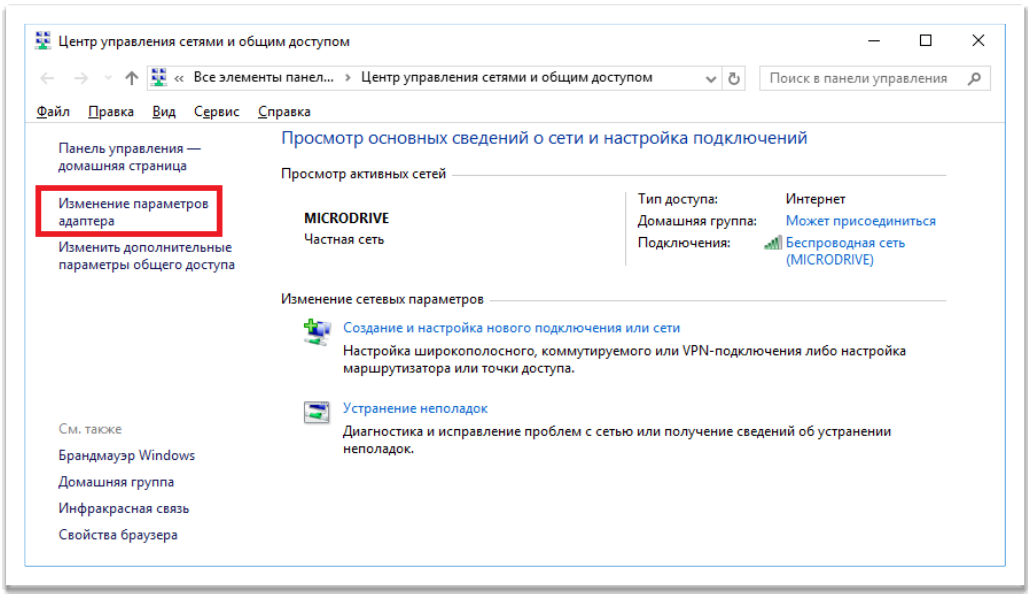

Рис.1.1. Центр управления сетями и общим доступом (Windows 10).

2. Правой кнопкой мыши щелкните по проводному сетевому подключению – «Свойства» (Рис.1.2).

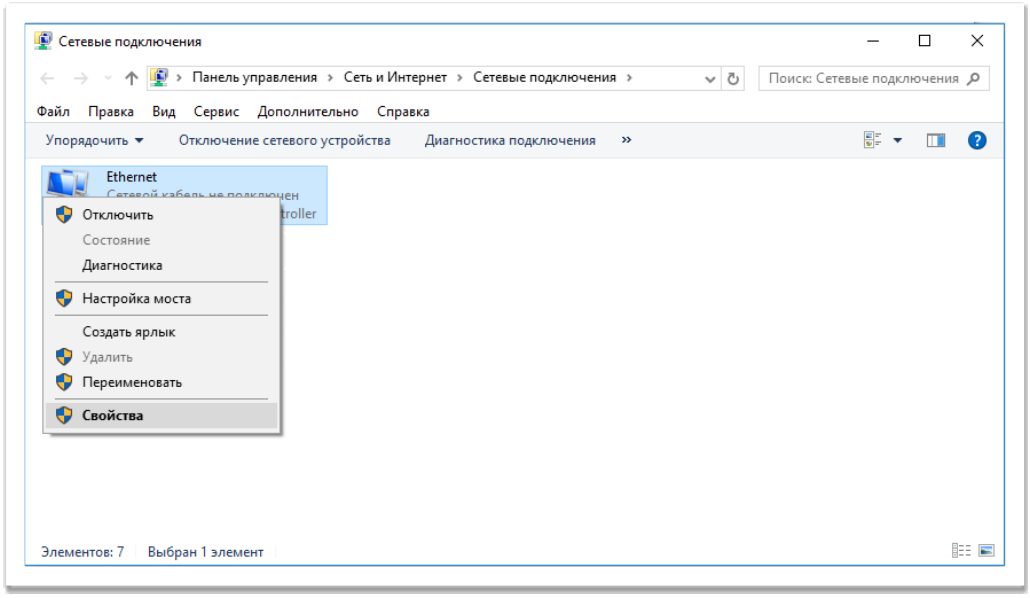

Рис.1.2. Изменения параметров сетевого адаптера.

3. Выделите компонент «IP версии 4» и нажмите кнопку «Свойства» (Рис.1.3).

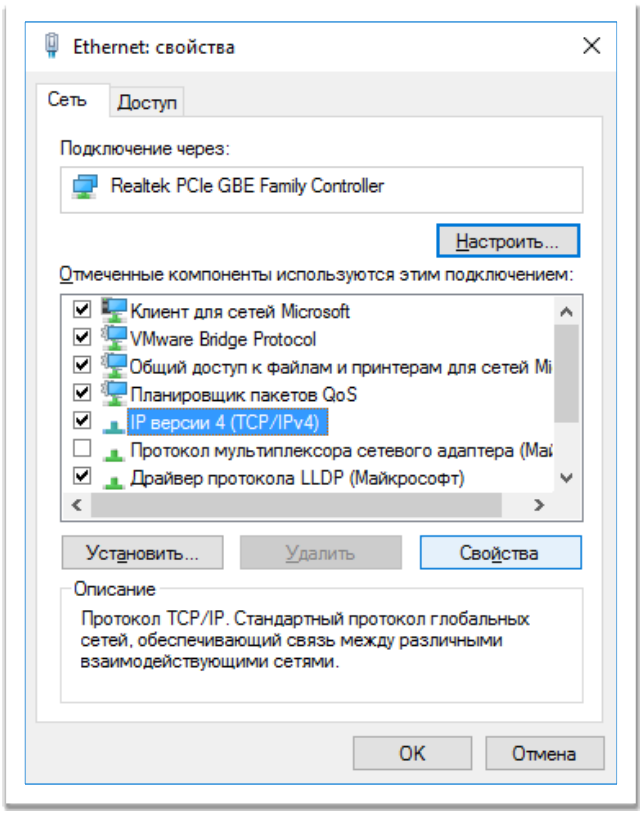

Рис.1.3. Свойства сетевого подключения.

4. Выберете получение настроек автоматически в обоих пунктах, нажмите «ОК» (Рис.1.4).

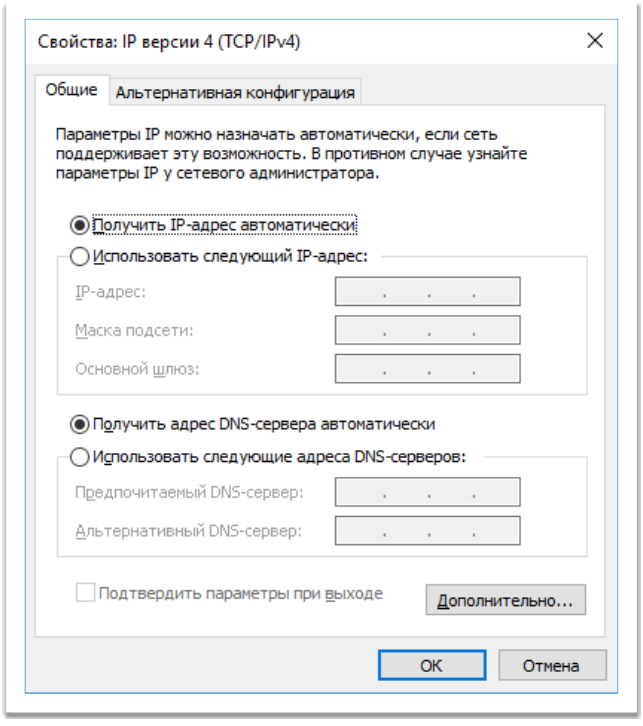

Рис.1.4. Настройка получения параметров IP автоматически.

5. По адресу **192.168.1.1** в браузере откроется форма входа в WEB-интерфейс устройства (Рис.1.5). Если пароль не установлен, нажмите «Войти».

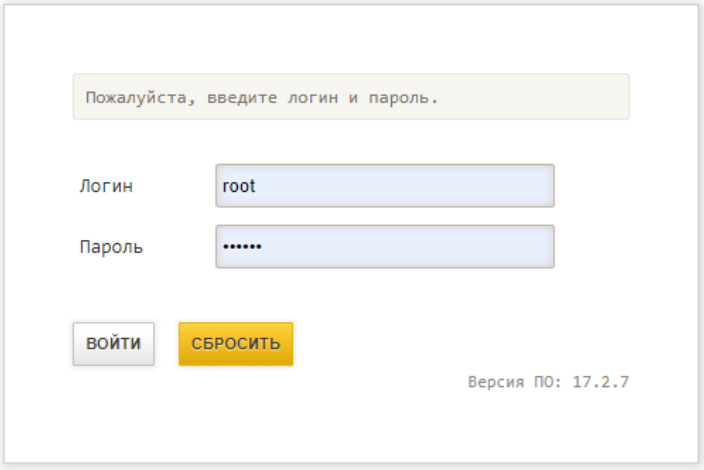

Рис.1.5. Авторизация WEB-интерфейса.

2. Меню – Статус

2.1. Обзор

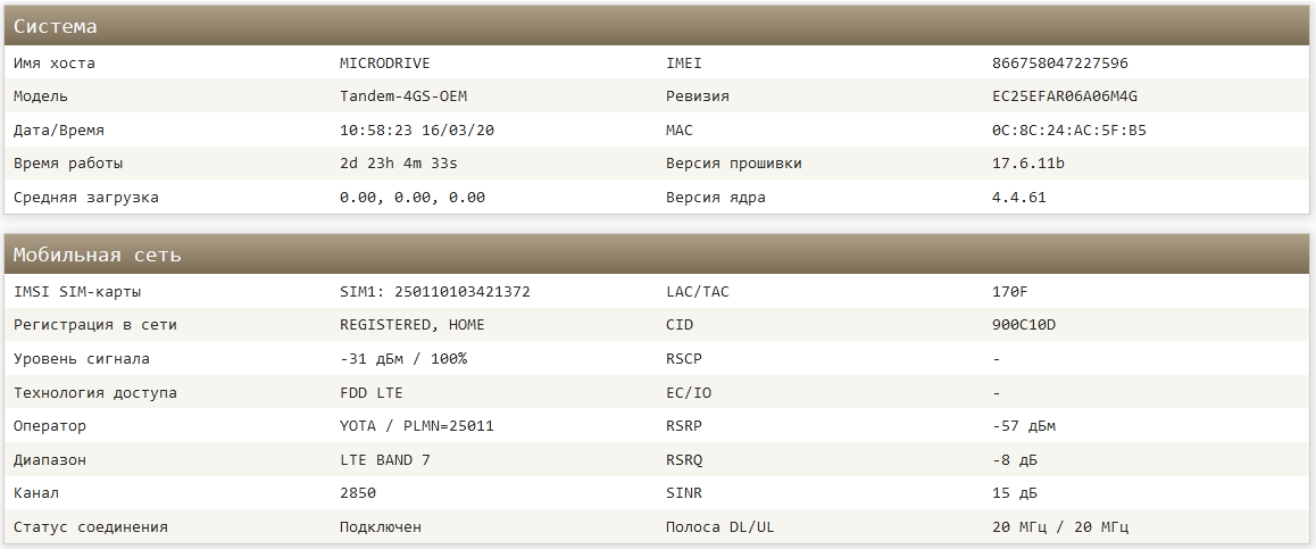

Рис.2.1. Меню Статус – Обзор.

Таблица 2.1. Описание полей меню Статус – Обзор.

№	Название поля	Пример значения	Описание
Система			
1	Имя хоста	MICRODRIVE	Символьное имя сетевого устройства
2	Модель	Tandem-4GL-OEM	Наименование модели устройства
3	Дата/Время	16:30:45 17/04/17	Отображает текущую время и дату в соответствии с установленным часовым поясом.
4	Время работы	10h 20m 30s	Время работы с момента включения. Обнуляется после перезагрузки
5	Средняя загрузка	0.01, 0.02, 0.28	Средняя загрузка процессора за 1, 5, 15 мин
6	IMEI	86114665610055	IMEI модема (международный идентификатор мобильных устройств)
7	Ревизия	EC25EFAR02A09M4G	Ревизия LTE модуля
8	MAC	1C:88:79:50:1B:F5	Заводской MAC-адрес
9	Версия прошивки	17.4.6	Версия прошивки
10	Версия ядра	4.4.61	Версия ядра Linux
Мобильная сеть			
1	IMSI SIM-карты	250002210456923	IMSI (международный идентификатор мобильного абонента). Используется для идентификации пользователя мобильной сети
2	Регистрация в сети	REGISTERED, HOME	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	-63 дБм / 81%	Уровень сигнала мобильной сети
4	Технология доступа	FDD LTE	Технология мобильной сети
5	Оператор	МТС / PLMN=25001	Имя мобильного оператора и код оператора
6	Диапазон	EUTRAN-BAND3	Частотный диапазон
7	Канал	3048	Канал сетевого подключения
8	Статус соединения	Подключен	Статус подключения к интернету по мобильной сети

9	LAC/TAC	1712	Код локации БС (LAC), Код зоны отслеживания (TAC) для сетей LTE
10	CID	0CF1168	Идентификатор соты
11	RSCP	-102 дБм	Мощность принятого сигнала (только для 3G)
12	EC/IO	-6 дБ	Отношение несущая/шум (только для 3G)
13	RSRP	-108 дБм	Среднее значение мощности принятых пилотных сигналов (только для LTE)
14	RSRQ	-6 дБ	Качество принятых пилотных сигналов (только для LTE)
15	SINR	17 дБ	Значение сигнал/шум (только для LTE)
16	Полоса DL/UL	20 МГц / 20 МГц	Полоса пропускания для входящего/исходящего трафика (только для LTE)
Сеть			
1	Статус IPv4 WAN	Не подключено	Статус подключения интернету (зона WAN) по IPv4
2	Статус IPV6 WAN	Не подключено	Статус подключения интернету (зона WAN) по IPv6
3	Активные соединения	30 / 16384 (0%)	Количество TCP/UDP соединений локальных служб с удаленным хостом
Аренды DHCP, Аренды DHCPv6			
1	Имя хоста (Хост)	-	Имена хостов, которым выделен IP-адрес
2	IPv4-адрес (IPv6-адрес)	192.168.1.125	Текущий IP-адрес выделенный хосту
3	MAC-адрес	90:94:e4:03:f4:85	MAC-адрес хоста, которому выдан IP-адрес
4	Оставшееся время аренды	11h 19m 58s	Время до следующей смены динамического IP-адреса хоста
5	DUID	0001000120754e10862 6649dfb3	Уникальный идентификатор DHCPv6

2.2. Интерфейсы

Состояние текущих интерфейсов отображено в меню «**Статус → Интерфейсы»**. С помощью кнопок «Соединить» и «Остановить» можно управлять состоянием интерфейса. Интерфейс отображается, если он включен в соответствующем разделе «Сеть».

Рис.2.2. Статус - Интерфейсы.

2.3. Межсетевой экран

Отображение и подсчет параметров межсетевого экрана находится в меню «**Статус → Межсетевой экран»**. Здесь в виде таблицы представлены настройки фильтрации, перенаправления пакетов и др. Можно сбросить счетчики пакетов и трафика соответствующей кнопкой и перезапустить межсетевой экран. Раздел разделен на 2 вкладки: «Межсетевой экран IPv4» и «Межсетевой экран IPv6». Настройка межсетевого экрана производится в меню «**Сеть → Межсетевой экран»**.

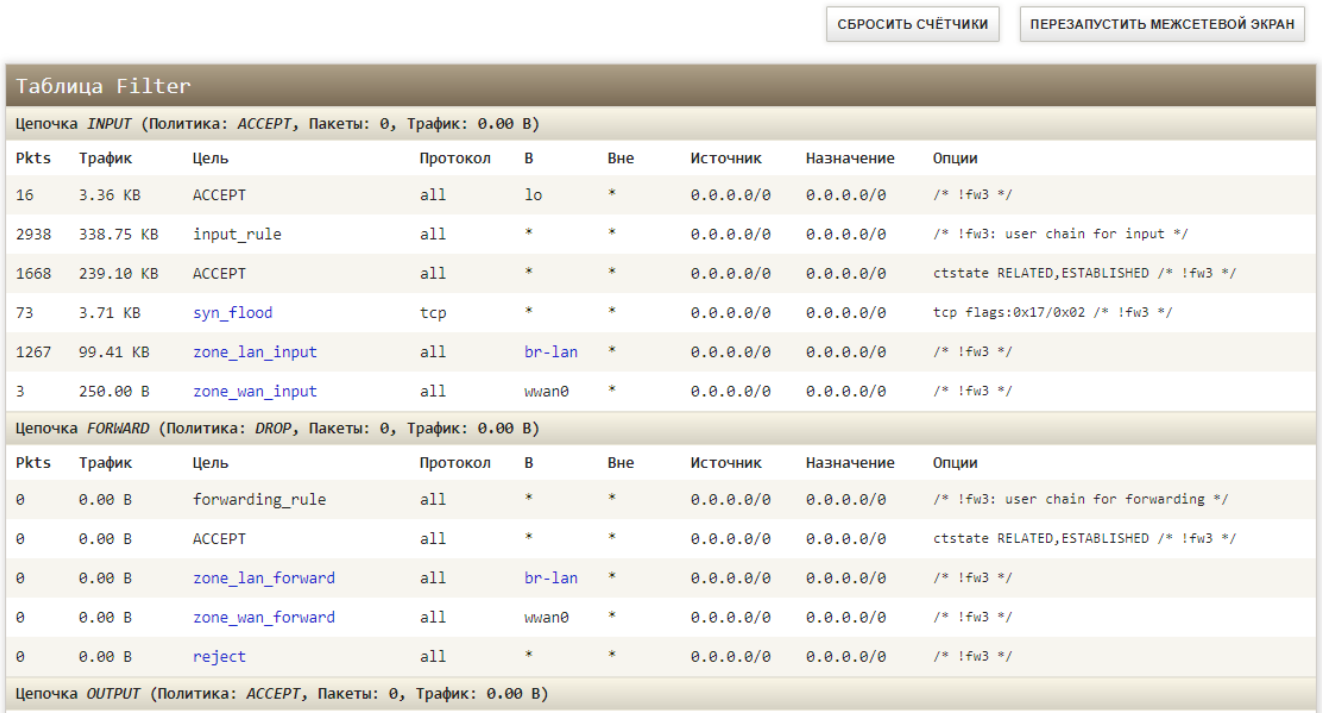

Рис.2.3. Статус межсетевого экрана.

Таблица 2.3. Описание таблиц в статусе межсетевого экрана.

№	Название таблицы	Описание
1	Filter	Предназначена для фильтрации трафика, то есть разрешения и запрещения пакетов и соединений
3	NAT	Предназначена для операций stateful-преобразования сетевых адресов и портов обрабатываемых пакетов
4	Mangle	Данная таблица предназначена для операций по классификации и маркировке пакетов и соединений, а также модификации заголовков пакетов (поля TTL и TOS)
5	Raw	Предназначена для выполнения действий с пакетами до их обработки системой conntrack

2.4. Маршруты

Таблица маршрутизации находится в меню «**Статус → Маршруты**».

Активные маршруты IPv4

Цель	Шлюз	Метрика	Интерфейс	Таблица
0.0.0.0/0	87.226.211.232	2	wwan0	main
87.226.211.224/28		2	wwan0	main
87.226.211.232		2	wwan0	main
192.168.0.0/24		0	br-lan	main

ARP

IP-адрес	MAC-адрес	Интерфейс
192.168.0.251	90:94:e4:03:f4:85	br-lan
192.168.0.15	ac:f1:df:0b:16:72	br-lan
192.168.0.1	e4:8d:8c:86:0f:d9	br-lan
192.168.0.21	50:3e:aa:55:a2:c2	br-lan
192.168.0.84	e8:39:35:ec:f4:9f	br-lan

Рис.2.4. Статус. Маршруты.

Таблица 2.4. Таблицы маршрута.

№	Название таблицы	Описание
1	Активные маршруты IPv4	Таблица маршрутизации по IPv4. Описывает соответствие между адресами назначения и интерфейсами, через которые следует отправить пакет данных до следующего маршрутизатора
2	ARP	ARP-таблица отображает IP и MAC подключенных к маршрутизатору сетевых устройств. А также интерфейс, через который устройство доступно
3	Активные маршруты IPv6	Таблица маршрутизации по IPv6. Описывает соответствие между адресами назначения и интерфейсами, через которые следует отправить пакет данных до следующего маршрутизатора
4	Соседние IPv6	Таблица содержит IPv6 и MAC-адреса соседних (ближайших) маршрутизаторов

2.5. Системный журнал

В системный журнал записываются все события, происходящие в маршрутизаторе, такие как: изменения настроек, подключение интерфейсов, проверка работоспособности процессов при загрузке и др.

К примеру, в журнале можно отследить, какие настройки APN использует интерфейс при подключении к мобильному интернету. Для проверки найдите в нем похожую строчку (Рис.2.5).

```
Mon Apr 17 16:16:16 2017 daemon.info cm[908]: SIM1 detected: imsi=250206691033304, status=READY
Mon Apr 17 16:16:16 2017 daemon.info cm[908]: set_default_profile: apn="internet"/""/""/none, pdp_type=ipv4v6
Mon Apr 17 16:16:16 2017 daemon.info cm[908]: set_preference: mode=gsm umts lte, band=gsm1800 egsm900 pgsm900 wcdma2100 wcdma850 wcdma900 b1 b3 k
Mon Apr 17 16:16:16 2017 daemon.info cm[908]: received SMS message
Mon Apr 17 16:16:16 2017 daemon.info cm[908]: get_registration_state: SIM1, PS=detached, CS=detached, PLMN=25002, Radio=UMTS, Reg=2
Mon Apr 17 16:16:17 2017 daemon.info cm[908]: get_registration_state: SIM1, PS=detached, CS=detached, PLMN=25020, Radio=LTE, Reg=2
Mon Apr 17 16:16:18 2017 daemon.info cm[908]: get_registration_state: SIM1, PS=attached, CS=attached, PLMN=25020, Radio=LTE, Reg=1
Mon Apr 17 16:16:18 2017 daemon.info cm[908]: set_data_call(ipv4): SIM1, apn="internet.tele2.ru"/""/""/none, WdsConnectionIPv4Handle=0x872c88a0
Mon Apr 17 16:16:19 2017 daemon.info cm[908]: usbnet_link_change(ipv4): ip=10.149.15.127, netmask=255.255.255.0, gw=10.149.15.128, mtu=1500, dns=
Mon Apr 17 16:16:19 2017 daemon.notice netifd: Interface 'modem' is now up
```

Рис.2.5. Запись событий в системный журнал.

2.6. Графики в реальном времени

В меню «**Статус → Графики**» в реальном времени можно посмотреть различную статистику в виде графиков в реальном времени. Например, график трафика через интерфейсы доступен на вкладке «Трафик» (Рис. 2.6). В таблице 2.6 расписаны все возможные варианты отображения графиков. На вкладке «Загрузка» отображается загрузка ЦП. Во вкладке «Соединения» - отображаются интернет соединения.

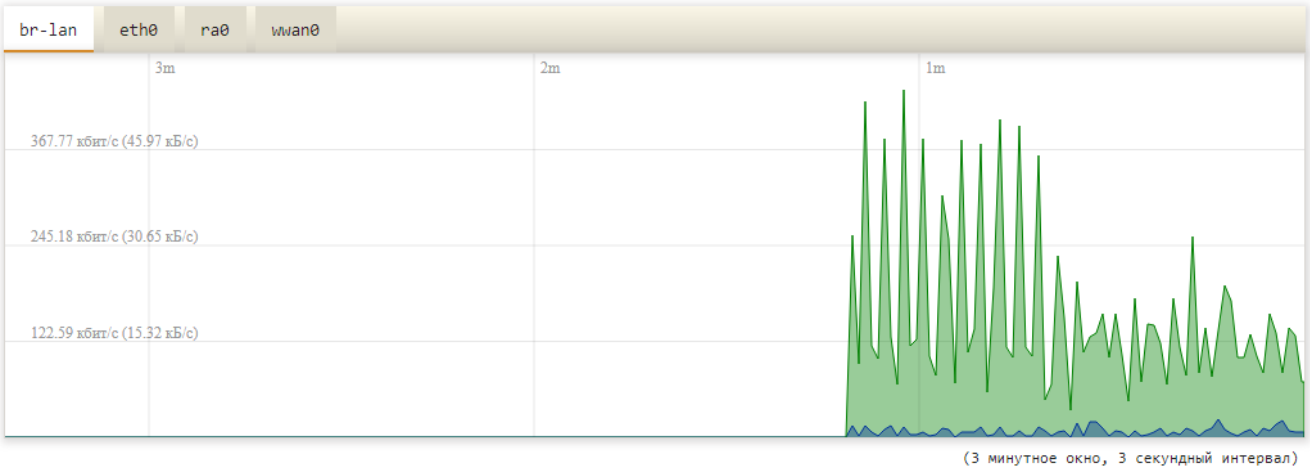

Рис.2.6. Графики в реальном времени. Вкладка «Трафик».

Таблица 2.6. Описание параметров построения графиков в реальном времени.

№	Название вкладки	Описание
1	Загрузка	Отображает уровень загрузки ЦП за последнюю минуту, 5 мин и 15
2	Трафик	Отображает входящий и исходящий трафик данных за последние 5 минут по всем интерфейсам. Выражается в Кбит/с
3	Соединения	Отображаются службы и их последние интернет-запросы

3. Меню – Система

3.1. Система

В меню «**Система → Система**» отображаются основные параметры вашего устройства, такие как имя хоста или часовой пояс. На вкладке «Журналирование» можно изменить настройки ведения журнала. (Рис.3.1).

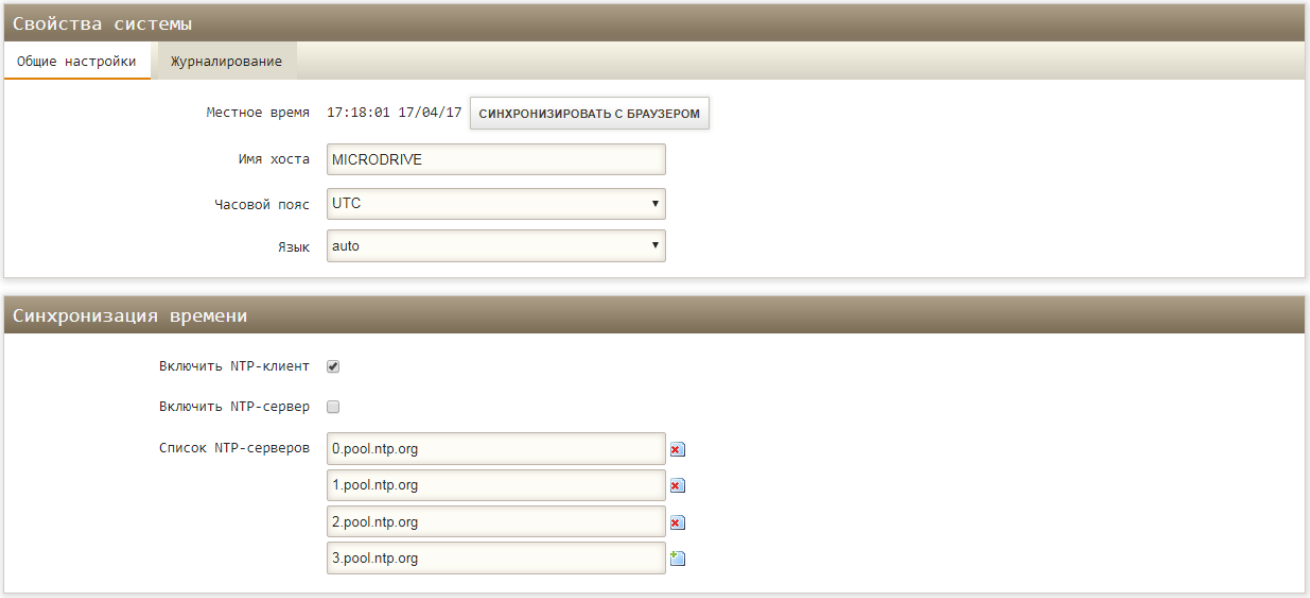

Рис.3.1. Система.

3.2. Управление

В меню «**Система → Управление**» можно задать пароль доступа к маршрутизатору. (Рис. 3.2). Здесь также расположены настройки SSH-сервера Dropbear, который позволяет подключаться к роутеру через консоль. Параметры SSH серверы расписаны в таблице 3.2. Кнопки «Добавить» и «Удалить» позволяют активировать или удалить SSH-сервер на разных интерфейсах и портах.

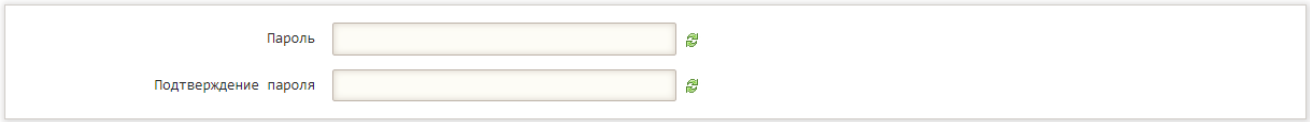

Рис.3.2. Установка пароля маршрутизатора.

Таблица 3.2. Описание параметров SSH-сервера Dropbear.

№	Название параметра	Описание
1	Интерфейс	Выбор интерфейса, по которому будет доступен сервер SSH, при выборе параметра «не определен» сервер будет доступен на всех интерфейсах
2	Порт	Порт данного процесса Dropbear
3	Аутентификация с помощью пароля	Разрешить SSH-аутентификацию с помощью пароля
4	Разрешить пользователю root вход с помощью пароля	Разрешить пользователю root вход с помощью пароля
5	Порты шлюза	Разрешить удаленным хостам подключаться к локальным перенаправленным портам SSH

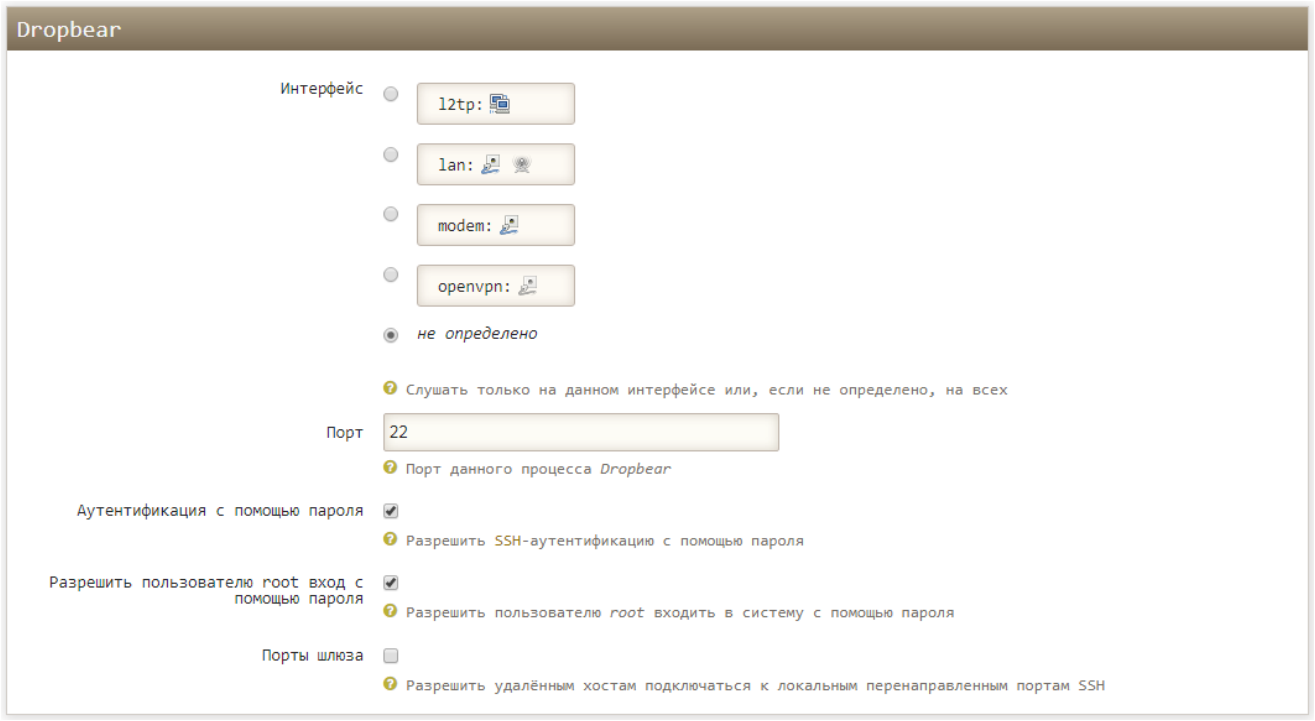

Рис.3.3. Настройка доступа через Telnet или SSH.

3.3. Резервная копия/прошивка

В меню «**Система → Резервная копия/прошивка**» можно выполнить сброс настроек устройства на заводские значения, сохранить и потом загрузить резервную копию файлов конфигурации, а также обновить прошивку устройства.

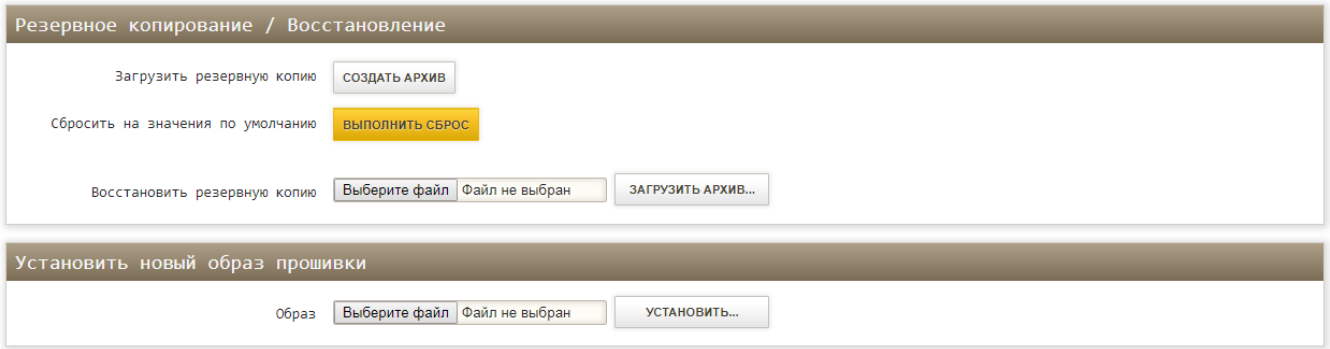

Рис.3.4. Резервная копия/прошивка.

3.4. Перезагрузка

В меню «**Система → Перезагрузка**» можно выполнить перезагрузку ОС системы устройства. Время перезагрузки составляет 30..60 сек.

4. Меню – Сервисы

4.1. AT/USSD/SMS/Поиск – AT-команды

На вкладке AT-команды можно отправлять AT-команды LTE-модулю. Пример отправки AT-команды модулю показан на (Рис.4.1).

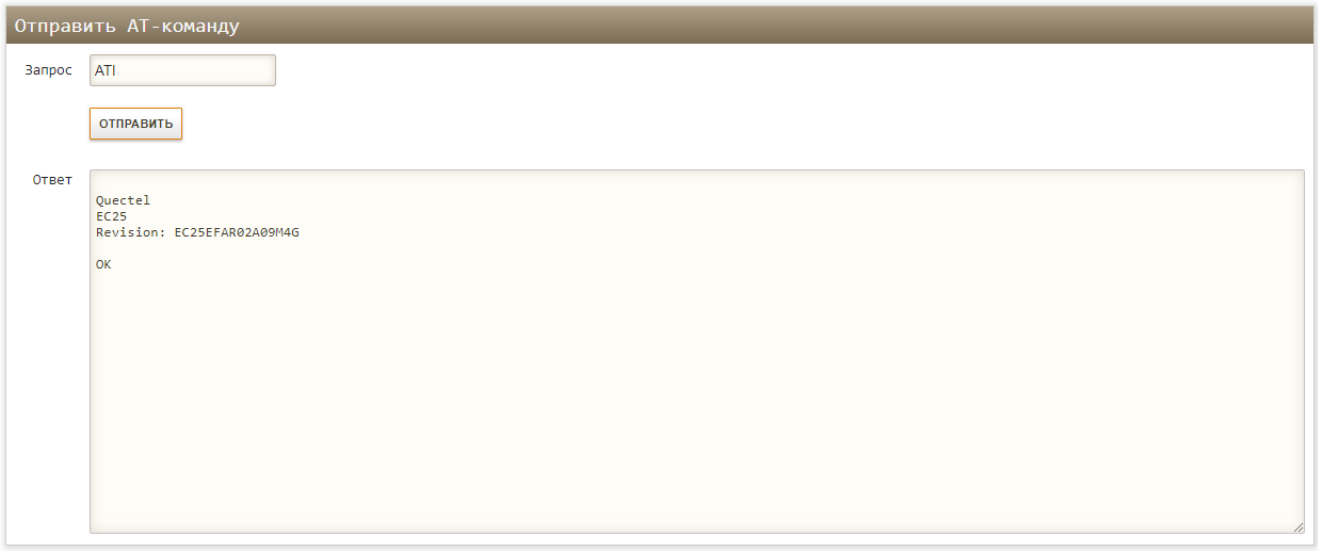

Рис.4.1. Отправка AT-команд.

Внимание!!! Отправка некоторых AT-команд может привести к некорректной работе роутера.

Использовать с осторожностью!

4.2. AT/USSD/SMS/Поиск – Отправить USSD

На этой вкладке можно отправлять USSD-запросы сотовому оператору для проверки баланса или получения другой информации. Пример отправки USSD-запросов показан на (Рис.4.2). Список USSD-запросов вашего оператора уточняйте на сайте оператора.

Для отправки запросов требуется, что бы устройство было зарегистрировано в голосовой сети.

Рис.4.2. Отправка USSD-запросов.

4.3. AT/USSD/SMS/Поиск – Отправить SMS

На этой вкладке можно отправлять SMS сообщения на мобильные номера (Рис.4.3).

Для отправки сообщений требуется, что бы устройство было зарегистрировано в голосовой сети, а на SIM-карте был положительный баланс.

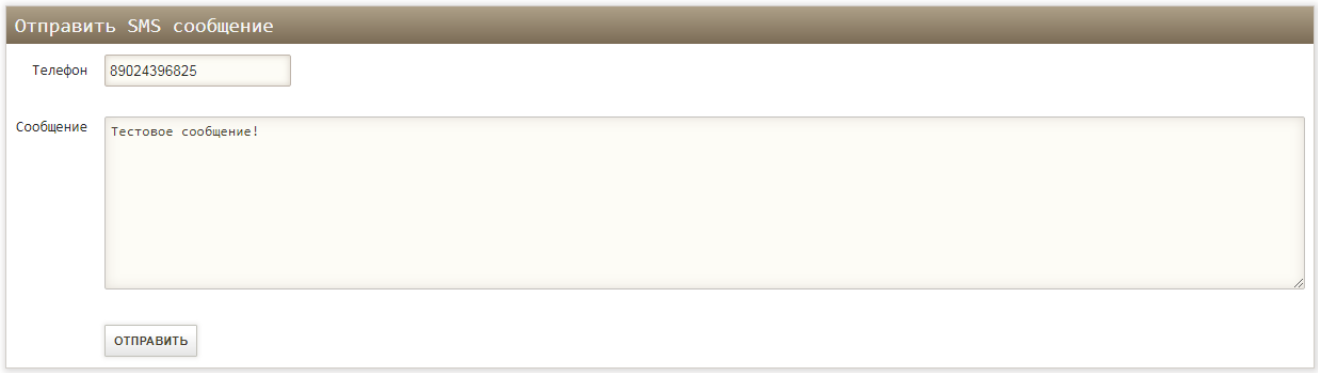

Рис.4.3. Отправка SMS.

4.4. AT/USSD/SMS/Поиск – Читать SMS

На этой вкладке можно прочитать все входящие SMS сообщения, полученные модулем LTE (Рис.4.4).

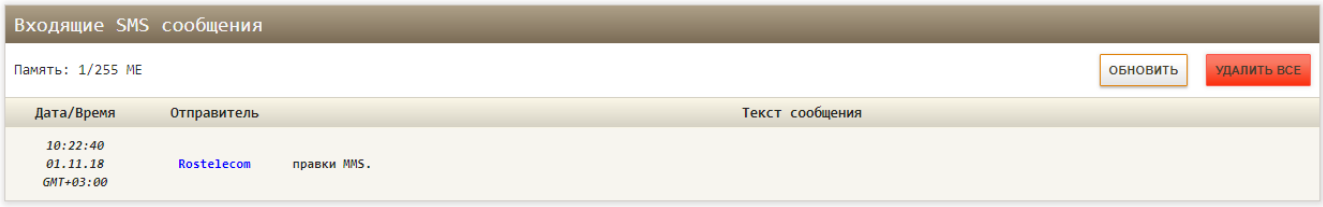

Рис.4.4. Чтение SMS.

Чтение сообщений инициируется при нажатии кнопки «Обновить». Кнопкой «Удалить все» можно удалить все SMS сообщения с SIM карты и из внутренней памяти. В верхнем левом углу параметр «Память» показывает свободную память, доступную память и тип памяти для SMS сообщений. Значение «ME» указывается на то, что SMS сообщения будут сохраняться/читаться с внутренней памяти LTE-модуля.

4.5. AT/USSD/SMS/Поиск – Поиск сетей

На этой вкладке можно выполнить поиск доступных мобильных сетей (операторов) (Рис.4.5).

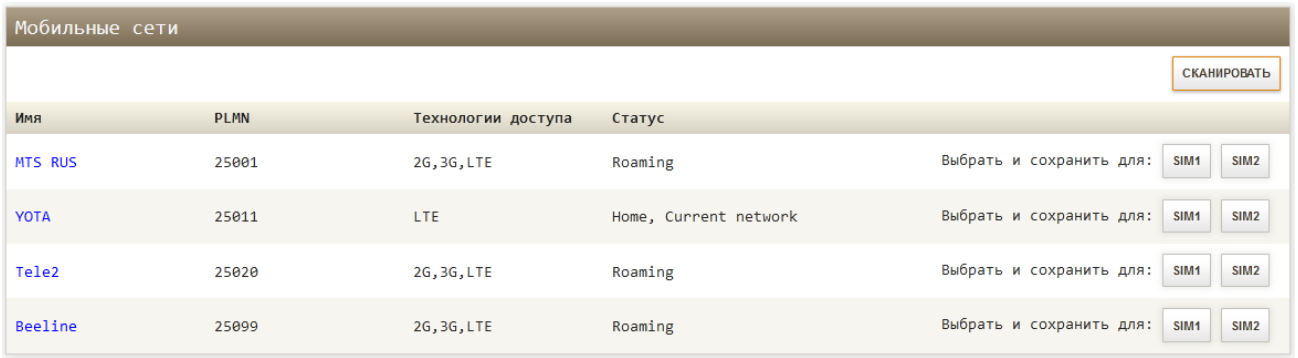

Рис.4.5. Поиск сетей (вариант с 2 SIM слотами)

Поиск мобильных сетей инициируется при нажатии кнопки «Сканировать». Интерфейс «modem» должен быть остановлен или выключен. Время сканирования не более 60 секунд. На результат сканирования влияют выбранные частотные диапазоны, но не технологии доступа. Таким образом, можно выполнить поиск сетей в необходимом диапазоне. После сканирования будет выведена таблица с найденными мобильными сетями. В колонке «Имя» выводится имя мобильного оператора, в колонке PLMN – уникальный идентификатор оператора, в колонке «Технологии доступа» - технологии, поддерживаемые оператором, в колонке «Статус» - состояние сети и выбранная сеть, в последней колонке – кнопки для ручного выбора мобильной сети для каждого SIM-профиля. Используйте ручной выбор сети только когда это действительно необходимо. При нажатии на кнопку, устройство попытается подключиться к сети, а значение PLMN сохранится в соответствующем параметре «**Сеть → Modem → SIM профиль → PLMN**». Для возврата в автоматический режим очистите этот параметр.

5. Меню – Сеть

5.1. Wi-Fi

В этом разделе выполняется настройка беспроводной сети. Можно задействовать либо отключить Wi-Fi соответствующей кнопкой. Для текущей сети Wi-Fi отображаются основные параметры, ниже находится список подключенных клиентов по Wi-Fi (Рис. 5.1.). Изменить параметры сети, включить или отключить Wi-Fi можно, нажав на кнопку «Редактировать».

Рис.5.1. Обзор Wi-Fi.

Нажав на кнопку «Редактировать», вы перейдете в меню настройки параметров беспроводной сети. (Рис. 5.2).

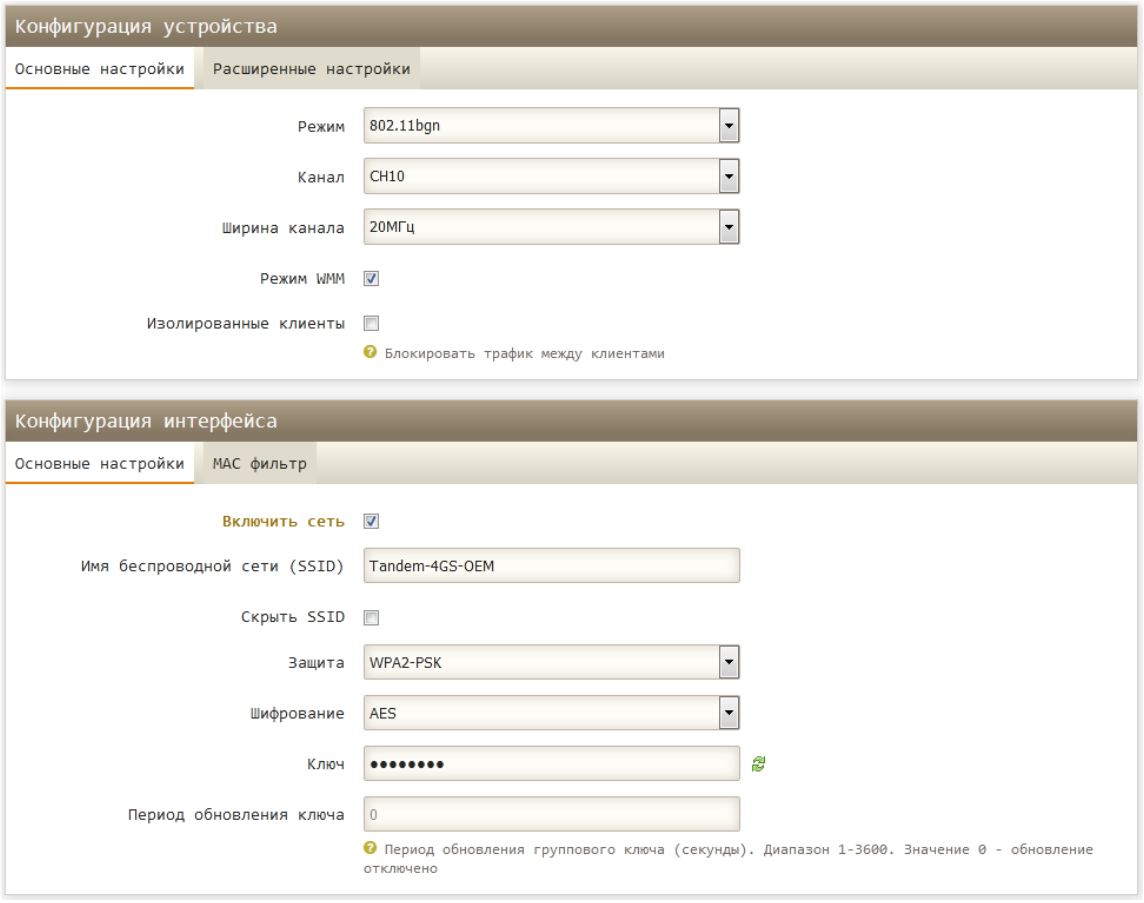

Рис.5.2. Конфигурация Wi-Fi.

Таблица 5.1. Конфигурация Wi-Fi.

№	Параметр	Описание
Конфигурация устройства. Основные настройки		
1	Режим	• 802.11b – Устаревший стандарт. Скорость до 11 Мбит/с • 802.11g – Более современный стандарт 802.11b. Скорость до 54 Мбит/с. Совместим с 802.11b • 802.11bg – Режим совместимости в стандартах 802.11b и 802.11g • 802.11gn – Самый популярный стандарт. Скорость до 150 Мбит/с. Совместимость с 802.11a/b/g • 802.11bgn – Режим совместимости со всеми стандартами b/g/n
2	Канал	Частотный канал работы беспроводной сети. В режиме «Авто» роутер выбирает наименее загруженный канал
3	Ширина канала	Позволяет управлять шириной полосы пропускания для передачи данных
4	Режим WMM	Включение режима дает приоритет в передаче пакетов мультимедийных данных
5	Изолированные клиенты	Трафик между клиентами Wi-Fi сети будет блокирован
Конфигурация устройства. Расширенные настройки		
1	Доступные каналы	Список доступных для выбора частотных каналов
2	Мощность передатчика	Настройка мощности передатчика Wi-Fi
3	Выбрать b/g защиту	Выбор режима позволяет подключаться к Wi-Fi старым устройствам работающими по стандартам 802.11b или 802.11g
4	Интервал маяка (Beacon)	Пакеты, рассылаемые точкой доступа, для синхронизации беспроводной сети. По умолчанию установлено значение 100 (рекомендуется)
5	Интервал DTIM	Интервал отправки уведомлений о доставке трафика
6	Порог фрагментации	Пакеты больше заданного значения будут фрагментироваться
7	Порог RTS	Время ожидания точкой доступа перед отправкой клиенту сообщения RTS (запрос на пересылку)
8	Короткая преамбула	Определяет длину блока CRC (циклическая контрольная сумма). Короткая преамбула увеличит пропускную способность сети, однако некоторые клиенты могут не поддерживать данный режим
9	Включить Short slot	Включение параметра уменьшает время ожидания после коллизии для повторной передачи (работает только в стандарте 802.11g)
10	Непрерывная передача (TX Burst)	Отдавать приоритет исходящему трафику
11	Поддержка IEEE 802.11H	Поддержка стандарта IEEE 802.11H, используемого для динамического снижения излучаемой мощности Wi-Fi
12	Режим совместимости	• Смешанный режим 802.11bgn – режим поддержки всех стандартов • Чистый режим 802.11n – режим работы с поддержкой только современного стандарта 802.11n
13	Интервал GI	Пустой промежуток времени между последовательно передаваемыми по беспроводной сети символами. Длинный интервал используется для снижения уровня ошибок, однако снижает скорость передачи
14	Использование RDG протокола	Включение поддержки протокола Reverse Direction Grant (Допуск обратной передачи)
15	Агрегация MSDU (A-MSDU)	Включение режима объединения фреймов в один большой кадр, работает в стандарте 802.11n
16	Включить Auto Block ACK	Включение автоматической блокировки запроса фрейма подтверждения получения пакетов
17	Принимать запросы BA	Включение режима Block acknowledgement – подтверждения блока, при котором используется одно подтверждение приема для составных кадров.
18	Запрет шифрования TKIP	Включение/Отключение запрета на шифрование по стандарту TKIP
19	Кодирование LDPC	LDPC - кодирование с малой плотностью проверок на четность
Конфигурация интерфейса. Основные настройки		
1	Включить сеть	Включение/Отключение Wi-Fi сети
2	Имя беспроводной сети (SSID)	Отображаемое имя беспроводной сети
3	Скрыть SSID	Скрытие имени беспроводной сети из вещания, используется для блокировки подключения новых абонентов к сети
4	Защита	• Open – открытая сеть без запроса пароля (не рекомендуется) • WPA-PSK – шифрование сети по стандарту WPA-PSK • WPA2-PSK – шифрование сети по современному стандарту WPA2-PSK (рекомендуется)

		• WPA/WPA2-PSK (Смешанный) – режим шифрования с поддержкой WPA-PSK и WPA2-PSK
5	Шифрование	• 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 (рекомендуется)
6	Ключ	Пароль вашей сети Wi-Fi, не менее 8 символов
7	Период обновления ключа	Период обновления группового ключа (секунды). Диапазон 1-3600. Значение 0 - обновление отключено
Конфигурация интерфейса. MAC фильтр		
1	Фильтр MAC-адреса	• Отключить – фильтр MAC-адресов отключен • Разрешить только перечисленные – разрешить подключаться к WiFi сети только клиентам с MAC-адресам перечисленными в параметре «Список MAC» • Разрешить все, кроме перечисленных – разрешить подключаться к WiFi сети всем клиентам кроме клиентов с MAC-адресам перечисленными в параметре «Список MAC»
2	Список MAC	Список MAC-адресов клиентов

5.2. MODEM

Для настройки интерфейса мобильной сети перейдите в меню «**Сеть → MODEM**». Настройки разделены на две части: общая конфигурация и SIM профили. В общей конфигурации интерфейса можно включить/отключить интерфейс, выбрать режим шлюза, задать метрику, DNS серверы и выбрать зону межсетевого экрана. В окне SIM профили находятся индивидуальные настройки для каждой SIM-карты (если устройство поддерживает более одной SIM-карты). Более подробное описание настроек смотрите в таблице 5.2 и 5.3. Статус подключения можно проконтролировать в меню **«Статус → Интерфейсы»** или «**Статус → Обзор**» в окнах «Мобильная сеть» и «Сеть».

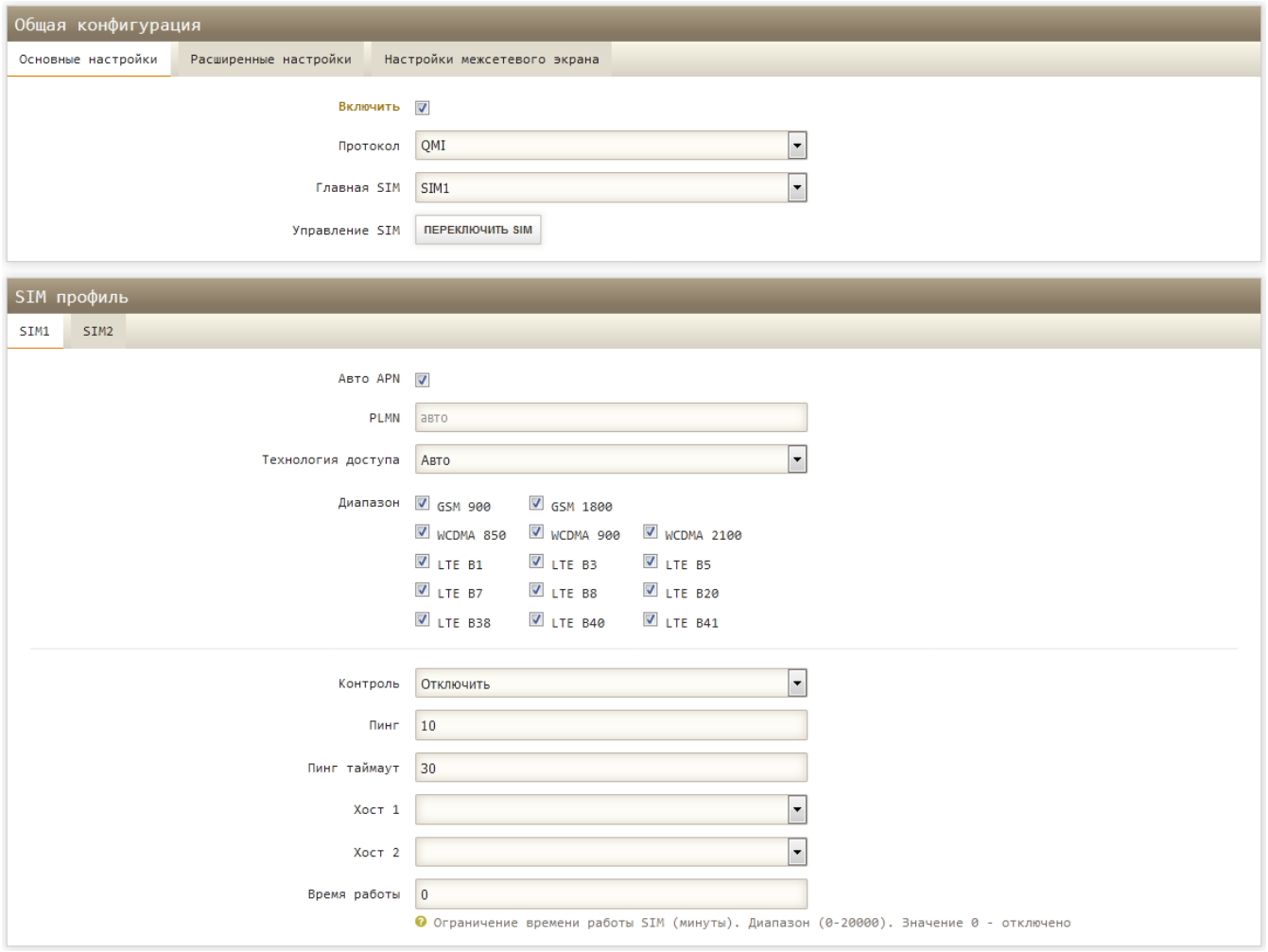

Рис.5.2. Основные настройки интерфейса «MODEM» (вариант с 2 SIM слотами).

Таблица 5.2. Общая конфигурация.

№	Параметр	Описание	Модели
Основные настройки			
1	Включить	Включить/Отключить интерфейс «MODEM». Если галочка установлена, то интерфейс будет пытаться запустить соединение сразу после загрузки операционной системы роутера	
2	Протокол	Протокол с LTE-модулем. Для мобильного интернета используется протокол QMI.	
3	Главная SIM	Задается SIM-слот после загрузки операционной системы	**2 SIM**
4	Управление SIM	Оперативное переключение на другой SIM-слот	**2 SIM**
Расширенные настройки			
1	Использовать шлюз по умолчанию	Если установлена галочка, то в таблицу маршрутизации будет добавлен маршрут «по умолчанию» через этот интерфейс	
2	Использовать метрику шлюза	Задает метрику маршрутов через этот интерфейс. Ввод определенной метрики может быть полезен при использовании нескольких WAN-интерфейсов. Метрика определяет приоритет одинаковых маршрутов.	
3	Использовать выданный DNS	Если установлена галочка, то будут использоваться DNS сервера, выданные оператором мобильной сети. Для ручного ввода DNS-адресов, снимите	

		галочку	
4	Использовать собственный DNS-сервер	Задается IP адрес DNS серверов	
Настройки межсетевого экрана			
1	Создать/назначить зону сетевого экрана	Укажите зону, к которой вы хотите прикрепить этот интерфейс. Для доступа в интернет должна стоять зона «wan»	

Таблица 5.3. SIM профиль.

№	Параметр	Описание	
SIM1/SIM2			
1	Авто APN	Если установлена галочка, то роутер автоматически определяет настройки (APN, имя пользователь, пароль, метод аутентификации) из внутренней базы данных. Автоматическое определение работает только для Российских сотовых операторов. Для использования специфических услуг вроде «выделенный IP», требуется вручную задавать эти настройки	
2	APN	Имя точки доступа оператора связи. Например: ***internet.mts.ru***	
3	Имя пользователя PAP/CHAP	Имя пользователя по протоколу аутентификации. Может быть пустым для большинства операторов	
4	Пароль PAP/CHAP	Пароль по протоколу аутентификации. Может быть пустым для большинства операторов	
5	Тип аутентификации	Выбор протокола аутентификации устройства	
6	PLMN	PLMN (уникальный идентификатор) предпочтительного мобильного оператора. Например: 25001 (МТС) или 25020 (Tele2). Модем будет пытаться зарегистрироваться в сети с указанным PLMN. Если параметр пустой или 0, модем будет регистрироваться в автоматическом режиме.	
7	Технология доступа	Выбор технологии доступа: только 2G, 3G, LTE либо автоматический выбор	
8	Диапазон	Выбор частотного диапазона	
9	Контроль	Включает/отключает функцию управления SIM-картами и контроля мобильного подключения. Для включения функции необходимо также задать IP адрес Хост1 и/или Хост2. Алгоритм работы описан в 5.2.1	
10	Пинг	Интервал (сек.) отправки тестовых пакетов на Хост1, Хост2. Тестовые пакеты отправляются по очереди на Хост1 и Хост2, с половинным интервалом	
11	Пинг таймаут	Допустимый интервал (сек.) ожидания ответов от Хост1, Хост2. Если по истечении интервала не было принято ни одного ответа, будет выполнено действие, заданное в параметре «**Контроль**»	
12	Время работы	Ограничение времени работы SIM-карты (минуты). Значение 0 – отключено. По истечении интервала будет выполнено действие, заданное в параметре «**Контроль**»	**2 SIM**

5.2.1 Алгоритм работы функции контроля мобильного подключения и автоматического переключения SIM-карт

Функция обеспечивает непрерывный контроль мобильного подключения (интернета) путем отправки тестовых пакетов до удаленных хостов. Тестовые пакеты отправляются к Хосту 1 и Хосту 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, будет выполнен 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 ранее чем через 1 минуту. Для исключения ложных перезапусков соединения или переключений SIM-карт, интервал «**Пинг таймаут**» должен быть больше интервала «**Пинг**» в 3 и более раз.

Для моделей с двумя и более SIM-картами, дополнительно может настраиваться лимит времени, 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.

Параметры	Профиль SIM1	Профиль 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

5.2.2 Тестирование

Для проверки функции контроля и переключения SIM-карт можно воспользоваться AT-командами в меню «**Сервисы → AT/USSD/SMS/Поиск»:**

AT+CFUN=4 - отключить радиопередатчик LTE модуля

AT+CFUN=1 - включить радиопередатчик LTE модуля

Для имитации отказа сотовой сети используйте команду **AT+CFUN=4.** Используйте системный журнал в меню «**Статус → Системный журнал»** для анализа работы. Служба, которая управляет мобильным подключением и управляет SIM-картами, создает записи в журнале с пометкой «cm».

Пример журнала:

```
. . . .
Thu Jun 11 11:34:00 2020 daemon.info cm[881]: SIM1, PS=detached, CS=detached, PLMN=25011, Radio=LTE, Reg=2  – обнаружена сеть YOTA
Thu Jun 11 11:34:01 2020 daemon.info cm[881]: SIM1, PS=attached, CS=detached, PLMN=25011, Radio=LTE, Reg=1  – регистрация в сети YOTA
Thu Jun 11 11:34:02 2020 daemon.info cm[881]: activate PDN(ipv4): SIM1, apn="internet.yota"/""/""/none …  – попытка подключиться
Thu Jun 11 11:34:02 2020 daemon.info cm[881]: CONNECTED: ipv4=10.62.73.22/255.255.255.252, ipv6=/, mtu=1500 – подключение установлено
. . . .
```

5.3. LAN

LAN интерфейс – это интерфейс сетевого моста (Bridge). Мост объединяет интерфейсы Wi-Fi (ra0) и Ethernet (eth0). Задать IP-адрес и маску подсети можно в меню «**Сеть → LAN**» (Рис. 5.4). По заданному IP-адресу будет доступен WEB-интерфейс роутера.

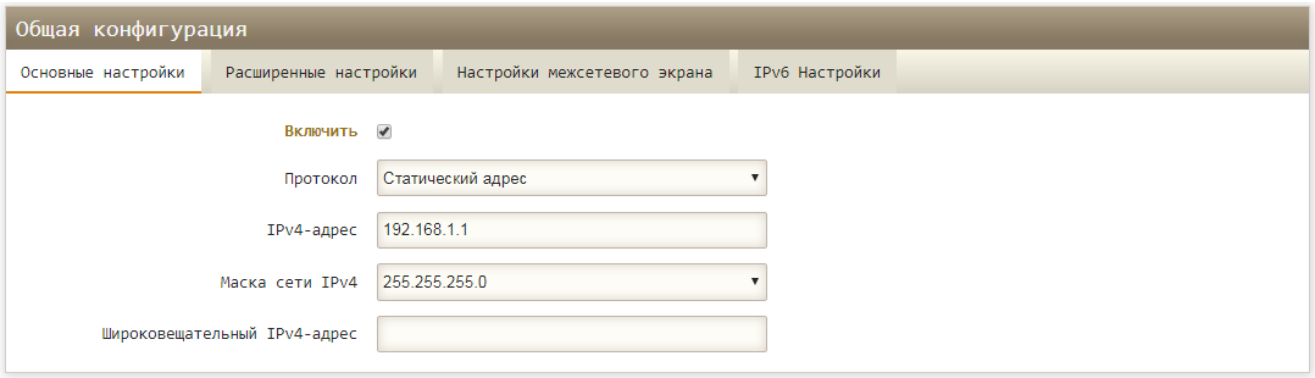

Рис.5.4. Установка IP-адреса и маски подсети LAN интерфейса.

Таблица 5.4. Конфигурация интерфейса LAN.

№	Параметр	Описание
Основные настройки		
1	Включить	Включить/Отключить интерфейс LAN. Если галочка установлена, то интерфейс будет запущен сразу после загрузки операционной системы ***Отключение интерфейса приведет к потере доступа к роутеру через Ethernet и Wi-Fi!!!***
2	Протокол	Режим работы интерфейса
3	IPv4-адрес	IP-адрес интерфейса. Должен быть задан в соответствии с общепринятыми правилами распределения сетевых адресов
4	Маска сети IPv4	Битовая маска сети IPv4 для определения размера сети, по умолчанию 255.255.255.0
5	Широковещательный IPv4-адрес	IP-адрес для передачи широковещательных пакетов в локальную сеть, по умолчанию - 192.168.1.255
Расширенные настройки		
1	Назначить MAC-адрес	Назначение MAC-адреса интерфейсу
2	Назначить MTU	MTU (Maximum Transmission Unit) определяет максимальный размер пакета данных через этот интерфейс
3	Использовать метрику шлюза	Задает метрику маршрутов через этот интерфейс
4	Использовать собственные DNS-серверы	Добавление DNS-адресов
Настройки межсетевого экрана		
1	Создать/назначить зону сетевого экрана	Укажите зону, к которой вы хотите прикрепить этот интерфейс. Для этого интерфейса должны быть задана зона – «lan»
IPv6 Настройки		
1	IPv6 длина префикса	Определяет количество бит в IPv6-адресе. По умолчанию 60
2	IPv6 длина sub-префикса	Определяет количество бит в IPv6-адресе подсети

В окне «DHCP-сервер» (Рис.5.5). Галочка «Включить DHCP» включает DHCP сервер на этом интерфейсе.

Диапазон выдаваемых IP-адресов задается параметрами «Старт», «Предел». Подробное описание настроек DHCP-сервера описано в таблице 5.5.

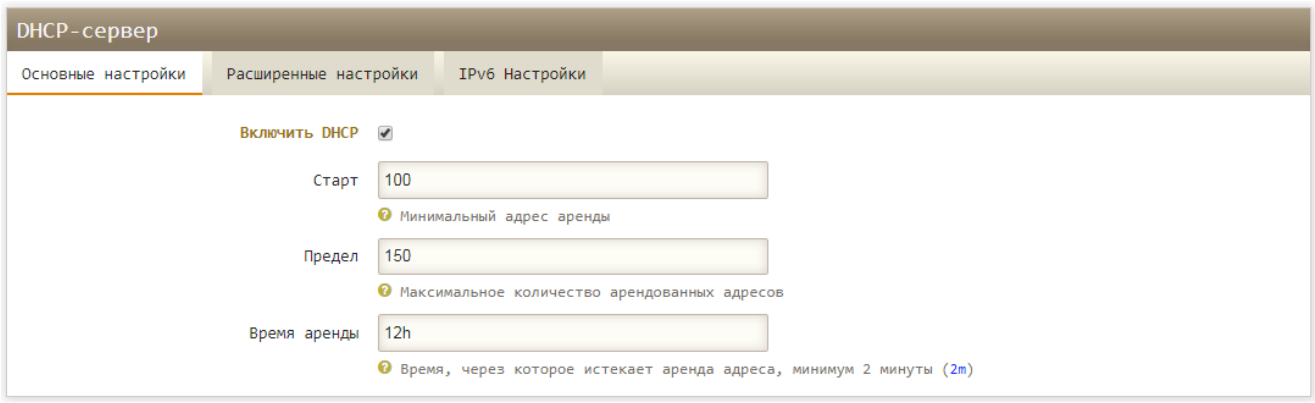

Рис.5.5. Настройка DHCP-сервера.

Таблица 5.5. Параметры DHCP-сервера.

№	Параметр	Описание
Основные настройки		
1	Включить DHCP	Отключить/Включить DHCP-сервер для данного интерфейса
2	Старт	Минимальный адрес, выдаваемый DHCP-сервером клиенту
3	Предел	Максимальное количество арендованных адресов
5	Время аренды	Время, через которое истекает аренда адреса, минимум 2 минуты
Расширенные настройки		
1	Динамический DHCP	Динамически выделять DHCP-адреса клиентам. Если выключено, то будут обслужены только клиенты с постоянно арендованными адресами
2	Принудительно	Использовать DHCP в этой сети, даже если найден другой сервер
3	Маска сети IPv4	Предопределение сетевой маски, отправляемую клиентам
4	DHCP-Настройки	Определить дополнительные опции DHCP, например, "6,192.168.2.1,192.168.2.2", чтобы известить клиентов о DNS-серверах
IPv6 Настройки		
1	Router Advertisement-Сервис	• Отключено – служба отключена • Server mode – служба включена, роутер является сервером DHCPv6 • Relay mode – режим трансляции Advertisement-сообщений для клиентов сети IPv6 • Hybrid mode – гибридный режим, объединяющий Server и Relay mode
2	DHCPv6-Сервис	• Отключено – служба отключена • Server mode – служба включена, роутер является сервером DHCPv6 • Relay mode – режим трансляции DHCPv6 сервера для клиентов сети IPv6 • Hybrid mode – гибридный режим, объединяющий Server и Relay mode
3	NDP-Прокси	Режим поиска соседних прокси-серверов DHCPv6
4	DHCPv6-Режим	• Stateless – назначение IPv6 адреса не сохраняет путь до клиента • Stateless+Statefull – гибридный режим сохранения пути до клиента • Statefull – DHCPv6 хранит путь до клиента
5	Всегда объявлять роутером по умолчанию	Объявлять роутером по умолчанию, даже если нет доступных публичных префиксов
6	Заявленные DNS серверы	Добавление DNS-серверов IPv6
7	Заявленные DNS домены	Добавление DNS-доменов IPv6

5.4. VPN

VPN – технология, которая позволяет создавать виртуальные частные сети, через мобильное интернет-подключение.

5.4.1 Интерфейс L2TP

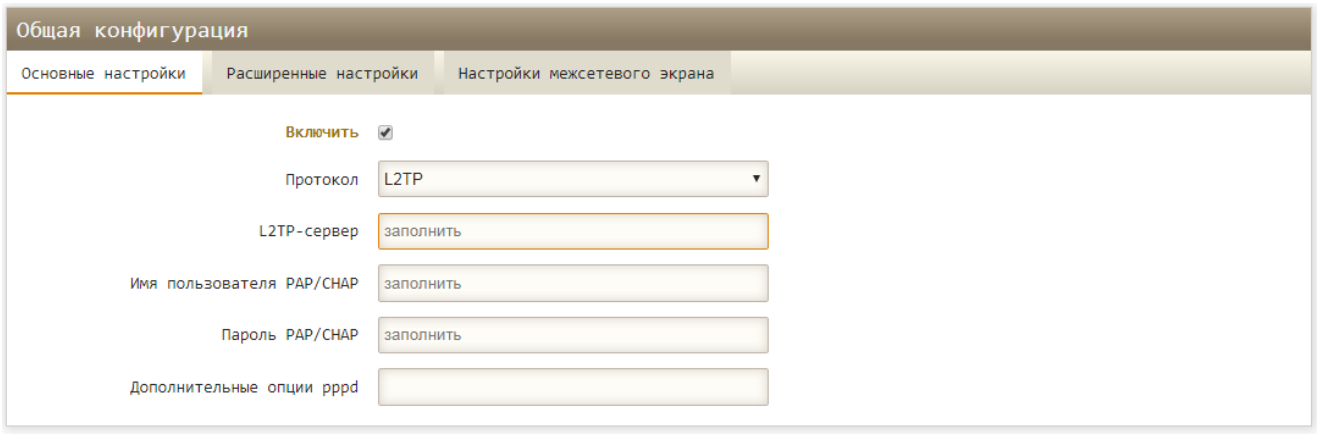

Рис.5.6. Настройка интерфейса VPN L2TP.

Таблица 5.6. Параметры VPN.

№	Параметр	Описание
1	Включить	Включить/Отключить интерфейс L2TP. Если галочка установлена, то интерфейс будет запущен сразу после загрузки операционной системы
2	Протокол	Выбор протокола. Доступен только L2TP протокол
3	L2TP-сервер	Доменное имя или IP-адрес удаленного узла (сервера), к которому будет подключаться клиент
4	Имя пользователя PAP/CHAP	Имя пользователя для авторизации на сервере
5	Пароль PAP/CHAP	Пароль для авторизации на сервере
6	Дополнительные опции pppd	Передать дополнительные опции службе pppd
Расширенные настройки		
1	Использовать шлюз по умолчанию	Если установлена галочка, то в таблицу маршрутизации будет добавлен маршрут «по умолчанию» через этот интерфейс
2	Использовать метрику шлюза	Задает метрику маршрутов через этот интерфейс. Метрика определяет приоритет одинаковых маршрутов
3	Назначить MTU	MTU (Maximum Transmission Unit) определяет максимальный размер пакета данных через этот интерфейс
4	Интервал эхо-запросов LCP	Отправлять серверу эхо-пакеты LCP с указанным интервалом (секунды). Используется для контроля соединения
5	Порог ошибок эхо-запросов LCP	После указанного кол-ва ошибок (отсутствие ответов) соединение с сервером будет установлено заново. Значение 0 используется для игнорирования ошибок
Настройки межсетевого экрана		
1	Создать/назначить зону сетевого экрана	Укажите зону, 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

5.4.2 Интерфейс OPENVPN

В ОС роутера установлен клиент OpenVPN 2.4.0. OpenVPN реализует следующие возможности:

- Создание VPN-туннеля типа «точка-точка» уровня L2/L3 с аутентификацией по общему секретному ключу (shared key) или без аутентификации.
- Создание VPN-туннеля типа «Сеть» уровня L2/L3 с аутентификацией TLS при помощи сертификатов и закрытых ключей (TLS-клиент). Дополнительная аутентификация по логину и паролю. Аутентификация канала управления TLS при помощи общего закрытого ключа.
- Перенаправление интернет трафика через туннель. Конфигурация VPN-шлюз.
- Сжатие LZO, LZ4
- Транспортный протокол – UDP или TCP.

Таблица 5.7. Параметры VPN.

№	Параметр	Описание	Опция
Основные настройки			
1	Включить	Включить/Отключить интерфейс VPN. Если галочка установлена, то интерфейс будет запущен сразу после загрузки операционной системы	
2	Протокол	Выбор протокола VPN. Доступен только OPENVPN протокол	
3	TUN/TAP	Выбор типа кадров при инкапсуляции. TUN (L3) – инкапсулируются кадры IPv4, TAP (L2) – инкапсулируются кадры Ethernet	***dev***
4	Мост	Добавить в мост LAN	
5	Транспортный протокол	Выбор транспортного протокола	***proto***
6	Удаленный хост/IP	Доменное имя или IP-адрес удаленного узла (сервера), к которому будет подключаться клиент	***remote***
7	Порт	Порт удаленного узла (сервера)	***port***
8	Сжатие	Выбор сжатия LZO. Значение «По умолчанию» – опция игнорируется, «Отключено» – сжатие отключено. «LZO» – алгоритм сжатия LZO, «LZ4» – алгоритм сжатия LZ4	***compress***
9	Пинг	Интервал, в секундах, отправки тестовых пакетов удаленному узлу (серверу) для проверки целостности соединения и актуализации NAT. Рекомендуемое значение – от 5 до 30 секунд	***ping***
10	Пинг таймаут	Интервал, в секундах, по истечении которого происходит повторное подключение, при отсутствии тестовых пакетов от удаленного узла (сервера)	***ping-restart***
11	Аутентификация	Выбор алгоритма аутентификации подключения	***secret, tls-client***
12	Шифрование	Выбор алгоритма шифрования канала передачи данных. Если установлено значение по умолчанию, будет использоваться алгоритм BF-CBC	***cipher***
13	Локальный VPN IP	IP-адрес локального интерфейса TUN/TAP	***ifconfig_l***
14	Удаленный VPN IP	IP-адрес удаленного интерфейса TUN/TAP	***ifconfig_r***
15	Маска сети VPN	Маска сетевого интерфейса TAP	***ifconfig***
16	Шлюз VPN IP	IP-адрес шлюза в сети VPN, через который могут быть добавлены маршруты	***route-gateway***
Расширенные настройки			
1	Дополнительная конфигурация	Задаются дополнительные опции клиента OpenVPN, которые будут добавлены к основной конфигурации при запуске интерфейса	
Настройки межсетевого экрана			
1	Создать/назначить зону сетевого экрана	Укажите зону, 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	
Аутентификация			
1	Общий ключ	Общий ключ для шифрования соединения типа точка-точка. Ключ должен включать заголовок: -----*BEGIN OpenVPN Static key V1*----- и заканчиваться: -----*END OpenVPN Static key V1*-----	***secret***
2	Сертификат CA	Сертификат удостоверяющего центра. Сертификат должен включать	***ca***

		заголовок: *-----BEGIN CERTIFICATE-----* и заканчиваться: *-----END CERTIFICATE-----*	
3	Сертификат клиента	Подписанный сертификат клиента. Содержит открытый ключ и дополнительные атрибуты: имя клиента, срок действия и др. Должен заканчиваться: *-----END CERTIFICATE-----*	***cert***
4	Ключ клиента	Закрытый ключ клиента. Ключ должен включать заголовок: *-----BEGIN PRIVATE KEY-----* и заканчиваться: *-----END PRIVATE KEY-----*	***key***
5	Логин	Дополнительная аутентификация по логину и паролю	
6	Пароль	Дополнительная аутентификация по логину и паролю	
7	TLS аутентификация	Включить/Отключить дополнительный уровень аутентификации канала управления TLS.	
8	Ключ TLS аутентификации	Общий ключ для шифрования канала управления TLS. Ключ должен включать заголовок: *-----BEGIN OpenVPN Static key V1-----* и заканчиваться: *-----END OpenVPN Static key V1-----*	***tls-auth***

5.4.3 Настройка туннеля L2 с аутентификацией по общему ключу (Shared secret)

В конфигурации OpenVPN туннеля TAP (L2) с аутентификацией по общему ключу одно из устройств (роутер) должно выступать в роли сервера и иметь статический белый IP-адрес, второе устройство (LTE-роутер) может иметь динамический IP-адрес (Рис.5.7). Пример настройки для клиента (LTE-роутера) приведен в таблице 5.8.

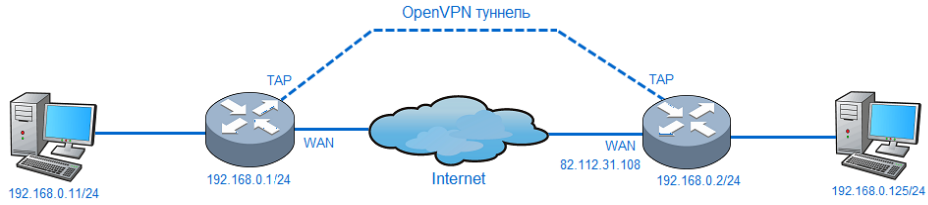

Рис.5.7. Пример топологии «точка-точка, уровень L2.

Таблица 5.8. Пример настройки для конфигурации Рис.5.7.

Параметр	Значение
Основные настройки	
TUN/TAP	TAP (L2)
Мост	LAN
Транспортный протокол	Может быть UDP или TCP
Удаленный хост/IP	82.112.31.108. Статический IP адрес или доменное имя второго узла
Порт	1194
Сжатие	По умолчанию
Пинг	10
Пинг таймаут	60
Аутентификация	Shared secret
Шифрование	AES-128-CBC
Локальный VPN IP	Оставить пустым
Маска сети VPN	Оставить пустым
Шлюз VPN	Оставить пустым
Настройка межсетевого экрана	
Зона	lan
Аутентификация	
Общий ключ	Скопируйте содержимое файла с общим ключом

192.168.0.11/24 – хост или сеть за LTE-роутером

192.168.0.1/24 – интерфейс сетевого моста LAN LTE-роутера, в который должен быть добавлен TAP интерфейс

192.168.0.125/24 – хост или сеть за роутером, выполняющего роль сервера

192.168.0.2/24 – интерфейс сетевого моста, в который должен быть добавлен TAP интерфейс

82.112.31.108 – WAN интерфейс

5.4.4 Настройка туннеля L2 с аутентификацией TLS

В конфигурации OpenVPN туннеля TAP (L2) с аутентификацией TLS должен присутствовать сервер, к которому будут подключаться клиенты (Рис.5.8). Клиенты могут иметь динамические или статические IP-адреса. Пример настройки для клиента (LTE-роутера) приведен в таблице 5.9.

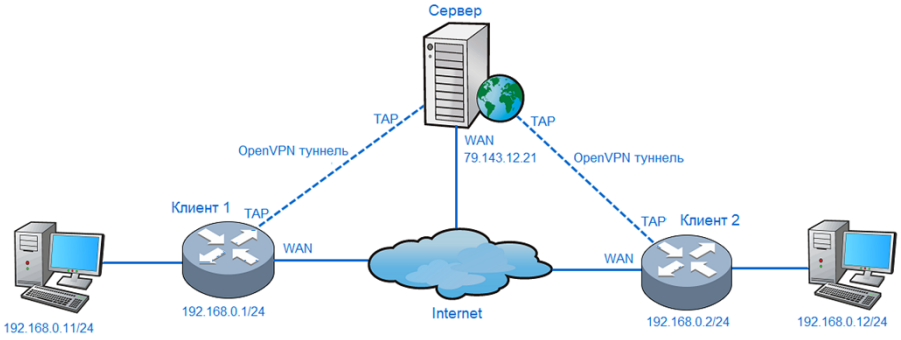

Рис.5.8. Пример топологии «Сеть», уровень L2.

Таблица 5.9. Пример настройки для конфигурации Рис.5.8.

Параметр	Значение
Основные настройки	
TUN/TAP	TAP (L2)
Мост	LAN
Транспортный протокол	Может быть UDP или TCP
Удаленный хост/IP	79.143.12.21. Статический IP адрес сервера
Порт	1194
Сжатие	По умолчанию
Пинг	10
Пинг таймаут	60
Аутентификация	TLS Client
Шифрование	AES-128-CBC
Настройка межсетевого экрана	
Зона	lan
Аутентификация	
Сертификат CA	Скопируйте содержимое файла с сертификатом CA
Сертификат клиента	Скопируйте содержимое файла с сертификатом клиента
Ключ клиента	Скопируйте 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	Отключена

192.168.0.11/24 – хост или сеть за Клиентом 1

192.168.0.1/24 – интерфейс сетевого моста Клиента 1, в который должен быть добавлен TAP интерфейс

192.168.0.12/24 – хост или сеть за Клиентом 2

192.168.0.2/24 – интерфейс сетевого моста Клиента 2, в который должен быть добавлен TAP интерфейс

79.143.12.21 – WAN интерфейс сервера

В конфигурации сервера следуют отключить функцию присвоения IP-адресов для клиентов (опция ***server-bridge*** без параметров).

5.4.5 Настройка туннеля L3 с аутентификацией по общему ключу (Shared secret)

В конфигурации OpenVPN туннеля TUN (L3) с аутентификацией по общему ключу одно из устройств (роутер) должно выступать в роли сервера и иметь статический белый IP-адрес, второе устройство (LTE-роутер) может иметь динамический IP-адрес (Рис.5.9). Пример настройки для клиента (LTE-роутера) приведен в таблице 5.10.

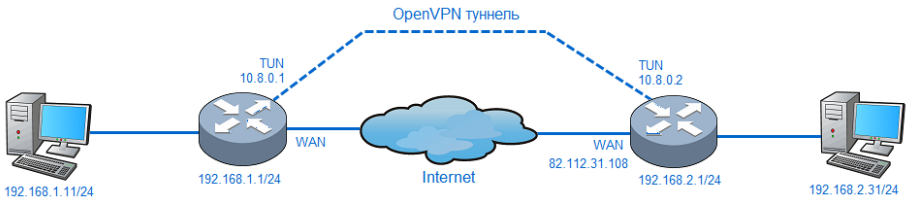

Рис.5.9. Пример топологии «точка-точка», уровень L3.

Таблица 5.9. Пример настройки для конфигурации Рис.5.10.

Параметр	Значение
Основные настройки	
TUN/TAP	TUN (L3)
Транспортный протокол	Может быть UDP или TCP
Удаленный хост/IP	82.112.31.108. Статический IP адрес или доменное имя второго узла
Порт	1194
Сжатие	По умолчанию
Пинг	10
Пинг таймаут	60
Аутентификация	Shared secret
Шифрование	AES-128-CBC
Локальный VPN IP	10.8.0.1
Удаленный VPN IP	10.8.0.2
Добавить маршрут	Сеть 192.168.2.0/24
Настройка межсетевого экрана	
Зона	lan
Аутентификация	
Общий ключ	Скопируйте содержимое файла с общим ключом

192.168.1.11/24 – хост или сеть за LTE-роутером

192.168.1.1/24 – интерфейс LAN роутера

192.168.2.31/24 – хост или сеть за роутером, выполняющего роль сервера

192.168.2.1/24 – интерфейс LAN роутера

10.8.0.1 – интерфейс TUN LTE-роутера

10.8.0.2 – интерфейс TUN удаленного узла, выполняющего роль сервера

82.112.31.108 – WAN интерфейс

5.4.6 Настройка туннеля L3 с аутентификацией TLS

В конфигурации OpenVPN туннеля TUN (L3) с аутентификацией TLS должен присутствовать сервер, к которому будут подключаться клиенты (Рис.5.10). Клиенты могут иметь динамические или статические IP-адреса. Пример настройки для клиента (LTE-роутера) приведен в таблице 5.11.

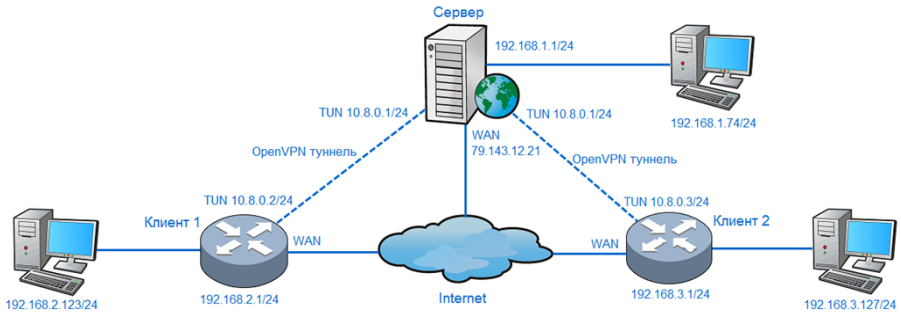

Рис.5.10. Пример топологии «Сеть», уровень L3.

Таблица 5.11. Пример настройки для конфигурации Рис.5.10.

Параметр	Значение
Основные настройки	
TUN/TAP	TUN (L3)
Транспортный протокол	Может быть UDP или TCP
Удаленный хост/IP	79.143.12.21. Статический IP адрес сервера
Порт	1194
Сжатие	По умолчанию
Пинг	10
Пинг таймаут	60
Аутентификация	TLS Client
Шифрование	AES-128-CBC
Настройка межсетевого экрана	
Зона	lan
Аутентификация	
Сертификат CA	Скопируйте содержимое файла с сертификатом CA
Сертификат клиента	Скопируйте содержимое файла с сертификатом клиента
Ключ клиента	Скопируйте 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	Отключена

192.168.2.123/24 – хост или сеть за Клиентом 1

192.168.2.1/24 – интерфейс LAN Клиента 1

192.168.3.127/24 – хост или сеть за Клиентом 2

192.168.3.1/24 – интерфейс LAN Клиента 2

192.168.1.74/24 – хост или сеть за Сервером

192.168.1.1/24 – интерфейс LAN Сервера

10.8.0.1/24 – интерфейс TUN Сервера

10.8.0.2/24 – интерфейс TUN Клиента 1

10.8.0.3/24 – интерфейс TUN Клиента 2

79.143.12.21 – WAN интерфейс 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.

5.4.7 VPN шлюз

Для перенаправления интернет трафика в туннель VPN может быть использована топология, показанная на рисунке 5.9 и 5.10.

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

1) Прямой маршрут до удаленного узла

Интерфейс	MODEM
Цель	82.112.31.108. Статический IP адрес
Маска сети	255.255.255.255
Шлюз	Оставить пустым
Метрика	Оставить пустым
MTU	Оставить пустым
Тип маршрута	unicast

2) Маршрут «по умолчанию»

Интерфейс	VPN
Цель	0.0.0.0
Маска сети	0.0.0.0
Шлюз	10.8.0.2
Метрика	Оставить пустым

MTU	Оставить пустым
Тип маршрута	unicast

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 и запретить входящий трафик.

5.4.8 Диагностика

Отслеживать статус VPN интерфейса можно в меню «**Статус → Интерфейсы**». Отладочные сообщения OpenVPN клиента будут записаны в системный журнал, прочитать системный журнал можно в меню «**Статус → Системный журнал».** Отправить «***ping***» можно в меню «**Статус → Диагностика**».

5.5. DHCP и DNS

Список настроек меню DHCP и DNS представлен в таблице 5.12.

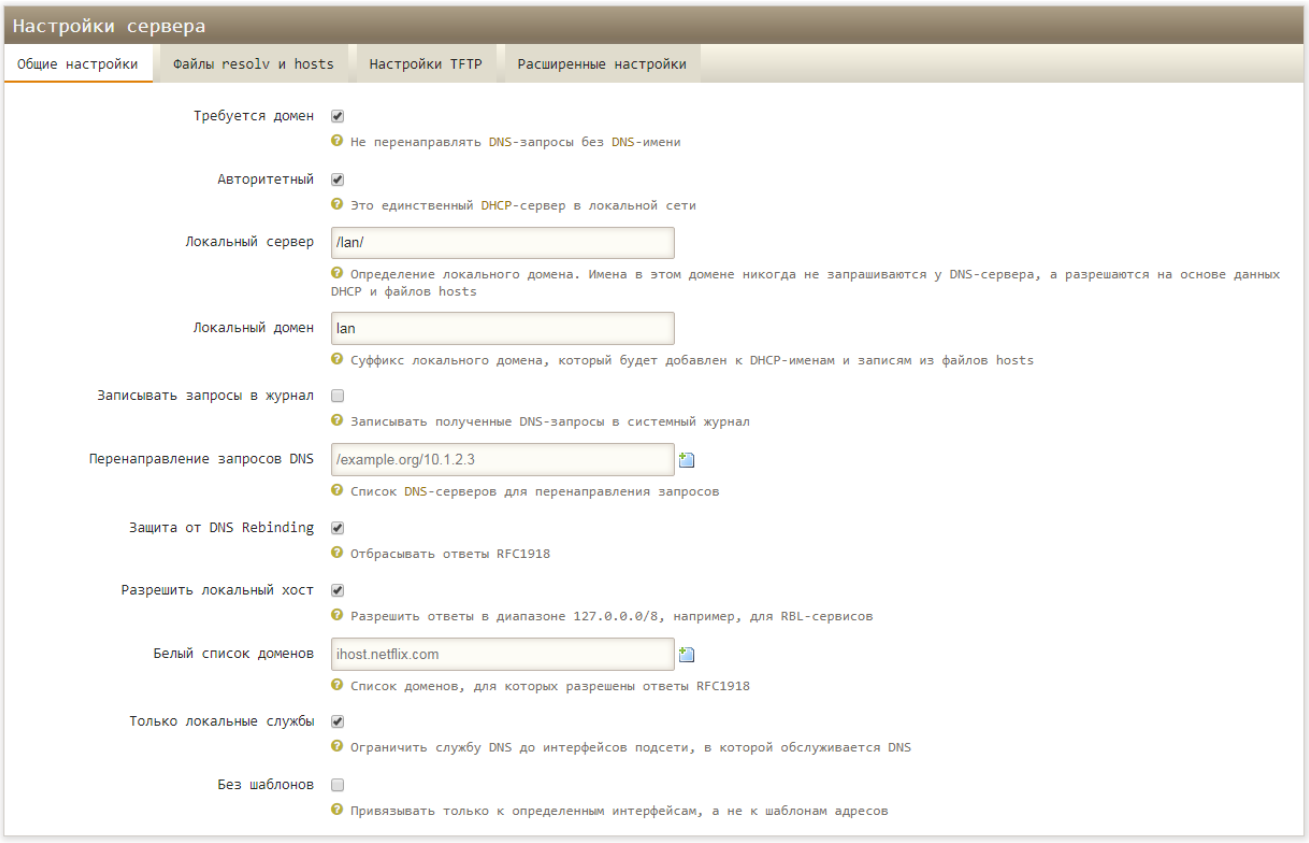

Рис.5.11. DHCP и DNS.

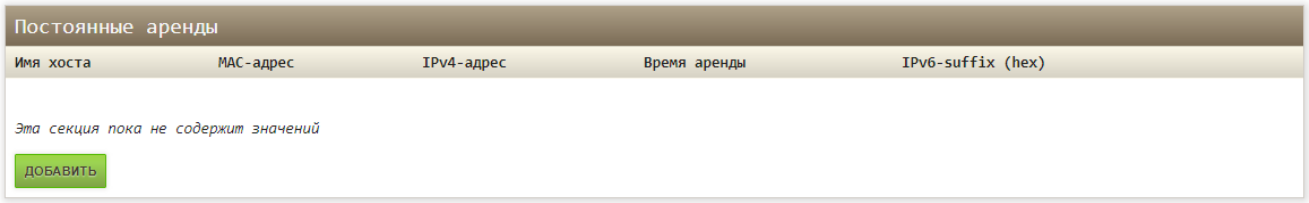

Рис.5.12. Постоянные аренды.

Таблица 5.12. Параметры DHCP и DNS.

№	Параметр	Описание
Общие настройки		
1	Требуется домен	Не перенаправлять DNS-запросы без DNS-имени
2	Авторитетный	Галочка означает, что это единственный DHCP-сервер в локальной сети
3	Локальный сервер	Определение локального домена. Имена в этом домене никогда не запрашиваются у DNS-сервера, а разрешаются на основе данных DHCP и файлов hosts
4	Локальный домен	Суффикс локального домена, который будет добавлен к DHCP-именам и записям из файлов hosts
5	Записывать запросы в журнал	Если установлена галочка, все DNS запросы будут записаны в системный журнал
6	Перенаправление запросов DNS	Список DNS-серверов для перенаправления запросов
7	Защита от DNS rebinding	Галочка включает защиту DNS от повторной привязки, отбрасывание ответов RFC1918
8	Разрешить локальный хост	Разрешить ответы в диапазоне 127.0.0.0/8, например, для RBL-сервисов
9	Белый список доменов	Список доменов, для которых разрешены ответы RFC1918
10	Только локальные службы	Ограничить службу DNS до интерфейсов подсети, в которой обслуживается DNS
11	Без шаблонов	Привязывать только к определенным интерфейсам, а не к шаблонам адресов

5.6. Имена хостов

В меню «**Сеть → Имена хостов**», для удобства администрирования сети, можно присвоить символьное имя конкретному IP-адрес. К примеру, можно выбрать IP-адрес из выпадающего списка и назвать этот хост «Printer1» (Рис. 5.12).

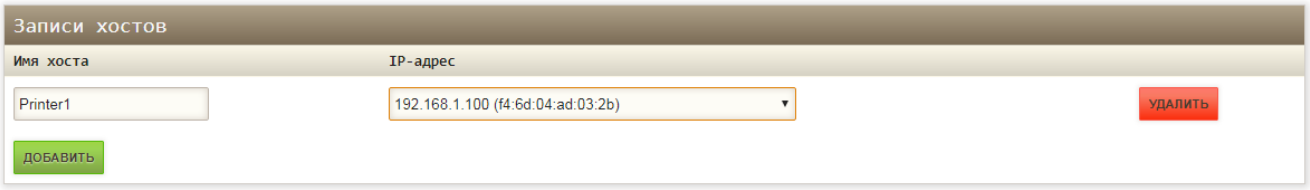

Рис.5.13. Имена хостов.

5.7. Статические маршруты

Добавить статический маршрут в таблицу маршрутизации. Маршрутизация служит для определения, через какой интерфейс и шлюз можно достичь нужного хоста или сети.

Меню содержит две таблицы для IPv4 и IPv6 маршрутов (Рис.5.14).

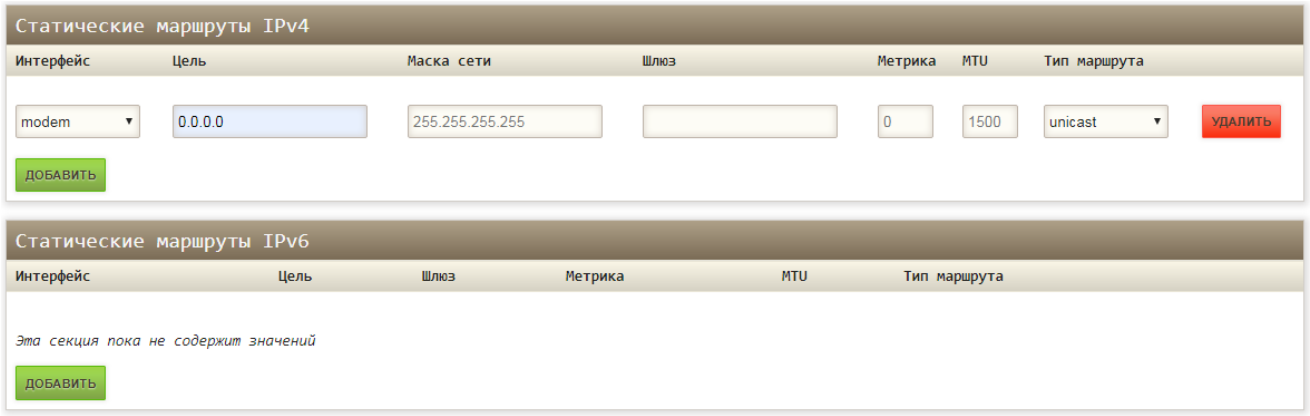

Рис.5.14. Статические маршруты.

Таблица 5.13. Сеть - Статические маршруты.

№	Параметр	Описание
1	Интерфейс	Выбор интерфейса, через который будет направляться трафик
2	Цель	Целевой IP-адрес или сеть, к которой пишется маршрут
3	Маска сети	Маска подсети адреса назначения
4	IPv4-адрес шлюза	Шлюз, через который будет идти маршрут до адреса
5	Метрика	Значение, влияющее на число переходов до определенного адреса по маршруту
6	MTU	Максимальный размер полезного блока данных одного пакета, который может быть передан протоколом без фрагментации.
7	Тип маршрута	Тип маршрута: локальный, широковещательный, однонаправленный, многонаправленный, пользовательский, недоступный, запрещенный, blackhole (перенаправление трафика на адрес для отброса)

5.8. Межсетевой экран

В меню «**Сеть → Межсетевой экран**» выполняется конфигурация межсетевого экрана, перенаправления портов, правила для трафика для интерфейсов LAN, WAN, VPN (Рис.5.15).

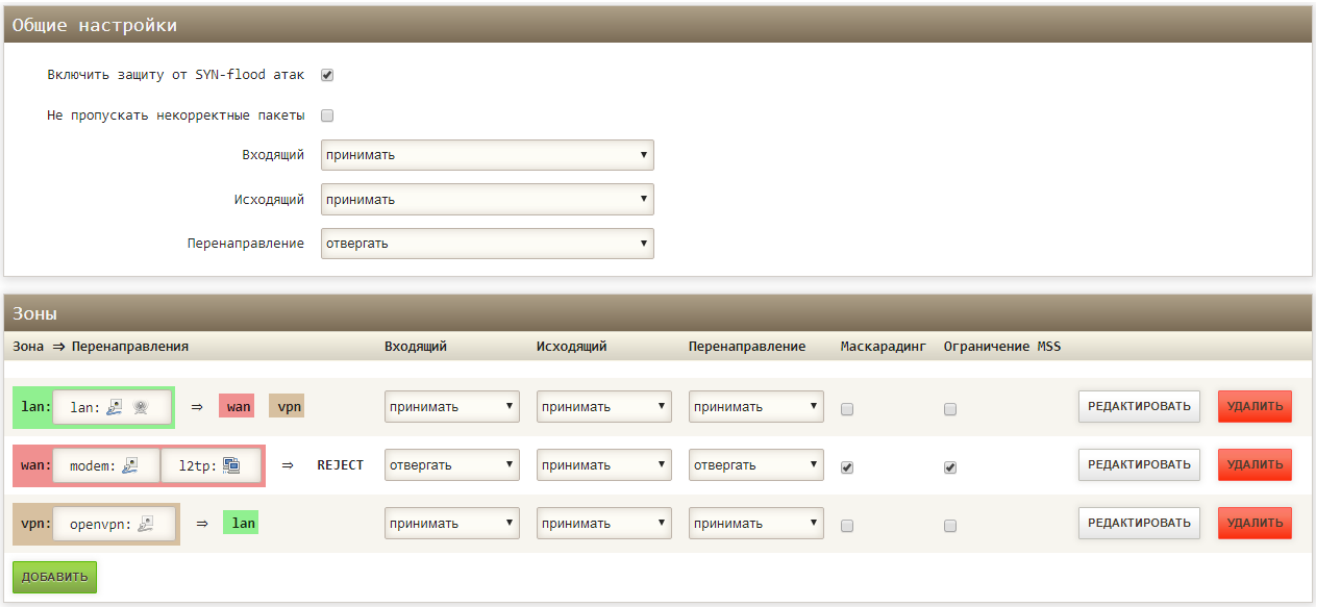

Рис.5.15. Межсетевой экран.

Общие настройки межсетевого экрана представлены в таблице 5.14.

Таблица 5.14. Межсетевой экран. Общие настройки, зоны.

№	Параметр	Описание
Общие настройки		
1	Включить защиту от SYN-flood атак	Галочка включает защиту от SYN-flood атак, заключающихся в отправке большого количества SYN-запросов злоумышленником
2	Не пропускать некорректные пакеты	Для дополнительной защиты установите галочку и firewall будет блокировать некорректные пакеты
3	Входящий	Принимать / отвергать /не обрабатывать входящий трафик
4	Исходящий	Принимать / отвергать /не обрабатывать исходящий трафик
5	Перенаправление	Принимать / отвергать /не обрабатывать перенаправление трафика
Зоны		
1	Зона - Перенаправление	Здесь можно добавить/удалить зоны. По умолчанию созданы 3 зоны: LAN – локальная сеть, WAN – интернет и VPN – виртуальная частная сеть
2	Маскарадинг	Включение маскарадинга – динамической подстановки сетевого адреса
3	Ограничение MSS	Включение ограничения максимального размера TCP сегмента (MSS) для предотвращения IP-фрагментации

Нажав на кнопку «Добавить», вы переходите в меню настройки новой зоны межсетевого экрана. Описание настроек зон в таблице 5.15.

Таблица 5.15. Межсетевой экран. Общие настройки, настройка зон.

№	Параметр	Описание
Общие настройки		
1	Имя	Имя новой зоны межсетевого экрана
2	Входящий	Принимать / отвергать /не обрабатывать входящий трафик
3	Исходящий	Принимать / отвергать /не обрабатывать исходящий трафик
4	Перенаправление	Принимать / отвергать /не обрабатывать перенаправление трафика
5	Маскарадинг	Включение маскарадинга – динамической подстановки сетевого адреса
6	Ограничение MSS	Включение ограничения максимального размера TCP сегмента (MSS) для предотвращения IP-фрагментации
7	Использовать сети	Можно объединить текущую зону с другими существующими зонами или с новой (галочка создать)
Расширенные настройки		
1	Использовать только семейство	Выбор какие протоколы использовать для текущей зоны (IPv4 и IPv6, либо

	протоколов	только один из них)
2	Использовать маскарадинг только для указанных подсетей-отправителей	Создать список подсетей - отправителей, для которых нужно использовать маскарадинг
3	Использовать маскарадинг только для указанных подсетей-отправителей	Создать список подсетей - получателей, для которых нужно использовать маскарадинг
4	Включить отслеживание соединений	Мониторинг соединения текущей зоны на ошибки и целостность пакетов. Отключено по умолчанию
5	Включить журналирование в этой зоне	Запись журнала событий, происходящих в текущей зоне

Перенаправление портов позволяет обращаться из Интернет к компьютеру во внутренней сети за маршрутизатором, использующим NAT (NAPT). Доступ осуществляется при помощи перенаправления трафика определенных портов с внешнего адреса маршрутизатора на адрес выбранного хоста в локальной сети. Описание настроек перенаправления портов представлено в таблице 5.16.

Таблица 5.16. Межсетевой экран. Перенаправление портов.

№	Параметр	Описание
1	Имя	Имя текущего перенаправления
2	Протокол	Протокол, по которому осуществляется подключение
3	Внешняя зона	Имя зоны, из которой будет осуществляться перенаправление
4	Внешний порт	Порт внешней зоны, который нужно перенаправить
5	Внутренняя зона	Имя зоны, в которую будет осуществляться перенаправление
6	Внутренний IP-адрес	IP-адрес хоста на который нужно выполнять перенаправление
7	Внутренний порт	Порт внутренней зоны, на который нужно перенаправить

Кнопкой «Добавить» можно создать несколько правил перенаправления портов. После создания нажмите «Сохранить и применить».

На вкладке «Правила для трафика» и «Пользовательские правила» можно установить дополнительные правила разрешения или запрета доступа к определенным портам, хостам или функциям.

5.9. Диагностика

В этом разделе меню осуществляется проверка интернет соединения, для этого используются команды:

- Эхо запрос
- Трассировка маршрута
- DNS-запрос

Например, для проверки доступности хоста в сети Интернет, можно отправить Эхо-запрос (5 ping-запросов) до адресата. Если хост доступен, то получим результат как на (Рис. 5.16).

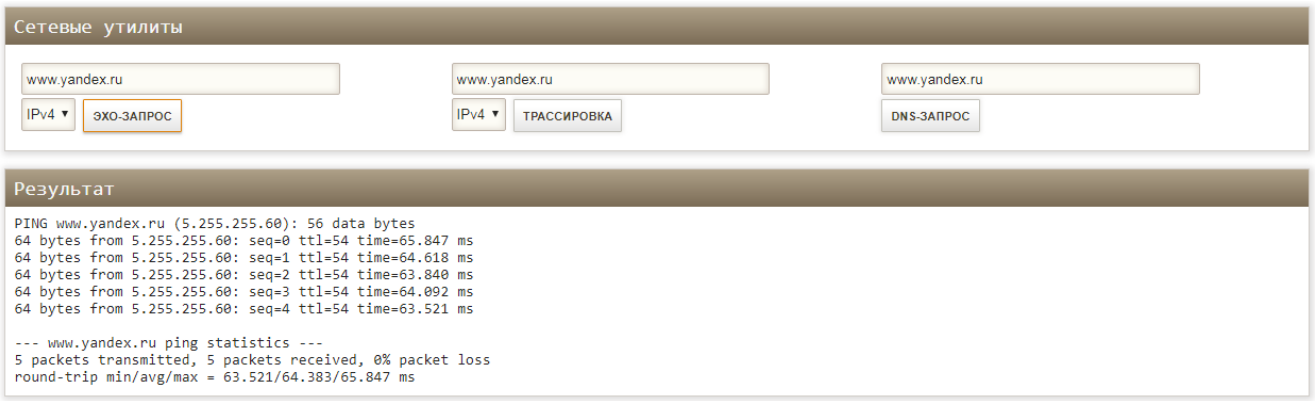

Рис.5.16. Диагностика. Эхо запрос.