

Руководство по WEB-интерфейсу

Содержание

| | |
|--|----|
| Подключение к WEB-интерфейсу и настройка сетевого адаптера | 3 |
| 1.1. Подключение к WEB-интерфейсу роутера | 3 |
| 1.2. Пример настройки сетевой карты для Windows 10..... | 3 |
| Меню – Статус | 6 |
| 2.1. Обзор | 6 |
| 2.2. Интерфейсы | 8 |
| 2.3. Межсетевой экран..... | 8 |
| 2.4. Маршруты | 9 |
| 2.5. Системный журнал | 10 |
| 2.6. Графики | 10 |
| Меню – Система | 11 |
| 3.1. Система..... | 11 |
| 3.2. Управление – Пароль | 11 |
| 3.3. Управление – SSH | 11 |
| 3.4. Управление – SMS..... | 12 |
| 3.5. Резервная копия/прошивка..... | 14 |
| 3.6. Перезагрузка | 14 |
| Меню – Сервисы | 15 |
| 4.1. AT/USSD/SMS/Поиск – AT-команды | 15 |
| 4.2. AT/USSD/SMS/Поиск – Отправить USSD | 15 |
| 4.3. AT/USSD/SMS/Поиск – Отправить SMS..... | 16 |
| 4.4. AT/USSD/SMS/Поиск – Читать SMS | 16 |
| 4.5. AT/USSD/SMS/Поиск – Поиск сетей..... | 16 |
| Меню – Сеть..... | 18 |
| 5.1. Wi-Fi | 18 |
| 5.2. MODEM..... | 21 |
| 5.3. LAN | 24 |
| 5.4. VPN – L2TP | 26 |
| 5.5. VPN – OPENVPN | 27 |
| 5.6. DHCP и DNS..... | 34 |
| 5.7. Имена хостов | 35 |
| 5.8. Статические маршруты | 35 |
| 5.9. Межсетевой экран..... | 36 |
| 5.10. Диагностика..... | 38 |

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 показано на Рис.1.1.

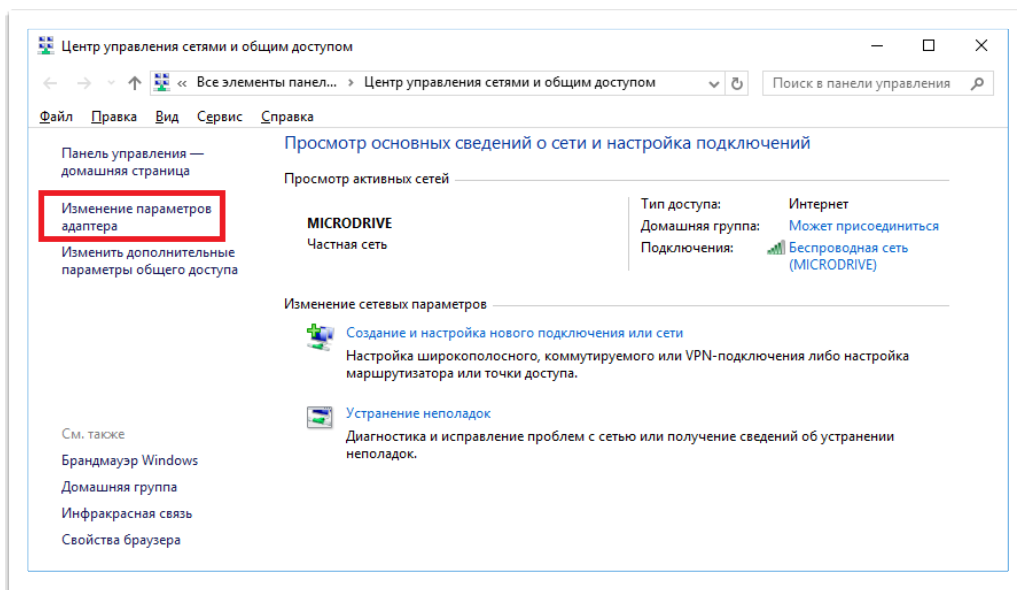


Рис.1.1. Центр управления сетями и общим доступом (Windows 10)

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

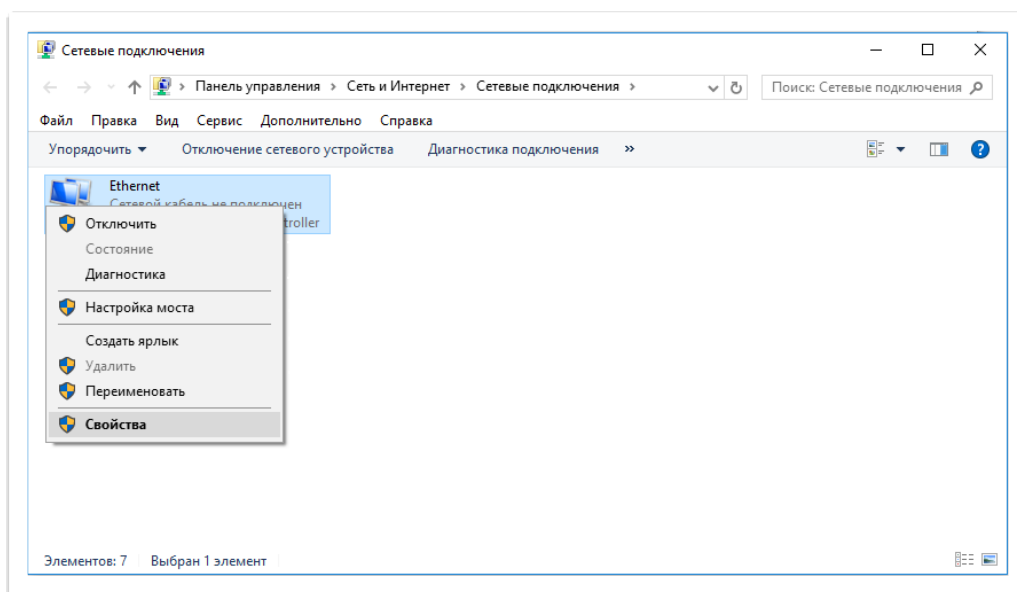


Рис.1.2. Изменения параметров сетевого адаптера

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

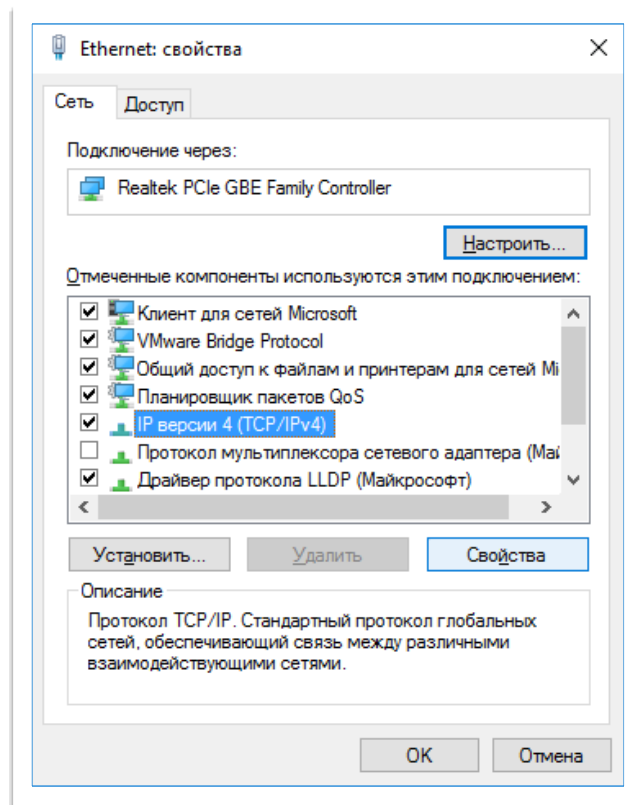


Рис.1.3. Свойства сетевого подключения

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

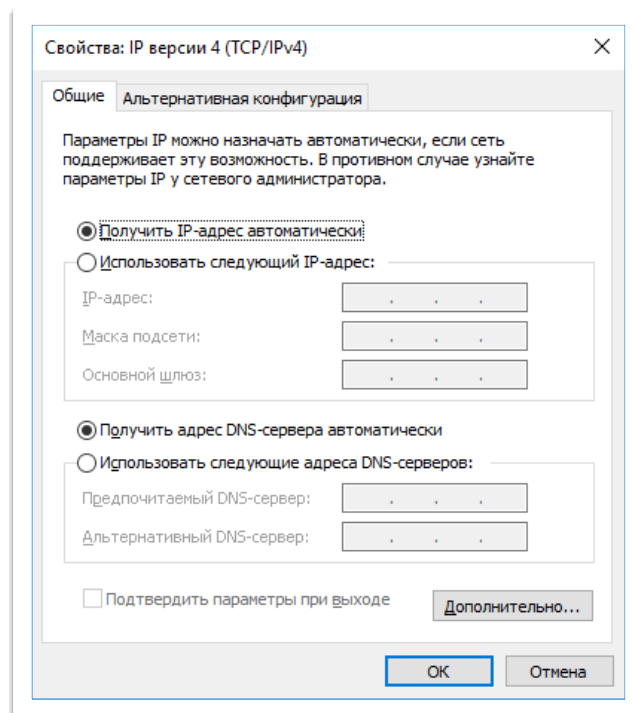


Рис.1.4. Настройка получения параметров IP автоматически

5. По адресу **192.168.1.1** в браузере откроется форма входа в WEB-интерфейс устройства. Если пароль не установлен, нажмите «Войти». Пример формы ввода пароля показан на Рис.1.5.

Пожалуйста, введите логин и пароль.

Логин

Пароль

Версия ПО: 17.2.7

Рис.1.5. Авторизация

Меню – Статус

2.1. Обзор

| Система | | | |
|--------------------|-----------------------|-----------------|-------------------|
| Имя хоста | MICRODRIVE | IMEI | 866758047227596 |
| Модель | Tandem-4GS-OEM | Ревизия | EC25EFAR06A06M4G |
| Дата/Время | 10:58:23 16/03/20 | MAC | 0C:8C:24:AC:5F:B5 |
| Время работы | 2d 23h 4m 33s | Версия прошивки | 17.6.11b |
| Средняя загрузка | 0.00, 0.00, 0.00 | Версия ядра | 4.4.61 |
| Мобильная сеть | | | |
| IMSI SIM-карты | SIM1: 250110103421372 | LAC/TAC | 170F |
| Регистрация в сети | REGISTERED, HOME | CID | 900C10D |
| Уровень сигнала | -31 дБм / 100% | RSCP | - |
| Технология доступа | FDD LTE | EC/IO | - |
| Оператор | YOTA / PLMN=25011 | RSRP | -57 дБм |
| Диапазон | LTE BAND 7 | RSRQ | -8 дБ |
| Канал | 2850 | SINR | 15 дБ |
| Статус соединения | Подключен | Полоса DL/UL | 20 МГц / 20 МГц |

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 | 250002211456923 | 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 | MTC / PLMN=25001 | Имя мобильного оператора и код оператора |
| 6 | Диапазон | LTE BAND 7 + 7 | Частотный диапазон или частотные диапазоны, если |

| | | | |
|-----------------------------------|-------------------------|---------------------------------|--|
| | | | используется режим агрегации |
| 7 | Канал | 3048 | Код радиочастотного канала |
| 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 (сектора) |
| 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) с учетом агрегации частотных диапазонов |
| 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

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




| Активные интерфейсы | | | |
|---|--|--|--|
| Интерфейс | Статус | Статистика | Действия |
|  br-lan | Подключен: 2h 29m 8s MAC: 1C:88:79:55:43:BF IPv4: 192.168.1.1/24 IPv6: fde8:e60e:8856::1/60 | RX: 1.98 MB (19123 пакет.) TX: 3.94 MB (18929 пакет.) | <input type="button" value="СОЕДИНИТЬ"/> <input type="button" value="ОСТАНОВИТЬ"/> |
|  wwan0 | Подключен: 0h 46m 17s MAC: 2E:35:3C:84:8E:A0 IPv4: 10.49.84.207/27 IPv6: | RX: 768.47 KB (5290 пакет.) TX: 1.69 MB (5229 пакет.) | <input type="button" value="СОЕДИНИТЬ"/> <input type="button" value="ОСТАНОВИТЬ"/> |
|  l2tp0 | Подключен: 0h 39m 43s MAC: 00:00:00:00:00:00 IPv4: 172.17.1.42/32 IPv6: | RX: 483.83 KB (3181 пакет.) TX: 1.06 MB (2995 пакет.) | <input type="button" value="СОЕДИНИТЬ"/> <input type="button" value="ОСТАНОВИТЬ"/> |

Рис.2.2. Статус - Интерфейсы

2.3. Межсетевой экран

В меню «Статус → Межсетевой экран» отображаются параметры межсетевого экрана. Здесь в виде таблицы представлены настройки фильтрации, перенаправления пакетов и др. Можно сбросить счетчики пакетов и трафика соответствующей кнопкой и перезапустить межсетевой экран. Раздел состоит из двух частей: «Межсетевой экран IPv4» и «Межсетевой экран IPv6». Настройка межсетевого экрана производится в меню «Сеть → Межсетевой экран».

| Таблица Filter | | | | | | | | |
|--|-----------|------------------|----------|--------|-----|-----------|------------|--|
| Цепочка INPUT (Политика: ACCEPT, Пакеты: 0, Трафик: 0.00 B) | | | | | | | | |
| Pkts | Трафик | Цель | Протокол | В | Вне | Источник | Назначение | Опции |
| 16 | 3.36 KB | ACCEPT | all | lo | * | 0.0.0.0/0 | 0.0.0.0/0 | /* !fw3 */ |
| 2938 | 338.75 KB | input_rule | all | * | * | 0.0.0.0/0 | 0.0.0.0/0 | /* !fw3: user chain for input */ |
| 1668 | 239.10 KB | ACCEPT | all | * | * | 0.0.0.0/0 | 0.0.0.0/0 | ctstate RELATED,ESTABLISHED /* !fw3 */ |
| 73 | 3.71 KB | syn_flood | tcp | * | * | 0.0.0.0/0 | 0.0.0.0/0 | tcp flags:0x17/0x02 /* !fw3 */ |
| 1267 | 99.41 KB | zone_lan_input | all | br-lan | * | 0.0.0.0/0 | 0.0.0.0/0 | /* !fw3 */ |
| 3 | 250.00 B | zone_wan_input | all | wwan0 | * | 0.0.0.0/0 | 0.0.0.0/0 | /* !fw3 */ |
| Цепочка FORWARD (Политика: DROP, Пакеты: 0, Трафик: 0.00 B) | | | | | | | | |
| Pkts | Трафик | Цель | Протокол | В | Вне | Источник | Назначение | Опции |
| 0 | 0.00 B | forwarding_rule | all | * | * | 0.0.0.0/0 | 0.0.0.0/0 | /* !fw3: user chain for forwarding */ |
| 0 | 0.00 B | ACCEPT | all | * | * | 0.0.0.0/0 | 0.0.0.0/0 | ctstate RELATED,ESTABLISHED /* !fw3 */ |
| 0 | 0.00 B | zone_lan_forward | all | br-lan | * | 0.0.0.0/0 | 0.0.0.0/0 | /* !fw3 */ |
| 0 | 0.00 B | zone_wan_forward | all | wwan0 | * | 0.0.0.0/0 | 0.0.0.0/0 | /* !fw3 */ |
| 0 | 0.00 B | reject | all | * | * | 0.0.0.0/0 | 0.0.0.0/0 | /* !fw3 */ |
| Цепочка OUTPUT (Политика: ACCEPT, Пакеты: 0, Трафик: 0.00 B) | | | | | | | | |

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

В меню «Статус → Маршруты» находится таблица маршрутизации.

| 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 меню «Статус → Системный журнал» находится системный журнал в который записываются все события, происходящие в маршрутизаторе. Например, в журнале можно отследить, какие настройки APN использует интерфейс при подключении к мобильному интернету. Пример системного журнала показан на Рис.2.5.

```

Mon Oct 26 10:04:51 2020 daemon.info cm[880]: SIM2, PS=detached, CS=detached, PLMN=25099, Radio=LTE, Reg=2
Mon Oct 26 10:04:57 2020 daemon.info cm[880]: SIM2, PS=attached, CS=attached, PLMN=25099, Radio=LTE, Reg=1
Mon Oct 26 10:04:58 2020 daemon.info cm[880]: activate PDN(ipv4): SIM2, apn="internet.beeline.ru"/"beeline"/"pap, WdsConnectionHandle=0x871d5510
Mon Oct 26 10:04:58 2020 daemon.notice netifd: Interface "modem" is now up
Mon Oct 26 10:04:58 2020 daemon.info dnsmasq[1316]: reading /tmp/resolv.conf.auto
Mon Oct 26 10:04:58 2020 daemon.info dnsmasq[1316]: using local addresses only for domain lan
Mon Oct 26 10:04:58 2020 daemon.info dnsmasq[1316]: using nameserver 10.10.30.118#53
Mon Oct 26 10:04:58 2020 daemon.info dnsmasq[1316]: using nameserver 10.10.30.122#53
Mon Oct 26 10:04:58 2020 daemon.info cm[880]: CONNECTED: ipv4=10.89.193.32/255.255.255.192, ipv6=/, mtu=1500

```

Рис.2.5. Запись событий в системный журнал

2.6. Графики

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

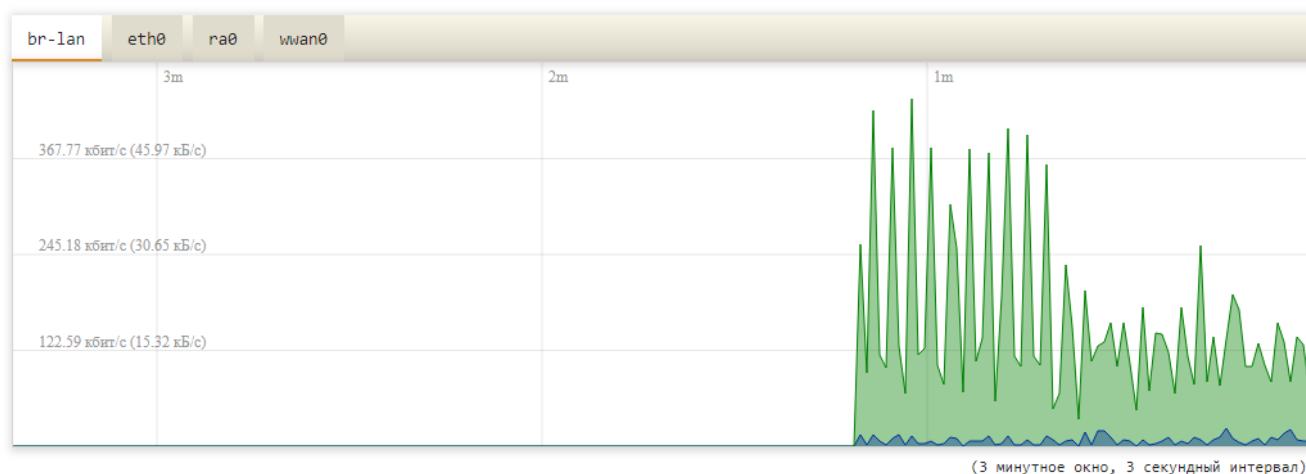


Рис.2.6. Графики в реальном времени. Вкладка «Трафик»

Таблица 2.6. Описание параметров построения графиков в реальном времени

| № | Название вкладки | Описание |
|---|------------------|---|
| 1 | Загрузка | Отображает уровень загрузки системы 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 |

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. Пример настроек показан на Рис.3.1.

Рис.3.1. Настройки системы

3.2. Управление – Пароль

В меню «Система → Управление → Пароль» можно задать (сменить) пароль доступа к маршрутизатору (смотри Рис. 3.2). Этот пароль также будет использоваться для доступа по SSH.

Рис.3.2. Установка пароля маршрутизатора

3.3. Управление – SSH

В меню «Система → Управление → SSH» расположены настройки SSH-сервера, который позволяет подключаться к роутеру через консоль и передавать файлы по протоколу SCP. Параметры SSH-сервера описаны в таблице 3.2. В разделе SSH-ключи можно дополнительно указать общий закрытый ключ. Если ключ не указан, то будет использоваться автоматически сгенерированный ключ, который будет обновляться при каждом сбросе питания. Пример настроек показан на Рис.3.3.

Рис.3.3. Настройки SSH

Таблица 3.2. Описание параметров SSH-сервера

| № | Название параметра | Описание |
|---|---------------------------------|---|
| 1 | Включить | Включить/Отключить SSH-сервер |
| 2 | Интерфейс | Выбор интерфейса, по которому будет доступен сервер SSH, при выборе параметра «любой» сервер будет доступен на всех интерфейсах |
| 3 | Порт | TCP Порт |
| 4 | Аутентификация с помощью пароля | Разрешить SSH-аутентификацию с помощью пароля |

3.4. Управление – SMS

В меню «Система → Управление → SMS» настраивается управление роутером через SMS сообщения. Принцип управления 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, со стороны роутера должны быть выполнены следующие условия:

- Встроенный сотовый модем роутера должен быть зарегистрирован в голосовой сети оператора. Некоторые операторы могут использовать сеть 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.

Пример настроек показан на Рис 3.3. Параметры SMS управления описаны в таблице 3.3

Рис.3.4. Настройки SMS управления

Таблица 3.3. Описание параметров функции SMS управления

| № | Название параметра | Описание |
|---|---------------------------|---|
| 1 | Включить | Включить/Отключить управление через SMS |
| 2 | Список телефонных номеров | Список доверенных телефонных номеров в международном формате «+7xxxxxxxxxx» |

3.5.1 SMS команды

Общий формат команд:

<имя команды> [<аргументы>]

Имя команды и аргументы не должны содержать заглавных букв. Команды и аргументы разделяются пробелами. Список доступных команд приведен в таблице 3.4.

Таблица 3.4. Описание команд

| Запрос (команда) | Пример ответа | Описание |
|---|--|---|
| info | Host ="MICRODRIVE" Model ="Tandem-4GL-OEM" 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. |
| 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 сигнала/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 соты |
| modem info | TYPE =EC25 Revision =EC25EUGAAR06A03M4 IMEI =865544003366702 SIM =1/1 IMSI =250207792022203 "ROSTELECOM" | Запросить информацию об LTE модеме (модуле). TYPE – Тип LTE модуля; Revision – Версия ПО LTE модуля; IMEI – Международный уникальный идентификатор LTE модуля; SIM – Текущая SIM карта/Количество SIM карт; IMSI – Международный идентификатор мобильного абонента и имя провайдера. |
| 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 |
| 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 строка – 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. |

| | | |
|---|--------------------------------------|--|
| <code>iface <name> up</code> | <code>iface modem up</code> OK | Запустить/Перезапустить интерфейс. <name> – имя интерфейса |
| <code>iface <name> down</code> | <code>iface l2tp down</code> OK | Остановить интерфейс. <name> – имя интерфейса |
| <code>iface <name> enable</code> | <code>iface l2tp enable</code> OK | Включить автозапуск интерфейса после сброса питания. <name> – имя интерфейса |
| <code>iface <name> disable</code> | <code>iface lan disable</code> OK | Отключить автозапуск интерфейса после сброса питания. <name> – имя интерфейса |
| <code>wifi on</code> | <code>wifi on</code> OK | Включить WiFi сеть |
| <code>wifi off</code> | <code>wifi off</code> OK | Отключить WiFi сеть |
| <code>reboot</code> | <code>reboot</code> OK | Перезагрузить роутер |

3.5. 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.

The screenshot shows two sections of the router's web interface:

- Резервное копирование / Восстановление**:
 - Загрузить резервную копию:
 - Сбросить на значения по умолчанию:
 - Восстановить резервную копию:
- Установить новый образ прошивки**:
 - Образ:

Рис.3.4. Резервная копия/прошивка

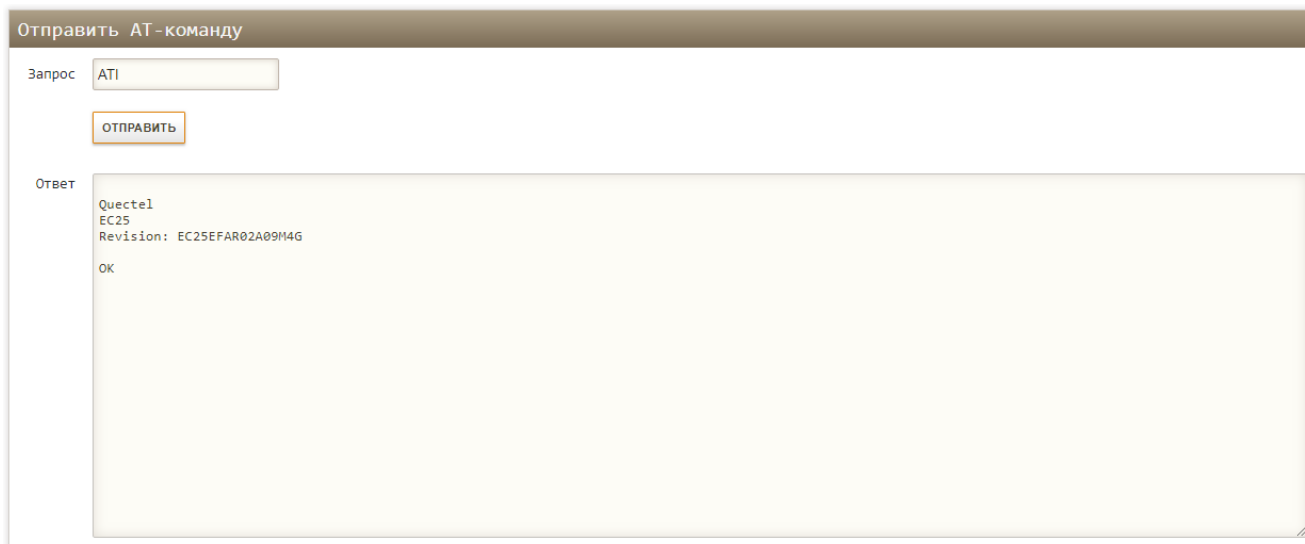
3.6. Перезагрузка

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

Меню – Сервисы

4.1. АТ/USSD/SMS/Поиск – АТ-команды

В меню «Сервисы → АТ/USSD/SMS/Поиск → АТ-команды» можно отправлять АТ-команды LTE-модулю. Пример отправки АТ-команды модулю показан на Рис.4.1.



Отправить АТ-команду

Запрос:

Ответ:

```
Quectel
EC25
Revision: EC25EFAR02A09M4G
OK
```

Рис.4.1. Отправка АТ-команд

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

Использовать с осторожностью!

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

В меню «Сервисы → АТ/USSD/SMS/Поиск → Отправить USSD» можно отправлять USSD-запросы сотовому оператору, например 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.



Отправить USSD сообщение

Запрос:

Ответ:

```
Ваша заявка принята. Ожидайте ответа по SMS.
```

Рис.4.2. Отправка USSD-запросов

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

В меню «Сервисы → AT/USSD/SMS/Поиск → Отправить SMS» На этой вкладке можно отправлять SMS сообщения на международные и местные мобильные номера. Пример отправки SMS сообщения приведен на Рис.4.3.

Для отправки сообщений требуется, что бы устройство было зарегистрировано в голосовой сети, а на лицевом счете должен положительный баланс.

Рис.4.3. Отправка SMS

4.4. AT/USSD/SMS/Поиск – Читать SMS

В меню «Сервисы → AT/USSD/SMS/Поиск → Читать SMS» выводится список входящих SMS сообщений, полученные LTE-модулем. Пример на Рис.4.4.

| Дата/Время | Отправитель | Текст сообщения |
|-----------------------------------|-------------|-----------------|
| 10:22:40 01.11.18 GMT+03:00 | Rostelecom | правки MMS. |

Рис.4.4. Входящие SMS сообщения

Входящие сообщения сохраняются во внутренней памяти LTE-модуля. Во избежание переполнения памяти, более «старые» сообщения автоматически удаляются. Кнопка «Обновить» предназначена для обновления списка сообщений. Кнопкой «Удалить все» можно удалить все SMS сообщения из внутренней памяти LTE-модуля. 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

В меню «Сервисы → AT/USSD/SMS/Поиск → Поиск сетей» можно выполнить поиск доступных мобильных сетей (операторов) Пример результата поиска на Рис.4.5.

| Имя | PLMN | Технологии доступа | Статус | Выбрать и сохранить для: |
|---------|-------|--------------------|-----------------------|--------------------------|
| MTS RUS | 25001 | 2G,3G,LTE | Roaming | SIM1 SIM2 |
| YOTA | 25011 | LTE | Home, Current network | SIM1 SIM2 |
| Tele2 | 25020 | 2G,3G,LTE | Roaming | SIM1 SIM2 |
| Beeline | 25099 | 2G,3G,LTE | Roaming | SIM1 SIM2 |

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.

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 (смотри Рис. 5.1.), ниже находится список подключенных клиентов по Wi-Fi. Изменить параметры сети, включить или отключить Wi-Fi можно, нажав на кнопку «Редактировать».

Беспроводная сеть

Диапазон: 2.4G | Канал: 10 | Скорость: 72.0 Мбит/с

| Сеть | Статистика | Действие |
|---|--|---------------|
| rа0 SSID: Tandem-43BF BSSID: 1c:88:79:55:43:be Защита: WPA2PSK | RX: 0 B (0 пакет.) TX: 0 B (0 пакет.) | РЕДАКТИРОВАТЬ |

Подключенные клиенты

| RSSI | MAC-адрес | Хост | IP-адрес | Сеть | Статистика |
|---------------------------|-----------|------|----------|------|------------|
| Нет подключенных клиентов | | | | | |

Рис.5.1. Обзор Wi-Fi

Нажав на кнопку «Редактировать», вы перейдете в меню настроек параметров беспроводной сети. Пример настроек показан на Рис. 5.2.

Конфигурация устройства

Основные настройки | Расширенные настройки

Режим: 802.11bgn

Канал: CH10

Ширина канала: 20МГц

Режим WMM:

Изолированные клиенты:

Блокировать трафик между клиентами

Конфигурация интерфейса

Основные настройки | MAC фильтр

Включить сеть:

Имя беспроводной сети (SSID): Tandem-4GS-OEM

Скрыть SSID:

Защита: WPA2-PSK

Шифрование: AES

Ключ: ●●●●●●

Период обновления ключа: 0

Период обновления группового ключа (секунды). Диапазон 1-3600. Значение 0 - обновление отключено

Рис.5.2. Конфигурация Wi-Fi

Таблица 5.1. Конфигурация Wi-Fi

| № | Параметр | Описание |
|---|---------------------------------|---|
| Конфигурация устройства. Основные настройки | | |
| 1 | Режим | <ul style="list-style-type: none"> 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 | Разрешить/Блокировать трафик между клиентами Wi-Fi сети |
| Конфигурация устройства. Расширенные настройки | | |
| 1 | Доступные каналы | Список доступных для выбора частотных каналов |
| 2 | Мощность передатчика | Настройка мощности передатчика Wi-Fi |
| 3 | Выбор 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 802.11N | Поддержка стандарта IEEE 802.11N, используемого для динамического снижения излучаемой мощности Wi-Fi |
| 12 | Режим совместимости | <ul style="list-style-type: none"> 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 | Аутентификация | <ul style="list-style-type: none"> • 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 | <ul style="list-style-type: none"> • TKIP – поадресное 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 | <ul style="list-style-type: none"> • 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

Раздел в меню «Сеть → MODEM» предназначен для настройки интерфейса мобильной сети. 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 | Задаёт 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 «wap» | |

Таблица 5.3. SIM профиль

| № | Параметр | Описание | Модели |
|------------------|---------------------------|--|--------------|
| 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 | |
| 6 | 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 | |
| 7 | Технология доступа | Выбор технологии доступа: <ul style="list-style-type: none"> • Авто – модем будет пытаться последовательно регистрироваться 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; • Предпочтительно LTE – до установления соединения с интернетом, модему запрещается регистрация в сети LTE (только 2G/3G). После установления соединения, модему разрешается регистрация во всех сетях (режим Авто). При наличии сети LTE, модем будет зарегистрирован в этой сети. | |
| 8 | Диапазон | Выбор частотного диапазона | |
| 9 | AT-команда | Дополнительная AT-команда, которая будет автоматически выполняться сразу после применения основных настроек. Результат выполнения команды можно проконтролировать в «Системном журнале» | |
| 10 | 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 | |
| 11 | Пинг | Интервал (сек.) отправки тестовых пакетов на Хост1, Хост2. Тестовые пакеты отправляются по очереди на Хост1 и Хост2, с половинным интервалом | |
| 12 | 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» | |
| 13 | 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

В меню «Сеть → LAN» находится раздел предназначенный для настройки интерфейса сетевого моста – LAN. 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 | Задаёт 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». 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. Пример настройки DHCP приведен на Рис.5.5.

DHCP-сервер

Основные настройки | Расширенные настройки | IPv6 Настройки

Включить DHCP

Старт
Минимальный адрес аренды

Предел
Максимальное количество арендованных адресов

Время аренды
Время, через которое истекает аренда адреса, минимум 2 минуты (2m)

Рис.5.5. Настройки 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 | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> 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 – L2TP

В меню «Сеть → VPN → L2TP» находится раздел предназначенный для настройки интерфейса L2TP. Пример настроек показан на Рис.5.6. Описание параметров в таблице 5.6.

Рис.5.6. Настройки интерфейса VPN L2TP

Таблица 5.6. Параметры VPN L2TP

| № | Параметр | Описание |
|-------------------------------------|--|---|
| Основные настройки | | |
| 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 | Задаёт 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 |

5.5. VPN – OPENVPN

В меню «Сеть → VPN → OPENVPN» находится раздел предназначенный для настройки интерфейса OPENVPN. Описание параметров приводится в таблице 5.7.

В ОС роутера установлен клиент OpenVPN 2.4.0. Клиент 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 OpenVPN |
|-------------------------------------|--|--|---------------------------|
| 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 | <i>dev</i> |
| 4 | Мост | Добавить в мост LAN | |
| 5 | Транспортный протокол | Выбор транспортного протокола | <i>proto</i> |
| 6 | Удаленный хост/IP | Доменное имя или IP-адрес удаленного узла (сервера), к которому будет подключаться клиент | <i>remote</i> |
| 7 | Порт | Порт удаленного узла (сервера) | <i>port</i> |
| 8 | Сжатие | Выбор сжатия LZO. Значение «По умолчанию» – опция игнорируется, «Отключено» – сжатие отключено. «LZO» – алгоритм сжатия LZO, «LZ4» – алгоритм сжатия LZ4 | <i>compress</i> |
| 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 | <i>ping</i> |
| 10 | Пинг таймаут | Интервал, в секундах, по истечении которого происходит повторное подключение, при отсутствии тестовых пакетов от удаленного узла (сервера) | <i>ping-restart</i> |
| 11 | Аутентификация | Выбор метода аутентификации, определяет топологию сети. Shared secret – подключение типа «Точка-Точка» аутентификация с общим ключом. TLS Client – подключение типа «Сеть», аутентификация с помощью сертификатов и/или пароля | <i>secret, tls-client</i> |
| 12 | Шифрование | Выбор алгоритма шифрования канала передачи данных. Значение «По умолчанию» – BF-CBC | <i>cipher</i> |
| 13 | Алгоритм аутентификации | Выбор алгоритма аутентификации. Значение «По умолчанию» – SHA1 | <i>auth</i> |
| 14 | Локальный VPN IP | IP-адрес локального интерфейса TUN/TAP | <i>ifconfig_l</i> |
| 15 | Удаленный VPN IP | IP-адрес удаленного интерфейса TUN/TAP | <i>ifconfig_r</i> |
| 16 | Маска сети VPN | Маска сетевого интерфейса TAP | <i>ifconfig</i> |
| 17 | Шлюз VPN IP | IP-адрес шлюза в сети VPN, через который могут быть добавлены маршруты | <i>route-gateway</i> |
| 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 заголовок: -----BEGIN CERTIFICATE----- и заканчиваться: -----END CERTIFICATE----- | ca |
| 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/Выбрать дополнительный уровень аутентификации или шифрования канала управления TLS. Возможные значения: «Аутентификация» – аутентификация без шифрования «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, то на клиенте должно быть задано 0 и на оборот | tls-auth, tls-crypt key- direction |
| 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, tls-crypt |

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

В конфигурации туннеля TAP (L2) с аутентификацией по общему ключу одно из устройств (Сервер) должно выступать в роли сервера и иметь статический белый IP-адрес, второе устройство (Клиент) может иметь динамический IP-адрес и работать за NAT. Текущая версия программного обеспечения поддерживает только режим клиента. Пример топологии показан на Рис.5.7. Пример настройки для клиента (роутера) приведен в таблице 5.8.

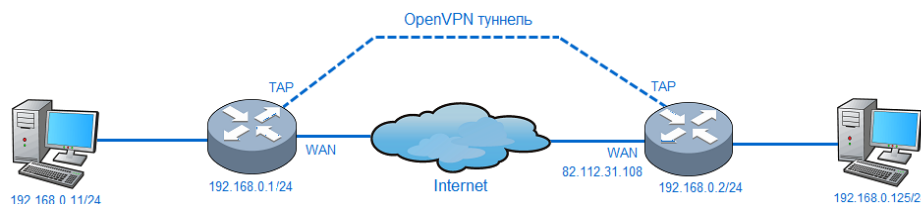


Рис.5.7. Пример топологии «Точка-Точка» (192.168.0.1 – Клиент, 192.168.0.2 – Сервер), уровень L2.

Таблица 5.8. Пример настройки для топологии «Точка-Точка», уровень L2

| 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 сервера OpenVPN |
| 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 межсетевых экранов | |
| Зона | lan |
| Аутентификация | |
| Общий ключ | Скопируйте содержимое файла с общим ключом |

- 192.168.0.11/24 – Хост или сеть за клиентом (роутером);
- 192.168.0.1/24 – Интерфейс сетевого моста LAN клиента (роутера), в который должен быть добавлен TAP OpenVPN интерфейс;
- 192.168.0.125/24 – Хост или сеть за сервером;
- 192.168.0.2/24 – Интерфейс сетевого моста, в который должен быть добавлен TAP OpenVPN интерфейс сервера;
- 82.112.31.108 – WAN интерфейс сервера.

5.6.2 Настройка туннеля L2 с аутентификацией TLS

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

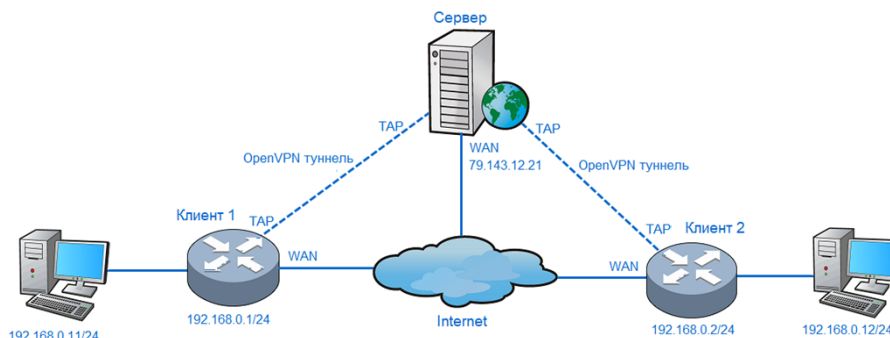


Рис.5.8. Пример топологии «Сеть», уровень L2

Таблица 5.9. Пример настройки для топологии «Сеть», уровень L2

| 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 межсетевое экрана | |
| Зона | lan или vpn |
| 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 OpenVPN 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 OpenVPN интерфейс;
- 79.143.12.21 – WAN интерфейс сервера.

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

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

В конфигурации туннеля TUN (L3) с аутентификацией по общему ключу одно из устройств (Сервер) должно выступать в роли сервера и иметь статический белый IP-адрес, второе устройство (Клиент) может иметь динамический IP-адрес и работать за NAT. Текущая версия программного обеспечения поддерживает только режим клиента. Пример топологии показан на Рис.5.9. Пример настройки для клиента (роутера) приведен в таблице 5.10.

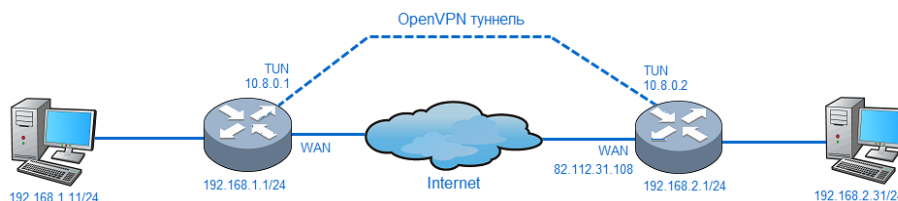


Рис.5.9. Пример топологии «Точка-Точка» (192.168.1.1 – Клиент, 192.168.2.1 – Сервер), уровень L3

Таблица 5.10. Пример настройки для топологии «Точка-Точка», уровень L3

| 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 или vpn |
| Аутентификация | |
| Общий ключ | Скопируйте содержимое файла с общим ключом |

- 192.168.1.11/24 – Хост или сеть за Клиентом (роутером);
- 192.168.1.1/24 – Интерфейс LAN Клиента (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 OpenVPN Клиента (роутера);
- 10.8.0.2 – Интерфейс TUN OpenVPN удаленного узла, выполняющего роль сервера;
- 82.112.31.108 – WAN интерфейс.

5.6.4 Настройка туннеля L3 с аутентификацией TLS

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

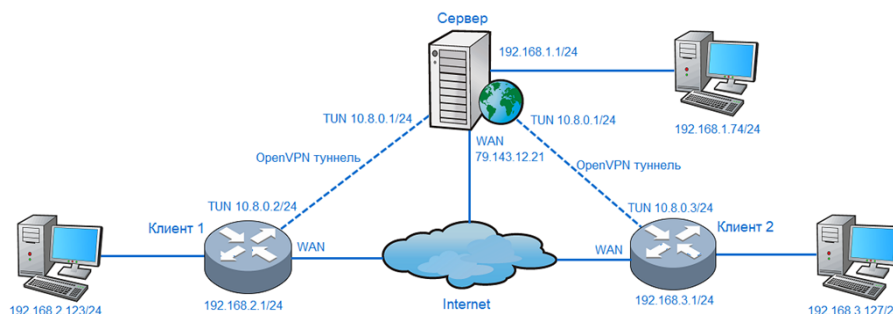


Рис.5.10. Пример топологии «Сеть», уровень L3

Таблица 5.11. Пример настройки для топологии «Сеть»

| 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 или vpn |
| 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 OpenVPN Сервера;
- 10.8.0.2/24 – Интерфейс TUN OpenVPN Клиента 1;
- 10.8.0.3/24 – Интерфейс TUN OpenVPN 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.

5.6.5 VPN шлюз

Конфигурация VPN-шлюз используется для перенаправления интернет трафика через интерфейс OPENVPN. Топология сети может быть «Точка-Точка» или «Сеть» (смотри Рис.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 (Сервера):

| | |
|--------------|-------------------------------------|
| 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 | OPENVPN |
| 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.

5.6.6 Диагностика

Отслеживать статус интерфейса OPENVPN 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».

5.6. DHCP и DNS

В меню «Сеть → DHCP и DNS» находится раздел предназначенный для настройки интерфейса DHCP/DNS сервера. Пример настроек показан на Рис.5.11 и Рис.5.12. Описание параметров приводится 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 |

5.7. Имена хостов

В меню «Сеть → Имена хостов», для удобства администрирования сети, можно присвоить символическое имя конкретному IP-адресу. Например, можно выбрать IP-адрес из выпадающего списка и назвать этот хост «Printer1» (смотри Рис. 5.13).

Рис.5.13. Имена хостов

5.8. Статические маршруты

Раздел в меню «Сеть → Статические маршруты», предназначен для добавления статических маршрутов 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. Пример настройки показан на Рис.5.14. Описание параметров приводится в таблице 5.13.

Рис.5.14. Статические маршруты

Таблица 5.13. Параметры таблицы «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 | Приоритет маршрута в таблице маршрутизации, 0 – максимальный приоритет |
| 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) |

5.9. Межсетевой экран

В меню «Сеть → Межсетевой экран» выполняется конфигурация межсетевого экрана, перенаправления портов, правила для трафика для интерфейсов LAN, WAN, VPN. Пример настройки показан на Рис.5.15. Общие настройки межсетевого экрана представлены в таблице 5.14.

The screenshot shows the 'Общие настройки' (General Settings) section with the following options:

- Включить защиту от SYN-flood атак:
- Не пропускать некорректные пакеты:
- Входящий:
- Исходящий:
- Перенаправление:

The 'Зоны' (Zones) section shows a table of rules:

| Зона | ⇒ | Входящий | Исходящий | Перенаправление | Маскарадинг | Ограничение MSS | Действия |
|----------------------|---|----------|--------------|-----------------|-------------------------------------|-------------------------------------|-----------------------|
| lan: lan: [icon] | ⇒ | wan | vpn | принимать | <input type="checkbox"/> | <input type="checkbox"/> | РЕДАКТИРОВАТЬ УДАЛИТЬ |
| wan: modem: [icon] | ⇒ | REJECT | 12tp: [icon] | отвергать | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | РЕДАКТИРОВАТЬ УДАЛИТЬ |
| vpn: openvpn: [icon] | ⇒ | lan | | принимать | <input type="checkbox"/> | <input type="checkbox"/> | РЕДАКТИРОВАТЬ УДАЛИТЬ |

There is a 'ДОБАВИТЬ' (ADD) button at the bottom left of the zones section.

Рис.5.15. Межсетевой экран

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 |

Для создания новой зоны, используйте кнопку «Добавить». После нажатия будет открыта форма 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 протоколов | Выбор какие протоколы использовать для текущей зоны (IPv4 и IPv6, либо только один из них) |
| 2 | Использовать маскардинг только для указанных подсетей-отправителей | Создать список подсетей - отправителей, для которых нужно использовать маскардинг |
| 3 | Использовать маскардинг только для указанных подсетей-отправителей | Создать список подсетей - получателей, для которых нужно использовать маскардинг |
| 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 IP-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.

5.10. Диагностика

В меню «Сеть → Диагностика» находятся диагностические утилиты:

- Эхо запрос
- Трассировка маршрута
- DNS-запрос

Например, с помощью утилиты «Эхо-запрос» можно проверить доступность удаленного узла или интернет соединения, для этого введите в соответствующее поле IP-адрес или доменное имя удаленного узла и нажмите кнопку «Эхо-запрос». Роутер пошлет 5 ping-запросов до адресата и если он доступен, то адресат вышлет ответ на этот запрос (смотри Рис.5.16).

The screenshot shows a web interface for network utilities. The top section is titled "Сетевые утилиты" (Network Utilities) and contains three input fields, each with "www.yandex.ru" entered. Below each field are buttons for "IPv4" (with a dropdown arrow), "ЭХО-ЗАПРОС" (Echo Request), "ТРАССИРОВКА" (Traceroute), and "DNS-ЗАПРОС" (DNS Query). The "ЭХО-ЗАПРОС" button is highlighted. The bottom section is titled "Результат" (Result) and displays the output of a ping command:

```
PING www.yandex.ru (5.255.255.60): 56 data bytes
64 bytes from 5.255.255.60: seq=0 ttl=54 time=65.847 ms
64 bytes from 5.255.255.60: seq=1 ttl=54 time=64.618 ms
64 bytes from 5.255.255.60: seq=2 ttl=54 time=63.840 ms
64 bytes from 5.255.255.60: seq=3 ttl=54 time=64.092 ms
64 bytes from 5.255.255.60: seq=4 ttl=54 time=63.521 ms

--- www.yandex.ru ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 63.521/64.383/65.847 ms
```

Рис.5.16. Диагностика. Эхо запрос