netshe_doc_chap3

Original file



NETSHe Lab

Универсальное программное обеспечение **NETSHe** **для сетевых устройств.** Часть 3. Меню веб-интерфейса.	
NETSHe Lab длительное время занимается разработками программного обеспечения для сетевых устройств, провайдеров услуг и операторов связи. Среди программного обеспечения центральное место занимает операционная система NETSHe, которая может быть использована в широком спектре сетевых устройств и сервисов.	
Версия 2 Апрель, 2020	Станислав Корсаков, ООО «Нетше лаб» (c) 2009-2020 Ярославль

Оглавление

Веб-интерфейс (WebUI) операционной системы NETSHe является полнофункциональным и унифицированным инструментом для настройки всех моделей устройств. В данном руководстве последовательно описываются разделы главного меню интерфейса, состав которых может изменяться в зависимости от модели устройства или назначения системы. По ходу повествования так же упоминается, как дополняется панель инструментов в зависимости от текущей страницы веб-интерфейса.

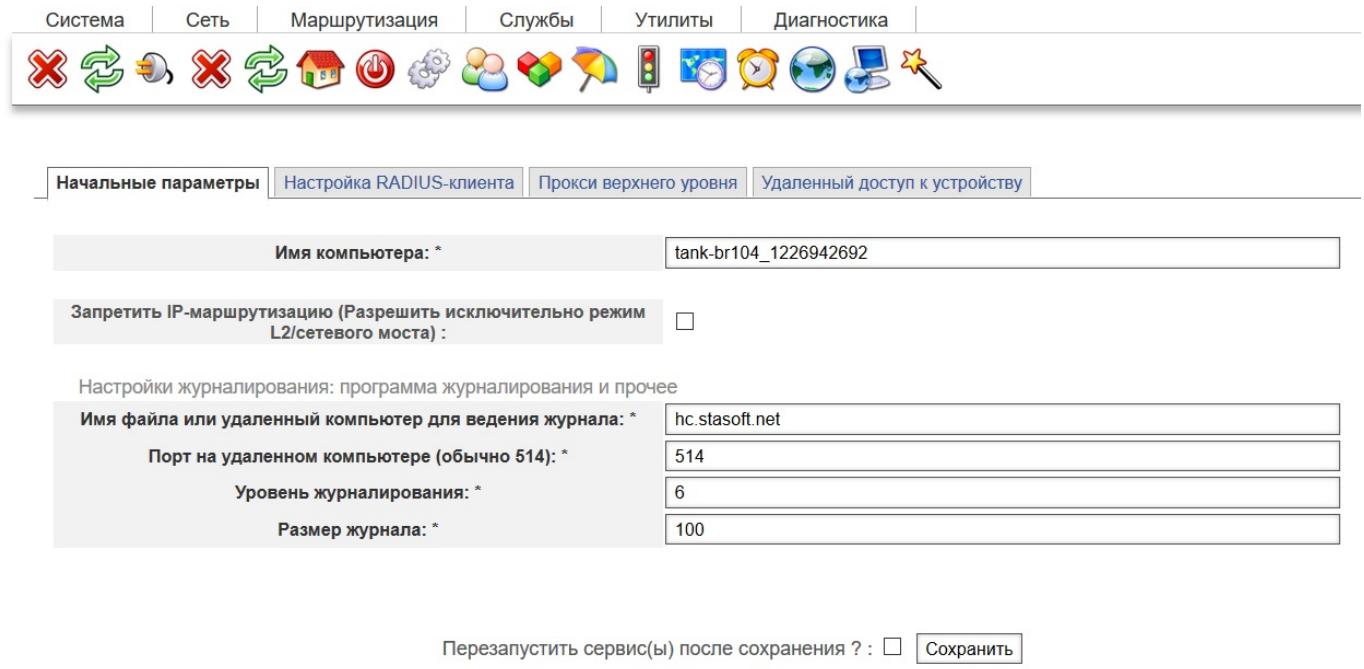
В предыдущей главе был описан процесс стартовой настройки системы с помощью мастера настройки, а так же способы подключения к управлению устройствами: WebUI, SSH, Telnet. Напомним, что WebUI можно открыть в браузере, введя в строке URL https://192.168.1.1:5556 (по умолчанию) и предоставив учетные данные root/root или superuser/abC123dEf_ .

Меню «Система»

Базовые установки системы

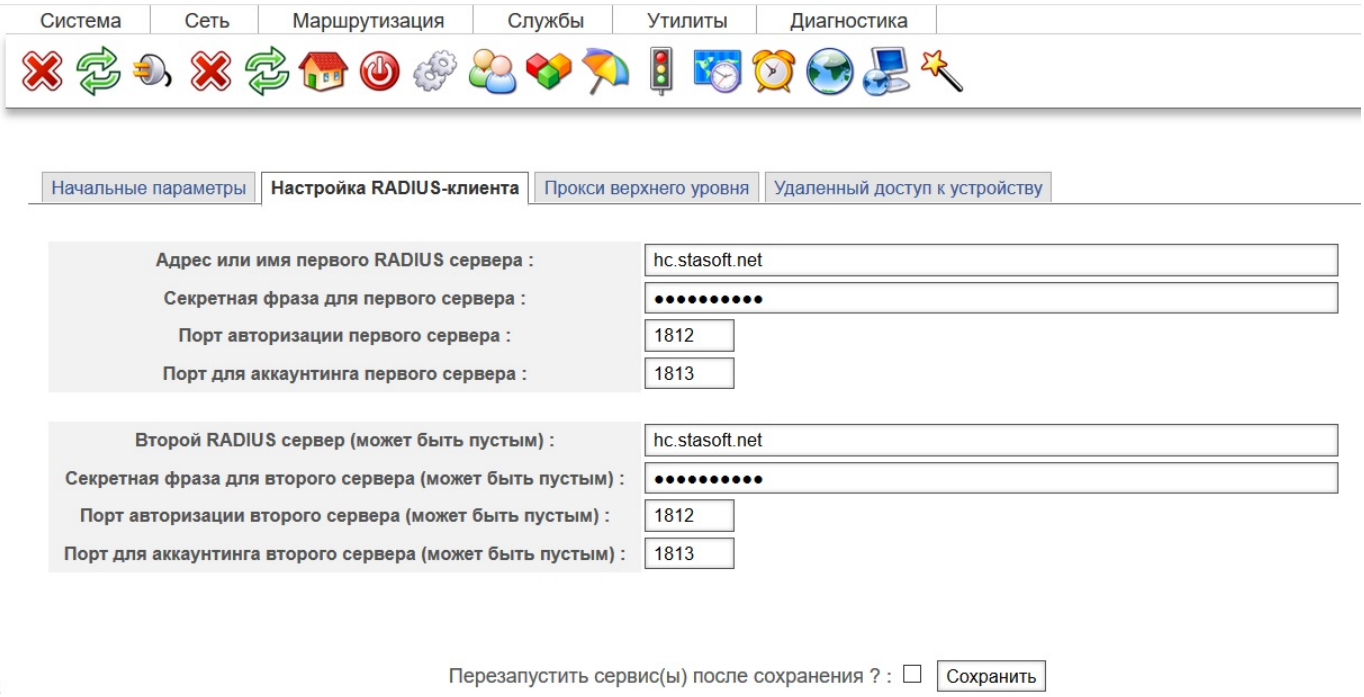
Закладка «Начальные параметры»

содержит поля для ввода имени устройства, имени файла или имени (адреса) удаленного компьютера для ведения системного журнала syslog, порт (в случае удаленного компьютера), уровень журналирования и размер журнала, при превышении которого новые записи в журнале будут затирать старые (циклическая запись).



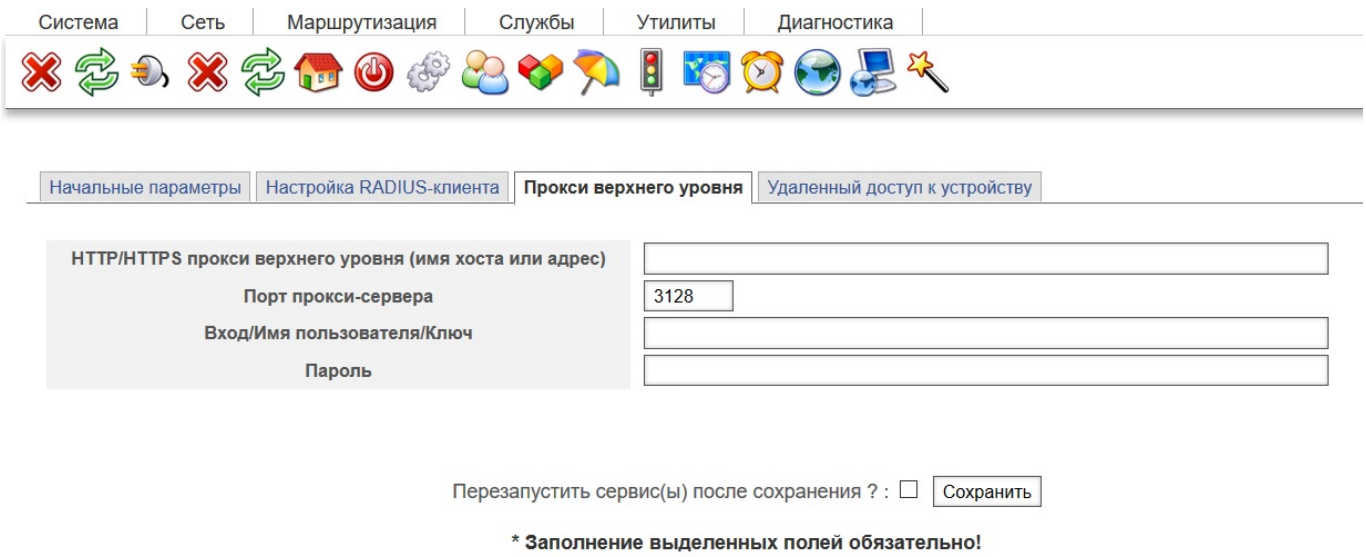
Закладка «Настройка RADIUS-клиента»

позволяет указать до двух RADIUS-серверов (первичный и резервный), которые могут быть использованы системой для авторизации и аккаунтинга клиентов, например, при PPTP/PPPoE/L2TP соединениях или работе хотспот контроллера. Серверы определяются адресом/именем компьютера, секретной фразой, портами авторизации и аккаунтинга.



Закладка «Прокси верхнего уровня»

позволяет указать HTTP прокси-сервер, на который будут перенаправляться все HTTP-запросы со встроенного прокси-сервера. Также данный сервер будет использован как прокси для работы менеджера пакетов и клиента динамической службы разрешения имен. Для использования следует ввести адрес/имя прокси-сервера, порт, на котором он принимает запросы, имя и пароль для авторизации (при необходимости).

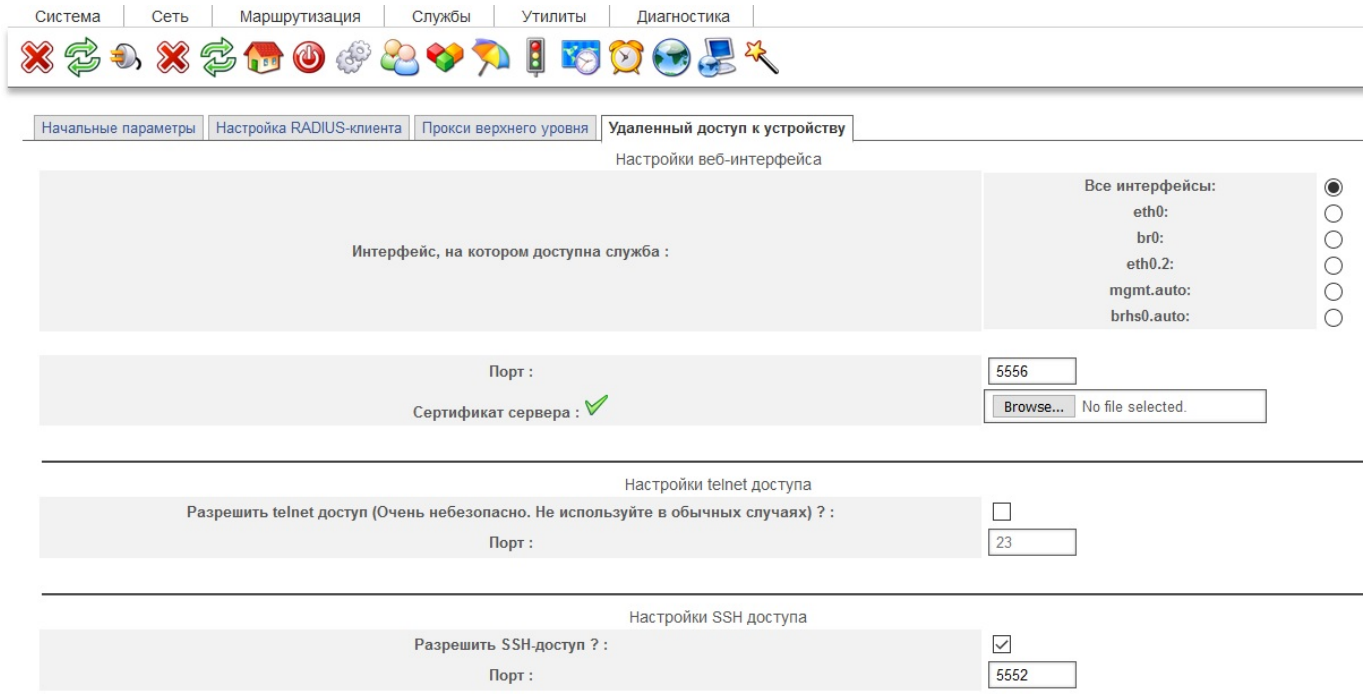


Закладка «Удаленный доступ к устройству»

позволяет определять и контролировать тип и возможности удаленного доступа к устройству. Удаленный доступ к устройству может осуществляться следующими способами:

1. через веб-интерфейс,
2. по протоколу telnet,
3. по протоколу SSH.

По умолчанию telnet выключен, а разрешенными являются только веб-интерфейс, как правило, на TCP-порту 5556 на LAN интерфейсах устройства, и SSH на TCP-порту 22 на всех интерфейсах устройства.



Стоит отметить крайне высокую уязвимость telnet доступа (пароль не запрашивается), которая не уменьшается возможностью ограничить telnet доступ каким-то определенным интерфейсом. Поэтому мы настоятельно рекомендуем не использовать telnet доступ.

SSH доступ не может быть ограничен каким-то одним интерфейсом или группой интерфейсов,

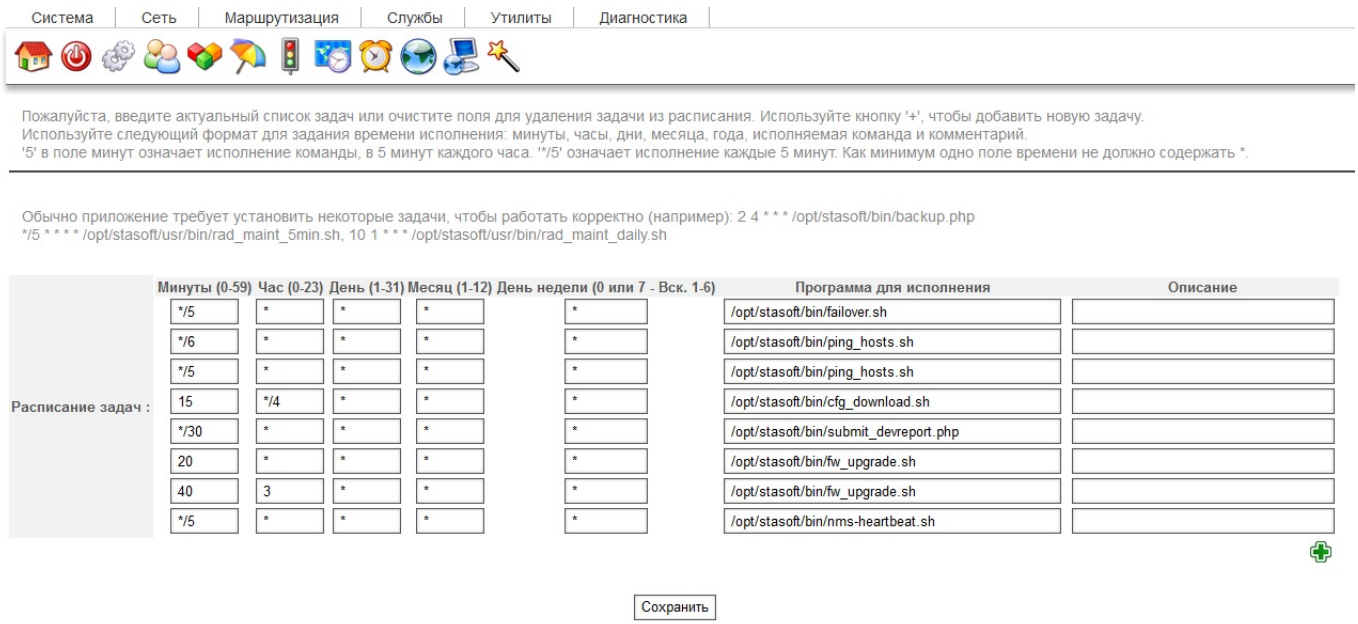
однако может быть назначен на порт, отличный от TCP 22, что мы настоятельно и рекомендуем сделать на рабочем устройстве.

Веб-интерфейс может быть доступен на всех интерфейсах устройства или назначен на конкретный интерфейс (умалчиваемое значение LAN). Кроме того, для веб-интерфейса может быть назначен порт, отличный от TCP 80 (стандартного HTTP). Настоятельно рекомендуем на рабочем устройстве разрешить веб-интерфейс на минимальном количестве сетевых интерфейсов и назначить его на порт, отличный от 80.

Кнопки в панели инструментов предлагают инструменты для остановки и запуска связанных служб (веб-интерфейс, telnet -сервер и т. п.)

Расписание задач

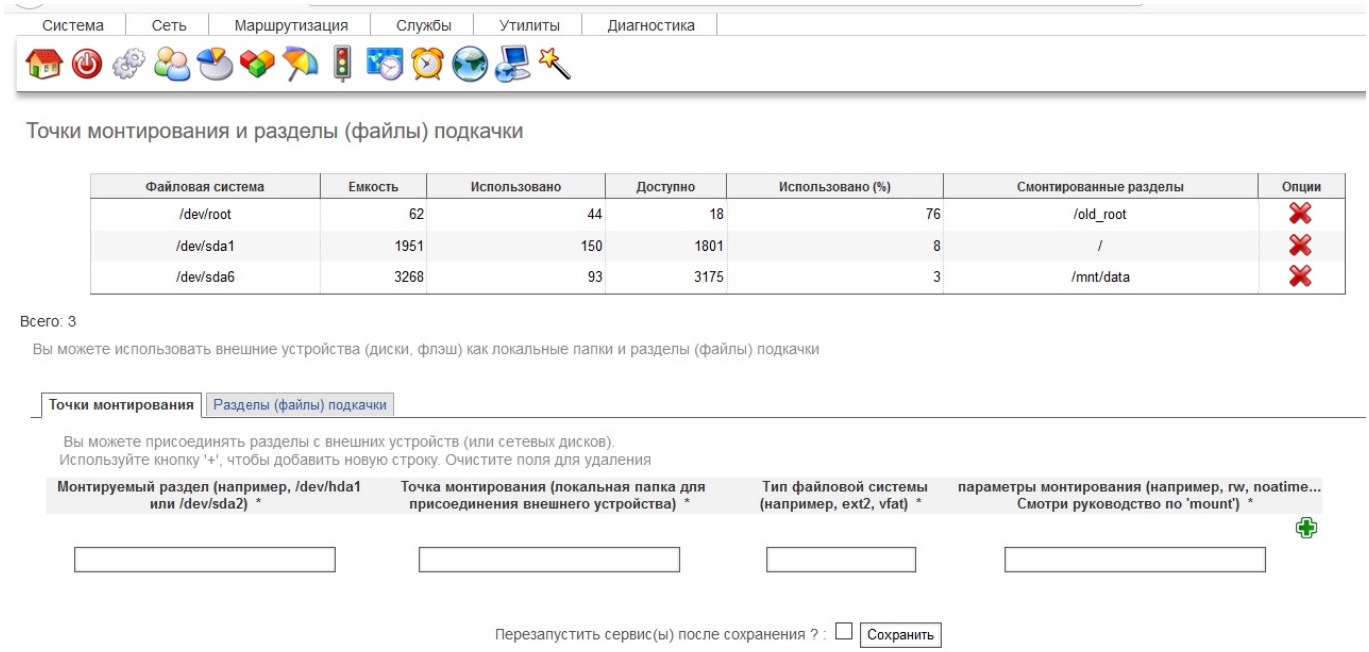
Позволяет управлять расписанием задач устройства. Синтаксис и поля полностью соответствуют таковому для **cron** в операционной системе Linux. Следует помнить, что введенные задания будут исполняться от пользователя *root*.



Примечание: система самостоятельно включает в расписание некоторые задачи (например, клиент сетевой службы синхронизации времени). Так же в расписание задач, как правило, включено выполнение скриптов для работы устройств NETSHe как контролируемых устройств со стороны NMMS. Например, */opt/stasoft/bin/cfg_download.sh* отсылает NMMS текущую конфигурацию.

Точки монтирования

В табличном виде представляет список смонтированных разделов с указанием точки монтирования, типа файловой системы, размера раздела и свободного пространства. Предоставляет возможность демонтировать раздел (используйте с крайней осторожностью).



Закладка «Точки монтирования»

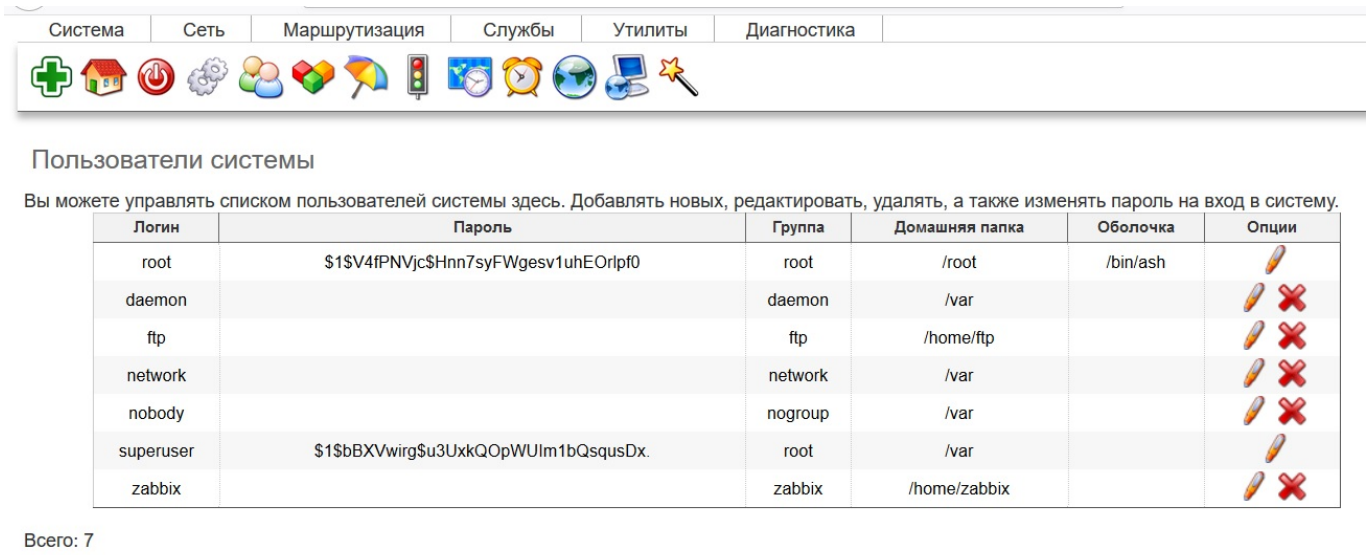
позволяет задать любое количество разделов с внешних устройств или сетевых ресурсов для монтирования их в файловой системе устройства. Задаются раздел физического устройства, каталог, в который будет осуществляться монтирование, тип файловой системы монтируемого раздела и дополнительные опции для команды **mount**.

Закладка «Разделы (файлы) подкачки»

задает заранее подготовленные (отформатированные как разделы подкачки) разделы или файлы на внешних устройствах для расширения размера памяти (использования в качестве разделов подкачки).

Пользователи

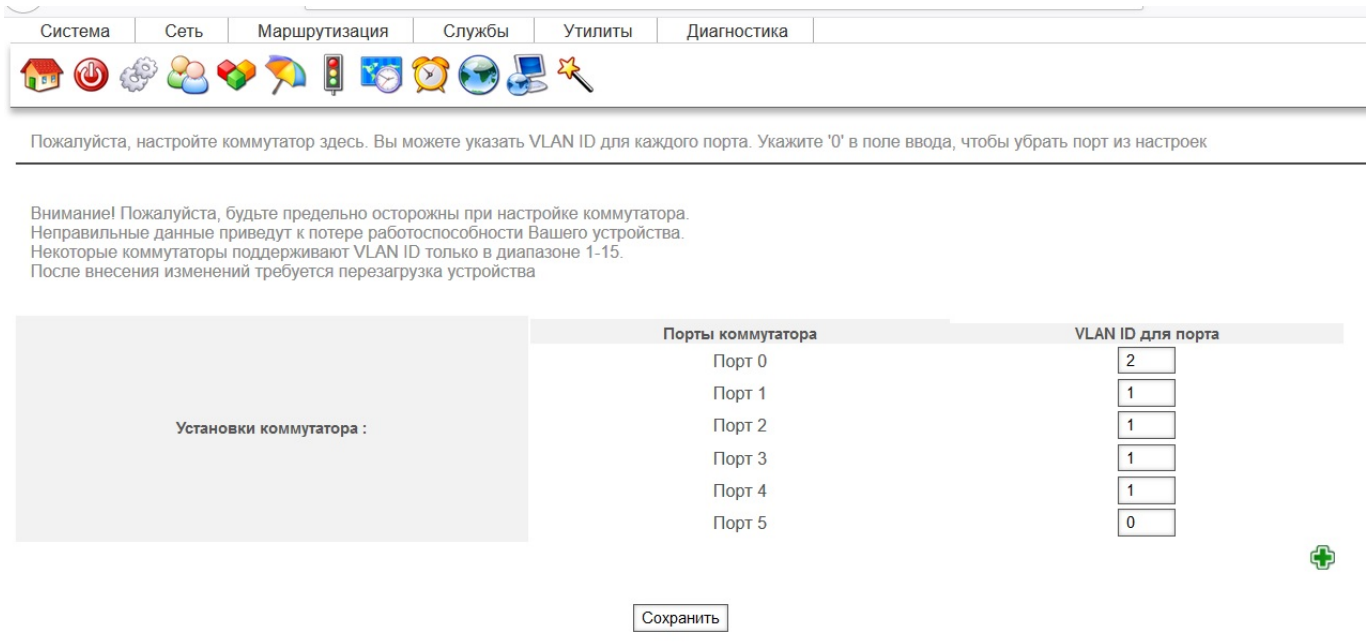
Представляет список системных пользователей с возможностью добавления, удаления и редактирования некоторых параметров. Пожалуйста, помните, что удаление пользователя root приведет к неработоспособности системы, обычно система не разрешает этого делать. Добавление пользователя с пустой оболочкой, оболочкой в виде */bin/false* или */bin/nologin* приведет к появлению в системе пользователя с правами «только для чтения» доступа в веб-интерфейс.



Иконки в панели инструментов и таблице пользователей означают добавление нового пользователя, редактирование параметров существующего и удаление пользователя. Диалог редактирования содержит поля для ввода и подтверждения нового пароля.

Управление Ethernet коммутатором

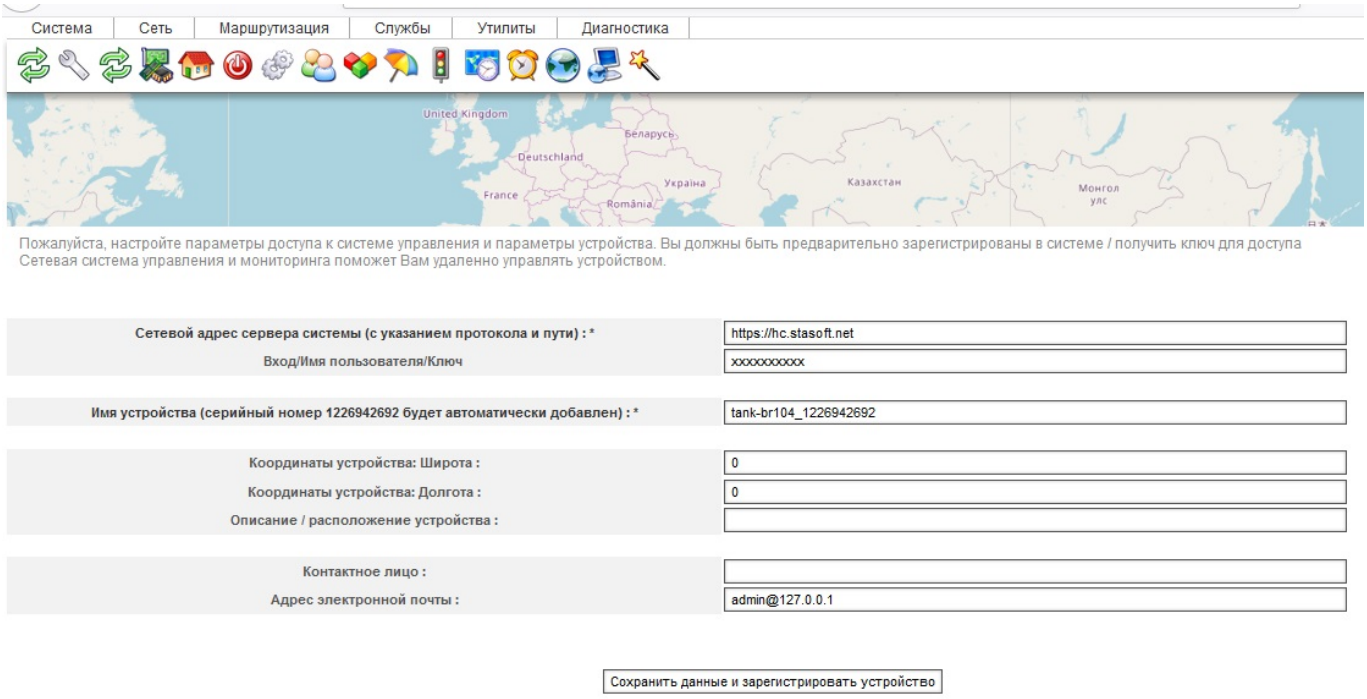
Представляет список портов встроенного модуля коммутатора. Каждому порту можно переопределить VLAN ID, так называемый VLAN на основе портов. Следует заметить, что эти действия нужно делать с особой осторожностью, полностью понимая их назначение.



Данный пункт не может быть использован для создания VLAN 802.1q.

Интеграция с системой управления и мониторинга

Страничка содержит параметры для подключения устройства к NMMS серверу: его адрес и ключ группы, в которую включается данное устройство. Помимо этого здесь же задаются географические координаты и адресная информация для отображения устройства на картах, встроенных в NMMS.



Панель инструментов прирастает иконками, относящимися к выгрузке/загрузке конфигурации устройства, обновлению программного обеспечения с NMMS.

Меню «Сеть»

Это меню содержит параметры сетевых объектов: интерфейсов, зон, мостов. А так же средств управления сетевым трафиком на интерфейсах устройства: межсетевой экран, фильтрация и приоритизация трафика.

Содержимое этого раздела меню будет описано в отдельной главе.

Меню «Маршрутизация»

Этот раздел главного меню отвечает за управление маршрутизацией на устройстве. В качестве пунктов этого меню есть средства статической и динамической маршрутизации, маршрутизации от источника и на базе политик.

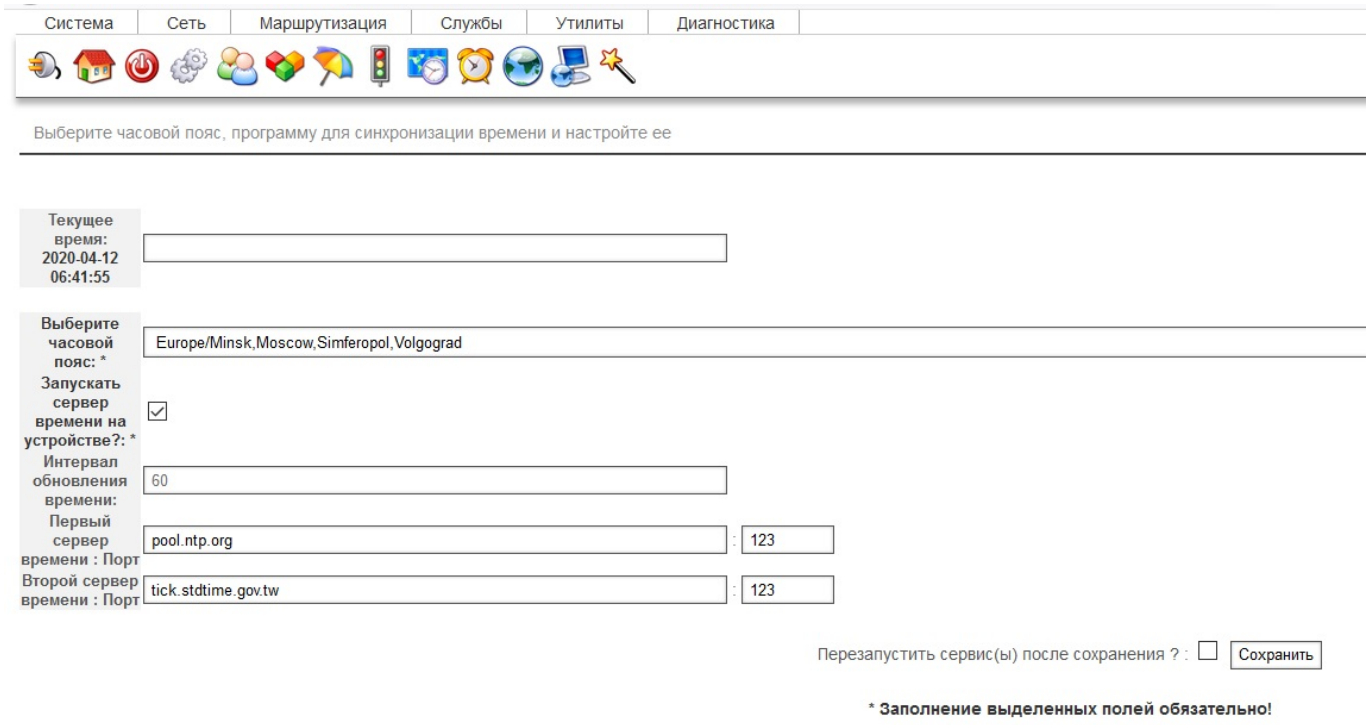
Содержимое этого раздела меню также будет описано в отдельной главе.

Меню «Службы»

Как правило, во всех пунктах этого меню в панель инструментов слева добавляется кнопка запуска соответствующего сервиса.

Установки времени и синхронизация

Этот пункт управляет установкой текущего времени устройства, часовым поясом и синхронизацией времени.



Синхронизация времени может осуществляться клиентской программой **ntpdate** с одним или более серверами времени в сети Интернет (в таком случае необходимо установить периодичность синхронизации) или сервером NTPD. В последнем случае сетевая служба времени становится доступной для клиентских устройств, подключенных к системе.

Концентратор доступа

Пункт «PPTP сервер»

задает такие настройки для сервера как:

1. Имя службы,
2. Интерфейс из зоны LAN, на котором доступна служба,
3. Локальный адрес (через этот адрес будет передаваться весь трафик) (необязательный параметр),
4. Первый адрес пула, из которого назначаются адреса клиентам (необязательный

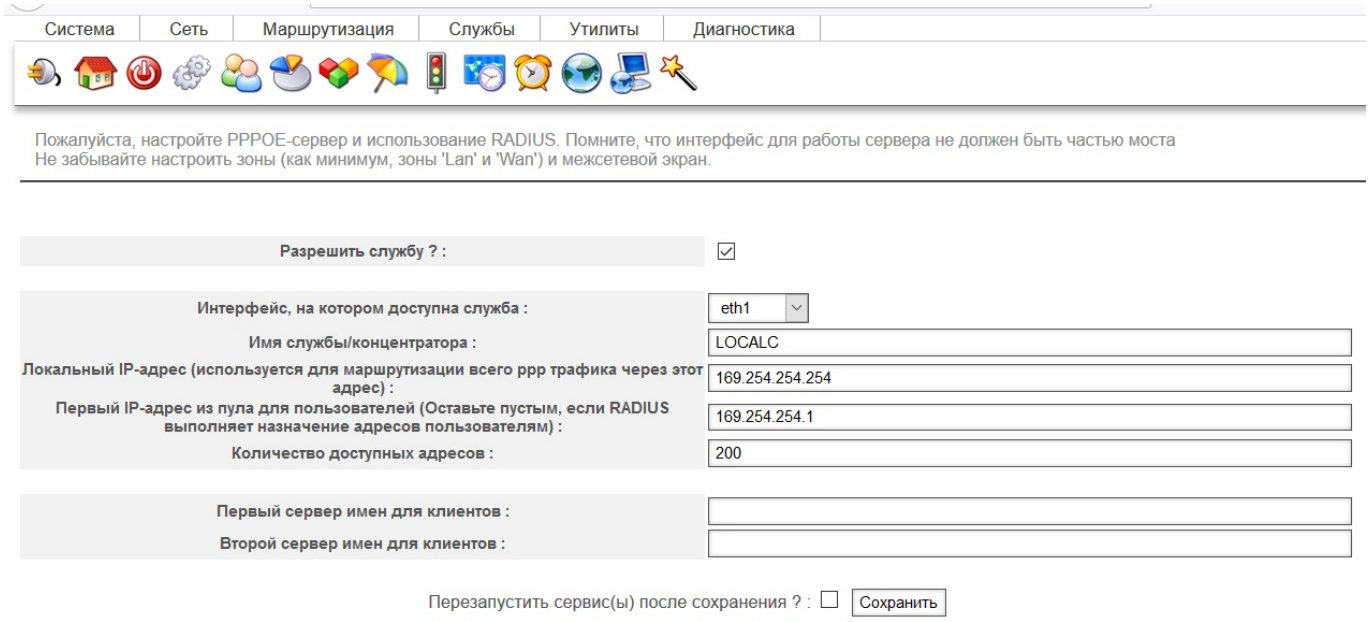
параметр. Не следует заполнять, если назначение адресов производится RADIUS-сервером),

5. Последний адрес пула, из которого назначаются адреса клиентам (необязательный параметр. Не следует заполнять, если назначение адресов производится RADIUS-сервером),

Все введенные адреса не должны пересекаться с иными адресами, используемыми на устройстве.

Пункт «PPPOE сервер»

содержит аналогичные настройки для данного протокола.



Стоит упомянуть, что PPPoE работает на базе широковещательных запросов канального уровня L2. С одной стороны, это означает автоматическую настройку связки клиент-сервер, с другой, накладывает ряд ограничений:

1. - клиентское устройство не может иметь маршрут по умолчанию,
2. - интерфейс, к которому привязан сервер PPPOE, не может иметь назначенного IP-адреса.

Пункт «L2TP сервер»

содержит аналогичные настройки, плюс возможность включения IPsec для соединений. В случае IPsec следует загрузить на устройство сертификат и ключ сервера.

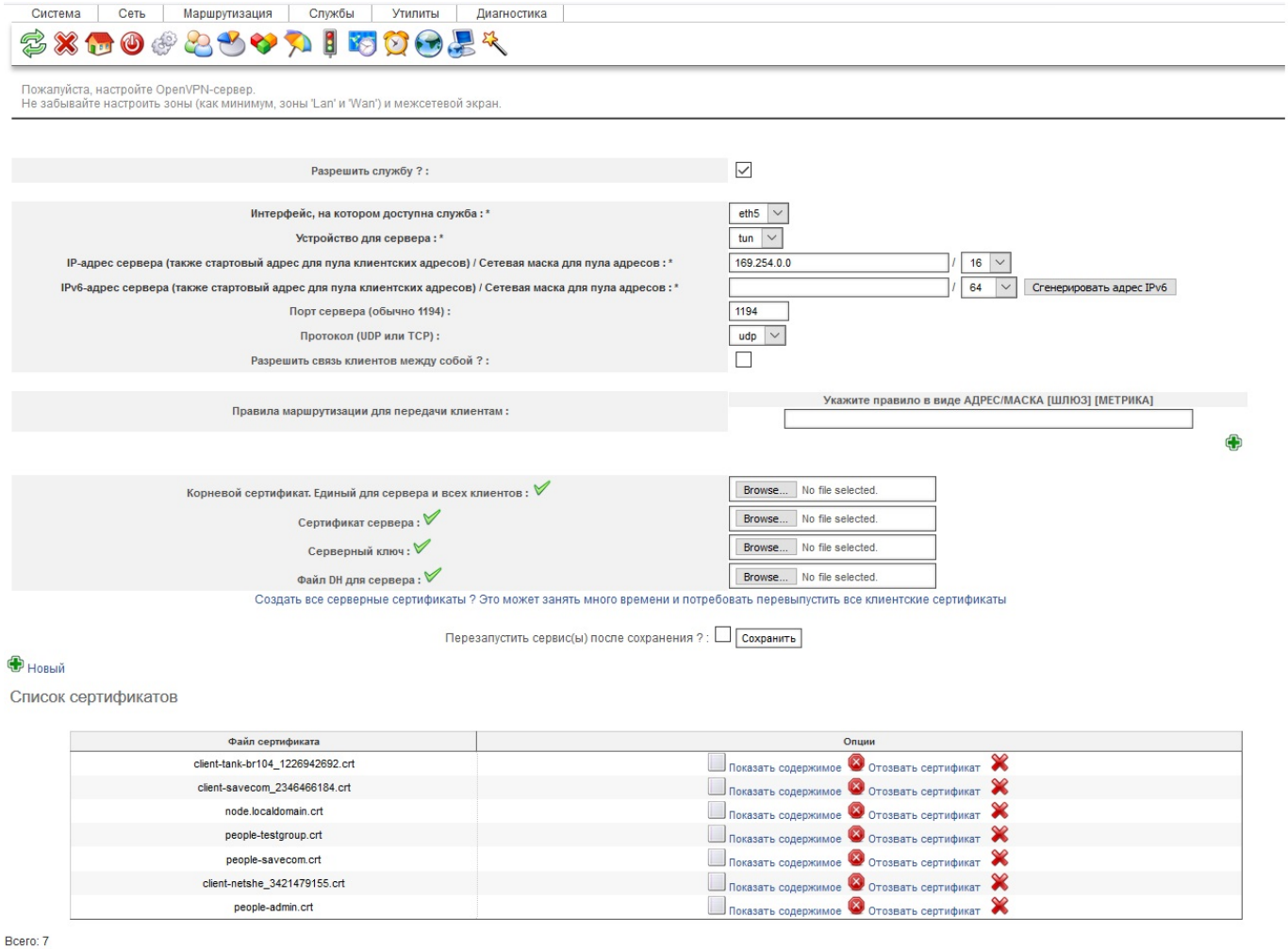
Пункт «Хотспот»

содержит средства управления хотспот-контроллером **chillispot.** Из параметров настроек доступны имя контроллера, внешний интерфейс, интерфейс на котором доступна служба (соответственно из зон WAN и LAN), UAM сервер и порт, а также секретная фраза для UAM сервера. Контроллер допускает указание сайтов (доменных имен), доступ к которым разрешен для неавторизованных пользователей.

Пункт «OpenVPN сервер»

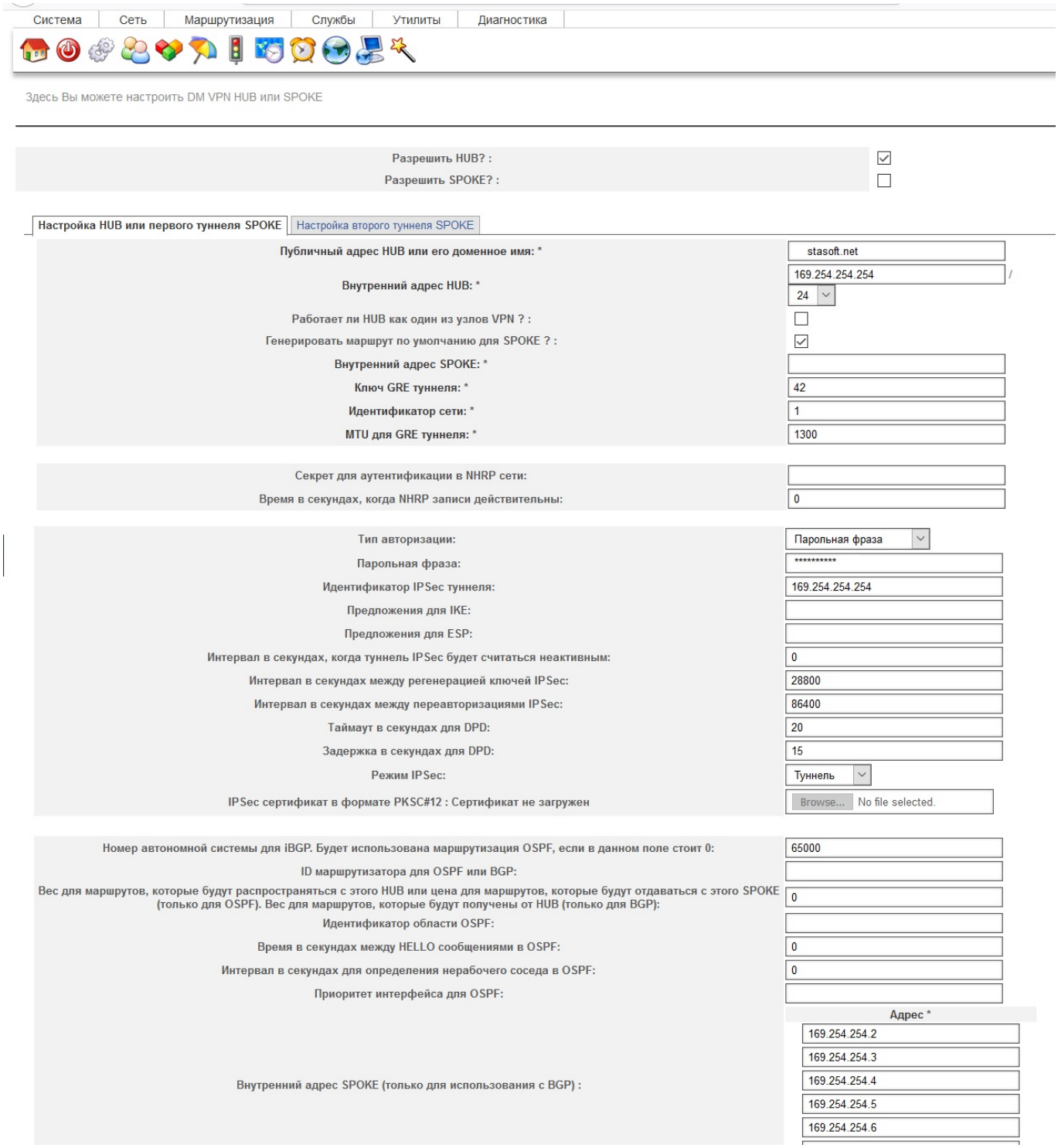
содержит средства для управления OpenVPN сервером. На закладке можно настроить:

1. - интерфейс, на котором будет доступна служба;
2. - пул адресов, выделяемых клиентам;
3. -порт сервера и протокол; загрузить корневой сертификат, сертификат сервера, ключ сервера и DH-файл.



Пункт «DM VPN»

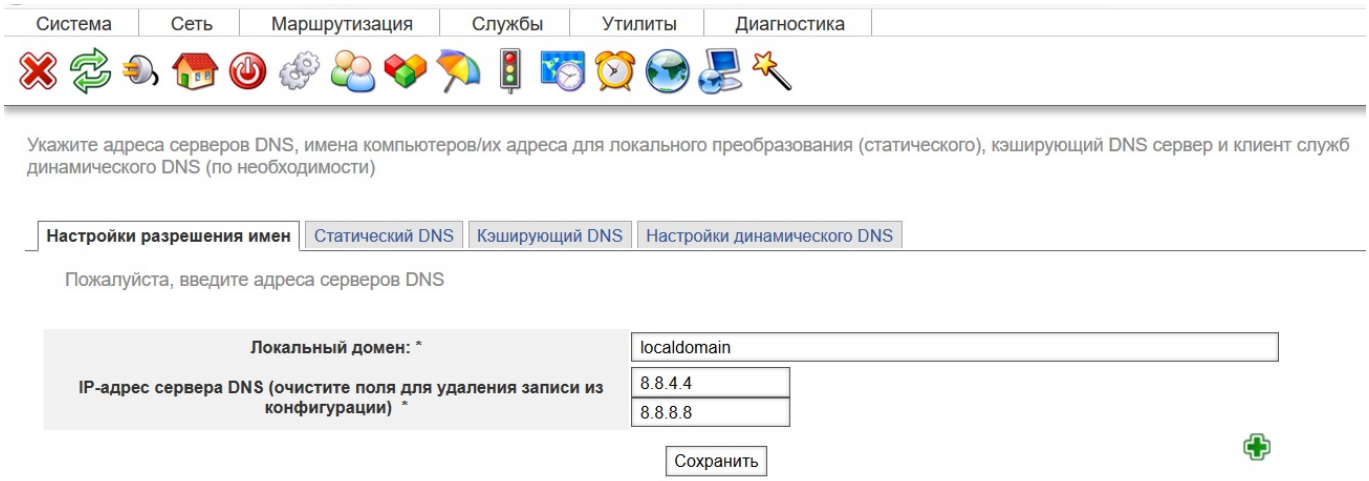
содержит параметры для Hub и Spoke в терминах динамического IPsec. Как правило, DM VPN применяется там, где нет возможности назначить публичный статический IP-адрес всем клиентам. Реализация DM VPN под NETSHe позволяет располагать клиентов даже за NAT. На следующей картинке показаны настройки Hub:



Служба разрешения имен

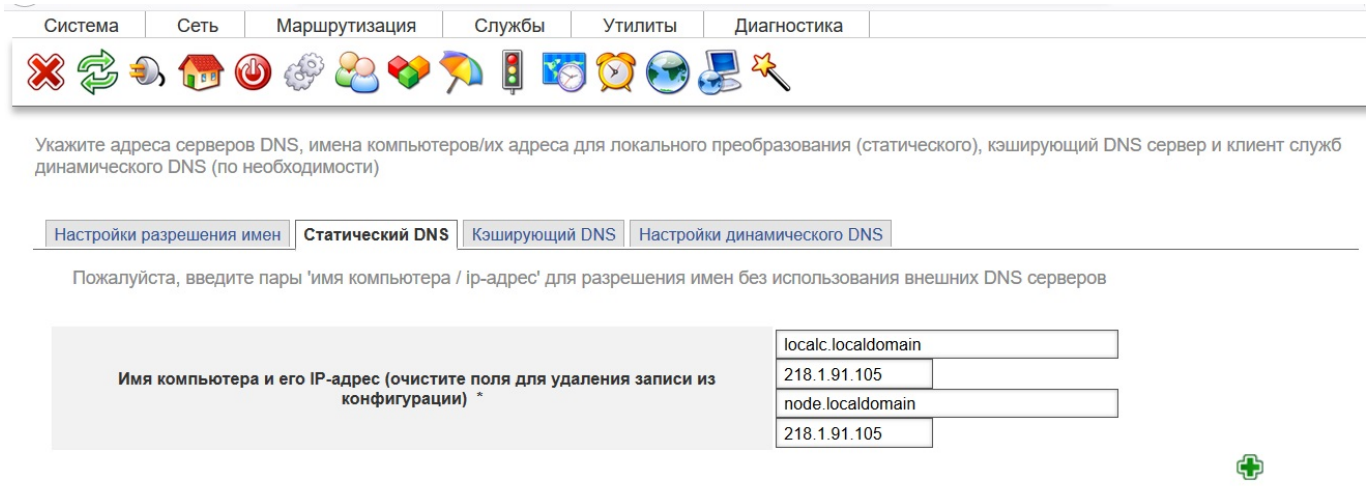
Настройка разрешения имен

позволяет указать домен, в котором работает устройство и один или более адресов внешних серверов разрешения имен.



Статический DNS

позволяет задать фиксированные пары доменное имя-адрес, которые будут разрешаться без обращения к серверам разрешения имен (т. е. Вы можете поставить в соответствие любой адрес любому доменному имени).



Кэширующий DNS

можно настроить зоны, на которых будет работать служба.

Настройки динамического DNS

можно выбрать поставщика услуг динамического DNS, внешний интерфейс для определения сетевого адреса, периодичность обновлений, имя пользователя службы и пароль.

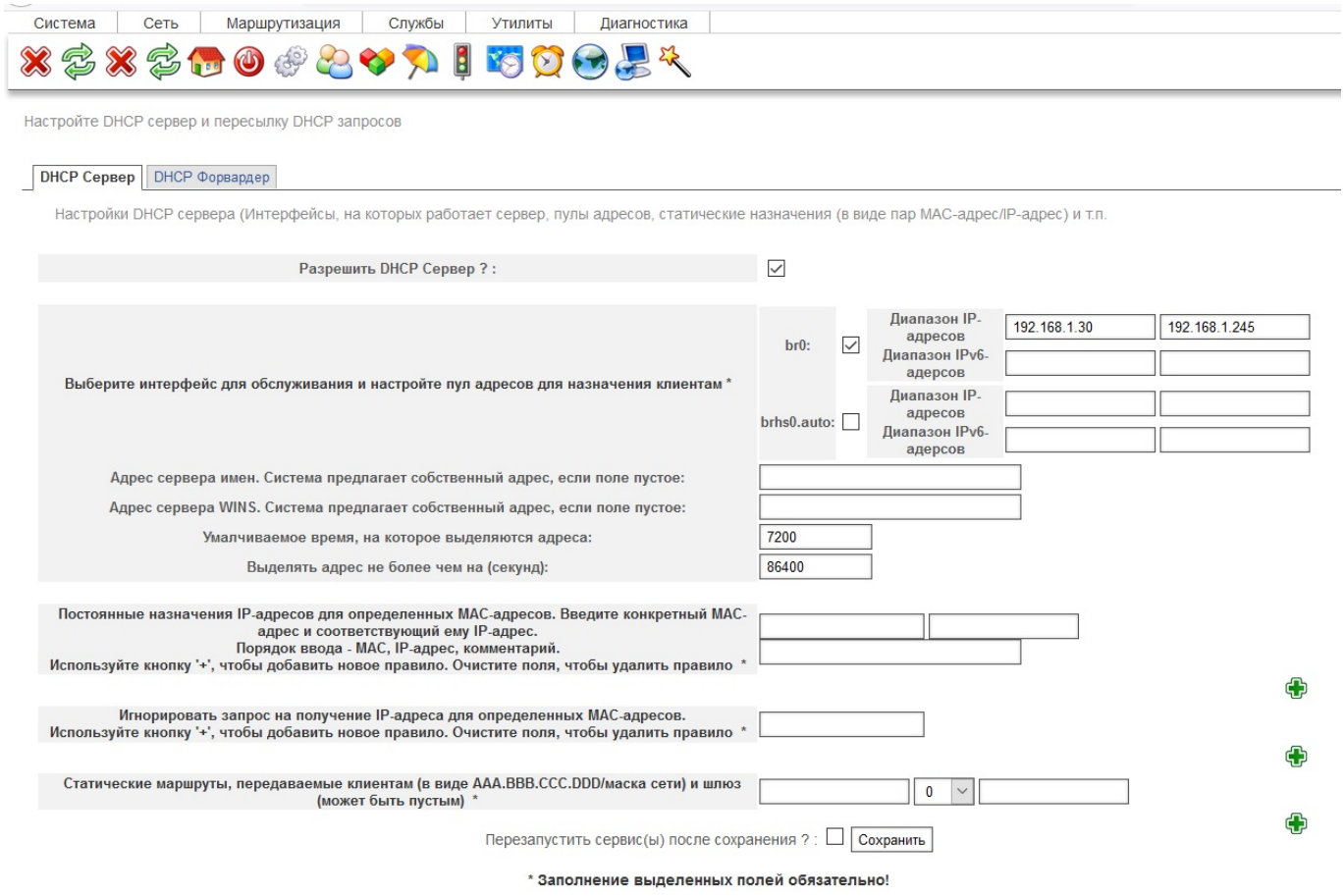
Напоминаем, что для пользования услугой динамического DNS Вы должны предварительно зарегистрироваться у выбранного поставщика услуги.

DHCP сервер и форвардер

Закладка «DHCP-сервер»

содержит средства настройки встроенного DHCP сервера (сервера, автоматически

назначающего сетевые адреса по запросам клиентов).



Параметрами настроек являются сетевые интерфейсы/зоны, на которых работает сервер; пул адресов, из которого будут автоматическим порядком выдаваться адреса; набор пар MAC-адрес/сетевой адрес для статического выделения адресов; список MAC-адресов, для которых запрещено выделение сетевых адресов.

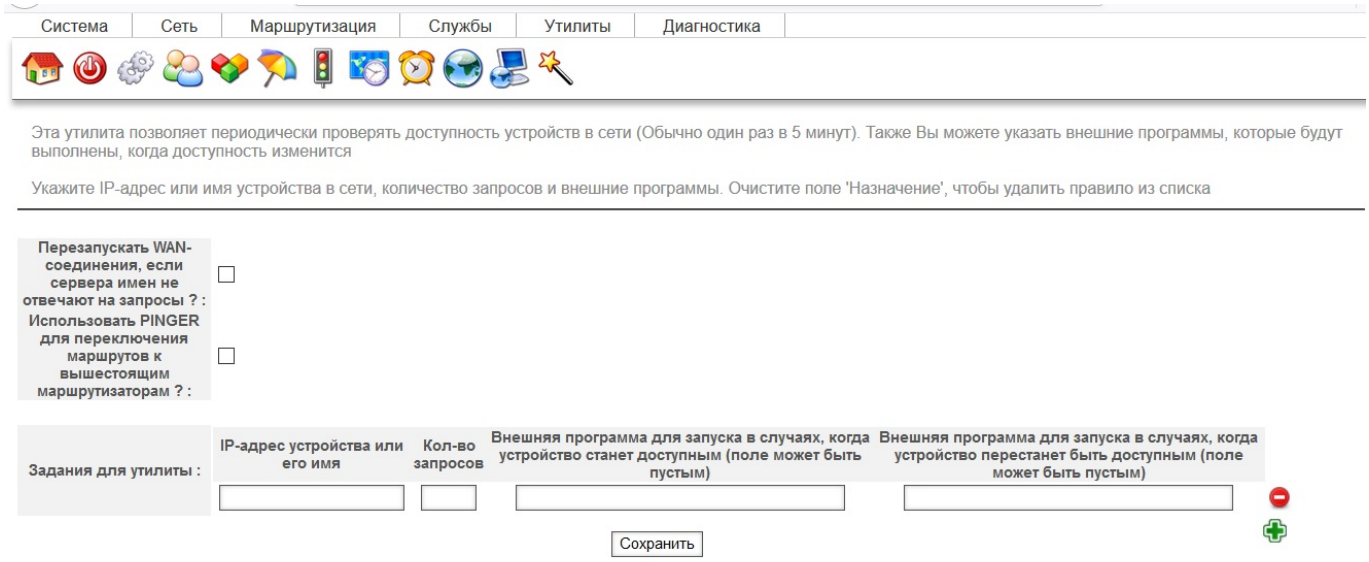
Закладка «DHCP-форвардер»

содержит средства для управления пересыльщиком DHCP запросов из внутренней сети на внешний DHCP сервер. Параметрами настройки являются адрес внешнего DHCP сервера, идентификатор устройства.

Сервер проверки соединений (pinger)

Представляет список IP-адресов для периодической проверки, где так же можно задавать реакцию в виде исполнения скрипта/команды на пропадание или появление проверяемого IP-адреса.

Следует заметить, что механизм pinger применяется при построении маршрутов и отказоустойчивых соединений, поэтому на этой странице присутствуют опции для включения или отключения этой связки.



Прокси и UPNP

Закладка «Служба UPNP”

предоставляет возможность настройки службы UPnP на устройстве. Настройки заключаются в выборе интерфейсов из зоны LAN, на которых доступна служба, скоростей внешнего интерфейса.

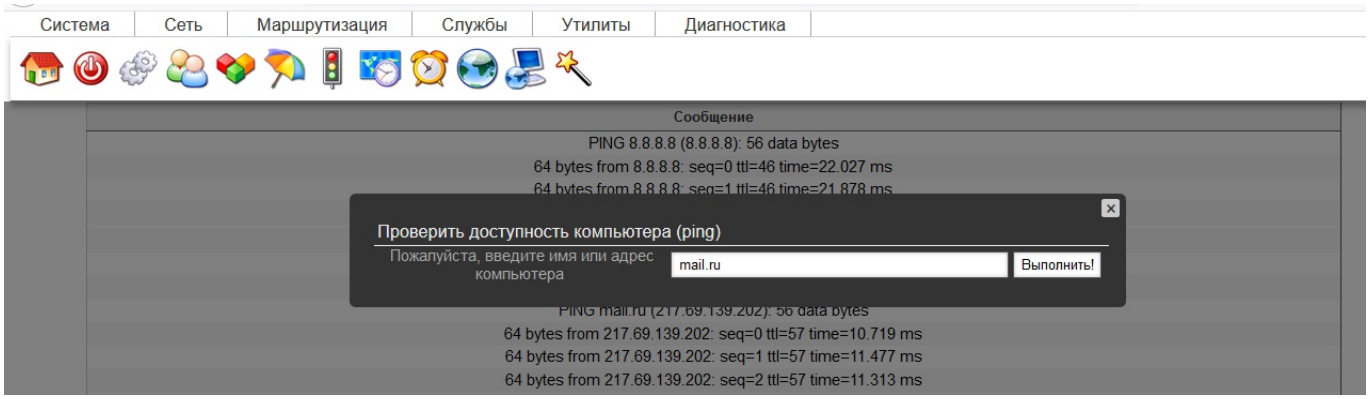
Закладка “HTTP/HTTPS прокси”

содержит средства для настройки прокси-сервера, таких как выбор внешнего интерфейса (из зоны WAN), интерфейса на котором доступна служба (только одного из зоны LAN), порт службы, ограничения на количество одновременных пользователей и использование прокси верхнего уровня.

Меню «Утилиты»

Доступность компьютера

Выполняет **ping** до указанного адреса или имени компьютера. Результат отражается на странице.

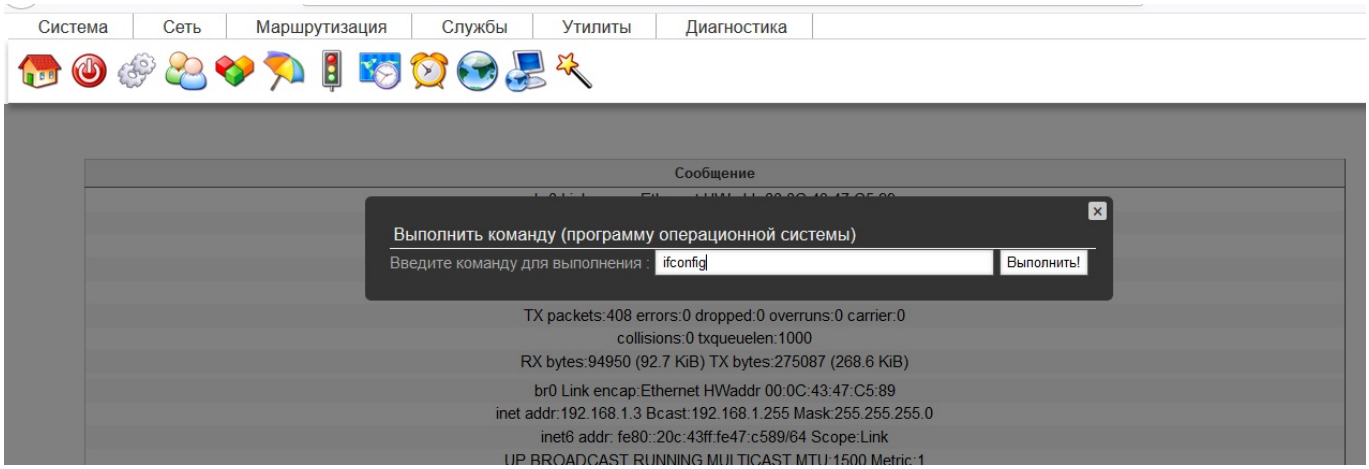


Проверить маршрут до компьютера

Выполняет **traceroute** до указанного адреса или имени компьютера. Результат отражается на странице, аналогично предыдущему пункту.

Выполнить программу

Предоставляет возможность выполнить любую команду, также как если бы Вы находились в консоли операционной системы. Вывод команды будет отражен на странице. Следует очень осторожно использовать эту функцию.



Перезагрузить

Выполняет перезагрузку устройства, выполняя **reboot.** Следует выждать 2-3 минуты перед новым обращением к устройству.

Остановить систему

Останавливает систему, выполняя **halt.** Новый запуск устройства возможен только после отключения и включения питания.

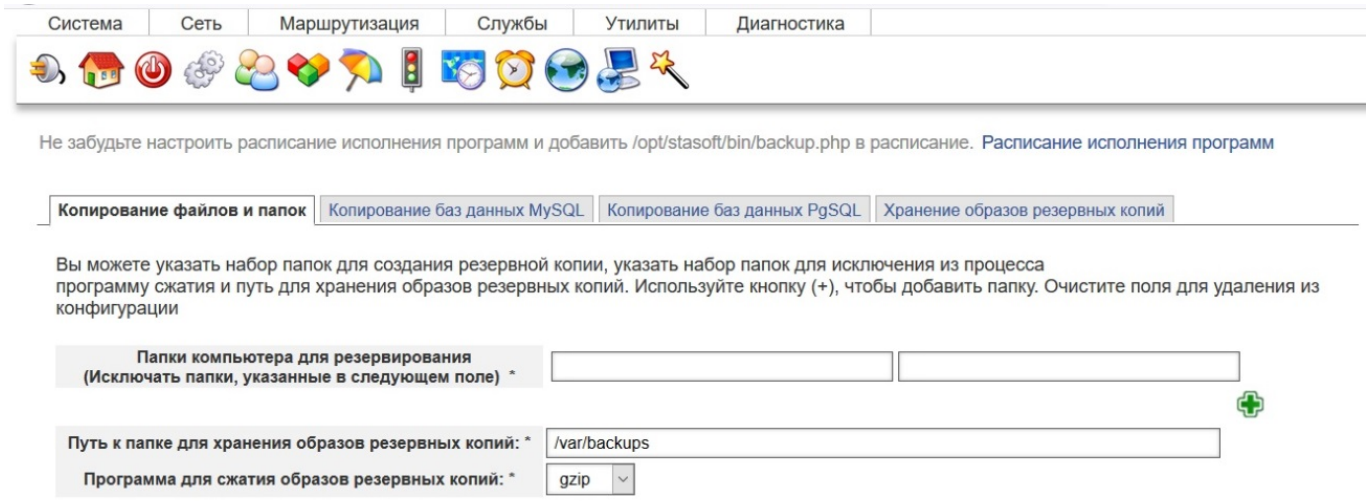
Перезапустить все сервисы

Как следует из названия, выполняется перезапуск всех сервисов без перезапуска устройства.

Создание/восстановление резервных копий.

Закладка** «Копирование файлов и папок»**

позволяет задать, какие именно каталоги системы требуется включать в образ резервного копирования. Помните, что Вы можете задать более одного каталога, используя кнопку «Добавить». Также для каждого каталога Вы можете указать подкаталоги, которые необходимо исключить из процесса резервного копирования.



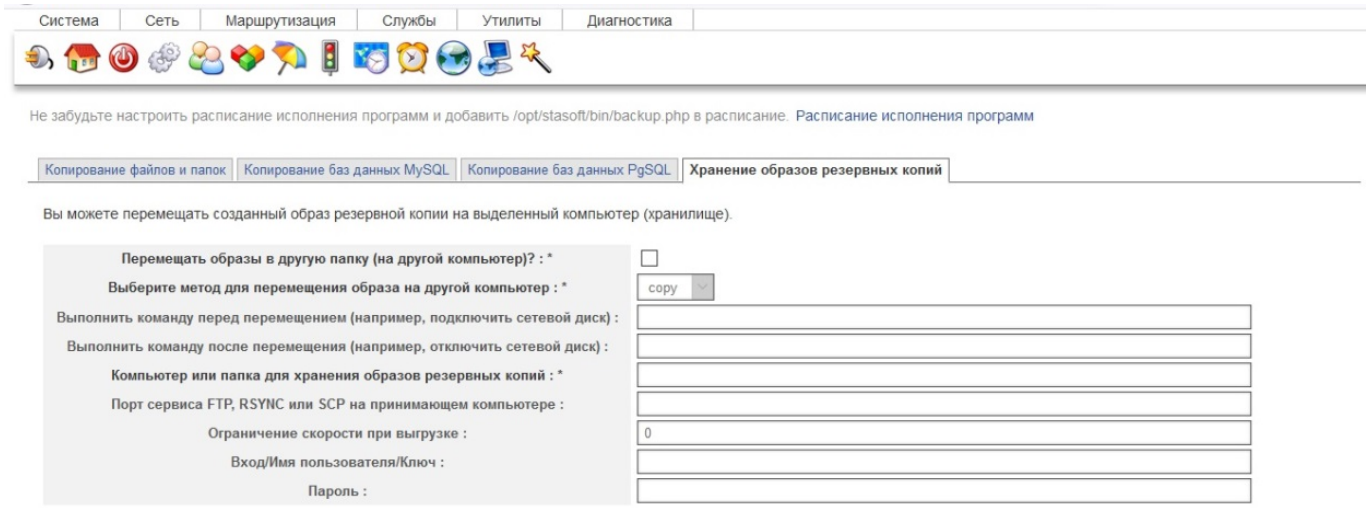
Одним из параметров настройки является выбор алгоритма сжатия для образов резервных копий (**gzip** или **bzip2**). На этой же закладке задается место (каталог файловой системы), в котором будут храниться резервные копии. Помните, что этот каталог не должен находиться на сетевом разделе, для осуществления резервного копирования у Вас в системе должен быть установлен программный пакет **rsync**, а также как минимум, один из архиваторов **gzip** либо **bzip2**.

Закладки «Копирование образов MySQL и PgSQL» .

При наличии установленных сервера(ов) и клиента(ов) MySQL и (или) PostgreSQL система позволяет производить полное резервное копирование всех баз данных обслуживаемых сервером. В этом случае в настройках следует указать логин и пароль superuser, каталог и метод сжатия. Готовые образы будут обрабатываться аналогично образам файлов и каталогов.

Закладка «Хранение образов резервных копий»

задает действия над образами резервных копий после их создания.



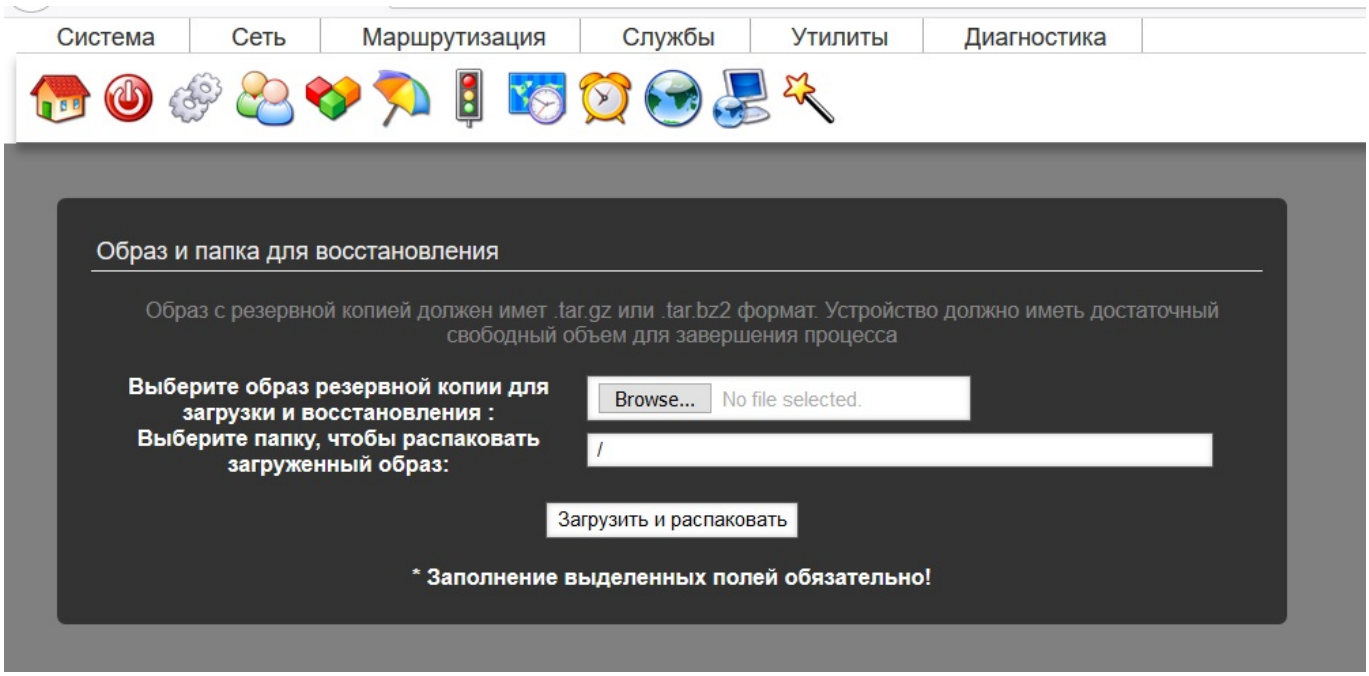
Такими действиями могут быть перемещение образа на удаленный сервер хранения встроенным клиентом ftp, либо по протоколам **scp** или **rsync** (требует установки соответствующих программ). Другим действием может быть перемещение или копирование образа на другой раздел устройства (другой физический накопитель), либо на сетевой раздел.

В качестве параметров настройки могут использоваться имя компьютера, на который осуществляется копирование, имя каталога, номер порта, вид протокола для связи, исполнение команд до и после копирования (например, **mount / unmount**).

Помните, что непосредственно создание резервных копий осуществляется командой *backup.sh*, время и периодичность вызова которой следует настроить в разделе «Расписания задач». Также резервное копирование может быть выполнено принудительно нажатием на кнопку «Выполнить резервное копирование» в панели инструментов.

Восстановление из образа.

Система имеет возможность загрузки на устройство и распаковки относительно указанного каталога резервного образа, которое создано встроенной системой резервного копирования и (или) имеет **.tar.gz** или **.tar.bz2** формат. При использовании следует учесть, что текущие файлы будут заменены на файлы из образа, а файлы, отсутствующие в образе/файловой системе, будут оставлены без изменений.



Сохранить текущий файл конфигурации/Загрузить новый файл конфигурации

Эти симметричные пункты меню позволяют сохранить конфигурацию системы NETSHe в виде текстового файла и, соответственно, заменить текущие настройки на указанные в загружаемом файле. Файл конфигурации сохраняется в папке «Загрузки», которая настроена в браузере.

Восстановить параметры по умолчанию.

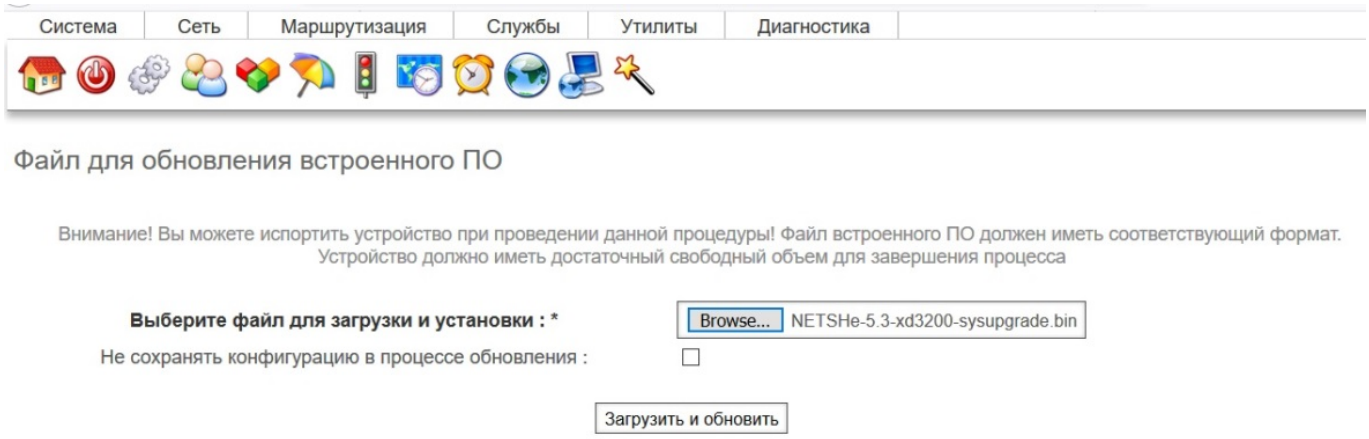
После выбора положительного ответа в диалоге текущая конфигурация системы будет заменена на заводские настройки. Подробно этот процесс описан в предыдущей главе. Используйте эту функцию с крайней осторожностью.

Обновление встроенного ПО

Функция позволяет загрузить в устройство и прошить новую прошивку (firmware). После загрузки предлагаемого файла система проверяет его MD5 хэш и версию. Дальнейшая установка производится только при соблюдении следующих условий:

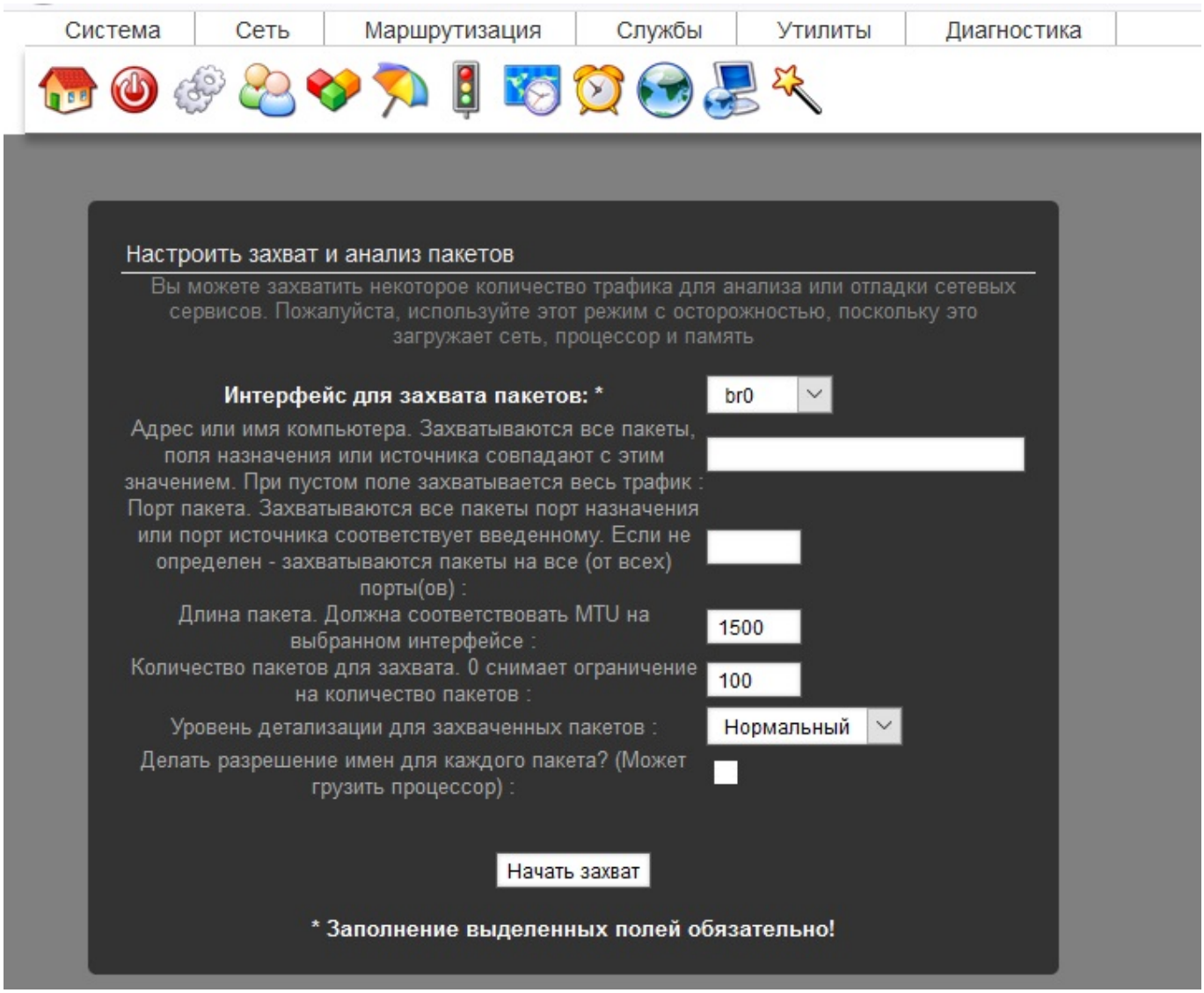
1. - если ПО подходит для модели данного устройства,
2. - версия загружаемого ПО выше версии текущего.

Пожалуйста, используйте эту функцию только тогда, когда понимаете, что вы делаете и располагаете файлами, имеющими соответствующий формат.



Захват пакетов

Вы можете захватить некоторое количество трафика для анализа или отладки сетевых служб. Фактически, для захвата и анализа трафика используется программный пакет **tcpdump**. Пожалуйста, используйте этот режим с осторожностью, поскольку это загружает сеть, процессор и память.



1. Для настройки Вы обязаны указать конкретный интерфейс для захвата трафика. Дополнительно Вы можете указать доменное имя или сетевой адрес компьютера. В этом случае будет захватываться только трафик, имеющий совпадения с этим адресом в поле получателя или отправителя (здесь речь идет применительно к протоколу IP). В случае если адрес не указан, будет захватываться весь трафик, проходящий через данный интерфейс и удовлетворяющий другим условиям (при их наличии).
2. Также Вы можете указать номер порта в качестве дополнительного критерия для захвата трафика. В таком случае будет захватываться трафик, порт отправителя или порт получателя которого совпадает с введенным значением.
3. Убедитесь, что параметр «Длина пакета» совпадает с размером MTU для выбранного интерфейса.
4. Введите количество пакетов для захвата. «0» означает неограниченное количество.

Процесс захвата можно будет прервать только нажатием соответствующей кнопки. Определите уровень детализации для захватываемого трафика, а также потребность в разрешении имени для каждого захватываемого пакета. Помните, что данная опция имеет смысл только, если в поле «Адрес или имя компьютера» введено доменное имя. Следует обратить внимание, что включение данной опции сильно нагружает процессор.

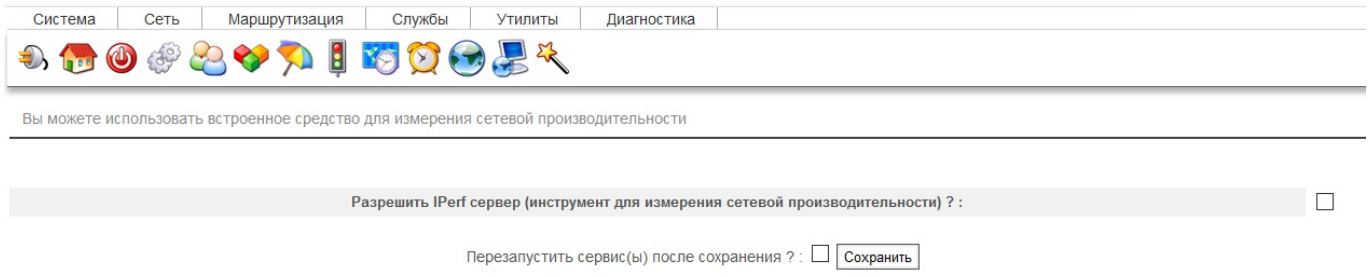
Общие рекомендации по использованию системы захвата пакетов.

Старайтесь указывать конкретные сетевые адреса и порты для захвата. Не включайте опцию разрешения имен для каждого пакета. Обязательно указывайте количество захваченных пакетов. **Помните, что данная операция всегда сильно нагружает процессор устройства и занимает много оперативной памяти.**

По завершении процесса захвата (по достижению указанного количества захваченных пакетов, либо по нажатию соответствующей кнопки) у Вас появится возможность выгрузить файл с захваченным и обработанным трафиком на локальный компьютер.

Сервер измерения сетевой производительности

Для измерения сетевой производительности в системе используется приложение **iperf** в режиме сервера. Это дает возможность измерения сетевой производительности при использовании **iperf** в режиме клиента с любого клиентского компьютера.



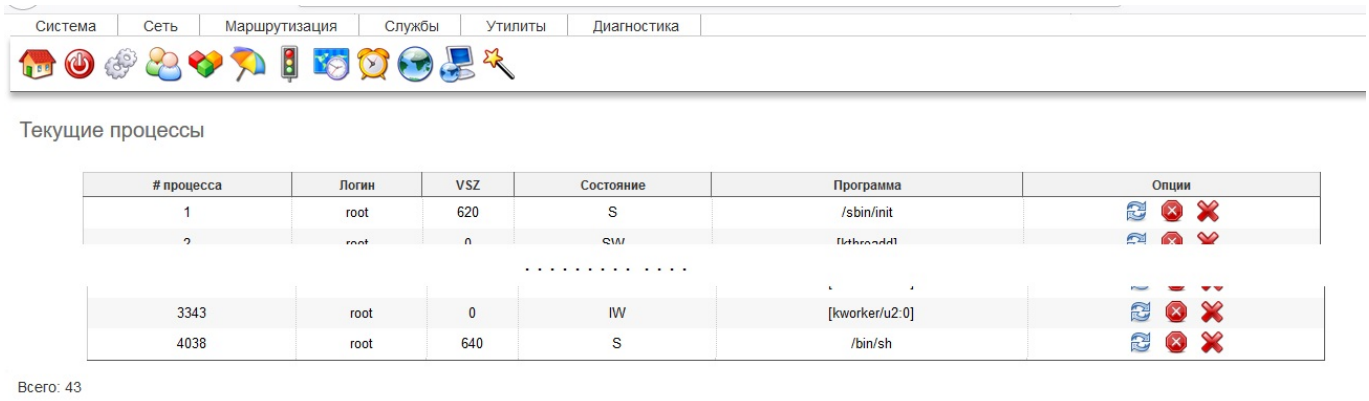
Меню «Диагностика»

Домашняя страница веб-интерфейса показывает основные сведения о системе и устройстве: версия операционной системы, версия ядра системы, тип и параметры процессора, размер оперативной памяти, сведения об интерфейсах, контроллерах и подключенных устройствах. Также в режиме, близком к реальному, отображает индикаторы загрузки процессора, памяти и разделов устройства, а так же графики загрузки интерфейсов.

Помимо этого система NETSHe предоставляет в веб-интерфейсе следующий набор средств диагностики, в большинстве своем построенный на базе консольных команд.

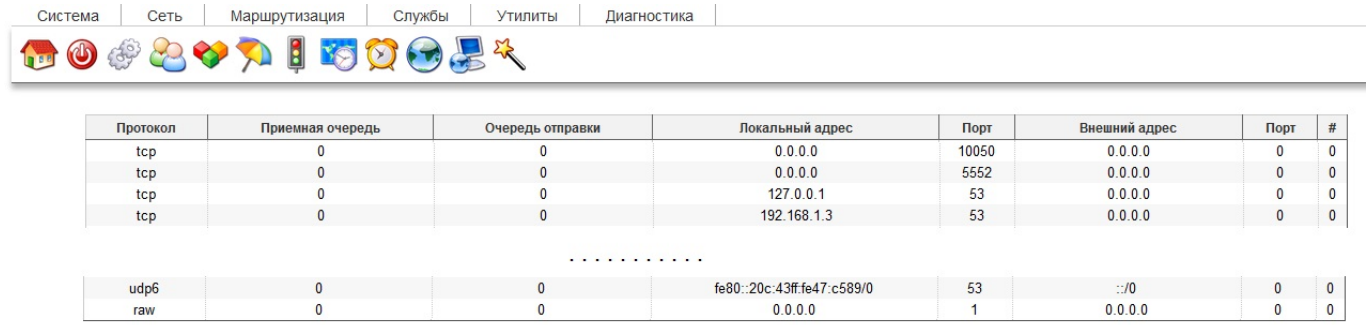
Процессы

Демонстрирует текущую системную таблицу процессов (**ps ax**) с возможностью послать любому процессу любой из трех сигналов: HUP, TERM и KILL, которые следует использовать с осторожностью.



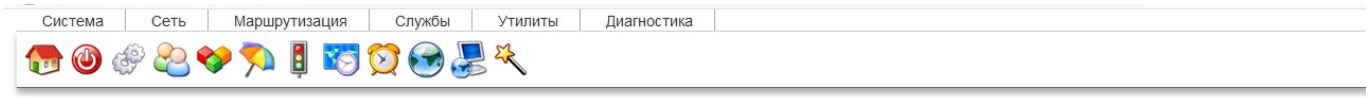
Текущие сессии

Показывает текущую системную таблицу соединений (**netstat -na**). Вывод автоматически обновляется.



Маршруты

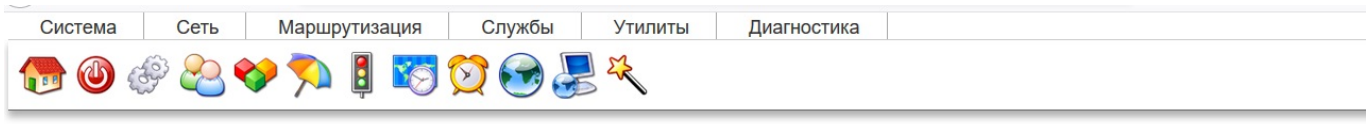
Демонстрирует текущую системную (main) таблицу маршрутизации (**netstat -nr**). Вывод автоматически обновляется.



Назначение	Шлюз	Метрика	Интерфейс
0.0.0.0/0	192.168.0.1	0	eth0.2
10.1.0.0/24	0.0.0.0	0	tun0.auto
192.168.0.0/24	0.0.0.0	0	eth0.2
192.168.1.0/24	0.0.0.0	0	br0
fe80::20c:43ff:fe47:c58a	::	1	eth0
. . . . .			
ff00::/8	::	1	tun0.auto
::/0	::	1	lo

Таблица MAC-адресов

Показывает системную таблицу соответствия IP- и MAC-адресов. Вывод автоматически обновляется.

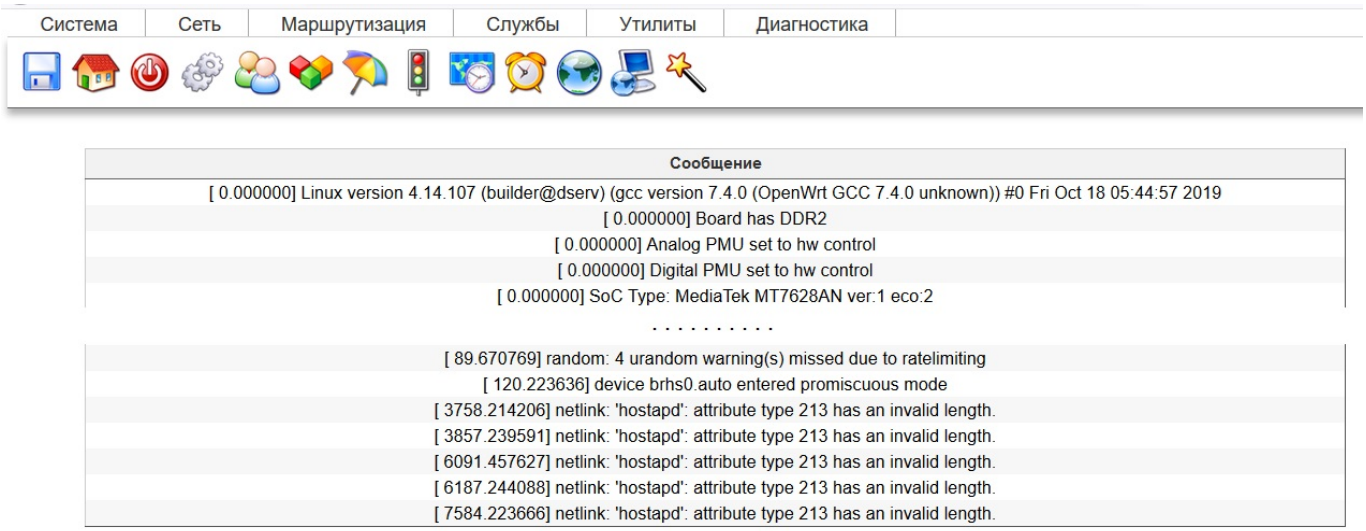


MAC	Адрес	Интерфейс
54:e4:bd:c7:c3:88	192.168.1.214	br0
78:d3:8d:e0:0d:09	192.168.0.1	eth0.2
48:45:20:cd:03:e3	192.168.0.145	eth0.2

Системные журналы

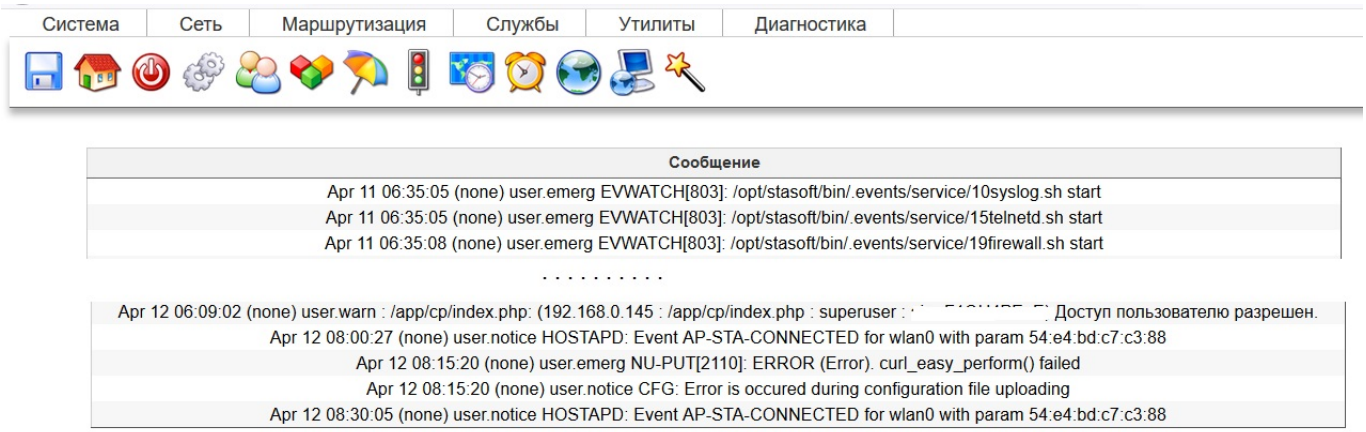
Аппаратный

демонстрирует вывод **dmesg**.



Общий

демонстрирует содержимое системного лог-файла **/var/log/messages**.



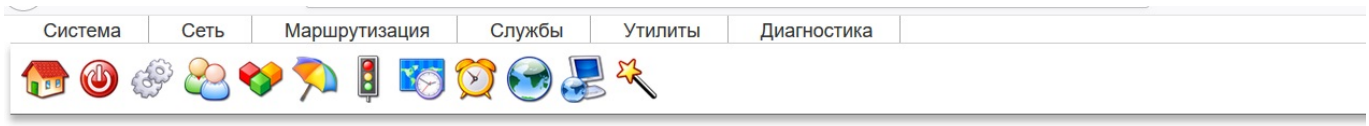
В панели инструментов появляется иконка для сохранения журналов.

Создания отчета для разработчика

Этот пункт подробно описан в предыдущей главе. В нем можно создать отчет, содержащий конфигурацию, журналы, статистику системы для разбора технической поддержкой. Отчет сохраняется в папке «Загрузки» браузера.

Правила МСЭ IPv4 / IPv6

Демонстрирует текущие правила межсетевого экрана (**iptables -vL**).

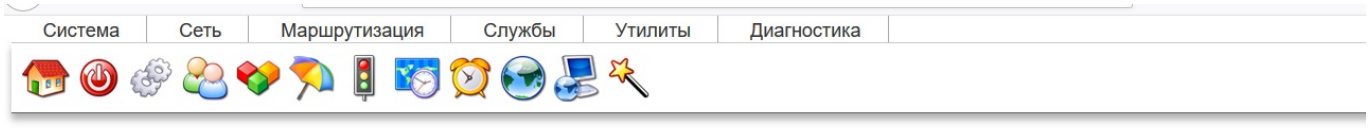


[Текущие правила и состояние межсетевого экрана]

Текущее состояние межсетевого экрана
Chain INPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
9720 1062K ACCEPT all -- any any anywhere anywhere ctstate RELATED,ESTABLISHED
3 570 ACCEPT all -- lo any anywhere anywhere
608 31616 syn_flood tcp -- any any anywhere anywhere tcp flags:FIN,SYN,RST,ACK/SYN
898 59932 input_rule all -- any any anywhere anywhere
897 59858 input all -- any any anywhere anywhere
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
. . . . .
Chain zone_Wan_output (0 references)
pkts bytes target prot opt in out source destination
0 0 output_Wan all -- any any anywhere anywhere

Адреса, выданные сервером DHCP

В табличном виде демонстрирует назначенные клиентам через обращение к DHCP-серверу сетевые адреса и их MAC-адреса.



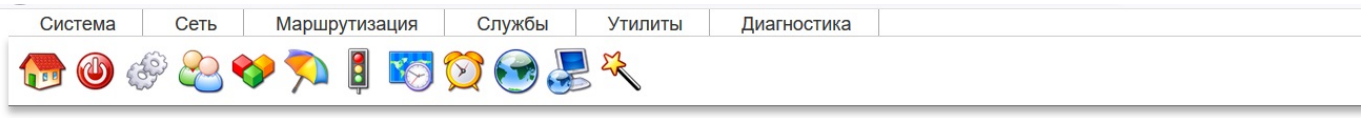
На какое время выделен адрес	MAC	Адрес	Имя клиента	Сообщение
1970-01-01 00:00:00	54:e4:bd:c7:c3:88	192.168.1.214	TeclastX98-W10H	01:54:e4:bd:c7:c3:88

Состояние системы фильтрации Ethernet-кадров

Демонстрирует текущие правила системы фильтрации Ethernet-кадров (**ebtables -vL**)

Состояние системы QOS

Показывает текущие правила системы управления трафиком.

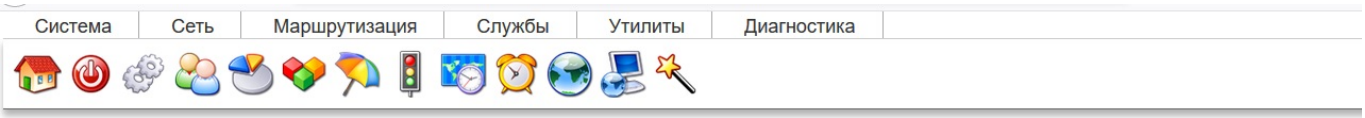


[Состояние системы качества обслуживания]

Сообщение
qdisc noqueue 0: dev lo root refcnt 2
qdisc fq_codel 0: dev eth0 root refcnt 2 limit 10240p flows 1024 quantum 1514 target 5.0ms interval 100.0ms memory_limit 4Mb ecn
qdisc noqueue 0: dev wlan0 root refcnt 2
qdisc noqueue 0: dev br0 root refcnt 2
qdisc noqueue 0: dev brhs0.auto root refcnt 2
qdisc noqueue 0: dev eth0.1 root refcnt 2
qdisc noqueue 0: dev eth0.2 root refcnt 2
qdisc mq 0: dev tun0.auto root
qdisc fq_codel 0: dev tun0.auto parent :1 limit 10240p flows 1024 quantum 1500 target 5.0ms interval 100.0ms memory_limit 4Mb ecn

Текущие сервера имен

Показывает список DNS серверов, глобально определенных в системе.



Сообщение
nameserver 8.8.8.8

Особенности работы веб-интерфейса при удаленном подключении с NMMS

Система Network Management and Monitoring Server (NMMS) описывается в последующих главах. Забегая вперед, только упомянем, что NMMS занимается централизованным управлением устройствами с ОС NETSHe и среди прочих возможностей обеспечивает подключение к веб-интерфейсу всех контролируемых устройств непосредственно из веб-интерфейса NMMS. Для обеспечения веб-доступа к устройствам из недоступных сетей применяется обратный HTTP-прокси и AJAX интерфейс.

Вследствие этого часть функционала WebUI устройства не может быть реализована полностью корректно. Тем не менее, из соображений унификации интерфейса, эти пункты оставлены в меню, тем более что многие из них частично функционируют. Это относится к следующим пунктам:

1. «Система→Расписание задач», «Система→Точки монтирования», «Службы→Сервис проверки соединений(pinger)». Некоторые пункты, содержащие на страницах пути файловой системы устройств, могут отображаться с путями в виде URL.
2. «Утилиты→Обновление встроенного ПО», «Утилиты→Загрузить новый файл конфигурации», «Утилиты→Восстановление из образа». Пункты, предполагающие загрузку (upload) файлов на устройство, в этой части не работают.
3. Пункт «Утилиты→Консоль» не работает. Для доступа к консоли есть специальная ссылка

в списке устройств NMMS у каждого включенного устройства.
4. Мастер первоначальной настройки работает, но на последнем шаге выдает ошибку, т.к. нет возможности вернуться из проксированной веб-страницы.

В остальном с помощью веб-интерфейса, при доступе к нему с NMMS, можно вносить изменения в конфигурацию устройства, управлять его функционалом так же, как если бы Ваш компьютер был подключен непосредственно к LAN порту устройства, а Вы бы открыли в браузере страничку https://192.168.1.1:5556 (по умолчанию).

From:
http://docs.netshe-lab.ru/ - **Документация по NETSHe**

Permanent link:
http://docs.netshe-lab.ru/doku.php?id=%D0%B3%D0%BB%D0%B0%D0%B2%D0%B0_3_-_%D0%BC%D0%B5%D0%BD%D1%8E_%D0%B2%D0%B5%D0%B1-%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D1%84%D0%B5%D0%B9%D1%81%D0%B0

Last update: **2020/07/20 10:19**