netshe_doc_chap1

Original file

NETSHe Lab

Универсальное программное обеспечение NETSHe для сетевых устройств. Часть 1. Общие сведения	
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 Март, 2020	Станислав Корсаков, ООО «Нетше лаб» (c) 2009-2020 Ярославль

Оглавление

Введение в NETSHe

В этом разделе Вы сможете узнать об устройстве NETSHe, основных функциях, системных требованиях NETSHe, способах и методах установки на устройства.

NETSHe представляет собой набор программного обеспечения для сетевых и встраиваемых устройств (маршрутизаторы, точки доступа), телевизионных приставок, сетевых хранилищ и многих других.

Программное обеспечение, построенное на базе ядра Линукс, включает в себя:

1. набор программных пакетов, реализующих функционал ПО;
2. подсистему хранения конфигурации системы/устройства;
3. подсистему инициализации;
4. подсистему событий, на основе которой происходит взаимодействие компонентов программного обеспечения;
5. веб-интерфейс управления устройством.

Основные функции NETSHe

NETSHe реализует следующий набор функций

в части сетевого взаимодействия:

1. Управление сетевыми интерфейсами (в том числе динамическими, туннельными и радио);
2. Виртуальные интерфейсы и алиасы;
3. Управление маршрутизацией (в том числе статической, на основе правил, динамической с применением RIP, OSPF, BGP);
4. Сетевой мост;
5. Объединение интерфейсов;
6. DHCP-сервер (автоматическое назначение IP-адресов клиентским машинам) и DHCP-форвардер (пересыльщик DHCP запросов с внутренней сети на внешний DHCP-сервер) с гибкими правилами выделения адресов (фильтрация по MAC-адресам/статическое выделение адресов/динамическое выделение);
7. Сервер и клиент службы времени, интегрированный с сервером DHCP;

в части формирования и управления трафиком:

1. Межсетевой экран с поддержкой зон;
2. Управление качеством обслуживания (QoS) и приоритизацией исходящего трафика;
3. Использование характерных для приложений последовательностей в трафике для построения правил межсетевого экрана и качества обслуживания (L7). Данная функция допускает написание правил фильтрации для определенных видов трафика, например, пиринговых сетей, а также повышение приоритета трафика аудио- и видео-приложений;
4. Фильтрация Ethernet-кадров;
5. HTTP-прокси с возможностью использования вышестоящего прокси-сервера (каскадирование);

в части туннелирования соединений:

1. Сервер доступа с поддержкой протоколов PPTP, PPPoE, L2TP с авторизацией на внешнем RADIUS-сервере;
2. Концентратор для частных выделенных сетей (VPN) на протоколах PPTP и L2TP с поддержкой IPSEC (в связке L2TP/IPSEC) и OpenVPN;
3. DM VPN хаб и спок;
4. IPSec клиент и сервер;

в части радио и беспроводных сервисов:

1. Расширенное управление радио-интерфейсами с поддержкой режимов клиента, базовой станции и повторителя, в том числе с режимами шифрования WEP и авторизации WPA-PSK, WPA-EAP, 802.11X;
2. Хот-спот контроллер с выделением адресов клиентам, авторизацией на внешнем UAM-сервере, управлением пропускной способностью и управляемым доступом к сайтам;

в части мониторинга и управления устройствами:

1. Управление программным обеспечением устройства. Возможность удаления установленных программных пакетов, установки новых, подключения новых репозиториев;
2. Управление пользователями устройства с разделением уровней доступа через веб-интерфейс (полный или только для чтения);
3. Управление внешними накопителями и разделами с возможностью подключения внешних накопителей с пользовательскими разделами, разделами физической памяти (своп) и т.п.;

4. Мониторинг состояния системы (памяти/процессора/сетевых интерфейсов и т. п.) в режиме реального времени с наглядным отображением в виде графиков;
5. Мониторинг состояния системы через SNMP протокол (сетевые интерфейсы и физические разделы);
6. Резервное копирование любых каталогов устройства на внешние устройства/ftp-сервер и т. п.;
7. Восстановление каталогов и файлов устройства из ранее сохраненных образов;
8. Сохранение и восстановление файлов конфигурации. Сброс конфигурации в стартовую;
9. Обновление прошивки устройства;
10. Захват и анализ сетевого трафика, проходящего через устройство;
11. Утилиты проверки доступности хостов и маршрутов к ним (ping, traceroute);
12. Остановка и перезагрузка системы;

Используемое программное обеспечение и права

В составе используется, либо использовалось в качестве основы для производной работы разнообразное программное обеспечение под соответствующими лицензиями. Например:

1. Ядро Linux, код которого распространяется под лицензией GPL2.
2. Yahoo User Interface library (http://yui.uahoo.com). Библиотека имеет BSD лицензию.
3. Некоторый код из проекта m0n0wall. Код распространяется под BSD лицензией.
4. Некоторый код из проекта pfsense и от Scott Ulrich. Код распространяется под BSD лицензией.
5. Некоторый код из проекта phpsysinfo, распространяемый под лицензией GPL v2.
6. Некоторые иконки и изображения - часть проекта Tango (Авторы - Ulisse Perusin uli.peru@gmail.com, Steven Garrity sgarrity@silverorange.com, Lapo Calamandrei calamandrei@gmail.com, Ryan Collier rcollier@novell.com, Rodney Dawes dobey@novell.com, Andreas Nilsson nisses.mail@home.se, Tuomas Kuosmanen tigert@tigert.com, Garrett LeSage garrett@novell.com, Jakub Steiner <jimmac@novell.com>). Набор иконок распространяется под лицензией Creative Commons 2.5.
7. Используемые изображения из набора Nuvola распространяются под лицензией LGPL v2.1. Автор - David Vignoni (david@icon-king.com).

Иной код, аудио-визуальные образы имеют своих авторов и распространяются в соответствии с их лицензиями.

Часть кода и изображений разработаны Станиславом Корсаковым, другими сотрудниками ООО «Нетше лаб» и распространяются под лицензией GPL v2. Остальная часть кода разработаны Станиславом Корсаковым, другими сотрудниками ООО «Нетше лаб» и распространяются на условиях коммерческой лицензии.

Если Вы обнаружили нарушение чьих-либо прав, пожалуйста, свяжитесь с нами по электронной почте info@stasoft.net.

Основная идея NETSHe

Основной идеей NETSHe является предоставление значительного функционала (зачастую отсутствующего у прямых конкурентов, либо присутствующих в более дорогих продуктах) и

управляемого через веб-интерфейс.

NETSHe является универсальным программным обеспечением, функционирующем на многих аппаратных платформах. Для всех этих платформ NETSHe реализует сходные функционал и интерфейс управления, что сокращает стоимость владения устройством.

Эффективное управление через веб-интерфейс снижает требования к квалификации владельца/обслуживающего персонала, что в свою очередь приводит к снижению стоимости сопровождения эксплуатации устройств.

Консоль или веб-интерфейс?

Безусловно, консоль дает максимальную гибкость в управлении устройством и максимальные возможности использования базового программного обеспечения. С другой стороны, консоль требует максимальной квалификации от эксплуатирующего персонала. При разработке NETSHe мы старались совместить максимальную гибкость управления устройствами, характерную для консоли, с простотой использования веб-интерфейса.

Терминология

Рассмотрим некоторые термины и понятия, которые применяются в отношении или внутри NETSHe.

Сетевые интерфейсы

Сетевой интерфейс - физическое или программное устройство, посредством которого система под управлением NETSHe связывается с другими устройствами.

(http://ru.wikipedia.org/wiki/Сетевой_интерфейс)

Примерами сетевых интерфейсов являются:

1. Ethernet-порт / Ethernet-интерфейс (http://ru.wikipedia.org/wiki/Ethernet). Внутри NETSHe обозначается как ethX, где X - число, записанное арабскими цифрами.
2. Виртуальный Ethernet-интерфейс, также VLAN-интерфейс (http://ru.wikipedia.org/wiki/VLAN). Внутри NETSHe обозначается как ethX.Y, где X и Y - числа, записанные арабскими цифрами. При этом X обозначает реальный Ethernet-порт, а Y указывает на номер VLAN (виртуальной локальной сети).
3. Алиас (или псевдоним) интерфейса. Чаще всего применяется к Ethernet-интерфейсам. Позволяет, например, назначить второй IP-адрес конкретному интерфейсу. Внутри NETSHe алиас для Ethernet-интерфейса обозначается как ethX:Y, где X и Y - числа, записанные арабскими цифрами. X обозначает реальный Ethernet-интерфейс, а Y указывает на порядковый номер алиаса / псевдонима.
4. Беспроводной интерфейс - радиомодуль, установленный в систему под управлением NETSHe. Внутри NETSHe обозначается как wlanX, где X - число, записанное арабскими цифрами. Каждому радиомодулю внутри NETSHe может быть сопоставлено до 8 сетевых

интерфейсов.

В приведенном примере Ethernet-интерфейс и беспроводной интерфейсы являются физическими устройствами и про них можно сказать, что они являются фиксированными интерфейсами (их нельзя изъять, не разобрав устройство). Очень часто к фиксированным интерфейсам применяется термин «порт».

Характерной чертой фиксированного интерфейса является MAC-адрес (http://ru.wikipedia.org/wiki/MAC-адрес)

Алиасы, виртуальные VLAN-интерфейсы и беспроводные сетевые интерфейсы являются программными реализациями поверх фиксированных интерфейсов, хотя и используют (могут использовать) в своей работе аппаратные возможности фиксированных интерфейсов.

Интерфейсы реализуемые программно, пусть даже с использованием дополнительно подключаемого оборудования вроде модемов, будем называть динамическими. Примерами таких являются интерфейсы, использующие множество протоколов типа «точка-точка» PPP, PPTP, PPPoE, L2TP и т.п. (http://ru.wikipedia.org/wiki/PPP_) Внутри NETSHe эти интерфейсы обозначаются как pppX (где X число, записанное арабскими цифрами), либо pppoe, l2tp, pptp, cellular (для упрощения восприятия и ассоциации с используемыми протоколами).

Также динамическими в NETSHe считаются туннельные интерфейсы. Внутри NETSHe туннельные интерфейсы типа IPv4-IPv4 обозначаются как tunX, туннельные интерфейсы типа IPv6-IPv4 обозначаются как tunsitX, а туннельные интерфейсы типа GRE обозначаются как tungreX (где X число, записанное арабскими цифрами). Пожалуйста, обратите внимание, что использование части «tun» в имени туннельного интерфейса обязательно.

Для интерфейсов типа «сетевой мост» (http://ru.wikipedia.org/wiki/Сетевой_мост) внутри NETSHe зарезервированы имена вида brX (где X число, записанное арабскими цифрами). Пожалуйста, обратите внимание, что использование части «br» в имени сетевого моста обязательно.

Особыми программными интерфейсами в NETSHe являются интерфейсы с именами bondX и teqlX. Такие интерфейсы служат для логического объединения существующих интерфейсов в «мега»-интерфейс с целью повышения пропускной способности и (или) резервирования каналов связи.

Loopback интерфейсы в NETSHe. В NETSHe можно создать неограниченное количество Loopback интерфейсов, имена которых должны начинаться с lo1 (lo1, lo2, lo3 и т. п.).

Также, в NETSHe имеются псевдо-интерфейсы. Например, политики для IPSec задаются аналогичным интерфейсам образом, но должны содержать в своем имени часть «ipsec».

Некоторые интерфейсы являются служебными внутри NETSHe, либо создаются автоматически. Чаще всего, подобные интерфейсы имеют часть «auto» в своем названии.

WAN, LAN, DMZ или зоны в NETSHe.

NETSHe (программное обеспечение) спроектировано с учетом концепции зон — логических групп сетевых интерфейсов, которые выполняют одинаковые функции и (или) к которым подключены сегменты вычислительной сети, требующие одинаковых правил взаимодействия (пропуска трафика и т.п.). Фиксированные сетевые интерфейсы, объединенные в зону, далее

трактуются как порты зоны. Например, порт LAN.

Управление многими сервисами внутри NETSHe построено с учетом концепции зон. Так, например, межсетевой экран работает только с настроенными зонами.

Минимальное количество настроенных зон в NETSHe — одна зона LAN. Максимальное количество зон в NETSHe не ограничено. В целях совместимости NETSHe оперирует стандартными зонами LAN, WAN и DMZ:

1. LAN — локальная сеть (http://ru.wikipedia.org/wiki/LAN).
2. WAN — внешняя по отношению к маршрутизатору сеть (http://ru.wikipedia.org/wiki/WAN).
3. DMZ — демилитаризованная зона (https://ru.wikipedia.org/wiki/DMZ_(компьютерные сети)).

Двойной доступ или Dual Access

В NETSHe не применяется термин Dual Access (двойной доступ) хотя механизм, который понимается под этим термином рядом производителей, реализован в NETSHe. Под данным термином понимается двухстадийное соединение с провайдером услуг.

Например: подключение к провайдеру через Ethernet-интерфейс с получением IP-адреса, маршрутов и т.п. через DHCP на первом этапе и подключение с использованием семейства протоколов типа «точка-точка» (PPPoE, PPTP, L2TP) на втором этапе.

Примером провайдера, использующего такое подключение, является Билайн:

1. Подключение к сети провайдера осуществляется через Ethernet-порт с выдачей провайдером клиенту IP-адреса, маршрутов, серверов имен. По завершении первой стадии подключения клиент получает доступ к локальным ресурсам провайдера и не имеет доступ в сеть Интернет.
2. На втором этапе устанавливается соединение по протоколу PPTP или L2TP с получением нового маршрута по-умолчанию, новых серверов имен и нового ip-адреса на новом интерфейсе (с именем l2tp или pptp).
3. По завершении второй стадии клиент получает доступ в сеть Интернет.

Такое двухстадийное подключение реализуется в NETSHe, как показано на примерах в документации.

Клонирование MAC-адреса

Термин «Клонирование MAC-адреса» не используется в NETSHe, хотя такой механизм реализован. Ряд провайдеров выполняет «привязку» клиента к конкретному порту своего оборудования по MAC-адресу.

Оставим за скобками суть и необходимость такой операции, которая для клиента оборачивается необходимостью выходить в сеть только с одного конкретного устройства, имеющего MAC-адрес зафиксированный провайдером, либо иметь возможность изменить MAC-адрес на своих устройствах на нужный.

NETSHe предоставляет возможность поменять MAC-адрес на произвольный на любом Ethernet-

интерфейсе устройства. При использовании данного механизма следует помнить, что кроме замены MAC-адреса на Ethernet-интерфейсе устройства, может потребоваться поменять и MAC-адрес на подключающемся к маршрутизатору устройстве (тот MAC-адрес, который клонируют).

Краткие сведения об устройстве NETSHe

NETSHe использует «срезы» SDK, ядра Linux и значительное число программных пакетов из состава OpenWRT, как основу для собственного SDK. «Срезы» производятся один-два раза в год и не привязаны к выходу версий OpenWRT. Чаще всего, NETSHe можно установить вместо OpenWRT, как и обратное - OpenWRT можно установить вместо NETSHe, используя стандартный механизм обновления / sysupgrade.

Обновление / замена NETSHe / OpenWRT могут быть произведены из веб-интерфейса NETSHe. Следует заметить, что конфигурации в процессе замены не сохраняются.

Мы не можем дать инструкций по установке / замене NETSHe и DD-WRT, NETSHe и других прошивок.

Пожалуйста, обратите внимание, что несмотря на использование значительного числа компонентов OpenWRT, NETSHe не является совместимой с OpenWRT системой, т.к.:

1. NETSHe использует измененный SDK;
2. Ряд пакетов различаются между собой (версии, примененные наборы патчей, набор компонентов, места установки);
3. В NETSHe отсутствует инфраструктура UCI/UBUS;
4. NETSHe использует ряд оригинальных пакетов, драйверов и патчей, отсутствующих в OpenWRT;
5. В NETSHe используется оригинальная система конфигурации и запуска, основанная на едином файле настроек;
6. В NETSHe присутствует собственная система событий;
7. Полностью разные веб-интерфейсы;
8. Отличаются минимальные системные требования.

Системные требования

Минимальными системными требованиями для NETSHe являются 8 Мегабайт ПЗУ (флэш-памяти) и 32 Мегабайта ОЗУ (оперативной памяти).

Рекомендуется использовать не менее 16 мегабайт ПЗУ и 64 мегабайт ОЗУ.

Поддерживаемым NETSHe является/может являться любое устройство, поддерживаемое OpenWRT и соответствующее вышеуказанным требованиям. Также, NETSHe поддерживает ряд устройств, для которых отсутствует поддержка OpenWRT. Поддержка иных устройств может быть реализована по заказу.

Требования к интернет-обозревателю на компьютере пользователя.

Для нормальной работы веб-интерфейса требуется любой современный интернет-

обозреватель с включенным приемом cookies, исполнением Java-скриптов и установленным флэш-плеером.

Установка и обновление NETSHe

Прошивки (или firmware) NETSHe поставляются в виде двоичных файлов с именами по типу NETSHe-версия-платформа.bin и NETSHe-версия-платформа-sysupgrade.bin.

Например, NETSHe-1.2-alfa-nx-sysupgrade.bin означает, что в файле находится обновление прошивки NETSHe до версии 1.2 для устройств ALFA Networks N2/N5. Данный файл можно использовать для обновления до NETSHe уже установленной на устройство прошивки NETSHe или OpenWRT.

Файл NETSHe-1.2-tl-wr1043nd.bin содержит прошивку NETSHe версии 1.2 для установки с помощью консольных утилит или из стандартной прошивки TP-Link.

Следует знать, что на все платформы поддерживают обновление прошивок через веб-интерфейс. Некоторые платформы имеют только один файл как для первоначальной прошивки, так и для обновления (NETSHe-5.3-ac4300-sysupgrade.bin).

Как правило, установка NETSHe на устройства выполняется производителем, однако иногда требуется установить/обновить встроенное ПО самостоятельно. Этот процесс зависит от моделей устройств и описан в документации к ним.

Консольный доступ к устройству.

По умолчанию, NETSHe предоставляет пользователю средства консольного доступа к устройству по протоколу ssh в случае нормального функционирования устройства и telnet в режиме восстановления после сбоя (failsafe mode).

SSH доступ может быть получен с помощью стандартных ssh-клиентов на Linux, xBSD, MacOS или с помощью PuTTY под Windows. Адрес LAN-интерфейса, логин и пароль для SSH-доступа полностью соответствует таковым для веб-интерфейса.

В режиме восстановления после сбоя предоставляется telnet-доступ без ввода имени пользователя и пароля по адресу 192.168.1.1 (на LAN порту).

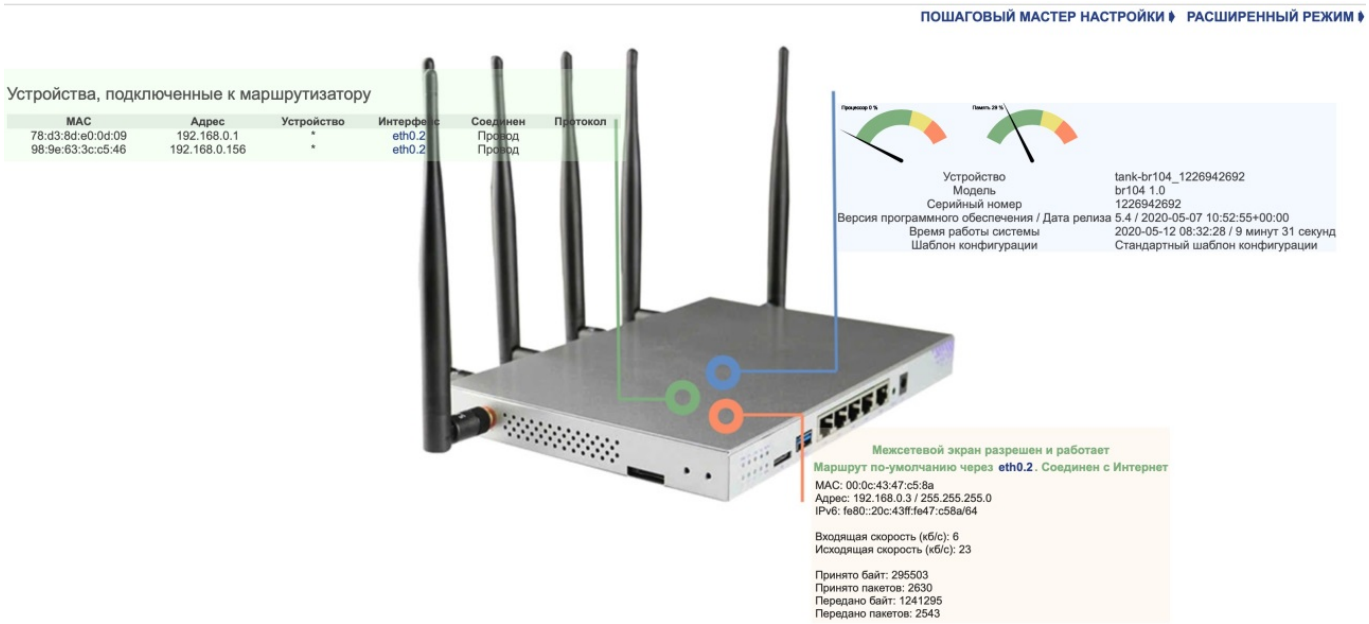
Использование веб-интерфейса

По умолчанию веб-доступ к устройствам открыт по SSL (TCP 443) со стороны LAN, однако средствами NETSHe можно изменять и номер TCP-порта, и интерфейсы привязки. Веб-интерфейс (WebUI) является полноценным и достаточным средством управления, включающем полный набор инструментов для всех задач управления. Если устройство находится под управлением NMMS (Network Management and Monitoring Server), то в качестве порта привязки как правило устанавливается TCP 5556. При этом с NMMS доступны WebUI всех контролируемых устройств и их консоли.

Общая компоновка веб-интерфейса

Веб-интерфейс может быть изменен по заказу, при этом общая компоновка предусматривает следующие элементы:

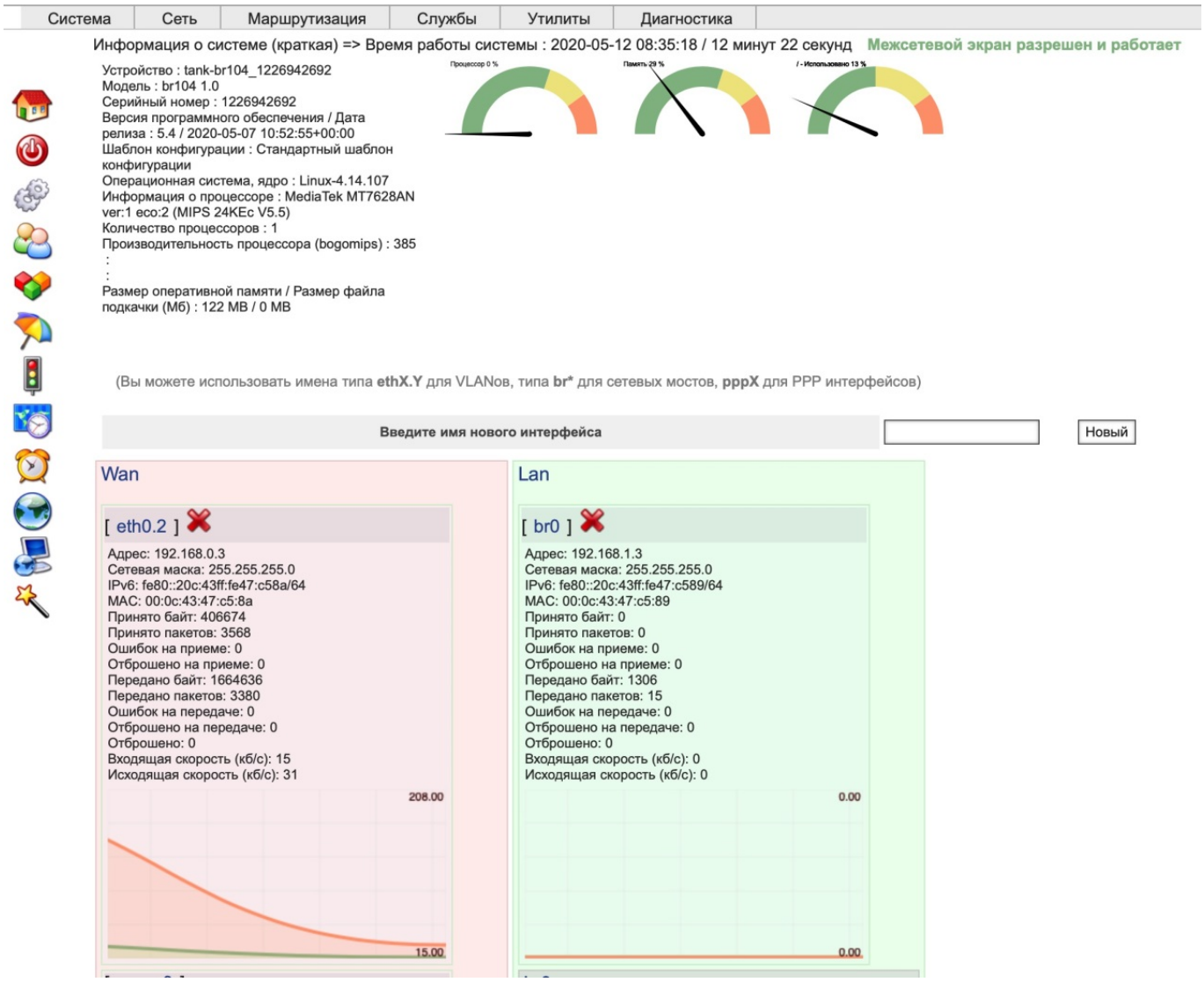
1. В верхней части страницы может располагаться главное меню и логотип компании, при нажатии на который Вы будете перенаправлены на ее сайт.
2. Главное меню является выпадающим и отделяет собственно рабочую часть страницы (область ввода/вывода информации от ее верхней части). В главном меню присутствуют все функции системы в сгруппированном виде, состав их может меняться в зависимости от модели или проекта.
3. Ниже главного меню может присутствовать так называемая панель инструментов, которая может содержать кнопки вызова функций, типичных для материала или задачи в рабочей части страницы. Например «Новый», «Остановить сервис», «Поиск» и т. п.
4. После изменения каких-либо параметров в рабочей части страницы следует сохранить изменения нажатием на кнопку «Сохранить». Часто на рабочей части присутствует опция «Перезапустить службы после сохранения», при ее нажатии вместе с «Сохранить» соответствующие службы будут перезапущены.
5. В веб-интерфейсе применяются типизированные иконки для обозначения сходных задач. Так иконка  применяется для обозначения действий типа «Добавить новую запись/свойство». Иконка в виде  обозначает действия по удалению чего-либо/остановке службы/приложения. Иконка в виде  обозначает операцию редактирования. Иконка в виде  обозначает перезапуск чего-либо/обновление содержимого.



При разработке системы мы стремились дать Вам современный и элегантный инструмент, максимально оперативно и в наиболее удобной форме представляющий данные о системе и событиях, происходящих в ней.

В частности, на странице «Информация о системе» (она же стартовая страница) мы в графике и режиме близком к онлайн отрисовываем загрузку процессора и памяти, разделов устройства, а также выводим информацию о ядре системы, типе процессора его производительности,

установленных контроллерах. На стартовой странице расширенного режима в виде графиков выводится информация о загрузке сетевых интерфейсов и параметрах радио интерфейсов.



Мастер настройки

Как и многие производители NETSHe включила в систему мастер настройки, который запускается при первом подключении к WebUI устройства. Шаги мастера реализуют минимально необходимые действия по стартовой настройке устройства. Однако мастер можно так же запустить в любое время с панели инструментов, в этом случае шаги мастера уже будут заполнены действующими параметрами.

Отличия документации от фактического состояния прошивки.

NETSHe — динамично развивающееся программное обеспечение, в которое постоянно вносятся изменения и улучшения. Мы стараемся поддерживать актуальным состояние документации, однако не считаем значительной проблемой некоторое несоответствие изображений в документации фактическому виду веб-интерфейса.

Например, могут не соответствовать темы оформления веб-интерфейса, некоторые служебные

изображения и сообщения, немного по-разному сгруппированы поля ввода, добавлены / удалены некоторые поля ввода / пункты меню.

Сообщить об ошибке

Создатели NETSHe - люди и, значит, имеют право на ошибки.

Мы будет очень благодарны Вам за любые сообщения об ошибках, которые Вы можете разместить в соответствующем разделе сайта сообщества (http://netshe-lab.ru) или просто послав нам по электронной почте на адрес info@netshe-lab.ru.

В сообщении, пожалуйста, постарайтесь как можно подробнее описать:
Когда и при каких обстоятельствах возникла ошибка?

Как она проявляется?

Что предшествовало появлению ошибки?

Если ошибка проявляется в веб-интерфейсе - сделайте скриншот и приложите его к сообщению.

Многие модели и реализации NETSHe имеют возможность генерации отчета разработчикам через соответствующий пункт меню веб-интерфейса. Кроме того, если Вы - опытный пользователь, то приложите, по-возможности, файлы /var/log/messages, /etc/.ssxapp/main.conf и вывод команды dmesg из консоли устройств.

www.netshe-lab.ru	(+7 4852) 90-89-30	Info@netshe-lab.ru