# Универсальное программное обеспечение для сетевых устройств NETSHe.

Руководство пользователя

Часть 1. Введение и основные функции

Станислав Корсаков, ООО «Нетше лаб»



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 встраиваемых систем, таких как сетевые устройства (маршрутизаторы, точки доступа), телевизионные приставки, сетевые хранилища и т. п., программное которых построено на базе операционных систем Линукс (OpenWRT или Debian) и NetBSD. Программное обеспечение включает в себя:

- подсистему хранения конфигурации системы/устройства;
- подсистему инициализации (стартовые скрипты);
- веб-интерфейс управления устройством.

## Использованное программное обеспечение и права

Используется Yahoo User Interface library (http://yui.uahoo.com). Библиотека имеет BSD лицензию.

Используется некоторый код из проекта m0n0wall. Код распространяется под BSD лицензией.

Используется некоторый код из проекта pfsense и от Scott Ulrich. Код распространяется под BSD лицензией.

Используется некоторый код из проекта phpsysinfo, распространяемый под лицензией GPL v2.

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.

Используемые изображения из набора Nuvola распространяются под лицензией LGPL v2.1. Автор - David Vignoni (david@icon-king.com).

Иная графика имеет своих авторов и распространяется в соответствии с их лицензиями.

Иной код и изображения разработаны Станиславом Корсаковым, другими сотрудниками ООО «Нетше лаб» и распространяются под лицензией GPL v2.

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, управляемого через веб-интерфейс. Эффективное управление через веб-интерфейс снижает требования к квалификации владельца/обслуживающего персонала, что в свою очередь приводит к снижению стоимости владения устройством.

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

Привнесение функционала, отсутствующего в аналогах, также является существенной идеей NETSHe.

### 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/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_...)

Примерами сетевых интерфейсов являются:

Ethernet-порт / Ethernet-интерфейс (http://ru.wikipedia.org/wiki/Ethernet). Внутри NETSHe обозначается как ethX (где X - число, записанное арабскими цифрами).

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). X обозначает реальный Ethernet-порт. Y указывает на номер VLAN (виртуальной локальной сети).

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. Y указывает на порядковый номер алиаса / псевдонима.

Беспроводной интерфейс - радиомодуль, установленный в систему под управлением NETSHe. Внутри NETSHe обозначается как wlanX (где X - число, записанное арабскими цифрами).

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».

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

Характерной чертой фиксированного интерфейса является MAC-адрес (http://ru.wikipedia.org/wiki/MAC-%D0%B0%D0%B4%D1%80%D0%B5%D1%81)

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_(%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB)

)
Внутри NETSHe эти интерфейсы обозначаются как pppX (где X число,

записанное арабскими цифрами).

Также динамическими интерфейсами в NETSHe считаются туннельные интерфейсы.

Внутри NETSHe туннельные интерфейсы типа IPv4-IPv4 обозначаются как tunX, туннельные интерфейсы типа IPv6-IPv4 обозначаются как sitX, а туннельные интерфейсы типа GRE обозначаются как greX (где X число, записанное арабскими цифрами).

Для интерфейсов типа "сетевой мост" (http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_...) внутри NETSHe зарезервированы имена вида brX (где X число, записанное арабскими цифрами).

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.

## WAN, LAN и 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:

- LAN — локальная сеть (http://ru.wikipedia.org/wiki/LAN).
- WAN — внешняя по отношению к маршрутизатору сеть (http://ru.wikipedia.org/wiki/WAN).
- DMZ — демилитаризованная зона (http://ru.wikipedia.org/wiki/DMZ_%28%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8%29).

## 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:

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

Примером провайдера, использующего такое подключение, является Билайн.
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.

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 pppX). 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, следует поменять и MAC-адрес на подключающемся к маршрутизатору устройстве (тот MAC-адрес, который клонируют).

## Краткие сведения об устройстве NETSHe

NETSHe основывается на срезе Backfire или срезе разрабатываемой версии Linux-дистрибутива для сетевых устройств OpenWRT (http://www.openwrt.org) с добавлением некоторых уникальных (в частности, веб-интерфейс NETSHe) программных пакетов и модификацией ряда пакетов.

Верно, что NETSHe можно установить вместо OpenWRT, как и обратно - OpenWRT можно установить вместо NETSHe, используя стандартный механизм обновления / sysupgrade.

Обновление / замена NETSHe / OpenWRT легко могут быть произведены в веб-интерфейсе NETSHe.

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

В общем случае мы можем отослать Вас к материалам сайта OpenWRT в поисках информации о возврате на оригинальные прошивки после установки NETSHe (http://wiki.openwrt.org/toh/start).

Следует заметить, что NETSHe не является полностью совместимой с OpenWRT.

- В NETSHe используется собственная система конфигурации и запуска, основанная на едином файле настроек.
- Ряд пакетов в NETSHe и OpenWRT устанавливаются в разные места.
- Ряд пакетов различаются между собой.
- Отсутствуют/присутствуют некоторые файлы/пакеты.
- В NETSHe отсутствует система настройки UCI.
- Отличаются минимальные системные требования

Для получения более полной информации Вы можете обратиться к NETSHe-SDK.

## Системные требования

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

Поддерживаемым NETSHe является/может являться любое устройство, поддерживаемое OpenWRT и соответствующее вышеуказанным требованиям.
Поддержка иных устройств может быть реализована по заказу.

## 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, например Alix. Также некоторые платформы имеют только один файл как для первоначальной прошивки, так и для обновления. Например, ASUS WL-500g Premium (NETSHe-1.2-brcm47xx.trx).

Рассмотрим установку NETSHe на устройства в примерах.

Установка NETSHe на устройство с предустановленной стандартной прошивкой от производителя. Для ASUS WL-500g Premium и TP-Link TL-WR1043ND воспользуемся функцией стандартного веб-интерфейса по обновлению прошивки и используем файл типа NETSHe-0.8.0-brcm47xx.trx, в первом случае, и NETSHe-0.8.0-tl-wr1043nd.bin во втором. Аналогичные файлы нужно использовать при прошивке устройств методами, использующими консоль и и(или) tftp-сервер.

http://wiki.openwrt.org/toh/tp-link/tl-wr1043nd#installation
http://wiki.openwrt.org/toh/asus/wl500gp#oem.installation.using.the.tftp...
http://wiki.openwrt.org/toh/ubiquiti/routerstation#installing.a.new.firm...

Установка NETSHe на устройства с установленной OpenWRT. Начиная с версии 0.8.0 NETSHe полностью совместима с OpenWRT в плане процедуры обновления прошивки (sysupgrade). Поэтому для установки следует использовать образ, имеющий в названии часть sysupgrade (например, NETSHe-0.8.0-tl-wr1043nd-sysupgrade.bin) и использовать стандартные функции веб-интерфейса для обновления прошивки (либо использовать команду sysupgrade из консоли).

Обратите внимание, что для обновления прошивок на устройствах ASUS WL-500g Premium следует использовать файл типа NETSHe-0.8.0-brcm47xx.trx

Следует заметить, что установка или обновление NETSHe вызовет двойную перезагрузку устройства и занимает от 3-х до 5-ти минут.

Ни при каких условиях не выключайте устройство, не вынимайте и не вставляйте какие-либо кабели до завершения процесса обновления / перепрошивки.

## Пример установки прошивки в устройство Ubiquiti RouterStation, Ubiquiti RouterStation Pro.

Для установки новой прошивки в RouterStation нам потребуется персональный компьютер с операционной системой имеющей tftp-клиент. Возьмем для примера, ОС Линукс и tftp-клиент *atftp*.

Включим RouterStation удерживая сервисную кнопку нажатой. Устройство перешло в режим загрузчика RedBoot, выставило на порту eth0 (порт POE) адрес 192.168.1.20 с маской 255.255.255.0 и ожидает загрузки нового образа прошивки по протоколу tftp.

Убедимся, что наш компьютер включен в ту же сеть, что и устройство. Установим нужный нам адрес на сетевом интерфейсе компьютера (Например, *ifconfig eth0:1 inet 192.168.1.1 netmask 255.255.255.0 up*) и запустим *atftp*.

Из командной строки atftp вводим:

verbose

trace

connect 192.168.1.20

put Путь_к_файлу_прошивки/Имя_файла_прошивки

и наблюдаем процесс передачи прошивки в устройство.

По завершении процесса даем загрузчику установить новую прошивку (это занимает от 3-х до 5-ти минут). В процессе установки ни в коем случае не выключайте устройство! В случае, если по какой-то причине в процессе установки произошло отключение питания, следует начать процесс заново.

Установка прошивки завершается автоматической перезагрузкой устройства. Получение управления со стороны NETSHe над устройством завершается второй перезагрузкой устройства.

После нормального завершения загрузки новой прошивки устройство становится доступно по адресу 192.168.1.1. SSH-доступ на порту 22, веб-интерфейс на порту 5556.

Следует помнить, что после установки новой прошивки работоспособной является учетная запись *root* с паролем *root*

Отличия материалов данного руководства 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.

Требования к интернет-обозревателю на компьютере пользователя.

Для нормальной работы веб-интерфейса требуется любой современный интернет-обозреватель с включенным приемом кук, исполнением яваскриптов и установленным флэшплеером.

## Консольный доступ к устройству.

По умолчанию, NETSHe предоставляет пользователю средства консольного доступа к устройству — 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).

## В процессе настройки я сломал маршрутизатор или режим восстановления после сбоя.

Что делать, если в процессе настройки Вы утратили связь с маршрутизатором, он перестал нормально работать, Вы не можете войти в консоль и веб-интерфейс?

В таком случае стоит воспользоваться режимом восстановления после сбоя. Режим восстановления после сбоя доступен для всех платформ, на которых работает NETSHe при условии наличия у устройства кнопки или микропереключателя reset.

Для входа в режим восстановления после сбоя следует выключить маршрутизатор, включить его и периодически кратковременно нажимать на кнопку reset.

Переключение маршрутизатора в режим восстановления сигнализируется по быстрому миганию светодиода питания и (или) по ответу маршрутизатора на пинг по адресу 192.168.1.1 при подключении кабеля к LAN-порту.

После переключения устройства в режим восстановления следует подключиться телнетом по адресу 192.168.1.1 и в консоли устройства дать команду firstboot.

После завершения команды firstboot и перезагрузки устройства (возможно двукратного) вы получите устройство, аналогичное только что прошитому и имеющего заводские настройки.

## Сообщить об ошибке

Создатели NETSHe - люди и, значит, имеют право на ошибки. Даже на несколько :)

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

Кроме того, если Вы - опытный пользователь, то приложите, по-возможности, файлы /var/log/messages, /etc/.ssxapp/main.conf и вывод команды dmesg из консоли устройства.

# ОСНОВНЫЕ ФУНКЦИИ NETSHe

NETSHe в вариантах для OpenWRT и Debian реализует следующий набор функций:

- Управление сетевыми интерфейсами (в том числе динамическими, туннельными и радио);
- Виртуальные интерфейсы и алиасы;
- Управление маршрутизацией (в том числе статической, на основе правил, динамической (RIP, OSPF, BGP);
- Межсетевой экран с поддержкой зон;
- Сетевой мост;
- Объединение интерфейсов;
- Управление качеством обслуживания и приоритизацией исходящего трафика;
- 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;
- Фильтрация Ethernet-фреймов;
- Расширенное управление радио-интерфейсами с поддержкой режимов клиента, базовой станции и репитера, в том числе с режимами шифрования WEP и авторизации WPA-PSK, WPA-EAP, 802.11X;
- Сервер доступа с поддержкой протоколов PPTP, PPPoE, L2TP с авторизацией на внешнем радиус-сервере;
- Концентратор для частных выделенных сетей (VPN) на протоколах PPTP и L2TP с поддержкой IPSEC (в связке L2TP/IPSEC) и OpenVPN;
- Хот-спот контроллер с выделением адресов клиентам, авторизацией на внешнем UAM-сервере, управлением пропускной способностью и управляемым доступом к сайтам;
- 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);
- Сервер и клиент службы времени. При этом сервер интегрирован с сервером DHCP;

- HTTP-прокси с возможностью использования вышестоящего прокси-сервера (каскадирование);
- Управление программным обеспечением устройства. Возможность удаления установленных программных пакетов, установки новых, подключения новых репозиториев;
- Управление пользователями устройства с разделением уровней доступа через веб-интерфейс (полный или только для чтения);
- Управление внешними накопителями и разделами с возможностью подключения внешних накопителей с пользовательскими разделами, разделами физической памяти (своп) и т.п.;
- Мониторинг состояния системы (памяти/процессора/сетевых интерфейсов и т. п.) в режиме реального времени с наглядным отображением в виде графиков;
- Мониторинг состояния системы через SNMP протокол (сетевые интерфейсы и физические разделы);
- Резервное копирование любых каталогов устройства на внешние устройства/фтп-сервер и т. п.;
- Восстановление каталогов и файлов устройства из ранее сохраненных образов;
- Сохранение и восстановление файлов конфигурации. Сброс конфигурации в умалчиваемую;
- Обновление прошивки устройства;
- Захват и анализ сетевого трафика, проходящего через устройство;
- Утилиты проверки доступности хостов и маршрутов к ним (ping, traceroute);
- Останов и перезагрузка системы;