NETSHe for OpenWRT

User Manual

Unit 1. Introduction and main features

Stanislav Korsakov

Yaroslavl

Contents

Introduction to NETSHe

The unit deals with main features and functions of NETSHe, its system requirements, ways and methods of its installation.

NETSHe is a set of software for embedded systems, such as network devices (routers, access points), set-top boxes, network storages and other Linux- (OpenWRT or Debian) and NetBSD –based systems. Software includes the following features:

- configuration storage subsystem
- pre-installed software and its own initialization subsystem (start-up scripts).
- management Web Interface

Credits

Main idea of NETSHe

The main idea of NETSHe is to provide a user with a considerable number of functions managed through web interface. Effective web-interface management reduces requirements to the user`s qualifications, which subsequently results in reducing the total cost of ownership.

NETSHe is general-purpose software functioning on numerous hardware platforms. For all these platforms NETSHe provides a general-purpose functional and a general management interface, that also reduces total cost of ownership.

Introduction of the functional which is not available in the analogs is another substantial contribution of NETSHe.

Console or Wb-Interface?

Undoubtedly, console provides maximum flexibility in software management and maximum opportunities for the users of basic software.

On the other hand, console requires the highest level of users` qualification.

When developing NETSHe, we did our best to combine maximum flexibility of the software management, which is typical for console, with user-friendly character of web-interface.

Glossary

Some terms and notions related to NETSHe are considered below.

Network interfaces

Network interface is a hardware or a software device enabling a NETSHe-managed system to connect with other systems.

(http://en.wikipedia.org/wiki/Network_interface_controller)

Examples of network interfaces are the following:

Ethernet-port / Ethernet-interface (http://en.wikipedia.org/wiki/Ethernet), figured as ethX in NETSHe(X is a number written in Arabic numerals)

Virtual Ethernet-Interface and VLAN-interface (http://en.wikipedia.org/wiki/VLAN), figured as ethX.Y in NETSHe(X and Y are numbers written in Arabic numerals). X is a real Ethernet-port. Y indicates the number of VLAN (Virtual Local Area Network).

Alias (or nickname) of interface mainly refers to Ethernet-Interfaces. It enables the user to assign the second IP-address to the particular interface. Within NETSHe alias for Ethernet is ethX:Y(X and Y are numbers written in Arabic numerals). X is a real Ethernet-interface. Y indicates the ordinal number of alias/nickname.

Wireless Interface is a radio-module installed into NETSHe-managed system. Within NETSHe it is wlanX (X is a number written in Arabic numerals).

The above-mentioned Ethernet-Interface and wireless Interface are devices that can be referred to as fixed interfaces (they can not be removed unless the device is dismantled).

Such fixed interfaces are often referred to as “ports”.

Aliases and virtual VLAN-interfaces are software implementations based on fixed interfaces, although they (can) use hardware resources of fixed interfaces.

Distinctive feature of the fixed interface is MAC-address(http://en.wikipedia.org/wiki/MAC_address)

Interfaces based on software even with the use of external devices like modems are referred to as dynamic.

These interfaces use numerous protocols like “point-to-point”, PPP, PPTP, PPPoE, L2TP, etc. (http://en.wikipedia.org/wiki/Point-to-Point_Protocol)

Within NETSHe these interfaces are indicated as pppX (X is a number written in Arabic numerals).

Dynamic interfaces in NETSHe also include tunnel interfaces.

Whithin NETSHe tunnel interfaces IPv4-IPv4 are indicated as tunX, tunnel interfaces IPv6-IPv4 are indicated as sitX, and tunnel interfaces GRE are indicated as greX (X is a number written in Arabic numerals).

For “a network bridge”-type of interfaces(http://en.wikipedia.org/wiki/Network_bridge) within NETSHe there are names like brX(X is a number written in Arabic numerals).

Special software interfaces in NETSHe are those named bondX and teqIX. Such interfaces are aimed at logical aggregation of existing interfaces into a single “mega”-interface in order to improve bandwidth management and/or backup of links.

WAN,LAN and DMS or zones in NETSHe

NETSHe (software) is designed taking into account conceptions of zones – logical groups

of network interfaces performing the same functions and/or connected to the segments of computer network demanding the same rules of interaction (e.g. traffic procession).

Fixed network interfaces integrated into a zone are further referred to as zone ports, e.g. LAN-port.

Management of many services within NETSHe is based on considering the concept of zones. E.g., a firewall functions only when the zones are setuped.

The minimum number of setuped zones in NETSHe is a single LAN-zone. The total number of zones is unlimited.

With the aim of compatibility NETSHe operates standard zones:LAN, WAN and DMZ.

LAN- an internal network (http://en.wikipedia.org/wiki/LAN)

WAN- an external towards the router network (http://en.wikipedia.org/wiki/Wide_area_network)

DMZ – a demilitarized zone (http://en.wikipedia.org/wiki/DMZ_%28computing%29).

Dual Access

The term dual access is not used in NETSHe, although the mechanism, which is meant by it by some manufacturers, is implemented in NETSHe

Dual access means a two-staged connection with the Internet service provider (uplink):

- connection to the provider through Ethernet-interface to assign an IP-address, routes, etc. with DHCP or with static settings.
- connection with the use of the protocol group like “point-to-point”, (PPPoE, PPTP, L2TP) on the second stage

Connection to the provider network is carried out through Ethernet-port ; an IP-address, routes, name servers are assigned to the client by the provider. Upon completion of the first stage of connection a client gets access to the internal resources of the provider, but not to the Internet.

On the second stage the connection through PPTP or L2TP protocols is established with the assignment of a new default route, new name servers and a new IP-address on the new interface (named pppX). Upon completion of the second stage a client obtains access to the Internet. This two-staged connection is implemented in NETSHe, as shown in the documentation examples.

MAC-address Cloning

The term “MAC-address Cloning” is not used in NETSHe, although this mechanism is implemented.

Some providers “fix” client to a specific port of their hardware according to MAC-address.

The essence and necessity of this operation are left aside, although it means that client is made to access the network from the only specific device with a MAC-address fixed by provider or to be able to change MAC-address on their hardware for the necessary one.

NETSHe offers an opportunity to change MAC-address for unconditioned on any Ethernet- and wireless- interface of the device.

While using this mechanism you should remember that besides the change of MAC-address on the Ethernet-interface of the device it is necessary to change MAC-address on the device connected to the router (Mac-address that is cloned).

NETSHe layout in brief

NETSHe is based on the snapshot of Backfire or on the development version of LINUX-distributive for network devices OpenWRT (http://www.openwrt.org) with the addition of some specific software packages (NETSHe web-interface, in particular) and modifications of some packages.

It is true that NETSHe can be installed instead of OpenWRT, vice versa OpenWRT can be installed instead of NETSHe using sysupgrade.

Upgrading/Replacement of NETSHe/OpenWRT can be easily performed in NETSHe web-interface.

We cannot give any instructions on installation/replacement of NETSHe and DD-WRT and other firmwares. For further information about return to the original firmware after installation of NETSHe you can refer to OpenWRT site. (http://wiki.openwrt.org/toh/start)

It should be noted that NETSHe is not completely compatible with OpenWRT:

- NETSHe uses its own system of configuration and starting based on a single configuration file.
- Some software packages in NETSHe and OpenWRT are installed in different places.
- Some software packages differ from each other.
- Some files/packages are (un)available.
- UCI configuration system is not available in NETSHe.
- Basic system requirements are different.

For more detailed information you can refer to NETSHe-SDK.

System requirements.

Basic system requirements for NETSHe are 8mgb flash-memory and 32 mgb RAM.

Any device supported by OpenWRT and up to above-mentioned requirements is/ can be supported by NETSHe. Support of other devices can be given by a special order.

NETSHe installation and upgrading

NETSHe firmware is delivered in the form of binary files named similar to NETSHe-version-platform.bin and NETSHe-version-platform- sysupgrade.bin.

E.g., NETSHe-1.2-alfa-nx-sysupgrade.bin means that the file contains NETSHe firmware image for upgrading the existing NETSHe or OpenWRT firmware up to 1.2 version for ALFA Networks N2/N5 devices.

File NETSHe-1.2-tl-wr1043nd.bin should be used to install NETSHe 1.2 version via console tools or from stock firmware web-interface of TP-Link.

Not all hardware devices can upgrade firmware via web-interface, e.g. Alix.

Some hardware devices have a single image both for initial flash and for upgrading, e.g. ASUS WL-500g Premium (a single image file NETSHe-1.2-brcm47xx.trx).

The following examples illustrate NETSHe installation.

NETSHe installation to replace stock firmware.

Use standard web-interface option for ASUS WL-500g Premium and TP-Link TL-WR1043ND devices to upgrade firmware.

Specify NETSHe-0.8.0-brcm47xx.trx file in first case and NETSHe-0.8.0-tl-wr1043nd.bin file in the latter.

Use the same files to flash devices via console tools and (or) tftp-server.

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...

Installation of NETSHe on OpenWRT-based devices.

'Sysupgrade' function of OpenWRT can be used to upgrade the device from OpenWRT to NETSHe 0.8 version and up.

OpenWRT can be installed instead of NETSHe from 0.8 version and up via standard web-interface of NETSHe. Use the image file of OpenWRT containing the word 'sysupgrade' in its name.

To upgrade firmware in devices such as ASUS WL-500g Premium you should use files which does not contain the word 'sysupgrade' in their names.

It should be noted that, installation or upgrading of NETSHe results in double system reboot and takes 3-5 minutes.

Under no circumstances should the device be powered off, plugged off or connected to any cables until the flash process is finished.

Firmware Flashing for Ubiquiti RouterStation, Ubiquiti RouterStation Pro.

To flash new firmware into the RouterStation you would require a PC with tftp-client.

Example for OS Linux with atftp.

Power on RouterStation with pressed service button. The device goes in RedBoot bootloader mode, assigns 192.168.1.20 with network mask 255.255.255.0 to eth0 (POE port) and waits for tftp connection to receive new firmware image.

Make sure you PC is connected to the same network as the device. Assign an IP-address from the same network to the network interface of your PC (e. g. ifconfig eth0:1 inet 192.168.1.1 netmask 255.255.255.0 up) and launch atftp.

From atftp-shell type in:

verbose

trace

connect 192.168.1.20

put Path_to_firmware_file_image/Firmware_file_name

Monitor firmware flashing process, which takes 3 to 5 minutes. Do not power of the device! In the event of any unexpected power cut-off during firmware flashing, start the whole process again from the beginning.

Firmware flashing ends up with automatic device re-boot. Wait for the second automatic device reboot, which will enable NETSHe to gain control over the system.

If firmware flashing is performed successfully, the device becomes accessible at 192.168.1.1. SSH-access at port 22, web interface at port 5556.

After new firmware flashing the system has only one account with login “root” and password “root”.

This user manual materials can differ from the actual state of flash firmware.

NETSHe is dynamically developing software which is constantly being developed and improved

We make efforts to update our documentation, however, we do not consider some discrepancy of images in documentation and actual web-interface design as a problem.

E.g.,web-interface design patterns, utility images and messages can differ, location of fields for typing in can vary, some fields for typing in/menu items can be added/deleted

Requirements to the Internet-browser on the user`s PC.

Normal operation of web-interface requires any up-to-date Internet-browser and execution of javascripts, cookies and flash-player are to be enabled in your browser.

Console Access to the device

By default NETSHe provides a user with means of console access to the device— ssh as long as the device and telnet function normally in failsafe mode.

SSH-access can be obtained with the help of standard Linux, xBSD, MacOS ssh-clients or Windows-based PuTTY.

LAN-interface address, login and password for SSH-access are identical to those for web-interface.

In failsafe mode telnet-access is provided without the input of the user name and password at the address 192.168.1.1 (on LAN-port).

What should I do if I have bricked a router?

In case you have lost the connection with the router during setup, it fails to work properly and you are unable to enter console and web-interface, you should use failsafe mode. Failsafe mode is available for all NETSHe platforms as long as the device has a reset button or a micro-switch.

To enter a failsafe mode you should power off the router, then power it on and periodically momentary press the reset button.

Switchover of the router into failsafe mode is indicated by fast LED blinking and/or according to the response of the router to ping at the address 192.168.1.1 when the cable is connected to LAN-port.

After switchover of the device into failsafe mode telnet should be connected at the address 192.168.1.1 and enter 'firstboot' command for the device console.

After 'firstboot' command is performed and the device is rebooted (maybe, twice) you get a device identical to the one with just flashed firmware and factory-made settings.

How to inform us about the bug in firmware?

NETSHe has been developed by people, consequently, it has a right to mistake, even some mistakes. We will be very grateful to you for any error reports, which can be send to a relevant section of the site (http://unity.stasoft.net) or to our e-mail address info@stasoft.net. We will appreciate a detailed description of the error circumstances, its demonstration and your prior steps.

If the error shows up in web-interface, please, make a screenshot and attach it to your message. If you are an experienced user , please attach the files/var/log/messages, /etc/.ssxapp/main.conf and 'dmesg' command output from device console.

MAIN FEATURES OF NETSHe

NETSHe for OpenWRT and Debian has the following features:

- Network interface management (including dynamic, tunnel and wireless)
- VLAN's and aliases;

- Advanced routing (static, multipath, rule-based, RIP, OSPF, BGP);
- Zone based firewall;
- Bridges with brouter and filtering capability;
- Interface bonding;
- Quality of Service, bandwidth management, traffic shaping, rate control and traffic prioritization;
- L7 based (application patterns based) IP-traffic filtering and marking;
- Extended management of wireless interfaces; Access Point, Ad-Hoc, Client and Repeater mode with (or without) variable WEP encryption modes, WPA-PSK, WPA2-PSK, WPA-EAP, WPA2-EAP, 802.11X authorization and key management;
- Access concentrator for variable VPN's (PPTP, L2TP and OpenVPN);
- IPSEC support for L2TP VPN solution;
- PPPoE access concentrator;
- Hot-spot controller with external UAM-authorization; walled garden and bandwidth management;
- Authorization and accounting through external radius-server;
- Built-in IP-address assignment or assignment through external radius-server;
- DHCP server with flexible rules; dynamic IP-address assignment; static IP-address assignment; configurable black-list mode for DHCP requests from specified MAC's;
- DHCP relay;
- Network time synchronization server and client. Server integration with DHCP server.
- Built-in HTTP proxy with ability to use upstream proxy;
- Full software management; support of external software repositories; software installation and deletion;
- User management; two levels of user access: full and read-only;
- External storage management; SWAP control;
- System monitoring; chart graphing in a near real-time mode;
- System monitoring through SNMP v2 protocol;
- Configurable system backup; backup images can be moved to external devices and/or network shares;
- Files and folders restoration;
- Backup and restoration of configurations;
- Firmware flashing;
- Traffic capture and analysis;
- System halt and reboot;
- Some helpful utilities.