

OpenWRT mit Raspberry Pi

Agenda

- Wieso, weshalb, warum?
- Ausgangslage
- Ziel
- Lösungssuche
- Lösungsansatz
- Umsetzung - Einrichtung OpenWRT auf Raspberry Pi 3B

Wieso, weshalb, warum?

- Internetserviceprovider hat Zugriff auf von ihm gestellten Router. Auch auf das lokale Netzwerk dahinter?
- Weiternutzung eines alten Routers, der keine Firmwareupdates mehr bekommt.

Ausgangslage

- ISDN-Anschluss.
- Router läuft nur, wenn Gerät benötigt wird.
- Reines LAN.

Ziel

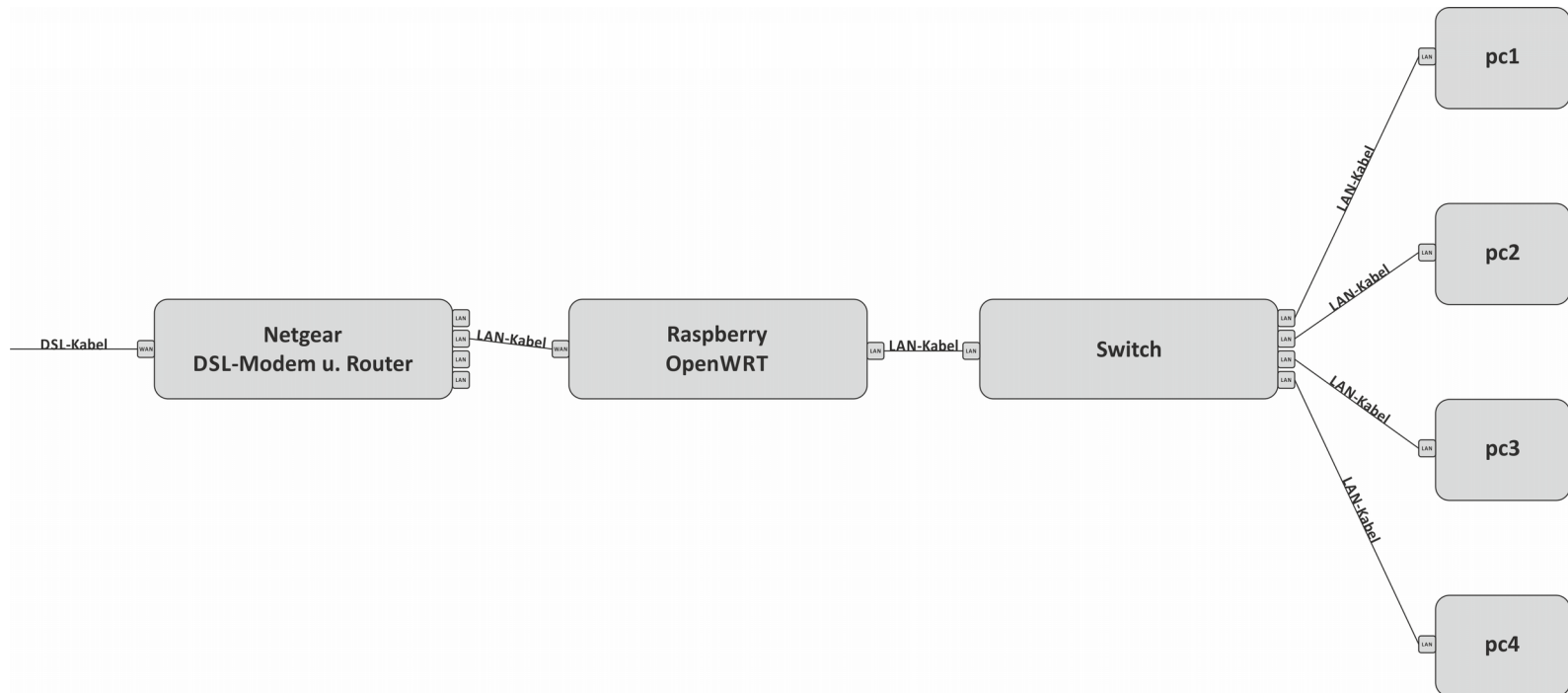
- Mehr Sicherheit.
- Weiternutzung bestehender Ressourcen, soweit möglich.
- Open Source.
- Raspi ausprobieren.

Lösungssuche

- Günters Vortrag zu OpenWRT 2013
 - <http://www.pc-treff-bb.de/Vortraege/openwrt.pdf>
- Recherche Internet
 - <https://openwrt.org> (kein passendes Image)
 - <https://lede-project.org> (Fork, passendes Image)
- Raspberry Pi Workshop 2017

Lösungsansatz

- Einrichtung eines Netzwerkes im Netzwerk, durch zwei, mittels **LAN-zu-WAN-**Verbindung, hintereinandergeschaltete (**kaskadierte**) Router.



Umsetzung (1) – Was wird benötigt?

- Linuxrechner
- Raspberry Pi 3B + Netzteil
- USB-Netzwerkadapter (**Achtung!** Passender Treiber vorhanden?)
 - <https://lede-project.org/packages/index/kernel-modules---usb-support>
- microSD
- USB-Adapter für microSD
- Eingangs(WLAN)router mit integriertem DSL-Modem
- Switch
- LAN-Kabel (mind. 3)
- passendes OpenWRT-Image
 - https://lede-project.org/toh/start?dataflt%5BBrand*%7E%5D=raspberry
 - https://wiki.openwrt.org/toh/start?dataflt%5BBrand*%7E%5D=raspberry
- Internetverbindung

Umsetzung (2) – OpenWRT auf SD-Karte flashen

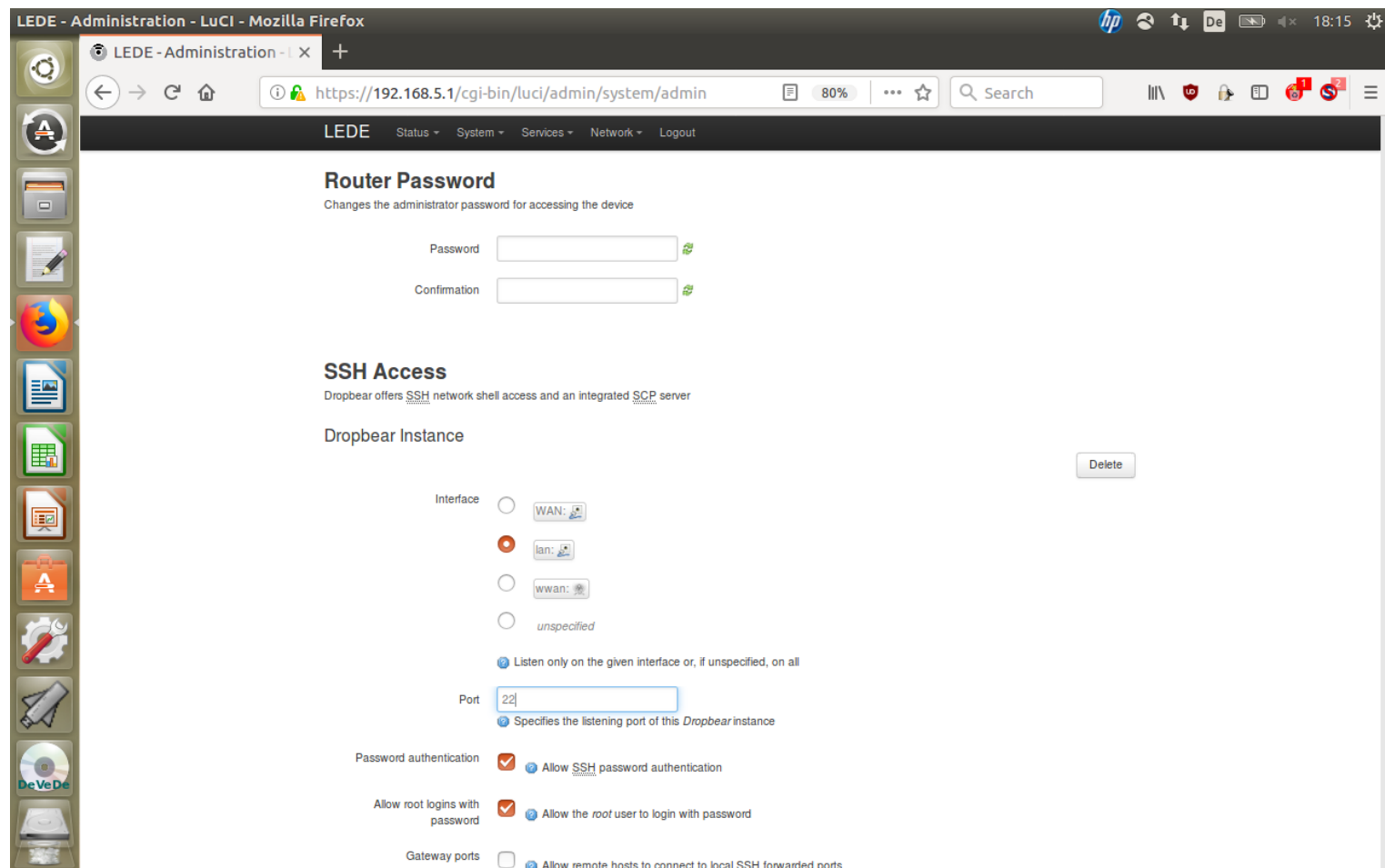
- Linuxrechner + USB-Adapter für microSD + microSD + passendes Image
- Terminalbefehl: `sudo fdisk -l` (Output sdX merken)
- Terminalbefehl: `sudo dd if=/Pfad/zur/Datei/lede-17.01.4-brcm2708-bcm2710-rpi-3-ext4-sdcard.img of=/dev/sdX bs=2M conv=fsync`

Umsetzung (3) – Erster Zugriff auf OpenWRT

- microSD in Raspi stecken, Netzteil anschließen, LAN-Kabel in Raspis RJ45-Buchse stöpseln, das andere Ende in den PC
- 2 Arten des Zugriffs:
 - 1) Per Weboberfläche (**LuCi**)
Standard IP: 192.168.1.1
 - 2) Per SSH (**Dropbear**)
Terminalbefehl: `sudo ssh root@192.168.1.1`

Umsetzung (4) – Passwort, SSH-Zugriff

- Web:



LEDE - Administration - LuCI - Mozilla Firefox

LEDE Administration - | X +

https://192.168.5.1/cgi-bin/luci/admin/system/admin

LEDE Status System Services Network Logout

Router Password

Changes the administrator password for accessing the device

Password

Confirmation

SSH Access

Dropbear offers [SSH](#) network shell access and an integrated [SCP](#) server

Dropbear Instance Delete

Interface WAN: **lan:** wwan: unspecified

Listen only on the given interface or, if unspecified, on all

Port Specifies the listening port of this Dropbear instance

Password authentication Allow [SSH](#) password authentication

Allow root logins with password Allow the *root* user to login with password

Gateway ports Allow remote hosts to connect to local SSH forwarded ports

- SSH Terminalbefehl: `passwd`

Umsetzung (5) – Zeit einstellen

LEDE - System - LuCI - Mozilla Firefox

LEDE - System - LuCI

https://192.168.5.1/cgi-bin/luci/admin/system/system

LEDE Status System Services Network Logout

System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

General Settings **Logging** Language and Style

Local Time Collecting data... Sync with browser

Hostname LEDE

Timezone Europe/Berlin

Time Synchronization

Enable NTP client

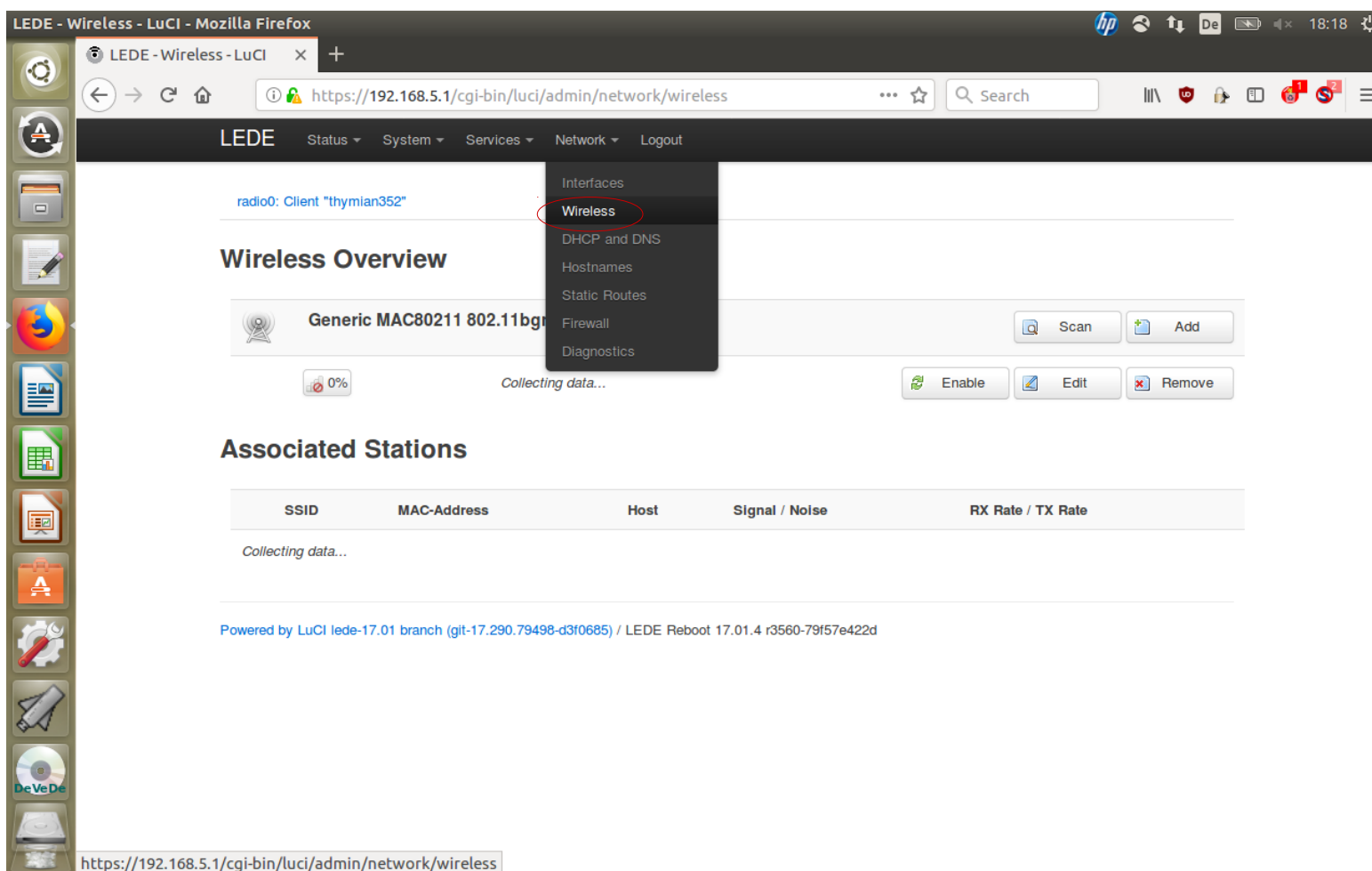
Provide NTP server

NTP server candidates

- 0.lede.pool.ntp.org
- 1.lede.pool.ntp.org
- 2.lede.pool.ntp.org
- 3.lede.pool.ntp.org

Umsetzung (6) – OS aktualisieren

- Raspi WLAN aktivieren und als Client an Erstrouter (Master) hängen. Auf Firewall (WAN) und Ländereinstellung achten.



LEDE - Wireless - LuCI - Mozilla Firefox

LEDE - Wireless - LuCI x +

https://192.168.5.1/cgi-bin/luci/admin/network/wireless

LEDE Status System Services Network Logout

radio0: Client "thymian352"

Wireless Overview

Generic MAC80211 802.11bg

0% Collecting data...

Scan Add Enable Edit Remove

Associated Stations

SSID	MAC-Address	Host	Signal / Noise	RX Rate / TX Rate
Collecting data...				

Powered by LuCI lede-17.01 branch (git-17.290.79498-d3f0685) / LEDE Reboot 17.01.4 r3560-79f57e422d

https://192.168.5.1/cgi-bin/luci/admin/network/wireless

Umsetzung (6) – OS aktualisieren

- OS aktualisieren.

LEDE - Software - LuCI - Mozilla Firefox

LEDE - Software - LuCI x +

https://192.168.150.1/cgi-bin/luci/admin/system/packages

LEDE Status **System** Services Network Logout

Software

Actions Configuration

No package lists available

Free space: 94% (237.75 MB)

Download and install package:

Filter:

Status

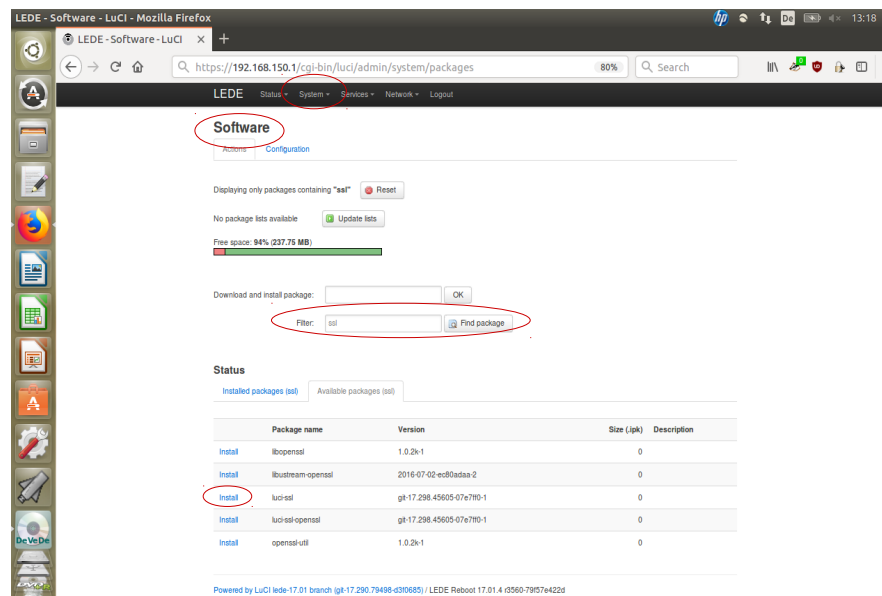
Installed packages Available packages

	Package name	Version
Remove	adblock	2.6.2-1
Remove	base-files	173.1-r3560-79f57e422d
Remove	brcm2708-gpu-fw	2017-03-03-78c4983379..28c
Remove	brcmfmac-firmware-43430-sdio	2016-09-21-42ad5367-1

Umsetzung (7) – Pakete nachinstallieren

- SSL (LuCi mit https-Unterstützung)
- uhttpd (Webserver u.a. mit TLS-Unterstützung)
- Werbeblocker
- Treiber für USB-Netzwerkadapter

➤ Web:



LEDE - Software - LuCI - Mozilla Firefox

LEDE - Software - LuCI x

https://192.168.150.1/cgi-bin/luci/admin/system/packages

LEDE Status System Services Network Logout

Software

Configuration

Displaying only packages containing "ssl"

No package lists available

Free space: 94% (237.75 MB)

Download and install package:

Filter:

Status

Installed packages (ssl) Available packages (ssl)

	Package name	Version	Size (apk)	Description
Install	libopenssl	1.0.2k-1	0	
Install	libstream-openssl	2016-07-02-ed81adaa-2	0	
Install	luci-ssl	git-17.298.45605-07e7f10-1	0	
Install	luci-ssl-openssl	git-17.298.45605-07e7f10-1	0	
Install	openssl-util	1.0.2k-1	0	

Powered by LuCI lede-17.01 branch (git-17.290.79468-d30685) / LEDE Reboot 17.01.4 d360-71957-e422d

➤ SSH:

```
pc_me@pc:~$ ssh root@192.168.1.1
root@192.168.1.1's password:
root@LEDE:~# opkg update
root@LEDE:~# opkg install luci-ssl luci-ssl-openssl uhttpd luci-app-uhttpd adblock luci-app-adblock kmod-usb-net kmod-usb-net-...
```

Umsetzung (8) – Netzwerk einrichten (1)

- Eingangsrouter - LAN

IP: **192.168.0.1**
Protocol: DHCP
DHCP range: 192.168.0.2 – 192.168.0.50
Subnet: 255.255.255.0

- Raspberry Pi – WAN (“eth1”)

IP: 192.168.0.51
Protocol: static
Subnet: 255.255.255.0
Gateway: **192.168.0.1**
DHCP server: disabled

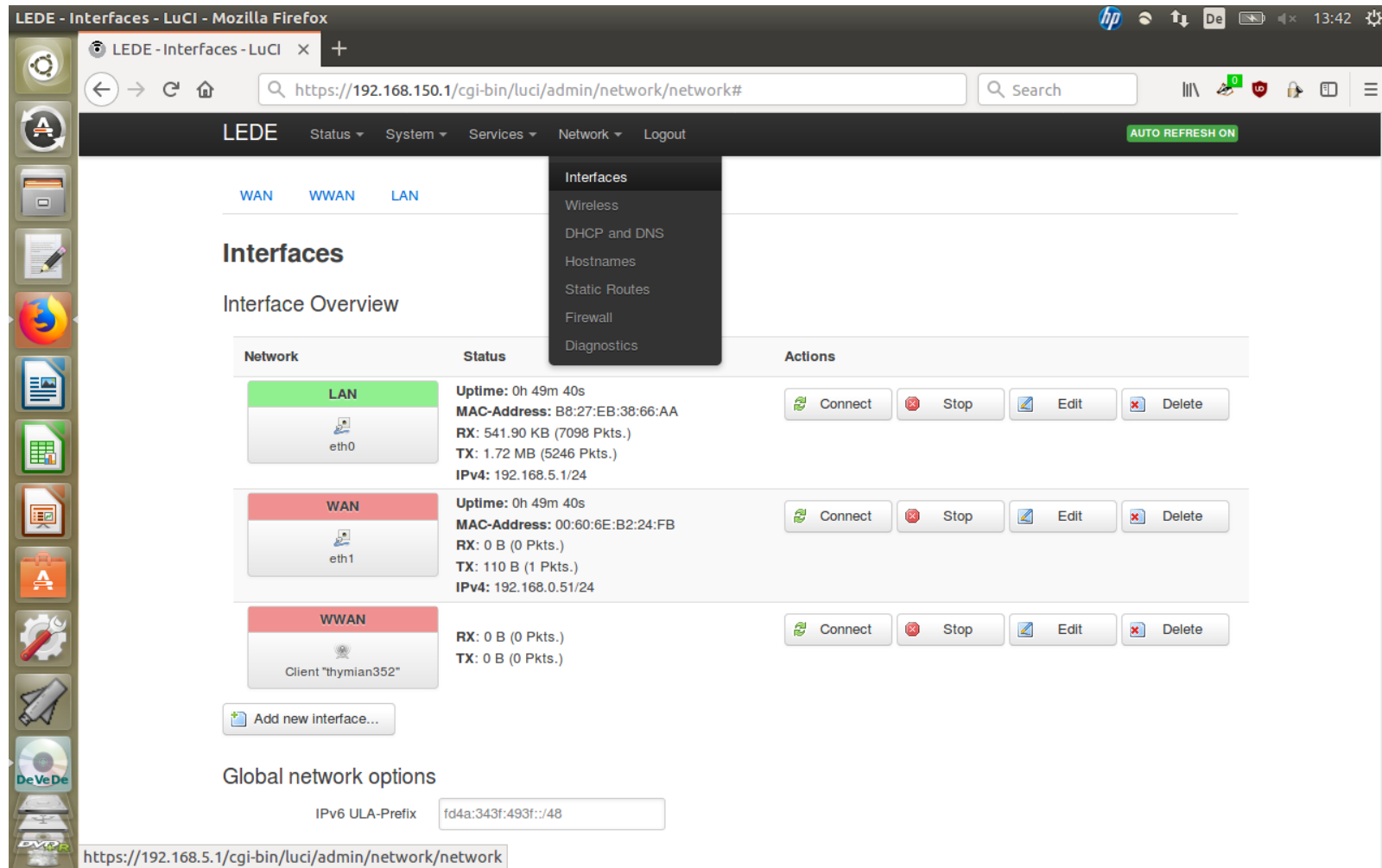
Firewall zone: wan
IPv6 abschalten.

- Raspberry Pi – LAN (“eth0”)

IP: **192.168.5.1**
Protocol: DHCP
DHCP range: 192.168.5.92 – 192.168.5.110
Subnet: 255.255.255.0

Firewall zone: lan
IPv6 abschalten.

Umsetzung (8) – Netzwerk einrichten (2)



LEDE - Interfaces - LuCI - Mozilla Firefox
 https://192.168.150.1/cgi-bin/luci/admin/network/network#

LEDE Status System Services Network Logout AUTO REFRESH ON

WAN WWAN LAN **Interfaces**

Interfaces
 Interface Overview

Network	Status	Actions
LAN eth0	Uptime: 0h 49m 40s MAC-Address: B8:27:EB:38:66:AA RX: 541.90 KB (7098 Pkts.) TX: 1.72 MB (5246 Pkts.) IPv4: 192.168.5.1/24	Connect Stop Edit Delete
WAN eth1	Uptime: 0h 49m 40s MAC-Address: 00:60:6E:B2:24:FB RX: 0 B (0 Pkts.) TX: 110 B (1 Pkts.) IPv4: 192.168.0.51/24	Connect Stop Edit Delete
WWAN Client "thymian352"	RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)	Connect Stop Edit Delete

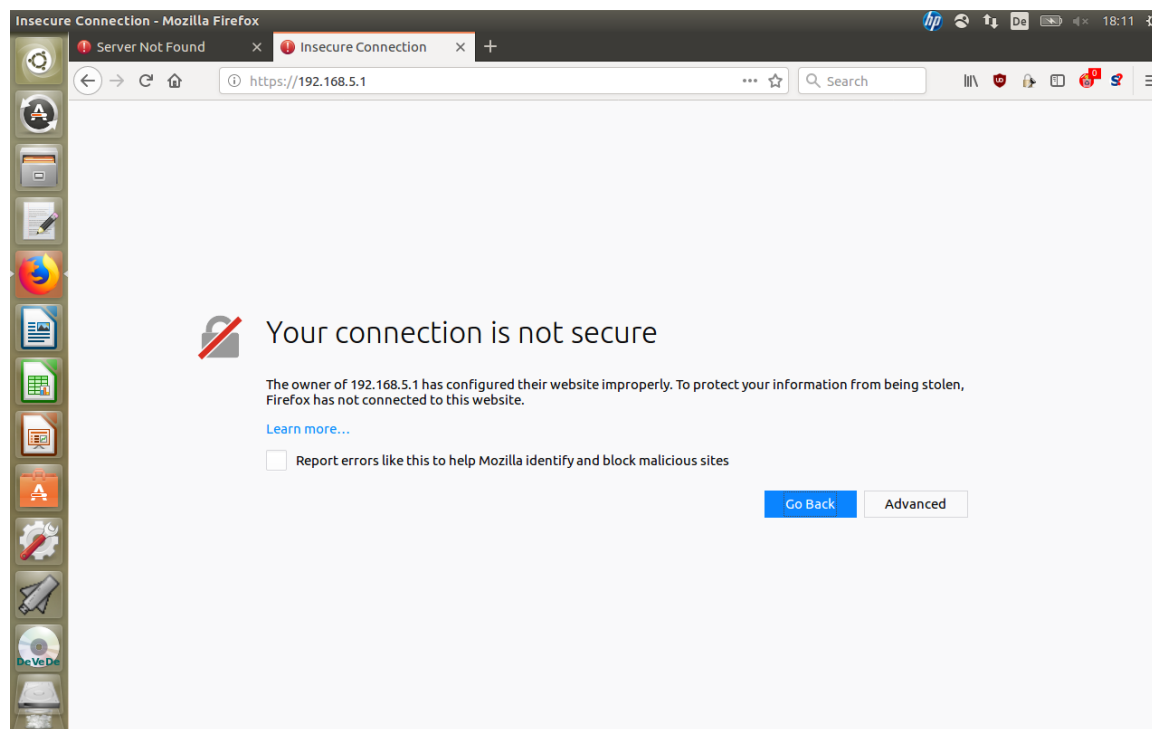
Add new interface...

Global network options
 IPv6 ULA-Prefix

https://192.168.5.1/cgi-bin/luci/admin/network/network

Umsetzung (9) – Raspi neu starten

- Raspi neu starten, da sich IP-Adresse geändert hat. Mit **neuer** Adresse (192.168.5.1) anmelden.
- Nicht erschrecken. LuCi https certificate warning erscheint (da selbst zertifiziert). Mutig auf „Akzeptieren“ klicken.



Umsetzung (10) – Firewall und DNS-Server

- Firewall einstellen:
 - Von innen nach außen alles erlaubt.
 - Von außen nach innen nichts erlaubt.
 - Weiterleitungen grundsätzlich verboten.

Zones

Zone → Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan: → wan	accept	accept	reject	<input type="checkbox"/>	<input type="checkbox"/>	Edit Delete
wan: wwan: WAN: → REJECT	reject	accept	reject	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit Delete

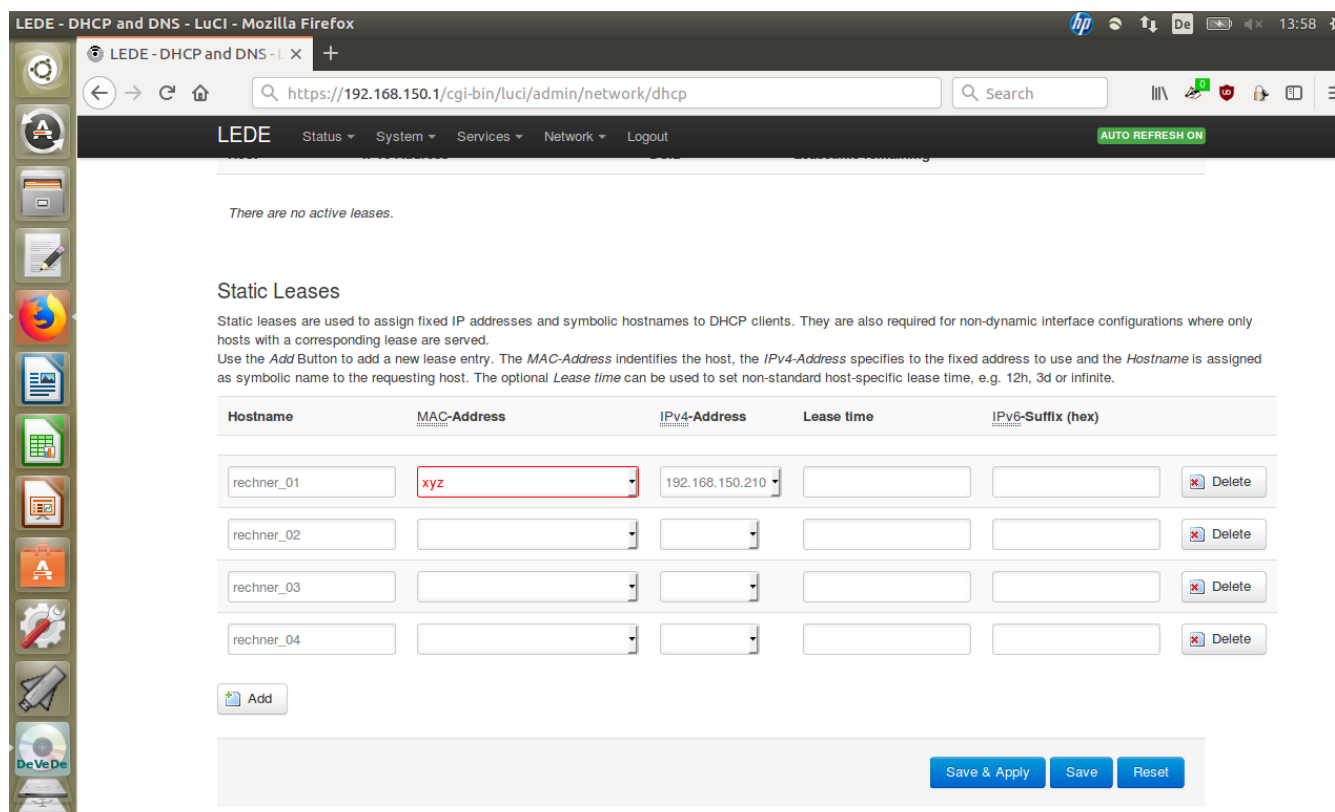
- DNS-Server einrichten: Entscheidung gegen den Platzhirschen, stattdessen für „Censurfridns Danmark“. Einstellung über → Network → Interfaces...

Umsetzung (11) – Raspi zusätzlich sichern

- Zugriff auf Raspberry Pi **nur** aus dem **LAN**.
- Zugriff per Webinterface **nur** über **HTTPS**. **Port 80** für Zugriffe aus dem LAN **schließen**.
- **SSH Port** vom Standard „22“ auf etwas größer „1024“ (besser größer „8000“) **ändern**.
- **Ports 22, 80 und 443** zusätzlich für Zugriffe aus dem WAN **schließen**. Dazu kleines Skript erstellen (→ Network → Firewall → Custom rules).

Umsetzung (12) – LAN zusätzlich sichern

- Zugang **nur** für definierte Geräte.
- Identifizierung erfolgt durch **MAC-Adressen**.



The screenshot shows the LEDE DHCP and DNS LuCI interface in a Mozilla Firefox browser. The page title is "LEDE - DHCP and DNS - LuCI - Mozilla Firefox". The address bar shows "https://192.168.150.1/cgi-bin/luci/admin/network/dhcp". The interface includes a navigation menu with "LEDE", "Status", "System", "Services", "Network", and "Logout". A green "AUTO REFRESH ON" button is visible in the top right.

The main content area displays "There are no active leases." and a section for "Static Leases". Below this, there is explanatory text: "Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served. Use the Add Button to add a new lease entry. The MAC-Address identifies the host, the IPv4-Address specifies the fixed address to use and the Hostname is assigned as symbolic name to the requesting host. The optional Lease time can be used to set non-standard host-specific lease time, e.g. 12h, 3d or infinite."

Hostname	MAC-Address	IPv4-Address	Lease time	IPv6-Suffix (hex)	
rechner_01	xyz	192.168.150.210			Delete
rechner_02					Delete
rechner_03					Delete
rechner_04					Delete

At the bottom of the table, there is an "Add" button. Below the table, there are three buttons: "Save & Apply", "Save", and "Reset".

Umsetzung (13) – Letzte Schritte

- **Testen**, ob alles geht.
 - › Raspi + Netzteil + USB-Netzwerkadapter
 - › Eingangsrouter per LAN-Kabel mit USB-Netzwerkadapter verbinden
 - › Raspis RJ45-Buchse per LAN-Kabel mit Rechner verbinden
 - › Browser öffnen. Webseite (heise.de) ansteuern et (hoffentlich) voilà!
- Konfigurationsdateien exportieren und sichern.
- **Dokumentieren.**

OpenWRT – Pro und Contra

- Open Source, d.h. jeder kann sehen, was vor sich geht.
- Entwickler reagieren schnell auf Sicherheitslücken.
- Kann sehr viel und ständig kommt mehr hinzu.
- Man muss sich selbst darum kümmern (Bsp. keine automatischen Updates) und trägt selbst das Risiko.
- Exportfunktion installierter Pakete und deren Konfiguration nicht automatisiert.

OpenWRT – Noch zu tun

- Portscan durchführen.
 - <https://www.heise.de/security/dienste/Netzwerk-check-2114.html>
- OpenWRT Benutzer anstelle von „root“ anlegen.
- SSH-Zugriff nur zertifizierten Clients erlauben (key-based authentication).

Quellen

- <https://openwrt.org>
- <https://lede-project.org>
- Günters Vortrag zu OpenWRT 2013 -
<http://www.pc-treff-bb.de/Vortraege/openwrt.pdf>



PC-Treff-BB

OpenWRT mit Raspberry Pi | Folie 26 von 27

© Katrin Eppler | 13.01.2018

Fragen?

Vielen Dank!