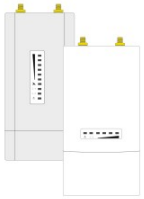
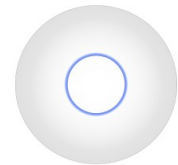





OpenWrt

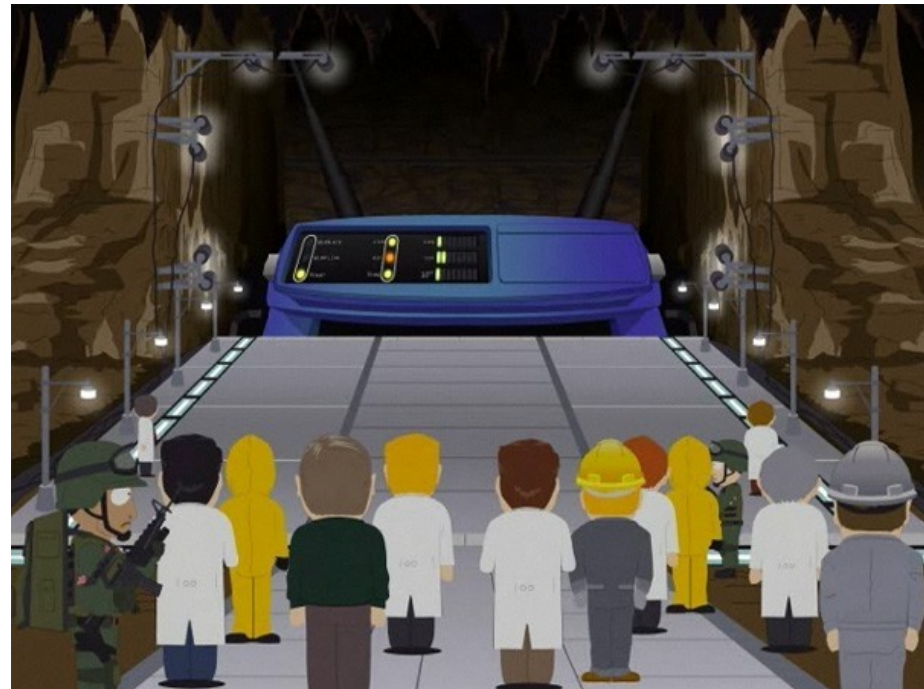
Wireless Freedom

(Vortrag von Moritz Warning)









Heute

- OpenWRT 
- Hardware 
- Installation 
- Flashen 
- Nutzen 



(Linksys WRT54G in "South Park")

Übersicht

- OpenWrt
 - Soetwas wie “Ubuntu” 
 - Basiert auf Linux 
 - Und BusyBox 
 - Für WLAN-Router 
- WLAN-Router
 - Netzwerk bzw. WLAN-Geräte 
 - 2.4 GHz / 5GHz 
 - z.B. Fritzbox...



Nutzen

- Freies Betriebssystem
- Webserver einrichten
- Festplatte per USB
 - billiges NAS
- USB Kamera
- Email-Server
- Sensoren/Aktoren per GPIO
- Volle Kontrolle / Sicherheit
- .. Ist eigentlich ein Linux server



Geschichte



- 2003:
 - Linksys WRT54G
 - GPL-Verletzung
- OpenWrt Projekt
- >700 Modelle
- OpenWrt 18.06




Slashdot Stories [Firehose >](#) All Popular Polls [Deals](#) [Submit](#)

Topics: [Devices](#) [Build](#) [Entertainment](#) [Technology](#) [Open Source](#) [Science](#) [YRO](#)

“ Catch up on stories from the past week (and beyond) at the [Slashdot story archive](#)

Is Linksys Violating The GPL?   **524**

 Posted by [timothy](#) on Sunday June 08, 2003 @02:18PM from the [could-just-be-a-glitch dept.](#)


[jap](#) writes


"According to [this post](#) on [LKML](#), [Linksys](#) is shipping firmware for (at least their) 802.11g access-points based on Linux - without any sourcecode available or mentioning of it on their site. This could be interesting: it might provide the possibility of building an ueber-cool accesspoint firmware with IPsec and native ipv6 support etc etc, using this information!"

Slashdot Stories [Firehose >](#) All Popular Polls [Deals](#) [Submit](#)

Topics: [Devices](#) [Build](#) [Entertainment](#) [Technology](#) [Open Source](#) [Science](#) [YRO](#)

“ Become a fan of Slashdot on [Facebook](#)

Linksys Releases GPLed Code for WRT54G   **335**

 Posted by [michael](#) on Sunday July 06, 2003 @08:50PM from the [happy-thoughts dept.](#)

[petree](#) writes

"I stumbled across this on the [Linksys](#) website. Linksys has apparently caved to [community pressure](#) and released the [GPLed source](#) for linux running on their [WRT54G](#). Cool Beans!"

Hardware

(von aussen)



Ubiquity loco m2/m5, 8MB/64MB
Outdoor, POE



Nexx WT3020 / 8MB/64MB
2.4 GHz / USB / ~12EUR



TP-Link: C1200, 16MB/128MB,
USB, Dualband, ~50EUR



TP-Link: CPE210/520, 8MB/64MB,
Outdoor



TP-Link, WR841nd, 4MB/32MB, ~15EUR
(Vorsicht v13+)



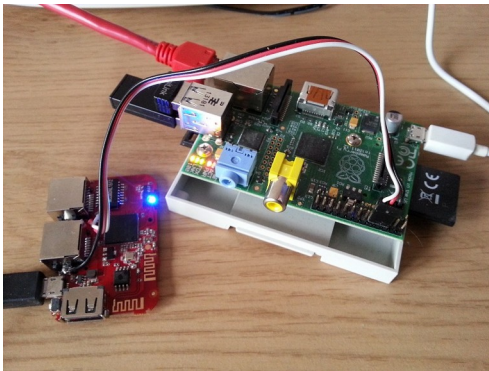
Ubiquity UniFi AP, 8MB/64MB, 80EUR

Power Over Ethernet (POE)
Richtfunk: bis zu ~15km
Omnidirectional: bis zu ~50m
USB2/3
100/1000 MBit
2.4GHz/5GHz/Dualband
Micro USB Stromversorgung

Aktuelle Hardwareempfehlungen
am besten aus dem Forum

(<https://forum.openwrt.org/t/whats-your-favorite-enthusiast-lede-openwrt-device/4477/17>)

Hardware Modding



- Antenne
- Speicher
- Sensoren
- LEDs

Hardware

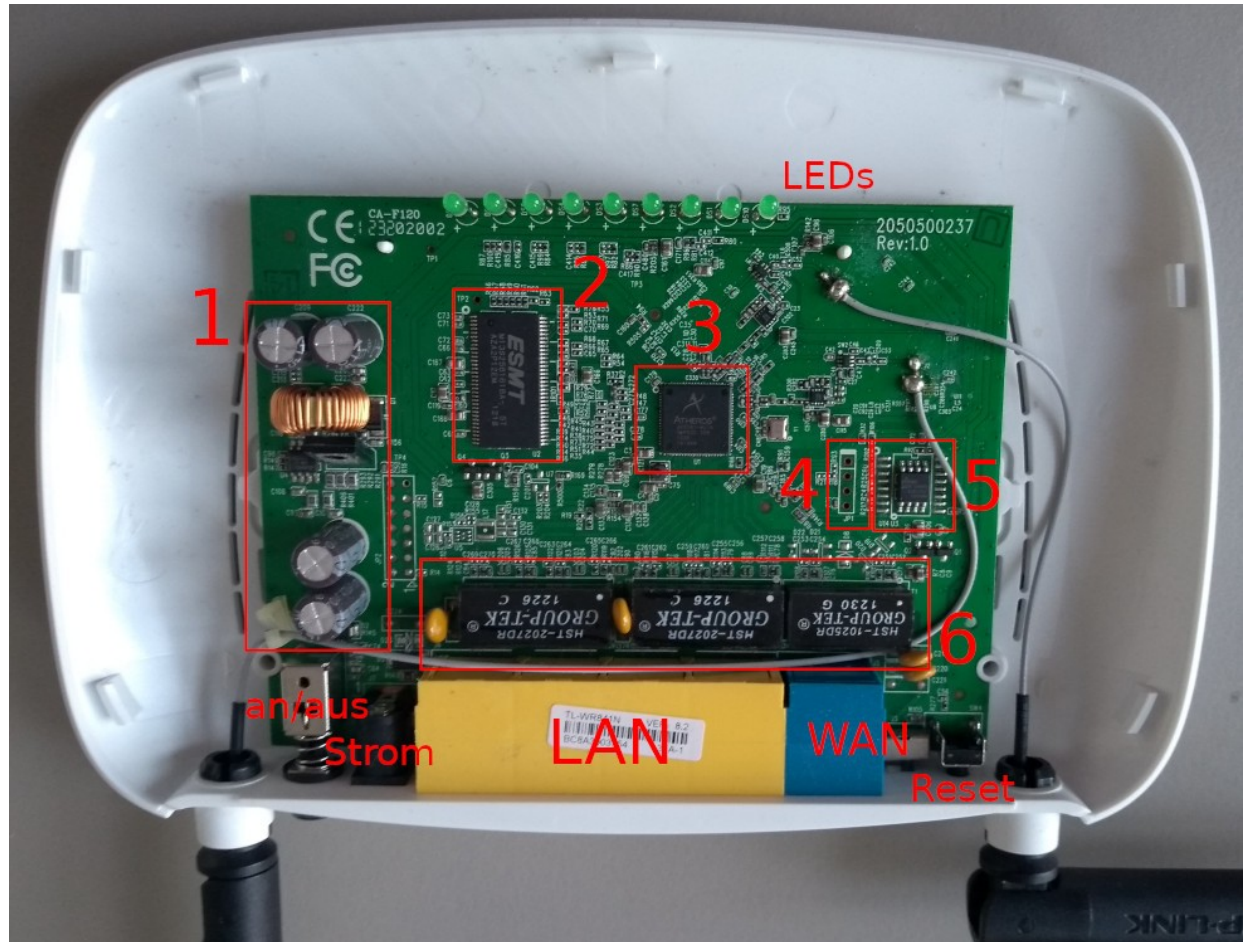
(innere Werte)

- Hersteller 
 - z.B. Ubiquity / TP-Link / D-Link / Mikrotik
- Oft 400-600 MHz CPU 
 - MIPS / ARM / x86
- 4-16MB Flash 
 - Empfehlung: 8MB oder mehr
- 32-64MB RAM 
- 2.4 GHz / 5 GHz / Dualband 
 - 5 GHz mehr Bandbreite

Hardware

(innen)

- 1) Stromwandler
Elkos/Spule
- 2) CPU/RAM
- 3) WiFi Chip (Atheros)
- 4) Serieller Anschluss
ohne Pins!
- 5) Flash (4MB)
- 6) Switch Transformer



Hardware Identifizieren

- Hardware-Revision:
 - Gleiches Model - andere Hardware!
- Gibt Verkäufer nie an ;-(



Modell: TL-WR841N
Revision: v8

Bei vielen Modellen werden alle Revisionen von OpenWrt unterstützt.

Besser: Vorher im Wiki nachschauen!
Nicht erschrecken, ist z.T. vollgestopft mit Informationen.

Firmware Finden



The screenshot shows the OpenWrt website homepage. At the top, there is a navigation bar with the OpenWrt logo and the tagline "Wireless Freedom". To the right of the logo, there are links for "Register" and "Log In", a search bar, and buttons for "Recent Changes", "Media Manager", and "Sitemap". Below the navigation bar, there is a "Welcome to the OpenWrt Project" banner with a language selector set to "English (en)".

The main content area features a sidebar on the left with a "Welcome to OpenWrt" section containing links to "Supported Devices", "Packages", "Downloads", "Documentation", "Submitting patches", "Reporting bugs", "Wiki contribution guide", "OpenWrt Forum", and "FAQ". Below this is an "About OpenWrt/LEDE" section with links to "Rules", "Infrastructure", "Trademark Policy", "About this site", and "Contact Us".

The main content area has a heading "Welcome to the OpenWrt Project" followed by a paragraph: "The OpenWrt Project is a Linux operating system targeting embedded devices. Instead of trying to create a single, static firmware, OpenWrt provides a fully writable filesystem with package management. This frees you from the application selection and configuration provided by the vendor and allows you to customize the device through the use of packages to suit any application. For developers, OpenWrt is the framework to build an application without having to build a complete firmware around it; for users this means the ability for full customization, to use the device in ways never envisioned."

Below this is a link to "Table of Hardware" and a reference to "About OpenWrt" pages. A section titled "CCC and OpenWrt: Technical guideline of German BSI for secure routers insufficient" follows, with a paragraph: "The recently released technical guideline for secure broadband routers is simply a disservice to customers. This guideline will not prevent widespread malfunction of routers and their security problems in the future. The consumers will not get a useful way to distinguish secure and long living devices from risky devices or the possibility to take care of the security by them self."

Another paragraph states: "Vendors are still allowed to block OpenWrt from the devices they sold, even after security support for the device was already terminated, making the device useless."

The next section discusses the Chaos Computer Club (CCC) and OpenWrt's involvement with the Bundesamt für Sicherheit in der Informationstechnik (BSI) and representatives of multiple device vendors and network operators. It lists two main demands:

1. Vendors have to inform customer before buying the product for all devices being sold in Germany, how long the device will get security updates in case problems are found.
2. The customer must have the possibility to install custom software on their devices, to have the possibility to fix security problems even after the official vendor support ended.

There is a link to "Press release in German" below the list.

The final section is titled "Download OpenWrt" and states: "The OpenWrt Community is proud to present the OpenWrt 18.06 stable version series. It is the first stable version after the OpenWrt/LEDE project merger and the successor to the previous stable LEDE 17.01 and OpenWrt 15.05 major releases."

A concluding paragraph says: "The OpenWrt 18.06 series focuses on modernizing many parts of the system, on backporting network offload support for eligible targets and on laying the groundwork for regular future release updates."



At the bottom, it states: "Current Stable Release - OpenWrt 18.06.2"

<https://openwrt.org>

Firmware Herunterladen

- Firmwaredateien
 - mit dem Browser über die Webseite
 - openwrt-<modell/version>-factory.bin
 - Für Erstinstallation
 - Wird als Firmwareupdate auf der Weboberfläche angewendet
 - openwrt-<modell/version>-sysupgrade.bin
 - Update - falls OpenWrt bereits installiert ist
 - “sysupgrade [-n] /tmp/openwrt-model.bin”
 - “-n” verwirft alle bisherigen Einstellungen
 - alle Programme werden verworfen => müssen neu installieren werden..
- Beispiel:
 - <https://downloads.openwrt.org/releases/18.06.2/targets/ar71xx/tiny/openwrt-18.06.2-ar71xx-tiny-tl-wr841-v8-squashfs-factory.bin>
 - <https://downloads.openwrt.org/releases/18.06.2/targets/ar71xx/tiny/openwrt-18.06.2-ar71xx-tiny-tl-wr841-v8-squashfs-sysupgrade.bin>
- *-factory.bin als Firmwareupdate in der Originalfirmware anwenden!
 (Manchmal auch nur über Bootloader/serielle Konsole/TFTP möglich)

Weboberfläche (1)

- Wenn alles gut geht: 
- “LuCI”
 - Im Browser 192.168.1.1 aufrufen
 - Alle üblichen Konfigurationen
 - WLAN Setup
 - Passwort
- Weitere Programme, LuCI Module, besondere Einstellungen:
 - => per Konsole 

Weboberfläche (2)

The screenshot displays the OpenWrt LuCI web interface. The browser address bar shows the URL `192.168.1.1/cgi-bin/luci/admin/status/overview`. The interface is divided into several sections:

- Status System:** A table showing system information:

Hostname	OpenWrt
Model	TP-Link TL-WR841N/ND v8
Architecture	Atheros AR9341 rev 1
Firmware Version	OpenWrt 18.06.2 r7676-cddd7b4c77 / LuCI oper
Kernel Version	4.9.152
Local Time	Wed Jan 30 12:29:50 2019
Uptime	0h 8m 57s
Load Average	0.25, 0.19, 0.11
- Memory:** Progress bars showing usage:


Total Available	7924 kB / 27856 kB (28%)
Free	5904 kB / 27856 kB (21%)
Buffered	2020 kB / 27856 kB (7%)
- Network:** Configuration for IPv4 and IPv6 upstream connections. Both show "Protocol: Not connected".

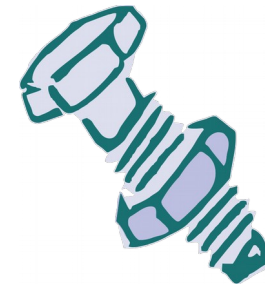
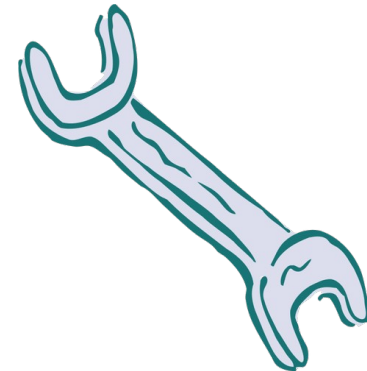
IPv4 Upstream	IPv6 Upstream
Protocol: <i>Not connected</i> Address: 0.0.0.0 Netmask: 255.255.255.255 Gateway: 0.0.0.0	Protocol: <i>Not connected</i> Address: :: Gateway: ::
Device: -	Device: -
- Active Connections:** A progress bar showing 37 / 16384 (0%).
- Active DHCP Leases:** A table listing active leases:

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
?	192.168.1.199	00:E0:8F:00:06:AC	11h 59m 58s

Additional features visible include a "No password set!" warning, an "Authorization Required" login form with fields for Username (root) and Password, and a footer indicating the system is powered by LuCI openwrt-18.06 branch.

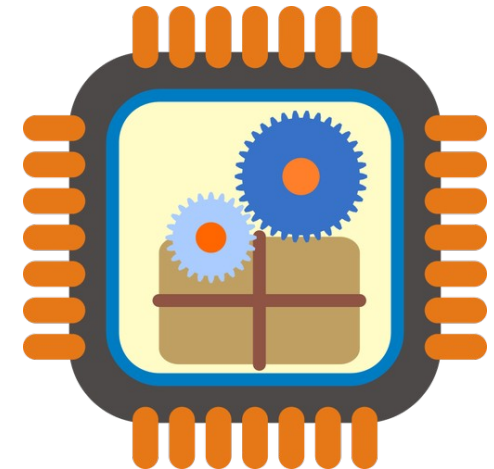
Konsole (1)

- Oder auch per SSH Konsole
- Basis Linux (Busybox)
 - ls, cd, cp, mv, rm, ...
 - Editor vi 
 - ansonsten nano installieren
- Konfiguration
 - /etc/config/network (VLANs)
 - /etc/config/firewall
 - /etc/config/system (LEDs :P)
 - /etc/config/wireless (SSID, WiFi-Passwort)
 -
 - Oder “uci set wireless.radio0.disabled=0”
 - uci ist z.B. sinnvoll für Scripte



Paketmanager

- “opkg update”
 - speichert Paketdatenbank nicht-flüchtig
 - unter */tmp*
- “opkg search ...”
 - Oder auf openwrt.org suchen.
- “opkg install nano”
 - Sonst mit vi



Paket-Setups

(Beispiele)

- Pakete um USB Stick anzusprechen:

- kmod-usb-storage
- block-mount
- kmod-fs-ext4
- kmod-fs-vfat
- kmod-nls-cp437
- Kmod-nls-iso8859-1



- Pakete für 3G-dongle

- comgt
- kmod-usb-serial
- kmod-usb-serial-option
- kmod-usb-serial-wwan
- usb-modeswitch



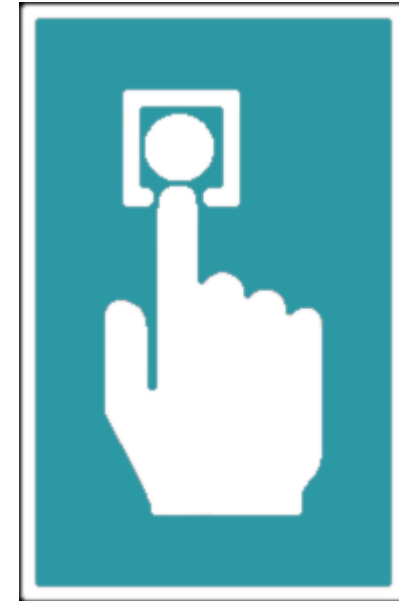
Sonstiges

- Nicht regelmäßig ins Flash schreiben
 - Kann nur 1000x Schreibzyklen
 - Wenn möglich /tmp verwenden
 - “scp image.bin root@192.168.1.1:/tmp/”
- Flash Dateisystem ist komprimiert
 - Squashfs
 - Änderungen werden immer angehängt
 - Auch Löschungen (Speicherplatz nimmt immer zu)

Failsafe

(wenn ihr euch ausgesperrt habt)

- Per Taster auslösbar
- Lädt Basiskonfiguration
- Erlaubt
 - Alle Einstellungen verwerfen
 - “first_boot”
 - Einstellungen reparieren
 - “mount_root”
 - Und dann mit dem Editor..



**Einfach ausprobieren!
Tut nicht weh. :P**

Failsafe aktivieren

Auslöseprozedur:

- 1) Router neu starten
 - 2) System-LED fängt an zu blinken
 - 3) Reset-Taste auslösen innerhalb von 3 Sekunden
 - 4) System-LED blinkt ganz schnell (~5/sec)
 - 5) PC per Netzwirkabel verbinden
 - 6) Sich selber 192.168.1.2/24 geben
- “ssh root@192.168.1.1” oder mit PuTTY unter Windows

Wenn Failsafe nicht hilft..

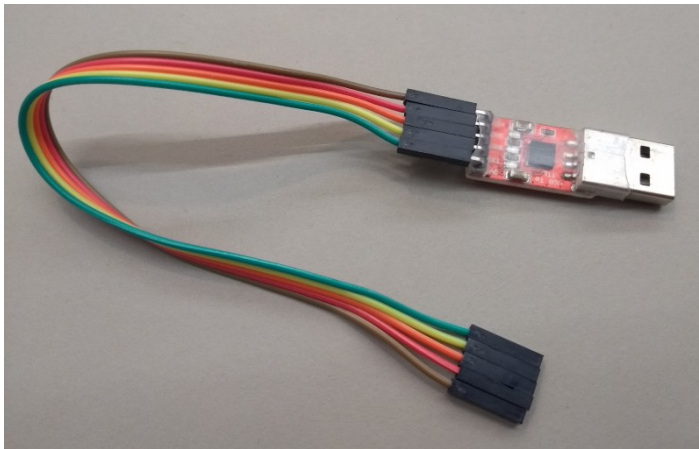
- Zugang
 - Failsafe geht in >95% der Fälle
 - Per serieller Konsole
 - serielle Pins suchen
 - Pins einlöten
 - Belegung herausfinden (im Internet suchen)
 - USB-to-TTL
 - Bootloader unterbrechen
 - Per Bootloader Weboberfläche – sehr bequem wenn vorhanden
 - per TFTP neu flashen
 - Chip Lesen/Schreiben mit Programmer
 - JTAG...



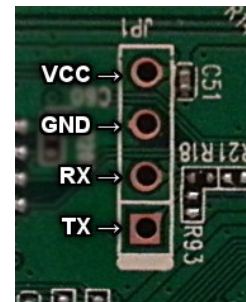
Serielle Konsole (1)

(fortgeschrittenes Thema)

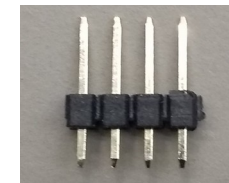
Nötig wenn Gerät nicht erreichbar und Failsafe nicht funktioniert.



USB zu TTL Wandler, ca. 5EUR



Serielle Pins auf der Platine



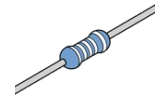
Pin Header

Pinbelegung z.B. im OpenWrt Wiki nachschauen.
Zur Not testen.

Serielle Konsole (2)

(fortgeschrittenes Thema)

- Nötig wenn Gerät nicht erreichbar und Failsafe nicht funktioniert
- 1) Serielle pins identifizieren TX / RX / GND
(VCC nie nötig)
 - 2) Pins anlöten
machmal Pull Down Widerstand nötig (Wiki prüfen)
 - 3) USB Adapter anschließen
 - 4) Serielle Konsole starten (z.B. "cutecom")
/dev/ttyUSB0 (Nutzerrechte!), richtige Baudrate
 - 5) Linux laden und per Konsole reparieren / zurücksetzen
 - 6) ... Oder Bootloader unterbrechen...



Serielle Konsole / TFTP (3b)

(fortgeschrittenes Thema)

- Bootlader unterbrechen mit Tastendruck
 - 1) Router-Konsole: Bootunterbrechen mit Befehl (z.B. "tpl" senden)
 - 2) Router/PC mit LAN Kabel verbinden
 - 3) PC: Netzwerk auf 192.168.1.111/24" konfigurieren
 - 4) Image auf PC platzieren (hängt vom tftp Server ab)
 - 5) TFTP Server auf PC starten (z.B. tftp-hpa)
 - 6) Auf Router-Konsole "setenv ipaddr 192.168.1.111"
"setenv serverip 192.168.1.100"

```

ar7240> tftpboot 0x80000000 openwrt-ar71xx-generic-tl-wr841n-v8-squashfs-factory.bin

Using eth0 device

TFTP from server 192.168.1.100; our IP address is 192.168.1.111

Filename 'openwrt-ar71xx-generic-tl-wr841n-v8-squashfs-factory.bin'.

Load address: 0x80000000

Loading: checksum bad

#####
#####

#####

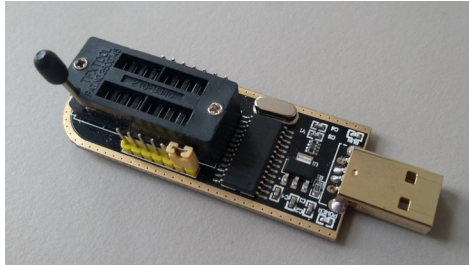
done

Bytes transferred = 3932160 (3c0000 hex)

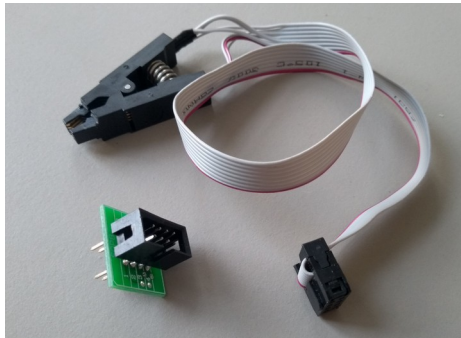
```

Flash Auslesen 1

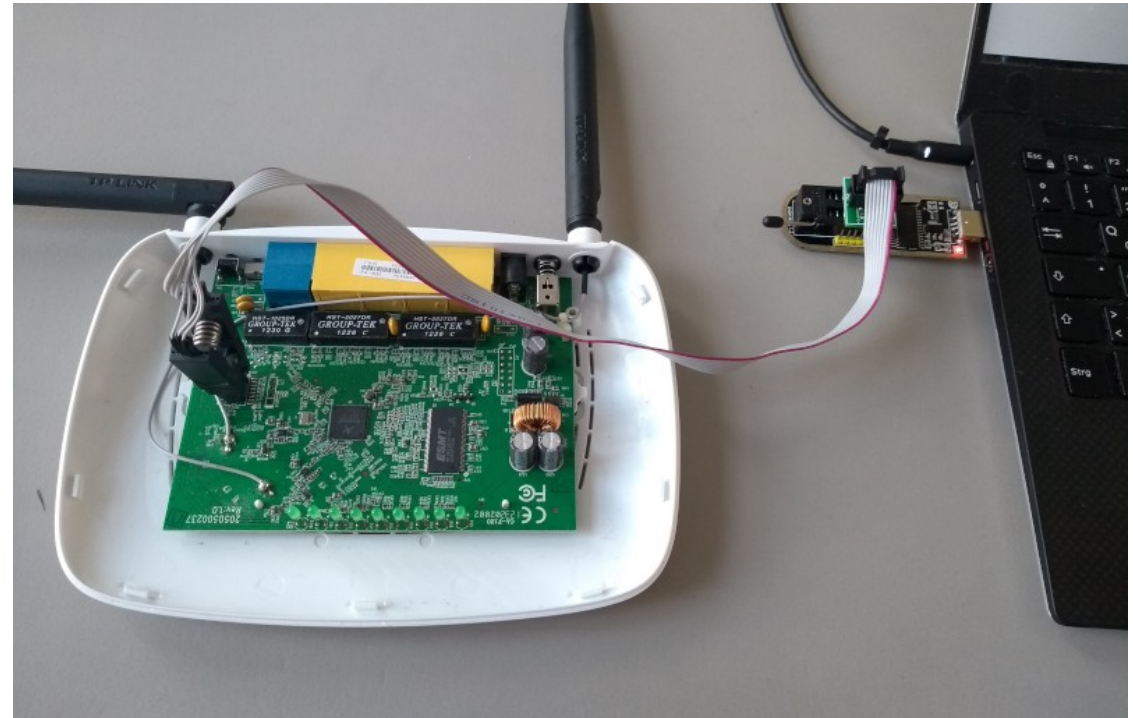
(sehr fortgeschrittenes Thema)



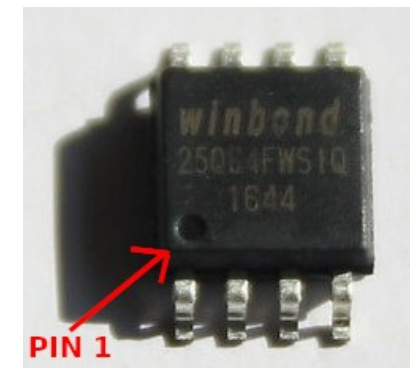
“Programmer”: CH341APro, ca. 5EUR



Flash 8 Pin Clip, ca. 5EUR



Notwendig wenn das Gerät nicht mehr startet und failsafe und der Zugriff per serieller Konsole nicht mehr hilft!

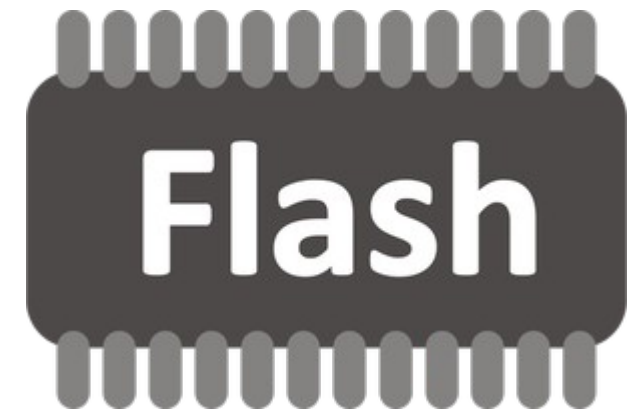


(Verpolen macht i.d.R. aber nichts kaputt)

Flash Auslesen 2

(sehr fortgeschrittenes Thema)

- Backup machen und wiederherstellen noch einfach
- Flashen mit anderer Abbild muss alte ART Partiton beibehalten!
 - ART enthält Kalibrationsdaten (**A**theros **R**adio **T**est)
 - Wenn falsch, dann darf das Gerät nicht mehr betrieben werden
 - Startet eventuell sogar nicht mehr
 - Erfordert Einfügen der Partition in Abbild!
- Lesen in Datei:
 - `“flashrom -c W25Q64.V -p ch341a_spi -r /tmp/data”`
- Analysieren:
 - `“flashread /tmp/data”`
 - 0x000000000000-0x000000040000 : "u-boot"
 - 0x000000040000-0x000000050000 : "u-boot-env"
 - 0x000000050000-0x000000200000 : "kernel"
 - 0x000000200000-0x0000007f0000 : "rootfs"
 - 0x0000003f0000-0x0000007f0000 : "rootfs_data"
 - 0x0000007f0000-0x000000800000 : "art"
 - 0x000000050000-0x0000007f0000 : "firmware"
- Verifizieren:
 - `“flashrom -c W25Q64.V -p ch341a_spi -w /tmp/data”`
- Schreiben:
 - `“flashrom -c W25Q64.V -p ch341a_spi -w /tmp/data”`
- `“W25Q64.V”` kommt aus List von `“flashrom -L”`



Firmware Selber Bauen (1)

- Benötigte Pakete:

- (apt install) subversion g++ zlib1g-dev build-essential git python time libncurses5-dev gawk gettext unzip file libssl-dev wget

- PC Linux Konsole:

```
git clone https://git.openwrt.org/openwrt/openwrt.git
```

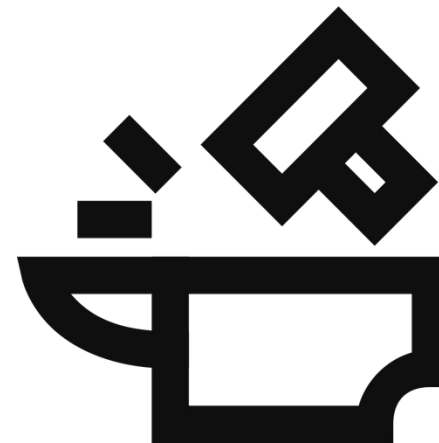
```
cd openwrt
```

```
./scripts/feeds update -a
```

```
./scripts/feeds install -a
```

```
make menuconfig
```

- 4GB RAM, ~15GB frei



Firmware Selber Bauen (2)

- Richtiges “Target System” und “Subtarget” auswählen.
- Dann ist auch das richtige “Target Profile” auswählbar!
- Im openwrt.org Wiki nachschlagen.

- 1) Jetzt Speichern & Beenden
- 2) Und “make -j4” ausführen.
- 3) Warten und Butterbrot schmieren.

```
File Edit View Search Terminal Help
.config - OpenWrt Configuration

OpenWrt Configuration
Arrow keys navigate the menu. <Enter> selects submenus ---> (or empty submenus
--->). Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes,
<M> modularizes features. Press <Esc><Esc> to exit, <?> for Help, </> for
Search. Legend: [*] built-in [ ] excluded <M> module <> module capable

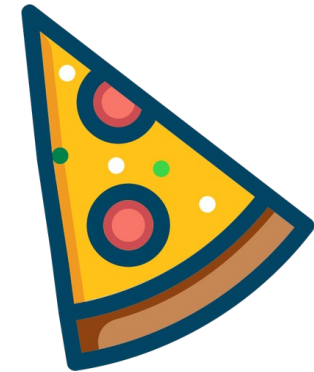
|| Target System (Atheros AR7xxx/AR9xxx) --->
  Subtarget (Devices with small flash) --->
  Target Profile (TP-LINK TL-WR841N/ND v8) --->
  Target Images --->
  Global build settings --->
  [ ] Advanced configuration options (for developers) ----
  [ ] Build the OpenWrt Image Builder
  [ ] Build the OpenWrt SDK
  [ ] Package the OpenWrt-based Toolchain
  [ ] Image configuration --->
    Base system --->
    Administration --->
    Boot Loaders ----
    Development --->
    Extra packages ----
    Firmware --->
    Fonts --->
    Kernel modules --->
    Languages --->
    Libraries --->
    LuCI --->
    Mail --->
    Multimedia --->
    Network --->
    Sound --->
    Utilities --->
    Xorg --->

<Select> < Exit > < Help > < Save > < Load >
```

“make menuconfig”

Firmware Selber Bauen (3)

```
[mwarning@xanax openwrt]$ make -j4
make[1] world
make[2] package/cleanup
make[2] target/compile
make[3] -C target/linux compile
make[2] diffconfig
make[2] package/compile
make[3] -C package/libs/libjson-c host-compile
make[3] -C package/libs/toolchain compile
make[3] -C package/libs/ncurses host-compile
make[3] -C package/system/fwtool host-compile
make[3] -C package/system/usign host-compile
make[3] -C package/kernel/gpio-button-hotplug compile
```



30min-2 Stunden je nach CPUs

```
make[3] -C package/network/utils/iptables compile
make[3] -C package/libs/openssl compile
make[3] -C package/network/config/firewall compile
make[3] -C package/network/services/hostapd compile
make[3] -C package/base-files compile
make[3] -C package/boot/uboot-envtools compile
make[3] -C package/kernel/mac80211 compile
make[2] package/install
make[2] target/install
make[3] -C target/linux install
make[2] package/index
make[2] checksum
[mwarning@xanax openwrt]$
```



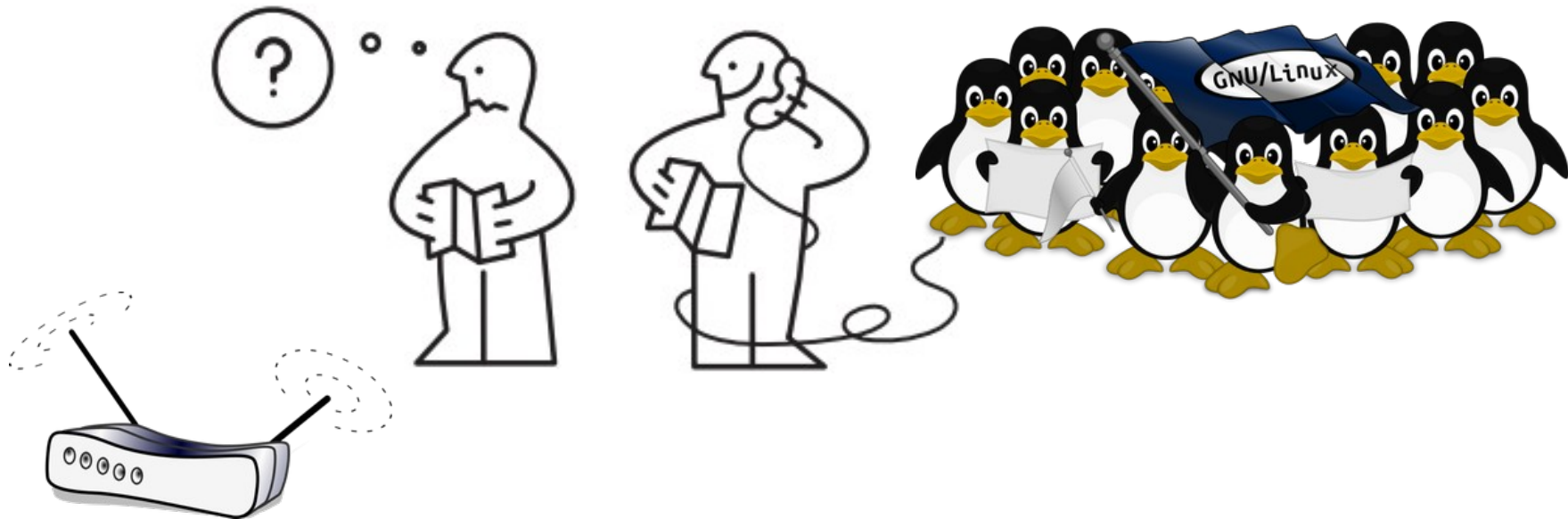
- Dateien zum Flashen in:
 ./bin/targets/ar71xx/tiny/openwrt-ar71xx-tiny-tl-wr841-v8-squashfs-factory.bin
- Optional: Dateien im ./files/ werden ins Image mit übernommen

Sonstiges

- Manche Firmwares werden gesichert vor “Manipulation”
 - TP-Link wr841 v13...
 - muss per tftp geschrieben werden
- Ursache: FCC / Regulierungsbehörden
- 5GHz Regulierung



Danke & Fragen



Links

- OpenWrt
 - Homepage: <https://openwrt.org>
 - Wiki: <https://wiki.openwrt.org>
 - Forum: <https://forum.openwrt.org>
- Docker Container
 - <https://github.com/mwarning/docker-openwrt-builder>
- Freetz für FritzBox:
 - <https://freetz.github.io/>

