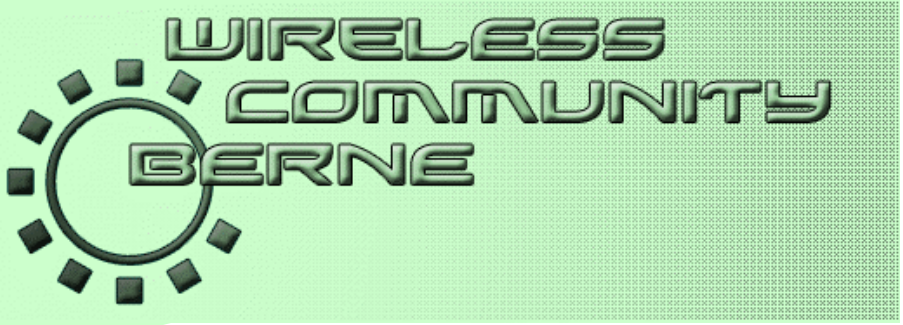


Linksys WRT54GS & OpenWRT

eine kleine Bastelei
an einem Router

Fabian Affolter

Overview

- Einleitung
- Hardware
- Firmware
- OpenWRT
- Modding am WRT54GS
- Quellen & Links

Einleitung

- Internet-Sharing-Router
- Switch mit 4 Ports und Wireless-G (802.11g)
- SpeedBooster-Technologie (35 % mehr Leistung)
- hohe Sicherheit:
  - branchenweit führende Kinderschutzfunktionen
  - 128-Bit-Wireless-Verschlüsselung
  - leistungsstarke SPI-Firewall

Hardware – Vorgänger-Modelle

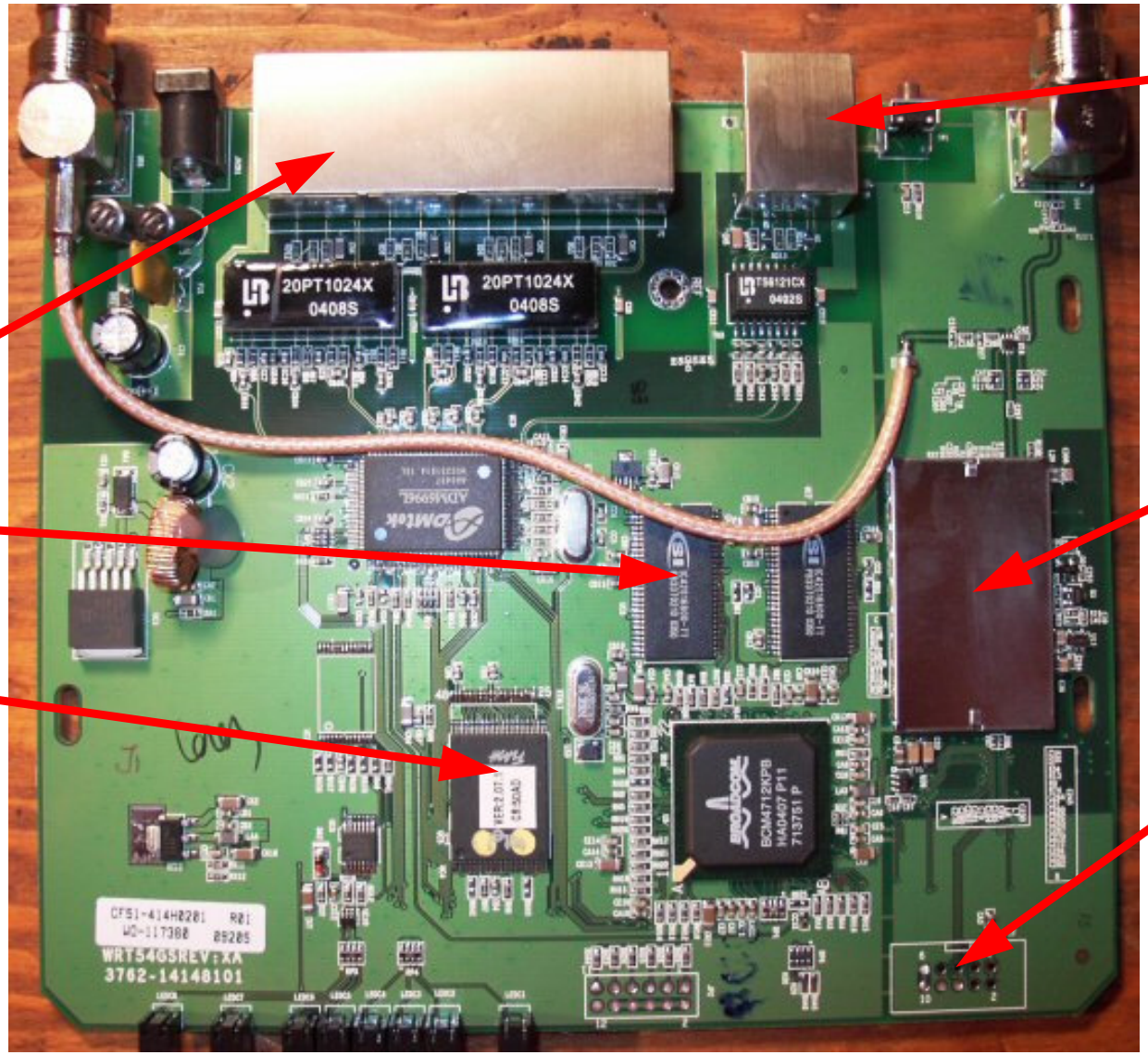
V 1.0	V 1.1	V 2
•125 MHz •WLAN Mini-PCI-Karte •16 MB RAM •4 MB Flash	•125 MHz •WLAN auf Board •16 MB RAM •4 MB Flash	•200 MHz •WLAN in CPU integriert •16 MB RAM •4 MB Flash •serielle Ports möglich

Hardware – WRT54GS

Feature	WRT54GS v1.0
Prozessor	BCM4712KPB
Speed (MHz)	200 MHz
Ethernet Switch	ADMtek ADM6996L 5port 10/100
RAM (MB)	32 MB
RAM Device	2 x IC42S16800-7T (8MB x 4)
Flash (MB)	8 MB
Flash Device	Intel
MAC	BCM4712KPB
Power Supply	12V DC 1.0A
Protokolle	802.11b/g + SpeedBooster, 802.3/u
Mainboard	CPU/MAC one chip solution, separates Wireless-Modul
Antennen-Connector	2x RP-TNC
Ports	
WAN	1x 10/100baseTX
LAN	4x 10/100baseTX
WLAN	1x
LEDs	8 LED Front-Panel
	Power, DMZ
WLAN	Act/Link
LAN (per port)	Link/Act
Internet	Link/Act

Hardware - Aussenansicht

Hardware - Innenansicht



WAN

Switch

HF-Teil

RAM

Flash

Serieller Port

Firmware

- Original-Firmware Linksys
- HyperWRT
- eWRT
- wifi-box
- Batbox
- Svesoft
- Tinypeap

Firmware - Original-Firmware Linksys

- Version 3.17.4 für WRT54GS ist aktuell
- wurde unter der GPL-Lizenz veröffentlicht
- Quellen-Code ~ 150 MB gross
- alle Einstellungen werden im NVRAM am Ende des Flash gespeichert
- WLAN-Treiber nur als Binär-Module (ähnlich Nvidia-Grafikkarten)

http://www.linksys.com/support/gpl.asp

Firmware - HyperWRT 2.0b3

für WRT54G & WRT54GS
basiert auf Linksys 3.37.2 firmware

Features

- Antenne-Auswahl & Sendeleistung kann variiert werden
- 13 Kanäle
- mehr Port Forwarding & Triggering Fields
- mehr QoS Device & Application Fields
- mehr Access Restrictions Policies & Blocked Services Fields
- Command Shell
- Telnet Daemon
- Startup & Firewall Scripts
- Uptime
- Reboot Button
- Startup & Firewall Scripts

http://www.hyperdrive.be/hyperwrt/

Firmware - eWRT 0.2 final

für WRT54G
basiert auf Sveasoft Samadhi2

Features

- NoCatSplash – auf NoCat basierendes Captive Portal
- Traffic shaping mit Wondershaper + iproute2
- SSH und Telnet Management
- Sendeleistung kann variiert werden
- Client Modus, Adhoc & WDS
- RSSI stats reporting für Clients
- Remote Syslogging

http://www.portless.net/menu/ewrt/

Firmware - restliche

Wifi-box	Batbox	Sveasoft	Tinypeap
• wurde im Vergleich zur Original-Firmware geringfügig erweitert • für den Heimbetrieb empfohlen	• Mini-Linux mit syslog, Httpd, vi, snort, mount, insmod, rmmod, top, grep, ls, ifconfig, iptables, ssh, iptraf • keine per-manenten Veränderungen der Firmware, nach Neustart ist alles wieder normal.	• sehr umfas-sende Firmware • kostet $ 20 • verstösst gegen die GPL-Lizenz der Linksys-Firmware	• Integriert einen kleinen RADIUS-Server, der die PEAP Authent-ifikation unterstützt. • So kann ein dedicated RADIUS Server gespart werden • setzt Sveasoft oder Linksys voraus

OpenWRT

- Grundlagen
- nützliche Software
- Vorbereitung WRT54GS
- Vorbereitung Installation
- Übertragung
- Dateisystem
- Erweiterungen
- Möglichkeiten

OpenWRT - Grundlagen

- OpenWRT ist eine Basis-Distribution, welche sich beliebig erweitern lässt
- schlank & fexibel
- Erweiterung durch optionale Pakete
- OpenWRT hat keine grafisches Front-End (Freifunk biete eine speziell angepasste Version mit Front-End an)
- Die Konfigurationseinstellungen werden im NVRAM gespeichert (wie bei der Original-Firmware).

OpenWRT - nützliche Software

Management & Installation

- tftp-Server
- telnet-Client
- ssh-Client

OpenWRT – Vorbereitung WRT54GS

Durch eine „Sicherheitslücke“ unter Administration / Ping ist es möglich beliebige Befehle an den WRT54GS zu senden.

```
;cp${IFS}*/*/nvram${IFS}/tmp/n
;*/n${IFS}set${IFS}boot_wait=on
;*/n${IFS}commit
;*/n${IFS}show>tmp/ping.log
```

So kann boot_wait aktiviert werden. Erhöhung der Wartezeit auf 3s beim Bootvorgang für Übertragung per tftp.

Achtung: **Der WAN-Port braucht eine IP-Adresse.**

OpenWRT - Vorbereitung Installation

Kompilierung

- Die Distribution wird über die Sourcen verbreitet und jeder kompiliert sie selber.
- Dafür braucht man etwa 1.3 GB freien Platz und ein Linux-System. (funktioniert auch mit Knoppix)

```
# tar zxvf buildroot.tar.gz
# cd buildroot
# make
```

Zeitaufwand

zwischen ein paar Minuten bis zu mehreren Stunden je nach vorhandener Hardware

OpenWRT - Übertragung

!!!! boot_wait muss aktiviert sein !!!!

IP-Adresse 192.168.1.1 Netmask 255.255.255.0

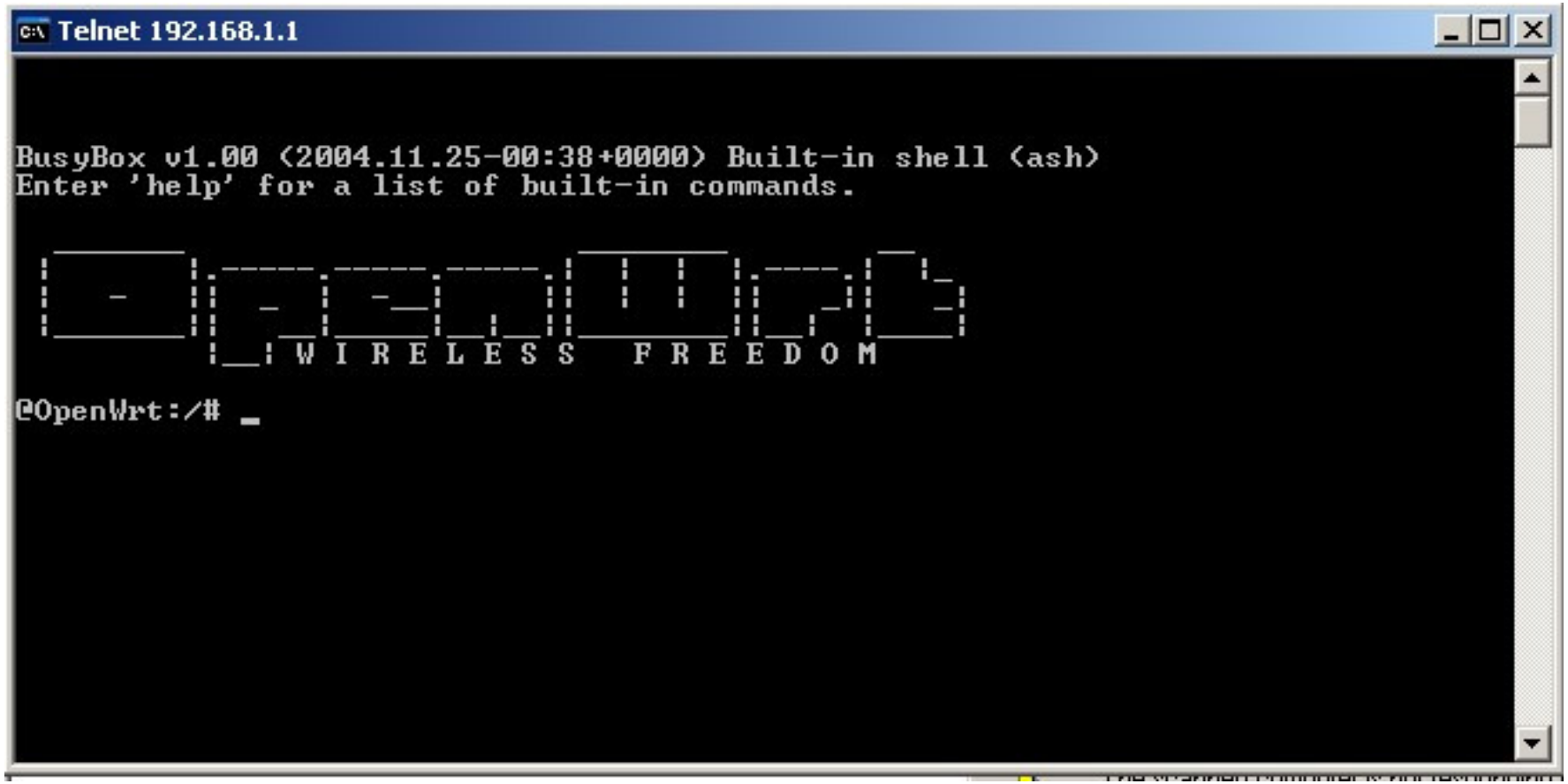
```
# cd /root/buildroot
# tftp 192.168.1.1
tftp> binary
tftp> rexmt 1
tftp> trace
Packet tracing on.
tftp> put openwrt-gs-code.bin
```

Router resetten, warten und starten lassen...

OpenWRT - Einloggen

Der Telnet-Server kann nun erreicht werden

```
# telnet 192.168.1.1
```



OpenWRT - Dateisystem

jffs2-Partition

- komprimiert
- meistens symlink

Aus diesem Grund müssen die Dateien, welche verändert werden sollen zuerst in den beschreibbaren Bereich des Speichers kopiert werden.

OpenWRT - Konfiguration

Konfiguration wird im NVRAM gespeichert

```
@OpenWrt:/# nvram show
```

OpenWRT liest die Werte aus dem NVRAM aus, kann aber auch mit Scripts gesteuert werden

OpenWRT - Konfiguration

SSID einstellen

```
@OpenWrt:/# nvram set wl0_ssid=node01
@OpenWrt:/# nvram commit
@OpenWrt:/# nvram get wl0_ssid
node01
@OpenWrt:/#
```

OpenWRT - Erweiterungen

ipkg ist yum oder apt-get sehr ähnlich, jedoch extrem schlank

```
@OpenWrt:/# ipkg install dropbear
```

OpenWRT - Möglichkeiten

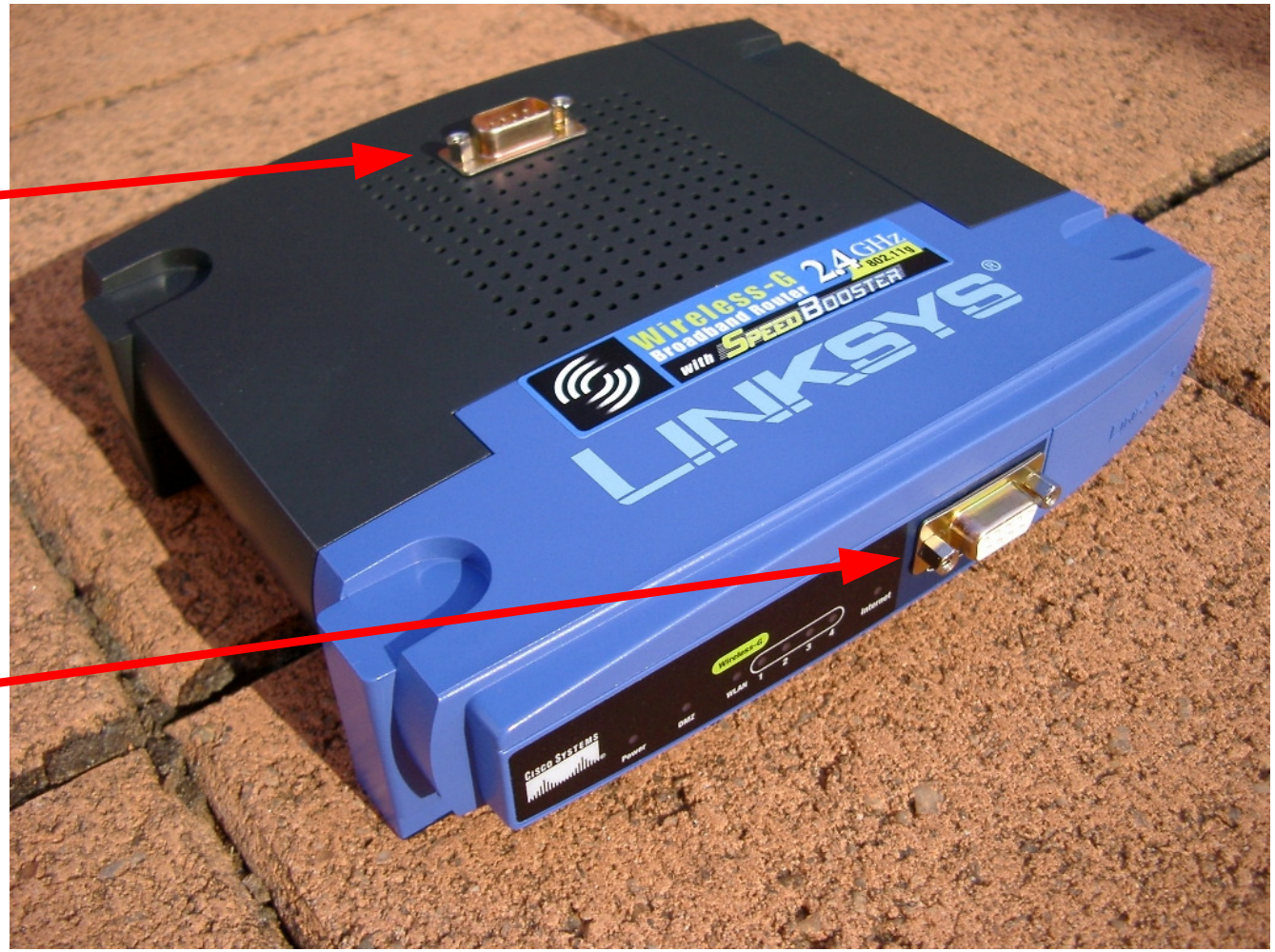
Wireless-Client
Access-Point
WDS-Mode
Monitor-Mode

Modding am WRT54GS

Serial-Port http://www.rwhitby.net/wrt54gs/serial.html

Modem oder sonstiges serielles Gerät

Konsole



Quellen & Links

- http://www.linksys.com
- http://www.openwrt.org
- http://www.linksysinfo.org/
- http://wiki.skyhub.de/index.php/Hauptseite

WIRELESS COMMUNITY BERNE

Fragen ???

Vielen Dank für die Aufmerksamkeit