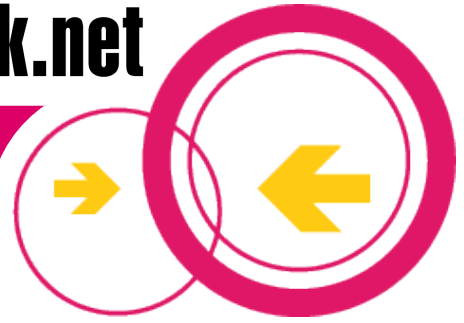
freifunk.net

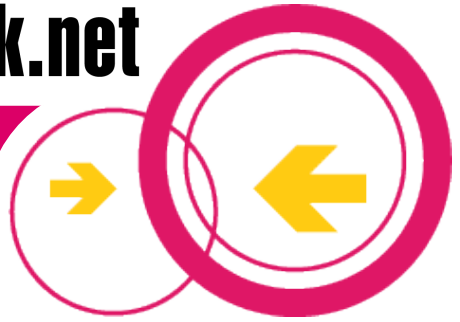


Brainwashing La Fonera

Mehr Spaß am Gerät

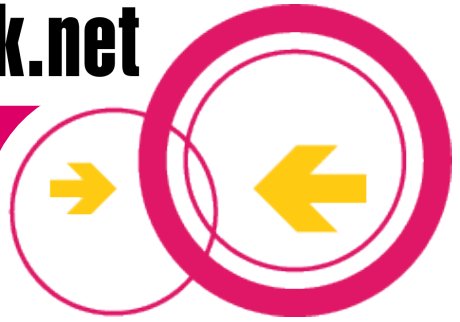
Zusammenstellung von
Mikolas „knox“ Bingemer

Easter(h)egg 2007
Hamburg



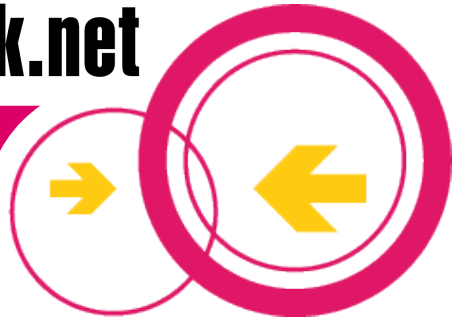
La Fonera

- ACCTON MR3201A
  http://www.accton.com/products/Datasheet/MR3201A.pdf
- Atheros System-on-Chip (SoC)
  http://www.atheros.com/pt/bulletins/AR5006AP_GBulletin.pdf
  - MIPS 4KEc V6.4 Prozessor
  - IEEE 802.11b, 802.11g
  - IEEE 802.11i (WEP, TKIP, AES)
- 16MB RAM, 8MB Flash



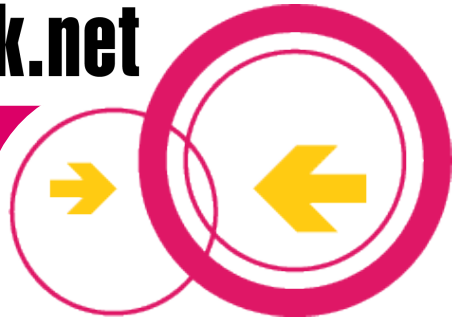
OpenWRT

- Freie Plattform für Embedded Linux
  http://dev.openwrt.org
- OpenWRT Kamikaze für Atheros SoC
  http://wiki.openwrt.org/OpenWrtDocs/Hardware/Fon/Fonera
- Vorkompilierte Snapshot Images
  http://downloads.openwrt.org/snapshots/atheros-2.6/
- Vorkompilierte Softwarepakete (OLSRD, X-Wrt, uvm.)
  http://ipkg.k1k2.de/packages/



Hacking La Fonera

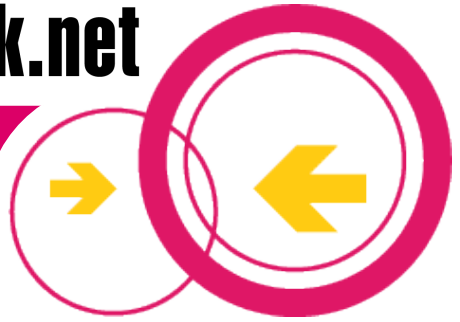
- Hacking La Fonera
  Aktivierung des SSH Daemons und Freischaltung der Ports
  http://stefans.datenbruch.de/lafonera/
  - Code Injection Script „Fondue“
    Remote Command Execution über das Webinterface
    http://stefans.datenbruch.de/lafonera/#fondue
  - Kolofonium Hack
    Kombiniert DNS Spoofing und Bash Scripting
    http://stefans.datenbruch.de/lafonera/#kolofonium



Serielle Schnittstelle

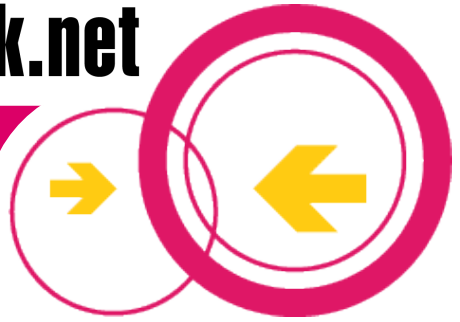
- Nullmodem: RX --> TX
- Terminal
  - 9600 Baud
  - 8 Bits
  - Keine Parität
  - 1 Stopbbit
  - Kein Handshake
    http://wiki.freifunk-hannover.de/FoneraTTY

Serielle Schnittstelle



RedBoot

- Open Source Bootloader
  http://ecos.sourceware.org/docs-latest/redboot/redboot-guide.html
  - Persistente Konfiguration
    http://ecos.sourceware.org/docs-latest/redboot/persistent-state-flash.html
    fconfig -l -n
    fconfig <parameter> <wert>
  - Ethernet Zugriff aktivieren
    fconfig bootp_my_ip 192.168.1.1
    fconfig gdb_port 31337

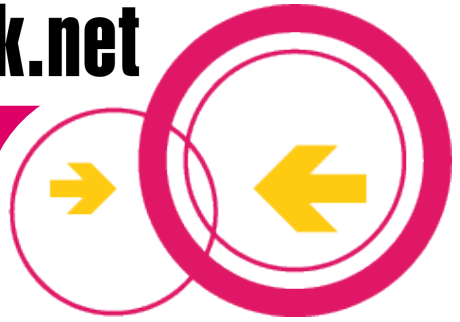


Flashen mit RedBoot

- Flash Image System (FIS)
  http://ecos.sourceware.org/docs-latest/redboot/flash-image-system.html
  - root-Dateisystem und Kernel überschreiben

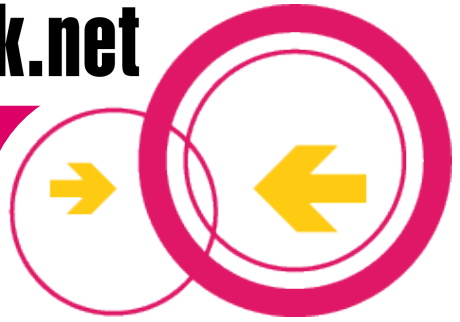
    fis init
    load -r -v -b %{FREEMEMLO} openwrt-atheros-2.6-root.jffs2-64k -m ymodem
    fis create -f 0xA8030000 -l 0x00700000 -e 0x00000000 rootfs
    load -r -v -b %{FREEMEMLO} openwrt-atheros-2.6-vmlinux.lzma -m ymodem
    fis create -r 0x80041000 -e 0x80041000 vmlinux.bin.l7
  - System booten

    fis load -l vmlinux.bin.l7
    fis exec



Flashen über Ethernet

- Übertragung mit tftp
  - Netzwerk konfigurieren
    ip_addr -h <server_ip> -l <fonera_ip>/24
  - root-Dateisystem und Kernel überschreiben
    fis init
    load -r -v -b %{FREEMEMLO} openwrt-atheros-2.6-root.jffs2-64k
    fis create -f 0xA8030000 -l 0x00700000 -e 0x00000000 rootfs
    load -r -v -b %{FREEMEMLO} openwrt-atheros-2.6-vmlinux.lzma
    fis create -r 0x80041000 -e 0x80041000 vmlinux.bin.l7
  - System booten
    fis load -l vmlinux.bin.l7
    fis exec



Netzwerk einrichten

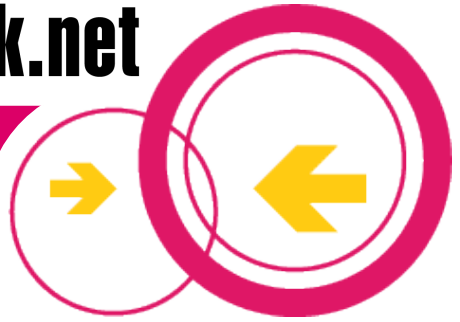
- /etc/config/network
  - IP-Adresse automatisch beziehen

```
config interface wan
        option ifname   eth0
        option proto    dhcp
```

  - IP-Adresse manuell setzen

```
config interface lan
        option ifname   eth0
        option proto    static
        option ipaddr   169.254.255.1
        option netmask  255.255.255.0
```

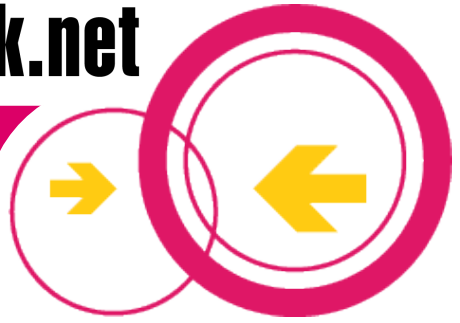
http://wiki.openwrt.org/OpenWrtDocs/KamikazeConfiguration



Wireless einrichten

- /etc/config/wireless

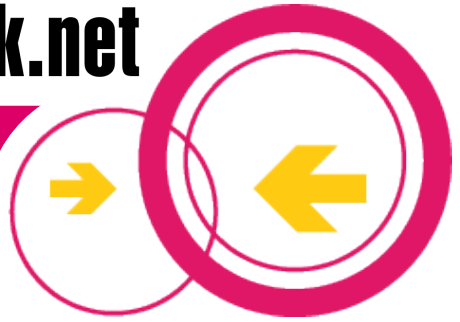
```
config wifi-device  wifi0
        option type     atheros
        option channel  1

config wifi-iface
        option device   wifi0
        option mode     adhoc
        option ssid     hannover.freifunk.net
        option bssid    CA:FF:EE:CA:FF:EE
        option encryption none
```



Wireless einrichten

- /etc/config/network

```
config interface wlan
        option ifname   ath0
        option proto    static
        option ipaddr   10.2.25.65
        option netmask  255.255.0.0
```



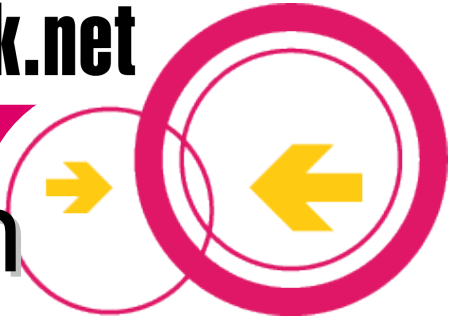
Antennen konfigurieren

- /etc/sysctl.conf
  - Diversity abschalten, RX- und TX-Antenne setzen

    ...
    dev.wifi0.diversity=0
    dev.wifi0.rxantenna=1
    dev.wifi0.txantenna=1
  - Reichweite optimieren

    ...
    dev.wifi0.ctstimeout = 25
    dev.wifi0.acktimeout = 25
    dev.wifi0.slottime = 11

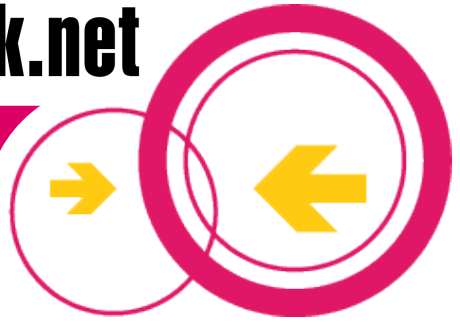
    http://madwifi.org/wiki/UserDocs/LongDistance



DNS und DHCP einrichten

- /etc/dnsmasq.conf

```
local=/.hannover.freifunk.net/
domain=hannover.freifunk.net
expand-hosts

server=195.50.140.250
server=212.222.128.68
server=62.26.26.62

dhcp-range=wlan,10.2.25.81,10.2.25.95,255.255.0.0,23m
dhcp-authoritative
dhcp-leasefile=/tmp/dhcp.leases
except-interface=eth0
```

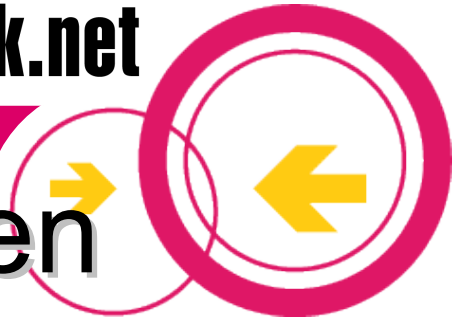


Firewall konfigurieren

- /etc/firewall.user
  - Forwarding aktivieren

    ### Act as Router
    iptables -A forwarding_rule -j ACCEPT
  - SSH Zugang öffnen

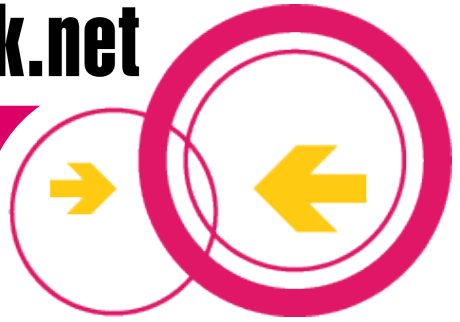
    ### Open port to WAN
    ## -- This allows port 22 to be answered by (dropbear on) the router
    iptables -t nat -A prerouting_wan -p tcp --dport 22 -j ACCEPT
    iptables -A input_wan -p tcp --dport 22 -j ACCEPT



Paket-Quellen konfigurieren

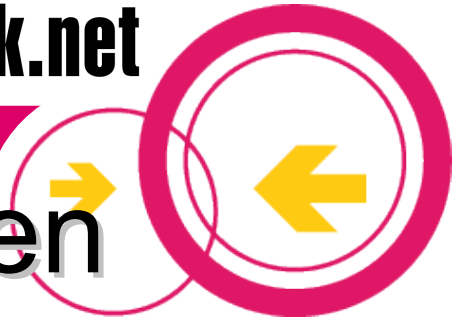
- /etc/ipkg.conf

```
src snapshots http://downloads.openwrt.org/snapshots/atheros-2.6/packages
src heini66 http://ipkg.k1k2.de/packages
dest root /
dest ram /tmp
```



OLSR

- OLSR Daemon und Module installieren
  ipkg update
  ipkg install olsrd olsrd-mod-nameservice olsrd-mod-dyn-gw olsrd-mod-httpinfo
- Konfigurieren
  http://wiki.freifunk-hannover.de/Fonera_mit_OLSR#OLSR_konfigurieren
- Daemon aktivieren und starten
  /etc/init.d/olsrd enable
  /etc/init.d/olsrd start
- HTTP-Info Webinterface
  http://<fonera-ip>:8080/



FON Funktionen nachbilden

- Heartbeat Script
  http://fon.freddy.eu.org/heartbeat/
- FON's Chillispot unter OpenWRT
  http://mrmuh.blogspot.com/2007/01/chillispot-for-openwrt-for-fon.html