

Fonera WLAN-Router Konvertierung für das HAMNET

Sebastian Kricner
DL1KSE

2012

<http://tuxwave.net>

Warnung:

Der Betrieb eines WLAN Gerätes auf
Frequenzen ohne Zulassung, wie z.B einer
Zulassung für die Teilnahme am
Amateurfunkdienst ist eine
Ordnungswidrigkeit und wird mit hohen
Bußgeldern geahndet.

Inhaltsverzeichnis

Vorwort.....	1
Kurzumriss Packet-Radio und HAMNET.....	2
Das alte Packet-Radio Netz.....	2
Review altes Packet-Radio Netz.....	4
Das HAMNET.....	5
IEEE 802.11 Technik im HAMNET.....	6
WLAN-Hardware.....	6
Atheros-Chipsatz.....	6
Fonera WLAN-Router.....	6
Fonera WLAN-Router Konvertierung.....	7
Allgemeine Information.....	7
Vorbereiten des Fonera.....	7
SSH-Zugriff freischalten.....	7
RedBoot für den Zugriff per Telnet vorbereiten.....	7
DD-WRT aufspielen.....	8
Den Fonera frequenzmäßig freischalten.....	8
Die WLAN MAC-Adresse ändern.....	8
Fonera HAMNET Konfiguration.....	9
Weitere Software auf den Fonera installieren.....	10
Monitor Modus mit dem Fonera.....	10
Eigene Scripte beim Bootup starten.....	12
DD-WRT SuperChannel ohne Aktivierung.....	12
OpenWRT und SuperChannel?.....	12

Vorwort

Das neue HAMNET ermöglicht schnelleren Datentransport als das alte Packet-Radio Funknetz. Da das alte Packet-Radio Funknetz als Folge des langsamen Datentransport oft nur noch sehr wenig genutzt wird, existieren auch immer weniger Digipeater. In Folge werden oft die Linkstrecken zu den noch verbleibenden Digipeatern durch getunnelte Verbindungen über das Internet ersetzt. Dies hat eine Fehlversorgung für den am funkgebundenen Datenaustausch interessierten Funkamateureur zur Folge.

Diesem Trend soll durch Einsatz modernerer Verfahren entgegengewirkt werden.

Das modernere Netz wird HAMNET genannt, eine Abkürzung für Highspeed Amateurradio Multimedia Network.

Das HAMNET wird auf Basis des IEEE 802.11 Standard betrieben.

IEEE 802.11 ist allgemein als Wireless Local Area Network (WLAN) oder auch WiFi bekannt.

Es ist ein Verfahren für die funkgebundene Datenübertragung für Computernetzwerke.

Es ermöglicht mit einigen Abwandlungen die funkgebundene Übertragung von Ethernet Frames (IEEE 802.3).

Der Einsatz im HAMNET ist mit einigen kleinen Details gleich.

Dieses Dokument beschreibt die Konversion eines Fonera WLAN-Routers für die Teilnahme am HAMNET.

Kurzumriss Packet-Radio und HAMNET

Das alte Packet-Radio Netz

Das ursprüngliche Packet-Radio Funknetz war seiner Zeit Vorreiter des Internets und erlaubte den Aufbau unterschiedlicher Systeme. So ermöglicht das Packet-Radio Funknetz den Austausch von Nachrichten per Mailboxen. Aber auch viele andere hilfreiche Anwendungen sind im Einsatz, so ermöglicht z.B ein sogenannter DX-Cluster in kurzer Zeit andere Funkamateure über neue DX-Verbindungen zu informieren.

Das Packet-Radio Netz hat jedoch einige größere Schwachstellen. Im Nachfolgenden werden einige solcher kurz behandelt.

Routing

Das Packet-Radio Netz nutzt vorwiegend als Transportprotokoll AX.25, aber auch sind NET/ROM und ROSE im Einsatz. Es ist somit notwendig an Netzübergängen in Netze mit verschiedenen Protokollen ein Protokoll in ein anderes umzusetzen.

Für das Routing von NET/ROM wird überwiegend der Software-Router TheNetNode (TNN) verwendet. Für AX.25 ist überwiegend Flexnet im Einsatz. Für den Austausch von Routen zwischen Flexnet und TNN ist entsprechende Software notwendig. So unterstützt z.B XNet den Austausch von Routen zwischen Flexnet und TNN.

Da die Anzahl der umsetzenden Knoten beschränkt ist, ist bei Ausfall derer keine Erreichbarkeit in Netzbereichen mehr gegeben. Dieser Umstand ist derzeit durch den Abbau an Knoten durch die geringer werdende Nutzung des Packet-Radio Netzes bedingt. Es sei anzumerken, dass die Stabilität des Packet-Radio Netzes durch öfteren witterungsbedingten Ausfall von Linkstrecken nicht überall gegeben ist, so dass die Wahrscheinlichkeit für alternative Routen zu derartiger Knoten weniger gegeben ist.

Dies bedeutet, dass insbesondere für funkbasierende Datennetze die Verfügbarkeit an möglichst vielen Linkstrecken und bei Verwendung verschiedener Protokolle die Anzahl der umsetzenden Knoten wichtig ist.

Auch besteht von Seiten der Software-Router das Problem der beschränkten Anzahl an Routen, die im System verwaltet werden können, so lassen sich mit Flexnet ca. 620 Routen im System unterbringen. Dies brachte das Packet-Radio Netz an den Rand der Leistungsfähigkeit und ermöglichte dennoch keine Erreichbarkeit aller Nodes.

Auf Grund der weniger werdenden Anzahl an Digipeatern ist es oftmals notwendig, die Linkstrecken alternativ über das Internet zu realisieren. In diesem Zusammenhang wurde zur Behebung des Problems der beschränkten Anzahl an Routen und zur Zusammenfassung der über das Internet geführten Linkstrecken eine Software namens IGATE entwickelt, welche es unter anderem ermöglicht viel mehr Routen zu verwalten. Dies kann jedoch weiterhin nicht alle Probleme im Routing lösen.

Engpässe in der Datenübertragung

Da das Packet-Radio Netz ebenfalls zu den Nutzerdaten gleichzeitig auch Daten anderer Dienste übertragen muss, hat dies eine Auslastung der verfügbaren Bandbreite zur Folge, so dass zeitkritische Daten sehr spät beim Empfänger eintreffen. Auf Grund der geringen Geschwindigkeit in großen Teilen des Netzes lässt sich dieses Problem leider auch nicht lösen, in dem man eventuell z.B Nachrichten der Mailboxen zu bestimmten Uhrzeiten sendet. Es ist keine Priorisierung für einzelne Datenpakete möglich. Dies könnte das Packet-Radio Netz für den einzelnen Nutzer erträglicher machen. Angenommen, die Zahl der Nutzer ist beschränkt, wäre ein Transport der Daten von den Mailboxen gleichzeitig möglich, wobei aber die Daten des Nutzers einen höheren Rang haben. Da aber auch DX-Cluster Daten transportiert werden, welche möglichst schnell im Netz verbreitet werden sollen, ist dies mit den geringen Übertragungsbandbreiten nicht einfach zu lösen.

Darüber hinaus muss jedes Paket einzeln bestätigt werden, was zusätzlich zu den ohnehin hohen Latenzen der Ansteuerung der Funkgeräte, der Erkennung der freien Frequenz und ggf. dem Demand Assigned Multiple Access (DAMA) eine weitere Verringerung des Durchsatzes zur Folge hat.

Das AX.25 Protokoll

Die Daten im Packet-Radio Netz werden über das sogenannte AX.25 Protokoll übertragen. Es ist eine Modifikation des ursprünglichen X.25 Protokolls. Es wurden Optimierungen vorgenommen, so dass beispielsweise einige Merkmale des X.25 für einen geringeren Protokoll-Overhead entfernt wurden und Verbesserungen für eine stabile Datenübertragung über Funk implementiert wurden. Diese Änderungen umfassen insbesondere das Timing und Retransmission bzw. Nachforderung verloren gegangener oder fehlerhaft übertragener Daten. Diese Modifikationen waren insbesondere deshalb notwendig, da meistens die Daten per Audio-Injektion am Funkgerät eingespielt wurden und die Ansteuerung der Funkgeräte je nach Typ und Konfiguration sehr unterschiedlich ausfielen. So musste z.B das Einschalten des Senders berücksichtigt werden in Hinsicht auf Einschwingverhalten, Relaisansteuerungen uvm. In Folge sind die AX.25 Frames sehr klein, was auch vorteilhaft ist, jedoch durch die hohen Latenzen zwischen Senden und Empfangsumschaltung einen geringen Datendurchsatz verursacht.

Review altes Packet-Radio Netz

Auf Grund der Schwächen des Packet-Radio Netzes gibt es nur noch wenige Nutzer. Viele Funkamateure sind auf das allgemeine Internet umgestiegen, welches in Verbindung mit modernen Access-Technologien schnelle Datendurchsätze zur Verfügung stellt. Eine zeitnahe Kommunikation ist kaum möglich. Das Packet-Radio Netz eignet sich nicht für die Übertragung von zeitkritischen Datenströmen. Dies ist insbesondere bei Events ein Problem, wenn viele Funkamateure beispielsweise auf eine Mailbox eines aktuellen Projektes zugreifen wollen. Siehe z.B das Bojen Experiment einige Jahre zuvor am Bodensee. Auch können Funkamateure so keine zeitkritischen Datenströme erhalten, für Anwendungen, wie etwa ferngesteuerter Funkstationen, Amateurfunkfernsehen, Messdaten usw.

Ein Einsatz des HAMNETs für „antennengeschädigte“ Funkamateure für die Steuerung von z.B ferngesteuerter Funkstationen wäre denkbar. In Städten gibt es allgemein immer mehr Störungen von Geräten unterschiedlicher Art.

Diesen Mißstand zu beseitigen sollte höchste Priorität besitzen, ist aber leider sehr schwer zu beseitigen.

Das HAMNET

Das HAMNET baut im Allgemeinen auf den bewährten Technologien des Internets auf. Es sollen zunächst im Folgenden die Schwächen des Packet-Radio Netzes in Hinsicht auf das HAMNET untersucht werden.

Routing

Im HAMNET wird allgemein die TCP/IP Protokollsuite eingesetzt. Dies geschieht zunächst für das IPv4 Protokoll. Eine Einführung des IPv6 Protokolls ist ohne größere Umstellungen möglich. Das AX.25 Protokoll kann über Tunnels über IP übertragen werden, sofern gewünscht. Für das Routing von IP Protokollen stehen viele Möglichkeiten zur Verfügung. Wie im Packet-Radio Netz kann man feste Routen vorgeben oder dynamisch über sogenannte Routing-Protokolle erhalten. Feste Routen eignen sich nicht für Austauschknotten. So kommen im HAMNET ebenso automatische Verfahren für den Austausch der Routing-Informationen zum Einsatz. Diese Verfahren haben sich bereits im Internet als robust erwiesen. Im HAMNET kommt das BGP (Border Gateway Protokoll) zum Einsatz. Durch verschiedene Möglichkeiten und allgemeiner Auslegung für den Betrieb mit großen Routing-Tabellen ist ein Engpass hier nicht zu erwarten.

Engpässe in der Datenübertragung

Im HAMNET kommt IEEE 802.11 zum Einsatz.

Da IEEE 802.11 für die Übertragung von IEEE 802.3 Ethernet Frames ausgelegt ist, lassen sich hier Technologien anwenden, welche es ermöglichen, die Frames so zu erweitern, dass Informationen über die Priorität eines Datenpakets übertragen werden. In Zusammenarbeit mit TCP/IP lassen sich Informationen über die Priorität eines Datenpakets auch auf der Layer 2 Ebene (Frame) abbilden (CoS). Dieses Verfahren nennt sich Quality of Service und ist als IEEE 802.1p spezifiziert. Aber ansonsten ist im Allgemeinen eher eine Priorisierung auf Layer-3 Ebene denkbar. Hierzu nutzt man sich des Modells der Differentiated Services (DiffServ). Es lassen sich durch dieses Verfahren, was von vielen Netzwerkgeräten bereits unterstützt wird Datenströme priorisieren. So wäre eine Übertragung kritischer Informationen bei ansonsten ausgelasteter Verbindungen zu einem höheren Grad sichergestellt.

Im Allgemeinen kann auch bei IEEE 802.11 Übertragungsschwierigkeiten kommen, jedoch lassen sich größere Datenmengen mit einer höheren Übertragungsgeschwindigkeit übertragen. Durch sogenanntes Windowing kann die Menge an zu übertragender Information pro Frame automatisch verkleinert oder vergrößert werden. So reduziert sich bei guter Verbindung die Anzahl der Bestätigungen.

Das TCP/IP Protokoll

Im Gegensatz zum Packet-Radio Netz werden mehrere Protokolle zur Übertragung eingesetzt. Dies ist dem OSI-Schichtenmodell konform. Dies verursacht zwar einen größeren Protokoll-Overhead, ist jedoch im Vergleich zu den geringen Geschwindigkeiten im Packet-Radio Netz nicht so ausgeprägt. Die verschiedenen Protokolle implementieren verschiedene Verfahren zur Übertragung von Daten über verschiedene Verbindungen. So kann wie bereits erwähnt die Datenmenge erhöht oder verringert werden, je nach Qualität der Verbindung. TCP/IP soll hier nicht weiter behandelt werden, es sei aus entsprechende Literatur verwiesen.

IEEE 802.11 Technik im HAMNET

WLAN-Hardware

Die im HAMNET verwendete Hardware ist grundsätzlich allgemein verfügbar. Diese Geräte sind also im Allgemeinen reine Konsumerprodukte. Verwendet werden aber auch Spezialversionen für Einsatzzwecke für den Militär oder Firmen mit speziellen Frequenzzuweisungen. Jedoch ändert sich am Verfahren der Übertragung nicht wesentlich. Lediglich werden die Geräte auf andere Frequenzen und Bandbreiten eingestellt, so dass diese nunmehr auf Frequenzen des Amateurfunkdienstes senden.

Eingesetzt werden bei den Austauschstationen vorwiegend Router von Mikrotik mit WLAN-Zusatzkarten vorwiegend auf Atheros-Basis.

Auch als Nutzerhardware werden vorwiegend Geräte auf Atheros-Basis eingesetzt.

Eine Liste von Geräten mit Atheros Chipsatz ist z.B hier zu finden:

<http://atheros.rapla.net/>

<http://wiki.openwrt.org/toh/start>

Atheros-Chipsatz

In WLAN Geräten werden verschiedene Chipsätze verwendet.

Der Hersteller Atheros stellt beispielsweise solche her.

Da es jedoch auch Bedarf für Spezialfälle, wie z.B dem Militär an diesen Chips gibt, stellt Atheros die Chips so her, dass diese sich durch schreiben spezieller Register im Chip bzw. unter Verwendung spezieller Firmware auch auf anderen Frequenzen verwendet werden können. Diese umfassen auch die Frequenzen für den Amateurfunkdienst.

Infos:

<http://www.qsl.net/kb9mwr/projects/wireless/modify.html>

<http://www.qsl.net/kb9mwr/projects/wireless/ham-how-to.html>

Der Fonera WLAN-Router basiert auf einem Atheros Chipsatz und eignet sich somit für den Einsatz für das HAMNET.

Fonera WLAN-Router

Der Fonera WLAN-Router ist ein Gerät, welches von <http://www.fon.com> vertrieben wird. Dieses Gerät wird normalerweise zur kostenpflichtigen Bereitstellung einer Internetverbindung für Außenstehende betrieben. Der Besitzer des Gerätes kann somit etwas Geld mit der eigenen Internetverbindung verdienen.

Für die Konvertierung eines Foneras liegen überwiegend Erfahrungen mit dem 2100 Modell vor. Der Autor hat sein Gerät von DL8RDS überlassen bekommen.

Das Gerät kann jedoch auch auf Ebay oder Flohmärkten etc. gefunden werden.

Fonera WLAN-Router Konvertierung

Allgemeine Information

Auf den Fonera kann grundsätzlich nicht ohne weiteres soweit zugegriffen werden, dass eine Konvertierung möglich ist.

Es stehen wahlweise zwei Möglichkeiten zur Verfügung:

- Zugriff über serieller Schnittstelle auf dem Fonera
- Zugriff über SSH und Telnet

Es wird beschrieben, wie eine Konvertierung ohne dem Zugriff auf die serielle Schnittstelle möglich ist.

Für den Zugriff über die serielle Schnittstelle braucht man einen Wandler, welcher die Signalspannungen von der seriellen Schnittstelle des Computers umwandelt auf 3.3V.

Statt einer seriellen Schnittstelle des Computers wird oft auch USB zu einem USB-Seriell Wandler Chip verwendet, dessen Signale wiederum auf 3.3V umgesetzt werden.

Solche Wandler werden oft für die Arbeit mit Mikrocontrollern verwendet und sind z.B auf Ebay zu finden. Stichworte wären:

usb ttl 3.3V

Vorbereiten des Fonera

Wenn das Gerät zuvor in Betrieb war, ist es notwendig das Gerät auf die älteste Firmware zurückzusetzen.

Hierfür ist es notwendig folgende Prozedur einige Male durchzuführen:

Es darf kein Netzkabel angeschlossen sein.

Drücken des Reset Knopfes für 20-30 Sekunden auf der Unterseite.

SSH-Zugriff freischalten

Die älteren Firmware Versionen des Fonera haben Sicherheitslücken im Webinterface.

Durch diese ist es möglich den SSH-Dämon auf dem Fonera zu starten, so dass man auf den Fonera zugreifen kann.

Das Verfahren wird auf folgender Seite beschrieben:

<http://stefans.datenbruch.de/lafonera/>

Je nach dem welche Firmware-Version man hat, sind die Verfahren unterschiedlich.

Bei dem Autor war fondue.pl erfolgreich im Einsatz.

Statt dem Perl-Script kann man es auch manuell durchführen, wenn man die jeweilige Sicherheitslücke verstanden hat.

RedBoot für den Zugriff per Telnet vorbereiten

<http://wiki.openwrt.org/toh/fon/fonera>

- Enabling Telnet into RedBoot, WITHOUT Serial Access

Für den Telnet-Zugriff innerhalb der 10 Sekunden nach dem Reboot:

```
echo -e "\0377\0364\0377\0375\0006" >break.bin; nc 192.168.1.254 9000 < break.bin;telnet  
192.168.1.254 9000
```

DD-WRT aufspielen

DD-WRT für den Fonera runterladen:

<http://dd-wrt.com/site/support/router-database>

- Nach „Fonera“ suchen
- Das aktuelle Release runterladen (linux.bin)
- Einen tftp Server auf einem lokalen Rechner installieren
- linux.bin in das Verzeichnis vom tftp verschieben
- Ab Schritt 4. von <http://dd-wrt.com/routerdb/de/download.php?file=3592>

Den Fonera frequenzmäßig freischalten

Man benötigt einen Schlüssel für die Freischaltung des sogenannten „SuperChannel“ Feature von DD-WRT:

http://www.dd-wrt.com/shop/catalog/product_info.php?products_id=717

Wenn man nach der Aktivierung die SuperChannel Funktion im DD-WRT Webinterface aktivieren möchte, vorher erst einen Kanal im AP Modus fest einstellen, sonst besteht die Gefahr, dass das Gerät nach dem Aktivieren auf einer ungewollten Frequenz sendet.

Die WLAN MAC-Adresse ändern

Für den Einsatz im HAMNET sollte man das eigene Rufzeichen in die MAC Adresse kodieren. Das Verfahren wird hier beschrieben:

<http://db0fhn.efi.fh-nuernberg.de/doku.php?id=projects:wlan:proposal>

Am einfachsten geschieht dies durch die Scripte, welche man am unteren Seitenende vorfindet.

Um die MAC-Adresse nun zu ändern:

Auf den Fonera per SSH einloggen und folgenden Befehl ausführen:

- `cat /dev/mtdblock/6 > /tmp/board_config`

Anschließend die board_config vom Fonera per scp runterladen (auf einem Rechner):

- `scp root@fonera_ip:./tmp/board_config board_config`

Die Datei board_config ist nun mit einem Hex-Editor zu ändern.

Die WLAN-MAC Adresse findet man als Offset 0x60.

Nun ist nach dem Editieren die board_config wieder auf den Fonera zu übertragen (am besten in /tmp) und wieder in den Flash-Speicher zu schreiben:

- `mtd -f write /tmp/board_config mtd6`

Anschließend den Fonera neu starten.

Fonera HAMNET Konfiguration

Für den Einsatz des Foneras im HAMNET ist zunächst im Webinterface SuperChannel zu aktivieren. Sollte sich der Fonera zu dem Zeitpunkt im AP Modus eingestellt sein, so ist explizit eine für die Allgemeinheit zugelassene Frequenz einzustellen, so dass der Fonera nach Aktivierung des SuperChannel Feature nicht auf unlizenziierten Frequenzen sendet.

Wichtiger Hinweis:

Für nachfolgende Konfiguration im „Client Bridge“ oder „Client“ Mode ist es notwendig in die „Scanlist“ Konfigurationseinstellung im Webinterface die Frequenz des HAMNET-Knotens einzugeben. Ansonsten könnte es sein, dass der Fonera bei fehlendem Empfang des Knotens versucht sogenannte Probe-Request Anfragen auf allen möglichen Frequenzen zu senden. Dies würde auch auf unlizenziierten Frequenzen geschehen.

Für den Betrieb im HAMNET wählt man wahlweise „Client Bridge“ oder „Client“ als Modus. Der Einsatz des Mode „Client Bridge“ sollte nur dann eingesetzt werden, wenn das Subnetz des HAMNET-Knotens über genügend IP-Adressen verfügt. D.h dieser Einsatz wäre z.B bei nur einem PC im eigenen LAN zu empfehlen. In diesem Falle wäre auch nur Kommunikation zum HAMNET möglich, sofern keine weiteren Einstellungen hinsichtlich der IP-Adressierung und der Routen auf dem Computer vorgenommen werden. Insbesondere bei Adressbezug durch DHCP wird im Normalfall immer nur eine IP-Adresse auf einem Interface konfiguriert. Somit ist eine sekundäre Adresse für ein eigenes Netzwerk gesondert zu konfigurieren.

Für die meisten Fälle wird der „Client“ Mode verwendet, d.h für eigene LAN mit mehreren Computersystemen. In diesem Fall fungiert der Fonera selbst als Client und bezieht eine IP-Adresse vom HAMNET-Knoten per DHCP. Das Routing wird hier mit NAT ergänzt, um die Konnektivität für mehrere Computersysteme über die einzelne IP-Adresse zur Verfügung zu stellen. Auch Voraussetzung für das Routing ist, dass der Fonera im gleichen Subnetz ist, wie die Computersysteme. Abschließend ist eine Route für das HAMNET auf den Computersystemen zu setzen, so dass der Fonera als Gateway genutzt wird. Für das HAMNET setzt man eine Route von 44.0.0.0/8.

Weitere Software auf den Fonera installieren

Zunächst ist im Webinterface des Fonera unter Administration jffs zu aktivieren.

Dazu wählt man folgendes aus:

- Enable jffs
- Clean jffs

Anschließend steht eine ca. 1.4 MB große Partition im Flash zur Verfügung.

In diese kann man Dateien speichern und stehen nach einem Neustart weiter zur Verfügung.

Software kann man hier runter laden:

<http://downloads.openwrt.org/kamikaze/8.09.2/atheros/packages/>

Diese lädt man zunächst per wget auf den Fonera:

- cd /tmp
- wget <http://downloads.openwrt.org/...>

Installieren:

- ipkg -d root install package_name.ipk

Empfehlenswert wäre es tcpdump zu installieren.

Benötigt werden hierfür libpcap und tcpdump.

Monitor Modus mit dem Fonera

Man kann den Fonera in den Monitor-Modus schalten, um z.B gefahrlos zu prüfen, ob man einen HAMNET Zugang empfangen kann.

Zunächst sollte man im Webinterface des Fonera unter Wireless den Mode auf Disabled setzen (In der Dropbox mit den Modes „Mixed“, „BG-Mixed“ usw.).

Anschließend könnte man folgendes Script ausführen:

```
#!/bin/sh

echo "Shutting down ath0"
ifconfig ath0 down

echo "Destroying ath0"
wlanconfig ath0 destroy

echo "Creating ath0 in monitor mode"
wlanconfig ath0 create wlandev wifi0 wlanmode monitor

echo "Setting 802.11 type of ath0 for tcpdump"
echo 801 > /proc/sys/net/ath0/dev_type

echo "Enabling superchannel"
echo 1 > /proc/sys/dev/wifi0/superchannel

echo "Listing channels..."
sleep 2
wlanconfig ath0 list chan|less

echo "Setting channel width"
read -p "Please enter channel WIDTH in MHz (5/10/20/40MHz):" channelbw
echo ${channelbw} > /proc/sys/dev/wifi0/channelbw

echo "Setting channel shift"
read -p "Please enter channel SHIFT in MHz (+-15/+-10/+-5/0):" channelshift
iwpriv ath0 channelshift ${channelshift}

echo "Setting channel"
read -p "Please enter freq (format: 2.362G):" freq
iwconfig ath0 freq ${freq}

echo "Setting ath0 up"
ifconfig ath0 up

echo "Now run:"
echo "tcpdump -i ath0 -n -s 2346"
```

Eigene Scripte beim Bootup starten

Das Script muss in /jffs mit aktiviertem jffs abgelegt werden.

Idealerweise erstellt man mit

- mkdir -p /jffs/etc/init.d/

ein „Init“ Verzeichnis.

Anschließend:

- nvram set rc_startup=/jffs/etc/init.d/*
- nvram commit

DD-WRT SuperChannel ohne Aktivierung

Es sollte möglich sein, „SuperChannel“ auch ohne Aktivierung zu nutzen.

Das Vorgehen wurde aber noch nicht getestet:

```
#!/bin/sh
echo 1 > /proc/sys/dev/wifi0/superchannel
echo 0 > /proc/sys/dev/wifi0/regdomain
echo 276 > /proc/sys/dev/wifi0/countrycode
iwpriv ath0 setscanlist +2192-2499
```

Statt +2192-2499 sollte man Frequenzen für HAMNET einsetzen.

Man müsste ggf. auch einige Parameter in Zusammenhang mit SuperChannel im nvram ändern, für das WebInterface.

Übrigens kann man im Webinterface ebenfalls unter „Scanlist“ die Frequenzen setzen.
z.B 2362-2362. Dies ist für den Client Mode relevant.

OpenWRT und SuperChannel?

Eventuell wäre es möglich das Kernel-Modul und den Kernel auch für OpenWRT einzusetzen und so SuperChannel auch mit OpenWRT einzusetzen.