HAMNET – Highspeed Amateurradio Multimedia Network

Jann Traschewski, DG8NGN (jann@gmx.de, dg8ngn@db0fhn.#bay.deu.eu)

TEIL 1
Grundlagen des Highspeed Amateurradio Multimedia Network

Definition

Der Begriff „HAMNET“ steht für Highspeed Amateurradio Multimedia Network. Es handelt sich um ein internationales Projekt zur digitalen Vernetzung von automatisch arbeitenden Amateurfunkstellen. Die gemeinsame Basis des HAMNET ist das TCP/IP-Protokoll unter Verwendung des für Funkamateure zugewiesenen IPv4-Adressbereichs 44.0.0.0/8 (Network 44) und des Routingprotokolls BGP4 (Border Gateway Protokoll), welches auch das Internet zusammenhält. Das HAMNET ist ein nichtöffentliches Netzwerk (Intranet) mit einem begrenzten Nutzerkreis (Funkamateure). Einzelne Netzsegmente können über das Internet oder WLAN (ISM) verbunden werden. Endnutzer können sich neben direktem Funkzugang auch über öffentliche Netze (z.B. dem Internet) unter Verwendung von Authentifizierungsmechanismen in das HAMNET einwählen. Innerhalb des HAMNET gilt jeder als vertrauenswürdig, so dass keine zusätzliche Authentifizierung erfolgen muss.

Geschichte

Die digitale Vernetzung von automatisch arbeitenden Amateurfunkstellen auf Basis des TCP/IP-Protokolls hat eine lange Geschichte.

Bereits im Jahre 1970 hat Hank Magnuski den Klasse A Adressblock 44.0.0.0/8 (http://www.ampr.org) zugewiesen bekommen. Bei der IANA (Internet Assigned Numbers Authority, http://www.iana.org) wird dieser Adressblock als „Amateur Radio Digital Communications“ aufgeführt (http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.txt). Seit einer langen Zeit verwaltet Brian Kantor, WB6CYT, das Netz.

Das „Network 44“ wird auch als „AMPRNet“ bezeichnet. Diese Abkürzung steht für „AMateur Packet Radio Network“ und ist von der Terminologie her an die Betriebsart Packet Radio gebunden. Mittlerweile geht die Nutzung des „Network 44“ aber weit über die Betriebsart Packet Radio hinaus. Daher kann auch das HAMNET ein Teil des AMPRNet sein. Auch der Begriff IPRT für „Internationale Packet Radio Tagung“ wurde mittlerweile mit „Fachtagung für digitale Datenübertragung im Amateurfunk“ untertitelt.

Bei dem Aufbau des Packet Radio Netzes in Deutschland wurde von Anfang an mit der Übertragung von TCP/IP-Paketen über AX.25 experimentiert. Der geschätzte Höhepunkt der Aktivität war Mitte der 90er Jahre und brachte zuletzt das sogenannte „HamWeb“ hervor. Viele Betreiber von Packet Radio Knoten hatten sich entschlossen, auch TCP/IP-Dienste wie HTTP anzubieten. Die Nutzer konnten so im „HamWeb“ surfen.

Im Laufe der Jahre haben die Anzahl der Medien und die verfügbaren Informationskanäle stark zugenommen. Die Attraktivität mit langsamen TCP/IP-über-AX.25-Verbindungen Informationen auszutauschen ging nach und nach verloren. Heute ist es zu einer der vielen Nischen im Amateurfunk geworden.

Der Einsatz von WLAN-Technik im Amateurfunk wurde im Jahr 2005 im Rahmen des Vortrags „PR-Knotensoftware auf embedded Hardware am Beispiel des Linksys WRT54GS“ von Jann Traschewski, DG8NGN, und Thomas Osterried, DL9SAU, angesprochen (http://www.iprt.de/IPRT2005/index.html). Schnell wurde klar, dass durch die Beschränkung von Amateurfunkaussendungen auf 10

MHz Bandbreite die zu der Zeit am Markt verfügbare Hardware in Deutschland nicht im Rahmen des Amateurfunks, sondern nur im lizenzfreien ISM-Band mit entsprechenden Parametern eingesetzt werden kann. Eine weitere Schwierigkeit war die Nutzung von Frequenzen außerhalb des ISM-Frequenzbandes. Jedoch hat Arsene, LX1TB, durch Austausch des Quarzes im Linksys WRT54 Linkstrecken in Luxemburg außerhalb des ISM-Bandes in Betrieb nehmen können (http://www.rlx.lu/~lx1tb/wrt54gs).

Ende 2005 tauchten dann erste Informationen über WLAN-Chipsätze unter dem Begriff „channel cloaking“ von Atheros auf dem Markt auf. Sie ermöglichten WLAN-Endgeräte mit reduzierter Bandbreite von 5MHz bzw. 10 MHz zu betreiben.

Erste Planungen eines digitalen Backbone in Österreich wurden im Jahr 2007 auf der IPRT von Wolf Höller, OE7FTJ, und Robert Kiendl, OE6RKE, vorgestellt (http://www.iprt.de/IPRT2007/talks.html#oe7ftj). Erst eine Änderung des dortigen Amateurfunkgesetzes ermöglichte den Aufbau des heutigen HAMNET im großen Stil in Österreich.

Um den Begriff „HAMNET“ gab es zuletzt einige Verwirrungen. Die Gefahr einer Doppelbelegung dieses Akronyms ist recht hoch. So existiert z.B. bereits ein als „HamNET“ bezeichnetes IRC-Netz (Internet Relay Chat) innerhalb des AMPRNet. Die Verwechslung mit dem HamWeb liegt auch recht nahe. Erweiterungen mit Versionsnummern sorgten zusätzlich für Irritationen. Eine von vielen getragene Variante ist nun das „HAMNET“ in Großbuchstaben ohne Erweiterung und bezeichnet das anfangs beschriebene „Highspeed Amateurradio Multimedia Network“.

Projektziele

Das Gesamtprojekt HAMNET hat sich zum Ziel gesetzt, automatisch arbeitende Amateurfunkstellen mit hohen Bitraten zu einem großen Netz zusammenzuschließen. In einer weiteren Phase möchte man durch Schaffung von High-Speed-Userzugängen die Möglichkeiten für Endnutzer deutlich verbessern.

Selbst wenn man dieses Ziel erstmal nur sekundär betrachtet und primär die Internetversorgung des D-Star- oder Echolinkrepeaters sicherstellen möchte, bietet es sich an, dies auf Basis des HAMNET-Standards durchzuführen. Sollte man sich später entschließen in die großflächige Vernetzung mit einzusteigen, fällt die Erweiterung der Infrastruktur relativ einfach aus.

Das HAMNET dient als Basisplattform zur Vernetzung digitaler Dienste und kann uns u.a. folgende Dienste bereitstellen:

- Packet Radio Interlinkstreckenersatz (AX.25 verpackt in UDP/IP)
- Verlegung der TCP/IP-über-AX.25-Dienste direkt auf IP
- Vernetzung/Steuerung von Voice-Repeatern (SVXLink, Asterisk, TheLinkBox)
- Vernetzung/Steuerung von ATV-Repeatern
- Vernetzung/Steuerung von Digital-Repeatern (D-Star, APCO25, MotoTRBO, NXDN)

Außerdem gibt es u.a. für Endnutzer folgende Möglichkeiten:

- Zugriff auf Remote Transceiver, Voice-Repeater, ATV-Relais und WebSDR
- Zugriff auf Packet Radio und Mailboxen des Winlink2000 Netzwerks

In der Anfangsphase kann das HAMNET sicher noch nicht alles bieten, aber mit dem großflächigen Ausbau werden immer mehr Möglichkeiten erschlossen. Eine ähnliche Entwicklung hat das Packet Radio Netz bereits hinter sich. Nach dem Netzaufbau haben sich die Dienste wie das Mailboxnetz, das Conversnetz, das DX-Clusternetz, das Funkrufnetz und das Sprachmailboxnetz erschlossen.

Das HAMNET wird uns eine Plattform für viele neue Projekte und Experimente innerhalb des Amateurfunks bieten. Die hohen Bitraten und niedrige Latenzzeiten zwischen den Knoten machen das Netz echtzeitfähig und erlauben es z.B. auch, Videostreams über mehrere Zwischenstationen (Hops) verlustfrei zu übertragen. Hier können Synergien mit ATV-Gruppen genutzt werden.

Eine neue Herausforderung für uns Funkamateure stellt die Zugangstechnologie mit hohen Bitraten zum HAMNET dar. Die HAMNET-Interlinktechnik auf Basis von WLAN-Komponenten ist nur bedingt für Endnutzerzugänge geeignet. Auf diesen hohen Frequenzbändern ist direkte Sicht vom Nutzer zum HAMNET-Knoten bis auf wenige Ausnahmen Voraussetzung. Dass es auch anders geht, zeigt uns das Mobilfunknetz der kommerziellen Provider. Erste mögliche Varianten zeigt der Vortrag „Datenübertragung mit OFDM als Zugangstechnik zu HAMNET! Wie könnte es gehen?“ von Michael Hartje, DK5HH, an der IPRT 2010 auf. Zunächst wird das Augenmerk auf den Aufbau der Interlinkstrecken des HAMNET gelegt werden. Zwischenlösungen können in Form von VPN-Zugängen über das Internet einen Zugang zum HAMNET ermöglichen.

Ein weiterer nicht zu verachtender Vorteil liegt in der Tatsache, dass es sich um ein abgeschlossenes Netzwerk handelt. Endnutzer innerhalb des Netzwerks müssen also nicht erst als Funkamateure verifiziert werden.

Das HAMNET bietet auch die Gelegenheit, sich neues Wissen über IT-Technik anzueignen. Vielleicht ist das auch eine Chance für die jüngere Generation gemeinsam mit den „old men“ ein Projekt auf die Beine zu stellen.

Gesetzliche Rahmenbedingungen

Deutschland

Erste Überlegungen WLAN-Komponenten im Amateurfunk einzusetzen scheiterten an der Verordnung zum Gesetz über den Amateurfunk (AFuV, http://bundesrecht.juris.de/bundesrecht/afuv_2005/gesamt.pdf). Unter $1 „Anwendungsbereich“ Ziffer 6. wird auf Anlage 1 verwiesen (Nutzungsbedingungen für die im Frequenznutzungsplan für den Amateurfunkdienst und den Amateurfunkdienst über Satelliten ausgewiesenen Frequenzbereiche). Position 19 und 21 führen die Frequenzbereiche 2320 MHz – 2450 MHz und 5650 MHz – 5850 MHz auf und sind mit den Fußnoten 9 und 13 gekennzeichnet. Die Fußnote 9 besagt, dass die belegte Bandbreite einer Aussendung maximal 10 MHz und bei Fernsehaussendungen maximal 20 MHz sein darf.

Im vierten Quartal 2008 haben wir die Bedingungen ausgelotet, unter denen wir die neue Technik auf unseren Amateurfunkfrequenzen einsetzen können - mit besonderem Augenmerk auf genutzte Bandbreite und Konformität zum DARC-Bandplan. Das Ergebnis dieser Arbeit haben wir dokumentiert (http://db0fhn.efi.fh-nuernberg.de/doku.php?id=projects:wlan:regulations).

Für das 13cm- und 6cm-Band sind nach dem DARC-Bandplan einige Bereiche für „Digital Link“ vorgesehen. Es ergibt sich zunächst folgendes gesetzes- und bandplankonforme Einsatzszenario:

- 2362 MHz +/-2,5 MHz
- 2397 MHz +/-2,5 MHz
- 5675 MHz +/-5 MHz (im ISM-Band)
- 5685 MHz +/-5 MHz (im ISM-Band)
- 5695 MHz +/-5 MHz (im ISM-Band)
- 5815 MHz +/-5 MHz

- 5825 MHz +/-5 MHz

Für automatisch arbeitende Stationen gibt es besondere Auflagen. Zur Erinnerung:

Nach $6 Ziffer 1 des Gesetz über den Amateurfunk (AFuG, http://bundesrecht.juris.de/bundesrecht/afug_1997/gesamt.pdf) ist das Bundesministerium für Wirtschaft und Technologie ermächtigt, die technischen Rahmenbedingungen für automatisch arbeitende Amateurfunkstellen festzulegen. Diese sind in der Verordnung zum Gesetz über den Amateurfunk (AFuV, http://bundesrecht.juris.de/bundesrecht/afuv_2005/gesamt.pdf) unter $13 „Fernbediente oder automatisch arbeitende Amateurfunkstellen“ geregelt. Abermals beschränkt uns hier die Anlage 1 erheblich: „Die maximal zulässige Strahlungsleistung für fernbediente oder automatisch arbeitende terrestrische Amateurfunkstellen beträgt oberhalb 30 MHz 15 Watt ERP“. Für den Individualbetrieb ist je nach Band und Lizenzklasse eine Leistung von bis zu 750 bzw. bis zu 75 Watt PEP erlaubt.

Die Verordnung zum Gesetz über den Amateurfunk sieht mit dem $16 „Technische und betriebliche Rahmenbedingungen für Amateurfunkstellen“ Absatz 2 eine Sonderregelung vor: „Die Regulierungsbehörde kann auf Antrag für besondere experimentelle und technisch-wissenschaftliche Studien mit einer Amateurfunkstelle Ausnahmen befristet gestatten. Dies kann unter zusätzlichen Auflagen erfolgen und von der Zuteilung eines weiteren Rufzeichens abhängig gemacht werden. Die besondere Regelung könnte hier neben der beschränkten Strahlungsleistung auch die begrenzte Bandbreite außer Kraft setzen.“

Auf Basis dieser Regelung wurde im ersten Quartal 2009 ein erster Antrag für eine „Experimentalfunkstelle“ mit genauer Beschreibung an die Bundesnetzagentur gesendet (http://db0fhn.efi.fh-nuernberg.de/doku.php?id=projects:wlan:proposal). Dabei wurde neben dem „wissenschaftlichen Aspekt“ besonders auf den Schutz vor ungewünschten Aussendungen, ausgelöst durch ISM-Anwender, eingegangen. Außerdem wurden mehrere Möglichkeiten der Stationsidentifizierung nach $11 „Rufzeichenanwendung“ der Verordnung zum Gesetz über den Amateurfunk aufgezeigt.

Aus dem Antrag im ersten Quartal 2009 ist bis heute keine Genehmigung hervorgegangen. Nachfragen haben ergeben, dass der Antrag dem Primärnutzer des 13cm- und 6cm-Bandes zur Verträglichkeitsuntersuchung vorliegt.

Diese Situation ist für den als Experimentalfunk charakterisierten Amateurfunk unbefriedigend. Bemühungen, den Missstand zu beseitigen und zufriedenstellende Lösungen für den Amateurfunk zu erwirken, sind im Gange. Wichtig ist, dass bis zu einer endgültigen Lösung dir Primärnutzer nicht durch unüberlegte Aktionen gestört werden, was uns langfristig die Möglichkeit einer Nutzung dieses Bereiches endgültig verbauen könnte.

Schweiz

In der Schweiz sind laut „Vorschriften betreffend den Amateurfunk 1.3 Art. 6 Frequenzbänder“ (http://www.bakom.admin.ch/themen/frequenzen/00689/01560/index.html) 100 Watt PEP auch für automatisch arbeitende Stationen (hier unbediente Stationen) erlaubt. Eine Begrenzung der Bandbreite gibt es nicht. Eine Bewilligung der Konzessionsbehörde (hier BAKOM) für unbediente Stationen dauert wenige Tage. Die Frequenzbereiche 2300 MHz bis 2450 MHz und 5650 MHz bis 5725 MHz sind nur mit Zusatzbewilligung der Konzessionsbehörde nutzbar. Die Bearbeitungszeit liegt bei mehreren Monaten. Der Frequenzbereich 5725 MHz bis 5850 MHz kann ohne Zusatzbewilligung der Konzessionsbehörde genutzt werden.

Österreich

In Österreich sind laut „Verordnung zur Durchführung des Amateurfunkgesetzes“ (BGBl.II.Nr.390/2008 – Novelle, http://www.bmvit.gv.at/telekommunikation/recht/aut/verordnungen/afv.html) $41 für Relaisfunkstellen (speziell „bei Amateurfunk-Fernsehen und bei Verbindung von Netzwerkknoten in Packet-Radio-Netzen“) über 440MHz maximal 200 Watt ERP erlaubt.
Die maximal belegbare Bandbreite beträget nach „Verordnung zur Durchführung des Amateurfunkgesetzes“ (BGBl.II.Nr.455/2003 – Novelle) $10 „für frequenz- oder phasenmodulierte Aussendungen“ 20MHz. Für das HAMNET sind die Frequenzbereiche 2400 MHz bis 2450 MHz, 5670 MHz bis 5760 MHz und 5762 MHz bis 5790 MHz nutzbar (http://wiki.oevsv.at/index.php/Frequenzen_Digitaler_Backbone). Eine Bewilligung ist auch in Österreich nötig und dauert zwischen wenigen Wochen bis zu 6 Monaten.

Folgende Beschränkungen verhindern derzeit den großen Aufbau des HAMNET in Deutschland:

1. Aufbau als Standardanwendung im Amateurfunk im Rahmen der Verordnung zum Gesetz über den Amateurfunk $13 „Fernbediente oder automatisch arbeitende Amateurfunkstellen“ lässt lediglich bis zu 15 Watt ERP zu.

2. Der Frequenzbedarf an einigen Standorten übersteigt bereits jetzt die Verfügbarkeit an Frequenzen nach dem Musterantrag unter Verwendung des $16 Absatz 2 AFuV.

3. Die Laufzeiten vom Antrag einer automatisch arbeitenden Amateurfunkstelle (als Sekundärnutzer) bis zur Erteilung der Genehmigung sind extrem zu hoch. Bisher sind noch keine erteilten Genehmigungen bekannt (Stand: 05.04.2010).

Folgende Anforderungen stellt das HAMNET:

Zu 1.:
Möchte man eine für Amateurfunkverhältnisse stabile und schnelle Verbindung aufbauen, so benötigt man einen Empfangspegel von ca. -66dBm. Linkstrecken werden bevorzugt im 6cm-Band aufgebaut, wobei sich rechnerisch für 15 Watt ERP (41,76dBm) eine Planungsreichweite von ca. 14km ergibt. Für eine Planungsreichweite von 100km benötigt man ca. 500 Watt ERP (57dBm). Mit ISM-Parametern (1 Watt ERP bzw. 30dBm) schafft man 4km.

Eine für uns weitaus flexiblere Lösung könnte eine Beschränkung der „Antenneneingangsleistung“ auf z.B. 1 Watt (30dBm) sein. Unter verpflichtender Angabe des Antennengewinns und Azimut, könnte die Behörde weiterhin die Leistungsbeschränkung kontrollieren.

Zu 2.:
Die bisher vorgeschlagenen Frequenzen für das HAMNET lassen sich in den Digitalbereich des Bandplans integrieren. Eine Trennung zwischen Digital-Bereich und ATV bzw. 10MHz- und 20MHz-Bandbreite erscheint nicht mehr zeitgemäß. Bereits heute wird ATV auf digitalen Linkstrecken übertragen. Eine Neugestaltung des Bandplans unter diesem Aspekt ist angeraten.

Die neue Technik erfordert auch ein Umdenken in der Richtfunkplanung. Verschiedene Polarisationen und schmale Öffnungswinkel ermöglichen einen ökonomischen Umgang mit den einzelnen Frequenzen. Die Simplextechnik ermöglicht unter Einbussen von Geschwindigkeit auch die Mehrfachbelegung von Frequenzen. Mit steigender Nutzung der Interlinkstrecken ist es aber ratsam für genügend Frequenzkapazitäten zur Einzelnutzung zu sorgen.

Zu 3.:
Ein Wechsel von der Genehmigungspflicht zur Meldepflicht zumindest in einigen Teilfrequenzbereichen ist wünschenswert. Dies wird bereits in anderen Ländern oder auch hierzulande für BFWA-Anwendungen (Broadband Fixed Wireless Access, http://www.bundesnetzagentur.de/media/archive/11239.pdf) praktiziert.

Eine Verträglichkeitsprüfung zwischen automatisch arbeitenden Stationen im HAMNET ist nicht notwendig und würde unnötige Kosten verursachen. Die Simplextechnik ermöglicht die Koexistenz mehrere Systeme auf einer Frequenz. Exklusive Frequenzen werden erst notwendig, wenn der Bedarf die Verfügbarkeit massiv überschreitet.

Zusammenfassend fällt auf, dass die gesetzlichen Rahmenbedingungen zur Ausübung des Amateurfunkhobbys leider stark von den nationalen Gegebenheiten abhängen. Der Nischenbereich „automatisch arbeitende Amateurfunkstellen“ innerhalb des Amateurfunks ist davon noch stärker betroffen. Ein klassisches Beispiel ist die Kopplung von Amateurfunk mit dem bzw. über das Internet. In Deutschland wurde dies mit dem Gesetz über den Amateurfunk im Jahre 1997 möglich; in Österreich wurde dies erst viele Jahre später ermöglicht; in der Schweiz war uns noch nie eine Beschränkung bekannt und in Frankreich ist es heute noch verboten. Bzgl. des HAMNET hängt nun Deutschland der Schweiz und Österreich hinterher. Wir bitten um Verständnis, dass hier in Deutschland erst noch die rechtliche Absicherung für das HAMNET-Projekt eingeholt werden muss. In der Zwischenzeit empfiehlt es sich, Bedarf durch Beantragung von HAMNET-Frequenzen nach dem Musterantrag zu zeigen. Wo es technisch möglich ist, sollte innerhalb von ISM-Parametern bereits mit dem Aufbau begonnen werden. Publikationen über das HAMNET helfen, weitere Unterstützung für dieses internationale Projekt einzuholen.

Organisation des Netzwerks

Das HAMNET ist eine Teilmenge des AMPRNet und benötigt zum Betrieb IP-Adressen aus dem Netzwerk 44.0.0.0/8 (44.x.x.x). Die Verwaltung der IP-Adressen wurde von Brian Kantor, WB6CYT, delegiert (http://noh.ucsd.edu/~brian/amprnets.txt). In Deutschland gab es im Oktober 2003 eine öffentliche Wahl der IP-Koordinatoren. Das Team besteht aus den drei Mitgliedern Egbert Zimmermann, DD9QP, Thomas Osterried, DL9SAU, und Thomas Maisl, DL3SBB, welches auch eine Webseite zum Thema „AMPRNet IP Koordination Deutschland“ unterhält (http://www.de.ampr.org). Deutschland ist derzeit der IP-Adressbereich 44.130.0.0/16 zugewiesen (44.130.x.x).

Im Gegensatz zu anderen Ländern sind hierzulande viele IP-Adressen für den Betrieb von TCP/IP über AX.25 Verbindungen in Verwendung. Der bisher belegte Adressraum kann deshalb nicht kurzfristig gelöscht bzw. umgewidmet werden. Daher hat sich das Koordinatorenteam zunächst entschlossen, die bisher ungenutzten IP-Adressbereiche 44.130.192.0/19 (44.130.192.0 bis 44.130.223.255) für das User-/Servicenetz und 44.130.224.0/20 (44.130.224.0 bis 44.130.239.255) für das Backbonenetz dem HAMNET-Deutschland zur Verfügung zu stellen.

Um sich mit der Notation von IP-Netzwerken vertraut zu machen, kann das Tool „ipcalc“ weiterhelfen. Es ist auf dem Linuxsystem DB0FHN-9 auch in Packet Radio verfügbar.

```
dg8ngn@db0fhn:~$ ipcalc -n 44.130.192.0/19
Address:   44.130.192.0         00101100.10000010.110 00000.00000000
Netmask:   255.255.224.0 = 19   11111111.11111111.111 00000.00000000
Wildcard:  0.0.31.255           00000000.00000000.000 11111.11111111
=>
Network:   44.130.192.0/19      00101100.10000010.110 00000.00000000
```

```
HostMin:   44.130.192.1         00101100.10000010.110 00000.00000001
HostMax:   44.130.223.254       00101100.10000010.110 11111.11111110
Broadcast: 44.130.223.255       00101100.10000010.110 11111.11111111
Hosts/Net: 8190                  Class A

dg8ngn@db0fhn:~$ ipcalc -n 44.130.224.0/20
Address:   44.130.224.0         00101100.10000010.1110 0000.00000000
Netmask:   255.255.240.0 = 20   11111111.11111111.1111 0000.00000000
Wildcard:  0.0.15.255           00000000.00000000.0000 1111.11111111
=>
Network:   44.130.224.0/20      00101100.10000010.1110 0000.00000000
HostMin:   44.130.224.1         00101100.10000010.1110 0000.00000001
HostMax:   44.130.239.254       00101100.10000010.1110 1111.11111110
Broadcast: 44.130.239.255       00101100.10000010.1110 1111.11111111
Hosts/Net: 4094                  Class A
```

Die Planung des HAMNET lässt sich nur zu einem gewissen Grad in der Theorie durchführen, da noch nicht abzusehen ist, wie sich das Netz entwickeln wird. Großzügige Reserven im IP-Adressraum sind von Vorteil. Aus dieser Sicht stellt sich die Frage, warum kein Netz mit „privaten“ IP-Adressen nach RFC1918 (ftp://ftp.ripe.net/rfc/rfc1918.txt) genutzt werden soll. Die Nutzung eines privaten Adressraums für ein Netz dieser Größenordnung führt unweigerlich zu Adresskonflikten. Hat man das komplette Netzwerk nicht unter einer einzigen administrativen Instanz, ist der Konfliktfall vorprogrammiert. Allein das D-Star-Netzwerk nutzt den kompletten Adressbereich 10.0.0.0/8 (10.x.x.x) für sich. Von den „Freifunknetzbetreibern“ im ISM-WLAN-Bereich sind negative Erfahrungen bekannt. Das Privileg einen eigenen Adressbereich aus dem Internet konfliktfrei nutzen zu können, sollte mit Blick auf künftige Entwicklungen nicht aufgegeben werden. Ein weiterer wichtiger Grund für die Nutzung des Adressbereichs 44.0.0.0/8 ist die mögliche Integration des HAMNET in das AMPRNet, die später genau beschrieben wird.

Neben dem IP-Adressraum muss man sich auch Gedanken zur zukünftigen Topologie dieses TCP/IP-Netzwerks machen. Schnell wird klar, dass ein Netzwerk in dieser Größe nicht auf Schicht 2 (hier Ethernet) des OSI-Schichtenmodell (http://de.wikipedia.org/wiki/OSI-Modell) betrieben werden kann. Um lokalen Datenverkehr auch lokal zu halten, ist es notwendig, die Schicht 3 (hier IP) zu nutzen. Der Versuch ein Netz komplett auf Schicht 2 zu realisieren, ist mit jedem Größenzuwachs zum Scheitern verurteilt. Die Anzahl der Broadcastaussendungen im gesamten Netz würde ansteigen und zu Lasten des Gesamtdurchsatzes gehen. Daher wird das HAMNET von Anfang an auf Schicht 3 geplant.

Die Administration des Netzwerks ist eine Aufgabe, die aufgrund der Netzgröße nicht zentral durchgeführt werden kann. Die Einteilung in sogenannte autonome Systeme (http://de.wikipedia.org/wiki/Autonomes_System) ermöglicht die Verteilung der Verwaltungslast und bietet einen größtmöglichen Freiraum für eigene Strukturierungen und Ausgestaltungen des Netzwerkes innerhalb einer Region. Funkamateure, die über Erfahrungen mit Netzwerken verfügen, können sich um die Verwaltung eines begrenzten Teils des HAMNET kümmern und unterstützen die Betreiber der HAMNET-Knoten, die nicht notwendigerweise die IT-Grundlagen selbst beherrschen oder erlernen müssen. Durch die Vernetzung der Standorte hat der Administrator eines autonomen Systems (AS) die Möglichkeit, nahezu alle Aufgaben aus der Ferne durchzuführen.

Jedes autonome System erhält eine netzweit eindeutige AS-Nummer. Für den privaten Gebrauch steht laut IANA der AS-Nummernbereich 64512 bis 65534 zur Verfügung (http://www.iana.org/assignments/as-numbers). Für Deutschland wurde vom DL-IP-Koordinatorenteam der Bereich 64620 bis 64669 reserviert. AS-Nummern und entsprechende Ansprechpartner werden in einer zentralen

Liste gepflegt (http://www.de.ampr.org/doku.php/dokumentation/as-nummern/as-list-de).

Neben den AS-Nummern werden vom DL-IP-Koordinatorenteam auch die IP-Adressbereiche für die einzelnen autonomen Systeme vergeben. Sie werden ebenfall in (http://www.de.ampr.org/doku.php/dokumentation/as-nummern/as-list-de) aufgelistet. In der Regel werden derzeit ein bis zwei /24-Netze aus dem User-/Service-Netzbereich und ein /24-Netz aus dem Backbone-Netzbereich einem autonomen System zugewiesen.

Für das Routing innerhalb eines autonomen Systems ist dessen Administrator verantwortlich. Dabei können verschiedene Technologien wie RIP, OSPF, iBGP oder einfaches Bridging genutzt werden. Wichtig ist die Schnittstelle zu anderen autonomen Systemen. Diese ist fest an das Border Gateway Protokoll BGP4 gebunden.

Wie oben schon erwähnt, gilt es, mit den Adressressourcen vernünftig umzugehen. AS-Nummern und IP-Netze werden in der Regel nur dann zugewiesen, wenn ein neues AS innerhalb eines nachvollziehbaren Zeitraumes zu mindestens einem weiteren Nachbar-AS eine (Link)Verbindung per eBGP aufbaut. Bei Nichtaktivität können AS-Nummern und Netze auch wieder entzogen und neu vergeben werden. Das BGP4-Protokoll ermöglicht ohne weiteren manuellen Eingriff die sehr schnelle Verteilung neuer Informationen im gesamten HAMNET.

Der vergebene AS-Nummernbereich kann im Bedarfsfall erweitert bzw. ein neuer Block hinzugefügt werden. Der AS-Nummernbereich für DL ist idealerweise in einem Block. Eine Teilung wirkt sich aber nur kosmetisch und nicht technisch aus. Der derzeitige IP-Adressbereich für das HAMNET in Deutschland ist etwas klein bemessen (ein /19 und ein /20). Darum laufen Bemühungen, ein weiteres /16-Netz (neben 44.130.0.0/16) für Deutschland zugeteilt zu bekommen.

TEIL 2
Planung des Netzes

Einleitung

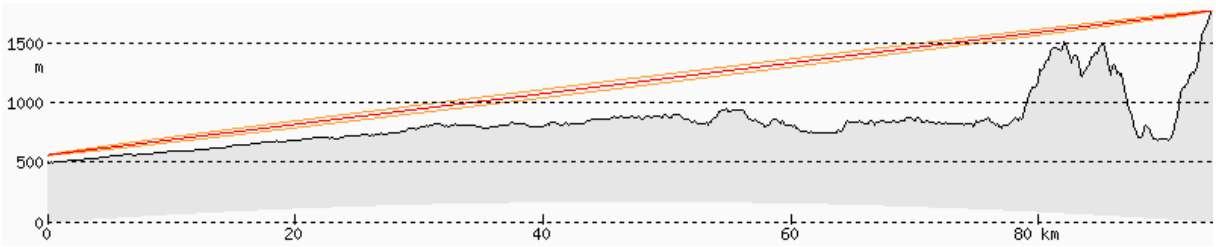
Im vorherigen Teil „HAMNET, Grundlagen des Highspeed Amateurradio Multimedia Network“ wurden die Grundlagen des HAMNET-Projektes erläutert. Im zweiten Teil soll es um die Praxis des HAMNET gehen.

Planung des HAMNET

Neben den organisatorischen Aufgaben in Zusammenarbeit mit dem DL IP-Koordinatorenteam ist es notwendig, sich um die Richtfunkplanung und der Aufteilung der zugewiesenen IP-Netze auf die einzelnen Standorte innerhalb eines autonomen Systems zu kümmern. Die AMPRNet IP Koordination Deutschland hat dazu eine frei editierbare Webseite auf ihrer Webseite angelegt (http://www.de.ampr.org/doku.php?id=dokumentation:as-nummern:hamnet-management).

Standort und Netzplanung

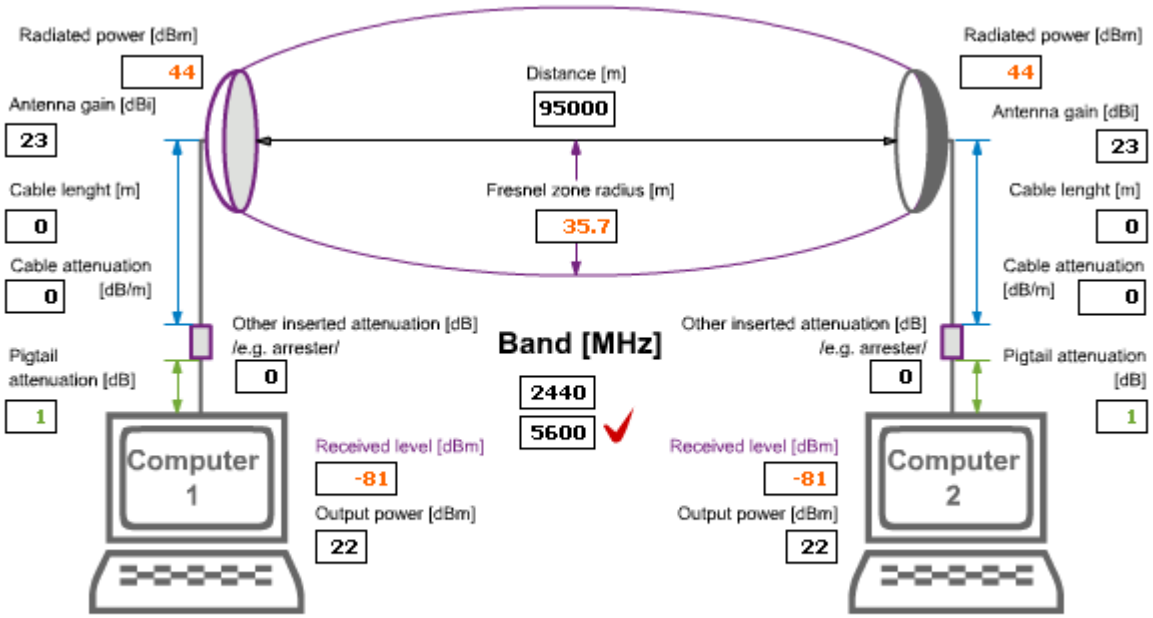
Zunächst sollen geplante HAMNET-Standorte mit Koordinaten und Antennenhöhe über Grund hinterlegt werden. Mit diesen Daten kann man mit wenig Aufwand bereits Geländeschnitte inklusive der Fresnelzone erstellen und Entfernungen zwischen den Standorten ermitteln. In Kooperation mit http://www.heywhatsthat.com können wir diesen Dienst kostenfrei anbieten. Das Verfahren ist auf der Webseite beschrieben.



Dynamisch generierter Geländeschnitt DB0ZKA - DB0GAP

Sind geplante HAMNET-Links als Ersatz für Packet-Radio-Linkstrecken angedacht, lohnt sich ein Blick auf das Packet Radio Crawler Projekt (http://db0fhn.efi.fh-nuernberg.de/doku.php?id=projects:prcrawler), welches Geländeschnitte von bereits existierenden Linkstrecken auf Knopfdruck bereitstellt (http://db0fhn.efi.fh-nuernberg.de/prmap/prmap-digiinfo.htm). So kann man schnell feststellen, ob ein Umstieg auf die HAMNET-Technik möglich ist. Sind die Daten der einzelnen HAMNET-Knoten zentral verfügbar, könnte man in Zukunft automatisierte Planungstools erstellen und über das Web bereitstellen.

Ist die Fresnelzone frei und die Entfernung bekannt, kann man eines der unzähligen Webapplets zur Berechnung des Linkbudget nutzen (http://en.jirous.com/calculation-wifi).



Linkbudgetrechnung DB0ZKA – DB0GAP mit einer Sendeleistung von 22dBm

Aus der errechneten Empfangsleistung geht die maximale Geschwindigkeit der Linkstrecke hervor. Dazu benötigt man die Leistungsdaten der verwendeten WLAN-Karten. Leider kann man sich nicht auf die Werte der Datenblätter verlassen. Teilweise existieren für ein und dieselbe Karte verschiedene Datenblätter mit verschiedenen Datenwerten. Ein mit der Praxis gut übereinstimmendes Datenblatt ist für die Wistron DCMA-82 Karte verfügbar (http://www.dd-wrt.com/shop/catalog/pdf/dcma82.pdf). Da die typische Ausgangsleistung der WLAN-Karten mit der Übertragungsrate abnimmt, müssen die Werte für Sender und Empfänger bei der Linkbudgetberechnung zusammen betrachtet werden. Sie sind zusätzlich großer Schwankung unterlegen:

[Average Power]
802.11a:
16dBm(min.), 18dBm(typical), 19dBm(max.) @ 54Mbps

17dBm(min.), 19dBm(typical), 20dBm(max.) @ 48Mbps
19dBm(min.), 20dBm(typical), 21dBm(max.) @ 36Mbps
20dBm(min.), 21dBm(typical), 22dBm(max.) @ 24Mbps
21dBm(min.), 22dBm(typical), 23dBm(max.) @ 6,9,12,18Mbps

[Sensivity]
-92 ~ -85dBm@ 6/9/12Mbps
-91 ~ -84dBm@ 18Mbps
-87 ~ -80dBm@ 24Mbps
-84 ~ -77dBm@ 36Mbps
-79 ~ -72dBm@ 48Mbps
-74 ~ -66dBm@ 54Mbps

Die Angabe der Leistung für 24Mbps wurde extrapoliert und nachträglich hier angegeben. Wie schon erwähnt, ist die Qualität der verfügbaren Datenblätter für günstige Endverbraucherprodukte nicht die beste. Im Datenblatt der Wistron DCMA-82 wurden z.B. auch die Empfängerempfindlichkeitswerte (Sensivity) für 802.11b und 802.11g vertauscht.

Mit den Werten aus dem Datenblatt kann man die Linkbudgetberechnung iterativ bestimmen. Für die Linkplanung DB0ZKA <-> DB0GAP (95km) gehen wir von Antennen mit 23dBi Gewinn aus.

Step	Durchsatz	TX-Power	RX-Pegel	notwendiger RX-Pegel
1	54Mbps	18dBm	-85dBm	-74dBm bis -66dBm
2	48Mbps	19dBm	-84dBm	-79dBm bis -72dBm
3	36Mbps	20dBm	-83dBm	-84dBm bis -77dBm
4	24Mbps	21dBm	-82dBm	-87dBm bis -80dBm
5	18Mbps	22dBm	-81dBm	-91dBm bis -84dBm
6	6/9/12Mbps	22dBm	-81dBm	-92dBm bis -85dBm

Die Linkstrecke würde rechnerisch mit stabilen 18Mbps laufen. Vermutlich würde oft auch ein Durchsatz von 24Mbps zur Verfügung stehen. Das Problem an der Rechnung ist, dass die Werte für eine Bandbreite von 20MHz gelten. Unter der Annahme, dass eine Halbierung der Bandbreite eine Halbierung der Übertragunsgeschwindigkeit, aber eine Signalverstärkung von 3dB (bei gleicher Stromaufnahme) bedeutet, ergibt sich folgende Tabelle für 10MHz Bandbreite:

Step	Durchsatz	TX-Power	RX-Pegel	notwendiger RX-Pegel
1	27Mbps	21dBm	-82dBm	-74dBm bis -66dBm
2	24Mbps	22dBm	-81dBm	-79dBm bis -72dBm
3	18Mbps	23dBm	-80dBm	-84dBm bis -77dBm
4	12Mbps	24dBm	-79dBm	-87dBm bis -80dBm
5	9Mbps	25dBm	-78dBm	-91dBm bis -84dBm
6	3/4,5/6Mbps	25dBm	-78dBm	-92dBm bis -85dBm

Die gleiche Iteration noch mal für eine Bandbreite von 5 MHz:

Step	Durchsatz	TX-Power	RX-Pegel	notwendiger RX-Pegel
1	13,5Mbps	24dBm	-79dBm	-74dBm bis -66dBm
2	12Mbps	25dBm	-78dBm	-79dBm bis -72dBm
3	9Mbps	26dBm	-77dBm	-84dBm bis -77dBm
4	6Mbps	27dBm	-76dBm	-87dBm bis -80dBm
5	4,5Mbps	28dBm	-75dBm	-91dBm bis -84dBm
6	1,5/2,25/3	28dBm	-75dBm	-92dBm bis -85dBm

Daraus geht hervor, dass ein Verzicht auf Bandbreite nicht in jedem Fall große Auswirkungen hat. In unserem Beispiel würde die Linkstrecke auch mit 10 MHz Bandbreite stabil mit 18Mbps laufen. Für die Grenzbereiche gilt dies nicht:
Unter Verwendung von 10MHz Bandbreite kann der anliegende Empfangspegel noch so gut sein; man wird nicht über den maximalen Durchsatz von 27Mbps

herauskommen. Ist der anliegende Empfangspegel so schlecht, dass mit 20MHz Bandbreite keine Verbindung mehr zustande kommt, kann die Umschaltung auf 5MHz Bandbreite die Verbindung erst ermöglichen (6dB mehr Signalpegel). Der geringe erreichbare Durchsatz könnte in der Praxis zumindest als Ersatz für einen PR-Link dienen. Kritische Linktests sollten auf alle Fälle mit 5MHz Bandbreite durchgeführt werden.

Unser Ziel ist es, ein zukunftsfähiges Hochgeschwindigkeitsnetz aufzubauen. Die Angaben über den Durchsatz in den Datenblättern sind Bruttowerte. Für die tatsächlich erreichbaren Durchsatzwerte kann man die Angabe nochmals etwa dritteln. Die Empfehlung lautet daher, sich mehr auf kurze Strecken zu konzentrieren, welche die volle Bandbreite ermöglichen, und nicht auf DX-Links zu setzen.

Ein bisher nicht erwähntes Tool zur Linknetzplanung ist Radio Mobile (http://www.cplus.org/rmw/english1.html). Eine Einführung würde den Rahmen dieses Skriptbeitrags sprengen. Es sei nochmals erwähnt, dass mit einer verfügbaren Standortdatenbank inkl. Koordinaten und Höhenangaben auch für Radio Mobile eine automatisierte Darstellung von Linkstrecken erreicht werden könnte.

Komponentenauswahl

Die Auswahl an Komponenten zum Aufbau des HAMNET erscheint riesig. Unter der Maßgabe ein hochbitratiges Netzwerk aufbauen zu wollen, ist zunächst ein Blick auf das Linkbudget sinnvoll. Unter Preis-/Leistungsverhältnissen und Praxiserfahrungen ergibt sich die Kombination einer 23dBi-Antenne und einer WLAN-Karte mit 21dBm Sendeleistung bei 10MHz Bandbreite mit höchstwertiger Modulation (27Mbps) als gute Lösung.

Genannte Kombination gibt es als handliche „All-in-One“-Lösungen. Es sind Flachantennen (30x30cm) gleich mit Montagemöglichkeit für WLAN-Boards (Enclosure) erhältlich. Die Speisung mit Strom und Daten erfolgt dabei über die Ethernetleitung (Power-over-Ethernet). Die mechanische Installation der Gesamthardware am HAMNET-Knoten ist leicht zu bewerkstelligen.

Bereits ab einer Entfernung von 20km reicht die Signalstärke (-66dBm) allerdings nicht mehr für die maximal mögliche Datenrate aus. Auch für kürzere Entfernungen sind solche Lösungen für Point-to-Point Strecken zu empfehlen, da die Verbindungsstabilität zunimmt, Störungsprobleme abnehmen und die Frequenz in kürzen Abständen an anderen Standorten ohne Beeinflussung wieder verwendet werden kann.

Ab 20km Entfernung kann die Verbindungsqualität durch größere Antennen gesteigert werden. Ab 23dBi werden die Antennen schnell sehr teuer. Bei erhöhter Windlast empfiehlt es sich auch noch genauer auf die Qualität der Antenne zu achten. Gitterspiegel werden oft mit guten Leistungsdaten beworben, die aber in der Praxis kaum nachzuvollziehen waren. Im Winter droht die Verbindung aufgrund von Eisbildung am Gitter zusammenzubrechen. Die Montage von größeren Antennen ist an manchen Standorten ein weiteres Problem.

Bisher haben wir auch keine größeren Antennen mit Enclosure für vernünftige Preise auf dem Markt entdecken können. Ist man auf ein Outdoor Enclosure angewiesen, muss zusätzlich die hohe Dämpfung der Kabel beachtet werden. Kommerziell genutzte Standorte könnten auch aktive Technik auf dem Antennenträger verbieten. Hochwertige Kabel können hier Abhilfe schaffen. In diesem Fall sollte man die Grenzfrequenz des geplanten Kabels beachten.

Eine weitere Möglichkeit ist die Steigerung der Ausgangsleistung, was aber zu Instabilitäten der WLAN-Karte z.B. durch Überhitzung führen könnte. Außerdem muss die notwendige Stromversorgung entweder über das Ethernetkabel oder als extra geführte Leitung gesichert sein. Aus

Kostengründen verzichten die meisten Hersteller darauf Power-over-Ethernet nach dem Standard 802.3af zu implementieren. Die Behelfslösung nutzt die freien Adern 4,5,7 und 8 des Ethernetkabels zur Stromversorgung. Der Spannungsabfall auf längeren Ethernetkabeln kann hier zu einem Problem werden.

Betriebliche Auflagen können an manchen Standorten auch andere Anforderungen stellen. Unter den Gesichtspunkten begrenzter Antennenzahl und begrenzter Stromaufnahme kann ein Point-to-Multipoint-Link eine ideale Lösung zur Vernetzung mehrerer Standorte sein.

Die bisher am HAMNET angeschlossenen Systeme in Bayern verwenden Komponenten von Mikrotik mit dem Basissystem „RouterOS“. Eine nähere Beschreibung des Aufbaus in Franken ist im Internet abrufbar (http://db0fhn.efi.fh-nuernberg.de/doku.php?id=projects:wlan:hamnet).

Die Komponenten von Mikrotik sind aufgrund des Funktionsumfangs und der leichten Bedienbarkeit über ein grafisches Benutzerinterface (GUI) besonders gut für das HAMNET geeignet. Der notwendige BGP-Router beim Einsatz als Router für Linkstrecken über die Grenzen eines AS hinweg ist gleich mit an Bord.

Gute Linksammlungen zum Erwerb von HAMNET-Komponenten sind auf dem Wiki des OEVSV zu finden (http://wiki.oevsv.at/index.php/Linkkomponenten_digitaler_Backbone). Außerdem habe ich eine kleine Linksammlung in einer E-Mail zusammengefasst:

Board: Mikrotik RB433AH oder RB411AH
WLAN-Karte: "Wistron DCMA82" (etwas dicker, daher max. 2 pro 433er-Board --> eine R5H-Karte koennte dazwischen passen (nicht zu empfehlen --> lieber 1x RB411AH + 1x Wistron DCMA82 und gut).

Antenne:
Ich bin ueber diesen allgemeinen Link von Mikrotik gestolpert (Accessories und Integrators durchschauen): http://www.mikrotik.com/mfm.php?category=2

Ich moechte eine Liste der moeglichen Antennen erstellen (nicht unbedingt der Bezugsquellen):
- Jirous JRC-24 EXTREME: http://en.jirous.com/antenna-5ghz/jrc-24-extrem (JR-200 Box dazu! -> RB411 passt, RB433 mit nur einer Karte)
- Mars Antennas MA-WA58-1XBRFR: http://www.mars-antennas.com/item/g_antennas_type_1-43.html (Ich glaube perfekt fuer RBxxx)
- ARC Wireless Solution ARC-IA5823B02: http://www.antennas.com/5.15-5.875ghz-23dbi-panel-antenna-for-arc-iestm,-integrated-enclosure-solution.html (Bezugsquelle: http://landashop.com/catalog/outdoor-aluminum-enclosure-integrated-antenna-p-470.html (-> Ich glaube RBxxx passend, da in Oberbayern eingesetzt).
- LANBOWAN LBW-523: keine Homepage. Ueber Landashop gefunden: http://landashop.com/catalog/lanbowan-outdoor-enclosure-ip65-23dbi-rj45-p-1220.html
- Poynting WLAN-A0042: http://www.poynting.co.za/ProductDetails.aspx?pid=375%20&DivisionId=2&DivisionName=Commercial
- MTI Wireless MT-900016: http://www.mtiwe.com/uploads/product/117.pdf (auch via Landashop, aber etwas teurer)
- ganz neu: ITELITE PRA50023: http://www.itelite.net/products-desc.php?id=400 (RB433 + RB411 passt)

Die polnischen Anbieter sind auch alle ganz nett:
http://www.technologic.pl
http://www.cyberbajt.pl/produkt/1237/gigaeter23-skrzynka-zewnetrzna.html
http://www.cyberteam.pl/produkt/show/308.html
http://www.interprojekt.com.pl/antennas-5ghz-integrated-c-31_94.html

Falls du was Bezahlbares mit mehr als 23dBi findest, dann bitte Info. Auch weitere Infos wo man wie die Mikrotikboards einbauen kann, waere interessant. Ebenso vernuenftige Bezugsquellen. Evtl. kann man da mal was zusammenstellen.

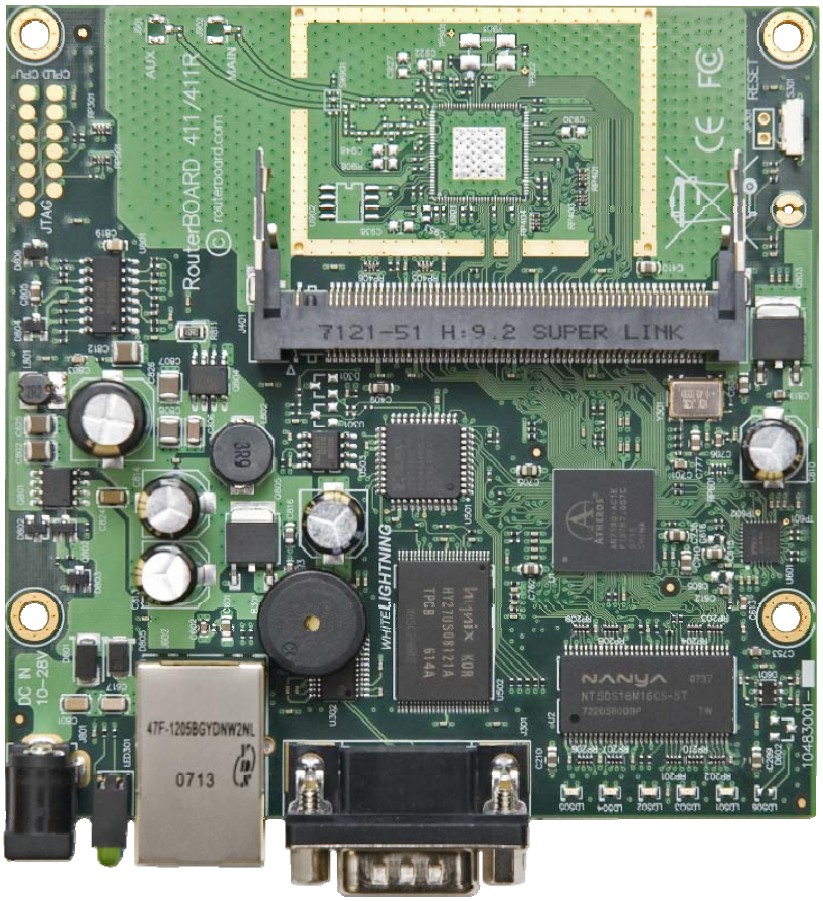
Beispielhafte Komponentenzusammenstellung

Ich persönlich würde zu folgenden Komponenten greifen, wenn ich einen neuen HAMNET-Knoten aufbauen würde: Pro Link eine einzelne Außeneinheit bestehend

aus Antenne mit Gehäuse für das WLAN-Bord, WLAN-Board mit Speisung über Ethernet und WLAN-Karte mit passendem Pigtail.

23dBi-Antenne:
Mars-Antenna MA-WA58-1XBRFR oder ARC Wireless Solution ARC-IA5823B02. Beide Antennen konnte ich nicht testen, da ich mich damals für Antennen von Jirous entschieden habe. Heute würde ich mich für die genannten Antennen entscheiden, da das integrierte Gehäuse für das WLAN-Board aus Aluminium gefertigt ist und die Abstrahlungen des WLAN-Boards nicht nach außen gelangen lässt. Achtung: Die Norm der Antennenbuchse muss zu den verfügbaren Pigtails passen. Es gibt verschiedene Ausführungen (evtl. auch welche mit direktem Anschluss für die WLAN-Karte). Neben den Steckverbindungen muss auch das geplante WLAN-Board in das Gehäuse passen. Am bequemsten ist dies, wenn das WLAN-Board ohne Modifikation direkt eingeschraubt werden kann. Dies konnte ich ebenfalls nicht testen.

WLAN-Board mit PoE:
Das Mikrotik RB411AH-Board sorgt mit seiner schnellen CPU für maximalen Datendurchsatz, bietet einen Steckplatz für eine WLAN-Karte und kann über Ethernet (nicht 802.3af) mit Strom versorgt werden. Die nötige Spannungsversorgung ist mit 12V bis 24V angegeben. Mit einem sogenannten PoE-Injector kann die Versorgungsspannung in das Kabel eingespeist werden. Als Ethernetkabel empfehlen sich geschirmte Kategorie 6 Kabel. Es sollte resistent gegenüber Sonneneinstrahlung sein (UV-fest).



Das Routerboard RB411AH

WLAN-Karte und Pigtail:
Von der Wistron DCMA82 WLAN-Karte liegen die meisten positiven Erfahrungsberichte aus dem HAMNET-Kreis vor. Abweichend von der Standardkonfiguration kann die Leistung um bis zu 6dB erhöht werden. Bei Erhöhung um mehr als 3dB ist die Stabilität des Systems evtl. gefährdet.

Ich habe die Modifikation aus dem OE-Wiki (http://wiki.oevsv.at/images/f/f5/RBmod.pdf) nur am Routerboard durchgeführt und hatte noch keine Probleme (ich komme allerdings ohne Leistungserhöhung aus). Bei Erhöhung der Sendeleistung ist der erhöhte Strombedarf auch nicht außer Acht zu lassen. Bei der Auswahl des Pigtails ist nach einem MMCX-Stecker Ausschau zu halten. Die Ausführung dieser Steckernorm erscheint qualitativ hochwertig.

Die Wistron DCMA82 WLAN Karte

Hat man an einem HAMNET-Knoten mehrere Linkstrecken aktiv, so werden die einzelnen „Outdoor-Units“ über einen zentralen Switch miteinander vernetzt. Wenn nicht unbedingt nötig, würde ich auf Lösungen mit mehreren WLAN-Karten pro WLAN-Board verzichten. Das Mikrotik RB433(AH) bietet zwar Platz für bis zu drei WLAN-Karten, aber dann kommt man nicht mit separatem Outdoorgehäuse für das Board aus. Außerdem ist die Anordnung der Mini-PCI-Slots für die WLAN-Karten ungeschickt gemacht, sodass maximal zwei Wistron DCMA-82-WLAN-Karten Platz haben. Im Vergleich zu anderen Karten fallen diese relativ dick aus. Persönlich habe ich noch keine Erfahrung mit mehreren Links an einem Standort. Die gegenseitige Beeinflussung wäre noch zu untersuchen. Der nötige Antennenabstand wird aber sicherlich nicht zu groß sein. Erfahrungen können bei den Kollegen aus Österreich erfragt werden.

Frequently asked Questions (FAQ):

F: Wie kann man sich gegen „Schwarzfunker“ schützen?
A: Es gibt keinen Schutz vor „Schwarzfunkern“. Der Einsatz von Verschlüsselung im Amateurfunk ist verboten. Zur Ermittlung des Schwarzfunkers kann der Funkmessdienst eingeschaltet werden.

F: Wie kann man sich gegen ungewollte Aussendungen des eigenen Systems hervorgerufen durch Geräte anderer Funkdienste in mehrfach genutzten Frequenzbändern schützen?
A: Die Verwendung von anderen Bandbreiten bietet schon guten Schutz. Es ist uns unklar, ob wir für Amateurfunkaussendungen initiiert durch Geräte des ISM-Bereichs strafbar gemacht werden können.

F: Wie kann ich verhindern, dass der konfigurierte Internetzugang auch von HAMNET-Usern genutzt werden kann?
A: Durch Trennung vom User-/Servicenetz vom Backbonenetz ist der Zugang auf eine begrenzte Region beschränkt. Am einfachsten ist es den Zugriff auf das Internet aus dem Netz 44.0.0.0/8 zu verbieten und nur die eigenen gewünschten Netzbereiche zu erlauben. Dies kann über die Firewall des letzten Routers zum Internet gelöst werden.

F: Warum muss zwischen User-/Servicenetz und dem Backbonenetz unterschieden werden?
A: Eine Trennung beider Netze auf Schicht 3 des OSI-Schichtenmodells verhindert die Flutung des HAMNET mit Datenverkehr der Schicht 2. Lokaler Datenverkehr wird lokal gehalten und belastet nicht das Linknetz. Mit wachsender Größe des Netzwerks wird diese Aufteilung immer wichtiger. Von Alternativen, wie dem Versuch mit Firewalls Schicht-2-Datenverkehr zu blockieren können wir nur stark abraten.

F: Wann wird eine weitere AS-Nummer innerhalb einer Region benötigt?
A: Ein AS sollte nicht mehr als 6 oder 7 iBGP-Router betreiben, da der Verwaltungsaufwand darüber sehr groß wird. Jeder neue iBGP-Router muss zu den existierenden iBGP-Routern eine Verbindung halten.

F: Welches AS-interne Routingverfahren wird empfohlen?
A: Prinzipiell können alle Routingprotokolle verwendet werden. In Versuchen hat sich gezeigt, dass internal BGP (iBGP) sich gut bewährt hat. Es soll sich aber keiner davon abhalten lassen, andere Protokoll wie OSPF, RIP oder OLSR zu verwenden. Auch ein großes gebridgtes Netz oder ganz neue Verfahren wären denkbar.

F: Soll Netzsegmentaggregierung verwendet werden?
A: Nein, solange keine Schwierigkeiten ohne Aggregierung von IP-Netzen festzustellen sind, möchten wir darauf verzichten. Die Aggregierung von IP-Netzen ist fehleranfällig und stellt vor allem in vermeshten Netzen mit Ringen ein Problem dar. Debugging kann hier sehr schwierig werden.

F: Was passiert, wenn ein Ring im HAMNET entsteht.
A: Bisher liegen nur Erfahrungen aus OE vor. Ist ein Ring auf Schicht 2 geschlossen, kann das Spanning Tree Protokoll (STP, http://de.wikipedia.org/wiki/Spanning_Tree_Protocol) eingesetzt werden. Alternativ ist die Auftrennung des Rings auf Schicht 2 unter Aufteilung der Äste mit verschiedenen Backbonenetzbereichen der Schicht 3 möglich.

Alternative Routerhard- und software

Die beschriebenen Netzpläne haben allgemeine Gültigkeit und sind nicht an die Hardware von Mikrotik oder RouterOS gebunden. Darum ist es sinnvoll, Vergleiche mit anderen Komponenten und anderer Software durchzuführen.

Auf den Komponenten von Mikrotik ist bereits das firmeneigene RouterOS mit der an die Hardware gebundene Softwarelizenz vorinstalliert. Die Softwarelizenz sollte den Level 4 haben. Damit können alle unsere Anforderungen erfüllt werden. Eine höhere Lizenz ist unnötig. Weitere Informationen zu den Lizenzen gibt es bei Mikrotik (http://wiki.mikrotik.com/wiki/Category:License).

Leider kann auf dem RouterOS keine Software von Drittherstellern installiert werden. Mikrotiks Firmenphilosophie ist es, das nur von ihnen getestete stabile Software auf ihren Produkten laufen darf und verhindert daher den Zugang auf die darunter laufende Linuxplattform. Es gibt Bedenken, dass Software von Drittanbietern das Gesamtsystem instabil machen würde und Mikrotik dafür verantwortlich gemacht werden würde.

Die Thematik mit der eingeschränkten Frequenzauswahl ist seit der RouterOS-Version 4.3 offiziell erledigt (http://wiki.mikrotik.com/wiki/Manual:Interface/Wireless#Advanced_settings). Es können nun alle Frequenzen der WLAN-Karte unabhängig von Zusatzlizenzen (Superchannel) genutzt werden.

Für die beschriebenen Standard HAMNET-Installationen stellt die Tatsache der geschlossenen Plattform kein Problem dar. Bisher ist mir auch kein Hack bekannt, der bei einem laufenden RouterOS Zugriff auf eine Linuxshell bietet. Möchte man trotzdem die ganze Freiheit einer Linuxinstallation nutzen, dann kann ein Linux wie OpenWRT auf der Mikrotikhardware installiert werden.

Im Gegensatz zu Mikrotik wirbt Ubiquiti (http://www.ubnt.com) mit seiner „Open Source“-Philosophie und dem Betriebsystem AirOS. Leider ist kein Softwarepaket für das BGP-Routing in der Standardfirmware enthalten. Flemming Frandsen stellt mit seinem AirOS+ aber einen Patch mit einer Anleitung zum Compilieren eines eigenen Firmwareimages mit den BGP-fähigen Softwareroutern Quagga und BIRD bereit (http://dren.dk/airos-plus.html). Die Konfiguration von Quagga oder BIRD ist allerdings nicht in grafischer Form z.B. über ein Webinterface verfügbar, sondern muss über Textdateien erledigt werden. AirOS bietet wie RouterOS alle verfügbaren WLAN-Kanäle und reduzierte Bandbreite (half/quarter) an.

OpenWRT ist eine Linuxdistribution für „embedded devices“. Wie bei einer normalen Linuxdistribution arbeitet es mit einem Paketmanagementsystem. Ziel ist es, ein Grundsystem für möglichst viele Plattformen und möglichst viel Speicherplatz für zusätzliche Pakete zu bieten. Derzeit ist die Version Kamikaze 8.09.2 stabil, aber seit dem 4.3.2010 steht bereits die Version Backfire 10.03 als Beta in den Startlöchern.

Uns Funkamateure interessiert primär die Unterstützung der einzelnen Funkmodule in Bezug auf reduzierte Bandbreite, freier Frequenzwahl und optimiertes Timing für längere Linkstrecken. Leider sind diese Punkte auch heute noch ein großes Problem. Hintergründe zum Thema sind von Steve Lampereur, KB9MWR, gut zusammengefasst worden (http://www.qsl.net/kb9mwr/projects/wireless/modify.html). Mit dem neuen Framework „mac80211“ (http://linuxwireless.org/en/developers/Documentation/mac80211) für Linux ist zwar eine gute Entwicklungsumgebung für quelloffene Wireless Treiber entstanden, aber unsere Anforderungen werden bisher noch nicht offiziell unterstützt. D.h. man kommt nicht um eigene Modifikationen der Treiber herum, wenn man außerhalb des ISM-Bandes mit reduzierter Bandbreite senden möchte.

OpenWRT kann sowohl auf den Mikrotik-Komponenten (Architektur: Mipsel) als auch auf den Ubiquiti-Komponenten (Architektur: Mips) laufen. Spezielle Softwarepakete für AX.25 wurden auf DB0FHN bereits zur Verfügung gestellt (http://db0fhn.efi.fh-nuernberg.de/doku.php#openwrt). Der Softwarestand ist allerdings nicht mehr der aktuellste. Mit den Softwareentwicklern des BIRD internet routing daemon (http://bird.network.cz) versuchen wir derzeit, das Paket „bird“ in den offiziellen OpenWRT Zweig einfließen zu lassen. Setzt man OpenWRT auf einem Mikrotik-Board ein, könnte man den seriellen Port zum Beispiel zum Anschluss eines RMNCs oder APRS-TNC nutzen. Daten serieller Schnittstellen können nach RFC2217 auch über ein Netzwerk übertragen werden. Hierfür gibt es das Paket ser2net.

Für die verbreitete Architektur x86 gibt es Komponenten von ALIX (http://www.pcengines.ch/alix.htm). Für diese Plattform steht bereits ein fertiges OpenWRT-Image mit modifizierten WLAN-Treibern von HB9XAR zur Verfügung (http://hamnet.tuxworld.ch/download). Da über den Compact-Flash Steckplatz eine Menge Speicher zur Verfügung steht, kann statt OpenWRT z.B. auch ein abgespecktes Debian/Linux (Voyage Linux) zum Einsatz kommen.

Die x86-Architektur kann beim Entwickeln von Software eine Menge Nerven sparen, da das umständliche Crosscompilieren entfällt. Soll am Standort ein Low-Power-PC für z.B. D-Star, Asterisk/app_rpt oder svxlink betrieben werden, da der Stromhaushalt extrem knapp ist, kann man über die Integration des HAMNET-Links in den Rechner nachdenken. Letztens ist mir erst ein neues Mainboard mit Intel Atom CPU durch seine komplette Fernadministrierbarkeit (Console Redirection, Virtual Media) positiv aufgefallen (http://www.supermicro.com/products/motherboard/ATOM/ICH9/X7SPA.cfm?typ=H&IPMI=Y).

Mit einer offenen Linuxplattform hat man unter Beachtung der CPU-Belastung die Möglichkeit z.B. auch einen AX.25-Knoten wie Xnet laufen zu lassen. Meist hat man jedoch sowieso einen PC am Standort und kann die benötigten Dienste dort implementieren. Meine Empfehlung ist es, das HAMNET autark aufzubauen, um Ausfallzeiten zu minimieren. Wer die Möglichkeit hat, kann Dienste hardwareseitig separieren.

Integration des HAMNET im AMPRNet

Nach der Definition des AMPRNet bzw. Network 44 (Nutzer des IP-Adressraums 44.0.0.0/8) ist das HAMNET bereits Teil des AMPRNet. Wie aber kann für wirkliche Konnektivität im AMPRNet gesorgt werden?

Das klassische Verfahren TCP/IP-Pakete innerhalb des Amateurfunks von A nach B zu transportieren, ist die Verwendung von AX.25. Dabei werden die TCP/IP-Pakete in AX.25-Frames eingepackt und über das Packet Radio Netz an ihr Ziel gebracht. Da das Packet Radio Netz nicht die ganze Welt umspannt, nutzt man Tunnel im Internet, um die einzelnen TCP/IP-Aktivitätszentren der Funkamateure miteinander zu verbinden. Diese sogenannten IPIP-Tunnel packen dabei die TCP/IP-Pakete wiederum in IP-Pakete (statt in AX.25-Pakete wie im klassischen Verfahren) ein und „tunneln“ diese an ihr Ziel über das Internet. Mit dem HAMNET steht uns jetzt eine Funktechnik zur Verfügung, welche ganz ohne Einpacken von TCP/IP-Paketen auskommt.

Das AMPRNet möchte alle TCP/IP-Aktivitäten unter Funkamateuren zu einem gemeinsamen Netz ausbauen. Unsere Hauptziele sind daher:

- Integration aller Teilnetze (IP über AX.25, IPIP, HAMNET) zu einem Netz
- Einfache Nutzung des Netzes sowohl für User als auch für Sysops
- Bestandssicherung des Network-44 gegenüber kommerzieller Interessen

Diese Ziele wurden an DB0FHN (Hochschule Nürnberg) und dem zentralen Packet Radio Knoten IGATE mit Augenmerk auf Nutzbarkeit versucht umzusetzen. Mit der Integration des HAMNET wird eine saubere Implementierung der Idee des TCP/IP-Routings unerlässlich. Dies erfordert die Umstrukturierung der bisherigen Infrastruktur und kann sich für TCP/IP-Knotenbetreiber innerhalb des AX.25-Netzes und dessen Nutzer auswirken. Die geplante Umsetzung soll nachfolgend erläutert werden.

Die zentrale Idee ist es, dass jeder Teilnehmer des AMPRNet seine lokalen IP-Netze dem Gesamtnetz bekannt macht:

- Im HAMNET werden die IP-Netze über die Grenzen autonomer Systeme hinweg mithilfe des BGP4-Protokolls übertragen.
- Im IPIP-Netz (TCP/IP-Gateways mit Tunnel über das Internet) werden die IP-Netze über eine Mailingsliste (E-Mail) täglich verteilt. In den vergangenen Monaten sind neue Entwicklungen wie die Nutzung des RIP-Protokolls (http://de.wikipedia.org/wiki/Routing_Information_Protocol) zu beobachten.
- Im AX.25-Netz sind keine Projekte zur Verteilung von Routinginformationen bekannt. Das INP3-Protokoll

(http://dl6mpg.net/nordlink/ftp/pub/documentation/INP/inp3.pdf) hätte Potential zur Verteilung der IP-Netze.

Die Tatsache, dass jeder Knoten seinen eigenen (oder mehrere) IP-Adressraum besitzt, lässt beim User die nomadische Nutzung von IP-Adressen nicht mehr zu. D.h. ein User muss am Knoten A eine vorgesehene IP-Adresse aus dem vom Sysop festgelegten IP-Adressraum für Knoten A nutzen und kann nicht eine IP-Adresse von Knoten B nutzen. Für den eventuellen Verlust an Komfort beim User muss durch technische Mittel eine Alternative gefunden werden (z.B. durch DHCP over AX.25).

Ein automatisches Routing (Vermitteln von IP-Netzen an Nachbarn) ist Voraussetzung für ein wartungsarmes und funktionierendes Netzwerk. Wichtig ist es, dass die Routinginformationen aktuell gehalten werden. Im HAMNET erledigt das BGP4-Protokoll diese Aufgabe in nahezu Echtzeit. Die Routen vom IPIP-Netz werden derzeit maximal einmal pro Tag aktualisiert. Leider lesen viele Gatewaybetreiber die Routinginformationen nur unregelmäßig manuell ein. Im AX.25-Netz werden die Routen sogar komplett manuell gesetzt. Leider hängt die Qualität der Routinginformationen stark von der Pflege selbiger ab.

Das neue HAMNET bringt von Anfang an mit dem BGP4-Routingprotokoll alles Notwendige für die Zusammenschaltung anderer Netze mit. Auf die Gegebenheiten des internationalen IPIP-Routings haben wir nur begrenzten Einfluss. Neuentwicklungen gehen nur langsam voran. Im AX.25-Netz haben wir die notwendigen Administrationsarbeiten an Packet Radio Knoten durch Einführung des IP-Routings über IGATE minimiert.

Zunächst ist eine zentrale Zusammenschaltung der Netze an DB0FHN und IGATE geplant.

HAMNET <-> IPIP-Netz:
Es werden die bekannten Routen des IPIP-Netzes über das BGP4-Protokoll in das HAMNET eingespeist. Eine automatische Bekanntgabe der aktiven IP-Netze aus dem HAMNET an das IPIP-Netz ist zur Zeit nicht möglich. Derzeit wird aber sämtlicher Datenverkehr für die IP-Netze 44.130.0.0/16 (Deutschland), 44.142.0.0/16 (Schweiz), 44.143.0.0/16 (Österreich), 44.151.0.0/16 (Frankreich) und 44.161.0.0/16 (Luxemburg) innerhalb des IPIP-Netzes an uns geschickt. Somit ist das Routing zwischen dem HAMNET und dem IPIP-Netz für genannte Netzbereiche komplett funktionsfähig. Auf längere Sicht ist es aber wünschenswert, wenn ein kompletter Austausch der Routen in Echtzeit erfolgen kann.

HAMNET <-> AX.25-Netz:
Momentan findet noch kein Austausch der Routen statt. Im IP-Router des AX.25-Knotens IGATE sind derzeit manuell die Routen zum HAMNET gesetzt (44.130.192.0/19 und 44.130.224.0/20 für Deutschland und 44.143.0.0/16 für Österreich). Ein Tool zum periodischen Einlesen der HAMNET-Routen in den IGATE-Knoten muss erst noch entwickelt werden. Dem HAMNET wird aktuell das gesamte deutsche IP-Netz 44.130.0.0/16 bekanntgegeben. Daher funktioniert ein bidirektionales Routing auch in dieses Netz bereits. Die Situation ist aber nicht zufriedenstellend, da nur die tatsächlich genutzten IP-Netze aus dem AX.25-Netz per BGP4 in das HAMNET eingespeist werden sollen.

Um später volle Flexibilität im Routing haben zu können, ist es notwendig, die genutzten IP-Netzbereiche so genau wie möglich angeben und verteilen zu können. Früher wurde an jedem TCP/IP-fähigen AX.25-Knoten alle Routen mit Zielrufzeichen und IP-Netzen händisch gepflegt. Da die Bereitschaft solche Routen händisch zu pflegen und damit die Funktionalität des Netzes masiv abgenommen hat, wurde der IGATE-Knoten TCP/IP-fähig gemacht. Jeder TCP/IP-Knotenbetreiber hat daher die Möglichkeit, einfach die Defaultroute nach IGATE zu definieren. Die Routinginformationen zu den einzelnen IP-Netzen im AX.25-Netz müssen dann nur noch zentral auf IGATE gepflegt werden. Daher

ist es nötig, dass die Betreiber von TCP/IP-Knoten im AX.25-Netz ihre eigenen IP-Netze an die Betreiber von IGATE melden. Diese IP-Netze sollen dann später per BGP4 im HAMNET verteilt werden.

Unter der Prämisse, dass jeder TCP/IP-Knoten (egal welchen Netzes) immer nur seine eigenen IP-Netze „announced“, ist eine Dezentralisierung des Übergangs in die verschiedenen Netze möglich. Möchte z.B. ein Betreiber eines HAMNET-Knotens auch einen TCP/IP-over-AX.25-Einstieg für Endnutzer bereitstellen, so kann er den geplanten Netzbereich auch selbst im HAMNET über BGP4 bekanntmachen oder auch gleich aus dem IP-Adressbereich für HAMNET herausbrechen. Er hat dann nur dafür zu sorgen, dass das lokale Routing auch funktioniert, und kann danach den IGATE-Administratoren mitteilen, dass das entsprechende IP-Netz nun selbst „announced“ wird und im IGATE-System entfernt werden soll.

Vor einiger Zeit wurde das Projekt „IP over IGATE“ (http://db0fhn.efi.fh-nuernberg.de/doku.php?id=projects:igate:ipoverigate) vorgestellt. Die beschriebene Konfiguration für XNet-Knoten bleibt mit einer Ausnahme erhalten. Mit der Version 1.39 Beta 04.03.2006 wurde folgende Option eingeführt:
„Priorisierung gelernter IP-Routen: Bei vielen Knoten sind die IP-Routen nicht gepflegt - deshalb priorisiert diese Betaversion die ARP-Einträge (gelernte oder statische) vor den IP-Routing-Einträgen. Damit sollte das IP-Routing in den meisten Fällen besser funktionieren. Mithilfe der neuen Befehlsfolge "ipr prio 1" kann der alte Zustand wiederhergestellt werden. Dann haben die IP-Routing-Einträge die Priorität.“

Um die nomadische Nutzung von IP-Adressen und folglich manipulierter Routingtabellen vorzubeugen, muss „ipr prio 1“ in der Konfiguration gesetzt werden. Die User können dann nur noch eine IP-Adresse aus dem von euch vorgesehenen Bereich nutzen. Für jeden TCP/IP-fähigen Digipeater (XNet, TNN, Wampes) ist dabei ein eigenes IP-Netz vorzusehen. IP-Adressen sollten an die Nutzer dynamisch vergeben werden. XNet kennt hierzu den Befehl GETIP. Nähere Konfigurationsbeschreibungen sind noch zu veröffentlichen.

Seit einigen Jahren kommen immer mal wieder Überlegung zur Nutzung von DHCP für IP-über-AX.25 auf. Mit der Einführung von dynamisch vergebenen Adressen für Endnutzer erscheint dies immer notwendiger. Auf der Knotenseite wäre zunächst eine entsprechende Erweiterung von Xnet/TNN und auf der Nutzerseite eine passende Erweiterung für PC/Flexnet32 sinnvoll.

Ausblick

Aus den Medien haben wir bereits erfahren, dass der gesamte IPv4-Adressraum zuneige geht. Das Privileg, ein Klasse A Netzwerk nur für den Amateurfunk nutzen zu können, sollte durch Zeigen von Bedarf auch verteidigt werden. Vereinzelnd sind Kopplungen zwischen dem Internet und dem Network 44 eingerichtet. Diese sind aber auf Experimente mit Amateurfunkcharakter und schmalbandiger Nutzung beschränkt. Ausgehende Verbindungen zum Internet wird der IGATE-Knoten auch nach der Neukonfiguration ermöglichen. Außerdem wird IGATE ein IP-Netz für Endnutzer bekommen, damit ein Betrieb auch auf Einstiegen möglich ist, welche keine direkte TCP/IP-Unterstützung anbieten.

Weitere Experimente können im IT-Bereich gemacht werden. Dem Einsatz von IPv6 auch im HAMNET spricht nichts entgegen. Hier können wertvolle Praxiserfahrungen für die Zukunft gesammelt werden. Experimente mit Multicasting oder Source Routing könnten auch spannend sein.

Direkte schnelle IP-basierte Usereinstiege in das HAMNET sind eine große Herausforderung für die Zukunft. Alternativ können Funkamateure auch über VPN-Zugänge (Authentifizierung nötig) über das Internet die Dienste des HAMNET nutzen. An DB0FHN und DB0RES ist dies bereits unter Nutzung des PPTP-Zugangs möglich.

Im HAMNET können auch Bild- und Sprachverbindungen aufgebaut werden. So kann ein Bild- oder Sprachnetz als Nutzlast innerhalb des HAMNET entstehen. Wie auch beim S&F (Store and Forward) verschiedener Mailboxen in Packet Radio kann dabei das Internet als Fallbacklösung konfiguriert werden.

Ein großes Thema, vermutlich für die IPRT 2011, wird die Ausarbeitung einer unverbindlichen „Policy“ für das HAMNET sein. Neben den gesetzlichen Einschränkungen (kein kommerzieller Einsatz) gilt es die Frage zu stellen, ob alles technisch Machbare auch wirklich sinnvoll ist. Ich halte die IPRT für eine geeignete Veranstaltung für demokratische Abstimmungen über den Inhalt einer solchen Policy. Ein Thema könnte sein, wie man mit Internetlinkstrecken zur Vernetzung von HAMNET-Zentren umgehen sollte. Der Sinn einer Policy sollte auf der IPRT 2010 diskutiert werden.

TEIL 3
Praktische Beispiele

Einleitung

Nachdem in den beiden vorherigen Beiträgen die Grundlagen des Highspeed Amateurradio Multimedia Network und die Aspekte behandelt wurden, die bei der Planung von Strecken und Netzen beachtet werden müssen, soll nun an praktischen Beispielen der Aufbau dieses Netzes beschrieben werden.

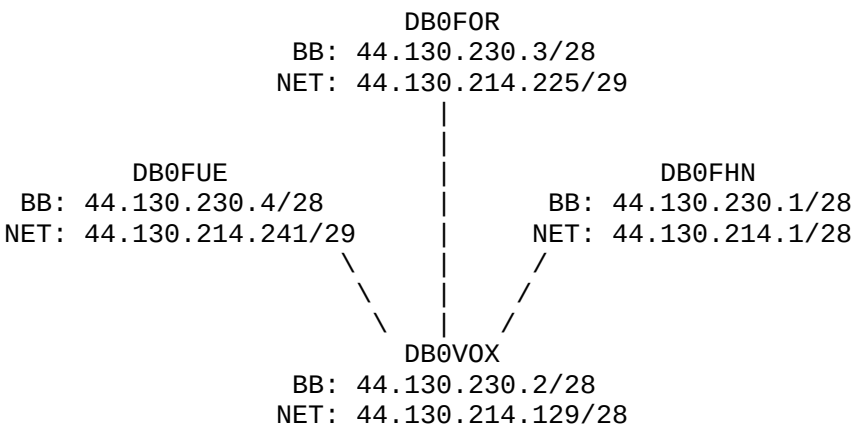
Konfiguration des autonomen Systems 64626

Meine Region hat von der DL-IP-Koordination neben der AS-Nummer 64626 den Adressbereich 44.130.230.0/24 für das lokale Backbonenetz und den Adressbereich 44.130.214.0/24 für das lokale User-/Servicenetz zugewiesen bekommen.

Um nicht alle Adressen des kompletten autonomen Systems zu verbrauchen, habe ich für jeden HAMNET-Standort Teilbereiche aus dem User-/Servicenetz herausgebrochen. Diesen Prozess nennt man „Subnetting“. Auf der Managementwebseite der DL-IP-Koordination (http://www.de.ampr.org/doku.php?id=dokumentation:as-nummern:hamnet-management) zeigt der Abschnitt „Hilfe zur Netzplanung“ die einzelnen Netzbereiche auf. Auch das bereits erwähnte Tool „ipcalc“ eignet sich hervorragend, um erste Erfahrungen mit „Subnetting“ zu sammeln. Auf der Managementseite habe ich meine genutzten Subnetze hinterlegt, sodass neben mir auch weitere Administratoren des gleichen autonomen Systems den Überblick behalten können (das Wiki ist frei editierbar). Beim Aufteilen des Netzes ist darauf zu achten, genügend IP-Adressen für jeden Standort einzuplanen.

Auch das Backbonenetzwerk habe ich auf ein /28-Netz heruntergebrochen und alle Router in ein Layer-2 Netzwerk (d.h. im gleichen Subnetz) untergebracht. Alle Router befinden sich also in einem gebridgten Netz. Die Routeradressen im Backbonenetzwerk sind inkl. Linkfrequenz und Bandbreite ebenso auf der Management-Webseite abgelegt.

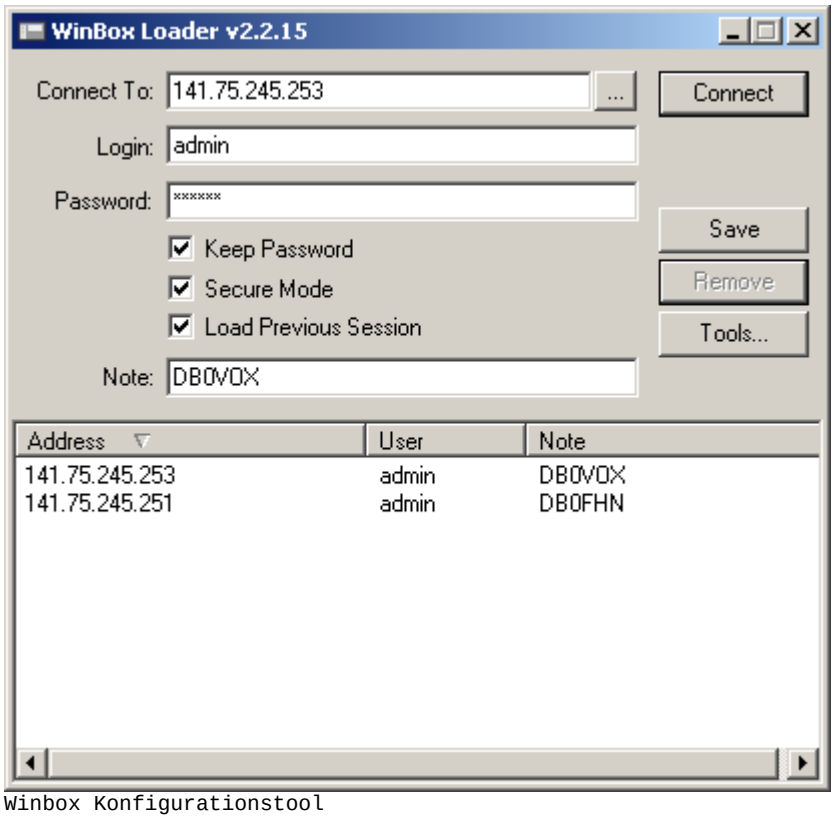
Die Toplogie des Netzes soll so aussehen:



In der Grafik ist jeweils die verwendete IP-Adresse im Backbonenetzwerk (BB) als auch die verwendete IP-Adresse im User-/Servicenetzwerk (NET) zu sehen. Durch die Angabe /<Netzmaske> kann das Netzwerk eindeutig beschrieben werden. „ipcalc“ kommt mit dieser Notation auch zurecht.

In diesem Setup wird nur eine einzige Frequenz mit Point-to-Multipoint-Technik verwendet. DB0VOX hat direkte Sicht zu den Standorten DB0FUE, DB0FOR und DB0FHN.

Die Konfiguration der WLAN-Boards kann mit dem graphischen Tool „winbox“ (http://www.mikrotik.com/download.html) erfolgen. In einem Layer-2 Netzwerk (Ethernet) kann das Board einfach über die MAC-Adresse angesprochen werden (dazu den Button „...“ neben „Connect“ drücken).



Winbox Konfigurationstool

Einen reinen Lesezugang habe ich für den Login „testuser“ ohne Passwort an DB0FHN und DB0VOX angelegt. Interessierte können sich auf DB0FHN (141.75.245.251) oder DB0VOX (141.75.245.253) über das Internet umsehen.

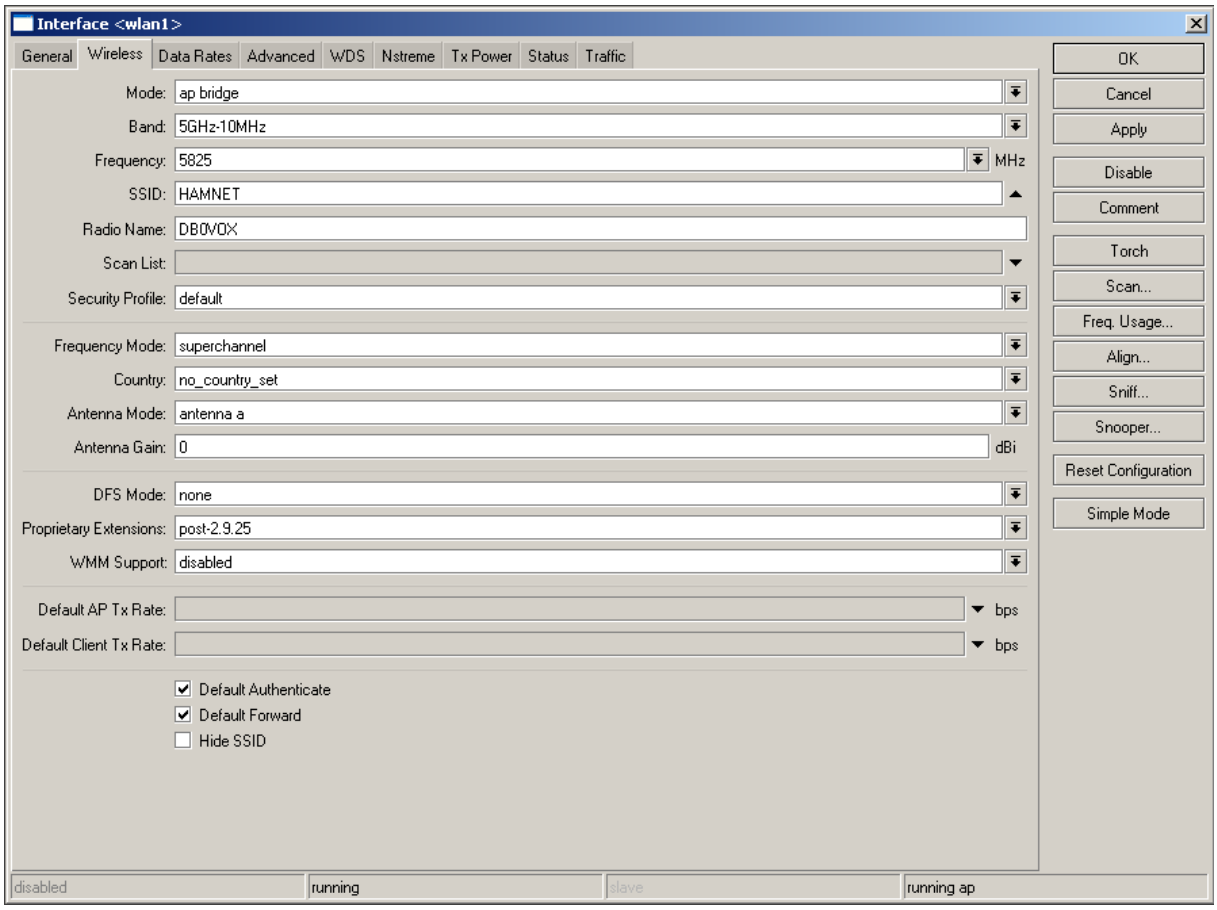
Zur Passwortverwaltung nutze ich persönlich seit Jahren das Programm Keepass (http://keepass.info). Für das HAMNET habe ich mir eine neue Untergruppe erstellt und für die jeweiligen Logins ein Macro in der URL-Spalte abgelegt: „cmd://c:\programme\winbox\winbox.exe 141.75.245.251 {USERNAME} {PASSWORD}“. So kann ich mich mit einem Doppelklick zu allen betreuten HAMNET-Knoten verbinden.

Zunächst wird die WLAN-Konfiguration festgelegt. DB0VOX soll die Zentrale des Point-to-Multipoint Links werden. Da sich die Stationen DB0FUE, DB0FOR und DB0FHN gegenseitig nicht hören, müssen wir hier das „hidden-station“-Problem beachten. An einem Packet Radio Knoten würde man solch ein Problem durch Aktivieren des DAMA-Modus lösen. Mikrotik hat im RouterOS eine Erweiterung des WLAN-Protokolls namens „Nstreme“ zur Verfügung gestellt. Aus der Featureliste:

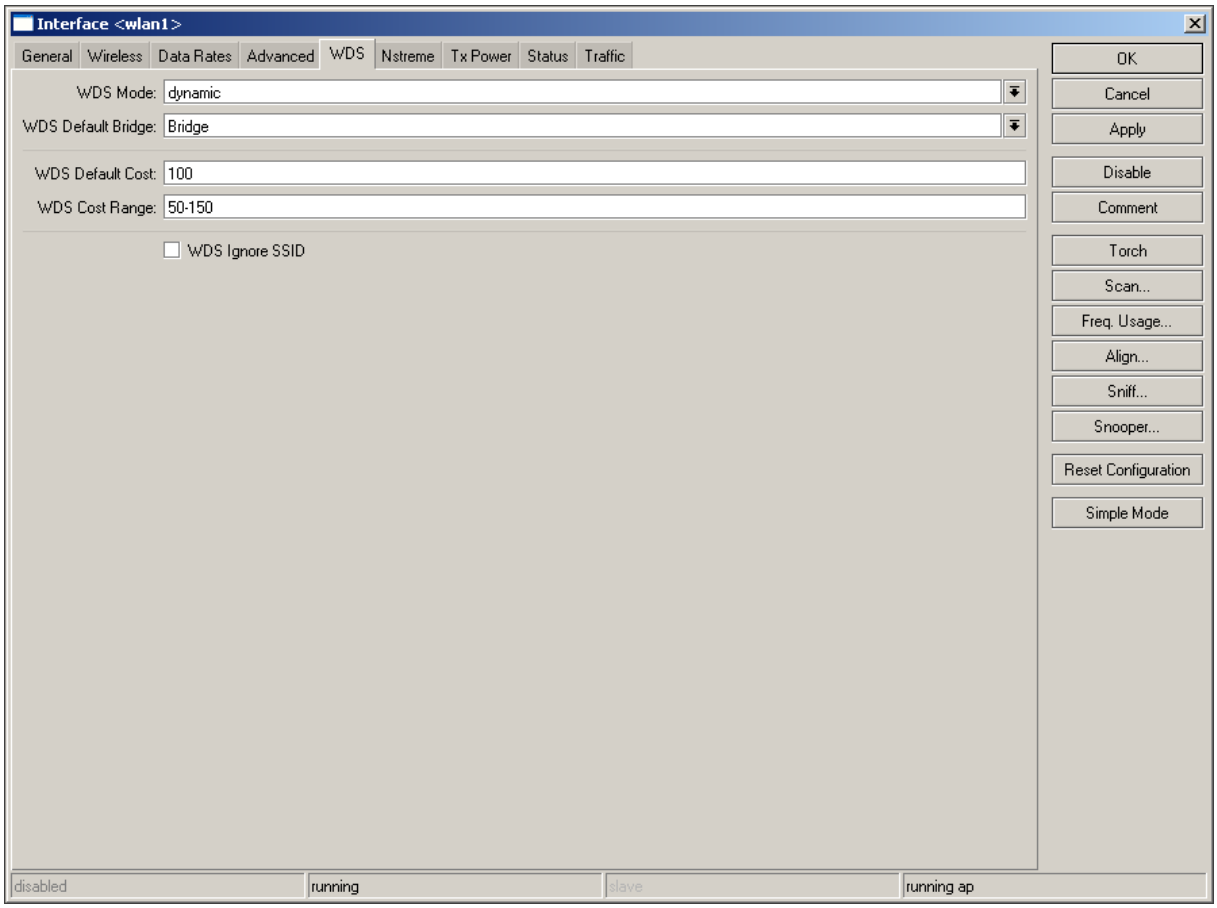
- Client polling. Polling reduces media access times, because the card does not need to ensure the air is "free" each time it needs to transmit data (the polling mechanism takes care of it)
- Very low protocol overhead per frame allowing super-high data rates
- No implied protocol limits on link distance
- No implied protocol speed degradation for long link distances
- Dynamic protocol adjustment depending on traffic type and resource usage

Konfiguration von DB0VOX

Als Erstes wird das WLAN-Interface konfiguriert. Der Wireless-Modus muss auf „ap-bridge“ stehen. Die Bandbreite wird durch Auswahl von „5GHz-10MHz“-Band reduziert. Jetzt noch die gewünschte Frequenz und die Standard-SSID „HAMNET“ eintragen. Als „Radio Name“ wird das eigene Rufzeichen (in diesem Fall DB0VOX) gewählt. Letzteres dient zur Stationsidentifizierung nach $11 der Verordnung zum Gesetz über den Amateurfunk (AFuV). Dabei kommt das MikroTik Neighbour Discovery Protocol (MNDP) zum Einsatz. „antenna a“ entspricht dem „main“-Anschluss der Wistron DCMA-82 WLAN-Karte.

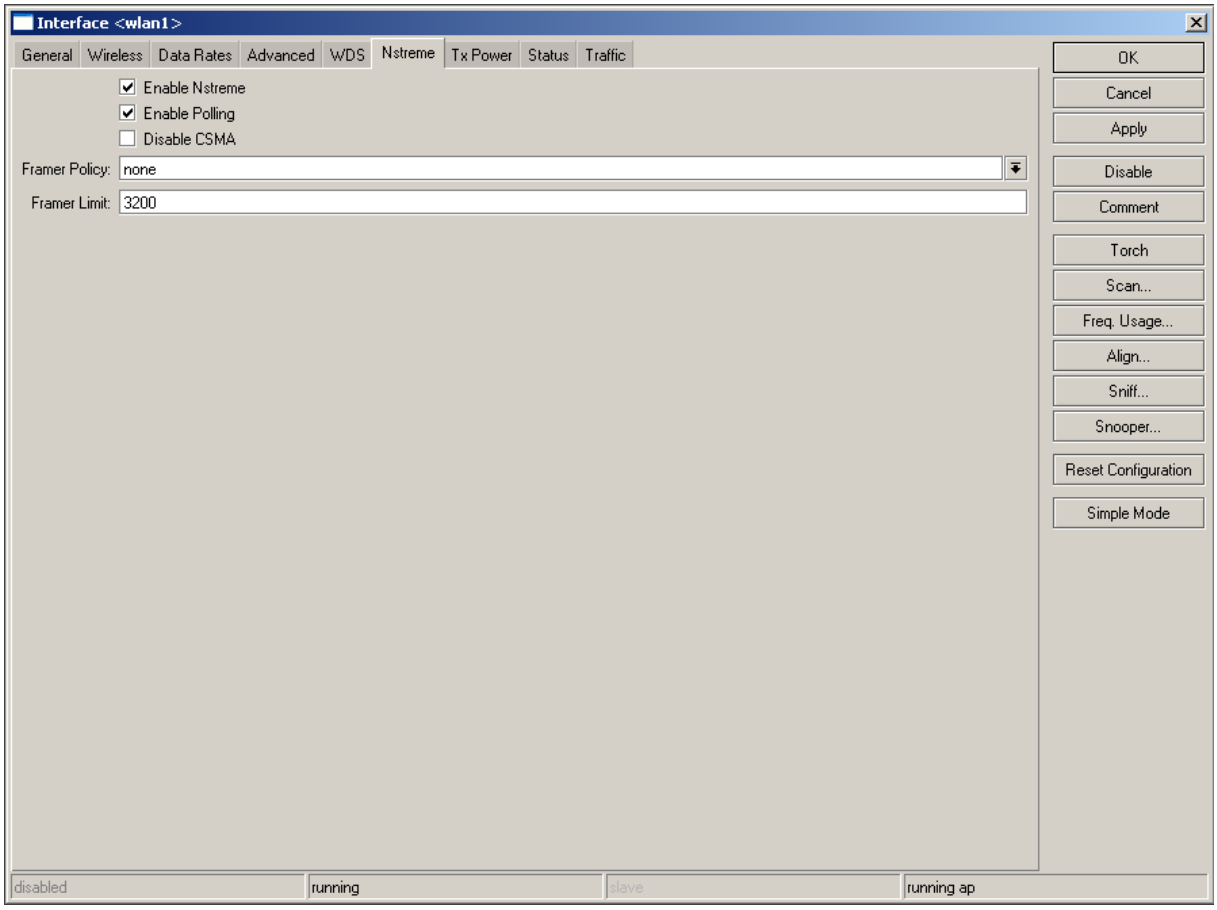


Da wir unser kleines Backbonenetzwerk für die vier Standorte gebridgt (Layer-2) betreiben wollen, müssen wir auf dem Mikrotikrouter eine neue Bridge anlegen. Nun muss das Wireless-Interface für den WDS-Betrieb (Wireless Distribution System) (http://de.wikipedia.org/wiki/Wireless_Distribution_System) konfiguriert werden. Alle neuen WDS-Clients, die sich am DB0VOX-System anmelden, werden jeweils über ein neues WDS-Interface im System eingebunden. Alle neuen WDS-Interfaces sollen zu einer Layer-2-Bridge automatisch hinzugefügt werden. Diese entsprechende Einstellung muss vorgenommen werden.

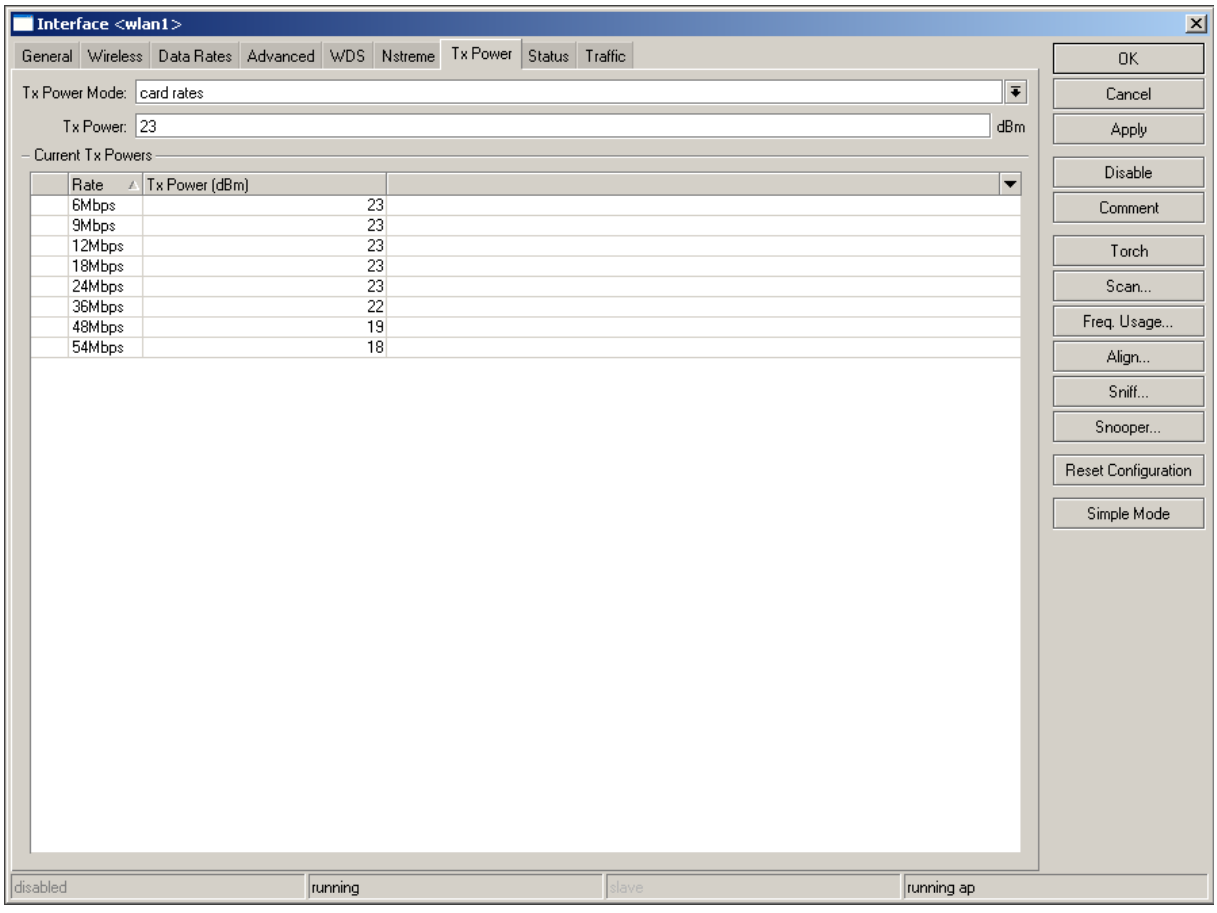


Alternativ zum dynamischen WDS-Mode könnte man auch den WDS-Mode auf „static“ setzen und alle WDS-Interfaces mit der MAC-Adresse des jeweiligen Linkpartners händisch hinzufügen. Diese wiederum müssten händisch der Bridge hinzugefügt werden. Dies hat den Vorteil, dass nur registrierte MAC-Adressen Zugriff erhalten.
Bei einem Point-to-Point-Link könnte man sich die Bridge auch komplett sparen und mit dem händisch erzeugten WDS-Interface weiterarbeiten.

Weiterhin wird der Nstreme-Modus aktiviert.



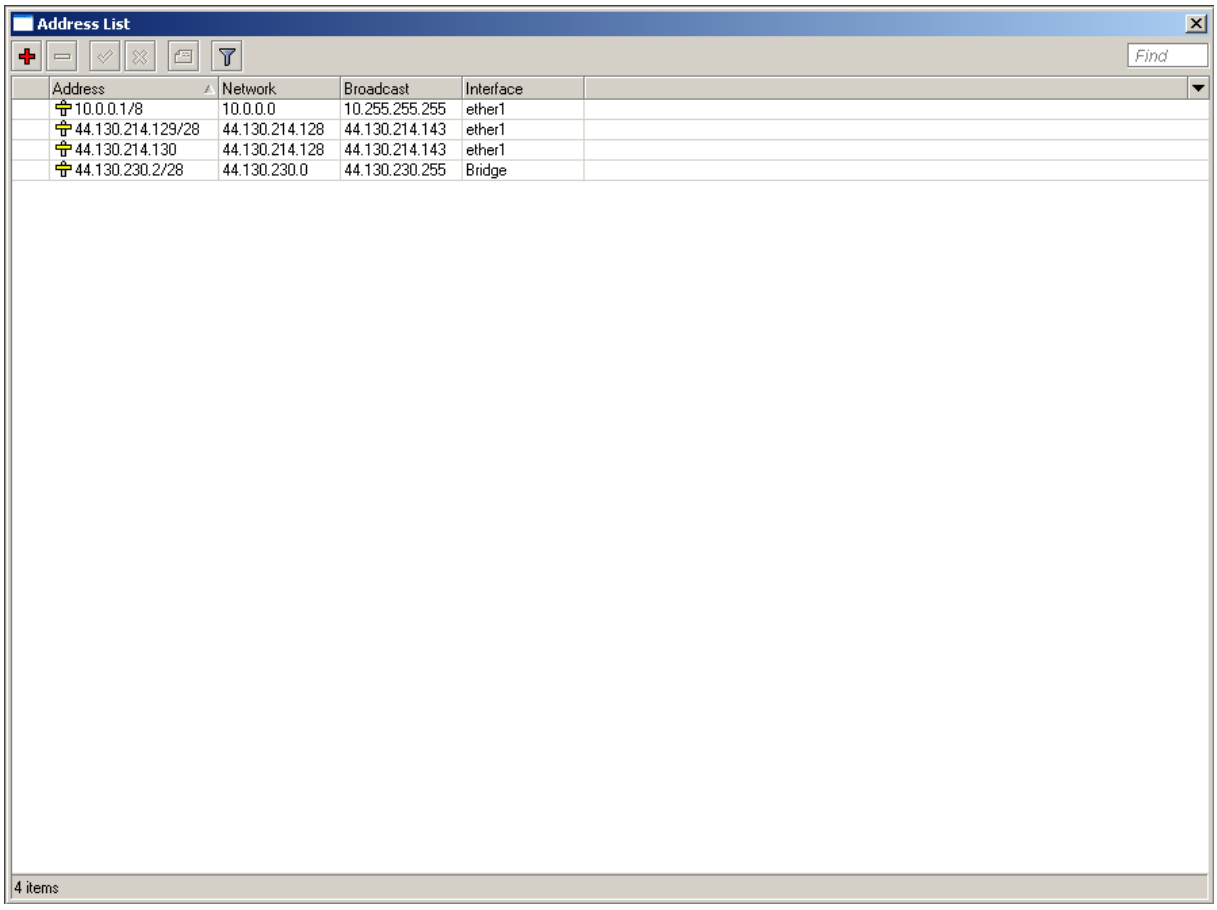
Die Sendeleistung stellen wir auf den Standardwert der Karte.



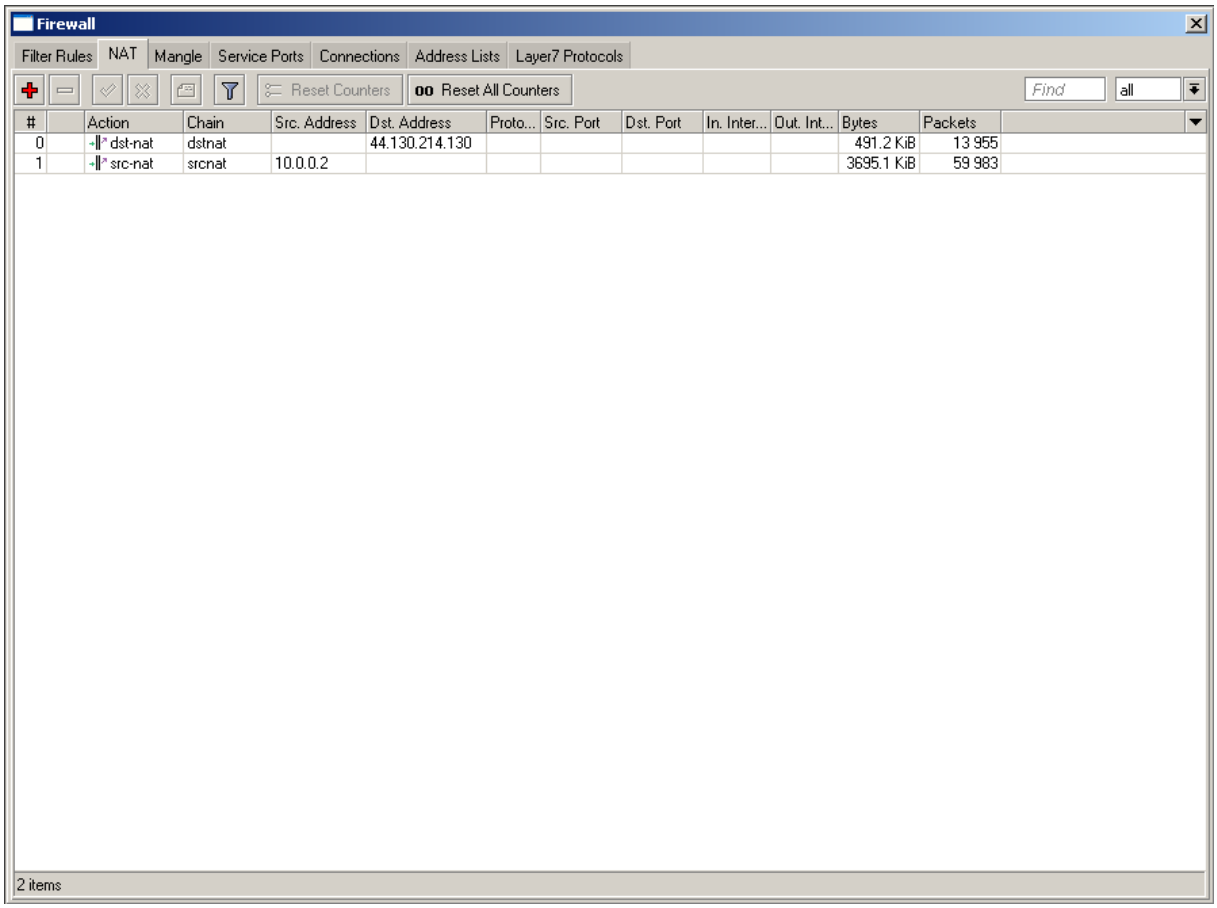
Die Wirelesskonfiguration ist damit abgeschlossen.

Nun können die IP-Adressen und IP-Netze den jeweiligen Interfaces zugeordnet werden. Dem Bridge-Interface wird die IP-Adresse 44.130.230.2/28 aus dem Backbonenetzwerk hinzugefügt. Die Eingabe mit /28 bewirkt dabei, dass die Netzwerkadresse und Broadcastadresse gleich korrekt gesetzt werden. Dem Ethernetinterface, an dem unsere Endgeräte am Standort über einen Switch dranhängen, weisen wir die geplante IP-Adresse 44.130.214.129/28 aus dem User-/Servicenetz zu.

Am Standort ist außerdem ein D-Star-Gateway aktiv. Laut Systembeschreibung sollte solch ein Gateway mit der Adresse 10.0.0.1/8 (D-Star-Gateway) und einem Defaultrouter 10.0.0.2/8 (Mikrotik-Router) betrieben werden. Um dieser Forderung nachzukommen, können wir dem Ethernetinterface einfach die benötigte Adresse 10.0.0.2/8 hinzufügen. Zusätzlich muss eine Adresse aus dem User-/Servicenetz gewählt werden, unter der später das D-Star-Gateway (10.0.0.1) erreichbar sein soll. Wir haben uns für die Adresse 44.130.214.130 entschieden.

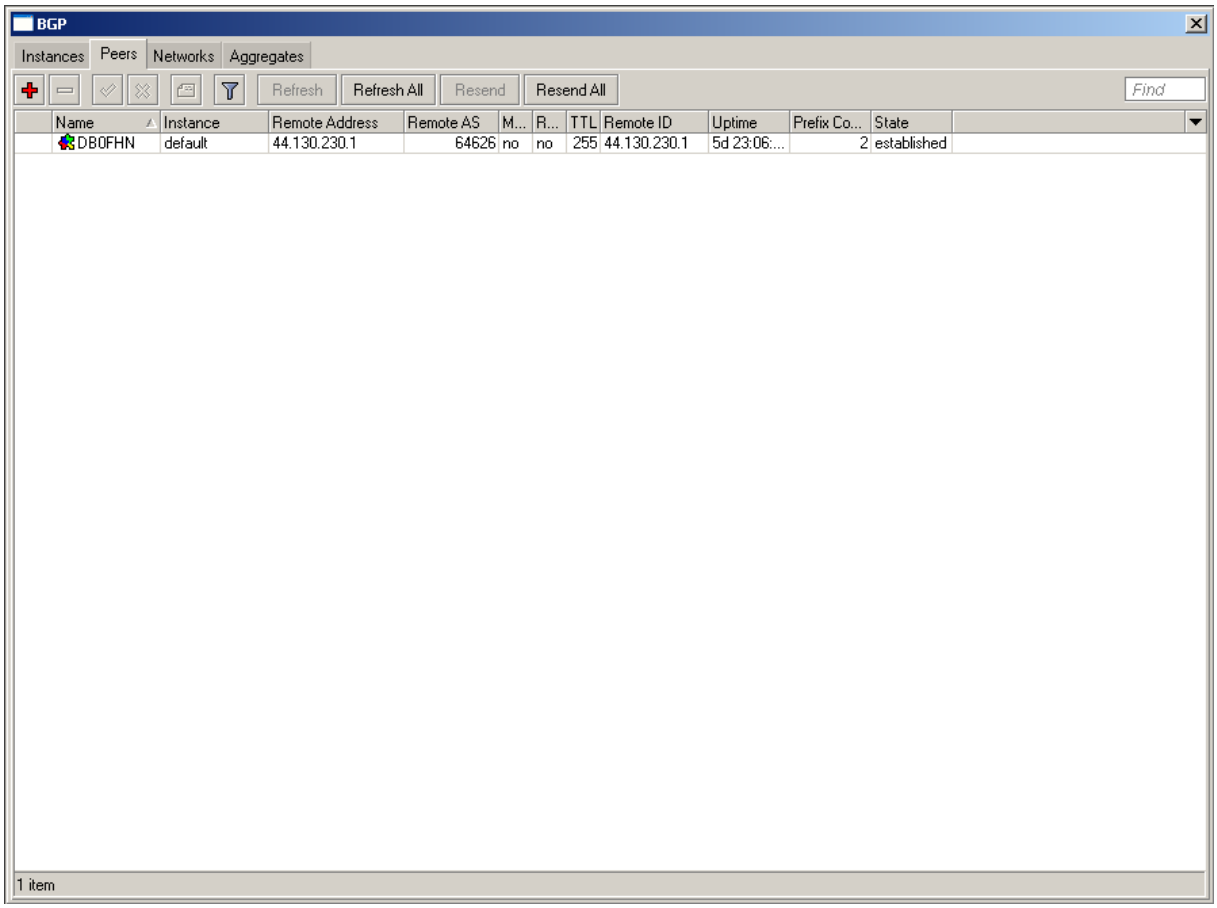


Um nun das D-Star-Gateway (10.0.0.1) unter der HAMNET-Adresse 44.130.214.130 ansprechbar zu machen, bedienen wir uns der sogenannten Network-Adress-Translation Technik (NAT, http://de.wikipedia.org/wiki/Network_Address_Translation). In der Firewall werden dazu unter NAT zwei neue Regeln hinzugefügt: In der chain „dstnat“ mit der destination-Adresse 44.130.214.130 wird die Aktion „dst-nat“ zur Adresse 10.0.0.2 eingerichtet. Zusätzlich wird in der chain „srcnat“ mit der source-Adresse 10.0.0.2 die Aktion „src-nat“ zur Adresse 44.130.214.130 hinzugefügt.

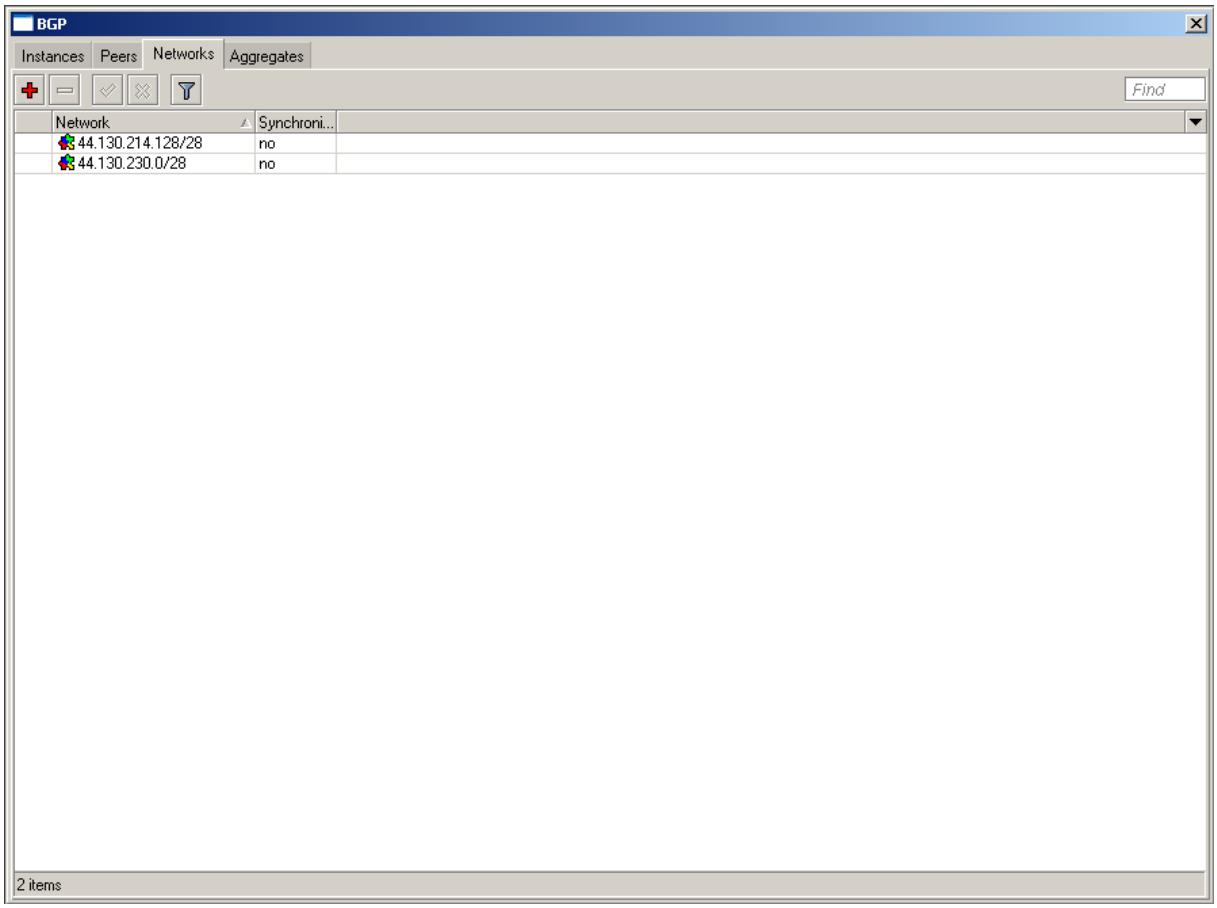


Als letzter Schritt muss das IP-Routing eingerichtet werden. Unter dem BGP-Routing trägt man für die Standard-Instanz seine eigene AS-Nummer ein (hier 64626). Nun müssen für alle weiteren BGP-Router mit der gleichen AS-Nummer jeweils ein BGP-Link eingetragen werden. Diese Links werden mit iBGP für „internal-BGP“ bezeichnet. Da DB0FUE und DB0FOR noch nicht QRV sind, haben wir zunächst nur den Linkpartner DB0FHN (Peer) in das IP-Routing aufgenommen. Beim Hinzufügen der Linkpartner ist darauf zu achten, dass „Nexthop Choice“ auf „force self“ gestellt wird.

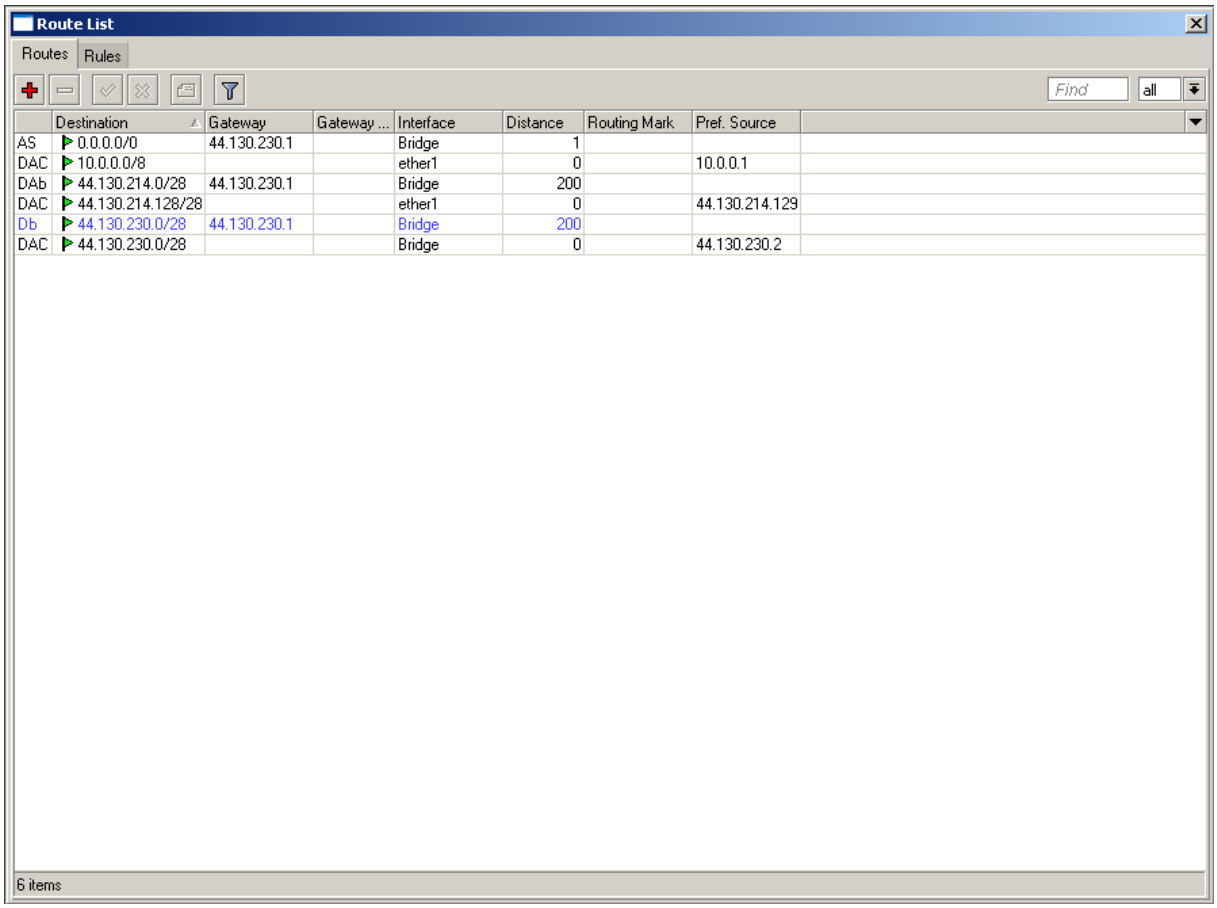
Nachdem der BGP-Router die TCP-Verbindung mit den eingetragenen Peers aufgebaut hat, werden die bekannten IP-Netze ausgetauscht. Zu jedem übertagenen IP-Netz wird auch ein „Nexthop“ mit übertragen. Da dies immer die Adresse des BGP-Routers, über den die Routinginformation reingekommen ist, sein soll, wird „Nexthop Choice“ auf „force self“ gestellt.



Unter „Networks“ werden jetzt alle eigenen Netzwerke zur Verbreitung im HAMNET eingetragen. Hier ist besondere Vorsicht geboten, da leicht falsche Informationen im gesamten HAMNET verbreitet werden könnten. Auf der Management-Webseite der DL-IP-Koordinatoren sollte auch eingetragen werden, ob ein Netz gerade aktiv ist.



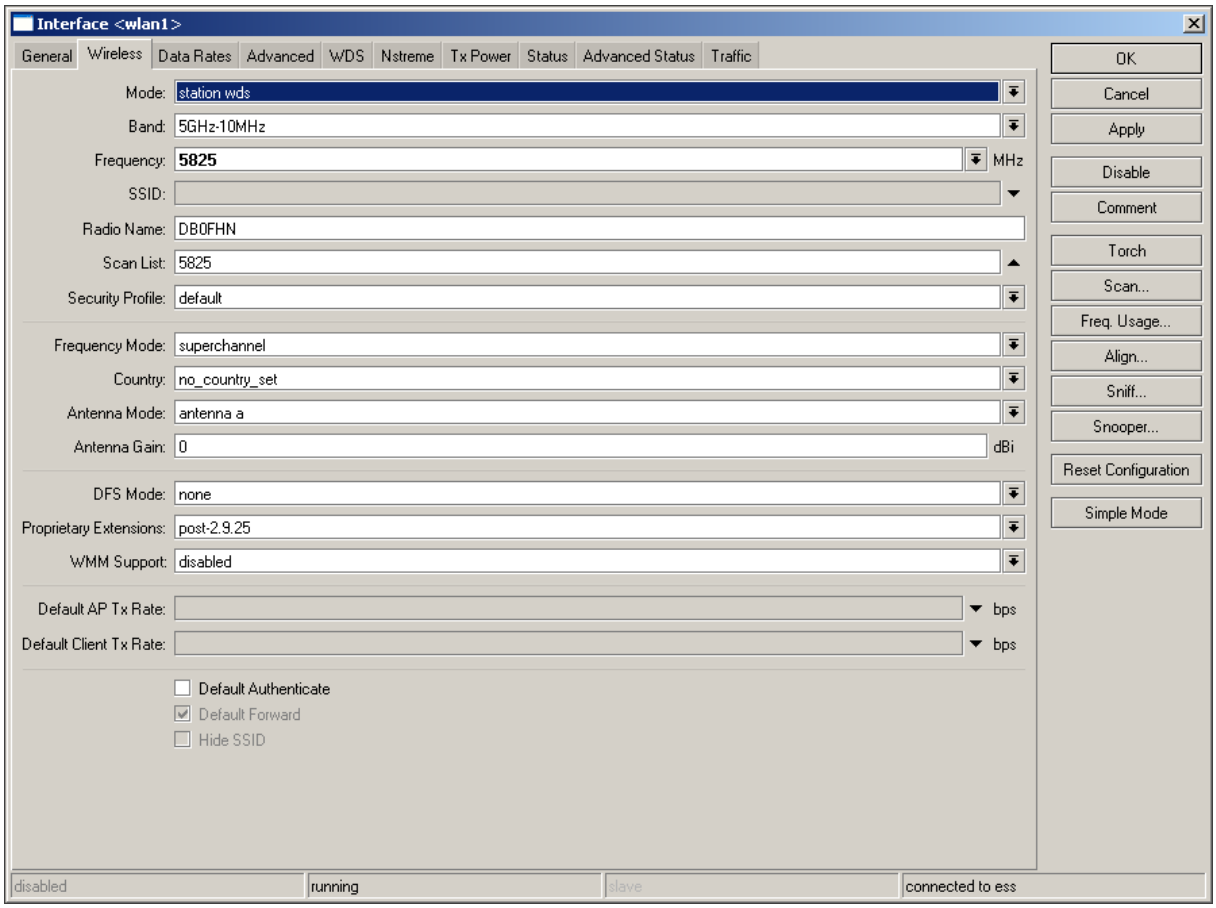
Da in der Regel nur Netze gemeldet („announced“) werden, die einem selbst gehören, muss zuletzt die Defaultroute (0.0.0.0/0) zum Internet manuell gesetzt werden. In unserem Fall ist das der Router von DB0FHN (44.130.230.1).



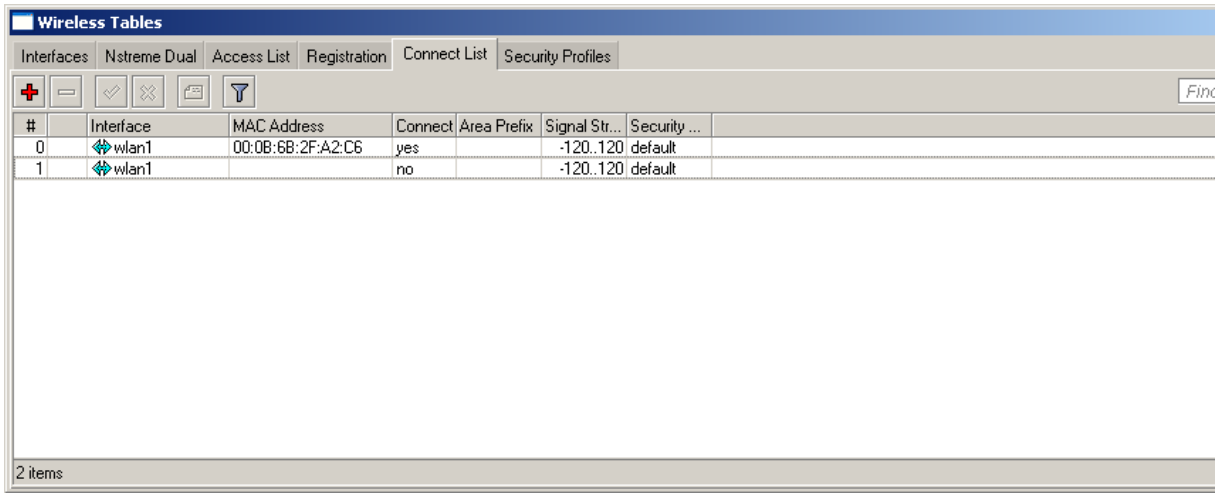
Damit ist die Konfiguration von DB0VOX abgeschlossen.

Konfiguration von DB0FHN

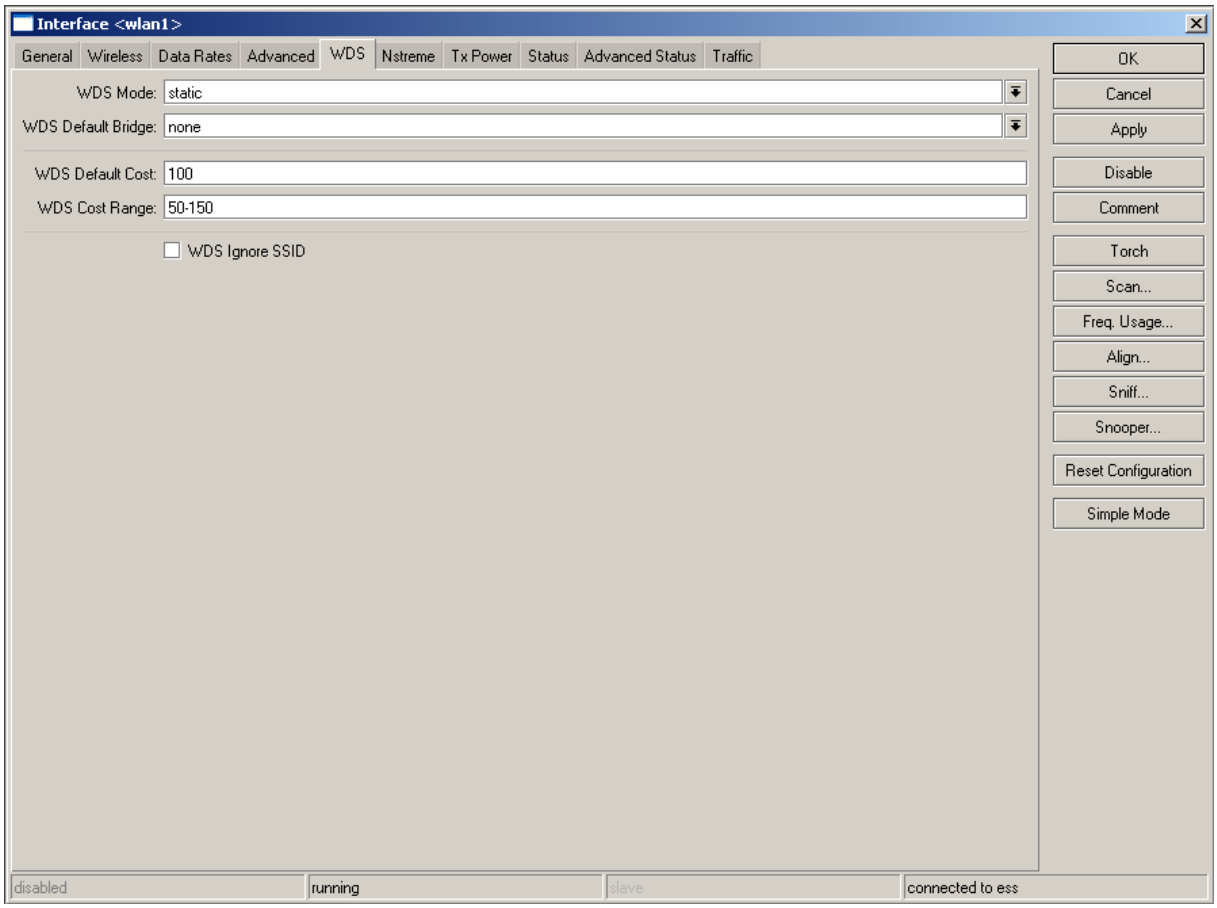
Als Erstes wird das WLAN-Interface konfiguriert. Der Wireless-Modus muss auf „station-wds“ stehen. Die Bandbreite wird durch Auswahl von „5GHz-10MHz“-Band reduziert. Jetzt noch die gewünschte Frequenz setzen und nur diese in der „Scan List“ eintragen. Eine SSID muss nicht eingetragen werden, da wir uns nach der MAC-Adresse von DB0VOX richten werden. Als „Radio Name“ wird das eigene Rufzeichen (in diesem Fall DB0FHN) gewählt.



In der „Connect List“ unter Wireless Tables werden nun zwei neue Einträge hinzugefügt. Ein Eintrag trägt die MAC-Adresse der Gegenstation (in dem Fall die MAC-Adresse von DB0VOX) mit dem Flag „Connect“ = yes und einen weiteren Eintrag ohne MAC-Adresse mit dem Flag „Connect“ = no. Somit ist sichergestellt, dass der Connect nur zu DB0VOX aufgebaut wird. Außerdem ermöglicht dies die Verwendung der einfach ESSID „HAMNET“ für sämtliche Linkstrecken im HAMNET.



Der WDS-Modus wird auf „static“ gesetzt und das Interface an keine Bridge gebunden. Wir werden das Interface direkt konfigurieren.

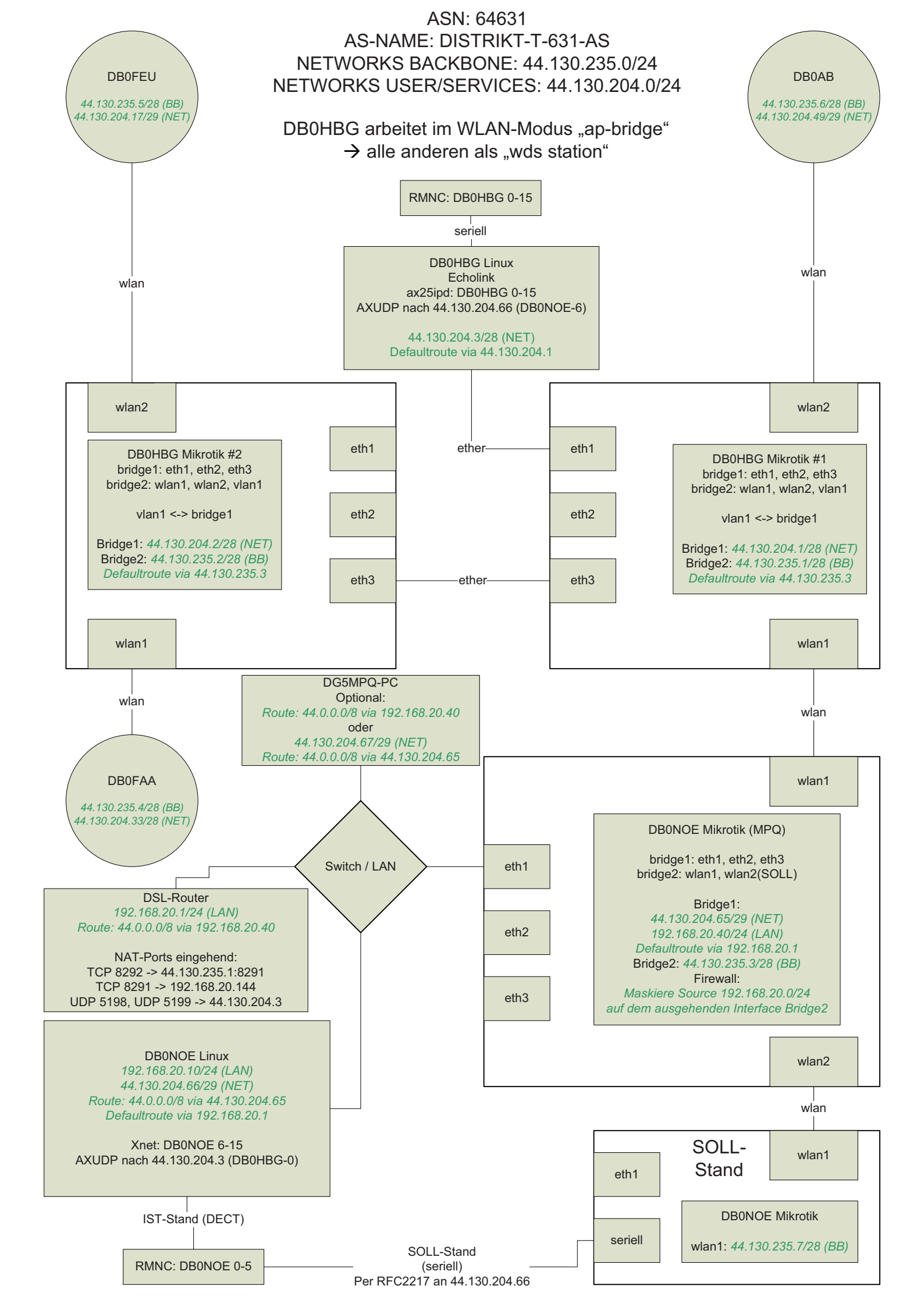


Noch nicht getestet habe ich den Wireless Modus „wds slave“. Interessant wäre es, wenn man auch direkt am DB0FHN-Standort über die Linkfrequenz für Servicearbeiten mit dem Notebook einsteigen könnte. Im Modus „station-wds“ funktioniert dies nicht.

Alle weiteren Schritte werden analog zur Konfiguration von DB0VOX durchgeführt. Das Backbonenetzwerk liegt nur auf dem WLAN-Interface an, da eine Bridge nicht existiert.

Die Linkstrecke DB0FHN <-> DB0VOX läuft nun seit dem Aufbau im September 2009 durchgehend stabil. Der Linktest nach DB0FUE hat inklusive des Routings auch bereits funktioniert.

Netzplan rund um den Distrikt T


ASN: 64631
AS-NAME: DISTRIKT-T-631-AS
NETWORKS BACKBONE: 44.130.235.0/24
NETWORKS USER/SERVICES: 44.130.204.0/24
DB0HBG arbeitet im WLAN-Modus „ap-bridge“
→ alle anderen als „wds station“
DB0FEU
44.130.235.5/28 (BB)
44.130.204.17/29 (NET)
DB0AB
44.130.235.6/28 (BB)
44.130.204.49/29 (NET)
RMNC: DB0HBG 0-15
seriell
DB0HBG Linux
Echolink
ax25ipd: DB0HBG 0-15
AXUDP nach 44.130.204.66 (DB0NOE-6)
44.130.204.3/28 (NET)
Defaultroute via 44.130.204.1
wlan
wlan
wlan2
DB0HBG Mikrotik #2
bridge1: eth1, eth2, eth3
bridge2: wlan1, wlan2, vlan1
vlan1 <-> bridge1
Bridge1: 44.130.204.2/28 (NET)
Bridge2: 44.130.235.2/28 (BB)
Defaultroute via 44.130.235.3
eth1
eth2
eth3
ether
ether
eth1
eth2
eth3
wlan2
DB0HBG Mikrotik #1
bridge1: eth1, eth2, eth3
bridge2: wlan1, wlan2, vlan1
vlan1 <-> bridge1
Bridge1: 44.130.204.1/28 (NET)
Bridge2: 44.130.235.1/28 (BB)
Defaultroute via 44.130.235.3
wlan1
wlan1
wlan
wlan
DG5MPQ-PC
Optional:
Route: 44.0.0.0/8 via 192.168.20.40
oder
44.130.204.67/29 (NET)
Route: 44.0.0.0/8 via 44.130.204.65
DB0FAA
44.130.235.4/28 (BB)
44.130.204.33/28 (NET)
wlan1
Switch / LAN
eth1
eth2
eth3
DB0NOE Mikrotik (MPQ)
bridge1: eth1, eth2, eth3
bridge2: wlan1, wlan2(SOLL)
Bridge1:
44.130.204.65/29 (NET)
192.168.20.40/24 (LAN)
Defaultroute via 192.168.20.1
Bridge2: 44.130.235.3/28 (BB)
Firewall:
Maskiere Source 192.168.20.0/24
auf dem ausgehenden Interface Bridge2
wlan2
DSL-Router
192.168.20.1/24 (LAN)
Route: 44.0.0.0/8 via 192.168.20.40
NAT-Ports eingehend:
TCP 8292 -> 44.130.235.1:8291
TCP 8291 -> 192.168.20.144
UDP 5198, UDP 5199 -> 44.130.204.3
DB0NOE Linux
192.168.20.10/24 (LAN)
44.130.204.66/29 (NET)
Route: 44.0.0.0/8 via 44.130.204.65
Defaultroute via 192.168.20.1
Xnet: DB0NOE 6-15
AXUDP nach 44.130.204.3 (DB0HBG-0)
wlan
SOLL-Stand
wlan1
eth1
seriell
DB0NOE Mikrotik
wlan1: 44.130.235.7/28 (BB)
IST-Stand (DECT)
RMNC: DB0NOE 0-5
SOLL-Stand
(seriell)
Per RFC2217 an 44.130.204.66

Der Netzplan wurde für das autonome System 64631 konzipiert. Man sieht in ihm die genaue Struktur der Netze an DB0HBG und DB0NOE. Die Linkpartner DB0AB, DB0FEU und DB0FAA sind nur mit ihren Backboneadressen und Netzwerkadressen angegeben. An DB0NOE existiert ein privates LAN (Netzwerk 192.168.20.0/24) mit einem DSL-Internetanschluss. Der DSL-Router ist eine Fritzbox und hat die Adresse 192.168.20.1. In diesem Netzwerk sollen neben einem temporären Netzteilnehmer (DG5MPQ) auch der Linuxserver von DB0NOE 192.168.20.10 und das Mikrotik-Routerboard 192.168.20.40 erreichbar sein. Damit das Netz 192.168.20.0/24 auch lokal bleibt, darf das Ethernet vom Mikrotik-Routerboard nicht mit den WLAN-Interfaces auf Layer-2-Ebene zusammengebridgt werden.

Für das User-/Servicenetz am DB0NOE-Standort wurde das Netzwerk 44.130.204.64/29 aus dem zugewiesenen Netz 44.130.204.0/24 herausgebrochen. Es kann bis zu 6 Rechner beheimaten und soll an allen drei Ethernetports anliegen, weshalb eth1, eth2 und eth3 zur bridge1 auf Layer-2-Ebene zusammengeschaltet werden. Der Bridge wird aus dem User-/Servicenetz die Adresse 44.130.204.65 zugeteilt. Somit sind noch 5 weitere IP-Geräte adressierbar.

Aus dem Backbonenetz 44.130.235.0/24 wurde für das gesamte Netz der Bereich 44.130.235.0/28 herausgebrochen. Das Backbonenetzwerk erstreckt sich über zwei WLAN-Interfaces (wlan1 & wlan2). Obwohl wlan2 erst geplant ist und das Backbonenetzwerk direkt auf dem wlan1-Interface konfiguriert werden könnte, ist es sinnvoll, sich für eine neue Bridge (bridge2) zu entscheiden und die Backbonenetzwerkadresse 44.130.235.3 dort zu definieren. Wird die zweite Karte aktiviert, so muss nur noch das wlan2-Interface der Bridge hinzugefügt werden. Es ist keine Rekonfiguration der IP-Adressen auf andere Interfaces nötig. Hat die Hardware (wie das Mikrotik RB411AH) nur einen Ethernetport und ein WLAN-Interface vereinfacht sich die Konfiguration, da selten eine Bridge benötigt wird.

An DB0HBG wird das gleiche Backbonenetz verwendet. Nur das User-/Servicenetz ist ein anderes (jeder Standort sollte sein eigenes User-/Servicenetz haben). Es ist das Netz 44.130.204.0/28 und kann bis zu 13 weitere Geräte neben dem Mikrotik-Board selbst beheimaten. An DB0HBG kommen zwei Mikrotik Routerboards mit jeweils drei Ethernetports zum Einsatz. Die drei Ethernetports werden wieder an jedem Board zu Bridges zusammengefasst (jeweils „bridge1“ genannt). „bridge1“ auf Board 1 erhält die Adresse 44.130.204.1 und die „bridge1“ auf Board 2 erhält die Adresse 44.130.204.2 aus dem User-/Servicenetz. Über ein LAN-Kabel werden beide Boards miteinander verbunden (über die Ports „eth3“).Das Backbonenetzwerk soll komplett gebridgt sein. Daher wird an jedem Board eine Bridge für sämtliche WLAN-Interfaces eingeplant und die entsprechend vorgesehenen Backbonenetzadressen gesetzt.

Jetzt ergibt sich das Problem, dass das Backbonenetzwerk auch gebridgt vom Board 1 zum Board 2 gelangen muss. Jedes Interface darf nur einer Bridge zugeordnet sein, da man sonst das User-/Servicenetz mit dem Backbonenetz vermischen würde und das User-/Servicenetz damit nicht lokal gehalten werden kann. Die einfachste Variante zur Lösung ist, das Interface „eth3“ aus der Bridge1 (User-/Servicenetz) zu entfernen und der Bridge2 (Backbonenetz) hinzuzufügen. Dabei können allerdings zwei LAN-Ports eines Boards nicht mehr für das User-/Servicenetz genutzt werden.

Alternativ kann man sich der „Virtual Local Area Netzwork“-Technik (VLAN, http://de.wikipedia.org/wiki/Virtual_Local_Area_Network) bedienen. Dabei wird einem beliebigen Interface ein VLAN-Interface mit einer bestimmten ID hinzugefügt. Wird einem weiteren Gerät im gleichen Netzwerk auf Layer-2-Ebene dem entsprechenden Interface ein VLAN-Interface mit derselben ID hinzugefügt, so können beide Geräte wie in einem neuen Layer-2 Netzwerk Informationen austauschen, ohne dass Pakete über das ganze Basisnetzwerk auftauchen. In unserem Fall haben wir auf beiden Boards der „bridge1“ (mit

dem User-/Servicenetz) das VLAN-Interface „vlan1“ mit derselben ID hinzugefügt. Der „bridge2“ (mit dem Backbonenetz) haben wir dann das „vlan1“ Interface hinzugefügt. Jetzt sind alle Ethernetports mit dem User-/Servicenetz belegt und „on-top“ wird der Backbonenetzwerkverkehr abgewickelt, ohne das IP-Pakete aus dem Backbonenetz im User-/Servicenetz zu sehen sind.

Am DB0HBG Standort befindet sich ein Echolinkgateway, welches mit Internet versorgt werden soll. Seine IP-Adresse aus dem User-/Servicenetz lautet 44.130.204.3. Das Echolinkgateway benötigt ein Standardgateway aus seinem eigenen Netz. Wir geben hier das Mikrotikboard 44.130.204.1 als Standardgateway an. Auch das Mikrotikboard benötigt ein Standardgateway, welchem die Pakete in Richtung Internet übergeben werden können. Der Pfad im Backbonenetzwerk verläuft zum Mikrotik-Router von DB0NOE. Es wird also als Standardgateway (neue Route mit 0.0.0.0/0) also die IP-Adresse 44.130.235.3 angegeben. Der Mikrotik-Router an DB0NOE muss das Paket an den DSL-Router weitersenden. Daher wird die Defaultroute via 192.168.20.1 (DSL-Router) eingetragen. Damit ist der Weg für ausgehende Pakete vom Echolink-Gateway zum Internet frei.

Der Rückweg aus dem Internet zum Echolinkgateway ist noch nicht definiert. Der DSL-Router kennt bisher nur das Netz 192.168.20.0/24 und kann deshalb Pakete für 44.130.204.6 (Echolinkgateway) nicht vermitteln. Ein Weg wäre, es auf dem Mikrotik-Board an DB0NOE sogenanntes Masquerading (http://de.wikipedia.org/wiki/Masquerading) einzurichten. Jeder DSL-Router kennt dieses Verfahren, da interne IP-Adressen nach RFC1918 (z.B. 192.168.20.40) nicht im Internet geroutet werden. Der DSL-Router bekommt nur eine IP-Adresse aus dem öffentlichen Internet von seinem Provider zugewiesen. Sämtlicher Datenverkehr aus dem Netz 192.168.20.0/24 muss der Router als in Richtung Internet „maskieren“. Selbes Verfahren wäre jetzt auch auf dem Mikrotik-Board möglich, welches ich aber nicht empfehle.

Die Grundregel lautet Masquerading bzw. Network Address Translation (NAT) zu vermeiden, wenn direktes Routing genutzt werden kann. Viele DSL-Router bieten die Möglichkeit, manuelle IP-Routen einzutragen. In unserem Fall ist es nötig, das Netz 44.0.0.0/8 im Router zu definieren. Es soll über das Gateway 192.168.20.40 (der Mikrotik-Router) gesendet werden. Damit ist auch der Rückweg vollständig beschrieben. Wie von Echolink gewohnt, müssen im DSL-Router noch die UDP-Ports 5198 und 5199 auf die IP-Adresse des Echolinkrechners (44.130.204.3) weitergeleitet werden.

Im User-/Servicenetz von DB0NOE soll der Linuxserver aus dem HAMNET erreichbar sein. Daher wird dem Server neben seiner LAN-Adresse 192.168.20.10 noch die Adresse 44.130.204.66 für das Ethernetinterface zugewiesen (IP-Aliasing). Wie beim DSL-Router, muss ihm noch die Route zum HAMNET (44.0.0.0/8) über das Gateway 44.130.204.65 (Mikrotikboard im User-/Servicenetz) mitgeteilt werden (Vorsicht: Nicht über 192.168.20.40 routen, da sonst abgehende Pakete mit der falschen Source-IP-Adresse auf die Reise gehen).

DB0NOE und DB0HBG sind Packet Radio Knoten und möchten AX.25 Linkstrecken über das HAMNET definieren. Auf dem Linuxserver läuft unter DB0NOE 6-15 ein AX.25-Knoten mit Xnet. Er ist seriell mit dem RMNC DB0NOE 0-5 verbunden. Der RMNC DB0HBG 0-15 hängt seriell am Echolinkrechner (Linux). Auf diesem läuft der ax25ipd, welcher serielle Pakete von DB0HBG in UDP-Pakete verpackt und über das HAMNET an die Zieladresse des DB0NOE-Linuxrechners verschickt. Dieser Pfad funktioniert auch in die andere Richtung.

Steckt man einen Rechner am LAN von DB0NOE an, so wird eine IP-Adresse aus dem Adresspool 192.168.20.0/24 mit dem Standardgateway 192.168.20.1 vom DSL-Router an den Rechner vergeben. Will dieser auf das HAMNET zugreifen, schickt er die Anfrage an den DSL-Router, welcher das Paket aufgrund der eingerichteten Netzroute nach 44.0.0.0/8 an den Mikrotik-Router schickt.

Das Paket würde jetzt mit der vorhin vergebenen Quell-IP-Adresse aus 192.168.20.0/24 auf die Reise gehen. Private LAN-Adressen werden aber im HAMNET wie auch im Internet nicht geroutet. Daher muss der Mikrotik-Router Pakete in Richtung HAMNET maskieren. Es dürfen nur ausgehende Pakete (in Richtung HAMNET) mit Quell-IP-Adressen aus 192.168.20.0/24 maskiert werden, da sonst Pakete aus dem Internet auch maskiert werden würden.

Möchte man den Weg vom zusätzlich eingesteckten Rechner zum HAMNET abkürzen, so kann man den Zwischenroutingschritt über den DSL-Router mit einer manuell gesetzten Netzroute nach 44.0.0.0/8 über 192.168.20.40 abkürzen.

Soll der eingesteckte Rechner auch direkt aus dem HAMNET angesprochen werden können, so muss zusätzlich auf dem Interface eine IP-Adresse aus dem User-/Servicenetzpool gesetzt werden. Dann muss die Route nach 44.0.0.0/8 allerdings über 44.130.204.65 gesetzt werden, da sonst abgehende Pakete mit der falschen Quell-IP-Adresse auf die Reise gehen.

Zur Konfiguration der Mikrotikboards über das Internet ist es notwendig, einen beliebigen TCP-Port vom DSL-Router auf den Port TCP-Port 8291 (Standard) des Mikrotikboards weiterzuleiten. Da nur eine IP-Adresse vom DSL-Provider zur Verfügung steht, aber zwei Boards angesprochen werden sollen, müssen verschiedene TCP-Ports zur Weiterleitung auf das entsprechende Board eingerichtet werden. Das Board von DB0NOE ist unter 8291 und das Board von DB0HBG unter 8292 erreichbar.

Zur Verbreitung der IP-Routen im HAMNET sollte an jedem Standort nur ein BGP-Router aktiv sein. Er ist nur dann nötig, wenn für ein funktionierendes Routing auch Routen ausgetauscht werden müssen. In unserem Fall muss das User-/Servicenetz von DB0HBG an DB0NOE und andersherum bekannt gemacht werden. Dazu wird ein BGP-Link (eine TCP-Session) zwischen beiden Boards eingerichtet. Da sie sich im gleichen AS befinden, wird automatisch „internal BGP“ gesprochen. Als Zieladressen werden die Adressen der Routerboards aus dem Backbonenetz verwendet. Ansonsten empfiehlt es sich die Routerboards über die User-/Servicenetzadresse anzusprechen. DB0HBG wird also seine eigenen Netze 44.130.204.0/28 und 44.130.235.0/28 announcen. DB0NOE wird seine eigenen Netze 44.130.204.64/29 und 44.130.235.0/28 announcen. Kommen weitere Linkpartner mit gleicher AS-Nummer hinzu, muss für jeden neuen Teilnehmer ein BGP-Link eingerichtet werden. Sind also alle geplanten Standorte des gleichen AS vernetzt (DB0AB, DB0FEU, DB0FAA, DB0HBG und DB0NEU), müssen 5 * 4 = 20 BGP-Sessions im Backbonenetz aktiv sein.

Netzplan rund um den Distrikt C

ASN: 64625
AS-NAME: DISTRIKT-C-625-AS
NETWORKS BACKBONE: 44.130.229.0/24
NETWORKS USER/SERVICES: 44.130.216.0/24

DB0AAT:
44.130.229.240/28 (BB) -> 44.130.229.252
44.130.229.240/28 (BB) -> 44.130.229.254
44.130.216.0/28 (NET)

DB0INN:
44.130.229.240/28 (BB) -> 44.130.229.253
44.130.216.32/29 (NET)

DB0HOB:
44.130.229.240/28 (BB) -> 44.130.229.248
44.130.229.240/28 (BB) -> 44.130.229.247
44.130.216.48/29 (NET)

DB0WAI:
44.130.229.240/28 (BB) -> 44.130.229.246
44.130.216.64/29 (NET)

DB0xxx (Neumarkt St. Veit):
44.130.229.240/28 (BB) -> 44.130.229.245
44.130.216.80/29 (NET)

BGP: NET + BB announcen!

DB0xxx
Neumarkt (St.Veit)
44.130.229.245/28 (BB)
44.130.216.81/29 (NET)

wds-static

Clubstation
Rosenheim
44.130.216.51/29 (NET)

wds-dyn

RMNC: DB0HOB 0-8

seriell

DB0HOB WRT54

Xnet: DB0HOB 9-15
Port+Link: 44.130.216.3 (DB0AAT-10)

44.130.216.52/28 (NET)
Defaultroute via 44.130.216.49

DB0WAI
44.130.229.246/28 (BB)
44.130.216.65/29 (NET)

wlan

wlan2

DB0HOB Mikrotik #1
eth1 -> vlan1

bridge1: eth1, eth2, wds-dyn(wlan2)
bridge2: wlan1, wds-static(wlan2), vlan1

bridge1: *44.130.216.49/29 (NET)*
bridge2: *44.130.229.248/28 (BB)*

Defaultroute via 44.130.229.253

eth2
(master)

Switch

eth3

ether

eth1

wlan1

ether

eth2
(master)

Switch

eth3

eth1

wlan1

DB0HOB Mikrotik #2
eth1 -> vlan1

bridge1: vlan1, eth2
bridge2: wlan1, wlan2, eth1

bridge1: *44.130.216.50/29 (NET)*
bridge2: *44.130.229.247/28 (BB)*

Defaultroute via 44.130.229.253

wlan2

wlan 5685 MHz 10 MHz

wlan1

DB0AAT Mikrotik #2 (RB411)

bridge1: wlan1, eth1

eth1: *44.130.229.252/28 (BB)*
Defaultroute via 44.130.229.253

eth1

ether

eth1

DB0AAT Mikrotik #1 (RB433)

bridge1: wlan1, eth1

bridge1: *44.130.229.254/28 (BB)*
eth2: *44.130.216.1/28 (NET)*
Defaultroute via 44.130.229.253

eth2
(master)

Switch

eth3

ether

ether

wlan1

DB0AAT WRT54

Xnet: DB0AAT 10-15
Port+Link: 44.143.42.101 (OE2XZR-10)
Port+Link: 44.130.216.52 (DB0HOB-9)
Port: 44.130.216.4 (PC1)
Port: 44.130.216.5 (PC2)
Port: 44.130.216.6 (PC3)

44.130.216.3/28 (NET)
Defaultroute via 44.130.216.1

PC1
44.130.216.4/28 (NET)
Defaultroute via 44.130.216.1
AX.UDP nach 44.130.216.3

wlan 5825 MHz 10 MHz

wlan1

seriell

RMNC: DB0AAT 0-9

eth1

eth2

eth3

DB0INN Mikrotik

eth1:
44.130.216.33/29 (NET)
192.168.178.44/24 (LAN)
Defaultroute via 192.168.178.1
wlan1: *44.143.47.1/29 (BB)*
wlan2: *44.130.229.253/28 (BB)*
Firewall:
Maskiere Source 192.168.178.0/24
auf dem ausgehenden Interface wlan1&2

PC
Optional:
Route: 44.0.0.0/8 via 192.168.178.44
oder
44.130.216.34/29 (NET)
Route: 44.0.0.0/8 via 44.130.216.33

wlan

ether

wlan2

wlan 5675 MHz 10 MHz

DSL-Router
192.168.178.1/24 (LAN)
Route: 44.0.0.0/8 via 192.168.178.44

NAT-Ports eingehend:
TCP 8291 -> *192.168.178.44*

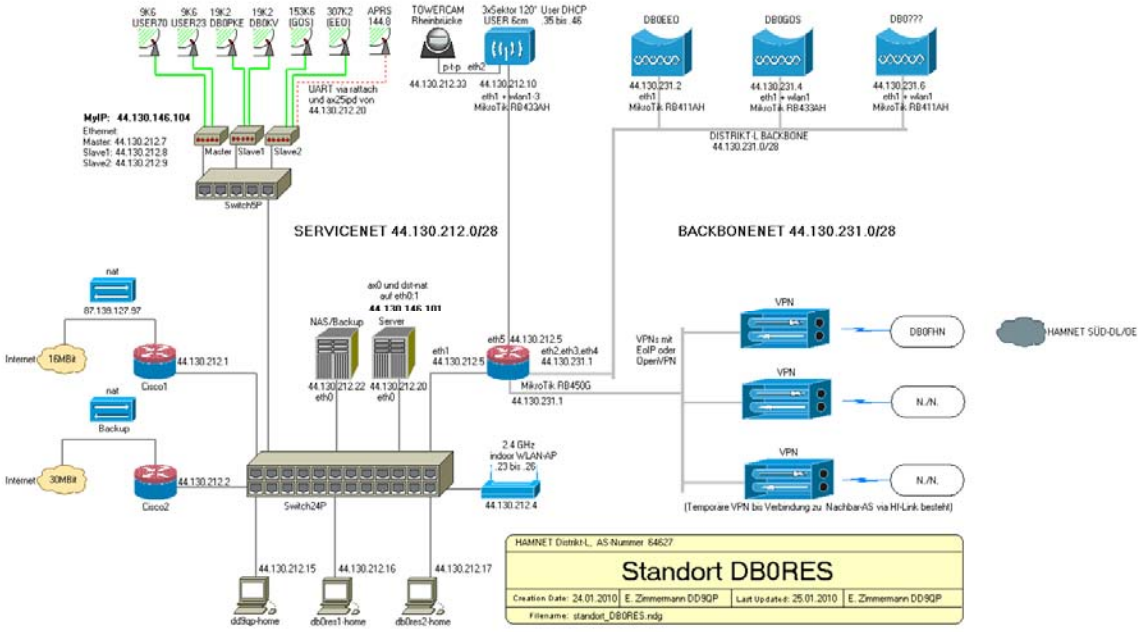
OE2XZR
44.143.47.6/29 (BB)

Der Netzplan ist ähnlich dem Netzplan vom AS64631. Ein paar Besonderheiten sind dennoch herauszustellen: Seit einigen Softwareversionen von RouterOS können die Ethernetports 2 und 3 zusammengeschaltet werden. D.h. direkter Datenverkehr zwischen beiden Ports muss nicht mehr durch die CPU geleitet werden. Der 2-Port-Switch wird bei der Konfiguration dann unter eth2 angesprochen.

Zwischen dem geplanten HAMNET-Link DB0HOB <-> Neumarkt (St. Veit) liegt die Clubstation Rosenheim. Sie soll innerhalb des User-/Service-Netzes von DB0HOB betrieben werden. Dazu ist es nötig, ein neues statisches WDS-Interface für den Backbonelink zu definieren. Dieses Interface wird fest an die Bridge des Backbonenetzwerks gebunden. Der WDS-Modus wird dennoch auf „dynamisch“ eingestellt und neue Interfaces automatisch an die Bridges des User-/Servicenetzwerks gebunden.

Sollen an der Clubstation auch Besucher mit ihren Notebooks als voll adressierbare Teilnehmer des HAMNET über ein LAN-Kabel „onair“ gehen können, so darf das Mikrotikboard an der Clubstation nicht mit Masquerading konfiguriert werden, sondern muss als transparente Bridge laufen. Auf dem Mikrotikboard an DB0HOB muss dann ein DHCP-Server freie IP-Adressen aus dem User-/Servicenetz und die eigene IP-Adresse als Standardgateway an DHCP-Clients vergeben. Es empfiehlt sich, genug Reserven für das User-/Servicenetz einzuplanen oder Platz zwischen den verschiedenen User-/Servicenetzen innerhalb eines AS zu lassen, um z.B. die Netzmaske von /29 auf /28 vergrößern zu können.

Netzpläne zur Übersicht lassen sich sehr schön mit dem freien Tool „Network Notepad“ erstellen (http://www.networknotepad.com).



Netzwerkplan DB0RES

Except where otherwise noted, this work is licensed under
http://creativecommons.org/licenses/by-nc-sa/3.0/