

# HAMServerPi Handbuch

Copyright DL3DCW

<http://forum.db0tv.ampr.org/viewforum.php?f=86>

bearbeitet von DJ7TH – Stand vom 31.03.2016



Raspberry Pi 2 Model B

# Inhaltsverzeichnis

<u>Titel</u>	<u>Seite</u>
<b>Einleitung</b>	<b>...3</b>
<b>Betriebssystem vorbereiten</b>	<b>...6</b>
<b>Netzwerkeinstellungen</b>	<b>...11</b>
<b>Webserver einrichten</b>	<b>...14</b>
<b>FTP-Server einrichten</b>	<b>...20</b>
<b>Mumble-Audio-Server einrichten</b>	<b>...22</b>
<b>Icecast-Video-Server einrichten</b>	<b>...25</b>
<b>TeamTalk-Server einrichten</b>	<b>...27</b>
<b>Mail-Server einrichten</b>	<b>...29</b>
<b>Jabber-Server einrichten</b>	<b>...32</b>
<b>APRS-Gateway einrichten</b>	<b>...34</b>
<b>APRS-Server einrichten</b>	<b>...37</b>
<b>SvxLink einrichten</b>	<b>...39</b>
<b>SvxServer einrichten</b>	<b>...43</b>
<b>VPN-Client einrichten</b>	<b>...45</b>
<b>PPTP VPN-Server einrichten</b>	<b>...47</b>

# Einleitung

Liebe HAMNET-Freunde,

erfreulicherweise schreitet der Ausbau des HAMNET in vielen Regionen Deutschlands mit der Einrichtung weiterer Linkstrecken und dem Aufbau von HF-Benutzerzugängen sehr schnell voran. Die Bedingungen sind also ideal, um über die Vernetzung von Relaisstandorten hinaus auch für den Nutzer attraktive Dienste zu schaffen und im HAMNET anzubieten.

Mit dem HAMServerPi gibt es nun ein Linux-Softwarepaket für Sysops, welche schnell und einfach grundlegende Dienste an ihrem Standort zur Verfügung stellen möchten, ohne sich zunächst tief in die einzelnen Themenbereiche einarbeiten zu müssen. Durch die Verwendung eines Raspberry Pi (Modell B, B+ oder aktuell 2B) sind Anschaffungs- und Betriebskosten absolut gering. Damit sollte eigentlich an fast jedem Standort ein solcher Server möglich sein.



*HAMServerPi: Raspberry Pi im Gehäuse mit DVB-T-Stick für APRS-Empfang*

Der HAMServerPi wurde von Amateuren für Amateure entwickelt. Dabei haben wir vor allem sehr großen Wert auf eine möglichst einfache Konfiguration und Bedienung gelegt. Bestimmt können einige Dinge anders gelöst oder auch besser gemacht werden. Es ist daher absolut erwünscht, die vorhandenen Vorlagen und Komponenten an die eigenen Anforderungen anzupassen, zu verbessern und vielleicht auch weiter auszubauen.

Der HAMServerPi umfasst derzeit die folgenden Linux-Programme:

- Betriebssystem für den Raspberry Pi (Raspbian)
- Webserver für HAMNET-Seiten (Nginx, PHP)
- CMS-System zur Webseitengestaltung (GetSimple)
- Besucherstatistik für den Webserver (HitCount)
- Widget zur Suchmaschinen-Anbindung (YaCy)
- FTP-Server für die Dateiübertragung (ProFTPD)
- APRS-RX-iGate mit DVB-T-Stick (PyMultimonAPRS)
- VOIP-Server für Audiokonferenzen (Mumble)
- Video-Server für HAMNET-ATV (Icecast)
- TeamTalk für Audio, Video, Chat (TeamTalk)
- Jabber-Server für Instant-Messaging (Prosody)
- E-Mail-Server mit Webmail-Client (Citadel)
- Telefonanlage für HAMNET-Telefonie (Asterisk)
- APRS-Server als Gateway zum APRS-IS (aprsd)
- Relaissteuerung/EchoLink-Gateway (SvxLink)
- Relaisvernetzung via TCP/IP (SvxServer)
- VPN-Client zur HAMNET-Anbindung (PPTP)
- HAMNET-Gateway (Forwarding/Masquerade)
- EchoLink Proxyserver (EchoLinkProxy)

Wie aus der vorstehenden Auflistung ersichtlich ist, handelt es sich beim HAMServerPi nicht um eine eigenständige Software, sondern um eine Zusammenstellung verschiedener, frei erhältlicher Linux-Programme, welche zur Benutzung auf einer Micro-SD-Speicherkarte fertig installiert werden können und unter dem Linux-Betriebssystem Raspbian bzw. Debian laufen. Die einzelnen Konfigurationsdateien wurden von uns für HAMNET-Zwecke angepasst und teilweise um zusätzliche Scripte ergänzt.

Die aktuellen Software-Versionen, sowie viele Beiträge mit Tipps & Tricks etc. findet man hier im HAMNET-Forum: <http://forum.db0tv.ampr.org/viewforum.php?f=86>

Weitere Infos und Technical Reference zum Raspberry Pi 2 Model B findet man hier: <http://de.rs-online.com/web/p/entwicklungskits-prozessor-mikrocontroller/8326274/>

und hier:

<http://docs-europe.electrocomponents.com/webdocs/144c/0900766b8144c4bc.pdf>

DBOEND ENNEPETA

HOME APPS FUNKZUF AUDIO VIDEO INFO WIKI:ENNA

AGDC SERVER FRIE - VOXU SERVER FRIE - ZUSCHAUER 1

## Willkommen

auf der HAMNET-Webseite der Reasfunkstelle DBOEND in Ennepetal (J031FH).

Dieser Webserver sowie fast alle hier beschriebenen Dienste laufen auf einem RaspberryPi und wurden mit dem Softwarepaket HAMServerPi realisiert. Weitere Informationen dazu in der Menüleiste oben unter (ZB).



Die Antennen bei DBOEND in Ennepetal auf dem Wasserschloßbehälter am Söding

### Aktuelle Meldungen

- Das FM-Relais ist nach Umbau wieder auf 439.275 MHz QRV
- Die Pichel-Radio-Hardware wurde abgebaut und die Frequenzen zurückgegeben
- Der APRS-Duplexer ist nach Umbau wieder auf 144.800 MHz QRV
- Der Aufbau des Funkruf-Senders erfolgte am 25.10.2013

### STANDORT

- Ennepetal, J031FH
- Breitengrad: 51°18'07"N
- Längengrad: 7°18'00"E
- Höhe: 520m über NN
- Qruaf: DQDDQD

### FREQUENZEN

- APRS: 144.800 MHz
- FM-Relais: 439.275 MHz
- Funkruf: 439.8075 MHz
- HAMNET: 5000.000 MHz

### UNSERE NACHBARN

- DQDDQD
- DQDDQD
- DQDDQD
- DQDDQD
- DQDDQD
- DQDDQD
- DQDDQD

### INTERESSANTE LINKS

- ZTU-Netzwerk
- Webfunktaste
- HAMNET-Forum
- Suchmaschinen

### WEITRE INFO

- Antennen-Baublog
- Antennen-Forum
- Hamradio-Store
- Qruaf

*Mit dem HAMServerPi lassen sich ganz einfach Webseiten erstellen*

Das Programmpaket darf für Amateurfunk-Zwecke (HAMNET) benutzt und auch verändert werden. Die Copyright-Hinweise (z.B. im Webseiten-Template) sowie mindestens ein Link zum HAMServerPi-Projekt unter <http://db0tv.ampr.org/hamsrvpi> müssen jedoch bestehen bleiben. Für alle sonstigen Programme gelten die jeweiligen Lizenzbestimmungen.

Bei der Weitergabe des HAMServerPi-Images sollte man nur das „rohe“ Softwarepaket und nicht eine Kopie der installierten Speicherkarte verwenden, da sonst auch die eigenen Einstellungen und Kennwörter weiterverteilt werden. Der Betrieb des HAMServerPi erfolgt auf eigene Verantwortung; jegliche Garantie, Gewährleistung und Haftung ist natürlich ausgeschlossen.

Bei jedem neu installierten HAMServerPi würden wir uns über eine kurze Info mit Angabe der URL entweder per eMail an [hamsrvpi@ruhrlink.org](mailto:hamsrvpi@ruhrlink.org) oder besser noch in der dafür vorgesehenen Rubrik hier im Forum unter [viewforum.php?f=88](http://viewforum.php?f=88) sehr freuen.

Und nun viel Spaß damit!

Frank, DL3DCW

# Betriebssystem vorbereiten

**Hinweis:** Der HAMServerPi wurde speziell für den Einsatz im HAMNET entwickelt. Eine Verwendung als Server im Internet ist nicht vorgesehen und auch nicht sinnvoll. Aus Sicherheitsgründen raten wir ausdrücklich davon ab, den HAMServerPi ohne eine sorgfältige Anpassung aller Kennwörter, aller Konfigurationsdateien und ohne Verwendung einer geeigneten Firewall als Server im Internet zu betreiben.

Das aktuelle Betriebssystem des HAMServerPi incl. aller Programme kann als Speicherkarten-Image im Internet über den nachstehenden Link auf den PC heruntergeladen werden: <http://www.hamserverpi.de/index.php?id=files>

Da die Datei sehr groß ist, sollte man für den Download über eine schnelle Internetverbindung verfügen. Es wird eine Micro-SD-Karte mit mindestens 4GB benötigt. Zudem ist für das schnelle Lesen und Beschreiben der SD-Karte eine hohe Geschwindigkeitsklasse (z.B. Class 10) von Vorteil. 32GB-SD-Karten gibt es aktuell bereits unter € 10,--

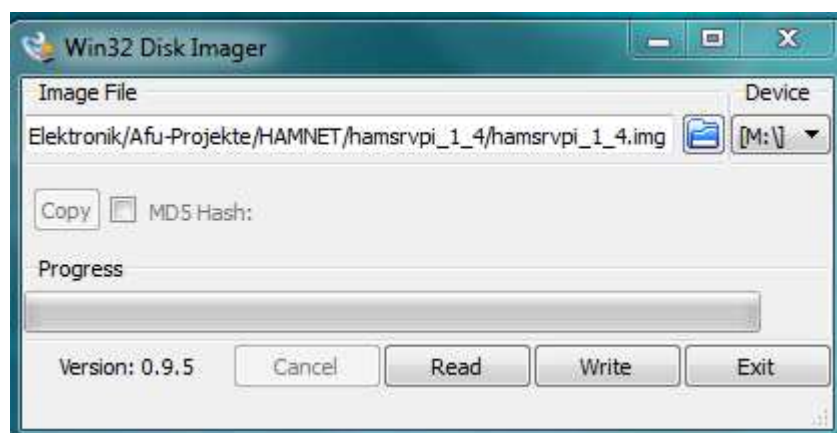
## 1. Speicherkarte beschreiben

Nach dem Herunterladen kann die Image Datei (aktuell hamsrvpi\_1\_4.img) entpackt und anschließend mit dem Programm Win32DiskImager:

<http://www.ruhrlink.org/downloads/Win32DiskImager-0.9.5-install.exe>

mit „Write“ auf die Speicherkarte geschrieben werden.

Achtung: Dabei werden alle auf der Karte vorhandenen Daten gelöscht!



**Tipp:** Mit dem Win32DiskImager können mit „Read“ auch Backups von der Speicherkarte erstellt werden. Dies empfiehlt sich vor allem dann, wenn man später größere Änderungen

am System vorgenommen hat. Für ein einfaches Wiederaufspielen sollte möglichst eine identische Karte (gleicher Typ und gleicher Hersteller) verwendet werden. Das Backup sollte anschließend mit einer "frischen" Speicherkarte auf einwandfreie Funktion geprüft werden.

## 2. Konfiguration vorbereiten

Anschließend braucht die Speicherkarte nur noch in den Kartenslot des Rasperrys eingesteckt und dieser durch Einspeisen der Betriebsspannung (5V) gestartet werden. Für die Konfiguration sollten entweder Monitor und Tastatur oder ein Netzwerkkabel zwecks Konfiguration mittels PC-Programm PuTTY (s. unten) angeschlossen sein.

**Hinweis:** Standardmäßig sind auf einem frisch installierten HAMServerPi bis zur manuellen Änderung die folgenden Zugangsdaten **für sämtliche Funktionen** gültig:

**Benutzername:** **sysop**

**Kennwort:** **hamsrvpi**

## 3. Konfiguration über das Netzwerk per PC + PuTTY

Alternativ kann der HAMServerPi auch per SSH (Port 22), z.B. mit dem Programm **PuTTY** über das Netzwerk konfiguriert werden. Dafür muss sich der LAN-Anschluss des PC im gleichen Netzwerksegment 192.168.1.xxx befinden oder um dieses erweitert werden. Das gilt auch für den DSL-Router (z.B. FritzBox als Gateway). Standardmäßig sind auf einem frisch installierten HAMServerPi die folgenden Netzwerkeinstellungen aktiv:

IP-Adresse: 192.168.1.200  
Subnetzmaske: 255.255.255.0  
Gateway: 192.168.1.1  
DNS-Server: 192.168.1.1



**Tipp:** in PuTTY sollte man unter „Window – Translation – Remote Character Set“ den Wert zwecks besserer Lesbarkeit von Umlauten etc. auf „UTF-8“ setzen und nach Eingabe aller Parameter mit „Save“ die Einstellungen von PuTTY als „Default Settings“ abspeichern, sodass sie nach erneutem Aufruf von PuTTY sofort wieder aktiv sind.

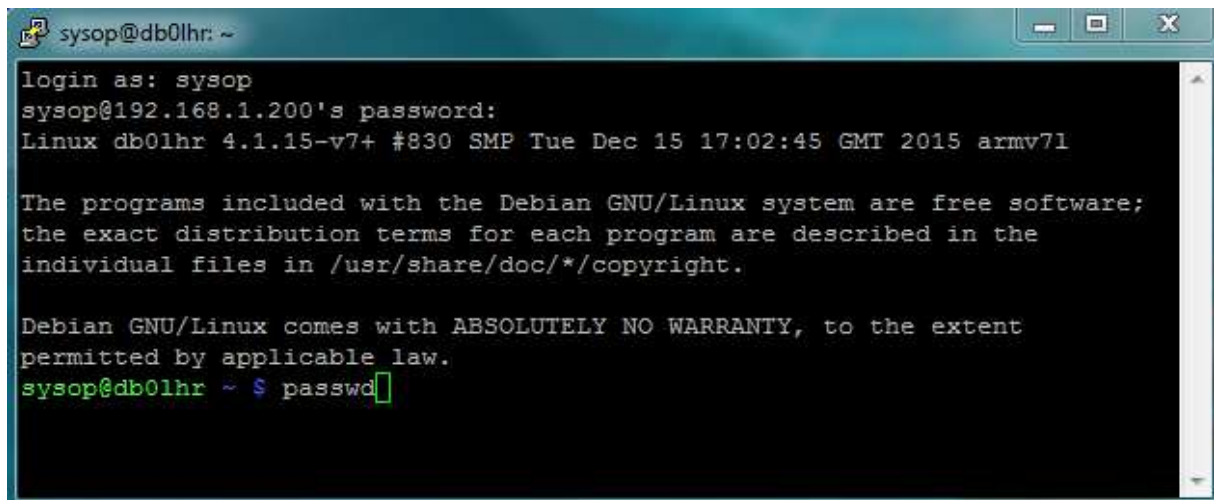
#### 4. Password ändern

**Hinweis:** Bevor man den HAMServerPi zum ersten Mal mit dem HAMNET verbindet, müssen auf jeden Fall in den einzelnen Funktionen alle Kennwörter individuell abgeändert werden, um das System vor unberechtigtem Zugriff zu schützen!

Nach dem Einloggen mit den obenstehenden Zugangsdaten kann das Password des Raspberrys mit dem folgenden Befehl geändert werden:

`passwd`

Anschließend wird das aktuelle sowie das neue Kennwort abgefragt. Das neue Kennwort muss danach noch einmal wiederholt werden. Hier ein Beispiel mit PuTTY:



```
sysop@db0lhr: ~  
login as: sysop  
sysop@192.168.1.200's password:  
Linux db0lhr 4.1.15-v7+ #830 SMP Tue Dec 15 17:02:45 GMT 2015 armv7l  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
sysop@db0lhr ~ $ passwd
```

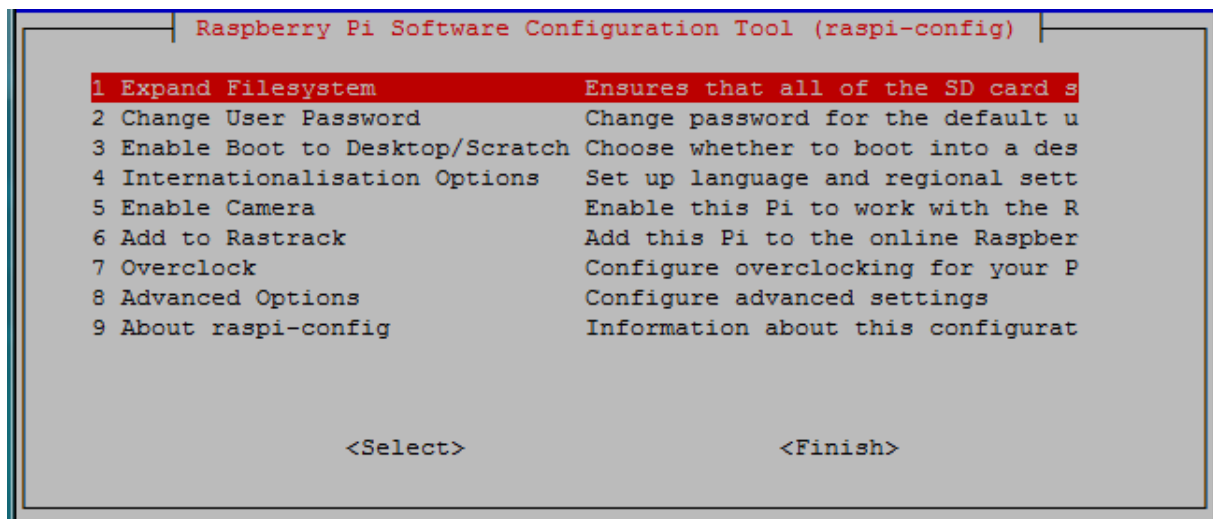
#### 5. Dateisystem anpassen

Die Konfigurationsoberfläche des Raspberrys über den Befehl

`sudo raspi-config`

aufrufen (kann man gegebenenfalls mit ESC wieder verlassen).





Den Punkt "Expand Filesystem" und danach "OK" auswählen. Nach einem Neustart wird das Dateisystem an die aktuelle Größe der eingelegten Speicherkarte angepasst.

Mit dem Kommando

```
df -h
```

kann anschließend überprüft werden, ob das Dateisystem erfolgreich vergrößert wurde.

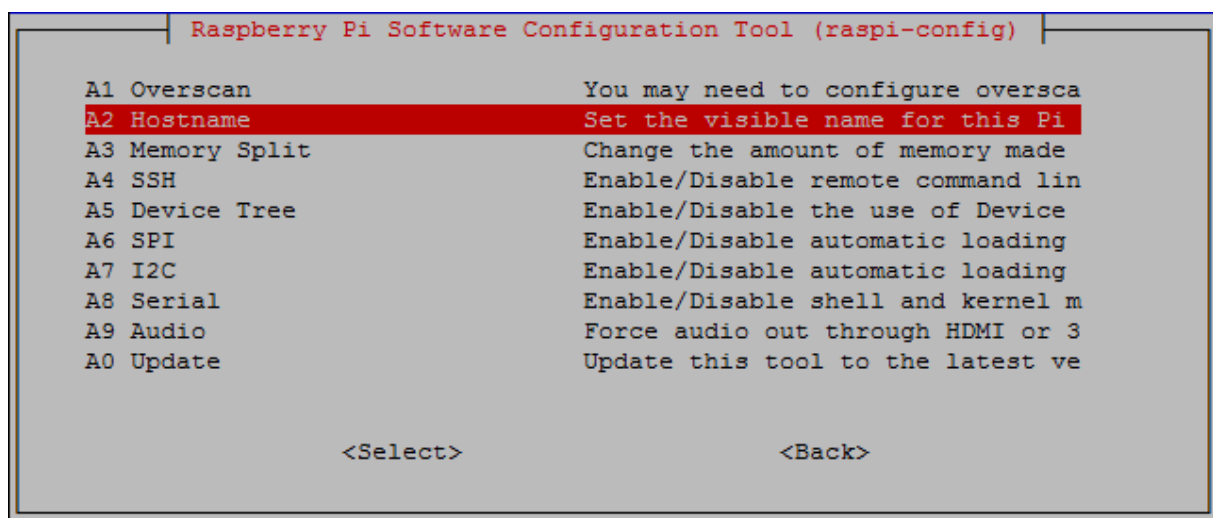
## 6. Hostnamen anpassen

Die Konfigurationsoberfläche des Raspberrys über den Befehl

```
sudo raspi-config
```

aufrufen.

Anschließend den Punkt "Advanced Options" und danach "Hostname" auswählen.



Als Hostnamen sollte man das Rufzeichen des Standorts in Kleinbuchstaben, also z.B. "db0end" eintragen. Anschließend den Raspberry neu starten.

## **7. System neu starten**

Ein Neustart des HAMServerPi, z.B. nach Konfigurationsänderungen, kann mit dem Befehl

```
sudo reboot
```

erfolgen.

## **8. System herunterfahren**

Zum geordneten Herunterfahren des HAMServerPi sollte immer den Befehl

```
sudo halt
```

verwendet werden. In sehr ungünstigen Fällen wird sonst die Speicherkarte zerstört. Erst wenn nur noch die rote LED leuchtet, darf die Stromversorgung getrennt werden.

## **9. Anwendungen einrichten**

Alle Anwendungen des HAMServerPi können einzeln und unabhängig voneinander eingerichtet werden. Es sollten jedoch nur die Funktionen aktiviert werden, welche auch wirklich benötigt werden. Zudem müssen vorher auf jeden Fall die Kennwörter der einzelnen Dienste abgeändert werden.

Die meisten Anwendungen laufen problemlos parallel, da sie nur relativ wenig Rechenleistung benötigen. Anwendungen wie PyMultimonAPRS, TeamTalk oder SvxLink erzeugen deutlich mehr CPU-Last. Daher kann es von Vorteil sein, nicht alle diese Dienste gleichzeitig zu aktivieren.

Mit dem Befehl

```
top
```

erhält man eine Übersicht über die aktuelle Systemauslastung.

Zurück zur Kommandozeile geht es mit "STRG-C".

# Netzwerkeinstellungen

Standardmäßig sind auf einem frisch installierten HAMServerPi die folgenden Netzwerk-Einstellungen aktiv:

IP-Adresse: 192.168.1.200

Subnetzmaske: 255.255.255.0

Gateway: 192.168.1.1

DNS-Server: 192.168.1.1

Damit der HAMServerPi im HAMNET erreichbar wird, müssen diese Einstellungen nun auf die am Standort gültigen Parameter abgeändert werden. Falls die Konfiguration bisher per SSH (z.B. via PuTTY) über das Netzwerk erfolgte, sollte man beachten, dass nach der Änderung der Server auch nur noch unter den neuen Einstellungen erreichbar ist.

**Hinweis:** Bevor man den HAMServerPi zum ersten Mal mit dem HAMNET verbindet, müssen auf jeden Fall die Kennwörter aller aktivierten Dienste individuell abgeändert werden. Dies sollte spätestens jetzt noch einmal genau überprüft werden. Eine Änderung der Standard-IP-Adresse erfordert natürlich auch in den nachfolgenden Anleitungen (z.B. Webserver einrichten) eine entsprechend angepasste Eingabe.

## 1. Änderung der LAN-Port IP-Adresse

Die Interface-Konfigurationsdatei in den Texteditor laden mit

```
sudo nano /etc/network/interfaces
```

und die IP-Adressen vom LAN-Port entsprechend den eigenen Vorgaben anpassen, z.B.:

```
# LAN
auto eth0
allow-hotplug eth0
iface eth0 inet static
address 192.168.0.154
netmask 255.255.255.0
gateway 192.168.0.1
```

Mit "Strg-X", anschließendem "J" und der Eingabetaste die Datei abspeichern. Mit

```
sudo /etc/init.d/networking reload
```

die neuen Einstellungen aktivieren.

## **2. Änderung der DNS-Server**

Die DNS-Konfigurationsdatei in den Texteditor laden mit

```
sudo nano /etc/resolv.conf
```

und die DNS-Server entsprechend anpassen. Wichtig: Es müssen immer die DNS-Server des eigenen AS bzw. des eigenen Distriktes verwendet werden. Für den Distrikt Westfalen-Süd sind das z.B. 44.225.52.20 und 44.225.28.20. Zusätzliche DNS-Server können in einer weiteren Zeile eingetragen werden.

```
nameserver 44.x.x.x
```

Danach mit "Strg-X", anschließendem "J" und der Eingabetaste die Datei abspeichern. Mit

```
sudo /etc/init.d/networking reload
```

die neuen Einstellungen aktivieren.

## **3. Änderung der NTP-Server (Zeitgeber)**

Die NTP-Konfigurationsdatei mit

```
sudo nano /etc/ntp.conf
```

in den Texteditor laden und die NTP-Server entsprechend anpassen. Wichtig: Es müssen immer die NTP-Server des eigenen AS bzw. des eigenen Distriktes verwendet werden. Für den Distrikt Westfalen-Süd sind das z.B. 44.225.52.20 und 44.225.28.20.

Zusätzliche NTP-Server können in einer weiteren Zeile eingetragen werden:

```
server 44.x.x.x iburst
```

Danach mit "Strg-X", anschließendem "J" und der Eingabetaste die Datei abspeichern.

DHCP für die NTP-Server deaktivieren mit

```
sudo mv /var/lib/ntp/ntp.conf.dhcp /var/lib/ntp/ntp.conf.dhcp.org
```

und anschließend die neuen Einstellungen aktivieren mit

```
sudo /etc/init.d/ntp restart
```

Ist der HAMServerPi mit dem HAMNET verbunden, können mit dem Befehl

```
ntpq -p
```

die NTP-Server getestet werden.

Nach Eingabe des Kommandos

```
date
```

sollte dann die aktuelle Uhrzeit und das Datum angezeigt werden.

Tipp:

Im Netzwerk-Router vom HAMNET sollten entsprechende Portfreigaben erfolgt sein.

**FRITZ!Box 7390** RL-Box

Angemeldet | [FRITZ!Box](#) | [FRITZ!NAS](#) | [MyFRITZ!](#) | ?

### Freigaben

Portfreigaben | Speicher | FRITZ!Box-Dienste | Dynamic DNS | VPN | IPv6

An FRITZ!Box angeschlossene Computer sind sicher vor unerwünschten Zugriffen aus dem Internet. Für einige Anwendungen wie z.B. Online-Spiele oder das Filesharing-Programm eMule muss Ihr Computer jedoch für andere Teilnehmer des Internets erreichbar sein. Durch Portfreigaben erlauben Sie solche Verbindungen.

#### Liste der Portfreigaben

Aktiv	Bezeichnung	Protokoll	Port	an Computer	an Port		
<input checked="" type="checkbox"/>	VPN-Server	TCP	1723	db0lhr	1723		
<input checked="" type="checkbox"/>	Audio-Server	TCP	64738	db0lhr	64738		
<input checked="" type="checkbox"/>	TT-Server	TCP	10333	db0lhr	10333		
<input checked="" type="checkbox"/>	VoIP-Server	TCP	5090	db0lhr	5060		
<input checked="" type="checkbox"/>	Web-Server	TCP	80	db0lhr	80		
<input checked="" type="checkbox"/>	RPI-Monitor	TCP	8888	db0lhr	8888		
<input checked="" type="checkbox"/>	Video-Server	TCP	9000-9001	db0lhr	9000-9001		
<input checked="" type="checkbox"/>	TT-Server	UDP	10333	db0lhr	10333		

Änderungen der Sicherheitseinstellungen über UPnP gestatten  
Geräte wie Smart-TV oder Smartphone bzw. Anwendungen mit UPnP-Unterstützung können im Heimnetz Sicherheitseinstellungen wie die Portfreigaberegeln der FRITZ!Box automatisch verändern. Aktivieren Sie diese Option aus Sicherheitsgründen nur, wenn Sie tatsächlich eingehende Verbindungen aus dem Internet gestatten möchten.

Hier ein Beispiel mit der FritzBox, testweise als HAMNET-Router verwendet.

# Webserver einrichten

Der Webserver ist eine zentrale Komponente des HAMServerPi. Zusammen mit dem Content-Management-System "GetSimple" können sehr einfach Webseiten mit weiterführenden Informationen zum Standort und den aktivierten Diensten erstellt werden. Für viele Funktionen des HAMServerPi gibt es bereits vorgefertigte Seiten sowie teilweise auch entsprechende Anleitungen. Eventuell erforderliche Zusatzprogramme können direkt von der Webseite des HAMServerPi heruntergeladen werden.

The screenshot shows the website for station DBOEND ENNEPETAL. The main content area includes a 'Willkommen' section with a photo of the antenna tower and a list of 'Aktuelle Meldungen'. The right sidebar contains several sections: 'STANDORT' with location details, 'FREQUENZEN' with frequency information, 'UNSERE NACHBARN' with a list of nearby stations, 'INTERESSANTE LINKS' with external links, and 'WEITRE INFO' with additional resources.

## 1. Konfiguration anpassen

Die Konfigurationsdatei des Webserver mit

```
sudo nano /etc/nginx/sites-enabled/default
```

in den Texteditor laden

und den Server-Namen `nocall...` entsprechend in den eigenen z.B. `db0end...` umbenennen:

```
server_name nocall.ampr.org
```

Danach mit "Strg-X", anschließendem "J" und der Eingabetaste die Datei abspeichern.

## 2. Server aktivieren

Der Webserver wird mit den Befehlen

```
sudo update-rc.d nginx defaults
sudo update-rc.d php5-fpm defaults
```

aktiviert und beim nächsten Neustart des Systems automatisch gestartet.

Mit den Befehlen

```
sudo update-rc.d nginx remove
sudo update-rc.d php5-fpm remove
```

kann der Webserver wieder deaktiviert werden.

**Tipp:** Weiterführende Informationen zu Nginx gibt es im Internet unter <http://www.nginx.org>.

## 3. Kennwort ändern

Über die URL <http://192.168.1.200/admin> gelangt man per Webinterface in den Administrationsbereich von GetSimple (Username: sysop, Passwort: hamsrvpi):



Nach dem Login kann nun unter dem Menüpunkt "Einstellungen" das Kennwort geändert werden.

**Tipp:** Weiterführende Informationen zu GetSimple gibt es im Internet unter

<http://www.get-simple.info>.

#### 4. Suchmaschinen-Feld einrichten

Der HAMServerPi verfügt über die Möglichkeit, ein Suchmaschinen-Eingabefeld auf der Webseite darzustellen. Bei Eingabe eines Suchbegriffs werden die Ergebnisse sofort dargestellt.



Das Suchmaschinen-Feld ist für die Anbindung einer YaCy-Suchmaschine geeignet. Es sollte dabei möglichst immer die Suchmaschine des eigenen Distriktes bzw. AS verwendet werden, um unnötigen Traffic zu vermeiden. Da die einzelnen Suchmaschinen in der Regel miteinander vernetzt sind, werden auch überregionale Suchergebnisse angezeigt. Beispiel für eine YaCy-Suchmaschine im HAMNET: <http://search.db0tv.ampr.org>.

Zum Aktivieren der Funktion die Suchmaschinen-Konfigurationsdatei mit

```
sudo nano /var/www/data/uploads/search/index.html
```

in den Texteditor laden und die nachstehenden Server-Bezeichnungen entsprechend den eigenen Vorgaben anpassen:

```
url   : 'http://search.servercall.ampr.org'  
link  : 'http://search.servercall.ampr.org'  
title : 'Suchergebnisse von SERVERCALL'
```

```
<form id="ysearch" method="get" accept-charset="UTF-8"  
action="http://search.servercall.ampr.org/yacyssearch.html"><p>
```

Danach mit "Strg-X", anschließendem "J" und der Eingabetaste die Datei abspeichern.

Nun im Admin-Bereich von GetSimple unter „Vorlagen/Vorlage bearbeiten“ die Datei „style.css“ aufrufen und unter „SIDEBAR“ den Wert für „margin“ auf 56px ändern:

```
/* SIDEBAR */  
aside {  
  float:right;  
  width:223px;  
  margin:56px 0 0 0;
```



Anschließend noch unter "Vorlagen/Komponenten bearbeiten" am Ende der Komponente „Sidebar“ die nachstehenden Zeilen anhängen bzw. die Kommentarzeichen „<!--“ und „-->“ entfernen:

```
<div style="position:absolute; left:760px; top:18px; ">
<?php include('data/uploads/search/index.html'); ?>
</div>
```

Nun wird das Suchmaschinen-Feld im oberen Bereich der rechten Menüleiste auf der Webseite des HAMServerPi angezeigt.

## 5. Besucherstatistik aktivieren

**Hinweis:** Die derzeit installierte Besucherstatistik "HitCount" versucht zeitweise eine Datei aus dem Internet nachzuladen. Daher kann es bei einer reinen HAMNET-Verbindung teilweise Probleme mit den Plugins geben. Eine Lösung befindet sich in Vorbereitung.

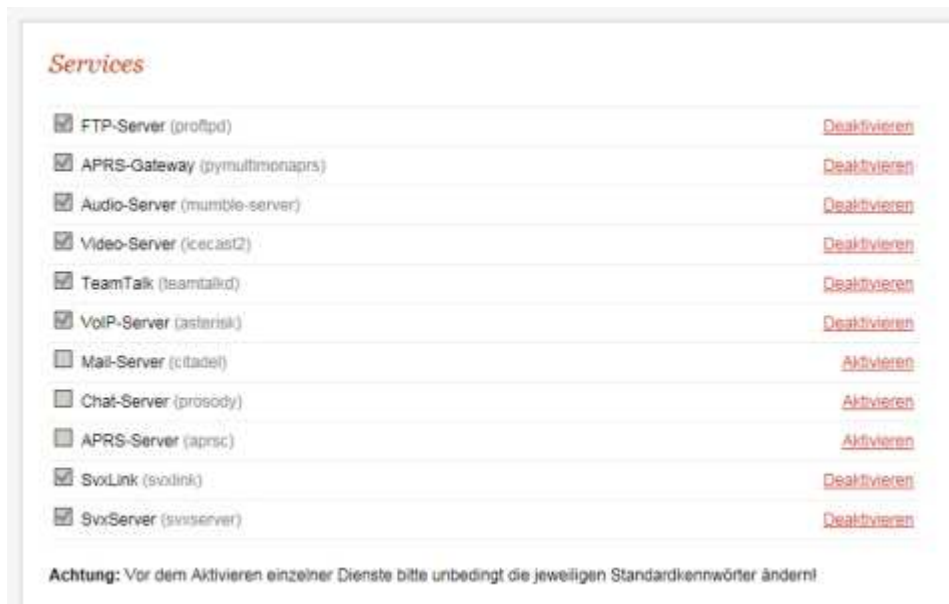
Der HAMServerPi verfügt zudem über eine Besucherstatistik für den Webserver. Diese Funktion kann im Admin-Bereich von GetSimple unter „Plugins/HitCount“ aktiviert werden.



Anschließend sind die Statistiken im Admin-Bereich von GetSimple unter "Support/Zugriffe & Besucher" sichtbar.

## 6. Control Manager aktivieren

Zum einfachen Ein-/Ausschalten einzelner Dienste über das Web-Interface gibt es ab Version 1.2 den "HAMServerPi Control Manager". Diese Funktion kann im Admin-Bereich von GetSimple unter „Plugin-Verwaltung“ aktiviert werden.



Anschließend die Datei "/etc/sudoers" mit

```
sudo nano /etc/sudoers
```

in den Texteditor laden und das Doppelkreuz vor "www-data ALL=(ALL) NOPASSWD: ALL" entfernen. Danach mit "Strg-X", anschließendem "J" und der Eingabetaste die Datei abspeichern.

**Achtung:** Spätestens jetzt sollte unbedingt das Standardkennwort von GetSimple geändert werden. Sollen weitere Dienste aktiviert werden, müssen dort ebenfalls alle zugehörigen Kennwörter angepasst werden. Ansonsten besteht keinerlei Schutz vor unberechtigtem Zugriff!

## 7. Webseite anpassen

Alle Anpassungen werden im Admin-Bereich von GetSimple vorgenommen. Es sollten mindestens folgende Änderungen durchgeführt werden:

Website-Name: **RUFZEICHEN Standort**

Website-Basis-URL: **IP-Adresse oder Domain-Name des Servers**

Danach muß noch die Startseite (Home) sowie das Impressum angepasst werden. Unter "Vorlagen/Komponenten bearbeiten" können zudem die Einträge in der rechten Menüleiste bearbeitet werden.

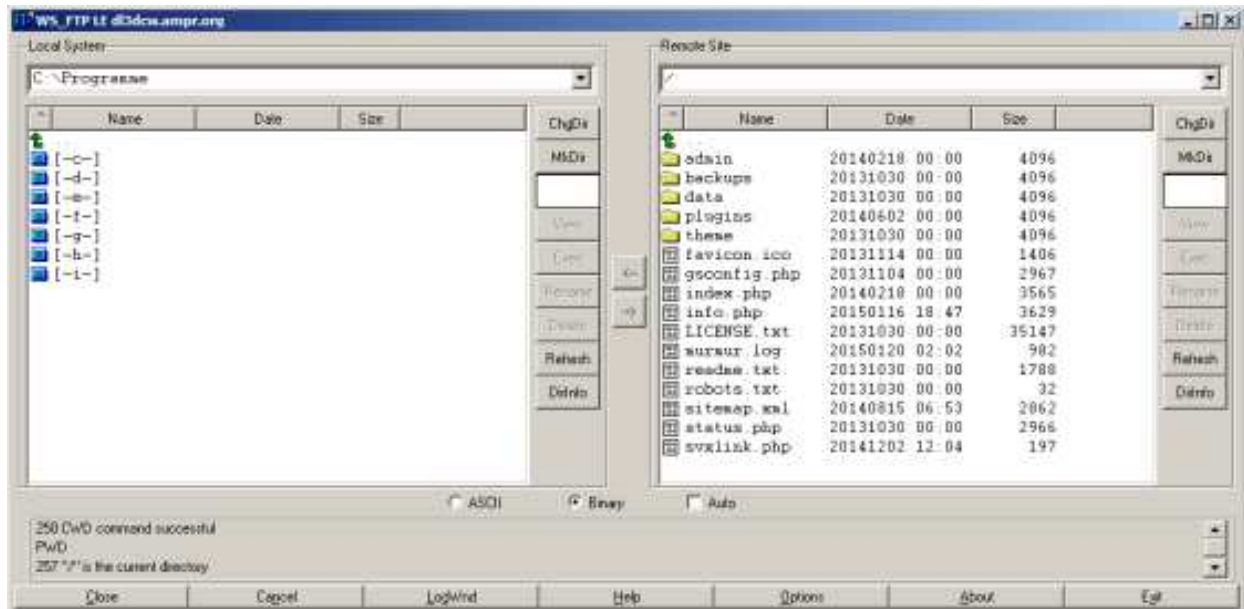
Für die meisten Dienste des HAMServerPi gibt es bereits vorgefertigte Webseiten. Alle Links auf diesen Seiten müssen noch an die eigene URL bzw. IP-Adresse angepasst werden. Sollen bestimmte Dienste nicht angeboten werden, können die zugehörigen Webseiten ausgeblendet werden. Dies erfolgt im Seitenbearbeitungsmodus unter "Optionen" durch Deaktivieren der Funktion "Diese Seite im Menü anzeigen".

**Tipps:** Nach umfassenden Änderungen sollte unter "Backup" eine Komplett-Sicherung der Webseite durchgeführt und anschließend die ZIP-Datei per Mausklick auf einen externen Rechner heruntergeladen werden. Dann kann man ein eventuell defektes System recht schnell wieder herstellen.

Im Netzwerk-Router ist folgender Port freizugeben: 80 (TCP)

# FTP-Server einrichten

Mit dem FTP-Server ist es sehr einfach möglich, beliebige Dateien auf den Webpace des HAMServerPi zu übertragen. Dies ist besonders hilfreich, wenn man oft an der Webseite arbeitet oder z.B. viele Bilder auf der Webseite darstellen möchte. Er ist somit eine sinnvolle und recht nützliche Ergänzung zu GetSimple. Standardmäßig erfolgt die Übertragung der Daten direkt in das Hauptverzeichnis des Webservers unter `"/var/www"`.



*Dateiübertragung zu einem entfernten HAMServerPi mit dem FTP-Programm WS\_FTP*

## 1. Kennwort ändern

Mit dem Befehl

```
id www-data
```

die User- (uid) und Gruppen-ID (gid) ermitteln und anstatt der vorgegebenen Werte (33) im nachstehenden Code ersetzen.

```
cd /etc/proftpd/; sudo ftpasswd --passwd --name sysop --uid 33 --gid 33 --home /var/www/ --shell /bin/false
```

Anschließend wird das neue Kennwort erfragt. Das neue Kennwort muss danach noch einmal wiederholt werden.

## 2. Server aktivieren

Der FTP-Server wird mit dem Befehl

```
sudo update-rc.d proftpd defaults
```

aktiviert und beim nächsten Neustart des Systems automatisch gestartet.

Mit dem Befehl

```
sudo update-rc.d proftpd remove
```

kann der FTP-Server wieder deaktiviert werden.

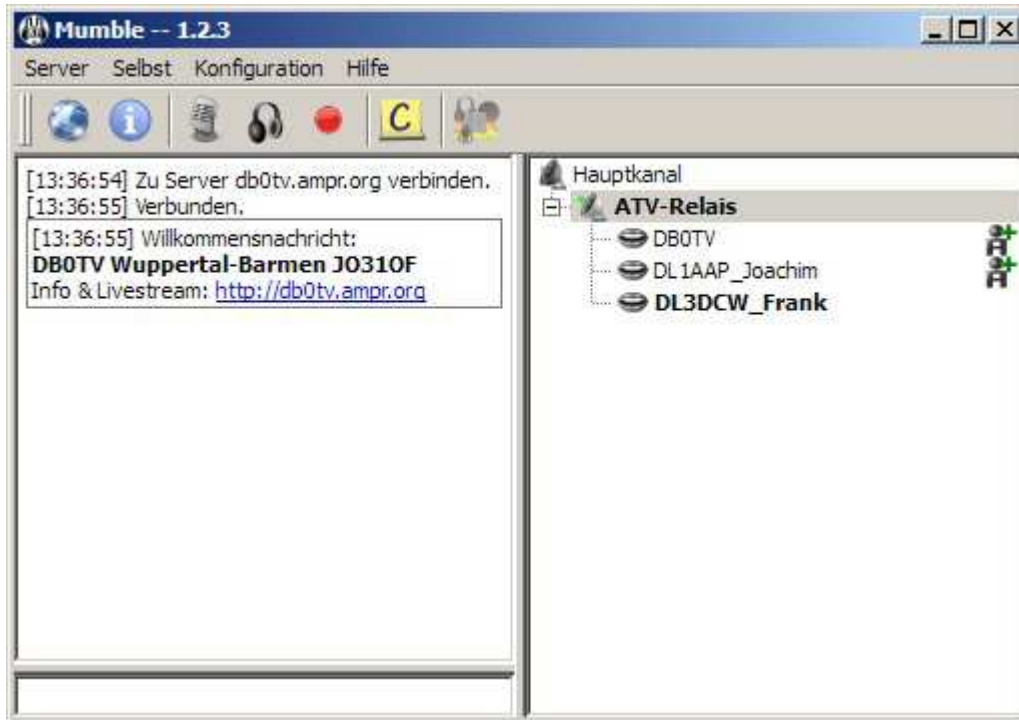
**Tipp:** Weiterführende Informationen zu ProFTPD gibt es im Internet unter:

<http://www.proftpd.org>

Um Daten vom und zum PC zu übertragen, eignet sich prinzipiell jeder FTP-Client wie z.B. das kostenlose Windows-Programm FileZilla.

# Mumble-Audio-Server einrichten

Der Mumble-Server ermöglicht die Übertragung von Sprache und beliebigen Audiosignalen über das HAMNET. Mit dem Programm Mumble sind dabei Vollduplexverbindungen sowie auch Konferenzen mit mehreren Teilnehmern möglich. Mumble hat sich für den Einsatz im HAMNET bestens bewährt; zudem werden damit niedrige Latenzzeiten und eine sehr gute Sprachqualität erreicht.



Übertragung von Sprache und Audiosignalen mit dem Programm Mumble

## 1. Kennwort ändern

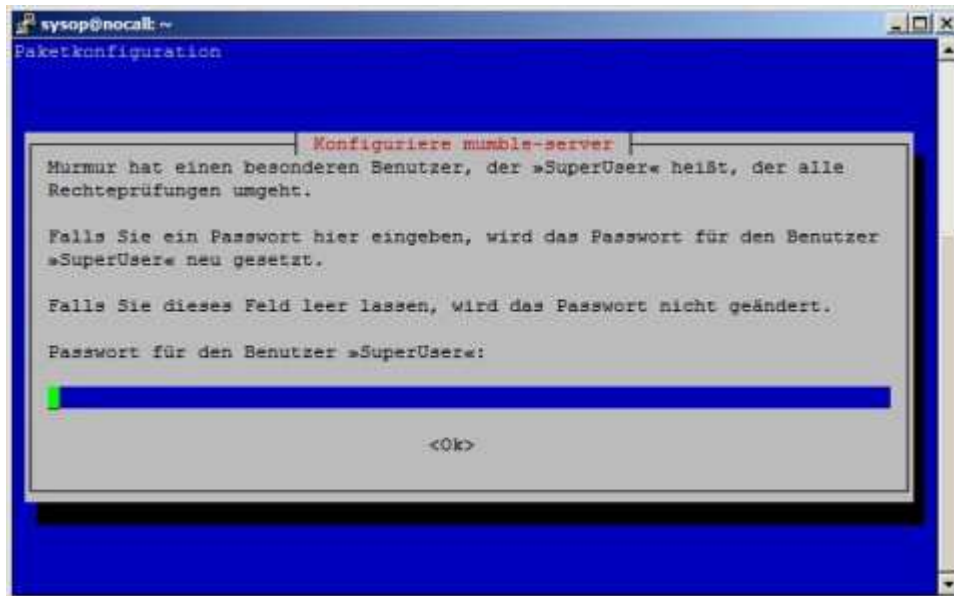
Mit dem Befehl

```
sudo dpkg-reconfigure mumble-server
```

die Konfigurationsoberfläche des Mumble-Servers aufrufen und die Fragen wie folgt beantworten:

Mumble-Server beim Booten automatisch starten? **Ja**

Soll dem Mumble-Server erlaubt werden, eine höhere Priorität zu nutzen? **Nein**



*Konfigurationsoberfläche des Mumble-Servers*

Anschließend kann das gewünschte Kennwort für den "SuperUser" eingegeben werden.

## 2. Konfiguration anpassen

Die Konfigurationsdatei des Mumble-Servers mit

```
sudo nano /etc/mumble-server.ini
```

in den Texteditor laden, den Begrüßungstext suchen und welcometext entsprechend den eigenen Vorgaben anpassen:

```
welcometext="<br><b>NOCALL Nowhere NOLOCATOR</b><br>Weitere Infos: <a href='http://nocall.ampr.org'>http://nocall.ampr.org</a>"
```

Danach in der folgenden Zeile noch das Rufzeichen des Standorts eintragen:

```
registerName=NOCALL
```

Nun mit "Strg-X", anschließendem "J" und der Eingabetaste die Datei abspeichern.

## 3. Server aktivieren

Der Mumble-Server wird mit dem Befehl

```
sudo update-rc.d mumble-server defaults
```

aktiviert und beim nächsten Neustart des Systems automatisch gestartet.

Mit dem Befehl

```
sudo update-rc.d mumble-server remove
```

kann der Mumble-Server wieder deaktiviert werden.

#### **4. Cronjob einrichten**

Damit die Logdatei des Mumble-Servers nicht zu groß wird, sollte sie regelmäßig per Cronjob gelöscht werden. Dazu den Befehl

```
sudo crontab -e
```

ausführen und das Doppelkreuz # vor den unten angegebenen Zeilen entfernen:

```
00 03 * * * /etc/init.d/mumble-server stop
01 03 * * * rm /var/www/murmur.log
02 03 * * * /etc/init.d/mumble-server start
```

Nun mit "Strg-X", anschließend "J" und der Eingabetaste die Datei abspeichern. Wird der Mumble-Server später einmal deaktiviert, dann müssen die Doppelkreuze wieder eingefügt werden. Dann wird der Server nicht ungewollt durch den Cronjob automatisch neu gestartet.

Bei deaktiviertem Mumble-Server sollte die Logdatei mit dem Befehl

```
sudo rm /var/www/murmur.log
```

komplett gelöscht werden, damit dies im Info-Bereich der Webseite entsprechend angezeigt werden kann.

**Tipps:** Weiterführende Informationen zu Mumble gibt es im Internet unter:

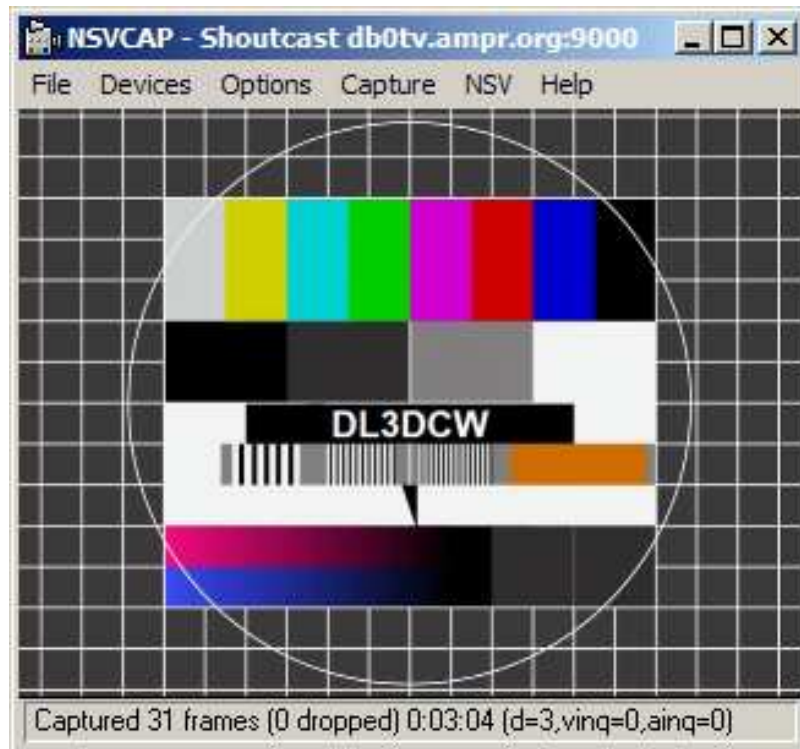
<http://mumble.sourceforge.net>

Im Netzwerk-Router ist folgender Port freizugeben: 64738 (TCP)



# Icecast-Video-Server einrichten

Der Icecast-Server ermöglicht das Senden von Bild und Ton über das HAMNET. Wie bei jeder digitalen Übertragung erfolgt auch diese nicht ganz "live" sondern erfordert ein wenig Zeit. Im Idealfall sind das in etwa zwei Sekunden; bei ungünstigen Voraussetzungen oder schlechten Verbindungen manchmal auch ein wenig mehr. Aus diesem Grund sollte die Audioübertragung möglichst getrennt über den getrennten Mumble-Server erfolgen.



*Videoübertragung via Icecast-Server mit NSVcap*

## 1. Kennwort ändern

Mit dem nachstehenden Befehl wird die Icecast-Konfigurationsdatei in einen Text-Editor geladen:

```
sudo nano /etc/icecast2/icecast.xml
```

Mit dem Cursortasten nun die Stelle

```
<admin-password>hamsrvpi</admin-password>
```

suchen und das Kennwort individuell abändern.

## 2. Konfiguration anpassen

Es sollten nun noch die nachstehenden Einträge individuell abgeändert werden:

```
<admin>mycall@nocall.ampr.org</admin>  
<hostname>nocall.ampr.org</hostname>
```

Danach mit "Strg-X", anschließendem "J" und der Eingabetaste die Datei abspeichern.

## 3. Server aktivieren

Der Icecast-Server wird mit dem Befehl

```
sudo update-rc.d icecast2 defaults
```

aktiviert und beim nächsten Neustart des Systems automatisch gestartet.

Mit dem Befehl

```
sudo update-rc.d icecast2 remove
```

kann der Icecast-Server wieder deaktiviert werden.

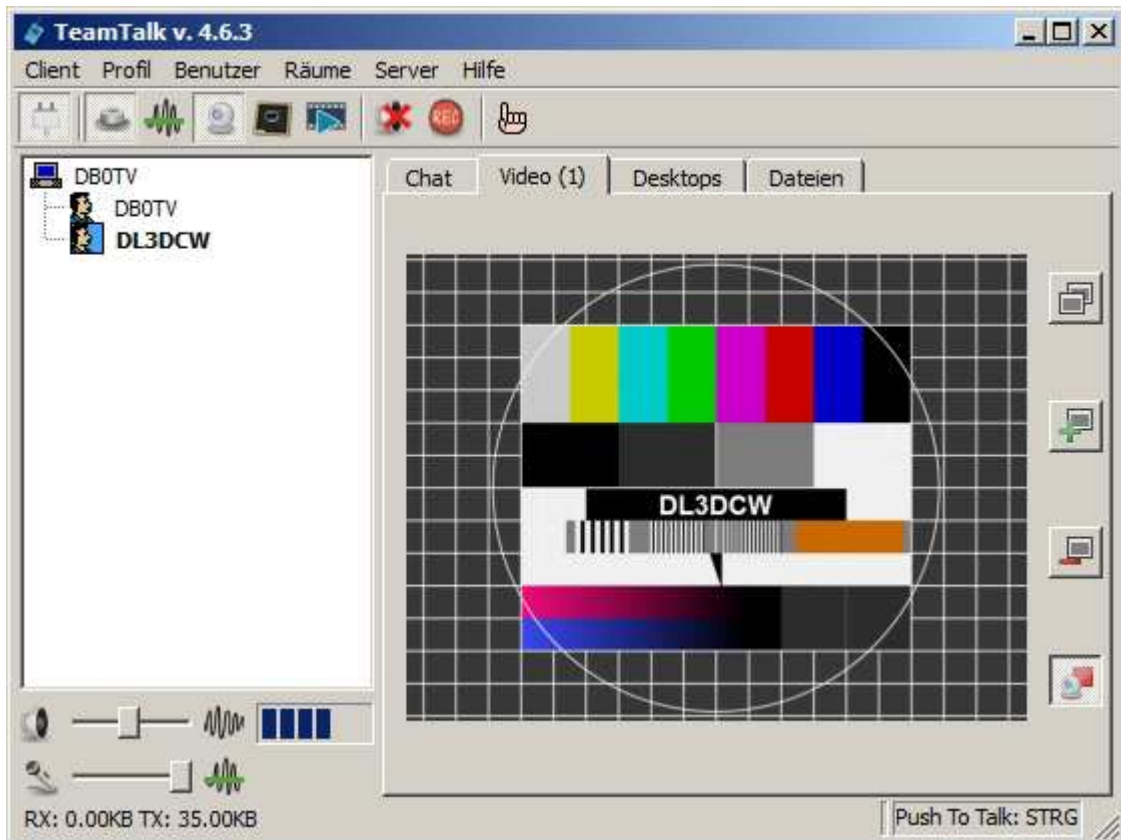
**Tipps:** Weiterführende Informationen zu Icecast gibt es im Internet unter:

<http://www.icecast.org>.

- Im Netzwerk-Router sind folgende Ports freizugeben: 9000 (TCP) + 9001 (TCP)
-

# TeamTalk-Server einrichten

TeamTalk in der erprobten Version 4.6.3 ermöglicht Audio- und Videokonferenzen mit sehr geringen Latenzzeiten über das HAMNET. Der auf Benutzerseite erforderliche Client beinhaltet dabei alle Funktionen in einer einzigen Software. Dadurch wird eine einfache und intuitive Bedienung erreicht. Das kostenlose Programm ist für viele Betriebssysteme wie Windows, Linux, Raspbian, Mac OS X sowie CentOS erhältlich. Eine Version für Smartphones befindet sich in Vorbereitung.



*Audio- und Videokonferenzen bei sehr geringen Latenzzeiten mit TeamTalk*

## 1. Konfiguration anpassen

Die Konfigurationsdatei des TeamTalk-Servers mit

```
sudo nano /opt/teamtalk/server/tt4svc.xml
```

in den Texteditor laden und die unten aufgeführten Zeilen entsprechend den eigenen Vorgaben anpassen:

```
<server-name>NOCALL</server-name>
```

Nun mit "Strg-X", anschließendem "J" und der Eingabetaste die Datei abspeichern.

## **2. Erweiterte Konfiguration**

Bei Bedarf kann mit dem Befehlen

```
cd /opt/teamtalk/server/  
sudo ./teamtalkd -wizard
```

ein Konfigurationsprogramm mit erweiterten Einstellmöglichkeiten aufgerufen werden. Damit ist dann u.a. die Einrichtung eines Benutzerkontos mit Administrator-Rechten möglich. Über dieses Konto kann der Server später auch über den TeamTalk-Client konfiguriert werden.

## **3. Server aktivieren**

Der TeamTalk-Server wird mit dem Befehl

```
sudo update-rc.d teamtalkd defaults
```

aktiviert und beim nächsten Neustart des Systems automatisch gestartet. Mit dem Befehl

```
sudo update-rc.d teamtalkd remove
```

kann der TeamTalk-Server wieder deaktiviert werden.

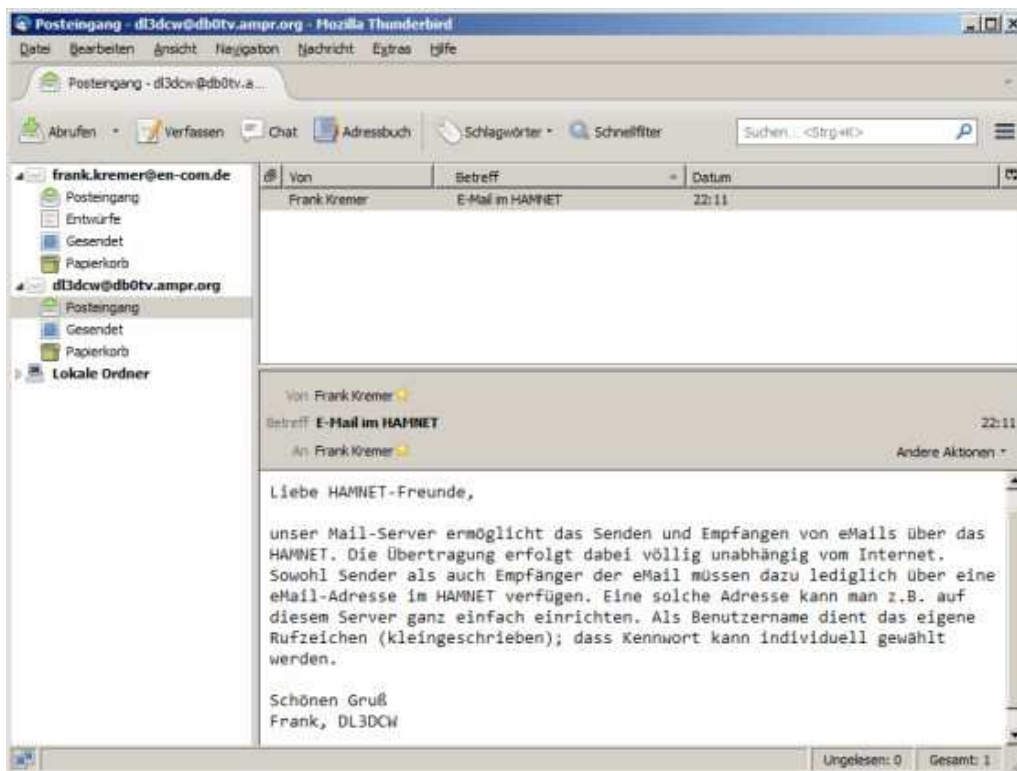
**Tipps:** Weiterführende Informationen zu TeamTalk gibt es im Internet unter

<http://www.bearware.dk>

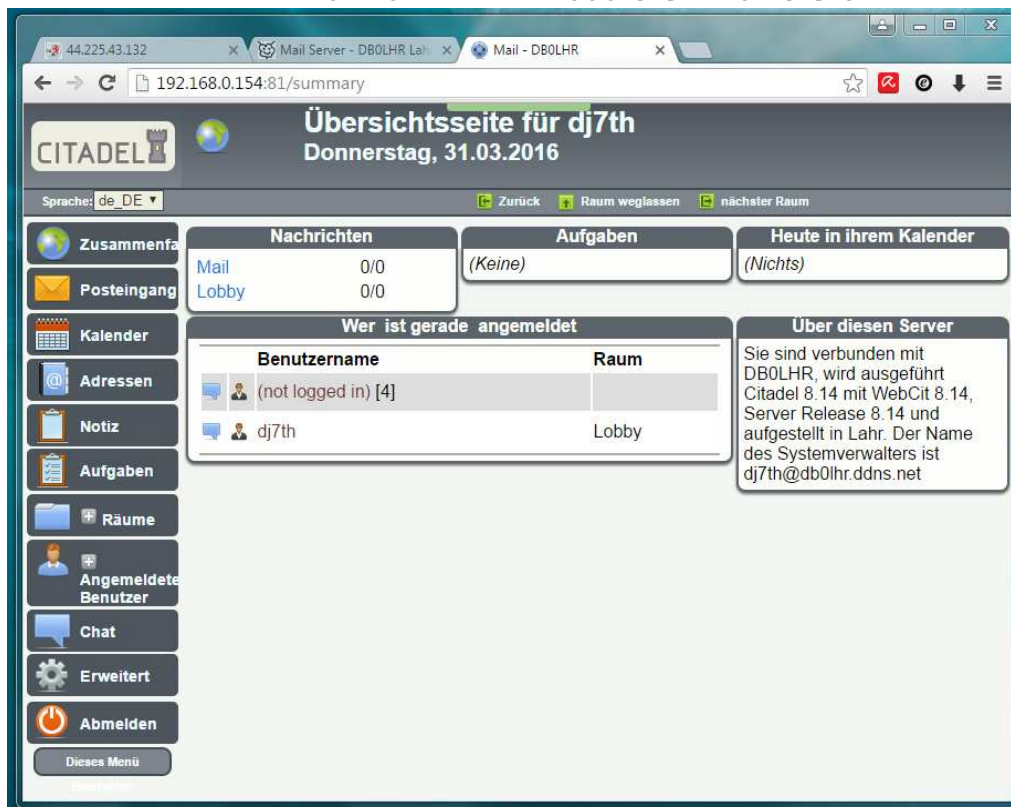
Im Netzwerk-Router ist folgender Port freizugeben: 10333 (TCP)

## Mail-Server einrichten

Der Mail-Server ermöglicht das Senden und Empfangen von E-Mails über das HAMNET. Die Übertragung erfolgt dabei völlig unabhängig vom Internet. Sowohl Sender als auch Empfänger der E-Mail müssen dazu lediglich über eine E-Mail Adresse im HAMNET verfügen.



*E-Mail via HAMNET mit üblichem Mail-Client*



*oder über den eingebauten Webmailer*

Eine Email-Adresse kann jeder Benutzer auf dem Server ganz einfach selbst einrichten.

## 1. Server aktivieren

Der Mail-Server wird mit den Befehlen

```
sudo update-rc.d citadel defaults  
sudo update-rc.d webcit defaults
```

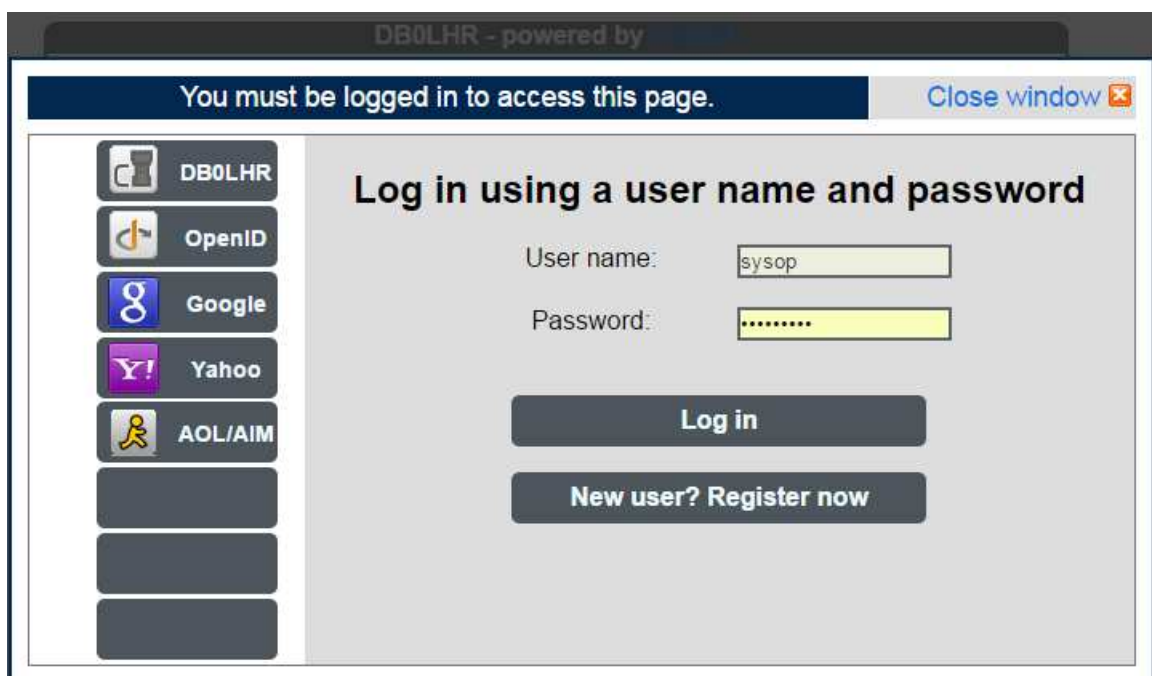
aktiviert und beim nächsten Neustart des Systems automatisch gestartet. Mit den Befehlen

```
sudo update-rc.d citadel remove  
sudo update-rc.d webcit remove
```

kann der Mail-Server wieder deaktiviert werden.

## 2. Kennwort ändern

Die Änderung des Kennwortes für den Mailserver wird über das Webinterface unter der URL <http://192.168.1.200:81> vorgenommen, sofern die URL noch nicht abgeändert ist:



The screenshot shows a web browser window titled "DB0LHR - powered by". The main content area has a dark blue header with the text "You must be logged in to access this page." and a "Close window" button. Below this, there is a sidebar with several login options: DB0LHR, OpenID, Google, Yahoo, and AOL/AIM. The main content area is titled "Log in using a user name and password" and contains a login form with fields for "User name:" (containing "sysop") and "Password:" (masked with dots). Below the form are two buttons: "Log in" and "New user? Register now".

Nach dem Login kann unter dem Menüpunkt „Erweitert“-„Ihre Biographie“ das Kennwort des sysop geändert werden. Dies gilt für den sysop als auch für die angemeldeten Benutzer. Im nachfolgenden Benutzer-Menü kann man links oben die Sprache wählen. Standard ist english oder wahlweise deutsch.

### 3. Konfiguration anpassen

Die nachstehende Konfiguration wird im Konfigurationsbereich des Mailservers unter der URL <http://192.168.1.200:81> als Benutzer „sysop“ vorgenommen. Alle erforderlichen Einstellungen befinden sich unter dem Menüpunkt "Verwaltung"-„Systemvorgaben bearbeiten“-„Allgemein“:

Allgemeine Standortskonfiguration	
Anmeldelogo wechseln	Anmeldelogo wechseln
Name des Knotens	<input type="text" value="DBOLHR-Pi"/>
Vollqualifizierter Domänenname	<input type="text" value="db0lhr.ampr.org"/>
Menschenlesbarer Knotenname	<input type="text" value="DBOLHR"/>
Telefonnummer	<input type="text" value="07824xxxxxx"/>
Eingabeaufforderung (nur für Textclients)	<input type="text" value="&lt;more&gt;"/>
Geografische Position dieses Systems	<input type="text" value="Lahr"/>
Name des Verwalters	<input type="text" value="dj7th@db0lhr.ddns.net"/>
Vorgabe Zeitzone für Kalendereinträge ohne Zeitzone	<input type="text" value="Europe/Berlin"/>

Bei den Änderungen sollte unbedingt die vorgegebene Syntax eingehalten werden, da sonst der Mailserver nicht ordnungsgemäß funktioniert. Die Vorgabe "nocall" wird durch das Rufzeichen des Servers, "Nowhere" durch den Standort und "mycall" durch das Rufzeichen des Sysops ersetzt.

**Tipp:** Weiterführende Informationen zu Citadel gibt es im Internet unter <http://www.citadel.org>

# Jabber-Server einrichten

Der Jabber-Server ermöglicht die dezentrale Kommunikation via Instant-Messenger über das HAMNET. Durch die Verwendung des XMPP-Protokolls funktioniert dies auch dann, wenn die Teilnehmer auf unterschiedlichen Servern eingeloggt sind.



*Instant Messaging mit Pidgin via Jabber/XMPP-Protokoll*

## 1. Konfiguration anpassen

Die Konfigurationsdatei des Jabber-Servers mit

```
sudo nano /etc/prosody/prosody.cfg.lua
```

in den Texteditor laden und die unten aufgeführten Zeilen, welche weit über den langen Text verteilt sind, suchen und entsprechend den eigenen Vorgaben anpassen:

```
admins = {"sysop@nocall.ampr.org" }  
VirtualHost "nocall.ampr.org"  
Component "conference.nocall.ampr.org" "muc"  
Component "proxy.nocall.ampr.org" "proxy65"
```

Nun mit "Strg-X", anschließendem "J" und der Eingabetaste die Datei abspeichern.



## 2. Server aktivieren

Der Jabber-Server wird aktiviert mit dem Befehl

```
sudo update-rc.d prosody defaults
```

und beim nächsten Neustart des Systems automatisch gestartet. Mit dem Befehl

```
sudo update-rc.d prosody remove
```

kann der Jabber-Server wieder deaktiviert werden.

**Tipp:** Weiterführende Informationen zu Prosody gibt es im Internet unter

<http://www.prosody.im>

## APRS-Gateway einrichten

Mit einem externen DVB-T-Stick kann der HAMServerPi auch als APRS-Gateway (RX) eingesetzt werden. Es ist dann nur noch eine Antenne für die APRS-Frequenz auf 144.800 MHz erforderlich. Geeignet ist z.B. der "DIGI VOX mini Air" von MSI. Die Sticks sind sehr klein, verfügen über eine MCX-Buchse für den Antennenanschluss und benötigen keine weitere Stromversorgung. Alternativ können aber auch alle anderen Sticks verwendet werden, die vom "rtl\_sdr"-Treiber unterstützt werden.

**Tip:** Der recht gut für APRS geeignete und an vielen Standorten eingesetzte "MSI DIGI VOX mini Air" ist im Moment leider sehr schlecht oder auch nur zu hohen Preisen zu bekommen. Wir konnten aber einen kleinen Restposten (neu und originalverpackt mit Zubehör) auftreiben. Weitere Infos unter [viewtopic.php?f=90&t=468](http://viewtopic.php?f=90&t=468).



*Der "DIGI Vox mini Air" von MSI*

### **1. Test des DVB-T-Sticks**

Mit dem Kommando

```
rtl_test
```

kann die Funktion des DVB-T-Sticks getestet werden.

### **2. Kalibrierung des DVB-T-Stick**

Mit dem nachfolgenden Befehl wird das GSM-Band (900MHz) gescannt und die empfangenen Basisstationen in einer Liste angezeigt. Dafür muss am DVB-T-Stick eine Antenne angeschlossen sein. Der Vorgang kann mehrere Minuten dauern.

```
kal -s GSM900
```

Anschließend wird die Kanalnummer der Basisstation mit dem stärksten Signal in der nachstehenden Befehlszeile eingefügt (anstatt der 36)

```
kal -c 36
```

Die so ermittelte Abweichung wird später unter "ppm" in die APRS-Konfigurationsdatei eingetragen.

### **3. Kennwort ermitteln**

Über den nachstehenden Befehl wird das APRS-Kennwort ermittelt. Anstatt "nocall" muss das eigene Rufzeichen (ohne SSID) verwendet werden:

```
/opt/pymultimonaprs/keygen.py nocall
```

Das so ermittelte Kennwort wird später unter "passcode" in die APRS-Konfigurationsdatei eingetragen.

### **4. Konfiguration anpassen**

Die APRS-Konfigurationsdatei mit

```
sudo nano /etc/pymultimonaprs.json
```

in den Texteditor laden und die nachstehenden Einstellungen entsprechend den eigenen Vorgaben anpassen:

```
"callsign": "NOCALL",  
"passcode": "0",  
"gateway": "servercall.ampr.org:14580",  
"ppm": 20.000  
"lat": 51.000000,  
"lng": 10.000000,
```

Unter "gateway" muss der nächste HAMNET-APRS-Server eingetragen werden. Im Distrikt Westfalen-Süd ist das z.B. "db0tv.ampr.org:14580". Danach mit "Strg-X", anschließendem "J" und der Eingabetaste die Datei abspeichern.

Mit dem Befehl

```
sudo pymultimonaprs -v
```

kann die Funktion des APRS-Gateways getestet werden.

## **5. Gateway aktivieren**

Das APRS-Gateway wird mit dem Befehl

```
sudo update-rc.d pymultimonaprs defaults
```

aktiviert und beim nächsten Neustart des Systems automatisch gestartet. Mit dem Befehl

```
sudo update-rc.d pymultimonaprs remove
```

kann das APRS-Gateway wieder deaktiviert werden.

**Tipp:** Weiterführende Informationen zu PyMultimonAPRS gibt es im Internet unter

<http://www.github.com/asdil12/pymultimonaprs>.

# APRS-Server einrichten

Der APRS-Server kann entweder als reiner HAMNET-Server oder auch als Gateway zwischen HAMNET-APRS-Stationen und dem APRS-IS eingesetzt werden. Es ist nicht erforderlich (und auch nicht sinnvoll), den APRS-Server auf jedem HAMServerPi zu aktivieren. Denn meistens ist ein HAMNET-APRS-Server pro Distrikt bzw. AS völlig ausreichend. Alle umliegenden HAMNET-APRS-Stationen (z.B. HAMServerPi mit PyMultimonAPRS oder Clients wie UI-View32) stellen eine Verbindung zu diesem Server her tauschen dann ihre Daten untereinander aus. Wenn der APRS-Server auch über eine Verbindung zum Internet verfügt, werden die Daten zudem ins weltweite APRS-System übertragen.

**Hinweis:** Bei aktiviertem APRS-Server kann die Status-Seite des Servers über den Port 14501 (z.B. <http://192.168.1.200:14501>) abgerufen werden. Die Anbindung der HAMNET-APRS-Stationen erfolgt über den Port 14580.

## 1. Kennwort ermitteln

Über den nachstehenden Befehl wird das APRS-Kennwort ermittelt. Anstatt "nocall" muss das eigene Rufzeichen (ohne SSID) verwendet werden:

```
/opt/pymultimonaprs/keygen.py nocall
```

Das so ermittelte Kennwort wird später unter "PassCode" in die Konfigurationsdatei des APRS-Servers eingetragen.

## 2. Konfiguration anpassen

Die Konfigurationsdatei des APRS-Servers mit

```
sudo nano /opt/aprsc/etc/aprsc.conf
```

in den Texteditor laden und die unten aufgeführten Zeilen entsprechend den eigenen Vorgaben anpassen:

```
ServerID NOCALL  
PassCode 0  
MyAdmin "Name, MYCALL"  
MyEmail mycall@nocall.ampr.org  
Uplink "Core rotate" full tcp rotate.aprs.net 10152  
#MagicBadness 42.7
```

Nun mit "Strg-X", anschließendem "J" und der Eingabetaste die Datei abspeichern.

### **3. Server aktivieren**

Der APRS-Server wird mit dem Befehl

```
sudo update-rc.d aprsc defaults
```

aktiviert und beim nächsten Neustart des Systems automatisch gestartet. Mit dem Befehl

```
sudo update-rc.d aprsc remove
```

kann der APRS-Server wieder deaktiviert werden.

**Tip:** Weiterführende Informationen zu aprsc gibt es im Internet unter

<http://he.fi/aprsc>.

# SvxLink einrichten

Mit passender Zusatzhardware kann der HAMServerPi auch als vollwertiges EchoLink/SvxLink-System eingesetzt werden. So verfügt die HAMServerPi RadioBox über einen integrierten VHF- bzw. UHF-Transceiver. Damit ist dann ein völlig eigenständiger Betrieb, z.B. als lokaler HotSpot möglich. An die TransceiverBox kann ein externer Transceiver und an die RepeaterBox ein Repeater angeschlossen werden. Dabei übernimmt SvxLink dann auch die komplette Steuerung. Die Anschlussbelegung der RepeaterBox ist kompatibel zur WX-Steuerung; ein Austausch ist somit problemlos möglich.



*HAMServerPi RadioBox: Mit VHF- oder UHF-Modul und Antennenbuchse*

## **1. Konfiguration anpassen**

Die SvxLink-Konfigurationsdatei in den Texteditor laden mit

```
sudo nano /etc/svxlink/svxlink.conf
```

und die nachstehenden Einstellungen entsprechend den eigenen Vorgaben anpassen:

```
[GLOBAL]  
LOGICS=SimplexLogic  
[SimplexLogic]  
CALLSIGN=NOCALL
```

Soll SvXLink nicht im Simplex-Modus sondern im Repeater-Modus betrieben werden, sind folgende Einstellungen erforderlich:

```
[GLOBAL]
LOGICS=RepeaterLogic
[RepeaterLogic]
CALLSIGN=NOCALL
```

Danach mit "Strg-X", anschließendem "J" und der Eingabetaste die Datei abspeichern.

## **2. EchoLink einrichten**

Die SvXLink-Konfigurationsdatei in den Texteditor laden mit

```
sudo nano /etc/svxlink/svxlink.conf
```

und die Zeile "MODULES" um den Eintrag "ModuleEchoLink" ergänzen:

```
[SimplexLogic]
MODULES=ModuleHelp,ModuleParrot,ModuleEchoLink
```

Abhängig vom Betriebsmodus muss der Eintrag "ModuleEchoLink" entweder unter "SimplexLogic" oder "RepeaterLogic" hinzugefügt werden.

Zur Übertragung von Status- und Standortmeldungen können die folgenden Einträge angepasst werden:

```
[GLOBAL]
LOCATION_INFO=LocationInfo

[LocationInfo]
LON_POSITION=10.00.00E
LAT_POSITION=51.00.00N
CALLSIGN=EL-NOCALL
FREQUENCY=999.999
TX_POWER=1
ANTENNA_GAIN=0
ANTENNA_HEIGHT=10m
ANTENNA_DIR=-1
```

Danach mit "Strg-X", anschließendem "J" und der Eingabetaste die Datei abspeichern.



Anschließend die EchoLink-Konfigurationsdatei in den Texteditor laden mit

```
sudo nano /etc/svxlink/svxlink.d/ModuleEchoLink.conf
```

und die nachstehenden Einstellungen entsprechend den eigenen Vorgaben anpassen:

```
[ModuleEchoLink]
SERVERS=europe.echolink.org
CALLSIGN=NOCALL-L
PASSWORD=TOPSECRET
SYSOPNAME=MYCALL
LOCATION=[HAMServerPi] Nowhere
```

**Hinweis:** HAMNET-Standorte verfügen in der Regel nicht über einen direkten Internetzugang. In diesem Fall kann für die EchoLink-Anbindung z.B. ein Proxyserver verwendet werden. Für Standorte im Distrikt Westfalen-Süd stellen wir für diesen Zweck gerne entsprechende Server zur Verfügung.

Die Daten des Proxyservers werden in den nachstehenden Zeilen eingetragen:

```
PROXY_SERVER=servercall.ampr.org
PROXY_PORT=8100
PROXY_PASSWORD=TOPSECRET
```

Danach mit "Strg-X", anschließendem "J" und der Eingabetaste die Datei abspeichern.

### **3. RadioBoard konfigurieren**

Zum Anpassen der Einstellungen des Transceiver-Moduls auf dem RadioBoard die TRX-Konfigurationsdatei mit

```
sudo nano /etc/trx/trx.conf
```

in den Texteditor laden und die nachstehende Zeile entsprechend den eigenen Vorgaben anpassen:

```
AT+DMOSETGROUP=1,000.0000,000.0000,0,6,0,4
```

Die einzelnen Werte hinter dem Eintrag "AT+DMOSETGROUP=" haben folgende Bedeutung:

1. Bandbreite (0=12.5kHz, 1=25.0kHz)
2. TX-Frequenz (z.B. 432.8750)
3. RX-Frequenz (z.B. 432.8750)
4. RX-CTCSS/CDCSS (0-121, 0=aus)
5. Squelch (0-8, 0=aus, 6=Standard)
6. TX-CTCSS/CDCSS (0-121, 0=aus)
7. Flag (4=Low Power, nicht ändern!)

Danach mit "Strg-X", anschließendem "J" und der Eingabetaste die Datei abspeichern.

**Hinweis:** Die Einstellungen werden jeweils beim Neustart des Systems zum Transceiver-Modul übertragen.

#### **4. SvxLink testen**

Mit dem Befehl

```
sudo svxlink
```

kann die Funktion des SvxLink-Systems getestet werden. So sollte z.B. nach dem Empfang des DTMF-Zeichens \* (Sternchen) eine kurze Sprachansage ausgesendet werden. Im Terminalfenster werden zudem Zustandsänderungen von PTT und Squelch sowie weitere Statusinformationen angezeigt.

#### **5. SvxLink aktivieren**

Ab Version HAMServerPi 1.2 wird SvxLink aktiviert mit

```
sudo update-rc.d svxlink defaults
```

und beim nächsten Neustart des Systems automatisch gestartet. Mit dem Befehl

```
sudo update-rc.d svxlink remove
```

kann SvxLink wieder deaktiviert werden.

**Tipp:** Weiterführende Informationen zu SvxLink gibt es im Internet unter <http://www.svxlink.org> und unter <http://www.svxlink.de>.

# SvxServer einrichten

Der SvxServer ermöglicht die Zusammenschaltung mehrerer Standorte zu einem permanenten SvxLink-Verbund. Da hierfür kein EchoLink und somit keine Internetverbindung erforderlich ist, funktioniert das auch bei reinen HAMNET-Standorten. Der SvxServer braucht nur an einem der Standorte eingerichtet und aktiviert zu werden. Alle beteiligten SvxLink-Systeme verbinden sich dann mit diesem Server.

**Hinweis:** Der SvxServer befindet sich derzeit in der Beta-Phase und wird daher noch nicht offiziell von SvxLink unterstützt.

## 1. SvxLink-Konfiguration anpassen

Zur Einrichtung einer Verbindung mit einem SvxServer die SvxLink-Konfigurationsdatei mit

```
sudo nano /etc/svxlink/svxlink.conf
```

in den Texteditor laden und die nachstehenden Einstellungen entsprechend den eigenen Vorgaben anpassen. Abhängig vom konfigurierten Betriebsmodus muss entweder "SimplexLogic" oder "RepeaterLogic" eingetragen werden. Unter "SERVERCALL" wird das Rufzeichen des entfernten SvxServers eingetragen.

```
[GLOBAL]
LOGICS=SimplexLogic,NetLogic
LINKS=NetLink

[NetLink]
CONNECT_LOGICS=SimplexLogic:9:SERVERCALL,NetLogic

[NetLogic]
CALLSIGN=NOCALL
```

Anschließend werden in den folgenden Zeilen die Zugangsdaten des SvxServers eingetragen:

```
[NetRx]
HOST=servercall.ampr.org
TCP_PORT=5210
AUTH_KEY="TOPSECRET"

[NetTx]
HOST=servercall.ampr.org
```

```
TCP_PORT=5210
AUTH_KEY="TOPSECRET"
```

Danach mit "Strg-X", anschließend "J" und der Eingabetaste die Datei abspeichern. Nach einem Neustart verbindet sich SvxBLink automatisch mit dem eingetragenen SvxBServer.

**Hinweis:** Zwischen allen beteiligten Systemen dürfen keine zusätzlichen EchoLink-Verbindungen aufgebaut werden. Dies kann man am besten mit einem Eintrag nach dem Muster "REJECT\_INCOMING=DB0XXX-L|DB0XXX-R" in der EchoLink-Konfigurationsdatei (ModuleEchoLink.conf) vermeiden.

## **2. SvxBServer-Konfiguration anpassen**

Der SvxBServer braucht nur auf einem der beteiligten Systeme eingerichtet werden. Dazu die SvxBServer-Konfigurationsdatei mit

```
sudo nano /etc/svxblink/svxbserver.conf
```

in den Texteditor laden und die nachstehenden Einstellungen entsprechend den eigenen Vorgaben anpassen:

```
[GLOBAL]
LISTEN_PORT=5210
AUTH_KEY="TOPSECRET"
```

Danach mit "Strg-X", anschließend "J" und der Eingabetaste die Datei abspeichern.

## **3. SvxBServer aktivieren**

Ab Version HAMServerPi 1.2 wird der SvxBServer mit

```
sudo update-rc.d svxbserver defaults
```

aktiviert und beim nächsten Neustart des Systems automatisch gestartet. Mit dem Befehl

```
sudo update-rc.d svxbserver remove
```

kann der SvxBServer wieder deaktiviert werden.

# VPN-Client einrichten

In der Regel wird der HAMServerPi direkt an einen HAMNET-Standort betrieben und an den jeweiligen Router oder aber abgesetzt über einen HF-Benutzerzugang angebunden. Somit ist der Server im HAMNET erreichbar und es sind keine weiteren Schritte erforderlich.

In sehr seltenen Fällen kann es jedoch erforderlich sein, die Verbindung zum HAMNET mit Hilfe einer VPN-Verbindung herzustellen. In diesem Fall ist ein Zugang zu einem VPN-Server erforderlich. Die entsprechenden Zugangsdaten (Adresse, Benutzername, Kennwort) erhält man beim Betreiber des jeweiligen VPN-Servers. Gegebenenfalls kann dieser auch eine feste IP-Adresse einrichten über die der Server dann im HAMNET erreichbar ist.

**Hinweis:** Die direkte Anbindung des HAMServerPi an das HAMNET ist auf jeden Fall einer VPN-Verbindung vorzuziehen. Denn meistens reicht die verfügbare Bandbreite eines normalen Internetanschlusses für einen zufriedenstellenden Betrieb nicht aus. Einfache Anwendungen werden vielleicht noch funktionieren, sobald aber etwas mehr Datendurchsatz erforderlich ist gelangt man damit sehr schnell an die Grenzen.

## 1. Konfiguration anpassen

Die Konfigurationsdatei für den VPN-Client mit

```
sudo nano /etc/ppp/peers/hamnet
```

in den Texteditor laden und die unten aufgeführten Zeilen entsprechend den eigenen Vorgaben anpassen:

```
pty "pptp vpn.servercall.org --nolaunchpppd --nobuffer --timeout 10"  
name srv-nocall
```

Der Eintrag "vpn.servercall.org" muss dabei durch die Adresse des VPN-Servers und der Eintrag "srv-nocall" durch den Benutzernamen ersetzt werden. Danach mit "Strg-X", anschließendem "J" und der Eingabetaste die Datei abspeichern.

## 2. Zugangsdaten anpassen

Zum Anpassen der Zugangsdaten die Konfigurationsdatei `/etc/ppp/chap-secrets` mit

```
sudo nano /etc/ppp/chap-secrets
```

in den Texteditor laden und die unten aufgeführten Zeilen entsprechend den eigenen Vorgaben anpassen:

```
srv-nocall PPTP topsecret
```

Hier muss der Eintrag `"srv-nocall"` durch den Benutzernamen und der Eintrag `"topsecret"` durch das zugehörige Kennwort ersetzt werden. Danach mit `"Strg-X"`, anschließend `"J"` und der Eingabetaste die Datei abspeichern.

## 3. VPN-Client aktivieren

Für den automatischen Start des VPN-Clients die Interface-Konfigurationsdatei `/network/Interfaces` mit

```
sudo nano /etc/network/interfaces
```

in den Texteditor laden und die Doppelkreuze unterhalb der Zeile `"# VPN"` wie nachstehend angegeben entfernen:

```
# VPN
auto tunnel
iface tunnel inet ppp
provider hamnet
```

**Hinweis:** In der Version des HAMServerPi 1.1 gibt es einen Fehler: In der letzten Zeile muss das Wort `"hamnet"` klein geschrieben werden.

Danach mit `"Strg-X"`, anschließend `"J"` und der Eingabetaste die Datei abspeichern. Nach einem Neustart des Systems wird der VPN-Client nun automatisch gestartet und die Verbindung zum HAMNET aufgebaut.

# PPTP VPN-Server installieren

GESCHRIEBEN VON JAN KARRES

[HTTP://JANKARRES.DE/2013/12/RASPBERRY-PI-PPTP-VPN-SERVER-INSTALLIEREN](http://jankarres.de/2013/12/raspberry-pi-pptp-vpn-server-installieren)

BEARBEITET VON ROLF -DJ7TH-

Ab und zu ist man in öffentlichen W-LAN Netzwerken, wie in einem Café oder an der Uni. Verwendet man dort das Internet einfach, so können meist alle Personen, die zur selben Zeit in dem W-LAN eingewählt sind, den Datenverkehr mitschneiden – ganz abgesehen vom Betreiber des Netzwerkes. Damit können auch Zugangsdaten und persönliche Informationen mitgeschnitten werden. Um dies zu verhindern, kann man den Internetverkehr durch eine verschlüsselte Verbindung leiten, einen sogenannten VPN-Tunnel. Dabei wird der Datenverkehr verschlüsselt an einen Server (in unserem Fall der Raspberry Pi zu Hause) geleitet, der wiederum die eigentlich gewünschten Abfragen ausführt und die Antworten wieder verschlüsselt zurück zu dir in das öffentliche Netzwerk sendet. Ein beliebter VPN Server, da er mit vielen Geräten von Haus aus kompatibel ist, ist PPTP. Daneben gibt es noch OpenVPN, der ebenfalls beliebt ist und zu dem ich bereits eine Installationsanleitung veröffentlicht habe. Auf die Vor- und Nachteile beider VPN-Server möchte ich an dieser Stelle jedoch nicht eingehen. Stattdessen erkläre ich im Folgenden wie man einen PPTP VPN-Server auf den Raspberry Pi installiert.

*Voraussetzung: Raspbian oder vergleichbare Distribution installiert*

**Wichtige Info:** Sherlock hat in den Kommentaren angemerkt, das die **Authentifizierung PPTP seit August 2012 als unsicher gilt**. Dies wurde damals durch Heise Security getestet. Mir war diese Umstand zum Zeitpunkt als das Tutorial verfasst wurde nicht bekannt. Ich kann euch an dieser Stelle nur dazu raten OpenVPN anstatt PPTP zu installieren.

## Step 1

Zunächst aktualisieren wir die bereits installierten Pakete des Betriebssystem, um sicherzugehen, dass diese aktuell sind.

```
sudo apt-get update && sudo apt-get upgrade
```

## Step 2

Nun installieren wir mittels des Paketmanagers *APT* den VPN-Server PPTP.

```
sudo apt-get install pptpd
```

### Step 3

Wir müssen nun in der Datei `/etc/pptp.conf` die lokale IP-Adresse des Raspberry Pi eintragen. Falls dir diese nicht bekannt sein sollte, kannst du diese im Router meist unter *Netzwerk, Verbundene Geräte* o.ä. herausfinden. In meinem Fall lautet die IP-Adresse 192.168.178.28 (muss im Folgenden durch die eigene IP-Adresse ersetzt werden). In dem Editor *nano* kann man mittels *STRG + X*, *Y* und *Enter* speichern.

```
sudo nano /etc/pptpd.conf
```

```
#localip 192.168.0.1
```

ersetzen durch

```
localip 192.168.178.28
```

### Step 4

Jetzt müssen wir am Ende der Datei `/etc/ppp/pptpd-options` folgende Zeilen einfügen. Der Parameter *ms-dns* definiert den DNS-Server, über den Domains aufgelöst werden. Hierbei kann natürlich auch ein anderer Server, z.B. aus der folgenden Liste, verwendet werden.

Öffentliche DNS-Server:

- OpenDNS: 208.67.222.222
- Chaos Computer Club Berlin: 213.73.91.35
- Google: 8.8.8.8
- HAMNET: 44.225.52.20

```
sudo nano /etc/ppp/pptpd-options
```

```
1 ms-dns 44.225.52.20
```

```
2 noipx
```

```
3 mtu 1490
```

```
4 mru 1490
```

### Step 5

Wir müssen nun noch eine Weiterleitung des Internetzugangs einrichten, sodass man über den Raspberry Pi auf das heimische Internet zugreifen kann.

```
sudo nano /etc/sysctl.conf
```

```
#net.ipv4.ip_forward=1
```

ersetzen durch

```
net.ipv4.ip_forward=1
```



### Step 6

Der Firewall auf dem Raspberry Pi müssen wir nun auch noch sagen, dass sie den Datenverkehr weiterleiten soll.

```
sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

### Step 7

Da die Firewall diese Anweisung nach jedem Neustart des Raspberry Pis löscht, müssen wir diese als Crontab eintragen, sodass sie bei jedem Start wieder definiert wird. Hierzu tragen wir einfach folgende Zeile am Ende der Crontab Datei ein.

```
sudo crontab -e
```

```
@reboot sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

### Step 8

Nun ist es an der Zeit, Benutzer anzulegen, die sich später mit dem PPTP VPN-Server verbinden können. Deren Zugangsdaten müssen wir nach folgendem Schema in die `/etc/ppp/chap-secrets` Datei eintragen. Pro Zeile darf ein Benutzer eingetragen werden.

```
sudo nano /etc/ppp/chap-secrets
```

mit folgendem Eingabe-Schema:

```
Benutzername[TAB]*[TAB]Kennwort[TAB]*
```

Beispiel:

```
Jan * SuperGeheimesPasswort *
```

### Step 8

Damit alle Änderungen übernommen werden, starten wir mittels folgenden Kommandos den PPTP VPN-Server neu.

```
sudo service pptpd restart
```

Fertig! Auf dem Raspberry Pi befindet sich nun ein einsatzbereiter PPTP VPN-Server. Wie man sich mit diesem unter verschiedenen Betriebssystemen verbindet, wird euch in den folgenden Anleitungen von anderen Bloggern/Webseiten erklärt. Was ich noch beim schreiben dieses Artikels bemerkt habe, ist, dass es manchmal bis zu einer Minute nach dem erfolgreichen Anmelden an den VPN-Server dauert, bis man über diesen auf das Internet zugreifen kann.

Anleitungen und Links nach Betriebssystemen:

- Windows XP
- Windows 7
- Windows 8
- Mac OS X
- Ubuntu
- iOS (iPhone/iPad)
- Android

### **Portfreigabe im Router**

Soll der VPN-Dienst auch außerhalb des eigenen Netzwerkes verfügbar sein, so müssen Ports im Router freigegeben werden.

Portfreigabe bei Fritz!Box und Speedport auf Port **1723 TCP**

Portforwarding benötigt man, da moderne Router eine Firewall beinhalten und Verbindungen an bestimmte Ports blockieren. Um diese jedoch freizugeben, verwendet man das Portforwarding oder auch Portfreigabe genannt.

Die in folgendem beschriebenen Vorgehensweisen funktionieren bei den Modellen AVM Fritz!Box 7390 und dem T-Com Speedport W 700V. Bei anderen Modellen kann die Vorgehensweise abweichend sein. Wenn du mit der folgenden Anleitung den entsprechenden Bereich nicht findest, schau bitte in die Betriebsanleitung deines Routers oder suche in Google nach „Portforwarding [Routername]“.

### **Anleitung für AVM Fritz!Box 7390**

#### **Step 1**

Zuerst müssen wir das Webinterface der Fritz!Box aufrufen, indem wir <http://fritz.box/> laden und, sofern gesetzt, uns mit einem Passwort einloggen.

#### **Step 2**

Nun gehen wir im Menü (links) auf *Internet* und auf den Unterpunkt *Freigaben*, um zu einer Übersicht der Portfreigabe zu gelangen.

## Freigaben

Portfreigaben

Speicher

FRITZ!Box-Dienste

Dynamic DNS

VPN

IPv6

An FRITZ!Box angeschlossene Computer sind sicher vor unerwünschten Zugriffen aus dem Internet. Für einige Anwendungen wie z.B. Online-Spiele oder das Filesharing-Programm eMule muss Ihr Computer jedoch für andere Teilnehmer des Internets erreichbar sein. Durch Portfreigaben erlauben Sie solche Verbindungen.

## Liste der Portfreigaben

Aktiv	Bezeichnung	Protokoll	Port	an Computer	an Port		
<input checked="" type="checkbox"/>	VPN-Server	TCP	1723	db0lhr	1723		
<input checked="" type="checkbox"/>	Audio-Server	TCP	64738	db0lhr	64738		
<input checked="" type="checkbox"/>	TT-Server	TCP	10333	db0lhr	10333		
<input checked="" type="checkbox"/>	VoIP-Server	TCP	5090	db0lhr	5060		
<input checked="" type="checkbox"/>	Web-Server	TCP	80	db0lhr	80		
<input checked="" type="checkbox"/>	RPI-Monitor	TCP	8888	db0lhr	8888		
<input checked="" type="checkbox"/>	Video-Server	TCP	9000-9001	db0lhr	9000-9001		
<input checked="" type="checkbox"/>	TT-Server	UDP	10333	db0lhr	10333		

Neue Portfreigabe

Änderungen der Sicherheitseinstellungen über UPnP gestatten

Geräte wie Smart-TV oder Smartphone bzw. Anwendungen mit UPnP-Unterstützung können im Heimnetz Sicherheitseinstellungen wie die Portfreigaberegeln der FRITZ!Box automatisch verändern. Aktivieren Sie diese Option aus Sicherheitsgründen nur, wenn Sie tatsächlich eingehende Verbindungen aus dem Internet gestatten möchten.

Übernehmen

Abbrechen

Aktualisieren

## Beispiel für die Portfreigaben in einer FritzBox

## Step 3

Um eine neue Portfreigabe anzulegen klicken wir nun auf den Button *Neue Portfreigabe*. Bei dem Dropdown *Portfreigabe* aktiv wählen wir *Andere Anwendungen*, um die Portfreigabe für einen beliebigen Service anlegen zu können. Nun können wir eine Bezeichnung der Portfreigabe wählen, welche lediglich strukturelle Relevanz hat. Daraufhin müssen wir das Protokoll wählen, in welchem der Service seine Daten sendet und empfängt. Falls dir dieser nicht bekannt ist, versuche erst **TCP** (meist benutzt) und probiere die anderen, falls TCP nicht funktioniert. Die dritte Einstellung hört auf den Namen *von Port*. Hierbei geben wir die Port(s) an, die zum Senden von Daten verwendet werden sollen. Nun müsst ihr den Raspberry Pi bzw. dessen IP-Adresse wählen, um diese Portfreigabe für den Minicomputer zu erlauben. Zuletzt muss *an Port* angegeben werden. Hier trägt man den Port ein, welcher zum Empfangen von Daten verwendet werden soll. In den meisten Fällen ist der Port zum Senden und Empfangen derselbe, z.B. **1723**

## Anleitung für T-Com Speedport W 700V

### Step 1

Zuerst müssen wir das Webinterface des Speedports aufrufen, indem wir <http://speedport.ip/> im Browser laden. Nun klicken wir auf *Konfiguration starten* und geben das gesetzte Passwort ein (steht meist hinten auf dem Speedport drauf).

### Step 2

Nun wählen wir im linken Menü den Punkt *Netzwerk* und auf der aufgerufenen Seite *NAT & Portregeln*. Auf der jetzt geladenen Seite gehen wir auf *PCs übernehmen & freigeben*.

### Step 3

In der vorliegenden Tabelle geben wir der internen IP-Adresse des Raspberry Pis einen Namen ohne Leer- und Sonderzeichen und speichern mit einem Klick auf *Übernehmen* ab.

### Step 4

Wir gehen mittels eines Klicks auf *Zurück* wieder auf die Seite, die wir in Step 2 aufrufen, wählen diesmal jedoch nicht *NAT & Portregeln* sondern *Port-Weiterleitung*. Im darauffolgenden Dialog klicken wir auf eines der zahlreichen *Neue Regel definieren*.

### Step 5

Jetzt können wir endlich die eigentliche Portweiterleitung einrichten. In dem Feld *Bezeichnung* geben wir der Portweiterleitung einen Namen, welcher keine technische Relevanz hat. Zusätzlich müssen wir die nebenstehende Checkbox mit der Bezeichnung *Aktiv* aktivieren, damit die Regel später auch umgesetzt wird. Unter *Gültig für PC*, wählen wir den soeben angelegten Namen des Raspberry Pis. Bei *TCP oder UDP* geben wir nun den Port an, welcher für den Raspberry Pi freigegeben werden soll (z.B. 1723). Wir bestätigen mit einem Klick auf *Speichern*.

Hier nochmals der Hinweis, dass die Einstellungen bei anderen Modellen woanders versteckt sein können. Meist sind diese jedoch an einer ähnlichen Stelle wie der, die ich im vorangegangenen Text beschrieben habe