freifunk.net Infoblatt

Wir suchen noch Mitstreiter und Aktivisten für unser Daten-Funknetzwerk „freifunk.net“. Dieses Infoblatt gibt einen Überblick über das Berliner freifunk.net und beantwortet mögliche Fragen.

Layer @: Motivation und Idee[*]

Geräte für die drahtlose Datenübertragung (WLAN, Wireless Local Area Network) haben mit Preisen von 20-100 Euro den Massenmarkt erobert. Die Datenübertragung über die Luft verursacht keine weiteren Kosten. Darüber hinaus ist die Datenübertragung über Grundstücksgrenzen hinweg legal. Damit besteht die Möglichkeit, ein unabhängiges Daten-Netzwerk auch privat zu betreiben. Diese Möglichkeit findet immer wieder begeisterte Anhänger. Je nach den Fähigkeiten und Vorstellungen der Betreiber entstehen dadurch ganz unterschiedliche drahtlose Netzwerke. Einige Beispiele:

- Hotspot-Modell: Ein Telekommunikationsanbieter bietet einen Internet-Zugriffspunkt gegen Gebühr an.
- WDS-Modell: Ein Betreiber bietet im Kiez Internet mit mehreren gekoppelten Zugriffspunkten an.
- Haus-Modell: Eine Hausgemeinschaft teilt sich einen schnellen Internet-Anschluss zur Kostenersparnis.
- Ad-hoc-Modell: Ein Bürger-Netzwerk bietet Funkübertragung über weitere Entfernungen.

Bei fast allen genannten Beispielen gibt es einen Zugriffspunkt (Master/Access Point) mit einer zentral verwalteten Funktion. Das freifunk.net ist ein Ad-hoc-Funknetzwerk (engl. Mesh). Im Unterschied zu anderen Funknetzwerken gibt es hier keine eindeutige Anbieter/Nutzer-Relation. Welche Dienste im freifunk.net angeboten werden, hängt von den Teilnehmern ab. Das kann der Internet-Zugang für eine Gruppe von Leuten sein. Aber auch Festplattenplatz für Backups, eine Audio-Übertragung für Freunde oder ein Netz von Web-Kameras sind möglich. Um die Datenübertragung auch über weitere Entfernungen zu ermöglichen, setzen wir auf diese Merkmale:

- Im Ad-Hoc-Modus kann jede Station mit jeder anderen Station gleichberechtigt kommunizieren.

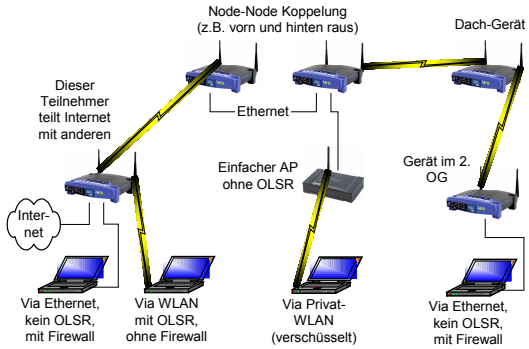
[*] Die erwähnten „Layer“ haben keine technische Funktion, sie dienen der Gliederung des Textes

- Es gibt keine Verschlüsselung auf der Funkebene. Damit kann jedermann am freifunk.net ohne zusätzliche technische Hürde teilnehmen.
- Die Teilnehmer sind mit der blockadefreien Durchleitung von Funknetz-Datenverkehr einverstanden.
- Sichere Übertragungen sind auf höheren Protokollebenen natürlich möglich. Beispiel: Die Übertragung von E-Mail kann bei GMX, Hotmail, Web.de u.a. problemlos auf Verschlüsselung mit SSL umgestellt werden. Geld-Transaktionen im Web sollten sowieso nur auf sicheren Seiten erfolgen, die mit dem SSL-Protokoll („https“) gesichert sind. Zwei Privatnetze kann man mit einem VPN-Produkt abhörsicher koppeln.
- Dienstanbieter schützen ihre kostenpflichtigen Ressourcen selbst. Beispiel: Jemand mit Internet-Flat-Rate stellt der freifunk.net-Gemeinde nur einen Teil der Datenrate zur Verfügung. Den Tauschbörsen-Videofreak in der Nachbarschaft schließt er mit einer Firewall-Regel vom seinem Internet-Zugang aus.

Layer A: Drahtlose Datenübertragung

- Erlaubt sind 100mW EIRP im 2.4 GHz Band (B/G Mode).
- Mit den Stummelantennen der WLAN-Router sind etwa 500 Meter möglich. Mit guten Richtantennen erreicht man auch bis zu 1000-2500 Meter.
- Diese Reichweiten sind **nur** bei Sichtverbindung möglich. Auch Bäume können stören.
- Gute Antennen verstärken in erster Linie den Empfang und blenden Störungen aus.
- Bei sehr hoher Nachbarschaftsdichte muss evt. die Sendeleistung begrenzt werden.

- In Berlin funken wir auf Kanal 10 im B/G-Mode mit der ESSID „olsr.freifunk.net“, der BSSID 02:ca:ff:ee:ba:be und mit vertikaler Polarisation: Stummel-Antennen aufrichten, BiQuad-Antennen horizontal (0-0-0-0) stellen. Einige Installationen funken allerdings mit horizontaler Polarisation (ausprobieren!).
- Bei guter Verbindung sind 50-200 Kbyte pro Sekunde im B-Mode möglich. Die Datenrate nimmt allerdings mit jeder weiteren Ad-hoc-Zwischenstation ab.
- Für längere Strecken existieren Links im Managed-Mode (BerlinBackBone, BBB).
- Eine Funktion „Antenna-Diversity“ besser ausschalten, RTS auf 250 einstellen. Für sehr schlechte Verbindungen die Fragmentation auf 500 einstellen, G-Mode auf „Auto B/G“.



Beispiel-Setup

Layer B: Kommunikation über TCP/IP

Jede Station im freifunk.net benötigt zunächst eine eindeutige IP-Adresse (z.B. 104.3.22.111) und eine Netzmaske (255.0.0.0). Unter der IP-Adresse kann jede Station von anderen Stationen aus erreicht werden. Die Verknüpfung aus IP-Adresse und Netzmaske zeigt an, welche anderen IP-Adressen zum freifunk.net gehören. Beispiele:

- 104.0.1.2: freifunk.net (weil erste Stelle 104)
- 216.239.57.104: Internet (IP von google.de)
- 192.168.1.1: Eine IP in einem Privatnetz

In Berlin vergeben wir IP-Adressen nach einem Postleitzahlen-Schema. Damit erhalten wir die Möglichkeit, zwischen den Stadtteilen den Datenverkehr besser zu steuern. Eine IP-Adresse kann durch Ausfüllen des Formulars „IP Vergabe“ auf der Seite http://www.olsrexperiment.de/ belegt werden. Durch wiederholtes Ausfüllen des Formulars können auch mehrere hintereinander liegende IP-Adressen belegt werden.

Bei der Einwahl in das Internet oder mit der Verbindung zu einem Access-Point (WLAN-Zugriffspunkt) wird einem Rechner üblicherweise eine gültige IP-Adresskonfiguration mitgeteilt. Dies umfasst eine IP-Adresse, die Netzmaske, das Standard-Gateway („wohin mit Internet-Anfragen“) und den DNS-Server zur Auflösung von DNS-Namen in IP-Adressen. Diese Konfiguration ist von einem Netzbetreiber oder von einem Administrator vorgegeben.

Weil es im freifunk.net aber keinen Administrator und auch keine technische Automatikkonfiguration gibt, müssen diese Angaben manuell eingestellt werden. Um beispielsweise einen Notebook unter Windows mit dem freifunk.net zu verbinden, muss man diese Schritte ausführen:

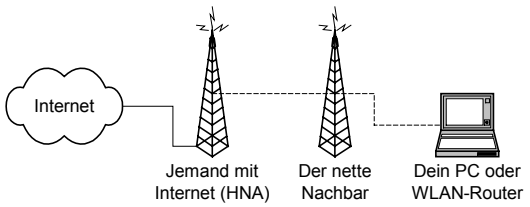
1. Stecke die WLAN-Karte ein (bei manchen Rechnern ist diese Karte bereits eingebaut).
2. Im Infobereich der Task-Leiste wird das Symbol für die drahtlose Netzwerk-Verbindung angezeigt. Über dieses Symbol erreicht man den Befehl „Nach Drahtlos-Netzwerken suchen“. Wähle „olsr.freifunk.net“ aus und drücke auf die Schaltfläche „Verbinden“. Der Dialog mit der Anzeige „Unsicheres Netzwerk“ muss mit „Trotzdem verbinden“ bestätigt werden. Eine vorhandene Firewall-Funktion muss ausgeschaltet werden.
3. War der Verbindungsversuch erfolgreich, rufe den Dialog „Erweiterte Einstellungen“ auf. Wähle den Listeneintrag „TCP/IP“ und gib im folgenden Dialog die IP-Adresse aus der IP-Vergabe, die Netzmaske 255.0.0.0 und der DNS-Server 195.50.140.250 ein.
4. Starte nun das OLSR-Dienstprogramm „OLSR-Switch“. Dieses Programm ermittelt erreichbare Stationen und Internet-Zugänge. Wähle die Schnittstelle mit der Funknetz-IP und aktiviere „ETX/LQ“ und „Fisheye-Routing“. Die aktuelle Version kann von http://www.olsr.org/ heruntergeladen werden. Weitere Infos und Tipps zur Konfiguration gibt es unter http://olsr.freifunk.net/ im Internet.

Hinweis: Gerade bei ersten Verbindungsversuchen mit Windows machen viele Leute Fehler. Sie können mit sehr ungeeigneten Einstellungen auch die Datenübertragung für Nachbarn stören oder gar blockieren. Dies ist ein weiterer Grund, weswegen wir die Verwendung eines WLAN-Routers mit Freifunk-Firmware empfehlen (siehe letzte Frage unter FAQ).

Layer C: Streckenführung mit OLSR

Das Routing-Protokoll für das freifunk.net heißt OLSR („Open Link State Routing“). Aber wozu

braucht man das überhaupt? Betrachte einmal folgende Situation:



Von deinem PC kannst du über die drahtlose Netzwerkverbindung einen Nachbarn direkt erreichen. Über eine WLAN-Karte sendest du dann Datenpakete an deinen Nachbarn. Wenn alles richtig konfiguriert ist, sendet der Nachbar auch direkt an deinen PC zurück. Dies kann man mit einem Echo-Request-Paket ("Ping") an die IP-Adresse deines Nachbarn prüfen. Wenn alles klappt, bekommst du ein Antwort-Paket zurückgesendet.

In der Beispielgrafik ist aber auch eine dritte Partei zu sehen: "Jemand mit Internet (HNA)". Die dritte Partei kannst du aber nicht direkt erreichen, sondern nur über den Nachbarn. Kein Problem denkst du: einfach ein Standard-Gateway einrichten und alles, was du nicht direkt erreichen kannst, an deinen Nachbarn senden. Der Nachbar wird die Datenpakete möglicherweise sogar weitersenden. Aber woher kennt die dritte Partei den Rückweg? Die Information "Rücksenden über den Nachbarn" steckt in den Datenpaketen einfach nicht drin. Datenpakete mit IP-Adressen, die die dritte Partei nicht direkt erreichen kann, wird sie möglicherweise einfach über die Internet-Verbindung weitersenden.

Benötigt wird ein Verfahren, um die Information "Ich bin über meinen Nachbarn zu erreichen!" im freifunk.net zu verbreiten. So ein Verfahren heißt "Routing-Protokoll", von denen es natürlich verschiedene gibt: beispielsweise RIP, OSPF oder eben OLSR. Ein OLSR-Dienstprogramm auf deinem PC kann regelmäßig diese Information an alle anderen Teilnehmer senden.

Gleichzeitig kümmert sich das OLSR-Dienstprogramm darum, die Netzwerk-Konfiguration an die aktuellen Gegebenheiten im freifunk.net anzupassen. Beispiele: Eine bessere indirekte Verbindung wird einer schlechteren direkten Verbindung vorgezogen. Beim Ausfall eines Gerätes wird eine alternative Route konfiguriert. Wir erreichen dies mit einer Erweiterung des OLSR-Protokolls („ETX/LQ“ mit Fisheye-Routing). Diese Erweiterung bewertet die Anzahl und Häufigkeit der empfangenen Hallo-Rundsendungen. Der Paketverlust bei solchen Rundsendungen („Broadcasts“) ist ein recht zuverlässiges Maß für die Effizienz einer Funkstrecke.

Layer D: Anwendungsregeln

- Freie Durchleitung des Funk-Datenverkehrs. Lies dazu das Pico Peering Agreement unter http://www.picopeer.net/PPA-de.html durch.
- Dienste können, müssen aber nicht mit der freifunk.net-Gemeinde geteilt werden.
- Es gibt keine absolute Anonymität im freifunk.net.
- Wir verwenden keine Datenverschlüsselung auf der Funk-Ebene.
- Die Stationen gehören den Betreibern. Wir erhalten kein Geld von Staat, Kirche oder Wirtschaft.
- Es gibt keine Funktionsgarantie und keine Beschwerdestelle für Fehlfunktionen.
- Wir sind kein drahtloser Internet-Provider. Wenn es zufällig Internet gibt, dann weil jemand seinen Anschluss mit anderen teilen mag.
- Unser Haupt-Internet-Zugang in der Bouchéstraße wird mit Privat-Spenden finanziert. Eine Accounting-Seite auf http://104.0.0.29/ informiert über den aktuellen Internet-Verbrauch über diesen Zugang.

FAQ

Frage: Ist die Funkstrahlung gefährlich?

Antwort: Nein. Es dürfen max. 100 Milliwatt Strahlung bei 2,4 GHz Frequenz abgegeben werden. Das ist ein vielfaches weniger als beispielsweise die Strahlungsleistung eines Mobiltelefons oder einer GSM-Sendeanlage. Oder anders: Es gibt eine gefährliche elektromagnetische Strahlung im Bereich 500.000 GHz, vor der niemand wirklich Angst hat: das Licht. Wir wissen, dass das mehrstündige Sonnenbad am Strand Auswirkungen hat. Der mehrjährige Aufenthalt unter einer am Schornstein montierten Taschenlampe ist im Gegensatz dazu ungefährlich. WLAN und Taschenlampe arbeiten mit etwa derselben Strahlungsleistung und beide senden auch keine besonders hochfrequenten UV-Strahlen aus.

Frage: Bin ich zur Verbindungsdatenspeicherung verpflichtet?

Antwort: Generell hat sich dazu noch niemand geäußert. Internet-Provider müssen dies für die Strafverfolgungsbehörden leisten. Damit niemand auf dumme Ideen kommt, verwenden wir ausschließlich Geräte, die mangels Speicherplatz

eine solche Möglichkeit nicht bieten. Da wir unverschlüsselt funken, spricht natürlich auch nichts gegen eine Abhörstation im freifunk.net.

Frage: Bei wem beschwere ich mich, falls etwas nicht funktioniert?

Antwort: Bei niemand. Es gibt zwar ein paar engagierte Leute. Also welche, die genug Ahnung haben um Beratung und Troubleshooting zu machen. Aber generell gilt: Probleme müssen selbst gelöst werden. Möglicherweise hilft das Gespräch mit den freifunk.net-Nachbarn. In Berlin treffen wir uns regelmäßig am Mittwoch Abend auf der c-base, Rungestr. 20, siehe: http://www.c-base.org/.

Frage: Was tun gegen Vandalen und übermäßigen Peer-to-Peer-Konsum?

Antwort: Wir haben keine freifunk.net-Polizei. Bisher läuft es ganz gut, möglicherweise weil die technischen Hürden den typischen Randalierer überfordern. Generell gilt: Ein Funknetzwerk ist technisch gegen DOS-Attacken nicht zu sichern. Störungen im freifunk.net beeinträchtigen auch die Datenübertragung der professionellen Anbieter. Übermäßiger Peer-to-Peer-Konsum belegt zudem im freifunk.net die zur Verfügung stehende Übertragungskapazität. Bisher hat es ausgereicht, wenn die Nachbarn die eine oder andere MAC-Adresse zeitweise sperren.

Frage: Funktioniert es wirklich ohne Administration?

Antwort: Nein, nicht ganz. Ein Beispiel: Auf der c-base funktioniert das freifunk.net wunderbar. Aber nicht am Mittwoch Abend. Es ist bei unseren Treffen häufig jemand mit einen fehlkonfiguriertem Gerät vor Ort, der dort das freifunk.net blockiert. Für die Fernverbindungen zwischen den Stadteilen setzen wir auf Punkt-zu-Punkt-Verbindungen mit Richtantennen im Managed-Mode. Die Leute, die das Kennwort für diese Stationen wissen, könnte man Administratoren nennen. Für Probleme vor Ort findet sich eigentlich immer jemand mit ausreichend Erfahrung und Hintergrundwissen. Das freifunk.net selbst ist von solchen lokalen Problemen so gut wie nie als ganzes betroffen.

Frage: Kann man völlig anonym Web-Seiten abrufen?

Antwort: Auch im freifunk.net wird eine IP-Adresse benötigt, die niemand anderes benutzt. Dafür haben wir einen Service, die IP-Vergabe unter http://www.olsrexperiment.de/. Die dort hinterlegte E-Mail-Adresse gibt allen anderen die Möglichkeit, bei technischen oder organisatorischen Problemen eine E-Mail zu senden. Für gesellschaftlich geächtete Abrufe wäre es sicher anonymer, sich gleich in das mehr oder weniger geschützte WLAN-Netz eines Nachbarn zu hacken - etwa 75% aller WLAN-Stationen haben keinen ausreichenden Schutz.

Frage: Was für Leute machen mit?

Antwort: Eine bunte Mischung. Wir haben Studenten, die am Wohnort kein preiswertes DSL bekommen und den Internet-Zugriff für die WG darüber machen. Jüngere männliche Funker sind in der Überzahl. Es gibt aber auch Frauen und ältere Mitfunker mit CB- und Amateur-Funkerfahrung. Es gibt welche, die wollen alles richtig machen und brauchen ewig. Es gibt welche, die stürzen in den nächsten Laden und kaufen zwei WRT54GS-Geräte um nach ein paar Versuchen frustriert aufzugeben. Es gibt Kontakte und Projekte mit Schulen, Kirchen, Kneipen und Kulturinstitutionen. Es gibt Visionäre, die eine globale Netzwerk-Allmende entstehen sehen, die zur Überwindung der digitalen Kluft und zur Unterstützung von Entwicklungsländern beitragen könnte. Es gibt Praktiker, die daraus eine Geschäftsidee machen wollen. Gerade in Berlin umfasst diese Mischung auch Leute mit Netzwerk-Ahnung, Antennen-Erfahrung, Programmierer, PR-Leute und Organisatoren, die eine Verbindung zur Kulturszene herstellen.

Frage: Was wäre mein Beitrag wert?

Antwort: Natürlich suchen wir immer wieder gute Standorte. Bist Du der Eigner dieser wunderbaren Suite im 38 Stock des Park-Inn-Hotels könnten wir uns durchaus zusammenraufen und das Gerät sowie die Antennen- und Software-Installation übernehmen. Ansonsten gilt: Du bist herzlich eingeladen mit Geräten, Know-how und Ausdauer am Aufbau des freifunk.net teilzunehmen. Für überlassene Internet-Datenübertragung findet sich sicher auch jemand, der ein Bier auf der c-base spendiert. Wir haben eine Kasse für unseren zentralen Internet-Zugang in der Bouchéstraße. Spenden für diesen Zugang sind gerne gesehen und von den direkten Nutznießern in gewisser weise gefordert (siehe unser Accounting unter http://104.0.0.29/ - nur im freifunk.net abrufbar).

Frage: Wo finde ich Anschluss?

Antwort: Überall da, wo engagierte Leute sich zusammenschließen. Es gibt aktive Gruppen in Friedrichshain, Kreuzberg, Mitte sowie in Hohenschönhausen und Weißensee. Größere Gruppen finden sich auch in Wien, London, Paris aber auch in Rostock, Weimar, München um nur einige zu nennen. Für die aktuelle Situation in Berlin existiert eine Karte, die fast in Echtzeit vorhandene

Verbindungen anzeigt. Siehe http://www.olsrexperiment.de/.

Frage: Sind auch andere Netzstrukturen möglich?

Antwort: Ja natürlich. Es steht dir frei, ein eigenes Funknetz mit anderen Regeln zu machen. Nicht jedes Funknetz ist so wie das Berliner freifunk.net organisiert. Beispiele: In Wien hat ein Teilnehmer so gut wie keine Konfigurationsmöglichkeiten. Für jeden Teilnehmer stellen sie dort eine extra zugeschnittene Firmware mit festen Einstellungen her. In London existiert auf jeder Station eine Zwangs-Webseite mit einer [Einverstanden]-Schaltfläche. Darüber wollen sie lokale Inhalte, Neuigkeiten sowie möglicherweise Werbung verbreiten. In Amsterdam geben sie nur wenige Konfigurationseinstellungen frei und achten insbesondere auf das Traffic-Shaping („Verkehrs-Optimierung“) der Internet-Zugänge. In Athen gibt es gar kein stadtweites Netz. Dafür existiert aber eine riesige Zahl von Access-Points, die man nutzen kann wenn man den Betreiber persönlich kennt. In Tschechien gibt es sehr viele einzelne Funknetze, die hauptsächlich über funknetz-internes Peer-to-Peer digitale Inhalte tauschen.

Frage: Wird es auf Dauer nicht eng in der Luft?

Antwort: Es gibt zwar mittlerweile bei Aldi WLAN-Babycams und Geräte zum Verlängern von Audioleitungen, aber diese werden normalerweise innerhalb von Gebäuden betrieben. Eine durchschnittliche Mauer ist auch eine Barriere für den WLAN-Funk. Mit gut ausgerichteten Antennen stören uns diese zusätzlichen WLAN-Geräte nicht. Zukünftig kann es aber nötig werden, in bestimmten Gebieten in den noch wenig belegten A-Mode (5 GHz) auszuweichen.

Frage: Wieso werden so viele Linksys-Geräte benutzt?

Antwort: Auf einem Notebook kann man die benötigte Software installieren und das Gerät in den Ad-Hoc-Modus umschalten. Und natürlich kann man das Notebook an den Schornstein nageln. Ein Notebook verbraucht allerdings viel Energie und ist für diesen Einsatz auch etwas zu schade. So ein WLAN-Access-Point oder WLAN-Router ist besser geeignet. Schon allein die Tatsache, dass keine anderen Anwendungen darauf laufen, garantiert einen störungsfreien Dauerbetrieb. Für diese Geräte setzen viele Hersteller das Betriebssystem Linux ein. Die Firma Linksys war einer der ersten Hersteller, der zur Veröffentlichung des Geräte-Quellcodes im Sinne der GPL (Linux-Lizenz-Bedingungen) „überredet“ werden konnte. Erst mit diesem Quellcode können wir die Software dieser Geräte (i.d.R. WRT54G oder WRT54GS, siehe http://www.freifunk.net/wiki/FreifunkFirmware) für unsere Zwecke anpassen. Mit einem Original-Gerät aus dem Kaufhaus funktioniert unsere Art der Vernetzung nämlich nicht. Mittlerweise stellen auch andere Hersteller Linux-Quellcodes zur Verfügung. Allerdings haben sich noch nicht für alle Gerätetypen und Hersteller auch Programmierer gefunden, die die notwendigen Anpassungen machen. Wenn du Ahnung und ein halbes Jahr Zeit hast, kannst du das ja selbst übernehmen. Wir setzen auch für bestimmte Strecken den Meshcube von 4G-Systems ein, ein etwas teureres Gerät mit zwei WLAN-Karten.

Frage: Dürft ihr die IP-Adressen 104.0.0.0/8 benutzen?

Antwort: Im Internet ist dieser Adressbereich als „für zukünftige Erweiterungen“ reserviert. Wir müssen aber nun wirklich nicht beim IETF fragen - das ist unser Netz. Wir verwenden diese IP-Adressen, um private IP-Adressbereiche (z.B. 192.168.0.0/16 für ein privates LAN) und den Funk-IP-Bereich gut trennen zu können. Diese Unterscheidung ermöglicht eine einfach Abgrenzung mit Firewall-Regeln. Andere Funknetze benutzen häufig 10.0.0.0/8 - daher müssen wir auch nicht umstellen, wenn wir mit einem dieser Netze zusammenschalten wollen.

Studenten-Frage: Warum macht ihr das völlig veraltete IPv4?

Praktiker-Antwort: Weil wir Dinge gerne zum Laufen bringen. Es ist beispielsweise viel interessanter, Multicast-IP für Radio-Rundsendungen zu realisieren als sich mit dem Eintippen langer IPv6-Adressen zu plagen. Aber vielleicht gibt es ja eines Tages eine wirklich wichtige Anwendung, die IPv6 erfordert.

Frage: Kann ich das Internet-Gateway fest einstellen?

Antwort: Nein, das geht nicht. Eine manuell gesetzte Default-Route stört andere Teilnehmer. Verwende statt dessen den Parameter „LinkQuality-Mult“ um die Auswahl des OLSR-Dienstprogramms zu optimieren oder konfiguriere einen IP-Tunnel.

Frage: Kann ich eine lange Antennenleitung verwenden?

Antwort: Jein. Nur spezielle Koax-Leitungen haben geringe Verluste im Hochfrequenz-Bereich. Eine

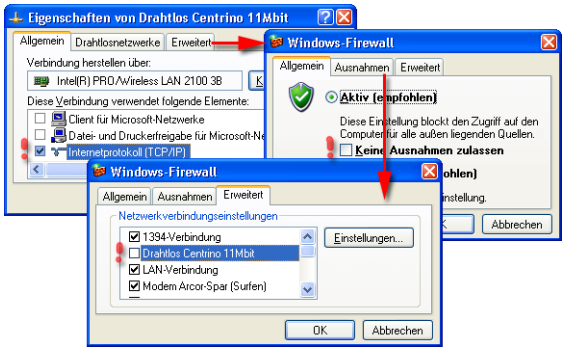
20 Meter lange und 12 mm dicke und steife Leitung kostet etwa soviel wie ein zweites Gerät. Ein zweites Gerät auf dem Dach oder ein Gerät an einer langen Ethernet-Leitung wäre besser geeignet.

Frage: Ist WLAN nicht generell unsicher?

Antwort: Die Sicherheit von Datenübertragung in öffentlichen Netzen hängt immer davon ab, ob du die möglichen Sicherheitsfunktionen auch benutzt. Das gilt für das Internet, für das Telefonnetz und natürlich auch für das freifunk.net. Die Übertragung auf der untersten Funk-Protokollebene ist gewollt offen, damit andere ohne technische Zusatzhürde teilnehmen können. Bei einem Linksys WRT54G mit Freifunk-Firmware schützen Firewall-Regeln das interne Drahtnetz vor unberechtigten Zugriffen aus dem Funknetz.
Tipp 1: Einen Windows-PC ohne zusätzlichen Schutz niemals mit öffentlichen Netzen verbinden.
Tipp 2: Keine WLAN-Ausrüstung im privaten Netzwerk ohne WPA-Verschlüsselung verwenden. Eine 128er WEP-Verschlüsselung kann man heute in nur 30 Minuten brechen.
Tipp 3: Schon einmal über verschlüsselte Telefonate nachgedacht?

Frage: Kann ich eine Firewall verwenden?

Antwort: Selbstverständlich. Allerdings sind die einfachen Firewall-Produkte (Windows-Firewall, SuseWall, Shorewall o.ä.) üblicherweise so eingestellt, dass der Datenverkehr von anderen blockiert wird. Ein paar Windows-Benutzer mit Standard-einstellungen behindern sich gern gegenseitig. Es ist besser und durchaus sicher genug, eine solche Firewall-Funktion für die WLAN-Karte nicht zu verwenden. Für Windows sollte man die Bindungen aller unnötigen Netzwerk-Protokolle an die WLAN-Karte ausschalten. Nur „TCP/IP“ wird wirklich benötigt, insbesondere „Windows-Netzwerk“ besser ausschalten.



Frage: Bin ich jetzt endlich drin?

Antwort: Rufe auf „ping 151.1.1.1“ (Windows-Kommandozeile oder Linux-Prompt). Kommt eine Antwort, kannst du offenbar diesen italienischen Provider erreichen. Gibt es keine Antwort, versuche „tracert -d 151.1.1.1“ (Windows) oder „traceroute -n 151.1.1.1“ (Linux), dies zeigt den Datenweg an. Möglicherweise ist deine IP-Adresse noch nicht in der IP-Vergabe registriert - Update immer um Mitternacht. Klappt das Ping, aber „google.de“ kann nicht aufgerufen werden, ist der DNS-Server ungültig. Konfiguriere DNS=212.222.128.68.

Frage: Ist das nicht alles zu kompliziert für mich?

Antwort: Nein, keineswegs. Auch wenn nicht alle diese Fragen und Antworten für dich einen Sinn ergeben, kannst du teilnehmen. Eine Standard-Konfiguration ist schnell und einfach hergestellt:

1. Kaufe einen WLAN-Router „Linksys WRT54GL“ (Preis: ca. 60,-- Euro).
2. Fülle das Formular „IP Vergabe“ unter http://www.olsrexperiment.de/ aus. Lade anschließend die angebotene Freifunk-Firmware-Datei für den WRT54G(L) herunter.
3. Lies die Kurzbedienungsanleitung für den WRT54G(L) und rufe dessen Admin-Webseite auf. Übertrage die Freifunk-Firmware-Datei mit der Firmware-Update-Funktion. Setze anschließend ein neues Kennwort. Es ist keine weitere Konfiguration nötig.
4. Kaufe eine wasserdichte große Tupperware-Schale und 50 Meter Klingeldraht-Doppellitze. Bohre 2 Antennen-Löcher in die Schale und montiere sie mit WRT54G(L) kopfüber unterhalb des Blitzableiters.
5. Stelle mit der Klingelleitung eine Verlängerung des Steckernetzteils her und schließe es an.

Sollte etwas nicht funktionieren: Die Original-Firmware wiederherstellen und das Gerät zurückbringen. Zur Stromversorgung können auch vorhandene Sat-Leitungen oder die 4 unbenutzten Adern einer Cat5-Netzwerkleitung verwendet werden. Optimieren kann man das Setup mit einer guten Antenne, z.B. eine Doppel-Biquad. Eine Bauanleitung mit 10-20 Euro Materialaufwand gibt es im Internet: http://martybugs.net/wireless/biquad/double.cgi. Antennen-Zubehör wie z.B. den RP-TNC-Antennenstecker für den Linksys gibt es bei Segor in Moabit (http://www.segor.de/).

Weitere Fragen beantwortet sicher gerne jemand auf der Freifunk-Mailing-Liste [wlanware], im Forum von olsrexperiment.de oder auf [Berlin Wireless] (siehe http://www.olsrexperiment.de/cgi-bin/mailman/listinfo/berlin).