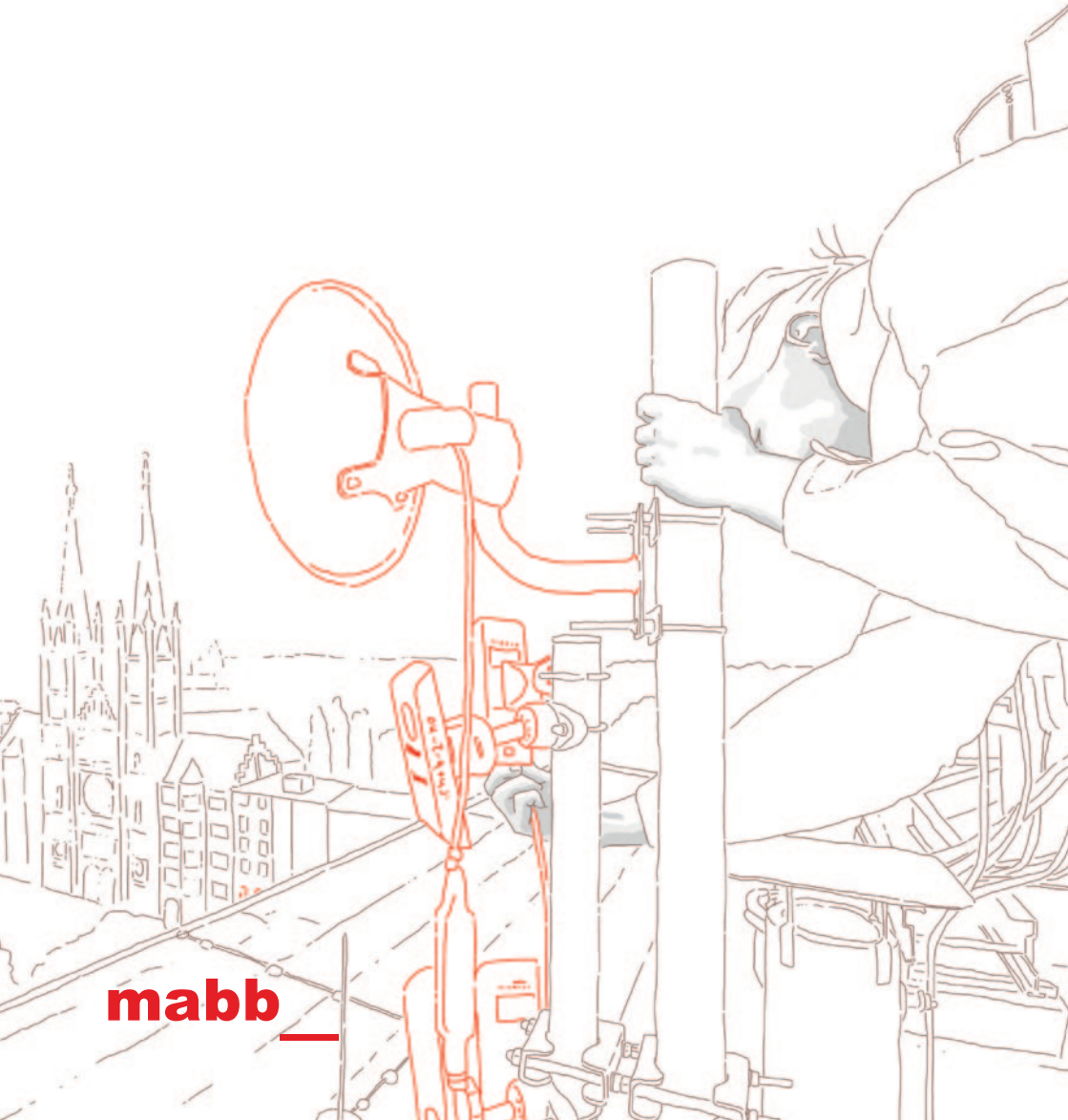


# WLAN FÜR ALLE

Freie Funknetze in der Praxis



**mabb**

»

Die mabb unterstützt die Freifunk-Initiative, da WLAN-Netze eine Schlüsselfunktion einnehmen, wenn es um zeitgemäße Formen der Mediennutzung geht. Die Vision der Freifunker gibt neue Impulse für Innovationen im Netz, auch weil sie von dem Ziel offener Kommunikation, nicht von Geschäftsmodellen geleitet sind.

Dr. Hans Hege

«

# Freie Funknetze in der Praxis

## WLAN FÜR ALLE

*WLAN im öffentlichen Raum, kostenlos und leicht zugänglich – die Nachfrage nach einem solchen Angebot steigt stetig. Inzwischen möchte jeder unterwegs Informationen online abrufen können, auch datenintensivere Inhalte. Mit den Volumengrenzen der Mobilfunk-Angebote ist das nicht zu schaffen.*

Hier kommt WLAN ins Spiel – nicht nur WLAN-Netze kommerzieller Anbieter, sondern auch die dezentralen Infrastrukturen der ehrenamtlich organisierten Freifunk-Community. Mehr als 6.000 öffentlich verfügbare WLAN-Hotspots wurden in den letzten zehn Jahren von über 100 Freifunk-Initiativen in Deutschland installiert. Allein in Berlin gibt es über 200 Zugangspunkte.

Die Medienanstalt Berlin-Brandenburg (mabb) unterstützt die Freifunker in Berlin seit 2012 bei der Modernisierung und Erweiterung ihrer Infrastruktur. So haben sich Geschwindigkeit und Nutzung des Berliner Freifunk-Netzes innerhalb von nur zwei Jahren vervielfacht. Das ist ein Anfang, aber noch nicht genug. Noch kennen zu wenige Bürger und Institutionen das Angebot der Freifunker. Und die, die es kennen, haben Bedenken und Vorbehalte, es zu nutzen oder gar selbst anzubieten. Fragen wie „Ist das Freifunk-Netz sicher?“, „Mache ich mich strafbar, wenn ich meinen Router für andere öffne?“ und „Haftete ich für illegale Downloads anderer?“ werden immer wieder gestellt.

Diese Fragen greift die Broschüre „WLAN FÜR ALLE – Freie Funknetze in der Praxis“ auf und erläutert, was sich hinter Freifunk verbirgt, welche Chancen und Risiken mit diesem Netz verbunden sind und was der Unterschied zu einem Internetanschluss kommerzieller Anbieter ist. Gleichzeitig gibt sie praktische Erläuterungen und Anwendungshinweise für Nutzer und Anbieter und zeigt Erfolgsgeschichten der letzten Jahre. Das Ziel ist, die Bekanntheit von Freifunk in der Öffentlichkeit zu vergrößern, weitere Kooperationen zu schaffen und mehr Nutzung zu erreichen. Öffentliche Einrichtungen wie Bürgerämter oder Rathäuser, aber auch die Bürger selbst sollen als Unterstützer gewonnen werden.



# Inhalt

	Editorial	4
<b>TEIL 1</b>	<b>DEFINITION UND GESCHICHTE</b>	
	Was ist Freifunk?	8
	Stationen 2002–2014	14
<b>TEIL 2</b>	<b>TECHNIK</b>	
	Mesh-Netze am Beispiel Berlin	20
	Freifunk in Zahlen	23
<b>TEIL 3</b>	<b>SICHERHEIT</b>	
	WLAN FÜR ALLE – aber sicher?	24
<b>TEIL 4</b>	<b>RECHT</b>	
	Ein Netz voller Fallgruben?	30
<b>TEIL 5</b>	<b>WEITERFÜHRENDE INFORMATIONEN</b>	
	Häufige Fragen	36
	Glossar	39
	Lektüre	43
	Impressum	45

VORWORT VON DR. HANS HEGE

# Editorial

*Was hat die mabb mit Freifunk zu tun? Das hat uns der Berliner Rechnungshof gefragt, als er von unserer Förderung des Backbone für die Berliner Freifunk-Netze erfuhr. Die Antwort: Es gehört seit ihrer Gründung zu den Aufgaben der mabb, offene Wege für Medien und Kommunikation zu unterstützen und auch nicht kommerziellen Initiativen Chancen zu eröffnen.*

Durch die Digitalisierung verändern sich nicht nur die klassischen Rundfunkübertragungswege, sie werden durch das Internet ergänzt und teilweise auch ersetzt. Die zweiseitige Kommunikation, ein früher Traum der Kabelkommunikation, wird Realität und ermöglicht neue Formen der Bürgerpartizipation. Durch den Breitbandausbau können auch audiovisuelle Medieninhalte über das Internet genutzt werden, mobil und portabel mit neuen Geräten wie Tablets und Smartphones.

WLAN-Netze haben eine Schlüsselfunktion für diese neuen Formen der Mediennutzung. Zuhause und am Arbeitsplatz ermöglichen sie einen einfachen Zugang zu Medieninhalten. Nach Schätzungen entfallen 90 Prozent des auf Tablets genutzten Datenvolumens auf WLAN-Netze. Nur 10 Prozent werden über Mobilfunknetze genutzt, deren Volumengrenzen besonders die datenintensive audiovisuelle Mediennutzung treffen.

Kommunikation und Mediennutzung finden auch im öffentlichen Raum statt, auf belebten Plätzen, in öffentlichen Gebäuden, im öffentlichen Nahverkehr. Nach mehrjähriger Beobachtung der Marktentwicklung hielt die mabb die Zeit für gekommen, Projekte zur Nutzung von WLAN im öffentlichen Raum zu unterstützen. Ziel des Projekts PUBLIC WIFI der mabb ist es, einen – wenn auch zeitlich begrenzten – kostenfreien Internetzugang im öffentlichen Raum zu erreichen und für audiovisuelle Medieninhalte eine unbegrenzte kostenfreie Nutzung zu ermöglichen.

Das Pilotprojekt mit Kabel Deutschland war ein Anstoß für die Einrichtung entsprechender WLAN-Hotspots in anderen Teilen Deutschlands und generell für den freien Empfang von WLAN. Noch dominiert aber im kommerziellen Bereich die Neigung, einen WLAN-Zugang unterwegs nur den eigenen Kunden und nur im Rahmen kostenintensiverer Tarife zu öffnen.

Umso wichtiger wird die nicht kommerzielle Alternative des Freifunks. Die mabb unterstützt die Erneuerung und den Ausbau des Rückgrats des Berlin Backbone zur Verbindung der verschiedenen Freifunk-Netze. Öffentliche Gebäude können dafür genutzt werden, auch die mabb stellt ihre Räumlichkeiten am Hackeschen Markt für einen Anschluss zur Verfügung. Die wichtigste Arbeit aber leisten die Freifunk-Initiativen: Sie helfen sich selbst und geben Anstöße zur Innovation, auch weil sie von dem Ziel offener Kommunikation, nicht von Geschäftsmodellen geleitet sind.

Der Freifunk-Verein ist deshalb auch Partner für das nächste Projekt der mabb im WLAN-Bereich, der Erprobung der Nutzung von Rundfunkfrequenzen mit ihren besonderen Empfangseigenschaften. Denn gerade im öffentlichen Raum kann die Reichweite der Hotspots noch vergrößert werden.

Dr. Hans Hege  
Direktor der Medienanstalt Berlin-Brandenburg





# Definition und Geschichte



## DEFINITION UND GESCHICHTE

# Was ist Freifunk?

*Freifunk ist der bekannteste Name für Initiativen, bei denen Bürger freie Daten-Funknetze aufbauen, die auch Zugang zum Internet bieten.*

Fast jeder hat heutzutage einen Router mit WLAN-Funktion zu Hause, der Zugang zum Internet schafft und das Signal drahtlos in die nähere Umgebung weiterverteilt. Wer in den Städten nach WLAN-Zugängen sucht, findet meist Dutzende verschiedener Netze, die von Privatpersonen, Cafés und vielen anderen unterhalten werden.

Die Grundidee von Freifunk basiert darauf, solche Netze nicht nur als getrennte Internet-Einwahlknoten zu nutzen, sondern untereinander zu verbinden und zu einem Bürgernetz zusammenzuschließen. So entsteht ein eigenes lokales Netz, in dem der Datenverkehr über alle beteiligten Stationen wandern kann. Mit dem Internet verbunden wird es unter anderem, indem Bürger ihren Anschluss zur Verfügung stellen und einen Teil der oft ungenutzten Bandbreite abgeben.

Solche Mikro-Netzwerke werden von den Freifunkern zu größeren Netzen verbunden: durch Funkverbindungen mit Outdoor-Routern in einer Nachbarschaft, mit Richtfunk über längere Strecken zwischen Stadtteilen oder Gemeinden. Im lokalen Netz können dann auch eigene Dienste angeboten werden. Im griechischen Pendant zum Freifunk etwa, dem „Athens Wireless Metropolitan Network“, gibt es neben Angeboten für Internettelefonie oder Videostreaming auch die lokalen Suchmaschinen namens „Woogle“ und „Wahoo“.

## Was ist die Vision hinter Freifunk?

Freifunk trägt es bereits im Namen, das „freie Netz“. Was genau ist damit gemeint? „Jeder Freifunker hat eine eigene Vorstellung von Freifunk. Viele teilen dabei ähnliche Ideen, Werte und Vorstellungen – das macht uns zu einer Community.“ So beschreibt es Jürgen Neumann, einer der Pioniere des Konzepts in Berlin und Mitgründer des Fördervereins freie Netzwerke. Die meisten Freifunker dürften aber übereinstimmen, dass es mehrere Merkmale sind, die solche freien Netze ausmachen:

- Sie sind für alle zugänglich.
- Es gibt keine Zensur.
- Sie werden nicht kommerziell betrieben.
- Sie gehören der Gemeinschaft.

»

## Der Bezirk Friedrichshain-Kreuzberg kooperiert mit den Freifunkern, um den Gedanken vom freien Internetzugang mit dem öffentlichen Raum zu verbinden. Im Fokus stehen Bürgerämter, Schulen und perspektivisch alle öffentlichen Räume.

Jana Borkamp, Bezirksstadträtin für Finanzen, Kultur und Weiterbildung in Berlin Friedrichshain-Kreuzberg

«

Solche gemeinschaftlich genutzten Ressourcen sind auch als Allmende oder *commons* bekannt: Sie sind weder in privater noch in staatlicher Hand; die Gemeinschaft stellt Regeln auf, um sie zu erhalten. So wie etwa Meere oder ein Dorfteich gemeinschaftlich genutzt werden können, machen es Freifunker mit dem Funksignal. Dabei geht es nicht unbedingt um eine politische Programmatik. Viele der Initiativen um freie Funknetze sind entstanden, weil es kein oder nur teures Internet gab, wo man es wollte. Da lag der Gedanke nahe, sich den Zugang zu teilen.

Die Idee des Teilens verbindet freie Funknetze mit weiteren Konzepten, die im Internet verbreitet sind – oft ohne dass man es unbedingt merkt. Bei freier Software etwa kann jeder Interessierte die Funktionsweise eines Programms untersuchen und sie verändern; freie Inhalte wie die Wikipedia kann jeder bearbeiten oder weiterverwenden. All diese Modelle – so die etwa vom US-Rechtsprofessor Eben Moglen formulierte Idee – sind miteinander verknüpft und tragen zu einer Kommunikations-Infrastruktur bei, die unabhängig und für alle zugänglich sein soll.

Vernetzung ist für viele Freifunker nicht nur eine technische, sondern ebenso eine soziale Idee – wenn etwa Bewohner eines Hauses oder einer Nachbarschaft sich zusammentun, um gemeinsam ein neues Netz einzurichten. Weil viele Freifunker zudem das Experimentieren und Lernen mit der Technik antreibt, können freie Funknetze auch an den Gedanken der (Medien-)Bildung anknüpfen.

### Wer betreibt Freifunk?

Letztlich werden freie Funknetze von allen Bürgern betrieben, die einen Teil dazu beitragen. In Deutschland haben sich aus den anfänglich lose verbundenen Tüftlern oftmals stadtweite oder regionale Vereine gebildet. Nicht jeder, der einen Router für Freifunk in sein Fenster stellt, muss aber Vereinsmitglied sein; es gibt keine zentrale Verwaltung oder Registrierung. So haben die Berliner Freifunker den Förderverein freie Netzwerke gegründet, der als Ansprechpartner auftreten kann und Veranstaltungen und Treffen organisiert. Drumherum gibt es eine deutlich größere Aktiven-Community.

## FREIFUNK: DAS MODELL IN ARNSBERG

Als eine der ersten Kommunen in Nordrhein-Westfalen hat die Stadt Arnsberg ein öffentliches WLAN-Netz eingerichtet, das seit Sommer 2014 freien Internetzugang für Bürger und Besucher der Altstadt bietet. Die Stadt hatte zunächst Angebote privatwirtschaftlicher Telekommunikationsunternehmen im Blick, die sich laut Bürgermeister Hans-Josef Vogel jedoch als nicht finanzierbar erwiesen. In Werkstattgesprächen über die weitere Entwicklung der Altstadt kam dann die Idee auf, an das Freifunk-Modell eines Bürgernetzes anzuknüpfen.

Die Besonderheit des in Arnsberg praktizierten Modells liegt in der koordinierten Zusammenarbeit der verschiedenen Beteiligten, die das Vorhaben eines Bürgernetzes gemeinsam angeschoben und realisiert haben:



- Stadt und Bürgermeister unterstützten das Vorhaben unter anderem, indem sie Ziele für eine erste Ausbaustufe festlegten und Kooperationspartner suchten. Ein Bürgernetz wurde auch Teil der Strategie „digitales Arnsberg“ des Bürgermeisters. Die Stadtverwaltung stellte zudem einen Teil ihrer IT-Infrastruktur und städtische Gebäude wie das Rathausdach zur Funkübertragung bereit.
- Der **Verkehrsverein** der Stadt sorgte für den Anschub, indem er die Kosten für die ersten Router als Grundbaustein des Netzes übernahm; sie betragen rund 2500 Euro. Bürger und Geschäftsleute gewannen der Verkehrsverein als Unterstützer. Um Touristen und Passanten auf das Netz hinzuweisen, wurden Schilder und Aufkleber entworfen. Für die weitere Kostendeckung gewann der Verkehrsverein erste Sponsoren wie die regionale Sparkasse.
- Aktive des **Freifunk-Vereins Rheinland** brachten technische Expertise ein, etwa bei der Anbindung ans Internet und der benötigten Software. Ortsgruppen aus Arnsberg und den Gemeinden Brilon und Soest gründeten dafür die Freifunk-Domäne Möhne.
- **Bürger** in der Altstadt und **Geschäftsleute** auf der lokalen Einkaufsmeile haben bislang rund 70 Router aufgestellt, im weiteren Umkreis sind es insgesamt etwa 100. Ihr Engagement beim Aufbau und der Unterhaltung des Netzes bildet sein eigentliches Rückgrat.

Rechtlich betrachtet, können die Vereine aber auch als Internetanbieter auftreten, für die im Unterschied zu Privatpersonen zum Teil günstigere rechtliche Voraussetzungen bestehen. Das ist in Berlin der Fall, wo der Verein den Datentransport zugleich so organisiert, dass für die einzelnen Beteiligten das Risiko minimiert wird, sich rechtliche Komplikationen einzuhandeln (siehe S. 32).

### Warum ist Freifunk wichtig?

Bei Freifunk-Netzen entsteht eine besondere Art von Netzen: Mesh-Netze – auch „vermaschte Netze“ genannt – basieren darauf, dass alle Teilnehmer untereinander Daten weiterreichen und es keine Zentrale gibt (siehe S. 20). Mesh-Netze sind nicht auf Funknetze beschränkt, auch Kabelnetze, reine Mobiltelefon-Netze oder Mischformen sind möglich. Mehrere Aspekte machen sie interessant:

- **Digitale Spaltung**

Auch wenn sich beim Zugang zum Internet in den letzten Jahren viel bewegt hat, ist das Problem nicht verschwunden: Nach wie vor sind einige Regionen in Deutschland kaum oder nur schlecht an das Internet angebunden – besonders dort, wo es rein privatwirtschaftlichen Anbietern nicht rentabel erscheint. „Neue Versuche, die digitale Spaltung zu überwinden, werden alternative Modelle des Besitzes, der Technologie, der Wirtschaftsentwicklung und der sozialen Inklusion prüfen müssen“, hält ein Bericht der New America Foundation fest.

- **Öffentliche Netze und neue Übertragungswege**

Für Kommunen kann Freifunk eine Option sein, städtische WLAN-Netze aufzubauen, indem sie an bestehende bürgerschaftliche Strukturen anknüpfen. So hat der Freifunk-Verein Rheinland zusammen mit dem Verkehrsverein der Stadt Arnsberg eine erste städtische Freifunk-Zone mit rund 70 Routern aufgebaut. Auch aus der Internetwirtschaft wird das Funknetz-Konzept beobachtet. So hat sich der Branchenverband Eco bereits dafür interessiert, zu untersuchen, ob der beim Freifunk eingesetzte Richtfunk als Alternative zu DSL-Leitungen auf der „letzten Meile“ zum Endkunden dienen kann; daneben könnten Mesh-Netze etwa für Internetprovider ohne Mobilfunklizenzen interessant sein.

»

**Neukölln ist mit seinen über 320.000 Einwohnern einer der spannendsten und buntesten Bezirke Berlins und wir Neuköllner sind stolz darauf. Umso wichtiger ist es, im Zeitalter des Internets rund um das Rathaus einen kostenlosen Internetzugang zu bieten. Mit der Einbindung des Neuköllner Rathausturmes im Frühjahr 2014 wurde das Angebot freier Netzwerke wieder um ein Stück erweitert.**

Heinz Buschkowsky, Bezirksbürgermeister Berlin-Neukölln

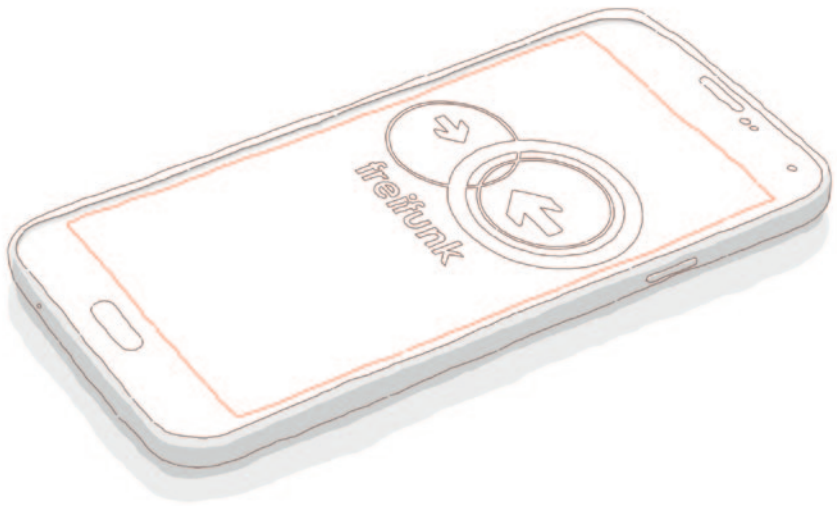
«

- **Dezentral hält besser**

Damit ein Mesh-Netz komplett ausfällt, müsste jedes einzelne seiner Teile ausfallen, was sehr unwahrscheinlich ist. Mesh-Netze werden daher auch unter dem Stichwort der Resilienz (etwa: Widerstandsfähigkeit) diskutiert. Das Konzept wurde bereits seit den 1980er-Jahren von Militärs erforscht. In den letzten Jahren wird es unter neuer Perspektive wieder verstärkt aufgegriffen. So untersucht das EU-geförderte Forschungsprojekt „Confine“, welche Rolle die Bürger-netze im Internet der Zukunft spielen können.

Anlässe für dieses neuerliche Interesse sind etwa die Versuche in autoritären Staaten, das Internet komplett abzuschalten, um den Informationsaustausch zu verhindern. Der als „Vater des World Wide Web“ bekannte Entwickler Tim Berners-Lee forderte zuletzt wiederum, das Internet als Antwort auf die von Edward Snowdens Enthüllungen ausgelöste Überwachungs- und Spionageaffäre erneut zu „dezentralisieren“.

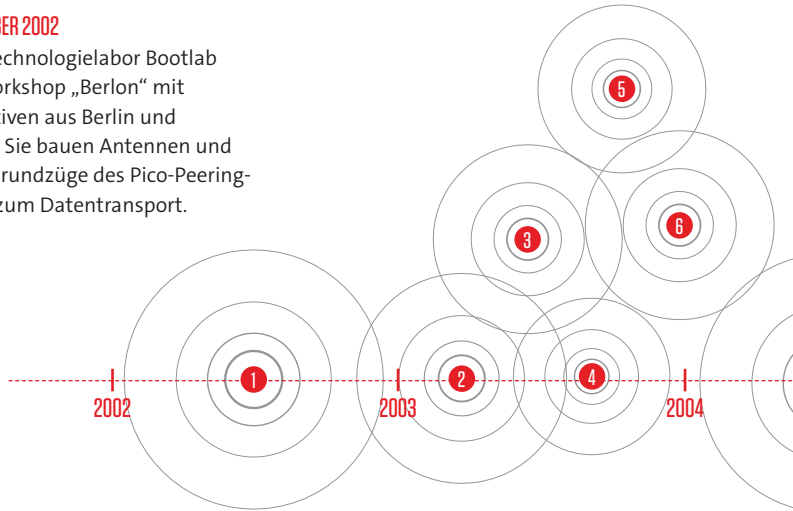
Ein weiteres Einsatzfeld sind Mesh-Netze im Katastrophenfall, besonders nach Naturkatastrophen. So nutzten etwa nach dem Hurrikan Sandy Bürger im Brooklyn Viertel Red Hook ein solches, bereits vorhandenes und weiter funktionsfähiges Netz. Es wurde um einen Dienst erweitert, über den Bewohner Schäden melden und lokale Informationen austauschen konnten. Zusammen mit der Katastrophenschutzbehörde wurde das lokale Netz provisorisch per Satellit ans Internet angebunden. Der dort eingesetzte technische Werkzeugkasten des „Commotion Wireless Project“ teilt viele Komponenten mit dem deutschen Freifunk.



# Stationen 2002–2014

## 1 12./13. OKTOBER 2002

Im Berliner Technologielaor Bootlab findet der Workshop „Berlon“ mit Funknetz-Aktiven aus Berlin und London statt. Sie bauen Antennen und diskutieren Grundzüge des Pico-Peering-Agreements zum Datentransport.



## 2 1./2. MÄRZ 2003

Auf einer Konferenz in Kopenhagen einigen sich die Teilnehmer verschiedener Länder auf das Pico-Peering-Agreement. Für den Datentransport in und zwischen freien Funknetzen gibt es nun einen kurzen, gemeinsamen Regelkatalog.

## 3 25. JULI 2003

Es gelten neue EU-Richtlinien für elektronische Kommunikationsnetze. Freifunker können sich durch die Vorgaben unter anderem sicherer sein, dass ihre Funknetze über Grundstücksgrenzen hinweg nicht unter Lizenzpflichten fallen.

## 4 10. SEPTEMBER 2003

Im Berliner Hackertreff C-Base gründet sich der Förderverein freie Netzwerke.

## 5 12.-14. SEPTEMBER 2003

Auf dem ersten Treffen des neuen Freifunk-Vereins erproben die Teilnehmer den dezentralen Datentransport. Zur Einstimmung nutzen sie auch Skat-Spielkarten, auf denen Nachrichten befestigt sind. Die Karten werden so lange ungelesen in der Runde weitergereicht, bis sie den Empfänger erreichen.

## 6 13. OKTOBER 2003

Mitarbeiter der französischen Forschungseinrichtung INRIA reichen einen Entwurf für das Routing-Protokoll OLSR bei der „Internet Engineering Task Force“ ein, dem für technische Standards zuständigen Internetgremium. Eine Weiterentwicklung nutzen später die Freifunker.

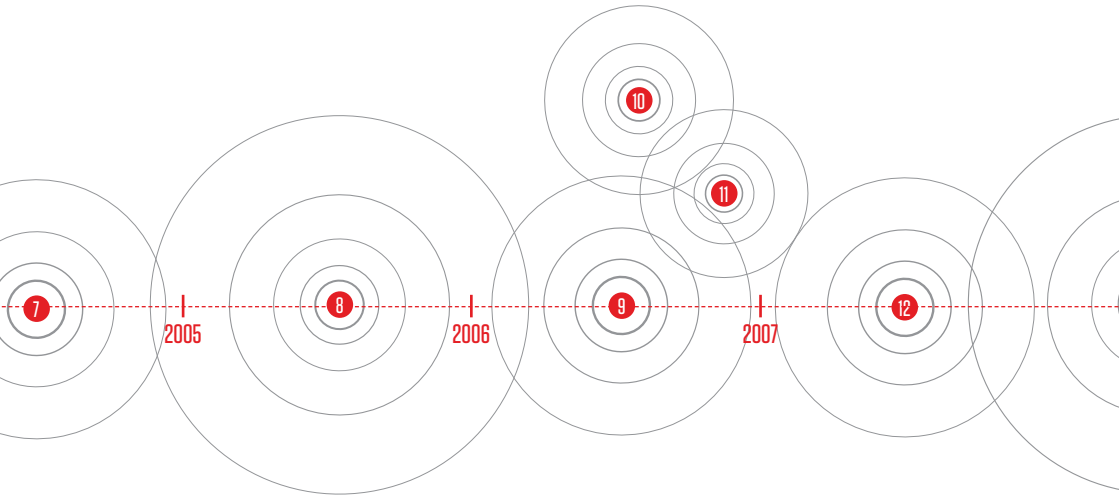


**7 5. JUNI 2004**

Berliner Freifunker testen auf der Konferenz „Wizards of OS 3“ in einem Feldversuch den Datentransport über das OLSR-Protokoll. Er erweist sich als langsamer als gedacht und bricht wiederholt ab, also verbessern sie es weiter.

**8 25. OKTOBER 2005**

Der erste Kirchturm in Berlin wird Teil des Freifunk-Netzes. Auf der Friedrichshainer Samariterkirche wird nun dafür eine Antenne installiert.

**9 13. APRIL 2006**

Forschern gelingt es in den venezolanischen Anden, eine 280 Kilometer lange Funkverbindung aufzubauen. Sie nutzen zwei normale WLAN-Router mit zusätzlichen Parabolantennen und übertragen PDF-Dokumente zwischen ihren Computern.

**10 24. JUNI 2006**

Ein lokales Funknetz im Dorf Gadov in der Prignitz ist nun ans Breitband-Internet angebunden. „Wir haben uns einen Satelliten angemietet“, berichtet ein Freifunker.

**11 22. OKTOBER 2006**

Im indischen Dharamsala beginnt der „World Summit for Free Information Infrastructures“, das erste internationale Treffen von Funknetz-Aktiven aus Europa, Israel, Nordamerika, Indien und Australien.

**12 15. OKTOBER 2007**

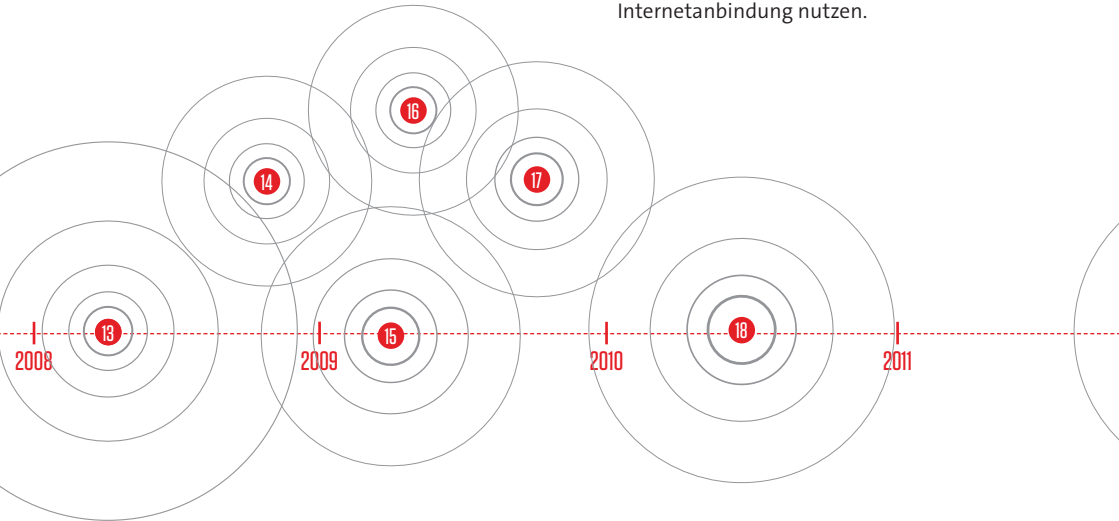
Das Projekt „Berlin Backyard Radio“ startet mit technischer Unterstützung der Freifunker. Über einen kleinen Sender am WLAN-Router kann jeder Interessierte eine Mikro-Radiostation mit einigen Metern Reichweite eröffnen.

**13 7. APRIL 2008**

Die Entwickler um Freifunk veröffentlichen einen Entwurf des BATMAN-Protokolls, das den Datentransport besser zu organisieren verspricht.

**16 24. MAI 2009**

Schulen in Afghanistan nutzen Mesh-Netze und Freifunk-Technik, um mehrere Klassenzimmer zu verbinden, berichtet der Freifunker Mario Behling, der dort Entwicklungsarbeit leistete. So können Schulen etwa die Wikipedia auch ohne Internetanbindung nutzen.



**14 24. APRIL 2008:**

Auf dem „Open Tech Summit“ in Taipeh treffen Freifunker auf Programmierer und Hardware-Macher aus aller Welt und tauschen sich über neue Entwicklungen aus.

**15 11. APRIL 2009**

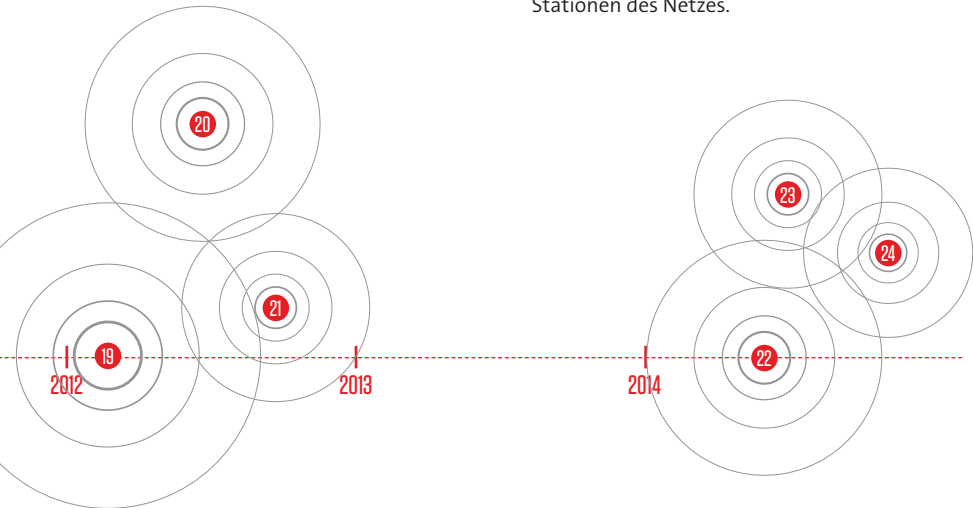
Wie leistungsfähig der Datentransport in Funknetzen sein kann, wird auf dem ersten „Wireless Battle Mesh“ in Paris ermittelt. Der Wettbewerb für verschiedene Routing-Protokolle findet ab nun regelmäßig in Europa statt.

**17 11. JUNI 2009**

Der Entwickler David Rowe dokumentiert den ersten Anruf mit einer „Mesh Potato“, einem Router mit analogem Telefonanschluss. Über Mesh-Netze und mit Rückgriff auf Freifunk-Entwicklungen sollen sie es ermöglichen, auch ohne Telefonnetz zu telefonieren, etwa in Entwicklungsländern.

**18 12. MAI 2010**

Der Bundesgerichtshof fällt das erste höchstrichterliche Urteil zur Störerhaftung eines WLAN-Betreibers. Für die Betreiber offener Netze wird die Rechtslage ungünstiger, da das Urteil unter anderem nahelegt, einen WLAN-Zugang zu verschlüsseln, damit Unbekannte keine Urheberrechte darüber verletzen können.



### 19 14. JUNI 2012

Die Berliner Freifunker beginnen im Rahmen einer Kampagne damit, rund 100 Router („Freedom Fighter Box“) für den Zugang zum Freifunk zu verschenken. Damit wenden sie sich gegen die Rechtsprechung zur Störerhaftung und für anonyme Netznutzung.

### 20 20. OKTOBER 2012

Die mabb fördert den Ausbau des Berliner Freifunk-Netztes. Standorte im bezirksübergreifenden Backbone-Netz können somit modernisiert oder neu erschlossen werden.

### 21 23. NOVEMBER 2012

Auf dem Dach des Rathauses Kreuzberg geht eine weitere Freifunk-Installation in Betrieb. Sechs Router mit Richtantennen verbinden es mit weiteren Backbone-Stationen des Netztes.

### 22 6. APRIL 2014

Der Berliner Internetknoten BCIX begrüßt die Freifunker als neuen Teilnehmer. Das Netz kann dort auch per Glasfaser mit dem Internet verbunden werden. An solchen Internetknoten tauschen die vielen einzelnen Netzwerke des Internets Daten aus.

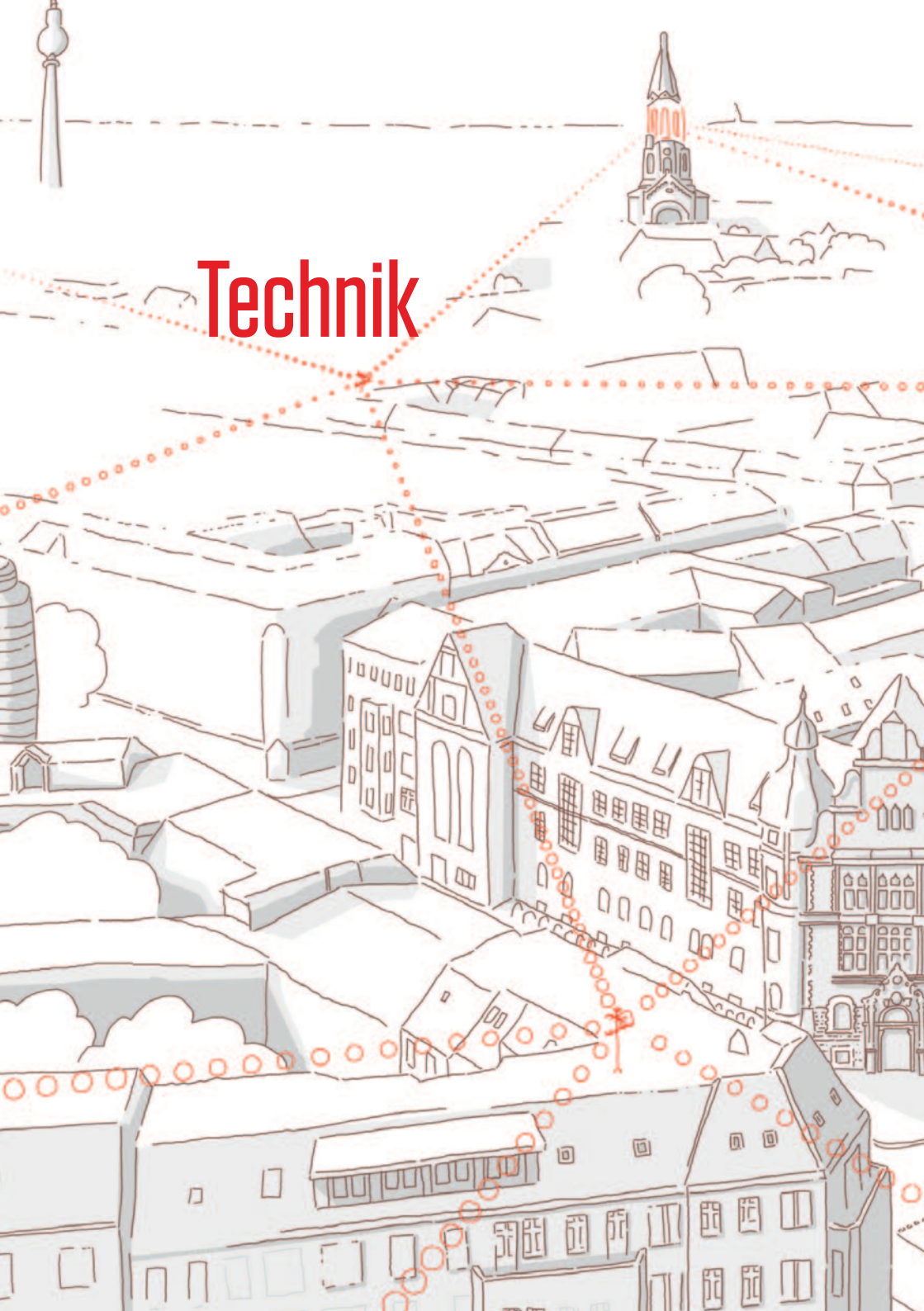
### 23 25. APRIL 2014

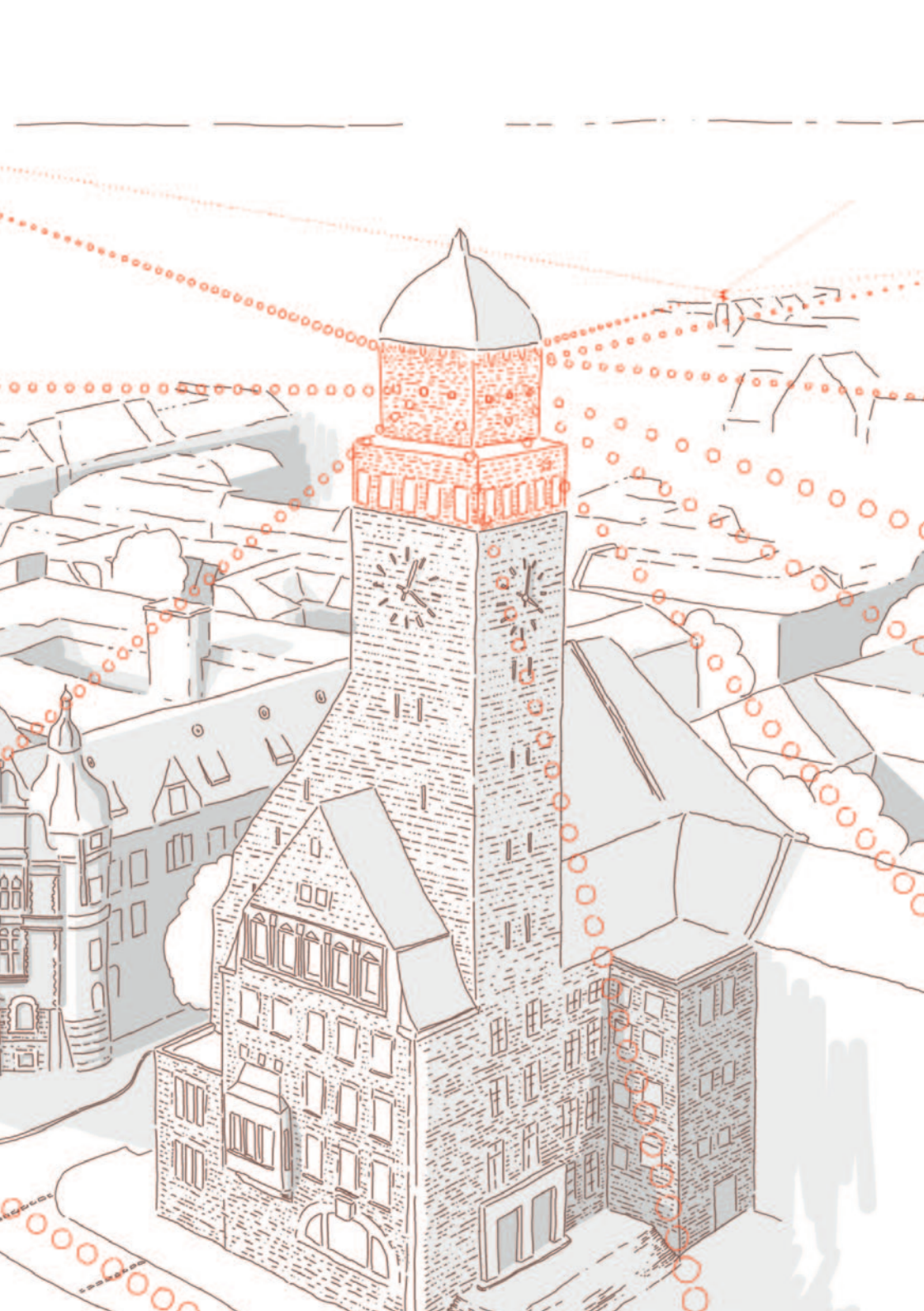
Ein zweites Berliner Rathaus, das Neuköllner, geht ans Netz und dient als Knotenpunkt für den Daten-Funkverkehr zwischen Tempelhof, Friedrichshain und Kreuzberg.

### 24 24. JULI 2014

Der Berliner Radiosender Flux FM ist nun auch über das Freifunk-Netz als Livestream zu empfangen.

# Technik





## TECHNIK

# Mesh-Netze am Beispiel Berlin

*Freifunker in Berlin gehörten zu den Pionieren des dezentralen Datentransports. Die Technologie entwickelten sie in weiten Teilen selbst.*

Die Idee, freie Netze in Bürgerhand aufzubauen, lag an vielen Orten gleichzeitig in der Luft, doch zu den Keimzellen gehörte eine WLAN-Funkstrecke, die seit dem Frühjahr 2002 zwei Häuser im Bezirk Friedrichshain verband. In der Rigaer Straße 83 im Norden gab es bereits Breitband. Über selbst gebastelte Dachantennen leiteten die Bewohner das Signal in den Süden weiter. Am anderen Ende, am Boxhagener Platz, betrieben einige Computerfreunde das alternative Internet-café „Lotec“.

Dort war in den Neunzigerjahren Glasfaser verlegt worden. Sie bot theoretisch hohe Übertragungsraten, damals aber nur ISDN-Geschwindigkeit, während anderswo DSL-Technik über Kupferkabel Einzug hielt. Kommerzielle Anbieter zogen erste ISDN-Flatrates wieder zurück, da sie ihrerseits hohe Minutenpreise an die Telekom zahlten. Als „Lotec“ die Flatrate gekündigt wurde, schuf die Funkstrecke ins „Tal der Breitbandlosen“ Abhilfe.

Das Projekt „Wlanhain“ des Informatikers Ulf Kypke-Burchardi versorgte so Haushalte im Friedrichshainer Süden per Funk mit Breitband aus dem Norden. Im Oktober 2002 trafen sich Interessierte aus Berlin und London zu einem Workshop, auf dem die Freifunk-Idee Gestalt annahm, ebenso das „Pico-Peering-Agreement“ über die Prinzipien des Datenverkehrs (siehe S. 40) in diesen Bürgernetzen. Regelmäßige Treffen im Berliner Hackertreff C-Base folgten; 2003 gründete sich der Förderverein Freie Netzwerke.

## „Peer-to-Peer“: Datenaustausch unter Gleichen

Freifunk basiert auf dem Modell der Kommunikation unter Gleichgestellten (*peers*), der Ansatz wird auch als „Peer-to-Peer“-Netz bezeichnet. Für dieses Modell gibt es viele Gründe, etwa geringere Kosten beim Netzaufbau. Die meisten WLAN-Netze dagegen arbeiten im sogenannten Infrastruktur-Modus, der auf einem hierarchisch aufgebauten Netz basiert. Bekannt ist das Prinzip vom Mobilfunk: Ohne die Basisstation eines Anbieters kann man nicht telefonieren. Technisch gesprochen ist die Basisstation ein „Master“ (Herr), die Teilnehmer sind „Clients“ (Klienten). Geht man von einem Netz von drei Teilnehmern aus, so können die Clients (A und C) nur mit dem Master (B) reden, nicht aber untereinander.

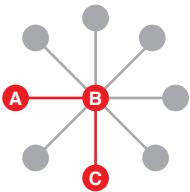


Abbildung 1:  
Zentralisiertes Netz

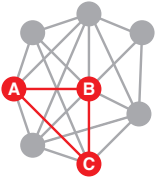


Abbildung 2:  
Peer-to-Peer-Verkehr  
im Mesh-Netz

Das zentralisierte Modell erlaubt Kontrolle und vereinfacht die Koordination, ist aber für ein freies Netz ineffizient. Es ist sinnvoll, wenn alle Teilnehmer stets mit dem Master kommunizieren, weil er eine interessante Dienstleistung anbietet. Für den Datenaustausch zwischen den Teilnehmern ist es weniger geeignet.

### Aus gegenseitigem Weiterleiten entsteht ein Mesh-Netz

Im Peer-to-Peer-Modus dagegen können alle Teilnehmer direkt miteinander kommunizieren, solange sie in Funkreichweite sind. Unter Ingenieuren heißt das „Ad-hoc-Netz“. Der Ansatz ist elegant und effizient, aber schwieriger umzusetzen. Ein Mesh-Netz ist ein dezentrales Peer-to-Peer-Netz, in dem alle Knoten sich gegenseitig beim Weiterleiten (Routing) der Daten helfen. Fällt eine Station aus, gibt es alternative Wege; das Netz kann sich selbst heilen. Kommen neue Knoten hinzu, werden sie automatisch eingebunden und erweitern es.

### Das Berliner Backbone-Netz

Backbone-Verbindungen sind die breiten Autobahnen im Netz, meist über Glasfaserleitungen. Für die Freifunker lag es zunächst nahe, dedizierte Funkstrecken zu verwenden. Dafür sind hohe, frei stehende Standorte mit Sichtverbindung und leistungsfähige WLAN-Geräte im 5-GHz-Band erforderlich; jede Endstelle einer solchen Punkt-zu-Punkt-Verbindung braucht eine eigene WLAN-Schnittstelle, Kabel und Antennen. Heute gibt es fertige, wasserdichte WLAN-Router mit integrierter Antenne im Handel.

## ROUTING: SO KOMMEN DIE DATEN AN IHR ZIEL

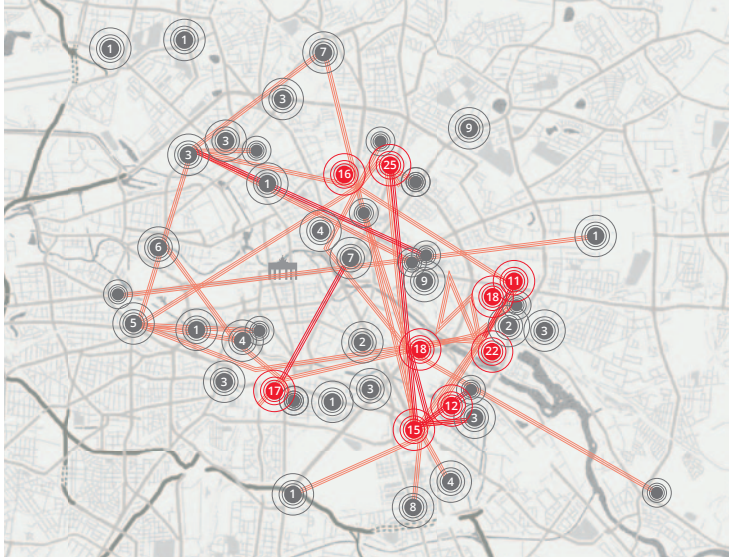
Woher weiß ein Datenpaket, welchen Weg es nehmen muss? Da sich der Aufbau eines Freifunk-Netzes ständig ändern kann, wird ein spezielles, sogenanntes Routing-Protokoll benötigt. Es regelt, welcher Teilnehmer wann für wen Daten weiterleitet.

Bei Freifunk kommen im Wesentlichen zwei solcher Protokolle zum Einsatz: **OLSR** (Optimized Link State Routing) verfolgt den Ansatz, alle Wege permanent vorauszuberechnen. Jeder Teilnehmer sendet ein kurzes Signal, um Nachbarn mit Funkkontakt zu identifizieren, und verbreitet diese Information weiter. Dies wird für alle Knoten wiederholt, bis die vollständige Netztopologie bekannt ist. Jeder Knoten besitzt eine Daten-

bank aller Wege und berechnet die kürzesten Routen, wodurch der Rechenaufwand hoch sein kann.

Eine Eigenentwicklung der Freifunker ist das Protokoll **BATMAN** (Better Approach To Mobile Ad-Hoc Networking). Die Grundidee ist, dass nicht jeder Knoten eine Datenbank aller Wege benötigt. Das BATMAN-Protokoll ermittelt nur Nachbarn, welche anderen Knoten sich im Netz befinden und an wen ein Datenpaket weitergereicht werden muss. Jeder Knoten benötigt daher nur Wegweiser. BATMAN ist heute zum Oberbegriff einer ganzen Klasse von Routing-Protokollen geworden. Sie alle teilen das Wissen über das Netz unter den Knoten auf.

Backbone-Netz des Berliner Freifunks im Oktober 2014 – je mehr Netzknoten vorhanden sind, desto besser ist die Abdeckung mit WLAN



Ein zentraler Router mit von den Freifunkern entwickelter Software verwaltet den Standort und organisiert den Datenverkehr im Backbone-Netz. Da jede einzelne Verbindung zwischen Standorten ein eigenes WLAN-Gerät benötigt und weitere Geräte den Zugang lokal verteilen, sind pro Standort schnell ein Dutzend WLAN-Router nötig. Durch die Förderung der mabb konnten die Berliner Freifunker mehrere Standorte modernisieren, etwa die Samariterkirche in Friedrichshain, die Emmauskirche in Kreuzberg und die Segenskirche im Prenzlauer Berg. Neue Standorte wie die Rathäuser in Neukölln und Kreuzberg wurden erschlossen.

Allerdings kommen nur noch wenige Gebäude infrage; viele werden bereits von Mobilfunkanbietern genutzt. Mit der Mitgliedschaft des Freifunks im Internetknoten BCIX ergibt sich jedoch die Möglichkeit, Datenverkehr innerhalb Berlins nun auch über die Glasfaser der BCIX-Partner zu leiten.

»

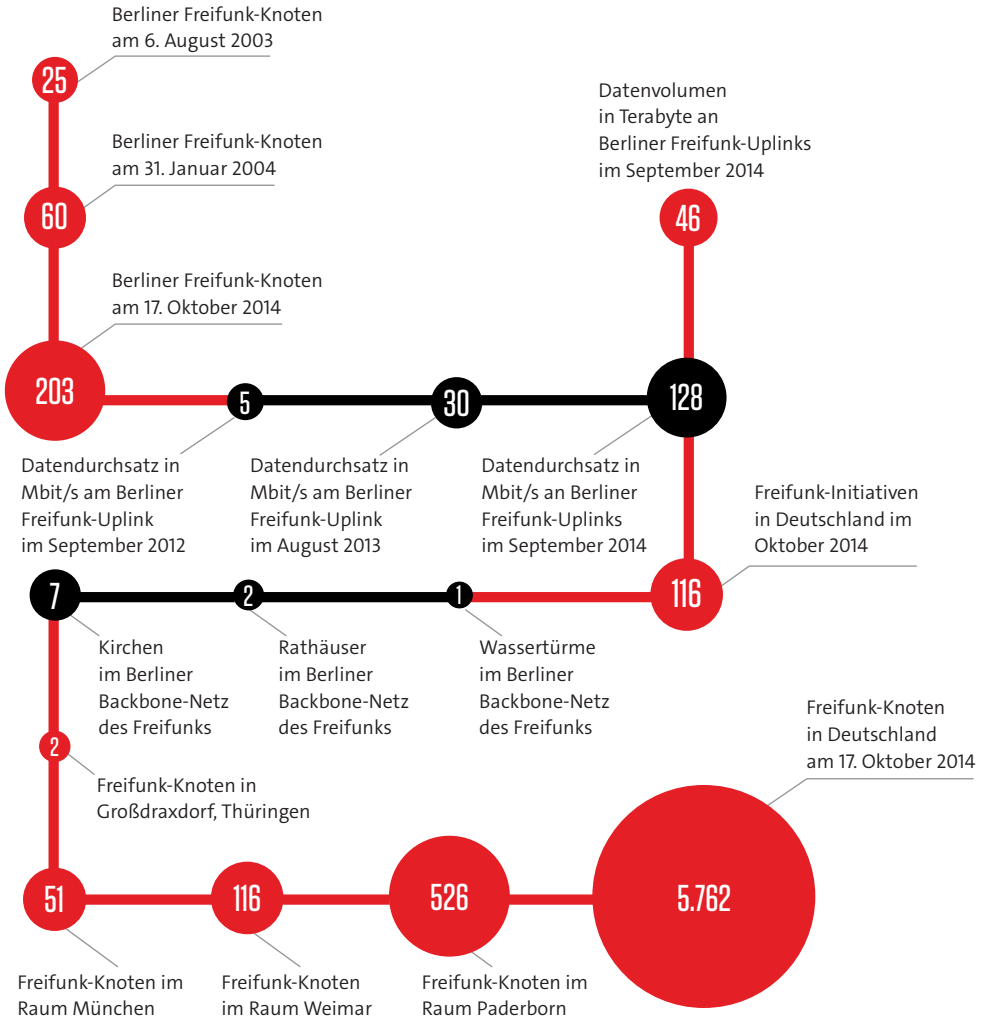
**Die Idee des Freifunks bringt die Stadt voran und steht für ein demokratisches Internet. Als neuem Peering-Partner zum Datenaustausch am BCIX steht Freifunk nun mehr Bandbreite zur Verfügung.**

Peter Lampe, Vorstandsvorsitzender des Berliner Internetknotens BCIX

«



# Freifunk in Zahlen



## SICHERHEIT

# WLAN FÜR ALLE – aber sicher?

*Ein offenes Funknetz gibt vielen Menschen Zugang zum Internet, doch wie steht es um die Sicherheit? Die Risiken sind beherrschbar, wenn Nutzer und Betreiber übliche Vorsichtsmaßnahmen treffen.*

Dass öffentliche Funknetze im Prinzip verwundbar sind, zeigte der amerikanische Entwickler Eric Butler im Jahr 2010. Er entwickelte das Programm „Firesheep“, das automatisch den Datenstrom anderer Nutzer eines solchen Funknetzes abhören konnte. Hunderttausende luden das Programm herunter; auch um die Sicherheit bei sich selbst zu überprüfen. Mit dem Programm ließen sich die Benutzerkonten von Diensten wie Twitter, Facebook und Amazon übernehmen, die Webdienste mussten eilig nachbessern.

## Verschlüsselung bei Webdiensten keine Ausnahme mehr

Die gute Nachricht: Im Zeitalter nach Edward Snowden sind viele Angriffe nicht mehr so einfach wie vor ein paar Jahren. Viele Anbieter haben Verschlüsselung in ihr Standard-Repertoire übernommen. Trotzdem müssen sowohl Betreiber als auch Nutzer eines offenen Netzes Vorsichtsmaßnahmen treffen, um ihre Sicherheit zu gewährleisten. Das fängt bei den üblichen Sicherheitsmaßnahmen an, die auch für jeden anderen Internetanschluss zu Hause gelten: Die neuesten Sicherheitsaktualisierungen sollten ständig installiert werden, besonders auf Windows-Computern empfiehlt sich der Einsatz von Antiviren-Programmen; man sollte Rechner und Benutzerkonten mit guten Passwörtern schützen.

In einem offenen Funknetz entfällt jedoch eine Vorsichtsmaßnahme, die jedem Nutzer zu Hause sonst empfohlen wird: Das Einschalten der WLAN-Verschlüsselung, die die Funkverbindung mit einem Passwort absichert und damit für Außenstehende unlesbar macht. Es liegt in der Idee eines offenen Netzes, dass die WLAN-Gastgeber auf ein solches Passwort verzichten.

Google, Amazon und sogar Wikipedia verschlüsseln heute ihren Datenverkehr komplett und schließen damit zufällige Daten-Schnüffler weitgehend aus. Andere Anbieter verschlüsseln lediglich kritische Daten wie Passwörter und Kreditkarteninformationen. Browser wie Chrome und Firefox zeigen mit einem kleinen Schloss-Symbol in der Adressleiste an, wenn eine Webseite verschlüsselt ist. Fehlt das Schloss, kann die Kommunikation im Prinzip mitgelesen werden, wenn keine anderen Vorsichtsmaßnahmen getroffen werden. Der Datenstrom enthält Informationen wie aufgerufene Webseiten, übertragene Bilder, gegebenenfalls auch ganze E-Mails.

### VPN: Der Tunnel im Netz – auch für mehr Sicherheit

Auch verschlüsselte Webseiten geben mitunter Daten Preis. Hacker sind einfallreich: Statt Usernamen und Passwort direkt abzugreifen, können sie zum Beispiel versuchen, die Cookies zu übernehmen, kleine Dateien, mit denen ein Browser sich gegenüber einem Anbieter automatisch ausweisen kann. Auch so kann ein Angreifer an einen fremden Account gelangen.

Ein Mittel, um solche Lauscher auszuschließen, ist der Aufbau einer weiteren Verschlüsselungs-Schicht. Sogenannte „Virtual Private Networks“ – kurz: VPN – bauen einen verschlüsselten Tunnel auf, durch den der komplette Datenstrom fließt. Solche VPN-Tunnel sind in freien Funknetzen vielfältig einsetzbar. So können die Endnutzer eine verschlüsselte Verbindung nach Hause, in ihr Firmennetzwerk oder zu einem kommerziellen VPN-Anbieter aufbauen und sind so auch ohne WLAN-Verschlüsselung vor Mitlauschern geschützt.

Viele Freifunk-Netze benutzen intern ebenfalls solche VPN-Tunnel. So werden die Daten etwa im Köln-Bonner Netz über ein dezentrales VPN geleitet. Hier dient es dem Schutz des Betreibers der Zugangspunkte. Wenn ein Freifunk-Nutzer unzulässiges Filesharing betreibt, taucht auf einer etwaigen Abmahnung dann nicht die IP-Adresse des WLAN-Gastgebers auf, sondern die des zentralen Freifunk-Zugangs. Andere freie Funknetze leiten den kompletten Datenverkehr ins Ausland, um die Unsicherheit bei der Störerhaftung (siehe S. 33) auch für den Betreiber selbst zu umgehen. Nachteil der VPN-Verlängerungen: Alle Nutzer müssen sich die Bandbreite des Datentunnels teilen. Dies kann zu längeren Ladezeiten führen, zeitkritische Anwendungen wie Internettelefonie oder Livestreams sind mitunter nicht mehr möglich.

»

**Die Gewährleistung eines Internetzugangs gehört zur Daseinsvorsorge. Mein langfristiges Ziel lautet: Wo öffentlicher Raum ist, soll auch ein öffentliches WLAN sein. Freifunk kann hierzu einen wichtigen Beitrag insbesondere dort leisten, wo erlösorientierte Modelle versagen.**

Björn Böhning, Chef der Berliner Senatskanzlei

«

### Abwägung zwischen technischer Isolierung und gemeinsamer Nutzung

Auch der lokale Aspekt eines offenen Funknetzes kann so verloren gehen. So können in einem offenen Netz relativ einfach Daten geteilt werden. Möglich sind etwa Streams eines lokalen Konzerts oder eigene Chaträume. Es ist eine Abwägungsfrage: Isoliert man die Teilnehmer voneinander, sind solche Gemeinschaftsdienste nicht möglich. In einem gemeinsamen lokalen Netz dagegen können die Teilnehmer auch eventuellen Angriffen gemeinsam ausgesetzt sein.

Ein Angreifer muss dabei nicht einmal mit Absicht handeln. Oft durchsucht Schadsoftware das lokale Netz nach weiteren Computern, die sie automatisiert infizieren kann. Teilweise geben auch Nutzer aus Versehen private Daten preis, etwa durch Netzwerkfreigaben auf der Festplatte eines veralteten, falsch konfigurierten Rechners. Solche schlecht eingerichteten Rechner sind an keinem Internetanschluss wirklich sicher.

### Router physisch sichern und aktuell halten

Wichtig für die Netzsicherheit sind auch die eingesetzten Router. In den letzten Jahren wurden Geräte vieler Hersteller als unsicher enttarnt. Wie die NSA-Affäre gezeigt hat, ist es oft einfacher, zentral massenhaft Daten abzugreifen, um anschließend die Daten Einzelner herauszusieben. Stark genutzte Router sind dankbare Ziele, da sie den Nutzer täuschen können; er sieht dann nur das, was ihn ein Angreifer sehen lässt.

Da Router als Mittler zwischen Internet und Endgerät auftreten, sind sie von beiden Seiten zu schützen. Schutz durch physische Sicherheit ist relativ einfach: WLAN-Router sollten nicht frei zugänglich sein, damit sie nicht manipuliert oder gestohlen werden können. Wenn die Geräte nicht in geschlossenen Räumen aufbewahrt werden können, empfehlen sich abschließbare Kästen für den Außen-einsatz.

Equso wichtig ist es, die Firmware der Router stets aktuell zu halten. Gerade in den letzten Jahren erwiesen sich viele kommerzielle Geräte in den Haushalten als verwundbar, die Hersteller liefern aber nur einige Zeit lang Sicherheitsaktualisierungen. Freifunk-Netze setzen auf alternative, offene Firmware. Open-Source-Software ist jedoch nicht mit Sicherheit gleichzusetzen; auch hier tauchen Verwundbarkeiten auf, durch die Angreifer Kontrolle über das Gerät erlangen können. Deshalb ist es unerlässlich, eine Firmware zu wählen, die auf absehbare Zeit weiterentwickelt wird, und sicherzustellen, dass aktuelle Updates auf allen Routern des Netzwerks installiert werden.

### Dezentralität bietet Schutz

Von konkreten Umsetzungsschwierigkeiten abgesehen, bieten freie Funknetze ein Prinzip, das im vergangenen Jahrzehnt immer weiter zurückgedrängt wurde: die Dezentralisierung. War das Internet als Netz aus vielen Netzen gestartet,

dient es heute immer mehr als bloßer Zugang zu zentralen Plattformen wie Google, Facebook oder Amazon, die damit auch zum begehrten Ziel für die Geheimdienste vieler Länder wurden.

Freie Funknetze haben das Potenzial, Keimzelle einer neuen Dezentralität im Internet zu sein. Wenn nicht mehr hinter jeder IP-Adresse ein einzelner Nutzer sitzt, wenn nicht jedes Foto zu Google hochgeladen wird, dann fällt es schwerer, allumfassende digitale Profile zu erstellen. Eine solche Dezentralität gibt es aber nicht bequem frei Haus; sie verlangt von den Teilnehmern auch, mehr Verantwortung für ihre Sicherheit zu übernehmen.

»

**Netzzugang ist ein Menschenrecht. Freie Netzwerke bieten allen Menschen neutralen Zugang offen an und entstehen, indem jede und jeder einen Teil beiträgt. Viele Privatpersonen und Institutionen wie die mabb haben das bereits erkannt und helfen beim Aufbau freier Infrastruktur. Ich wünsche mir, dass sich Politik und Verwaltung flächendeckend dazu bekennen und Gemeinschaftsnetzen Unterstützung und Mittel bereitstellen.**

Monic Meisel, Mitgründerin des Fördervereins freie Netzwerke

«



www.pavelson.it



# Recht



## RECHT

# Ein Netz voller Fallgruben?

*Meldepflichten, Frequenznutzung, Sicherheit, Datenschutz und Haftung – bei freien Funknetzen gibt es einige Rechtsfragen. Worauf es besonders ankommt, wenn das freie Funknetz juristisch im grünen Bereich arbeiten soll.*

## Darf man seinen Internetanschluss mit anderen teilen?

Zunächst sollte geklärt werden, ob der jeweilige Internetanbieter es erlaubt, den eigenen Anschluss für eine Mitnutzung durch Dritte freizugeben. Das ist gesetzlich nicht verboten, die Internetanbieter können es aber vertraglich ausschließen. Manche Anbieter erlauben eine Drittnutzung nur, wenn sie diese schriftlich genehmigt haben, so zum Beispiel derzeit die Deutsche Telekom, Unity Media, Netcologne und Congstar. Andere gestatten zwar grundsätzlich eine Mitnutzung, verbieten es dem Hauptnutzer aber, ungefragt oder überhaupt Geld dafür zu verlangen, so zum Beispiel Kabel Deutschland, Tele Columbus, Vodafone, O2, Kabel BW und Easybell. Von den bekannteren Anbietern verbietet lediglich 1&1 eine Drittnutzung außerhalb der „häuslichen Gemeinschaft“.

Da sich diese vertraglichen Bestimmungen ändern können, empfiehlt sich ein Blick in die allgemeinen Geschäftsbedingungen (AGB) des jeweiligen Anbieters. Sie sind auch auf den Webseiten der Anbieter meist leicht zu finden. Erfährt der Anbieter von einem Verstoß gegen die Bedingungen, kann er unter Umständen den Vertrag kündigen.

→ Im Zweifel sollte der Internetanbieter um Erlaubnis gefragt werden, wenn man seinen Anschluss für ein freies Funknetz zur Verfügung stellen will.

## Muss ich ein freies Netzwerk anmelden?

Wer seinen eigenen Internetanschluss über WLAN der Öffentlichkeit zur Mitnutzung anbietet, handelt rechtlich als sogenannter Access Provider, da er die technische Infrastruktur für den Internetzugang bereitstellt und Informationen aus dem Netz zum Internetnutzer durchleitet. Access Provider sind Anbieter von Telekommunikationsdiensten; für sie gelten die Bestimmungen des Telekommunikationsgesetzes (TKG), aber auch Regelungen aus dem Telemediengesetz (TMG).

Wer ein Funknetz in Betrieb nimmt, braucht keine Genehmigung. Nach den Vorgaben des TKG kann aber eine Mitteilung erforderlich sein: Wenn es sich um ein



„gewerbliches öffentliches Telekommunikationsnetz“ handelt, muss es bei der Bundesnetzagentur angemeldet werden. Ein freies Funknetz, das einer unbestimmten Nutzerzahl zur Verfügung stehen soll, ist öffentlich. Um darüber hinaus gewerblich zu sein, muss es nicht unbedingt mit der Absicht eingerichtet worden sein, einen Gewinn zu erzielen. Es genügt etwa, dass ein Entgelt von den Nutzern erhoben wird, um die Betriebskosten zu decken. Das gilt auch, wenn sich die Teilnehmer an dem freien Netzwerk zu einem Verein zusammengeschlossen haben und für die Kostendeckung von allen Mitgliedern Beiträge erhoben werden. Auch ein Cafébetreiber, der mit einem kostenlosen WLAN Kunden locken will, handelt in diesem Sinne gewerblich.

Wenn rein altruistische Motive vorliegen – also jeder Interessierte das Netz kostenfrei nutzen kann und die Betreiber für ihre eigenen Internet-Anschlüsse selbst aufkommen – ist das Netz nicht gewerblich und man muss es auch nicht anmelden. Das wird bei WLAN-Netzen in Privatwohnungen oder öffentlichen Einrichtungen wie Schulen zumeist der Fall sein. Eine andere Frage ist es, ob es weitere rechtliche Vorteile bringen kann, ein Freifunk-Netz anzumelden. So sind einige Juristen der Ansicht, dass eine Anmeldung bei eventuellen Streitfällen den einzelnen WLAN-Gastgeber begünstigt (siehe S. 33).

→ **Sobald ein Freifunk-Anbieter als gewerblich gilt, muss das Netz bei der Bundesnetzagentur angemeldet werden. Im Zweifelsfall kann eine Anmeldung weitere Vorteile bringen.**

### Welche Vorschriften zu Sicherheit und Datenschutz sind zu beachten?

Das Telekommunikationsgesetz (TKG) sieht einige technische Schutzmaßnahmen vor, die alle Anbieter von Telekommunikationsdiensten beachten müssen. Sie dienen auch dem Schutz des Fernmeldegeheimnisses und personenbezogener Daten. Bei freien Funknetzen ist dieser Aspekt dann überschaubar, wenn vom WLAN-Gastgeber keine oder kaum Nutzerdaten überhaupt erfasst werden. Da etwa der Router für gewöhnlich bestimmte Daten dennoch speichert, muss dessen Administrator-Zugang aber in jedem Fall durch ein sicheres Passwort geschützt sein. Die WLAN-Geräte selbst müssen vor unbefugtem Zugriff durch Dritte geschützt werden. Wird ein Gerät außerhalb der Wohnung platziert, sollte es daher zum Beispiel in einem abschließbaren Kasten installiert werden.

Der Datenverkehr im Funknetz selbst läuft zunächst ohne eine eigene Verschlüsselungs-Schicht. Die eigenen Daten mittels Firewall, Passwörtern und weiteren üblichen Vorkehrungen vor Fremdzugriff zu schützen, ist daher auch Aufgabe jedes einzelnen Teilnehmers und Nutzers (siehe S. 24). Das ist bei freien Funknetzen nicht anders als etwa bei einem offenen WLAN in einem Café. Für Risiken, die sich daraus ergeben können, ist der Anbieter des Zugangs nicht verantwortlich.

Wer eine für die Öffentlichkeit bestimmte Telekommunikationsanlage betreibt, muss auch bestimmte Maßnahmen treffen, um das Netzwerk vor Störungen, Angriffen und Katastrophen zu schützen. Den TKG-Vorgaben nach ist es

verpflichtend, einen Sicherheitsbeauftragten zu benennen, ein Sicherheitskonzept zu erstellen und der Bundesnetzagentur vorzulegen. Zwar sind diese Vorgaben im Fall eines einzelnen Funknetz-Betreibers nicht so streng auszulegen wie etwa bei großen Internetanbietern. Es bietet sich aber an, trotzdem ein vereinfachtes Konzept zu erarbeiten, das eine schematische Darstellung des Netzwerks sowie Angaben zu den eingesetzten Telekommunikationssystemen umfasst (zu Vorlagen siehe die weiterführenden Links auf S. 43). Wer nur als privater WLAN-Gastgeber ein einzelnes Netz einrichten will, bei dem Betreiber und Verantwortlicher identisch sind, bei dem wird es aber in der Regel weder notwendig noch sinnvoll sein, einen Sicherheitsbeauftragten zu benennen.

→ Die Router müssen vor physischen Einwirkungen und mit sicherem Passwort vor Fremdzugriff geschützt werden. Es bietet sich an, ein einfaches Sicherheitskonzept zu erstellen. Der Betreiber haftet nicht für diejenigen Risiken, die sich aus mangelnden Sicherheitsvorkehrungen der Nutzer ergeben können.

### Wie ist das rechtliche Verhältnis der Teilnehmer untereinander?

Die Teilnehmer eines freien Netzwerkes binden sich zunächst rechtlich weder untereinander noch im Verhältnis zu den Nutzern. Daran ändert sich auch dann nicht viel, wenn sich die Freifunker darauf einigen, mit dem „Pico-Peering Agreement“ ihre Zusagen näher zu konkretisieren. Mit dieser Vereinbarung bestätigen die Teilnehmer, dass sie freien Datentransit über ihr Netz anbieten wollen und dass sie die durchlaufenden Daten weder störend beeinträchtigen noch verändern (siehe S. 40). Daraus folgen aber nur wenige Verpflichtungen. Die Vereinbarung stellt im Gegenteil klar, dass gerade kein Betrieb oder bestimmter Service garantiert wird. Das kann dann anders sein, wenn sich die Freifunker in einem Verein organisiert haben. Dann gelten die Rechte und Pflichten, die sich aus dem Vereinsstatut ergeben.

→ Für die bloßen Betreiber eines freien Funknetzwerks folgen daraus keine Verpflichtungen, einen Dienst oder Internetzugang bereitzustellen, für Mitnutzer besteht somit auch kein Anrecht auf einen WLAN-Service.

### Sind die Betreiber für unrechtmäßiges Verhalten der Nutzer verantwortlich?

Wer lediglich als Nutzer über ein freies Funknetz im Internet surft, der muss sich wie gewöhnlich an Recht und Gesetz halten, darf also zum Beispiel niemanden beleidigen oder Musikdateien illegal anbieten. Hier ergeben sich insoweit keine Besonderheiten. Was folgt aber für die Betreiber, wenn ein Nutzer doch einmal eine Rechtsverletzung begangen hat? Solange es um strafrechtliche Verantwortlichkeit geht, lautet die kurze Antwort: nicht viel. Hier ist nur der Täter selbst verantwortlich.

Anders sieht es mit möglichen zivilrechtlichen Ansprüchen aus. Hier kann der Betreiber für das Verhalten eines Nutzers haften. Um Schadensersatz wird es dabei selten gehen; dafür müsste der WLAN-Betreiber selbst Täter oder Teilnehmer der Rechtsverletzung sein. Wenn ein Nutzer die Verletzung selbst begangen hat

und dabei das WLAN eines Freifunkers nur zum Durchleiten der Daten gebrauchte, besteht an diesem Punkt für den Betreiber kein Risiko.

Das gilt aber der derzeitigen Rechtsprechung nach nicht für mögliche Ansprüche auf Unterlassung. Hier kommt die sogenannte Störerhaftung ins Spiel. Ein Störer ist, vereinfacht gesagt, jemand, der selbst nicht Täter ist, aber mit seinem Handeln dazu beiträgt, dass Rechtsverletzungen geschehen. Wer als Störer für eine Rechtsverletzung mitverantwortlich gemacht wird, haftet dann auf Unterlassung. Das bedeutet, dass der Verletzte von ihm verlangen kann, eine andauernde Rechtsverletzung zu beseitigen und zu erklären, dass sich diese nicht wiederholen wird.

→ Grundsätzlich ist der Täter für Rechtsverletzungen verantwortlich. Wer ein freies Funknetz anbietet, haftet nicht auf Schadensersatz bei fremden Rechtsverletzungen. Möglich sind aber Unterlassungsansprüche aufgrund der Rechtsprechung zur Störerhaftung.

### Welche Folgen hat die Störerhaftung und was kann ein Funknetz-Betreiber tun, um sich abzusichern?

Grundsätzlich ist eine Störerhaftung bei verschiedenen Rechtsverletzungen möglich, praktisch relevant ist sie vor allem bei Abmahnungen für unerlaubtes Filesharing, die in großem Maßstab verschickt werden. Auf den Störer können dann Kosten zukommen, denn die Anwaltskosten kann der Verletzte vom Störer zurückverlangen. Für Urheberrechts-Abmahnungen gilt seit September 2013, dass die Anwaltskosten für den Abgemahnten in einfachen und erstmaligen Fällen maximal 147,56 Euro betragen dürfen. In der Praxis wird diese Regelung unterschiedlich ausgelegt; es werden auch weiterhin höhere Kosten verlangt, die sich immer nach dem angenommenen Streitwert richten.

Weil über die Störerhaftung potenziell sehr viele Personen als verantwortlich in Betracht kommen, hat die Rechtsprechung zusätzliche Pflichten als Kriterium eingeführt. Nur wer als WLAN-Gastgeber auch zumutbare Prüfpflichten missachtet hat, haftet demnach als Störer. Da ein Unterlassungsanspruch (siehe vorherige Frage) unabhängig von Ansprüchen gegen den tatsächlichen Rechtsverletzer besteht, muss ein Anschlussinhaber bei einem Rechtsstreit unter Umständen zunächst zeigen, dass er nicht Täter war; anschließend, dass er auch keine Prüfpflichten verletzt hat.

»

**Auch in Schulen kann Freifunk etwas zur Bildung beitragen, indem Lehrer und Schüler in den Aufbau eines Netzes eingebunden werden. So wie die einen Beete im Schulgarten anlegen, stellen die anderen Freifunk-Router auf. Bei beidem lässt sich etwas lernen und alle haben etwas davon.**

Andreas Pittrich, Bürgerdeputierter in der Bezirksverordneten-Versammlung Friedrichshain-Kreuzberg

«

Betreibern von freien Funknetzen helfen diese Prüfpflichten jedoch nicht viel, denn der Bundesgerichtshof hat für private Anschlussinhaber festgestellt, dass dies unter anderem bedeutet, ein WLAN-Netz gegen den Zugriff durch Dritte mit einem Passwort zu schützen. Eine solche Verpflichtung widerspricht jedoch offensichtlich der Grundidee freier Funknetze.

Ob auch andere Sicherungsmaßnahmen im Fall eines Rechtsstreits ausreichen können, lässt sich derzeit nicht mit Sicherheit sagen. Der Jurist Reto Mantz hat vorgeschlagen, folgende technische Maßnahmen zu erwägen:

- Nutzer des Netzwerks können durch eine Bildschirmmeldung beim Einwählen (Splash-Screen) auf die Pflicht zu rechtstreuem Verhalten hingewiesen werden.
- Der Betreiber kann solche Ports blockieren, über die typischerweise Filesharing-Anwendungen laufen oder auch
- ein sogenanntes „Zapp“-Skript einrichten, das einen Rechner zeitweilig blockiert, wenn er in kurzer Zeit viele Verbindungen aufnimmt, was auf die Nutzung eines Filesharing-Dienstes hindeutet.
- Der Betreiber kann durch eine Anmeldung bei der Bundesnetzagentur und eine genaue Dokumentation der Netz-Einrichtung (siehe S. 30) im Zweifel nachweisen, dass er Maßnahmen ergriffen hat und für sich Providerstatus beansprucht.

Allerdings bietet keine dieser Vorkehrungen eine Garantie, dass es nicht doch zu einer Haftung kommen kann, wenn über das Netz des Anschlussinhabers Rechtsverletzungen begangen wurden; die Rechtsprechung bietet ein disparates Bild. Der Betreiber demonstriert zumindest guten Willen. Deshalb haben einige Gruppen von Freifunkern begonnen, auf technische Übergangslösungen zurückzugreifen. Sie leiten den Datenverkehr zunächst ins Ausland um oder organisieren ihn so, dass eventuelle Abmahnungen bei einem Verein als Access Provider landen und nicht beim einzelnen Anschlussinhaber (siehe S. 25).

→ **Da der Anschlussinhaber bei einer Abmahnung für fremde Rechtsverletzungen im Zweifel die Anwaltskosten trägt, bleibt für Freifunk-Betreiber ein Risiko. Betreiber sollten genau prüfen, mit welchen technischen Maßnahmen sie es verringern und für den einzelnen WLAN-Gastgeber minimieren können.**

### Warum haftet ein Freifunk-Betreiber im Zweifel als Störer, aber nicht ein kommerzieller Internetanbieter?

An sich gilt für Access Provider – und damit auch für Anbieter eines freien Funknetzes mit Internetzugang – eine gesetzliche Haftungsprivilegierung. Das bedeutet, dass sie nicht für fremde Informationen verantwortlich sind, die sie lediglich übermitteln oder zu denen sie einen Zugang vermitteln. Sie müssen

den Datenverkehr auch ausdrücklich nicht überwachen oder nach Rechtsverletzungen forschen. Erst wenn sie Kenntnis von einer Rechtsverletzung haben, sind sie auch haftbar. Es ist allerdings bis heute nicht eindeutig geklärt, ob auch private Anbieter von WLAN-Netzen unter dieses sogenannte Provider-Privileg fallen.

→ Die weitere Rechtsprechung – oder der Gesetzgeber – muss zeigen, ob auch für nicht kommerzielle oder kleine private Anbieter von freien Funknetzen das Provider-Privileg gelten kann. Bis dahin bleibt ihre rechtliche Einordnung nicht eindeutig.

### Wie geht es mit der Störerhaftung weiter?

Derzeit versuchen zwei Freifunker vor Gerichten, die Rechtslage genauer zu klären. Daneben hat das Landgericht München im September 2014 in einem weiteren Streitfall den Europäischen Gerichtshof angerufen. Er soll darüber befinden, ob ein gewerblicher Anbieter eines einzelnen, bewusst offenen WLANs für Rechtsverletzungen haftet. Bis hier ein Ergebnis vorliegt, wird es allerdings noch dauern.

Daneben gibt es die Möglichkeit, dass der Gesetzgeber die Lage klarstellt. Hier hat etwa der Verein Digitale Gesellschaft einen Gesetzentwurf vorgestellt, der das Provider-Privileg ausdrücklich auf nicht gewerbliche Betreiber von Funknetzen erstrecken und Unterlassungsansprüche ausschließen soll. Initiativen der SPD, der Linken und der Grünen zum Thema in Bundestag und Bundesrat konnten sich bis jetzt nicht durchsetzen.

In ihrem Koalitionsvertrag vom Herbst 2013 haben sich die Fraktionen von CDU/CSU und SPD im Grundsatz auf eine Reform verständigt. Bislang ist noch unklar, wie sie genau umgesetzt werden soll. Im August 2014 veröffentlichte Berichte deuten darauf hin, dass private, nicht kommerzielle WLAN-Gastgeber bei einer Lockerung auch außen vor bleiben könnten.

Auf europäischer Ebene gibt es zudem Entwürfe für ein neues Regelungspaket zum digitalen Binnenmarkt; es zielt unter anderem auf lokale und nicht gewerbliche Funknetze und könnte die rechtlichen Anforderungen für sie neu ordnen. Ob und wann es umgesetzt wird, ist derzeit noch offen. In beiden Fällen bleibt abzuwarten, ob und wie sich der politische Willensbildungsprozess noch entwickelt und ob die Rahmenbedingungen für freie Funknetze dadurch verbessert werden.

→ Freifunk-Betreiber sollten die weitere Entwicklung verfolgen, da sowohl von Gerichten als auch den Gesetzgebern neue Entscheidungen zur Störerhaftung und weitere Regelungen zu erwarten sind. Gilt auch für sie eine Haftungsprivilegierung, würde dies die weitere Entwicklung freier Funknetze deutlich begünstigen.

## WEITERFÜHRENDE INFORMATIONEN

# Häufige Fragen

## Was unterscheidet Freifunk von anderen Internetanbietern?

Der Internetzugang ist bei Freifunk letztlich nur Bestandteil eines umfassenden Konzepts, das im Aufbau von Bürgernetzen besteht. In diesen Netzen sind auch eigene lokale Dienste und Angebote ähnlich wie im Intranet einer Firma oder Organisation möglich. Die Freifunk-Gruppen verstehen sich als nicht kommerzielle Initiativen, die auf dem gemeinschaftlichen Einsatz aller Beteiligten basieren und eine freie Infrastruktur aufbauen. Manche Freifunk-Vereine sind rechtlich betrachtet auch Internetanbieter, bei anderen Netzen ist jeder Beteiligte selbst Anbieter.

## Braucht man spezielle Technik, um Freifunk zu empfangen?

Ist an einem Standort bereits ein Freifunk-Netz zu empfangen, benötigt man nur ein WLAN-fähiges Gerät, um sich mit dem Netz zu verbinden. Viele freie Funknetze lassen sich am Namen des WLAN-Netzwerks (SSID) erkennen, etwa „leipzig.freifunk.net“. Wie bei offenen WLAN-Netzen generell ist es allerdings häufig empfehlenswert, einen VPN-Dienst zu nutzen, der den Datenverkehr zusätzlich verschlüsselt (siehe S. 25). Die Software dafür ist auf modernen Computern und mobilen Geräten meist bereits installiert.

## Braucht man spezielle Technik, um Freifunk zu betreiben?

Das hängt davon ab, auf welche Weise man mitmachen möchte. Die einfachste Möglichkeit besteht darin, das Freifunk-Netz mit einem WLAN-fähigen Router zu erweitern. Er kann mit dem Internet verbunden werden, um zusätzliche Bandbreite einzuspeisen. Viele Freifunk-Initiativen bieten passende, fertig ausgerüstete Router an. Es lassen sich auch einige handelsübliche Router anpassen, indem eine eigene Software (Firmware) aufgespielt wird. Für größere Reichweiten mit Sichtkontakt kommen fertige oder selbst gebaute Outdoor-Router und Richtfunk-Antennen zum Einsatz.

## Muss ich eine Außenantenne anmelden?

Eine Außenantenne für Freifunk-Netze muss nicht angemeldet werden. WLAN-Geräte funkten in den Frequenzbereichen von 2,4 GHz und 5 GHz, die zur Nutzung durch die Allgemeinheit freigegeben wurden. Funkanlagen dürfen auch mehrere Grundstücke zu einem einheitlichen Netz verbinden; eine maximale Reichweite ist nicht vorgegeben. Allerdings dürfen nur Geräte verwendet

werden, die in Deutschland zugelassen sind. Dazu müssen sie über ein CE-Zeichen verfügen, mit Typenbezeichnung, Seriennummer und dem Hersteller-namen versehen sein. Die zulässige Sendeleistung darf aber nicht überschritten werden: Im Frequenzbereich von 2,4 GHz beträgt sie maximal 100 mW, im unteren 5-GHz-Band (5,15 bis 5,35 GHz) maximal 200 mW, im oberen (5,47 bis 5,725 GHz) höchstens 1000 mW.

Mieter einer Wohnung oder eines Hauses müssen allerdings ihren Vermieter oder die Hausverwaltung um Erlaubnis fragen, bevor sie eine Antenne außen anbringen. Als Mieter hat man keinen Anspruch darauf, dass dieser Bitte entsprochen wird. Bei größeren Vernetzungsvorhaben erleichtert es ein abgestimmtes Vorgehen mit Freifunk-Vereinen oder auch weiteren kommunalen Einrichtungen oder Unternehmen erfahrungsgemäß, neue Standorte zu erschließen.

### Gibt es spezielle Regeln im Freifunk?

Neben den allgemeinen gesetzlichen Vorgaben für Anbieter und Nutzer (siehe S. 30) haben die Initiativen für freie Funknetze im sogenannten „Pico-Peering-Agreement“ einige Grundregeln für den Datenverkehr festgelegt. „Pico-Peering“ bedeutet dabei so viel wie Datenaustausch im kleinsten Maßstab – gemeint sind die einzelnen Beteiligten, die einen Knotenpunkt fürs Netz oder ihren Internetanschluss bereitstellen, aber auch der Austausch zwischen einzelnen Teilnetzen. Die Vereinbarung umfasst im Wesentlichen vier Grundregeln. Wer mitmacht,

- bietet ungestörten Datentransit über ein freies Netz an,
- dokumentiert die zum Datenaustausch nötigen Informationen öffentlich unter einer freien Lizenz und ist mindestens mit einer E-Mail-Adresse erreichbar,
- bietet keine Garantien für seinen Dienst und kann ihn jederzeit einstellen,
- kann eigene, ergänzende Nutzungsbedingungen aufstellen.

### Was kostet Freifunk?

Wer Freifunk nur passiv zum Surfen nutzt, für den ist er kostenlos. Wer seinen WLAN-Anschluss auch aktiv anderen zur Verfügung stellen will, kann bei vielen Freifunk-Initiativen einen zusätzlichen, speziell angepassten WLAN-Router erwerben oder ein eigenes Modell selbst anpassen. Die auf den Routern installierte Software – meist eine Version der Firmware „Open WRT“ – ist kostenlos. Die günstigsten geeigneten Router sind derzeit für rund 15 bis 20 Euro erhältlich. Für den Betrieb fallen dann noch Stromkosten je nach Modell an. Bei eigenen (Dach-)Antennen für größere Strecken kommt es auf das konkrete Vorhaben an. Von Eigenbau-Antennen bis zu professionellen Installationen im vierstelligen Kostenbereich ist alles möglich.

### Wie finanziert sich Freifunk?

Der Großteil des Aufwands wird von den Aktiven in ehrenamtlicher Arbeit getragen. Viele der Initiativen in Deutschland sind auch als Vereine organisiert, die von Mitgliedsbeiträgen getragen werden und Geld- und Sachspenden entgegennehmen können, um etwa weitere laufende technische Kosten aufzubringen. Die mabb hat den Freifunk-Ausbau in Berlin 2013 und 2014 mit zusammen 80.000 Euro gefördert. Die bei Freifunk eingesetzte Software ist meist unter Open-Source-Lizenzen kostenlos erhältlich.

### Wer kann bei der Einrichtung oder technischen Fragen helfen?

Die meisten Initiativen in Deutschland veranstalten in regelmäßigen Abständen Treffen, die ein guter Anlaufpunkt sind. Daneben betreiben sie auch Mailinglisten, regionale Websites und Foren, auf denen Anleitungen zu finden und teilweise technische Diskussionen möglich sind.



# Glossar

<b>Ad-hoc-Netz</b>	Als Ad-hoc-Netze werden Netze bezeichnet, die ohne dauerhaft festgelegte Infrastruktur auskommen. Kommt ein Knoten zum Netzwerk hinzu, wird er dynamisch eingebunden.
<b>Allmende</b>	Bezeichnet allgemein gemeinschaftlich genutzte Ressourcen oder die Rechtsform des gemeinschaftlichen Eigentums. Bei digitalen Gütern wird auch von der „digitalen Allmende“ gesprochen, bei freien Funknetzen gelegentlich von der „Netzwerk-Allmende“.
<b>Backbone</b>	Bezeichnet das Rückgrat eines Netzwerks, das seine Teilbereiche verbindet. Backbone-Verbindungen im Internet bestehen häufig aus Glasfasernetzen, die einzelne Netzbetreiber verbinden. Das Berliner Freifunk-Backbone besteht aus Richtfunkverbindungen zwischen hohen Standorten.
<b>BATMAN</b>	→ Protokoll
<b>Client</b>	Als Client wird ein Programm bezeichnet, das einen Dienst auf einem anderen Computer (Server) nutzt, zum Beispiel wenn ein Browser eine Webseite anfragt.
<b>Cookies</b>	Cookies sind kleine Textdateien auf dem Computer, mit deren Hilfe sich eine Webseite zum Beispiel den Benutzer oder seine Einstellungen merken kann.
<b>DSL</b>	DSL-Übertragungsverfahren (Digital Subscriber Line) schaffen Zugang zum Internet über die Kupferleitungen des Telefonnetzes. Freifunk-Initiativen entstanden zunächst häufig dort, wo DSL-Angebote nicht verfügbar waren, etwa in Gebieten, die in den Neunzigerjahren mit Glasfaser-Leitungen erschlossen wurden.
<b>Firewall</b>	In der Regel eine Software, die unerwünschten Datenverkehr blockiert und erwünschten passieren lässt.
<b>Firmware</b>	Bezeichnet Software, die fest (engl. <i>firm</i> ) mit einem Gerät verbunden ist und dessen Funktionen koordiniert, wie das Betriebssystem bei einem Computer. Freifunk-Initiativen spielen bei → Routern zumeist die „Open WRT“-Firmware auf, die auf dem → Open-Source-Betriebssystem Linux basiert.

<b>Freie Software</b>	→ Open Source
<b>IP-Adresse</b>	Eine Nummer, die ein Gerät im Internet identifiziert. Urheberrechts-Abmahnungen etwa basieren in der Regel darauf, dass die IP-Adresse des Anschlussinhabers (→ Störerhaftung) beim Anbieten geschützter Werke öffentlich sichtbar ist.
<b>Master</b>	Ein Master (Herr) ist in einem hierarchisch verwalteten Netzwerk diejenige Recheneinheit, die die Steuerung oder Ressourcenverwaltung übernimmt.
<b>Mesh-Netz</b>	Ein Netzwerk, in dem jeder Knoten den Datenverkehr weiterleiten kann und somit kein hierarchischer Aufbau oder ein festes Zentrum entsteht.
<b>Open Source</b>	Bezeichnet Computerprogramme, bei denen jeder den zugrundeliegenden Quelltext einsehen, verändern oder weitergeben kann. Wenn die Lizenz dem Nutzer bestimmte Freiheiten erlaubt, ist häufig auch von freier Software die Rede, einem sehr ähnlichen Konzept.
<b>Open WRT</b>	→ Firmware
<b>OLSR</b>	→ Protokoll
<b>Peer-to-Peer-Netze</b>	Ein Oberbegriff für Netzwerke, deren Teilnehmer gleichgestellt (als <i>peers</i> ) kommunizieren und deren Knoten somit direkt Daten austauschen können.
<b>Peering</b>	Von Peering spricht man, wenn einzelne Netzbetreiber ihren Datenverkehr austauschen, etwa verschiedene Zugangsanbieter an einem Internetknoten („Peering Point“).
<b>Pico-Peering-Agreement</b>	Das Pico-Peering-Agreement ist eine international erarbeitete Übereinkunft, die Grundprinzipien für den Datenverkehr in freien Funknetzen festhält. Die Teilnehmer bekennen sich zu freiem Datentransit, offener Dokumentation und schließen Leistungsgarantien aus.
<b>Port</b>	Ports sind Nummern, die verschiedenartige Verbindungen eines Geräts unterscheiden, damit zum Beispiel der E-Mail-Datenverkehr an das E-Mail-Programm geleitet wird. Sie sind wie Zimmernummern in einem Haus, während man sich → IP-Adressen wie Hausnummern vorstellen kann.

<b>Protokoll</b>	Ein Protokoll legt technisch fest, wie Daten übertragen werden. Ein → Routing-Protokoll regelt, auf welchen Wegen Daten übertragen werden und wie die Wegbeschreibungen im Netz verbreitet werden. In freien Funknetzen sind dafür besonders das OLSR-Protokoll („Optimized Link State Routing“) und das BATMAN-Protokoll („Better Approach To Mobile Ad-hoc Networking“) relevant.
<b>Resilienz</b>	Bezeichnet allgemein die Fähigkeit eines Systems, mit Störungen umzugehen und sie auszugleichen. → Mesh-Netze gelten als resilient, da es keine Zentrale gibt, bei deren Ausfall auch das gesamte Netz ausfallen würde.
<b>Richtfunk</b>	Dient zur Funkübertragung zwischen festen Standorten, indem das Signal gebündelt wird. Im Freifunk werden Richtfunk-Antennen für größere Punkt-zu-Punkt-Verbindungen zwischen einzelnen Standorten genutzt.
<b>Router</b>	Im allgemeinen Sinn Geräte, die Daten zwischen Computernetzen bewegen. → DSL-Router verbinden das häusliche Netz mit dem Internet. Heutige WLAN-Router kombinieren meist einen WLAN-Zugangspunkt mit einem Router und einem DSL-Modem, das die Internetverbindung herstellt. Beim Freifunk werden meist angepasste Router mit der → Firmware „Open WRT“ verwendet.
<b>Routing</b>	Als Routing wird die Auswahl geeigneter Wege zum Datentransport in einem Netzwerk bezeichnet. In freien Funknetzen kommen dafür häufig die → Protokolle OLSR und BATMAN zum Einsatz.
<b>SSID</b>	Eine SSID (Service Set Identifier) bezeichnet den öffentlichen Namen eines WLAN-Netzes.
<b>Störerhaftung</b>	Bezeichnet allgemein die Haftung desjenigen, der an einer Rechtsverletzung mitgewirkt hat, ohne selbst Täter oder Teilnehmer zu sein. Der derzeitigen Rechtsprechung nach können WLAN-Gastgeber besonders für Urheberrechtsverletzungen Dritter auf Unterlassung haften, wenn sie bestimmte Prüfpflichten verletzen.

<b>Uplink</b>	Bezeichnung allgemein eine Verbindung in ein übergeordnetes Netzwerk, hier speziell die Verbindung eines Freifunk-Netzes mit dem Internet.
<b>Verschlüsselung</b>	Dient dem Schutz von Informationen vor Kenntnisnahme durch Dritte. In einem offenen WLAN wird der Datenverkehr zunächst unverschlüsselt übertragen, er kann aber über eine Transportverschlüsselung zum Beispiel mit „HTTPS“-Verbindung oder ein → VPN geschützt werden.
<b>VPN</b>	Ein Virtual Private Network (VPN) ist eine verschlüsselte Anbindung eines Rechners an ein entferntes Netzwerk, die auch den Datenverkehr vor Mitlesern schützt. Die notwendige Software dafür ist bereits in den meisten modernen Betriebssystemen und auch in Smartphones integriert.
<b>WLAN</b>	Bezeichnet ein drahtloses lokales Netzwerk (Wireless Local Area Network). Technisch sind solche Funknetze in der „IEEE 802.11“-Norm spezifiziert. Diese Norm des „Institute of Electrical and Electronics Engineers“ enthält eine ganze Reihe technischer Standards, darunter auch für → Mesh-Netze.

# Lektüre

## Mitmachen

- freifunk.net: Übersicht über Initiativen in Deutschland und weitere Informationen zum Mitmachen  
<http://freifunk.net/wie-mache-ich-mit/>
- Karte: Zugangspunkte für Public Wifi und Freifunk in Berlin und Potsdam  
<http://publicwifi.de/>

## Recht/ Sicherheit

- Bundesnetzagentur: Ausführliche Informationen zur Frequenznutzung im 2,4- und 5-GHz-Band  
<http://tinyurl.com/bnetza-wlan>
- Bundesnetzagentur: Katalog von Sicherheitsanforderungen für Telekommunikationssysteme und die Verarbeitung personenbezogener Daten  
<http://tinyurl.com/anbieterpflichten>
- „TKG-Starterpaket“: Mustervorlagen zur Bundesnetzagentur-Meldung, Nutzerbelehrung und Sicherheitskonzept von Reto Mantz  
<http://offenenetze.de/?p=2828>
- „Post vom Anwalt, was tun?“ Hinweise zur Vorgehensweise bei Abmahnungen von iRights.info  
<http://irights.info/?p=6852>

## Technik

- „Wireless Networking in the Developing World“: Freies Buch und E-Book zum Download, 3. Aufl. 2013  
<http://wndw.net/>

## Politik

- Leonhard Dobusch, Christian Forsterleitner, Manuela Hiesmair (Hg.): Freiheit vor Ort – Handbuch kommunale Netzpolitik, 2011. Freies Buch und E-Book zum Download  
<http://freienetze.at/freiheit-vor-ort-handbuch-kommunale-netzpolitik>

### Zur Herausgeberin

Die mabb ist die gemeinsame Medienanstalt der Länder Berlin und Brandenburg. Ihre Regulierungsaufgaben nimmt sie bei bundesweiten Veranstaltern und Plattformen zusammen mit den gemeinsamen Organen der Medienanstalten der Länder wahr. Entsprechend ihrem gesetzlichen Auftrag fördert die mabb darüber hinaus Medienkompetenz und -ausbildung sowie Projekte mit neuen Übertragungstechniken in Berlin und Brandenburg. Bereits in früheren Projekten hat die mabb die Entwicklung des Breitbandinternets unterstützt.

### Zu den Autorinnen und Autoren

#### **Corinna ‚Elektra‘ Aichele**

arbeitet als Software- und Hardwareentwicklerin und hat die Freifunk-Technologie aktiv mitgestaltet, so beim Routing-Protokoll BATMAN und dem Telefon-Router „Mesh-Potato“. Sie hat den Funk-Einsatz international unterrichtet, ist Autorin des Buches „Mesh“ und Coautorin von „Wireless Networking in the Developing World“.

#### **Dr. Hans Hege**

ist Direktor der Medienanstalt Berlin-Brandenburg (mabb).

#### **Torsten Kleinz**

ist freier Journalist aus Köln und schreibt besonders über den Einfluss von neuen Techniken auf die Gesellschaft. In diesem Rahmen begleitet er Projekte wie Freifunk seit 15 Jahren. Er schreibt für Medien wie die c't, Zeit Online und ZDF Hyperland.

#### **Henning Lahmann**

ist Jurist, Journalist und freier Mitarbeiter beim iRights.Lab. Er promoviert über völkerrechtliche Regelungen im Internet und war wissenschaftlicher Mitarbeiter an den Universitäten Kiel und Potsdam. 2010 hat er das Blog „No Fear Of Pop“ gegründet.

#### **David Pachali**

ist freier Journalist und Redakteur bei iRights.info. Er konzipierte und betreute Publikationen wie „Öffentlichkeit im Wandel“ (Heinrich-Böll-Stiftung, 2012), „Überwachte Gesellschaft“ (2013) und „Groundbreaking Journalism“ (2014, iRights.Media).

## Impressum

### **Herausgeberin**

Medienanstalt Berlin-Brandenburg (mabb)  
Kleine Präsidentenstraße 1  
10178 Berlin

### **Ansprechpartner**

Steffen Meyer-Tippach

# **mabb**

<http://mabb.de>

1. Auflage 2014

### **Beiträge von**

Corinna ‚Elektra‘ Aichele: Mesh-Netze am Beispiel Berlin  
Henning Lahmann: Ein Netz voller Fallgruben?  
Torsten Kleinz: WLAN FÜR ALLE – aber sicher?  
David Pachali: Was ist Freifunk?, Häufige Fragen, Stationen 2002-2014

### **Redaktion**

David Pachali



<http://irights-lab.de>

### **Illustrationen**

Rosendahl Berlin,  
<http://rosendahl-berlin.de>

### **Lektorat**

Jörg Garbers

### **Gestaltung**

Beate Autering, beworx

### **Druck**

Medialis Offsetdruck, Berlin

### **Lizenz**

Die Texte, Grafiken und Illustrationen sind freigegeben unter der Creative-Commons-Lizenz Namensnennung 4.0 (Details siehe <http://creativecommons.org/licenses/by/4.0>). Anzugeben sind Autor/Illustrator, Herausgeberin, Quelle und Lizenz (Bezeichnung und URL).



