Das Franzis Praxisbuch

192 Seiten pures FRITZ!Box-Know-how

Rudolf G. Glos

FRITZ!Box

Konfigurieren · Tunen · Absichern

- FRITZ!Box einrichten, aktualisieren und absichern
- Die FRITZ!Box als Daten- und Mediaserver nutzen
- Sicherer Fernzugriff auf Ihr Heimnetz per VPN

FRANZIS

Inhaltsübersicht

1 WLAN- & DSL-Basics

Ein WLAN-Funknetz erfüllt viele Wünsche. Es erspart einem vor allem das lästige Strippenziehen. Derzeit gibt es für WLAN im Wesentlichen zwei unterschiedliche Standards – je nachdem, welche WLAN-Steckkarte Sie nutzen, sendet diese im 2,4- oder 5-GHz-Funkbereich oder, wie die neue, topaktuelle FRITZ!Box 7390 dank zweier Antennen, in beiden. Die Funkleistung von 2,4 GHz ist mittlerweile veraltet, da es nur 11 MBit/s übertragen kann. Das 5-GHz-Funknetz schafft per Standard 54 MBit/s.

Firmenspezifische Lösungen und der WLAN-Standard 802.11n bieten bei gleicher Funkleistung schon das Doppelte, diese Technik ist jedoch nicht vollständig standardisiert und macht somit speziell aufeinander abgestimmte Komponenten notwendig.

Bild 1.1 Das FRITZ!-Logo.

1.1 Kriterien für die WLAN-Reichweite

Ein WLAN-Router wie die FRITZ!Box bietet standardmäßig eine Strahlungsleistung von ca. 100 mW, was der im WLAN-Standard spezifizierten Maximalleistung entspricht. Damit kommen Sie problemlos durch dicke Wände in der Wohnung oder im Haus, und im Freien kann die Reichweite bis zu 100 Meter für eine Funkübertragung betragen.

Bild 1.2 Die FRITZ!Box Fon WLAN 7390 vereint mit VDSL, ADSL, Telefonanlage, WLAN, DECT-Basis, Gigabit-Ethernet und internem Netzwerkspeicher alle für die Kommunikation wichtigen Funktionen in einem Gerät. Damit setzt AVM neue Maßstäbe beim Internetanschluss und bei der Vernetzung zu Hause.

Die WLAN-Reichweite und somit auch die Übertragungsbandbreite hängen jedoch stark von der Umgebung ab, in der das Gerät eingesetzt wird. Für den Einsatz in der Wohnung reicht die Standardantenne in der Regel aus. Anders schaut es bei der WLAN-Versorgung in einem Haus aus, das typischerweise mit Keller, Erd- und Obergeschoss ausgestattet ist. Hier ist die Wahl des Standorts der Antenne das A und O.

So finden Sie den idealen Aufstellungsort für die FRITZ!Box

Im Idealfall befindet sich die FRITZ!Box möglichst zentral in dem zu versorgenden Bereich. Wichtig ist ein freier, unverdeckter Standort, der eine möglichst ideale Sicht zur Antenne sicherstellt. Hat das Haus Stahlbetondecken, sorgt die Positionierung beispielsweise im Treppenhaus für eine bessere Übertragungsqualität, als stünde die FRITZ!Box im Arbeitszimmer zwischen dem Bücherstapel im Regal.

Achten Sie grundsätzlich darauf, dass schon kleine Positionsveränderungen des WLAN-Routers erheblichen Einfluss auf die Übertragungsstärke haben können. Daher lautet hier der Grundsatz: so zentral wie möglich mit keiner oder wenig Sichteinschränkung. Ist keine Sichtverbindung möglich, suchen Sie den Ort mit den geringsten Hindernissen zwischen Sender und Empfänger. Achten Sie auch hier auf Materialien wie Stahlbeton, Metallflächen, Wasser etc., die für eine große Abschirmung sorgen.

Doch manchmal lässt sich die FRITZ!Box nicht an dem zunächst vorgesehenen Platz aufstellen, da andere Mitbewohner ein Veto einlegen oder die Wohnung bzw. das Haus stark verwinkelt ist. In diesem Fall kann eine größere Antenne an der FRITZ!Box den nötigen Erfolg bringen, die Sende- und Empfangsleistung zu verbessern.

Mehrere Etagen mit einem Access Point vernetzen

Haben Sie vor, mehrere Etagen zu vernetzen, kann die Anschaffung von Access Points für die oberen Etagen sinnvoll sein. Dazu setzen Sie im Treppenhaus einen Access Point, der auf der Etage das Signal problemlos verteilt. Innerhalb des Treppenhauses reicht die Leistung der meisten Router aus, um einen Access Point mit voller Leistung anzusprechen.

Was ist ein Ad-hoc-Modus und was ein Infrastrukturmodus?

Ein WLAN lässt sich wahlweise im Ad-hoc-Modus oder im Infrastrukturmodus betreiben. Im Ad-hoc-Modus kommunizieren die Stationen, also die Rechner, direkt miteinander. Ad-hoc-Verbindungen sind quasi Point-to-Point-Verbindungen, von denen aber jede Station mehrere haben kann – ein Vorteil des Funknetzes. Der Ad-hoc-Modus ist für Anwender geeignet, die kein großes Funknetz aufbauen möchten, sondern nur schnell zwei WLAN-Geräte miteinander verbinden wollen.

Der Infrastrukturmodus braucht stattdessen einen sogenannten Access Point, über den die WLAN-Komponenten kommunizieren und auch auf das kabelgebundene Netz wie Internet etc. zugreifen können. Access-Point-Technik liefern alle WLAN-Router, die Sie im Handel kaufen können. So macht ein Access Point nichts anderes, als die Daten zwischen WLAN und LAN hin- und herzuschieben, und stellt somit eine Sende- und Empfangseinheit dar.

1.2 Aktuelle WLAN-Standards

WLANs arbeiten mit bestimmten Standards, die Funkfrequenz, Kanalnummer und Übertragungsgeschwindigkeit festlegen. Für den Aufbau eines WLAN bedeutet das zunächst, dass alle Komponenten einen gemeinsamen Standard beherrschen müssen, um zusammenzuarbeiten. Funknetze verständigen sich per Funk, dazu brauchen sie eine gemeinsame Frequenz. Die gemeinsame Frequenz gehört zusammen mit anderen Daten zur Norm, die für die Kommunikation benötigt wird.

Die Basisnorm heißt 802.11. Wie bei allem in der Welt gibt es aber auch hier unterschiedliche Normen, die ungünstigerweise nur anhand des Abschlussbuchstabens zu unterscheiden sind. In diesem Fall gibt also 802.11b, 802.11g etc. Die verschiedenen Normen, auch Standards genannt, haben unterschiedliche Frequenzen, unterschiedliche Reichweiten und unterschiedliche Übertragungsgeschwindigkeiten. So sieht die Welt der Funknetze derzeit aus:

IEEE-Standard	Beschreibung	Bemerkung
802.11	Protokoll und Übertragungsverfahren für drahtlose Netze (bis 1997 für 2 MBit/s bei 2,4 GHz definiert).	Grundlage für alle WLAN-Standards.
802.11a	WLAN mit bis zu 54 MBit/s im 5-GHz-Bereich, 12 nicht überlappende Kanäle, Modulation: OFDM (*Orthogonal Frequency Division Multiplexing*).	In Deutschland eher unüblich und selten. Nicht mehr aktuell.
802.11b	WLAN mit bis zu 11 MBit/s im 2,4-GHz-Bereich, 3 nicht überlappende Kanäle.	Früher WLAN-Standard in Europa, immer noch in älteren Centrinos zu finden.
802.11b+	WLAN mit bis zu 22 MBit/s im 2,4-GHz-Bereich, Modulation: PBCC.	Modifizierte Variante des 802.11b-Standards. Verbreitung eher gering.
802.11c	Wireless Bridging zwischen Access Points.	
802.11d	Anpassungen an regionale Regulierungen und Besonderheiten wie den Frequenzbereich.	
802.11e	Erweitert WLAN um QoS (*Quality of Service*) – Priorisierung von Datenpaketen, z. B. für Multimedia-Anwendungen und Streaming.	
802.11f	Roaming zwischen Access Points verschiedener Hersteller.	
802.11g	54-MBit/s-WLAN im 2,4-GHz-Band, Modulation: OFDM.	Dieser Standard steckt in allen modernen Notebooks und wird von nahezu allen modernen WLAN-Geräten beherrscht. Darunter geht perspektivisch nichts mehr.
802.11h	Ergänzungen zu 802.11a für Europa: DFS (*Dynamic Frequency Selection*) und TPC (*Transmit Power Control*).	
802.11i	WPA2: Verbesserung der Verschlüsselung: AES, 802.1x (aufbauend auf WEP und WPA).	WPA2 ist inzwischen mit vielen Adaptern für den Standard g oder höher möglich.
802.11j	Japanische Variante von 802.11a.	

802.11k	Bessere Messung/Auswertung/Verwaltung der Funkparameter wie Signalstärke macht ortsbezogene Dienste möglich.	
802.11m	Zusammenfassung früherer Ergänzungen sowie Bereinigung von Fehlern aus vorausgegangenen Spezifikationen.	
802.11n	WLAN-Erweiterung mit 108 bis 320 MBit/s.	Dieser Standard steckt in allen modernen Notebooks und wird von nahezu allen modernen WLAN-Geräten beherrscht. Die neueste Generation der WLAN-Router bietet ebenfalls 802.11n – auch das aktuelle AVM-Spitzenmodell FRITZ!Box Fon WLAN 7390.
802.11o	Definiert die Sprachpriorisierung gegenüber dem klassischen Datenverkehr im WLAN.	
802.11p	Erweiterung des 802.11a-Standards für den Einsatz in Fahrzeugen (DSRC/Car2Car-Technik).	Diese Car2Car-Technik steckt noch in den Kinderschuhen.
802.11q	WLAN-Unterstützung von VLAN (*Virtual LAN*).	Ist nur bei einer leistungsfähigen Funkverbindung sinnvoll.
802.11r	Hier wird das sogenannte Fast Roaming beim Wechsel zwischen unterschiedlichen Access Points definiert.	Gerade bei Telefonaten via VoIP eine Herausforderung. Derzeit ohne Gesprächsunterbrechungen nicht möglich.
802.11s	Verbesserung von WDS (*Wireless Distribution System*): Hier werden WLAN-Geräte als Relais zum nächstgelegenen Access Point genutzt. Damit werden die Übertragungsrate und vor allem die Netzabdeckung der bestehenden Access-Point-Infrastruktur deutlich verbessert.	WDS funktioniert derzeit häufig nur mit einheitlichen Geräten eines Chipsatz- oder Geräteherstellers – mit der Einführung des Standards WLAN Mesh Network gehören diese Probleme (hoffentlich) der Vergangenheit an.
802.11t	Einheitliche Test- und Prüfverfahren für die Funknetze sind in diesem WPP-Standard (*Wireless Performance Prediction*) festgelegt.	
802.11u	Hier wird eine eventuelle »Zusammenarbeit« mit anderen Funkstandards wie DECT, Handynetzen und Ähnlichem definiert.	
802.11v	Wireless Network Management.	Wie im kabelgebundenen Netzwerk auch.
802.11w	Protected Management Frames.	
802.11z	Hier ist das sogenannte DLS (*Direct Link Setup*) definiert, das Direktverbindungen zwischen zwei WLAN-Clients, die über einen Access Point verbunden sind, ermöglicht.	
802.11aa	Erweitert die QoS (aus 802.11e) um weitere Funktionen für die Videoübertragung.	
802.11ad	Gigabit-WLAN.	Zukunftsmusik!

Die Einheit MBit pro Sekunde (MBit/s) wird leicht mit der in der PC-Branche üblichen Angabe MByte verwechselt. Tatsächlich besteht ein Byte aus acht Bit, die theoretisch mögliche Geschwindigkeit bei 11 MBit/s beträgt in MByte gerechnet ein Achtel, also etwas mehr als 1,3 MByte/s. Allerdings werden diese Werte in der Praxis nicht erreicht, weil zusätzlich zu den Nutzdaten auch administrative Informationen übertragen werden. Mehr als 600 bis 700 KByte/s sind selten drin. Gleiches gilt für den g-Standard, also rund 4 bis 5 MByte/s.

Für Sie ist wichtig, welchen Einsatz Sie für Ihr WLAN planen. Ein WLAN zum Surfen im Internet vom Sofa aus wäre auch bei 11 MBit/s noch ausreichend schnell, solange die volle Sendeleistung erreicht wird. Die meisten DSL-Anschlüsse stellen zwischen 2 und 6 MBit/s bereit, da ist ausreichend Luft nach oben. Für die schnellen 16-MBit/s-Zugänge ist der ältere Standard aber zu langsam. Aktuelle Komponenten versprechen Übertragungsleistungen von 108 MBit/s und mehr.

Diese Werte werden normalerweise nur erreicht, wenn die Komponenten aus einem Haus stammen. AVM ermöglicht 125 MBit/s lediglich in Verbindung mit dem hauseigenen FRITZ!Box-System und USB- oder Cardbus-Adapter aus dieser Baureihe. Besitzer eines älteren Centrino-Notebooks kommen in der Regel nicht in den Genuss solcher Geschwindigkeiten, weil der Chipsatz herstellerspezifische Ansätze nicht unterstützt.

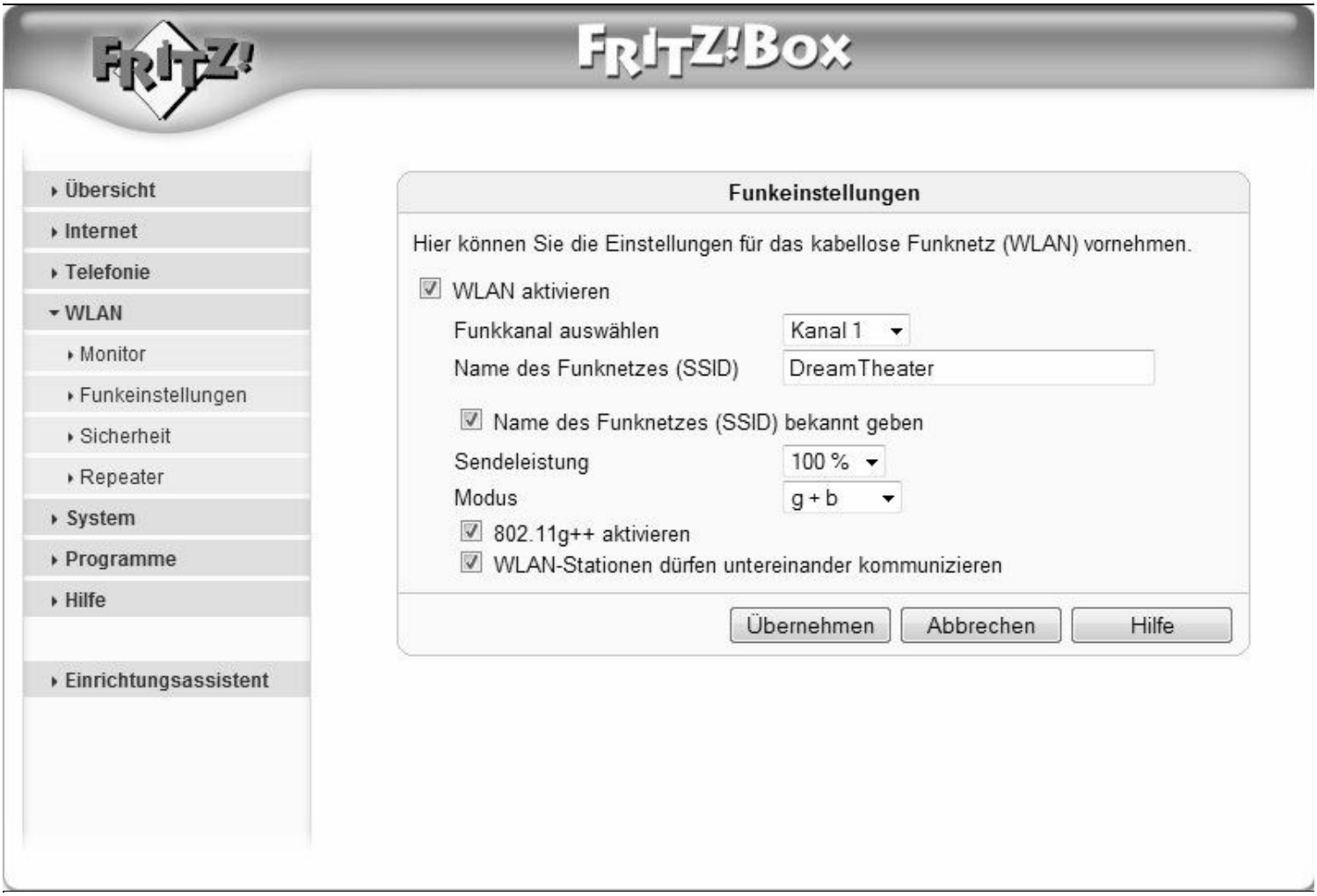


Bild 1.3 Der schnelle 802.11g++-Modus funktioniert nur mit hauseigenen FRITZ!-Komponenten. Kommt es mit einem FRITZ!-AVM-Gerät zu Verbindungsproblemen, sollten Besitzer einer WLAN-FRITZ!Box diesen Schalter deaktivieren.

Beim Kauf von WLAN-Komponenten sollten Sie daher darauf achten, dass alle den gleichen Standard unterstützen, denn das WLAN-System ist abwärtskompatibel. Bei langsameren Komponenten schaltet das ganze Netzwerk auf die niedrigere Geschwindigkeit herunter. Es genügt eine ältere Komponente, und schon werden alle schnelleren ausgebremst. Gleiches gilt auch für die automatische Reduzierung der Übertragungsrate bei Verbindungsproblemen aufgrund dämpfender Wände oder dergleichen. Das ganze Netz wird langsamer.

Beim Kauf neuer WLAN-Geräte auf 802.11n-Kompatibilität achten

Gerade beim Kauf von neuen WLAN-Komponenten wie Routern oder WLAN-Adaptern fürs Notebook oder den PC, aber auch bei NAS-Lösungen sollten Sie auf die 802.11n-Kompatibilität achten. Der 802.11n-WLAN-Standard gehört zur Grundausstattung in einem modernen WLAN. Macht das schmale Budget keine Komplettumstellung auf 802.11n möglich, lässt sich hier schrittweise vorgehen:

Da der 802.11n-Standard abwärtskompatibel ist, können solche Komponenten auch in ein bestehendes »älteres« WLAN integriert werden, und ebenso lässt sich ein 802.11n-tauglicher WLAN-Router oder Zugriffspunkt so konfigurieren, dass er auch Verbindungswünsche von älteren WLAN-Komponenten entgegennimmt.

Der 802.11n-Standard wird in der Werbung vor allem wegen seiner höheren Datentransferrate gepriesen. Tatsächlich hängt es in der Praxis vom Zusammenspiel und der Kompatibilität der verbundenen WLAN-Geräte ab, ob ein neuer Geschwindigkeitsmaßstab erreicht werden kann. So lässt sich unterm Strich nicht mal 100 MBit/s unter guten Bedingungen erreichen. Das ist zwar deutlich schneller als ein »alter« WLAN-Router mit 54 MBit/s, doch im Vergleich zu einem kabelgebundenen Netzwerk ist noch deutlich Luft nach oben.

Hat man jedoch noch ein altes WLAN-Modell im Einsatz oder steigt in Sachen WLAN erst ein, kann man mit dem 802.11n-Standard den Wechsel bzw. den Einstieg in das drahtlose Netzwerk wagen. Im Gegensatz zur »alten« WLAN-Technik reicht der neue Standard für mehrere hochauflösende Videostreams aus und macht endlich ruckelfreie Video-/TV-

Übertragungen im Heimnetz möglich. Zusätzlich bieten manche Geräte der neuesten WLAN-Generation noch weitere Features, die einen Umstieg attraktiver machen:

Wer bei der Datensicherung noch immer mit einer externen Festplatte arbeitet, kennt das Problem: Sind in einem Heimnetz mehrere PCs im Einsatz und sollen Daten schnell und problemlos übertragen werden, wird das Umstecken einer externen Festplatte von einem PC zum anderen schnell lästig. Einfacher und vor allem bequemer sind Festplatten, die direkt im Netzwerk angeschlossen sind: Hier lässt sich von jedem PC oder Mac – auch gleichzeitig – darauf zugreifen. Mit einer passenden FRITZ!Box mit USB-Festplattenanschluss erweitern Sie die Möglichkeiten des Heimnetzwerks enorm.

1.3 DSL- und WLAN-Komponenten

Um ein WLAN aufzubauen, benötigen Sie nur wenige Komponenten. Wenn Sie ein Komplettpaket von einem der großen DSL-Anbieter erworben haben, ist alles schon dabei. Kaufen Sie die Komponenten einzeln, weil Sie bereits einen DSL-Zugang haben, sollten Sie anhand folgender Liste einkaufen gehen:

- **DSL-/WLAN-Router**: Der Router hat die Funktion, das Netzwerk zu realisieren, indem er die nötigen Anschlüsse per Funk und eventuell für Netzwerkkabel bereitstellt. Außerdem stellen neue Modelle die Verbindung zur DSL-Leitung her, fungieren also auch als DSL-Modem. Im Sinne des Funknetzes ist er der sogenannte Access Point, der Zugriffspunkt, der die teilnehmenden Computer verbindet. Möchten Sie auf den Internetzugang verzichten, genügt auch ein Access Point zur drahtlosen Vernetzung von PCs. Das ist in Privathaushalten aber eher selten der Fall.
- **WLAN-Adapter**: Der WLAN-Adapter wird benötigt, um drahtlos mit dem Router kommunizieren zu können. WLAN-Adapter gibt es in Form von Steckkarten für normale PCs, als PCMCIA- oder Cardbus-Adapter für Notebooks, als USB-Lösung für stationäre PCs und Notebooks oder als Bestandteil des Notebooks. Im letzteren Fall ist der WLAN-Adapter in den Chipsatz integriert.
- **Kabel Splitter-zu-Router:** Dieses Kabel wird normalerweise mit dem Router geliefert und verbindet den Splitter mit dem Router. Ob WLAN oder nicht, auf dieses Kabel können Sie nicht verzichten. Alles andere kann kabellos funktionieren, aber an dieser Stelle wird noch auf absehbare Zeit eine sichtbare Kabelverbindung benötigt.
- **Netzwerkkarte**: Wenn Sie den PC, über den der Router und das Netz eingerichtet werden, über ein Kabel an den Router anschließen möchten, muss der Computer mit einer Netzwerkkarte ausgestattet sein. Ist das nicht der Fall, können Sie eine solche Karte günstig nachrüsten oder auch die Erstverbindung per Funk erledigen. Dazu benötigen Sie nur einen der oben genannten WLAN-Adapter für den PC. Es empfiehlt sich aber, die Erstverbindung über ein Netzwerkkabel zu realisieren. Moderne Notebooks haben heutzutage beides, Netzwerkanschluss und WLAN-Adapter. Desktop-PCs sind seit rund fünf Jahren in der Regel mit einem Netzwerkanschluss ausgestattet.
- **Netzwerkkabel**: Weitere PCs können bei vielen Routern auch kabelgebunden angeschlossen werden. Ob der Router Ihrer Wahl das zulässt, müssen Sie prüfen. Viele Router, die einzeln verkauft werden, bieten vier Netzwerkanschlüsse, sodass zusätzlich zum WLAN auch ein kleines Kabelnetzwerk aufgebaut werden kann. Je nach Einsatzzweck ist das sehr praktisch, denn Sie können zwei stationäre PCs im Arbeitszimmer per Kabel vernetzen und Daten austauschen, während Sie sich mit dem Notebook per WLAN ins Internet aufmachen. Sollen mehrere PCs per Kabel angeschlossen werden, benötigen Sie die entsprechende Anzahl Kabel.

Manche Router brauchen besondere Kabel, sogenannte Kreuzkabel. Prüfen Sie beim Einkauf, ob dem Router ein passendes Kabel beiliegt. Ein Kreuzkabel ist anders verschaltet als ein Netzwerkkabel, es kann nur zur Verbindung zwischen Router und dem ersten PC oder für eine Direktverbindung zweier PCs über die Netzwerkbuchse eingesetzt werden.

Eine Besonderheit der FRITZ!Box soll nicht verschwiegen werden: Sie können vor allem bei älteren FRITZ!Box-Modellen statt eines Netzwerkkabels auch ein USB-Kabel verwenden, das der Box beiliegt. Bei den meisten anderen Routern ist das nicht der Fall. Moderne FRITZ!Box-Modelle bieten diese USB-Schnittstelle für den Anschluss von USB-Druckern oder Speichermedien wie USB-Stick oder USB-Festplatte. Solche Geräte können Sie problemlos anschließen, es muss dann nur ein entsprechender Treiber installiert werden, damit sie laufen.

1.4 Highspeed-Internet mit VDSL

Das neue DSL, wie VDSL (*Very High Speed Digital Subscriber Line*) auch manchmal umgangssprachlich genannt wird, ermöglicht deutlich höhere Datenübertragungsraten als die älteren und entsprechend weiter verbreiteten ADSL- und ADSL2+-Standards . Derzeit sind zwei VDSL-Standards verabschiedet worden, von denen der aktuellere VDSL2-Standard in Deutschland zum Einsatz kommt.

Dank der Abwärtskompatibilität zum älteren ADSL2+-Standard halten sich die Kosten für die Endgeräte sowie die Leitungen in Grenzen, sofern der Abstand zwischen dem Anschluss des Endgeräts und der Vermittlungsstelle nicht zu groß ist.

VDSL ist bei der Telekom ein sogenanntes Hybridnetz, da es aus einer Kombination aus Glasfaser- und Kupferleitungen aufgebaut ist. Die Glasfaserkabel sind von der Vermittlungsstelle bis zu den großen, nahezu überdimensionalen Schaltkästen auf dem Gehsteig verlegt. Die Gesamtkapazität eines VDSL-Kastens auf dem Gehweg umfasst nach Aussage eines Telekom-Technikers derzeit in der Regel 100 bis 200 Haushalte. Von dort aus geht es dann mit der gewöhnlichen Kupferleitung zum VDSL-Kunden.

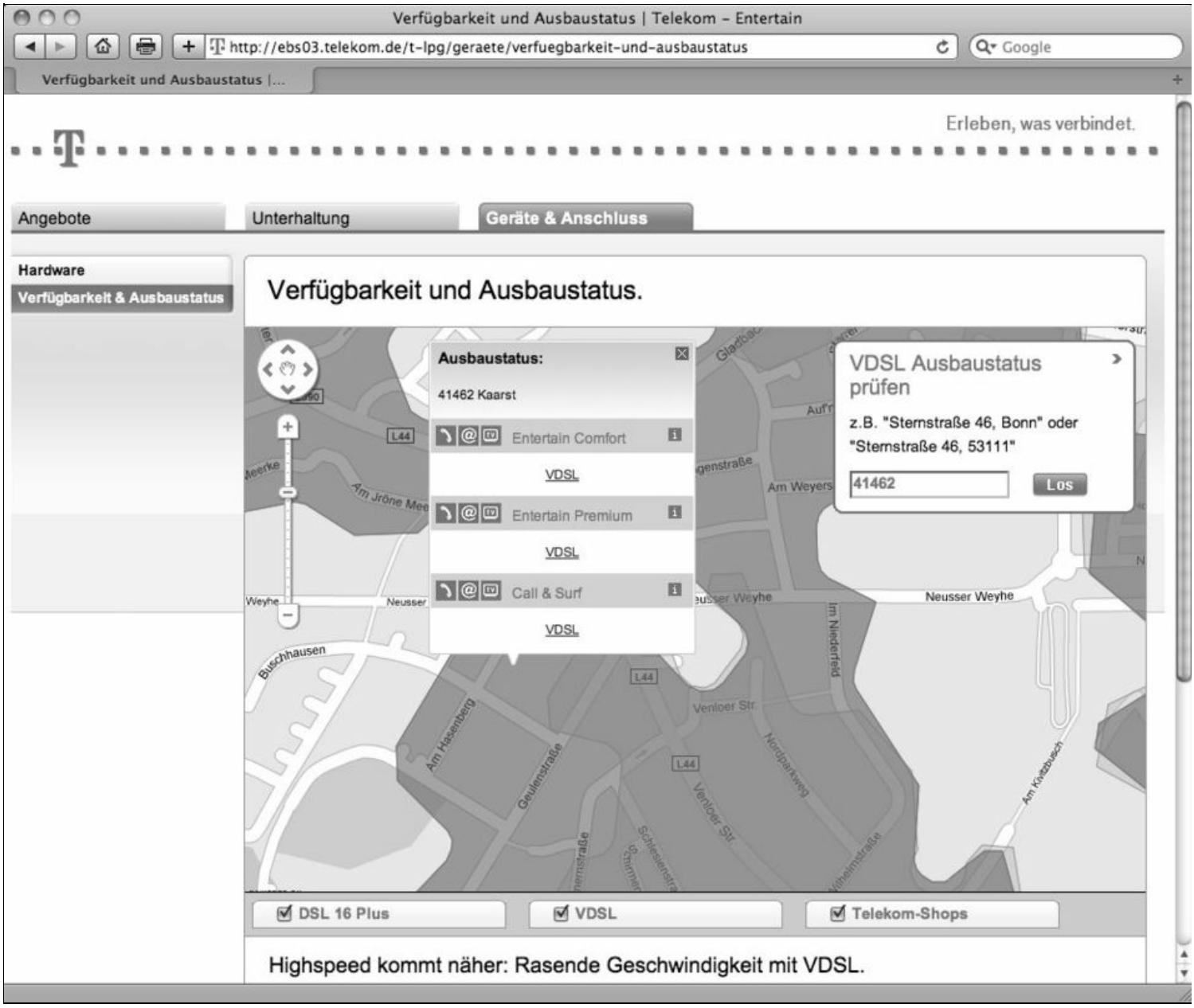


Bild 1.4 Gerade in Ballungszentren stehen die Chancen gut, in den Genuss des schnellen VDSL zu kommen. Prüfen Sie die Verfügbarkeit und den Ausbaustatus unter *http://bit.ly/ajqz77*.

Prüfen Sie nach, ob VDSL auch wirklich geschaltet ist

Durch die kürzere Strecke der Kupferleitung kann diese nun eine höhere Geschwindigkeit aufnehmen, da die Leitungsverluste niedriger sind. Mit der VDSL-Technik ist nicht nur ein schnelleres Internet, sondern auch das in manch anderen europäischen Ländern bereits eingeführte Triple-Play aus Telefon, Internet und IPTV möglich. Mit der schnelleren VDSL-50-Variante kommt sogar hochauflösendes IPTV in HD-Qualität mit dem Telekom-Produkt Entertain in das heimische Wohnzimmer.

Doch allein mit der Bestellung über das Internet oder dem Besuch in einem T-Punkt-Laden ist es nicht getan: Ob VDSL und Entertain im Endeffekt auch wirklich geschaltet werden können, hängt davon ab, ob in dem großen grauen VDSL-Kasten in Ihrer näheren Umgebung auch ein entsprechender Port frei ist oder nicht. Wenn nicht, nimmt die Telekom in der Regel dennoch die Bestellung entgegen und schaltet den Anschluss einfach auf ADSL2+ mit dem Produkt DSL16+ .

In der Praxis ist DSL16+ für HD-Fernsehen jedoch deutlich zu langsam. Sie haben in dem Fall aber die Möglichkeit, vom Vertrag zurückzutreten, falls die zugesagte Leistung (hier: VDSL) nicht erbracht werden kann.

Lesezeichen

http://bit.ly/ajqz77
DSL-Verfügbarkeit prüfen: Vor allem in Ballungszentren stehen die Chancen gut, in den Genuss des schnellen VDSL zu kommen.

VDSL-Komponenten des Telekom-Komplettpakets

Um mit VDSL ins Internet zu kommen, sind wie beim herkömmlichen DSL nur wenige Komponenten notwendig. Haben Sie ein Komplettpaket vom derzeit einzigen VDSL-Anbieter, der Telekom, erworben, ist alles bereits dabei:

- **Splitter**: Wenn Sie bereits DSL nutzen, verfügen Sie schon über einen Splitter , steigen Sie erst jetzt auf DSL um, gehört der Splitter zum Lieferumfang des DSL-Providers. Der Splitter wird an die TAE-Telefonbuchse angeschlossen und trennt das Telefon- vom DSL-Signal. Es ist sinnvoll, zunächst den Splitter und den Router anzuschließen, um die Reichweite der Kabel rund um Ihren Telefonanschluss festzustellen. Der Standort des VDSL-Routers spielt eine entscheidende Rolle für die WLAN-Übertragungsleistung. Je freier die Antenne oder das Gerät selbst (manche Router haben die Antenne im Gehäuse verbaut) senden und empfangen kann, desto besser.
- **(V)DSL-WLAN-Router**: Der Router hat die Funktion, das Netzwerk zu realisieren, indem er die nötigen Anschlüsse per Funk und eventuell für Netzwerkkabel bereitstellt. Außerdem stellen neue Modelle die Verbindung sowohl zur ADSL- als auch zur VDSL-Leitung her, fungieren also auch als DSL-Modem. Im Sinne des Funknetzes ist er der sogenannte Access Point, der Zugriffspunkt, der die teilnehmenden Computer verbindet.
- **Kabel Splitter-zu-Router**: Dieses Kabel wird normalerweise mit dem Router mitgeliefert und verbindet den Splitter mit dem Router. Ob WLAN oder nicht, auf dieses Kabel können Sie nicht verzichten. Alles andere kann kabellos funktionieren, aber an dieser Stelle wird noch auf absehbare Zeit eine sichtbare Kabelverbindung benötigt.
- **Netzwerk-/Ethernetkabel**: Weitere PCs können bei vielen VDSL-Routern auch kabelgebunden angeschlossen werden. Die meisten Router von der Telekom bieten vier Netzwerkanschlüsse, sodass zusätzlich zum WLAN auch ein kleines Kabelnetzwerk aufgebaut werden kann. Je nach Einsatzzweck ist das sehr praktisch, denn Sie können zwei stationäre PCs im Arbeitszimmer per Kabel vernetzen und Daten austauschen, während Sie sich mit dem Notebook per WLAN ins Internet begeben. Sollen mehrere PCs per Kabel angeschlossen werden, benötigen Sie die entsprechende Anzahl Kabel.

1.5 Schnelles Internet via Funk

Ist UMTS bereits Vergangenheit? Mit LTE (Long Term Evolution) steht wieder ein neuer Mobilfunkstandard in den Startlöchern. LTE richtet sich bevorzugt an Anwender in ländlich vernachlässigten Gebieten, die immer noch nicht in den Genuss schneller Internetverbindungen gekommen sind. Über die Preise schweigen sich die Anbieter allerdings derzeit noch aus.

Bild 1.5 AVM präsentiert zur CeBIT 2011 erstmals eine FRITZ!Box für den neuen Mobilfunkstandard LTE. Damit bietet der Berliner Kommunikationsspezialist künftig für die wichtigen Zugangstechnologien LTE, Kabel und VDSL FRITZ!Box-Modelle an.

2 FRITZ!Box einrichten

Die FRITZ!Box stellt die Verbindung Ihres Computers und aller anderen netzwerkfähigen Geräte wie z. B. eines Notebooks oder iPads mit dem DSL-Anschluss und damit zum Internet her. Richten Sie eine FRITZ!Box erstmalig ein, gibt es für die Verbindung zwischen Box und Computer zwei Möglichkeiten: zum einen die Verbindung mit einem Ethernetkabel (Netzwerkkabel), zum anderen die drahtlose Verbindung über einen WLAN-Adapter.

Vorzugsweise verbinden Sie einen lokalen Desktop-PC oder noch besser ein transportables Notebook per Ethernetkabel mit der FRITZ!Box.

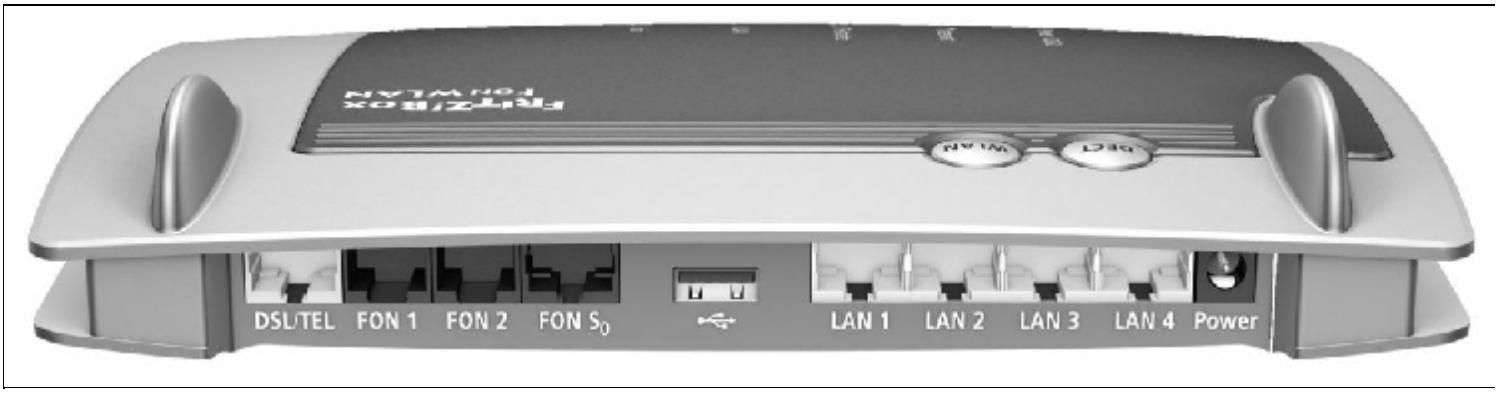


Bild 2.1 Die DSL/TEL-Buchse (links) stellt die Verbindung zum Internet Service Provider her.

Alle aktuellen Desktop-PCs verfügen bereits ab Werk über einen Netzwerkanschluss. Besitzt Ihr Rechner keinen Netzwerkanschluss, müssen Sie eine entsprechende Netzwerkkarte nachrüsten. Sie können aber auch direkt auf WLAN setzen und den PC über einen USB-WLAN-Adapter mit dem Router verbinden.

Bild 2.2 Hier der FRITZ!WLAN-USB-Stick N 2.4. Der neue Stick unterstützt WLAN N im 2,4-GHz-Frequenzbereich und erreicht Übertragungsraten bis zu 150 MBit pro Sekunde.

Achten Sie darauf, FRITZ!Box und Computer mit dem Kabel zu verbinden, das im Lieferumfang des Routers enthalten ist. Oft sind diese Kabel farbcodiert und werden in der Anleitung genau beschrieben. Erst wenn die Verbindung mit dem richtigen Kabel steht, schalten Sie Router und PC ein.

2.1 Erste Anmeldung an der FRITZ!Box

Für die erstmalige Anmeldung an der FRITZ!Box bekommt die Netzwerkschnittstelle per DHCP automatisch eine IP-Adresse zugewiesen. Ist das nicht der Fall, stellen Sie sie auf DHCP um. Danach kommen Sie ganz einfach über Ihren Webbrowser (Safari, Firefox, Opera oder Internet Explorer) in die Benutzeroberfläche des WLAN-Routers.

Starten Sie dazu Ihren Webbrowser und geben Sie die FRITZ!Box-Adresse in die Adresszeile des Webbrowsers ein. Die Adresse ist, unabhängig von Herstellungsjahr und Modell, bei der FRITZ!Box immer:

```
http://fritz.box
```

oder

```
http://192.168.178.1
```

In der Regel haben die FRITZ!Box-Modelle keinen Passwortschutz. Oftmals hat der Provider hier den WLAN-Schlüssel als Konfigurationspasswort gesetzt. Sind Sie auf der Konfigurationsseite der FRITZ!Box, wird dieser Schutz aus Sicherheitsgründen aktiviert und ein persönliches Passwort verwendet – allerspätestens nach Abschluss der Konfiguration sollten Sie es jedoch einstellen.

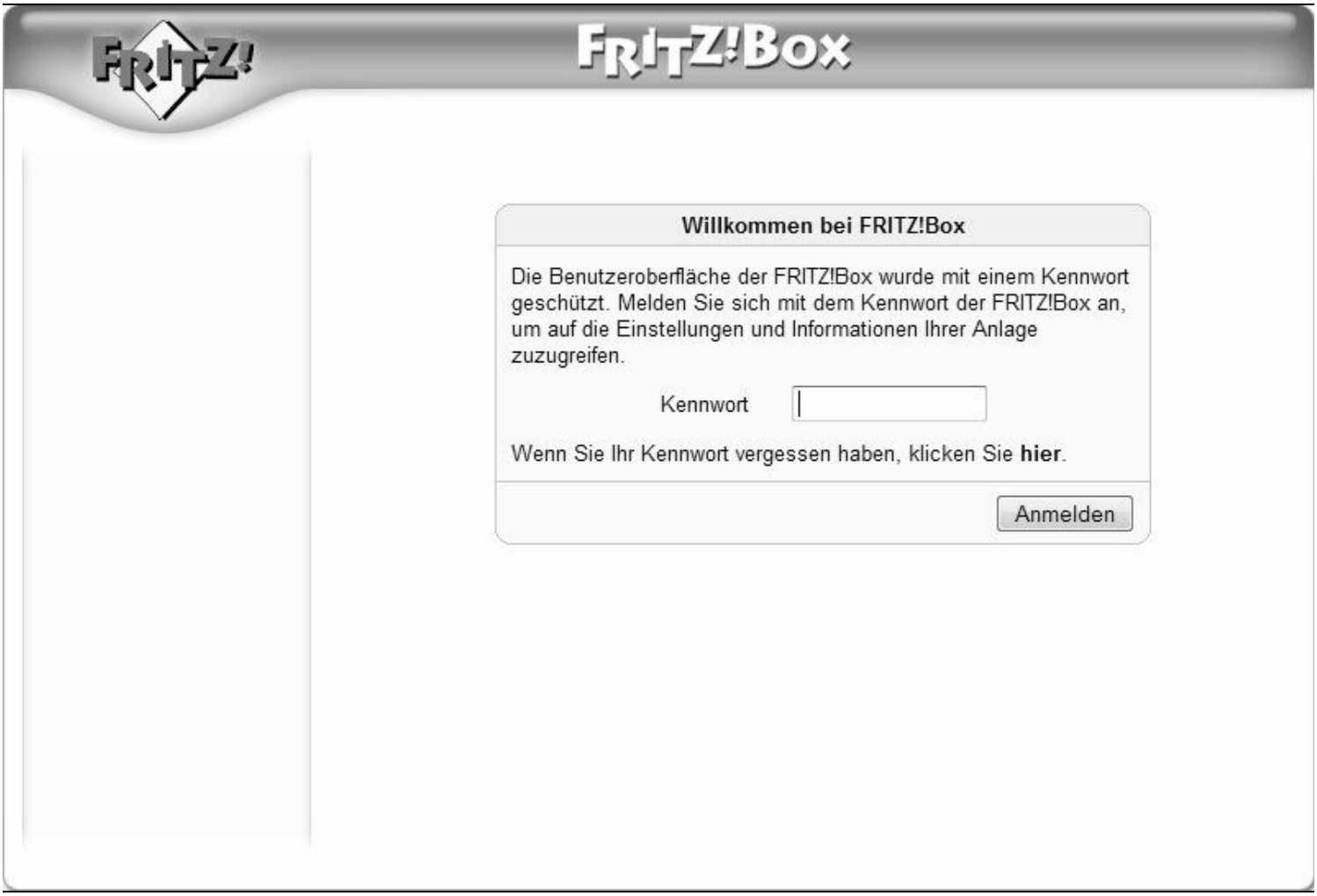


Bild 2.3 Aber sicher: Ein vernünftiger WLAN-Router sichert die Konfiguration per Zugangskennung ab.

Die Verbindung zur FRITZ!Box wird nicht aufgebaut?

Wenn keine Verbindung zum Router zustande kommt, sollten Sie folgendermaßen vorgehen:

1. Zunächst untersuchen Sie die Stromversorgung der FRITZ!Box – Stecker am Netz? Prüfen Sie die Position und den Sitz des Netzwerksteckers. Da bei älteren Modellen die Buchse für das Kabel zum DSL-Splitter und die Buchse für den ersten Netzwerkrechner nebeneinanderliegen, kann man sich leicht vertun.
2. Dann prüfen Sie die eingegebene IP-Adresse noch einmal auf Vertipper. Ist kein Schreibfehler zu sehen, heißt es, die Adresse erneut mit der Angabe im Handbuch abzugleichen.
3. Ist das Netzwerkkabel an Ihrem Rechner fest eingesteckt, und handelt es sich wirklich um die Netzwerkschnittstelle? Haben Sie das richtige Kabel verwendet? Meist sind die Kabel farbcodiert.

Wenn alles in Ordnung ist, sollte die FRITZ!Box nicht nur laufen, sondern auch auf die Kontaktaufnahme des PCs reagieren. Es gibt ganz seltene Fälle, in denen ein Kabel defekt ist. Bei fabrikneuen Geräten kann man das meist ausschließen, aber es kommt dennoch vor. Es ist also noch Testpotenzial vorhanden. Wir gehen aber davon aus, dass es bei Ihnen läuft.

Mit dem Assistenten durch die Erstinstallation

Ist der WLAN-Router in Ihrem Netzwerk angeschlossen, muss er konfiguriert werden. Abhängig vom Routermodell stehen dafür verschiedene Möglichkeiten zur Verfügung. Die FRITZ!Box prüft unmittelbar nach dem erstmaligen Einstecken des DSL-Routers die Netzwerkumgebung. Hier werden sämtliche angeschlossenen PCs sowie die Internetverbindung geprüft und, falls möglich, gleich konfiguriert. Zunächst ermittelt die FRITZ!Box, ob sie ordnungsgemäß an einem DSL-Splitter angeschlossen ist. Ist das der Fall, leitet ein Assistent durch die Erstinstallation.

Achten Sie darauf, die passenden Installations- und Konfigurationsparameter sowie den Benutzernamen und das Kennwort aus den Zugangsunterlagen Ihres Internet Service Providers griffbreit zu haben.

Bild 2.4 Ist die FRITZ!Box noch nicht konfiguriert, bietet ein Einrichtungsassistent an, das nach dem Einschalten vorzunehmen.

Werkseitig eingestelltes FRITZ!Box-Kennwort sofort ändern

Nach Abschluss der Erstkonfiguration sollten Sie die FRITZ!Box mit einem eigenen neuen Kennwort sofort gegen unerwünschte Veränderungen absichern. Denn es wäre ärgerlich, wenn all Ihre Mühe umsonst wäre, weil ein Spaßvogel im Heimnetz auf die FRITZ!Box zugreifen und die Einstellungen verändern könnte. Im Zweifelsfall kämen Sie selbst nicht mehr hinein.

Über den Webbrowser erreichen Sie per *Übersicht/Einstellungen/Erweiterte Einstellungen/System/FRITZ!Box-Kennwort* den entsprechenden Dialog. Am besten notieren Sie sich das Kennwort und bewahren es an einem sicheren Ort auf.

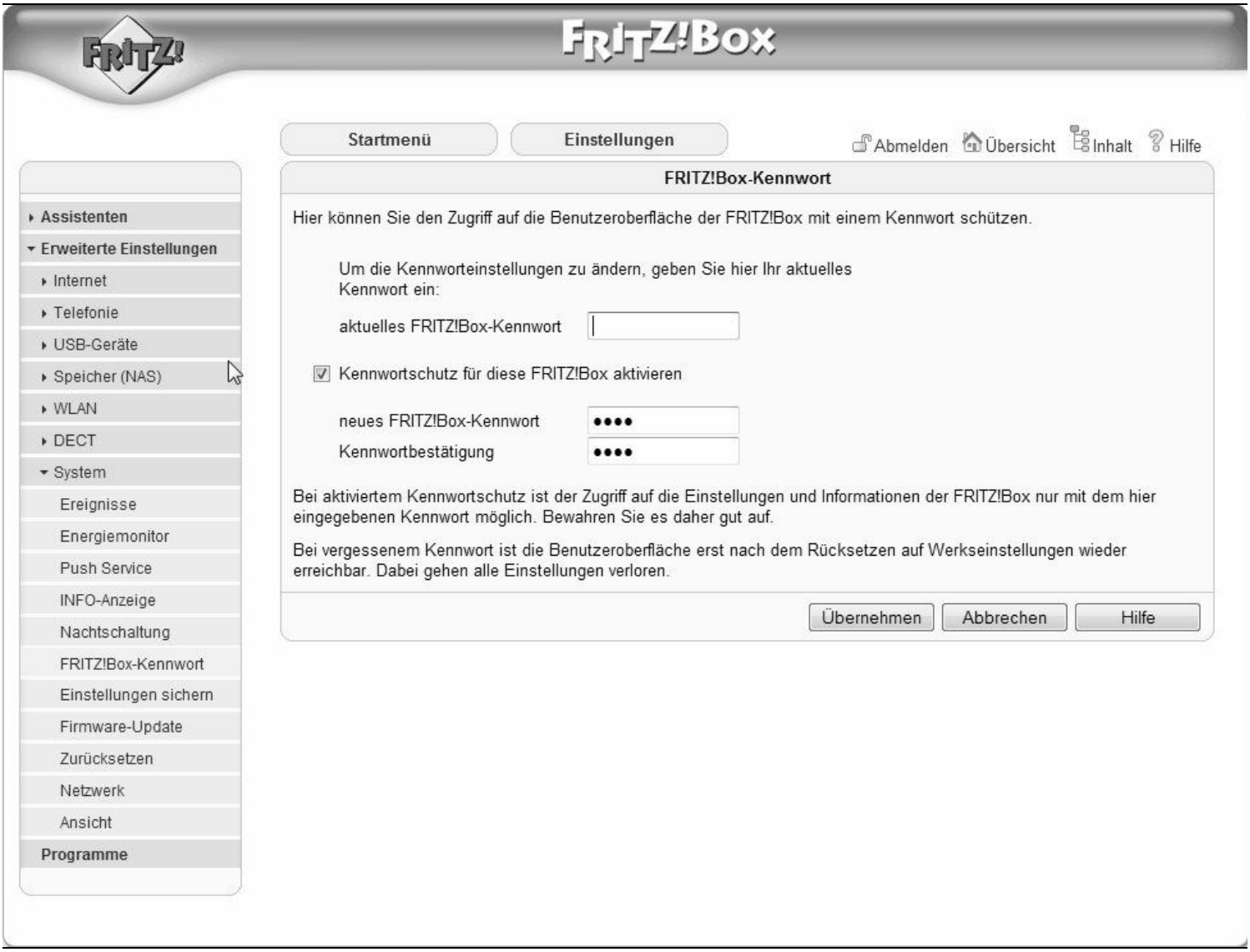


Bild 2.5 Damit der Kennwortschutz aktiviert werden kann, setzen Sie das Häkchen bei *Kennwortschutz für diese FRITZ!Box aktivieren*.

Wer die Internetverbindung selbst konfigurieren möchte, wählt bei der FRITZ!Box auf der Startseite der Weboberfläche den Punkt *Einrichtungsassistent* aus, der Schritt für Schritt die für eine Internetverbindung notwendigen Einstellungen abfragt. Hier brauchen Sie selbstverständlich die passenden Installations- und Konfigurationsparameter sowie den Benutzernamen und das Passwort aus den Zugangsunterlagen des Internet Service Providers.

2.2 Anpassen der Standardeinstellungen

Beim erstmaligen Einrichten des Routers können Sie möglicherweise die Standardeinstellungen ohne Änderungen übernehmen. Sicherer und für Fortgeschrittene empfehlenswert ist jedoch eine manuelle Konfiguration des Geräts.

Konfiguration der persönlichen Internetzugangsdaten

Die Konfiguration der Internetzugangsdaten nehmen Sie im Menü *Internet/Zugangsdaten* vor. Hier geben Sie den Konto- bzw. Benutzernamen ein. Falls Ihr Internetanbieter Ihnen einen bestimmten Hostnamen mitgeteilt hat (z. B. *X00132454*), geben Sie ihn hier an. Bei T-Online beispielsweise setzt sich der Log-in-Name aus zwei wesentlichen Komponenten zusammen: der geheimen Anschluss- und der Benutzerkennung, die jeweils aus zwölf Stellen bestehen. Achten Sie deshalb bei der Konfiguration auf die Reihenfolge Anschlusskennung + T-Online-Nummer + (#) Mitbenutzersuffix + @t-online.de. Ein möglicher Benutzername wäre demnach *111111111112222222222220001@t-online.de* .

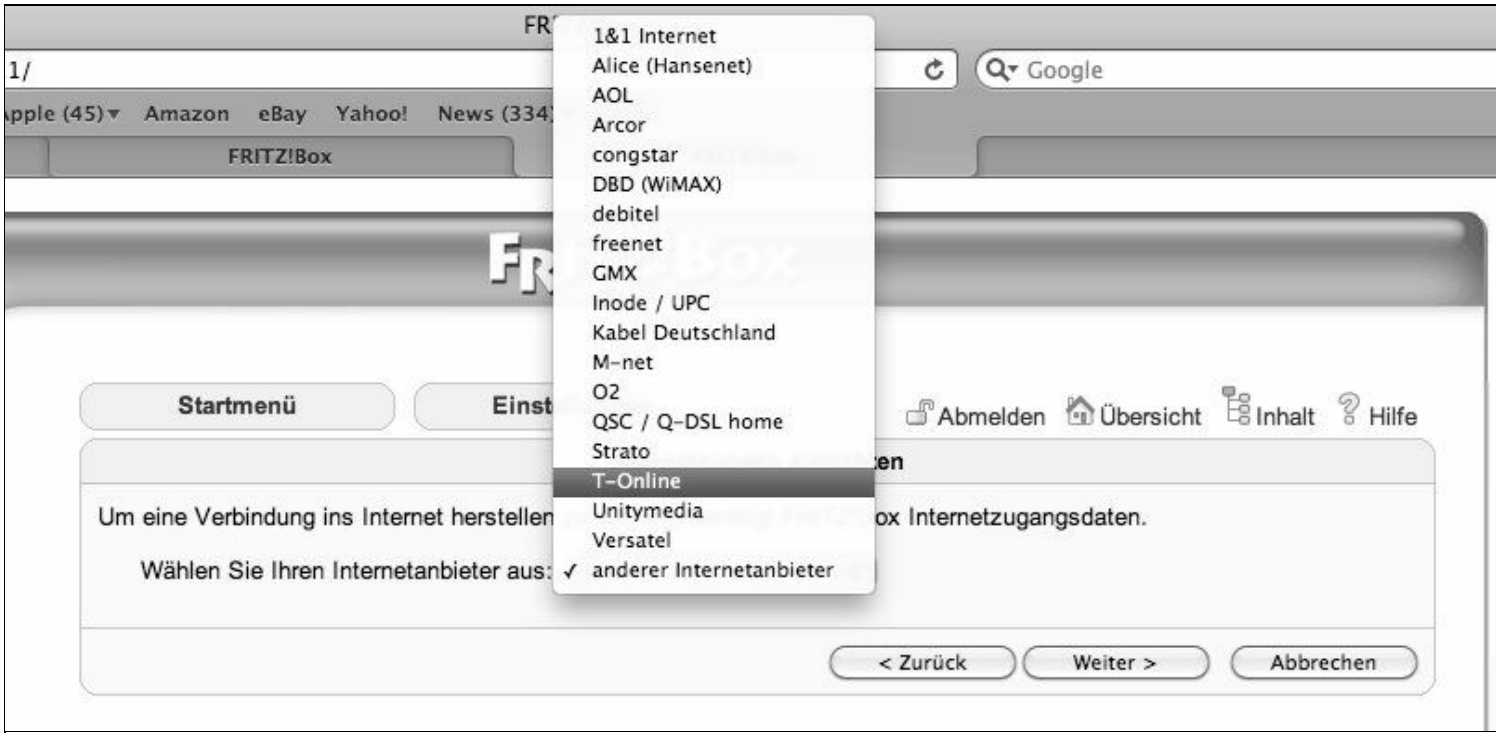


Bild 2.6 Hier wählen Sie zunächst den Anbieter aus dem Drop-down-Menü aus. Ist der gewünschte nicht dabei, wählen Sie die Option *anderer Internetanbieter*.

Für eine Verbindung ins Internet benötigt die FRITZ!Box eine IP-Adresse. Stellt die FRITZ!Box eine Verbindung zu Ihrem Internetanbieter her, bezieht sie automatisch eine IP-Adresse, die aus einem Adresspool des Internetanbieters zur Verfügung gestellt wird. Nur wenige Internetanbieter vergeben eine feste (oder statische) IP-Adresse – falls Sie eine solche haben, finden Sie die erforderlichen Informationen in den Unterlagen des ISP (*Internet Service Provider*).

In diesem Fall wählen Sie *Statische IP-Adresse verwenden* und tragen die IP-Adresse, die Subnetzmaske sowie die Gateway-IP-Adresse in die entsprechenden Felder ein. Bei der Internetkonfiguration der FRITZ!Box wählen Sie dafür im Bereich *Zugangsdaten* nicht die Option *Internetzugang über DSL*, sondern den Punkt *Internetzugang über LAN* aus. Anschließend lassen sich die vom ISP angegebenen IP-Adressparameter eintragen.

Pro und kontra: dynamische Vergabe von IP-Adressen

Die FRITZ!Box ist standardmäßig als DHCP-Server konfiguriert. DHCP (*Dynamic Host Configuration Protocol*) spielt seine Vorteile vor allem in großen Netzwerken aus. Damit bekommen alle an den Router angeschlossenen Computer – egal ob WLAN oder nicht – automatisch die TCP/IP-Konfiguration zugewiesen. Hersteller empfehlen meist, diese Einstellungen nicht zu ändern und den Router auch als DHCP-Server zu verwenden.

DHCP, die dynamische Vergabe von IP-Adressen im Netz, ist Segen und Fluch zugleich. Zunächst ist es für jeden Netzwerkeinsteiger praktisch, dass er sich um die Vergabe solcher IP-Adressen nicht kümmern muss. Das klappt genau so wie die Einwahl ins Internet. Wenn Sie sich jedoch nicht penibel an die Ratschläge zur Absicherung des Netzwerks halten und beispielsweise SSID-Broadcasting und Verschlüsselung nicht so ernst nehmen, ist die automatische Vergabe kritisch. Ein fremder »Besucher« bekommt automatisch eine IP-Adresse und kann sich im Netz bewegen, surfen und, und, und. Bei festen IP-Adressen ist zwar die Einrichtung aufwendiger, aber schon aufgrund der Zuordnung zu Ihren Computern eine Grundabsicherung in Sachen Netzwerkzugriff.

Besitzen Sie nur wenige Computer, die Sie mit Ihrer FRITZ!Box versorgen, ist es oft sinnvoller und sicherer, den DHCP-Server zu deaktivieren und die angeschlossenen Clients per Hand zu konfigurieren. Dadurch haben Sie nicht nur einen genauen Überblick darüber, welcher PC sich im Netzwerk mit welcher IP-Adresse befindet, sondern machen es möglichen Eindringlingen auch schwerer, sich eine IP-Adresse in Ihrem Heimnetz zu »besorgen«.

Ist DHCP aktiviert, tragen Sie bei der Option *IP-Anfangsadresse* die erste Adresse bzw. im Feld *IP-Endadresse* die letzte Adresse im zusammenhängenden IP-Adressbereich ein. Trotz DHCP können Sie auch eine IP-Adresse für einen PC im LAN reservieren. Damit erhält dieser PC immer dieselbe IP-Adresse, wenn er auf den DHCP-Server zugreift. Das ist besonders bei Servern der Fall, die oft permanente IP-Einstellungen benötigen, weil die Portweiterleitung aktiv ist.

Bild 2.7 Bei der FRITZ!Box ist der DHCP-Server ab Werk bereits eingeschaltet. Wer Detaileinstellungen vornehmen möchte, öffnet über das Menü *Erweiterte Einstellungen/System/Netzwerk* im Register *IP-Einstellungen* per Klick auf die Schaltfläche *IP-Adressen* die entsprechende Konfigurationsseite.

Ist die abgebildete Konfigurationsseite nicht erreichbar bzw. nicht sichtbar, müssen Sie möglicherweise zunächst die Expertenansicht aktivieren, die Sie über *Erweiterte Einstellungen/System/Ansicht* erreichen. Hier können Sie anschließend die IP-Adressparameter der FRITZ!Box verändern.

Wird die FRITZ!Box in ein bestehendes Heimnetz integriert, legen Sie im Bereich *IP-Adresse* diese entsprechend für Ihr Heimnetz fest. Nutzt Ihr Heimnetz beispielsweise den Bereich 192.168.123.X, weisen Sie der FRITZ!Box eine feste IP-Adresse (hier: *199*) zu. Bei einem aktivierten DHCP-Server lassen sich zudem noch die Anzahl der möglichen Clients und die zu vergebenden IP-Adressen einstellen.

Bild 2.8 Ist der DHCP-Server aktiviert, legen Sie hier auf Wunsch die Anzahl der möglichen nutzbaren IP-Adressen fest. Wird die IP-Adresse der FRITZ!Box geändert, sollten Sie sie sich auch merken, da diese Änderung dazu führen kann, dass die FRITZ!Box anschließend nicht mehr erreichbar ist.

Haben Sie beispielsweise nur fünf Geräte in Ihrem Netzwerk im Betrieb, können Sie die Adressvergabe auf diese fünf Geräte beschränken, indem Sie den Bereich entsprechend (beispielsweise von 20 bis 25) konfigurieren. Danach wird die IP-Subnetzmaske eingestellt, die den Netzwerkanteil der IP-Adresse angibt. Der Router berechnet automatisch die Subnetzmaske, basierend auf der zugewiesenen IP-Adresse. Sofern keine Subnetze zum Einsatz kommen, verwenden Sie 255.255.255.0 als Subnetzmaske.

Die IP-Adresse eines DNS-Servers eintragen

Je nach FRITZ!Box-Modell richten Sie nun den DNS-Server ein. Dieser wird zur Suche von Webadressen basierend auf ihren Namen verwendet und löst den DNS-Namen in einer IP-Adresse auf. Stehen in den ISP-Unterlagen eine oder zwei DNS-Serveradressen, tragen Sie einfach die primäre und die sekundäre Adresse im Konfigurationsdialog ein. In der Regel reicht der Eintrag *Automatisch vom ISP abrufen*, wenn der ISP den DNS-Server automatisiert zur Verfügung stellt. Näheres dazu finden Sie in Ihren Unterlagen zum DSL-Zugang.

Bei den meisten Modellen der FRITZ!Box ist das Konfigurieren der DNS-Serveradressen des ISP standardmäßig nicht möglich. Möchten oder müssen Sie mit dem PC dennoch einen anderen DNS-Server verwenden, muss bei der IP-Konfiguration des PCs die entsprechende IP-Adresse des gewünschten DNS-Servers eingetragen werden.

Hier wählen Sie über die Systemsteuerung bei *Netzwerkverbindungen* die Schnittstelle aus, die für den Internetzugang sorgt, und klicken dort auf *Eigenschaften*. Im Register *Allgemein* ist das TCP/IP-Protokoll zu finden – dort klicken Sie abermals auf *Eigenschaften*. Nun können Sie den Punkt *DNS-Adressen automatisch beziehen* auf *Folgende DNS-Serveradressen verwenden* umstellen und dort die IP-Adresse des gewünschten DNS-Servers eintragen. Nach dem

Neustart des PCs sind diese Netzwerkeinstellungen aktiv, und der in der FRITZ!Box eingetragene DNS-Server wird vom PC nicht mehr verwendet.

MAC-Adresse der FRITZ!Box konfigurieren

Im nächsten Schritt wird gegebenenfalls die MAC-Adresse der FRITZ!Box konfiguriert. Eine MAC-Adresse (Media Access Control) ist eine eindeutige Hardwareadresse in einem Netzwerk, die für zusätzliche Sicherheit beim Verbindungsaufbau sorgt, weil jeder Netzwerkkomponente eine eindeutige Adresse zugeordnet ist (in den meisten Fällen ist das die Netzwerkkarte). Selten kommt es vor, dass ein Internetanbieter nur eine bestimmte MAC-Adresse für den Internetzugriff zulässt, mit der (und nur mit der!) eine Verbindung zustande kommen darf. Bei älteren FRITZ!Boxen ist das Ändern der MAC-Adresse nicht ohne Weiteres möglich. Zwar existiert ein Weg über eine Recovery-Konsole via FTP, doch dieser ist ausschließlich Spezialisten vorbehalten. Zu groß ist hier das Risiko, dass die FRITZ!Box nach dem Eingriff nicht mehr startet. Die MAC-Adresse der FRITZ!Box finden Sie über die Kommandozeile heraus.

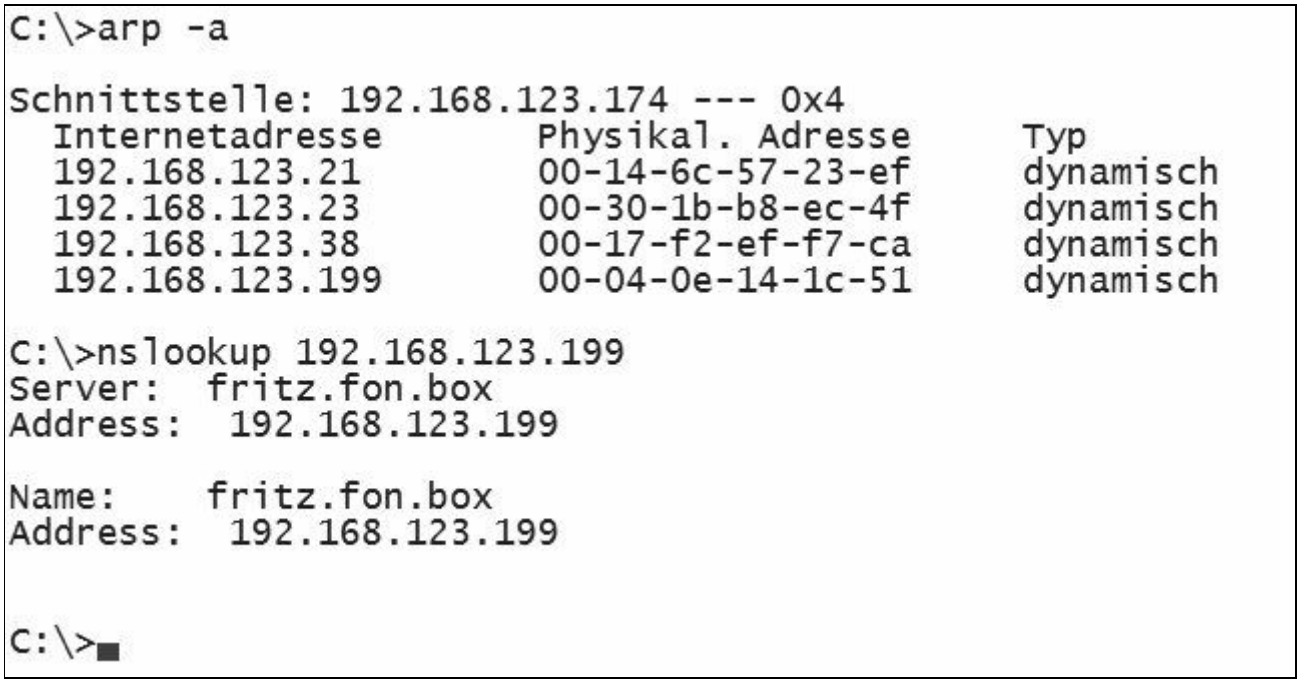


Bild 2.9 Mit dem Befehl *arp –a* im DOS-Fenster liefert *arp* zu jeder IP-Adresse die aktuell zugeordnete MAC-Adresse.

Bei neuen FRITZ!Box-Modellen bzw. FRITZ!Boxen mit einer aktuellen Firmware ist das Konfigurieren der MAC-Adresse etwas umständlicher gelöst. Damit Sie überhaupt an die Einstellung für die Netzwerkparameter herankommen, muss im Hauptmenü zunächst die sogenannte Expertenansicht aktiviert werden. Diese finden Sie über *Übersicht/Einstellungen/System/Ansicht/Expertenansicht aktivieren.*

Bild 2.10 Um die Einstellung für die Netzwerkparameter zu ändern, müssen Sie die *Expertenansicht* aktivieren.

Internetzugang über LAN 1

Das Ändern der IP- bzw. MAC-Adresse der FRITZ!Box ist nur dann möglich, wenn der Internetzugriff über die Option *Internetzugang über LAN 1* konfiguriert ist. In diesem Fall ist die FRITZ!Box an ein bereits vorhandenes Netzwerk (LAN) oder einen anderen DSL-Router angeschlossen, der die Zugangsdaten für den Provider für das Netzwerk zur Verfügung stellt.

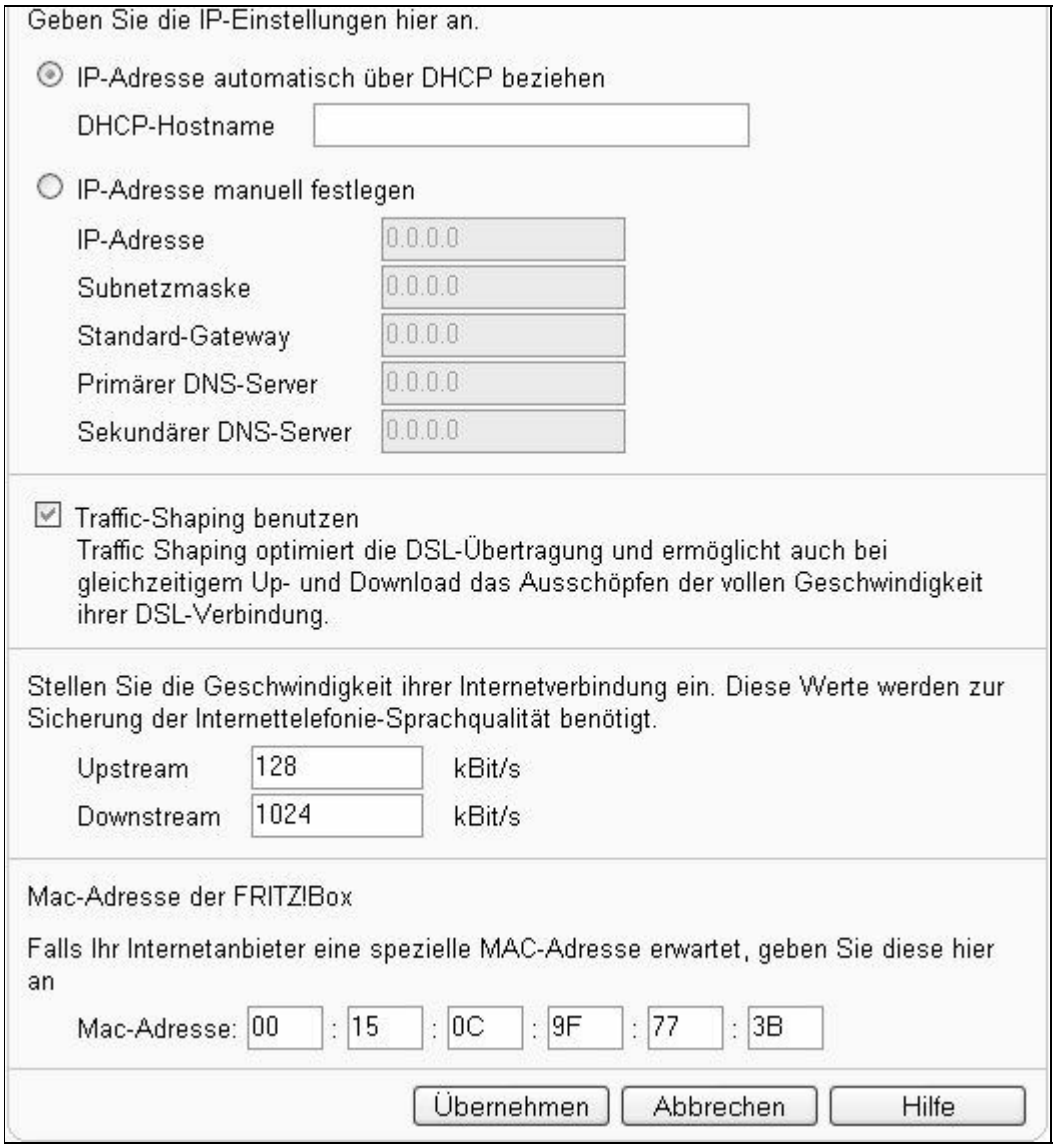


Bild 2.11 Erwartet der Internetanbieter eine spezielle MAC-Adresse für die Internetverbindung, tragen Sie diese hier ein.

Dauerhafte Internetverbindung oder mit Zeittakt?

Internetverbindung ist nicht gleich Internetverbindung. Obwohl die meisten Komplettangebote eine Flatrate bieten, kann es sein, dass sich für manche Zwecke der Stundentarif lohnt, der nach einem bestimmten Zeittakt und Tarif zu bezahlen ist. Abhängig vom Vertrag (Flat/Stundentarif etc.) mit Ihrem Internetanbieter kann die falsche Konfiguration des DSL-Routers dann richtig Geld kosten: Ist er falsch eingestellt, hält der Router die Internetverbindung rund um die Uhr aufrecht, auch wenn kein Rechner angeschaltet ist.

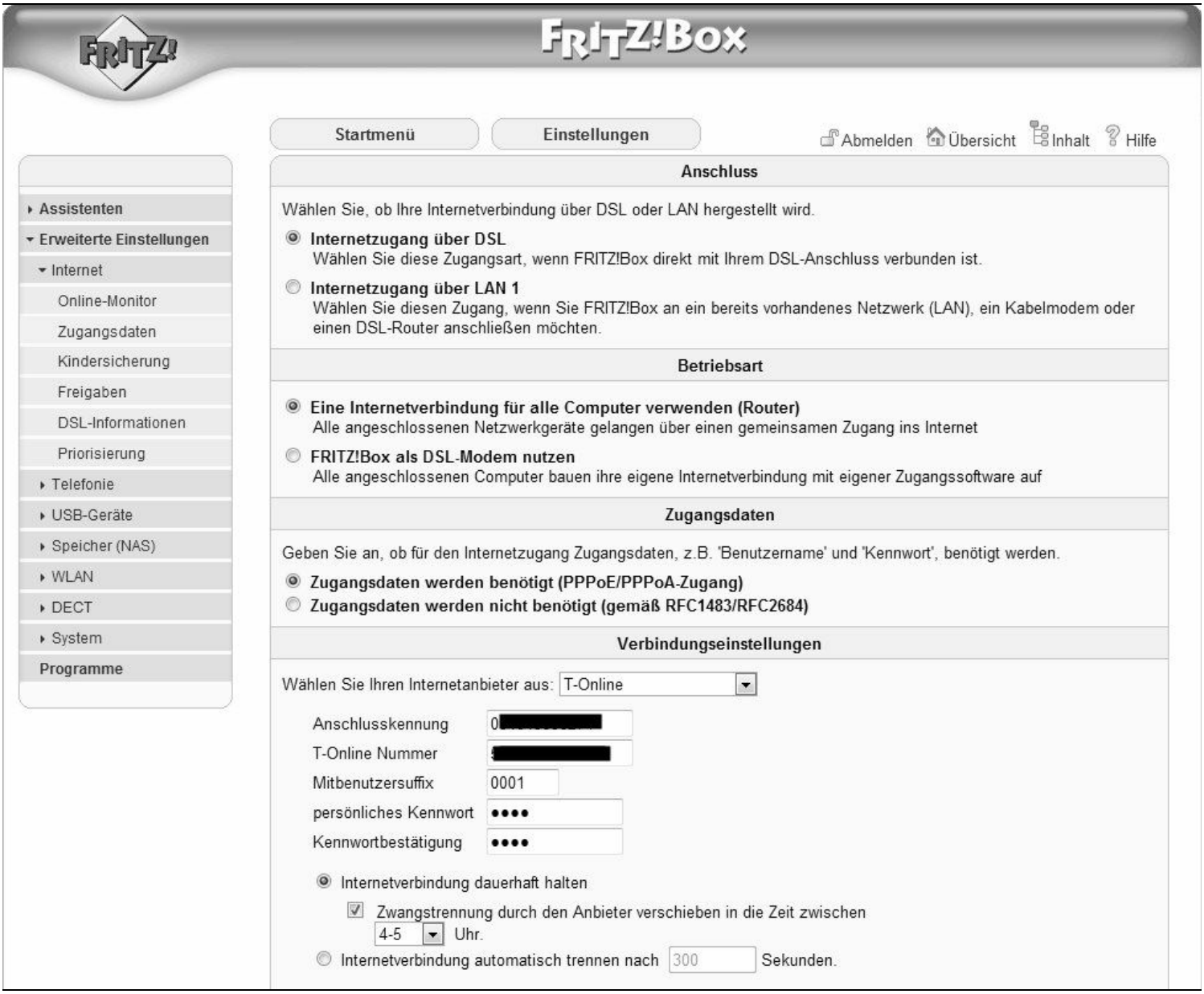


Bild 2.12 Über die Weboberfläche unter *Übersicht/Erweiterte Einstellungen/Internet/Zugangsdaten* prüfen Sie im Bereich *Verbindungseinstellungen bei der Option Internetverbindung dauerhaft halten* die Verbindungseinstellungen der FRITZ!Box.

Haben Sie eine Flatrate, kann diese Option normalerweise aktiviert bleiben. So wird die Internetverbindung nach jedem Time-out automatisch hergestellt, wenn der Router aus dem Heimnetz Verbindungswünsche mit dem Internet feststellt.

Wenn andere Funknetze stören, hilft ein Kanalwechsel

Beim Funkkanal können Sie häufig die Werkeinstellung beibehalten, es sei denn, es machen sich Störstrahlungen von einem anderen WLAN-Router in der Umgebung bemerkbar. Dies zeigt sich vor allem in Schwierigkeiten beim Verbindungsaufbau und in der Geschwindigkeit. Hängen in der Nachbarschaft einige andere WLAN-Router an der Steckdose, kann das Umkonfigurieren des Kanals einen Geschwindigkeitsschub bringen.

So läuft das WLAN wieder wie geschmiert: Im Konfigurationsmenü Ihres WLAN-Routers stehen Ihnen 13 Kanäle zur Verfügung. Dabei beträgt der Abstand der Mittenfrequenzen jeweils 5 MHz. Bedingt durch die große Bandbreite jedes einzelnen Funkkanals, kommt es zu Überschneidungen der Frequenzbänder. Wird Ihr WLAN immer langsamer oder bricht die Verbindung ganz ab, ist das in den meisten Fällen auf eine Überschneidung mehrerer Funkkanäle zurückzuführen. Für beste Funkqualität sollten daher alle im Umkreis befindlichen WLANs mit einem Abstand von fünf Kanälen betrieben werden. Sendet Ihr Nachbar in seinem WLAN auf Kanal 6, wechseln Sie zu Kanal 1, 11, 12 oder 13, und Ihr WLAN läuft wieder wie geschmiert.

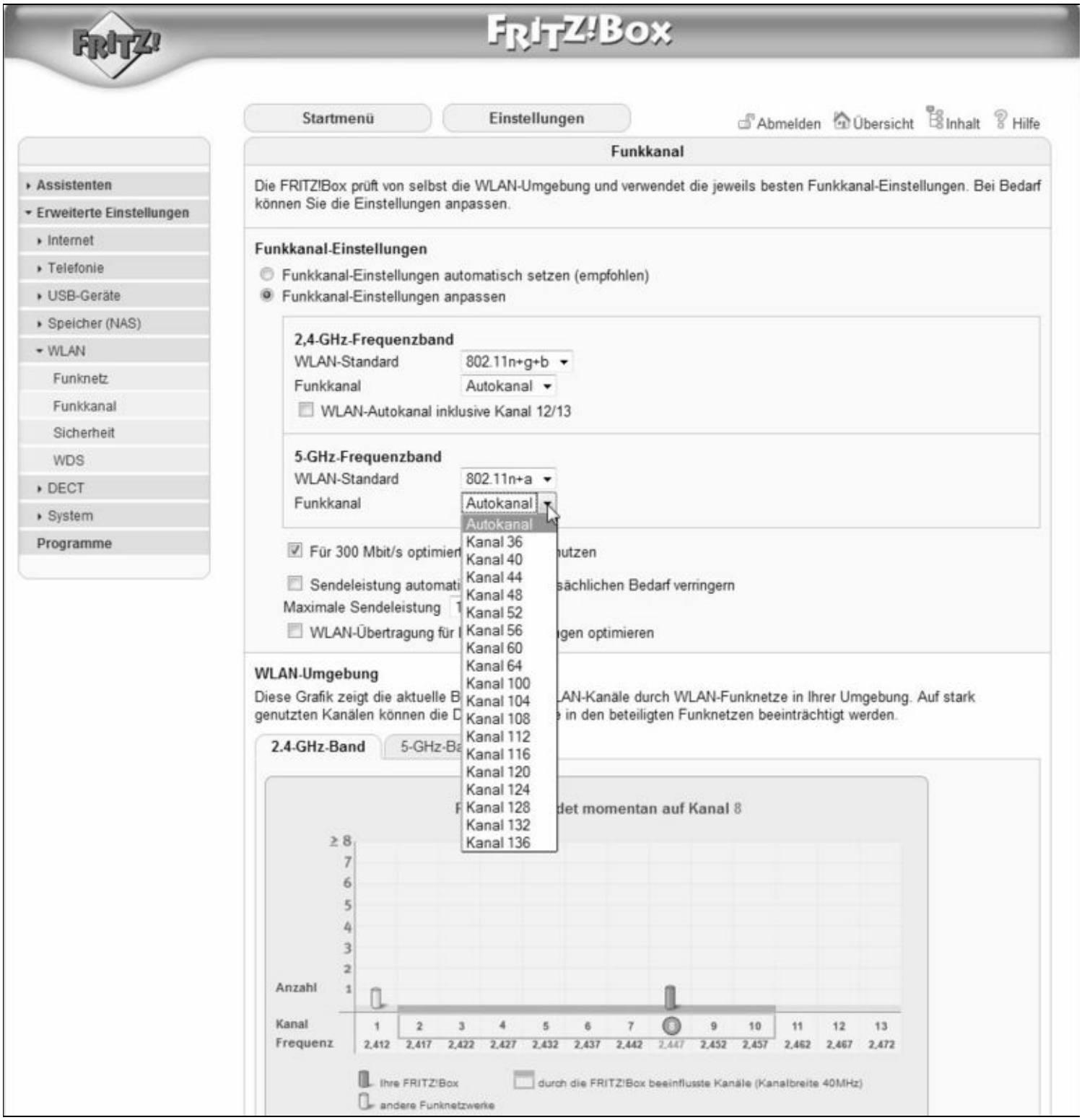


Bild 2.13 FRITZ!Box-Spezialität: Kommt es auf einem Kanal zu Übertragungsspitzen, wechseln Sie in diesem Dialog einfach den Kanal. Hier lassen sich die Kanäle des 2,4-GHz- und des 5-GHz-Frequenzbands getrennt konfigurieren.

Feintuning der WLAN-Geschwindigkeit: Wer keine Uraltgeräte (mit dem alten 802.11b-Standard) mehr im Einsatz hat oder haben möchte, wählt im Drop-down-Menü bei *WLAN-Standard* anstelle des Standardeintrags *802.11n+g+b* die Einstellung *802.11n+g* aus. Damit verhindern Sie, dass ältere Geräte nach dem b-Standard das WLAN-Netz auf 11 MBit/s drosseln.

Portfreigaben für die Internettelefonie festlegen

Wer mit seinem Computer über das Internet telefonieren möchte, sollte darauf achten, dass die Konfiguration der Firewall bzw. des DSL-WLAN-Routers vornehmlich von der eingesetzten SIP-Software auf dem Rechner abhängig ist. Da eine NAT-Firewall (*Network Address Translation*) nach außen eine IP-Adresse und nach innen im Heimnetz mehrere IP-Adressen zu versorgen hat, kann es beim Telefonieren hier anfänglich zu Problemen kommen, sollte NAT, also die Portweiterleitung, falsch konfiguriert sein. NAT macht nichts anderes, als eine IP-Adresse in einem Datenpaket durch eine andere zu ersetzen. Bei einem Router bzw. einer Firewall sorgt NAT dafür, private IP-Adressen auf öffentliche IP-Adressen abzubilden.

Bei NAT kennt der Telefonieclient die aktuelle Internet-IP-Adresse nicht, er besitzt ja eine lokale nach dem Muster *192.168.X.X*. Deshalb nutzen die SIP-Gateways die Absender-IP-Adresse, also die Internetadresse des DSL-WLAN-Routers. Dafür ist der STUN-Server (*Simple Traversal of UDP through NAT*) des VoIP-Anbieters zuständig. Der versorgt den Telefonieclient mit den nötigen Informationen, damit es mit dem Telefonieren auch funktioniert.

Eine Firewall bzw. ein DSL-WLAN-Router kann nur Daten von außen zu einem bestimmten Client transportieren, wenn bekannt ist, wohin diese weitergeleitet werden müssen. Dafür sorgt der interne Initialisierungsvorgang der SIP-Software bzw. des IP-Telefons. Damit das Telefonieren mit einer NAT-Firewall auch erfolgreich verläuft, müssen in der Regel folgende Ports konfiguriert sein:

Benötigte Ports*	Programm/Protokoll
80 (TCP)	Freigabe, Registrierung
3478–3479 (UDP)	NAT/STUN (STUN ist nur notwendig, wenn NAT benutzt wird)
5004 (UDP)	RTP
5060 (UDP)	SIP Signal Telefon
5062 (UDP)	SIP Signal Anrufbeantworter
5069 (UDP)	iPhone Freenet
5070, 5072 (UDP)	1&1 SoftPhone, Nero SIPPS
8000–8006 (UDP)	X-Lite
8000–8012 (UDP)	X-Pro
10000–10012 (UDP)	Datenverkehr Nikotel-Telefon
16384–16390 (UDP)	Datenverkehr Freenet-iPhone
30000–30012 (UDP)	Datenverkehr Nikotel-Anrufbeantworter
* Alle ein- und ausgehenden UDP- und TCP-Ports.	

Für SIP wird in der Regel immer UDP-Port 5060 benötigt. Meist überwacht eine Firewall nur den eingehenden Datenverkehr, teure und restriktive Produkte sorgen jedoch auch beim ausgehenden Datenverkehr für Sicherheit.

Bild 2.14 Bei der FRITZ!Box ist für die Internettelefonie via PC unter *Portfreigabe* jeder notwendige Port einzutragen.

Für VoIP sind in der Firewall bzw. Portfreigabe meist zusätzlich die Ports 5062, 5070, 5072, 3478 und 30000 bis 30005 freizugeben, damit das Telefonieren auch möglich ist. Hier aktivieren Sie *port forwarding* für die oben angegebenen Ports und leiten sie auf den Rechner um, von dem aus ins Internet telefoniert wird.

Durch die Umleitung der Daten, die auf Port 5060 auf dem Router bzw. der Firewall eintreffen, sorgt dieser Mechanismus dafür, dass sie an den vorgesehenen Rechner im Netzwerk weitergeleitet werden. Der ist nach außen von der Firewall geschützt und außerhalb des Routers bzw. der Firewall nicht direkt erreichbar. Abhängig davon, welches SIP-Programm verwendet wird, können noch zusätzliche oder andere Ports maßgeblich sein. Kommt es hier zu Problemen, hilft die Suche in den Foren bzw. auf der Website des jeweiligen Herstellers weiter.

Mit aktivierter Nachtschaltung sparen Sie Strom

Trotz Flatrate wird der Internetzugang in den wenigsten Fällen rund um die Uhr benötigt. Gerade wer die WLAN-Schnittstelle der FRITZ!Box für den Internetzugang nutzt, kann mit etwas Feinkonfiguration ein paar Kilowatt Strom sparen. Drücken Sie vor dem »Zubettgehen« manuell den WLAN-Schalter am FRITZ!Box-Gehäuse, haben Sie die WLAN-Funktion einfach per Knopfdruck ausgeschaltet.

Wem das zu umständlich ist, der kann dafür auch die Nachtschaltungsfunktion der FRITZ!Box nutzen, mit der sich die WLAN-Funktionen für einen definierten Zeitraum komplett ausschalten lassen. Sie aktivieren die Nachtschaltung unter *Übersicht/Erweiterte Einstellungen/System/Nachtschaltung*.

!&fritz7390-40.tif!

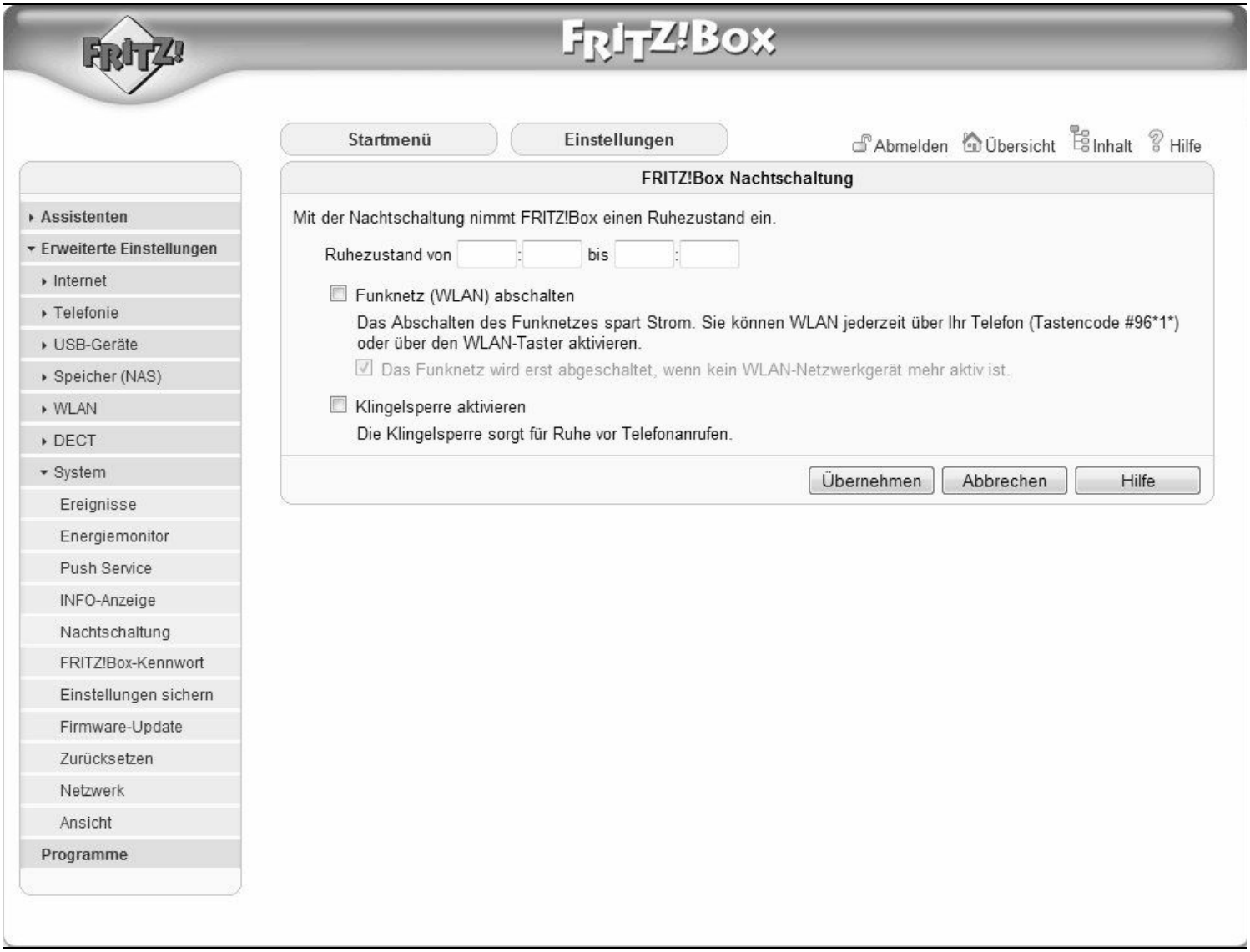


Bild 2.15 Wer nachts ruhig schlafen möchte, kann neben der Nachtschaltung auch per Mausklick eine nächtliche Klingelsperre aktivieren, die für Ruhe vor Telefonanrufen über die Anschlüsse der FRITZ!Box sorgt.

Nutzen Sie die WLAN-Funktion zudem nur in den eigenen vier Wänden – beispielsweise nur in einem Raum –, können Sie zusätzlich Strom sparen, indem Sie die Funkleistung der FRITZ!Box reduzieren. Das sorgt nicht nur für weniger Strahlung im Haus, sondern auch für weniger Störsignale in der Nachbarschaft sowie etwas mehr Schutz vor ungebetenen Eindringlingen, da die reduzierte WLAN-Funkleistung im Idealfall an der Hauswand scheitert.

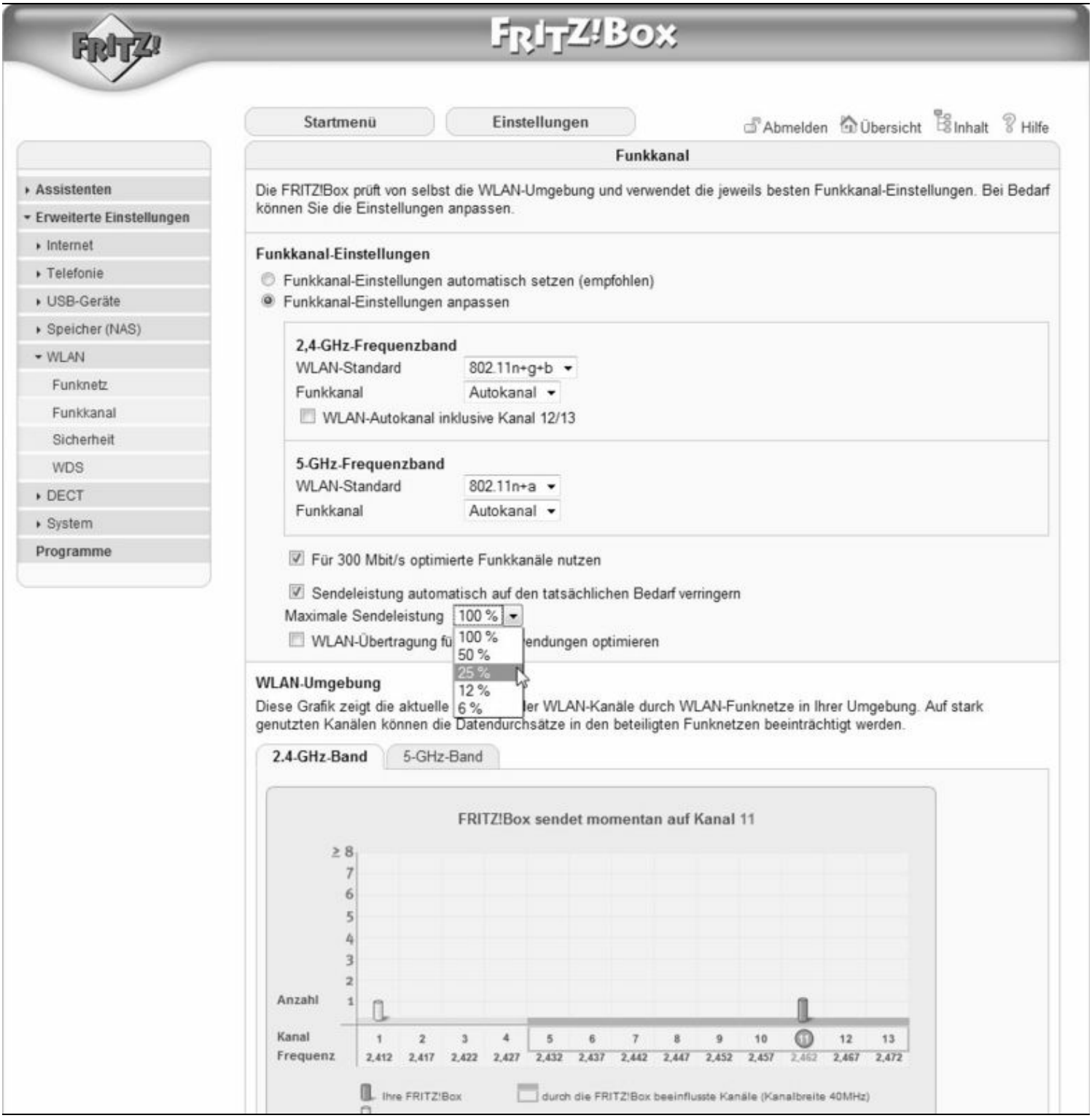


Bild 2.16 Die Hauswand als natürliche Firewall: Kommen die eingesetzten WLAN-Geräte ausschließlich in einem einzigen Raum zum Einsatz, ist eine reduzierte Sendeleistung völlig ausreichend.

Wird nur wenig Energie benötigt, um die Verbindung zum Internet herzustellen, wird bei aktiviertem TCP (Transmission Power Control) auch die Funkleistung auf die tatsächlich benötigte Energiemenge reduziert. Über die Benutzeroberfläche der FRITZ!Box stellen Sie die Funkleistung auf Ihre persönliche Umgebung zu Hause ein.

3 FRITZ!Box-Sicherheit

Das Aufsetzen eines drahtlosen Netzwerks ist leichter, als Sie denken. Normalerweise genügen ein Browser und die Eingabe der wichtigsten Standardeinstellungen, und dann kann es losgehen mit dem kabellosen Surfvergnügen. Doch wollen Sie auf Nummer sicher gehen, sollten Sie vorher das WLAN-Netzwerk dicht machen, damit niemand anderer als Sie selbst über das Funknetz arbeiten kann. Denn: Viele Schmarotzer können auf Ihre Kosten mitsurfen.

3.1 Grundlegende Sicherheitseinstellungen

Haben Sie eine Flatrate, gibt es zwar bezüglich der Kosten keinen Unterschied, steht jedoch eines Tages bei Ihnen der Staatsanwalt vor der Haustür, hat ein Eindringling möglicherweise über Ihren Internetanschluss Unfug getrieben. Deshalb sollten Sie die vorhandenen Sicherheitsmechanismen des Routers nicht nur kennen, sondern auch nutzen.

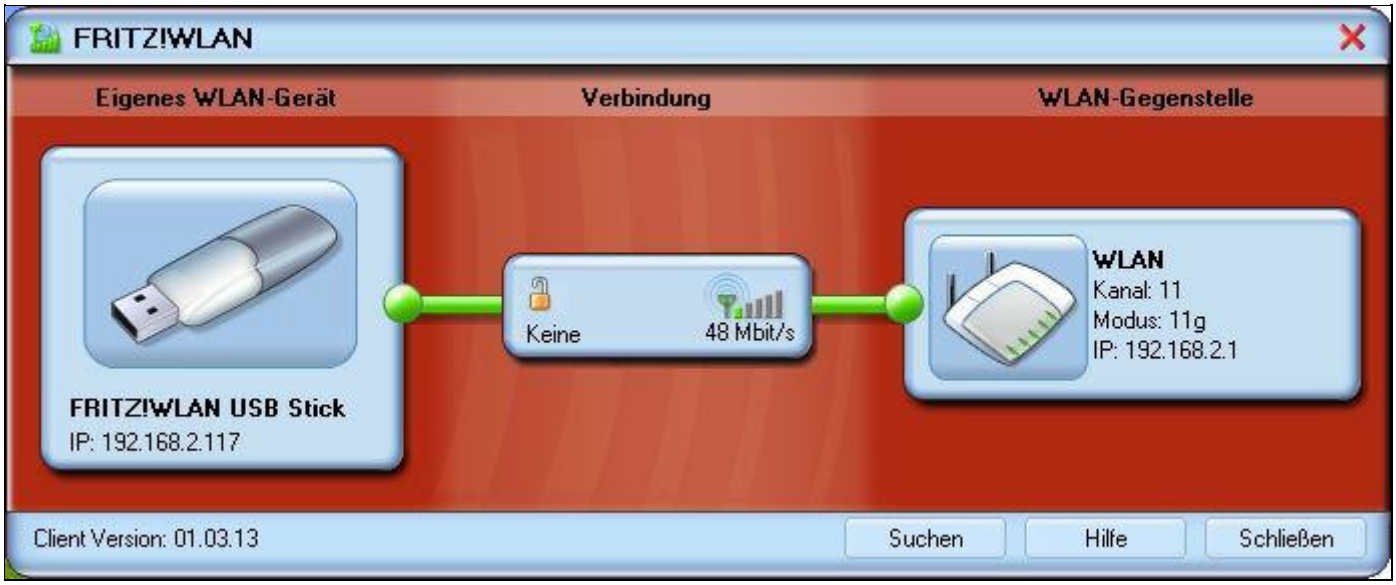


Bild 3.1 Ausprobiert: Das ungesicherte Funknetz *WLAN* kann problemlos angesprochen werden – ganz einfach mit einem USB-WLAN-Adapter.

So machen Sie die SSID für andere unsichtbar

Das Wichtigste für eine sichere WLAN-Konfiguration ist eine sichere und unsichtbare SSID (Service Set Identifier) . Mit der SSID ist nach Abschluss der Konfiguration das WLAN für die Umgebung sichtbar. Jeder, der sich an das Netz anmelden möchte, benötigt diesen Netzwerknamen (SSID), und sämtliche WLAN-Geräte müssen ihn kennen. Funknetze werden in der Standardeinstellung mit dieser Kennung angezeigt, die Kennung wird sozusagen mitgesendet.

Ändern Sie sofort die Standardeinstellung des Herstellers. Die FRITZ!Box hat im Auslieferungszustand als SSID meist den Namen des Geräts eingetragen, z. B. FRITZ!Box Fon WLAN 7390. Der ist für potenzielle Angreifer nicht nur zu sehen, sondern bei verborgener SSID dennoch leicht zu erraten, er wird auch in den Supportforen der Hersteller für jedes Routermodell genannt.

Ein sicherer SSID-Name besteht aus einer zufälligen Reihenfolge von Zahlen und Buchstaben, gemischt mit Groß- und Kleinbuchstaben. Möglich ist auch eine nur Ihnen bekannte Kombination aus persönlichen Daten, Namen sowie Groß- und Kleinschreibung (z. B. MeineOmaIngridhatte3Hundeund2Katzen!).

Konfigurieren Sie eine neue SSID und notieren Sie sich diese Kennung auf einem Zettel, der sich im WLAN-Handbuch befindet, die FRITZ!Box bietet Ihnen aber auch das Ausdrucken der Einstellungen an. Wer ganz auf Nummer sicher gehen möchte, ändert in regelmäßigen Abständen diesen SSID-Namen, um es etwaigen Eindringlingen auf Dauer schwer zu machen.

Das ist natürlich nur dann richtig sinnvoll, wenn die Rundumsendung der SSID (SSID-Ratio) versteckt wird. Der SSID-Name der FRITZ!Box lässt sich im Menü *Übersicht/Einstellungen/WLAN/Funkeinstellungen* bzw. bei den aktuellen Firmwareversionen über *Übersicht/Erweiterte Einstellungen/WLAN/Funknetz* ändern.

Bild 3.2 Spezialität der topaktuellen FRITZ!Box 7390: Erst wenn das Häkchen bei *2,4-GHz-Frequenzband* und/oder *5-GHz-Frequenzband* gesetzt ist, lässt sich der Name der SSID auf einen beliebigen Namen setzen.

Profis richten das WLAN-Netzwerk mit einem sicheren SSID-Namen ein und deaktivieren anschließend das SSID-Ratio – also das Versenden des SSID-Namens an die Umgebung. Bei der FRITZ!Box nehmen Sie hierfür das Häkchen bei *Name des Funknetzes (SSID) bekannt geben* heraus. Nur passend konfigurierte WLAN-Karten und WLAN-VoIP-Telefone können anschließend den WLAN-Router noch sehen und mit ihm Verbindung aufnehmen. Damit haben Sie schon viel für die Absicherung getan, denn eine komplizierte SSID, die man nicht einfach erraten kann, muss von einem potenziellen Hacker erst einmal herausgefunden werden.

Manchmal praktisch: Neuere FRITZ!Boxen wie die FRITZ!Box Fon WLAN 7390 bzw. *neuere* Firmwareversionen lassen hier auch eine getrennte Handhabung des 2,4-GHz- bzw. 5-GHz-Frequenzbands zu. So lassen sich ältere WLAN-Geräte mit einer anderen SSID betreiben – sprich, die FRITZ!Box drosselt die Geschwindigkeit der schnellen WLAN-Geräte nicht auf den kleinsten gemeinsamen Standard.

Verfahren für die Verschlüsselung von Funknetzen

Ebenso wichtig wie die SSID ist die Verschlüsselung des WLAN. Damit sich beispielsweise Nachbarn nicht per Funk über die FRITZ!Box in das Internet einwählen können, sollten, neben dem Verzicht auf die SSID-Rundumsendung, unbedingt die WEP- oder WPA-/WPA2-Sicherheitsoptionen aktiviert werden.

Die Standards sind unterschiedlich sicher (WEP ist vergleichsweise unsicher, WPA2 bisher nicht knackbar), ihre Verwendung hängt aber von den genutzten Geräten ab. Ältere Geräte können über USB-Adapter auch zur Unterstützung moderner Standards gebracht werden, entscheidend ist letztlich der Router.

Das am häufigsten eingesetzte Verfahren zur Verschlüsselung ist bei älteren WLAN-Routern WEP, das für Wired Equivalent Privacy steht – übersetzt etwa kabelnetzäquivalenter Schutz. Beim Einsatz von WEP ist ein sogenannter Netzwerkschlüssel für die Verschlüsselung notwendig. Diesen können Sie bei der Konfiguration des Routers selbst eingeben. WEP ist allerdings problemlos innerhalb einiger Minuten knackbar. Das sollten Sie wissen. Wenn Sie also nur auf WEP setzen können, weil Ihre Netzwerkgeräte keine andere Verschlüsselungstechnologie unterstützen, müssen Sie regelmäßig den Schlüssel und idealerweise auch die SSID wechseln.

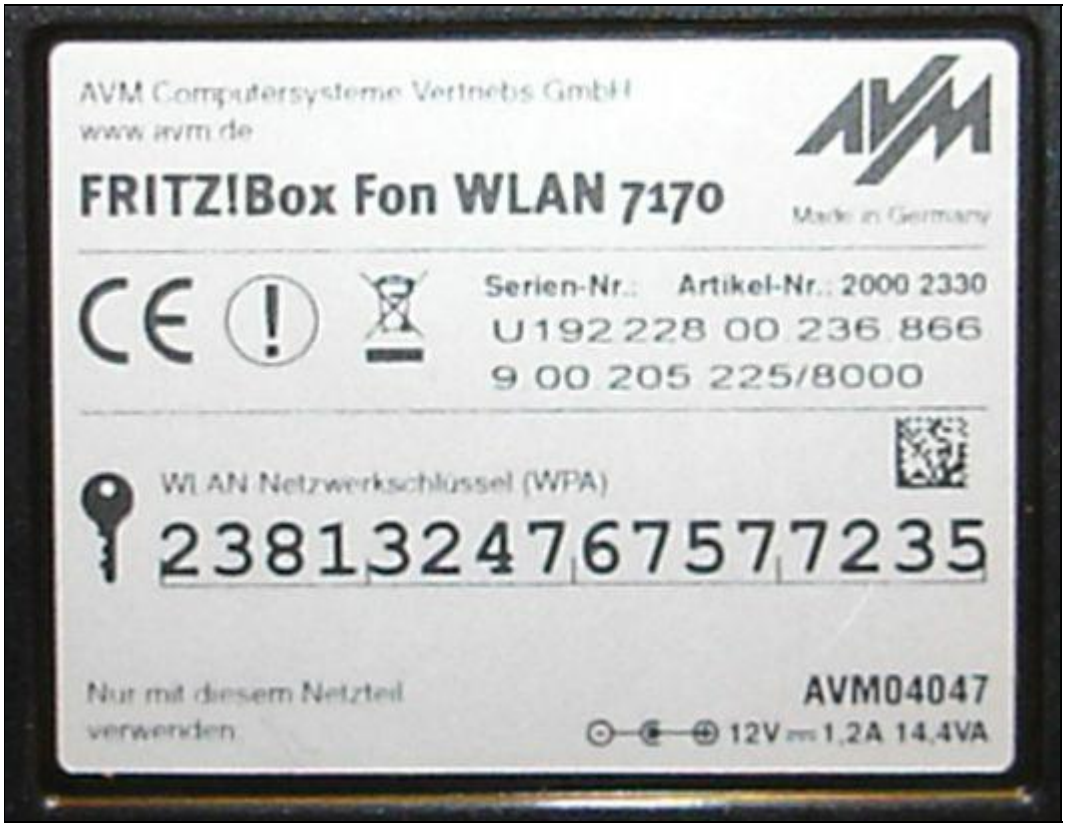


Bild 3.3 Neuere FRITZ!Box-Modelle sind ab Werk schon mit einem sicheren WPA2-Schlüssel vorkonfiguriert. Dieser befindet sich auf der Bodenplatte des Geräts.

Abhängig von der Geräteinfrastruktur im Heimnetz, sind unterschiedliche Schlüssellängen möglich. Im Zweifelsfall nutzen Sie den längsten Schlüssel. Denn je länger der Schlüssel ist, desto sicherer ist auch die Datenübertragung. So sind meist eine 64-Bit-Verschlüsselung (auch manchmal 40 Bit genannt) und eine 128-Bit-Verschlüsselung möglich. Abhängig vom »kleinsten gemeinsamen Nenner« stehen hier folgende Optionen zur Verfügung:

Schlüsseltypen	Beschreibung
Deaktivieren	Keine Datenverschlüsselung (nicht zu empfehlen).
WEP (Wired Equivalent Privacy)	64-Bit- oder 128-Bit-WEP-Datenverschlüsselung verwenden (nutzen, wenn die übrigen WLAN-Geräte kein WPA-PSK oder WPA2 unterstützen). Wenn WEP aktiviert ist, können Sie die vier Datenschlüssel manuell eingeben oder automatisch erstellen lassen. Diese Werte müssen auf allen PCs und Access Points in Ihrem Netzwerk identisch sein und verwendet werden.
WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)	WPA-PSK-Standardverschlüsselung verwenden (empfohlen). Manche WLAN-Karten unterstützen diese Verschlüsselung nicht. In diesem Fall nutzen Sie 128-Bit-WEP. Auch hier ist ein Verschlüsselungswert erforderlich.
WPA2-AES (Advanced Encryption Standard)	Bieten der Router und die angeschlossenen Geräte WPA2 oder WPA-AES an, sollte aus Sicherheitsgründen diese Verschlüsselung genutzt werden. Dieser Sicherheitsstandard ist derzeit das Maß aller Dinge und in Verbindung mit einem nicht erratbaren Schlüsselwert eine sichere Sache.

Ende des Jahres 2004 wurde WPA2, also die 802.11i-Spezifikation für WLANs, festgelegt. Dafür ist in der Regel neue Hardware, beispielsweise ein WLAN-Router sowie passende WLAN-Karten, notwendig. WPA2 verwendet statt des

Verschlüsselungsprotokolls RC4 den sichereren *Advanced Encryption Standard* (AES). Nutzen Sie immer die aktuellste Verschlüsselung.

Beim Kauf immer auf WPA2-Kompatibilität achten

Achten Sie beim Kauf von WLAN-Komponenten auf die WPA2-Kompatibilität, es ist ärgerlich, nur aufgrund eines Geräts die Sicherheit des gesamten WLAN-Netzes zu schwächen. Wenn für eine ältere FRITZ!Box eine aktuelle Firmware angeboten wird, können Sie auch auf moderne Verschlüsselungsstandards umstellen.

So erstellen Sie einen einfachen WEP-Schlüssel

Beim Erstellen eines Sicherheitsschlüssels im WEP-Verfahren stehen meist zwei unterschiedliche Methoden zur Verfügung: Sie können entweder den Schlüssel automatisch erstellen lassen oder selbst manuell einen eingeben.

Bei der automatischen Schlüsselerstellung geben Sie ein Wort oder eine Zeichenfolge in das Feld *Kennwort* ein und klicken auf die Schaltfläche *Erstellen*. Anschließend baut der Router selbstständig einen WEP-Schlüssel im Hexadezimalformat zusammen. In diesem Format werden nur die Zahlen von 0 bis 9 sowie die Buchstaben von A bis F genutzt.

Bei der Verschlüsselungsstärke 64 Bit füllt der Router automatisch alle vier Schlüsselfelder mit einem Schlüsselwert auf, bei der Verschlüsselungsstärke von 128 Bit ist das lediglich ein Wert. Egal ob Sie 64 Bit oder 128 Bit nutzen, dieser Schlüsselwert oder einer der Werte wird anschließend beim Einrichten der WLAN-Netzwerkkarte gebraucht.

Im manuellen Eingabemodus wählen Sie aus, welcher der vier Schlüssel (im Fall von 64 Bit) verwendet werden soll, und geben die Informationen zum WEP-Schlüssel für das Netzwerk im Hexadezimalformat in das ausgewählte Schlüsselfeld ein. Bei der WEP-Verschlüsselungsstärke von 64 Bit geben Sie 10 Hexadezimalzahlen ein, bei der WEP-Verschlüsselungsstärke von 128 Bit tragen Sie 26 Hexadezimalzahlen ein. Damit lässt sich die WLAN-Karte sicher mit dem WLAN-Router verbinden.

So erstellen Sie einen sicheren WPA-/WPA2-Schlüssel

Als sehr sicher schätzen Experten die Sicherheitsverschlüsselung WPA-PSK ein, das neuere WPA2-AES wird als noch sicherer eingestuft. Aus diesem Grund sollten Sie dieses Verfahren für Ihr WLAN-Netzwerk nutzen. Ältere Centrino-Notebooks (beispielsweise Baujahr 2004) beherrschen allerdings meist nur WPA-PSK. Bei der Schlüsselerstellung geben Sie ein Wort bzw. eine Zeichenfolge in das Feld *Kennwort* ein, das mindestens 8 und maximal 63 Zeichen lang sein darf. So können Sie beispielsweise ein ähnlich langes Kennwort wie dieses nutzen:

```
AdamundEvagehenindenWaldundholen6Äpfelheraus!GibtesApfelkuchen.
```

Es kann aber auch etwas Persönliches mit Ziffern etc. sein. Sie sollten es sich jedoch auf Papier notieren, da es beim Einrichten des WLAN-Client-PCs für die Verbindung gebraucht wird. Ist die Verschlüsselung aktiviert, ist der Grundstein gelegt, damit keine Fremden über Ihren WLAN-Router Unfug anstellen können. Anschließend aktivieren Sie die Protokollierung, damit Sie über sämtliche Aktivitäten des WLAN-Routers informiert sind.

Bild 3.4 Die FRITZ!Box unterstützt mit WPA2 die derzeit aktuellste Verschlüsselung für WLANs. Lässt sich WPA2 bei einer betagten FRITZ!Box nicht auswählen, hilft in der Regel ein Firmware-Update, um die Box auf den aktuellen Stand zu bringen.

Wireless-Modus-Einstellungen richtig festlegen

Fast alle aktuellen WLAN-Router sind abwärtskompatibel, doch veraltete WLAN-Netzwerkkarten können manchmal nicht im Auto-Modus (automatische Erkennung des verwendeten Modus) betrieben werden und fordern den passenden Wireless-Modus explizit an, damit eine Übertragung überhaupt zustande kommen kann. So sind folgende Wireless-Moduseinstellungen möglich:

Wireless-Modus	Beschreibung
n + a	Hier können sowohl 802.11a- als auch 802.11n-konforme Wireless-Geräte verwendet werden. Die Geschwindigkeit wird jeweils an das langsamste Gerät angepasst. 802.11a-Geräte erreichen eine maximale Bruttodatenrate von 54 MBit/s – achten Sie also auf den Einsatz von schnellen 802.11n-Geräten.
n + g	Damit können sowohl 802.11g- als auch 802.11n-konforme Wireless-Geräte verwendet werden. Die Geschwindigkeit wird jeweils an das langsamste Gerät angepasst.
b + g	Es können sowohl 802.11g- als auch 802.11b-konforme Wireless-Geräte verwendet werden. Die Geschwindigkeit wird jeweils an das langsamste Gerät angepasst.
g	Im g-Modus können nur 802.11g-konforme WLAN-Geräte genutzt werden. Die Geschwindigkeit liegt standardmäßig bei 54 MBit/s und wird nur bei Verbindungsproblemen angepasst.
g++	Diese Bezeichnung ist vor allem bei neueren AVM-Geräten verbreitet. Dieser erweiterte g-Modus lässt sich nur mit hauseigenen AVM-Geräten nutzen.
b	Vergangenheit: Hier können alle 802.11b-konformen WLAN-Geräte verwendet werden. Zudem können 802.11g-konforme WLAN-Geräte im 802.11b-Modus betrieben werden. Die Geschwindigkeit orientiert sich am b-Standard, liegt also bei 11 MBit/s.
nur 108 MBit/s	Bei aktuellen Geräten nicht mehr vorhanden: Wie bei g++ auch, ist dieser Modus herstellerabhängig. Der 108-MBit/s-Modus kann nur von kompatiblen 802.11g-Wireless-Geräten genutzt werden.
n + g + b	Es können alle 802.11n-, 802.11g- und 802.11b-Geräte verwendet werden.
Für 300 MBit/s optimierte Funkkanäle nutzen	Je schneller, desto besser: Ist die FRITZ!Box auf dem neuesten Stand, sollen die neuen WLAN-Geräte auch den schnellsten Standard nutzen dürfen.

Im b-Modus können alle 802.11b-konformen WLAN-Geräte verwendet werden. Zudem können 802.11g-konforme WLAN-Geräte auch im 802.11b-Modus betrieben werden. Ist die Option *108 Mbit/s-Einstellungen/Erweiterte 108 Mbit/s-Einstellungen deaktivieren* vorhanden und markiert, deaktiviert der Wireless-Router die Datenkomprimierung, das Packet-Bursting und die Unterstützung großer Frames. Wer beispielsweise eine PSP (PlayStation Portable) mit einem Netgear-Router nutzen möchte, muss dieses Feature ausschalten.

Diese Funktion ist bei manchen FRITZ!Box-Modellen bei den WLAN-Einstellungen unter 802.11g++ versteckt. Soll beispielsweise eine mobile PSP-Spielkonsole via WLAN mit dem Heimnetzwerk oder dem Internet verbunden werden, muss also eingegriffen werden: Der in der PSP eingebaute WLAN-Standard der ersten Generation ist 802.11b, der eine Übertragungsgeschwindigkeit von etwa 11 MBit/s ermöglicht. Im PSP-Betrieb muss der FRITZ!Box-g++-Schalter daher zwingend deaktiviert werden. Schnellere Datenübertragungsraten sind derzeit mit der PSP nicht möglich.

Wichtige Systemereignisse unbedingt aufzeichnen lassen

Ein Protokoll ist prinzipiell eine detaillierte Aufzeichnung der Webseiten, auf die die angeschlossenen Rechner in Ihrem Netzwerk zugegriffen haben bzw. zuzugreifen versucht haben. Aus Sicherheitsgründen sollten Sie, falls vorhanden, diese Option aktivieren. Damit können Sie, sollte es zu Zwischenfällen oder Problemen kommen, nachschauen, was welcher Computer angestellt hat oder auch nicht. Die FRITZ!Box bietet derzeit keine Protokollierung der Webseiten, sondern nur eine Dokumentation wichtiger Systemereignisse wie Internetverbindungsauf- und -abbau, Onlinezeit sowie das verbrauchte Onlinedatenvolumen.

Fungiert die FRITZ!Box auch als VoIP-Telefonzentrale, wird zusätzlich eine Anrufliste mitdokumentiert. In der Anrufliste werden alle ein- und ausgehenden Telefonate erfasst, die mit der FRITZ!Box geführt wurden. Ob allerdings eine Rufnummer protokolliert wird, hängt davon ab, ob Ihr Telefonanschluss das unterstützt. Kommen bei einem Analoganschluss keine Rufnummernübermittlungen an, kann auch die Box nichts anzeigen. Dann sehen Sie nur die von Ihnen getätigten Telefonate.

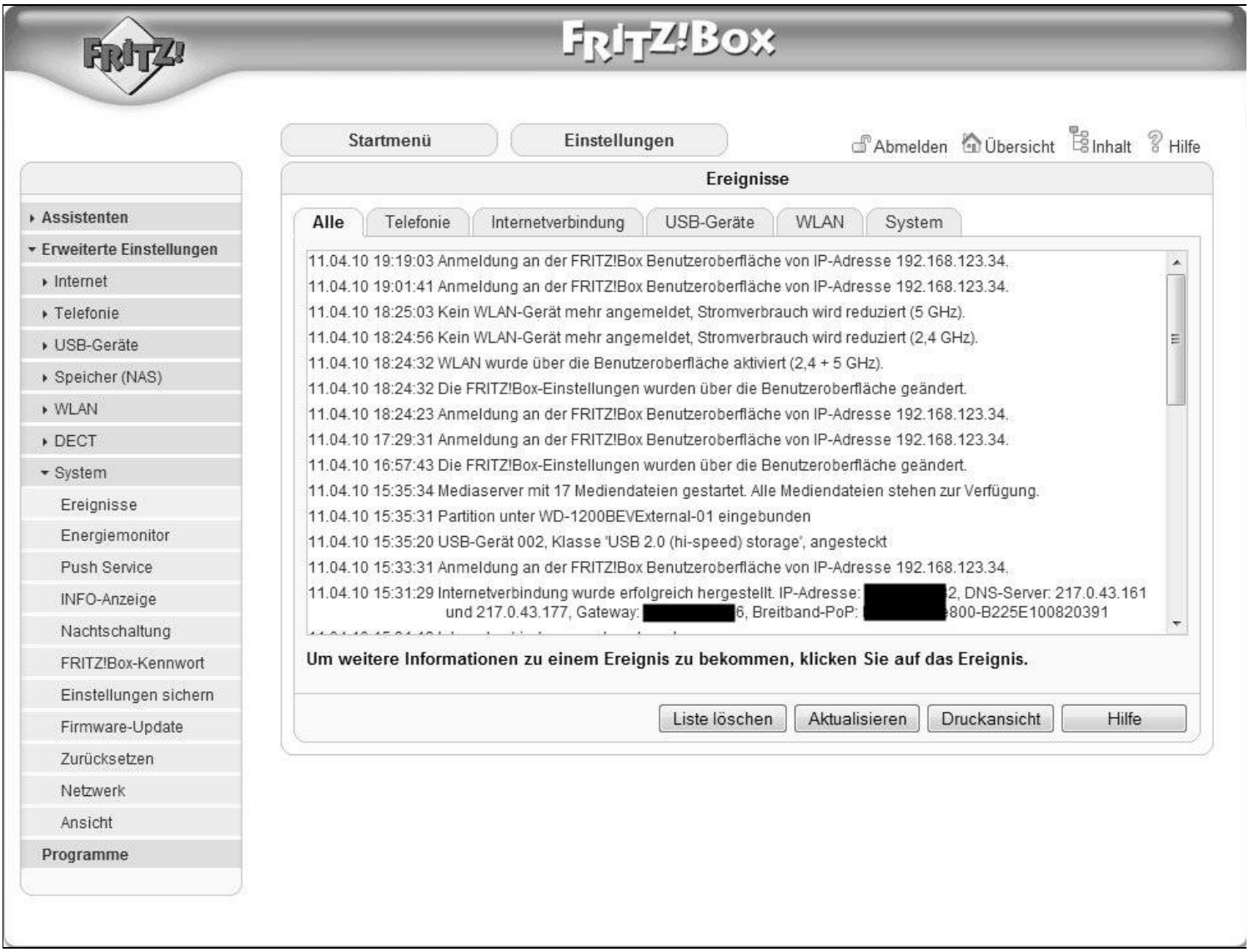


Bild 3.5 Spartanisch: In Sachen Protokollierung beschränkt sich die FRITZ!Box auf die wesentlichen Ereignisse. Diese sind via Weboberfläche über *Übersicht/Ereignisse* abrufbar.

Manche WLAN-Router bieten zusätzlich zur Protokollierung eine Content-Filterung. Ist diese Option aktiviert, ist in den Protokollen zu sehen, wann ein Rechner in Ihrem Netzwerk auf eine gesperrte Site zuzugreifen versucht hat. Bei einer aktivierten E-Mail-Benachrichtigung wird Ihnen das Protokoll automatisch in einer E-Mail zugestellt, Sie brauchen dann nicht immer über den Webseitendialog des Routers zu gehen.

Inaktive Dienste in der FRITZ!Box-Firewall sperren

Ein wesentlicher Sicherheitsaspekt bei der Konfiguration der FRITZ!Box sind die konfigurierten Dienste sowie die geöffneten Ports der integrierten Firewall. Eine Firewall muss prinzipiell zwei Funktionen erfüllen: Sie muss den PC und andere an ihn angeschlossenen Geräte nach außen in Richtung Internet absichern, damit Eindringlinge keine Chance haben. Dazu soll die Firewall den auf dem PC laufenden Programmen und Spielen eine sichere Verbindung nach außen gewähren.

Die Firewall überwacht den Datenstrom an sogenannten Ports, das sind virtuelle Ein- und Ausgänge, die der PC verwaltet. Bei der Übertragung von Daten wird ein Port festgelegt und verwendet, Standardfunktionen wie FTP (File Transfer Protocol) oder HTTP haben vorgegebene Ports. Da ein Programm aber auch an einem beliebigen Port warten kann, macht die Firewall außerhalb der bekannten Ports meist zunächst mal dicht.

Portnummer	Beschreibung
20/21	FTP
80/8080	HTTP
53	DNS
110	POP3

1723	PPTP
25	SMTP
995	POP/SSL
143	IMAP
993	IMAP/SSL

Je weniger Ports geöffnet sind, desto weniger Angriffsfläche bietet die FRITZ!Box. Wird der Router zu konservativ konfiguriert, ist das Heimnetz oder der PC zwar optimal abgesichert, aber unter Umständen leidet die Funktionalität. Wer mit seinem Spiele-PC hinter einer FRITZ!Box oder einer Personal Firewall online zocken möchte, muss den Router entsprechend einstellen, damit die Rückmeldungen von Spielserver und Mitspielern aus dem Internet auch zum PC zurückkommen. Erst dann kann dieser richtig mitfraggen. Welche Ports Sie für den PC im Endeffekt öffnen, hängt von Ihren persönlichen Ansprüchen und Sicherheitsbedürfnissen ab.

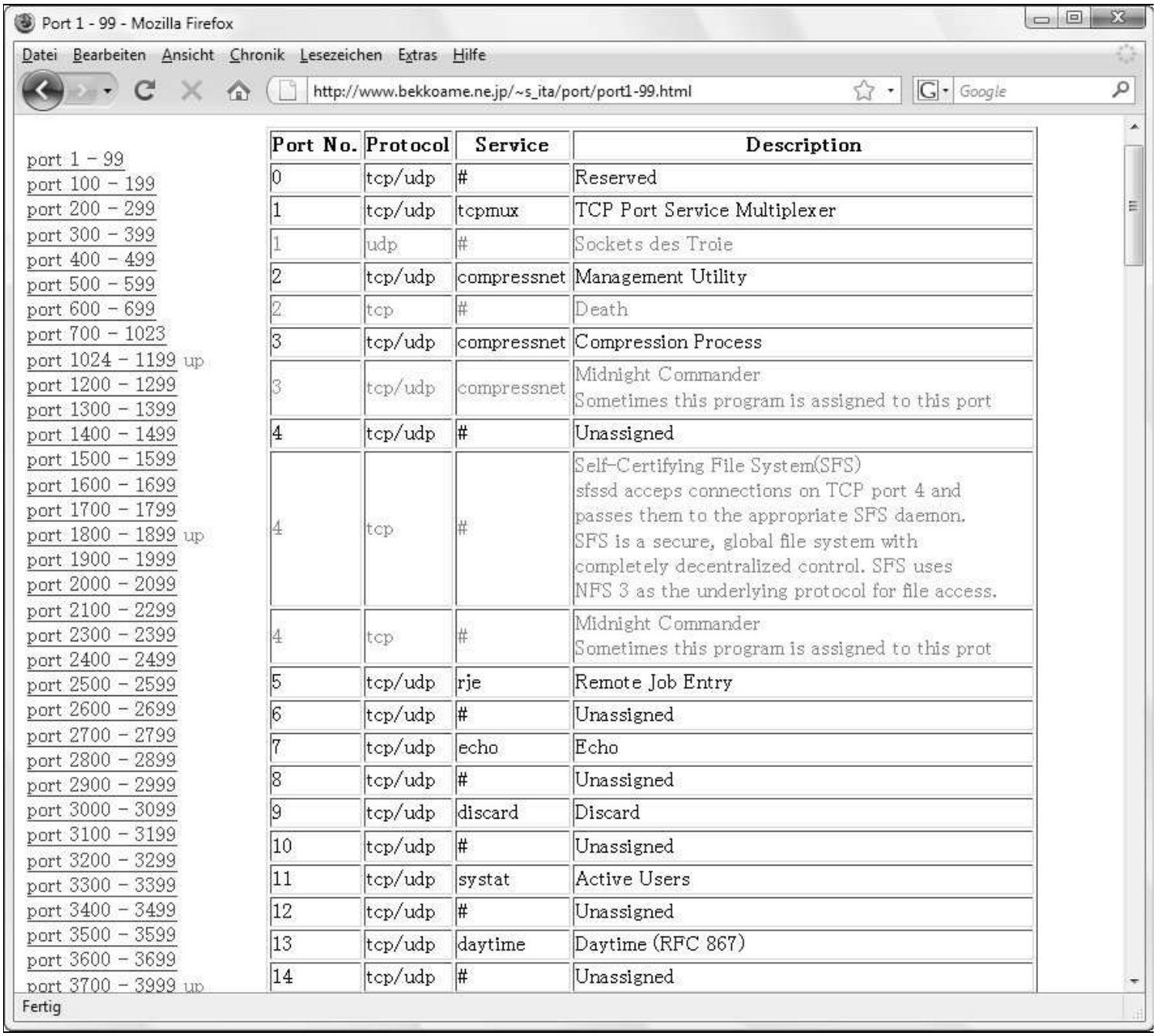
Insgesamt gibt es 65.535 verschiedene Ports. Damit bestimmten Anwendungen feste Portnummern zugewiesen werden können, sind die Ports im Wesentlichen in drei Gruppen unterteilt:

Bereich/Portnummer	Beschreibung
0 bis 1023	Well Known Ports
1024 bis 49151	Registered Ports
49152 bis 65535	Dynamic und/oder Private Ports

Beim Netzwerk-Gaming hängt es vor allem vom Spiel ab, welche Ports zur Verfügung stehen müssen. Damit das Spielen grundsätzlich funktioniert, sind meist folgende Ports nach ICMP (Internet Control Message Protocol) notwendig:

```
53
80
443
```

ICMP dient dem Austausch von Fehler- und Informationsmeldungen bei TCP/IP- und UDP-Protokollen. Es sorgt dafür, dass eine Verbindung stabil bleibt – sprich aufrechterhalten wird – und es zu keinen ungewollten Verbindungsabbrüchen kommt. Ob weitere Ports gebraucht werden, steht im Handbuch zum Spiel. Dort sollte beschrieben sein, welche Ports offen sein müssen, damit das Spiel online gespielt werden kann. Welche Ports es gibt und wofür welcher TCP- bzw. UDP-Port zuständig ist, ist auf folgender Webseite zusammengefasst:



Port No.	Protocol	Service	Description
0	tcp/udp	#	Reserved
1	tcp/udp	tcpmux	TCP Port Service Multiplexer
1	udp	#	Sockets des Troie
2	tcp/udp	compressnet	Management Utility
2	tcp	#	Death
3	tcp/udp	compressnet	Compression Process
3	tcp/udp	compressnet	Midnight Commander Sometimes this program is assigned to this port
4	tcp/udp	#	Unassigned
4	tcp	#	Self-Certifying File System(SFS) sfssd acceps connections on TCP port 4 and passes them to the appropriate SFS daemon. SFS is a secure, global file system with completely decentralized control. SFS uses NFS 3 as the underlying protocol for file access.
4	tcp	#	Midnight Commander Sometimes this program is assigned to this prot
5	tcp/udp	rje	Remote Job Entry
6	tcp/udp	#	Unassigned
7	tcp/udp	echo	Echo
8	tcp/udp	#	Unassigned
9	tcp/udp	discard	Discard
10	tcp/udp	#	Unassigned
11	tcp/udp	systat	Active Users
12	tcp/udp	#	Unassigned
13	tcp/udp	daytime	Daytime (RFC 867)
14	tcp/udp	#	Unassigned

Bild 3.6 Für jeden Einsatzzweck sind die Ports 1 bis 65535 hier übersichtlich beschrieben: *www.bekkoame.ne.jp/~s_ita/port/port1-99.html*.

Die TCP- und UDP-Ports (User Datagram Protocol) sorgen für die Kommunikation auf Netzwerk- bzw. Anwendungsebene. Grundsätzlich gilt: Weniger ist mehr. Je weniger Ports geöffnet und Dienste verfügbar sind, desto weniger Angriffsfläche bietet der DSL-Router nach außen. So können Sie die Nutzung bestimmter Internetdienste wie das Surfen im WWW (HTTP), das File Transfer Protocol (FTP) und viele andere für alle oder einige Benutzer in Ihrem Netzwerk blockieren. Doch Vorsicht: Wird der Router zu sicher eingestellt, leidet die Funktionalität, weil bestimmte Programme nicht mehr richtig funktionieren.

Wer beispielsweise einen Webserver (HTTP-Protokoll mit Port 80) hinter einem Router oder einer Personal Firewall betreiben möchte, muss den DSL-Router so einstellen, dass die Anfragen aus dem Internet auch bis zum Server kommen können. Erst dann kann dieser reagieren und die Anfragen beantworten. Welchen Port Sie öffnen, hängt von dem eingesetzten Serverprogramm und vor allem von Ihren persönlichen (Sicherheits-)Bedürfnissen ab.

So richten Sie die Porteinstellungen der FRITZ!Box ein

Der Router kann auch so eingestellt werden, dass bestimmte Ports am Router offen sind, die Daten, die dort ankommen, aber nur an einen bestimmten Rechner bzw. eine bestimmte IP-Adresse weitergeleitet werden. Diese Technik läuft unter Portweiterleitung bzw. Port-Triggering.

Die Porteinstellungen der FRITZ!Box richten Sie auf der Weboberfläche über *Übersicht/Erweiterte Einstellungen/Internet/Freigaben/Portfreigaben* ein.

Bild 3.7 Per Klick auf die Schaltfläche *Neue Portfreigabe* richten Sie eine neue Verbindung von außen auf einem PC im Netzwerk ein.

Ports einzeln angeben

Leider ist es bei der FRITZ!Box mit älteren Firmwareversionen nicht möglich, einen ganzen Portbereich (beispielsweise 16384 bis 16389) zur Weiterleitung freizugeben. Wer einen Block von TCP- oder UDP-Ports in der Firewall freigeben möchte, muss jeden Port einzeln angeben. Sie ersparen sich unter Umständen Konfigurationsarbeit, wenn Sie zunächst die aktuelle Firmware in die FRITZ!Box einspielen. Das erledigen Sie im Webbrowser per *Übersicht/Einstellungen/System/Firmware-Update*.

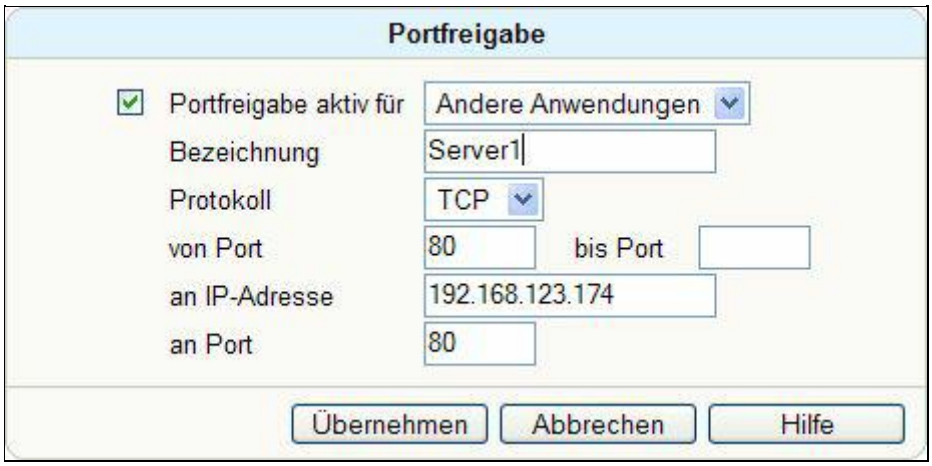


Bild 3.8 Nach einem Firmware-Update lassen sich Portbereiche bei einer Portfreigabe einrichten.

Portfreigabe und Zieladresse

Achten Sie darauf, dass bei der Konfiguration einer Portfreigabe die Zieladresse immer gleich bleibt. Hier ist es möglicherweise besser, für den Zielrechner im heimischen Netz wie oben beschrieben eine feste IP-Adresse einzurichten. Verwenden Sie im Zweifelsfall statt einer DHCP-Adresse für den PC eine statische IP-Adresse. Mithilfe der FRITZ!Box-Portfreigabe lassen sich so Dienste und verwendete Ports explizit bestimmten Rechnern im Heimnetz zuordnen.

Per Mail über den Systemzustand informieren lassen

Bei der FRITZ!Box ist in der Benutzeroberfläche ein sogenannter Push Service integriert, der den Anwender auf Wunsch per Mail über den Systemzustand und über Änderungen informiert. Grundvoraussetzungen dafür sind selbstverständlich ein E-Mail-Konto und die passenden Zugangsdaten, damit die FRITZ!Box entsprechend konfiguriert werden kann.

Bild 3.9 Über die Weboberfläche via *Übersicht/Erweiterte Einstellungen/System/Push Service* richten Sie das gewünschte E-Mail-Konto ein, das die Systemmeldungen der FRITZ!Box in Empfang nehmen soll.

Sind sämtliche Einstellungen eingetragen, können Sie per Klick auf die Schaltfläche *Push-Service testen* die ordnungsgemäße Funktion überprüfen. Haben Sie nach wenigen Minuten eine E-Mail im Posteingang, können Sie mit einem Klick auf die Schaltfläche *Übernehmen* die Einstellungen speichern.

3.2 Erweiterte Sicherheitseinstellungen

Viele WLAN-Router bieten neben den Standard-Wireless-Einstellungen auch eine Option an, mit der Sie erweiterte Einstellungen für das Funknetz konfigurieren können. Bei der FRITZ!Box hängt es von der eingesetzten Firmwareversion sowie vom FRITZ!Box-Modell ab, welche Optionen im Bereich *Übersicht/Erweiterte Einstellungen/WLAN* zur Verfügung stehen. Mit der Auswahl der Option *WLAN aktivieren* können Sie auf andere Optionen zugreifen. Benutzen Sie kein WLAN, schalten Sie es über diese Option am Router aus.

!&fritz7390-43.tif!

Bild 3.10 Nur wer einen AVM-USB-Stick im Einsatz hat, muss das Häkchen bei *AVM Stick & Surf aktivieren* setzen.

Zusätzlich können bei manchen FRITZ!Box-Modellen noch verschiedene Einstellungen zum Übertragungsmodus vorgenommen werden, die Einfluss auf die Sendeleistung und Übertragungsqualität haben.

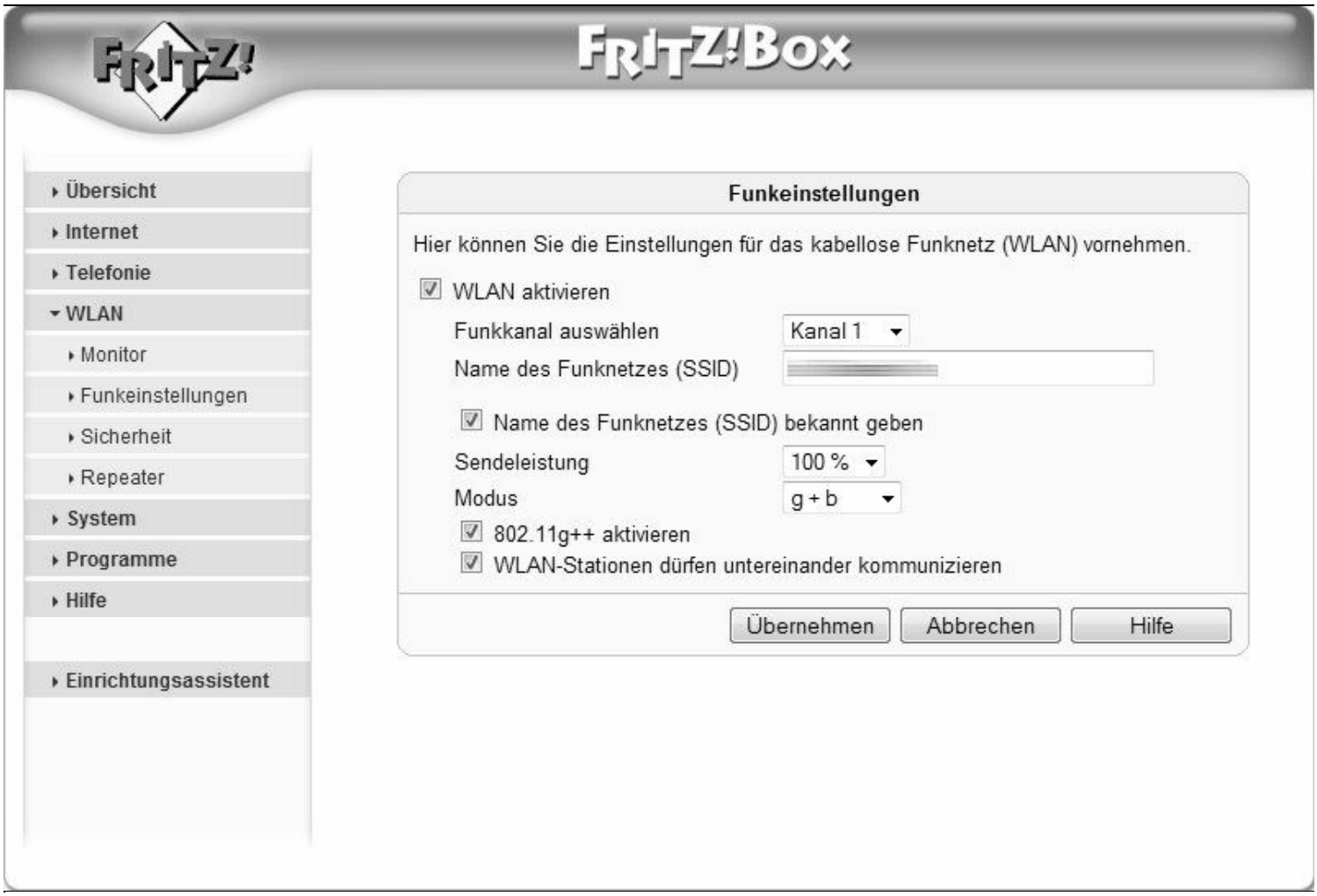


Bild 3.11 Abhängig von den verwendeten WLAN-Komponenten konfigurieren Sie den Übertragungsmodus.

- *Name des WLAN-Funknetzes (SSID)*: Hier lässt sich der Name des WLAN-Netzes konfigurieren. Ist das Häkchen bei *WLAN aktivieren* gesetzt, sendet die FRITZ!Box ihren Netzwerknamen (SSID – *Service Set Identifier*) an alle Wireless-Stationen.
- *Funkkanal auswählen*: Dieser Schalter legt fest, welche Betriebsfrequenz der Router nutzen soll. Hier können Sie die Werkeinstellung beibehalten, es sei denn, es sind Störstrahlungen von einem anderen WLAN-Router in der Umgebung vorhanden. Dies macht sich vor allem durch Schwierigkeiten beim Verbindungsaufbau und in der Geschwindigkeit bemerkbar. Hängen in der Nachbarschaft einige andere WLAN-Router an der Steckdose, kann das Umkonfigurieren des Kanals einen Geschwindigkeitsschub bringen.
- *Name des WLAN-Funknetzes sichtbar*: Ist diese Option aktiviert, sendet der Wireless-Router seinen Netzwerknamen (SSID – *Service Set Identifier*) an alle Wireless-Stationen. Stationen, die keine SSID (oder den Wert null) haben, können dann die korrekte SSID für Verbindungen zu diesem Access Point annehmen.
- *AVM Stick & Surf aktivieren*: Diese Option ist für USB-Adapter aus dem Hause AVM gedacht. Setzen Sie einen AVM-USB-Adapter ein, sollte hier das Häkchen gesetzt werden.

Für mehr Sicherheit ist die Option Sicherheit bei der FRITZ!Box ideal: Hier können Sie den Zugang auf das WLAN auf Grundlage der MAC-Adresse des PCs beschränken.

Zugriffsliste für neue Netzwerkgeräte einrichten

Standardmäßig wird jedem drahtlosen Computer, der mit einer korrekten SSID, dem richtigen Verschlüsselungsstandard sowie dem passenden Schlüssel ausgestattet ist, Zugang zum drahtlosen Netzwerk gewährt. Jeder Router beinhaltet jedoch eine MAC-Adressfilterung, bei der Computer basierend auf ihren MAC-Adressen eine Verbindung zum Router aufbauen dürfen oder auch nicht.

Bei einer FRITZ!Box sorgen Sie für mehr Sicherheit, wenn Sie per *Übersicht/WLAN/Monitor* die Option *Keine neuen WLAN-Netzwerkgeräte zulassen* aktivieren, nachdem der PC mit WLAN-Karte erstmalig Verbindung mit dem WLAN-

Router aufgenommen hat. Diese Option aktivieren Sie erst dann, wenn der DSL-Router fertig konfiguriert und erstmals erfolgreich eine Verbindung zwischen Computer und DSL-Router hergestellt worden ist. In diesem Fall merkt sich die FRITZ!Box die MAC-Adresse des Computers und verweigert anderen Geräten die Zusammenarbeit.

!&fritz7390-43.tif!

Bild 3.12 Nur bei der erstmaligen Konfiguration des WLAN-Netzwerks braucht der Schalter *Alle neuen WLAN-Geräte zulassen* aktiviert zu sein. Sind die gewünschten Geräte einmal mit der FRITZ!Box verbunden worden, »merkt« sich die FRITZ!Box deren MAC-Adresse.

Wird beim Eintragen des Geräts der Gerätename nicht angezeigt, können Sie selbst einen beschreibenden Namen für den PC eingeben, den Sie der MAC-Adresse hinzufügen. Wie alle anderen wichtigen Ereignisse dokumentiert die FRITZ!Box auch die An- und Abmeldevorgänge der WLAN-Stationen. Über die Weboberfläche unter *Übersicht/System/Ereignisse* im Register *WLAN* können Sie das Protokoll einsehen. Hier finden Sie auch die abgelehnten Zugriffe. Das kann ein Hinweis darauf sein, dass von außen jemand versucht, auf Ihr WLAN zuzugreifen.

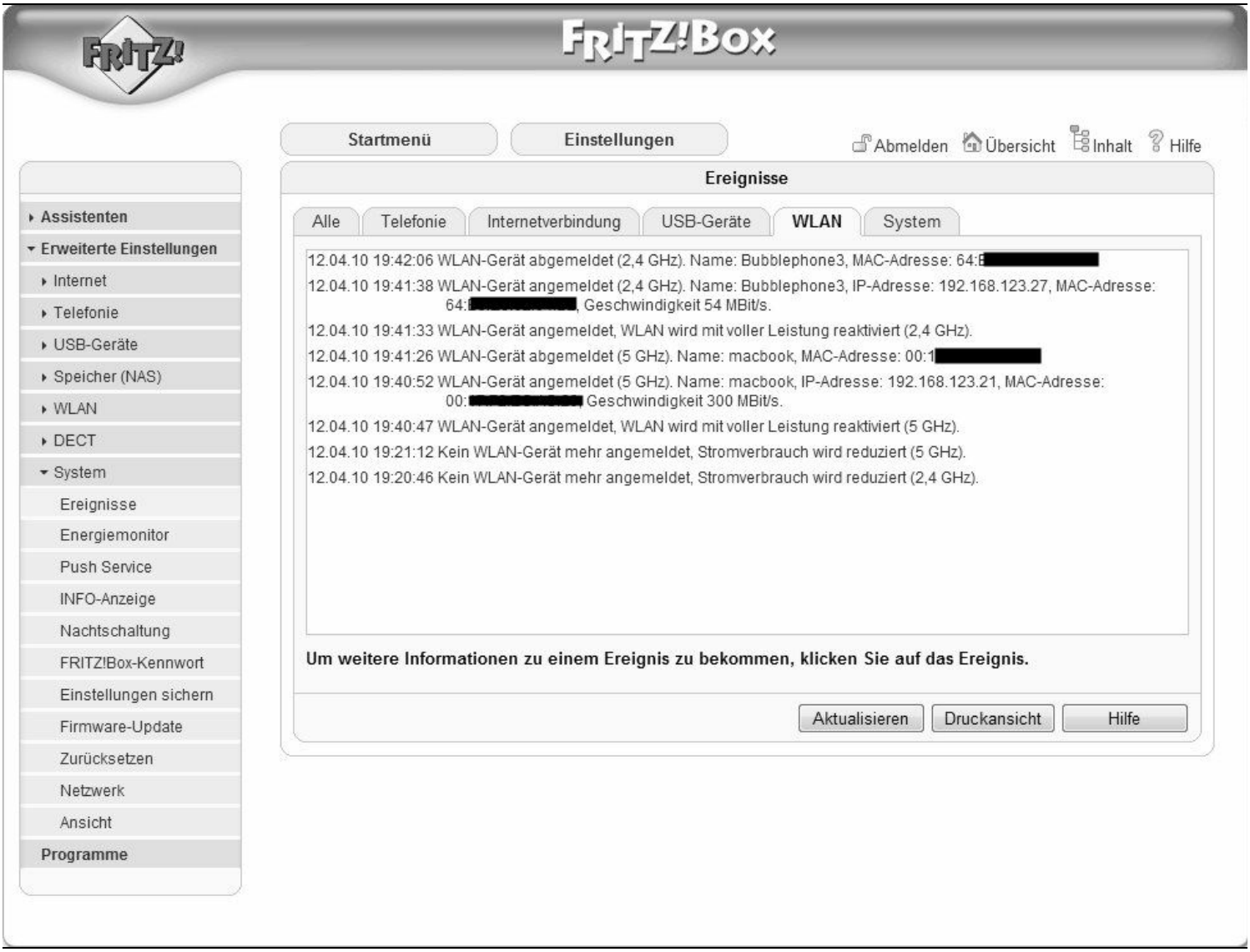


Bild 3.13 Sämtliche An- und Abmeldevorgänge an der FRITZ!Box sowie die zugewiesenen IP-Adressen und dazugehörige Verbindungsgeschwindigkeiten werden in dem Protokoll erfasst.

Zugang erlaubt? – Angeschlossene Netzwerkgeräte prüfen

Jeder vernünftige Router bietet einen Dialog, der eine Übersicht über angeschlossene Geräte liefert. In der Regel sind die IP-Adresse, der Gerätename, den Sie unter Windows vergeben haben, und die MAC-Adresse für jeden eingeschalteten Computer zu sehen, der mit dem Router verbunden ist.

Das ist besonders praktisch, wenn Sie vermuten, dass sich ein Fremder in Ihrem Netz befindet. In diesem Fall sollten Sie die Sicherheitseinstellungen der FRITZ!Box nochmals überprüfen. Dazu schalten Sie am besten alle Ihre PCs, die über das Funknetz zugreifen, aus, und es sollte nur noch ein Rechner mit seiner MAC-Adresse (unbedingt notieren) zu sehen sein. Gibt es weitere, müssen Sie sich Gedanken machen.

Mithilfe der FRITZ!Box können Sie die Verbindungen direkt unterbrechen. Sie sollten aber sofort die SSID wechseln, sie unsichtbar machen und die Verschlüsselung mit einem neuen Schlüssel aktualisieren. Danach gilt es, die Protokolle daraufhin zu überprüfen, was alles aufgerufen wurde. Rechtlich sieht es so aus, dass die Nutzung unzureichend gesicherter Funknetze eine Grauzone ist, denn für Sicherheit hat jeder selbst zu sorgen.

Bei einer FRITZ!Box sorgen Sie für mehr Sicherheit, wenn Sie die Option *Keine neuen WLAN-Netzwerkgeräte zulassen* aktivieren, nachdem der PC mit WLAN-Karte erstmalig Verbindung mit dem WLAN-Router aufgenommen hat. In diesem Fall merkt sich die FRITZ!Box die MAC-Adresse des PCs und verweigert die Zusammenarbeit mit anderen Geräten.

Bild 3.14 Standardmäßig erhält jede WLAN-Karte, die mit einer passenden SSID konfiguriert ist, Zugriff auf das drahtlose Netzwerk. Für mehr Sicherheit bei der FRITZ!Box sorgt dieser Dialog: Hier können Sie den Zugang auf das WLAN auf Grundlage einer MAC-Adresse beschränken, falls Sie den Schalter bei *WLAN-Zugang auf die bekannten WLAN-Geräte beschränken* umlegen.

Standardmäßig wird jedem drahtlosen Gerät, das mit einer korrekten SSID und dem passenden Schlüssel ausgestattet ist, Zugang zu dem drahtlosen Netzwerk gewährt. Jeder Router bietet jedoch eine MAC-Adressfilterung, bei der Geräte basierend auf ihren MAC-Adressen eine Verbindung zum Router aufbauen dürfen – oder auch nicht.

So richten Sie für den Familien-PC die Kindersicherung ein

Nutzen Sie im Haushalt einen Computer und melden sich Ihre Kinder mit ihren eigenen Benutzernamen darauf an, können Sie die Kindersicherung der FRITZ!Box nutzen. Bevor Sie die Kindersicherung auf der FRITZ!Box aktivieren, muss auf dem Windows-PC eine spezielle AVM-Software installiert werden.

Den Link auf die Internetseite von AVM zu dem entsprechenden Windows-Programm *FRITZ!Box Kindersicherung* finden Sie im Hauptmenü Ihrer FRITZ!Box über *Einstellungen/Programme*. Im Zusammenspiel mit diesem Programm können Sie die FRITZ!Box nun so konfigurieren, dass der Computer im Kinderzimmer nur zu bestimmten Zeiten und in begrenztem Umfang in das Internet kann.

Zunächst installieren Sie das Windows-Programm *FRITZ!Box Kindersicherung* – in der Regel klicken Sie die Installation problemlos durch. Anschließend melden Sie sich am PC im Kinderzimmer mit dem Kinder-Account an und stellen eine Internetverbindung her, etwa für das Windows-Update oder das Update des Virenscanners. In diesem Fall kennt die FRITZ!Box anschließend den Windows-Benutzer SYSTEM, der für Windows-Updates und Updates von Virenschutzprogrammen zuständig ist. Anschließend bekommen Sie den Benutzernamen SYSTEM sowie den Benutzernamen des Kindes im Kindersicherungsdialog angezeigt.

!&fritz7390-61.tif!

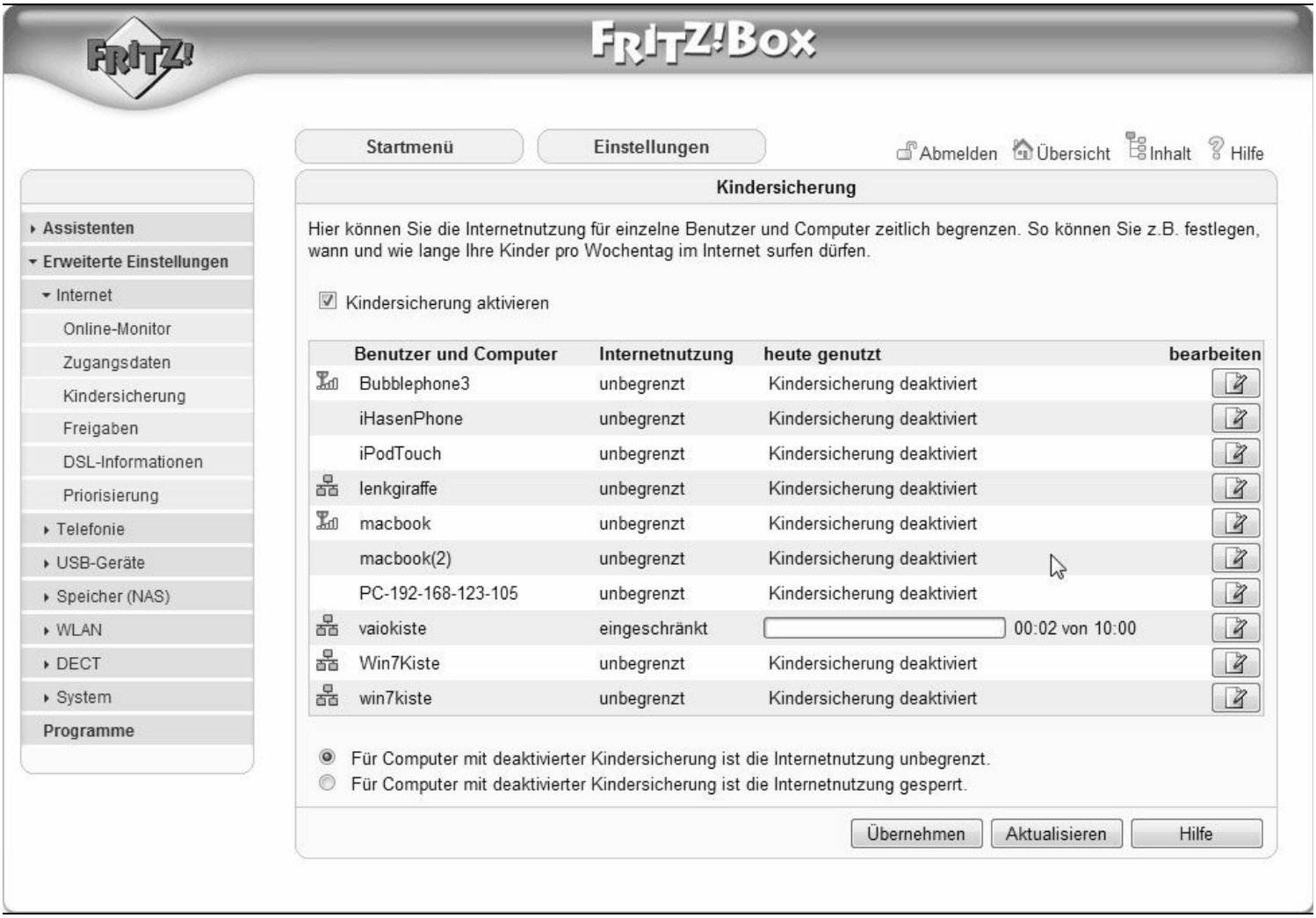


Bild 3.15 Wenn Sie die Kindersicherung nicht benötigen, achten Sie darauf, dass sie ausgeschaltet ist. Andernfalls sorgt die Kindersicherung auf Port 14013 für überflüssige Kommunikation im Heimnetzwerk.

Im nächsten Schritt aktivieren Sie über *Einstellungen/Erweiterte Einstellungen/Internet/Kindersicherung* das Häkchen bei *Kindersicherung aktivieren*. Anschließend wählen Sie in der Geräteliste den zu beschränkenden Computer bzw. Benutzer aus und legen in der darauf erscheinenden Übersicht die zeitliche Beschränkung der Internetnutzung fest. Hier lassen sich in den entsprechenden Feldern die Zeitintervalle festlegen, in denen das Internet genutzt werden darf. Es sind unterschiedliche Einstellungen für Montag bis Donnerstag, für den Freitag und für das Wochenende möglich.

Niemals ohne aktivierte Firewall ins Internet

Grundsätzlich gilt: Beim Surfen im Internet sollte die Firewall zwingend eingeschaltet sein. Die SPI-Firewall (Stateful Port Inspection) schützt das Netzwerk vor DoS-Attacken (Denial of Service, Überlastung des Systems durch eine Unzahl von Anfragen) und anderen Übeltätern. Die Firewall ist in der Regel bei den meisten Herstellern ab Werk standardmäßig aktiviert.

Auf Pings am Internetport nicht reagieren

Das Suchen von potenziellen Opfern für DoS-Angriffe etc. wird über den *ping*-Befehl realisiert. Auf diese Weise kann ein anderer Rechner feststellen, ob die angepingte Maschine noch läuft und für Anfragen aus dem Netz erreichbar ist. Manche Modelle lassen sich so konfigurieren, dass sie nicht auf einen Ping aus dem Internet reagieren. Finden Sie eine Option ähnlich wie *Auf Ping am Internet-Port reagieren*, sollten Sie sie deaktivieren, es sei denn, Sie haben einen guten Grund, sie aktiviert zu lassen. Das hat übrigens nichts mit der Möglichkeit des »Anpingens« im heimischen Netzwerk, die Sie weiter unten kennenlernen werden, zu tun. Der netzinterne Ping wird anders interpretiert als einer über den Internetport.

Prüfen, ob der konfigurierte MTU-Wert passt

Das Konfigurieren der MTU-Größe (Maximum Transmission Unit – maximale Übertragungseinheit) hat weniger mit Sicherheit zu tun, es dient eher dem Feintuning und der Totaloptimierung des DSL-Routers.

Bei der FRITZ!Box kann kein MTU-Wert eingestellt werden. Lässt der DSL-Router hier einen Eingriff zu, lohnt es sich, die Einstellungen zu überprüfen. Der passende MTU-Wert für die meisten Ethernetnetzwerke beträgt 1.500 Byte oder 1.492 Byte für PPPoE-Verbindungen bzw. 1.436 Byte für PPTP-Verbindungen. Bei einigen Internetanbietern ist möglicherweise das Reduzieren der maximalen Übertragungseinheit notwendig.

Wenn der MTU-Wert nicht passt, kann es passieren, dass manche Seiten nicht aufgerufen werden können. Um zu prüfen, ob der konfigurierte MTU-Wert passt oder nicht, verwenden Sie einfach den *ping*-Befehl:

Bild 3.16 Mit dem *ping*-Befehl überprüfen Sie die eingestellte MTU-Größe. Kommt die Meldung *Paket müsste fragmentiert werden, DF-Flag ist jedoch gesetzt*, ist die MTU-Konfiguration in Ordnung.

Mit dem Befehl:

```
ping –f –l 1464 www.franzis.de
```

auf der Kommandozeile prüfen Sie die MTU-Einstellungen für die TCP/IP-Verbindung. Geben Sie beispielsweise einen anderen MTU-Wert mit dem Befehl

```
ping -f -l 1460 www.franzis.de
```

ein, erscheint folgende Rückmeldung:

```
Antwort von 80.237.218.241: Bytes=1460 Zeit=64ms TTL=47
Antwort von 80.237.218.241: Bytes=1460 Zeit=61ms TTL=47
Antwort von 80.237.218.241: Bytes=1460 Zeit=61ms TTL=47
Antwort von 80.237.218.241: Bytes=1460 Zeit=61ms TTL=47
```

Der Ping geht also durch den DSL-Router zum Zielserver mit der IP-Adresse 80.237.218.241, der anschließend fehlerfreie Pakete zurücksendet. Addieren Sie nun 28 Byte für den notwendigen IP/ICMP-Header zu den 1460 Byte, beträgt der ideale Wert 1488. Abhängig von der Verbindung stellen Sie die passende MTU ein.

Bei manchen Anbietern ist dieser Wert mit 1492 angegeben. Sind einige Webseiten nicht zu erreichen oder treten Probleme beim Upload von Dateien oder E-Mails auf, prüfen Sie den MTU-Wert des Routers. Testen Sie Werte wie 1488, 1492 und 1500 – der ideale Wert hängt vom Provider ab. Im Zweifelsfall erkundigen Sie sich im Supportbereich auf der Webseite Ihres Internetproviders nach dem idealen MTU-Wert. Diese Maßnahme sorgt auch für eine bessere Qualität beim

Telefonieren über das Internet. Also unbedingt testen!

So schalten Sie das TR-069-Kommunikationsprotokoll aus

Weitgehend unbemerkt hat AVM die FRITZ!Box mit einer Funktion beglückt, die zumindest in der Fachwelt in Verruf geraten ist: Die TR-069-Schnittstelle unterstützt eine vom Anwender losgelöste Wartung mit einer beim Provider installierten Gegenstelle. Theoretisch könnte so auf den Router zugegriffen werden, um Logdateien oder Konfigurationen zu lesen und zu ändern. Selbst das Einschleusen eines Lauschprogramms oder Trojaners wäre theoretisch möglich.

Dieses geheimnisvolle Kommunikationsprotokoll TR-069 ist sowohl in der FRITZ!Box als auch beim T-Home Speedport standardmäßig aktiviert – ärgerlich für den Anwender, dass die Fernwartungsschnittstelle ungefragt eingeschaltet ist. Während sich die Option bei früheren Firmwareversionen der FRITZ!Box über *Einstellungen/Netzwerk/Anbieter-Dienste* per Option *Automatische Einrichtung durch den Dienstanbieter zulassen* derzeit (noch) abschalten lässt, ist das bei den Telekom-Speedport-Modellen nicht so einfach möglich.

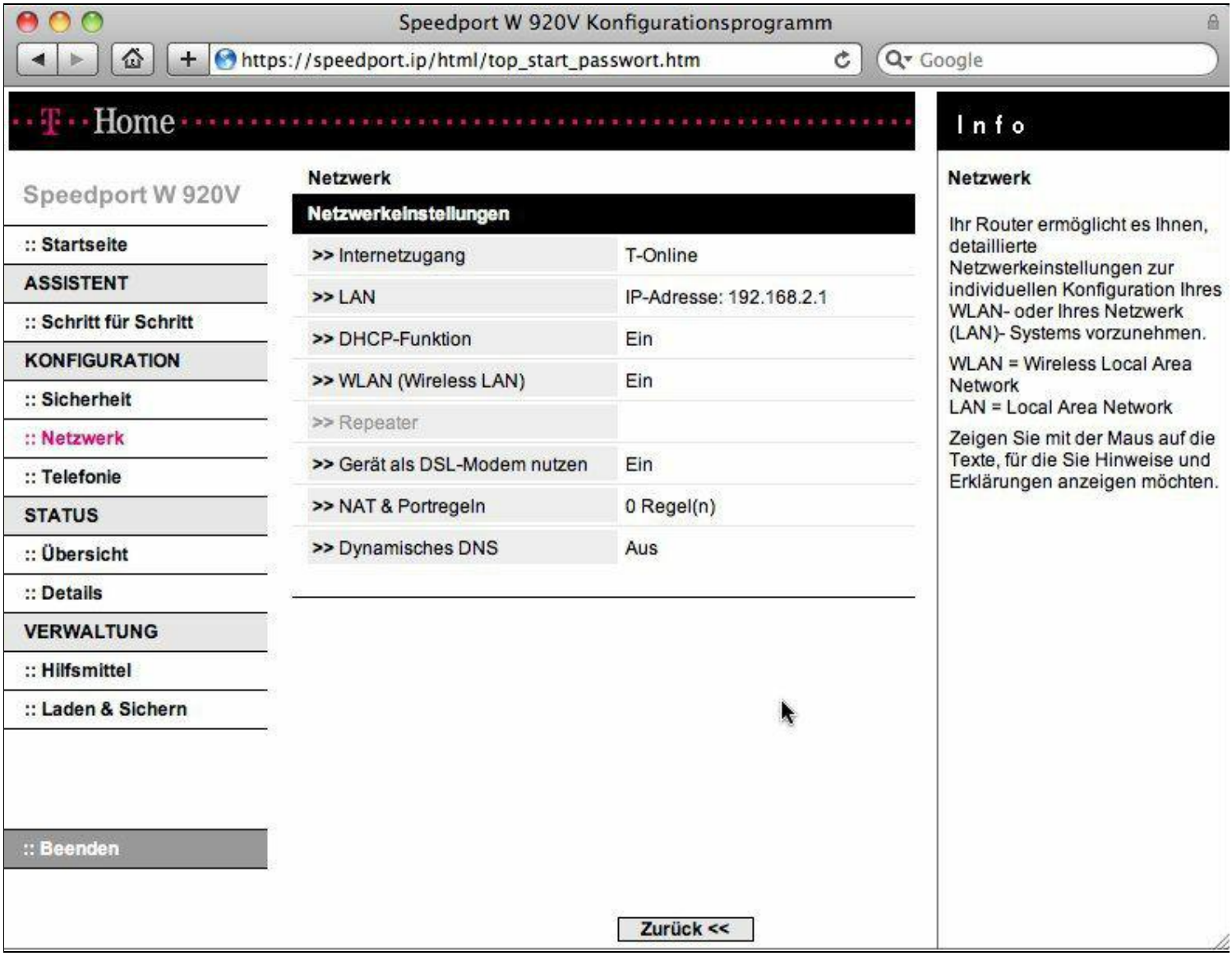


Bild 3.17 Beim T-Home Speedport ist weit und breit keine Funktion zum Abschalten des TR-069-Protokolls zu sehen. Hier hilft nur der Umweg über eine selbst gebaute FRITZ!Box-Firmware.

Auf den ersten Blick ist das Ändern der Option nicht leicht: Die Funktion *Automatische Updates zulassen* ist standardmäßig aktiviert, grau unterlegt und lässt sich zunächst nicht ändern.

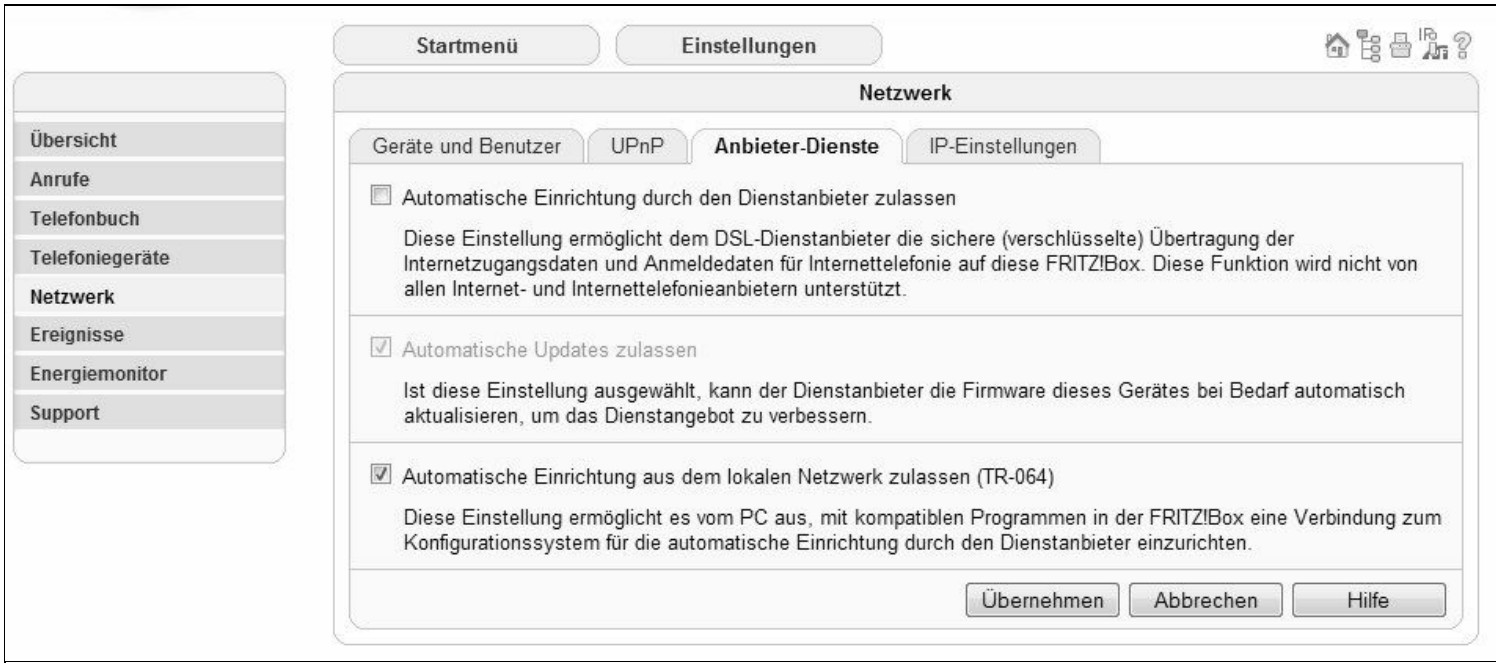


Bild 3.18 Unglücklich gelöst: Da die Option *Automatische Updates zulassen* ausgegraut und somit für den Anwender nicht zugänglich ist, lässt sie sich aus Anwendersicht nicht abschalten.

Um sämtliche Häkchen in diesem Dialog zu entfernen, muss zunächst das Häkchen bei *Automatische Einrichtung durch den Dienstanbieter zulassen* aktiviert sein, damit der ausgegraute Eintrag bei *Automatische Updates zulassen* abgeschaltet werden kann. Anschließend nehmen Sie das Häkchen bei *Automatische Einrichtung durch den Dienstanbieter zulassen* wieder heraus.

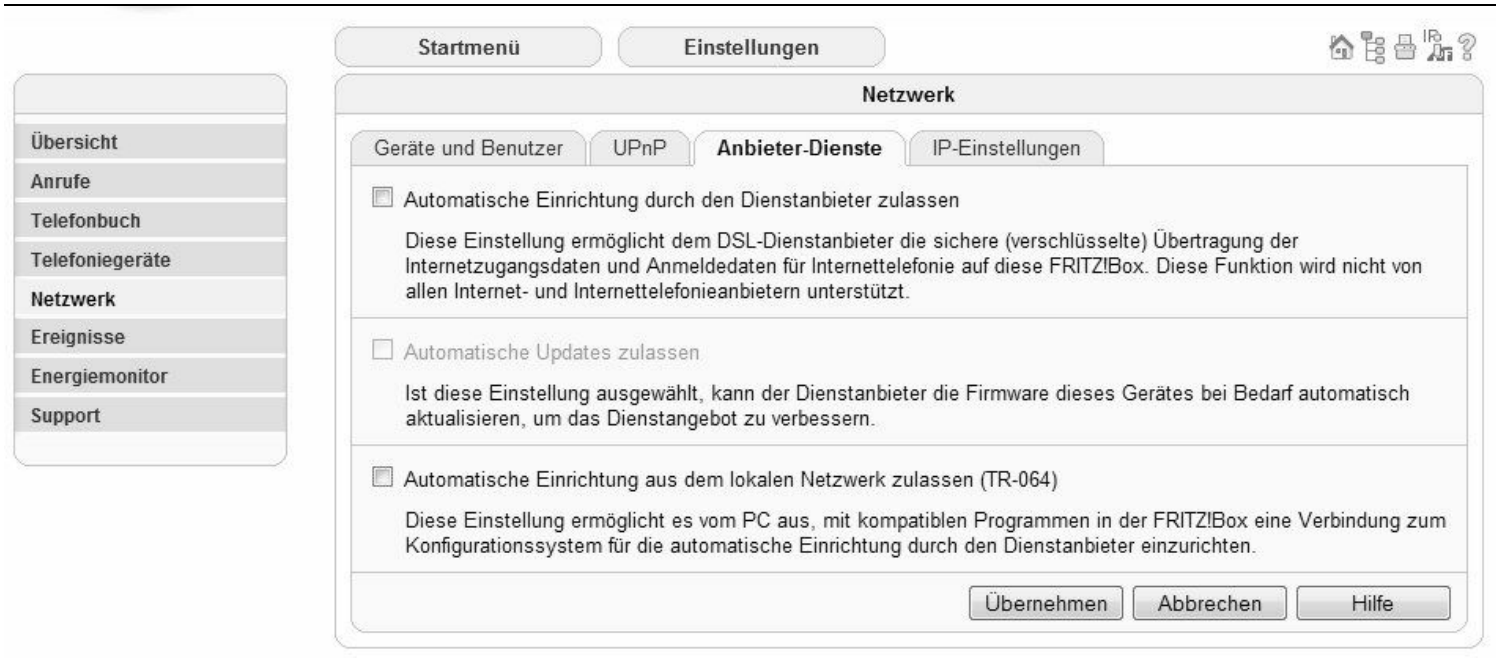


Bild 3.19 Datenschutzfetischisten entfernen in diesem Dialog sämtliche Häkchen. Obwohl die TR-064-Schnittstelle offiziell nur für das Heimnetz gedacht ist, ist das Deaktivieren sicher kein Fehler.

Sind die unerwünschten Häkchen entfernt, muss die FRITZ!Box neu gestartet werden, um die tückischen Systemdienste abzuschalten.

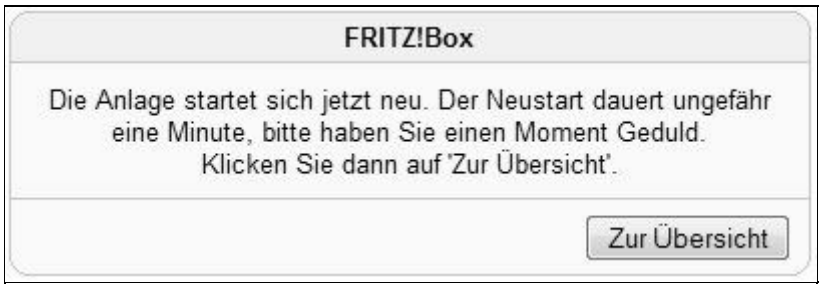


Bild 3.20 Der Neustart der Anlage dauert weniger als zwei Minuten. Anschließend ist zumindest ein Scheunentor zu.

Solange es noch möglich ist, sollten Sie diese Schnittstelle abschalten. Denn ist die TR-069-Schnittstelle aktiviert, ist der Serviceprovider in der Lage, die Konfiguration zu sperren, damit der Kunde nicht mehr auf die entsprechenden Menüoptionen zugreifen kann. Im dümmsten Fall sind, abgesehen von den Mitlesern, auch Leistungseinschränkungen zumindest nicht unmöglich.

Bei den neuen FRITZ!Box-Modellen wie dem Fon WLAN 7390 mit Firmwareversion 84.04.82 finden Sie diese Einstellungen über *Erweiterte Einstellungen/System/Netzwerk/Anbieter-Dienste*.

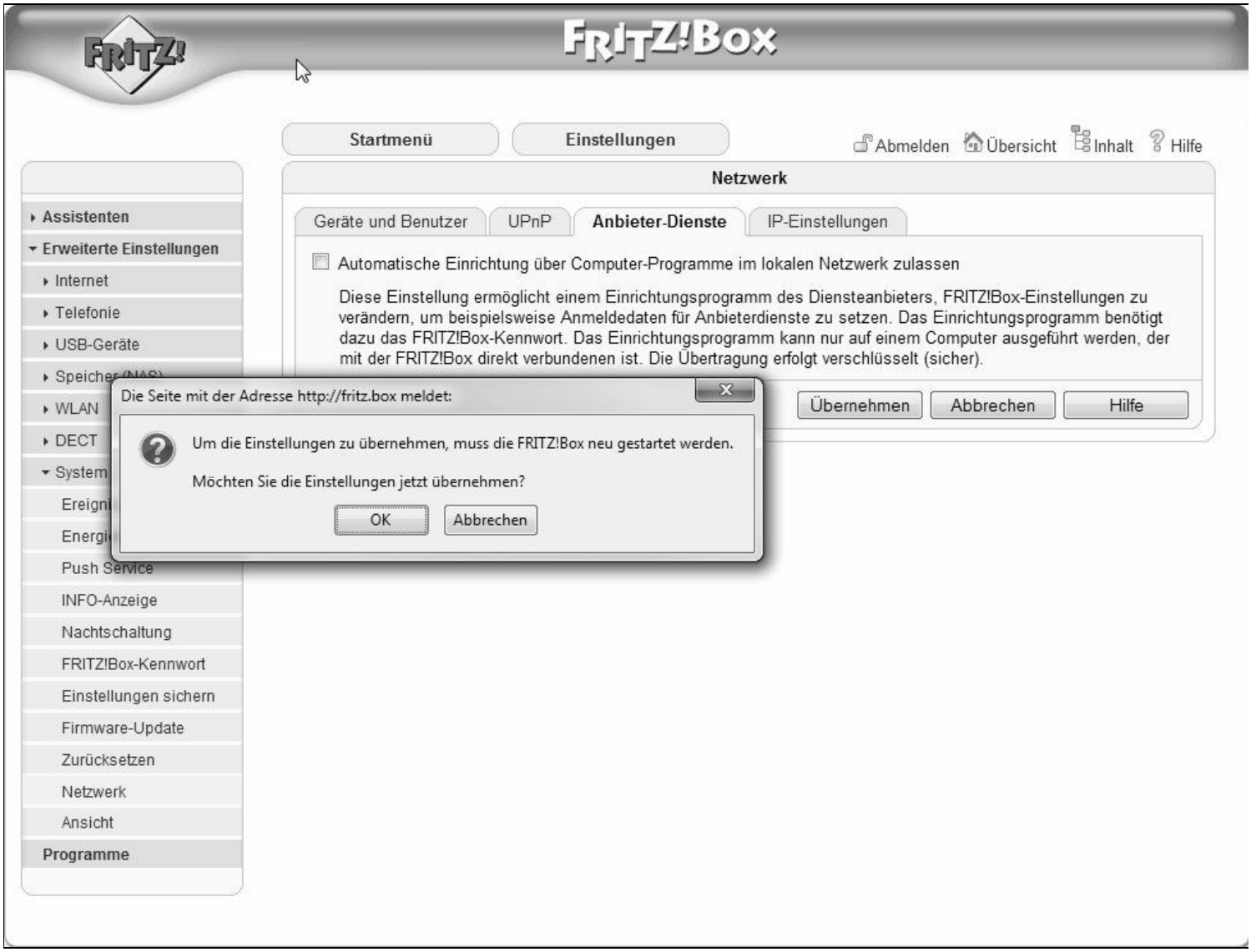


Bild 3.21 Nachdem das Häkchen entfernt wurde, fordert die FRITZ!Box einen Neustart der Anlage an, was weniger als zwei Minuten dauert.

Nach dem Neustart sind die Änderungen aktiv – in der aktuellen Firmware hat AVM hier die früheren Optionen *Automatische Updates zulassen* sowie *Automatische Einrichtung aus dem lokalen Netzwerk zulassen (TR-064)* entfernt.

3.3 Checkliste aller Sicherheitseinstellungen

Für alle, die eine Checkliste bevorzugen: Hier finden Sie sämtliche sicherheitsrelevanten Einstellungen für die WLAN-FRITZ!Box im Schnellüberblick:

Sicherheitsmerkmal	Beschreibung
MAC-Adresse einrichten	Standardmäßig wird jedem drahtlosen PC, der mit einer korrekten SSID, der passenden Verschlüsselung und dem richtigen Netzwerkschlüssel kommt, Zugang zu Ihrem drahtlosen Netzwerk gewährt. Jeder Router bietet jedoch eine MAC-Adressfilterung, durch die PCs basierend auf ihren MAC-Adressen eine Verbindung zum Router aufbauen dürfen oder nicht. Sämtliche drahtlosen Clients müssen zudem über die korrekten SSID- und WEP- bzw. WPA-Einstellungen verfügen, die in den Wireless-Einstellungen konfiguriert werden, um auch das WLAN nutzen zu können.
DHCP ausschalten und feste IP-Adressen zuweisen	Der Router ist standardmäßig als DHCP-Server (*Dynamic Host Configuration Protocol*) konfiguriert, wodurch die TCP/IP-Konfiguration aller an den Router angeschlossenen Computer festgelegt ist. Schalten Sie DHCP aus und vergeben feste IP-Adressen, muss ein Angreifer mit Mühe und Not per Zufall eine verwendete IP-Adresse selbst herausfinden. Der Nachteil: ein etwas höherer Konfigurationsaufwand beim WLAN-PC.
WEP-/WPA-PSK-/WPA2-Verschlüsselung nutzen	Das A und O: Nutzen Sie die sicherste Verschlüsselung (derzeit WPA2) über das Funknetz, auch wenn es etwas Zusatzaufwand bei der Installation bedeutet. Allerdings müssen alle Geräte diesen Standard unterstützen.
Router bei Nichtgebrauch ausschalten	Nicht nur gut für die Umwelt und den Geldbeutel, sondern auch für die Sicherheit des Heimnetzes. Gehen Sie ins Bett oder außer Haus, schalten Sie den WLAN-Router aus. Wenn Sie den Router auch als Telefonanlage (FRITZ!Box) nutzen, sollten Sie auf die Abschaltung verzichten.
Passwörter und Key regelmäßig ändern	Jede Verschlüsselung ist früher oder später knackbar. Deshalb sollten Sie regelmäßig die Passwörter sowie WEP-Schlüssel sowohl im Router als auch am WLAN-PC ändern. Bei WPA2 können Sie nach dem derzeitigen Stand wohl darauf verzichten.
Router-Standardpasswort ändern	Besonders wichtig: Kennt ein Angreifer das Passwort des WLAN-Routers, kann er machen, was er will. Deswegen sollten Sie umgehend nach der Konfiguration das Routerpasswort ändern.
Router-Firmware regelmäßig checken	Kein Produkt ist perfekt, und Sicherheitslücken kommen bei jedem Hersteller vor. Bessere Hersteller bieten dann eine neue Firmware, um Sicherheitslöcher zu stopfen und dem Router neue Funktionalitäten einzuhauchen.
Protokollierung aktivieren und Protokolle auswerten	Zum Nachschauen; zwar lästig und zeitraubend, aber unheimlich hilfreich bei der Suche nach Fehlern und Problemlösungen. Hier spüren Sie Rechner im Netzwerk auf, die mit fremder MAC-Adresse unterwegs sind.
Nicht benötigte Dienste und Webseiten deaktivieren	Weniger ist mehr: Je mehr Dienste und Ports nach außen – also im Internet – zur Verfügung stehen, desto größer ist die Angriffsfläche. Aktivieren Sie also nur Dienste wie HTTP, FTP, Mail etc., die wirklich notwendig sind.
Firewall und Portsecurity aktivieren	Ohne aktivierte Firewall sollte niemand mehr in das Internet gehen. Zu groß ist die Gefahr, Opfer eines Angriffs zu werden. Jeder vernünftige DSL-WLAN-Router bringt eine Firewall mit – aktivieren Sie sie auch!
Wireless-Zugriffsliste einrichten	Standardmäßig wird jedem drahtlosen PC, der mit einer korrekten SSID (*Service Set Identifier*), dem passenden Verschlüsselungsstandard sowie dem richtigen Schlüssel konfiguriert ist, Zugang zu Ihrem drahtlosen Netzwerk gewährt. Erhöhte Sicherheit können Sie erzielen, indem Sie den Zugang zum drahtlosen Netzwerk auf bestimmte PCs beschränken, und zwar auf Grundlage ihrer MAC-Adressen. Klicken Sie im Menü *Wireless-Konfiguration* auf *Zugriffsliste konfigurieren*, um das Menü *Wireless-Zugriffsliste* aufzurufen.
SSID-Rundumsendung ausschalten (SSID-Broadcast deaktivieren)	Wenn diese Option aktiviert ist, sendet der Wireless-Router seinen Netzwerknamen (SSID – *Service Set Identifier*) an alle Wireless-Stationen.
Ping am Internet-Port ausschalten	Wenn Sie wollen, dass der Router auf einen Ping aus dem Internet reagiert, deaktivieren Sie, falls vorhanden, diese Option. Das kann als Diagnosewerkzeug verwendet werden. Sie sollten die Option deshalb nur aktivieren, wenn Sie einen triftigen Grund dazu haben.
Sichere LAN-IP-Adresse verwenden	Für die IP-Adresse des WLAN-Routers nutzen Sie eine IP-Adresse aus dem privaten Netzwerkbereich *192.168.X.X*. Beim Einsatz einer öffentlichen IP-Adresse kommt es sonst zu Problemen bei der Netzwerkverbindung.
Remote-Zugriff ausschalten	Die Routerfernsteuerung ist nur in Unternehmen und Ähnlichem sinnvoll. Der Router kommt zu Hause zum Einsatz und sollte auch dort konfiguriert werden. Deshalb, falls vorhanden, ausschalten!
SSID ändern	Ein sicherer SSID-Name besteht aus einer zufälligen Reihenfolge von Zahlen und Buchstaben, gemischt mit Groß- und Kleinbuchstaben.
Passenden Wireless-Modus wählen	Zufallsprinzip sorgt für Sicherheit: Abhängig von der genutzten WLAN-Karte können Sie den Router so

konfigurieren, dass er nur ein ganz bestimmtes Übertragungsprotokoll nutzt, das natürlich zu Ihren WLAN-Netzwerkkarten passt. So können Sie abhängig vom Routermodell beispielsweise den WLAN-Zugriff auf 802.11g-konforme WLAN-Geräte beschränken. Aufgrund der Kartenvielfalt muss der potenzielle Angreifer schon zufällig eine ähnliche Karte einsetzen.

3.4 Backup der FRITZ!Box-Einstellungen

Ist die FRITZ!Box ordnungsgemäß und sicher konfiguriert, sollten Sie die vorgenommenen Einstellungen sichern. Bessere Geräte bieten dafür eine Möglichkeit, die Einstellungen in einer Konfigurationsdatei zu speichern. Bietet Ihr Modell diese Option nicht an, sollten Sie die gemachten Einstellungen per Screenshot speichern und ausdrucken. Dafür drücken Sie einfach die [Druck]-Taste, um diesen Bildschirm in die Zwischenablage zu kopieren. Anschließend öffnen Sie beispielsweise Word und fügen mit der Tastenkombination [Strg]+[V] den Inhalt der Zwischenablage ein. Schließlich speichern Sie das Dokument oder drucken es wie gewohnt aus.

FRITZ!Box-Einstellungen in einer Datei sichern

Gehen Sie folgendermaßen vor: In der Benutzeroberfläche wählen Sie *Erweiterte Einstellungen/System/Einstellungen sichern*. Geben Sie Ihr Kennwort ein und bestätigen Sie mit *Einstellungen sichern*.

!&fritz7390-45.tif!

Bild 3.22 Übersichtlich gelöst: Das Sichern und Wiederherstellen der FRITZ!Box-Konfiguration geschieht in ein und demselben Dialog.

Arbeiten mehrere Anwender mit dem heimischen Rechner, ist es unter Umständen sinnvoll, die FRITZ!Box-Konfiguration passwortgeschützt auf der Festplatte abzulegen, damit kein Unbefugter die Konfigurationsparameter einsehen oder gar ändern kann. In diesem Fall geben Sie im Bereich *Kennwort* sowie *Kennwortbestätigung* ein Passwort ein. Um die

Einstellungen auf die Festplatte herunterzuladen, genügt der Klick auf die Schaltfläche *Einstellungen sichern*.

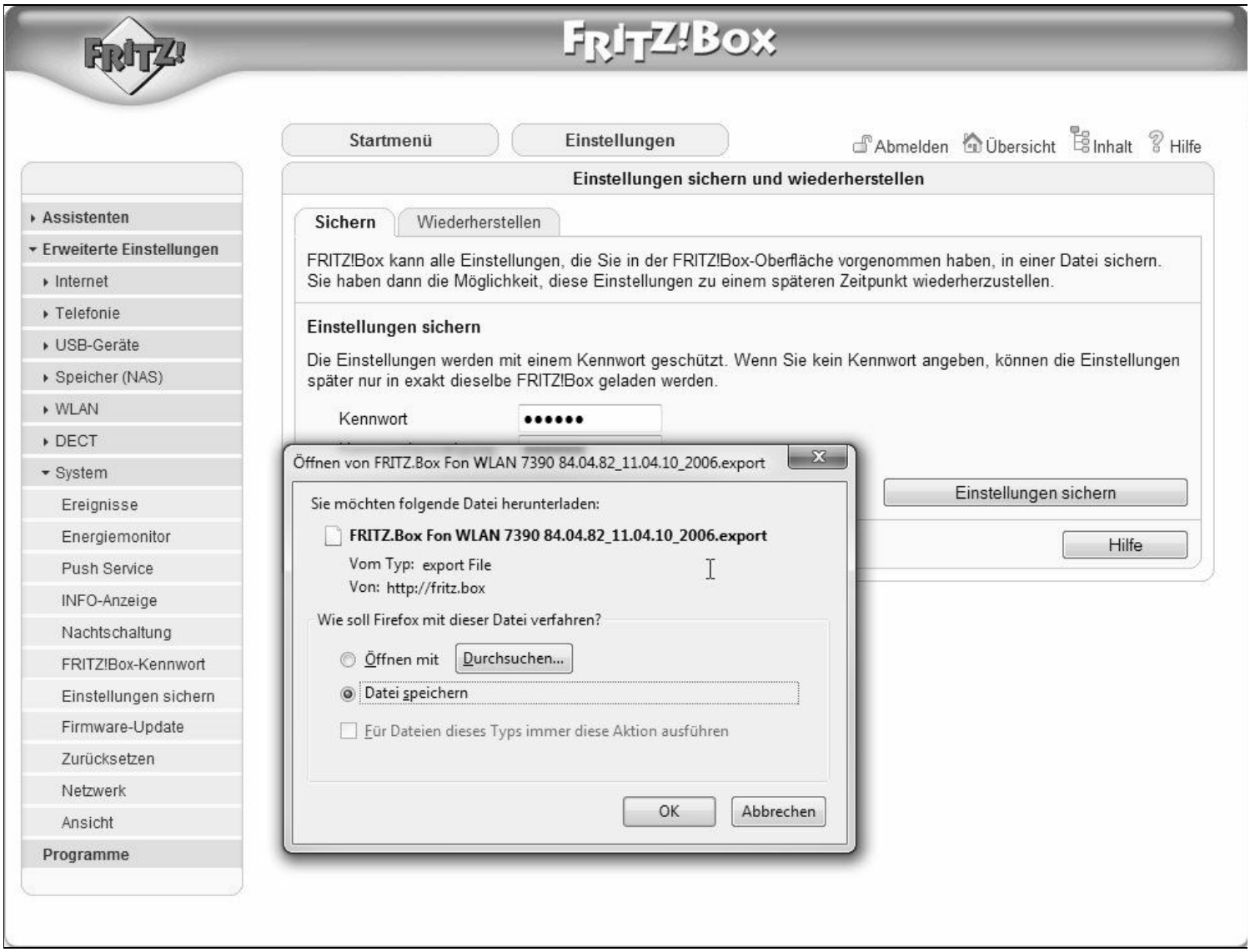


Bild 3.23 Die FRITZ!Box exportiert die Konfiguration in eine Datei mit der Bezeichnung *FRITZ!Box.export*.

Sie können die Routereinstellungen aus dieser Datei wiederherstellen. In der Regel sollten Sie darauf achten, dass Sie beim Wiederherstellen oder Löschen der Routereinstellungen nicht online sind. Ziehen Sie vorsichtshalber das Internetkabel heraus.

4 Firmware aktualisieren

Kein Hersteller ist perfekt: Täglich gibt es neue Veröffentlichungen über Sicherheitslücken und Angriffsmöglichkeiten verschiedenster Routermodelle. Meist wird mit unterschiedlichen Hackertools versucht, den Router zu kompromittieren oder ihn per Buffer Overflow-Mechanismen in einen nicht betriebsfähigen Zustand zu versetzen. Deshalb sollten Sie regelmäßig auf den Supportseiten des Herstellers nach neuer Firmware Ausschau halten. Oft gehen Verbesserungen der Sicherheit auch mit Erweiterungen der Funktionalität oder sogar der Implementierung neuer Standards wie der WPA2-Verschlüsselung einher.

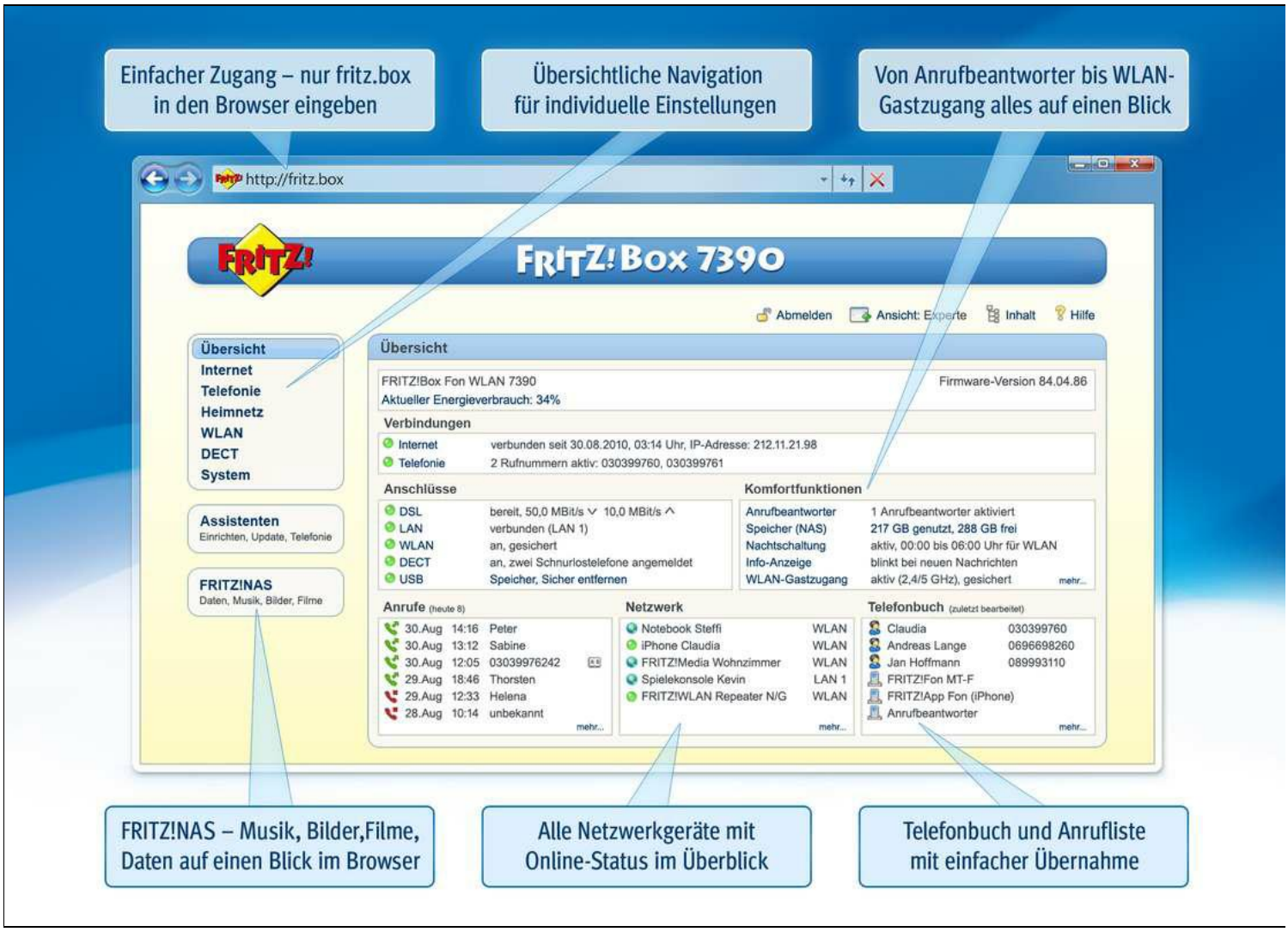


Bild 4.1 AVM bietet für die FRITZ!Box-Modelle 7390, 7320, 7270 und 7240 ab sofort die besten Entwicklungen aus dem FRITZ!-Labor als großes, kostenfreies Upgrade an. Diese Firmware enthält zahlreiche neue Leistungsmerkmale rund um die Bereiche WLAN, NAS, IPv6 und Telefonie. Eine neue Benutzeroberfläche informiert rund um Internet, Heimnetz und Telefonie und bietet intuitiv und schnell individuelle Anpassungen (siehe AVM-Website: *http://www.avm.de/de/News/artikel/online_update.html*).

4.1 Nach neuer Firmware suchen

Ist eine Internetverbindung eingerichtet, bieten manche Geräte auch eine Aktualisierung der Firmware ohne Umwege an. Dafür steht eine Option auf den Routerkonfigurationsseiten zur Verfügung. Hier sucht der Router selbstständig die aktuellste Version auf den Supportseiten.

Bild 4.2 Bei der FRITZ!Box können Sie die Firmware entweder über den AVM-Server (hier Schaltfläche *Neue Firmware suchen*) oder über eine Firmwaredatei (Register *Firmware-Datei*), die sich auf der Festplatte befindet, aktualisieren.

Je nach Herangehensweise müssen Sie bei einem Direktdownload nach dem Herunterladen diese Datei entpacken, bevor Sie das Gerät mit der neuen Firmware aufrüsten können. In einigen Fällen kann es sein, dass der Router nach dem Einspielen der Firmware neu konfiguriert werden muss.

Deshalb ist es sinnvoll, vor dem Einspielen der neuen Firmware die Routereinstellungen zu sichern. Bei den neueren Modellen verlangt die FRITZ!Box das Anfertigen eines Backups mit den Einstellungen, bevor eine neue Firmware aufgespielt werden kann. Hierzu klicken Sie zunächst bei *Übersicht/Einstellungen/Erweiterte Einstellungen/System/Firmware-Update* auf die Schaltfläche *Einstellungen sichern*.

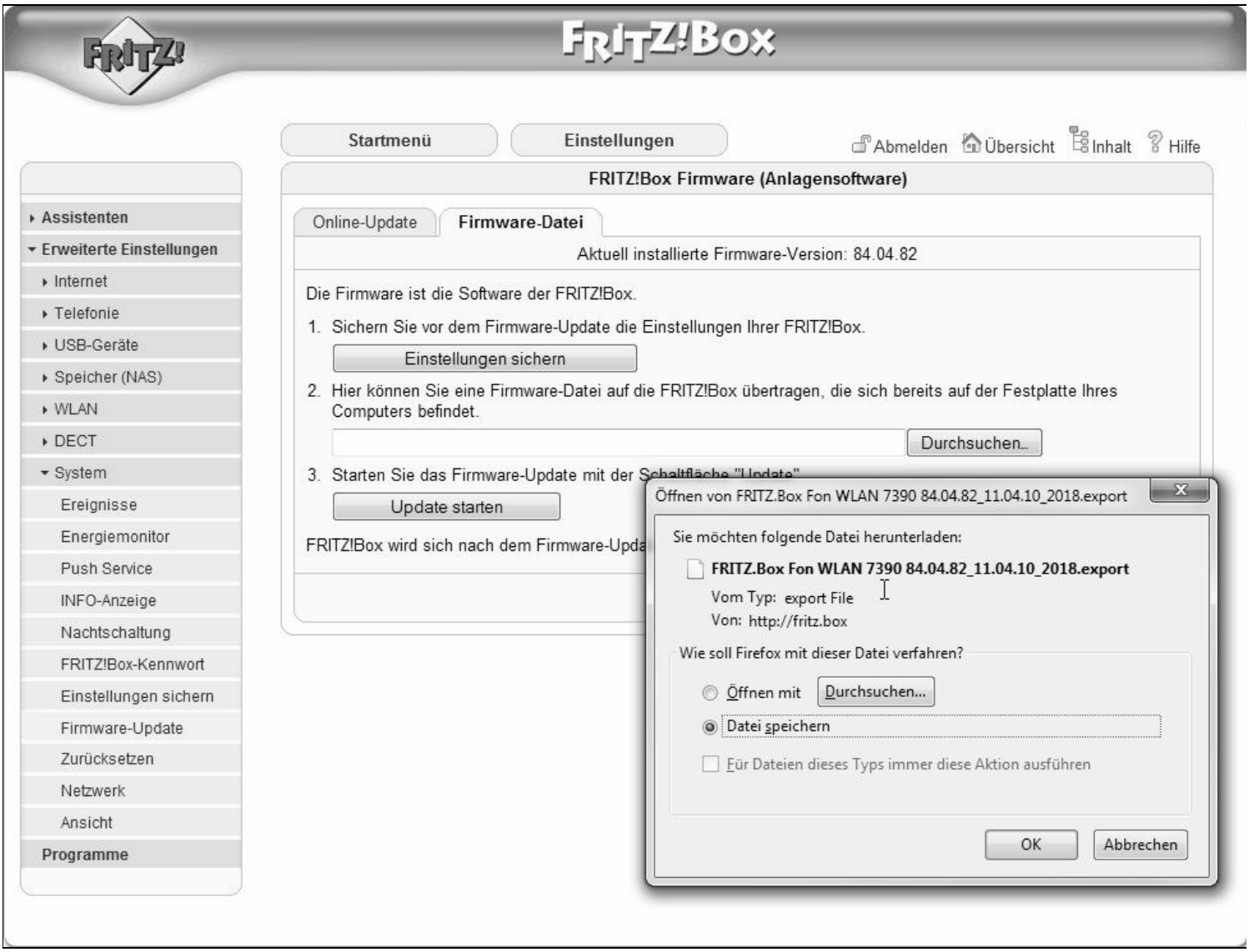


Bild 4.3 Zunächst sichern Sie die aktuellen Einstellungen der FRITZ!Box auf die Festplatte.

4.2 Firmware in den Router laden

Sind die Einstellungen gespeichert, kann die neue Firmware in die Box geladen werden. Dafür wählen Sie zunächst über die *Durchsuchen*-Schaltfläche den Pfad zur Firmwaredatei aus.

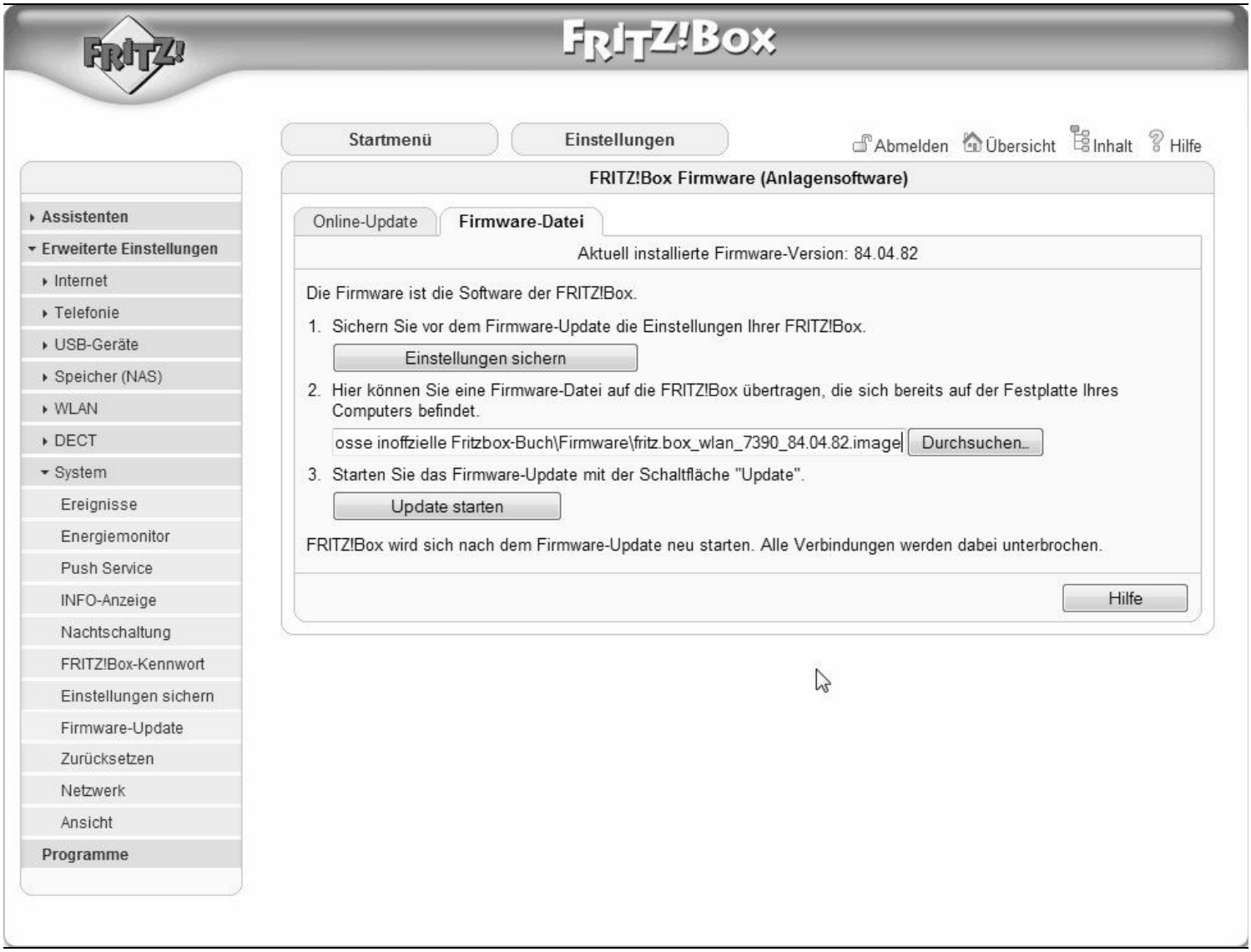


Bild 4.4 Entweder via Internet oder über eine Firmwaredatei: Eine frische Firmware sorgt für Sicherheit.

Mit einem Klick auf eine der Schaltflächen *Update*, *Hochladen* oder *Firmware aktualisieren* spielt der Router die neue Firmware selbstständig ein.

Bild 4.5 Bitte warten: Während der Übertragung der Firmware auf den Router darf die Stromversorgung nicht unterbrochen werden.

Während dieses Vorgangs darf der Router weder ausgeschaltet werden noch online (also im Internet) sein. Ist der Vorgang abgeschlossen, rufen Sie den *Routerstatus* auf und prüfen die Firmwareversion, um sicherzustellen, dass auf dem Router nach dem Update die neueste Software installiert ist.

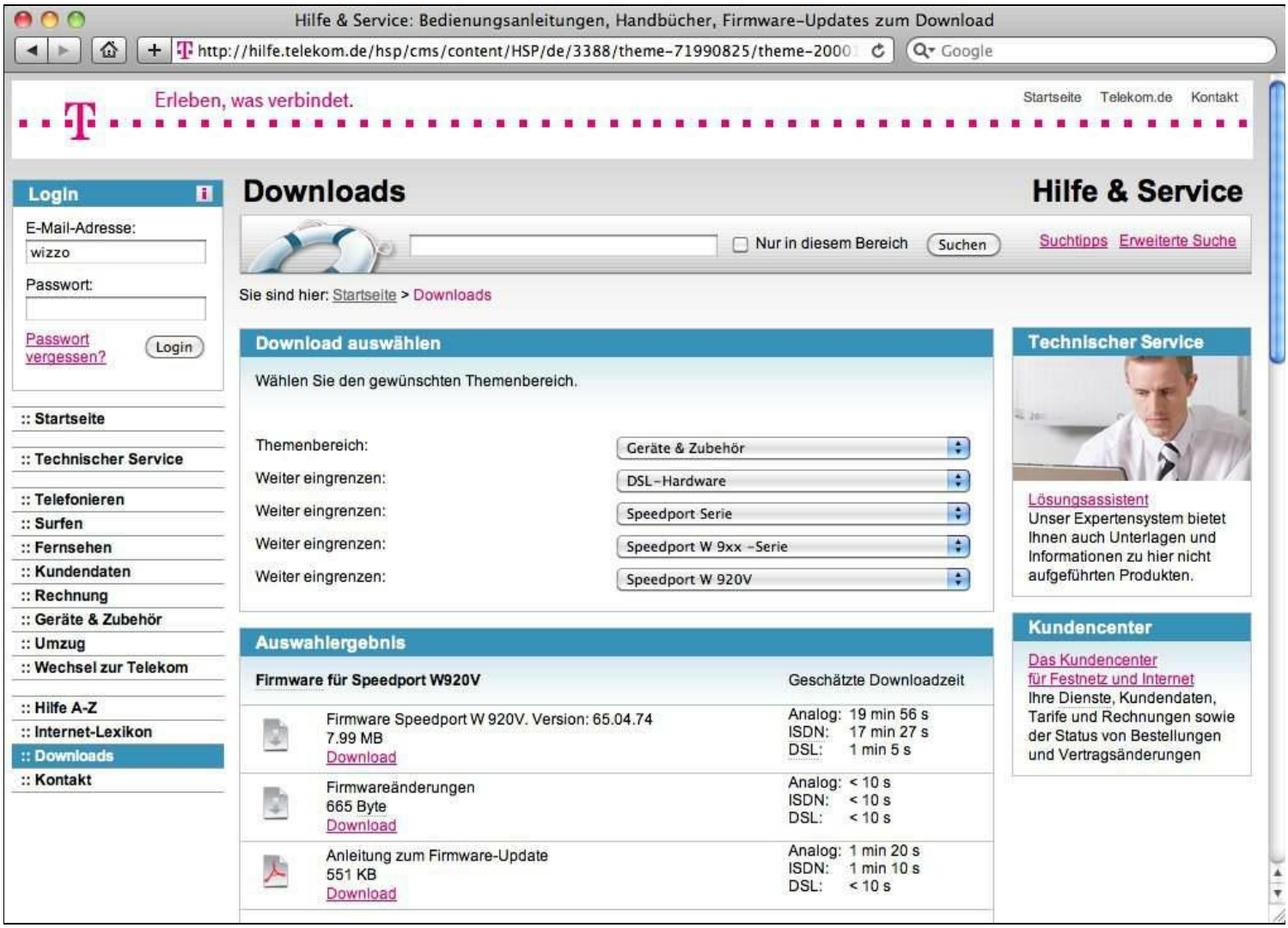


Bild 4.6 Arbeiten Sie mit dem T-Home Speedport, vergleichen Sie die Firmwareversion im Menü des Routers mit der auf der Telekom-Website angegebenen Firmwareversion.

Warum lässt Windows das Firmware-Update nicht zu?

Ein Firmware-Update der FRITZ!Box ist bekanntlich von Zeit zu Zeit nicht nur sinnvoll, sondern aus Sicherheitsgründen auch ratsam. Neue Funktionen und das Stopfen von Sicherheitslücken sorgen dafür, dass der Computer bzw. das Heimnetz vor etwaigen Angriffen aus dem Internet geschützt bleibt. Setzen Sie Windows Vista oder Windows 7 mit einem älteren Internet Explorer als Version 8 ein, ist ein Firmware-Update nicht auf Anhieb möglich.

Der Grund: Die Sicherheitseinstellungen des standardmäßig installierten Internet Explorers oder auch der Firewall lassen das Ausführen des Firmware-Updates nicht zu. Haben Sie sich aus dem Internet eine aktuelle Firmwaredatei besorgt, erscheint beim eigentlichen Firmware-Update die Meldung *Bitte den vollständigen Pfadnamen angeben*, und die Installation ist nicht möglich.

Bild 4.7 Wie gewohnt: Unter *Übersicht/Erweiterte Einstellungen/System/Firmware-Update* spielen Sie eine frische Firmware ein.

Bild 4.8 Erhalten Sie bei einem Firmware-Update die Fehlermeldung *Bitte den vollständigen Pfadnamen angeben*, ist das Firmware-Update mit diesem Browser nicht möglich.

Abhilfe schafft das Ändern der Sicherheitseinstellungen im Internet Explorer oder das temporäre Deaktivieren der aktiven Schutzprogramme, z. B. der Windows-Firewall. Nach dem Update können Sie die Schutzprogramme wieder einschalten.

Empfehlenswerter ist auf jeden Fall das Aktualisieren des Internet Explorers auf die aktuellste Version via Windows Update oder gar der komplette Umstieg auf den Mozilla Firefox-Browser. Firefox kennt die beschriebenen Update-Probleme nicht.

5 Erste Hilfe beim Crash

Bis die FRITZ!Box mit den optimalen Einstellungen konfiguriert ist, ist es ein weiter Weg. Treten Konfigurationsfehler auf, hängt es zunächst davon ab, ob und auf welche Art und Weise die FRITZ!Box modifiziert wurde. Wer die Originalfirmware unangetastet gelassen und die FRITZ!Box nicht mit einer gemoddeten Firmware bespielt hat, kann es zunächst mit dem AVM-Support probieren und so den Fehler korrigieren.

5.1 Nur die Ruhe bewahren!

Gerade wenn versehentlich wichtige Netzwerkparameter wie IP-Adressen verändert werden, kann es sein, dass die FRITZ!Box nicht mehr so funktioniert, wie sie eigentlich soll, der Internetzugriff nicht mehr möglich ist oder gar der Zugriff auf die Benutzeroberfläche der FRITZ!Box scheitert.

Wer sich jedoch bereits in die Tiefen des FRITZ!Box-Hackens begeben hat, für den sind die AVM-Türen verständlicherweise geschlossen. Hier sind andere Wege nötig, um die FRITZ!Box wieder zur Zusammenarbeit zu bewegen. Manchmal reicht ein simpler Neustart, um nach dem Reboot über die Weboberfläche den Fehler auszubügeln. Es gibt aber auch weitere Kniffe, um die FRITZ!Box wieder zum Leben zu erwecken.

Was tun, wenn man das Kennwort vergessen hat?

Für Vergessliche: Wer das Kennwort der FRITZ!Box-Konfigurationsoberfläche vergessen hat, braucht nicht zu verzweifeln. Denn die FRITZ!Box lässt sich innerhalb der ersten zehn Minuten nach dem Neustart per Webbrowser auf die AVM-Werkeinstellungen zurücksetzen. In dieser Zeit ist das Konfigurationsmenü trotz aktivierten Passwortschutzes ohne Passwort zugänglich.

Bild 5.1 AVM liefert bei seinen FRITZ!Boxen eine undokumentierte Passwortrücksetzseite mit – *http://fritz.box/html/vergessen.html*.

Doch nicht nur bei einem Passwortproblem, sondern auch bei einer »verkonfigurierten« FRITZ!Box können Sie mit den

Werkeinstellungen der FRITZ!Box wieder von vorn beginnen.

Bild 5.2 Bevor Sie auf *OK* klicken, sollten Sie unbedingt alle Zugangsdaten gesichert haben.

Vor dem Wiederherstellen der Werkeinstellungen

Stellen Sie Werkeinstellungen der FRITZ!Box wieder her, werden auch sämtliche anderen Konfigurationsparameter wie Providerzugangsdaten, Port-/Firewall-Einstellungen, Netzwerkparameter etc. auf die Standardeinstellungen gesetzt. Notieren Sie unbedingt alle wichtigen Zugangsdaten und hinterlegen Sie sie zu Hause an einem sicheren Ort. Den Router auf die Werkeinstellungen zurücksetzen und wieder neu aufsetzen, kostet »nur« Zeit. Wenn Sie aber darüber hinaus Ihre Internetzugangsdaten nicht mehr wissen, haben Sie ein Problem. In dem Fall müssen Sie sich an die Hotline des Internetproviders wenden und die Zugangsdaten neu anfordern. Das kostet Zeit, Geld und Nerven.

Sollte der Zugriff auf die FRITZ!Box jedoch per Webbrowser nicht möglich sein, weil die Netzwerkparameter nicht stimmen, können Sie mithilfe eines angeschlossenen Telefons die FRITZ!Box ebenfalls zurücksetzen. Dieser Trick funktioniert natürlich nur für die FRITZ!Box mit der »Fon«-Erweiterung und einer neueren Firmware.

Ist das Telefon eingesteckt, können Sie die FRITZ!Box mit der Tastenfolge *#991*15901590** auf die Werkeinstellungen bringen. Anschließend warten Sie zwei bis drei Minuten, die FRITZ!Box müsste selbstständig einen Neustart durchführen. Danach ist sie mit den jungfräulichen Einstellungen konfiguriert.

Sie erreichen die FRITZ!Box nun über ihre Standard-IP-Adresse *http://192.168.178.1* oder über *http://fritz.box*. Der standardmäßig aktivierte DHCP-Server ist in diesem Fall eingeschaltet, unter Umständen müssen die Netzwerkeinstellungen des Computers in der Systemsteuerung auf *IP-Adresse und DNS-Adresse automatisch beziehen* umgestellt werden.

So finden Sie die versteckte IP-Adresse 192.168.178.254

Standardmäßig arbeitet die FRITZ!Box als DHCP-Server und versorgt die angeschlossenen Computer mit einer IP-Adresse und weiteren Netzwerkparametern. Grundsätzlich lässt sich die FRITZ!Box über den Webbrowser entweder mit der IP-Adresse oder mit ihrem Namen (*http://fritz.box*, *http://fritz.box.fon*, *http://fritz.box.wlan*, abhängig vom FRITZ!Box-Modell) ansprechen, um auf die Konfigurationsseiten der Box zu gelangen.

1. Dafür öffnen Sie den Webbrowser und probieren diese Möglichkeiten durch. Standardmäßig ist die FRITZ!Box auf das Subnetz *192.168.178.X* konfiguriert und lässt sich via LAN-Schnittstelle über die IP-Adresse *192.168.178.1* ansprechen.
2. Haben Sie jedoch die Adressparameter falsch eingetragen oder gar vergessen, ist der Zugriff auf die FRITZ!Box zunächst nicht möglich. Nach einem Neustart der Box kann der Computer auf die FRITZ!Box zugreifen, wenn der eingebaute DHCP-Server noch aktiviert ist. In diesem Fall stellen Sie die Netzwerkkonfiguration des Computers auf *IP-Adresse und DNS-Adresse automatisch beziehen* um.
   Anschließend bekommt der Computer eine zum Subnetz der FRITZ!Box passende Konfiguration übergeben. Nun ist auch der Zugriff auf die Konfigurationsseiten der Box wieder möglich.
3. Noch schwieriger wird es, wenn der DHCP-Server der FRITZ!Box deaktiviert wurde. Die angeschlossenen Computer können die FRITZ!Box nicht finden, solange sich die Geräte nicht in einem gemeinsamen Subnetz befinden. Um diesen Konfigurationsfehler zu beheben, hilft die fest eingestellte IP-Adresse *192.168.178.254* der FRITZ!Box. Stellen Sie die IP-Adresse der Netzwerkkarte des Computers, die mit der FRITZ!Box Verbindung aufnehmen soll, neu ein.

Der Zugang über die IP-Adresse klappt nicht?

Manche FRITZ!Box-Modelle mit mehreren LAN-Anschlussbuchsen lassen den Zugriff über die IP-Adresse 192.168.178.254 nur über einen bestimmten Anschluss (in der Regel den nächstliegenden zur Stromversorgung) zu. Klappt der Zugang über die IP-Adresse nicht, stecken Sie das Netzwerkkabel einfach in eine andere Buchse um und probieren es erneut.

1. Dafür wechseln Sie in der Systemsteuerung und in den Eigenschaften der LAN-Verbindung zu den IP-Adressparametern und stellen hier eine feste IP-Adresse wie beispielsweise *192.168.178.10* sowie für die Subnetzmaske die Adresse *255.255.255.0* ein. Für den DNS-Server sowie für die Gateway-Adresse tragen Sie die IP-Adresse der FRITZ!Box ein, also *192.168.178.254*. Anschließend können Sie über die IP-Adresse *http://192.168.178.254* auf die Weboberfläche der FRITZ!Box zugreifen und mögliche fehlerhafte Einstellungen berichtigen.

Hardcore-Crash? Dann hilft das AVM-Tool weiter

Ist die Konfiguration der FRITZ!Box richtig verpfuscht oder hat es beim Einspielen einer neuen Firmware einen Stromausfall gegeben, startet die FRITZ!Box nicht mehr wie gewohnt. So deutet beispielsweise das Blinken aller LEDs darauf hin, dass ein Firmware-Update nicht erfolgreich durchgeführt wurde. Jetzt muss das Firmware-Update auf einem anderen Weg eingespielt werden.

In diesem Fall und in anderen Hardcore-Fällen hilft ein Recovery-Tool des FRITZ!Box-Herstellers AVM. Für die meisten FRITZ!Box-Modelle bietet AVM auf seinem FTP-Server ein passendes Recovery-Werkzeug an. Ist es auf dem FTP-Server nicht zu finden, ist es über den E-Mail-Support erhältlich. Wer die mit der FRITZ!Box mitgelieferte CD noch zur Hand hat, wird auch dort unter Umständen fündig: Bei neueren Modellen ist dieses Recovery-Werkzeug mit auf der Scheibe.

Recovery-Werkzeug: modellabhängig

Abhängig von den FRITZ!Box-Modellen, die zum Leben erweckt werden sollen, sind die Recovery-Werkzeuge unterschiedlich. Das Wiederherstellungsprogramm darf ausschließlich zur Wiederherstellung der im Dateinamen angegebenen FRITZ!Box verwendet werden.

Zur Auswahl des Recovery-Werkzeugs gehen Sie folgendermaßen vor:

1. Zunächst stellen Sie eine Verbindung zum AVM-FTP-Server her. Dafür geben Sie in der Adresszeile des Webbrowsers die URL *ftp://ftp.avm.de* ein. Danach wechseln Sie in das passende Unterverzeichnis. Jedes FRITZ!Box-Modell hat auf dem FTP-Server von AVM seinen eigenen Ordner.

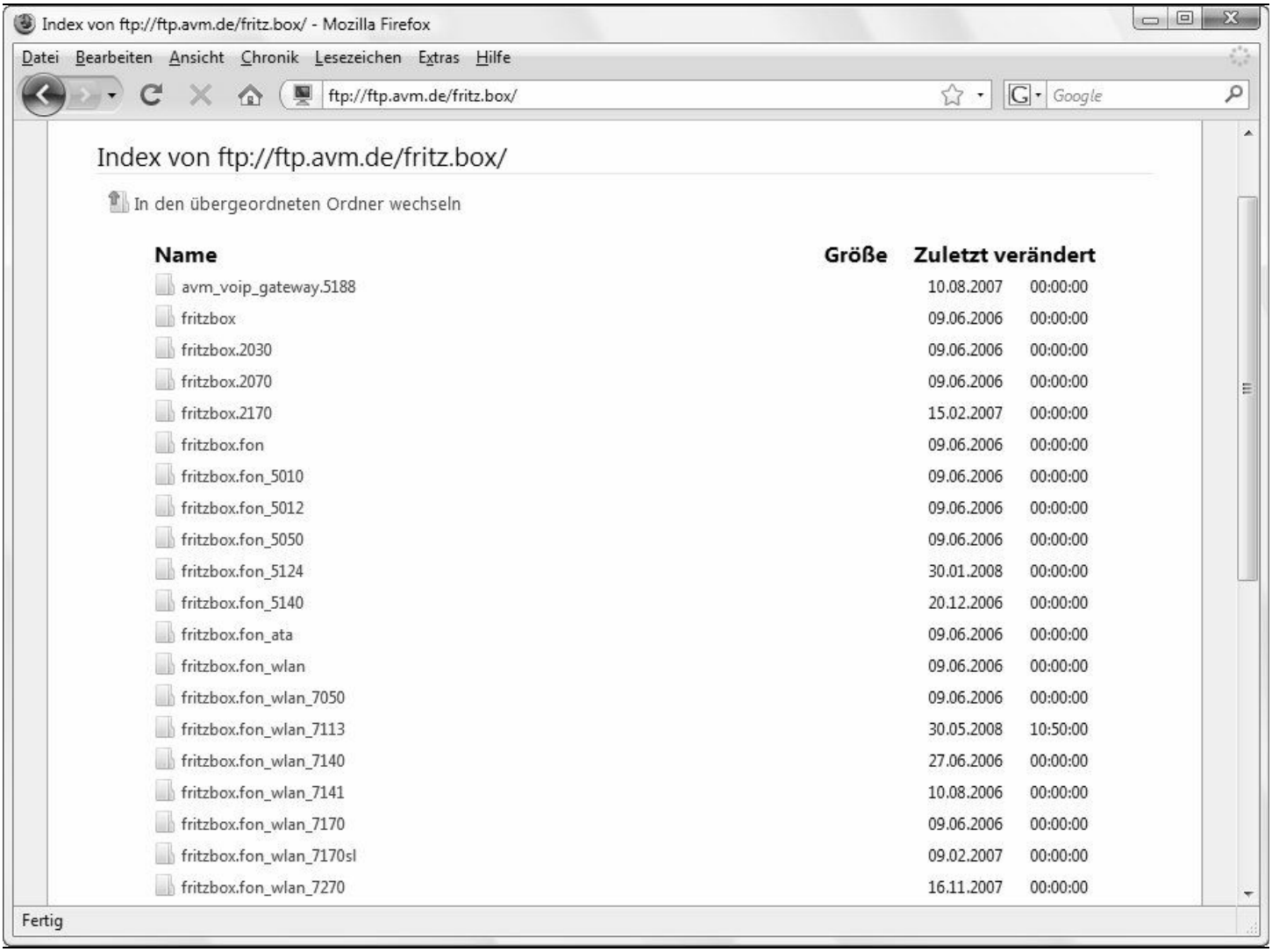


Bild 5.3 Hier ist für nahezu jede FRITZ!Box das wichtige Wiederherstellungsprogramm erhältlich: *ftp://ftp.avm.de*

2. Dort finden Sie (in der Regel im Unterverzeichnis *x_misc\deutsch*) eine Datei, die mit der Bezeichnung *recover-image.exe* endet. Um auf Nummer sicher zu gehen, codiert AVM in den Namen dieser Datei das entsprechende FRITZ!Box-Modell sowie die in dem Recovery-Programm enthaltene Firmwaredatei.

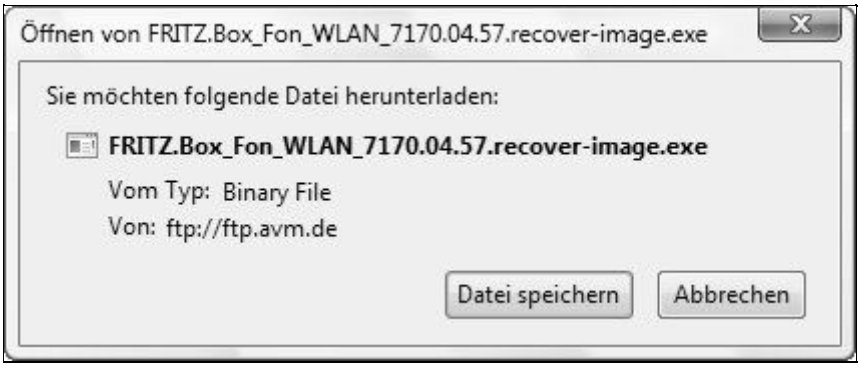


Bild 5.4 So ist beispielsweise die Datei FRITZ.Box_Fon_WLAN_7170.04.57.recover-image.exe für die FRITZ!Box 7170 vorgesehen und bringt die Firmwareversion 04.57 für dieses Gerät mit.

3. Laden Sie die Datei, die dem Typ Ihrer FRITZ!Box entspricht, auf Ihren PC. In diesem Beispiel haben wir die FRITZ!Box 7170 verwendet – die Herangehensweise ist bei anderen Modellen nahezu identisch.

TCP/IP-Netzwerkkonfiguration überprüfen

Zunächst stellen Sie sicher, dass die FRITZ!Box mit dem Netzwerkkabel an der Netzwerkkarte des Computers angeschlossen ist. Anschließend überprüfen Sie im folgenden Abschnitt die TCP/IP-Netzwerkkonfiguration des Computers.

1. Über *Start/Einstellungen/Systemsteuerung/Netzwerk- und Internetverbindungen/Netzwerkverbindungen* wählen

Sie per Rechtsklick auf die LAN-Verbindung der Netzwerkkarte, die mit der FRITZ!Box verbunden ist, den Kontextmenüpunkt *Eigenschaften* aus.

2. Markieren Sie hier *Internetprotokoll TCP/IP* und klicken Sie auf *Eigenschaften*. Schalten Sie DHCP aus und aktivieren Sie *Folgende IP-Adresse verwenden*. Nun können Sie bei *IP-Adresse* die IP-Adresse 192.168.178.10 eintragen, sofern kein anderer Computer im lokalen Netzwerk diese Adresse bereits besitzt. Für *Subnetzmaske* tragen Sie die Adresse 255.255.255.0 ein, für *Standardgateway* und *Bevorzugter DNS-Server* verwenden Sie die IP-Adresse 192.168.178.1, die für die FRITZ!Box vorgesehen ist. Bestätigen Sie per Klick auf die *OK*-Schaltfläche die Änderungen und beenden Sie mit Klick auf *Schließen* diesen Dialog.
3. Damit das Wiederherstellen der Firmware auch klappt, muss zudem das sogenannte IP-Filtering ausgeschaltet sein. Dazu gehen Sie folgendermaßen vor: Über *Start/Einstellungen/Systemsteuerung/Netzwerkverbindungen* wählen Sie im Menü *Ansicht* die Option *Details* aus.
4. In der Liste der Netzwerk- und DFÜ-Verbindungen wählen Sie mit einem Rechtsklick die LAN-Verbindung aus, bei der die Netzwerkkarte in der Spalte *Gerätename* eingetragen ist. Dort klicken Sie auf *Eigenschaften* und wählen im Feld *Diese Verbindung verwendet folgende Elemente* den Eintrag *Internetprotokoll (TCP/IP)* aus.
5. Anschließend markieren Sie bei *Eigenschaften/Erweitert* nach Auswahl der Registerkarte *Optionen* im Feld *Optionale Einstellungen* den Eintrag *TCP/IP-Filter* und klicken auf *Eigenschaften*. Ist das Häkchen bei der Option *TCP/IP-Filter aktivieren* gesetzt, nehmen Sie es heraus und bestätigen per Klick auf *OK* die Änderung.

Wiederherstellungsprogramm der FRITZ!Box starten

1. Sobald die Verbindung PC-seitig konfiguriert ist, starten Sie das Wiederherstellungsprogramm der FRITZ!Box. Dazu braucht die FRITZ!Box nicht mit Strom versorgt zu werden, lediglich das Netzwerkkabel zwischen der FRITZ!Box und dem Computer muss eingesteckt sein.

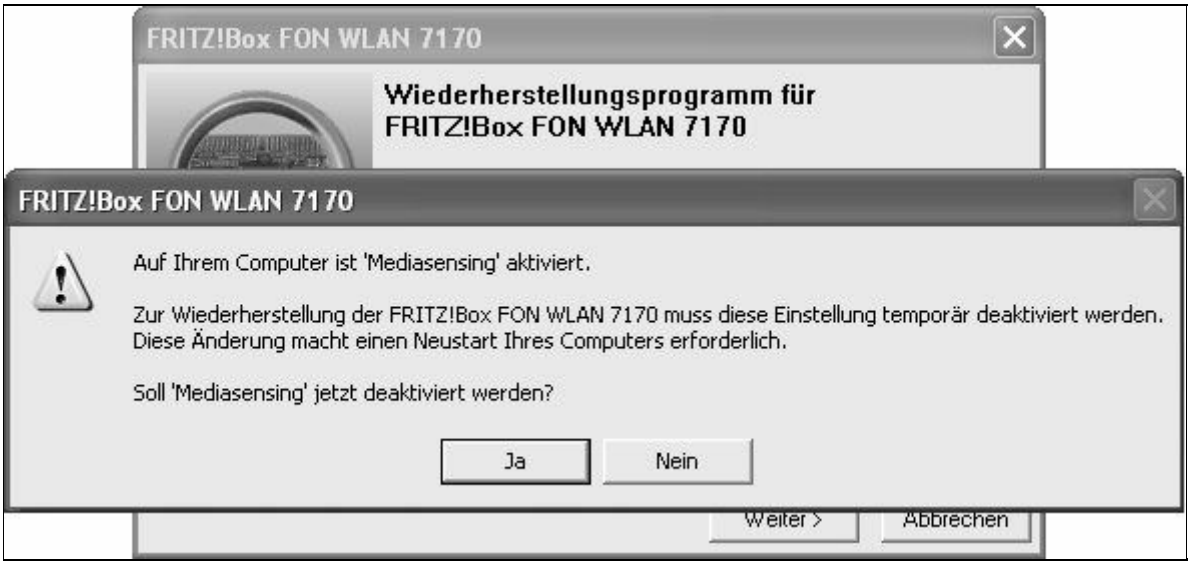


Bild 5.5 Damit sich das »Mediasensing« am PC deaktivieren lässt, müssen Sie am Computer mit Administratorrechten angemeldet sein.

2. Sind Sie als Administrator bzw. als Benutzer mit Administratorrechten am Computer angemeldet, können Sie das zur FRITZ!Box passende Recovery-Programm starten. Halten Sie sich nur an die Anweisungen des Wiederherstellungsprogramms. Erst mal schaltet das Recovery-Programm »Mediasensing« temporär aus, was zunächst einen Rechnerneustart erforderlich macht.

Bild 5.6 Nach dem Deaktivieren des Mediasensing muss der Computer neu gestartet werden.

3. Nach dem Neustart des Computers müssen Sie sich erneut mit Administratorrechten anmelden. Ist auf dem Computer eine PC-Firewall (z. B. Windows XP-Firewall (ab SP2), Vista-Firewall oder Norton Internet Security) aktiv, schalten Sie sie für die Zeit der FRITZ!Box-Reparatur aus. Unter Windows Vista und XP deaktivieren Sie die Windows-eigene Firewall über *Systemsteuerung/Sicherheitscenter/Sicherheitseinstellungen verwalten für/Windows-Firewall*. Nun können Sie das FRITZ!Box-Recovery-Programm neu starten.

Bild 5.7 Nach dem Neustart ist die FRITZ!Box auf die Werkeinstellungen zurückgesetzt und sollte nun wie gewohnt einsetzbar sein.

Befolgen Sie einfach die Anweisungen auf dem Bildschirm. Erst wenn das Programm Sie dazu auffordert, die FRITZ!Box wieder mit Strom zu versorgen, stecken Sie das Stromkabel in die FRITZ!Box ein. Nach der erfolgreichen Wiederherstellung verlangt das Recovery-Programm einen Neustart der FRITZ!Box.

FRITZ!Box mit dem Konsolenbefehl telnetd checken

Der Zugriff auf die FRITZ!Box über Telnet ist aus Sicherheitsgründen nur im sicheren privaten Heimnetz zu empfehlen. Damit über das Internet kein Schindluder getrieben werden kann, hat AVM den Konsolenzugriff auf die FRITZ!Box standardmäßig deaktiviert. Für Profis hat AVM jedoch ein Hintertürchen offen gelassen – der Telnet-Dienst telnetd lässt sich mit einem an der FRITZ!Box angeschlossenen Telefon einfach ein- und wieder ausschalten.

Um den Telnet-Dienst mit einem an der FRITZ!Box angeschlossenen Telefon einzuschalten, wählen Sie am Telefon einfach:

```
#96*7* ANRUFTASTE
```

und zum Ausschalten:

```
#96*8* ANRUFTASTE
```

Jede Änderung wird mit einem kurzen Bestätigungston quittiert und ist umgehend aktiv. Zudem bleibt die Änderung auch nach einem Neustart der FRITZ!Box aktiv – im Zweifelsfall sollten Sie aus Sicherheitsgründen Telnet auch nur dann aktivieren, wenn es benötigt wird.

Das Passwort für den Zugriff via Telnet ist dasselbe, das für den Zugriff via Weboberfläche gesetzt ist. Da Telnet auch nach einem Neustart der FRITZ!Box aktiv bleibt, sollten Sie Telnet aus Sicherheitsgründen nach den Wartungsarbeiten an der FRITZ!Box wieder abschalten.

Vergessene Kennwörter per Kommandozeile auslesen

Die FRITZ!Box dient nicht nur als Schaltzentrale für den Internetzugang, sondern lässt sich auch für andere Dienste wie beispielsweise die Telefonie nutzen. Einmal richtig eingerichtet, braucht man in der Regel die Passwörter für VoIP höchst selten. Bei einem Routerwechsel, einem Firmware-Update oder einem Hardware-Reset kann es jedoch vorkommen, dass die Passwörter wieder wichtig werden – wer sie vergessen hat, kann sie per Kommandozeile auslesen. Dazu verbinden Sie sich via Telnet oder SSH – falls Freetz installiert ist – mit der FRITZ!Box.

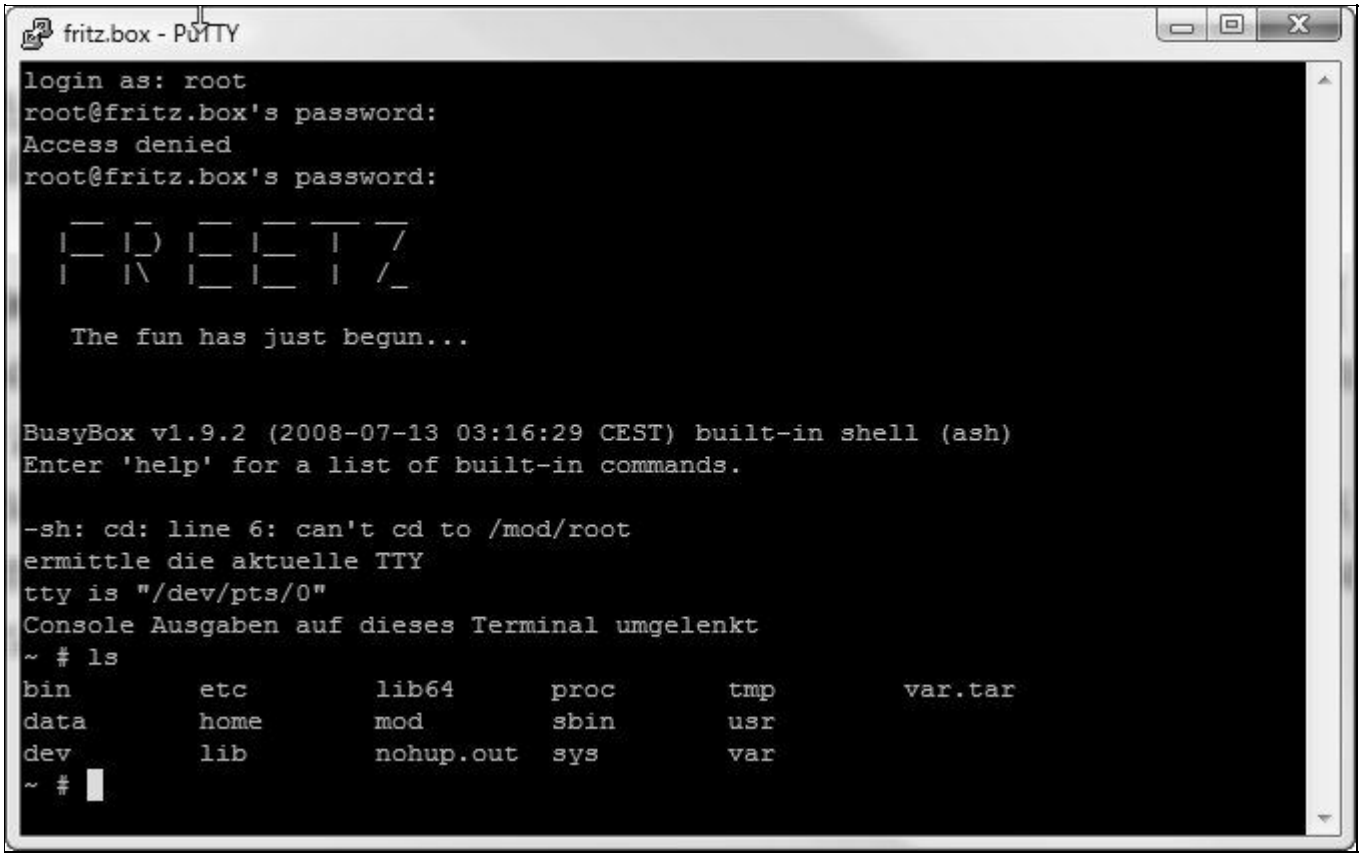


Bild 5.8 Zum Einloggen via SSH verwenden Sie den Root-User – das Passwort ist im Idealfall gleich dem der Weboberfläche.

Sind Sie per SSH oder Telnet mit der FRITZ!Box verbunden, liegen die Geheimnisse in Reichweite: Um beispielsweise das

Voice over IP-(VoIP-)Passwort auf der FRITZ!Box auszulesen, sind nur zwei Befehle notwendig:

```
allcfgconv -C voip -c -o /var/tmp/voip.cfg
cat /var/tmp/voip.cfg
```

Das Vorgehen ist nicht nur auf die Internettelefonie beschränkt, sondern lässt sich auch auf sämtliche FRITZ!Box-Kennwörter ausweiten:

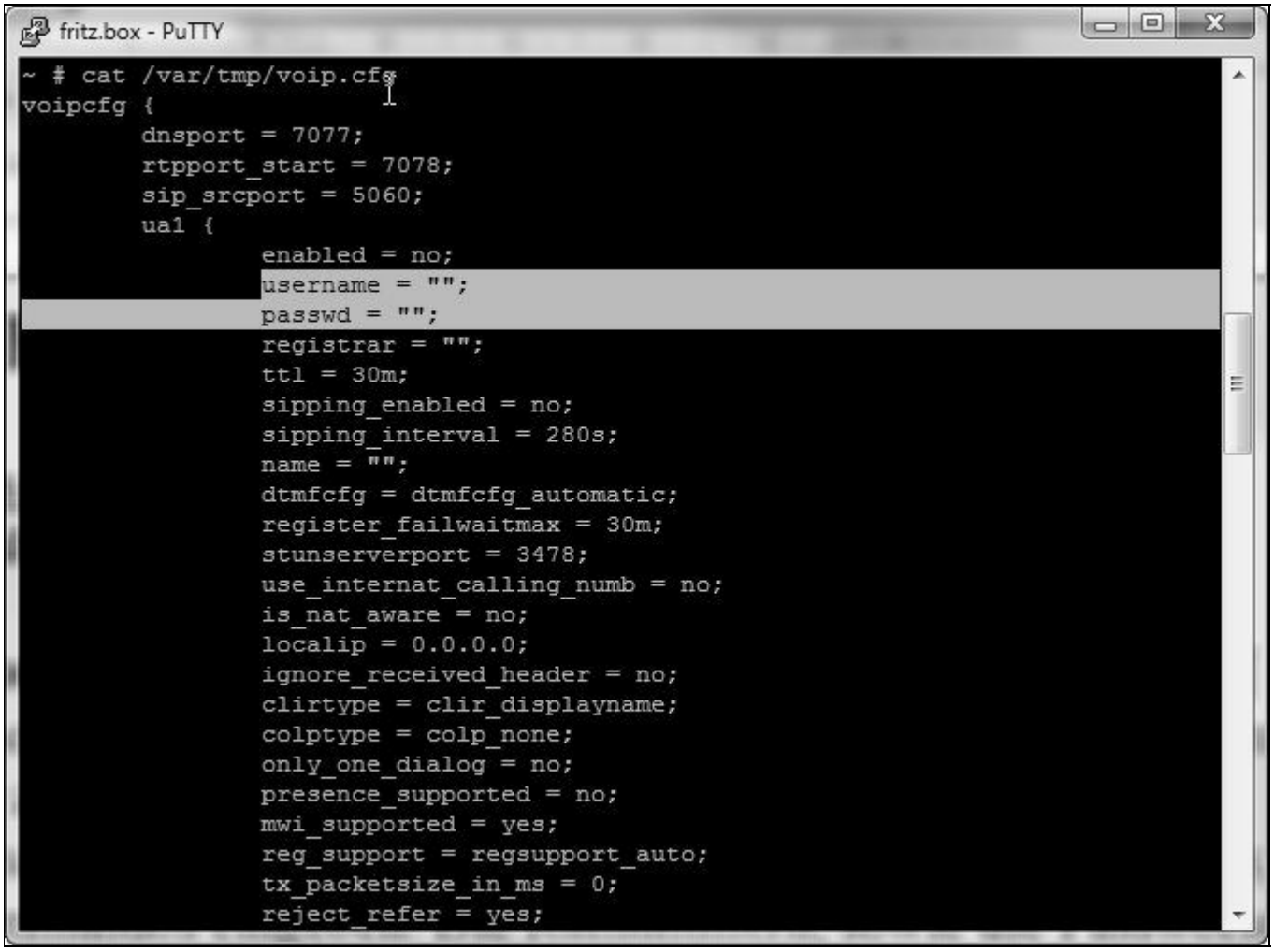


Bild 5.9 Nach Eingabe der Kommandos werden die Rufnummern sowie die Passwörter im Klartext angezeigt.

Um weitere in der FRITZ!Box gespeicherte Kennwörter auszulesen, nutzen Sie diese Kommandos:

```
allcfgconv -C ar7 -c -o /var/tmp/ar7.cfg
grep passwd /var/tmp/ar7.cfg
```

Mit dem grep-Befehl werden sämtliche Zeilen ausgeworfen, in denen beispielsweise passwd steht.

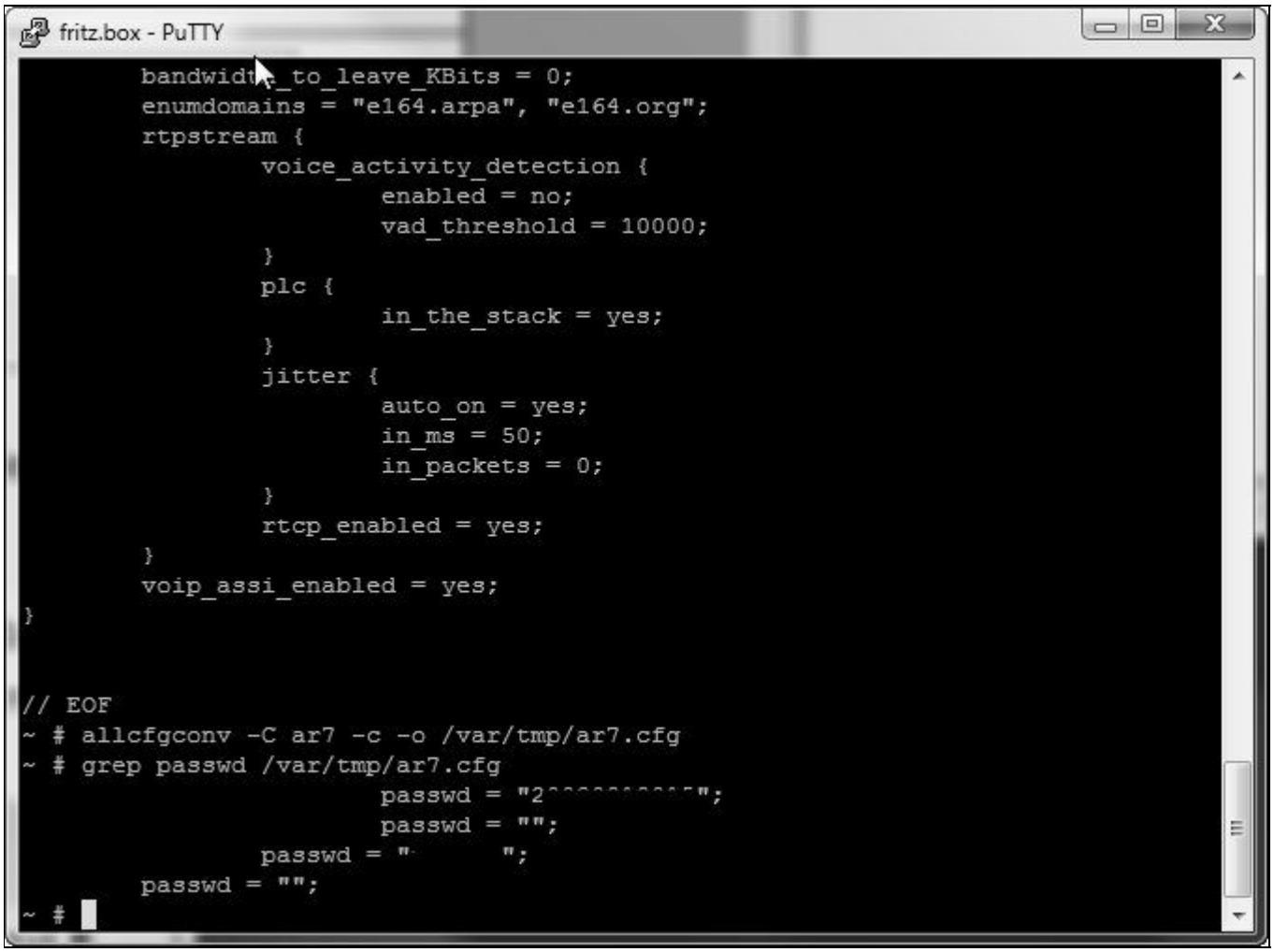


Bild 5.10 Die Konfigurationsdatei *ar7.cfg* ist die Schaltzentrale der FRITZ!Box-Konfiguration.

Diese Beispiele zeigen umso mehr, wie wichtig es ist, sicherzustellen, dass der telnetd-Dienst abgeschaltet und die FRITZ!Box mit einem sicheren Kennwort geschützt ist. Erst dann können Sie sich einigermaßen sicher sein, dass hier keine unbefugten Zugriffe erfolgen.

5.2 Schnellzugang zur FRITZ!Box

Wer seine FRITZ!Box häufig (um)konfiguriert und verschiedene Einstellungen sowie Parameter testet, für den ist das Eintippen der IP-Adresse oder der URL oftmals nervig. Wem schon ein Klick zu viel ist, der wünscht sich einen bequemeren Schnellzugang über den Browser. Hier hat AVM (derzeit noch im Laborbereich erhältlich) ein Add-on entwickelt, das über die simple Lesezeichenfunktion des Browsers hinausgeht.

Lesezeichen

http://bit.ly/9jtGoM

Hier finden Sie das FRITZ!Box AddOn für den Internet Explorer und Mozilla Firefox.

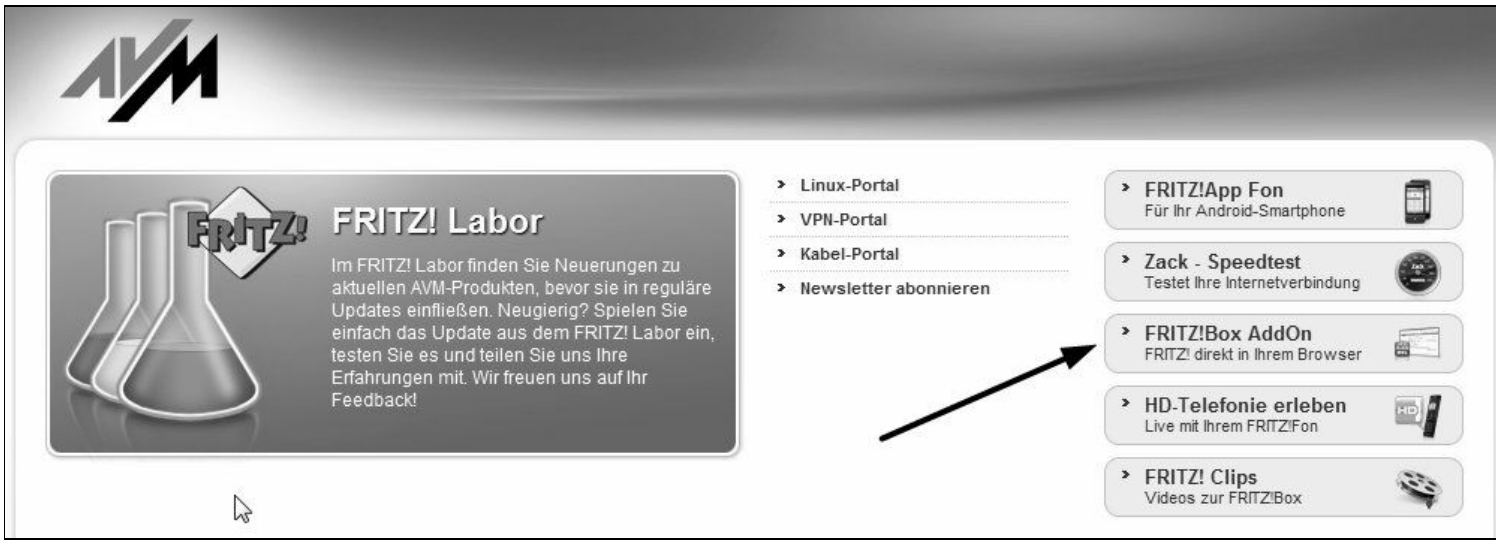


Bild 5.11 Ein Kick auf die Schaltfläche *FRITZ!Box AddOn* startet den Download.

Das FRITZ!Box AddOn lässt sich im Firefox-Browser direkt nach dem Klick auf das Programmsymbol installieren, während der Internet Explorer zunächst den Download der Add-on-Datei sowie die manuelle Installation verlangt.

Bild 5.12 Nach dem Neustart von Firefox ist die Installation des Add-ons abgeschlossen.

Nach Installation bzw. Neustart des Browsers steht in der oberen Browserleiste ein FRITZ!Box-Button zur Verfügung, über den bekannte, aber auch neue Funktionen wie der direkte Zugriff auf den FRITZ!Box-Speicher (FRITZ!Box-intern als auch USB-Speicher) oder den Firmware-Onlinecheck gestartet werden können.

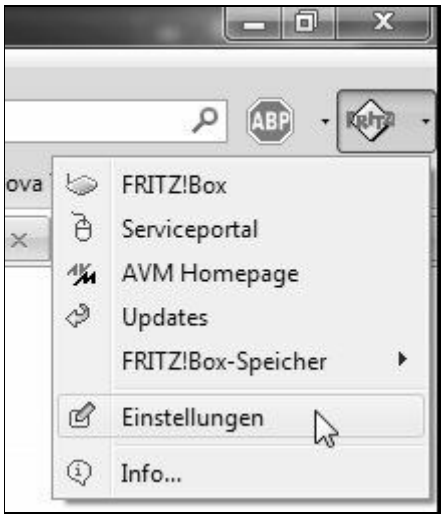


Bild 5.13 Rechts oben neben der Adresszeile des Browsers nistet sich das Add-on ein …

Bild 5.14 Selbstverständlich: Neben dem Firmwarecheck ermöglicht die Browsererweiterung den direkten Zugang zur FRITZ!Box.

Dieses Add-on prüft selbstständig, ob für die verwendete FRITZ!Box im Heimnetz eine Aktualisierung bei AVM bereitsteht – Telefoniefreunde werden sich über die integrierte Wählfunktion per Mausklick, mit der sich Telefonrufnummern aus Webseiten wählen lassen, freuen.

5.3 Fehlersuche im Netzwerk

Oft hat man das Gefühl, dass das Netzwerk langsamer ist als sonst, der Download lässt auf sich warten, oder der Browser hat ein Problem mit der Namensauflösung. Manchmal treibt einen aber auch nur die pure Neugierde, herauszufinden, mit welchen Gegenstellen ein gestartetes Programm kommuniziert und welche Daten dabei übertragen werden. Hier nutzen Sie grundsätzlich einen sogenannten Sniffer – allgemein ist das eine Software, die sämtlichen Datenverkehr aufzeichnet und die Pakete bzw. die darin befindlichen Daten lesbar aufbereitet. AVM hat der FRITZ!Box einen eingebauten Sniffer spendiert, den Sie für eigene Zwecke wie Fehlersuche und Diagnose nutzen können.

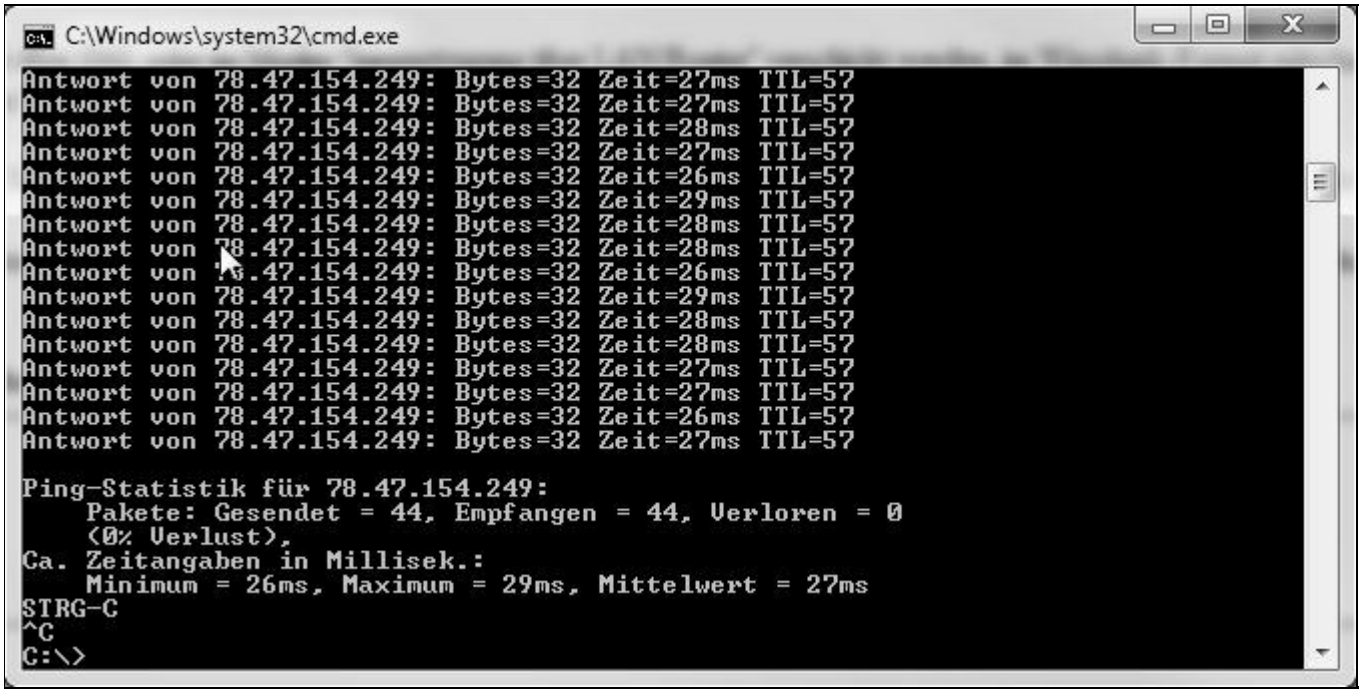


Bild 5.15 *http://fritz.box/html/capture.html*: Nach dem FRITZ!Box-Log-in erscheint eine spartanische Passworteingabe; per Mausklick können Sie an jeder FRITZ!Box-Netzwerkschnittstelle lauschen.

Die FRITZ!Box kann zu Diagnosezwecken sämtliche Daten, die über DSL oder im Modus *Internetzugang über LAN/Router* verschickt werden, mitprotokollieren. Das geschieht im Wireshark-Format, in dem Sie anschließend die mitgeschnittenen Daten öffnen und analysieren können. Aus Datenschutzgründen der Hinweis: Sie dürfen nur Ihren eigenen PC bzw. das eigene Heimnetz abhören, denn in so einem Mitschnitt sind neben den Daten eventuell auch Zugangsdaten und Kennwörter enthalten.

Lesezeichen

http://www.wireshark.org/
Hier finden Sie die aktuellste Version der Freeware Wireshark.

Grundsätzlich starten Sie das Logging auf der Seite *http://fritz.box/html/capture.html* über die entsprechende *Start*-Schaltfläche und speichern die Datei auf der Festplatte ab.

Hier wird der Mitschnitt fortlaufend in die Download-Datei geschrieben. Zum Beenden des Mitlesens drücken Sie immer die *Stop*-Schaltfläche – Sie dürfen den laufenden Download nicht abbrechen.

Möchten Sie diesen Paketmitschnitt nun lesen bzw. analysieren, brauchen Sie Wireshark. Um das Ganze jetzt in der Praxis zu betrachten, setzen Sie mit Ihrem Computer einen Ping auf einen beliebigen Host ab und analysieren den Datenverkehr. In diesem Beispiel wird www.franzis.de als Zielhost verwendet.

Prüfen, ob eine Hostadresse im Netzwerk erreichbar ist

Seitdem es TCP/IP gibt, gibt es auch das Ping-Programm. Damit lässt sich überprüfen, ob eine Hostadresse in einem Netzwerk überhaupt erreichbar ist. Dafür erzeugt der *ping*-Befehl spezielle Pakete, die an die angegebene Adresse (IP-Adresse oder DNS-Adresse) geschickt und von dieser automatisch beantwortet werden.

Je nachdem, wie lang die Reaktionszeit und der Weg der Anfrage sind, stellt das Ping-Programm die Geschwindigkeit der Datenpakete entsprechend dar. Hier gilt: je kleiner die Ping-Werte, desto schneller die Verbindung. Heute gilt der *ping*-Befehl jedoch als nicht mehr verlässlich genug, da die meisten DSL-WLAN-Router, aber auch moderne Betriebssysteme wie Windows 7 und Mac OS X Ping-Anfragen aus Sicherheitsgründen ignorieren.

In einem heterogen Netzwerk mit Mac OS X und Windows-PCs ist eine Analyse der Verbindungen nicht immer gleich auf Anhieb möglich. Grundsätzlich gilt: Ist eine Netzwerkverbindung richtig eingestellt, sollten Sie den Rechner erfolgreich »anpingen« können – egal ob von Mac OS X in Richtung Windows oder umgekehrt.

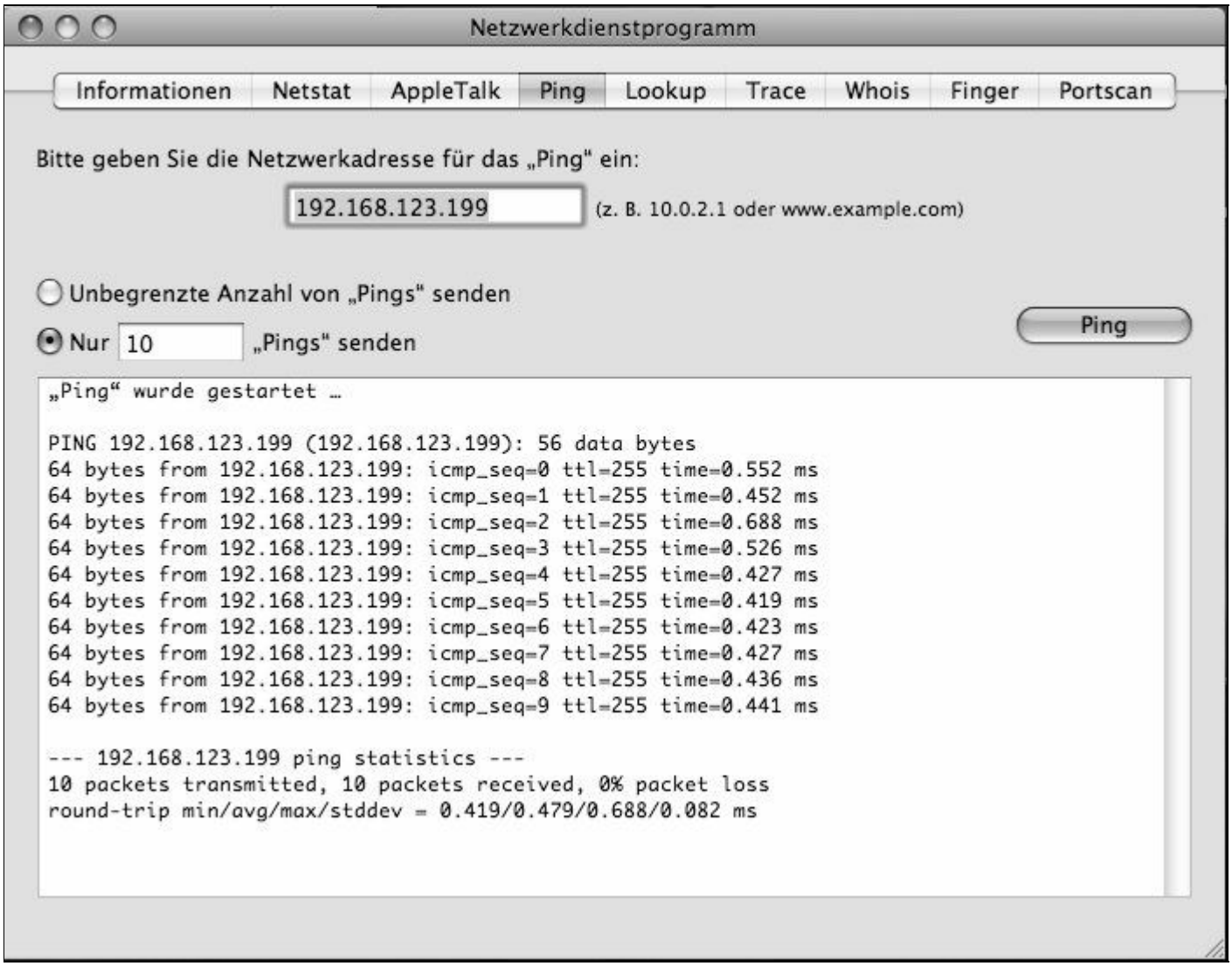


Bild 5.16 Entweder der DNS-Name oder eine IP-Adresse kann für den *ping*-Befehl genutzt werden.

Unter Windows muss gegebenenfalls noch ein kleiner Eingriff geschehen, damit sich der *ping*-Befehl einsetzen lässt: Das erledigen Sie in der DOS-Eingabeaufforderung bzw. im *Ausführen*-Dialog mit dem Befehl *ping [IP-ADRESSE]*. In diesem Beispiel geben Sie den Befehl *ping 192.168.0.1* ein. Ist beispielsweise bei Windows Vista der *Ausführen*-Befehl im Startmenü ausgeblendet, können Sie ihn per Mausklick aktivieren.

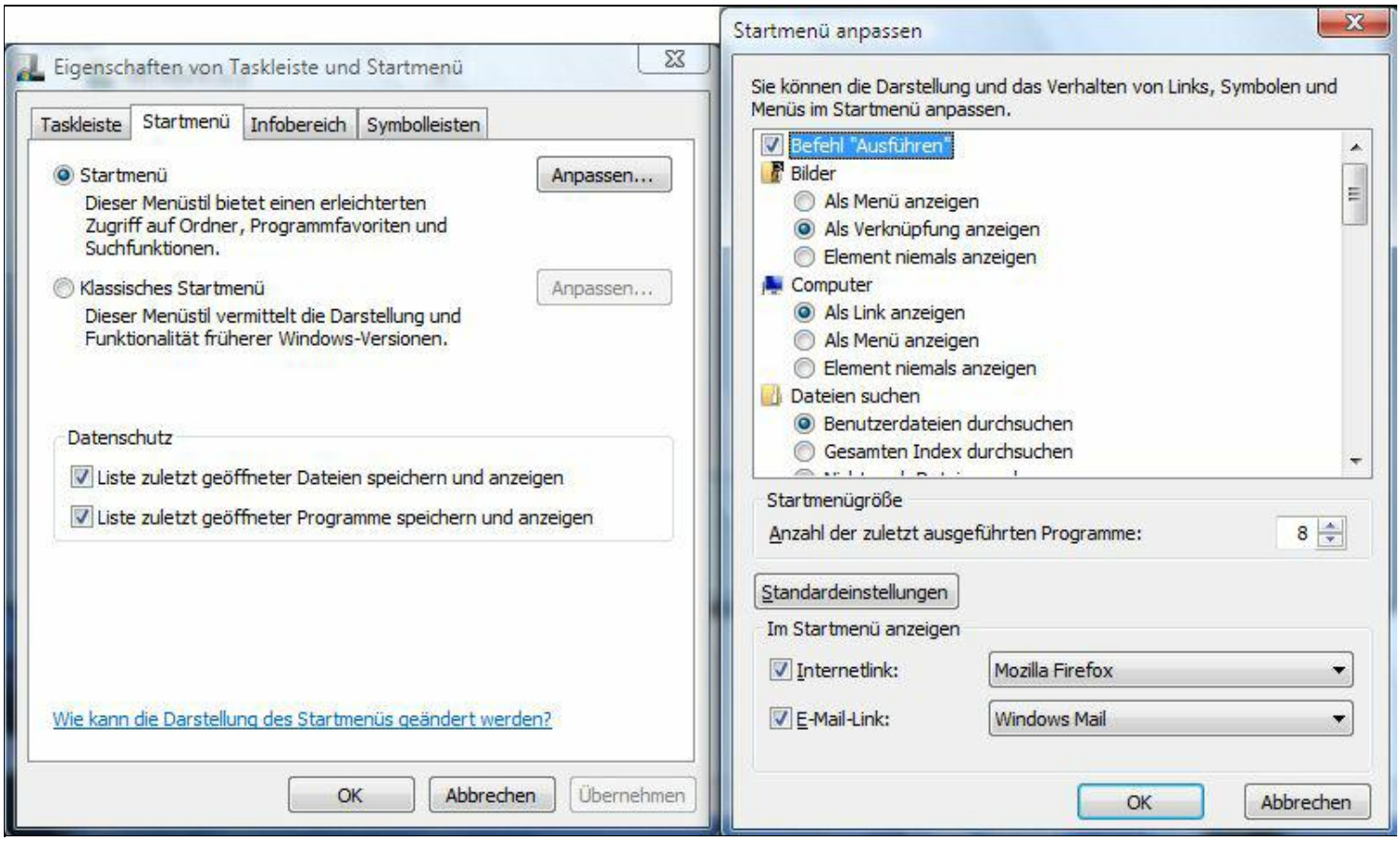


Bild 5.17 Über *Eigenschaften von Taskleiste und Startmenü* und Klick auf die Schaltfläche *Anpassen* aktivieren Sie den *Ausführen*-Befehl bei Windows Vista.

Klappt das Anpingen trotz richtiger IP-Konfiguration nicht, liegt das in der Regel an der Windows-Firewall. Diese ignoriert in der Standardeinstellung sämtliche eingehenden Ping-Anfragen. Um der Firewall die Annahme des *ping*-Befehls im Heimnetz zu erlauben, öffnen Sie über das Startmenü die Windows-Firewall *Windows-Firewall mit erweiterter Sicherheit*.

Dort wählen Sie *Eingehende Regeln* und aktivieren die Regel *Datei- und Druckerfreigabe (Echoanforderung – ICMPv4 eingehend)*. Ist diese Regel mehrmals zu sehen, schalten Sie Ping für das gewünschte Netzwerkprofil (im Heimnetz *Domäne, Privat*) frei. Ist das Anpingen nun möglich, können Sie erstmalig mit Wireshark arbeiten.

So prüfen Sie die Netzwerkverbindungen mit Wireshark

1. Nach Installation sowie Start von Wireshark öffnen Sie über das Datei-öffnen-Menü *File/Open* den von der FRITZ!Box erzeugten Mitschnitt der DSL-Dose, die im Download-Verzeichnis mit der Bezeichnung *fritzbox-vcc0_DD.MM.YY_HHSS.eth* zu finden ist. Der Platzhalter DD.MM.YY_HHSS steht für Datum und Uhrzeit des Capture-Vorgangs. Haben Sie noch keine Netzwerkdaten zum Analysieren, führen Sie erst mal folgende Schritte durch:
   - Logging-Seite der FRITZ!Box aufrufen (*http://fritz.box/html/capture.html*).
   - FRITZ!Box-Kennwort eingeben, um die Seite zu öffnen.
   - Auf dem Computer Konsole/Ausführen/DOS-Fenster öffnen wählen und dort *ping www.franzis.de* (Mac) bzw. *ping -t www.franzis.de* (Windows) eingeben.
   - Die erste *Start*-Schaltfläche auf der Logging-Seite der FRITZ!Box anklicken (Mitschnitt auf DSL-Ebene). Hier wird der Mitschnitt fortlaufend in eine Download-Datei geschrieben.
   - Mit *OK* den Download der Datei bestätigen.
   - *ping*-Abfrage auf dem Computer stoppen, [Strg]+[C] drücken.
   - Nach ein paar Minuten das Mitschneiden per Klick auf die *Stop*-Schaltfläche beenden.

2. Anschließend öffnen Sie mit Wireshark über das Menü *File/Open* den von der FRITZ!Box erzeugten Mitschnitt. Da hier kein Filter aktiv ist, wurde sämtlicher Netzwerkverkehr, der über die DSL-Schnittstelle in das Internet ging, mitgeschnitten. Das Programmfenster ist im Wesentlichen in drei Bereiche aufgeteilt. Im oberen Bereich finden Sie die

Paketliste (*packet list-pane*), in der Mitte die Paketdetails (*packet details-pane*) sowie unten die hexadezimale Paketanzeige (*packet bytes-pane*). Die in der Paketliste angezeigten Spalten lassen sich über das Menü Edit/Preferences anpassen – das ist aber zunächst nicht notwendig.

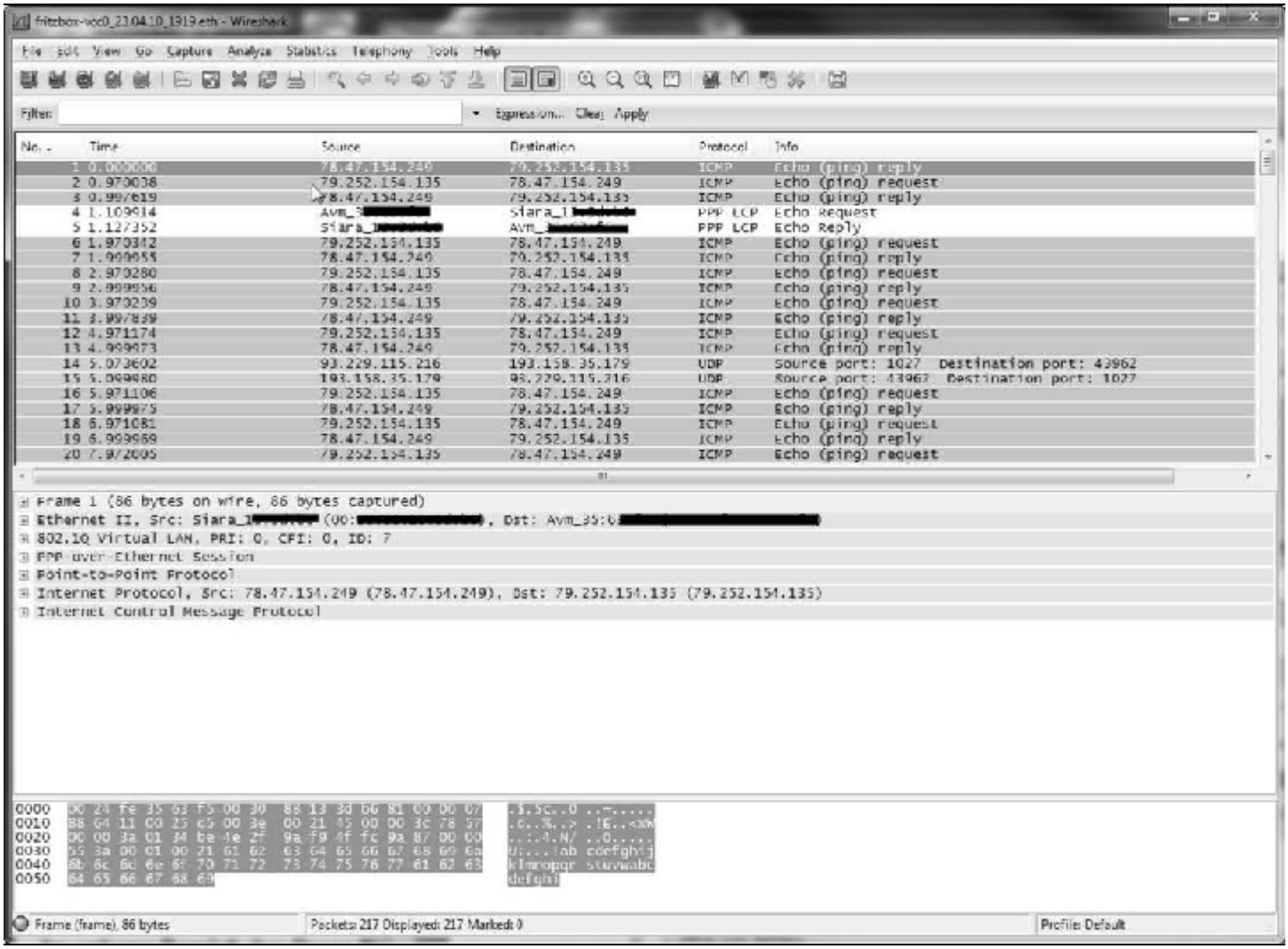


Bild 5.18 So oder so ähnlich sieht die geöffnete Mitschnittdatei der FRITZ!Box im Wireshark-Fenster aus.

3. Auf den ersten Blick wirkt Wireshark also sehr unübersichtlich, vor allem die vielen unterschiedlichen IP-Adressen und verschiedenen Protokolle ragen zunächst heraus – bei einem längeren Mitschnitt ist die Suche nach Brauchbarem ziemlich anstrengend und kontraproduktiv. Aus diesem Grund setzen Sie jetzt einen Filter, um die Ansicht auf die eigentlichen Nutzdaten einzugrenzen.
   Um beispielsweise den Datentransfer von und zu der (externen) IP-Adresse der FRITZ!Box zu sehen, setzen Sie einen Filter auf die IP-Adresse. Da die IP-Adresse bei DSL-Anschlüssen in der Regel täglich wechselt, holen Sie die aktuelle IP-Adresse einfach aus der FRITZ!Box-Startseite. Öffnen Sie den Browser und anschließend die FRITZ!Box-Konfigurationsseite mithilfe des FRITZ!Box-Zugangkennworts und notieren Sie sich die IP-Adresse.

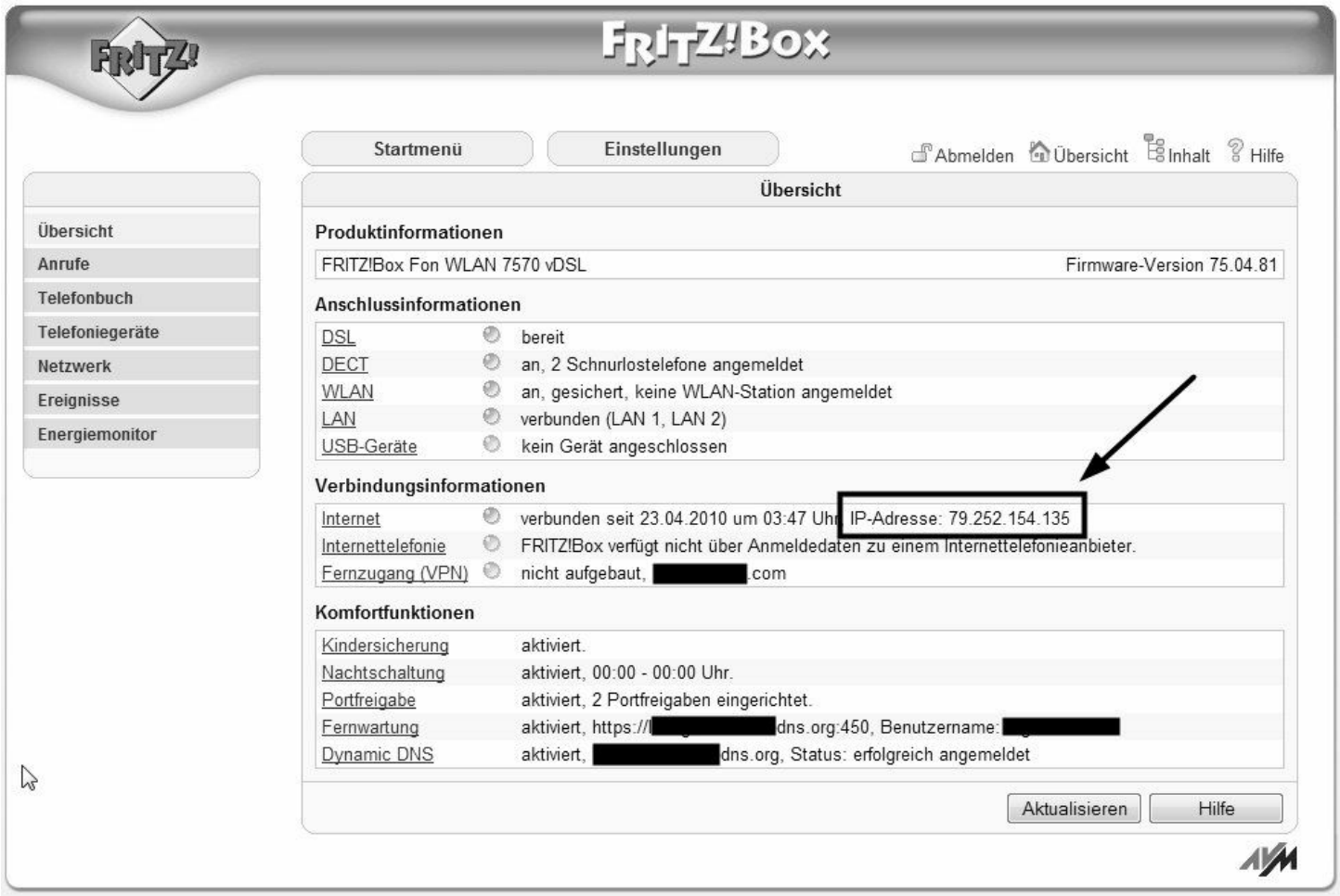


Bild 5.19 Übersichtlich: Auf der FRITZ!Box-Startseite ist nach dem Log-in im Bereich *Verbindungsinformationen/Internet* auch die externe IP-Adresse zu finden.

4. Anschließend nutzen Sie diese IP-Adresse zum Filtern der Ausgabe. In diesem Beispiel ist die externe IP-Adresse der FRITZ!Box die Adresse *79.252.154.135*. Tragen Sie diese unter der Menüleiste in das Eingabefeld *Filter* mit einem führenden ip.addr == ein, also:

```
ip.addr == 79.252.154.135
```

und klicken Sie auf die nebenstehende Übernehmen-Schaltfläche *Apply*. Nachstehende Vergleichsoperatoren sind bei Wireshark erlaubt – hier dürfen Sie sowohl die englische als auch die C-ähnliche Abkürzung nutzen. So können Sie alternativ den Filter

```
ip.addr eq 79.252.154.135
```

nutzen.

Englische Abkürzung	Bedeutung	C-ähnlich	Beispiel
eq	Equal	==	*ip.src eq 79.252.154.135*
ne	Not equal	!=	*ip.src != 79.252.154.135*
gt	Greater than	>	*frame.len > 16*
lt	Less than	<	*frame.len lt 0x100*
ge	Greater than or equal to	>=	*frame.len ge 255*
le	**Less than or equal to**	<=	*frame.len le 0x10*

1. Nun zeigt Wireshark nur noch diejenigen Frames an, die die eingetragene Filterbedingung erfüllen, also jene, in denen die gewünschte IP-Adresse vorkommt. Um diesen Filter wieder zu entfernen, klicken Sie auf die Schaltfläche *Clear*.

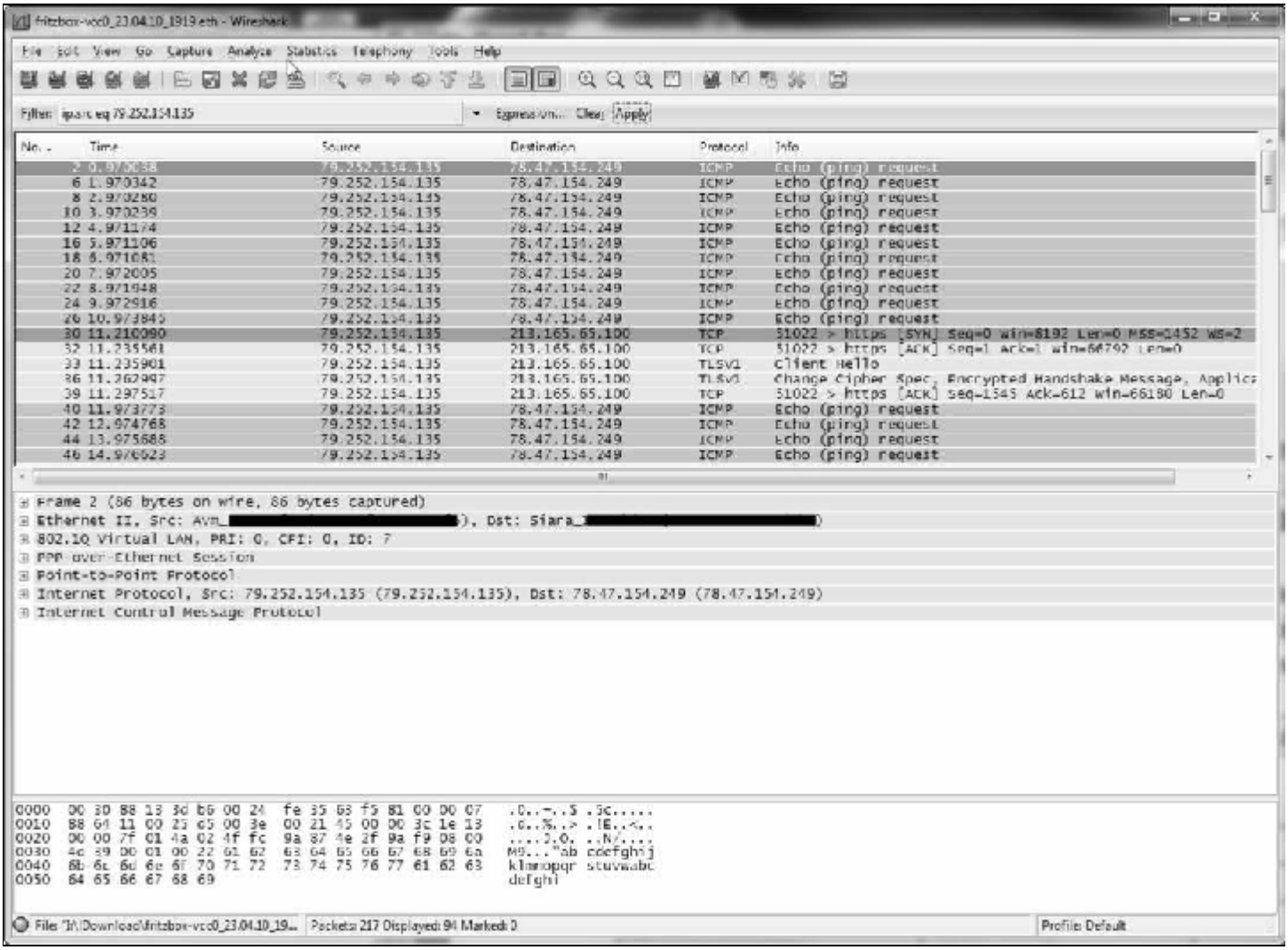


Bild 5.20 Eingedampft: Nun ist die Datenausgabe auf die externe Adresse *79.252.154.135* beschränkt.

2. Möglicherweise ist die gefilterte Datenausgabe noch immer zu groß – dann hilft ein zusätzlicher Filter weiter: Mithilfe von booleschen Operatoren lassen sich Filter kombinieren und erweitern.
   In diesem Beispiel wird nun das Ergebnis des abgesetzten *ping*-Befehls gesucht und die Antwort – das Echo auf die Anfrage – analysiert; bekanntlich nutzt *ping* das ICMP-Protokoll (*Internet Control Message Protocol*), in dem IP-Pakete über ICMP gesendet werden. Wird kein Echo empfangen, stuft ICMP den Zielrechner als nicht erreichbar ein.

   Kommt eine Rückmeldung, liefert ICMP die gemessene Zeit bis zur Ankunft des Echos am Sendehost. Mit dem Filter

   ```
   ip.addr eq 79.252.154.135 && icmp
   ```

   schränken Sie die Ansicht auf das ICMP-Protokoll ein. Neben dem UND-Operator stehen noch weitere Operatoren zur Verfügung. Die wichtigsten sind:

Englische Abkürzung	Bedeutung	C-ähnlich	Beispiel
and	Logical AND	&&	*ip.addr eq 79.252.154.135 && icmp*
or	Logical OR	||	*ip.scr==79.252.154.135 or ip.src==192.178.1.1*
xor	**Logical XOR**	^^	*tr.dst[0:3] == 0.8.19 xor tr.src[0:3] == 0.8.19*
not	**Logical NOT**	!	*not tcp*

Mit dem &&-Operator wird nun die Ansicht auf das ICMP begrenzt:

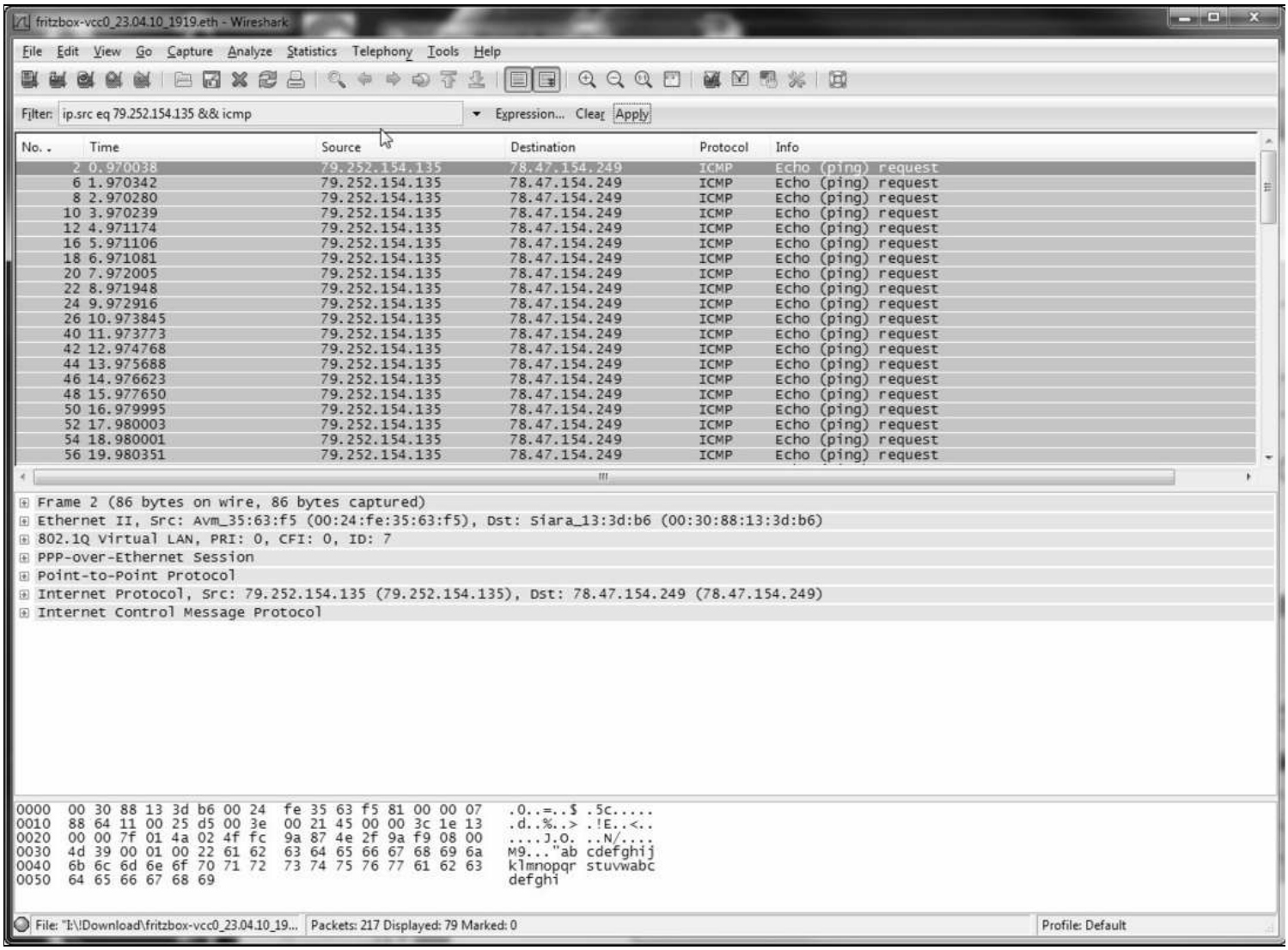


Bild 5.21 Jetzt sind nur noch ICMP-Pakete mit der externen FRITZ!Box-IP-Adresse sichtbar.

1. Im nächsten Schritt schauen Sie sich ein Paket im Detail an. Dafür markieren Sie im oberen Bereich in der Paketliste irgendeinen Frame – links in der Spalte *No.* wird die Nummer des Frames angezeigt. Da ein oder mehrere Filter aktiv sind, sind die Nummern natürlich nicht fortlaufend sichtbar. Die Spalte *Source* zeigt den Absender, die Spalte *Destination* den Empfänger des Frames. Welches Protokoll hierfür genutzt wird, steht in der Spalte *Protocol*, während die Spalte *Info* zusätzliche Bemerkungen zum aktuellen Frame liefert.
2. In diesem Beispiel ist zu sehen, dass sämtliche *ICMP Echo (ping) request* von der FRITZ!Box-eigenen IP-Adresse zu der IP-Adresse von *www.franzis.de* führen. Wählen Sie jetzt einen beliebigen Frame aus, und die sogenannten Schichten (engl. Layer) werden im mittleren Teil des Programmfensters aufgelistet. Per Anklicken des Plussymbols klappen Sie die Ansicht des entsprechenden Layers auf:

```
Frame 2 (86 bytes on wire, 86 bytes captured)
Arrival Time: Apr 23, 2010 19:19:14.017319000
Time delta from previous captured frame: 0.970038000 seconds
Time delta from previous displayed frame: 0.970038000 seconds
Time since reference or first frame: 0.970038000 seconds
Frame Number: 2
Packet Length: 86 bytes
Capture Length: 86 bytes
Frame is marked: False
Protocols in frame: eth:vlan:pppoes:ppp:ip:icmp:data
Coloring Rule Name: ICMP
Coloring Rule String: icmp || icmpv6
```

3. Hier sind Informationen wie Größe des Frames (*Packet Length*), aufgezeichnete Größe (*Capture Length*) sowie Zeit und Zeitdifferenz zum vorgehenden Frame (*Time delta*) herauszulesen. In der nächsten Zeile finden Sie Informationen zum OSI-Layer 2 (Ethernet II). Dort sind die MAC-Adressen von Absender und Empfänger des Pakets zu finden.

Interessanter ist das IP (*Internet Protocol*). Im OSI-Layer 3 finden Sie Informationen zu IP-Flags, die TTL (*Time to live*), das Protokoll sowie die genutzten Absender- und Empfänger-IP-Adressen.

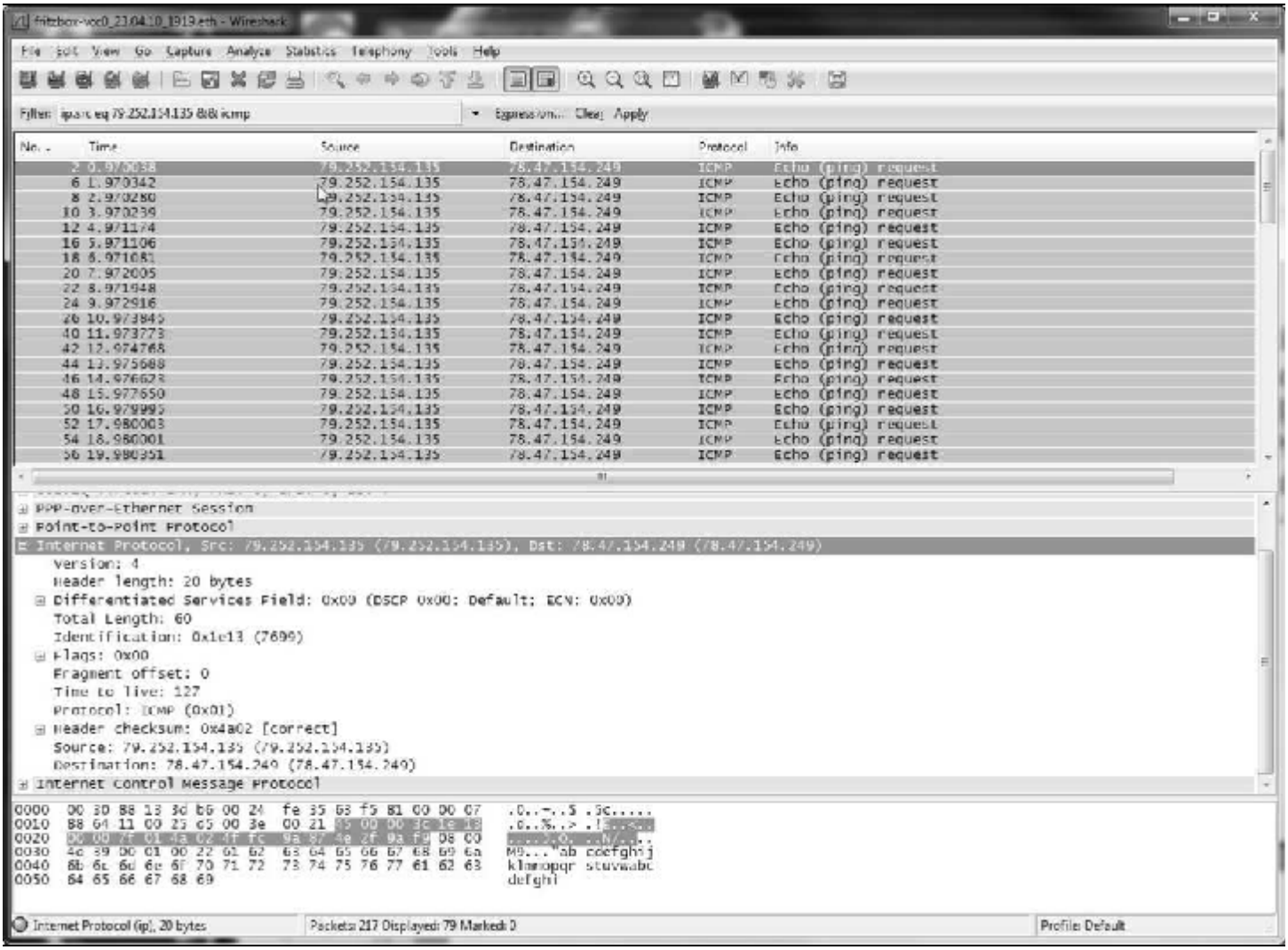


Bild 5.22 IP-Paket im Detail: Schritt für Schritt kommen weitere Informationen zum Vorschein.

4. Zu guter Letzt finden Sie in der letzten Zeile die decodierte Ausgabe des ICMP-Protokolls, das eine Codierung bestehend aus *Type* und *Code* verwendet. Hier sollte nun

```
Type: 8 (Echo (ping) request)
Code: 0 ()
Checksum: 0x4d39 [correct]
Identifier: 0x0001
Sequence number: 34 (0x0022)
Data (32 bytes)
```

auftauchen. Im unteren Ergebnisfenster ist der Hexdump des ausgewählten Frames zu sehen. Im Beispiel nutzt der *ping*-Befehl das Alphabet (ab cdefghij klmnopqr stuvwabc defghi) als Payload (Nutzlast).

```
0000  00 30 88 13 3d b6 00 24  fe 35 63 f5 81 00 00 07 .0..=..$ .5c.....
0010  88 64 11 00 25 d5 00 3e  00 21 45 00 00 3c 1e 13 .d..%..> .!E..<..
0020  00 00 7f 01 4a 02 4f fc  9a 87 4e 2f 9a f9 08 00 ....J.O. ..N/....
0030  4d 39 00 01 00 22 61 62  63 64 65 66 67 68 69 6a M9..."ab cdefghij
0040  6b 6c 6d 6e 6f 70 71 72  73 74 75 76 77 61 62 63 klmnopqr stuvwabc
0050  64 65 66 67 68 69                                defghi
```

Es ist also alles in bester Ordnung, der *ping*-Befehl wurde sauber abgearbeitet. Finden Sie hingegen eine oder mehrere ICMP-Anfragen, die nicht beantwortet wurden – weil *Echo_Request* fehlt –, war der Zielhost nicht erreichbar.

Das einfache Beispiel zeigt, wie Sie mit der FRITZ!Box relativ komplexe Sachverhalte aufklären können. Angehenden Netzwerkanalysespezialisten wird damit schnell klar, warum manche Protokolle wie beispielsweise Telnet via Internet tabu sein sollten – werden hier doch Benutzerinformationen wie Kennung und Passwort im Klartext übertragen. Mit etwas

Wireshark-Erfahrung und den passenden Filtern ist das entsprechende Paket schnell gefunden.

6 USB-Festplatte andocken

Die meisten Anwender sind Backup-Muffel. Tritt aber dann aus heiterem Himmel der Daten-GAU ein, ist der Ärger groß. Der Datenverlust muss nicht einmal auf Fehlbedienung, versehentliches Löschen von Daten oder auf einen Hacker- bzw. Virenangriff zurückzuführen sein, sondern auch Hardwaredefekte, ein Festplattencrash oder gar ein Diebstahl des Rechners oder Notebooks sorgen für Datenverlust. Crasht ein Rechner, hilft in der Regel nur der Start von einem zweiten, nachträglich installierten Windows, um die Daten auf einen alternativen Datenträger umzukopieren. Ist Windows dann neu installiert, müssen die Daten, die Systemeinstellungen, die Mailordner und Lesezeichen sowie Browseroptionen wieder zurückkopiert werden. Wer einmal diese ganze Prozedur mitgemacht und endlos Zeit verschleudert hat, der weiß, wie wertvoll ein zuverlässiges Backup sein kann.

6.1 Anschluss an der FRITZ!Box

Die meisten FRITZ!Boxen von AVM und ihre OEM-Geschwister besitzen an der Geräterückseite eine USB-Buchse für den Anschluss eines Druckers, USB-Sticks oder einer USB-Festplatte, die nach erfolgter Konfiguration über die FRITZ!Box-Weboberfläche sämtlichen Computern im Heimnetzwerk zur Verfügung gestellt werden kann. Was liegt also näher, als diesen Anschluss zu nutzen? Sie benötigen einfach eine Festplatte in einem externen Gehäuse, die über den USB-Anschluss an die FRITZ!Box angeschlossen werden kann. Dieser Vorgang dauert eine Weile. Mit einem Neustart des Systems wird die Aktualisierung abgeschlossen.

Bild 6.1 Western Digital My Passport Essential – externe USB-Festplatte für den Anschluss an die FRITZ!Box. (Foto: Western Digital)

Warum zieht die USB-Festplatte keinen Strom?

Die USB-Spezifikation hat die Grenze für die Stromaufnahme auf 500 mA festgelegt. Für Geräte, die diese Grenze überschreiten, muss die Stromversorgung extern hergestellt werden. Um den fehlerfreien Betrieb der USB-Festplatte an der FRITZ!Box zu gewährleisten, eignet sich am besten ein aktiver USB-Hub mit eigener Stromversorgung, der an den Router angeschlossen wird. Die USB-Festplatte wird dann an den USB-Hub angeschlossen.

USB-Festplatte an der FRITZ!Box anmelden

Grundsätzlich ist die Einrichtung einer USB-Festplatte schnell erledigt: einfach das USB-Kabel der Festplatte in die Gehäuserückseite der FRITZ!Box einstecken und einen kleinen Moment warten.

1. Sind Sie auf der Konfigurationsseite der FRITZ!Box eingeloggt, prüfen Sie über *Erweiterte Einstellungen/USB-Geräte* bei *Geräteübersicht*, ob dort ein Massenspeichergerät gefunden wurde.
2. Wird die USB-Festplatte nicht augenblicklich erkannt, können Sie über das Menü bei *Folgende Massenspeicher sind an der FRITZ!Box angeschlossen* auf den darunterliegenden Eintrag mit der USB-Festplatte klicken und diese über die *Aktualisieren*-Schaltfläche neu initialisieren. Falls die USB-Festplatte eine eigene Stromversorgung mitbringt, achten Sie darauf, dass das Gerät angeschaltet und damit die Festplatte betriebsbereit ist.

Bild 6.2 Zunächst wird die USB-Festplatte mit der Bezeichnung *ExternalHDD-Partition-0-1* erkannt – abhängig von der installierten Firmware und dem FRITZ!Box-Modell kann diese Bezeichnung jedoch abweichen.

3. Ist die Festplatte eingerichtet, soll nach dem Willen von AVM das Programm *FRITZ!Box USB-Fernanschluss* installiert werden, um anschließend Daten austauschen zu können. Der Haken: Dieses steht nur für Windows-Anwender zur Verfügung, eine native 64-Bit-Unterstützung dafür und auch andere Betriebssysteme wie Linux oder Mac OS X bleiben jedoch außen vor.

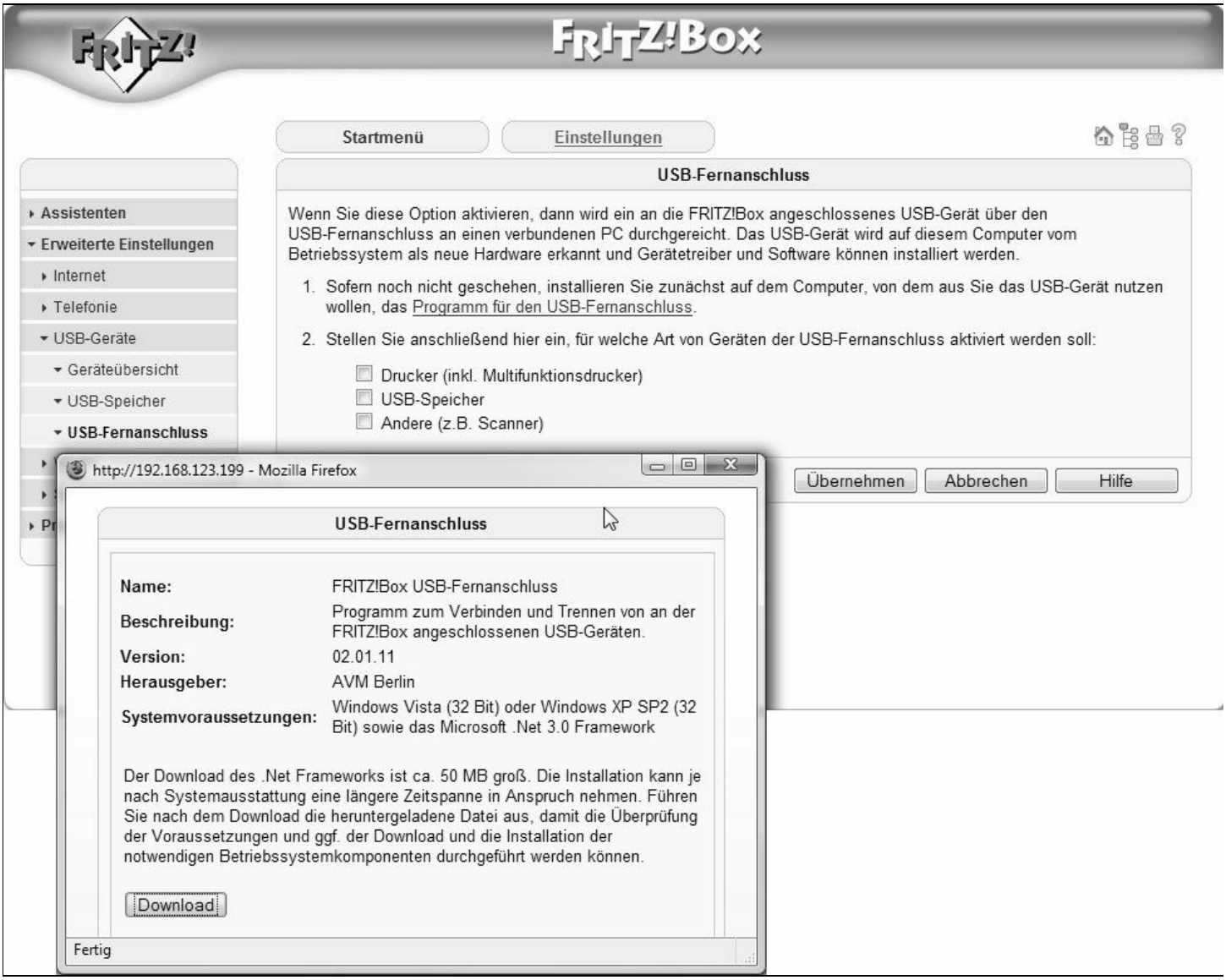


Bild 6.3 Neben dem eigentlichen Programm *FRITZ!Box USB-Fernanschluss* ist zusätzlich noch die Installation des .NET Framework mit ca. 50 MByte notwendig.

4. Wer die »reine« AVM-Lösung wählt, kann, wie in nachstehender Abbildung zu sehen, die Zugriffsberechtigung auf die Festplatte für den Netzwerkzugriff entweder auf *nur Lesezugriff* oder auf *Lese- und Schreibzugriff* einstellen. Für ein Plus an Sicherheit sorgt der Kennwortschutz, dafür ist das Häkchen bei *Kennwortschutz aktivieren* zu setzen und das gewünschte Kennwort samt Bestätigung in den weiteren Feldern einzutragen. Wer die Daten für Benutzer aus dem Internet freigeben möchte, findet auch dafür in diesem Dialog die entsprechenden Konfigurationsmöglichkeiten.

Bild 6.4 Für den Zugriff aus dem Internet ist eine eingerichtete dynamische Adresse bei *dyndns.org* oder bei alternativen Anbietern notwendig, was im Register *Dynamic DNS* erledigt wird.

Doch das Gelbe vom Ei ist das alles nicht, und eine wirkliche Verbesserung und Erweiterung der FRITZ!Box schafft erst eine selbst gebaute Firmware, mit der Sie weitere Funktionen nach Wunsch nachrüsten und den Standardfunktionsumfang aufbohren können. Damit stellen Sie nicht nur neue Funktionen auch für andere Betriebssysteme wie Linux und Mac OS X zur Verfügung, sondern können nun auch die an der FRITZ!Box angeschlossene Festplatte als Netzwerkfreigabe für das gesamte Heimnetz ohne Installation etwaiger Hilfsmittel für den Zugriff verwenden.

6.2 Daten mit der Festplatte synchronisieren

Eine unkomplizierte Datensynchronisation ermöglichen viele Tools. Suchen Sie per Google einfach nach *Freeware Tools Synchronisation Download*. Etliche Programme sind bereits mit dem Funktionsumfang der Freewareversion für die meisten Zwecke geeignet. In der Bedienung sind sie einfach – manche bieten zusätzliche Funktionen wie zeitliche Synchronisation und Datenüberprüfung.

Für das folgende Beispiel wird die Freeware Allway Sync verwendet. Sie präsentiert sich einfach und intuitiv.

Lesezeichen

http://www.allwaysync.com

Nach dem Download und der Installation des Programms starten Sie Allway Sync.

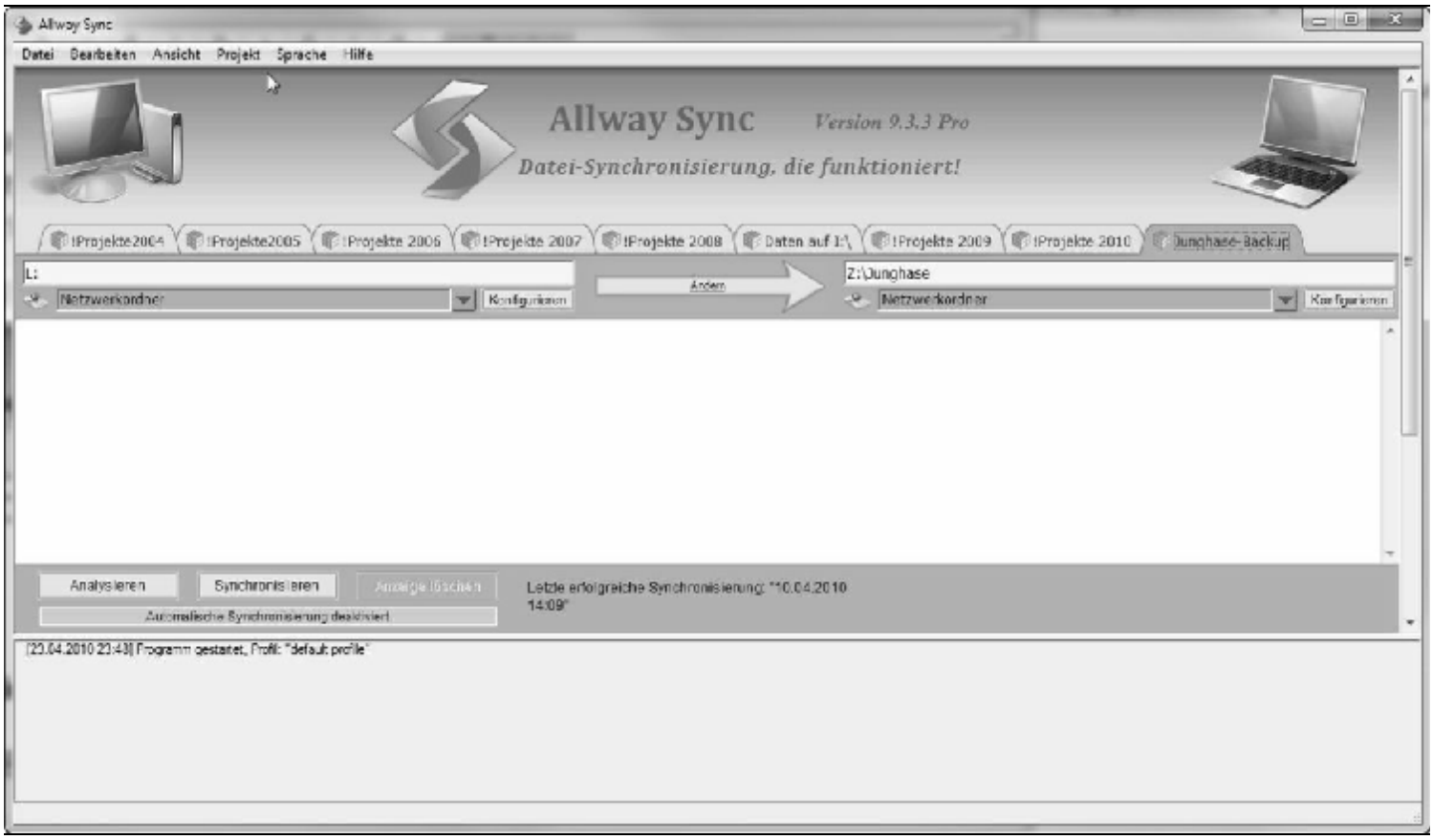


Bild 6.5 Allway Sync bietet eine übersichtlich gestaltete Benutzeroberfläche: Im linken Bereich ist der Quellordner, im rechten Bereich der Zielordner für die Synchronisation anzugeben.

Voraussetzung für den Betrieb mit der FRITZ!Box-Festplatte ist natürlich, dass im Windows Explorer ein Laufwerkbuchstabe für eine Freigabe auf der FRITZ!Box-Festplatte zur Verfügung steht.

Laufwerkbuchstabe für die USB-Festplatte festlegen

1. Klicken Sie auf die *Analysieren*-Schaltfläche, wird der angegebene Ordner mit den darin enthaltenen Dateien samt Unterverzeichnissen mit dem Ziellaufwerk abgeglichen, und die Unterschiede werden dokumentiert.
2. Mit Klick auf die Schaltfläche *Synchronisieren* starten Sie den Kopiervorgang zur Synchronisation. Das Kopieren der Daten auf die Internetfestplatte erfolgt via Windows-Netzwerklaufwerk.

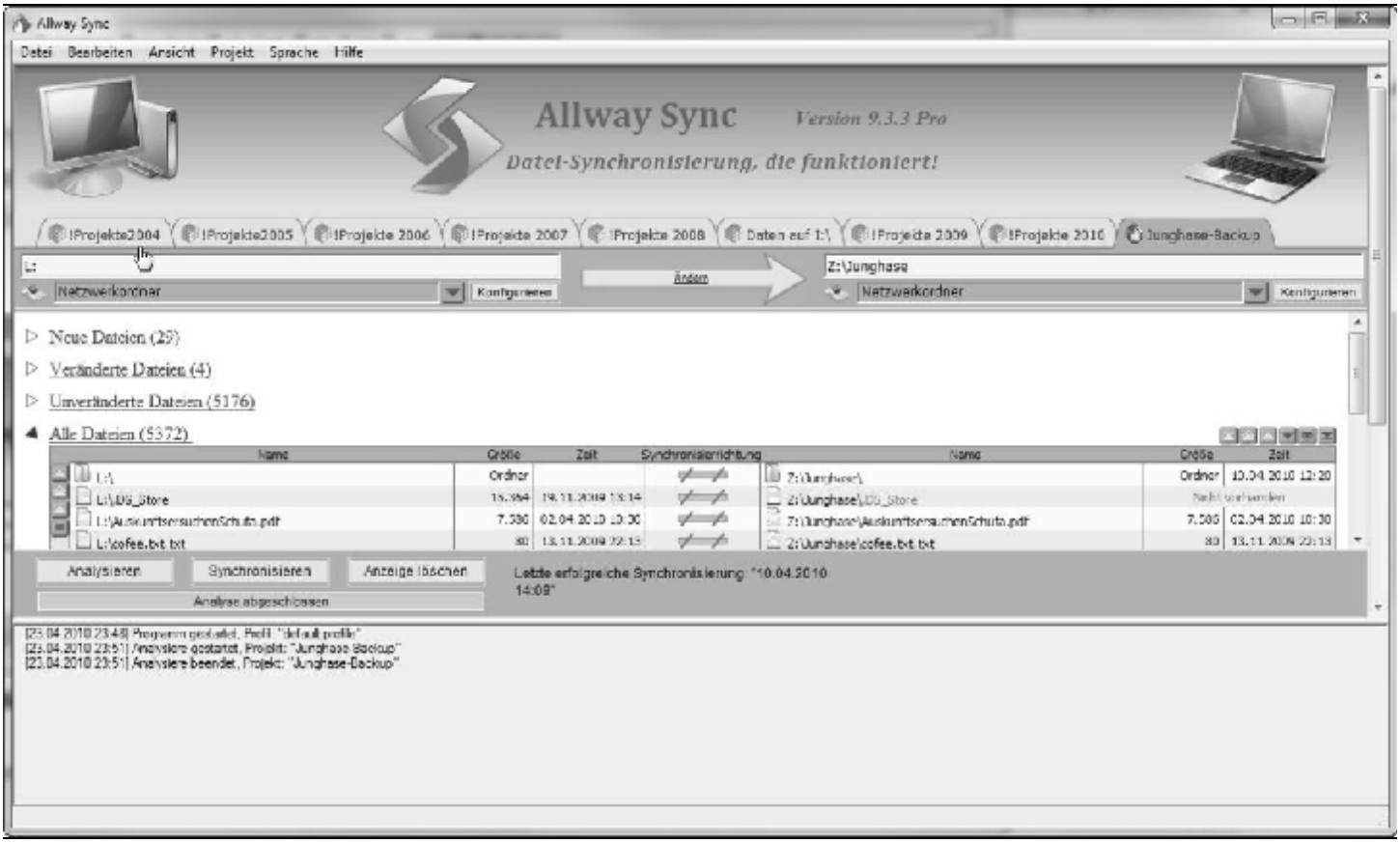


Bild 6.6 Allway Sync bemerkt Dateidatums- und Strukturkonflikte und zeigt sie bei der Analyse an.

Abhängig davon, wie viele Daten transportiert werden müssen und wie groß die zur Verfügung stehende Bandbreite (Upload-Geschwindigkeit) ist, dauert das Kopieren eine gewisse Zeit. Ist der Kopiervorgang abgeschlossen, starten Sie anschließend nochmals eine Analyse, um festzustellen, ob sämtliche Daten auch korrekt kopiert und übers Netzwerk übertragen wurden.

Freigegebene Daten auf der USB-Festplatte verschlüsseln

Der Administrator des Anbieters, der Ihnen den Speicherplatz zur Verfügung stellt, kann prinzipiell auf jeden Ordner und jede Datei auf Ihrer Internetfestplatte zugreifen. Bei persönlichen oder heiklen Daten ist es deswegen empfehlenswert, diese Daten zunächst lokal zu verschlüsseln oder zumindest mit einem Passwort vor dem lesenden Zugriff zu sichern. Hier bieten die gängigsten Packprogramme wie WinRAR, 7-Zip oder WinZip die Möglichkeit, das Öffnen eines Archivs mit einem Passwort abzusichern. Anschließend übertragen Sie wie gehabt die Archivdateien auf die Internetfestplatte.

6.3 Vom Router in die Datenwolke

Mit der rasanten Verbreitung von schnellen DSL-Anschlüssen und dem entsprechenden Platzangebot beim Anbieter ist es für wichtige Dateien durchaus sinnvoll, sie auch außerhalb der eigenen vier Wände zu sichern. Wer gerade an seiner Doktorarbeit schreibt oder sehr wichtige Daten auf seiner Festplatte hat, sollte immer vom schlimmsten Fall ausgehen: Die Daten sollten auch dann noch verfügbar sein, wenn das Arbeitszimmer abgebrannt ist oder der Computer abraucht und die externe USB-Festplatte crasht.

Kostenloser Speicherplatz oder doch besser zahlen?

Anbieter wie GMX, web.de und andere statten ihre Kunden mit einer Menge an Speicherplatz im Netz aus. Das zahlende Publikum bekommt noch mehr Platz angeboten – bei GMX TopMail beispielsweise sind es derzeit über 10 GByte Kapazität. GMX TopMail bietet einen »wachsenden« Speicher für E-Mails, Fotos und andere Dokumente. Monat für Monat kommen zu Ihrem Speicherkontingent 100 MByte hinzu, sobald Sie das Kontingent erreicht haben. Sie brauchen sich um nichts zu kümmern, der Speicherplatz passt sich den Bedürfnissen an. Wer Geld für Speicherplatz zahlen möchte, sollte also abwägen und vergleichen. Hier eine Auswahl der Angebote – weitere finden Sie im Internet.

Anbieter	Produkt	Speicherplatzkapazität	Informationen
Freenet	MailBasic	k. A.	www.freenet.de
Freenet	MailPlus	5 GByte	www.freenet.de
Freenet	MailPower	Unbegrenzt	www.freenet.de
GMX	FreeMail	1 GByte	www.gmx.de
GMX	ProMail	5 GByte	www.gmx.de
GMX	TopMail	>10 GByte	www.gmx.de

Die Tabelle verdeutlicht, dass Sie schon kostenlos massig Speicherplatz bekommen – doch viele Lösungen haben oft einen entscheidenden Nachteil: Daten können nur über eine Webseite in das entsprechende Postfach hochgeladen werden. Das einfache Kopieren via Datei-Explorer o. Ä. funktioniert erst mal nicht.

Lesen Sie jetzt, wie das mit der FRITZ!Box trotzdem bewerkstelligt werden kann. Damit lässt sich der Speicherplatz als virtuelle Festplatte im Netz nutzen. Anschließend werden Dateien und Verzeichnisse in ein im Windows Explorer eingebundenes Onlinelaufwerk gespeichert.

Wer vermeiden möchte, dass die Daten auf dem Network Storage ohne Weiteres von anderen (etwa Administratoren des Betreibers) eingesehen werden können, verschlüsselt die Daten vor der Übertragung zusätzlich. Das geht schon mit einfachen Mitteln wie beispielsweise mit Kompressionsprogrammen wie UnRarX und StuffIt unter Mac OS oder WinRAR, 7-Zip etc. unter Windows – die meisten Programme am Markt bieten dafür einen Passwortschutz beim Erstellen der Archivdateien an. Soll das Archiv entpackt werden, ist das passende Passwort notwendig, damit der Zugriff auf den Inhalt möglich ist.

Egal ob Sie den Kennwortschutz verwenden oder nicht, ein Kompressionsprogramm sollten Sie in jedem Fall einsetzen. Das presst die Originaldateien nicht nur auf ein kleines, erträgliches Maß zusammen, sondern sorgt auch für schnellere Datenübertragungsraten. Zudem lässt sich der Platz auf dem Network Storage besser ausreizen. Die Datenübertragung auf den Webspeicherplatz erfolgt via FRITZ!Box-Cache mittels WebDAV, einem eigens dafür geschaffenen HTTP-kompatiblen Protokoll.

Mit WebDAV können auf einfache Weise Daten von der lokalen an der FRITZ!Box angeschlossenen Festplatte auf einen Internetserver hochgeladen werden. Das bietet nicht nur Speicherplatz, sondern lässt sich auch als Laufwerk im Finder unter Mac OS bzw. im Windows Explorer einbinden. Welchen Vorteil das haben kann, lesen Sie im nächsten Abschnitt, in dem das am Beispiel der GMX-Lösung demonstriert wird.

So koppeln Sie WebDAV-Speicher mit der FRITZ!Box

Das GMX MediaCenter dient als Onlineablage für wichtige Daten, für Digitalbilder, MP3-Files sowie auch für Fax- und Sprachnachrichten. Damit haben Sie wichtige Dateien von jedem PC aus, der mit einem Internetanschluss versorgt ist, jederzeit griffbereit. Das MediaCenter ist eine an die GMX-Mailbox gekoppelte Onlinefestplatte. Bei einem TopMail-Account stehen mehr als 10 GByte Speicher für E-Mails und Dateien zur Verfügung.

Praktisch ist auch die Attachment-Funktion, damit lassen sich direkt aus einer E-Mail heraus Attachments mit einem Klick in das GMX MediaCenter verschieben. Besonders bequem: Dank WebDAV lassen sich die Mediacenter von 1&1, web.de, GMX etc. mit der FRITZ!Box koppeln und anschließend als Freigabe bzw. Netzlaufwerk nutzen.

In der neuen FRITZ!Box 7390 hat AVM einen internen Speicher mit 512 MByte Kapazität verbaut, der als Netzwerkspeicher (NAS) für die angeschlossenen Computer zur Verfügung gestellt werden kann. Die dort gespeicherten Daten können zunächst per FTP zur Verfügung gestellt werden, doch mit der Zeit wird der Speicherplatz recht knapp. Sie können dann an eine der beiden USB-Schnittstellen der FRITZ!Box (USB 2.0) einen USB-Stick oder besser gleich eine externe USB-Festplatte anschließen, um den verfügbaren Speicherplatz zu erweitern.

Bild 6.7 Neue praktische Möglichkeiten mit der neuen FRITZ!Box: Wer den sogenannten Onlinespeicher eines Internetanbieters im Einsatz hat, kann dessen Inhalt auf die angeschlossene USB-Festplatte der FRITZ!Box spiegeln. Dafür setzen Sie das Häkchen bei *Online-Speicher aktivieren*, wählen den Dienstanbieter aus und tragen die Anmeldedaten des Servers ein (WebDAV).

Um den Onlinespeicher der FRITZ!Box beispielsweise unter Windows einzubinden, tragen Sie in der Adressleiste im Explorer einfach *\\fritz.box* ein. Anschließend erscheint eine Kennwortabfrage. Hier ist der Benutzername standardmäßig *ftpuser* – das dazugehörige Kennwort setzen Sie unter *Einstellungen/Erweiterte Einstellungen/Speicher (NAS)/Einstellungen* im oberen Bereich bei *Berechtigung für den Netzwerkzugriff*.

Bild 6.8 Im Windows Explorer tragen Sie für den Benutzer *ftpuser* das persönliche Kennwort ein.

Abhängig von der Download-Geschwindigkeit des Internetanschlusses dauert es anschließend einen Moment, bis der Onlinespeicher gespiegelt auf der USB-Festplatte vorhanden ist. Er dient vorwiegend als Cache und weniger als Backup – kann jedoch auch als Sicherheitskopie für den Onlinespeicher genutzt werden. Hier ist lediglich darauf zu achten, dass für den Cache auch immer genügend freier Speicherplatz auf der USB-Festplatte zur Verfügung steht.

Anschließend wird der Inhalt wie ein lokaler Ordner im Explorer angezeigt. Das Bearbeiten, Löschen, Kopieren und Verschieben von Dateien und Ordnern ist wie gewohnt mit dem Explorer möglich. Für das händische Verschieben und Kopieren von Daten auf den Network Storage ist das GMX MediaCenter also eine äußerst praktische Sache. Das Arbeiten an verschiedenen Computern wie Macbooks oder auch innerhalb von Heim- und Firmennetzwerken erfordert oft ein bequemeres automatisiertes Abgleichen von Datenbeständen. Damit sind entsprechende Daten immer auf dem gleichen Stand.

7 FRITZ!Box-Mediaserver

Um den in der FRITZ!Box eingebauten Mediaserver nutzen zu können, muss zunächst ein USB-Speicher an der USB-Schnittstelle der FRITZ!Box angeschlossen sein. Nahezu jede moderne FRITZ!Box ist mit einem oder mehreren USB-Anschlüssen ausgestattet. An den USB-Anschluss der FRITZ!Box lässt sich neben den üblichen USB-Geräten wie USB-WLAN-Stick, USB-Festplatte und USB-Drucker auch ein USB-Hub anschließen, an dem wiederum bis zu drei USB-Geräte angeschlossen werden können.

Die »USB-Dreifach-Steckdose« lässt hier entweder drei USB-Speicher (Stick und/oder Festplatte) oder zwei USB-Speicher (Stick und/oder Festplatte) mit einem USB-Drucker zu. Derzeit ist es standardmäßig »noch« nicht möglich, mehr als einen USB-Drucker an dem USB-Anschluss der FRITZ!Box zu nutzen.

7.1 Mediendaten fließen lassen

Ist ein USB-Hub oder sind über einen USB-Hub mehrere USB-Speicher an der FRITZ!Box angeschlossen, wird der Speicher von der FRITZ!Box in der Regel automatisch erkannt, sofern er mit dem FAT32-Dateisystem formatiert ist.

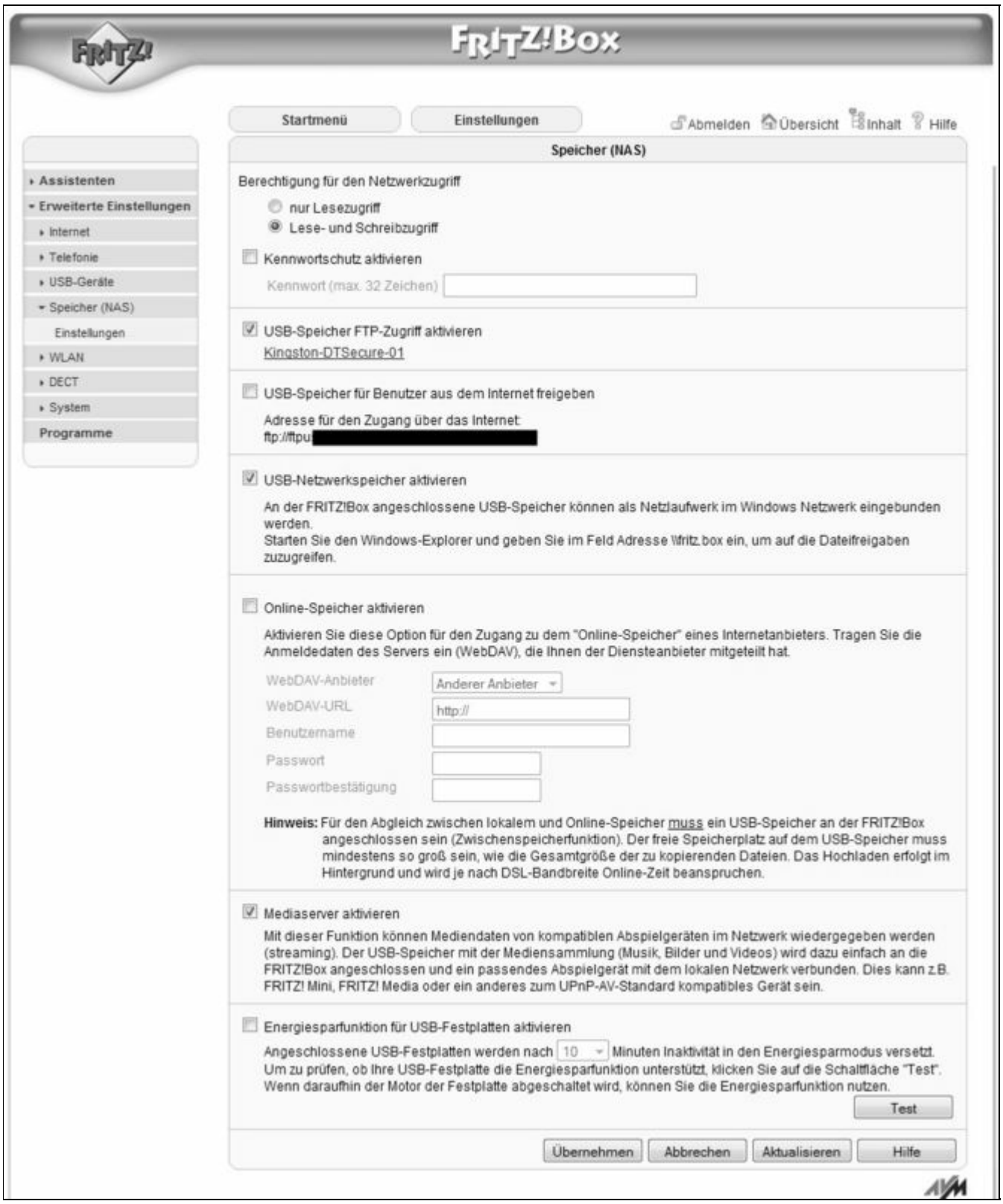


Bild 7.1 Ist der USB-Speicher an der FRITZ!Box angeschlossen und erfolgreich initialisiert, wird er im Bereich *Einstellungen/Erweiterte Einstellungen/Speicher (NAS)/Einstellungen* angezeigt. Für das schnelle Befüllen im Heimnetz nutzen Sie am besten den FTP-Zugriff.

Wird das Kontrollkästchen *Mediaserver aktivieren* aktiviert, erzeugt die FRITZ!Box automatisch die dazu nötige Verzeichnisstruktur auf dem USB-Speicher. In diesem Verzeichnis liegt anschließend die Mediensammlung (Musik, Bilder und Videos), die dann von kompatiblen Abspielgeräten im Heimnetzwerk wiedergegeben bzw. in Neudeutsch gestreamt werden kann.

7.2 Mediaserver mit Musik befüllen

Für den unkomplizierten Zugriff in einem Windows-Heimnetz sollten Sie sowohl das Häkchen bei *USB-Speicher FTP-Zugriff aktivieren* als auch ein Häkchen bei *USB-Netzwerkspeicher aktivieren* setzen. Damit können an der FRITZ!Box angeschlossene USB-Speicher als Netzlaufwerk im Windows Netzwerk eingebunden werden.

Dafür starten Sie Ihren Webbrowser und geben im Feld *Adresse* http://fritz.box ein, um auf die Dateifreigaben zuzugreifen. Per Kontextmenü der rechten Maustaste (*Netzlaufwerk verbinden*) weisen Sie anschließend auf Wunsch den gewünschten Laufwerkbuchstaben zu.

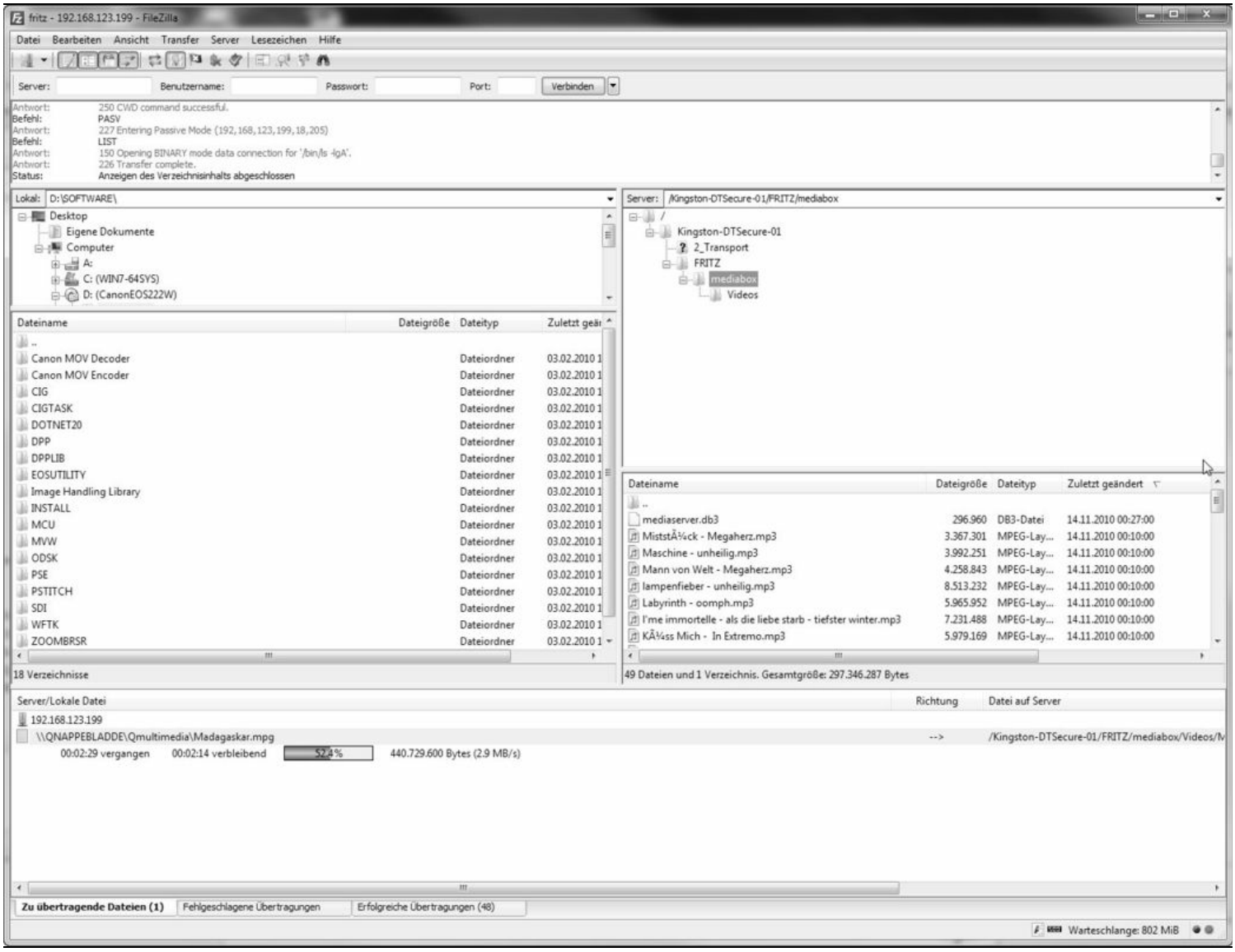


Bild 7.2 Egal ob Windows, Mac oder Linux: Mit einem FTP-Client greifen Sie über den FTP-Port direkt auf den USB-Speicher der FRITZ!Box zu. So lässt sich auch von einem entfernten Computer aus die heimische Multimedia-Sammlung bequem verwalten.

Ist der FRITZ!Box-Mediaserver nach Ihren Vorlieben mit Musik, Bildern und Videos befüllt, steht der Inhalt sämtlichen Computern und UPnP-AV-Standard-kompatiblen Geräten zur Verfügung. Für die Wiedergabe am Windows-Computer reicht der bordeigene Windows Media Player aus. Hier finden Sie im Übersichtsfenster im Bereich *Andere Medienbibliotheken* übersichtlich aufbereitet den auf die FRITZ!Box geladenen Inhalt.

Bild 7.3 Egal ob Playstation 3, Mac oder Windows-Computer: Die im Speicher der FRITZ!Box befindlichen Multimedia-Dateien lassen sich nun im Heimnetz abspielen.

Für das erstmalige Befüllen der Mediathek auf dem USB-Speicher können Sie diesen aus Zeitgründen auch direkt an die USB-Schnittstelle des Computers hängen. Dank des kompatiblen FAT32-Formats steht die Verzeichnisstruktur des FRITZ!Box-Mediaservers nach dem Einrichten über die FRITZ!Box auch direkt am Computer zur Verfügung.

Der Vorteil der beschriebenen FRITZ!Box-Lösung ist, dass Filme, Musik und Bilder auch bei ausgeschaltetem Computer im gesamten Heimnetzwerk verfügbar sind. Bietet der Fernseher, die TV-Box oder die Spielkonsole eine UPnP-AV-Schnittstelle, können die Mediendaten dort direkt von der FRITZ!Box bzw. dem USB-Speicher wiedergegeben werden.

7.3 Hochauflösender TV-Genuss

Fernsehen im HD-Format – spätestens seit dem Umstieg der öffentlich-rechtlichen TV-Anstalten hat sich das hochauflösende Fernsehen HD-TV auch im Massenmarkt etabliert. Doch hat die Wohnung oder das Haus keinen Kabelanschluss oder ist das Anbringen einer SAT-Schüssel nicht erlaubt, macht sich in Sachen HD-TV schnell Ernüchterung breit, denn das Überall-TV DVB-T eignet sich aus Bandbreitengründen nicht für das HD-Format.

Was sind die Mindestvoraussetzungen für den IPTV-Empfang?

Glaubt man den bunten Werbebeilagen in der Tageszeitung, sorgt hier zumindest in Großstädten und Ballungszentren die IPTV-Technik für Abhilfe, die neben dem hochauflösenden HD-Signal auch weitere Vorteile wie beispielsweise zeitversetztes Anschauen, die TV-Aufnahme auf Festplatte, eine elektronische Programmzeitschrift und weitere Features mitbringen kann.

Bild 7.4 Hier finden Sie eine ausführliche Übersicht über WebTV- und IPTV-Sender: *http://bit.ly/dHm09I*.

Grundsätzlich ist für den Empfang von IPTV meist ein DSL-Anschluss mit mindestens 16 MBit/s Voraussetzung. Da IPTV in der Regel im Zusammenhang mit Triple Play derzeit nur im Paket mit Telefon- und Internetanschluss erhältlich ist und somit eine Internet-Flatrate sozusagen obligatorisch ist, bleibt es nicht bei einem Basispreis. Meist wurde solchen Paketen noch eine Telefon-Flatrate in das deutsche Festnetz hinzugepackt. Die meisten Angebote unterscheiden sich in der Regel in den Zusatzleistungen.

In welchen Städten und Wohngebieten VDSL verfügbar ist, erfahren Sie auf der hier gezeigten Webseite *http://bit.ly/f7YTaF* . Klicken Sie im Bereich *Verfügbarkeit prüfen* auf die Schaltfläche *Prüfen*.

Bild 7.5 Entertain mit VDSL. Beim Marktführer T-Home gibt es unterschiedliche Bandbreiten – DSL 16+, VDSL 25 und VDSL 50 –, aber nur mit dem schnellen VDSL ist das hochauflösende HD-IPTV möglich.

7.4 Entertain mit Tücken

Die Vorteile von IPTV liegen auf der Hand, die damit verbundenen Nachteile erschließen sich nach und nach und kommen in der täglichen Praxis ans Licht. Da, wie der Name IPTV schon erahnen lässt, das Fernsehsignal über eine konventionelle Internetverbindung via TCP/IP in das Wohnzimmer kommt, ist das Fernsehen auch nur mit funktionsfähigem Internetanschluss möglich.

Im Zusammenhang mit IPTV taucht ebenfalls ständig der Begriff Multicast auf: Dabei werden die TV-Signale, die für alle Kunden bestimmt sind, komplett zu einem Verteiler im näheren Umkreis gesendet, der wiederum die Kundschaft in der Nähe mit IPTV versorgt. So braucht der IPTV-Anbieter nicht jeden einzelnen Sender separat zum Kunden zu schicken – bei Video on Demand (VoD) ist nämlich genau das der Fall. Hier findet statt der Multicast- eine sogenannte Unicast-Übertragung statt, und zwar nicht nur aus Abrechnungsgründen, sondern auch weil damit der Kunde den gewünschten Inhalt anschauen kann, wann er möchte.

Ist der Receiverspeicher mit einer USB-Festplatte erweiterbar?

TV-Aufnahmen werden bequem über die Fernbedienung oder automatisch per Timer auf die im Receiver eingebaute Festplatte gespeichert. Je nach ihrer Größe ist die Festplatte mehr oder weniger schnell voll, und anschließend werden die Aufnahmen nach dem FIFO-Prinzip (First In First Out) gelöscht, um Platz für neue Aufnahmen zu schaffen.

Das Erweitern des Speicherplatzes mithilfe einer externen USB-Festplatte war mal versprochen, ist aber trotz eines vorhandenen USB-Anschlusses am Receiver seitens der Telekom nicht vorgesehen. Aktuell kann der USB-Anschluss des IPTV-Receivers wenigstens noch als Ladestation für MP3-Player, Handys, iPhones etc. genutzt werden – wer will, kann sogar einen USB-Tischventilator anschließen. Wie auch immer, dank der Telekom spart man sich einen USB-Adapter für diesen Zweck.

Als Videoarchiv taugt der Receiver auch nur bedingt: Die Aufnahmen werden verschlüsselt auf der internen

Receiverfestplatte abgelegt und können auch nicht so einfach auf einen Computer kopiert oder beispielsweise auf eine DVD gebrannt werden. So eignet sich die IPTV-Box weder zur Datensicherung der Lieblingsfilme noch zum Aufbau einer eigenen Film-Mediathek, da bei einer Reparatur des Receivers oder gar bei einem Receiverfestplattencrash die darauf gespeicherten Daten verloren sind.

Zusätzlich absurd wird die Aufnahmefunktion durch die Einschränkung, dass sich die Aufnahmen von der Receiverfestplatte ebenfalls nur bei aktivem Internetanschluss abspielen lassen, der Telekom-Logik folgend natürlich nicht an irgendeinem Anschluss – beispielsweise bei Freunden oder Nachbarn – nein, es muss zwingend der eigene T-Home-Anschluss sein. Ist der Internetanschluss aus welchem Grund auch immer unterbrochen, bleibt der TV-Bildschirm schwarz, und das Abspielen der lokal auf der Receiverfestplatte gespeicherten Aufnahmen ist nicht möglich.

Somit eignet sich der T-Home-Receiver also nur für TV-Aufnahmen, die auch mal »verloren gehen« dürfen. Für langfristige Archivierungen gibt es dankenswerterweise Lösungen zum Selbstbau, die Sie mithilfe der FRITZ!Box und einer daran angeschlossenen Festplatte sowie einem Computer mit installiertem VLC-Player realisieren können.

7.5 TV-Programm per Doppelklick

Kein großes Geheimnis ist der Einsatz des VLC-Players samt einer IPTV-Playlist. Die öffentlich-rechtlichen Sender stellen im Internet eine fix und fertig konfigurierte Playlist zur Verfügung, mit der alle ARD- und ZDF-Programme mit einem einfachen Doppelklick aufgerufen werden können.

Bild 7.6 Auf der Webseite von ARD Digital finden Sie im Bereich *IPTV/Software-Download* den VLC Media Player und eine VLC-Playlist für T-Home: *http://bit.ly/hCVvMm*.

Ist der kostenlose VLC-Player – *www.videolan.org/vlc/* – installiert, lassen sich die digitalen Programme von ARD und ZDF mithilfe dieser Playlist auf dem Computer abspielen und mit dem VLC-Player auch auf die lokale Festplatte oder auf einer Freigabe im heimischen Netzwerk speichern.

Um die Playlist in VLC einzubinden, öffnen Sie im Menü *Ansicht/Playlist* im Playlist-Dialogfenster über *Manage/Open Playlist* die M3U-Datei. Anschließend erscheint der Inhalt der Playlist in der VLC-Wiedergabeliste, die Sie bequem per Mausklick steuern können. Ist der gewünschte TV-Kanal gestartet, können Sie ihn bis zur vollen Bildschirmgröße auf Ihrem

Bildschirm beliebig skalieren.

Die VLC-Playlist lässt sich natürlich für eigene Zwecke bearbeiten und mit weiteren nicht öffentlichen Kanälen ergänzen. Öffnen Sie die M3U-Datei mit einem einfachen Texteditor wie Notepad, Primalscript, Ultraedit oder der kostenlosen Alternative Notepad++ (*http://notepad-plus-plus.org*), die erweiterte Bearbeitungsfunktionen zur Verfügung stellt und mehr ist als ein einfacher Ersatz für das Windows-eigene Werkzeug Notepad.

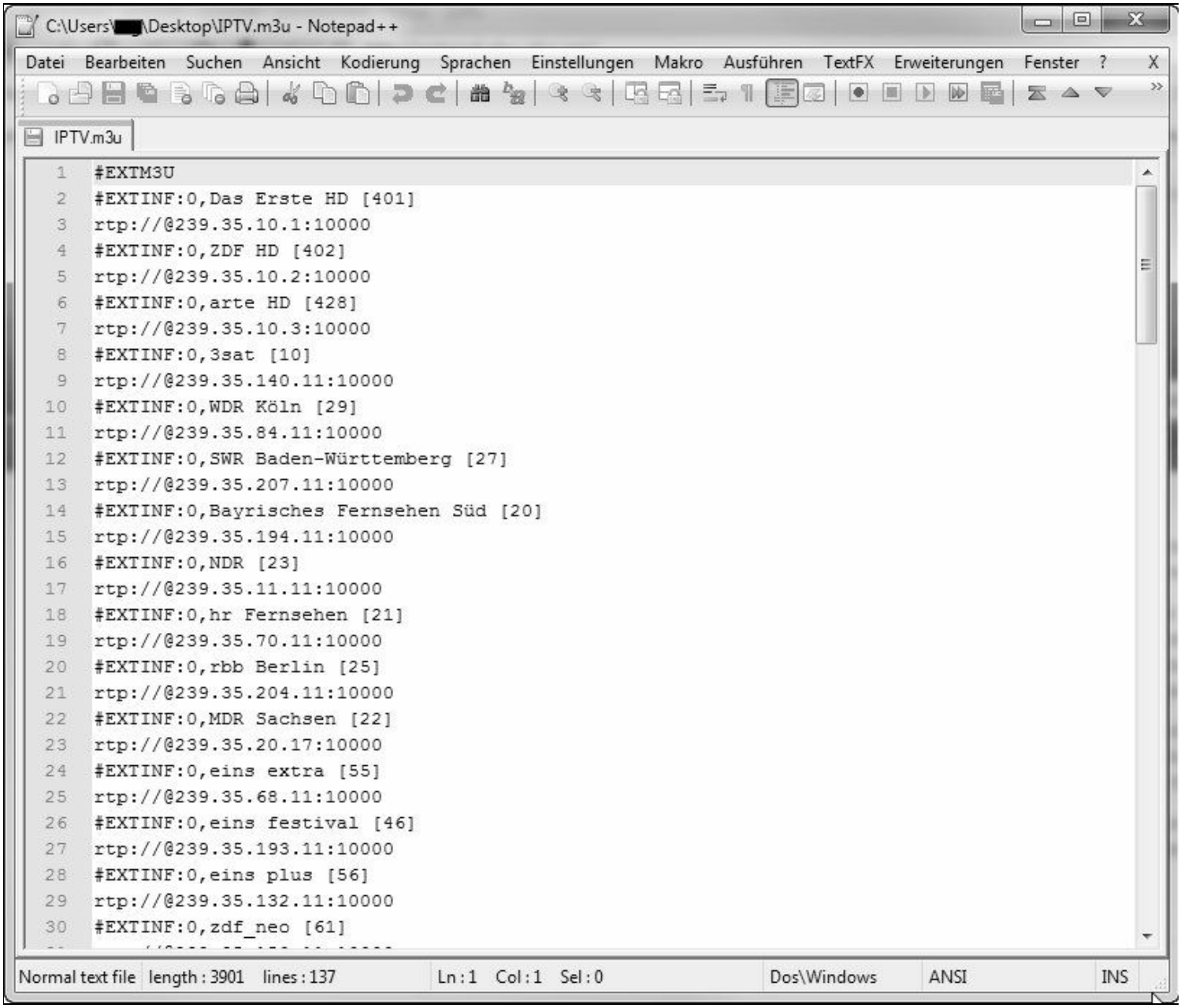


Bild 7.7 Die M3U-Datei muss mit dem Header *#EXTM3U* versehen sein, anschließend sind zeilenweise die entsprechenden Kanäle mit Beschreibung sowie deren RTP-Adresse mit Port *10000* eingetragen.

Je nach IPTV-Anbieter (Telekom, Alice etc.) sind die Multicast-Adressen unterschiedlich. In Sachen T-Home sind derzeit folgende Kanäle bzw. IP-Adressen aktuell. Beachten Sie, dass sich diese unregelmäßig aufgrund von Programmwechseln ändern können.

Kanal	IP-Adresse
Das Erste HD	239.35.10.1
ZDF HD	239.35.10.2
ARTE HD	239.35.10.3
CNN International	239.35.3.11
Das Vierte	239.35.3.12
ARTE	239.35.4.11

ZDFtheater	239.35.5.11
Tele 5	239.35.20.1
NDR	239.35.11.11
Anixe SD	239.35.20.2
QVC	239.35.12.11
Sat1 HD	239.35.20.3
Pro7 HD	239.35.20.4
Deluxe Lounge HD	239.35.20.6
Kabel 1 HD	239.35.20.7
ARD 2	239.35.20.8
TV 5 Monde Europe	239.35.18.11
MDR	239.35.20.17
Deluxe Music	239.35.67.11
EinsExtra	239.35.68.11
HR	239.35.70.11
K-TV	239.35.72.11
Nickelodeon	239.35.75.11
Radio Bremen	239.35.76.11
DMAX	239.35.76.12
MTV	239.35.77.12
n-tv	239.35.79.11
WDR	239.35.84.11
WDR 2	239.35.84.11
ZDF	239.35.86.11
Das Erste	239.35.129.11
Bloomberg	239.35.130.11
EinsPlus	239.35.132.11
HSE 24	239.35.134.11
Bibel TV	239.35.137.11
N24	239.35.138.11
PHOENIX	239.35.139.11
3SAT	239.35.140.11
RTL	239.35.143.11
SR	239.35.145.11
VIVA	239.35.147.11
ZDFneo	239.35.150.11
EinsFestival	239.35.193.11
BR	239.35.194.11
Euronews	239.35.196.11
BR-alpha	239.35.202.11
RBB	239.35.204.11
Ki.Ka	239.35.205.12
SWR	239.35.207.11
RTL2	239.35.208.11

ZDFinfo	239.35.214.11
TIMM	239.35.214.12

Um beispielsweise den TV-Sender MTV der VLC-Playlist hinzuzufügen, öffnen Sie die M3U-Datei mit einem Editor und ergänzen am Dateiende die zwei folgenden Zeilen:

```
#EXTINF:0,MTV Germany [71]
rtp://@239.35.77.12:10000
```

Anschließend speichern Sie die Datei und binden via *Ansicht/Playlist* im *Playlist*-Dialogfenster über *Manage/Open Playlist* die geänderte Playlist erneut in VLC ein.

So automatisieren Sie die Aufnahme eines TV-Kanals

Die Vorzüge des kostenlosen VLC-Players sind allseits bekannt, und die Flexibilität des Programms samt Kommandozeilensteuerung macht VLC auch für eigene maßgeschneiderte Zwecke interessant – beispielsweise für die automatisierte Aufnahme eines Kanals. Ist VLC einmal eingerichtet, reicht prinzipiell der Aufruf von *vlc.exe* gefolgt von der RTP-Adresse auf der Kommandozeile aus, um die Wiedergabe zu starten. Für die Aufnahme ist eine Skriptdatei der bequemere Weg, da VLC verschiedene Übergabeparameter zur Steuerung benötigt.

In diesem Beispiel haben wir eine Batchdatei mit der Bezeichnung *VLCrec.bat* erstellt – diese Datei können Sie sich im Download-Bereich *buch.cd* herunterladen, nach Belieben verändern und auch ergänzen. Wichtig ist zunächst, dass Sie den Speicherpfad (das Verzeichnis, in das VLC die Aufnahme speichern soll) sowie gegebenenfalls den Programmpfad von VLC (unter Windows Vista/7 in der Regel *C:\Program Files (x86)\VideoLan\VLC*) anpassen.

```
@echo off
**********************************************************************
::
:: Speicherort anpassen – hier U:\FRITZ\mediabox\Videos
SET DEST_PATH=U:\FRITZ\mediabox\Videos

:: ggf. VLC-Pfad anpassen – hier "C:\Program Files (x86)\VideoLan\VLC\"
SET VLC_PATH="C:\Program Files (x86)\VideoLan\VLC\"

::
**********************************************************************
SET KANAL=%1
SET REC_TIME=%2
SET FILENAME=%3
:: Parameter checken
IF "%REC_TIME%" equ "" cls&&GOTO err2
IF "%FILENAME%" equ "" set FILENAME=%KANAL%_%DATE%
SET error=0
```

Der Speicherpfad ist in diesem Beispiel das gemappte Laufwerk *U:\FRITZ\mediabox\Videos* der an der FRITZ!Box angeschlossenen Festplatte. Da der Mediaserver der FRITZ!Box über das FRITZ!Box-Menü aktiviert ist, hat er selbstständig die Verzeichnisstruktur *\fritz\mediabox* angelegt.

Damit die VLC-Aufnahmen auch vom FRITZ!Box-Mediaserver genutzt werden können, speichern Sie sie gleich dort ab – das zusätzliche Verzeichnis *Videos* im Verzeichnis *\FRITZ\mediabox* dient nur der eigenen Übersicht. Der FRITZ!Box-Mediaserver scannt automatisch sämtliche Unterverzeichnisse nach Bild-, Video- und Musikdateien.

VLCrec.bat im Einsatz: Aufnahme über die Kommandozeile

Legen Sie die Datei *VLCrec.bat* in ein eigenes Verzeichnis oder speichern Sie sie einfach auf dem Desktop Ihres Computers. Über *Start/Ausführen/cmd* öffnen Sie die DOS-Kommandozeile und wechseln per *cd*-Befehl in das Verzeichnis, in dem Sie die *VLCrec.bat*-Datei gespeichert haben.

Je nach Ablageverzeichnis und Windows-Version sind hier Administratorrechte notwendig. Dazu wählen Sie über *Start/Suchen / cmd* per Klick auf *cmd* im Kontextmenü den Eintrag *Als Administrator ausführen* aus. Anschließend verbinden Sie sich als User *ftpuser* mit der NAS-Freigabe der FRITZ!Box – hier verwenden Sie den *net use*-Befehl:

```
C:\Windows\system32>net use u: \\fritz.nas\FRITZ.NAS /user:ftpuser
kennwort /PERSISTENT:yes
```

Mit dem Schalter */PERSISTENT:yes* am Ende des Befehls bleiben Benutzer und Kennwort gespeichert und müssen nicht immer neu eingegeben werden.

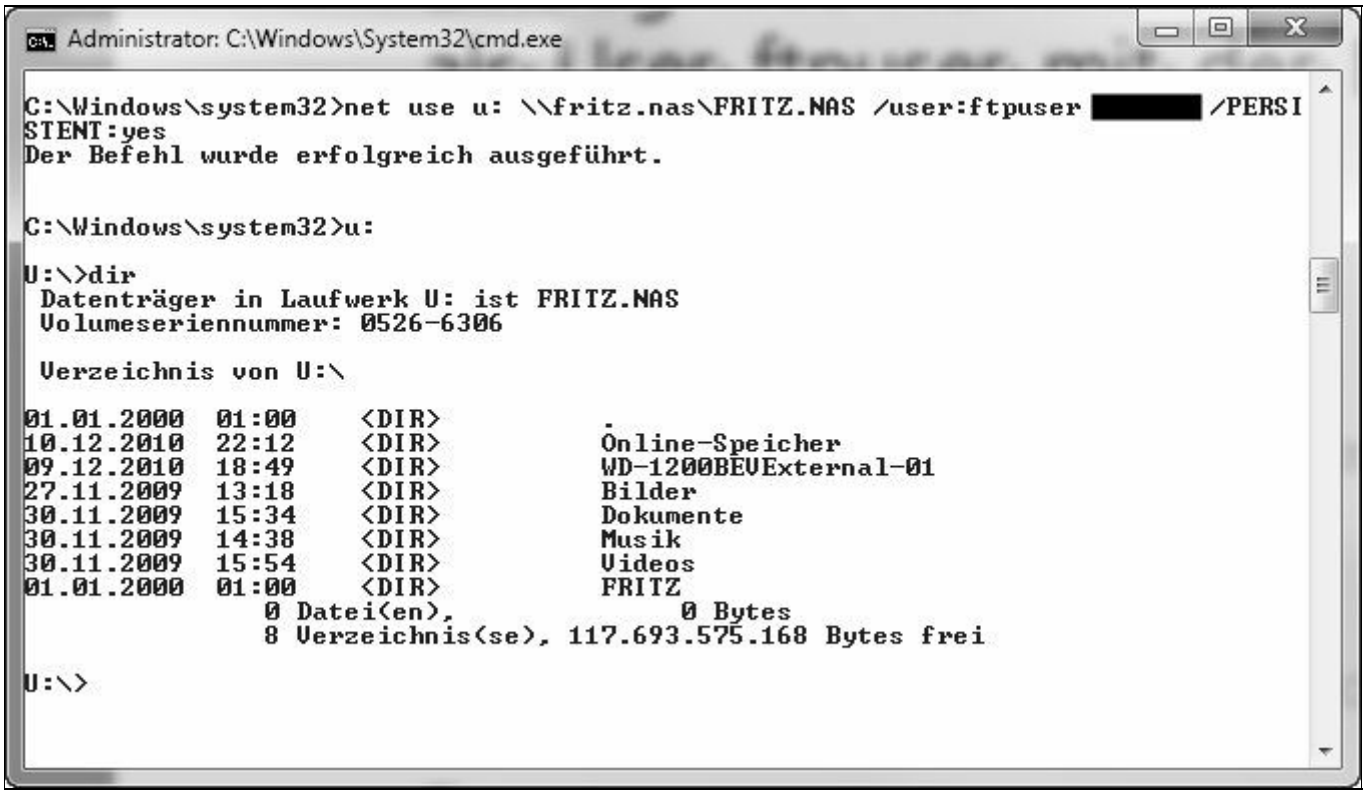


Bild 7.8 Nach dem Start der Administrator-Shell verbinden Sie sich als *ftpuser* mit der USB-Festplatte der FRITZ!Box.

Da Sie sich nach Starten der Kommandozeile im Windows-Verzeichnis befinden, tragen Sie nun den Befehl

```
cd %USERPROFILE%\Desktop
```

ein, falls Sie die *VLCrec.bat* auf dem Desktop gespeichert haben. Die Skriptdatei *VLCrec.bat* ist weitestgehend selbsterklärend. Zum Aufruf sind drei Parameter notwendig: der erste Parameter ist der Kanal, der zweite die Aufnahmedauer in Sekunden und der dritte der Dateiname ohne Dateinamenerweiterung.

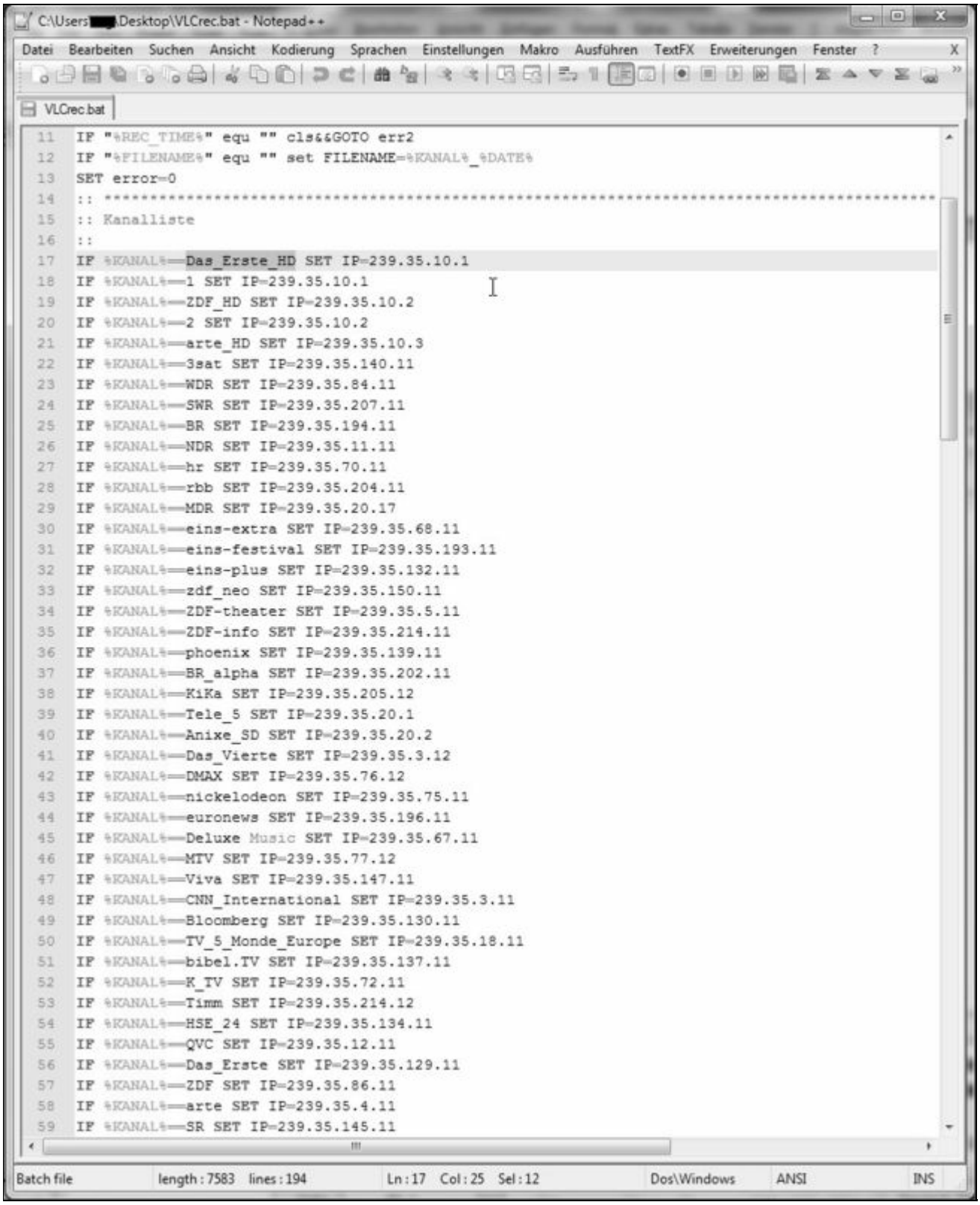


Bild 7.9 In der Datei *VLCrec.bat* finden Sie im Bereich *Kanalliste* die Kanalbezeichnungen – beispielsweise *Das_Erste_HD*.

Möchten Sie zum Beispiel einen fünfminütigen Musikclip vom Sender MTV auf die Festplatte sichern, rechnen Sie zunächst zwei Minuten in Sekunden um (2 * 60 = 120 Sekunden) und geben folgenden Befehl auf der Kommandozeile an:

```
VLCrec MTV 120
```

Ist der dritte Parameter (der Dateiname) beim Aufruf nicht vorhanden, baut das Skript ihn zur Laufzeit aus Kanal und Datum zusammen. Anschließend öffnet sich automatisch der VLC-Player – das Skript ist standardmäßig so eingestellt, dass die Aufnahme des Kanals auch mit Bildschirmausgabe erfolgt (Schalter: *dst=display*).

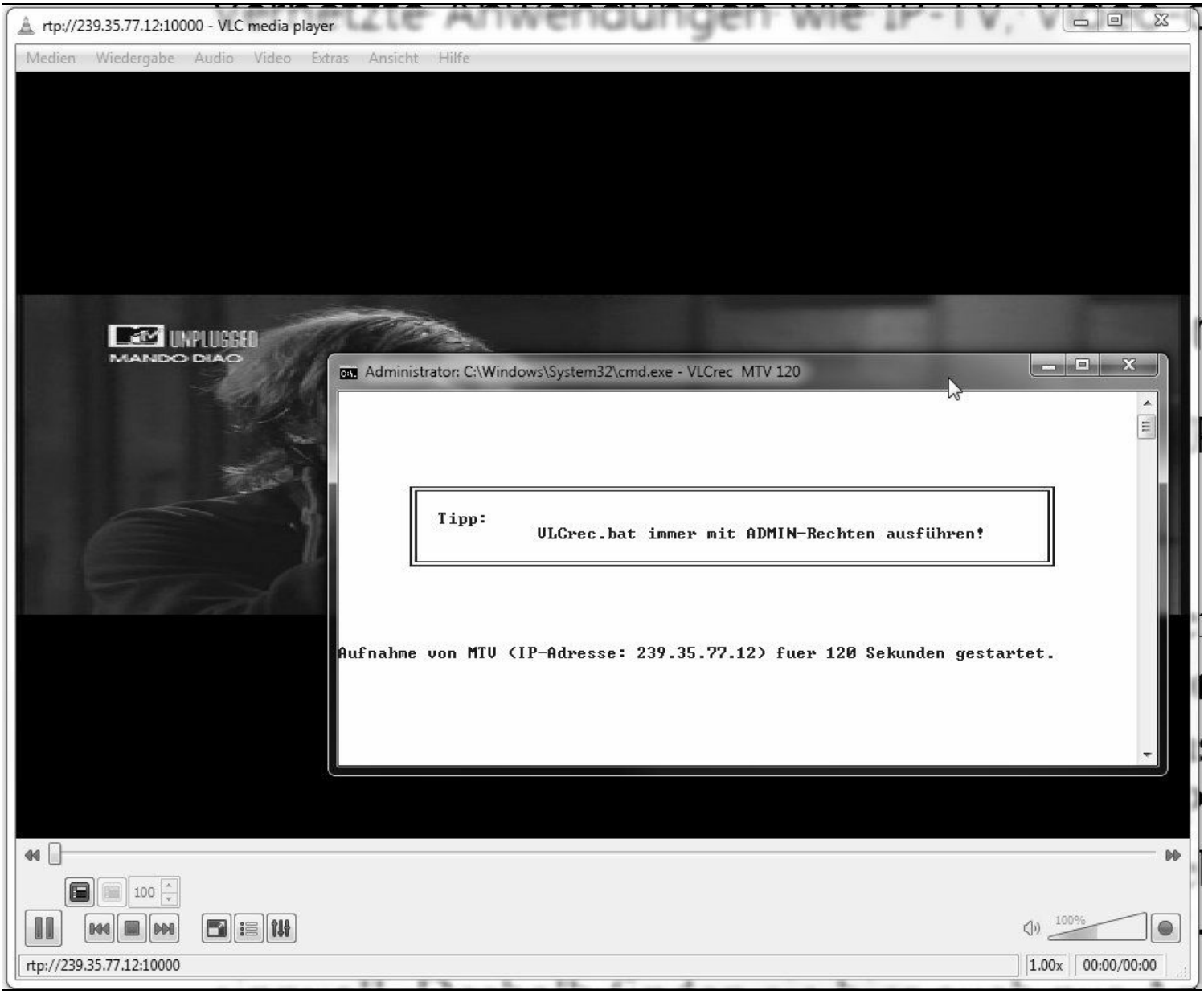


Bild 7.10 Nach dem Start via Kommandozeile wird der gewünschte Kanal im VLC-Player angezeigt und im Hintergrund über die Kommandozeile auf die Festplatte gespeichert.

Nach Ablauf der Aufnahmedauer prüft das Skript, ob noch ein VLC-Prozess aktiv ist. Ist das der Fall, wird er automatisch beendet. Anschließend ist die Aufnahme im gewünschten Ordner gespeichert und kann umgehend vom angeschlossenen Streamplayer im Heimnetz angeschaut werden.

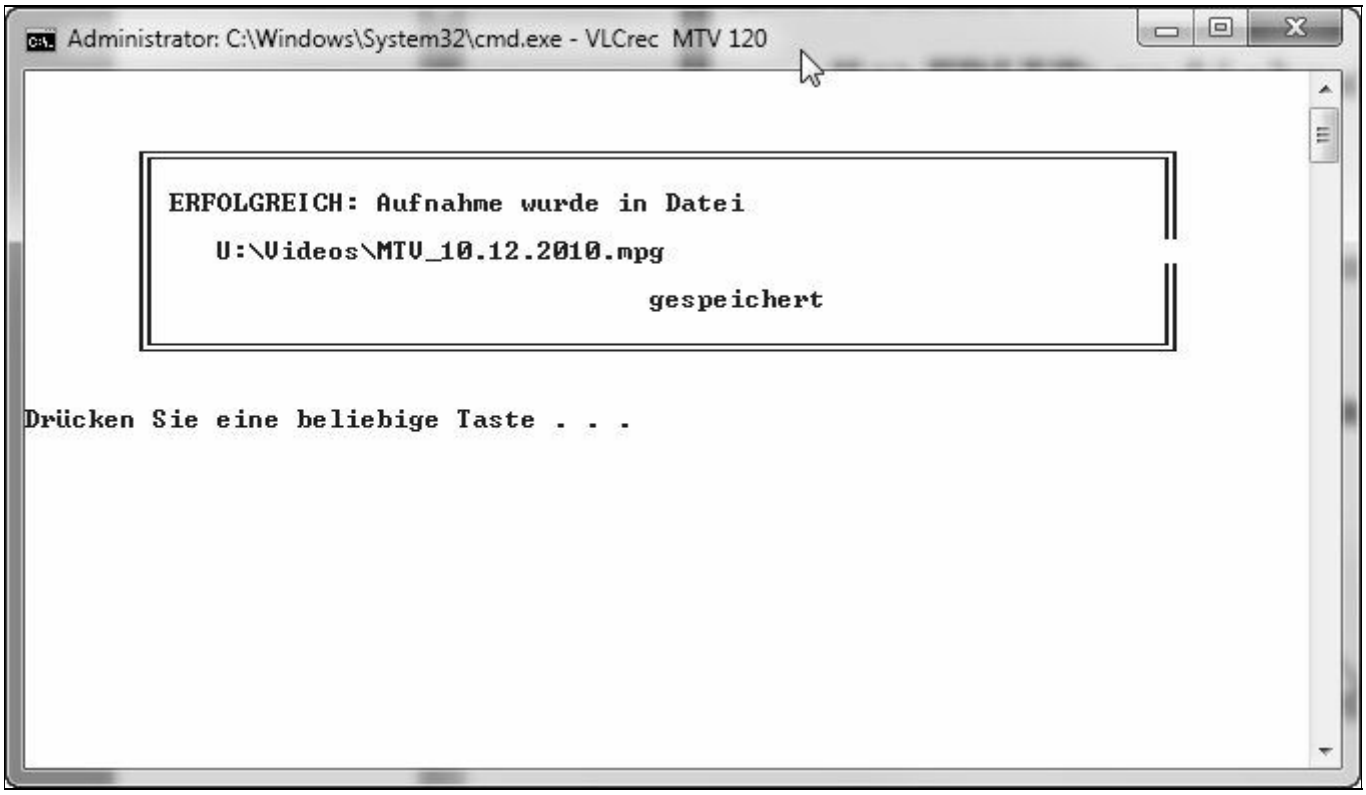


Bild 7.11 Erfolgreich gespeichert: Nach Abschluss der Aufnahme wirft das Skript eine Erfolgsmeldung aus, und nach einem Tastendruck ist das Skript beendet.

Die Aufnahme liegt nun im MPEG/TS-Format (Transport Stream) vor – hier können Sie sie über den FRITZ!Box-Mediaserver für sämtliche Geräte im Heimnetz freigeben, die Aufnahme auf DVD brennen oder sie anschließend für mobile Geräte wie iPad, iPhone und andere konvertieren.

7.6 Aufnahme im Player anschauen

Ist über die FRITZB!Box-Oberfläche das Optionsfeld *Mediaserver aktivieren* eingeschaltet, erscheint der Mediaserver auch in der Netzwerkübersicht von Windows mit der Bezeichnung *AVM FRITZ!Mediaserver*. Per Doppelklick darauf lässt er sich beispielsweise mit dem Windows Media Player nutzen.

Bild 7.12 Unmittelbar nach der Aufnahme steht das Videomaterial abrufbereit im Heimnetz.

Wer die beschriebene Methode ausgiebig nutzt, wird mit der Zeit feststellen, dass der Speicherbedarf der HD-Aufnahmen vergleichsweise groß ist. Egal ob die Aufnahme auf Festplatte mit dem Mac oder einem PC erfolgt: Eine HD-Aufnahme braucht Platz auf der Festplatte – viel Platz!

Da pro Minute für Bild und Ton einiges an Kapazität benötigt wird, sollten Sie, bevor Sie einen kompletten Spielfilm auf die Festplatte speichern, zunächst den zu erwartenden Platzbedarf auf der FRITZ!Box-Festplatte oder auf der lokalen Festplatte im Computer grob kalkulieren. Nehmen Sie einfach einen kürzeren Film oder nur einen kleinen Filmschnipsel auf, um die Kapazität einer Aufnahme mit längerer Spieldauer zu berechnen.

Dann wählen Sie auf der Festplatte die Aufnahmefilmdatei aus, prüfen den benötigten Speicherplatz und teilen diesen durch die Spieldauer der Filmdatei, um damit den Platzbedarf auf der Festplatte für eine Minute Film zu berechnen. Die Spieldauer der Filmdatei zeigt eine Abspielsoftware wie beispielsweise Video LAN Client an.

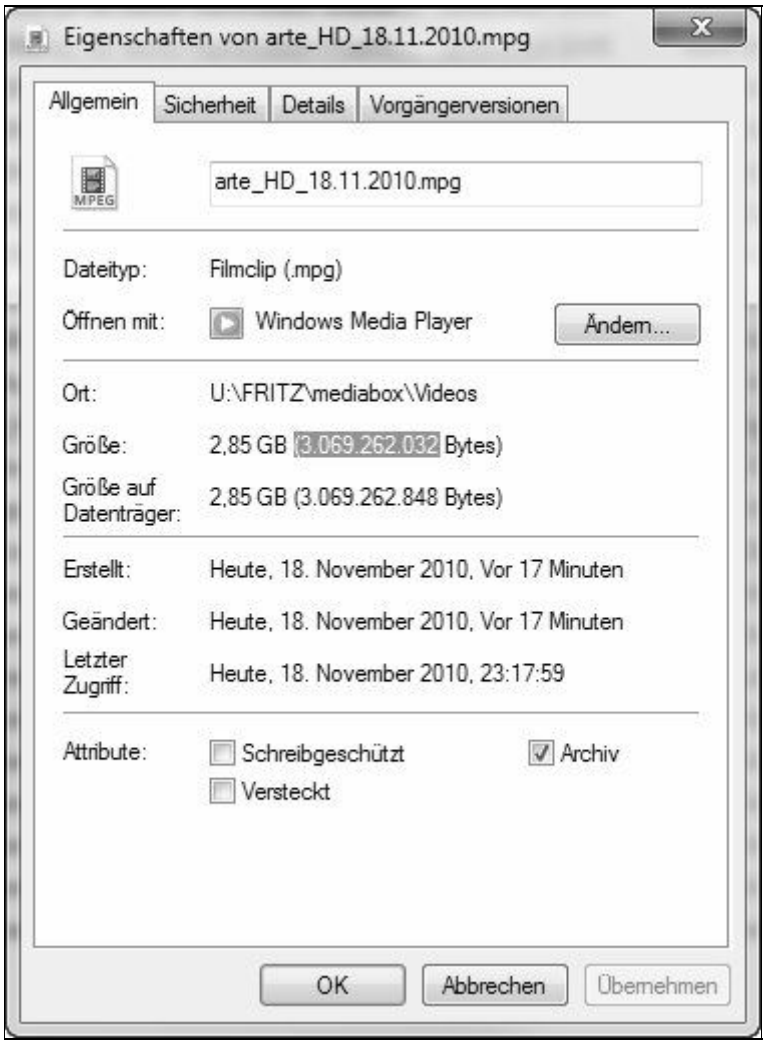


Bild 7.13 Speicherfresser: Gerade HD-Aufnahmen benötigen mehrere GByte Kapazität auf der Festplatte.

In diesem Beispiel ist die Datei 3.069.262.032 Byte groß und besitzt eine Spieldauer von 1:07:31. Eine Stunde hat bekanntlich 3.600 Sekunden, hinzuaddiert werden 7 Minuten (= 420 Sekunden) sowie 31 Sekunden, was in der Summe 4.051 Sekunden entspricht.

```
1:07:31 = 4051 Sekunden = 3.069.262.032 Bytes
1 Sekunde = 757655,40 Bytes = 739,89 KBytes

1 Minute = 44393,87 KBytes = 43,35 MBytes
90 Minuten = 3901,80 MByte = rd. 3,81 GByte
```

Diese einfache Rechnung zeigt, dass das FAT32-Dateisystem bei HD-Aufnahmen schnell an seine Grenzen stößt, sofern der Inhalt in eine einzelne Datei geschrieben wird. Bei FAT32 liegt die maximale Dateigröße bei 4 GByte (= 4.294.967.295 Byte), das entspricht 5.668,76 Sekunden, also etwas weniger als 95 Minuten. Mit etwas Timeshift und Puffer bei der Aufnahme wird es bei einem Film mit einer Standardspieldauer von 90 Minuten schnell knapp. Spätestens wenn Werbung im Film hinzukommt, ist mit FAT32 schnell Schluss mit der Aufnahme.

7.7 Auf das Dateisystem kommt es an

Offiziell unterstützt die FRITZ!Box »nur« FAT32 sowie das NTFS-Dateisystem. Letzteres hat den Vorteil, dass damit die lästige FAT32-Beschränkung in Sachen Dateigröße wegfällt. Bedingt durch die Architektur des NTFS-Dateisystems, dauert der (Schreib-)Zugriff jedoch gefühlte Ewigkeiten und sorgt bei längeren Aufnahmen für Ruckler und Bildstörungen. Das wiederum macht im dümmsten Fall die gesamte Aufnahme unbrauchbar.

Alternativ zu den DOS-/Windows-Dateisystemen steht für neuere FRITZ!Box-Modelle eine neue Firmware (ab 04.86) mit eingebauter ext2-Linux-Dateisystemunterstützung zur Verfügung. In jedem Fall sollten Sie nach einer frischen Firmware auf den AVM-Seiten Ausschau halten, bei neueren Modellen ersparen Sie sich den Firmwareumbau via Freetz, mit dem Sie

eine speziell auf Ihren Bedarf zugeschnittene Firmware erstellen können.

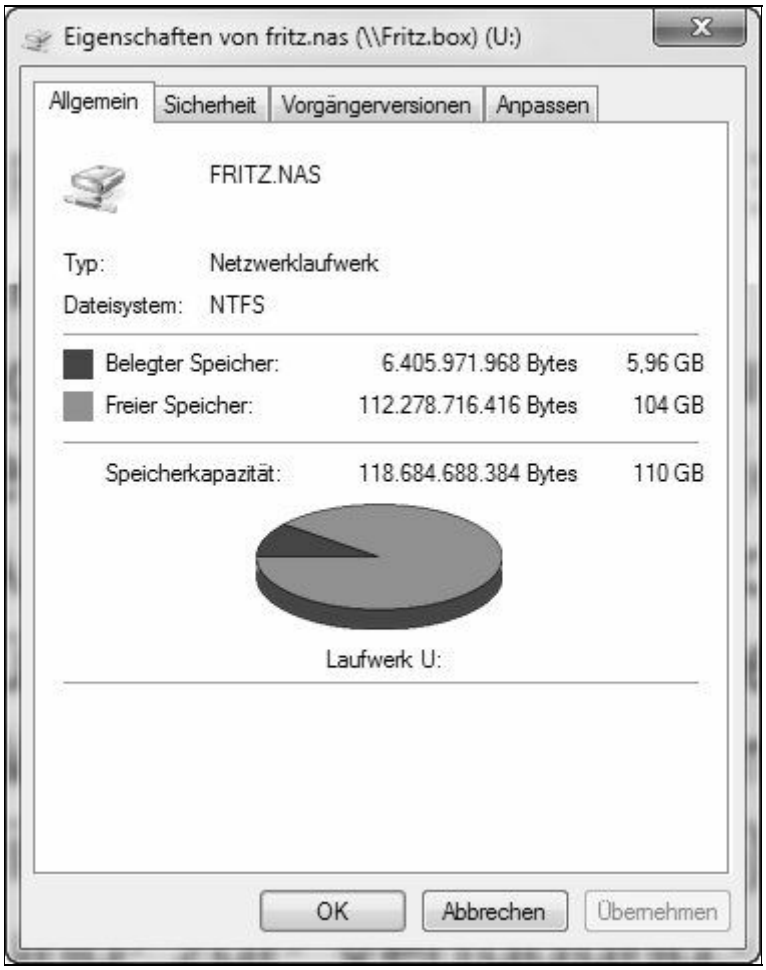


Bild 7.14 Die ext2-Partition der externen USB-Festplatte an der FRITZ!Box erscheint unter Windows als NTFS-formatiertes Netzwerklaufwerk.

Für FRITZ!Boxen ohne frische Firmware mit eingebauter ext2-Unterstützung hilft ein von AVM undokumentierter Kniff:

Nutzen Sie einfach das Linux-Dateisystem ext2 oder ext3 für die externe Festplatte der FRITZ!Box mit einer gemoddeten Firmware. Da das Linux-Dateisystem standardmäßig bisher nicht von der Originalfirmware von AVM unterstützt wird, war bzw. ist für ältere FRITZ!Box-Modelle dafür eine Anpassung der Firmware nötig.

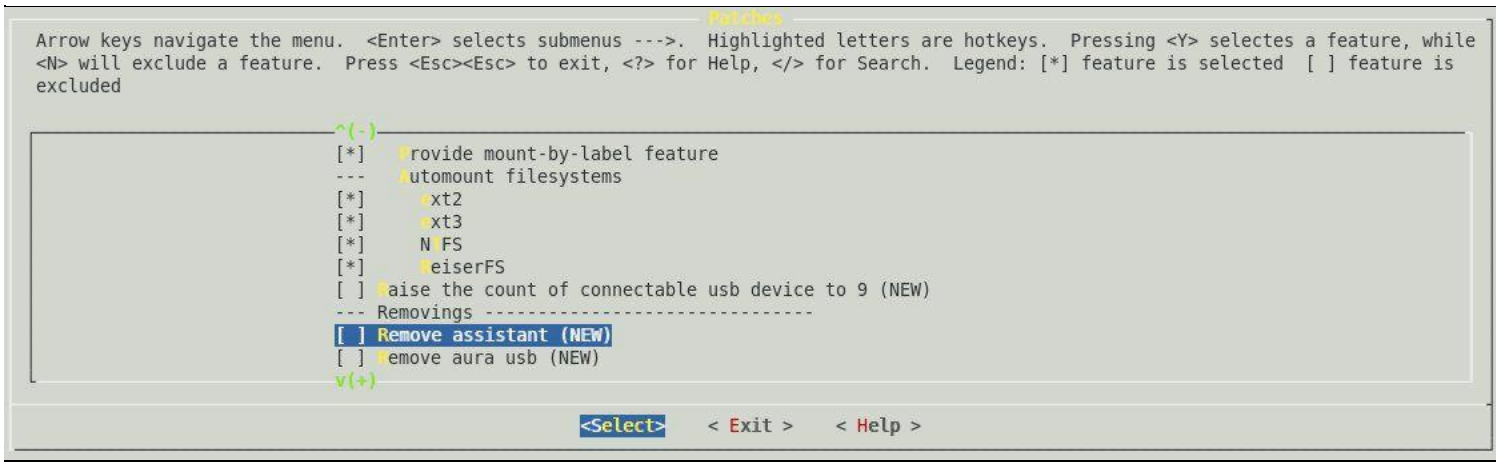


Bild 7.15 Für die Unterstützung weiterer Dateisysteme bieten die Tools speed2fritz bzw. Freetz einfache Möglichkeiten.

FAT32- in das ext2/ext3-Dateisystem umwandeln

Um eine Festplatte in das Linux-Dateiformat ext2/ext3 zu bringen, nutzen Mac OS- und Windows-Anwender am besten eine virtuelle Maschine (VMware etc.) samt darauf installiertem Linux. Verwenden Sie im Terminal den Befehl:

```
sudo apt-get install gparted
```

um das übersichtliche Partitions- und Formatierungswerkzeug zu installieren. Wer auf Linux verzichten will, kann alternativ die *gparted*-Live-CD nutzen (*http://gparted.sourceforge.net/livecd.php*).

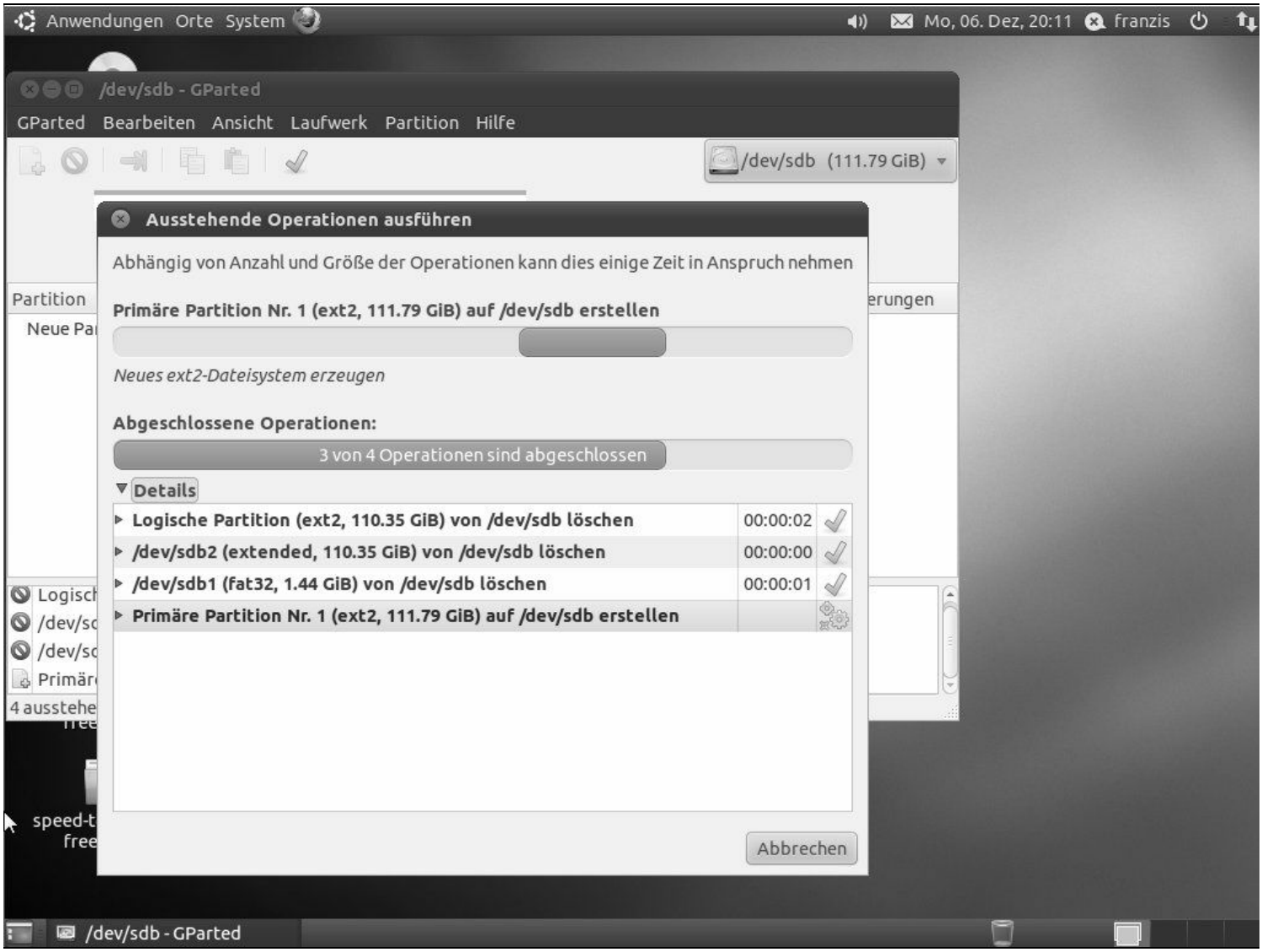


Bild 7.16 Für die Umwandlung von Festplatte oder USB-Stick in das Linux-ext2-/ext3-Format nutzen Sie am besten das Partitionierungswerkzeug *gparted*.

Ist die USB-Festplatte partitioniert und mit dem Dateisystem ext2 formatiert, wird sie manchmal auch von der FRITZ!Box, spätestens aber von Freetz erkannt. Im FRITZ!Box-Menü – *Startmenü/Ereignisse/USB-Geräte* – wird das Einstecken registriert.

```
Partition unter WD-1200BEVExternal-01 eingebunden
USB-Gerät 1002, Klasse 'USB 2.0 (hi-speed) hub', angesteckt
USB-Gerät 1003, Klasse 'USB 2.0 (hi-speed) storage', angesteckt
```

Nachstehendes Beispiel zeigt das Log einer »gefreetzten« FRITZ!Box – hier steht */dev/sda* für die USB-Festplatte und */dev/sda1* für die erste Partition der USB-Festplatte.

```
Partition unter uStor01 (/dev/sda1) eingebunden
USB-Gerät 003, Klasse 'USB 2.0 (hi-speed) storage', angesteckt
USB-Gerät 002, Klasse 'USB 2.0 (hi-speed) hub', angesteckt
```

Falls Sie mit Freetz die FRITZ!Box aufgebohrt haben, können Sie im nächsten Schritt via Freetz-Samba die Verzeichnisfreigaben einrichten. Das alles ist bei den neueren FRITZ!Box-Firmwareversionen nicht nötig, da die ext2-Festplatte von der AVM-Firmware erkannt wird. Bei einer Freetz-Lösung im obigen Beispiel wurde nur eine ext2-Partition genutzt und mithilfe des Eintrags

```
/var/media/ftp/uStor01 EXT2BLADDE 1 0
```

in die Freetz-Samba-Optionen eingetragen.

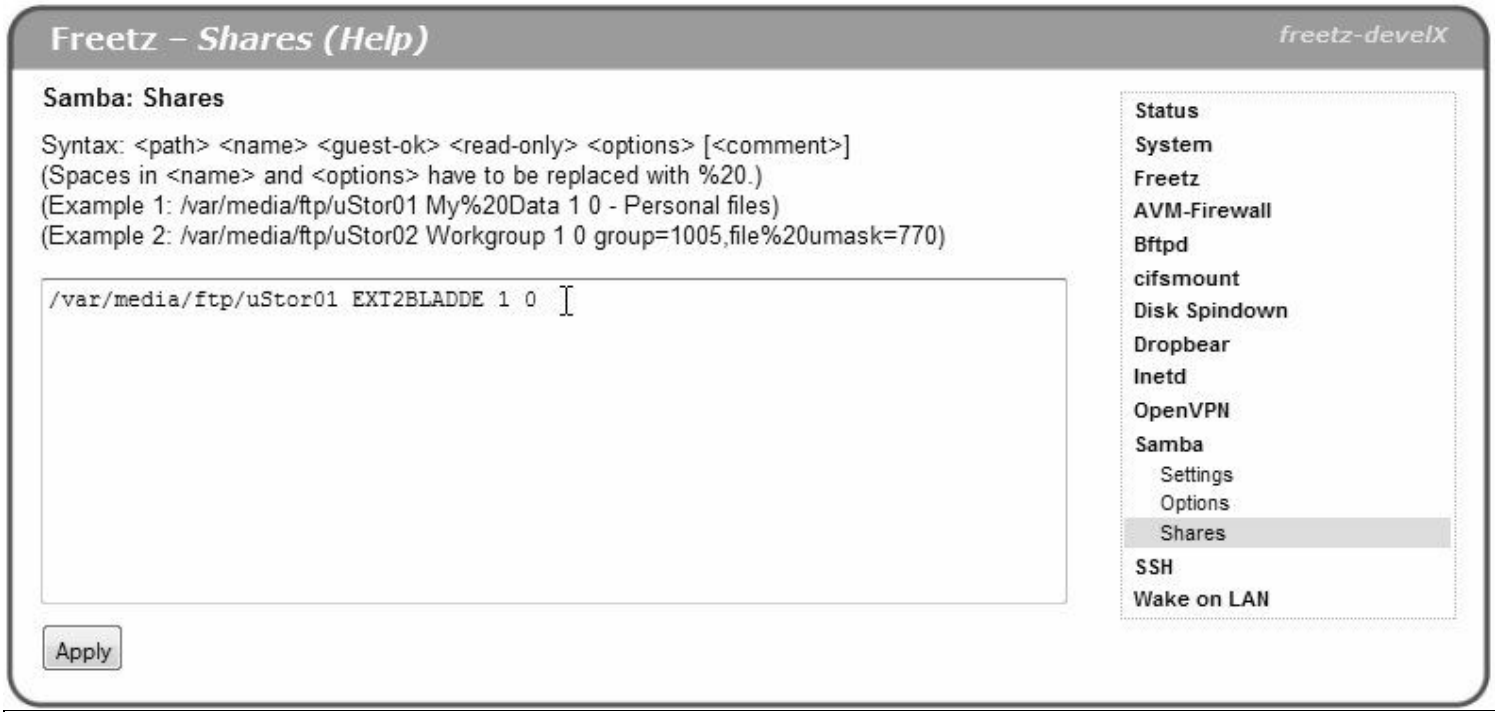


Bild 7.17 Nur eine Zeile Code ist für die Samba-Konfiguration notwendig, um die ext2-Partition im Heimnetz verfügbar zu machen.

Im nächsten Schritt tragen Sie optional weitere Samba-Optionen ein:

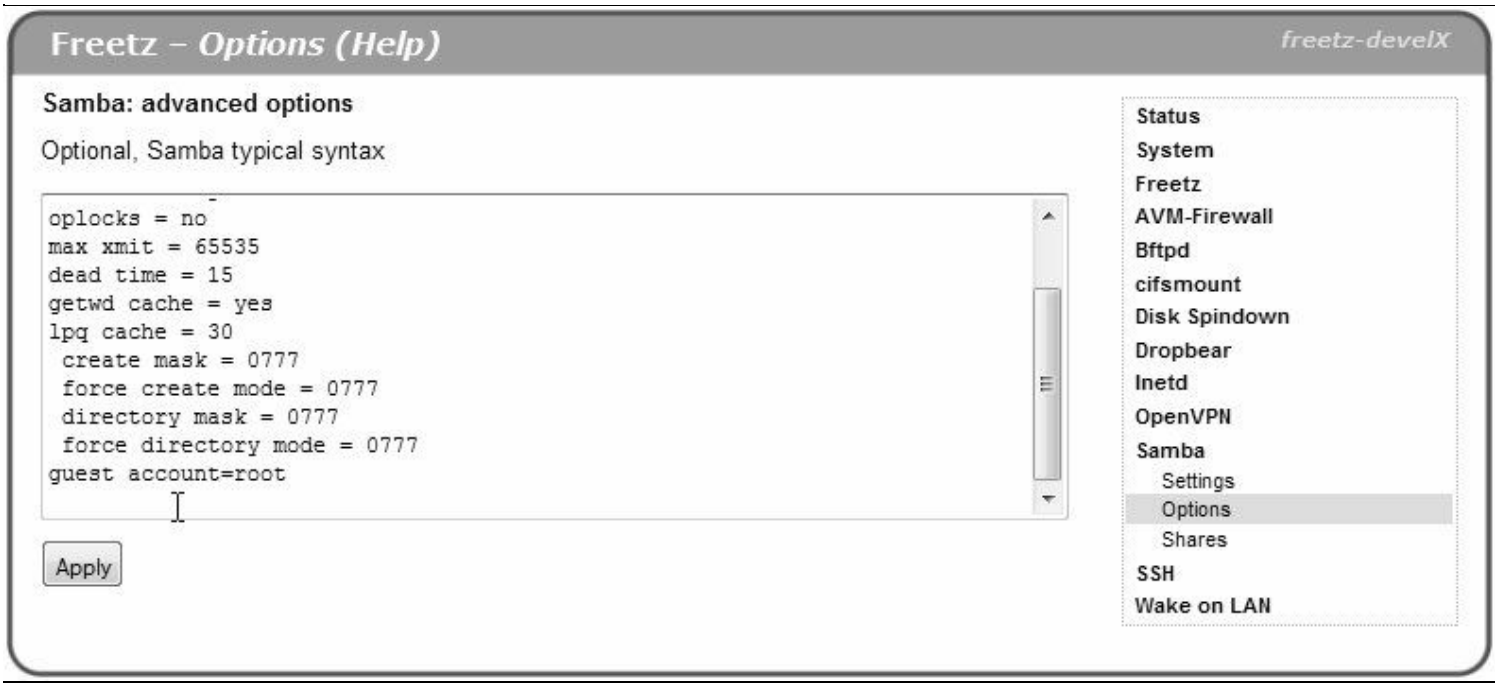


Bild 7.18 Um überhaupt Schreibzugriff auf die Samba-Freigabe von Windows aus zu bekommen, muss der Eintrag *guest account=root* im Menübereich *Options* eingetragen werden. Fehlt dieser Eintrag, ist nur lesender Zugriff auf die Freigaben im Heimnetz möglich.

Per Klick auf die *Übernehmen*- bzw. *Apply*-Schaltfläche werden die Samba-Dienste beendet und neu gestartet. Anschließend ist die Änderung sofort im Netzwerk aktiv – im Windows Explorer oder Mac OS Finder ist der FRITZ!Box-Samba-Server in der Netzwerkumgebung sichtbar.

8 Zugriff auf das Heimnetz

Das Wichtigste vorab: Remotezugriffstechniken wie die von Windows bekannte Remotedesktopverbindung, die plattformübergreifende VNC-Technik und dergleichen sollten aus Sicherheitsgründen grundsätzlich über sichere Verbindungen wie HTTPS, SSL oder besser VPN geführt werden. Möchten Sie, dass der Zugriff auf Ihr Heimnetzwerk immer zur Verfügung steht, setzt das einen permanent eingeschalteten Computer voraus, der dadurch in seinen Leerlaufzeiten unnötig Strom verbraucht und damit Geld kostet. Das muss nicht sein: Die FRITZ!Box ist in der Regel ohnehin immer eingeschaltet, aber dennoch deutlich energiesparender als ein permanent eingeschalteter Computer.

8.1 Computer im Heimnetz fernsteuern

Mit der FRITZ!Box steuern Sie mithilfe der sogenannten Wake on LAN-Funktion die Geräte in Ihrem Heimnetzwerk. Hier lässt sich der gewünschte Computer einfach per Mausklick aus der Ferne einschalten, um nach ein paar Minuten des Hochfahrens mit einem Fernwartungsprogramm via SSL oder VPN auf ihn zuzugreifen. In diesem Abschnitt lesen Sie, wie Sie aus dem Internet auf die Benutzeroberfläche der FRITZ!Box zugreifen und einen Computer im Heimnetzwerk starten.

So geben Sie die sichere Fernwartung der FRITZ!Box frei

Sind die Experteneinstellungen der FRITZ!Box aktiviert, finden Sie, wie im nachstehenden Dialog bei *Einstellungen/Erweiterte Einstellungen/Internet/Freigaben* zu sehen, das Häkchen bei *Fernwartung freigeben*. Anschließend wählen Sie einen beliebigen Benutzernamen plus Kennwort für den Zugriff auf die FRITZ!Box-Log-in-Seite aus. Achten Sie aus Sicherheitsgründen darauf, dass sich Benutzername und Kennwort von Ihrem Windows-Zugang bzw. vom FRITZ!Box-Kennwort unterscheiden.

Sicherheitsfetischisten wählen im gleichen Dialogfenster noch einen alternativen Port für den Zugriff via HTTPS-Protokoll aus. Anstelle des Standardports 443 können Sie Portadressen aus dem Bereich 450 bis 499 verwenden. HTTPS (*HyperText Transfer Protocol Secure*) steht für das sichere Hypertext-Übertragungsprotokoll, das in diesem Beispiel über Port 450 übertragen werden soll.

Grundvoraussetzung für den bequemen Zugriff auf die FRITZ!Box über das Internet ist natürlich ein eingerichteter dynamischer DNS-Name.

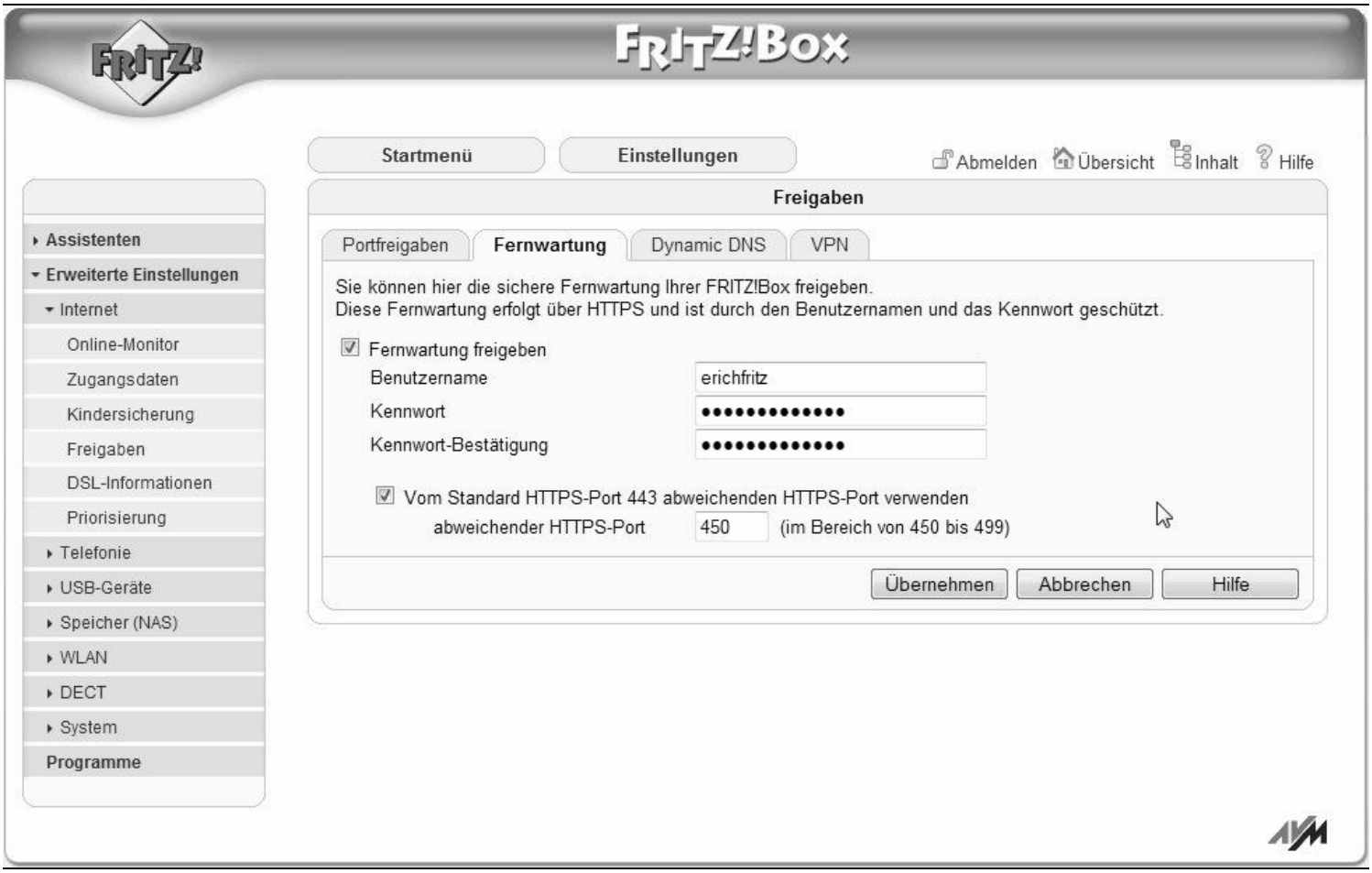


Bild 8.1 Sind die Einstellungen festgelegt, klicken Sie auf die *Übernehmen*-Schaltfläche.

Sicherer Zugriff auf die FRITZ!Box mit HTTPS

Dank des dynamischen DNS brauchen Sie sich nicht die externe WAN-IP-Adresse der FRITZ!Box zu merken, die ja in der Regel bei Privatkunden alle 24 Stunden vom Provider geändert wird. In diesem Beispiel greifen Sie über den dynamischen DNS-Namen https://meinheimserver.homedns.org:450 und das HTTPS-Protokoll über den selbst definierten Port 450 auf Ihre FRITZ!Box zu Hause zu.

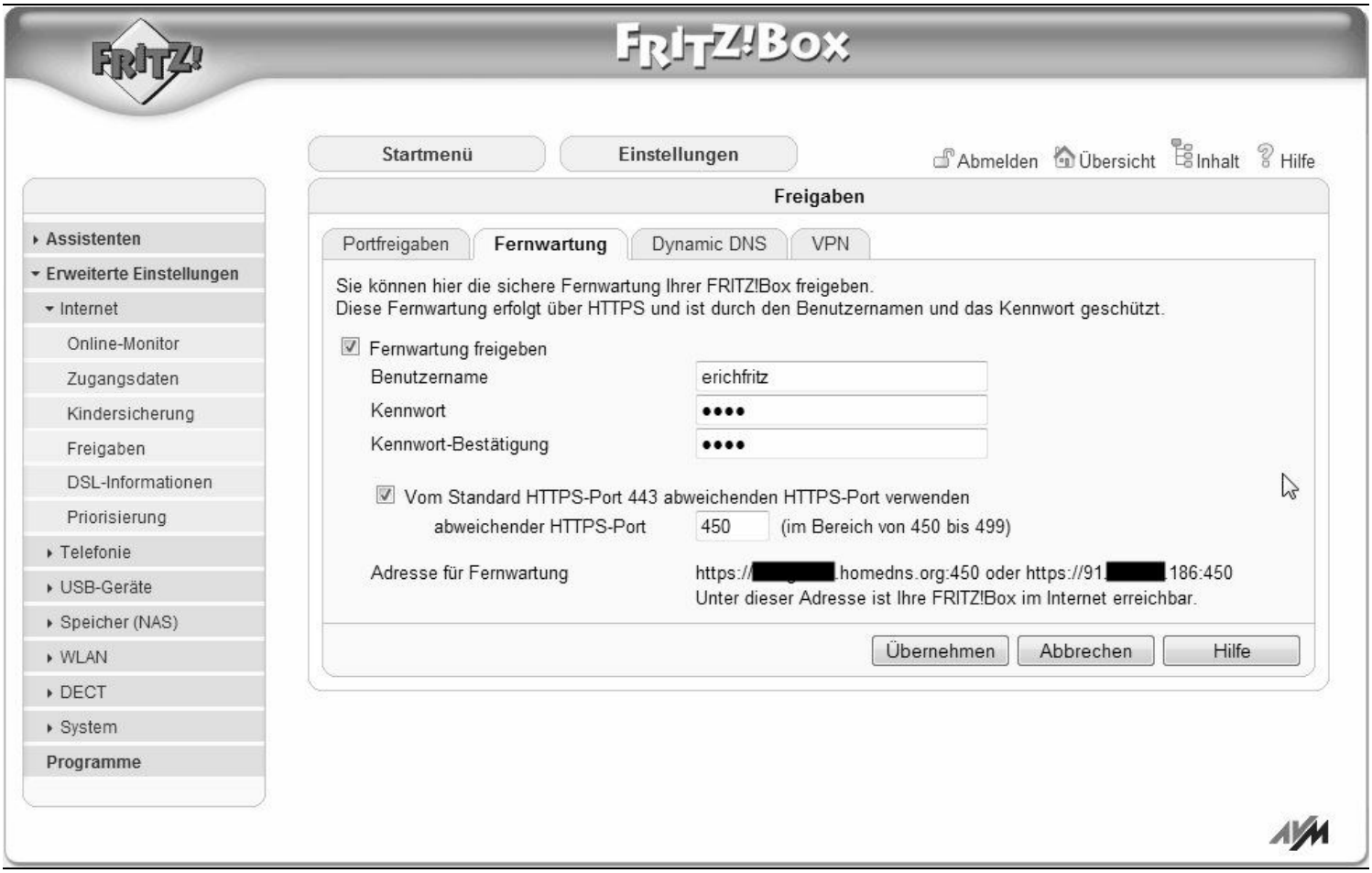


Bild 8.2 Sind die neuen Einstellungen per Klick auf die *Übernehmen*-Schaltfläche bestätigt, wirft die FRITZ!Box im selben Dialog auch die eingerichtete Fernwartungsadresse aus.

Nun ist die FRITZ!Box im Internet unter der konfigurierten DynDNS-Adresse erreichbar. Nach dem Aufruf der Adresse prüft der Browser zunächst das Zertifikat der HTTPS-Ausgabe. Hier lässt sich auf Wunsch vom Browser das von der FRITZ!Box generierte Zertifikat anzeigen. Da diese HTTPS-Verbindung auf das eigene Heimnetz zeigt, können Sie also dem Zertifikat für diese Sitzung oder auch permanent vertrauen.

Dafür klicken Sie auf die *Fortfahren*-Schaltfläche (Safari), die Schaltflächen *Ich kenne das Risiko/Ausnahmen hinzufügen/Sicherheits-Ausnahmeregel bestätigen* (Firefox) bzw. *Laden dieser Website fortsetzen (nicht empfohlen)* (Internet Explorer 8), um das Zertifikat zu genehmigen. Andernfalls wird die HTTPS-Verbindung nicht hergestellt, und der Zugriff auf die FRITZ!Box wird unterbunden.

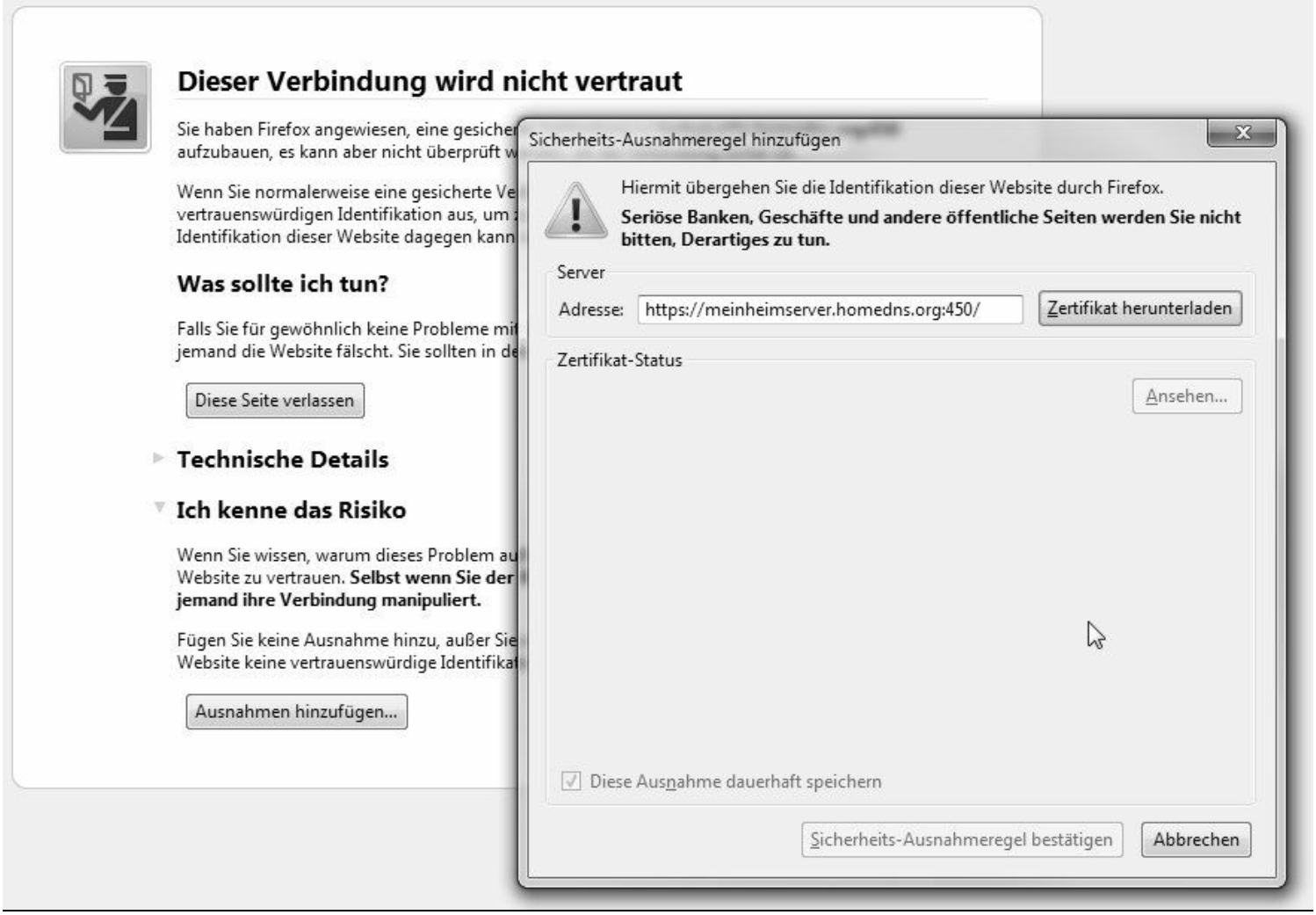


Bild 8.3 Viele Klicks sind bei Firefox notwendig, um endlich auf die HTTPS-Log-in-Seite der FRITZ!Box zu kommen.

Bei Safari reicht der Klick auf die *Fortfahren*-Schaltfläche, um zum Benutzername/Kennwort-Dialog zu gelangen.

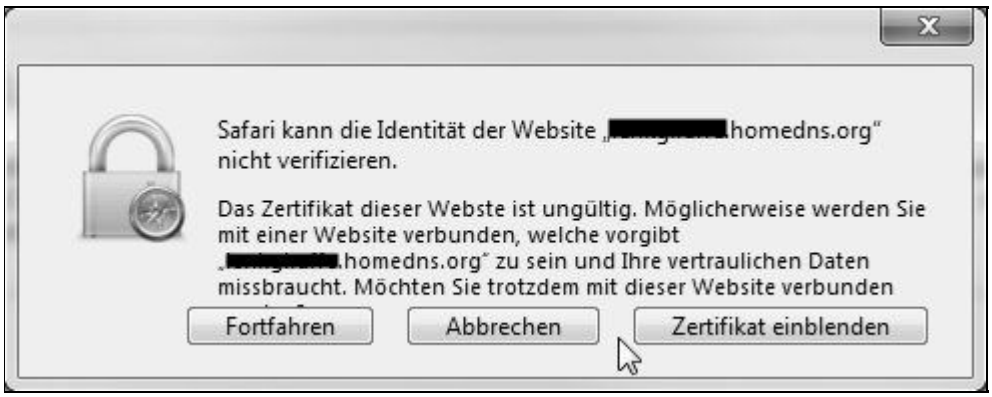


Bild 8.4 Auf Wunsch kann hier auch der Inhalt des Zertifikats eingeblendet werden. Für den Zugriff auf die FRITZ!Box-Webseite muss jedoch zwingend auf die *Fortfahren*-Schaltfläche im Safari-Browser geklickt werden.

Anschließend fragt die FRITZ!Box Benutzername und Kennwort für den Zugriff auf die Benutzeroberfläche ab.

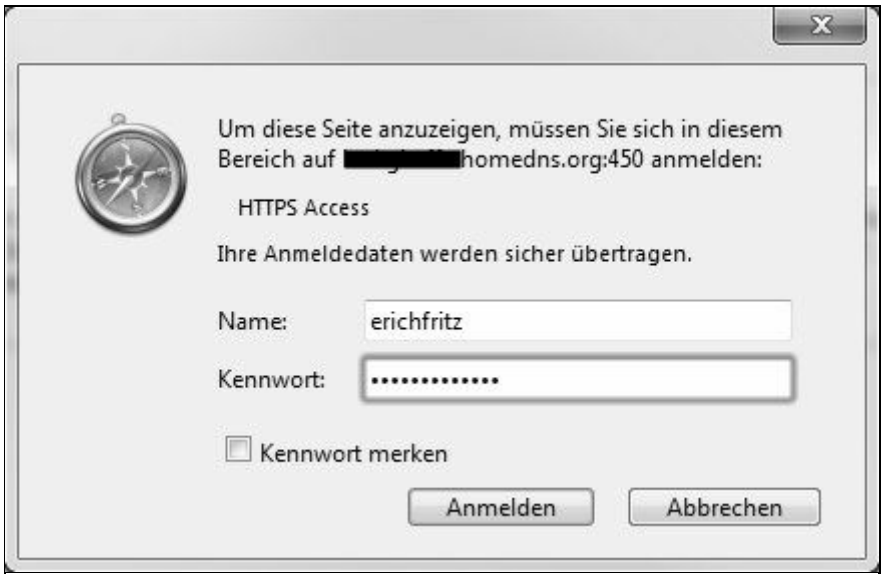


Bild 8.5 Nun tragen Sie den Benutzernamen sowie das Kennwort für den Zugriff auf die HTTPS-Seite der FRITZ!Box ein.

Ist die Log-in-Hürde genommen, erscheint der Gerätedialog der FRITZ!Box. Hier können Sie das schon bekannte Gerätekennwort des Geräts nutzen, um auf die Konfigurationsseiten zuzugreifen.

Bild 8.6 Erfolgreich über das Internet verbunden: Nun können Sie sich wie gewohnt an der FRITZ!Box anmelden.

Im nächsten Schritt wecken Sie den gewünschten Computer in Ihrem Heimnetz auf. Dafür sind prinzipiell nur wenige Klicks notwendig, falls folgende Voraussetzungen erfüllt sind:

1. Der Computer bzw. dessen Netzwerkkarte unterstützt Wake on LAN.
2. Wake on LAN ist im Computer-BIOS eingeschaltet.
3. Der Computer hat eine »feste« IP-Adresse.

Während Punkt 1 in diesem Buch vorausgesetzt wird (nahezu jeder Computer mit Onboard-Netzwerkschnittstelle besitzt ein Boot-EPROM für die Netzwerkschnittstelle), ist das Einschalten von Wake on LAN im Computer-BIOS oftmals eine wahre Schnitzeljagd.

Aktivitätsmodus im BIOS einschalten

Neben dem Boot-EPROM bzw. der Wake on LAN-tauglichen Netzwerkschnittstelle muss der Computer den sogenannten ACPI-Standard (*Advanced Configuration and Power Interface*) unterstützen, und im BIOS muss der Aktivitätsmodus S3, S4 oder S5 eingeschaltet sein.

ACPI-Aktivitätsmodi	Beschreibung	Leistung
S0	Eingeschalteter Normalzustand, bei dem sich einzelne Komponenten im Stand-by-Modus befinden können.	je nach Energiemodus und Auslastung
S1	Monitor oder LCD wird auf Stromsparen gestellt.	20–200 Watt
S2	Monitor oder LCD wird auf Stromsparen gestellt – zusätzlich ist der Prozessor im Sleep-/Halt-Modus.	20–200 Watt
S3	Suspend-to-RAM (STR): Das Betriebssystem sichert den Systemzustand im Arbeitsspeicher und schaltet dann das Netzteil in den Soft-off-Zustand. Hier beträgt die Aufweckzeit weniger als eine Minute.	2–20 Watt
S4	Suspend-to-Disk (STD): Das Betriebssystem sichert den Systemzustand in eine Datei auf der Festplatte und schaltet dann das Netzteil in den Soft-off-Zustand. Die Aufweckzeit dauert hier länger, der komplette Startvorgang (BIOS, Betriebssystem booten) kann mehrere Minuten dauern.	2–20 Watt
S5	»Normales« Herunterfahren (Soft-off-Zustand). Hier wird der Computer über die Software (das installierte Betriebssystem) heruntergefahren, und das Netzteil wird in den Soft-off-Zustand geschaltet.	0–10 Watt

In der Regel befindet sich der Schalter für Wake on LAN in den *Energie/Power Management Setup*-Einstellungen des Computers. Bei einem PC kontrolliert das *Power Management Setup* die Energiesparfunktionen des Mainboards, der Videoausgabe und der Festplatten.

Hier haben Sie die Möglichkeit, alle Strom führenden Geräte anzupassen, um Strom – sprich bares Geld – zu sparen. Gerade wenn der Rechner rund um die Uhr verfügbar sein soll, ist es sinnvoll, die Energiespareinstellungen zu aktivieren, nicht jedes Gerät muss zu jeder Zeit permanent zur Verfügung stehen.

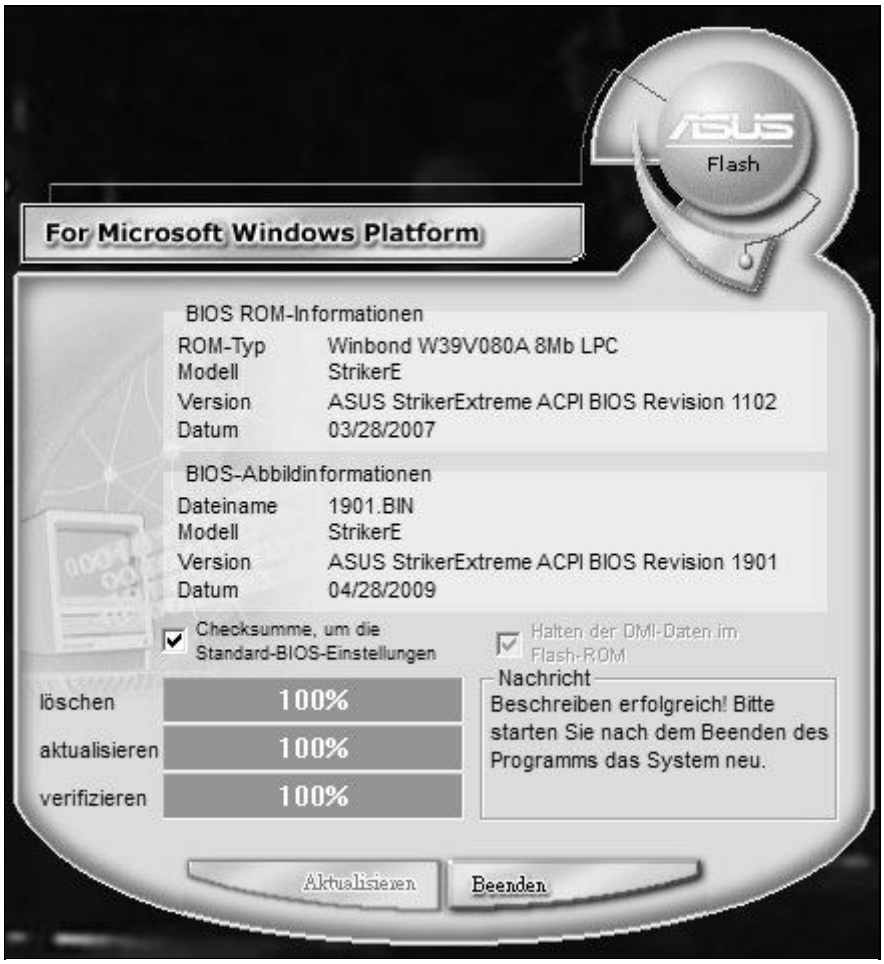


Bild 8.7 Finden Sie im BIOS keinen Eintrag zu Wake on LAN, APM, S3, S4, S5 etc., sollten Sie das BIOS des Computers auf den aktuellen Stand bringen, um diese Funktionen gegebenenfalls nachzurüsten.

Im *Power Management Setup* können Sie alles anpassen, was es im Stromsparbereich zu konfigurieren gibt: Angefangen vom An- und Ausschalten des Rechners bis hin zum Aufwecken von unterschiedlichen Geräten wie Tastatur, Maus, PCI-Karten und anderen können Sie hier nahezu alles detailliert einstellen. Im nachfolgenden Beispiel findet sich die Wake on LAN-Funktion im Bereich *APM Konfiguration* bei *Einschalten per PCI/PCIe*:

```
Phoenix – AwardBIOS CMOS Setup Utility
Energie
APM Konfiguration
Neustart nach Stromausfall[Ausschalten]
PWR Taste <4 Sekunde[Instant-Off]
Einschalten per PCI/PCIe[Aktiviert]
...
```

Standardmäßig ist das Einschalten durch PCI-Geräte deaktiviert. Da die Netzwerkkarte und damit Wake on LAN zu den PCI/PCIe-Komponenten auf einem Mainboard zählt, muss im BIOS der Schalter auf Aktiviert (enabled) umgestellt werden.

Abhängig von Hersteller und BIOS des Rechners können auch folgende Optionen im *Power Management Setup* auftauchen:

Energie/Power Management Setup-Option	Beschreibung
Soft-Off by PWR-BTTN	Ist der Schalter auf *Instant Off* oder *On/Off* eingestellt, schaltet sich der Rechner nach Beendigung des Betriebssystems automatisch ab. Steht hier *Suspend* oder *Delay 4 sec.*, muss der An-/Ausschalter länger als 4 Sekunden gedrückt werden, um den Rechner auszuschalten. Drücken Sie kürzer als 4 Sekunden auf den Schalter, wechselt der Rechner in den Soft-off-Zustand, die aktuelle Arbeitsumgebung bleibt damit erhalten.
Wake-Up by PCI-Card	Mit dieser Option legen Sie fest, welche PCI-Karte den Rechner aus dem Schlafzustand aufweckt, wenn sie (von außen) angesprochen wird. Das ist beispielsweise sinnvoll, wenn Sie mit einer Faxkarte arbeiten.
Wake-Up by LAN	Mit der *Wake-Up by LAN*-Option lässt sich das Aufwecksignal über das LAN (Netzwerk) einstellen, damit der Rechner aus dem Stand-by-Modus aktiviert wird.

USB KB/MS Wakeup From S3	S3 hat nichts mit alten Grafikkarten zu tun, sondern bezeichnet den STR-(*Suspend-to-RAM*-)Modus. Mit aktivierter (*enabled*) Option *USB KB/MS Wakeup From S3* weckt eine Aktivität an einem angeschlossenen USB-Gerät den Rechner aus dem sogenannten S3-Schlafzustand auf.
Resume by Alarm	Kommt ein Anruf am angeschlossenen Modem bei aktiviertem *Resume by Alarm* an, wird der Rechner aus dem Stand-by-/Suspend-Modus geweckt. Ist die Option aktiviert (*enabled*), können Sie Zeit und Datum des gewünschten Monats eingeben. Mit dem Datum 0 wird der Rechner jeden Tag zur gleichen Zeit gestartet.

Je nachdem, wie alt der Rechner und das BIOS sind, steht für die Konfiguration von AGP-/PCI-Steckkarten der *PnP/PCI Configuration*-Dialog zur Verfügung, falls im *Energie/Power Management Setup* keine Wake on LAN- bzw. APM-Schalter vorhanden sind. Ist der Wake on LAN-Schalter im Computer aktiviert, ist noch ein kleiner Eingriff in der FRITZ!Box-Konfiguration notwendig, damit der Computer trotz DHCP seine »feste« IP-Adresse bekommt.

Computer per Wake on LAN einschalten

Trotz DHCP können Sie auch eine IP-Adresse für ein Gerät im heimischen LAN reservieren. Damit erhält das Gerät immer dieselbe IP-Adresse, wenn es auf den DHCP-Server zugreift. Das ist besonders bei Computern nützlich, die mit einer angepassten Portkonfiguration etwa für Fernzugriff, VPN, SSL, Remotedesktop oder dergleichen genutzt werden sollen.

Gerade bei aktivierter Portweiterleitung sorgen permanente IP-Einstellungen für eine geringere Fehlerquote. Hierfür suchen Sie im Menü *Erweiterte Einstellungen/System/Netzwerk* im Register *Geräte und Benutzer* den entsprechenden Computer heraus, der später über Wake on LAN von der FRITZ!Box geweckt werden soll, und klicken im rechten Bereich auf die *Bearbeiten*-Schaltfläche, um zu dem nachstehenden Dialog zu gelangen.

Per Klick auf die *Übernehmen*-Schaltfläche bekommt der ausgewählte Computer zukünftig immer die gleiche IP-Adresse aus dem für die FRITZ!Box festgelegten IP-Bereich. In diesem Dialog ist auch die Schaltfläche *Computer starten* untergebracht, mit der Sie später das ausgewählte Gerät aus der Ferne einschalten können. Die FRITZ!Box erzeugt so ein Wake on LAN-Signal, das zu dem ausgewählten Gerät geschickt und dort ausgewertet wird und dann den Start aus dem Stand-by-Modus veranlasst.

Nun ist die FRITZ!Box für den externen Zugriff eingerichtet, und der Computer lässt sich per Wake on LAN einschalten. Für den Zugriff auf die Benutzeroberfläche des heimischen Computers stehen jetzt zwei Möglichkeiten zur Verfügung:

- Nutzen Sie den direkten, unverschlüsselten Weg via Remotedesktopverbindung, VNC etc., muss ein Mitleser/Eindringling die Benutzeraccount-Kennwort-Kombination kennen. Das ist zumindest besser als gar kein Schutz.
- Noch sicherer und empfehlenswerter ist es, die komplette Verbindung bzw. Remotedesktopverbindung über SSH oder VPN zu tunneln – hier bringt die FRITZ!Box! eigene Bordmittel mit, die Sie auch unbedingt nutzen sollten.

Netzwerkkarteneinstellungen im Geräte-Manager prüfen

Ab Windows XP ist die ACPI-Funktionalität erst richtig im PC angekommen: Hier finden sich unter *Systemsteuerung/Geräte-Manager* bei der Netzwerkkarte bzw. bei den Netzwerkanschlüssen Optionen für Wake on LAN bzw. die Handhabung des sogenannten *Magic Packet*, mit dem ein schlafender PC aus dem Dämmerschlaf geholt werden kann.

Zunächst prüfen Sie, ob im Register *Erweitert* des genutzten Netzwerkadapters im Feld *Eigenschaft* die Option *Aktivierung durch Magic Packet* existiert. Ist das der Fall, schauen Sie, ob der Wert auf *Aktiviert* eingestellt ist – falls nicht, holen Sie das jetzt nach.

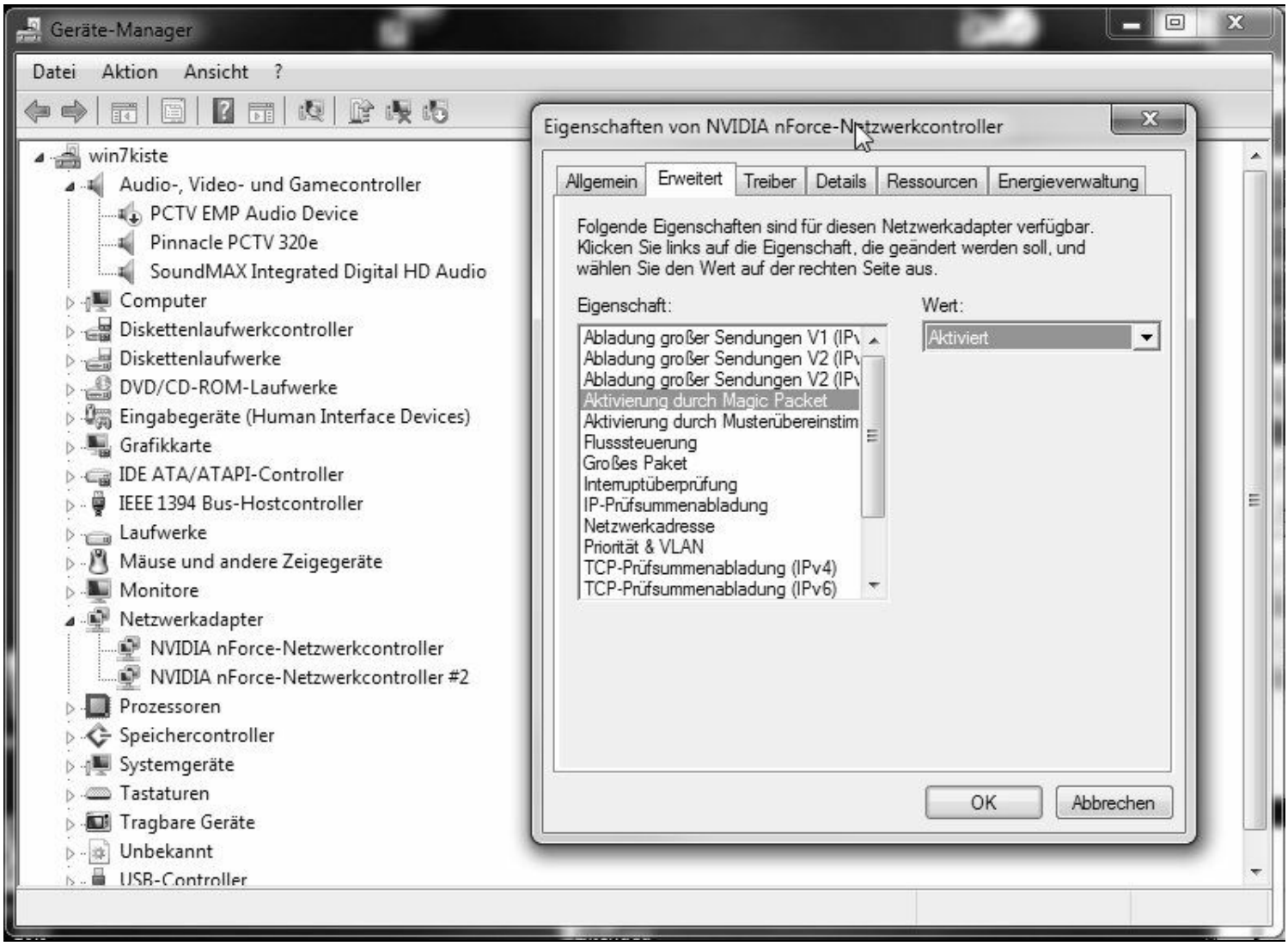


Bild 8.8 Sind mehrere Netzwerkadapter im *Geräte-Manager* zu sehen, schalten Sie am besten bei beiden Schnittstellen Wake on LAN ein.

Die zweite Anlaufstelle ist im gleichen *Eigenschaften*-Dialog das Register *Energieverwaltung* (bei älteren Windows-Versionen auch *Energieoptionen* genannt). Hier sollten sämtliche Häkchen – wie im nachstehenden Dialog zu sehen – gesetzt sein. Anschließend sollte der PC zumindest für die Modi S3 (*Suspend-to-RAM*, Windows: Stand-by) und S4 (*Suspend-to-Disk*, Windows: Ruhezustand) Wake on LAN-tauglich sein.

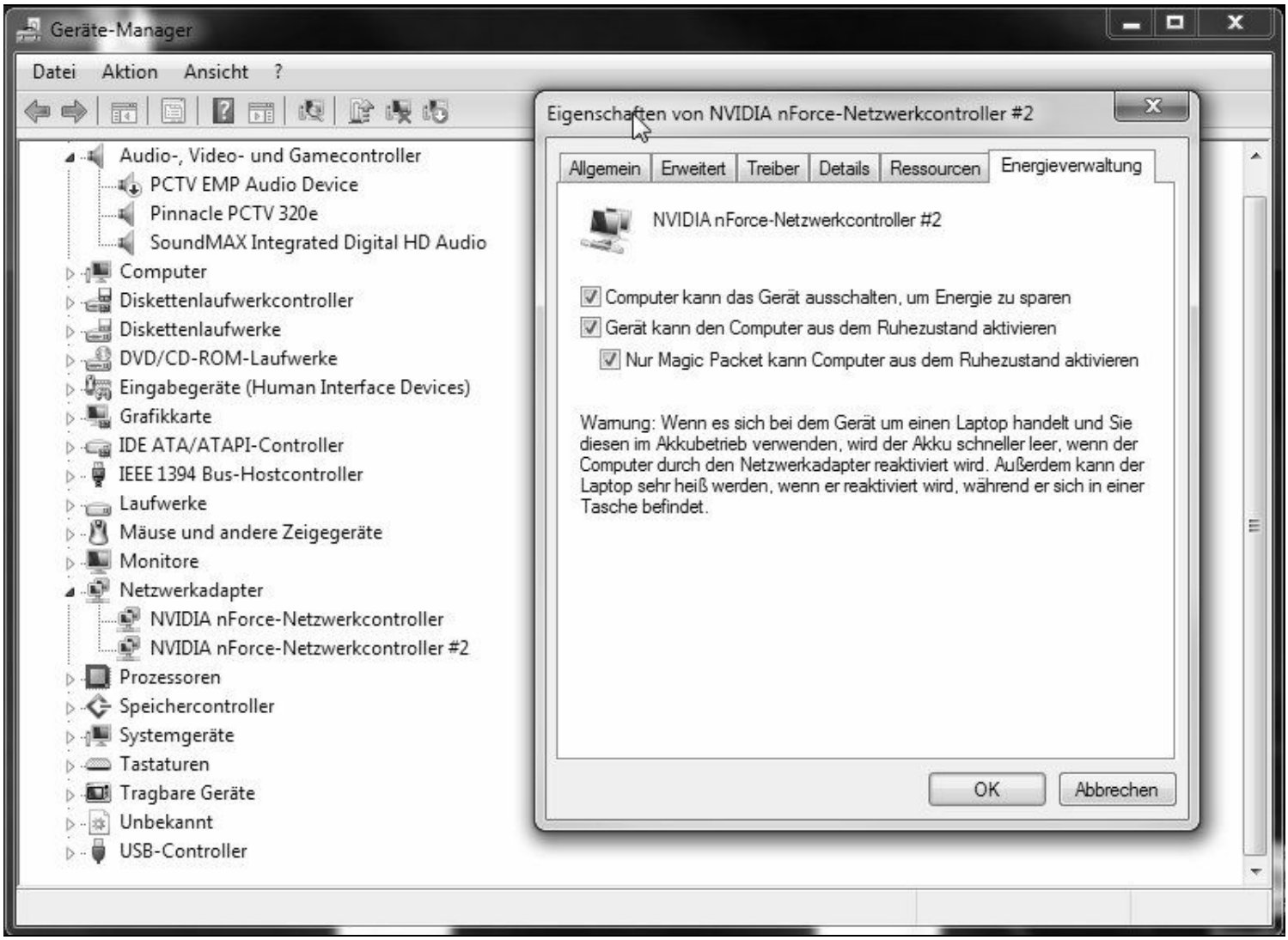


Bild 8.9 Im Register *Energieverwaltung* setzen Sie sämtliche Häkchen, um die ACPI-Steuerung zu aktivieren.

Gerade bei älteren Netzwerkkarten bzw. Mainboards mit älteren Onboard-Schnittstellen verweigert Windows bzw. der PC das Aufwecken im ACPI-Modus S5 (*Soft-Off*) – hier bleibt der Rechner bei gesendetem Magic Packet häufig ausgeschaltet. Warum das so ist, erfahren Sie, wenn Sie weiterlesen.

Stand-by oder Soft-off? Das ist die Preisfrage. Manchmal kommt es nämlich vor, dass das BIOS das Aufwecken des Computers aus dem Soft-off-Zustand erlaubt, aber in der Praxis funktioniert das Wake on LAN ausschließlich dann, wenn der PC in den Stand-by-Modus gebracht worden ist – in Windows über Start/Herunterfahren/Energie sparen. Ob die eingebaute bzw. in den meisten Fällen die Onboard-Netzwerkkarte auch sämtliche Wake on LAN- bzw. ACPI-Modi unterstützt, finden Sie unter Windows 7 über den *Eigenschaften*-Dialog der Netzwerkverbindung heraus. Nicht alle Mainboards bzw. Netzwerkkarten unterstützen sämtliche ACPI-Modi. Manche unterstützen nur den Stand-by-Modus, andere zusätzlich auch den Ruhezustand.

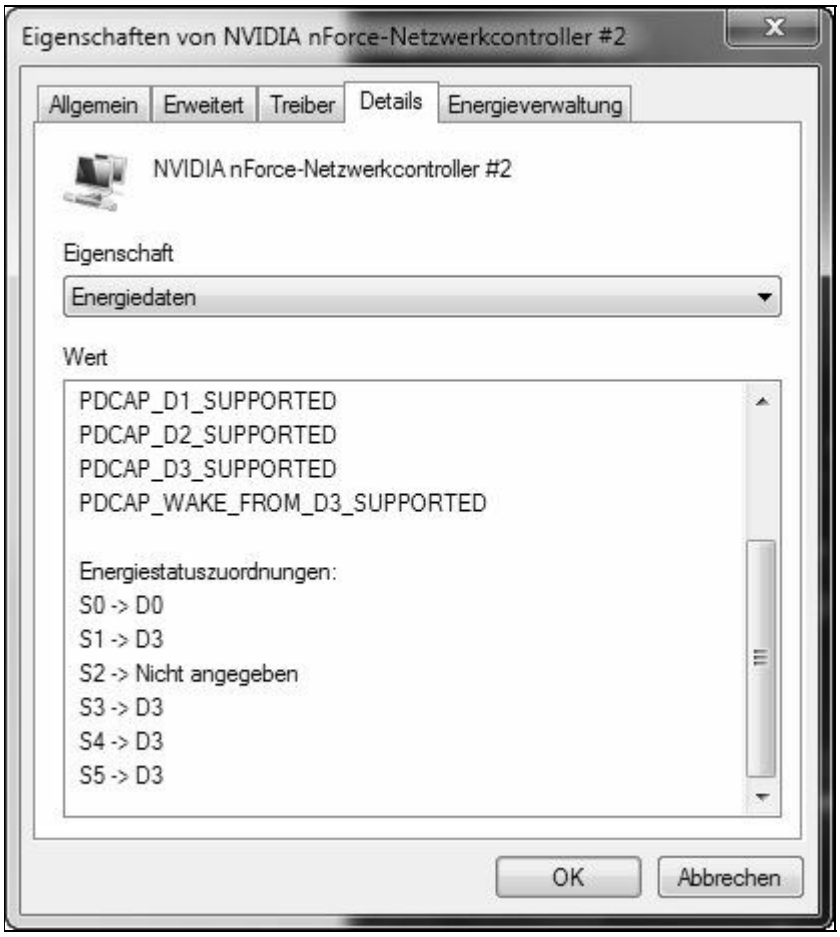


Bild 8.10 Hier wählen Sie im Register *Details* den Eintrag *Energiedaten*, um den Funktionen der Netzwerkkarte in Sachen Wake on LAN auf den Zahn zu fühlen.

Bei älteren Windows-Versionen ist der *Energiedaten*-Eintrag in *Energiekapazität* und *Energiestatuszuordnungen* aufgeteilt. Im Fall des gezeigten Zustands unterstützt die Netzwerkschnittstelle mit der Zuordnung *PDCAP_WAKE_FROM_D3_SUPPORTED* alle drei ACPI-Modi: S3 (*Suspend-to-RAM*, Betriebszustand wird in den RAM geschrieben), S4 (*Suspend-to-Disk*, Betriebszustand wird auf die Festplatte geschrieben) und S5 (*Soft-Off*, Herunterfahren des PCs). Alternativ können Sie auch über ein DOS-Fenster mit dem Befehl:

```
powercfg /devicequery wake_armed
```

herausfinden, welche Geräte gerade so eingerichtet sind, dass sie den Computer aus dem Stand-by-Modus reaktivieren dürfen.

```
powercfg /devicequery S4_supported
```

listet hingegen die Geräte, die den Ruhezustand unterstützen, auf. Grundsätzlich lassen sich mit dem Werkzeug ***Powercfg.exe*** die Energieeinstellungen des Computers einrichten sowie die Modi für Ruhezustand und Stand-by nach Wunsch festlegen.

8.2 Zugriff auf das Heimnetz mit VPN

Mit einem VPN (Virtual Private Network) können Benutzer von unterwegs einfach und sicher über das Internet auf das heimische Netzwerk zugreifen. Hier werden die zu übertragenden Daten beim Sender verschlüsselt, über einen sogenannten Tunnel sicher über das öffentliche Internet zum Empfänger geschickt und anschließend entschlüsselt. Durch das »Tunneling« wird sichergestellt, dass die Daten weder mitgelesen noch manipuliert werden können. Damit können Sie beispielsweise vom PC im Urlaubshotel Bilder der Digitalkamera auf Ihre heimische Festplatte sichern, beliebige Daten von zu Hause herunterladen und vieles mehr.

Je nach Modell des DSL-WLAN-Routers ist die VPN-Technik bereits im DSL-WLAN-Router integriert und macht das Einrichten einer VPN-Verbindung nahezu kinderleicht. Trotzdem lauern Gefahren. Da der Datenverkehr im Internet im

Allgemeinen ungesichert abläuft, muss dafür gesorgt werden, dass nicht jeder die Verbindungsdaten mitlesen oder gar manipulieren kann.

Hier setzt VPN an und verschlüsselt den Datenstrom zwischen den beiden Teilnehmern. Zusätzlich autorisieren sich beide Gegenstellen vor dem Verbindungsaufbau, damit sich kein unbefugter Teilnehmer einfach so mal einklinkt. Für die Verschlüsselung der Verbindung bietet die VPN-Technik mehrere Möglichkeiten, am weitesten verbreitet ist der IPSec -Standard, der auch in den meisten VPN-tauglichen DSL-WLAN-Routern implementiert ist.

Benutzerfernzugang oder Koppeln eines entfernten Netzwerks?

Grundsätzlich wird beim Einrichten einer VPN-Verbindung zwischen dem Benutzerfernzugang und der Kopplung entfernter Netzwerke unterschieden. Bei dem benutzerbasierten VPN-Zugang verbindet sich ein Benutzer aus dem Internet mit seinem Notebook oder einem PC im Internetcafé via VPN mit dem Heimnetzwerk. Hier initiiert der entfernte Client die VPN-Verbindung, anschließend wird ihn eine IP-Adresse aus dem Heimnetz zugewiesen, um einen Datenaustausch zu ermöglichen.

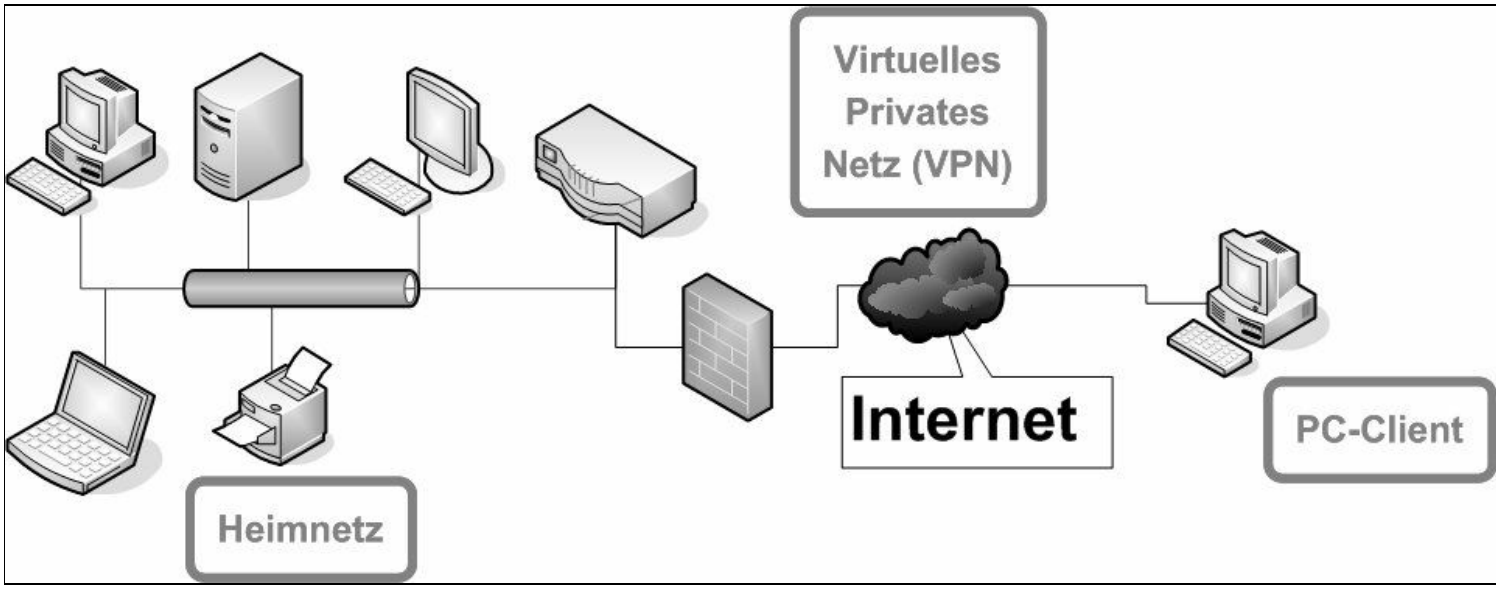


Bild 8.11 Bei einer aktiven VPN-Verbindung arbeitet der PC-Client so, als wäre er direkt mit dem Heimnetz verbunden. Hier kann der Benutzer auf Dateifreigaben oder NAS-Festplatteninhalte zugreifen.

Neben dem benutzerbasierten Zugriff lässt die VPN-Technik auch die Kopplung zweier Netze über das Internet zu. Damit lassen sich zwei Netzwerke zu einem gemeinsamen »Heimnetzwerk« vereinigen. In der Praxis kommt das vorwiegend im Unternehmensbereich zum Einsatz, etwa wenn ein Unternehmen einen räumlich getrennten Standort in das Unternehmensnetzwerk integrieren möchte. Bei der Kopplung von Netzwerken über VPN kann der Verbindungsaufbau von beiden Seiten erfolgen – hier ist auch kein Software-VPN-Client auf dem PC/Mac notwendig, da diese Aufgabe auf beiden Seiten der VPN-taugliche DSL-Router oder Switch übernimmt.

Diese Technik können Sie sich gerade im Zeitalter des Breitbandanschlusses zunutze machen: So ist es mit verhältnismäßig wenig Aufwand möglich, mit Freunden ein gemeinsames Netzwerk aufzubauen, ohne dass die eigentliche Verbindung dank der VPN-Sicherheit irgendwelchen Gefahren ausgesetzt ist.

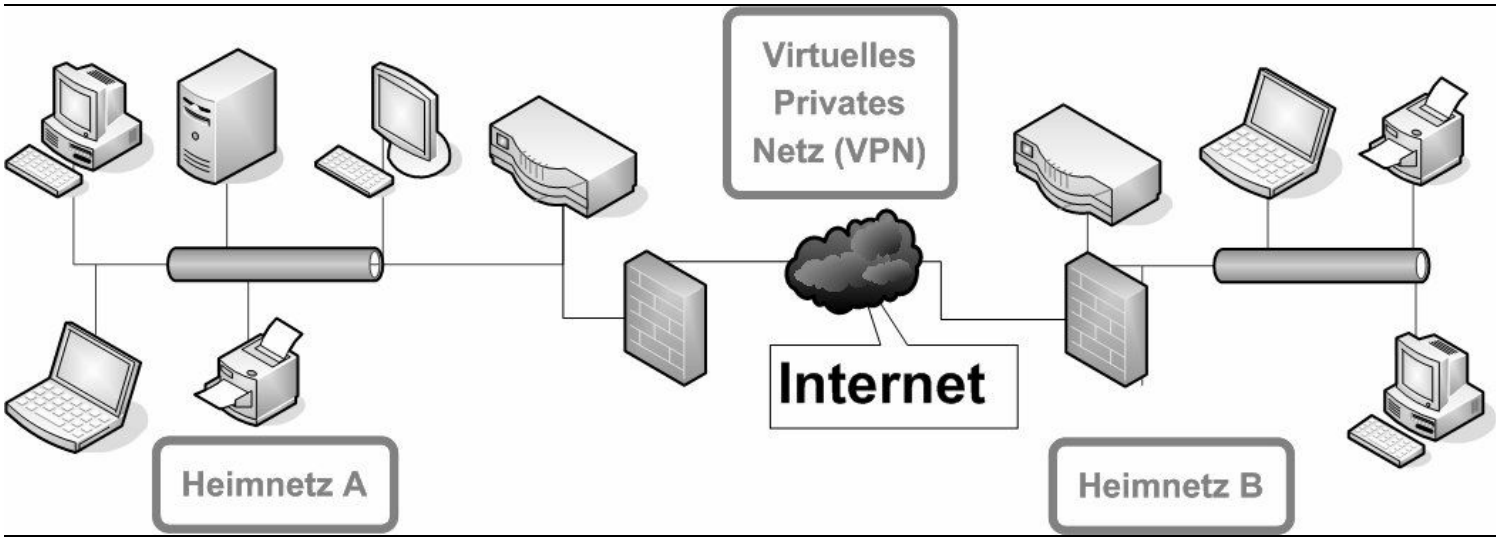


Bild 8.12 Sind zwei Netzwerke miteinander verbunden, können sämtliche Geräte aus Heimnetz A auf alle Geräte in Heimnetz B zugreifen. Damit lassen sich – abhängig von der DSL-Up- und -Downstream-Geschwindigkeit – Daten hin- und hertransferieren, gemeinsame Musik- und Videobestände nutzen und vieles mehr.

Bei einer VPN-Verbindung wird also das private Heimnetz mit einem anderen Netzwerk oder/und mit einem VPN-Client über das Internet verbunden. Damit eine VPN-Verbindung aufgebaut werden kann, braucht der VPN-Client bzw. die VPN-Gegenstelle des entfernten Netzwerks die passenden IP-Informationen des Heimnetzes. Ist eine VPN-Verbindung erfolgreich hergestellt, ist darüber jede IP-basierte Anwendung wie sicherer E-Mail-Abruf, Zugriff auf vertrauliche Daten im Heimnetz, Fernwartung und vieles mehr möglich.

So testen Sie mit der FRITZ!Box Ihren DSL-Anschluss

Da bei einer VPN-Verbindung in der Regel ein höheres Datenaufkommen entsteht, sollten auch aus Performancegründen auf beiden Seiten schnelle Internetzugänge zur Verfügung stehen. Der Knackpunkt ist hier der Datendurchsatz. Trotz 16er-DSL-Anschlüssen und schneller ist die Upload-Geschwindigkeit das Nadelöhr: Je nach Anbieter und Zugang ist bei manchen Anbietern sogar schon bei 384 KBit/s Schluss.

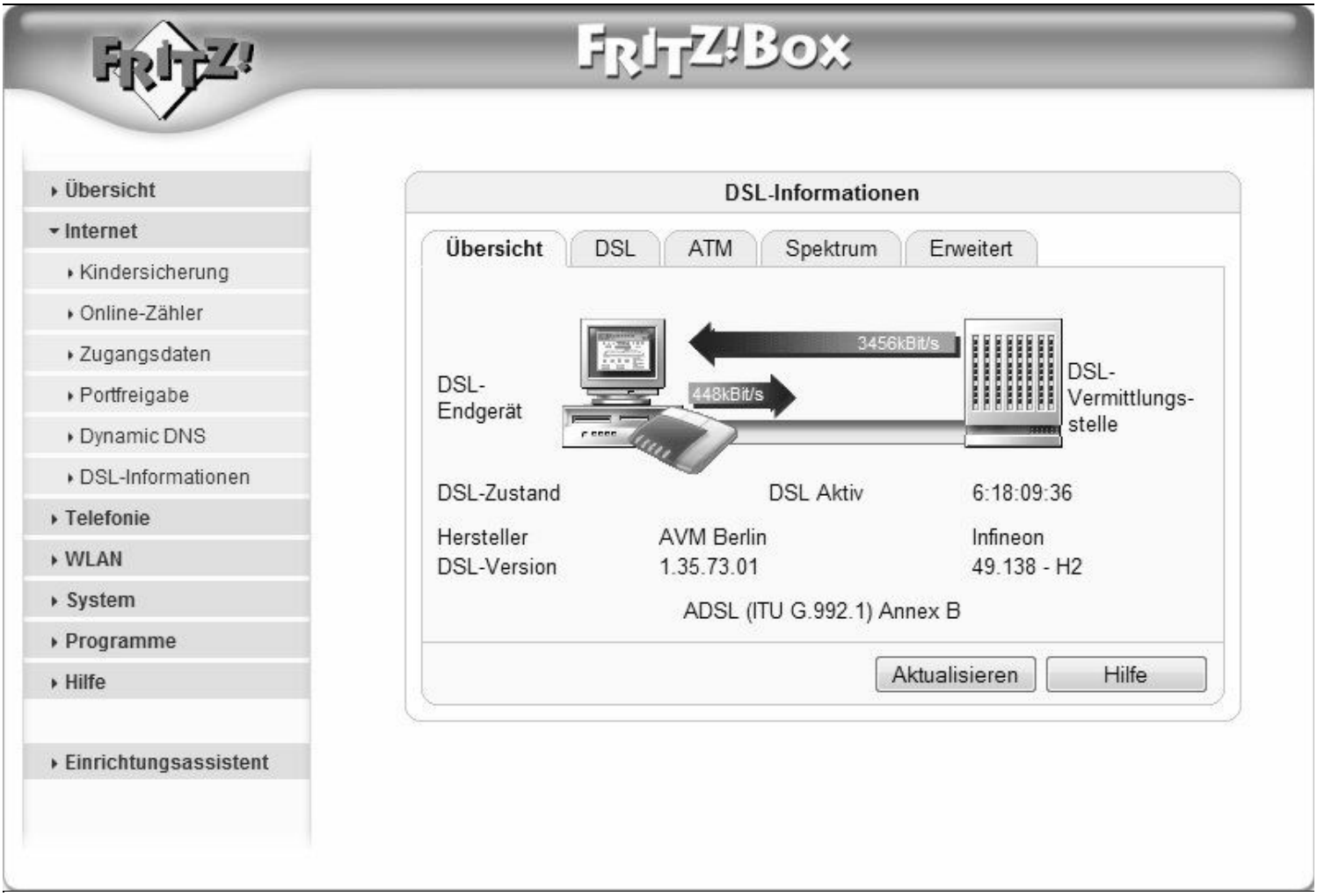


Bild 8.13 Jeder DSL-Router zeigt die Verbindungsdaten und die Geschwindigkeit zur Vermittlungsstelle in seinem Konfigurationsmenü an.

Bei einem DSL-Anschluss mit 16 MBit (Download) bieten die meisten Anbieter eine Upload-Geschwindigkeit von 1 MBit/s – die Praxiswerte schwanken jedoch stark. Wie schnell Ihr DSL-Anschluss tatsächlich ist, lässt sich mithilfe diverser Testseiten im Internet überprüfen.

Lesezeichen

http://bit.ly/1laF3x
Mit dieser URL rufen Sie den DSL Speedtest auf.

Geben Sie nach dem Aufruf der Seite den Namen Ihres Providers, die angegebene Geschwindigkeit sowie die Postleitzahl ein und klicken Sie auf die Speedtest jetzt starten-Schaltfläche.

Nach rund einer Minute haben Sie Auskunft darüber, ob der DSL-Zugang das leistet, was er verspricht. Liegt die Upload-Geschwindigkeit des DSL-Anschlusses im Bereich um 500 KBit/s – je mehr, desto besser –, läuft auch die Geschwindigkeit des VPN-Zugriffs zumindest zufriedenstellend ab. Damit lässt sich einigermaßen arbeiten, doch möchten Sie beispielsweise GByte-große Dateien aus Ihrem Heimnetz herunterladen, bleibt die DSL-Upload-Geschwindigkeit Ihres DSL-Anschlusses der limitierende Faktor.

Bild 8.14 Zu gering! Für einen 6.000er-Anschluss ist das Testergebnis ernüchternd. Hier sorgt eventuell ein Anruf bei der Provider-Hotline für Abhilfe.

Voraussetzungen für den VPN-Verbindungsaufbau

Neben der ausreichenden Bandbreite müssen die beiden Kommunikationspartner einen unterschiedlichen privaten IP-Adressbereich verwenden, da sonst nach dem VPN-Verbindungsaufbau keine eindeutige Adresszuordnung möglich wäre. Gäbe es in beiden Netzen ein Gerät mit der Beispiel-IP-Adresse 192.168.123.22, wäre beim Datenaustausch via VPN-Tunnel nicht klar, ob das Gerät in Heimnetz A oder Heimnetz B adressiert werden soll. Ebenso scheitert ein Datenaustausch mit einem Gerät im gemeinsamen Heimnetz, falls mit diesem über eine VPN-Verbindung kommuniziert werden soll, da hier die Zieladresse immer direkt und nicht über das Gateway angesprochen wird.

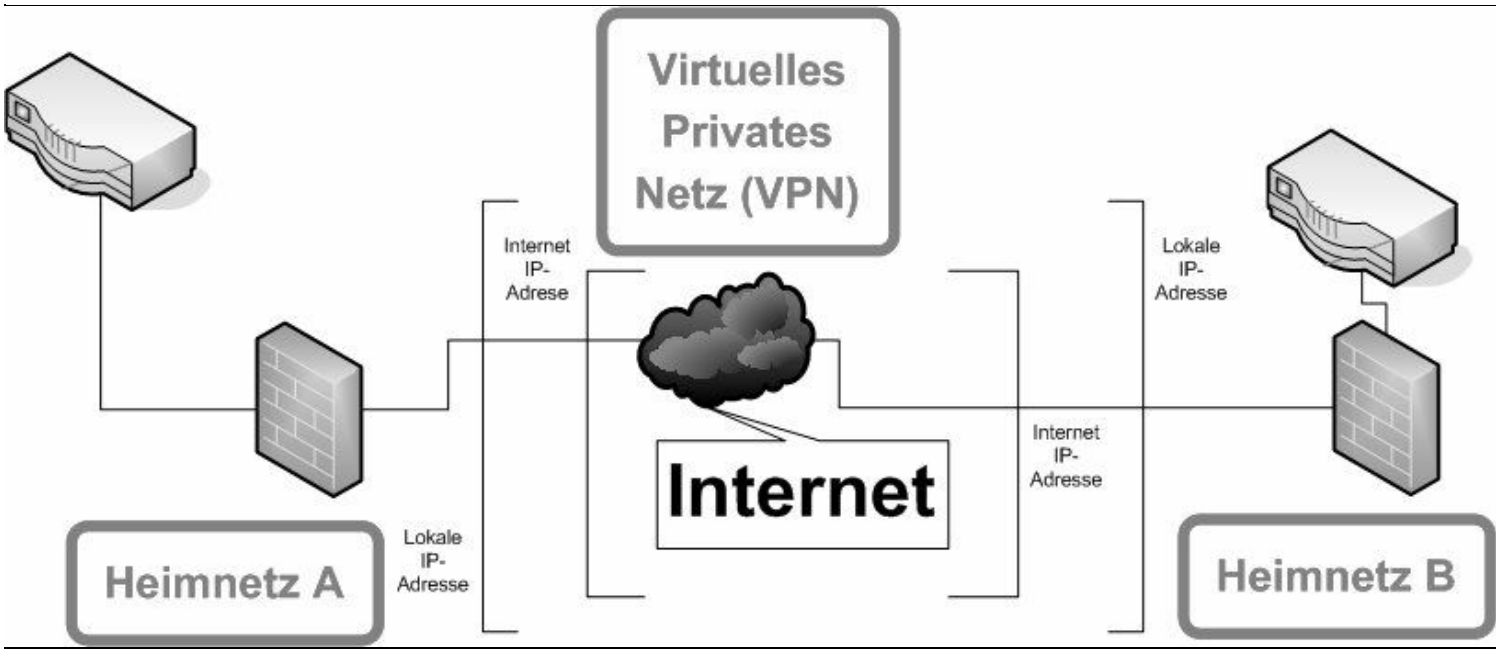


Bild 8.15 Bei einer VPN-Verbindung kommen sowohl öffentliche als auch lokale IP-Adressen zum Einsatz. Das VPN-Netzwerk wird mit öffentlichen Internet-IP-Adressen verbunden.

Um eine VPN-Verbindung aufzubauen, sind grundsätzlich vier IP-Adressen notwendig – die beiden öffentlichen Internet-IP-Adressen der Teilnehmer sowie die privaten Adressen der Netze (oder des VPN-Clients des Benutzers), die mit dem VPN miteinander gekoppelt werden. Da in der Regel die öffentlichen IP-Adressen dynamisch sind, also häufiger wechseln, erfolgt der Verbindungsaufbau nicht mit der öffentlichen IP-Adresse, sondern mit einer statischen IP-Adresse, deren Daten über einen DNS-Anbieter zur Verfügung gestellt werden können.

8.3 Konfiguration der VPN-Verbindung

Um von unterwegs über VPN auf das Heimnetz zuzugreifen, werden ein VPN-tauglicher DSL-WLAN-Router sowie ein spezieller Software-VPN-Client auf dem Notebook, Mac oder PC benötigt. Egal welches VPN-Verfahren bzw. Protokoll (PPTP, L2TP, IPsec, SSL etc.) eingesetzt wird, beide Kommunikationspartner müssen dasselbe verwenden, damit eine Verbindung zustande kommt. In den meisten SOHO-Lösungen ist das IPSec-Protokoll implementiert, das dazugehörige Schlüsselprotokoll ISAKMP/IKE sorgt für die eigentliche Verschlüsselung der Verbindung.

In diesem Abschnitt wird die Konfiguration einer VPN-Verbindung von einem entfernten PC und Mac zu einer VPN-tauglichen FRITZ!Box erklärt. Grundsätzlich sind hier folgende Arbeitsschritte notwendig:

- Erstellen der Konfigurationsdatei für die FRITZ!Box.
- Erstellen der Konfigurationsdatei für den benutzerbasierten Zugang.
- Importieren der Konfigurationsdatei in die FRITZ!Box.
- Gegebenenfalls Installation eines VPN-Clients und Konfiguration des VPN-Clients anhand der FRITZ!Box-Konfigurationsdatei.

Bei der Kopplung zweier Netze entfällt der letzte Schritt, hier wird einfach auf beiden Seiten die Konfigurationsdatei eingespielt.

So erstellen Sie die VPN-Config-Datei für den FRITZ!Box

Die FRITZ!Box erhält ihre VPN-Konfiguration über eine sogenannte Config-Datei, in der die wichtigsten Parameter für die Verbindung abgelegt sind. Um Tipp- und Syntaxfehler auszuschließen, stellt AVM einen Assistenten mit der Bezeichnung FRITZ!Box-Fernzugang einrichten für die Erzeugung der Config-Dateien zur Verfügung, der auf dem AVM-Webserver zum Download bereitsteht.

Lesezeichen

http://bit.ly/9gFu5L

FRITZ!Box-Fernzugang einrichten: Dies ist der Download-Link des Assistenten.

Bevor Sie loslegen, sollten Sie jedoch nachstehende Informationen für die VPN-Konfiguration parat haben. Fehlt auch nur eine Kleinigkeit, wird die VPN-Verbindung scheitern. Am besten tragen Sie Ihre Daten in nachstehende Tabelle ein:

Information	Beispiel	Ihre Daten
Benutzername	ihremail@adresse.de	
Dynamischer DNS-Name oder öffentliche IP-Adresse	ihrdnsname.homedns.org	
Dynamischer DNS-Benutzername	ihrdnsname	
Dynamisches DNS-Passwort	password	
IP-Netz zu Hause	192.168.123.0	_____._____._____.0
Subnetzmaske	255.255.255.0	255._____._____._____

1. Nach dem Download und der Installation starten Sie das Programm. Wer mit einer Einwahlverbindung bzw. einer wechselnden öffentlichen IP-Adresse im Internet unterwegs ist, braucht eine dynamische DNS-Adresse bei einem FreeDNS-Anbieter. Profiuser mit fester IP-Adresse können stattdessen diese nutzen. Den Dynamic DNS-Account richten Sie unter *Erweiterte Einstellungen/Internet/Fernzugang/Dynamic DNS* ein. Starten Sie das Programm

FRITZ!Box-Fernzugang einrichten und klicken Sie auf die Schaltfläche *Neu*.

Bild 8.16 Spartanisch: Nach dem Start des Assistenten klicken Sie auf die Schaltfläche *Neu*.

2. Es meldet sich ein Assistent, der Ihnen drei Optionen zu Auswahl anbietet. Wählen Sie die Option *Fernzugang für einen Benutzer einrichten* aus und klicken Sie auf *Weiter*.

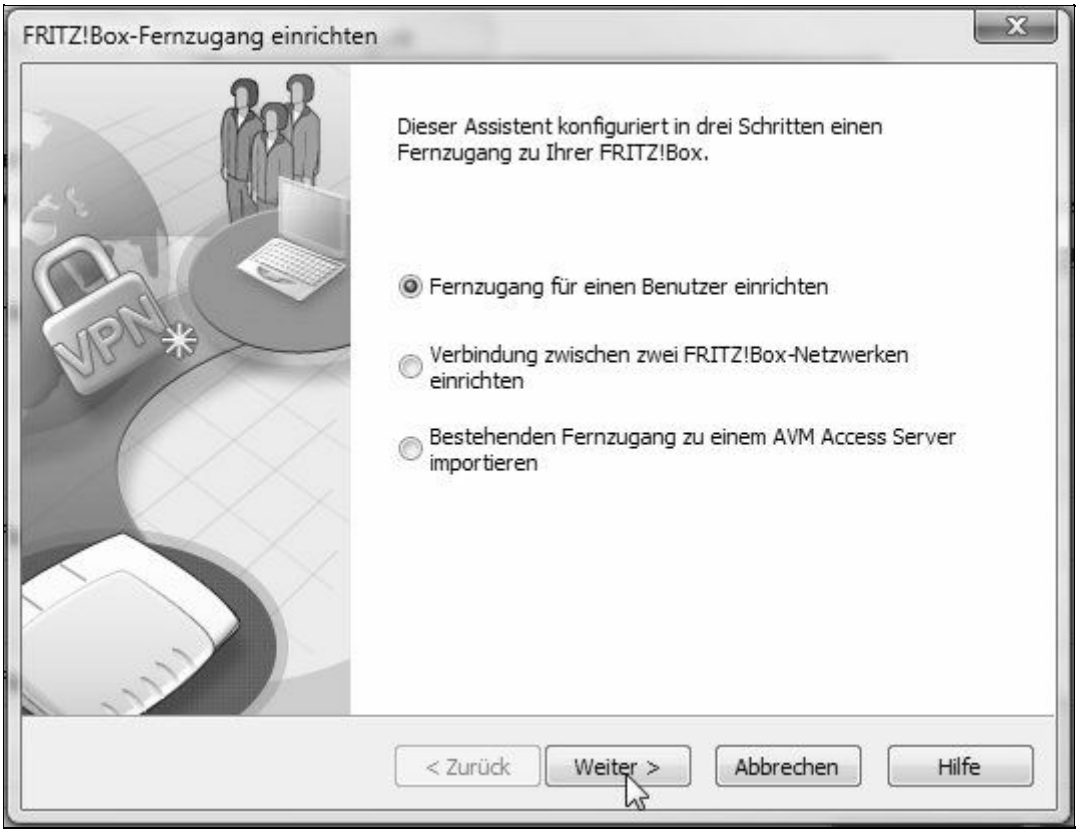


Bild 8.17 Abhängig davon, welche Art der VPN-Verbindung erstellt werden soll, wählen Sie hier die entsprechende Option aus. Bei der Kopplung zweier Heimnetze ist die zweite Option die richtige – für den benutzerspezifischen VPN-Zugang zum Heimnetz ist *Fernzugang für einen Benutzer einrichten* auszuwählen.

3. Tragen Sie in das Eingabefeld *E-Mail-Adresse des Benutzers* die E-Mail-Adresse des Users ein. Das ist der Benutzername – es braucht nicht unbedingt eine E-Mail-Adresse zu sein, auch ein beliebiger Benutzername lässt sich verwenden. Das entsprechende Passwort zu diesem Benutzernamen erzeugt der Assistent automatisch.

Bild 8.18 In diesen Dialog tragen Sie E-Mail oder Benutzername ein und klicken anschließend auf die *Weiter*-Schaltfläche.

4. Im nächsten Dialog tragen Sie in das Eingabefeld *Name* den in der FRITZ!Box konfigurierten dynamischen DNS-Domainnamen ein. Alternativ kann hier eine IP-Adresse eingetragen werden. Profiuser mit fester öffentlicher IP-Adresse zu Hause brauchen den Umweg über den dynamischen DNS-Namen nicht zu gehen.

Bild 8.19 Nach dem Eintragen des FRITZ!Box-Namens und der IP-Adresse oder des dynamischen DNS-Namens klicken Sie auf die *Weiter*-Schaltfläche, um zum nächsten Konfigurationsschritt zu gelangen.

5. Falls die FRITZ!Box im Heimnetz die Standardkonfiguration für den IP-Adressbereich verwendet, nutzen Sie die Option *Werkseinstellungen der FRITZ!Box für das IP-Netzwerk übernehmen*. In diesem Fall stellt die FRITZ!Box den Adressbereich 192.168.178.0 für die Geräte im Heimnetz zur Verfügung.

Wer hingegen den IP-Adressbereich nach seinen persönlichen Wünschen konfiguriert hat, wählt die Option *Anderes IP-Netzwerk verwenden* und trägt das IP-Netzwerk sowie die Subnetzmaske ein.

Anschließend geben Sie die IP-Adresse ein, die der Computer beim VPN-Verbindungsaufbau erhalten soll. Achten Sie darauf, dass die IP-Adresse nicht bereits von irgendeinem Gerät in Ihrem Heimnetz verwendet wird, damit es nicht zu Verwechslungen und damit IP-Adresskonfikten kommt.

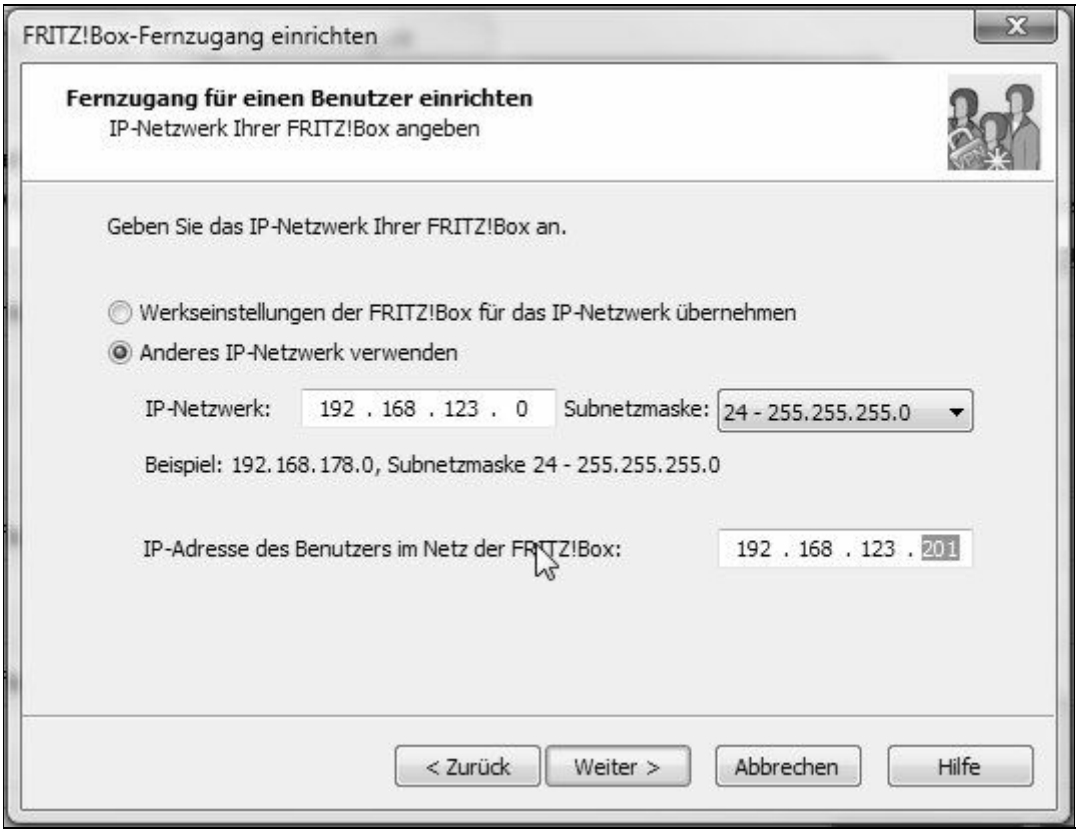


Bild 8.20 Nach dem Klick auf die *Weiter*-Schaltfläche erzeugt der Assistent die Konfigurationsdatei für die FRITZ!Box.

6. Jetzt erzeugt der Assistent die Konfigurationsdateien für die FRITZ!Box und den Benutzerzugang, was einen kleinen Moment dauert. Im nächsten Dialog können Sie auswählen, was mit den erstellten Konfigurationsdateien als Nächstes passieren soll.

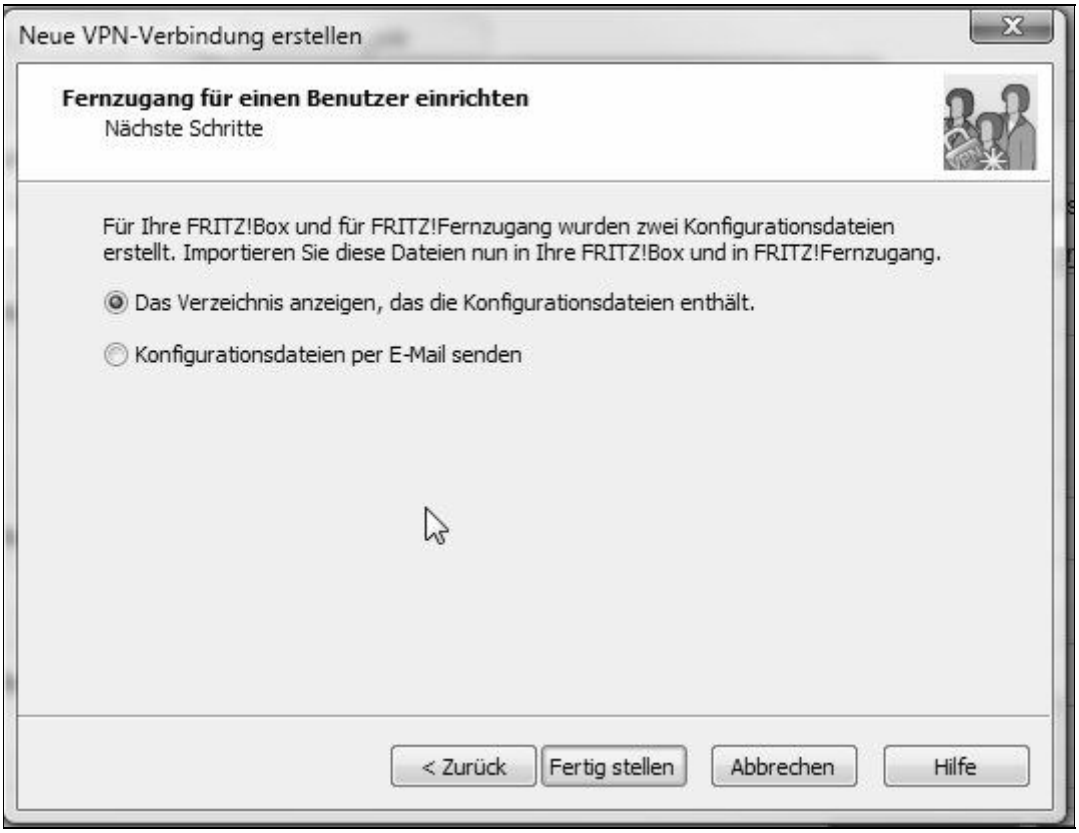


Bild 8.21 Völlig ausreichend: Lassen Sie sich einfach das Verzeichnis anzeigen, in dem der FRITZ!Box-Assistent die Konfigurationsdateien abgelegt hat.

7. Um die Einstellungen besser zu verstehen, sind hier die relevanten Bereiche der beiden erstellten Beispieldateien abgedruckt. In der benutzerspezifischen Konfigurationsdatei *vpnuser.cfg* ist im Bereich *targets* unter *name/remotehostname* der dynamische DNS-Name (hier: *ihrdnsname.homedns.org*) eingetragen. Weiterhin sind der Benutzername (*user_fqdn*) sowie das verschlüsselte Passwort (*key*) für den Verbindungsaufbau wichtig, diese Informationen brauchen Sie immer, auch wenn ein alternativer VPN-Client für den Zugriff verwendet wird.

```
targets {
        policies {
                name = "ihrdnsname.homedns.org";
                connect_on_channelup = no;
                always_renew = no;
                reject_not_encrypted = no;
                dont_filter_netbios = yes;
                localip = 0.0.0.0;
                virtualip = 192.168.123.201;
                remoteip = 0.0.0.0;
                remotehostname = "ihrdnsname.homedns.org";
                localid {
                        user_fqdn = "ihremail@adresse.de";
                }
                mode = mode_aggressive;
                phase1ss = "all/all/all";
                keytype = keytype_pre_shared;
                key = "9bdde4d6K83ki17b3Uc3dd2_0316d7e0e8";
                cert_do_server_auth = no;
                use_nat_t = no;
                use_xauth = no;
                use_cfgmode = no;
                phase2ss = "esp-all-all/ah-none/comp-all/pfs";
                accesslist = "permit ip any 192.168.123.0 255.255.255.0";
                wakeupremote = no;
        }
}
```

Bild 8.22 Bei der benutzerbasierten Konfigurationsdatei sind der dynamische DNS-Name bei *remotehostname* sowie die IP-Adressparameter bei *virtualip* und *accesslist* zunächst das A und O, um die VPN-Verbindung erfolgreich aufbauen zu können.

Unter *accesslist* (Zugriffsregel) ist das IP-Netz angegeben, auf das per VPN zugegriffen werden darf. In diesem Fall hat das entfernte Netz den Bereich *192.168.123.0/24*. Bei Bedarf kann diese Liste durch ein Komma getrennt erweitert werden – das ist jedoch in der Regel nicht notwendig. Wer den Zugriff auf einen einzelnen Fileserver beschränken möchte, kann das ebenfalls hier tun – statt des Netzwerks lässt sich eine einzelne Hostadresse eintragen.

fritzbox.cfg

```
vpncfg {
        connections {
                enabled = yes;
                conn_type = conntype_user;
                name = "ihremail@adresse.de";
                always_renew = no;
                reject_not_encrypted = no;
                dont_filter_netbios = yes;
                localip = 0.0.0.0;
                local_virtualip = 0.0.0.0;
                remoteip = 0.0.0.0;
                remote_virtualip = 192.168.123.201;
                remoteid {
                        user_fqdn = "ihremail@adresse.de";
                }
                mode = phase1_mode_aggressive;
                phase1ss = "all/all/all";
                keytype = connkeytype_pre_shared;
                key = "9bdde4d6K83ki17b3Uc3dd2_0316d7e0e8";
                cert_do_server_auth = no;
                use_nat_t = no;
                use_xauth = no;
                use_cfgmode = no;
                phase2ss = "esp-all-all/ah-none/comp-all/pfs";
                accesslist =
                        "permit ip 192.168.123.0 255.255.255.0 192.168.123.201 255.255.255.255";
        }
        ike_forward_rules = "udp 0.0.0.0:500 0.0.0.0:500",
                            "udp 0.0.0.0:4500 0.0.0.0:4500";
}


// EOF
```

Bild 8.23 Der *key* (das Kennwort) wird vom *FRITZ!Box-Fernzugang einrichten*-Assistenten automatisch generiert und verschlüsselt. Wer möchte, kann händisch nachbessern.

Bei *remote_virtualip* ist die IP-Adresse angegeben, die der Client nach dem Abarbeiten der VPN-Sicherheitsparameter zugewiesen bekommt. Wer nachträglich die IP-Adresse verändern möchte, passt hier diesen Eintrag an und importiert die Konfigurationsdatei *fritzbox.cfg* erneut in die FRITZ!Box, um dieser die Änderung bekannt zu machen.

So übertragen Sie die VPN-Konfiguration in die FRITZ!Box

Die FRITZ!Box lässt bis zu fünf gleichzeitige VPN-Verbindungen zu. Für jede Verbindung wird unter Umständen eine eigene Konfigurationsdatei benötigt. Um die erzeugte Konfigurationsdatei *fritzbox.cfg* in die FRITZ!Box zu übertragen, öffnen Sie zunächst über den Webbrowser die Benutzeroberfläche der FRITZ!Box. Dort gehen Sie über *Erweiterte Einstellungen/Internet/Freigaben* in das Register *VPN*. Mithilfe der *Durchsuchen*-Schaltfläche ist zunächst die entsprechende *fritzbox.cfg*-Konfigurationsdatei auszuwählen.

Bild 8.24 Klicken Sie auf die Schaltfläche *VPN-Einstellungen importieren* und anschließend auf die *OK*-Schaltfläche.

Die Konfigurationsdateien für die VPN-Verbindung befinden sich bei Windows Vista und Windows 7 hier:

```
%USERPROFILE%\AppData\Roaming\AVM\FRITZ!Fernzugang\
```

und bei Windows XP in diesem Verzeichnis:

```
%USERPROFILE%\Anwendungsdaten\AVM\FRITZ!Fernzugang\
```

Dort ist ein Verzeichnis mit dem gleichen Namen wie der von Ihnen gewählte dynamische DNS-Domainname sowie die Konfigurationsdatei *fritzbox.cfg* für die FRITZ!Box zu finden.

Bild 8.25 Nach dem erfolgreichen Import der Konfigurationsdatei ist die FRITZ!Box bereit, VPN-Verbindungen mit dem entfernten Benutzer aufzubauen.

Im nächsten Abschnitt wird der Zugriff vonseiten des entfernten Benutzers eingerichtet. Für Windows-Anwender stellt AVM einen speziellen Client zur Verfügung, der, wie im nächsten Abschnitt beschrieben, installiert und mithilfe der Konfigurationsdatei eingerichtet wird.

So richten Sie den Zugriff seitens des entfernten Benutzers ein

1. Ist das kostenlose Programm *FRITZ!Fernzugang* von AVM (www.avm.de) heruntergeladen und installiert, benötigen Sie zunächst die Konfigurationsdatei *vpnuser.cfg*, in der sämtliche notwendigen Verbindungsinformationen für den VPN-Zugriff enthalten sind. Die *vpnuser.cfg* befindet sich bei Windows Vista und Windows 7 im Verzeichnis:

   ```
   %USERPROFILE%\AppData\Roaming\AVM\FRITZ!Fernzugang\
   ```

   und bei XP unter:

   ```
   %USERPROFILE%\Anwendungsdaten\AVM\FRITZ!Fernzugang\
   ```

   und zwar in einem Unterverzeichnis mit der gleichen Bezeichnung wie der von Ihnen gewählte dynamische DNS-Domainname. Starten Sie über das Startmenü das Programm *FRITZ!Fernzugang*.

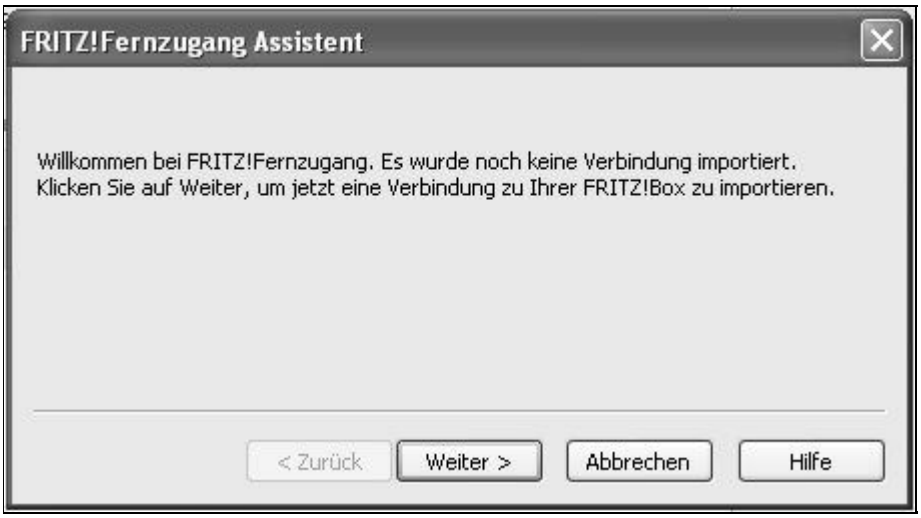


Bild 8.26 Nach dem Programmstart meldet sich umgehend ein Assistent, mit dem die Konfigurationsdatei importiert werden kann.

2. Im nächsten Schritt geben Sie den Pfad zur *vpnuser.cfg* an. Per Ordnersymbol können Sie die lokale Festplatte durchsuchen.

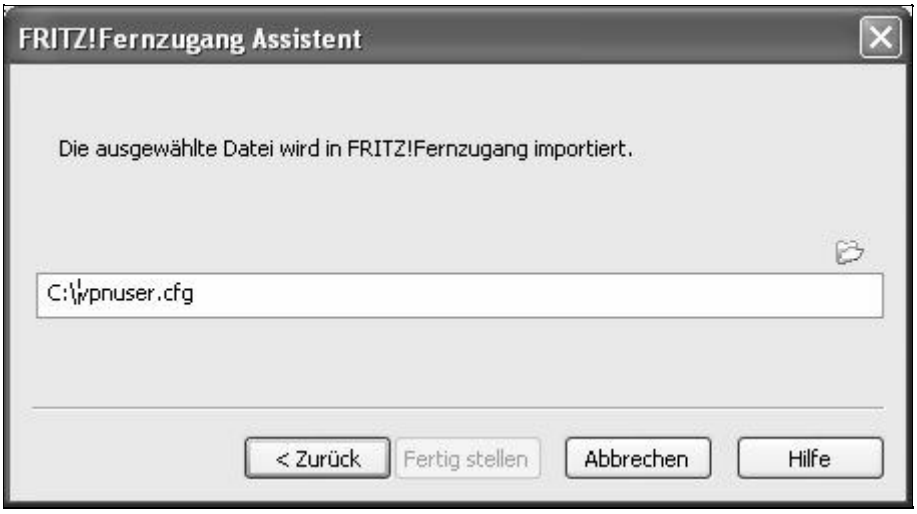


Bild 8.27 Ist die Konfigurationsdatei ausgewählt, klicken Sie auf die Schaltfläche *Fertig stellen*. Alternativ können Sie auch den Assistenten per Klick auf *Abbrechen* beenden und die Konfigurationsdatei manuell importieren.

3. Um die Konfigurationsdatei ohne Assistenten zu importieren, genügt der Datei/Importieren-Befehl, der prinzipiell das Gleiche bewirkt wie der Assistent. Nach dem Import befindet sich im Programmfenster ein Verbindungssymbol für die erstellte Verbindung. Per Klick auf den grünen Telefonhörer wird der Verbindungsaufbau gestartet.

Bild 8.28 Damit eine VPN-Verbindung zur Heimnetz-FRITZ!Box aufgebaut werden kann, muss sie auch über ihren dynamischen DNS-Namen im Internet erreichbar sein. Ist das nicht der Fall, erscheint diese Fehlermeldung.

4. Ist der dynamische DNS-Name über das Internet erreichbar, baut die FRITZ!Box anschließend die VPN-Verbindung auf.

Bild 8.29 Erfolgreich: In der Statusleiste informiert das Programm FRITZ!Fernzugang über den aktuellen Status der Verbindung.

5. Nun können Sie schalten und walten, wie Sie möchten, Sie befinden sich in Ihrem Heimnetz. Die Dateifreigaben sind über Ihre IP-Adresse erreichbar, hier genügt die Eingabe von *\\IP-Adresse* – beispielsweise *\\192.168.123.100\Daten* – im *Ausführen*-Dialog von Windows, um auf die Freigabedaten auf dem PC mit der IP-Adresse *192.168.123.100* zugreifen zu können.

8.4 VPN-Zugriff auch mit Mac OS X

Wer von unterwegs mit seinem Mac auf seine Daten zu Hause ohne Spione und »Mitleser« zugreifen möchte, kann auch damit die VPN-Funktionen der FRITZ!Box nutzen. Doch nicht nur der Datenzugriff, sondern auch der Datentransport auf Dateifreigaben zu Hause ist möglich und überaus praktisch – gerade dann, wenn im Urlaub die Kapazität der Speicherkarte in der Digitalkamera zur Neige geht und man seine Bilder einfach und vor allem sicher auf die heimische Festplatte speichert.

Neben dem entsprechend konfigurierten DSL-WLAN-Router mit VPN-Funktionalität ist lediglich ein VPN-Client für Mac OS X notwendig, der kostenlos zur Verfügung steht. Anhand der weitverbreiteten FRITZ!Box 7170 wird dieser praktische Anwendungsfall nun beschrieben. Je nach DSL-WLAN-Routermodell mit VPN-Funktionen lässt sich die Beschreibung auch auf andere Modelle übertragen.

Mit einem entfernten Mac auf das Heimnetz zugreifen

Ist die FRITZ!Box mit der passenden Konfigurationsdatei bestückt, lässt sich auch mit einem entfernten Mac auf das Heimnetz zugreifen. Hier wird lediglich ein VPN-Client wie IPSecuritas benötigt.

Lesezeichen

http://bit.ly/Ases

IPSecuritas: Hier finden Sie den kostenlosen VPN-Client IPSecuritas.

1. Im Gegensatz zu anderen, kommerziellen Lösungen ist IPSecuritas Freeware und steht kostenlos zum Download bereit. Nach Download und Installation von IPSecuritas für Mac OS X konfigurieren Sie zunächst den VPN-Client anhand der benutzerbasierten *vpnuser.cfg* des Windows-Programms *FRITZ!Box-Fernzugang einrichten*.
2. Ohne diese Datei lässt sich die VPN-Verbindung ebenfalls einrichten, Sie müssen in dem Fall jedoch sicherstellen, dass das genutzte Passwort (*key*) mit jenem in der FRITZ!Box übereinstimmt. Die Konfiguration starten Sie über *Finder/Programme/IPSecuritas* und wählen in der Menüleiste *Verbindungen/Verbindungen bearbeiten* aus. Anschließend erscheint folgender Dialog:

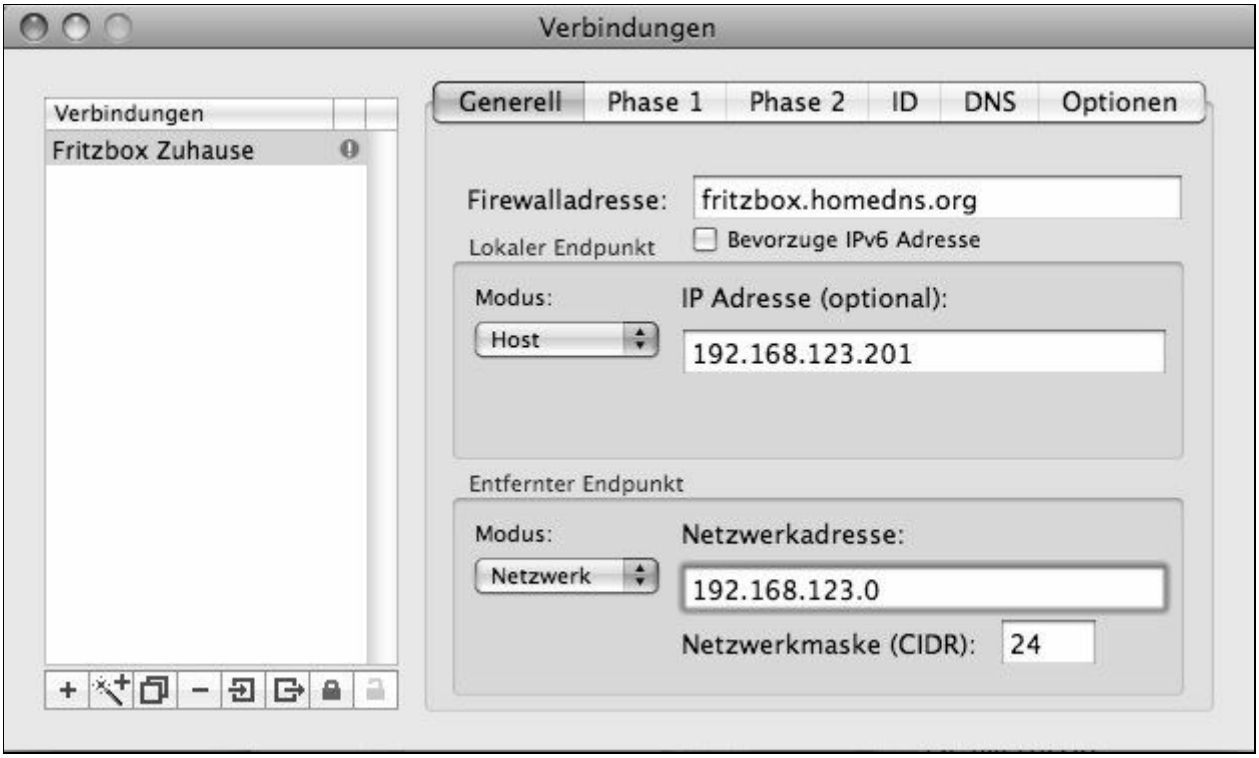


Bild 8.30 Zunächst klicken Sie links im unteren Bereich auf das Plussymbol und tragen einen aussagekräftigen Namen für die VPN-Verbindung ein.

3. Im Register *Generell* tragen Sie bei *Firewalladresse* den dynamischen DNS-Namen ein, unter dem Ihr Heimnetz im

Internet erreichbar ist. Wer stattdessen eine feste IP-Adresse von seinem Internetprovider bekommen hat, nutzt diese. Anschließend tragen Sie bei *Modus/Host* die IP-Adresse ein, die der Mac als lokale IP-Adresse im Heimnetz nutzen soll – in diesem Beispiel wurde die IP-Adresse *192.168.123.201* eingerichtet.
Diese befindet sich im gleichen Adressbereich wie das entfernte Heimnetz. Das wird hier unter *Entfernter Endpunkt/Netzwerk* mit dem Adressbereich *192.168.123.0* sowie der Netzwerkmaske *24* – was *255.255.255.0* entspricht – konfiguriert. Anschließend wechseln Sie in das Register *Phase 1*.

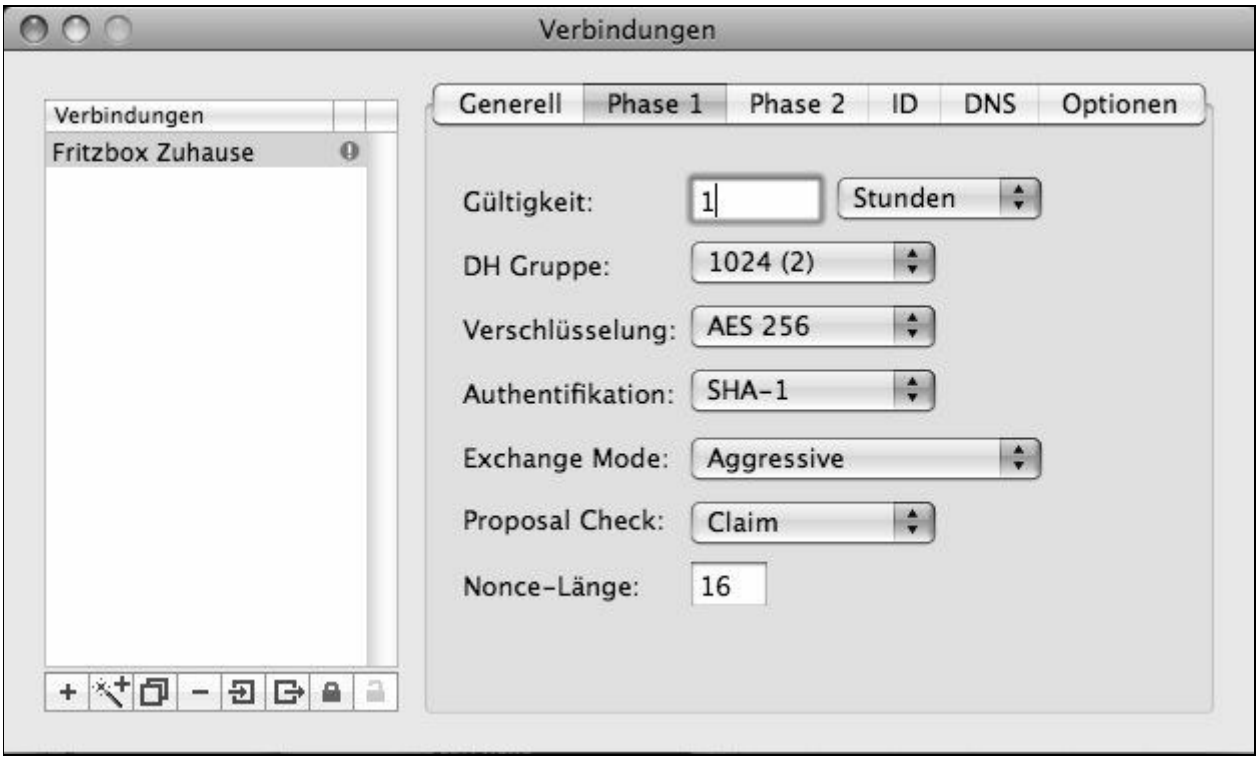


Bild 8.31 Die Gültigkeit der VPN-Verbindung lässt sich in Sekunden-, Minuten- und Stunden-Intervallen einrichten. Auf der sicheren Seite sind Sie mit dem Eintrag *1 (Stunden)*.

4. Weiterhin stellen Sie den Diffie Hellman-Eintrag bei *DH Gruppe* auf *1024 (2)*, die *Verschlüsselung* auf *AES 256* sowie die *Authentifikation* auf den Hash-Algorithmus *SHA-1* um. Für den Modus für die IKE-Phase 1 stellen Sie bei *Exchange Mode* die Option *Aggressive* ein, die weiteren Einstellungen entnehmen Sie der Abbildung.

Bild 8.32 Wenige Klicks: In *Phase 2* wählen Sie das *AES 256*-Verschlüsselungsverfahren sowie *SHA-1* für die *Authentifikation* aus.

5. Analog werden in *Phase 2* Verschlüsselungsverfahren und Authentifikation konfiguriert, die Einstellungen können Sie der Abbildung entnehmen. Im Register *ID* verwenden Sie den Benutzernamen sowie das Passwort, die per *fritzbox.cfg* in die FRITZ!Box importiert wurden. In diesem abgedruckten Beispiel steht dort *ihremail@adresse.de*.

fritzbox.cfg

```
vpncfg {
        connections {
                enabled = yes;
                conn_type = conntype_user;
                name = "ihremail@adresse.de";
                always_renew = no;
                reject_not_encrypted = no;
                dont_filter_netbios = yes;
                localip = 0.0.0.0;
                local_virtualip = 0.0.0.0;
                remoteip = 0.0.0.0;
                remote_virtualip = 192.168.123.201;
                remoteid {
                        user_fqdn = "ihremail@adresse.de";
                }
                mode = phase1_mode_aggressive;
                phase1ss = "all/all/all";
                keytype = connkeytype_pre_shared;
                key = "9bdde4d6K83ki17b3Uc3dd2_0316d7e0e8";
                cert_do_server_auth = no;
                use_nat_t = no;
                use_xauth = no;
                use_cfgmode = no;
                phase2ss = "esp-all-all/ah-none/comp-all/pfs";
                accesslist =
                        "permit ip 192.168.123.0 255.255.255.0 192.168.123.201 255.255.255.255";
        }
        ike_forward_rules = "udp 0.0.0.0:500 0.0.0.0:500",
                            "udp 0.0.0.0:4500 0.0.0.0:4500";
}


// EOF
```

Bild 8.33 Das Passwort für den Zugriff auf das Heimnetz entnehmen Sie der *fritzbox.cfg* – es steht bei *key* innerhalb der Anführungszeichen.

6. Stellen Sie bei *Lokale Identifikation* das Optionsfeld auf *User FQDN* um und tragen Sie im nächsten Feld die Benutzerkennung (hier die E-Mail-Adresse) ein. Bei *Entfernte Identifikation* stellen Sie *Adresse* ein. Bevor Sie bei *Preshared Key* das Passwort aus der *fritzbox.cfg* per Copy-and-Paste hineinkopieren, stellen Sie sicher, dass die *Authentifikationsmethode* auf den Eintrag *Preshared Key* eingestellt ist.

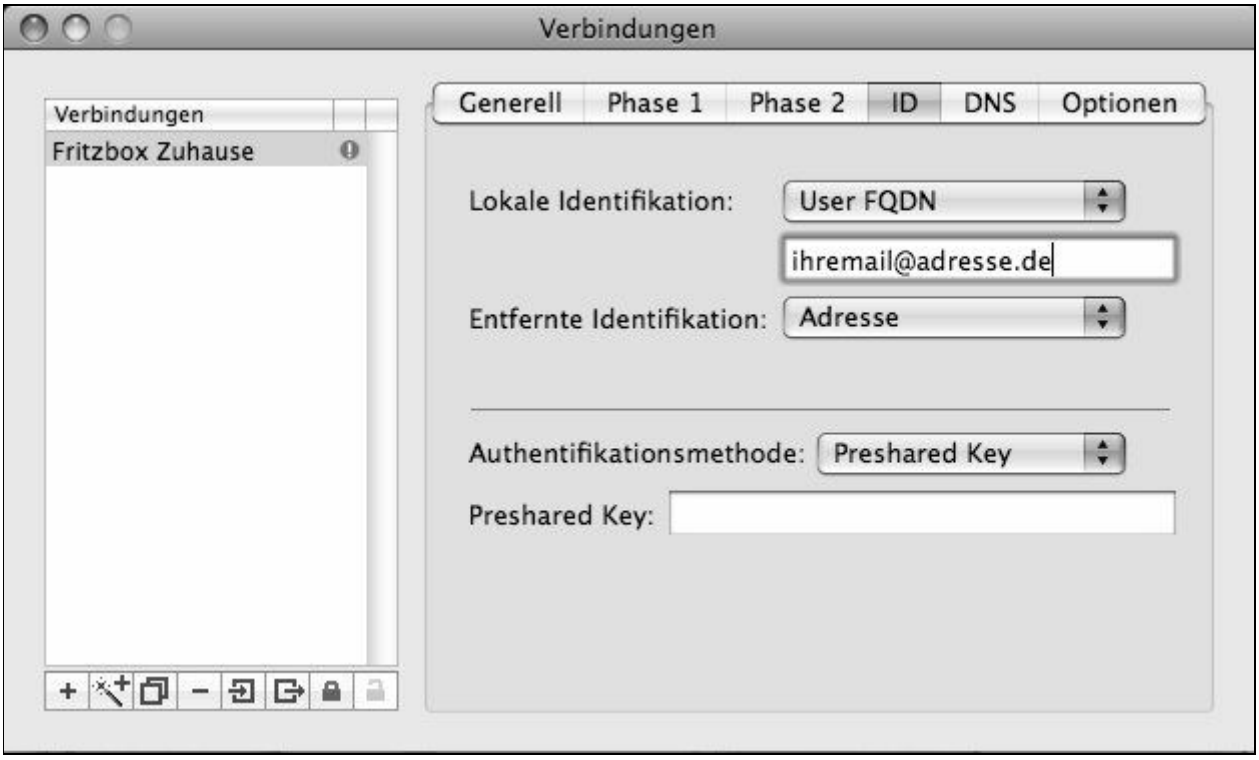


Bild 8.34 Sind die Einstellungen im Register *ID* eingetragen, öffnen Sie gleich das Register *Optionen*. Das Register *DNS* findet nur dann Beachtung, wenn Sie in Ihrem Heimnetz einen eigenen DNS-Server für die lokale Namensauflösung betreiben. In der Regel ist das jedoch nicht der Fall.

7. Im Register *Optionen* setzen Sie die Häkchen so, wie in nachstehender Abbildung gezeigt. Nach Abschluss der Konfiguration schließen Sie das Verbindungsfenster.

Bild 8.35 Das A und O sind in diesem Dialog die beiden Häkchen bei *IPSec DOI* und *Lokale IP in entf. Netzwerk*.

Erster VPN-Verbindungsaufbau und Datenaustausch

Die erstellte Verbindung ist nun im Statusfenster von IPSecuritas sichtbar. Haben Sie extern eine Internetverbindung aufgebaut, starten Sie einfach per Klick auf die *Start*-Schaltfläche eine VPN-Verbindung zu Ihrem Heimnetz zu Hause.

Bild 8.36 Nach der Konfiguration des Verbindungsprofils sind Sie nur noch einen Klick von Ihrem Heimnetz entfernt.

Nach einem kurzen Augenblick ist die Verbindung in das Heimnetz aufgebaut. Nun stehen im Finder die Heimnetzfreigaben zur Verfügung.

Bild 8.37 Im Verbindungsfenster weist IPSecuritas mit *IPSec aktiv* und einem grünen Lämpchen auf eine aktive Verbindung hin.

Auf der Gegenseite – im Heimnetz – zeigt die Konfigurationsseite der FRITZ!Box eine aktive eingehende VPN-Verbindung an. Im Übersichtsdialog leuchtet das grüne Lämpchen bei Fernzugang.

Bild 8.38 Ist der VPN-Zugriff erfolgreich hergestellt, wird neben dem Status *hergestellt* auch der aktive VPN-Benutzername im Übersichtsfenster der FRITZ!Box angezeigt.

Bei einer aktiven VPN-Verbindung können Sie auf die verfügbaren Dateifreigaben im Heimnetz – beispielsweise auf NAS-Server, Time-Capsule-Netzwerkfestplatte und dergleichen – zugreifen. Gehen Sie dazu im *Finder*-Menü über *Gehe zu* zum Dialog *Mit Server verbinden*. Dort tragen Sie das zu verwendende Protokoll sowie die IP-Adresse der Freigabe ein. So greifen Sie beispielsweise mit dem Eintrag *smb://192.168.123.20* auf die Windows-Samba-Freigaben des Geräts mit der IP-Adresse *192.168.123.20* zu.

8.5 FRITZ!Box-FTP-Server im Einsatz

Windows 7, Vista und XP bieten von Haus aus keine Serverdienste und Programme an, mit denen Sie Daten, Musik, Videos und vieles mehr im heimischen Netz und auch im Internet Freunden und Bekannten bequem zur Verfügung stellen könnten. In der Vergangenheit war dafür ein Extrarechner mit installiertem Linux oder ein gemieteter Server notwendig, der permanent im Netz zur Verfügung steht.

Der ganze Aufwand mit zusätzlichem Rechner und Linux muss nicht sein, mithilfe einer dynamischen IP-Adresse machen Sie Ihr FRITZ!Box-Heimnetz im Internet bekannt. Mit dem in der FRITZ!Box eingebauten FTP-Server stellen Sie die Daten im Netz oder im Internet zu Verfügung.

Das Beste: Mit der in der FRITZ!Box eingebauten Benutzerverwaltung ist der Zugriff auf den FTP-Server eingeschränkt, damit nicht jeder Schindluder damit treiben kann. Beim Einrichten einer solchen Lösung gehen Sie grundsätzlich folgendermaßen vor:

- Dynamische DNS-Adresse einrichten.
- Dynamischen DNS-Client installieren und konfigurieren, falls der DSL-Router keinen DynDNS-Mechanismus unterstützt.
- FTP-Server installieren und konfigurieren.
- Benutzer und Benutzergruppen einrichten.
- Verzeichnisse für FTP-Server freigeben.

Lesen Sie nun, was dynamisches DNS ist, wofür es benötigt wird und wie Sie einen kostenlosen Anbieter wie DynDNS installieren und konfigurieren.

Voraussetzung für den Betrieb von FRITZ!Box-FTP

Jedes Mal, wenn Sie sich in das Internet einloggen, bekommt Ihr Computer automatisch vom Provider eine IP-Adresse zugeteilt. TCP und IP sind die wichtigsten Protokolle, die für die Kommunikation zwischen Rechnern möglich sind – es gibt jedoch auch weitere Protokolle wie beispielsweise FTP (File Transfer Protocol), das zur Übertragung von Dateien über TCP/IP-Netzwerke eingesetzt wird.

Jeder Computer, der in einem Netzwerk TCP/IP nutzen möchte, benötigt eine IP-Adresse. Diese IP-Adresse lautet bei jeder Einwahl anders – sie stammt aus einem IP-Adresspool, den der Internetprovider reserviert hat.

Mit einem Klick der rechten Maustaste auf das Symbol *Netzwerkumgebung* rufen Sie das Kontextmenü der Verbindung auf. Im Register *Allgemein* kommen Sie mit einem Klick auf *Eigenschaften* an die TCP/IP-Einstellungen der Netzwerkkarte. Dort steht meist *IP-Adresse automatisch beziehen* und *DNS-Serveradresse automatisch beziehen*.

Mit dem Befehl *ipconfig /all* erfahren Sie im MS-DOS-Eingabefenster die aktuelle IP- und DNS-Serveradresse Ihres Rechners. Eine DNS-Serveradresse ist notwendig, um überhaupt im Internet surfen zu können. Nur mit DNS weiß der Rechner, welche zugehörige IP-Adresse beispielsweise der Name *www.franzis.de* besitzt.

Der DNS-Server des Internetanbieters löst den Namen in eine IP-Adresse auf und leitet die Anfrage an den entsprechenden Rechner weiter. Dank der DNS-Technik funktioniert das alles automatisch, und Sie brauchen sich keine komplizierten IP-Adressen zu merken. Ist die IP-Adresse eines Rechners bekannt, ist er eindeutig identifizierbar.

```
Ethernetadapter LAN-Verbindung 8:

        Verbindungsspezifisches DNS-Suffix:
        Beschreibung. . . . . . . . . . . : 3Com EtherLink XL 10/100 PCI-TX-NIC (3C905B-TX) #3
        Physikalische Adresse . . . . . . : 00-01-02-0D-5B-59
        DHCP aktiviert. . . . . . . . . . : Nein
        IP-Adresse. . . . . . . . . . . . : 192.168.123.174
        Subnetzmaske. . . . . . . . . . . : 255.255.255.0
        Standardgateway . . . . . . . . . : 192.168.123.199
        DNS-Server. . . . . . . . . . . . : 192.168.123.199

C:\>ipconfig /all
```

Bild 8.39 Mit dem Befehl *ipconfig /all* können Sie in einem MS-DOS-Eingabefenster unter Windows die vom Provider zugeteilte IP-Adresse erfahren, falls der PC mit einer DSL-Direktverbindung verbunden ist.

Soll auf Ihren Rechner zugegriffen werden können, etwa weil Sie einem Bekannten Dokumente oder Musik zur Verfügung stellen wollen, benötigt dieser die IP-Adresse Ihres Rechners. Genau diese IP-Adresse ist abhängig von der Internetverbindung und ändert sich bei jedem Einloggen ins Netz, da Sie keine Standleitung und keine feste IP-Adresse haben. Bei einem DSL-Router schauen Sie einfach in das Statusfenster der DSL-Routerkonfigurationsseiten – hier ist die aktuelle Internet-IP-Adresse zu sehen.

Der Anbieter teilt Ihrem PC bei jeder neuen Einwahl eine IP-Adresse aus seinem Adresspool zu, und Ihre Bekannten müssen abermals bei Ihnen die aktuelle IP-Adresse nachfragen, wenn sie von Ihnen Musik, Daten und anderes laden wollen. Damit Sie nicht täglich von diesen Fragen belästigt werden, können Sie mithilfe von Dynamic DNS Ihrem Rechner einen individuellen, festen Domainnamen zuweisen, auch wenn dieser keine feste IP-Adresse im Internet besitzt.

Der Vorteil von DNS ist, dass Sie den Computer auch über seinen Namen ansprechen können. Es ist einfacher, statt einer IP-Adresse wie *http://192.168.123.1* die Adresse *http://IHRDOMAINNAME.dyndns.org* einzutippen. Namen lassen sich ja bekanntermaßen leichter merken als Zahlen bzw. IP-Adressen. Für das dynamische DNS gibt es verschiedene Anbieter, die ihre Dienste zum Teil kostenlos anbieten.

```
C:\>ping www.franzis.de

Ping www.franzis.de [80.237.189.137] mit 32 Bytes Daten:

Antwort von 80.237.189.137: Bytes=32 Zeit=37ms TTL=54
Antwort von 80.237.189.137: Bytes=32 Zeit=37ms TTL=54
Antwort von 80.237.189.137: Bytes=32 Zeit=37ms TTL=54
Antwort von 80.237.189.137: Bytes=32 Zeit=36ms TTL=54

Ping-Statistik für 80.237.189.137:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 36ms, Maximum = 37ms, Mittelwert = 36ms

C:\>
```

Bild 8.40 Mit dem Befehl *ping -a DNS-Name* finden Sie die IP-Adresse eines DNS-Namens heraus. In diesem Beispiel lautet die IP-Adresse für *www.franzis.de* *80.237.189.137*.

Geben Sie beispielsweise *http://IHRDOMAINNAME.dyndns.org* in die Adressleiste des Webbrowsers ein, erkennt dieser mittels des *http*-Kürzels, dass er das HTTP-Protokoll verwenden muss. Die Zeichenfolge // bedeutet, dass es sich um eine absolute URL handelt. Mit der URL *IHRDOMAINNAME.dyndns.org* wird ein Kontakt zum DNS-Server Ihres ISP (Internet Service Provider) hergestellt. Damit wird der DNS-Name in eine IP-Adresse umgewandelt.

Neben DynDNS gibt es noch weitere Anbieter, die eine solche Funktionalität zur Verfügung stellen. Drei typische kostenlose sind die in der folgenden Tabelle aufgeführten. Die Vorgehensweise ist im Prinzip immer die gleiche, für welche Sie sich entscheiden, bleibt Ihnen überlassen.

Lesezeichen

http://www.no-ip.com
http://www.dyndns.org
http://www.opendns.be http://bit.ly/Ases
Hier eine Auswahl kostenloser Anbieter – von oben nach unten: no-ip.com, DynDNS und Open DNS Belgien.

Egal für welchen Anbieter Sie sich entscheiden, die nachstehende Prozedur des Registrierens, Einrichtens und der Konfiguration des Clients bleiben Ihnen nicht erspart. Anhand des Anbieters DynDNS finden Sie hier die notwendigen Schritte im Detail. Bei einem anderen Anbieter läuft es vergleichbar ab. Bei dem Anbieter DynDNS können Sie nach der Anmeldung über den Menüpunkt *Dynamic DNS* kostenlos bis zu fünf Subdomainadressen anlegen. Als Domainerweiterung stehen Namen wie *dyndns.org*, *dnsalias.net*, *homeftp.net* und viele mehr zur Verfügung.

Ihr eigener Computer zu Hause wäre dann zum Beispiel unter der Webadresse IHRDOMAINNAME.dyndns.org im Internet zu erreichen. Für den privaten Anwender reicht das in der Regel aus. Wer mehr haben möchte, muss Geld bezahlen. Dafür können Sie einen »echten« Domainnamen ohne eine Erweiterung wie dyndns.org mit der wechselnden IP-Adresse verbinden.

So richten Sie eine dynamische DNS-Adresse ein

Egal ob DynDNS, no-ip.com oder andere – das Einrichten einer dynamischen DNS-Adresse verläuft prinzipiell immer nach folgendem Schema:

1. Rufen Sie in Ihrem Browser mit www.dyndns.org die DynDNS-Website auf und klicken Sie hier auf den Link Create Account. Auf dem Onlineregistrierungsformular legen Sie zunächst einen Benutzernamen fest und geben sowohl eine E-Mail-Adresse als auch ein Passwort an.

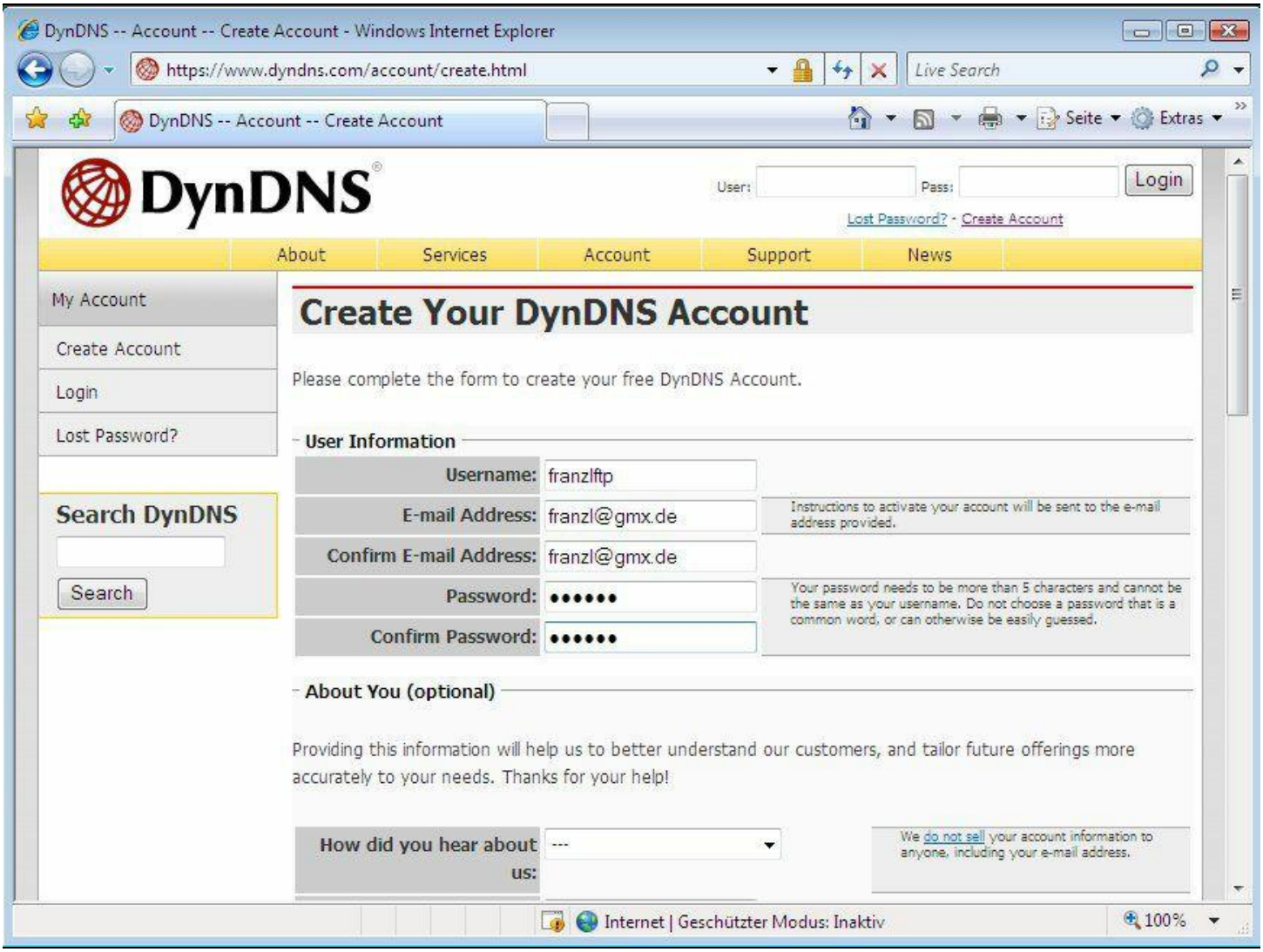


Bild 8.41 Eingabe der Benutzerinformationen.

2. Mit einem Klick auf die Schaltfläche *Create Account* schließen Sie die Registrierung nach Lesen und Bestätigen der Geschäftsbedingungen ab. Die Mühlen beim Anbieter beginnen zu mahlen, und der Account wird eingerichtet. Kurz danach erhalten Sie ein E-Mail vom Anbieter, über die Sie den soeben erstellten Account bestätigen.

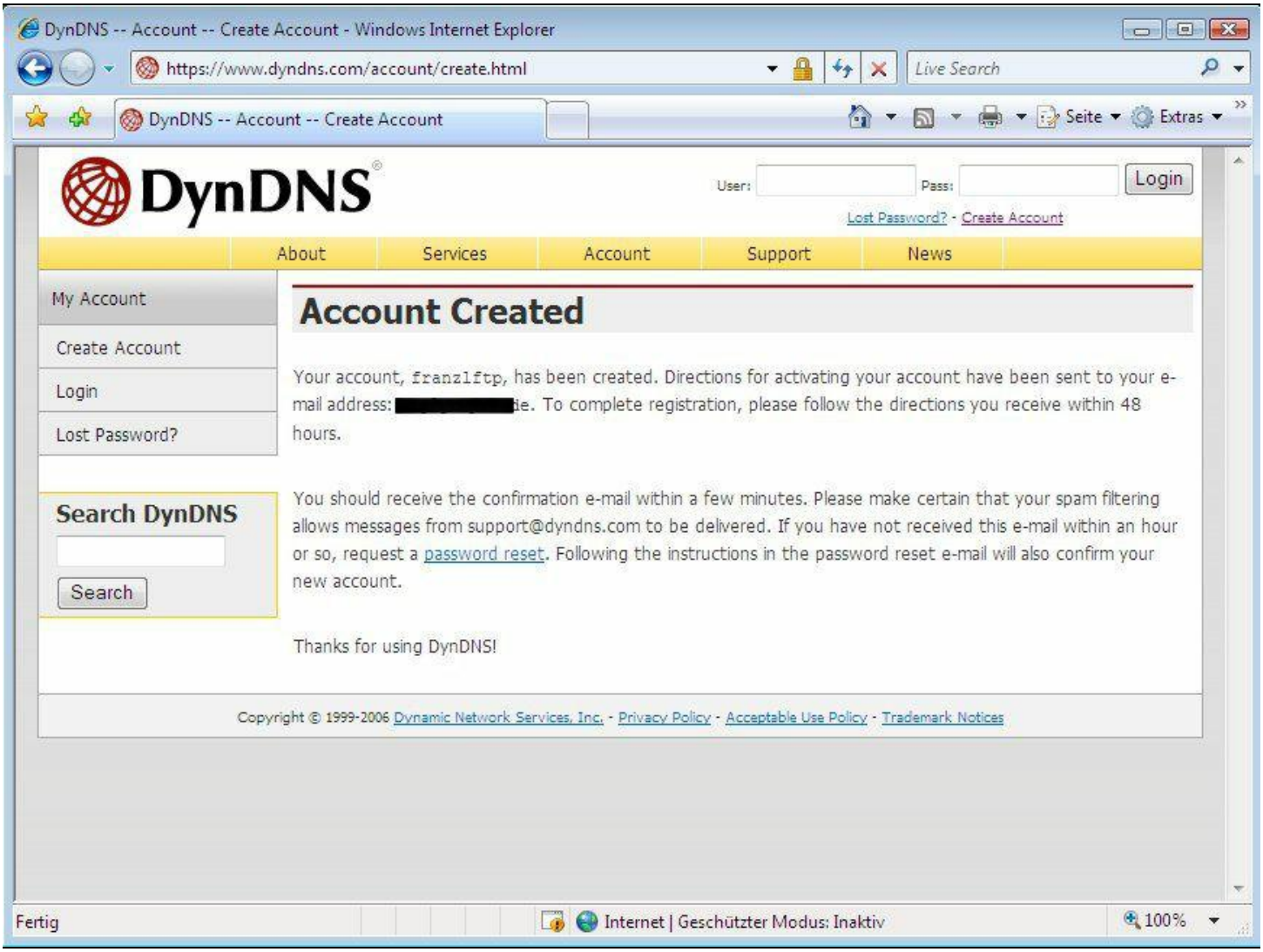


Bild 8.42 Der Account wird eingerichtet.

3. Loggen Sie sich jetzt bei DynDNS ein und erstellen Sie einen DNS-Namen. Der DNS-Name, den Sie hier festlegen, wird Ihr Internet-Domainname, der mit der Endung *dyndns.org* komplettiert wird. Über *Account* und *Login* gelangen Sie zu den persönlichen Einstellungen. Über *My Services*/*My Hosts*/*Dynamic DNS* und *New Dynamic DNS Host* tragen Sie den Namen der gewünschten Domain ein. Anschließend stellen Sie den Domainnamen (hier: dyndns.org) Ihrer Wahl ein. Das war's.
4. Nach einem Klick auf die Schaltfläche *Add Host* ist Ihre dynamische Domain im Internet aktiv. Jetzt benötigen Sie nur noch einen Mechanismus für das Übermitteln Ihrer IP-Adresse an den Anbieter. In das Feld Hostname tragen Sie den gewünschten DNS-Namen für Ihren PC ein. Daneben wählen Sie die gewünschte Domain aus.

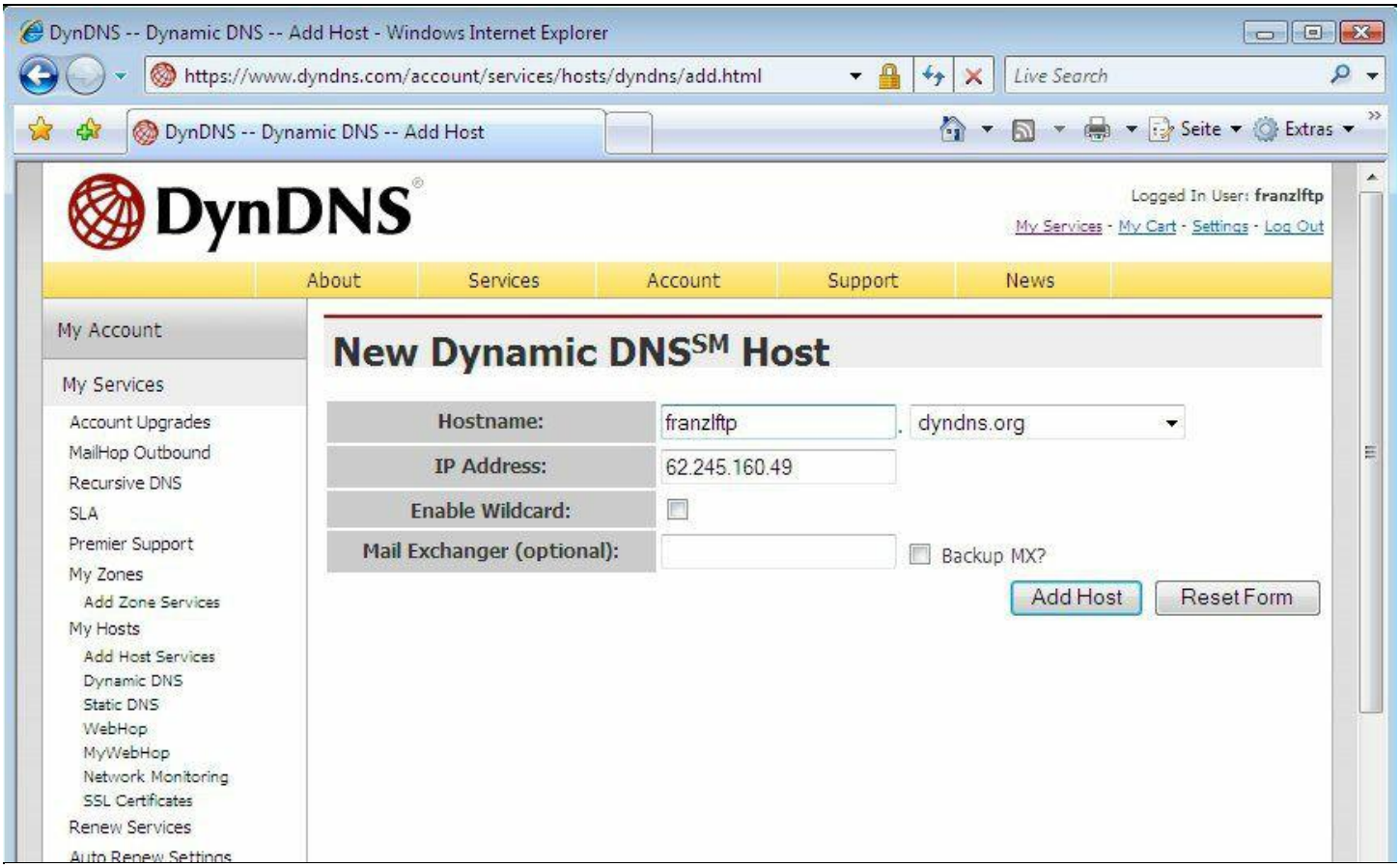


Bild 8.43 DNS-Namen auswählen.

5. Ändert sich die IP-Adresse, sollte der heimische Rechner die neue IP-Adresse dem DNS-Anbieter automatisch mitteilen. Das geschieht über einen Agenten, der im Hintergrund läuft. Unter *www.dyndns.org/services/dyndns/clients.html* finden Sie den passenden Client für das Betriebssystem. Wer einen DSL-Router mit entsprechender DynDNS-Funktionalität im Einsatz hat, braucht natürlich keinen Client auf dem Rechner zu installieren – nahezu jedes FRITZ!Box-Modell bringt mit der aktuellsten Firmware diese Funktion mit. Sobald Sie die Datei entpackt haben, installieren Sie den Client. Im Fall des DirectUpdater-Clients klicken Sie so lange auf *Next*, bis die Installation abgeschlossen ist. Die Standardeinstellungen sollten auf Anhieb funktionieren.

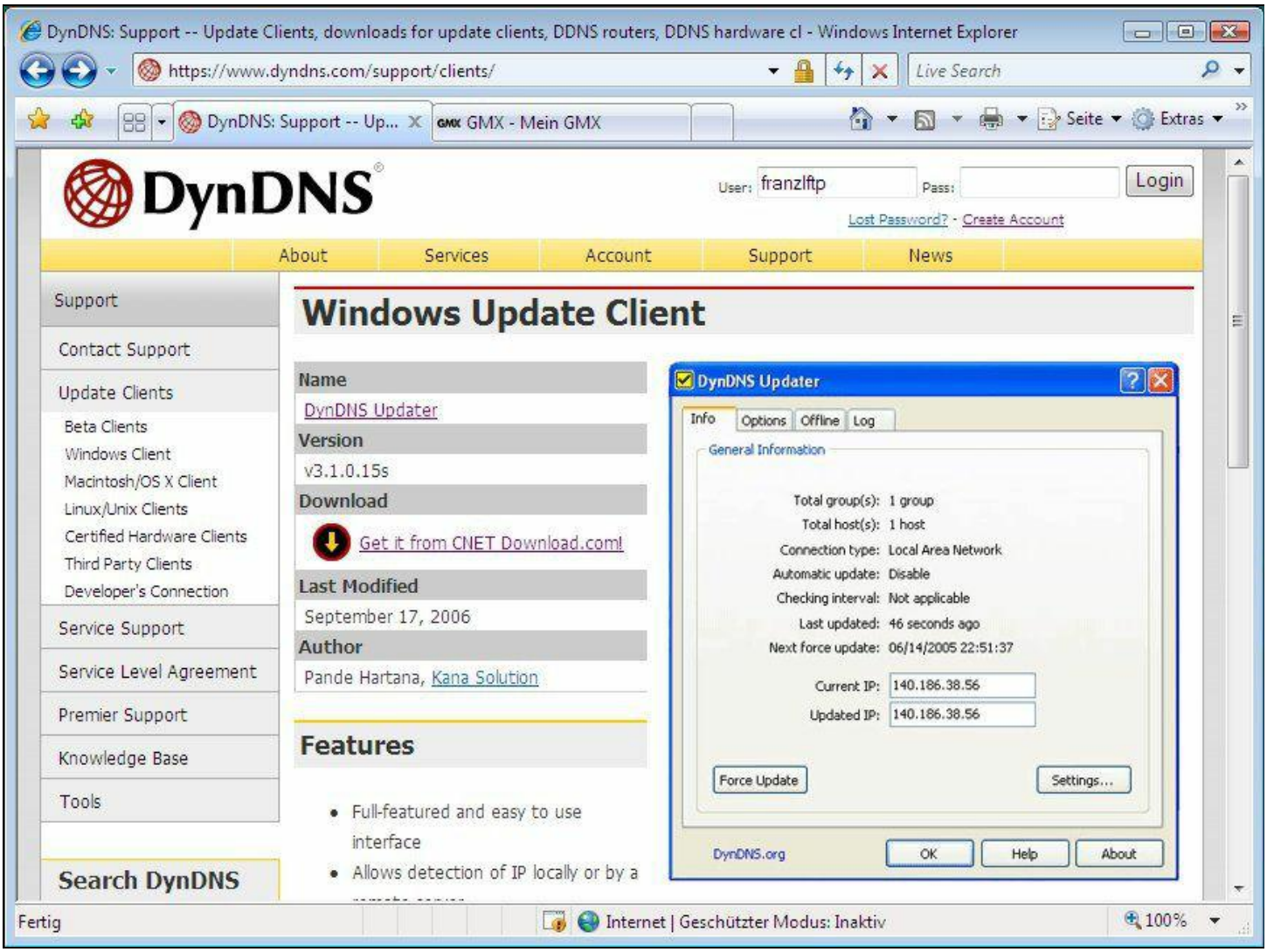


Bild 8.44 Client konfigurieren und Verbindungsdaten eintragen.

6. Nach der Installation nistet sich der DynDNS-Client in der Windows-Taskleiste als Dienst ein. Mit der rechten Maustaste wählen Sie im Kontextmenü *Launch Admin now* und passen die Verbindungsdaten für DynDNS an. Danach klicken Sie im Register *Status* auf *Create*.
   Zunächst wählen Sie Anbieter und Domainname aus und tragen das Passwort dafür ein.

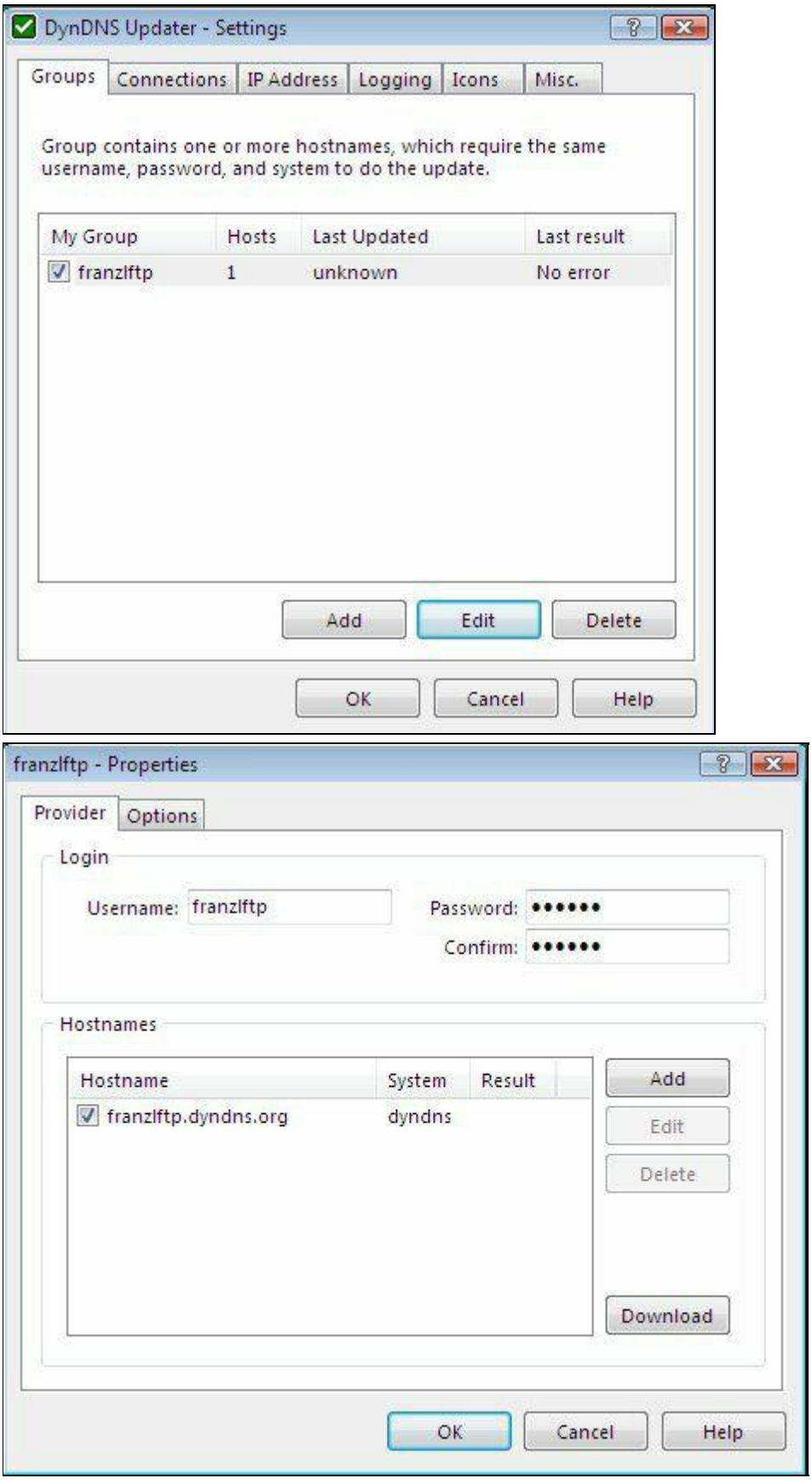


Bild 8.45 Klicken Sie auf *Edit* und überprüfen Sie die Einstellungen des Hostnamens und des Passworts. Sind diese Informationen korrekt eingetragen, übermittelt der PC in regelmäßigen Abständen die aktuelle IP-Adresse an den DynDNS-Server.

7. Mit einem Ping (*ping IHRDOMAINNAME.dyndns.org*) im DOS-Fenster können Sie das Ergebnis überprüfen. Liefert der *ping*-Befehl eine Antwort samt IP-Adresse zurück, ist alles in Ordnung. Falls nicht, zeigt *ping* die Fehlermeldung *Zielhost nicht erreichbar*. In diesem Fall ist zu prüfen, ob der Agent die IP-Adresse übermittelt hat. Im Register *Logging* erhalten Sie in der Logdatei des Agenten Informationen darüber.

8.6 Alternative zum FRITZ!Box-FTP

Eine Alternative zu dem in der FRITZ!Box eingebauten FTP-Server ist CesarFTP, eine einfach einzurichtende und leistungsfähige Freewarelösung. Auch wer mit der englischen Sprache auf Kriegsfuß steht, kann unbesorgt weiterlesen: CesarFTP ist zwar auf Englisch, aber durchgängig leicht bedienbar. Damit können Sie Dateien, Musik, Videos und vieles mehr für andere zur Verfügung stellen und zum Download anbieten. Zusätzlich können die Besucher Dateien hochladen und auf Ihrem Rechner ablegen, vorausgesetzt, es ist ihnen erlaubt. Besonders interessant: Es können verschiedene Benutzergruppen angelegt werden, damit nicht alle, die sich auf Ihrem FTP-Server einloggen, die gleichen Rechte haben.

Mit detaillierten Einstellungen und dem leistungsfähigen virtuellen Dateisystem legen Sie selbst fest, was welcher Besucher in welchem Ordner sehen, laden, verändern oder löschen darf. Damit Ihnen Ihre Besucher nicht zu viel Übertragungsbandbreite rauben, können Sie für die Benutzer oder Benutzergruppen eine sogenannte Ratio-Funktion aktivieren. Damit kann der Besucher auf Ihrer Seite beispielsweise nur so viele Daten herunterladen, wie er selbst für andere auf Ihrem FTP-Server zur Verfügung stellt und hochlädt. Für Erbsenzähler lässt sich das Tauschverhältnis gar byteweise abrechnen.

Sollten Sie noch keine Erfahrungen mit einem FTP-Client gemacht haben, kein Problem – weiter unten wird gezeigt, wie Sie mit einem FTP-Programm auf Ihren oder einen x-beliebigen FTP-Server zugreifen und Daten laden können. Doch dazu später mehr – jetzt geht es erst mal an die Installation des FTP-Servers.

So installieren und konfigurieren Sie CesarFTP

Die Installation des CesarFTP-Servers ist innerhalb weniger Minuten erledigt. Normalerweise sind Installation und Konfiguration eines FTP-Servers zeitraubende Angelegenheiten – CesarFTP ist schon sehr gut voreingestellt, damit Sie als Einsteiger sofort loslegen können.

Lesezeichen

http://bit.ly/9IMAAk
Hier der Download-Link von der CHIP-Website. Sie können auch nach CesarFTP googeln und die Setup-Datei CesarFTP.exe auf Ihre Festplatte laden.

1. Nach dem Download starten Sie mit einem Doppelklick auf die Setup-Datei CesarFTP.exe die Installation. CesarFTP weist darauf hin, dass während der Installation keine anderen Programme in Betrieb sein sollen. Deswegen wird empfohlen, diese während der Installation zu beenden. Mit Klick auf Next gelangen Sie zum nächsten Schritt.
2. Wie viele andere Programme bringt auch CesarFTP seine eigenen Lizenzbedingungen mit. Obwohl Freeware, sichert sich der Hersteller hier gegen etwaige Schäden ab, die durch sein Produkt entstehen könnten. Mit Klick auf *Yes* kommen Sie zum nächsten Dialog.

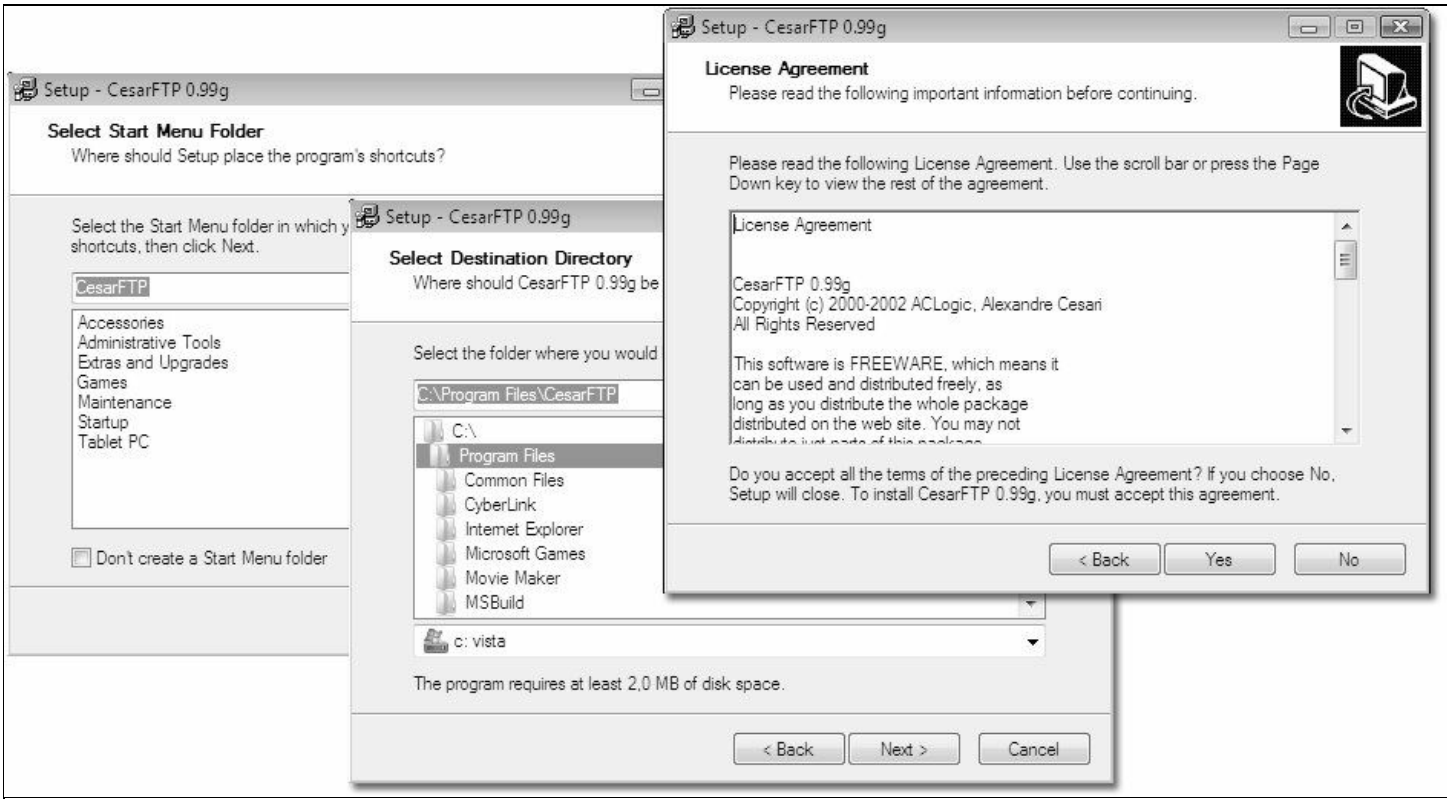


Bild 8.46 Nun legen Sie den Speicherort der Programmdateien von CesarFTP fest. Normalerweise sind die Voreinstellungen in Ordnung.

3. Wenn Sie das Programm in einem anderen Ordner installieren möchten, geben Sie diesen Installationspfad an. Möchten Sie CesarFTP in einer anderen Programmgruppe im Startmenü unterbringen, können Sie diese Gruppe ebenfalls hier angeben. Mit *Next* geht es wieder weiter.
4. Wer es übersichtlich mag, aktiviert die Option Create a desktop icon. In diesem Fall wird für das Programm eine Desktopverknüpfung angelegt. Noch mal ein Klick auf *Next* und ein weiterer Klick auf die Schaltfläche *Install* startet die Übertragung der Programmdateien in den Programmordner.

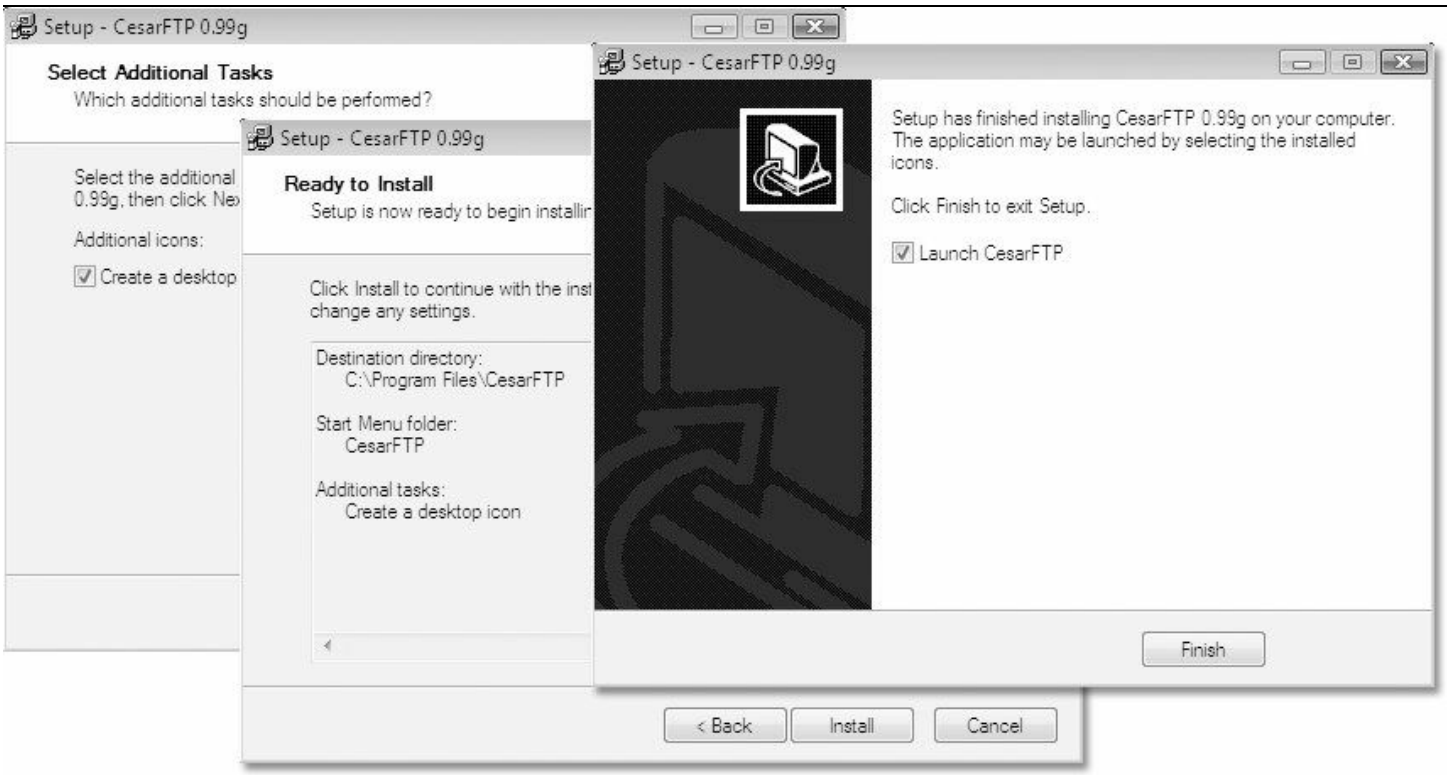


Bild 8.47 Mit *Finish* wird die Installation von CesarFTP abgeschlossen. Ist das Kontrollkästchen *Launch CesarFTP* aktiviert, wird CesarFTP sofort gestartet.

5. Prinzipiell sollte der FTP-Server nach der Installation reibungslos laufen. CesarFTP ist sehr gut vorkonfiguriert, dennoch

sind einige wenige, aber wichtige Einstellungen vorzunehmen. So erfreut manchen Besucher ein persönlicher Begrüßungstext beim Log-in. Alternativ können Sie auch Nutzungsbedingungen oder Informationen zum Inhalt des FTP-Servers eingeben. Setzen Sie Windows XP, Windows Vista oder Windows 7 ein, ist es zusätzlich sinnvoll, den Start des FTP-Servers als Service einzutragen. In diesem Fall wird der FTP-Server automatisch beim Booten Ihres Rechners gestartet und ist für alle im Internet erreichbar.

Bild 8.48 Beim erstmaligen Start von CesarFTP schlägt die Windows-Firewall Alarm. Soll ein entfernter Rechner mit dem installierten FTP-Server Kontakt aufnehmen dürfen, klicken Sie die Schaltfläche *Nicht mehr blocken* an.

6. Über die Menüleiste und *Settings/Edit Server Options* gelangen Sie zu den Konfigurationseinstellungen des FTP-Servers. Im Register *General* nehmen Sie kleinere Einstellungen vor, so bestimmen Sie beispielsweise den Begrüßungstext für Ihre Besucher.
   Im Register *IP Configuration* erledigen Sie die IP-Konfiguration des FTP-Servers, indem Sie die IP-Adresse des FTP-Servers in Ihrem Netz einstellen.

   Im Register Ban werden die IP-Adressen unerwünschter Störenfriede gespeichert, die Sie einfach per Mausklick »rauskicken« können.

   Schauen Sie ab und an in das Register *Log*. Logdateien sind das A und O, um Fehlern und verdächtigen Aktivitäten auf dem FTP-Server auf die Schliche zu kommen. Dafür lassen Sie von CesarFTP sämtliche Dateioperationen sowie Verbindungs- und Log-in-Vorgänge protokollieren.

Nach den Grundeinstellungen richten Sie Gruppen und Benutzer ein, damit nicht jeder auf Ihrem Rechner Narrenfreiheit hat. Prinzipiell sollten Sie sich genau überlegen, wer auf den FTP-Server zugreifen darf und wer nicht. Der Server ist zwar nur für den Personenkreis sichtbar, der den Domainnamen oder die IP-Adresse des Rechners kennt, trotzdem ist der Einsatz einer Benutzerverwaltung sinnvoll: So können manche Ihrer Freunde nur herunterladen, andere dürfen zusätzlich Dateien löschen oder bearbeiten.

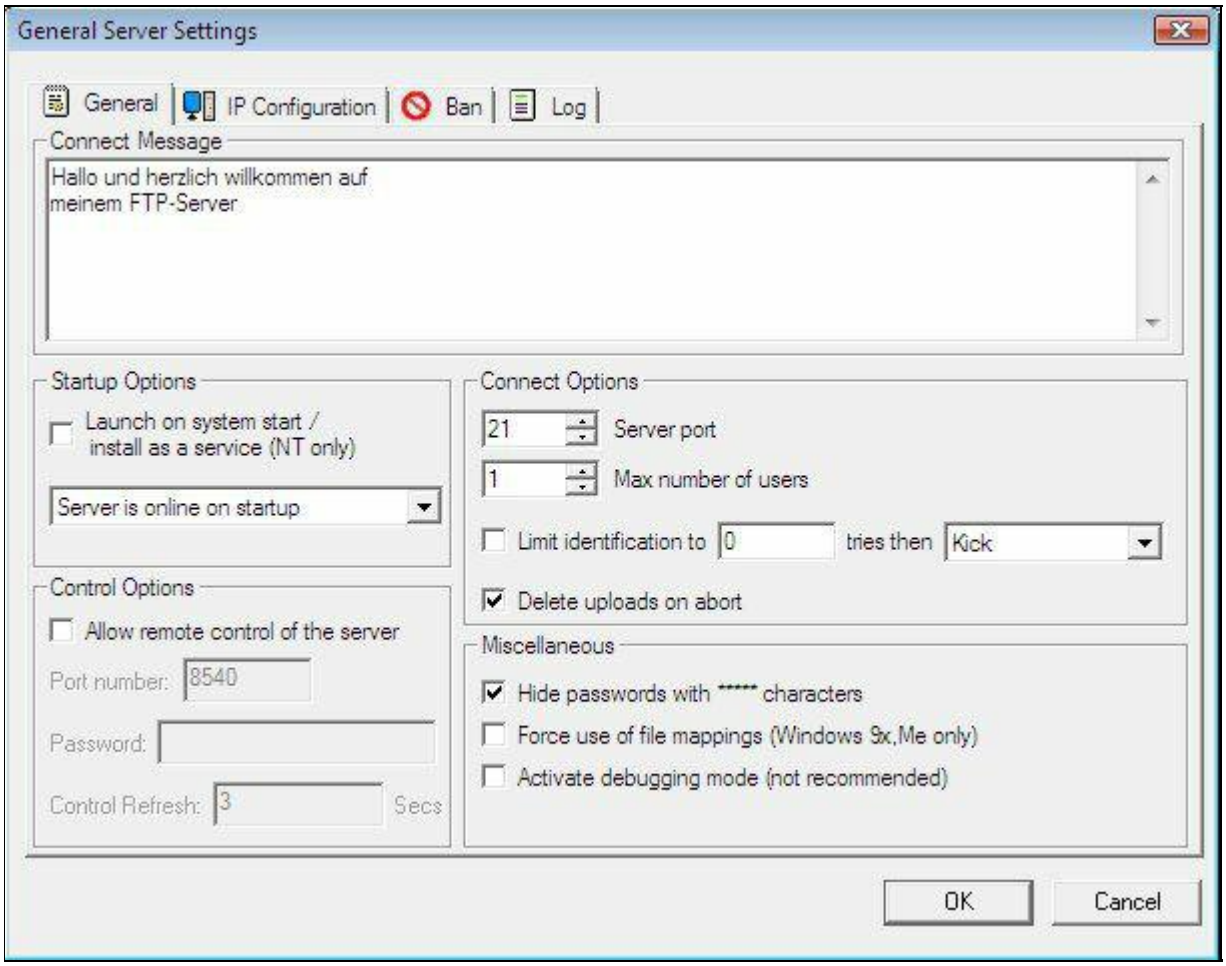


Bild 8.49 Beim Start von CesarFTP erscheint eine übersichtliche und aufgeräumte Oberfläche. Über *Startup Options* können Sie das Startverhalten von CesarFTP steuern.

Gemeinsames Verzeichnis für eine Benutzergruppe anlegen

Die Benutzung von CesarFTP ist denkbar einfach. Nach Installation und Konfiguration des FTP-Servers befindet sich dieser im Active Mode, und die Arbeit kann beginnen. Die Benutzerverwaltung finden Sie in der Menüleiste unter *Settings/Edit Users & Groups*.

1. Je nachdem, wie viele Benutzer auf den FTP-Server zugreifen sollen, können Sie für jeden einzelnen ein eigenes Verzeichnis auf der Festplatte anlegen und es dem jeweiligen Benutzer zuordnen.
   Oder Sie verwenden ein gemeinsames Verzeichnis für alle Benutzer. In diesem Fall legen Sie eine Gruppe an und machen die Benutzer zu Mitgliedern der Gruppe. Der Vorteil des Einsatzes einer Benutzergruppe beim FTP-Server liegt auf der Hand: Es müssen nicht jedem Anwender separat die Rechte dafür zugeteilt werden, was er darf und was nicht.

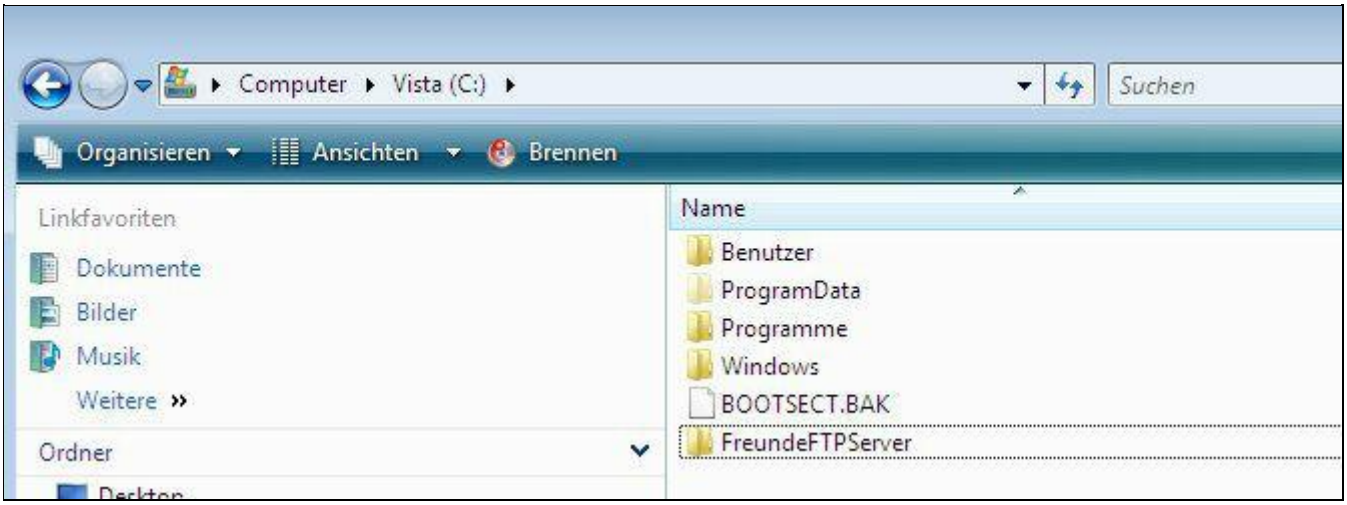


Bild 8.50 Im Windows Explorer legen Sie einen Ordner, hier *C:\FreundeFTPServer*, für die Besucher des FTP-Servers an.

2. Über das Menü *Settings*/*Edit User & Groups* öffnen Sie die Benutzerverwaltung. Hier richten Sie im Dialogfeld User & Group settings eine oder mehrere Gruppen ein. Wie Sie die Gruppe benennen, bleibt Ihnen überlassen.

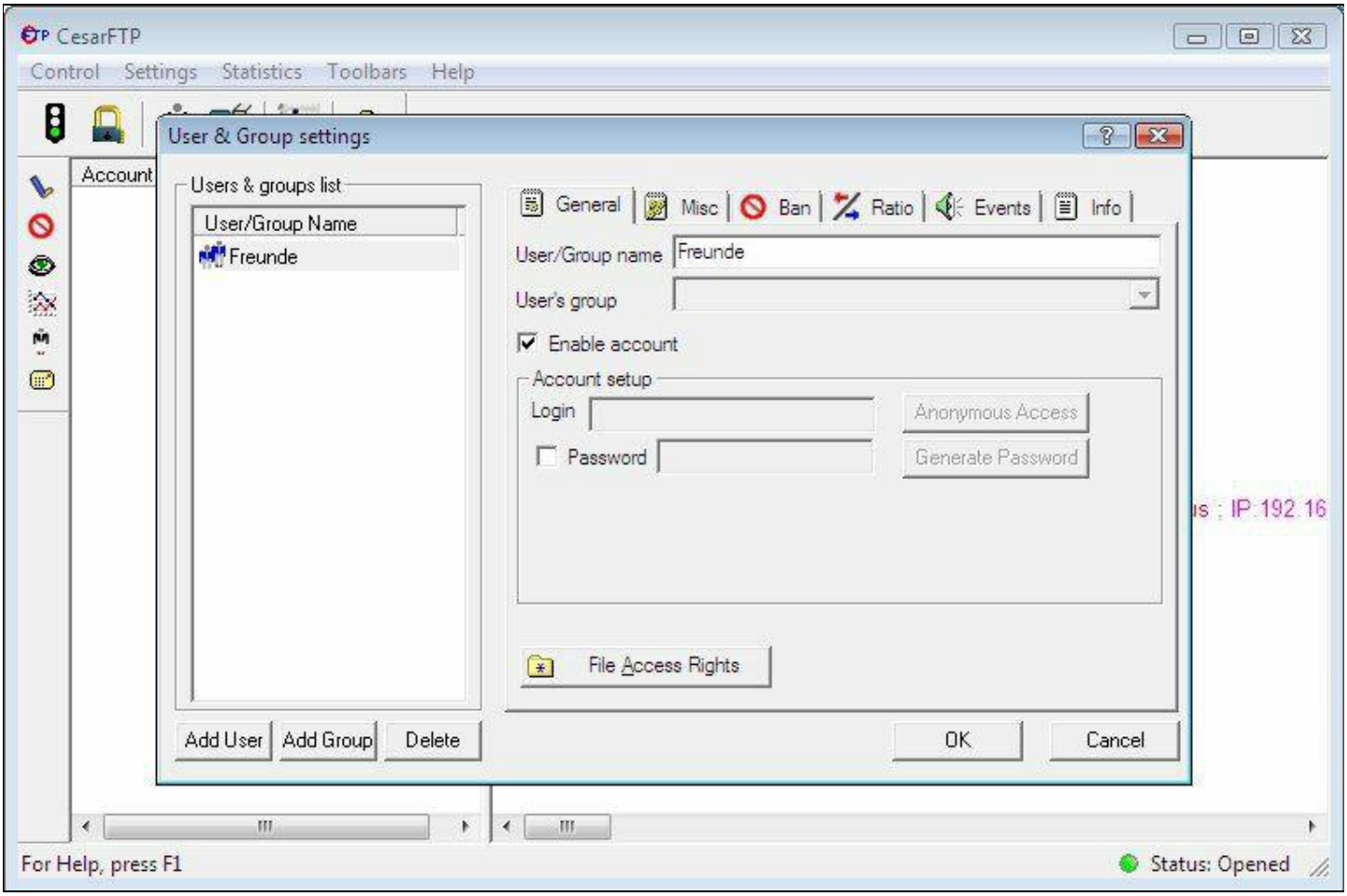


Bild 8.51 Mit einem Klick auf die Schaltfläche *File Access Rights* öffnet sich ein neues Fenster, der CesarFTP-Browser.

3. Wechseln Sie im oberen Fensterbereich zu dem Ordner, den Sie für die Besucher freigeben möchten, hier *C:\FreundeFTPServer*, und ziehen Sie ihn mit der Maus in den unteren Bereich zu der entsprechenden Gruppe. Benennen Sie später im unteren Bereich einen Ordner um, hat das keinen Einfluss auf den Namen des Ordners auf der Festplatte, da CesarFTP ein virtuelles Dateisystem verwendet. So lassen sich unterschiedliche Ordner auf der Festplatte für eine Gruppe oder einen Benutzer freigeben.

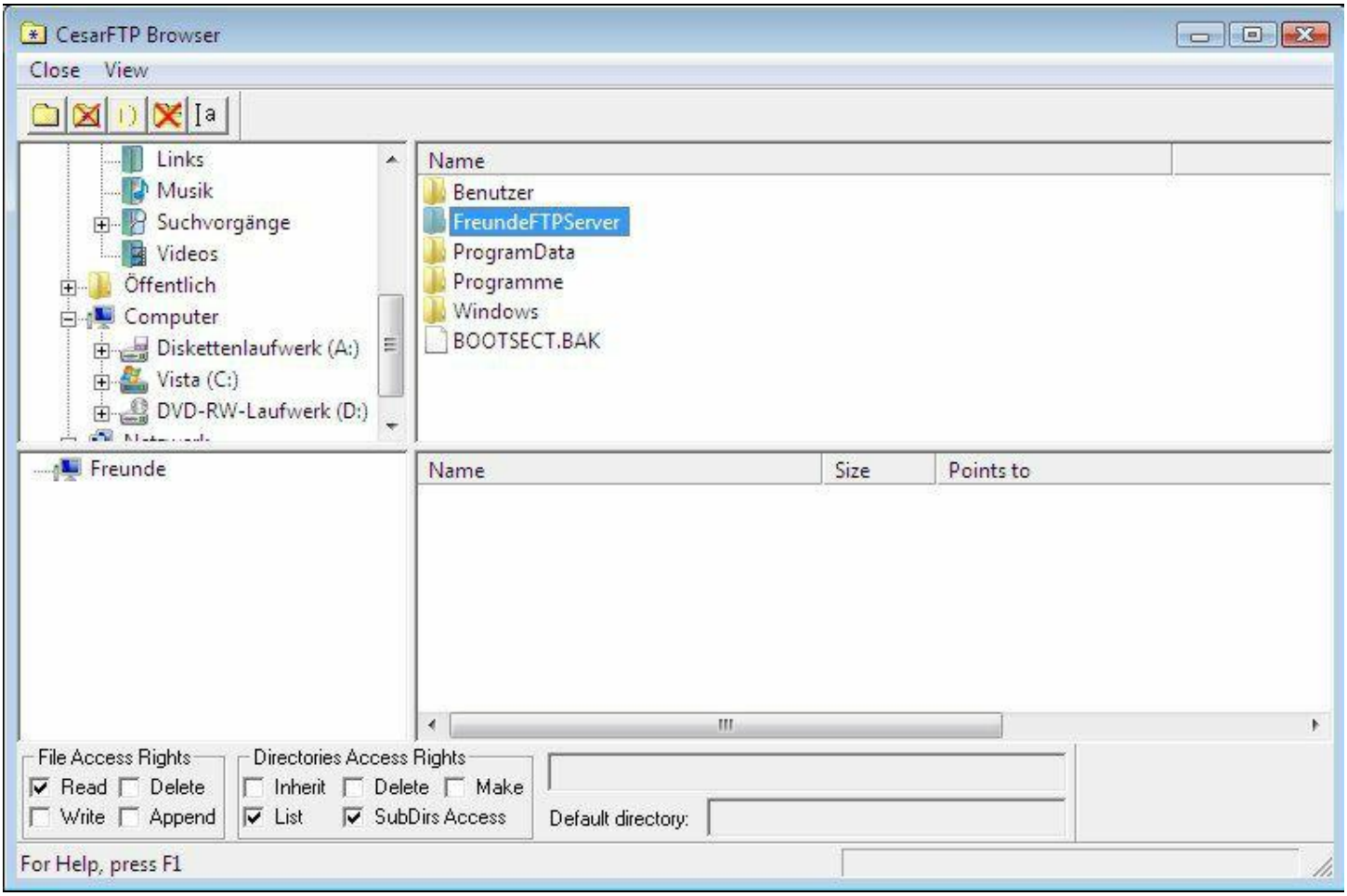


Bild 8.52 Im unteren Bereich des CesarFTP-Browsers unter *File Access Rights* können Sie pro Gruppe festlegen, was diese mit den Dateien anstellen darf, die Sie zum Zugriff freigegeben haben.

4. Es gibt normalerweise keinen Grund, jemanden etwas löschen zu lassen – mit dem Schalter *Read* sind Sie auf der sicheren Seite. Sind viele Besucher auf Ihrem FTP-Server zu erwarten, sollten Sie entsprechend viele Gruppen und Ordner anlegen, damit die Wartung des FTP-Servers übersichtlich bleibt.

Benutzergruppen um Benutzerinformationen ergänzen

Sind die Gruppen bei CesarFTP angelegt, können sie mit Benutzerinformationen ergänzt werden. Die Benutzer erben die Eigenschaften der Gruppe. Der Vorteil ist, dass Sie nicht jeden Benutzer einzeln konfigurieren müssen. In diesem Abschnitt legen Sie einen oder mehrere Benutzer an und ordnen sie den jeweiligen Gruppen zu.

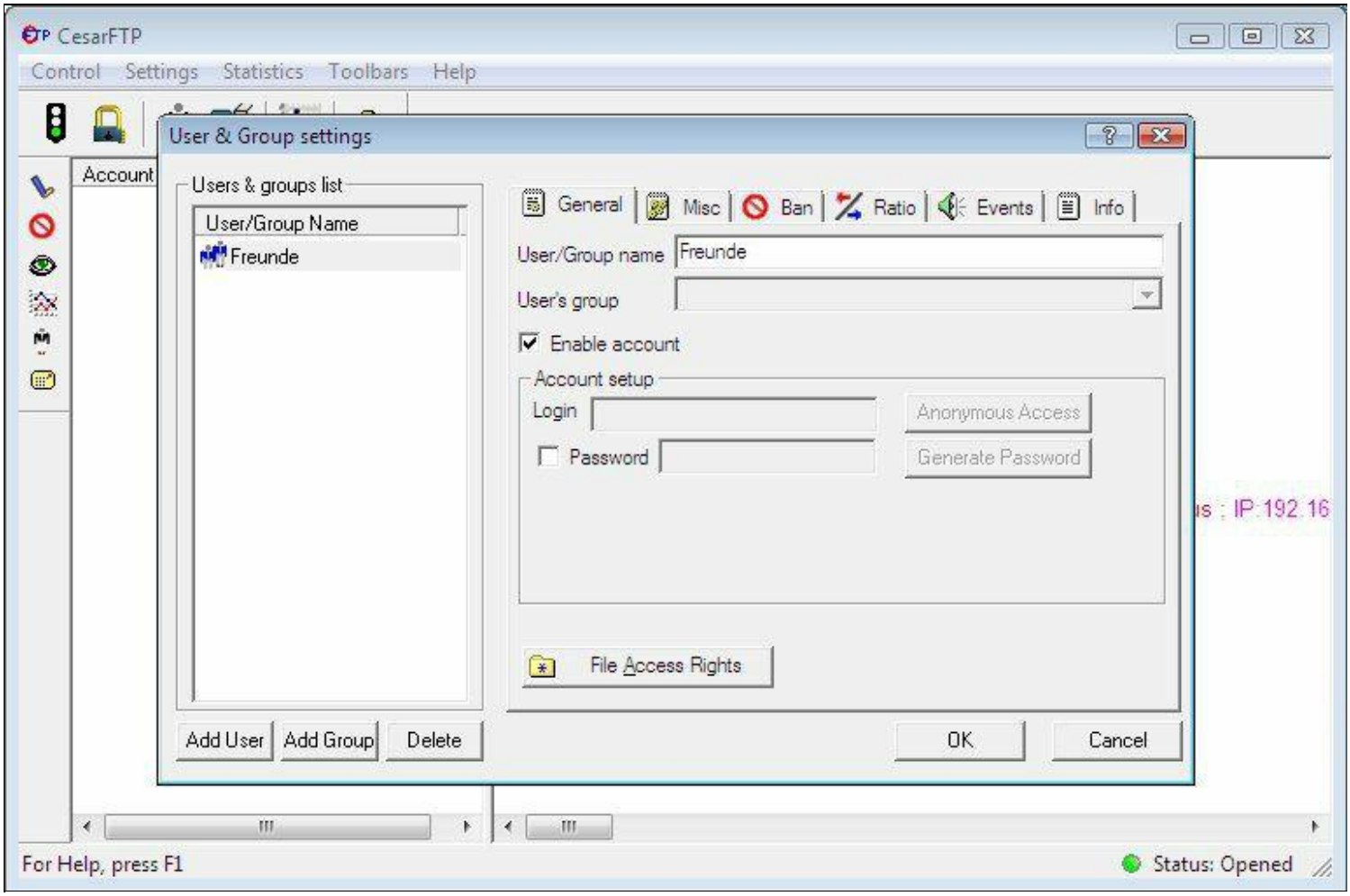


Bild 8.53 Mit einem Klick auf die Schaltfläche *Add User* fügen Sie einen neuen Benutzer dem FTP-Server hinzu. Im Bereich *User/Group name* tragen Sie den Namen des Benutzers ein.

Über das Menü *Settings/Edit User & Groups* kommen Sie zur Benutzerverwaltung. Dort können Sie beliebig viele Benutzer einrichten und sie dann einer oder mehreren Gruppen zuordnen. Dazu ist die Gruppe auszuwählen, zu der ein Benutzer gehören soll. Es kann auf Wunsch auch ein einzelner Benutzer ohne Gruppenzugehörigkeit angelegt werden, der beispielsweise mehr Rechte hat als alle anderen.

Zugangsinformationen konfigurieren

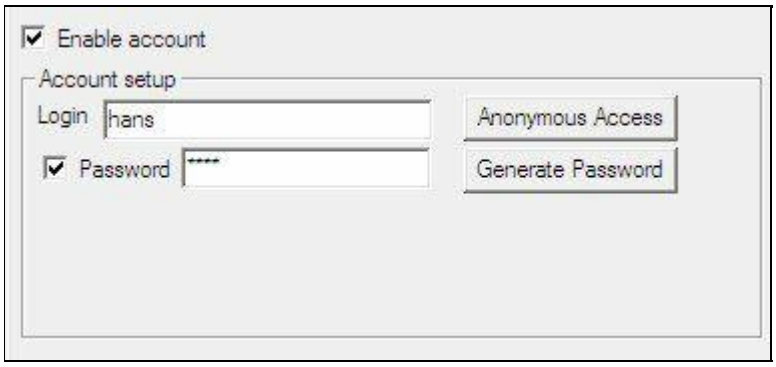


Bild 8.54 Hier ist für den Benutzer ein Log-in-Name (hier *hans*) einzutragen.

Aktivieren Sie das Häkchen bei *Password*, damit ein Passwort gesetzt werden kann. Anschließend ist das Passwort für den neuen Benutzer einzugeben – für Faule generiert der Klick auf *Generate Password* ein Passwort aus Sonderzeichen, Text und Zahlen. Dieses übermitteln Sie dann als Serverbetreiber dem User, damit der sich mit seiner Kennung auf Ihrem FTP-Server anmelden kann.

Rechte für Ordner setzen

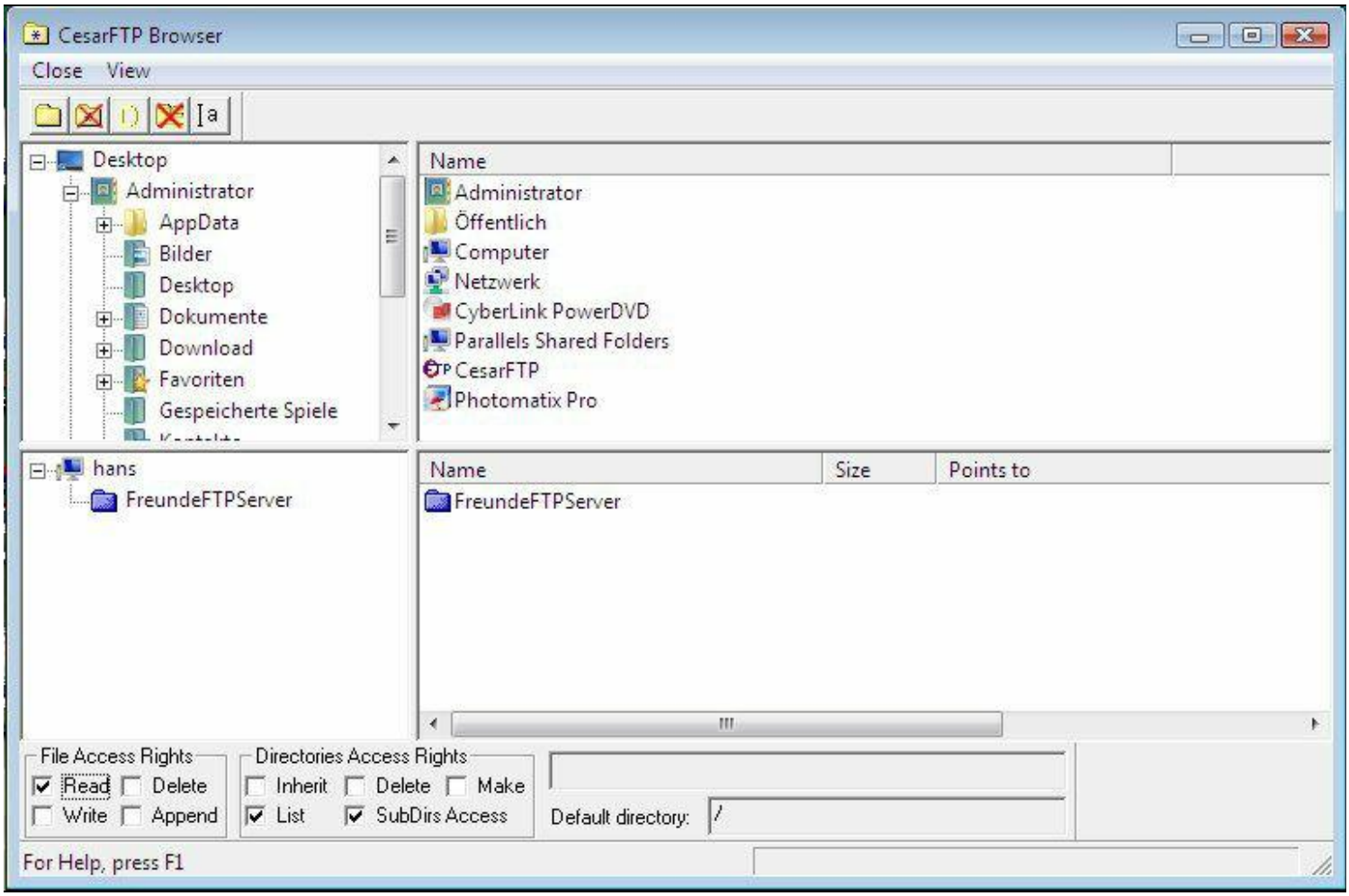


Bild 8.55 Der neue Benutzer erbt die Rechte der Gruppe. Ist der neue Benutzer jedoch nicht innerhalb eines Gruppencontainers untergebracht, kann er gesondert konfiguriert werden.

Markieren Sie diesen Benutzer und legen Sie mit einem Klick auf *File Access Rights* fest, was er auf dem FTP-Server anstellen darf und was nicht. Ist erst einmal eine größere Zahl von Benutzern angelegt, sehen Sie sie in einer übersichtlichen Liste. Mit einer durchdachten Gruppenstruktur haben Sie Überblick über die Rechte jedes einzelnen Benutzers. Mit Klick auf *Enable Account* können Sie das markierte Benutzerkonto vorübergehend deaktivieren und später jederzeit wieder aktivieren. Wer es ganz ausführlich mag, kann im Register *Info* für jeden Benutzer den Vornamen, den Nachnamen, eine Adresse sowie Kommentare dazu erfassen.

Upload-Verzeichnis für Benutzer einrichten

Das Konfigurieren eines Upload-Verzeichnisses bei CesarFTP verläuft prinzipiell analog zum Vorgang *Benutzer einrichten*. Zusätzlich sind hier bei der Rechtevergabe noch andere Parameter zu setzen.

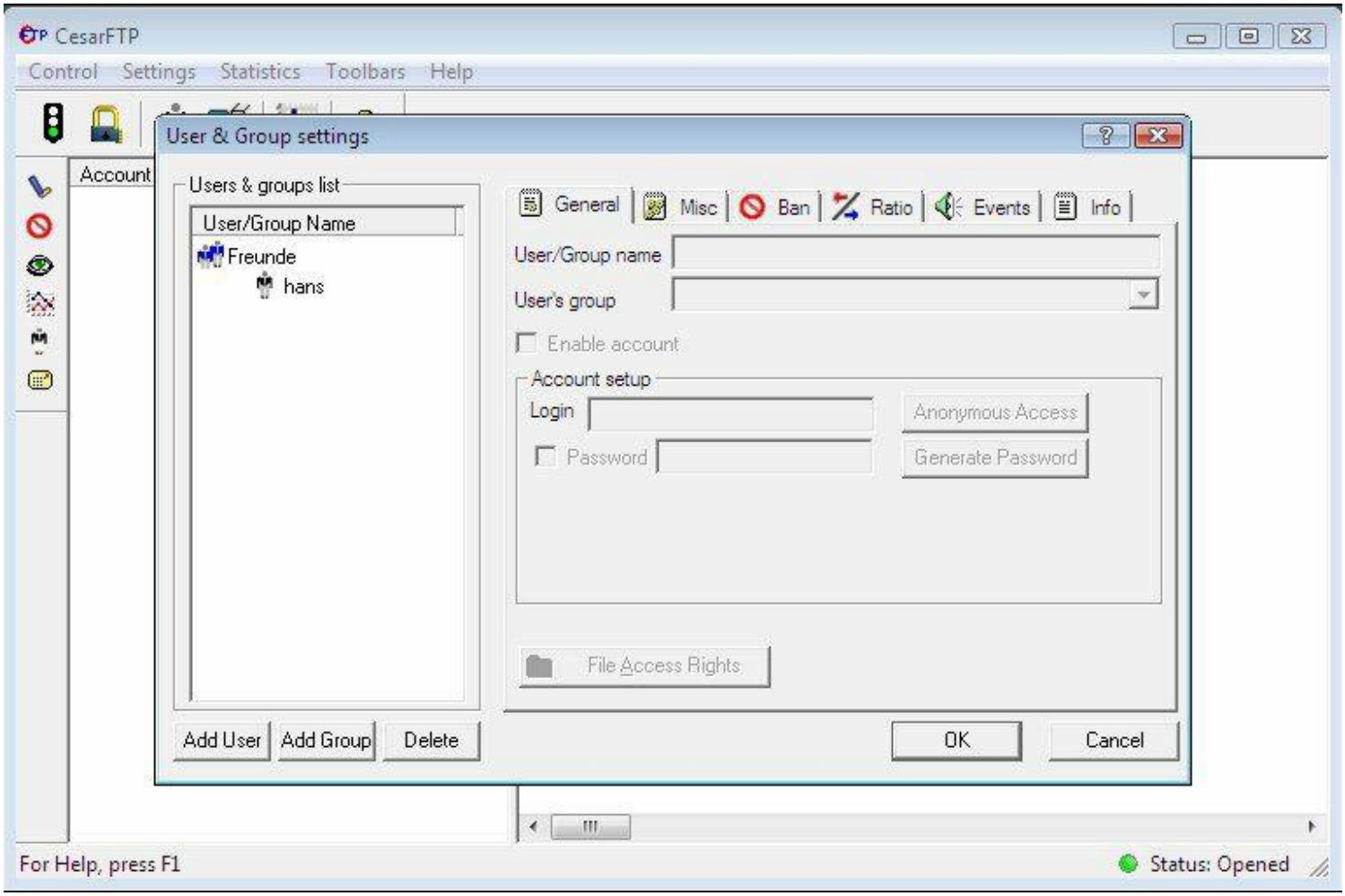


Bild 8.56 Über *Settings* in der Menüleiste öffnen Sie *User & Group settings*. Erstellen Sie über *Add User* einen neuen Account oder wählen Sie den, der geändert werden soll.

Die Benutzer können damit nicht mehr nur Dateien saugen, sondern auch Daten auf dem FTP-Server ablegen. Voraussetzung dafür ist, dass ein Benutzer-Account für den Benutzer angelegt ist, der auf dem FTP-Server Daten hochladen darf, und dass dafür ein freigegebenes Verzeichnis existiert.

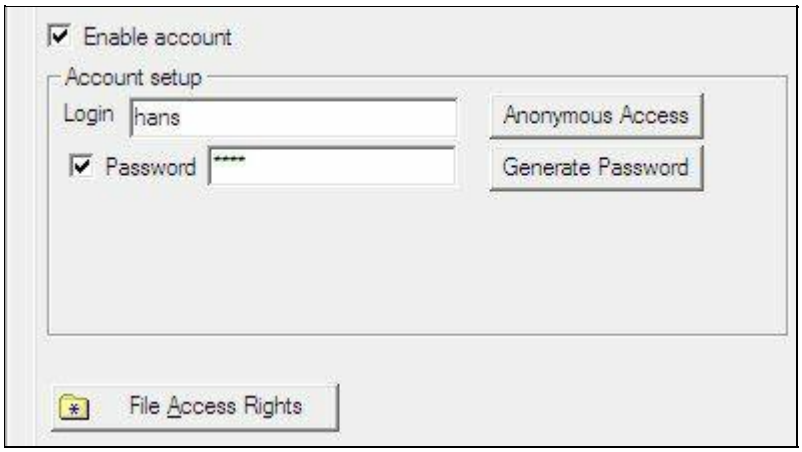


Bild 8.57 Öffnen Sie mit einem Klick auf *File Access Rights* den Dateibrowser von CesarFTP. Haben Sie noch keinen Ordner zum Hochladen angelegt, erstellen Sie mithilfe des Windows Explorer ein neues Verzeichnis.

Ordner zuordnen

Hier können Sie beliebig viele Ordner und Dateien, auch von verschiedenen Quelllaufwerken, unterbringen. Das virtuelle Dateisystem von CesarFTP bietet mit seiner Rechtestruktur vielfältige Möglichkeiten. Markieren Sie den Ordner, der für das Hochladen der Dateien zur Verfügung stehen soll, und aktivieren Sie das Kontrollkästchen *Inherit*, nachdem Sie die *File Access Rights* auf *Read* und *Write* gesetzt haben.

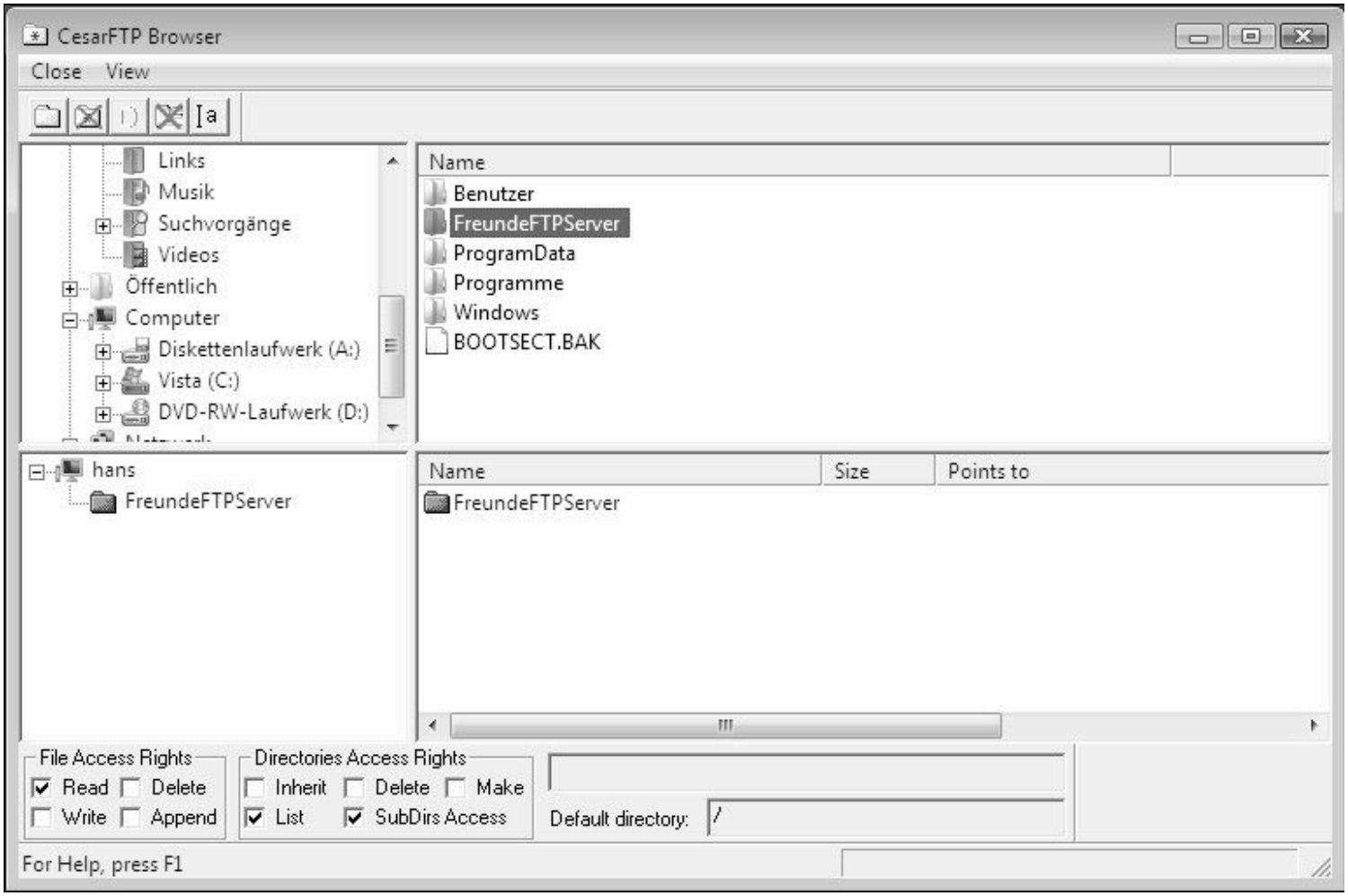


Bild 8.58 Im Dateibrowser von CesarFTP suchen Sie im oberen Fenster den frisch angelegten Ordner und ziehen ihn per Drag-and-Drop in das untere Zielbereichsfenster.

Soll nur das Hochladen von Dateien möglich sein, deaktivieren Sie das *Read*-Kontrollkästchen. Möchten Sie das Wiederaufnehmen von abgebrochenen Downloads erlauben, aktivieren Sie die Option *Append*. Mit *Make* können Sie den Anwendern erlauben, selbst Ordner auf Ihrem FTP-Server anzulegen. Keinesfalls sollten Sie das Kontrollkästchen *Delete* aktivieren, da die Gäste sonst Dateien löschen können.

Konfiguration abschließen

Schließen Sie nun per *Close* in der Menüleiste den CesarFTP-Dateibrowser und klicken Sie auf *OK* zum Speichern der Einstellungen. Jetzt können Sie mit einem beliebigen FTP-Client die Einstellungen testen.

Wer keinen FTP-Client installieren möchte, kann sich auch mit Hausmitteln behelfen: Ohne Installationsaufwand funktioniert das Saugen von einem FTP-Server auch mit dem Internetbrowser: Möchten Sie lediglich Dateien herunterladen, können Sie Webbrowser wie Firefox oder Internet Explorer als FTP-Client nutzen.

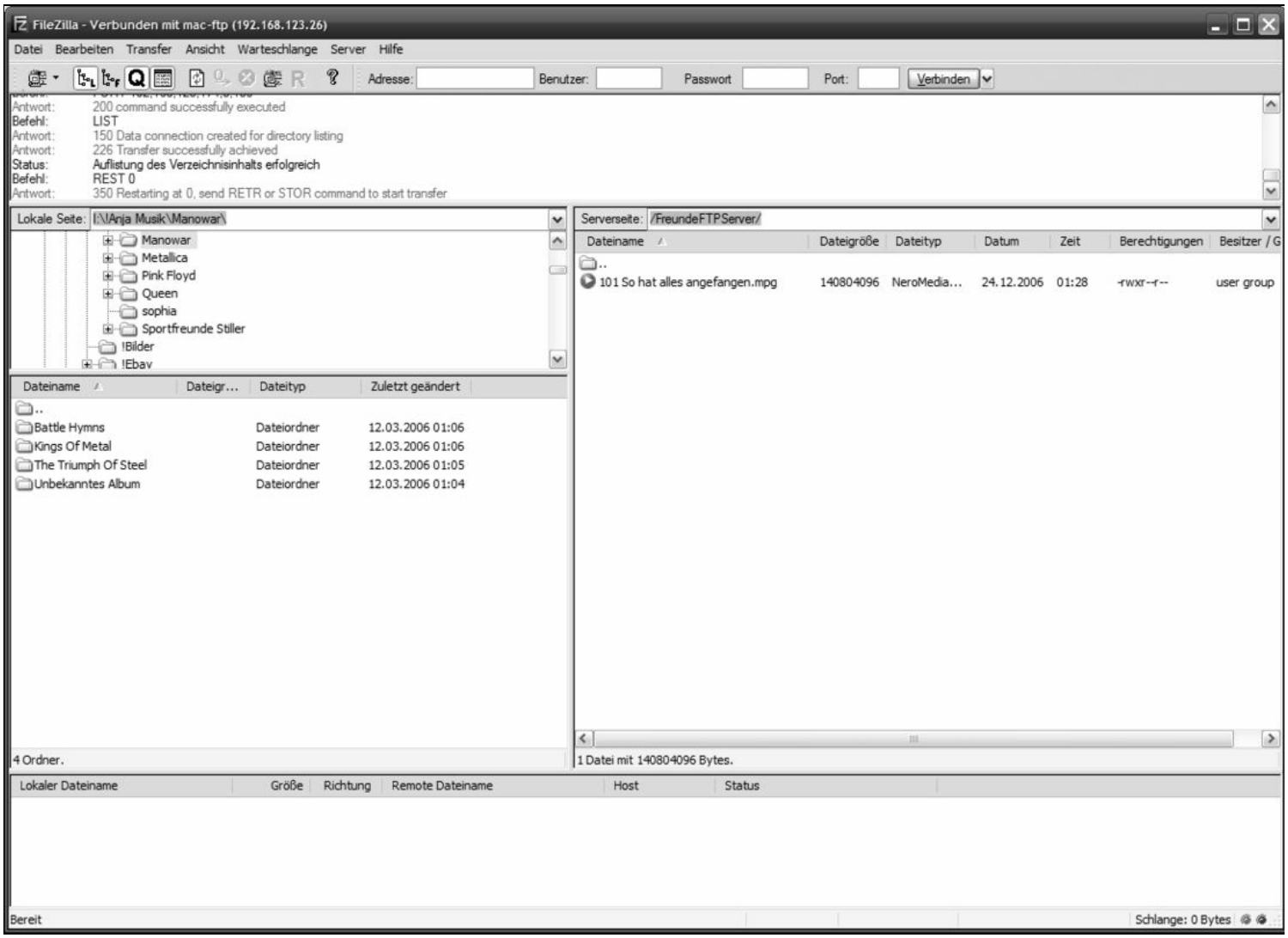


Bild 8.59 Ein User hat sich auf dem eingerichteten FTP-Server eingeloggt.

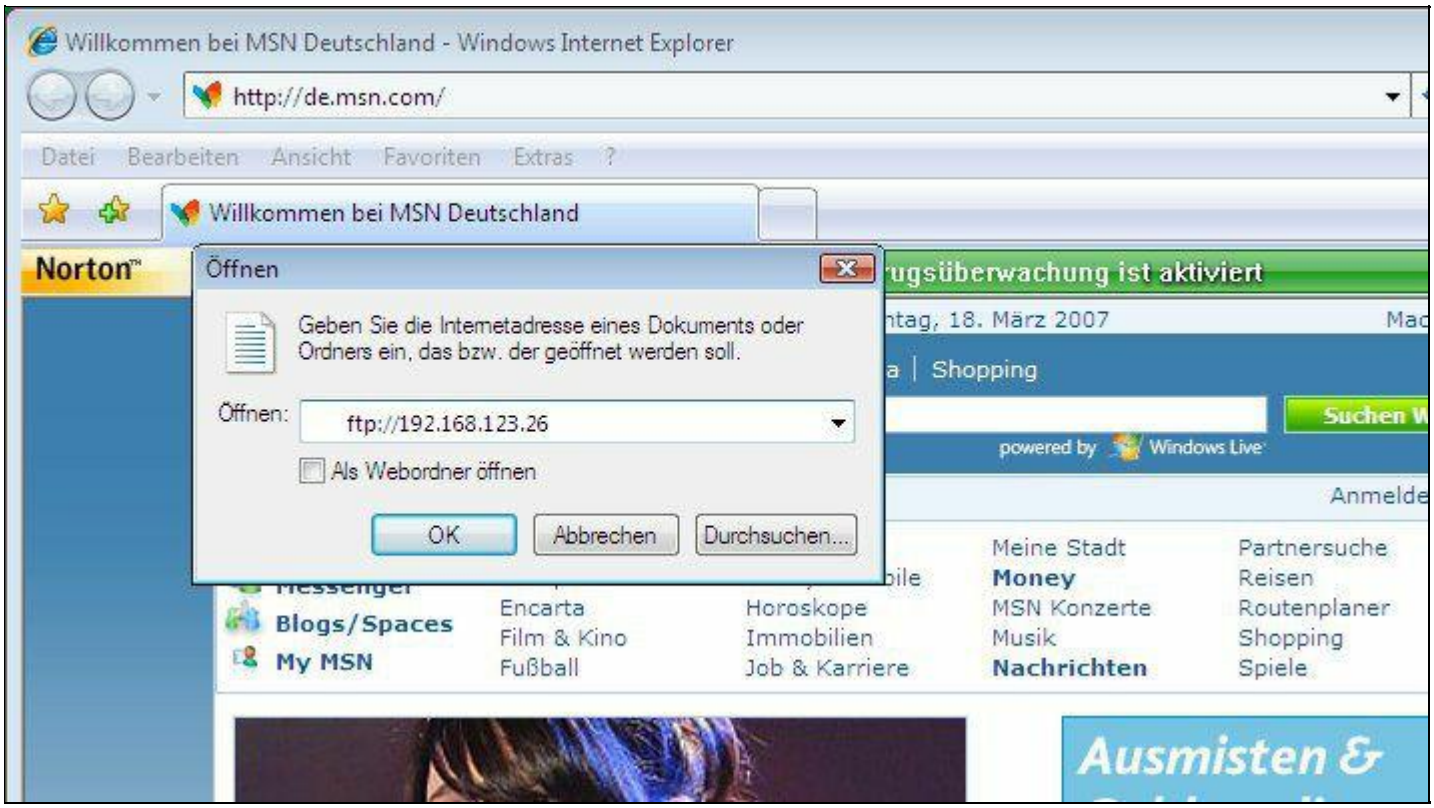


Bild 8.60 Im Webbrowser wählen Sie *Datei/Öffnen* und geben nach *ftp://* die Adresse des FTP-Servers ein. Das kann entweder eine IP-Adresse oder ein DNS-Name sein.

Das geht ganz einfach: Im *Datei öffnen*-Dialog geben Sie den entsprechenden FTP-Server ein. Der Webbrowser erkennt automatisch, ob die Dateien im Binär- oder ASCII-Modus übertragen werden sollen. Noch einfacher geht es mit einem vollwertigen FTP-Client wie FileZilla, mit dem Sie nicht nur Dateien auf einen FTP-Server hochladen, sondern auch mehrere FTP-Server verwalten können.

Stichwortverzeichnis

G

H

I

W

Z

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte Daten sind im Internet über http://dnb.ddb.de abrufbar.

Herausgeber: Ulrich Dorn
EPUB-Bearbeitung und Konvertierung: www.goebel-software.com
Coverart & -design: www.ideehoch2.de

ISBN 978-3-645-22028-6