



Rubrik **Netzwerke**
 Thema **WLAN**
 Umfang **39 Seiten**
 eBook **01464**
 Autor **CHIP Communications GmbH**

Dies eBook zeigt Ihnen, wie Sie ihr WLAN richtig einrichten, absichern, nutzen. Am Beispiel der Fritzbox wird gezeigt, wie ein Router richtig konfiguriert wird.





WLAN optimieren

Absichern - Drucken - Pannenhilfe

eload24 AG
Sonnenhof 3
CH-8808 Pfäffikon SZ

info@eload24.com
www.eload24.com

Copyright © 2011 eload24 AG
(C) 2011 CHIP Communications GmbH
Alle Rechte vorbehalten.

Trotz sorgfältigen Lektorats können sich Fehler einschleichen. Autoren und Verlag sind deshalb dankbar für Anregungen und Hinweise. Jegliche Haftung für Folgen, die auf unvollständige oder fehlerhafte Angaben zurückzuführen sind, ist jedoch ausgeschlossen.

Copyright für Text, Fotos, Illustrationen:
CHIP Communications GmbH

Coverfoto: © Scyza - istockphoto.com

Inhalt

Fritzbox - der Volksrouter	3
Mit der Fritzbox Kontakt aufnehmen.....	3
Fritzbox-Einstellungen sichern	4
Aktuelle Firmware einspielen	4
Nachts herrscht Funkstille.....	5
Energie und Geld sparen	5
Unerwünschte Anrufer ignorieren.....	6
Höhere Reichweite erzielen	6
Auskunftsfreudige Statusanzeige	7
DSL-Problemen auf der Spur	7
Externe USB-Festplatte anschließen	8
USB-Speicher konfigurieren	9
Multimediadateien streamen	10
WLAN zwölfmal schneller	11
Unknackbares WLAN	20
Private Druckerzentrale	27
Worauf kommt es an?	27
Tinte oder Laser?	27
Einrichtung unter Windows XP.....	29
Einrichtung unter Windows Vista.....	29
Einrichtung unter Windows 7.....	30
Pannenhilfe mit System	31

Fritzbox - der Volksrouter

Überdurchschnittlich gut ausgestattet, jede Menge interessante Funktionen und ausgesprochen zuverlässig – für viele Anwender ist die **Fritzbox die erste Wahl**. Wir zeigen, was das Gerät so alles kann.

Ganz gleich ob 3170, 7270 oder das Spitzenmodell 7390 – die vom deutschen Unternehmen AVM entwickelten Fritzbox-Modelle haben hierzulande einen sehr guten Ruf. Dass Fritzboxen von vielen Internet-Providern quasi als kostenlose Dreingabe an Neukunden verteilt werden, ist aber nicht der Hauptgrund

für die Beliebtheit: Die Fritzbox zeichnet sich dadurch aus, dass die Ausstattung stimmt und sich durch Firmwareupdates immer neue Funktionen nachrüsten lassen.

Ganz neu im Angebot ist die Fritzbox 6360 Cable. Die WLAN-Router-Kabelmodem-

Kombination ermöglicht es endlich auch PC-Nutzern, die ihre Internetverbindung über das Fernsehkabel herstellen, in den Genuss einer Fritzbox zu kommen.

In diesem Beitrag zeigen wir Ihnen, wie Sie Ihre Fritzbox perfekt konfigurieren, um vom vollen Funktionsumfang zu profitieren. Wir nutzen die weit verbreitete Fritzbox 7270, doch die Anleitungen lassen sich auch auf viele andere Modelle anwenden, da das Konfigurations-Interface bei den Geräten nahezu identisch ist.

Mit der Fritzbox Kontakt aufnehmen

Um mit dem Fritzbox-Feintuning beginnen zu können, müssen Sie natürlich erst einmal Kontakt mit dem WLAN-Router aufnehmen.

Starten Sie dazu Ihren Internet-Browser und rufen Sie das Installationsmenü der Fritzbox durch Eingabe der URL „fritz.box“ auf. Sollte die Kontaktaufnahme nicht funktionieren, erreichen Sie das Routermenü auch über die IP-Adresse des WLAN-Gerätes. Probieren Sie als Erstes **http://192.168.178.1** aus. Das ist die Einstellung, unter der die Fritzbox im Auslieferungszustand zu erreichen ist.

Sollte das nicht zum Erfolg führen, ermitteln Sie die Adresse, indem Sie unter Windows 7



Erst sichern:
Nachdem Sie die aktuellen Einstellungen gespeichert haben, können Sie mit der Fritzbox herumexperimentieren.

auf „Start“ klicken, in das Suchfeld den Befehl „cmd“ eingeben und mit der Eingabetaste bestätigen. Auf der Kommandozeile tippen Sie den Befehl „ipconfig /all“ ein und drücken die Eingabetaste. Dort finden Sie die Werte für den DHCP-Server und das Gateway, die beide auf die IP-Adresse der Fritzbox verweisen. Nun sollte die Verbindung aber klappen.

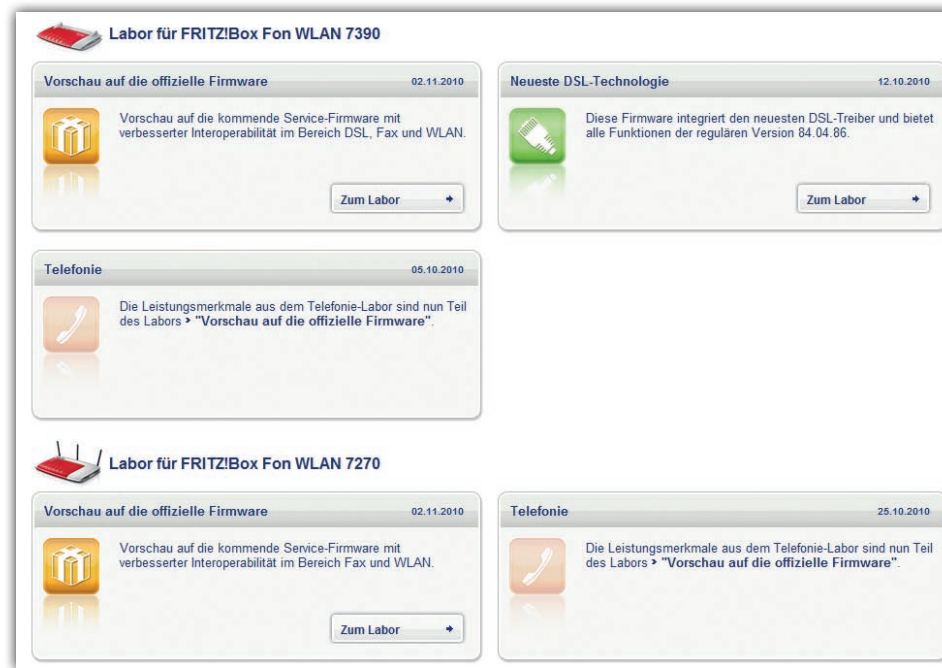
Fritzbox-Einstellungen sichern

Bevor Sie sich an das Update Ihrer Fritzbox machen, sollten Sie alle Einstellungen sichern. Gehen Sie auf „System“ und klicken Sie auf „Einstellungen sichern“. Im Register „Sichern“ können Sie ein Kennwort eingeben, um zu verhindern, dass Unbefugte die von Ihnen angelegte Sicherung einspielen.

Haben Sie vor, die Einstellungen der Fritzbox in ein anderes Gerät zu laden, ist es zwingend erforderlich, die Datei mit einem Passwort zu schützen. Nach einem Klick auf „Sichern“ speichern Sie die Datei, die die etwas kryptische Bezeichnung „FRITZ.Box_Fon_WLAN_7270_v2_54.04.86_05.11.10_0711.export“ hat, auf Festplatte.

Aktuelle Firmware einspielen

Nun können Sie über „System“ und „Firmware-Update“ nach einer neuen Steuerungs-Software für das Gerät suchen. Dazu klicken



Labor-Firmware:
Hiermit erweitern Sie das Funktionsspektrum Ihrer Fritzbox.

Sie auf „Neue Firmware suchen“. Steht eine neue Firmware zum Download bereit, folgen Sie zum Einspielen ganz einfach den Bildschirmmanweisungen.

Experimentierfreudige Nutzer, die gerne eine so genannte Labor-Firmware von www.avm.de/Labor/index.php3 herunterladen und einspielen wollen, gehen anders vor. Zunächst einmal laden Sie die Firmware, die für Ihr Gerät geeignet ist, herunter und speichern diese auf Festplatte. In unserem Beispiel klicken wir auf der Labor-Webseite im Bereich

„Labor für FRITZ!Box Fon WLAN 7270“ auf den Link „zum Labor“, bestätigen die Hinweise mit „Ja, ich habe diesen Hinweis gelesen und möchte jetzt den Download starten“ und laden die für unser Gerät entwickelte, 22,7 MB große Datei mit einem Klick auf „Download“ herunter.

Ist die Firmware-Datei auf Festplatte gespeichert, klicken Sie in der Fritzbox-Konfigurationsmaske auf „System“ und „Firmware-Update“. Wenn Sie das Register „Firmware-Datei“ auswählen, fordert Sie

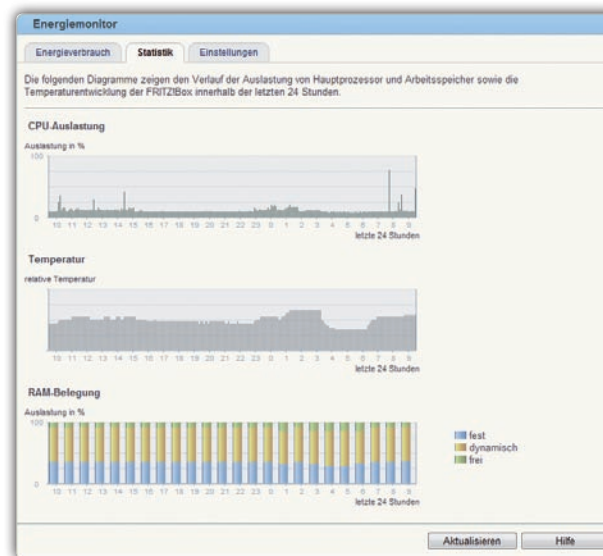
die Fritzbox auf, die aktuellen Einstellungen zu sichern. Dies sollten Sie auch tun. Anschließend können Sie nach einem Klick auf „Durchsuchen“ den Pfad zur soeben heruntergeladenen Firmware-Datei angeben. In unserem Beispiel lautet der Dateiname „fritzbox-labor-7270v2-18563.zip“.

Ein abschließender Klick auf die Schaltfläche „Update“ leitet die Firmware-Aktualisierung ein. Nach Abschluss des Updates startet die Fritzbox dann neu.

Nachts herrscht Funkstille

Doch auch in der Standardversion der aktuellen Firmware gibt es eine Reihe interessanter Funktionen, die Ihnen helfen, Ihr WLAN auf Vordermann zu bringen. Zunächst einmal sollten Sie die Expertenansicht aktivieren, damit Ihnen alle Optionen zur Verfügung stehen. Diese Darstellung können Sie unter „System“ und „Ansicht“ einschalten.

Wenn Sie nicht häufig nächtliche Downloads planen, ist es mehr als ratsam, die Nachtschaltung Ihrer Fritzbox zu aktivieren. Klicken Sie auf „System“, wählen Sie „Nachtschaltung“ und geben Sie im Register „WLAN“ an, wann Ihr Drahtlos-Netzwerk Feierabend machen kann. Arbeiten Sie dagegen regelmäßig länger, sollten Sie zusätzlich die Option „Das Funknetz wird



Statistik: Interessante Informationen rund um Ihre Fritzbox finden Sie im Bereich „Statistik“.

erst abgeschaltet, wenn kein WLAN-Netzwerkgerät mehr aktiv ist“ auswählen. Soll auch der Klingelton zeitgesteuert deaktiviert werden, legen Sie im Register „Klingelsperre“ fest, zu welchen Uhrzeiten Ruhe herrschen soll.

Energie und Geld sparen

Für kostenbewusste Anwender ist der „Energiemonitor“ von Interesse, der sich ebenfalls in der Rubrik „System“ findet.

Das Register „Energieverbrauch“ informiert Sie über den aktuellen Energieverbrauch und

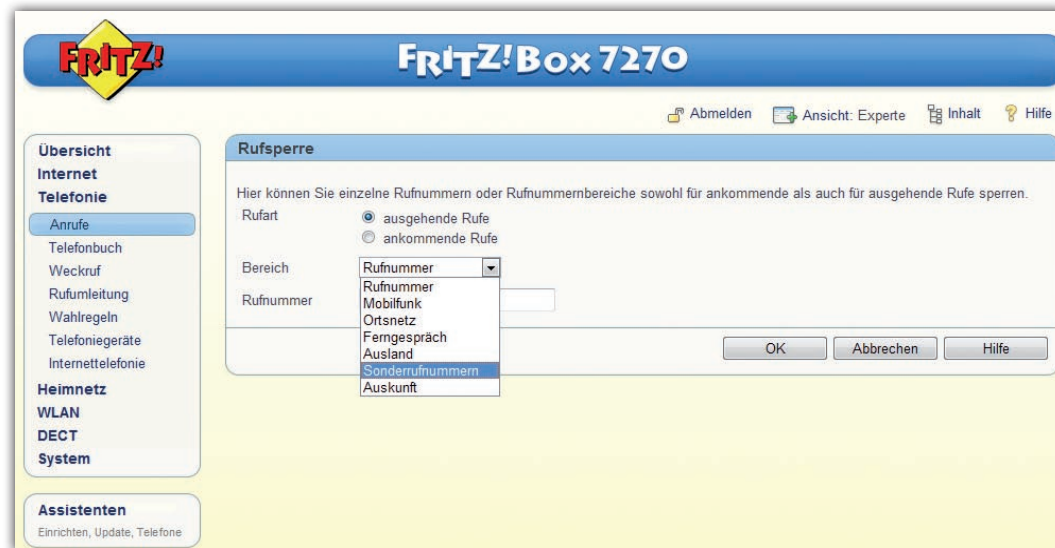
Tipp

Netzwerkfähig dank Streaming-Stick

Geräte, die einen USB-Port, aber keine Netzwerkschnittstelle besitzen, gelangen mit dem pffiffigen AVM Streaming-Stick ins Wireless LAN. Für die Streaming-Funktion benötigen Sie einen Fritz WLAN-USB-Stick 1.1. Das ist die alte Generation mit dem WLAN-g-Standard und einer Bruttoübertragungsrate von 54 MBit/s, neuere n-Sticks funktionieren leider nicht. In der Praxis erzielen Sie mit dem Fritz WLAN-USB-Stick 1.1 Nettotransferraten von 20 bis 25 MBit/s. Das reicht für das Streamen von Musik und das Bereitstellen von Bildern. Bei der Wiedergabe von Videos kann es in Extremfällen aber zu Aussetzern kommen.

die mittleren Verbrauchswerte der letzten 24 Stunden. Im Bereich „Statistik“ erhalten Sie Details zu „CPU-Auslastung“, „Temperatur“ und „RAM-Belegung“.

Zum Abschalten nicht benötigter LAN-Anschlüsse klicken Sie auf die Registerkarte „Einstellungen“. Für die vier LAN-Anschlüsse der Fritzbox stehen Ihnen die Varianten „immer aktivieren“, „automatische Erkennung“ und „deaktiviert“ zur Verfügung, wobei der erste Anschluss – LAN1 – immer nur die ersten beiden Werte aufweisen kann. Haben Sie diese Einstellungen geändert, klicken Sie zum Speichern auf „Übernehmen“.



Unerwünschte Anrufer ignorieren

In den erweiterten Einstellungen des Telefoniemoduls, das Sie über Klicks auf „Telefonie“, „Anrufe“ und „Anrufe sperren“ erreichen, bietet Ihnen die Fritzbox die Möglichkeit zum Blockieren von Anrufern mit bekannten sowie unterdrückten Rufnummern. Außerdem können Sie mit dieser Funktion verhindern, dass sich bestimmte Telefonnummern anwählen lassen. Dies ist vor allem bei ausgehenden Anrufen hilfreich, wenn Sie Ihre Kosten unter Kontrolle halten möchten. Eine weitere Einsatzmöglichkeit: Eltern können damit verhindern, dass ihre Kinder unkontrolliert in der Weltgeschichte herumtelefonieren.

Klicken Sie auf die Schaltfläche „Neue Rufsperrung“, wählen Sie aus, ob Sie einen ankommenden oder ausgehenden Anruf sperren wollen, tippen Sie bei „Rufnummer“ die gewünschte Telefonnummer ein und bestätigen Sie mit einem Klick auf „OK“. Sollten hingegen alle Anrufer, bei denen die Rufnummernanzeige unterdrückt ist, ignoriert werden, wählen Sie bei Bereich „Ohne Rufnummer“ aus.

Praktisch: Mithilfe der im Ausklappenmenü bei „Bereich“ bereits vorkonfigurierten Sperren können Sie unter anderem alle Telefonate mit Mobilfunknummern, Sonderrufnummern und der Auskunft unterbinden.

Höhere Reichweite erzielen

Wie bereits an anderer Stelle erwähnt, lässt sich die Fritzbox auch als Repeater verwenden, um so die Reichweite des WLANs zu erhöhen. Neben der Fritzbox benötigen Sie dazu ein zweites Gerät, das den Standard WDS (Wireless Distributed System) unterstützt, im Idealfall ist das natürlich auch eine Fritzbox.

Volle Kontrolle: Legen Sie fest, welche ankommenden und ausgehenden Gespräche erlaubt sind.

Überprüfen Sie zunächst einmal die Firmware Ihrer geplanten Repeater-Station – falls die Version niedriger ist als xx.04.06, ist eine Aktualisierung unumgänglich. Aktivieren Sie dann die Expertenansicht, gehen Sie auf „WLAN“ und „Funkeinstellungen“ und schalten Sie Ihr Funknetz an.

Für die nächsten Arbeitsschritte auf der Basisstation benötigen Sie die MAC-Adresse Ihres Repeaters. Die finden Sie unter „WLAN“ und „Funkeinstellungen“ im Bereich „Funknetz“ bei „MAC-Adresse dieser FRITZ!Box“.

Wichtig ist, dass die Basisstation und die angeschlossenen Repeater jeweils den gleichen Funkkanal nutzen. Passen Sie diesen im Router, der zukünftig als Repeater fungieren soll, an. Den aktuellen Funkkanal der Basisstation finden Sie über Klicks auf „WLAN“ und „Funkkanal“ heraus.

WDS

Mit WDS (Wireless Distribution System) können Sie die Reichweite Ihres WLAN-Funknetzes vergrößern, zum Beispiel mit einer weiteren FRITZ!Box. Das Gerät, das den Internetzugang herstellt, dient als Basisstation, das andere als Repeater.

Hinweise

- Alle verwendeten WLAN-Geräte müssen das Verfahren WDS unterstützen. Der AVM FRITZ!WLAN Repeater funktioniert nicht nach dem WDS-Verfahren. Verwenden Sie für seine Einrichtung das Verfahren [WPS](#).
- Die WDS-Basisstation und alle WDS-Repeater müssen auf dem selben Funkkanal arbeiten. Deshalb darf in der FRITZ!Box nicht die Funktion 'Autokanal' eingestellt sein. Die Einstellung für den Funkkanal können Sie auf der Seite '[Funkkanal](#)' ändern.
- Die Verbindungen zwischen der WDS-Basisstation und den WDSRepeatern müssen mit der gleichen Verschlüsselung gesichert sein.

☒ WDS aktiv

Betriebsart

☒ Basisstation
Diese FRITZ!Box ist eine Basisstation für andere Repeater.

☐ Repeater
Diese FRITZ!Box ist ein Repeater für eine andere Basisstation.

Repeater-Auswahl

Wählen Sie hier das WLAN-Gerät, das in Ihrem WLAN-Funknetz als Repeater arbeiten soll. Sie können bis zu 3 Geräte auswählen und als Repeater verwenden. Die Liste enthält alle WLAN-Geräte, die in Ihrer Umgebung gefunden wurden und die Geräte, die Sie selbst hinzugefügt haben.

WLAN-Geräte

	Name(SSID)	Kanal	MAC-Adresse
<input checked="" type="checkbox"/>	CHFB	11	00:1F:3F:D5:23:FE
<input type="checkbox"/>	ZombieNet	6	00:13:49:68:71:A5

WLAN-Leistung erhöhen: Mittels WDS können Sie mehrere Fritzboxen zusammenschalten.

Bei der Konfiguration des Repeaters gehen Sie genauso vor. Einziger Unterschied: Nachdem Sie „WDS aktiv“ angeklickt haben, wählen Sie „Repeater“ aus. Wenn Sie in der Basisstation die Art der Verschlüsselung festgelegt haben, müssen Sie im Repeater natürlich die gleichen Werte setzen.

Auskunftsfreudige Statusanzeige

Als in der Praxis sehr hilfreich hat sich die Info-LED entpuppt. Denn das Lämpchen kann weit mehr als nur den Status der WLAN-Verbindung anzeigen. Klicken Sie auf „System“, „Info-Anzeige“, um selbst vorzugeben, wann das Lämpchen blinken respektive leuchten soll. Zur Auswahl stehen unter anderem „Anruf in Abwesenheit – LED blinkt“, „Neue Nachricht im Anrufbeantworter – LED blinkt“ und „Gerät über USB angeschlossen – LED leuchtet“. Wählen Sie die gewünschte Funktion aus und bestätigen Sie mit „Übernehmen“.

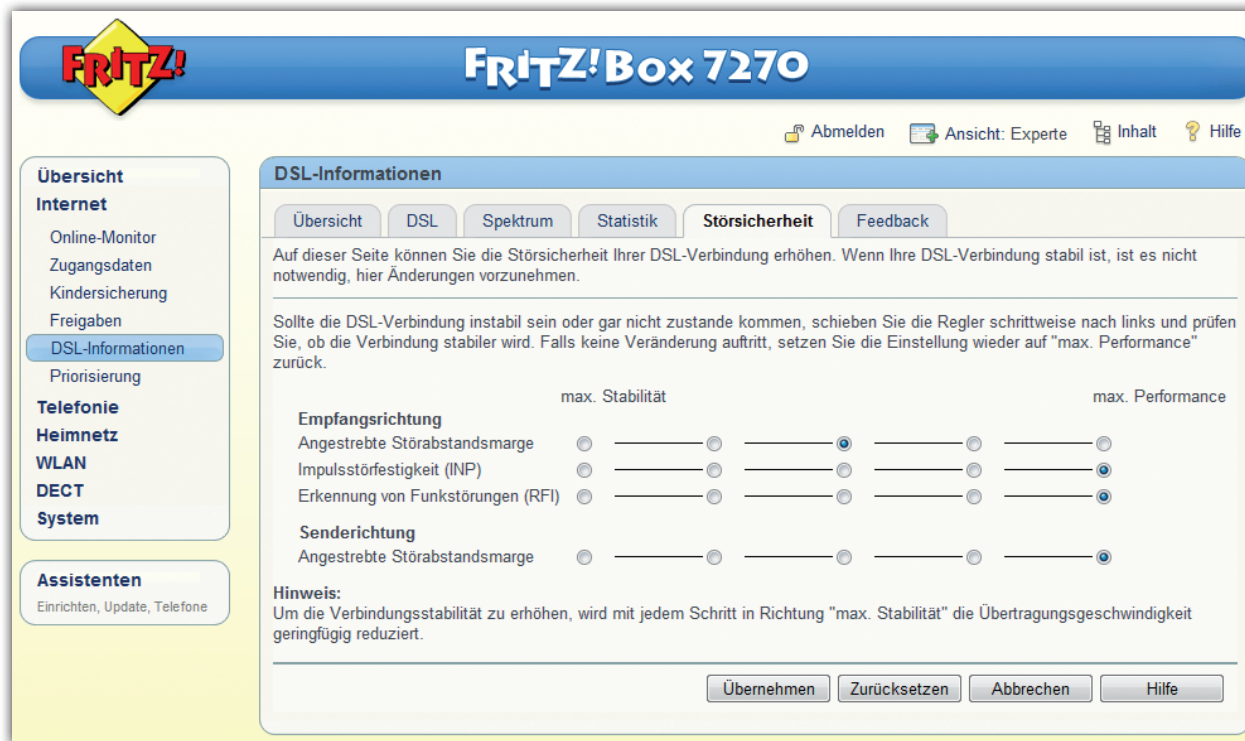
DSL-Problemen auf der Spur

Hilfreich für alle Nutzer, die Probleme mit ihrer DSL-Verbindung haben, sind die im Bereich „Internet“ und „DSL-Informationen“ zusammengefassten Angaben. So erfahren Sie etwa durch einen Blick in das Register „Übersicht“, wie lange die Internetverbindung bereits steht, wie schnell Daten herunter- und hochgeladen werden und mit

Wechseln Sie nun in das Menü „WLAN“, „WDS“ und schalten Sie die WDS-Funktion ein, indem Sie die Option „WDS aktiv“ anklicken. Definieren Sie diesen Router als „Basisstation“ und wählen Sie im Bereich „WLAN-Geräte“ die Komponente aus, die als Repeater fungieren soll. Sollte der Router nicht in der Liste aufgeführt sein, klicken Sie auf „WLAN-Gerät hinzufügen“,

geben die MAC-Adresse an und bestätigen mit „Übernehmen.“

Im Bereich „Sicherheit“ aktivieren Sie „WPA2-Verschlüsselung“ und wählen ein sicheres Passwort. Zum Schluss notieren Sie sich die MAC-Adresse der Basisstation und bauen die Verbindung zum Repeater auf.



Stabilere Internetverbindung: Hakt es mal wieder oder treten Aussetzer auf, können die im Bereich „Störsicherheit“ untergebrachten Funktionen Abhilfe schaffen.

welcher Vermittlungsstelle die Fritzbox verbunden ist. Wesentlich detaillierter – und vor allem bei der Fehlersuche für Techniker interessant – sind die Angaben, die Ihnen im Register „DSL“ präsentiert werden.

Und wer gerne experimentiert, sollte einen Blick auf das Register „Störsicherheit“ werfen. Denn hier können Sie die Fritzbox mit

wenigen Mausklicks so konfigurieren, dass die Stabilität der DSL-Verbindung erhöht wird. Falsch machen können Sie nichts, da Sie die Grundeinstellung jederzeit wieder aktivieren können. Klicken Sie bei allen Einträgen die Option „max. Performance“ an und bestätigen Sie mit „Übernehmen“. Daraufhin wird die DSL-Verbindung getrennt und sofort wiederhergestellt. Sollte

es dann zu Übertragungsproblemen kommen, stellen Sie den Originalzustand wieder her.

Andersherum funktioniert es natürlich auch. Kommt es zu Verbindungsabbrüchen oder anderen Problemen, sollten Sie sich bei allen Parametern für „max. Stabilität“ entscheiden. Möglicherweise reicht dieser Eingriff aus, um zukünftig störungsfrei im Internet unterwegs zu sein.

Externe USB-Festplatte anschließen

Dank USB-Port lassen sich an der Fritzbox auch externe Speichermedien anschließen. Der Sinn der Sache? Darauf gespeicherte Multimediainhalte lassen sich im ganzen Heimnetzwerk streamen. Wir gehen davon aus, dass Sie die Festplatte bereits mit entsprechenden Inhalten gefüllt haben, etwa mit MP3-Musik.

Trennen Sie die externe Festplatte vom PC und stecken Sie sie am USB-Port der Fritzbox ein. Beachten Sie, dass es sich um ein Festplattengehäuse mit einer eigenen Stromversorgung handeln sollte. Falls Sie mehr als eine Festplatte nutzen möchten, schließen Sie an die Fritzbox einen aktiven USB-Hub an und an ihn bis zu drei USB-Speicher. Erkennt die Fritzbox die externe



Vielfältig sind die Optionen, die die Fritzbox bei der Konfiguration eines USB-Speichers anbietet.

Festplatte, wird sie in der Verwaltungsmaske unter „Heimnetz“, „USB-Geräte“ und „Geräteübersicht“ angezeigt.

Falls Sie keine externe Festplatte zur Hand haben, können Sie natürlich auch einen USB-Stick verwenden. Auf einen 4-GB-Byte-Stick passen rund 1.000 MP3-Songs.

USB-Speicher konfigurieren

Im Bereich „Heimnetz“, „USB-Geräte“ bringen Sie das Register „Geräteübersicht“ nach vorne und klicken unter „Aktivierte Optionen“ auf „Einstellungen“. Sie gelangen in den Bereich „Speicher (NAS)“. Im Register „Sicherheit“ ist als Berechtigung für den Netzwerkzugriff – „im Heimnetz“ und „aus dem Internet“ – standardmäßig

die Option „lesen und schreiben“ gesetzt. Übernehmen Sie die Einstellung, um den Speicher auch zukünftig mit neuen Daten befüllen zu können. Aktivieren Sie den Kennwortschutz nicht, da nicht alle Player die Möglichkeit bieten, das Passwort für Zugriff auf den Speicher einzugeben.

Interessant ist die im Register „Aktivierung“ untergebrachte Option „Speicher für Benutzer aus dem Internet freigeben“. Ist diese Option aktiviert, können Sie sich mit jedem internetfähigen PC an der Fritzbox anmelden und Dateien auf den Speicher kopieren und laden. Das ist praktisch, wenn Sie etwa Ihre Fotos noch direkt vom Urlaubsort sichern möchten.

Info

Das etwas andere Streaming: Fritz WLAN Repeater N/G

Die Hauptaufgabe des rund 70 Euro teuren Fritz WLAN Repeater N/G von AVM ist es, ein Heimfunknetzwerk einfach zu erweitern und eine größere Reichweite zu erzielen. Dazu wird der Repeater einfach in eine Steckdose eingesteckt und über das Webinterface vom PC aus konfiguriert. Die Entwickler haben sich noch ein ganz besonderes Extra einfallen lassen: Dank der Audioanschlüsse kann der Repeater beliebige Audioinhalte mithilfe eines Kabels an eine Stereoanlage übermitteln.

Als Audioquelle kann dabei ein Windows-Programm, beispielsweise der Windows Media Player 12, dienen. Dazu muss am Computer das Programm für die Audiobrücke installiert werden. Die Stereoanlage schließen Sie dann per Kabel (digital oder analog) an den Fritz WLAN Repeater an. Wenn Sie nun mit dem Mediaplayer Musik am PC wiedergeben und die Stereoanlage entsprechend konfiguriert ist, hören Sie dort das Gleiche wie am PC.

Falls das Abspielgerät keine Anschlussmöglichkeit für Kabel bietet, aktivieren Sie den UKW-Sender im Fritz WLAN Repeater N/G und stellen Sie ein Radio auf die entsprechende Frequenz ein. So nutzen Sie jedes handelsübliche UKW-Radio als Empfänger für Musikinhalte.

Um in den Genuss der Streaming-Funktion der Fritzbox zu kommen, müssen Sie die Option „Mediaserver aktiv“ einschalten. Dann erst können zum UPnP-AV-Standard kompatible Abspielgeräte auf Musik, Bilder und Videos zugreifen, die Sie auf dem Netzwerkspeicher abgelegt haben. Ist der USB-Speicher mit der Fritzbox verbunden und ist die UPnP-Musikbox aktiviert, wird im Hintergrund automatisch eine Datenbank angelegt. Aus ihr baut die Fritzbox die Titelliste für den UPnP-Media-Server auf. Die Box erkennt übrigens auch Musikdateien in Unterordnern.

Tipp: Die Energiesparfunktion für USB-Festplatten sollten Sie im Bereich „USB-Geräte“ aktivieren und die Vorgabe „10 Minuten“ beibehalten. Klicken Sie auf den Button „Übernehmen“. Die Vorbereitungen sind abgeschlossen und Sie können endlich mit einem ersten Streaming-Test beginnen.

Multimediadateien streamen

Am Windows-7-Rechner öffnen Sie den Windows-Explorer. Klicken Sie in der linken Spalte auf „Netzwerk“, um im rechten Fensterbereich alle Netzwerkgeräte anzuzeigen. Im Abschnitt „Multimedia“ sollte der Eintrag „AVM FRITZ!Mediaserver“ auftauchen. Das ist der soeben eingerichtete Netzwerkspeicher.

Per Doppelklick auf das Symbol oder über das Kontextmenü der rechten Maustaste rufen Sie den Windows Media Player auf. Hier klicken Sie links unten in der Oberfläche auf „AVM FRITZ!Mediaserver“. Rechts im Fenster werden nun die Symbole „Musik“, „Videos“, „Bilder“, „TV-Aufzeichnungen“ und „Wiedergabelisten“ angezeigt. Klicken Sie auf „Musik“ und danach etwa auf „Interpret“ oder „Album“, um einen Titel zur Wiedergabe zu öffnen.

Klappt das, arbeitet der Speicher an der Fritzbox, wie er soll, und Sie können weitere Geräte verbinden. Dabei kann es sich um weitere Computer handeln oder auch um ein Abspielgerät im Wohnzimmer

Artur Hoffmann

WLAN zwölfmal schneller

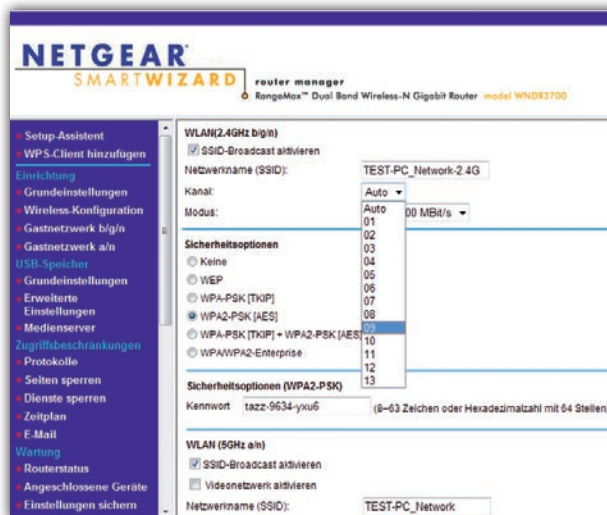
Wenn die Daten mal wieder durch das WLAN tröpfeln und die Signalstärke nahezu gegen null geht, ist guter Rat teuer. Unsere **zwölf Tipps gegen WLAN-Frust** verhelfen Ihnen zu einem flotteren Funknetz.

Nahezu jeder WLAN-Nutzer weiß, dass die Übertragungsleistung nicht jederzeit optimal ist. Es kann immer wieder zu nervigen Signalaussetzern kommen. Selbst wenn Sie einen besonders leistungsstarken Router kaufen, sind Sie davor nicht gefeit. Denn in einem Haus oder einer größeren Wohnung ist der Empfang nie überall ganz ungestört.

Der Hintergrund ist, dass die Hersteller der Funker zwar auf neueste Antennentechnik setzen, die hohen Datendurchsatz bringt – allerdings nur in einem relativ kleinen Umkreis. Eine Schwachstelle sind häufig die kleinen Standardantennen. Selbst die auf dem ersten Platz der CHIP-Bestenliste stehende Fritzbox Fon WLAN 7390 hat nur eine mittelmäßige Reichweite. Doch diese Probleme lassen sich lösen – mit WLAN-Tuning der ganz besonderen Art.

Wir zeigen, wie Sie Ihrem Router mit starken Antennen zu 60 Prozent mehr Leistung verhelfen und so weiter als mit jedem normalen

Gerät funken. Außerdem geben wir Ihnen handfeste Tipps zum Firmware-Tuning und für die Wahl des perfekten Router-Standorts. Der erste Abschnitt des Beitrags beinhaltet allgemeine Tipps und Tricks, im zweiten Teil geht's dann ans Eingemachte.



Der beste Funkkanal: Oft genügt es, den vom WLAN-Router genutzten Kanal zu ändern, um die Leistung zu verbessern.

1 Auf anderem Kanal schneller funken

Das 2,4-GHz-Frequenzband, das die meisten WLAN-Netze nutzen, ist im Haushalt übersät mit Störquellen wie Mikrowellenherden, DECT-Telefonen und Bluetooth-Handys. Die schlechte Nachricht: Fürs deutsche WLAN stehen zwar offiziell 13 Kanäle zur Verfügung (2,412 GHz bis 2,472 GHz), die jeweils eine Bandbreite von 20 MHz haben. Allerdings können immer nur drei Kanäle parallel genutzt werden, ohne sich gegenseitig zu stören.

Als Faustregel gilt: Bei Netzwerken, die räumlich dicht beieinanderstehen, sollte zwischen zwei benutzten Kanälen ein Abstand von mindestens fünf Kanälen liegen. Mit dem englischsprachigen Freeware-Tool Easy WiFi Radar 1.0 (www.makayama.com) finden Sie ganz genau heraus, welche Kanäle die Funker in Ihrer Umgebung nutzen.

Praktische Funktion: Moderne WLAN-Router wie die Fritzbox suchen automatisch nach dem besten Kanal. Falls diese Option bei Ihrem Modell fehlt, stellen Sie den besten Kanal einfach selbst ein. Dazu rufen Sie die Konfigurations-Maske Ihres WLAN-Routers im Browser auf, wechseln in die entsprechende Rubrik und geben manuell ein, welcher Kanal verwendet werden soll.

Tipp: Sind alle Kanäle belegt, nutzen Sie den Kanal, auf dem sich die stärksten Nachbarnetze tummeln. Das hört sich absurd an, hat aber einen praktischen Hintergrund: Diese deutlichen Signale kann Ihr Router besser von den eigenen Signalen trennen als schwache Pakete.

2 Genutztes Frequenzband wechseln

Bringt die Auswahl des besten WLAN-Kanals keinen großen Geschwindigkeits- und Reichweitenvorteil und sind Sie im Besitz eines Dualband-Routers, sollten Sie das Frequenzband wechseln – von 2,4 auf 5 GHz.



Schneller und weiter: Mit Zusatzantennen schalten Sie den WLAN-Turbo ein.

Dualband-Router setzen – wie es die Bezeichnung bereits verrät – auf beide Funkbänder. Sie binden 2,4-GHz-Geräte ein und funken zusätzlich störungsfrei auf dem weitgehend ungenutzten 5-GHz-Band. Voraussetzung ist allerdings ein 5-GHz-Adapter am PC, der auf dieser Frequenz funken kann.

Solche Geräte sind nicht besonders teuer und werden inzwischen von verschiedenen Herstellern angeboten. Aktuelle Notebooks beherrschen die 5-GHz-Frequenz von vornherein, sodass Sie in dem Fall kein Geld in ein Extra-Gerät investieren müssen.

3 Ausstattung: Antennen finden

Am Beispiel der weit verbreiteten Fritzbox 7390 zeigen wir Ihnen Schritt für Schritt, wie Sie Ihren Router aufrüsten; bei anderen Modellen funktioniert das meist analog. Vor allem Fenster, dicke Wände und Störstrahlungen elektronischer Geräte machen den Funkern zu schaffen. Das Lösungswort heißt: Sendeleistung. Die ist ab Werk oft zu gering, obwohl die Router mehr bringen könnten. In der Regel liegt das an den schwachen Antennen. Obwohl es starke Antennen mit bis zu 20 dBi Gewinn gibt (im Vergleich zum Normstrahler), finden sich in den Standardroutern gerade einmal Funkstäbe mit 2 dBi. Die Lösung ist also eigentlich simpel: Neue Antennen müssen her. Das Schwierige dabei ist



Ein spezieller Adapter erleichtert das Tuning.

die richtige Auswahl und der passende Anschluss. Für die Fritzbox empfiehlt sich die kostengünstige, 19 Zentimeter lange Antenne TL-ANT2405C von TP-Link mit 5 dBi (www.amazon.de, ca. sieben Euro). In unserem Test konnten wir mit ihr ein Leistungsplus von 60 Prozent erreichen. Sie arbeitet omnidirektional, strahlt also um 360 Grad. Wollen Sie gezielt die Funkwellen in eine Richtung lenken, nutzen Sie besser eine Richtfunkversion. Die müssen Sie nicht für teures Geld kaufen, wie Sie im Abschnitt „WLAN-Antenne im Eigenbau“ (Tipp 5) erfahren.

Achtung: Bei Routern nach 802.11n-Standard, die 300 MBit/s übertragen, benötigen Sie zwei Antennen. Den Tempogewinn erreichen die Geräte durch einen Trick: Spatial

Multiplexing (räumliche Datenübertragung). Dabei teilt der Router die zu übertragenden Bits auf zwei Datenkanäle auf, was theoretisch bis zu 100 Prozent mehr Geschwindigkeit bringt. Die einzelnen Kanäle unterscheiden sich nur durch ihre räumlichen Signaturen, also die Richtungen, aus denen die Signale bei den Antennen ankommen. Dazu müssen Sie letztere noch speziell ausrichten.



WLAN-Router-Tuning mithilfe einer alten CD-Spindel – so etwas funktioniert in der Praxis tatsächlich reibungslos.

4 Anpassung: Adapter verwenden

Ist Ihr Router nicht mit einer Schraubantenne ausgestattet, sondern vertraut er wie die Fritzbox auf eine interne Variante, benötigen Sie einen Adapter, um die Antennen auf dem Board des Routers anzubringen. Diesen können Sie natürlich selbst

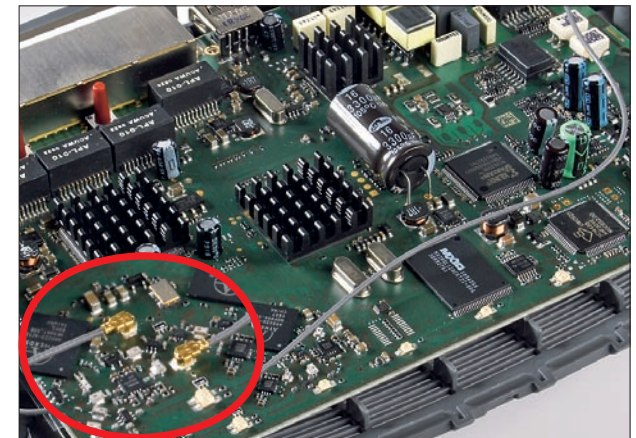
bauen, die Einzelteile kosten aber fast genauso viel wie das fertige Produkt. Für die Fritzbox braucht es pro Antenne ein Adapterkabel von einer RP-SMA-Buchse auf einen Ultraflach-Stecker, etwa das 40835B von InLine (www.inline-info.de, ca. zwei Euro).

Auf den Seiten von InLine finden Sie aber auch noch weitere Adaptervarianten für Router anderer Hersteller. Achten Sie dabei auf die Länge des Kabels. Für Fritzboxen passen die Adapter auf jeden Fall – bei anderen Herstellern sollten Sie zuerst das Gerät öffnen und die erforderliche Kabellänge prüfen.

5 WLAN-Antenne im Eigenbau

Wer nicht viel Geld ausgeben will, um die Leistung seines Funknetzwerkes spürbar zu steigern, kann sich seine Antenne selbst bauen. Ein wenig handwerkliches Geschick vorausgesetzt, machen Sie mit einer Antenne Marke Eigenbau aus Ihrem schlappen WLAN ein waschechtes Turbo-Funknetzwerk.

Beispielsweise richtet eine aufsteckbare Parabolantenne die Signale wesentlich zielgerichteter in eine Richtung als die Standardantennen der Hersteller. Diese Variante ist vor allem dann zu empfehlen, wenn Hindernisse die Funkverbindung empfindlich stören. In diesen Fällen bringt das Eigenbau-Parabol-Modell spürbar mehr



Vorsicht! Beim Lösen der MIMO-Antennen ist eine ruhige Hand gefragt.

Datendurchsatz, wie unsere Versuche im CHIP-Labor gezeigt haben.

Und mit dem Rundstrahler von Vallstedt Networks (www.vallstedt-networks.de) gewinnen Sie bei alten WLAN- Routern immerhin 10 dB. Kein Scherz: Als Basis dient eine alte CD-Spindel. Wer diese Richtantenne nachbauen will, muss allerdings mit einem LötKolben umgehen können. Hinweis: Aktuelle Router-Modelle nach dem 802.11n-Standard funktionieren mit dieser Antenne nicht.

Für Router mit zwei Antennenanschlüssen basteln Sie eine Doppel-Parabolantenne. Sie sendet die Signale gebündelt in eine Richtung. Als Baumaterial dient Pappe, die Sie

mit Metallfolie bekleben. Die englischsprachige Bauanleitung finden Sie unter www.freeantennas.com. Auf dieser Webseite erwarten Sie noch weitere Schritt-für-Schritt-Anleitungen, sodass Sie auch andere Antennen nachbauen können.

6 Einbau: Router aufrüsten

Um bei der Fritzbox 7390 die Antennen zu wechseln, müssen Sie das Gerät zunächst öffnen. Dazu benötigen Sie einen Torx-Schraubendreher der Größe T6 (www.conrad.de, ca. sechs Euro). Mit diesem lösen Sie die vier Schrauben auf der Unterseite des Routers.

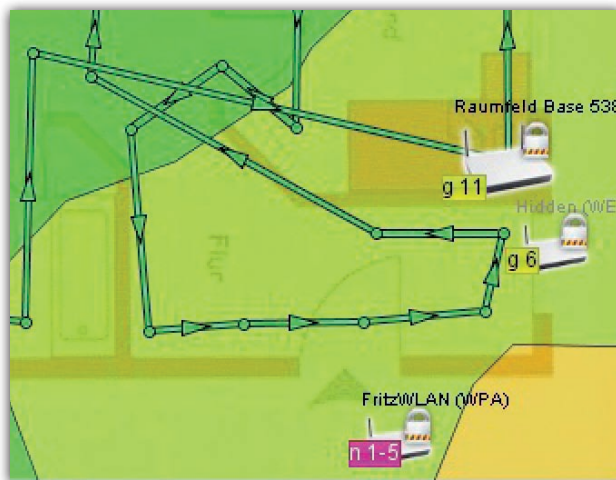
Hinweis: Zwei Schrauben verstecken sich unter den vorderen Gummifüßen. Um den Deckel abzuheben, drücken Sie mit einem Kreuzschlitz-Schraubendreher oder einem stumpfen Messer die Nut (in der Mitte an der Oberseite, vorn) zur Seite. Dann lösen Sie vorsichtig den Deckel. Die beiden integrierten MIMO-Antennen können Sie relativ einfach aus der Halterung ziehen; die Anschlusskabel lösen Sie mithilfe eines kleinen Schlitz-Schraubendrehers ganz vorsichtig vom Board, indem Sie die Stecker an jeder Seite leicht anheben.

Für die neuen Antennen müssen Sie nicht einmal Löcher bohren. Führen Sie einfach

die Kabel durch die vorgebohrten Wandhalterungen an der Unterseite der Fritzbox. Dann drücken Sie die Kabel sanft auf beide Stecker des Boards und schließen die Fritzbox wieder. Die anderen Kabeln können Sie nun mit den Antennen verschrauben.

7 Optimierung: Antennen ausrichten

Verfügt Ihr Router wie die Fritzbox über mehrere Antennen, gilt es noch, die Strahler richtig auszurichten, da sonst die einzelnen Funkwellen interferieren und sich auslöschen, sobald ein Wellental auf einen Wellenberg trifft.



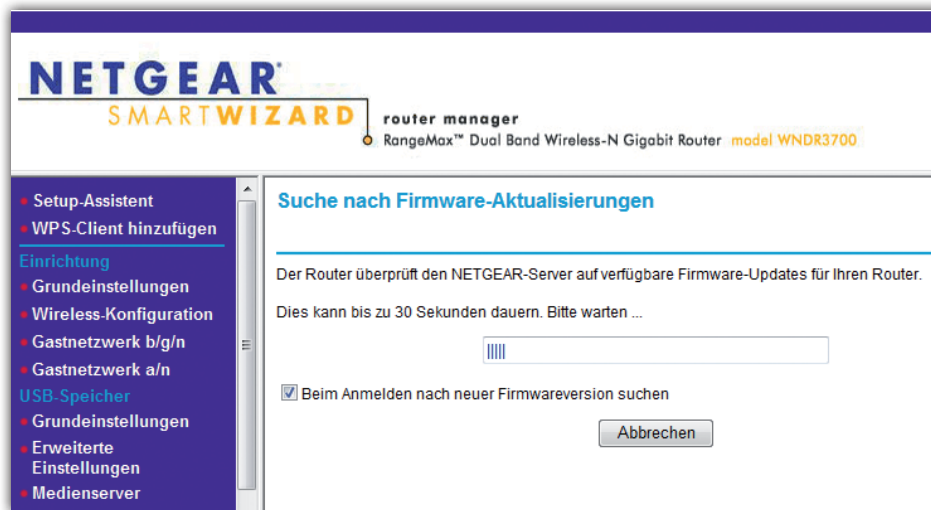
Signal-Karte: Mit dem Tool HeatMapper finden Sie den optimalen Routerstandort.

Damit alles optimal funktioniert, müssen die Antennen mindestens eine Wellenlänge oder ein Vielfaches davon auseinander stehen – bei den WLAN-Signalen sind das rund zwölf Zentimeter. Die Wellenlänge erhält man, wenn man die Ausbreitungsgeschwindigkeit (also die Lichtgeschwindigkeit) durch die Frequenz teilt, die im WLAN auf 2,4 GHz (IEEE 802.11g) festgelegt ist. Die TP-Link-Antennen sind mit einem Magnetfuß ausgestattet, sie lassen sich also perfekt – zum Beispiel an der Unterseite von Metallregalen – aufhängen.

8 Tuning: Optimalen Standort finden

Im eBook (Nr. 01463 »Der Weg zum perfekten WLAN«) haben wir Ihnen gezeigt, nach welchen Kriterien Sie den optimalen Aufstellort für Ihren WLAN-Router finden. Reicht die Sendeleistung dennoch nicht aus, um im ganzen Haus drahtlos surfen zu können, müssen Sie härtere Geschütze auffahren und die englischsprachige Freeware HeatMapper 1.02 (www.ekahau.com) einsetzen.

Zuerst legen Sie fest, wo Sie surfen wollen – egal, ob auf der Couch oder im Garten, HeatMapper findet entsprechend dazu immer den perfekten Router-Standort. Nach der Installation der Software auf einem Notebook sollten Sie in Ihren Unterlagen nach dem



Grundriss Ihrer Wohnung suchen und diesen als Bilddatei einscannen. Starten Sie die Software, wählen Sie die Option „I have a map image“ und laden Sie Ihren Grundriss. Dann stellen Sie Ihr Notebook an den zuvor ausgewählten Surfstandpunkt. Bewegen Sie sich anschließend mit dem eingeschalteten Router langsam durch Ihre Wohnung – HeatMapper denkt dann, dass sich der Rechner bewegt. Parallel machen Sie alle paar Schritte auf dem angezeigten Grundriss einen Mausklick an der Stelle im Plan, an der Sie sich in der Wohnung befinden.

Um den perfekten Standort für Ihren Router zu finden, drücken Sie die rechte Maustaste in HeatMapper; es erscheint eine „Heatmap“,

die über Ihren Grundriss gelegt ist. Diese zeigt, an welchen Stellen der Wohnung der WLAN-Empfang sehr gut ist (grün), wo weniger gut (gelb) und auch, welche Bereiche schlechten Empfang (rot) haben. Dabei gibt es bei jeder der drei Farben auch Abstufungen in Bezug auf Helligkeit und Intensität.

Je grüner ein Bereich ist, umso besser. HeatMapper zeigt zunächst das Signal aller in der Umgebung entdeckten WLAN-Access-Points (APs) an. Wenn Sie zur Optimierung Ihres Netzwerks nur die Heatmap für Ihren AP oder Router anzeigen lassen wollen, suchen Sie nach dem Gerät auf der Karte und fahren mit dem Mauszeiger darauf. Jetzt wechselt die Karte und zeigt nur noch den

Bereich Ihres WLAN-Routers an. Zudem wird der Name Ihres WLAN-Netzes angezeigt, so dass Sie sicher sein können, den richtigen AP gefunden zu haben.

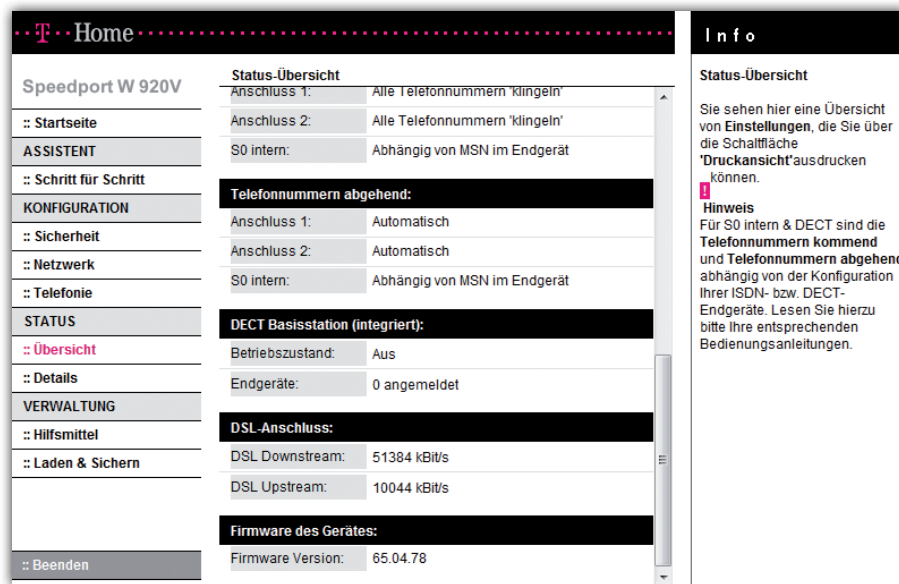
9 Neue Firmware für mehr Speed

Auch WLAN-Router kommen ab und an in den Genuss von Aktualisierungen, bei denen die Firmware auf den neuesten Stand gebracht wird. Die exakte Vorgehensweise ist zwar von Gerät zu Gerät verschieden, doch im Grunde genommen gibt es nur zwei Möglichkeiten: das automatische Online-Update und die manuelle Variante.

Update-Automatik: Router wie der Netgear WNDR 3700 prüfen jedesmal, ob eine neue Firmware zur Verfügung steht.

Ganz gleich, wie Sie die neue Firmware auf die Box bekommen – die Verbindung zwischen PC und WLAN-Router sollte dabei zwingend per Netzkabel hergestellt werden. Denn nur dann ist auf jeden Fall sichergestellt, dass nichts schiefgehen kann.

Ebenfalls nicht vergessen dürfen Sie, die aktuellen Einstellungen zu sichern. Denn während der Aktualisierung der Firmware wird der Router fast immer in den Auslieferungszustand zurückgesetzt. Und was ist, wenn Sie bei Ihrem Modell die Einstellungen nicht sichern können? Dann müssen Sie in den sauren Apfel beißen und sich diese aufschreiben.



Bevor Sie sich auf die Suche nach einer aktuellen Firmware machen, müssen Sie zunächst einmal die Versionsnummer der derzeit verwendeten ausfindig machen.

Tipp

Laborfirmware für die Fritzbox

AVM, der Hersteller der Fritzbox, bietet neben der regulären Firmware auch eine so genannte Laborfirmware zum Download an. Diese zeigt immer den letzten Stand der Entwicklung, ist aber möglicherweise noch nicht ganz ausgereift, besitzt also Beta-Status. Manchmal beseitigt sie aber schon bestimmte Probleme, ohne dass Sie lange auf das nächste Firmware-Update warten müssten. Info: www.avm.de/labor

Geräte sind wenigstens so benutzerfreundlich, Sie automatisch auf die passende Downloadseite zu lenken. Das ist zumindest eine kleine Hilfe.

Es nicht immer zwingend nötig, dem WLAN-Router eine neue Firmware zu spendieren. Finden Sie bei einem Besuch auf der Webseite des Herstellers etwa heraus, dass nur uninteressante Funktionen integriert wurden, und läuft der Router einwandfrei, können Sie sich die Aktualisierung guten Gewissens schenken. Denn auch hier gilt das ungeschriebene PC-Gesetz: „Never change a running system“.

Bietet Ihr WLAN-Router eine Funktion zur automatischen Online-Aktualisierung, sind Sie fein raus. Denn dann reduziert sich der Updatevorgang auf wenige Mausklicks. Sie

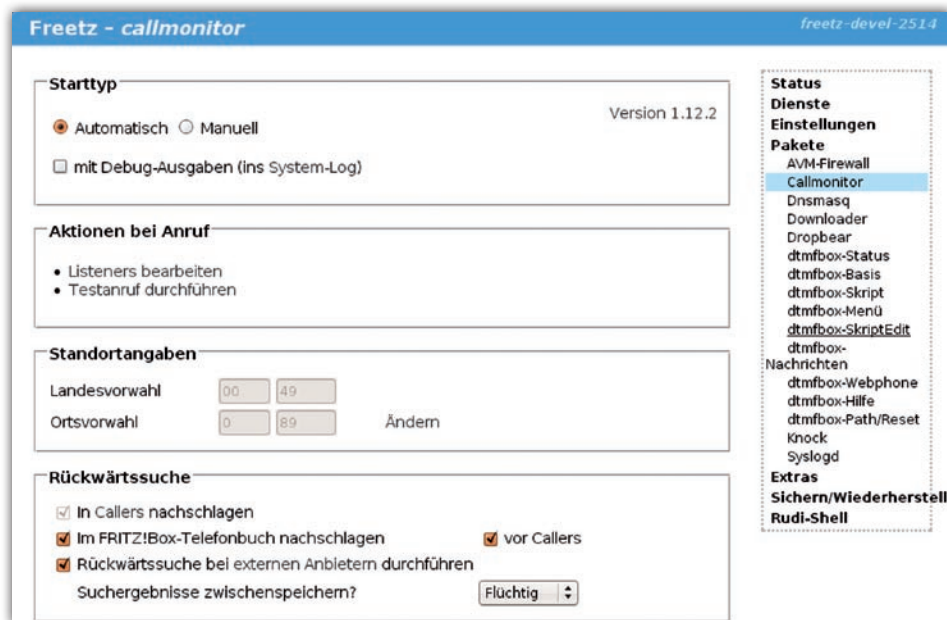
entscheiden sich für die entsprechende Funktion, klicken sich durch die einzelnen Dialoge, und am Ende ist Ihr WLAN-Router mit einer neuen Firmware ausgestattet.

Ein weiterer Vorteil dieser Methode, die unter anderem von allen Fritzboxen angeboten wird: Sie können nicht aus Versehen eine Firmware einspielen, die gar nicht für Ihren WLAN-Router gedacht ist.

10 Firmware manuell installieren

Ein wenig zeitaufwändiger gestaltet sich das Router-Update, wenn Sie die Firmware manuell einspielen müssen. Einige

Gehört Ihr Modell aber zu den Geräten, die keinerlei Hilfestellungen bieten, müssen Sie zunächst einmal die derzeit verwendete Firmware-Version in Erfahrung bringen. Diese Information finden Sie in der Verwaltungsmaske des WLAN-Routers. Bevor Sie jetzt der Hersteller-Homepage einen Besuch abstatten, notieren Sie sich diese Angabe und schreiben sich auch die exakte Bezeichnung des WLAN-Routers auf. Diese Informationen sind von größter Wichtigkeit, da viele Hersteller ähnlich klingende Produktnamen verwenden.



Mit einer alternativen Firmware holen erfahrene Nutzer das Maximum aus ihrer Fritzbox heraus. Bei experimentierfreudigen Nutzern ganz besonders beliebt ist Freetz.

Im Bereich „Support“, unter „Downloads“ oder auf der Produktseite des Geräts suchen Sie dann nach einer neuen Firmware. Sind Sie fündig geworden, sollten Sie zuerst die Beschreibung durchlesen, um zu erfahren, was die neue Firmware überhaupt bringt. Sind interessante neue Funktionen an Bord oder werden Fehler, von denen Sie betroffen sind, ausgebessert, laden Sie die Datei auf Ihren PC herunter.

Rufen Sie dann die Konfigurationsmaske Ihres Routers auf und wechseln Sie zum entsprechenden Update-Bereich. Im Normalfall

müssen Sie auf eine Schaltfläche klicken, den Pfad zur soeben heruntergeladenen Datei angeben, das Update starten und den Bildschirmanweisungen folgen. Im letzten Schritt ist es oft nötig, den WLAN-Router neu zu starten, damit die Änderungen wirksam werden.

11 Cleveres Firmware-Tuning

Das letzte Quäntchen Leistungsplus bekommen Sie mit Software-Tweaks. Speziell für die Fritzbox gibt es die freie Firmware Freetz (<http://trac.freetz.org>), mit der Sie versteckte Features freischalten

können – etwa, um die Geschwindigkeit an DSL-Anschlüssen mit hoher Dämpfung zu erhöhen. Zusätzlich kann diese Firmware noch die WLAN-Sendeleistung erhöhen. Auch bei Linksys- und Buffalo-Routern funktioniert dieser Trick, die Alternativ-Firmware finden Sie unter www.dd-wrt.com. Bei vielen anderen Router-Modellen genügt es, die US-Version der Firmware aufzuspielen. Beachten Sie aber, dass so präparierte Router die in Deutschland gültige gesetzliche Höchstgrenze von 100 mW überschreiten können.

Damit Sie im gesetzlichen Rahmen bleiben, sollten Sie die maximal zulässige Leistung Ihrer Router-Antennenkombination rechnerisch überprüfen: Ziehen Sie zunächst den Wert des Antennengewinns Ihres Routers (Einheit dBi, in den technischen Daten des Geräts) vom Grenzwert 20 dBm ab.

Den so ermittelten Wert (in dBm) müssen Sie in Watt umrechnen. Einen Rechner dafür finden Sie auf der Website www.convertworld.com/de/leistung/dBm.html. Das Ergebnis tragen Sie dann in der Konfigurationsoberfläche ein. So haben Sie Ihren Router maximal ausgereizt – zusammen mit den Aufstelltipps sollte die WLAN-Abdeckung dann in der gesamten Wohnung optimal sein.

WDS

Mit WDS (Wireless Distribution System) können Sie die Reichweite Ihres WLAN-Funknetzes vergrößern, zum Beispiel mit einer weiteren FRITZ!Box. Das Gerät, das den Internetzugang herstellt, dient als Basisstation, das andere als Repeater.

Hinweise

- Alle verwendeten WLAN-Geräte müssen das Verfahren WDS unterstützen. Der AVM FRITZ!WLAN Repeater funktioniert nicht nach dem WDS-Verfahren. Verwenden Sie für seine Einrichtung das Verfahren [WPS](#).
- Die WDS-Basisstation und alle WDS-Repeater müssen auf dem selben Funkkanal arbeiten. Deshalb darf in der FRITZ!Box nicht die Funktion 'Autokanal' eingestellt sein. Die Einstellung für den Funkkanal können Sie auf der Seite [Funkkanal](#) ändern.
- Die Verbindungen zwischen der WDS-Basisstation und den WDSRepeatern müssen mit der gleichen Verschlüsselung gesichert sein.

☒ WDS aktiv

Betriebsart

☒ Basisstation
Diese FRITZ!Box ist eine Basisstation für andere Repeater.

☐ Repeater
Diese FRITZ!Box ist ein Repeater für eine andere Basisstation.

Repeater-Auswahl

Wählen Sie hier das WLAN-Gerät, das in Ihrem WLAN-Funknetz als Repeater arbeiten soll. Sie können bis zu 3 Geräte auswählen und als Repeater verwenden. Die Liste enthält alle WLAN-Geräte, die in Ihrer Umgebung gefunden wurden und die Geräte, die Sie selbst hinzugefügt haben.

WLAN-Geräte

	Name(SSID)	Kanal	MAC-Adresse
<input type="checkbox"/>	--- nicht gefunden ---	2	00:03:C9:8B:D8:05
<input checked="" type="checkbox"/>	WLAN-7A3707	2	00:12:BF:7A:37:D4

Gekoppelte Fritzboxen: Zwei oder mehrere Fritzboxen lassen sich mittels WDS zu einem Mega-WLAN zusammenzuschließen. Damit überbrückt man selbst größere Funkstrecken.

12 Repeater spiegeln das Signal

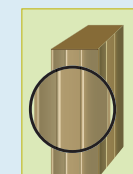
Ist die WLAN-Leistung immer noch nicht zufriedenstellend, müssen Sie in den sauren Apfel beißen und Geld für einen zusätzlichen Router ausgeben, den Sie als Repeater einsetzen. Oder Sie entscheiden sich gleich für einen Repeater, etwa den Fritz WLAN Repeater N/G (www.avm.de, rund 70 Euro), Linksys WET610N Bridge (www.linksysbycisco.com/DE/de/home, ca. 65 Euro) oder Netgear Universal Wireless-N 300

Tipp

Die WLAN-Feinde

Eine Rigipswand killt Ihr Funknetz – eine Holzwand nicht. Diese Aufstellung zeigt die Durchlässigkeit der Materialien.

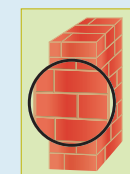
- Hohe Durchlässigkeit des Signals
- Mittlere Durchlässigkeit des Signals
- Niedrige Durchlässigkeit des Signals



HOLZWAND

95 %

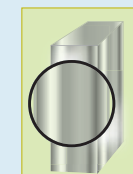
Geringfügige Mengen Wasser stören hier nur wenig die Signale des Funknetzes



ZIEGELSTEIN

70 %

Gebackene Ziegel enthalten zwar wenig Wasser, allerdings stört der Materialmix



ALUMINIUM

90 %

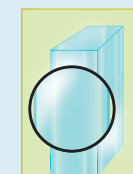
WLAN-Datenfunk durchdringt dieses Material relativ ungehindert



BETON

60 %

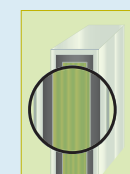
Besonders Stahlbeton ist ein WLAN-Killer: Wasser und Metall absorbieren die Strahlen



GLAS

75 %

Bei Glas stört vor allem Metallbedampfung den ungehinderten Datendurchfluss



RIGIPS

50 %

Das Material enthält Wasser, das die 2,4-GHz-WLAN-Strahlung absorbiert

Repeater (www.netgear.de, rund 45 Euro). Diese Geräte tragen das WLAN-Signal auch in die entferntesten Ecken einer Wohnung, sodass Sie in den Genuss einer spürbar höheren Geschwindigkeit kommen. Ein Plus gegenüber einem doppelten Router: Die Repeater sehen recht hübsch aus und sind deutlich kleiner als ein Router.

Um einen zweiten WLAN-Router als zusätzlichen Access Point einzusetzen, vertrauen Sie auf das Wireless Distribution System (WDS). Die meisten neuen Geräte beherrschen diese Technik, die dafür sorgt, dass die Kontaktaufnahme reibungslos klappt. Einzige Voraussetzung ist, dass beide Geräte auf dem gleichen Kanal funken und mit dem gleichen Verschlüsselungsverfahren arbeiten.

Zwei Fritzboxen verbinden Sie etwa, indem Sie im Menü „WLAN“ auf „WDS“ klicken. Im Bereich „WDS“ markieren Sie die Option „WDS aktiv“ und wählen die gewünschte Betriebsart aus. Bei der Fritzbox, die als WLAN-Zentrale genutzt wird, entscheiden Sie sich bei „Betriebsart“ für „Basisstation“, das zweite Gerät konfigurieren Sie als „Repeater“. Praktisch ist, dass Sie die Gegenstelle ganz bequem aus einer Liste auswählen können. Anstatt sich also mit den MAC-Adressen

der Geräte zu beschäftigen, markieren Sie die Fritzbox, die als Repeater bzw. Basisstation fungieren soll, und bestätigen die Auswahl mit „Übernehmen“. Sie können bis zu drei Geräte als Repeater nutzen. Nach der Kopplung gehört die unterdurchschnittliche Sende- und Empfangsleistung endgültig der Vergangenheit an.

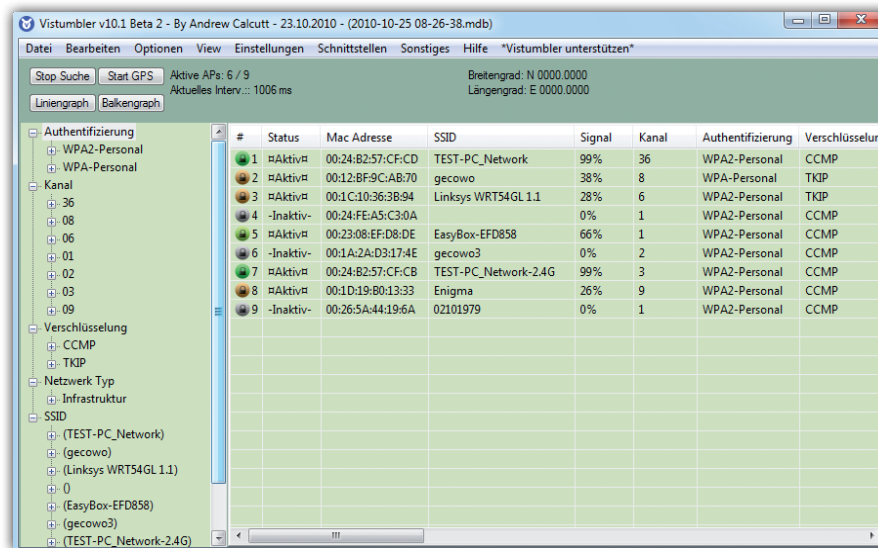
Artur Hoffmann

Unknackbares WLAN

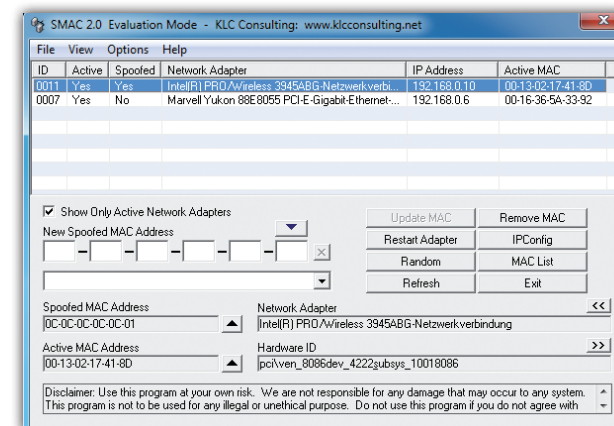
Der Router ist die WLAN-Kommunikationszentrale. Und die muss sicher vor Hackern sein. Wir zeigen, **wie Sie verhindern, dass Angreifer in Ihr WLAN eindringen**, und erklären, wie Sie Schwachstellen aufspüren.

WLAN-Betreiber sind gesetzlich verpflichtet, den Zugang zu ihrem Drahtlos-Netzwerk per Passwort zu schützen, um ungebetene Besucher auszusperren. Doch nicht nur das Kennwort spielt in Bezug auf die WLAN-Sicherheit eine Rolle. Auch Ports, MAC-Adressen-Filter

und die Datenpakete sind wichtig. Wir zeigen Ihnen, wie Sie Ihr heimisches WLAN auf Sicherheitslücken abklopfen, die Risiken beseitigen und das Drahtlos-Netzwerk abriegeln. Speziell auf die bombensichere Konfiguration der Fritzbox gehen wir auf Seite 3 ein.



Der WLAN-Sniffer Vistumbler v10 zeigt die SSIDs aller erreichbaren Drahtlos-Netzwerke in übersichtlicher Form an.

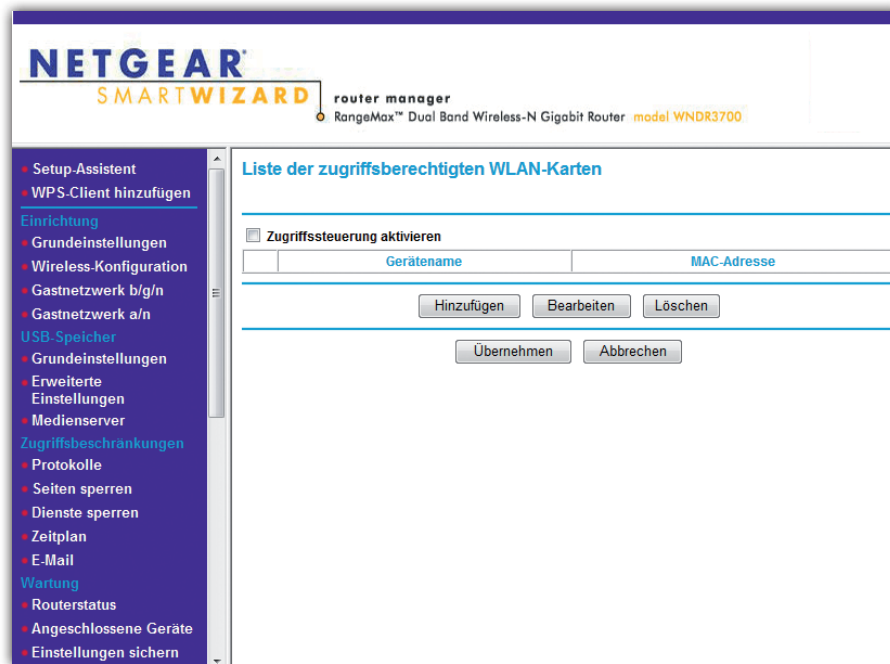


Ob die von Ihnen konfigurierte MAC-Filterung wirklich funktioniert, ermitteln Sie mithilfe von SMAC 2.0.

1 Kontrolle deckt Lücken auf

Als Erstes sollten Sie ermitteln, ob Ihr Netzwerk wirklich gut versteckt oder immer noch sichtbar ist. Rufen Sie dazu in Windows die Einstellungen für drahtlose Netzwerke auf und sehen Sie nach, ob dort die SSID Ihres Netzes erscheint. Das sollte bei deaktivierter Übermittlung der SSID nicht passieren.

Nun kommt der Härtetest mit einem speziellen Scan-Programm. Gute Dienste leistet unter Windows 7 und Vista der kostenlose WLAN-Scanner Vistumbler v10 (www.vistumbler.net), den Sie als Administrator starten müssen. Das Tool liefert Ihnen vielfältige Informationen zu allen in der Nähe befindlichen WLANs. Unter anderem finden Sie heraus, auf welchen Kanälen sie senden, welche Verschlüsselungsmethode zum Einsatz kommt und wie stark das Signal ist. Zwar können Sie auch mit dieser Software nicht erkennen, wie der Name des Netzwerks lautet, aber das versteckte WLAN ist schon mal sichtbar.



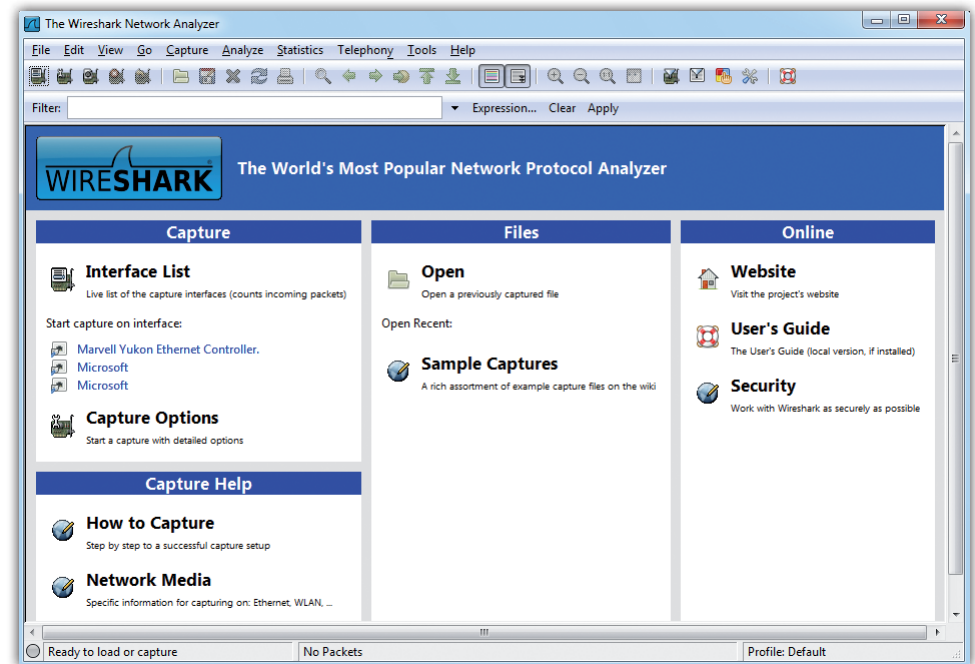
So nicht! Es ist ratsam, die MAC-Filterung einzuschalten und ausschließlich bekannten Geräten die WLAN-Nutzung zu erlauben.

2 Schwachpunkte gezielt ermitteln

Der Check mit Vistumbler ist nur ein erster Test, der Ihnen einen schnellen Überblick verschaffen soll. In einem zweiten Schritt sollten Sie ausprobieren, ob der MAC-Filter Ihres Routers funktioniert. Tragen Sie die MAC-Adressen Ihrer WLAN-Adapter in die Filterliste ein, sodass eine Verbindung nur über diese Hardware zustande kommen

kann. Kontrollieren Sie, ob Ihre Netzwerkkarten nach dem Anmelden am Netzwerk eine IP-Adresse zugewiesen bekommen.

Um zu überprüfen, ob alles funktioniert, greifen Sie auf SMAC 2.0 (www.klccconsulting.net/smac) zurück. Sinn und Zweck des englischsprachigen Tools ist es, jedem Netzwerkadapter eine beliebige MAC-Adresse zuzuweisen.



Die Bedienfreundlichkeit von Wireshark ist im Laufe der Zeit gestiegen, sodass das Sniffing-Tool nun auch von weniger versierten Nutzern verwendet werden kann.

Starten Sie das Programm als Administrator und geben Sie die neue MAC-Adresse ein. Das Programm ändert nicht die physikalische MAC-Adresse, sondern manipuliert sie lediglich innerhalb der übermittelten Pakete. Da der Router die scheinbar geänderte Adresse nicht kennt, darf der Computer mit diesem WLAN-Adapter natürlich keinen Zugriff aufs Netz erhalten und auch keine IP-Adresse zugewiesen bekommen.

Es gibt zwei Versionen von SMAC: Mit der kostenlosen Software können Sie die MAC-Adressen nur auf „0C0C0C0C0C01“ ändern. Das reicht für einen schnellen Sicherheitscheck völlig aus. Bei der Standard Edition, die rund 20 Euro kostet, ist diese Beschränkung aufgehoben, was aufwändigere Tests ermöglicht.

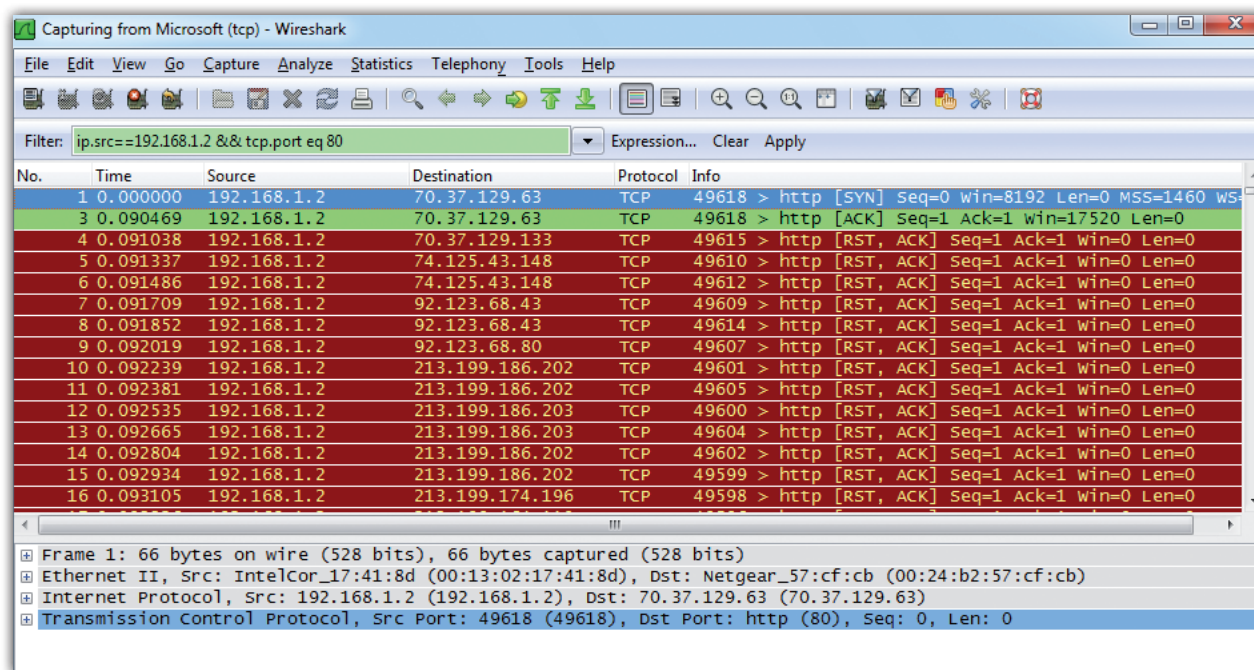
3 Wer darf ins WLAN rein?

Welche Geräte in Ihrem WLAN unterwegs sind, erfahren Sie auch durch einen Blick in die Konfigurationsmaske des Routers. Schließlich haben Sie die MAC-Adressen der Computer und Endgeräte, denen der Zugriff auf das WLAN gestattet ist, in die entsprechende Maske eingegeben. Das Problem: Leider zeigen nicht alle Router die komplette Liste der zugelassenen Geräte an. So beschränkt sich beispielsweise der Telekom-Router Speedport W 902V auf die Anzeige von zehn Einträgen. Wesentlich informativer ist die Fritzbox.

4 Datenpakete unter die Lupe nehmen

Damit Sie sehen, welche Inhalte beim Belauschen Ihres WLANs für Angreifer abrufbar sind, sollten Sie die Datenpakete mit einem Analyseprogramm untersuchen.

Bewährt hat sich das englischsprachige Wireshark 1.4.1 (www.wireshark.org), das kostenlos unter der GNU General Public License



Dem Schnüffler Wireshark entgeht kein Paket, das im Netzwerk gesendet oder empfangen wird.

vertrieben wird. Wireshark unterstützt in der aktuellen Version nahezu alle gängigen Protokolle und Medientypen. Findet es entsprechende Pakete im belauschten Netzwerkverkehr, so markiert es sie farblich und bereitet sie zur weiteren Analyse vor.

Wireshark lässt sich in allen gebräuchlichen Netzwerken einsetzen. Auch bei der Hardware ist der Netzwerkscanner nicht wählerisch und unterstützt praktisch alle aktuellen Geräte – kabelgebundene ebenso wie drahtlose.

Genauere Infos zur Kompatibilität finden Sie in den FAQ (www.wireshark.org/faq.html).

Wählen Sie nach dem Start des Programms zunächst einmal unter „Interface List“ die Netzwerkkarte aus, mit der Sie den Netzwerkverkehr beobachten wollen. Zum Test Ihres WLANs ist das natürlich der WLAN-Adapter. Voraussetzung ist allerdings, dass Ihr Access Point als Hub arbeitet (das ist der Normalfall) und daher sämtliche Datenpakete an alle WLAN-Clients weitergegeben werden.

5 Ports gezielt überwachen

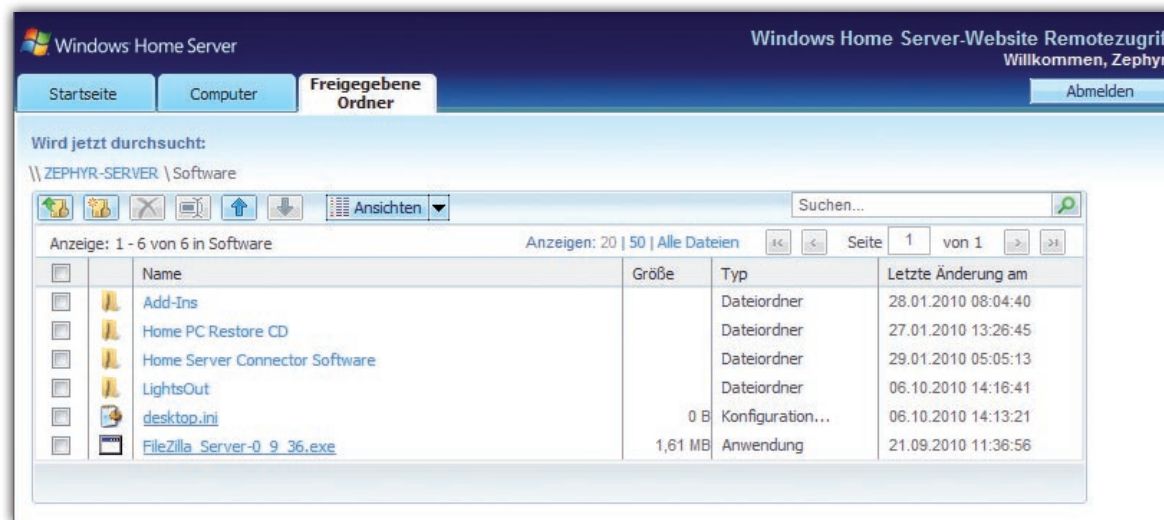
Mithilfe von Filtern können Sie in Wireshark die Analyse auf verschiedene Protokolle oder IP-Adressen einschränken, beispielsweise wenn Sie die Aktionen eines Eindringlings beobachten möchten, den Sie gerade entdeckt haben. Die jeweiligen Filterregeln lassen sich relativ unkompliziert über einen speziellen Regel-Assistenten zusammenstellen.

Wireshark kennt zwei verschiedene Filter: Capture Filters und Display Filters. Mithilfe der Capture Filters legen Sie vor Beginn eines Scans fest, welche Pakete, IP-Adressen und Ports das Tool überwachen soll. Dies ist ein probates Mittel, um für einen Einsatzzweck uninteressante Pakete zu ignorieren

Info

Grenzen der Portweiterleitung

Einige Router bieten nicht die Möglichkeit, interne IP-Adresse und Port zu trennen. Somit muss ein interner Webserver, der auf Port 80 läuft, auch von außen mit Port 80 angesprochen werden. Das kann in der Praxis durchaus von Nachteil sein: Ein möglicher weiterer interner Webserver, der unter einer anderen IP-Adresse, aber auch auf Port 80 erreichbar ist, könnte dann von außen nicht mehr angesprochen werden, weil Port 80 schon auf den anderen Rechner geroutet wird.



Um aus dem Internet auf einen Windows Home Server zugreifen zu können, müssen die entsprechenden Ports im Router umgeleitet werden.

oder zu verhindern, dass die Protokolldatei bei längeren Scans zu groß wird.

Wollen Sie etwa den Netzwerkverkehr der drei bei der E-Mail-Übertragung verwendeten TCP-Ports 25 (SMTP), 110 (POP3) und 143 (IMAP) protokollieren, verwenden Sie als Capture-Filter den Befehl „tcp port 25 or tcp port 110 or tcp port 143“.

Display Filters kommen nach dem Scan zum Einsatz. Die Nutzung der Display-Filters-Funktion ist ebenso einfach wie die Definition der Capture Filters; die Kombination mehrerer Filter ist ebenfalls möglich. Allerdings

unterscheidet sich die Syntax. Um etwa die Paketanzeige auf den vom Netzwerkadapter mit der IP-Adresse 192.168.0.15 über Port 80 verursachten Traffic zu begrenzen, tippen Sie den Befehl „ip.src==192.168.0.15 && tcp.port eq 80“ ein. Der logische Operator „&&“ bedeutet in diesem Zusammenhang, dass Wireshark nur Einträge anzeigt, die beiden Kriterien entsprechen.

6 Ports sind die Bindeglieder

Nachdem Sie nun die größten Sicherheitslöcher Ihres WLANs entdeckt und gestopft haben, steht das Feintuning auf dem Programm. Zunächst kümmern Sie sich um die Ports.

Tipp

Sichere Passwörter finden

In der Praxis sehr sinnvoll ist die Verwendung so genannter Passwortphrasen wie „Mein Sohn Anton ist drei Jahre jünger als meine Tochter Ella“. Das Passwort setzt sich dabei aus den Anfangsbuchstaben der Wörter zusammen: „msaidjjam-te“. Durch das Ersetzen von Buchstaben durch ähnlich aussehende Zahlen – etwa 4 für a, 1 für i und 7 für t – wird das Passwort noch stärker: „ms413jj4m73.“

Der Großteil aller Anwender geht über einen Provider ins Internet, der ihm eine einzelne öffentliche IP-Adresse zur Verfügung stellt. Der DSL-Router oder der jeweilige Access Point bekommt diese IP-Adresse zugewiesen und ist damit aus dem Internet erreichbar.

Da diese Adresse aber nur einem einzigen Gerät zugewiesen werden kann, ist sie damit „verbraucht“. Ihre Computer im heimischen Netzwerk verfügen hingegen über lokale Adressen, die Sie daran erkennen, dass sie mit „192.168.“ beginnen. Diese Adressen sind aus dem Internet nicht direkt erreichbar, da nur die IP-Adresse des Access Points von Ihrem Provider geroutet, also weitervermittelt wird. Somit kann nur der Router mit beiden Seiten kommunizieren. Er ist es auch, der dafür sorgt, dass Anfragen aus dem lokalen Netz ins Internet gelangen und



Bei nahezu allen modernen WLAN- Routern können Sie Ports gezielt sperren.

Antworten an den richtigen Rechner zurückgesendet werden.

Wichtig ist, dass nahezu alle Router mittels Port Forwarding Anfragen aus dem Internet in das lokale Netz weiterleiten können. Interessant ist dieses Port Forwarding vor allem dann, wenn Sie einen eigenen Webserver an Ihrem Internetanschluss betreiben wollen oder File-Sharing-Software einsetzen.

Immer mehr Access Points sind zudem mit einer Firewall ausgestattet, die das Netzwerk

vor Eindringlingen schützen sollen. Zum anderen gibt es aber auch Router, die Denial-of-Service-Attacken abblocken können.

7 Gezieltes Port-Blocking

Netzwerkports sind virtuelle Adressen, über die bestimmte Dienste genutzt werden können. Das setzt natürlich voraus, dass ein Serverdienst darauf wartet, hier Daten angeliefert zu bekommen. Durch das Blockieren so eines Ports wird sichergestellt, dass der Dienst nicht benutzt oder gar für Attacken auf das dahinter liegende Netzwerk

genutzt werden kann. Zwischen dem Rechner im Internet und dem Server, also dem PC in Ihrem LAN, steht genau diese Firewall.

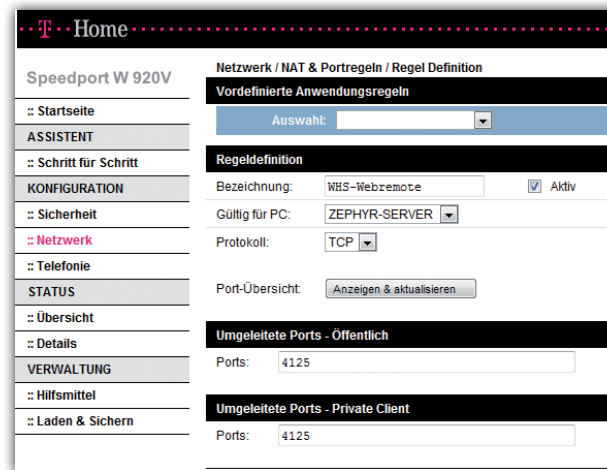
Aber in der Regel will man nicht immer und alles blocken. So möchte man als Serviceanbieter, dass einige oder alle Leute auf diese Dienste zugreifen können. Das ist der Fall, wenn man zum Beispiel seine Homepage auf dem eigenen Rechner hat und im Internet zur Verfügung stellen möchte oder den Fernzugriff auf seinen Windows Home Server oder NAS erlauben will. So etwas macht natürlich nur dann Sinn, wenn der eigene Rechner permanent mit dem Internet verbunden ist.

Beim Speedport W 902V finden Sie die Funktion zum Sperren und Weiterleiten bestimmter Ports im Bereich „Netzwerk“ und „Nat- & Portregeln“. Fritzbox-Besitzer klicken auf „Internet“ und wählen dann „Freigaben“.

8 Serverdienste im Netzwerk

Sie haben eine Flatrate und einen DSL-fähigen Router, der das Port Forwarding beherrscht? Gut, denn dann können Sie Ihren eigenen Webserver im Internet verfügbar machen.

Dienste auf einem Server sind durch die Portnummer gekennzeichnet. Feste Ports sind etwa 21 für FTP, 80 für HTTP und 25



Betreiben Sie in Ihrem LAN ein Gerät, das aus dem Internet erreichbar sein soll, sind die entsprechenden Ports umzuleiten.

respektive 110 für Mailversand und -empfang. Wir beschränken uns in diesem Beispiel der Einfachheit halber auf einen Webserver, den Sie betreiben und über den Router ins Internet bringen möchten. Zudem gehen wir von TCP als Protokoll aus und lassen UDP der Einfachheit halber außen vor.

Ein Webserver stellt wie oben beschrieben die Inhalte auf Port 80 bereit. Da zu jedem Webserver auch eine IP-Adresse gehört, wird ein lokaler Webserver zum Beispiel unter 192.168.1.10 mit Port 80 angesprochen.

Mit einem Browser stellen Sie Ihre Anfrage von Haus aus auf Port 80, sodass Sie

nur noch die IP-Adresse oder URL eingeben müssen. Wie schon beschrieben, würde eine Anfrage auf den Router mit Port 80 vom Internet aus nicht beachtet, weil dieser keinen Webserver für das Internet darstellt. Der Router muss diese Anfrage also weiterleiten. Und da der Port 80 richtig ist, muss folglich nur die IP-Adresse des eigentlichen Servers angesprochen werden, in diesem Fall 192.168.1.10. Setzen Sie auf Sicherheit, dann werden Sie stattdessen lieber Port 443 ansprechen wollen. Dieser Port ist für die sichere HTTPS-Kommunikation reserviert, und Eingaben im Browser werden mit https:// eingeleitet. Auf diese Weise können Sie beliebige Dienste verteilen. Es ist beispielsweise möglich, einen separaten Server für Webdienste, einen für Mail und vielleicht auch einen für den Zugang aus dem Internet, beispielsweise per SSH (Port 22) unter nur einer externen, also aus dem Internet erreichbaren, IP-Adresse bereitzustellen.

9 DoS: Ganz gemeine Attacken

Immer wieder berichten Medien über so genannte Denial-of-Service-Attacken, die komplette Firmen-Netzwerke lahmlegen. Vereinfacht ausgedrückt basieren solche DoS-Angriffe auf dem Prinzip der Überlastung. Ein Computer wird so lange mit Anfragen zugemüllt, bis er unter der Last zusammenbricht. Die Website, die Sie auf Ihrem



Aus dem Internet eintreffende Anfragen mit unbekannter Zielangabe landen erst einmal auf dem DMZ-Server.

Rechner bereitstellen möchten, wäre in so einem Fall nicht mehr erreichbar, da der Router die Anfragen nicht mehr bearbeiten könnte.

Um diesem Fall entgegenzuwirken, kann bei manchen Routern die Anzahl der Anfrage-Einträge begrenzt werden. Kommen in dieser Zeit weitere Anfragen herein, werden sie kurzerhand abgewiesen und müssen erneut gestellt werden. Insofern ist diese Maßnahme ein sinnvoller Schutz, den es übrigens auch bei Firewalls in Unternehmen gibt.

Etwas einfacher gestrickt ist die zweite Möglichkeit: Der Router nimmt hierbei nach einer Häufung von Anfragen eine gewisse Zeit einfach überhaupt keine Anfragen mehr

an. Damit ist dann allerdings der ganze Anschluss blockiert – und komplett lahmgelegt.

10 Demilitarisierte Zone einrichten

Es gibt auch Router, die Ihnen eine DMZ (Demilitarisierte Zone) bereitstellen. Das Grundprinzip: Sie bestimmen einen im lokalen Netzwerk integrierten Computer als DMZ-Server, der als Puffer zwischen Internet und Heim-Netzwerk fungiert. Kann der Router aus dem Internet eintreffende Anfragen an keinen bestimmten Computer im Netzwerk weiterleiten, landen sie beim DMZ-Server.

Der Vorteil: Es ist nicht mehr notwendig, jeden einzelnen Port weiterzuleiten. Sie geben nur an, welche IP-Adresse der Server hat. Allerdings ist es dann nicht mehr möglich, Ports zu tauschen, also etwa Port 81 auf die interne IP-Adresse 192.168.1.10 mit Port 80 zu leiten.

Bietet Ihnen Ihr WLAN-Router eine Funktion zum Schutz vor Port-Scans, schalten Sie sie selbstverständlich auch ein.

11 TCP oder UDP als Alternative

Selbst bei den Protokollen unterscheiden sich die Geräte. Denn nicht alle Router bieten eine Trennung von TCP und UDP an. Doch wo liegen die Unterschiede?

Beziehungsweise: Wieso sollte man überhaupt ein anderes Protokoll als das übliche TCP verwenden?

Vereinfacht ausgedrückt, wartet eine UDP-Verbindung im Gegensatz zu TCP nicht auf eine Bestätigung, dass die Pakete erhalten wurden. Daher wird für die meisten Dienste (Mail, Webseiten usw.) TCP benutzt. Denn der Versender im Netz/Internet muss ja schließlich gewährleisten, dass die einzelnen Datenpakete auch tatsächlich beim Empfänger ankommen.

In den Fällen, in denen es auf Geschwindigkeit und nicht so sehr auf eine exakte Übermittlung ankommt, wie etwa bei der Sprachkommunikation über das Internet mittels Voice over IP, wird UDP benutzt.

Da für das Abrufen von HTML-Seiten der Port 80 festgelegt ist und TCP benutzt wird, brauchen Sie sich nicht weiter darum zu kümmern. Im Zweifelsfall wird einfach alles an den Server weitergeleitet, also TCP und UDP, je nachdem, welcher Art die ankommenden Pakete sind. Und da es normalerweise nicht vorkommt, dass UDP-Pakete auf Port 80 zu einem anderen Server geleitet werden sollen, ist diese Einstellung auch in den allermeisten Fällen nicht notwendig.

Artur Hoffmann

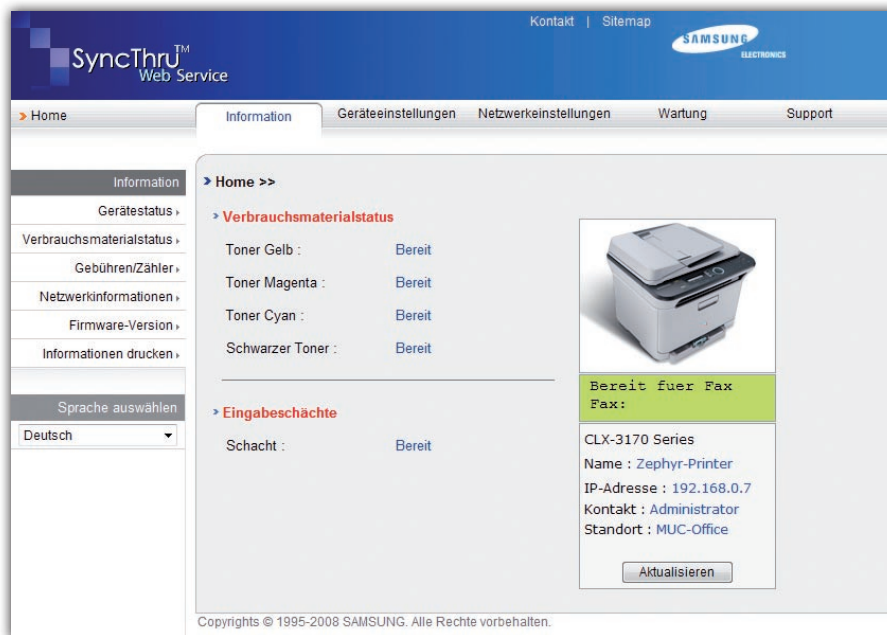
Private Druckerzentrale

Alle PCs und netzwerkfähigen Multimedia-Geräte sind in Ihrem Heim-WLAN verbunden. Jetzt fehlt nur noch der passende **Netzwerk-Drucker**. Wir zeigen Ihnen, worauf es beim Kauf ankommt und wie Sie drahtlos drucken.

Netzwerk-Drucker, die sich kabellos in das Heim-LAN einbinden lassen, liegen voll im Trend. Sie lassen sich von jedem Rechner im Netz aus nutzen und problemlos über ein Web-Interface konfigurieren. Kein Wunder also, dass es immer mehr Geräte gibt.

Noch besser: Schon ab knapp 50 Euro steigen Sie in die Welt des drahtlosen Druckens ein, denn so viel müssen Sie für das Tinten-Multifunktionsgerät Lexmark Interpret S405 (www.lexmark.de) ausgeben. In diesem Beitrag erklären wir Ihnen Schritt für Schritt, worauf

Sie beim Kauf achten sollten, und zeigen auch gleich, wie Sie einen netzwerkfähigen Drucker unter XP, Vista und Windows 7 installieren.



Praktische Netzwerk-Drucker: Die Konfiguration erfolgt von jedem PC aus mithilfe eines beliebigen Web-Browsers.

Worauf kommt es an?

Abgesehen vom Preis stellt natürlich die Art des Druckers das entscheidende Kaufkriterium dar. Soll es ein Tintenstrahler sein, möchten Sie sich einen Laserdrucker zulegen oder sind Sie auf der Suche nach einem Multifunktionsgerät zum Drucken, Faxen und Scannen? Jede einzelne Geräteklasse hat ihre ganz bestimmten Vor- und Nachteile.

Haben Sie diese Frage beantwortet, müssen Sie sich noch überlegen, auf welche Art und Weise das Gerät in Ihr Netzwerk eingebunden werden soll. Drucker, die mit einer Netzwerkschnittstelle ausgestattet sind, gibt es inzwischen wie Sand am Meer. Das Angebot an Geräten, die sich per Drahtlos-Verbindung in ein WLAN integrieren lassen, ist hingegen noch überschaubar. Auf Preisvergleichsportalen im Internet finden sich rund 30 derzeit verfügbare WLAN-fähige Drucker. Und in der CHIP-Bestenliste sind auch nur wenige Geräte mit WLAN-Anschluss aufgeführt. Ganz anders sieht es auf Seiten der Multifunktionsgeräte aus. Von den 55 getesteten Tinten-Geräten lassen sich 36 Modelle kabellos in das Netzwerk einbinden.

Tinte oder Laser?

Drucker, die auf die Tintenstrahlmethode vertrauen, sind sehr günstig in der Anschaffung. Doch jeder weiß, dass die Folgekosten



Multifunktionsgeräte: Hier haben Sie die größte Auswahl an WLAN-fähigen Modellen.

ungleich höher sind, da die Hersteller bei den Farbpatronen kräftig zulegen. Wer aber nicht übermäßig viel druckt, kommt mit einem Tintenstrahler durchaus auf seine Kosten. Etwa mit dem Epson Stylus Office B40W (www.epson.de, ca. 90 Euro).

Anwender, die keine Kompromisse eingehen möchten, und für die ein gestochen scharfes Schriftbild von größter Wichtigkeit ist, müssen zu einem Laserdrucker greifen. Solche Geräte kosten ein wenig mehr als ihre Tintenstrahler-Pendants und auch der Toner

reißt ein größeres Loch in die Brieftasche. Doch unterm Strich sind die laufenden Kosten geringer.

Der Einstieg beginnt bereits bei knapp 100 Euro, die Sie in den HP LaserJet P1102w (www.hp.com) investieren müssen. Wollen Sie in Farbe drucken, stellt der Brother HL-3070CW (www.brother.de, ca. 260 Euro) die derzeit günstigste Alternative dar.

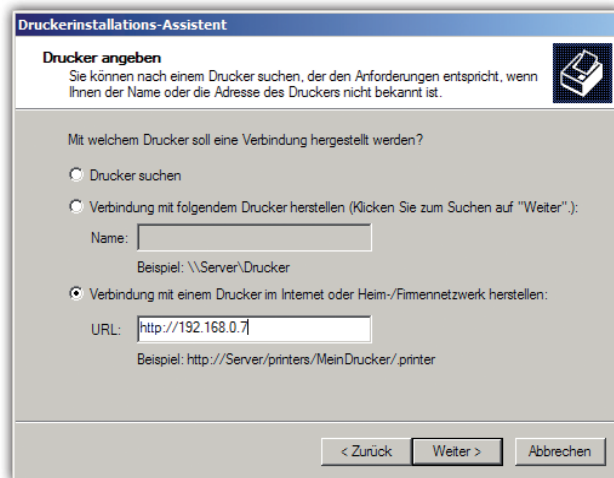
Im Privatbereich haben Multifunktionsgeräte Tintenstrahlern und Laserdruckern schon

lange den Rang abgelaufen. Kein Wunder, schließlich vereinigen solche Modelle Funktionen verschiedener Geräte in einem Gehäuse. Sie können damit in Farbe drucken, Vorlagen einscannen und kopieren sowie Faxnachrichten empfangen und versenden.

Praktisch: In keinem anderen Segment ist die Auswahl an Geräten, die schon ab Werk mit einem WLAN-Sender ausgestattet sind, größer. Neben dem bereits erwähnten Tinten-Allrounder Lexmark Interpret S405 zeichnet sich auch der HP Deskjet F4580 (ca. 60 Euro) durch seinen niedrigen Preis aus.

Ähnlich gut sieht es bei den Laser-Multifunktionsgeräten aus. Für das günstigste Schwarz-Weiß-Laser-Modell – Samsung SCX-3205W (www.samsung.de) – müssen Sie 175 Euro ausgeben. Und wer gleich in die Oberklasse einsteigen will, greift zu einem Farb-Laser-Multifunktionsgerät wie dem Samsung CLX-3175FW für rund 330 Euro.

Auf dieses Gerät gehen wir übrigens auch im folgenden Praxisteil ein. Dabei gehen wir davon aus, dass das Gerät bereits im WLAN-Netzwerk eingebunden ist; sprich, dass die drahtlose Verbindung zwischen Drucker und WLAN-Router steht. Notieren Sie sich außerdem die IP-Adresse, unter der das Gerät im Netzwerk erreichbar ist.



Windows XP: Oft erkennt Windows den Netzwerkdrucker nicht automatisch. Dann müssen Sie die IP-Adresse des Geräts eingeben.

Einrichtung unter Windows XP

Nicht besonders komfortabel ist die Einrichtung eines WLAN-Druckers unter Windows XP. Kein Wunder, denn als das Betriebssystem veröffentlicht wurde, gab es noch überhaupt keine Drahtlos-Drucker.

Legen Sie die Installations-CD in das Laufwerk ein und klicken Sie auf „Start“, „Systemsteuerung“, „Drucker und Faxgeräte“. Wenn Sie auf „Drucker hinzufügen“ klicken, startet der Einrichtungsassistent. Klicken Sie auf „Weiter“, wählen Sie „Netzwerkdrucker oder Drucker, der an einen anderen Computer angeschlossen ist“ aus und bestätigen

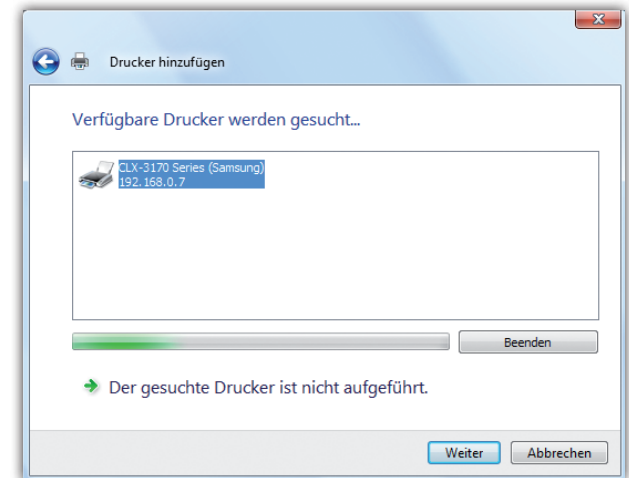
Sie mit „Weiter“. Markieren Sie die Option „Drucker suchen“ und klicken Sie auf „Weiter“. Sollte Windows XP nicht fündig werden, klicken Sie auf „Zurück“, markieren „Verbindung mit einem Drucker im Internet oder Heim-/Firmennetzwerk herstellen“ und tippen die IP-Adresse Ihres Druckers, etwa „http://192.168.0.7“, ein.

Im daraufhin geöffneten Dialog „Druckerinstallations-Assistent“ klicken Sie auf „Daten-träger“. Geben Sie den Pfad zur Treiberdatei an und bestätigen Sie die beiden folgenden Dialoge mit „OK“. Windows XP will dann wissen, ob das neue Gerät als Standarddrucker genutzt werden soll. Bestätigen Sie mit Klicks auf „Ja“, „Weiter“ und „Fertig stellen“.

Zum Abschluss rufen Sie die Konfigurationsmaske Ihres Druckers auf, indem Sie die IP-Adresse des Geräts in den Browser tippen. Hier können Sie – abhängig davon, welches Modell Sie nutzen – zahlreiche weiterführenden Funktionen konfigurieren. Das von uns verwendete Multifunktionsgerät ist unter anderem in der Lage, eintreffende Faxe in eine PDF-Datei umzuwandeln und an eine beliebige E-Mail-Adresse zu versenden.

Einrichtung unter Windows Vista

Wesentlich einfacher als unter Windows XP geht die Einrichtung unter Vista vonstatten.



Windows Vista: Hier wird der Netzwerkdrucker automatisch gefunden, sofern bereits eine Verbindung zum Router besteht.

Wählen Sie „Start“ und „Systemsteuerung“ und doppelklicken Sie auf „Drucker“.

Ein Klick auf „Drucker hinzufügen“ startet den Assistenten. Markieren Sie „Einen Netzwerk-, Drahtlos- oder Bluetoothdrucker hinzufügen“ und klicken Sie auf die Schaltfläche „Weiter“, um die Suche zu starten. Sie markieren das Gerät, das Sie einrichten wollen, und klicken erneut auf „Weiter“.

Legen Sie die zum Lieferumfang gehörende Installations-CD in das Laufwerk ein, da sie im nächsten Schritt benötigt wird. Im Dialog „Den Druckertreiber installieren“ klicken Sie

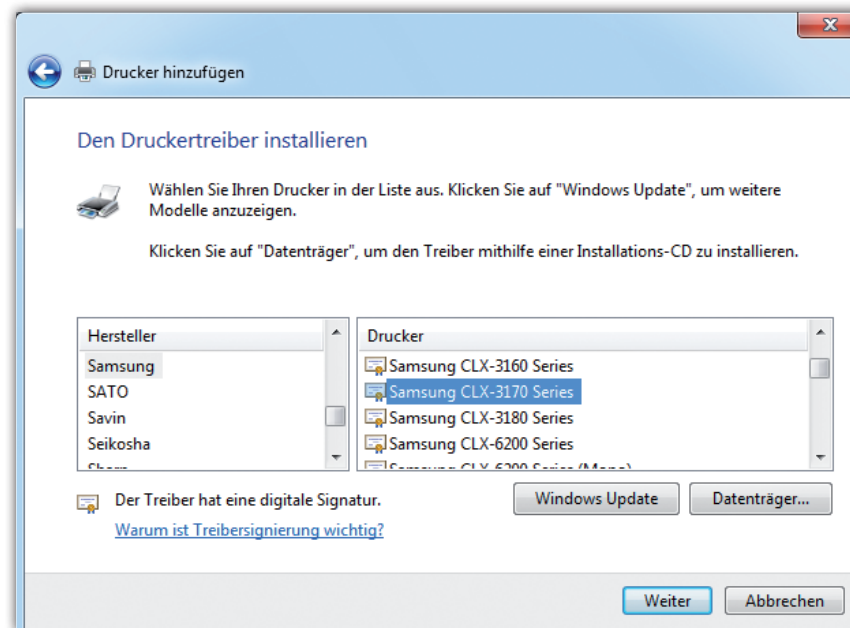
auf „Datenträger“, geben dann den Pfad zum Laufwerk an, wählen den Treiber aus und bestätigen mit „Weiter“. Anschließend können Sie dem Gerät einen „Druckernamen“ verpassen und auf Wunsch eine Testseite drucken. Mit „Fertig stellen“ beenden Sie die Einrichtung.

Einrichtung unter Windows 7

Im Handumdrehen erledigt ist die WLAN-Drucker-Einbindung auch unter Windows 7. Klicken Sie auf „Start“, wählen Sie „Geräte und Drucker“ und entscheiden Sie sich dann für „Drucker hinzufügen“.

Im Dialog „Welchen Druckertyp möchten Sie installieren“ klicken Sie auf „Einen Netzwerk-, Drahtlos- oder Bluetoothdrucker hinzufügen“. Anschließend durchsucht Windows 7 das Netzwerk nach entsprechenden Geräten. Wird das Betriebssystem fündig, listet es die entdeckten WLAN-Drucker inklusive deren Bezeichnung und IP-Adresse auf. Markieren Sie das gewünschte Gerät und klicken Sie auf „Weiter“, damit Windows 7 „das Treibermodell“ ermittelt.

Kann das Betriebssystem die Treiber nicht direkt einspielen, müssen Sie im Dialog „Den Druckertreiber installieren“ Hersteller und Modell auswählen. Werden Sie nicht fündig, ist es ratsam, zunächst einmal das Windows-Update per Klick auf die gleichnamige



Schaltfläche zu bemühen. Dieser Vorgang kann durchaus einige Minuten dauern, da die Geräteliste aktualisiert wird. Ist Ihr Druckermodell nun aufgeführt, markieren Sie den entsprechenden Eintrag und klicken Sie auf „Weiter“.

Kann der Einrichtungsassistent das Gerät nicht finden, ist das nicht weiter schlimm, da Sie ja im Besitz der Treiber-CD sind. Klicken Sie auf „Zurück“, wählen Sie „Datenträger“ aus und legen Sie die zum Lieferumfang gehörende CD oder DVD ein. Im Dialog „Geben Sie einen Druckernamen ein“

tippen Sie eine aussagekräftige Bezeichnung ein, starten die Treiberinstallation mit „Weiter“ und klicken auch im folgenden Schritt auf „Weiter“. Um zu überprüfen, ob alles geklappt hat, klicken Sie auf „Testseite drucken“. Funktioniert alles, schließen Sie den Assistenten mit „Fertig stellen“.

Artur Hoffmann

Windows 7: Die Geräteunterstützung ist so groß, dass Sie problemlos online nach dem Treiber suchen können.

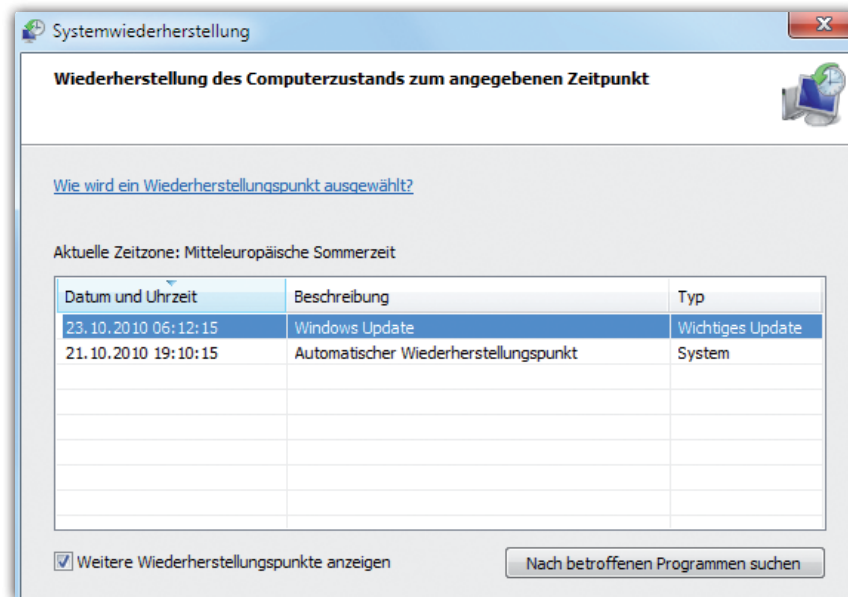
Pannenhilfe mit System

Macht das WLAN mal Ärger, ist die **Suche nach dem Fehler** nicht immer einfach, da viele Komponenten das Problem verursachen können. Mit der richtigen Strategie kommen Sie aber dennoch zum Ziel.

Sie haben Ihr Drahtlos-Netzwerk eingerichtet und es läuft perfekt. Das ist gut für Sie – hoffentlich bleibt es auch so. Denn schließlich gilt in der IT-Welt die Regel, dass minimalste Änderungen gravierende Auswirkungen haben können. Ganz gleich, ob Sie einen neuen Treiber installieren, ein falsches

Passwort eingeben oder einen Port nicht geöffnet haben – unterschiedlichste Probleme lassen meist nicht lange auf sich warten.

Unser großer Pannenhilfe-Guide unterstützt Sie bei der zielgerichteten Fehlersuche. Mit der richtigen Strategie können Sie nahezu allen typischen WLAN-Wehwechen auf die Schliche kommen und sie auskurieren. Dazu finden Sie noch einige weitere interessante Tipps & Tricks, die sich in der WLAN-Praxis bestens bewährt haben.



***Hat die Installation einer Software** oder eines Treibers das Problem verursacht, hilft die Systemwiederherstellung von Windows weiter.*

1 Spannungsversorgung checken

Wie jeden Tag wollen Sie nach der Arbeit ins Internet, um Ihre E-Mails zu checken und ein wenig zu surfen. Doch es kann keine Verbindung hergestellt werden.

Was sich banal anhört, stellt sich in der Praxis als eine der häufigsten Fehlerursachen heraus: fehlende Spannungsversorgung oder falsche Kabelverbindungen. Wie leicht vergisst man, dass man den Netzstecker des Routers gezogen hat, um kurzzeitig ein anderes Gerät anzuschließen.

Überprüfen Sie auch, ob der WLAN-Adapter noch am Rechner angeschlossen ist. Manchmal denkt man nicht daran, ihn wieder einzustecken, nachdem zum Beispiel die Digitalkamera am USB-Port angeschlossen war. Schauen Sie auch zweimal nach, ob alle Netzkabel am Router in den richtigen Anschlüssen stecken. Bei manchen Routern ist die Beschriftung der Buchsen am Gerät nicht deutlich zu erkennen. Bei Unklarheiten hilft auch ein Blick in das Handbuch des Routers weiter.

2 Letzte Änderung herausfinden

Ein monatelang einwandfrei laufendes WLAN funktioniert von einem Tag auf den anderen nicht mehr. Das ist gar nicht ungewöhnlich.

Hat Ihr drahtloses Netzwerk schon einmal funktioniert, sollten Sie unbedingt Ihre letzten Schritte nachvollziehen. Haben Sie zum Beispiel eine neue Firmware auf dem Router installiert, kann es sein, dass beim Einspielen die Werkseinstellungen des Geräts wiederhergestellt wurden. Die Installation eines neuen Treibers auf dem Computer kann ebenfalls zu Konflikten mit dem WLAN-Treiber führen.

Aber auch Software kann die Netzwerkinstallation negativ beeinflussen: Von so genannten Netzwerk-Optimierungs-Tools etwa sollten Sie lieber die Finger lassen. Diese Tools richten oft eher Schaden an. Haben Sie einen Wiederherstellungspunkt gesetzt oder ein Image des Betriebssystems gespeichert, sollten Sie den alten Zustand wiederherstellen, in dem das WLAN noch richtig funktioniert hat.

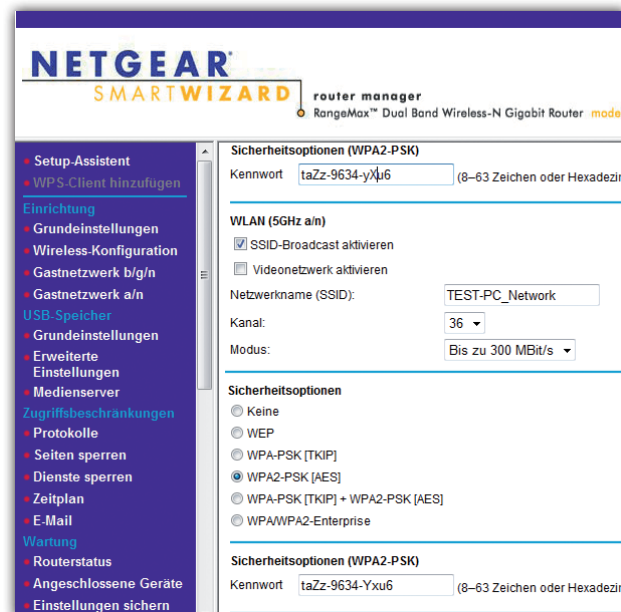
3 Router überprüfen

Die Spannungsversorgung ist intakt, und Sie haben auch keinerlei Änderungen an der Konfiguration durchgeführt. Trotzdem können Sie keine WLAN-Verbindung herstellen. Haben Sie alle vorhandenen Kabel überprüft und Ihre letzten Schritte rekonstruiert, doch das Netzwerk funktioniert immer noch nicht, verbinden Sie Router und Computer testweise mit einem Netzkabel. Haben Sie per Kabel Zugriff auf die Administrationsoberfläche, können Sie den WLAN-

Router schon einmal von der Fehlerliste streichen, was die Suche deutlich erleichtert. Überprüfen Sie daher im nächsten Schritt, ob die WLAN-Einstellungen auf PC und Router übereinstimmen. Wichtig ist dabei die Schreibweise der SSID und des Passworts für die WLAN-Datenverschlüsselung.

4 Falsches Passwort

Um ein Netzwerk zu verschlüsseln, geben Sie auf dem Router und den angeschlossenen Computern ein Passwort ein. Vertippen



Sowohl bei der SSID als auch beim Passwort kommt es auf die richtige Schreibweise an, insbesondere auf Groß- und Kleinschreibung.

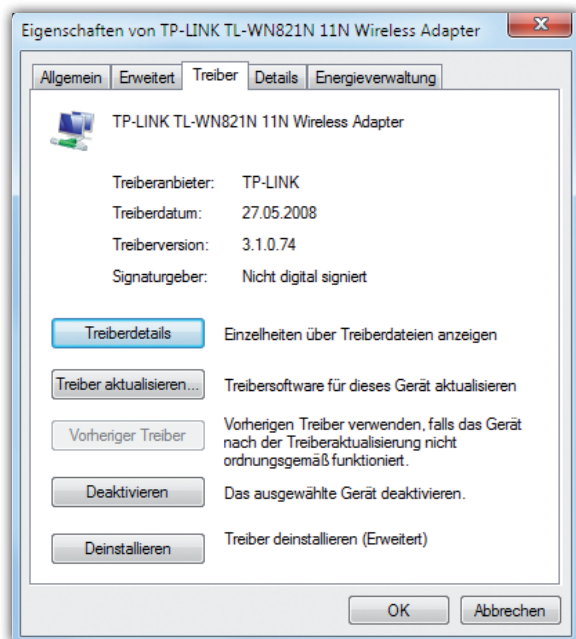
Sie sich oder stimmen Groß- und Kleinschreibung nicht überein, zeigt Ihnen das drahtlose Netzwerk nicht immer eine Fehlermeldung an. Es scheint, als seien Sie mit dem Router verbunden. Sie bekommen allerdings keine gültige IP-Adresse zugewiesen und können aus diesem Grund auch nicht auf andere Computer oder das Internet zugreifen.

Um Schreibfehler zu vermeiden, gehen Sie so vor: Tippen Sie Ihr Passwort in ein leeres Editor-Dokument. Den Editor finden Sie unter „Start“, „Alle Programme“ und „Zubehör“. Überprüfen Sie die korrekte Schreibweise und kopieren Sie das Passwort aus dem Dokument in die Dialog-Box im Router-Menü und in die Software Ihrer WLAN-Karte. So stellen Sie sicher, dass beide Versionen des Passworts exakt gleich geschrieben sind.

5 Alte Treiber und Firmware

Die Hersteller von WLAN-Geräten merken oftmals erst nach der Auslieferung, dass es zu Problemen mit ihrer Hardware kommt. Häufig sind dann Treiber oder Firmware der Geräte für seltsame Verbindungsabbrüche oder Abstürze verantwortlich.

Verwenden Sie stets die aktuellste Version des Treibers oder der Firmware. Netter Nebeneffekt der Aktualisierung: Manche Router bekommen auf diesem Weg sogar neue



Auch die Treiber für WLAN-USB-Sticks werden von den Herstellern aktualisiert. Ein Update kann nicht schaden.

Funktionen kostenlos dazu. Welche Firmware Ihr Router verwendet, finden Sie über die Administrationsoberfläche des Gerätes heraus. Gehen Sie anschließend auf die Hersteller-Webseite, um zu überprüfen, ob eine neue Firmwareversion zur Verfügung steht.

Auch Software und Treiber für WLAN-Karten und -USB-Sticks werden oft verbessert. Um den von Ihnen verwendeten Treiber zu ermitteln, öffnen Sie die „Systemsteuerung“.

Dort klicken Sie erst auf „System“, dann auf „Geräte-Manager“. Navigieren Sie zu dem Eintrag „Netzwerkadapter“. Mit einem Doppelklick auf das Gerät konfigurieren Sie dann die Eigenschaften des WLAN-Adapters.

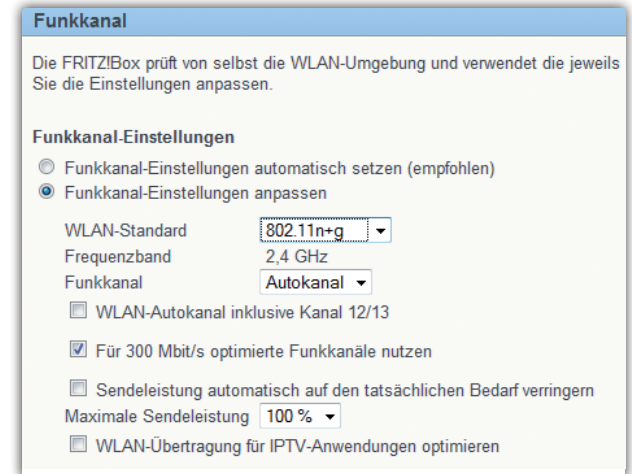
An dieser Stelle sehen Sie auf der Registerkarte „Treiber“, welche Version und welches Erstellungsdatum der von Ihnen verwendete Treiber besitzt. Überprüfen Sie danach, ob auf der Hersteller-Webseite eventuell eine neuere Version zum Download bereitsteht.

6 b-Geräte im g- oder n-Netzwerk

Sie besitzen ein Notebook, das mit dem Standard 802.11b arbeitet, und wollen es in Ihr brandneues 802.11n-Funknetzwerk integrieren. Das Gerät findet den Netzwerknamen (SSID); auch die Netzwerkschlüssel stimmen exakt überein – es kann sich seltsamerweise dennoch nicht verbinden.

Die Netzwerkstandards 802.11b, g und n sind natürlich kompatibel. Damit jedoch der langsamere Standard 802.11b ein g- oder n-Netzwerk nicht ausbremst, können Sie den WLAN-Router in der Administrationsmaske auf die Einstellung „nur g“ oder „nur 802.11n+g“ schalten.

Der große Nachteil dieser Einstellung: Die veralteten, aber noch vorhandenen b-Karten

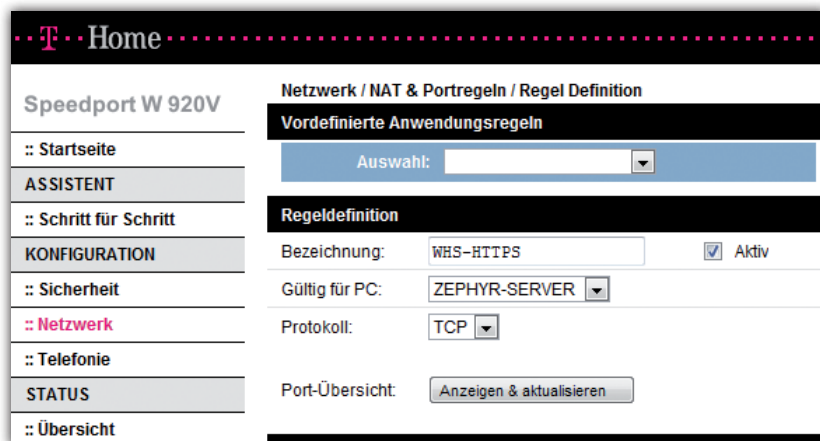


Mit dieser Einstellung sperrt die Fritzbox alle 802.11b-Geräte von der Nutzung des Drahtlos-Netzwerkes aus.

lassen sich nicht mehr ins Funknetzwerk einbinden. Überprüfen Sie also die WLAN-Einstellungen Ihres Routers und schalten Sie das drahtlose Netzwerk auf die Option „nur 802.11n+g+b“ um, wenn Sie auch anderen Geräten, die noch nach diesen älteren Standards funken, den Zugriff erlauben wollen.

7 Wichtige Ports gesperrt

Die im WLAN-Router integrierte Firewall erlaubt in der Grundeinstellung nur den Datenverkehr über gängige Ports. Wollen Sie aber eine P2P-Software laufen lassen oder einen Windows Home Server aufsetzen, bekommt das Programm keinen Zugriff auf das Internet, da der dazu benötigte Port gesperrt ist.



Damit aus dem Internet eintreffende Daten den WLAN-Router passieren dürfen, müssen Ports freigegeben und weitergeleitet werden.

Damit das Programm funktioniert, müssen Sie auf dem Router die benötigten Ports freigeben. Damit aber die Firewall ihre Schutzfunktion behält, sollten Sie nur die wirklich notwendigen Ports freigeben. Wollen Sie weitere Freigaben zur Firewall hinzufügen, finden Sie etwa unter www.iana.org/assignments/port-numbers eine ausführliche Liste von Anwendungen und deren zugehörige Ports.

8 Tatsächliche Reichweite des Funknetzes

Die WLAN-Reichweite ist von der Umgebung abhängig. Hersteller geben bis zu 50 Meter in Gebäuden und 100 bis 300 Meter im Freien als Maximalreichweiten an. Doch Wände, Bäume und Elektrogeräte verringern diesen Wert.

Die Frequenz eines WLANs liegt mit 2,4 oder 5 GHz sehr hoch, nämlich im Mikrowellenbereich. Deshalb können etwa Wassermoleküle die Energie aufnehmen und bei hoher Feuchtigkeit die Reichweite einschränken. Beachten Sie außerdem, dass mit wachsender Entfernung die Qualität der Verbindung sinkt – und damit auch die Geschwindigkeit.

Legen Sie den Access Point daher nicht in die hinterste Ecke unterm Schreibtisch, platzieren Sie ihn lieber oben im Regal, damit er gut in alle Himmelsrichtungen funkt. Auch sollte der WLAN-Router nicht direkt auf anderen Geräten liegen – vor allem nicht auf der Mikrowelle, die die gleiche Frequenz benutzt.

Ebenfalls zu beachten: Die Linie zwischen Access Point und Client sollte möglichst auf direktem Weg durch Zwischenwände gehen, also am besten im 90-Grad-Winkel zur Wand. Sonst legen die Funkwellen zu weite Wege durch die abschirmende Wand zurück.

9 Netzwerkgeräte mit unbekannter IP-Adresse aufspüren

Sie haben ein neues Gerät in Ihr Netzwerk integriert – oder vermuten, dass sich jemand unerlaubt in Ihr Netzwerk eingeklinkt hat. Da Sie aber die IP-Adresse nicht kennen, können Sie nicht handeln. Das ist nur die halbe Wahrheit.

Anstatt sich mit dem DOS-Kommandozeilen-Relikt „arp“ (Address Resolution Protocol), der alle Netzwerkgeräte auflistet, zu beschäftigen, greifen Sie zum kostenlosen Tool MAC Scanner 1.1 (www.colasoft.com).

Das englischsprachige Tool hilft nämlich auch dann weiter, wenn sich Ihr Netzwerkgerät in einem anderen Adressbereich aufhält. Für diesen Fall können Sie das Suchgebiet auf eine andere IP-Range umstellen und so die Adresse herausbekommen. Wenn Sie nun die gefundene IP-Adresse in die Adresszeile Ihres Browsers eingeben, gelangen Sie auf die Konfigurationsseite des Geräts.

10 WLAN-Router in ein bestehendes Netzwerk integrieren

In Firmennetzen übernimmt ein eigener DHCP-Server die Verteilung von IP-Adressen an die angeschlossenen Clients. Wollen Sie einen Access Point an ein solchermaßen konfiguriertes LAN anschließen, kann es zu Konflikten kommen, denn auch der WLAN-Router enthält einen eigenen DHCP-Server.

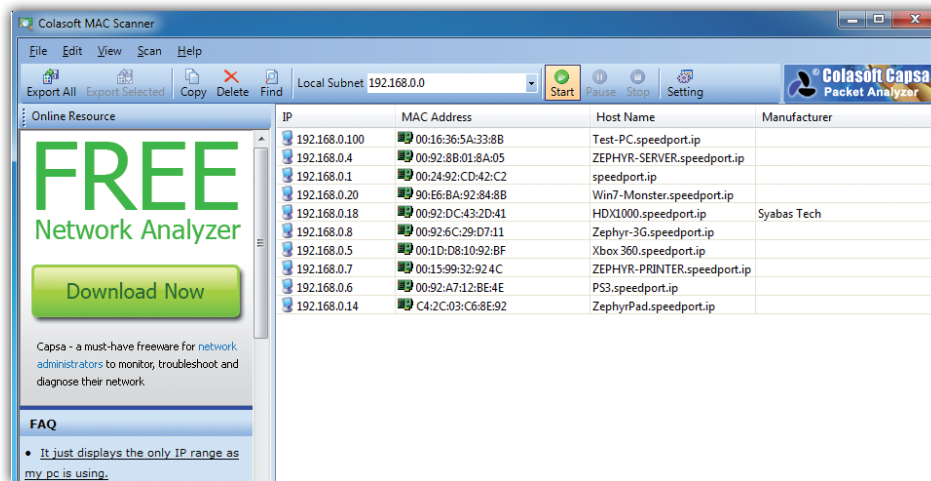
Verteilen darf die IP-Adressen eines Netzwerks immer nur ein Gerät, sonst könnten Adressen doppelt vergeben werden, und die Kommunikation wäre gestört. Deshalb kann man im Setup der Wireless-Geräte den DHCP-Server abstellen. Das sollten Sie tun, bevor Sie das lokale Netz mit eigenem DHCP-Server an Ihren Access Point anschließen. Andernfalls bekommen Sie früher oder später Ärger mit dem Netzwerkadministrator.

Bei einigen neuen Routern lässt sich der Adressbereich frei konfigurieren, sodass man ihn auch auf den Adressbereich des eigenen lokalen Netzes einstellen kann. Das kann zum Beispiel in Absprache mit dem Netzwerkadministrator geschehen: Er weist Ihnen einfach einen Adressbereich von zum Beispiel 20 Adressen zu, die Sie anschließend über Ihren Access Point lokal verteilen dürfen.

Arbeitet Ihr Rechner im IP-Adressbereich des Firmennetzes, können Sie in vielen Fällen nicht mehr auf das Web-Interface Ihres Access Point zugreifen. Die Konfigurationsmaske ist nämlich meist auf Adressen à la 192.168.x.x fest eingestellt – Zugriffe aus anderen Adressbereichen erlaubt er nicht.

Wollen Sie etwas an der Konfiguration ändern, müssen Sie die IP-Adresse Ihres Rechners per Hand auf einen Wert im Adressbereich 192.168.x.x einstellen. Den Eintrag für Standardgateway und DNS-Serveradresse können Sie frei lassen. Wichtig sind nur die lokale IP und die Subnetzmaske. Für Letztere nehmen Sie einfach den von Windows automatisch vorgeschlagenen Standard 255.255.x.x.

Nur wenn Sie im Router den Adressbereich des DHCP-Servers manuell angeben können, klappt die Integration in ein bestehendes LAN.



Mit dem kostenlosen Tool Colasoft MAC Scanner spüren Sie alle im Netzwerk vorhandenen Endgeräte auf.

11 DSL-Geschwindigkeit testen

Am Anfang ist es vielleicht nur ein Gefühl, dann wird es allmählich zur Gewissheit: Ihr DSL-Anschluss ist gar nicht so flott, wie der Provider es im Prospekt verspricht.

Wie aber lässt sich überprüfen, mit welchem Tempo die Daten übertragen werden? Ganz einfach: Mit einem DSL-Speedtest (siehe Bild auf Seite 37), den mehrere Dienstleister im Internet kostenlos anbieten. Sie finden solche webbasierten Geschwindigkeits-Checks beispielsweise unter www.speedmeter.de, www.speed.io oder www.dsl-speed-messung.de.

Es empfiehlt sich durchaus, an mehreren Tagen und zu unterschiedlichen Uhrzeiten

entsprechende Testläufe zu starten. Denn die Ergebnisse werden immer ein wenig schwanken. Was aber tun, wenn die tatsächliche Geschwindigkeit dauerhaft und deutlich unter der versprochenen und bezahlten Leistung liegt? Im Grunde genommen bleibt Ihnen nur ein Anbieterwechsel übrig. Denn die meisten Provider sichern sich über entsprechende Klauseln im Kleingedruckten, sprich in den Allgemeinen Geschäftsbedingungen (AGB), ab.

Geschwindigkeitsprobleme im WLAN können auch daher rühren, dass Geräte mit verschiedenen WLAN-Standards eingesetzt werden. Hier hilft meist ein Austausch der entsprechenden Komponenten.

12 Freigaben für Standardnutzer

Wenn Sie mit einem Windows-Rechner als Server im WLAN arbeiten, kann es sein, dass Sie nicht auf eine Freigabe zugreifen können. Und das, obwohl doch dort „Jeder“ als Standardnutzer eingetragen ist.

Der Grund: Windows fasst unter dem Gruppennamen „Jeder“ nur die in der Benutzerverwaltung bereits registrierten Benutzer zusammen – und erlaubt damit keineswegs den Vollzugriff von allen innerhalb des Netzwerks. Falls Sie also auf freigegebene Ordner nicht zugreifen können, obwohl dort „Jeder“ zumindest Leserechte hat, liegt es wahrscheinlich daran, dass Sie am Server gar nicht als Benutzer registriert sind. Die Lösung für das Problem ist denkbar einfach: Holen Sie die Registrierung nach, indem Sie ein neues Benutzerkonto einrichten.

13 Mehrere IP-Adressen anlegen

Viele netzwerkfähige Geräte lassen sich via Web-Interface konfigurieren. Fast immer gibt es eine werkseitig voreingestellte IP, die Sie nur in Ihren Browser eintippen müssen, um auf die Konfigurations-Oberfläche zu kommen. Schwierig wird es, wenn Sie in Ihrem Heimnetz einen anderen IP-Bereich verwenden. Die voreingestellte IP-Adresse des neuen Gerätes ist dann für Ihren Browser nicht erreichbar.

Bevor Sie jetzt Ihr gesamtes Netzwerk auf den IP-Bereich des neuen Gerätes umstellen, können Sie in Ihrem Rechner auch eine Art Brücke in den anderen IP-Bereich einrichten. Über die Eigenschaften der aktiven Netzwerkverbindung gelangen Sie an das TCP/IP-Protokoll (v4). Markieren Sie den Eintrag und klicken Sie auf „Eigenschaften“. Im nächsten Fenster gelangen Sie über „Erweitert...“ in ein Konfigurationsfenster, in dem Sie dann eine zusätzliche IP-Adresse eintragen können.

Wählen Sie eine Adresse, die sich nur im letzten Block von der vorgegebenen IP des



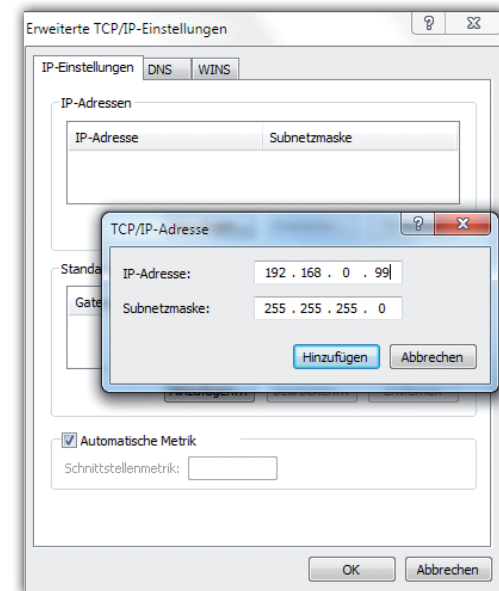
Webbasierte Geschwindigkeitstests geben Aufschluss, ob Ihre Internetverbindung so schnell ist, wie vom Provider behauptet.

neuen Gerätes unterscheidet. Sollte das Fenster mit dem Eintrag „DHCP aktiviert“ blockiert sein, müssen Sie eine Stufe zurückgehen und den Eintrag „IP-Adresse automatisch beziehen“ deaktivieren. Optimal ist es, wenn Sie in das Feld die Adresse eintragen, die der Rechner zuvor schon vom DHCP-Server (Router) bekommen hat. Diese Adresse finden Sie, wenn Sie im Kontextmenü der aktiven Netzwerkverbindung auf „Status“ und „Details“ klicken. Nachdem Sie Ihr neues Gerät eingerichtet – und DHCP eingestellt – haben, sollten Sie alle Änderungen an Ihrem Rechner rückgängig machen.

14 Mit fest zugewiesener IP-Adresse unterbrechungsfrei surfen

Auch so etwas kann passieren: Nach einigen Tagen korrekter Funktion bricht plötzlich die WLAN-Verbindung des angeschlossenen Notebooks zusammen.

Das Problem lässt sich nur über einen Router-Neustart beheben – die Reparaturfunktion von Windows ist machtlos. Das Problem entsteht durch die dynamische Vergabe der IP-Adressen (Internet Protocol) über DHCP (Dynamic Host Configuration Protocol). Sie können es vermeiden, indem Sie im Router eine feste IP-Adresse für das Notebook in Ihrem lokalen Netzwerk vergeben.



Sie können jedem Netzwerkadapter eine oder mehrere Alternativ-IP-Adressen zuweisen.

Starten Sie zuerst den Router neu, damit die Netzwerkverbindung wieder funktioniert, und schalten Sie danach alle beteiligten Rechner im Netzwerk ein. Dann melden Sie sich über den Browser an der Administrationsoberfläche des Routers an. Wenn Sie beispielsweise einen Speedport W502 nutzen, wählen Sie die Befehle „Netzwerk“ und „NAT & Portregeln“ und klicken dann auf „PCs übernehmen und freigeben“. Dort sehen Sie die aktuelle Zuordnung der internen IP-Adressen zu den einzelnen Rechnern. Klicken Sie für die jeweiligen Rechner auf

Profi-Tipp

Fritzbox 7270 als vollwertiger UMTS-Router

Wegen Baggerarbeiten, Providerwechsel oder Umzug sind Sie wochenlang ohne DSL-Anschluss. Sie haben eine arbeitslose Fritzbox und für unterwegs einen UMTS-Surfstick. Was liegt da näher, als beide zu verbinden? UMTS-Sticks funktionieren nicht nur direkt am Notebook oder PC. An eine Fritzbox Fon WLAN 7270 angeschlossen, machen sie diese zum vollwertigen HSDPA-Router. Abhängig von Datenvertrag, UMTS-Stick und verfügbarer Infrastruktur können Sie bis zu 7 MBit/s Downlink und über 5 MBit/s Uplink erreichen – das ist schneller als mancher DSL-Anschluss. Um den Stick zu nutzen, sollten Sie Ihre Fritzbox auf die aktuelle Firmware aktualisieren. Die Einrichtung über das Webinterface geht kinderleicht: Wählen Sie als Zugangsart einfach den Stick und als Anbieter Ihren Provider aus. Geben Sie zuletzt die PIN ein. Nachdem die Daten übernommen wurden, surfen Sie drahtlos über Ihre Fritzbox 7270.

„Übern.“, um diese Zuordnung fest zu speichern. Andere Modelle besitzen eine ähnliche Funktion zur festen Vergabe der IP-Adressen im Netzwerk. Damit ist das Problem grundsätzlich bereits behoben.

Wir empfehlen, auch auf Seiten der im Netzwerk verbundenen Rechner die feste Zuordnung vorzunehmen. Im Dialog „Eigenschaften“ suchen Sie im Register „Netzwerk“

unter „Diese Verbindung verwendet folgende Elemente“ den Eintrag für das „Internetprotokoll Version 4 (TCP/IPv4)“. Markieren Sie ihn und klicken Sie auf „Eigenschaften“. Ändern Sie im folgenden Fenster die Einstellung auf „Folgende IP-Adresse verwenden“. Hinter „IP-Adresse“ tragen Sie jetzt die jeweils im Router festgelegte Adresse ein, zum Beispiel „192.168.2.100“. Die „Subnetzmaske“ sollte stets „255.255.255.0“ sein. Als „Standardgateway“ verwenden Sie erneut die Einstellung des Routers, etwa „192.168.2.1“.

Speedport W 920V	
Status-Details / Netzwerk	
LAN	
Routename:	Speedport_W_920V_65-04-78
IP-Adresse Router:	192.168.0.1
Subnetzmaske:	255.255.255.0
MAC-Adresse LAN:	C2:24:C2:CD:42:C2
DHCP-Server:	Ein
Internetverbindung	
T-Online	Immer online
Öffentliche WAN-IP:	80.137.82.100
Gateway-Adresse:	87.186.224.66

Im Routermenü erfahren Sie, unter welchen IP-Adressen primärer und sekundärer DNS-Server zu erreichen sind.

Wichtig ist außerdem noch die richtige Adresse für „Bevorzugter DNS-Server“. Dieser Server sorgt für die Namensauflösung der Domänen, also die Umwandlung von

Profi-Tipp

Das richtige Passwort

Dass man sein Funknetz mit einer Verschlüsselung absichern sollte, dürfte klar sein. Empfehlenswert ist mindestens WPA, besser ist WPA2. Achten Sie aber darauf, hier kein zu einfaches Passwort einzustellen, das sich beispielsweise anhand einer so genannten Wörterbuch-Attacke knacken lässt. Solche Passwörter sind zwar leichter im Gedächtnis zu behalten, aber auch unsicherer. Besser sind Kombinationen aus Buchstaben, Ziffern und zugelassenen Sonderzeichen. Für WPA werden zudem mindestens acht Zeichen empfohlen. Wer ein nahezu unknackbares Passwort generieren will, findet Hilfestellung im Netz, etwa bei www.gajin.at.

www-Adressen in die numerischen IP-Adressen der Server. Alle Werte können Sie in den Konfigurationsdialogen des Routers nachsehen. Bestätigen Sie die Einstellungen schließlich mit „OK“ und prüfen Sie den Internetzugriff.

15 Fritzbox-Telefongespräch während der Aufnahme vom AB übernehmen

Sie sind oft nur Sekunden zu spät zum Telefon gekommen. Da war aber schon der Anrufbeantworter dran. Sie mussten warten, bis Ihr Gesprächspartner seine Mitteilung ausgesprochen hatte, bevor Sie zurückrufen konnten.

Wenn Ihre Telefonate über eine Fritzbox laufen, können Sie sich das Gespräch vom Anrufbeantworter heranholen. Drücken Sie dazu auf Ihrem Telefon die Tastenfolge „*09“. Voraussetzung ist, dass der Anrufbeantworter in der Fritzbox als Telefoniegerät angemeldet ist. Beim integrierten AB funktioniert das Ganze ohne weitere Einstellungen sofort.

Artur Hoffmann