

# Das Online Handbuch

Enthüllt: Providerwahl, E-Mail, eBay, Google,  
Skype, Chatten, Instant Messaging  
und vieles mehr

THOMAS JOOS



Markt+Technik

# 3



## Einrichtung der Hard- und Software

# KAPITEL 3

## Einrichtung der Hard- und Software

### Kapitelübersicht

- >> **Einrichtung der Hardware von ISDN und analogen Modems**
- >> **Oleco – der Internet Least Cost Router**
- >> **Anschluss und Einrichtung von DSL**
- >> **Hotspots – öffentliche WLANs**
- >> **DSL-Tuning**



Nachdem Sie sich für einen Provider entschieden haben und die DSL-Leitung geschaltet ist, müssen Sie zunächst die notwendige Hardware verkabeln und anschließen. Gehen Sie dazu wie in der Anleitung der Geräte beschrieben vor.

Auf den nächsten Seiten erfahren Sie den Aufbau, wie er für alle Geräte identisch ist. Einen Schwerpunkt dieses Kapitels habe ich auf den Anschluss der DSL-Komponenten gelegt, da diese Technologie am meisten verbreitet ist. Ferner gehe ich auf den Anschluss von ISDN und analogen Modems ein. Die Installation von Lösungen wie Kabel-TV und Powerline wird von einem Techniker durchgeführt, Sie selbst müssen keine Hardware installieren.

### 3.1 Einrichtung der Hardware von ISDN und analogen Modems

Wenn Sie mit ISDN oder einem analogen Modem einen Internetzugang einrichten wollen, müssen Sie zunächst die PC-Karte einbauen. Wenn es sich bei Modem oder ISDN-Karte um ein externes Gerät handelt, schließen Sie die dafür vorgesehene Verbindung an den PC an (bei ISDN meistens USB, bei Modems ein Com-Port).

Nachdem Sie die Hardware mit dem PC verbunden haben, muss die Software des Geräts, Treiber genannt, installiert werden. Meistens werden Sie automatisch nach einem Datenträger gefragt, legen Sie die CD des Herstellers ein und installieren Sie die notwendige Software.

Lesen Sie sich die Informationen durch, die während der Installation auftauchen, und beantworten Sie diese. Kleiner Tipp am Rande: Wenn Sie eine ISDN-Karte eines namhaften Herstellers wie AVM gekauft haben und eine der Meldungen nicht verstehen, antworten Sie mit *Ja* oder *Weiter*. Die Installation eines ISDN-Treibers dieses Herstellers wird Ihren Computer nicht zum Abstürzen bringen.

#### 3.1.1 Besonderheiten von ISDN-Karten

Bei ISDN-Karten muss außer dem Treiber noch der CAPI-Treiber installiert werden. Dieser Treiber ist für die Verbindung der Karte zur späteren Verbindung mit *Oleco* (siehe nächster Abschnitt) notwendig. Verbinden Sie den Anschluss der ISDN-Karte mit einem ISDN-Kabel oder einem Netzwerkkabel mit dem ISDN-NTBA.

Tipp . . . . .

*Sie können ein Netzkabel für die Verbindung zwischen ISDN-Karte und NTBA verwenden, aber Sie können kein ISDN-Kabel als Netzkabel zwischen den PCs oder von PC zu DSL-Router verwenden. Netzwerkkarten sind mit mehr Anschlüssen belegt als ISDN-Karten. Im Lieferumfang von ISDN-Karten ist meistens ein passendes ISDN-Kabel enthalten.*

*Der NTBA ist das Gerät, das an Ihrer Telefondose angeschlossen ist und an dem wiederum Ihre ISDN-Telefone oder Ihre ISDN-Telefonanlage angeschlossen ist. Der NTBA hat noch einen freien Anschluss, den Sie mit der ISDN-Karte im PC verbinden.*

### Genauere Installationsanleitung der Hardware

Gehen Sie für die Installation der Hardware Schritt für Schritt vor:

- >> Fahren Sie den PC herunter und stecken Sie alle Kabel aus (merken Sie sich, welches Kabel wo steckt, und machen Sie sich eventuell eine Skizze).
- >> Wenn Sie eine externe ISDN-Karte gekauft haben, verbinden Sie diese mit dem USB-Anschluss und dem Stromanschluss und dann das ISDN-Kabel mit der ISDN-Dose.
- >> Führen Sie diese Tätigkeiten wegen der statischen Entladung nicht auf dem Teppichboden aus.
- >> Schrauben Sie den Deckel des PCs auf, so dass Sie die Steckplätze sehen.
- >> Wählen Sie einen freien Steckplatz und bauen Sie die Karte ein. Entfernen Sie zuvor ein vorhandenes Steckblech. Vermeiden Sie auf jeden Fall den Kontakt mit der Hauptplatine. Schrauben Sie die Karte fest und schließen Sie den PC wieder.
- >> Schrauben Sie den Deckel zu und schließen Sie den PC wieder an.
- >> Fahren Sie das Betriebssystem hoch. Der PC müsste beim Starten melden, dass neue Hardware gefunden wurde.
- >> Legen Sie die Installations-CD in Ihr CD-ROM-Laufwerk.



Abbildung 3.1: Meldung von Windows XP, wenn neue Hardware gefunden wird

- >> Wenn Windows XP seinen Standardtreiber für die AVM Fritz!-Karte installiert, ist das kein Problem. Nach der Installation dieses Standardtreibers können Sie mit Hilfe der AVM-CD ein Update des Treibers und die Installation der notwendigen Programme durchführen. Stellen Sie sicher, dass sich die AVM-CD im Laufwerk befindet.
- >> Nachdem Windows die Installation abgeschlossen hat, verschwindet das Symbol für die Installation neuer Hardware und im *Gerätemanager* wird die Fritz!-ISDN-Karte ohne Fehler angezeigt. Den Gerätemanager finden Sie, wenn Sie auf *Systemsteuerung* -> *System* -> *Registerkarte Hardware* -> *Gerätemanager* klicken. Hier finden Sie die Fritz-!-ISDN-Karte unter *Netzwerkadapter*.

### Installation der notwendigen Software

Nachdem Sie die Hardware richtig installiert haben und Windows XP seinen Standardtreiber verwendet, sollten Sie den Treiber auf die aktuelle Version der AVM-CD updaten sowie die restlichen Programme von AVM zur Diagnose und Überwachung installieren. Gehen Sie dazu wie folgt vor:

- >> Wenn Sie die Autostart-Option der CD aktiviert haben, beginnt das Installationsprogramm automatisch. Wenn das Setup-Programm nicht automatisch startet, klicken Sie doppelt auf die Datei *Setup.exe* (wenn Dateieindungen bei Ihnen deaktiviert sind, wird die Datei nur als *setup* ohne Endung angezeigt).
- >> Wählen Sie die Option *Installieren* bzw. *Update* und klicken Sie so lange auf *Weiter*, bis die Installation beginnt. Zwischenfragen, ob Dateien überschrieben oder neu installiert werden sollen, können Sie immer mit *Ja* beantworten.
- >> Wenn das Betriebssystem meldet, dass Sie einen nicht signierten Treiber installieren, bestätigen Sie dieses Fenster und fahren mit der Treiberinstallation fort. Verfahren Sie so bei allen weiteren Fragen, die während der Installation des CAPI-Treibers auftreten.
- >> Nach ein bis zwei Minuten ist die Installation abgeschlossen und Sie werden zum Neustart des PCs aufgefordert. Nach dem Neustart können Sie mit der Installation der restlichen AVM-Software beginnen.

### *Installation der AVM-Software nach der Installation des Treibers*

- >> Nach dem Neustart des Rechners erscheint der Begrüßungsbildschirm der Installationssoftware. Klicken Sie hier auf *Weiter*.
- >> Lassen Sie die Software in den Standardinstallationsordner kopieren und wählen Sie als Installationsvariante ebenfalls *Standard*. Sie müssen an dieser Stelle keine Konfigurationen vornehmen.

### *Installation des CAPI-Treibers*

Im Anschluss erfolgt die wichtigste Installation, nämlich die des AVM-CAPI-Treibers. Diese Software ermöglicht es Oleco, die ISDN-Karte zu verwenden um damit eine Verbindung ins Internet aufbauen zu können. Installieren Sie die AVM-CAPI-Software und bestätigen Sie alle Meldungen des Betriebssystems.

Nach den Installationen der Software steht die ISDN-Karte zur Verfügung und Sie können fortfahren.

### 3.1.2 Besonderheiten zu Modems

Wenn Sie ein Modem einsetzen, verkabeln Sie das Gerät wie in der Anleitung beschrieben. Bei jedem Modem kommt ein Kabel ins Stromnetz, eines an den Rechner (der COM-Stecker passt nur an eine Buchse, Verwechslung nicht möglich) und ein Kabel wird mit der Telefondose verbunden.

Wenn Sie nur einen Anschluss für Ihre Telefondose zur Verfügung haben, müssen Sie sich in einem Elektromarkt einen Verteiler kaufen. Dieser hat ein Kabel, das Sie in die Dose stecken, und einen Anschluss für Ihr Telefon sowie zwei weitere für Anrufbeantworter oder Modem.

Nachdem Sie das Gerät ordentlich verkabelt haben, können Sie unter *Systemsteuerung -> Telefon und Modemoptionen -> Registerkarte Modems* das Modem installieren. Idealerweise ist beim Modem aber eine Installations-CD dabei, die Sie bei der Installation unterstützt. Wenn nicht, können Sie über die Registerkarte *Modems* mit Hilfe eines Assistenten Ihr Modem einrichten.

## 3.2 Oleco – der Internet Least Cost Router

Mit Oleco können Sie sehr kostengünstig mit ISDN oder analogem Modem per Internet-by-Call eine Verbindung ins Internet aufbauen.

*Wenn Sie noch Internetanfänger sind und über keinerlei Erfahrung im Internet verfügen, arbeiten Sie zunächst das Buch durch, bevor Sie sich entscheiden, ein solches Programm zu installieren.*

Stop .....

*Die nachfolgenden Installationsanleitungen sind für Internetnutzer gedacht, die bereits über etwas Erfahrung im Internet verfügen, eine installierte ISDN-Karte in ihrem PC haben und derzeit über eine teure Vertragsbindung surfen.*

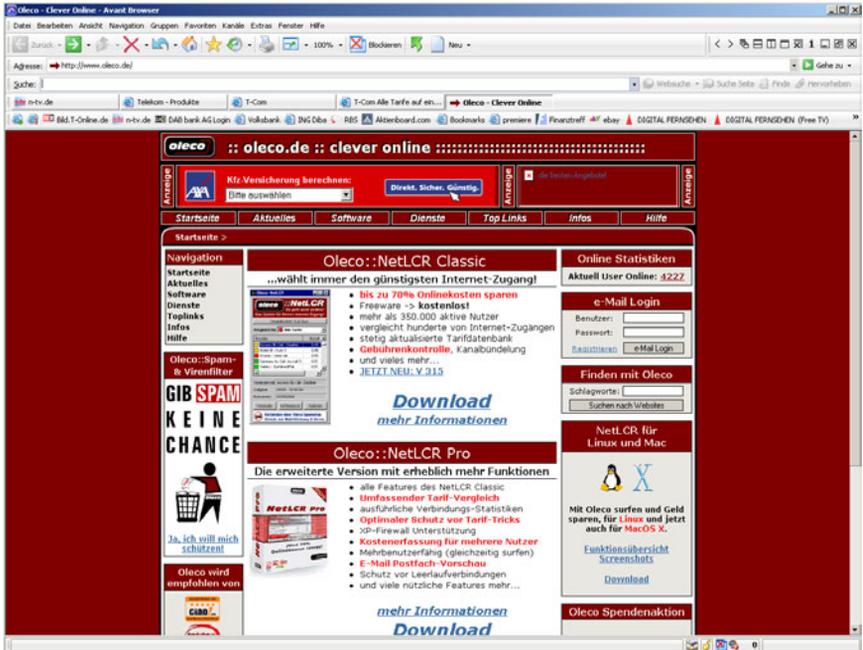


Abbildung 3.2: Downloadseite des Least Cost Routers Oleco

### 3.2.1 Download von Oleco

Sie finden Oleco auf der Internetseite [www.oleco.de](http://www.oleco.de).

Wenn Sie bereits einen Internetzugang haben, können Sie Oleco dort herunterladen. Sollten Sie noch über keinen Internetzugang verfügen, ist die beste Alternative, einen Freund zu fragen, der dies für Sie erledigt. Wenn Sie am Arbeitsplatz einen Internetzugang haben, laden Sie sich Oleco hier herunter oder fragen in Ihrer EDV-Abteilung nach. Irgendwie werden Sie das Programm bestimmt bekommen. Oleco hat eine Größe von 1,3 Mbyte und passt sogar auf eine Diskette.

Direkt auf der Startseite finden Sie den Downloadlink und können sich die Datei herunterladen. Auf dieser Seite finden Sie die Downloadmöglichkeit der Pro-Version. Für Privathaushalte reicht allerdings die Freeware-Version aus. Um das Programm herunterzuladen, klicken Sie mit der Maus auf den Link *Download*. Im nächsten Fenster klicken Sie auf den Link *Download hier*. Sie können die Datei lokal speichern.





Abbildung 3.4: Downloadfenster von Oleco



Abbildung 3.5: Warnung der Windows XP SP2 Firewall

Vor der Installation von Oleco müssen Sie Ihre ISDN-Karte installiert haben.

Im ersten Schritt müssen Sie die Lizenzvereinbarung akzeptieren und Ihre Vorwahl sowie die ersten drei Stellen Ihrer Telefonnummern eingeben. Auf Grund dieser Informationen kann Oleco bei der Verbindungsauswahl auf regionale Anbieter Rücksicht nehmen.

Im Installationsfenster wird das bereits installierte Modem vorgeschlagen. Wählen Sie im Dropdown-Menü das Modem bzw. die ISDN-Karte aus, über die Sie die Verbindung aufbauen wollen. Als Installationspfad können Sie es bei dem Vorschlag *C:\Programme\oleco* belassen. Lassen Sie die Verknüpfung im Startmenü und auf dem Desktop anlegen, damit Sie schnell und bequem an das Programm kommen.

Wenn alle Eingaben stimmen, können Sie mit einem Klick auf die Schaltfläche *Installieren* die Installation von Oleco starten. Nach der Installation erhalten Sie ein Warnfenster, das Sie darauf hinweist, dass die Datenbank für die Internetverbindungen nicht auf dem neuesten Stand ist. Sie müssen

einmal mit der ebenfalls günstigen Oleco-Verbindung ins Internet gehen, damit die Datenbank aktualisiert wird. Danach wird die Datenbank bei jedem weiteren Verbindungsaufbau automatisch erneut aktualisiert.



Abbildung 3.6: Installation von Oleco

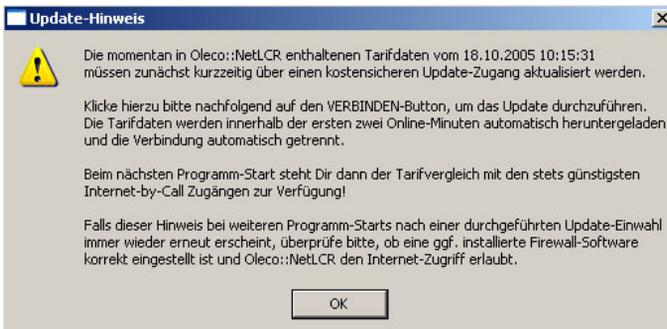


Abbildung 3.7: Meldung über nicht aktuelle Daten

### 3.2.3 Verbindungsaufbau mit Oleco

Nachdem Sie die Datenbank aktualisiert haben, zeigt Oleco beim Starten alle Verbindungsdaten und die dazugehörigen Kosten an. Oben im Startfenster wird eine Information über alle Verbindungskosten angezeigt, die bisher über Oleco angefallen sind. In der Spalte *Euro/h* sehen Sie die Kosten, wenn Sie eine Stunde mit dem ausgewählten Tarif mit dem Internet verbunden sind.



Abbildung 3.8: Oleco-Verbindungsdaten

Über die Schaltfläche *Verbinden* wird die ausgewählte günstige Verbindung angewählt und Sie sind mit dem Internet verbunden.

### Tipp .....

*Verbinden Sie sich nur mit Tarifen, die von Oleco empfohlen werden (grünes Viereck). Bei diesen Tarifen ist sichergestellt, dass der Provider die Gebühren gegenüber Oleco bestätigt hat und diese verbindlich sind. Alle anderen Tarife, solche mit einem gelben und roten Viereck, sollten Sie nicht verwenden, da nicht garantiert werden kann, ob sich der Provider an die Vereinbarungen hält.*

*Wählen Sie am besten einen Tarif dessen Takt mit »1« angegeben ist (nicht mehr in der Abbildung zu sehen, es ist die Spalte rechts von Euro/h).*

*Bei dieser Taktrate werden die Kosten pro Sekunde abgerechnet und nicht pro Minute. Das hat den Vorteil, dass Sie bei einer 30 Sekunden langen Verbindung, um zum Beispiel Ihre E-Mails herunterzuladen, wirklich nur 30 Sekunden bezahlen und keine ganze Minute. Wenn Sie viele kurze Verbindungen aufbauen, können Sie den einen oder anderen Euro durch sekundengenaue Abrechnung sparen.*

Wenn Sie die Schaltfläche *Kaffeekasse* drücken, bauen Sie eine Verbindung mit dem Oleco-Tarif auf. Zuvor erscheint ein Fenster, das Sie über die Kosten dieser Verbindung informiert. Diese Kosten werden auf Ihrer nächsten Telefonrechnung ausgewiesen. Oleco ist Freeware, wenn Sie spenden, helfen Sie auf diese Weise dem Entwicklungsteam.

Datum	Uhrzeit	Dauer	Kosten	Provider
06.04.05	16:07:10	00:06:01	0,054 Euro	Arcor - Basistarif
06.04.05	16:00:17	00:01:14	0,018 Euro	Germany by Call...
06.04.05	16:02:11	00:10:43	0,122 Euro	Freenet - Busin...
06.04.05	16:52:57	00:10:27	0,122 Euro	Freenet - Busin...
06.04.05	19:20:15	00:06:04	0,067 Euro	Freenet - Super...
06.04.05	19:35:04	00:03:40	0,038 Euro	Freenet - Super...

Gesamt Onlinezeit: 00:38:09      Gesamtkosten: 0,42 Euro

Löschen      Drucken      OK

**Wichtiger Hinweis:**  
Diese unverbindliche Gebühren-Übersicht kann aus software-technischen Gründen unvermeidliche Ungenauigkeiten enthalten. Selbstverständlich werden Dir vom jeweiligen Zugangs-Anbieter nur die tatsächlichen Kosten in Rechnung gestellt!

**Interessantere Verbindungs-Statistiken auch für mehrere Benutzer?**  
Teste kostenlos den erweiterten Oleco:NetL CR PRO !  
Infos findest Du auf der Produkt-Homepage <http://www.netlcrpro.de>

Abbildung 3.9: Gesamtkosten der Verbindungen mit Oleco

Wenn Sie auf die Schaltfläche *Gesamtkosten* klicken, zeigt Ihnen Oleco in einem neuen Fenster alle Kosten bei den Providern an, mit denen Sie bisher über Oleco eine Verbindung aufgebaut haben. Diese Informationen können Sie mit Ihrer Telefonrechnung vergleichen. Sie können sich die Verbindungskosten über die Schaltfläche *Drucken* ausdrucken lassen.

### 3.2.4 Konfiguration von Oleco

Über die Schaltfläche *Optionen* können Sie die Einstellungen von Oleco anpassen. Hier sollten Sie nur Änderungen vornehmen, wenn Sie genau wissen, was Sie tun. Notieren Sie sich vorsichtshalber zuvor die Standardeinstellungen, damit Sie gegebenenfalls die durchgeführten Änderungen wieder rückgängig machen können.

#### Registerkarte Gebühren

Im Konfigurationsfenster stehen Ihnen vier Registerkarten zur Verfügung, um Oleco an Ihre Bedürfnisse anzupassen. Die erste Registerkarte ist die Karte *Gebühren*.

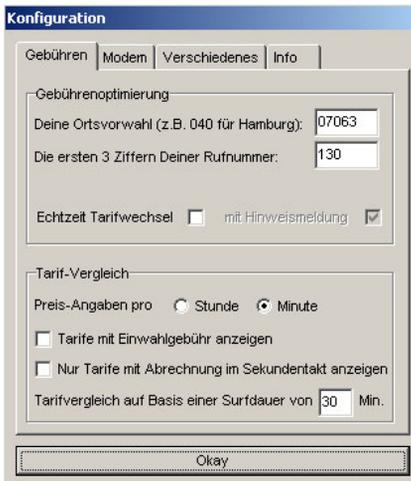


Abbildung 3.10: Konfiguration von Oleco

Auf dieser Registerkarte können Sie überprüfen, ob Ihre Ortsvorwahl und die ersten Stellen der Rufnummer stimmen. Anhand dieser Daten kann Sie Oleco mit günstigen Regionalanbietern verbinden. Wenn Sie die Option *Echtzeit Tarifwechsel* aktivieren, trennt Oleco die Verbindung zum Internet, wenn zum jeweiligen Zeitpunkt und während einer Verbindung ein anderer Provider einen besseren Tarif anbietet.

Viele Provider haben zu unterschiedlichen Uhrzeiten unterschiedliche Verbindungspreise. Wenn Sie die Option *mit Hinweismeldung* aktivieren, werden Sie vor dem Trennvorgang von Oleco informiert. Standardmäßig

Im Bereich *Tarif-Vergleich* können Sie weitere Optionen einstellen.

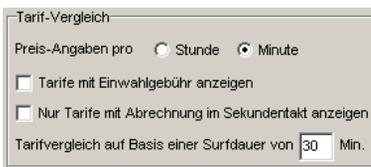


Abbildung 3.11: Tarif-Vergleich auf der Registerkarte »Gebühren«

Sie können sich die Preisangabe auf der Startseite in Minuten anzeigen lassen. Wenn Sie die Option *Tarife mit Einwahlgebühr anzeigen* aktivieren, werden auf der Startseite die Tarife angezeigt, die bei der Einwahl eine zusätzliche Einwahlgebühr verlangen. Diese Gebühren kommen zu den Verbindungskosten noch dazu. Die Aktivierung kann ich Ihnen nicht empfehlen, da die Kosten dadurch deutlich höher werden.

Bei Aktivierung der Option *Nur Tarife mit Abrechnung im Sekundentakt anzeigen* werden die bereits beschriebenen Tarife mit Minutentakt aus dem

Vergleich ausgeschlossen. Diese Option sollten Sie nur in Ausnahmefällen aktivieren.

Um den optimalen Tarif für Sie zu finden, geht Oleco von einer standardmäßigen Surfdauer von 30 Minuten aus. Wenn Ihre durchschnittliche Verbindungsdauer höher oder niedriger ist, können Sie die Zeitspanne hier verändern. Nach meiner Erfahrung sollte Sie diese Option so eingestellt lassen, wie sie ist, da die Erfahrungswerte aller Oleco-Nutzer in die Kalkulation mit einbezogen werden.

Weitere Einstellungen nehmen Sie auf der Registerkarte *Modem* vor. Hier können Sie Konfigurationen vornehmen, die Ihre ISDN-Karte oder Ihr analoges Modem betreffen.

### Registerkarte Modem

Zunächst können Sie auf dieser Registerkarte das Modem bzw. die ISDN-Karte ändern, die Oleco zum Verbindungsaufbau ins Internet verwenden soll. An dieser Stelle können Sie die ISDN-Kanalbündelung aktivieren. Eine Kanalbündelung ist ein Verbindungsaufbau mit zwei ISDN-Leitungen. Sie erreichen dadurch doppelte Geschwindigkeit, haben aber die doppelten Kosten. Nicht alle Internetanbieter unterstützen diese Kanalbündelung. Daher kann es bei Aktivierung durchaus zu Fehlern beim Verbindungsaufbau kommen.

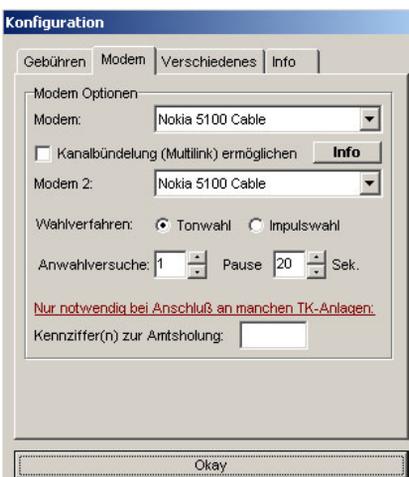


Abbildung 3.12: Registerkarte »Modem« der Oleco-Konfiguration

Das Wahlverfahren sollten Sie auf *Tonwahl* stehen lassen, da mittlerweile alle Verbindungsknoten dieses Wahlverhalten unterstützen. Wenn beim Verbindungsaufbau zum Provider einmal die eine oder andere Leitung besetzt sein sollte, können Sie auf dieser Registerkarte festlegen, wie oft Oleco einen Verbindungsaufbau versuchen soll. Die letzte Option ist für den Einsatz an einer Telefonanlage gedacht, bei der man eine Ziffer vorwählen muss.

## Stop .....

Falls die Auswahl fehlschlägt, sollten Sie in den Modemeinstellungen von Windows (Systemsteuerung) die Option Vor dem Wählen auf Freizeichen warten ausschalten.

### Registerkarte Verschiedenes

Die letzten Optionen finden Sie auf der Registerkarte *Verschiedenes*. An dieser Stelle können Sie weitere Einstellungen vornehmen.



Abbildung 3.13: Registerkarte »Verschiedenes« der Oleco-Konfiguration

Beim Öffnen der Anwendung können Sie sich verschiedene Informationen in der Titelleiste anzeigen lassen. Standardmäßig werden keine weiteren Informationen in der Titelleiste dargestellt. Folgende Informationen können Sie sich zusätzlich anzeigen lassen:

- >> *Gebühren*
- >> *Onlinezeit*
- >> *Zeit bis Taktende*

Sie können sich die Uhr Ihres PCs bei jedem Verbindungsaufbau zum Internet von einer Atomuhr stellen lassen. Diese Option ist standardmäßig in Oleco bereits aktiviert. Dadurch stellen Sie sicher, dass die Uhrzeit Ihres Rechners immer auf dem aktuellen Stand ist. Derzeit verwendet Oleco die Atomuhr der Universität Erlangen.

Wenn der Internet Explorer aufgerufen wird und noch keine Verbindung zum Internet besteht, versucht er automatisch den als Standardverbindung eingetragenen Anbieter anzuwählen. Dies kann ganz unbemerkt vom Benutzer geschehen. 0900-Dialer machen sich diesen Umstand zunutze. Oleco kann durch Aktivieren dieser Option veranlasst werden, einen Warnhinweis

zu zeigen, falls über die Standardverbindung versucht wird, eine Verbindung zum Internet aufzubauen.

Aktiviert man die Option *Startverhalten*, wird nach dem Trennen einer bestehenden Verbindung Oleco nicht beendet, sondern das Programm zeigt die Providertabelle und den derzeit günstigsten Tarif an.

### 3.2.5 Häufige Fragen zu Oleco und Probleme

*Wann und wie wird Oleco aktualisiert?*

Oleco aktualisiert sich automatisch beim Starten mit den neuesten Verbindungsdaten. Wenn Oleco länger als 30 Tage nicht benutzt wurde, wird eine Verbindung über einen für den Benutzer kostensicheren Zugang aufgebaut. Die Tarifdaten-Aktualisierung läuft innerhalb weniger Sekunden ab. Die Verbindung wird nach der Aktualisierung getrennt.

Wenn die Provider-Daten aktualisiert sind, besteht kein Zwang zur Aktualisierung. Allerdings empfiehlt es sich auf Dauer, immer mit der aktuellsten Version zu arbeiten. Sie können daher ab und zu mal auf der Oleco-Homepage überprüfen, ob eine neue Version zur Verfügung steht.

*Welche Telefonkosten fallen beim Verbindungsaufbau mit Oleco an?*

Neben Ihren Grundgebühren für den Telefonanschluss fallen bei Verwendung von Oleco nur die Kosten pro Sekunde/Minute an, die in den Tarifübersichten beschrieben sind.

Es kann im Gebührenzähler durchaus zu Abweichungen kommen, da der genaue Zeitpunkt einer Anrufannahme des Providers nicht ganz genau ermittelt werden kann. Allerdings sind die angezeigten Kosten in Oleco eher höher als die auf der Telefonrechnung, Sie haben also durchaus eine gewisse Sicherheit.

*Warum sind nicht alle Tarife enthalten?*

Durch die Vielzahl an Tarifen besteht durchaus die Möglichkeit, dass der eine oder andere Tarif noch nicht in Oleco angezeigt wird. In Oleco gibt es aber genügend günstige Tarife, die preislich durchaus ähnlich sind. Es kommt selten vor, dass ein Tarif nicht angezeigt wird. Tarife, die eine Anmeldung oder Registrierung erfordern, werden nicht angezeigt.

*Wie werden die Verbindungskosten abgerechnet, die mit Oleco entstehen?*

Alle Verbindungen, die über Oleco hergestellt werden, sehen Sie in der Telefonrechnung im Abschnitt *Beträge anderer Anbieter*. Oleco selbst kostet nichts.

*Oleco wählt keine Verbindung.*

Es kann viele Gründe geben, warum Oleco nicht wählt, aber zu 99 % liegen diese an Ihrem Computer und nicht an Oleco. Überprüfen Sie zunächst, ob alle Kabel richtig gesteckt sind und am ISDN-Anschluss oder Modem alle Lichter leuchten. Der Modem- oder ISDN-Treiber muss richtig installiert sein.

*Oleco und AOL*

Wenn Sie parallel zu Oleco einen AOL-Vertrag haben, kann es zu Problemen führen, die an der Konfiguration von AOL liegen. Wenn Sie mit AOL arbeiten, ist es äußerst schwierig, gleichzeitig Oleco einzusetzen.

*Wählt Oleco 0900er-Nummern?*

Oleco wählt niemals eine 0900er-Nummer. Wenn das bei Ihnen der Fall ist, hat sich eine Oleco-Fälschung eingeschlichen, die als Dialer arbeitet. Davor kann Sie Oleco leider nicht schützen.

*Unterstützt Oleco DSL?*

Oleco unterstützt derzeit keine DSL-Verbindungen.

*Wie beende ich eine Verbindung?*

Solange die Verbindung aufgebaut ist, befindet sich das kleine Oleco-Symbol in der Taskleiste (rechts unten bei der Uhr). Klicken Sie einfach doppelt auf das Symbol und trennen Sie die Verbindung. Sie können mit der Tastenkombination **[Strg]+[Alt]+[H]** die Oleco-Verbindung ebenfalls trennen.

*Was ist, wenn der günstigste Provider nicht funktioniert?*

Wählen Sie einfach den nächstgünstigen Provider aus.

*DFÜ-Wächter, 0900-Warner, Gebührenzähler, ISDN-/CAPI-Tools, Fritz!Web*

Alle Programme, die gleiche oder ähnliche Aufgaben wie Oleco übernehmen sollen, können zu wechselseitigen Beeinflussungen führen und sollten deshalb für die Dauer der Oleco-Einwahl deaktiviert werden. Im Zweifelsfall lässt sich einfach ausprobieren, ob bestimmte Programme mit Oleco kooperieren.

*T-Online-/AOL-Software*

Die beiden größten Provider nehmen mit ihrer Software zum Teil recht umfangreiche Änderungen am PC vor. Sie sollten generell auf die Zusatzprogramme beider Anbieter verzichten. Der Einsatz eines Tools wie Oleco macht keinen Sinn, wenn Sie ohnehin bereits einen Vertrag mit einem Online-Dienst eingegangen sind.

*Funktioniert Oleco im Ausland?*

Derzeit werden keine ausländischen Provider berücksichtigt.

## 3.3 Anschluss und Einrichtung von DSL

Nachdem Sie Ihren DSL-Anschluss und Ihren DSL-Tarif beantragt haben, schickt Ihnen der Provider die notwendigen Daten und Geräte zu. Das Datum der Aktivierung Ihres DSL-Anschlusses wird Ihnen ebenfalls mitgeteilt.

### 3.3.1 Inventur – ist alles da?

Am Tag der Aktivierung sollten Sie zunächst kontrollieren, ob alles zur Verfügung steht, was Sie für den DSL-Anschluss zum Internet benötigen:

- >> DSL-Splitter (siehe *Abbildung 3.14*)
- >> DSL-Modem oder Kombigerät mit DSL-Router
- >> Wenn Sie kein Kombigerät bestellt haben, benötigen Sie DSL-Splitter, -Modem und -Router als eigenständige Geräte.
- >> Bedienungsanleitung des DSL-Routers
- >> Netzkabel vom DSL-Router zu Ihrem PC
- >> DSL-Anschlusskabel vom DSL-Modem zum DSL-Router
- >> Anschlusskabel vom DSL-Splitter zum DSL-Modem
- >> Zugangsdaten des Internetproviders



Abbildung 3.14: DSL-Splitter

### 3.3.2 Anschluss der notwendigen Geräte und Kabel

Die Verkabelung unterscheidet sich abhängig davon, ob Sie ISDN oder einen analogen Anschluss einsetzen. Wenn Sie ein Kombigerät gekauft haben, unterscheidet sich die Verkabelung ebenfalls etwas, da keine Verbindung vom Modem zum Router hergestellt werden muss.

Auf den folgenden Seiten erfahren Sie genauer, wie Sie beim Anschluss Ihrer Geräte vorgehen sollen. Zur Erleichterung habe ich ein paar Grafiken erstellt, die Sie bei der Installation unterstützen sollen. Weitere sehr wichtige Hinweise finden Sie in *Kapitel 11.5*.

#### Installation bei analogem Anschluss ohne Kombigerät (DSL-Modem und DSL-Router eigenständige Geräte)

Wenn Sie DSL bei einem analogen Anschluss anschließen, müssen Sie keinen NTBA, keine Telefonanlage oder ISDN-Telefon berücksichtigen. Sie benötigen nur Ihr Telefon, den PC, den DSL-Splitter, das DSL-Modem und den DSL-Router.

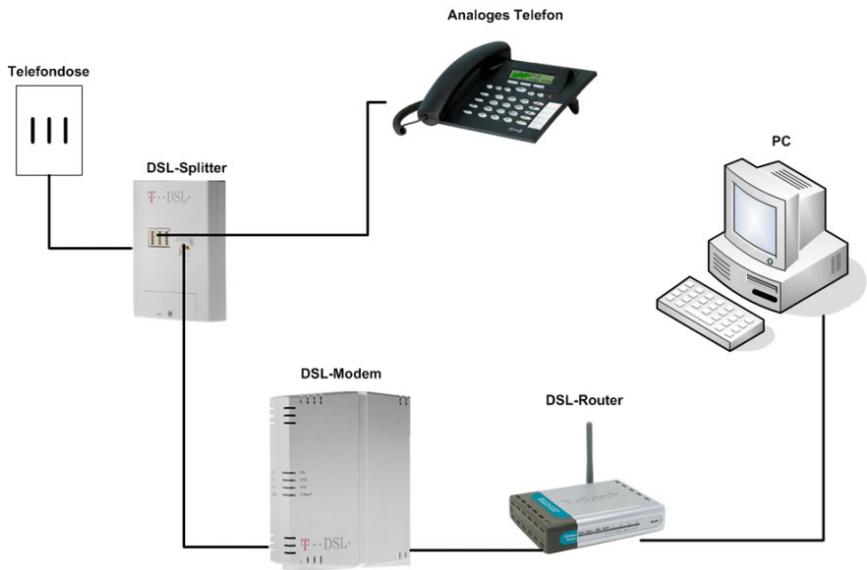


Abbildung 3.15: DSL-Anschluss mit analogem Telefonanschluss

- >> Zunächst müssen Sie den DSL-Splitter in die TAE-Telefondose an der Wand anschließen. Der DSL-Splitter wiederum hat drei zusätzliche Buchsen, an die Sie Ihr Telefon, Fax und Anrufbeantworter anschließen können. Schließen Sie zunächst den DSL-Splitter an und dann an den DSL-Splitter Ihr analoges Telefon, Anrufbeantworter oder Fax. Ihr Telefon sollte nach diesem Schritt normal funktionieren.

- >> Am entsprechenden Anschluss des DSL-Splitters wird, wie in *Abbildung 3.15* gezeigt, ein Kabel zum DSL-Modem gelegt. Während der DSL-Splitter die Aufgabe hat, das Telefonsignal vom DSL-Signal zu trennen, hat das DSL-Modem die Aufgabe, die abgesplitteten DSL-Signale zu verarbeiten. Wenn das DSL-Modem einen Stromanschluss hat, können Sie diesen als Nächstes einstecken.
- >> Am DSL-Modem befindet sich eine Leuchtdiode, die mit *Sync* oder *DSL* oder ähnlich beschriftet ist (schauen Sie dazu in der Anleitung des Geräts nach). Wenn Sie das Modem aktivieren, leuchtet dieses Licht zunächst rot, was bedeutet, dass noch kein Signal von der DSL-Gegenstelle empfangen wird, oder es blinkt. Dieses Licht sollte nach einigen Minuten grün leuchten, was signalisiert, dass das DSL-Modem Verbindung zu der Gegenstelle aufgebaut hat. Leuchtet dieses Licht weiter rot oder blinkt, sollten Sie den Support des Internetproviders anrufen, da dieser messen kann, ob Ihr Modem erreicht wird oder nicht.
- >> Im weiteren Schritt wird an das DSL-Modem der DSL-Router angeschlossen. Am DSL-Router ist der Anschluss für DSL als *WAN* oder *DSL* gekennzeichnet.
- >> Der PC wird mit einem Netzkabel an den DSL-Router angeschlossen (Steckplatz LAN oder ähnlich beschrieben).

### Installation bei analogem Anschluss mit Kombigerät (DSL-Modem und DSL-Router als ein Gerät)

Wenn Sie ein Kombigerät einsetzen, entfällt die Verkabelung von DSL-Modem zu DSL-Router und von DSL-Router zu PC. Es wird einfach wie zuvor der DSL-Splitter an das DSL-Modem angeschlossen und das DSL-Modem an den PC.

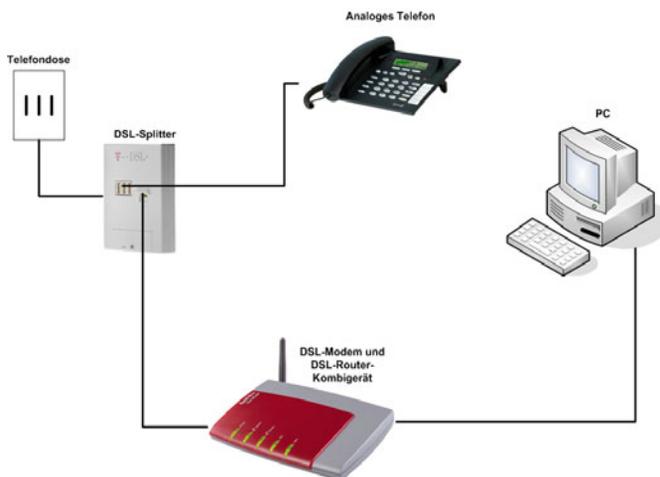


Abbildung 3.16: Anschluss bei analogem Telefonanschluss mit Kombigerät

Die entsprechenden Anschlüsse bei solchen Kombigeräten sind eindeutig beschrieben und nicht zu verwechseln. Überprüfen Sie jedoch bei jedem Steckvorgang, ob Sie das Gerät in den richtigen Anschluss am DSL-Router bzw. Kombigerät stecken. Sie können recht schnell einen Schaden am Gerät verursachen, wenn Sie unsachgemäß verkabeln.

**Installation von DSL bei ISDN**

Wenn Sie ISDN verwenden, ist es zunächst unerheblich, ob Sie ein Kombigerät oder getrennte Geräte für DSL-Router und DSL-Modem einsetzen. Die Unterschiede liegen lediglich in der Verkabelung des Telefons.

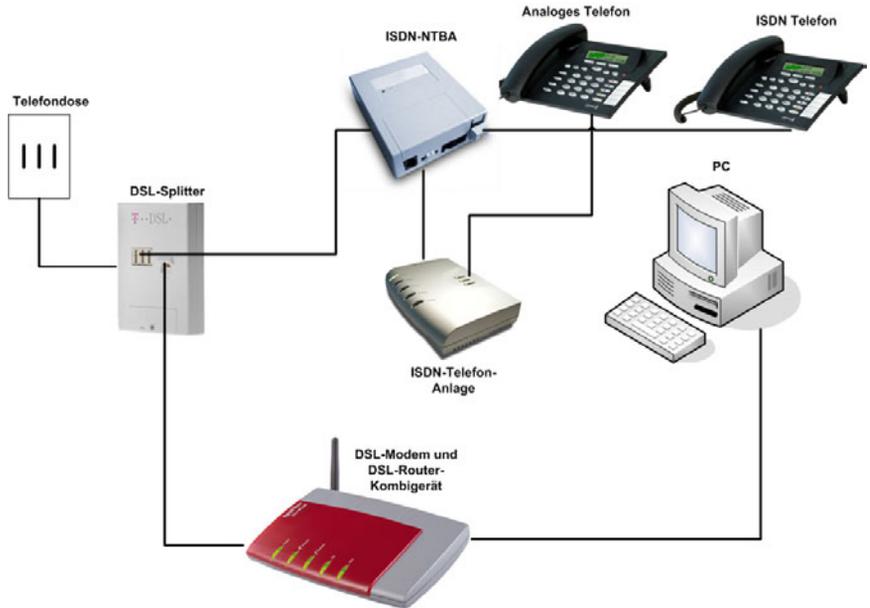


Abbildung 3.17: DSL-Anschluss bei ISDN

**3.3.3 Überprüfung der Installation**

Nachdem Sie alle Installationsmaßnahmen durchgeführt machen, sollte das DSL-Modem eine Verbindung zum DSL-Netz aufgebaut haben.

**Stop** .....

*Am DSL-Modem befindet sich eine Leuchtdiode, die mit Sync oder DSL oder ähnlich beschriftet ist (schauen Sie dazu in der Anleitung des Geräts nach). Wenn Sie das Modem aktivieren, leuchtet dieses Licht zunächst rot, was bedeutet, dass noch kein Signal von der DSL-Gegenstelle empfangen wird. Dieses Licht sollte nach einigen Minuten grün leuchten, was signalisiert, dass das DSL-Modem Verbindung zu der Gegenstelle aufgebaut hat. Leuchtet dieses Licht weiter rot oder blinkt, sollten Sie den Support des Internetproviders anrufen, da dieser messen kann, ob Ihr Modem erreicht wird oder nicht.*

Nach dem Anschluss sollten Ihre Telefone fehlerfrei funktionieren. Schalten Sie als Nächstes Ihren PC an. Am DSL-Router muss das Licht am entsprechenden LAN-Anschluss leuchten. Das zeigt an, dass der PC richtig mit dem DSL-Router verkabelt ist.

### 3.3.4 Verbindungsaufbau mit dem Provider

Im nächsten Schritt müssen Sie den DSL-Router so konfigurieren, dass er mit dem Internetprovider Verbindung aufbaut. Das DSL-Modem ist lediglich dazu da, die DSL-Leitung herzustellen und in Funktion zu halten. Ohne DSL-Modem ist kein Verbindungsaufbau zum Provider möglich. Es ist sehr wichtig, dass die DSL-Verbindung grün angezeigt wird, wodurch signalisiert wird, dass das Modem eine DSL-Verbindung hat. Ohne diese Verbindung ist eine weitere Konfiguration nicht möglich.

Halten Sie als Nächstes die Verbindungsdaten Ihres Providers bereit.

*Die Konfigurationsoberflächen der verschiedenen DSL-Router unterscheiden sich deutlich. Die Oberfläche, die Sie auf den nachfolgenden Abbildungen sehen, ist nicht unbedingt mit Ihrer identisch. Die einzelnen Bezeichnungen sind aber bei allen Routern sehr ähnlich. Viel können Sie an dieser Stelle nicht falsch machen. Bei einer fehlerhaften Konfiguration wird lediglich keine Internetverbindung hergestellt, Sie können nichts kaputtmachen. Seien Sie nicht frustriert, wenn eine Konfiguration nicht gleich funktioniert, sondern tasten Sie sich so lange in den Optionen vor, bis alles funktioniert.*

Info .....

Die Konfiguration von DSL-Routern erfolgt immer über eine so genannte *Weboberfläche*. Sie konfigurieren Ihren DSL-Router, indem Sie mit dem Internet Explorer Verbindung über das Netzwerk zum DSL-Router aufbauen. Die komplette Konfiguration wird über den Internet Explorer durchgeführt.

#### Konfiguration des DSL-Routers

Der erste Schritt besteht darin, zwischen DSL-Router und Ihrem PC eine Netzwerkverbindung herzustellen. Über diese Netzwerkverbindung werden Sie zukünftig die Verbindung mit dem Internet aufbauen.

#### Netzwerkeinstellungen des PCs

Um eine Verbindung zu Ihrem Router herzustellen, müssen Sie diesen zunächst wie beschrieben mit dem PC verkabeln und einschalten.

Stellen Sie zunächst sicher, dass die Leuchtdiode des LAN-Anschlusses Ihres PCs und die Leuchtdiode des Ports am DSL-Router, an den Sie den PC angeschlossen haben, leuchtet.

Die Konfiguration des Routers erfolgt über das Netzwerk mit dem Internet Explorer. Wenn Sie noch keine Erfahrung mit einem Browser haben, so werden Sie an dieser Stelle Ihre ersten (wertvollen) Erfahrungen machen. Der Netzwerkaufbau wird über TCP/IP hergestellt. Sie sollten vor der Konfiguration *Kapitel 1* und *Kapitel 2* durchgearbeitet und verstanden haben. Ansonsten wird die Konfiguration Ihres Routers zum Lotteriespiel.

Verwenden Sie parallel zu meinen Anleitungen das Handbuch Ihres Geräts. Sie können keinen Schaden anrichten, wenn Sie an dieser Stelle den einen oder anderen Fehler machen.

**IP-Adresse und DHCP-Funktion des Routers konfigurieren**

Wenn Sie den PC mit dem Router verbunden haben, sollte die Netzwerkverbindung in den meisten Fällen schon hergestellt sein. In *Kapitel 1* haben Sie gelesen, wie die IP-Adressierung eines PCs und von Netzwerkgeräten durchgeführt wird. Die Verbindung in einem Netzwerk wird mit dem TCP/IP-Protokoll hergestellt, wobei alle Geräte des Netzwerks eine eigene IP-Adresse haben müssen (wie alle Häuser in der Straße eine eigene Hausnummer haben).

Die meisten Router sind mit einer Funktionalität ausgestattet, die sich *DHCP* nennt. DHCP ist die Abkürzung für *Dynamic Host Control Protocol*.

Bei DHCP nimmt der Router die Funktion eines so genannten DHCP-Servers ein. Ein DHCP-Server hat eine gewisse Anzahl von IP-Adressen in seinem Vorrat, die er an PCs automatisch verteilen kann. Dazu müssen die Geräte so konfiguriert sein, dass Sie eine IP-Adresse von einem DHCP-Server annehmen. Die meisten Betriebssysteme, auch Windows XP und Windows Vista, sind standardmäßig so eingestellt. Wenn Ihr Router als DHCP-Server konfiguriert ist, hat Ihr PC automatisch eine IP-Adresse beim Start erhalten. Den Ablauf dieser Vergabe einer automatischen Zuweisung der IP-Adresse finden Sie in *Abbildung 3.18*. In Unternehmensnetzwerken, die fast alle mit DHCP arbeiten, läuft die Funktion genau gleich ab.

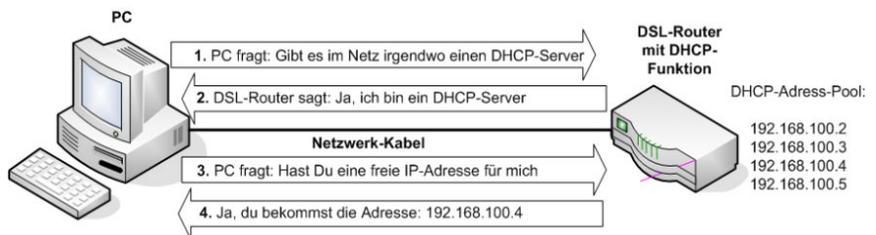


Abbildung 3.18: Vergabe von IP-Adressen

Es ist allerdings nicht immer sichergestellt, dass diese DHCP-Funktion eingestellt und aktiviert ist. Wenn die DHCP-Konfiguration des Routers nicht korrekt durchgeführt wurde, erhalten Sie keine IP-Adresse. Aber das ist kein Problem, Sie können die IP-Adresse an Ihrem PC sowie am DSL-Router

auch manuell vergeben. Man spricht in einem solchen Fall von einer statischen IP-Adresse im Unterschied zu einer dynamischen IP-Adresse bei DHCP. Bei den meisten Routern ist DHCP aktiviert.

### Testen des Verbindungsaufbaus zum DSL-Router

Zunächst müssen Sie in der Bedienungsanleitung lesen, wie Sie eine Verbindung zum DSL-Router herstellen können. Jeder Hersteller verwendet andere Möglichkeiten. Wenn Sie eine AVM Fritz!Box einsetzen, müssen Sie zum Beispiel *fritz.box* in das Adressfeld Ihres Internet Explorers eingeben.

Damit die Verbindung zum DSL-Router und die DHCP-Funktion funktionieren, hat der Hersteller den Router vorkonfiguriert.

Der Router braucht eine statische IP-Adresse und den dazugehörigen DHCP-Pool, um IP-Adressen an verbundene Computer vergeben zu können. In der Bedienungsanleitung finden Sie die IP-Adresse des Routers.

Oft wird darauf hingewiesen, dass Sie mit einem bestimmten *URL* Verbindung zu Ihrem Router aufbauen sollen. *URL* ist die Abkürzung für *Uniform Resource Locator*. Dies ist ein weiterer Fachbegriff, den Sie auf Ihren Reisen im Internet öfters finden werden. Ein *URL* ist nichts anderes als eine Internetadresse, zum Beispiel:

`http://www.telekom.de`

Ebenso wie die Internetseite der Telekom hat Ihr Router einen URL. Diesen URL erfahren Sie im Handbuch. Er wird wahrscheinlich irgendwie so aussehen:

`http://192.168.0.153`

oder:

`http://fritz.box`

Um Verbindung zu Ihrem Router aufzubauen, müssen Sie als Nächstes den Internet Explorer auf Ihrem Rechner starten:

*Start -> Programme -> Internet Explorer*

Wenn dieser mit einer Fehlermeldung startet, ist das kein Problem, Hauptsache, er öffnet sich und Sie können eine Adresse in das Adressfeld eingeben. Geben Sie den in Ihrer Bedienungsanleitung genannten URL in das Adressfeld des Internet Explorers ein. Nach kurzer Zeit sollte sich ein neues Fenster öffnen, in dem Sie sich authentifizieren müssen.

Geben Sie in dem Feld den Benutzernamen und das Kennwort an, um sich am DSL-Router zu authentifizieren. Diese Daten stehen in der Anleitung zu Ihrem Router. Wenn Sie die Daten eingegeben haben, sollte sich die Konfigurationsoberfläche des Routers aufbauen. Erscheint das Authentifizierungsfenster wieder, haben Sie sich vertippt. Geben Sie die Daten noch einmal ein.

**Stop .....**

Stellen Sie während der Konfiguration sicher, dass die beschriebene Authentifizierung zu Ihrem Router aktiviert ist, und ändern Sie das Standardkennwort des Routers zum nächstmöglichen Zeitpunkt auf ein Kennwort Ihrer Wahl ab. Wählen Sie aber kein einfaches Kennwort wie den Familiennamen oder Ähnliches. Wenn Ihr DSL-Router Wireless LAN-Funktionalität hat und der DHCP-Server aktiviert ist, kann jeder außerhalb Ihres Hauses mit einem Notebook Verbindung zum Router aufbauen. Der Einbrecher kann auf Ihre Kosten surfen oder Unsinn im Internet anstellen, für den Sie haften.

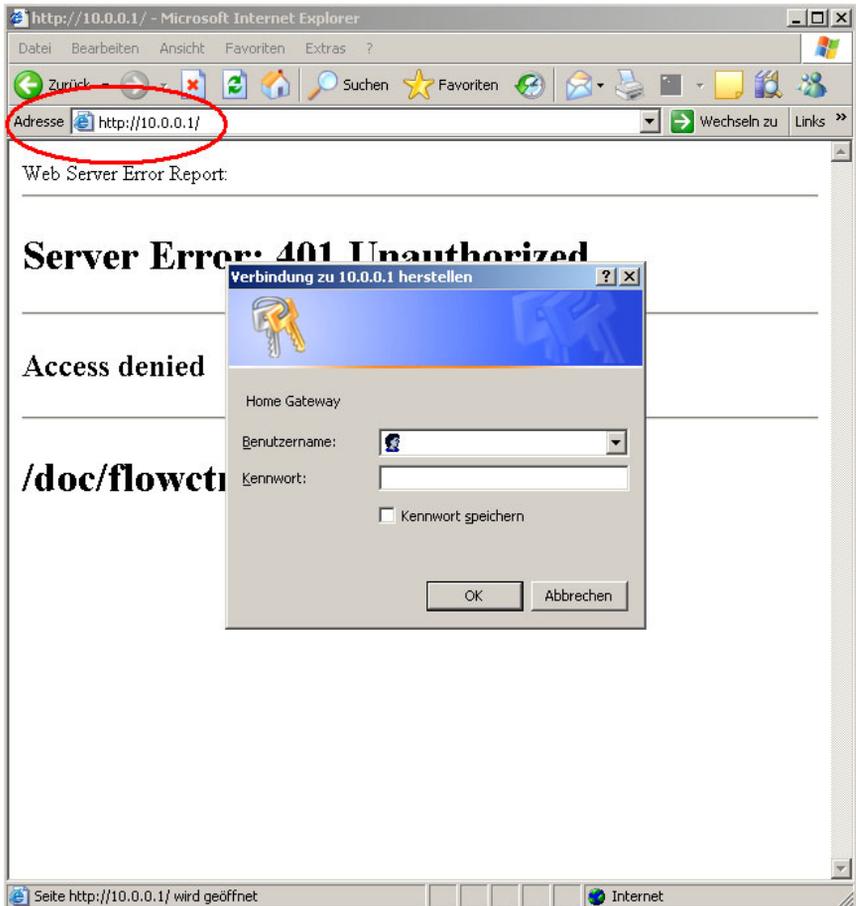


Abbildung 3.19: Eingabe des URL für die Konfiguration des Routers

Nachdem Sie sich mit den richtigen Daten an Ihrem Router authentifiziert haben, öffnet sich die Konfigurationsoberfläche.

Wenn Sie an dieser Stelle sind und das DSL-Synchronisierungslicht Ihres DSL-Modems leuchtet, haben Sie den größten Teil hinter sich gebracht und die Verkabelung richtig durchgeführt. Jetzt sind nur noch wenige Einstellungen vorzunehmen, damit Sie sich mit dem Internet verbinden können.

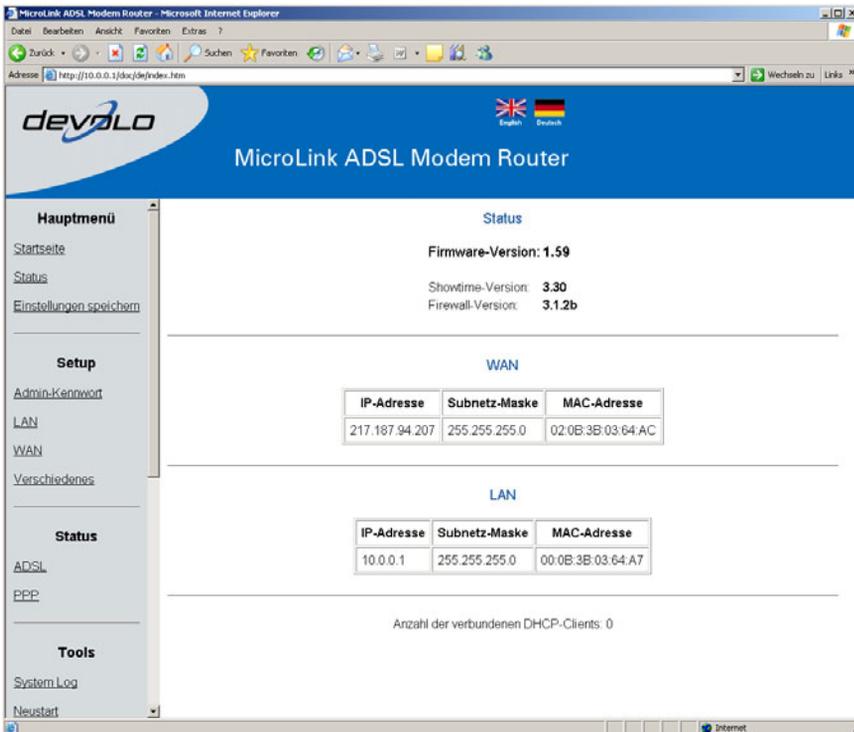


Abbildung 3.20: Konfigurationsoberfläche eines DSL-Routers

### Keine Verbindung zum DSL-Router – Fehlersuche

Wenn sich das Konfigurationsfenster nicht öffnet und keine Authentifizierung durchgeführt werden muss, ist die Verbindung zu Ihrem Router nicht hergestellt. Sie müssen sich auf die Fehlersuche begeben.

Wenn man in der EDV Fehler sucht, geht man immer nach dem Ausschlussprinzip vor. Man schließt mögliche Fehler aus, um dem eigentlichen Fehler näher zu kommen. In den nächsten Schritten gehe ich die Punkte durch, an denen der Verbindungsaufbau scheitern kann.

- >> Als Erstes sollten Sie sicherstellen, dass die Lichter des DSL-Routers leuchten und er eingeschaltet ist.
- >> Überprüfen Sie als Nächstes, ob das Netzkabel zwischen Router und PC richtig eingesteckt ist (Achtung! Sie können für die Verbindung zwischen Router und PC kein ISDN-Kabel verwenden, sondern nur ein Netzkabel).
- >> Überprüfen Sie, ob die Leuchtdioden am LAN-Anschluss des PCs leuchten. Es sollten zwei Dioden zu sehen sein. Eine Diode leuchtet fest und zeigt an, dass das Kabel mit einem anderen Netzwerkgerät verbunden ist und generell funktioniert. Das zweite sollte möglichst blinken

und zeigt dadurch an, dass Netzwerkverkehr zwischen den beiden Geräten hergestellt ist. Wenn ein Licht leuchtet, sind Sie schon einen Schritt weiter, es kann nur noch an der Konfiguration liegen. Leuchtet keine Diode, steckt das Kabel entweder am falschen Anschluss des Routers oder ist defekt. Das Kabel muss in einem Anschluss stecken, der mit *LAN*, *PC1-4* oder ähnlich beschriftet ist. Probieren Sie, ob ein anderes Kabel funktioniert.

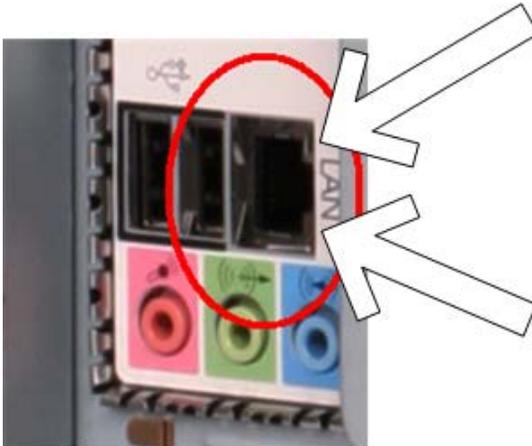


Abbildung 3.21: Leuchtdioden der LAN-Schnittstelle des Rechners

- >> Der nächste Schritt ist, dass Sie im BIOS überprüfen, ob die Netzwerkkarte überhaupt aktiviert ist. Starten Sie dazu den Rechner neu und gehen Sie in das BIOS des PC (meistens mit der Taste `[Entf]` oder `[F1]`). Schauen Sie sich alle Optionen an, bis Sie zur LAN-Schnittstelle kommen, und überprüfen Sie, ob diese auf *enabled* (aktiviert) steht. Ist sie *disabled* (deaktiviert), aktivieren Sie die Schnittstelle. Wenn die Schnittstelle nicht aktiviert war und Sie sie aktivieren, müssen Sie beim nächsten Starten des PCs sicherstellen, dass der Treiber für die Netzwerkkarte installiert und diese im Gerätemanager angezeigt wird. Zur Installation der Netzwerkkarte müssen Sie unter Umständen die Treiber-CD einlegen, die Sie beim Kauf Ihres PCs mitbekommen haben. Viele Netzwerkkarten werden von Windows XP automatisch erkannt und installiert. In diesem Fall brauchen Sie nur die Windows XP-CD.
- >> Nachdem Windows die Installation abgeschlossen hat, verschwindet das Symbol für die Installation neuer Hardware und im *Gerätemanager* wird die Netzwerkkarte ohne Fehler angezeigt. Den Gerätemanager finden Sie unter *Systemsteuerung* -> *System* -> *Registerkarte Hardware* -> *Gerätemanager*. Hier finden Sie die Netzwerkkarte unter *Netzwerkadapter*.

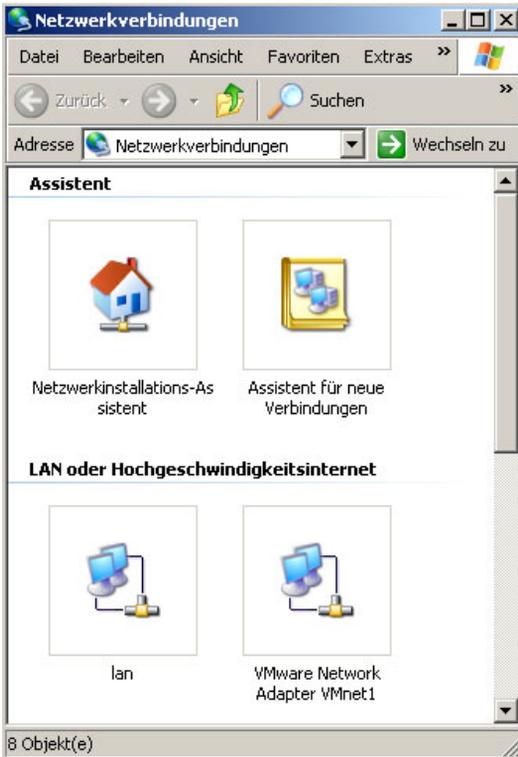


Abbildung 3.22: Netzwerkkumgebung eines PCs mit LAN-Verbindungen

- >> Wenn die Karte richtig installiert, der Router eingeschaltet und das Netzkabel verbunden ist, sollte das Verbindungslicht leuchten. In jedem Fall muss zunächst sichergestellt sein, dass dieses Licht leuchtet, erst dann steht fest, dass der PC mit dem Router kommunizieren kann.
- >> Überprüfen Sie als Nächstes in der *Netzwerkkumgebung* auf Ihrem Desktop, ob eine LAN-Verbindung angezeigt wird. Das ist ein sicheres Zeichen, dass die Netzkarte richtig installiert wurde.
- >> Wird hier keine LAN-Verbindung angezeigt, ist die Netzkarte nicht aktiviert oder nicht installiert. Die Netzwerkkumgebung finden Sie auf dem Desktop. Klicken Sie dazu mit der rechten Maustaste auf die *Netzwerkkumgebung* und wählen Sie *Eigenschaften*. Abhängig vom PC kann es durchaus vorkommen, dass mehrere Netzwerkverbindungen angezeigt werden, aber mindestens eine sollte zu sehen sein.



Abbildung 3.23: Status einer aktivierten Netzwerkverbindung

- >> Wird die LAN-Verbindung eines PCs angezeigt (Abbildung 3.22), kann es sich nur noch um ein Konfigurationsproblem handeln. In diesem Fall überprüfen Sie die Konfiguration der LAN-Verbindung. Überprüfen Sie, ob die LAN-Verbindung aktiviert ist. Wenn Sie eine LAN-Verbindung mit der rechten Maustaste anklicken, können Sie diese aktivieren oder deaktivieren. Die Verbindung muss aktiviert sein. Wenn Sie die Verbindung mit der rechten Maustaste anklicken, können Sie sich den Status der Verbindung anzeigen lassen. An dieser Stelle sollte hinterlegt sein, dass die Verbindung hergestellt ist (Abbildung 3.22).
- >> Wenn Ihre Hardware nicht defekt ist und richtig installiert wurde, müssen Sie sich die TCP/IP-Konfiguration Ihres PCs ansehen. Sie können in den TCP/IP-Einstellungen weitere Konfigurationen vornehmen sowie die Konfiguration der Verbindung überprüfen. Schauen Sie sich aber zunächst den Status der Netzwerkverbindung in der Netzwerkumgebung an.
- >> Wenn Sie im Status der Netzwerkverbindung keinen Fehler erkennen können, führt der nächste Weg zu den Eigenschaften der Verbindung. Diese erreichen Sie über die Schaltfläche *Eigenschaften* im Status der Verbindung oder indem Sie die LAN-Verbindung mit der rechten Maustaste anklicken und *Eigenschaften* wählen. Beide Wege führen zum gleichen Ziel, nämlich der Konfiguration Ihrer TCP/IP-Einstellungen.

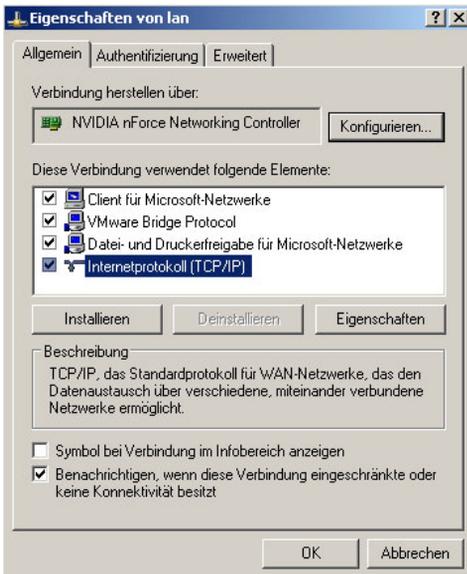


Abbildung 3.24: Eigenschaften einer LAN-Verbindung

- >> Wie Sie in *Abbildung 3.24* erkennen können, wird in den Eigenschaften der Netzwerkumgebung das TCP/IP-Protokoll angezeigt. Markieren Sie die Option *Internetprotokoll (TCP/IP)* und klicken Sie auf die Schaltfläche *Eigenschaften*.

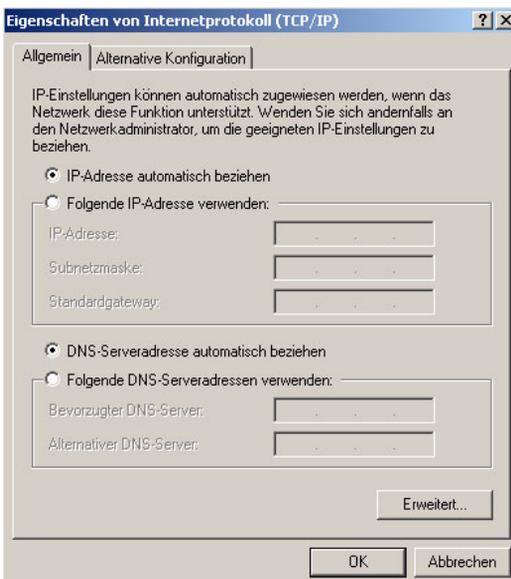


Abbildung 3.25: Eigenschaften von TCP/IP

- >> Bei Ihnen sollte die Konfiguration genauso aussehen wie in *Abbildung 3.25*. Ihre Netzwerkkarte ist in diesem Fall darauf konfiguriert, eine IP-Adresse vom DHCP-Server zu empfangen.
- >> Wenn sonst alles funktioniert, deutet das Problem darauf hin, dass der DHCP-Server in Ihrem Router nicht aktiviert ist, er keinen DHCP-Server hat oder dieser nicht funktioniert. In diesem Fall können Sie die Konfiguration jetzt manuell vornehmen. Denken Sie daran, dass Sie für alle weiteren PCs und Notebooks, die Sie mit dem DSL-Router verbinden, diese Einstellungen vornehmen müssen. Jeder PC benötigt eine eigene IP-Adresse und muss sich zugleich im selben Subnetz befinden, wie in *Kapitel 1* und *Kapitel 2* beschrieben.
- >> Wenn Sie die IP-Adresse manuell vergeben, setzen Sie die Markierung auf die Option *Folgende IP-Adresse verwenden* sowie die Option *Folgende DNS-Serveradressen verwenden* und tragen die notwendigen Daten ein (siehe unten).

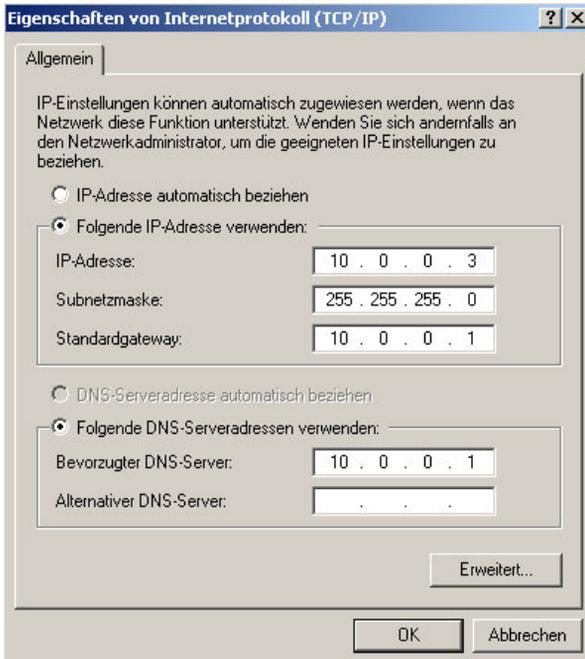


Abbildung 3.26: Konfiguration von statischen IP-Adressen

- >> In diesem Beispiel hat der DSL-Router die IP-Adresse *10.0.0.1*. Die Adresse Ihres Routers entnehmen Sie bitte der Anleitung. Es ist wichtig, dass Sie Ihrem PC eine IP-Adresse geben, die im selben Subnetz wie die des Routers ist. Am einfachsten geben Sie Ihrem PC die nächste Adresse. Wenn Ihr Router die IP-Adresse *192.168.170.1* hat, geben Sie Ihrem PC *192.168.170.2*.

- >> Tragen Sie in das Feld *IP-Adresse* eine IP-Adresse ein, die sich im selben Subnetz befindet wie die des. Fast alle Router verwenden als Subnetzmaske ein C-Klasse-Netz 255.255.255.0. Um eine richtige IP-Adresse in diesem Bereich zu wählen, müssen die ersten drei Stellen identisch mit der Adresse des Routers sein. In diesem Beispiel wäre das 10.0.0.x Wählen Sie als letzte Stelle eine Zahl, die sich von der des Routers unterscheidet. Im Beispiel habe ich die 3 gewählt. Die IP-Adresse des PCs ist 10.0.0.3. Wenn Ihr Router die IP-Adresse 192.168.0.253 hat, wählen Sie zum Beispiel 192.168.0.10. Die ersten drei Stellen sind gleich, die letzten unterscheidet sich. Tragen Sie bei *Subnetzmaske* noch das C-Klasse-Netz ein (255.255.255.0).
- >> Bei *Standardgateway* tragen Sie die IP-Adresse des DSL-Routers ein. Das *Standardgateway* hat die Aufgabe, alle Netzwerkanfragen, die nicht zum internen Netzwerk geschickt werden, ins Internet zu schicken. Dazu muss der PC wissen, wie die Adresse dieses Standardgateways lautet.
- >> Bei *DNS-Server* tragen Sie ebenfalls die IP-Adresse des Routers ein.

*Ein DNS-Server (Domain Naming Service) ist dafür zuständig, IP-Adressen und Namen im Internet zu verbinden.*

Info .....

*Wie Sie wissen, hat jeder PC im Internet eine eigene IP-Adresse. In Ihrem Browser geben Sie jedoch nicht diese IP-Adresse ein, sondern den URL zum Beispiel <http://www.telekom.de>.*

*Der PC muss wissen, wo er diesen URL finden kann. Dazu fragt er seinen DNS-Server, in unserem Fall den Router. Der Router wiederum fragt den DNS-Server Ihres Providers. Dieser wird ihm mittels DHCP automatisch bei der Anmeldung ins Internet zugewiesen.*

*Ohne diesen Eintrag werden Sie später mit Ihrem Webbrowser zwar ins Internet kommen, es kann sich aber keine Seite aufbauen, weil der Webbrowser nicht weiß, wo er die Internetseiten finden kann.*

- >> An dieser Stelle ist die Konfiguration der Netzwerkeinstellungen abgeschlossen und Sie können mit OK die Konfiguration beenden. Schließen Sie alle Fenster. Im nächsten Schritt überprüfen Sie, ob Ihr PC Verbindung mit dem DSL-Router über das Netzwerk aufbauen kann.
- >> Zur Überprüfung der Netzwerkverbindung verwenden wir den *Ping*-Befehl. Dieser Befehl ist Bestandteil des Betriebssystems. Er dient dazu, zu überprüfen, ob sich zwei Netzwerkgeräte miteinander unterhalten können. Dazu schickt der pingende PC ein Netzwerkpaket zu einer IP-Adresse. Diese Adresse antwortet auf das Paket. Das Ergebnis wird daraufhin auf Ihrem Bildschirm angezeigt. Antwortet die Gegenstelle ohne Fehler, können Sie davon ausgehen, dass die Netzwerkverbindung funktioniert. Um ein anderes Netzwerkgerät anzupingen, müssen Sie eine Kommandokonsole öffnen.

- >> Klicken Sie auf den *Start*-Knopf und wählen Sie *Ausführen*. Geben Sie in dem Feld *Ausführen* den Befehl *cmd* ein und klicken Sie auf *OK*, es öffnet sich daraufhin eine Kommandokonsole.

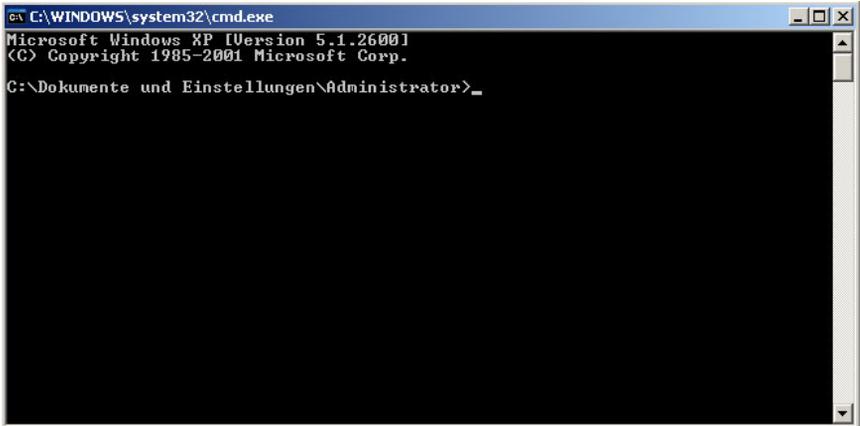


Abbildung 3.27: Geöffnete Kommandokonsole

- >> Im nächsten Schritt geben Sie den Befehl *ping* gefolgt von der IP-Adresse Ihres DSL-Routers ein.

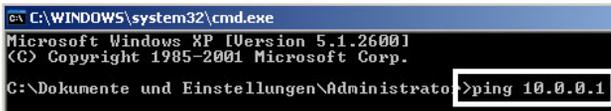


Abbildung 3.28: Eingabe des Ping-Befehls

- >> Drücken Sie auf die Taste . Der Befehl beginnt mit seiner Arbeit, verschickt Netzwerkpakete zu dem Router und dieser schickt sie zurück. Erst wenn der Router diese Pakete fehlerfrei zurückschickt, können Sie sicher sein, dass die Netzwerkverbindung einwandfrei funktioniert. Wenn der Verbindungsaufbau zu der Weboberfläche noch immer nicht funktioniert, können Sie ein physikalisches Verbindungsproblem ausschließen. Wenn Sie keine Antwort auf Ihre Pakete bekommen oder eine Fehlermeldung, überprüfen Sie noch einmal ganz genau, ob Sie die richtigen IP-Einstellungen vorgenommen haben und sich kein Tippfehler eingeschlichen hat.
- >> Wenn Sie den Router gebraucht gekauft haben, überprüfen Sie, ob Sie irgendwo einen Knopf für das Zurücksetzen auf die Werkseinstellungen finden. Eventuell hat der Vorbesitzer die IP-Adresse des Routers geändert.
- >> Wenn Sie eine positive Antwort des Routers erhalten, ist die Netzwerkkonfiguration in Ordnung und Sie können den Verbindungsaufbau zur Weboberfläche testen. Die Antwortzeiten sollten wie in *Abbildung 3.29* aussehen.

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Dokumente und Einstellungen\Administrator>ping 10.0.0.1

Ping wird ausgeführt für 10.0.0.1 mit 32 Bytes Daten:

Antwort von 10.0.0.1: Bytes=32 Zeit=1ms TTL=64
Antwort von 10.0.0.1: Bytes=32 Zeit=1ms TTL=64
Antwort von 10.0.0.1: Bytes=32 Zeit<1ms TTL=64
Antwort von 10.0.0.1: Bytes=32 Zeit<1ms TTL=64

Ping-Statistik für 10.0.0.1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
    Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 1ms, Mittelwert = 0ms

C:\Dokumente und Einstellungen\Administrator>

```

Abbildung 3.29: Positive Antworten des DSL-Routers

>> Wenn der Verbindungsaufbau noch immer nicht funktioniert, haben Sie mit Sicherheit eine Personal Firewall installiert. Diese blockiert die Signale zum Router. Deaktivieren Sie die Firewall für die Konfiguration des Routers und testen Sie, ob nach der Deaktivierung der Verbindungsaufbau funktioniert.

### Konfiguration des DSL-Routers

Nachdem Sie sich erfolgreich am Router authentifiziert haben, sollte sich die Konfigurationsoberfläche des Routers aufbauen.

#### Allgemeine Informationen

Abhängig von Modell und Hersteller sieht die Oberfläche unterschiedlich aus. Die einzelnen Schritte zur Konfiguration sind allerdings ähnlich, haben aber oft etwas abweichende Bezeichnungen.

Wenn Sie sich ein bisschen durch die Konfiguration geklickt haben, werden Sie recht schnell die passenden Einstellungen an Ihrem Router finden. Viel müssen Sie am Router nicht konfigurieren, da die meisten Dinge bereits vom Werk aus richtig eingestellt wurden. Einige Einstellungen, wie die Eintragung der Providerdaten, müssen vorgenommen werden. Wenn es sich bei Ihrem Router um ein Wireless-LAN-fähiges Gerät handelt, müssen Sie diese Funktion ebenfalls konfigurieren.

*Da es sich bei DSL-Routern mit eingebautem Wireless-LAN um Geräte handelt, die per Funk außerhalb Ihres Haushalts erreichbar sind, sollten Sie den Abschnitt weiter hinten in diesem Kapitel über Wireless LAN auf jeden Fall berücksichtigen. Ein WLAN ist eine Einladung für Hacker und Jugendliche, die sich einen Spaß machen, in der Nachbarschaft DSL-Router mit offenen Funknetzwerken aufzuspüren.*

*Bevor Sie die Wireless-LAN-Schnittstelle aktivieren, arbeiten Sie zunächst den Abschnitt über die Wireless-LAN-Sicherheit in diesem Kapitel durch und stellen die entsprechenden Optionen in Ihrem Router ein. Wenn Ihr DSL-Router keinen Funkzugang hat, können Sie diesen Abschnitt überspringen.*

Stop .....

Die DSL-Konfiguration umfasst folgende Bereiche:

- >> Zugangsdaten des Providers
- >> Einstellung der Router-Firewall für die Sicherheit

*Eintragen der Providerdaten*

Der erste und wichtigste Schritt ist das Eintragen des Benutzernamens und des Kennworts, welches Sie von Ihrem Provider zur Auswahl erhalten haben.

Wenn der Benutzername in den Unterlagen nicht eindeutig definiert ist, lassen Sie sich vom telefonischen Support die genaue Syntax des Benutzernamens in einem DSL-Router durchgeben. Idealerweise hat Ihnen der Provider bereits einen eindeutigen Namen und Kennwort zugeteilt.

Tragen Sie die Daten in Ihren DSL-Router ein. Meistens finden Sie diesen Bereich unter WAN (für Wide Area Network), PPP. Klicken Sie sich durch das Menü des Routers durch. Benutzernamen und Kennwort kann man nur an eine Stelle eintragen. Wenn Sie das Feld gefunden und die Daten eingetragen haben, bestätigen Sie Ihre Eingaben im Webbrowser. Oft gibt es innerhalb des Fensters noch einen speziellen Link oder eine Schaltfläche, auf die Sie klicken müssen, damit die Informationen gespeichert werden.

Wenn Sie die Daten eingetragen und gespeichert haben, verlassen Sie das Konfigurationsmenü und starten den Router neu. Verbinden Sie sich wieder und überprüfen Sie, ob Ihre Daten gespeichert wurden.

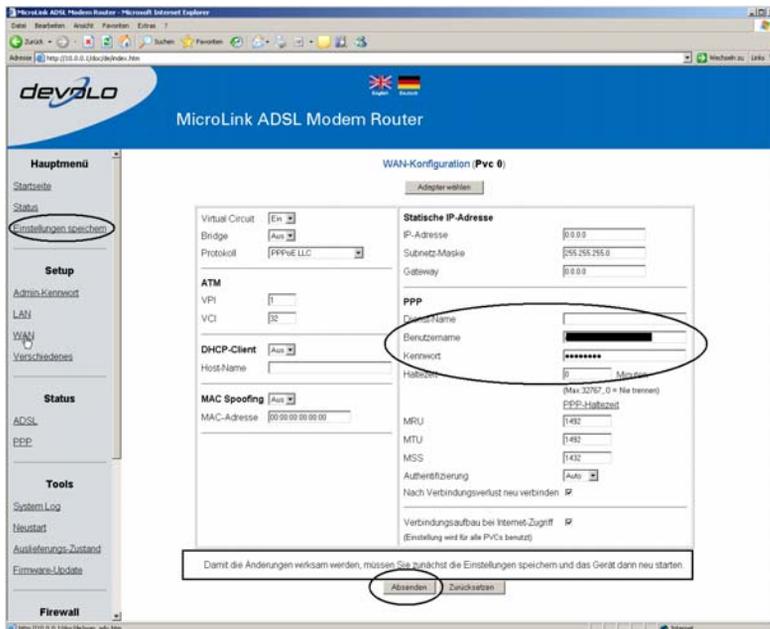


Abbildung 3.30: Konfiguration von Benutzernamen und Kennwort

Sie können auf den einzelnen Seiten noch verschiedene andere Optionen einstellen. Ändern Sie aber nur Optionen, deren Bedeutung Ihnen was sagt. Die anderen Einstellungen lassen Sie am besten so, wie sie bereits werkseitig hinterlegt sind.

### *Konfiguration des Verbindungsaufbaus*

Außer Ihren Providerdaten sollten Sie innerhalb der verschiedenen Menüs noch die unten aufgezählten Punkte konfigurieren. Die benannten Konfigurationen können an verschiedenen Stellen des Menüs untergebracht sein.

- >> *Verbindungsaufbau bei Internetzugriff.* Diese Option besagt, dass der Router sich mit Ihrem Provider verbindet, sobald auf einem PC eine Abfrage ins Internet gestartet wird. Diese Option sollte bei Ihrem Router gesetzt sein, um sicherzustellen, dass ein Verbindungsaufbau zum Internet stattfindet, sobald Sie auf Ihrem PC den Webbrowser starten.
- >> *Haltezeit.* Irgendwo in den Optionen sollte hinterlegt sein, wie lange der Router die Verbindung mit dem Internet aufrechterhält, wenn keine Internetanfragen von den PCs mehr kommen. Der Router wird automatisch die Verbindung trennen, wenn über den definierten Zeitpunkt keine Verbindung mehr gebraucht wird. Bei den meisten Routern können Sie diesen Bereich so konfigurieren, dass die Verbindung dauerhaft bestehen bleibt. Eine solche Einstellung macht aber nur bei Flatrates Sinn. Bei Volumen- und vor allem bei zeitbasierten Tarifen sollten Sie die Verbindung so kurz wie möglich bestehen lassen. Idealerweise sollten Sie bei Volumen- oder Zeittarifen den Router ausschalten, wenn Sie ihn nicht mehr benötigen.
- >> *Nach Verbindungsverlust neu verbinden.* Diese Option besagt, dass der Router sofort wieder eine Internetverbindung aufbaut, wenn diese durch den Provider oder Leitungsschwierigkeiten unterbrochen wird.

Weitere Optionen müssen Sie bezüglich der Verbindungen nicht einstellen. Lassen Sie die Einstellungen in Ihrem Router so, wie sie werkseitig vorgenommen wurden. Sie können die Einstellungen später immer noch ändern, wenn dazu Bedarf besteht.

### *Aktivierung der Firewall*

Normalerweise ist die Firewall bei den einzelnen DSL-Routern bereits standardmäßig aktiviert. Überprüfen Sie aber in den Einstellungen, ob die Firewall Ihres DSL-Routers eingeschaltet ist. Meistens finden Sie diese Einstellungen unter *Firewall*, *SPI-Firewall* oder irgendeine Bezeichnung mit NAT (*Network Adress Translation*).

Die Firewall in DSL-Routern ist eine so genannte *Stateful Inspection*-Firewall. Sie lässt Datenpakete von Ihrem internen Netz ohne Probleme nach außen. Versucht aber ein Angreifer von außerhalb eine Verbindung aufzubauen, lässt das die Firewall nicht zu.

Es gibt hunderte Programme, die von verschiedenen Internetnutzern dazu verwendet werden, das Internet nach Routern mit deaktivierter Firewall zu durchsuchen, um Schaden anzurichten. Es findet kein gezielter Angriff statt, sondern Sie werden nur Opfer des Zufalls, wenn Sie sich nicht schützen. Nach meinen Erfahrungen kommt es oft binnen einer Minute, nachdem man sich ins Internet eingewählt hat, zu einem Angriff. Die Firewall des Routers ist die erste Bastion vor Angriffen aus dem Internet.

An dieser Stelle ist Ihr Router für den Verbindungsaufbau konfiguriert. Starten Sie den Router gegebenenfalls neu. Nach dem Neustart sollte die Verbindung zum Internet aufgebaut werden. Sie sehen das bei jedem Router an einer anderen Stelle. Zum einen sollte es ein spezielles Kontrolllicht auf der Vorderseite des Routers geben, zum anderen sollten Sie in der Konfiguration des Routers sehen, dass er sich mit dem Internet verbunden hat. Spätestens wenn die WAN-Schnittstelle, die Schnittstelle ins Internet, eine IP-Adresse vom DHCP-Server des Providers erhalten hat, wissen Sie, dass die Verbindung funktioniert.

Status		
Firmware-Version: <b>1.59</b>		
Showtime-Version: <b>3.30</b>		
Firewall-Version: <b>3.1.2b</b>		
WAN		
IP-Adresse	Subnetz-Maske	MAC-Adresse
217.187.94.207	255.255.255.0	02:0B:3B:03:64:AC
LAN		
IP-Adresse	Subnetz-Maske	MAC-Adresse
10.0.0.1	255.255.255.0	00:0B:3B:03:64:A7

Abbildung 3.31: Erfolgreicher Verbindungsaufbau

Wenn der Verbindungsaufbau nicht funktioniert, stellen Sie sicher, dass Ihre Verbindungsdaten richtig eingetragen wurden, dass die Kabelverbindung zum DSL-Modem und vom Modem zum DSL-Splitter richtig hergestellt ist und dass das Synchronisierungslicht des DSL-Modems leuchtet und zeigt, dass eine DSL-Verbindung hergestellt wurde. Meistens liegt ein fehlerhafter Verbindungsaufbau an falsch eingetragenen Benutzerdaten, Wenn Sie nicht sicher sind, ob die Daten stimmen, probieren Sie einfach verschiedene Anordnungen aus.

Tipp . . . . .

Bei T-Online-Zugängen ist die Syntax zum Beispiel

Anschlusskennung T-Online-Nummer erf/0001@tonline.de

Die Anschlusskennung und die T-Online-Nummer werden direkt hintereinander geschrieben, gefolgt von einer Raute (#), der Mitbenutzernummer (meistens 0001) und dem Kürzel @t-online.de.

### Letzte Konfigurationsmaßnahmen

Bevor Sie im Internet surfen, sollten Sie die Konfiguration des Routers fertig stellen.

**Verschiedenes**

---

HTTP-Server-Zugang

Jeder

Eingeschränkt

LAN

WAN IP-Adresse

Subnetz-Maske

HTTP-Server-Port

---

FTP-Server

FTP-Zugang aus dem WAN sperren

---

DMZ

DMZ-Host-Adresse

---

DHCP

Aus

DHCP-Server

DHCP-Relay

DHCP-Relay-Adresse

Abbildung 3.32: Änderungen in der Konfiguration

Die nächste wichtige Option ist das Ändern des Standardkennworts des Administrators. Schreiben Sie das neue Kennwort am besten in Ihre Bedienungsanleitung.

Weitere Optionen, die Sie ändern sollten, betreffen den Zugriff auf die Konfigurationsoberfläche. Dieser Zugriff sollte nur vom internen Netzwerk gestattet sein, nicht über das Internet. Bei den meisten Routern ist diese Option bereits aktiviert, aber überprüfen Sie diese Einstellung besser noch einmal. Sie finden diese Option wie im Beispiel unter *HTTP-Server* (siehe *Abbildung 3.32*).

Wenn Sie den DHCP-Server nicht benötigen, sollten Sie ihn deaktivieren. Wenn Sie nur wenige PCs im Haushalt haben, ist die statische Vergabe der IP-Adresse sicherer als das Nutzen eines DHCP-Servers. Vor allem wenn Sie ein Wireless-LAN-fähiges Gerät einsetzen, erhält jeder Nutzer, der Verbindung zum Netzwerk aufbauen kann, automatisch eine IP-Adresse zugeteilt. Dieses Sicherheitsloch können Sie durch das Deaktivieren des DHCP-Servers schließen.

Eventuelle FTP-Serverzugänge auf dem Router können Sie deaktivieren. *FTP* steht für *File Transfer Protocol* und dient zur Übermittlung von Dateien ins Internet.

Verbindungsaufbau bei Internet-Zugriff	Ein
Verbindungsaufbau bei ADSL-Link	Ein
<hr/>	
Zeitzone	(+1) Amsterdam, Berlin, Bern, Rome
Sommerzeit	Ja
Benutzerdefinierter Zeit-Server	207.46.130.100

Abbildung 3.33: Weitere Optionen

Auch die in *Abbildung 3.33* gezeigten Optionen zum Verbindungsaufbau sollten Sie setzen und die Uhrzeit des Routers einstellen. Ich habe die IP-Adresse eines Zeitservers im Internet eingetragen, mit dem sich mein Router automatisch synchronisiert, so dass die Uhrzeit immer stimmt. Wenn bei Ihrem Router keine Option zum Hinterlegen eines Zeitserver vorgesehen ist, macht das weiter nichts aus.

**Testen der Internetverbindung**

Wenn Sie alles richtig gemacht haben, können Sie den Internet Explorer öffnen und eine Verbindung zum Internet aufbauen.

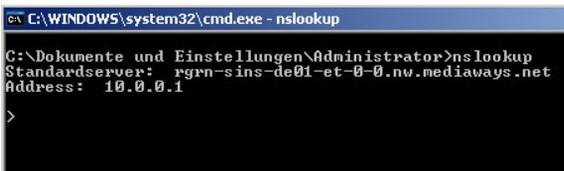
Geben Sie dazu in der Adressleiste die Adresse einer Internetseite ein, zum Beispiel:

`http://www.spiegel.de`

Wenn die Seite aufgebaut wird, sind Sie mit der Konfiguration Ihres Routers fertig und alles funktioniert.

Wird die Seite nicht aufgebaut, sollten Sie nochmals ein paar Dinge überprüfen:

- >> Der wichtigste Punkt ist, dass der Router eine Verbindung ins Internet aufgebaut hat. Testen Sie das zunächst.
- >> Wenn der Router eine Internetverbindung aufgebaut hat, kann es nur an der Verbindung von Ihrem PC zum Router liegen, dass der Aufbau nicht funktioniert.
- >> Wenn der Router keine Verbindung aufbaut, liegt es am Router. Überprüfen Sie über die Weboberfläche, ob dem Router eine IP-Adresse vom Provider für die WAN-Schnittstelle zugeteilt wurde.
- >> Im nächsten Schritt sollten Sie eine Kommandokonsole über *Start/Ausführen* -> *cmd* öffnen.
- >> Überprüfen Sie, ob Ihr PC die Namen aus dem Internet in eine IP-Adresse umwandeln kann. Dazu ist der Eintrag des DNS-Servers vorgegeben. Um das zu überprüfen, geben Sie in der Kommandozeile den Befehl *nslookup* ein.

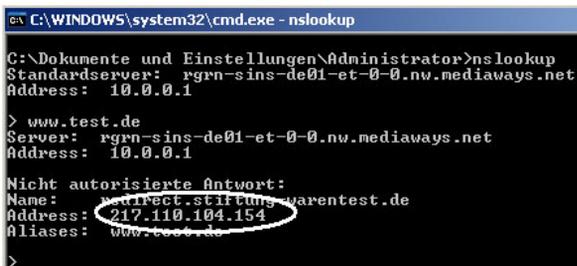


```

C:\WINDOWS\system32\cmd.exe - nslookup
C:\Dokumente und Einstellungen\Administrator>nslookup
Standardserver:  rgrn-sins-de01-et-0-0.nw.mediaways.net
Address:  10.0.0.1
>
  
```

Abbildung 3.34: Starten von nslookup

Dieses Programm dient zur Überprüfung, ob eingegebene Namen im Internet Explorer zu einer IP-Adresse aufgelöst werden können. Wenn Sie *nslookup* starten, kann es durchaus sein, dass eine Fehlermeldung erscheint und der Name des DNS-Servers nicht aufgelöst werden kann. Das ist nicht weiter schlimm und kann von Ihnen ignoriert werden.

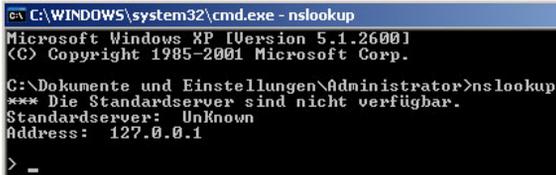


```

C:\WINDOWS\system32\cmd.exe - nslookup
C:\Dokumente und Einstellungen\Administrator>nslookup
Standardserver:  rgrn-sins-de01-et-0-0.nw.mediaways.net
Address:  10.0.0.1
> www.test.de
Server:  rgrn-sins-de01-et-0-0.nw.mediaways.net
Address:  10.0.0.1
Nicht autorisierte Antwort:
Name:    www.test.de
Address: 217.110.104.154
Aliases: www.test.de
>
  
```

Abbildung 3.35: Namensauflösung im Internet

Nur wenn eine Meldung kommt, dass kein DNS-Server für diese Verbindung konfiguriert ist, haben Sie sich wahrscheinlich während der IP-Konfiguration vertippt (siehe *Abbildung 3.36*). Geben Sie den Namen `www.testde` ein. Lassen Sie das `http` vor dem Namen weg. Drücken Sie auf . Das Programm sollte den Namen `www.testde` ohne Fehlermeldung in eine IP-Adresse auflösen (siehe *Abbildung 3.35*).



```

C:\WINDOWS\system32\cmd.exe - nslookup
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Dokumente und Einstellungen\Administrator>nslookup
*** Die Standardserver sind nicht verfügbar.
Standardserver: Unknown
Address: 127.0.0.1

>

```

Abbildung 3.36: DNS-Server kann nicht gefunden werden

- >> Wie Sie sehen, hat der PC mit dem Namen `www.testde` im Internet die IP-Adresse `217.110.104.154`. Notieren Sie sich die IP-Adresse (es kann durchaus sein, dass die IP-Adresse, die Sie erhalten, von der Adresse im Screenshot abweicht).
- >> Wenn kein DNS-Server konfiguriert ist (siehe *Abbildung 3.36*), müssen Sie sich in den IP-Einstellungen vertippt haben. Korrigieren Sie diesen Fehler und versuchen Sie es noch einmal.
- >> Geben Sie in Ihrem Internet Explorer in die Adressleiste `http://` gefolgt von der IP-Adresse Ihrer `nslookup`-Ausgabe ein, im Beispiel `http://217.110.104.154`. Es sollte sich die Startseite der Stiftung Warentest öffnen. In diesem Fall ist alles in Ordnung.
- >> Überprüfen Sie als Nächstes, ob in den IP-Einstellungen Ihres Rechners die IP-Adresse des DSL-Routers bei der DNS-Konfiguration eingetragen ist, wie ich es beschrieben habe. Wenn Sie alle Daten richtig eingetragen haben, sollten Sie ohne Probleme ins Internet kommen.

Wenn Sie den Internet Explorer öffnen und eine Adresse eingeben, sollte der Verbindungsaufbau funktionieren.

### 3.3.5 Anbindung weiterer PCs an das Internet

Im Anschluss können Sie weitere PCs an das Internet anbinden. Sie können entweder die LAN-Schnittstellen am DSL-Router mit dem jeweiligen PC verbinden oder die Wireless-LAN-Schnittstelle des Routers konfigurieren.

Wenn Sie weitere PCs anbinden, müssen Sie lediglich ein Netzkabel vom DSL-Router zu diesem PC legen und die IP-Konfiguration, wie bereits beschrieben, anpassen. Alle Einstellungen des neuen PCs sind dabei identisch mit den Einstellungen des ersten PCs.

Der einzige Unterschied ist, dass Sie eine andere IP-Adresse verwenden müssen. Nehmen Sie dazu eine im gleichen Bereich, die sich vom ersten PC und vom Router unterscheidet. Sobald Sie die Einstellungen vorgenommen haben, sollten Sie mit dem PC ins Internet kommen. Wenn Sie am ersten PC problemlos ins Internet kommen, am zweiten jedoch nicht, führen Sie die Fehlersuche durch, die ich weiter vorn erläutert habe.

### 3.3.6 WLAN – Wireless LAN – Funknetzwerke

Die eleganteste und modernste Art, Computer miteinander zu vernetzen, ist das *Wireless LAN* (WLAN).

#### Allgemeine Informationen zu WLAN

Es werden keinerlei Kabel zwischen den Geräten benötigt, da sämtliche Daten über Funk übertragen werden. Bidirektionale Funkübertragungen ermöglichen die drahtlose Kommunikation mit anderen Geräten in einem begrenzten Radius. Somit ermöglicht ein WLAN einem PC die Kommunikation mit einem Netzwerk mit Funk als Transportmedium. Das Herzstück eines drahtlosen Netzwerks ist der *Access Point*, über den der Datenaustausch stattfindet. Viele DSL-Router sind mit einem Access Point ausgestattet.

WLAN ist das Kürzel für *Wireless Local Area Network*, was übersetzt nichts anderes als *kabelloses lokales Netzwerk* bedeutet.

Der Aufbau eines kabellosen Netzwerks wird mit Windows XP und Windows Vista besonders einfach. Das aktuelle Microsoft-Betriebssystem unterstützt bereits drahtlose Netzwerke.

#### Hardware für WLAN

Wenn Sie ein neues drahtloses Netzwerk aufbauen wollen, benötigen Sie zunächst die passende Hardware.

#### *Einsatz einer WLAN-Netzwerkkarte*

Um mit einem PC oder Notebook eine Verbindung mit einem drahtlosen Netzwerk herzustellen, brauchen Sie zunächst eine WLAN-Netzwerkkarte. Die gängigen Modelle sind derzeit WLAN-Karten für den Standard-PCI-Bus, PCMCIA-Karten für Notebooks und WLAN-Karten, die direkt über USB mit dem PC verbunden werden können.

Für den Einsatz im Standard-PC werden in der Regel *PCI(Peripheral Component Interconnect)*-WLAN-Einsteckkarten verwendet. Diese Karten lassen sich ohne größeren Aufwand in den PC einbauen und abhängig vom verwendeten Betriebssystem in Betrieb nehmen. Natürlich sollten Sie vor dem Kauf prüfen, ob Ihr PC noch einen freien PCI-Steckplatz besitzt.

Gegenüber USB-Adaptern muss beim Einbau einer PCI-Netzwerkkarte der PC geöffnet werden.

Um WLAN-Netzwerkkarten mit einem Notebook zu verwenden, wird der *PCMCIA* (*Personal Computer Memory Card*)-Slot verwendet. Die meisten Notebooks verfügen über zwei PCMCIA-Steckplätze. PCMCIA-Karten haben die Form und Größe einer Kreditkarte und können ohne Probleme in das Notebook eingebaut werden.

Abhängig vom Betriebssystem sollten diese Karten automatisch erkannt werden und nach der Installation des entsprechenden Treibers betriebsbereit sein. Die einfachste Methode, Ihren PC oder Ihr Notebook WLAN-tauglich zu machen, ist mit einem USB-WLAN-Adapter.

Die Besonderheit von *USB* (*Universal Serial Bus*) ist, dass der Anschluss nicht nur die Daten übertragen kann, sondern auch bis zu gewissen Grenzen die Stromversorgung für das angeschlossene Gerät übernehmen kann. Zusätzlich zeichnet sich der USB-Anschluss durch seine guten Plug&Play-Eigenschaften aus. In der Regel stecken Sie das USB-Gerät bei laufendem Betrieb ein. Der PC oder das Notebook erkennt das Gerät und nach der Installation des entsprechenden Treibers können Sie Ihre WLAN-Karte bereits benutzen.

Sie sollten beim Kauf eines USB-WLAN-Adapters unbedingt darauf achten, dass Ihr USB-Anschluss die Geschwindigkeit Ihres Adapters verarbeiten kann. Es gibt zwei verschiedene Spezifikationen von USB.

In der Version 1.1 werden Geschwindigkeiten von bis zu 12 Mbps unterstützt. Version 2.0 unterstützt bereits Geschwindigkeiten von bis zu 480 Mbps. Eine USB-Schnittstelle mit 12 Mbps hat mit einem Adapter, der bis zu 54 Mbps unterstützt, nicht die volle Leistung des WLAN.

**Tipp** . . . . .

*Notebooks, die mit der Intel Centrino-Technologie ausgestattet sind, haben bereits eine Wireless-LAN-Netzwerkkarte fest eingebaut. Solche Notebooks können sofort in einem Funknetzwerk verwendet werden.*

*Wireless LAN Access Point einsetzen*

Ein Access Point ist ein eigenständiges Wireless-LAN-Gerät, das nicht mit einem PC verbunden werden muss. Vergleichbar mit einem Netzwerk-Switch, fungiert der Access Point als Vermittlungsstelle des Netzwerks. Viele DSL-Router sind mit einem Access Point kombiniert. Mitglieder eines drahtlosen Netzwerks unterhalten sich nicht direkt miteinander, sondern senden alle Daten zum Access Point. Der Access Point nimmt diese Daten entgegen und leitet sie an den entsprechenden Empfänger im Netzwerk weiter.

Ein Access Point kann mit einem kabelgebundenen Netzwerk kombiniert werden. Sie können PCs an den DSL-Router anschließen und zusätzlich PCs oder Notebooks mit Funknetzwerkkarten.

Jeder WLAN-Adapter unterstützt zwei verschiedene Betriebsmodi. Ähnlich wie beim kabelgebundenen Netzwerk müssen Computer nicht unbedingt über einen Switch miteinander verbunden sein, sondern können sich direkt miteinander unterhalten. Diese Betriebsart wird *Ad-hoc-Modus* genannt. Wird das WLAN mit einem oder mehreren Access Points betrieben, spricht man vom *Infrastruktur-Modus*.

Nähern sich zwei Computer mit WLAN-Adaptoren im *Ad-hoc-Modus*, können diese ohne weitere Maßnahmen miteinander kommunizieren. Der Datenverkehr wird nicht wie beim *Infrastruktur-Modus* durch einen Access Point geregelt, sondern erfolgt von Computer zu Computer. Dementsprechend verhält es sich mit der Performance von WLANs im *Ad-hoc-Modus*. Werden mehr als drei WLAN-Geräte miteinander verbunden, kann es aufgrund von WLAN-spezifischen Funkkanalzugriffsmethoden zu Verbindungsabbrüchen im WLAN kommen. Die Reichweite von *Ad-hoc-Netzwerken* ist im Regelfall (abhängig von Hindernissen und Witterungsverhältnissen) auf ca. 30 m begrenzt.

Anders als bei Ad-hoc-Netzen besteht bei WLANs im Infrastruktur-Modus keine direkte Verbindung zwischen zwei oder mehreren Computern. Ein Access Point regelt den Datenverkehr zwischen den verschiedenen Clientcomputern. Ein solcher Access Point kann beliebig viele Computer bedienen.

Jeder Access Point besitzt einen *SSID (Service Set Identifier)*. Diese Stationskennung können Sie im Access Point eingeben und frei wählen. Access Points können miteinander gekoppelt werden, um die Reichweite zu erhöhen.

### **WLAN in Betrieb nehmen**

Auf den nachfolgenden Seiten wird die Einrichtung eines Funknetzwerks erläutert.

#### *Aktivierung WLAN im DSL-Router*

Um den Access Point zu konfigurieren, müssen Sie sich mit der Weboberfläche des DSL-Routers verbinden. Wenn Sie den Benutzernamen und das Kennwort richtig eingegeben haben, gelangen Sie auf die Verwaltungsseite des Routers. Gehen Sie als Nächstes in das Menü, in dem Sie die WLAN-Eigenschaften einstellen können. Meistens sind diese Menüs mit *Wireless* oder *WLAN* beschriftet.

An dieser Stelle können Sie alle Einstellungen von Verschlüsselung über SSID und Broadcast bis zur Konfiguration einer manuellen IP-Adresse vornehmen. Bevor Sie mit der Absicherung des Systems beginnen, sollten Sie zuerst überprüfen, ob die Access-Point-Funktion am Gerät aktiviert ist. Diese Einstellung ist unter dem Punkt *Wireless* zu finden. Sie sehen die Möglichkeiten *Enable* (Wireless LAN aktiv) und *Disable* (Wireless LAN nicht aktiv). Setzen Sie gegebenenfalls diesen Punkt auf *Enable*, um den Access Point für WLAN

zu aktivieren. Nachdem die Einstellung mit *Apply* bestätigt wurde, führt der Access Point automatisch einen Neustart durch und ist danach mit aktivem WLAN betriebsbereit.

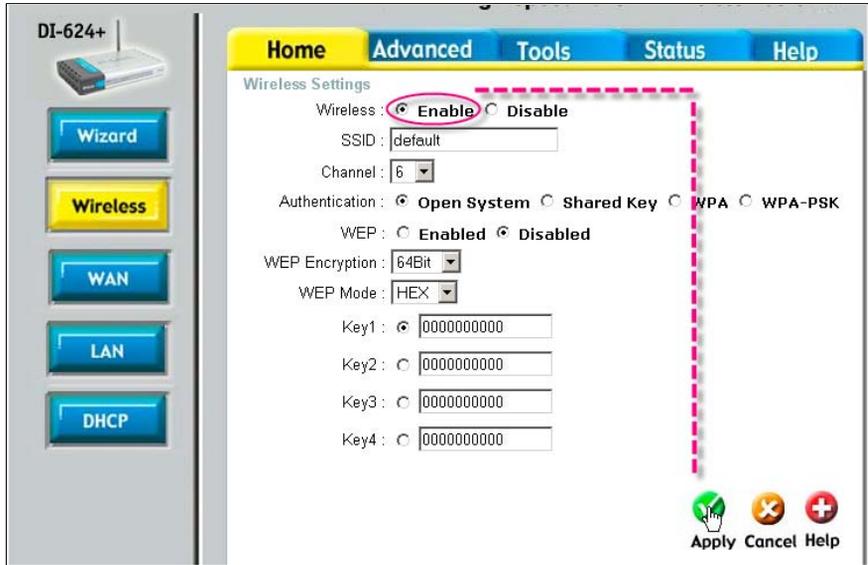


Abbildung 3.37: Aktivierung der Wireless-Funktion eines Routers

*Vorbereiten des PCs für WLAN*

Nachdem die Vorkonfiguration des Access Points abgeschlossen ist, können Sie sich dem Computer zuwenden. Sie sind inzwischen so weit, dass der Computer über eine kabelgebundene Verbindung Kontakt mit dem Access Point aufnehmen kann. Jetzt geht es darum, den Computer für die Verbindung mit Wireless LAN vorzubereiten. Abhängig von der WLAN-Netzwerkarte, die Sie verwenden, weicht die Konfiguration geringfügig von diesem Beispiel ab.

In diesem Beispiel wird ein PCMCIA-Adapter des Herstellers Netgear verwendet. Die Hersteller der Hardware liefern zu den Produkten im Regelfall eine CD aus, die einen Treiber und eine Verbindungssoftware enthält. Allerdings werden diese Treiber und Verbindungswerkzeuge von den Herstellern ständig verbessert und um wichtige Funktionen erweitert. So erhöht sich beim Einsatz eines neueren Treibers oft die Stabilität und Performance eines Produkts. Aus diesem Grund empfiehlt es sich grundsätzlich, vor der ersten Installation im Internet nach dem aktuellen Treiber und dem aktuellen Verbindungstool zu schauen.

Eine Übersicht der Support-Homepages von fast allen Hardwareherstellern finden Sie unter:

[www.treber.de](http://www.treber.de)

oder:

[www.heise.de/ct/treiber](http://www.heise.de/ct/treiber)

Wenn Sie den aktuellsten Treiber heruntergeladen haben, können Sie mit der Installation des Adapters beginnen. Wenn Sie sich für einen USB-Adapter entschieden haben, stecken Sie diesen in laufendem Betrieb einfach in den Rechner ein.

Sollten Sie sich für einen PCI-Adapter entschieden haben, schalten Sie den Computer aus, entfernen den Netzstecker und bauen die Karte ein. In diesem Beispiel wird ein PCMCIA-Adapter verwendet, der ebenfalls in laufendem Betrieb eingesteckt werden kann.

### Installation des WLAN-Adapters

Der WLAN-Adapter ist eingebaut und Windows hat den Adapter erkannt. In diesem Beispiel wird der WLAN-Adapter von Windows zwar erkannt, aber Windows verfügt über keinen Treiber, um die Karte zu starten. Der Adapter wird vom Windows-Gerätemanager als unbekanntes Gerät angezeigt.

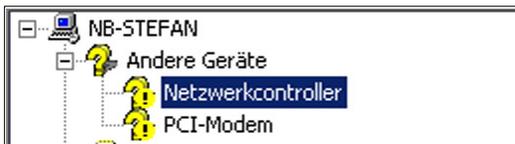


Abbildung 3.38: Nicht erkanntes Netzwerkgerät

Wenn der Treiber über eine Setup-Routine verfügt, wird die Installation besonders einfach. Starten Sie im Verzeichnis des Treibers die Datei *Setup.exe*. Es meldet sich der Installationsassistent des Adapters und bietet die Möglichkeiten *Abbrechen* und *Weiter*. Nach einem Klick auf *Weiter* fragt der Assistent nach dem Pfad, in dem er die Software installieren soll. Ein weiterer Klick auf *Weiter* und die Installation kann mit einem letzten Klick auf den *Fertigstellen*-Button abgeschlossen werden.

Ab sofort steht Windows der passende Treiber zur Verfügung und der Adapter wird aktiviert. Werfen Sie einen Blick in den Gerätemanager und überprüfen Sie, ob das gelbe Ausrufezeichen verschwunden ist. Der WLAN-Adapter wird mit seinem richtigen Namen im Unterpunkt *Netzwerkadapter* zu sehen sein.



Abbildung 3.39: Installierte Funknetzwerkarte

*Konfiguration des WLAN-Adapters*

Der WLAN-Adapter ist installiert und bereit, eine Verbindung zu einem drahtlosen Netzwerk herzustellen. Allerdings sollten Sie vorher noch eine wichtige Entscheidung treffen: Wollen Sie das Konfigurationsprogramm des Herstellers verwenden oder das Windows-eigene Konfigurationsprogramm? Windows XP mit installiertem Service Pack 2 oder Windows Vista bietet derzeit die beste Wireless-LAN-Unterstützung. Durch diverse Assistenten macht es Windows dem Benutzer besonders leicht, die Konfiguration eines drahtlosen Netzwerks durchzuführen.

Die Konfigurationsprogramme der Hersteller sind in der Regel einfach und problemlos zu bedienen. Wenn Sie das Konfigurationsprogramm des Herstellers verwenden wollen, sollten Sie das Windows XP mitteilen. In diesem Fall klicken Sie auf *Start* und anschließend auf *Einstellungen* und wählen *Systemsteuerung* aus. Klicken Sie doppelt auf das Symbol *Netzwerkverbindungen*. Es öffnet sich ein Fenster mit einer Liste aller verfügbaren Netzwerkadapter. In dieser Liste sollten Sie einen Adapter mit dem Namen *Drahtlose Netzwerkverbindung* vorfinden. Klicken Sie mit der rechten Maustaste auf diesen Adapter und wählen Sie im Kontextmenü *Eigenschaften* aus. Wechseln Sie auf die Registerkarte *Drahtlosnetzwerke* und entfernen Sie den Haken bei der Option *Windows zum Konfigurieren der Einstellungen verwenden*. Bestätigen Sie Ihre Angaben mit *OK*.

Leider kommt es vor allem bei der Verwendung verschiedener Hardware immer wieder zu Kompatibilitätsproblemen zwischen der Konfigurationssoftware auf den Computern und verschiedenen Access Points. Vor allem bei der Konfiguration der WEP-Schlüssel kommt es immer wieder zu Schwierigkeiten. In diesem Beispiel wird die mitgelieferte Software deaktiviert und die automatische Konfiguration von Windows genutzt.

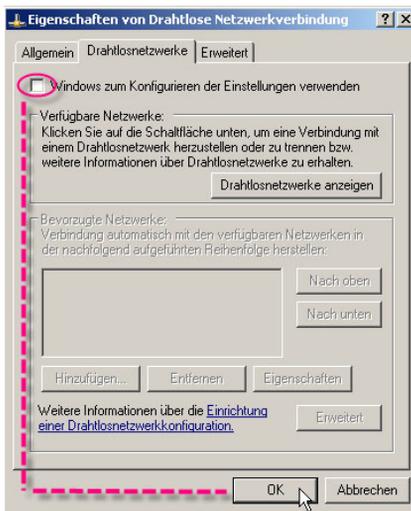


Abbildung 3.40: Deaktivierung der Windows-Steuerung für das Funknetzwerk

### Verbindungsaufbau zwischen PC und WLAN

Nach dem Abschluss der Adapterkonfiguration können Sie die erste Verbindung mit dem drahtlosen Netzwerk herstellen. In der Zwischenzeit ist Ihnen eventuell aufgefallen, dass Windows festgestellt hat, dass sich ein drahtloses Netzwerk in Reichweite befindet. Ist die vorherige Konfiguration des WLAN-Adapters fehlerfrei durchgelaufen, sollte diese Meldung unten rechts in Ihrer Taskleiste erscheinen.

Nach einem Klick auf diese gelbe Box sollte sich das Windows XP-Wireless-LAN-Verbindungsfenster öffnen. In diesem Fenster meldet Windows XP den Fund eines unsicheren drahtlosen Netzwerks. Windows XP deklariert dieses Netzwerk deshalb als unsicher, weil es keine aktive Verschlüsselung feststellen kann. Dessen sind Sie sich natürlich vollkommen bewusst und stellen über einen Klick auf den Button *Verbinden* eine Verbindung mit dem WLAN her. Windows meldet noch einmal, dass dieses Netzwerk nicht sicher ist. Diese Meldung kann vorerst ignoriert werden und Sie können den Button *Trotzdem verbinden* anklicken. Als Name des Netzwerks zeigt Windows XP *default* an.

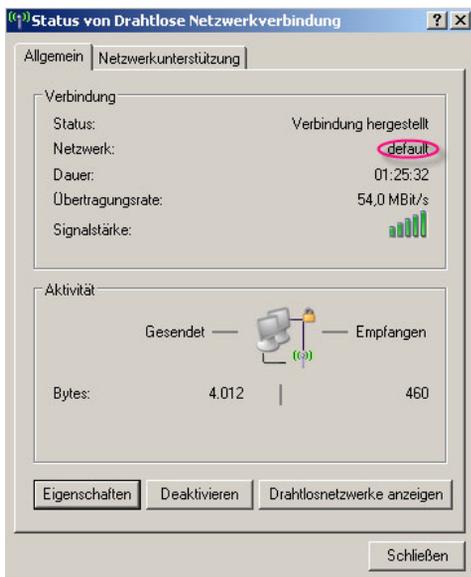


Abbildung 3.41: Verbindung zum Funknetzwerk

Dieser Name ist der *SSID* (*Service Set Identifier*), der standardmäßig vom Hersteller hinterlegt wurde. Mit dieser Konfiguration kann jedes WLAN-Gerät in der näheren Umgebung eine Verbindung mit diesem drahtlosen Netzwerk herstellen.

Wenn Windows eine erfolgreiche Verbindung mit dem WLAN herstellt, sollte das rote Kreuz unten rechts in der Taskleiste verschwunden sein.

Stattdessen sollten Sie einen kleinen Monitor mit Funkwellen sehen. Nach einem Doppelklick auf dieses Symbol sollte sich ein Fenster mit dem Titel *Status von Drahtlose Netzwerkverbindung* öffnen.

In diesem Fenster wird die Stärke des WLAN-Signals in grünen Balken angezeigt. Mit Hilfe dieser Anzeige können Sie später den Access Point besser positionieren. Im Feld *Netzwerke* steht der vordefinierte Name Ihres drahtlosen Netzwerks, in diesem Fall *default*. Wie beim Anschluss der kabelgebundenen Netzwerkkarte sollten Sie testen, ob der Computer über die drahtlose Verbindung eine IP-Adresse beziehen kann.

Gehen Sie dazu auf *Start* und wählen Sie *Ausführen*. Löschen Sie alles aus der Zeile, tippen Sie *cmd* ein und klicken Sie anschließend auf *OK*. Es sollte sich eine DOS-Box öffnen und Sie befinden sich in der Kommandozeile von Windows XP.

Tippen Sie den Befehl *ipconfig* ein. Im Ausgabefenster sollte zusätzlich zum ersten Adapter der WLAN-Adapter angezeigt werden.

### Sicherheit in Funknetzwerken – Theorie

Aufgrund der Problematik, dass bei einem drahtlosen Netz die Daten durch sich frei ausbreitende Funkwellen übertragen werden, sollten Sie der Absicherung Ihres WLAN besondere Aufmerksamkeit schenken.

Durch den Einsatz von Funkwellen muss ein Angreifer nicht bis in Ihre Wohnung vordringen. In der Regel reicht die Sendeleistung eines WLAN über den gewünschten Abdeckungsbereich hinaus. Die Art eines Netzwerkangriffs, bei der nicht in das entsprechende Gebäude eingedrungen werden muss, wird als *Parking Lot Attack* bezeichnet.

Durch das Plug&Play-Networking bei WLANs entstehen weitere Probleme. Die Anbindung, Authentifizierung und Identifizierung der WLAN-Teilnehmer sollen möglichst automatisiert erfolgen. Derzeit sind fast alle gängigen WLAN-Geräte mit Sicherheitsmechanismen ausgestattet, doch haben diese erhebliche Sicherheitslücken oder sind in der Grundeinstellung der Geräte deaktiviert.

Untersuchungen zeigen immer wieder, dass noch ein sehr großer Teil von WLANs durch keine der derzeit bekannten Sicherheitsmechanismen geschützt ist.

#### *Folgen eines Angriffs auf ein Wireless LAN*

Zunächst sollten Sie sich darüber Gedanken machen, welche Möglichkeiten ein unerwünschter Teilnehmer an Ihrem WLAN hat.

Hat es ein Angreifer geschafft, sich mit Ihrem Wireless LAN zu verbinden, wird dieser grundsätzlich als normales Netzwerkmitglied Ihres WLAN behandelt. Dies hat zur Folge, dass Informationen, die Sie anderen Benut-

zern im Netzwerk bereitstellen, eingesehen, manipuliert oder im schlimmsten Fall vernichtet werden können.

Auch ohne eine direkte Teilnahme an Ihrem bestehenden Windows-Netzwerk wird es dem Angreifer aufgrund niedriger Sicherheitsstandards relativ einfach gemacht, auf nicht freigegebene Dateien zuzugreifen. Ein Angreifer könnte zum Beispiel mit einem Protokollierungstool den gesamten Datenverkehr aufzeichnen und die gesammelten Daten zu einem späteren Zeitpunkt auslesen.

Es wird relativ schnell deutlich, dass die Absicherung und richtige Konfiguration in Bezug auf Sicherheit extrem wichtig sind. Funktionen wie *SSID Broadcast* der Wireless Access Points machen es unerwünschten Teilnehmern besonders einfach, drahtlose Netzwerke aufzuspüren und sich mit diesen zu verbinden.

### *Wardriving – WLANs aufspüren*

Die gezielte Suche nach drahtlosen Netzwerken, um diese abzuhören oder in sie einzubrechen, wird als *Wardriving* bezeichnet.

Der Begriff Wardriving ist namentlich angelehnt an den Begriff *Wardialing*, eine beliebte Hackermethode der 80er Jahre, bei der über Zufallsprinzip verschiedene Telefonnummern angerufen wurden, um zu überprüfen, ob auf der Gegenseite ein Computer die Verbindung entgegennimmt.

Inzwischen haben sich in Hackerkreisen Gruppen gebildet, die sich auf das Aufspüren unverschlüsselter Funknetze spezialisiert haben.

Beim Wardriving versucht der Angreifer zunächst, ein WLAN ausfindig zu machen. Dazu fährt er mit dem Auto oder einem Fahrrad durch Wohn- oder Industriegebiete. Ausgestattet mit Notebook und speziellen Programmen zum Aufspüren von WLANs, versucht er Funknetzwerke in seiner Umgebung zu orten. Bei einer Fahrt durch ein Industrie- oder Wohngebiet dauert es in der Regel nicht besonders lange, bis die ersten Netzwerke auf dem Bildschirm erscheinen.

Oft wird für das Aufspüren von WLANs das kostenlose Programm *NetStumbler* (<http://www.netstumbler.com>) benutzt, das bei einem WLAN in Reichweite sofort ein akustisches Signal und detaillierte Informationen zum gefundenen Netzwerk ausgibt.

Ist es dem Wardriver gelungen, ein Netzwerk aufzuspüren, beginnt er in der Regel damit, den Datenstrom abzuhören. Im Anschluss daran wird er sich eine Schwachstelle suchen, um eine Verbindung mit dem Netzwerk herzustellen.

Bei vollkommen unverschlüsselten Netzwerken braucht der Angreifer nicht nach einer Lücke im System zu suchen, sondern kann sofort und ohne Umwege am Netzwerk teilnehmen.

*Welche Ausrüstung wird für WLAN-Hacking benötigt?*

Um drahtlose Netzwerke aufzuspüren oder in diese einzudringen, bedarf es keiner besonderen Ausrüstung.

Ein Notebook mit funktionierender Wireless-LAN-Karte und eines der vielen Tools zum Aufspüren von Netzwerken reichen bereits aus.

Sniffer erledigen die eigentliche Arbeit des Aufstöberns und Hackens. Dem Angreifer steht eine Reihe von unterschiedlichen Sniffern zur Auswahl.

*NetStumbler*

Diese Freeware ist das am meisten verbreitete Tool zum Aufspüren von WLANs. Zusätzlich liefert NetStumbler Informationen über die eingesetzten Clientadapter und Access Points. Zusätzlich unterstützt NetStumbler mit entsprechender Hardware GPS (Global Positioning System).

Die Informationen von Herstellerdaten der Access Points können für weitere Attacken genutzt werden.

*Airopeek*

Dieses kommerzielle Tool vom Anbieter WildPackets ([www.wildpackets.com](http://www.wildpackets.com)) stellt einen professionellen Protokoll-Analyzer für drahtlose Netze zur Verfügung. Airopeek ist in erster Linie kein WLAN-Sniffer, sondern soll WLAN-Administratoren bei der Suche nach Sicherheitslücken unterstützen. Die Hauptaufgabe der Software ist die detaillierte Information des Anwenders über das Geschehen in seinem Funknetzwerk. Die meisten gängigen WLAN-Karten werden unterstützt.

*Rechtliche Folgen bei einem Einbruch in ein WLAN*

Durch die rasante Verbreitung von WLANs nimmt die Anzahl schlecht oder ungeschützter Netzwerke enorm zu. Aufgrund der leicht zu bedienenden Aufspürungstools sowie der weit verbreiteten Anleitungen im Internet nimmt die Zahl der Angriffe auf solche Netzwerke stark zu. Eine genaue Zahl steht zwar nicht fest, sie wird aber enorm hoch eingeschätzt.

In der Öffentlichkeit wird schon das Suchen nach drahtlosen Netzwerken als Straftat verurteilt. Diese weit verbreitete Meinung ist allerdings nicht richtig. Die Suche nach drahtlosen Netzwerken ist völlig legal.

Allerdings ist das unerlaubte Eindringen in und Abhören von Funknetzwerken laut dem Telekommunikationsgesetz strafbar. Dabei ist es irrelevant, ob das betroffene Netzwerk geschützt oder ungeschützt ist. Verstöße gegen dieses Gesetz werden hauptsächlich mit hohen Geldstrafen und teilweise mit Freiheitsstrafen geahndet.

Handelt es sich bei einem Angriff um ein gesichertes Funknetzwerk, so macht sich der Angreifer nicht nur des Abhörens von Daten strafbar, sondern des Ausspähens von Daten, was laut Strafgesetzbuch die Strafe um zwei bis drei Jahre erhöhen kann.

Das Verändern oder Beschädigen von Daten im Funknetz zieht ebenfalls rechtliche Konsequenzen mit sich. So kann der Angreifer wegen Datenveränderung mit mindestens zwei Jahren Freiheitsstrafe rechnen. Bei einer Beschädigung von Daten, die zusätzlich zu Störungen des betrieblichen Ablaufs beiträgt, liegt Computersabotage vor, was die Strafe auf bis zu fünf Jahren erhöhen kann.

### *Schutzmaßnahmen vor WLAN-Hackern*

Sie können sich gegen Wardriving und andere unerwünschte Zugriffe auf Ihr Wireless LAN schützen. Es liegt auf der Hand, dass es zwingend erforderlich ist, die verfügbaren Sicherheitsmechanismen richtig zu konfigurieren und zu aktivieren, um sich vor Übergriffen und Missbrauch zu schützen.

In der Realität sieht es leider etwas anders aus. Bei Tests in Wohn- und Industriegebieten werden häufig aktive WLANs ohne jeglichen Schutz gefunden, und wenn sie geschützt sein sollten, dann werden oft veraltete oder schlecht konfigurierte Sicherheitsstandards angewendet.

### *WEP-Protokoll*

Für die Absicherung eines Funknetzwerks wird oft das *WEP-Protokoll* (*Wired Equivalent Privacy*) verwendet. Das Protokoll hat jedoch einige Sicherheitslücken und kann durch Auslesen der Verschlüsselung in wenigen Sekunden geknackt werden.

### *So funktioniert das WEP-Protokoll*

Das WEP-Protokoll ist dennoch eine wichtige Sicherheitskomponente. Geringer Schutz ist besser als gar keiner. Bei der Verschlüsselung mit WEP legt der Anwender auf seinem Access Point einen *WEP-Key* fest. Ein *WEP-Key* ist eine Zeichenkette von Zahlen und Buchstaben. Gültige Zeichen beim *WEP-Key* sind die Zahlen 0 bis 9 und die Buchstaben a bis f sowie A bis F.

Grundlage für die Berechnung der Zufallszahlen ist der vom Anwender festgelegte *WEP-Key*, ein rein statischer Schlüssel, der auf allen Access Points und Clients zum Einsatz kommt. Dieses Verfahren birgt Sicherheitsrisiken, ein Angreifer kann versuchen, den Schlüssel rechnerisch zu rekonstruieren. Nur sehr wenige WLAN-Lösungen sehen für jeden Client einen eigenen Schlüssel vor.



Abbildung 3.42: Einführung eines WEP-Keys

Der WEP-Key wird vom Benutzer definiert und sollte möglichst aus einer komplexen Zahlen- und Buchstabenreihe bestehen. Um die Sicherheit zu erhöhen, sollte der definierte WEP-Key in regelmäßigen Abständen geändert werden. Nachteilig wirkt sich allerdings der sinkende Datendurchsatz aus, der durch den Ver- und Entschlüsselungsvorgang verursacht wird.

**Info** .....

*Der verwendete WEP-Key muss jeder Station im drahtlosen Netzwerk bekannt sein, sonst kann kein Zugriff erfolgen!*

*Authentifizierung im Wireless LAN*

Ein Access Point im drahtlosen Netzwerk ist mit einer eindeutigen Stationskennnummer, SSID (Service Set Identifier) genannt, versehen. Um Stationen im drahtlosen Netz eindeutig zu identifizieren, werden zum einen das Open-System- und zum anderen das Shared-Key-Verfahren angewendet.

*Open-System-Verfahren*

Wie der Name schon sagt, handelt es sich bei der *Open-System-Authentifizierung* um eine »offene Methode«. Hierbei werden verschiedene Access Points an ihrem SSID erkannt. Jede Station mit gleichem SSID kann diesem WLAN beitreten. Auf den Clientstationen sind die WLAN-Karten in der Regel so konfiguriert, dass jede Station jedem Wireless LAN beitreten kann.

Open System ist die denkbar einfachste Form der Authentifizierung. Versucht eine Station sich mit Open System bei einer anderen Station zu authentifizieren, die ebenfalls Open System als Authentifizierungsform gewählt hat, wird die Identität ohne Prüfung akzeptiert.

### *Shared-Key-Verfahren*

Shared-Key-Authentifizierung ist optional und erfordert den Einsatz von WEP. Hierbei wird ein gemeinsamer WEP-Schlüssel zur Authentifizierung verwendet. Die Station sendet einen unverschlüsselten Text, der von der Station, die authentifiziert werden möchte, verschlüsselt zurückgesendet werden muss. Alle Stationen sowie der Access Point müssen über den gleichen Schlüssel verfügen.

### *Filtern von MAC-Adressen*

Ein weiterer beliebter Schutzmechanismus, um drahtlose Netzwerke vor unbefugten Zugriffen zu schützen, ist die MAC-Adressenfilterung. Jedes Netzwerkgerät besitzt eine eindeutige Kennnummer, die zur eindeutigen Identifizierung des jeweiligen Geräts dient. Beim Einschalten des Geräts wird die MAC(*Media Access Control*)-Adresse gesetzt und kann in den meisten Fällen nicht verändert werden.

Bei der Filterung mit MAC-Adressen muss die MAC-Adresse von jedem Gerät, dem Zugriff auf den entsprechenden Access Point gewährt werden soll, in die Filterliste eingetragen werden. Im Grund findet dann nichts anderes als ein Namensabgleich statt. Meldet sich eine Station mit dem passenden Namen – egal ob gefälscht oder nicht –, wird dieser Station der Zugriff gewährt.

*Die MAC-Adresse, die Sie am Access Point eintragen müssen, können Sie am lokalen Client erfragen. Starten Sie dazu über Start/Ausführen ->cmd eine Kommandokonsole. Geben Sie in der Kommandokonsole den Befehl ipconfig /all ein. Daraufhin wird die MAC-Adresse unter Pysikalische Adresse ausgegeben (siehe Abbildung 3.44).*

**Tipp** . . . . .

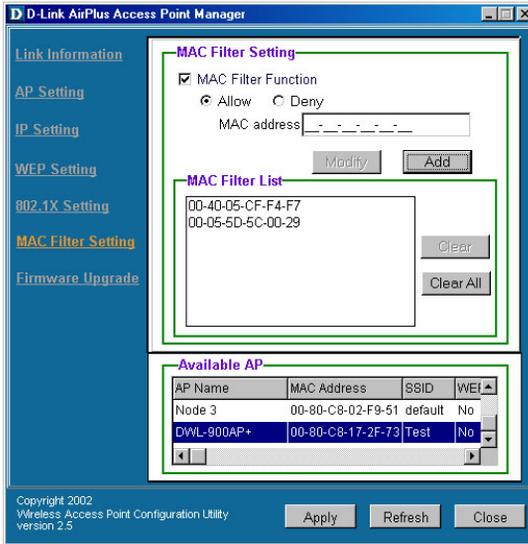


Abbildung 3.43: Filterung nach MAC-Adressen

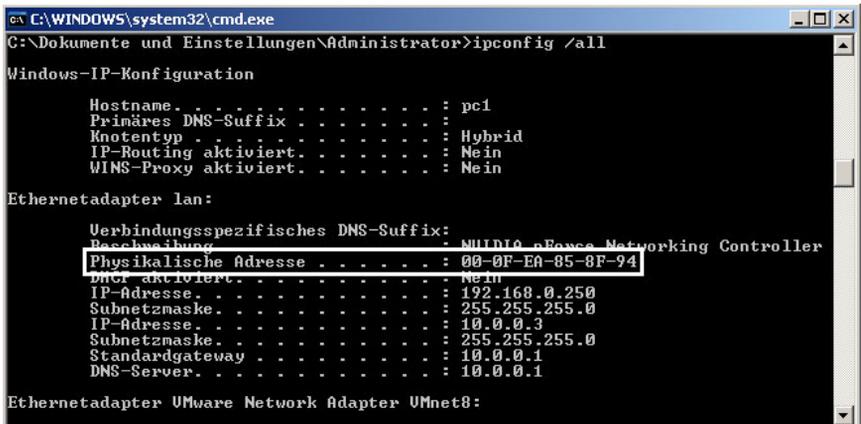


Abbildung 3.44: Ausgabe der MAC-Adresse über ipconfig/all

### SSID und SSID Broadcast

Der selbst definierbare Name eines Access Points wird als SSID (Service Set Identifier) bezeichnet. Die Hardwarehersteller liefern die Access Points standardmäßig mit aktiviertem SSID Broadcast aus.

Der Access Point »ruft« den Namen Ihres WLAN in regelmäßigen Intervallen in das drahtlose Netzwerk. Um eine Verbindung mit einem drahtlosen Netzwerk aufnehmen zu können, muss einem PC dieser Name (SSID) bekannt sein. Bei eingeschaltetem SSID Broadcast kann jeder den Namen Ihres WLAN sehen – erwünschte und unerwünschte Teilnehmer. Um es einem Angreifer nicht zu einfach zu machen, sollten Sie unbedingt den vorgegebenen Netzwerknamen (oft *default* oder *WLAN*) ändern.

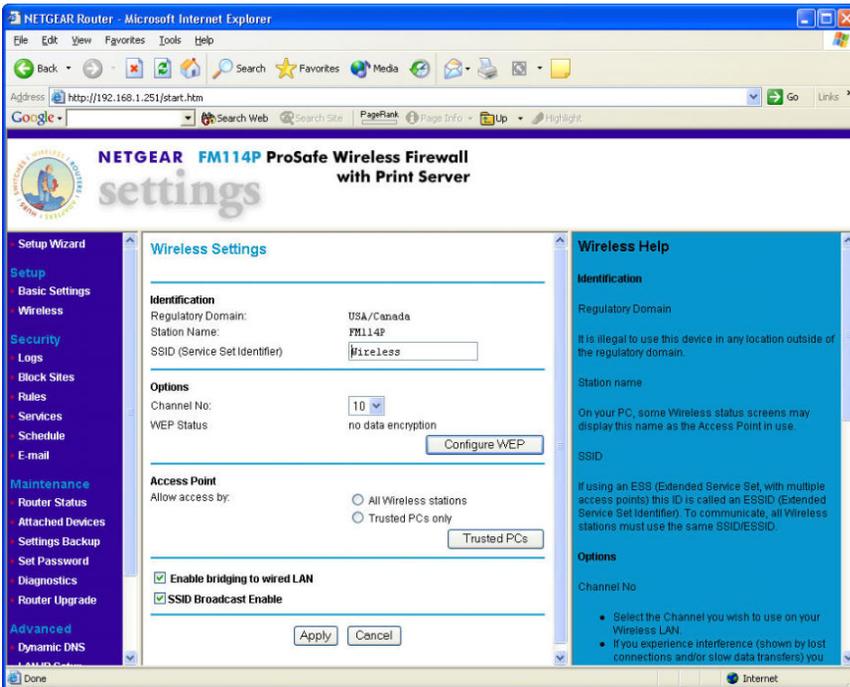


Abbildung 3.45: SSID-Broadcast-Einstellungen

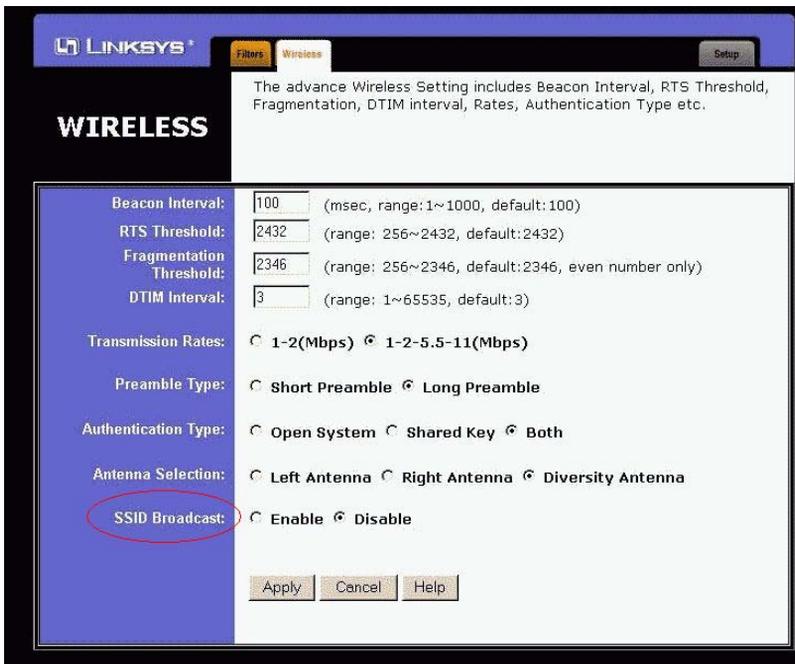


Abbildung 3.46: Deaktivierung von SSID Broadcast

Lassen Sie bei der Vergabe des Netzwerknamens keinerlei Rückschlüsse auf die verwendete Hardware oder sonstige Informationen Ihres Netzwerks zu. Als Nächstes sollten Sie die Funktion *SSID Broadcast* deaktivieren. Drahtlose Netzwerke mit ausgeschaltetem *SSID Broadcast* sind für Angreifer wesentlich unattraktiver als völlig offene Netze.

#### *Absicherung eines WLAN Access Points*

Der Access Point ist das Herzstück des drahtlosen Netzwerks. In dieser Zentrale werden alle relevanten Einstellungen des WLAN vorgenommen. Für die Konfiguration des Access Points wird wie bei der DSL-Router-Funktionalität eine Weboberfläche benutzt.

Diese Verwaltungszentrale wird in der Regel durch die Eingabe von Benutzername und Kennwort geschützt. Gelingt es einem Angreifer, dieses Verwaltungsprogramm zu öffnen, ist er in der Lage, den Access Point zu konfigurieren und sich so einen Zugang zum Netzwerk einzurichten. Aus diesem Grund sollten Sie unbedingt darauf achten, ein komplexes Kennwort aus Buchstaben und Ziffern zu vergeben.

#### *Absicherung der DHCP-Funktion*

In den meisten Access Points oder Kombigeräten aus DSL-Routern und Access Points ist ein DHCP-Server integriert. Das DHCP(Dynamic Host Configuration Protocol)-Protokoll dient zur automatischen IP-Adressenkonfiguration von Netzwerkkomponenten. Sollte es dem Angreifer gelingen, eine dynamische IP-Adresse vom DHCP-Server zu beziehen, sind für ihn sämtliche Türen und Tore offen. Der Hacker ist in Ihrem Netz und kann auf Netzwerkfreigaben zugreifen, Daten verändern oder löschen und Viren im Netz verbreiten. Zudem besteht die Gefahr, dass der Angreifer auf Ihre Kosten im Internet surft.

Aus diesem Grund empfiehlt es sich, die DHCP-Funktion auf Ihrem Access Point zu deaktivieren und die Vergabe von IP-Adressen manuell durchzuführen. Leider ist das keine zuverlässige Methode, ein drahtloses Netzwerk vollständig zu schützen, aber es ist eine weitere Hürde für jeden Angreifer und erfüllt in Kombination mit den anderen Schutzmechanismen durchaus seinen Zweck.

#### *WPA-Protokoll zur Sicherung eines WLAN*

Derzeit gelten mit WPA verschlüsselte Netze als einbruchsicher. Die Einrichtung dieses Protokolls erläutere ich Ihnen im nächsten Abschnitt.



Abbildung 3.47: WPA-Einstellung an einem Access Point

### Sicherheit in Funknetzwerken – Praxis

Nachdem Sie sich in die theoretischen Ansätze der WLAN-Sicherheit eingelesen haben, können Sie diese Sicherheitseinstellungen an Ihrem DSL-Router mit aktiviertem Wireless Access Point aktivieren.

Das Wireless LAN ist voll betriebsbereit. Der Access Point ist konfiguriert und der Client kann sich mit dem drahtlosen Netzwerk verbinden. Leider kann sich nicht nur Ihr Computer zum WLAN verbinden, sondern jeder PC, der in Reichweite ist. Zusätzlich bekommt jeder Computer, der sich an Ihrem WLAN anmeldet, automatisch eine IP-Adresse zugewiesen und kann mit allen Computern in Ihrem Netzwerk kommunizieren. Der Access Point ist derzeit gegen Angreifer völlig ungeschützt. Da das Standardpasswort, über das die Administrationswebseite geöffnet wird, noch nicht geändert wurde, kann jeder beliebige Teilnehmer Ihren Access Point verwalten. Aus diesem Grund sollten Sie Ihr Wireless LAN mit allen zur Verfügung stehenden Mitteln schützen.

#### *Deaktivieren des DHCP-Servers*

Im ersten Schritt sollten Sie den DHCP-Server des Access Points deaktivieren. DHCP ist für die automatische Vergabe von IP-Adressen zuständig. Ein Angreifer wird zunächst versuchen, eine IP-Adresse zu bekommen. Diese Aktion verkleinert die Angriffsfläche und ist ein wichtiger Bestandteil für den Schutz eines WLAN.

Bevor Sie den DHCP-Server auf Ihrem Router deaktivieren, sollten Sie auf allen PCs zunächst eine statische IP-Adresse eintragen.

SSID eines Access Points ändern

Der SSID (Service Set Identifier) steht für den Namen Ihres drahtlosen Netzwerks. Abhängig vom Hersteller werden im Auslieferungszustand Standardnamen vergeben. In diesem Beispiel lautet der vordefinierte SSID des Herstellers *default*. Der SSID kann bei eingeschaltetem SSID Broadcast von jedem eingesehen werden. Der Name des Netzwerks sollte deswegen in keinem Fall Rückschlüsse auf die Herkunft oder sonstige Informationen des Netzwerks zulassen. Am besten vergeben Sie einen kryptischen Namen, der keinerlei Rückschlüsse auf Information zulässt. In diesem Beispiel verwenden Sie den SSID-Namen »H7WQLCC«. Bei dem Access Point, der in diesem Beispiel verwendet wird lässt sich der SSID unter dem Menüpunkt *Wireless* ändern. Nach Eingabe des neuen SSID bestätigen Sie die Änderungen mit *Apply* und starten den Access Point neu. Danach ist die Änderung aktiv.

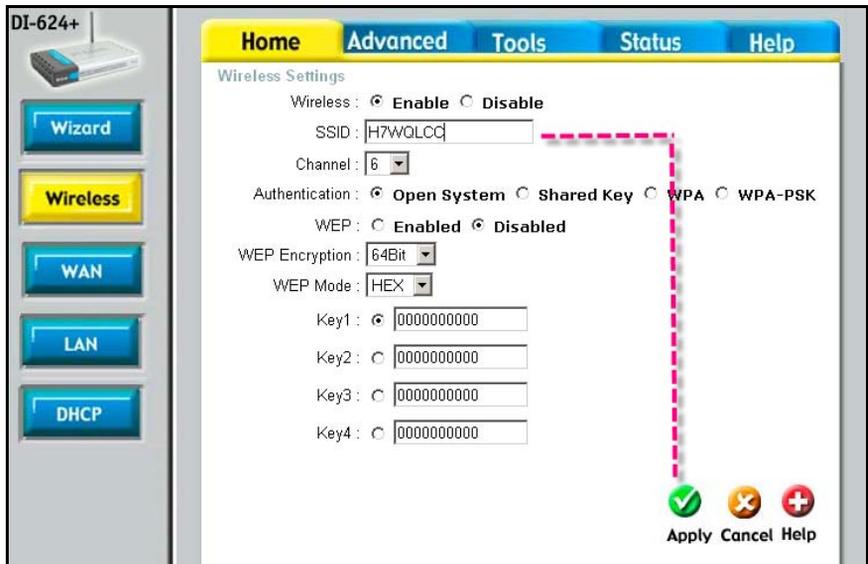


Abbildung 3.48: Definition eines neuen SSID

Windows XP verliert nach dem Ändern des SSID die Verbindung zum Access Point. Klicken Sie doppelt auf das WLAN-Monitorsymbol in der Taskleiste. Es öffnet sich der Verbindungsmanager für drahtlose Netzwerke. Wählen Sie auf der linken Seite die Funktion *Netzwerke aktualisieren* aus. Windows XP beginnt mit der Suche nach neuen drahtlosen Netzwerken. Nach kurzer Zeit erscheint ein neues Netzwerk mit dem Namen »H7WQLCC«. Nach einem Klick auf die Schaltfläche *Verbinden* stellt Windows die Verbindung zum drahtlosen Netz wieder her. Gelingt dieser Vorgang, haben Sie erfolgreich den SSID des Netzwerks geändert.

### SSID Broadcast deaktivieren

Sie haben den SSID Ihres Access Points inzwischen erfolgreich geändert. Durch die Funktion *SSID Broadcast* wird der Name des Netzwerks vom Access Point in regelmäßigen Intervallen im Netzwerk veröffentlicht. Ist ein Angreifer auf der Suche nach offenen Funknetzen, kann er mit der Bezeichnung H7WQLCC keine Rückschlüsse auf die Herkunft des Netzwerks ziehen, aber verbinden kann er sich ohne Probleme.

Im Auslieferungszustand ist die SSID-Broadcast-Funktion auf den Access Points fast immer aktiviert. Aus diesem Grund sollten Sie das Broadcasting auf dem Access-Point nachträglich deaktivieren. Nachdem die Funktion *SSID Broadcast* deaktiviert wurde, können sich nur noch Geräte mit dem drahtlosen Netzwerk verbinden, denen der Netzwerkname bekannt ist.

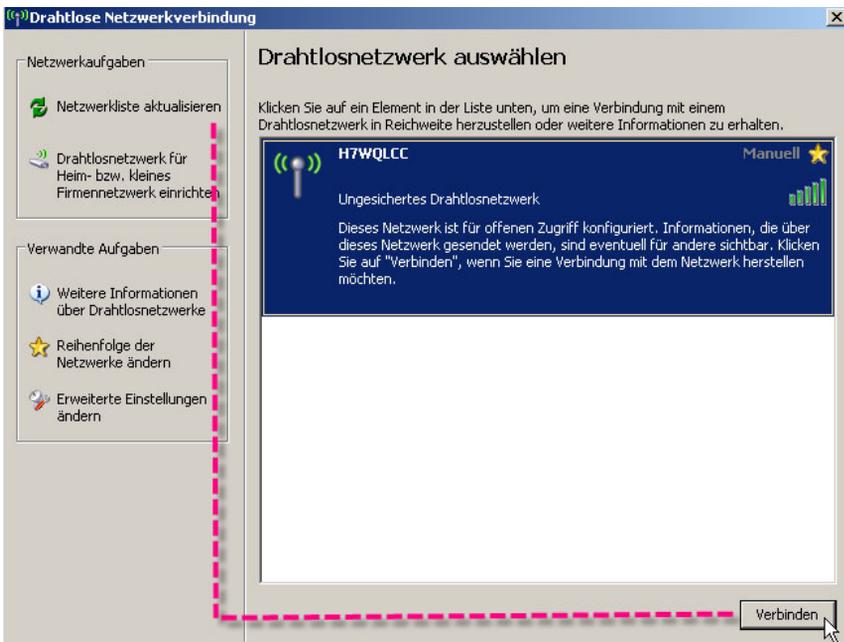


Abbildung 3.49: Neues Netzwerk gefunden

Um SSID Broadcasting zu deaktivieren, stellen Sie eine Verbindung mit der Verwaltungswebseite des Access Points her. Bei dem im Beispiel verwendeten Access Point lässt sich die Funktion über den Menüpunkt *Performance – Advanced* deaktivieren. Aktivieren Sie im Feld *SSID Broadcast* die Option *Disabled* und bestätigen Sie Ihre Auswahl. Der Access Point sollte danach neu gestartet werden.

Nach dem Neustart verliert Windows XP nicht die Verbindung mit dem Wireless LAN. Obwohl der Netzwerkname noch nicht manuell definiert wurde, kann eine Verbindung mit dem WLAN hergestellt werden. Das liegt daran, dass Windows XP alle drahtlosen Netze, mit denen es verbunden war, in einer Liste hinterlegt. In dieser Liste steht der neue Name des WLAN – »H7WQLCC«.

Um zu testen, ob die deaktivierte SSID-Broadcast-Einstellung funktioniert, können Sie das drahtlose Netzwerk aus der Liste der drahtlosen Netze entfernen und Windows zu einer neuen Suche auffordern.

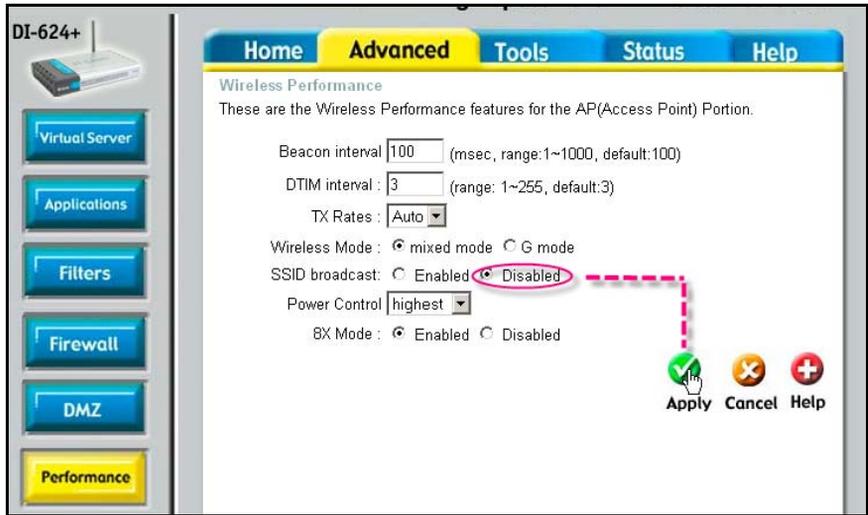


Abbildung 3.50: Deaktivieren des SSID Broadcasts

Um die Liste der drahtlosen Netze zu löschen, führen Sie einen Doppelklick auf das WLAN-Monitorsymbol in der Taskleiste aus. Im Verbindungsmanager für drahtlose Netzwerke klicken Sie auf die Schaltfläche *Trennen*. Dadurch wird die Verbindung mit Ihrem drahtlosen Netzwerk unterbrochen. In der Box *Verwandte Aufgaben* klicken Sie auf den Punkt *Erweiterte Einstellungen ändern*. Es sollte sich das Eigenschaftsfenster der drahtlosen Netzwerkverbindung öffnen. Wechseln Sie auf die Registerkarte *Drahtlosnetzwerke* und entfernen Sie die vorhandenen Netzwerke *default* und *H7WQLCC*.

Starten Sie den Verbindungsmanager für drahtlose Netzwerke. Windows kann keine drahtlosen Netzwerke mehr finden. Dies trifft auch zu, wenn Sie die Schaltfläche zur Aktualisierung der Netzwerkliste anwählen. Durch das Deaktivieren der SSID-Broadcast-Funktion haben Sie die Sicherheit Ihres drahtlosen Netzwerks um ein Vielfaches erhöht.

### Manuelle Verbindung zu einem WLAN

Nachdem Sie die SSID-Broadcast-Funktion deaktiviert haben, veröffentlicht Ihr Access Point seinen Netzwerknamen nicht mehr. Sie können die Verbindung zum Wireless LAN nur noch manuell durchführen. Diese Konstellation ist nicht mehr so bequem wie mit dem Assistenten, aber dafür wesentlich sicherer.

Um Ihr WLAN unter Windows XP manuell der Liste hinzuzufügen, starten Sie den Verbindungsmanager für drahtlose Netzwerke. Wählen Sie in der Box *Verwandte Aufgaben* die Funktion *Erweiterte Einstellungen ändern* aus. Wechseln Sie zur Registerkarte *Drahtlosnetzwerke* und klicken Sie auf den Button *Hinzufügen*. Es öffnet sich ein neues Fenster, in dem Sie an oberster Stelle den SSID selbst definieren können. Geben Sie hier den Namen des drahtlosen Netzwerks ein, in diesem Fall wäre das »H7WQLCC«. Bei *Datenverschlüsselung* wählen Sie die Option *Deaktiviert*. Bestätigen Sie Ihre Angaben mit *OK* und Windows XP wird automatisch wieder Verbindung zu Ihrem drahtlosen Netzwerk aufnehmen.

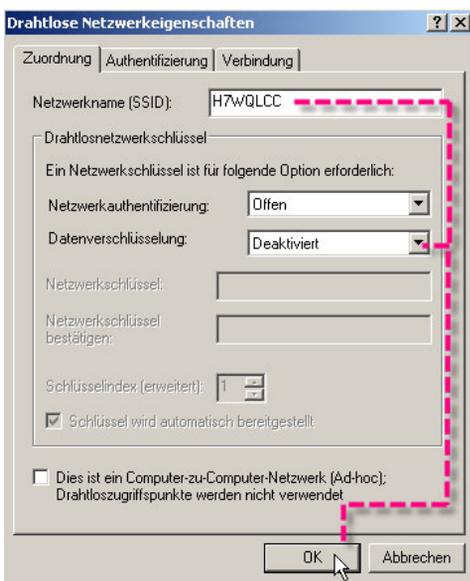


Abbildung 3.51: Manuelle Verbindung zum Funknetzwerk

### Passwort am Access Point ändern

Es ist Ihnen mit Sicherheit aufgefallen, dass Sie bei jeder Anmeldung am Access Point das vordefinierte Kennwort des Herstellers eingegeben haben. Dieser Punkt ist besonders kritisch und wird häufig bei der Absicherung eines drahtlosen Netzwerks vergessen. Stellen Sie sich nur vor, Sie haben Ihr WLAN mit allen nur erdenklichen Sicherheitsmaßnahmen abgesichert und es gelingt jemandem, durch Eingabe des Standard- oder zu einfach gewählten Kennworts die Verwaltungswebseite Ihres Access Points zu öffnen. Diese

Person ist in der Lage, alle von Ihnen getroffenen Einstellungen auszulesen oder zu verändern.

Aus diesem Grund sollten Sie grundsätzlich das Standardkennwort am Access Point durch ein komplexes Kennwort ersetzen. Sie sollten dieses Kennwort möglichst regelmäßig ändern. Bei der Wahl des Kennworts sollten Sie auf Wörter, die in Wörterbüchern stehen, verzichten. Ein Angreifer könnte ein solches Kennwort mit einem so genannten *Brute-Force-Angriff* (Wörterbuchattacke) knacken und sich Zugriff verschaffen.

Bei einem *Brute-Force-Angriff* gibt ein Hackerprogramm alle bekannten Wörter in sehr kurzer Zeit ein und kann sich dadurch recht schnell Zugriff verschaffen. Zusätzlich sollten Sie auf Namen oder Geburtstage verzichten, da diese Kennwörter relativ schnell erraten werden können. Es empfiehlt sich, ein Kennwort aus Buchstaben, Zahlen und Sonderzeichen zu generieren. Diese Kennwörter bieten den größten Schutz. Ein Beispielkennwort wäre zum Beispiel »Kx9!ä++Wysk843\$\$«.

Um das Standardkennwort am Access Point zu ändern, starten Sie erneut die Verwaltungsw Webseite Ihres Access Points. Bei dem Access Point in diesem Beispiel wird das Kennwort über den Menüpunkt *Admin – Tools* geändert. Geben Sie in der Zeile *New Password* Ihr neues Kennwort ein. Wiederholen Sie die Eingabe des Passworts im Feld *Confirm Password*. Bestätigen Sie Ihre Eingabe und starten Sie den Access Point neu. Durch die Änderung des Standardkennworts haben Sie sichergestellt, dass niemand unautorisiert auf Ihren Access Point zugreifen kann, und die Sicherheit Ihres drahtlosen Netzwerks erneut um einen wesentlichen Faktor erhöht.

### *Mac-Adressen filtern*

Eine weitere sehr effektive Methode, ein drahtloses Netzwerk vor unbefugten Zugriffen zu schützen, ist die Filterung von MAC-Adressen. Jedes Netzwerkgerät, jeder PC, jede Netzwerkkarte, jeder Printserver oder Access Point verfügt über eine eindeutige Nummer. Diese Nummer wird *MAC-Adresse* genannt. Diese eindeutige Nummer macht jedes Netzwerkgerät weltweit einmalig. In einem drahtlosen Netzwerk können Sie diese MAC-Adressen für sich nutzen. Durch die Eindeutigkeit von MAC-Adressen können Sie Ihrem Access Point beibringen, nur die Verbindung mit einem vordefinierten Satz von MAC-Adressen zu erlauben. Meldet sich eine MAC-Adresse am Access Point, die nicht auf der Liste erlaubter Adressen steht, wird der Access Point die Verbindung verweigern.

Leider bietet diese Methode keinen vollständigen Schutz, da es diverse Möglichkeiten gibt, MAC-Adressen zu fälschen. Kennt ein potentieller Angreifer nur eine MAC-Adresse auf der Liste der erlaubten Adressen, ist es ein Leichtes für ihn, die entsprechende Adresse zu fälschen und eine Verbindung mit dem WLAN aufzubauen. Doch als zusätzliche Schutzmaßnahme hat sich die Filterung von MAC-Adressen durchaus bewährt und sollte in jedem Fall aktiviert werden.

Bevor Sie die Filterung von MAC-Adressen aktivieren, sollten Sie sich alle MAC-Adressen, die mit dem Access Point Verbindung aufnehmen sollen, notieren. Sie sollten in diesem Punkt sehr sorgfältig vorgehen, da Sie sich schnell selbst vom System aussperren können, wenn Sie nur eine Ziffer der MAC-Adresse falsch eingeben. Zum Ermitteln der MAC-Adressen Ihrer Netzwerkkarten können Sie den bereits beschriebenen Befehl *ipconfig* verwenden. Allerdings reicht in diesem Fall die Eingabe von *ipconfig* nicht aus. Die korrekte Syntax wäre *ipconfig /all*.

Wenn Sie sich alle benötigten MAC-Adressen notiert haben, können Sie mit der Konfiguration des Access Points beginnen und dort die Adressen eintragen. Starten Sie hierzu die Verwaltungswebseite Ihres Access Points. Bei dem im Beispiel verwendeten Access Point sind die benötigten Einstellungen unter *Advanced – Filters* zu finden. Hier angekommen, wählen Sie die Option *Mac-Filters* und anschließend *Only allow computers with MAC adress listed below to access the network* aus. Das Aktivieren dieser Funktion hat zur Folge, dass nur Computer mit einer eingetragenen MAC-Adresse eine Verbindung mit dem Access Point aufbauen können. Im Feld *Name* können Sie für die entsprechende MAC-Adresse einen Computernamen eintragen. Dieses Feld hat allerdings keine Funktion und dient einzig und allein zur besseren Übersicht. Die benötigten MAC-Adressen in diesem Fall wären *00-09-5B-97-F7-D8* für den WLAN-Adapter und *00-0B-DB-15-1F-AF* für den kabelgebundenen Adapter.

Vergessen Sie nicht, die MAC-Adresse des Computers, der mit Kabel verbunden ist, am Access Point als erlaubte Adresse zu hinterlegen. Tragen Sie im ersten Schritt immer die MAC-Adresse ein, von der Sie den Access Point verwalten, sonst könnte es passieren, dass Sie sich selbst vom System aussperren.

Wenn Sie eine falsche Adresse eintragen, sperren Sie sich unter Umständen selbst aus. Wenn Sie alle benötigten MAC-Adressen eingetragen haben, bestätigen Sie Ihre Angaben. Der Access Point führt einen Neustart durch und schaltet den MAC-Adressenfilter aktiv. Wenn Sie die MAC-Adressen richtig ermittelt und eingetragen haben, sollte sich Ihr Computer nach dem Neustart automatisch wieder mit dem WLAN verbinden.

### *Remote Management deaktivieren*

Fast alle Access Points mit integriertem DSL-Router bieten die Funktion *Remote Management* an. Diese Funktion erlaubt es, den Access Point von jedem beliebigen Computer über das Internet zu verwalten. Natürlich wird für diese Verwaltung ein Kennwort benötigt, was aber für einen Angreifer mit genügend Ausdauer kein Riesenproblem darstellt. Um wirklich alle Lücken zu schließen, sollten Sie diese Funktion am Access Point unbedingt deaktivieren. Häufig ist diese Funktion bereits von den Herstellern deaktiviert und kann bei Bedarf aktiviert werden.

WPA-Verschlüsselung aktivieren – das Hochsicherheits-WLAN

Inzwischen haben Sie eine ganze Menge an Sicherheitsvorkehrungen getroffen. Allerdings sind die Daten, die über das Funknetzwerk gesendet werden, noch unverschlüsselt. Aus diesem Grund sollten Sie, sofern Ihr Access Point und die eingesetzten WLAN-Adapter dies unterstützen, die WPA-Funktion aktivieren. Die Abkürzung WPA steht für *Wireless Protected Access*. Mit Hilfe der WPA-Verschlüsselung können Sie Ihr drahtloses Netzwerk relativ unkompliziert und schnell absichern.

In diesem Beispiel aktivieren wir WPA-PSK, wobei die Abkürzung PSK für *Pre-Shared Key* steht. Der Pre-Shared Key ist ein Schlüssel, der dem Access Point und allen WLAN-Teilnehmern zur Verfügung stehen muss. Mit Hilfe dieses Master-Schlüssels ändert der Access Point in regelmäßigen Intervallen die Verschlüsselung. Dieser Vorgang wird dynamischer Schlüsselwechsel genannt. Wie beim Verwaltungskennwort für den Access Point empfiehlt es sich, für den PSK eine komplexe Reihe aus Buchstaben, Zahlen und Sonderzeichen zu wählen. Der PSK sollte zudem mindestens aus 20 Zeichen bestehen. In diesem Beispiel lautet der PSK *bgtr%k,#\*smz!<c(jist*.

Zum Aktivieren von WPA mit PSK am Access Point öffnen Sie die Verwaltungswebseite. Bei diesem Access Point ist die WPA-Verschlüsselung unter *Home – Wireless* zu finden.

Aktivieren Sie hier die Funktion WPA-PSK und geben Sie in das Feld *Passphrase* den gewünschten Pre-Shared Key ein. Im Feld *Confirmed Passphrase* wiederholen Sie die Eingabe.

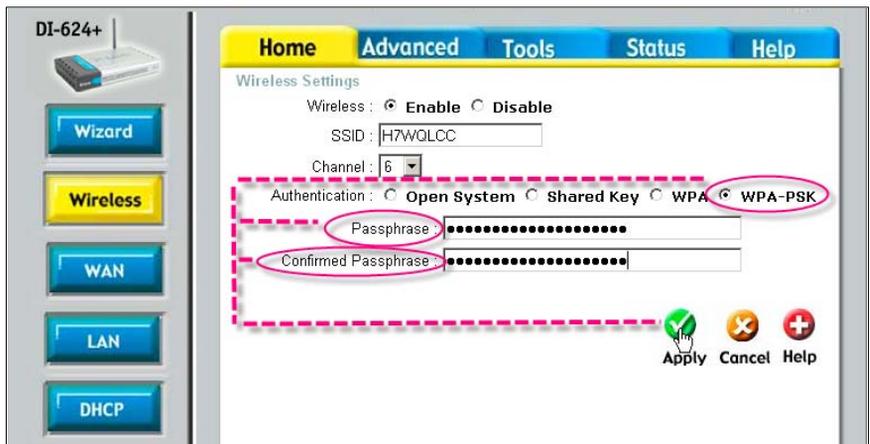


Abbildung 3.52: WPA auf dem Router aktivieren

Nach dem Neustart des Access Points werden Sie feststellen, dass Sie keine Verbindung mehr mit Ihrem WLAN aufbauen können. Klicken Sie auf das kleine WLAN-Monitorsymbol in der Taskleiste. Es sollte sich der Verbindungsmanager für drahtlose Netzwerke öffnen. Wählen Sie den Punkt *Netzwerkliste aktualisieren*. Windows findet das drahtlose Netzwerk als *Sicherheitsaktiviertes Drahtlosnetz (WPA)* wieder.

Klicken Sie auf die Schaltfläche *Verbinden*. Im Anschluss daran werden Sie von Windows aufgefordert, den *Pre-Shared Key* einzugeben. Geben Sie in das Feld *Netzwerkschlüssel* den Pre-Shared Key ein, den Sie auf dem Access Point definiert haben. Im Feld *Netzwerkschlüssel bestätigen* wiederholen Sie die Eingabe des PSK und bestätigen Ihre Angaben mit dem *Verbinden*-Button.

Wenn Sie den Pre-Shared Key korrekt eingegeben haben, beginnt Windows mit dem Verbindungsaufbau zum drahtlosen Netzwerk. Ab diesem Moment können Sie das WLAN wieder wie gewohnt benutzen.

Wenn Sie die WPA-Verschlüsselung erfolgreich aktiviert haben, erhöht sich die Sicherheit Ihres drahtlosen Netzwerks um ein Vielfaches. Zusammen mit den anderen Methoden haben Sie Ihr WLAN bestmöglich abgesichert.

#### *Verschlüsselung aktivieren (WEP)*

Für den Fall, dass Ihr Access Point oder einer Ihrer PCs keine Verschlüsselung mit WPA unterstützt, können Sie die ältere *WEP (Wireless Equivalent Privacy)*-Verschlüsselung nutzen. Sie können Ihr Netzwerk mit WEP weitgehend vor Attacken schützen, allerdings erreichen Sie nie denselben Schutz wie mit WPA. Aus diesem Grund ist es empfehlenswert, schon vor der Anschaffung zu überprüfen, ob die gewünschte Hardware WPA-tauglich ist.

Bei der Eingabe des WEP-Schlüssels gilt es zu beachten, dass Sie nur die Zeichen a bis f und 0 bis 9 verwenden dürfen. Bei einer 128-Bit-Verschlüsselung muss der Schlüssel zudem exakt 26 Zeichen lang sein. Bei der Vergabe des WEP-Schlüssels sollten Sie auf sich wiederholende Zeichen verzichten und den Key so komplex wie möglich gestalten.

Ein WEP-Key für eine 128-Bit-Verschlüsselung wäre zum Beispiel *F384baCe13D61bfA95deE38c7c*.

Um die WEP-Verschlüsselung zu aktivieren, starten Sie die Verwaltungswebseite Ihres Access Points. Bei diesem Access Point ist die WEP-Funktion unter *Wireless – Home* zu finden. Wählen Sie im Feld *Authentication* die Funktion *Shared Key*. Anschließend setzen Sie im Feld *WEP* die *Enabled*-Funktion. Im Dropdown-Menü *WEP Encryption* wählen Sie *128 Bit* aus. Im Feld *Key1* geben Sie den aus 26 Zeichen bestehenden WEP-Schlüssel ein. Bestätigen Sie Ihre Angaben.

Wie bei WPA ist Windows XP nach der Umstellung auf WEP nicht in der Lage, eine Verbindung mit dem Access Point aufzubauen. Wenn Sie sich zum WLAN verbinden wollen, fordert Windows Sie auf, den WEP-Schlüssel einzugeben.

Wenn Sie den Schlüssel richtig eingegeben haben und Windows trotzdem keine Verbindung aufbauen kann, müssen Sie noch eine Änderung in Windows vornehmen. Windows geht nach der Eingabe des WEP-Schlüssels davon aus, dass es sich um ein Open System WLAN handelt. Ihr WLAN arbeitet allerdings im Shared-Key-Modus. Sie müssen Windows so konfigurieren, dass Shared Key (Gemeinsamer Schlüssel) unterstützt wird.

Gehen Sie dafür über die *Systemsteuerung* zu den *Netzwerkverbindungen*. Klicken Sie dort mit der rechten Maustaste auf den WLAN-Adapter und wählen Sie im Kontextmenü *Eigenschaften* aus. Wechseln Sie anschließend auf die Registerkarte *Drahtlosnetzwerke* und markieren Sie im Feld *Bevorzugte Netzwerke* Ihr WLAN. In diesem Fall ist der Name des WLAN *H7WQLCC*. Klicken Sie auf den *Eigenschaften*-Button, es öffnet sich das Eigenschaftsfenster dieser WLAN-Verbindung.

In diesem Fenster wählen Sie unter *Netzwerkauthentifizierung* im Dropdown-Menü die Funktion *Gemeinsam verwendet (Shared Key)* aus und geben in den Feldern *Netzwerkschlüssel* und *Netzwerkschlüssel bestätigen* erneut den definierten WEP-Key ein. Bestätigen Sie Ihre Angaben mit *OK*. Anschließend baut Windows XP eine Verbindung zu Ihrem WLAN auf.

#### *Windows-Firewall aktivieren*

Um die Sicherheit noch ein wenig zu erhöhen, können Sie die in Windows XP integrierte Firewall für die WLAN-Verbindung aktivieren. Da in diesem Beispiel ein Access Point mit integriertem DSL-Router verwendet wird, ist die Aktivierung der Firewall besonders sinnvoll. Um die Windows-interne Firewall zu aktivieren, öffnen Sie über die *Systemsteuerung* erneut die *Netzwerkverbindungen*. Klicken Sie mit der rechten Maustaste auf den WLAN-Adapter und wählen Sie im Kontextmenü *Eigenschaften* aus. Wechseln Sie zur Registerkarte *Erweitert*. Klicken Sie unter dem Punkt *Windows-Firewall* auf den *Einstellungen*-Button.

Es erscheint das Eigenschaftsfenster der Windows-Firewall. Klicken Sie nun auf den Punkt *Aktiv* neben dem grünen Schild. Bestätigen Sie Ihre Angaben mit *OK*. Die Firewall steht ab Windows XP SP2 zur Verfügung. Die detaillierte Konfiguration dieser Sicherheitsmaßnahme finden Sie in *Kapitel 5 »Workshop: Sicherheit im Internet«*.

## 3.4 Hotspots – öffentliche WLANs

Eine weitere Möglichkeit, ins Internet zu gelangen, sind so genannte *Hotspots*. Hotspots sind öffentlich zugängliche Funknetzwerke zum Beispiel an Flughäfen, in Bahnhöfen oder Innenstädten. Wenn Sie ein Notebook mit Funknetzwerkkarte besitzen und sich im Bereich eines Hotspots befinden, können Sie im Internet surfen. Im Grunde genommen sind die Funknetzwerke, die ich in diesem Kapitel beschrieben habe, genau die Technologie, mit denen Hotspots funktionieren.

### 3.4.1 Allgemeine Informationen zu Hotspots

Sie können in der Innenstadt während eines Espresso oder Cappuccino bequem im Internet surfen oder Ihre E-Mails abrufen.

Da Sie sich über Wireless LAN (WLAN) mit dem Internet verbinden, fallen nicht so hohe Kosten an wie bei der Verbindung über Mobilfunkkarte per UMTS oder GPRS. Die Geschwindigkeit und die Stabilität der Verbindung sind deutlich höher. Hotspots sind meistens gekennzeichnet und fallen recht schnell auf. Schließlich würde ein Hotspot nicht viel bringen, wenn Sie nicht wüssten, dass er da ist (*Abbildung 3.53*).

Hotspots sind meistens über Breitbandanschlüsse an das Internet angebunden und aus diesem Grund sehr schnell. Meistens verkaufen die Provider den Zugang auf Zeitbasis. Viele Hotspots an Bahnhöfen, Flughäfen oder sonstigen öffentlichen Orten sind kostenlos. Informieren Sie sich beim lokalen Betreiber, was der Zugang kostet und ob es einen kostenlosen Zugang gibt.

### 3.4.2 Anmeldung an einem Hotspot

Viele Provider oder Mobilfunkbetreiber bieten ihren Kunden an, ihre Hotspots überall nutzen zu können. Die Abrechnung der Nutzung erfolgt über die Abrechnung des Internetzugangs oder die Telefonrechnung.

Um sich an einem Hotspot anzumelden, gehen Sie genauso vor, wie Sie sich an Ihrem Heimfunknetz verbinden. Zunächst müssen Sie Windows das Netzwerk suchen lassen und sich verbinden. Da die öffentlichen Hotspots von Natur aus offen sein sollen, gibt es selten WEP oder die beschriebene WPA-Verschlüsselung. Der Verbindungsaufbau zu einem Hotspot ist daher ähnlich einfach wie zu einem ungesicherten Access Point eines DSL-Routers. Sie müssen keine besonderen Einstellungen am Internet Explorer vornehmen.

## Tipp . . . . .

Wenn Sie Ihr Notebook oder Ihren PC auf statische IP-Adressen umgestellt haben, müssen Sie für das Nutzen eines Hotspots normalerweise auf DHCP zurückstellen. Schauen Sie sich die Anleitung in diesem Kapitel an und machen Sie sich mit der Bedienung vertraut. Nach der Umstellung sollten Sie ihren PC neu booten, damit Sie von dem Hotspot eine Adresse zugeteilt bekommen.



Abbildung 3.53: Hotspot in Köln

Meistens öffnet sich eine spezielle Internetseite, die Sie über den weiteren Umgang mit dem Hotspot informiert und die Abrechnungsmodalitäten erläutert.

**Berliner Flughäfen** Flughafeninformation und Flugauskunft  
0180 5000 186 (0,12 Euro/Min.)

Hotspot - Das Wireless Lan Berliner Flughäfen English Impressum Kontakt  
BBI - Berlin Brandenburg International

Start  
Sendebereich  
Kontakt  
Impressum

Willkommen beim **WLAN** der Berliner Flughäfen

Surfen Sie von hieraus kostenlos auf unseren Seiten oder verbinden Sie sich ins Internet über folgende Provider:

O<sub>2</sub> Vodafone T-Mobile HotSpot  
swisscom euromobil

**Haftungsausschluss**  
Die Berliner Flughäfen haften nicht für die Geschäftsbeziehungen zwischen Kunde und Provider. Die Berliner Flughäfen sind nicht Vertragspartei oder Vermittler von Leistungen. Es gelten ausschließlich die Bedingungen der jeweiligen Provider. Bei Reklamationen wenden Sie sich bitte an den Provider, über den Sie Ihre Verbindung ins Internet getätigt haben.

Powered by **PSInet**

Abbildung 3.54: Hotspot am Berliner Flughafen

Der Provider 1&1 bietet zum Beispiel Hotspots für seine Kunden kostenlos an. AOL ist in diesem Bereich sehr unbequem und lässt die Nutzung der Hotspots nur mit der eigenen Software zu. Aus diesem Grund erscheint mir AOL nicht der richtige Provider für einen Internetzugang.

*Im Internet finden Sie unter folgenden Adressen eine Auflistung von Hotspots:*

[www.mobilaccess.de](http://www.mobilaccess.de)

[www.portald.de/hotspot\\_portald](http://www.portald.de/hotspot_portald)

[www.hotspot-bcatbns.de](http://www.hotspot-bcatbns.de) (*weltweites Angebot*)

**Tipp . . . . .**

mobileaccess.de  
- public spots in deiner nähe -  
03.01.2006  
+++ Pilotprojekt: Bahn und T-Mobile bringen

**Wireless LAN HotSpots**

name	plz	ort	adresse	info
OpEN sNET	65929	Frankfurt	Melchior Strasse 32	details
Haus Zum Damenpfad	26486	Wangerooge	Peterstr. 27	details
Journal	79761	Waldshut	Kaiserstrasse	details
Dresden-Hotspot	01159	Dresden	Kesselsdorferstraße 16	details
Dresden-Hotspot	01169	Dresden	Kesselsdorferstraße 208	details
openlan 2	85570	Markt Schwaben	Poinger Str. 37	details
hotspotlietzensee	14057	Berlin	Riehlstrasse 16c	details
Amy's Malaysia Restaurant	10629	Berlin	Wilmersdorfer Str. 79	details
naaak2	10405	Berlin	Knaackstr. 28 - 34	details
Internetzugang per WLAN	63069	Offenbach	Marienstr.	details
Cafe Luftsprung	90402	Nürnberg	Unterer Bergauer Platz 10	details
Internetzugang per WLAN	65719	Hofheim	Martin-Wohmann-Str.	details
umts hotspot	38226	Salzgitter	Alter Mühlenweg 6	details
Pension Siegel	97070	Würzburg	Reisgrubengasse 7	details
United-Skynet	38442	Wolfsburg	Rosenwinkel.5	details
Thunder	68789	St. Leon Rot	Opelstr. 22	details
Cafe M	52066	Aachen	Dammstr.	details
THE DOUBLE M	21255	Tostedt	Am Sande 4	details
Gropius Hotspot	12351	Berlin	Johannisthaler Chaussee 317	details
Walfino im Phönixbad	85521	Ottobrunn	Haidgraben 21	details
Großes Haus Schmidten	70736	Fellbach	Butterstraße 1	details
Stadtmuseum und Stadtarchiv	70734	Fellbach	Hintere Straße 26	details
Schwabenlandhalle	70734	Fellbach	Tainer Straße 7	details
Verwaltungsstelle Oeffingen	70736	Fellbach	Hauptstraße 1	details
Verwaltungsstelle Schmidten	70736	Fellbach	Brunnenstraße 1	details
Rathaus	70734	Fellbach	Marktplatz 1	details
Haltestelle Lutherkirche	70734	Fellbach	Tainer Straße	details
Haltestelle Schwabenlandhalle	70734	Fellbach	Tainer Straße	details
Haltestelle Rathaus	70173	Stuttgart	Rathaus	details
Haltestelle Schlossplatz	70173	Stuttgart	Schlossplatz	details

Navigation: << 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 >>

Abbildung 3.55: Hotspotliste von www.mobileaccess.de

### 3.5 DSL-Tuning

Oft lesen Sie in Zeitungen oder im Internet von ganz speziellen Tricks, mit denen Sie die DSL-Geschwindigkeit im Internet steigern können. Dazu bleibt nur eines zu sagen: Humbug.

Sie werden durch das Setzen von irgendwelchen Registrykeys keine zusätzliche Geschwindigkeit erreichen. Die eine oder andere Tuningmaßnahme mag vielleicht 1 bis 2 % mehr Geschwindigkeit bringen, aber es muss schon viel getuned werden, bis Sie diese Geschwindigkeitssteigerung erreichen.

Wenn Sie per DSL-Router an das Internet angebunden sind, was aus meiner Sicht absolute Notwendigkeit ist, bringen irgendwelche DSL-Tuning-Tipps am PC überhaupt nichts, da die DSL-Geschwindigkeit durch den Router bestimmt wird, nicht durch den PC.

### 3.5.1 Fastpath

Die einzige Methode, um die Geschwindigkeit von DSL-Anschlüssen zu steigern, ist die Umstellung des DSL-Anschlusses auf den *Fastpath-Modus*. Mit diesem Modus werden die Antwortzeiten gesenkt und die Internetverbindung wird für Online-Spiele schneller. Die Internetverbindung zum normalen Surfen profitiert weniger von der Umstellung.

Sie sollten auf Fastpath umstellen (sofern Ihr Provider das unterstützt), wenn Sie Geschwindigkeitsprobleme bei Online-Spielen haben. Bei Fastpath werden die *DSL-Interleaving-Fehlerkorrekturen* abgeschaltet, so dass die Ping-Antwortzeiten deutlich verkürzt werden. Provider berechnen für die Umstellung auf Fastpath meistens eine Einmalgebühr und monatliche Gebühren für den Betrieb. Die Interleaving-Fehlerkorrekturen sollen *Burstfehler* bei der Datenübertragung verhindern. Bei so genannten Burstfehlern kann es passieren, dass durch eine Störung des DSL-Signals Daten zerstört werden. Diese Fehler treten relativ selten auf, zerstören aber viele Bits hintereinander.

Bei der Umstellung auf Fastpath wird diese Interleaving-Fehlerkorrektur abgeschaltet. Endbenutzer erhalten durch das Abschalten keine Nachteile und keine großen Vorteile, abgesehen davon, dass die Antwortzeiten schneller werden, Online-Spiele flüssiger funktionieren.