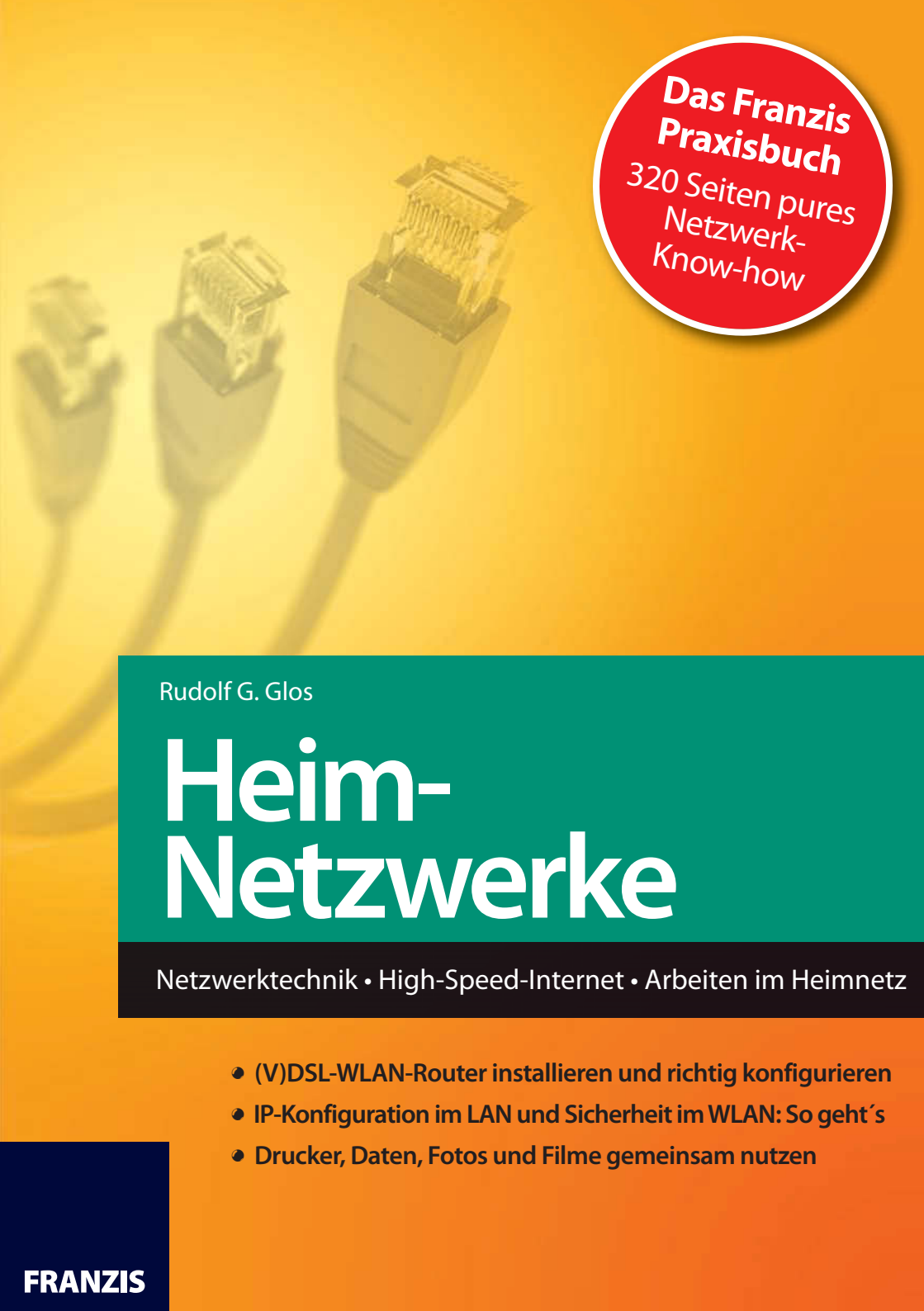

Das Franzis Praxisbuch
320 Seiten pures Netzwerk-Know-how

Rudolf G. Glos

Heim-Netzwerke

Netzwerktechnik • High-Speed-Internet • Arbeiten im Heimnetz

- (V)DSL-WLAN-Router installieren und richtig konfigurieren
- IP-Konfiguration im LAN und Sicherheit im WLAN: So geht´s
- Drucker, Daten, Fotos und Filme gemeinsam nutzen

FRANZIS

Rudolf G. Glos

Heim-Netzwerke

Rudolf G. Glos

Heim-Netzwerke

Netzwerktechnik • High-Speed-Internet • Arbeiten im Heimnetz

FRANZIS

Bibliografische Information der Deutschen Bibliothek

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

Satz: DTP-Satz A. Kugge, München
art & design: www.ideehoch2.de
Druck: CPI-Books
Printed in Germany

ISBN 978-3-645-60193-1

Inhaltsverzeichnis

1 Grundlegende Netzwerktechnik

Wer heutzutage mehr als einen PC besitzt – sei es, weil ein neuer angeschafft wurde, sei es, weil zu Hause ein zweiter zum Spielen oder für die Kinder eingesetzt wird –, kommt um das Thema Netzwerk nicht herum. Wurden früher Daten über Disketten ausgetauscht oder war die Verbindung zweier PCs mittels Parallelkabel das Höchste der Gefühle, sind heute die ausgetauschten Datenmengen so groß und die Technik so simpel, dass sich unterhalb eines Kabelnetzwerks eigentlich nichts mehr anbietet. Moderne PCs tragen dem Rechnung, indem sie schon ab Werk mit den notwendigen Schnittstellen ausgerüstet sind, diese also bereits auf dem Mainboard integriert sind.

Heute ist das Thema Netzwerkeinrichtung ohne dedizierten Server samt Software unter Windows keine große Sache mehr. Es klappt reibungslos, solange nur Rechner mit Windows Daten austauschen, Drucker gemeinsam nutzen oder Internetzugriff haben sollen. Etwas kritischer wird es, wenn unterschiedliche Windows-Versionen vernetzt werden sollen, dann muss man ein wenig Hand anlegen, damit es klappt.

1.1 Ein Netzwerk an einem DSL-Anschluss

Einen zusätzlichen Schub hat das Thema Netzwerk durch die nahezu flächendeckende Verfügbarkeit von DSL-Zugängen bekommen. Früher war ein ISDN-Zugang zwar dank *Internet Connection Sharing* (ICS) ab Windows 98 problemlos möglich, zum gleichzeitigen Surfen genügte die Bandbreite von 64 KBit/s aber nicht. DSL stellte bereits zum Start genug Bandbreite bereit, um einen Zugang aufzuteilen und dennoch schnell genug surfen oder Mails abrufen zu können. Da für den DSL-Zugang auch Netzwerkkarten oder -anschlüsse am PC gebraucht werden, ist aus Herstellersicht die Ab-Werk-Ausstattung moderner PCs mit Netzwerkkarten bzw. -schnittstellen nur folgerichtig.

Über ein Netzwerk kann die Internetverbindung mit allen vernetzten PCs geteilt werden. Also: Einer zahlt … und alle Rechner im Heimnetzwerk surfen! Mit DSL reicht die Bandbreite für alle, denn die eine Leitung kann benutzt werden, um

beliebig viele Rechner dranzuhängen. Zum Surfen genügt die Grundausstattung mit 1 MBit/s, wenn Daten hochgeladen werden sollen, sind allerdings schon 2 MBit/s nicht mehr ausreichend. Bei neuen Anschlüssen liegt der Standard inzwischen bei 6 MBit/s, damit steht genügend Bandbreite zur Verfügung.

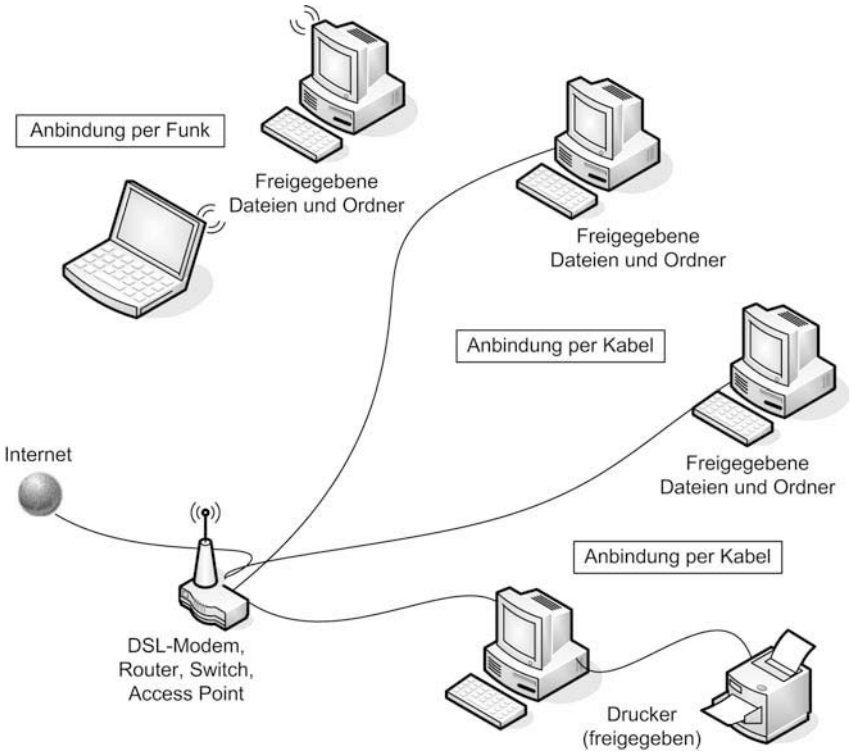

Bild 1.1: Beispiel eines Netzwerks, bestehend aus Kabel- und WLAN-Verbindungen mit Datei- und Druckerfreigaben.

Da beim Abschluss eines neuen DSL-Vertrags in den meisten Fällen ein WLAN-Router im Lieferumfang enthalten ist, sind Funknetze heute nahezu flächendeckend vorhanden. Allerdings steigt mit zunehmender Funknetzdichte auch das notwendige Wissen, um das Netz clever abzusichern. Aber auch das ist bei einem Computer neuerer Bauart kein Problem mehr, denn diese beherrschen die derzeit aktuelle WPA2-Verschlüsselungstechnologie.

Kritischer wird es, wenn Sie z. B. ein älteres Notebook integrieren möchten – hier kann oftmals lediglich eine WEP-Verschlüsselung mit geringer Sicherheit eingestellt werden. Ist das der Fall, hilft nur die Anschaffung einer separaten WLAN-Lösung via USB, die das Sicherheitsniveau nicht senkt.

1.2 Betriebssysteme und Protokolle

Schon lange vor Windows 8 stellten Windows 3.11 für Workgroups und Linux die Basistechnologie für Heimnetzwerke zur Verfügung. Allerdings verwendete Windows seinerzeit statt TCP/IP das Netzwerkübertragungsprotokoll NetBEUI, das eindeutig auf den Datenaustausch verkabelter PCs zugeschnitten war. Linux beherrschte aufgrund seiner UNIX-Wurzeln dagegen standardmäßig TCP/IP.

TCP/IP wurde als Internetprotokoll bekannt und leitete einen wesentlichen Umschwung in der Netzwerkwelt ein: Es wurde zum Standardprotokoll, weil es hersteller- und plattformübergreifend zur Übertragung von Daten eingesetzt werden konnte. Während Windows nach und nach TCP/IP als Standard übernahm, blieben die alten Protokolle aus Kompatibilitätsgründen erhalten. Das hat bis heute bestimmte Sicherheitslücken im Bereich der Datei- und Druckerfreigabe zur Folge.

Der wesentliche Unterschied zwischen Windows und Linux besteht allerdings darin, dass die Betriebssystemversionen von Microsoft keine klassische Serversoftware enthalten. Boten frühere Windows-Versionen wenigstens noch den Personal Internet Server zur Bereitstellung von HTML-Seiten im Internet an, stehen heute zwar für alle wesentlichen Netzwerkaufgaben Spezialprogramme von Microsoft bereit, allerdings sind sie für Privatleute unerschwinglich bzw. für den Hausgebrauch mit unnötigen Funktionen überladen.

Linux als Open-Source-System bietet hingegen auch die nötige Serversoftware kostenlos an, um aus einem PC einen Datei-, Druck-, Internet- oder Mailserver zu machen. Das funktioniert aufgrund der geringeren Systemanforderungen sogar mit vergleichsweise schwachbrüstigen PCs, denen unter Windows XP oder gar Windows Vista längst die Luft ausginge.

Wenn Sie nun aber einen ordentlichen Windows-PC zum Server umfunktionieren wollen, ist das mit den Windows-Versionen von Apache (Internetserversoftware) und Samba (Dateiserversoftware) kein Problem. Mit Apache realisieren Sie einen eigenen Webserver, der per DynDNS über Ihre DSL-Leitung angebunden werden kann, mit Samba steht ein Fileserver für zu Hause bereit.

1.3 Aufbau eines Client-Server-Systems

Grundsätzlich steht jeder, der Daten über ein Netzwerk schicken möchte, vor der Frage, wie das Netzwerk aufgebaut sein soll. Im Industriebereich gibt es da keine Diskussion, hier wird grundsätzlich eine Serverlösung vorgesehen. Das bedeutet, dass ein oder mehrere Rechner ausgewählte Aufgaben für alle am Netz angeschlossenen Rechner übernehmen, also Daten bereitstellen (Dateiserver), Druckaufträge abwickeln (Druckserver), Internetseiten bereitstellen (Internetserver) oder den Mailverkehr organisieren (Mailserver). Je nach Umfang dieser Aufgaben sind die Rechner entsprechend dimensioniert.

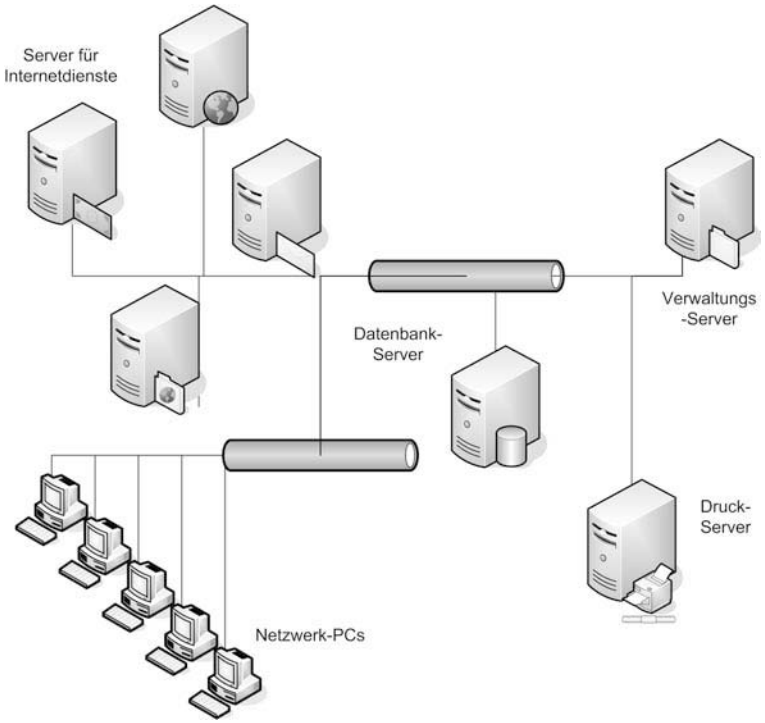

Bild 1.2: Typischer Aufbau eines Servernetzwerks.

An diesen Servern hängen sogenannte Clients, die die bereitgestellten Dienste nutzen. Im Computersprachgebrauch spricht man von Client-Server-Systemen. In einem solchen Umfeld spielen dann auch Aspekte wie die Benutzerverwaltung und

die Rechtevergabe – »Wer darf was mit welchen Daten machen?« – eine wesentliche Rolle. Schließlich soll nicht jeder die Daten der Buchhaltung einsehen können oder den teuren Farbdrucker der Werbeabteilung zur Ausgabe gescannter CD-/DVD-Cover verwenden. Für große Netze werden daher ausgeklügelte Administrationsmöglichkeiten und Netzwerkmanagementprogramme eingesetzt, um das Client-Server-System in schnellen und geordneten Bahnen zu halten.

Daten gezielt im Netzwerk verteilen

Für die Verteilung der Daten in solchen Netzwerken waren ursprünglich sogenannte Hubs zuständig, die die Daten komplett an alle angeschlossenen Systeme verteilten. Mit immer größeren Netzen wurde die Belastung durch den ungeordneten Datenverkehr so hoch, dass eine Alternative entwickelt werden musste: der Switch. Jetzt war es möglich, die Daten gezielt zu verteilen und die Netzbelastung in Grenzen zu halten. Der Switch ersetzte den Hub nahezu überall.

Ein Hub ist bei geringem Datenvolumen, das im Netz übertragen wird, eine einfache Lösung. Er agiert wie ein Bürobote, der bei jeder Postverteilung grundsätzlich alle Büros aufsucht und dann prüft, ob er etwas dabeihat. Kein Problem, solange es nur ein paar Briefe oder Faxe sind. Steigt aber die Briefmenge, braucht er zu lange bzw. werden zu viele Menschen bei der Arbeit gestört.

Der Switch ist cleverer: Er schaut vorher auf das Namensschild und die Adressierung und besucht nur die Büros, für die er etwas hat. Selbst bei großen Mengen spart das Zeit. Für den Übergang von einem Netz zum nächsten wurde das Konzept des Switchs, also des partiell intelligenten Lastverteilers, noch einmal erweitert, der Router kam hinzu. Er wickelt alle Aufträge ab, die von den Clients an ein anderes Netz geschickt werden. Ob es sich beim adressierten Netz um ein weiteres Unternehmensnetz handelt oder um das Internet, spielt keine Rolle.

1.4 Peer-to-Peer-Netze für zu Hause

Jenseits der großen Netzwerke haben die Privatanwender oder Arbeitsgruppen in kleineren Büros ganz andere Bedürfnisse: Sie benötigen normalerweise keinen speziellen Server, der Daten bereitstellt, sondern möchten nur Daten zwischen zwei oder mehreren PCs austauschen. Auch muss die Benutzerverwaltung nicht kompliziert die unterschiedlichsten Ansprüche abdecken.

Dementsprechend sieht das Netzkonzept hier etwas anders aus: Zwei oder auch mehr PCs sind prinzipiell gleichberechtigt, sie sollen Daten austauschen können und sind dazu miteinander verbunden. Da alle gleichwertig sind, spricht man von einem Peer-to-Peer-Netz.

In einem Peer-to-Peer-Netz kann jeder PC Server und Client sein, indem er einerseits Daten bereitstellt, andererseits aber auch wieder welche von anderen abruft. Für solche privaten Netze war der Hub lange Zeit ein ideales Produkt, denn das Datenaufkommen war gering, die Vorteile eines Switchs erschlossen sich erst bei einer größeren Anzahl teilnehmender PCs.

Zwei PCs mit einem Patchkabel verbinden

Die einfachste Form des gleichberechtigten Netzes ist die Direktverbindung zweier PCs per Kabel. Es lassen sich schnell Daten hin- und herkopieren, Drucker und Internet können gemeinsam genutzt werden. Mit der Verbreitung des WLAN hat das Thema Peer-to-Peer noch einmal eine Erweiterung erfahren, denn zwischen zwei WLAN-fähigen PCs ist ein schneller Datenaustausch im sogenannten Ad-hoc-Modus möglich. Dazu wird eine Direktverbindung auf Funkebene hergestellt. Das klappt zwischen stationärem PC und Notebook genauso wie zwischen zwei tragbaren PCs.

Bei einer PC-Direktverbindung können Sie zwei Rechner direkt mit einem sogenannten gekreuzten Kabel miteinander verbinden. Ein gekreuztes Kabel (Crossover-Kabel) ist einfach ein ganz normales Patchkabel (Twisted Pair), bei dem am einen Ende die Sende- und Empfangsleitung vertauscht ist. Setzen Sie keinen Hub oder Switch ein, sollten Sie unbedingt darauf achten, dass es wirklich gekreuzt ist, sonst lässt sich keine Verbindung zwischen den beiden Netzwerkkarten aufbauen. Ein gekreuztes Kabel hat normalerweise eine rote Markierung am Kabel und kostet je nach Länge 5 bis 10 Euro.

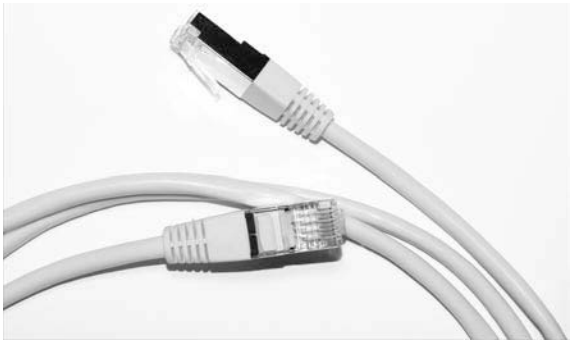

Bild 1.3: Solange nur zwei PCs im Einsatz sind, können diese über ein gekreuztes Patchkabel verbunden werden. Ein Hub oder Switch ist hier nicht notwendig.

Zeitgemäße Technik für die eigenen vier Wände ist kabellos

Peer-to-Peer-Netzwerke und Ad-hoc-Verbindungen sind allerdings nicht mehr wirklich zeitgemäß: Auch Privathaushalte stellen inzwischen ähnliche Ansprüche in Sachen Internetzugang wie kleine Unternehmen und sind auch weitaus anspruchsvoller, was die Verkabelung angeht. Wer hat schon Lust, für ein kleines Netz zwischen zwei oder drei Computern Kabel durch die Wohnung oder das Haus zu legen? Wo in Bürogebäuden Kabelschächte sind, haben Wohnungen bestenfalls Fußleisten.

Und so wird nach dem Telefon jetzt der Computer vom Kabel befreit. Einige wenige Freaks bauen sich zu Hause ihren eigenen Server für Multimedia-Dateien etc. Aber auch da zeichnet sich ein klarer Trend ab – zeitgemäße Technik fürs Wohnzimmer ist kabellos.

Wohnzimmergeräte wie Apple TV oder aber auch die Sony Playstation weisen den Weg: attraktive Technik fürs Wohnzimmer, Vernetzung per WLAN und ein grauer, rauschender Server irgendwo in einem Arbeitszimmer oder im Keller. Ob dieser Server dann mit Windows oder mit Linux realisiert wird, spielt keine Rolle, denn beide Systeme beherrschen TCP/IP und WLAN-Standards vom Typ 802.11.

1.5 TCP/IP, die Internetprotokollfamilie

Wie auch immer Ihr Netzwerk Daten übertragen wird und welches Betriebssystem Sie auch einsetzen, an TCP/IP, der Internetprotokollfamilie, kommen Sie nicht vorbei. Jetzt brauchen Sie sich aber nicht mit so diffizilen Dingen wie Protokollschichten, Headern oder dergleichen herumzuschlagen, für Sie genügen die Basics der Adressierung. Außerdem müssen Sie wissen, dass TCP/IP festlegt, wie Daten im

Internet und im Netzwerk übermittelt werden. Bei einer Netzwerkverbindung oder einer Internetverbindung wird keine direkte Verbindung zwischen zwei Punkten hergestellt, wie das beispielsweise beim Telefonieren der Fall ist.

Die Daten werden vielmehr in kleine Pakete zerlegt und auf den Weg zum Ziel geschickt. Wo sie hinmüssen, steht in der Adresse. Am Ziel werden die Pakete dann wieder in der richtigen Reihenfolge zusammengesetzt. Auch das wird über TCP/IP gesteuert, denn Reihenfolge und Anzahl der Pakete werden ebenfalls übermittelt. Dazu kommen noch ein paar Prüfgeschichten und sonstige Informationen – das muss Sie aber nicht interessieren.

Zusammensetzung einer TCP/IP-Adresse

Damit ein Rechner über TCP/IP angesprochen werden kann, muss seine Adresse, die sogenannte IP-Adresse, bekannt sein. Die Adressierung ist bei TCP/IP in ihrer Struktur festgelegt, auf der Basis der Version IPv4 können bis zu 4.294.967.296 Rechner in ein Netzwerk integriert werden. IPv4 nutzt 32-Bit-Adressen, die Weiterentwicklung IPv6 hingegen setzt auf 128-Bit-Adressen.

Eine TCP/IP-Adresse ist immer identisch aufgebaut: Sie setzt sich zusammen aus einem Netzwerkteil und einen Hostteil (Adressenteil). In der Regel ist die 32-Bit-Adresse in einen 24-Bit-Netzwerkteil und einen 8-Bit-Hostteil aufgeteilt. Der Hostteil wird im LAN (im lokalen Netzwerk) zugeteilt, während der Netzwerkteil von der IANA (*Internet Assigned Numbers Authority*) vergeben wird, die über die Vergabe der offiziellen IP-Adressen wacht.

Für die Konfiguration des Hostteils sind in einem sogenannten Class-C-Netzwerk – das ist ein typisches privates Netz – 254 Geräteadressen für angeschlossene Clients verfügbar. Die Endadresse *255* ist für den Broadcast (zu Deutsch: Rundruf, also Übertragung an alle) reserviert, während die Adresse *0* für das Netzwerk selbst reserviert ist. Für die Aufteilung des Netzwerk- und Hostteils ist die Netzmaske zuständig: Im Fall eines Class-C-Netzwerks gibt die Adresse *255.255.255.0* eine sogenannte Trennlinie zwischen beiden Teilen an. Die binäre *1* steht für den Netzwerkteil, die *0* steht für den Adressteil.

So entspricht die Netzwerkmaske

```
255.255.255.0
```

und binär

```
11111111.11111111.11111111.0000000
```

Die ersten 24 Bit (die Einsen) sind der Netzwerkanteil.

Sie müssen sich aber gar nicht mit der Adressvergabe herumschlagen, denn der heimische Rechner ist immer mit folgenden Daten ansprechbar: So sind einige Klassen von Netzwerkadressen für spezielle Zwecke reserviert, anhand deren man ablesen kann, mit welchem Netzwerk man es zu tun hat. Beispielsweise ist eine IP-Adresse beginnend mit *192.X.X.X* oder *10.X.X.X* ein internes, in Ihrem Fall ein Heimnetzwerk.

Adressbereich	Netzwerk
192.168.0.0	Heimnetz, bis zu 254 Clients
172.16.0.0	Unternehmensnetz, bis zu 65.000 Clients
10.0.0.0	Unternehmensnetz, bis zu 16 Mio. Clients

Sobald aus einem heimischen Rechner ein Netz aus mehreren Computern wird, beginnt die IP-Adresse mit *192.168.0.* Auf dieser Basis können in das Netz bis zu 254 Geräte eingebunden werden, indem die letzte Zahl von 0 bis 254 hochgezählt wird. Allerdings hat kaum jemand zu Hause so viele Geräte im Einsatz, es wird bei überschaubaren Adressbereichen bleiben.

Adresszuweisung: dynamisch oder statisch?

Gewöhnen Sie sich für die Vergabe der IP-Adressen entweder die automatische Zuweisung via DHCP oder eine statische Zuweisung mit festen Adressen an. Arbeiten Sie mit festen Adressen, sollten Sie gegebenenfalls nur ausgewählte, leicht merkbare IP-Adressen verwenden, also *192.168.0.1* für den Router, *192.168.10* für den zentralen Rechner und für weitere die Endnummern *20*, *30* etc. Wer generell Schwierigkeiten hat, sich die Nummern zu merken, kann die Rechner beispielsweise nach Alter nummerieren – in der Regel weiß man genau, welchen PC man zuerst gekauft hat.

Localhost: die Standard-IP-Adresse

Egal ob als Betriebssystem Windows, Linux, Mac OS oder was auch immer zum Einsatz kommt: Jeder PC besitzt – unabhängig davon, ob er im Internet oder im heimischen Netzwerk betrieben wird – eine Standard-IP-Adresse. Diese wird als Localhost mit der IP-Adresse *127.0.0.1* bezeichnet.

Windows-Anwender können diese Einstellung in der Datei *hosts* im Windows-Verzeichnis *C:\WINDOWS\system32\drivers\etc* prüfen. Die *hosts*-Datei lässt sich mit einem Editor wie Notepad öffnen und bearbeiten. Verhält sich der heimische PC beispielsweise nach einem Virenbefall oder Trojanerangriff seltsam und werden Webseiten fehlerhaft dargestellt bzw. wird auf andere Webseiten weitergeleitet, wurde in der Regel die *hosts*-Datei manipuliert.

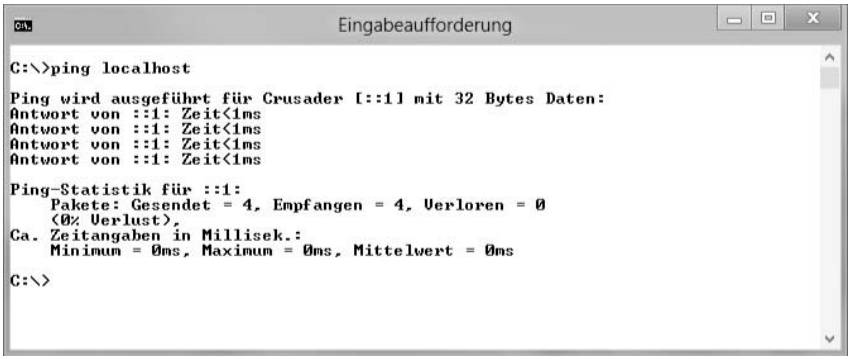

Bild 1.4: Der Rechner *localhost* wird in der *hosts*-Datei konfiguriert. Mit einem *ping localhost* wird die IP-Adresse zurückgegeben.

Reibungslose Kommunikation via Gateway

Der Vollständigkeit halber sei hier auch das sogenannte Gateway erwähnt. Innerhalb des Heimnetzwerks können sämtliche Geräte direkt miteinander kommunizieren und Daten austauschen. Soll hingegen eine Verbindung zu einem Gerät aufgebaut werden, das sich nicht innerhalb des adressierbaren Adressbereichs befindet, müssen diese Heimnetze miteinander verbunden werden. Diese Aufgabe übernimmt das Gateway bzw. der Router, der quasi sämtliche verfügbaren Netzwerke »kennt« und die Pakete bzw. Anforderungen entsprechend weiterleitet und empfängt. Im Internet sind demnach einige Router im Betrieb, da es technisch nahezu unmöglich ist, dass ein einzelner Router alle verfügbaren Netze kennt und direkt adressieren kann.

In der Regel hat der Router auch einen DHCP-Server eingebaut, der für die Vergabe der IP-Adressen im Heimnetz zuständig ist. Sind Daten für eine IP-Adresse außerhalb des Heimnetzes bestimmt, werden sie automatisch an das konfigurierte Standardgateway, also den Router, weitergeleitet. Verbindet sich der heimische

DSL-WLAN-Router mit dem Internet, versteckt dieser das private Netz hinter der öffentlichen IP-Adresse, die der DSL-WLAN-Router beim Verbindungsaufbau vom Internetprovider erhalten hat. Dieser Mechanismus der Adressumsetzung, NAT (*Network Address Translation*) genannt, sorgt dafür, dass die Datenpakete vom Heimnetz in das Internet (und wieder zurück) gelangen.

Übermittlung von IP-Adressen im Internet

Alle Server im Internet sind ebenfalls über eine IP-Adresse ansprechbar, aber das könnte sich keiner merken. Wer weiß schon, dass sich *www.franzis.de* hinter *217.64.171.171* verbirgt? Deshalb gibt es im Internet zentrale Server, deren einzige Aufgabe darin besteht, für die von Ihnen eingegebene Internetadresse (URL) den richtigen Zahlencode bereitzustellen.

Nichts anderes passiert nämlich bei der Eingabe der URL: Der Rechner übermittelt seine Anfrage im Klartext an den sogenannten *Domain Name Server* (DNS). Ein DNS-Server führt eine Liste mit Domain-Namen und den IP-Adressen, die jedem Namen zugeordnet sind.

Wenn ein Computer die IP-Adresse zu einem bestimmten Namen benötigt, sendet er eine Nachricht an den DNS-Server. Dieser sucht die IP-Adresse heraus und sendet sie an den PC zurück. Kann der DNS-Server die IP-Adresse lokal nicht ausfindig machen, fragt er einfach andere DNS-Server im Internet, bis die IP-Adresse gefunden ist.

Damit die Daten, die Sie angefordert haben – und im Internet wird jede Seite aus übermittelten Daten aufgebaut –, auch wieder zu Ihnen bzw. zu Ihrem Rechner zurückgelangen, braucht der Server Ihre IP-Adresse. Nun wird nicht jedem Internetteilnehmer kurzerhand eine IP-Adresse verliehen – dafür gibt es einfach nicht genug Adressen. Stattdessen hat jeder Provider einen Pool mit IP-Adressen, die jeweils nach Bedarf vergeben werden.

Wenn Sie sich in das Internet einloggen, teilt Ihnen der Provider eine Adresse zu, die so lange gültig ist, bis Sie die Verbindung trennen oder bei einem DSL-Anschluss 24 Stunden vorbei sind. Bei der nächsten Einwahl erhalten Sie eine andere Adresse aus dem Pool.

Diese Technik ist quasi nichts anderes als die eines DHCP-Servers (*Dynamic Host Configuration Protocol*). Damit bekommen alle an ein Netzwerk angeschlossenen Computer, egal ob WLAN oder nicht, automatisch die TCP/IP-Konfiguration

zugewiesen. Zusammen mit Ihrer Anfrage bei einer URL wird also Ihre eigene dynamische Adresse übermittelt, damit Sie auch eine Antwort bekommen.

Aus dem Internet sieht man nur den Router

Wenn Sie Ihr Netzwerk mit einem Router für den Internetzugang ausstatten, übernimmt Ihr Router künftig einen Teil der Aufgaben rund um die Adressierung. Das macht Ihnen das Leben nicht nur etwas leichter, sondern vor allem viel sicherer, denn nach außen tritt lediglich der Router in Erscheinung, Ihren PC bekommt das Internet nicht so leicht zu sehen. Das beginnt schon damit, dass von außen die zugewiesene Adresse des Rechners nicht mehr zu sehen und zu verwenden ist, sondern die des Routers. Alle Anfragen stellt der Router, alle Antworten nimmt er entgegen und leitet sie netzwerktechnisch betrachtet als Switch innerhalb des heimischen Netzes an den passenden Rechner weiter.

Für den Router gibt es also intern den Nummernkreis *192.168.X.X* und nach außen alle anderen. Der einzelne Rechner ist nicht mehr direkt ansprechbar, sondern die Adresse ist immer die des Routers. Das ist ein erster Schritt in Richtung mehr Sicherheit im Internet, denn nun kann nicht mehr direkt auf möglicherweise offene Ports Ihres Rechners oder eines anderen im Netz zugegriffen werden. Noch mehr Sicherheit bietet eine im Router aktivierte Firewall, deren Ziel es ist, nur zulässige und ungefährliche Pakete durchzulassen und bestimmte Pakete kurzerhand abzulehnen. Sie nehmen ja auch nicht jede Nachnahme an.

2 Mit WLAN überall online sein

WLAN (*Wireless Local Area Network*) ist mittlerweile nicht nur breit etabliert, sondern auch durch die niedrigen Preise erschwinglich wie nie. Das Schöne: Mit Smartphone, Tablet oder Notebook können Sie drahtlos nicht nur zu Hause, sondern fast überall online sein, vorausgesetzt, es ist ein sogenannter Hotspot in der Nähe, mit dem sich der WLAN-Anschluss des Smartphones bzw. per Notebook WLAN-Karte oder WLAN-USB-Stick verbinden kann. Das ist nach wie vor trendy und in vielen Coffeeshops, am Flughafen oder in Bahnhöfen zu beobachten.

Den meisten Spaß macht WLAN aber zu Hause. Möchten Sie den Kabelsalat ein für alle Mal aus dem Wohnzimmer verbannen oder mit Ihrer Familie oder Freunden gemeinsam den Internetanschluss ohne langwieriges Kabelverlegen nutzen, ist WLAN erste Wahl.

2.1 WLAN-Funknetze und ihre Vorteile

Obwohl WLAN primär für mobile Endgeräte wie Notebooks gedacht ist, können Sie auch stationäre Computer mit einer WLAN-Karte nachrüsten – entsprechende sind ab 10 Euro erhältlich. Ein Grund dafür kann beispielsweise der fehlende Internetzugang im Wohnzimmer sein – sprich, man möchte sich das Strippenziehen und Löcherbohren in den Wänden ersparen.

Auch für ältere Notebooks ist das Nachrüsten via PCMCIA-(PC-Card-)WLAN-Karte problemlos möglich, eine Karte kostet hier um die 30 Euro. Für Notebooks wie für Desktop-PCs gibt es eine besonders praktische Variante, den WLAN-USB-Stick. Das oft bei Uralt-Notebooks vorhandene USB 1.1 ist zwar nicht mehr zeitgemäß, reicht aber für die langsamen WLAN-Standards völlig aus. High-Speed-WLAN realisieren Sie damit ab USB 2.0, was nahezu jeder Computer neuerer Bauart beherrscht.

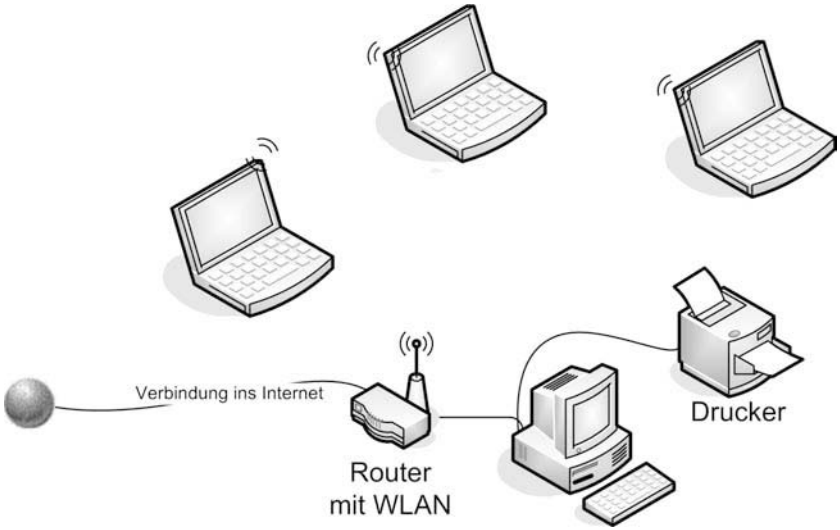

Bild 2.1: Desktop-PCs werden normalerweise per Kabel angeschlossen, Notebooks nehmen per Funk Kontakt auf.

Ein WLAN-Funknetz bietet viele Vorteile. Im Netzwerk können Sie Verbindung zu anderen Rechnern und sonstigen Geräten wie Druckern, Videoservern etc. durch Wände und eingeschränkt auch über mehrere Etagen aufbauen, ohne Kabel legen zu müssen. Außerdem ermöglicht dieses Netzwerk, mit einem Drucker mehrere Rechner zu versorgen, auf Daten zuzugreifen oder MP3s vom PC aus in der ganzen Wohnung zu hören.

Unterschiedliche WLAN-Standards

Derzeit gibt es für WLAN im Wesentlichen zwei unterschiedliche Standards: Je nachdem, welche WLAN-Steckkarte Sie nutzen, sendet diese im 2,4-GHz- oder im 5-GHz-Funkbereich. Die Funkleistung von 2,4 GHz ist mittlerweile veraltet, da es nur 11 MBit/s übertragen kann. Das moderne 5-GHz-Funknetz schafft per Standard 54 MBit/s. Firmenspezifische Lösungen bieten bei gleicher Funkleistung schon das Doppelte, diese Technik ist jedoch nicht standardisiert und macht somit speziell aufeinander abgestimmte Komponenten notwendig. Damit kommen Sie problemlos durch dicke Wände in der Wohnung oder im Haus, und im Freien kann die Reichweite um die 100 Meter für eine Funkübertragung betragen.

Mit Aufwand, also mit speziellen Antennen (ab 50 Euro), lässt sich die Reichweite bei freier Sicht auf einige hundert Meter und mit speziellen Richtantennen sogar auf bis zu zwei Kilometer erhöhen.

WLAN-Betrieb im Ad-hoc-Modus

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

WLAN-Betrieb im Infrastrukturmodus

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

2.2 WLAN-Router für das Heimnetzwerk

Für das Netzwerk zu Hause nutzen Sie einen DSL-fähigen WLAN-Router, mit dem Sie alle Räume der Wohnung mit Internet versorgen können, ohne in jedem einzelnen Raum Löcher durch die Wand bohren zu müssen. Als Erstes wird der Router ausgepackt und aufgestellt. Anschließend kommt der Rundstecker der Stromversorgung in das Gerät. Auf der Rückseite des Routers sehen Sie eine Buchse mit der Aufschrift DSL/TEL, in die Sie das Kabel des DSL-Modems stecken.

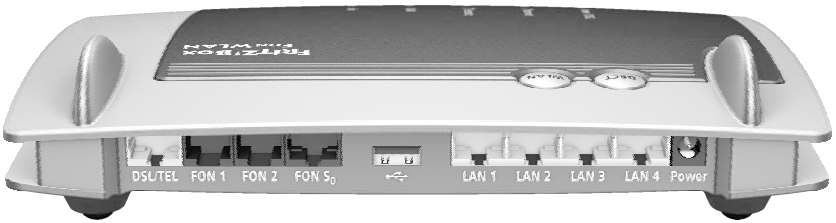

Bild 2.2: Über die DSL/TEL-Buchse (links) stellen Sie die Verbindung zum Internet Service Provider her. Hier eine FRITZ!Box Fon WLAN 7390 von AVM. (Foto: AVM)

Damit ist eine permanente Internetverbindung möglich, ohne dass ein Computer im Netzwerk laufen muss. Anschließend können Sie hier sowohl kabelgebundene Netzwerkkarten als auch WLAN-Netzwerkkarten mit einem WLAN-Router in einem gemeinsamen Netz betreiben.

Zum Einrichten und Konfigurieren des WLAN-Routers schließen Sie ihn aus Sicherheitsgründen per Twisted-Pair-Netzwerkkabel an. Das sollten Sie auch bei Notebooks beherzigen, die standardmäßig immer mit WLAN-Adaptern ausgestattet sind. Für die Ersteinrichtung ist Funk eigentlich tabu.

Grundvoraussetzung für eine WLAN-Verbindung mit einem WLAN-Router ist eine WLAN-Karte. Befindet sich in Reichweite ein WLAN-Router, können Sie kabellose Geräte miteinander verbinden und beispielsweise den Internetanschluss zur Verfügung stellen. Auch wenn die Verbindung allgemein als unsicher gilt, kann durch geschickte Konfiguration die Übertragung mithilfe verschiedenster Mechanismen sicherer gemacht werden.

Phänomen Elektrosmog
Immer wieder in der Diskussion und nicht wegzuleugnen – WLANs tragen durch ihre elektromagnetische Strahlung mit zum Phänomen Elektrosmog bei. Ähnlich wie Schnurlostelefone sind WLANs dauerhaft auf Sendung, auch wenn gerade keine Daten übertragen werden. Wenn Sie die Bildung von Elektrosmog einschränken möchten, können Sie die meisten Router mit einer Nachtschaltung abschalten. Geht das nicht, hilft nur die Methode »Stecker ziehen«. Vorsicht ist jedoch geboten, wenn Sie Internettelefonie (VoIP) nutzen. In diesem Fall sollten Sie das komplette Abschalten vermeiden, denn dann können Sie auch nicht mehr telefonieren.

Stichwortverzeichnis

Rudolf G. Glos

Heim-Netzwerke

Netzwerktechnik • High-Speed-Internet • Arbeiten im Heimnetz

DSL und drahtlose Netzwerkverbindungen einzurichten, ist keine Hexerei! Egal ob Sie einfach den Kabelsalat satthaben oder mit der ganzen Familie gemeinsam das Internet entdecken wollen – in wenigen Schritten können Sie ein WLAN selbst installieren. Was dafür nötig ist, wie Sie Ihr eigenes Heimnetz aufbauen und wie Sie damit schnell und sicher im Internet unterwegs sind, zeigt Ihnen dieses Buch.

Netzwerktechnik-Grundlagen

Sie erfahren, worauf Sie beim Gerätekauf achten sollten und wie Sie Ihr Heimnetz in Betrieb nehmen. Daneben lernen Sie den Aufbau eines Client-Server-Systems kennen und erfahren, wie die Daten per TCP/IP-Protokoll im Netzwerk übertragen werden.

DSL-WLAN-Router einrichten

Hier finden Sie das nötige Know-how, um aus dem Stand ein drahtloses Funknetz zum Laufen zu bringen. Natürlich werden auch die wesentlichen Sicherheitsaspekte im Detail besprochen.

Highspeed-Internet mit VDSL

Lesen Sie hier, was Sie alles brauchen, um den Spurwechsel auf die Highspeed-Datenautobahn ganz ohne Probleme zu vollziehen.

Das Heimnetz sicher machen

In diesem Teil des Buches lernen Sie alle Kniffe kennen, um Ihr Netzwerk nach außen abzusichern. Danach ist es für potenzielle Angreifer unsichtbar und so gut wie nicht nicht mehr zu knacken.

Andere Funknetze stören das eigene WLAN

Störstrahlungen anderer WLAN-Router beeinträchtigen die Geschwindigkeit und machen Schwierigkeiten beim Verbindungsaufbau. Lesen Sie hier, was Sie tun müssen, damit Ihr WLAN wieder läuft wie geschmiert.

Netzwerkfreigaben für Daten und Drucker

Wenige Mausklicks genügen, um Daten für andere Benutzer freizugeben und Drucker gemeinsam zu nutzen. Das gilt auch für externe Festplatten, zum Beispiel als Musikspeicher.

Aus dem Inhalt:

Über den Autor:

Rudolf G. Glos, Jahrgang 1975, hat bereits über 40 Computerbücher veröffentlicht. Mit einem Ingenieurstudium und einem Volontariat legte er die Grundlagen für seine spätere Arbeit als Journalist bei Fachzeitschriften sowie in diversen elektronischen Medien.

9 783645 601931

10,– EUR [D]
ISBN 978-3-645-60193-1