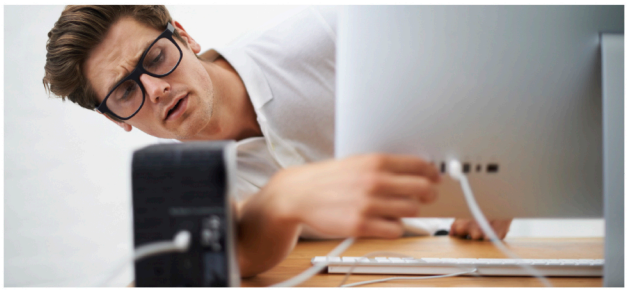
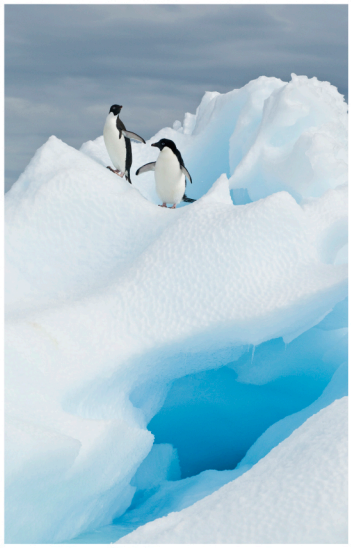
Axel Schemberg
Martin Linten
Kai Surendorf

LINUX · WINDOWS · macOS · SOFTWARE

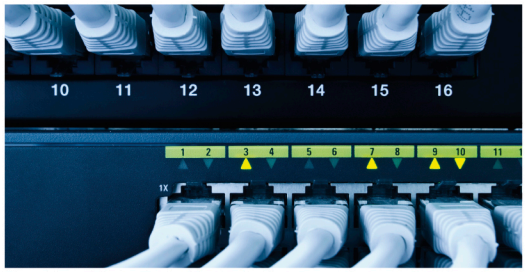


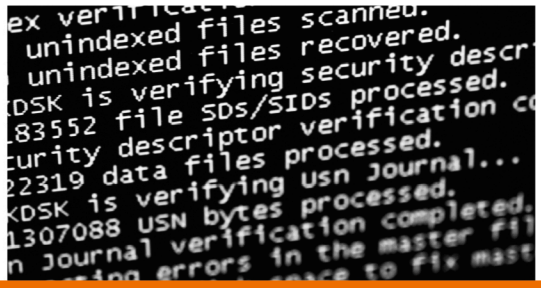


TROUBLESHOOTING

CLOUD · HARDWARE

DSL · WLAN · IP-ADRESSEN · VoIP



SICHERHEIT · BACKUP

# PC-Netzwerke

## Das umfassende Handbuch

- Heimnetzwerke für PC und Mac, zu Hause und im Büro
- LAN und WLAN planen und einrichten, auch mit mobilen Lösungen
- Smart-Home-Projekte mit Raspberry Pi und Mikrocontrollern

Vollständiger Netzwerkserver siegfried6
und viele Tools zum Download

Rheinwerk
Computing

# Kapitel 3
# Grundlagen der Kommunikation

*Dieser Teil des Buches soll Ihnen einen vertieften Überblick über das theoretische Gerüst von Netzwerken geben und damit eine Wissensbasis für die weiteren Kapitel des Buches schaffen. Das Verständnis der Theorie wird Ihnen bei der praktischen Arbeit, insbesondere bei der Fehleranalyse, helfen.*

Aktuelle Netzwerke sind strukturiert aufgebaut. Die Strukturen basieren auf verschiedenen technologischen Ansätzen.

Wenn Sie ein Netzwerk aufbauen wollen, dessen Technologie und Struktur Sie verstehen möchten, dann werden Sie ohne Theorie sehr schnell an Grenzen stoßen. Sie berauben sich selbst der Möglichkeit eines optimal konfigurierten Netzwerks.

In Fehlersituationen werden Ihnen die theoretischen Erkenntnisse helfen, einen Fehler im Netzwerk möglichst schnell zu finden und geeignete Maßnahmen zu seiner Beseitigung einzuleiten. Ohne theoretische Grundlagen sind Sie letztlich auf Glückstreffer angewiesen.

Dieses Buch legt den Schwerpunkt auf die praxisorientierte Umsetzung von Netzwerken und konzentriert sich auf die Darstellung von kompaktem Netzwerkwissen.

Ein Computernetzwerk kann man allgemein als Kommunikationsnetzwerk bezeichnen. Ausgehend von der menschlichen Kommunikation erkläre ich die Kommunikation von PCs im Netzwerk.

## 3.1 Kommunikation im Alltag

Als *Kommunikation* bezeichnet man im Alltag vieles. So wird *Telekommunikation* oft als Kommunikation bezeichnet.

Wenn Menschen miteinander reden, dann nennen wir das Kommunikation. Auch wenn sie nicht reden, sondern lediglich durch ihre Körpersprache etwas ausdrücken, kann man das Kommunikation nennen. Wichtig ist nicht, über welches Medium Informationen übertragen werden, sondern der Informationsaustausch selbst ist das Entscheidende.

Jede Art von Kommunikation besteht aus den folgenden Komponenten:

- Sender
- Empfänger
- Übertragungsmedium
- Regeln
- Kodierung des Inhalts

Die Punkte 1 und 2 sind wohl nicht erläuterungsbedürftig, doch was ist ein *Übertragungsmedium* (Punkt 3)? Beim Sprechen wird Schall über die Luft, bei einem Bild die Farbe über Lichtreflexion und bei der Telekommunikation elektrische Spannung durch Kabelleitungen übertragen; die Medien sind Luft, Licht und das Kabel.

Entweder benutzen beide Gesprächspartner das gleiche Medium, oder es gibt einen Wandler, der die Informationen umwandelt. Beispielsweise wandelt das Telefon die akustischen Signale der menschlichen Sprache in elektrische Spannung um. Diese Spannung wird dann über Leitungen transportiert, bis sie schließlich beim empfangenden Telefon wieder in akustische Signale zurückgewandelt wird. Zumindest war das vor 50 Jahren in der Telefonie so.

*Regeln* (Punkt 4) in der menschlichen Kommunikation sind – soweit sie erfolgreich verlaufen soll – z. B.: »Mit vollem Mund spricht man nicht«, »Lass mich ausreden«, »Jetzt spreche ich!« und Ähnliches. Im Allgemeinen unterbricht man einen anderen beim Sprechen nicht, so dass er ausreden kann. Macht Ihr Gesprächspartner eine Sprechpause, so können Sie sich äußern, das besagt die Regel.

Die *Kodierung des Inhalts* (Punkt 5) meint z. B. eine Sprache (Deutsch). Eine Sprache selbst hat schon viele eigene Details. Wenn man sie verstehen will, muss man wissen, welche Wörter welche Bedeutung haben und wie grammatische Beziehungen hergestellt werden.

Erfüllen beide Partner die Punkte 1 bis 5, dann kommt es zu einer erfolgreichen Kommunikation. Sie können sich unterhalten und somit in beide Richtungen Informationen austauschen.

## 3.2 Kommunikation zwischen Computern

Auch bei der Kommunikation zwischen Computern sind die gerade genannten Bestandteile wichtig:

- Sender
- Empfänger
- Übertragungsmedium
- Regeln
- Kodierung(en)

Es gibt also hinsichtlich der betrachteten Anforderungen keinen Unterschied zwischen der menschlichen und der PC-Kommunikation. Selbstverständlich handelt es sich bei PCs um »dumme« Kommunikationsteilnehmer, und so müssen die Regeln zu eindeutigen Informationen führen, damit sie für PCs verwertbar sind.

Wichtig ist ebenfalls, dass es Medienwechsel geben kann. Ein Handygespräch zu einem Festnetzanschluss erfolgt bis zum Sendemast des Mobilfunkbetreibers über Funk. Dort wird dann eine Transformation in elektrische oder optische Signale auf Kabelbasis vorgenommen.

Es ist sinnvoll, für alle Anwendungen, die über ein Netzwerk kommunizieren wollen, wiederkehrende Aufgaben einheitlich zu lösen. Es werden für jede Anwendung Schnittstellen bereitgestellt, auf denen sie aufsetzen kann. Bestimmte Aufgaben wie eindeutige Adressierung müssen daher nicht von jeder Anwendung gelöst werden, sondern werden zentral (z. B. vom Betriebssystem) übernommen.

## 3.3 Was ist nun ein Netzwerk?

Als *Netzwerk* bezeichne ich die Verbindung von mindestens zwei PCs. Selbstverständlich können auch andere Netzwerkteilnehmer als PCs in ein Netzwerk eingebunden werden. Dieses Buch wird die Einbindung z. B. von UNIX-Workstations und Ähnlichem nicht weiter beschreiben, sondern sich auf die Verbindung von PCs mit den Betriebssystemen Windows, Linux oder macOS konzentrieren. Ich werde daher im weiteren Verlauf dieses Buches den Begriff *PC* verwenden; allgemeiner formuliert steht der PC stellvertretend für *Netzwerkteilnehmer*.

Wenn ich von einem Netzwerk oder *LAN* spreche, dann meine ich ein Netzwerk, das auf dem Ethernet-Standard basiert. Ethernet (siehe Kapitel 6, »Ethernet«) ist ein Standard zum Kodieren von Datenpaketen und zum Senden und Empfangen von Daten. Man kann sagen, dass Ethernet die grundsätzlichen Dinge der Netzwerkkommunikation und den Zugang zum Netzwerk regelt. Um die Ausführungen zu Ethernet besser verstehen zu können, ist es notwendig, einen kurzen Exkurs zur grundlegenden Struktur eines Netzwerks (siehe Kapitel 4, »Netzwerktopologien«) und zum grundlegenden Aufbau der Kommunikationsschichten (siehe Kapitel 5, »Kommunikationsmodelle«) zu machen.

# Kapitel 4
# Netzwerktopologien

*Der Begriff Topologie bedeutet Anordnung oder Aufbau. Es gibt verschiedene Ansätze für den Aufbau eines Netzwerks. Damit legen Sie indirekt fest, wie PCs in Ihrem LAN mit anderen PCs verkabelt werden können.*

Das *Link Layer Discovery Protocol* (*LLDP*), das nach IEEE 802.1ab normiert wurde, ermöglicht die Identifikation benachbarter Geräte in einem Netzwerk. Dazu verwendet es spezielle Ethernet-Multicast-Pakete (siehe Abschnitt 6.10.2, »Ethernet-Multicast«), um damit z. B. Informationen zwischen Switches auszutauschen.

Die Firma AVM integriert LLDP in die neueren Firmwareversionen einer FRITZ!Box und ermöglicht so die Erkennung, Darstellung und Optimierung der Kommunikationswege in einem Mesh-Netzwerk (siehe Abschnitt 7.20, »WLAN-Mesh«).

Man kann Netzwerke in verschiedenen Topologien aufbauen. Grundsätzlich unterscheidet man zwischen der Bus-, der Ring- und der Sterntopologie. Die Unterschiede möchte ich Ihnen im Folgenden kurz vorstellen.

## 4.1 Bustopologie

Die Urform von Ethernet, der heute üblichen Vernetzungstechnik für lokale Netze (siehe Kapitel 6, »Ethernet«), war die *Bustopologie* (siehe Abbildung 4.1).

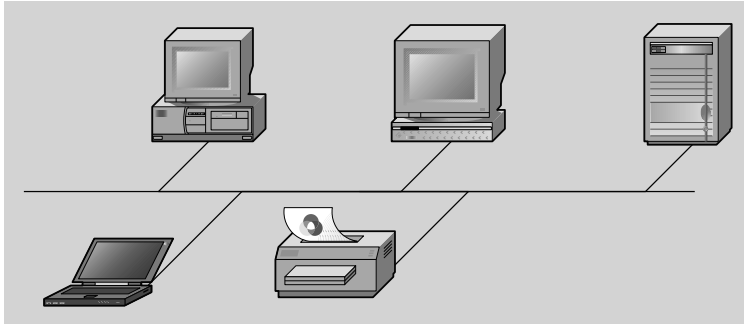


**Abbildung 4.1** Bustopologie

Ähnlich wie eine Hauptwasserleitung gibt es ein zentrales Kabel, an das alle teilnehmenden Stationen mit Stichleitungen angeschlossen werden. Ein eindeutiges Merkmal ist, dass dadurch eine dezentrale Struktur entsteht: Jedes Gerät ist gleichrangig an den Bus angeschlossen. Kommt es zu einer Störung der »Hauptwasserleitung«, sind alle angeschlossenen Stationen von dieser Störung betroffen. Diejenigen von Ihnen, die die *BNC-Verkabelung* noch kennen, wissen, dass es sich bei dieser Art von Netzwerken um Museumsstücke handelt.

## 4.2 Ringtopologie

*Token-Ring* und *ATM* sind Beispiele für eine *Ringtopologie* (siehe Abbildung 4.2). Vereinfacht erklärt wandert ein Token (dt. *Zeichen, Symbol*; stellen Sie sich einen Stab beim Staffellauf vor) im Kreis – daher der Name Token-Ring. Wenn das Token frei ist, kann jeder Netzteilnehmer das Token nehmen, ein Netzwerkpaket daranhängen und es innerhalb des Kreises an einen anderen Netzwerkteilnehmer schicken. Bei ATM, der schnelleren Variante der Ringtopologie, wandert nicht ein einziges Token im Kreis, sondern es fährt – bildlich gesprochen – ein Güterzug. Erwischt Ihr PC einen leeren Waggon – eine ATM-Zelle –, kann er seine Daten dort ablegen und weiterreisen lassen.

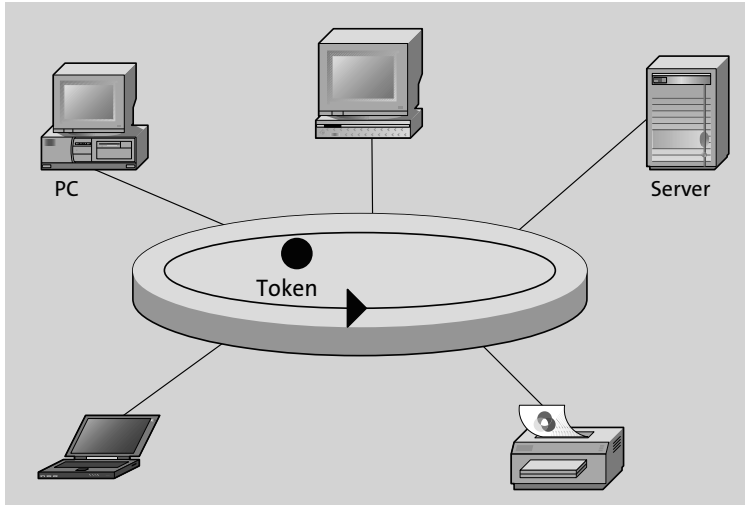



**Abbildung 4.2** Ringtopologie

Token-Ring wird auch als *Toter Ring* bezeichnet, weil diese Technologie mittlerweile ausgestorben ist. ATM konnte sich im LAN nicht durchsetzen, weil es zu kostenintensiv betrieben werden muss. Im Bereich der Weitverkehrsnetze hat sich die Technologie etabliert, wird dort aber inzwischen ebenfalls verdrängt.

## 4.3 Sterntopologie

Die *Sterntopologie* ist die Struktur, die sich bei Twisted-Pair-Verkabelungen ergibt (siehe Abbildung 4.3). Fast Ethernet und Gigabit-Ethernet, die schnellen Varianten von Ethernet, werden ausschließlich in Sterntopologie realisiert.

Wenn Ethernet – mit 10 Mbit/s – über eine Twisted-Pair-Verkabelung betrieben wird, handelt es sich ebenfalls um eine Sternstruktur. Es gibt ein zentrales Element, ursprünglich den Hub (dt. *Radnabe*), von dem sternförmig die Zuleitungen zu den einzelnen Netzteilnehmern – wie die Speichen eines Rades – führen.

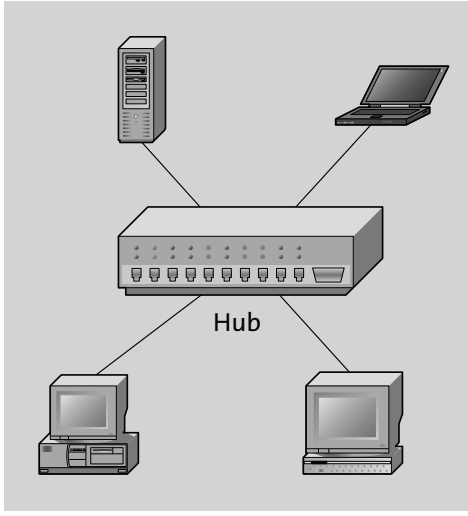



**Abbildung 4.3** Sterntopologie

Jeder Netzteilnehmer hat eine eigene Zuleitung. Ist eine Zuleitung gestört, bleiben die anderen Teilnehmer davon unbehelligt.

# Kapitel 5
# Kommunikationsmodelle

*Das Wort »Kommunikationsmodell« wird Sie vielleicht ein wenig verschrecken. Es klingt aber komplizierter, als es ist. Mit einer Einschätzung haben Sie allerdings recht: Es ist Theorie. Mit einem Modell haben Sie Ihr komplettes Netzwerk verstanden.*

Damit die Kommunikation in einem Netzwerk allgemein beschrieben werden kann, wurden kluge Leute damit beauftragt, ein Kommunikationsmodell zu entwickeln. Diese Leute fanden heraus, dass es möglich ist, die wesentlichen Leistungen in einem Netzwerk in verschiedene Aufgaben zu gliedern. Diese Aufgaben werden im Kommunikationsmodell als *Schichten* bezeichnet. Jede Schicht erfüllt eine Hauptaufgabe, damit die Kommunikation im Netzwerk stattfinden kann. Sie erinnern sich sicherlich noch an Abschnitt 3.1, »Kommunikation im Alltag«, der das Thema menschliche Kommunikation behandelt. Analog zu den dort genannten Voraussetzungen für die menschliche Kommunikation werden im Kommunikationsmodell die Schichten definiert.

Lernen Sie, in den Schichten dieser Kommunikationsmodelle zu denken und insbesondere Probleme anhand dieser Einteilungen zu lösen. Wenn Sie das Modell der Netzwerke verstanden haben und in diesen Schichten denken gelernt haben, werden Sie auch Netzwerke leicht verstehen!

Eine Schicht muss für eine eindeutige Adressierung im Netzwerk sorgen. Eine weitere muss regeln, wann Daten gesendet werden – im Ergebnis eine Art Vorfahrtsregelung für das Netzwerk.

Wenn schließlich alle Aufgaben festgelegt sind, müssen sie noch praktisch umgesetzt werden. Es gibt definierte Schnittstellen zu den benachbarten Schichten. Wenn es also mehrere Implementierungen (Umsetzungen) einer Schicht gibt, sind sie beliebig austauschbar, weil die Schichten unabhängig voneinander arbeiten.

Es existieren zwei bekannte konkurrierende Kommunikationsmodelle, auf deren Struktur sämtliche Netzwerke basieren: *DoD* und *ISO/OSI*. Diese beiden Modelle widersprechen sich nicht. Allerdings sind sie unterschiedlich umfangreich, und

dadurch entspricht die Schicht 1 des DoD-Modells nicht der Schicht 1 des ISO/OSI-Modells. Leider verwenden die beiden Modelle nicht die gleichen Bezeichnungen für die einzelnen Schichten.

Wenn Sie einige der nachfolgenden Begriffe nicht kennen, seien Sie unbesorgt, diese werden alle in den folgenden Kapiteln erklärt. Wenn Sie schon jetzt neugierig sind, finden Sie eine kurze Definition der Begriffe und Abkürzungen im Glossar.

## 5.1 DoD-Modell

Das *Department of Defense* (*DoD*), das US-Verteidigungsministerium, hat ein theoretisches Modell entwickeln lassen, nach dem ein Netzwerk aufgebaut werden sollte (siehe Tabelle 5.1).

| Nr. | Schicht | Beispiele in der Praxis | | | |
|---|---|---|---|---|---|
| 4 | Process | HTTP | SMTP | FTP | DNS |
| 3 | Transport | TCP | | UDP | |
| 2 | Internetwork | IP | | IPX | |
| 1 | Network Access | Ethernet | ATM | FDDI | TR |

**Tabelle 5.1** Das DoD-Modell

Die Physik, also das Kabel und die Signalisierung, vermissen Sie sicherlich in dem abgebildeten Modell. Sie können sich diese als weitere Schichten vorstellen, die unterhalb von *Network Access* angeordnet sind.

- *Network Access* ist die Netzzugangsschicht. Eine Umsetzung dieser Schicht ist Ethernet, das ich noch ausführlich erläutern werde. Aufgabe: Wann darf gesendet werden? Wie wird gesendet? Wie lautet die Adressierung?
- *Internetwork*: Die bekannteste Implementierung ist das *Internet Protocol* (*IP*). Aufgabe: Wie bringe ich die Daten zum Empfänger? Wie ist die Wegewahl?
- *Host-to-Host*, auch *Session-Layer* genannt. Aufgabe: Überwachen der Kommunikation (sind alle Pakete angekommen?) und Adressieren der Pakete an die richtige Anwendung
- *Process*: Ihre Anwendungen. Aufgabe: Was auch immer die Aufgabe der jeweiligen Software ist.

Das DoD-Modell verfügt über vier Schichten, die Sie in der praktischen Arbeit in Ihrem Netzwerk wiederfinden werden. Sie verwenden als Netzwerkverfahren Ethernet,

denn Sie verwenden Ethernet-Karten. Sie vergeben *IP*-Adressen, vielleicht kennen Sie auch *TCP*/*UDP*-Ports. Und sicherlich haben Sie schon einmal in die Adresszeile Ihres Browsers *http://...* eingegeben. Wie die einzelnen Schichten in Form der verschiedenen Verfahren (Ethernet, IP, TCP und HTTP) zusammenarbeiten, werde ich im weiteren Verlauf darstellen.

## 5.2 ISO/OSI-Modell

ISO ist die *International Organization for Standardization*, also das Gremium für international gültige Standards. Dort wurde das *ISO/OSI-7-Schichtenmodell* entwickelt, um die Kommunikation innerhalb des Netzwerks zu beschreiben (siehe Tabelle 5.2). Statt der vier Schichten des DoD-Modells gibt es dort sieben Schichten (engl. *layers*).

| Nr. | Schicht | Beispiele | | | |
|---|---|---|---|---|---|
| 7 | Application | HTTP | SMTP | FTP | DNS |
| 6 | Presentation | | | | |
| 5 | Session | | | | |
| 4 | Transport | TCP | | UDP | |
| 3 | Network | IP | | IPX | |
| 2 | Data Link | Ethernet | ATM | FDDI | TR |
| 1 | Physical | Manchester | 10B5T | Trellis | |

**Tabelle 5.2** ISO/OSI-7-Schichtenmodell

Die Aufgaben der einzelnen Schichten entsprechen denen des DoD-Modells. Im Unterschied zum DoD-Modell gibt es als Schicht 1 den *Physical Layer*, dieser regelt die Kodierung der Bits in Stromsignale. Daher entspricht die Schicht 2 des ISO/OSI-Modells der Schicht 1 des DoD-Modells.

Der *Presentation* und der *Session Layer* haben nur wenig Bedeutung erlangt, weil die dort vorgesehenen Funktionen durch die Applikationsschicht, den *Application Layer*, erfüllt werden.

Der direkte Vergleich der beiden Modelle in Tabelle 5.3 verdeutlicht, dass die Unterschiede eigentlich gar nicht so groß sind.

| DoD | ISO | Schicht | Beispiele | | | |
|---|---|---|---|---|---|---|
| 4 | 7 | Application | HTTP | SMTP | FTP | DNS |
| | 6 | Presentation | | | | |
| | 5 | Session | | | | |
| 3 | 4 | Transport | TCP | | UDP | |
| 2 | 3 | Network | IP | | IPX | |
| 1 | 2 | Data Link | Ethernet | ATM | FDDI | TR |
| | 1 | Physical | Manchester | 10B5T | Trellis | |

**Tabelle 5.3** Vergleich zwischen dem DoD- und dem ISO/OSI-Modell

[+] Das ISO/OSI-7-Schichtenmodell hat im Netzwerkbereich deutlich die größere Bedeutung der beiden Modelle erlangt. Es prägt die Begrifflichkeiten der Netzwerktechnologie (Layer-3-Switch), daher bezeichne ich in diesem Buch die Schichten nach dem ISO/OSI-Modell, so dass Sie sich an die Benutzung der Schichtenbezeichnungen gewöhnen können.

## 5.3 Ablauf der Kommunikation

Ich möchte in diesem Abschnitt beschreiben, wie die einzelnen Schichten zusammenarbeiten, also wie die Kommunikation im Netzwerk funktioniert. Dazu werde ich mein Beispiel auf der Applikationsschicht beginnen.

[»] Stellen Sie sich vor, Sie geben z. B. die Adresse *http://www.web.de* im Adressfeld Ihres Browsers ein. Wenige Sekunden später ist die Webseite des Anbieters *WEB.DE* vollständig auf Ihren Bildschirm übertragen. Zwischen der Eingabe der Adresse in den Browser und dem Erscheinen der Webseite liegen viele übertragene Datenpakete und viel Netzwerkkommunikation.

Der Ablauf ist in Tabelle 5.4 dargestellt. Jedes Datenpaket wird auf die gleiche Art und Weise abgearbeitet.

| Schritt | Beschreibung | ISO/OSI |
|---|---|---|
| 1 | Ihre Anfrage nach der Webseite wird in ein HTTP-Datenpaket verpackt und über eine Betriebssystemschnittstelle an TCP übergeben. | 7 |
| 2 | Sie möchten einen Webserver ansprechen, d. h. HTTP-Pakete mit ihm austauschen. Es ist festgelegt, dass HTTP dem TCP-Port 80 entspricht. Entsprechend wird nun ein TCP-Paket erzeugt, in dessen Datenteil das HTTP-Paket enthalten ist und in dessen Verwaltungsteil (engl. *header*) die Zielnummer 80 (TCP-Serverport) steht. Zusätzlich wird dort ein zufälliger TCP-Port Ihres PCs eingetragen, z. B. 1333, auf dem Ihr Browser horcht. | 4 |
| 3 | Der Webserver von WEB.DE hat eine IP-Adresse. Anhand dieser IP-Adresse kann der Weg zu ihm gefunden werden. Das IP-Paket enthält im Datenteil das TCP-Paket (mit dem HTTP-Paket aus Schritt 1) und im Verwaltungsteil (Header) die Ziel-IP-Adresse sowie die IP-Adresse Ihres PCs als Quell-IP-Adresse. | 3 |
| 4 | Sie senden das Datenpaket in Ihrem LAN aus, daher muss dieses Datenpaket mit dem Ethernet-Verfahren übertragen werden.<br>Es entsteht ein Ethernet-Paket, das neben den ineinander verpackten Paketen aus den Schritten 1 bis 3 die Ziel-Quell-MAC-Adresse enthält. Dies ist die MAC-Adresse Ihres DSL-Routers.<br>Die Netzwerkkarte führt nun das Ethernet-Verfahren durch und sendet erst, wenn die Leitung frei ist. | 2 |
| 5 | An Ihre Netzwerkkarte ist ein Kupferkabel angeschlossen, daher können Informationen über dieses Medium nur als elektrische Spannungen übertragen werden.<br>Jede binäre Null wird durch keine Spannung und jede binäre Eins durch eine Spannung von 5 Volt dargestellt. | 1 |
| 6 | Das Paket wird über das Internet übertragen und passiert dabei viele Router. Schließlich wird das Paket vom Webserver empfangen. | – |
| 7 | Der Empfänger stellt an seiner Netzwerkkarte wechselnde Spannungen fest. Er interpretiert für 5 Volt eine binäre Eins und bei keiner Spannung eine binäre Null. Das Ergebnis ist eine Folge von Binärziffern. | 1 |

**Tabelle 5.4** Kommunikation im ISO/OSI-Modell

| Schritt | Beschreibung | ISO/OSI |
|---|---|---|
| 8 | Von der Netzwerkkarte erhält der Netzwerkkartentreiber ein Datenpaket im Ethernet-Format. Es enthält seine MAC-Adresse als Ziel-MAC-Adresse und eine Quell-MAC-Adresse. Im Datenteil befindet sich ein IP-Paket. | 2 |
| 9 | Das IP-Paket enthält als Ziel-IP-Adresse die IP-Adresse des Webservers und die Quell-IP-Adresse Ihres PCs zu Hause. Im Datenteil befindet sich ein TCP-Paket. | 3 |
| 10 | Das TCP-Paket wendet sich an den Serverport 80, also an den Webserver. Entsprechend wird der Datenteil an die Webserver-Applikation übergeben. Eine Antwort muss an den TCP-Clientport 1333 gerichtet werden. | 4 |
| 11 | Der Webserver-Prozess bekommt ein HTTP-Paket, in dem die Hauptwebseite angefordert wird. | 7 |

**Tabelle 5.4** Kommunikation im ISO/OSI-Modell (Forts.)

Ihre Anfrage an die Webseite geht von einer Applikation (einem Programm) aus, das ein Applikationsdatenpaket erzeugt. Dieses Paket wandert – logisch gesehen – die ISO/OSI-Schichten hinunter (Schicht 7, 4, 3, 2 und 1) und wird schließlich als elektrisches Signal übertragen. Der Webserver von WEB.DE empfängt ein elektrisches Signal mit seiner Netzwerkkarte und erzeugt daraus ein Datenpaket. Dieses beginnt seine Wanderung die ISO/OSI-Schichten hinauf (Schicht 1, 2, 3, 4 und 7) und wird auf der Applikationsschicht von der Anwendung Webserver verarbeitet.

[»] Das Verfahren, das ich in Abbildung 5.1 beispielhaft für eine HTTP-Anfrage dargestellt habe, findet für jedes Datenpaket statt.

Das klingt alles sehr kompliziert. Warum also macht man es nicht einfacher? Es könnte doch direkt Anwendung mit Anwendung sprechen, oder? Denkbar, doch zwischen Ihnen und dem Webserver von WEB.DE liegen noch weitere Providernetzwerke. Alle Komponenten müssten die Anwendung bzw. das HTTP-Protokoll direkt verstehen. Die Anwendung, also z. B. der Browser, müsste sich darum kümmern, wie sie den Eingang von Paketen überwacht und wie man zum Ziel *http://www.web.de* kommt. Außerdem müsste sie die Integrität der Daten überwachen und wie die Signale auf dem Kabel in elektrische Spannung umgesetzt werden. Das sind sehr viele Aufgaben, die diese Applikation erfüllen müsste. Wenn Sie nur das HTTP-Protokoll betrachten, ist der Aufwand gleich groß wie bei der Entwicklung selbständiger Schichten.

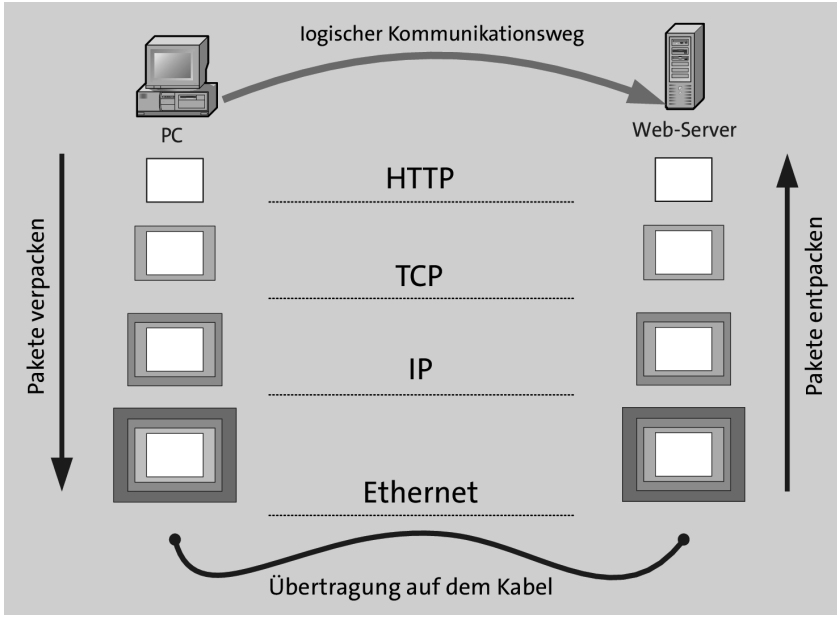



**Abbildung 5.1** Datenkommunikation nach ISO/OSI-Modell

Über das Internet kommunizieren noch weitere Applikationen Ihres PCs (z. B. FTP, SIP und SMTP), und jede dieser Anwendungen müsste sich um alle Teile der Netzwerkkommunikation kümmern. Dies würde bedeuten, dass einerseits die Entwicklung von Anwendungen sehr komplex und andererseits die Übermittlung von Daten über allgemeine Netzwerke (z. B. das Internet) fast unmöglich würde – schließlich müsste jedes Netzwerkgerät, insbesondere der Router, z. B. die programmspezifische Adressierung verstehen, denn IP-Adressen gäbe es dann ja nicht.

# Kapitel 7
# Wireless LAN

*Drahtlose Netzwerke haben viele Vorteile und sind zurzeit ein großer Verkaufserfolg. Auch außerhalb der Netzwerke wird alles drahtlos: Tastaturen, Mäuse und Headsets werden mit Bluetooth-Funk versorgt. Mobile Geräte sind weitverbreitet. Dieser Trend setzt sich auch bei Netzwerken durch. Bevor Sie sich für den Einsatz dieser Technik entscheiden, sollten Sie jedoch einige Besonderheiten beachten.*

Im *ISM-Band* von 2,4 GHz darf jedermann innerhalb seines Grundstücks[1] mit einer maximalen Sendeleistung von 100 mW funken. Dem Benutzer entstehen keine Lizenzkosten oder Ähnliches. Zudem ist dieses Frequenzband international reserviert.

Leider arbeiten neben verschiedenen Funktechniken auch Mikrowellenherde[2] und diverse andere Geräte auf genau diesem Frequenzband, so dass es vielfältige Störquellen gibt. Es bestehen zudem einige Einschränkungen, so dass Sie sich bei einem Einsatz außerhalb von Deutschland zusätzlich über die besonderen rechtlichen Vorschriften des betreffenden Landes informieren sollten.

Im 5-GHz-Band darf unter bestimmten Voraussetzungen – so dient z. B. der automatische Kanalwechsel bei erkanntem eigenem Störpotential mittels *Dynamic Frequency Selection* (*DFS*) insbesondere dem Schutz von *Primärnutzern* wie dem Militär oder Wetterradarsystemen – mit bis zu einem Watt Leistung gesendet werden. Die höhere Leistung kann aufgrund der höheren Dämpfung jedoch nur teilweise in größere Reichweiten umgesetzt werden.

Für alle WLAN-Varianten gilt gleichermaßen, dass es sich bei den angegebenen Datenraten um Bruttodatenraten handelt. Erst nach Abzug der Steuerungsdaten erhalten Sie die Nettodatenrate. Außerdem teilen sich alle Teilnehmer die Bandbreite.

1 Ein grundstücksübergreifendes Netzwerk ist bei der Bundesnetzagentur anzeigepflichtig, aber genehmigungsfrei.

2 Gefährdet sind die WLAN-Kanäle 9 und 10.

## 7.1 IEEE 802.11

In Tabelle 7.1 und in Tabelle 7.2 möchte ich Ihnen einen Überblick über den Buchstabensalat im Bereich der WLANs verschaffen.

| Arbeitsgruppe | Wi-Fi-Generation | Arbeitsgebiet |
|---|---|---|
| 802.11 | | Urform des WLANs von 1997, mit 2 Mbit/s im 2,4-GHz-Band |
| 802.11a | | 54-Mbit/s-WLAN im 5-GHz-Band |
| 802.11b | | 11-Mbit/s-WLAN im 2,4-GHz-Band |
| 802.11g | | 54-Mbit/s-WLAN im 2,4-GHz-Band |
| 802.11h | | 54-Mbit/s-WLAN im 5-GHz-Band mit den europäischen Ergänzungen DFS und TPC |
| 802.11j | | Entspricht 802.11a, aber Frequenzbereich für Japan. |
| 802.11n | Wi-Fi 4 | Verbesserungen für schnellere WLANs mit 150 Mbit/s pro Datenstrom im 5-GHz- und 2,4-GHz-Band |
| 802.11p | | Kommunikation zwischen Fahrzeugen im 5,9-GHz-Frequenzband |
| 802.11ac | Wi-Fi 5 | Gigabit-WLAN im 5-GHz-Band |
| 802.11ad | | Gigabit-WLAN im 60-GHz-Band |
| 802.11ax | Wi-Fi 6 | 11-Gigabit-WLAN |
| 802.11be | Wi-Fi 7 | 40-Gigabit-WLAN |
| 802.11ay | | Nachfolger von 802.11ad |

**Tabelle 7.1** IEEE 802.11: Übertragungsverfahren

Mit der Einführung von IEEE 802.11ax hat die *Wi-Fi Alliance* (siehe Abschnitt 7.12, »Wi-Fi Alliance«) beschlossen, zusätzlich zu den kryptischen Namen der Standards mit den *Wi-Fi-Generationen* sprechendere Namen einzuführen.

Es gibt einzelne Chips und somit auch Geräte, die drei oder mehr Standards gleichzeitig unterstützen und somit ähnlich wie Tri-Band-Handys universell funktionieren. Für sie gilt das Gleiche wie für Handys: Es war schon immer teurer, einen besonderen Geschmack zu haben.

Alle Teilnehmer im WLAN teilen sich die Bandbreite. Gibt es also neun Stationen, die gleichzeitig einen WLAN-Zugang (*Access Point*) mit 54 Mbit/s benutzen, dann stehen im Idealfall jeder Station 6 Mbit/s zur Verfügung. Zudem beträgt die effektive Nutzdatenrate in etwa die Hälfte der gerade genannten Bruttodatenrate. Aktuelle Standards verwenden *MIMO*-Technik (siehe Abschnitt 7.13.5, »Multiple Input, Multiple Output«) und *Multi-User MIMO* (siehe Abschnitt 7.13.6, »Multi-User MIMO«).

| Arbeitsgruppe | Arbeitsgebiet |
|---|---|
| 802.11c | Wireless Bridging |
| 802.11d | »World Mode«, Anpassung an regionsspezifische Regulatorien |
| 802.11e | QoS- und Streamingerweiterung für 802.11a/g/h |
| 802.11f | Inter Access Point Protocol = IAPP, macht z. B. Handover (Roaming zwischen Access Points) möglich |
| 802.11i | Authentifizierung/Verschlüsselung für 802.11a/b/g/h (AES, 802.1x) |
| 802.11k | Erweiterung, die ortsbezogene Dienste zulassen soll (*location-based services*) |
| 802.11m | Weiterentwicklung der Standards (Maintenance) |
| 802.11r | Fast Handover, Roaming zwischen Access Points |
| 802.11s | Aufbau von Mesh-Netzwerken |
| 802.11t | Testverfahren (WPP) und Messverfahren |
| 802.11u | Zugangsverwaltung von Hot Spots (*Hotspot 2.0*, *Passpoint*) |
| 802.11v | WLAN-Management |
| 802.11w | Datenintegrität und Sicherheit |
| 802.11-2012 | zusätzliches 3,7-GHz-Band (3.650 bis 3.700 MHz) |

**Tabelle 7.2** IEEE 802.11: Ergänzungen

Ein Access Point verrät seinen *Service Set Identifier* (*SSID*) durch *Beacons* (dt. *Signalfeuer*). Ein Beacon-Paket enthält unter anderem die SSID, MAC-Adresse, maximale Datentransferrate und Zeitinformationen.

In einem Beacon kann eine *Traffic Indication Map* (*TIM*) enthalten sein. Die TIM ist eine Nachricht, die WLAN-Clients aus dem Energiesparmodus aufweckt, denn aus Energiespargründen können WLAN-Clients im *Polled Access Mode* (*PAM*) betrieben werden. Wenn Daten für diese Clients am Access Point vorhanden sind, werden die Clients angesprochen und mit einer TIM aufgeweckt.

Es gibt zwei Möglichkeiten für den Betrieb eines WLANs:

- Im *Ad-hoc-Modus* funkt eine WLAN-Karte zu einer anderen WLAN-Karte. Dabei können mehrere WLAN-Verbindungen gleichzeitig bestehen. Der einzige Nachteil im Vergleich zum Infrastruktur-Modus ist die geringere Sende- und Empfangsleistung. Andere Ausdrücke sind *Peer-to-Peer-Netz* oder *Independent Basic Service Set* (*IBSS*).
- Der *Infrastruktur-Modus* kann betrieben werden, wenn man über mindestens einen *Access Point* (*AP*) verfügt. Ein AP ist eine Empfangsanlage, meist mit integrierter Antenne für ein WLAN, und wird üblicherweise mit einem Steckernetzteil oder über das LAN-Kabel mit Strom versorgt. Gewöhnlich stellt der AP auch die Verbindung zum drahtgebundenen LAN her.

»Welchen Modus soll ich einsetzen?«, werden Sie sich fragen. Im Ad-hoc-Modus wird ein WLAN aufgebaut, wenn man nur eine begrenzte Zahl von Clients untereinander spontan verbinden will und keinen Zugang in das kabelgebundene LAN benötigt. Meistens wird WLAN im Infrastruktur-Modus verwendet.

Ein wesentlicher Unterschied zwischen drahtgebundenen und drahtlosen Netzen ist aus physikalischer Sicht, dass man bei einem drahtlosen WLAN keine Kollisionen erkennen kann. Es kann aber aufgrund des nicht deterministischen Zugangsverfahrens immer zu Kollisionen kommen, die bei Ethernet durch das CSMA/CD-Verfahren behandelt werden. Wenn man Kollisionen nicht erkennen kann, ist es auch nicht möglich, den Fall einer Kollision zu behandeln. Bei WLAN gilt daher *CSMA/CA*: Dies steht für *Collision Avoidance*, die Kollisionsvermeidung. Bei diesem Verfahren hört die sendewillige Station das Medium – also den Funkkanal – ab. Falls dieser frei ist, wartet sie mit dem *Interframe Space* (*IFS*) eine weitere definierte Zeit ab. Ist das Medium am Ende der Wartezeit immer noch frei, wird gesendet. Der Mechanismus funktioniert nur dann, wenn sich alle Stationen gegenseitig empfangen können.

[»] Stellen Sie sich vor, dass drei Stationen im Abstand von jeweils 100 Metern voneinander aufgestellt werden, so dass die beiden äußeren Stationen 200 Meter entfernt sind und sich nicht gegenseitig empfangen können (siehe Abbildung 7.1). Möchten die Stationen A und C zu Station B senden, kann der CSMA/CA-Mechanismus keine Kol-

lisionen verhindern, weil Station A nicht feststellen kann, dass gleichzeitig Station C sendet, und daher das Medium als frei erkennt.

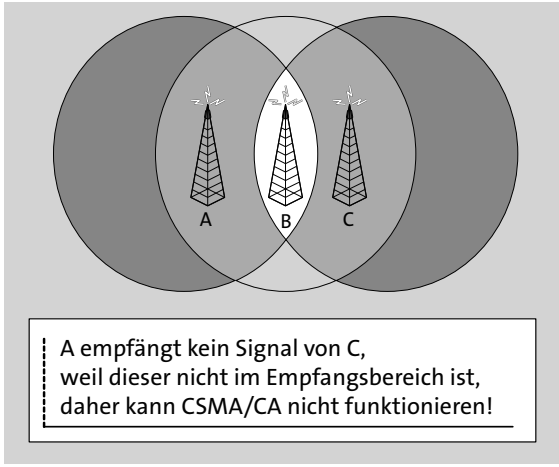



**Abbildung 7.1** CSMA/CA funktioniert hier nicht.

Es kann und wird bei WLANs also unvermeidbar zu Kollisionen kommen. Daher wurde schon auf dieser Protokollschicht – eigentlich wäre das Aufgabe von TCP – ein Sicherungsmechanismus implementiert. Gesendete Frames werden vom Empfänger durch ein *ACKnowledge* bestätigt. Kommt das ACK nicht, beginnt die Sendestation mit der Wiederholung (*Retransmission*) nach einer vorher definierten Zeit.

Bei sehr vielen WLAN-Clients an einem Access Point kann das CSMA/CA-Verfahren nicht mehr ordentlich durchgeführt werden. In diesem Fall wird *Request To Send* (*RTS*) angewendet, und ein WLAN-Client muss sich das Senderecht zuvor vom Access Point erteilen lassen.

WLANs bieten die Möglichkeit, Pakete zu fragmentieren, also zu zerteilen. Der Wert des *Fragmentation Thresholds* gibt an, wie viele Bytes ein Datenpaket groß sein muss, damit es fragmentiert wird. Die Fragmentierung von Paketen führt zu überflüssigen Kontrollinformationen und verschlechtert die Performance des WLAN-Zugangs. Sie sollten den Wert möglichst hoch setzen und nur dann nach unten verändern, wenn es zu defekten Datenpaketen oder Kommunikationsstörungen kommt.

Eine Regelung für das *Roaming*, also das Wandern zwischen verschiedenen Access Points, gab es lange Zeit gar nicht. Der Standard IEEE 802.11r aus dem Jahr 2008 ermöglicht heute ein sehr schnelles Roaming zwischen Access Points, das sogar den Ansprüchen der Telefonie genügt.

Andere Ungenauigkeiten führten dazu, dass zu Beginn der WLAN-Ära die Komponenten eines Herstellers mit denen anderer Hersteller häufig inkompatibel waren. Abhilfe

schaffte die *Wi-Fi Alliance* (siehe Abschnitt 7.12, »Wi-Fi Alliance«). Diese zertifiziert die Kompatibilität zwischen den beteiligten Herstellern durch das Wi-Fi-Zertifikat. Auf dieser Basis arbeiten heute die meisten WLAN-Komponenten verschiedener Hersteller problemlos zusammen.

Eine standardisierte Funktion von IEEE 802.11a/b/g/n ist es, eine niedrigere Datenrate auszuhandeln, wenn die Empfangsbedingungen schlechter werden. Die maximale Bandbreite kommt nur bei gutem Empfang zustande, wenn sich Sender und Empfänger in unmittelbarer Nähe zueinander befinden. Wenige Zentimeter entscheiden zum Schluss über den Empfang; man spricht auch vom *Link*. Zwischen den Herstellern gibt es massive Unterschiede, was die Sende- und Empfangsqualität angeht. Dabei ist Stahlbeton das größte Hindernis für Funkverbindungen. Es kommt beim Aufstellen eines Access Points deshalb auf die geschickte Standortwahl an, um den WLAN-Clients möglichst gute Datenraten bieten zu können (siehe Abschnitt 7.16, »Antennenausrichtung und Position«).

Mittels IEEE 802.11a/b/g/n lassen sich mit Richtfunkantennen auch längere Strecken überbrücken, wenn Sichtkontakt besteht. Möglich sind ein bis zwei Kilometer bei relativ geringen Datenraten. Diese Verbindung ist störanfällig bei Regen, Schnee, vorbeifliegenden Vögeln, Baukränen und ähnlichen Hindernissen.

## 7.2 IEEE 802.11b

Mit 11 Mbit/s bietet dieser Standard keine zeitgemäße Datenrate mehr. Die Geschwindigkeit ist für einige Anwendungen ausreichend, so z. B. für den normalen DSL-Internetzugang, doch für Multimedia, also z. B. einen Film, sind die 5 Mbit/s tatsächliche Datenrate einfach zu wenig.

Die Standards sind abwärtskompatibel. IEEE 802.11 beherrscht Datenraten von 1 oder 2 Mbit/s. IEEE 802.11b hat vier Bandbreitenstufen von 11, 5,5, 2 und 1 Mbit/s.

Die Firma Texas Instruments verwendete in ihren WLAN-Chips optional statt der üblichen DSSS- eine PBCC-Kodierung. Dieses Verfahren eignet sich auch für höhere Datenraten. Unter der Bezeichnung *11b+* wurden Geräte verkauft, die Geschwindigkeiten von 22 oder 44 Mbit/s unterstützten. Wenn Sie sowohl WLAN-Karten als auch einen Access Point einsetzen, der dieses unterstützt, spricht nichts dagegen, diese Geschwindigkeitserhöhung zu nutzen.

## 7.3 IEEE 802.11a/h

IEEE 802.11a/h bietet Bruttodatenraten von 54 Mbit/s, netto werden unter guten Bedingungen 20 Mbit/s erreicht. Bei diesem Standard wird ein anderes Frequenzband als bei IEEE 802.11b/g benutzt, es liegt im 5-GHz-Bereich. In den USA war das gewünschte Frequenzband vorher unbenutzt und konnte für WLANs verwendet werden. In Europa und auch in Deutschland waren gewisse Bereiche für Satelliten reserviert. Erst seit der Verabschiedung von IEEE 802.11h im September des Jahres 2003 kann der Standard sorgenfrei in Europa eingesetzt werden. Es handelt sich dabei um den gleichen Standard wie beim US-amerikanischen IEEE 802.11a, jedoch gibt es zwei Erweiterungen zur Frequenzwahl und Sendeleistung:

- *Dynamic Frequency Selection* (*DFS*): Ein benutzter Kanal wird erkannt und erzwingt einen Kanalwechsel.
- *Transmit Power Control* (*TPC*): Schutz anderer Funksysteme; mit implementiertem DFS darf jedoch wieder etwas stärker abgestrahlt werden.

IEEE 802.11a/h ist aufgrund des anderen Frequenzbands nicht mit den älteren oder anderen 802.11-Varianten abwärtskompatibel.

Das 5-GHz-Frequenzband ist frei von Störquellen, weil es ausschließlich für die drahtlose Datenkommunikation reserviert ist. Aufgrund von 19 Kanälen à 20 MHz ist es möglich, mehr WLAN-Clients bei höheren Datenraten anzubinden, als es bei IEEE 802.11b/g mit drei Kanälen möglich ist.

Ein Vergleich der Firma Intersil ergab, dass die Reichweite von 11a in Großraumbüroumgebungen – amerikanischer Büroeinsatz – schlechter ist als bei 11g. Diese Erfahrung kann ich auch für die deutsche Massivbauweise bestätigen; die Funkabdeckung ist hier wesentlich geringer.

## 7.4 IEEE 802.11g

Im Juni 2003 wurde 11g verabschiedet, die Übertragungsrate beträgt brutto 54 Mbit/s, in der Realität werden unter optimalen Bedingen etwa 20 Mbit/s als Nettodatendurchsatz erreicht. Es gibt keinen grundsätzlichen Unterschied zu 11b, außer dass es viermal so schnell ist. Daher gelten auch die unter 11b gemachten Aussagen.

Wie 11b verwendet auch 11g das ISM-Frequenzband bei 2,4 GHz, wodurch es keinerlei Probleme hinsichtlich der Freigabe durch die Bundesnetzagentur gab. 11g ist damit zudem abwärtskompatibel mit 11b, aber es wirken dadurch auch dieselben Störquellen, nämlich Mikrowellenherde und Bluetooth. Deutlich mehr störenden Einfluss als Mikrowellengeräte haben allerdings benachbarte WLANs.

## 7.5 IEEE 802.11n – WiFi 4

Der inzwischen auch unter dem Namen *Wi-Fi 4* bekannte Standard aus dem Jahr 2009 erfüllt folgende Ziele:

- Die auch als *Spatial Multiplexing* bekannte *MIMO*-Technik (siehe Abschnitt 7.13.5, »Multiple Input, Multiple Output«) steigert die Datenrate mit zwei, drei oder vier Antennen (2TX, 3TX oder 4TX) auf 150 Mbit/s pro Datenstrom.
  Beim Einsatz von zwei Antennen liegt die Bruttodatenrate bei bis zu 150 Mbit/s, bei vier Antennen bis zu 300 Mbit/s unter Verwendung von 20 MHz pro Kanal. Durch *Channel Bonding* (siehe Abschnitt 7.13, »Beschleunigertechniken«) kann die jeweils doppelte Datenrate – also max. 600 Mbit/s – erzielt werden, dazu werden zwei 20-MHz-Kanäle zusammengeschaltet.
- Der neue *High-Through-put-Modus* verwendet die Technik *Frame Bursting*.
- Mehrere Frames können zu einem größeren Frame zusammengeführt werden. Dadurch wird *Frame Aggregation* effektiver, und im Ergebnis werden höhere Nutzdatenraten erzielt.
- Durch Verbesserungen des Kodierungsverfahrens werden höhere Datenraten erzielt. So steigt die Datenrate durch den Einsatz von MIMO nicht auf 108, sondern auf 150 Mbit/s.

Abschnitt 7.13, »Beschleunigertechniken«, fasst die wichtigsten Beschleunigungsverfahren zusammen.

## 7.6 IEEE 802.11ac – WiFi 5

Der auch als *Wi-Fi 5* geläufige Standard für Gigabit-WLAN nach IEEE 802.11ac wurde im Dezember des Jahres 2013 verabschiedet. Dieser als *Wave 1* bezeichnete Standard mit einer theoretischen Bruttodatenrate von 1.300 Mbit/s wurde im Jahr 2016 mit dem Ergebnis *Wave 2* und theoretischen 2.167 Mbit/s überarbeitet. Netto ist in der Praxis maximal etwa die Hälfte der Bruttodatenrate zu erwarten.

Ein WLAN nach 11ac findet im 5-GHz-Band statt und muss dementsprechend – genauso wie IEEE 802.11a – die in Abschnitt 7.3, »IEEE 802.11a/h«, beschriebenen europäischen Normen DFS und TPC erfüllen. Die 11ac-Router sind abwärtskompatibel mit dem 11n-Standard.

Der Access Point verwendet beim Senden zum WLAN-Client *Multi-User MIMO* (siehe Abschnitt 7.13.6, »Multi-User MIMO«) mit bis zu drei (Wave 1) bzw. vier (Wave 2) Kanälen. Außerdem nutzt Wi-Fi 5 *Beamforming* (siehe Abschnitt 7.13.4, »Beamforming«).

## 7.7 IEEE 802.11ax – WiFi 6

Das *High Efficiency WLAN* wurde im Jahr 2018 normiert. Im Vergleich zum Vorgänger Wi-Fi 5 verdoppelt sich bei *Wi-Fi 6* nicht nur die Anzahl der für *Multi-User MIMO* (siehe Abschnitt 7.13.6, »Multi-User MIMO«) verwendeten Kanäle von 4 auf 8. Darüber hinaus kommt MU-MIMO jeweils in Sende- und Empfangsrichtung zum Einsatz. Dabei bedienen Access Points dieses Standards sowohl das 2,4-GHz-Band als auch das 5 GHz-Band. Geräte, die den Standard *Wi-Fi 6E* unterstützen, können zusätzlich das Frequenzband bei 6 GHz nutzen. Dieses Band ermöglicht hohe Datenraten auf kurze Entfernungen.

Das bei LTE (siehe Abschnitt 13.9, »LTE«) und WiMAX (siehe Abschnitt 13.11, »WiMAX«) bewährte Verfahren *Orthogonal Frequency-Division Multiple Access* (*OFDMA*) bildet die Datenübertragung mit Hilfe von – in Bezug auf Anzahl und Größe individuell an die jeweiligen Bedingungen anpassbaren – Unterkanälen ab. Diese *Resource Units* gruppieren die verfügbaren *Subcarrier*, in die ein Kanal von 20, 40, 80 oder 160 MHz Breite unterteilt ist.

Mit Hilfe des *Basic Service Set* (*BSS*) *Colorings* markieren Access Points ihren Datenverkehr eindeutig, wodurch jeder Empfänger im WLAN die Kommunikation seines Access Points von der Kommunikation anderer Access Points im gleichen Frequenzband leicht unterscheiden kann. Dadurch eignet sich WiFi 6 insbesondere für Orte, wo viele Access Points und Teilnehmer in räumlicher Nähe zueinander kommunizieren, z. B. auf Messen oder in Hotels.

Die Funktion *Target Wakeup Time* (*TWT*) kann Geräte des *Internet of Things* (*IoT*) für eine definierte Zeit in den Schlaf schicken. Das ermöglicht die Reduzierung des Stromverbrauchs WLAN-basierter Geräte im Smart Home (siehe Kapitel 49, »Hausautomation«).

## 7.8 IEEE 802.11be – WiFi 7

Zum Zeitpunkt der Drucklegung dieses Buches wird am *Extremely High Throughput WLAN* gearbeitet. Es gilt als sicher, dass die Nutzung des 6-GHz-Bandes neben dem 2,4-GHz-Band und dem 5-GHz-Band verpflichtend wird. Die Modulationsdichte könnte im Maximum auf QAM-4096 ansteigen (siehe Abschnitt 7.13.7, »Quadratur-Amplituden-Modulation«).

Während bei Wi-Fi 6 jeder WLAN-Client maximal einen Kanal in genau einem Band nutzen kann, könnte Wi-Fi 7 mit Hilfe von *Multi-Link-Operation* (*MLO*) die parallele Nutzung mehrerer Bänder ermöglichen. Ob Technologien wie *Multi Access*

*Point* (*Multi AP*), also die parallele Nutzung mehrerer Access Points mitsamt Lastverteilung, Einzug in den Standard erhalten, bleibt jedoch noch abzuwarten.

## 7.9 IEEE 802.11ad

Der Standard für 7-Gigabit-WLAN nach IEEE 802.11ad wurde im Jahr 2012 verabschiedet. Der Standard 11ad beschreibt WLAN im lizenzfreien 60-GHz-Band. Der Vorteil ist, dass die verfügbare Bandbreite in diesem Bereich relativ groß ist. Die Kanäle können dementsprechend breiter als im 2,4- oder 5-GHz-Band ausgestaltet werden, die Transferrate ist dementsprechend hoch.

Die Kehrseite der Medaille: Die Dämpfung ist bei Funk mit Wellenlängen im Millimeterbereich allein schon durch das Element Sauerstoff enorm groß; ein WLAN ist damit auf die Abmessungen einer kleinen Wohnung beschränkt. Optimalerweise besteht eine Sichtverbindung; eine normale Hauswand dürfte für 11ad bereits eine nicht zu bewältigende Herausforderung sein.

Das ist auf den ersten Blick ein großer Nachteil, muss es aber nicht zwangsläufig sein. Die gegenseitige Störung von benachbarten WLANs – bei 2,4- und 5-GHz-Netzen immer ein Thema – scheint im 60-GHz-Band sehr unwahrscheinlich.

Die Spezifikation leidet an Ungenauigkeiten[3] und konnte sich daher nicht durchsetzen. Die Hoffnungen ruhen nun auf dem Nachfolger IEEE 802.11ay.

## 7.10 IEEE 802.11ay

Die vier MIMO-Kanäle des 11ad-Nachfolgers ermöglichen auf kurze Distanz eine theoretische Übertragungsgeschwindigkeit von bis zu 176 Mbit/s. Damit eignet er sich z. B. für die drahtlose Übertragung der 3D-Inhalte von Multimedia und Spielen und auf eine *Virtual-Reality-Brille*.

## 7.11 IEEE 802.11e

IEEE 802.11e ist der Standard für die Priorisierung von Daten im WLAN. Sein Ziel ist es, den verschiedenen Bedürfnissen von Daten im WLAN besser gerecht zu werden.

In den meisten privaten Haushalten werden DECT-Telefone genutzt. Aus der Sicht eines Netzwerkers wird man in Zukunft diese Telefone durch WLAN-Telefone ersetzen. Dazu muss das WLAN selbstverständlich diese Daten ohne Zeitverzögerung transpor-

3 *https://www.elektronik-kompendium.de/sites/net/2112051.htm*

tieren, was insbesondere dann eine Herausforderung ist, wenn parallel zum WLAN-Telefonat noch ein Datendownload über WLAN transportiert werden muss.

Die Priorisierung von Daten innerhalb eines WLANs wird den Standard IEEE 802.11n ergänzen. Davon werden im Ergebnis sowohl Privatanwender als auch große Firmen profitieren.

## 7.12 Wi-Fi Alliance

Die Interoperabilität, also die Zusammenarbeit von Geräten verschiedener Hersteller, normiert und testet die *Wi-Fi Alliance*. Wi-Fi steht – in Anlehnung an Hi-Fi – für *Wireless Fidelity*. Es gibt ein eigenes Logo, das für interoperable Produkte vergeben wird (siehe Abbildung 7.2).


**Abbildung 7.2** Wi-Fi-Logo; Quelle: https://www.wi-fi.org

Wenn Sie Wireless-LAN-Produkte kaufen, sollten Sie Wert auf dieses Logo legen, denn nur dies garantiert Ihnen, dass das Gerät auch mit Geräten anderer Hersteller funktioniert. Welche Produkte mit welchen Eigenschaften zertifiziert sind, können Sie unter *https://www.wi-fi.org* nachschauen.

## 7.13 Beschleunigertechniken

Die bestehenden 54-Mbit-WLAN-Techniken sind seit vielen Jahren auf dem Markt, doch der Nachfolgestandard IEEE 802.11n ließ auf sich warten und wurde erst im Jahr 2009 endgültig verabschiedet. Um dem Bedürfnis insbesondere privater Kunden nach mehr Bandbreite im WLAN gerecht zu werden, setzen die Hersteller der WLAN-Chipsätze verschiedene Beschleunigungstechniken ein.

Diese können herstellerspezifisch sein und funktionieren dann nur bei Geräten mit dem gleichen WLAN-Chipsatz. Kaufen Sie daher passende Geräte eines Herstellers, um die volle Geschwindigkeit nutzen zu können, oder noch besser: Achten Sie auf die Zertifizierung durch die Wi-Fi Alliance.

[!]

### 7.13.1 Channel Bonding

Beim *Channel Bonding* werden einfach zwei Funkkanäle à 20 MHz gleichzeitig genutzt. Zusammen mit der Breite des Frequenzbandes verdoppelt sich die Datenrate. Diese Technik führt bei IEEE 802.11n und bei einigen herstellerspezifischen 802.11g-Varianten dazu, dass durch die benötigten 40 MHz bis zu neun der dreizehn Kanäle im 2,4-GHz-Band belegt werden. Nur so kann ausreichend Frequenzband zusammengeschaltet werden (siehe Tabelle 7.3 sowie Tabelle 7.5).

| primärer Kanal | sekundärer Kanal | blockierte Kanäle |
|---|---|---|
| 1 | 5 | 1 bis 7 |
| 2 | 6 | 1 bis 8 |
| 3 | 7 | 1 bis 9 |
| 4 | 8 | 2 bis 10 |
| 5 | 9 oder 1 | 3 bis 11 oder 1 bis 7 |
| 6 | 10 oder 2 | 4 bis 12 oder 1 bis 8 |
| 7 | 11 oder 3 | 5 bis 13 oder 1 bis 9 |
| 8 | 12 oder 4 | 6 bis 13 oder 2 bis 10 |
| 9 | 13 oder 5 | 7 bis 13 oder 3 bis 11 |
| 10 | 6 | 4 bis 12 |
| 11 | 7 | 5 bis 13 |
| 12 | 8 | 6 bis 13 |
| 13 | 9 | 7 bis 13 |

**Tabelle 7.3** Channel Bonding im 2,4-GHz-Band: Der sekundäre Kanal liegt 20 MHz über oder unter dem primären Kanal; Quelle: https://en.wikipedia.org/wiki/IEEE_802.11n-2009.

Zwei dieser WLANs in räumlicher Nähe zueinander schließen sich gegenseitig fast aus. Diese Technik ist im 2,4-GHz-Band in hohem Maße unsozial und mit der zunehmenden Verbreitung von WLANs in Städten immer weniger vereinbar. Mit IEEE 802.11n ist sie dennoch offiziell in das 2,4-GHz-Band eingeflossen. Im Gegensatz dazu beschränkt sich der Standard 802.11ac auf die 19 Funkkanäle im 5-GHz-Band.

### 7.13.2 Frame Bursting

Um den Nutzdatenanteil bei der Übertragung zu erhöhen, wird zwischen zwei Datenpaketen nicht die DIFS-Wartezeit eingehalten, sondern nur die kürzere für *ACKnowledge*-Bestätigungspakete (*ACK*) vorgesehene SIFS-Wartezeit. Der Vorteil liegt weniger in der gesparten Zeit als darin, den Funkkanal öfter belegen zu können (im Gegensatz zu anderen WLAN-Clients, die immer die DIFS-Wartezeit abwarten). Das Verfahren bringt also nur Vorteile, wenn mehrere WLAN-Clients auf einem Funkkanal arbeiten. Standardisiert wurde die Technik in IEEE 802.11e, dem Standard für Quality of Service bei WLAN.

### 7.13.3 Frame Aggregation

Ein WLAN-Frame darf bis zu 2.304 Bytes groß werden, ein Ethernet-Frame hingegen nur 1.518 Bytes (siehe Abschnitt 6.12, »Das Ethernet-Datagramm«). Bei Verwendung von *Frame Aggregation* werden mehrere Ethernet-Frames zusammengefasst und in einem überlangen WLAN-Frame übertragen.

Es existieren zwei Verfahren:

- *MAC Service Data Unit* (*MSDU*): Mehrere Ethernet-Frames werden in einen aggregierten MSDU-Frame mit einer Größe von bis zu 7.935 Bytes integriert.
- *MAC Protocol Data Unit* (*MPDU*): Die Ethernet-Frames werden einzeln in MPDU-Frames eingepackt und in Blöcken verschickt. Der Empfänger quittiert die empfangenen Blöcke, was bei einer hohen Fehlerrate in der Übertragung von Vorteil sein kann.

Da die umfangreichen Metainformationen der WLAN-Frames durch die Zusammenfassung nicht mehr so häufig übertragen werden müssen, erhöht sich die Nutzdatenrate zu Lasten des Overheads deutlich und steigt um ca. 30 Prozent.

### 7.13.4 Beamforming

Ein Access Point sendet grundsätzlich in alle Richtungen mit der gleichen Stärke – unabhängig davon, wo sich der Empfänger befindet, für den die Übertragung gedacht ist. Beamforming nutzt die Interferenzen mehrerer gleichzeitig sendender Antennen, um die Signalabstrahlung in Zielrichtung des Empfängers zu fokussieren.

Das rudimentär im Standard 802.11n (siehe Abschnitt 7.5, »IEEE 802.11n«) implementierte und letztlich im Standard 802.11ac (siehe Abschnitt 7.6, »IEEE 802.11ac«) normierte *Explicit Beamforming* testet die jeweils aktuellen Übertragungsbedingungen mit Hilfe spezieller Pakete.

Das nicht standardisierte *Implicit Beamforming* unternimmt den Versuch, den Empfänger anhand von verlorenen Paketen zu orten. Dadurch kann ein Access Point diese Art von Beamforming auch mit WLAN-Clients betreiben, die Explicit Beamforming nicht beherrschen.

Das Explicit Beamforming ist eine Grundlage für *Multi-User MIMO* (siehe Abschnitt 7.13.6, »Multi-User MIMO«).

### 7.13.5 Multiple Input, Multiple Output

Die MIMO-Technik ist für Nicht-Nachrichtentechniker schwierig zu verstehen. Ähnlich wie beim Channel Bonding wird gleichzeitig mehrfach gesendet, allerdings auf demselben Kanal.

*MIMO* steht für *Multiple Input, Multiple Output*. Übersetzt bedeutet dies etwa »mehrere rein, mehrere raus« und will ausdrücken, dass Daten parallel übertragen werden. Die Daten werden bei MIMO nicht auf getrennten Kanälen parallel übertragen, denn das wäre ja Channel Bonding, sondern parallel auf demselben Kanal. Auf einem WLAN-Kanal werden parallel bis zu vier Signale gleichzeitig ausgesendet.

Das Problem, das nun ohne weitere Maßnahmen auftritt, ist, dass sich die Signale untrennbar bereits beim Sender vermischen und der Empfänger mit diesem Signalbrei nichts anfangen kann. Die Entwickler von IEEE 802.11n haben sich also ein technisches Verfahren einfallen lassen, das auf Orthogonal Frequency-Division Multiplexing (OFDM) basiert. Dieses Verfahren verteilt ein Signal auf mehrere sogenannte *Subcarrier* (dt. *Unterträger*) und macht es damit widerstandsfähiger. MIMO nutzt neben der räumlichen Dimension der Unterkanäle nun noch eine zeitliche Dimension; die Unterkanäle werden zeitlich orthogonal versetzt, damit sich das Ausgangssignal beim Empfänger sauber wiederherstellen lässt.

Nun könnte man MIMO mit einer einzigen Antenne betreiben, allerdings müsste man dazu neue, schnelle Chips entwickeln, die in sehr großen Stückzahlen produziert werden müssten, damit man sie günstig verkaufen könnte. Das kostet Zeit und Geld. Die Alternative ist, einfach bestimmte Teile eines WLAN Access Points doppelt, dreifach oder vierfach einzubauen, und daraus resultieren Geräte mit mehreren Antennen. Der WLAN-Client wird auch zukünftig nur eine Antenne benötigen. Das zu erklären, würde tief in die Nachrichtentechnik führen, deshalb verzichte ich hier darauf.

Im Vergleich zum Multi-User MIMO wird dieses Verfahren auch als *Single-User MIMO* bezeichnet.

### 7.13.6 Multi-User MIMO

In einem normalen Haushalt – und damit auch in einem durchschnittlichen WLAN – müssen häufig mehrere Endgeräte parallel mit WLAN versorgt werden. Ein Access Point, der Multi-User MIMO (*MU-MIMO*) beherrscht, kann gleichzeitig mit mehreren Teilnehmern kommunizieren.

Jeder einzelne Anwender muss nicht so lange auf ein Signal warten, was die durchschnittliche Geschwindigkeit Ihres Netzwerks im Vergleich zum herkömmlichen Single-User MIMO (siehe Abschnitt 7.13.5, »Multiple Input, Multiple Output«) deutlich anhebt.

### 7.13.7 Quadratur-Amplituden-Modulation

Während eine klassische Funkübertragung auf einer Trägerwelle stattfindet, verwendet die *Quadratur-Amplituden-Modulation* (*QAM*) zwei sich überlagernde Trägerwellen, die jedoch – vergleichbar mit den Winkelfunktionen Sinus und Cosinus – um 90° verschoben sind. Die beiden Komponenten werden auch als *I-Signal* und *Q-Signal* bezeichnet. Durch die Überlagerung können in einem Frequenzband platzsparend mehrere Informationen zusammengefasst und gleichzeitig übertragen werden.

QAM-16 kann sechzehn verschiedene Zustände – auch als *Symbole* bezeichnet – übertragen (siehe Abbildung 7.3).

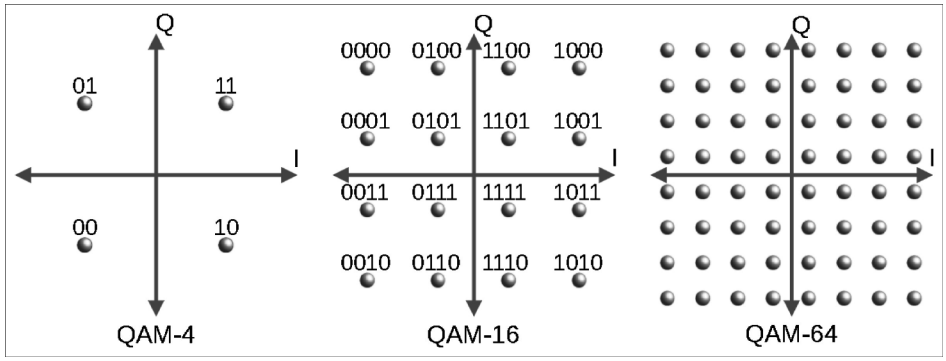



**Abbildung 7.3** QAM-4, QAM-16 und QAM-64 im Vergleich

Die Anzahl der gleichzeitig übertragbaren Bits hängt vom jeweils gewählten Verfahren ab (siehe Tabelle 7.4). Zusammen mit der Informationsdichte in den einzelnen Symbolen steigt auch die Anfälligkeit für Störungen, worunter auch die Reichweite leidet. Daher passt sich die in der Praxis verwendete Modulation in der Regel an die jeweiligen Übertragungsverhältnisse an.

| QAM Modulation | Bits pro Symbol | Anwendung in Standard |
|---|---|---|
| QAM-4 | 2 | |
| QAM-16 | 4 | |
| QAM-32 | 5 | |
| QAM-64 | 6 | IEEE 802.11a/h |
| QAM-256 | 8 | IEEE 802.11ac |
| QAM-1024 | 10 | IEEE 802.11ax |
| QAM-4096 | 12 | evtl. IEEE 802.11be |

**Tabelle 7.4** Effizienz und Verwendung der QAM-Verfahren

## 7.14 Kanalwahl

Die richtige Wahl des Kanals ist entscheidend für Ihr WLAN. Dabei macht es einen enormen Unterschied, ob Ihr WLAN im 2,4-GHz-Band oder im 5-GHz-Band funkt. Die Problematik wird sich absehbar durch das *Basic Service Set* (*BSS*) *Coloring* (siehe Abschnitt 7.7, »IEEE 802.11ax – WiFi 6«) entspannen.

### 7.14.1 2,4-GHz-Band

In Europa kann im ISM-Band aus 13 Kanälen ausgewählt werden, die jeweils einen Abstand von 5 MHz haben. Da jeder Funkkanal etwas mehr als 20 MHz belegt, stören sich nebeneinanderliegende Funkkanäle gegenseitig. Bei WLAN-Geräten, die für den internationalen Einsatz vorgesehen sind, werden oftmals nur die Kanäle 1 bis 11 genutzt – in den USA dürfen die Kanäle 12 und 13 nicht verwendet werden –, so dass es nur drei überlappungsfreie Kanäle gibt: Kanal 1, 6 und 11 (siehe Tabelle 7.5).

Wenn Sie ein WLAN aufbauen möchten, dann ist es sehr sinnvoll, einen Kanal zu wählen, der fünf Kanäle von allen Nachbar-WLANs entfernt ist. Die einzelnen Kanäle eines WLANs im 2,4-GHz-Frequenzband sind lediglich 5 MHz auseinander, aber 22 MHz breit. Aus diesem Grund sollte der Abstand zu WLANs von Nachbarn fünf Kanäle betragen. Nur so sind die Frequenzen der WLANs überlappungsfrei und stören sich nicht gegenseitig. Nutzen Sie ausschließlich die Kanäle 1, 6 oder 11.

Verhalten sich Ihre Nachbarn auf dieselbe Weise, können Sie gegenseitige Störungen sehr einfach minimieren. Ein störendes Nachbar-WLAN kann die Leistung Ihres WLANs erheblich beeinflussen, und die Leistung sinkt dann sehr deutlich. Daher sollten Sie den Kanal Ihres WLANs gezielt aussuchen. Ist eine überschneidungsfreie Kanalwahl nicht möglich, sollten Sie möglichst schwache andere WLANs überlappen lassen. Hilft auch das nicht, kann ein WLAN nach IEEE 802.11n und damit verbunden ein Wechsel in das 5-GHz-Band die Lösung sein.

Die Besonderheiten, die sich aus der parallelen Nutzung mehrerer Funkkanäle für den Standard IEEE 802.11n ergeben, beschreibe ich in Abschnitt 7.13.1, »Channel Bonding«.

Das Programm inSSIDer (*http://www.metageek.net/products/inssider*) zeigt Ihnen verfügbare WLANs mit Kanal an; so können Sie Nachbar-WLANs aufspüren und Ihre eigene Konfiguration danach richten. Es gibt *Wi-Fi-Finder* oder auch *WLAN Detector* genannte Geräte, die WLAN-Signale melden. Die einfachsten mit einigen LEDs zur Anzeige des Ergebnisses gibt es schon für unter 20 €. Komfortablere Geräte, die auch die SSID und die Verschlüsselungsart anzeigen, kosten ca. 60 €.

| Kanal | Frequenzmitte in GHz | überlappungsfrei mit Kanal |
|---|---|---|
| 1 | 2,412 | 6 bis 13 |
| 2 | 2,417 | 7 bis 13 |
| 3 | 2,422 | 8 bis 13 |
| 4 | 2,427 | 9 bis 13 |
| 5 | 2,432 | 10 bis 13 |
| 6 | 2,437 | 1 und 11 bis 13 |
| 7 | 2,442 | 1 bis 2 und 12 bis 13 |
| 8 | 2,447 | 1 bis 3 und 13 |
| 9 | 2,452 | 1 bis 4 |
| 10 | 2,457 | 1 bis 5 |
| 11 | 2,462 | 1 bis 6 |
| 12 | 2,467 | 1 bis 7 |
| 13 | 2,472 | 1 bis 8 |

**Tabelle 7.5** Funkkanäle im ISM-Band: Jeder Kanal belegt 22 MHz.

Beide Verfahren, 11a und g, ermöglichen die höheren Datenraten bei vergleichbarer Sendeleistung gegenüber 11b durch den Einsatz von Orthogonal Frequency-Division Multiplexing (OFDM). Durch diese Kodierungsverfahren wird insbesondere eine höhere Widerstandsfähigkeit gegenüber Störquellen erreicht.

### 7.14.2 5-GHz-Band

Aus dem 5-GHz-Band sind in Europa die drei Unterbänder *UNII-1* (5.150 MHz bis 5.250 MHz), *UNII-2* (5.250 MHz bis 5.350 MHz) und *UNII-2 Extended* (5.470 MHz bis 5.725 MHz) nutzbar.

Die Nutzung der Kanäle des Unterbandes UNII-1 (siehe Tabelle 7.6) ist nur im Innenbereich erlaubt. TPC und DFS sind in diesem Subband nicht vorgeschrieben. Die maximale Sendeleistung beträgt 200 mW.

| Kanal | Frequenzmitte in GHz | Frequenzspektrum in GHz |
|---|---|---|
| 36 | 5,180 | 5,170–5,190 |
| 40 | 5,200 | 5,190–5,210 |
| 44 | 5,220 | 5,210–5,230 |
| 48 | 5,240 | 5,230–5,250 |

**Tabelle 7.6** Das Unterband UNII-1

Auch das Unterband UNII-2 (siehe Tabelle 7.7) ist nur im Innenbereich erlaubt. DFS ist zwingend erforderlich, bei Verwendung von TPC darf anstatt mit 100 mW mit 200 mW gesendet werden.

| Kanal | Frequenzmitte in GHz | Frequenzspektrum in GHz |
|---|---|---|
| 52 | 5,260 | 5,250–5,270 |
| 56 | 5,280 | 5,270–5,290 |
| 60 | 5,300 | 5,290–5,310 |
| 64 | 5,320 | 5,310–5,330 |

**Tabelle 7.7** Das Unterband UNII-2

Die Nutzung des Unterbandes UNII-2 Extended (siehe Tabelle 7.8) ist sowohl im Innen- als auch im Außenbereich erlaubt. DFS ist zwingend zu verwenden, mit TPC steigt die maximale Sendeleistung von 500 mW auf 1.000 mW.

DFS wird z. B. in einer FRITZ!Box so implementiert, dass der Router nach einem Neustart oder einer Konfigurationsänderung zehn Minuten lang das Frequenzband überwacht, bevor WLAN-Clients sich anmelden können. Wird erst später im Betrieb die mögliche Störung eines Primärnutzers wie dem Militär, Wetterradarsystemen oder der Flugsicherung erkannt, wird auch dann ein automatischer Kanalwechsel durchgeführt, wenn der Kanal fest konfiguriert wurde.[4]

| Kanal | Frequenzmitte in GHz | Frequenzspektrum in GHz |
|---|---|---|
| 100 | 5,500 | 5,490–5,510 |
| 104 | 5,520 | 5,510–5,530 |
| 108 | 5,540 | 5,530–5,550 |
| 112 | 5,560 | 5,550–5,570 |
| 116 | 5,580 | 5,570–5,590 |
| 120 | 5,600 | 5,590–5,610 |
| 124 | 5,620 | 5,610–5,630 |
| 128 | 5,640 | 5,630–5,650 |
| 132 | 5,660 | 5,650–5,670 |
| 136 | 5,680 | 5,670–5,690 |
| 140 | 5,700 | 5,690–5,710 |

**Tabelle 7.8** Das Unterband UNII-2 Extended

Da die Implementierung von TPC und DFS relativ aufwendig ist, bilden einige Hersteller die Unterbänder UNII-2 und UNII-2 Extended in ihren WLAN-Komponenten nicht ab. Die alleinige Unterstützung der vier Kanäle im Band UNII-1 darf meiner Meinung nach eigentlich nicht zu der Aussage führen, ein Router oder Access Point decke das 5-GHz-Band ab. In der Praxis habe ich leider erleben müssen, dass die Hersteller preisgünstigerer Hardware dies manchmal ganz anders sehen.

4 *https://avm.de/service/wissensdatenbank/dok/FRITZ-Box-7583/3599_DFS-Wartezeit-oder-Radarerkennung-trotz-Kanal-36-48*

## 7.15 Sendeleistung

Grundsätzlich sollten Sie die Sendeleistung Ihres eigenen WLANs so gering wie möglich halten. Dadurch können weniger potentielle Hacker das Signal Ihres WLANs empfangen. Außerdem reduziert eine Anpassung der Sendeleistung an das benötigte Maß die Gefahr der unnötigen Störung eines Nachbar-WLANs erheblich.

Bei schlechten Empfangsbedingungen – z. B. aufgrund von Überlappungen des eigenen Funkkanals mit dem eines benachbarten WLANs – kann eine schwache Sendeleistung des Access Points zu niedrigeren Datenraten führen. Im ersten Schritt empfehle ich eine Aufteilung und Ausnutzung aller Frequenzen im 2,4-GHz- und 5-GHz-Band in Kooperation mit den Betreibern aller benachbarten WLANs. Ist die Reichweite eines WLANs im 5-GHz-Band ausreichend, sollte diesem Band regelmäßig der Vorzug vor dem 2,4-GHz-Band gegeben werden, damit benachbarte WLANs weniger gestört werden müssen.

Ist es absolut nicht möglich, einen überlappungsfreien Funkkanal zu finden, hilft oftmals die Regulierung der Sendeleistung. Sie können die anderen Betreiber der WLANs bitten – vorausgesetzt, Sie kennen sie –, die Sendeleistung der einzelnen WLANs zu verringern, so dass deren individuelle Reichweite und damit auch der jeweils gegenseitig störende Einfluss geringer wird.

[!] Leider ist es nicht bei jedem Access Point möglich, die Sendeleistung einzustellen.

Sollte die Sendeleistung zur Abdeckung Ihres Grundstücks noch nicht ausreichen, gibt es drei weitere Möglichkeiten:

- Verstärker
- Antennen
- Repeater

[!] Der Einsatz von Verstärkern oder anderen Antennen dient zur Steigerung der Reichweite. Der Einsatz ist nicht ganz unproblematisch, weil die Sendeleistung von 100 mW EIRP nicht überschritten werden darf. Diese ergibt sich aus der reinen Sendeleistung zuzüglich Kabel und Antenne. Beim Einsatz von Verstärkern und/oder anderen Antennen passiert es leicht, dass Sie mit dem Betrieb Ihres WLANs die zulässige Höchstgrenze von 100 mW/20 dBm überschreiten. Das ist jedoch nicht zulässig.

[»] Sie finden viele Anbieter von Austauschantennen im Internet. Einige sind auf einzelne Router oder Hersteller spezialisiert. Die Firma *FRIXTENDER* (*https://frixtender.de*) verspricht eine Verbesserung der Reichweite mit externen Antennen bei diversen FRITZ!Boxen und Speedport-Routern. Dieses geschieht trotz einer Öffnung des Routergehäuses nach Angaben der Firma ohne Verlust der Herstellergarantie. Ein Anten-

nenset an meiner FRITZ!Box führte tatsächlich zu einer Verbesserung der Leistung. Von den maximal in Aussicht gestellten 7 dBi Gewinn habe ich in meinen Tests durchschnittlich 4 dBi gemessen.

WLAN-Repeater sind in ihrer Wirkungsweise mit Hubs vergleichbar, ihren veralteten kabelgebundenen Verwandten (siehe Abschnitt 6.9, »Hub«). Sie geben ein empfangenes Signal verstärkt wieder aus. Sie haben die Wahl zwischen dedizierten Geräten für diesen Einsatz und normalen Access Points, die diese Funktion[5] häufig als Option anbieten. Doch Vorsicht: Jeder Repeater halbiert den Datendurchsatz in der Funkzelle, weil er jeden Frame wiederholt und dadurch Sendezeit auf dem Funkkanal belegt. Eine Ausnahme bilden *Cross-Band-Repeater* (siehe Abschnitt 7.20, »WLAN-Mesh«).

## 7.16 Antennenausrichtung und Position

Ähnlich wie bei der Erhöhung der Sendeleistung geht es bei der optimierten Ausrichtung des elektromagnetischen Feldes auf den Kommunikationspartner um die Verbesserung der Empfangsbedingungen. Daher kann ein Geschwindigkeitsgewinn nur für die Anwender möglich sein, die bisher noch nicht die volle Geschwindigkeit nutzen konnten.

Stabantennen strahlen rechtwinklig ab. Die theoretisch ideale Verbindung zwischen Sender und Empfänger besteht also, wenn die beiden räumlich parallel zueinander stehen. Je länger die Antenne, desto geringer der Abstrahlwinkel, und umgekehrt. Wollen Sie also mehrere Stockwerke mit einer Antenne abdecken, ist eine kurze Antenne vielleicht die bessere Wahl.

Der Standort für den Access Point ist natürlich abhängig von vielen Faktoren, nicht zuletzt von der örtlichen Versorgung mit Kabeln und der Ästhetik. Grundsätzlich eignet sich ein zentraler Punkt jedoch besser als die Ecke eines Raumes. Eine höhere Position im Raum kann außerdem zu einer insgesamt besseren elektromagnetischen Ausstrahlung eines Gebäudes führen.

## 7.17 Sicherheit von WLANs

Ein WLAN ist in besonderer Weise anfällig, da im Gegensatz zu kabelgebundenen Netzwerken durch die Funkübertragung jede Station in Reichweite eine potentielle Gefahr darstellt. Beachten Sie unbedingt die Hinweise zur Sicherheit Ihres WLANs in Kapitel 35, »WLAN und Sicherheit«!

5 Die Funktion heißt bei einigen Routern WLAN-Bridge oder WDS.

## 7.18 Hot Spots

Weltweit nimmt die Anzahl der sogenannten *Hot Spots* stark zu. Bei einem Hot Spot handelt es sich um einen öffentlichen Wireless-LAN-Zugang, der meist einen Internetzugang ermöglicht. In vielen Cafés der Kette Starbucks wurden weltweit Hot Spots installiert, in Flughäfen und Hotels sollen Geschäftsreisende ihre Aufenthaltszeit besser nutzen können.

### 7.18.1 FON

Die *Fonero* genannten Mitglieder der *Wi-Fi-Community* der Firma *FON* (siehe *http://www.fon.com*) teilen ihren Internetzugang mit anderen Foneros. Mit dem speziellen WLAN-Router *La Fonera* auf Basis einer bekannten Firmware (siehe Abschnitt 38.2, »OpenWrt – ein freies Betriebssystem für Router«) kann jeder die Verbindung der anderen mitnutzen.

Die Deutsche Telekom bietet in Kooperation mit FON das Produkt *WLAN TO GO* an. Dabei teilen Telekom-Kunden ihren DSL-Zugang mit Telekom-Nutzern und Foneros. Dafür können sie im Gegenzug mit ihren Zugangsdaten deren Anschlüsse mitnutzen. Obwohl die Router von AVM ab der Firmwareversion 6.20 die Spezifikation 802.11u und damit die Voraussetzungen für Hotspot 2.0/Passpoint erfüllen, lässt die Telekom für WLAN TO GO aktuell nur wenige Speedport-Modelle zu. Im Internet finden Sie auf der Seite *http://www.t-mobile.de/netzausbau* neben der Abdeckung mit mobilem Internet auch die Orte, an denen ein WLAN TO GO zur Verfügung steht. Da neue Standards für den Mobilfunk deutlich höhere Datenraten erlauben und sich damit die Lastsituation in den Netzen etwas entspannt (siehe Kapitel 13, »Kabelloser Internetzugang«), entfernt die Telekom die Funktion nach und nach aus der Firmware ihrer Internetrouter.

### 7.18.2 Freifunk

Das dezentral organisierte Projekt *Freifunk* basiert ebenfalls auf OpenWrt. Jeder Teilnehmer stellt seinen Router für den Datenverkehr der anderen zur Verfügung. Ob sich in Ihrer Umgebung ein Hot Spot oder eine lokale Gruppe befindet, der Sie sich anschließen können und die Ihnen bei der Einrichtung Ihres Routers hilft, erfahren Sie z. B. auf der Seite *http://www.freifunk-karte.de* im Internet. In der Schweiz gibt es unter dem Namen *Openwireless* (*https://wiki.freifunk.net/Openwireless*) ein artverwandtes Projekt, der Verein *FunkFeuer* (*http://www.funkfeuer.at*) ist in Österreich aktiv.

Es ist etwas schwer zu sagen, was Freifunk ist. Unter dem Begriff fasst man Menschen und Technik zusammen, die sich für freie Netzwerke einsetzen bzw. damit experimentieren. Es gibt keine übergeordnete Organisation oder einen, der sagt, wo es langgeht.

Freifunk ist sehr anarchisch, was es für Neulinge in dem Thema sehr undurchsichtig macht. Heute interessieren sich die Nutzer fast ausschließlich für den über Freifunk bereitgestellten Internetzugang. Das eigentliche Ziel von Freifunk ist aber eher, ein eigenes, dezentrales Netz aufzubauen und in diesem selbst Dienste anzubieten.

Die Politik kann diese *Bürgernetze* fördern, indem sie den Freifunkern Zugang zu den Dächern öffentlicher Gebäude gewährt. Gleichzeitig bedrohen die *Störerhaftung* – also die eventuelle Haftung des Anbieters für Rechtsverstöße Dritter – und drohende Vorschriften zur anlasslosen Vorratsdatenspeicherung die Zukunft der freien Funknetze. Meist auf Ebene einer Stadt oder eines Stadtteils schließen sich Leute zusammen, die sich dort um Freifunk kümmern wollen. In einigen Fällen gründen diese einen eingetragenen Verein, meist ist es aber ein eher loser Zusammenschluss. Wenn Sie sich mit Freifunk beschäftigen wollen, müssen Sie die für Ihren Ort zuständige Community ausfindig machen.


**Abbildung 7.4** Das Logo von Freifunk

Die nächste Ebene ist die *Freifunk-Domäne*, eventuell auch Sub-Domäne. Eine Domäne betreibt Technik und stellt Software für die Freifunk-Router bereit. Jede Community gehört zu genau einer Domäne. *Freifunk-Vereine* betreiben mit dem Übergang ins Internet einerseits Technik, bringen sich häufig aber auch in die politische Diskussion ein oder stellen Logos und Werbematerial bereit. Der Internetauftritt *https://www.freifunk.net* wird ebenfalls von einem Freifunk-Verein betrieben.

Die ursprüngliche Idee war, dass wir uns alle einen billigen *Freifunk-Router* ins Fenster stellen, der sich auch in das Mesh-Netzwerk (siehe Abschnitt 7.20, »WLAN-Mesh«) unserer Community verbindet. So wären alle Nachbarn miteinander verbunden und könnten auch noch über dieses Netzwerk kommunizieren, wenn alle Internetprovider ihre Dienste abschalten würden. Bisher ist diese Idee nicht Wirklichkeit geworden, und sie würde vermutlich auch technisch nicht funktionieren.

Grundsätzlich funktioniert Freifunk so, dass der als *Freifunk-Node* bezeichnete Freifunk-Router einen Tunnel zu einem als *Freifunk-Gateway* oder *Supernode* bezeichneten Server der Domäne im Internet aufbaut. Vergleichbar mit DS-Lite (sie-

he Abschnitt 14.7.6, »DS-Lite«) bekommt jeder Teilnehmer im Freifunknetz eine private IPv4- und eine globale IPv6-Adresse. Alle Teilnehmer und Nodes einer Domäne befinden sich in einem IP-Subnetz. Obwohl die Störerhaftung entfallen ist, wird der Internetverkehr mittels VPN-Tunneln zu einem Internetexit beispielsweise beim Freifunk Rheinland geleitet.

Auch nach dem Wegfall der rechtlichen Hürden in Deutschland bietet Ihnen Freifunk eine relativ einfache und sichere Möglichkeit, Ihr internes Netz vor den Gästen zu schützen. Surfen die Gäste über Freifunk, landet alles in einem Tunnel Richtung Supernode. Der Zugriff auf interne, eigene Geräte des Internetspenders ist nicht möglich, da alles im Tunnel gekapselt ist. Ein weiterer Vorteil ist, dass die Gäste mit einer IP der Domäne im Internet unterwegs sind. Es ist nicht nachvollziehbar, über welchen Freifunk-Router sie surfen.

Ein weiterer großer Vorteil sind die freiwilligen Freifunker. Sie planen und unterstützen in der Regel unentgeltlich, wo Netzwerkexperten für dieselbe Tätigkeit einen ordentlichen Stundenlohn in Rechnung stellen würden. Für die Nutzer ist Freifunk sehr angenehm. Es bedarf keines WPA-Passwortes, es handelt sich einfach um ein offenes WLAN. Einmal die SSID FREIFUNK im Smartphone als WLAN ausgewählt, nutzt das Smartphone Freifunk automatisch in jeder Kneipe, in der es verfügbar ist.

[!] Aus Sicherheitsgründen empfehle ich Ihnen, über das Freifunk-Netzwerk immer einen VPN-Tunnel zu Ihrem Router aufzubauen (siehe Kapitel 37, »Virtual Private Network«) und diesen für sämtliche Kommunikation mit dem Internet zu nutzen.

## 7.19 WLAN-Direktverbindungen

Mit *Wi-Fi Direct* bauen Sie eine direkte WLAN-Verbindung zwischen zwei oder mehr Teilnehmern auf. Einer der Teilnehmer wird dabei zum Access Point und muss den Standard Wi-Fi Direct unterstützen. Die anderen Teilnehmer melden sich an diesem Access Point an. Auf der dadurch entstehenden Verbindung setzen dann Protokolle wie *Miracast* (siehe Kapitel 46, »Streaming Media«) auf.

Der Nachteil von Wi-Fi Direct ist, dass eine bestehende WLAN-Verbindung der WLAN-Schnittstelle am Mobilgerät für die Wi-Fi-Direct-Verbindung getrennt werden muss.

## 7.20 WLAN-Mesh

Zur Abdeckung mehrerer Räume oder mehrerer Etagen sind in der Regel auch mehrere Access Points nötig. In einer klassischen WLAN-Infrastruktur belegen die ausgestrahlten WLANs mehrere Kanäle oder stören sich gegenseitig. Ein Client muss bei

schlechter Verbindung zum Access Point selbständig einen Wechsel auf ein anderes Band – also z. B. vom 5-GHz-Band zum 2,4-GHz-Band – oder zu einem anderen Access Point initiieren. Wenn der Wechsel des Bandes vom Access Point initiiert wird, nennt die Firma AVM dieses Verfahren *Band Steering*.

Da die Access Points häufig nicht mit Netzwerkkabeln am LAN angeschlossen sind, wird anstelle eines zusätzlichen Access Points oft ein WLAN-Repeater eingesetzt. Ein solcher empfängt das Signal und gibt es verstärkt wieder aus, was die Sendezeit verdoppelt und damit die Geschwindigkeit halbiert. Nur *Cross-Band-Repeater* übersetzen das Signal, z. B. vom 2,4-GHz-Band auf das 5-GHz-Band.

In jedem Fall liegt einem klassischen WLAN eine sternförmige, hierarchische Struktur zugrunde. Der Ausfall des Access Points ist gleichbedeutend mit dem Ausfall des gesamten WLANs. Beim *WLAN-Mesh* nach IEEE 802.11s hingegen wandert die Intelligenz von einem zentralen Access Point in einen dezentralen Aufbau hinein, was völlig neue Möglichkeiten eröffnet und die Definition einiger Begriffe notwendig macht.

- *Mesh-Knoten*: Bilden mit anderen Mesh-Knoten ein Mesh-Netzwerk. Sollte ein Knoten ausfallen, bemerkt dies das Netzwerk und sucht sich einen alternativen Weg über andere Knoten.
- *Mesh Access Point*: Mesh-Knoten und gleichzeitig ein herkömmlicher WLAN-AP für Teilnehmer, die nicht vollwertiger Teil des Mesh-Netzwerks sein können oder sein wollen
- *Mesh-Portal*: Mesh-Knoten und gleichzeitig Verbindungsglied zu einem anderen Netzwerk

Es wird grundsätzlich zwischen zwei Arten von Mesh-Netzwerken unterschieden.

- *Infrastruktur-Mesh*: Nur einzelne Mesh-Knoten – in der Regel Mesh Access Points und Mesh-Portale – dürfen Mesh-Knoten sein. Diese marktgängige Variante wird meist als proprietäres Produkt angeboten.
- *Client-Mesh*: Jeder Client ist gleichzeitig vollwertiger Mesh-Knoten und erhöht dadurch Stabilität und Reichweite des gesamten Mesh-Netzwerkes.

Mesh-Systeme verwenden immer ein separates *Backbone* auf einem eigenen Kanal, weshalb Mesh-Knoten in der Regel mit Hilfe mehrerer Antennen die anderenfalls – vergleichbar wie beim WLAN-Repeater – drohende Halbierung der Geschwindigkeit verhindern. Der Backbone-Kanal dient – in der Regel – ausschließlich der autonomen Konfiguration des Mesh-Netzwerks und der Synchronisation der Teilnehmer.

Das Routing der Datenpakete innerhalb des Mesh-Netzwerks zum Ziel findet nicht wie bei IP (siehe Kapitel 14, »Das Internetprotokoll«) auf Layer 3, sondern auf Layer 2 (siehe Kapitel 6, »Ethernet«) des ISO/OSI-Modells (siehe Abschnitt 5.2, »ISO/OSI-Modell«) statt. Mit Hilfe des MAC-Routings versucht das Netzwerk selbständig, für alle Daten-

ströme den effizientesten Weg zu finden und gleichzeitig möglichst wenige Teilnehmer des Mesh-Netzwerks unnötig zu belasten.

Um jedem Client den richtigen Access Point zuzuweisen, verwendet das Mesh-Netzwerk verschiedene Standards für das Management der WLAN-Clients und das Roaming zwischen Access Points. In der Praxis ist das nicht so einfach, denn die wenigsten Nutzer achten beim Kauf ihres Mobilgerätes darauf, welche Standards von ihrem Gerät und dem jeweils installierten Betriebssystem unterstützt werden.

- IEEE 802.11k: Der *Neighbor Report* stellt eine Liste mit Kanälen zur Verfügung, die als Roamingzielpunkt dienen könnten.
- IEEE 802.11v: Das *BSS Transition Management* empfiehlt dem Client einen anderen Access Point.
- IEEE 802.11r: *Fast BSS Transition* verkürzt die Zeit für die Authentifizierung am Access Point während eines Roamingvorganges.

Ob nun *Google Wifi*, *Netgear Orbi*, *TP-Link Deco* oder ein anderes Mesh-System für Sie das am besten geeignete ist, finden Sie heraus, indem Sie Ihre Anforderungen aufnehmen und genau mit den durchaus unterschiedlichen Leistungen der Anbieter abgleichen.

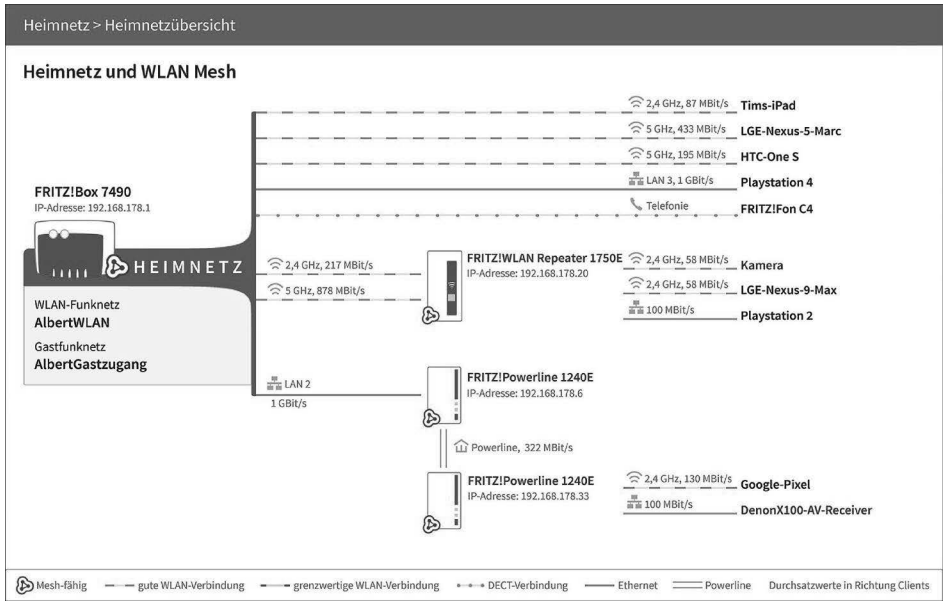



**Abbildung 7.5** Alle Clients werden im WLAN-Mesh verwaltet; Quelle: http://avm.de.

Dabei sollten Sie auch berücksichtigen, wie Sie vorhandene Infrastruktur weiterverwenden können. Die Firma AVM integriert z. B. die Produkte *FRITZ!Powerline* und *FRITZ!WLAN-Repeater* (siehe Abbildung 7.5).

Die Hersteller suggerieren, ein Mesh-WLAN sei einfacher aufzubauen als ein klassisches WLAN. Diese Einschätzung teile ich nicht in jedem Fall.

## 7.21 Abgrenzung zu anderer drahtloser Kommunikation

Drahtlose Netzwerke werden häufig verwechselt. WLAN, Bluetooth und NFC sind aber schon allein aufgrund der Reichweite nicht austauschbar.

Mit Bluetooth verbinden Sie Geräte in unmittelbarer Nähe. Der Name *Near-Field Communication* untertreibt, denn die Reichweite beträgt nur wenige Zentimeter.

### 7.21.1 Bluetooth

Der Name *Bluetooth* leitet sich ab vom dänischen König Harald Blauzahn. Dieser der Sage nach sehr kommunikationsfreudige Herrscher vereinte in seiner Regentschaft mehrere kleine skandinavische Fürstentümer zu einem Königreich.

Bluetooth ist ein Standard nach IEEE 802.15 für den Kurzstreckenfunk im ISM-Funkband bei 2,4 GHz. Er ist für die Versorgung von Headsets, Tastaturen, Mäusen und ähnlichem Zubehör gedacht. Man spricht in diesem Zusammenhang auch von einem *Personal Area Network* (*PAN*).

Der Bluetooth-Standard kennt mehrere Versionen:

- *Bluetooth 1.0* und *Bluetooth 1.1* kommen im sogenannten *Basic-Rate-Modus* nicht über eine Geschwindigkeit von 723,3 Kbit/s hinaus.
- Mit *Bluetooth 1.2* erhöht sich die Übertragungsrate auf maximal 1 Mbit/s.
- *Bluetooth 2.0+EDR* und *Bluetooth 2.1+EDR* beherrschen Datenraten von maximal 2.196,6 Kbit/s, verdreifachen also die ursprüngliche Datenrate. *EDR* steht dabei für *Enhanced Data Rate* (dt. *verbesserte Datenrate*). Dabei spart die schnellere Übertragung zusätzlich Energie, weil für die gleiche Datenmenge weniger lang gefunkt werden muss.
- *Bluetooth 3.0* kann vorübergehend in einen optionalen WLAN-Modus schalten und die maximalen Datenraten denen von WLAN anpassen.
- Mit der Version 4.0 wurde *Bluetooth Low Energy* (*LE*) als besonders stromsparende Bluetooth-Variante in den Standard integriert. Dieser Standard wird nicht zuletzt wegen seiner Verwendung in Smartphones und anderen mobilen Geräten auch als *Bluetooth Smart* bezeichnet. Die Standards *Bluetooth 4.0*, *Bluetooth 4.1*

und *Bluetooth 4.2* sind aufgrund der eingeführten AES-Verschlüsselung nicht abwärtskompatibel. Bluetooth LE führt mit den *Beacons* außerdem eine Möglichkeit ein, in der Nähe befindlichen mobilen Geräten per *Advertising*, einer Art von Broadcast, eine Nachricht zukommen zu lassen, was unter anderem Anwendungen wie Indoor-Navigation ermöglicht. Unter Bluetooth 4 ist die Größe der Nachrichten auf 31 Bytes beschränkt.

- *Bluetooth 5* bietet entweder mehr Datendurchsatz oder mehr Reichweite, was durch die Erhöhung der Sendeleistung von 10 mW auf 100 mW ermöglicht wird. Sensoren (siehe Kapitel 49, »Hausautomation«) und *Wearables*, also z. B. Fitnessarmbänder, können über Advertising nun Nachrichten mit einer Größe von 255 Bytes verteilen.

Geräte, die sowohl das klassische Bluetooth als auch Bluetooth LE unterstützen, werden als *Bluetooth Smart Ready* bezeichnet.

Bluetooth-Geräte werden anhand ihrer Sendeleistung in drei Klassen unterteilt:

- Klasse 1: Sendeleistung 10 bis 100 mW, Reichweite bis 100 Meter
- Klasse 2: Sendeleistung 0,01 bis 2,5 mW, Reichweite bis 50 Meter
- Klasse 3: Sendeleistung 0,01 mW, Reichweite bis 10 Meter

Dabei hat die Klasse nichts mit der Datenrate zu tun, sondern eher mit dem vorgesehenen Anwendungsfall. In ein Mobiltelefon wird Bluetooth der Klasse 1 integriert, weil dies z. B. den drahtlosen Abgleich mit dem PC ermöglicht und dabei aber nur 1 mW an Sendeleistung benötigt. Bei der Vernetzung von PCs spielt Bluetooth keine gewichtige Rolle, weil die Bandbreite zu gering ist. Weitere Informationen finden Sie im Internet auf der Seite *http://www.bluetooth.com*.

### 7.21.2 Near-Field Communication

Vielleicht haben Sie sich schon einmal gefragt, wie die Zugangskontrolle zu den Skiliften, der programmierbare Hotelzimmerschlüssel auf einer Chipkarte, die Identifizierung von Kühen an der automatischen Melkmaschine oder das bargeldlose Bezahlen im Stadion eigentlich funktioniert? Dahinter steckt die Technologie *Radio-Frequency Identification* (*RFID*).

Per RFID kommuniziert ein Lesegerät mit einem *Transponder*. Dieser auch *Etikett* oder *Tag* genannte Mikrochip verfügt in der Regel über keine aktive Stromversorgung. Er bezieht die für seine Nachrichten benötigte Energie vielmehr passiv aus dem Sendesignal des Lesegerätes.

Es wird zwischen *Read-only-Transpondern* und *Read-Write-Transpondern* unterschieden. Im Unterschied zu einem Read-only-Transponder können Sie die im zwischen

einem einzigen Bit und mehreren Kilobyte großen Speicher eines Read-Write-Transponders abgelegten Informationen nachträglich anpassen.

*Near-Field Communication* (*NFC*) ist nun eine RFID-Variante, mit der Sie sich das Leben auch im privaten Umfeld bequemer einrichten können (siehe Abbildung 7.6). Die mit Hilfe Ihres NFC-fähigen Smartphones programmieren NFC-Tags verteilen Sie an häufig frequentierten Orten. Klassischerweise wird dann z. B. im Auto Bluetooth angeschaltet und die Navigations-App gestartet, während die WLAN-Schnittstelle in der Regel nicht benötigt wird. Am Arbeitsplatz angekommen, soll das Mobiltelefon lautlos sein, zu Hause aktivieren Sie dann sehr schnell und bequem wieder die zuvor deaktivierte WLAN-Schnittstelle.

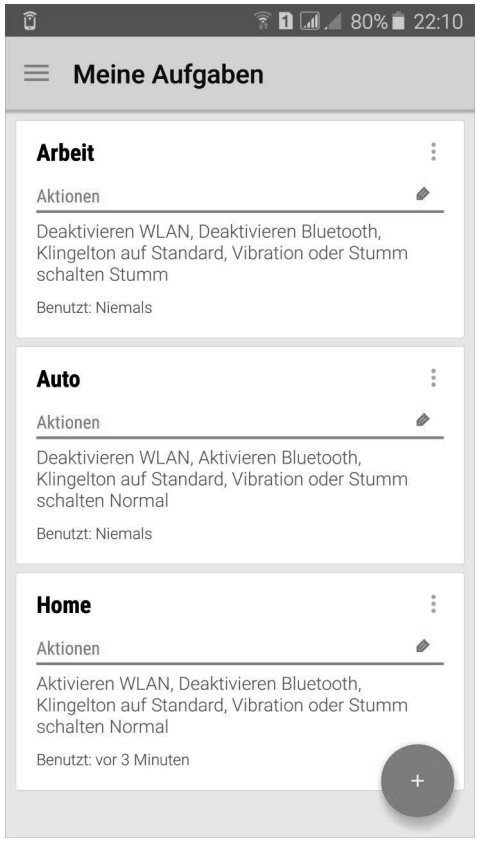



**Abbildung 7.6** Trigger verwaltet und programmiert RFID-Chips.

Abhängig von den auf dem Chip zu hinterlegenden Informationen benötigen Sie mehr oder weniger Speicher. Die Programmierung von drei Befehlen – z. B. WLAN aus, Bluetooth an, Tonschema lautlos – belegt schon ca. 90 Bits Platz. Achten Sie daher darauf, dass die Speichergröße des von Ihnen bestellten NFC-Tags zu Ihren Anforde-

rungen passt! Es ist angenehmer, wenn Sie später feststellen, dass Sie ein bisschen zu großzügig ausgewählt haben, als dass die Programmierung und der Komfort an ein paar Bits scheitern.

[+] Wenn Sie noch tiefer in die Automation Ihres Android-Gerätes einsteigen wollen, empfehle ich Ihnen die App *Tasker*. Dieses Schweizer Messer ist genau das richtige Werkzeug, wenn Ihnen die Möglichkeiten von Trigger nicht ausreichen.

[»] Das mobile Bezahlsystem der Sparkassen und *Google Pay* nutzen jeweils die NFC-Funktion geeigneter Kartenterminals.

### 7.21.3 Long Range Wide Area Network

Das Übertragungsprotokoll *Long Range Wide Area Network* (*LoRaWAN*) wurde für das *Internet of Things* (*IoT*; dt. *Internet der Dinge*) entwickelt. Die Reichweite der Sender beträgt mehrere Kilometer. In einigen Ländern – z. B. in der Schweiz – wird eine LoRaWAN-Infrastruktur z. B. für die kostengünstige Übertragung von Messdaten und Statusmeldungen verwendet.

[»] Mit dem *Arduino MKR WAN 1300* können Sie auf der Frequenz von 868 MHz das Internet der Dinge selbst nutzen.

## 7.22 Ausblick

Die Anforderungen an WLANs und insbesondere die verfügbaren Bandbreiten steigen. Mit 11n stehen die üblichen 100 Mbit/s, die wir vom kabelgebundenen Ethernet kennen, für WLAN unter idealen Empfangsbedingungen als Nutzdatenrate zur Verfügung. Die Entwicklung bei den Geschwindigkeiten wird sich weiter Richtung Gigabit-WLAN und darüber hinaus orientieren, und es gibt nicht nur theoretische Nachweise, dass dies mit vorhandener Technik möglich ist.

Damit kehrt sich das Geschwindigkeitsverhältnis von WLAN zu LAN vielerorts um: WLANs werden mit 802.11ac und 802.11ad plötzlich schneller als die meisten kabelgebundenen Netzwerke. Und manches Unternehmen wird sich fragen müssen, ob die vorhandene kabelgebundene Netzwerkinfrastruktur für das neue WLAN optimal geeignet ist. Die Investition – und damit die eigentliche Hürde für die noch nicht verabschiedeten WLAN-Standards – dürften nicht die Access Points, sondern vielmehr die nachfolgende Infrastruktur sein.

Auch im Markt der Privatanwender finden mit 11n und 11ac Schritte in Richtung 5-GHz-Band statt; somit sollte es zukünftig vielleicht wieder etwas leichter möglich sein, einen freien Kanal für sein eigenes WLAN zu finden.

Die mögliche Nutzung des 60-GHz-Bandes mit 11ad stellt den Kunden in Zukunft vor mehr Auswahlmöglichkeiten. Umso wichtiger ist es für Sie, zwecks Investitionsschutzes vor einer Kaufentscheidung Ihre Bedürfnisse zu analysieren, sich genauestens zu informieren und beraten zu lassen.

Die weiteren Entwicklungen werden insbesondere bei der Optimierung von WLANs, z. B. der Integration von Quality of Service nach IEEE 802.11e, stattfinden.

IEEE 802.11i ist nach wie vor gängiger Standard (siehe Abschnitt 35.3, »WPA2«). Die wenigen Schwachstellen werden durch den Nachfolger beseitigt (siehe Abschnitt 35.4, »WPA3«). Verfahren, die der Vereinfachung der Konfiguration eines WLANs dienen sollen, sollten Sie vor einem Einsatz unbedingt kritisch prüfen, was ich in Abschnitt 35.6, »Wi-Fi Protected Setup«, am Beispiel WPS deutlich mache.

# Kapitel 19
# DHCP

*DHCP steht für Dynamic Host Configuration Protocol. DHCP weist PCs und anderen Geräten im LAN automatisch eine Netzwerkkonfiguration zu. Lästiges Einrichten von Hand ist nicht mehr nötig.*

Sie können, müssen sich aber nicht zwingend für eine vollständige Netzwerkkonfiguration mit dem *Dynamic Host Configuration Protocol* (*DHCP*) entscheiden. Es ist manchmal auch durchaus sinnvoll, jeweils einen Teilbereich im Netzwerk für manuell konfigurierte *statische* und einen Teilbereich für von einem DHCP-Server verwaltete *dynamische IP-Adressen* zu reservieren.

Die Einrichtung von DHCP in Ihrem Netzwerk läuft folgendermaßen ab: Stellen Sie die PCs im LAN so ein, dass sie ihre IP-Adresse automatisch beziehen, also DHCP durchführen. Das ist die Standardeinstellung fast aller Betriebssysteme. Wenn Sie nun einen PC einschalten, stellt dieser eine Anfrage nach einer IP-Konfiguration ins Netzwerk. Üblicherweise antwortet der DHCP-Server und weist dem PC eine IP-Adresse, eine Subnetzmaske und möglicherweise ein Standardgateway zu. Die Clients, also die PCs, bekommen die Konfiguration nicht auf unbestimmte Zeit, sondern nur für einen begrenzten Zeitraum, z. B. 24 Stunden. Ist die Gültigkeit abgelaufen, muss der Client beim DHCP-Server nachfragen, ob die Gültigkeit verlängert wird oder ob sich etwas ändern soll. Über diesen Mechanismus können Änderungen im Netzwerk (z. B. ein neues Standardgateway) automatisch im LAN verteilt werden.

Bei DHCP handelt es sich um ein Standardverfahren, das bei allen Betriebssystemen Unterstützung findet. DHCPv4-Pakete werden auf dem UDP-Port 67 für Clients und Port 68 für Server versendet, DHCPv6-Pakete auf dem UDP-Port 546 für Clients und Port 547 für Server.

DHCP bietet im Gegensatz zu seinem Vorläufer *BootP* die Möglichkeit, *dynamisches DHCP* durchzuführen. Dynamisch bedeutet, dass ein IP-Adressbereich definiert wird, innerhalb dessen der DHCP-Server IP-Adressen verteilen kann.

Alternativ kann die IP-Adresse an die MAC-Adresse geknüpft werden; dies ist auch das Verfahren bei BootP. Einer festgelegten MAC-Adresse wird immer eine festgelegte IP-Adresse zugewiesen.

Welche Vorteile bietet das DHCP-Verfahren?

- Automatische Konfiguration der LAN-Clients: Sie müssen die Clients nicht mehr manuell konfigurieren, sondern die Einrichtung erfolgt zentral am DHCP-Server.
- Richtlinien: Sie können im DHCP Richtlinien für die Konfigurationsparameter umsetzen, die dann automatisch auf alle Clients angewendet werden.
- Mehrere IP-Subnetze: Ein DHCP-Server kann für mehrere IP-Subnetze zuständig sein. Hierfür ist die zusätzliche Funktion *DHCP Relay* erforderlich.
- Eindeutige IP-Adressen: Der DHCP-Server verhindert, dass IP-Adressen doppelt vergeben werden. Daher kann es bei vollständiger Anwendung von DHCP keine IP-Konflikte geben.
- Effiziente Speicherung der Daten: Die Konfigurationsdaten werden auf dem DHCP-Server abgelegt. Sollte der Client neu installiert werden, stehen die DHCP-Daten wieder zur Verfügung.
- Unterstützung weiterer Anwendungen: Insbesondere automatische Installationsverfahren, z. B. das *Preboot eXecution Environment* (PXE), benötigen DHCP, um die notwendigen Informationen für die Netzwerkinstallation zu bekommen.

[!] Es besteht die Gefahr eines konkurrierenden DHCP-Servers. Wenn jemand absichtlich oder unabsichtlich einen DHCP-Server betreibt, der falsche oder bereits vergebene IP-Adressen vergibt, dann kann dadurch schnell ein komplettes Netzwerk in Mitleidenschaft gezogen werden. In einem solchen Fall muss man den Störenfried schnell ausfindig machen, was bei einem so unscheinbaren Ding wie einem DSL-Router nicht so einfach ist. Ist dies gelungen, müssen alle PCs neu gestartet werden, damit sie die richtige IP-Konfiguration bekommen.

Ein DHCP-Server sollte möglichst immer verfügbar sein, weshalb diese Funktionalität zu Hause gerne auf den DSL-Routern liegt. Falls Sie selbst einen DHCP-Server aufsetzen möchten, haben Sie diese Möglichkeit mit dem Netzwerkserver siegfried (siehe Abschnitt 43.6, »DHCP-Server«).

## 19.1 Die einzelnen Pakete

Es gibt vier unterschiedliche DHCP-Pakete, die während der Vergabe einer IP-Konfiguration zwischen dem Client und dem Server ausgetauscht werden:

- DHCP DISCOVER
- DHCP OFFER
- DHCP REQUEST
- DHCP ACKNOWLEDGE

#### DISCOVER

Der *DHCP DISCOVER* ist ein Broadcast-Paket (siehe Abschnitt 6.10.1, »Ethernet Broadcast«) mit ungefähr folgendem Inhalt: »An alle: Ich brauche eine gültige IP-Konfiguration!« Möglicherweise ergänzt der PC die Anfrage noch um den Zusatz: »Ich akzeptiere nur Angebote, die mindestens folgenden Inhalt umfassen: ...«

Diese Anfrage wird im gesamten IP-Netz von allen PCs und Servern empfangen. Weil der anfragende PC noch keine IP-Adresse hat, gibt es in diesem Paket auch keine Absender-IP-Adresse, sondern lediglich eine MAC-Adresse.

#### OFFER

Jeder DHCP-Server im IP-Netz – es könnten ja mehrere sein – empfängt das *DHCP DISCOVER* des PCs (des Clients). Der DHCP-Server kontrolliert, ob er eine IP-Adresse zuweisen kann, insbesondere, ob noch eine freie dynamische oder eine statische IP-Adresse existiert. Wenn ja, dann macht er ein Angebot (engl. *offer*): »Ich biete dir IP-Adresse ..., Subnetzmaske ...«

Sollte beispielsweise der zur Verfügung stehende Bereich von dynamisch zu vergebenden IP-Adressen ausgeschöpft sein, kommt kein *DHCP OFFER* vom DHCP-Server.

Die IP-Adresse, die der DHCP-Server dem PC angeboten hat, wird zunächst reserviert.

#### REQUEST

Der PC hat möglicherweise mehrere Angebote erhalten und kann sich nun eines davon aussuchen. Üblicherweise überprüft der Client, welcher DHCP-Server alle angefragten Optionen mitliefert. Alle unvollständigen Angebote werden ignoriert, und von den verbleibenden wird jenes angenommen, das zuerst empfangen wurde.

Das ausgewählte Angebot wird jetzt beim DHCP-Server mittels *REQUEST* noch einmal angefragt (engl. *request*). Es könnte ja sein, dass sich in der Zwischenzeit eine Änderung ergeben hat.

#### ACKNOWLEDGE

Der DHCP-Server überprüft die erneute Anfrage und schickt in aller Regel eine Bestätigung (engl. *acknowledgement*), auch *ACK* genannt. Die Alternative zur Bestätigung wäre die Ablehnung mittels *DHCPNAK*. Der Client müsste dann wieder mit einem *DISCOVER* beginnen.

Damit ist das übliche Verfahren abgeschlossen. Der Client hat eine IP-Adresse und kann im LAN über seine IP-Adresse erreicht werden.

Sie halten das Verfahren für aufwendig? Das ist es aber nicht. Das gesamte Verfahren tauscht vier Datenpakete und damit sehr wenig Daten aus. Im Normalfall benötigt der gesamte Vorgang nicht mehr als ein paar Millisekunden.

Optionale und zusätzliche Pakete beschreibe ich im Folgenden.

#### INFORM

Beim *INFORM* handelt es sich um eine Anfrage an einen DHCP-Server, in der nach weiteren Informationen gefragt oder Informationsaustausch zwischen verschiedenen DHCP-Servern betrieben wird.

#### DECLINE

Der Client kann die ihm vom DHCP-Server zugewiesene IP-Konfiguration mit *DECLINE* ablehnen. Dies passiert z. B. dann, wenn der Client feststellt, dass ein anderer PC dieselbe IP-Adresse besitzt. Würde er die IP-Adresse akzeptieren, käme es zu einem IP-Adressenkonflikt.

#### RELEASE

Ein *RELEASE* wird vom Client ausgesendet, wenn er die IP-Konfiguration zurückgeben möchte. Der DHCP-Server weiß, dass die IP-Adresse wieder vergeben werden kann.

## 19.2 Der DHCP-Ablauf

Nachdem ich Ihnen die einzelnen DHCP-Pakete erläutert habe, möchte ich Ihnen nun die Arbeitsweise von DHCP genauer schildern. Abbildung 19.1 zeigt den vollständigen Ablauf von DHCP.

### 19.2.1 Initialisierung

Im Status der Initialisierung (engl. *init*) führt der Client ein *DHCP DISCOVER* aus. Aus den Angeboten, die der Client bekommt (*DHCP OFFER*), muss er eines auswählen (engl. *select*). Die ausgewählte IP-Konfiguration wird angefragt (*DHCP REQUEST*). Üblicherweise bestätigt der DHCP-Server die Anfrage (*DHCPACK*). Ein *DHCPNAK* (*Not Acknowledge*) würde zurück in den Zustand der Initialisierung führen, ebenso ein durch den Client ausgesendetes *DHCPDECLINE*.

Bis zu diesem Punkt wurden alle Pakete als Broadcast versendet!

### 19.2.2 Gebundenheit

Die IP-Konfiguration wird angenommen. Wenn 50 Prozent der Gültigkeitsdauer (engl. *lease*) abgelaufen sind, fragt der PC gezielt per *Unicast*[1] ausschließlich bei dem ihm bekannten DHCP-Server nach, ob die Gültigkeit verlängert (engl. *renew*) wird. Falls die Anfrage bestätigt wird (*DHCPACK*), geht es zurück in den gebundenen Zustand (engl. *bound*).

### 19.2.3 Erneuerung

Ist der DHCP-Server nicht mehr erreichbar, wartet der Client, bis 87,5 Prozent der Gültigkeitsdauer abgelaufen sind. Er sendet bis zum Ablauf der Gültigkeit – auf Englisch heißt dieser Zustand *rebinding* – Anfragen per Broadcast an alle DHCP-Server. Kommt eine Bestätigung, befindet sich der Client im gebundenen Zustand, ansonsten wechselt er in den Zustand Initialisierung.

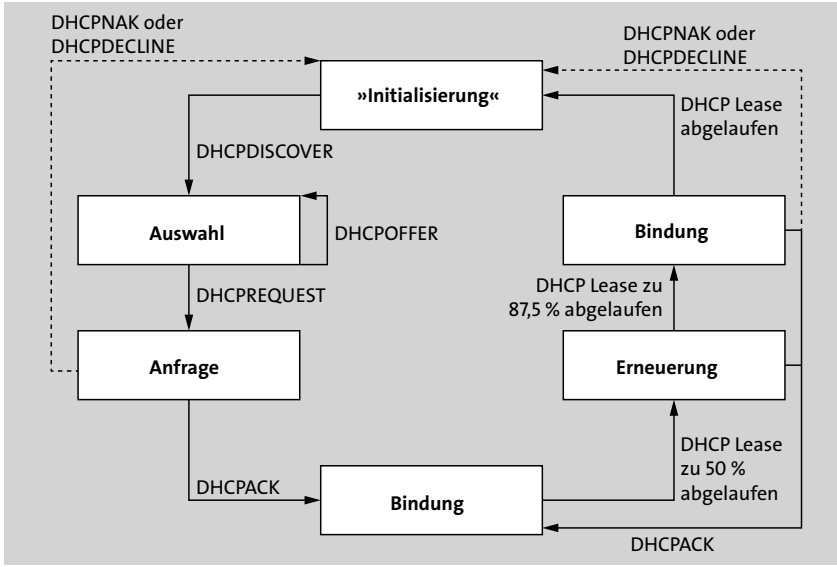



**Abbildung 19.1** Zustände des DHCP-Clients

Sollte der Client bis zum Ablauf der Gültigkeit seiner IP-Konfiguration keine Bestätigung bekommen, muss er die IP-Konfiguration löschen. Dies bedeutet, dass er im LAN nicht mehr erreichbar ist und dort nicht mehr arbeiten kann.

1 Ein Unicast ist eine Kommunikationsverbindung mit genau einem Empfänger.

## 19.3 IPv6-Konfiguration

IPv6 bietet mehr Möglichkeiten der IP-Konfiguration. Jede Variante hat Vor- und Nachteile. Insbesondere bei DHCPv6 ändert sich einiges gegenüber DHCPv4, und mit *SLAAC* (siehe Abschnitt 19.3.1, »IPv6-Autokonfiguration mit SLAAC«) gibt es erstmals einen zuverlässigen Mechanismus ganz ohne weitere Dienste im Netzwerk.

[+] Wenn Sie mit SLAAC (siehe Abschnitt 19.3.1, »IPv6-Autokonfiguration mit SLAAC«) auskommen, dann empfehle ich Ihnen: Lassen Sie DHCPv6 weg!

Alternativ könnten Sie – wie schon bei IPv4 – die IPv6-Konfiguration manuell vornehmen. Vielleicht nutzen Sie diese Möglichkeit in Ihrem IPv4-Netz zurzeit und konfigurieren die Adressen mancher Systeme manuell, wie beispielsweise die Ihres NAS (siehe Kapitel 40, »Netzwerkspeicher«). Bei IPv6 empfehle ich Ihnen das nicht, denn die manuelle Pflege von IPv6-Adressen ist sehr fehleranfällig. Die vielen Teile einer IPv6-Adresse und deren hexadezimale Schreibweise erschweren die Eingabe gegenüber einer IPv4-Adresse erheblich. Bei einer IPv4-Adresse ist der Hostteil üblicherweise nur das vierte Byte, also eine Zahl zwischen 1 und 254. Bei IPv6 sind es bis zu 16 Zeichen für das Prefix (siehe Abschnitt 14.7.1, »IPv6-Adressen«) und weitere 16 Zeichen für den Hostanteil.

[!] Die statische Konfiguration ist auch aus einem anderen Grund in einem LAN keinesfalls zukunftsfähig: Es existiert kein NAT (siehe Abschnitt 14.7, »IP-Version 6«). Ihr Provider wird Ihnen mindestens ein /64-Subnetz zuweisen, üblich ist sogar ein /56-Subnetz. Damit stehen Ihnen mindestens $2^{64}$ IPv6-Adressen zur Verfügung. Gleichzeitig bedeutet dies, dass jeder Netzwerkteilnehmer eine offizielle IPv6-Adresse bekommt und ausschließlich mit dieser im Internet surfen kann. Bei Endkundenanschlüssen ist es jedoch üblich, dass der Provider das Prefix eines Subnetzes im Turnus von 24 Stunden wechselt. Das würde bei einer statischen IPv6-Konfiguration bedeuten, dass Sie regelmäßig nach Ablauf von 24 Stunden manuell die statische IPv6-Konfiguration aller PCs in Ihrem LAN erneuern müssten.

### 19.3.1 IPv6-Autokonfiguration mit SLAAC

Jeder IPv6-Router sendet regelmäßig *Router Advertisements* (*RA*) (siehe Abschnitt 15.2, »Neighbor Discovery Protocol«) in das LAN. Mehr braucht es nicht, um eine vollständige IPv6-Konfiguration im Netzwerk zu erhalten. Wechselt das Prefix Ihres offiziellen /64-Subnetzes, sendet der Router aktualisierte RAs, und alle Netzwerkteilnehmer erstellen eine neue IPv6-Konfiguration.

Dieses Verfahren heißt *Stateless Address Autoconfiguration* (*SLAAC*). Zustandslos (engl. *stateless*) bedeutet, dass die IP-Konfiguration nicht zentral verwaltet wird, sondern dass der Netzwerkteilnehmer aufgefordert wird, sich aus dem mitgeliefer-

ten Prefix (siehe Abschnitt 14.7, »IP-Version 6«) selbständig eine IPv6-Adresse zu generieren. Mittels *Duplicate Address Detection* (*DAD*) stellt er anschließend sicher, dass diese Adresse nicht bereits verwendet wird. Dazu sendet er die Nachricht *Neighbor Solicitation* an die von ihm errechnete Adresse. Kommt von dort ein *Neighbor Advertisement* als Antwort zurück, muss er eine andere Adresse bilden.

Neben dem Prefix erfährt ein Netzwerkteilnehmer aus dem RA auch das Standardgateway und das IPv6-Subnetz für den Routingeintrag. Alle modernen Betriebssysteme unterstützen darüber hinaus *Recursive DNS-Server* (*RDNSS*), worüber im RA auch die IPv6-Adresse des DNS-Servers (siehe Kapitel 20, »Namensauflösung«) mitgeteilt werden kann. Ältere Geräte unterstützen mitunter kein RDNSS. In diesem Fall haben Sie die Option, DHCPv6 für die IPv6-Konfiguration zu nutzen.

### 19.3.2 DHCPv6

DHCP für IPv6 hat sich gegenüber DHCP für IPv4 an vielen Stellen geändert. Leider ist es so, dass die Normierungsgruppen für IPv6 und DHCP nicht gut miteinander kooperieren. Im Ergebnis wird die IPv6-Konfiguration komplizierter, als es nötig wäre.

Ich möchte einige wesentliche Neuerungen herausgreifen:

- Die Identifizierung der DHCPv6-Clients und der jeweiligen Netzwerkschnittstelle, der eine IPv6-Adresse zugewiesen werden soll, erfolgt anhand des *DHCP Unique Identifier* (*DUID*) und des *Identity Association Identifier* (*IAID*) und nicht – wie bei DHCPv4 üblich – anhand der MAC-Adresse.
- Das Defaultgateway kann nicht per DHCPv6 gesetzt werden. Diese Information muss stattdessen dem Router Advertisement entnommen werden.
- Ein Client, der eine Zeit lang nicht mit dem Netzwerk verbunden war, kann mit der Nachricht *CONFIRM* die Gültigkeit seiner ursprünglich zugewiesenen Adresse überprüfen lassen.
- Ein Server kann einen seiner DHCP-Clients mit der Nachricht *RECONFIGURE* auffordern, eine ganze Konfiguration oder Teile davon neu anzufordern.
- Es gibt *Stateless DHCPv6*, bei dem der DHCP-Server keine IP-Adresse zuweist.

Zwei Arten von DHCPv6 werden mit Hilfe der Flags *Managed Configuration* (*M-Flag*) und *Other Configuration* (*O-Flag*) im Router Advertisement (siehe Abschnitt 15.2, »Neighbor Discovery Protocol«) unterschieden:

- *Stateful DHCPv6*: Die zustandsbehaftete (engl. *stateful*) Konfiguration wird zentral von einem DHCPv6-Server verwaltet. Der Netzwerkteilnehmer wird mit gesetztem M-Flag im Router Advertisement aufgefordert, sich dort seine komplette Konfiguration samt Netzwerk-Prefix abzuholen.

- *Stateless DHCPv6*: Ohne ein gesetztes M-Flag wird die IPv6-Konfiguration mittels SLAAC (siehe Abschnitt 19.3.1, »IPv6-Autokonfiguration mit SLAAC«) gebildet. Ein im Router Advertisement gesetztes O-Flag weist auf ergänzende Konfigurationsanteile – wie z. B. DNS- oder NTP-Server – hin, die über DHCPv6 verteilt werden.

Ohne Router Advertisement funktioniert DHCPv6 also nicht.

DHCPv6 setzt gleichzeitig auf Bewährtes, wie Sie Tabelle 19.1 entnehmen können.

| Type | Beschreibung | IPv4-Pendant |
|---|---|---|
| SOLICIT (1) | Der Client sucht einen DHCP-Server (Beginn einer DHCP-Aushandlung). | DISCOVER |
| ADVERTISE (2) | Der Server reagiert auf SOLICIT-Nachrichten. | OFFER |
| REQUEST (3) | Der Client fragt eine konkrete neue Lease an. | REQUEST |
| CONFIRM (4) | Der Client testet die Gültigkeit seiner Lease. | REQUEST |
| RENEW (5) | Der Client will seine Lease verlängern (Unicast zu bekanntem Server). | REQUEST |
| REBIND (6) | Wird per Multicast gesendet, wenn auf RENEW keine Antwort kam. | REQUEST |
| REPLY (7) | Wird vom Server auf SOLICIT, REQUEST, RENEW und REBIND gesendet. | ACKNOWLEDGE |
| RELEASE (8) | Der Client gibt seine Lease wieder frei (z. B. beim Shutdown oder Reboot). | RELEASE |
| DECLINE (9) | Der Client meldet dem Server, dass eine Adresse am Link bereits genutzt wird (DAD). | DECLINE |
| RECONFIGURE (10) | Der Server sendet dem Client die Nachricht, dass sich die Konfiguration geändert hat. | – |
| INFORMATION-REQUEST (11) | Der Client fragt zusätzliche Parameter und Optionen an. | INFORM |
| RELAY-FORW (12) | Der DHCP-Relay-Agent sendet Anfragen weiter. | – |
| RELAY-REPL (13) | Ein Server antwortet dem DHCP Relay Agent. | – |

**Tabelle 19.1** DHCPv4 und DHCPv6 im Vergleich

Die typische DHCPv6-Kommunikation läuft wie folgt ab:

1. SOLICIT
2. ADVERTISE
3. REQUEST
4. REPLY

Setzt ein Client die Option *Rapid Commit* in seiner SOLICIT-Anfrage und ist der Server ebenfalls entsprechend konfiguriert, werden ADVERTISE und REQUEST übersprungen. Das Netzwerk wird dadurch auf Kosten der Ausfallsicherheit entlastet.

Auf der Internetseite *http://www.elektronik-kompendium.de/sites/net/1902141.htm* finden Sie ein ausführliches Beispiel für den kompletten Ablauf einer IPv6-Konfiguration mitsamt Router Advertisement.

## 19.4 Das DHCP-Datagramm

Falls dort nichts Abweichendes vermerkt ist, entspricht eine Zeile des DHCPv4-Datagramms in Abbildung 19.2 32 Bits.

Das DHCPv4-Datagramm ist bis zu 576 Bytes groß.

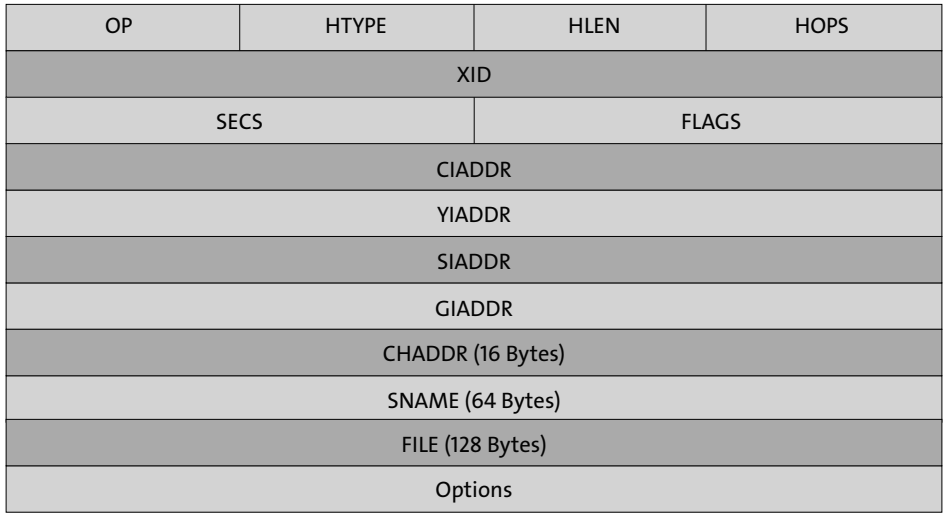



**Abbildung 19.2** Das DHCP-Datagramm

- *Operation Code* (*OP*): Haben diese 8 Bits den Wert 1, handelt es sich um eine Anfrage (z. B. ein REQUEST oder ein DISCOVER). Bei einem Wert von 2 handelt es sich hingegen um eine Antwort (z. B. OFFER oder ACKNOWLEDGE).

- *Hardware type* (*HTYPE*): Diese 8 Bits enthalten den Hardwareadresstyp und damit die Art des Netzwerks. Der Wert 1 steht z. B. für 10-Mbit/s-Ethernet, der Wert 6 für die schnelleren Ethernet-Varianten (siehe Kapitel 6, »Ethernet«). Die Felder HTYPE und HLEN finden sich mit gleicher Bedeutung noch an einer anderen Stelle (siehe Abschnitt 15.3, »Das ARP-Datagramm«).
- *Hardware length* (*HLEN*): Dieses Byte enthält die Länge der Hardwareadresse in Bytes, für Ethernet (MAC) entsprechend den Wert 6.
- *HOPS*: Da ein DISCOVER als Broadcast gesendet wird, wird er von Routern in der Regel nicht weitergeleitet und kann so nicht in ein anderes Netzwerksegment gelangen, selbst wenn dort eine Konfiguration für den Client vorhanden wäre. Nur Router mit der Funktion *DHCP Relay* bzw. *BootP Relay* können DHCP helfen, die Grenzen eines Netzwerksegmentes zu überwinden. Die Anzahl dieser *DHCP-Relay-Agents* wird von den Routern selbst in diesen 8 Bits hochgezählt, um Schleifen zu erkennen.
- *Transaction Identifier* (*XID*): Mit Hilfe der von ihm erzeugten 4 Bytes großen ID ordnet der DHCP-Client die Antworten des DHCP-Servers seinen Anfragen zu.
- *Seconds* (*SECS*): Die Zeit in Sekunden, seit der die aktuelle Anfrage des DHCP-Clients läuft. DHCP Relays können dieses Feld auswerten und nur Anfragen weiterleiten, die bereits eine gewisse Lebensdauer überschritten hat.
- *FLAGS*: Von diesen 16 Bits wird nur das erste als *Broadcast-Flag* benutzt. Besitzt der Client während der Anfrage keine gültige IP-Adresse, setzt er dieses Flag und signalisiert dem Server, dass dieser mit einem Broadcast antworten soll.
- *Client IP Address* (*CIADDR*): Sollte der Client bereits eine gültige IP-Konfiguration besitzen, teilt er sie in 4 Bytes mit.
- *Your IP Address* (*YIADDR*): Die 4 Bytes große IP-Adresse, die der Server an den anfragenden Client vergibt.
- *Server IP Address* (*SIADDR*): In diese 4 Bytes trägt der Server seine IP-Adresse ein.
- *Gateway IP Address* (*GIADDR*): Die 4 Bytes große IP-Adresse des Relay Agents.
- *Client Hardware Address* (*CHADDR*): Diese 16 Bytes enthalten die Hardwareadresse des anfragenden Netzwerkteilnehmers, für Ethernet also die MAC-Adresse.
- *Server Name* (*SNAME*): Mit diesen 64 Bytes kann ein DHCP-Server dem Client zusammen mit der Konfiguration seinen Namen übermitteln.
- *Boot Filename* (*FILE*): Der DHCP-Server kann dem Client in diesen 128 Bytes den Namen einer Datei mitteilen, die er über das *Trivial File Transfer Protocol* (*TFTP*) von einem Server laden soll, der als Option mitgegeben wird.
- *Options*: Optionale Parameter in maximal 312 Bytes, die den eigentlichen Inhalt der Kommunikation darstellen.

## 19.5 Das DHCPv6-Datagramm

Eine Zeile in Abbildung 19.3 entspricht 32 Bits.

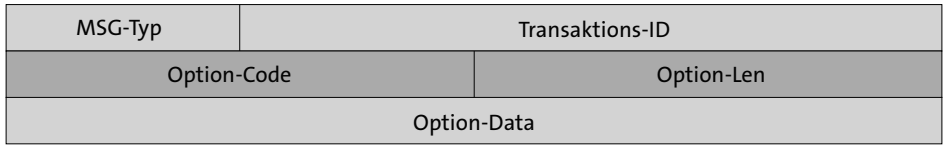



**Abbildung 19.3** Das DHCPv6-Basis-Datagramm

- *Message Type* (*MSG-Typ*): In diesen 8 Bits findet sich der Typ der jeweiligen Nachricht (siehe Tabelle 19.1).
- *Transaktions-ID*: Mit Hilfe dieser 3 Bytes großen ID können Anfragen und Antworten einander zugeordnet werden.
- *Option-Code*: Diese 16 Bits spezifizieren die in der jeweiligen Nachricht enthaltene Option.
- *Option-Len*: In diesen 16 Bits ist die Länge des Feldes *Option-Data* in Bytes gespeichert.
- *Option-Data*: der eigentliche Inhalt der Kommunikation

Andere zusätzlich in DHCPv6 definierte Datagramme – z. B. für DHCP-Relay-Nachrichten – weichen von dem oben beschriebenen Basisdatagramm zur Kommunikation zwischen DHCP-Server und Client ab. Sie finden eine komplette Beschreibung der Unterschiede in englischer Sprache unter *https://www.rfc-editor.org/rfc/rfc3315.txt*.

# Kapitel 40
# Netzwerkspeicher

*Mit der Verbreitung von Netzwerken, dem sinkenden Preis von Festplattenvolumen und dem Speicherverbrauch durch Fotos, Videos und Musik stieg der Bedarf an netzwerkfähigen Speicherlösungen: NAS.*

Zunächst gab es *Network Attached Storage* (*NAS*) nur für das professionelle Umfeld. Lösungen für den Heimanwender oder kleinere geschäftliche Netzwerke wurden meist auf PC-Basis und mit Windows- oder Linux-Betriebssystemen erstellt: ein alter PC, Windows oder Linux drauf, eine SMB-Freigabe erstellt, fertig.

Es gibt im Wesentlichen vier unterschiedliche Möglichkeiten für ein NAS:

- eine Linux-Distribution auf PC-Hardware
- eine Linux-Distribution auf einem Einplatinencomputer (siehe Abschnitt 55.4, »Raspberry NAS«)
- eine spezielle Hardwarelösung
- ein Router mit externem USB-Datenspeicher

Wenn Sie sich mit dem Thema NAS beschäftigen und Testberichte dazu lesen, werden Sie feststellen, dass üblicherweise die Frage des Datendurchsatzes im Fokus steht. Oftmals ist das schnellste NAS im Test auch der Testsieger. Die Argumentation ist auch grundsätzlich richtig, schließlich will man beim Speichern oder Abrufen der Daten nicht auf das NAS warten. Andererseits ist in vielen Fällen fraglich, ob mit den typischen Programmen eines Privatanwenders auch nur annähernd messbarer Datendurchsatz erzeugt werden kann.

Ein gutes Beispiel für den NAS-Einsatz ist die digitale Bildersammlung. Alle sollen auf die Fotos zugreifen können. Ein 3 MByte großes Foto bedeutet aber lediglich 24 Mbit; entsprechend dauert es selbst bei einem langsamen NAS weniger als eine Sekunde, dieses Foto zu laden. Ob es nun aber letztendlich 0,3 oder 0,001 Sekunden dauert, ist bei einem Bild irrelevant.

Der zweite Einsatzzweck ist das Backup von Dateien. Hier ist Datendurchsatz gefordert; schließlich will man nicht auf die Fertigstellung des Backups warten. Zu beachten ist, dass ein Schreibvorgang in der Regel deutlich länger dauert als ein Lesevorgang. Nach meinen Beobachtungen lasten z. B. Backuptools eine gebräuchliche

Netzwerkverbindung (siehe Abschnitt 6.3, »Gigabit-Ethernet«) durchschnittlich zu etwa 60 Prozent aus. Insbesondere bei der Verarbeitung vieler kleiner Dateien ist der Flaschenhals häufig die Anwendung und nicht das NAS oder das LAN.

[+] Möglichkeiten, wie Sie Ihren PC am besten sichern, finden Sie in Kapitel 45, »Netzwerkbackup«, beschrieben. Dort stelle ich verschiedene Ansätze vor.

## 40.1 EasyNAS, FreeNAS, OpenMediaVault und Co.

Wenn Sie ausschließlich Speicherplatz im Netzwerk möchten und weitere Funktionen der heutigen NAS-Systeme für Sie uninteressant sind, kann eine spezielle Linux-Distribution wie *FreeNAS* (*https://www.freenas.org*) oder *OpenMediaVault* (*https://www.openmediavault.org*) für Sie interessant sein.

*EasyNAS* (*https://easynas.org*) basiert auf der Distribution openSUSE und verwendet das *B-Tree Filesystem* (siehe Abschnitt 43.4, »Das B-Tree Filesystem«).

[+] Vor der Verwendung alter PC-Hardware für ein NAS muss ich aus mehreren Gründen warnen. Entweder ist der Stromverbrauch moderat, dann wird die Leistung nicht stimmen, oder der Stromverbrauch ist – verglichen mit modernen Systemen – exorbitant. Der zweite Grund betrifft die Ausfallsicherheit: Alte Komponenten, insbesondere alte Festplatten, gehören meiner Meinung nach nur bedingt in ein NAS, denn dort möchten Sie Ihre Daten sicher ablegen.

Bitte berücksichtigen Sie die gerade angeführten Überlegungen, wenn Sie über ein Selbstbau-NAS nachdenken. Die Lösung mag grundsätzlich reizvoll sein, der Weg zu einer komfortablen Lösung ist allerdings steinig. Die Stromkosten eines 80-Watt-NAS belaufen sich im Jahr auf stolze 140 €, so dass die Lösung innerhalb von drei Jahren bei den Betriebskosten in etwa dieselben Kosten verursacht wie für die Anschaffung.

Leider bleiben die Spezialdistributionen hinsichtlich ihrer Performance deutlich hinter aktuellen Linux-Distributionen und insbesondere hinter OpenSolaris zurück.

Wenn Sie sich ein Beispiel für ein kleines NAS anschauen wollen, dann finden Sie eine Beschreibung in Abschnitt 55.4, »Raspberry NAS«.

## 40.2 Router mit externer USB-Platte

Eine beliebte Minimallösung ist es, einen Router über seine USB-Schnittstelle mit einer externen USB-Festplatte zu erweitern und Netzlaufwerke anzubieten.

Bevor Sie diese Lösung in Betracht ziehen, bedenken Sie bitte, dass eine einzelne USB-Platte auch ausfallen kann. Diese Platten sind nicht für den Dauerbetrieb ausgelegt; dies erhöht das Ausfallrisiko, wenn sich die Platte nicht in den Schlaf schicken lässt. Eine weitergehende Sicherung der Daten kann üblicherweise nicht erfolgen; daher sollten auf dieser Lösung nur Daten abgelegt werden, die entweder auf anderen PCs noch vorhanden sind oder deren Verlust Sie leicht verschmerzen können.

### 40.2.1 DSL-Router

Was bietet nun der DSL-Router als Fileserver? Das hängt natürlich vom Router selbst ab. Die bekannten und beliebten FRITZ!Box-Modelle können die USB-Platte per SMB oder FTP im Netzwerk zur Verfügung stellen. Es ist möglich, einen Kennwortschutz zu vergeben. Es gibt jedoch keine Benutzerverwaltung; jeder Benutzer hat also – abgesehen vom einheitlichen Kennwortschutz – Zugriff auf alle Dateien.

Ein häufiges Problem sind USB-Platten, die ihren Strom vom USB-Port beziehen. Der Strom an der FRITZ!Box reicht in einigen Fällen nicht aus, so dass Sie für eine zusätzliche externe Stromzufuhr sorgen müssen. In diesem Fall kann das nur ein USB-Hub mit eigener Stromversorgung sein.

Während der Datendurchsatz früherer Router mit USB 1.1 oder USB 2.0 häufig nicht über 2 Mbit/s bzw. 16 Mbit/s hinausging, erreichen heutige Modelle über USB 3.0 auf schnellen SSD-Speichern in der Spitze Werte von mehr als 500 Mbit/s beim Lesen und 200 Mbit/s beim Schreiben. Eine FRITZ!Box bietet zusätzlich die Möglichkeit, Multimediadateien mit einem Streamingserver im Netzwerk bereitzustellen (siehe Kapitel 46, »Medienstreaming«).

Der große Vorteil dieser Lösung ist ganz klar der Preis:

- keine zusätzliche Hardware
- kein zusätzlicher Stromverbrauch (von der USB-Platte abgesehen)
- kein zusätzlicher Netzwerkanschluss
- kein Lärm

Insgesamt bietet diese Lösung Basisfunktionalitäten. Sie ist weit entfernt von den Möglichkeiten, die selbst einfache NAS-Systeme bieten.

## 40.3 Hardware-NAS

Häufig ist die Anschaffung eines Hardware-NAS die vernünftigste Lösung. Oder zumindest ist es langfristig die günstigere Lösung, wenn Sie die Stromkosten berücksichtigen.

Was bietet ein solches NAS heute üblicherweise? Natürlich hängt der Leistungsumfang stark vom Preis ab.

- Zu den Standarddiensten eines NAS gehören Dateifreigaben über Protokolle wie Samba (siehe Abschnitt 43.7, »Samba als Fileserver«) und NFS.
- Die *Synchronisierung* der Dateien zwischen verschiedenen Anwendern und Plattformen wird häufig mit vom Hersteller des NAS bereitgestellter Clientsoftware ermöglicht.
- Für die Datensicherung auf ihr System bieten die Hersteller in der Regel ebenfalls Lösungen an.
- Wenn Sie es vielleicht von Ihrer Arbeit mit virtuellen Maschinen kennen (siehe Abschnitt 41.2, »Oracle VM VirtualBox«), dann werden Sie eine Snapshot-Funktionalität auf Ihrem NAS sicherlich auch nützlich finden. Dazu muss das Filesystem Ihres NAS diese Funktionalität unterstützen, so wie dies z. B. beim *B-Tree Filesystem* der Fall ist (siehe Abschnitt 43.4, »Das B-Tree Filesystem«).
- Sie können Ihr NAS für die Ablage und das Streamen von Multimediainhalten (siehe Kapitel 46, »Medienstreaming«) nutzen. Soll Ihr NAS zugleich als komplettes Media Center – vergleichbar einer Lösung wie Kodi – dienen (siehe Abschnitt 46.4, »Kodi Home Theater«), muss es natürlich über entsprechende Schnittstellen zum Anschluss eines TV-Gerätes verfügen.
- Einige Hersteller integrieren Werkzeuge zur Kollaboration in ihre NAS-Systeme. Dazu zählen z. B. ein Teamkalender oder eine private Cloud-Office-Lösung (siehe Kapitel 48, »Cloud-Computing«).
- Die Nutzung des NAS als Host für Zwecke der Virtualisierung (siehe Kapitel 41, »Virtualisierung«) benötigt selbstverständlich deutlich mehr verfügbare Hardwareressourcen.
- Häufig können Sie die Aufnahmen Ihrer Raumüberwachung (siehe Abschnitt 46.2.1, »Netzwerkkamera«) direkt von Ihrem NAS verwalten lassen.
- Ein dauerhaft eingeschaltetes NAS ist auch eine mögliche Basis für Ihr Smart Home (siehe Kapitel 49, »Hausautomation«). Sie finden im Internet diverse Anleitungen für die Installation von z. B. FHEM (siehe Abschnitt 50, »FHEM-Steuerzentrale«) oder openHAB auf gängigen NAS-Systemen.
- Viele NAS-Systeme ermöglichen die integrierte Bereitstellung von Datenbanken. Eine zentrale Datenbank können Sie u. a. für Ihr Home Theater nutzen (siehe Abschnitt 46.4.3, »Medienverwaltung«) und z. B. eine im Wohnzimmer begonnene Videowiedergabe ohne lästige vorherige Suche der richtigen Position im Film komfortabel im Schlafzimmer fortsetzen.

### 40.3.1 Art und Anzahl der Festplatten

Obwohl eigentlich jede Festplatte in einem NAS genutzt werden kann, bieten die Hersteller in Bezug auf Hardware und Firmware auf den jeweiligen Einsatzzweck abgestimmte Modelle an. Festplatten für Desktop-PCs, die heute in der Regel durch SSD-Speicher abgelöst werden, erreichen durch eine höhere Umdrehungsgeschwindigkeit eine bessere Performance. Allerdings benötigen sie auch deutlich mehr Strom, was sie in einem für den Dauerbetrieb konzipierten NAS unwirtschaftlich macht. Die speziell für den Einsatz in einem NAS vorgesehenen Festplatten benötigen hingegen weniger Strom und tolerieren die in den Ruhezeiten des NAS üblichen Parkvorgänge des Schreib-/Lesekopfes oft besser.

Ich empfehle Ihnen, vor einer Anschaffung von Festplatten auf die Kompatibilitätsliste des Herstellers Ihres jeweiligen NAS-Systems zu achten.

Wie viele Festplatten braucht das NAS? Viele Nutzer entscheiden sich für einen Kompromiss und damit zwei Festplatten. So ist es möglich, die Daten mittels RAID 1 zu spiegeln; die Datensicherheit ist also gegenüber der Lösung mit einer Platte erhöht. Eine weitergehende Datensicherung ist dennoch unbedingt zu empfehlen. Der Einsatz von wenigen Festplatten mit mehr Kapazität verbraucht im Betrieb zudem weniger Energie als der Einsatz mehrerer Festplatten mit weniger Speicherplatz und amortisiert sich daher in der Regel schnell.

Der Einsatz von SSD-Speichern in einem NAS empfiehlt sich aufgrund der höheren Anschaffungskosten in der Regel nur, wenn Sie die schnelle SSD als Cache vor den langsameren Festplatten einsetzen. Viele NAS-Systeme bieten diese Funktionalität.

Wir können uns hinsichtlich der Festplattenkonfiguration (siehe Tabelle 40.1) voll und ganz auf den Aspekt der Datensicherheit konzentrieren. Weitere Aspekte wie Zuwachs des Datentransfers kommen bei den Einsteiger-NAS-Systemen nicht zum Tragen.

Ich habe in einigen Fachpublikationen gelesen, dass die Spiegelung des RAID 1 keinen erheblichen Vorteil bringe, da sie lediglich den Ausfall einer Platte abdecke. Genau das wird aber doch der häufigste Fall sein. Die Wahrscheinlichkeit, dass beide Platten zusammen ausfallen, ist doch eher gering.

Ich gehe davon aus, dass die Daten auf Ihrem NAS für Sie wichtig sind, und kann Ihnen nur wärmstens empfehlen, den Schwerpunkt auf Sicherheit zu legen. Entsprechend ist RAID 1 mein Favorit und punktet auch gegenüber JBOD. RAID 0, bei dem alle Daten verloren sind, wenn eine Platte defekt ist, verbietet sich von selbst.

Für eine Lösung mit einer Platte spricht, dass sie deutlich günstiger in der Anschaffung ist und etwa 10 Watt weniger an Strom verbraucht. 10 Watt klingt wenig, bei einem 24-Stunden-Betrieb kommt man aber auf jährliche Kosten von zurzeit etwa 20 €.

| Anzahl Platten | Konfiguration | Wirkung |
|---|---|---|
| ≥ 2 | RAID 0 | Die Daten werden immer auf allen Platten verteilt, totaler Datenverlust beim Defekt einer Platte. |
| ≥ 2 | RAID 1 | Spiegelung aller Daten auf einem Spiegel, daher nur die halbe Kapazität; beim Defekt einer Platte sind die Daten vollständig auf der anderen Platte vorhanden. |
| ≥ 2 | JBOD | Die Platten wirken wie eine große Festplatte. Daten werden entweder auf der einen oder auf der anderen Platte gespeichert. Beim Defekt sind »nur« die Daten der defekten Platte verloren. |
| ≥ 3 | RAID 5 | Die Daten werden reihum auf alle Platten verteilt, zusätzlich werden auf mindestens einer Platte Paritätsinformationen geschrieben (rechenintensiv!). Beim Ausfall einer Platte stehen weiterhin alle Informationen zur Verfügung. Die Gesamtkapazität des Verbundes vermindert sich effektiv nur um die Paritätsinformationen. |

**Tabelle 40.1** Möglichkeiten der Konfiguration von Festplatten

### 40.3.2 Fallstricke bei der Auswahl

Nachdem Sie sich nun für die Anzahl der Platten entschieden haben, geht es jetzt um die konkreten Produkte. Ich kann Ihnen nur wärmstens empfehlen, sich mit Testberichten ausführlich zu informieren. Die Seite *https://www.smallnetbuilder.com* ist in englischer Sprache, im deutschsprachigen Internet werden öfter Tests auf *https://www.tomshardware.com* veröffentlicht.

Mögliche Probleme bei Hardware-NAS sind:

- laute Lüftergeräusche
- inkompatible Festplatten (Herstellervorgaben beachten!)
- niedriger Datendurchsatz
- nicht funktionierender Schlafmodus (Hibernation) für Platten
- keine Weiterentwicklung der NAS-Firmware
- funktionale Einschränkungen, Funktionen nicht nutzbar

Ergebnis meiner Recherche war, dass die NAS-Systeme üblicherweise lauter sind als erhofft. Nicht selten sind es die Lüftergeräusche, die den unangenehmsten Lärm verursachen. Für das Wohnzimmer oder gar Schlafzimmer taugen diese Systeme nicht.

Die NAS-Performance hängt insbesondere mit der CPU und dem RAM zusammen. Kleinere oder billigere NAS sind tendenziell auch langsamer. Dabei sind die Festplatten nicht die Ursache für Performanceengpässe; sie leisten 400 Mbit/s oder mehr. Das ist ein Wert, von dem die meisten NAS-Systeme beim Datendurchsatz um den Faktor zehn entfernt sind. Entsprechend sollten Sie bei der Festplattenauswahl eher Wert auf geringen Stromverbrauch und geringe Lärmentwicklung legen.

Bevor Sie sich für ein Hardware-NAS entscheiden, empfehle ich Ihnen, die jeweilige Benutzeroberfläche des Herstellers zu testen. Sie finden z. B. eine Onlinedemo des *QNAP-NAS-Betriebssystems* (*QTS*) unter *https://www.qnap.com/de-de/live-demo*, eine Livedemo des *DiskStation Managers* (*DSM*) von Synology im Internet unter der Adresse *https://demo.synology.com/de-de/dsm*.

In Abbildung 40.1 sehen Sie ein Webinterface eines Hardware-NAS der Firma QNAP. Es zeichnet sich durch einen großen Funktionsumfang aus, wie z. B. Überwachungsstation für IP-Kameras, iTunes-Server, Webserver mit MySQL-Datenbank und diverse Cloud-Dienste (siehe Kapitel 48, »Cloud-Computing«). Sie zahlen bei der eierlegenden Wollmilchsau auch für den großen Funktionsumfang. Das ist nur sinnvoll, wenn zumindest einige dieser Funktionen auch genutzt werden.

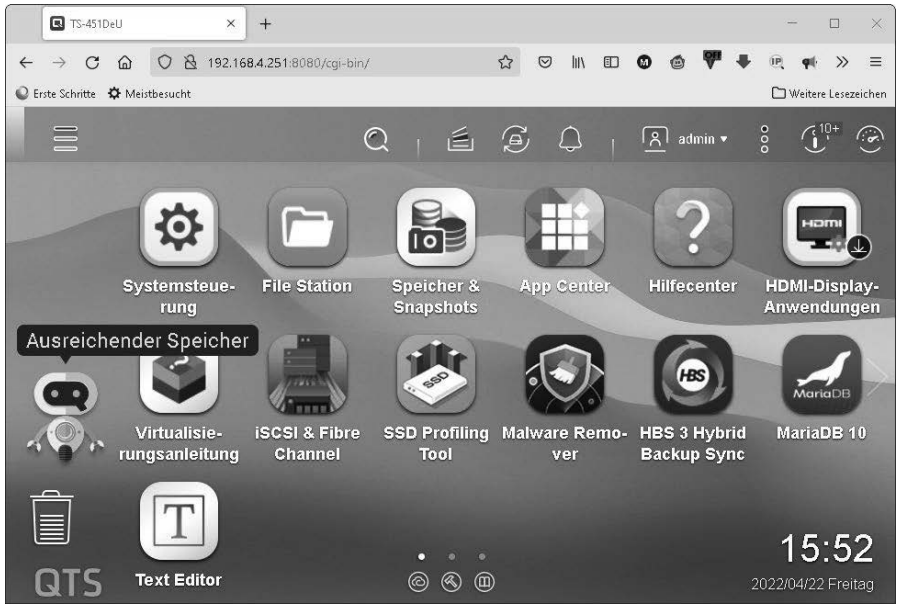



**Abbildung 40.1** Webinterface eines Hardware-NAS

### 40.3.3 Einbindung ins Netzwerk

Die erste Hürde, die Sie bei der NAS-Einrichtung nehmen müssen, ist, das NAS im LAN zu finden. Alle NAS sind bei der Auslieferung auf DHCP gestellt, so dass sie eine IP-Konfiguration vom Router bekommen, wenn dieser als DHCP-Server aktiv ist.

Bei vielen Routern kann man im Webinterface nachschauen, welche IP-Adressen vergeben wurden. Suchen Sie direkt beim Punkt DHCP oder im Bereich Status & Log.

Viele Hersteller von NAS-Lösungen bieten auf der dem Produkt beiliegenden CD ein Programm, das das NAS im Netzwerk sucht. Ob das NAS gefunden wird, ist nicht immer sicher. Im Fall des Qfinder Pro von QNAP hat es geklappt (siehe Abbildung 40.2).

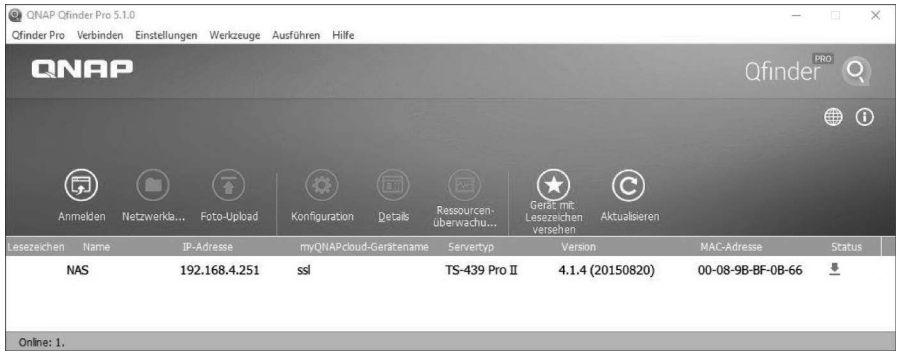



**Abbildung 40.2** Gefunden: mein NAS

Sollten Sie das NAS weder im DHCP-Server noch mit dem Assistenten finden, bleiben noch einige wenige Möglichkeiten. Sie können versuchen, das Gerät per `ping` aus einem Windows-Eingabefenster heraus anzusprechen.

```
for /L %i in (1,1,254) do
   @(ping -n 1 -w 20 192.168.1.%i|find ".%i: B")
```

**Listing 40.1** Mit Hilfe einer Schleife durchsuchen Sie Ihr Subnetz.

Es dauert ein wenig, weil von 192.168.1.1 bis 192.168.1.254 alle IP-Adressen angepingt werden. Angezeigt werden nur die Stationen, die erreicht werden. Eine weitere Möglichkeit ist der Einsatz eines Portscanners wie *nmap* (*https://nmap.org*). Ich empfehle einen Scan des Webserver-Ports 80 mit folgendem Kommando:

```
nmap -p 80 192.168.1.0/24
```

Das Ergebnis dauert nur wenige Sekunden, Sie bekommen sogar den Hersteller anhand der MAC-Adresse aufgelistet, so dass Sie üblicherweise direkt entscheiden können, welche IP-Adresse zu Ihrem NAS gehört.

Ich empfehle Ihnen, über das NAS-Webinterface eine feste IP-Konfiguration einzustellen. Ansonsten könnte es passieren, dass die IP-Adresse des NAS wechselt und Sie die Konfiguration für die Netzlaufwerke anpassen müssen.

# Vorwort

Die Möglichkeiten scheinen unbegrenzt: Smart Home, Streaming, Virtualisierung, Cloud-Computing, IPv6 und mobiles Internet sind heute in aller Munde – doch was genau verbirgt sich eigentlich hinter diesen Begriffen? Wie kann man die neuen Technologien ganz praktisch für sich nutzen?

Dieses Buch legt zunächst die Grundlagen und vertieft danach alle aktuellen Themen, wobei – wie schon in den ersten acht Auflagen – der Schwerpunkt eindeutig auf der Praxis liegt. Ihnen geht es vielleicht auch so wie uns: Was Sie selbst ausprobieren, ist besser verständlich und bleibt besser im Gedächtnis.

Damit Sie Netzwerkfunktionen bequem testen können, liegt dem Buch wieder eine DVD mit Software und mehreren virtuellen Maschinen bei. Eine dieser virtuellen Maschinen ist siegfried, der bewährte Server für zu Hause. Testen Sie siegfried zusammen mit den anderen virtuellen Maschinen von der Buch-DVD auf Ihrem PC, ohne dass eine Veränderung Ihres Systems oder eigene Hardware erforderlich ist.

Nicht nur bei den Themen Hausautomation, Raspberry Pi, Medienstreaming, Voice over IP, Virtualisierung und Cloud legen wir viel Wert auf praxisnahe und nachvollziehbare Projekte. Diese machen großen Spaß bei der Umsetzung und helfen ganz nebenbei, Ihr neu erworbenes Wissen zu festigen und zu vertiefen.

Wir sind uns sicher, dass uns mit dieser Auflage die Verknüpfung von Information, Praxisbeispielen und Software aus einer Hand erneut geglückt ist. So wünschen wir Ihnen gutes Gelingen und viel Freude mit diesem Buch!

Erst nachdem wir ein Buch geschrieben hatten, konnten wir nachvollziehen, dass sich Autoren üblicherweise bei ihren Familien bedanken. An euch, die ihr Rücksicht genommen und uns äußerst geduldig ertragen habt: Vielen Dank!

**Axel Schemberg**, **Martin Linten** und **Kai Surendorf**

# Inhalt

## TEIL I Netzwerk-Grundwissen



## TEIL II Lokale Netze

## TEIL III Weitverkehrsnetze



## TEIL IV Höhere Protokollschichten

## TEIL V Praxiswissen

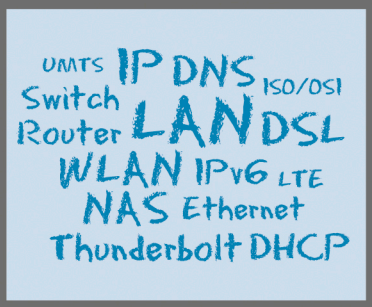
# Anhang

# PC-Netzwerke

»Alles für den engagierten Einsteiger«
administrator

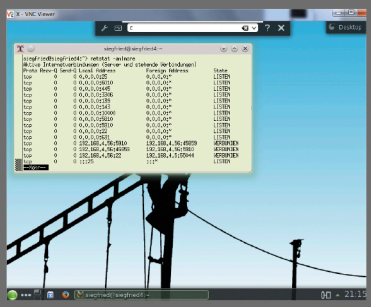
## Theorie und Praxis miteinander verbinden

Nichts geht ohne Netzwerk! Von den Protokollen und der Verkabelung bis zur Heimautomation begleitet Sie dieses Buch bei allen Fragen rund um Ihr Heimnetz. So verstehen Sie, wie Datenverkehr funktioniert, konfigurieren Ihre Router, Firewalls und Clients sicher und setzen spannende Projekte mit FHEM um.




*Grundlagen verstehen*


*Theorie in Praxis übersetzen*



*Viele Beispielprojekte*

### Alles, was Sie für den Netzwerk-Start benötigen

Dieses Standardwerk ist bewährt, praxisnah und randvoll mit Informationen zu allen Aspekten der Netzwerktechnik. Von den Schichten des OSI-Modells bis zur Wahl des richtigen Kabels werden alle Grundlagen besprochen.

### Machen Sie Ihr Netzwerk sicher

Verschlüsseln Sie Mails mit PGP, analysieren Sie den Netzwerkverkehr mit Wireshark und prüfen Sie offene Ports – schon mit wenigen Handgriffen können Sie Ihr Netzwerk sicherer machen.

### Spannende Praxis-Projekte

Eigene Server einrichten, Heimautomationsprojekte mit FHEM umsetzen oder mit dem Raspberry Pi einen eigenen Router bauen: In Ihrem Netz können Sie überraschend viel selbst machen! Werkzeuge und vorbereitete Lösungen finden Sie bei den Materialien zum Buch.

openSUSE-Netzwerkserver siegfried6 mit vielen Tools zu Administration, Backup, Verschlüsselung

**Axel Schemberg** und **Martin Linten** sind Experten in Sachen Netzwerk und UNIX/Linux. Beide sind im Rechenzentrum der Finanzverwaltung NRW tätig und vermitteln ihre Kenntnisse in zahlreichen Seminaren. **Kai Surendorf** ist Fachautor und Experte für die Themen macOS, UNIX und Webtechnologien.

### Aus dem Inhalt



Rheinwerk Computing

9 783836 285285

**€ 29,90 [D]**
€ 30,80 [A]

ISBN 978-3-8362-8528-5
Netzwerke & Datenbanken