Wireless LANs

802.11-WLAN-Technologie und praktische Umsetzung im Detail

von
Jörg Rech

4., akt. u. erw. Aufl.

Heise Zeitschriften 2012

Verlag C.H. Beck im Internet:
www.beck.de
ISBN 978 3 936931 75 4

Inhaltsverzeichnis: Wireless LANs – Rech

1 Einführung in Funknetzwerke

Einleitung

Lokale Netzwerke (LAN) sind heutzutage ein unverzichtbarer Bestandteil der modernen Kommunikationswelt. Daten und Informationen lassen sich unabhängig von ihrer Größe problemlos und komfortabel zwischen den Systemen austauschen. Haben drahtgebundene Netzwerklösungen, wie beispielsweise Ethernet, schon seit längerem in Büros, in der Industrie und im Privatbereich Einzug gehalten, so bahnt sich seit der Jahrtausendwende ein neuer Trend an. Denn zunehmend kommen drahtlose Netzwerklösungen zum Einsatz, die eine Datenübertragung völlig losgelöst vom Datenkabel ermöglichen. Für den Anwender ergibt sich dadurch eine große Flexibilität, Mobilität und eine Vielzahl von Möglichkeiten. Mit der drahtlosen Netzwerktechnik wird man letztendlich auch der Tatsache gerecht, dass man heute nicht mehr mit rein stationären Systemen arbeitet, sondern zunehmend mit mobilen Systemen, wie beispielsweise Notebooks, Tablet PCs oder PDAs (Personal Digital Assistants). Diese Systeme erhalten durch die drahtlose Netzwerktechnik ihre tatsächliche Mobilität, da für den Datenaustausch keine drahtgebundene Anbindung an ein Netzwerk mehr notwendig ist. Befindet sich das System innerhalb einer bestimmten Reichweite, so ist der drahtlose Datenaustausch möglich, wobei das System während der Datenübertragung auch seinen Standort verändern darf.

Anwendungsbeispiele

Wireless-LAN-Lösungen (WLAN) bieten die Möglichkeit, die Produktivität zu steigern und Kosten zu sparen. Durch die drahtlose Netzwerkanbindung ist ein flexibler Zugriff auf vorhandene Netzwerkressourcen möglich, E-Mails können beispielsweise unabhängig vom Standort empfangen beziehungsweise versendet werden. Außendienstmitarbeiter benötigen keine festen Arbeitsplätze mit Netzwerkanschluss, sondern können sich innerhalb der Firma von jedem beliebigen Standort aus im Netzwerk anmelden und Daten austauschen. Dynamische Arbeitsgruppen auf Kongressen, Messen, Workshops

oder während Meetings lassen sich temporär auf einfachste Art und Weise kurzfristig realisieren, da man durch den Einsatz eines WLANs auf eine Verkabelung verzichten kann.

Mobile Lagerverwaltung

Prozesse, bei denen die Mobilität eine unverzichtbare Voraussetzung darstellt, wie beispielsweise Inventuren und Lagerverwaltung, lassen sich durch WLAN-Lösungen problemlos umsetzen. Ältere, unter Denkmalschutz stehende Gebäude, bei denen eine herkömmliche Netzwerkverkabelung undenkbar ist, lassen sich über WLAN-Lösungen vernetzen. Auf diese Weise lassen sich diese Gebäude pr oblemlos erschließen und gewerblich nutzen. Schulen, bei denen eine herkömmliche Netzwerkverkabelung fehlt, können mit WLAN-Lösungen versorgt werden, damit von den Klassenzimmern aus der Zugriff aufs Internet möglich ist.

Gebäudeanbindung

Des Weiteren lassen sich Gebäude auf einem Firmengelände oder Campus über eine WLAN-Lösung drahtlos miteinander verbinden, wodurch die Anmietung einer kostspieligen Standleitung nicht mehr nötig wird. Generell erzielt man eine hohe Kostenersparnis, da man auf herkömmliche Verkabelung verzichten kann, die bislang einen großen Kostenanteil innerhalb der Netzwerkinfrastruktur darstellte.

Drahtloser Internetzugang

Aber auch im privaten Bereich halten WLAN-Lösungen verstärkt Einzug. Mit der Hilfe von WLAN-Lösungen lässt es sich beispielsweise vom Sofa aus bequem surfen oder man kann im Garten E-Mails abrufen und beantworten. Eine Netzwerkverkabelung innerhalb des privaten Gebäudes wird nicht mehr benötigt, damit der Internetzugang der ganzen Familie in den verschiedenen Räumen zur Verfügung steht. Dies ist besonders in Mietwohnungen vorteilhaft, bei denen eine nachträgliche Kabelinstallation generell problematisch oder sogar nicht erlaubt ist.

Hotspots

Auch Hotspots werden imme r beliebter, die in Ballungsgebieten den drahtlosen Internetzugang bereitstellen. Hotspots sind Internetzugänge, die über feste Zugangspunkte (Access Points) über WLAN-Clients zugänglich sind. Flughafengebäude, Bahnhöfe, Cafés, Restaurants oder Hotels sind nur einige Beispiele, in denen man heute bereits Hotspots im großen Stil vorfindet. Hier hat man die Möglichkeit, gegen eine bestimmte Gebühr für eine gewisse Zeit drahtlos auf das Internet zuzugreifen.

Die Anwendungsbereiche für die WLAN-Technologien und das Einsatzspektrum sind theoretisch unbegrenzt. Es ist zu erwarten, dass WLAN einen ähnlichen Hype auslöst wie die Handys in den 90er Jahren.

1.1 Einteilung der Funklösungen

Grundsätzlich werden bei der drahtlosen Datenübertragung die Lösungen in Abhängigkeit zu der erzielbaren Ausdehnung oder Distanz in drei Gruppen, das WPAN (Wireless Personal Area Network), das WLAN (Wireless Local Area Network) und das WWAN (Wireless Wide Area Network), unterteilt.

WPAN

WPAN dient der Datenübertragung über geringe Distanzen bis etwa 10 m. Bestes Beispiel hierfür ist ein Datenabgleich zwischen einem PDA und einem Rechner. Die am weitesten verbreiteten WPAN-Lösungen sind Bluetooth und IrDA. Bei Bluetooth handelt es sich um eine Funklösung und bei IrDA in der Version 1.x um eine Lösung im infraroten Frequenzbereich. Bluetooth bietet eine Datenrate von 1 MBit/s und IrDA in der Version 1.1 eine Datenrate von 4 MBit/s. Großer Nachteil der IrDA-Lösung ist, dass die Datenübertragung einen direkten Sichtkontakt voraussetzt, weshalb sich diese Lösung nicht gerade als benutzerfreundlich erweist.

WLAN

In einem WLAN ist die räumliche Ausdehnung begrenzt, wobei sich die erzielbare Ausdehnung durch die verwendete Netzwerktechnologie ergibt. Dabei stehen die erzielbare Datenrate und Reichweite in einer Wechselbeziehung. Je höher die Datenrate, umso niedriger ist die Reichweite, die erzielt werden kann. Ein WLAN erstreckt sich in der Regel über ein Gebäude oder ein Firmengelände, wobei die Abgrenzung des WLANs eher technisch geprägt ist und eine genaue Abgrenzung per Definition eher Sache des Betreibers ist. Die heute am weitesten verbreiteten WLAN-Lösungen sind die IEEE-802.11-Lösung, HiperLAN und HomeRF, die später in diesem Kapitel noch detailliert betrachtet werden. Bei den drei Kontrahenten kann man jedoch gleich vorweg festhalten, dass heute im WLAN-Bereich die IEEE-802.11-Lösung eine dominierende Rolle eingenommen hat. Der Schwerpunkt dieses Buches ist deshalb auf die WLAN-Lösung nach dem IEEE-802.11-Standard ausgerichtet.

WWAN

Ein WWAN erstreckt sich im Vergleich zum WLAN über eine größere Entfernung, wobei sich diese über mehrere Städte hinweg ausdehnen kann. Bedingt durch die großen Entfernungen und die geringen Bandbreiten, die zur Verfügung stehen, sind nur geringe Datenraten erzielbar. Die bekanntesten WWAN-Lösungen sind GPRS (General Packet Radio Service) und UMTS (Universal Mobile Telecommunication System). GPRS steht heute bei den meisten Mobilfunk-Providern als Dienstleistung zur Verfügung. Mobilfunknetze für UMTS befinden sich hingegen noch im Aufbau und können zur Zeit nur in den Großstädten genutzt werden. GPRS bietet eine maximale Datenrate von

171,2 kBit/s, wobei die meisten Mobilfunk-Provider den Anwendern nur ein Drittel dieser Datenrate bereitstellen. Die maximale Datenrate von UMTS beträgt 2 MBit/s, hierbei wird allerdings vorausgesetzt, dass sich das Mobilfunknetz in der Endausbaustufe befindet und man sich bei der Datenübertragung an einem festen Standort aufhält. Bewegt man sich während der Datenübertragung, z.B. in einem PKW, sinkt die erzielbare Datenrate auf etwa 384 kBit/s. Neben den geringen Datenraten haben die WWAN-Lösungen den großen Nachteil, dass, anders als bei den WPAN- und WLAN-Lösungen, die Datenübertragung gebührenbehaftet ist. Hier bezahlt der Anwender mit jedem übertragenen Byte eine bestimmte Gebühr an den Betreiber des Mobilfunknetzes.

1.2 Geschichte der drahtlosen Kommunikation

Drahtlose Historie

Die Idee der drahtlosen Datenübertragung ist nicht neu, sondern eigentlich ein relativ alter Hut. Denn betrachtet man die Historie von Ethernet, der heute am weitesten verbreiteten drahtgebundenen Netzwerktechnologie, so basiert dessen Entwicklung auf einem experimentellen Funknetzwerk namens Aloha. Das Aloha-System wurde Ende der sechziger Jahre an der Universität von Hawaii entwickelt, um einen Datenaustausch zwischen den Hawaii-Inseln zu ermöglichen. Mit Hilfe von Aloha wurden sieben Campus-Standorte auf vier Inseln mit dem Zentralrechner aus Oahu vernetzt, wodurch auf die Nutzung teurer Telefonleitungen verzichtet werden konnte. Erste kommerzielle Funklösungen für den WLAN-Bereich wurden Anfang der 90er Jahre auf den Markt gebracht. Diese Lösungen hatten jedoch drei gravierende Nachteile. Die erzielbare Reichweite und die Datenrate waren sehr gering, und wollte man ein Funknetzwerk aufbauen, so musste man auf Produkte eines einzelnen Herstellers zurückgreifen, da es sich ausschließlich um proprietäre Lösungen handelte. Letzteres hemmte auch in den 90er Jahren die Marktdurchdringung. Dieser Problematik widmete sich das IEEE (Institute of Electrical and Electronical Engineers) mit der Zielsetzung, einen weltweit anerkannten Standard zu veröffentlichen. Dieses Ziel wurde auch 1997 mit der Verabschiedung des IEEE-802.11-Standards umgesetzt.

1.2.1 Das IEEE-Konsortium

IEEE-Konsortium

IEEE steht für »Institute of Electrical and Electronical Engineers«, auch ausgesprochen als »I-triple-E«. Das IEEE ist eine Vereinigung von Ingenieuren mit Sitz in USA, deren Mitgliederzahl mittlerweile auf

über 380.000 Personen aus etwa 150 verschiedenen Ländern angewachsen ist. Die Mitglieder kommen primär aus den Entwicklungsabteilungen größerer Firmen, die entsprechende Netzwerkprodukte oder Chipsätze herstellen. Die Hauptaufgabe des IEEE liegt in der Ausarbeitung, Verabschiedung und Veröffentlichung von Standards im Netzwerkbereich. Das IEEE wurde 1980 in New York gegründet. Seit dieser Gründung wurde an der Standardisierung verschiedener Netzwerklösungen gearbeitet.

802-Netzwerkstandards

Bedingt durch die Tatsache, dass das Netzwerkprojekt im Jahr 1980 (80) im Monat Februar (2) ins Leben gerufen wurde, wurde als Oberbegriff aller kommenden Netzwerkstandards der Name 802 gewählt. So erhielt beispielsweise der Ethernet-Standard die Bezeichnung 802.3, der Token-Ring-Standard die Bezeichnung 802.5 und der WLAN-Standard die Bezeichnung 802.11. All diese 802-Standards haben gemeinsam, dass sie auf den unteren zwei Schichten des OSI-Referenzmodells angesiedelt sind. Hierbei handelt es sich um die Bitübertragungsschicht, die vom IEEE als PHY benannt wird, und die Sicherungsschicht. Die Sicherungsschicht ist wiederum vom IEEE in zwei Teilschichten, LLC (Logical Link Control) und MAC (Media Access Control), unterteilt. LLC wird von allen IEEE-Netzwerktechnologien gleichermaßen verwendet, wodurch der Datenaustausch zwischen verschiedenen Netzwerktechnologien vereinfacht wird. MAC definiert primär den Medienzugriff, wobei dieser in Abhängigkeit von der Netzwerktechnologie unterschiedlich ausgeführt ist.

1.2.2 Der IEEE-802.11-Standard

IEEE-802.11-Standard

Für die Standardisierung des WLANs griff das IEEE auf den 802.3-Standard zurück, der die heute am weitesten verbreitete drahtgebundene Netzwerktechnologie (Ethernet) spezifiziert. Dies wird deutlich, wenn man das WLAN-Zugriffsverfahren CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) betrachtet, welches dem Zugriffsverfahren von Ethernet, dem CSMA/CD (Carrier Sense Multiple Access / Collision Detection) sehr ähnlich ist (siehe Kap. 4). Wie beim Ethernet erfolgt bei der IEEE-WLAN-Lösung die Verwaltung des Medienzugriffs dezentralistisch. Jede Station steht dabei in Konkurrenz zu den anderen Stationen und ist für den Medienzugriff selbst verantwortlich. Über das Zugriffsverfahren CSMA/CA wird dennoch für einen geregelten Medienzugriff gesorgt, bei dem jede Station die Chance hat, auf das Übertragungsmedium zuzugreifen, um Daten zu übertragen. Sehr oft wird deshalb die 802.11-WLAN-Lösung auch als Wireless Ethernet bezeichnet. Man muss an dieser Stelle jedoch deutlich hervorhe-

ben, dass es sich beim WLAN nicht um eine drahtlose Variante von Ethernet handelt, sondern um ein eigenständiges Protokoll, das durch einen eigenen Standard spezifiziert ist.

802.11-Grundstandard

Der am 26. Juni 1997 verabschiedete 802.11-Standard definiert einen MAC-Layer und drei PHY-Layer (siehe Abschnitt 1.7), mit denen der drahtlose Datenaustausch ermöglicht wird. Die verschiedenen PHY-Typen definieren unterschiedliche Übertragungsverfahren, mit denen Datenraten von 1 und 2 MBit/s realisiert werden. Grundsätzlich kommen zwei Funklösungen oder eine optische Lösung in Frage. Bei den Funklösungen wird als Übertragungsmedium auf elektromagnetische Wellen zurückgegriffen, die in einen Frequenzbereich des 2,4-GHz-Frequenzbandes übertragen werden. Bei dem im 2,4-GHz-Band genutzten Frequenzbereich handelt es sich um das sogenannte ISM-Band (Industrial, Scientific, Medical). Das ISM-Band darf weltweit lizenz- und genehmigungsfrei für industrielle, wissenschaftliche und medizinische Anwendungen genutzt werden, wobei beispielsweise in Deutschland die Sendeleistung auf 20 dBm (100 mW) begrenzt ist. Durch die Nutzung des ISM-Bandes ergibt sich der Vorteil, dass für den Betrieb eines WLAN keine Genehmigung erforderlich ist und dass keine lizenzbehafteten Betriebsgebühren anfallen. Die beiden Funklösungen arbeiten entweder nach dem Verfahren des Frequency Hopping Spread Spectrum (FHSS) oder dem des Direct Sequence Spread Spectrum (DSSS) (siehe Kap. 3). Die optische Lösung ermöglicht die Datenübertragung über Licht im infraroten Wellenlängenbereich von 850 bis 950 nm. Dieser optischen Lösung wird heute jedoch keine große Aufmerksamkeit gewidmet, da es keine WLAN-Produkte auf dem Markt gibt, die mit Infrarottechnologie arbeiten.

802.11b

Da man im WLAN-Bereich stetig höhere Datenraten anstrebt, wurde der IEEE-802.11-Grundstandard entsprechend erweitert beziehungsweise modifiziert. Dafür bildet das IEEE immer wieder Arbeitsgruppen, die die technische Erweiterung umsetzen. Eine Weiterentwicklung auf der PHY-Ebene stellt die IEEE-802.11b-Standarderweiterung, auch 802.11/HR (High Rate) genannt, dar, die am 9. Dezember 1999 verabschiedet wurde, wobei IEEE auf Entwicklungen von Harris und Lucent aufbaute. Im IEEE 802.11b ist ein entsprechender PHY definiert, der nach dem DSSS-Verfahren arbeitet und im 2,4-GHz-Frequenzband eine zusätzliche Datenrate von 5,5 und 11 MBit/s definiert. Somit konnte man jetzt brutto betrachtet dieselbe Datenrate erzielen wie in der Grundversion des drahtgebundenen Ethernets, das eine Datenrate von 10 MBit/s hat.

802.11a

Eine weitere Arbeitsgruppe verabschiedete am 16. September 1999 die IEEE-802.11a-Standarderweiterung, die ein WLAN mit einer

Datenrate von 6, 9, 12, 18, 24, 36 und 54 MBit/s im 5-GHz-Band spezifiziert. Hierbei wird allerdings nicht mehr nach dem DSSS-Verfahren gearbeitet, sondern nach dem Orthogonal-Frequency-Division-Multiplexing-Verfahren (OFDM).

802.11h

Hatten sich die Lösungen laut IEEE 802.11 und IEEE 802.11b seit der Jahrtausendwende in Europa schnell verbreitet, so verlief die Verbreitung von Produkten laut IEEE 802.11a dort eher schleppend. Zwar ist in Deutschland seit dem 13. November 2002 das 5-GHz-Frequenzband für die Nutzung einer breitbandigen Datenübertragung durch die RegTP (Regulierungsbehörde für Telekommunikation und Post) freigegeben, jedoch sind hierfür bei der 802.11a-Lösung gewisse Anpassungen erforderlich, um die Produkte in vollem Leistungsumfang betreiben zu können. Diese geforderten Anpassungen werden durch die 802.11h-Standarderweiterung umgesetzt, die am 11. September 2003 verabschiedet wurde. Wesentlicher Bestandteil der Standarderweiterung ist die Implementierung von TPC (Transmit Power Control) und DFS (Dynamic Frequency Selection). Da diese Standarderweiterung erst 2003 verabschiedet wurde und die Hersteller mit der Implementierung von TPC und DFS erst nachziehen mussten, ist die Verbreitung von 802.11a/h-Produkten bei uns heute eher noch gering. Zwar können 802.11a-Produkte auch ohne die genannten Anpassungen seit dem 13. November 2002 in Deutschland betrieben werden, jedoch nur mit drastischen Einschränkungen in der zulässigen Sendeleistung und der Anzahl der nutzbaren Kanäle (siehe Abschnitt 3.4.11). Erst durch die 802.11h-Erweiterung können die 5-GHz-WLAN-Produkte in vollem Leistungsumfang bei uns in Europa genutzt werden. Werden heute 802.11a-Produkte eingekauft, so sollte man sich beim Hersteller vergewissern, dass diese Produkte TPC und DFS unterstützen beziehungsweise sich durch einen Treiber oder ein Firmware-Update auf 802.11h erweitern lassen. Andernfalls läuft man Gefahr, dass diese Produkte nur mit eingeschränkter Leistung betrieben werden können.

802.11g

Eine weitere Standarderweiterung erfolgte am 12. Juni 2003 durch die 802.11g-Arbeitsgruppe. Mit 802.11g wurde ein weiterer Wireless Highspeed PHY definiert, der ebenfalls Datenraten von 6, 9, 12, 18, 24, 36 und 54 MBit/s ermöglicht. Wesentlicher Vorteil bei der 802.11g-Lösung ist die Tatsache, dass man hierbei nicht im 5-GHz-Frequenzband, sondern im 2,4-GHz-Band arbeitet. Diese Lösung kann demnach ohne die Implementierung von TPC und DFS betrieben werden. Einzige Voraussetzung hierbei ist, dass die Sendeleistung die zulässige Grenze des ISM-Bandes von 20 dBm (100 mW) nicht überschreitet. Demnach können die Produkte ohne Problem in Europa

betrieben werden. Das IEEE wollte mit der 802.11g-Lösung die schleppende Einführung der 802.11a/h-Lösung kompensieren und den Marktanforderungen einer WLAN-Highspeed-Lösung zeitlich gerecht werden. Es hat sich bestätigt, dass die 802.11g-Lösung besonders in Europa eine große Marktverbreitung erfahren hat.

Die Tabelle 1–1 zeigt die technische Gegenüberstellung der auf den PHY-Layer bezogenen Implementierungen des Grundstandards und der Erweiterungen.

Tab. 1–1 *Übersicht 802.11-PHY-Layer*

(Teil-)Standard	Datenraten	Übertragungs-verfahren	Frequenzband
IEEE 802.11	1 und 2 MBit/s	Optisch	Infrarot
IEEE 802.11	1 und 2 MBit/s	FHSS	2,4 GHz
IEEE 802.11	1 und 2 MBit/s	DSSS	2,4 GHz
IEEE 802.11a	6, 9, 12, 18, 24, 36 und 54 MBit/s	OFDM	5 GHz
IEEE 802.11b	5,5 und 11 MBit/s	DSSS	2,4 GHz
IEEE 802.11g	6, 9, 12, 18, 24, 36 und 54 MBit/s	OFDM	2,4 GHz
IEEE 802.11n[a]	Bis 600 MBit/s	OFDM	2,4 oder 5 GHz
IEEE 802.11ac[a]	Bis 6,9333 GBit/s	OFDM	5 GHz
IEEE 802.11ad[a]	Bis 6,75675 GBit/s	SC oder OFDM	60 GHz

a. Siehe folgende Abschnitte.

Neben den Erweiterungen auf der PHY-Ebene gibt es noch zahlreiche Standarderweiterungen, die der Sicherheit, der Implementierung von QoS (Quality of Service) sowie der Kommunikation zwischen den Access Points dienen. Teilweise sind diese Standarderweiterungen bereits verabschiedet oder werden zur Zeit von verschiedenen Arbeitsgruppen noch erarbeitet.

802.11d Die 802.11d-Erweiterung wurde am 14. Juni 2001 verabschiedet und ermöglicht einen Informationsaustausch zwischen den WLAN-Stationen und Access Points, mit deren Hilfe sich die Stationen automatisch auf die länderspezifischen Gegebenheiten, wie beispielsweise zulässige Sendeleistung und nutzbare Kanäle, einstellen können (siehe Abschnitt 4.8). Die 802.11d-Funktion ist besonders für international Reisende praktisch, deren WLAN-Karten sich automatisch anpassen können. Man spricht in diesem Zusammenhang auch von internationalem Roaming.

802.11e Durch die am 22. September 2005 verabschiedete 802.11e-Erweiterung werden Ergänzungen auf der MAC-Ebene vorgenommen, die

QoS-Fähigkeit und eine Performanceverbesserung implementiert, die für die Unterstützung zeitkritischer Anwendungen, wie beispielsweise die Sprachübertragung, notwendig sind (siehe Abschnitt 4.9).

802.11f

Die 802.11f-Standarderweiterung wurde am 12. Juni 2003 verabschiedet und definiert ein sogena nntes Inter Access Point Protocol (IAPP), das die Kommun ikation zwischen den Access Points vereinheitlicht (siehe Abschnitt 2.3).

802.11i

Die 802.11i-Standarderweiterung wurde am 24. Juni 2004 verabschiedet und sorgt für eine verbesserte und zeitgerechte Sicherheit für die per WLAN übertragenen Daten (siehe Kap. 10).

802.11n

Die 802.11n-Erweiterung wurde am 11. September 2009 verabschiedet. Sie beschreibt High-Throughput-Erweiterungen (siehe Kapitel 5), die auf dem PHY- und MAC-Layer definiert sind und Datenraten bis 600 MBit/s ermöglichen.

802.11ac

Im September 2008 nahm die sogenannte Very High Throughput Study Task Group ihre Arbeit auf. Diese Arbeitsgruppe soll die 802.11ac-Standarderweiterung definieren und verabschieden (siehe Kapitel 6). Ziel der 802.11ac-Arbeitsgruppe ist es, Erweiterungen auf der PHY- und MAC-Ebene zu definieren, die im 5-GHz-Band Datenraten bis 6,9333 GBit/s ermöglichen sollen. Das IEEE plant, die neue 802.11ac-Lösung Ende 2013 zu verabschieden.

802.11ad

Im Dezember 2008 begann die sogenannte Very High Throughput in the 60 GHz Band Study Task Group ihre Arbeit. Diese Arbeitsgruppe soll die 802.11ad-Standarderweiterung erarbeiten (siehe Kapitel 6). Diese Standarderweiterung soll neue PHY-Varianten und Erweiterungen auf der MAC-Ebene definieren, die im 60-GHz-Band Datenraten von 6,75675 GBit/s ermöglichen sollen. Das IEEE plant, die neue 802.11ad-Erweiterung bis Ende 2012 zu verabschieden.

802.11p

Die 802.11p-Arbeitsgruppe arbeitet an E rweiterungen auf der PHY-Ebene, die den drahtlosen Datenaustausch von Endgeräten, die auf Fahrzeugen montiert sind, optimieren soll.

802.11r

Die 802.11r-Arbeitsgruppe arbeitet an Erweiterungen auf der MAC-Ebene, die das Roaming, also Wandern zwischen verschiedenen Access Points verbessern sollen, was sich primär für VoIP-Anwendungen positiv auswirken soll. Einbußen in der Sp rachqualität und Gesprächsunterbrechungen sollen vermieden werden.

802.11s

Die 802.11s-Arbeitsgruppe definiert den Aufbau von sogenannten Wireless Mesh Networks. Sie werden beispielsweise bei der drahtlosen Gebäudevernetzung eingesetzt oder ermöglichen einfach den Verzicht drahtgebundener Verbindungen zwischen den Access Points. Mittelpunkt der 802.11s-Erweiterung wird die Definition eines Routing-Protokolls sein, das den Datenaustausch zwischen den redundanten Ver-

bindungswegen des Mesh-Netzwerks regelt und optimiert (siehe Abschnitt 2.7).

Tabelle 1–2 zeigt in der Übersicht die wichtigsten 802.11-Arbeitsgruppen und Standarderweiterungen.

Tab. 1–2 802.11-Arbeitsgruppen und -Standarderweiterungen

Arbeitsgruppen	Beschreibung
IEEE 802.11d	Bietet länderspezifischen Informationsaustausch für internationales Roaming
IEEE 802.11e	MAC-Erweiterung für die Implementierung von Quality of Service und einer Performanceverbesserung
IEEE 802.11f	Definition des Inter Access Point Protocols (IAPP)
IEEE 802.11i	MAC-Erweiterung zur Verbesserung der Datensicherheit
IEEE 802.11p	Optimierung für Datenaustausch auf Fahrzeugen
IEEE 802.11r	Optimierung des Roaming (Fast Roaming)
IEEE 802.11s	Definition eines drahtlosen Mesh-Netzwerks

1.3 Weitere Funklösungen

Neben der WLAN-Lösung, die durch das IEEE spezifiziert ist, gibt es weitere Funklösungen, die einen drahtlosen Datenaustausch ermöglichen. Hierbei handelt es sich um HiperLAN, HomeRF, Bluetooth, ZigBee und WiMax die nachfolgend im Überblick beschrieben werden.

1.3.1 HiperLAN

HiperLAN

HiperLAN steht für High Performance Radio Local Area Network, dahinter verbirgt sich eine weitere WLAN-Lösung, die von ETSI (European Telecommunications Standards Institute) ins Leben gerufen wurde. Die erste Version von HiperLAN wurde 1996 von ETSI durch den EN-300652-Standard spezifiziert und bot eine maximale Datenrate von 23,529 MBit/s. HiperLAN/1 arbeitet im 5-GHz-Frequenzband. Als Modulationsverfahren nutzt HiperLAN/1 das GMSK (Gaussian Minimum Shift Keying), das ebenfalls bei GSM-Mobilfunknetzen verwendet wird. Das Zugriffsverfahren ist dezentralistisch und basiert auf einem ständigen Informationsaustausch aller benachbarten Stationen. Hierbei ist vorgesehen, dass Routing-Tabellen dynamisch aufgebaut werden und eine Datenweiterleitung über mehrere Stationen hinweg ermöglicht wird.

HiperLAN/2

Im Jahr 1998 wurde eine neue Projektgruppe namens BRAN (Broadband Radio Access Network) ins Leben gerufen, um das Hiper-

LAN/2 zu en twickeln. Der Hi perLAN/2-Grundstandard wurde im Februar 2000 als ETSI Dokument TR 101 683 verabschiedet. HiperLAN/2 arbeitet ebenfalls im 5-GHz-Frequenzband und stellt eine maximale Datenrate von 54 MBit/s zur V erfügung. HiperLAN/2 unterscheidet sich g rundsätzlich von HiperLAN/1, wobei beispielsweise QoS unterstützt wir d. Man bezeichnet HiperLAN/2 deshalb auch oft als Wireless-ATM (Asynchronous Transfer Mode). HiperLAN/2 verwendet denselben PHY wie die IEEE-802.11a-Lösung und arbeitet nach dem OFDM-Verfahren. Anders als bei HiperLAN/1 wird bei HiperLAN/2 die Zugriffskontrolle über einen Access Point zentral verwaltet. Die Zugriffskontrolle basiert auf dem Time Division Multiple Access (TDMA) und dem Time Division Duplex (TDD) Verfahren, welche erlauben, dass mehrere Stationen gleichzeitig einen einzelnen Kanal ohne Interferenzen nutzen können (siehe Abschnitt 1.5.1). Dies wird ermöglicht, indem jede St ation einen sogenannten Zeitschlitz, bei HiperLAN/2 MAC-Rahmen genannt, vom Access Point zugeteilt bekommt. Diese Zuteilung findet unter der Berücksichtigung der einzelnen Dienstgüten (QoS) statt, wobei darauf geachtet wird, dass Verbindungen mit hohen Dienstgüteanforderungen begünstigt werden können. Jeder Rahmen wird sowohl für den Downlink als auch für den Uplink benutzt und weist eine Länge von 2 ms auf. Pro Rahmen werden in diesem Zeit raum bei einer OFD M-Symbollänge von 4 µs genau 500 OFDM-Symbole übertragen.

Entsprechende Schnittstellen zu Ethernet, IP und der dritten ATM-Version sind bei HiperLAN/2 zwecks Anbindung an drahtgebundene Infrastrukturen vorgesehen. Innerhalb geschlossener Gebäude können Distanzen von bis zu 30 m und außerhalb bis 150 m überbrückt werden. Als Verschlüsselungsverfahren sieht HiperLAN/2 das DES (Data Encryption Standard) oder 3-DES vor (siehe Kap. 10).

HiperACCESS

Neben HiperLAN/2 arbeitet BRAN zur Zeit an weiteren Lösungen, die die »Hiper-Familie« ergänzen sollen. Bei den beiden Lösungen handelt es sich um HiperACCESS und HiperLINK. HiperACCESS soll zukünftig die Überbrückung großer Entfernungen ermöglichen und ist technisch ein Verteilungsnetzwerk. Hierbei wird über eine Punkt-zu-Mehrpunkt-Verbindung eine Datenrate von bis zu 27 MBit/s ermöglicht. HiperACCESS arbeitet im 42-GHz-Frequenzband und soll dabei Entfernungen von bis zu 5 km überwinden können.

HiperLINK

HiperLINK soll Punkt-zu-Punkt-Verbindungen sowie im 17-GHz-Frequenzband eine Datenrate von 155 MBit/s unterstützen, wobei Distanzen von über 150 m überbrückt werden können. Hierdurch sollen sich beispielsweise zwei HiperLAN/2-Knoten miteinander verbinden lassen.

Auch wenn HiperLAN/1 ein großer Flop war und sich im Markt nie durchgesetzt hat, war die Euphorie bei HiperLAN/2, HiperACCESS und HiperLINK seinerzeit anfänglich erstaunlich groß. Firmen wie beispielsweise Philips, Panasonic und SONY hatten auf HiperLAN/2, HiperACCESS sowie HiperLINK aufgesetzt und arbeiteten an entsprechenden Produkten.

1.3.2 HomeRF

HomeRF

HomeRF (Home Radio Frequency) ist eine weitere WLAN-Lösung, die auf einem proprietären Industriestandard basiert und speziell für Privatanwender konzipiert ist. HomeRF zeichnet sich durch eine einfache Installation und preiswerte Produkte aus. Diese Lösung spielt jedoch heute keine große Rolle mehr, da sich die IEEE-802.11-Lösungen auch im Privatbereich durchgesetzt haben. Firmen wie Intel und Hewlett Packard haben deshalb ihre Aktivitäten im HomeRF-Bereich zugunsten von WLAN eingestellt. Bei HomeRF erfolgte eine asynchrone Datenübertragung im lizenzfreien 2,4-GHz-ISM-Band. Für Sprachübertragung wurden die Echtzeitmerkmale der gängigen DECT-Telefonie (Digital Enhanced Cordless Telecommunication) genutzt. Als Übertragungsverfahren stützte sich HomeRF auf das FHSS-Verfahren (siehe Abschnitt 3.2), wobei innerhalb des 2,4-GHz-Frequenzbandes 75 Kanäle im Abstand von 1 MHz genutzt werden. Die erste HomeRF Version 1.2 bot eine Datenrate von 1,6 MBit/s. Die zweite Version von HomeRF unterstützte bereits eine Datenrate von 10 MBit/s, wobei eine weitere Steigerung auf 20 MBit/s geplant war. Die 20 MBit/s sollen durch eine Kanalbündelung realisiert werden. Hierzulande gibt es nur wenige HomeRF-Produkte, die eine Zeit lang von der Deutschen Telekom oder Siemens vertrieben wurden.

1.3.3 Bluetooth

Bluetooth

Bei Bluetooth handelt es sich um eine Nahbereichsfunktechnologie, für kleinere Übertragungsstrecken bis etwa 10 m, die sich problemlos in Geräte jeglicher Bauart integrieren lässt. Der Grundsatz von Bluetooth, der bei den Bluetooth-Entwicklern im Vordergrund stand, war die Funkanbindung von mobilen oder feststehenden Geräten über geringe Distanzen. Bluetooth soll die Kabelanbindung zu den Peripherien ersetzen, wobei dies über eine robuste, wenige komplexe und kostengünstige Lösung erfolgen soll. Die eigentliche Bluetooth-Hardware ist somit sehr kompakt und zeichnet sich durch eine geringe Leistungsaufnahme aus, weshalb sich Bluetooth in portablen Geräten wie beispielsweise PDAs oder Handys problemlos implementieren lässt.

Special Interest Group

Bluetooth wurde im Jahr 1994 ins Leben gerufen, indem die Firma Ericsson eine Studie initiierte, mit dem Ziel, eine kostengünstige und stromsparende Lösung für die drahtlose Anbindung zwischen Mobiltelefonen und deren Zubehör zu finden. Die eigentliche Entwicklung von Bluetooth begann dann 1998, als sich fünf Unternehmen (Ericsson, Nokia, IBM, Intel und Toshiba) zusammenfanden und die Bluetooth Special Interest Group, kurz SIG, gründeten. Der Name Bluetooth wurde übrigens von einigen an der Entwicklung beteiligten Ingenieuren gewählt, die Fans von Harald Blåtand (Blauzahn) waren. Harald Blauzahn war im 10. Jahrhundert Wikingerkönig von Dänemark und hatte das Land mit Norwegen vereint. Die Namensfinder assoziierten die Vereinigung mit der nahtlosen Integration von Peripheriegeräten, die durch Bluetooth letztendlich ermöglicht werden soll.

802.15.1-Standard

Die Bluetooth SIG veröffentlichte im Juli 1999 die erste Bluetooth-Spezifikation mit der Version 1.0. Erste Bluetooth-Geräte kamen im Jahr 2000 in kleinen Stückzahlen auf den Markt. Im Februar 2001 folgte dann eine überarbeitete Spezifikation mit der Version 1.1 und im November 2003 die Version 1.2, auf der heute die meisten Bluetooth-Geräte basieren. Mittlerweile ist auch das IEEE auf Bluetooth aufmerksam geworden und hat einen zu Bluetooth kompatiblen IEEE-802.15.1-Standard verabschiedet. Dabei wurde der untere Bereich von Bluetooth, der im OSI-Referenzmodell in etwa mit der Bitübertragungsschicht vergleichbar ist, spezifiziert, damit sich dieser in die übrigen IEEE-802-Netzwerkstandards einordnen kann. Des Weiteren wurde von der SIG im November 2004 die Bluetooth-Spezifikation 2.0 + EDR (Enhanced Data Rate) verabschiedet, die Bluetooth zu einer Bruttodatenrate von bis zu 3 MBit/s verhilft.

Piconet

Bluetooth unterstützt Punkt-zu-Punkt- und Punkt-zu-Multipunkt-Verbindungen. Bluetooth-Geräte, die zueinander in Reichweite stehen, können eigenständig eine Kommunikationsverbindung aufbauen, ohne dass eine Konfiguration notwendig ist. Die Kommunikationspartner bilden dabei ein sogenanntes Pico net, das die einfachste Form einer Bluetooth-Kommunikation ist und räumlich betrachtet ein kleines Netzwerk darstellt. Innerhalb des Piconets übernimmt ein Blueto oth-Gerät die Rolle des Masters und das andere die Rolle als Slave. Grundsätzlich kann jedes Bluetooth-Gerät die Rolle als Master oder Slave übernehmen. Die Rollenzuteilung erfolgt zufällig und kann gegebenenfalls während einer laufenden Verbindung getauscht werden. Solange sich innerhalb eines Piconets nur ein Master und ein Slave gegenüberstehen, arbeitet Bluetooth im sogenannten Mono-Slave-Modus. Jedoch können bis zu sieben zusätzliche aktive Bluetooth-Geräte innerhalb

eines Piconets als Slave aufgenommen werden. Sind mehr als ein aktiver Slave innerhalb des Piconets vorhanden, so arbeitet Bluetooth im Multi-Slave-Modus. In diesem Fall wird der Kanal auf mehrere Slaves aufgeteilt. Die Kommunikation innerhalb des Piconets erfolgt grundsätzlich über den Master, eine direkte Verbindung zwischen den Slaves ist generell nicht möglich.

FHSS-Verfahren

Bluetooth arbeitet, wie der Großteil der WLAN-Lösungen, im lizenz- und genehmigungsfreien 2,4-GHz-ISM-Band. Als Übertragungsverfahren wird bei Bluetooth das FHSS-Verfahren angewendet. Die Sendeleistung von Bluetooth ist in drei Klassen unterteilt:

Klassen

- Klasse 1 mit 20 dBm (100 mW)
- Klasse 2 mit 4 dBm (2,5 mW)
- Klasse 3 mit 0 dBm (1 mW)

Heutige Bluetooth-Lösungen arbeiten in der Regel mit einer Sendeleistung von 0 dBm, wodurch eine Reichweite zwischen 10 cm und 10 m erzielt werden kann. Es gibt jedoch bereits auch Bluetooth-Lösungen für den Internetzugang, die nach der 1. Klasse arbeiten und Reichweiten von 100 m erzielen können. Diese Lösungen werden von den Herstellern auch gerne zur Vernetzung von PCs oder Notebooks angepriesen, jedoch bleibt hierbei trotz der 100 m der Nachteil, dass die maximal erzielbare Datenrate auf 1 MBit/s oder 3 MBit/s begrenzt ist. Eine wirkliche Konkurrenz zu WLAN stellt somit Bluetooth aus heutiger Sicht nicht dar. Es war natürlich auch nie die Absicht der Entwickler, Bluetooth als Netzwerklösung einzusetzen, sondern Bluetooth sollte ausschließlich eine ideale Lösung sein, um Peripherien an Geräte drahtlos anbinden zu können.

Zugriffsverfahren

Als Zugriffsverfahren nutzt Bluetooth das Time-Division-Duplex-Verfahren (TDD) mit einer Slotlänge von 625 µs. Die Daten werden als Pakete übertragen. Wobei bei der Paketübertragung, je nach Pakettyp, entweder ein Slot oder fünf Slots durch ein Bluetooth-Device belegt werden können.

Bluetooth-Bandbreite

Bluetooth überträgt die Daten entweder symmetrisch mit 433,9 kBit/s in beiden Richtungen oder asymmetrisch mit unterschiedlichen Bandbreiten für den Downstream und Upstream. Die unterschiedlichen Datenraten werden über bestimmte Kanäle bereitgestellt, wobei eine Verbindung entweder leitungs- oder paketorientiert sein kann. Bluetooth kann den Anwendungen entweder einen asynchronen Datenkanal oder bis zu drei simultane synchrone Sprachkanäle zur Verfügung stellen. Es besteht jedoch auch die Möglichkeit, einen asynchronen Datenkanal mit einem synchronen Sprachkanal zu kombinieren. Ein Sprachkanal kann eine Bandbreite von 64 kBit/s in beide Richtungen

bereitstellen. Der asynchrone Datenkanal kann in zwei unterschiedlichen Varianten zum Einsatz kommen. In der asymmetrischen Ausführung liefert er einen Downstream mit einer Bandbreite von 723,2 kBit/s und einen Upstream mit 57,6 kBit/s. Diese Ausführung lässt sich beispielsweise zum Surfen nutzen, bei dem man via DSL sowieso nur einen Downstream mit hoher Bandbreite und einen Upstream mit geringer Bandbreite bereitgestellt bekommt. In der symmetrischen Variante stellt der asynchrone Datenkanal eine Bandbreite von 433,9 kBit/s in beiden Richtungen bereit. Diese Variante eignet sich beispielsweise für Netzwerkanwendungen, bei denen ein Datenaustausch zwischen zwei Rechnern realisiert werden soll, um kleine Datenmengen auszutauschen.

Bluetooth-Geräte, die der Spezifikation 2.0 + EDR entsprechen, erzielen die höhere Bruttodatenrate durch die Verwendung der PSK-Modulation anstelle der GFSK-Modulation (siehe Kap. 3). Für die Datenrate von 2 MBit/s nutzt EDR pi/4DQPSK und für 3 MBit/s 8DPSK, wobei die Symbolrate mit 1 Millionen Symbole pro Sekunde, wie bei Bluetooth 1.0, 1.1 und 1.2, beibehalten wird. Auf diese Weise bleiben die wesentlichen Eigenschaften der älteren Bluetooth-Versionen erhalten und somit auch die Abwärtskompatibilität zu den bisherigen Bluetooth-Geräten.

1.3.4 ZigBee

ZigBee

Als Funktechnik für Steuerungs- und Überwachungssysteme sowie für die Vernetzung von intelligenten Sensoren bahnt sich eine neue Funktechnologie an, die den Namen ZigBee trägt. Mit Hilfe von ZigBee lassen sich WPANs realisieren, deren Anwendungsspektrum von der Heim- und Gebäudeautomatisierung, Industrie und Automatisierungstechnik, Spedition und Logistik, Medizintechnik bis hin zur Bedienung von Computer-Peripherie und Unterhaltungselektronik reicht. ZigBee baut auf der IEEE-Spezifikation 802.15.4 auf und zeichnet sich durch eine hohe Zuverlässigkeit, geringe Kosten, geringe Leistungsaufnahme, geringe Datenrate und hohe Sicherheit aus. Für die Datenübertragung kommen verschiedene Frequenzbereiche in Betracht, wobei in Europa das 2, 4-GHz-ISM-Band genutzt werden kann, auf dem 16 Kanäle und eine Datenrate von 250 kBit/s bereitgestellt werden können und zusätzlich ein 868-MHz-Band, bei dem über einen Kanal die Bandbreite von 20 kBit/s zur Verfügung stehen. ZigBee ist in der Lage automatisch nach freien Kanälen zu suchen, wodurch eine Koexistenz zu anderen Funktechnologien gewährleistet werden soll. Die Netzwerktopologie stützt sich vornehmlich auf eine Mesh- und Tree-Topo-

logie, über die redundante Übertragungspfade bereitgestellt werden können, wodurch die Datenübertragung besonders zuverlässig sein soll. Die Reichweite liegt je nach verwendeter Sendeleistung zwischen 10 m und 75 m, wobei über ein ausgeklügeltes Powermanagement mit kurzen Aktivitätszeiten eine hohe Lebensdauer für die Batterie erreicht wird, sodass beispielsweise batteriebetriebene Sensoren eine lange Betriebszeit aufweisen können. ZigBee zeichnet sich weiterhin dadurch aus, dass für eine fehlerfreie Datenübertragung nur ein geringer Signal-Rausch-Abstand benötigt wird, sodass ZigBee auch in rauen Industrieumgebungen eine zuverlässige Datenübertragung bietet.

1.3.5 WiMax

WiMax

Wireless Interoperability for Microwave Access (WiMax) steht für eine weitere Funktechnologie, die in der Grundversion unter dem IEEE-802.16a-Standard spezifiziert ist. Die Umsetzung von WiMax ist in verschiedenen Ausbaustufen geplant. Die erste Ausbaustufe sieht die Versorgung von Gebäuden mit schnellen Internetzugängen über externe Antennen vor. Die zweite Ausbaustufe soll den Einsatz von Indoor-Antennen ermöglichen, und in der dritten Ausbaustufe soll WiMax die Anbindung von mobilen Endgeräten wie Notebooks und Mobiltelefonen ermöglichen. Die verschiedenen Ausbaustufen werden über entsprechende 802.16-Standarderweiterungen spezifiziert. WiMax entspricht also einer Weitverkehrsfunktechnik, über die breitbandige und drahtlose MANs (Metropolitan Area Networks) aufgebaut werden können, die es den Netzbetreibern ermöglichen, die letzte Meile zum Verbraucher abzudecken. Die neue Funktechnologie könnte somit zukünftig besonders in ländlichen Gegenden interessant sein, in denen drahtgebundene Internetanbindungen fehlen, aber zukünftig sich auch als mögliche Konkurrenz zu UMTS etablieren. WiMax verspricht Datenraten von bis zu 70 MBit/s und maximale Reichweiten von bis zu 50 km. Hierbei handelt es sich um theoretische Spitzenwerte, die nur bei stationären Endgeräten und direkten Sichtverbindungen erzielt werden können. Bei mobilen Endgeräten sieht es gänzlich anders aus, denn WiMax unterliegt ebenfalls den Gesetzen der Physik. Bei sogenannten Non-Line-of-Sight-Verbindungen, also ohne direkte Sichtverbindung, verringert sich die erzielbare Datenrate auf 20 MBit/s und die Reichweite auf etwa 600 m. Als Frequenzbereich ist in Deutschland der Bereich von 3,4 bis 3,6 GHz und von 2,5 bis 2,69 GHz vorgesehen.

1.4 WLAN-Rechtsgrundlagen

WLAN-Rechtsgrundlagen

Der Einsatz von funkbasierten IEEE-WLANs erfolgt in der Regel im 2,4-GHz-ISM-Band oder 5-GHz-Frequenzband, die von IEEE 802.11 festgelegt sind. Die Nutzung von Frequenzen beziehungsweise Frequenzbändern ist international durch verschiedene Stellen ger egelt. Der verwendete Frequenzumfang der einzelnen Frequenzbänder ist international festgelegt und steht nicht überall im gleichen Umfang zur Verfügung: Von Nation zu Nation variieren die nutzbaren Unterbänder. Folgende Institutionen oder Regulierungsbehörden sind für Freigabe und Aufteilung der 2,4-GHz- und 5-GHz-Frequenzbänder innerhalb Europas, den USA und Japan zuständig (siehe Tab. 1–3).

Tab. 1–3
Institutionen, die standortabhängig für die Freigabe der Frequenzbänder zuständig sind

Standort	Frequenz band	Institution	Norm
Europa	2,4 GHz	European Telecommunications Standards Institute (ETSI)	EN ETSI 300-328
Frankreich	2,4 GHz	European Telecommunications Standards Institute (ETSI)	SP/DGPT/ATAS/23, EN ETSI 300-328
Spanien	2,4 GHz	European Telecommunications Standards Institute (ETSI)	EN ETSI 300-328
Europa	5 GHz	European Telecommunications Standards Institute (ETSI)	EN ETSI 301-893
USA	2,4 GHz	Federal Communications Commission (FCC)	CFR47, Part 15, Sections 15.205, 15.209, 15.247
USA	5 GHz	Federal Communications Commission (FCC)	CFR47, Part 15,sections 15.205 and 15.209; and Subpart E, sections 15.401–15.407
Japan	2,4 GHz	Association of Radio Industries and Businesses (ARIB)	RCR STD-33A
Japan	5 GHz	Ministry of Post and Telecommunication (MPT)	MPT Ordinance for Regulating Radio Equipment, Article 49.20

Bundesnetzagentur

In Deutschland ist die Bundesnetzagentur unter anderem für die Frequenzordnung und für die Überwachung der Frequenzbänder zuständig. Die Bundesnetzagentur erhielt am 13. Juli 2005 ihren Namen, als die Regulierungsbehörde für Telekommunikation und Post (RegTP), die am 1. Januar 1998 aus dem Bundesministerium für Post und Telekommunikation (BMPT) und dem Bundesamt für Post und Telekom-

munikation (BAPT) hervorging, umbenannt wurde. Die Bundesnetzagentur ist unter folgender Adresse erreichbar:

- Bundesnetzagentur für Elektrizität, Gas,
  Telekommunikation, Post und Eisenbahnen
  Tulpenfeld 4 · 53113 Bonn
  http://www.Bundesnetzagentur.de
  Tel.: 0228/14-0
  Fax: 0228/14 8872

Verfügung 89/2003

Für die Bundesrepublik ist innerhalb des ISM-Bandes der WLAN-Betrieb genehmigungs- und gebührenfrei. Mit der Verfügung 122/1997 im Amtsblatt 14/1997 vom BMPT wird der Betrieb von drahtlosen 2,4-GHz-Datenfunkanlagen seit dem 21. Mai 1997 geregelt. Im November 1999 ist diese Amtsblattverfügung durch die Verfügung 154/1999 im Amtsblatt 22/1999 abgelöst worden, die durch die RegTP veröffentlicht wurde. Aktuell gilt die Verfügung 89/2003, die am 17. Dezember 2003 im Amtsblatt 25/2003 von der RegTP veröffentlicht wurde. WLANs gelten als nichtöffentliche Anwendungen; die eingesetzten 2,4-GHz-Systeme müssen lediglich dem 1994 durch das europäische Standardisierungsinstitut für Telekommunikationsangelegenheiten ETSI (European Telecommunications Standards Institute) verabschiedeten Standard ETS 300-328 entsprechen. Für die 5-GHz-Produkte muss der ETSI-Standard EN 301-893 berücksichtigt werden. Das 5-GHz-Frequenzband ist durch RegTP mit Verfügung 35/2002 im Amtsblatt 22/2002 seit dem 13. November 2002 für die breitbandige Datenübertragung ebenfalls freigegeben worden. Die Regulierung der 5-GHz-Bänder ging allerdings bislang innerhalb der EU nur schleppend voran. Dies soll sich durch einen Beschluss ändern, der am 14. Juli 2005 in Brüssel gefasst wurde. Laut diesem Beschluss wurden die Mitgliedsstaaten aufgefordert, den 5-GHz-Bereich (5150-5350 MHz und 5470-5725 MHz) bis zum 31. Oktober 2005 nun endlich EU-weit einheitlich zu regulieren.

Zulässige Sendeleistungen

Die beiden Standards ETS 300-328 und EN 301-893 regeln jeweils die technischen Voraussetzungen und Zulassungskriterien für Datenfunksysteme im entsprechenden Frequenzband. Im Wesentlichen betrifft dies die Aufteilung des vorhandenen Frequenzbandes in einzelne Kanäle und die maximal zulässige Sendeleistung, die im 2,4-GHz-ISM-Band auf 20 dBm (100 mW) und im 5-GHz-Frequenzband auf 23 dBm (200 mW) oder 30 dBm (1 W) begrenzt ist. Damit im 5-GHz-Band die maximalen Sendeleistungen verwendet werden dürfen, ist jedoch die Implementierung von TPC und DFS vorausgesetzt (siehe Abschnitt 3.4.11, 4.6.8 und 4.6.9). Um eine Zulassung zu erhalten, muss ein Her-

steller die Einhaltung der in ETS 300-328 beziehungsweise EN 301-893 vorgeschriebenen Kriterien durch ein Zeugnis eines unabhängigen und zugelassenen Testlabors nachweisen. In Deutschland unterliegen die WLAN-Einrichtungen allgemein den Gesetzen über Funkanlagen und Telekommunikationseinrichtungen (FTEG) und den Gesetzen über die elektromagnetische Verträglichkeit von Geräten (EMVG).

1.4.1 Grundstücksübergreifende Datenübertragung

Grundstücksübergreifende Datenübertragung

Die geltenden Verfügungen ersetzen die bisher gültige Allgemeingenehmigung für Funkanlagen bei der Breitband-Datenübertragung innerhalb der Grenzen eines Grundstücks durch eine allgemein gültige Zuteilung. Sie regelt sowohl die Anwendung solcher Datenfunkanlagen im grundstücksübergreifenden Bereich als auch für den Betrieb innerhalb eines Grundstücks. Bis dahin war es nicht erlaubt, Daten über die Grenzen privater Grundstücke hinweg zu übertragen. Mit dem Erlass dieser Verfügungen ist es nun jedermann gestattet, solche grundstücksübergreifenden Übertragungen zu installieren und zu nutzen. Die Installation der Anlagen geschieht durch den Betreiber selbst, eine Abnahme durch die Bundesnetzagentur oder andere Stellen ist nicht vorgeschrieben. Nach der bisherigen Verfügung 154/1999 war für die Errichtung einer grundstücksübergreifenden 2,4-GHz-Übertragungseinrichtung eine formlose Mitteilung an die RegTP notwendig, die Angaben über den Standort und technische Eckdaten beinhaltete. Die Meldepflicht wurde in Deutschland mit der Veröffentlichung der Verfügung 89/2003 aufgehoben. Somit ist eine Meldung heute nicht mehr notwendig.

BFWA

Die Bundesnetzagentur hat am 30. August 2007 mit der Verfügung 47/2007 einen zusätzlichen Bereich des 5-GHz-Bandes für die Nutzung freigegeben. Dieser Bereich liegt von 5,755 GHz bis 5,875 GHz und ist ausschließlich für den so genannten Broadband Fixed Wireless Access (BFWA) vorgesehen, der mit einer bis zu 36 dBm (4000 mW) mittleren äquivalenten isotropen Strahlungsleistung (EIRP, siehe Abschnitt 7.3.4) arbeiten darf. Darunter fallen ortsfeste Funkstrecken mit hoher Reichweite. Diese Freigabe ist ausschließlich für Internet-Provider bestimmt, die auf dessen Basis den Breitbandausbau in ländlichen Regionen durchführen und gewerblich umsetzen. Eine private Nutzung, beispielsweise für die Vernetzung von unterschiedlichen Firmenstandorten, ist nicht zulässig. Der freigegebene Frequenzbereich darf unter Einsatz von TPC und DFS verwendet werden. Der Betrieb von BFWA-Funkstrecken ist genehmigungsfrei, muss jedoch gemäß §6 des Telekommunikationsgesetzes (TKG) angemeldet

werden. Ein entsprechendes Meldeformular kann unter dem folgenden Link heruntergeladen werden:

- *http://www.bundesnetzagentur.de/cln_1931/DE/Sachgebiete/Telekommunikation/RegulierungTelekommunikation/Meldepflicht/Meldepflicht_Basepage.html.*

1.4.2 Rechtgrundlage für Hotspots

Rechtsgrundlage für Hotspots

Innerhalb Deutschlands ist die Telekommunikationsdienstleistung durch das aktuelle Telekommunikationsgesetz (TKG) vom 22. Juni 2004 geregelt, das zuletzt durch Artikel 2 des Gesetzes vom 24. März 2011 (BGBl. I S. 506) geändert worden ist. Laut § 6 des TKGs besteht eine Meldepflicht, wenn gewerblich öffentliche Telekommunikationsnetze oder gewerblich Telekommunikationsdienste angeboten werden. Unter diesen Paragrafen fallen auf jeden Fall auch WLAN-Hotspots, die öffentlich mit gewerblichen Absichten betrieben werden. Früher war die Meldepflicht daran gebunden, ob eine Telekommunikationsdienstleistung grundstücksübergreifend angeboten wird, diese Festlegung ist nach aktueller Gesetzeslage gänzlich entfallen. Die Einstufung als gewerblich erfolgt unabhängig von der Gewinnerzielungsabsicht, sondern es reicht aus, wenn die Telekommunikationsdienstleistung mit der Absicht der Kostendeckung der Öffentlichkeit angeboten wird. Als Öffentlichkeit wird jeder unbestimmte Personenkreis betrachtet. Nach der Gewerbeverordnung handelt jemand gewerblich, wenn er eine Tätigkeit selbständig, regelmäßig und in der Absicht betreibt, einen Ertrag oder sonstige wirtschaftliche Vorteile zu erzielen. Somit kann die Bindung der Meldepflicht an die gewerbliche Gewinnerzielungsabsicht gegebenenfalls Grenzfallbetrachtungen hervorrufen. Einem Bistrobetreiber könnten beispielsweise streng genommen Gewinnerzielungsabsichten unterstellt werden, wenn er einen gebührenfreien Hotspot betreibt und dadurch die Verweildauer seiner Gäste erhöht, um den Umsatz an Getränken und Speisen entsprechend zu steigern.

Meldepflicht

Die Meldepflicht dient dazu, der Bundesnetzagentur die Möglichkeit zu geben, ein Verzeichnis der Betreiber öffentlicher Telekommunikationsnetze und der Anbieter gewerblicher Telekommunikationsdienste zu erstellen und für die Öffentlichkeit anzubieten. Des Weiteren dient die Meldepflicht der Regulierungsbehörde für die Überwachung der Tätigkeit auf dem Telekommunikationsmarkt und die Auferlegung von Verpflichtungen nach dem TKG. Laut TKG sind die Aufnahme, Änderung und Beendigung der Tätigkeit sowie Änderungen der Firma unverzüglich und schriftlich bei der Regulierungsbe-

hörde zu melden. Für die Meldung stellt die Bundesnetzagentur auf ihrer Homepage ein achtseitiges Meldeformular bereit, das als PDF-Datei unter folgendem Link zum Download bereitsteht:

- *http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/Meldepflicht/MeldeformularFebr2012pdf.pdf*

Das ausgefüllte Meldeformular ist an folgende Dienststelle zu senden:

- Bundesnetzagentur für Elektrizität, Gas,
  Telekommunikation, Post und Eisenbahnen
  Referat 513-7
  Liselotte-Herrmann-Straße 20a · 09127 Chemnitz

Die Meldung selbst ist für den Betreiber erst einmal nicht mit Kosten verbunden. Eine unterlassene, nicht rechtzeitige oder unvollständige Meldung kann jedoch nach § 148 (1) Nr. 2 TKG mit einem Bußgeld von bis zu 10.000 € geahndet werden.

Des Weiteren kann dem WLAN-Hotspot-Betreiber laut § 144 TKG von der Bundesnetzagentur ein jährlicher Telekommunikationsbeitrag in Rechnung gestellt werden. Der Telekommunikationsbeitrag soll einen Beitrag für die Finanzierung der Bundesnetzagentur liefern. Derzeit gibt es hierzu allerdings noch keine Gebührenverordnung, jedoch beabsichtigt die Bundesnetzagentur zukünftig den jährlichen Telekommunikationsbeitrag einzufordern. Die Höhe des jährlichen Telekommunikationsbeitrags ist im Moment also noch völlig unklar, soll aber voraussichtlich umsatzgebunden sein.

Schutzmaßnahmen

Betreibt man einen meldepflichtigen Hotspot, so ist es jedoch mit der Meldepflicht und den eventuell jährlich anfallenden Telekommunikationsgebühren alleine nicht getan, denn der Betreiber muss zusätzlich technische Schutzmaßnahmen gemäß § 109 TKG treffen. Die Schutzmaßnahmen müssen sicherstellen, dass personenbezogene Daten geheim gehalten, unerlaubte Netzzugriffe verhindert und Störungen, welche die Netzfunktionsfähigkeit beeinträchtigen können, abgewehrt werden. Hierzu muss der Betreiber alle erforderlichen, ihm möglichen und zumutbaren technischen Vorkehrungen treffen. Inwieweit technische Vorkehrungen und sonstige Schutzmaßnahmen als angemessen betrachtet werden können, lässt das TKG allerdings offen. Im TKG ist lediglich der Passus verankert, dass die Vorkehrungen und sonstigen Schutzmaßnahmen als angemessen betrachtet werden, wenn der dafür erforderliche technische und wirtschaftliche Aufwand in einem angemessenen Verhältnis zur Bedeutung der zu schützenden Rechte und zur Bedeutung der zu schützenden Einrichtungen für die Allgemeinheit

steht. Ein WLAN-Hotspot-Betreiber sollte in diesem Zusammenhang auf jeden Fall sicherstellen, dass die Daten über aktuell verfügbare Sicherheitsverfahren wie beispielsweise WPA(2) geschützt sind. Eine WEP-Verschlüsselung wird heute sicher nicht mehr als ausreichende Schutzmaßnahme betrachtet.

Sicherheitskonzept

Des Weiteren schreibt das TKG vor, dass derjenige, der Telekommunikationsdienste für die Öffentlichkeit anbietet, eine(n) Sicherheitsbeauftragte(n) zu benennen hat und ein Sicherheitskonzept erstellen muss. Welche Qualifikationen ein(e) Sicherheitsbeauftragte(r) haben muss und welche Aufgaben mit der Benennung verbunden sind, ist im TKG allerdings nicht geregelt. Aus dem Sicherheitskonzept muss jedoch hervorgehen, welche Telekommunikationsanlagen eingesetzt und welche Telekommunikationsdienste für die Öffentlichkeit erbracht werden, von welchen Gefährdungen auszugehen ist und welche technischen Vorkehrungen oder sonstigen Schutzmaßnahmen zur Erfüllung der Verpflichtungen aus dem TKG getroffen oder geplant sind. Das Sicherheitskonzept ist der Bundesnetzagentur unverzüglich nach Aufnahme der Telekommunikationsdienste vom Betreiber vorzulegen, verbunden mit einer Erklärung, dass die darin aufgezeigten technischen Vorkehrungen und sonstigen Schutzmaßnahmen umgesetzt sind oder unverzüglich umgesetzt werden. Werden von der Bundesnetzagentur anhand des Sicherheitskonzeptes Sicherheitsmängel festgestellt, so kann sie vom Betreiber die unverzügliche Beseitigung verlangen.

Da die aktuelle Gesetzeslage einige Interpretationsfreiräume zulässt, sollte man die Meldepflicht und die Notwendigkeit der Schutzmaßnahmenimplementierung auf jeden Fall prüfen, falls man einen öffentlichen Hotspot betreiben möchte. Dasselbe gilt für die aktuellen Entwicklungen über die mögliche Erhebung der jährlichen Telekommunikationsgebühren.

Internetzugang

Auch sollte man im Vorfeld prüfen, welcher Internetzugang für die Umsetzung eines Hotspots auch tatsächlich geeignet ist. Viele Restaurantbetreiber möchten beispielsweise ihren Gästen eine Zusatzdienstleitung in Form eines Hotspots anbieten. Dahinter steht die Überlegung, eine DSL-Flatrate anzumieten, diesen preisgünstigen Internetzugang mit einem Wireless Router zu erweitern und auf diese Weise den Hotspot kostengünstig bereitzustellen. Jedoch muss man hierbei berücksichtigen, dass es heute noch Internet-Provider gibt, die in ihren Nutzungsbestimmungen die Bereitstellung des Internetzugangs für die Öffentlichkeit oder eine Mehrfachnutzung verbieten. Diese Einschränkung kann bei der Anmietung des Internetzugangs auf Basis einer kostengünstigen Flatrate vorhanden sein. Hier verfahren die Internet-Provider jedoch sehr unterschiedlich, weshalb auf jeden Fall

eine Prüfung der Vertragsbedingungen im Vorfeld erfolgen sollte. Die genannte Einschränkung entfällt in der Regel bei der Anmietung eines Profitarifes.

Ein weiterer zu berücksichtigender Aspekt bei der Einrichtung eines Hotspots ist die Tatsache, dass der Vertragspartner eines Internet-Providers für den Inhalt der über den bereitgestellten Internetzugang übertragenen Daten gegenüber dem Provider erst einmal verantwortlich ist. Nach § 9 TKG ist der Betreiber eines geteilten Netzzuganges zwar nicht für das rechtliche Fehlverhalten der übrigen Benutzer verantwortlich, jedoch muss der Betreiber im Zweifelsfall nachweisen können, dass eine andere Person den Netzzugang missbraucht hat. Hackerangriffe sowie die Übertragung von rechtsradikalen und pornografischen Inhalten sind hier denkbar. Dies ist besonders kritisch, wenn der Internetzugang über den Hotspot lange zur Verfügung steht und unbeobachtet genutzt werden kann, wie beispielsweise in Hotelzimmern. In diesem Fall kann eine personenbezogene Protokollierung der Zugriffszeiten bei einer späteren strafrechtlichen Verfolgung durch die Staatsanwaltschaft im Sinne des juristischen Schutzes hilfreich sein. Bisher sind zwar noch keine Präzedenzfälle bekannt, die strafrechtlich verfolgt und gerichtlich entschieden wurden. Jedoch hat uns das Zeitalter des Internets schon viele Fälle aufgezeigt, und es ist nicht auszuschließen, dass auch Hotspots ein Potenzial für kriminelle Handlungen bieten. Technisch lässt sich die personenbezogene Protokollierung über eine Authentifizierung realisieren, bei der bestimmte Accounts zugrunde gelegt werden, die vorher personenbezogen verteilt werden.

1.5 Drahtlos versus drahtgebunden

Drahtlose Datenübertragung

Vergleicht man die drahtgebundene mit der drahtlosen Datenübertragung, so muss man allgemein festhalten, dass der drahtlose Datenaustausch in der Umsetzung technisch aufwändiger ist. Dies liegt darin begründet, dass die Daten während der Übertragung gewissen Randbedingungen ausgesetzt sind, gegen die die übertragenen Daten geschützt werden müssen. Weiterhin gibt es bei der drahtlosen Datenübertragung keine Abgrenzung, wohingegen bei dem drahtgebundenen Datenaustausch eine fast hundertprozentige Abgrenzung über das Datenkabel erfolgt. Unterschiede sind im Wesentlichen in der Störanfälligkeit, der Sicherheit und der erzielbaren Datenrate vorhanden.

Störungen

Die Daten sind bei der drahtlosen Übertragung wesentlich störanfälliger, denn jede elektromagnetische Störung kann das übertragene Signal nachhaltig beeinflussen. Als Störungen kommen elektromag-

netische Störquellen in Frage, die beispielsweise durch größere Maschinen mit hoher Leistungsaufnahme generiert werden können. So können laufende Elektromotoren oder Schaltkontakte in Relais oder Schütze Störungen hervorrufen. Aber auch benachbarte Datenübertragungseinrichtungen, die auf demselben oder benachbarten Frequenzband arbeiten, können die Datenübertragung negativ beeinflussen. Demnach müssen bei den drahtlosen Übertragungseinrichtungen entsprechende Fehlererkennungsmechanismen implementiert sein, die Übertragungsfehler erkennen oder sogar beseitigen können. Fehlerhaft übertragene Daten müssen unter Umständen erneut übertragen werden, wodurch die Performance sinken kann.

Durch die fehlende Abgrenzung kann theoretisch jeder, der sich in der Reichweite eines drahtlosen Datenübertragungssystems befindet, die Daten abhören, manipulieren oder fremde Daten in das System einbringen. Deshalb müssen bestimmte Mechanismen greifen, um dieses Sicherheitsrisiko zu minimieren oder gänzlich auszuschließen. In der Praxis werden die Daten deshalb in der Regel verschlüsselt übertragen, wodurch die Daten zwar weiterhin abgehört werden können, jedoch ohne Kenntnis des geheimen Schlüssels nicht ausgewertet werden können. Die Sicherheitsmechanismen benötigen in der Regel eine Rechenleistung, wodurch eine gewisse Prozessorleistung des Systems benötigt wird. Weiterhin kann durch die Sicherheitsmechanismen bei der Datenübertragung ein Overhead entstehen, wodurch die Nettodatenrate sinkt.

Datenraten

Anfänglich ließen sich bei der drahtlosen gegenüber der drahtgebundenen Datenübertragung nur vergleichsweise niedrigere Datenraten erzielen, da man in den vorhandenen Frequenzbändern nur geringe Bandbreiten zur Verfügung hat. Letztere ergeben sich aus der Tatsache, dass die vorhandenen Frequenzbänder auf mehrere Nutzer beziehungsweise Dienste aufgeteilt werden müssen. Möchte man hohe Datenraten erzielen, so erfordert dies in der Regel komplexere Verfahren, die aufwändiger in der Implementierung sind und einen höheren Leistungsverbrauch bedingen. Dieser wirkt sich bei mobilen Systemen nachteilig aus, da diese meist mit Akkus oder Batterien betrieben werden, deren Kapazität begrenzt ist. Die im Verhältnis zu den drahtgebundenen Lösungen geringeren Datenraten, die bei der drahtlosen Datenübertragung erzielt werden können, sind somit der Preis für Mobilität und Flexibilität. Mittlerweile ist die Technik jedoch so weit vorangeschritten, dass auch hier Datenraten erzielt werden können, die oberhalb der 100 MBit/s-Grenze liegen. Deshalb stellen WLAN-Lösungen zunehmend einen Ersatz für die drahtgebundenen Netzwerke dar. Sie haben sich als sinnvolle Ergänzung etabliert, die immer dann eingesetzt wer-

den kann, wenn Mobilität und Flexibilität gefragt sind. Zudem gibt es häufig Standorte, an denen eine herkömmliche Netzwerkverkabelung nicht installiert werden kann und die man somit gewerblich nicht erschließen könnte. Typische Beispiele hierfür sind denkmalgeschützte und historische Gebäude.

1.5.1 Multiple-Access-Problematik

Multiple-Access-Problem

Bei der drahtlosen Datenübertragung muss man die Tatsache berücksichtigen, dass das Funkmedium innerhalb eines Empfangsbereichs ein Shared Media darstellt, woraus sich zwangsweise ein Multiple-Access-Problem ergibt. Der Unterschied zu dem drahtgebundenen Shared Media liegt jedoch darin, dass viele potenzielle Anwender auf das Funkmedium zugreifen können. Bei drahtgebundenen Netzwerken können nur die Komponenten auf das Medium zugreifen, die direkt an das Netzwerk angeschlossen sind. Die Anzahl der potenziellen Benutzer ist jedoch beim Funkmedium theoretisch unbegrenzt, eine Einschränkung kaum möglich. In der Nachrichtentechnik kennt man vier grundsätzliche Verfahren, um dem Multiple-Access-Problem entgegenzuwirken:

- Time Division Multiple Access, kurz TDMA. *TDMA*
  Über ein Zeitmultiplexverfahren wird jedem Benutzer für eine bestimmte Dauer das Übertragungsmedium zur Datenübertragung zugeteilt. Die Dauer richtet sich nach einer festgelegten Zeitscheibe.
- Frequency Division Multiple Access, kurz FDMA. *FDMA*
  Mit Hilfe des Frequenzmultiplexverfahrens wird die Bandbreite des zur Verfügung stehenden Frequenzbandes in disjunkte Kanäle unterteilt. Jedem Benutzer steht dauerhaft ein eigener Kanal für die Datenübertragung zur Verfügung.
- Code Division Multiple Access, kurz CDMA. *CDMA*
  Bei diesem Verfahren werden die Daten beim Senden über einen Code verschlüsselt, um eine Abgrenzung zwischen unterschiedlichen Systemen zu erzielen. Nur die Empfänger mit demselben Code können die empfangenen Daten wieder entschlüsseln. Bei der Verschlüsselung handelt es sich jedoch nicht um eine Datenverschlüsselung im Sinne der Kryptographie, sondern um ein Verfahren, das dem Multiple-Access-Problem entgegenwirken soll.
- Space Division Multiple Access, kurz SDMA. *SDMA*
  SDMA ist ein Raummultiplexverfahren, bei dem die beschränkte Reichweite der übertragenen Signale zugrunde gelegt wird. Ab einer bestimmten Reichweite ist beispielsweise das Signal einer

elektromagnetischen Welle so stark abgeschwächt, dass ein System auf demselben Kanal betrieben werden kann, ohne das andere System zu stören.

Zudem ist bei der drahtlosen Datenübertragung die Anzahl von potenziellen Störungen relativ groß. Bei einem drahtgebundenen Übertragungsmedium können Störungen bereits wirkungsvoll verhindert werden, indem man Störern den Zugang zum Netzwerkkabel verweigert. Da das genutzte Frequenzband des WLANs lizenz- und genehmigungsfrei ist, ist die Wahrscheinlichkeit relativ hoch, dass Störungen allein durch andere technische Einrichtungen entstehen, die dasselbe Frequenzband nutzen. Ein klassisches Beispiel dafür sind die Mikrowellengeräte, die mit relativ hoher Leistung ebenfalls im 2,4-GHz-Frequenzband arbeiten. Demnach müssen für die technische Umsetzung von WLANs Lösungen angewendet werden, die eine fehlerfreie Datenübertragung dennoch gewährleisten.

Spread-Spektrum-Technologie

Die Lösung dieses Problems liegt in der sogenannten Spread-Spectrum-Technologie (SST). Ursprünglich hatte das Militär die Spread-Spectrum-Technologie mit dem Ziel entwickelt, eine störunempfindliche und verschlüsselte Datenübertragung zu realisieren. Mittlerweile wird sie aber in großem Ausmaß in der zivilen Nachrichtentechnik eingesetzt. Über die Spread-Spectrum-Technologie wird das schmalbandige Nutzsignal gespreizt, wodurch man die Informationseinheiten über einen größeren Frequenzbereich überträgt, als für die eigentliche Informationsübertragung nötig wäre. Hierdurch wird das übertragene Signal unempfindlicher gegen Störer, da diese über einen größeren Frequenzbereich auftreten müssten, um die Information zu vernichten. Störer sind allgemein schmalbandig, demnach können sie nur einen Teil der gespreizten Nutzinformation nachhaltig beeinflussen.

DSSS versus OFDM

Auf der physikalischen Ebene der IEEE-WLAN-Lösungen wird vorwiegend entweder die Direct-Sequence-Spread-Spectrum-Technologie (DSSS) oder die Orthogonal-Frequency-Division-Multiplexing-Technologie (OFDM) angewendet. Bei beiden Verfahren handelt es sich letztendlich um eine Kombination von TDMA, FDMA und CDMA. Zudem wird im WLAN-Bereich mit den geringen Sendeleistungen das SDMA-Verfahren ausgenutzt, um eine mehrfache Kanal- beziehungsweise Frequenznutzung zu ermöglichen.

In Kapitel 3 wird ausführlich auf das DSSS- und OFDM-Verfahren eingegangen.

1.5.2 Modulationsverfahren

Modulationsverfahren

Bei der drahtlosen Datenübertragung werden die Nutzinformationen nicht direkt übertragen, sondern sendeseitig durch eine Modulation in einen Frequenzbereich verschoben, den eine Antenne abstrahlen kann. Empfangsseitig wird die Information über eine Demodulation wieder in den ursprünglichen Frequenzbereich verschoben. Die Modulation auf eine hohe Frequenz – der so genannten Trägerfrequenz – ist notwendig, damit das eigentliche Nutzsignal über größere Entfernungen überhaupt drahtlos übertragen werden kann. Die Darstellung von Informationen kann durch die Änderung von Amplitude (Amplitudenmodulation), Frequenz (Frequenzmodulation) oder der Phasenlage (Phasenmodulation) realisiert werden.

Amplitudenmodulation

Amplitudenmodulation

Bei der Amplitudenmodulation wird einem Trägersignal mit fester Frequenz die gewünschte Information als Amplitudenänderung aufmoduliert und übertragen. Die Amplitudenmodulation ist störanfällig, weil die Information in der Amplitude steckt. Störer treten allgemein in der Amplitude auf, wodurch die Information relativ einfach verfälscht werden kann.

Frequenzmodulation

Frequenzmodulation

Bei der Frequenzmodulation bleibt die Amplitude des Trägers konstant. Für die Darstellung des Nutzsignals wird die Frequenz des Trägers verändert. Die Frequenzmodulation ist relativ unempfindlich gegenüber Störern, da diese in der Regel in der Amplitude auftreten.

Phasenmodulation

Phasenmodulation

Bei der Phasenmodulation bleibt ebenfalls die Amplitude des Trägersignals konstant. Das Nutzsignal bewirkt eine Veränderung der Phase des Trägers um einen bestimmten Bereich. Wie bei der Frequenzmodulation ist auch eine phasenmodulierte Übertragung sehr unempfindlich gegen äußere Störungen.

Bei der Modulation von digitalen Signalen kommen, wie bei der analogen Modulation, Verfahren wie die Amplituden-, Frequenz- und Phasenmodulation in Frage. Jedoch muss man hierbei berücksichtigen, dass die digitalen Signale nicht wertkontinuierlich sind, d.h. es wird nur zwischen einer bestimmten Anzahl unterschiedlicher Kennzustände gesprungen. Deshalb spricht man hierbei nicht mehr von einer Modulation, sondern von Umtastung oder dem englischen Begriff Shift

Keying. Im WLAN-Bereich kommen vorwiegend die Verfahren Frequency Shift Keying (FSK) und Phase Shift Keying (PSK) zum Einsatz. Bei FSK und PSK handelt es sich um ein digitales moduliertes Signal.

Die Qualität eines demodulierten Signals wird über die sogenannte Bitfehlerrate (BFR, engl. Bit Error Rate, BER) beschrieben, die das Verhältnis der verfälschten zu den übertragenen Bits beschreibt.

1.5.3 Die Frequenz

Frequenz

In der Elektrotechnik werden zwei verschiedene Spannungsarten unterschieden, die Gleichspannung und die Wechselspannung. Bei der Gleichspannung ist die Höhe und die Polarität der Spannung unabhängig von der Zeit stets gleich. Betrachtet man hingegen eine Wechselspannung, so ändert sich die Höhe und die Polarität der Spannung periodisch. Die Wechselspannung aus unserem Spannungsversorgungsnetz verändert sich beispielsweise in der Polarität und in der Höhe periodisch nach einer Sinusfunktion. Für den periodischen Spannungsverlauf wird eine bestimmte Zeit beansprucht, die als Periodendauer bezeichnet wird. In der Elektrotechnik gibt man über die Frequenz die Anzahl von Schwingungen pro Sekunde an, wobei die Frequenz und die Periodendauer reziprok zueinander im Zusammenhang stehen: Je niedriger die Periodendauer, desto höher ist die Frequenz. Man errechnet demnach die Frequenz nach der Formel Frequenz = 1/Periodendauer und gibt sie in der Einheit Hertz (Hz) an. Dabei entspricht 1 Hertz einer Schwingung pro Sekunde. Unser Wechselspannungsversorgungsnetz arbeitet beispielsweise mit einer Frequenz von 50 Hz (siehe Abb. 1–1).

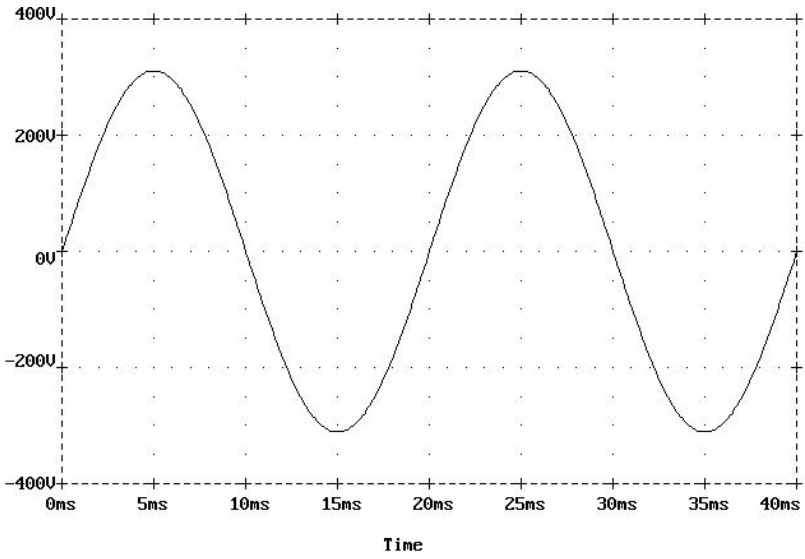

Abb. 1–1
Verlauf einer 50-Hz-Wechselspannung

1.5.4 Exkurs Pegelwerte und Dezibel

Pegelwerte und Dezibel

In den vorangegangenen Abschnitten sind bereits häufig Wertangaben in dB und dBm aufgeführt worden. Da diese Einheiten nicht jedem Netzwerker gebräuchlich sind, möchte ich sie an dieser Stelle kurz beschreiben.

Pegelverhältnis

Anstelle von direkten Leistungen rechnet man in der Nachrichtentechnik allgemein mit logarithmierten Größen, da in der Regel die Leistungsangaben über viele 10er-Potenzen variieren. Ein Leistungsverhältnis errechnet sich aufgrund der Rechenregeln für den Logarithmus aus dem Pegelverhältnis P_1/P_0. Eine Pegeldifferenz wird dabei definiert als Pegeldifferenz = 10 log P_1/P_0. In dieser Pegeldifferenz bezeichnet log den Logarithmus zur Basis 10. Aus der Umkehrung der Pegeldifferenz ergibt sich demnach das dazugehörige

$$\text{Leistungsverhältnis} = 10^{\text{Pegeldifferenz}/10}$$

Die Pegeldifferenz ist einheitslos. Um anzudeuten, dass die Angabe durch eine Rechenvorschrift entstanden ist, erhält die Pegeldifferenz die Pseudoeinheit dB (Zehntel-Bel, benannt nach Alexander Graham Bell). Die 10 in der Angabe der Pegeldifferenz (10 log P_1/P_0) ergibt sich aus der Tatsache, dass man mit der Einheit dB und nicht Bel arbeitet (1 Bel = 10 dB). Im Folgenden sind einige Leistungsverhältnisse als Beispiel aufgeführt:

Leistungsverhältnis

- Leistungsverhältnis 1 ↔ 0 dB ($10^0 = 1$)
- Leistungsverhältnis 10 ↔ 10 dB ($10^1 = 10$)
- Leistungsverhältnis 100 ↔ 20 dB ($10^2 = 100$)
- Leistungsverhältnis 2 ↔ 3 dB ($10^{0,3} = 2$)

In der Praxis ist es hilfreich, wenn man sich die dargestellten Beispielwerte merkt. Bei der Übertragung von elektromagnetischen Wellen erfahren diese Dämpfungen oder gegebenenfalls auch Verstärkungen. Möchte man diese Effekte mathematisch betrachten, ist eine Multiplikation und Division einzelner Leistungsverhältnisse notwendig. Nach den Rechenregeln für den Logarithmus wird eine Multiplikation zur Addition und eine Division zur Subtraktion, wie es in den folgenden Beispielen dargestellt ist:

- Leistungsverhältnis 8 = 2 × 2 × 2 ↔ 3 dB + 3 dB + 3 dB = 9 dB
- Leistungsverhältnis 0,5 = 1/2 ↔ 0 dB - 3 dB = - 3 dB

Aus den beiden Beispielen ist ersichtlich, dass Leistungsverhältnisse größer 1 positive dB-Werte annehmen und Leistungsverhältnisse kleiner 1 negative dB-Werte annehmen. Positive dB-Werte entsprechen einer Leistungssteigerung und negative dB-Werte eine Leistungsreduzierung. In Tabelle 1–4 sind die wichtigsten Leistungsverhältnisse (Werte gerundet) dargestellt.

Tab. 1–4
dB-Leistungsverhältnisse

Steigerung	Faktor	Reduzierung	Faktor
0 dB	× 1	0 dB	× 1
1 dB	× 1,25	-1 dB	× 0,8
3 dB	× 2	-3 dB	× 0,5
6 dB	× 4	-6 dB	× 0,25
10 dB	× 10	-10 dB	× 0,1
12 dB	× 16	-12 dB	× 0,06
20 dB	× 100	-20 dB	× 0,01
30 dB	× 1000	-30 dB	× 0,001

Sendeleistungsangaben

In der Nachrichtentechnik ist es gebräuchlich, für die Angaben der Sendeleistungen auf die Sendeleistung von 1 mW Bezug zunehmen. In diesem Fall wird die Einheit dBm verwendet. Demnach sind zum Beispiel 20 dBm = 10 log (100 mW / 1 mW).

Die Leistung von 1 Watt entspricht beispielsweise dem Wert von 30 dBm (1 Watt = 1000 mW = 10 × 10 × 10 × 1 mW ↔ 10 dB + 10 dB + 10 dB + 0 dB= 30 dBm). Tabelle 1–5 zeigt verschiedene Leistungsangaben mit der Einheit dBm.

dBm	Leistung [mW]	dBm	Leistung [mW]
0 dBm	1 mW	0 dBm	1 mW
1 dBm	1,25 mW	-1 dBm	0,8 mW
3 dBm	2 mW	-3 dBm	0,5 mW
6 dBm	4 mW	-6 dBm	0,25 mW
7 dBm	5 mW	-7 dBm	0,20 mW
10 dBm	10 mW	-10 dBm	0,10 mW
12 dBm	16 mW	-12 dBm	0,06 mW
13 dBm	20 mW	-13 dBm	0,05 mW
15 dBm	32 mW	-15 dBm	0,03 mW
17 dBm	50 mW	-17 dBm	0,02 mW
20 dBm	100 mW	-20 dBm	0,01 mW
30 dBm	1000 mW	-30 dBm	0,001 mW
40 dBm	10000 mW	-40 dBm	0,0001 mW

Tab. 1–5
Leistungsangaben in dBm

Werden zu den Leistungsangaben in dBm bestimmte Leistungsverhältnisse in dB addiert oder subtrahiert, so ergibt sich für das Ergebnis die Einheit dBm, zum Beispiel 30 dBm - 10 dB = 20 dBm.

1.5.5 Bitrate und Datenrate

Datenrate

Die Bitrate oder Datenrate gibt die Anzahl der Bits an, die während einer Zeiteinheit von einer Sekunde übertragen werden. In der Netzwerktechnik ist es allgemein üblich, die Übertragungsgeschwindigkeit in Bits pro Sekunde anzugeben, wobei man als Präfix die entsprechenden Zehnerpotenzen kBit/s (kilo = 10^3), MBit/s (Mega = 10^6) und GBit/s (Giga = 10^9) verwendet.

> In der Netzwerktechnik werden bei der Umrechnung der Bitrate oder Datenrate immer die Zehnerpotenzen zugrunde gelegt, d.h. 1 MBit/s entspricht 1000 kBit/s oder 1000000 Bit/s. In vielen anderen Bereichen der EDV (Elektronischen Daten-Verarbeitung) wird hingegen mit Zweierpotenzen gerechnet. So entspricht beispielsweise eine 1 KByte große Datei dem Datenvolumen von 1024 Bytes (zur Unterscheidung häufig mit großem »K«).

1.5.6 Paketvermittlung versus Leitungsvermittlung

Paketvermittlung

Bei den Computernetzwerken wird für die Datenübertragung die gesamte Bandbreite des Übertragungsmediums jeweils für eine relativ kurze Zeit in Anspruch genommen. Das Übertragungsmedium verfügt

in der Regel über eine hohe Bandbreite. Betrachtet man hingegen den Datenaustausch über eine ISDN-Leitung, so wird hier bei einer geringen Bandbreite die gesamte Bandbreite für einen gewissen Zeitraum dauerhaft in Anspruch genommen. Praktisch sieht dies in der Form so aus, dass man eine dedizierte Punkt-zu-Punkt-Verbindung zwischen den Verbindungspartnern für die gewünschte Dauer des Datenaustauschs schaltet; man spricht in diesem Fall von einer verbindungsorientierten Verbindung. Nachteilig ist natürlich bei diesem Verfahren, dass für die Dauer der geschalteten Verbindung die Leitung bzw. der Kanal für andere Verbindungen nicht genutzt werden kann.

Shared Media

In einem lokalen Netzwerk wird ein vorhandenes Medium gemeinsam verwendet (Shared Media), dies verhält sich ähnlich wie bei einer Unterhaltung von mehreren Personen, die sich in einem Raum befinden. Um die Daten zielgerichtet zum gewünschten Empfänger übertragen zu können, werden die Daten, die als Datenpakete zusammengefasst sind, mit Adressinformationen versehen. Die Datenpakete werden demnach ähnlich wie Briefe oder Pakete beim Versand über die Post verschickt. Diese Art der Kommunikation bezeichnet man als Paketvermittlung. Dafür muss keine dedizierte Verbindung zwischen den Kommunikationspartnern aufgebaut werden; deshalb spricht man hier von einem verbindungslosen Dienst.

1.6 Gesundheit

Gesundheitsrisiken

Immer dann, wenn Daten und Informationen per Funk übertragen werden, kommt das Thema Gesundheit und Gesundheitsrisiken auf den Tisch. Hierbei stellt sich vornehmlich die Frage, inwieweit sich die elektromagnetischen Wellen auf den menschlichen Organismus auswirken. Seit längerem ist bekannt, dass Funkwellen Wärme erzeugen, wobei die Wärmewirkung von der Frequenz und von der Leistung der abgestrahlten Funkwellen abhängig ist. Hierbei ist auch die Entfernung zur Sendeeinrichtung entscheidend, da die Leistung mit dem Quadrat der Entfernung abnimmt. Vergrößert man beispielsweise den Abstand von 10 cm auf 1 m, so beträgt die eingestrahlte Leistung nur noch ein Hunderstel der Sendeenergie.

Sendeleistung

Allgemein kann man festhalten, dass WLAN-Einrichtungen weitaus harmloser sind als Mobilfunkeinrichtungen. Diese Aussage lässt sich anhand der Sendeleistung belegen. Die Sendeleistung von WLAN-Einrichtungen beträgt gegenüber der von Mobilfunktelefonen maximal ein Zwanzigstel. Bei handelsüblichen Mobilfunktelefonen kann die Sendeleistung bis zu 2 Watt betragen. Zudem werden Mobilfunktelefone sehr oft unmittelbar am Kopf betrieben, wohingegen sich

WLAN-Adapter in der Regel in einem Abstand von etwa 60 cm befinden, falls diese beispielsweise in einem PCMCIA-Slot eines Notebooks betrieben werden. Die Unbedenklichkeit wird in der Praxis durch die Tatsache unterstrichen, dass WLANs in Krankenhäusern betrieben werden dürfen, wohingegen der Betrieb von Mobilfunktelefonen grundsätzlich verboten ist.

DIN VDE 0848 und 26. BImSchV

Elektromagnetische Felder rufen eine elektrische Feldstärke, magnetische Feldstärke und eine Leistungsflussdichte hervor. Primär entscheidend ist aus heutiger Betrachtungsweise die Leistungsflussdichte der hochfrequenten elektromagneti schen Strahlung, die die thermischen Effekte hervorruft. Hierbei berücksichtigt man, dass die Absorption elektromagnetischer Strahlung in biologischen Geweben zu einer Erwärmung dieser Gewebe führt. Für Deutschland gilt als gesetzlicher Grenzwert im 2,4-GHz- und 5-GHz-Frequenzband für die Leistungsflussdichte der Wert von 10 W/m2, der in der DIN VDE 0848, Teil 2 und nach der 26. Verordnung zum Bu ndes-Immissionsgesetz (26. BlmSchV) der Strahlenschutzkommission festgelegt ist. Beide Normen stützen sich auf die Empfehlungen der ICNIRP (International Committee on Non-Ionizing Radiation Protection) und legen Grenzwerte im Frequenzbereich von 10 MHz und 300 GHz fest.

WLAN-Gutachten

Am 2. Okt ober 2001 wurde von der Universität Bremen beim Nova-Institut für Ökologie und Innovation (*http://nova-institut.de*) ein Gutachten in Auftrag gegeben, das die Belastung durch hochfrequente elektromagnetische Strahlung eines 2,4-GHz-WLANs beleuchten sollte. Nach diesem Gutachten ruft ein WLAN-Netzwerkadapter im Notebook im Abstand von 60 cm eine mitt lere Leistungsflussdichte von lediglich 3,15 mW/m2 hervor. Selbst bei einem minimalen Abstand von 20 cm wurde eine maximale Leistungsflussdichte von 158 mW/m2 und bei 10 cm von 49,9 mW/m2 gemessen. Bei einem Access Point wurde im Abstand von 2,5 m eine Leistungsflussdichte von 0,66 mW/m2 gemessen. Hierbei ist zu berück sichtigen, dass ein Access Point nicht ständig ein Signal aussendet. Erst bei der Volllastsituation kann man von einem dauerhaften Sendefall ausgehen, bei dem im WLAN ein Signal kontinuierlich ausgesendet wird. Im Vergleich dazu führen DECT-Telefone im Schnitt, bei einem Abstand von 40 bis 60 cm, bereits zu einer Leistungsflussdichte von etwa 170 mW/m2. Die Basisstation einer DECT-Einrichtung sendet ständig Signale aus, unabhängig davon, ob gerade telefoniert wird oder nicht, wobei mit einer k urzen Pulsleistung bei einer Sendepause von 10 Millisekunden gearbeitet wird. Diese Ergebnisse zeigen deutlich auf, dass sämtliche Messwerte weit unterhalb der von der DIN VDE 0848, Teil 2 und der 26. BlmSchV vorgegebenen Grenzwerte liegen. Die Sicherheit von Personen im Umfeld der WLAN-Einrichtun-

gen sollte demnach aus heutiger Betrachtungsweise gewährleistet sein, da genug Reserven vorhanden sind.

nova-Vorsorgewerte

Das Nova-Institut geht zudem einen Schritt weiter und hat sogenannte nova-Vorsorgewerte definiert, die bei einem Hundertstel der gesetzlichen Grenzwerte liegen. Hierdurch sollen nachteilige Auswirkungen für den Menschen ausgeschlossen werden. Dies wird damit begründet, dass man sich bei den Auswirkungen der elektromagnetischen Strahlung nicht ausschließlich auf thermische Effekte stützen sollte. Man geht davon aus, dass dauerhafte elektromagnetische Strahlungen auch Schädigungen des Immunsystems hervorrufen können, die die Entstehungen von Krankheiten begünstigen können. Wissenschaftlich sind diese Betrachtungen jedoch heute noch umstritten. Richtet man sich allerdings vorsorglich nach dem nova-Vorsorgewert für die Leistungsflussdichte von 100 mW/m2, so wurde dieser im erstellten Gutachten nur bei einer Messung im geringen Abstand überschritten. Wird der übliche Abstand von 60 cm eingehalten, so liegt der gemessene Wert von 3,15 mW/m2 deutlich unter dem nova-Vorsorgewert. Um allen Diskussionen aus dem Weg zu gehen, sollte man vorsorglich die WLAN-Anwender darauf hinweisen, dass ein typischer Abstand von 50 bis 60 cm (übliche Schreibtisch-Entfernung) zum WLAN-Adapter eingehalten werden sollte. Vorzugsweise sollten die Access Points mit zusätzlichen Antennen ausgestattet werden, und bei den WLAN-Stationen sollte auf den Einsatz von zusätzlichen Antennen verzichtet werden, falls die WLAN-Stationen mit einem größerem Abstand zum Access Point arbeiten. Falls an den WLAN-Stationen dennoch mit externen Antennen gearbeitet werden muss, sollten diese so ausgerichtet werden, dass sie nicht in Richtung der Anwender abstrahlen. Diese Empfehlungen sollen lediglich dazu beitragen, dass neben dem weit unterschrittenen gesetzlichen Grenzwert auch der nova-Vorsorgewert eingehalten wird, um allen Bedenken beim Einsatz von WLAN aus dem Weg zu gehen. Somit ist man auf der sicheren Seite, auch für den Fall, dass heutige gesetzliche Grenzwerte zukünftig durch neue wissenschaftliche Erkenntnisse nach unten korrigiert werden.

1.7 OSI-Referenzmodell

OSI-Referenzmodell

Die Kommunikation innerhalb eines Netzwerks wird anhand eines Netzwerkmodells beschrieben, wobei man sich das sogenannte Open Systems Interconnection Referenzmodell (OSI Reference Model) zugrunde legt. Das OSI-Referenzmodell wurde zwischen 1977 und 1984 (1984 in der ISO-Norm 7498 festgeschrieben) entworfen und ist

in sieben Teilschichten unterteilt, die auch als Layer bezeichnet werden. Jede Schicht des OSI-Referenzmodells stellt eine bestimmte Funktion zur Verfügung, die als Dienst bezeichnet wird und einen funktionellen Beitrag für den Ablauf der Kommunikation zwischen zwei Computern leistet.

In den Anfängen der Netzwerktechnologien gab es viele firmenspezifische Standards. Zu dieser Zeit war es undenkbar, dass ein Datenaustausch zwischen Einrichtungen unterschiedlicher Hersteller möglich war. Man erkannte rechtzeitig diese Problematik und entwarf deshalb eine entsprechende Netzwerkarchitektur, die als Basis für die heutzutage offenen Plattformen dient. Aus dieser Intention heraus entstand das OSI-Referenzmodell, das heutzutage allgemein als Grundlage für die Definition von Standards für offene Systeme im Kommunikationsbereich dient. Bei dem OSI-Referenzmodell handelt es sich allerdings ausschließlich um ein Modell, das eine Standard-Netzwerkarchitektur beschreibt und wesentlich zum Verständnis der funktionellen Zusammenhänge im Netzwerk beiträgt.

Abb. 1–2
Zeigt das siebenschichtige OSI-Referenzmodell

Sieben Schichten

Jede Schicht im OSI-Referenzmodell, mit Ausnahme der untersten Schicht, hat eine darunter liegende Nachbarschicht und jede Schicht, außer der obersten Schicht, hat eine darüber liegende Nachbarschicht. Die Schichten stellen jeweils ihre Dienste der darüber liegenden Schicht zur Verfügung und nutzen ihrerseits die Dienste der darunter liegenden Schicht. Die Kommunikation zwischen den Schichten erfolgt über definierte Schnittstellen.

Dienste

Durch die Funktion beziehungsweise den Dienst einer Schicht wird in der Gesamtbetrachtung die Funktion einer darunter liegenden Schicht erweitert. Jede Schicht folgt beim Ausführen ihrer Funktion gewissen definierten Regeln, die als Protokolle bezeichnet werden. Die

Kommunikation zwischen zwei Computern findet immer nur zwischen den Schichten der gleichen Ebene statt und wird als virtuelle Kommunikation bezeichnet. Damit die virtuelle Kommunikation zwischen zwei Computern stattfinden kann, müssen auf den gegenüberliegenden Schichten der gleichen Ebene jeweils dieselben Protokolle implementiert sein. Die Schichten derselben Ebene werden als Peers und die korrespondierenden Protokolle derselben Ebene als Peer Protocol bezeichnet. Die Peers tauschen während der Kommunikation ihre Informationen in einem Format aus, das auf beiden Seiten verstanden wird und als Protokoll-Dateneinheit (PDU = Protocol Data Unit) bezeichnet wird. Eine PDU ist in zwei Teile aufgeteilt, den Header für Protokollinformationen (Protocol Control Information, PCI) und die Dateneinheit (Service Data Unit). Der Dienst, der von einer Schicht zur Verfügung gestellt wird, wird durch eine oder mehrere Arbeitseinheiten (Entities) umgesetzt. Der Zugriff auf die Arbeitseinheiten erfolgt über sogenannte Service Access Points (SAP); sie stellen quasi eine Adresse dar, über die auf die verschiedenen Funktionen zugegriffen werden kann.

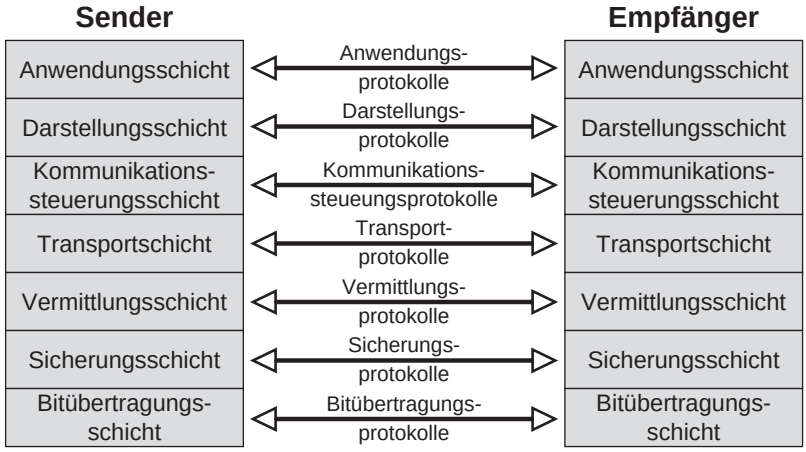

Abb. 1–3 *Die virtuelle Kommunikation findet immer auf derselben Ebene statt*

Virtuelle Kommunikation

Wie bereits erwähnt, findet bei der Kommunikation zwischen zwei Computern die virtuelle Kommunikation jeweils auf derselben Ebene statt. Die Daten bewegen sich dabei von dem einen Computer vertikal nach unten bis zur untersten Schicht im Referenzmodell, der Bitübertragungsschicht. Auf der Bitübertragungsschicht bewegen sich die Daten horizontal zum Computer, mit dem kommuniziert werden soll. Auf diesem Computer laufen die Daten dann wieder vertikal nach oben in die einzelnen Schichten. Die Daten erreichen auf diese Weise

die jeweils gleichen Schichten (Peers) auf dem gege nüberliegenden Computer, zwischen denen auch die Kommunikation jeweils stattfindet (siehe Abb. 1–4).

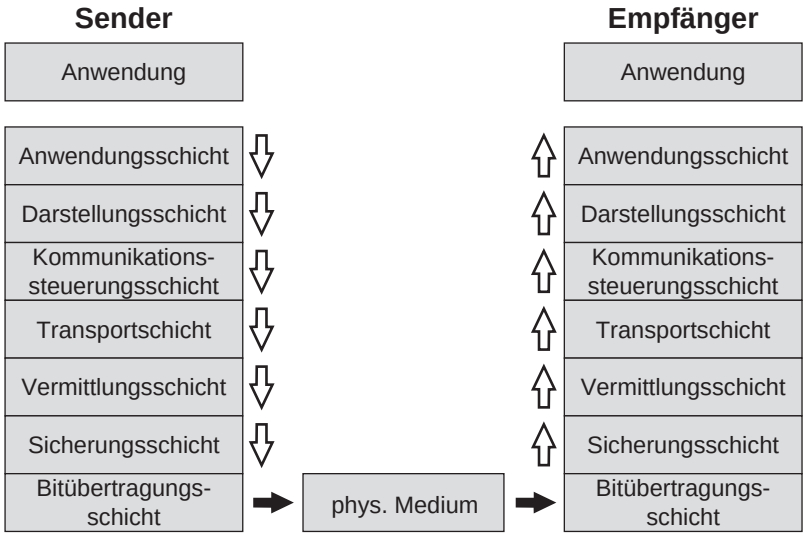

Abb. 1–4
Zeigt die Kommunikationswege innerhalb des OSI-Referenzmodells

Jede Schicht des OSI-Referenzmodells stellt unabhängig von den anderen Schichten bestimmte Funktionen oder Dienste zur Verfügung.

Die Bitübertragungsschicht

Bitübertragungsschicht

Die Bitübertragungsschicht, auch physikalische Schicht genannt (engl. Physical Layer), ist die unterste Schicht des OSI-Referenzmodells. Die Bitübertragungsschicht stellt einen Dienst bereit, mit dessen Hilfe die Daten als Bitstrom physikalisch über ein Übertragungsmedium von einem Computer zu einem anderen Computer übertragen werden können. Es handelt sich in dem Fall um eine ungesicherte und physikalische Verbindung, die nach Bedarf auf dem Übertragungsmedium auf- und abgebaut wird. Auf der Bitübertragungsschicht sind beispielsweise das Übertragungsmedium und damit verbunden die physikalischen Eigenschaften der Datensignale definiert, über die der Datenstrom auf dem jeweiligen Medium übertragen wird. Dazu gehören die Art und Größe des Datensignals, die Bit- oder Bytesynchronisation, die Codierungs- und Modulationsverfahren. Des Weiteren ist auf der Bitübertragungsschicht das Interface definiert, d.h. der physikalische Anschluss und welche Art von Verbindungselementen verwendet werden. Man kann zusammengefasst sagen, dass auf der B itübertrag-

ungsschicht die elektrische und mechanische Definition des Interface und das Übertragungsmedium definiert werden.

Die Sicherungsschicht

Sicherungsschicht

Die Sicherungsschicht (engl. Data Link Layer) ist die zweite Schicht des OSI-Referenzmodells. Aufgabe der Sicherungsschicht ist es, einen fehlerfreien Datenaustausch zu gewährleisten. Dazu werden die Daten zu Einheiten zusammengefasst, die als Datenpakete oder Frames bezeichnet werden. Die Datenpakete haben ein bestimmtes Format und werden in der Regel durch eine Prüfsumme ergänzt, über die eine Fehlererkennung möglich ist. Des Weiteren wird auf der Sicherungsschicht der Zugriff auf das Übertragungsmedium durch ein entsprechendes Zugriffsverfahren durchgeführt.

Die Sicherungsschicht wird in der Praxis in zwei Teilbereiche unterteilt, wobei der untere Teilbereich durch die verschiedenen standardisierten Netzwerktechnologien wie Ethernet oder Wireless LAN abgedeckt wird. Der obere Bereich umfasst Logical Link Control laut Standard IEEE 802.2. Der obere Teilbereich wird von allen IEEE-Netzwerktechnologien gleichermaßen verwendet, wodurch der Datenaustausch zwischen verschiedenen IEEE-Netzwerktechnologien vereinfacht wird.

Die Vermittlungsschicht

Vermittlungsschicht

Die nächste Ebene im OSI-Referenzmodell ist die Vermittlungsschicht, auch Netzwerkschicht genannt (engl. Network Layer). Sie sorgt für den eigentlichen Datentransfer zwischen den Computern, indem sie die Wegfindung (Routing) zwischen den Computern übernimmt. Stellen die unteren beiden Schichten nur eine Kommunikation zwischen zwei angrenzenden Computern innerhalb eines Netzwerks zur Verfügung, so bietet die Vermittlungsschicht eine Möglichkeit zur Kommunikation über die Grenzen eines Netzwerks hinaus. Die Daten werden dazu mit entsprechenden Ziel- und Quelladressen versehen, über die das zielgerichtete Routing durchgeführt werden kann. Die Adressierung auf der dritten Ebene ist von den darunter liegenden Schichten unabhängig; das Routing kann sich auf diese Weise über mehrere logisch strukturierte Netzwerke erstrecken. Erst durch die Adressierungsmöglichkeiten auf der dritten Ebene ist eine Bildung von hierarchisch untergliederten Teilnetzwerken möglich, zwischen denen ein Datenaustausch ermöglicht wird.

Die Transportschicht

Transportschicht

Die Transportschicht (engl. Transport Layer) ist auf der vierten Ebene platziert und vermittelt zwischen den drei obersten Schichten des OSI-Referenzmodells und den unteren vier Schichten, die das Transportsystem darstellen. Im Grunde tauschen zwei Programme untereinander Daten aus, wenn zwei Computer miteinander kommunizieren. Die Transportschicht sorgt dafür, dass die Daten der Vermittlungsschicht an die richtigen Programme auf dem Computer ausgeliefert werden. Diese Schicht sorgt so für die Zuverlässigkeit des Datentransfers und den gleichzeitigen Zugriff mehrerer Dienste oder Anwendungen auf dieselben Transportmechanismen. Die Transportschicht stellt damit für die übergeordneten Instanzen einen transparenten Datenkanal zur Verfügung.

Auf der Transportschicht werden die Daten in kleine Teileinheiten aufgeteilt, wie sie von der Vermittlungsschicht weitergeleitet werden können (Fragmentierung). Auf der anderen Seite, der Empfängerseite, werden die Daten von den Diensten der Transportschicht wieder zu einem gesamten Datenblock zusammengesetzt. Dabei wird von den Diensten der Transportschicht dafür gesorgt, dass die Daten empfangsseitig in der richtigen Reihenfolge ankommen, damit sie wieder eine logische Dateneinheit bilden.

Die Kommunikationssteuerungsschicht

Kommunikationssteuerungsschicht

Die Kommunikationssteuerungsschicht, auch Sitzungsschicht genannt (engl. Session Layer), ist die fünfte Schicht im OSI-Referenzmodell. Sie stellt einen anwendungsorientierten Dienst zur Verfügung und sorgt für einen Verbindungsauf- und -abbau sowie die Darstellung der Übertragungsdaten in einer von der darüber liegenden Ebene unabhängigen Form. Der Anmeldevorgang wird im Fachjargon als Aufbau einer Sitzung (Session) bezeichnet. Eine Sitzung stellt die Grundlage für eine virtuelle Verbindung zwischen zwei Prozessen dar, die auf räumlich getrennten Computern ausgeführt werden. Für den Sitzungsaufbau, die Sitzungsüberwachung und das Beenden einer Sitzung kommen unterstützende Funktionen zum Tragen, wie zum Beispiel die Echtheitsbestätigung und die Sicherheitsmechanismen für den Zugriff auf Ressourcen.

Die Darstellungsschicht

Darstellungsschicht

Die Darstellungsschicht (engl. Presentation Layer) ist die sechste Schicht innerhalb des OSI-Referenzmodells. Sie ist für die Kommunikation und das Weiterreichen von Daten zwischen der Sitzungsschicht

und den Anwendungen verantwortlich und beinhaltet bestimmte Funktionen, die für die Kommunikation innerhalb eines Netzwerks benötigt werden. Dazu gehören Schnittstellen zu Netzwerkressourcen wie beispielsweise Drucker oder Speichermedien. Auf der Darstellungsschicht wird festgelegt, in welcher Form die Daten dem Anwender präsentiert werden. Hierzu gehören beispielsweise die Art und die Länge des Datentyps. Ebenfalls kann auf der Darstellungsschicht eine Komprimierung oder Verschlüsselung von Daten eine Rolle spielen.

Die Anwendungsschicht

Anwendungsschicht

Die Anwendungsschicht (engl. Application Layer) ist die oberste und siebte Schicht des OSI-Referenzmodells; sie bildet das Bindeglied zwischen dem Anwender und den Anwendungsprozessen über das Netzwerk. Auf der Anwendungsschicht sind die anwendungsspezifischen Protokolle angesiedelt, wobei Details zu Programmen oder Anwendungen, die von den Netzwerkbenutzern während ihrer Arbeit im Netzwerk genutzt werden, auf der Anwendungsschicht enthalten sind. Zu den Protokollen gehören beispielsweise das File Transfer Protocol (FTP), mit dem Dateien über ein Netzwerk übertragen werden können, oder TELNET, mit dem remote auf einen Computer zugegriffen werden kann und Befehle ausgeführt werden können.

Die Unterteilung des OSI-Referenzmodells

Unterteilung des OSI-Referenzmodells

Betrachtet man die Dienste, die von den sieben Schichten bereitgestellt werden, so fällt auf, dass man das OSI-Referenzmodell in zwei Bereiche aufteilen kann. Die eigentlichen Transportmechanismen, die für die Datenübertragung über ein Netzwerk sorgen, sind auf den untersten vier Schichten angesiedelt. Die unteren beiden Schichten entsprechen dabei der Netzwerktechnologie, wie beispielsweise Ethernet oder Wireless LAN. Die dritte und vierte Schicht beinhaltet die Protokolle wie TCP/IP oder IPX/SPX.

> Die folgenden Kapitel dieses Buches werden sich im Wesentlichen mit den unteren zwei Schichten des OSI-Referenzmodells beschäftigen.

Die oberen drei Schichten des OSI-Referenzmodells sind anwendungsorientiert, sie bilden die Schnittstelle zu den Netzwerkanwendungen und den Netzwerkanwendern.

1.8 Ein Überblick über den Inhalt dieses Buchs

Inhalt dieses Buchs

Das Buch wurde mit dem Ziel geschrieben, theoretisches und praxisnahes Wissen für den Aufbau sowie die Einrichtung eines WLANs zu vermitteln. Neben dem praxisnahen Inhalt wird auch detailliert auf den 802.11-Standard eingegangen und aufgezeigt, wie die drahtlose Datenübertragung technisch umgesetzt wird. Dabei werden primär die unteren zwei Schichten des OSI-Referenzmodells abgehandelt. Diese beiden Schichten beziehen sich auf die technische Implementierung von WLAN. Abgerundet werden diese Informationen durch die Darstellung aktueller WLAN-Produkte und der praktischen Umsetzung eines WLANs. Zudem werden Aspekte der Netzwerksicherheit und Fehleranalyse betrachtet, wobei auf die gesteigerten Anforderungen, die bei der drahtlosen Datenübertragung auftreten, explizit eingegangen wird.

Kapitel 2

Kapitel 2 bietet einen Überblick über die realisierbaren WLAN-Netzwerkformen.

Kapitel 3

Kapitel 3 geht intensiv auf den Physical Layer des IEEE-802.11-Standards und dessen Erweiterungen ein und beschreibt, wie es heute bei der drahtlosen Datenübertragung technisch möglich ist, Datenraten von 1 bis 54 MBit/s zu realisieren.

Kapitel 4

Kapitel 4 beschreibt die Implementierung des WLAN-MAC-Layers und erklärt, wie das Zugriffsverfahren und die Sicherungsmechanismen im IEEE-802.11-Standard implementiert sind, mit deren Hilfe eine sichere Datenübertragung per Funk überhaupt möglich ist.

Kapitel 5

In Kapitel 5 wird die 802.11n-Standarderweiterung beschrieben, die Datenraten von bis zu 600 MBit/s ermöglicht. Dieses Kapitel geht detailliert auf die 802.11n-Erweiterungen auf dem PHY- und MAC-Layer ein, die die Effizienz der Datenübertragung wesentlich steigern und hohe Datenraten erzielen.

Kapitel 6

Kapitel 6 geht auf die zukünftigen Very-High-Throughput-Erweiterungen (VHT) ein, die als IEEE 802.11ac und IEEE 802.11ad verabschiedet werden sollen. 802.11ac arbeitet im 5-GHz-Band und 802.11ad im 60-GHz-Band. Beide Lösungen sollen Datenraten von annähernd 7 GBit/s ermöglichen.

Kapitel 7

Kapitel 7 setzt sich mit der Antennentechnologie auseinander, die im WLAN-Bereich zum Einsatz kommt. In diesem Kapitel wird aufgezeigt, welche Antennenparameter relevant sind und welche Antennen eingesetzt werden können, um die Reichweite oder Zuverlässigkeit der Datenübertragung zu erhöhen. Des Weiteren wird die Reichweitenkalkulation am Beispiel einer Richtfunkstrecke betrachtet.

Kapitel 8 Kapitel 8 zeigt auf, welche WLAN-Komponenten beim Errichten eines WLANs eingesetzt werden können und welche Lösungen es für die Einbindung von PCs, Notebooks oder PDAs gibt.

Kapitel 9 Kapitel 9 widmet sich der praktischen Umsetzung eines WLANs. Hier wird aufgezeigt, wie ein WLAN geplant wird und wie eine professionelle Funkausleuchtung durchgeführt werden kann. Praktische Tipps helfen dem Netzwerkadministrator bei der Umsetzung oder Optimierung eines WLANs.

Kapitel 10 Kapitel 10 geht auf die Sicherheitsaspekte eines WLANs ein. In diesem Kapitel werden die Gefahren und Risiken durchleuchtet, die bei der drahtlosen Datenübertragung entstehen können. Zudem werden aktuelle Sicherheitslösungen auf der Basis von 802.11i beziehungsweise WPA(2) detailliert betrachtet, mit denen eine sichere drahtlose Datenübertragung realisiert werden kann. Des Weiteren wird die Wi-Fi-Proteced-Setup-Methode (WPS) beschrieben.

Kapitel 11 Kapitel 11 ist das abschließende Kapitel dieses Buches, in dem auf die Fehleranalyse eingegangen wird. In diesem Kapitel wird beschrieben, wie man bei einer eventuell notwendigen Fehleranalyse vorgehen sollte, um diese möglichst effektiv zu gestalten. Anhand von Beispielszenarien werden die Möglichkeiten der Protokollanalyse aufgezeigt.