3. Auflage

Gerhard Lienemann

TCP/IP Grundlagen und Praxis

Protokolle, Routing, Dienste, Sicherheit

→ Mit Beiträgen von Dirk Larisch

dpunkt.verlag

Gerhard Lienemann arbeitete ab 1991 für etwa 12 Jahre als Netzwerkadministrator in einem produzierenden Betrieb, bevor er ins technische Management wechselte. Seitdem war er zunächst zuständig für operative Kommunikationssicherheit und übernahm dann zusätzlich die Betreuung eines europäischen Netzwerkteams. Nur kurze Zeit später erweiterte er seine Verantwortung auf ein globales Netzwerkteam in Asien, Nord- und Südamerika. Seiner Leidenschaft »IT-Kommunikation« ist er auch nach dem Ausscheiden aus dem aktiven Berufsleben treu geblieben.

Gerhard Lienemann

TCP/IP – Grundlagen und Praxis

Protokolle, Routing, Dienste, Sicherheit

3., aktualisierte und überarbeitete Auflage

Mit Beiträgen von Dirk Larisch

dpunkt.verlag

Gerhard Lienemann
feedback@tcip-grundlagen.de

Lektorat: Michael Barabas
Lektoratsassistenz: Julia Griebel
Copy-Editing: Petra Heubach-Erdmann, Düsseldorf
Satz: inpunkt[w]o, Haiger (*www.inpunktwo.de*)
Herstellung: Stefanie Weidner, Frank Heidt
Umschlaggestaltung: Helmut Kraus, *www.exclam.de*
Druck und Bindung: mediaprint solutions GmbH, 33100 Paderborn

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über *http://dnb.d-nb.de* abrufbar.

ISBN:
Print 978-3-86490-960-3
PDF 978-3-96910-957-1
ePub 978-3-96910-958-8
mobi 978-3-96910-959-5

3., aktualisierte und überarbeitete Auflage 2023

Wieblinger Weg 17
69123 Heidelberg

Die Vorauflage dieses Buchs ist 2014 im Heise Verlag (Hannover) erschienen: Gerhard Lienemann/Dirk Larisch: TCP/IP – Grundlagen und Praxis, 2., aktualisierte Auflage (ISBN 978-3-944099-02-6).

Hinweis:
Dieses Buch wurde auf PEFC-zertifiziertem Papier aus nachhaltiger Waldwirtschaft gedruckt. Der Umwelt zuliebe verzichten wir zusätzlich auf die Einschweißfolie.

PEFC zertifiziert
Das Papier für dieses Buch stammt aus nachhaltig bewirtschafteten Wäldern und kontrollierten Quellen.
www.pefc.de
PEFC/04-31-0810

Schreiben Sie uns:
Falls Sie Anregungen, Wünsche und Kommentare haben, lassen Sie es uns wissen: *hallo@dpunkt.de*.

5 4 3 2 1 0

Vorwort

Vor Ihnen liegt nun das Buch »TCP/IP – Grundlagen und Praxis« in der dritten überarbeiteten Auflage. Für mich als Autor ist dies schon eine überaus bemerkenswerte Situation, da sich das Buch mittlerweile – wenn man die Vorgängerbücher (»TCP/IP – Grundlagen« bzw. »TCP/IP – Praxis«) mit einbezieht – über 25 Jahre im Verkauf befindet und offenbar immer noch den einen oder anderen Interessierten anspricht. Das Thema an sich unterliegt zwar keinen sich stets grundlegend ändernden Technologien (was »eine« Erklärung dafür ist). Allerdings haben sich im TCP/IP-Umfeld über die Jahrzehnte Disziplinen herausgebildet, die ohne TCP/IP und die dazugehörige Protokollfamilie nicht denkbar sind.

Denken wir beispielsweise an das Internet der Dinge (IoT = *Internet of Things*), so beruhen sämtliche heute im Einsatz befindlichen »Smart Devices« immer noch auf Adressierung und Kommunikation nach TCP/IP-Netzwerkprotokollen. Eine programmierbare und über WLAN steuerbare Deckenlampe wird danach genauso »angesprochen« wie ein Router im Netzwerk eines Industrieunternehmens. Das wird sich auch in absehbarer Zukunft voraussichtlich nicht ändern (mal davon abgesehen, dass in der alten IP-Version 4 verfügbare Adressen knapp geworden sind und daher die neue IP-Version 6 in vielen Fällen bereits »übernommen« wurde).

Dieses und andere aktuelle Themen habe ich nun in dieses Buch aufgenommen und hoffe, damit den heutigen Anforderungen einer ganzheitlichen Betrachtung des Themas Rechnung zu tragen. Sie werden daher auch keine umfänglichen Rückblicke in die Vergangenheit zur TCP/IP-Historie finden, sondern eher Ausblicke in eine mögliche Zukunft.

Damit Sie sich aber gleich zurechtfinden, wenn Sie das Buch in die Hand nehmen, gebe ich Ihnen nun einen Überblick über die Aktualisierungen, die das Buch hoffentlich zu einem sinnvollen Hilfsmittel auch für das TCP/IP der 20er Jahre unseres Jahrhunderts macht:

Die ersten Kapitel werden Ihnen sicher bekannt vorkommen, wenn Sie eine der vorherigen Auflagen des Buches bereits kennen. Es handelt sich hier um Grundlegendes der TCP/IP-Welt. Allerdings habe ich dort, wo es mir sinnvoll erschien, Passagen oder ganze Kapitel weggelassen und neue Passagen bzw. Unterkapitel ergänzt.

In Kapitel 7 (Sicherheit) habe ich beispielsweise im letzten Abschnitt eine völlig andere Denkweise zur Datensicherheit angestoßen, die nicht – wie in der Vergangenheit – primär auf einen Schutz des Perimeters mit Firewalls setzt, sondern einen Sicherheitsschild als Schichtenmodell zur Diskussion stellt, bei dem die Daten im Mittelpunkt stehen.

In Kapitel 8 (Troubleshooting) habe ich exemplarisch das bekannte Analysetool »WireShark« vorgestellt.

Dem Buch habe ich dieses Mal auch einen Anhang beigefügt, in dem die Themen »Das neue TCP/IP-Umfeld« und »TCP/IP-Konfiguration« angesprochen werden. Während das neue TCP/IP-Umfeld eine kurze Reise in das »Internet der Dinge« unternimmt und verwandte Themen behandelt, habe ich im zweiten Anhang anhand unterschiedlicher Plattformen bzw. Betriebssysteme gezeigt, wie bzw. wo dort TCP/IP-Parameter konfiguriert werden.

Ich wünsche Ihnen viel Freude mit diesem Buch und bitte um viele kritische Kommentare, die ich dann in eine vielleicht nächste Auflage einfließen lassen kann. Sie erreichen mich per E-Mail unter *feedback@tcpip-grundlagen.de*.

Gerhard Lienemann

Inhalt

1 Netzwerke

Wie wir heute wissen, entwickelte sich die zunächst durch Teilung von Ressourcen begründete Netzwerk-Implementierung in Unternehmen (z.B. durch die Einführung von Abteilungsdruckern oder gemeinsam genutzte Speichermedien) in den letzten zwei Jahrzehnten zunehmend zu einem Umfeld komplexer weltweiter Kommunikation. Dabei wurde bereits recht früh der Grundstein für eine Standardisierung der »Sprache der Kommunikation« gelegt. Mit Gründung des Internets in den frühen 80er Jahren des letzten Jahrhunderts wurde die Netzwerkprotokollfamilie »TCP/IP« ins Leben gerufen. Sie sorgte dafür, dass Daten zwischen Kontinenten, Ländern und einzelnen Standorten nach festgelegten Kriterien übertragen werden konnten. Das Regelwerk besitzt bis heute seine Gültigkeit und basiert im Wesentlichen auf die in diesem Kapitel dargestellten Standards.

Schnell entstanden die ersten lokalen Netzwerke (LAN = *Local Area Network*), die dann nach und nach über entsprechende Anbindungen mehr und mehr zu standortübergreifenden WAN-Netzwerken (WAN = *Wide Area Network*) ausgebaut wurden.

1.1 Netzwerkstandards

Wie bei jeder Technologie, so werden auch im Netzwerkbereich bestimmte Vorgaben, Normen oder Standards benötigt, an denen sich die verschiedenen Entwicklungen orientieren. Bei der Behandlung von Netzwerkstandards sind dies insbesondere das ISO/OSI-Referenzmodell sowie die Normierungen und Vorgaben des IEEE *Institute of Electrical and Electronic Engineers* (Institut der elektrischen und elektronischen Ingenieure), aber ebenso auch bestimmte Kommentierungen von Entwicklungen, die unter der Bezeichnung RFC (*Request For Comment*) allgemein üblich sind und vom IETF (*International Engineering Task Force*) verwaltet werden.

1.1.1 OSI als Grundlage

Zur Vereinheitlichung der Datenübertragung wurde das OSI-Referenzmodell geschaffen, das bestimmte Vorgaben für die Kommunikation offener Systeme darlegt. Das OSI-Modell ermöglicht den Herstellern, ihre Produkte für den Netzwerkeinsatz aufeinander abzustimmen und Schnittstellen offenzulegen.

Dies ist somit die Basis für sämtliche Festlegungen im sogenannten ISO- bzw. OSI-Schichtenmodell, wobei die einzelnen Schnittstellen dieser Norm auf insgesamt sieben Schichten, sogenannte *Layer*, verteilt werden. Jede Schicht wiederum erfüllt bei der Kommunikation eine bestimmte Funktion. Das OSI-Schichtenmodell diente in der Vergangenheit, aber auch heutzutage noch generell als Grundlage für die Kommunikationstechnologie. Dabei liegt der Sinn und Zweck darin, dass die Teilnehmer der Kommunikation (z.B. Rechner) über genormte Schnittstellen miteinander kommunizieren. Im Einzelnen setzt sich das OSI-Referenzmodell aus den folgenden Schichten zusammen:

Schicht 1 – Physical Layer

Auf dem *Physical Layer* (physikalische Schicht) wird die physikalische Einheit der Kommunikationsschnittstelle dargestellt. Diese Schicht (Bit-Übertragungsschicht) definiert somit sämtliche Definitionen und Spezifikationen für das Übertragungsmedium (Strom-, Spannungswerte), das Übertragungsverfahren oder auch Vorgaben für die Pinbelegung, Anschlusswiderstände usw.

Schicht 2 – Data Link Layer

Der sogenannte *Data Link Layer* (Verbindungsschicht) ermöglicht eine erste Bewertung der eingehenden Daten. Durch Überprüfung auf die korrekte Reihenfolge und die Vollständigkeit der Datenpakete werden beispielsweise Übertragungsfehler direkt erkannt. Dazu werden die zu sendenden Daten in kleinere Einheiten zerlegt und als Blöcke übertragen. Ist ein Fehler aufgetreten, werden einfach die als fehlerhaft erkannten Blöcke erneut übertragen.

Schicht 3 – Network Layer

Der *Network Layer* (Netzwerkschicht) übernimmt bei einer Übertragung die eigentliche Verwaltung der beteiligten Kommunikationspartner, wobei insbesondere die ankommenden bzw. abgehenden Datenpakete verwaltet werden. In dieser Vermittlungsschicht erfolgt unter anderem eine eindeutige Zuordnung über die Vergabe der Netzwerkadressen, indem der Verbindung weitere Steuer- und Statusinformationen hinzugefügt werden. In einem Netzwerk eingesetzte Router arbeiten immer auf der Schicht 3 des OSI-Referenzmodells.

Schicht 4 – Transport Layer

Auf dem *Transport Layer* (Transportschicht) werden die Verbindungen zwischen den Systemschichten 1 bis 3 und den Anwendungsschichten 5 bis 7 hergestellt. Dies geschieht, indem die Informationen zur Adressierung und zum Ansprechen der Datenendgeräte (z. B. Arbeitsstationen, Terminals) hinzugefügt werden. Aus dem Grund enthält diese Schicht auch die meiste Logik sämtlicher Schichten. Im Transport Layer wird die benötigte Verbindung aufgebaut und die Datenpakete werden entsprechend der Adressierung weitergeleitet. Somit ist diese Schicht unter anderem auch für Multiplexing und Demultiplexing der Daten verantwortlich.

Schicht 5 – Session Layer

Der *Session Layer* (Sitzungsschicht) ist die Steuerungsschicht der Kommunikation, wo der Verbindungsaufbau festgelegt wird. Tritt bei einer Übertragung ein Fehler auf oder kommt es zu einer Unterbrechung, wird dies von dieser Schicht abgefangen und entsprechend ausgewertet.

Schicht 6 – Presentation Layer

Die Anwendungsschicht (*Presentation Layer*) stellt die Möglichkeiten für die Ein- und Ausgabe der Daten bereit. Auf dieser Ebene werden beispielsweise die Dateneingabe und -ausgabe überwacht, Übertragungskonventionen festgelegt oder auch Bildschirmdarstellungen angepasst.

Schicht 7 – Application Layer

Schicht 7 ist die oberste Schicht des OSI-Referenzmodells (*Application Layer*), auf der die Anwendungen zum Einsatz kommen. Dies ist somit die Schnittstelle zwischen dem System (z. B. Rechner oder sonstige Hardware) und einem Anwendungsprogramm.

1.1.2 IEEE-Normen

Neben dem ISO-Schichtenmodell existieren weitere Vorgaben oder Normen für den Netzwerkbereich. Eine wichtige Institution ist dabei das IEEE (*Institute of Electrical and Electronics Engineers*).

Das IEEE (gesprochen *Ai Trippel I*) ist ein Berufsverband für Ingenieure und ein amerikanisches Normungsgremium, das sich generell mit Festlegungen, Standards und Normen für die Kommunikation auf den beiden untersten Ebenen des OSI-Schichtenmodells (*Physical Layer*, *Data Link Layer*) beschäftigt. Die einzelnen Definitionen in Bezug auf die Datenübertragung werden allesamt unter dem Titel des »Komitee 802« zusammengefasst. Eine der ersten Definitionen des Komitees war die Verabschiedung des Ethernet-Zugriffsverfahrens CSMA/CD (*Carrier Sense*

Multiple Access with Collision Detection). Im Dezember 1980 trat eine spezielle Projektgruppe (802.5) zusammen, um das Zugriffsverfahren für den Token-Ring-Bereich zu standardisieren. Ein Jahr später konstituierte sich dann die Token-Bus-Projektgruppe (802.4). Die zahlreichen IEEE-Arbeitsgruppen sind verschiedenen Themen gewidmet und beschäftigen sich vor allem mit Netzwerktopologien, Netzwerkprotokollen oder Netzwerkarchitekturen. Die wichtigsten der Normen und Arbeitsgruppen sind nachfolgend aufgeführt. Details hierzu können aber auch jederzeit auf der Website des IEEE unter *www.ieee.org* nachgelesen werden.

IEEE 802.1

Der IEEE-Standard mit der Bezeichnung 802.1 beschreibt den Austausch der Daten unterschiedlicher Netzwerke. Dazu gehören Angaben zur Netzwerkarchitektur und zum Einsatz von Bridges (Brücken). Zusätzlich erfolgen hier auch Angaben über das Management auf der ersten Schicht (*Physical Layer*). IEEE 802.1 wird in der Fachliteratur auch mit dem Namen *Higher Level Interface Standard* (HLI) bezeichnet.

IEEE 802.1Q

Innerhalb des Arbeitskreises HLI (*Higher Level Interface*) beschäftigt sich die Arbeitsgruppe 802.1Q mit der Definition des Standards für den Einsatz virtueller LANs (VLANs).

IEEE 802.2

Im Arbeitskreis 802.2 wird eine Definition für das Protokoll festgelegt, mit dem die Daten auf der zweiten Ebene des OSI-Modells (*Data Link*) behandelt werden. Dabei wird unterschieden zwischen dem verbindungslosen und dem verbindungsorientierten Dienst. Die Einordnung dieses Standards im OSI-Referenzmodell erfolgt auf Schicht 2.

IEEE 802.3

Dies ist eine Definition, die im Bereich der Netzwerke eine der wichtigsten Vorgaben darstellt, denn mit 802.3 wird neben der Topologie, dem Übertragungsmedium und der Übertragungsgeschwindigkeit auch ein ganz spezielles Zugriffsverfahren beschrieben bzw. vorgegeben: CSMA/CD, was als Abkürzung für *Carrier Sense Multiple Access, Collision Detection* steht. Darüber hinaus werden weitere Definitionen festgelegt, die sich allesamt mit dem Einsatz des Übertragungsmediums befassen (10Base-2, 10Base-5, 10Base-T, 100Base-T, Fast Ethernet, Gigabit Ethernet usw.). Der Standard wird in der Ethernet Working Group des IEEE stets erweitert und aktualisiert. Hier einige Beispiele:

IEEE 802.3ab

Diese Arbeitsgruppe spezifiziert die notwendigen Vorgaben, um den Einsatz von Gigabit Ethernet auf UTP-Kabeln (*Twisted Pair*) der Kategorie 5 zu ermöglichen. Die Standardisierung erfolgte im Jahre 1999.

IEEE 802.3ac

Diese Arbeitsgruppe befasst sich mit MAC-Spezifikationen (*Media Access Control*) und Vorgaben für das Management des Ethernet-Basisstandards, inklusive bestimmter Vorgaben für den Einsatz virtueller LANs (VLANs). Die Standardisierung erfolgte im Jahre 1998.

IEEE 802.3an

Im Jahr 2006 wurde der Standard 802.3an verabschiedet, der eine Übertragung von 10 Gbit auf herkömmlichen Kupferkabeln des Typs *Twisted Pair* vorsieht. Beim Einsatz von Cat6-Kabeln können Daten über eine Distanz von 100 Metern übertragen werden, mit Cat5e-Kabeln immerhin noch über eine Distanz von 22 Metern.

IEEE 802.3db

Diese Gruppe innerhalb des neueren Projekts 802.3-2018 beschäftigt sich mit den physischen Spezifikationen und Parametern für den Betrieb von 100-, 200- und 400-Gigabit-Ethernet-Netzwerken via Glasfaser unter Verwendung einer 100-Gigabit-Signalisierung. Dieser Standard wurde am 3. Juni 2020 verabschiedet und hat zunächst eine Laufzeit bis zum 31. Dezember 2024.

IEEE 802.3z

Diese Arbeitsgruppe legt Standards für Gigabit Ethernet fest, insbesondere für den Einsatz von Gigabit Ethernet auf Kupferkabeln der Kategorie 5 (siehe auch 802.3ab), aber ebenso für die Übertragung mittels Glasfaserkabel. Dieser Standard wurde im Jahre 1998 verabschiedet.

IEEE 802.4

Während sich 802.3 mit Ethernet beschäftigt, wird in der Definition 802.4 der Token-Bus-Standard proklamiert und entsprechende Festlegungen werden getroffen.

IEEE 802.5

Als Ergänzung zu 802.4 legt dieser Arbeitskreis eine Definition für den Token Ring fest. Dazu zählt die Definition der Topologie, des Source Routing, des Übertragungsmediums und auch der Übertragungsgeschwindigkeit.

IEEE 802.6

Dieser Standard beschreibt den Einsatz von MANs, also die sogenannten *Metropolitan Area Networks*. Zusätzlich beschäftigt sich diese Gruppe auch mit dem Bereich der DQDB-Protokolle (*Distributed Queue Dual Bus*).

IEEE 802.7

Mit den Festlegungen innerhalb dieser Arbeitsgruppe (*Broadband Technical*) werden bzw. wurden Vorgaben für den Einsatz der Breitbandtechnologie festgelegt.

IEEE 802.8

802.8 beschäftigt sich ausschließlich mit dem Einsatz von Lichtwellenleitern bzw. Glasfaserkabeln (*Fiber Optic*) innerhalb eines Netzwerks.

IEEE 802.9

Die Inhalte dieses Standards beziehen sich auf die Einbeziehung von Sprachübertragung in die allgemeine Kommunikation. Auf diese Art und Weise sollen in einem solchen ISLAN (*Integrated Services LAN*) alle Datenendgeräte (Rechner, Drucker, Telefon, Fax usw.) an einer einzigen Schnittstelle betrieben werden können.

IEEE 802.9a

Die isochrone Technik für die Echtzeitübertragung von Daten im LAN bis an den Arbeitsplatz ist Inhalt dieser Arbeitsgruppe.

IEEE 802.10

Der Arbeitskreis mit der Bezeichnung 802.10 beschäftigt sich vornehmlich mit generellen Sicherheitsfragen. Zu diesem Zweck wurde auch eine entsprechende Vorgabe verabschiedet, die den Namen SILS trägt (*Standard for Interoperable LAN Security*).

IEEE 802.11

Die in 802.11 zusammengesetzte Projektgruppe beschäftigt sich mit dem Einsatz drahtloser LANs (WLAN). Auf die einzelnen Basis-Standards dieser Projektgruppe wird in Abschnitt 1.2.2 näher eingegangen.

IEEE 802.12

Ergebnis dieser Arbeitsgruppe ist ein Standard für ein 100-Mbit-Verfahren für den Multimedia-Einsatz, das den Namen *Demand Priority* (DP) trägt. Es handelt sich dabei um ein Zugriffsverfahren (vergleichbar mit CSMA/CD aus 802.3), bei dem ein Repeater die einzelnen Datenendgeräte nach Übertragungswünschen abfragt (Polling-Verfahren).

IEEE 802.14

Der Auftrag der 802.14-Arbeitsgruppe besteht bzw. bestand darin, Standards und Normen für den Bereich von Kommunikationsfunktionen in Kabelnetzen (Kabelfernsehen) auszuarbeiten. Diese Bestrebungen sind in der Literatur auch häufig unter der Abkürzung CATV (*Cable Television*) zu finden.

IEEE 802.15

Die kabellose Anbindung von Rechnern ist Auftrag dieser Arbeitsgruppe. In Erweiterung zur Arbeitsgruppe 802.11, die sich mit drahtlosen LANs (WLANs) beschäftigt, wird in dieser Gruppe die Gesamtheit der kabellosen Anbindungsmöglichkeiten auf Basis des WPAN (*Wireless Personal Area Network*) betrachtet. Darunter fallen beispielsweise Technologien für den kabellosen Einsatz auf kurzen Distanzen (z. B. Bluetooth, ZigBee).

IEEE 802.16

Als Ergänzung zur Arbeitsgruppe 802.15 beschäftigt sich diese Arbeitsgruppe mit der kabellosen Anbindung in der Breitbandtechnik. Bekannt geworden ist diese Technik unter dem Namen WIMAX (*Worldwide Interoperability for Microwave Access*), die als Alternative zum Festnetz-DSL angesehen werden kann.

1.2 Netzwerkvarianten

Neben Festlegungen, Standards und Normen entscheiden letztlich der Anwender und natürlich die Industrie über entsprechende Produktpaletten, also welche Formen der Netzwerkvarianten zum Einsatz kommen. Heutzutage kann man festhalten, dass bei sämtlichen Neuinstallationen fast durchweg der Netzwerktyp *Ethernet* verwendet wird. Was es damit auf sich hat und welche sonstigen Varianten darüber hinaus zur Verfügung stehen (Token Ring, ATM usw.), wird in Abschnitt 1.2.4 in einer Übersicht dargestellt.

Während sich Ethernet und Token Ring als etablierte LAN-Standards im Laufe der letzten Jahrzehnte in den Unternehmen als verlässliche Kommunikationsgebilde durchgesetzt haben und FDDI bzw. ATM als Hochgeschwindigkeitstechnologie mit hohen Übertragungskapazitäten in Backbones eingesetzt wurden, wurden Fast Ethernet und Gigabit Ethernet für Hochgeschwindigkeits-LANs mit gewachsenen Anforderungen immer bedeutsamer und sind in zahlreichen Netzwerken bereits vollständig implementiert.

Noch Ende des vergangenen Jahrhunderts reichten Ethernet-Kapazitäten von 2 bis 10 Mbit/s und Token-Ring-Geschwindigkeiten von 4 bis 16 Mbit/s für den anfallenden Datenverkehr völlig aus. Diese Situation hat sich mittlerweile jedoch deutlich verändert, da die Übertragung multimedialer Objekte wie Bilder, Grafiken, Video- und Audiosequenzen in Netzwerken immer wichtiger geworden

ist. Netzwerkstrukturen, die unter den Schlagworten *Corporate Networking*, *Voice over IP* oder *Videoconferencing* zusammengefasst werden, tragen dazu bei, höchste Bandbreiten im lokalen Netzwerk zur Verfügung stellen zu müssen, sodass der Bedarf an Hochgeschwindigkeitstechnologien wie dem Gigabit Ethernet mit Kapazitäten von 1.000, 10.000 Mbit/s und mehr nur eine Frage der Zeit war.

Zwar entwickelte man auch für die Token-Ring-Technik Komponenten mit höherer Leistung (*High Speed Token Ring* = HSTR), es zeigte sich aber, dass der Markt diese Technik nur dann annahm, wenn ein Unternehmen, das bereits primär Token-Ring-Netzwerke einsetzte, auf eine deutlich höhere LAN-Geschwindigkeit umstellen musste und den Wechsel zu Ethernet nicht vornehmen wollte. Heute ist die Token-Ring-Technologie auf globaler Basis weitgehend verschwunden und wird auch nicht mehr weiterentwickelt, sodass in diesem Buch fast ausschließlich Ethernet als Netzwerkvariante im Detail erläutert wird.

1.2.1 Ethernet

Durch Einsatz eines speziellen Zugriffsverfahrens mit dem Namen CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*) verdichtete sich bereits in den 70er Jahren des vorigen Jahrhunderts der Ethernet-Standard. Dabei repräsentiert Ethernet einen Standard, der physikalisch auf einer reinen Bus-Topologie beruht. Diesen Bus kann man sich als ein Kabel vorstellen, das an seinen beiden Enden durch jeweils einen Abschlusswiderstand terminiert wird (Terminator) und über sogenannte Transceiver dem jeweiligen Endgerät (z. B. Rechner mit Ethernet-Netzwerkcontroller) einen Netzwerkzugang ermöglicht.

Auch wenn es für die Hochgeschwindigkeitstechnologien alternative LAN-Zugriffsverfahren bzw. entsprechende Entwicklungen gab (z. B. 100VG-AnyLAN), hat sich heutzutage Ethernet mit dem CSMA/CD-Verfahren als Grundlage und Standard durchgesetzt. Dabei beruht das CSMA/CD-Verfahren auf folgenden Überlegungen:

Eine Station (Rechner in einem lokalen Netzwerk) möchte Daten übertragen. Zu diesem Zweck versucht sie, über die eingebaute Netzwerkkarte auf dem Übertragungsmedium zu erkennen, ob eine andere Station Daten überträgt (*Carrier Sense*). Wenn das Medium besetzt ist (*Collision Detection*), zieht sich die Station wieder zurück und wiederholt diesen Vorgang in unregelmäßigen Abständen, bis die Leitung frei ist. Dann beginnt sie mit dem Übertragungsvorgang. Alle am Netz befindlichen Rechner überprüfen den *Header* des ankommenden Datenpakets (*Frame*), und nur derjenige, dessen eigene Adresse mit der Zieladresse im Frame übereinstimmt, beginnt mit dem Empfangsprozess (siehe Abb. 1–1).

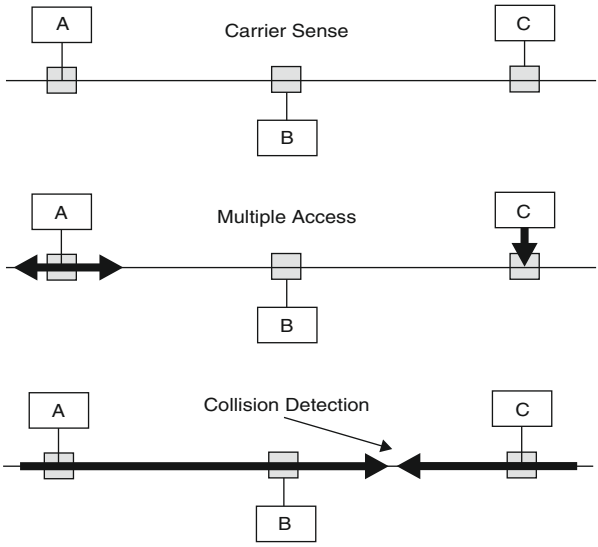

Abb. 1–1 *CSMA/CD-Zugriffsverfahren im Ethernet*

Dabei ist bei der gleichzeitigen Übertragung mehrerer Stationen zu beachten, dass das Prinzip der Kollisionserkennung (*Collision Detection*) dazu führt, dass die erste sendende Station ihren Sendeprozess unmittelbar abbricht und ein Störsignal (Jam-Signal) produziert. Ein erneuter Sendeversuch wird innerhalb zufällig generierter Intervalle wiederholt. Zufällig gebildete Intervalle minimieren das Risiko überproportional steigender Kollisionen. Kommt nach weiteren Sendeversuchen mit unterschiedlich langen Wartezeiten und fünf weiteren, gleich großen Zeitintervallen keine störungsfreie Übertragung zustande, wird die nächsthöhere Protokollschicht informiert und muss nun ihrerseits geeignete Sicherungsmechanismen durchführen.

Bei der Betrachtung des Ethernet-Standards (Version 2) ist zu berücksichtigen, dass dieser leicht vom 802.3-Standard abweicht. Die Differenzen zeigen sich insbesondere in unterschiedlichen maximalen Signalrundlaufzeiten und im Aufbau der Datenpakete (*Frames*). So befindet sich im Ethernet-Frame auf Byte-Position 20 ein Zwei-Byte-Typenfeld, aus dem das hier eingesetzte höhere Protokoll hervorgeht. Anschließend beginnt der Datenteil. Im IEEE-802.3-Frame hingegen fehlt das Typenfeld. Stattdessen gibt es ein gleich großes Längenfeld, in dem die Gesamtlänge des Frames eingesetzt wird. Anschließend folgt der LLC-Header (*Logical Link Control*) mit den Daten. Daraus ergibt sich eine Inkompatibilität von Rechnern, die mit diesen beiden Standards arbeiten und miteinander kommunizieren wollen. In Abbildung 1–2 sind die Unterschiede im Frame-Aufbau dargestellt.

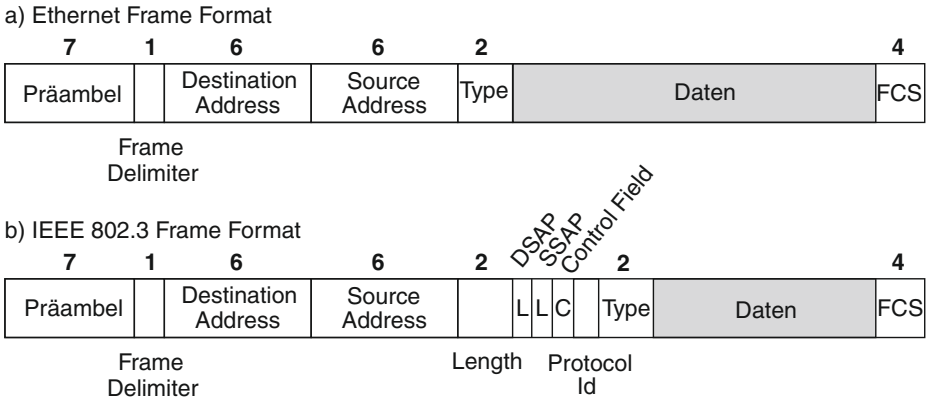

Abb. 1–2 *Unterschiede im Aufbau der Datenpakete*

Fast Ethernet

Fast Ethernet beschreibt einen als IEEE 802.3u definierten Standard, der aus dem klassischen Ethernet hervorgegangen ist. Seine Implementierung wird als 100BaseT bezeichnet und stellt eine Bandbreite von 100 Mbit/s zur Verfügung. 100BaseT beruht auf dem IEEE-802.3-Standard und ist somit in der Lage, beide Geschwindigkeiten, also sowohl 10 Mbit/s als auch 100 Mbit/s, im lokalen Netzwerk zu realisieren. Auch das Frame-Format ist für beide Implementierungen identisch.

Da 100BaseT das gleiche Zugriffsverfahren wie 10BaseT verwendet (CSMA/CD), ist eine Reduktion der als *Collision Domain* bezeichneten Entfernung zwischen zwei Ethernet-Stationen von etwa 2000 Metern auf 200 Metern erforderlich. Das Design einzelner Netzwerksegmente ist abhängig von den für dieses Verfahren eingesetzten Medien. 100BaseTX-, 100BaseFX- und 100BaseT4-Medien unterscheiden sich jeweils im Kabeltyp, in der Anzahl einzelner Adern und in den verwendeten Anschlusstypen. Fast Ethernet hat in den letzten Jahren jedoch deutlich an Bedeutung verloren und wird zunehmend durch die neueren Gigabit-Standards ersetzt. Dies gilt nicht nur für industrielle Netzwerke, sondern auch für die eingesetzten Netzkomponenten im privaten Bereich.

Gigabit Ethernet

Die unmittelbare Weiterentwicklung von Fast Ethernet stellt Gigabit Ethernet dar. Aus Sicht des ISO/OSI-Layers 2 (*Data Link Control*) in Richtung höherer Protokollschichten ist die Architektur von Gigabit Ethernet mit dem IEEE-802.3-Standard identisch. Allerdings mussten die 1999 neu geschaffenen Standards IEEE 802.3z (Gigabit Ethernet über Glasfaser) und IEEE 802.3ab (Gigabit Ethernet über Kupferkabel 1000BaseT) hinsichtlich der physikalischen Schicht angepasst werden, damit Geschwindigkeiten von bis zu 1000 Mbit/s erreicht werden können.

Die leicht modifizierte Gigabit-Ethernet-Architektur geht aus Abbildung 1–3 hervor. Eine medienunabhängige Schnittstelle (GMII = *Gigabit Media Independent*

Interface) innerhalb der physikalischen Schicht sorgt für Transparenz gegenüber den höheren Protokollschichten.

Das Medium spielt beim Gigabit Ethernet eine herausragende Rolle. Glasfaserkabel (Medien 1000BaseCX, 1000BaseLX und 1000BaseSX) sind aufgrund ihrer Materialbeschaffenheit und der anwendbaren Codierungsverfahren für solch hohe Geschwindigkeiten besonders gut geeignet. Aber auch die am 1000BaseT orientierten Twisted-Pair-Kabel lassen sich für das Gigabit Ethernet verwenden, vorausgesetzt, es werden alle vier Adernpaare für die Signalübermittlung verwendet (für 10BaseT oder 100BaseT sind zwei der vier Adernpaare ausreichend). Während der Einsatz des Glasfaserkabels Übertragungsstrecken bis zu 5000 Metern erlaubt, verringert sich die Distanz beim 1000BaseT, also beim Kupferkabel, auf etwa 100 Meter. Dieses ist daher lediglich zur Überwindung kurzer Entfernungen bzw. innerhalb von Verteilerschränken verwendbar.

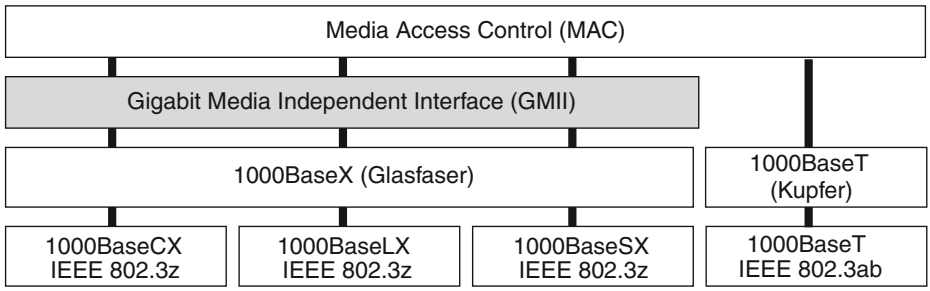

Abb. 1–3 *Darstellung der modifizierten Architektur bei Gigabit Ethernet*

Heute beschäftigen sich technische Arbeitsgruppen (z.B. im IEEE im Projekt 802.3 df) bereits mit der Spezifikation und Implementierung von 800 Gigabit Ethernet (GbE) oder gar 1,6 Terabit Ethernet (TbE).

100VG-AnyLAN

Parallel zur Entwicklung von Fast Ethernet wurde im letzten Jahrhundert die 100VG-AnyLAN-Technologie geschaffen, die alternativ andere LAN-Zugriffsverfahren als das CSMA/CD nutzen kann.

Im IEEE-802.12-Standard ist das von Hewlett Packard entwickelte 100VG-AnyLAN als Alternative zum CSMA/CD-Zugriffsverfahren definiert und kann gewissermaßen als Synthese aus Ethernet und Token Ring betrachtet werden; weder Token Ring noch 100VG-AnyLAN haben heutzutage jedoch noch eine praktische Bedeutung. Der LAN-Zugriff wird im Wesentlichen vom angeschlossenen Hub oder Switch bestimmt und vermeidet zufällig orientierte Zugriffszyklen wie beim CSMA/CD-Verfahren. Konkurrierende Übertragungsanfragen werden vom Hub nach Prioritäten abgewickelt (nur eine einzige Station kann zu einem bestimmten Zeitpunkt Daten übertragen – Kollisionen werden somit vermieden), sodass sich diese Technologie besonders für Multimedia-Datenverkehr eignet. Es besteht

eine Frame-Kompatibilität zu Ethernet- und Token-Ring-Netzwerken, sodass ein 100VG-AnyLAN-Segment einfach durch Installation einer Bridge in bestehende Ethernet- oder Token-Ring-Segmente integriert werden kann.

HINWEIS

Die Netzwerkvariante 100VG-AnyLAN hat heutzutage so gut wie keine Bedeutung mehr und kommt insbesondere bei Neuinstallation nicht mehr zum Einsatz.

1.2.2 Wireless LAN (IEEE 802.11)

Überall dort, wo eine Verkabelung zur Einrichtung eines Netzwerks nicht infrage kommt oder besondere Anforderungen hinsichtlich der Mobilität vorliegen, ist der Einsatz funkbasierter Kommunikationstechnologien zu empfehlen. Die heute verfügbare Technik liefert ausreichend Möglichkeiten, um die in einem Netzwerk erforderlichen Aufgaben zufriedenstellend zu lösen. Nachfolgend sind die verfügbaren Standards, Komponenten und die erforderlichen Sicherheitsmechanismen erläutert.

WLAN-Standards

Im Standard IEEE 802.11, der in seinen Einzelstandards die heute verfügbaren Techniken darstellt, sind die wesentlichen Merkmale und Funktionen erläutert und definiert. Hier einige wichtige Beispiele:

- *IEEE 802.11a*
  WLAN-Standard (1999), der auf einer Brutto-Datenrate von etwa 54 Mbit/s und dem 5-GHz-Band basiert. Seit November 2002 ist dieser Standard auch für Deutschland zugelassen (gem. Order Nr. 35/2002 vom 13. November 2002 – Regulierungsbehörde für Telekommunikation und Post).
- *IEEE 802.11b*
  WLAN-Standard (1999), der auf einer Brutto-Datenrate von etwa 11 Mbit/s und dem 2,4-GHz-Band basiert. Es handelt sich hierbei um die derzeit verbreitetste WLAN-Variante.
- *IEEE 802.11g*
  WLAN-Standard aus dem Jahr 2003, der auf einer Brutto-Datenrate von etwa 54 Mbit/s und dem 2,4-GHz-Band basiert. Dieser Standard ist abwärtskompatibel zu IEEE 802.11b, sodass hier ein zukünftig hoher Verbreitungsgrad sehr wahrscheinlich ist.
- *IEEE 802.11h*
  WLAN-Standard, der eine Adaption des IEEE-802.11a-Standards für Europa repräsentiert. In Europa erfolgt die Radar-Kommunikation ebenfalls im 5-GHz-Band, sodass hier besondere Vorkehrungen zur Steuerung der Datenübertragung vorgenommen werden müssen.

- *IEEE 802.11n (Wi-Fi 4)*
  Der sogenannte »n-Standard« 802.11n wurde Ende 2009 verabschiedet und ermöglicht eine Brutto-Datenrate von theoretisch bis zu 600 Mbit/s. Die Übertragung erfolgt im 2,4-GHz-Band und optional auch unter 5 GHz.
- *IEEE 802.11ac (Wi-Fi 5)*
  IEEE 802.11ac stellt die Weiterentwicklung des 802.11n-Standards dar und sorgt für eine Verbesserung der theoretischen Übertragungsgeschwindigkeit auf mehr als das Doppelte (1,2 Gbit/s). Außerdem liefert es eine weitaus stabilere Datenübertragung auf hohem Niveau. Diese Stabilität konnte der Vorgänger Wi-Fi 4 nicht bieten, da er nicht über das Beam-Forming-Verfahren verfügt und somit eine gezielte Ausrichtung des Funksignals auf Endgeräte und Access Points unter Verwendung mehrerer (mindestens zwei) Antennen möglich ist.
- *IEEE 802.11ax (Wi-Fi 6)*
  Der seit Anfang 2020 etablierte Standard IEEE 802.11ax liefert im 2,4-GHz- und 5-GHz-Frequenzband mittlerweile eine vielfach höhere Datenübertragungsrate von theoretisch 10 Gbit/s und mehr, da der Datenstrom parallel mehrere Geräte erreichen kann. Die theoretischen Geschwindigkeiten sind allerdings nur unter Laborbedingungen realisierbar. In der Praxis sorgen sich gegenseitig störende Router und nicht immer optimale Signalqualitäten für deutliche Performance-Einbrüche; insbesondere für vom Router entfernte Endgeräte (Wi-Fi 6 benötigt zur Ausnutzung seiner erhöhten Geschwindigkeiten ein sehr gutes Signal).
- *IEEE 802.11ad*
  IEEE 802.11ad nutzt ein völlig anderes Frequenzband als die zuvor dargestellten Standards: das 60-GHz-Band. Hier sind sehr hohe Geschwindigkeiten von bis zu 7 Gbit/s möglich und durch die Frequenzbandunabhängigkeit ist eine Kommunikation gegenüber Störungen kaum anfällig. Allerdings ist die Reichweite der Kommunikation auf etwa 9 Meter beschränkt, sodass dieser Standard eher innerhalb von Räumen bzw. eng umfassten Bereichen eingesetzt wird (z.B. bei der Übertragung von hoch aufgelösten Videos, wie 4K). Dieser Standard wird gemeinsam mit dem IEEE 802.11ay auch als *Wireless Gigabit* bezeichnet.
- *IEEE 802.11ah*
  Die Besonderheit dieses Funkstandards ist seine erhöhte Reichweite. Er wird im 900-MHz-Band betrieben und liefert Datenkommunikation bis zu 1 km Entfernung allerdings mit einer niedrigen Datenrate von mindestens 100 kbit/s. Dieser Standard wird auch als Low-Power-Wi-Fi oder offiziell auch Wi-Fi HaLow bezeichnet. Er kommt primär bei der Datenkommunikation im SmartHome-Bereich (auch in IoT- – *Internet of Things* – Umgebungen) zum Einsatz, da der geringe Energieverbrauch und die Robustheit gegenüber Hindernissen und »dicken Betonwänden« einen gegenüber anderen WLAN-Standards deutlichen Vorteil bedeuten. Dies ist allerdings derzeit nur Theorie. Stand Anfang 2022 gibt

es kaum Produkte für diesen Standard auf dem Markt, auch wenn von der Wi-Fi-Alliance für die nächsten Jahre vielversprechende Erfolge prognostiziert werden (Wi-Fi-Alliance-Veröffentlichung vom 2. November 2021, Austin, Texas: *WiFi Certified HaLow delivers long range, low power WiFi*).

- *IEEE 802.11ay*
  Als Erweiterung und Verbesserung des IEEE-802.11ad-Standards wurde IEEE 802.11ay im März 2021 mit einer deutlich höheren Datenrate von 20–40 Gbit/s verabschiedet. Reichweite: ca. 300 bis 500 Meter.
- *IEEE 802.11be (Wi-Fi 7)*
  Dieser Standard stellt die Weiterentwicklung des Wi-Fi 6 dar und soll u.a. eine bis zu vier Mal höhere Datenrate ermöglichen. Man erwartet somit Datenübertragungsraten von 30 bis 40 Gbit/s. Ein weiterer Fokus liegt auf datenintensiven Echtzeit-Anwendungen zum Beispiel im Bereich Virtual oder Extended Reality. Damit wird Wi-Fi 7 zu einer ersten ernst zu nehmenden Alternative zum Festnetz-Ethernet. Derzeit erwartet man allerdings eine Standardisierung erst für das Jahr 2024.

HINWEIS

Sämtlichen heute im Einsatz befindlichen WLAN-Standards ist gleich, dass es sich um ein *Shared Medium* handelt; dies bedeutet, dass sich die angegebene Bandbreite jeweils nur auf einen einzigen Netzwerkknoten bezieht. Nutzen mehr als ein Knoten (z.B. mehrere Rechner) das Netzwerk, so muss die verfügbare Bandbreite geteilt werden. Zusätzlich reduzieren Störeinflüsse im Funknetz die Übertragungsqualität der Daten, sodass in einem WLAN in der Praxis beispielsweise bei mehreren miteinander kommunizierenden Rechnern (je nach genutztem Standard) von deutlich reduzierten Übertragungsraten ausgegangen werden muss.

Komponenten

In einem WLAN spielt der Begriff »Zelle« eine entscheidende Rolle. Eine Zelle bezeichnet die Zusammenfassung einzelner im WLAN miteinander kommunizierender Netzwerkknoten. Die Identifikation einer Zelle erfolgt über den sog. ESSID (*Extended Service Set Identifier*). Jeder Zelle sollte im WLAN ein eigener Funkkanal zugeordnet werden.

In einem WLAN lassen sich grundsätzlich zwei verschiedene Topologieformen antreffen:

- *Ad-hoc-Modus*
  Dem Ad-hoc-Modus liegt eine direkte Kommunikation der einzelnen Netzwerkknoten zugrunde. Grundsätzlich kommuniziert hier jeder mit jedem und verwendet dabei die gemeinsam zugeordnete ESSID. Eine solche Topologie ist zumeist dann vorteilhaft, wenn lediglich kleine überschaubare Netzwerke (z.B. für temporäre Arbeitsgruppen oder Besprechungen) gebildet werden sollen. Eine Ad-hoc-Topologie ist mit dem übrigen Netzwerk nicht verbunden und stellt somit eine

autonome Kommunikationseinheit dar. In einer Sonderform des Ad-hoc-Netzwerks ermöglicht ein nach IEEE 802.11s konzipiertes WLAN Mesh (vermaschtes Funknetz) die »Selbst-Organisation« von Netzwerk-Teilnehmern (zumeist mobile Endgeräte wie Handys, Tablets, Sensoren, Smart Devices usw.).

- *Infrastruktur-Modus*
  Der Topologie-Infrastruktur-Modus stellt in einem WLAN den Regelfall dar. Hier werden sogenannte *Access Points* benötigt, die den Zugang zum kabelbasierten Netzwerk herstellen und somit die Funkzelle in das übrige Unternehmensnetzwerk integrieren. Der Infrastruktur-Modus ermöglicht die Nutzung gemeinsamer Netzwerkressourcen (Festplatten, Drucker, Kommunikationseinrichtungen usw.), siehe hierzu auch Abbildung 1–4.

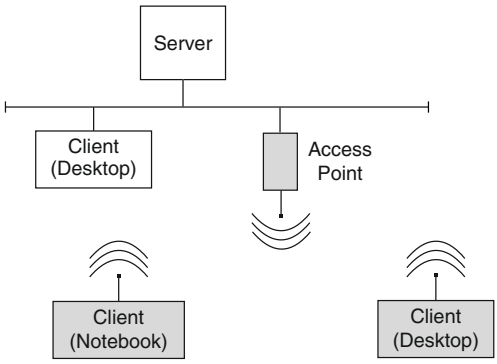

Abb. 1–4 *WLAN-Betrieb im Infrastruktur-Modus*

Neben den unterschiedlichen Topologien gibt es in einem WLAN weitere charakteristische Komponenten oder Merkmale, die nachfolgend erläutert werden.

- *Access Point*
  Wie bereits erwähnt, kommen Access Points lediglich in Infrastruktur-Modus-Netzwerken zum Einsatz; sie stellen dort die Schnittstelle zwischen Funknetz und dem kabelgebundenen Netzwerk dar. Der gesamte Datenverkehr der Funkzelle wird über einen Access Point geführt, sofern mit dem Kabelnetz kommuniziert werden soll. Er ist Medienübergang, Brücke und Schnittstelle zwischen den Netzwerken. Zahlreiche Router- oder Switch-Hersteller bieten ihre Geräte bereits in einer Access-Point-Variante an.
- *WLAN-Controller*
  Jeder Netzwerkknoten muss zur Funkkommunikation in einem WLAN mit einem WLAN-Controller ausgestattet sein. Je nach Endgerät handelt es sich um eine PC-Steckkarte, einen USB-Dongle oder um eingebaute Komponenten, die fest mit der übrigen Hardware verbunden sind. Mittlerweile werden heute Notebooks, Tablets oder auch Mobilfunkgeräte mit eingebauten WLAN-Controllern ausgestattet, sodass der separate Einsatz von Zusatzkarten nicht mehr erforderlich ist.

- *Antennen*
  WLAN-Controller und Access Points besitzen jeweils unterschiedlich ausgeprägte Antennen, die für den Versand und Empfang der Daten zuständig sind. Je nach Hardwareerfordernissen handelt es sich dabei um Flachantennen, kleine Stabantennen oder größere Richtantennen, um die Funkreichweite zu vergrößern.

WLAN-Charakteristik

Die Schicht *Physical Layer* im ISO/OSI-Referenzmodell auf Schicht 1 wird beim IEEE-802.11-Standard durch einen PMD- und einen PLCP-Sub-Layer dargestellt. Während der PMD (*Physical Medium Dependent Sub-Layer*) für die Signalmodulation und -codierung zuständig ist, bildet das PLCP (*Physical Layer Convergence Protocol*) die allgemeingültige Schnittstelle zur übergelagerten Steuerungsschicht (*MAC Layer*).

Bei der physikalischen Datenübertragung werden in Funknetzen nach IEEE 802.11 zur Erhöhung der Datensicherheit sogenannte *Spread-Spectrum-Technologien* eingesetzt. Die beiden Verfahren lauten FHSS (*Frequency Hopping Spread Spectrum*) und DSSS (*Direct Sequence Spread Spectrum*).

Bei FHSS wechseln Sender und Empfänger zyklisch die benutzte Frequenz, wobei sie die gleiche Reihenfolge einhalten (*Hopping Sequence*). Die durch andere Sender verursachten Störungen werden minimiert, da nur diejenigen Sender und Empfänger miteinander kommunizieren können, die auch mit gleicher Hopping Sequence arbeiten. Bei diesem Verfahren ist allerdings der technische Aufwand auf der MAC-Ebene recht hoch, da die Frequenzwechsel gesteuert und synchronisiert werden müssen. Aufgrund besserer Leistungswerte hat sich jedoch DSSS – insbesondere für IEEE 802.11b – durchgesetzt. Im Gegensatz zu FHSS wird bei DSSS das Signal nicht zeitlich versetzt auf verschiedenen Kanälen versendet, sondern als schmalbandiges Signal durch Multiplexe mit einem PN-Code (*Pseudo-Noise*) direkt in ein breitbandiges Signal umgewandelt. Da dadurch die Sendeintensität unter die Rauschgrenze abgesenkt wird, kann das Signal nur noch von Stationen empfangen werden, die mit dem gleichen PN-Code arbeiten.

Der MAC-Layer weist bei 802.11 eine enge Verwandtschaft mit der kabelgebundenen Variante 802.3 auf. Allerdings muss der drahtlose Standard auf die Besonderheiten der Übertragungsstrecke Rücksicht nehmen. Aufgrund der Signalcharakteristik entfällt die Möglichkeit zum Erkennen von Kollisionen. Daher greift 802.11 auf eine Zugangskontrolle nach dem CSMA/CA-Verfahren zurück.

CSMA/CA steht für *Carrier Sense Multiple Access with Collision Avoidance*. Es beschreibt den Zugriff auf einen gemeinsamen Kanal, indem dieser auf das Vorhandensein eines Trägersignals getestet wird. Der Unterschied zu IEEE 802.3 besteht in der *Collision Avoidance* (Kollisionsvermeidung), deren Implementierung als DCF (*Distributed Coordination Function*) oder PCF (*Point Coordination Function*) realisiert wird. Das DCF-Verfahren wird insbesondere im *Ad-hoc-Modus* eingesetzt, während das PCF-Verfahren im Infrastrukturbetrieb (Verwen-

dung von Access Points, die beispielsweise zur Koordination der Kanalvergabe verwendet werden) zur Anwendung kommt.

Für eine ungefähre Einschätzung der möglichen Reichweiten (z.B. bei IEEE 802.11b) ist es wenig sinnvoll, theoretische Werte zugrunde zu legen. Danach wäre bei einer Netto-Datenrate von etwa 2 Mbit/s eine Reichweite von etwa 400 Metern im Freien und etwa 45 Metern in geschlossenen Räumen realisierbar. Tatsächlich kann davon ausgegangen werden, dass in einer »normalen Bürolandschaft« bei der Durchquerung einer Etagendecke und dreier weiterer Wände (Entfernung ca. 5 Meter Luftlinie) ein Netto-Datendurchsatz von vielleicht 500 bis 700 kbit/s erreicht werden kann. Ähnliche Werte erhält man auch bei einer Messung auf derselben Etage bei Durchquerung von drei Raumwänden. Es ist daher festzustellen, dass die theoretischen Werte in Realumgebungen stark relativiert werden müssen. Eine wesentlich günstigere Umgebung (z.B. bei freier Fläche) ist dagegen eher selten anzutreffen.

Im Unterschied zum kabelbasierten Netzwerk, in dem störende Einwirkungen von außen heute relativ selten auftreten, ist das Funknetz bei der Datenübertragung zahlreichen Einflüssen ausgesetzt. So ist beispielsweise die Verwendung von Metall in Gebäuden für ein WLAN äußerst hinderlich, da die Dämpfung der Funkwellen eine Kommunikation deutlich beeinträchtigt. Aber auch die Verarbeitung von Stahlbeton führt zu einer nachteiligen Charakteristik. Im Wesentlichen störungsfrei erfolgt die Kommunikation in freier Natur oder auch bei der Durchquerung von Holzwänden oder Glas. Eine Störquelle der besonderen Art kann ein Mikrowellengerät darstellen. Da dieses auf der gleichen Frequenz »funkt« und zudem eine – trotz Abschirmung – oft mehr als hundertfache Abstrahlung produziert, sollte ein WLAN Access Point oder WLAN-Controller in möglichst ausreichender Entfernung zum Mikrowellengerät positioniert werden.

Unter Hotspots versteht man öffentliche WLAN-Zugangspunkte, die an Flughäfen, in Restaurants, Krankenhäusern oder Hotels den Gästen bzw. Patienten zur Verfügung gestellt werden. Die Abrechnung für die Dauer der Nutzung erfolgt entweder über bereits vorhandene Identifikationskriterien (Benutzername, Kennwort) bei sogenannten WISPs (*Wireless Internet Service Provider*) oder auch anderen Providern, bei denen der Kunde bereits ein Abrechnungskonto besitzt (z.B. Mobilfunk-Provider). In einigen Fällen kann die Nutzung auch aufgrund käuflich erworbener Zeitkontingente erfolgen.

Sicherheitsaspekte

Insbesondere bei der Nutzung von Hotspots ist die Sicherheit der Datenkommunikation von großer Bedeutung. Funknetze bieten wegen der recht einfachen Zugangsmöglichkeit eine besonders gute Angriffsfläche für Hacker bzw. Cracker, sofern keine ausreichenden Sicherheitsmaßnahmen getroffen wurden. Die folgende Aufstellung zeigt eine Übersicht der wichtigsten Kriterien, die für die Realisierung einer minimalen Basissicherheit in WLANs berücksichtigt werden sollten:

- *ESSID*
  Die ESSID (*Extended Service Set Identifier*) ermöglicht die Zuordnung einer eindeutigen ID. Bei vielen Produkten wird als Standardwert für die ESSID der Modellname des WLAN-Routers verwendet. Wird hier keine eigene Kennung der WLAN-Zelle vergeben, ist die Wahrscheinlichkeit unliebsamer »Zuhörer« während der eigenen Kommunikation recht hoch. Da diese Kennung bei Hotspots in der Regel allen Benutzern bekannt gemacht wird, ist die Sicherheitsqualität der ESSID eher fragwürdig.
- *MAC-Adresse*
  Jeder WLAN-Controller besitzt – wie übrigens jede andere Netzwerkkomponente auch – eine weltweit eindeutige *burnt-in address*. Diese Adresse (MAC = *Media Access Control*) sollte bei der Konfiguration des Access Point dediziert angegeben werden, sodass ein Zugriff von Benutzern mit anderen MAC-Adressen zurückgewiesen wird.
- *DHCP*
  Die Aktivierung der dynamischen Vergabe von IP-Adressen mittels DHCP (*Dynamic Host Configuration Protocol*) ist in einem WLAN nicht zu empfehlen. Denn sollte es jemandem gelingen, in das eigene Netzwerk einzudringen, würde er automatisch eine IP-Adresse erhalten, mit der er sich dann im Netzwerk frei bewegen kann. Eine dedizierte Vergabe von IP-Adressen erhöht in kleineren Netzen den Administrationsaufwand nur unerheblich, stellt aber einen weiteren wirkungsvollen Schutz gegenüber Eindringlingen und ihren Aktivitäten dar.
- *Verschlüsselung*
  Zur Wahrung der Datenintegrität sollten Schlüssel zur Datenverschlüsselung angelegt werden. Die hierbei anfänglich verwendete Technik wird als WEP (*Wired Equivalent Privacy*) bezeichnet und heute als nicht mehr ausreichend sicher angesehen. Das aktuell empfohlene Verschlüsselungsverfahren WPA3 wird bei Wi-Fi-6-basierter Funk-Hardware meist direkt implementiert und sollte mit eigenen Schlüsseln versehen werden. Diese sollten allerdings aus Sicherheitsgründen regelmäßig geändert werden.

HINWEIS

Bei der Festlegung der WPA-Version im jeweiligen Gerät ist darauf zu achten, dass die gewählte Version mit allen teilnehmenden Komponenten kompatibel ist. Können in einigen Netzwerkknoten lediglich WPA2-Schlüssel eingerichtet werden, so sind die entsprechenden Geräte nicht in der Lage, mit WPA3-abgesicherten Komponenten zu kommunizieren. Als Konsequenz muss dann – je nach Sicherheitsanforderung – entschieden werden, ob die ältere, lediglich WPA2-fähige Hardware ausgetauscht werden muss oder ob ein »Downgrading« auf WPA2 als ausreichend angesehen wird.