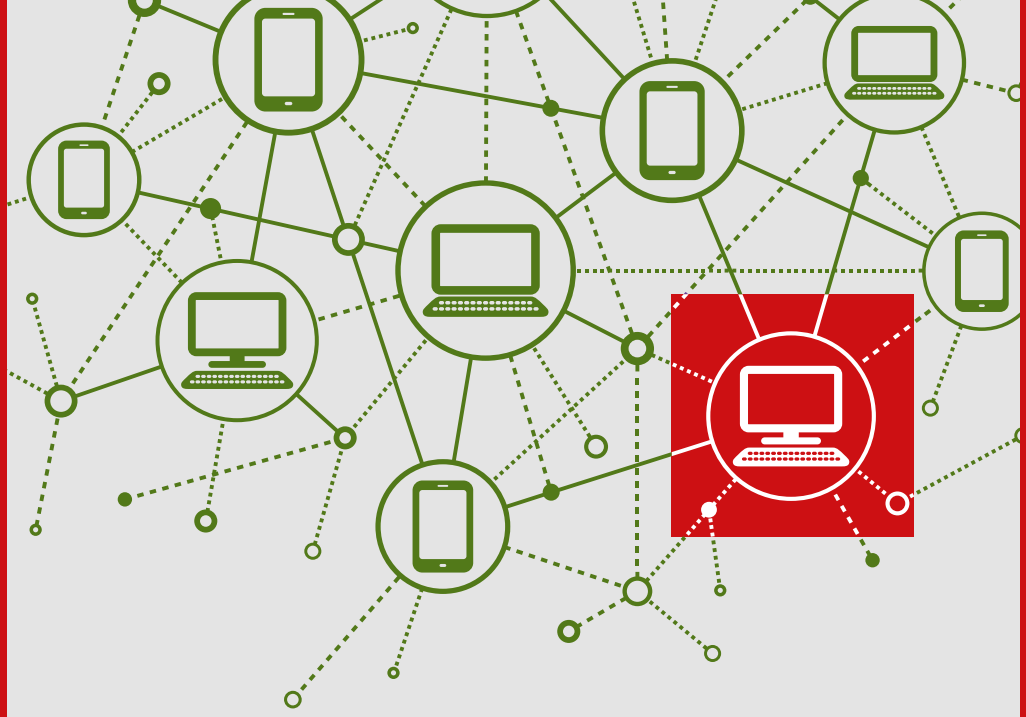

Wolfgang **RIGGERT**
Ralf **LÜBBEN**

RECHNER-NETZE

EIN EINFÜHRENDES LEHRBUCH

8., aktualisierte Auflage

Im Internet: **Lehrvideos, Quizzes, Mind-Maps und Lösungen**

HANSER

Disclaimer zur Barrierefreiheit

Der Carl Hanser Verlag unternimmt große Anstrengungen, um seine Produkte barrierefrei zu machen. Dazu gehört auch, dass Bilder oder Tabellen für blinde und sehbehinderte Menschen zugänglich gemacht werden. Dies geschieht durch zusätzliche beschreibende Texte (Alternativtexte), die in den Daten integriert sind. Die Alternativtexte können von assistiven Technologien (z. B. Screenreadern) vorgelesen werden. Bei der Erstellung dieser Texte kommt eine KI zum Einsatz. Die inhaltliche Verantwortung liegt weiterhin bei den Lektor:innen und Autor:innen.

Riggert / Lübben
Rechnernetze

Bleiben Sie auf dem Laufenden!

Hanser Newsletter informieren Sie regelmäßig über neue Bücher und Termine aus den verschiedenen Bereichen der Technik. Profitieren Sie auch von Gewinnspielen und exklusiven Leseproben. Gleich anmelden unter

www.hanser-fachbuch.de/newsletter

Lehrbücher zur Informatik

Begründet von

PROF. DR. MICHAEL LUTZ UND PROF. DR. CHRISTIAN MÄRTIN

weitergeführt von

PROF. DR. CHRISTIAN MÄRTIN

Hochschule Augsburg Fachbereich Informatik

Zu dieser Buchreihe

Die Werke dieser Reihe bieten einen gezielten Einstieg in grundlegende oder besonders gefragte Themenbereiche der Informatik und benachbarter Disziplinen. Alle Autoren verfügen über langjährige Erfahrung in Lehre und Forschung zu den jeweils behandelten Themengebieten und gewährleisten Praxisnähe und Aktualität.

Die Bände der Reihe können vorlesungsbegleitend oder zum Selbststudium eingesetzt werden. Sie lassen sich teilweise modular kombinieren. Wegen ihrer Kompaktheit sind sie gut geeignet, bestehende Lehrveranstaltungen zu ergänzen und zu aktualisieren.

Die meisten Werke stellen Ergänzungsmaterialien wie Lernprogramme, Software-Werkzeuge, Online-Kapitel, Beispielaufgaben mit Lösungen und weitere aktuelle Inhalte zur Verfügung.

Lieferbare Titel in dieser Reihe

- Rainer Oechsle, Parallele und verteilte Anwendungen in Java
- Wolfgang Riggert / Ralf Lübben, Rechnernetze
- Georg Stark, Robotik mit MATLAB

Wolfgang Riggert
Ralf Lübben

Rechnernetze

Ein einführendes Lehrbuch

8., aktualisierte Auflage

HANSER

Über die Autoren:
Prof. Dr. Wolfgang Riggert unterrichtete an der Hochschule Flensburg in den Bereichen Rechnernetze und Informationsmanagement.
Prof. Dr.-Ing. Ralf Lübben lehrt an der Hochschule Flensburg in den Bereichen Rechnerarchitekturen, Betriebssysteme und Rechnernetze.

Print-ISBN: 978-3-446-48429-0
E-Book-ISBN: 978-3-446-48470-2

Die allgemein verwendeten Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Alle in diesem Werk enthaltenen Informationen, Verfahren und Darstellungen wurden zum Zeitpunkt der Veröffentlichung nach bestem Wissen zusammengestellt. Dennoch sind Fehler nicht ganz auszuschließen. Aus diesem Grund sind die im vorliegenden Werk enthaltenen Informationen für Autor:innen, Herausgeber:innen und Verlag mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Autor:innen, Herausgeber:innen und Verlag übernehmen infolgedessen keine Verantwortung und werden keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Weise aus der Benutzung dieser Informationen – oder Teilen davon – entsteht. Ebenso wenig übernehmen Autor:innen, Herausgeber:innen und Verlag die Gewähr dafür, dass die beschriebenen Verfahren usw. frei von Schutzrechten Dritter sind. Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt also auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benützt werden dürften.

Die endgültige Entscheidung über die Eignung der Informationen für die vorgesehene Verwendung in einer bestimmten Anwendung liegt in der alleinigen Verantwortung des Nutzers.

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

Dieses Werk ist urheberrechtlich geschützt.
Alle Rechte, auch die der Übersetzung, des Nachdruckes und der Vervielfältigung des Werkes, oder Teilen daraus, vorbehalten. Kein Teil des Werkes darf ohne schriftliche Einwilligung des Verlages in irgendeiner Form (Fotokopie, Mikrofilm oder einem anderen Verfahren), auch nicht für Zwecke der Unterrichtgestaltung – mit Ausnahme der in den §§ 53, 54 UrhG genannten Sonderfälle –, reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.
Wir behalten uns auch eine Nutzung des Werks für Zwecke des Text und Data Mining nach § 44b UrhG ausdrücklich vor.

© 2025 Carl Hanser Verlag GmbH & Co. KG, München
Vilshofener Straße 10 | 81679 München | info@hanser.de
www.hanser-fachbuch.de
Lektorat: Frank Katzenmayer
Herstellung: le-tex publishing services GmbH, Leipzig
Coverkonzept: Marc Müller-Bremer, www.rebranding.de, München
Covergestaltung: Max Kostopoulos
Titelmotiv: © istockphoto.com/Ani_Ka
Satz: Eberl & Koesel Studio, Kempten
Druck: CPI Books GmbH, Leck
Printed in Germany

Inhalt

Vorwort zur achten Auflage ..... **XI**

1 Netzwerkgrundlagen und -architektur **1**

1.1 Basiselemente eines Netzwerkes 3
1.2 Netzwerkkategorien 7
1.3 Netzwerkarchitekturen 10
1.4 Datenübertragung 15
1.5 Protokolle und Standards 21
1.6 ISO-/OSI-Referenzmodell 23
1.7 Zusammenfassung 32
1.8 Wissensüberprüfung 33

2 Übertragungsmethoden und -medien **35**

2.1 Übertragungsverfahren 36
2.2 Strukturierte Verkabelung 41
2.3 Glasfaserverkabelung 45
2.3.1 Historie 46
2.3.2 Kabelaufbau 46
2.3.3 Arbeitsweise 47
2.3.4 Eingesetzte Technik 48
2.3.5 Qualitätsparameter 50
2.3.6 Glasfaserprofile 53
2.3.7 Glasfaserkabelarten 55

2.3.8 Steckverbindungen ... 56
2.3.9 Bewertung ... 58
2.4 Twisted-Pair-Verkabelung ... 59
2.4.1 Qualitätsparameter ... 61
2.4.2 EIA/TIA-568-Standard ... 63
2.4.3 ISO/IEC-Standard 11801 und EN 50173 ... 64
2.4.4 Bewertung ... 68
2.5 Zusammenfassung ... 70
2.6 Wissensüberprüfung ... 70

3 Ethernet-Technologie ... 71
3.1 Historie ... 72
3.2 Paketaufbau ... 76
3.3 Zugriffsverfahren: CSMA/CD ... 80
3.4 Signalverlauf ... 86
3.5 Standards ... 88
3.6 Fehlerquellen ... 94
3.7 Verfahrensbewertung ... 95
3.8 Zusammenfassung ... 97
3.9 Wissensüberprüfung ... 97

4 Ethernet-Standards ... 99
4.1 Die nahe Vergangenheit: Fast-Ethernet ... 99
4.1.1 Vorteile ... 100
4.1.2 Bestandteile ... 101
4.1.3 Varianten ... 102
4.1.4 Auto-Negotiation-Technologie ... 104
4.2 Die Gegenwart: Gigabit-Ethernet ... 106
4.2.1 Physikalische Grundlagen ... 107
4.2.2 Varianten ... 108
4.2.3 Besonderheiten ... 110
4.3 Gegenwart und Zukunft: 10-GbE und höher ... 111
4.3.1 Eigenschaften ... 112
4.3.2 Vorteile ... 115
4.4 Technologische Trends ... 117

4.5 Zusammenfassung ... 125
4.6 Wissensüberprüfung ... 125

5 IP-Protokollfamilie ... 127
5.1 IP – Internet Protocol ... 130
5.1.1 Fragmentierung ... 136
5.1.2 Routing-Optionen ... 136
5.1.3 Routing ... 138
5.2 ARP – Address Resolution Protocol ... 139
5.3 ICMP – Internet Control Message Protocol ... 142
5.4 Dynamic Host Configuration Protocol ... 146
5.5 Domain Name System ... 150
5.6 Zusammenfassung ... 155
5.7 Wissensüberprüfung ... 156

6 IP-Adressierung ... 157
6.1 IP-Adressstruktur ... 158
6.1.1 Class-A-Adressen ... 160
6.1.2 Class-B-Adressen ... 160
6.1.3 Class-C-Adressen ... 161
6.1.4 IP-Adressinterpretation ... 161
6.1.5 IP-Adressen mit besonderer Bedeutung ... 162
6.2 Subnetzbildung ... 164
6.3 VLSM – Variabel lange Subnetzmasken ... 169
6.3.1 Grenzen der Subnetzbildung ... 169
6.3.2 VLSM-Voraussetzungen ... 170
6.4 Private Adressvergabe oder Network Address Translation ... 173
6.5 CIDR – Classless Inter-Domain Routing ... 175
6.6 Verwaltungsfunktionen auf IP-Basis ... 177
6.7 Zusammenfassung ... 178
6.8 Übungen ... 179
6.9 Wissensüberprüfung ... 180

7 IPv6 ... 183
7.1 Historie ... 184
7.2 Entwurfsziele ... 185

7.3 Technische Betrachtung ... 187
7.4 Die wichtigsten Merkmale ... 187
7.4.1 Header ... 187
7.4.2 Headererweiterungen ... 190
7.4.3 Adressformat ... 194
7.4.4 IPv6-Adressmanagement ... 200
7.4.5 Begleitprotokolle ... 202
7.5 Migrationswege ... 205
7.5.1 Tunneling ... 205
7.5.2 Dual-IP-Stack ... 206
7.6 Mobile IPv6 ... 207
7.6.1 Kommunikationsablauf ... 208
7.6.2 Technischer Hintergrund ... 209
7.7 Überlegungen zur Sicherheit ... 211
7.8 Zusammenfassung ... 215
7.9 Übungen ... 217
7.10 Wissensüberprüfung ... 218

8 TCP/UDP-Protokoll ... 219

8.1 TCP im Detail ... 220
8.1.1 Besonderheiten ... 221
8.1.2 Merkmale ... 221
8.1.3 Verbindungsmanagement ... 225
8.1.4 Fehlervermeidungsmechanismen ... 227
8.2 UDP – User Datagram Protocol ... 231
8.3 Überlegungen zur Sicherheit ... 233
8.4 Transport Layer Security und QUIC ... 235
8.5 QoS – Quality of Service ... 239
8.5.1 Klassifikation ... 242
8.5.2 Congestion Avoidence ... 243
8.5.3 Congestion Management ... 245
8.6 Netzneutralität ... 248
8.7 Zusammenfassung ... 250
8.8 Wissensüberprüfung ... 251

9 Layer 2 – Geräte, Protokolle und Konzepte ... 253
9.1 Switches ... 254
9.1.1 Eigenschaften ... 254
9.1.2 Arbeitsweise ... 256
9.1.3 Switching-Verfahren ... 258
9.1.4 Erweiterungsmöglichkeiten ... 261
9.1.5 Kapazitätssteigerung ... 261
9.1.6 Switch-Architekturen ... 263
9.1.7 Switch-Typen ... 265
9.2 Spanning-Tree ... 266
9.3 Virtuelle LANs ... 272
9.3.1 VLAN-Typen ... 273
9.3.2 Trunk ... 274
9.3.3 VLAN-Management ... 275
9.3.4 Link Aggregation, Spanning Tree und VLAN ... 276
9.4 Überlegungen zur Sicherheit ... 278
9.4.1 Angriffsziel: STP-Bridge ... 278
9.4.2 Angriffsziel: STP-Parameter ... 279
9.4.3 Angriffsziel: MAC-Tabelle ... 280
9.5 Zusammenfassung ... 283
9.6 Übungen ... 283
9.7 Wissensüberprüfung ... 284

10 Layer 3 – Geräte, Protokolle und Konzepte ... 285
10.1 Router ... 286
10.1.1 Bedeutung ... 286
10.1.2 Routing-Ablauf ... 288
10.1.3 Routing-Methoden ... 291
10.1.4 Unterschiede zwischen Routern und Switches ... 294
10.2 Routing ... 295
10.2.1 Bedeutung ... 296
10.2.2 Routing-Protokolle – allgemeine Klassifizierung ... 296
10.3 Routing-Protokolle ... 301
10.3.1 RIP – Routing Information Protocol ... 302
10.3.2 OSPF – Open Shortest Path First ... 305

10.3.3 BGP – Border Gateway Protocol ... 307
10.4 Routingprobleme ... 319
10.5 Einsatzaspekte von Switches und Routern ... 321
10.6 Überlegungen zur Sicherheit ... 322
10.7 Zusammenfassung ... 324
10.8 Wissensüberprüfung ... 324

11 Verwaltung von Netzwerken ... 325
11.1 Netzwerkmanagement ... 326
11.1.1 Netzwerkstatistiken ... 328
11.1.2 FCAPS-Modell ... 330
11.1.3 SNMP ... 331
11.1.4 syslog ... 338
11.2 Überlegungen zur Sicherheit ... 338
11.2.1 Allgemeine Bedrohungen ... 339
11.2.2 Fehleranalyse ... 341
11.2.3 Übungen ... 352
11.3 Zusammenfassung ... 353
11.4 Wissensüberprüfung ... 354

12 Wireless Local Area Networks ... 355
12.1 IEEE 802.11-Standards ... 357
12.2 Wireless-Architekturen ... 364
12.3 Modulationsverfahren und Kanäle ... 365
12.4 Zugriffsmethoden: CSMA/CA ... 368
12.5 Rahmentypen ... 372
12.6 Anmeldeverfahren ... 375
12.7 Sicherheit ... 377
12.8 Zusammenfassung ... 382
12.9 Wissensüberprüfung ... 383

13 Literatur ... 385

Index ... 391

Vorwort zur achten Auflage

Es gibt Technologien, die das Zeug dazu haben, das Wirtschaftsleben zu revolutionieren. Künstliche Intelligenz (KI) gehört in diese Kategorie. Ein stetiges Wachstum des Datenvolumens, die zunehmende globale Vernetzung und die Digitalisierung vieler Lebensbereiche erfordern Lösungen, die jenseits herkömmlicher Muster liegen. KI ist eine mögliche Antwort auf diese Herausforderungen. Die Umsetzung gelingt aber nur, wenn die zugrunde liegende Infrastruktur in Form von Netzwerken hierfür gerüstet ist. Netzwerke müssen daher flexibel auf diese Entwicklungen reagieren können. Voraussetzung dafür sind Maßnahmen, die die Leistungsfähigkeit der Netze und Anbieter stärken, gepaart mit verlässlichen Rahmenbedingungen, die die technologischen Trends unterstützen. Zu diesen Entwicklungen gehören [Cisco24]:

- **IoT (Internet of Things):** Anwendungen nutzen zunehmend die Daten von Sensoren, die als Microservices nahe an den erfassenden Devices entstehen. Damit ergeben sich nicht nur Anforderungen an die Sicherheit, sondern auch Fragen des Datentransports.
- **Künstliche Intelligenz:** Um das Potenzial zu erschließen, bedarf es Rechenleistung zur Entscheidungsunterstützung vor Ort. Dies bringt neue Gesichtspunkte der Verteilung automatisierter Systeme mit sich.
- **Mobilität:** Alle benötigten Dienste und Applikationen sollten auf jedem Gerät unabhängig vom Ort nutzbar sein. Hierzu sind Wireless-Verbindungen notwendig, die Skalierbarkeit, Sicherheit und ausreichende Kapazität zur Verfügung stellen.
- **Sicherheit:** Durch die zunehmende Digitalisierung der Wirtschaft erhöhen sich die Angriffsflächen für Hacker. Das Netzwerk muss daher Bedrohungen frühzeitig erkennen und darauf angemessen reagieren.
- **Datenverkehr:** Durch die weiter wachsende Nutzung von Videodaten und dem Auftauchen von Virtual und Augmented Reality steigt der Austausch von Daten, die besondere Anforderungen an die Qualität der Übertragung stellen.

Daraus lässt sich die elementare Rolle von Netzwerken für konkrete Anwendungen wie z. B. den Transport von Sensordaten ablesen. IoT, KI, große Bandbreite und Sicherheit reifen zu Schlüsselaspekten für die (Mobil)-Kommunikation der Zukunft.

Vor diesem Hintergrund und um den Blick auf das Netzwerkgeschehen zu weiten, enthält die neue Auflage Überlegungen zu:

- den Institutionen, die das Internet gestalten,
- Erweiterungen von Ethernet auf den industriellen Bereich,
- Erweiterungen und Alternativen zu TCP für eine sichere Datenübertragung,
- zum Routingprotokoll, das wesentlich die Wegewahl im Internet bestimmt.

Wir – das Autorenteam – hoffen, weiterhin den Lernenden/Lehrenden ein zukunftsorientiertes Lehrbuch anbieten zu können, dass ihren Ansprüchen Rechnung trägt.

Ralf Lübben und *Wolfgang Riggert*

Flensburg, im Mai 2025

Ergänzendes Material zum Buch steht auf *plus.hanser-fachbuch.de* zur Verfügung:

Lehrvideos, Quizzes zur Lernkontrolle, Mind-Maps der wichtigsten Konfigurationsbefehle für Cisco Router/Switches und die Lösungen zu den Aufgaben

1 Netzwerkgrundlagen und -architektur

Lernziele

Nach der Beendigung dieses Kapitels sollte der Leser in der Lage sein, folgende Fragen zu beantworten:

- Wie sind Netzwerke hinsichtlich ihrer Topologie aufgebaut?
- Aus welchen Basiskomponenten bestehen Netzwerke?
- Wie ist der Netzzugang geregelt?
- Was sind die Vorteile eines Schichtenmodells?
- Welche Funktionalität ist auf welcher Ebene des Schichtenmodells angesiedelt?

Kapiteleinführung

Netzwerke sind heutzutage allumfassend gegenwärtig. In Unternehmen bilden sie das Rückgrat der Informationsinfrastruktur. Angefangen von Netzwerken mit nur wenigen Rechnern, reicht das Spektrum moderner Lösungen bis zu weltweiten Verbünden, in denen viele Rechnerwelten eine integrative Einheit mit größtmöglicher Produktivität bilden. Triebfeder dieses verbindenden Elementes ist das Internet. Als leistungsfähige Werbeplattform und stets verfügbarer Vertriebskanal für viele Arten von Produkten und Dienstleistungen überwindet es traditionelle Marktgrenzen und ist damit Basis des Geschäftserfolges.

Geprägt sind Netzwerke durch drei allgemeine Anforderungen:

- Die Geschwindigkeit muss für die Partner des Datenaustausches zufriedenstellend ausfallen, ohne dass große Schwankungen in der Antwortzeit, selbst zu Spitzenlastzeiten, auftreten.
- Das Management der Netzkomponenten und der Endstationen muss einfach sein.
- Die Kosten des Betriebes müssen in vertretbarem Rahmen liegen.

Getrost der Prämisse *„Nichts ist so beständig wie der Wandel“* fällt es zunehmend schwerer, Leitlinien für eine zukunftssichere Netzplanung aufzustellen. In einer Welt, in der sich die Innovationszyklen ständig verkürzen, Produkte innerhalb eines Quartals veralten und das Internet alle Geschäftsbereiche umwälzt, bleiben auch die Netzwerktechnologie und ihre Prinzipien kaum ausgespart. Dennoch lassen sich einige Trends erkennen:

- Zukünftige Anwendungen verlangen die Übertragung großer Datenmengen. Dazu zählen Augmented- und Virtual-Reality-Anwendungen, Streaming-Dienste mit hohen Datenraten für Full-HD-Videos oder Cloud-Gaming-Dienste, bei denen Video- und Kontrolldaten in Echtzeit übertragen werden. Aber auch die Übermittlung von Röntgenbildern hoher Auflösung zwischen medizinischen Einrichtungen oder gar die Übertragung des Operationsgeschehens zwischen Krankenhäusern ist keineswegs nur Vision, sondern schon Realität.
- Die Zukunft zeigt eine Applikationslandschaft, die hohe Ansprüche an Antwortzeit und Güte der Übertragung stellen wird. Den durch die neuen Anwendungen dramatisch wachsenden Ansprüchen an die Bandbreite gesellt sich eine revolutionäre Veränderung des Verkehrsmusters hinzu. Die alte 80-20-Regel, nach der 80 % der Datenlast im Segment oder dem Unternehmen verbleiben und nur 20 % die Segmentgrenze überschreiten, wird durch Client-Server-Architekturen, das Internet und die VLAN-Bildung regelrecht auf den Kopf gestellt. Dieser Wandel, gekoppelt mit der Dezentralisierung der Datenquellen allgemein, macht die Datenflüsse eines Netzes unvorhersehbar und hochdynamisch.
- Die Veränderungen in den Anwendungen, in der Zahl der Netzbenutzer und im Verkehrsmuster machen verständlich, warum Organisationen gezwungen sind, permanent Teile ihres Netzes zu restrukturieren und auf Technologien mit höherer Bandbreite umzustellen.

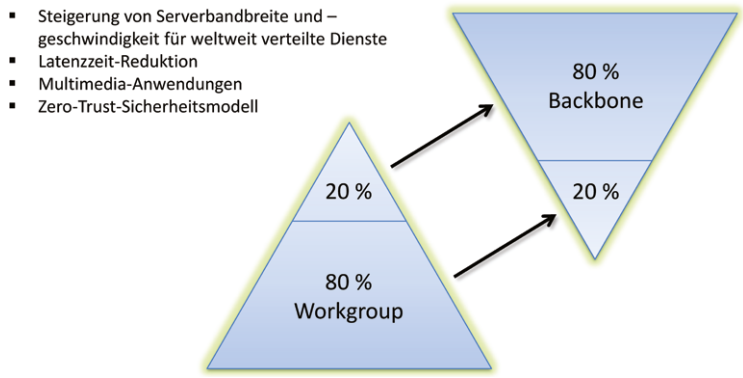

Bild 1.1 Veränderte 80-20-Regel

Dennoch existieren auch in diesem Meer von Unwägbarkeiten einige Fixpunkte. Zu den Grundprinzipien gehören Aspekte wie:

- Kommunikationsrichtung und Anzahl der Kommunikationspartner,
- Topologie/Architektur und Ausdehnung,
- Protokolle und Dienste,
- Signalcodierung und Übertragungsmedium,
- Fehlerbehandlung und Datenflusskontrolle,
- Wegewahl/Routing.

Diese Begriffe bilden praktisch die unverrückbaren Säulen des Netzgebäudes, um die sich alle neuen Entwicklungen ranken und an denen sie sich orientieren.

Häufig fallen in diesem Zusammenhang Begriffe wie Server, Netzwerkbetriebssysteme oder Adapter sowie der Verweis auf zahlreiche Vorteile wie Kostenreduzierung oder Produktivitätssteigerung.

1.1 Basiselemente eines Netzwerkes

Netzwerke bieten nicht nur die Befreiung des PCs aus seinem isolierten Wirkungsbereich, sondern verlangen dazu vier Elemente, die das Grundgerüst ihrer Infrastruktur bilden:

- die **Endgeräte der Nutzer**, seien es traditionelle Rechner, iPads oder Wearables, die Zugang zu einem Netz finden sollen,
- die **Infrastrukturkomponenten**, die den Anschluss und die Kopplung der Rechner leisten. Dazu zählen die in den Geräten verbauten Netzwerkkarten, aber auch eigenständige Komponenten wie Switches oder Router,
- die **physische Verbindung** der einzelnen Elemente durch Kabel oder Funkwellen,
- die **Protokolle** als Sprache und Syntax, damit sich die Netzteilnehmer an bestimmte Spielregeln halten und die Übertragungswünsche nicht im Chaos enden.

Damit sich der Netzwerkzug in Bewegung setzen kann, fehlen noch die Schienen, die Weichen und der Fahrplan:

- **Netzwerkkarte:** In jedem in das Netzwerk zu integrierenden Rechner muss eine Netzwerkkarte installiert sein. Erst über diese Weiche kann der Teilnehmer an den Leistungen des Verbundes partizipieren. Jede Anfrage oder Mitteilung an andere Teilnehmer wird über dieses Medium in das Netzwerk eingespeist. Die Netzwerkkarte ist zuständig für die Übertragung und den Empfang aller Nachrichten.

- **Verbindung:** Die Verbindung zwischen den Netzwerkkarten und damit zwischen den einzelnen Teilnehmern in Form der Schienen wird über Netzwerkkabel oder drahtlos hergestellt. Für kabelgebundene Verbindungen stehen zwei Typen zur Auswahl: Twisted-Pair-Kabel oder Lichtwellenleiter. Sie unterscheiden sich hinsichtlich der zulässigen Geschwindigkeit und technischer Parameter des Übertragungsmediums: elektrischer oder Lichtimpuls.
- **Netzwerkfähiges Betriebssystem**: Für die Kommunikation müssen die Teilnehmer eines Netzwerkes dieselbe Sprache sprechen, diese Regeln werden in Protokollen beschrieben und müssen letztendlich in Software umgesetzt werden. Heutzutage implementieren nahezu alle Betriebssysteme diese Softwarekomponenten, um über Netzwerke miteinander zu kommunizieren. Weiterhin benötigen die Betriebssysteme passende Treiber, um Hardware zur Kommunikation wie Netzwerkkarten zu unterstützen. Der Weg dahin führte aber über spezielle Varianten wie Novell Netware, das zu Spitzenzeiten einen Marktanteil von 80 % besaß.

Diese Grundelemente offenbaren eine offenkundige Komplexität der Netzwerkidee. Daher bleibt die grundlegende Frage: Welche Vorteile bietet eine Vernetzung von Endgeräten? Das Augenmerk zur Beantwortung richtet sich dabei auf den funktionalen Verbundgedanken:

- **Datenverbund** gewährt den Zugriff auf räumlich verteilte Daten.
- **Lastverbund** gestattet eine optimale Prozessorauslastung. Damit kann eine Verteilung der Rechenlast zu Spitzenzeiten erreicht werden.
- **Funktionsverbund** erweitert die lokale Funktionalität durch den Zugriff auf gemeinschaftlich netzwerkweit genutzte Ressourcen.
- **Leistungsverbund** ermöglicht im Falle einer algorithmischen Zerlegung eines Problems die Verteilung der Rechenlast auf mehrere Knoten. Ein typisches Beispiel hierfür ist die Berechnung von Schlüsseln der symmetrischen Verschlüsselungsalgorithmen.
- **Verfügbarkeitsverbund** stellt eine Mindestleistung bei Ausfall einzelner Komponenten zur Verfügung. Fällt ein Netzknoten aus, kann der Anwender im Idealfall einen Nachbarrechner nutzen, ohne auf die netzweiten Ressourcen verzichten zu müssen. Lediglich die lokalen Anwendungen bleiben von der Bearbeitung ausgeschlossen. Damit wächst die Verfügbarkeit des Gesamtsystems.

Nicht alle Merkmale sind von gleicher Wichtigkeit. Im Unternehmenskontext spielen Aspekte des Last- oder Leistungsverbundes eher eine untergeordnete Rolle, während Daten- und Funktionsverbund die herausragenden Eigenschaften darstellen.

Voraussetzung für eine möglichst komfortable Nutzung von Netzwerken sind einige Aspekte, deren Bedeutung als selbstverständlich vorausgesetzt wird, die sich aber erst im Laufe der technischen Entwicklung herauskristallisiert haben. Ohne sie wäre eine Verbreitung von Netzwerken, wie wir sie heute kennen, kaum möglich gewesen:

- **Räumliche Trennung:** Geräte in einem Netz haben zu ihrem Kommunikationspartner eine räumliche Distanz. Daraus ergibt sich eine Verzögerung durch eine Signallaufzeit. Dem Nutzer begegnet dieser Aspekt durch die Antwortzeit. Aber auch die verfügbare Bandbreite, die Verzögerung von Sendungen oder die Fehlerrate des Mediums bedingt durch die unterschiedliche Lokalität können den Nutzer beeinträchtigen.
- **Unabhängigkeit der Knoten:** Die einzelnen Geräte eines Netzes handeln autonom, d. h. sie unterliegen keinen Abstimmungsmechanismen hinsichtlich anderer Teilnehmer. Die Entscheidung zum Senden einer Nachricht treffen die Rechnerknoten ohne Rücksicht auf den Zustand des Netzes und seiner Elemente.
- **Heterogenität der Knoten:** Die Netzknoten können sich hinsichtlich Hardware, Betriebssystem und Anwendung beträchtlich unterscheiden. Zur Teilnahme am Netzbetrieb bestehen keine Voraussetzungen hinsichtlich dieser Merkmale. Zum Datenaustausch zwischen den Knoten ist damit keine Kenntnis der genauen Konfiguration eines Gegenübers erforderlich. Die Knoten müssen lediglich die TCP-/IP-Protokolle unterstützen.

Neben den bereits hervorgehobenen Vorteilen eines Netzwerkes zeigt sich, dass im Zeitalter des Internets Kommunikationsinseln einen Fremdkörper darstellen, sodass es nur folgerichtig sein kann, die Vorzüge einer unternehmensweiten Vernetzung auszuschöpfen:

- **Gemeinsame Datenbestände sorgen für aktuelle Information:** Die wohl wichtigste Aufgabe eines Netzwerkes ist der Datenverbundgedanke mit einer zentralen Speicherung von Datenbeständen. Änderungen und Aktualisierungen der Daten finden ihren sofortigen Niederschlag im System, ohne dass es der individuellen Abstimmung und des bidirektionalen Austausches der Anwender bedarf.
- **Transparenz:** Zu den Basiseigenschaften verteilter Systeme gehört es, ihre Komplexität vor dem Benutzer geheim zu halten. Dies geschieht hinsichtlich des Ortes, des Zugriffs, der Namen, der Replikation, des Ausfalls. Der Zugriff auf Netzressourcen bildet damit keinen gesonderten schwierigen Vorgang, sondern im Gegenteil, das Netzwerk erweitert die Möglichkeiten des Anwenders, ohne dass dieser seine bisherigen Arbeitsgewohnheiten ändern muss.
- **Teilung teurer Peripherie:** Aufgrund der Ablage von Programmen und Daten auf einem zentralen Knoten muss auch nur dieser mit entsprechenden Speicherkapazitäten ausgestattet sein. Die einzelnen Rechnerknoten selbst benötigen nur noch geringe Speichergrößen. Darüber hinaus können hochwertige Geräte in das Netz-

werk integriert werden, die, einmal angeschafft, allen Anwendern gleichermaßen zur Verfügung stehen.

- **Zentrale Programmverteilung:** Da jeder Rechner über das Netzwerk erreicht werden kann, gibt es die Alternative, ein Anwendungsprogramm nur einmal auf einem zentralen Server zu installieren und von allen Anwendern gleichermaßen nutzen zu lassen oder eine gezielte Verteilung dieses Programms über das Netzwerk auf bestimmte Rechnerknoten vorzunehmen. Auf diese Weise ist es nicht mehr notwendig, jeden einzelnen Arbeitsplatz aufzusuchen, um dort Installationen, Wartung oder Aktualisierungen auszuführen.
- **Kontrollmöglichkeiten:** Da Netzwerkressourcen nicht im Überfluss existieren, besteht der Bedarf nach einer gerechten Zuteilung. Spätestens hier sind Einsichten in das Nutzungsmuster nötig, um die Erfassung, Abrechnung und Aufbereitung der Leistungen zu ermöglichen. Die Bedeutung zeigt sich insbesondere im Cloud-Computing.

Neben diesen Gesichtspunkten bleibt die Antwortzeit eine wichtige Eigenschaft. Da ein Wesensmerkmal eines Netzwerkes die gemeinsame Nutzung von Ressourcen ist, besteht auf dem Weg zu zentralen Elementen eine Konkurrenz zwischen allen Teilnehmern, die zu einer Verschlechterung der Antwortzeit führen kann. Diese Situation schließt ein, dass jeder Nutzer nur über einen bestimmten Anteil der Übertragungskapazität verfügen kann. Je höher die Nutzerzahl, desto geringer die Kapazität. Als Folge eines sinkenden Bandbreitenanteils steigt dann die Antwortzeit. Der Verteilungsaspekt der Software selbst erlangt damit eine bedeutende Rolle. Geleitet von dem Verlangen nach hoher Performance und kurzen Antwortzeiten ist die Frage nach der optimalen Verteilung keineswegs trivial, sondern hängt im Gegenteil von einer Vielzahl von Rahmenbedingungen ab.

Da verteilte Systeme allen Benutzern den gemeinsamen Gebrauch der Ressourcen ermöglichen, treten Sicherheitsanforderungen auf, die fünf Merkmale unterstreichen:

- Autorisierung – ist der Benutzer berechtigt, auf Netzressourcen zuzugreifen?
- Vertraulichkeit – werden die Daten nur von den Berechtigten verarbeitet?
- Integrität – erreicht die Nachricht den Empfänger unverändert?
- Authentisierung – ist der Kommunikationspartner derjenige, der er vorgibt zu sein?
- Nichtabstreitbarkeit – ist das Absenden bzw. Empfangen der Nachricht eindeutig beweisbar?

Mit diesen Merkmalen lässt sich eine sichere Kommunikation gewährleisten, sodass zwei Kommunikationspartner sicher Nachrichten miteinander austauschen können. Aber was bedeutet „sicher“ genau? Zwei Kommunikationspartner möchten sicher sein, dass der Inhalt ihres Datenaustausches nur ihnen bekannt ist und nicht Dritten. Sie wollen zudem zusätzlich Gewissheit haben, dass nur sie miteinander kommuni-

zieren und kein Lauscher ihre Daten abfängt oder manipuliert und nur berechtigte Teilnehmer den Kommunikationskanal benutzen. Sowohl Sender als auch Empfänger sollten in der Lage sein, die Identität des jeweils anderen zu bestätigen. Zur Sicherstellung dieser Anforderungen kommen kryptografische Verfahren und Authentifizierungskonzepte zum Einsatz.

1.2 Netzwerkkategorien

Netzwerke sind kein uniformes Konstrukt, sondern es wird versucht, sie zu systematisieren und zu kategorisieren. Eine gängige Typisierung unterscheidet nach:

- Reichweite,
- administrativer Verantwortung,
- Topologie,
- Technologie.

Der geografische Bereich, den ein Netzwerk abdeckt, wird üblicherweise dreigeteilt:

- Local Area Network (LAN),
- Metropolitan Area Network (MAN),
- Wide Area Network (WAN).

Local Area Networks (LANs) sind Netzwerke des Unternehmens/der Organisation. Ein LAN ist dabei auf das Firmen- oder Campusgelände begrenzt. Oft wird der Radius von 500 m als Ausdehnungsmaximum genannt, was auf die technische Begrenzung der ersten Netzwerktechnologien zurückgeht. Als besonderes Merkmal ist jedes Unternehmen Eigentümer dieser Infrastruktur, d. h. die Institution ist im Besitz der Endgeräte, der Infrastrukturkomponenten wie Switches und der Verbindungsmechanismen wie Kabel. Darüber hinaus fallen keine weiteren Kosten an.

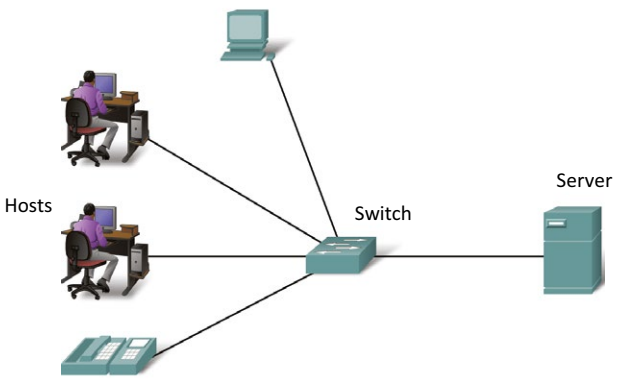

Bild 1.2
LAN

Die eingesetzte Technologie und der verwendete Kabeltyp bestimmen wesentlich die exakten Entfernungsrestriktionen und die Anzahl der Knoten, die ein LAN bilden.

Metropolitan Area Networks (MANs) bilden häufig Verbindungsnetze zwischen Institutionen. Ihr Hauptaugenmerk liegt auf der Bildung von Kommunikationsverbünden jenseits der geografischen Organisations-/Unternehmensgrenzen unter eigener Administration und Kontrolle. Beispiel hierfür könnten Forschungsverbünde zwischen Standorten sein, z. B. den Universitäten des Ruhrgebietes oder den räumlich verteilten Instituten der Münchener Universitäten.

Wide Area Networks (WANs) verbinden die unterschiedlichen LANs der Organisationen/Unternehmen über eine gesonderte Infrastruktur, die sich im Besitz spezialisierter Dienstleister, den sog. Internet Service Providern befindet. Für die Nutzung dieser Infrastruktur sind dementsprechend Entgelte zu entrichten. Ähnlich wie das Autobahnnetz, das Orte nicht direkt verbindet, besitzt ein WAN keine explizit angebundenen Teilnehmerstationen. Benutzer sind also immer Teil eines LANs oder MANs, die entweder regional begrenzt verbunden werden oder aber unter Zuhilfenahme eines WANs räumlich unbegrenzt gekoppelt werden.

WANs sind Netzwerke, die Routingprotokolle zur Wegewahl der zu übertragenden Informationen nutzen. LANs hingegen beruhen in der Regel auf dem Broadcastprinzip, wie es vom Rundfunk her bekannt ist.

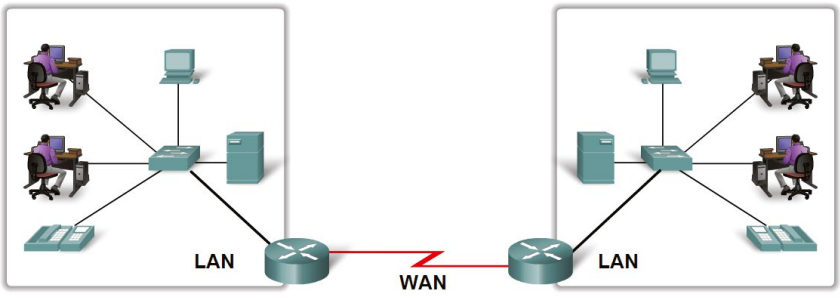

Bild 1.3 WAN

Ein flexibler, zukunftsfähiger Netzaufbau setzt ein entsprechendes Design voraus. Der Topologie kommt große Bedeutung zu, denn schließlich bildet sie das Rückgrat des Netzes, das nur mit großem Aufwand verändert werden kann. Eine Topologie lässt sich hinsichtlich dreier Merkmale beurteilen:

- **Skalierung:** Wie verhält sich der Aufbau bei einer Erweiterung oder Reduzierung von Stationen?

- **Fehlertoleranz:** Wie reagiert das Netz auf den Ausfall einer Station oder einer Verbindung zwischen Rechnern?
- **Verkabelungsaufwand:** Welcher Aufwand entsteht, um alle Stationen anzuschließen?

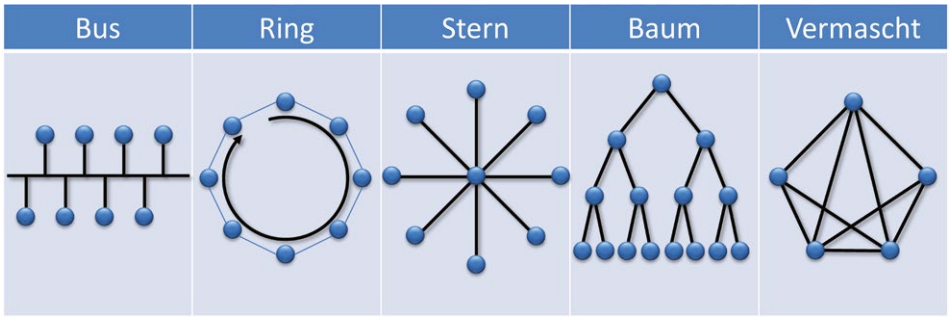

Bild 1.4 Netzwerktopologien

Unter Berücksichtigung dieser Fragestellungen lassen sich drei Grundformen bewerten:

- **Bus:** Dieser Aufbau verwendet ein zentrales Kabel. Die einzelnen Rechner müssen sich vergleichbar den Haltestellen einer Buslinie gesondert an dieses Medium anschließen. Dazu ist ein eigenes Anschlusskabel für jeden Rechner notwendig. Die Enden der Buslinie müssen durch einen Abschlusswiderstand ordnungsgemäß terminiert werden. Bei dieser Topologie wird nur sehr wenig Kabel benötigt. Rechner können sehr einfach am Netzverkehr teilnehmen, aber auch durch Lösen der Verbindung zum zentralen Kabel wieder zu Kommunikationsinseln werden. Sobald aber das Buskabel unterbrochen wird, kommt das gesamte Netzwerk zum Erliegen.
- **Ring:** Jede Station besitzt genau einen linken und einen rechten Nachbarn. Der Ring ist gerichtet, d. h. die Nachrichten werden in definierter Weise weitergeleitet. Diese Tatsache birgt allerdings das Problem, dass bei Ausfall einer Station, der Ring unterbrochen ist, d. h. dass Signale diese Stelle nicht passieren können und demzufolge das Gesamtnetz seine Funktionsfähigkeit verliert. In der Praxis werden durch einen zweiten, entgegen gerichteten Ring entsprechende Vorkehrungen getroffen, um immer einen geschlossenen Ring zu gewährleisten. Als Vorteil zeichnen diese Struktur die einfache Erweiterbarkeit und der geringe Kabelbedarf aus.
- **Stern:** Bei diesem Aufbau besitzt jeder Rechner eine eigene Verbindung zu einer zentralen Verteilereinheit. Zwar wird deutlich mehr Kabel als bei der busförmigen Variante benötigt, jedoch sind bei einem Ausfall eines Netzkabels keine anderen Rechner betroffen. Herausragendes Merkmal eines Sterns ist seine leichte

Ausbaufähigkeit und seine Ausfallsicherheit. Einziger Schwachpunkt ist die zentrale Verteilerstelle, deren Ausfall nicht kompensiert werden kann.

Tabelle 1.1 Topologievergleich

	Stern	Bus	Ring
Verkabelungsaufwand	-	+ +	+
Skalierbarkeit	+ +	+	+ +
Fehlertoleranz	+	+	-

Derzeit hat sich der Stern als „State of the Art“ durchgesetzt. Praktisch jede Technologie lässt sich auf diese Struktur abbilden. Im Kernbereich von Netzen werden häufig zentrale Elemente redundant ausgelegt, sodass Ausfälle einzelner Verteiler Stationen nicht zum Gesamtausfall des Netzwerkes führen.

Die physikalische Topologie beschreibt den Aufbau des Netzwerkes, d. h. die Form, in der die Kabel verlegt sind. Die logische Topologie verweist auf den Pfad, den die Daten von der Quelle zum Ziel nehmen. Beide Formen können übereinstimmen (Ethernet), müssen es aber nicht (Token-Ring).

Ein weiterer Ansatz, ein Netzwerk zu beschreiben, legt seine verwendete Technologie zugrunde. Dabei werden Merkmale wie Topologie, Kabeltyp, Entfernungsrestriktionen, Kontrollinformationen oder Adressen beleuchtet.

1.3 Netzwerkarchitekturen

Die Gestaltung und der Aufbau betrieblicher Anwendungssysteme sind stark mit den IT-technischen Möglichkeiten verwoben. Dies zeigt sich in mehreren Paradigmenwechseln, die sich im Laufe der Evolution der Informationstechnologie und der sie begleitenden Option der Verteilung der Ressourcen vollzogen haben.

Stand mit dem Aufkommen von Rechnern zunächst die Verarbeitung von Massendaten und die Bewältigung von Routinetätigkeiten im Vordergrund, so hat sich dieses Bild hin zu einer flexiblen Nutzung der vielfältigsten Aufgaben durch mobile Geräte gewandelt. Drei Entwicklungslinien lassen sich ausmachen:

- monolithische Anwendungssysteme,
- Client-/Server-Architekturen,
- Cloud-Computing.

Monolithische Anwendungssysteme

Das charakteristische Merkmal dieser Form der Datenverarbeitung ist ein zentraler Rechner (Mainframe) mit angebundenen Terminals, die selbst über keine Rechenkapazität verfügen und folglich nur als reine Präsentationsgeräte genutzt werden können. Diese Architektur verband Funktionalität und Datenverwaltung als untrennbare Einheit. Die Verbindung mit anderen Rechensystemen war schwierig bis unmöglich, sodass diese Konstellation denkbar integrationsfeindlich war. Aber nicht nur die mangelnde Integrationsmöglichkeit stellte eine Hürde dar. Weitere Probleme erwuchsen aus:

- dem Problem, dass Unterstützung neuer Anforderungen stets neue Systeme verlangte,
- den schneller als den Leistungszuwachs steigenden Kosten,
- der teuren Pflege und Wartung,
- der mangelhaften Skalierbarkeit.

Client-/Server-Architekturen

Mit dem Aufkommen der PCs als kleine preiswerte Recheneinheiten Mitte der 1980er-Jahre und der gleichzeitigen Möglichkeit der Vernetzung dieses neuen Gerätetyps ergab sich das Potenzial der räumlichen begrenzten Verteilung von Rechenkapazität. Diesem Gedanken folgend sind heutige Anwendungssysteme verteilte Systeme, deren Funktionalität und Datenbestand als kooperierende Elemente betrachtet werden. Die Verteilung kennt zwei Ausprägungen, die sich danach richten, wer und durch wen die Ressourcen betreut werden:

- In einer **Peer-to-Peer-Umgebung** arbeitet jeder Rechner gleichberechtigt und jeder Nutzer administriert seine eigenen Betriebsmittel.
- In einer **Client-/Server-Architektur** werden Anwendungen und Datenbestände auf verschiedene Rechner im Netz verteilt. Aus Sicht des Anwenders erscheint das verteilte System aber als integrierter Dienst.

Dem letzten Gedanken folgend lassen sich Rechner grundsätzlich in zwei verschiedene Gruppen einteilen: Server und Clients. Server sind Rechner, die ihre Ressourcen und Dienste der Allgemeinheit zur Verfügung stellen, Clients sind Leistungsnehmer. Diese Art der Gruppierung ist das heute vorherrschende Verarbeitungsprinzip und wird als Client-/Server-Architektur bezeichnet. Es beschreibt die Vorstellung, dass die Kooperation einem Grundschema folgt:

- Die Initiative einer Zusammenarbeit geht vom Client aus, indem er Aufträge an einen Dienstanbieter, den Server, schickt, der seine Bereitschaft bekundet hat, für bestimmte Dienste verfügbar zu sein. Dabei gilt eine „*1:n-Beziehung*“ in beide Richtungen. Der Client kann im Laufe der Verarbeitung auf mehrere Server zugreifen und ein Server kann verschiedene Clients bedienen. Aus der Sicht des

Servers – also des Empfängers einer Anforderung – heißt diese Verteilung, er bietet nur bestimmte Dienste an, sodass ihn keine beliebigen überraschenden Nachrichten erreichen können. Auch nimmt er Anforderungen nur entgegen, wenn er „frei“ ist.

Dennoch kann die Auslastung nur prognostiziert werden, sodass Unsicherheit darüber besteht, welche Kapazität er vorhalten muss, um für alle Anwendungsfälle gewappnet zu sein. Dieser Informationsmangel kann zur Verschwendung von Ressourcen führen, wenn keine gleichmäßige Auslastung vorliegt und Lastspitzen mit der gleichen Performance wie ein unterdurchschnittlicher Verkehr bedient werden sollen.

Tabelle 1.2 Vor- und Nachteile von Peer-to-Peer- und Client-/Server-Netzwerken

Peer to Peer	Client/Server
Vorteile	
preiswerte Implementierung	zentralisierte Administration – alle Daten können zentral gesichert werden
kein Netzwerkadministrator notwendig	Skalierbarkeit und flexible Architektur
	verbesserte Sicherheit
Nachteile	
geringe Skalierbarkeit, wenn die Kommunikationsbeziehungen mit Anzahl der Knoten steigt	Server verlangen höherwertige Ausstattung
Sicherheitsprobleme	Administrator notwendig
jeder Nutzer benötigt bedingt Administrationskenntnisse	Single Point of Failure in Form des Servers

Welche Dienste letztlich ein Server erbringt, hängt von der Konfiguration des Anwendungssystems ab. Das Drei-Schichten-Modell der Anwendungsentwicklung, das Präsentations-, Anwendungs- und Datenhaltungsschicht unterscheidet, ist häufig der Orientierungsmaßstab. Der Verteilungsaspekt der Software selbst spielt eine bedeutende Rolle. Geleitet von dem Verlangen nach hoher Performance und kurzen Antwortzeiten ist die Frage nach der optimalen Aufteilung der Komponenten auf die drei Basiskategorien keineswegs trivial, sondern hängt im Gegenteil von einer Vielzahl von Rahmenbedingungen ab. Neben diesem Aspekt ermöglicht dieses Konzept erst den Entwurf der Anwendungen, wie sie heutzutage den Anwenderalltag dominieren. Nur die Verteilung und die Verbindung durch Netzwerke erlaubt die flexible Auswahl der Orte, an denen die Anwendung betrieben und die Daten gespeichert werden. Daraus resultiert ein weiteres Designkriterium: Wo werden die einzelnen Schichten

räumlich platziert und über welche Netzwerkverbindung werden sie erreicht. Daran lässt sich ablesen, welche Bedeutung Breitbandnetzen zukommt.

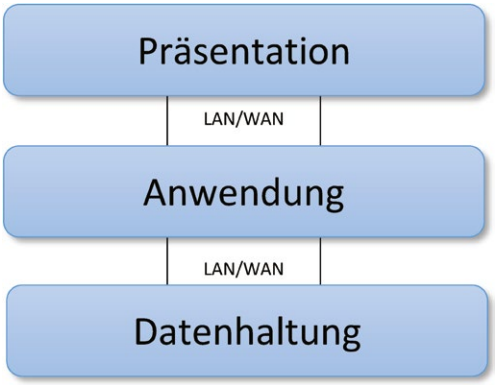

Bild 1.5
3-Schichten-Modell

Cloud-Computing

Während die Client-/Server-Architektur noch dadurch geprägt ist, dass die Ressourcen in der Verfügungsgewalt des einzelnen Unternehmens oder der einzelnen Organisation liegen und oft nur unzureichend genutzt werden, geht die nächste Idee einen Schritt weiter und verlagert die Anwendungs- oder Datenschicht in das Internet.

Cloud-Computing beschreibt die Bereitstellung von gemeinsam nutzbaren und flexibel skalierbaren IT-Leistungen über Netzwerke. Idealtypisches Merkmal ist die Verfügbarkeit im Self-Service-Modus in Echtzeit. Zusammengefasst beschreiben fünf charakteristische Eigenschaften das Cloud-Computing:

- Verfügbarkeit von Ressourcen nach Bedarf,
- Breitbandzugriff,
- Zusammenführung von Ressourcen,
- flexible Buchungsmöglichkeit der Ressourcen,
- Abrechnung nach Verbrauch.

Cloud-Computing bietet den Nutzern eine Umschichtung von Investitions- zu Betriebsaufwänden. Insbesondere für Unternehmen, die noch über keine eigene IT-Infrastruktur verfügen, bietet sich mit diesem Angebot eine Alternative. Kriterien für die Nutzung dieser IT-Dienstleitungen orientieren sich an der Art des Services, dessen Bedeutung für den Kunden, dem Standardisierungsgrad und Sicherheitserwägungen. Cloud-Computing bietet verschiedene Servicemodelle an:

- Infrastructure as a Service (IaaS),
- Platform as a Service (PaaS),
- Software as a Service (SaaS).

Die Merkmale der Serviceebenen lassen sich Tabelle 1.3 entnehmen.

Tabelle 1.3 Serviceebenen des Cloud-Computings

Typ	Beschreibung
IaaS	Zurverfügungstellung von Infrastrukturkomponenten wie Speicher oder virtualisierten Servern und deren Nutzung über das Netz
PaaS	Bereitstellung von Laufzeit- und Entwicklungsplattformen, um Anwendungen auch mit Datenbankanbindungen zu erstellen
SaaS	Angebot von Software als beständige Leistung, um Geschäftsprozesse auf der Plattform des Dienstleisters mit Internettechniken zu nutzen.

Cloud-Computing basiert auf zwei grundsätzlichen Ausprägungen:

- Public Cloud,
- Private Cloud.

Während die erste Form auf einer variablen, individuell abzurechnenden Grundlage für jedermann zur Verfügung steht, wendet sich die zweite Variante an eine vorab definierte Nutzergruppe, für die Betrieb und Management durch ein beteiligtes Unternehmen oder eine gemeinsame Organisation vorgenommen werden. Mit der Hybride Cloud gibt es eine dritte Form, die als „Mischangebot“ die Private mit der Public Cloud verbindet.

Das ausschlaggebende Motiv für eine Entscheidung zugunsten des Cloud-Computings ist das Potenzial der Kostensenkung. Begleitende Argumente sind in:

- der Konzentration auf das Kerngeschäft,
- der schnellen Realisierbarkeit,
- der großen Flexibilität und Skalierbarkeit

zu sehen. Die Geschwindigkeit der Verfügbarkeit der Dienste verschafft dem Nutzer Vorteile beim Markteintritt und der Umsetzung von Geschäftsideen. Auf der anderen Seite können Entwickler ihre Applikationen auf temporären Plattformen testen, ohne auf die Installation von Testumgebungen zu warten. Neben diesen ökonomischen und technischen Vorteilen liegt der Wertmutstropfen im Bereich des Datenschutzes und der Datensicherheit. Das mangelnde Vertrauen hierin stellt das größte Hemmnis für eine zügige Marktentwicklung dar. Aber auch Aspekte der Interoperabilität zwischen Cloud-Anbietern, die Ausgewogenheit zwischen Individual- und Standardlösung und die organisatorischen Rahmenbedingungen in den Unternehmen und die Abhängigkeit von einer performanten und stabilen Netzverbindung erweisen sich als Probleme. Auf der anderen Seite sieht sich auch der Anbieter der Cloud-Infrastruktur Problemen gegenüber:

- die mangelnde Interoperabilität beeinträchtigt ein Wechsel potenzieller Nutzer,
- die Erfolgsabhängigkeit von der Komplexität des Soft- und Hardwareangebots. Insbesondere Anwendungssysteme wie ERP-Software erfordern Know-how durch die Komplexität der Optionen,
- die Einhaltung der vereinbarten Service-Level Agreements mit den Kunden.

Die Idee der Verlagerung von Anwendungen und Infrastrukturkomponenten überzeugt nicht nur durch die technische Machbarkeit, sondern auch durch ihre handfesten Vorteile. Diese Vorteile beurteilen kleinere und mittlere Unternehmen mit wenig IT-Know-how naturgemäß anders als große Unternehmen. Letztlich ergibt sich aber eine weitere Option zur Gestaltung der IT-Landschaft.

1.4 Datenübertragung

Die grundlegende Idee des Informationstransportes in Netzwerken besteht darin, Nachrichten in kleine Einheiten, sog. Pakete zu zerlegen, diese mit Adress- und Steuerdaten zu versehen und sie dann zuzustellen. Diese Entscheidung der Einteilung der zu übertragenden Daten in kleine autonome Einheiten bildet eine wesentliche Designvorgabe. Sie bedeutet darüber hinaus, dass sämtliche im Netzwerk transportierten Informationen separiert werden. Dies betrifft alle Arten von Daten von traditionellen Dateien, bis hin zu Bildern oder Audiostreams.

Vor der eigentlichen Übertragung der Daten erfolgt daher die logische Gruppierung in Pakete. Diese Pakete bilden eine Sequenz von Fragmenten der Ursprungsdaten. Sie sind leicht zu handhaben und für den Nutzer einfach zu interpretieren. Darüber hinaus besitzen Pakete mehrere Vorteile:

- Die Einteilung in Pakete hindert Rechner daran, die Netzwerkbandbreite zu monopolisieren.
- Gehen Pakete auf dem Übertragungsweg verloren, müssen nicht die gesamten Ursprungsdaten neu gesendet werden, sondern nur die verlorenen Pakete.
- Abhängig von der Auslastung des Netzwerkes können Pakete selbstständig unterschiedliche Wege zum Ziel nehmen, da sie autonome Einheiten bilden.

Das Konzept erinnert an die Versendung von Postpaketen. Auch dort wird eine Sendung zunächst in mehrere Einzelteile gestückelt, die den Größen- und Gewichtsanforderungen der Post entsprechen. Anschließend werden sie verpackt und einzeln mit den Empfängerdaten beschriftet. Als letzter Schritt erfolgt dann die Übergabe an das Verteilsystem der Post. Damit wird die Übertragung beliebig großer Informationsblöcke möglich, d. h. das Volumen unterliegt keinerlei Größenbeschränkungen. Allerdings können die einzelnen Pakete verschiedene Wege durch das Netz nehmen und

müssen – abhängig von der Technologie auf dem Weg zum Ziel – möglicherweise häufiger fragmentiert werden. Dennoch bleibt die Entscheidung, sämtliche Informationen in Paketform zu übertragen, eine der weitreichendsten Designentscheidungen im Netzwerkbereich.

Um Pakete von einem Ort zu einem anderen zu transportieren, sind prinzipiell zwei Arten von Übertragung möglich: **Leitungs- und Paketvermittlung**.

Die Übertragung in Form von Paketen wird als **Paketvermittlung** bezeichnet. Bei der Paketvermittlung durchqueren die Pakete als unabhängige und eigenständige Einheiten das Netz und können in den Vermittlungsknoten zwischengespeichert werden. Dies ist ein wesentlicher Vorteil, da nun die Übertragungsgeschwindigkeit zwischen einzelnen Teilstrecken keine Begrenzung mehr darstellt. Allerdings erscheint die Architektur als ein Netzwerk von Warteschlangen. Jeder zu passierende Netzknoten empfängt das Paket und leitet es an seine Ausgangsschnittstelle, die aber Ziel vieler Sendungen sein kann, sodass hier die Möglichkeit zu Überlastsituationen entsteht. Die Existenz der Warteschlangen erzeugt Verzögerungen in der Paketzustellung oder Paketverluste, wenn die Warteschlangen überlaufen. Die Paketverluste verursachen Paketwiederholungen und haben damit eine weitere Belastung des Übertragungsweges zur Folge. Für den Anwender ist dieser Ablauf nicht wahrnehmbar. Er benötigt und erhält keinerlei Informationen über den Übertragungsweg. Im Regelfall kann er diese Informationen auch nicht erlangen, da sich Übertragungswege dynamisch ändern. Die Paketvermittlung weist insbesondere dann einen großen Vorteil auf, wenn Informationen nur sporadisch übertragen werden (Aufruf einer Webseite, Abrufen/Versenden von E-Mails), da Zeiten, in denen das Übertragungsmedium ungenutzt ist, durch andere Teilnehmer genutzt werden können. Hierdurch kann eine Steigerung der Auslastung erreicht werden.

Die **Leitungsvermittlung** hängt von der Anbindung der einzelnen Teilnehmer ab. Dabei wird im Voraus über den Weg vom Ursprung zum Ziel entschieden. Für die Kommunikation wird die gesamte Leitung reserviert, d. h. niemand sonst kann diese teilen oder benutzen. Im Grunde wird die Leitung für die Zeit des Anrufs gemietet. Das ist der Grund für den vergleichsweise hohen Preis. Andererseits bedeutet es aber auch, dass eine qualitativ hochwertige und zuverlässige Verbindung entsteht, da eine dedizierte Bandbreite zur Verfügung steht. Leitungsvermittlung wird hauptsächlich für Sprachanrufe verwendet.

Die Leitungsvermittlung hat den Vorteil, dass Dienstgüten im Hinblick auf die Übertragungsgeschwindigkeit jederzeit eingehalten werden können und die Signallaufzeiten konstant sind, d. h. keine Verzögerungen zwischen Sender und Empfänger auftreten. Allerdings ist der Verbindungsaufbau zeitintensiv. Kommunikationsbeziehungen mit mehreren Partnern bedürfen eines wiederholten Verbindungsaufbaus und beide Teilnehmer müssen mit gleicher Kapazität senden und empfangen. Insbesondere wenn nur kurze Nachrichten übertragen werden, kann die Verbindungsverwaltung mehr Zeit als die eigentliche Übertragung beanspruchen.

Tabelle 1.4 Leitungs- vs. Paketvermittlung

Leitungsvermittlung	Paketvermittlung
Der Weg zwischen Quelle und Ziel wird für die Dauer der Verbindung aufgebaut.	Der Weg wird von den Routern bestimmt.
Alle Daten nehmen den gleichen Weg.	Jedes Paket nimmt seinen eigenen Weg.
Die Daten erreichen das Ziel sequenziell.	Pakete kommen in zufälliger Reihenfolge an.
Die Bandbreite wird für jeden Anruf zugeordnet.	Die verfügbare Bandbreite wird gemeinsam genutzt.
Daten werden nur an der Quelle verarbeitet.	Daten werden an verschiedenen Punkten des Netzwerks verarbeitet.
Alle Daten kommen zur gleichen Zeit an.	Pakete erreichen das Ziel zu unterschiedlichen Zeiten.

Je nach Distanz zwischen den kommunizierenden Rechnern unterscheiden sich die für die Paketzustellung verwendeten Verfahren:

Teilstrecken- oder Store-and-Forward-Netze übertragen die einzelnen Pakete als eigenständige Einheiten vollständig getrennt voneinander. Für das Auffinden des optimalen Weges durch den Netzdschungel nutzen sie spezielle Algorithmen. Die Folge dieser Art des Paketversands ist, dass die einzelnen Pakete ihren Empfänger in beliebiger Reihenfolge erreichen und dort erst wieder zu einer einheitlichen Sendung zusammengesetzt werden müssen. Allerdings können die einzelnen Pakete auf ihrem Weg zum Ziel auch Staus umgehen und trotz längerer Strecke ihr Ziel schneller erreichen als Pakete, die auf den kürzesten, aber verstopften Weg warten. Voraussetzung für eine erfolgreiche Paketvermittlung ist eine ausreichende Zwischenspeicherkapazität der Vermittlungsstellen, denn erst nach genauer Kenntnis des Ziels und der Informationen über die Strecke dorthin kann der Knoten eine verlässliche Entscheidung über den weiteren Weg in Richtung Ziel treffen.

Diffusions- oder Broadcastnetze sind auf kleine Entfernungen ausgerichtet. Die Nachricht erreicht alle angeschlossenen aktiven Knoten und der Empfänger wählt das an ihn gerichtete Paket aus. Dieses Verfahren verlangt keine aufwendige Wegewahl und keine Zwischenspeichermöglichkeit. Wohl aber müssen alle potenziellen Empfänger das Paket daraufhin prüfen, ob es an sie adressiert ist. Hierfür sind einerseits CPU-Ressourcen der einzelnen Netzknoten notwendig, andererseits verlangt die Prüfung eine gewisse Zeitdauer.

Nachdem geklärt ist, dass Informationen im Netzwerk in Form von Paketen übertragen werden, die entweder in Leitungs- oder Paketvermittlung den Empfänger erreichen, der selbst wieder über mehrere Vermittlungsstationen in einem Teilstrecken- oder Diffusionsverbund angesteuert wird, steht noch eine Kernfrage aus: Wie ist der Zugang der einzelnen Station zu einem Übertragungsmedium geregelt?

Zwei Verfahren sind denkbar:

- **aktive Ankopplung:** Der Netzteilnehmer nimmt das gesamte Paket vom Medium, prüft es daraufhin, ob es an ihn gerichtet ist, und generiert es für die Nachfolgestationen vollständig neu. Der Netzknoten fungiert als Paketregenerator, ein Konzept, das bei Einsatz von Glasfaserkabeln geboten ist, da optische Signale nicht aufspaltbar sind.
- **passive Ankopplung:** Jede Station auf dem Weg zum Ziel prüft das Paket. Damit wird das Ursprungssignal des Paketes im Zeitverlauf immer schwächer, sodass nach einer bestimmten Anzahl passierter Teilnehmer die Qualität nicht mehr ausreicht, um die Wertigkeit des Signals eindeutig zu erkennen.

Auf die Art der Ankopplung hat die einzelne Station jedoch keinen Einfluss. Sie wird von der zugrundeliegenden Technologie bestimmt. Ebenso verhält es sich mit der Steuerung der Konkurrenzsituation der einzelnen Teilnehmer, die sich um das Senderecht und die Übertragungskapazität bewerben. Auch für die Koordination des Zugriffs kommen zwei Strategien infrage:

- **wahlfreier Zugriff:** Alle Stationen arbeiten unabhängig voneinander und versuchen autonom einen Zugriff, sobald das Medium nicht belegt ist. Für diesen Vorschlag sind keine Kontroll- und Steuerinformationen notwendig.
- **verteilt gesteuerter Zugriff:** Alle Stationen erhalten einen Zugriff, sobald sie im Besitz einer Sendeberechtigung sind, die sie zuvor beantragen und erhalten müssen. Die Existenz dieser Sendeberechtigung macht ein Management für die Vergabe und ihren Fehler- und Verlustfall notwendig.

Der Kommunikationsfluss zwischen den Netzteilnehmern verläuft abhängig von der Technologie in drei Formen:

Kommunikationsrichtungen

simplex: In dieser Variante läuft der Nachrichtenfluss nur in eine Richtung, nämlich vom Sender zum Empfänger – Kabelfernsehen oder Rundfunk.

halbduplex: Hier kann zwar jeder Knoten senden und empfangen, aber nicht beides gleichzeitig – Ampelregelung zur Verkehrsführung auf einer normalen Straße mit halbseitiger Baustelle.

vollduplex: Jeder Knoten kann sowohl Nachrichten senden als auch gleichzeitig empfangen. Für den Netzbetrieb ist dieses Verfahren charakteristisch, da kein Netzteilnehmer ausschließen kann, dass er während einer Sendung Kontrollinformationen empfangen muss, um seine Übertragung einzustellen. Gleiches gilt für einen Server, der Anforderungen von vielen Clients erhält und diese simultan verarbeitet.

Das ursprüngliche Ethernet wird im Halbduplex-Modus betrieben, das heutzutage verbreitete, modernere Switched-Ethernet nutzt einen Vollduplex-Modus. Beim WLAN spielt allerdings der Halbduplex-Gedanke weiterhin eine entscheidende Rolle.

Die unterschiedlichen Formen können als Gradmesser der Übertragungskapazität gelten. Dabei lassen Vollduplex-Verbindungen, da sie in beide Richtungen simultan übertragen, als die ausgereifteste Variante die doppelte Datenübertragungsrate zu. Aber auch die Zahl der involvierten Netzteilnehmer kann Rückschlüsse auf die Netzleistung geben.

Anzahl der Kommunikationsteilnehmer

Unicast: Hierbei handelt es sich um die klassische Form des Datenaustausches in Form einer Punkt-zu-Punkt-Verbindung, bei der einem Sender genau ein Empfänger zugeordnet ist.

Anycast: Stellt eine Unicast-Verbindung zu der nächstgelegenen Station einer Gruppe her.

Multicast: Eine ausgewählte Gruppe ist das Ziel der Nachricht. Daraus ergeben sich mehrere Einsatzfelder:

- **Content-Push-Distribution:** Informationsdienste wie Wetter, Nachrichten, Börsenkurse, Software-Updates
- **Verteilung zentraler Datenbestände:** Informationskioske, Produktdatenblätter, Service- und Schulungsunterlagen, Videokonferenzen
- **Broadcast:** Eine Sendung wird allen erreichbaren Stationen des Netzes zugestellt. Dieser Mechanismus findet z. B. bei der Ermittlung der logischen Adresse eines Rechners oder im Netzwerkmanagement Anwendung.

Das Anycast-Konzept wird insbesondere durch die neue Version 6 des Internet-Protokoll IP unterstützt.

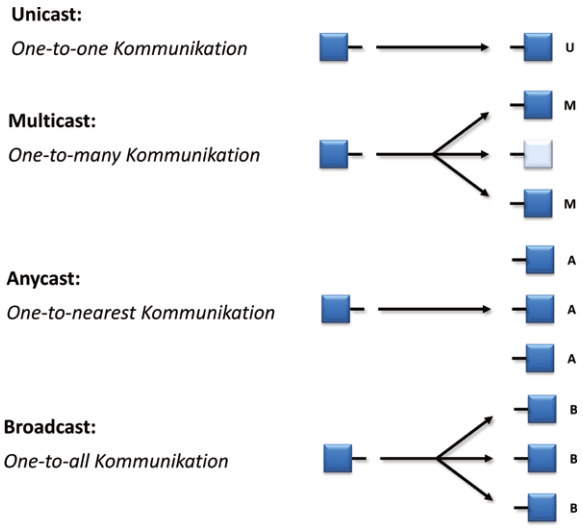

Bild 1.6
Anzahl der Kommunikationsteilnehmer

Als letzter Aspekt der Leistungsfähigkeit eines Netzwerkes kann die Kapazität des zugrundeliegenden Mediums angesehen werden. Drei Messgrößen dienen hier zur Beurteilung:

- **Bandbreite** ist ein theoretisches Maß dafür, wie viele Informationen innerhalb einer bestimmten Zeit von einem Ort zu einem anderen fließen können. Die Maßeinheit dafür ist bits per second (bps). Der Nutzer bucht diesen Nominalwert bei seinem Internet Service Provider.
- **Durchsatz** gibt die aktuell transportierte Datenmenge an und spiegelt damit die augenblickliche Verkehrssituation wider. Dieser Wert weicht im Normalfall von der Bandbreite ab in dem Sinne, dass er geringer ausfällt.
- **Goodput** ist ein Maß für die übertragenen Nutzdaten, d. h. Nettodaten ohne Protokolloverhead.

Die tatsächlich zur Verfügung stehende Bandbreite kann mit Werkzeugen wie Speedtest gemessen werden. Die an einem Standort überhaupt mögliche Anschlussbandbreite zeigt der Breitbandatlas bis auf Straßenebene eines Ortes unter: *https://gigabitgrundbuch.bund.de/GIGA/DE/Breitbandatlas/Vollbild/start.html*.

Auf dem Weg zu einem Netzwerk ist es aber nicht nur bedeutsam, die genauen Anforderungen festzulegen, sondern auch deren Umsetzung. Zu den wichtigen Eigenschaften, die heutige Netzwerke umfassen sollten, gehören:

- **Skalierbarkeit:** Einem Netz müssen problemlos weitere Knoten hinzuzufügen sein. Mit dieser Eigenschaft wird dem weiteren Ausbau und der flexiblen Reaktion auf geänderte Rahmenbedingungen sowie der stetigen Zunahme des Vernetzungsgrades Rechnung getragen.
- **Robustheit:** Die Netzinfrastruktur muss durch Stabilität und Fehlertoleranz geprägt sein. Da Netzwerke in Client-/Server-Umgebungen zu einer kritischen Komponente für das gesamte Unternehmen geworden sind und der Unternehmenserfolg entscheidend auf einem funktionstüchtigen Netz beruht, bedeuten minimale Ausfallzeiten einen Wettbewerbsverlust.
- **Migration:** Das Netzdesign muss den leichten Übergang auf neue Techniken und Netztopologien zulassen. Der stete Wandel in der Informationsverarbeitung bringt die Notwendigkeit mit sich, einen Übergang auf technologische Änderungen zu ermöglichen, ohne die gesamte Netzinfrastruktur auszutauschen. In diesem Sinne wird Investitionssicherheit für ein Netzdesign großgeschrieben.
- **Autokonfiguration:** Neue Netzkomponenten müssen ohne großen Aufwand integrierbar sein. Nicht nur höhere Bandbreite für Multimedia-Anwendungen steht auf der Wunschliste der Netzbetreiber, sondern auch zunehmend die Möglichkeit, alle Daten von Sprache bis Video über eine Netzinfrastruktur abzuwickeln. Der-

artig komplexe Anforderungen können nur durch spezielle Kopplungsgeräte erbracht werden. Der einfache Austausch alter gegen neue Geräte, ohne Störung des Netzbetriebs, ist hier die Idealvorstellung.

1.5 Protokolle und Standards

Wenn Teilnehmer in einem Netzwerk miteinander kommunizieren möchten, benötigen sie Regeln, nach denen sie Informationen in Form von Paketen austauschen können. Diese Regeln müssen von allen Kommunikationspartnern stets gleich interpretiert werden. Die Zusammenfassung dieser Regeln erfolgt in Protokollen, die damit ein einheitliches Schema für einen bestimmten Zweck, z. B. die Wegewahl im Internet, festlegen. Neben ihrer eigentlichen Bestimmung müssen Protokolle aber weitere Rahmenbedingungen definieren. Dazu kann die Beantwortung unterschiedlichster Fragen zählen:

- Welche Größe hat das Paket?
- Welche Nachrichten unterstützt das Protokoll?
- Welche Angaben enthält eine bestimmte Nachricht?
- Was passiert, wenn ein Paket verloren geht?
- Wie wird auf einen Fehler/eine Beschädigung reagiert?

Anhand dieser Fragen lässt sich ablesen, dass Protokolle komplexe Gebilde sein können, deren Implementierung eine herausfordernde Aufgabe darstellen kann. Hinzu kommt ein weiterer Aspekt: Damit eine nahtlose weltweite Kommunikation möglich ist, muss der Gültigkeitsbereich von Protokollen grenzenlos sein. Alle Kommunikationspartner unabhängig vom Standort und der Nationalität müssen die Regeln bedingungslos akzeptieren. Dies setzt voraus, dass international anerkannte Gremien die Regeln entwerfen und weiterentwickeln.

Das Internet ist ein global verteiltes Netzwerk, das aus vielen freiwillig miteinander verbundenen autonomen Systemen besteht. Die Koordination und Verwaltung einer derartigen Struktur verlangt einheitliche Richtlinien und technische Standards, die sicherstellen, dass es jederzeit funktioniert und weiterentwickelt wird. Eine Schwierigkeit liegt allerdings darin, dass das Internet Informationen und Daten über alle nationalen Staaten hinwegbewegt und viele Organisationen und Einrichtungen einen Teil der physischen Infrastruktur besitzen. Aus diesem Aufbau folgt, dass kein zentrales Leitungsgremium existiert, das für die allgemeine Verwaltung zuständig ist, sondern ein Flickenteppich von Organisationen und Akteuren, die die globale Interoperabilität des Internets sicherstellen. Sechs Organisationen haben sich dieser Aufgabe verschrieben (siehe Tabelle 1.5).

Tabelle 1.5 Internetorganisationen

Name	Abkürzung	Link
Internet Engineering Task Force	IETF	*www.ietf.org*
Internet Research Task Force	IRTF	*www.irtf.org*
Internet Architecture Board	IAB	*www.iab.org*
Internet Society	ISOC	*www.internetsociety.org*
Internet Corporation for Assigned Names and Numbers	ICANN	*www.icann.org*
Institute of Electrical and Electronics Engineers	IEEE	*www.ieee.org*

Die einzelnen Organisationen erfüllen folgende Aufgaben:

- Die **Internet Engineering Task Force** fördert eine breite Palette von Internetstandards auf der Grundlage von technischen Dokumenten, den sog. Request für Comments (RFC). Obwohl die RFCs nicht verpflichtend sind, bieten sie ein Rahmenwerk für alle Fragen bezüglich der Netzwerktechnik. Ein Verzeichnis aller RFCs, die von einem RFC-Editor verwaltet werden, ist unter der Adresse *https://www.rfc-editor.org* verfügbar. Ein Schlüssel für die schnelle Entwicklung des Internets ist im offenen Zugang zu den RFCs zu sehen. Jedermann kann RFCs vorschlagen, wobei die Vorgehensweise dazu in RFC 5000 festgelegt ist. Für die Entwicklung von Standards zu zentralen Themen wie Internet allgemein, Routing, Transport oder Real-Time Applications werden einzelne Working Groups gebildet. Ein Überblick hierzu ist unter folgendem Link zu finden: *https://www.ietf.org/html.charters/wg-dir.html.* Ein einmal abschließend veröffentlichter RFC ist öffentlich und unveränderlich. Er kann nicht korrigiert, sondern nur durch neuere RFCs abgelöst werden. Die Struktur und der Stil eines RFCs ist durch RFC 7322 vorgegeben. Die IETF selbst ist eine offene Organisation, die keine formale Mitgliedschaft kennt.
- Die **Internet Research Task Force** ist weniger bekannt als die IETF. Ihr Hauptanliegen liegt in der Entwicklung des Internets durch langfristig eingerichtete Forschungsgruppen, die Themen zu Protokollen, Anwendungen, Architektur und Technologie im Auge haben.
- Das **Internet Architecture Board** überwacht die Entwicklungen von IETF und IRTF.
- Die **Internet Society** setzt sich als Organisation für eine offene Entwicklung und Nutzung des Internets für alle Menschen weltweit ein. Alle RFC-Dokumente unterliegen dem Copyright der ISOC.
- Die **Internet Corporation for Assigned Names and Numbers** koordiniert die Adressvergabe, d. h. ist für die IP-Adresse, die Top-Level-Domains, Protokollnum-

mern und andere zentrale Parameter verantwortlich. Zur Wahrung der IP-Adressvergabe existiert mit der Internet Assigned Numbers Authority (IANA) eine eigene Abteilung des ICAAN, die in fünf regionale Registrierungsstellen (RIR) für bestimmte Weltregionen aufgeteilt ist:

- Afrika: *https://afrinic.net*,
- Asien-Pazifik: *https://apnic.net*,
- Kanada und USA: *https://arin.net*,
- Lateinamerika und Karibik: *https://lacnic.net*,
- Europa und Naher Osten: *https://ripe.net*.

- Das **Institute of Electrical and Electronics Engineers** widmet sich Standards zu Netzwerken allgemein und zur Telekommunikation. Dazu gehören die Gruppen IEEE 802.3 für Ethernet und IEEE 802.11 für WiFi. Im Gegensatz zu den Vereinbarungen der IETF handelt es sich bei den Übereinkünften der IEEE um verbindliche Standards.

Dass auch Netzwerknerds Humor haben, zeigen einige offizielle RFCs: so z. B. eine Lobeshymne auf das Arpanet (RFC 527), Wissenschaftsgeschichte in Versform (RFC 1121) oder The Twelve Days of Christmas aus der Sicht eines gestressten Netzwerkadministrators (RFC 1882).

Trotz der Möglichkeit, dass jedermann sich an der IETF beteiligen kann, sieht die Praxis anders aus. Die jährlich viermal stattfindenden Treffen erfordern ein hohes Budget. Die Folge des hohen finanziellen Einsatzes ist, dass nur Mitarbeiter von Unternehmen zu den Teilnehmern gehören. Dies verzerrt die Erstellung von IETF-Standards in Richtung der Interessen großer Unternehmen. Ähnliches gilt für die ICANN, die sich zum Teil aus der Erhebung von Lizenzgebühren der Initiatoren der generischen Top-Level-Domains (gTLD) generiert. Die ursprüngliche Idee eines offenen Ansatzes wird damit verfehlt und in der Realität dient das Lizenzmodell der Regulierung und Steuerung der Branchenakteure, die eine gTLD besitzen.

1.6 ISO-/OSI-Referenzmodell

Die Beschreibung der Möglichkeiten, wie eine Station in das Netzwerk integriert wird, zeigt, dass es allgemeiner Verhaltensrichtlinien bedarf, auf deren Grundlage sich Stationen miteinander unterhalten und sich gegenseitig verstehen. Sende- und Empfangsstationen müssen sich an bestimmte Spielregeln halten, damit die Übertragungswünsche der Netzteilnehmer nicht im Chaos enden.

Zur Veranschaulichung der Struktur eines Kommunikationsablaufs zwischen zwei Teilnehmern dient ein logisches Modell. Die Grundidee besteht darin, den Kommuni-

kationsvorgang in eine Hierarchie von Funktionsschichten zu gliedern. Jede Schicht bietet der ihr übergeordneten Schicht Funktionen an und kann Dienste der unter ihr liegenden Schicht in Anspruch nehmen, ohne ihre Funktionsweise zu kennen. Dem Anwender bleibt die Schichtung verborgen. Die Schichten der gleichen Ebene kommunizieren über Protokolle miteinander. Sie beinhalten definierte Regeln, nach denen die beiden Kommunikationspartner zusammenarbeiten und der nächst höheren Ebene ihre Dienstleistung anbieten.

Die Kommunikation zwischen Rechnern in offenen, heterogenen Systemen wird heutzutage durch das ISO-/OSI-Referenzmodell beschrieben. Das Referenzmodell ist ein konzeptioneller Rahmen, der Funktionen und Schemata für den Kommunikationsvorgang enthält. Dieser Rahmen teilt den Kommunikationsvorgang in sieben aufeinander aufbauende Schichten ein, denen allgemeine Vereinbarungen und Inhalte zugrunde liegen. Allerdings enthält diese Spezifikation keine Implementierungsvorgaben, sodass eine generelle Umsetzung in Produkte nicht möglich ist. Sie dient lediglich als Leitlinie für den Entwurf und die Implementierung von Standards, Geräten und Kommunikationsverfahren. Der Vorteil dieser Vorgabe beruht in erster Linie auf der offenen allgemein verbindlichen Vorstellung eines Kommunikationsvorganges in Form eines Architekturmodells. Darüber hinaus dient die Beschreibung der Funktionen der einzelnen Schichten als Basis für eine präzise Spezifikation von Protokollen und schafft dadurch letztlich eine weitgehend herstellerneutrale Begriffswelt. Daher ist es theoretisch möglich, das Protokoll einer einzelnen Schicht durch eine Neuentwicklung zu ersetzen, ohne die Funktionen der anderen Schichten zu beeinträchtigen.

Die Protokolle regeln den Kommunikationsablauf, ähnlich wie die Unterhaltung zweier Personen bestimmten Vereinbarungen folgt. Jede Schicht des Senders nutzt ihr eigenes Protokoll, um virtuell mit der entsprechenden Schicht des Empfängers zu kommunizieren. Die ausgetauschten Informationen werden in sog. **PDUs** (Protocol Data Units) übertragen. Diese PDUs enthalten je nach Schicht Prüfdaten, Adressen oder Informationen über übergeordnete Protokolle.

Der Prozess des Durchwanderns der OSI-Schichten macht eine permanente Neuaufteilung der Informationen notwendig, da alle Protokolle nur bestimmte Paketgrößen akzeptieren – **Fragmentierung**. Zur Übertragung selbst werden die PDU-spezifischen Informationen an die zu übertragenen Daten angeheftet – **Encapsulation**. Auf Empfängerseite verläuft der Prozess analog – **De-Encapsulation:**

1. Lesen der schichtspezifischen Information.
2. Abtrennen der PDU-spezifischen Daten.
3. Weiterleiten der verbliebenen Daten an die übergeordnete Schicht.

Den Ablauf auf drei Ebenen verkürzt zeigt folgendes Beispiel.

Verkürztes Philosophenmodell

Der Philosoph Hill in England möchte seinem chinesischen Kollegen Xiu eine wichtige Fachfrage stellen. Ihr Kommunikationsmedium wäre die Fachsprache der Philosophen. Nun spricht Herr Hill nur englisch, Herr Xiu nur chinesisch. Um dennoch eine Verständigung zu ermöglichen, bedienen sich beide der Hilfe von Dolmetschern. Wie gewöhnlich verfasst Herr Hill seine Frage in Englisch und übergibt diese einem Dolmetscher, der sie in eine beliebige Zwischensprache z. B. Italienisch übersetzt. Wie kommt nun die Nachricht vom Dolmetscher des Herrn Hill zum Dolmetscher des Herrn Xiu? Da beide Philosophen Computer-Freaks kennen, die ständig über das Internet miteinander Nachrichten austauschen, lassen sie ihre ins Italienische übersetzte Frage einfach von diesen übermitteln. Beide Computernutzer müssen dazu kein Wort Italienisch kennen; sie haben lediglich die Aufgabe, die Worte korrekt zu übertragen. Sobald die Nachricht den chinesischen Computer-Freak erreicht, übergibt er diese dem Dolmetscher, der sie ins Chinesische transformiert und Herrn Xiu überreicht. Auf diese Art können zwei Philosophen miteinander sprechen, ohne die Muttersprache ihres Partners zu beherrschen.

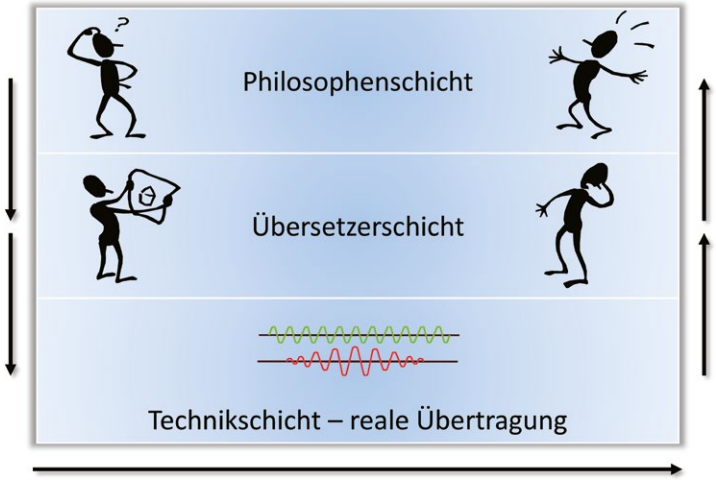

Bild 1.7 Philosophenmodell mit drei Schichten

Wie Bild 1.7 verdeutlicht, findet die eigentliche Übertragung ausschließlich auf der untersten, der Technikschicht statt. Diese Ebene und die Übersetzungsschicht können ohne Funktionseinbuße ausgetauscht werden. Falls der italienische Dolmetscher ausfällt, könnte Französisch als Zwischensprache dienen bzw. falls die Internetnutzung nach China untersagt ist, kann auf Fax ausgewichen werden. Damit wird deutlich, dass die Protokolle bis auf die Schnittstellen voneinander unabhängig und beliebig ersetzbar sind.

Im Unterschied zu den Diensten oder Funktionen, die für die vertikale Kommunikation zwischen den Schichten verantwortlich sind, regeln Protokolle die Kommunikation zweier Partner auf gleicher Ebene, also in horizontaler Richtung. In diesem Sinne ist die Einigung auf Italienisch als Übersetzungs- und das Internet als Transportmedium die Verständigung auf Protokolle.

Die detaillierte und standardisierte Kommunikation nach dem ISO-/OSI-Referenzmodell im Netzwerkumfeld basiert auf sieben Schichten. Die Gesamtheit der sieben OSI-Schichten wird oft als Stack bezeichnet. Die untersten Schichten dieses Modells präsentieren netzorientierte Funktionen, die oberen werden als anwendungsbezogen eingestuft. Der Ablauf erfolgt beim Sender streng von oben (Schicht 7) nach unten (Schicht 1) und beim Empfänger in der umgekehrten Richtung.

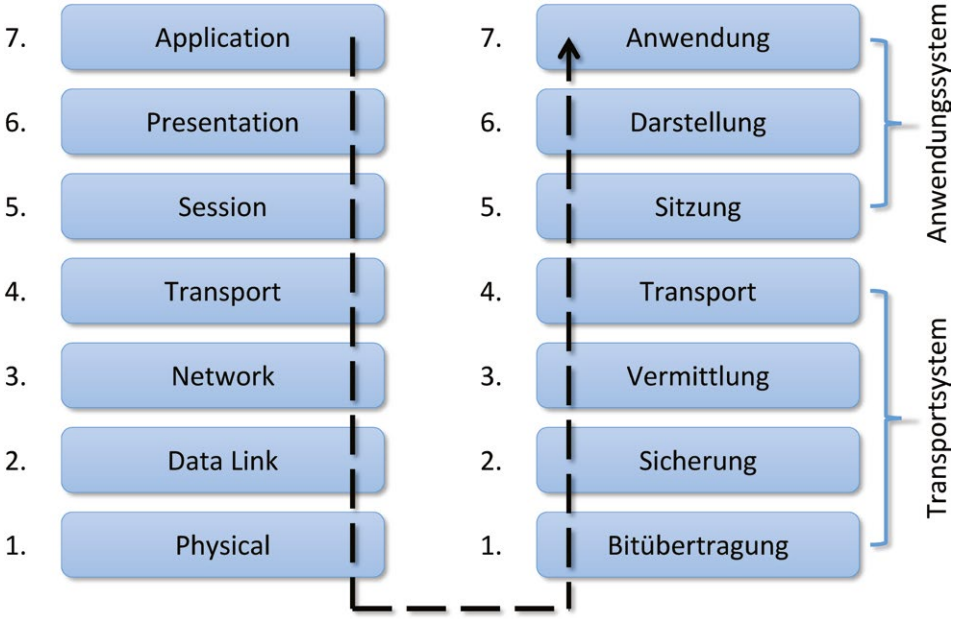

Bild 1.8 ISO-/OSI-Referenzmodell

Neben dem OSI-Modell existiert die Vorstellung der Internetwelt in Form des DoD (Department-of-Defense)-Modells über eine funktionale Gliederung des Kommunikationsvorganges. Eine Gegenüberstellung beider Konzepte zeigt Bild 1.9.

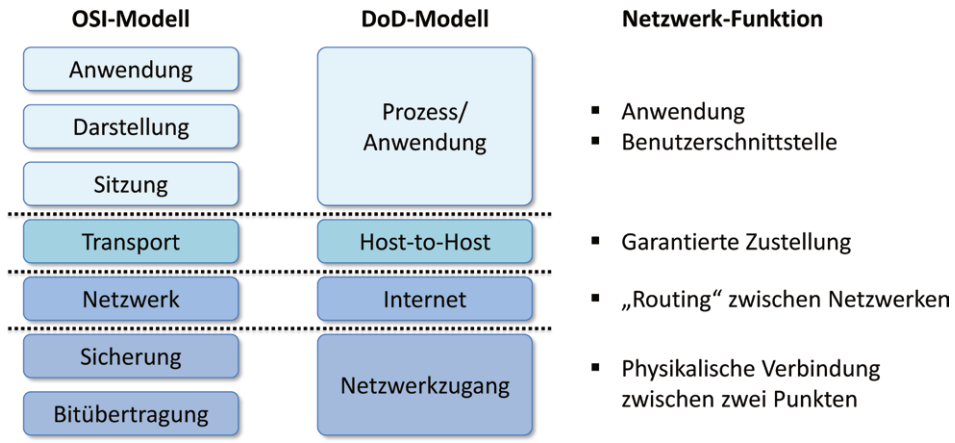

Bild 1.9 Vergleich: ISO-/OSI-Referenzmodell – DoD-Modell

Was ist nun der Inhalt der einzelnen Schichten?

- **Bitübertragungsschicht:** Hier werden die elektrischen, mechanischen und funktionalen Parameter zur physikalischen Übertragung festgelegt. Die Grundfunktion besteht in der Bereitstellung der physikalischen Verbindung und deren kontinuierlicher Betriebsbereitschaft. Zur Gewährleistung dieser Anforderungen sind mehrere grundlegende Details zu klären:

- Wie wird gewährleistet, dass ein Bit der Wertigkeit 1 sowohl vom Sender als auch vom Empfänger als solches erkannt wird?
- Welcher elektrischen Größe entspricht eine logische Eins, welcher eine logische Null?
- Wie viele Mikrosekunden soll die Dauer der Übertragung eines Bits dauern?
- Wie wird eine Verbindung aufgebaut und wie wird sie eingestellt?
- Kann eine Übertragung in beide Richtungen erfolgen?

In Netzwerken werden drei Medien genutzt:

- **Kupfer:** hier beruht die Signalisierung auf elektrischen Impulsen,
- **Glasfaser:** hier bildet ein optisches Signal die Grundlage der Signalisierung,
- **Luft:** hier werden Radio- oder Lichtwellen über die Luft übertragen.

In allen drei Formen ist es notwendig, den Beginn und das Ende einer Übertragung mitzuteilen. Dies geschieht über besondere Bitfolgen. Um die Bitfolgen selbst mit semantischem Inhalt zu versehen, ist ein Codierungsschema erforderlich, das Gruppen von Bits zu logischen Einheiten zusammenfasst. Auf diese Weise gelingt es, Buchstaben, Zeichen und Zahlen abzubilden. Die Bitfolgen selbst müssen entsprechend des Mediums signalisiert werden. Hierzu sind bestimmte Schemata notwendig, die vor allem auch eine zweifelsfreie Erkennung des übermittelnden Symbols durch den

Empfänger ermöglichen müssen. Zur Spezifikation der Funktionalität gehören außerdem Vereinbarungen der Festlegung von Kabeln und Steckern.

- **Sicherungsschicht:** Die primäre Aufgabe dieser Schicht besteht in der Gruppierung des übertragenen Bitstroms in logische Einheiten. In Abhängigkeit von der eingesetzten Netztechnologie entstehen Rahmen oder Frames unterschiedlichen Inhalts und variierender Größe. Die auf diese Weise zusammengefassten Rohdaten enthalten eine Prüfsumme, sodass auf der Übertragungsstrecke entstehende Veränderungen der Bitfolge erkannt werden. In Abhängigkeit davon, ob eine Fehlerkorrektur eingeleitet wird oder nicht, wird zwischen gesichertem und ungesichertem Dienst unterschieden. Darüber hinaus findet eine funktionale Trennung in zwei Aufgabenbereiche statt:
  - **Media Access Control (MAC):** Steuerung des Zugriffs auf das Übertragungsmedium. Dazu lassen sich zwei Methoden unterscheiden: **kontrolliert**, d. h. jede Station nutzt ein ihr zugeteiltes Zeitintervall zur Übertragung, **wettkampfbasiert**, d. h. die sendewilligen Stationen konkurrieren um die Übertragungsmöglichkeit.
  - **Logical Link Control (LLC):** Verwaltung der logischen Verbindung, Fehleranalyse und Flusskontrolle. Dafür gilt es drei Fragen zu beantworten: Welche Knoten kommunizieren miteinander, wann beginnt und endet eine Kommunikation, welche Fehler können während der Kommunikation auftreten?

Die Adressen dieser Ebene werden als physikalische Adressen angesehen. Sie erlauben den Pakettransport innerhalb eines lokalen Netzwerkes, geben aber keine Auskunft darüber, in welchem Netzwerk und wo sich die Station befindet. Damit haben diese Adressen keine Bedeutung über die Grenze des lokalen Netzes hinaus. Die Bedeutung im lokalen Netzwerk ergibt sich daraus, dass üblicherweise keine Punkt-zu-Punkt-Verbindungen existieren, sondern viele Stationen miteinander vermascht sind.

- **Netzwerkschicht:** Um ein Paket zustellen zu können, ist eine Adresse erforderlich. Dazu dient eine logische Adressierung, auf deren Grundlage im nächsten Schritt ein Paketleitweg der Nachricht vom Quell- zum Zielrechner gewählt wird. Dieses als **Routing** bekannte Verfahren sucht einen günstigen Pfad nach unterschiedlichen Kriterien. Dazu können eine gleichmäßige Lastverteilung, hoher Durchsatz, geringe Kosten oder höchstmögliche Sicherheit zählen. Durch ein hierarchisches Adressschema entsteht zudem ein logisches Netzwerk, das im Gegensatz zum physikalischen Netzwerk der Sicherungsschicht keine Verbindungseinzelheiten wie Kupfer- oder Glasfaserkabel oder die Signalisierung kennt. Dementsprechend lässt sich eine **physikalische Topologie**, die die Anordnung der Knoten und deren Verbindung kennt, von **der logischen Topologie**, die den Weg beschreibt, wie ein Netzwerk Pakete zwischen den Knoten transferiert, unterscheiden. Die Schicht wird benötigt, um einzelne lokale Netze miteinander zu verbinden und Pakete zwischen diesen Netzen weiterzuleiten.