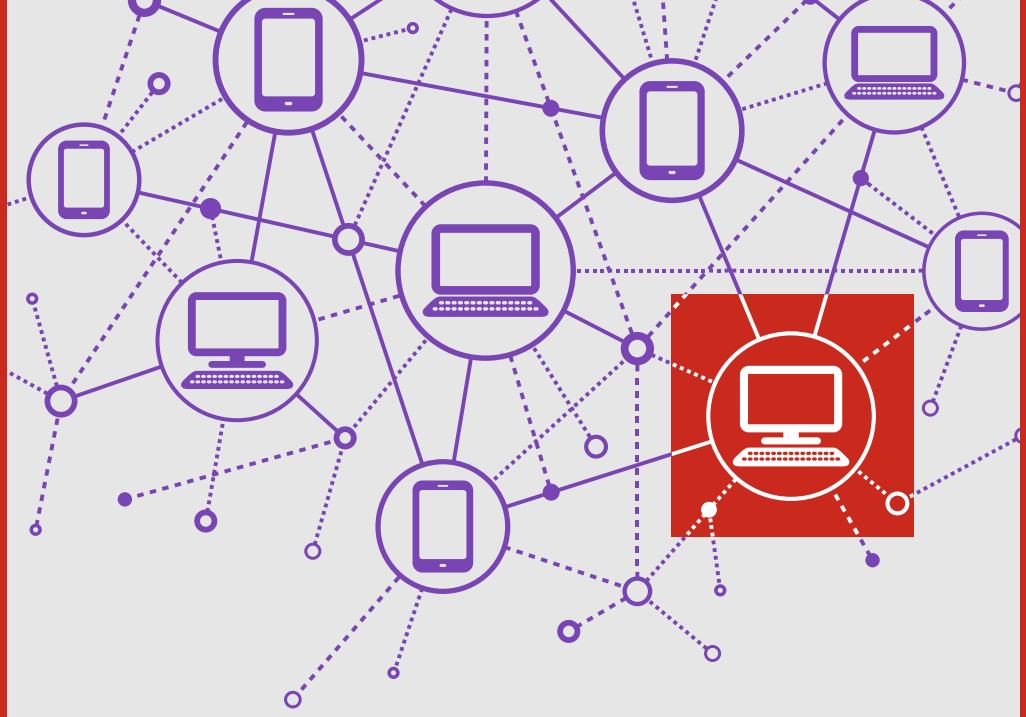

Wolfgang **RIGGERT**
Ralf **LÜBBEN**

RECHNER-NETZE

EIN EINFÜHRENDES LEHRBUCH

7., aktualisierte und erweiterte Auflage

Im Internet: Quizzes, Mind-Maps und die Lösungen zu den Aufgaben

HANSER

Riggert / Lübben

Rechnernetze

Ihr Plus – digitale Zusatzinhalte!

Auf unserem Download-Portal finden Sie zu diesem Titel kostenloses Zusatzmaterial. Geben Sie dazu einfach diesen Code ein:

plus-kfces-jfgkv

plus.hanser-fachbuch.de

Bleiben Sie auf dem Laufenden!

Unser **Computerbuch-Newsletter** informiert Sie monatlich über neue Bücher und Termine. 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
- Rolf Socher, Theoretische Grundlagen der Informatik

Wolfgang Riggert
Ralf Lübben

Rechnernetze

Ein einführendes Lehrbuch

7., aktualisierte und erweiterte Auflage

HANSER

Autoren:

Prof. Dr. Wolfgang Riggert, Hochschule Flensburg

Prof. Dr.-Ing. Ralf Lübben, Hochschule Flensburg

Herausgeber:

Prof. Dr. Christian Märtin, Hochschule Augsburg

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.

Lektorat: Frank Katzenmayer
Herstellung: Frauke Schafft
Covergestaltung: Max Kostopoulos
Coverkonzept: Marc Müller-Bremer, www.rebranding.de, München
Titelbild: © istockphoto.com/Ani_Ka
Satz: Eberl & Koesel Studio GmbH, Altusried-Krugzell
Druck und Bindung: CPI books GmbH, Leck
Printed in Germany

Print-ISBN 978-3-446-47280-8
E-Book-ISBN 978-3-446-47382-9
E-Pub-ISBN 978-3-446-47383-6

Vorwort zur 7. Auflage

Trends wie die zunehmende Globalisierung, der digitale Wandel oder die Nachhaltigkeit in allen Bereichen der Wirtschaftstätigkeit betreffen auch immer die Netzwerke als Basisinfrastruktur. So zeigt die Globalisierung, dass die Verbindungen zwischen Systemen, Menschen, Geschäftsprozessen und Orten nicht nur verteilter, sondern auch zunehmend komplexer werden und dadurch die Bedeutung der Netzwerke steigen, sowie ihre Architektur und Sicherheit herausfordern. Die Digitalisierung setzt Netzwerke voraus, die flexibel auf neue Herausforderungen reagieren und sich innovativen Dienstleistungen und Prozessen anpassen. Begleitet wird die steigende Automatisierung durch zeitsensitive und ausführungskritische Aspekte, die eine zuverlässige und zeitgerechte Zustellung der übertragenen Daten sicherstellen müssen. Aus diesen Erkenntnissen resultiert die Einschätzung, dass bis 2023 mehr als 60 % der Unternehmen Netzwerke als den Kern ihrer digitalen Strategie einschätzen [PiSK19]. Die technologischen Trends, die diese Entwicklung unterstützen, konzentrieren sich auf fünf Bereiche:

- **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:** Nutzer sind es heutzutage gewohnt, alle benötigten Dienste und Applikationen auf jedem Gerät unabhängig vom Ort zu nutzen. 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 das Auftauchen von Virtual und Augmented Reality steigt der Austausch von Daten, die besondere Anforderungen an die Qualität der Übertragung stellen.

Vor diesem Hintergrund greift die neue Auflage Gesichtspunkte wie Sicherheit, QoS (Quality-of-Service) und aktuelle Wireless-Technologien auf. Damit sollen aktuelle Entwicklungen antizipiert und dem Lehrenden/Lernenden ein zukunftsorientiertes Lehrbuch angeboten werden. Wir – das Autorenteam – hoffen, dass uns dieser Anspruch gelingt.

Ergänzendes Material zum Buch steht unter dem Link *plus.hanser-fachbuch.de* zur Verfügung. Online ist auf HanserPlus umfangreiches Zusatzmaterial erhältlich: Quizzes, Linksammlungen und die Lösungen zu den Aufgaben.

Inhalt

Ergänzendes Material auf https://plus.hanser-fachbuch.de

Lösungen zu den Kapitelfragen
Die Abbildungen des Buches
Mind Maps
Quizzes auf Basis von Kahoot!

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 schlagen ein neues Kapitel in der Informationsverarbeitung auf. In vielen Unternehmen bilden sie heute das Rückgrat der Informationsinfrastruktur. Angefangen von Netzwerken, die nur fünf Rechner verbinden, reicht das Spektrum moderner Lösungen bis hin zu weltweiten Verbünden, in denen viele Rechnerwelten eine integrative Einheit mit größtmöglicher Produktivität bilden. Triebfeder für die fortschreitende Vernetzung ist das Internet. Als leistungsfähige Werbeplattform und Vertriebskanal für viele Arten von Produkten und Dienstleistungen überwindet es traditionelle Marktgrenzen mit Geschäftsmodellen wie E-Commerce. Infolge dieses Booms werden leistungsfähige Netzwerke, die eine Vielzahl von Nutzern innerhalb akzeptabler Antwortzeiten bedienen, eine notwendige Voraussetzung.

Im Vordergrund für den Betrieb und den Ausbau von Netzwerken stehen drei 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 neu zu strukturieren und auf Technologien mit höherer Bandbreite umzustellen.

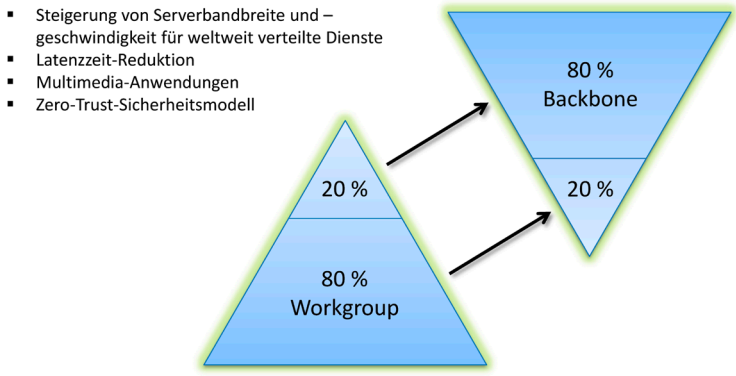

Bild 1.1 Veränderte 80/20-Regel

Dennoch existieren auch in diesem Meer von Unwägbarkeiten einige Fixpunkte. Diese Begriffe bilden praktisch die unverrückbaren Säulen des Netzgebäudes, um die sich alle neuen Entwicklungen ranken und an denen sie sich orientieren. 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.

Netzwerke bieten mehr als nur die Befreiung des PCs aus seinem isolierten Wirkungsbereich. 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

Eine Netzstruktur basiert auf vier Elementen:

- den **Rechnern oder Knoten**, die verbunden werden sollen,
- den **Infrastrukturkomponenten**, die den Anschluss und die Kopplung der Rechner im Gesamtkontext leisten. Zu ihren Aufgaben gehört es, Datensignale zu regenerieren und dann zu übertragen (Signalisierung), Informationen über die möglichen Wege im Netzwerk bereitzustellen, andere Geräte über Fehler im Netz zu informieren, Datenverkehr gemäß den Dienstgüteanforderungen zu klassifizieren oder Datenströme anhand von Sicherheitsrichtlinien zu erlauben oder zu unterbinden,
- der **Verkabelung**, die die physikalische Verbindung der einzelnen Elemente sicherstellt. Neben der kabelgebundenen Möglichkeit existiert die Anbindung von Endgeräten an die Netzwerkinfrastruktur über drahtlose Alternativen,
- dem **Protokoll**, das die Regeln für einen Nachrichtenaustausch festlegt. Dazu gehört die Definition von Nachrichtentypen und der Übertragungseinheit, d. h. des Datenpaketes, seines Inhaltes und seiner Größe und Struktur, sowie den Austauschprinzipien zwischen den Netzteilnehmern.

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 Glasfaserkabel. 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.

Die Vorteile eines Netzwerkes erstrecken sich auf unterschiedliche Bereiche:

- **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.

Die Leistungsfähigkeit eines Netzwerkes lässt sich anhand dreier Faktoren beurteilen:

- **Bandbreite:** Sie ist der Ausdruck für die Kapazität, die das Medium bewältigen kann. Sie misst das Informationsvolumen, das von einem zu einem anderen Ort in einer gegebenen Zeitspanne übertragen werden kann. Die übliche Maßeinheit ist Bit/s.
- **Durchsatz:** Er gibt die aktuell transportierte Menge an Daten an und spiegelt damit die augenblickliche Verkehrssituation und kein theoretisches Maximum wider.
- **Goodput:** Er ist das Maß für die übertragenen Nutzdaten, d. h. der reinen Nettodaten ohne den verwaltungsmäßig notwendigen Protokolloverhead.

1.2 Netzwerkkategorien

Netzwerke werden zur besseren Systematisierung, zur einfacheren Verwaltung und zur übersichtlicheren Fehlersuche in Kategorien eingeteilt. Eine gängige Typisierung unterscheidet nach:

- Personal Area Network (PAN),
- Reichweite,
- administrativer Verantwortung,
- Topologie,
- Technologie.

Der geografische Bereich, den ein Netzwerk abdeckt, wird aufgeteilt in:

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

PANs sind Netze mit geringer Reichweite, die das Umfeld einer Person abdecken, z. B. zur Kommunikation von Computern, Smartphones und Wearables. Häufig wird hierzu Bluetooth als drahtlose Funktechnologie verwendet.

LANs sind Netzwerke von Unternehmen. Jedes Unternehmen hat ein starkes Interesse daran, diese Infrastruktur unter eigener Kontrolle zu betreiben und zu warten, um das Herzstück der Informationstechnologie autonom zu halten. Es ist dabei auf das Firmen- oder Campusgelände und in seiner Ausdehnung ohne Zusatzmaßnahmen auf 500 m beschränkt.

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

Unter einem **MAN** ist ein Regionalnetz mit einem Ausdehnungsradius von ca. 100 km zu verstehen. Ein **WAN** hingegen ist keiner geographischen Beschränkung unterworfen.

MANs bilden häufig Verbindungsnetze zwischen Institutionen. Ihr Hauptaugenmerk liegt auf der Bildung von Kommunikationsverbünden jenseits der geographischen Unternehmensgrenzen unter eigener Administration und Kontrolle.

WANs verbinden die unterschiedlichen LANs der Unternehmen über eine gesonderte Infrastruktur, die sich im Besitz spezialisierter Dienstleister befindet. 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 oder aber unter Zuhilfenahme eines WANs räumlich unbegrenzt gekoppelt werden.

WANs sind Netzwerke, die Routing-Protokolle zur Wegewahl der zu übertragenen Informationen nutzen. LANs hingegen beruhen in der Regel auf dem Broadcast-Prinzip, wie es vom Rundfunk her bekannt ist.

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?

Unter Berücksichtigung dieser Fragestellungen lassen sich mehrere Grundformen beschreiben sowie eine Kombination dieser:

- **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.
- **Baum:** Ausgehend von einem Wurzelknoten verzweigt sich das Netzwerk in mehrere Äste. Die Wurzel und Knoten stellen hierbei Infrastrukturkomponenten zur Weiterleitung von Daten dar. Die Knoten am Ende sind Endgräte wie PCs und Laptops. Kommt es zu Ausfällen an der Wurzel oder in den mittleren Schichten, werden Äste voneinander getrennt.
- **(Voll-)Vermascht:** Knoten haben eine oder mehrere Verbindungen zu weiteren Knoten. Ist jeder Knoten mit jedem anderen verbunden, wird dies als vollvermascht bezeichnet. Die Vollvermaschung bietet einen hohen Schutz gegenüber Ausfällen von Knoten und Verbindungen, erfordert aber einen hohen Aufwand bei der Verkabelung. Deswegen haben häufig nur Knoten mit zentraler Funktion viele Verbindungen, so dass beim Ausfall von Verbindungen alternative Wege möglich sind. Prominentestes Beispiel ist das Internet. Dieses besteht aus einer Vermaschung von vielen wiederum vermaschten Netzen.

Derzeit hat sich der Stern und als dessen Erweiterung der Baum als „State of the Art“ im LAN durchgesetzt. Im Kernbereich von Netzen werden häufig zentrale Elemente redundant ausgelegt und miteinander vermascht, sodass Ausfälle einzelner Infrastrukturkomponenten nicht zum Gesamtausfall oder zur Segmentierung des Netzwerkes führen. Typisch ist diese Topologie für die Vernetzung im Bereich der LANs auf Basis von Ethernet.

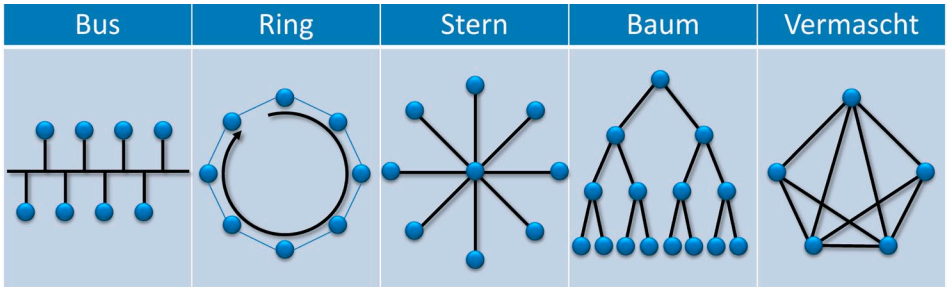

Bild 1.2 Netzwerktopologien

Tabelle 1.1 Topologievergleich

	Bus	Ring	Stern	Baum	Vermascht
Verkabelungsaufwand	++	+	–	+	–
Skalierbarkeit	+	++	++	++	++
Fehlertoleranz	+	–	+	+	++

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 Rechner zunächst die Verarbeitung von Massendaten und die Bewältigung von Routinetätigkeiten im Vordergrund, so hat sich dieses Bild 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 verbindet Funktionalität und Datenverwaltung als untrennbare Einheit. Die Verbindung mit anderen Rechensystemen ist schwierig bis unmöglich, sodass diese Konstellation denkbar integrationsfeindlich ist. Aber nicht nur die mangelnde Integrationsmöglichkeit stellt eine Hürde dar. Weitere Probleme:

- die Unterstützung neuer Anforderungen verlangt stets neue Systeme,
- die schneller als der Leistungszuwachs steigenden Kosten,
- die teure Pflege und Wartung,
- die mangelhafte Skalierbarkeit.

Peer-to-Peer- und 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 richtet, 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 Ver-

teilung, 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.

Welche Auswirkungen eine Vernetzung dezentraler Knoten auf einzelne Nutzer hat, zeigen folgende drei Aspekte:

- **Räumliche Trennung:** Ressourcen in einem Netz haben zu ihrem Kommunikationspartner eine räumliche Distanz. Daraus ergibt sich eine Verzögerung der Signale, die sich letztlich in der Übertragungsdauer niederschlägt. Dem Nutzer begegnet dieser Aspekt durch die Antwortzeit. Aber auch die verfügbare Bandbreite, die Verzögerung von Sendungen oder die Fehlerrate des Mediums können den Nutzer beeinträchtigen.
- **Unabhängigkeit der Knoten:** Die einzelnen Rechner eines Netzes handeln autonom, d. h. sie unterliegen keinem Abstimmungsmechanismus 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 Knoten des Netzes unterscheiden sich hinsichtlich Hardware, Betriebssystem und Anwendung. Zur Teilnahme am Netzbetrieb bestehen keine Voraussetzungen hinsichtlich bestimmter Ausstattungsmerkmale. Zum Datenaustausch zwischen den Knoten ist damit keine Kenntnis der genauen Konfiguration eines Partners erforderlich.

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

Vorteile Peer-to-Peer	Vorteile Client/Server
preiswerte Implementierung	zentralisierte Administration – alle Daten können zentral gesichert werden
kein Netzwerkadministrator notwendig	Skalierbarkeit und flexible Architektur
	verbesserte Sicherheit
Nachteile Peer-to-Peer	**Nachteile Client/Server**
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 Leistung 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 1.3
3-Schichten-Modell

Cloud-Computing

Während die Client/Server-Architektur 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 (Tabelle 1.3) an:

Tabelle 1.3 Serviceebenen des Cloud-Computings

Typ	Beschreibung
Infrastructure as a Service (IaaS)	Zurverfügungstellung von Infrastrukturkomponenten wie Speicher oder virtualisierten Servern und deren Nutzung über das Netz
Platform as a Service (PaaS)	Bereitstellung von Laufzeit- und Entwicklungsplattformen, um Anwendungen auch mit Datenbankanbindungen zu erstellen
Software as a Service (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 oder
- 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 wird. 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-Computing 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 sowie die Abhängigkeit von einer leistungsstarken und stabilen Netzverbindung erweisen sich als Probleme. Auf der anderen Seite sieht sich auch der Anbieter der Cloud Infrastrukturproblemen gegenüber:

- die mangelnde Interoperabilität beeinträchtigt ein Wechsel potenzieller Nutzer,
- die Erfolgsabhängigkeit von der Komplexität des Soft- und Hardwareangebots – insbesondere Anwendungssysteme wie ERP-Software erfordern spezialisiertes 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 Netzzugang und Pakettransport

Eine Kernfrage ist die Regelung des Zugangs der einzelnen Stationen zum Übertragungsmedium. Für die Ankopplung eines Rechners sind zwei Verfahren 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 zugrunde liegenden 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 in Frage:

- **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.

Die grundlegende Idee des Informationstransportes in Netzwerken besteht darin, Nachrichten in kleine Einheiten, sog. Pakete oder Frames, zu zerlegen, diese mit Adress- und Steuerdaten zu versehen und sie dann zuzustellen. Vor einer Übertragung der Daten erfolgt ihre logische Gruppierung in Pakete. Diese Fragmente der Ursprungsdaten sind leichter zu handhaben und für den Nutzer besser zu interpretieren. Darüber hinaus besitzen Pakete mehrere Vorteile:

- Die Paketeinteilung hindert Rechner daran, die Netzwerkbandbreite zu monopolisieren.
- Gehen Pakete auf dem Übertragungsweg verloren, muss nicht die gesamte Information neu gesendet werden, sondern nur Teile.
- Abhängig von der Auslastung können Pakete unterschiedliche Wege zum Ziel nehmen.

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 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 (Wegewahl) und müssen – abhängig von der Technologie – möglicherweise häufiger fragmentiert werden.

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 wie-

der 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 Broadcast-Netze** 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.

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 Internet Protocol Version 6 (IPv6) unterstützt.

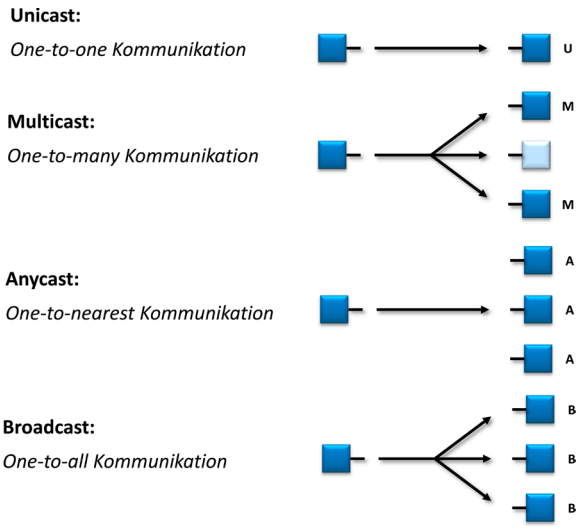

Bild 1.4 Anzahl der Kommunikationsteilnehmer

Die Übertragungsform selbst trennt zwischen **Leitungs- und Paketvermittlung**. In Analogie zum Telefondienst wird bei der Leitungsvermittlung für die Dauer der Sitzung bzw. des Telefongespräches eine exklusive Verbindung zwischen den

Kommunikationspartnern aufgebaut. Eine Alternative bietet sich mit der Paketvermittlung an, deren Ablauf dem der Briefpost entspricht. Die zu übermittelnde Nachricht wird zu mehreren Paketen zusammengestellt, mit Absender- und Empfängeradresse versehen und einer bekannten Versandstelle übergeben. Jedes Paket nimmt nun – ähnlich wie ein Brief – einen Weg durch das Beförderungsnetz, ohne dass der Absender den genauen Weg kennen muss. Im Gegensatz zur Leitungsvermittlung besteht zwischen Absender und Adressat keine ständige Verbindung.

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

Bei der **Paketvermittlung** durchqueren die Pakete das Netz als unabhängige und eigenständige Einheiten und können in den Vermittlungsknoten zwischengespeichert werden. Hierin liegt ein wesentlicher Vorteil, da nun die Übertragungsgeschwindigkeit zwischen einzelnen Teilstrecken keine Begrenzung mehr darstellt. Damit wird das Netzwerk aber zu einem Netzwerk von Warteschlangen. Jeder zu passierende Netzknoten empfängt das Paket und leitet es an seine Ausgangsschnittstelle, die aber Ziel vieler Sendungen sein kann, sodass die Möglichkeit von Überlastsituationen entsteht. Die Existenz der Warteschlangen erzeugt Verzögerungen in der Paketzustellung oder Paketverluste, wenn die Warteschlangen überlaufen. Die Paketverluste verursachen Paketwiederholungen (Retransmission) und haben damit eine weitere Belastung des Übertragungsweges zur Folge. Für den Anwender ist dieser Ablauf transparent. Er benötigt und erhält keinerlei Informationen über den Übertragungsweg, der sich zudem dynamisch ändern kann. 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, es durch andere Teilnehmer verwendet werden kann. Hierdurch kann eine Steigerung der Auslastung erreicht werden.

Ein lokales Netz besitzt nur eine begrenzte Ausdehnung. Häufig ist es auf eine Abteilung oder ein Gebäude ausgelegt. Im Zeitalter des Intra-/Internets sind Kommunikationsinseln aber ein Fremdkörper, sodass es nur folgerichtig sein kann, eine unternehmensweite Vernetzung anzustreben. Folgende Sachverhalte sind dabei zu beachten:

- **Gemeinsame Datenbestände sorgen für aktuelle Information:** Die wohl wichtigste Aufgabe eines Netzwerkes ist die zentrale Speicherung von Datenbeständen. Änderungen und Aktualisierungen der Daten finden ihren soforti-

gen 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 oder des Ausfalls. Der Zugriff auf Netzressourcen bildet damit keinen gesonderten und 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 einer zentralen Station muss auch nur diese mit großen Speichermedien ausgestattet sein. Die einzelnen Rechnerknoten selbst benötigen nur noch eine geringe Speicherkapazität. Darüber hinaus können hochwertige Geräte in das Netzwerk 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 Installation, Wartung oder Aktualisierung 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. Dass diese Auswertung zuvor erfasste Daten voraussetzt, zeigt, dass eine gewisse Nutzerkontrolle unumgänglich ist.
- **Verschlechterung der Antwortzeiten:** Da ein Wesensmerkmal eines Netzwerkes die gemeinsame Nutzung von Ressourcen ist, besteht auf dem Weg zu zentralen Elementen eine Konkurrenz zwischen allen Teilnehmern. Diese Situation schließt ein, dass jeder Nutzer nur über einen bestimmten Anteil der Übertragungskapazität verfügen kann. Je höher die Nutzerzahl, desto geringer die Kapazität des Einzelnen. Als Folge eines sinkenden Bandbreitenanteils steigt 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 wie Lokalität oder Netzdesign ab.

- **Notwendigkeit eines Netzadministrators:** Durch die Verteilung der Daten und Programme auf heterogene, autonome, miteinander kooperierende Rechnersysteme erhöht sich die Komplexität des Gesamtsystems, dessen Pflege, Wartung und Ausbau viel Aufwand und technisches Know-how erfordert.
- **Sicherheit:** Da verteilte Systeme allen Benutzern den gemeinsamen Gebrauch der Ressourcen ermöglichen, treten Sicherheitsanforderungen auf:
  - 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?

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 Wettbewerbsgewinn.
- **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. Derartig 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 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 Kommunikationsvorgang 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.

Wie Bild 1.5 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.

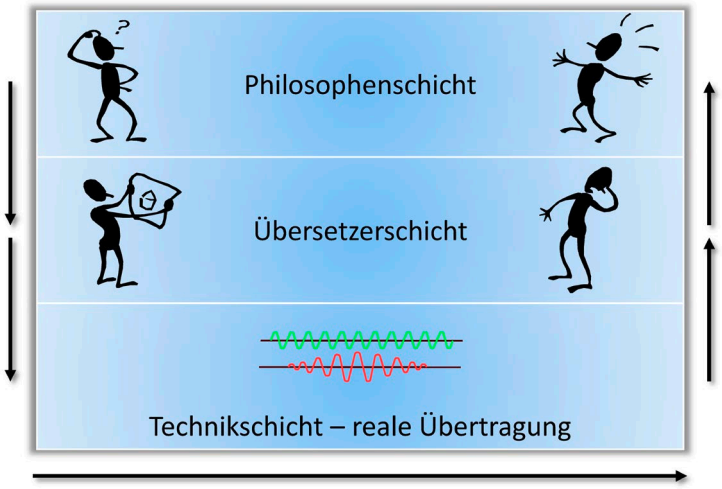

Bild 1.5 Philosophenmodell mit drei Schichten

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.

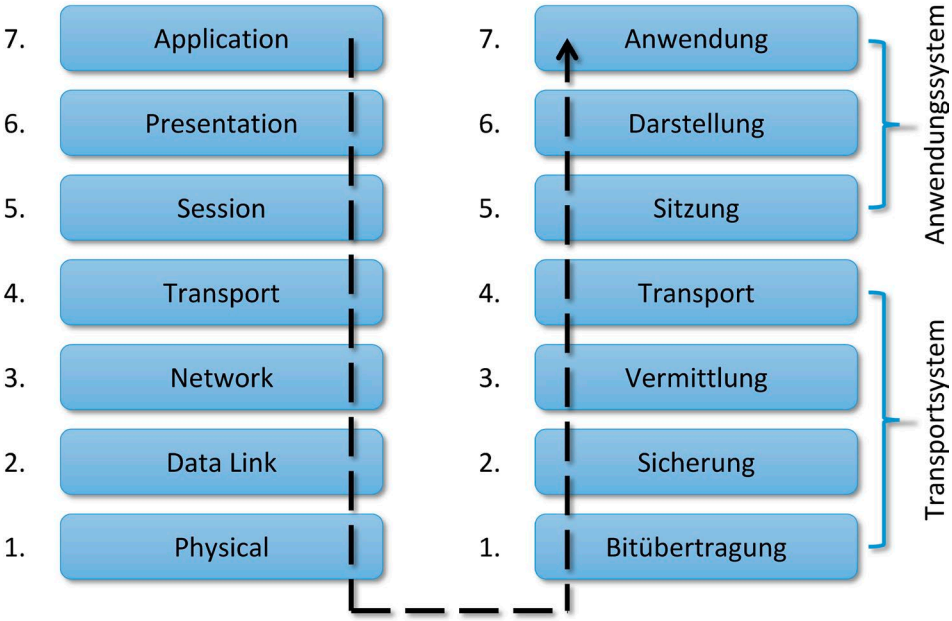

Bild 1.6 ISO/OSI-Referenzmodell

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 das nachfolgende Bild 1.7.

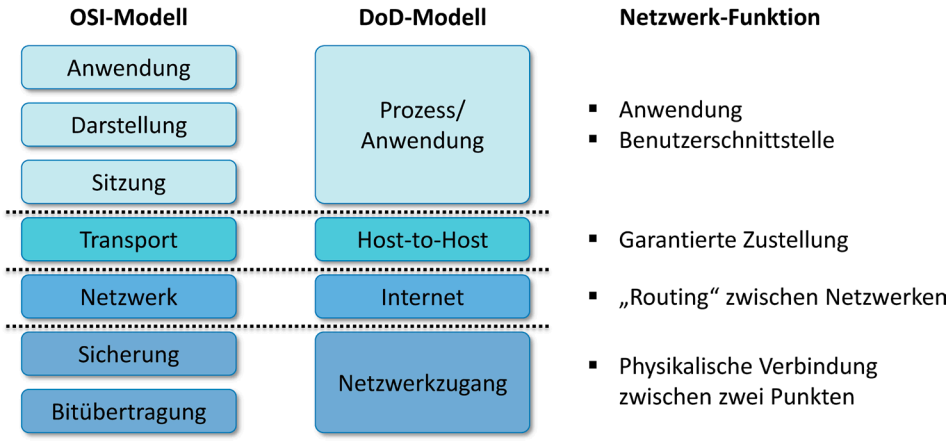

Bild 1.7 Vergleich: ISO/OSI-Referenzmodell – DoD-Modell

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 zur 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, und **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.

- **Transportschicht:** Diese Ebene stellt einen universellen Transportservice bereit. Sie richtet sich schwerpunktmäßig auf den Verbindungsaufbau, den Unterhalt und den Abbau mit gesicherten Qualitätsmerkmalen. Die Transportqualität sichert, dass
  - die richtigen Bits übertragen,
  - die Reihenfolge nicht verändert,
  - keine Bits verschluckt,
  - keine Sequenzen doppelt übertragen

  werden. Um den Datenstrom zwischen Sender und Empfänger den Netzcharakteristika optimal anzupassen, existieren Datenkontrollalgorithmen, die für eine gleichmäßige Auslastung der Verbindung sorgen, bei Überlast die Datenrate drosseln oder bei freiem Medium die Übertragungskapazität bis zur Leistungsgrenze ausschöpfen.

Die logischen Einheiten der Ebene 2 bis 4 tragen unterschiedliche Bezeichnungen. Die Protocol Data Units (PDUs) auf der Transportebene heißen Segmente, diejenigen der Schicht 3 Pakete und auf Schicht 2 wird von Frames gesprochen.

- **Sitzungsschicht:** Hier werden die Synchronisation und der Dialogablauf zwischen zwei Kommunikationsteilnehmern geregelt. So wird diese Schicht zum Ort, an dem das Netzwerkbetriebssystem einen wichtigen Teil seiner Funktionalität entfaltet.
- **Darstellungsschicht:** Prozessoren stellen Informationen in einem bestimmten Code dar. Big-Endian-CPUs wie die meisten RISC-Prozessoren verwenden das MSB-Format (Most Significant Byte), Little-Endian-CPUs wie die Intel-Familie stützen sich auf die LSB-Darstellung (Least Significant Byte). Unterscheiden sich die Darstellungsformate der am Kommunikationsprozess beteiligten Rechner, kommt es notgedrungen zu Fehlinterpretationen. Um diesen Effekt