Kapitel 2
Die Grundlage des Internets: TCP/IP-Referenzmodell

„Die Grenzen meiner Sprache bedeuten die Grenzen meiner Welt."
– Ludwig Wittgenstein, (1889 – 1951)

Das weltumspannende und allgegenwärtige Internet verbindet heute Rechner, Telefone, Unterhaltungselektronik und bald auch Haushaltsgeräte und Waren unseres täglichen Bedarfs. Mehr und mehr dringt es in alle Bereiche unseres Lebens vor. Damit alle diese unterschiedlichen Geräte ungestört und effizient miteinander kommunizieren können, muss ihre Kommunikation festen Regeln – sogenannten Kommunikationsprotokollen – folgen. Diese Kommunikationsprotokolle bilden das sogenannte TCP/IP-Referenzmodell. Es modelliert einzelne Schichten der Internet-Kommunikation, legt deren Aufgaben, ihren Abstraktionsgrad und Ihre Komplexität fest, und beschreibt den jeweiligen Funktionsumfang. Mit welchen Mitteln und auf welche Weise diese Spezifikationen umgesetzt werden, legt das Modell jedoch nicht fest, sondern überlässt dies der jeweiligen Implementation. Auf diese Art und Weise konnte das TCP/IP Referenzmodell aus der Praxis heraus Gestalt annehmen und bildet heute wie auch in Zukunft eine solide Basis für alle Kommunikationsaufgaben im Internet.

2.1 Kommunikationsprotokolle und Schichtenmodell

Widmen wir uns zunächst kurz den Grundlagen der Rechnerkommunikation. Die Hardware eines Computernetzwerkes setzt sich aus Komponenten zusammen, deren Aufgabe darin besteht, Informationen kodiert in Form von Bits von einem Rechner zu einem anderen zu übertragen. Würde man die Rechnerkommunikation ausschließlich auf dieser Ebene organisieren wollen, wäre das vergleichbar mit der Programmierung eines Rechners in einer rudimentären Maschinensprache, d.h. unter ausschließlicher Verwendung von Nullen und Einsen. Dadurch würde der notwendige Aufwand und die damit einhergehende Komplexität der zu bewältigenden Aufgaben praktisch unbeherrschbar. Ähnlich wie in der Rechnerprogrammierung wurden deshalb zur Steuerung und Nutzung von Rechnernetzen komplexe Softwaresysteme – sogenannte Netzwerkbetriebssysteme – geschaffen, mit deren Hilfe Rechnernetze

C. Meinel, H. Sack, *Internetworking*, X.media.press,
DOI 10.1007/978-3-540-92940-6_2,

auf bequemere Art und Weise von einer höheren Abstraktionsebene aus, gesteuert und genutzt werden können.
Diese Netzwerkbetriebssysteme basieren auf der Idee, Kommunikationsaufgaben und -funktionen in unterschiedlicher Abstraktion und Komplexität zu behandeln. Dabei werden Aufgaben und Funktionalität des gleichen Abstraktionslevels gebündelt in sogenannten Schichten betrachtet. Aufeinander aufbauend werden so unterschiedliche Schichten definiert, die mit zunehmenden Abstraktionsgrad unterschiedlich komplexe Kommunikationsaufgaben abhandeln und dem Benutzer oder einer Computeranwendung über geeignete Schnittstellen zur Verfügung stellen. Das entstehende Modell wird als **Schichtenmodell der Kommunikation** bezeichnet. Die auf den unterschiedlichen Schichten agierenden Kommunikationsprotokolle greifen über die im Schichtenmodell beschriebenen Schnittstellen ineinander und bieten gemeinsam als Familie von Kommunikationsprotokollen (Protokollfamilie, Protocol Suite) ein funktionstüchtiges Netzwerkbetriebssystem.
Der Nutzer, wie auch die meisten Anwendungsprogramme, die über das Netzwerk kommunizieren, um Daten auszutauschen und Dienste anzubieten, kommen lediglich mit diesem Netzwerkbetriebssystem in Kontakt und nur äußerst selten mit der darunter verborgenen Netzwerk-Hardware.

2.1.1 Protokollfamilien

Zur Kommunikation müssen sich – übrigens nicht nur im Falle der digitalen Kommunikation in Rechnernetzen – alle kommunizierenden Parteien auf gemeinsame feste Regeln zum Austausch von Nachrichten einigen. Dies betrifft sowohl die zur Kommunikation verwendete Sprache, als auch alle Verhaltensregeln, die eine effiziente Kommunikation erst ermöglichen. Diese Verhaltensregeln werden in der Fachsprache mit dem Begriff **Kommunikationsprotokoll** oder **Protokoll** zusammengefasst. Ein Kommunikationsprotokoll legt sowohl das Format der von den Kommunikationspartnern auszutauschenden Nachrichten fest und spezifiziert auch sämtliche Aktionen, die zur Übermittlung dieser Nachrichten notwendig sind. Im Falle der Kommunikation in Rechnernetzen heißt die Software, mit der das Netzwerkprotokoll auf einem Rechner implementiert wird, **Protokoll-Software**. Während die Entwicklung der ersten Rechnernetze vornehmlich nur die beteiligte Hardware fokusierte und die Protokollsoftware nur als zweitrangig angesehen wurde, hat sich diese Strategie grundlegend verändert. Protokollsoftware ist heute sehr komplex hochgradig strukturiert. Anstelle ein riesiges, komplexes und universelles Netzwerkprotokoll bereitzustellen, das sämtliche anfallenden Aufgaben der Netzwerk-Kommunikaton regelt, wurde das Problem der Netzwerk-Kommunikation nach dem Prinzip „Teile-und-Herrsche“ (*divide et impera*, *divide and conquer*) in eine Vielzahl einzeln handhabbarer Teilprobleme zerlegt, zu deren Lösung jeweils eigene problemspezifische (Teil-)Protokolle bereitgestellt werden.
Die verschiedenen Teilprobleme werden jeweils von speziellen Protokollen abgehandelt, die aber – und dies ist das zweite zu lösende, in seiner Komplexität nicht

zu unterschätzende Problem – alle reibungslos ineinandergreifen und zusammenarbeiten müssen. Um dieses Zusammenspiel zu gewährleisten, wird die Entwicklung der Protokoll-Software als eine umfassend zu lösende Gesamtaufgabe angesehen und durch die Bereitstellung einer zusammengehörigen **Familie von Protokollen** (Protokollstapel, Protocol Suites) gelöst, in der alle Einzelprotokolle effizient miteinander interagieren und im Zusammenspiel das Gesamtproblem der Netzwerk-Kommunikation lösen.
Zwar besitzen die unterschiedlichen Protokollfamilien viele gemeinsame Konzepte, doch da sie in der Regel unabhängig voneinander entwickelt wurden, sind sie nicht kompatibel. Dennoch ist es möglich, verschiedene Protokollfamilien gleichzeitig und parallel auf den Rechnern eines Netzwerks einzusetzen, und diese alle sogar dieselbe physikalische Netzschnittstelle nutzen zu lassen, ohne dass es dabei zu Störungen kommt.
Der Begriff „Protokoll“ wird üblicherweise in zwei unterschiedlichen Bedeutungen verwendet. Einerseits bezieht sich der Begriff des Protokolls auf die Definition einer abstrakten Schnittstelle (Interface). Dazu zählen sämtliche Funktionen und Operationen, die über diese Schnittstelle zur Verfügung gestellt werden. Andererseits werden unter dem Protokollbegriff sämtliche zur Kommunikation ausgetauschten Nachrichtenformate und deren Bedeutung zusammengefasst. Die Definition des Protokolls – die **Protokollspezifikation** – erfolgt meist in einer Kombination aus spezifizierendem Text, Abbildungen, Zustandsübergangsdiagrammen und Algorithmen in Pseudocode. Die Spezifikation muss so präzise sein, dass unterschiedliche Implementationen der Protokolle interoperabel sind, dass also zwei der verschiedenen Implementationen erfolgreich Nachrichten austauschen können.

2.1.2 Schichtenmodell

Um die Protokoll-Designer in ihrer Arbeit zu unterstützen, wurden Werkzeuge und Modelle entwickelt, die den Gesamtprozess der Netzwerk-Kommunikation feingliedrig aufschlüsseln und hierarchisch aufeinander aufbauend anordnen. So werden klare Schnittstellen zwischen den einzelnen Hierarchiestufen festgelegt, die die weitgehend unabhängige Entwicklung und Verbesserung der auf diesen Stufen jeweils angesiedelten Netzwerkprotokolle ermöglichen und so weit wie möglich vereinfachen. Die bekannteste Modellvariante ist das **Schichtenmodell** (Layering Model, Protocol Stack) (siehe Abb. 2.3). Der gesamte Netzwerk-Kommunikationsprozess wird dabei in einzelne übereinander angeordnete Schichten (Layers) aufgeteilt, wobei jede Schicht ein bestimmtes Teilproblem der Netzwerkkommunikation adressiert und eine neue Abstraktionsebene der Kommunikation hinzugefügt. Die oberste Schicht bietet schließlich das Interface für Anwendungsprogramme, die Nachrichten mit Anwendungen auf anderen Rechnern austauschen wollen. Auf der Basis eines solchen Schichtenmodells konstruiert der Protokoll-Designer eine vollständige Protokollfamilie, den sogenannten **Protokollstapel**, bei dem die einzelnen Protokolle jeweils genau die auf einer Schicht adressierten Aufgaben lösen.

Prinzipiell ist in einem solchen Schichtenmodell die Übertragung einer Nachricht von einem Anwendungsprogramm des einen Rechners zu einem Anwendungsprogramm des anderen Rechners so organisiert, dass die Nachricht auf dem Ursprungsrechner über die verschiedenen Protokollschichten von oben nach unten durchgereicht und teilverarbeitet wird, dann physikalisch über das Übertragungsmedium übertragen und am Bestimmungsrechner dieselben Protokollschichten in umgekehrter Reihenfolge, also von unten nach oben, durchlaufend schließlich an die Anwendung übergeben wird (siehe Abb. 2.1).

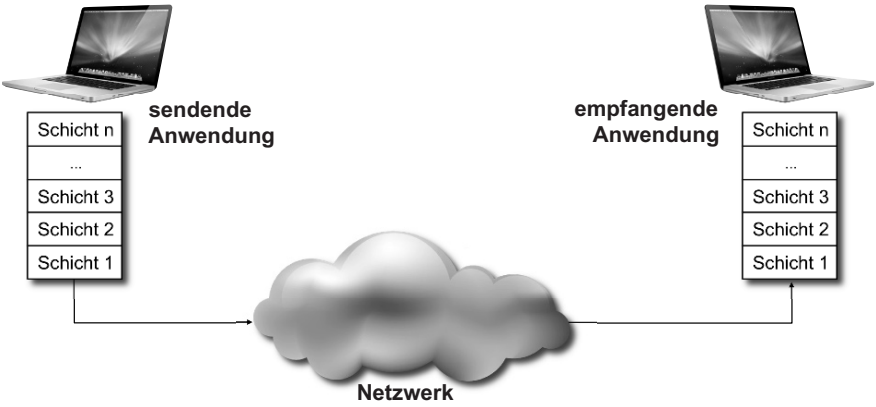


Abb. 2.1 Datenübertragung über einen Protokollstapel

Im Schichtenmodell ist jede Schicht für die Lösung eines bestimmten Teils der zahlreichen Aufgaben verantwortlich, die im Rahmen der Netzwerk-Kommunikation anfallen. Um diese Aufgaben korrekt erledigen zu können, werden auf Seiten des sendenden Rechners auf jeder einzelnen Schicht des Protokollstapels Kontroll- und Steuerinformationen kreiert und verwendet, die den zu übertragenden Daten hinzugefügt werden (siehe Abb. 2.2). Beim empfangenden Rechner werden diese Zusatzinformationen von der zur jeweiligen Schicht korrespondierenden Protokoll-Software ausgelesen und weiterverarbeitet, so dass die zu übertragenden Daten am Ende korrekt und in Originalgestalt abgeliefert werden können.
Gemäß dem Schichtenmodell der Netzwerkkommunikation muss die Protokoll-Software einer bestimmten Schicht *k* auf dem Rechner des Empfängers genau die Nachricht empfangen, die von der Protokoll-Software der Schicht k des sendenden Rechners übertragen wurde. Dies bedeutet, dass jede Veränderung, die die Protokolle einer bestimmten Schicht an den zu übertragenden Daten vornehmen, beim Empfänger wieder vollständig rückgängig gemacht werden muss. Fügt Schicht *k* den zu übertragenden Daten zusätzliche Steuer- und Kontrollinformationen an, muss Schicht *k* auf dem Empfängerrechner diese wieder entfernen. Findet in Schicht *k* eine Verschlüsselung der Daten statt, müssen auf Empfängerseite in der Schicht *k* die verschlüsselten Daten wieder entschlüsselt werden (siehe Abb. 2.4).

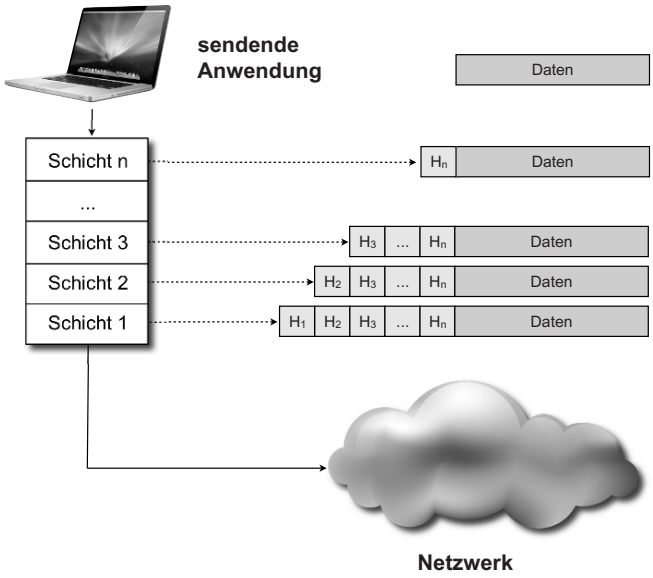


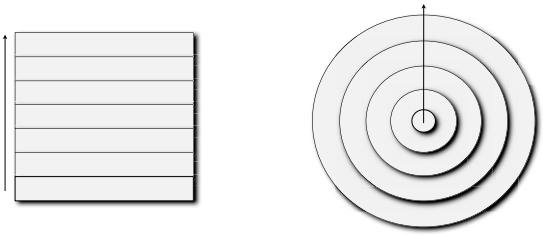
Abb. 2.2 Jede Schicht des Protokollstapels fügt eigene Steuer- und Kontrollinformationen (H_n...H_1) zu den zu übertragenden Daten hinzu

Die eigentliche Kommunikation erfolgt in den Protokollstapeln also immer in vertikaler Richtung. Beim Versenden von Daten fügt jede Protokollschicht ihre Steuer- und Kontrollinformationen zu diesen Daten hinzu. Typischerweise werden diese Informationen dann dem von der darüberliegenden Schicht zur Übertragung übergebenen Datenpaket als Header vorangestellt, man sagt, das Datenpaket wird „gekapselt". Aus diesen Zusatzdaten erhält die Protokollsoftware auf der Empfängerseite bzw. in einem Zwischensystem in der korrespondierenden Protokollschicht die notwendigen Steuer- und Kontrollinformationen, die eine korrekte und zuverlässige Weiterverarbeitung der übertragenen Daten gewährleisten. Auf den einzelnen Protokollschichten erscheint das so, als würde die Protokollsoftware auf beiden Seiten, bei Sender und Empfänger, direkt miteinander kommunizieren, während die Daten aber tatsächlich vertikal durch den Protokollstapel weitergeleitet werden. Diese scheinbar direkte Kommunikation auf den einzelnen Schichten wird auch als **virtuelle Kommunikation** bezeichnet (siehe Abb. 2.5).

Damit definiert jede Protokollschicht zwei verschiedene Schnittstellen. Damit Anwendungen die Dienste eines Protokolls auf dem eigenen Computer nutzen können, wird das sogenannte **Dienst-Interface** (Service Interface) definiert. Das Dienst-Interface legt sämtliche Operationen fest, die lokale Anwendungen mit dem Protokoll ausführen können. Zusätzlich wird in jeder Protokollschicht auch eine Schnittstelle zum Gegenstück bei der entsprechenden Protokollschicht auf einem anderen Computer definiert, das sogenannte **Partner-Interface** (Peer Interface).

Allgemeines zu Schichtenmodellen

Schichtenmodelle spielen in der Kommunikationstechnik, aber auch in anderen Gebieten der Informatik eine bedeutende Rolle. In abgewandelter Darstellung entsprechen diese auch dem **Schalenmodell**, das anstelle von hierarchisch aufeinander gestapelten Schichten aus einzelnen Schalen besteht.



Der Einsatz eines solchen Modells ist aus folgenden Gründen sinnvoll:

- **Teile und Herrsche (Divide et Impera / Divide and Conquer)**
  Nach dieser Strategie wird ein komplexes Problem in einzelne Teilprobleme zerlegt, die jedes für sich betrachtet, einfacher handhabbar und lösbar sind. Oft ist es dadurch überhaupt erst möglich, das Gesamtproblem zu lösen.
- **Unabhängigkeit**
  Die einzelnen Schichten kooperieren, indem jede Schicht stets nur die Schnittstellenspezifikation ihres direkten Vorgängers nutzt. Bei fest vorgegebener Schnittstellenspezifikation spielt der innere Aufbau einer Schicht für die anderen Schichten keine Rolle, so dass die Implementationen auf einer Schicht ohne weiteren Aufwand direkt gegen verbesserte Implementationen ausgetauscht werden können, die sich lediglich nur an der jeweiligen Schnittstellenspezifikationen orientieren müssen. Die Implementationen der einzelnen Schichten werden damit **unabhängig** von denen der anderen Schicht und ein **modularer** (baukastenartiger) Aufbau des Gesamtsystems wird ermöglicht.
- **Abschirmung**
  Jede einzelne Schicht kommuniziert jeweils nur mit den beiden direkt benachbarten Schichten. Damit wird eine **Kapselung** der einzelnen Schichten erreicht, wodurch die zu bewältigende Komplexität drastisch sinkt.
- **Standardisierung**
  Die Aufgliederung des Gesamtproblems in einzelne Schichten erleichtert auch die Entwicklung von Standards. Eine einzelne Schicht und ihre Schnittstellen mit den benachbarten Schichten lassen sich jeweils schneller und leichter standardisieren, als das komplexe Gesamtsystem.

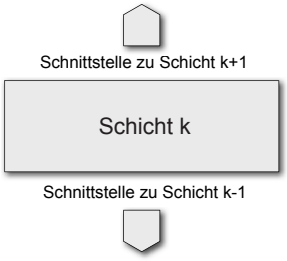


Abb. 2.3 Allgemeines zum Schichtenmodell

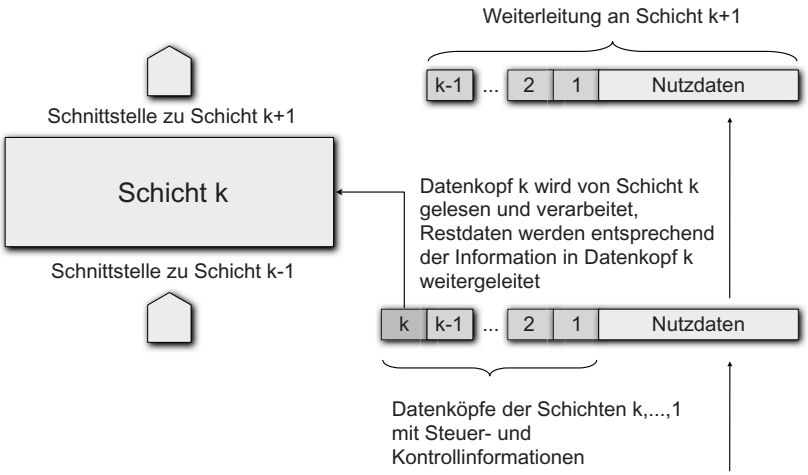


Abb. 2.4 Jede Schicht des Protokollstapels liest aus den empfangenen Daten den zur Schicht zugehörigen Datenkopf (Header) mit den für die Verarbeitung auf dieser Schicht notwendigen Steuer- und Kontrollinformationen

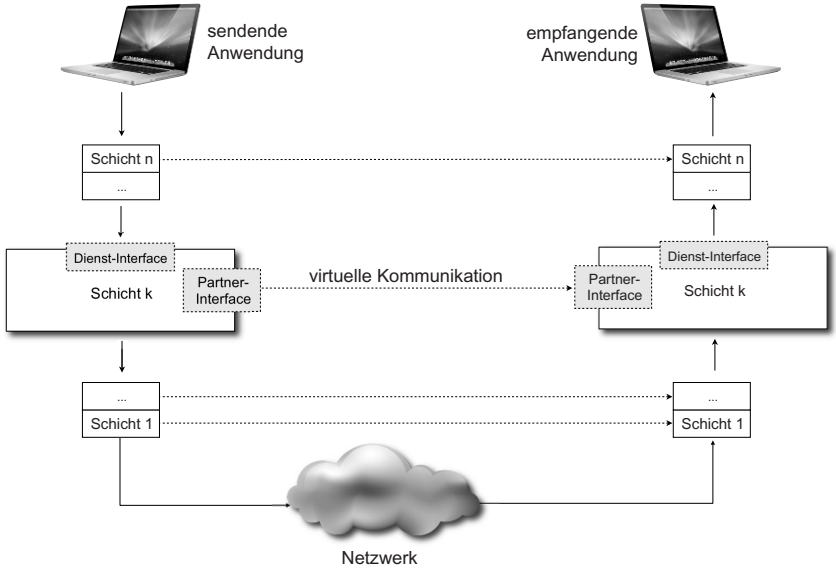


Abb. 2.5 Auf jeder Ebene kommunizieren die einzelnen Schichten des Protokollstapels scheinbar horizontal direkt miteinander (**virtuelle Kommunikation**), tatsächlich erfolgt die Kommunikation aber vertikal

Das Partner-Interface spezifiziert das Format von Nachrichten, die zwischen den benachbarten Protokollschichten auf unterschiedlichen Rechnern ausgetauscht werden und legt deren Bedeutung fest. Allerdings erfolgt die Kommunikation über das Partner-Interface auf indirekte Weise, d.h. jede Protokollschicht kommuniziert mit ihrem Gegenstück durch Übergabe von Nachrichten an eine niedrigere bzw. höhere Protokollschicht, die diese Nachricht auf gleiche Weise an ihr eigenes Gegenstück auf dem entfernten Rechner sendet.
Wird eine Protokollfamilie in Form eines Schichtenmodells realisiert, müssen beim Entwurf der beteiligten Protokolle einige grundlegende Aspekte beachtet werden, die schichtübergreifend für mehrere bzw. für alle Protokollschichten gelten. Damit eine Nachricht zwischen Sender und Empfänger tatsächlich ausgetauscht werden kann, muss auf jeder Schicht eine bestimmte Form der **Adressierung** realisiert werden, damit unter der Vielzahl der möglichen Empfänger der richtigee identifiziert werden kann. Darüber hinaus müssen auf jeder Schicht Regeln für den **Datentransfer** festgelegt werden. Fließen Daten dabei in beide Richtungen (bidirektional, Duplex-Betrieb) oder ist der Datenverkehr nur in einer Richtung möglich (unidirektional, Simplex-Betrieb)? Können im Rahmen einer Kommunikationsverbindung mehrere (logische) Kanäle aufgebaut und verwendet werden, z.B. ein Kanal für reguläre Daten, ein Kanal zur Steuerung der Kommunikation und ein weiterer Kanal für Daten mit hoher Priorität. Ebenfalls müssen bei der Übertragung aufgetretene Fehler erkannt bzw. korrigiert werden (**Fehlerkontrolle**). Diese Aufgabe ist für alle Schichten relevant und wird in unterschiedlichen Schichten mit verschiedenartigen Verfahren realisiert. Nachrichten werden aufgrund technischer und logischer Parameter zum Transfer in den einzelnen Schichten in kleinere Untereinheiten zerlegt (**Fragmentierung**). Da nicht in jeder Schicht die Einhaltung einer bestimmten Empfangsreihenfolge garantiert werden kann, müssen die einzelnen Untereinheiten mit einer eindeutigen **Identifikation**, z.B. einer Nummerierung, versehen werden, die es erlaubt, die Originalnachricht am Ende wieder zusammenzusetzen. Ein weiteres zu lösendes Problem besteht darin, zu verhindern, dass in einer Schicht ein besonders schneller Sender einen langsamen Empfänger mit Nachrichten überhäuft. Dazu kommen unterschiedliche Verfahren der **Flusssteuerung** zum Einsatz, die eine gleichmäßige Auslastung des Netzwerks gewährleisten sollen. Einzelne Verbindungen zwischen Sender und Empfänger können in darüber- oder darunterliegenden Schichten zusammengefasst bzw. wieder auseinanderdividiert werden. Dieses **Multiplexing** (bzw. Demultiplexing) muss in jeder Schicht transparent erfolgen, d.h. findet in einer tieferen Schicht ein Multiplexing statt, sollte die darüberliegende Schicht davon nicht beeinflusst werden. Existieren mehrere alternative Verbindungswege zwischen Sender und Empfänger in einem Netzwerk, müssen **Routing**-Entscheidungen getroffen werden, die festlegen, welche Teilstrecken jeweils in einem Netzwerk zur aktuellen Nachrichtenweiterleitung gewählt werden sollen.
Im Schichtenmodell sind die aufeinander aufbauenden Schichten durch einen nach oben hin zunehmenden Grad an Abstraktion gekennzeichnet. Während auf den Hardware-nahen Schichten Datenpakete übertragen werden, werden in den weiter oben im Protokollstapel angesiedelten Schichten Nachrichten verschickt, die von der Protokollsoftware auf den tiefer liegenden Schichten in Datenpakete zerlegt

(fragmentiert) werden. Die höher gelegenen Schichten verbergen diese Details der Kommunikation vor den Benutzern und stellen komfortable **Dienste** zur Kommunikation und Datenübertragung zur Verfügung. Grundsätzlich unterscheidet man bei diesen Diensten zwischen **verbindungslosen Diensten** (Connectionless Services) und **verbindungsorientierten Diensten** (Connection-Oriented Services). Verbindungslose Dienste arbeiten analog zum traditionellen Postsystem, d.h. jede Nachricht wird gleich einem Brief oder einem Paket mit einer vollständigen Empfängeradresse versehen und unabhängig von allen anderen Nachrichten durch das Netzwerk gesendet. Da verbindungslose Dienste keinen festen Wege durch das Netzwerk vorgegeben, kann die Reihenfolge der empfangenen Nachrichten-Pakete von der des Senders abweichen. Ein **zuverlässiger Dienst** (Reliable Service) bestätigt den erfolgreichen Versand einer Nachricht stets durch eine Empfangsbestätigung des Empfängers. Der Sender erlangt dadurch Gewissheit darüber, ob der Empfänger die versendete Nachricht tatsächlich erhalten hat. Bei einem **unzuverlässigen Dienst** (Non Reliable Service) ist das Senden von Empfangsbestätigungen nicht vorgesehen.

Ein **verbindungsorientierter Dienst** dagegen funktioniert ähnlich wie das Telefon, d.h. bevor Nachrichten übermittelt werden können, muss zunächst eine Verbindung zum Empfänger aufgebaut werden. Entlang dieser Verbindung werden dann alle Nachrichten versendet, bis die Verbindung von beiden Kommunikationspartnern wieder abgebaut wird. Zuverlässige verbindungsorientierte Dienste können Daten als **Nachrichtenfolgen** (Message Sequences) senden, wobei streng darauf geachtet wird, dass Nachrichtengrenzen beim Versand erhalten bleiben. Alternativ dazu können zuverlässige verbindungsorientierte Dienste Nachrichten auch als **Byteströme** (Byte Streams) versenden. Dabei werden Nachrichtengrenzen nicht beachtet. Eine weitere Variante sind unzuverlässige, aber verbindungsorientierte Dienste. Hier wird vor dem Datentransfer zwar eine Verbindung aufgebaut, Sender und Empfänger bestätigen aber nicht den Empfang erhaltener Nachrichten. Diese Variante wird z.B. bei der Übertragung von Audio- oder Videodaten gewählt, da hier Übertragungsverzögerungen, die durch ausbleibende Empfangsbestätigungen ausgelöst werden können, nicht akzeptabel sind. Auftretende Übertragungsfehler werden als Bildstörung oder Rauschen wahrgenommen und z.B. bei Live-Übertragungen eher toleriert als Verzögerungen.

Ein **verbindungsloser Dienst** wird als **Datagrammdienste** (Datagram Service) bezeichnet. Bei einer Analogie mit der traditionellen Post entspricht ein Datagrammdienst etwa einem Telegramm oder einer Postkarte, bei der der Sender keine Rückmeldung über einen erfolgreichen Empfang erhält. Beschränkt sich die (verbindungslose) Kommunikation zwischen Sender und Empfänger auf den Austausch einer einzelnen Nachricht (Datagramm), spricht man von einem **Anforderungs-/Antwortdienst** (Request-Reply Service).

Ein zuverlässiger, verbindungsloser Dienst ist von Vorteil (**zuverlässiger Datagrammdienst**), wenn etwa nur eine kurze Nachricht sicher versendet werden soll, ohne dass dazu eine explizite Verbindung aufgebaut werden soll. Diese Variante lässt sich mit einem Einschreibebrief mit Rückschein vergleichen, bei dem der Sender bei Erhalt der Empfangsbestätigung sicher sein kann, dass der Empfänger auch

tatsächlich den Brief erhalten hat. Tabelle 2.1 stellt die unterschiedlichen Dienstarten noch einmal in der Übersicht dar.

Tabelle 2.1 Dienstarten

	Dienst	Beispiel
verbindungs-orientiert	zuverlässiger Nachrichtenstrom	Folge von einzelnen Bildern
	zuverlässiger Bytestrom	Terminal Login
	unzuverlässige Verbindung	Videostream
verbindungslos	unzuverlässiges Datagramm	unbestätigte E-Mail Nachricht
	bestätigtes Datagramm	bestätigte E-Mail Nachricht
	Anforderung/Antwort	Client-/Server Handshake

Die Unterscheidung zwischen **Protokollen** und **Diensten** (Services) ist in diesem Zusammenhang von besonderer Bedeutung. Während Protokolle Regeln und Datenformate bestimmen, nach denen Daten innerhalb einer bestimmten Schicht ausgetauscht werden, bezeichnet der Dienst eine Sammlung von Operationen (Dienstprimitiven), die eine Schicht einer darüberliegenden Schicht zur Verfügung stellt (vgl. Abb. 2.5). Unter Dienstprimitiven versteht man einzelne Operationen, die eine bestimmte Aktion veranlassen oder über deren Status Bericht erstatten (vgl. Abb. 2.6). Die Spezifikation eines Dienstes fasst die im Dienst zusammengefassten **Dienstprimitive** zusammen. Dabei wird aber nicht spezifiziert, auf welche Weise dieser Dienst tatsächlich implementiert wird, sondern lediglich die Schnittstellenbeschreibung zwischen zwei benachbarten Schichten im Protokollstapel. Protokolle dagegen dienen zur Ausführung der in der jeweiligen Schicht zur Verfügung stehenden Dienste.

Dem vorgestellten Schichtenmodellfolgend haben sich zwei bedeutende **Referenzmodelle** entwickelt, das ISO/OSI-Referenzmodell und das TCP/IP-Referenzmodell. Als Referenzmodell wird dabei ein abstraktes Modell bezeichnet, auf dessen Grundlage konkrete Implementationen entworfen werden können. Mit den beiden genannten Referenzmodellen sind jeweils bestimmte Protokolle verknüpft, die auf den einzelnen Schichten des Modells angesiedelt sind, und die die in dieser Schicht definierten Dienste verfügbar machen. Das ISO/OSI-Modell und seine Protokolle wurden theoretisch konzipiert und hatten lediglich didaktisch klärende Bedeutung als anschauliches Modell, um die mit jeder Schicht verknüpften Aufgaben und Dienste aufzuzeigen. Das TCP/IP-Referenzmodell dagegen erwuchs aus der praktischen Entwicklung des Internets und seiner Protokolle in der Praxis.

Dienstprimitive zur Implementierung eines verbindungsorientierten Dienstes

Um einen verbindungsorientierten Dienst zu realisieren, müssen Dienstprimitive für die folgenden Operationen verfügbar sein:

- **Verbindungsaufbau**:
  Um eine Verbindung zu einem Kommunikationspartner (auf der gleichen Schicht im Protokollstapel) aufzubauen, wird eine Operation benötigt, die als Parameter die Adresse des Kommunikationspartners übernimmt und an diesen eine Anmeldung versendet (CONNECT).
- **Warten auf Verbindung**:
  Wenn ein Kommunikationspartner bereit ist, eine Verbindung mit einem anderen Kommunikationspartner aufzunehmen, wird er dazu in einen speziellen Zustand versetzt, in dem er auf einen Verbindungsaufbau wartet (LISTEN).
- **Senden von Nachrichten**:
  Ist eine Verbindung etabliert, kann der aktive Kommunikationspartner seinem Gegenüber eine Nachricht senden (SEND).
- **Empfangen von Nachrichten**:
  Ist eine Verbindung etabliert, begibt sich wechselweise einer der Kommunikationspartner in eine speziellen Zustand, in dem er auf eine Nachricht seines Gegenübers wartet (RECEIVE).
- **Verbindungsabbau**:
  Um zum Abschluss einer Kommunikation die Verbindung zu einem Kommunikationspartner aktiv zu beenden, wird eine entsprechende Operation benötigt (DISCONNECT).

Man unterscheidet den aktiven Kommunikationspartner, der einen Kommunikationsvorgang startet (Client) und den passiven Kommunikationspartner (Server), der darauf wartet, dass zu ihm eine Kommunikation aufgebaut wird, um z.B. Dienste oder Informationen abzufragen. Ein Server ist zunächst im LISTEN Zustand und wartet auf einen Verbindungsaufbau. Der Client startet seine Anfrage mit einem CONNECT zu einem bestimmten Server und wartet auf eine Antwort. Erhält der Server die Verbindungsanforderung, bestätigt er diese und führt RECEIVE aus, um auf gesendete Daten vom Client zu warten. Der Client führt nach Erhalt der Bestätigung des Verbindungsaufbaus SEND aus, um weitere Anforderungen nach Diensten oder Daten zu versenden, und führt als nächstes RECEIVE aus, um auf die Antwort des Servers zu warten. Auf diese Weise entspannt sich ein wechselseitig geführter Dialog zwischen Client und Server, der durch die Ausführung eines DISCONNECT von Client-Seite aktiv beendet wird. Der Server führt daraufhin ebenfalls DISCONNECT aus und begibt sich danach wieder in den Zustand LISTEN (siehe auch Abschnitt 8.1.4).

Abb. 2.6 Beispiel zur Anwendung von Dienstprimitiven

Exkurs 1: ISO/OSI-Referenzmodell

Für die Entwicklung von Netzwerkprotokoll-Familien wurde ab 1977 von der International Standards Organisation (ISO) das **ISO/OSI Referenzmodell** für die Kommunikation in offenen Netzwerken (Open Systems Interconnection) bereitgestellt. Es untergliedert den Gesamtprozess der Netzwerkkommunikation in sieben einzelne Schichten und ist konzipiert als gedankliches Werkzeug zur Entwicklung von Protokollfamilien (siehe Abb. 2.7).

Die vor der ISO/OSI-Initiative existierenden Netzwerkprotokolle waren überwiegend proprietärer Natur und von den einzelnen Netzwerk-Geräteherstellern selbst entwickelt worden. Zu diesen Prä-ISO/OSI-Netzwerk-Protokollstandards zählen z.B. IBM SNA, AppleTalk, No-

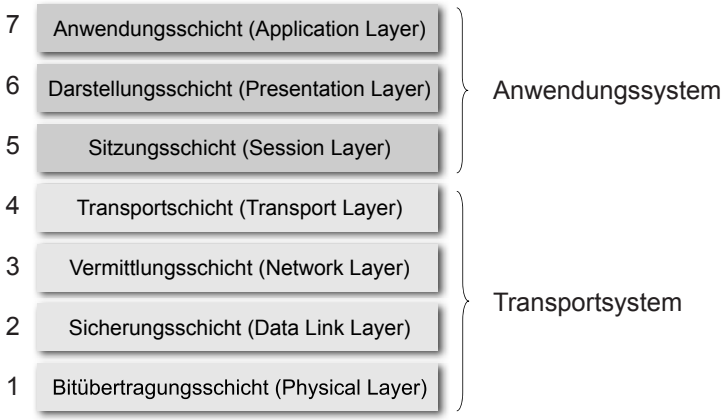


Abb. 2.7 Die einzelnen Schichten des ISO/OSI-Referenzmodells

vell Netware und DECnet, die alle untereinander nicht kompatibel sind. Während die Standardisierungsbemühungen um ISO/OSI noch liefen, gewann die dem Internet zugrunde liegende Protokollfamilie TCP/IP in heterogenen Netzwerken, die sich aus Komponenten unterschiedlicher Hersteller zusammensetzten, rasant an Bedeutung und setzte sich auf breiter Basis durch, noch bevor eine abschließende Standardisierung von ISO/OSI gelang.

Das ISO/OSI-Referenzmodell trägt den Namen **Open Systems Interconnection**, weil es zur Verbindung offener Systeme bestimmt war, d.h. Systeme, die für die Kommunikation mit anderen Systemen offen stehen. Als Grundgedanke beim Design des ISO/OSI-Referenzmodells sollte jede einzelne Schicht eine genau definierte Funktion implementieren und eine neue, höhere Schicht stets dann eingefügt werden, wenn ein neuer Abstraktionsgrad zur Erledigung der zu bewältigenden Aufgaben notwendig war. Das ISO/OSI-Modell selbst bietet keine Netzwerkarchitektur, es werden lediglich die Aufgaben der einzelnen Schichten festgelegt und keine Aussage über die zur Realisierung der dort definierten Funktionalität notwendigen Dienste und Protokolle getroffen.

Im ISO/OSI-Referenzmodell entspricht die unterste Schicht im Protokollstapel der eigentlichen Netzwerk-Hardware (physikalische Ebene). Die darauf aufbauenden Schichten umfassen jeweils Firmware und Software, die auf dieser Netzwerk-Hardware eingesetzt werden. Die oberste Schicht, Schicht sieben, ist schließlich die Anwendungsschicht, die eine Schnittstelle bereitstellt zwischen dem Kommunikationssystem und den verschiedenen Anwendungen, die das Kommunikationssystem für ihre Zwecke nutzen wollen. Die Schichten (1-4) werden allgemein als **Transportsystem**, die Schichten (5-7) als **Anwendungssystem** bezeichnet, die zunehmend allgemeinere Funktionalitäten des Kommunikationsprozesses bereitstellen. Obwohl sie denselben Namen tragen, dürfen sie nicht mit den eigentlichen Anwendungsprogrammen verwechselt werden, die selbst außerhalb des Schichtenmodells stehen.
Die einzelnen Schichten des ISO/OSI-Referenzmodells sind mit den folgenden Aufgaben befasst:

- **Schicht 1: Bitübertragungsschicht (Physical Layer)**
  Die Bitübertragungsschicht definiert physikalische und technische Eigenschaften des Übertragungsmediums (Übertragungskanals). Speziell werden darin die Beziehungen zwischen der Netzwerk-Hardware und dem physikalischen Übertragungsmedium geregelt, wie z.B. Layout und Belegung von Steckverbindungen mit ihren optisch oder elektri-

schen Parametern, Kabelspezifikationen, Verstärkerelemente, Netzwerkadapter, verwendete Übertragungsverfahren usw.

Zu den wichtigsten Aufgaben der Bitübertragungsschicht zählen:

- Aufbau und Beendigung einer Verbindung zu einem Übertragungsmedium und
- Modulation, d.h. Konvertierung binärer Daten (Bitstrom) in (elektrische, optische oder Funk-) Signale, die über einen Kommunikationskanal übertragen werden können.

Wichtige Protokollstandards dieser Schicht sind z.B.

- ITU-T V.24, V.34, V.35
- ITU-T X.21 und X.21bis
- T1, E1
- SONET, SDH (Synchronous Digital Hierarchy), DSL (Digital Subscriber Line)
- EIA/TIA RS-232-C
- IEEE 802.11 PHY

- **Schicht 2: Sicherungsschicht (Data Link Layer)**
  Im Gegensatz zur Bitübertragungsschicht, deren Hauptanliegen in der Regelung der Kommunikation zwischen einer einzelnen Netzwerkkomponente und dem Übertragungsmedium besteht, befasst sich die Sicherungsschicht mit der Interaktion mehrerer (d.h. mindestens zwei) Netzwerkkomponenten. Die Sicherungsschicht gewährleistet, dass entlang einer Punkt-zu-Punkt Verbindung trotz gelegentlicher Fehler, die in der Bitübertragungsschicht auftreten können, eine zuverlässige Übertragung stattfinden kann. Diese Punkt-zu-Punkt Verbindung kann dabei entweder als direkte Verbindung ausgeführt sein oder auch über ein im Broadcastverfahren arbeitendes **Diffussionsnetzwerk** realisiert werden, wie z.B. bei Ethernet oder WLAN. In einem Diffusionsnetzwerk können alle angeschlossenen Rechner die übertragenen Daten aller anderen angeschlossenen Rechner empfangen, ohne dass dazu irgendwelche Zwischensysteme nötig wären.

  Zu den auf der Sicherungsschicht zu bewältigenden Aufgaben zählen

  - die Organisation von Daten in logische Einheiten, die auf der Sicherungsschicht als **Rahmen** (Frames) bezeichnet werden,
  - die Übertragung von Rahmen zwischen Netzwerkkomponenten,
  - das Bitstopfen, d.h. das Ergänzen nicht vollständig gefüllter Rahmen mit speziellen Fülldaten und
  - die zuverlässige Übertragung von Rahmen durch einfache Fehlererkennungsverfahren, wie z.B. die Prüfsummenberechnung.

  Zu den bekannten Protokollstandards dieser Schicht zählen:

  - BSC (Bit Synchronous Communication) und DDCMP (Digital Data Communications Message Protocol), PPP (Point-to-Point Protocol)
  - IEEE 802.3 (Ethernet)
  - HDLC (High Level Data Link Control)
  - X.25 LAPB (Link Access Procedure for Balanced Mode) und LAPD (Link Access Procedure for D-Channels)
  - IEEE 802.11 MAC (Medium Access Control)/LLC (Logical Link Control)
  - ATM (Asynchronous Transfer Mode), FDDI (Fiber Distributed Data Interface), Frame Relay

- **Schicht 3: Vermittlungsschicht (Network Layer)**
  Die Vermittlungsschicht stellt funktionale und prozedurale Mittel zur Verfügung, die den Transfer von Datensequenzen variabler Länge (**Datenpakete**) von einem Sender zu einem Empfänger über ein oder mehrere Netzwerke hinweg ermöglichen.

  Zu den Aufgaben der Vermittlungsschicht zählen:

  – die Zuweisung von Adressen zu End- und Zwischensystemen,
  – die zielgerichtete Weiterleitung von Datenpaketen von einem Ende des Netzwerks zum anderen (**Routing**) und damit
  – die Verknüpfung einzelner Netzwerke (**Internetworking**),
  – die Fragmentierung und Reassemblierung von Datenpaketen, da unterschiedliche Netzwerke von unterschiedlichen Transportparameter bestimmt werden, und
  – die Weiterleitung von Fehler- und Statusmeldungen bzgl. erfolgter Zustellung von Datenpaketen.

  Zu den wichtigsten Protokollstandards, die auf dieser Schicht angesiedelt sind, zählen:

  – ITU-T X.25 PLP (Packet Layer Protocol)
  – ISO/IEC 8208, ISO/IEC 8878
  – Novell IPX (Internetwork Packet Exchange)
  – IP (Internet Protocol)

- **Schicht 4: Transportschicht (Transport Layer)**
  Die Transportschicht ermöglicht einen transparenten Datentransfer zwischen Endanwendern und stellt den darüberliegenden Schichten einen zuverlässigen Transportdienst zur Verfügung. Die Transportschicht definiert dabei die Einzelheiten, die für eine zuverlässige und sichere Datenübertragung notwendig sind. Hier wird sichergestellt, dass eine Folge von Datenpaketen fehlerfrei, vollständig und in der richtigen Reihenfolge vom Sender zum Empfänger gelangt. Auf der Transportschicht erfolgt ebenfalls die Abbildung von Netzwerkadressen auf logische Namen. Damit stellt die Transportschicht den beteiligten Endsystemen eine Ende-zu-Ende Verbindung zur Verfügung, die die Einzelheiten der dazwischenliegenden Netzwerkinfrastruktur verbirgt und daher als **transparent** bezeichnet wird. Die Protokolle auf dieser Schichte zählen zu den komplexesten Protokollen in der Netzwerk-Kommunikation.

  Zu den bedeutendsten Protokollstandards auf Schicht 4 gehören:

  – ISO/IEC 8072 (Transport Service Definition)
  – ISO/IEC 8073 (Connection Oriented Transport Protocol)
  – ITU-T T.80 (Network-Independent Basic Transport Service for Telematic Services)
  – TCP (Transmission Control Protocol), UDP (User Datagram Protocol), RTP (Real-time Transport Protocol)

- **Schicht 5: Sitzungsschicht (Session Layer)**
  Die Sitzungsschicht wird auch als Kommunikationssteuerungsschicht bezeichnet und steuert den Dialog zwischen zwei über das Netzwerk verbundenen Rechnern.

  Zu den Hauptaufgaben der Sitzungsschicht zählen:

  – Einrichtung, Management und Beendigung von Verbindungen zwischen lokalen und entfernten Anwendungen,
  – Steuerung von Voll-Duplex-, Halb-Duplex- oder Simplex-Datentransport, und
  – Einrichtung von Sicherheitsmechanismen, wie z.B. Authentifikation über Passwort-Verfahren.

Wichtige Protokollstandards dieser Schicht sind:

- SAP (Session Anouncement Protocol), SIP (Session Initiation Protocol)
- NetBIOS (Network Basic Input/Output System)
- ISO 8326 (Basic Connection Oriented Session Service Definition)
- ISO 8327 (Basic Connection Oriented Session Protocol Definition)
- ITU-T T.62 (Control Procedures for Teletex and Group 4 Facsimile Services)

- **Schicht 6: Darstellungsschicht (Presentation Layer)**
  Die Darstellungsschicht stellt einen Kontext zwischen zwei Entitäten (Anwendungen) der darüberliegenden Anwendungsschicht her, so dass die beiden Anwendungen unterschiedliche Syntax (z.B. Datenformate und Kodierungen) und Semantik verwenden können. Die Darstellungsschicht sorgt also für eine korrekte Interpretation der übertragenen Daten. Dazu wird die jeweils lokale Kodierung der Daten in eine spezielle, einheitliche Transferkodierung für die Darstellungsschicht umgesetzt und beim Empfänger in die dort lokal gültige Kodierung zurückverwandelt. Zusätzlich zählen Datenkomprimierung und Verschlüsselung zu den Aufgaben dieser Schicht.

  Zu den wichtigsten Protokollstandards der Darstellungsschicht zählen:

  - ISO 8322 (Connection Oriented Session Service Definition)
  - ISO 8323 (Connection Oriented Session Protocol Definition)
  - ITU-T T.73 (Document Interchange Protocol for Telematic Services), ITU-T X.409 (Presentation Syntax and Notation)
  - MIME (Multipurpose Internet Mail Extensions), XDR (External Data Representation)
  - SSL (Secure Socket Layer), TLS (Transport Layer Security)

- **Schicht 7: Anwendungsschicht (Application Layer)**
  Die Anwendungsschicht bietet eine Schnittstelle für Anwendungsprogramme, die das Netzwerk für ihre Zwecke nutzen wollen. Anwendungsprogramme selbst gehören nicht in diese Schicht, sondern nutzen lediglich deren Dienste. Die Anwendungsschicht stellt einfach handhabbare Dienstprimitive zur Verfügung, die sämtliche netzwerkinternen Details vor dem Anwender oder dem Programmierer des Anwendungsprogrammes verbergen und so eine einfache Nutzung des Kommunikationssystems ermöglichen. Zu den wichtigsten Funktionen der Anwendungsschicht zählen unter anderem:

  - Identifikation der Kommunikationspartner,
  - Feststellung der Verfügbarkeit von Ressourcen und
  - Synchronisation der Kommunikation.

  Zu den wichtigen Protokollstandards, die auf dieser Schicht angesiedelt sind, gehören:

  - ISO 8571 (FTAM, File Transfer, Access and Management)
  - ISO 8831 (JTM, Job Transfer and Manipulation)
  - ISO 9040 und 9041 (VT, Virtual Terminal Protocol)
  - ISO 10021 (MOTIS, Message Oriented Text Interchange System)
  - FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (Hypertext Transfer Protocol), etc.
  - ITU-T X.400 (Data Communication for Message Handling Systems). ITU-T X.500 (Electronic Directory Services)

Seit der Entwicklung des ISO/OSI-Referenzmodells haben sich die Konzepte für Protokollfamilien an verschiedenen Stellen zwar geändert und viele der neu entwickelten Protokolle passen gar nicht mehr genau in dieses Schema, ein Großteil der Terminologie, insbesondere Bezeichnung und Nummerierung der einzelnen Schichten, hat sich aber bis heute erhalten.

Weiterführende Literatur:

U. Black: OSI – A Model for Computer Communications Standards, Upper Saddle River, NJ, USA (1991)

H. Zimmermann: OSI Reference Model – The ISO Model of Architecture for Open Systems Interconnection, in IEEE Transactions on Communications, vol. 28, no. 4, pp. 425–432 (1980)

2.2 Die physikalische Schicht als Basis der Rechnerkommunikation

Die Protokolle in der untersten Schicht des TCP/IP-Referenzmodells (der Netzzugangsschicht) setzen auf dem physikalischen Übertragungsmedium (Übertragungskanal) auf. Dieses Übertragungsmedium wird auch als **physikalische Schicht** (Physical Layer) bezeichnet, üblicherweise aber nicht zum Protokollstapel des TCP/IP-Referenzmodells gezählt (vgl. Abb. 2.10). Die physikalische Schicht zusammen mit den vier Schichten des TCP/IP-Referenzmodells bildet deshalb das sogenannte hybride TCP/IP-Referenzmodell. Im ISO/OSI-Referenzmodell dagegen ist die physikalische Schicht unter dem Namen „Bitübertragungsschicht“ als eine eigene Schicht vorgesehen.

2.2.1 Physikalische Übertragungsmedien

Allgemein definiert die physikalische Schicht die physikalischen und technischen Eigenschaften eines zur Datenübertragung genutzten physikalischen bzw. analogen Übertragungsmediums. Speziell werden dabei die Beziehungen zwischen der Netzwerk-Hardware und dem physikalischen Übertragungsmedium geregelt, wie z.B. Layout und Belegung von Steckverbindungen mit ihren optisch/elektrischen Parametern, Kabelspezifikationen, Verstärkerelementen, Netzwerkadaptern, verwendete Übertragungsverfahren usw. Die eigentliche Aufgabe der physikalischen Schicht besteht darin, eine Folge von Bits (Bit Stream) in eine Folge von physikalischen Signalen zu übersetzen, die über das Übertragungsmedium vom Sender zum Empfänger übermittelt werden.

Je nach Beschaffenheit des Übertragungsmediums unterscheidet man unterschiedliche Methoden und Verfahren, wie Informationen, also Bitfolgen, sicher und zuverlässig in physikalische Signale umgewandelt werden können, um diese über das

Übertragungsmedium zu senden und auf Empfängerseite wieder korrekt zur Ausgangsinformation zusammenzusetzen. Dieser Vorgang wird als **Modulation** und in umgekehrter Richtung als **Demodulation** bezeichnet.
Medien zur Datenübertragung lassen sich prinzipiell in **kabelgebundene** (geführte) Übertragungsmedien und **kabelungebundene** (ungeführte) Übertragungsmedien aufteilen. Bei den kabelgebundenen (geführten) Übertragungsmedien werden elektromagnetische Wellen entlang einem festen Medium weitergeleitet. Zu diesen zählen verschiedene Varianten von Kupferkabeln, wie z.B. verdrillte Kabelpaare (Twisted Pair) oder Koaxialkabel (Drahtweg, Stromleiter), oder verschiedene Glasfaserkabelvarianten (Fiber Optics) (Lichtweg, Wellenleiter). Kabelgebundene Übertragungsmedien bieten eine hohe Datensicherheit und schnelle Übertragungsgeschwindigkeiten. Um zu einem Netzwerk auf Basis kabelgebundener Übertragungsmedien Zugang zu erlangen, muss zuerst ein direkter, physikalischer Kontakt hergestellt werden. Die hohe Übertragungsgeschwindigkeit resultiert aus den niedrigen Fehlerrate, die dank guter Abschirmungsmöglichkeiten erreicht werden können. Allerdings sind kabelgebundene Netzwerkarchitekturen mit erheblichen Kosten verbunden, da Kabel bezahlt und verlegt werden müssen.

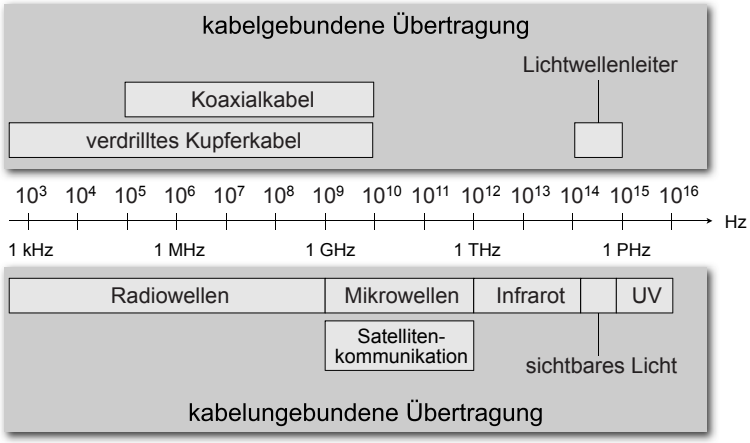


Abb. 2.8 Kabelgebundene und -ungebundene Übertragungsmedien im elektromagnetischen Spektrum

Bei den kabelungebundenen (ungeführten) Übertragungsmedien werden die elektromagnetischen Wellen über unterschiedliche Frequenzbereiche des elektromagnetischen Spektrums hinweg im Raum übertragen. Dazu zählen die Funkübertragung via Kurzwelle oder Ultrakurzwelle, Mikrowellenübertragung, Infrarot oder Laserlicht. Man unterscheidet zwischen gerichteter Übertragung, wie z.B. bei einer Laser-Strecke, Richtfunk oder Satelliten-Direktfunk, und ungerichteter (isotroper) Übertragung, wie z.B. bei Mobilfunk, terrestrischem Rundfunk oder Satelliten-

Rundfunk. Gegenüber kabelgebundenen Übertragungsmedien ist eine leiterlose Netzwerkarchitektur flexibel und für den mobilen Einsatz ideal geeignet. Kosten für eine aufwändige Verkabelung fallen nicht an. Andererseits aber ist kein direkter, physikalischer Kontakt nötig, um in ein kabelungebundenes Netzwerk einzudringen. Daher sind hier aufwändige softwaretechnische Absicherungsmaßnahmen, wie z.B. verschlüsselte Datenübertragung notwendig. Auch liefern kabelungebundene Übertragungsmedien nur eine geringere Übertragungsgeschwindigkeit, da Reflexionen an Gegenständen oder atmosphärische Störungen die Signalübertragung beeinträchtigen.

2.2.2 Charakterische Eigenschaften physikalischer Übertragungsmedien

Alle physikalischen Übertragungsmedien sind jeweils bestimmten Begrenzungen unterworfen. Dies betrifft die maximal pro Zeiteinheit transportierte Information (Bandbreite) oder die Geschwindigkeit, mit der sich ein Signal auf einem Übertragungsmedium ausbreiten kann. Generell unterliegt jedes Signal, das sich entlang eines physikalischen Übertragungsmediums ausbreitet, einer Signaldämpfung, d.h. mit steigender Entfernung vom ausgehenden Sender schwächt sich das Signal zunehmend ab. Im Gegensatz zu einem idealen Übertragungsmedium sind reale Übertragungsmedien stets Störungen (Rauschen) ausgesetzt. Schwächt die Signaldämpfung das Signal so stark ab, dass dieses nicht mehr vom Rauschen zu unterscheiden ist, lässt sich das Signal auf Empfängerseite nicht mehr rekonstruieren und korrekt interpretieren. Daher muss ein Signal entlang eines Übertragungsmediums stellenweise wieder aufgefrischt, d.h. verstärkt werden, um es sicher und möglichst unverfälscht empfangen zu können.
Abhängig von den physikalischen Eigenschaften des Übertragungsmediums kommen unterschiedliche Modulationsverfahren zum Einsatz, um eine möglichst effiziente Kodierung und Übertragung der binären (digitalen) Information über ein physikalisches (analoges) Medium zu gewährleisten. Die unterschiedlichen physikalischen Übertragungsmedien, ihre Beschränkungen und charakteristischen Eigenschaften, sowie ihr Einsatz im Internet werden detailliert in Kap. 3 besprochen.

2.3 Das TCP/IP-Referenzmodell

Die komplexen Aufgaben, die mit der Rechnerkommunikation im Internet verbunden sind, werden mit Hilfe unterschiedlicher Protokolle geregelt, die hierarchisch ineinandergreifen und deren Funktionalität sich, wie im vorangegangenen Kapitel dargestellt, am besten mit Hilfe eines **Schichtenmodells** darstellen lässt.
In jeder einzelnen Schicht ist eine Reihe von Aufgaben definiert, die von den dieser Schicht zugeordneten Protokollen erledigt werden muss. Dabei müssen die

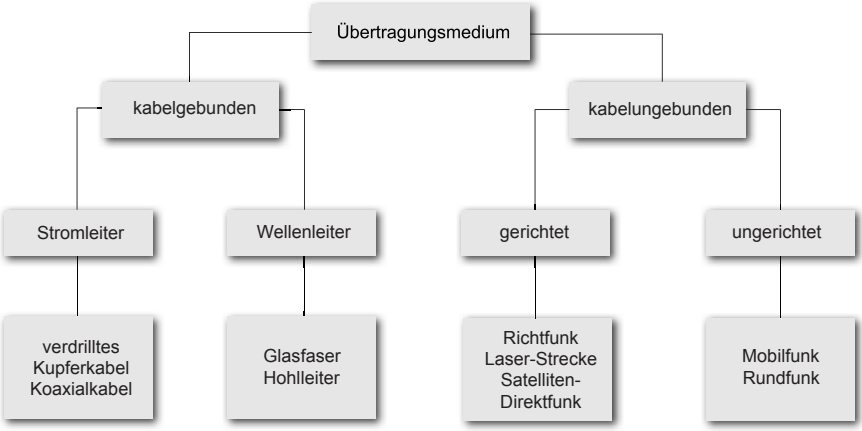


Abb. 2.9 Klassifikation der physikalischen Übertragungsmedien

Protokolle die jeweiligen Schnittstellen zu den unmittelbar benachbarten Schichten oberhalb und unterhalb der eigenen Schicht berücksichtigen. Die Schnittstellen zu den auf dem selben Netzwerkendgerät benachbarten Schichten werden als **Dienst-Interface** bezeichnet. Ein Protokoll stellt dabei über das Dienst-Interface einer höher im Protokollstapel befindlichen Schicht einen bestimmten Dienst zur Verfügung und kann bei der Erledigung seiner Aufgaben auf die Dienste der tiefer gelegenen Schichten zurückgreifen. Zusätzlich definiert ein Protokoll eine weitere Schnittstelle zu seinem Gegenstück auf einem entfernten Netzwerkendgerät, in der Form und Bedeutung von Nachrichten definiert werden, die zwischen den Netzwerkendgeräten ausgetauscht werden. Diese Schnittstelle wird daher auch als **Partner-Interface** bezeichnet. Während die tatsächliche Kommunikation innerhalb des Schichtenmodells über Dienst-Interfaces in vertikaler Richtung zwischen den benachbarten Schichten erfolgt und der eigentliche Datenaustausch lediglich auf der untersten Ebene, der physikalischen Schicht, abläuft, besteht zwischen den Schichten der gleichen Ebene auf den unterschiedlichen Netzwerkendgeräten über das Partner-Interface eine scheinbare, virtuelle Verbindung, über die die Daten und Steuerinformationen ausgetauscht werden, die jeweils diese Protokollschicht betreffen.

Bei der Entwicklung des Internets stand der Gedanke im Vordergrund, eine nahtlose Kommunikation über eine Vielzahl unterschiedlicher Netzwerkarchitekturen hinweg zu ermöglichen. Ausgehend von den beiden primären Protokollen des Internets, dem **Internet Protocol** (**IP**) und dem **Transmission Control Protocol** (**TCP**) wurde die darauf aufbauende Architektur schließlich als TCP-IP-Referenzmodell bezeichnet. Das eigentliche **TCP/IP-Referenzmodell** umfasst vier Schichten (Schicht 2–5). Zusammen mit einer zusätzlichen Netzwerk-Hardwareschicht (Schicht 1) entsteht ein aus fünf Schichten bestehendes hybrides TCP/IP-Referenzmodell (vgl. Abb. 2.10).

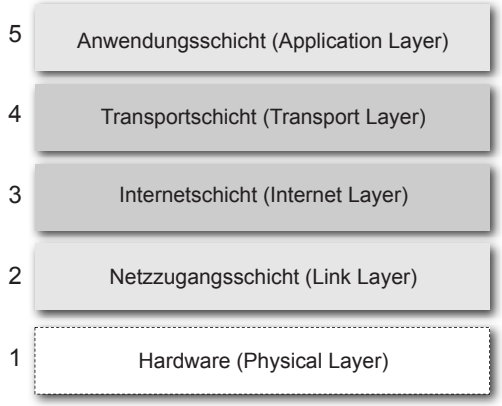


Abb. 2.10 Das TCP/IP-Referenzmodell umfasst vier Schichten (2-5), zusammen mit der Netzhardwareschicht (1) wird das Modell auch als hybrides TCP/IP-Referenzmodell bezeichnet

Die **Netzzugangsschicht** (Link Layer) des TCP/IP-Referenzmodells entspricht den ersten beiden Schichten des ISO/OSI-Referenzmodells (Bitübertragungsschicht und Sicherungsschicht). Ihre Hauptaufgabe besteht in der sicheren Übertragung von in Datenpaketen zusammengefassten Bitfolgen. Ihr folgt die **Internetschicht** (Internet Layer), die der Vermittlungsschicht des ISO/OSI-Referenzmodells entspricht, und deren Hauptaufgabe darin besteht, zwei an beliebigen Stellen im heterogenen Kommunikationsnetzwerk befindlichen Endsystemen die Datenkommunikation zu ermöglichen. Die darüberliegende **Transportschicht** (Transport Layer) entspricht der gleichnamigen Schicht des ISO/OSI-Referenzmodells. Sie ermöglicht es, zwei Anwendungsprogrammen auf unterschiedlichen Rechnern des Kommunikationsnetzwerks zuverlässig und verbindungsorientiert Daten auszutauschen. Die **Anwendungsschicht** (Application Layer) des TCP/IP-Referenzmodells schließlich fasst die drei obersten Schichten des ISO/OSI-Referenzmodells zusammen und dient als Schnittstelle zu den eigentlichen Anwendungsprogrammen, die über das Netzwerk miteinander kommunizieren wollen.

Das **TCP/IP-Referenzmodell** steht im deutlichen Gegensatz zum ISO/OSI-Referenzmodell. Anders als das ISO/OSI-Referenzmodell wurde es nicht theoretisch konzipiert und geplant entworfen, sondern leitete sich aus den in der Praxis des Internet eingesetzten Protokollen ab. Das ISO/OSI-Protokoll dagegen wurde theoretisch geplant und verabschiedet, bevor die Protokolle entworfen wurden, die die verschiedenen Funktionen der Schichten des ISO/OSI-Referenzmodells implementieren. Praktisch werden diese Protokolle heute aber nicht mehr verwendet, während die aus der Praxis erwachsenen Protokolle des TCP/IP-Referenzmodells heute das Internetd ominieren.

Im folgenden werden wir das dem Internet zugrunde liegende TCP/IP-Referenzmodell näher beleuchten. Nach einem kurzen Ausflug in die historische Entwicklung werden Gemeinsamkeiten und Unterschiede zwischen TCP/IP-Referenzmodell und

ISO/OSI-Referenzmodell diskutiert. Anschließend werden die einzelnen Schichten des TCP/IP-Referenzmodells detailliert vorgestellt.

2.3.1 Historisches und Abgrenzung zum ISO/OSI-Referenzmodell

Das Internet und sein Vorgänger, das ARPANET, entstand ab 1969 als reines Forschungsnetzwerk, das zu Beginn lediglich vier, wenig später aber bereits mehrere hundert Rechner aus Universitäten, Forschungsinstituten und militärischen Einrichtungen über zunächst angemietete Telefonleitungen miteinander verband. Als aber technologisch unterschiedliche Netzwerke, wie z.B. Satellitennetzwerke und Funknetzwerke mit dem Internet verbunden werden sollten, waren die ursprünglich eingesetzten Netzwerkprotokolle schnell mit der notwendigen Übersetzung des Datenverkehrs von einem Netzwerk in das andere überfordert.
Als *Robert E. Kahn* (*1938) 1972 im DARPA Information Processing Technology Office (IPTO), das zu dieser Zeit für die Weiterentwicklung des Internet verantwortlich war, seine Arbeit an der Datenübertragung in Satellitennetzwerken und Funknetzwerken aufnahm, wurde ihm schnell bewusst, dass es vorteilhaft wäre, den Datenverkehr auch über unterschiedliche Netzwerktechnologien hinweg zu ermöglichen. Daher musste ein neues, flexibles Netzwerkparadigma entwickelt werden, bei dem die Vernetzung heterogener Netzwerke unterschiedlichster Technologie von Anfang an im Mittelpunkt stand. 1973 stieß *Vinton Cerf* (*1943) zu Kahns Team, der das zu dieser Zeit noch im ARPANET als Netzwerkprotokoll eingesetzte **Network Control Program** (NCP) mitentwickelt hatte, um zusammen mit Kahn an Protokollen für eine offenen Netzwerkarchitektur zu arbeiten.
Im Sommer 1973 stellten Kahn und Cerf eine fundamental erneuerte Netzwerkarchitektur vor, deren Hauptmerkmal darin bestand, die unterschiedlichen Netzwerktechnologien über ein gemeinsames, über den jeweiligen Protokollen der eigentlichen Netzwerktechnologien agierendes „Internetworking Protokoll“ virtuell zu einem Netzwerk zu vereinen. Im Gegensatz zum bestehenden ARPANET, in dem das Netzwerk selbst für den zuverlässigen Datentransport zuständig war, sollten von jetzt an die mit dem Netzwerk verbundenen Endgeräte (Hosts) für die zuverlässige Datenübertragung verantwortlich sein. Die Funktionalität des Netzwerks selbst beschränkte sich von diesem Zeitpunkt an nur noch auf einen möglichst einfachen Transport von Datenpaketen. Durch diesen Kunstgriff gelang es Kahn und Cerf auch die unterschiedlichsten Netzwerktechnologien miteinander zu verbinden. Die Verbindung der verschiedenen Netzwerke sollte über spezielle Rechner erfolgen, den sogenannten **Paketvermittlern** (Router), die ausschließlich für die Weiterleitung von Datenpaketen zwischen unterschiedlichen Netzwerken zuständig sind.
Bis 1974 arbeitete Cerfs eigene Forschungsgruppe an der Stanford University an der ersten Spezifikation des **Transmission Control Protocol** (TCP, RFC 675). Dabei wurden sie stark von der Netzwerk-Forschungsgruppe des Xerox PARC (Palo Alto Research Center) beeinflusst, die an der PARC Universal Packet Protocol Suite (PARC UPPS) arbeitete. Mit der technischen Umsetzung beauftragte die

DARPA die Firma BN Technologies, die Stanford University und das University College London, die den neuen Protokollstandard auf unterschiedlichen Hardware-Plattformen implementieren sollten. Nach den Versionen TCP v1 und TCP v2 wurde das Protokoll in TCP v3 und IPv3 aufgespalten und getrennt weiterentwickelt. Die resultierende Netzwerkarchitektur wurde später nach diesen beiden wichtigsten Protokollen, TCP und IP (Internet Protocol), als TCP/IP-Referenzmodell (RFC 1122) bekannt und mündete 1978 in der Entwicklung einer operationellen Version **TCP/IP v4** (Version 4), die auch heute noch im Internet eingesetzt wird. Dabei konnte bereits 1975 der Nachweis der Einsatzbereitschaft von TCP/IP erbracht werden, als zwei unterschiedliche Netzwerke zwischen der Stanford University und dem University College London via TCP/IP miteinander verknüpft wurden. 1977 erfolgte ein Test mit drei unterschiedlichen Netzwerkarchitekturen zwischen den USA, Großbritannien und Norwegen.

Der endgültige Umstieg des vollständigen Internets auf TCP/IP v4 wurde zum 1. Januar 1983 vollzogen. Robert E. Kahn und Vinton Cerf erhielten 2004 für ihre Leistungen den Turing Award, die höchste Auszeichnung in der Informatik. 2005 wurden beide mit dem höchsten zivilen Orden der USA, der Presidential Medal of Freedom ausgezeichnet. Im Rahmen des 2. Deutschen IPv6 Gipfels 2009 am Hasso-Plattner-Institut in Potsdam wurde Robert E. Kahn zum HPI-Fellow ernannt, eine Ehrung, die er mit der Bundeskanzlerin Frau Dr. Angela Merkel und seit 2011 auch mit seinem ehemaligen Kollegen Vinton Cerf teilt.

Sowohl das ARPANET als auch das Internet existierten bereits, als die ISO die Entwicklung und Standardisierung des ISO/OSI-Referenzmodells in Angriff nahm, so dass sich das im Internet manifestierende TCP/IP-Referenzmodell einen entscheidenden Einfluss auf die Entwicklung des ISO/OSI-Rererenzmodells hatte. Die sieben Schichten des ISO/OSI-Referenzmodells lassen sich auf die Protokollarchitektur des Internets übertragen, wobei das TCP/IP-Referenzmodell lediglich vier Schichten (bzw. fünf Schichten als hybrides TCP/IP-Referenzmodell, wenn man die physikalische Schicht hinzunimmt) umfasst. In den einzelnen Schichten des TCP/IP-Referenzmodells werden Einsatzmöglichkeiten und Anwendungsbereiche (Netzzugang, Internet, Transport, Anwendung) beschrieben, während im ISO/OSI-Referenzmodell konkrete Vorschriften angegeben werden für Betriebsabläufe, Semantik der Daten und Netzwerktechnologien. Das TCP/IP-Referenzmodell beinhaltet keine konkreten Hardware-Spezifikationen und standardisiert nicht die physikalische Datenübertragung an sich, sondern bindet diese Aspekte an die Implementationen der einzelnen Schichten.

Die heute bedeutendste Protokollfamilie, die TCP/IP-Protokollsuite, basiert nicht auf den Spezifikationen eines Standardisierungskommitees, sondern erwuchs von Anfang an aus den Anforderungen und Erfahrungen der Entwicklung des Internets. Zwar lässt sich das ISO/OSI-Referenzmodell soweit anpassen, dass es auch zur Beschreibung des TCP/IP Protokollstapels dienen kann, aber beide gehen von gänzlich verschiedenen Grundlagen aus. Das **TCP/IP-Referenzmodell** wurde tatsächlich erst dann vollständig ausdefiniert, nachdem die in ihm beschriebenen Protokolle implementiert waren und sich erfolgreich im Einsatz befanden. Dies hatte zwar den Vorteil, dass die beschriebenen Schichtenspezifikationen perfekt mit den

Protokollimplementationen übereinstimmten, eine Anwendung dieses Modells auf andere Protokollfamilien war damit aber nicht ohne weiteres möglich. Die erste Beschreibung des TCP/IP-Referenzmodells (RFC 1122) stammt bereits aus dem Jahr 1974, also noch bevor die erste Spezifikation des ISO/OSI-Modells erfolgte.
Prinzipiell lässt sich die TCP/IP-Protokollfamilie in vier einzelne Schichten unterteilen, die um die Kernschichten TCP und IP herum organisiert sind (vgl. Abb. 2.10). Tatsächlich finden sich in der Literatur auch Beschreibungen des TCP/IP-Referenzmodells, die fünf verschiedene Schichten umfassen. Dabei wurde eine die Kommunikationshardware beschreibende Schicht (physikalische Schicht, Hardware, Physical Layer) mit in das ursprünglich vier Schichten umfassende TCP/IP-Referenzmodel aufgenommen. Dieses fünfschichtige Modell wird auch oft als **hybrides TCP/IP-Referenzmodell** bezeichnet. Die Bezeichnungen der einzelnen Schichten entsprechen denen des zugrunde liegenden RFC 1122 und werden im vorliegenden Buch durchgängig verwendet.
Die vier Schichten des TCP/IP-Referenzmodells lassen sich in folgender Weise mit den sieben Schichten des ISO/OSI-Referenzmodells vergleichen (siehe auch Abb. 2.11):

- Schicht 2 des TCP/IP-Referenzmodells (Netzzugangsschicht, Link Layer) wird in der Literatur auch oft als Data Link Layer, Network Access Layer oder Host-to-Network Layer bezeichnet und entspricht den ersten beiden Schichten des ISO/OSI-Referenzmodells (Bitübertragungsschicht und Sicherungsschicht).
- Schicht 3 des TCP/IP-Referenzmodells (Internetschicht, Internet Layer) wird auch als Netzwerkschicht, Network Layer oder Internetwork Layer bezeichnet und entspricht der Schicht 3 des ISO/OSI-Referenzmodells (Vermittlungsschicht).
- Schicht 4 des TCP/IP-Referenzmodells (Transportschicht, Transport Layer) wird auch als Host-to-Host Layer bezeichnet und entspricht der Schicht 4 des ISO/OSI-Referenzmodells (Transportschicht).
- Schicht 5 des TCP/IP-Referenzmodells (Anwendungsschicht, Application Layer) entspricht den Schichten 5 – 7 des ISO/OSI-Referenzmodells (Sitzungsschicht, Präsentationsschicht, Anwendungsschicht).

In den folgenden Abschnitten werden die Aufgaben und Protokolle der einzelnen Schichten des TCP/IP-Referenzmodells vorgestellt

2.3.2 Netzzugangsschicht

In der Netzzugangsschicht (Link Layer) des TCP/IP-Referenzmodells werden die ersten beiden Schichten des ISO/ISO-Referenzmodells, die Schichten 1 (Bitübertragungsschicht) und 2 (Sicherungsschicht) zusammengefasst, wobei die Netzzugangsschicht nicht die Aspekte der physikalischen Schicht beinhaltet, die Teil des ISO/OSI-Referenzmodells sind. Die Netzzugangsschicht ist damit die unterste

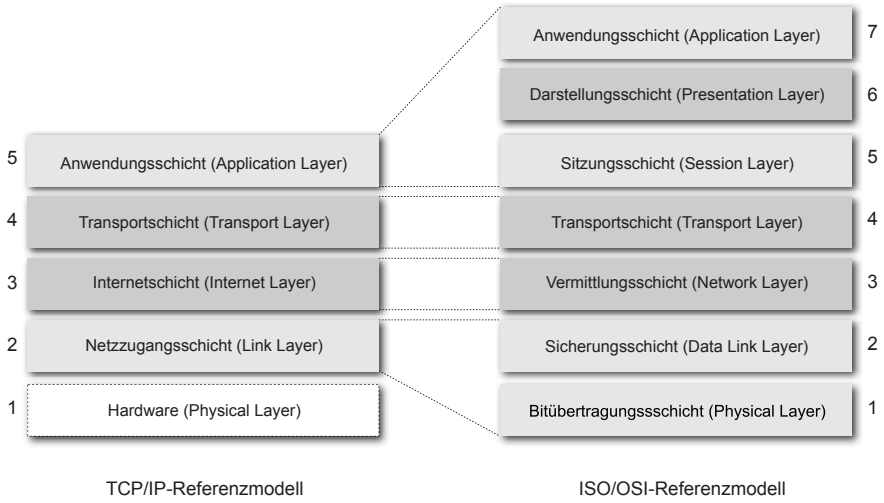


Abb. 2.11 Gegenüberstellung des TCP/IP-Referenzmodells und des ISO/OSI-Referenzmodells

Schicht des TCP/IP-Referenzmodells. Die Hauptaufgabe der Netzzugangsschicht besteht in der sicheren Übertragung von einzelnen Datenpaketen zwischen zwei benachbarten Endsystemen. Zu übertragende Bitfolgen werden zu festen Einheiten (Datenpaketen) zusammengefasst und mit den zur Übertragung notwendigen Zusatzinformationen versehen, wie z.B. Prüfsummen zur einfachen Fehlererkennung. Die benachbarten Endsysteme können entweder direkt durch ein Übertragungsmedium miteinander verbunden sein oder an einen sogenannten Bus (Diffusionsnetzwerk) angeschlossen sein, der mehrere Endsysteme direkt, also ohne Zwischensysteme miteinander verbindet.
Man unterscheidet in dieser Schicht zwischen **gesicherten** und **ungesicherten Diensten**. In ungesicherten Diensten werden als fehlerhaft erkannte Datenpakete eliminiert. Die Anforderung einer daraufhin notwendigen Übertragungswiederholung erfolgt aber erst auf einer höheren Schicht des Protokollstapels. Ein gesicherter Dienst hingegen übernimmt die Anforderung einer Übertragungswiederholung selbst.
In lokalen Netzen (LANs) wird die Schicht 2 des TCP/IP-Referenzmodells für gewöhnlich in zwei weitere Teilschichten aufgeteilt:

- **Media Access Control (MAC)**
  Diese Teilschicht regelt den Zugriff auf das gemeinsam mit (vielen) anderen Rechensystemen genutzte Übertragungsmedium. Da diese beim Zugriff auf das Übertragungsmedium in Konkurrenz stehen, müssen Protokollmechanismen vorgesehen werden, die einen für alle Teilnehmer gerechten und effizienten Zugriff erlauben (**Multiple Access Protocols**). Dies schließt Methoden zur Entdeckung bzw. zur Vermeidung von Kollisionen ein, da mehrere Teilnehmer eventuell zur gleichen Zeit Daten übertragen möchten (**Collision Detection**, **Collision Avoi-**

dance). Zudem muss jeder Netzteilnehmer auf dieser Schicht über eine individuelle und eindeutige Adresse verfügen, über die er angesprochen werden kann (**MAC Adressierung**). Auf der MAC-Subschicht können bereits verschiedene (aber homogene) Teilnetze über einen sogenannten **Switch** miteinander verbunden werden (**LAN Switching**). Dabei werden Datenpakete jeweils nur innerhalb des Teilnetzes weitergeleitet, in dem sich der jeweilige Zielrechner befindet. Der Switch übernimmt hier die Aufgabe der Filterung des Datenverkehrs (**MAC Filtering**). Es lassen sich zwei verschiedene Arten von Switch unterscheiden: Der **Store-and-Forward** Switch speichert die zu filternden Datenpakete stets bevor deren Analyse und anschließende Weiterleitung erfolgt, der **Cut-Through** Switch erledigt die Weiterleitung ohne vorherige Zwischenspeicherung. Zusätzlich fallen in dieser Subschicht Aufgaben der Warteschlangenverwaltung (**Data Packet Queueing** und **Scheduling**) an, wenn Datenpakete nicht schnell genug weitergeleitet werden können, bevor neue Datenpakete angeliefert werden, und über die Priorität der Weiterleitung entschieden werden muss.

- **Logical Link Control (LLC)**
  Diese Teilschicht bildet die sogenannte Sicherungsschicht des LANs. Die in ihr geregelten Aufgaben liegen auf einer höheren Abstraktionsebene als die der darunter gelegenen MAC-Teilschicht, auf der sie unmittelbar aufsetzt. Probleme und Aufgabenstellungen der LLC-Teilschicht wurden im **IEEE 802.2** Standard festgelegt. Zu den Aufgaben zählt das Vermeiden von Überlastsituationen bei potenziellen Empfängern von übertragenen Daten durch gezielte Eingriffe in den Datenfluss (**Flusssteuerung**) und die Steuerung der Datenübertragung (**Link Management**). Über die LLC-Subschicht findet auch eine erste Kontrolle bzgl. der Qualität der übertragenen Daten statt. Datenübertragungsfehler müssen erkannt und, falls möglich, korrigiert werden. Zu diesem Zweck implementieren die auf der LLC-Subschicht angesiedelten Protokolle unterschiedliche **Fehlererkennungs- und -korrekturverfahren**. Zusätzlich synchronisiert die LLC-Subschicht das Senden und Empfangen von Dateneinheiten (Datenpaketen). Dazu müssen Daten entsprechend den physikalischen und logischen Bedingungen der jeweils gewählten Übertragungsform in größenbeschränkte Datenpakete unterteilt werden (**Fragmentierung**), wobei nach der Übertragung stets Beginn und Ende eines Datenpakets korrekt erkannt werden müssen (**Datenpaketsynchronisation**). Daneben gewährleistet die LLC-Teilschicht die sogenannte **Multiprotokollfähigkeit**, also die Fähigkeit zur gleichzeitigen Nutzung verschiedener Kommunikationsprotokolle.

Zu den wichtigsten Protokollen der Netzzugangsschicht des TCP/IP-Referenzmodells zählen die von der IEEE gemäß dem **IEEE 802** LAN-Standard standardisierten LAN-Protokolle, also Technologien wie **Ethernet** (IEEE 802.3), **Token Ring** und **FDDI** (IEEE 802.5) sowie verschiedene drahtlose **WLAN** Technologien (IEEE 802.11), die in Kap. 4 detailliert beschrieben werden.

Die wichtigsten Protokolle aus der Netzzugangsschicht der TCP/IP-Protokollfamilie sind:

- **ATM (Asynchronous Transfer Mode)**
  ATM ist ein paketvermitteltes Netzwerkprotokoll, das zu transportierende Daten in Zellen fester Größe (Cell Relay) zerlegt und weiterleitet. Hinter diesem Designprinzip stand die Idee, zeitkritische Echtzeitdaten, wie z.B. Video- oder Audioinformation, gemeinsam mit regulären Daten über ein einheitliches Protokoll zu vermitteln, wobei darauf geachtet wurde, Schalt- und Transferverzögerungen möglichst klein zu halten. ATM arbeitet verbindungsorientiert und etabliert dazu eine virtuelle Verbindung zwischen zwei Endpunkten im Netzwerk, bevor der eigentliche Datentransfer startet. ATM kommt sowohl im LAN als auch in Weitverkehrsnetzen, sogenannten WANs (Wide Area Networks), zum Einsatz.
- **ARP (Address Resolution Protocol) und RARP (Reverse Address Resolution Protocol)**
  Mit Hilfe des in RFC 826 beschriebenen ARP Protokolls kann die MAC-Adresse eines Hosts ermittelt werden aus der IP-Adresse des in der darüberliegenden Schicht arbeitenden Internetprotokolls. Dies ist dann von Bedeutung, wenn ein Datenpaket aus dem Internet in einem lokalen Netzwerk angeliefert wird und aus der darin hinterlegten IP-Adresse des Empfängers zur Weiterleitung im LAN dessen MAC-Adresse ermittelt werden muss. ARP kommt dabei nur in LANs bzw. in Punkt-zu-Punkt Verbindungen zum Einsatz. Den umgekehrten Dienst liefert das in RFC 903 standardisierte RARP Protokoll, das zu MAC Adressen jeweils eine zugehörige IP-Adresse ermittelt.
- **NDP (Neighbor Discovery Protocol)**
  Die Funktionen des NDP Protokolls ähneln sehr dem ARP Protokoll und dienen der Erkundung und Entdeckung weiterer Hosts im lokalen Netzwerk. Der Unterschied zwischen ARP und NDP besteht darin, dass NDP für die nächste Generation des Internetprotokolls IPv6 entwickelt wurde, während ARP unter der aktuellen Version IPv4 arbeitet.
- **LLTD (Link Layer Topology Discovery)**
  Das proprietäre LLTD Protokoll wurde von der Firma Microsoft entwickelt zur Erkundung der jeweils vorliegenden Netzwerktopologie und zur Überprüfung der in einem Netzwerk gewährleisteten Dienstqualität (Quality of Service).
- **SLIP (Serial Line Internet Protocol) und PLIP (Parallel Line Interface Protocol)**
  SLIP, festgelegt in RFC 1055, und PLIP sind einfache Punkt-zu-Punkt Netzwerkprotokolle, die dem Transport von gekapselten, also in Datenpakete des SLIP bzw. PLIP Protokolls verpackten IP-Datenpaketen zwischen Personal Computern über eine serielle (SLIP) oder parallele Schnittstelle dienen. SLIP und PLIP wurden weitgehend durch das modernere PPP Protokoll verdrängt.
- **PPP (Point to Point Protocol)**
  PPP ist ein einfaches Punkt-zu-Punkt Netzwerkprotokoll, das der Verbindung zweier Netzknoten dient. PPP wird von den meisten Internet Service Providern (ISPs) genutzt, um ihren Kunden eine Wählverbindung über eine Standard-Telefonleitung ins Internet anzubieten. Moderne Zugänge via DSL (Digital Subscriber Line) werden von den ISPs über die gekapselten Protokollvarianten PP-

PoE (PPP over Ethernet, RFC 2516) und PPPoA (PPP over ATM, RFC 2364) realisiert.

- **STP (Spanning Tree Protocol)**
  STP wurde im IEEE 802.1D Standard festgelegt und beschreibt ein Protokoll, das Zyklenfreiheit innerhalb einer aus mehreren Netzsegmenten bestehenden LAN-Architektur gewährleisten soll. Wie der Name des Protokolls bereits sagt, wird aus dem vorliegenden Netzwerkgraphen ein sogenannter Spannbaum (Spanning Tree) erzeugt. Über den Spannbaum wird sichergestellt, dass das LAN keine geschlossenen Kreise enthält, über die Datenpakete für unbegrenzte Zeit unterwegs wären.

2.3.3 Internetschicht

Die Hauptaufgabe der Internetschicht des TCP/IP-Referenzmodells besteht darin, Datenkommunikation zwischen zwei Endsystemen im Kommunikationsnetzwerk über eventuell unterschiedliche Netzwerkarchitekturen hinweg zu ermöglichen. Die in der Internetschicht beschriebene Methode zur Überbrückung und Vereinigung unterschiedlicher Netzwerkarchitekturen mit Hilfe spezieller Zwischensysteme (Router) wird auch als **Internetworking** bezeichnet. Die dazu zu lösenden Aufgaben werden in RFC 1122 beschrieben. Zum Internetworking braucht es ein über die jeweiligen Netzwerkgrenzen hinweg eindeutiges Adressierungsschema (**IP Adressierung**) . Die zu versendenden Datenpakete müssen jeweils mit den Adressen von Sender und Empfänger versehen werden, um korrekt zugestellt werden zu können. Da die Kommunikation über ein oder mehrere eigenständig operierende Netzwerke hinweg erfolgt, müssen die Rechner an den Verbindungs- und Vermittlungsstellen (Zwischensysteme, Router) in der Lage sein, den zur korrekten Weiterleitung der Datenpakete einzuschlagenden Verbindungsweg auszuwählen (**Routing**). Bei der Vermittlung von Datenpaketen über unterschiedliche Netzwerktypen hinweg gelten oftmals unterschiedliche Regelungen bzgl. der Maximalgröße einzelner Datenpaket (Maximum Transmission Unit). Die vermittelnden Zwischensysteme müssen daher Datenpakete, die in ein Netzwerk mit stärkeren Beschränkungen vermittelt werden sollen, entsprechend zerlegen (**Fragmentierung**) und beim Empfänger wieder zusammensetzen[1]. Darüber hinaus können zwischen den überbrückten Netzwerken weitere technische Unterschiede auftreten, die über entsprechende Transfer- und Umrechnungsmethoden ausgeglichen werden müssen, wie z.B. die Vermittlung zwischen verschlüsselten Netzwerken und unverschlüsselten Netzwerken oder unterschiedliche zeit- oder mengenbasierte Abrechnungsmodalitäten.
Die drei auf der Internetschicht zu lösenden Basisaufgaben sind:

[1] Diese Aufgabe wurde in der neuen Version des Internet Protokolls IPv6 fallengelassen, da dort jeweils die an der Kommunikation beteiligten Endsysteme selbst eine Vorabfragmentierung übernehmen, um dadurch eine schnellere Vermittlung der Daten zu ermöglichen

- Ausgehende Datenpakete müssen an die nächste Vermittlungsstelle bzw. an das empfangende Endsystem weitergeleitet werden. Dazu muss das zuständige Kommunikationsprotokoll den nächsten (direkten) Empfänger (**Next Hop**) entlang des zu vermittelnden Weges auswählen und das Datenpaket an diesen senden durch Übergabe an das jeweils zuständige Protokoll in der Netzzugangsschicht.
- Ankommende Datenpakete müssen entpackt, die Kontroll- und Steuerinformationen aus dem Header des Datenpakets ausgelesen und die transportierten Nutzdaten ggf. an das in der darüberliegenden Schicht aktive Transportprotokoll weitergegeben werden.
- Zusätzlich werden noch Diagnoseaufgaben übernommen und eine einfache Fehlerbehandlung implementiert. Allerdings werden in der Internetschicht lediglich unzuverlässige Dienste (**Unreliable Services**) angeboten, d.h. es wird keine Garantie dafür übernommen, dass ein versendetes Datenpaket auch tatsächlich seinen Empfänger erreicht. Der Transport erfolgt lediglich „so gut es geht“ (**best effort**). Die Kontrolle über eine zuverlässige Kommunikation obliegt den beiden Kommunikationsendpunkten (Sender und Empfänger) und wird auf einer höheren Schicht des TCP/IP-Referenzmodells durchgeführt, um das Netzwerk auf dieser Schicht von dieser schwierigen Aufgabe zu entlasten. Durch diese „best effort“-Strategie wurde die Skalierbarkeit und Fehlertoleranz der Internet-Technologie überhaupt erst ermöglicht. Nur so konnte das Internet auf die seine heute erreichte Größe anwachsen.

Das zentrale Protokoll der Internetschicht ist das **Internet Protokoll** (**IP**). IP bietet eine unzuverlässige und datenpaketorientierte Ende-zu-Ende Übertragung von Nachrichten. Es ist verantwortlich für Fragmentierung und Defragmentierung in sogenannte **IP-Datagramme** und verfügt über Protokollmechanismen zur Weitervermittlung über Zwischensysteme hinweg zum designierten Empfänger der Nachricht. IP existiert heute in den zwei Versionen IPv4 (RFC 791) und IPv6 (RFC 2460) und zählt im Internet zu den wichtigsten Protokollen überhaupt.
Daneben kommt auf der Internetschicht das Protokoll **ICMP (Internet Control Message Protocol)** zum Einsatz, in dessen Zuständigkeit die Meldung bestimmter Fehler liegt, die während einer IP-Übertragung auftreten können, sowie weitere Diagnoseaufgaben, wie z.B. das Versenden von Echo-Requests, um die Erreichbarkeit eines Rechners und die dazu benötigte Übertragungszeit zu testen. ICMP ist ein Protokoll, das direkt auf IP aufsetzt. Es existieren zwei unterschiedliche Varianten des ICMP Protokolls jeweils für IPv4 (RFC 792) und IPv6 (RFC 4443).

Neben IP und ICMP gehören noch weitere Protokolle zur Internetschicht des TCP/IP-Protokollstapels, wie z.B.:

- **IPsec (Internet Protocol Security)**
  Hinter IPsec steht eine Protokollsuite zur sicheren Abwicklung des IP Datenverkehrs. Innerhalb eines Datenstroms können IP Datagramme authentifiziert (Authentication Header, AH) und verschlüsselt (Encapsulating Security Payload, ESP) werden (RFC 4835). Zusätzlich gehören zu IPsec Protokolle zur Verhandlung, Etablierung und zum Austausch sicherer kryptografischer Schlüssel (Internet Key Exchange Protocol, IKE, RFC 2409).

- **IGMP (Internet Group Management Protocol)**
  Das IGMP Protokoll (RFC 1112, RFC 2236, RFC 3376) dient der Verwaltung von IP Multicast-Gruppen von Endsystemen innerhalb eines TCP/IP-Netzwerks. Spezielle Multicast-Router verwalten Adresslisten von Endsystemen, die über eine Multicast-Adresse gemeinsam angesprochen werden können. Durch die Nutzung von Multicast-Adressen vermindert sich die Last beim Sender und im gesamten Netzwerk. IGMP existiert nur in einer Version für IPv4, da IPv6 Multicasting anders realisiert.
- **OSPF (Open Shortest Path First)**
  Das OSPF Protokoll (RFC 2328) ist ein sogenanntes Link-State Routingprotokoll, das IP-Datagramme innerhalb einer einzelnen Routing Domäne (Autonomous System) vermittelt. Damit gehört es zur Gruppe der Interior Gateway Protocols (IGP). OSPF ist das am weitesten verbreitete Routing Protokoll im Internet.
- **ST 2+ (Internet Stream Protocol, Version 2)**
  Das Internet Stream Protocol (ST, RFC 1190, und ST 2+, RFC 1819) ist ein experimentelles Protokoll der Internetschicht, das in Ergänzung zum Internet Protocol einen verbindungsorientierten Transport von Echtzeitdaten unter Gewährleistung einer stabilen Dienstgüte (Quality of Service) leisten soll.

2.3.4 Transportschicht

Die primäre Aufgabe der Transportschicht im TCP/IP-Referenzmodell, die etwa der Schicht 4 des ISO/OSI-Referenzmodells entspricht, besteht in der Einrichtung und Nutzung einer Kommunikationsverbindung zwischen zwei Anwendungsprogrammen, die auf unterschiedlichen Rechnern im Netzwerk residieren. Die Protokolle der Transportschicht etablieren eine direkte, virtuelle Ende-zu-Ende Kommunikationsverbindung. Um mehreren Anwendungsprogrammen auf demselben Rechner eine parallele Kommunikation zu erlauben, zählt auch ein statistisches Multiplexing zu den allgemeinen Aufgaben der Transportschicht. Zur eindeutigen Identifikation wird jedem Anwendungsprogramm eine sogenannte Portnummer zugeordnet. Jede in der Transportschicht übertragene Dateneinheit muss jeweils die Portnummern von Sender und Empfänger enthalten, um korrekt übermittelt werden zu können. Zusammen mit der IP-Adresse definiert die Portnummer einen sogenannten Netzwerk Socket, einen eindeutigen Verbindungs-Endpunkt im Netzwerk. Auf der Transportschicht wird ebenfalls eine komplexe Flusssteuerung (Flow Control) realisiert, die dafür sorgt, dass Überlastsituationen nach Möglichkeit vermieden werden (Congestion Avoidance). Schließlich wird noch sichergestellt, dass die übertragenen Daten fehlerfrei und in der richtigen Reihenfolge (Sequenznummern) beim Empfänger ankommen. Dazu dient ein Quittungsmechanismus, über den der Empfänger korrekt übertragene Datenpakete bestätigen bzw. fehlerhafte Datenpakete neu anfordern kann.

Anders als die Internetschicht, steht die Transportschicht nicht unter der Kontrolle des Netzbetreibers, sondern bietet dem Anwender bzw. dem Anwendungsprogramm des kommunizierenden Endsystems die Möglichkeit, Einfluss auf Probleme in der Datenübertragung zu nehmen, die nicht von der Internetschicht behandelt werden. Dazu zählt die Überbrückung von Ausfällen auf der Internetschicht und die Nachlieferung von Datenpaketen, die in der Internetschicht verloren gegangen sind. Die Transportschicht ist in der Lage, beliebig lange Pakete (Streams) zu übertragen. Eine lange Nachricht wird dazu in Segmente unterteilt, die einzeln und unabhängig transportiert und beim Empfänger anschließend wieder zusammengesetzt werden.
Das **Transport Control Protokoll (TCP)** als ein weiteres Kernstück der Internet-Protokoll-Architektur ist das populärste Protokoll der Transportschicht im TCP/IP-Referenzmodell. Standardisiert als RFC 793 realisiert es einen zuverlässigen, verbindungsorientierten, bidirektionalen Datenaustausch zwischen zwei Endsystemen, der im TCP/IP-Referenzmodell auf einem unzuverlässigen, verbindungslosen Datagrammdienst der Internetschicht aufsetzt. TCP ermöglicht den Aufbau sogenannter **Virtueller Netzwerke** (Virtual Circuits). Nach der Einrichtung einer virtuellen Verbindung wird ein Datenstrom (Byte Stream) übertragen, der die paketorientierte Übertragung von Nachrichten für die darüberliegende Anwendungsschicht verbirgt. Ein zuverlässiger Dienst wird dabei durch einen Quittierungsmechanismus (Automatic Repeat Request, ARQ) realisiert, über den die Übertragung verlorengegangener Daten veranlasst wird.
Neben TCP ist das **Universal Datagram Protokoll (UDP)** das zweite prominente Protokoll der Transportschicht. Standardisiert als RFC 768 überträgt es eigenständige Dateneinheiten, sogenannte Datagramme, zwischen Anwendungsprogrammen, die auf unterschiedlichen Rechnern im Netzwerks residieren. Allerdings ist die Übertragung unzuverlässig, d.h. eventuell mit Datenverlust, Vervielfachung von Datagrammen und Reihenfolgeveränderungen verbunden. Die als falsch erkannten Datagramme werden von UDP verworfen und erreichen den Empfänger erst gar nicht. UDP zeichnet sich gegenüber TCP durch eine deutlich geringere Komplexität aus, was sich in einem erhöhten Datendurchsatz niederschlägt. Allerdings wird dies mit einem drastischen Verlust an Zuverlässigkeit und Sicherheit bezahlt. Das darüberliegende Anwendungsprogramm muss selbst für eine Beseitigung möglicher Fehler des UDP Protokolls sorgen.
Weitere wichtige Protokolle der Transportschicht sind:

- **DCCP (Datagram Congestion Control Protocol)**
  DDCP (RFC 4340) ist ein nachrichtenorientiertes Protokoll der Transportschicht, das neben dem zuverlässigen Verbindungsaufbau und -abbau auch Überlastmeldungen verteilt (Explicit Congestion Notification, ECN), Überlaststeuerungsfunktionen bereitstellt (Congestion Control) und zur Aushandlung von Übertragungsparametern genutzt werden kann.
- **RSVP (Resource Reservation Protocol)**
  Das RSVP (RFC 2205) Protokoll dient zur Anforderung und Reservierung von Netzwerkressourcen für mittels IP zu übertragende Datenströme. Es ist nicht zum eigentlichen Transport von Daten bestimmt und ähnelt den Protokollen ICMP

und IGMP der Internetschicht. RSVP kann sowohl von Endsystemen oder Routern eingesetzt werden, um zuvor spezifizierte Dienstqualitäten zu reservieren und aufrecht zu erhalten.

- **TLS (Transport Layer Security)**
  Als Nachfolger des **Secure Socket Layer Protokolls (SSL)** stellt TLS (RFCs 2246, 4346 und 5246) kryptografische Protokolle für den sicheren Datentransport im Internet bereit. Dabei verschlüsseln TLS und SSL einzelne TCP-Segmente. TLS stellt Protokolle zur Aushandlung von Übertragungsparametern (Peer Negotiation), zum Austausch von kryptografischen Schlüssen und zur Authentifikation, sowie für Verschlüsselung und digitaler Signatur bereit.
- **SCTP (Stream Control Transmission Protocol)**
  SCTP (RFC 4960) ist ein Vorschlag für eine hochskalierbare und performantere Version des ursprünglichen TCP Protokolls und ist spezialisiert auf die Übertragung großer Datenmengen.

2.3.5 Anwendungsschicht

Die in der Anwendungsschicht des TCP/IP-Referenzmodells verfügbaren Funktionen umfassen die Aufgaben der Schichten 5-7 des ISO/OSI-Referenzmodells. Grundsätzlich dient die Anwendungsschicht als Schnittstelle zu den eigentlichen Anwendungsprogrammen, die über das Netzwerk kommunizieren wollen (Process-to-Process Communication). Die Anwendungen selbst befinden sich dabei außerhalb dieser Schicht und auch außerhalb des TCP/IP-Referenzmodells überhaupt.
Die angebotenen Dienste und Programmierschnittstellen (Application Programming Interfaces, API) der Anwendungsschicht verfügen über ein hohes Abstraktionsniveau, das den Anwender bzw. die kommunizierenden Anwendungen vor den Details der Kommunikation, die auf den niedrigeren Protokollschichten geregelt werden, weitgehend abschirmt. Dabei übernehmen Protokolle und Dienste der Anwendungsschicht üblicherweise Übersetzungen und Umformungen von Daten zwischen Anwendungsprogrammen auf der semantischen Ebene. Zu den hier angesiedelten Diensten zählen Namensdienste (Naming Services), die dazu dienen, IP-Adressen in lesbare Namen zu übersetzen und umgekehrt, Umleitungsdienste (Redirect Services), die nicht erfüllbare Anfragen zu einem anderen Host umleiten, sowie Verzeichnisdienste und Netzwerkmanagementdienste.
Die Protokolle der Anwendungsschicht arbeiten meist nach dem Client/Server-Kommunikationsprinzip. Ein aktiver Client kontaktiert einen passiv wartenden Server und übermittelt diesem eine Dienstanfrage. Der Server nimmt die Anfrage des Clients entgegen, verarbeitet sie und sendet dem Client eine Antwort, d.h. im positiven Fall den angefragten Dienst, zurück.

Einige wichtige der zahlreichen auf der Anwendungsschicht der TCP/IP-Protokollfamilie angesiedelten Protokolle sind z.B.:

- **TELNET (TELecommunication NETwork)**
  TELNET (RFC 854) ermöglicht die Einrichtung einer interaktiven, bidirektionalen Kommunikationsverbindung zu einem entfernten Rechner und stellt dazu eine Kommandozeilenschnittstelle zur Verfügung, mit der auf dem entfernten Rechner ein virtuelles Terminal via TCP eingerichtet wird, auf dem Befehle und Aktionen ausgelöst werden können.
- **FTP (File Transfer Protocol)**
  FTP (RFC 959) dient der Übertragung und Manipulation von Dateien zwischen zwei über ein TCP/IP-Netzwerk verbundenen Rechnern. Dabei arbeitet FTP nach dem Client-/Server Paradigma, d.h. ein Client initiiert die Verbindung und fragt einen Dienst an, der Server nimmt den Verbindungswunsch entgegen und beantwortet die Dienstanfrage. Die eigentliche Datenübertragung und die Übertragung von Kontroll- und Steuerkommandos erfolgt bei FTP über zwei unterschiedliche TCP-Ports.
- **SMTP (Simple Mail Transfer Protocol)**
  SMTP (RFC 821) ist ein einfach strukturiertes Protokoll zur Übertragung von elektronischer Post im Internet. Heute wird in der Regel ESMPT (Extended SMTP, RFC 5321) eingesetzt, das eine transparente Übertragung von Nachrichten unterschiedlicher Formate gestattet. SMTP wird von Message Handling Systemen (MHS) des E-Mail-Dienstes zum Versenden und Empfangen von Nachrichten verwendet. Endsysteme, d.h. Systeme auf denen der Endnutzer arbeitet, verwenden SMTP lediglich zum Versenden von E-Mail Nachrichten, die von einem Mailserver weitergeleitet werden.
- **HTTP (Hypertext Transport Protocol)**
  Das HTTP Protokoll (RFC 2616 u.a.) wird zur Datenübertragung im World Wide Web verwendet. Wie viele andere Protokolle der Anwendungsschicht arbeitet es nach dem Client-/Server-Paradigma und setzt auf das zuverlässige Transportprotokoll TCP auf.
- **RPC (Remote Procedure Call)**
  Das RPC Protokoll (RFC 1057 und RFC 5531) dient der Inter-Prozess-Kommunikation, d.h. es erlaubt einem Computerprogramm eine externe, auf einem entfernten Rechner liegende Subroutine aufzurufen, die extern ausgeführt wird und dem aufrufenden Rechner lediglich ein Ergebnis übermittelt, das dort anschließend weiterverarbeitet wird.
- **DNS (Domain Name System)**
  Der DNS Dienst etabliert einen Namens- und Verzeichnisdienst, der die Zuordnung zwischen lesbaren Endsystemnamen (Zeichenketten) zu IP-Adressen für alle am Internet teilnehmenden Systeme liefert. Der über DNS verwaltete Namensraum für Endsystemnamen ist hierarchisch organisiert und arbeitet mit lokalen Zwischenspeichern und Proxies, damit eine effiziente Umsetzung gewährleistet ist. DNS ist unter RFC 1123 und in zahlreichen weiteren RFCs standardisiert.
- **SNMP (Simple Network Management Protocol)**
  Mit Hilfe des SNMP Protokolls können Netzwerkmanagement Systeme einzelne,

an ein Netzwerk angeschlossene Systeme überwachen, verwalten und kontrollieren. SNMP ist in RFC 3411 und in zahlreichen weiteren RFCs standardisiert.

- **RTP (Real-time Transport Protocol)**
  Mit Hilfe des RTP Protokolls (RFC 1889) lassen sich Echtzeit Audio- und Videodaten über das Internet übertragen. Zu diesem Zweck definiert das RTP Protokoll ein eigenes Datenformat für den effizienten Transport eines Mediendatenstromes. Üblicherweise wird der Transport und die erreichte Dienstqualität mit Hilfe des RTCP (RTP Control Protocol) überwacht. Obwohl der Protokollstandard das TCP Protokoll zum eigentlichen Datentransport vorsieht, wird in der Praxis jedoch meist das unzuverlässigere, dafür aber schnellere UDP Protokoll eingesetzt, um inhärente Wartezeiten beim Verbindungsmanagement und der Fehlerkorrektur zu vermeiden.

2.4 Glossar

Authentifikation (auch **Authentifizierung**): Dient dem Nachweis der Identität eines Benutzers. Bei der Authentifikation werden zur Identitätsprüfung Zertifikate einer vertrauenswürdigen Instanz verwendet und zur Überprüfung der Integrität einer Nachricht digitale Signaturen erstellt und und mitversendet.

Broadcast: Eine Broadcast-Übertragung entspricht einem Rundruf, also einer gleichzeitigen Übertragung von einem Punkt aus zu allen Teilnehmern. Klassische Broadcast-Anwendungen sind Rundfunk und Fernsehen.

Client: Bezeichnet ein Programm, das einen Server kontaktiert und von diesem Informationsdienstleistungen anfordert. Der im WWW eingesetzte Browser ist in diesem Sinne ein Client. Aber es gibt auch andere Clients im WWW, die WWW-Server kontaktieren und Informationen von diesen herunterladen, wie z.B. Suchmaschinen oder Agenten.

Client/Server-Architektur: Eine Anwendung wird arbeitsteilig auf mehreren, durch ein Netzwerk verbundenen Computern ausgeführt. Der Server stellt dabei bestimmte Dienstleistungen bereit, der Client auf der anderen Seite fordert Dienstleistungen an. Außer dem Erteilen und Beantworten von Auftragsbeziehungen sind die Komponenten voneinander unabhängig. Schnittstellen und die Art der Kommunikation zur Auftragserteilung und Beantwortung sind eindeutig festgelegt.

Diffusionsnetzwerk (Broadcastnetzwerk): In einem Diffusionsnetzwerk wird das Signal eines Senders von allen im Netz verbundenen Rechnern unter Berücksichtigung der jeweiligen Laufzeitverzögerung empfangen. Jeder Empfänger muss dabei selbst feststellen, ob die Nachricht für ihn bestimmt ist und ob er sie verarbeitet oder nicht.

Flusssteuerung (Flusssteuerung, Flow Control): Klasse von Verfahren zur Gewährleistung einer gleichmäßigen und möglichst kontinuierlichen Datenübertragung zwischen Netzwerkendgeräten, die nicht synchron arbeiten. Die Flusssteuerung greift regulierend in die Sendefolge der Netzwerkendgeräte ein und drosselt die Sendeleistung, wenn entlang des Weges zum Empfänger Stausituationen auftreten, um potenzielle Datenverluste zu vermeiden.

Fragmentierung/Defragmentierung: Aufgrund technischer Restriktionen ist die Länge der Datenpakete, die ein Kommunikationsprotokoll in einem paketvermittelten Netzwerk versendet, unterhalb der Anwendungsschicht stets beschränkt. Ist die Länge der zu versendenden Nachricht größer als die jeweils vorgeschriebene Datenpaketlänge, wird die Nachricht in einzelne Teilnachrichten (Fragmente) zerlegt, die den vorgegebenen

Längenrestriktionen entsprechen. Damit die einzelnen Fragmente nach der Übertragung beim Empfänger wieder korrekt zur Ursprungsnachricht zusammengesetzt (defragmentiert) werden können, müssen sie mit **Sequenznummern** versehen werden, da die Übertragungsreihenfolge im Internet nicht immer garantiert werden kann.

Internetworking: Das Überbrücken mehrerer verschiedener, von einander separierter Netzwerke (LANs, WANs) zu einem Internet. Dazu werden geeignete Vermittlungsrechner (Router) benötigt, die den Weg eines Datenpakets durch den Netzwerkverbund vermitteln und für eine sichere Zustellung sorgen. Dem Benutzer erscheint der Netzwerkverbund als homogenes, virtuelles Netz (Internet).

Internetstandard: Da in der Entwicklung des Internets viele Firmen und Organisationen beteiligt waren, bestand die Notwendigkeit, einheitliche Protokolle und Schnittstellen zu entwerfen, um so den Entwicklungsaufwand zu vereinfachen. Diese werden in Form von Internet-Standards in einem öffentlichen Standardisierungsprozess verabschiedet, der es prinzipiell jedem Benutzer ermöglicht, zu einem neuen Vorschlag für einen zukünftigen Standard Stellung zu beziehen (Request for Comment, RFC) und so die Entwicklung des Internets mit zu lenken.

Internet Protocol (IP): Protokoll auf der Netzwerkschicht des TCP/IP-Referenzmodells. Als einer der Grundpfeiler des Internets sorgt IP dafür, dass das aus vielen heterogenen Einzelnetzwerken bestehende globale Internet als einheitliches, homogenes Netzwerk erscheint. Ein einheitliches Adressierungsschema (**IP-Adressen**) sorgt für eine weltweit eindeutige Rechneridentifikation. IP stellt dazu einen **verbindungslosen, paketvermittelten Datagrammdienst** bereit, der keine Dienstgütegarantien erfüllen kann, sondern stets nach dem **Best-Effort**-Prinzip arbeitet. Zur Kommunikation von Steuerungsinformation und Fehlermeldungen dient das **ICMP**-Protokoll als integraler Bestandteil von IP. Zur Zeit ist das IP-Protokoll der Version 4, IPv4 noch weitläufig im Einsatz, wird aber aufgrund der Adressknappheit zusehends von IPv6 abgelöst.

ISO/OSI-Referenzmodell: Eine Spezifikation der ISO, die als Grundlage für die Entwicklung von Kommunikationsstandards entworfen und publiziert wurde. Dabei handelt es sich um ein Referenzmodell für die Datenübertragung, das aus sieben Schichten (Layers) besteht, und das Ziel verfolgt, dass verschiedene Rechner- und Protokollwelten über einheitliche Schnittstellen miteinander kommunizieren können. Das ISO/OSI-Referenzmodell verliert gegenüber dem TCP/IP-Referenzmodell, der dem Internet zugrunde liegende Protokollstandard, zunehmend an Bedeutung.

Kommunikationsprotokoll: Ein Kommunikationsprotokoll (auch einfach Protokoll) ist eine Sammlung von Regeln und Vorschriften, die das Datenformat von zu übermittelnden Nachrichten sowie sämtliche Mechanismen und Abläufe zu ihrer Übertragung festlegen. Sie enthalten Vereinbarungen über den Auf- und Abbbau einer Verbindung zwischen den Kommunikationspartnern, sowie über die Art und Weise der Datenübertragung.

Kryptografie: Teilgebiet der Informatik und der Mathematik, das sich mit der Konstruktion und Bewertung von Verschlüsselungsverfahren beschäftigt. Das traditionelle Ziel der Kryptografie liegt im Schutz der Vertraulichkeit von Informationen vor dem Zugriff unberechtigter Dritter. Mit der Nutzung der Kryptografie können aber auch Sicherheitsziele, wie z.B. Integrität oder Verbindlichkeit realisiert werden.

Leitungsvermittlung: Methode des Nachrichtenaustauschs über ein Netzwerk, bei der zu Beginn des Nachrichtenaustauschs eine exklusive, feste Verbindung zwischen den kommunizierenden Endgeräten aufgebaut wird, die für die gesamte Dauer der Kommunikation bestehen bleibt. Analoge Telefonnetze funktionieren z.B. nach diesem Prinzip.

Local Area Network (LAN): Räumlich begrenztes Rechnernetz, das nur eine begrenzte Anzahl von Endgeräten (Rechnern) aufnehmen kann. Ein LAN ermöglicht eine effiziente und gleichberechtigte Kommunikation aller daran angeschlossenen Endsysteme. In der Regel teilen sich dazu die angeschlossenen Rechner ein gemeinsam genutztes Übertragungsmedium.

Multicasting: Bei einer Multicast-Übertragung sendet eine Quelle gleichzeitig an eine Gruppe von Empfängern. Es handelt sich dabei um eine 1:n-Kommunikation. Multicasting wird häufig zur Übertragung von Multimediadaten genutzt.

Netzanwendung: Ein Anwendungsprogramm, dessen Ablauf den Zugriff auf Ressourcen einschließt, die nicht lokal auf dem ausführenden Rechner verfügbar sind, sondern auf einem entfernten Rechner über das Netzwerk erreichbar liegen.

Paketheader: In einem paketvermittelten Netzwerk fordern die verwendeten Kommunikationsprotokolle die Fragmentierung der zu übertragenden Informationen in einzelne Datenpakete. Um sicherzustellen, dass die Datenpakete korrekt übertragen werden, den designierten Empfänger erreichen und dort wieder zur Originalinformation zusammengesetzt werden können, werden den Datenpaketen Steuer- und Kontrollinformationen in einem sogenannten Datenpaketheader vorangestellt.

Paketvermittlung Die vorherrschende Kommunikationsmethode in digitalen Netzen. Die Nachricht wird dabei in einzelne Datenpakete fester Größe zerlegt und die Pakete werden einzeln und unabhängig voneinander vom Sender über eventuell vorhandene Vermittlungsstellen zum Empfänger gesendet. Man unterscheidet **verbindungsorientierte** und **verbindungslose** (Datagrammnetze) Paketvermittlungsnetze. In verbindungsorientierten Paketvermittlungsnetzen wird vor dem Start der eigentlichen Datenübertragung eine Verbindung über fest gewählte Vermittlungsstellen im Netz aufgebaut. In verbindungslosen Paketvermittlungsnetzen wird dagegen kein fester Verbindungsweg festgelegt.

Protokollstapel: Die verschiedenen Teilprobleme der Netzwerkkommunikation werden jeweils von speziellen Protokollen abgehandelt, die alle reibungslos miteinander zusammenarbeiten müssen, um das Gesamtproblem der Netzwerkkommunikation zu lösen. Um dieses Zusammenspiel zu gewährleisten wird die Entwicklung der Netzwerkprotokoll-Software als komplett zu lösende Gesamtaufgabe angesehen und zu ihrer Lösung jeweils eine zusammengehörige **Familie von Protokollen** (Protocol Suites) entwickelt, die die anfallenden Teilaufgaben lösen und effizient miteinander interagieren. Da sich das Gesamtproblem der Netzwerkkommunikation mit Hilfe eines **Schichtenmodells** repräsentieren lässt und die einzelnen Protokolle einer Protokollfamilie jeweils einer bestimmten Schicht zugeordnet werden können, wird von einem **Protokollstapel** gesprochen. Die bekanntesten Protokollstapel sind die TCP/IP-Protokollsuite des Internets und das oft als Lehrbeispiel dienende ISO/OSI-Schichtenmodell.

Quality of Service (Dienstgüte): Quantifiziert die Leistung eines Dienstes, der von einem Kommunikationssystem angeboten wird. Diese wird über die Dienstgüteattribute Leistung, Leistungsschwankung, Zuverlässigkeit und Sicherheit beschrieben, die jeweils über eigene, quantifizierbare Dienstgüteparameter spezifiziert werden.

Rechnernetz: Ein Rechnernetz (**Netzwerk**, **Computer Network**) bietet den an das Netz angeschlossenen, autonomen Rechnersystemen, die jeweils über eigenen Speicher, eigene Peripherie und eigene Rechenfähigkeit verfügen, die Infrastruktur zum Datenaustausch. Da alle Teilnehmer miteinander vernetzt sind, bietet das Rechnernetz jedem Teilnehmer die Möglichkeit, mit jedem anderen der Netzteilnehmer in Verbindung zu treten.

Referenzmodell: Als Referenzmodell wird üblicherweise ein abstraktes Modell bezeichnet, auf dessen Grundlage speziellere Modelle abgeleitet bzw. konkrete Implementationen abgeleitet werden können. Oft werden Referenzmodelle als allgemeines Vergleichsobjekt herangezogen, es ermöglicht den Vergleich mit anderen Modellen, die die gleichen Sachverhalte beschreiben. Im Bereich der Computernetzwerke existieren zwei bekannte Referenzmodelle, das heute meist nur zu didaktischen Zwecken genutzte ISO-OSI-Referenzmodell und das im Internet tatsächlich implementierte TCP/IP-Referenzmodell.

Request for Comments (RFC): Neue Technologien im Internet reifen in der Diskussion von Experten und werden festgehalten in sogenannten RFCs. Im Zuge des Internet-Standardisierungsprozesses entstand daraus eine durchnummerierte Sammlung von Do-

kumenten in denen Technologien, Standards und Sonstiges mit Bezug zum Internet dokumentiert und standardisiert wurde.

Router: Vermittlungsrechner, der in der Lage ist, zwei oder mehrere Teilnetze miteinander zu verbinden. Router arbeiten in der Transportschicht (IP-Layer) des Netzwerks und sind in der Lage, ankommende Datenpakete gemäß ihrer Zieladresse auf der kürzesten Route durch das Netzwerk weiterzuleiten.

Routing: In einem WAN liegen entlang des Weges zwischen Sender und Empfänger oft mehrere Schaltelemente, die eine Vermittlung der versendeten Daten an den jeweiligen Empfänger übernehmen. Die Ermittlung des korrekten Weges vom Sender zum Empfänger wird als Routing bezeichnet. Die dedizierten Vermittlungsstellen (**Router**) empfangen dabei ein versendetes Datenpaket, werten dessen Adressinformation aus und leiten es entsprechend an den/die designierten Empfänger weiter.

Schichtenmodell: Komplexe Probleme lassen sich hierarchisch in Teilprobleme zerlegen, die alle aufeinander aufbauen. Die so entstehende Schichtung der einzelnen Teilprobleme, erleichtert die Modellierung des Gesamtproblems. Das Abstraktionsniveau nimmt auf jeder einzelnen Schicht zu, so dass eine Schicht, die höher im Schichtenmodell angesiedelt ist, vor Detailproblemen abgeschirmt ist, die auf einer niedrigeren Schicht abgehandelt werden. Schichtenmodelle spielen in der Kommunikationstechnik, aber auch in anderen Gebieten der Informatik eine bedeutende Rolle. In abgewandelter Darstellung entsprechen diese auch dem **Schalenmodell**, das anstelle aus hierarchisch aufeinander aufbauenden Schichten aus einzelnen Schalen besteht.

Server: Bezeichnet einen Prozess, der von Clients kontaktiert wird, um diesen Informationen zurückzuliefern oder Ressourcen zur Verfügung zu stellen. Oft wird auch der Rechner, auf dem ein Server-Prozess abläuft, als Server bezeichnet.

Sicherheit: In der Netzwerktechnik werden unter dem Begriff Sicherheit verschiedene Sicherheitsziele (Dienstgüteparameter) zusammengefasst, die den Grad der Unversehrtheit und Authentizität der übertragenen Daten beschreiben. Zu den wichtigsten Sicherheitszielen gehören **Vertraulichkeit** (kein unberechtigter Dritter ist in der Lage, die Datenkommunikation zwischen Sender und Empfänger abzuhören), **Integrität** (Unversehrtheit der empfangenen Daten), **Authentizität** (Garantie der Identität der Kommunikationspartner), **Verbindlichkeit** (rechtsverbindlicher Nachweis einer erfolgten Kommunikation) und **Verfügbarkeit** (Garantie, dass ein Dienstangebot tatsächlich verfügbar ist).

Transmission Control Protocol (TCP): Protokollstandard auf der Transportschicht des TCP/IP-Referenzmodells. TCP stellt einen zuverlässigen, verbindungsorientierten Transportdienst bereit, auf dem viele Internet-Anwendungen basieren.

TCP/IP-Referenzmodell (auch TCP/IP-Protokollsuite, TCP/IP-Kommunikationsmodell): Bezeichnet ein Kommunikationsschichtenmodell für das Internet. Das TCP/IP-Referenzmodell unterteilt sich in vier Protokollschichten (Netzzugangsschicht, Internetschicht, Transportschicht und Anwendungsschicht) und ermöglicht es, dass verschiedene Rechner- und Protokollwelten über einheitliche Schnittstellen im Internet miteinander kommunizieren können.

Topologie: Unter der Topologie eines Rechnernetzes versteht man die geometrische Form der Verteilung der einzelnen Rechnerknoten innerhalb des Netzwerks. Verbreitete Topologien für Rechnernetzwerke sind **Bustopologie**, **Ringtopologie** und **Sterntopologie**.

Überlast (Congestion): Ein Netzwerk kann mit seinen Betriebsmitteln (Übertragungsmedien, Router und andere Zwischensysteme) eine bestimmte Last (Kommunikation, Datenübertragung) bewältigen. Nähert sich die im Netzwerk erzeugte Last zu 100% der vorhandenen Kapazität an, tritt eine Überlast (Congestion) auf, auf die das Netzwerk in geeigneter Weise reagieren muss, um Datenverluste und den Zusammenbruch der Kommunikation zu vermeiden.

verbindungsorientierter/-loser Dienst: Man unterscheidet grundsätzlich zwischen **verbindungsorientierten** und **verbindungslosen** Diensten im Internet. Verbindungsorientierte Dienste müssen vor dem Start der eigentlichen Datenübertragung eine Verbindung im Netz aufbauen. Die so festgelegte Verbindungsstrecke wird für die Dauer der gesamten Kommunikation genutzt. Verbindungslose Dienste wählen vorab keinen festen Verbindungsweg. Die versendeten Datenpakete werden jeweils unabhängig voneinander auf möglicherweise verschiedenen Wegen über das Internet übertragen.

Wide Area Network (WAN): Frei skalierbares Rechnernetz, das keiner räumlichen oder kapazitätsmässigen Beschränkung unterliegt. Einzelne Teilnetze werden dabei durch Vermittlungssysteme (Router) miteinander verbunden, die den Datentransfer im WAN koordinieren. Die WAN-Technologie liefert die Grundlagen für das **Internetworking**.

http://www.springer.com/978-3-540-92939-0

Internetworking
Technische Grundlagen und Anwendungen
Meinel, C.; Sack, H.
2012, XIII, 978 S. 360 Abb., 1 Abb. in Farbe., Hardcover
ISBN: 978-3-540-92939-0