LEHRBUCH

Andriy Luntovskyy
Dietbert Gütter

Moderne Rechnernetze

Protokolle, Standards und Apps in kombinierten drahtgebundenen, mobilen und drahtlosen Netzwerken

Springer Vieweg

Moderne Rechnernetze

Andriy Luntovskyy
Dietbert Gütter

Moderne Rechnernetze

Protokolle, Standards und Apps in kombinierten drahtgebundenen, mobilen und drahtlosen Netzwerken

Springer Vieweg

Andriy Luntovskyy
Berufsakademie Sachsen
Dresden, Deutschland

Dietbert Gütter
Staatliche Studienakademie Dresden
Berufsakademie Sachsen
Dresden, Sachsen, Deutschland

ISBN 978-3-658-25616-6 ISBN 978-3-658-25617-3 (eBook)
https://doi.org/10.1007/978-3-658-25617-3

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

Planung/Lektorat: Reinhard Dapper
Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Geleitwort

Das vorliegende Lehrbuch eignet sich sehr gut als vorlesungsbegleitende Literatur zum Themengebiet der Rechnernetze. Es wendet sich an Studierende und Dozentinnen und Dozenten der Informatik und der Elektrotechnik und Informationstechnik an Technischen Hochschulen und Studienakademien im deutschsprachigen Raum. Auch für ein Fernstudium, die berufsbegleitende Weiterbildung sowie auszugsweise für Fachseminare kann das Buch sinnvoll eingesetzt werden. Die Autoren verfügen selbst über viele Jahre Erfahrung als Dozenten im universitären sowie im berufsbezogenen Bildungsbereich und veröffentlichten bereits andere einschlägige Fachbücher zur Planung und Optimierung von Rechnernetzen sowie zu Architekturen verteilter Softwaresysteme.

Das Werk gibt einen breiten Überblick über Grundlagen, Technologien und Anwendungen von Rechnernetzen und ist dem entsprechend in drei größere Komplexe gegliedert: Teil I führt in die Prinzipien der Datenübertragung ein und stellt die Internet-Schichtenarchitektur als wichtiges Fundament vor. Teil II präsentiert die verschiedenen kabelgebundenen wie auch drahtlosen Netzwerktechnologien einschließlich aktueller Entwicklungen des Mobilfunks. Teil III schließlich widmet sich den anwendungsorientierten Schichten von Rechnernetzen und behandelt dabei auch aktuelle Fragestellungen zu Cloud und Fog Computing, Virtualisierung, Multimedia-Applikationen, Industrie 4.0 und dem Internet der Dinge.

Dabei zeichnet sich dieses Lehrbuch besonders aus durch einen deutlichen Praxisbezug, durch konkrete Anwendungsszenarien und Implementierungsbeispiele sowie durch umfangreiche begleitende Übungen; die Übungsaufgaben sind in einem separaten, begleitenden Übungsbuch übersichtlich zusammengestellt, gefolgt von den zugehörigen Musterlösungen, und sie korrespondieren direkt mit den entsprechenden Teilen des Lehrbuchs.

Diese besonderen Merkmale sind sicherlich gerade für ein berufsintegriertes Studium an staatlichen Studienakademien, Berufsakademien und dualen Hochschulen von besonderer Bedeutung, sie unterstützen aber zweifelsohne auch die Motivation und den Lernerfolg in praxisorientierten Lehrveranstaltungen an

Technischen Hochschulen. Durch eine gut verzahnte, übergreifende Sicht auf Architekturen, Dienste, Dienstqualität und Effizienzfragen wird letztlich auch eine gesamtheitliche Sicht auf Technologien der Rechnernetze und die damit verbundenen technisch-gesellschaftlichen Transformationsprozesse vermittelt.

Abschließend sei allen Leserinnen und Lesern dieses Lehrbuchs und des begleitenden Übungsbuches viel Erfolg bei ihren Studien beziehungsweise ihrer Aus- und Weiterbildung gewünscht – die praxisorientierte Betrachtungsweise und die integrierten Übungen werden hierfür bestimmt förderlich sein!

Prof. Dr. habil. Dr. h. c. Alexander Schill
Professur für Rechnernetze
TU Dresden
Dresden
im Jahre 2018

Danksagung

In den Inhalt des Lehrbuches wurden auch didaktisch bewährte Beispiele von Dozenten der TU Dresden und BA Dresden übernommen. Wir danken dafür Prof. Dr. rer. nat. habil. Dr. h. c. Alexander Schill, Dr. habil. Josef Spillner, Dr.-Ing. Marius Feldmann, Dr. Iris Braun, Dr. Thomas Springer, Prof. Dr. Tenshi Hara und vielen weiteren unserer Kollegen, Gleichgesinnten und Mitstreitern.

Einige Beispiele wurden aus dem Wissensbestand Skripte LS Rechnernetze an der TU Dresden [3] mit Anpassungen und Erweiterungen zitiert.

Inhaltsverzeichnis

Über die Autoren

Prof. Dr. habil. Andriy Luntovskyy
ist Professor an der BA Dresden. An der BA Dresden arbeitet er seit 2008. Im Zeitraum 2001 bis 2008 arbeitete Herr Luntovskyy als wiss. MA am Lehrstuhl Rechnernetze an der Technischen Universität Dresden. Seine „Alma Mater" ist die Technische Universität Kiew „Igor Sikorsky KPI" (Abschluss 1989).

Interessen-/Lehrgebiete:
1. Rechnernetze und mobile Kommunikation
2. Verteilte Systeme und angewandte Datensicherheit
3. Softwaretechnik und Betriebssysteme
4. Grundlagen der Programmierung/Informatik.

Kontakt: Staatliche Studienakademie Sachsen (BA Dresden), Andriy.Luntovskyy@ba-dresden.de

Dr. rer. nat. Dietbert Gütter (em.)
ist nebenberuflicher Dozent an der TU Dresden und an der BA Dresden. Seine „Alma Mater" ist die Technische Universität Dresden (Promotion 1974). Er arbeitete mehr als 40 Jahre in Dresden als wiss. MA am Lehrstuhl Rechnernetze an der TU Dresden, BA Dresden und anderen akademischen Institutionen.

Interessen-/Lehrgebiete:
1. Rechnernetze und Betriebssysteme
2. Netzwerkpraxis und -projektierung
3. Web-Anwendungen und Softwaretechnik
4. Informations- und Kommunikationssysteme.

Kontakt: Technische Universität Dresden, Dietbert.Guetter@tu-dresden.de

Grundlagen und übertragungsorientierte Schichten

„I have never really found it difficult to explain basic laws of nature to children. When you reach them at their level, you can read in their eyes their genuine interest and appreciation“ (original text).

„Ich habe es niemals schwer gefunden, den Kindern Grundgesetze der Natur zu erklären. Wenn man sie auf ihrem Niveau erreicht, kann man in ihren Augen ihr echtes Interesse und ihre Würdigung erkennen.“
(Albert Einstein, 1870–1955)

Inhalte und kurzfassende Hinweise

Teil I beinhaltet eine allgemeine Einführung in das Gebiet der Rechnernetze sowie Zwischenfragen und Übungsaufgaben.

Inhaltliche Schwerpunkte Teil I sind wie folgt:

- Historie und typische Übertragungsmedien (Bitübertragungsschicht, Schicht 1)
- Medienzugriff (Sicherungsschicht, Schicht 2, bzw. MAC-Teilschicht, d. h. sog. Medium Access Control)
- Rechnernetzarchitekturen, Netzhardware und Netzsoftware
- gängige Referenzmodelle (s. Abschnitte „ISO-Architektur“ und „Internet-Architektur“)
- Schichten 3–4: Vermittlungsschicht, Transportschicht
- Sicherheitsaspekte in Netzen
- Kurzfassung Rechnernetzapplikationen, Schichten 5–7 (weitere Details werden im Teil III vermittelt)
- Planung, Optimierung und Betriebssicherung im Lebenszyklus von Rechnernetzen.

Die weiterführenden Teile II und III behandeln konkrete aktuelle Rechnernetztechnologien und verteilte Anwendungslösungen.

Inhaltsverzeichnis

Lernziele Teil I

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_1

1

Das Teil I hat als Ziel, den Studierenden die Grundlagen von Rechnernetzen und deren Anwendungen zu vermitteln.

Ausgehend von einer historischen Einführung werden die Probleme der Rechnervernetzung in abstrakter Form behandelt. Dabei wird der allgemeine Stoff weitgehend nach dem ISO/OSI-Referenzmodell geordnet, während die konkreteren Betrachtungen auf aktuelle Lösungen verweisen.

Speziell werden zunächst die Grundbegriffe wie Rechnernetzdienste und –protokolle besprochen und die Grundarchitektur des Internets vorgestellt.

Danach werden die wichtigsten Rechnernetzprobleme behandelt. Für konkrete Realisierungen wird auf den Inhalt der Teile II und III verwiesen.

Die Autoren verweisen an bestimmten Stellen auf das ausführliche und praxisnahe Buch von A. Tanenbaum [17] sowie auf den Wissensbestand Skripte LS Rechnernetze an der TU Dresden [16].

Die begleitenden Aufgaben haben zum Teil das Ziel, dass die Studierenden eine relative Sicherheit bei der Lösung einfacher Probleme bzgl. der Rechnernetze und der Datenübertragung erreichen. Bevor Sie das Studium der Teile II und III beginnen, sollten Sie alle Aufgaben des Teiles I gelöst haben und selbstständig die Lösung ähnlicher Probleme beherrschen.

Zusätzlich werden praktische Aufgaben und begleitende Musterlösungen in einem separaten Übungsbuch angeboten. Teilweise fußt der Inhalt der Studienhafte auf didaktisch bewährten Übungsmaterialien der TU Dresden und der BA Dresden (Studienakademie Sachsen). Für wertvolle Anregungen danken die Autoren besonders den Kollegen Prof. Dr. rer. nat. habil. Dr. h. c. Alexander Schill, Dr. habil. J. Spillner und Dr.-Ing. M. Feldmann.

WISSEN:
Die Studierenden erhalten zunächst im Teil I eine Einführung in das Wissenschaftsgebiet der Rechnernetze. Die aktuellen Vorstellungen des Standes der Technik, der Internetstandards, der Nutzung mobiler Netzwerke und verteilter Rechnernetzanwendungen stehen in den Teilen II und III im Mittelpunkt.

Die Studierenden werden durch das Studium aller drei Teile befähigt, zu Entwicklungstrends von Rechnernetzarchitekturen und Verteilten Systemen und der damit verbundenen Probleme Stellung nehmen zu können, sowie die Datensicherheitsaspekte von Rechnernetzen und -anwendungen beurteilen zu können und auch moderne Lösungen zu Clouds, Parallel und Fog Computing, IoS/IoT zu bewerten und auf der Basis einer hinreichenden konzeptionellen Fundierung in die Praxis umzusetzen.

Historie

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_2

2.1 Programmierbare Rechenautomaten

Die Grundprinzipien der mechanischen Rechenmaschinen und erste praktisch nutzbare Prototypen wurden bereits im 17. Jahrhundert entwickelt

- 1623 Wilhelm Schickard
- 1645 Blaise Pascal
- 1673 Gottfried Wilhelm Leibniz.

Diese Maschinen wurden ständig weiter vervollkommnet und bis in die Mitte des 20. Jahrhunderts routinemäßig in Verwaltung, Ökonomie und Technik eingesetzt.

Mechanische Rechenmaschinen erlaubten die automatische Ausführung der arithmetischen Grundrechenarten. Sie verfügten aber in der Regel über keine internen Datenspeicher und konnten keine Algorithmen abarbeiten. Der menschliche Bediener musste entscheiden, in welcher Reihenfolge einzelne Rechenoperationen ausgeführt werden sollten. Danach gab er für jede Rechenoperation die Operanden ein, startete die Rechenoperation und schrieb evtl. Zwischen- oder Endresultate auf Papier. Besonders für routinemäßige Berechnungen, etwa von linearen Gleichungssystemen, war dies sehr mühevoll.

Deshalb gab es bereits im 19. Jahrhundert Ideen zur Entwicklung von programmierbaren Rechenautomaten (Computer). Charles Babbage konzipierte 1833 einen ersten Computer, die sogenannte „Analytical Engine", die ein mechanisches Rechenwerk aufwies und ein lochkartenbasiertes Steuerwerk, das die Organisation der Abarbeitung von Rechenoperationen übernehmen konnte. Ada Lovelace schuf für diese Maschine um 1842 die Grundlagen der Programmierungstechnik. Die „Analytical Engine" war leider aufgrund ihrer mechanischen Komplexität nicht funktionsfähig und die Erkenntnisse von Babbage gerieten in Vergessenheit. Um 1896 entwickelte der Amerikaner Herman Hollerith erfolgreich die elektromechanische Lochkartenverarbeitungstechnik. Diese Technik erlaubte die Massenverarbeitung von Daten für einfache statistische Verfahren und wurde für diese Anwendungen erst Mitte des 20. Jahrhunderts von modernen Computern verdrängt [15, 17, 18, 19].

Sehr bedeutsam waren die theoretischen Forschungen von Alan Turing, der 1936 die sogenannte Turingmaschine einführte, die als mathematisches Modell die Berechenbarkeit von Algorithmen untersuchen kann.

Im Verlauf des 2. Weltkriegs wurden leistungsfähige Rechenmaschinen entwickelt zur Unterstützung der Entschlüsselung von Funksprüchen und der Unterstützung kernphysikalischer Berechnungen. Als erster moderner Computer gilt der 1941 von Konrad Zuse entwickelte Rechner Z3, der allerdings noch

auf elektromechanischen Bauteilen beruhte und noch einige konstruktive Mängel aufwies.

Der erste Computer auf vollelektronischer Basis ENIAC (Electronic Numerical Integrator and Computer) wurde 1946 in den USA von J. Presper Eckert und John W. Mauchly für den Einsatz in der US-Armee vorgestellt. Er war für damalige Verhältnisse von gewaltiger Größe und Leistungsfähigkeit.

Die nachfolgenden Computer basierten auf dem theoretischen Architekturmodell (1944) nach John v. Neumann. Auf dieser Grundlage gab es eine bis heute andauernde permanente und kreative Weiterentwicklung der Computertechnik.

Moderne Systeme sind gekennzeichnet durch Verwendung hochintegrierter elektronischer Schaltkreise, hohe Taktraten und zeitparallele Ausführung mehrerer Operationen [19].

2.2 Mehrbenutzersysteme

Vor der Nutzung mikroelektronischer Schaltkreise war die Nutzung von Computern sehr kostenintensiv. Deshalb realisierte man in den 60er-Jahren Computersysteme, die mehreren Nutzern gleichzeitig zur Verfügung stehen sollten. Ein Computer besitzt dabei ein permanent installiertes Betriebssystem (Systemsoftware), das die Gesamtleistung des Computers auf mehrere (quasi-)zeitparallel arbeitende Prozesse aufteilt [18]. Jeder Prozess arbeitet dabei die Anweisungsfolgen eines Programmes ab. Derartige Systeme bezeichnet man als Multitasking-Systeme.

Die Erweiterung eines Multitaskingsystems zu einem Multiusersystem geschieht wie folgt [15, 18]:

Jeder (menschliche) Nutzer besitzt ein eigenes Gerät (Terminal) zur Ein-/Ausgabe von Kommandos u. a. Informationen. Diesem Terminal ist ein nutzerspezifischer Prozess zugeordnet, der das Starten von weiteren nutzerspezifischen Prozessen ermöglicht.

Damit mehrere Benutzer an einem Computersystem sinnvoll arbeiten können, muss das Rechnerbetriebssystem einige Bedingungen erfüllen:

- Anmelden zugelassener Nutzer
  (Starten einer „Sitzung“, meist über Angabe eines Login-Namens und eines Passwortes)
- Gewährleistung eines Speicherschutzes für die gestarteten Prozesse
- evtl. Kommunikation mit anderen Nutzern
- Abmelden von Nutzern und Freigabe belegter Ressourcen.

Die großen Computerfirmen der 60-er Jahre entwickelten jeweils eigene Konzepte, die wenig kompatibel waren (proprietäre Architekturen).

Eine Ausnahme bildete das Betriebssystem UNIX und dessen Derivate. Diese Betriebssysteme [18] realisieren ein leistungsfähiges Multiusersystem. Da der Quellcode im Wesentlichen an amerikanischen Universitäten entwickelt und als relativ offener Code bereitgestellt wurde, verbreiteten sich Unix-Betriebssysteme sehr schnell. Am bekanntesten ist Linux (1992, Linus Torvalds).

2.3 Rechnerverbundsysteme

Relativ frühzeitig (60-er Jahre) erkannte man auch, dass es sinnvoll ist, mehrere Rechner zu koppeln. Beispielsweise ist es effizient, wenn in einem Rechenzentrum sich die einzelnen Rechner auf bestimmte Aufgaben spezialisieren. So sollte der Rechner mit dem schnellsten Prozessor hauptsächlich rechenintensive Aufgaben realisieren, z. B. Simulationen u. a. wissenschaftliche Berechnungen und andererseits von einfachen Aufgaben wie Eingabe, Ausgabe und Drucken von Daten entlastet werden.

Wenn mehrere gekoppelte Rechner zusammenarbeiten, spricht man von einem Rechnerverbundsystem [17]. Der Nutzen des Rechnerverbundes ergibt sich aus

- Kommunikationsverbund
- Ressourcenverbund
- Steuerungsverbund.

Beim Kommunikationsverbund werden Nachrichten zwischen den Rechnern ausgetauscht, z. B. Kommandos zum Starten von Prozessen auf anderen Rechner oder zur Kommunikation zwischen den Bedienern des Rechnerverbundsystems.

Beim Ressourcenverbund erfolgt eine gemeinsame Nutzung von Hard- und Softwarekomponenten, z. B. von Druckern, von Datenträgern oder von Dateiinhalten.

Beim Steuerungsverbund erfolgt eine verteilte Verarbeitung auf mehreren Computern, z. B. bei der Automatisierung von Fabriken oder zur Reduktion der Verarbeitungszeit bei Simulationen.

Die frühen Rechenzentren waren mit Einzelrechnern ausgestattet. Um Kosten zu sparen, spezialisierte man die Rechner. Preiswerte Satellitenrechner übernahmen das Einlesen der Kundendaten und das Drucken der Ergebnislisten. Die eigentliche Verarbeitung erfolgte an Hochleistungsrechnern (Mainframes). Die Datenübergabe zwischen den Rechnern erfolgte durch den Austausch von Datenträgern, meist von Magnetbändern (◘ Abb. 2.1).

Diese Offline-Datentransporte waren personal- und zeitaufwendig. Deshalb wurden Geräte (Kanal-Kanal-Adapter) entwickelt, die einen direkten Datenaustausch (Online-Kopplung) zwischen den Rechnern unterstützten (◘ Abb. 2.2).

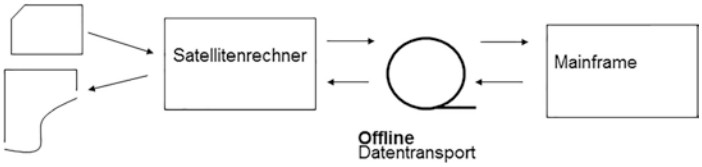


Abb. 2.1 Offline-Datenaustausch zwischen Computern

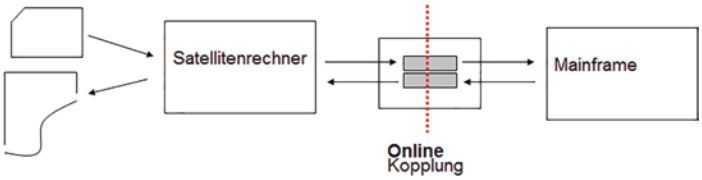


Abb. 2.2 Online-Datenaustausch zwischen Computern

Die Kanal-Kanal-Adapter (KKA) waren periphere Geräte beider Rechner. Die Treiberfunktionen waren „Prüfen, ob KKA-Puffer frei", „Schreiben" und „Lesen". Diese Funktionen wurden von speziellen Dienstprogrammen des Betriebssystems genutzt, z. B. für den Dateiaustausch zwischen den gekoppelten Rechnern. Die KKA und deren Treiber waren meist an einen Rechner- und Betriebssystemtyp gebunden. Geräte unterschiedlicher Hersteller konnten nicht gekoppelt werden.

Aufbauend auf dem Kommunikationsverbund wurden teilweise auch komplexe Rechnerverbundsysteme mit mehreren Computern und Ressourcen- und Steuerungsverbundfunktionen mit dem Ziel realisiert, den Auftragsdurchsatz zu erhöhen.

So wurden die Aufträge an Terminalrechnern entgegengenommen und den vorgesehenen Arbeitsrechnern zur Verarbeitung übergeben. Im Falle von Havarien wurden Ersatzrechner beauftragt, teilweise auch bei Überlastung von Arbeitsrechnern. Arbeitsteilig konnten Dienstleistungen anderer Rechner in Anspruch genommen werden.

In den 60-iger Jahren war die Computeranzahl sehr gering. Die Anfahrwege zu den Rechenzentren waren teilweise erheblich. Deshalb begann man dezentral einfache Terminalrechner aufzustellen und diese mit den Mitteln der Datenfernverarbeitung an die Rechenzentren anzubinden.

Die Datenübertragung erfolgte i. a. über das analoge Telefonnetz, sodass die Rechenzentren prinzipiell von überall her erreichbar waren. Die beteiligten Datenstationen wurden dabei unterteilt in eine Datenendeinrichtung DEE (bzw. DTE, Data Terminal Equipment) und eine Datenübertragungseinrichtung DUE (bzw. DCE, Data Communication Equipment). Die DTE sind dabei die Nutzcomputer der Anwender (Terminal,

Abb. 2.3 Datenfernverarbeitung

Großrechner) und die DCE i. a. gemietete Geräte, welche die Signalanpassung zwischen den computerspezifischen Signalen und den Signalformen des Übertragungsnetzes vornehmen. Die DCE werden auch als Modems (Modulation/Demodulation) bezeichnet (Abb. 2.3).

Dabei gab es große Probleme wegen der Inkompatibilität der verschiedenen Einzellösungen, außerdem waren die Übertragungseinrichtungen (Modems) und die Nachrichtenverbindungen langsam und nicht sehr zuverlässig.

Der Aufwand zum Aufbau von Rechnerverbundsystemen war erheblich und nur leistungsfähigen Rechenzentren möglich. Speziallösungen dominierten. Dabei wurden i. a. Rechner und Betriebssysteme nur eines Herstellers integriert. Meist wurden auch nicht alle Verbundfunktionen realisiert.

2.4 Frühe Rechnernetzarchitekturen

2.4.1 Sicherungsprotokoll HDLC

Das Protokoll HDLC (High-Level Data Link Control) ist ein von der ISO normiertes Netzwerkprotokoll, das auf dem von der Fa. IBM in den 60er-Jahren entwickelten SDLC-Protokoll basiert. Es wurde zunächst in Systemen der Datenfernverarbeitung implementiert und wurde auch später in andere Netzarchitekturen integriert (ISO, ITU, DoD). Außerdem diente es als Ausgangsbasis zur Entwicklung anderer Protokolle, z. B. des häufig verwendeten PPP-Protokolls (Point-to-Point Protocol, s. ► Abschn. 6.1.3).

HDLC stellt ein Protokoll für die Übertragung von Bitströmen über Punkt-zu-Punkt-Verbindungen dar und unterstützt sowohl 2-Punkt-Verbindungen als auch Baumstrukturen. HDLC kann in zwei Verwendungsmodi betrieben werden [3, 4, 16, 17]:

- NRM (Normal Response Mode)
  Eine privilegierte Primärstation regelt die Übertragung. Dies wurde vor allem für die Ansteuerung entfernt aufgestellter Terminals genutzt.
- ABM (Asynchronous Balanced Mode)
  Alle verbundenen Partnerstationen sind gleichberechtigt.

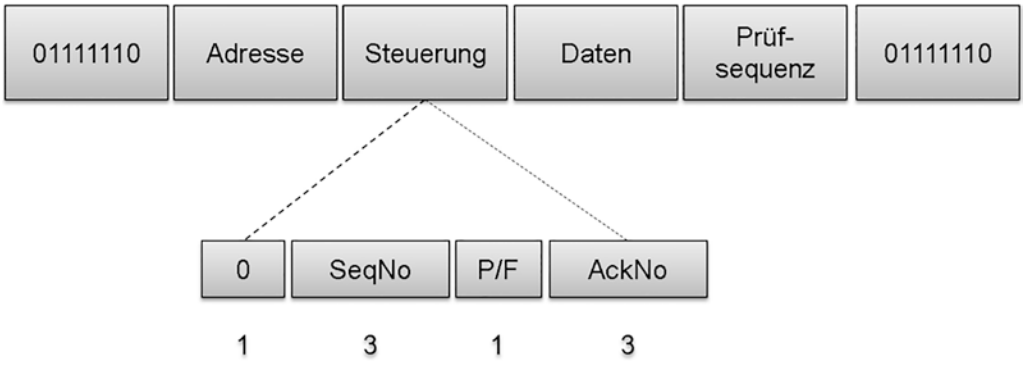
Die physisch übertragenen Nachrichten werden als Rahmen (Frames) bezeichnet. Die Frames besitzen Begrenzerkennungen zur Anfangs- und Enderkennung (Synchronisation).

Ein regulärer HDLC-Rahmen enthält zwei Framebegrenzer mit der Binärsequenz „01111110“ (8 Bit). Weitere Frameparameter sind in ◘ Abb. 2.4 aufgeführt:

Frameaufbau:
- Startbegrenzer (8 Bit)
- Adresse (8 Bit)
- Steuerfeld (8 Bit) mit
  SeqNo = Sendeframenummer 0…7
  P/F = Poll/Final für Polling-Steuerung;
  AckNo = Quittungsnummer 0…7 für Kommunikationspartner
  (Piggyback-Bestätigung, erfordert keine Extranachricht)
- Nutzdaten (variable Länge)
- Prüfsequenz nach CRC-16, die über den Frameinhalt gebildet wird.
- Endbegrenzer (8 Bit)

Inhaltlich ist HDLC ziemlich komplex. Es gibt mehrere Rahmenarten:
- Informationsrahmen
- Überwachungsrahmen (Receive (not) Ready, Reject (go-back-n), Selective Reject)
- Nicht nummerierte Frames (Steuerung, Verbindungsverwaltung, Polling).

Da in HDLC beliebige Bitfolgen übertragen werden dürfen, muss verhindert werden, dass im Datenteil die „verbotene“ Bitfolge des Endebegrenzers auftritt. Dies geschieht durch das sogenannte Bitstuffingverfahren.



◘ **Abb. 2.4** Rahmenformat für HDLC

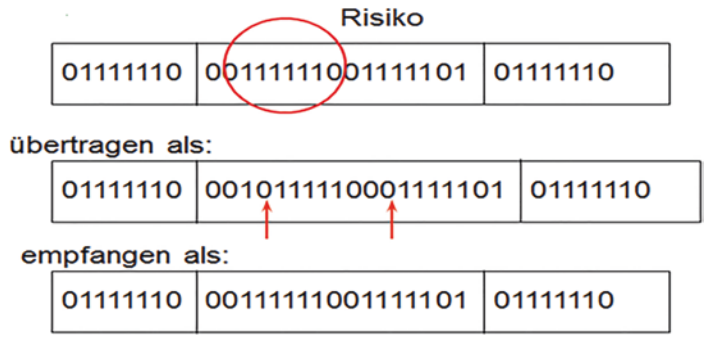


Abb. 2.5 Bitstuffing bei HDLC

Dieses Verfahren läuft folgendermaßen ab (Abb. 2.5):

- Der Sender fügt (hardwaremäßig unterstützt) nach jeder fünften „1“ in den Nutzdaten jeweils eine „0“ ein.
- Der Empfänger prüft im Datenteil auf die Sequenz „0111110“ und entfernt (hardwaremäßig unterstützt) die letzte Null der Sequenz.

Hinweis: Beim Endbegrenzer erkennt der Empfänger nicht „0111110“ sondern „01111110“. Dadurch wird das Ende korrekt erkannt.

Zur Zeit der Entwicklung von HDLC wurden meist analoge Telefonleitungen für die Übertragung genutzt. Vorteilhaft war deren problemlose Verfügbarkeit. Allerdings sind analoge Telefonleitungen stark störbehaftet, was zu Fehlern in den Nutzdaten an der Empfängerseite führt. Um diese Fehler zu erkennen enthält ein HDLC-Frame eine 16-Bit-Prüfsequenz über den Frameinhalt. Die Prüfsequenz wird vom Sender berechnet und in den Frame eingefügt. Der Empfänger berechnet die Prüfsequenz erneut und bei Nichtübereinstimmung mit der empfangenen 16-Bit-Sequenz im Frame wird ein Übertragungsfehler erkannt.

Genauere Informationen zur Fehlererkennung und -korrektur finden Sie im ▶ Abschn. 3.1.3.

2.4.2 IBM SNA

Die Firma IBM dominierte bis in die 70er Jahre den gesamten Datenverarbeitungsmarkt und beherrscht auch heute noch den Markt für Großrechner. Frühzeitig führte IBM Datenfernverarbeitungstechnologien für die IBM-Gerätetechnik ein. Später wurde diese zu einer Rechnernetzarchitektur SNA (Systems Network Architecture) weiterentwickelt.

SNA-Netze besitzen eine relativ zentralistische Konzeption. Die Hauptaufgabe besteht in der Verbindung von Rechenzentren

(mit IBM-Rechnern) und in der Bereitstellung dezentraler Zugriffsmöglichkeiten auf die zentralen Großrechner. Nachteilig ist, dass die SNA-Architektur nicht herstellerunabhängig ist.

Rechnerverbundsysteme nach SNA-Modell besitzen eine logische 6-Schichten-Architektur.

- Application
- Presentation Services
- Data Flow Control
- Transmission Control
- Path Control
- Data Link Control.

Die unterste Schicht (Date Link Control) realisiert die Steuerung des Datenstroms auf den Verbindungsleitungen zwischen den Computern. In der darauf aufsetzenden Path-Control-Schicht werden Übertragungsnachrichten für die Übertragung über die Data-Link-Control-Schicht aufbereitet. In der Transmission-Control-Schicht erfolgt eine Steuerung des Datenflusses mit dem Ziel, eine zuverlässige Übertragung zwischen Quell- und Zielrechner zu erreichen und sowohl die Übertragungswege als auch den Zielrechner nicht zu überlasten. Die Data-Flow-Control-Schicht unterstützt die Zusammenarbeit zwischen Anwendungsprozessen über eine sogenannte Sitzungssteuerung und die Darstellungsschicht (Presentation Services) gestattet die Zusammenarbeit von Prozessen, die unterschiedliche Datenformate verwenden.

In der Anwendungsschicht befinden sich die eigentlichen Anwendungen, die die Dienste der darunterliegenden Schichten in Anspruch nehmen können.

Die SNA-Architektur hatte großen Einfluss auf die Diskussionen der Entwicklung des OSI-Referenzmodelles der ISO für herstellerunabhängige („offene“) Netzwerke.

Die kommerzielle Bedeutung dieser Rechnernetze war bis in die frühen 90-er Jahre sehr hoch, da in vielen wichtigen Wirtschaftszweigen, wie dem Bankwesen, die Massendatenverarbeitung auf IBM-Großrechnern erfolgte. Später erfolgte eine schrittweise Überführung der SNA-Netze in eine internetartige Architektur.

2.4.3 Novell Netware

In den 80-er Jahren entstanden die ersten lokalen Rechennetze (LAN), die meist einen Verbund sehr ressourcenschwacher Rechner (Clients) mit einem leistungsstärkeren Rechner (Server) realisierten.

Client und Server sind genaugenommen Anwendungsprozesse. Der Client erteilt Aufträge, der Server führt sie aus und

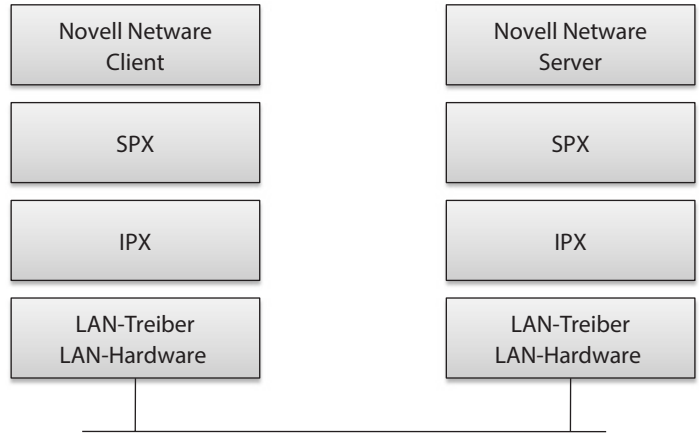


Abb. 2.6 Novell-Architektur

informiert den Client über das Ergebnis. Die Kommunikation erfolgt mithilfe der Rechnernetzsoftware über das sogenannte Netzwerkbetriebssystem.

Die größte Bedeutung erlangte die von der Fa. Novell entwickelte LAN-Architektur für Personalcomputer-Netze. In dieser Architektur erfolgt der Zugriff auf das Netz über einen LAN-spezifischen Treiber mit standardisierter Treiberschnittstelle. Darüber existieren zwei Schichten, welche die Protokolle IPX (Internetworking Packet Exchange) und SPX (Sequenced Packet Exchange) realisieren. IPX realisiert hierbei die Nachrichtenübertragung vom Quell- zum Zielrechner, wobei u. U. mehrere Zwischenrechner passiert werden müssen. SPX steuert die Nachrichtenübertragung und korrigiert IPX-Fehler. Auf diesen Schichten baut ein Netzwerkbetriebssystem Novell Netware auf. Das Betriebssystem der Arbeitsstationen wird um einen Novell-Client erweitert, mit dessen Hilfe die Dienste eines Novell-Serverrechners in Anspruch genommen werden können.

Die wichtigsten Anwendungsdienste von Novell-Netware-Netzen waren der Zugriff der Clients auf das Dateisystem des Fileservers und ein Druckservice für die Clients (Abb. 2.6).

2.4.4 ARPANET

Das historisch älteste Rechnernetz ist das 1969 in Betrieb genommene ARPANET. Vom US-Verteidigungsministerium wurde an die ARPA (Defense Advanced Research Projects Agency) die Entwicklung eines Rechnernetzes in Auftrag gegeben, das folgende Kriterien erfüllen sollte:

- Realisierung eines flächendeckenden Rechnernetzes (WAN),
- Anschluss beliebig vieler Computer beliebiger Architektur,
- automatische Nachrichtenverkehrsumleitung bei Verbindungsleitungsausfällen.

1972 gab es bereits hunderte Rechner in über 50 Rechenzentren, überwiegend auf dem US-amerikanischen Festland, aber auch in Hawaii und Westeuropa.

Hauptbestandteile des ARPAnet waren:

- **Arbeitsrechnersystem**
  Verbund leistungsfähiger Computer, die die eigentlichen Verarbeitungsfunktionen im Netz realisierten. Die wichtigsten Anwendungsdienste waren der Fernstart von Programmen, der Transfer von Dateien, die Bedienung entfernter Computer und ein E-Mail-System.
- **Netzwerksteuersystem**
  Eine Reihe von Routinen, die die Steuerung logischer Verbindungen zwischen den Endsystemen regelten. Für die Übertragung der Steuerinformationen wurde das Kommunikationssystem genutzt
- **Kommunikationssystem**
  Die Kommunikation zwischen den Endsystemen erfolgte nicht über das klassische leitungsvermittelte Telefonsystem sondern über ein Paketvermittlungsnetz. Dazu wurden Telefonleitungen gemietet und fest zwischen einfachen Vermittlungsrechnern IMP (Interface Message Prozessor) geschaltet. Diese nahmen von den Endsystemen partitionierte und einzeln adressierte Nachrichteneinheiten (Pakete) entgegen und sendeten diese über zumeist mehrere andere IMPs bis zum Zielrechner. Für jedes Paket wurde eine neue Wegeberechnung durchgeführt, sodass eine flexible Reaktion auf Netzprobleme möglich war.
- **Zugriffsysteme**
  System einfacher Zugriffscomputer (Terminals) ohne wesentliche eigene Verarbeitungskapazität. Die Terminals wurden i. a. über einen sogenannten TIP (Terminal Interface Processor) gebündelt an das Kommunikationssystem angeschlossen.

Ab ca. 1973 entwickelte sich aus dem ARPANET das Internet, in dem vor allem die zahlreichen UNIX-Minirechner der Universitäten weltweit verbunden waren. Technisch wurde vor allem das Kommunikationssystem im Wesentlichen übernommen, so sind z. B. die IMPs die Vorläufer der Router im Internet.

2.5 Zwischenfragen/Übungsaufgaben

2.5.1 Rechnerverbundsysteme

a) Was versteht man unter den Verbundfunktionen „Kommunikationsverbund“, Ressourcenverbund“ und „Steuerungsverbund“?
b) Benennen Sie zu den obigen Verbundsystemen jeweils ein Beispiel und diskutieren Sie die Vorteile.

2.5.2 Frühe Rechnernetzarchitekturen

a) Vergleichen Sie die proprietären Rechnernetzarchitekturen „Novell Netware“ und „IBM SNA“.
b) Charakterisieren Sie die Architektur des „ARPAnet“.

Übertragungsmedien und Medienzugriff

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_3

3.1 Medien

3.1.1 Ausgewählte Medien

Die Problematik wird in diesem Teil nur kurz angesprochen und in den weiteren Teilen vertieft.

Zur Übertragung von Informationen ist jedes Medium geeignet, das es gestattet, physikalische Eigenschaften in Raum und Zeit weiter zu transportieren [17].

Beispiele für Übertragungsmedien und deren ausgenutzte physikalische Eigenschaften sind:

Luft Schall - (Luftdruckschwankungen)
elektromagnetische Wellen (Frequenz-, Phasen-, Amplitudenwechsel)
elektrische Kabel - Impulse (Spannungswechsel)
Lichtwellenleiter - Impulse (Helligkeitswechsel)

Weitere Details zu den Übertragungsmedien, strukturierter Verkabelung finden Sie in Teil II.

3.1.2 Signale und nachrichtentechnische Kanäle

In unseren Teilen beschränken wir uns auf digitale Übertragungen. Zunächst soll kurz der Unterschied zwischen Information und Signal erläutert werden.

Eine Information ist immer mit einer semantischen Bedeutung behaftet und wird in einer festgelegten abstrakten Form (abstrakte Syntax) notiert. Zur konkreten Bearbeitung muss die abstrakte Syntax in einer physikalischen Darstellung (lokale Syntax) vorliegen. Die abstrakte Syntax einer Information wird i. a. in einer Programmiersprache beschrieben, z. B. die Definition einer ganzen Zahl mit dem Wert „1024“. Die lokale Syntax des Computers beschreibt dann die Realisierung der Speicherung, z. B. eine binäre Darstellung in einem Speicherwort von 64 Bit, beginnend mit dem höchstwertigen Bit.

Für eine Nachrichtenübertragung werden die Nachrichteninhalte in eine Folge von Signalen s(t) umgewandelt (kodiert). s(t) beschreibt dabei den zeitlichen Verlauf einer Eigenschaft des Übertragungsmediums. Die Signale breiten sich räumlich aus von der Nachrichtenquelle bis zur Nachrichtensenke (Übertragungskanal).

- **Modell des digitalen Nachrichtenkanals**

Abb. 3.1 zeigt als Beispiel die Umwandlung von Bitfolgen in eine Folge von elektrischen Impulsen, die über ein Kabel übertragen werden. Dabei wurde eine einfache Kodierung gewählt:

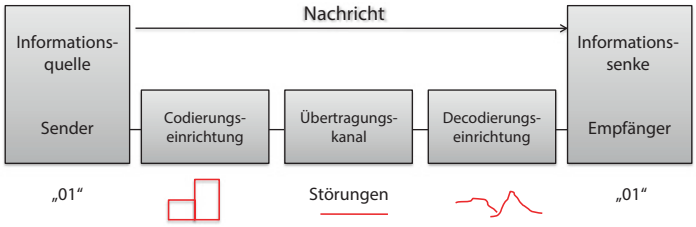


Abb. 3.1 Modell des digitalen Nachrichtenkanales

- Rechteckimpulse mit einer festen Impulsdauer T
- zwei mögliche Amplituden A0 (niedrig) und A1 (hoch) „0“ wird kodiert mit einem Impuls der Amplitude A0 und „1“ mit einem Impuls der Amplitude A1.

Im Übertragungskanal werden die Signale gedämpft (Amplitudenreduktion wegen Energieverlust), gestört (Fremdeinwirkung) und auch verzerrt (veränderte Signalform). Dies bedeutet, dass beim Empfänger nicht die Signalfolge s(t) ankommt, sondern eine veränderte Signalfolge s´(t).

Beim Eintreffen der Signalfolge s´(t) beim Empfänger wird diese dekodiert, d. h. als Bitfolge im Speicher des Zielrechners abgelegt. Wenn die im Kanal auftretenden Störungen nicht zu groß sind, stimmen die Bitfolgen im Quell- und Zielrechner überein, d. h. es gibt keinen Informationsverlust trotz auftretender Störungen.

Man kann mithilfe der Fourieranalyse zeigen, dass die Signalverformungen beim Passieren eines Übertragungskanales durch die Frequenzabhängigkeit der Signaldämpfung verursacht werden. Bei einer Dämpfung von Null ist das empfangene Signal s´(t) identisch mit dem Sendesignal s(t), bei einer frequenzunabhängigen Dämpfung ergibt sich $s'(t) = k * s(t)$ mit $0 < k < 1$.

Die Signaldämpfung ist definiert als Verhältnis von Sendeleistung und Empfangsleistung (dimensionlos). In der Praxis benutzt man vorwiegend die logarithmierte Dämpfung (Einheit dB bzw. Dezibel).

$$D_{log} = 10 \cdot \log \left(\frac{\text{Sendeleistung}}{\text{Empfangsleistung}} \right) \tag{3.1}$$

In vielen Fällen gibt es aber eine frequenzabhängige Dämpfung, z. B. bei einem sogenannten Bandpass (s. Abb. 3.2). Bei diesem darf nur ein eingeschränkter Frequenzbereich B zwischen einer unteren Frequenz f_u und einer oberen Frequenz f_o genutzt werden. Deshalb wird das Signal außerhalb dieses Bereiches stark gedämpft, sodass die Signalleistung auf den

zugelassenen Bereich B konzentriert wird. Die Darstellung der Übertragungsfunktionen Dämpfung und Leistungsdichte in ◘ Abb. 3.2 ist rein qualitativ. Detailliertere Betrachtungen zu diesen Funktionen finden Sie in Teil II.

Für den bandbreitenbegrenzten Nachrichtenkanal gilt das folgende Gesetz (Nyquist-Theorem):

$$SR < 2 * B \tag{3.2}$$

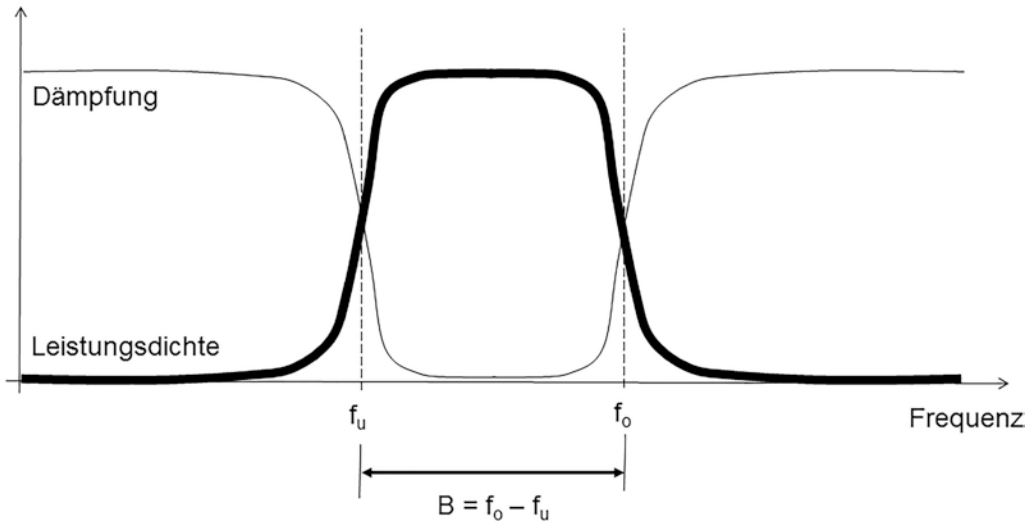
wobei B die Bandbreite des Kanals darstellt, gemessen in Hz, und SR die Schrittrate (Signale pro Zeiteinheit). Die Schrittrate wird gelegentlich auch als Baudrate bezeichnet (gemessen in Bd).

Im Beispiel der ◘ Abb. 3.1 haben wir eine binäre Kodierung gewählt, d. h. ein Signal mit zwei verschiedenen Werten (2-stufig). In diesem Fall wird mit einem Signal genau ein Bit transportiert (Binärkanal). Für den Binärkanal gilt, dass die Datenrate, gemessen in Bit/s, gleich der Schrittrate ist.

Es ist aber auch möglich, mehrstufige Signale zu verwenden. Beispielsweise kann man für den Fall von 4 Stufen (bezeichnet mit S0, S1, S2 uns S3) mit einem Signal zwei Bit transportieren

- Signal mit Wert S0 Bitfolge „00“
- Signal mit Wert S1 Bitfolge „01“
- Signal mit Wert S2 Bitfolge „10“
- Signal mit Wert S3 Bitfolge „11“.

Entsprechend kann man mit einem 8-stufigen Signal drei Bit transportieren, mit einem 16-stufigen Signal vier Bit, …, mit einem 1024-stufigen Signal zehn Bit. Allgemein gilt, dass der



◘ **Abb. 3.2** Übertragungsfunktionen eines bandbreitenbegrenzten Kanals

Informationsgehalt I eines Signales, gemessen in Bit/Signal, gleich dem dualen Logarithmus der Stufenzahl des Signales ist.

$$I = ld\ (S) \tag{3.3}$$

Die für die Praxis interessante Größe der Datenrate, gemessen in Bit/s, ergibt sich dann zu:

$$DR = SR * I \tag{3.4}$$

bzw. nach Kombination mit dem Nyquisttheorem zu:

$$DR = SR * ld\ (S) \tag{3.5}$$

Beispiel 3.1

Es soll für das in ◘ Abb. 3.1 diskutierte Beispiel berechnet werden, wieviel Bandbreite bei einer Impulsdauer von T = 10 ns gewährleistet sein muss und wie hoch die Datenrate bei Verwendung 16-stufiger Signale ist.

–	Die Schrittrate beträgt SR = 1/T	SR = 1/T = 100 MBd.
–	Aus dem Nyqist-Theorem folgt B > SR/2	B > SR/2 > 50 MHz.
	Die Datenrate beträgt DR = 10^8 * ld(16) Bit/s	DR = 10^8 * ld(16) Bit/s = 400 MBit/s

Rein formal beschränkt das Nyquist-Theorem nicht die erzielbare Datenrate, wenn es keine Obergrenze für die Stufung der Signale gibt. In der Realität wird diese Obergrenze aber durch das sogenannte Rauschen gesetzt. Unter Rauschen versteht man Störeinflüsse, die ein Signal in nicht vorhersehbarer Weise verfälschen und nur stochastisch behandelbar sind. Rauscheinflüsse können beispielsweise durch elektromagnetische Störquellen in der Nachbarschaft eines Kanales entstehen.

Eine wichtige Größe ist der sogenannte Signal-Rauschabstand SNR (Signal-to-Noise-Ratio), der durch das Verhältnis der Nutzleistung des Signales und der Störleistung des Rauschsignales definiert ist:

$$SNR = P_{Nutzsignal} / P_{Rauschsignal} \tag{3.6}$$

bzw. gemessen in Dezibel (verzehnfachter dekadischer Logarithmus von SNR)

$$SNR_{DB} = 10 * \log\ (SNR). \tag{3.7}$$

Für den rauschbehafteten Übertragungskanal ergibt sich die Datenrate nach folgendem Gesetz (Nyquist, Shannon, Raabe, Whittaker, Kotelnikow):

$$DR < B * ld(1 + SNR). \tag{3.8}$$

Die Anwendung der Formeln (3.5) und (3.8) kann zu unterschiedlichen Obergrenzen für die erzielbare Datenrate führen!

Dann gilt der kleinere der beiden Werte:

$$DR < \min (2 * B * \text{ld } S, B * \text{ld } (1 + SNR)) \tag{3.9}$$

3

Beispiel 3.2

Wir berechnen für das modifizierte Beispiel 3.1 die max. erzielbare Datenrate bei einer Kanalbandbreite von 70 MHz und für eine SNR von 7.

$$\mathbf{DR} < 70 * 10^6 * \text{ld } (1 + 7) \text{ Bit/s} < 210 \text{ MBit/s}$$

Dies ist ein Widerspruch zur Datenrate von 400 MBit/s im Beispiel 3.1. Wegen des hohen Rauschens ist eine Signalstufung von 16 nicht erreichbar, da sonst die Fehlerquote beim Dekodieren des Empfangssignales zu groß ist.

Eine Lösung kann in der Verwendung einer reduzierten Signalstufung von 4 bestehen. Dann ergibt sich eine Datenrate von 200 MBit/s.

Die sogenannte Spektraleffizienz SE ist definiert durch:

$$SE = DR/B. \tag{3.10}$$

Die SE beschreibt, wie gut das im Nachrichtenkanal zur Verfügung gestelltes Frequenzband (Spektrum) ausgenutzt wird.

Die einfachste Kodierung erreicht man mit einem NRZ-Binärkode (Non Return To Zero). Dabei wird je nach Bitwert der Signalpegel auf „0“ oder „1“ gesetzt (s. ◘ Abb. 3.3). Ein derartiger Kode ist jedoch nicht für längere Bitfolgen geeignet, da die Synchronisation nicht gewährleistet werden kann. Beispielsweise müsste man eine Folge von 28 Nullen sicher von einer Folge von 29 Nullen unterscheiden können. Dies überfordert die Genauigkeit von Systemuhren.

Ein besser geeigneter Kode ist der sogenannte Manchesterkode (s. ◘ Abb. 3.4) bei dem eine logische XOR-Verknüpfung von Bitfolge und Zeittakt erfolgt. Im Ergebnis werden für jedes Bit zwei Signale mit unterschiedlichen Pegeln übertragen, z. B. für Bitwert „1“ erst Pegel hoch, dann Pegel niedrig und für Bitwert „0“ erst Pegel niedrig, dann hoch. Der Manchesterkode hat sehr gute Synchronisationseigenschaften und eignet sich zum Übertragen längerer Bitfolgen. Allerdings verschenkt er 50 % der Bandbreite für die Synchronisation und dies ist uneffektiv.

◘ **Abb. 3.3** NRZ-Binärkodierung

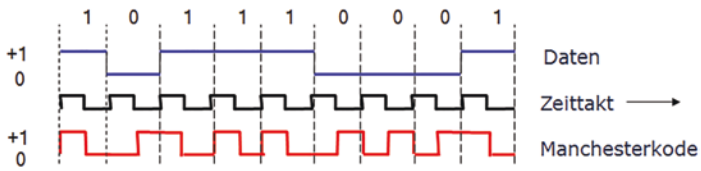


Abb. 3.4 Manchesterkodierung

In Hochleistungsnetzen werden effektivere Kodes eingesetzt, z. B. PAM-16 für die 10-Gigabit-Ethernettechnologie. Dabei kann ein Signal 16 verschiedene Werte annehmen, also vier Bit übertragen. Die Synchronisation wird über die Verwendung sogenannter Blockkodes erreicht. Dabei werden jeweils n Bit gepuffert und durch m Signalen ausgegeben. Die Zuordnung von Bitfolgen zu Signalfolgen wird so gestaltet, dass keine langen Folgen von Signalen mit gleichem Pegel entstehen.

3.1.3 Übertragungsfehler: Erkennung und Korrektur

Bei der Übertragung von Signalen über ein Medium treten mitunter folgende Probleme auf:

- Verfälschungen durch thermisches Rauschen
- Störspannungen durch Induktionseinflüsse von „benachbarten" Signalströmen
- frequenzabhängige Verzerrungen etc.

Übersteigen die Störungen ein zulässiges Maß, werden die übertragenen Signale beim Empfänger nicht korrekt dekodiert [4, 6, 17, 16].

In der Praxis werden nicht einzelne Signale sondern strukturierte Signalfolgen gesendet, sogenannte Frames. Die einzelnen Signale dienen hauptsächlich der Übertragung von Anwenderinformationen, aber auch der Lösung übertragungstechnischer Probleme, z. B. der Frameanfangs- und Enderkennung und der Signalsynchronisation.

Signalverfälschungen können zum Verlust des Frames auf der physischen Ebene führen, z. B. wenn der Frameanfang nicht erkannt wird.

Problematischer sind Signalverfälschungen im Nutzinhalt des Frames. Diese kann zu Einzelbitfehlern und sogar Bündelfehlern in den Nutzdaten an der Empfängerseite führen.

Deshalb wird in modernen Übertragungsprozeduren eine Prüfsequenz zur Fehlererkennung für empfangene Nutzdaten in jeden Frame integriert (s. ► Abschn. 2.4.1 für HDLC-Prozedur).

Naheliegend für die Wahl der Prüfsequenz wäre eine Summierung über die einzelnen Oktetts (Bytes) des Nachrichteninhaltes.

Aus technischen und mathematischen Gründen nutzt man ein anderes Verfahren, das sogenannte Divisionsrestverfahren CRC (Cyclic Redundancy Check). Dabei wird der Frameinhalt durch ein sogenanntes Generatorpolynom dividiert und der erhaltene Divisionsrest dient als Prüfsequenz. Je höher der Grad n des Generatorpolynoms ist, umso besser ist die erreichte Prüfgenauigkeit. Man spricht deshalb auch von CRC-n-Verfahren.

Die CRC-Implementierung kann sehr effizient erfolgen, da sie mittels Schieberegistern in Hardware realisiert werden kann. Das CRC-Verfahren wird in sehr vielen LAN-Technologien genutzt. Wir führen an dieser Stelle die Generatorpolynome für das CRC-16-Verfahren von HDLC und das CRC-32-Verfahren bei den LAN nach IEEE 802.x an.

CRC-CCITT: $x^{16}+x^{12}+x^5+1$ - (HDLC-Prozedur)

CRC-32: $x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$ - (IEEE 802.x)

Der folgende Exkurs beschreibt das CRC-Verfahren im Detail (für Interessenten):

Exkurs

Für Interessenten erläutern wir an dieser Stelle, wie eine CRC-n-Prüfsumme im Detail ermittelt wird:

1. Der Frameinhalt wird als binäres Quellwort genommen und um n Binärstellen erweitert (Linksschieben um n Stellen). Dadurch ergibt sich das sogenannte binäre Arbeitspolynom.
2. Es wird eine ganzzahlige binäre Polynomdivision durchgeführt. Unser Arbeitspolynom wird durch das im Standard vorgegebene Generatorpolynom n-ten Grades geteilt. Die n-stellige Sicherungssequenz ergibt sich aus dem ganzzahligen binären Divisionsrest.
3. Das erweiterte Quellwort wird um diesen Rest ergänzt (Rest wird zum Wort addiert).
4. Das modifizierte Quellwort wird übertragen.
5. Nach dem Empfang kontrolliert der Empfänger die Prüfsequenz. Dazu wird das empfangene Wort (einschließlich der Prüfsequenz) durch das im Standard vorgegeben Generatorpolynom n-ten Grades dividiert.
6. Der Divisionsrest muss bei korrekter Übertragung den Wert 0 besitzen. Ist der Wert ungleich 1 liegt ein Übertragungsfehler vor.

[**Vermerk:**]
Binäre Division bedeutet lediglich Rechtsschieben um 1 Stelle und bitweises XOR bei führender „1"

Eine Fehlererkennung bedeutet noch keine Fehlerkorrektur.

Je nach Anwendung ist eine Fehlerkorrektur unbedingt erforderlich oder auch nicht. Zwei Beispiele sollen dies verdeutlichen.

Bei einem Dateitransfer ist es unbedingt erforderlich, dass die Dateikopie auf der Empfängerseite keinerlei Fehler oder Verluste

enthält. Scheitert die Übertragung eines Frames muss deshalb eine Übertragungswiederholung erfolgen.

Andererseits ist es evtl. sinnvoll bei der Übertragung eines Videostromes (seltene) Bitfehler zu tolerieren, da sich eine Übertragungswiederholung verfälschter Frames als Verschlechterung von Echtzeitparametern der Übertragung auswirkt (kurze Pause im Strom).

In der Regel wird heutzutage auf eine Fehlerkorrektur auf der physikalischen Ebene der Informationsübertragung verzichtet und diese Dienstleistung höheren Schichten der Rechnernetzsoftware überlassen.

Als Ausnahme soll an dieser Stelle kurz auf die Verwendung selbstkorrigierender Kodierung verwiesen werden. Diese sind in Spezialfällen sinnvoll, beispielsweise bei Übertragungen im Kosmos, bei denen Übertragungswiederholungen extremen Zeitverlust bedeuten.

Bei selbstkorrigierender Kodierung wird im Anwendungsteil die Information mit hoher Redundanz versendet. Die zugelassenen Codeworte unterscheiden sich dabei jeweils in mindestens n Bitpositionen (Hammingdistanz). Die redundante Information dient der eventuell erforderlichen Korrektur der empfangenen Nutzinformation.

Auszug aus der Fehlertheorie [17]:

- Verfälschungen der Signale sind im Kanal bei Frameübertragung möglich.
  Einzelbitfehler und Bündelfehler (mehrere Fehler in einer Bitfolge) können auftreten.
  Wahrscheinlichkeit, dass nur 1 Bit in Bitfolge verfälscht wird, ist am größten.
- Algorithmus sucht zuerst nach 1-Bit-Fehlern.
  - Ergibt sich aus der empfangenen Bitfolge eine zulässige Bitfolge, wenn man 1 Bit ändert?
  - Wenn ja, wird angenommen, dass ein Bit verfälscht wurde
  - Wenn nein, wird nach 2-Bit-Fehlern gesucht
- Algorithmus endet nach (n − 1) Schritten.

Beispiel 3.3

Erlaubt sind drei Codeworte A, B und C, die mit zwei Bit dargestellt werden könnten, aber in einer redundanten Form mit fünf Bit dargestellt werden.

- ***A = 00000***
- ***B = 00111***
- ***C = 11001***

Die Hammingdistanz d ergibt sich in diesem Beispiel zu d = 3, weil sich im Beispiel A und B in 3 Bitpositionen unterscheiden, A und C in 3 Bitpositionen und B und C in 4 Bitpositionen.

Problem:
Wenn sich die Bitfolgen in d Bitpositionen unterscheiden, dann kann bei diesem Fehler wieder eine gültige Bitfolge entstehen, d. h. der Fehler kann nicht erkannt werden!
Abhängig von der Hammingdistanz d

- kann erkannt werden, dass (Bitfehler) vorliegen, wenn weniger als maximal (d – 1) Abweichungen auftreten
- können Übertragungsfehler sogar korrigiert werden, wenn max. (d − 1)/2 (ganzzahlig aufgerundet) Abweichungen vorliegen.

Empfangene Worte ***Wi*** werden mit den Codeworten verglichen.

- ***W1*** = ***00010***
- ***W2*** = ***00111***
- ***W3*** = ***11011***

Ergebnis:
Am nächsten liegen das

- Wort W1 zum Codewort A (nur Einzelbitfehler)
- Wort W2 zum Codewort B (kein Fehler)
- Wort W3 zum Codewort C (nur Einzelbitfehler)

Es treten keine Mehrfachbitfehler auf, deshalb gute Erkennung und Korrektur.

3.2 Mehrfachzugriff auf Medien

3.2.1 Zugriffskonkurrenz

Ein besonders einfach zu nutzendes Medium ist eine Zweipunktverbindung, z. B. über ein elektrisches Kabel. Dabei unterscheidet man

- Simplexkanal
- Halbduplexkanal
- und Vollduplexkanal.

Beim Simplexkanal erfolgt eine Übertragung nur in einer Richtung, z. B. über eine Sendeader eines Kupferkabels. Ein Beispiel wäre das zyklische Senden einer Temperaturinformation an einen Verarbeitungsrechner. Bei einem Simplexkanal gibt es keine(!) Medienzugriffskonflikte.

Ein Dialog zwischen zwei Stationen ist nur über einen Duplexkanal möglich. Über einen Vollduplexkanal kann man zeitgleich in beide Richtungen senden, z. B. indem ein Kupferkabel für jeden der zwei Dialogteilnehmer eine Sende- und eine Empfangsader bereitstellt (◘ Abb. 3.5).

Auch bei einem Vollduplexkanal gibt es keine Medienzugriffskonflikte.

Schwieriger wird es, wenn nur eine Cu-Ader im Kabel existiert für die Kommunikation zwischen zwei Teilnehmern. Falls beide Stationen gleichzeitig senden, überlagern sich deren Signale (Kollision) und ein ordnungsgemäßer Empfang ist nicht möglich. Beim Halbduplexkanal wird das Problem überwunden durch eine Zugriffssteuerung, die zu einem konkreten Zeitpunkt nur einem Teilnehmer das Senden gestattet. Eine einfache Realisierung wäre, dass immer abwechselnd gesendet werden muss.

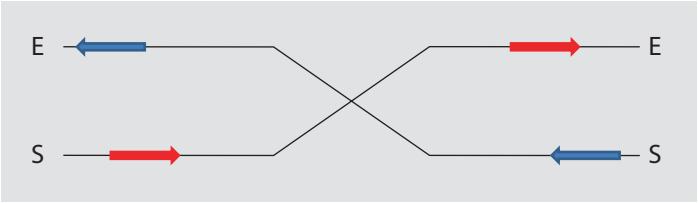


Abb. 3.5 Duplexübertragung in einem Overcross-Kabel

Wesentlich komplizierter wird die Problematik der Medienzugriffskonflikte, wenn mehr als zwei Teilnehmer ein(!) Medium nutzen wollen (Multiplexing). Dies ist beispielsweise der Fall, wenn in einem Raum mehrere Teilnehmer per Funk Informationen austauschen wollen. Es gibt zwei Lösungsarten zur Lösung des Problems

- deterministische Zugriffsteuerungen
- und stochastische Zugriffssteuerungen.

Beide Lösungen werden im Folgenden behandelt [17].

3.2.2 Deterministische Zugriffsverfahren

3.2.2.1 Zeitmultiplex

Beim Zeitmultiplex *(TDM – Time Division Multiplexing)* wird gesichert, dass zu einem Zeitpunkt nur ein Teilnehmer senden darf. Eine triviale Lösung für eine Zweipunktverbindung wurde bereits im ▶ Abschn. 3.2.1 vorgestellt.

Zeitmultiplexverfahren können auch bei mehr als zwei Teilnehmern eingesetzt werden. Jedem Teilnehmer werden individuell kurze Zeitschlitze (Time Slots) zugeordnet, in denen nur er senden darf. Damit Zeitmultiplex funktioniert, muss im System eine exakte Zeitsynchronisation gewährleistet sein.

Eine einfache Lösung besteht darin, dass der Zeitablauf für n Teilnehmer in Zyklen mit n Zeitschlitzen eingeteilt wird. Dann kann jede Station in ihrem Time Slot senden und muss dann $(n-1)$ Zeiteinheiten warten, bis sie weiter senden darf (s. Abb. 3.6).

Es gibt auch komplexere Lösungen, in denen die Zeitschlitze dynamisch zugeordnet werden (s. ATM-Netze [13, 16, 17]) und nicht jeder Teilnehmer gleich oft Time Slots erhält (s. Abb. 3.7).

3.2.2.2 Frequenzmultiplex

Beim Frequenzmultiplex *(FDM – Frequency Division Multiplexing)* wird das zur Verfügung stehende Frequenzband in mehrere Subbänder unterteilt, über die zeitgleich, aber mit geringerer Bandbreite gesendet werden kann. Die Subbänder

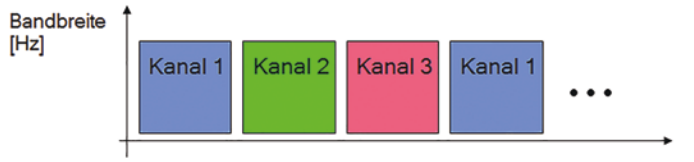


Abb. 3.6 Zeitmultiplexverfahren

Abb. 3.7 Statistisches oder dynamisches Zeitmultiplexverfahren

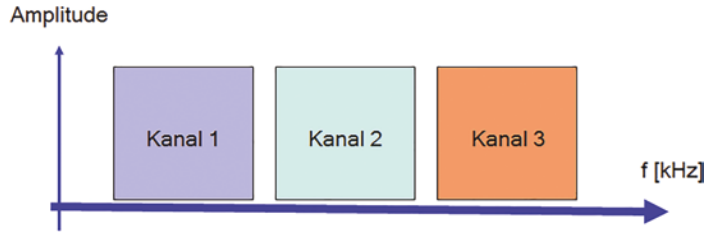


Abb. 3.8 Frequenzmultiplexverfahren

schließen nicht unmittelbar aneinander, sondern werden durch kleine Sperrbänder abgegrenzt.

Das Frequenzmultiplexprinzip illustriert Abb. 3.8.

Beispiele für Frequenzmultiplexing sind der klassische Rundfunk und die DSL-Verfahren.

Die als Wellenlängenmultiplexverfahren bezeichneten Multiplextechnologien für Lichtwellenleiter stellen im Grunde genommen auch eine Variante des Frequenzmultiplexes dar. Bei diesen werden Strahlen mehrerer Wellenlängen (Farben) zeitparallel über eine Faser übertragen. Wellenlängen können aber problemlos in Frequenzen umgerechnet werden.

3.2.2.3 Raummultiplex

Das Frequenzmultiplexverfahren ist für Funknetze mit hohen Teilnehmerzahlen und großen Ausdehnungen nur eingeschränkt nutzbar. Die Anzahl der zur Verfügung stehenden Funkfrequenzbänder ist beschränkt und eine Mehrfachnutzung von Frequenzen kann zu gegenseitigen Störungen durch Interferenz führen.

Einen Ausweg bietet das Raummultiplexverfahren *(SDM – Space Division Multiplexing)*.

Dabei wird ausgenutzt, dass die Signalenergie mit dem Abstand zur Antenne absinkt.

Innerhalb einer sogenannten Zelle wird jeweils eine Frequenz genutzt. Die Nachbarzellen müssen(!) andere Frequenzen nutzen, damit es keine Störungen an den Zellgrenzen gibt. Die Sendeleistungen sind so beschränkt, dass in einem gewissen Abstand von der Sendeantenne die Signalleistungen keine signifikanten Störungen verursachen. Ab diesem Abstand kann dann die gleiche Frequenz in einer anderen Funkzelle genutzt werden.

Wichtige Einsatzfelder für Raummultiplexverfahren sind die Mobilfunknetze, z. B. GSM und LTE.

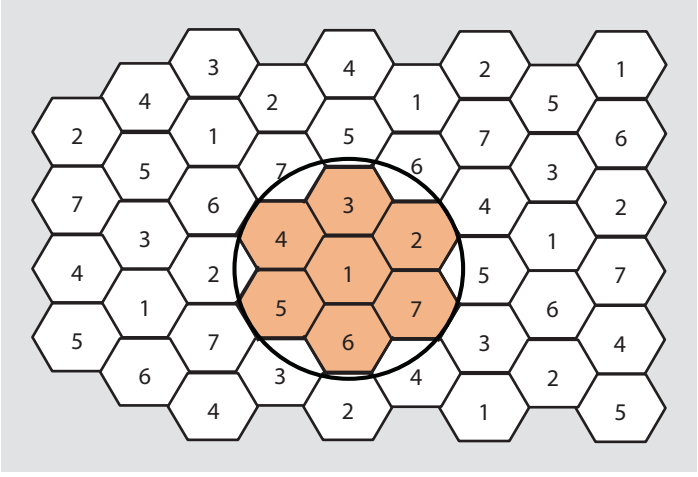
In ◘ Abb. 3.9 wird ein Raummultiplexsystem mit 7 unterschiedlichen Frequenzen dargestellt.

Raummultiplexverfahren finden neben der Nutzung in zellenorientierten Funknetzen auch Anwendung bei:

- kabelgebunden Techniken durch Verwendung mehrerer Kabeladern,
- Funkübertragungen durch Nutzung von Richtfunkstrecken.

3.2.2.4 Codemultiplex

Das Codemultiplexverfahren *(CDM – Code Division Multiplexing)* ist relativ kompliziert und soll an dieser Stelle nur grob vereinfacht dargestellt werden. Es ist ein modifiziertes Frequenzmultiplexverfahren, bei dem mehrere Teilnehmer gleichzeitig auf mehreren Frequenzen senden, aber mit unterschiedlichen Sendeleistungen und Signaldarstellungen, geregelt durch einen sogenannten Sendecode. Für unabhängige Beobachter ergeben



◘ **Abb. 3.9** Raummultiplex und Zellenstruktur

sich scheinbar sinnlose Summensignale. Bei Kenntnis des Sendecodes kann aber aus dem Summensignal die Sendeinformation extrahiert werden.

Codemultiplex wird z. B. bei der Mobilfunktechnologie UMTS eingesetzt. Dort dient es vor allem der Abhörsicherheit.

Weitere Details zu den Multiplexverfahren (u. a. OFDM – Orthogonal FDM) können Sie im Teil II finden.

3.2.2.5 Kombinationen verschiedener Multiplexverfahren

Es ist prinzipiell möglich, mehrere Multiplexverfahren zu kombinieren. Dies erfolgt z. B. bei den modernen Mobilfunktechnologien.

3.2.2.6 Master/Slave-Verfahren

Das Master/Slave-verfahren wird auch als Polling- bzw. Stationsabfrageverfahren bezeichnet. Das Prinzip besteht darin, dass eine privilegierte Station des Netzwerkes die anderen Stationen zunächst nach Sendewünschen abfragt und dann den Stationen nach einem vorgegebenen Algorithmus eine Sendeerlaubnis erteilt.

Derartige Verfahren werden vor allem bei Echtzeitproblemen eingesetzt, etwa in der Fertigungssteuerung eines Betriebes.

Ein einfaches Beispiel wäre das Abfragen von Sensoren in einer Chemiefabrik. Das Bedienpersonal arbeitet dabei oft in einer Systemwarte. Dort müssen alle relevanten Informationen zum Produktionsprozess verfügbar sein, um eine effiziente Steuerung des Produktionsablaufes zu gewährleisten. Das Problem besteht dabei darin, dass u. U. tausende von Sensoren nach verschiedenen Kriterien abgefragt werden müssen. So kann es bei einem kritischen Sensor (z. B. Kesseldruck) erforderlich sein, aller 10 Millisekunden die aktuellen Parameter zu ermitteln, bei anderen unkritischen Sensoren (z. B. Raumheizung) kann ein Abfragezyklus von 10 min ausreichen. Alarmsensoren (z. B. Feueralarm) werden gar nicht routinehaft abgefragt, aber sie müssen im Alarmfall sehr schnell Meldungen absenden können.

Mittels Master/Slave-Verfahren können derartige Probleme effizient gelöst werden. In der Regel ist eine individuelle Optimierung der Abfrageprioritäten und -reihenfolgen für jeden Anwendungsfall erforderlich.

Ein weiteres Echtzeitproblem ist die Sprachübertragung in WLAN nach 802.11. Bei hoher WLAN-Auslastung ist bei dem normalerweise verwendeten stochastischen Zugriffsverfahren CSMA/CA keine gute Sprachverständigung garantiert. Deshalb können die Accesspoints auch im Master/Slave-Modus arbeiten, der hier als PCF (Point Coordination Function) bezeichnet wird.

3.2.2.7 Tokenverfahren

Tokenverfahren sind derzeit nur in speziellen Netzwerken von Bedeutung. Da diese Verfahren aber eine theoretisch wichtige Medienzugriffstechnologie darstellen, werden sie in diesem Teil vorgestellt.

Ein Token ist eine Berechtigungsmarke zum Senden über das Sammelmedium. Sie ist zu einem Zeitpunkt nur einer Station zugeteilt. Diese darf dann eine vorgegebene maximale Zeitspanne THT (Token Holding Time) senden und muss danach das Senderecht weitergeben.

Tokenverfahren sind grundsätzlich für Echtzeitprobleme geeignet, da für jede Station eine maximale Wartezeit ((n − 1)*THT) auf das Senderecht angegeben werden kann. Meist ist die Wartezeit kürzer, da nicht jede Station ihr Senderecht wahrnimmt.

Tokenverfahren ähneln den Zeitmultiplexverfahren, jedoch sind die Zeitslots für das Senden flexibel (zwischen 0 … THT).

Weiterhin besitzen Tokenverfahren ein positives Hochlastverhalten. Prinzipiell kann eine 100 %-ige Auslastung erreicht werden.

- **Token Ring – IEEE 802.5**

Das Verfahren wurde ursprünglich 1984 von der Fa. IBM eingeführt. IEEE 802.5 erlaubt Prioritäten bei der Übertragung und hat gute Echtzeit- und Hochlasteigenschaften. Token Ring war bis Anfang der 90er-Jahre eine leistungsfähige LAN-Technologie mit Datenraten von 4 bzw. 16 MBit/s und ein starker Konkurrent für Ethernet-LAN. Danach erfolgten keine wesentlichen Weiterentwicklungen mehr und Token Ring wurde von Ethernet-LAN verdrängt. Wir behandeln die Technologie an dieser Stelle dennoch, um grundlegend die Tokenzugriffssteuerung zu erläutern.

IEEE 802.5 ist durch die Verwendung eines physischen Ringes gekennzeichnet (◘ Abb. 3.10). Als Medium waren Twisted-Pair-Kabel und auch Lichtwellenleiter vorgesehen. Jede Station besitzt eine Anschlusseinheit für den Ring, die jeweils eine Sendeeinrichtung S und eine Empfangseinrichtung E besitzt. Ein Rechner ist im Besitz des Senderechtes. Dieser sendet eine physische Nachricht (Frame), die aus einer Folge gerichteter Signale besteht. An der physisch nächsten Station empfängt die Anschlusseinheit ein Signal, regeneriert Signalamplitude und Signalform und sendet das regenerierte Signal weiter zum nächsten Rechner und so fort. Nach einem vollständigen Signalumlauf empfängt der Tokenbesitzer die umgelaufenen Signale und entfernt sie vom Ring.

Der Frameinhalt besteht aus einem Header, den Übertragungsdaten und einem Trailer. Im Header steht u. a. die

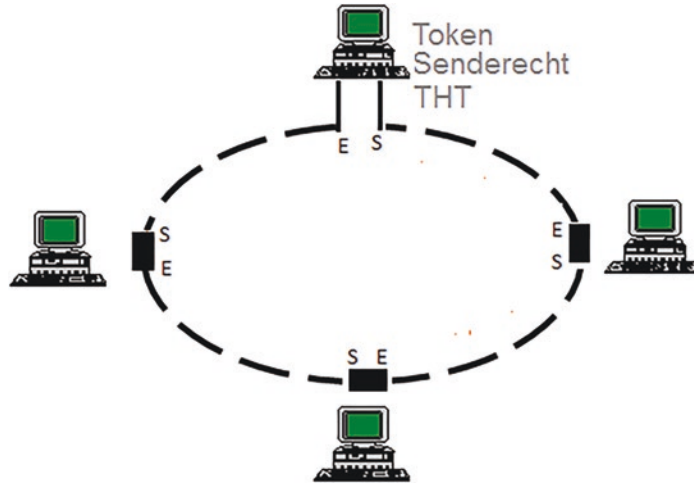


Abb. 3.10 Physischer Ring bei IEEE 802.5

Adresse des Zielrechners, der Trailer enthält eine Kontrollsequenz. Wie bereits erwähnt, läuft der Frame einmal über die volle Länge des Ringes. Beim Passieren einer Station prüft diese, ob der Frame an sie adressiert ist. Im positiven Fall fertigt die adressierte Station eine Kopie des Frameinhaltes an und veranlasst die Verarbeitung des Inhaltes. Außerdem setzt sie ein Quittungsbit im Trailer des weiterlaufenden Frames. Nach vollständigem Frameumlauf weiß dann der Tokenbesitzer, dass der Ring fehlerfrei arbeitet und dass der Empfängerrechner den Frameinhalt erhalten hat.

- **Token Bus – IEEE 802.4**

Diese Technologie wurde ursprünglich von der Fa. General Motors für die Fertigungssteuerung entwickelt. Token Bus ist heute nicht mehr aktuell, soll aber aufgrund seines originellen Konzeptes dennoch hier erwähnt werden.

Bei IEEE 802.4 wird das Tokenverfahren nicht über einen physischen Ring realisiert, sondern es wird ein logischer Ring über einem physischen Bus organisiert. Da bei der Tokenweitergabe kein physischer Nachfolger existiert, muss der „logische" Nachfolger explizit adressiert werden.

Token Bus besitzt die folgenden Charakteristika:

- Realzeitfähigkeit und Eignung für Hochlast
- Berücksichtigung von Prioritäten für den Medienzugriff
- Koaxialkabel oder Twisted-Pair-Kabel als Übertragungsmedium
- Datenrate 10 MBit/s
- Aufwändige Installation und Verwaltung
- Komplexe Protokolle für Aufnahme neuer Stationen in den logischen Ring, Abmelden von Stationen, Systemanlauf usw.

3.2.3 Stochastische Zugriffsverfahren

3.2.3.1 ALOHA und Slotted ALOHA

ALOHA ist ein theoretisch interessantes historisches Medienzugriffsverfahren und war ursprünglich durch das Satellitenpaketnetz ALOHAnet bekannt. Das ALOHA-Protokoll wurde erstmals 1971 an der Universität Hawaii eingesetzt [16, 17].

Ursprünglich ging es um ein unkoordiniertes (stochastisches) Wettbewerbsverfahren mit mehreren dezentralen Stationen. Die Kommunikation erfolgte über eine Zentrale (oft durch Satelliten realisiert). Für Uplink- und Downlink-Modi wurden unterschiedliche Frequenzen verwendet (◘ Abb. 3.9):

- f1: 407,35 MHz (Stationen => Zentrale, Uplink)
- f2: 413,475 MHz (Zentrale => Stationen, Downlink).

Ablauf des Medienzugriffs beim Verfahren pure ALOHA

1. Jede Station sendet einen Frame über f1, wenn sie Sendedaten vorrätig hat.
2. Im positiven Fall empfängt die Zentrale den Frame korrekt und sendet ihn über die Frequenz f2 weiter zur Empfangsstation.
   Im negativen Fall wird der Frame nicht korrekt empfangen, z. B. weil mehr als eine Station gleichzeitig sendet (Kollision). Dann wird der kollidierte Frame vernichtet und nicht weitergegeben.

ALOHA gibt keine Garantie, dass ein Frame erfolgreich übertragen wird. Deshalb werden alle Übertragungen quittiert. Erst nach positivem Erhalt der Quittung ist gesichert, dass der Empfänger die Nachricht erhalten hat.

Die Wahrscheinlichkeit einer Kollision bei der Übertragung kann modellmäßig berechnet werden. Danach bietet Pure ALOHA brauchbare Übertragungseigenschaften bis zu max. etwa 18 % des Kanaldurchsatzes. Wird die Last weiter erhöht, treten gehäuft Kollisionen auf und der Kanaldurchsatz sinkt bis zur Unbrauchbarkeit.

Eine erhebliche Verbesserung konnte durch das Verfahren Slotted ALOHA erreicht werden (Brauchbarkeit bis max. etwa 36 % des Kanaldurchsatzes). Bei Slotted ALOHA sendete die Zentrale zusätzlich ein Taktsignal zur Einteilung der Zeit in Zeitabschnitte (Slots). Die Teilnehmer dürfen nur am Beginn eines neuen Slots senden, Dadurch wird die Kollisionswahrscheinlichkeit etwa halbiert.

Die Erfahrungen beim Einsatz des ALOHA-Verfahrens gingen in die verbesserten Verfahren CSMA/CD und CSMA/CA ein.

3.2.3.2 CSMA/CD-Verfahren

Das CSMA/CD-Verfahren wurde vor allem bekannt dadurch, dass es in den ersten LAN vom Ethernet-Typ zum Einsatz kam.

Zunächst etwas zur Terminologie [17]:

- MA bedeutet „Multiple Access" und damit, dass ein Mehrfachzugriff auf ein Medium unterstützt wird.
- CS bedeutet „Carrier Sense", das Abhören vor dem Senden. Ein Sender beginnt nur mit einer Übertragung, wenn das Medium frei ist, bzw. wenn kein anderer Teilnehmer sendet. Eine Sendekollision wird dadurch erheblich reduziert, aber nicht komplett verhindert.
- CD bedeutet „Collision Detection". Damit ist gemeint, dass während der Frameübertragung weiter das Medium abgehört wird, ob es doch zu einer Kollision gekommen ist. Dann wird die Frameübertragung abgebrochen und nach einer stochastisch berechneten Wartezeit wiederholt. Als Verlustzeit geht dann nicht die Übertragungszeit ein, sondern nur die wesentlich kürzere Zeit von Sendebeginn bis zur Kollisionserkennung.

Beim ALOHA-Verfahren konnte man Carrier Sense nicht realisieren. CS funktionierte nicht, weil Richtfunk bei den Satellitenstrecken verwendet wurde und damit etwa nicht festgestellt werden konnte, ob etwa zur gleichen Zeit von einer Nachbarinsel zum Satelliten gesendet wurde. Ebenfalls war die Implementierung einer Kollisionserkennung aufgrund der großen Entfernungen zum Satelliten erschwert.

Der hinter CSMA/CD stehende Ablaufalgorithmus ist in ◘ Abb. 3.11 dargestellt.

3.2.3.3 CSMA/CA-Verfahren

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) ist eine weitere Modifikation des CSMA-Verfahrens und besonders in Funknetzen (WLAN) verbreitet.

Das Verfahren CSMA/CD ist in den Funknetzen nicht realisierbar [17, 13], da Kollisionen nicht immer erkannt werden können.

Unter CA („Collision Avoidance" versteht man ein Verfahren, Kollisionen möglichst zu vermeiden. Der wesentliche Unterschied zu CD besteht darin, dass man nicht nach(!) einer aufgetretenen Kollision wechselnde Wartezeiten für eine Übertragungswiederholung bestimmt sondern vor(!) einer Übertragung stochastische Wartezeiten organisiert.

Der hinter CSMA/CA stehende Ablaufalgorithmus ist in ◘ Abb. 3.12 dargestellt.

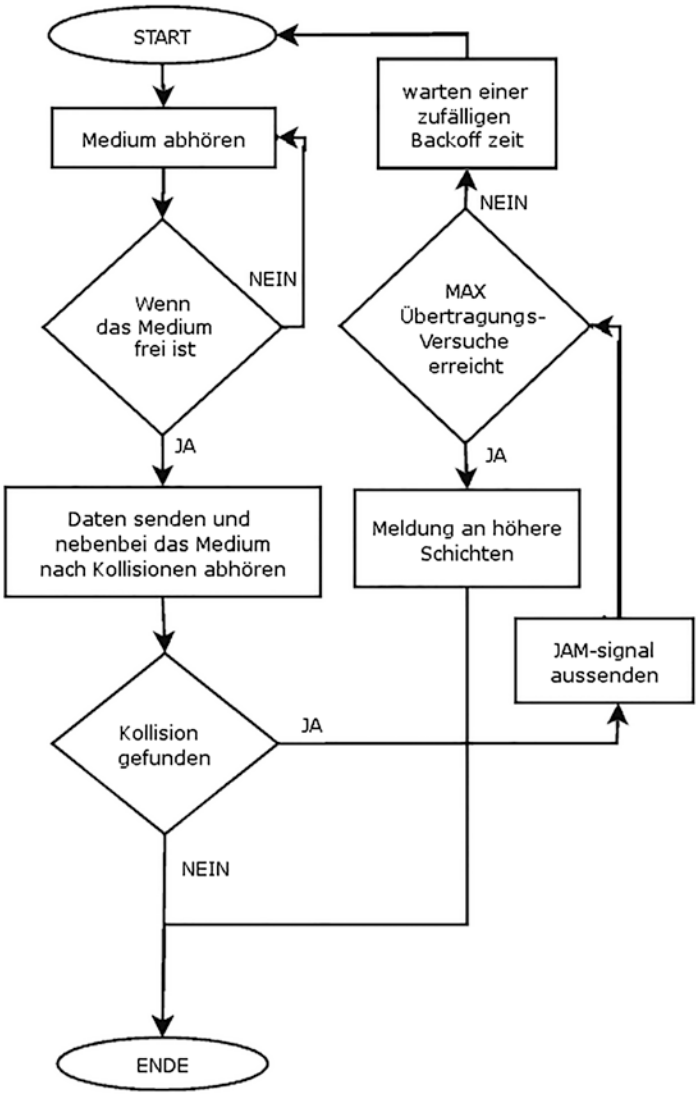


Abb. 3.11 CSMA/CD-Verfahren

- **Ablauf von CSMA/CA**

1. sendewillige Station hört Medium vor dem Senden ab
2. wenn frei (Kanalzugriff erfolgreich), dann senden, sonst 3.
3. wenn besetzt, abwarten eines „back off"-Intervalls und beginne bei wieder bei Schritt 1.
4. Wiederholung bis gesendet werden kann oder Maximalwert von Sendeversuchen erreicht ist.

CSMA/CA reduziert die Kollisionswahrscheinlichkeit erheblich, erreicht aber keine restlose Kollisionsvermeidung. Deshalb

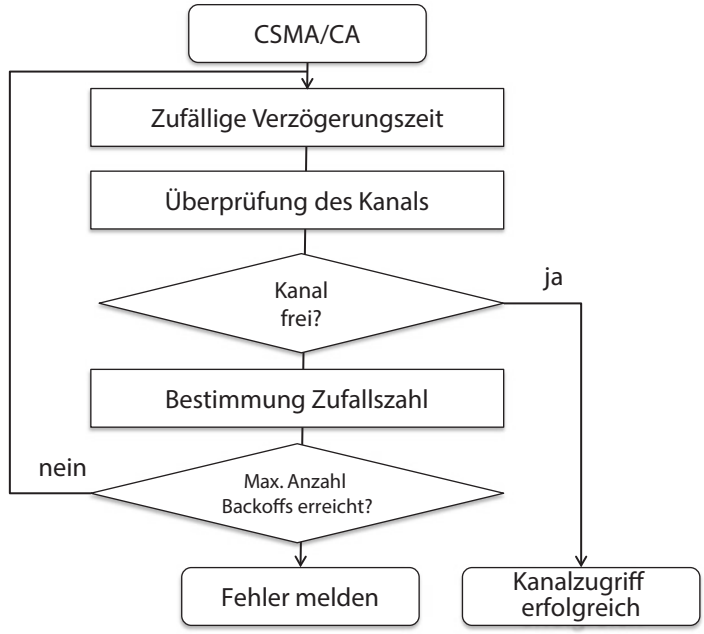


Abb. 3.12 CSMA/CA-Verfahren

müssen die Frames quittiert werden und in den seltenen Fällen einer Kollision wiederholt übertragen werden.

Im Falle von WLAN treten noch spezielle Effekte bei der CS-Funktion auf. Diese Probleme können mittels der zusätzlichen CTS/ RTS –Nachrichten beseitigt werden (Details s. Teil II)

3.2.3.4 Beaconing-Verfahren

Das Beaconing-Verfahren kommt meist bei Funknetzen zum Einsatz. Wesentliche Entwicklungsziele für das Beaconing-Verfahren sind geringe Leistungsaufnahme für einen langen Betrieb über Batterieversorgung, kostengünstige Hardware, sichere Funkübertragung und Parallelbetrieb mit anderen Funksendern.

Das Verfahren findet seine Verwendung anstelle des CSMA/CA (d. h. „Beacon-disabled“) und oft in der Kombination mit Zeitmultiplex (TDM). Der Begriff kommt grundsätzlich aus dem Schifffahrtwesen: Beacon bedeutet außerdem „Boje“, „Schifffahrtszeichen“, „Seezeichen“.

Das eigentliche „Beaconing“ (wie Orientierung nach Leuchtfeuer) bietet eine höhere Effizienz für WLAN oder Pikonetze, wie bspw. ZigBee, Bluetooth etc. Für diese Funknetzwerke (Abb. 3.13) mit geringer Reichweite sind die sog.

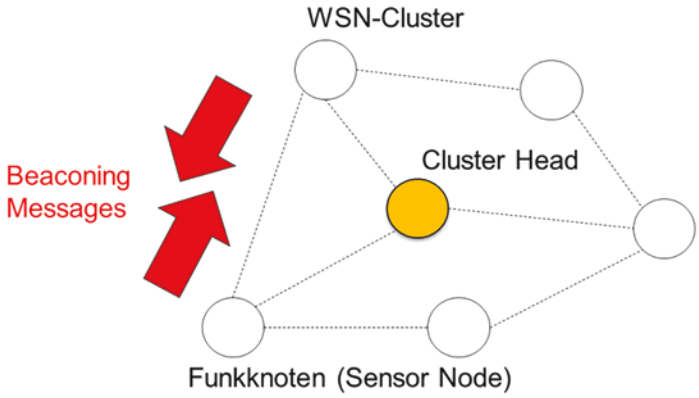


Abb. 3.13 Beaconing in einem Wireless Sensor Network

energieeffiziente Medienzugriffsprotokolle aufgrund deren i. d. R. geringen Energieressourcen von großer Bedeutung [8, 10, 13, 16, 17].

So „wachen" die energieautarken Teilnehmer in den ZigBee-Pikonetzen (IEEE 802.15.4) immer bei einer Beacon-Message „auf" und legen sich bei fehlendem Datenübertragungsbedarf zum längeren „Schlafen" („Duty Cycle" nur bis zu 6 % der Gesamtzeit, restliche Zeit – minimaler Energieverbrauch). Die 16 TDMA-Zeitschlitze ermöglichen in der Kombination mit Beaconing eine Energieeinsparung bis zu 94 % (also im Verhältnis: 16/17).

3.3 Zwischenfragen/Übungsaufgaben

3.3.1 Signalausbreitung

a) Wieviel Stufen muss ein Signal mindestens haben, um 3 Bit zu übertragen?
b) Wie stark müssen sich 2 Signalstufen mindestens unterscheiden, wenn Rauschspannungen 1mV (fast) nie überschreiten?
c) Eine Netzwerkkarte sendet mit einer Datenrate von 2,5 GBit/s Signalfolgen mit einem Signalinformationsgehalt von 4 Bit. Berechnen Sie die Schrittrate und die Signaldauer.
d. Folgende Bitfolge 101110001011001110111100 soll mithilfe elektrischer Rechteckimpulssignale (8 Signalstufen) übertragen werden. Zeichnen Sie die Signalfolge in ein Signal-/Zeitdiagramm ein.

3.3.2 Nyquist-Theorem

a) Wie hoch muss die Bandbreite nach Beispiel 3.3.1c) mindestens sein?
b) Wie hoch muss der Signal-Rauschabstand nach Beispiel 3.3.1c) und mit der Bandbreite von Beispiel 3.3.2a) mindestens sein?

3.3.3 Medienzugriff

a) Vergleichen Sie deterministische und stochastische Zugriffsverfahren bezüglich ihrer Eignung für Echtzeitanwendungen.
b) Verdeutlichen Sie Gemeinsamkeiten und Unterschiede zwischen Zeitmultiplex- und Frequenzmultiplexverfahren (TDM bzw. FDM).
c) Inwieweit ergänzen Raummultiplex (SDM) und Zellularstrukturen die herkömmlichen TDM- und FDM-Verfahren?

Rechnernetzarchitekturen und -Dienste

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_4

4.1 Ziele und Anwendungsfelder von Rechnernetzen

Rechnernetze sind aus unserem Alltag und der Wirtschaft nicht mehr wegzudenken. Die wichtigsten Ziele von Rechnernetzen sind wie folgt [7, 10, 16, 17]:

1. Höherer Komfort und Kosteneinsparungen bei Dienstleistungen
   - Büroautomatisierung
   - Finanzsysteme
   - Cloud Services (Auslagerung von Dienstleistungen in das weltweite Netzwerk)
2. Intelligente Vernetzung
   - Fertigungssteuerung innerhalb des Projektes „Industrie 4.0“
   - Grids („smarte“ Services wie Lieferung von Strom oder Wasser in modernen Versorgungsnetzen)
   - gemeinsame Ressourcennutzung von Hard- und Softwarekomponenten
   - hohe Zuverlässigkeit durch Redundanz
3. Soziale Medien
4. Parallele Verarbeitung
   - High-Performance-Computing
   - Universelle Datenbereitstellung

Ausblick: „Industrie 4.0“ (s. Teil III) integriert Themen wie folgt: universelle, „intelligente Vernetzung“, Robotik, Internet of Things, Augmented Reality, 3D-Drucker, RFID etc.

Alle diese Ziele erfordern hohe Zuverlässigkeit aller Teilkomponenten durch Redundanz, optimierte Dienstschnittstellen und eine einfache Integration neuartiger Dienste und Systeme.

An dieser Stelle geben wir eine kleine Auswahl wichtiger Netzdienste, Applikationen und Apps:

1. Klassische Anwendungen
   E-Mail (SMTP), Filetransfer (FTP), Remote Login (Telnet, SSH)
2. Globale Informationssysteme
   (z. B. WWW, Google, Wikipedia)
3. Soziale Medien
   Facebook, Twitter, …
4. Büroautomatisierung
   z. B. Workflows, Groupware,
   Finanzielle und Banking-Systeme (SWIFT, …)
5. Multimediakommunikation
   Skype, Voice over IP (VoIP/SIP), Videokonferenzen (SIP)
   Social Networks und Amateur-Videohosting, Streaming (YouTube)
6. Verteilte Verarbeitung
   Cluster Computing, XaaS Clouds (universeller Clouddienst)
   Unterstützung der Fertigungssteuerung (z. B. ZigBee, EnOcean).
7. Mobile Apps
   Native, Web-basierte, …

4.2 Dienste und Protokolle

Ein Rechnernetz (RN) ist ein System von Computern, zwischen denen ein automatischer Nachrichtenaustausch möglich ist. Die Kommunikation erfolgt dabei nach standardisierten Vorschriften [13, 16, 17].

Basis aller Rechnernetze ist die Realisierung des Kommunikationsverbundes durch ein Kommunikationsnetz, das angeschlossenen Rechnern den Informationsaustausch ermöglicht (◘ Abb. 4.1).

Die Anwendungsdienste in Rechnernetzen sind vielfältig. Sie lassen sich in die Dienstklassen Kommunikationsverbund, Ressourcenverbund und Steuerungsverbund einordnen.

In einem funktionsfähigen Rechnernetz gibt es verschiedene Arten von Standards.

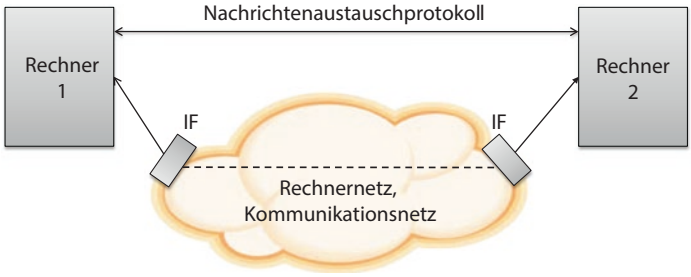
Eine Rechnernetzarchitektur besteht i.a. aus mehreren hierarchischen Schichten. Jede Schicht repräsentiert einen Dienst. In einer *Dienstspezifikation* muss festgelegt sein, welche Dienstleistungen die Schicht erbringt und wie die Nutzerschnittstelle *IF* der Schicht aussieht. Der Informationsaustausch erfolgt in vertikaler Richtung zwischen dem Dienstnutzer und dem hierarchisch darunter befindlichen Dienstbereitsteller [17] (vgl. Abschn. 5 über ISO-Architektur).

Die internen Funktionsprinzipien einer Schicht sind für deren Nutzung uninteressant (transparent). Für die Implementierung einer Schicht ist hingegen wichtig, wie sie arbeiten soll. Dazu werden dienstbereitstellende Instanzen innerhalb der Schicht definiert und Prozeduren vereinbart, nach deren Regeln (Protokollen) die Zusammenarbeit erfolgen muss. Der Informationsaustausch zur Gewährleistung eines Protokolls erfolgt horizontal [17] (vgl. Abschn. 5 über ISO-Architektur).

Protokolle beinhalten Aussagen über:

- die Syntax auszutauschender Nachrichten,
- die zulässigen Nachrichtenreihenfolgen,
- Zeitschranken und Fehlerreaktionen.

XaaS (Everything as a Service) ist ein Sammelbegriff für alle möglichen Cloudservices, vgl. zu klassischen IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service) und SaaS (Software-as-a-Service), s. Teil III.



◘ **Abb. 4.1** Rechnernetz: allg. Darstellung

Diese sogenannte *Protokollspezifikation* muss gewährleisten, dass die von der Schicht geforderten Dienstleistungen korrekt erbracht werden.

Die Instanzen einer Schicht können Dienstleistungen der nächstniederen Schicht innerhalb der Hierarchie in Anspruch nehmen.

Für die einzelnen Schichten gibt es u. U. mehrere alternative Protokolle. Durch konkrete Auswahl der speziellen Protokolle für jede Schicht wird eine eindeutige Protokollarchitektur erreicht (Protokollstack, Protokollprofil, Protokollsuite).

Die beiden wichtigsten Architekturmodelle sind das theoretisch gut ausgearbeitete Referenzmodell der Standardorganisation ISO und das pragmatische Modell der Internet-Architektur.

Etwa 1980 begann die Entwicklung spezieller lokaler Rechnernetztechnologien, z. B. für die Vernetzung eines Gebäudes. Seitdem unterscheidet man flächendeckende Rechnernetze WAN (Wide Area Networks) von lokalen Rechnernetzen LAN (Local Area Networks).

4.3 Darstellung von Diensten und Protokollen

Dienste und Protokolle lassen sich auf verschiedene Weise darstellen [4, 17]:

- Verbale Notation
- Pseudokode
- Grafische Darstellungen
  Ablaufdiagramm oder Weg-Zeit-Diagramm (◘ Abb. 4.2)
  Zustandsdiagramm oder Zustandsübergangsdiagramm (◘ Abb. 4.3)
- Spezielle Spezifikationssprachen
- Visualisierung mittels Protokollanalysatoren und Protokollsimulatoren [2, 12].

Die verbale Darstellung steht gewöhnlich am Anfang einer Entwicklung. Der schon präzisiertere Pseudokode besteht aus einer Mischung von verbalen und formalen Notationen. So können z. B. die Daten konkret in einer geeigneten abstrakten Programmiersprache beschrieben werden und die Art des Datenaustausches in verbaler Form.

Die grafischen Darstellungen sind sehr beliebt wegen ihrer Übersichtlichkeit. Sie erlauben die vollständige Beschreibung von Diensten und Protokollen.

Wir beschränken uns im Folgenden auf Dienstbeschreibungen, bei denen 2 Prozesse A und B mittels eines X-Dienstes kommunizieren [16, 17]. Je nach der inhaltlichen Rolle werden die beteiligten Prozesse als Client/Server, als Initiator/Responder, als Koordinator/Teilnehmer usw. bezeichnet.

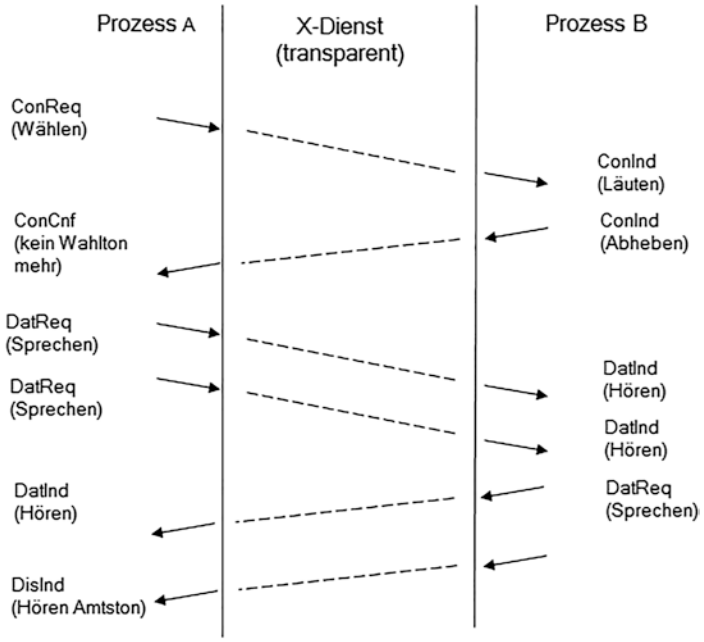


Abb. 4.2 Ablaufdiagramm (Weg-Zeit-Diagramm) für einen Fernsprechdienst

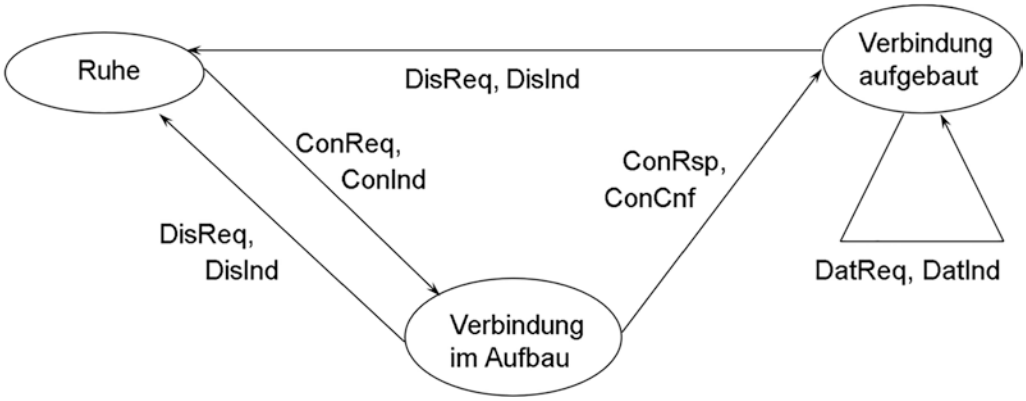


Abb. 4.3 Zustandsdiagramm für einen Fernsprechdienst [16]

Ein Dienst besteht aus sog. Dienstprimitiven (Dienstelementen Basiselemente). Die Dienstelemente beinhalten Operationen und Status-Elemente. Die Dienstelemente werden an der Dienstschnittstelle ausgetauscht.

Es gibt vier Operationen des X-Dienstes:

- Anforderung (Request/Req)
- Anzeige (Indication/Ind) oft eine Folge einer Anforderung auf der Partnerprozessseite

- Bestätigung (Response/Rsp)
- Bestätigungsanzeige (Confirmation/Cnf).

Bestätigungsoperationen werden nur bei kritischen Abläufen vorgenommen, z. B. beim Eröffnen einer Übertragungsverbindung. Im Normalfall arbeitet man mit unbestätigten Operationen.

Der Status eines X-Dienstes wird mittels der folgenden Nachrichtentypen abgebildet:

- Con: Connect (Verbindungsaufbau)
- Dat: Data (Datenübertragung)
- Dis: Disconnect (Verbindungsabbau)
- Abo: Abort (Abbruch einer Verbindung aus technischen Gründen).

Im folgenden Beispiel (s. ◘ Abb. 4.2) wird ein Ablaufdiagramm für den speziellen X-Dienst „Telefonieren" diskutiert. Nach einem bestätigten Verbindungsaufbau (Dienstelemente ConReq, ConInd, ConRsp, ConCnf) folgt eine Phase gegenseitiger unbestätigter Kommunikation (DatReq, DatInd), abgeschlossen von einem unbestätigten Verbindungsabbau. (DisReq, DisInd). Es ist hervorzuheben, dass dieses Ablaufdiagramm nur einen Ablauf beschreibt. Es existieren aber auch andere mögliche Abläufe, z. B. kann es sein, dass der Empfänger beim Verbindungsaufbau nicht abhebt (kein ConRsp gibt). Der Dienst wird erst vollständig beschrieben, wenn alle(!) möglichen Abläufe dargestellt werden.

Ablaufdiagramme sind übersichtlich zur Beschreibung der häufigsten Abläufe, aber wenig geeignet zur Beschreibung eines kompletten Dienstes mit allen Ausnahmesituationen.

Dafür eignen sich Zustandsdiagramme besser (s. ◘ Abb. 4.3). In diesem Diagramm werden Zustände und Übergangsereignisse in einem Graphen zusammengefasst. Ausgehend vom Zustand „Ruhe" erfolgt die Dienstelementekombination ConReq/ConInd und verursacht einen Übergang in den Zustand „Verbindung im Aufbau". Von diesem gibt es aber zwei mögliche Weiterführungsereignisse, die Verbindungsbestätigung mit ConRsp/ConCnf, aber auch die Verbindungsabweisung mit DisReq/DisInd. Im positiven Fall erfolgt ein Übergang in den Zustand „Verbindung aufgebaut". Die Ereignisse Sprechen/Hören bzw. DatReq/DatInd führen nicht zum Verlassen dieses Zustandes, wohl aber ein Verbindungsabbruch mit DisReq/DisInd.

Für die Algorithmierung und software-technische Implementierung sind die Zustandsdiagramme besser geeignet. Für die Überschaubarkeit der zeitlichen Abläufe eignen sich Ablaufdiagramme besser.

4.4 Rechnernetztopologien und -strukturen

Zu den grundlegenden Rechnernetz-Strukturen gehören (s. ◘ Abb. 4.4):

- **Punkt-zu-Punkt-Kanäle**

z. B. in Weitverkehrsnetzen (WAN = Wide Area Network).

Hierbei wird jeweils von den Netzwerkadaptern ein Kabel zu einem anderen Netzwerkadapter geführt. Auf dieser Basis können beliebige Strukturen der Leitungsführung (Topologie) gebildet werden, z. B. Sterne, Bäume und auch irreguläre Strukturen (s. ◘ Abb. 4.4).

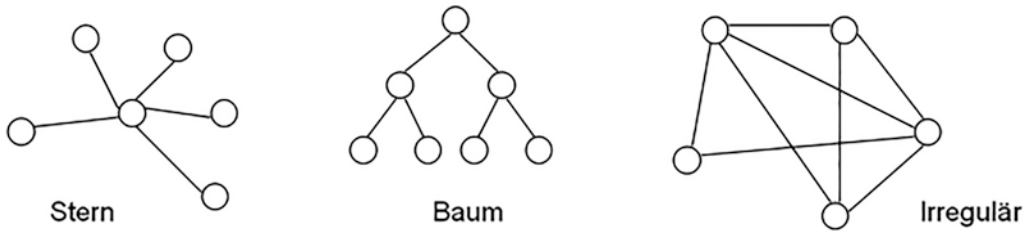
- **Rundsendekanäle**

z. B. bei lokalen Netzen (LAN = Local Area Network).

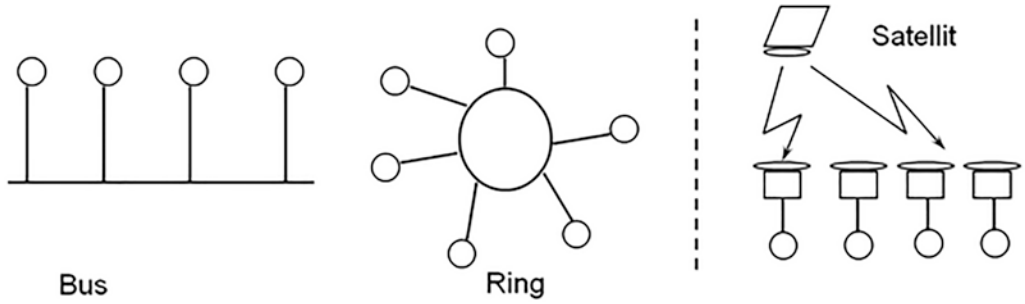
Man unterscheidet Broadcast-, Multicast- und dezentrale Strukturen.

Von besonderer Bedeutung sind die Strukturen Bus (z. B. Industrienetze), Ring (z. B. SDH/Sonet) sowie WLAN (IEEE 802.11x) und Satellitenfunk (z. B. Inmarsat oder GPS) wie es in ◘ Abb. 4.5 zu sehen ist.

Rechnernetztechnologien mit Rundsendekanälen erfordern i. A. eine komplizierte Steuerung des Medienzugriffes, um Übertragungskollisionen zu vermeiden.



◘ **Abb. 4.4** Rechnernetz-Strukturen auf Basis von Punkt-zu-Punkt-Kanälen [16]



◘ **Abb. 4.5** Rechnernetz-Strukturen mit Rundsendekanälen [16]

4.5 Maßeinheiten in der Netzwerkpraxis

Bei konkreten Angaben in Datenblättern von Netzwerkkomponenten sowie bei konkreten Berechnungen von Datenraten, Durchsätzen usw. werden häufig Fehler bei der Verwendung von Maßeinheiten gemacht. Deshalb weisen wir an dieser Stelle noch einmal auf die korrekte Nutzung hin [11].

Insbesondere bei der Speichergröße von Datenträgern haben sich Maßangaben durchgesetzt, die auf 2er-Potenzen beruhen, aber ähnlich notiert werden wie die üblichen Maßeinheiten auf der Basis der 10er-Potenzen, weil $2^{10} = 1024$ ungefähr 1000 ist.

Beispielsweise besitzt ein Hauptspeicherchip der Größe 500 MB exakt eine Größe von 5242880 Byte, aber eine Turbine der Leistung 500 MW besitzt genau eine Leistung von 500 000 W. Dies entspricht einer Abweichung von ca. 5 %.

Die Netzwerktechnik orientiert sich an der weltweit anerkannten physikalischen Nomenklatur SI (frz. „Système international d'unités"). Die SI-Präfixe entsprechen den 10er-Potenzen (bspw. k, M, G, T etc.). Für die Binärpräfixe gibt es einen Vorschlag von E. Engelhardt zur sinnvollen Notation [11] (◘ Tab. 4.1).

Wir möchten einen weiteren Hinweis geben. In vielen Werbebroschüren werden Maßeinheiten prinzipiell falsch wiedergegeben.

So wird z. B. von einer Übertragungsrate von 1 GBit gesprochen, korrekt wäre aber eine Übertragungsrate von 1 GBit/s.

Bitte achten Sie auf die richtige Verwendung.

◘ **Tab. 4.1** Abweichungen der Präfixe nach 2er-Potenzen zu den SI-Präfixen

SI-Präfixe	2er-Potenz	10er-Potenz	Binärpräfixe	Unterschied (%)
1 kB (Kilobyte)	~ 2^{10} Byte	= 10^3	Kibibyte, KiB/KB	2,4
1 MB (Megabyte)	~ 2^{20} Byte	= 10^6	Mebibyte; MiB	4,9
1 GB (Gigabyte)	~ 2^{30} Byte	= 10^9	Gibibyte, GiB	7,4
1 TB (Terabyte)	~ 2^{40} Byte	= 10^{12}	Tebibyte; TiB	10,0
1 PB (Petabyte)	~ 2^{50} Byte	= 10^{15}	Pebibyte; PiB	12,6
1 EB (Exabyte)	~ 2^{60} Byte	= 10^{18}	Exbibyte; EiB	15,3
1 ZB (Zettabyte)	~ 2^{70} Byte	= 10^{21}	Zebibyte; ZiB	18,1
1 YB (Yottabyte)	~ 2^{80} Byte	= 10^{24}	Yobibyte; YiB	20,9

4.6 Zwischenfragen/Übungsaufgaben

4.6.1 Dienst/Protokoll

a) Grenzen Sie die Begriffe Dienst und Protokoll gegeneinander ab!
b) Vergleichen Sie beide Protokolldarstellungsformen Ablauf- und Zustandsdiagramm bezüglich
   - Übersichtlichkeit beim Normalablauf
   - Anzahl der Diagramme bei alternativen Abläufen
   - Vorlage für Programmierung und Implementierung!

4.6.2 Topologien

a) Wie viele Verbindungsleitungen benötigen Sie bei Sterntopologie, um 5 Rechner zu verbinden?
b) Wie viele Verbindungsleitungen benötigen Sie in einem Netz mit 5 Rechnern bei vollvermaschter Topologie (jeder Rechner ist mit jedem anderen Rechner über eine Leitung verbunden)?
c) Wie erhöht sich die Leitungszahl in den Fällen a) und b), wenn ein zusätzlicher Rechner in das Netz eingebunden wird?

4.6.3 Maßeinheiten

a) Wieviel Zeit benötigt ein System mit einer Übertragungsrate von 1GBit/s zur Übertragung von 1GByte Information?

ISO-Architektur

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_5

5.1 Normung

Für die breite Nutzung von Rechnern ist es außerordentlich wichtig, dass die wichtigsten Schnittstellen standardisiert und allgemein akzeptiert sind.

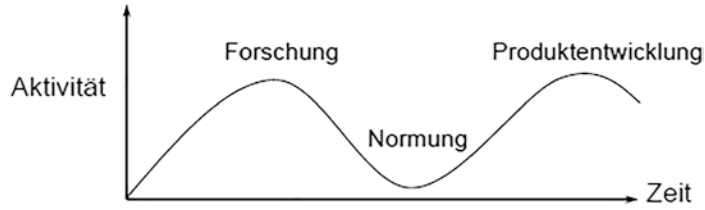
Deshalb gehen wir an dieser Stelle kurz auf die Normungsproblematik ein [13, 16, 17]:

- Das erste Problem der Rechnernetznormung besteht darin, dass die Kommunikation in stark heterogenen Umgebungen stattfindet.
- Das zweite Problem besteht im Nebeneinander von offiziellen (de-jure) und praktisch bewährten Normen (de-facto) und in einem schwer zu überschauenden „Dickicht" international Normungsorganisationen.

Hier eine Auswahl wichtiger Normungsorganisationen [16]:

- ITU: International Telecommunications Union der United Nations
- ITU-T: Telefon- und Datenkommunikation (z. B. GSM, UMTS, ATM)
- ETSI: European Telecommunications Standards Institute
- IETF: Internet Engineering Task Force (Internet-Protokolle)
- ISO: International Organization for Standardization (z. B. OSI-Modell, …)
- IEEE: Institute of Electrical and Electronics Engineers (IEEE 802.x, Ethernet, WLAN, …)
- CEN: Europäisches Komitee für Normung)
- ANSI: American National Standards Institute usw.

Als drittes Problem existiert die Trägheit insbesondere der offiziellen Normung (nach David Clark, @MIT/IAB). ◘ Abb. 5.1 stellt den fast destruktiven Einfluss träger Normung auf die Verzögerung von Produktentwicklungen dar!



◘ **Abb. 5.1** Trägheit der offiziellen Normung

5.2 OSI-Referenzmodell

Um 1970 gab es bereits den Bedarf nach universeller Computervernetzung. In der Praxis gab es jedoch nur proprietäre, firmenspezifische Lösungen, z. B. IBM SNA (s. ► Abschn. 2.4). Es war nahezu unmöglich, in diese proprietären Netze Computer anderer Hersteller zu integrieren.

Deshalb begann man Mitte der 70er Jahre in der internationale Standardorganisation ISO (International Standardization Organisation) mit der Entwicklung von Standards für offene, d. h. firmenunabhängige, Rechnernetze. Diese *offenen* Standards sollten alle Einzelheiten der Rechnerkopplung festlegen, ohne sich auf bestimmte Computer- und Betriebssystemtypen festzulegen.

Das vom Subkomitee ISO/TC97/SC16 im Jahr 1979 vorgeschlagene Architekturmodell offener Systeme trägt den Namen „Reference Model of Open Systems Interconnection", im Weiteren kurz als OSI-Referenzmodell bezeichnet. Dieses Modell setzte sich durch für die Analyse, Bewertung und den Vergleich von Rechnernetzarchitekturen und wurde 1984 als offizieller Standard ISO 7498 verabschiedet. Der Standard ISO 7498 besteht aus zwei wesentlichen Teilen, der Festlegung einer sauberen OSI-Terminologie und dem Vorschlag eines 7-Schichten-Modells.

Die begleitenden detaillierten Standards der ISO für die einzelnen OSI-Schichten haben sich hingegen nicht durchsetzen können. Deshalb werden sie in diesem Buch nicht behandelt.

Der hohen Komplexität von Rechnernetzen entspricht das OSI-Referenzmodell durch den Vorschlag einer streng hierarchischen 7-Schichten-Architektur (s. ◘ Abb. 5.2). Da in der Literatur oft die englischen Schichtenbezeichnungen verwendet werden, sind in ◘ Tab. 5.1 die Schichtenbezeichnungen gegenübergestellt [3, 5, 15, 17].

Die Funktionalität der einzelnen Schichten wird später erläutert.

An dieser Stelle soll das wesentliche Konzept des OSI-Modelles erläutert werden [17]:

1. Schichtenkonsistenz: keine schichtenübergreifenden Funktionalitäten sind erlaubt, eventuelle Überschneidungen in Implementierungen müssen vermieden werden!
2. Kapselungsprinzip: die zu übertragende Nachrichten, Pakete, Frames werden Schicht zu Schicht gekapselt. Interne Header werden bei einer Übergabe von Schicht zu Schicht gefiltert.
3. Jede Schicht erfüllt einen Dienst, gekennzeichnet durch:
   - Dienstzugangspunkt (SAP = Service Access Point): Schnittstelle der Schicht, Übergabestelle für Dienstelemente, versehen mit einer Zugriffsadresse

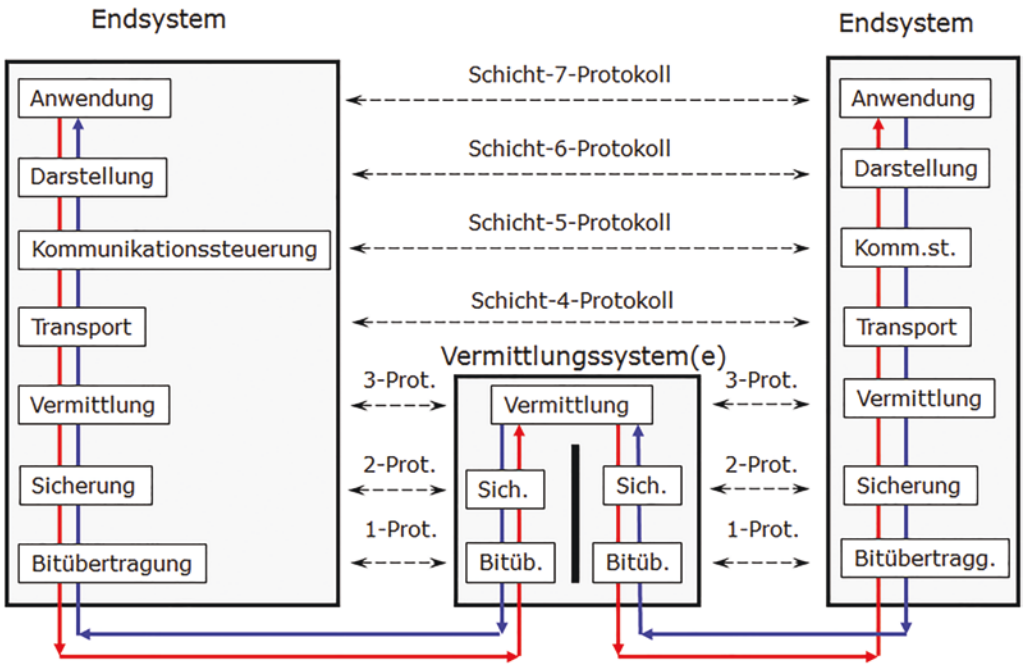


Abb. 5.2 OSI-Referenzmodell: Schichtenstruktur

Tab. 5.1 Schichten des OSI-Referenzmodelles

Nr.	Deutsche Bezeichnung	Englische Bezeichnung	Kommentar
7	Anwendungs-schicht	Application layer	Verarbeitungs-orientierte Schichten
6	Darstellungs-schicht	Presentation layer	
5	Kommunikations-steuerungsschicht oder auch Sitzungsschicht	Session layer	
4	Transportschicht	Transport layer	Übertragungs-orientierte Schichten
3	Vermittlungs-schicht oder auch Netz-werkschicht	Network layer	
2	Sicherungsschicht	Data link layer	
1	Bitübertragungs-schicht	Physical layer	

- Protokoll: Regeln zur Steuerung der Kommunikation innerhalb einer Schicht
- Instanz: Element einer Schicht (z. B. Softwareprozess) Die Instanzen erbringen die Funktionalität der Schicht durch die Realisierung von Protokollen.

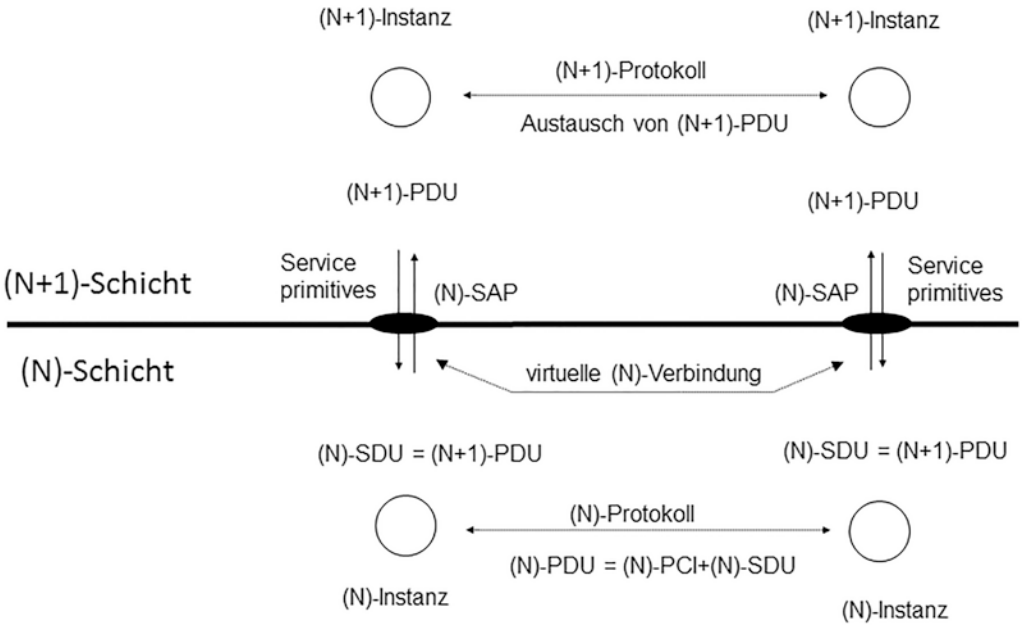
Zum tieferen Verständnis der *OSI-Terminologie* wird im Folgenden eine abstrakte Schicht (N) einer Rechnernetz-Architektur vorgestellt.

Die (N)-Schicht (layer) bietet Instanzen (entities) der Schicht (N + 1) einen (N)-Dienst (service) an. Den Dienstnutzern (service user) der (N + 1)-Schicht bleibt dabei verborgen, wie der Dienstbereitsteller (service provider) in der (N)-Schicht seine Aufgabe erfüllt.

Die Nutzung des Dienstes erfolgt durch den Austausch von Dienstelementen (primitives) über Dienstzugriffspunkte SAP (service access points). In ◘ Abb. 5.3 wird das komplexe Zusammenspiel zweier Schichten dargestellt.

Zwei Instanzen der (N + 1)-Schicht erfüllen das (N + 1)-Protokoll ihrer Schicht, indem sie sogenannte PDU (Protocol Data Units) austauschen. Dazu nutzen sie den (N)-Dienst. Im Beispiel bilden zwei Dienstzugriffspunkte der (N)-Schicht eine virtuelle Verbindung, über die Protokolldateneinheiten versendet werden können.

Aus Sicht der (N)-Instanzen der (N)-Schicht sind die zu übertragenden Protokolldaten der (N + 1)-Schicht völlig



◘ **Abb. 5.3** OSI-Referenzmodell: Interaktion zwischen zwei Schichten

transparente Servicedateneinheiten (SDU, Service Data Units). Aus diesen SDU und zugefügter Protokollsteuerinformation PCI (Protocol Control Information) werden die Protokolldateneinheiten der (N)-Schicht gebildet.

Falls der (N)-Dienst die Dienste einer darunterliegenden (N − 1)-Schicht in Anspruch nehmen muss, geschieht dies nach dem gleichen Schema wie beim Zusammenwirken der Schichten (N + 1) und (N).

Die Dienstprimitive werden nach folgendem Schema bezeichnet:

<Diensterbringer - Id.> - <Dienststatus> <Dienstoperation> <Parameter>

Die Diensterbringeridentifikation kennzeichnet die diensterfüllende Schicht. Unter Dienststatus werden inhaltlich zusammengehörige Dienstleistungen zusammengefasst, z. B. Eröffnen einer virtuellen Verbindung (CONNECT), Datenübertragung (DATA) und Trennen einer Verbindung (DISCONNECT). Die Dienstoperationen „Anfordern Dienst" (request), „Anzeige Dienstresultat" (indication), „Bestätigen Dienst" (response) und „Anzeigen Bestätigung" (confirm) präzisieren die Dienstleistung. Parameter können z. B. Adressen, geforderte Dienstqualitäten usw. sein.

Die Dienstzugriffspunkte kennzeichnen Nachrichtenquelle und -senke. Man unterscheidet verbindungslose und verbindungsorientierte Kommunikation.

Bei verbindungsloser Kommunikation wird jede Nachricht komplett adressiert und vom Diensterbringer unabhängig von Vorgänger- und Nachfolgenachrichten übertragen. Folge ist ein großer Informationsoverhead und eine geringe Dienstgüte. So ist z. B. die richtige Empfangsreihenfolge nicht gesichert.

Bei verbindungsorientierter Kommunikation wird zunächst zwischen den (N)-SAP eine virtuelle (N)-Verbindung aufgebaut. Dabei werden Ressourcen reserviert und in der anschließenden Datentransferphase treten deshalb weniger Störungen auf. Der Nachrichten-Overhead ist dabei verringert, weil anstelle der Adressen eine kürzere Verbindungsidentifikation verwendet werden kann. Außerdem kann der Diensterbringer eine höhere Dienstqualität sichern, z. B. die richtige Empfangsreihenfolge. Die Datentransferphase wird durch den Abbau der Verbindung beendet.

Es gibt bestätigte und unbestätigte Dienste. Datenübertragungen sind z. B. meist unbestätigt. Eine Senderinstanz fordert die Übertragung mit dem Dienstprimitiv DATA request. Die Partnerinstanz auf dem anderen Rechner erhält daraufhin eine Empfangsanzeige mit dem Dienstprimitiv DATA indication (s. ◘ Abb. 5.4).

Eine Verbindungseröffnung ist dagegen bestätigt (s. ◘ Abb. 5.5). Die Initiatorinstanz fordert die Verbindung mit dem Dienstprimitiv CONNECT request. Die Partnerinstanz, der Responder, erhält dann eine Anzeige über den Verbindungswunsch durch

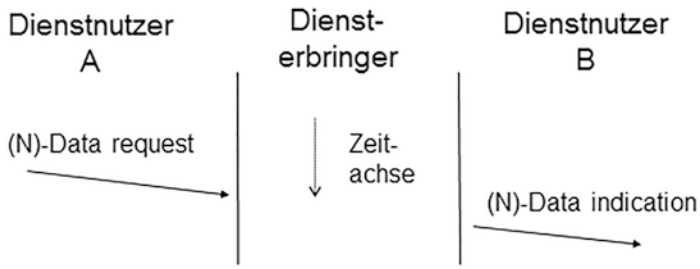


Abb. 5.4 Ablaufdiagramm für unbestätigte Datenübertragung

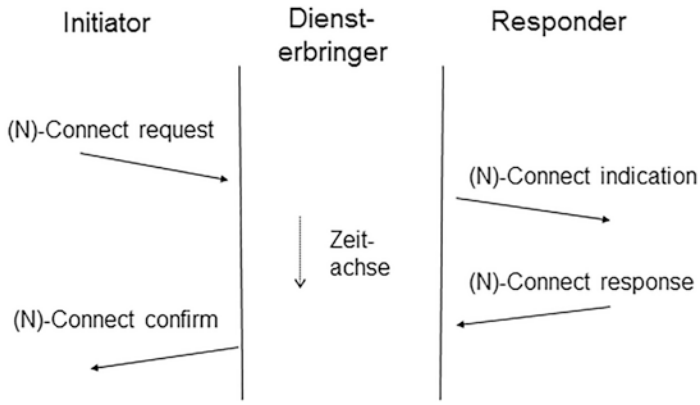


Abb. 5.5 Ablaufdiagramm für bestätigte Verbindungseröffnung

das Dienstprimitiv CONNECT indication. Für den Fall, dass der Responder einverstanden ist, gibt er die Bestätigung mit dem Dienstprimitiv CONNECT response. Daraufhin erhält der Initiator die Anzeige der Bestätigung durch das Dienstprimitiv CONNECT confirm.

5.3 OSI-Modell: Schichtenfunktionalität

Die sieben Schichten des OSI-Referenzmodelles wurden bereits in Tab. 5.1 aufgelistet. Im Folgenden werden die Funktionalitäten der einzelnen Schicht kurz vorgestellt.

5.3.1 Bitübertragungsschicht

Die Bitübertragungsschicht ist die unterste Schicht des OSI-Modelles. Sie hat die Aufgabe der Übertragung von beliebigen Bitströmen zwischen zwei Rechnern über einen Kommunikationskanal.

Standards für diese Schicht müssen u. a. mechanische, elektrische oder optische Festlegungen treffen, um ein konkretes physikalisches Übertragungsmedium optimal zu nutzen.

Im Einzelnen können dies z. B. Vorschriften zu Kabelarten, Steckerformen, Impulsspannungen, Taktraten und Synchronisationsmechanismen sein.

5.3.2 Sicherungsschicht

Die Sicherungsschicht soll die sichere Übertragung von Nachrichten über einen Nachrichtenübertragungskanal der Bitübertragungsschicht gewährleisten.

Dies kann wie folgt erreicht werden. Die Nachrichten werden als Rahmen (Frames) bezeichnet. Jeder Rahmen muss redundante Informationen enthalten, mit deren Hilfe der Empfänger eindeutig Anfang und Ende des Rahmens und auch evtl. Bitverfälschungen erkennen kann.

In der OSI-Sicherungsschicht sind für den Fall unzuverlässiger Übertragungstechnologien neben der Erkennung von Übertragungsfehlern auch Mechanismen zur Fehlerkorrektur vorgesehen. Dazu muss der korrekte Empfang eines Rahmens beim Empfänger dem Sender quittiert werden. Im Fehlerfall wird das Senden wiederholt. Da es auch passieren kann, dass Quittungsnachricht verloren gehen, kann es zum unnötigen Wiederholen kommen. Deshalb muss der Empfänger auch Duplikate erkennen und verwerfen können.

Eine weitere Aufgabe der OSI-Sicherungsschicht ist die sogenannte Flusssteuerung. Diese soll absichern, dass es bei der Übertragung nicht zu Überlastungen kommt.

Das OSI-Modell gibt keine Implementierungsvorschriften. Die ISO hat für die Implementierung der Schichten 1 und 2 beispielsweise die ursprünglich von der Fa. IBM entwickelte HDLC-Prozedur vorgeschlagen.

Speziell für lokale Rechnernetze gibt es ein präzisiertes Modell für die OSI-Schicht 2 von der US-amerikanischen Standardisierungsorganisation IEEE (s. ◘ Abb. 5.6), welches eine Unterteilung der Schicht in eine technologieabhängige Unterschicht MAC (Media Access Control) und eine technologieunabhängige Unterschicht LLC (Logical Link Control) vornimmt und somit erlaubt, bei gleicher Nutzerschnittstelle verschiedenste LAN-Technologien zu integrieren.

Jede Netzwerkkarte besitzt eine MAC-Adresse mit einer Länge von 48-Bit (Notation: 6 Byte in hexadezimaler Darstellung, jeweils durch Doppelpunkt getrennt). Die Hersteller garantieren dabei die weltweite Eindeutigkeit der Adressen,

Das Protokoll der LLC-Schicht ist dabei an das ältere HDLC-Protokoll angelehnt. LLC fügt u. a. in den Datenteil

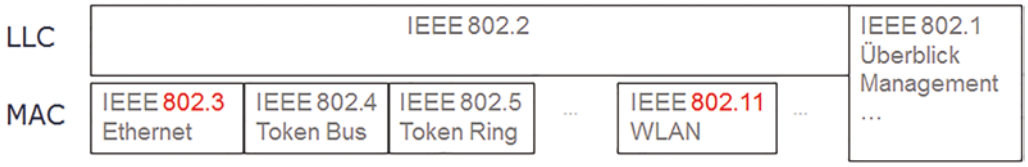


Abb. 5.6 LAN-Architektur nach IEEE

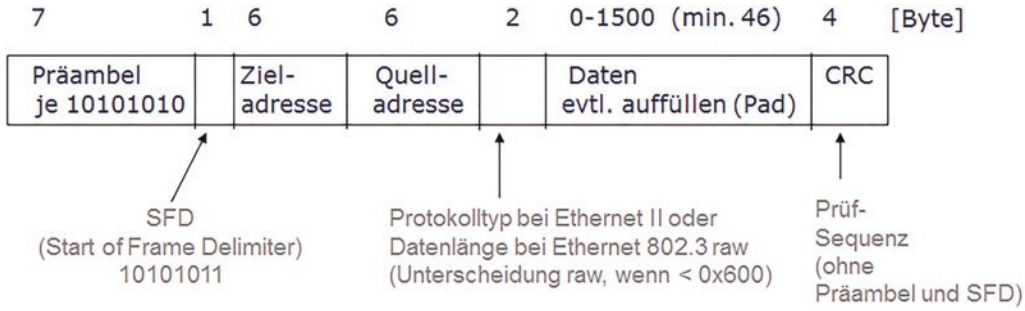


Abb. 5.7 Ethernet Frameaufbau

des Frames zwei Kennungen ein, die es gestatten, mehrere Nutzprotokolle in der Schicht 3 zu nutzen (Multiplexing).

In der Praxis haben sich die Ethernet-Technologien der Arbeitsgruppe IEEE 802.3 weitgehend durchgesetzt. Diese besitzen folgenden Frameaufbau (s. Abb. 5.7).

Die ersten 8 Bitoktetts dienen der Synchronisation, danach kommen die MAC-Adressen von Empfänger und Absender, gefolgt von einer 16-Bit-Längenangabe, einem max. 1500 Byte langen Nutzdatenteil und einer abschließenden Framechecksequenz (32 Bit). Danach ist eine Sendepause vorgeschrieben (Inter Frame Gap), um Framefolgen eindeutig trennen zu können.

Dieses als Ethernet 802.3raw bezeichnet Format ist allerdings nicht mehr üblich. Beim aktuellen Ethernet-II-Format wird anstelle der Längenangabe eine Kennung für das nutzende Protokoll eingefügt, z. B. (hexadezimal) 0x800 für IPv4. Dadurch wird es möglich auf die LLC-Schicht zu verzichten.

5.3.3 Vermittlungsschicht

Die Vermittlungsschicht hat die Aufgabe, Übertragungen zwischen nichtbenachbarten Computern zu organisieren. Dazu leiten die Endsysteme, die alle sieben Schichten des OSI-Modelles realisieren, ihre Nachrichten über eine Reihe von Vermittlungssystemen weiter, bei denen nur die untersten drei Schichten realisiert sind.

Es werden keine einfachen Leitungstopologien vorausgesetzt, sondern es sind ausdrücklich irreguläre Strukturen zugelassen. Dadurch tritt das Problem der Wegewahl auf. Das System der Vermittlungsrechner muss gewährleisten, dass alle Nachrichten ihr Ziel auf einem möglichst optimalen Weg finden.

Weitere Aufgabe der Vermittlungsschicht sind die Verbindung heterogener Teilnetze (Anpassungsprobleme z. B. bei unterschiedlichen Framegrößen) und die Abrechnung von anfallenden Übertragungskosten.

Das OSI-Modell fordert keine Qualitätsgarantien für die Übertragung. Die ISO gab verschiedene Implementierungsorientierungen, favorisierte aber lange Zeit die verbindungsorientierte Übertragung nach dem ITU-Standard X.25.

5.3.4 Transportschicht

Die Transportschicht ist die höchste datenübertragungsorientierte Schicht. Sie muss eine sichere und effiziente Nachrichtenübertragung zwischen den datenverarbeitungsorientierten Nutzerinstanzen der Transportschicht gewährleisten. Die unteren Schichten sichern die Übertragung zwischen direkt verbundenen Rechnern oder organisieren ein schrittweises Weiterreichen. Die Transportschicht ist dagegen eine Ende-zu-Ende-Schicht.

I. a. werden virtuelle Transportverbindungen angeboten, wobei auch mehrere gleichzeitige Verbindungen (Multiplexing) möglich sind.

Beim Eröffnen einer Verbindung können Dienstgüteparameter angegeben werden, z. B. ein geforderter Mindestdurchsatz.

Die Nutzdaten werden in kleinere Einheiten zerlegt und mithilfe der Vermittlungsschicht übertragen. Evtl. Mängel der Vermittlungsschicht müssen dabei ausgeglichen werden. Dies können z. B. Nachrichtenverluste, Reihenfolgeverletzungen, Verbindungsabbrüche der Vermittlungsschicht sein.

Eine weitere Aufgabe der Transportschicht ist die Flusssteuerung, die eine unsinnige Belastung des Netzes und der Endsysteme verhindern soll, wenn z. B. Quellrechner Nachrichten schneller senden als die Zielrechner die Nachrichten verarbeiten können.

5.3.5 Kommunikationssteuerungsschicht

Die Kommunikationssteuerungsschicht ist die erste datenverarbeitungsorientierte Schicht. Sie wird nur auf Endsystemen realisiert. Es geht bei dieser Schicht nicht um eine verbesserte Übertragung sondern um die Lösung von Synchronisationsproblemen und Aspekte der Steuerung von Dialogen.

Synchronisationsprobleme können z. B. auftreten, wenn einer der beteiligten Kommunikationspartner abstürzt. Zur Problemlösung wird ein komplexer Mechanismus angeboten, bei dem es den Nutzern ermöglicht wird sogenannte Sicherungspunkte zu setzen. Dabei erfolgt eine Sicherung aller relevanten Verarbeitungsdaten. Nach einem evtl. Systemabsturz kann die Verarbeitung ab dem Stand des letzten Sicherungspunktes fortgesetzt werden.

Die Dialogsteuerung gestattet die Vereinbarung der Kommunikationsinitiativen (Aktivitäten) und der Verarbeitungsrichtung (Simplex-, Duplex- und Halbduplexkommunikation). Für die Kommunikation von Anwenderprozessen müssen Regeln bestimmt werden. So kann z. B. festgelegt werden, dass in einer Produktionssteuerungsanlage ein Messwertgeber regelmäßig von einer Messwarte abgefragt wird aber auch die umgekehrte Verfahrensweise, das der Messwertgeber von sich aus regelmäßig an die Warte sendet. Die Kommunikationsregeln bestimmen nach inhaltlichen Gesichtspunkten, welcher Prozess die Kommunikationsinitiative übernimmt und welcher Prozess passiv ist.

Die Kommunikationssteuerungsschicht bietet die Möglichkeit, den Datenaustausch zu gliedern, Als Beispiel soll die Übertragung einer Serie von Dateien dienen. Die Dateisätze können als Nachrichten verschickt werden. Die Übertragung einer großen Datei wird in mehrere Dialogeinheiten gegliedert. Die Übertragung einer gesamten Datei kann als Aktivität definiert werden. Die Kommunikationssteuerungsschicht erlaubt das flexible Beginnen, Unterbrechen, Weiterführen und Beenden von Aktivitäten.

Für die Problematik der Kommunikationssteuerungsschicht interessierten sich die wenigsten Anwendungsprogrammierer. Die von der ISO vorgeschlagenen Implementierungsstandards wurden weitgehend ignoriert.

5.3.6 Darstellungsschicht

Die Darstellungsschicht unterstützt Instanzen der Anwendungsschicht, indem sie Mechanismen bereitstellt, mit deren Hilfe Informationen zwischen den Rechnern im Netz ausgetauscht werden können, auch wenn sie unterschiedliche Informationsdarstellungen haben.

Weiterhin hat die Darstellungsschicht die Aufgaben der evtl. Komprimierung und Verschlüsselung von Übertragungsdaten.

Voraussetzung der verteilten Verarbeitung ist, dass die beteiligten Prozesse sich verstehen, d. h. dass sie bei einem Datenaustausch Sender und Empfänger alle Informationen in gleicher Weise interpretieren.

Dies ist trivial bei homogenen Rechnernetzen, die aus gleichartigen Rechnern mit gleichen Betriebssystemen bestehen. In Rechnernetzen mit Rechnern und Betriebssystemen beliebiger Hersteller kann es dagegen zu Interpretationsunterschieden beim Nachrichtenaustausch kommen.

Selbst für die interne Abspeicherung von Buchstaben, Ziffern und Zahlwerten existieren unterschiedliche Codes. Umso mehr gilt dies für komplexe Datenstrukturen.

Es gibt mehrere Lösungsmöglichkeiten für das Verständigungsproblem in heterogenen Netzen. Erstens kann der Sender die Informationen in die Darstellung des Empfängers konvertieren und danach versenden. Zweitens kann der Datenaustausch in der Senderdarstellung erfolgen, dann muss der Empfänger die Konvertierung vornehmen. Bei diesen Verfahren muss jeder Rechner alle denkbaren Konvertierungsverfahren beherrschen. Deshalb kann es sinnvoll sein, die Informationen in einer Transfersyntax darzustellen, bei der u. U. beide Kommunikationspartner konvertieren müssen.

Im OSI-Modell ist eine Darstellungsschicht vorgesehen, deren Dienste die Instanzen der Anwendungsschicht von der Darstellungsproblematik entlasten.

Die Anwendungsinstanzen verwenden eine abstrakte Syntax, z. B. die Bezeichnung INTEGER. Die lokale Darstellung kann dabei durchaus unterschiedlich sein. Die Übertragung erfolgt in einer Transfersyntax, die ein Bitmuster beschreibt. Für die ISO-gerechte Darstellungsnotation wurde die Sprache ASN.1 entwickelt.

Die Darstellungsschicht verfügt über Kodierregeln für die Umwandlung der abstrakten Syntax in eine standardisierte Transfersyntax. Beim Aufbau einer Darstellungsverbindung werden Darstellungskontexte vereinbart, welche die genaue Zuordnung einer Transfersyntax zu einer abstrakten Syntax festlegen (◘ Abb. 5.8). Die Transfersyntaxdarstellung enthält neben den Werten von Variablen auch noch deren Typ und Länge, z. B. für die Zahl 1000 die Angaben (INTEGER, 4 Byte, 1000).

Eine Informationskonvertierung kann auch erforderlich sein, wenn sehr große Datenmengen ausgetauscht werden müssen, die stark komprimiert werden können. Dies ist i. a. bei Multimediadaten der Fall. Bei Videos können z. B. 100 MByte pro Sekunde anfallen, die durch Kompression ohne wesentlichen Informationsverlust auf 1 % des Wertes reduziert werden. Die Übertragung unkomprimierter Videodaten wäre in Rechnernetzen überhaupt nicht realisierbar.

Viele Informationen unterliegen dem Datenschutz. Die Nachrichtenübertragung in Rechnernetzen, vor allem in WAN, kann schwer gegen Missbrauch geschützt werden. Ein Ausweg ist die Übertragung verschlüsselter Daten. Inzwischen existieren sichere und praktikable kryptographische Verfahren.

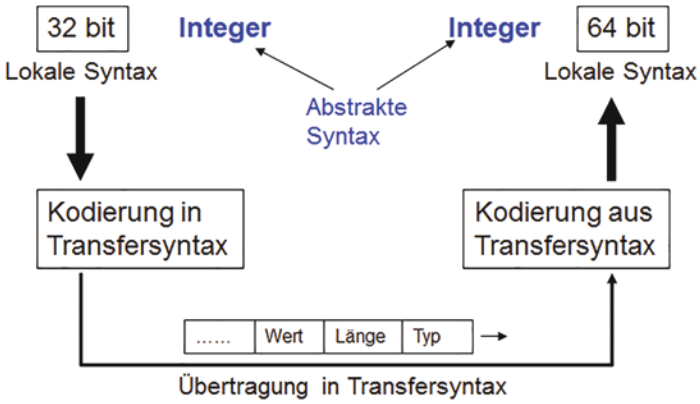


Abb. 5.8 Informationsaustausch in heterogenen Systemen

Die Verschlüsselung bzw. Entschlüsselung ist ebenfalls eine Aufgabe der Darstellungsschicht.

Die Problematik der Darstellungsschicht ist hochaktuell. Die von der ISO vorgeschlagenen Implementierungen sind allerdings ungebräuchlich. Jedoch werden einige Aspekte in aktuellen Anwendungen genutzt, z. B. die Sprache ASN.1 beim Rechnernetzmanagement.

5.3.7 Anwendungsschicht

Die höchste Schicht des OSI-Modells ist die Anwendungsschicht. Sie beinhaltet für den Menschen direkt nutzbare Anwendungen, wie Dateitransfer, E-Mail, Computerfernbedienung.

Weiterhin werden komfortable Unterstützungen für den Anwendungsprogrammierer bereitgestellt.

Die Zielstellung der OSI-Anwendungsschicht ist weiterhin aktuell, die von der ISO vorgeschlagenen Implementierungen wurden aber größtenteils durch Internetapplikationen verdrängt.

Einige Standards finden aber auch heute noch breite Anwendung, z. B. der Verzeichnisstandard nach X.500.

5.3.8 Bewertung des OSI-Konzepts

Das OSI-Referenzmodell ist kein Implementierungsmodell und legt deshalb keine detaillierte Netzwerkarchitektur fest. Es stellt vielmehr einen Rahmenstandard dar und beinhaltet die Abstraktion der OSI-Problematik.

Jedoch entwickelte die ISO auch Standards für die einzelnen OSI-Schichten. Bei den unteren Schichten wurden meist bewährte Standards übernommen, z. B. von der internationalen

Telekommunikationsstandardbehörde ITU (bzw. CCITT) oder vom amerikanischen Fachverband IEEE (Institute of Electrical and Electronics Engineers). Für die oberen Schichten wurden eigene ISO-Standards verabschiedet, die sich jedoch in der Regel nicht nachhaltig durchgesetzt haben.

Für die Begriffsbildung in der Informatik, für das Einarbeiten in die Rechnernetztechnologie und für den Vergleich verschiedener kommerzieller Rechnernetze ist das Referenzmodell von großem Wert.

5.4 Zwischenfragen/Übungsaufgaben

5.4.1 OSI-Schichtenarchitektur

a) Erklären Sie die Begriffe Dienstzugriffspunkt (Service Access Point) und Dienstelement (Service Primitive).
b) Kann eine Instanz der OSI-Schicht 5 direkt auf Dienste der Schicht 3 zugreifen?

5.4.2 Schichten im OSI-Referenzmodell

a) Ein Rechnernetz mit einer 7-Schichtenarchitektur habe pro Schicht einen Verlust der Übertragungsrate von 10 % infolge Overhead. Wie hoch ist die Anwendungs-Übertragungsrate in einem Fast-Ethernet-LAN (100 MBit/s)?
b) Welche der OSI-Schichten beschäftigt sich jeweils mit
   - Übertragung von Bitströmen
   - Ende-zu-Ende-Kommunikation
   - Wegewahl?
c) Warum benötigen Vermittlungsstellen weniger Schichten?

Internet-Architektur

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_6

6.1 Internet-Schichtenmodell

Das Internet hat bereits eine relativ lange Geschichte. Die Internet-Architektur wurde entwickelt, um Rechnernetze anderer Architektur an das ARPANET anzuschließen. Dabei ging man sehr pragmatisch vor. Es wurden einfache, ressourcensparende und schnell realisierbare Lösungen bevorzugt. Im Ergebnis entstand das dezentral konzipierte Internet, das genaugenommen aus vielen miteinander verbundenen Rechnernetzen besteht, die aber alle die Internet-Protokolle verwenden. Lediglich die Adressenvergabe erfolgt teilweise zentral.

In der Praxis hat sich das Vorgehen bewährt. Im Bereich der flächendeckenden Rechnernetze ist das Internet das mit Abstand größte Netz [16, 17].

Die Internetarchitektur hat einen wesentlich pragmatischeren Ansatz als die theoretisch anspruchsvollere OSI-Architektur. So werden z. B. die Begriffe „Dienst“ und „Protokoll“ nicht so sauber getrennt wie beim OSI-Modell [17]. Deswegen diskutieren wir auch bei Internetproblemen teilweise nach der OSI-Terminologie.

Bei der Internet-Architektur wird vorausgesetzt, dass für die Funktionalität der unteren zwei OSI-Schichten technische Lösungen existieren. Die darüber liegenden Internetschichten für die Vermittlungsschicht und die Transportschicht, das Paketvermittlungsprotokolle IP (Internet Protocol) und die Transportprotokolle UDP und TCP (Transmission Control Protocol) bilden den eigentlichen Kern der Internetarchitektur. Die Funktionalität der OSI-Schichten 5 bis 7 werden innerhalb der Internet-Anwendungsschicht von den Applikationen mit abgedeckt und es existiert keine strenge Schichtenkonsistenz.

Genaugenommen hat also die Internet-Architektur nur vier Schichten (s. ◘ Abb. 6.1).

Die ersten Internetapplikationen (in den 70er-Jahren) waren Unterstützungen der Computerfernbedienung (Telnet), des Filetransfers (FTP) und der E-Mail-Kommunikation (SMTP). Große Bedeutung hat davon nur noch die E-Mail-Kommunikation mittels SMTP.

Jedoch erfolgte eine ständige Erweiterung um neue Dienste und qualitative Verbesserungen, sodass heute eine vollständige Übersicht aller Applikationen unmöglich erscheint.

Hier eine Auswahl aktueller Applikationen:

- WWW (World Wide Web): ursprünglich ein System zur Bereitstellung wissenschaftlicher Dokumente, inzwischen tatsächlich weltweit verbreitet für verschiedenste Nutzungen.
- Skype: ein sehr beliebtes (Video)-Telekonferenzprogramm insbesondere für die preiswerte internationale Mensch-Mensch-Kommunikation.

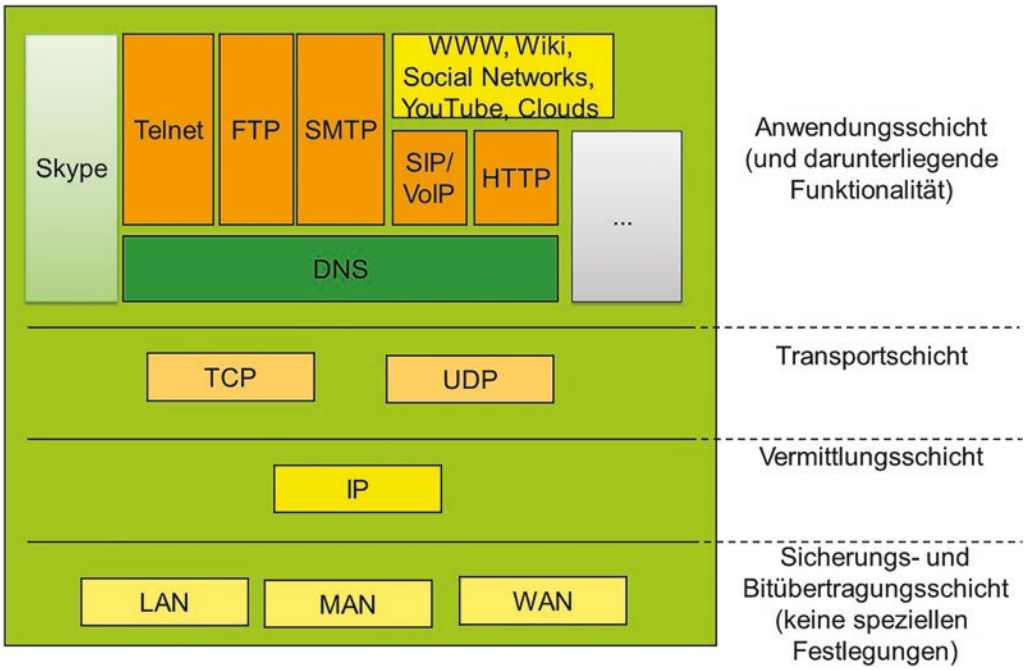


Abb. 6.1 Internet-Architektur

- SIP (Session Initiation Protocol): Basisprotokoll zur Telefonie über das Internetprotokoll IP.
- DNS (Domain Name System): Verzeichnisdienst zur Zuordnung von Namen zu Internetadressen, eigentlich ein klassischer Dienst, aber immer noch unverzichtbar.

Das Internet ist eigentlich eine „Netz von Netzen" und besteht aus autonomen Systemen AS, die juristisch und ökonomisch selbstständig sind, aber miteinander kommunizieren können, weil sie alle mit den gleichen Kommunikationsprotokollen arbeiten.

In der Praxis unterscheidet man die Begriffe „Internet" als weltweites Kommunikationsnetz und „Intranet" als abgeschlossenes Netz in einem Unternehmen bzw. einer Wohnung. Die Intranet benutzen dabei reservierte Adressen, die nur Intranet-intern verwendet werden können.

6.1.1 Internet: historische Entwicklung

Die Geschichte des Internet und die wichtigsten Entwicklungstrends sind in Tab. 6.1 kurz dargestellt [16]:

Tab. 6.1 Geschichte des Internet und Entwicklungstrends

1970	ARPANET (ca. 100 Rechnernetze), 50 kBit/s-Leitungen
1973	TCP/IP, Internetzwerk-Architektur
1974	Verbesserte TCP/IP-Versionen, PRNET (Packet Radio), 100 kBit/s, SATNET (Satellite Net), 64 kBit/s, (USA, Deutschland, Italien etc.)
1979	ARPA ICCB (Internet Configuration Control Board)
1980	Internet-kompatible lokale Netze
1983	Implementierung von TCP/IP im Betriebssystem UNIX und Etablierung an den Universitäten als Kommunikationsstandard, Vereinheitlichung der Netzkopplung
1984	Abspaltung des MILNET, Spezielle Förderung des CSNET (Comp. Science Net)
1985	IAB (Internet Activity Board) mit Task Forces als Ersatz für ICCB, neue Netze in Europa etc.
1989	IAB aufgeteilt in IETF (Internet Engineering Task Force) und IRTF (Internet Research Task Force)
1990	NSFNET (National Science Foundation Net) mit bis zu 1,5 MBit/s als Ersatz für ARPANET
1992	WWW (World Wide Web); Internet Society (starke Industriebeteiligung)
1995	Neue Protokolle (IP next generation etc.)
1999	Zunehmende Verbreitung von Electronic Commerce und Multimedia
2000	Weitere deutliche Leistungserhöhung; Gigabit-Wissenschaftsnetz; zunehmender Einsatz optischer Netze, WDM (Wave Division Multiplex), OFDM (Orthogonal Frequency Division Mutiplex)
2002	Web Services (WS), flexible Anwendungsprotokolle
2005	Verbreitung von Service Oriented Architectures (SOA), IoS (Internet of Services)
2007	Semantic/Web 2.0, Erweiterungen WS-*
2011	Cloud Computing, Smart Grid, IoT (Internet of Things), mobiles Internet 4G (5G ab Jahre 2020)
2014	Einsatz universeller intelligenter Vernetzung in der Industrie („Industrie 4.0“)
Ab 2018	Fog Computing, Robotik Apps in Kooperation mit Cloud Computing
*(sog. WS-Star)	

6.1.2 Unterstützte Basisnetze

Nach dem Internetkonzept kann jede Netztechnologie (Funktionalität der OSI-Schichten 1 und 2) für das Internet genutzt werden. In der Regel ist eine einmalige Schnittstellenanpassung zur Vermittlungsschicht IP erforderlich, deren Aufwand jedoch gering ist.

- **Übersicht [11]**

1. Lokale Netze (LAN; Local Area Network)/Metropolitan-Netze (MAN)
   - Klassische LAN: Ethernet, Token Ring, Token Bus
   - Moderne Ethernet-LAN: bis zu 100 GBit/s
   - Wireless LAN (drahtlose lokale Netze)

2. Weitverkehrsnetze (WAN, i. d. R. öffentlich)
   - Klassische WAN: ATM (Asynchroner Transfermodus), Frame Relay, SDH/SONET
   - MPLS (Multiprotocol Layer Switching)
   - WAN mit Hochgeschwindigkeits-Ethernettechnologien
   - WiMAX (Worldwide Interoperability for Microwave Access)
   - MBWA (Mobile Broadband Wireless Access).
3. Zugangstechnologien (öffentlich, privat)
   - DSL (Digital Subscriber Line)
   - (Kabel-)Modem (Modulation/Demodulation über analoge Leitungen)
4. Mobilfunknetze (öffentlich)
   - GSM (Global System for Mobile Telecommunication)
   - UMTS (Universal Mobile Telecommunication System)
   - CDMA (Code Division Multiple Access)
   - HSDPA (High Speed Downlink Packet Access)
   - LTE (Long-Term Evolution)
   - künftige 5G-Netze (IMT 2020).

Details zu den Netzwerktechnologien werden in Teil II diskutiert.

6.1.3 Internetzugang per PPP (Point-to-Point Protocol)

PPP ist ein Protokoll der Sicherungsschicht (Layer 2) für Internet-Zugang, z. B. über Kabelmodem oder xDSL. Der Aufbau des PPP-Frames ähnelt dem eines HDLC-Frames (s. ◘ Abb. 6.2).

- **PPP-Frameaufbau**
  - Startbegrenzer (8 Bit)
  - Adresse (8 Bit), fester Wert
  - Steuerfeld (8 Bit). fester Wert
  - Angabe des nutzenden Protokolls (8 oder 16 Bit)
  - Nutzdaten (variable Länge, bis 1500 Byte)
  - Prüfsequenz nach CRC-16, die über den Frameinhalt gebildet wird.
  - Endbegrenzer (8 Bit).

Begrenzer 01111110	Adresse (fest vorgegeben) 11111111	Steuerung (fest vorgegeben) 00000011	Protokoll-Angabe	Nutzdaten (meist bis 1500 Byte)	Prüfsequenz 16 Bit	Begrenzer 01111110

◘ **Abb. 6.2** Rahmenformat für PPP

PPP hat eine weitergehende Funktionalität als HDLC. So sind auch Aufgaben höherer Schichten integriert, u. a. das Aushandeln von Kommunikationsparametern (Zuteilung von Adressen, Masken usw.), Sicherheitsüberprüfungen und Datenkompressionen.

6.2 Vermittlungsschicht (IP)

Die IP-Schicht (OSI-Layer 3) übernimmt die folgenden Aufgaben [3, 7, 16, 17]:

- Paketvermittelte Übertragung durch sogenannte IP-Router
  IP-Pakete können bis zu 64 K Datenbytes beinhalten. In der Praxis haben sie aber nur eine Datenlänge der Nutzgröße von Ethernet (1500 Byte).
- Einheitliche Adressierung (gewährleistet Subnetzunabhängigkeit der darüber liegenden Transportschicht),
  IP-Pakete besitzen eine IP-Zieladresse im Paket-Header.
- Wegewahl (Routing),
  schrittweise Weiterleitung vom Quellrouter über diverse Zwischenstationen bis zum Zielrouter,
- Aufstellen, Anpassen und Optimieren der Einträge von Wegewahltabellen (Routingtabellen);
  Die Routingtabellen beinhalten dabei mindestens die Angabe des nächsten Routers auf dem Weg zum Ziel und die Angabe einer Wegebewertung (administrativen Distanz). Die Bewertung wird i.a. aufgrund mehrerer statischer Informationen berechnet, z. B. Datenraten der Leitungen, durchschnittliche Auslastungen usw. Prinzipiell können aber auch dynamische Informationen berücksichtigt werden, z. B. Stauinformationen.
- Bereitstellung geeigneter Routingprotokolle zur Bestimmung des optimalen Weges.
- weitere Funktionalitäten, wie z. B. Austausch von Steuernachrichten mittels des Protokolls ICMP (Internet Control Message Protocol), Überlastüberwachung usw.

Das IP-Protokoll existiert seit 1973 in der Version IPv4, die auch heute noch im anwendernahen Bereich dominiert. Schrittweise erfolgt jedoch eine Umstellung auf das modernere Protokoll IPv6.

Es existieren mehrere Routingprotokolle, die alternativ genutzt werden können [16].

- Das älteste Routingprotokoll RIP (Routing Information Protocol) war für die Wegewahl innerhalb eines relativ kleinen Netzwerkes (unter 30 Tabelleneinträge) konzipiert und konnte nicht flexibel mit unterschiedlich großen Netzwerken umgehen.

Deshalb wurde es in den 90er-Jahren zum Protokoll RIPv2 weiterentwickelt, das prinzipiell auch heute noch aktuell ist.
- OSPF (Open Shortest Path First), ein besonders häufig genutztes Routingprotokoll, das flexibel in unterschiedlich großen Netzwerken genutzt werden kann.
- IS-IS (Intermediate System to Intermediate System), dieses besitzt eine ähnliche Funktionalität wie OSPF, hat jedoch mittlerweile wenig praktische Relevanz.
- EIGRP (Enhanced Interior Gateway Routing Protocol) ist eine häufig genutzte Alternative zu OSPF. Das Protokoll ist für Cisco-Router optimal zugeschnitten.
- Im Unterschied zu den oben genannten Routingprotokollen befasst sich das Protokoll BGP (Border Gateway Protocol) mit dem Routing zwischen autonomen Systemen AS (s. Abschn. 6.2.3).

Die Wegewahlverfahren können untergliedert werden in globale, verteilte, lokale und hierarchische Verfahren [16, 17].

1. Global (Link State Routing):
   Die gesamte Topologie eines (Teil-)Netzes ist allen Routern bekannt. Topologieänderungen werden allen Routern mitgeteilt.
   Für das Routing ermitteln die Router den „kürzesten" Weg innerhalb des Topologiegraphen und leiten die Datenpakete entsprechend weiter.
   Das Protokoll OSPF arbeitet z. B. nach diesem Prinzip (s. Abschn. 6.2.1).
2. Verteilt (Distance Vector Routing):
   Die Router kennen nicht die gesamte Topologie des Netzwerkes, sondern zunächst nur ihre Nachbarrouter und den „Abstand" zu diesen. Regelmäßig werden die Routinginformationen zwischen den Nachbarroutern ausgetauscht, sodass schrittweise eine sogenannte Distanzvektortabelle aufgebaut werden kann, die für jedes Ziel den optimalen Nachbarrouter und die „Länge" des Übertragungsweges enthält.
   Das Protokoll RIPv2 arbeitet z. B. nach diesem Prinzip.
3. Lokal (kein dynamischer Austausch von Weginformationen):
   - Hot Potato: Bei alternativen Wegen sofort Absenden an Weg mit kürzester lokaler Warteschlange.
   - Rückwärtslernen: Bei Paketankunft die Absenderadresse auswerten und zukünftig Pakete für dieses Ziel in Gegenrichtung senden.
   - (Selektives) Fluten: Paket an alle Nachbarn (oder Teilmenge) weiterleiten

3. Hierarchisch:
   Kombination globaler Verfahren (wie bspw. OSPF) innerhalb von autonomen Systemen und dem sogenannten Grenzrouting (z. B. mit BGP) zwischen verschiedenen Autonomen Systemen.

6.2.1 Globales Wegewahlverfahren OSPF

Das Routingverfahren OSPF (Open Shortest Path First) enthält intern einen von dem Mathematiker Edsger W. Dijkstra entwickelten Algorithmus für die Suche des kürzesten Pfades innerhalb eines Graphen.

Die „Länge" des Pfades ist in der Regel die Anzahl der zu passierenden Router, aber es können auch komplexere Metriken verwendet werden, welche die Verzögerungszeit, die geografische Entfernung, die Auslastung und auch Kosten berücksichtigen.

Der Dijkstra-Algorithmus soll im Folgenden beschrieben werden [17].

Voraussetzung ist die Kenntnis des Topologiegraphen, der alle Router als Knoten und die Verbindungsleitungen als bewertete Kanten enthält.

Nun besteht die Routingaufgabe darin, den kürzesten Weg vom Quell- zum Zielrechner zu bestimmen. Im Endergebnis soll jeder Knoten im Netzwerk eine Beschriftung erhalten mit dem Inhalt (Entfernung zum Ziel, Nachfolger).

Der Dijkstra-Algorithmus kennt vorläufige und permanente Knotenbeschriftungen. Zunächst besitzen die Knoten keine Beschriftungen. Dann erhält der Zielknoten eine triviale permanente Kennung, da er keinen Nachfolger hat und die Zielentfernung Null ist. Danach werden schrittweise die weiteren Knoten permanent beschriftet nach folgender Prozedur:

/* Gesucht: kürzester Pfad zum Knoten X */

1. *X permanent und Arbeitsknoten*
2. *Bei allen Nachbarn Abstand zu Arbeitsknoten ermitteln und Knoten*
   vorläufig beschriften, wenn neuer Abstand kleiner als alter, ersetzen
3. *Untersuchung aller bisher vorläufig beschrifteten Knoten im Graph, kleinster wird permanent und Arbeitsknoten*
4. *Wenn Endknoten permanent, dann terminiere, sonst (2)*

In ◘ Abb. 6.3 wird der Algorithmus an einem Beispiel erläutert. Es werden jeweils die Teilbilder kommentiert.

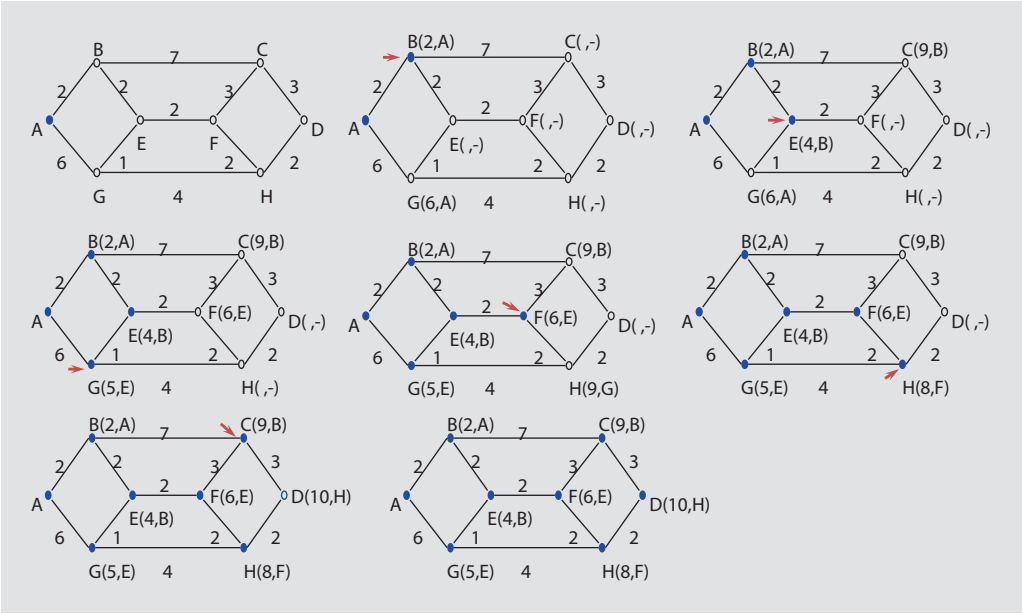


Abb. 6.3 OSPF Wegewahlverfahren

Vorgehen:

1. Knoten A wird als Arbeitsknoten markiert.
2. Abstandsbestimmung für Nachbarknoten B und G zum Arbeitsknoten A
   Kantenbeschriftung bei B und G eintragen
   Knoten B wird neuer Arbeitsknoten, da Abstand kürzer, Beschriftung wird permanent
3. Abstandsbestimmung für Nachbarknoten C und E zum Arbeitsknoten B
   Kantenbeschriftung bei C und E eintragen
   Knoten E wird neuer Arbeitsknoten, da kürzester Abstand, Beschriftung wird permanent
4. Abstandsbestimmung für Nachbarknoten F und G zum Arbeitsknoten E
   Kantenbeschriftung bei F eintragen und bei G aktualisieren
   Knoten G wird neuer Arbeitsknoten, da kürzester Abstand, Beschriftung wird permanent
5. Abstandsbestimmung für Nachbarknoten H zum Arbeitsknoten G
   Kantenbeschriftung bei H eintragen
   Knoten F wird neuer Arbeitsknoten, da kürzester Abstand, Beschriftung wird permanent
6. Abstandsbestimmung für Nachbarknoten C und H zum Arbeitsknoten F
   Kantenbeschriftung bei H aktualisieren

Knoten H wird neuer Arbeitsknoten, da kürzester Abstand, Beschriftung wird permanent

7. Abstandsbestimmung für Nachbarknoten D zum Arbeitsknoten H
   Kantenbeschriftung bei D eintragen
   Knoten C wird neuer Arbeitsknoten, da kürzester Abstand, Beschriftung wird permanent
8. Abstandsbestimmung für Nachbarknoten D zum Arbeitsknoten C
   keine neue Kantenbeschriftung bei D erforderlich
   Knoten D wird letzter Arbeitsknoten, Beschriftung wird permanent, Algorithmus beendet

Ein Auswerten des permanent beschrifteten Graphen ergibt z. B.

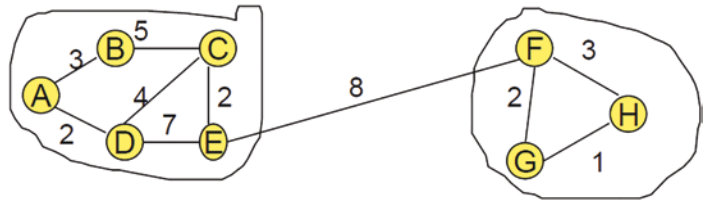
- Weg D → A
  Weglänge: 10
  Strecke: D → H → F → E → B → A
- Weg C → A
  Weglänge: 9
  Strecke: C → B → A;

6.2.2 Hierarchisches Wegewahlverfahren OSPF und BGP

Das Verfahren kombiniert die Protokolle OSPF und BGP (s. ◘ Abb. 6.4) und ist für weltweite Verbindungen großer Netze sehr gut geeignet.

Ein autonomes System AS besteht aus einer Ansammlung von IP-Netzwerken, die von einem Provider betrieben werden. Innerhalb der abgegrenzten Bereiche der autonomen Systeme werden i. A. verteilte Wegewahlverfahren mit dynamischer Anpassung an Topologieänderungen genutzt, oft mittels OSPF.

Befinden sich die Ziele nicht im gleichen AS ist ein AS-AS-Routing erforderlich. Der globale Austausch von Informationen erfolgt mittels des BGP-Protokolls (Border Gateway Protocol) zwischen den verschiedenen AS. Diese besitzen jeweils eine weltweit eindeutige AS-Adresse. Jedes AS meldet den



◘ **Abb. 6.4** Hierarchisches Wegewahlverfahren: OSPF + BGP

anderen, welche Teilnetze in ihm integriert sind. Dadurch kann das Ziel-AS ermittelt werden.

Beim AS-AS-Routing werden nicht nur rein technische Parameter, wie Entfernung, optimiert, sondern auch ökonomische und politische Aspekte berücksichtigt.

Innerhalb des Ziel-AS erfolgt wieder ein AS-internes Routing. Quell- und Ziel-AS müssen nicht zwingend die gleichen internen Routingverfahren benutzen [16].

6.2.3 Überlastüberwachung

Eine der weiteren Funktionalitäten der Netzwerkschicht die Überlastüberwachung. Diese kann z. B. durch die Nutzung von sogenannten Choke-Paketen erfolgen, die einen Sender zur Reduktion der Sendedatenrate veranlassen sollen.

Das Problem besteht darin, dass die Übertragungsdauer von Paketen im Internet nicht vernachlässigt werden kann. Wenn der Sender auf Überlastungen beim Empfänger zu stark reagiert, kann es zu Regelschwingungen kommen, d. h. es wechseln sich Phasen mit Überlastung und Phasen mit relativen „Leerlauf" miteinander ab.

Deshalb erfolgt meist eine allmähliche Anpassung an veränderte Lastverhältnisse. Regelmäßig wird die Last gemessen. Die aktuelle Last wird mit der vorher gemessenen Last verglichen und nur wenn die durch einen Anpassungsfaktor a gewichtete neue Last einen Schwellwert übersteigt, wird eine Choke-Nachricht gesendet.

$$\text{Last}_{\text{neu}} = a * \text{Last}_{\text{alt}} + (1 - a) * \text{Last}_{\text{aktuell}}, \tag{6.1}$$

a = 0 - sofortige Aktualisierung

0 < a < 1 - Anpassung; je größer a, desto langsamer

Nach Empfang eines Choke-Paketes sollte der Sender dann seine Übertragung für eine bestimmte Zeit einstellen bzw. stark reduzieren. Dadurch erfolgt die Begrenzung der Datenrate (Traffic Shaping).

Weitere Techniken zur Überlastverhinderung innerhalb der Vermittlungsschicht sind über QOS-Kontrollen (Quality of Service) möglich.

Zu Einen können für die zu übertragenden Pakete Verkehrsklassen unterschiedlicher Priorität (Differentiated Services) definiert werden. Dann werden die priorisierten Pakete bevorzugt und staufrei transportiert. Dies ist beispielsweise sinnvoll, um Sprachdaten bei der Internettelefonie (Voice over IP) in guter Verständigungsqualität zu transportieren.

Des Weiteren ist die Reservierung von Datenraten über den Übertragungsweg mittels des RSVP-Protokolls (Resource Reservation Protocol) möglich.

In den meisten Fällen erfolgt im Internet allerdings keine Staukontrolle innerhalb der Vermittlungsschicht, sondern es wird erwartet, dass in der nächsthöheren Transportschicht Überlastprobleme verhindert werden. Dies leistet z. B. das TCP-Protokoll (Transmission Control Protocol), nicht aber das UDP-Protokoll (User Datagram Protocol).

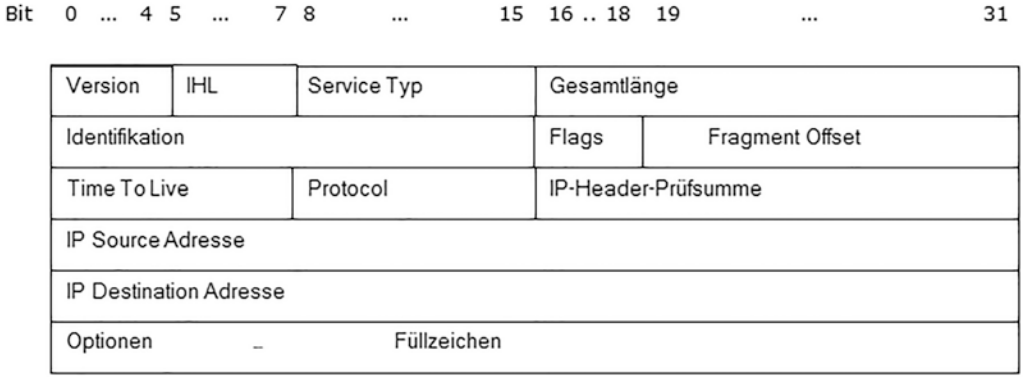
6.2.4 Internet Protocol (IPv4) und logische Adressierung

Wir beschränken unsere Betrachtungen zunächst auf das traditionelle Protokoll IPv4.

Bei diesem erfolgt eine paketorientierte Übertragung von einem Quell- zu einem Zielrechner ohne Qualitätssicherung. Ein Paket besteht aus einem Header von 20 Bytes, evtl. um Optionen verlängert, und einem daran anschließenden Datenteil. In ◘ Abb. 6.5 ist der Aufbau eines Paketkopfes in Zeilen von jeweils 32 Bit bzw. 4 Byte dargestellt [17].

Legende zur Abbildung:

- **Version** - Versionsnummer hier Zahl „4“
- **IHL** - Länge des Headers (variabel)
- **Servicetyp** - Prioritätenangabe
  (wird in der Praxis von den meisten Routern ignoriert)
- **Gesamtlänge** - Paketlänge (theoretisch bis 65536 Bytes)
  in der Praxis meist max. 1500 Byte, damit Paket in einen Ethernet-frame passt
- **Identifikation** - dient der eindeutigen Identifizierung einzelner Datenpakete,
  erforderlich, da IP keine korrekte Reihenfolge beim Empfänger garantiert



◘ **Abb. 6.5** IPv4-Header

- **Flags** - Anzeige, ob ein Paket zerteilt (fragmentiert) wurde,
  evtl. erforderlich, wenn das Paket für eine Teilstrecke zu groß ist
- **Fragment Offset** - Position der Fragmentdaten relativ zum Anfang des unfragmentierten Pakets
- **Time to Live** - TTL, Maximale Lebensdauer bzw. Angabe der maximalen Teilstecken,
  Jeder Router dekrementiert die TTL-Angabe,
  falls TTL = 0 wird Paket verworfen und Quellrechner informiert.
- **Protocol** - Angabe des Transportprotokolls
- **IP**-Headerprüfsumme - dient der Fehlerprüfung des Headers, aus Zeitgründen nicht des Paketinhalts
- **IP**-Adressen - 32-Bit-Adressen zur eindeutigen Identifikation von Quell- und Zielrechner

Die IPv4-Adressen besitzen eine Länge von 32 Bit und sind reine Identifikationsnummern, d. h. sie beinhalten keine Informationen zur Lokalisierung, wie Länder-, Stadtkennung usw.

Sie werden byteweise dezimal notiert und jeweils durch einen Punkt getrennt, z. B.
141.76.40.3

Die IP-Adressvergabe erfolgt durch die zentrale Organisation IANA (Internet Assigned Numbers Authority) bzw. deren regionalen Unterorganisationen RIR (Regional Internet Registries), z. B. für Europa in Amsterdam.

Die IP-Adressen werden unterteilt in einen Anteil „Netzwerkadresse“ und einen Anteil „Hostadresse“. Die Router werten für die Wegewahl nur die Netzadresse aus. Erst im Zielnetz wird die Hostadresse genutzt, um das IP-Paket an den konkreten Zielrechner zu senden.

Ursprünglich verwendete man eine starre Aufteilung des Adressraumes in Netzwerkklassen. Netze der Klasse A beginnen nach dieser Regelung mit dem Bitwert 0, Netze der Klasse B mit der Bitfolge 10 und Netzwerke der Klasse C mit der Bitfolge 110 (s. ◘ Abb. 6.6). Die für Mehrpunktkommunikation (Multicasting) reservierten Adressen der Klasse D beginnen mit der Bitfolge 1110, der Rest ist reserviert.

Die oben erwähnte Adresse 141.76.40.3 ist demnach eine B-Klassen-Adresse mit dem Netzwerkadressenanteil 141.76 und dem Hostanteil 40.3 (s. ◘ Abb. 6.7).

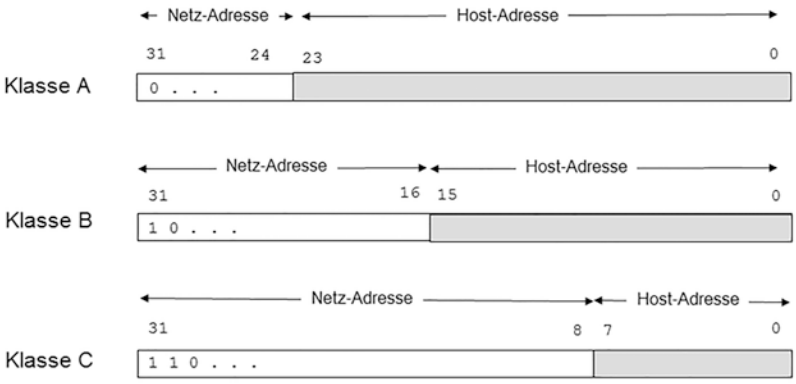
Die meist gefragten IPv4-Adressen gehören den Klassen B und C an.

Beispiel 6.1

Beispielhafte Adressen aus der Klasse B und Kommentare:
129.13.0.0 - (Netzwerkadresse – alle Rechnerbits auf „0“ gesetzt)
129.13.4.53 - (ein bestimmter Rechner)
129.13.255.255 - (Broadcast – alle Rechnerbits auf „1“ gesetzt)

Klasse A	0(1)	Netz (7)			Host (24)		(1.... bis 126....)
Klasse B	1(1)	0(1)	Netz (14)		Host (16)		(128.1.... bis 191.254....)
Klasse C	1(1)	1(1)	0(1)	Netz (21)	Host (8)		(192.1.1.... bis 223.254.254....)
Klasse D	1(1)	1(1)	1(1)	0(1)	Multicast-Adresse (28)		(224.... bis 239....)
Klasse E	1(1)	1(1)	1(1)	1(1)	0(1)	reserviert	

a) Bereiche für A, B, C, D und E



b) Schemata „Netzadresse-Hostadresse“ für A, B und C

Abb. 6.6 IPv4 – Klassenbildung

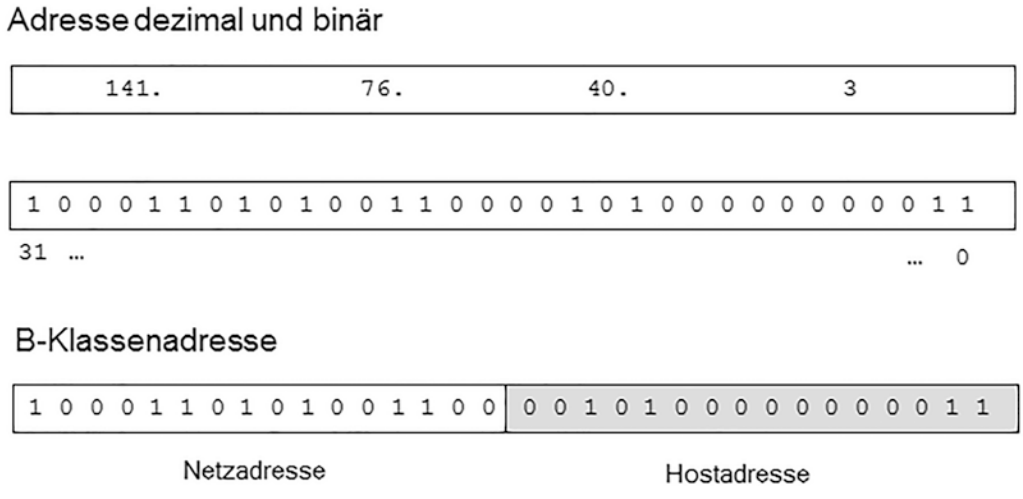


Abb. 6.7 Beispiel einer B-Klassenadresse

Die A-Klasse-Netze waren für die Internetadministration vorgesehen, die B-Klasse-Netze für Universitäten und Großunternehmen und die C-Klasse-Netze für kleinere Unternehmen.

Nachteilig an der IP-Klasseneinteilung ist die ineffektive Nutzung des IP-Adressraumes. Beispielsweise besitzen Universitäten in der Regel weniger als 2^{16} Rechner und Kleinunternehmen weniger als 2^8 Rechner, d. h. ein großer Teil der zugeteilten Adressen wird nicht genutzt.

Ein weiterer Nachteil besteht in der zu geringen Anzahl an verfügbaren Netzwerkadressen. So stehen für Universitäten und Großunternehmen nur 2^{14} (ca. 16000) verschiedene Netzwerkadressen zur Verfügung, was bereits Anfang der 90er-Jahre zu Engpässen führte.

Deshalb wird heutzutage die Klasseneinteilung von IP-Adressen nur in speziellen Fällen praktiziert, sondern es wird die Nutzung von CIDR (Classless Inter-Domain Routing) empfohlen. CIDR beschreibt ein Verfahren zur effizienteren Nutzung des bestehenden IPv4-Adressraumes.

6.2.5 Subnetzmasken und Subnetting

Ein erster Schritt zur effektiveren Nutzung des IP-Adressraumes ist eine Unterteilung großer Netze in Subnetze [17].

Dazu wird im Gegensatz zur Klasseneinteilung eine flexible Aufteilung der IP-Adressen in Netzwerk- und Hostanteil realisiert. Für die Notation existieren zwei Möglichkeiten:

- Angabe einer Netzwerkmaske
  (32-Bit-Folge mit Wert „1“ an Positionen des Netzanteiles
  und Wert „0“ an Positionen des Host-Anteiles)
- Angabe der Bitstellen des Netzwerkanteiles.

So soll aus dem Adressraum des bereits erwähnten B-Klassennetzwerkes ein kleineres Subnetz gebildet werden, dass einen Netzwerkanteil von 24 Bit und einen Hostanteil von 8 Bit besitzt. Dieses Beispiel illustriert ◘ Abb. 6.8.

Die Netzadresse wird aus der IP-Adresse und der Maske durch bitweises „logisch UND“ gebildet, der Hostanteil durch „logisch UND“ mit der negierten Maske. Im obigen Beispiel ergibt sich als Netzwerkadresse 141.76.40.0 und als Hostadresse 3.

Für die Hostadressen gibt es zwei Einschränkungen. Alle Host-Bits auf „0“ gesetzt ergibt die Netzwerkadresse und ist nicht als Rechneradresse erlaubt. Alle Host-Bits auf „1“ gesetzt ergibt die sogenannte Broadcastadresse, die ebenfalls nicht als Rechneradresse erlaubt ist. Vielmehr adressiert sie alle(!) Stationen im Subnetzwerk.

Bisher haben wir nur Masken betrachtet, die an einer Bytegrenze enden. Dies ist aber nicht selbstverständlich.

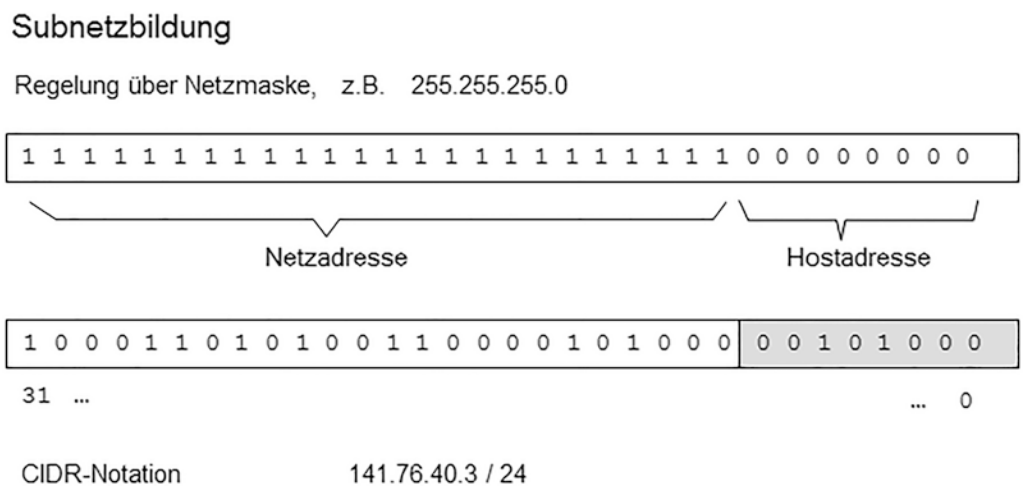


Abb. 6.8 Subnetzbildung

Die Aufteilung in beliebige Anteile erfordert sog. Mischmasken zur internen Aufgliederung in weitere Subnetze.

Beispiel 6.2
Mischmaske (gehört zu keiner Klasse!):
255.255.255.192
(entspricht: 11111111.11111111.11111111.11*000000*),
d. h. (16 + 10) Bit für Subnetzkennung und 6 Bit für Hostkennung.

Die Techniken wie Klassenbildung, Subnetting, CIDR verlieren weitgehend ihre Bedeutung mit der Einführung von IPv6 (s. weitere Abschnitte), da der zur Verfügung stehende Adressraum bei IPv6 mehr als ausreichend groß ist.

6.2.6 Adressierung in Intranet und Network Address Translation (NAT)

IP-Adressen sind „normalerweise" weltweit eindeutig. Es gibt jedoch auch Ausnahmen, die sogenannten privaten Adressen. Diese kommen zum Einsatz im sogenannten Intranet (LAN mit Internetinfrastruktur). In Tab. 6.2 sind die Adressräume der privaten Adressen dargestellt [7, 16, 17].

Durch die Nutzung privater Adressen in Intranet werden globale Adressen in Größenordnungen eingespart. Beispielsweise nutzen fast alle Schulen in Deutschland sowie private DSL-Nutzer die gleichen Intranetadressen im Bereich 192.168.x.y.

Tab. 6.2 Subnetting und Intranet

Netzadressbereich	Notation	Anzahl Adressen	Anzahl Netze gemäß Netzklasse
10.0.0.0 bis 10.255.255.255	10.0.0.0/8	$2^{24} = 16.777.216$	1 privates A-Netz mit 16.777.216 Adressen; 10.0.0.0/8
172.16.0.0 bis 172.31.255.255	172.16.0.0/12	$2^{20} = 1.048.576$	16 private B-Netze mit jeweils 65.536 Adressen; 172.16.0.0/16 bis 172.31.0.0/16
192.168.0.0 bis 192.168.255.255	192.168.0.0/16	$2^{16} = 65.536$	256 private C-Netze mit jeweils 256 Adressen; 192.168.0.0/24 bis 192.168.255.0/24

Die privaten Adressen sind innerhalb eines Intranets unbegrenzt nutzbar, können aber nicht ohne weiteres außerhalb genutzt werden. Dazu müssen sie in globale Adressen transformiert werden.

Dies löst das NAT-Protokoll mit folgenden Modifikationen [16].

1. Static NAT:
   feste Zuordnung, z. B. 192.168.54.3 => 214.15.23.1
2. Dynamic NAT:
   dynamische Zuordnung der ersten freien globalen IP-Adresse aus einem Adresspool; Rechner sind dann von außen nicht direkt abrufbar (bspw. Problem bei Voice-over-IP).
3. NAT/PAT (NAT + Port Address Translation):
   zusätzliche Berücksichtigung von TCP-Portnummern bei der Adressabbildung.
   Diese Modifikation ist am leistungsfähigsten, da komplette LANs/Intranets über eine einzige globale IP-Adresse verfügbar werden.

Beispiel 6.3

Die Aufgabe des NAT/PAT besteht konkret darin, dass im Gateway (NAT-Router) die Quell-Adressen (IP:Port) durch eine Adresskombination (Gateway-IP:Gateway-Port) ersetzt werden, d. h. die private, nicht weltweit routbare IP-Absenderadresse wird zu einer globalen Adresse!

Intranet-Hosts			*Gateway*	
Quell IP:Port	*Ziel IP:Port*	<=>	*Quell IP:Port*	*Ziel IP:Port*
192.168.0.5:5000	*170.0.0.1:80*		*213.0.0.3:6000*	*170.0.0.1:80*
192.168.0.8:5000	*170.0.0.1:80*		*213.0.0.3:6001*	*170.0.0.1:80*
192.168.0.9:5001	*170.0.0.1:80*		*213.0.0.3:6002*	*170.0.0.1:80*

6.2.7 IP-Hilfsprotokolle

Um den IP-Betrieb zu gewährleisten, sind einige Hilfsprotokolle erforderlich, z. B.:

- **ICMP** - für den Austausch von Steuerinformationen zwischen den Internetroutern
- **ARP** - für die Abbildung der IP-Adressen auf MAC-Adressen im LAN-Bereich
- **RARP** - als reverse Funktion zu ARP
- **NAT** - für die Abbildung von lokalen auf globale Adressen
- **BOOTP** - für die Vorbereitung des Bootens eines Betriebssystems über das Netzwerk
- **DHCP** - für die Unterstützung der Konfiguration der Internetprotokolle

Einige Protokolle werden im Weiteren diskutiert.

Das ICMP (Internet Control Message Protocol) ist vor allem für die Fehleranzeigen innerhalb der IP-Schicht vorgesehen. So wird beispielsweise die Flussteuerung (ähnlich „Choke-Pakete“) unterstützt und es werden Fehlermeldungen bei Nichterreichbarkeit ausgetauscht. So kann z. B. ein TTL-Wert zu klein sein, das Zielnetzwerk oder der Zielrechner nicht existieren oder nicht betriebsbereit sein. ICMP-Nachrichten können auch innerhalb von Programmen für das Netzwerkmanagement verwendet werden. Ein bekanntes Beispiel ist die Verwendung des Befehles zum Test auf Erreichbarkeit von Rechnern und zur Messung der Laufzeit zwischen Quell- und Zielrechner.
ping <hostname>

bzw. des Befehls traceroot zur Bestimmung der Routerabfolge auf dem Weg zwischen Quell- und Zielrechner.
tracert <hostname>

6.2.8 IP Multicast

Normalerweise erfolgt ein Nachrichtenaustausch im Internet zwischen zwei Rechnern. Dies kann bei einer Gruppenkommunikation zu Problemen führen. Betrachten wir als Beispiel die Video-Übertragung von einem Quellrechner an n Zielpartnerrechner. Eigentlich müssen n Informationsströme mit identischem Inhalt simultan übertragen werden. Dies belegt enorme Netzwerkressourcen und ist deshalb kostenintensiv. Außerdem kann es zur Überlastung von Leitungen führen, insbesondere nahe beim Quellrechner.

Es ist deshalb effektiver, den Datenstrom baumförmig zu verteilen. Beispielsweise soll ein Strom von einer amerikanischen Universität an jeweils drei Universitäten in drei europäischen Ländern gesendet werden. Dann ist es zweckmäßig, zunächst

einen(!) Strom über den Atlantik zu senden, diesen dann in drei Strömen in die Länder zu transportieren und abschließend in jedem Land drei Ströme an die beteiligten Universitäten zu leiten.

Diese Vorgehensweise verwirklicht eine effiziente Weiterleitung ohne Redundanz und wird als IP Multicasting bezeichnet. Das zugrunde liegende Übertragungsprotokoll heißt IGMP (Internet Group Management Protocol). Bei diesem IP Multicasting müssen sich die interessierten Empfängerteilnehmer bei einem empfängernahen Multicast-Router unter Nutzung einer Multicast-Adresse (meist D-Klasse, z. B. 224.19.3.56) anmelden. Dieser meldet dann die Empfängergruppe bei einem Multicast-Router an, der näher an der Quelle Ziel liegt. Nach mehreren Stufen ist dann der Baum vom Quellrechner zu den Empfängerrechnern aufgebaut.

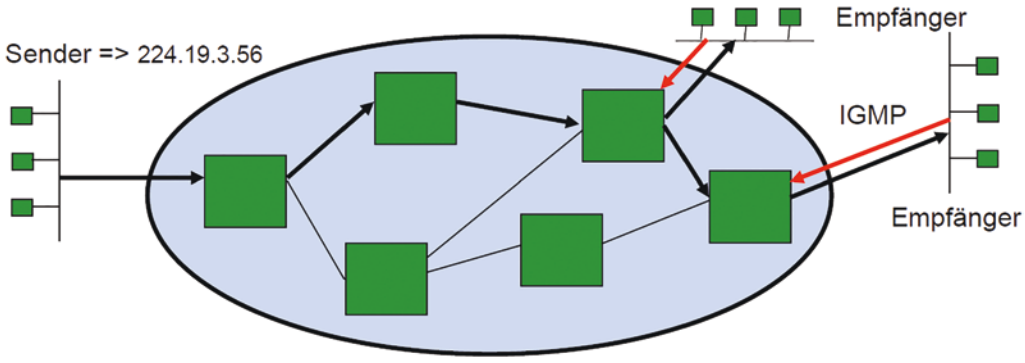
Die optimale Baumstruktur wird über Varianten des Dijkstra-Algorithmus (s. Abschn. 6.2.1) ermittelt. Während der Übertragungen erfolgt eine regelmäßige Überprüfung der Teilnehmer-Bereitschaft durch Testnachrichten der Multicast-Router (◘ Abb. 6.9).

6.2.9 IPsec: Layer3-Sicherheitsmechanismen

Das Protokoll IPsec ermöglicht eine kryptografische Absicherung auf der IP-Ebene. Die folgenden Sicherheitsziele werden verfolgt:

- **Vertraulichkeit** - (Übertragung verschlüsselter Daten)
- **Authentisierung** - (Zielrechner kann IP-Quelladresse überprüfen.)

Verschiedenste Verschlüsselungsstandards können zwischen den Kommunikationspartnern eingesetzt werden, z. B. DES, TripleDES oder AES. Für das Schlüsselmanagement dient das Protokoll IKMP (Internet Key Management Protocol),



◘ **Abb. 6.9** IP Multicast per Internet Group Management Protocol

basierend auf IKSAKMP (Internet Security Association and Key Management Protocol).

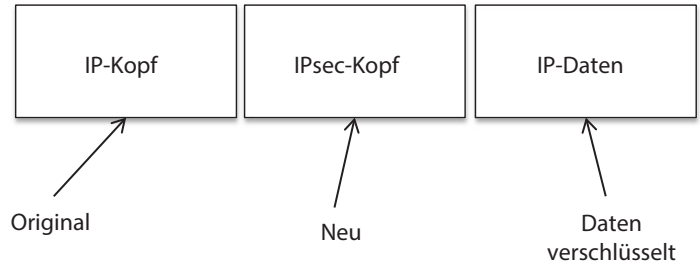
Es existieren zwei verschiedene Realisierungsformen:

- Transportmodus
- Tunnelmodus.

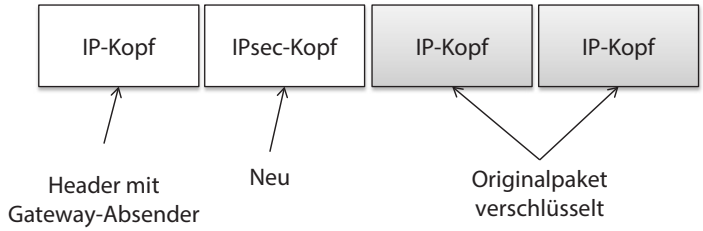
Im Transportmodus bleibt der IP-Paketheader prinzipiell erhalten, aber es wird ein modifizierter Paketinhalt berechnet. Dieser ergibt sich aus dem verschlüsselten Datenteil des originalen IP-Pakets und einem vorangestellten IPsec-Header (s. ◘ Abb. 6.10).

Vorteilhaft ist die einfache Realisierung. Es müssen aber sowohl der Quell- als auch der Zielrechner das Protokoll IPsec beherrschen. Nachteilig ist, dass beim Abfangen der IP-Pakete ein Angreifer eine Verkehrsanalyse machen kann, d. h. er weiß, wer mit wem zu welchem Zeitpunkt kommuniziert hat.

Im Tunnelmodus wird der sichere Austausch verschlüsselter Informationen zwischen zwei abgeschlossenen Firmennetzen unterstützt. Der innere Verkehr erfolgt ohne Verschlüsselung. Der äußere Verkehr erfolgt über sogenannte Gateways, die unter anderem die Verschlüsselung durchführen. Dabei wird das IP-Paket zunächst normal an ein Gateway gesendet. Im Gateway wird das komplette Paket verschlüsselt und mit einem neuen IP- und IPSec-Header versehen (s. ◘ Abb. 6.11). Als Quell- und Zieladressen werden die IP-Adressen des Quell- und des Zielgateways verwendet.



◘ **Abb. 6.10** IPsec-Transportmodus



◘ **Abb. 6.11** IPsec-Tunnelmodus

Nach Empfang des verschlüsselten Paketes erfolgt im Zielgateway die Entschlüsselung. Das gewissermaßen „ausgepackte" Paket wird danach zum eigentlichen Zielrechner gesendet.

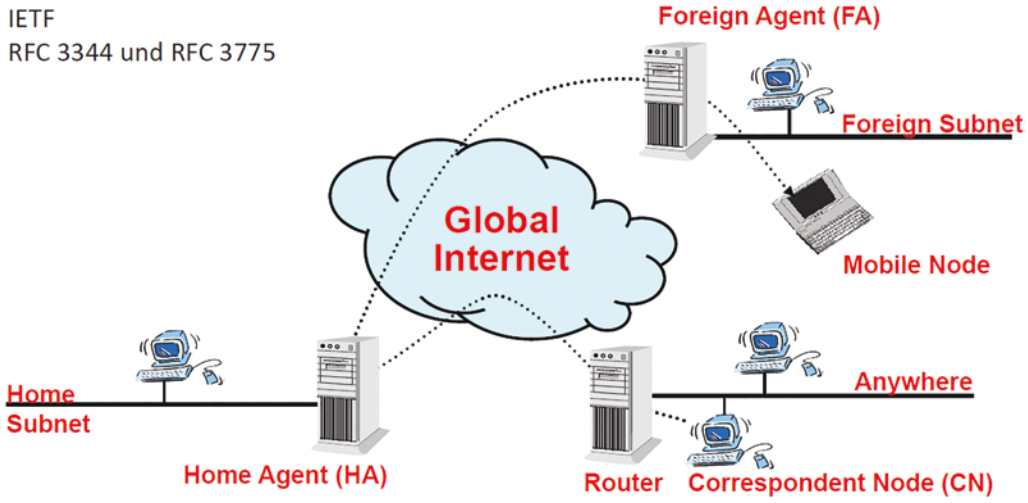
Vorteilhaft ist, dass lediglich die Gateways das IPsec-Protokoll beherrschen müssen. Außerdem sind Verkehrsanalysen nur eingeschränkt möglich. Angreifer können nur Anfangs- und Endpunkt des Tunnels feststellen, nicht aber Quell- und Zielrechner. Zur Verschleierung der Feststellung der Kommunikationsintensität können in verkehrsschwachen Zeiten sogenannte „Dummy"-Nachrichten versendet werden, die keine inhaltliche Bedeutung haben.

6.2.10 Mobile IP

Mobile-IP ist die von der Internetstandardorganisation IETF entwickelte und erweiterte Version des IP-Protokolls (RFC 3344 und RFC 3775) für mobile Endgeräte, die an unterschiedlichen Standorten an unterschiedliche IP-Netze angeschlossen werden, dabei aber ihre angestammte IP-Adresse behalten sollen.

Mobile IP erlaubt die uneingeschränkte Erreichbarkeit mobiler Endgeräte bei Beibehaltung ihrer Adresse und den nahtlosen Übergang zwischen Subnetzen (◘ Abb. 6.12). Die Schnittstellen der mobilen Endeinrichtungen zu den kabelgebundenen lokalen Netzen sind die Access Points (AP) in den unterschiedlichen IP-Subnetzen.

Das Problem der Adressierung wird dadurch gelöst, dass die Teilnehme zwei Adressen besitzen, eine permanente (Home Address) und eine temporäre IP-Adresse (COA).



◘ **Abb. 6.12** Architektur von Mobile IP

In der Architektur von Mobile IP sind die folgenden Komponenten vorgesehen [16]:

- Mobile Node (MN) mit permanenter IP-Adresse aus dem Heimatnetz (Home Subnet)
- Home Agent (HA) mit Kenntnis des aktuellen Aufenthaltsortes aller MN aus seinem Subnetz, ähnlich wie beim Mobilfunk GSM-HLR (analog in 3G-4G-Netzen)
- Foreign Agent (FA) für Zuteilung temporärer IP-Adressen COA (Care of Address) und Weiterleitung von Paketen an MN, ähnlich GSM-VLR
- Care of Address – temporäre Adresse eines mobilen Rechners aus dem Zielnetz (Foreign Subnet)
- Correspondent Node (CN) – konventioneller Kommunikationspartner im Festnetz.

Der allgemeiner Ablauf von mobile IP sieht aus wie folgt aus: MN migriert von HA zum FA mit der Aufrechterhaltung der konventionellen IP-Adressen sowie COA und bleibt für alle herkömmlichen Router ohne jegliche Änderungen erreichbar (transparente Kommunikation über Layer 3). Die FAs kümmern sich um regelmäßiges Update der Lokation des MN, informieren des HA und leiten die IP-Pakete von den herkömmlichen Routern weiter.

6.2.11 Dynamic Host Configuration Protocol (DHCP)

Normalerweise kann ein Computer erst das Internet nutzen, wenn die wichtigsten Konfigurationsparameter vorliegen. Die Eingabe der Werte für das Betriebssystem erfordert Administratorrechte und ist zeitlich aufwendig.

Deshalb wurde das Protokoll DHCP zur automatischen Vergabe von IP-Adressen und weiteren Konfigurationsdaten (wie z. B. Subnetzmaske) entwickelt. DHCP ist in flächendeckenden Netzen (z. B. in DSL-Modems), in LAN/Intranet und auch im mobilen Umfeld verfügbar.

Einen beispielhaften DHCP-Ablauf kann man in ◘ Abb. 6.13 sehen. Dabei werden vom Client über einen Broadcastruf Konfigurationsparameter angefordert (DHCPDISCOVER), danach gibt der zuständige DHCP-Server eine Angebot (DHCPOFFER). Der Client fordert anschließend verbindlich die vorgeschlagenen Konfigurationsparameter an (DHCPREQUEST) und bekommt sie zugeteilt (DHCPACK).

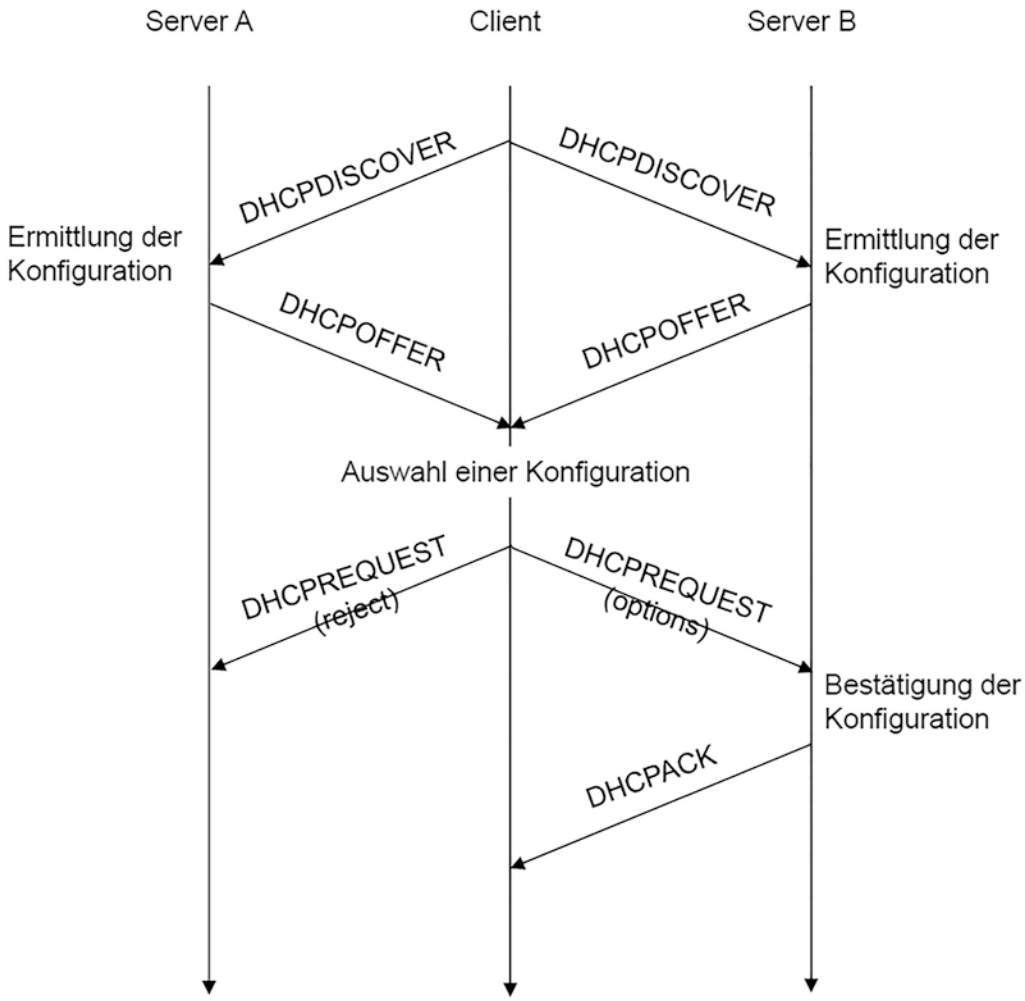


Abb. 6.13 Ein Szenario für zwei DHCP-Server und einen DHCP-Client

6.2.12 IPng und IPv6

Das Protokoll IPv4 hat sich jahrzehntelang bewährt, stößt jedoch an seine Grenzen. Der Nachfolger heißt IPng (IP next Generation) bzw. IPv6. Das Protokoll stellt eine wesentlich verbesserte Version dar. Alle positiven Features von IPv4 werden übernommen und neue hinzugefügt.

Der Hauptvorteil ist die Nutzung eines wesentlich größeren Adressraumes mit 128-Bit-Adressen (16 Byte). Für die Notation der IPv6-Adressen werden jeweils 16-Bit in Hexadezimalschreibweise zusammengefasst und mittels „:“ getrennt, z. B. [16]:
2017:0eb8:85a3:08d3:1319:8b2e:0370:7344

IPv6-Adressen erweitern die zulässige Anzahl von Knoten von 2^{32} bis auf $2^{128} = 3{,}4{*}10^{38}$. Dies ist mehr als ausreichend für alle gegenwärtig vorstellbaren Anwendungen.

Ein großer Fortschritt ist auch die Einführung neuer Adresstypen, z. B. strukturierte Adressen, die Angaben zur Lokalisierung enthalten, wie Land, Region, Provider usw. Dies erleichtert das Routing erheblich.

Im IPv6-Header sind spezielle Angaben zur Übertragungsqualität vorgesehen (Traffic Classes, Flow Labels). Dadurch wird die verbesserte Unterstützung von Quality of Service, etwa via MPLS, ermöglicht.

Ebenso wird eine vereinfachte und damit effizientere Fehlerbehandlung direkt in der IPv6-Schicht vorgenommen, was bei IPv4 im Wesentlichen den OSI-Schichten 2 und 4 überlassen wurde.

Außerdem wurden diverse Optimierungen bzgl. der Datenformate für 64-Bit-Speicherarchitekturen vorgenommen und die Unterstützung für die Netzwerkadministration wesentlich erweitert.

[Vermerk]

Seit 2014 vergibt die IANA keine IPv4-Adressen mehr, weil der Adressvorrat erschöpft ist. Die breite Einführung von IPv6 in der Praxis erfolgt dennoch eher schleppend, obwohl die Protokollimplementierungen in Betriebssystemen und Netzwerksoftware seit vielen Jahren verfügbar sind.

6.3 Transportschicht (TCP/UDP)

Die Internet-Transportschicht übernimmt die folgenden Aufgaben [17]:

- Ende-zu-Ende-Übertragung zwischen Anwendungsprozessen
  Da mehrere Prozesse auf einem Rechner parallel kommunizieren können, muss eine Multiplexingfunktion realisiert sein.
- Zuverlässige Ende-zu-Ende Datenübertragung, auch bei unzuverlässiger (nicht beeinflussbarer) Vermittlungsschicht eines Netzbetreibers
- Fehlerbehandlung (Ende-zu-Ende)
- Flusskontrolle (ebenfalls Ende-zu-Ende).

Dazu stehen die Protokolle TCP oder UDP zur Verfügung [17]. Diese genügen für die meisten Basisanwendungen (Ausnahme: Multidiakommunikation, s. in Teil III).

6.3.1 Schnittstelle zur Anwendung. Sockets

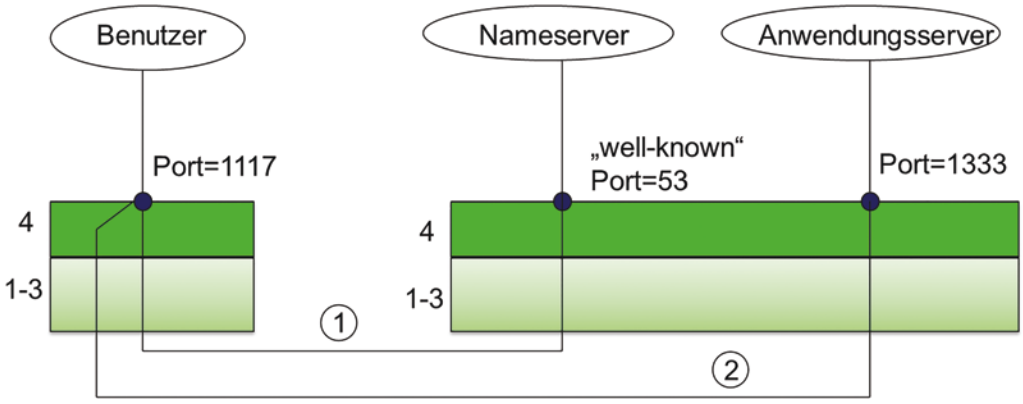
Die Schnittstelle zwischen Transportschicht und Anwendung bilden die sogenannten Sockets. Diese werden über die Angabe einer Socketadresse adressiert, die aus der IP-Adresse des Rechners und einer Portnummer besteht.
IP-Adresse [Port-Nr.]

Die Portnummer repräsentiert einen Speicherbereich für die Nachrichtenübergabe. Der Mechanismus ist bei UDP und bei TCP identisch, die Portnummernvergabe erfolgt aber unabhängig.

Ein Beispiel zur Verwendung von Portnummern ist in ◘ Abb. 6.14 dargestellt. Ein Client kommuniziert auf seinem Rechner vom Port 1117. Er will mit einem Server kommunizieren, dessen Namen (Anwendungsserver) und dessen Portnummer (1333) er kennt. Da er die IP-Adresse des Servers nicht kennt, fragt er bei einem Nameserver nach, dessen Socketadresse (IP und Port 53) er kennt. Dieser antwortet mit der Angabe der IP-Adresse des Anwendungsservers. In diesem Fall besitzt der Anwendungsserver die gleiche IP-Adresse wie der Nameserver. Nun kann die eigentliche Kommunikation zwischen dem Client (Port 1117) und dem Anwendungsserver (Port 1333) beginnen.

Die Bezeichnung Port (oder Anwendungszugangspunkt) ist bei TCP und UDP gleich. Die „Port“ hat eine Länge von 16-Bit, somit existieren Portnummern von 0 bis 65535. Die Ports 0-1023 sind fest reserviert (sog. „well-known“), z. B. Port 53 für dns, Port 80 für http etc. Die Festlegung der sog. „well-known“ Ports wird genauso wie bei IP-Adressen durch IANA (Internet Assigned Numbers Authority) standardisiert.

In ◘ Tab. 6.3 werden einige Beispiele für „well-known“ Ports dargestellt [3, 6, 7, 16]:



◘ **Abb. 6.14** Nutzung von Ports der Transportschicht

Tab. 6.3 Beispiele für „well-known" Ports

Dienst oder Protokoll	Protokoll	Portnummer
DNS (Domain Name System)	UDP, TCP	53
Daytime	UDP, TCP	13
Echo	UDP, TCP	7
Finger (Information about all users on the specified computer)	TCP	79
FTP (File Transfer Protocol)	UDP, TCP	21
Gopher (Vorläufer von WWW)	TCP	70
HTTP (Hypertext Transfer Protocol)	TCP	80
IRC (Internet Relay Chat)	TCP	194
Qotd (Quote of the Day)	UDP, TCP	17
DHCP (Dynamic Host Configuration Protocol)	UDP	67
SMTP (Simple Mail Transfer Protocol)	TCP	25
POP3 (Post Office Protocol, Email)	UDP, TCP	110
Telnet (rlogin)	TCP	23
Time (NTP, Network Time Protocol)	UDP	123

Weitere Details zu den o.g. Protokollen finden Sie in Quellen [16, 17] sowie in den Teilen II und III.

6.3.2 Protokoll UDP (User Datagram Protocol)

Das UDP-Protokoll ist durch den Standard RFC 768 definiert. Es stellt ein sehr einfaches Transportprotokoll dar mit folgenden Eigenschaften [17]:

- verbindungslos, keine Fehlerkorrektur, keine Flusssteuerung
- geringer Overhead
- keine Verzögerung durch Verbindungsaufbau
- geringe Betriebssystembelastung
- geringe Zuverlässigkeit

De facto ist UDP eine Erweiterung der IP-Schnittstelle mit keiner Verbesserung der Übertragungseigenschaften, aber mit der Möglichkeit, mehrere Anwendungsprozesse parallel zu bedienen. Die UDP-Protokoll-Dateneinheiten (Segmente) werden als IP-Pakete versendet und besitzen folgenden Aufbau (s. Abb. 6.15):

Im Inhaltsteil eines IP-Paketes befindet sich das Segment mit einem nur 8 Byte langen Header und den UDP-Daten. Der

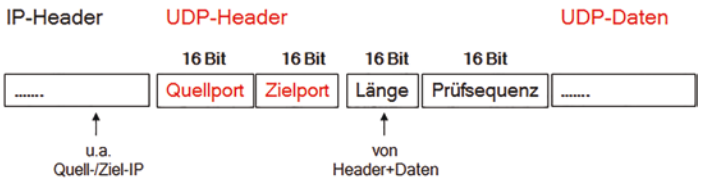


Abb. 6.15 Struktur eines UDP-Segmentes

Quell-Port (16 Bit)		Ziel-Port (16 Bit)
Sequenznummer (32 Bit)		
Piggyback Acknowledment (32 Bit)		
TCP Header length	Steuerbits	Fenstergröße (16 Bit, variabel)
Prüfsumme	urgent Pointer (relativer Bezug zu wichtiger Folgenummer)	
Optionsfeld (z.B. Aushandeln der Puffergröße)		
DATEN		

Abb. 6.16 TCP – Segmentstruktur

Header enthält die Angaben zum Quell- und zum Zielport. Zur Bildung der Socketadressen werden die IP-Adressen dem IP-Header entnommen. Weiterhin enthält der Header noch eine Längenangabe und eine Prüfsequenz über den UDP-Header und die Daten.

UDP ist zwar wenig leistungsfähig, ist aber gut geeignet als Basis für applikationsspezifische Ende-zu-Ende-Steuerungen in höheren Schichten. Dies wird beispielsweise oft für Echtzeitübertragungen genutzt (Sprache, …).

6.3.3 Protokoll TCP (Transmission Control Protocol)

Wesentlich leistungsfähiger ist das TCP-Protokoll mit folgenden Eigenschaften [17]:

- Beliebige Nachrichtenlänge, intern als Pakete von max. 64 kByte übertragen
- Reihenfolgegarantie, 32-Bit-Folgenummern
- Verbindungsauf-/abbau mit Dreiwege-Quittungsverfahren
- Fenster-basierte Flusskontrolle
- Fehlerbehandlung durch erweitertes Prüfsummenverfahren (in Software).

Die Struktur von TCP-Segmenten ist in Abb. 6.16 aufgeführt:

Der Header von 20 Byte Länge plus evtl. Optionen beinhaltet wie bei UDP Portangaben und eine Prüfsumme. Dazu kommen aber eine ganze Reihe anderer Parameter, die der Verbesserung der Übertragungsqualität dienen.

Alle Segmente werden pro Richtung nummeriert. Die Sequenznummer kennzeichnet die Richtung vom Sender zum Empfänger, die Quittungsnummer (Acknowledge) kennzeichnet die nächste erwartete Sequenznummer in Gegenrichtung. Da man für die Quittierung meist keine extra Nachricht benötigt, sondern die Quittungsinformation beim Senden mit im Segment-Header unterbringt, spricht man auch von einer Rucksackquittung (Piggyback).

Die Sequenznummer dient der Sicherung der richtigen Reihenfolge. TCP korrigiert nutzertransparent evtl. Reihenfolgeverletzungen beim Empfänger.

Grundsätzlich werden alle lückenlos übertragenen Segmente quittiert. Durch Auswertung der Quittungsnummern kann festgestellt werden bis zu welchem Zeitpunkt die Übertragung korrekt erfolgte. Es können im Sonderfall sogenannte duplizierte Quittungen auftreten. Angenommen ein Sender würde die Segmente mit den Nummern 5, 6, 7, 8, 9 senden und das Netz liefert die Segmente in der Reihenfolge 5, 6, 8, 9, 7 an den Empfänger. Dann wäre die Quittungsnummernreihenfolge 5, 6, 6, 6, 9. Das Segment 6 wurde dreimal quittiert (duplizierte Quittungen), weil das nächste erwartete Segment 7 noch ausstand. Mit dessen Eintreffen werden dann mit der akkumulierten Quittung auf 9 alle vorherigen Segmente bestätigt.

Im Verlustfall (Timeout auf ausstehende Quittung) erfolgt eine Übertragungswiederholung. Die Größe der Timeoutzeit wird dabei etwas größer als die doppelte durchschnittliche Übertragungszeit gesetzt.

Die 6 Steuerbits dienen mehreren Aufgaben:

- **URG (urgent flag)** - kennzeichnet aktuelles Byte (Adresse s. URG-Pointer)
  soll sofort vom Empfänger bearbeitet werden
- **ACK (acknowledgement flag)** - kennzeichnet gültige Quittungs-Nr. (sonst ignorieren)
- **PSH** - (push flag) fordert sofortiges Senden, soll Datenpufferung verhindern
- **RST (reset flag)** - fordert Abbrechen einer Verbindung
- **SYN** - initialisiert Verbindung (Antwort mit SYN + ACK oder RST
  Synchronisation der Sequenznummern)
- **FIN (finish flag)** - Freigabe der Verbindung, es folgen keine Daten mehr

Zunächst soll der Verbindungsaufbau (3-Wege-Handshake) zwischen zwei TCP-Instanzen diskutiert werden (s. ◘ Abb. 6.17).

1. Zunächst sendet der Initiator ein Segment (eigene Segmentnummer x zufällig gewählt) mit gesetztem SYN-Flag.
2. Der Responder erhält dieses Segment und schickt ein Antwortsegment (eigene Segmentnummer y zufällig gewählt, erwartete nächste Segmentnummer in Gegenrichtung gleich x + 1) mit gesetztem SYN- und ACK-Flag.

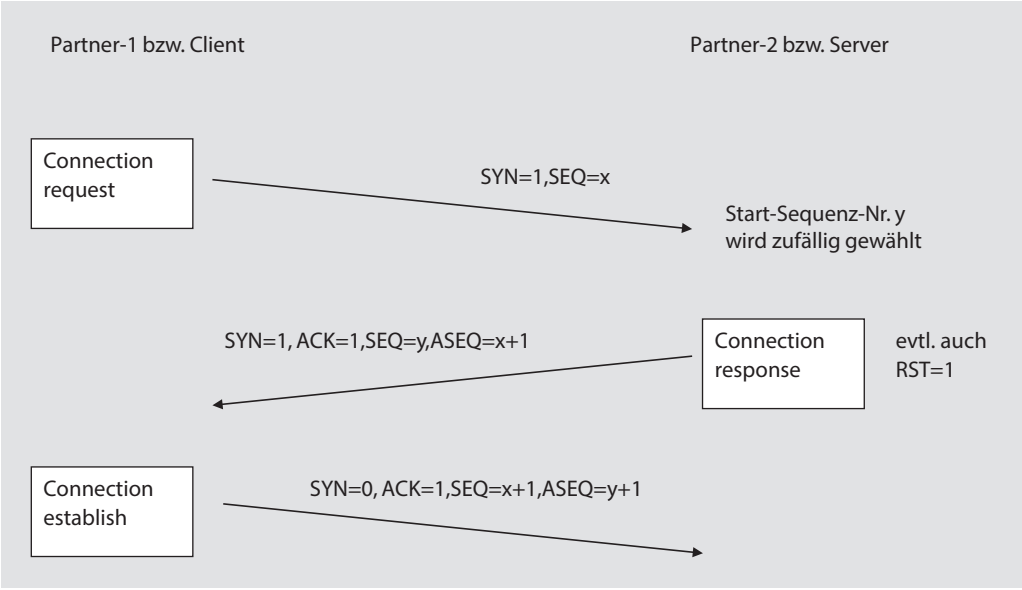


Abb. 6.17 TCP Verbindungsaufbau

3. Der Initiator erhält die Antwort und quittiert diese (Segmentnummern x + 1 bzw y + 1) mit gesetztem ACK-Flag und nichtgesetztem SYN-Flag.
4. Nach dem Empfang des Quittungssegmentes beim Responder ist die Verbindung aufgebaut.

Entsprechend erfolgt der quittierte Verbindungsabbau durch Austausch von Segmenten mit gesetztem FIN-Flag (s. Abb. 6.18).

Weiterhin löst das TCP-Protokoll auch Aufgaben der Fluss- und Staukontrolle, die im nächsten Abschnitt diskutiert werden.

6.3.4 Adaptive Flusskontrolle

TCP ermöglicht eine adaptive Flusskontrolle. Diese hat zwei verschiedene Aufgaben:

- Verhinderung der Überlastung des Empfängers
  z. B. kann ein Netzwerkdrucker dauerhaft nicht mehr Daten empfangen als er drucken kann, weil ansonsten der Puffer im Speicher überläuft. Deshalb sollte der Sender seine Sendedatenrate reduzieren.
- Verhinderung der Überlastung des Übertragungsnetzwerkes
  z. B. kann ein DSL-Router in der Regel nur bis 100 MBit/s übertragen. Wenn Sender und Empfänger aber in LAN mit mehreren hundert MBit/s senden, stauen sich Daten im Router und es kommt zum Speicherüberlauf mit Datenverlusten.

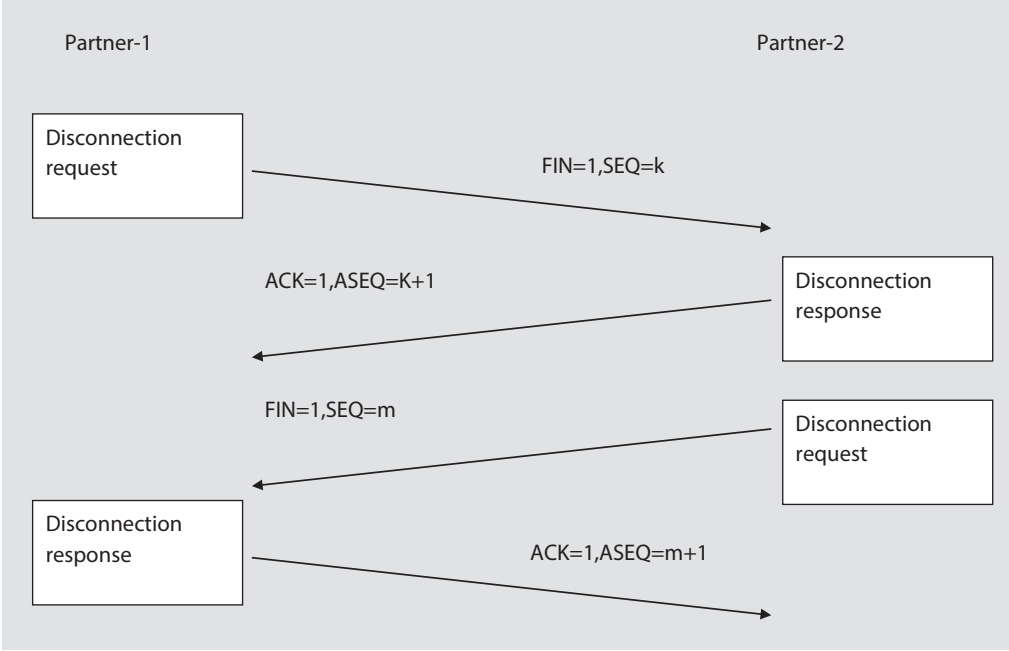


Abb. 6.18 TCP Verbindungsabbau

TCP realisiert beide Aufgaben durch den Einsatz von sogenannten Schiebefensterprotokollen [17].

Die Überlastung des Empfängers verhindert TCP dadurch, dass in jeder Nachricht (auch in Quittungen) ein sogenanntes Empfangsfenster mitgeteilt wird. Dieses beinhaltet die maximale Größe des Empfangspuffers. Der Sender muss gegebenenfalls eine Sendepause einlegen, wenn das Sendefenster „zu klein" ist.

Schwieriger ist die Verhinderung der Überlastung des Netzwerkes. TCP kommuniziert nicht mit den hierarchisch untergeordneten Routern der IP-Schicht, sondern kann nur aus dem Beobachten des Netzverhaltens Schlussfolgerungen ziehen.

So wird beim „Slow Start" -Algorithmus zunächst mit einem geringen Durchsatz die Verbindung getestet. Im positiven Fall wird der Durchsatz so lange gesteigert, bis Fehler auftreten, dann wird der Durchsatz wieder reduziert. Man unterscheidet schwere Fehler (Segmentverluste, Timeouts), bei deren Auftreten der Durchsatz stark reduziert wird und Fehlerhinweise (duplizierte Quittungen), bei deren Auftreten der Durchsatz weniger reduziert wird.

Einen bespielhaften Ablauf (TCP Reno) können Sie Abb. 6.19 entnehmen. Die Fenstergröße steigt zuerst exponentiell, danach bis zum nächsten Fehler linear und steigt schrittweise weiter.

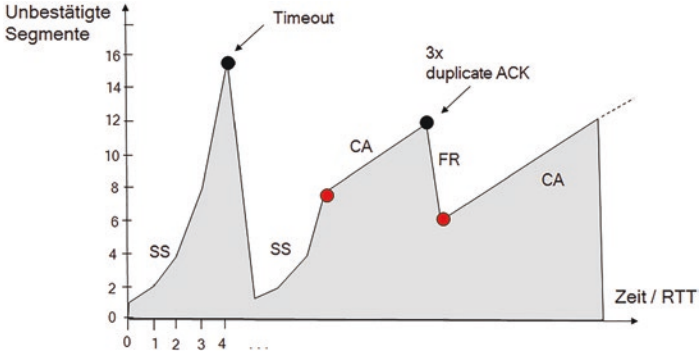


Abb. 6.19 TCP Reno: Zeitdiagramm mit „Slow Start", „Congestion Avoidance" und Fehlerreaktionen [3, 4]

1. *Festlegung einer maximalen Sendefenstergröße sowie eines Schwellwerts unterhalb dieses Maximums*
2. *Beginn mit Fenstergröße 1 („Slow Start"), exponentielle Erhöhung bis zum Schwellwert bei erfolgreich bestätigten Nachrichten, lineare Erhöhung (CA, Congestion Avoidance) nach Überschreiten des Schwellwerts bis zum Maximum*
3. *Zurücksetzen der Fenstergröße auf 1 bei Ablauf eines Timeout, (z. B. bei Paketverlust)*
   Halbieren des Schwellwertes, weiter mit „Slow Start"
4. *Zurücksetzen der Fenstergröße auf halben aktuellen Wert beim Auftreten von drei duplizierten Quittungen, weiter mit linearer Erhöhung.*

6.4 Protokollanalysatoren und Netzwerksimulatoren

6.4.1 Protokollanalysator Wireshark

Protokollanalysatoren haben die Aufgabe, die zwischen den Protokollinstanzen ausgetauschten Protokolldateneinheiten zu beobachten und zu speichern, sowie eine nutzerfreundliche Ausgabe dieser Daten zu gewährleisten. Ein bekanntes Beispiel stellt das Programm Wireshark [20] dar, welches eine Analysekomponente zwischen Netzwerkkartentreiber und Netzwerkprotokollstack einfügt. Dadurch können alle über die Netzwerkkarte gesendeten und empfangenen physischen Nachrichten registriert werden. Die dadurch entstehenden Datenmengen sind i.a. erheblich. Es gibt aber Filteroptionen, mit deren Hilfe man diese Datenmengen reduzieren kann, indem man sich auf wenige Protokolle konzentriert, z. B. auf UDP und TCP.

Wireshark selbst bietet nur eine einfache Visualisierung in Textform, jedoch gibt es vielfältige Ergänzungssoftwareprodukte zur komfortableren Darstellung und zur intelligenten Auswertung der gewonnenen Daten.

Kompakte Protokoll- und Netzwerksimulatoren mit Visualisierungsfunktionalitäten sind für die Netzwerkentwicklung wichtig. Für Studierende ist von Vorteil, dass es auch Freeware-Lösungen gibt. An der Stelle bietet es sich an, u. a. die folgenden Simulatoren zu diskutieren [2, 12].

6.4.2 NS-3 (Network Simulator)

NS-3 (Network Simulator) ist der Nachfolger der Reihe von Simulatoren NS-1 und NS-2 und stellt in sich eine diskrete ereignisgetriebene Simulationssoftware mit Visualisierungsfunktionalitäten für Netzwerke und Netzwerksprotokolle dar. Die Simulatoren NS-2 und NS-3 (meist in C++ und Python implementiert) fanden bereits seit Jahrzehnten ihre breite Anerkennung in Forschung und Lehre [2].

Der typische Ablauf für NS-2/NS-3 kann in die folgenden Schritte aufgeteilt werden:

1. Topology Definition (Topologieeingabe): der Graph des Netzwerkes mit Knoten und Kanten wird definiert, der NS-3 bietet entsprechende Container und Hilfen zur Unterstützung der Topologiebeschreibung.
2. Model Development (ggf. Modellentwicklung): Modelle der Knoten und Protokolle werden zur Simulation hinzugefügt, bspw. für UDP, IPv4, Point-to-Point-Geräte und Links sowie Applikationen. Meistens sind diese in den Bibliotheken bereits vorhanden, ansonsten gibt es gute Systemunterstützungen. Diese ergänzen den Funktionsumfang um weitere Simulationsmodelle und Protokolle.
3. Node and Link Configuration (Konfigurierung): Für die Modelle kann man ihre Standardwerte einstellen wie bspw. MTU (Maximum Transfer Unit).
4. Execution (Ausführung): Simulationssoftware erzeugt Ereignisse (Events), die Daten werden über das Netzwerk (über die Knoten und Kanten) unter Nutzung definierter Protokolle transferiert, die Ankunftszeiten der Ereignisse werden geloggt (die Zeitstempel werden fixiert).
5. Performance Analysis (Performanceanalyse): nachdem die Simulation zu Ende ist, werden die Daten zur Auswertung (Event Tracing) nach ihren Zeitstempeln verfügbar. Diese Daten können visualisiert werden sowie statistisch analysiert werden (R-Tool).

6. Graphical Visualization (Visualisierungsfunktionalität): die Rohdaten oder die statistisch verarbeiteten Daten können mittels der Tools Gnuplot, Matplotlib oder XGRAPH visualisiert werden.

[Vermerk]

Als Nachteile der Programme NS-2 und NS-3 kann man das Folgende bemerken:

- Die Basistools sind ohne GUI relativ komplex handhabbar (nur Analysetools beherrschen GUI), sowie sind die Simulationen oft zeitaufwendig.
- Die User müssen gut über die Skriptsprachen (u. a. Tcl/Tk), Bedienungstheorie (Queuing Theory) und Modelliertechniken informiert sein.

■ Netzwerksimulator OMNeT++

Der Netzwerksimulator OMNeT++ wurde in C++ implementiert [12] und beinhaltet Komponenten-/Protokollbibliotheken und ein Basisframework zur Simulation (u. a. für IP, HTTP). Die Basissoftware ist für den nicht-kommerziellen Einsatz im akademischen Bereich zur Forschung und Lehre freigegeben und gut geeignet. OMNEST ist eine erweiterte Version des Systems für kommerzielle Nutzung [12].

Durch den modularen Aufbau von OMNeT++ lässt es sich durch zahlreiche Frameworks erweitern. Das System nutzt u. a. INET [12] als externes Framework zur Unterstützung von folgenden Modellen zu den Protokollen:

- Internet: Protokolle wie IPv6, TCP, UDP, FTP, DHCP
- Routing und Netzzugang: BGP (Border Gateway Protocol), PPP, Ethernet
- Drahtlose Netze: WLAN und WSN (Wireless Sensor Networks)
- Mobile Netze (z. B. 3G, LTE) sowie die Bewegungsmodelle, die Bewegung der Objekte bei deren Simulation bestimmen
- MANET (Mobile Ad hoc NETworks) [12].

[Vermerk:]

Auch der Netzwerksimulator OMNeT++ ist gut geeignet zum fundierten Erlernen von Netzwerkprotokollen, Kommunikationsverfahren, Netzkopplungselementen und -technologien sowie Modelliertechniken [3, 7, 16].

6.5 Zwischenfragen/Übungsaufgaben

6.5.1 Routing

Gegeben sei ein Netz mit folgender Topologie und Kostenbewertung der Übertragungspfade (◘ Abb. 6.20)

a) Wovon können die Kostenbewertungen im realen Netz abhängen?
b) Bestimmen Sie schrittweise den kürzesten Pfad von A nach D nach dem Verfahren „Shortest Path Routing“ von Djikstra.

6.5.2 IP-Adressierung

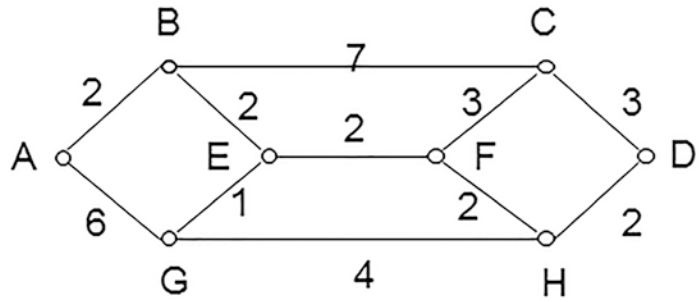
Eine Firma besitzt einen IP-Adressbereich von 128.10.192.0 bis 128.10.199.255

a) Der Bereich soll in mehrere Subnetze mit jeweils 30 Hosts aufgeteilt werden.
b) Geben Sie eine geeignete Maske an!
c) Wie viele Subnetze können adressiert werden?

Teilen Sie die IP-Adresse 128.10.192.70 in Netz- und Host-Anteil auf.

6.5.3 Nutzerschnittstelle TCP/UDP

a) Welche Aufgabe haben Portnummern?
b) Welche Dienstqualität bieten UDP bzw. TCP?
c) Was sind die Ziele der Fluss- und der Staukontrolle?



◘ **Abb. 6.20** Netzwerkgraph

Rechnernetzapplikationen

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_7

7.1 Verteilte Systeme und Anwendungen

Der Begriff „Verteilte Verarbeitung“ charakterisiert die Arbeit von Systemen, bei denen ein Anwendungsdienst durch Zusammenwirken mehrerer Prozesse erbracht wird. Die hierfür erforderliche Prozesskommunikation kann auf einem Rechner mithilfe der lokalen Prozesskommunikation realisiert werden oder in Rechnernetzen mithilfe von Diensten der Transportschicht [7, 14, 15, 17].

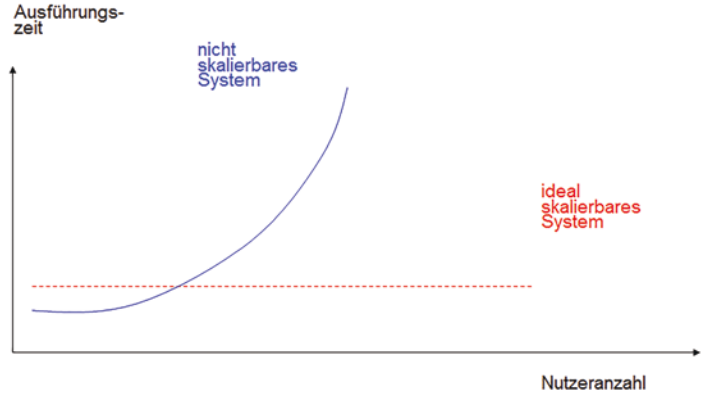
Verteilte Verarbeitung bringt einige Vorteile gegenüber dem Einsatz monolithischer Systeme.

Es besteht die Möglichkeit, dezentrale Dienste zu organisieren, bei denen von Clientrechnern Dienste von Serverrechnern angefordert werden. Die Clients sind anwendernah und ermöglichen dennoch den Zugriff auf die Ressourcen anderer Rechner. Die Anwender haben schnellen, komfortablen Zugriff und die teuren, knappen Ressourcen können besser ausgelastet werden.

Außerdem ist bei verteilten Systemen prinzipiell die Skalierbarkeit gegeben. Dies bedeutet, dass die Ausführungszeit eines Dienstes nicht wesentlich von der Anzahl der Dienstnutzer abhängt (◘ Abb. 7.1).

Als Beispiel möge die Steuerung von Geldautomaten dienen. Ein zentralistisches System kann effizient einige wenige Geldautomaten steuern, aber es würde ab einer gewissen Zahl angeschlossener Automaten überlastet sein. Eine Großbank muss deshalb verteilte Systeme einsetzen.

In verteilten Systemen (VS) laufen komplizierte Vorgänge ab. Die Implementierung ist deshalb schwierig. Dennoch überwiegen die Vorteile. Die klare Trennung der Subsysteme erleichtert die Testung und Wartung, verringert die Störanfälligkeit und gewährleistet höhere Änderungsfreundlichkeit.



◘ **Abb. 7.1** Skalierbarkeit in verteilten Systemen

Die verteilte Verarbeitung ist in weiten Bereichen noch Gegenstand wissenschaftlicher Forschung. Komplexe Probleme sind u. a. Zuverlässigkeit, Robustheit, Datensicherheit, Datenkonsistenz.

Abschnitt zur vertieften Studie

Das *ODP-Referenzmodell* (Open Distributed Processing Reference Model) der ISO führt fünf Betrachtungspunkte (Viewpoints) zu Beurteilung verteilter Systeme ein,

- den *Enterprise viewpoint* für die Anwendungsanforderungen,
- den *Information viewpoint* für die Definition von Datenobjekten,
- den *Computation viewpoint* für die Grobstruktur der Anwendung,
- den *Engineering viewpoint* für die Abbildung von Softwaremoduln auf einzelne Rechner und den Technology viewpoint für die Beschreibung von Hardware und Betriebssystemen.

Ein verteiltes System (VS) besteht aus unabhängigen, über ein Rechnernetz kommunizierenden Rechnern, wobei keine zentrale Systemsteuerung existiert und der Verteilungsaspekt für die Benutzer des Systems möglichst transparent ist.

Die Rechner verrichten eine Kooperationsaufgabe gemeinsam: also eine Rechnernetzapplikation wird ausgeführt, wobei ihre einzelnen Teile zu unterschiedlichen Netzwerkknoten gehören.

Die wichtigen Merkmale der verteilten Systeme sind wie folgt:

- Kopplung räumlich verteilter Rechner mittels Rechnernetz
- Kooperation mit dem Ziel, eine bestimmte Anwendungsfunktionalität zu erbringen
- Kein gemeinsamer physikalischer Speicher, keine strikt synchronisierten Uhren
- Dezentrale Organisation und Verwaltung
- Häufig auch Fehlertoleranz und Lastausgleich durch Replikation.

Die software-technische Realisierung von verteilten Systemen erfolgt oft auf der Basis

- des Client/Server-Modells bzw. durch verteilte Objekte und Software-Komponenten
- die P2P-Systeme, wobei die zu kommunizierenden Partner gleichberechtigt sind.

7.1.1 Verteilte Anwendungen

Verteilte Anwendungen streben einen Nutzen durch Verbundfunktionen an.

Durch den *Havarieverbund* bleiben bei Computerausfällen keine Nutzeraufträge liegen, durch den *Lastverbund* wird ein

höherer Auftragsdurchsatz erzielt, durch den *Funktionsverbund* können Rechner Dienstleistungen anderer Computer nutzen und deshalb Aufträge beliebiger Art entgegennehmen, durch den *Datenverbund* entfallen kosten- und zeitaufwendige Datentransporte, durch einen *Ressourcenverbund* können Investitionen gespart werden.

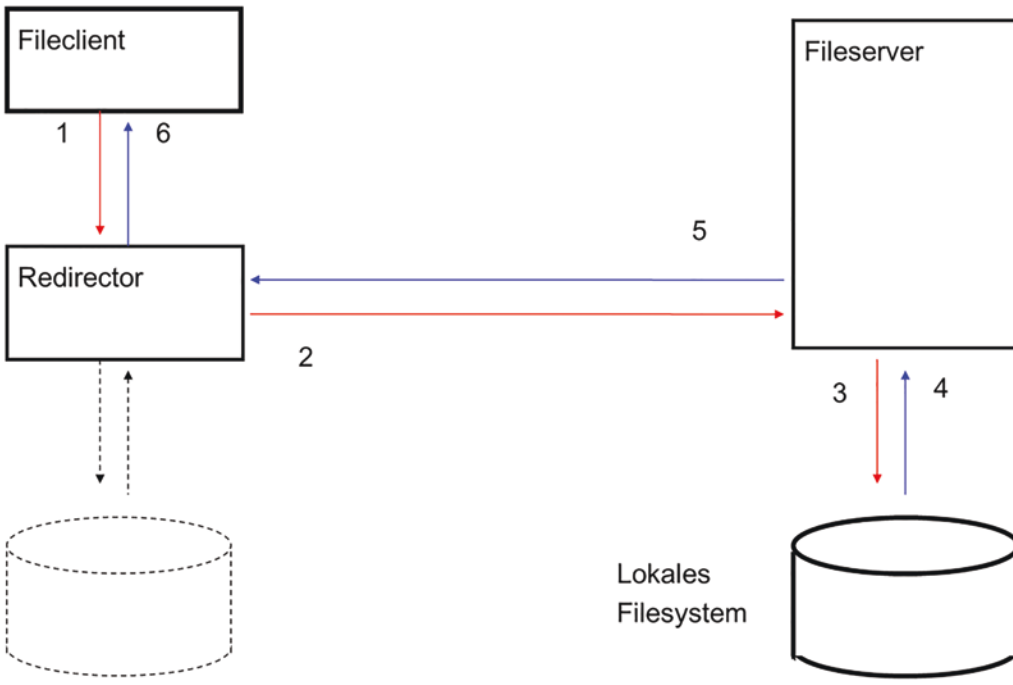
Bei der verteilten Verarbeitung erteilen Clientprozesse Aufträge. Ein Serverprozess führt sie aus und informiert den Client über das Ergebnis.

7.1.2 Verteiltes Filesystem

Eine verbreitete Verbundlösung ist die Realisierung eines verteilten Filesystems in Netzwerkbetriebssystemen. Dabei können die Anwendungsprozesse als Fileclienten auf das Dateisystem anderer Computer in gleicher Weise zugreifen wie auf ihr eigenes Filesystem.

Nachfolgende ◘ Abb. 7.2 zeigt das Funktionsprinzip.

Ein Anwendungsprogramm setzt einen Betriebssystemruf für das Dateisystem ab (1). Das Dateisystem ist in Netzwerkbetriebssystemen um einen Redirector erweitert, der entscheiden muss, ob es sich um einen lokalen Aufruf handelt oder nicht. Im



◘ **Abb. 7.2** Ablauf im Verteilten Filesystem

ersteren Fall reicht der Redirector den Ruf an das lokale Dateisystem weiter, im zweiteren Fall bildet er eine Nachricht, die alle Aufrufparameter enthält und schickt diese mithilfe von Rechnernetzkommunikationsdiensten an einen Fileserverprozess (2). Dieser wertet die Nachricht aus, passt die Parameter an sein lokales Betriebssystem an und realisiert einen Aufruf seines Dateisystems (3). Die Ergebnisparameter (4) des Rufes schickt der Server in einer Nachricht (5) an den Auftraggeber. Dieser analysiert die Nachricht, wandelt die Ergebnisparameter in seine Betriebssystemform um und übergibt sie dem Clientprozess (6).

Der gesamte Vorgang läuft für den Fileclient transparent ab. Dies bedeutet, dass die gesamte lokal verfügbare Software auch rechnernetztauglich ist. Es ist nicht erforderlich, dass beide Filesysteme identisch sind. So kann z. B. der SAMBA-Prozess auf LINUX-Servern als Fileserver für Windows-PC arbeiten.

7.1.3 Datenkonsistenz

Greifen mehrere Clienten auf die gleichen Daten zu, ergibt sich das Problem der Datenkonsistenz. Datenkonsistenz bedeutet, dass die Werte von Variablen auf allen Rechnern korrekt sind.

Im folgenden Beispiel arbeiten zwei Prozesse mit derselben Variablen, die initial den Wert „5“ besitzt. Client 1 erhöht die Variable um 1, Client 2 erniedrigt sie um 1. Im Ergebnis müsste die Variable wieder den Wert „5“ haben. Durch Ineinanderschachtelung der Schreibzugriffe wird aber die Datenkonsistenz verletzt. Im speziellen Fall ergeben sich auf allen beteiligten Rechnern falsche Variablenwerte (◘ Abb. 7.3).

Die Sicherung der Datenkonsistenz kann durch eine Datenzugriffssteuerung erreicht werden. Die einfachste Möglichkeit ist, einen Sperrmechanismus für den Datenzugriff zu realisieren. Ein interessierter Prozess beantragt einen Zugriff und erhält das Zugriffsrecht nur, wenn die Daten „frei“ sind. Im positiven Fall kann der Prozess die Daten bearbeiten und gibt diese danach wieder frei.

Abgewiesene Prozesse können eine Information über die Sperrung erhalten und selbst über Nachfolgeaktionen entscheiden oder sie werden automatisch in einen Wartezustand versetzt.

Sperrmechanismen sichern zwar die Datenkonsistenz, führen jedoch zur Verlangsamung der Verarbeitung im Netz durch Warteschlangenbildung. Deshalb strebt man eine Minimierung der Sperrungen an. Eine generelle Sperrung ganzer Dateien ist am einfachsten zu lösen, jedoch ineffizient. Deshalb wird die Sperrung auf bestimmte Bereiche einer Datei beschränkt.

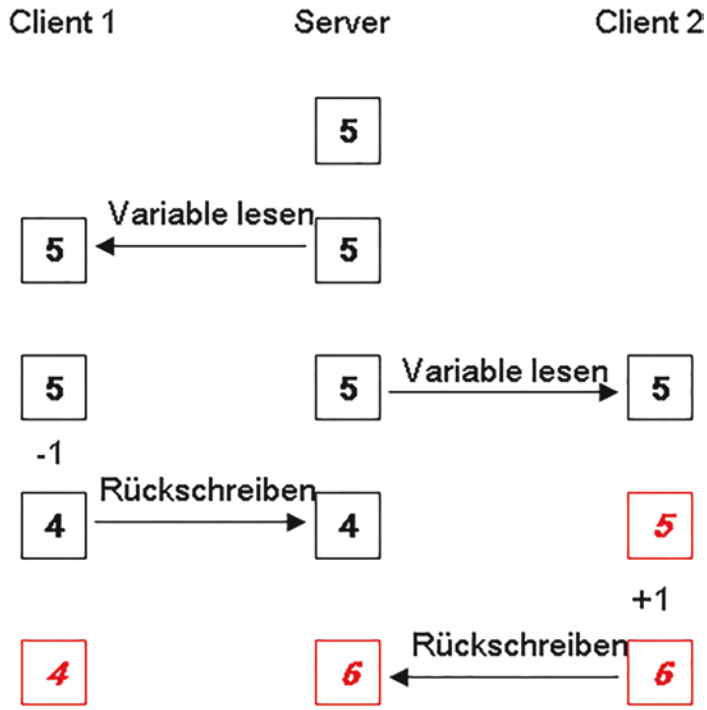


Abb. 7.3 Datenkonsistenz im Verteilten System

Außerdem ist zu berücksichtigen, dass nicht bei jedem Mehrfachzugriff Probleme entstehen. Beispielsweise gibt es keine Datenkonsistenzverletzung, wenn alle Nutzer nur lesend zugreifen. Bei Schreibzugriffen müssen alle weiteren Interessenten abgewiesen werden, jedoch kann der „dirty read"-Zugriff gestattet werden. Dieser garantiert bewusst nicht die Korrektheit übergebener Daten. Eine sinnvolle Anwendung des „dirty read"-Zugriffs liegt z. B. vor, wenn ein Manager sich für den Umsatz seines Unternehmens interessiert. Er nimmt zugunsten des schnelleren Zugriffes eine evtl. Ungenauigkeit in Kauf, da er nur die Größenordnung des Umsatzes wissen will.

Besonders unangenehm ist es, wenn eine Sperrung sehr lange Zeit andauert, ohne dass eine intensive Nutzung stattfindet. Dies ist zum Beispiel der Fall, wenn ein Mitarbeiter einen Datenbankbereich sperrt um Veränderungen vorzunehmen, aber durch eine andere Arbeit an der zügigen Erledigung gehindert wird. In derartigen Fällen kann durch die Datenzugriffsteuerung ein Entzug des Zugriffsrechtes veranlasst werden.

7.1.4 Ressourcenverbund und Funktionsverbund

Auf ähnliche Weise wie der Zugriff auf entfernte Datenträger kann auch die Nutzung anderer Geräte realisiert werden.

Spezialisierte Serverprozesse nutzen die Geräte auf Antrag von Clientprozessen.

Bei einigen Geräten, die nur exklusive Nutzung erlauben, z. B. Netzwerkdrucker müssen Warteschlangenverwaltungen implementiert werden, die clientseitig oder serverseitig arbeiten.

Der Funktionsverbund bietet noch allgemeinere Dienstleistungen als der Ressourcenverbund. Zielstellung ist die Abarbeitung beliebiger Prozeduren auf anderen Rechnern. Diese Methode wird auch als RPC bzw. Remote Procedure Call bezeichnet (s. Details im Teil III).

7.2 Klassische Client/Server-Architekturen und Peer-to-Peer

Verteilte Systeme unterteilen sich nach der Art der Kommunikation [7, 14, 15]:

1. Client-Server-Kommunikation (C-S)
   - Kommunikation über Sockets (Transport: TCP/UDP)
   - Prozedurenfernaufruf (RPC, Remote Procedure Call)
   - Methodenfernaufruf (RMI, Remote Method Invocation, und CORBA, Common Object Request Broker Architecture)
   - Asynchrone Kommunikation (MQ, Message Queuing).
2. Peer-to-Peer-Kommunikation (gleichberechtigte Partner, P2P) ist von der C-S zu unterscheiden, weil Peer – „Partner, kein Diener ist."
   - P2P Services dienen hauptsächlich der Realisierung von Tauschbörsen für Dateien (File-Sharing wie z. B. BitTorrent, Napster etc.), mit denen vorwiegend Musik- und Videodateien (MP3, AVI, MPEG usw.) (nicht selten illegal) getauscht werden.

Die ◘ Abb. 7.4 zeigt eine Gegenüberstellung eines reinen C-S-Modelles mit einem unterbeauftragten Server und einem angeschlossenen Datenbanksystem und einem P2P-Modell, bei dem alle Peers gleichberechtigt sind, aber auch evtl. eine Serverlösung nutzen können (hybride Lösung) [10, 14].

Beispiele für eine C-S-Lösung sind die Dienste WWW, Wikipedia, Youtube und die Cloud-Dienste von Amazon [1, 10]. Beispiele für eine P2P-Lösung sind die Dienste Skype, Viber, BitTorrent und spezielle Grids (BOINC).

Weitere Details zur Client/Server-Architektur sowie deren Alternative P2P können Sie Teil III entnehmen.

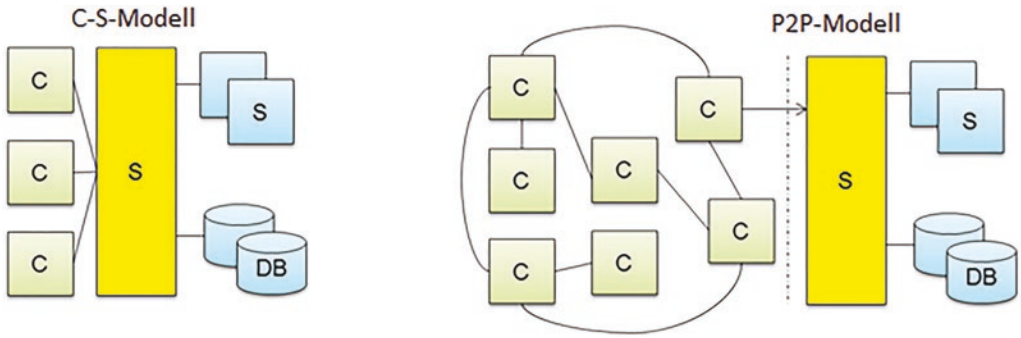


Abb. 7.4 Gegenüberstellung von C-S und P2P-Modellen

7.3 Multimediakommunikation und Mobile Computing

Die Multimediakommunikation erfolgt heutzutage durch eine Vielzahl unterschiedlicher Medien und Endgeräte und kann dabei verschiedene Sinnesorgane des Zuhörers ansprechen wie Text, Audio, Bilder, Animationen und Videos (Medien) und erlaubt einem User, die gewünschten Daten interaktiv zu verteilen [17]. Dazu dienen je nach Zielsystem verschiedenen sogenannte Codecs (Codierungs-/Dekodierungsverfahren).

Weitere Details zur Multimediakommunikation finden Sie im Teil III.

Für viele Aufgaben ist es heutzutage einfacher und schneller, ein Smartphone oder Tablet anstelle eines Computers oder Laptops zu verwenden.

Mobile Computing, auch Ubiquitäres Computing, setzt die Verfügbarkeit mehrerer Mobilfunk-, Satellitenfunk- und Drahtlosnetze voraus, u. a. GPRS, UMTS, HSDPA, LTE und auch 5G/IMT2020 sowie GPS/Galileo, auch WLAN IEEE 802.11, WSN und BT IEEE 802.15.1/4. Diese werden in Teil II detailliert vorgestellt [8, 11].

Mobile Applikationen (Apps) sind ein wichtiger Begleiter im Smartphone-Zeitalter. Nahezu für jede Lebenslage und jeden Sachverhalt gibt es heutzutage eine App.

Mobile Betriebssysteme und Apps kombinieren die typischen Features für den PC mit den neuen Feature für mobile Nutzung von diversen Netzwerken/Sensoren (im Sinne von Netzwerkadaptern): Zellularnetze 3G-4G, Bluetooth, WLAN, GPS -Mobilenavigation, Touchscreen, Fotokamera, Videokamera, Spracherkennung und -Aufzeichnung (Speech Recognition, Voice Recorder), Musikplayer, Near Field Communication, Infrarotblaster.

Durch den eingeschränkten Platz (in der Regel bietet ein Smartphone nur etwa 20 % der verfügbaren Fläche eines Desktops), sind die Designer gezwungen, sich auf das Wichtigste zu konzentrieren (RWD für den Clientteil, Responsive Webdesign).

Auch auf den kleinsten Geräten sollen die Kerninformationen der Webseiten zur Verfügung stehen und vor allem einfach zu finden sein.

Die Verteilung von mobilen Apps wird durch die sog. App Stores in den gängigen Betriebssystemen realisiert. Es wird zwischen drei Typen mobiler Apps unterschieden: Webapps, native Apps und hybride Apps (s. Teil III). Durch den Einsatz moderner Frameworks (Virtualisierungstools) ist der Übergang zwischen diesen drei Typen immer möglich!

Weitere Details zum Mobilen und Ubiquitären Computing entnehmen Sie in Teil III.

7.4 Basisdienste im Internet

7.4.1 DNS (Domain Name Service)

Die Internet-Anwendungen nutzen die Übertragungsdienste des TCP/IP-Protokolls. Die dabei verwendeten IP-Adressen für die beteiligten Rechner sind wenig komfortabel. Deshalb wurden sog. Internetrechnernamen eingeführt. Jeder Internetrechnername kann eindeutig auf eine IP-Adresse abgebildet werden [17].

Der Aufbau eines solchen Namens soll an einem Beispiel diskutiert werden. Die einzelnen Bestandteile sind durch Punkte getrennt. Die Interpretation erfolgt von rechts nach links.

artist.inf.tu-dresden.de

Der letzte Parameter, (im Beispiel *artist*), charakterisiert eindeutig einen Rechner in einer weltweit eindeutigen Domäne (z. B. *inf.tu-dresden.de*). Die Domänenbezeichnung beginnt mit der Angabe einer Top-Level-Domäne, im obigen Fall *de* als Bezeichnung für den deutschen Teil des Internet. Bis auf die USA bilden alle Staaten jeweils eine Top-Level-Domäne. Weiterhin gibt es inhaltlich bezogene Einteilungen, z. B. *com* für die Wirtschaft und *gov* für die Regierung. Die Top-Level-Domänen werden in Domänen (i.o. Fall *tu-dresden*) unterteilt, evtl. auch noch in Subdomänen (z. B. *inf*). Die Domänennamen werden auf Antrag durch ein NIC (Network Information Center) zugeteilt.

Neben der komfortableren Adressierung hat die Verwendung von Internetrechnernamen noch den Vorteil, dass Anwendungen ohne Probleme die Netze wechseln können, d. h. andere IP-Adressen erhalten. Die Erreichbarkeit ist trotzdem gegeben, wenn der Rechner- und der Domänenname beibehalten wird.

In der Anfangsphase des Internet erfolgte die Verwaltung von symbolischen Namen zentral in einer einzigen Datei HOSTS.TXT, die von allen Internetrechnern regelmäßig kopiert wurde. Mit wachsender Größe des Internet wurde diese Arbeitsweise zu

aufwendig und es wurde ein dezentral organisierter Anwendungsdienst *DNS* (Domain Name Service) für die Zuordnung von IP-Adressen zu den Internetrechnernamen eingeführt.

Jeder Internetrechner muss mindestens einen DNS-Server kennen. Bei unbekannter IP-Adresse eines Partnerrechners wird der Name-Server befragt. Dieser kommuniziert ggf. mit weiteren DNS-Servern.

7.4.2 Remote Login (per Telnet)

Der älteste Internet-Anwendungsdienst ist *TELNET,* mit dessen Hilfe andere Rechner im Internet fernbedient werden können. TELNET ist nicht grafikfähig, es bietet die Kommandoschnittstelle des Betriebssystems des Zielrechners. Dies funktioniert natürlich nur, wenn dieser es zulässt, d. h. auf dem Partnerrechner muss ein unsichtbarer Dämon-Prozess existieren, der mit TELNET zusammenarbeitet. Selbstverständlich muss auch der entfernte Nutzer eine Nutzungsberechtigung (Login) besitzen.

Vorwiegend für UNIX-Rechner existiert im Internet mit dem X-WINDOW-System auch eine grafische Oberfläche für die Fernbedienung anderer Rechner.

TELNET ist inzwischen veraltet und wird heutzutage durch die leistungsfähigere und sicherere Applikation SSH ersetzt.

7.4.3 File Transfer (per FTP, File Transfer Protocol)

Der Anwendungsdienst *FTP* ist ebenfalls einer der ältesten Internetanwendungen und ermöglicht den Dateitransfer im Internet. Es können Dateien zu einem anderen Rechner gesendet bzw. von diesem angefordert werden. Auf einem Rechner startet der Nutzer ein FTP-Clientprogramm, auf dem anderen Rechner muss ein Dämonprozess die FTP-Serverrolle übernehmen.

FTP ist inzwischen ebenfalls veraltet und wird heutzutage durch die leistungsfähigere und sicherere Applikation SFTP ersetzt.

7.4.4 Email (per SMTP, Simple Mail Transfer Protocol)

Der Dienst *SMTP* realisiert die Übermittlung von elektronischer Post (E-Mail). Er gehört zu den ältesten Diensten, ist jedoch immer noch aktuell, da leistungsfähige Zusätze zur Datendarstellung und Datenverschlüsselung existieren.

Die E-Mailadressen bestehen aus zwei Angaben. Nach einem Trennzeichen @ steht der Name des Internetrechners. Vor dem

Trennzeichen steht der Nutzername für diesen Rechner. Als Beispiele werden die E-Mail-Adressen der Autoren angegeben.
Andriy.Luntovskyy@ba-dresden.de
Dietbert.Guetter@tu-dresden.de

Auch bei SMTP muss ein E-Mail-Programm des Nutzers (Client) mit einem E-Mail-Server zusammenarbeiten, der i.a. als ständig empfangsbereiter Dämonprozess auf dem Zielsystem realisiert ist.

Die empfangenen Nachrichten werden ohne Zutun des Nutzers in einer nutzereigenen Mailbox abgelegt. Mithilfe eines E-Mail-Programmes kann jeder Nutzer auf seine Mailbox zugreifen. Wann er das tut, liegt in seinem Ermessen.

Der E-Mail-Transfer erfordert im Gegensatz zum FTP-Dateitransfer keine Zugriffsberechtigung für den Zielrechner.

Ursprünglich wurde nur das Senden von ASCII-Texten unterstützt. Für einfache Mitteilungen reicht dies, der Dateitransfer per E-Mail wird jedoch eingeschränkt. Deshalb wurde der Standard MIME (Multipurpose Internet Mail Extensions) verabschiedet, in dem Vorschriften zur Codierung verschiedenster Dateitypen als ASCII-Text festgelegt sind. Fortgeschrittene E-Mail-Programme erledigen die Codierung und Decodierung ohne Mitwirkung des Nutzers.

Sensible Daten sollten verschlüsselt werden, da das Internet gegenüber Lauschangriffen nicht sicher ist. Dazu stehen sichere Verfahren, wie z. B. PGP (Pretty Good Privacy) zur Verfügung.

Bei SMTP wird vorausgesetzt, dass der Zielrechner immer betriebsbereit ist und stets über das Internet erreichbar ist. Diese Voraussetzungen gelten i. a. für Rechner an Universitäten, jedoch nicht für private Personalcomputer oder für die LAN kleiner Betriebe. Häufig ist nur ein zeitweiliger Internetanschluss realisiert, um Leitungskosten zu sparen. Ebenfalls werden die Computer meist nachts abgeschaltet. Die Nutzer können sich beim Senden an die Betriebszeiten halten, für den Empfang gibt es jedoch Probleme, da nicht vorhersehbar ist, wann E-Mails eintreffen. Die Lösung des Problems besteht darin, dass man sich die Nachrichten an einen permanent empfangsbereiten E-Mail-Server schicken lässt, der die Funktion eines Nachrichtenspeichers übernimmt. Die Nachrichten können zu beliebigen Zeitpunkten abgeholt werden, dafür gibt es spezielle Protokolle, z. B. POP3 und IMAP.

7.4.5 WWW (World Wide Web)

WWW realisiert einen Informationsdienst auf Basis eines dezentralen Hypertextsystems. Es wurde 1989 am europäischen Kernforschungszentrum CERN entwickelt, die breite Einsatzreife

wurde 1994 erreicht. Heutzutage kann man von einer universellen Verfügbarkeit ausgehen.

Die Grundidee des WWW-Dienstes besteht darin, dass die Nutzer an den Arbeitsstationen über ein komfortables, einfach zu bedienendes Browserprogramm (Client) verfügen, mit dessen Hilfe sie Informationen, sog. WWW-Seiten, von WWW-Servern holen können. Nebenbei soll auch die Nutzung von FTP und TELNET mithilfe des Browsers möglich sein (◘ Abb. 7.5).

Das Protokoll HTTP (Hyper Text Transfer Protocol) wird für den Informationsaustausch zwischen WWW-Client und WWW-Server verwendet. Jede WWW-Seite auf jedem WWW-Server im Internet kann über die zugehörige Adresse URL (Uniform Resource Locator) angefordert werden. Am nachfolgenden Beispiel wird der URL-Aufbau diskutiert.

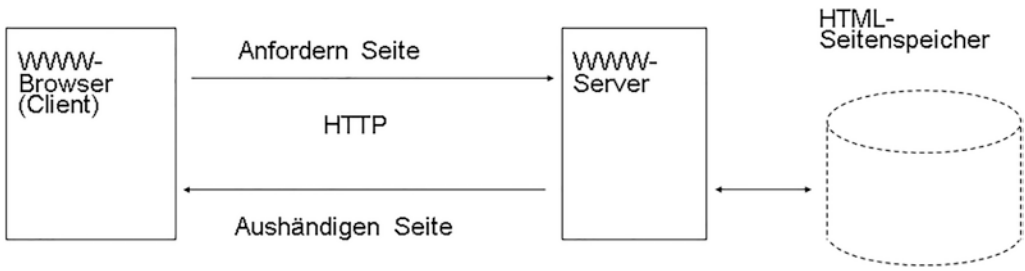
http://www.tu-dresden.de/index.html

7

Ein vollständiger URL beginnt (von links nach rechts) mit der Angabe des Zugriffsprotokolls, abgeschlossen durch einen Doppelpunkt. HTTP ist Standard, aber auch andere Protokolle sind möglich. Danach folgt der mit den Zeichen//und/begrenzte Internetname des WWW-Servers (z. B. ► www.tu-dresden.de), anschließend Angaben zur Lokation auf dem Server. Diese Informationen beinhalten immer einen Dateinamen (bspw. index.html), meist sind zusätzlich Verzeichnisinformationen vorgestellt. Standardwerte zur Eingabeerleichterung sind möglich.

Die WWW-Seiten werden in der Dokumentenbeschreibungssprache *HTML* (Hypertext Markup Language) dargestellt. HTML beschreibt ein Dokument oft nicht in allen Layout-Details, die konkrete Darstellung obliegt dem Browser. So kann z. B. in HTML für einen Absatz eine Einrückung gefordert werden, die Weite des Einrückens ist dann Sache des Browsers.

HTML gestattet Verweise auf andere Dateien, die in das Dokument eingebettet werden sollen. Dies betrifft vor allem Bilder (meist Dateien im PING- oder JPEG-Format). Das Anfordern einer WWW-Seite bewirkt also in der Regel einen Transport mehrerer Dateien.



◘ **Abb. 7.5** Kommunikation per HTTP

Der Hauptvorteil von HTML besteht darin, dass ein Dokument Verweise auf beliebige andere Dokumente im WWW besitzen kann. Dazu werden markierten Dokumentteilen Referenzverweise in Form eines URL auf das andere Dokument zugeordnet. Es besteht die Möglichkeit, Präsentationen zu erarbeiten, deren Teile weltweit vernetzt sind.

Verweise können auch auf Nicht-HTML-Dokumente erfolgen. Die Darstellung erfordert dann oft neben dem Browser noch weitere Hilfsprogramme, beispielsweise den Acrobat Reader für PDF-Dateien oder sogenannte Player zum Abspielen von Audio- und Videodaten.

Ursprünglich war das WWW nur ein Informationsbereitstellungssystem. Moderne WWW-Server erlauben auch das Ausführen von Programmen. Dazu können WWW-Seiten sogenannte Formulare beinhalten, in denen das Bearbeitungsprogramm und die zugehörigen Eingabeparameter festgelegt werden. Beim Aktivieren schickt der Browser die Formularinformationen zum Server, dieser startet das Bearbeitungsprogramm. Die Übermittlung der Ergebnisparameter erfolgt in HTML-Seiten.

Die Anwendungen sind sehr vielfältig. So können Datenbankinformationen weltweit angeboten werden. Der Zugriff ist dabei völlig unabhängig von Rechner- und Betriebssystemtyp des Browserrechners. Bekannte Beispiele für derartige Datenbanken sind die WWW-Suchmaschinen.

In vielen Fällen ist das Abarbeiten von Programmen auf dem Serverrechner nicht sinnvoll, da diese sehr schnell überlastet werden können. Deshalb besteht auch die Möglichkeit, Programme in HTML-Seiten einzubinden, die auf dem Browserrechner abgearbeitet werden.

Dafür sind als aktuelle Ansätze AJAX und HTML5, sowie ActiveX (Microsoft-spezifisch) und Java-Applets denkbar (s. Teil III).

Vermerk

Bei Verwendung von Maschinencode wäre die Nutzung auf spezielle Rechner und Betriebssysteme eingeschränkt. Aus diesem Grund wird oft alternativ Java-Bytecode verwendet, der interpretativ abgearbeitet wird. Die entsprechenden Programme werden als Java-Applets bezeichnet. Ein Konkurrenzkonzept für die Java-Applets wurde von der Fa. Microsoft mit den ActiveX-Controls entwickelt.
Der WWW-Dienst ist durch diese Erweiterungen sehr leistungsfähig geworden. Jedoch gibt es Sicherheitsbedenken bei der Nutzung von Active-X und Java-Applets. Diese können verschiedene Arten von Schadsoftware mit sich bringen und eventuell auf dem Clientrechner installieren.
Daher favorisiert man häufig den Einsatz von AJAX für die Realisierung interaktiver Webseiten auf Client-Seite.

Die Realisierung Verteilter Systeme auf Basis von Java-Anwendungen ist auch möglich. Die objektorientierte Sprache Java erlaubt eine effektive und systemunabhängige Programmierung und unterstützt u. a. einen entfernten Methodenaufruf für Objekte RMI (Remote Method Invocation, s. Teil III).

Durch die Plattformunabhängigkeit der übersetzten Programme können viele Probleme der verteilten Verarbeitung einfacher gelöst werden. So wird die Menge geeigneter Serverrechner nicht durch heterogene Hardware oder Betriebssysteme eingeschränkt. Dem steht zwar eine etwas höhere Abarbeitungszeit von Java-Programmen entgegen, insgesamt ist das Konzept jedoch sehr aussichtsreich für die Zukunft.

7.5 Zwischenfragen/Übungsaufgaben

7.5.1 Allgemeine Problem von Netzapplikationen

a) Warum ist die Skalierbarkeit in verteilten Systemen so wichtig?
b) Benennen Sie zwei Dienste, bei denen die Sicherung der Datenkonsistenz gewährleistet sein muss.

7.5.2 Applikationen

a) Beschreiben Sie das Zusammenwirken von Client und Server anhand des WWW.
b) Diskutieren Sie die einzelnen Bestandteile des DNS-Namens ► www.inf.tu-dresden.de.

Planung, Optimierung und Betriebssicherung von Rechnernetzen

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_8

8.1 Lebenszyklus von Rechnernetzwerken

Rechnernetzwerke sind in allen Bereichen der Wirtschaft und des privaten Lebens von hoher Bedeutung. Engpässe oder gar Ausfälle können großen Schaden verursachen.

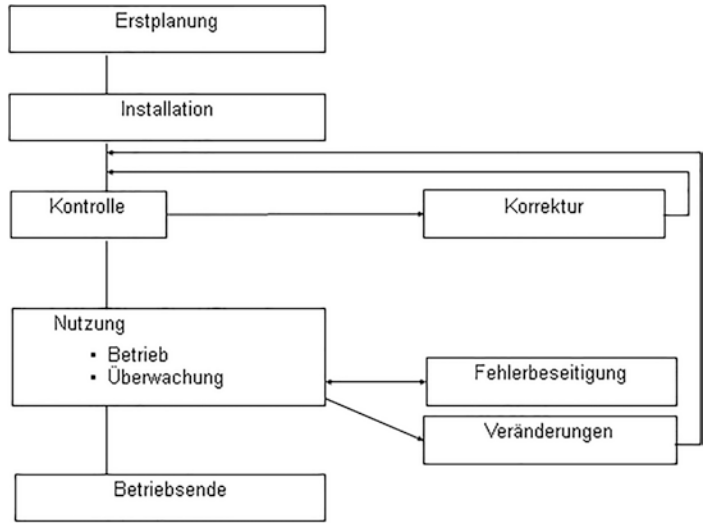
Es ist deshalb die Aufgabe der Netzwerkspezialisten, den Nutzern eine zuverlässige, leistungsfähige, preiswerte und komfortable Infrastruktur zur Verfügung zu stellen. Aufgrund der Komplexität heutiger Netzwerke ist ein professioneller Netzwerkentwurf erforderlich. Durchdachte Planungen verringern die Kosten der Netzwerke und sorgen für einen reibungslosen Betrieb ohne Engpässe. Veränderte Nutzungsanforderungen führen i. a. zu regelmäßigen Netzwerkoptimierungen, bei denen ebenfalls ein planvolles Vorgehen sinnvoll ist.

Der Aufbau und der Betrieb kleiner Rechnernetze ist heutzutage eine simple Aufgabe. Einfache Bausätze sind im Handel erhältlich, sodass selbst Menschen ohne einschlägige Kompetenz in der Lage sind, ein Ethernet-LAN oder WLAN im Privatbereich zu installieren und zu nutzen.

Jedoch ist ab einer gewissen Komplexität eines Netzwerkes ein professionelles Herangehen erforderlich [11, 17].

Über den gesamten Lebenszyklus sind folgende Phasen zu unterscheiden (◘ Abb. 8.1):

Der Prozess der Erstplanung wird hauptsächlich als top-down-Entwurf realisiert und unterteilt sich in Grob- und Feinplanung. Planungsgrundsätze sind dabei die Vermeidung von chaotischen Systemen, die Fehler enthalten bzw. keine effiziente Fehlersuche ermöglichen. Das Netzwerk sollte für



◘ **Abb. 8.1** Lebenszyklus eines Netzwerkes

einen längeren Zeitraum erweiterbar sein und Netzwerkveränderungen sollten effizient durchgeführt werden können.

Man muss auf jeden Fall über die folgenden Planungseinzelphasen hinweg denken:

- Zielspezifikation
- Quantitative Anforderungen
- Echtzeitanforderungen
- Auswahl der Hard- und Softwarekomponenten (Computer, Kopplungselemente, Verkabelung)
- Lastanforderungen
- Kostenanalyse [10].

Die Grobplanung hat die Aufgabe, die wesentlichen Rahmenbedingungen für ein Rechnernetzprojekt festzulegen. Daran sind i. a. mehrere Personen beteiligt, Vertreter der zukünftigen Nutzer, Architekten, Netzwerkspezialisten und andere. Zunächst muss die Anforderungsspezifikation erstellt werden. Dies ist sehr wichtig und keineswegs trivial. Auf Basis der Anforderungsspezifikation werden dann einzelne Teilprobleme benannt sowie Schnittstellen und Lösungskonzeptionen erarbeitet. Die Konzeptionen müssen Grundsatzentscheidungen enthalten, die die Erfüllung der Leistungsanforderungen und die Einhaltung eines vorgegebenen Kostenrahmens garantieren. Spezielle Details sollte die Grobplanung nicht vorschreiben, z. B. Typangaben zu Kabeln und Geräten, Standorte von WLAN Access Points usw.

Die Grobplanung wird i. w. über Diskussion zwischen den Projektbeteiligten erarbeitet. Diese sollten möglichst Praxiserfahrung und Managementqualitäten besitzen. Die Planungsergebnisse müssen fehlerfrei sein und für die gesamte Netzplanungsphase Gültigkeit behalten, andernfalls kann es zu schwerwiegenden Kosten- und Terminproblemen kommen. Häufig kommt es in solchen Fällen zu juristischen Konsequenzen, da Unternehmensnetzwerke oft einen sehr hohen materiellen Wert darstellen.

Nach Abschluss der Grobplanung kann die Feinplanung erfolgen. Diese wird meist von hochspezialisierten Fachleuten realisiert. Unter Berücksichtigung des aktuellen Standes der Technik müssen für die einzelnen Projektteile sehr detaillierte Festlegungen getroffen werden.

Auf Basis konkreter Installationspläne werden Netzwerke i. a. durch beauftragte Bau- und Elektroinstallationsfirmen realisiert. Selbst bei qualifizierter Ausführung der Arbeiten sind fertiggestellte Netzwerke wegen ihrer hohen Komplexität meist noch fehlerbehaftet. Die Netzübergabe erfolgt deshalb erst nach aufwendigen Kontrollmessungen und entsprechenden Korrekturen. Ziel ist mindestens die Validierung der Netzwerkanforderungen, ggf. wird eine Zertifikation bzgl. der Einhaltung von Standards durchgeführt. Eine detaillierte Netzwerkdokumentation ist Bestandteil der Netzübergabe.

Der Hauptteil des Netzwerklebenszyklus ist die Nutzungsphase. Im laufenden Betrieb ist zur Sicherung der Netzqualität eine permanente, leistungsfähige Netzwerkanalyse erforderlich, vorwiegend durch das Netzwerkmanagement. Dieses stellt diverse Netzwerkprobleme fest, z. B. defekte Komponenten, lange Wartezeiten usw. Basierend auf diesen Informationen können Schwachstellen erkannt und beseitigt werden. Im Laufe der Nutzungsphase verändern sich i. a. die Anforderungen an das Netzwerk, z. B. durch Steigerung der Nutzungsintensität oder durch Einführung neuer Anwendungsdienste. In der Regel können die sich daraus ergebenden Probleme durch regelmäßige kleinere Maßnahmen gelöst werden, z. B. durch Ersetzen von Switches, Austausch einzelner Netzkarten usw. Dieses Vorgehen erfolgt als Bottom-Up-Entwurf. Alle Veränderungen müssen exakt dokumentiert werden.

Die Nutzungsphase wird dann beendet, wenn einfache Netzerweiterungen nicht mehr zur Erfüllung von Anwenderanforderungen ausreichen. Der Netzwerklebenszyklus ist zu Ende und es wird die Planung eines neuen Netzwerkes begonnen.

8.2 Grob- und Feinplanung

Die Gründe für die Planung neuer Rechnernetzwerke sind vielfältig [11]. Entsprechend unterschiedlich sind der Umfang und die Komplexität der Aufgabenstellung eines Projektes. Nachfolgend werden einige Projekttypen angeführt. Eine starre Abgrenzung der Projekttypen ist dabei nicht möglich (◘ Tab. 8.1).

Ein Projekt beginnt immer mit einer Kontaktaufnahme zwischen dem Auftraggeber und i. a. mehreren Auftragnehmern, z. B. mit einem Architekten und einem Netzwerk-Ingenieurbüro.

In vielen Fällen sind die Auftraggeber keine IT-Spezialisten. Sie können relativ genau sagen, welche Applikationen sie nutzen bzw. zukünftig nutzen wollen. Ebenso können sie erwartete Qualitätsanforderungen an das Netz formulieren. Jedoch sind sie in aller Regel nicht in der Lage, konkrete Ursachen für Schwachstellen ihres Altnetzes zu benennen bzw. detaillierte technische Forderungen an das neue Netz zu stellen.

Deshalb wird i. a. wie folgt vorgegangen [11]:

1. Eröffnen Projektdokumentation mit der Erfassung allgemeiner Daten, wie
   - Kontaktdaten der Projektbeteiligten
   - Projektbeginn
   - Grobe Vorstellungen des Auftraggebers zu den Netzzielen
   - Zeit- und Finanzrahmen

Tab. 8.1 Typen von Netzwerkprojekten

Typ	Bezeichnung	Aufgaben
I	Modernisierung von Netzen, die i. w. noch den Nutzeranforderungen genügen	Schwachstellenermittlung ggf. Ersetzen Netzwerkkarten ggf. Ersetzen Vermittlungstechnik ggf. Ersetzen Servertechnik
II	Ergänzung von Netzen um zusätzliche Komponenten	z. B. neuartige Dienstleistungen Backup-System WLAN
III	Erneuerung von Netzen, die den Nutzeranforderungen nicht mehr genügen	zusätzlich zu I) Neuplanung der Netzinfrastruktur Beibehaltung der Gebäudeinfrastruktur (EV-Räume, Kabelkanäle, …)
IV	Entwurf vollständig neuer Netzwerke	Ermittlung der Anwenderanforderungen Planung der Gebäudeinfrastruktur (Kabelkanäle, EV-Räume, Serverräume) Planung der strukturierten Verkabelung Planung WLAN, Vermittlungstechnik Planung Servertechnik ggf. Planung der Arbeitsstationen

2. Erfassung des IST-Zustandes
   - Geländekarten und Gebäudepläne
   - Verkabelung
   - Gerätebestand
   - Nutzungsart und -intensität
   - Netzwerkmanagementdaten, wie Fehlerstatistiken usw.
   - oft ist eine aktuelle Netzwerkanalyse durch den Auftragnehmer erforderlich
3. Präzisierte Angaben zur zukünftigen Nutzung (SOLL-Zustand)
4. Geplante Anwendungen mit Zeitrahmen der Einführung
   - Arbeitsplatzlokalisierung
   - Gebäudeveränderungen (Verkabelung, Verteiler- und Serverräume)
5. Kostenvoranschlag
6. Festlegungen
7. Projektunterteilung in Realisierungsphasen
   - Festlegung von Verantwortlichkeiten
   - verbindlicher Zeitplan für alle Realisierungsphasen
   - verbindlicher Kostenrahmen
   - vertragliche Fixierung
   - Anlegen von Lasten- und Pflichtenheften.
   - Angaben zur Anzahl der Nutzer und deren Nutzungsintensität

Nach der Grobplanung schließt sich die Phase der Feinplanung an. In dieser werden die einzelnen Punkte schrittweise bis in die letzten Details festgelegt.

8.3 Rechnernetzmanagement

Moderne Rechnernetze sind sehr komplex. Deshalb ist ein Netzwerkmanagement, d. h. die Überwachung des Netzwerkes bzgl. Störungen, Engpässen, Fehlern oder Umbauten erforderlich.

Einfache Managementaufgaben können mit speziellen Dienstprogrammen gelöst werden, im Internet beispielsweise mit den Diensten PING, NETSTAT, IPCONFIG usw.

Mittels PING kann ermittelt werden, ob ein bestimmter Rechner erreichbar ist, wie schnell die Übertragung ist und wie viele Kommunikationsrechner im Netz passiert werden. NETSTAT liefert Informationen über die Belegung der TCP/IP-Ressourcen. Mithilfe von IPCONFIG können die Schnittstellen zum Basisnetzwerk verwaltet werden.

Mithilfe dieser einfachen Managementwerkzeuge können größere Netze aber nicht verwaltet werden.

Moderne Computernetzwerke sind sehr komplex und sind gekennzeichnet durch [17]:

- hohe Anzahl von Arbeitsplatz- und Serverrechnern
- hohe Anzahl von Netzwerkkopplungselementen (Switches, Router, …)
- hohe Nutzeranzahl
- Heterogenität bei Hardware und Betriebssystemen
- unterschiedliche Anwendungssoftware
- hohe Sicherheitsanforderungen
- schwierige Sicherung der Betriebsfähigkeit.

Die Administration derartiger Netzwerke ist arbeitsaufwendig und teuer. Ohne Computerunterstützung gibt es Probleme bei Konzeption und Dokumentation und bei Fehlersuche und -beseitigung

Die ISO entwickelte umfangreiche Vorstellungen zum *OSI-Management.* Es wird zwischen Systemmanagement SM (Systems Management), Schichtenmanagement LM (Layer Management) und Protokollmanagement LE (Layer Entity Operations) unterschieden. Verwaltet werden Managementobjekte in sog. MIB (Management Information Base) durch Agentensysteme. Die MIB enthalten die für die Verwaltung des Netzes relevanten Informationen.

Das Management unterteilt sich in verschiedene Teilbereiche (s. ◘ Abb. 8.2). Im Weiteren beschränken wir uns auf das Netzwerkmanagement.

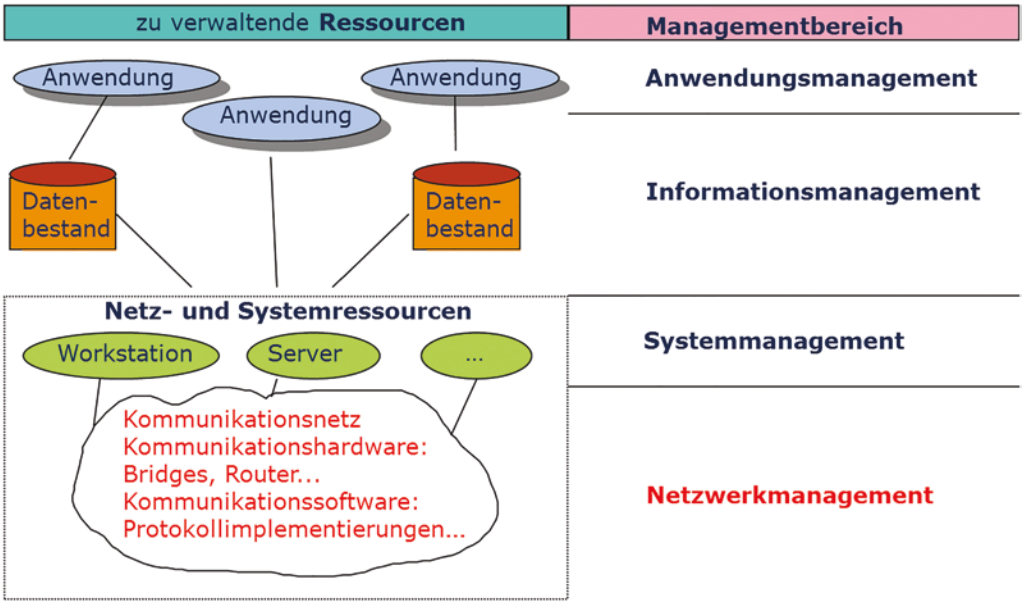


Abb. 8.2 Teilbereiche für das Management

Managementanwendungsprogramme können mithilfe spezieller Managementprotokolle mit den Agentensystemen zusammenarbeiten, um die MIB-Informationen zu lesen oder zu ändern.

Die Realisierung des Managements erfolgt als verteiltes System, um Zuverlässigkeit, Produktivität, Leistung und Sicherheit zu gewährleisten [11, 17].

Netze, die nach der Internettechnologie arbeiten, benutzen mitunter das ISO-gerechte Management mittels CMOT (Common Management Information Protocol over TCP/IP). Meist wird jedoch das einfachere SNMP (Simple Network Management Protocol) genutzt, welches auf dem verbindungslosen Transportprotokoll UDP aufbaut.

SNMP definiert eine Verwaltungsinformationsdatenbank MIB (Management Information Base), in der Informationen über verwaltete Objekte gespeichert sind. Objekte sind z. B. Workstation, Server, Router, Protokollparameter, Systeminformationen.

Die MIB ist i. a. verteilt realisiert, der Zugriff erfolgt über Verwaltungsagenten MA (Management Agents). Die Auswertung bzw. das Verändern der MIB ist Aufgabe von Netzwerk-Verwaltungsanwendungen NMA (Network Management Application). Die NMA können auf beliebigen Rechnern im Netz laufen und den Verwaltungsagenten Lese- oder Schreibaufträge erteilen.

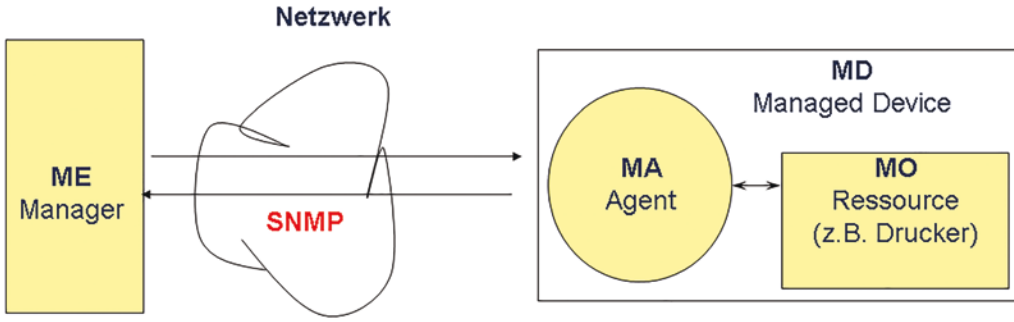
Beim Rechnernetzmanagement wird unterschieden in viele zu überwachende Geräte MD (Managed Devices), die über einen Agenten selbstständig Informationen über wichtige Systemeigenschaften (MO, Managed Objekts) verwalten, und auswertende

Managementprogramme ME (Manager). Der Nachrichtenaustausch zwischen den ME- und MD-Komponenten wird über das SNMP-Protokoll geregelt (◘ Abb. 8.3).

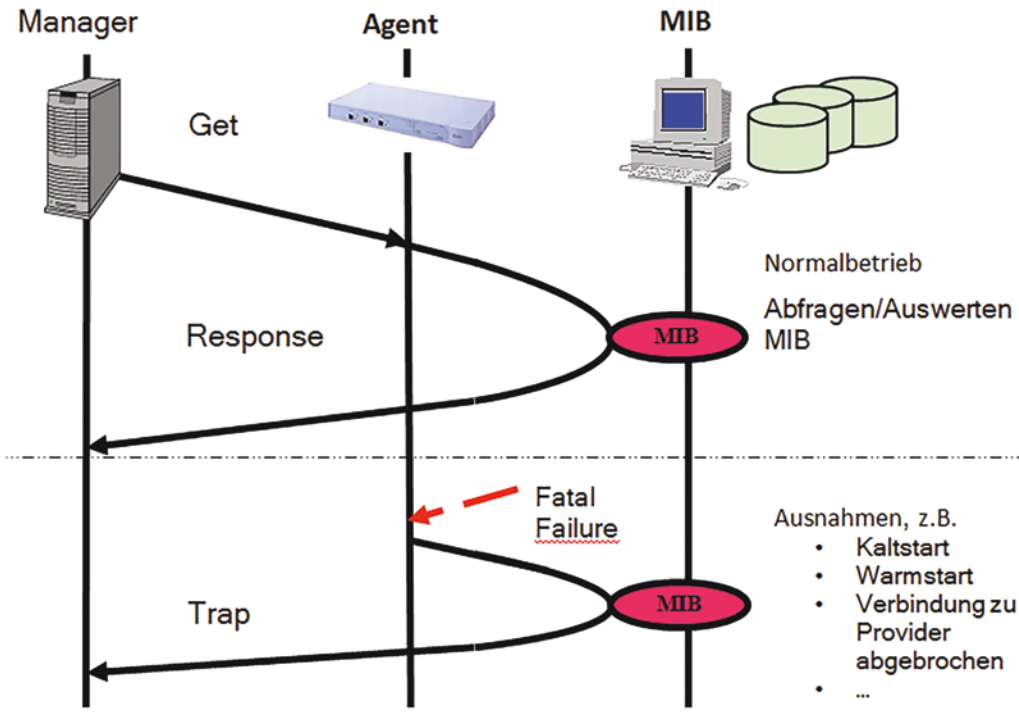
Der Managementdienst besteht aus einer Reihe von Dienstelementen. Bei den wichtigsten Funktionen geht die Initiative vom Manager aus, z. B. über die Dienstelemente (◘ Abb. 8.4):

- **SetRequest** - Einstellen (Verändern) eines Attributwertes einer MD-Ressource

  z. B. Rücksetzen eines Zählers auf Null.



◘ **Abb. 8.3** SNMP-Architektur



◘ **Abb. 8.4** Kommunikationsablauf „Manager – Agent – MIB“

- **GetRequest** - Lesen eines Attributwertes auf dem MD
  z. B. Lesen des aktuellen Wertes eines Zählers
- …

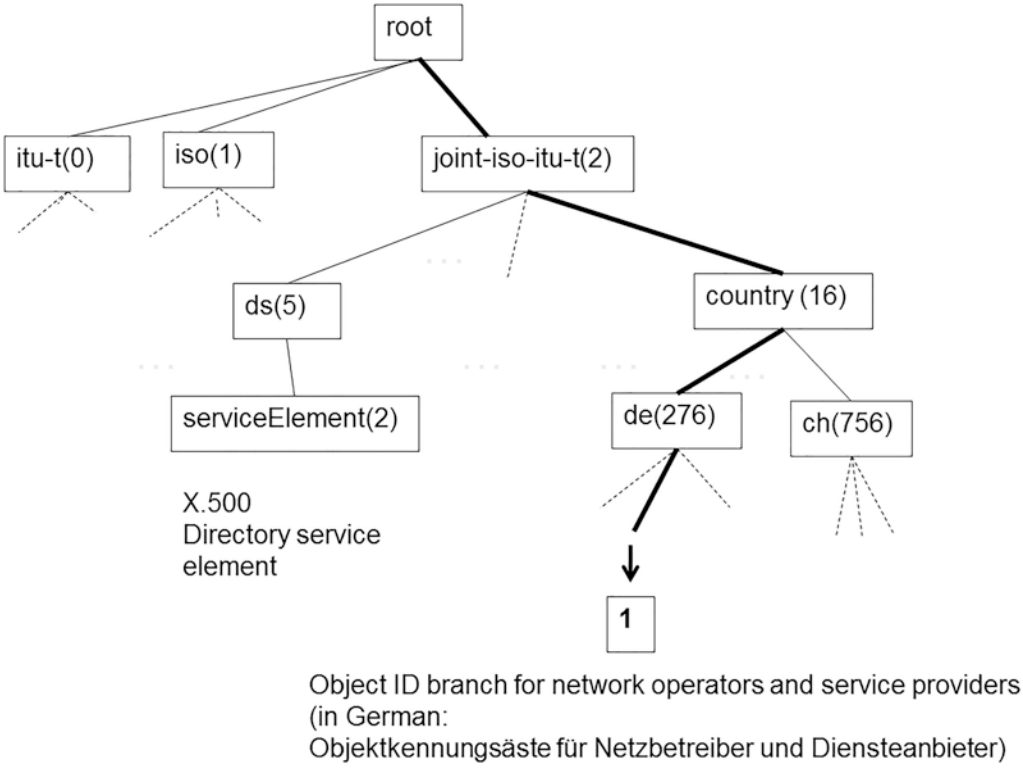
Bei weiteren Dienstelementen ist das MD der Initiator

- **GetResponse** - Antwort auf GetRequest des ME
- **Trap** - unaufgeforderte Ausnahmemeldung des Agenten
- …

Besonders wichtig ist beim Management die eindeutige Bezeichnung der Ressourcen. So soll z. B. die Abfrage der Rechneradresse (GetRequest) für jede Rechnernetzkomponente in gleicher Weise erfolgen, unabhängig von der Art oder dem Hersteller des Gerätes.

Dies wurde über ein international standardisierte MIB (Management Information Base) erreicht. Eine MIB stellt eine spezielle Datenbank mit einer Baumstruktur dar.

Ausgehend von der Wurzel (Root) des Baumes teilt sich die MIB zunächst in einen Teil, der von der Standardorganisation ITU verwaltet wird, einen Teil, der durch die Organisation ISO verwaltet wird und einen gemeinsam verwalteten Teilbaum. Die Teilbäume verzweigen sich dann weiter. Die ◘ Abb. 8.5 zeigt zwei Beispiele:



◘ **Abb. 8.5** Struktur MIB und Navigation zw. den Objekten

- den Zugriff auf den Teilbaum des Verzeichnisdienstes X.500 der ISO.
- und den Zugriff auf die Objektkennungsäste der deutschen Netzbetreiber und Diensteanbieter

Die Identifikation eines MO erfolgt über die Angabe der Position im MIB-Baum. Dazu sind die Zweige des Baumes in jeder Ebene von links nach rechts durchnummeriert, z. B. besitzt Deutschland im Unterbaum country(16) die Position 276 und die Schweiz die Position 756.

Die Notation einer MO-ID wird durch die Wegangabe, ausgehend von der Wurzel, bestimmt. Dies kann auf zwei Weisen erfolgen, zum einen über die Notation in der Sprache ASN.1, zum anderen durch die bloße Angabe der Positionen von links (dot-Notation).

Wir zeigen an dieser Stelle die Identifikation der Informationen zu den deutschen Providern.

ASN1-Notation - {joint-iso-itu-t(2) country(16) de(276) 1}

Dot-Notation - 2.16.276.1

Die ziemlich kryptische Dot-Notation wird i. a. nur von den spezialisierten Netzadministratoren genutzt.

Die für das Netzwerk relevanten Informationen findet man in der MIB im Unterzweig der ISO, danach verzweigt man zu Organisationen, weiter zum DOD (Verteidigungsministerium der USA) und weiter zu den Internetinformationen. Die sog. MIB-II enthält die wesentlichen Parameter zur Konfiguration und zum Protokollverlauf (s. ◘ Abb. 8.6).

So kann man zum Beispiel den Systemnamen eines Gerätes abfragen über die Angabe der ID in ASN.1- oder Dot-Notation:

{iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1)
system1(1) sysName(5)}
1.3.6.1.2.1.1.5

Ein zweites Beispiel wäre die Abfrage der mittels des Transportprotokolls UDP empfangenen Nachrichtensegmente.

{iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) udp(7)
udpInDatagrams(1)}
1.3.6.1.2.1.7.1

Die wichtigsten Betriebssysteme beinhalten adhoc-Systemprogramme zum Abfragen von MIB-Informationen. Diese sind jedoch wenig komfortabel, deshalb ist es sinnvoll, speziellen Managementprogramme zu nutzen (s. Details zu den NWM-Tools und Plattformen in Teil III).

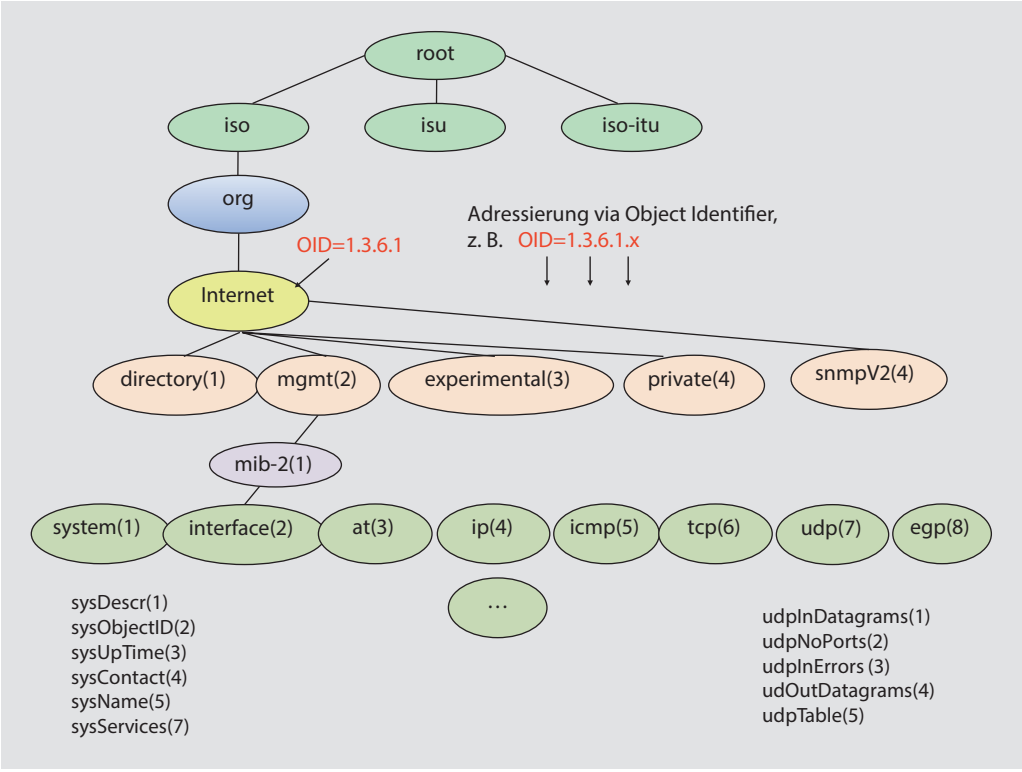


Abb. 8.6 Struktur MIB-II

8.4 Zwischenfragen/Übungsaufgaben

8.4.1 Netzwerkplanung

a) Was bedeutet der „Lebenszyklus“ eines Netzwerkes? Welche Phasen gehören zu diesem Zyklus?

8.4.2 Netzwerkmanagement

a) Diskutieren Sie die Aufgaben des SNMP-Managers und des SNMP-Agenten.

Ausblick Teil I

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_9

In diesem Teil wurden Ihnen die Grundlage zu den Netzwerken mitgeteilt.

Wir haben die wichtigsten Netzwerkarchitekturen dabei diskutiert und die Funktionalität von übertragungsorientierten Schichten des OSI-Referenzmodells präsentiert. Außerdem sind wir auf wichtige Protokolle der Internetarchitektur eingegangen.

Wir schätzen ein, dass Sie aufgrund dieser Kenntnisse weitere Kapitel zu den Netzwerktechnologien, Kopplungsgeräten und Übertragungsmedien selbstständig durcharbeiten können.

Im Teil II erhalten Sie weitere Hinweise zu spezielleren Themen und werden dadurch befähigt, auch zu der Auswahl von Netzwerktechnologien, Kopplungsgeräten und Übertragungsmedien Stellung zu nehmen.

Da alle drei Teile eine Einheit bilden, verzichten wir in den ersten beiden Teilen auf ein Glossar und verweisen auf ein zusammenfassendes Glossar im Teil III.

Lösungen zu Zwischenfragen/Übungsaufgaben Teil I

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_10

Zu ► Abschn. 2.5

► Abschn. 2.5.1 Rechnerverbundsysteme

a) Was versteht man unter den Verbundfunktionen „Kommunikationsverbund", „Ressourcenverbund" und „Steuerungsverbund"?

b) Benennen Sie zu den obigen Verbundsystemen jeweils ein Beispiel und diskutieren Sie die Vorteile.

► Abschn. 2.5.2 Frühe Rechnernetzarchitekturen

a) Vergleichen Sie die proprietären Rechnernetzarchitekturen „Novell Netware" und „IBM SNA".

b) Charakterisieren Sie die Architektur des „ARPAnet".

Zu ► Abschn. 2.5.1a) und b)

Kommunikationsverbund - Möglichkeit des Austausches von Informationen

z. B. Bitströme, Nachrichten, …

schnellere Reaktionen bei Anwendungen

Ressourcenverbund - Bereitstellung von Ressourcen für mehrere Computer

z. B. Netzwerkdrucker, Datenbanken, …

Kosteneinsparungen

Steuerungsverbund - kollektive Lösung eines Problems

z. B. Steuerung eines Produktionsablaufes

Automatisierung

Lösung von Problemen, die ein Computer nicht schafft

Zu ► Abschn. 2.5.2a)

IBM SNA - weltweiter Verbund von Großrechnern

sehr leistungsfähig

aber proprietär auf Produkte der Fa. IBM beschränkt

Zu ► Abschn. 2.5.2b)

ARPAnet - relativ offene Architektur,

Verbund beliebiger Rechner möglich

erstmalige Nutzung der Paketvermittlungstechnik

Zu ► Abschn. 3.3

► Abschn. 3.3.1 Signalausbreitung

a) Wieviel Stufen muss ein Signal mindestens haben, um 3 bit zu übertragen?

b) Wie stark müssen sich 2 Signalstufen mindestens unterscheiden, wenn Rauschspannungen 1 mV (fast) nie überschreiten?

c) Eine Netzwerkkarte sendet mit einer Datenrate von 2,5 GBit/s Signalfolgen mit einem Informationsgehalt von 4 Bit. Berechnen Sie die Schrittrate und die Signaldauer.

d) Folgende Bitfolge 101110001011001110111100 soll mithilfe elektrischer Rechteckimpulssignale (8 Signalstufen) übertragen werden. Zeichnen Sie die Signalfolge in ein Signal-/Zeitdiagramm ein.

► Abschn. 3.3.2 Nyquist-Theorem

a) Wie hoch muss die Bandbreite nach Beispiel 3.3.1c) mindestens sein?
b) Wie hoch muss der Signal-Rauschabstand nach Beispiel 3.3.1c) und mit der Bandbreite von Beispiel 3.3.2a) mindestens sein?

► Abschn. 3.3.3 Medienzugriff

a) Vergleichen Sie deterministische und stochastische Zugriffsverfahren bezüglich ihrer Eignung für Echtzeitanwendungen.
b) Verdeutlichen Sie Gemeinsamkeiten und Unterschiede zwischen Zeitmultiplex- und Frequenzmultiplexverfahren (TDM bzw. FDM).
c) Inwieweit ergänzen Raummultiplex (SDM) und Zellularstrukturen die herkömmlichen TDM- und FDM-Verfahren?

Zu ► Abschn. 3.3.1a)
Signal: **Zusammenhang Informationsgehalt-Stufung**

$I = \mathrm{ld}(S) \qquad S = 2^I$
$I = 3\ \mathrm{Bit/Signal}\ \ S = 2^3 = 8 \rightarrow 8\ \mathrm{Stufen\ erforderlich}$

Zu ► Abschn. 3.3.1b)
Rauschspannung 1 mV → Messwerte weichen ab vom ungestörten Signalwert
Messwert − 1 mV < Signalwert < Messwert + 1 mV
Korrekte Zuordnung in einem Bereich von 2 mV möglich
Min. Abstand zweier Signalpegel > 2 mV (■ Abb. 10.1)

Zu ► Abschn. 3.3.1c)
Ein Signal transportiert 4 Bit, damit

$SR = DR/4 = \left(2{,}5 * 10^9 * 1/\mathrm{s}\right)/4 = 6{,}25 * 10^8/\mathrm{s}$
$T_{\mathrm{Signal}} = 1/SR = 1{,}6\,\mathrm{ns}$

Zu ► Abschn. 3.3.1d)
8 Signalstufen sind ausreichend für 3 Bit Information.
Kodierung der Signalstufen:
0 ← 000 1 ← 001 2 ← 010 3 ← 011 4 ← 100 5 ← 101 6 ← 110 7 ← 111

Bildung von 3-Gruppen:

101	110	001	011	001	110	111	100
5	6	1	3	1	6	7	4

Signalverlauf: (■ Abb. 10.2)

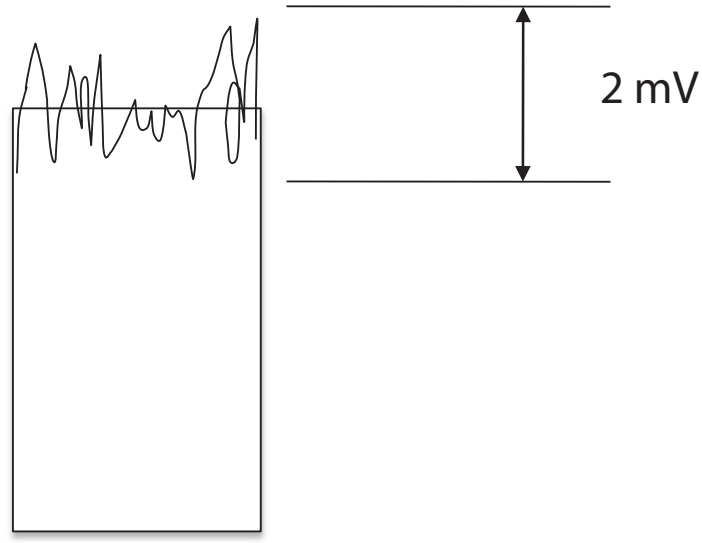


Abb. 10.1 Verrauschtes Signal

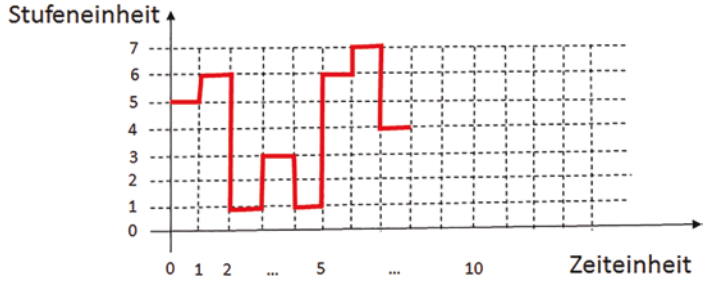


Abb. 10.2 Signal-/Zeitverlauf

Zu ► Abschn. 3.3.2a)

Nyquist-Theorem - $SR < 2 * B$

$$B > SR/2 = 3{,}125 * 10^8 * 1/s = 312{,}5 \text{ MHz}$$

Zu ► Abschn. 3.3.2b)

Nyquist/Shannon - $DR < ld(1 + SNR) * B$

$ld(1 + SNR) = DR/B$

$1 + SNR = 2^{DR/B}$

$SNR = 2^{DR/B} - 1 = 2^8 - 1 = 255$

Zu ► Abschn. 3.3.3a)

Deterministischer Zugriff

Zu jeder Zeit ist nur ein Rechner berechtigt, auf das Medium zuzugreifen. Deshalb gibt es keine Kollisionen. Eine Echtzeiteignung ist gegeben, da eine maximale Wartezeit angegeben werden kann.

Stochastischer Zugriff
Teilnehmer entscheiden selbst, wann sie auf das Medium zugreifen. Durch ausgefeilte Algorithmen wird versucht, die Kollisionswahrscheinlichkeit zu verringern.

Da Kollisionen aber nicht grundsätzlich ausgeschlossen werden können, ist es nicht möglich eine 100 %-ige Garantie für eine bestimmte max. Wartezeit anzugeben. Stochastische Verfahren eignen sich demnach nicht für strenge Echtzeitanwendungen.

Zu ► Abschn. 3.3.3b)

Zeitmultiplex - Mehrfachnutzung des Mediums möglich
Nutzer sendet periodisch mit voller Bandbreite,
darf aber das Medium nur begrenzte Zeit nutzen (Slot)
Eignung nur für Digitaltechnik

Frequenzmultiplex - Mehrfachnutzung des Mediums möglich
Bandbreite wird unter den Nutzern aufgeteilt
jeder Nutzer kann ständig seinen zugeteilten Bereich nutzen
Eignung für Digital-und Analogtechnik

Zu ► Abschn. 3.3.3c)
Sowohl TDM- als auch FDM-Verfahren eigene sich nur für begrenzte Teilnehmerzahlen in überschaubaren Raumgrößen.

Durch Reglementierung von Sendeleistungen kann erreicht werden, dass „ähnliche" Systeme räumlich getrennt arbeiten und sich nicht stören, obwohl sie die gleichen Frequenzen und Zeitslots nutzen.

Zu ► Abschn. 4.6

► Abschn. 4.6.1 Dienst/Protokoll

a) Grenzen Sie die Begriffe Dienst und Protokoll gegeneinander ab!
b) Vergleichen Sie beide Protokolldarstellungsformen Ablauf- und Zustandsdiagramm bezüglich
   - Übersichtlichkeit beim Normalablauf,
   - Anzahl der Diagramme bei alternativen Abläufen,
   - Vorlage für Programmierung und Implementierung!

► Abschn. 4.6.2 Topologien

a) Wie viele Verbindungsleitungen benötigen Sie bei Sterntopologie, um 5 Rechner zu verbinden?
b) Wie viele Verbindungsleitungen benötigen Sie in einem Netz mit 5 Rechnern bei vollvermaschter Topologie (jeder Rechner ist mit jedem anderen Rechner über eine Leitung verbunden)?
c) Wie erhöht sich die Leitungszahl in den Fällen a) und b), wenn ein zusätzlicher Rechner in das Netz eingebunden wird?

► Abschn. 4.6.3 Maßeinheiten

a) Wieviel Zeit benötigt ein System mit einer Übertragungsrate von 1 GBit/s zur Übertragung von 1 GByte Information?

Zu ► Abschn. 4.6.1a)

Dienst

Auf Anforderung eines Dienstnutzers von einem Dienstbereitsteller geleistete Menge standardisierter Funktionen zur Gewährleistung der Kommunikation mehrerer Dienstnutzer.

Der Informationsaustausch erfolgt in vertikaler Richtung zwischen dem Dienstnutzer und dem hierarchisch darunter befindlichen Dienstbereitsteller.

Protokoll

Menge der Regeln, nach denen die Kommunikation zwischen zwei (hierarchisch auf gleichem Niveau befindlichen) Kommunikationseinrichtungen (Instanzen) abläuft. Der Informationsaustausch zur Gewährleistung eines Protokolls erfolgt horizontal.

Zu ► Abschn. 4.6.1b)

Ablaufdiagramme (auch Weg-/Zeit-Diagramme, Zeitfolgediagramme)

Vorteil - dynamische Beschreibung des Dienstverhaltens aus Nutzersicht
leicht zu verstehen

Nachteil - Ein Diagramm beschreibt nur einen Ablauf,
viele Diagramme sind zur Beschreibung aller Abläufe erforderlich
schlechte Vorlage für Implementierung

Zustandsdiagramme (auch Automatenmodelle)

Vorteil - Folge von Zustandsübergängen sichtbar
(Zustand n > Ereignis > Zustand n + 1)
gute Vorlage zur Implementierung

Nachteil - zeitliche Reihenfolge nicht direkt sichtbar
oft unübersichtlich

Zu ► Abschn. 4.6.2a)

Jeder von n Rechnern hat bei Sterntopologie genau eine Leitung zum Sternkoppler.

Bei $n = 5$ sind deshalb 5 Leitungen erforderlich.

Zu ► Abschn. 4.6.2b)

Jeder von n Rechnern hat bei vollvermaschter Topologie genau $(n - 1)$ Leitungen zu den anderen Rechnern, insgesamt gibt also $n * (n - 1)$ Leitungen.

Bei $n = 5$ sind deshalb 20 Leitungen erforderlich $(5 * 4)$.

Im Falle von Duplexleitungen reduziert sich der Leitungsbedarf auf die Hälfte, also 10 Leitungen.

Zu ► Abschn. 4.6.2c)
Bei n = 6 Rechnern ergeben sich für Sternkopplung 6 Leitungen, also eine Leitung mehr.

Bei Vollvermaschung ergeben sich 30 = 6 * 5 Leitungen, also 10 Leitungen mehr.

Zu ► Abschn. 4.6.3a)
Datenraten werden in echten Zehnerpotenzen angegeben, Speichergrößen dagegen Stufen von 2er-Potenzen.

$$\begin{aligned} \text{DR} = 1\ \text{GBit/s} &= 10^9\ \text{Bit/s} \\ \text{Sp} = 1\ \text{GByte} &= 2^{30}\ \text{Byte} \quad \text{bzw. } 1{,}073741824 * 10^9\ \text{Byte} \\ &\qquad\qquad\quad \text{bzw. } 8{,}589934592 * 10^9\ \text{Bit} \end{aligned}$$

Es ergibt sich Übertragungsdauer T von:
T = Sp/DR = 8,589934592 s

Zu ► Abschn. 5.4

► Abschn. 5.4.1 OSI-Schichtenarchitektur

a) Erklären Sie die Begriffe Dienstzugriffspunkt (Service Access Point) und Dienstelement (Service Primitive).
b) Kann eine Instanz der OSI-Schicht 5 direkt auf Dienste der Schicht 3 zugreifen?

► Abschn. 5.4.2 Schichten im OSI-Referenzmodell

a) Ein Rechnernetz mit einer 7-Schichtenarchitektur habe pro Schicht einen Verlust der Übertragungsrate von 10 % infolge Overhead. Wie hoch ist die Anwendungs-Übertragungsrate in einem Fast-Ethernet-LAN (100 MBit/s)?
b) Welche der OSI-Schichten beschäftigt sich jeweils mit
   - Übertragung von Bitströmen
   - Ende-zu-Ende-Kommunikation
   - Wegewahl?
c) Warum benötigen Vermittlungsstellen weniger Schichten?

Zu ► Abschn. 5.4.1a)
Dienstelemente realisieren Bestandteile eines Dienstes. Sie können z. B. als Prozeduren realisiert werden. Dabei können Aufruf- und Ergebnisparameter übergeben werden.

Dienstzugriffspunkte kennzeichnen die Übergabestelle der Dienstelemente. Meist verfügen sie über eine netzeindeutige Kennung (Adresse).

Zu ► Abschn. 5.4.1b)
Nein, denn Instanzen einer Schicht können immer nur Dienste der unmittelbar darunter liegenden Schicht zugreifen.

Zu ► Abschn. 5.4.2a)

Jede Schicht reduziert die Bruttodatenrate auf die Nettodatenrate (90 %) - $NR = BR * 0{,}9$

Bei 7 Schichten bedeutet dies - $NR_7 = BR_1 * 0{,}9^7$

Insgesamt wird die Bruttodatenrate von 100 MBit/s reduziert auf:

$$NR_7 = 0{,}478 * 100\,\text{MBit/s} = 47{,}8\,\text{MBit/s}$$

Zu ► Abschn. 5.4.2b)

Bitübertragungsschicht	(Physical Layer)	OSI-Schicht 1
Transportschicht	(Transport Layer)	OSI-Schicht 4
Vermittlungsschicht	(Network Layer)	OSI-Schicht 3

Zu ► Abschn. 5.4.2c)

Die Vermittlungseinrichtungen interessieren sich nicht für den Anwendungsaspekt, sondern nur für die (evtl. schrittweise) Weitervermittlung.

Deshalb benötigen sie nur die OSI-Schichten 1–3.

10

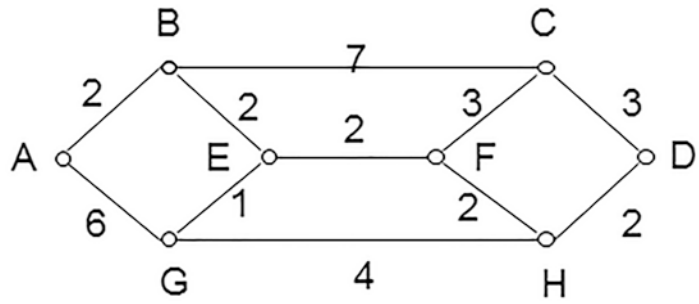
Zu ► Abschn. 6.5

► Abschn. 6.5.1 Routing

Gegeben sei ein Netz mit folgender Topologie und Kostenbewertung der Übertragungspfade (◘ Abb. 10.3)

a) Wovon können die Kostenbewertungen im realen Netz abhängen?

b) Bestimmen Sie schrittweise den kürzesten Pfad von A nach D nach dem Verfahren „Shortest Path Routing“ von Dijkstra.



◘ **Abb. 10.3** Netzwerkgraph

► Abschn. 6.5.2 IP-Adressierung
Eine Firma besitzt einen IP-Adressbereich von 128.10.192.0 bis 128.10.199.255

a) Der Bereich soll in mehrere Subnetze mit jeweils 30 Hosts aufgeteilt werden.
b) Geben Sie eine geeignete Maske an!
c) Wie viele Subnetze können adressiert werden?
   Teilen Sie die IP-Adresse 128.10.192.70 in Netz- und Host-Anteil auf.

► Abschn. 6.5.3 Nutzerschnittstelle TCP/UDP

a) Welche Aufgabe haben Portnummern?
b) Welche Dienstqualität bieten UDP bzw. TCP?
c) Was sind die Ziele der Fluss- und der Staukontrolle?

Zu ► Abschn. 6.5.1a)
Die Bewertungen der Kanten im Netzwerkgraph hängen ab von:

- Datenrate
- durchschnittlicher Auslastung
- Zuverlässigkeit
- Mietkosten
- …

Zu ► Abschn. 6.5.1b)

1. zunächst Wahl des ersten Arbeitsknotens A
2. Beschriftung der Nachbarknoten B mit B(2,A) und G mit G(6,A)
3. Weiter mit Wahl des nächsten Arbeitsknotens B (niedrigster Wert)
4. Beschriftung der Nachbarknoten C mit C(9,B) und E mit E(4,B)
5. Weiter mit Wahl des nächsten Arbeitsknotens E (niedrigster Wert)
6. Beschriftung der Nachbarknoten F mit F(6,E) und G mit G(5,E), besser als G(6,A)
7. Weiter mit Wahl des nächsten Arbeitsknotens G (niedrigster Wert)
8. Beschriftung des Nachbarknotens H mit H(9,G)
9. Weiter mit Wahl des nächsten Arbeitsknotens F (niedrigster Wert)
10. Beschriftung des Nachbarknotens F mit H(8,F), besser als G(9,G)
11. Weiter mit Wahl des nächsten Arbeitsknotens H (niedrigster Wert)
12. Beschriftung des Nachbarknotens D mit D(10,H)

13. Weiter mit Wahl des nächsten Arbeitsknotens C (niedrigster Wert)
14. keine neue Beschriftung erforderlich (keine Verbesserung)
15. Ende mit Wahl des letzten Arbeitsknotens D

Der Graph zeigt die kürzesten Wege zu A für jeden Knoten.
Die Wegekosten von D zu A betragen 10.
Der Weg ergibt sich zu: H über F, dann über E und B bis zu A.

Weg von A nach D: - A → B → E → F → H → D

Zu ► Abschn. 6.5.2a)

128	10	192	0
10000000	00001010	11000000	00000000
128	10	199	255
10000000	00001010	11000111	11111111

Hostanteil: 11 Bit

Adressanzahl - $2^{11} = 2048$

Maske - 255.255.248.0

2 Host-Adressen sind in jedem Netz reserviert:
00…00 - für Netzadresse

11…11 - für Broadcastadresse
30-er Netz erfordert 32-Adreßraum → - 5 Bit Hostanteil

Submaske - 255.255.255.224

Zu ► Abschn. 6.5.2b)
6 Bit - übrig für Subnetzadressierung (11 Bit – 5 Bit)

2^6 - = 64 Subnetze möglich (mit je max. 30 Hosts)

Zu ► Abschn. 6.5.2c)

128.10.192.70	IP	11000000 01000110
	Maske	11111111 11100000
	Netz	128.10.192.64
	Host-ID	6

Zu ► Abschn. 6.5.3a)
Portnummern (16 Bit) repräsentieren einen Speicherbereich auf einem Rechner zur Informationsübergabe zwischen Transportschicht und deren Nutzerprozessen.

Dies ermöglicht eine (quasi-)parallele Kommunikation mehrerer Nutzerprozesse über mehrere unterschiedliche Ports.

Zu ► Abschn. 6.5.3b)
Das verbindungslose UDP bietet gegenüber IP zusätzlich das Multiplexen mehrerer Anwendungsnachrichtenströme.

Nachrichtenverluste sind möglich, die korrekte Reihenfolge empfangener Nachrichten ist nicht gesichert.

Eine Steuerung des Nachrichtenflusses erfolgt nicht.

TCP ist verbindungsorientiert und bietet eine gesicherte Übertragung. Verlorene Informationen werden durch Übertragungswiederholung trotzdem dem Empfänger übermittelt, dies erfolgt nutzertransparent.

TCP verhindert durch eine Flusssteuerung die Überlastung des Empfängers und durch eine Staukontrolle die Überlastung des Netzwerkes.

Bei Übertragung von Echtzeitdaten (z. B. Sprachinformationen) verzichten die Nutzer oft auf die höhere Qualität von TCP und realisieren ihre eigene Übertragungssteuerung über UDP.

Zu ► Abschn. 6.5.3c)
Die Flusskontrolle dient der Verhinderung der Überlastung des Empfängers. Der Empfänger informiert ständig den Sender, wie viele Bytes er momentan noch aufnehmen kann (Empfangsfenster).

Die Staukontrolle soll Netzüberlastungen verhindern, z. B. zu lange Warteschlangen in Routern.

Durch Beobachtung des Netzverhaltens (Fehler) wird ein sogenanntes Staufenster geführt, das regelt, wie viel Bytes momentan unquittiert gesendet werden dürfen.

Zu ► Abschn. 7.5

► Abschn. 7.5.1 Allgemeine Problem von Netzapplikationen

a) Warum ist die Skalierbarkeit in verteilten Systemen so wichtig?
b) Benennen Sie zwei Dienste, bei denen die Sicherung der Datenkonsistenz gewährleistet sein muss.

► Abschn. 7.5.2 Applikationen

a) Beschreiben Sie das Zusammenwirken von Client und Server anhand des WWW.
b) Diskutieren Sie die einzelnen Bestandteile des DNS-Namens ► www.inf.tu-dresden.de.

Zu ► Abschn. 7.5.1a)

Skalierbarkeit - bedeutet, dass bei einer Netzwerkvergrößerung die Wartezeit

auf Netzwerkdienstergebnisse nicht (wesentlich) steigt.

Dienste wie DNS, Google, Wikipedia, …

sind nur bei guter Skalierbarkeit sinnvoll nutzbar

Zu ► Abschn. 7.5.1b)
Dienste, bei denen die Sicherung der Datenkonsistenz gewährleistet sein muss.

z. B. - verteilte Transaktionen in Datenbanken
kollektiver Zugriff auf veränderliche Dokumente

Zu ► Abschn. 7.5.2a)
Grundfunktionalität

WWW-Client
fordert über das HTTP-Protokoll Dateien unter Angabe einer URL-Adresse vom Server an (HTML-Seiten).
Weiterhin realisiert er eine nutzerfreundliche Darstellung des Seiteninhaltes.

WWW-Server
verwaltet HTML-Seiten und sendet sie nach Anforderung (über das HTTP-Protokoll) dem Client zu.

Zu ► Abschn. 7.5.2b)
Von rechts nach links:
top level domain - de
domain - tu-dresden
sub level domain - inf
computer name - www

Diese hierarchische Untergliederung erleichtert die Verwaltung des Namensraumes innerhalb des DNS.

Zu ► Abschn. 8.4
Zu ► Abschn. 8.4.1a)
Unter dem „Lebenszyklus“ eines Netzwerkes versteht man alle organisatorischen Aufgaben beginnend mit der Planung eines Netzwerkes über den Netzwerkbetrieb (Kontrolle, Reparatur) bis zur Modernisierung oder Netzwerkstilllegung.

Zu ► Abschn. 8.4.2a)
SNMP-Agent - Bestandteil der Firmware zu überwachender Geräte
Sammelt Betriebsparameter
und speichert sie in einer Datenbank MIB
SNMP-Manager - Software zur Unterstützung des Netzwerkadministrators
fordert von den Agenten (über das Protokoll SNMP) Informationen an
und speichert ein Abbild des gesamten Netzwerkes
meist in komfortabler Form
(grafische Darstellung der zeitlichen Entwicklung)

Netzwerktechnologien und Mobile Kommunikation. Netzkopplung und Verkabelung

„Schreib den ersten Satz so, dass der Leser unbedingt auch den zweiten lesen will".
(William Cuthbert Faulkner, 1897–1962, amerikanischer Schriftsteller und Nobelpreisträger für Literatur)

Inhalte und kurzfassende Hinweise

Im Teil I wurden Ihnen Grundkenntnisse über die Referenzarchitektur und Basisstrukturen der Netzwerke, Protokolle und Dienste, sowie über die Datenübertragung im nachrichtentechnischen Kanal, über Frameaufbau und Medienzugriffsverfahren, IP-Betrieb und Routing vermittelt.

In diesem Teil wird darauf aufgebaut und Ihnen im Detail vermittelt, wie man auf dieser Basis bestimmte Netzwerkmuster (drahtgebunden, drahtlos, mobil, satellitenbasiert) verwendet und in eine effiziente Vernetzung (mit und ohne Verkabelung) umsetzt. Besonderer Wert wird dabei auf die strukturierte Verkabelung, eine gute Strukturierung organisatorischer Bereiche in Netzwerken, sowie auf die Datensicherheit und den sinnvollen Einsatz von aktiven Kopplungselementen gelegt. Dies ermöglicht die Wiederverwendbarkeit der Netzwerkfragmente und deren besseres Management.

Inhaltliche Schwerpunkte sind wie folgt:

- Abschnitt „Drahtgebundene und drahtlose Netze"
- Abschnitt „Mobile Kommunikation"
- Abschnitt „Netzkopplung und Verkabelung"

Moderne Netzwerkmuster werden in deren Weiterentwicklung repräsentiert (u. a. 40-100GbE, 5G, SAT-Funk, 6LoWPAN).

Gegenüber Teil I werden die Kenntnisse zu den Schichten 2 (Sicherungsschicht) und 3 (Vermittlungsschicht) erweitert. IP gilt als allgemeinnütziges Protokoll in allen Netzwerkmustern (drahtgebunden, drahtlos, mobil, satellitenbasiert). Die schwierige Problematik der Normung in den Rechnernetzen und Zertifizierung der Verkabelung wird den Studierenden durch aussagefähige Beispiele verdeutlicht.

Inhaltsverzeichnis

Lernziele Teil II

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_11

Dieser Teil vermittelt Kenntnisse und Fertigkeiten, die benötigt werden, um von der Problemstellung der Datenübertragung in Netzwerken über bestimmte Netzwerkmuster (drahtgebunden, drahtlos, mobil, satellitenbasiert) zu kostengünstiger, energiesparender und effizienter Vernetzung zu gelangen.

11.1 Voraussetzungen Teil II

Für die Arbeit im Teil II werden die Kenntnisse des Teiles I vorausgesetzt. Insbesondere sollten Sie den Einsatz der OSI- und Internet-Referenzarchitekturen sowie von Basisstrukturen der Netzwerke, Protokolle und Dienste, Datenübertragung im nachrichtentechnischen Kanal, Frameaufbau und Medienzugriffsverfahren, IP-Betrieb und Routing beherrschen.

11.2 Lernziele und vermitteltes Wissen

Auf der Basis der o. g. Voraussetzungen werden Ihnen weitere Details zur Nutzung der Netzwerke vermittelt, u. a.:

1. Welche geeigneten Netzwerkmuster (drahtgebunden, drahtlos, mobil, satellitenbasiert) existieren und welche praxisrelevante Eigenschaften haben diese?
2. Wie organisiert man strukturierte Verkabelung und zertifiziert diese?
3. Wie setzt man auf dieser Basis eine gute Strukturierung organisatorischer Bereiche in Netzwerken, Datensicherheit und einen sinnvollen Einsatz von aktiven Kopplungselementen um?
4. Wie gelangt man gegenüber Teil I auf der Basis der übertragungsorientierten Schichten zu einer kostengünstigen, energiesparenden und effizienten Vernetzung?

Weiterhin wird die schwierige Problematik der Normung in Rechnernetzen und der Zertifizierung der Verkabelung den Studierenden durch aussagefähige Beispiele verdeutlicht. Außerdem werden teilweise Kenntnisse aus weiteren Quellen zitiert, u. a. aus dem Wissensbestand Skripte LS Rechnernetze an der TU Dresden [16], sowie aus eigenen Büchern der Autoren [10, 11]. Diese Problematik wird durch weitere praktische Beispiele ergänzt.

WISSEN:
Sie beherrschen die Technik der kostengünstigen, energiesparenden und effizienten Vernetzung unter Nutzung bestimmter Netzwerkmuster (drahtgebunden, drahtlos, mobil, satellitenbasiert) und der Konzepte der strukturierten Verkabelung. Besonderer Wert wird dabei auf eine gute Strukturierung

organisatorischer Bereiche in Netzwerken gelegt, sowie auf die Datensicherheit und den sinnvollen Einsatz von aktiven Kopplungselementen. Dies ermöglicht die Wiederverwendbarkeit der Netzwerkfragmente und deren besseres Management.

Wir schätzen ein, dass Sie aufgrund dieser Kenntnisse die vereinfachten Modellaufgaben und Projektierungsabläufe nach dem Erlernen der Inhalte des Teiles II selbstständig lösen können.

Drahtgebundene und drahtlose Netze

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_12

12.1 Kerntechnologien – Übersicht, Integration und Interoperabilität

In moderne Netzwerke werden diverse Netztechnologien eingebunden, deren Interoperabilität deshalb sehr wichtig ist. Im Weiteren werden die allgemein anerkannten Abkürzungen verwendet [10, 11, 13, 14, 15, 16, 17, 18, 19]:

- PAN für Personal Area Network.
- LAN für Local Area Network (lokale Netze).
- WLAN für Wireless LAN (drahtlose lokale Netze).
- MAN für Metropolitan Area Network (städtische Netze).
- WiMAX für Worldwide Interoperability for Microwave Access (drahtlose städtische Netze).
- WAN für World Area Network (Weitverkehrsnetze).
- LON für Local-Operation Networks (Automatisierungsnetze).
- WSN für Wireless Sensor Networks (drahtlose Sensorpikonetze).
- 3G für 3.Generation des Mobilfunks (u. a. UMTS).
- 4G für 4.Generation des Mobilfunks (u. a. LTE).
- 5G für 5.Generation des Mobilfunks (künftig IMT2020).
- DSL für Digital Subscriber Line (verbreiteter Typ von Internetanschlüssen).
- MPLS für Multiprotocol Label Switching als Integrationsnetzwerke.

Einige der Abkürzungen werden in weiteren Abbildungen des Abschnittes erklärt.

Typische Netze besitzen LAN mit strukturierter Verkabelung, ergänzende drahtlose WLAN, sowie eine Internetanbindung, drahtgebunden über DSL bzw. drahtlos über LTE (künftig 5G-Netze). Kennzeichnend ist eine allgemeine Dienstintegration (◘ Abb. 12.1). Neben Anwendungen der Bürokommunikation (WWW, Fileservice, Druckservice, …) gibt es zunehmend Dienste für multimediale Kommunikation (Konferenzsysteme, VoIP, TVoIP, …), sowie für Gebäude- und Maschinenautomatisierung.

Die aufgeführte Übersicht (◘ Abb. 12.2) ordnet die modernen Rechnernetze nach Datenrate [MBit/s] und Mobilität bzw. Bewegungsgeschwindigkeit [km/h].

Einige der oben aufgeführten Netzwerkstandards, wie z. B. ATM, WiMAX, ISDN, X.25 sind veraltet und haben derzeit nur

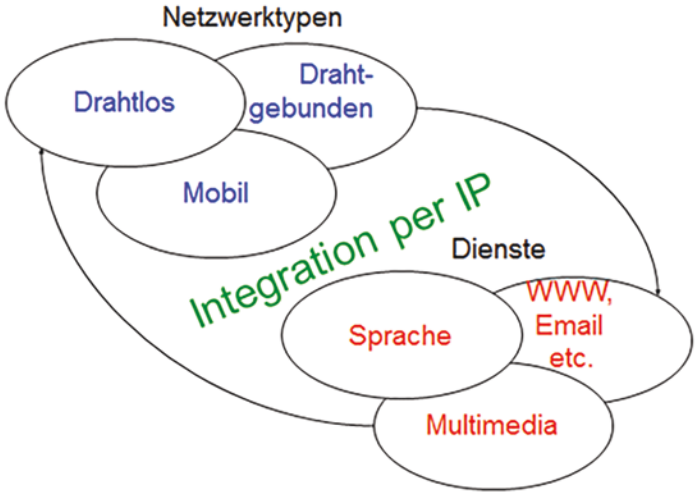


Abb. 12.1 Dienstintegration in modernen Netzwerken

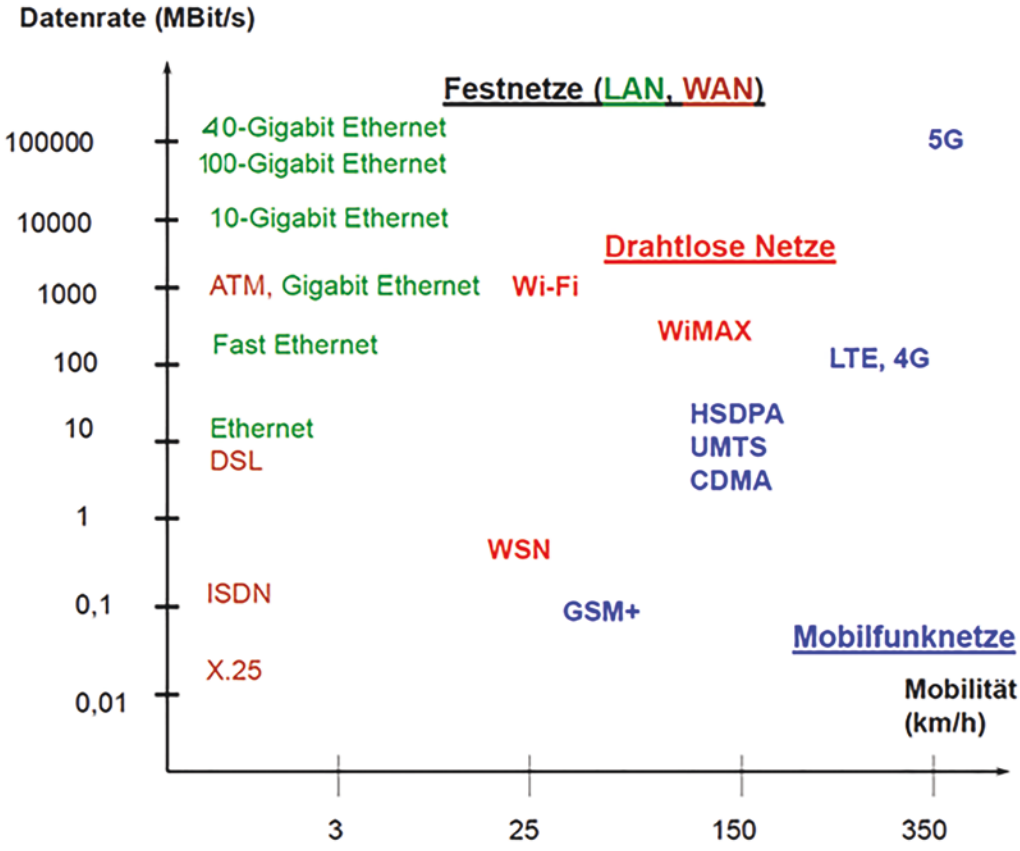


Abb. 12.2 Mobilität vs. Datenrate bei aktuellen Rechnernetztechnologien

historische Bedeutung. Für die Bedürfnisse der Praxis ist es sinnvoll, die betrachteten Rechnernetztechnologien in die folgenden Gruppen aufzugliedern, die später ausführlich erläutert werden [17].

1. **Gruppe LAN, WAN (MAN):**
   - Ethernet (busförmige historische Struktur), FastEthernet,
   - (100-,40-,10-)GigabitEthernet, überwiegend hierarchische Strukturen
   - Wi-Fi (Wireless Fidelity), Wireless LAN, drahtlose LAN mit stochastischem Medienzugriffsverfahren
   - Automatisierungsnetze in der Industrie und im Facility Management/Intelligent House
2. **Gruppe WAN:**
   - ATM (Asynchronous Transfer Mode) und MPLS (Multi-Protocol Layer Switching), die Weitverkehrsnetze mit QoS-Unterstützung und Dienstklassenvergabe
   - (100-,40-,10-)Gigabit Ethernet, leistungsstarke LAN-Technologie, z. T. auch integriert in Weitverkehrsnetze.
3. **Gruppe Zugangsnetze:**
   - DSL (Digital Subscriber Line), typischer digitaler Internetanschluss für Privatanwender, Homeoffices sowie Mittelstandsunternehmen anhand der FDM/OFDM-Technik, die den digitalen Zugang über herkömmliche Telefonleitungen bereitstellt.
   - Kabel-Modem (cable modem), Internet-Kommunikation mithilfe der Modulation/Demodulation über existierende Fernsehkabelsysteme.
   - ISDN (Integrated Services Digital Network), herkömmliches digitales Netzwerk für Sprach- und Datenkommunikation, veraltet.
   - MPLS (Multiprotocol Label Switching) als Integrationsnetzwerke für gängige Zugangsnetze, u. a. DSL, VPN.
4. **Gruppe Mobilfunknetze:**
   - GSM (Global System for Mobile Telecommunication), Mobilfunknetze der 2. Generation.
   - UMTS (Universal Mobile Telecommunication System), Mobilfunknetze der 3. Generation.
   - HSDPA (High Speed Downlink Packet Access), eine leistungsfähigere UMTS-Variante, wird auch als 3,5G oder UMTS-Broadband bezeichnet.
   - LTE (Long Term Evolution) als sog. 3,9G und LTE Advanced als 4G mit Datenrate bis 1000 MBit/s zur Ablösung von 3G- und WiMAX-Systemen.
   - IMT 2020 als künftige 5. Generation des Mobilfunks mit signifikanter Erhöhung der Datenrate bis auf 10 GBit/s und QoS-Verbesserungen, wie geringere Latenz und Multimediaintegration und Cloud Computing

5. **Gruppe drahtlose Funknetze:**
   - Drahtlose Pikonetze WSN (Wireless Sensor Networks) mit Schwerpunkt Energieeffizienz.
   - Drahtlose städtische Makronetze oder MAN, für die Zugangstechnik WiMAX (Worldwide Interoperability for Microwave Access).

Integration aktueller Funknetze Die Funknetze funktionieren im Bereich [11, 16]:

–	Frequenzbereich	10^5	…	10^{12} Hz
–	Wellenlängenbereich	3 km	…	300 µm

Aktuelle Funknetze belegen i .d. R. Frequenzbereiche von 900 bis 35 GHz (GSM, UMTS, LTE, WLAN, 5G etc.).

Funknetze können sich gegenseitig stören (Interferenz usw.). Deshalb besitzen viele Funknetze Sendeleistungsbeschränkungen und Zellstrukturen. Die entsprechenden Zellausdehnungen (bzw. Sendereichweiten) variieren je nach Technologie von 10 m bis 100 km.

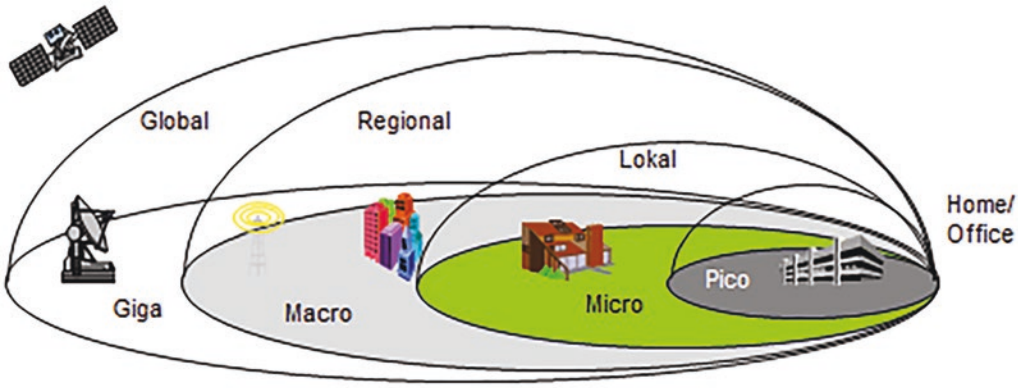
Die Pikonetze (Bluetooth, ZigBee) und Mikronetze (WLAN) mit geringer Ausdehnung werden interoperabel zu Funklösungen (GSM, UMTS, LTE, 5G, …) und Satellitensystemen (Ortungssysteme GPS, Galileo, sowie weitere Dienste mit geostationären Satelliten und Satellite Base Augmentation Systems). Der Einsatz hierarchischer Zellenstrukturen (Piko-, Mikro-, Makro, Gigazellen) ist dadurch überall möglich (◘ Abb. 12.3).

- Transnationale Netzbetreiber, Satelliten.
- Nationale Netzbetreiber.
- Campus, Stadtviertel, Ballungsgebiete.
- „Hotspots“ – Bahnhöfe, Cafes, Flughäfen, Hotels.

Die aktuellen 4G-Systeme befinden sich im schrittweisen Ausbau und stellen auch die Interoperabilität mit den Gebäude- und Campusvernetzungen bereit. Es geht um weitere dichtere Integration zwischen Sprach- und Datenübertragungsdiensten über IP mit vielfältigen Einsatzszenarien. Ein typisches Szenario ist:

- Drahtlose Übertragung von Sprache und Multimedia.
- Drahtgebundenes bürotypisches LAN.
- IP-Telefondienste per WLAN usw.
- Die Zuordnung der aktuellen Netzwerktechnologien zu den oben genannten Zelltypen wird in ◘ Abb. 12.4 gezeigt.

Normung Der Löwenanteil dieser Technologien wurde durch das IEEE-Gremium (Institute of Electrical and Electronics



Typ	Distanz	Datenrate (MBit/s)	Mobilität (km/h)	Einsatz bei 3G und 4G
Giga Cell	~100 km	0,144..10	1,3 km/s oder 4700	Transnationale Netzbetreiber, Satelliten
Macro Cell	~10 km	0,144..0,384	500	Nationale Netzbetreiber
Micro Cell	~1000 m	0,384...2	120	Campus, Stadtviertel, Ballungsgebiete
Pico Cell	~10 m	2..10	10	„Hotspots" – Bahnhöfe, Cafes, Flughäfen, Hotels

Abb. 12.3 Hierarchische Zellenstrukturen für 3G/4G/5G- Mobilfunk

12

Engineers) standardisiert, bspw. IEEE 802.3 Ethernet. Zu den weiteren Standardisierungsgremien im Bereich Netzwerke gehören in erster Linie ITU-T (Telefon- und Datenkommunikation, z. B. für ATM, GSM, UMTS) und ISO (International Organisation for Standardisation), z. B. für das OSI-Modell. Eine Liste relevanter IEEE-Standards wurde in Tab. 12.1 zusammengefasst.

Alle oben erwähnten Normen für Rechnernetze (Telekommunikationsnetzwerke) sind sog. „De-jure-Normen" oder offizielle Standards. Deren Hauptbedeutung liegt in der Bereitstellung der Kommunikation in heterogenen Systemen. Weitere Normen gelten als „De-facto"-Normen bzw. Industriestandards, wie z. B. IBM PC, anfangs Unix/Linux, TCP/IP. Nachfolgend werden einige der oben erwähnten Technologien im Detail veranschaulicht.

12.1.1 ATM-Netze (Asynchronous Transfer Mode)

ATM ist eine Netztechnologie, die in Weitverkehrsnetzen eingesetzt wurde (noch früher auch in LAN). Sie ist verbindungsorientiert (virtuelle Verbindungen) und basiert auf einer

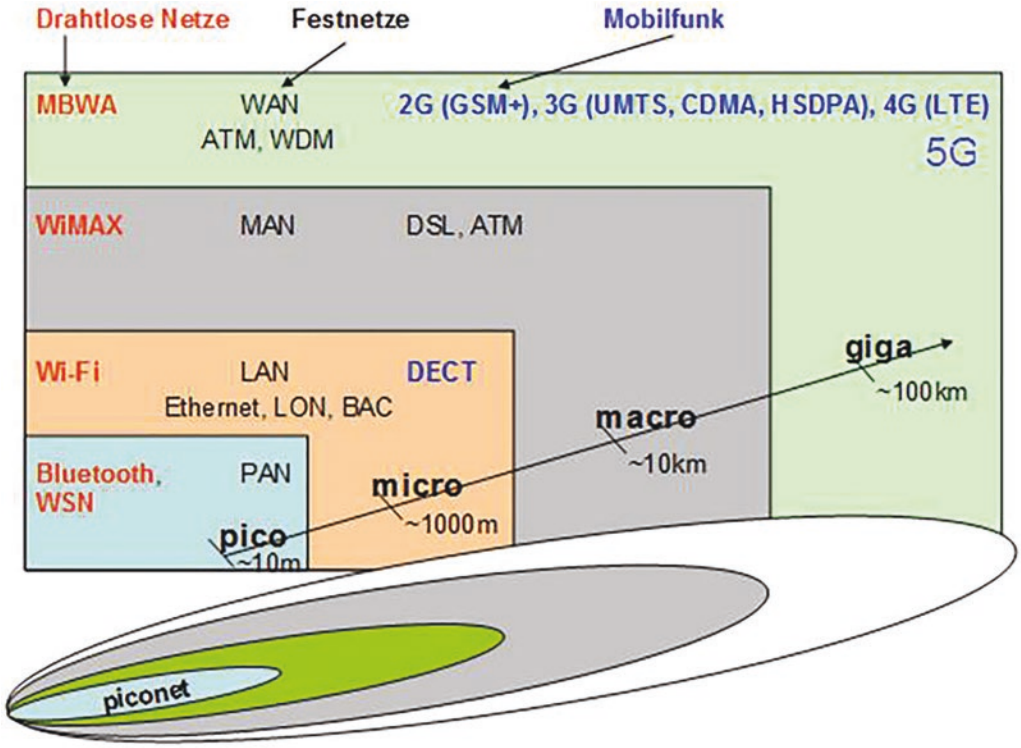


Abb. 12.4 Netzwerktechnologien und Zellgrößen

Zeitmultiplex-Datenübertragung in Form von Paketen fester Länge, den sog. „Zellen" (cells) mit einer Größe von 424 Bit (53 Byte). Davon bilden 5 Byte den Zellkopf und max. 48 Byte den Dateninhalt. Der konstante Overhead (Zusatzdatenratenverlust pro Paketkopfübertragung) liegt damit über 9 %.

ATM ermöglichte als erste Netztechnologie eine Kanalintegration verschiedenartiger Datenströme (konstante, variable Datenraten, …) unter Garantie einer geforderten Dienstqualität (QoS – Quality of Service im Rahmen eines Dienstnutzungsvertrages SLA – Service Level Agreement; weitere Details dazu [11]). Es wurde eine weitgehende Integration diverser Nachrichtenverkehrsklassen (Daten, Text, Grafik, Sprache, Video) realisiert (Abb. 12.5).

Dabei müssen die Nutzer Dienstklassen (A-D und X) angeben werden und diese werden dann auf QOS-Parameter abgebildet, wie z. B. Bitrate, Delay oder Jitter. Die ATM-Steuerung organisiert dann die Zuordnung der zu übertragenen Zellen auf Zeitschlitze (Zeitmultiplextechnologie).

Tab. 12.1 IEEE-Standards für Rechnernetze

802.1	High Level Interface
802.2	Logical Link Control
802.3	CSMA/CD LAN
802.4	Token-Bus LAN
802.5	Token-Ring LAN
802.6	MAN Metropolitan Area Networks (DQDB)
802.7	Broadband Technical Advisory Group
802.8	Fibre Optics Technical Advisory Group
802.9	Integrated Voice and Networks (Isochronous LANs)
802.10	Network Security
802.11	Wireless Networks
802.12	Demand Priority Access (100VG-AnyLAN)
802.14	Cable Modems
802.15	Wireless Personal Area Network
802.16	Broadband Wireless Access
802.17	Resilient Packet Ring
802.18	Radio Regulatory Technical Advisory Group (RRTAG)
802.19	Coexistence TAG
802.20	Mobile Broadband Wireless Access (MBWA) Working Group
802.21	Medienunabhängiges Handover
802.22	Wireless Regional Area Networks
802.30	100 Base-X, 100 Base-T, Fast Ethernet

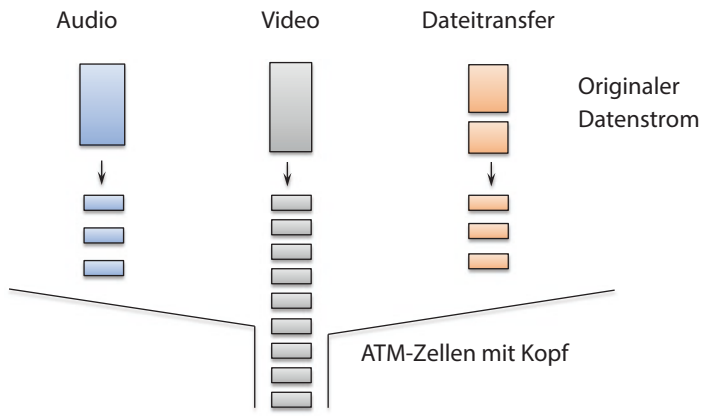


Abb. 12.5 Asynchronous Transfer Mode

Asynchroner Transfermodus:
- Übertragung kleiner „Zellen“ fester Größe (53 Byte)
- Verbindungsorientiert, paketvermittelt (hier: Paket = Zelle)
- Statistisches Zeitmultiplex

Standardisierung (praxisrelevant nur im WAN-Bereich):
- LAN: ATM-Forum, IETF (Internet Engineering Task Force)
- WAN: ITU (International Telecommunication Union).

Wichtige Grundgedanken der ATM-Technologie, wie das Konzept der virtuellen Verbindungen, wurden von der aktuellen MPLS-Technologie übernommen.

12.1.2 Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) ist eine effiziente Integrationstechnik für aktuelle Zugangsnetze und Weitverkehrsnetze [3, 7, 16].

MPLS verwirklicht eine Abbildung auf existierende Netztechnologien wie ATM, Frame Relay, Gigabit Ethernet, VPN bzw. die direkte Implementierung durch spezielle MPLS-Hardware unmittelbar über Lichtwellenleitern (SONET).

MPLS-Pakete sind wesentlich größer (Orientierung an Ethernet 1500 Byte) als ATM-Zellen mit fixierter Größe von 53 Byte. Dadurch wird der Overhead wesentlich verringert (Header-Anteil geringer) [16].

Die Komponenten der MPLS-Architektur sind wie folgt (◘ Abb. 12.6):
- der Quell-Host (i. d. R. in einem LAN)
- Ingress-Router und Egress-Router
- der Ziel-Host.

Ein MPLS-Tunnel wird zwischen Sender- und Empfänger-LANs (sog. Quell- und Zielsysteme) durch das Gesamtnetz ermittelt (z. B. per IP-Routing und RSVP, Resource Reservation Protocol). Am Eingang des MPLS-Tunnels agiert dabei der Ingress Router, am Ausgang agiert der Egress Router.

MPLS ermöglicht eine effiziente Weiterleitung von Paketen entlang vordefinierter Pfade (auch Hierarchie von Pfaden möglich) gemäß ihrer sog. Forward Equivalence Class (FEC). Über die Pfade werden alle Pakete eines Datenstroms (bspw. für eine Videokonferenz) gleich behandelt. Diese Weiterleitung wird durch Labels gesteuert, die jeweils aufeinander folgende Pfadabschnitte kennzeichnen. Auf diese Weise garantiert MPLS erforderliche Dienstqualitäten (QoS) bei zeitkritischen Anwendungen.

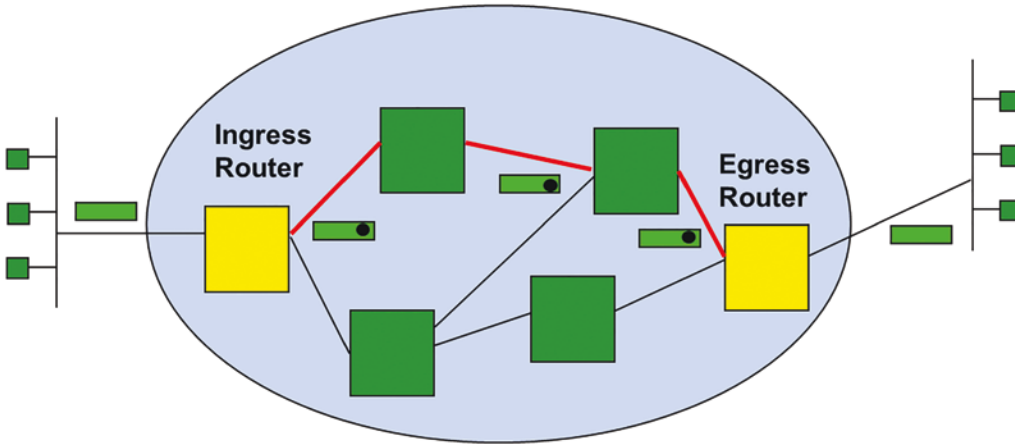


Abb. 12.6 MPLS-Architektur

Der Gesamtablauf zwischen dem Quell-Host, den Ingress/Egress-Routern zu dem Ziel-Host im MPLS-Netzwerk enthält die folgenden Schritte [16]:

1. Pfad („Tunnel“) durch das Gesamtnetz wird ermittelt (z. B. mittels IP-Routing)
2. Label Distribution Protocol (LDP) legt Labels für diesen Pfad fest
3. Ingress Router markiert eingehende Pakete gemäß Forward Equivalence Class (FEC) mit passendem Label
4. Effiziente netzinterne Weiterleitung gemäß vorgegebenem Pfad (vgl. ATM)
   dabei Umwandlung Eingangslabel → Ausgangslabel durch jeden Switch
5. Egress Router entfernt Label und leitet Pakete ins Zielsystem weiter.

12.1.3 Mobilfunknetze der 3. Generation. HSDPA, High-speed Downlink Packet Access

Dieser Standard agiert als Erweiterung von UMTS (Universal Mobile Telecommunications System, Broadband UMTS) im Rahmen der dritten Mobilfunkgeneration [11, 16]. HSDPA bietet gegenüber UMTS eine Reihe wesentlicher Verbesserungen. So beträgt die Datenrate bis 14,4 MBit/s im Downlink, d. h. der Übertragung von einer Basisstation (oder dem Netzwerkprovider) zum User bzw. bis 10,8 MBit/s im Uplink (aufwärts vom User zum Netzwerkprovider). Die Technologie ist auf der Kombination von Zeitmultiplex (TDMA), Kanalbündelung (channel bundling)

und fortgeschrittener adaptiver Kodierung aufgebaut. Es werden breitbandige Codemultiplexverfahren (W-CDMA, wideband code multiplex) sowie ein intelligentes Bandbreitenmanagement eingesetzt. Weiterhin unterstützt HSDPA einen separaten Managementkanal. Die HSDPA-Technologie dient als Basis für die Weiterentwicklung des mobilen Internet und der multimedialer Kommunikation (Videotelefon, Fernsehen, Spiele).

12.1.4 Drahtlose lokale und städtische Netze WLAN und WiMAX

Drahtlose Vernetzungen Wi-Fi/WLAN und WiMAX sind heutzutage sehr verbreitet [11, 16].

Der Einsatz von WLAN ist fast überall möglich, z. B. gibt es Lösungen für Büros und Privatnutzer und öffentliche Zugangspunkte (Hotspots) in Hotels und an Hochschulen, auf Bahnhöfen und Flughäfen. Die Datenraten liegen aktuell durchschnittlich im Bereich von 100 bis 1000 MBit/s.

Die WiMAX-Technik wies ein rasantes Wachstum von 2004 bis 2009 auf. Die aktuellen Standards für WiMAX spielen in manchen Ländern die Rolle von 4G-Netzen. Die WiMAX-Netze sind für ein breites Frequenzband von 10 bis 66 GHz (sowohl lizenzfrei als auch -pflichtig) ausgelegt. WiMAX-Systeme werden dabei in mehreren Modi eingesetzt (Backbones, Zugangsnetze, Zellularstrukturen), welche die flexible Zusammenarbeit mit WLAN und 3G (LTE) – Zellenstrukturen sichern. Die Datenraten sind spezifikationsabhängig und liegen im Bereich 40 bis 100 MBit/s.

In diesen Netztechnologien wurden erstmalig moderne Raummultiplexmethoden (SDM, Space Division Multiplexing) in Kombination mit innovativer Antennentechnik verwendet (MIMO, Multiple Input Multiple Output).

- **Aktuelle Technologien**

werden in den nachfolgenden Abschnitten im Detail vorgestellt.

12.2 Ethernet-Familie IEEE 802.3

12.2.1 Basistechnologien (IEEE 802.3)

Grundlagen zu Ethernet Die Ethernet-Familie besteht aus mehreren Generationen und spielt seit langem die Rolle einer Kerntechnologie für lokale Rechnernetze. Das erste Ethernet war 10Base5 mit einer Datenrate von 10 MBit/s, die auf alle aktiven Netznutzer aufgeteilt wurde („Shared Medium“). Eine Kopplung

mehrerer Ethernet-LAN erfolgte ohne Lasttrennung über Multiportrepeater (Hubs). Die z.Zt. leistungsfähigsten Ethernet-LAN (10 GbE) realisieren ein Datenrate von 10 Gigabit/s. Gekoppelt wird über leistungsfähige Switches mit Lasttrennung.

Die Anwendungsgebiete in modernen IT sind vielfältig (◘ Tab. 12.2). Die Tabelle stellt die Zusammenhänge zwischen Ethernet-Standards, Kabeltypen und maximal zulässigen Ausdehnungen dar [11].

Switched-Ethernet ◘ Abb. 12.7 präsentiert ein integriertes Szenario für ein „Switched-Ethernet", d. h. eine über Switches verbundene Hierarchie von Ethernet-LAN. Dabei erfolgt eine schrittweise Datenratenmigration verschiedener Hierarchieebenen, z. B. durch den Einsatz der Ethernet-Standards Fast-Ethernet, Gigabit-Ethernet und 10 Gb-Ethernet.

Switched-Ethernet ermöglicht eine zeitparallele Vermittlung aller Verkehrsströme durch die Switch-Hardware und hat den Vorteil, dass es keine Framekollisionen gibt, sodass jeder Station die volle Ethernet-Datenrate zur Verfügung steht (◘ Abb. 12.7a und b). Damit wird Ethernet zum „Switched

◘ **Tab. 12.2** Ethernet und verbreitete Kabeltypen [3, 4, 11]

Kabeltyp	Ethernet-Standard	Ausdehnung (m)
RG58 Kabel thin (Thinwire)	10Base2	185
RG8 Kabel thick (Thickwire)	10Base5	500
CAT-3 Kabel UTP	10Base-T	100
CAT-5 Kabel UTP	10Base-T	100
	100Base-T	100
Multimode-Glasfaser	1000Base-SX	550
	10GBase-SR	82
	10GBase-LX4	300
Singlemode-Glasfaser	1000Base-SX	2000
	1000Base-LX	10.000
	10GBase-LX4	10.000
	10GBase-ER	40.000
Monomodeglasfaser	1000Base-LX	10.000
STP	1000Base-CX	25
Doppelt-twinaxiale Kupferkabel	10GBase-T	100

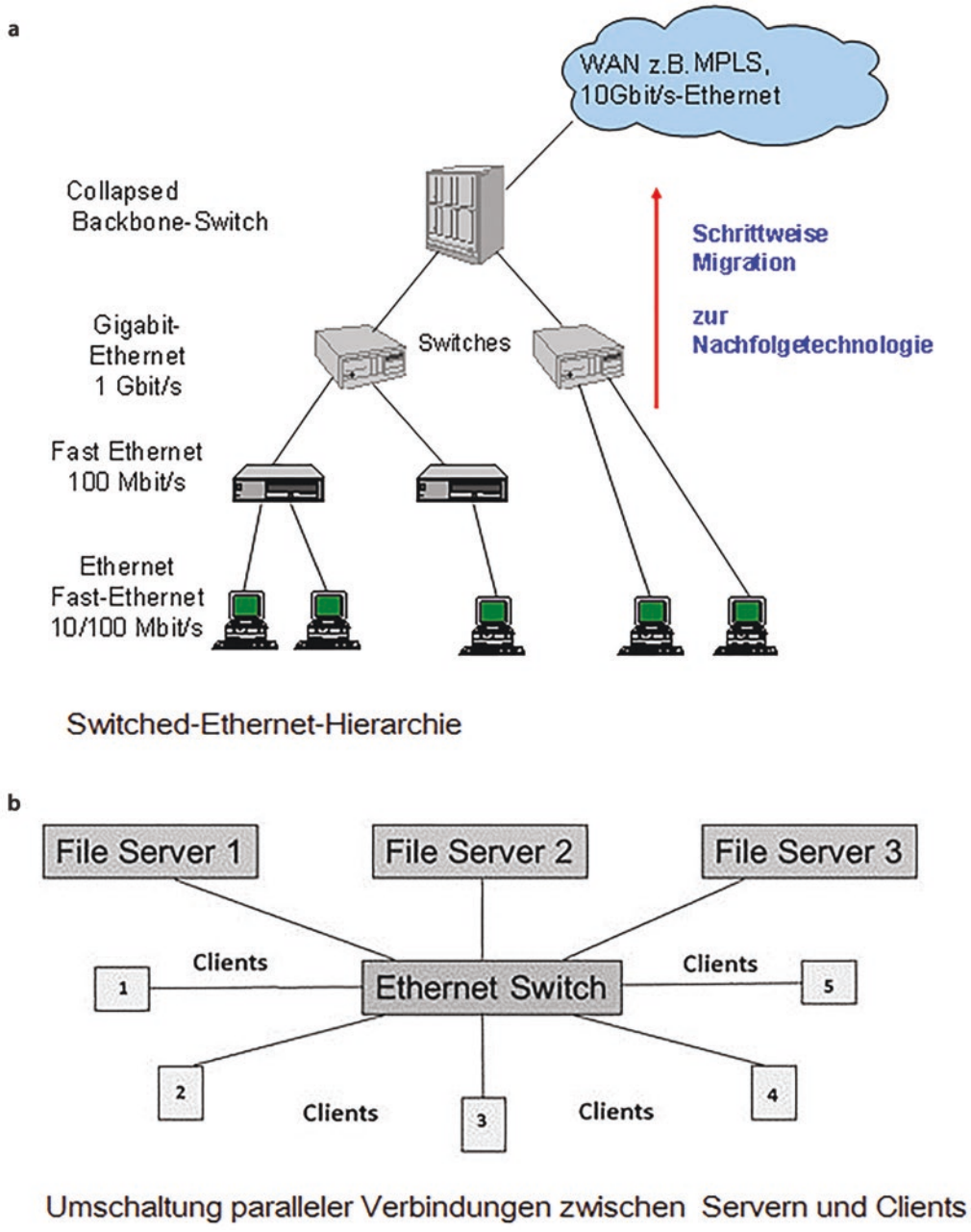


Abb. 12.7 Switched Ethernet: **a** Switched-Ethernet-Hierarchie; **b** Umschaltung paralleler Verbindungen zwischen Servern und Clients

Medium". Unterstützt werden Duplexübertragungen mit einem breiten Ethernet-Datenratenspektrum von 10 bis zu mehr als 10.000 MBit/s. Die Vermittlung erfolgt i. d. R. sehr schnell (Mikrosekunden-Bereich).

Ein weiterer Vorteil der Technik liegt darin, dass in einem Netzwerk die Aufteilung der Stationen in unterschiedliche virtuelle lokale Netze (VLAN) möglich ist, unabhängig von der Position der Station in der Baumhierarchie. Dieses fortgeschrittene Konzept dient der Schaffung von Sicherheitszonen auf der OSI-Schicht zwei und ermöglicht einen authentisierten Frame-Verkehr im Ethernet.

Die Technologien Fast-/Gigabit-Ethernet bzw. 10 GBit Ethernet weisen trotz erhöhter Datenraten (100 MBit/s, 1 GBit/s bzw. 10 GBit/s) eine Kompatibilität zu den älteren Ethernet-Konzepten auf.

Als Übertragungsmedium wird meist TP-Kupferkabel (mindestens Kategorie 5) oder Lichtwellenleiter verwendet. Die LAN-Segmentlänge liegt im Bereich von 100 m bei Kupferkabeln bis zu mehreren km bei Lichtwellenleitern im 10 GBit/s-Ethernet. 10GbE wird auch für die Zugangsnetze (z. B. für ein sog. „Ethernet in the First Mile / Last Mile“) und sowie für Teilstrecken in Weitverkehrsnetzen eingesetzt. Als Übertragungsmedien kommen hier immer Lichtwellenleiter zum Einsatz. ◘ Tab. 12.3 stellt die Parameter der aktuellen Standards von Ethernet-Familie nBase-X dar.

12.2.2 10GbE, 40GbE, 100GbE (IEEE 802.3ae/an/ba/bg/bj/bm)

Die Hochleistungsnetze 10, 40, 100Gigabit-Ethernet gewinnen immer größere Bedeutung bei den bürotypischen LAN (Standard IEEE 802.3ae/an/ba/bg/bj/bm). Die charakteristischen Datenraten von 10-40-100 GBit/s werden meist über Multi- und Monomodelichtwellenleiter als Übertragungsmedien erzielt, jedoch gewinnen Lösungen mit Kupferkabeln an Bedeutung.

Als Kopplungsgeräte werden Layer2-Switches bzw. Switches mit MPLS- Funktionalität verwendet. Die wichtigsten Einsatzbereiche für 10GbE sind:

- Backbones in einem Unternehmens-LAN.
- Zugangsnetze (Last Mile/EFM) („Ethernet in the Last Mile“).
- Weitverkehrsnetze (über Synchronous Optical Networking, SONET bzw. Synchronous Digital Hierarchy, SDH).

Als Basis für 10GbE wird seit einigen Jahren die SONET/SDH-Infrastruktur (◘ Tab. 12.4) und eine Kodierung mit Zeit- und Wellenlängenmultiplex (TDM und WDM) genutzt [11, 16]. Bei SDH wird 8000 Mal pro Sekunde ein Frame gesendet. Die Übertragung von 10GbE-Frames über SONET/SDH-Infrastruktur erfolgt mit einem viel kleineren Overhead als bei ATM.

Tab. 12.3 Parameter der aktuellen Standards von Ethernet-Familie nBase-X [3, 4, 11]

Standard	Übertragungsrate und -Medium	Länge
100Base-TX (IEEE 802.3u)	100 Mbps, UTP, 2 Paare	100 m
100Base-T4	100 Mbps, UTP, 4 Paare	100 m
100Base-FX	100 Mbps, Optische Faser, multimode, 62,5/125 µm und 50/125 µm	412 m/2 km
1000Base-SX (IEEE 802.3z)	1 Gbps, Optische Faser, multimode 62,5/125 µm	260 m
1000Base-SX	1 Gbps, Optische Faser, multimode 50/125 µm	500 m
1000Base-LX	1 Gbps, Optische Faser, multimode 62,5/125 µm	400 m
1000Base-LX	1 Gbps, Optische Faser, multimode 50/125 µm	550 m
1000Base-LX	1 Gbps, Optische Faser, monomode, 9/126 µm	10 km
1000Base-CX	1 Gbps, Sonderkabel STP bzw. Koaxialkabel	25 m
1000Base-T (IEEE 802.3ab)	1 Gbps, UTP Kat 5, 4 Adern, Echokompensation	100 m

Tab. 12.4 Synchronous Digital Hierarchy [11]

SDH-Dienst	Framegröße (Byte)	Übertragungsrate, DR
STM-1	2430	155,52 MBit/s (ATM OC-3)
STM-4	9720	622,08 MBit/s (ATM OC-12)
STM-8	19.440	1244 MBit/s
STM-16	38.880	2488 MBit/s (ATM OC-48)
STM-64	155.520	9953 MBit/s (ATM OC-192)

Nahtlose Migrationsmöglichkeiten bietet (100-,40-,10-)GbE zur Ethernet-Familie (Eth, Fast Eth, GbE) durch Rückwärtskompatibilität (Frameformate, Switching im Vollduplex-Modus, …). Die Parameter der Ethernet-Familie 10GBase-X sind in Tab. 12.5 abgebildet.

Die aktuellen Netze von 40 Gigabit Ethernet (40GbE) und 100 Gigabit Ethernet (100GbE) wurden von den Entwicklungsgruppen definiert (IEEE 802.3ba-2010, 802.3bg-2011, 802.3bj-2014, 802.3bm-2015).

Da 40/100 Gigabit Ethernet eher die Zukunft für Büro- und Firmenvernetzung darstellen, diskutieren wir einige Details zum LAN-üblichen 10GbE, sowohl für Technologien mit Glasfaser- als auch mit Cu-Kabeln.

Für LAN gibt es im Nahbereich „10GbE"-Versionen über Kupferkabel, z. B. 10GBase-CX4 (IEEE 802.3an) mit dmax = 15 m bzw. zunehmend 10GBase-T mit dmax = 100 m.

Bei längeren Strecken werden grundsätzlich Glasfaserkabel eingesetzt. Grundsätzlich gibt es zwei Arten des physikalischen

Tab. 12.5 Parameter der Ethernet-Familie 10GBase-X [11]

Standard	Übertragungsmedien	Länge
10GBase-LX4 (IEEE 802.3ae)	Optische Faser, Multimode	300 m
10GBase-LW4	Optische Faser, Monomode	10 km
10GBase-SR	Optische Faser, Multimode	82 m (300 m)
10GBase-LR	Optische Faser, Monomode	10 km
10GBase-ER	Optische Faser, Monomode	40 km
10GBase-SW, LW, EW	Optische Faser, SDH STM-64	wie bei „R“
10GBase-CX4 (IEEE802.3an)	Kupferkabel	15 m
10GBase-T	TP Kat 6a, 4 Adernpaare, Echokompensation	100 m
40GBase-SR4	40 Gigabit Ethernet mit Glasfaser (Wellenlängen bei 850 nm)	100–150 m
40GBase-LR4	40 Gigabit Ethernet mit Glasfaser (Wellenlängen von 1270 nm, 1290 nm, 1310 nm und 1330 nm)	Bis zu 10 km
100GBASE-SR10/ 100GBASE-ER4, oft als Bündelung von 40 Gigabit Ethernet -Links	100 Gigabit Ethernet (100GbE), kompatibel mit 40 Gigabit Ethernet	Bis zu 40 km

Interfaces. Die LAN PHY-Implementierung ermöglicht typische Bitraten bis zu 10,000 GBit/s, während die WAN PHY-Implementierung mit Bitraten bis zu DR = 9,584640 GBit/s angeboten wird. Die WAN PHY – Subschicht ist optional und kompatibel zu TDM-Netzwerken SDH/SONET. Dadurch kann eine existierende Infrastruktur flexibel genutzt werden. Die Kapselung von Ethernet-Frames erfolgt in sog. SONET-Envelops. Der Wert 9,584640 GBit/s ist typisch für SONET/SDH und kompatibel zu ATM (Bündelung von 16 Kanälen mit je 622 MBit/s). Des Weiteren setzt 10GbE die folgenden wichtigen Konzepte ein [11, 16]:

1. DWDM, Dense Wave Division Multiplexing und WWDM, Wide Wave Division Multiplexing:
   - Unabhängige Informationsströme (Lichtimpulsfolgen) durch einen Lichtwellenleiter unter Nutzung mehrerer Wellenlängen/Frequenzen (eng gepackt mit ca. 100 GHz Abstand).
   - typischerweise Nutzung von Wellenlängen von 1530 nm bis 1560 nm
   - Technik für effiziente Übertragung mehrerer Wellenlängen (colors of light) von mehreren Laserquellen über einen LWL.
   - jede Laserquelle wird zum Senden von einer einzelner optischen Wellenlänge kalibriert, ebenso die zugehörige Empfänger-Laserdiode.

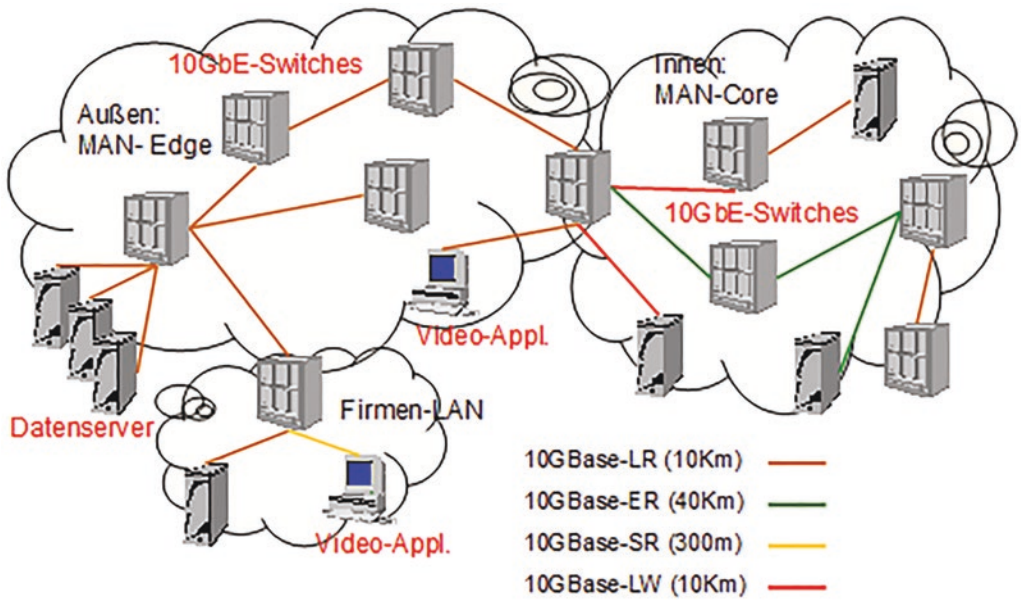
2. OC-192, Optical Carrier Level – X:
   - Bitrate von SONET – 9,584640 GBit/s (Bündelung von 16 Kanälen mit ATM OC12 → x16 ATM OC12 mit je 622 MBit/s).
3. PMD, Physical Media Dependent:
   - Teil von PHY, verantwortlich für Signalübertragung, Verstärkung, Modulation und Wave Shaping, Unterstützung verschiedener Übertragungsmedien.

In ◘ Abb. 12.8 ist ein Szenario für mehrere 10GbE-Einsätze zu sehen. Diverse Substandards 10GbE-ermöglichen flexible Netzwerkausdehnungen (d) zwischen 300 m und 40 km über optische Fasern, evtl. im Nahbereich über Kupferkabel, z. B.:

- 10GBase-LR (d = 10 km).
- 10GBase-ER (d = 40 km).
- 10GBase-SR (d = 300 m).
- 10GBase-LW (d = 10 km).

Vielfältige Dienste können angeboten werden: Videoapplikationen, Datenserver, VoIP etc.

In ◘ Tab. 12.6 werden 10Gigabit-Ethernet -Spezifikationen (Übertragungsmedien) und deren maximale Ausdehnungen (d) im Zusammenhang mit Frequenz (F) und Lichtwellenlänge (λ) betrachtet. Die diskutierten 10GbE-Substandards/PMDs sind: LR, ER, SR, LW, SW, EW, LX4.



◘ **Abb. 12.8** Ein Szenario mit 10GbE

Tab. 12.6 10Gigabit-Ethernet, Längen [11]

LWL	62,5 µm Multimode-LWL (MMF)		50 µm Multimode-LWL (MMF)			Mono mode-LWL
Faktor MHz * km	160	200	400	500	2000	–
SR/SW 850 nm serial	26 m	33 m	66 m	82 m	300 m	–
LR/LW 1310 nm serial	–	–	–	–	–	10 km
ER/EW 1550 nm serial	–	–	–	–	–	40 km
LX4 1310 nm WWDM	300 m, 500 MHz * km		240 m	300 m	–	10 km

MMF, Mono mode faser MMF – Multimode LWL
SMF, Single mode faser SMF – Monomode LWL

Unter dem Begriff „10GbE“ versteht man meist den Standard IEEE802.3ae. IEEE 802.3ae weist eine für das Ethernet optimierte Architektur auf. Die Architekturkomponente von Standard IEEE802.3ae repräsentiert Abb. 12.9.

Einige mögliche leistungsfähige Einsatzbeispiele sind:

- „letzte Meile“ (Last Mile) zur Nutzer-Anbindung an ein WAN.
- Anbindung der Server in einem Cluster oder in der privaten Cloud in Szenarien für das Verteilte Rechnen.
- Kopplung von LAN an Storage Area Networks (SAN) in Backupszenarien.

12.2.3 Standardisierungen in LAN durch IEEE 802 und ISO

Die Standardisierung wurde bereits in Teil I vorgestellt. An dieser Stelle wird die Einordnung der LAN-Technologien in Abb. 12.10 präzisiert. Einige der aufgeführten Standards (Token Ring, Token Bus) sind inzwischen veraltet. Weitere Standards sind u. a.: Wi-Fi 802.11 (Wireless Fidelity) oder Wireless LAN; 802.15 Bluetooth oder Pikonetze; 802.16 WiMAX (Worldwide Interoperability for Microwave Access) sowie 802.1q oder virtuelles LAN und 802.1p für die Priorisierung von „LAN-Datenströmen“, z. B. Sprache gegenüber Daten („Class of Service“).

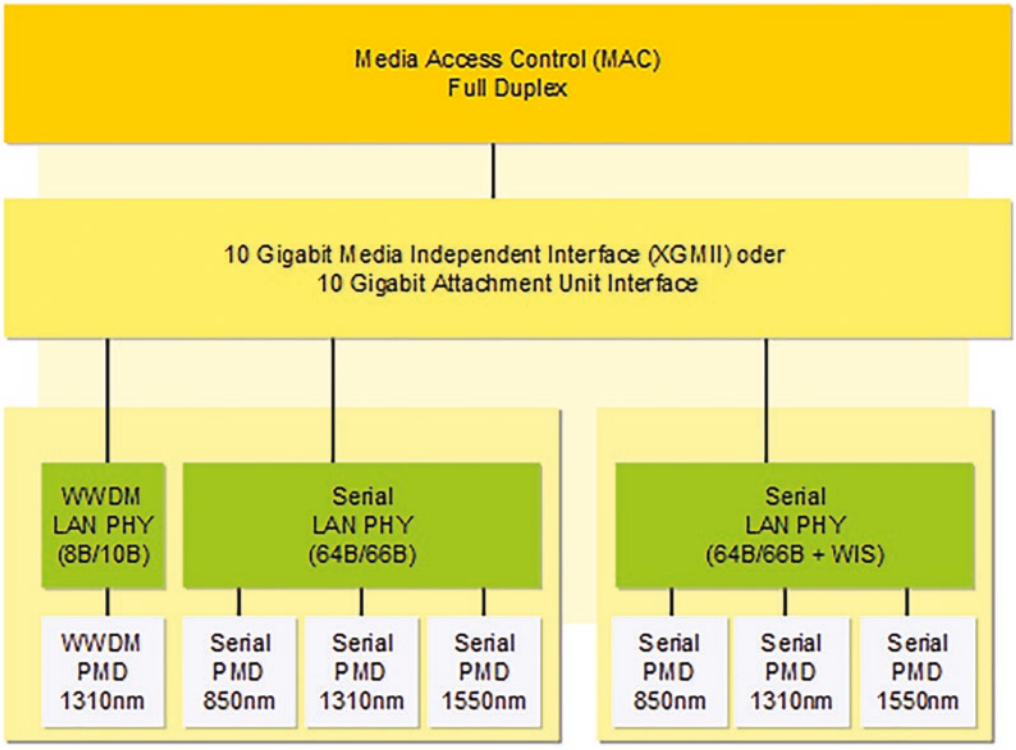


Abb. 12.9 Architekturkomponenten von IEEE802.3ae [11]

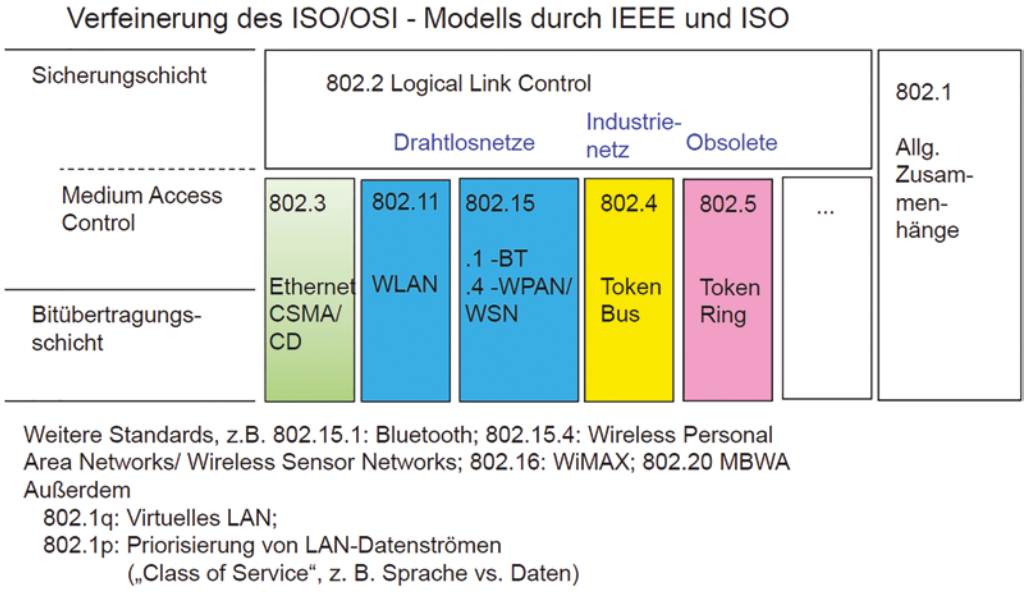


Abb. 12.10 Standardisierung zu LAN [11, 16]

Der Standard IEEE 802.3af ermöglicht die duale Nutzung von existierenden Cu-TP-Datenkabeln, zum einen als Basis eines Bürokommunikations-LAN, zu anderen für die Gerätestromversorgung. Diese Technologie wird Power over Ethernet genannt (s. ► Abschn. 4.6).

12.3 Drahtlose lokale Netze IEEE802.11 – WLAN

12.3.1 Normenübersicht IEEE 802.11. Aktuelle Standards

In ◘ Tab. 12.7 sind technische Charakteristiken von IEEE 802.11-Netzen aufgeführt [10, 13, 16, 17].

Herkömmliche drahtlose Netze Wi-Fi 802.11 b,a,g verwenden adaptive Multiplex-, Modulations- und Bandspreizverfahren. Der konsequente Einsatz von OFDM bei Wi-Fi seit dem Jahr 2000 brachte bedeutsame Datenratenerhöhungen durch eine

◘ **Tab. 12.7** Technische Charakteristiken von aktuellen Wi-Fi (IEEE802.11)-Netzen [11]

Standard	Frequenzband	Datenrate	Layer 2	Kompatibilität
802.11	2,4 GHz	2 MBit/s	FHSS/DSSS	Obsolete
802.11 a	5 GHz	54 MBit/s	OFDM	Keine internationale Anerkennung, z. T. inkompatibel durch nationale Restriktionen
802.11 b	2,4 GHz	11 MBit/s	Hauptsächlich DSSS	802.11
802.11 g	2,4 GHz	54 MBit/s	Hauptsächlich OFDM	802.11/802.11b
802.11 n	2,4 GHz (evtl. 5 GHz)	350 … 600 MBit/s	OFDM, OFDMA, MIMO-Technik	802.11/802.11b (evtl. 802.11a)
802.11 ac, auch Wi-Fi 5	5 GHz	1,3–6,93 Gbit/s	Verbesserte MIMO-2D-Strukturen	Kompatibel zu .11n
802.11 ad	60 GHz (Mikrowellenbereich)	DR = 7 GBit/s	MIMO-3D-Strukturen	Kompatibel zu .11n
802.11 ah	900 MHz, Wi-Fi HaLow	Unter 1 Gbit/s	Energieeffizient, größere Reichweite, wenig Abschattung	u. U. Interferenz zu GSM900
802.11 ax, auch Wi-Fi 6	2,4 und 5 GHz, auch für weitere ISM-Bänder im Bereich 1–6 GHz konzipiert	11 Gbit/s	Effiziente Codierung, OFDMA, MIMO-3D-Strukturen, erhöhte Datensicherheit durch WPA3	Kompatibel zu .11ac (Wi-Fi 5)

optimierte Spektraleffizienz (Verhältnis der Datenrate zur Kanalbandbreite). Nachfolgende Tabelle zeigt den Zusammenhang von Frequenzband, Modulation und Bandspreizverfahren genauer (◘ Tab. 12.8).

Eine weiterführende Normenübersicht für drahtlose lokale Netze IEEE802.11 ist in ◘ Tab. 12.9. dargestellt.

12.3.2 Basistandard IEEE 802.11n

2010 erfolgte die Verabschiedung des Basisstandards 802.11n. Der Standard gilt als wesentliche Optimierung von 802.11, 802.11a und 802.11g. Die neusten Standards 802.11ac (Wi-Fi 5, 2016) und 11ax (Wi-Fi 6, 2019) sind Weiterentwicklungen des Basisstandards 11n, die bessere QoS sowie Datensicherheit garantieren können ggf. per WPA3.

Vermerk

WPA1,2,3 (Wi-Fi Protected Access) sind die nacheinanderfolgenden Spezifikationen für die Verschlüsselung in drahtlosen lokalen Netze (WLAN). WPA1,2,3 bilden i. W. die Grundlage für den WLAN-Sicherheitsstandard IEEE 802.11i. Nachdem sich die Wired Equivalent Privacy (WEP) als unsicher erwiesen hatte, wurde der Begriff WPA als Pseudostandard etabliert. Die Nachfolger des WPA sind die fortgeschrittenen Verfahren WPA2 und WPA3 (2019).

Die Die Datenraten stiegen von 54 MBit/s bis auf 300 und später 600 MBit/s. Gleichzeitig bietet der Standard leicht höhere Reichweiten für hohe Bitraten. Die wichtigsten technischen Merkmale von IEEE 802.11n sind:

- Frame Aggregation.
- Packet Bursting.
- MIMO/Raummultiplex.

Dabei funktionieren 802.11n-Geräte in den Frequenzbändern F = 2,4 GHz und F = 5 GHz mittels OFDMA und adaptiver Modulation mit BPSK, QPSK, 16QAM, 64QAM. Die maximalen Bruttodatenraten lagen anfangs bei 300 und liegen derzeit bei DR = 600 MBit/s bei Reichweiten von 70 m innerhalb und 250 m außerhalb von Gebäuden.

Zu einem liegt diese Datenratenerhöhung an der Frame Aggregation Methode. MAC- Datenframes werden dabei zusammengefasst (Aggregate) und mit einem gemeinsamen PHY-Header versehen. Eine Block-ACK quittiert alle aggregierten Datenframes. Dadurch wird der Overhead signifikant verringert. Die Methode liefert bis zu 40 % Effizienzsteigerung gegenüber bisherigen Modi (◘ Abb. 12.11). Die Methode ist nur bei

Tab. 12.8 IEEE 802.11 b,a,g: Zusammenhang „Frequenzband, Modulation und Bandspreizverfahren“ [11]

Band-spreizverfahren	DSSS		CCK		OFDM								Frequenz
Modulation	DBPSK	DQPSK	DQPSK		BPSK		QPSK		16QAM		64QAM		
Datenrate (MBit/s)	1	2	5,5	11	6	9	12	18	24	36	48	54	
802.11a					x	x	x	x	x	x	x	x	5 GHz
802.11b	x	x	x	x									2,4 GHz
802.11g	x	x	x	x	x	x	x	x	x	x	x	x	

DSSS: Direct Sequence Spread Spectrum
OFDM: Orthogonal Frequency Spread Spectrum
DBPSK: Differential Binary Phase Shift Keying
DQPSK: Differential Quadrature Shift Keying
BPSK: Binary Phase Shift Keying
QPSK: Quadrature Phase Shift Keying
CCK: Complementary Code Keying
16QAM: 16 Point Quadrature Amplitude Modulation
64QAM: 64 Point Quadrature Amplitude Modulation

Tab. 12.9 Auszüge zur weiteren Normen für drahtlose lokale Netze IEEE802.11 [11]

Standard	Kurze Beschreibung
802.11i	Substandard (2004) für Datensicherheit bei WLAN (AES-Verschlüsselung und RSA-Authentisierung) basierend auf WPA/WPA2 (erweiterte Sicherheitsmechanismen)
802.11j	Erweiterungen von 802.11a für japanischen Markt (2004)
802.11n	Weiterentwicklung seit 2006 von 802.11 und 802.11g; 2009 evtl. von 802.11a; Frequenzband F = 2,4 und 5 GHz; die maximalen Bruttodatenraten liegen bei DR = 600 MBit/s; Einsatz mehrerer Sende- und Empfangsantennen nach dem MIMO-Verfahren (Multiple Input Multiple Output) seit November 2009
802.11o	Soll die Priorisierung von Sprache im WLAN gegenüber dem Datenverkehr definieren
802.11p	Erweiterung zu 802.11a für den Einsatz in Fahrzeug-zu-Fahrzeug-Netzen (WAVE – Wireless Access for the Vehicular Environment, voraussichtlich 2009)
802.11r	Fast Roaming beim Wechsel zwischen Access Points
802.11s	ESS (Extended Service Set) for Mesh Networking (voraussichtlich 2009)
802.11u	Interoperabilität mit anderen, nicht 802-konformen Netzen
WPA/WPA2/WPA3	WiFi Protected Access; Ursprünge für 802.11i

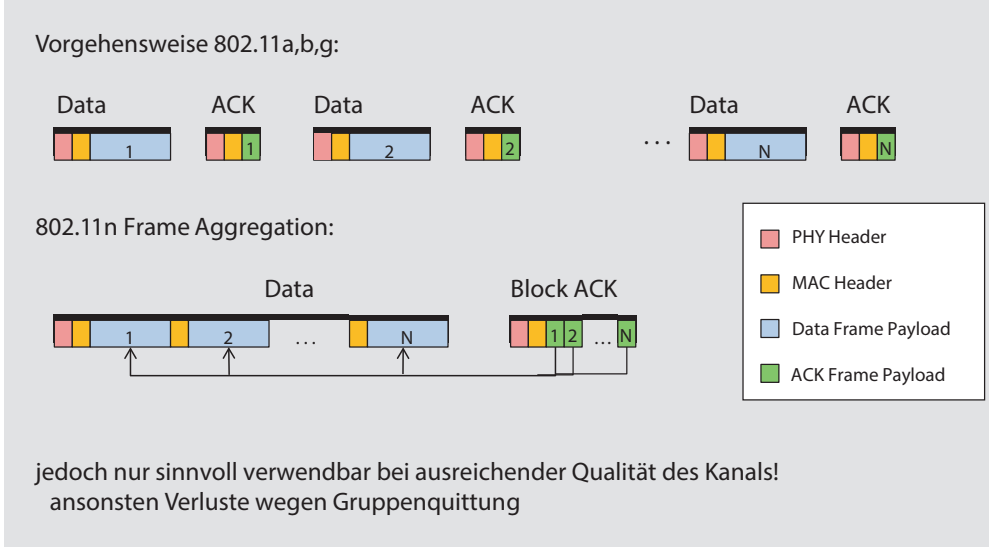


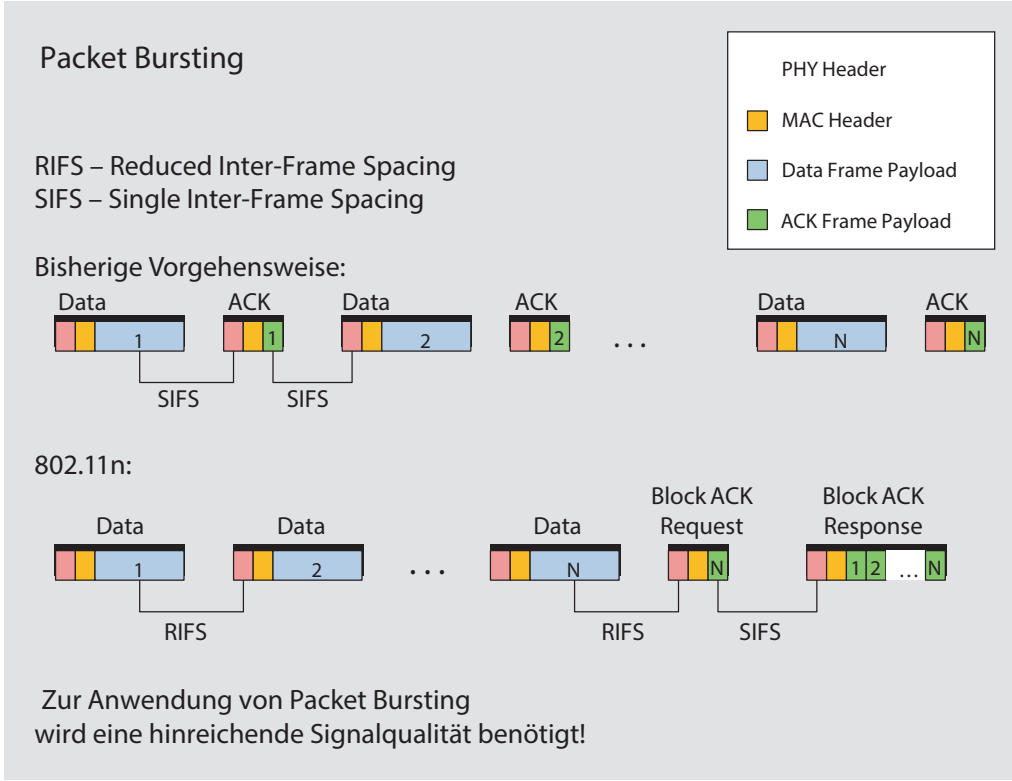
Abb. 12.11 Frame Aggregation bei IEEE 802.11n

ausreichender Qualität des Kanals sinnvoll verwendbar. Ansonsten kann die bisherige Vorgehensweise wie bei 802.11a,b,g weiter genutzt werden.

Weiterhin wurde das beschleunigte Framesenden (Packet Bursting Methode) bei IEEE 802.11n zur Datenratenerhöhung

eingesetzt (◘ Abb. 12.12). Zur Anwendung des Packet Bursting wird eine hinreichende Signalqualität benötigt. Um Kollisionen zu vermeiden, wurden anstelle der SIFS (Single Inter-Frame Spacing) reduzierte Wartezeiten (RIFS, Reduced Inter-Frame Spacing) für das burstartige Senden eingeführt, was die Ruhe-Phasen bei der Übertragung im Vergleich zu der bisherigen Vorgehensweise bei 802.11a,b,g deutlich reduziert.

Des Weiteren wird eine rasante Datenratenerhöhung durch den Einsatz mehrerer Sende- und Empfangsantennen erreicht, die nach dem MIMO-Verfahren (Multiple Input Multiple Output) arbeiten (◘ Abb. 12.13). MIMO verwirklicht räumliches Multiplexing (Raummultiplex, oder SDM, Spatial Division Multiplexing). Im Gegensatz zu SISO-Antennenkonfigurationen (Single Input Single Output) werden bei MIMO mehrere Datenströme mit unterschiedlicher Richtcharakteristik übertragen. Der ursprüngliche Datenstrom wird zuerst in mehrere Teilströme zerlegt (Sender Tx); diese werden dann parallel über mehrere Richtantennen auf der gleichen Frequenz übertragen. Der Empfänger (Rx) kann die Einzelströme erkennen und setzt sie wieder zusammen. Die Anzahl der parallel übertragbaren



◘ **Abb. 12.12** Packet Bursting bei IEEE 802.11n

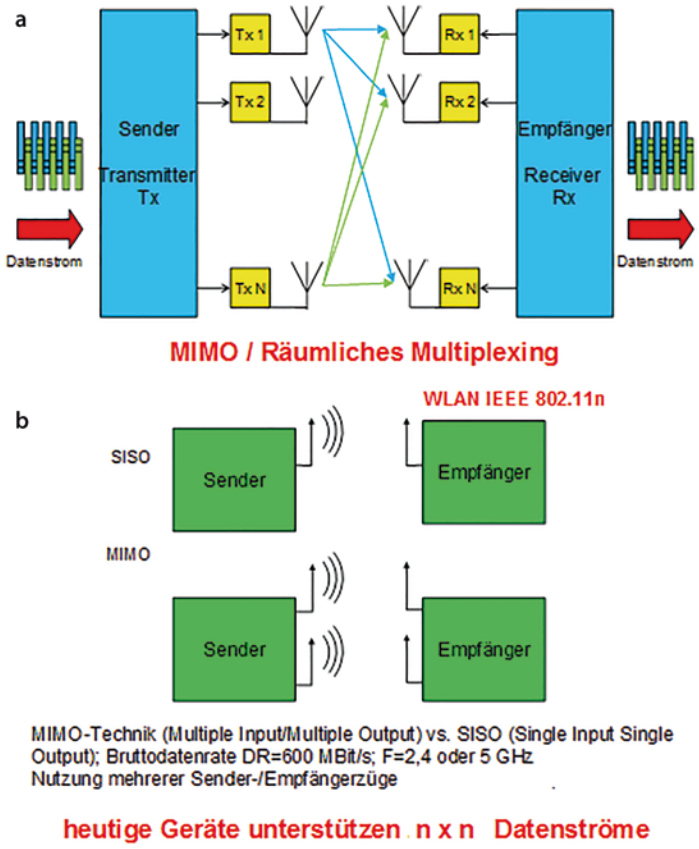


Abb. 12.13 Einsatz der MIMO-Technik bei IEEE 802.11n

Datenströme ist von der Leistung der Sende-/Empfangseinheiten abhängig. Im Standard IEEE 802.11n werden bis zu 4 Datenströme definiert (MIMO-Streams).

MIMO funktioniert bei direkter Sichtverbindung nur bedingt: bei 2 Antennen ist unterschiedliche Polarisation möglich, Senden in mehreren Ausbreitungsrichtungen ist mangels Reflexionen nicht möglich.

Die deutliche Datenratenerhöhung beruht auf der Kombination fortgeschrittener Methoden (Abb. 12.14). Durch gleichzeitigen Einsatz der Techniken von MIMO, Frame Aggregation und Packet Bursting werden die Daten in 802.11n-WLAN-Geräten mit minimiertem Overhead nebenläufig und sehr effizient übertragen. Weitere Erhöhung von Datenraten erzielt man durch das Channel Bonding und Short Guard Interval.

Der Standard IEEE 802.11n sieht die Verwendung von je 40 MHz -Kanälen vor (→ zwei 20 MHz Kanäle zusammengefasst) in den beiden Frequenzbändern 2,4 und 5,0 GHz (s. Verteilung in Abb. 12.15). Jedoch nur bei 5 GHz ist es sinnvoll anwendbar

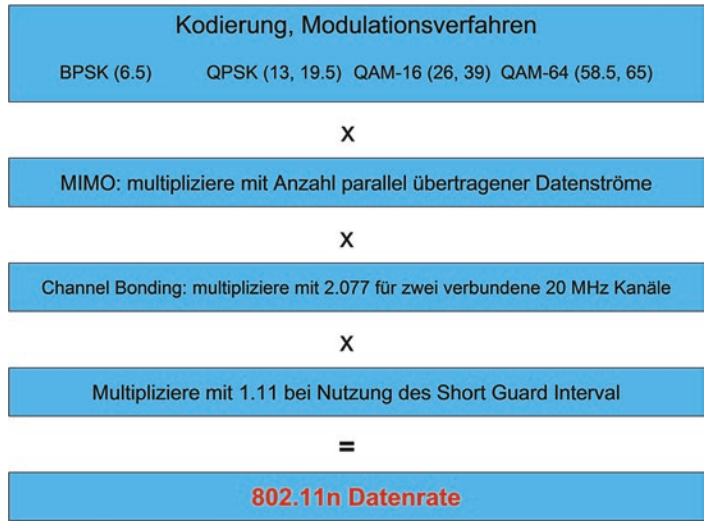
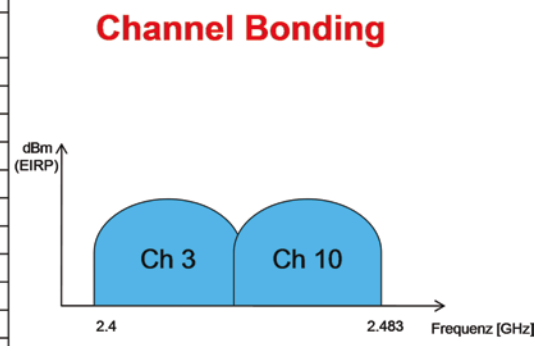


Abb. 12.14 Quellen der Erhöhung von Datenraten bei 802.11n

2.4 GHz Spektrum	
Kanal-nummer	Kanal [GHz]
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462

5 GHz Spektrum			
Kanal-nummer	Kanal [GHz]	Kanal-nummer	Kanal [GHz]
34	5.170	108	5.540
36	5.180	112	5.560
38	5.190	116	5.580
40	5.200	120	5.600
42	5.210	124	5.620
44	5.220	128	5.640
46	5.230	132	5.660
48	5.240	136	5.680
52	5.260	140	5.700
56	5.280	149	5.745
60	5.300	153	5.765
64	5.320	157	5.785
100	5.500	161	5.805
104	5.520	165	5.825



EIRP: Equivalent Isotropic Radiated Power

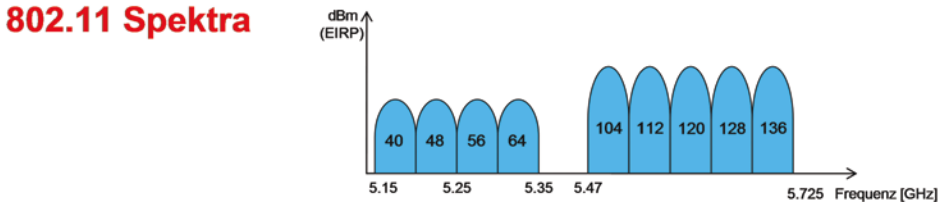


Abb. 12.15 Channel Bonding

(2,4 GHz → 3 überlappungsfreie Kanäle; 5 GHz → 24 überlappungsfreie Kanäle). Das „neighborhood-friendly" Channel Bonding Verfahren wird nur aktiviert, wenn keine zu starken Interferenzen durch benachbarte Netze vorliegen.

Die folgenden optimierten 802.11-Datenraten werden durch Channel Bonding und Short Guard Interval in der Spezifikation 2009 vorgesehen (◘ Abb. 12.16).

Die sog. Guard Intervalle werden generell in der Nachrichtentechnik eingesetzt, um die Interferenzen bei digitaler Übertragung zu verhindern [11, 16]. Der Einsatz des *Short Guard Interval* an dieser Stelle stellt in sich einen gewissen Kompromiss dar, damit sich bestimmte Übertragungen nicht deutlich vermischen und durch diese erhöhte Störfestigkeiten gegenüber Ausbreitungsverzögerungen, Echos etc. erhöhte Datenraten erzielt werden können.

12.3.3 Projektierung und Optimierung von WLAN

Merkmale Drahtgebundene und drahtlose LAN haben grundlegende Unterschiede hinsichtlich Planungsaufwand, Robustheit, Komplexität der Endgeräte, Übertragungsraten und Routingprozesse, Betriebsart, Verwaltung, Frequenzen, Fähigkeiten der Endgeräte, Dienste, nationale/internationale Regulierungen (s. ◘ Tab. 12.10).

1 Datenstrom			2 Datenströme			3 Datenströme			4 Datenströme		
Basis-datenrate	Mit Channel bond.	Mit Short Guard Interval	Basis-datenrate	Mit Channel bond.	Mit Short Guard Interval	Basis-datenrate	Mit Channel bond.	Mit Short Guard Interval	Basis-datenrate	Mit Channel bond.	Mit Short Guard Interval
6.5	13.5	15	13	27	30	19.5	40.5	45	26	54	60
13	27	30	26	54	60	39	81	90	52	108	120
19.5	40.5	45	39	81	90	58.5	121.5	135	78	162	180
26	54	60	52	108	120	78	162	180	104	216	240
39	81	90	78	162	180	117	243	270	156	324	360
52	108	120	104	216	240	156	324	360	208	432	480
58.5	121.5	135	117	243	270	175.5	264.5	405	234	486	540
65	135	150	130	270	300	195	405	450	260	540	600

◘ **Abb. 12.16** Datenraten bei IEEE 802.11n

Tab. 12.10 Vergleich: drahtgebundene vs. drahtlose LANs [16]

Merkmal	Drahtgebundene LANs	Drahtlose LANs
Betriebsart	Nur Infrastrukturmodus	Infrastruktur- und Ad-hoc Betrieb möglich
Verwaltung	Planung, aufwendige Kabelverlegung	Keine Kabelverlegung, im Ad-hoc Modus auch keine Planung
Frequenzen	Kabelgebunden: TP Kat. 5 – 7. LWL	Funk: 2,4 GHz, 5 GHz
Fähigkeiten der Endgeräte	Gerätegröße wird durch notwendige Kabelverbindung festgelegt, keine Mobilität	Mobilgeräte möglich (Smartphones, RFID-Tags oder Radio Frequency ID Tags), Endgeräte komplexer, wenn ad hoc Modus unterstützt wird
Dienstgüte	Bandbreite bei drahtgebundenen LANs um Größenordnungen höher, Übertragungsfehlerrate bei drahtlosen LANs ebenfalls um Größenordnungen besser (Bitfehlerrrate 10^{-9} statt 10^{-14})	
nationale/Internationale Regulierung	Keine Regulierung notwendig, Standardisierte Technologie erhöht jedoch Interoperabilität	Nationale/internationale Regulierung aufgrund der bereits vollständig belegten Funkfrequenzen notwendig, i. d. R. langwieriger Prozess, deshalb Nutzung des lizenzfreien ISM-Bands (Industrial, Scientific and Medical), deshalb Einschränkung des Frequenzbereichs und der Sendeleistung

Wi-Fi-Netze/WLAN werden in zwei folgenden Modi verwendet:

- Ad-hoc -Netze (spontane drahtlose Netze).
- Infrastrukturerweiterung als LAN-Zugang und anhand der Zellularstrukturen (s. Abb. 12.17).

Für Ad-hoc Netzwerke ist keinerlei Infrastruktur notwendig. Wenn sich Endgeräte im gegenseitigen Übertragungsbereich befinden, können sie direkt kommunizieren, bzw. zwischen weiteren Endgeräten Daten weiterleiten. Ad-hoc Strukturen weisen hohe Flexibilität auf, da keinerlei Planung und Infrastruktur notwendig ist. Dafür sind die Endgeräte komplexer, weil Medienzugriff, Dienstgüte und Vermittlung in den Endgeräten realisiert werden müssen. Die Verwendung von Ad-hoc Strukturen nutzt den sog. Beaconing Access zwischen den mobilen Knoten. Ad-hoc-Strukturen werden im Rahmen dieses Buches nicht weiter betrachtet.

Von größerem praktischem Interesse ist die Modellierung von Ausleuchtungen für die einzelnen AP (Access Points) als Zugangspunkte zu einem LAN oder von Zellularstrukturen mit einem bestimmten Aufbau- und Frequenzmehrfachnutzungsmuster (Cluster). Durch sog. Clustering werden geographische Bereiche in zellularen Funknetzen in Funkzellen mit unterschiedlichen Frequenzbändern strukturiert. Bezeichnet man

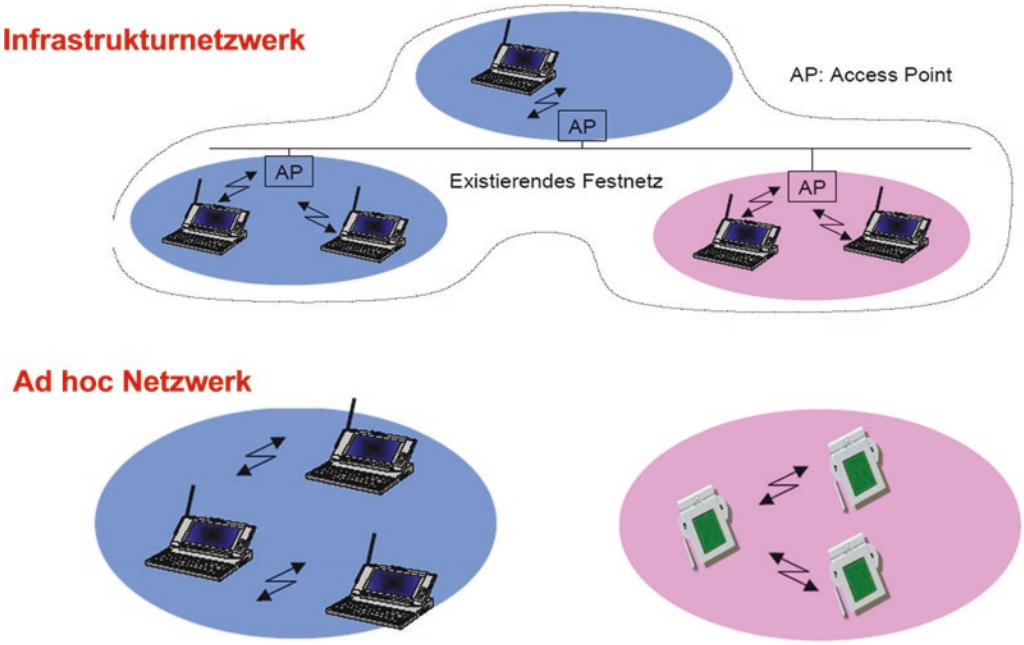


Abb. 12.17 Infrastruktur- vs. Ad-hoc Netzwerke

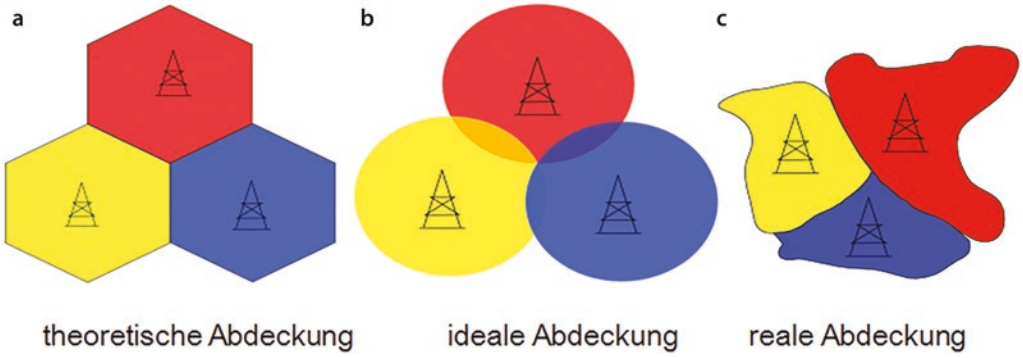


Abb. 12.18 Abdeckung in Zellularstrukturen

mit D den Abstand zweier Basisstationen mit derselben Sendefrequenz, R den Zellradius und k die Clustergröße, gilt i. d. R. folgender Zusammenhang:

$$D = R \cdot \sqrt{3 \cdot k} \tag{12.1}$$

Geometrische Modelle zum Flächendecken in einem zellularen WLAN sehen etwa so aus, wie es in Abb. 12.18 zu entnehmen ist.

Basisprobleme Die folgenden Probleme ergeben sich beim Einsatz drahtloser Netze:

- Optimale Standorte von Access Points sind nicht einfach berechenbar.
- Das zeit- und frequenzabhängige Auftreten von Dämpfung, Abschattung, Reflexion, Brechung, Streuung, Beugung bzw. eine Überlagerung dieser Effekte ist zu berücksichtigen.

Die exakte Stärke des Signals in drahtlosen Netzen für beliebige Empfangspunkte kann nur näherungsweise vorherberechnet werden. Die Vorausberechnung der Signalfeldstärken ist nur mittels Modellierungstechniken realisierbar. Jedoch sind zusätzliche Messungen vor Ort während der Installation unbedingt wahrzunehmen.

Die Zellularstrukturen werden hauptsächlich im Modus Outdoor verwendet. Für Grundrisse mit großer Fläche bzw. in Großhallen werden auch Indoor-WLAN-Zellen eingesetzt. Für eine Zellstruktur nach Wi-Fi (IEEE 802.11) mit N_{AP} Zugangspunkten werden die folgenden Kenngrößen und QoS-Parameter ermittelt oder modelliert:

- Aufstellung der $AP_i, i = 1, \ldots N_{ap}$ auf dem ganzen Geländegrundriss oder in spezifizierten Empfangszonen (Zugangsgebiete).
- Zulässige Useranzahl N, Nutzungsprofil und Lastverteilung zwischen AP.
- 2D-Zellen-, Gebäude-/Geländegeometrie und Abdeckungsfläche.
- Verfügbare Datenrate DR.
- Installations- und Wartungskosten für projektierte Lösung K.

Gleichzeitig wird die Problematik der Frequenzverteilung und der Zugangsgebiete (Access Areas) berücksichtigt (3D-Fall). In Spezialfällen kann auch die Antennenhöhe und das Umgebungsprofil (Punktehöhen auf der digitalen geografischen Karte) bei der Projektierung von Wi-Fi (IEEE 802.11) berücksichtigt werden. Präzisere Koordinaten können per GPS [10, 11, 16, 19] ermittelt werden.

Antennen Die folgenden Antennentypen werden bei Wi-Fi/WLAN eingesetzt (◘ Tab. 12.11).

Die ◘ Abb. 12.19a zeigt eine Antennencharakteristik für einen Rundstrahler, ◘ Abb. 12.19b charakterisiert eine Sektorantenne und ◘ Abb. 12.19c eine Richtantenne(Planarantenne).

Der Einsatz von Antennen für WLAN-Indoor kann folgendermaßen aussehen (◘ Abb. 12.20).

Tab. 12.11 Einsatz diverser Antennentypen im WLAN [11]

Einsatz	Rundstrahler	Sektorantenne	Richtantenne
Wohnungen, Privathäuser	+++	+	–
Hörsäle, Konferenzsäle	+++	+	–
Kleine Räumlichkeiten	+++	++	–
Bahnhöfe, Flughäfen	++	+++	–
Büros	+++	++	–
Flure in den Gebäuden	–	+++	++
Höfe, gekurvte Gebäudegrundrisse	+	+++	–
Städtischer Bebau (Street Canyon)	–	+++	++
Line-of-sight (LOS)	–	–	+++

Frequenzverteilung für die Zellularstrukturen IEEE 802.11 Eines der wichtigsten Projektierungsprobleme bei mobilen und drahtlosen Netzen ist die Raumaufteilung (Raummultiplex). Raummultiplex ermöglicht flächendeckende Mehrfachnutzung von Frequenzen in Zellularstrukturen (Cell Reuse Pattern/ Coverage) bei raren Frequenzressourcen.

Eine Zellularstruktur (Cluster) eines Funknetzwerkes besitzt eine Anzahl $N_{cluster}$ unterschiedlicher Frequenzen.

Ein solcher Cluster (Abb. 12.21) kann elliptische oder Kreisform besitzen in Abhängigkeit von den (i,j) –Indices bei dessen Rundgang (Cluster-Roundtrip). Die Zellen werden durch natürliche Zahlen durchnummeriert (1, 2, 3,… $N_{cluster}$). Bei $(i = j)$ hat der Cluster eine runde Form (die sektorenförmige Abdeckung passt in den Umkreis). Auf der Basis des D/R – Verhältnisses wird für einen Cluster mit $N_{cluster}$ Zellen der Sicherheitsabstand D berechnet, ab dem Signalinterferenzen für dieselben Frequenzen von verschiedenen Zellen ignoriert werden können:

$$D = \begin{cases} R \cdot \sqrt{i^2 + ij + j^2}, & i \neq j \\ R \cdot \sqrt{3N_{cluster}}, & i = j = N_{cluster} \end{cases} \tag{12.2}$$

Dabei sind R – effektiver Umkreisradius bei Nutzung von 6-Sektorantennen, (i,j)– Indexen für den Clusterrundgang. Der Summand $(i \cdot j)$ versteht sich als „gegenseitiger Einfluss" von Zellen im Cluster.

Mehrere Frequenzplanungsbeispiele zeigt Abb. 12.22. Die Frequenzzuweisung $\{1, 2, \ldots k, \ldots N_{cluster}\}$ zu den Zellen wird durch Färbung illustriert. Die Anzahl unterschiedlicher Frequenzen variiert dabei von drei bis zwölf. Wenn ein Cluster

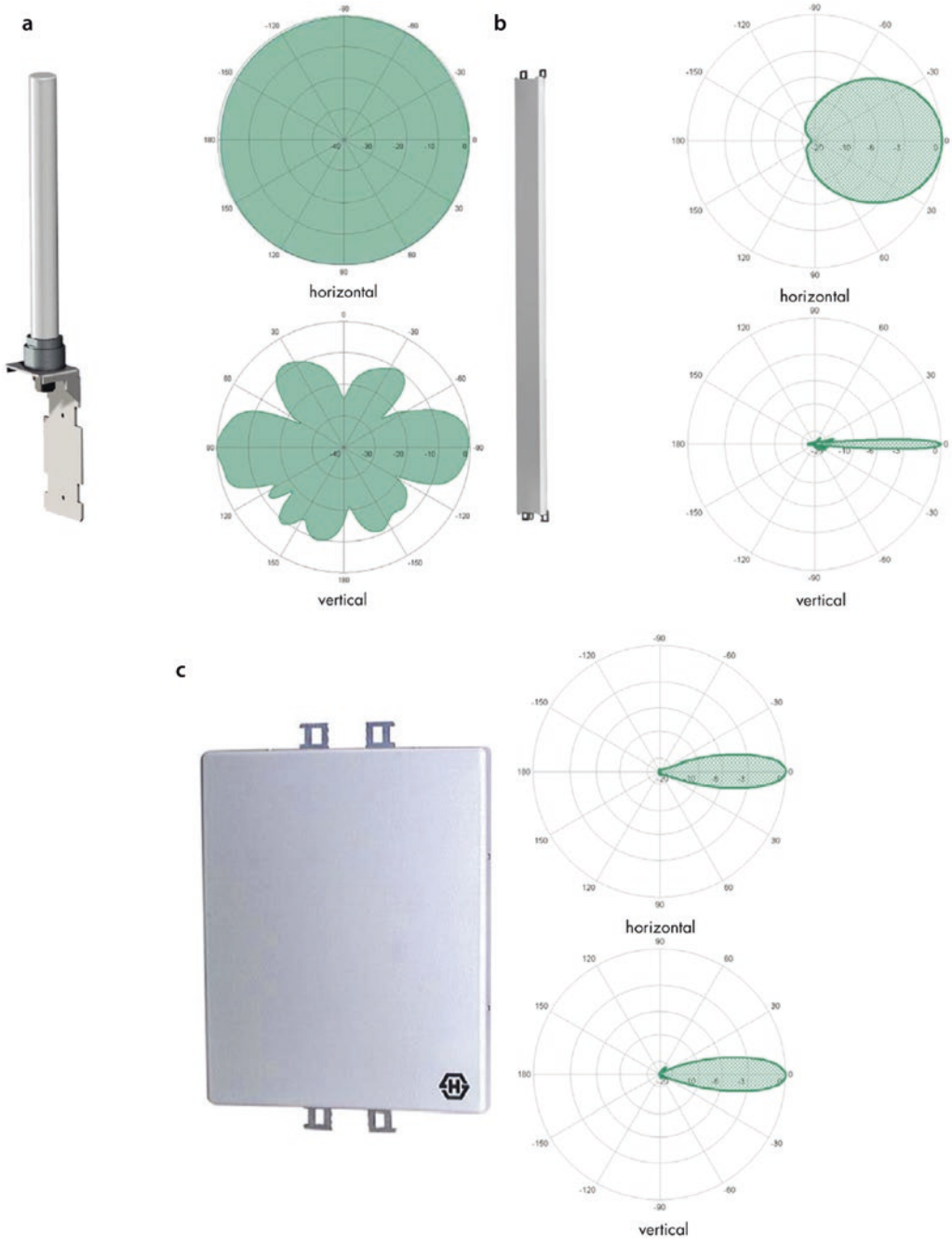


Abb. 12.19 Antennenbeispiele (Firma Huber + Suhner: ► http://www.hubersuhner.com)

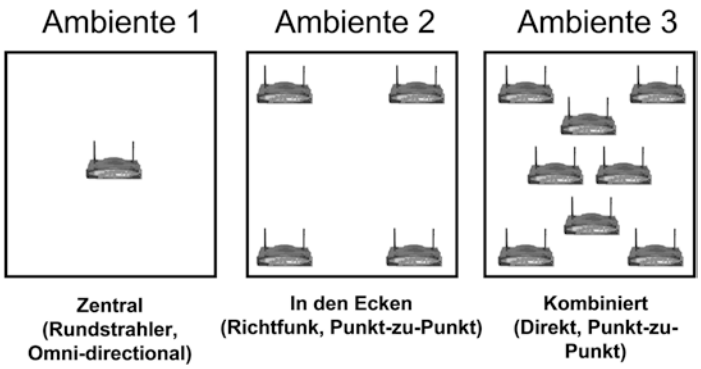
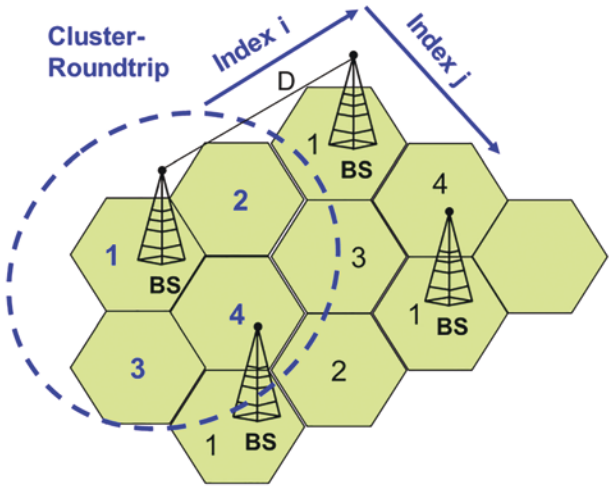


Abb. 12.20 Antenneneinsatzbeispiele für WLAN-Indoor



Verhältnis «D/R»	Zellenanzahl (Kreis) $N_{cluster}$
3,46	4
4,6	7
6	12
7,55	19
3	3

Abb. 12.21 Raummultiplex (cell reuse pattern) in Zellularstrukturen

mehr Zellen als Frequenzen besitzt, wird das Muster nach einem Sicherheitsabstand D wiederholt. Die Sendeleistung der Zellen muss so gering sein, dass die Zellen im Abstand D nicht wesentlich durch Interferenz gestört werden.

In Abb. 12.23 sind einige Beispiele einer sinnvollen Frequenzverteilung für IEEE 802.11 – Netze aufgeführt.

Modulationstypen, Datenraten und QoS-Parameter Zu den Kenngrößen von QoS (Quality of Service), die bei WLAN von Bedeutung sind, gehören die folgenden Metriken:

- *SE* – Spektraleffizienz nach Nyquist (Spectrum Efficiency, [bit/s/Hz]).
- *DR* – Datenrate.
- PR_x, S – Signalqualität (Empfangfeldstärke oder Sensibilität).

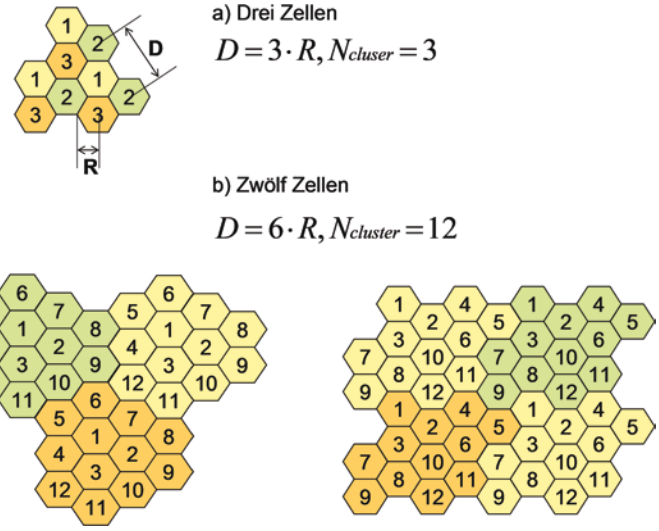


Abb. 12.22 Beispiele verschiedener Funkzellencluster für Funknetze

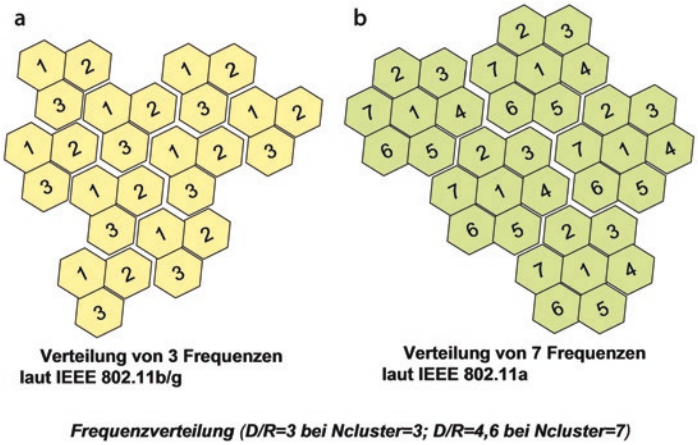


Abb. 12.23 Frequenzverteilung bei IEEE 802.11-Substandards

- *SNR* – Signal-zu-Rausch-Abstand (Signal-Noise-Ratio).
- *C/I&N* – Träger-Interference-Rausch-Abstand (Carrier to Interference & Noise Power Ratio).
- *R* – Reichweite (max. zulässige Distanz).

Die erwähnten Parameter werden durch den Modulationstyp beeinflusst.

Die Wi-Fi-Systeme nutzen die folgenden Modulationsmethoden: BPSK – Binary Phase Shift Keying, QPSK – Quadrature Phase Shift Keying, 16QAM – Quadrature Amplitude Modulation (4Bit-16Symbol-Mapping), 64QAM – Quadrature Amplitude Modulation (6Bit-64Symbol-Mapping).

Die Modulationsart QAM repräsentiert eine Kombination von Phasen- und Amplitudenmodulation. Mit einer Erhöhung des Informationsgehaltes bei der Signalkodierung (Bit/Signal) steigt auch die Spektraleffizienz, sowie SNR und Reichweite werden optimiert (◘ Abb. 12.24a und b).

Spektraleffizienz Die Spektraleffizienz nach Nyquist *SE* (Spectrum Efficiency) wird in [bit/s/Hz] gemessen und charakterisiert, wie gut die verfügbare Bandbreite durch bestimmte Netzwerkstechnologien für die Datenübertragung ausgenutzt wird.

Von besonderer Bedeutung wird diese Größe bei den Funknetzen (UMTS, HSDPA, LTE, WLAN, WiMAX etc.), da es um effiziente Nutzung der raren und preisintensiven Ressource Frequenzbandbreite geht. Aus der Informationstheorie sind die Theoreme von Nyquist-Shannon-Kotelnikow (rauschfreier Kanal) und Shannon-Hartley (SNR-Abstand-Theorem) bekannt:

$$DR = \begin{cases} 2B \cdot \log_2 S, \\ B \cdot \log_2 (1 + SNR), \end{cases} \tag{12.3}$$

wobei *DR* die Datenrate [Bit/s], *B* die Bandbreite [Hz], *SNR* das Signal-Rausch-Verhältnis (Signal-to-Noise-Ratio) und S die Anzahl der Darstellungsformen (Stufen) eines Signals sind. $\log_2 S$ beschreibt dann die Anzahl der Informationsbits eines Kodierungssymbols (s. ◘ Abb. 12.25). Für jede Technologie begrenzt eine der Formeln von (▶ Gl. 12.3) die spektrale Effizienz SE = DR/B:

$$SE = \begin{cases} 2 \cdot \log_2 S & = const_1 \\ \log_2(1 + SNR) & = const_2, \end{cases} \tag{12.4}$$

$$\rightarrow$$

$$SE = \frac{DR}{B} = min(const_1, const_2)$$
$$= \varphi(Multiplex, Modulation, Codierung, SNR)$$

Die Spektraleffizienz wird demnach durch Multiplex- und Signalkodierungsverfahren, sowie durch das SNR bestimmt.

Beispiele:

Für Übertragungen mit Modems in (hochwertigen) analogen Telefonnetzen ergibt sich:

$$DR = 56\,\text{kBit/s},\ B = 4\,\text{kHz} \Rightarrow SE = 14\frac{\text{Bit/s}}{\text{Hz}} \tag{12.5}$$

a

Modulations-verfahren	BPSK	QPSK	8PSK	16QAM	64QAM
Anzahl Bit pro Signalschritt-Symbol (pro Baud)	1	2	3	4	6
Störsicherheit	hoch				gering
SNR (Signal-2-Noise-Ratio), dB	6	12	18	24	> 24
Bereich, Zellgröße	groß				klein

Legende:

- PSK – Phasenumtastung, engl. Phase Shift Keying
- BPSK – Binary PSK, QPSK – Quadrature PSK(Quadraturphasenumtastung)
- QAM – Quadraturamplitudenmodulation, eine fortgeschr. Kombination von PM und AM
- 16QAM – Quadrature Amplitude Modulation (mit Abbildung von 4Bit und 16 Symbolen)
- 64QAM – Quadrature Amplitude Modulation (mit Abbildung von 6Bit und 64 Symbolen)

b

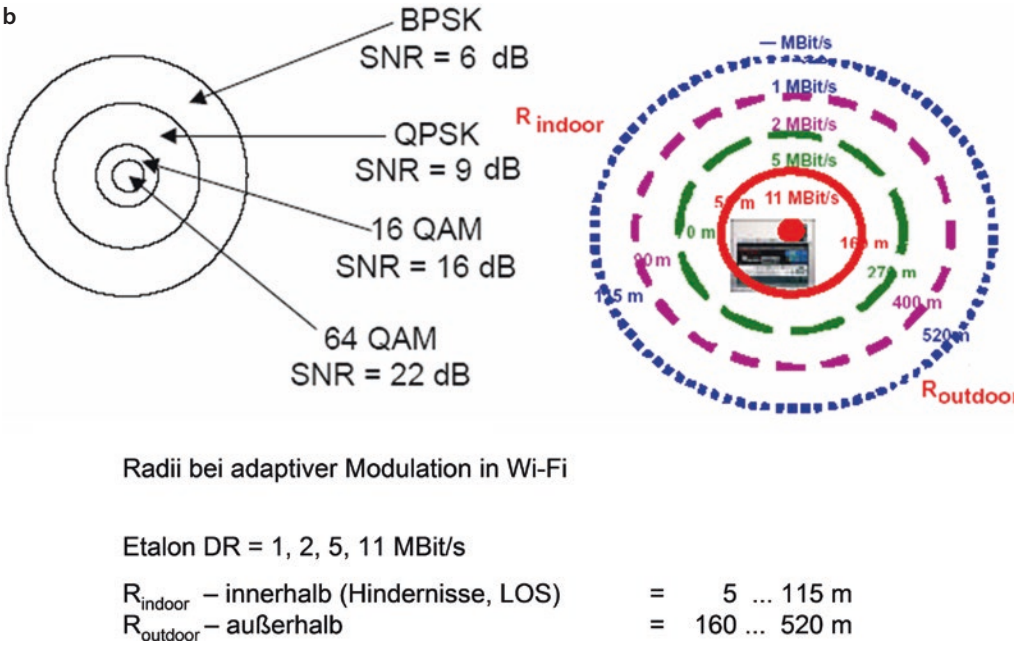


Abb. 12.24 Modulationstypen und Datenraten

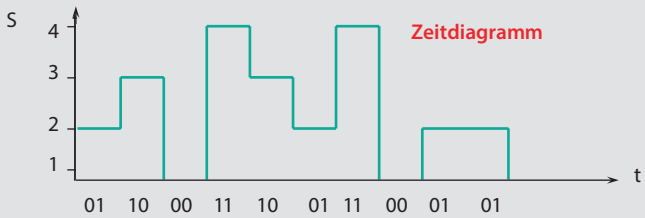


Abb. 12.25 Folge von 2-Bit-Signalen (4 Stufen)

Weiterhin beträgt für die UMTS-Mobilfunknetz-Zellen der Spektraleffizienzwert $SE = 0{,}2\frac{\text{Bit/s}}{\text{Hz}}$; bei Mobilfunknetzen wie IEEE 802.20 MBWA und LTE beträgt dieser Wert $SE = 1\frac{\text{Bit/s}}{\text{Hz}}$.

Die geringeren SE-Werte für Funknetze ergeben sich aus dem ungünstigen SNR in realen Umgebungen.

Medienzugriff mittels CSMA/CA Das Verfahren CSMA/CD ist in Funknetzen nicht anwendbar, da Kollisionen nicht immer erkannt werden können. Alternativ wird das Prinzip „listen before talking" verfolgt.

Für WLAN sollen die Probleme des Medienzugriffes gelöst werden durch die Zugriffsmethode *CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)* und weitere Optimierungszusätze. Der grundsätzliche CSMA/CA-Ablauf ist:

1. *Sendewillige Station hört Medium vor dem Senden ab*
2. *wenn Kanal frei, Abwarten eines zufälligen „back off"-Zeitintervalls, danach Senden*
3. *Kollision sehr unwahrscheinlich, aber nicht unmöglich. ggf. Wiederholung bzw. Abbruch wenn Maximalwert von Sendeversuchen erreicht ist.*

Mit der Nutzung von CSMA/CA in Funknetzen sind zwei Anomalien verbunden. Die Problematik ist unter den Namen „Hidden Terminals" (1. Problemfall versteckte Geräte) und „Exposed Terminals" (2. Problemfall ausgelieferte Geräte) bekannt (Abb. 12.26).

Der 1. Problemfall versteckter Geräte kann folgendermaßen beschrieben werden:

- A und C liegen nicht im gegenseitigen Funkbereich.
- A sendet zu B und belegt den Funkkanal.
- C möchte ebenfalls zu B senden, kann den belegten Funkkanal nicht erkennen und sendet deshalb.

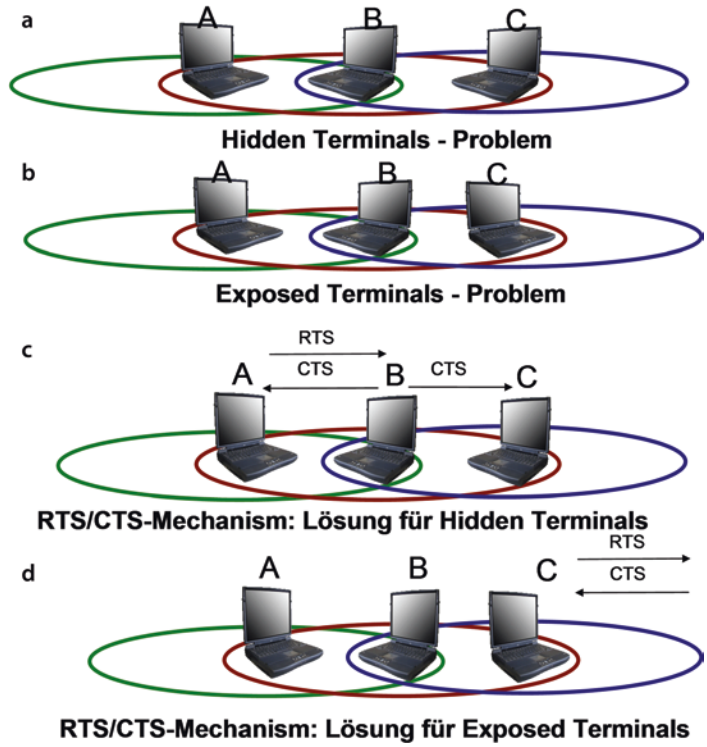


Abb. 12.26 Verbesserter Medienzugriff per CSMA/CA mit CTS/RTS-Zusatznachrichten

12

- Es entsteht eine Kollision bei B, B kann die Daten nicht rekonstruieren.
- A erkennt die Kollision ebenfalls nicht.

A ist vor C und C vor A versteckt.

Der 2. Problemfall ausgelieferter Geräte beschreibt folgende Situation:

- B sendet an A und C will an andere Station (nicht A oder B) senden
- C erkennt die Signale von B und wartet, bis B Übertragung beendet
- Es gibt einen unnötigen Wartevorgang, da die Signale von C keine Kollision bei A hervorrufen

C ist den anderen Stationen ausgeliefert.

Die Lösung liegt in der Ergänzung des CSMA/CA-Verfahrens um den RTS/CTS-Zusatzmechanismus (Request To Send/Clear To Send). Durch Austausch von Zusatznachrichten RTS und CTS wird das Netzverhalten im WLAN optimiert:

Lösung 1. Problemfall versteckter Geräte:
- A schickt B eine Nachricht RTS und B sendet im Gegenzug CTS falls B zur Übertragung bereit ist.
- andere mögliche Sender (C) empfangen ebenfalls das CTS-Signal und verschieben ihre Übertragung.

Lösung 2. Problemfall ausgelieferter Geräte:
- C sendet zu gewünschtem Empfänger RTS.
- falls dieser bereit ist erhält C die Nachricht CTS und kann senden.

Optimierungsaufgaben bei WLAN-Projektierung Die optimale Aufstellung von Zugangspunkten (Access Points, AP) nach WLAN IEEE 802.11 stellt sich als Mehrschrittoptimierungsprozedur dar. Generell kann man diese Optimierungsaufgabe für AP-Konstellationen folgendermaßen definieren:

$$\min N_{AP} \wedge \max\ (Coverage(x, y)\ \wedge QoS) \tag{12.6}$$

wobei N_{AP} die Anzahl der AP, $Coverage(x, y)$ die Abdeckungsfläche (x, y) bei akzeptablem Empfang und QoS die Einschränkungen auf die Parameter von *QoS (Quality of Service)* sind, speziell:
- SE – Spektraleffizienz nach Nyquist (Spectrum Efficiency, [bit/s/Hz]).
- DR – Datenrate.
- PR_x, S – Signalqualität (Empfangsfeldstärke oder Sensibilität).
- SNR – Signal-Rausch-Abstand (Signal-Noise-Ratio).
- ***C/I&N*** – Träger-**Interferenz**-Rausch-Abstand (Carrier to Interference & Noise Power Ratio).
- R – Reichweite (max. zulässige Distanz).

12.4 Drahtlose städtische Netze IEEE802.16 – WiMAX

Referenzarchitektur von WiMAX Der gegenwärtig aktuelle WiMAX-Standard basiert auf den Standards IEEE 802.16-2009, -2004 und IEEE 802.16 a,d,e. Mobile WiMAX ist besonders beliebt in Südkorea. In anderen Regionen spielen IEEE 802.20, 802.16a/d/e/m und 4G eine größere Rolle. WiMAX bietet Datenraten bis 134 Mbit/s. Die Technologie setzt unterschiedliche (hierarchische) Zellstrukturen ein (z. B. ein lizenzfreies „Wireless-DSL“ in der Kombination mit WLAN oder einem Entlastungsbackbone in den 3G-Systemen). Die Zellgrößen

variieren zwischen 5 km und 30 km in Abhängigkeit von der Frequenz und Mobilität. In ◘ Tab. 12.12 werden ausgewählten Standards zu IEEE 802.16 kurz umrissen.

IEEE 802.16 -Netze bieten eine sehr flexible Architektur für Zellular- oder Backhaul-Konfigurationen. Eine MS oder SS bekommt Zugang zu einem ASN und weiter zu den Home und Visited CSN (Abkürzungslegende siehe ◘ Abb. 12.27). Die Architektur bietet Handover und Roaming zwischen WiMAX-Providern. Ein CSN ermöglicht den Übergang zum ASP und zum Internet über die standardisierten Schnittstellen R1 bis R5 für Daten- und Signalisierungskanäle.

Die Modulationsart QAM repräsentiert eine Kombination von Phasen- und Amplitudenmodulation. Mit einer Bitanzahlerhöhung bei der Signalkodierung steigt auch die Spektraleffizienz. QAM optimiert außerdem den SNR und die Reichweite (◘ Abb. 12.28).

Typische Konfigurationen Die WiMAX-Technik ist hauptsächlich für die Internet-Anbindung ländlicher Regionen konzipiert. Es gibt aber auch weitere Anwendungsmöglichkeiten. Eine wichtige Rolle spielen Dualendgeräte bspw. mit WiMAX-Backbone und WLAN-Transport für VoIP/TVoIP-Übertragungen (Fernseh- und Sprachdienste über vollkommen drahtlose DSL-Zugangsnetze).

12

◘ **Tab. 12.12** Standardfamilie IEEE 802.16 [11]

Merkmal	802.16	802.16a	802.16e/802.16-2005	802.16d/802.16-2004/2009	802.16m-2010
Einsatz seit	2001	2003	2005	2004	aktuell
Band F, GHz	10–66	2–11	2–6	10–66, wie 802.16a	F > 10 GHz
DR, MBit/s	32–135	75	15	134	Zwei Modi: WMAN DR < 1 GBit/s; Mobile WMAN DR < 100 MBit/s
Modulations-verfahren	QPSK, 16QAM, 64QAM	OFDM 256, QPSK, 16QAM, 64QAM	OFDM 256, QPSK, 16QAM, 64QAM	OFDM, QPSK, 16QAM, 64QAM	OFDM, QPSK, 16QAM, 64QAM
Zellgröße, km	2–5	7–10	2–5	bis 50	–
LOS (Sicht-linien-Bedingung)	LOS	NLOS	NLOS	NLOS	–
Mobilität, km/h	–	–	150	130	–

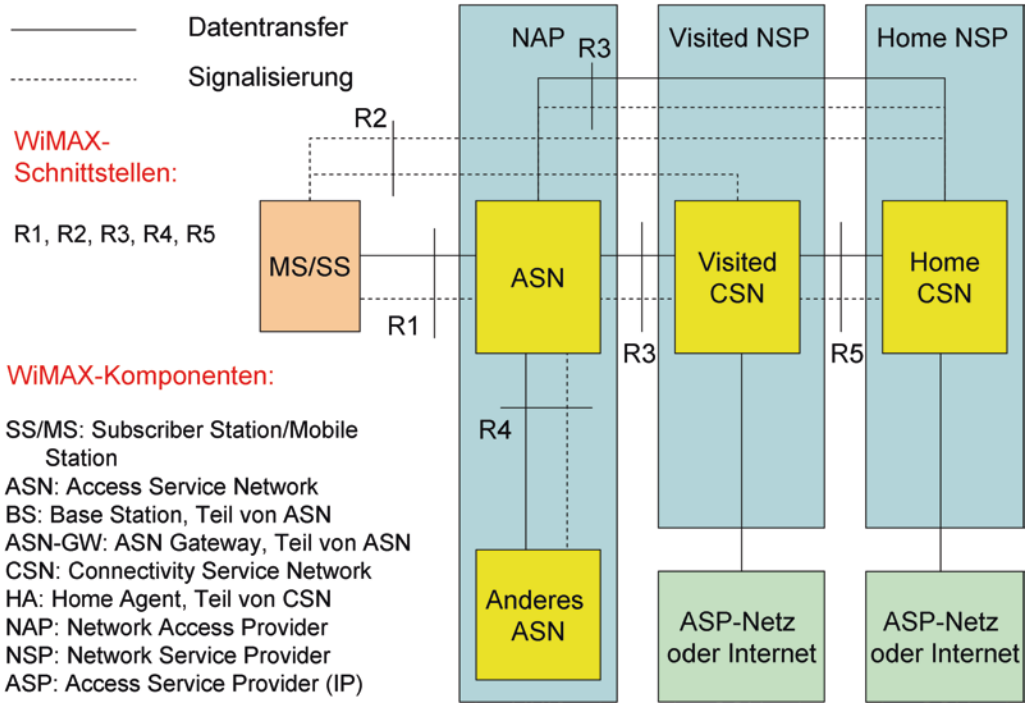


Abb. 12.27 Referenzarchitektur von WiMAX

Dank flexibler WiMAX-Systeme können stationäre Zugänge, Wireless DSL, mobile Zugänge mit bis 180 km/h Geschwindigkeit und Campuspikonetze realisiert werden. Einige Nutzungen sind in Abb. 12.29 dargestellt:

- Fixed – IEEE 802.16-2004/2009.
- Fixed and portable – IEEE 802.16a.
- Nomadic – IEEE 802.16e (mobiler WiMAX-Substandard).

Für mobile Anwendungen 3G/4G bietet WiMAX auch ein breites Spektrum von Integrationsmöglichkeiten, die unten aufgeführt werden. Z. B. kann die Clientmobilität bis zu 130 km/h betragen in Makrozellen einer Größe von 1,5 bis 5 km bei $DR = 15$ MBit/s pro Kanal und Kanalbandbreiten von 5 MHz.

Einige Beispiele der Interoperabilität von WiMAX-Systemen zu Mobilfunknetzen finden Sie in Abb. 12.30. Die Kopplung erfolgt über MSC (Mobile Switching Center) der 2G-Mobilfunknetze, wobei das WiMAX mehrere WLAN-Access Points integrieren kann (s. Variante a). Entsprechend ist es auch möglich, einen Zusammenschluss mehrerer UMTS-3G-Zellen in einer Makrozelle von WiMAX zu realisieren (s. Variante b).

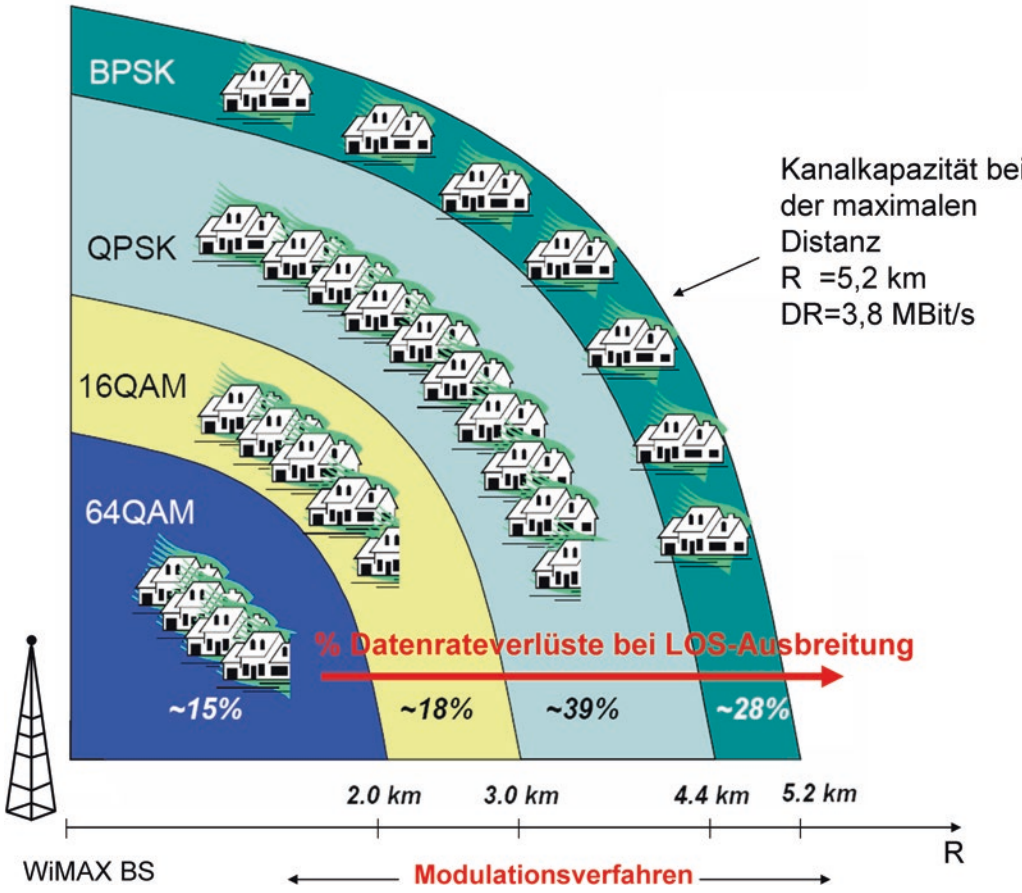
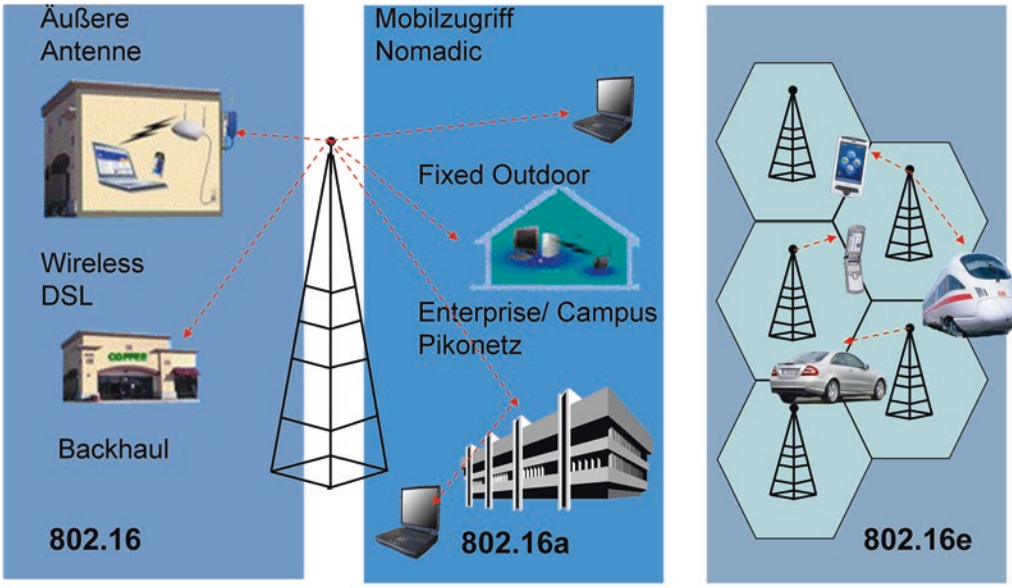


Abb. 12.28 Adaptive Modulation in WiMAX-Systemen

12.5 Automatisierungsnetze. Feldbusse

Grundlagen Feldbusse Seit Anfang der 60-er Jahre werden Computer auch in der Industrie eingesetzt. In den Betrieben existieren verschiedene Kommunikationsebenen:

- die Betriebsebene für Verwaltung, Entwicklung und Management,
- die Leitebene für die Verwaltung einzelner Betriebsteile (Fertigung, Lager usw.),
- die Systemebene für die Anlagensteuerung,
- die Prozessebene zur Maschinensteuerung mit einfachen, robusten Spezialcomputern, den SPS (speicherprogrammierbare Steuerung) und
- die Feldebene mit Sensoren und Aktoren (Abb. 12.31).



Zugangstyp	Standards
Fixed	802.16
Fixed and portable	802.16a
Nomadic	802.16e

Abb. 12.29 Netzwerktypen für WiMAX-Systeme

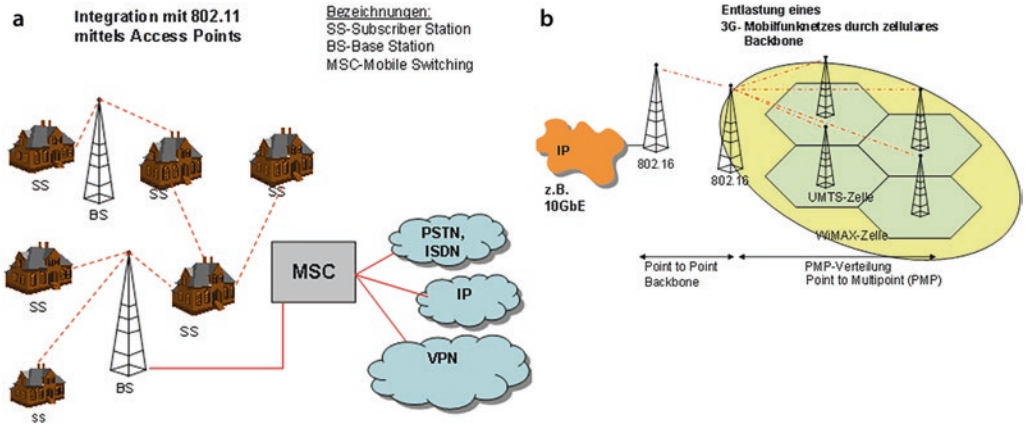


Abb. 12.30 Interoperabilität von WiMAX-Systemen zu Mobilfunknetzen

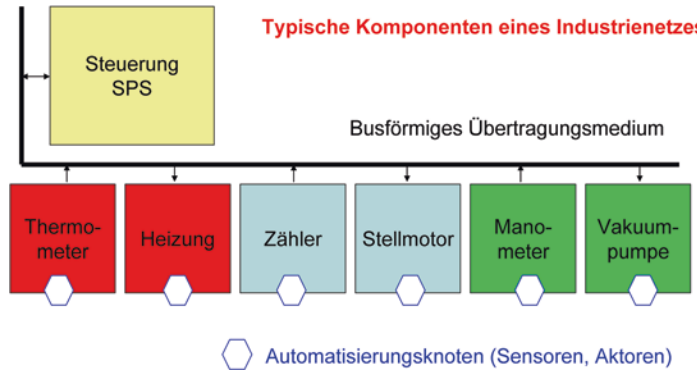


Abb. 12.31 LAN in der Automatisierungstechnik

Als kommunikationstechnische Plattform für die Betriebs- und Leitebene dienen normale bürotypische LAN, meist Ethernet-Lösungen. In der Feld- und Prozessebene werden wegen der hohen Echtzeitanforderungen spezielle Industrie-LAN eingesetzt. Die Systemebene ist an beide LAN angeschlossen.

Begriff „SPS" steht für „Speicherprogrammierbare Steuerung", auf Englisch: „Programmable Logic Controller (PLC)". Der Nachrichtenverkehr in den unteren Ebenen besteht überwiegend aus der Übertragung von Messwertdaten von den Sensoren zur SPS und von Stellwertdaten von der SPS zu den Aktoren.

Die Übertragungsdaten sind kurz, deswegen tragen die Pakete einen spezifischen Namen: „Telegramme". Es werden i. a. keine extremen Anforderungen an die LAN-Übertragungsrate gestellt. Wichtiger ist die Zuverlässigkeit, die Vermeidung von Wartezeiten und die Echtzeitfähigkeit (garantierte Reaktionszeiten, Realtime).

Die problemspezifische Zentralisierung führte dazu, dass die Industrie-LAN ursprünglich sternförmig realisiert wurden. Dabei führt von der SPS zu jedem einzelnen Feldgerät eine eigene Datenleitung. Die SPS agiert als Master und die Feldgeräte als Slave, d. h. die Initiative zur Datenübertragung geht immer von der SPS aus. Moderne Fertigungssysteme verwenden in der Regel Feldbusse. Dabei sind alle Feldgeräte und die SPS über eine Datenleitung verbunden.

Die Netze decken meistens die Aufgaben der OSI-Schichten 1 und 2 ab, die Anwendungsdienste setzen i. a. direkt auf Schicht 2 auf. Die LAN-Zugriffsverfahren sind sehr unterschiedlich und basieren meist auf einem Zeitmultiplexverfahren (TDMA). Die Belegung der Zeitschlitze wird über einen Busmaster gesteuert. Einige Verfahren nutzen auch das CSMA/CA-Verfahren. International verbreitet sind u. a. die Feldbusse (Tab. 12.13):

Tab. 12.13 Ausgewählte Standards für Feldbusse [3, 4, 6, 7, 8, 9, 11]

INTERBUS-S	Universalbus für MSR-Anlagen
PROFIBUS	Universalbus für MSR-Anlagen
CAN/CANopen	von Bosch und Intel entwickelt, vor allem als Automobilbussystem
LON	steht für „Local Operating Network", komplexes System, insbesondere für Facility Management bzw. Echelon, 1990; ANSI/EIA-709/852; Control Network Protocol (EN14908, 2007)
KNX (ehemals EIB)	Feldbus für Facility Management, Konnex-Bus-2002 von Konnex Association, EN50090/ ISO/IEC 14543; der Konnex Standard ist im Wesentlichen Weiterentwicklung des EIB (steht für „European Installation Bus"), der mit Übertagungsmedien Twisted Pair und PLC (Powerline) starke Verbreitung findet
BACnet	Layer 3 – Automatisierung (Management Level)

Gebäudeautomatisierungsnetze Die aktuellen Gebäudeautomatisierungssysteme (BAS, Building Automation Systems) übernehmen diverse Funktionen wie z. B. Heizung, Lüftung, Klimatechnik (HLK), oder im Englischen „HVAC" (Heating, Ventilating and Air Conditioning). Des Weiteren kann es auch um Zugangssysteme (human access, security control) gehen. Diese breite Funktionalität wird über intelligente Knoten (Sensoren, Controller, Aktoren, Monitore) im Feldbus als Kommunikationsmedium realisiert.

Diverse Protokolle werden dabei betrieben: EIB/Konnex, LON, BACnet, CAN, Ethernet etc. Als Softwarelösungen für Gebäudeautomatisierungsnetze (Layer 5–7) werden Middleware (OSGi, Open Services Gateway Initiative, und OPC, OLE for Process Control) sowie und Web Services empfohlen.

Integration und Interoperabilität. Häufig werden Gebäudeautomatisierungsnetze moderner Gebäude in bürotypischen LAN integriert. Solche Lösungen weisen eine hohe Qualität und Verkabelungs-/Gerätewiederverwendbarkeit auf. In Abb. 12.32 ist ein integriertes Szenario für die Bürokommunikations- sowie Automatisierungsvernetzung zu sehen.

Das Management erfolgt über die verfügbaren Gateways und die existierende LAN- bzw. TCP/IP-Infrastruktur. Die Experten können die Systeme sowohl vor Ort als auch im Remote Modus verwalten. Ein weiterer Vorteil der Integration liegt darin, dass die Netzwerkprojektierung für die beiden Systeme (strukturierte Verkabelung, Ausleuchtung drahtloser Strecken, Einsatz von Kopplungsgeräten, Installation der Protokolle und Dienste etc.) aufwand- und kostenersparend erfolgen kann.

Die Schnittstellen zu den Feldbussen können über einfache Gateways realisiert werden. Diese Gateways übertragen die

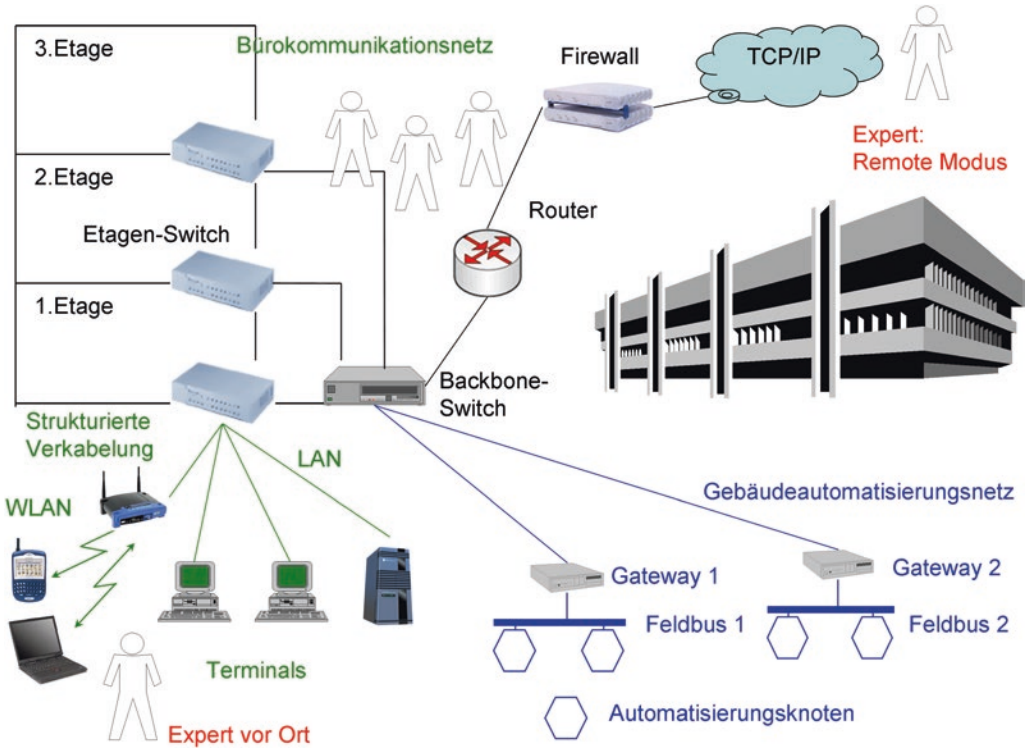


Abb. 12.32 Integriertes Szenario für die Bürokommunikations- sowie Automatisierungsvernetzung

12

Tab. 12.14 Analyse von Integrationsmöglichkeiten für Gebäudeautomatisierungsnetze mit Bürokommunikationsnetzwerken [11]

Ebene	Einsatz von Bürokommunikationsnetzwerken
Feldebene	Abtastung und Kontrolle z. B. mittels Ethernet/WLAN, z. T. in Echtzeit
Automatisierungsebene	Integration und Interoperabilität heterogener Feldbus-Segmente durch Ethernet/IP-Gateways; Einsatz von IP-Kontroller und BAS-Services über IP
Managementebene	Distant Monitoring eines BAS, Facility Management unter Nutzung von Web-Interface über Desktop-PC und PDA

Feldbusspezifische Nachrichten mittels TCP/IP über Ethernet, WLAN bzw. weitere Netze, Power Line Communication (PLC) und Powerline Homeplug.

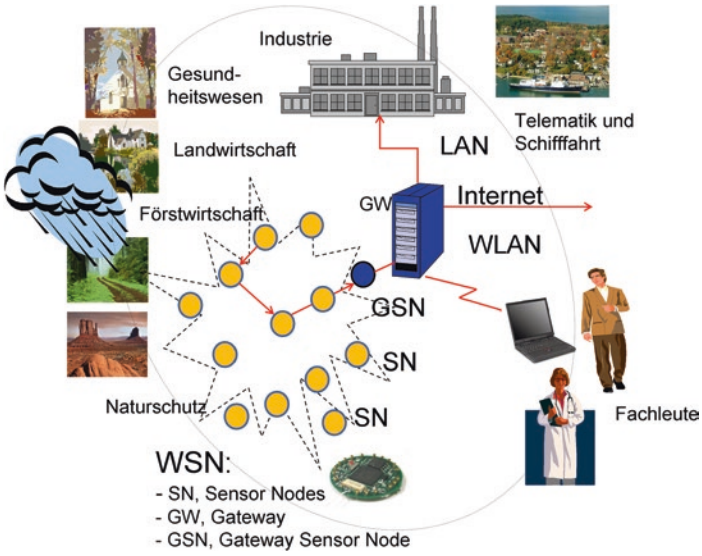
Einige Varianten der Integration von Gebäudeautomatisierungsnetzen mit Bürokommunikationsnetzwerken, bürotypischen LAN, werden in Tab. 12.14 veranschaulicht.

12.6 Sensorpikonetze – WSN

Im Unterschied zu den bisher diskutierten Netzen, bei denen die Dienstgüte- und Kostenanforderungen (QoS vs. Kosten) von größter Bedeutung waren, ist es für die ***Wireless Sensor (Pico-) Networks (WSN)*** typisch, dass verschiedene Aspekte der Energieeffizienz in Betracht gezogen werden müssen. Die Energieeffizienz bei drahtlosen Sensornetzwerken ist eine entscheidende Voraussetzung für deren Langlebigkeit, niedrige Wartungskosten und hohe Zuverlässigkeit. Als Erstes wird ein kurzer Überblick über verbreitete WSN-Systeme gegeben. Anschließend werden die wichtigsten Kompromisse (Tradeoffs) zwischen diversen Faktoren diskutiert, die ***Energieeffizienz*** und ***Dienstqualität*** auf den verschiedenen Netzwerkschichten beeinflussen.

12.6.1 Überblick drahtloser Sensor-Netzwerke

Grundlagen Drahtlose Sensornetze sind mittlerweile zu einer ausgereiften Technologie geworden und spielen von Jahr zu Jahr eine wichtigere Rolle für industrielle Fertigung, intelligente Häuser, automatisierte Gebäude und die Beobachtung im Freien: in Land- und Forstwirtschaft, Umweltschutz und Schifffahrt (◘ Abb. 12.33). Diese Liste möglicher Anwendungen von WSN ist jedoch bei Weitem nicht komplett. Fortgeschrittene WSN ersetzen in Zusammenspiel mit WLAN- und WiMAX-Netzen zunehmend konventionelle



◘ **Abb. 12.33** Struktur eines WSN

Kommunikationssysteme für vielfältige Netzwerkdienste und Automatisierungssysteme.

Ein allgemeines Sensornetz besteht aus einer Vielzahl verteilter und unabhängiger Sensorknoten (SN) mit Funkmodulen, die in der Lage sind, technische Parameter oder Umweltparameter zu erfassen. Es existiert eine Vielzahl von Sensortechnolologien und -typen (◘ Tab. 12.15). All diesen Technologien gemein ist als wichtigste Problematik der energieeffiziente Betrieb der Sensornetze. Energieeffiziente Sensorknoten zeichnen sich durch Langlebigkeit sowie Interoperabilität und Gewährleistung von Dienstgüteanforderungen (QoS) im konstruierten WSN aus. Außerdem besitzen sie hohe Zuverlässigkeit und kostengünstige Möglichkeiten zur Anpassung.

Architektur Drahtlose Sensor-Netzwerke verwenden größtenteils in Harvard-Architektur implementierte Mikrokontroller (◘ Abb. 12.34) mit Programmspeichern von ca. 128 KB und Datenspeichern von ca. 64 KB. Die üblichen Frequenzbänder für WSN liegen bei F = 315…916 MHz (Mica2, Mica2Dot) und F = 2,4 GHz (ZigBee IEEE 802.15.4, Imote). Die üblichen Reichweiten der Sensorknoten betragen zwischen 30 und 150 m. Beim Senden und Empfangen von Daten wird jeweils eine Spitzenleistung von ca. 1000 mW für eine kurze Zeit (Duty time) benötigt, 100 mW im Ruhezustand und 0,05 mW im Schlafmodus. Die durchschnittliche Sendeleistung in einem Zeitintervall beträgt in realen Szenarien PTx = 4…10 dBm (meist unter 10 mW). Zur Gewährleistung der Anforderungen bezüglich Energieeffizienz und Echtzeitverhalten werden nur kurze Datenpakete (Telegramme, TL ≈ 100 Byte) mit vergleichsweise geringem Overhead verwendet. Der Zustandsübergang eines Sensorknotens (SN, Sensor Node) verbraucht Energie und verlangsamt das Netzwerk insgesamt.

Der Ansatz des Energy Harvesting ermöglicht die Gewinnung von Energie aus der Umwelt (Bewegungsenergie, Sonnenlicht, Wärme etc.) und damit eine Reduzierung des Batterieverbrauchs. Die ausschließliche Energieversorgung von Sensorknoten mittels Energy Harvesting ist jedoch aufgrund der Unstetigkeit der genutzten Energiequellen nicht möglich. Daher müssen die Knoten mit Bedacht platziert werden, außerdem ist eine Optimierung der Routen zum Gateway (GSN) empfehlenswert (s. bspw. EnOcean-Netzwerke).

Die auf den Knoten genutzte Software (BS – Betriebssystem, Anwendungen, API, MW – Middleware) muss zudem sehr kompakt sein. Die ausgeführten Tasks und zu verarbeitende Daten werden häufig zuerst vorläufig eingeplant (Scheduling) und gruppiert (Telegram Aggregation). Zur Minimierung des Energieverbrauchs für die Kommunikation (SN – SN und SN – GW) sowie zur Steigerung der Performanz des Gateways

Tab. 12.15 Eigenschaften verbreiteter WSN Systeme [8, 11]

Eigenschaft	EnOcean	KNX-RF	Z-Wave	Zig Bee (IEEE 802.15.4)	Scatter-web	Nano NET
Frequenz, MHz	868	868	868	2400	868	2400
MAC-Schicht	Beacon	–	CSMA	Beacon CSMA	–	CSMA/ CA, TDMA, ALOHA
Topologie	Stern/Mesh	Stern	Stern/Mesh	Stern/Mesh	Baum/Mesh	Mesh
Datenrate, KBit/s	125	16,4	9,6/40	250	20	2000
Anzahl von Knoten	2^{32}	256	2^{32}	2^{16}	255	2^{48}
Sicherheit	AES	–	Mittel-fristig	AES	–	+
Energie-Verbrauch	Sehr gering	Gering	Gering	Gering	Gering	Mittel
Kollisionswahrschein-lichkeit	Sehr gering	+	+	Gering	Gering	Sehr gering
Energy Harvesting	Ja	Nein	Nein	Nein	Nein	Nein
Reichweite, m	30–300	10–100	20–200	10–75	10–100	40–250

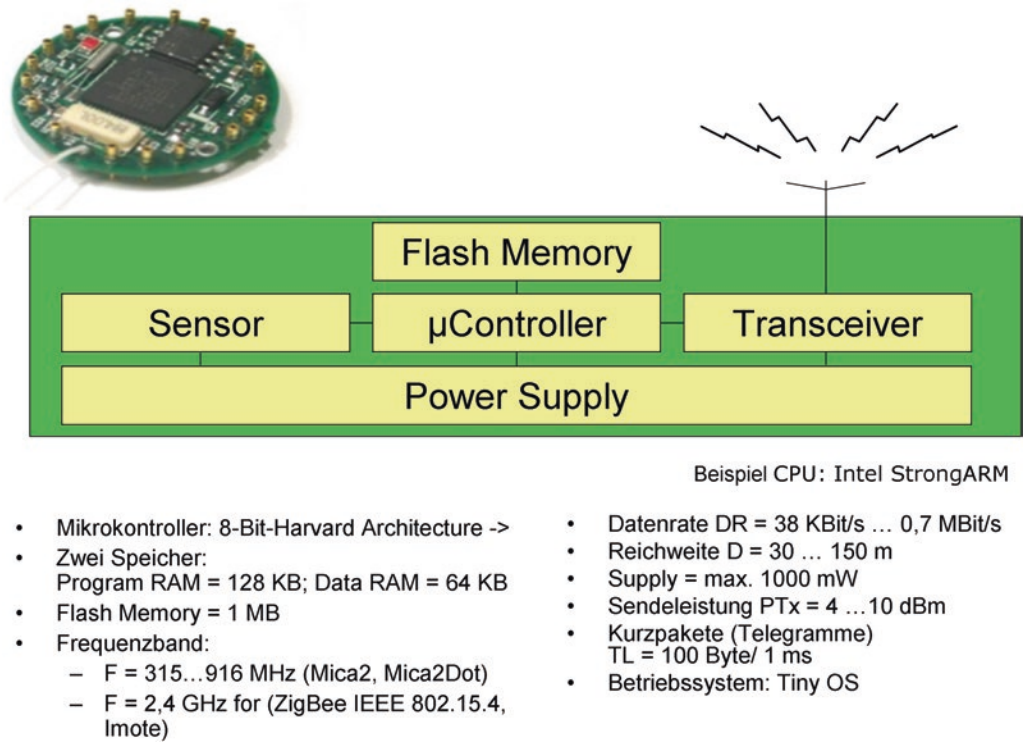


Abb. 12.34 Beispiel eines drahtlosen Sensors

sind die Konzepte Caching, Threading und Redundanz/Replikation in Betracht zu ziehen. Die Task-Abarbeitung in den Anwendungen erfolgt ereignisbasiert. Als Betriebssystem für Sensorknoten wird beispielsweise Tiny OS genutzt. Es weist einen geringen Bedarf an Speicher und Rechenleistung auf.

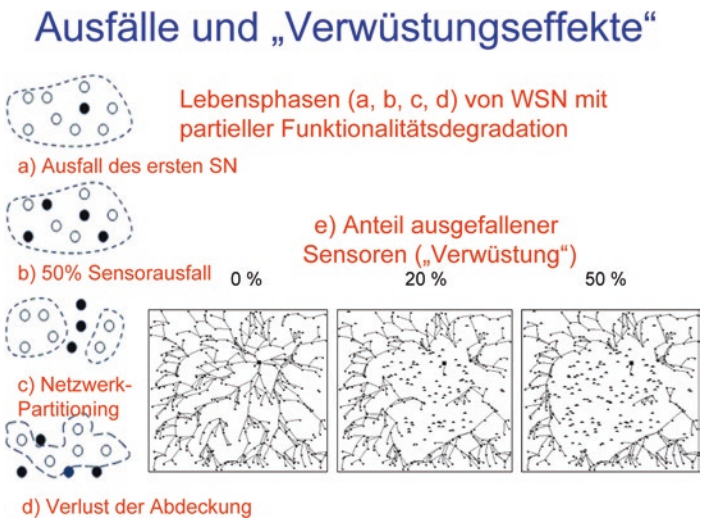
Entwurf energieeffizienter drahtloser Sensornetze Wichtige Eigenschaften energieeffizienter WSN sind:

- Effiziente Batterien mit hoher Lebensdauer in den Sensorknoten, eventuell kombiniert mit Energy Harvesting.
- Energiemanagement.
- Effiziente Protokolle (Schichten 2, 3) mit reduziertem Datenverkehr und geringem Overhead.
- Effiziente Betriebssysteme und Anwendungen.
- Optimierte Topologie (Hierarchie, Clustering).
- Redundante Planung und Funktionalitätsreservierung.
- Kombinierte Ansätze (Schichtenübergreifender Entwurf).

Heutzutage wird der Entwurf von WSN durch eine Vielzahl von Energiemanagement-Methoden und Planungswerkzeugen unterstützt. Der schichtenübergreifende Ansatz kombiniert existierende Modelle, Methoden und Werkzeuge innerhalb eines integrierten Frameworks und bietet signifikante Vorteile, da eine umfassende Abwägung zwischen Anforderungen der Energieeffizienz und der Dienstgüte stattfindet. Die Methoden für den Entwurf energieeffizienter WSN können gemäß der Schichtenarchitektur folgendermaßen klassifiziert werden:

- Hardware (ausgerichtet auf PHY-Layer).
- Ausgerichtet auf MAC-Layer.
- Ausgerichtet auf Topologie (ein wichtiges Thema, Details folgen unten).
- Ausgerichtet auf Routing.
- Ausgerichtet auf Anwendungen.

Effizientes Energiemanagement für WSN bedeutet in erster Linie, dass der Gesamt-Energieverbrauch eines WSN durch Optimierung des Energieverbrauchs der Sensorknoten (ausgedrückt in W/Bit, W/Ereignis) reduziert werden muss. Eine derartige Optimierung führt zu einer Erhöhung der die Lebensdauer (time-to-live, TTL) des WSN, ausgedrückt in 1000 h oder 100 d. Folgende Parameter sind üblich: T1 – Zeit bis zum Ausfall des ersten Sensorknoten; T2 – Zeit, bis 50 % der Knoten ausgefallen sind; T3 – Zeit, bis das Netzwerk in mehrere Teile („Inseln“) zerfällt; T4 – Zeit, bis die Flächendeckung des Netzwerk zurückgeht. Die TTL-Parameter werden in ◘ Abb. 12.35 veranschaulicht.



◘ **Abb. 12.35** Time-to-live Parameter von Sensorknoten

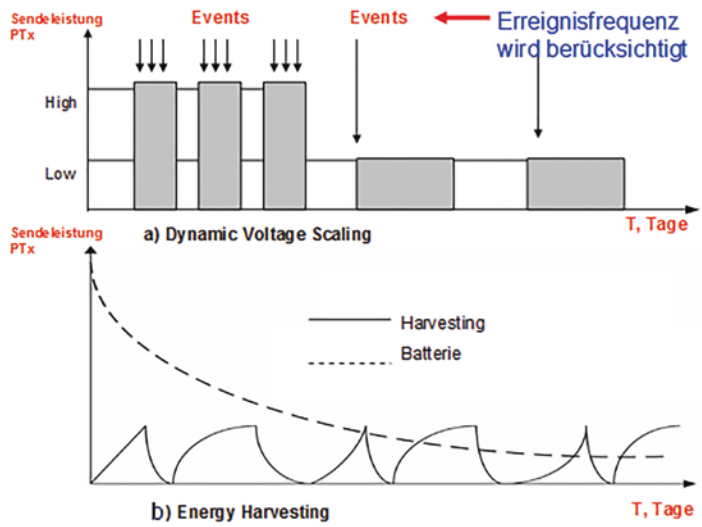
Schichtenübergreifender Entwurf energieeffizienter WSN Der schichtenübergreifende Entwurf von WSN muss Wechselwirkungen zwischen den widersprüchlichen Anforderungen Energieeffizienz und Dienstgüte berücksichtigen und angemessene Kompromisse finden:

Hardware:

- Höhere Übertragungsfrequenz: mehr Daten pro TDMA Slot sowie kompakte Komponenten, aber komplexere Modulationstechniken und höhere Energieanforderungen;
- Niedrige Sendeleistung: geringerer Energieverbrauch beim Senden, aber geringerer Signal-Rausch-Abstand (SNR) und geringerer Datendurchsatz;
- Niedrige Spannung der Komponenten: niedriger Energieverbrauch der CPU, aber auch geringere CPU-Leistung.
- Höhere Kapazität der Batterien: längere Lebensdauer, aber auch größere Abmessungen. Das gilt auch für Energy Harvesting-Ansätze, die ausreichend leistungsfähige Energiequellen und Batterien benötigen um die nichtkontinuierliche Energieversorgung auszugleichen, vgl. ◘ Abb. 12.36.

MAC-Schicht:

- Längere Sensor-Duty-Cycles in Kommunikationsprotokollen (z. B. synchrones on-demand TDMA oder Advanced Asynchronous CSMA/CA mit RTS/CTS oder Rendezvous): bessere Auslastung, aber größere Latenzzeiten.



◘ **Abb. 12.36** Energieverbrauchsoptimierungsansätze

Topologie:
- Cluster von Knoten nach einheitlichem Plan (scheduled) mit geringerem Duty-Cycle: geringerer Energieverbrauch in Sensorknoten durch kürzere Distanzen, aber größere Latenzzeiten durch Overhead und höherer Energieverbrauch beim Cluster-Head.
- Dichte WSN mit redundanten Knoten: höhere Verfügbarkeit und Zuverlässigkeit, aber auch höherer Datenverkehr und damit mehr Kollisionen von Datentelegrammen sowie häufigere Timeouts

Routing:
- Hochentwickelte Routing-Algorithmen (z. B. Geographic Routing): erhöhen die Zuverlässigkeit der Nachrichtenübertragung, verursachen aber höhere Routing-Komplexität und aufwendigere Routing-Anpassungen im Fall von Änderungen der Topologie.

Software/Anwendungen:
- Kompaktes Betriebssystem und sonstige Softwarekomponenten aufgrund begrenzter CPU-Leistung und RAM-Kapazität: bessere Ressourcenausnutzung, aber geringere Genauigkeit durch Datenaggregation sowie Notwendigkeit spezieller Algorithmen für verteilte statistische Vorverarbeitung großer Datenmengen.

Diese Kompromisse (Tradeoffs) sollten in der Entwurfsphase berücksichtigt werden, um das Ziel eines langlebigen WSN mit hoher QoS sowie Verfügbarkeit und Interoperabilität der Knoten zu erreichen.

Optimierung der Topologie Die erste wichtige Entscheidung beim Entwurf der Topologie eines WSN ist die Wahl zwischen Single-Hop und Multi-Hop Routing Methoden.

Folgende Aspekte sind zu berücksichtigen: wer kommuniziert mit wem (Stern, Cluster oder Mesh); keine vollständige Kenntnis der Topologie, nur Informationen zur lokalen Umgebung vorhanden; häufige Topologieveränderung, An-/Abkopplung, Mobilitätsaspekte; Routingalgorithmen; sowie, selbstverständlich, die Energieeffizienz der Lösung.

12.6.2 Anwendungsfälle bei WSN-Entwurf. ZigBee. EnOcean

System ZigBee Der Name „ZigBee“ leitet sich vom ZickZack-Nahrungssuchetanz der Bienen ab und bezeichnet dadurch den Datenverkehr in einem vermaschtem Netz [10, 11, 16, 19]. System

ZigBee wird als ***Wireless Personal Area Network (WPAN)*** aufgebaut und nutzt die IEEE 802.15.4- Festlegungen für Schichten PHY- und MAC-Layer. Hier eine kurze Entstehungsgeschichte von ZigBee-Systemen [11]:

- 1998 – ZigBee wurde durch Philips gestartet.
- 2001 – IEEE 802.15.4 Group für ZigBee gegründet.
- 2002 – ZigBee Alliance von mehr als 230 Firmen zusammengeschlossen (u. a. Philips, Mitsubishi).
- 2005 – erste ZigBee-Produkte kamen auf den Markt.
- ab 2007 – permanente Verbesserungen bzgl. des Energieverbrauchs und der Datensicherheit.

ZigBee-Produkte entsprechen vollkommen den Anforderungen für die Low-Rate Wireless Personal Area Networks:

- Long-life- Batterien.
- Secure Networking (AES- Kryptoalgorithmus).

ZigBee-Systeme funktionieren im ISM-Band mit $F = 2{,}4$ GHz und besitzen Datenraten von $DR = 0{,}25$ MBit/s bei Reichweiten von 10 bis 75 m. In der MAC-Layer wird entweder CSMA/CA implementiert oder mit sog. Beacon-Signalen (Leuchtfeuer) gearbeitet. Die Beacon-Signale werden von einer sendewilligen Station nach längeren Kommunikationspausen gesendet, dadurch werden alle Netzteilnehmer der Umgebung für eine gewisse Zeitspanne in Empfangsbereitschaft versetzt. Durch dieses Verfahren sind Kollisionen sehr unwahrscheinlich.

ZigBee bietet Kompatibilität zu alternativen Lösungen auf dem Niveau der Schichten 1 und 2:

- USA – 915 MHz; 40 kBit/s
- Europa – 868 MHz; 20 kBit/s

Es sind aber eventuelle Interferenzen mit existierenden WLAN zu berücksichtigen. Die wichtigsten Anwendungsbereiche von ZigBee-Produkten sind:

- Structural Health Monitoring (Gesundheitswesen).
- Facility Management (Gebäudemanagement).
- Smart Metering (intelligente Messtechnik) usw.

System EnOcean EnOcean GmbH mit Sitz in Oberhaching bei München ist eine Tochter der Siemens AG. EnOcean, ein System drahtloser Sensoren mit eigener Stromquelle bzw. mit Energy Harvesting, findet im Bereich der Gebäudeautomatisierung breite Verwendung. EnOcean bietet eine besonders hohe Energieeffizienz. EnOcean-Systeme sind praktisch seit 2001 bekannt. 2008 erschien die EnOcean Alliance aus vielen namhaften Firmen (DE, FR, EU, USA), u. a. Siemens und Osram.

EnOcean-Produkte funktionieren auf Entfernungen von 10 bis 300 m. Beim Entwurf von EnOcean-Systemen wird weitgehend ein optimierter Cross-Layered-Ansatz verfolgt. Die MAC-Layer ist Beaconing-basiert. Die Kollisionswahrscheinlichkeit ist aber dabei sehr gering. Um deren Wirkung zu minimieren, wird ein dreimaliges, pseudozufälliges Absetzen kurzer Telegramme (Nachrichtenlänge von 14 Byte) verwendet. Die Systeme funktionieren im Frequenzband F = 868 MHz und bieten niedrige Datenraten DR = 125 kBit/s. Dafür sind EnOcean-Strukturen robust und energiesparend.

Eventuell entstehen Interferenzen zu den folgenden Funknetzen:

- GSM, DECT – kommt aber relativ selten vor.
- ZigBee 802.15.4 – ist mit zu berücksichtigen.

Der Einsatz von EnOcean-Produkten erfolgt durch mehr als 50 Systemintegratoren, die ihre Endprodukte für die Gebäudeautomatisierung (Licht, Beschattung, Heizung/Klima/Lüftung), Industrieautomatisierung sowie die Automotive-Branche entwickeln und fertigen. Systeme EnOcean sind meist preisgünstiger als ihre Rivalen und genießen weitgehende Marktunterstützung (DE, FR, EU). Ein Nachteil der Technologie verglichen mit anderen WSN ist das Fehlen eines integrierten Sicherheitsmechanismus.

EnOcean ist ein gutes Beispiel für die beim Entwurf von WSN einzugehenden Kompromisse. Folgende Entwurfsentscheidungen wurden zur Anpassung an das geringe durch Energy Harvesting gewonnene Energieangebot getroffen [8, 9, 10, 11]:

- Single-Hop zum Cluster-Head: Flooding zwischen Cluster-Heads; Datenverarbeitung in Cluster-Heads;
- MAC-Schicht: keine Kollisionserkennung, aber Beaconing; unidirektionale Kommunikation zwischen Sensoren und Cluster-Heads;
- Begrenzte Energie: kurze Telegramme (1 ms) und Duty Cycle (0,1–1 %).

Integriertes Szenario mit WSN ◘ Abb. 12.37 führt ein integriertes Szenario mit LAN, WLAN, LON, WSN etc. auf für ein automatisiertes Büroambiente mit HLK (Heizung, Lüftung, Klimatisierung).

Das WSN besteht aus den räumlich verteilten autonomen Sensorknoten (SN), die zusammen mit LON und CAN ein kooperatives Monitoring von physikalischen und Umweltbedingungen übernehmen (u. a. Temperatur, Heizung, Schall, Ausstrahlung, Vibration, Druck, Bewegung oder Schadstoffkonzentration). Die Heterogenität des Szenarios wird durch

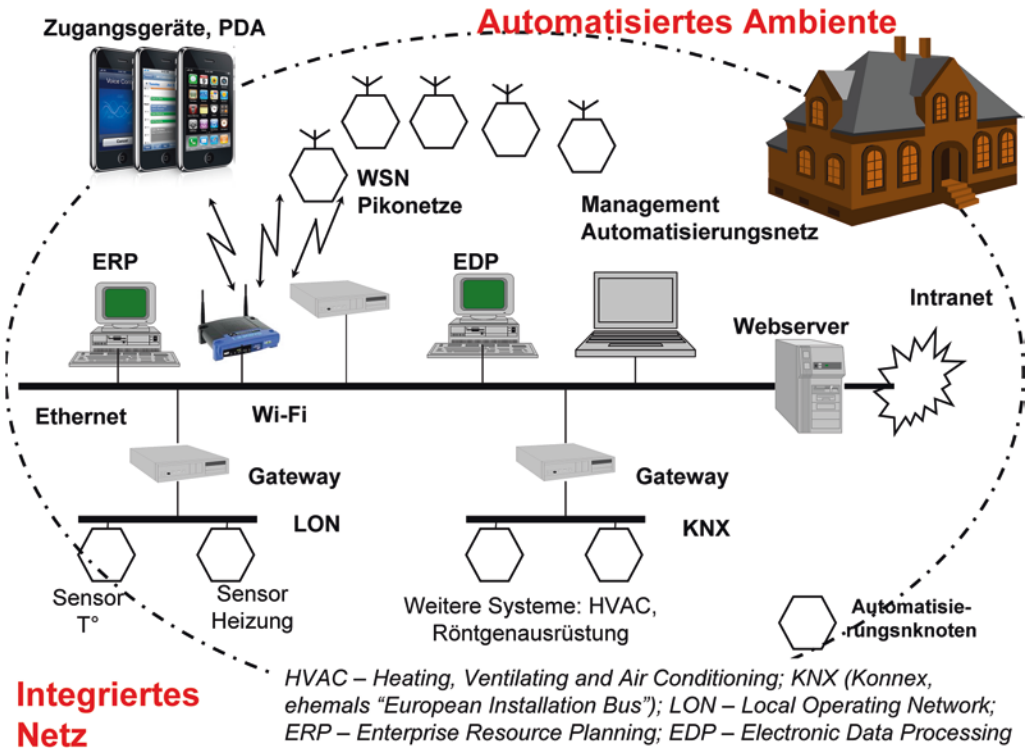


Abb. 12.37 Integriertes Szenario

12

Einsatz von IP-Gateways ausgeglichen. Die Integration mit Bürokommunikationsnetzwerken (LAN und Indoor-WLAN) erfolgt über Gateways (GW), die über Möglichkeiten verfügen, weitere Messungen und Rohdatenverarbeitung durchzuführen. Der Zugang zu den vorverarbeiteten Messergebnissen erfolgt über Web-Interfaces, Web Services sowie spezialisierte Middleware (u. a. OSGi, Open Services Gateway Initiative). Ein mobiler Zugang zu den erfassten Daten wird auch durch moderne Smartphones (WLAN, Bluetooth), mit installierten spezialisierten Apps gesichert.

12.7 Zwischenfragen/Übungsaufgaben

12.7.1 Ethernet

Weshalb darf die Framelänge bei Ethernet einen bestimmten Wert nicht unterschreiten? Wie groß ist dieser bei IEEE 802.3?

Schlagen Sie je eine kostengünstige Ethernetversion vor für nachfolgende Anforderungen und nennen Sie die für diese Version vorgeschriebenen Medien:

- Datenrate mindestens 1 GBit/s, Streckenlängen mindestens 500 m
- Datenrate mindestens 10 GBit/s, Streckenlängen nur 10 m
- Datenrate mindestens 30 GBit/s, Streckenlänge mindestens 5 km

12.7.2 WLAN

a) Welche grundlegenden Unterschiede und Gemeinsamkeiten bestehen zwischen leitungsgebundenen und drahtlosen LANs? Betrachten Sie dabei die Betriebsart, Management, Frequenzen, Fähigkeiten der Endgeräte, Dienste, nationale/internationale Regulierung!
b) Vergleichen Sie Infrastrukturnetzwerke und Ad-hoc-Netzwerke hinsichtlich Planungsaufwand, Robustheit, Komplexität der Endgeräte, Übertragungsraten und Routing!
c) Vergleichen Sie die Eigenschaften der elektromagnetischen Wellen in den für WLAN IEEE 802.11a/b/g/n/ac/ad verwendeten Frequenzbereichen!
d) Welche Lösungsmöglichkeiten bestehen für die Abdeckung größerer geographischer Gebiete bzw. Gebäude mit WLAN?
e) Erläutern Sie die MIMO-Technik am Beispiel von neuen WLAN-Standards!

Mobile Kommunikation

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_13

Mobile Zellularnetze integrieren Satellitenfunknetze sowie die konventionellen drahtgebundenen und drahtlosen Netze (Kerntechnologien). Mobile Zellularnetze werden in der Literatur üblicherweise in fünf Generationen 1G – 5G eingeteilt [10, 11, 13, 14, 15, 16, 17, 18, 19].

Dieser Abschnitt wird aufgebaut wie folgt:

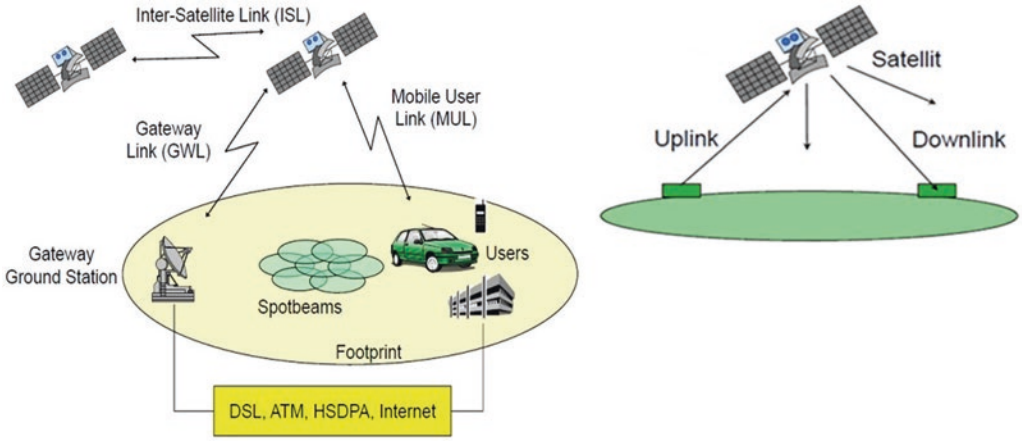
- Satellitenfunk (Architektur, Satellitenbahnen, Bewegungsgesetze, Dienste)
- Mobile Zellularnetze 1G – 4G (Entwicklungstrends und aktuelle LTE-Technik)
- 5G – Neue Generation des Mobilfunks (Forschungsfelder und Ausblick).

13.1 Satellitenfunk

13.1.1 Architektur und wesentliche Charakteristiken

Die terrestrische 4G-Architektur wurde um satellitenbasierte Funksysteme erweitert (◘ Abb. 13.1). Hauptmerkmale dieser Systeme sind [10, 11, 16, 17]:

- Aufbau von Gigazellen mit der Ausdehnung ca. 1000…10.000 km;
- mittlere bis große Nachrichtenlaufzeit (Latenz);
- große Frequenzbandbreite;
- viele verfügbare Übertragungskanäle;
- effiziente Zeitmultiplextechniken.



◘ **Abb. 13.1** Satellitenbasierte Funksysteme. (Quelle: ► rn.inf.tu-dresden.de)

Beispiel 13.1
Geostationäre Satelliten (GEOs) umfliegen die Erde in ca. 36.000 km Höhe. Dabei treten Latenzen von ca. 0,24 s auf, weil die Funkwellen 72.000 km auf dem Weg vom Sender über den Satelliten zum Empfänger zurücklegen müssen. Die hohe Latenz beeinflusst die Echtzeitkommunikation, aber die anderen Kommunikationsarten sind nicht betroffen.

Satelliten nutzen typischerweise verschiedene Frequenzen für den Up- und den Download, meist 4/6 GHz bzw. 12/14 GHz bei Bandbreiten von jeweils 500 MHz.

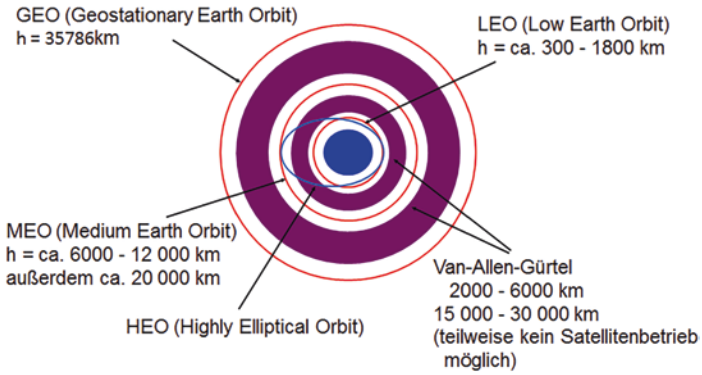
Dies ermöglicht Datenraten von 50 Mbit/s. Damit sind beispielsweise 800 digitale Sprachkanäle mit 64 kbit/s realisierbar (800×64 kBit/s = 50.000 kBit/s). Die Gesamtdatenrate wird dabei mittels der Zeitmultiplextechnologie auf die einzelnen Subkanäle aufgeteilt.

Satellitenbasierte Funksysteme enthalten die folgenden Komponenten:

- GGW – Gateway Ground Stations;
- Footprint (Abdeckungsbereich eines Systems mehrerer Satelliten);
- Spotbeams (phys. Ausleuchtungsbereich eines Satelliten);
- ISL – Inter-Satellite Links;
- MUL – Mobile User Links;
- GWL – Gateway Links.

IP-Backbone zur Ankopplung terrestrischer Gateways und stationärer Empfänger, realisiert z. B. über DSL, MPLS/ATM sowie regionalspezifische Technologien wie bspw. HSDPA, LTE.

Man unterscheidet verschiedene Satellitenklassen, die sog. GEO-, MEO-, LEO- und HEO-Satelliten (s. ◘ Abb. 13.2). Als Legende zur Abbildung gilt: LEO – Low Earth Orbit; MEO – Medium Earth Orbit; HEO – Highly-Elliptical Orbit; GEO – Geostationary Earth Orbit.



◘ **Abb. 13.2** Klassen von Satellitensystemen: GEO, MEO, LEO und HEO

13.1.2 Satellitenbahnen und -bewegungsgesetze

Die Satellitenbahnen können mit hoher Genauigkeit durch die Keplerschen Planetenbewegungsgesetze beschrieben werden (Johannes Kepler, 1571–1630). Außerdem basiert die Berechnung von Satellitenbahnen auf den Theorien von N. Kopernikus (1473–1543), G. Galilei (1564–1642) und I. Newton (1643–1727).

Wir nutzen folgende Formeln:
Kreisfrequenz mit Umlaufdauer T bzw. Umlauffrequenz f

$$\omega = 2\pi f = 2\pi/T \tag{13.1}$$

Nach Newton:
Erdanziehungskraft auf dem Niveau der Erdoberfläche.
(Erdradius R, Erdmasse M, Satellitenmasse m, Gravitationskonstante γ, Erdbeschleunigung g)

$$F_G = \gamma Mm/R^2 \tag{13.2}$$

$$\text{bzw.} \quad F_G = gm \tag{13.3}$$

$$\text{damit} \quad \gamma M = gR^2 \tag{13.4}$$

Erdanziehungskraft $F_G(r)$ und Zentrifugalkraft $F_Z(r)$ in Orbithöhe r

$$F_G(r) = \gamma Mm/r^2 = gR^2 * m/r^2 \tag{13.5}$$

$$F_Z(r) = m\omega^2 r \tag{13.6}$$

Gleichsetzen und Umstellen liefert

$$gR^2 * m/r^2 = m\omega^2 r \tag{13.7}$$

$$\text{bzw.} \quad r^3 = gR^2/\omega^2 \tag{13.8}$$

Berücksichtigung von (3.1) liefert

$$r^3 = gR^2T^2/(2\pi)^2 \tag{13.9}$$

Nach Johannes Keplers Satz: $T^2/r^3 = \text{const}$

Unter Berücksichtigung der Höhe h über dem Erdboden ergibt sich:

$$h = r - R \tag{13.10}$$

Mit den bekannten Werten von $g = 9{,}81\ m/s^2$, $R = 6370$ km, $T = 24$ h, ergibt sich für den Sonderfall geostationärer Satelliten (GEO) eine Distanz von $r = 42.156$ km bzw. eine Satellitenhöhe von 35.786 km. Äquivalent kann man erdnähere Bahnen berechnen (◘ Abb. 13.3).

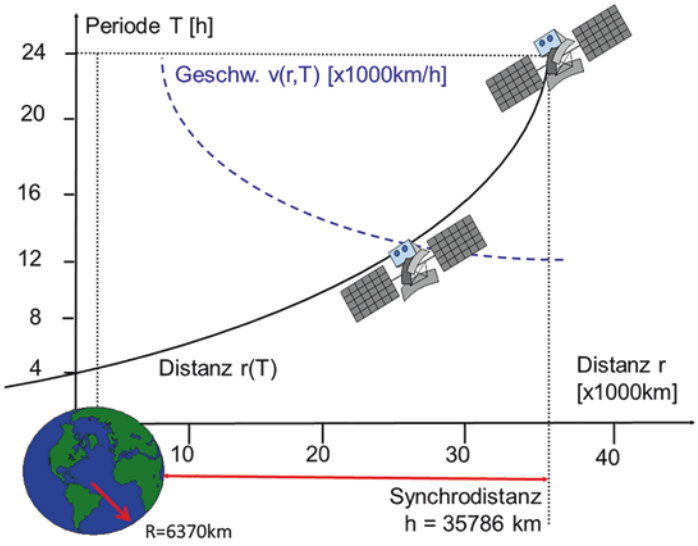


Abb. 13.3 Zusammenhang zwischen Umlaufzeit und Abstand zum Erdmittelpunkt. (Quelle: ► rn.inf.tu-dresden.de)

13.1.3 Systembeispiele

Die GEO- Systeme arbeiten im konstanten Erdabstand und besitzen einen relative hohe Latenz Δ:

$$\Delta = 2h/c = 2 \times 35.786 \text{ km}/300.000 \text{ km/s} = 0{,}239 \text{ s} \quad (13.11)$$

Im allgemeinen Fall besitzen die geosynchronen Umlaufbahnen einen Inklinationswinkel, z. B. von 0° Grad (geostationär), 90° (Polarbahn) bis zu 180° (sog. retrograde SAT mit Gegenläufigkeit zur Erddrehung). Die „reinen" GEOs haben die Inklination (Neigung) von 0° Grad, T = 24 h, h = 35.786 km und bewegen sich dem Äquator entlang. Im anderen Fall sind diese Satelliten vom Subtyp IGSO (Inclined Geosynchronous Orbit), d. h. die Inklination (Neigung) ist ungleich 0° Grad und besitzt einen 8-förmigen Footprint.

Die o. g. SAT-Systeme kommen zum Einsatz für die Navigation, Seeüberwachung, im SAT-Fernsehen und beim Air Traffic Control. Internetlinks sind zwar möglich, aber insbesondere Telefonie wird durch höhere Latenzen sehr beeinträchtigt.

Systembeispiele für GEO sind: Inmarsat, Eutelsat Hot Bird, Astra, Amos uvm.

Die nichtstationären LEO-Systeme sind charakterisiert durch:

- Abstand h von der Erde von ca. 300–1800 km;
- kurze Signallaufzeiten von 5–10 ms, niedrige Sendeleistung bei Eignung für Telefonie;
- jedoch sind zur Empfangsbereichsabdeckung mehr Satelliten erforderlich (>50) bei häufigen Übergaben (Handover) in Zeiträumen von ca. 10 min;
- kürzere Lebenserwartung (5–8 Jahre) wegen der atmosphärischen Reibung.

Systembeispiele sind: Iridium, Teledesic, Globalstar, ISS. ◘ Abb. 13.4 illustriert die ISS (Int. Weltraumstation) als bekanntestes LEO-Satellitensystem und der Menschheit erste Raumfahrt am 12.04.1961 (Juri Gagarin, Flugdauer = 108 min, Höhe h = ca. 400 km, LEO).

Die MEO-Systems operieren meist in Höhen über 10.000 km und erfordern eine geringere Anzahl von Satelliten (ca. 12 …24). Sie benötigen weniger Satelliten bei seltenerem Handover (Perioden ca. 6–13 h). MEO besitzen eine Lebensdauer bis zu 10 Jahren. Gegenüber LEO-Systemen besitzen sie eine höhere Signallaufzeit von 70 bis 80 ms, sowie höhere Sendeleistungen bei Eignung für Datenübertragung und Navigation [8, 11, 16].

Systembeispiele sind: ICO RTT (SAT-Links für 3G/4G), Navigationssatellitensysteme.

Ein Vergleich der verschiedenen Systeme wird in ◘ Tab. 13.1 und 13.2 gegeben. Die wichtigsten Kennwerte von Kommunikationssatelliten sind: Klassen, Dienste und Anwendungsbereiche, Anzahl von Transpondern, lizensiertes Frequenzband, Orbithöhe, Umlaufperiode, Datenrate, Sendeleistung, Signalverzögerung (Latenz), Einsatzdauer.

Die Navigationssysteme (◘ Tab. 13.3) stellen ein wichtiges und bekanntes Beispiel für die Nutzung von MEO-Satelliten dar (teilweise in Kooperation mit GEO-Satellitensystemen sowie geosynchronen SAT-Systemen).

◘ Abb. 13.4 LEO – Satellitensysteme. (Quelle: ▶ reflektion.info, NASA)

Tab. 13.1 Systembeispiele von Satellitenfunk [8, 10]

SAT-Typ	Klasse	Orbit, h	Anzahl von Satelliten	F-Band	DR. max	Services
Orbcomm	LEO, 2000, ursprünglich kommerziell,	775–800 km	27 kleine Satellite, m = 45 kg; 2G – seit 2014 further 18	VHF band, 137–150 MHz	48–57,6 kbit/s	Emails, Telefonie
Inmarsat	GEO, 1979 kommerziell	35.786 km	5–11, fünf Generationen!	–	492 kbit/s	Navigation, TV, Internet-Links, Seeüberwachung, Air Traffic Control, Kooperation mit GPS, EGNOS
Globalstar	LEO, 1991–1994	1400 km	48 + 4	–	144 kbit/s mit Kanalbündelung	Telefonie, Datentransfer data
ICO RTT	MEO, 1998–2000	10.390 km	10 + 2	–	–	Telefonie, Datentransfer data
Teledesic	LEO, 1997–2002	700 km	288, m = 120 kg	28,6–29,1 GHz	100 MBit/s UL, 720 Mbit/s DL	Telefonie, Internetlinks
Iridium	LEO, 1997–1998	780 km	66 (+6)	–	2,4/4,8 kbit/s	Telefonie, Datentransfer

Tab. 13.2 Vergleich von Satellitenfunk: GEO-, MEO-, LEO-Systeme [8, 10]

Satellitenklasse, Inbetriebnahme, Anzahl und DR-Nennwerte	GEO	MEO	LEO
Distanz, km	h = 35.786 km; r = 42.156 km	r-R = 6000–12.000 km, respectively 20.200	r-R = 300–1800 km
Periode, T	24 h	6–12 h	90–120 min
Latenz, t	0,25 s	70–80 ms	10 ms
Sendeleistung, W	10	5	1
Einsatzbereich	ca. 2000 SAT: Intelsat 1–3 (1965, 1967, 1969), Marisat (1976), Inmarsat-A (1982), Inmarsat-C (1988) etc.	ICO 10+2	Iridium – 66+6 Globalstar – 48+4/144 kBit/s Teledesic (2003) – 288/2–64 MBit/s Orbcomm – 35
Typische Datenrate, kBit/s	0,1–1	10	1–64.000
Mittlere Lebenserwartung, Jahre	15	10	5–8

Tab. 13.3 Vergleich von SAT-Navigationssystemen [8, 10]

Typ des Navigationssystems	Höhe, h	Periode, T	Anzahl von Satelliten	Stand 2016
GPS (USA)	20.200 km	12 h	31 (24 erforderlich)	Betrieb
GLONASS (RF)	19.100 km	11 h 15′	28	Betrieb
Galileo (EU)	23.222 km	14 h	30	Im Aufbau
Beidou (China)	21.500 km + GEO + geosynchrone SAT	12 h 52′ für MEO	21 (35 erforderlich)	seit 2004 für den asiatischen Bereich in Betrieb, weltweit verfügbares Netz befindet sich im Aufbau
IRNSS (Indian Regional Navigation Satellite System)	35.786 km (nur geosynchrone Satellitensysteme)	24 h	7 (nur 7 erforderlich)	Im Aufbau

13.2 Mobile Zellularnetze 1G-5G

Die konventionellen Telekommunikationstechniken integrieren mobile Zellularnetze und Satellitenfunknetze und werden üblicherweise in der Literatur eingeteilt in fünf Generationen (Abb. 13.5). Im Schnitt passiert der Generationswechsel aller 10 Jahre. Die Spitzendatenraten der einzelnen Generationen zeigt die Abbildung.

Einen Vergleich existierender Generationen von Mobilfunknetzen gibt Tab. 13.4:

Die Generationen (Kürzel G) begannen mit 1G und 2G/Global System for Mobile Communications (GSM) mit einigen Erweiterungen. Danach folgten 3G/Universal Mobile Telecommunications System (UMTS) die beschleunigte Version High Speed Download Packet Access (HSDPA) (mitunter bezeichnet als 3.5G). Diese Technik hat sich weltweit durchgesetzt und wird schrittweise durch 4G/Long-Term Evolution (LTE) abgelöst und zu LTE Advanced weiterentwickelt. Mittelfristig konzentrieren sich die Forschungsaktivitäten auf 5G bzw. auf den künftigen Standard für International Mobile Telecommunications (IMT) 2020.

Die modernste 5.-te Generation 5G wird mittelfristig eingeführt, wahrscheinlich nach 2020, nachdem die hohen Entwicklungs- und Investitionskosten für die aktuelle 4G sich amortisiert haben.

Zellulare Funknetze erlauben die Einteilung großer geografischer Bereiche in Funkzellen, die jeweils unterschiedliche Frequenzen nutzen.

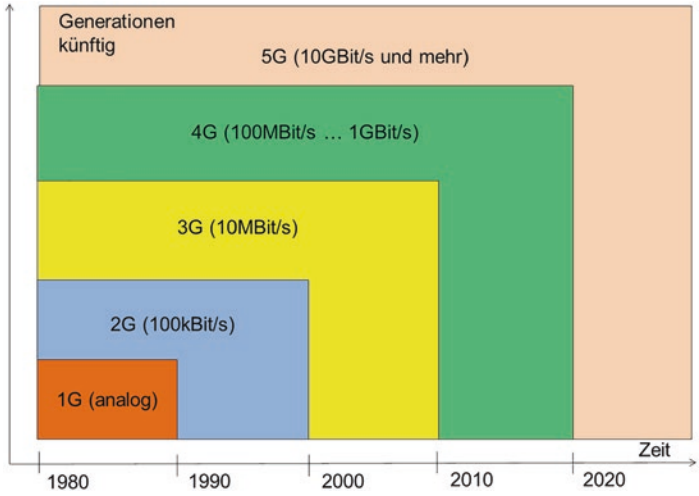


Abb. 13.5 Generationen des Mobilfunks

Tab. 13.4 Vergleich der Eigenschaften von fünf Generationen des Mobilfunks. (Quelle: ► www.elektronik-compendium.de)

Generation	Technologie	Übertragungstyp	Datenrate
1G	AMPS	Analog, leitungsvermittelt, veraltet!	–
2G	GSM	Digital, leitungsvermittelt	9,6 kbit/s
2.5G	HSCSD	Digital, leitungsvermittelt	57,6 kbit/s
	GPRS	Digital, paketvermittelt	115 kbit/s
2.75G	EDGE	Digital, paketvermittelt	236 kbit/s
3G	UMTS/UTRA FDD	Digital, meist paketvermittelt	384 kbit/s
3G	UMTS/UTRA TDD	Digital, paketvermittelt	2 Mbit/s
3.5G	HSPA (HSDPA, HSUPA)	Digital, paketvermittelt	14,4 Mbit/s
3.9G	LTE	Digital, paketvermittelt	150 Mbit/s
4G	LTE Advanced	Digital, paketvermittelt, aktueller Standard	1 Gbit/s
5G	IMT2020	Digital, paketvermittelt	10… 100 Gbit/s

Die aktuelle 3G/4G-Architektur von Mikro- und Makrozellen kann ergänzt werden durch die Anbindung von Satellitenfunk (Gigazellen) sowie WPAN, WLAN, WiMAX usw. Dadurch entstehen hierarchische Strukturen, u. a. extragroße und nichtterrestrische Zellen bis zu kleinen Pikozellen (s. Tab. 13.5).

Tab. 13.5 Hierarchische Zellstruktur für Mobilfunk [8, 10, 16]

Zelltyp	Zellgröße	DR (Mbit/s)	Mobilität (km/h)	Einsatz in 2G, 3G, 4G
Gigazellen (World Cell)	ca. 100 km	0,144 … 10 kbit/s	1,3 km/s, ca. 4700 km/h	Transnationale Netze, Satelliten (nichtterrestrisch)
Makrozellen	ca. 10 km	0,144… 0,384	Ca. 500 km/h	Campus, Stadtgebiete
Mikrozellen	ca. 100 m	0,384 … 2	Ca. 120 km/h	Gewerbegebiete
Pikozellen	ca. 10 m	2 … 100	10 km/h	Hotspots

Die Zellgröße wird bestimmt durch die Eigenschaften der Antennen (Reichweite, Gewinn) und der Funkelektronik (Sendeleistung, Empfangsempfindlichkeit).

Je größer die Zelle ist, umso mehr Teilnehmer können erfasst werden. Anderseits sind höhere Signalstärken und ein komplizierteres Verbindungsmanagement erforderlich. Femtozellen besitzen die kleinsten Zellgrößen, sind meist in Wohnanlagen installiert, erlauben bis zu 16 parallele Verbindungen und sind kompatibel zu WLAN.

Beispiel 13.2

Nach Angaben der Experte gibt es eine enorme nutzergetriebene Steigerung der Datenraten bis 2022.
Aufgrund dessen wird Wachstum des mobilen Datenverkehrs weltweit 2020-2021 bis zu 40-50 Exabyte/Monat prognostiziert.

Im Jahr 1993 betrug die 2G-Datenrate 0,2 MBit/s, deshalb war die Sprachübertragung über das (mobile) Internet nicht praktikabel.

Die 3G-Zeit begann 2001 mit der Einführung von UMTS mit einer permanent verbesserten Datenrate beginnend mit 0,39 MBit/s. Im Jahr 2008 wurden mit der Erweiterung HSPA 7,2 und zwei Jahre später mit HSDPA+ sogar 42 Mbit/s erreicht.

Die Generation 4G (LTE) startete 2011 mit 150 Mbit/s und wurde 2014 mittels LTE Advanced auf 450 Mbit/s gesteigert.

Weil sowohl LTE-Netzwerke als auch Satellitenfunksysteme den aktuellen Stand der Technik darstellen, werden sie im Folgenden näher erläutert.

13.2.1 OFDM-basierte Systeme

Die Bezeichnung OFDM steht für Orthogonal Frequency-Division Multiplexing. Obwohl das Konzept schon Jahrzehnte

bekannt war, gab es erst ab ca. 1990 praktische Realisierungen durch schnelle Schaltkreise (Fast-Fourier-Transformation).

Zu den praktischen Beispielen gehören DSL, einschließlich ADSL und VDSL, DAB und DVB-T, WiMAX und Bluetooth sowie moderne WLAN-Netzwerke auf der Basis von IEEE 802.11g, 11n oder höher. Die konsequente Nutzung von OFDM in WLAN-Netzwerken führte zu signifikanten Erhöhungen der Datenrate aufgrund optimaler spektraler Effizienz, die sich auf das Verhältnis von Datenrate zu Kanalbandbreite bezieht. Mit dieser Technik lassen sich Datenraten von ca. 600 MBit/s und eine Reichweite von 70 m innerhalb von Gebäuden und 250 m außerhalb von Gebäuden erreichen.

OFDM realisiert zeitparallele Signalströme über verschieden Teilfrequenzen (carrier) eines Frequenzbandes (Multiplexing). OFDM ist charakterisiert durch eine hohe spektrale Effizienz.

Signale besitzen eine Trägerfrequenz und belegen darüber und darunter einen kleinen Frequenzbereich Eine Besonderheit von OFDM ist, dass Frequenzüberlappung eingeschränkt möglich ist, falls die Trägerfrequenzen zueinander „orthogonal" sind. Orthogonalität zweier benachbarter Frequenzen liegt dann vor, wenn der Trägerfrequenzabstand derart ist, dass beim Leistungsdichtemaximum des einen Signales die Leistungsdichte des Nachbarsignales einen Nulldurchgang aufweist. Die Technik ist robust gegenüber Schmalbandstörungen.

OFDMA (Orthogonal Frequency Division Multiple Access) ist eine verbesserte OFDM-Variante, die mehreren Nutzern je nach Bedarf evtl. sogar mehrere orthogonale Frequenzen zuweisen kann [66].

Kurz gesagt, OFDMA ist OFDM-Zuordnung „on Demand". Die Beziehung zwischen OFDMA, OFDM und „klassischem" Frequenzmultiplex (FDM – Frequency Division Multiplexing) ist in ◘ Abb. 13.6 zusammengefasst.

13.2.2 Fortgeschrittene Modulation FQAM und MIMO-Strukturen

Die in OFDM eingesetzten Modulationsverfahren reichten jedoch nicht mehr für erhöhte Anforderungen. Die Methoden BPSK, QPSK, 16QAM und 64QAM haben insbesondere eine sehr ungleiche Energieverteilung. Im Zentrum der Zelle ist die Energiedichte höher als nötig, dagegen ist sie an den Zellrändern kritisch.

Innerhalb von 5G werden wesentliche Leistungsverbesserungen erreicht über das neue, erweiterte Modulationsverfahren mit dem Titel FQAM (Feher's Quadrature Amplitude Modulation), speziell eine Erhöhung der Zellkapazität und eine

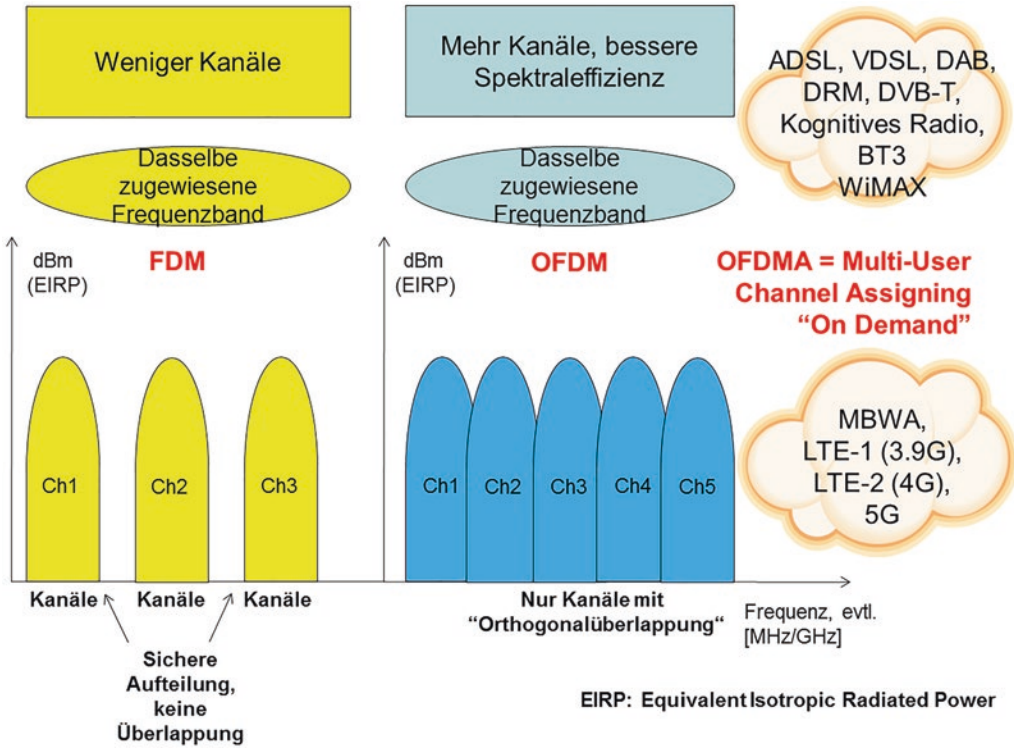


Abb. 13.6 Bessere Spektraleffizienz (Nutzung vom Frequenzband) bei OFDM und OFDMA

13

bessere Energieverteilung innerhalb einer Funkzelle. Erreicht wird eine möglichst gleichmäßige Energieversorgung, insbesondere eine bessere Versorgung der Empfänger an den Zellrändern. FQAM wird auch als Post-OFDM-Methode bezeichnet.

Die Implementierung von 5G erfordert, dass leistungsstärkere MIMO-Verfahren in einer typischen Kombination bereitgestellt werden: Mehrbenutzer-MIMO mit 3D-Arrays von Antennen. Multi-User MIMO (MU-MIMO) ist ein Satz moderner MIMO-Antennen, die nicht nur in einem 2D-Raster, sondern in einem 3D-Würfel angeordnet sind [8, 10].

Die 5G-Systeme nutzen sowohl MU-MIMO als auch deren Erweiterung: FD-MIMO (Full-Dimension MIMO). FD-MIMO ermöglicht die eigentliche Bereitstellung der 3D-Arrays von Antennen. Diese Strukturen besitzen die folgenden Parameter (M, N, K), wobei M horizontale Antennen sind, N vertikale Antennen und K Antennen pro Subarray. Zum Beispiel sind (8, 4, 2) -Strukturen typisch für 5G-Hardware. Die Verwendung solcher fortgeschrittenen MIMO-Strukturen (MU-/FD-MIMO) zeigt ◘ Abb. 13.7.

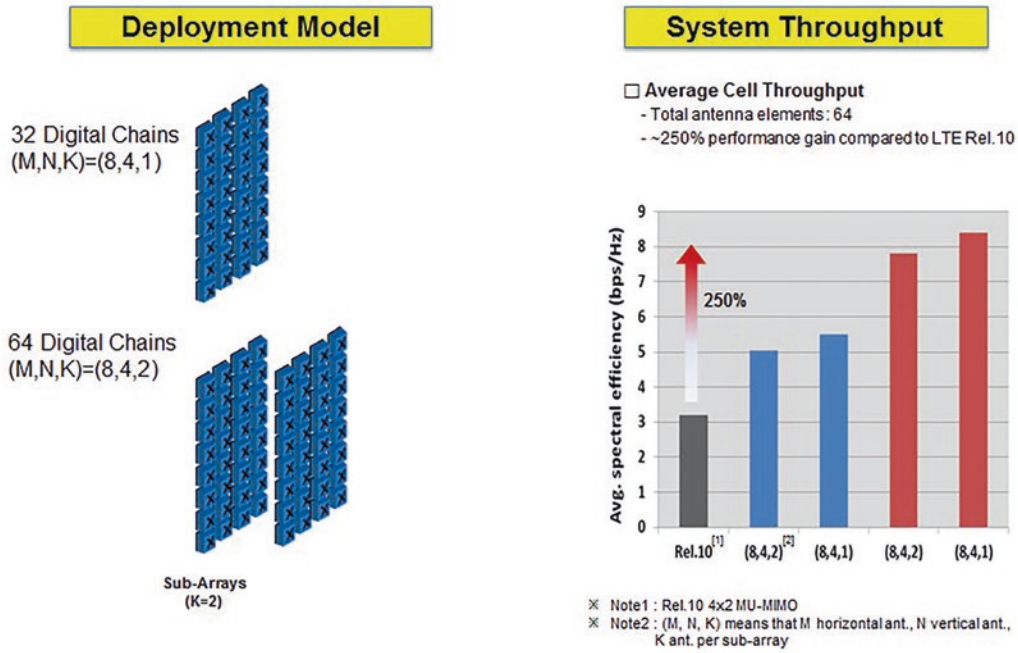


Abb. 13.7 Fortgeschrittene 3D-MIMO-Strukturen

13.2.3 4G und LTE: aktuelle Mobilfunknetze

Die Mobilfunktechnologie LTE (Long Term Evolution) wurde 2004 durch 3rd Generation Partnership Project (3GPP) initiiert. Die Vorteile liegen in der Erweiterung von HSDPA mit höheren Datenraten bis 1000 MBit/s Downlink und 75 MBit/s Uplink bei aufrechterhaltener UMTS-Kompatibilität. Die Spektraleffizienz liegt bei 1…3 Bit/s/Hz, gegenüber 0,2 Bit/s/Hz bei 3G.

Die Datenratenerhöhung erfolgt mittels der zugrunde legenden Kombination vom adaptiven OFDMA (Orthogonal Frequency Division Multiplex Access) und verbesserten MIMO-Antennen (MIMO – Multiple Input – Multiple Output). Eine große Flexibilität bietet der Einsatz flexibler Kanalbandbreiten (von 1,4 MHz bis 20 MHz) im Vergleich zu UMTS mit einer statischen Bandbreite von 5 MHz pro Kanal. Daraus folgt eine bessere Adaptation zu den Netzwerknutzungsmustern mit sehr kleiner Latenzzeit unter 5 ms.

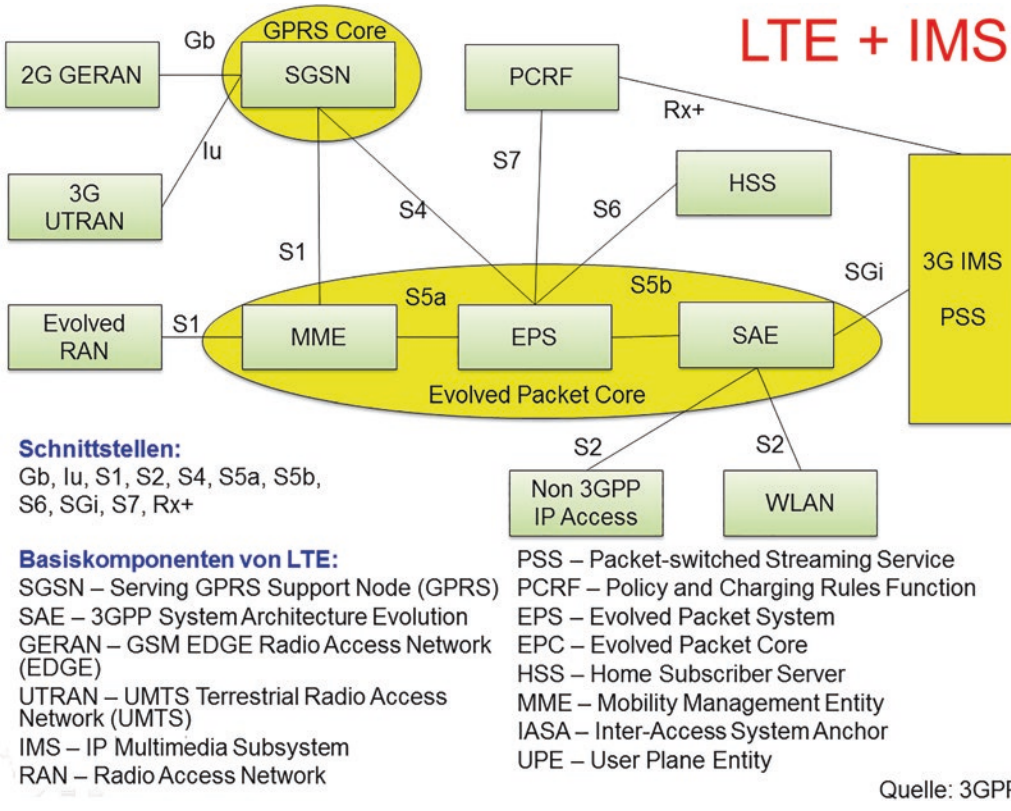
Derzeit sind LTE und LTE-II (LTE Advanced) offizielle Standards bei mehreren Provider-Implementierungen weltweit. In Deutschland hat die Bundesnetzagentur 2010 die Frequenzen in den Bereichen F = 0,8 GHz, F = 1,8 GHz, F = 2 GHz und 2,6 GHz (ehemals von UMTS) für die LTE-Dienste zugewiesen.

LTE bietet auch die Basis zur Bereitstellung von IMS (IP Multimedia Subsystem). Dabei nutzt das IMS das effiziente SIP-Protokoll (Session Initiation Protocol, RFC 3261), um

Telefondienste anzubieten. Die Systemarchitektur in der Kombination von LTE und IMS ist in ◘ Abb. 13.8 dargestellt. Die Grundkomponenten dieser Architektur sind [11]:

- SGSN – Serving GPRS Support Node (GPRS);
- SAE – 3GPP System Architecture Evolution;
- GERAN – GSM EDGE Radio Access Network (EDGE);
- UTRAN – UMTS Terrestrial Radio Access Network (UMTS);
- IMS – IP Multimedia Subsystem;
- PSS – Packet-switched Streaming Service;
- PCRF – Policy and Charging Rules Function;
- EPS – Evolved Packet System;
- EPC – Evolved Packet Core;
- HSS – Home Subscriber Server;
- MME – Mobility Management Entity;
- IASA – Inter-Access System Anchor;
- UPE – User Plane Entity.

Das System basiert auf GPRS, EDGE, UMTS-Technologien (GERAN, UTRAN, SAE) und ist vollständig paketorientiert. Die IMS-Plattform ermöglicht Voice over IP (VoIP) mit



◘ **Abb. 13.8** Referenzarchitektur von 4G/LTE (Long Term Evolution)

Unterstützung herkömmlicher Protokolle (◘ Abb. 13.9) sowie Datendienste auf Basis von SIP und anderen standardisierten Protokollen.

Die Referenzarchitektur sichert die Interoperabilität mit herkömmlichen 3GPP-Funktechnologien (vgl. Abb. Architektur LTE). LTE koexistiert mit UTRAN (3G) und GERAN (EDGE).

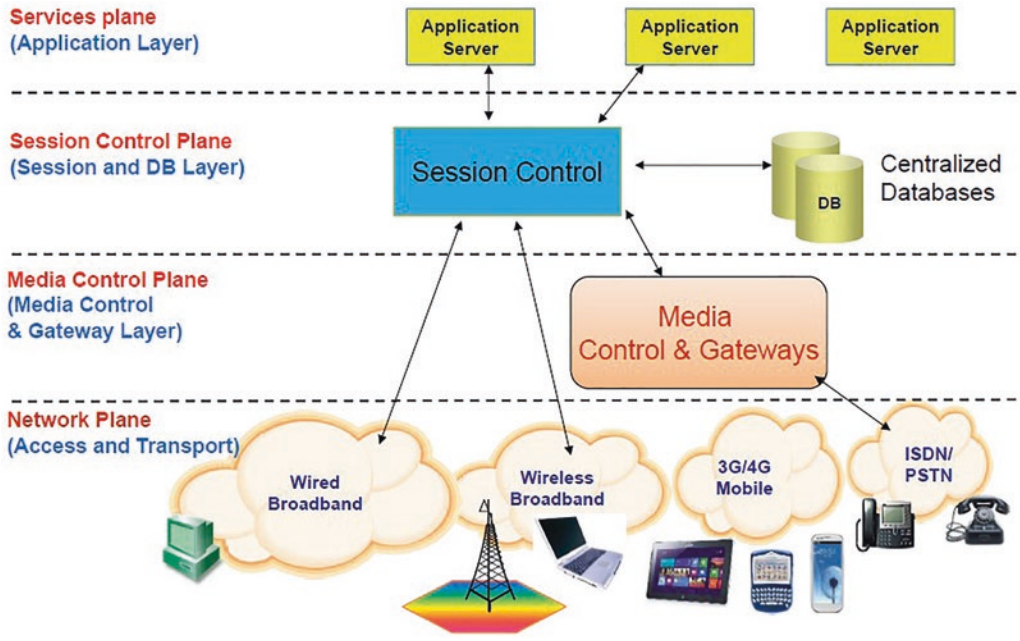
Eine Optimierung für die Paketübertragung und die Unterstützung von IP-Multimedia Subsystemen (IMS) mit sämtlichen Zugangstechnologien wurde dabei vorgesehen [11, 16].

Als Bausteine der UTRA-UTRAN Long Term Evolution Technologie gelten u. a. (vgl. Abb.):

- **Technologie SGSN** - Serving GPRS Support Node (Infrastruktur von GPRS)
- **Technologie GERAN** - GSM EDGE Radio Access Network (Infrastruktur von GSM/EDGE)
- **Technologie 3GPP** - System Architecture Evolution (SAE).
- **IMS** - IP Multimedia Subsystem usw.

LTE bietet deutliche Verbesserungen beim Medienzugriff:

- Multiplexverfahren:
  Downlink: Orthogonal Frequency Division Multiplexing (OFDM)
  Uplink: Single Carrier-Frequency Division Multiple Access (SC-FDMA)



◘ **Abb. 13.9** IMS Architektur mit vier Ebenen

- Modulationsverfahren:
  Downlink: QPSK, 16QAM, 64QAM
  Uplink: BPSK, QPSK, 8PSK, 16QAM.
- 5-fach erhöhte Spektraleffizienz (SE):
  im Vergleich zu 3G ($5 \times 0{,}2$ Bit/s/Hz/Zelle = 1 Bit/s/Hz/Zelle)!

Innerhalb von IMS-Architektur werden vier Ebenen definiert und die folgenden Komponenten benutzt: AS – Application Server; CSCF – Call Session Control Function; BGCF –Breakout Gateway Control Function; MGCF – Media Gateway Control Function; MGW – Media Gateway. Die erste Ebene ist die Benutzerebene oder das Gateway, welches das System mit einem IP-Uplink verbindet. Die zweite ist die Steuerungsebene oder die Gatewaysteuerung. Durch diese Ebene werden Anruferidentifizierungs- und Abrechnungsinformationen ausgetauscht. Die dritte ist die Rufsteuerung (session control). Die vierte ist die Dienstefunktionsebene. Sie enthält unter anderem Funktionen zur Überprüfung der Verbindungsqualität für Notrufe, zur Verbindung zu Messaging-Diensten (SMS) und zur Anbindung von Prepaid-Anrufen an das System. Die Authentifizierungs-, Autorisierungs- und Abrechnungsfunktionalität muss durch die Kommunikationspartner abgesichert werden. Das Diameter-Protokoll (RFC 6733) wird dafür innerhalb von IMS verwendet.

IMS basiert grundsätzlich auf der herkömmlichen Architektur für multimediale Kommunikation für die „klassischen Festnetze“ mit der Vielfalt der Protokolle und Codecs für VoIP, Telekonferenzen (s. ◘ Abb. 13.10), wobei die primäre Rolle der Einsatz von SIP und RTP spielt.

13.2.4 Mobilfunknetze – MBWA

Der heute eher obsolete Standard IEEE 802.20 für drahtlose Netze war gewissermaßen ein Versuch der Weiterentwicklung des wohlbekannten Standards IEEE 802.16. Die Abkürzung „MBWA“ steht für den „Mobile Broadband Wireless Access“. Aktuell wurde die Weiterentwicklung des Standards de-facto eingestellt. Diese Technologie ist außerdem als „iBurst“ bekannt. Die erwähnte Technologie MBWA/iBurst suchte eine eigene Nische zwischen Wi-Fi (WLAN) und dem Mobilfunk (UMTS, HSDPA, LTE-I, LTE-II und 5G mittelfristig).

Der MBWA-Standard unterstützt adaptives Multiplexing mit Übergangsmöglichkeiten zwischen TDD, FDD und Half-Duplex FDD sowie der Nutzung von adaptiven Kanalbandbreiten von 5, 10 und 20 MHz. Des Weiteren verfügt MBWA über die folgenden Vorteile:

- höhere Mobilität von 250 km/h bis 350 km/h und Datenraten von 1 MBit/s bis 80 MBit/s mit Automotive-Anwendung.
- Kleine Latenzzeiten, variable Zellgrößen mit mehr als 100 gleichzeitigen Sessions je Sektor.

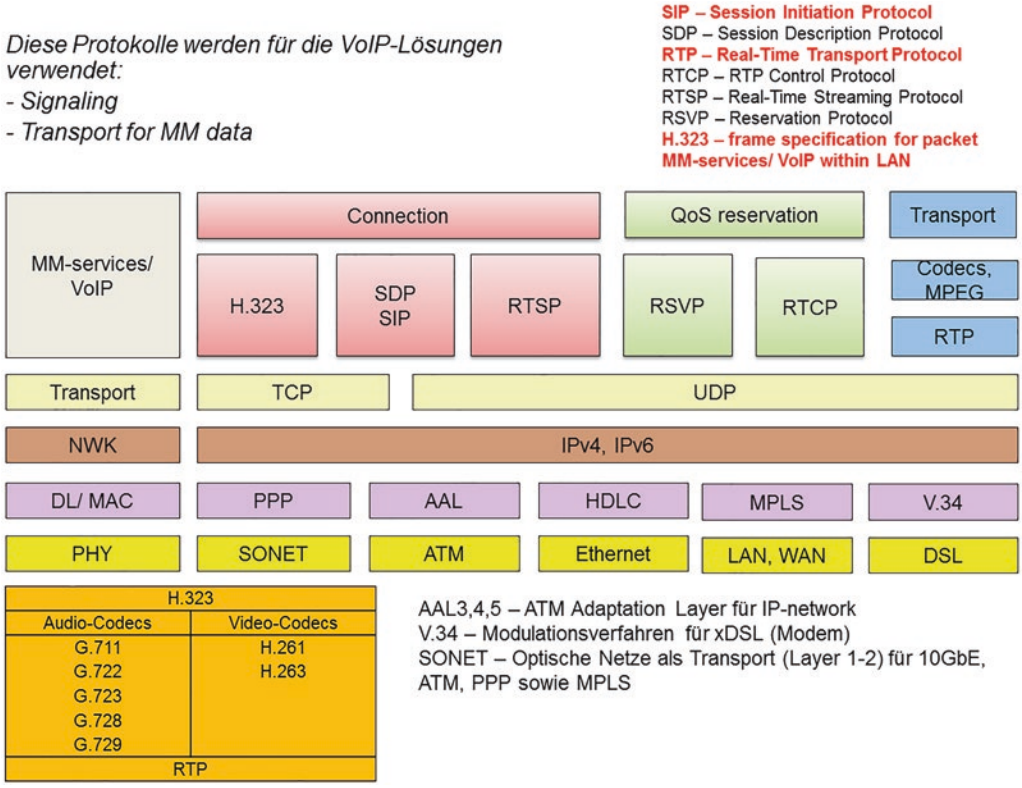


Abb. 13.10 Allgemeine Architektur für herkömmliche Protokolle für VoIP und Multimedia

- Einsatz im Modus NLOS (non-line-of-sight) für In- und Outdoor-Kommunikation.
- Handover- und Roaming-Mechanismen.
- Paketorientierung und IP-Datenverkehr, QoS pro Verbindung (Layer 4).

Die Technologie ist auf lizenzpflichtige Bänder unterhalb 3,5 GHz mit variablen Bandbreiten orientiert. Die Spektraleffizienz (SE) des Verfahrens MBWA ist sehr hoch mit SE $\geq$ 1 Bit/s/Hz im Vergleich zu UMTS mit 0,2 Bit/s/Hz/Zelle für UMTS/CDMA. Die Technologie implementiert außerdem Datensicherheitskonzepte, u. a. ist End-to-End-Security (Layer 4) mittels AES obligatorisch.

Außerdem unterstützt MBWA schmalbandige Sprachdienste mit verringerter Datenrate und bis zu 100 Telefongespräche je 1 MHz Bandbreite. Für die Optimierung des Signal-Rausch-Abstandes wird ein fortgeschrittenes Modulationsverfahren verwendet: layered frequency hopping FHSS + OFDM (Frequency Hopping Spread Spectrum + Orthogonal Frequency Division Multiplex).

Einige Nachteile von MBWA sind:

- Kostenpflichtige Lizenzen bei F = 3,5 GHz.
- Bereitstellung von QoS ausschließlich über die Transportschicht (Layer 4).

13.3 5G – Neue Generation des Mobilfunks

13.3.1 Anforderungen und Visionen zu 5G

Eine sehr bekannte Definition für 5G als neue Generation der mobilen Kommunikation ist in [8, 9, 10] zu finden:

„In der evolutionären Sicht wird 5G in der Lage sein, drahtloses WWW zu unterstützen, die hochflexible dynamische Ad-hoc-Funknetze ermöglichen. In revolutionärer Hinsicht ist diese intelligente Technologie in der Lage, die ganze Welt ohne Grenzen zu verbinden".

Diese sehr breite Definition unterstreicht die neuen Anforderungen und motiviert uns, einen weiteren Blick auf die Mobilkommunikationsgenerationen zu werfen.

Vermerk

Die Inhalte des Manuskripts zu diesem Buchprojekt wurden bis inkl. Mai 2018 sorgfältig erarbeitet.
Die beschriebenen technischen Details sind i. W. auch heute hochaktuell, was für die Telekommunikationsbranche ganz wichtig ist.

Die Netzwerkspezialisten von der Deutschen Telekom, Samsung, Huawei, NTT DoCoMo, Amtel, Telefonica, Vodafone, Ericsson und von anderen Telekommunikationsbetreibern [10] arbeiten intensiv an den Vorstellungen zur Mobilkommunikation der Zukunft, den technischen Voraussetzungen sowie am neuen Standard 5G/IMT 2020.

Die Verwendung von Frequenzen, die wesentlich über 5 GHz liegen (Wellenlänge im mm-Bereich), ist aufgrund der starken Dämpfung in dichten Stadtgebieten problematisch. Eine Erhöhung der Sendeleistungen zur Verbesserung der Reichweiten ist nur begrenzt erlaubt. Auf der anderen Seite ist eine niederfrequente Übertragung nicht immer möglich: notwendige Lizenzen und (inter-) nationale Regelungen sind Hindernisse. Daher sind andere neue Methoden und internationale Abstimmungen und Konventionen erforderlich.

Die Forschung über die 5G-Technologie erzielte erste Erfolge im Jahr 2012 in Frankreich mit dem Erreichen von Datenraten über 4 GBit/s. Im Jahr 2013 wurden durch die japanische Firma

NTT DoCoMo Mobilfunkkomponenten vorgestellt, die Datenraten bis zu 10 GBit/s (Uplink) erreichen bei einer Frequenz von 11 GHz und einer Bandbreite von 400 MHz. Die Messungen wurden dabei zum Teil an Fahrzeugen mit einer Geschwindigkeit von 9 km/h durchgeführt. Eine weitere Steigerung der Leistungsparameter erreichte das Unternehmen Samsung Electronics im Oktober 2014 mit Datenraten von 2 GBit/s bei einer Fahrzeuggeschwindigkeit von 110 km/h und Datenraten von 7,5 GBit/s bei stationären Bedingungen. Dabei wurde eine Frequenz um 28 GHz genutzt.

Obwohl der offizielle 5G-Start meist für die Jahre 2020–2021 eingeplant wurde, gibt es mittlerweile einige Länder und Mobilfunkprovider, die 5G-Systeme schon erfolgreich eingesetzt haben.

Der aktuelle 5G Status Quo sieht folgendermaßen aus:

- Im Juli 2019 wurde in Deutschland nach erfolgreichen Tests das Mobilfunknetz der 5. Generation eingeführt (Deutsche Telekom, Vodafone, Telefonica Germany).
- Die Schweiz hat die 5G-Frequenzbänder 2019 drei großen Anbietern zugeordnet: Swisscom, Sunrise und Salt. Im Juli 2019 wurden im Land 334 Antennenmasten mit 5G-Frequenzen in Betrieb genommen.
- Ausbau der 5G-Infrastruktur und Antennentechnologie (3D-MIMO) erfolgt europaweit und in den USA
- Huawei und Samsung gelten mittlerweile als die größten Software- und Hardware-Hersteller für 5G-Systeme weltweit.
- Die aktuellen Forschungen konzentrieren sich vor allem auf fortgeschrittene Antennentechniken und Methoden zur Interferenzminimierung. Besondere Zentren der Forschung, Entwicklung und Testung sind u. a. Ishigaki (NTTDoCoMo), Seoul (Samsung), Stockholm (Ericsson), Dresden (Vodafone Chair, 5GLab@TU Dresden), London (King's Royal College), Lund University (Schweden) und Peking (Huawei).

Der heutige Stand der Systemarchitektur ist in ◘ Abb. 13.11 dargestellt [3, 4, 6, 7, 8, 9, 10].

Legende zur 5G-Architektur:

- 4G mit SAE – 3GPP System Architecture Evolution;
- GERAN – GSM EDGE Radio Access Network (EDGE);
- UTRAN – UMTS Terrestrial Radio Access Network (UMTS);
- IMS – IP Multimedia Subsystem;
- SDN – Software-Defined Networking;
- RAT – Radio Access Technology (Handover);
- DIDO/Multiuser-Wireless;
- MIMO, mehrere Tx/Rx-Antennen.

Die aktuellen Forschungen konzentrieren sich vor allem auf fortgeschrittene Antennentechniken und Methoden zur

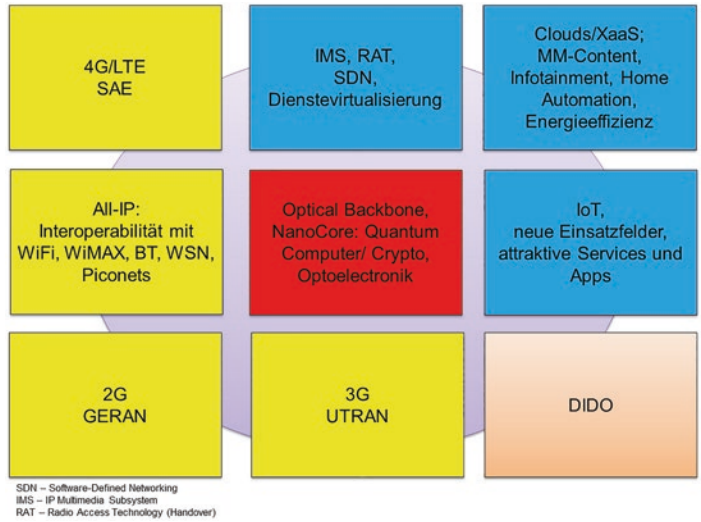


Abb. 13.11 Architektur 5G

Interferenzminimierung. Besondere Zentren der Forschung, Entwicklung und Testung sind u. a. Ishigaki (NTTDoCoMo), Seoul (Samsung), Stockholm (Ericsson), Dresden (Vodafone Chair, 5GLab@TU Dresden), London (King's Royal College), Lund University (Schweden) und Peking.

Die wichtigsten 5G Anforderungen sind wie folgt:

- Weltweite Nutzung der bestehenden 4G-Infrastruktur mit Erweiterung durch flexible WLAN-konforme Kommunikation unter internationalen Abstimmungen und Konventionen;
- Mittelfristiges Erreichen der Datenrate von 10 GBit/s;
- Diese Rate entspricht den aktuellen Anforderungen an den Download von Multi-Media-Inhalten;
- Sehr geringe Latenzen, Echtzeiteignung
- Breite Nutzung der verfügbaren Frequenzbänder: mm-Band mit F = 30 bis 300 GHz;
- Interoperabilität mit alternativen mobilen und drahtlosen Funknetzen.

Die fortschrittliche Antennentechnik MIMO wird bereits in diversen Netzwerktechnologien wie WiMAX 802.16a/d/e/m, WLAN 802.11n/ac/ad, LTE und anderen eingesetzt. MIMO-Antennen ermöglichen heute eine Kommunikation mit jeweils bis zu 16 Sende- und Empfangsantennen. Dadurch sind Datenraten von 10 GBit/s und darüber möglich, was eine 100-fache Steigerung gegenüber der aktuellen Spitzen-Datenrate von LTE bedeutet. Für den Standard IMT 2020/5G ist der breite Einsatz von 3D-Arrays für mehrfache Eingangs- und Mehrfachausgangskanäle (MIMO bis $16 \times 16 \times 16$) vorgesehen [10, 16].

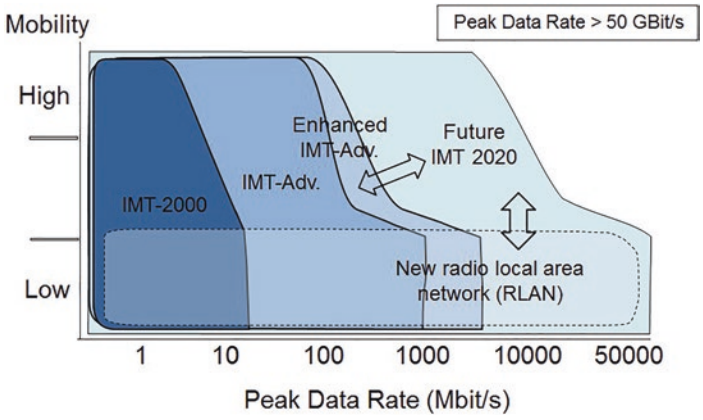


Abb. 13.12 Übergang von 3G zu 5G: Datenraten und Mobilität

In Abb. 13.12 sind die Datenraten und Mobilitäten für mobile Benutzer in den Kommunikationssystemen von 3G, 4G und 5G dargestellt. Die Peak-Datenrate wird somit mehr als 50 Gbit/s erreichen.

Seriöse Studien prognostizieren für das Jahr 2020 eine starke Erhöhung der Nutzerzahlen in Funknetzen auf bis zu 50 Mrd. Geräte, teilweise auf dem Niveau 5G. Dabei liegen die Prioritäten der 5G-Aktivitäten von Telekommunikationsunternehmen auf folgenden Gebieten:

- Digitale Ökonomie, Fernsteuerung von Maschinen;
- Intelligentes Stromnetz (Smart Grid), Intelligentes Messen (Smart Metering);
- Internet-Touch-Technologien („taktiles“ und „haptisches“ Internet);
- Städte der Zukunft (Smart Cities);
- Internet der Dinge, IoT (Internet of Things).

Die wichtigsten 5G-Foren für die Weiterentwicklung von Spezifikationen und Testgrundlagen für zukünftige Telekommunikationsprotokolle sind:

- 5G PPP (5G Infrastructure Public-Private Partnership);
- METIS (Mobile and wireless communications Enablers for Information Society by year 2020).

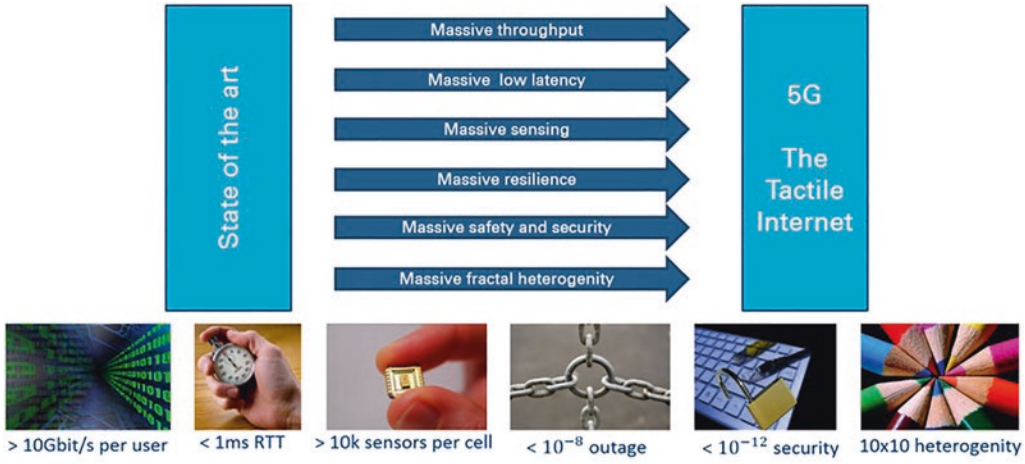
13.3.2 Forschungslabor 5GLab@TU Dresden

Zusätzlich zu den kommerziellen Forschungsaktivitäten der Hersteller von Telekommunikationstechnik gibt es auch 5G-Aktivitäten in mehreren Universitäten und Forschungslaboren. An der Technischen Universität Dresden existiert ein solches modernes 5G-Laboratorium am Vodafone Lehrstuhl für

Mobilkommunikationssysteme. Die Schwerpunkte der Forschung sind u. a. Arbeiten zur Erhöhung der Datenraten, zur Verbesserung der Netzabdeckung und der Verbindungsstabilität [10]. Die Forscher können ein breites Spektrum von 5G-Technologien evaluieren und testen. Dazu gehören: LTE, IEEE 802.20, 802.16e, 802.16a/d/e/m, Multigigabit Standard WiGig 60 GHz, IEEE 802.11ad, IEEE 1905, Bluetooth v4.2 und LoWPAN.

Das 5GLab umfasst Netzwerkhardware und -software, Computerchips, Spektrometer und Cloud-Computing-Services. Die Anforderungen an die 5. Generation nach den Ideen und anfänglichen Ergebnissen des 5GLab [10] sind in ◘ Abb. 13.13 dargestellt. Die Mitarbeiter des 5GLab gehen von der Vorstellung aus, dass die bisherigen mobilen Funknetze sich i. w. auf die bloße Bereitstellung von IP-Diensten und die Übertragung von Multimediainhalten von einem Ort zum anderen beschränken und im Gegensatz dazu die neue Generation in der Lage sein muss, eine breite Palette von Objekten in Echtzeit zu steuern, mit nur unwesentlichem menschlichem Eingreifen im Rahmen des IoT (internet of Things). Dazu erfolgen am 5GLab Forschungen und Untersuchungen zur Optimierung bestehender Systeme und mobiler Funknetzwerke, vor allem in Bezug auf Datenrate, Latenz, Interferenzen und Zuverlässigkeit. Die Vorhaben des 5GLab.de sind in ◘ Abb. 13.14 dargestellt.

Der Satz *„Das Internet wird in unseren Sinnen und Empfindlichkeiten verschwinden…“* (von E. Schmidt, ex-CEO von Google) zeigt die Wichtigkeit von menschlichen Interaktionen (taktil, haptisch) im künftigen Internet (5G Tactile Internet). Die Grundanforderungen für diese Umwandlung in das neue 5G Tactile Internet werden durch erweiterte QoS-Parameter charakterisiert: Datenrate bis ca. 10 GBit/s, Latenz von 1 ms



◘ **Abb. 13.13** Grundanforderungen zu 5G laut 5GLab (TU Dresden)

Abb. 13.14 Aktuelle Forschungsvorhaben von 5GLab (TU Dresden) zum 5G Tactile Internet

(auch als RTT, Round Trip Time, bezeichnet), 10.000 Sensoren pro Zelle, $\times 10^{-8}$ wenig wahrscheinlicher Ausfall sowie mehr Sicherheit und Heterogenität.

13.3.3 Huawei und 5G

Huawei Technologies wurde 1987 gegründet und gehört heute zu den weltweit größten Telekommunikationsgeräte- und Mobiltelefonherstellern, u. a. für Herrstellung von 5G-Systemen.

Vermerk

- In letzter Zeit wurden intensiv Probleme der Datensicherheit bei der 5G-Technik diskutiert. Insb. wurde dem Telekommunikationsriesen Huawei vorgeworfen, geheime Überwachungsschnittstellen in ihre Mobilfunktechnik zu integrieren. Bspw. berichtete das „Wall Street Journal" (05.03.2020, s. „► https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256") über langjährige Spionageaktivitäten. Die Seriosität der Vorwürfe ist schwierig zu validieren. Es ist durchaus möglich, dass sie zutreffen. Aber auch andere Wettbewerber könnten ähnliche Spionagesoftware integriert haben.
- Die Autoren sind gegen ein grundsätzliches Embargo für beliebige Firma, befürworten aber eine sorgfältige Prüfung aller Mobilfunklösungen und eine Offenlegung der technischen Interna, bspw. durch Open Source Software. Für sicherheitsrelevante Bereiche, wie bspw. Polizei und Militär, sind grundsätzlich nur nachweisbar sichere Lösungen zu nutzen.
- Bezüglich der teilweise politisch und ökonomisch motivierten Aussagen zur 5G-Technik möchten die Autoren als reine Wissenschaftler weiterhin keine Stellung nehmen.

Nach Ansicht von Huawei Technologies gibt es die drei wichtigsten Design-Ziele für 5G:

- Implementierung von „massiver Kapazität“ und „massiver Konnektivität“
  (ähnlich der Vorstellungen des 5GLab).
- Flexible und effiziente Nutzung aller verfügbaren Spektren für verschiedene Netzwerk-Einsatz-Szenarien (siehe DIDO-Konzept).
- Ein adaptives Netzwerklösungs-Framework.

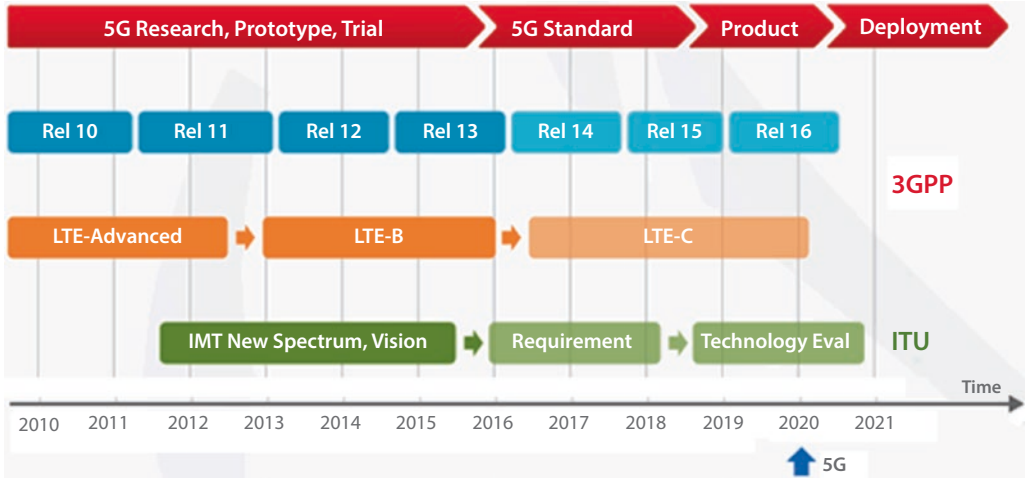
Die Ergebnisse aus der Erforschung von Clouds und softwaredefinierten Netzwerken werden die gesamten Vorstellungen über mobile Netze verändern.

Huawei plant die folgenden Arbeitsschritte (◘ Abb. 13.15).

Wie man sehen kann, laufen die Anstrengungen für die 5G-Entwicklung parallel zum Einsatz der neuen Verbesserungen für 4G/LTE bis zum LTE-C Release 16 [10]. Die neuen Entwicklungen für alle Funkzugangsknoten erfordern die optimale Beherrschung grundlegender Funktechnologien, wie der Endgeräte-Luftschnittstelle, der Netzwerkschnittstelle (Provider-RAN, Radio Access Network) und der Hochfrequenzverstärker.

Neben den bewährten Frequenzbändern sollen für zukünftige 5G-Mobilfunknetze die höheren Frequenzbänder E-L genutzt werden (◘ Abb. 13.16). Dies bedeutet die breite Frequenzspanne von 2–60 GHz bzw. den Wellenlängenbereich zwischen 15 cm und 0,5 cm.

Kommerzielle Netzlösungen innerhalb von 5G erfordern als integrale Bestandteile neben einer fortschrittlichen Funkübertragung auch einen Glasfaserzugang für das Festnetz. Die Interoperabilität innerhalb der 5G-Netzwerkarchitektur



◘ **Abb. 13.15** 5G: geplante Vorhaben der Fa. Huawei

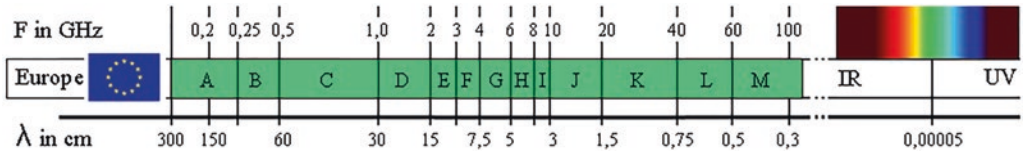


Abb. 13.16 Frequenzbänder E–L

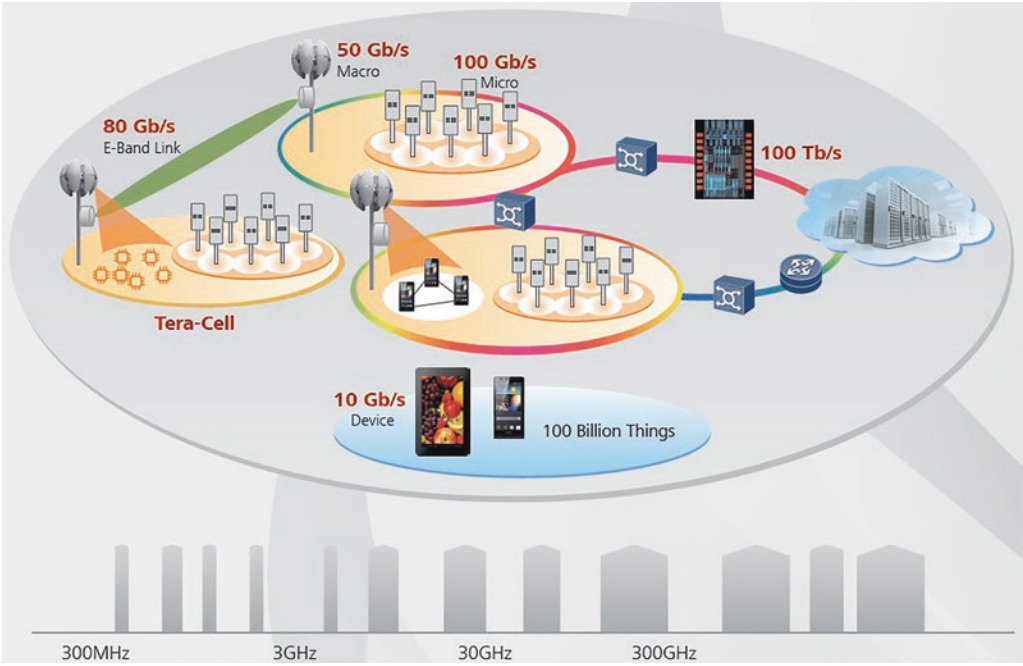


Abb. 13.17 Huawei 5G-Netzwerkarchitektur

sowie die zukünftige Erweiterung der bisher verwendeten 3G-Zellhierarchie (nach Huawei) ist in Abb. 13.17 dargestellt. Die Tera-Zellen umfassen auch übliche 3G-4G Makro- und Mikrozellen als vorgelagerte Netze (Backhauls). Die Festnetzanbindung erfolgt mit Datenraten bis zu 100 TBps.

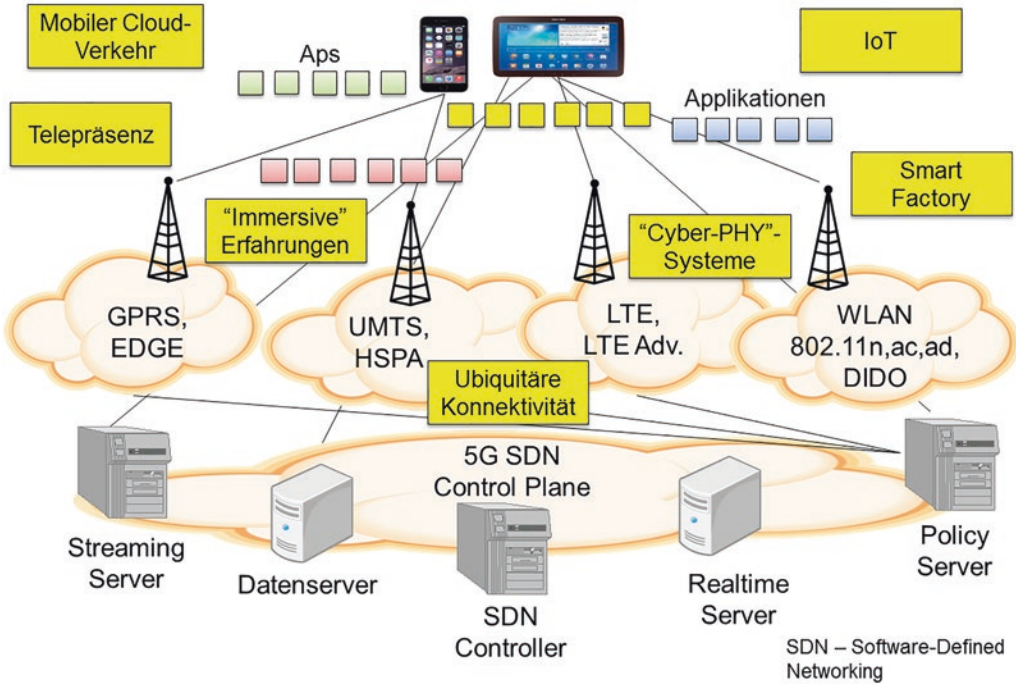
13.3.4 Architektur und Virtualisierung von Providerkernnetzen

Die Verwendung von SDN (Software-Defined Networking) für Software-Implementierungen von Providerkernnetzen vereinfacht den Netzbetrieb. Es wird den Unternehmen und Anbietern ermöglicht, herstellerunabhängige Funktionen für das Management und die Steuerung von Netzwerkkomponenten und -diensten von einem einheitlichen Bereitstellungszentrum zu erhalten.

Software-Implementierungen für 5G-Prototypen von Providerkernnetzen können nach Vorstellungen von führenden Firmen und Konsortien wie VMWare, CISCO, EMC2, OpenStack, Citrix, Vodafone, Samsung, Huawei (◘ Abb. 13.18) auf Netzwerken basieren, die u. a. die folgenden Protokolle von SDN verwenden: OpenFlow, VXLAN sowie Virtualisierungskonzepte wie VMWare vSwitch, Citrix Xen-Produkte uvm.

Die Virtualisierungsdienste, die über SDN durchgeführt werden, spielen als Teil des 5G/IMT 2020 eine wichtige Rolle. Bei diesem Konzept werden verbesserte Funktechnologien sowie Datenbanksysteme zur Frequenzzuteilung (DIDO) eingesetzt bei Einbeziehung der Infrastruktur auf Basis bestehender Systeme mit 4G/SAE, 3G/UTRAN und 2G/GERAN. Solch komplexe Systeme sind ohne virtualisiertes Management nicht beherrschbar.

Durch die Verwendung der SDN-Routinen wird die Arbeit der Netzwerkadministratoren vereinfacht. Sie müssen nicht Hunderte von Konfigurationskommandos für verschiedenste Switches oder Router eingeben. Das Netzwerk kann schnell in Echtzeit modifiziert werden. Dementsprechend kann die Vorbereitungszeit für neue Applikationen und Services erheblich



◘ **Abb. 13.18** Multimodaler 5G-Zugriff mittels SDN

reduziert werden. Mit geringerem Investitionsaufwand kann ein vielfältiges 5G-Serviceangebot erreicht werden:

- „Everything on Cloud" (Haltung regulärer Daten in den Wolken);
- Telepräsenz;
- Ubiquitäre Anbindung ans Netz;
- Echtzeitsteuerung;
- Gefühlte Realität („Immersive" Experience) etc.

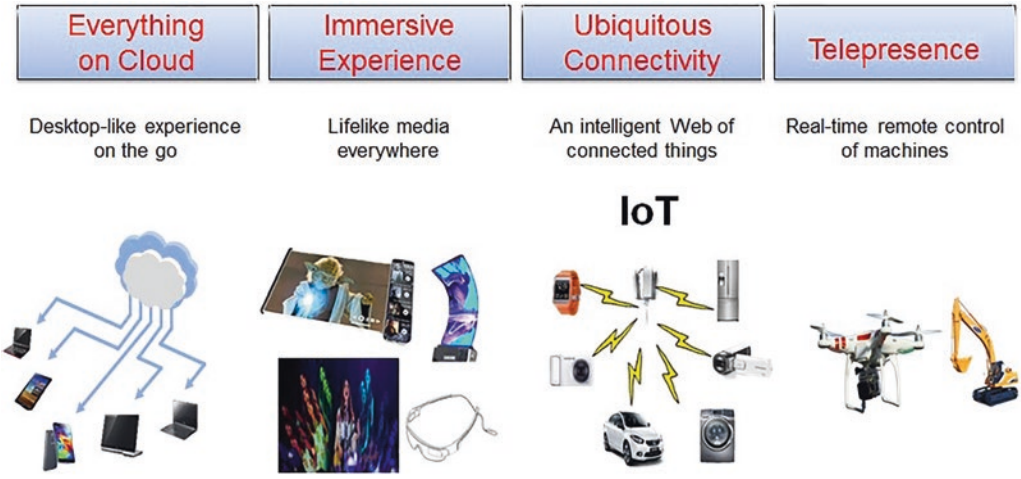
13.3.5 5G: neue Möglichkeiten laut Samsung

Die Vorstellungen von Anbietern wie Samsung Electronics [10] zu den Fähigkeiten von 5G-Systemen im Bereich der Dienstleistungen und mobilen Anwendungen sind in ◘ Abb. 13.19 dargestellt.

Eine weitere vielversprechende Anwendung für 5G/IMT 2020 Netzwerke entsteht im Bezug auf die Einrichtung von IoT-Anwendungen (Internet of Things) [9, 10]. Wichtigste Punkte sind dabei die Interoperabilität verschiedener physikalischer Funknetzwerke und die Virtualisierungstechnologie für die Kerndienste, die miteinander und mit der externen Umgebung (6LoWPAN, SDN) interagieren.

Die folgenden Szenarien der 5G-Implementierung in Bezug auf IoT- und Ubiquitous-Computing-Anwendungen sind praxisrelevant und werden in den nächsten Jahren über das Stadium von Forschungsprototypen hinaus realisiert:

- Intelligentes Haus, Intelligente Produktion, Intelligentes Gesundheitswesen;
- Intelligente Technik bei Fernoperationen, Fahrzeugen und gefährlichen Arbeiten;
- (Smart) Einzelhandel, Verkehr, Stadt.



◘ **Abb. 13.19** Die neuesten Fähigkeiten von 5G-Systemen

Die Hardware-Trends in Richtung 5G-Konnektivität führen auch zu neuen Software-und Daten-Trends. Laut der Consultingfirma Gartner Inc. gehört heutzutage „Big Data" zu den bedeutendsten Trends in der IT-Infrastrukturentwicklung sowie die Virtualisierung und Energieeffizienz der IT. Riesige Datenmengen verschiedenster Typen im Bereich bis zu 100 Exabyte (10^{18}) müssen dabei mit hoher Geschwindigkeit bei Sicherung der Datenkonsistenz und -Qualität übertragen werden (5 V-Konzept von „Big Data", d. h. Volume, Velocity, Variety, Veracity und Value [10]). Wichtige Datenquellen sind z. B. geographische Informationssysteme (GIS) und andere Datenbanken, parallele Cluster und Netze, semantische und soziale Netzwerke. Typischerweise verwendet man dafür die Begriffe Web 2.0 und Web 3.0, Cloud Computing sowie das intelligente Internet der Dinge.

Die Akkumulation großer Datenmengen ist heute typisch für Handel und Marketing, elektronische Zahlungen, Prozessautomation, für internationale Justiz- und Kriminologie sowie für die Pharma- und Werbebranche. Eine große Zahl von Wissenschafts- und Forschungsinstituten, Organisationen und Universitäten sammeln, speichern und berechnen große Mengen technischer und wissenschaftlicher Informationen. Oft ist eine solche große Informationsmenge nicht strukturiert, sodass sie durch eine außerordentliche Komplexität des Informationsmanagements gekennzeichnet ist. Außerdem kommt es zu einem signifikanten Anstieg des Netzwerkverkehrs und über die Heterogenität geografisch verteilter Daten innerhalb mehrerer Rechenknoten steigt die Datenmenge noch mehr an. 5G wird sicher diese Tendenz zur großen Datenerfassung und -verarbeitung verstärken.

13.3.6 5G: Interoperabilität zu anderen Netzwerken

5G-Netze werden zukünftig höchstwahrscheinlich zum Alltag gehören. Trotzdem ist zu erwarten, dass es notwendig ist, 5G mit anderen drahtlosen Übertragungstechniken zu ergänzen, z. B. wegen Konnektivitätsproblemen aufgrund geringer Signalstärke, Überlastung aufgrund zu vieler Geräte oder des Nutzerwunsches nach Anonymität.

Interoperabilität zu Netzwerktechnologien. Ein Vergleich des 5G-Mobilfunknetzes und einiger seiner Vorgänger mit drahtlosen Protokollen, die möglicherweise gegenseitige Interoperabilität bieten, ist in ◘ Abb. 13.20 mit den entsprechenden Abständen und Datenraten in logarithmischen Maßstäben dargestellt. Die folgenden Netzwerktechnologien müssen die Interoperabilität mit 5G/IMT2020 gewährleisten (vgl. Abbildung):

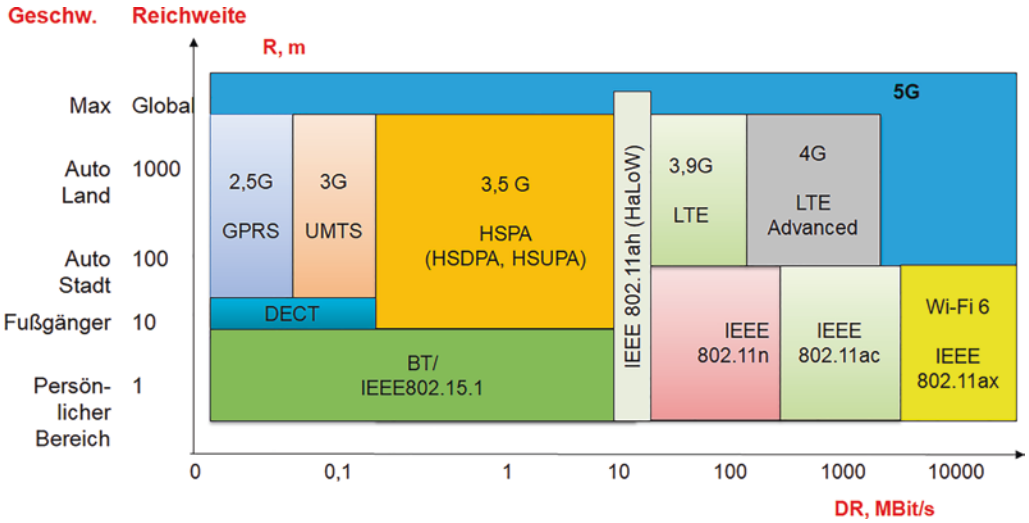


Abb. 13.20 Vergleich von Reichweiten und Datenraten für verschiedene Funknetzwerke

Mobile WiMAX, WiGig, IEEE 802.11ad, IEEE 1905, Piconets: WSN, Bluetooth, 6LoWPAN.

Mit dem im Jahr 2013 eingeführten IEEE 802.11ac werden größere Kanalbandbreiten bis zu 160 MHz möglich. Darüber hinaus sind optimierte Modulation und 8×8 MIMO vorgesehen, was zu einer deutlich höheren Datenrate von 6936 MBit/s führt. Die aktuellen Produkte unterstützen jedoch i. A. nur 3×3 MIMO, eine Bandbreite von 80 MHz und folglich eine Datenrate von 1299 MBit/s.

Das 60 GHz Band liegt im Frequenzbereich 57 bis 66 GHz und wird durch einen Kanalabstand von 2160 MHz in vier Kanälen mit einer Bandbreite von 1760 MHz geteilt. Eine große Bandbreite wird benötigt, um eine hohe Datenrate von 7 GBit/s zu erreichen.

Der Multi-Gigabit-Standard WiGig arbeitet im 60 GHz-Band. WiGig wurde von der WiGig Alliance mit dem IEEE-Standard 802.11ad für die Kooperation mit anderen Protokollen wie USB 3.0, HDMI und PCI-Express mit einer Datenrate von 7 GBit/s entwickelt und ist vorgesehen für die Nutzung in Wohnhäusern. Die Empfangsqualität wird erheblich reduziert beim Durchdringen von Wänden.

Im Gegensatz zum herkömmlichen WLAN ist IEEE 802.11ad nur für wenige Meter Reichweite ausgelegt. Dies ergibt sich u. a. aus der hohen Absorption durch Sauerstoff bei 60 GHz.

Im Vergleich dazu ist IEEE 1905 ein Standard, der einen Netzwerk-Enabler (Anpasser digitaler Heimnetzwerke) definiert, der sowohl drahtlose als auch drahtgebundene Technologien unterstützt: IEEE 802.11 (Wi-Fi), IEEE 1901 (HomePlug, HD-PLC), IEEE 802.3 Ethernet und Multimedia über Coax (MoCA). Der

Standard wurde im Jahr 2010 von der Gruppe 1905.1 spezifiziert unter Beteiligung von weiteren 30 Organisationen. Drei Jahre später wurde der Entwurf der P1905.1-Spezifikation endgültig durch das IEEE genehmigt und veröffentlicht.

13.3.7 Interoperabilität mit 6LoWPAN

6LoWPAN ist ein Kommunikationsprotokoll zur Funkdatenübertragung mit niedrigem Energieverbrauch (s. ► Abschn. 12.6). Interessant ist die Kombination dieses anwenderfreien und ressourcenschonenden Kurzreichweitenprotokolles mit 5G-Netzen, die hohe Leistungsdaten besitzen, aber auch einen hohen Ressourcenverbrauch haben. Im Rahmen von 5G wird 6LoWPAN zusätzlich zu WPAN auch als Wireless Neighborhood Area Network (WNAN) bezeichnet (Angrenzung an Zellularnetzwerke einschließlich 2G-5G [10]).

Um die Eigenschaften von 5G und 6LoWPAN zu kombinieren, wurde 2015 eine neue Kommunikationsklasse mit dem Namen Low Power Wide Area Network (LPWAN) eingeführt. LPWAN ermöglicht die Kommunikation von Sensoren über 10 Meilen ohne Hindernisse bzw. über 3 Meilen in dichten städtischen Gebieten mit einer Akkulaufzeit von 10 Jahren! In Europa werden dafür Frequenzbänder um 433 bzw. zwischen 853 und 870 MHz genutzt, in China der Bereich zwischen 779 und 787 MHz und in Nordamerika der Bereich zwischen 902 und 928 MHz.

Der Standard LoRaWAN erreicht noch größere Entfernungen, indem er den Verkehr von Knoten (Sensoren) in Routern oder Gateways konzentriert, den Verkehr über ein drahtloses Netzwerk von mindestens 3G-Qualität tunnelt und an Applikationsserver weiterleitet, die die Daten verarbeiten. Die Übertragung ist verschlüsselt und auf einen geringen Energieverbrauch der Sensoren ausgerichtet, um Batterieressourcen zu sparen [10]. Die Gateways können an Türmen neben mobilen Kommunikations-Basisstationen installiert werden. Die Datenrate reicht umgebungsabhängig von 0,3 bis 50 kBit/s.

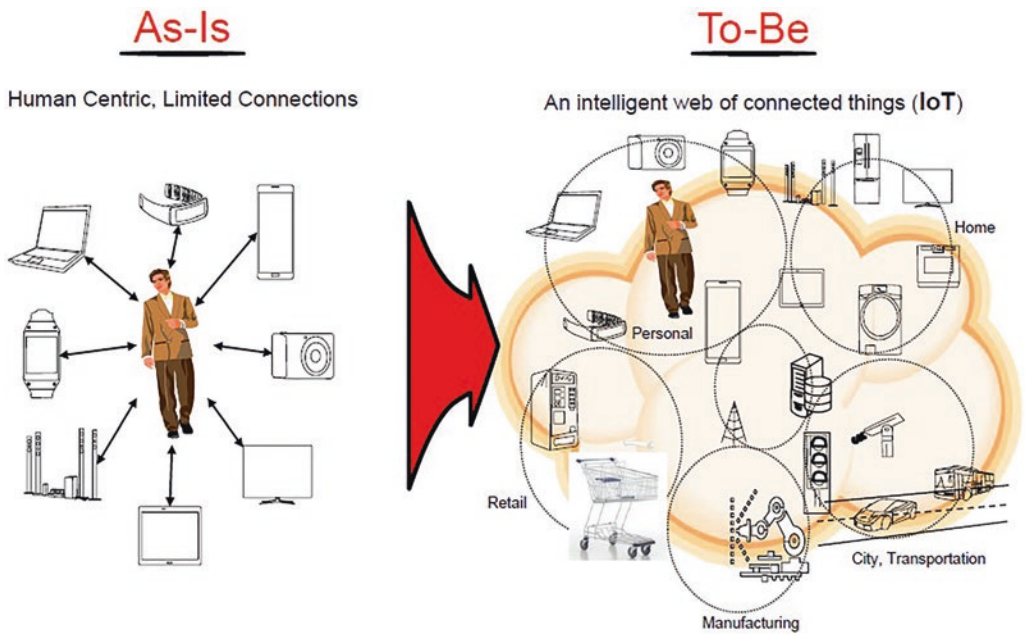
13.3.8 Künftiger Standard IMT 2020: Einsatzszenarien

Durch den zukünftigen leistungsfähigen Standard IMT 2020 werden viele neue attraktive Dienstleistungen und Infotainment-Anwendungen entstehen. Folgende Implementierungsszenarien sind möglich [10]:

- Mehr mobile Verbindungen mit steigendem mobilen Datenverkehr;
- Mehr mobiler Cloud-Verkehr und mobile Zahlungen;
- Verbundene „Dinge“ (IoT), sowie virtuelle „immersive“ Realität (VR – Virtuelle Realität).

Die Kombination von kleinen Netzwerkzellen, insbesondere Nanotechnologie, mit Cloud Computing, IP-Architektur wurde unter dem Namen Nanocore [10] vorgeschlagen. Die Nanoausrüstung wäre der logische Nachfolger des heutigen Trends der schrumpfenden Gerätegrößen von Desktop-PCs über Mobiltelefone, Smart-Uhren bis zu sog. Wearables (Hörgeräte, körperintegrierte Chips, Kleidungszubehör, …). Zukünftig werden über 5G-Netze vielfältige neue Anwendungsgebiete erschlossen [4, 8, 10] (s. ◘ Abb. 13.21).

a) Neue Sensoren und Anwendungen für behinderte Menschen;
   z. B. Gesundheits-, Fitnesskontrolle und Medizinvorschläge durch die Kombination von Hardware-Sensoren, integrierten Anwendungen und Netzdiensten;
b) 5G-Sensoren zur Steuerung von Häusern (Heizung, Lüftung, Türen), Gärten, Laptops, Autos, Fahrrädern, …;
c) Teilung der Arbeitslast von Mobiltelefonen in Grids und P2P-Systemen;



◘ **Abb. 13.21** Universelle Verbindungsfähigkeit durch 5G

In diesem Fall sind Systeme erforderlich, welche den besten Server oder Service für ausgelagerte Aktivitäten finden.

d) Optimierung des Ressourcenmanagements für mobile Geräte (Energieverbrauch, Optimierung der Funkabdeckung);
e) Intelligente Netzwerk und Internet der Dinge (IoT, Internet of Things).

13.3.9 Optimierungsfaktoren und Nutzungsqualität

Welche Faktoren sollen im neuen 5G/IMT 2020 Standard optimiert werden? Die Beantwortung der Frage ist nichttrivial, da eine signifikante Leistungssteigerung nur erreichbar ist durch einen Kompromiss bei der Erfüllung folgender, teilweise widersprüchlichen Forderungen:

- Hohe Zellkapazität und Datenratenverbesserung an den Zellrändern;
- Erweiterte MIMO-Nutzung für Multi-User-Betrieb mit 3D-Arrays von Antennen;
- Verbesserte Modulationsverfahren und damit spektrale Effizienzsteigerung (SE);
- Interferenzkorrektur;
- bessere Kosteneffizienz und QoE-Optimierung (Optimierung der Quality of Experience);
- effizientes Verbindungsmanagement und Latenzminimierung.

Im Folgenden werden einige optimierte Parameter von 5G gezeigt (◘ Tab. 13.6).

◘ **Tab. 13.6** Optimierte 5G-Parameter

Parameter	Werte
QoE (Quality of Experience)	Datenrate und Reaktionszeiten
Zelldurchsatz	10,0 GBit/s
Ende-zu-Ende-Netzwerklatenz (E2E)	<5 ms
Luftschnittstellenverzögerung (Latenz)	1 ms
Kostenreduktion	rasant im Vergleich zu 4G aufgrund des SDN und Virtualisierung der Netzwerkdienste (kostengünstige Betrieb und Management)
Zeitparallele IoT-Verbindungen	10… 20 Mal mehr als 4G
„Bit/Costs"-Faktor	ca. 50 Mal besser

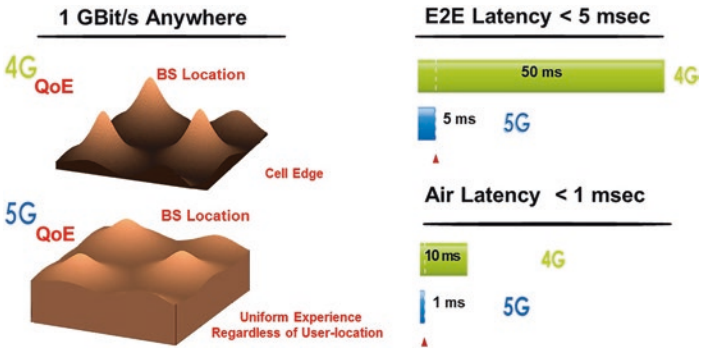


Abb. 13.22 Perfekte „User Experience" durch 5G-Vernetzung

Die überlegenen Eigenschaften bzgl. Datenraten und Latenzzeiten von 5G im Vergleich zu ihrem Vorgänger 4G zeigt Abb. 13.22. Bei 5G ist gewährleistet, dass die Empfangsfeldstärken sowohl nahe der Basisstationen als auch am Zellenrand fast gleichmäßig groß sind, d. h. dass sie unabhängig von den Nutzerpositionen innerhalb der Kommunikationszellen sind. Deshalb gibt es praktisch keine positionsabhängige Beeinträchtigung der Sende- und Empfangsqualität [10].

13.3.10 Kostenmodelle von 5G

Im Weiteren werden die Betreiberkosten diskutiert, die an die abonnierten Benutzer weitergegeben werden können. Die 5G-Systeme müssen die aufgebauten Verbindungen etwa 50 Mal kostengünstiger als 4G/LTE-Systeme betreiben, um eine Investitionsamortisierung zu erreichen und die Modernisierung bestehender Netzwerke und Zell-Basisstationen durchführbar zu machen. Dies wird als Bit/Kosten-Faktor von 50 bezeichnet. Die 5G-Kostenstruktur zeigt Abb. 13.23.

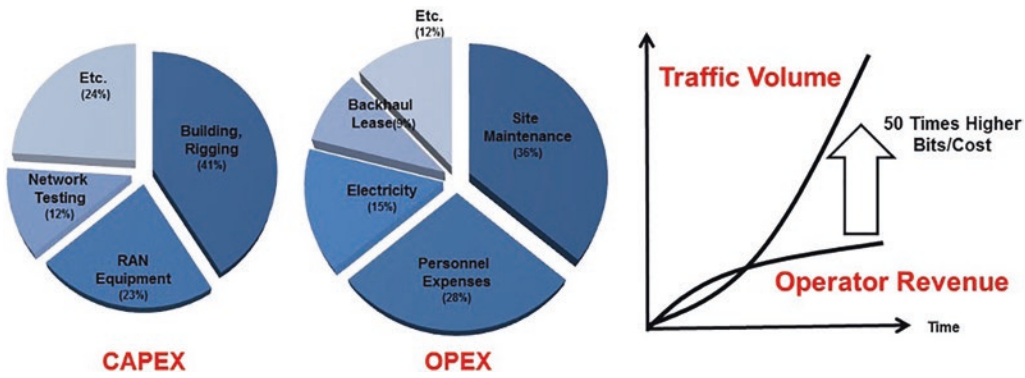


Abb. 13.23 Kostenstruktur in 5G

Die finanziellen Konsequenzen des Einsatzes der 5G-Infrastruktur für die Anbieter können wie folgt berechnet werden:

$$\begin{aligned} Expenditures &= CAPEX + OPEX; CAPEX \rightarrow \min \vee OPEX \rightarrow \min \\ Profit &= Revenue(anno) - CAPEX(partial) - OPEX(anno) \rightarrow \max \\ ROI &= \frac{Revenue - Expenditures}{Expenditures} \times 100\ \% \end{aligned} \tag{13.12}$$

wobei

N – Abschreibungsperiode mit Modifikationen [bspw. in Jahren],

ROI – Return of Investments (Rendite),

OPEX – Operational Expenditures (d. h. Betriebskosten für Personal, Verbrauchsmaterialien, Strom, Reparaturen und Modifikationen),

CAPEX – Capital Expenditures (Investitionen für Hardware, Entwicklungs-, Bau- und Technikkosten),

anno – jährlich und partial – Amortisationssatz anteilig per anno sind.

13.3.11 DIDO: Ressourcenzuweisungsverfahren für künftiges WLAN innerhalb 5G

DIDO (auch als „pCell" bekannt) ist eine Technologie, die unter Berücksichtigung internationaler Vorschriften und Konventionen für die verwendeten Frequenzen ein flexibles Mehrbenutzer-WLAN bietet (Quelle: ► Rearden.com/Artemis). Die Technologie soll die bestehenden GERAN-, UTRAN-, SAE- und IMS-Mobilfunkinfrastrukturen der Vorgängergenerationen 2G-4G durch ein flexibles, weltweites WLAN erweitern. Dabei werden Datenbanken für verfügbare Frequenzbänder und Web-basierte Inhalte genutzt, die sog. DIDO-Rechenzentren.

Die Verwendung eines breiten Frequenzspektrums ist dadurch vorbereitet. Pionier des DIDO-Ansatzes ist die Firma Rearden (USA) mit Aktivitäten von Steve Perlman [10]. Heute gehört DIDO zu den bedeutendsten Forschungsfeldern bei 5G. In ersten Experimenten wurde DIDO im Frequenzbereich von 1 MHz bis 1 GHz getestet. Weiterentwicklungen sind in Arbeit für folgende Wellenlängen (λ) und Frequenzbänder (F):

- HF High Frequency (100 m/3 MHz–10 m/30 MHz);
- UHF Ultra High Frequency (1 m/300 MHz–1 dm/3 GHz);
- SHF Super High Frequency (1 dm/3 GHz–1 cm/30 GHz);
- EHF Extremely High Frequency (1 cm/30 GHz–1 mm/300 GHz)

Die erwarteten DIDO-Vorteile sind in ◘ Abb. 13.24 dargestellt. Ohne DIDO kann die Kommunikation von 3 Benutzern und 3 dargestellten Access Points (APs) evtl. mit

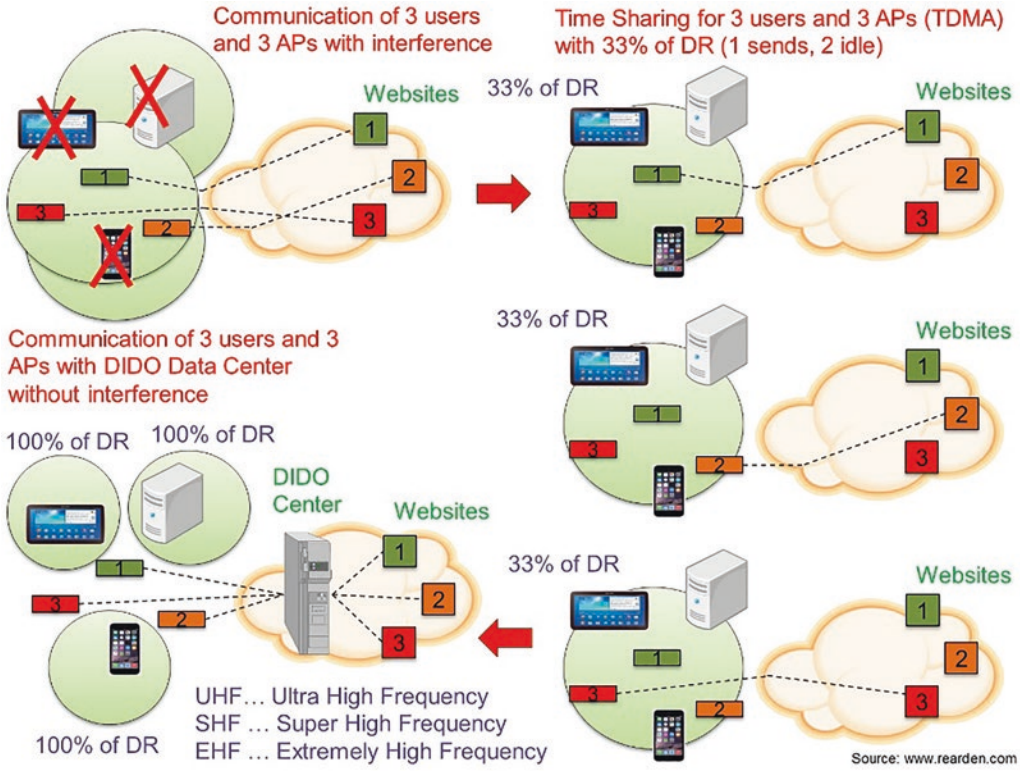


Abb. 13.24 DIDO Vorteile: volle Bandbreite für alle beteiligten User. (Quelle: Rearden)

Kanalüberlagerungen bzw. Interferenzen erfolgen. Mittels der Verwendung eines DIDO-Rechenzentrums wird die störungsfreie Kommunikation mehrerer Benutzer mit mehreren Websites erreicht. Konkret ist ein Time-Sharing (TDMA) für 3 Benutzer und 3 APs mit jeweils 33 % der Datenrate nicht mehr erforderlich, weil ein störungsfreier Betrieb bei voller Bandbreite über mehrere Frequenzen gewährleistet ist (FDMA).

In höheren Schichten der Architektur können drei unabhängige WWW-Sitzungen aufgebaut werden.

Die allgemeine DIDO-Architektur zeigt Abb. 13.25. Die folgenden DIDO-Komponenten werden genutzt:

- DIDO-fähige Endgeräte (z. B. Tablets, Smartphones, Notebooks, Desktops/PCs);
- DIDO-Access Points (5G- und WLAN-fähig) für Verwaltung von Zellen unterschiedlicher Größe über variable Entfernungen (Reichweiten); diese fungieren als Bestandteile von
- DIDO-Rechenzentren (Wireless Clouds), die Rolle von Contentprovidern für die DIDO-Endgeräte übernehmen.

Das Verfahren wird an einem Beispiel mit 5 Usern und 5 APs (Access Points) vorgestellt. Die Verbindungen zu 5 verschiedenen

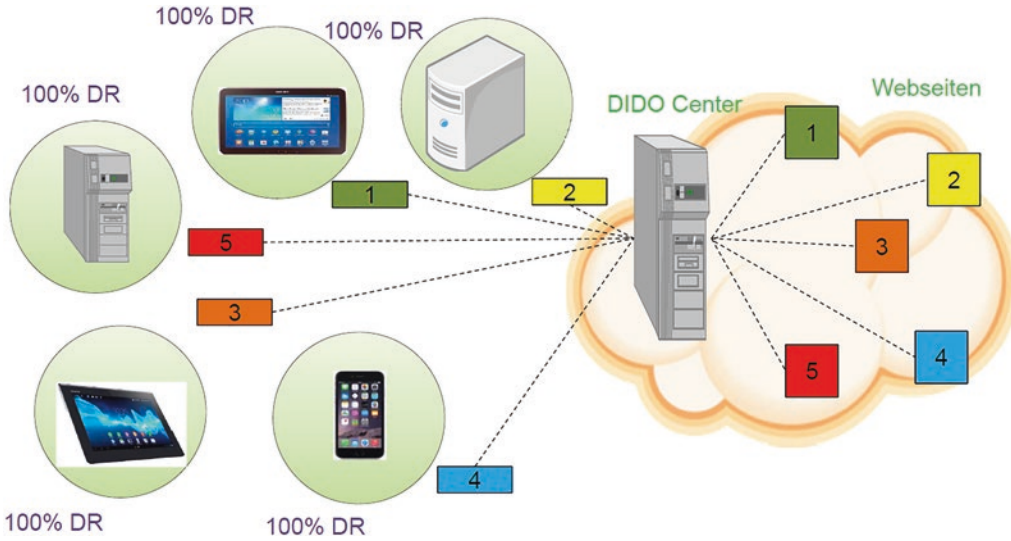


Abb. 13.25 Allgemeine DIDO-Architektur (Quelle: Rearden/Artemis/pCell)

Webseiten werden bereitgestellt. Es gibt keine Störung unter den Nutzern, da alle Benutzer den Vorteil von 100 % der Datenrate des Kanals erhalten. Außerdem spielt es keine Rolle, wo sich die APs befinden oder welche Benutzer wo eingeloggt ist. Jeder Benutzer erhält die Daten von der Website, mit der er verbunden ist, über einen eigenen drahtlosen Kanal [10].

Der einzige Nachteil von DIDO ist die Notwendigkeit von zwischenstaatlichen Vereinbarungen und bestimmten Regulierungsstellen, um ein breites Spektrum von Frequenzen zu nutzen. DIDO muss Rücksicht auf länderspezifische Besonderheiten nehmen, insbesondere bei niedrigeren Frequenzen, d. h. innerhalb des HF-Bandes (100 m/3 MHz–10 m/30 MHz). Deren Nutzung ist aber notwendig, weil bei diesen Frequenzen große Entfernungen überspannt werden können.

DIDO Rural ist in Abb. 13.26 dargestellt. DIDO-APs in ländlichen (rural) Gebieten können weit über längere Distanzen als herkömmliche WLAN-APs oder Zell-Basisstationen übertragen. Die Übertragung kann über die bekannten „Himmelswellen“ (Near-Vertical Incidence Sky Waves, NVIS) erfolgen. Dabei werden die Funksignale bei Frequenzen um 5 MHz im steilen Winkel gegen den Himmel gesendet. Dadurch werden tote Zonen um die Sendeantenne vermieden, trotzdem kann ein Zelldurchmesser von etwa 900 km abgedeckt werden, was den Anforderungen entspricht. NVIS sind die Alternative zu den Bodenwellen (GWaves), bei denen flach abgestrahlt wird und die nur etwa einen Durchmesser von 70 km bedecken können, bevor sie durch die Krümmung der Erde blockiert werden [10].

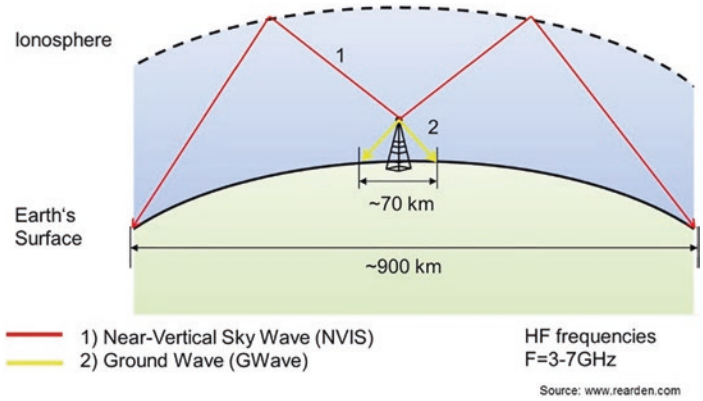


Abb. 13.26 Funktechnik bei DIDO Rural

13.4 Quo vadis? Ausblick zur 5G

Heutzutage ist die mobile Kommunikation mit der Bereitstellung von IP-Diensten und der Übertragung von Multimediainhalten von einem Ort zum anderen beschäftigt, aber morgen wird die neue Funknetzgeneration 5G in der Lage sein, eine breite Palette von Objekten in Echtzeit mit nur unwesentlichem menschlichem Eingriff zu kontrollieren (IoT und anderen attraktive Anwendungen). Deshalb wird 5G große Beiträge zu den meisten aktuellen Telekommunikations- und Computerthemen erbringen, darunter besonders für die große Datenerfassung und -Verarbeitung (Big Data). Die DIDO-Methode zielt darauf ab, überall ein flexibles Mehrbenutzer-WLAN bereitzustellen.

Die 5G-Technologie bietet eine Möglichkeit, die derzeitigen Begrenzungen von LANs und LTE/4G-Netzen zu überschreiten. Mehrere prominente Unternehmen bereiten auch Schritte zum breiten Einsatz von 5G vor. Das Unternehmen Microsoft beabsichtigt, den Zugang zu 10 Mio. Wi-Fi-Hotspots anzubieten. Über seine Internettelefonie-Tochter Skype bietet Microsoft bereits heute den WiFi-Zugang zu rund zwei Millionen Hotspots weltweit. Unter dem Label „Microsoft WLAN" werden den Kunden der Office- und Skype-Produkte die Zugriffsrechte eingeräumt.

13.5 Zwischenfragen/Übungsaufgaben

13.5.1 Zellulare Mobilfunknetze

a) Durch so genanntes Clustering werden geographische Bereiche in zellularen Funknetzen in Funkzellen mit unterschiedlichen Frequenzbändern strukturiert. Bezeichnet D

den Abstand zweier Basisstationen mit derselben Sendefrequenz, R den Zellradius und k die Clustergröße, gilt folgender Zusammenhang:

$$D = R \cdot \sqrt{3k}$$

Wie sieht ein Cluster aus, das für Zellen gleicher Frequenzen einen $D = 6 \cdot R$ Abstand ermöglicht?

b) Was sind die Hauptunterschiede von GSM und UMTS und wie werden die höheren Datenraten erzielt? Was ist HSDPA und LTE?

13.5.2 In Richtung 5G

Die 5. Generation des Mobilfunks bezeichnet die nächste wichtige Phase der aktuellen Entwicklung von Mobilfunkstandards.

a) Welche Unterschiede bietet 5G hinsichtlich der Vorgänger 3G/4G!
b) Beschreiben Sie kurz die wichtigsten Netzwerktechnologien, die 5G-Einsatz künftig unterstützen sollen.
c) Analysieren Sie das Szenario in ◘ Abb. 13.18! Erklären Sie die Rollen jeweiliger Komponenten der Architektur.

13.5.3 Satellitenfunk und Ortungssysteme

a) Geben Sie Ihre Beispiele von satelliten-basierten Kommunikationssystemen! Welche Dienste realisieren diese?
b) Klassifizieren Sie die satelliten-basierte Systeme nach Orbithöhe (GEO, MEO, LEO). Vergleichen Sie diese bzgl. der DR, Sendeleistung, Distanz, Lebensdauer, Signalverzögerung, Handover!
c) Ein Satellit hat Entfernung zur Erde h = 20.200 km. Berechnen Sie die Periode T(r)! Zu welcher Klasse (Einsatzbereich) würden Sie diesen einordnen?
d) Vergleichen Sie die satelliten-basierte Ortungssysteme wie GPS, GALILEO usw.!

Netzkopplung und Verkabelung

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_14

Dieses Kapitel befasst sich mit der Infrastrukturplanung kabelgebundener lokaler Rechnernetze, speziell werden aktive Netzkopplungsgeräte (Switches, Router, Access Points, Gateways, Firewalls) sowie die Eigenschaften der Übertragungsmedien und deren Eignung für die strukturierte Verkabelung sowie typische Fehlerquellen behandelt. Die aktuellen Netzwerkklassen bzw. -kategorien werden vorgestellt und es wird auf die Methodik der Qualitätsmessung und der Zertifizierung eingegangen.

14.1 Aktive Netzkopplungsgeräte

In der Praxis erfolgt die eigentliche Kopplung von Netzwerken (Subnetzen, Einzelknoten, Terminals und Endgeräten) durch diverse **passive Übertragungsmedien** (Kabelsysteme – Metallleiter, Lichtwellenleiter, Luftschnittstelle – Funk, IR, Laser etc.) und mittels **aktiver** Netzkopplungsgeräte, u. a. Hubs, Switches, Router, Access Points (AP), Gateways (GW), Firewalls (FW), d. h. durch die sog. **aktiven Kopplungselemente.** Dieses Oxymoron soll dem Leser verdeutlichen, dass die Umwandlung von Daten, die Verstärkung der Signale, die Fehlerkorrektur usw. im Netz i. d. R. von den **aktiven Kopplungselementen** übernommen wird [3, 14–19].

14.1.1 Netzkopplung und Gateways

Zu den wichtigsten Anforderungen zur aktiven Netzkopplung [1, 3], gehören die folgenden (s. Abb. 14.1):

- Aufbau eines Verbundsystems
- Heterogenitätsabbau durch die aktiven Kopplungselemente
- Effiziente Datenübertragung u. a. mit QoS-Garantien durch die aktiven Kopplungselemente
- Anpassung von Paketlängen.

Zu den wichtigsten Netzkopplungskonzepten gehören die folgenden Koppelelemente (s. Abb. 14.2), die in Bezug auf des OSI-Referenzmodell als Layer-N-Gateways bezeichnet werden. Diese lassen sich den Schichten 1 bis 7 entsprechend zuordnen.

Repeater können mehr als 2 Ports besitzen, dann werden diese **Hubs** genannt (Multiportrepeater). Das Element übernimmt lediglich nur Verstärkung und Regeneration elektrischer Signale ohne Fehlerkorrekturroutinen (Schicht 1).

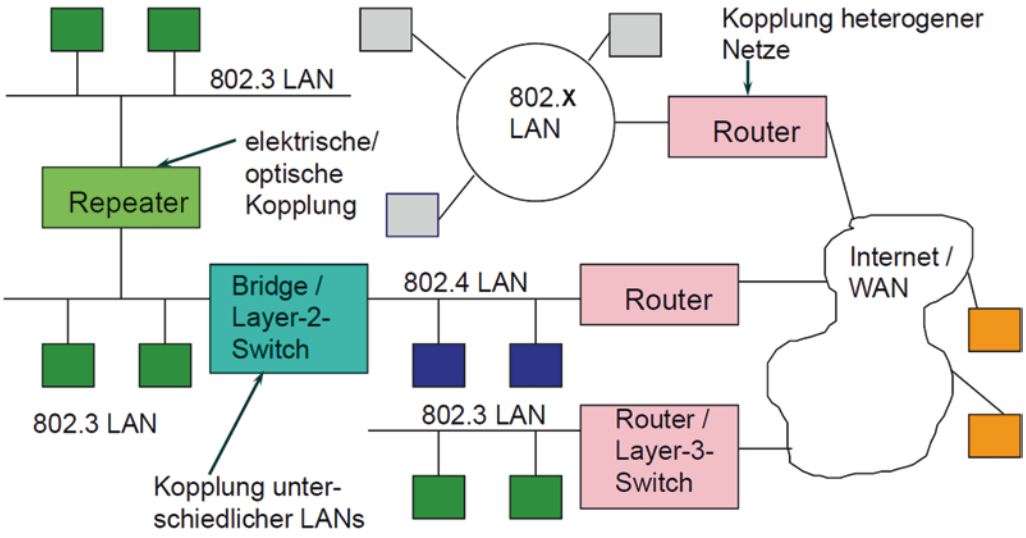


Abb. 14.1 Aktive Netzkopplung: integriertes Szenario

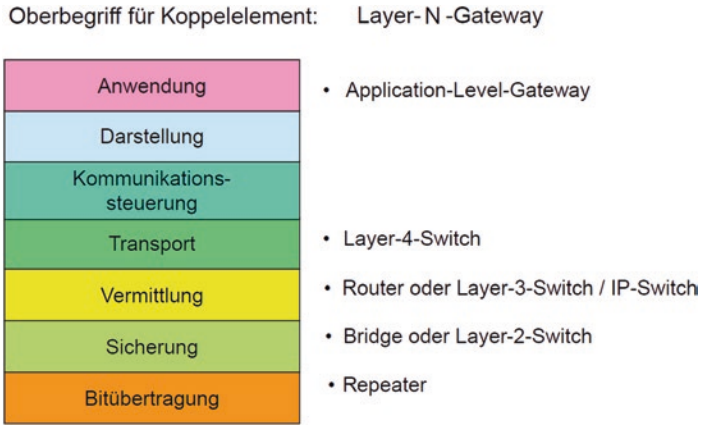


Abb. 14.2 Netzkopplungskonzepte: Einordnung zu den OSI-Schichten

Bridges bilden die Basis für fortgeschrittene **Switches** (s. weitere Abschn.) durch die integrierten Routinen für die Umwandlung von Daten, Regeneration der Signale, Anpassung der Pakete und Fehlerkorrektur (Schicht 2). Die Switches ermöglichen die sog. Durchschaltung angeschlossener Leitungen, mit anderen Worten „Switching".

Die **Router** koppeln heterogene Netzwerke zu einem weiträumigen Verbundsystem (Intranet, Extranet, Internet). Die angekoppelte Netzwerkknoten und Endgeräte sind IP-fähig und interagieren unter Nutzung universeller Adressen, die in den sog. Routingtabellen abgespeichert sind. Die Ermittlung

der optimalen Adresstabellen nennt man „Routing“, das zum IP-Betrieb abwechselnd und ergänzend innerhalb der Schicht 3 stattfindet.

Oft liegt das Netzwerkkopplungsdilemma dabei in der folgenden Ebene: „Switching“ oder „Routing“. Was ist effizienter bei der Datenübertragung im Netz?

Ehemals bedeutete der Begriff „Gateway“ auch einen (Software-)Router, der zwei heterogene Netzwerke (autonome IP-Bereiche) untereinander mit Filterung/Anpassung/Absicherung ankoppelt.

Die **Gateways** (Applikation-Level-GW) sind aktive Kopplungselemente der verarbeitungsorientierten Schichten 5–7 und funktionieren oft schichtenübergreifend (2–7) und anwendungsspezifisch, bspw. zwecks Erhöhung der Datensicherheit (als Filter, eine FW) oder Intrusion Detection (IDS, ID System) oder für die Anpassung heterogener Anwendungen/Rechnerarchitekturen (Virtualisierungsschicht in Betriebssystemen).

14.1.2 Switching

Die Bridges spielen heutzutage nur eine untergeordnete Rolle in der Rechnernetzpraxis, da der Betrieb von Switches überall favorisiert ist. „Switching“ als Routine im Netzbetrieb wird durch die sog. Layer-2-Switches übernommen. Trotzdem ist die Rolle der Bridges groß, da die Grundprinzipien gleich sind.

Sowohl Bridges als auch Switches nutzen die folgenden wichtigen Protokolle:

- „Translating Bridge“ – Verfahren zur Umwandlung der Frameformate und Datenratenanpassung
- „Transparent Bridge“ – Verfahren
- „Spanning Tree“ – Verfahren
- sowie „Source Routing“ – Verfahren.

Durch den Einsatz von Switches werden dabei die nachstehenden Ziele verfolgt (◘ Abb. 14.3):

- LAN-Kopplung erfolgt über mittlere Entfernungen.
- Trennung organisatorischer Bereiche und verschiedener Verkehrsströme wird bereitgestellt.
- Zuverlässigkeit und Sicherheit wird garantiert.
- Begrenzung der Netzlast erfolgt durch selektives Filtern und Weiterleiten von Nachrichten.
- gegen Störungen und unberechtigte Weiterleitung wirken fast alle Layer-N-Gateways.

Die Verzögerungszeit Δt liegt derzeit bei Switches im Mikrosekundenbereich, wobei die Datenraten im GBit/s – Bereich spielen.

Im Allgemeinen kann die Verarbeitungsverzögerung in den Bridges/Switches außerdem durch die Übersetzungsroutinen verursacht werden (s. ◘ Abb. 14.4). In diesem bespielhaften Modell

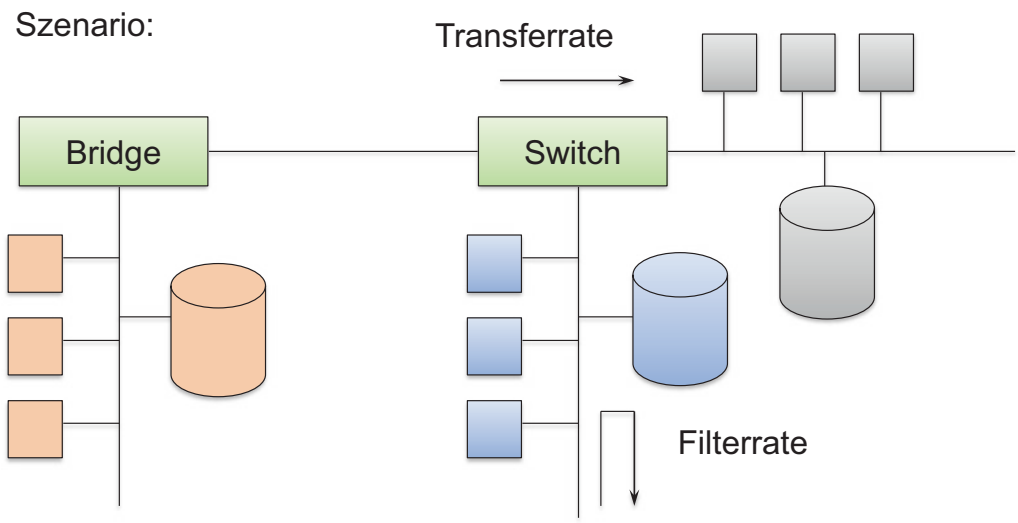


Abb. 14.3 Rolle von Bridges und Switches in Netzwerken: selektives Filtern und Weiterleiten

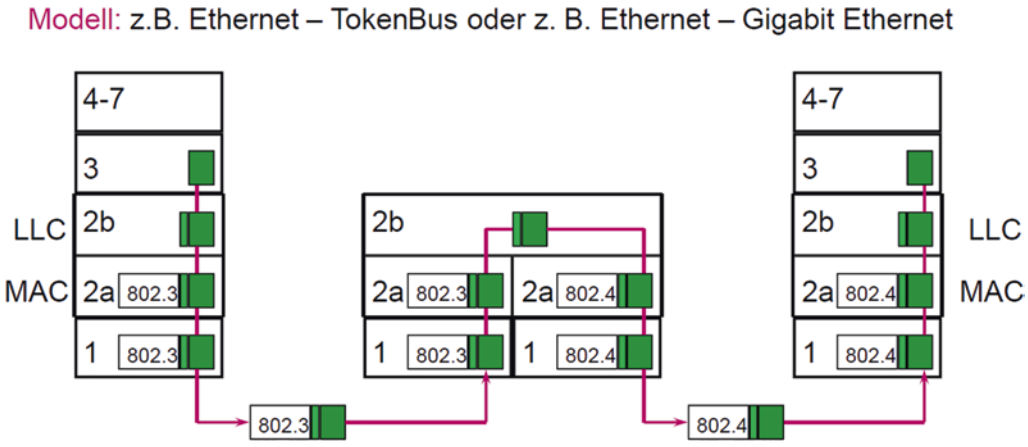


Abb. 14.4 Beispiel „Translating Bridge"

wird die folgende Umwandlung vorgenommen: Ethernet – Token Bus oder z. B. Ethernet – Gigabit Ethernet.

Die Aufgaben des sog. Translating Bridge sind dabei wie folgt:

- Formatanpassung (z. B.: Längenfeld bzw. Rahmenbegrenzung)
- Leistungsanpassung und Pufferung (z. B. 0,01 … 40 GBit/s)
- Anpassung von Rahmenlängen (Fragmentieren/Reassemblieren, z. B.
- durch hierarchisches Nummernschema).

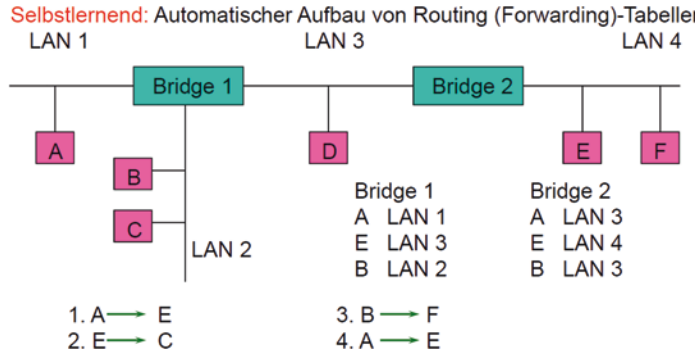


Abb. 14.5 Beispiel „Transparent Bridge"

Transparent Bridge Ein Beispiel für das Verfahren „Transparent Bridge" ist in Abb. 14.5 erkennbar. Die Topologie-Erkennung erfolgt durch Auswertung der Quelladressen, was den schrittweisen Tabellenaufbau ermöglicht. Diese Tabellen heißen „Forwarding"-Tabellen (von „weiterleiten" – „to forward") und beinhalten die physikalische MAC-Adressen der anzukoppelnden Netzgeräte und den zugehörigen E/A-Port.

Das zugrundeliegende Verfahren und das darauf basierende Protokoll „Transparent Bridge" funktioniert wie folgt:

- Fluten, falls Zielrechner noch unbekannt.
- Neuer Eintrag Quell-MAC/LAN-Port, falls Quelladresse noch nicht bekannt.
- Löschen von Einträgen nach bestimmter Zeit zur Anpassung an Topologieänderungen.

Bei der initialen Adressierung der Frames (von … bis …) wie in obiger Abbildung sehen die Forwarding Tabellen (FT) nach wenigen Schritten (Selflearning) für die erfasste Topologie folgendermaßen aus (Tab. 14.1):

Tab. 14.1 Beispielhafte Forwarding Tabellen für Bridge 1 und Bridge 2

FT Bridge 1		FT Bridge 2	
Ziel	LAN	Ziel	LAN
A	LAN1	A	LAN3
E	LAN3	E	LAN4
B	LAN2	B	LAN3

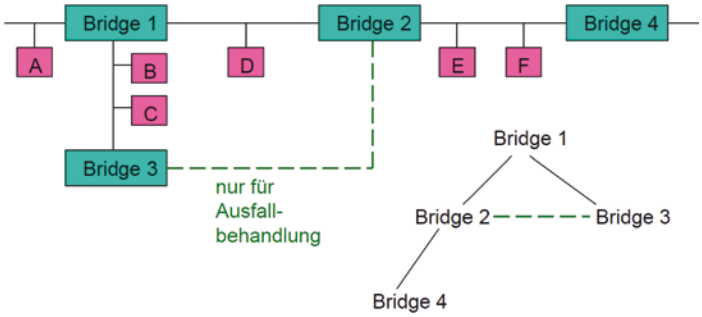


Abb. 14.6 Beispiel „Spanning Tree"

Spanning Tree Ein weiteres Basisverfahren heißt „Spanning Tree" (ST).

Die Nutzung des Verfahren hilft beim Lösen des folgenden Problems: Mehrfachwege in der Topologie und die dadurch entstehenden Endlosschleifen. Die Idee basiert auf dem Dijsktra-Algorithmus, d. h. dem Aufbau eines virtuellen überspannenden Baums über vermaschte LANs (Abb. 14.6). Der Aufbau eines „überspannenden Baumes" mit eindeutigen Wegen löst das Problem komplett. Das Verfahren funktioniert durch einen dezentralen Algorithmus zur Ermittlung des kürzesten Weg zur Wurzel (muss zu Beginn des Algorithmus manuell gewählt werden).

Bridges mit Source-Routing Ein spezielles Verfahren in Bridgetechnik heißt „Source Routing". Dieses funktioniert vereinfacht wie folgt (s. Abb. 14.7):

- Die LANs werden eindeutig nummeriert (i. d. R. mit 12 Bit-Codierung)
- Die Bridges – nur innerhalb der LAN (mit 4 Bit)
- Der Sender gibt vollständigen Weg zum Ziel an (B1, LAN2, B2, LAN3, B3,…). Die Wegermittlung erfolgt initial durch das Fluten und Rückwärtslernen mittels sog. Suchrahmen

Der Vorteil des Verfahrens liegt in der besseren Bandbreitennutzung durch Nutzung alternativer Pfade im Netz. In dem in der Abbildung referenzierten Beispiel wird ein Frame vom

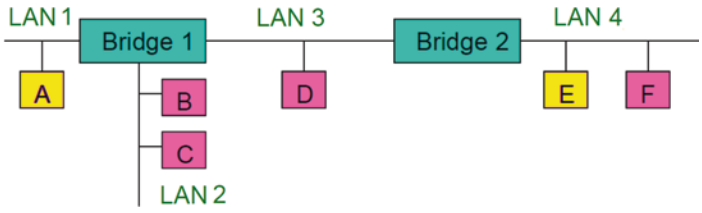


Abb. 14.7 Beispiel „Source Routing"

Tab. 14.2 Vergleich von Bridge-Verfahren: TB vs. SR

Eigenschaften des Verfahrens	Transparent Bridge (TB)	Bridge mit Source Routing (SR)
Art der Kommunikation	Verbindungslos	Verbindungs-orientiert
Konfigurierung	Automatisch	Manuelle Nummerierung
Wegewahl	Nicht optimal (über-spannender Baum)	Optimal
Funktionalität wird realisiert durch	Durch Bridge	Rechner (Endsystem)
Einsatz	Regelbetrieb (IEEE 802.1)	Testfälle, Spezialfälle

Rechner A im LAN 1 zum Rechner E im LAN 4 gesendet. Dabei wird der komplette Übertragungsweg spezifiziert:
A → E = {Bridge 1; LAN 3; Bridge 2; LAN4}

Den Vergleich von beiden Verfahren kann man in Tab. 14.2 sehen.

Die Bridges kann man auch als Zweiportswitches betrachten.

Layer-2-Switches Nachdem wir die Basis für die Switches verstanden haben diskutieren wir das Grundprinzip von Layer-2-Switches. Die Layer-2-Switches sind derzeit die in der Praxis wichtigsten aktiven Kopplungselementen in Netzwerken.

Das Ziel liegt in der zeitparallelen Vermittlung mehrerer Eingangsports an mehrere Ausgangsports (mehr als zwei). Dies bringt eine hohe Leistung und muss i. d. R. durch die Hardware-Realisierung unterstützt werden. Das „Herz" der parallelen Vermittlung mehrerer E/A-Ports ist die sog. „Switching Matrix" oder „Switching Fabrik" (s. Abb. 14.8).

Der typische Einsatz von Switches erfolgt auf Schicht 2 in lokalen Netzen (Switched Ethernet bzw. MPLS-Netze). Dabei sind die Switches im Prinzip „Multiport Bridges". Ein spezieller Fall ist die Virtualisierung von Switches durch das sog. Software-Defined Networking (SDN) mit den Protokollen OpenFlow oder VXLAN (s. Teil III), wobei die Switches und deren Protokolle als effiziente Software emuliert werden.

Die Layer-2-Switches lassen sich nach der Realisierung in zwei Arten unterscheiden:

1. „Cut-Through-Switch" (CT-Switch):
   Ankommende Frames werden nach Prüfung der Zieladresse sofort weitergeleitet, d. h. effizient, mit kurzer Verzögerung, aber problematisch bei unterschiedlichen Datenraten und bei Fehlern.

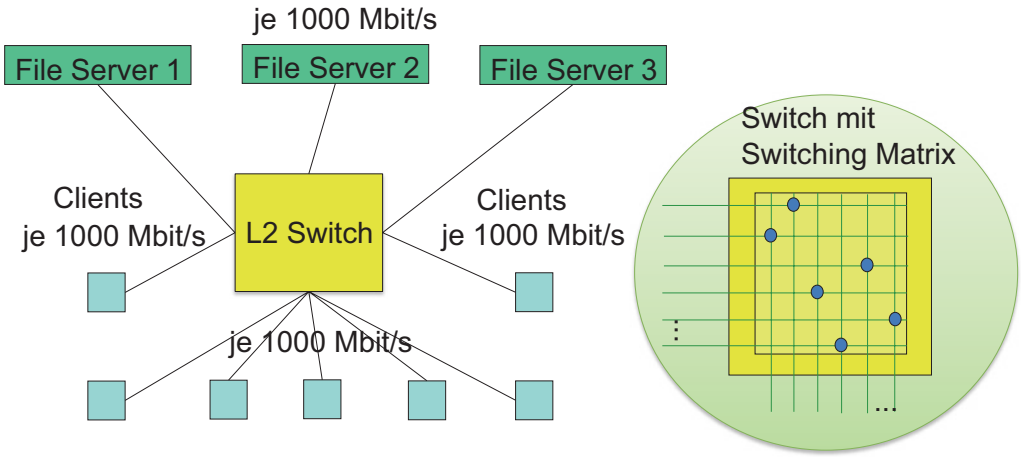


Abb. 14.8 „Switching Matrix" bei einem Layer-2-Switch

2. „Store-and-Forward-Switch" (SF-Switch):
   Gesamter Frame wird im Switch zwischengespeichert, die Prüfsumme wird kontrolliert und erst dann wird weitergeleitet => einfach; Pufferung; Datenratenanpassung möglich, allerdings größere Verzögerung im Switch.
3. Mischform (CT + SF):
   Zuerst als SF, weiterhin bei der Verringerung der Fehlerrate im Datenstrom als CT für effiziente Weiterleitung von MAC-Frames.

14.1.3 Routing

Als „Rivale" zum „Switching" in der Schicht 2 funktioniert „Routing" in der Schicht 3. Ein Router realisiert das folgende Kopplungsmodell (s. Abb. 14.9). Die Implementierung eines Routers erfolgt in der Regel in Hardware, ist aber auch in Software auf Standard-PCs möglich.

Die folgenden Routinen werden dabei implementiert [3]:

- 3a: Subnet-Zugriffsschicht: Adressierung, Weiterleitung in homogenen Netzen
- 3b: Subnet-Erweiterungsschicht: Anpassung von Formaten und Adressen
- 3c: Internet-Teilschicht: Kopplung unter einheitlichen Bedingungen.

Die Router koppeln heterogene Netzwerke zu einem weiträumigen Verbundsystem (Intranet, Extranet, Internet). Als Kopplungselement ermöglicht der Router den Einsatz von IP (Internet Protocol) und begleitenden Routingprotokollen, wie

Achtung! Ehemals bedeutete der Begriff „Gateway" auch einen Router bzw. „Border Router" (Router an der Grenze)!

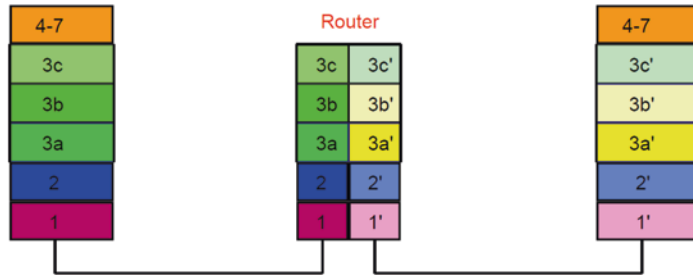


Abb. 14.9 Router: Kopplungsmodell

z. B. OSPF (Open Shortest Path First) und BGP (Border Gateway Protocol). Das Routingprotokoll OSPF eignet sich am besten für die verschlossenen kleineren IP-Bereiche, BGP wirkt dagegen optimal an der Grenze solcher Bereiche (s. Teil I).

Die angekoppelten IP-Router, IP-Subnetze und die IP-fähigen Endgeräte interagieren unter Nutzung universeller (weltweit eindeutiger) Adressen, die in den sog. Routingtabellen mit zugehörigen Wegeinformationen abgespeichert werden. Die Ermittlung der optimalen Adresstabellen nennt man „Routing", das zum IP-Betrieb abwechselnd und ergänzend über die Schicht 3 stattfindet.

Ein Beispiel zum Aufbau einer Routingtabelle für den Router 1 entnehmen Sie in Abb. 14.10. Die unmittelbar erreichbaren Netzwerke 192.168.2.0 und 192.168.1.0 (direkte Routen) haben eine einfache Metrik (bspw. Anzahl von Hops = 0). Über den Router 2 kann man das Netz 192.168.0.0 mit der Metrik 1 erreichen.

Die Netzadressen der Klasse C sowie die konformen Masken 255.255.255.0 sind in den erwähnten Netzen privat (wie es in Intranets typisch ist). Außerhalb dieser drei Netze ist über den Router 3 (Adresse 192.168.0.254 im Intranet 192.168.0.0) der Ausgang zum Internet möglich über die zweite, weltweit routebare Adresse des Routers 3 (138.52.4.11).

Der Router 3 muss NAT-fähig sein und ermöglicht dabei die Umwandlung der privaten Adressen in weltweit routebare Adressen (hier IPv4-Adresse der Klasse B). In der Routingtabelle des Routers1 wird ein fiktives Maß für Internet-Zugang angenommen (Metrik 6).

Oft liegt in der Rechnernetzpraxis das Netzwerkkopplungsdilemma vor: „Switching" oder „Routing"? Was ist effizienter bei der Datenübertragung im Netz? Als Abhilfe verwendet man die nachfolgende Kombination.

Hybride Lösung: IP-Switches/Layer-3-Switches Ein hybrider IP-Switch/Layer-3-Switch ist eine leistungsfähige Kombination von einem Router und einem Switch. Zunächst erfolgt Routing

Router 1:

Netzadresse	Netzmaske	Router	Anzahl Hops
192.168.0.0	255.255.255.0	192.168.1.1	1
192.168.1.0	255.255.255.0	*	0
192.168.2.0	255.255.255.0	*	0
0.0.0.0	0.0.0.0	192.168.1.1	6 (fiktives Maß für Internet-Zugang)

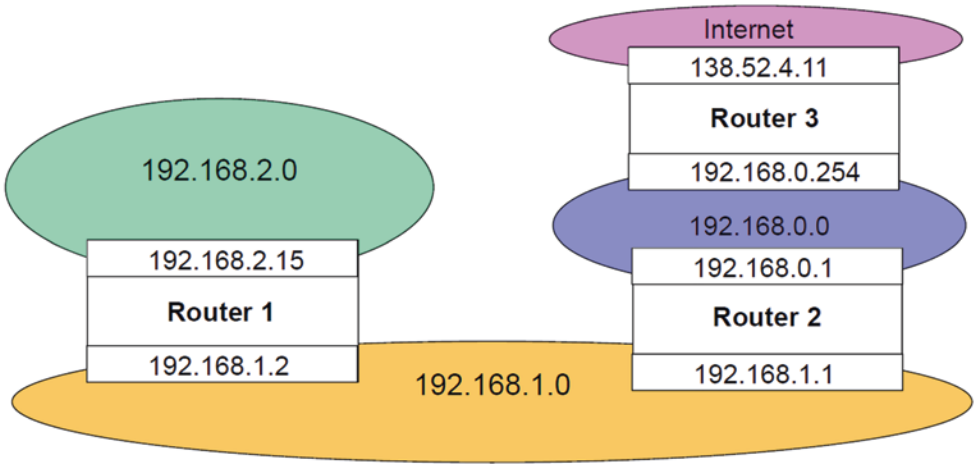


Abb. 14.10 Beispiel einer Routingtabelle (hier: für Router 1)

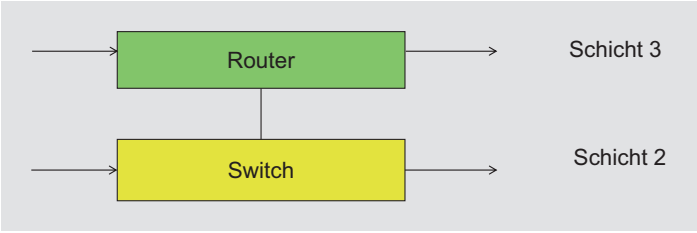


Abb. 14.11 Hybride Lösung: Layer 2 (Frames) + Layer 3 (IP-Datagramme)

mit Übertragung von IP-Datagrammen, bei längerer Dauer von Datenströmen wird ggf. auf Switching umgeschaltet. Der Transfer von LAN-Frames kann ggf. auch auf Basis von MPLS (Multiprotocol Label Switching) erfolgen. Ein hybrider IP-Switch realisiert das folgende Kopplungsmodell (Abb. 14.11).

Diese leistungsfähige Kombination (Routing + Switching) optimiert die entstehenden Verzögerungen bei der aktiven Kopplung.

14.1.4 WLAN Access Points

Ein WLAN Access Point (AP) steht für einen drahtlosen Zugangspunkt oder für eine Basisstation. AP wird ein

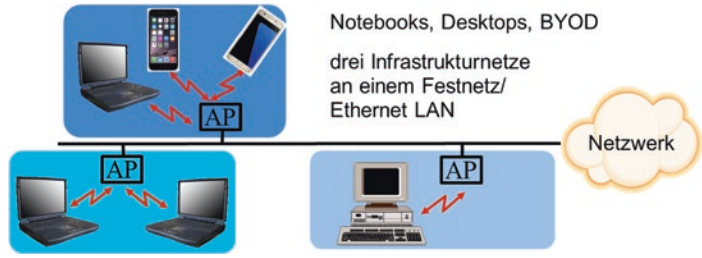


Abb. 14.12 Beispiel „WLAN im Infrastrukturmodus mit drei APs"

elektronisches Gerät genannt, das als Schnittstelle für drahtlose und drahtgebundene Kommunikationsgeräte fungiert. Man unterscheidet im WLAN-Einsatz zwei Modi:

- Infrastrukturmodus
- Ad-hoc-Modus

Im Infrastrukturmodus sieht die Kommunikation ähnlich einem Stern-Netzwerk aus. Der Access-Point ist zentraler Punkt dabei. Der AP koordiniert die Netzknoten (Notebooks, Desktop PCs, Smartphones sowie BYOD – Bring Your Own Device) und vermittelt Nachrichten in andere Netze (s. Abb. 14.12).

Der Zugriff zum drahtlosen Medium erfolgt per CSMA/CA-Protokoll mit Ergänzungen in Form RTS/CTS (s. vorige Abschnitte). Die Kommunikation im drahtgebundenen Teil kann per CSMA/CD oder individuell als Switched Ethernet realisiert werden.

Ad-hoc-Netze entstehen spontan und organisieren und verwalten sich selbst. Im Ad-hoc-Modus braucht ein Funknetz keinen AP, sondern die Kommunikation zwischen zwei Endgeräten erfolgt über den WLAN-Adapter (Netzkarte).

Ad-hoc-Modus in einem WLAN funktioniert ähnlich einem Peer-to-Peer-Netzwerk, dabei ist keine zentrale Station bzw. übergeordnete Infrastruktur vorhanden und alle Netzknoten treten gleichwertig auf (Abb. 14.13).

Abb. 14.13 Beispiel „WLAN im Ad-hoc-Modus mit drei APs"

Oft kommt ein zusätzlicher Beaconing-Mechanismus zum Einsatz. Dieser vervollständigt das CSMA/CA-Verfahren (s. Teil I). Jeder Knoten sendet in regelmäßigen Abständen ein Beacon-Signal („Beacon" steht auf Englisch für Leuchtfeuer). Dies dient dazu, jedem Knoten die Knoten bekannt zu machen, die er direkt erreichen kann.

OLSR, das Optimized Link State Routing Protocol, wurde für mobile Ad-hoc- Netze entwickelt. Es arbeitet als tabellengestütztes Protokoll, welches die Änderungen an den Topologieinformationen des Netzwerkes speichert. Die Knoten welche als Multipoint Relay (MPR) von Nachbarknoten ausgewählt wurden geben diese Änderungen regelmäßig in ihren Kontrollnachrichten bekannt. Dabei gibt ein Knoten regelmäßig dem Netzwerk bekannt, dass er Verbindung hat zu Knoten, die als MPR ausgewählt waren. Bei der Routenberechnung werden die MPRs benutzt, um einen Weg von einem Knoten zu einem beliebigen Knoten im Netzwerk zu finden. Das Protokoll benutzt die MPRs, um effizient Kontrollnachrichten über das Netz zu senden (nach ETSI).

Die allgemeine IEEE 802.11-konforme Architektur für die WLAN-Kommunikation beinhaltet die folgenden Komponenten für die Kombination drahtloser und drahtgebundener Kommunikationsgeräte (◘ Abb. 14.14).

Die Architekturkomponenten haben die folgende Bedeutung:

- Station (STA): Endgerät mit 802.11-Schnittstelle
- Access Point (AP): erlaubt den angemeldeten Stationen den Zugang zum Distribution System
- Basic Service Set (BSS): AP und zugehörige Stationen
- Independent BSS (IBSS): WLAN im Ad-hoc-Modus
- Distribution System: verbindet mehrere BSS über die Zugangspunkte und formt damit ein logisch größeres Netz
- Extended Service Set (ESS): die über das Distribution System verbundenen Funknetze
- Portal: ermöglicht Übergang in andere Netze (drahtloser und drahtgebundener Art).

14.1.5 Firewalls

Die Firewalls (FW) spielen bei der Netzwerkskopplung eine besonders wichtige aber auch duale Rolle:

- einerseits sind diese bloß normale aktiven Komponenten, die sog. Layer-N-Gateways,
- andererseits fungieren diese als spezielle Sicherungssysteme, die ein Netz oder angekoppeltes Terminal/Endgerät/einzelner Computer vor unerwünschten Netzwerkzugriffen schützten.

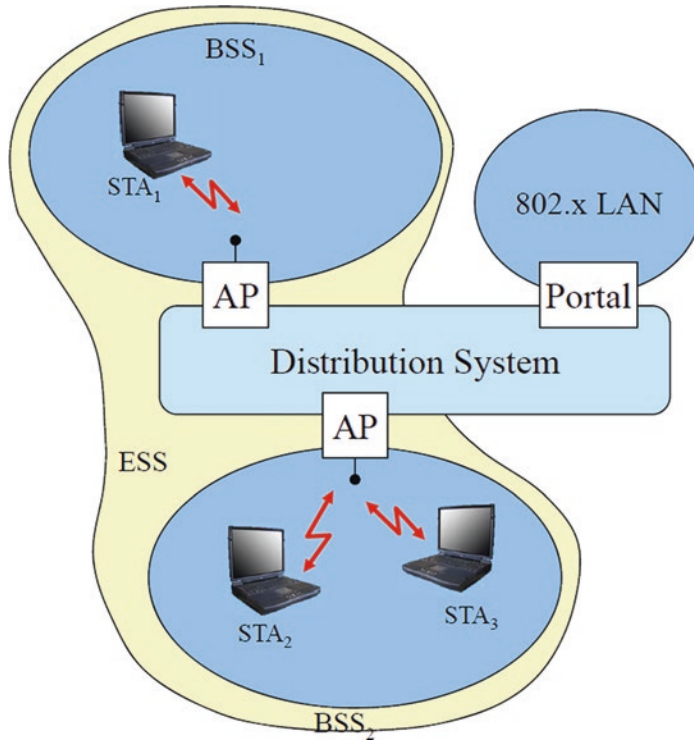


Abb. 14.14 IEEE 802.11 -Architektur für WLAN-Kommunikation

Die Firewall-Konzepte sind dadurch von spezieller Bedeutung für die Absicherung der Datenübertragung in Netzwerken und Anwendungen. Aus diesem Grund wurden die Firewall-Konzepte in Teil III ausgelagert!

Dort gehen wir mehr ins Detail bzgl. der Einordnung ins OSI-Referenzmodell, bzgl. der Zuordnung der Filterungsmöglichkeiten, sowie deren fortgeschrittene Filtereigenschaften, bzgl. Protokollanalyse, Intrusion Detection und Prevention (IDS/IPS), u. a. auch CIDN (Collaborative Intrusion Detection Networks).

14.2 Praktisch relevante Übertragungsmedien

Trotz des aktuellen Booms für Funknetze leisten kabelgebundene Netze den überwiegenden Anteil aller Datenübertragungen, weil sie i.a. den Teilnehmern höhere Nutzdatenraten bereitstellen. Hauptursache ist, dass es in Kabelnetzen geringere Störungen gibt und sich dadurch effizientere Signalkodierungsverfahren mit höheren Datenraten einsetzen lassen [5].

Die wichtigsten Kabelarten sind:

- Asymmetrische Kabel
- Koaxialkabel
- Symmetrische Kabel
- Hohlleiter
- Lichtwellenleiter.

Asymmetrische elektrische Kabel (Abb. 14.15) gibt es in verschiedenen Ausführungen. Am einfachsten sind Kabel mit 2 oder mehr Adern (isolierte Drähte). Eine Ader ist mit dem Null-Potential verbunden, die anderen transportieren elektrische Signale. Der Null-Leiter kann eingespart werden, wenn auf beiden Seiten ein gemeinsames Erdpotential existiert. Ein sauberer Potentialausgleich ist jedoch problematisch. Die asymmetrischen Kabel sind anfällig gegen induktive Störeinflüsse, z. B. durch andere Netzwerkkabel, Mikrowellengeräte usw., außerdem stören sie selbst die Umgebung. Sie können nur im Niederfrequenzbereich verwendet werden. Die hohen Übertragungsraten in modernen Rechnernetzen erfordern aber Übertragungsfrequenzen im MHz- und im GHz-Bereich. Für die meisten Netztechnologien sind asymmetrische Kabel daher nicht geeignet.

Koaxialkabel (Abb. 14.16) sind spezielle asymmetrische Kabel. Sie sind rotationssymmetrisch aufgebaut und besitzen einen elektrischen Innenleiter mit umliegender Isolation (Dielektrikum) und eine geerdete Abschirmung. Sie sind für

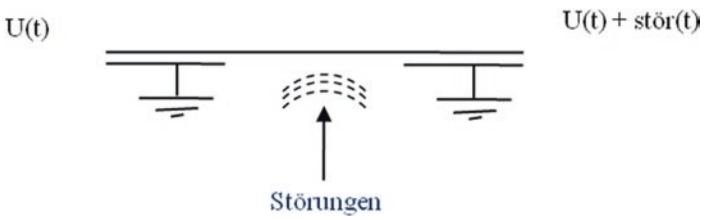


Abb. 14.15 Asymmetrische Kabel

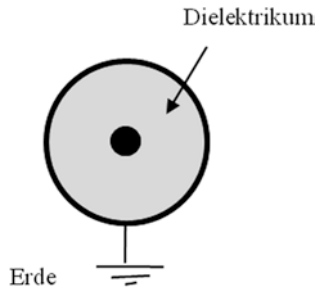


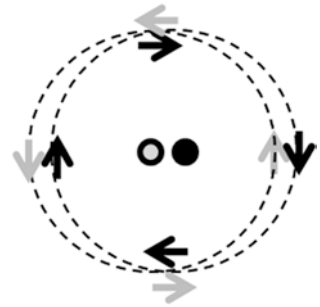
Abb. 14.16 Koaxialkabel

den Hochfrequenzbereich geeignet und besitzen ein gutes Störverhalten. Die Schirmung verhindert weitgehend das Ein- und Austreten elektromagnetischer Felder. Der Potentialausgleich an den Kabelenden kann jedoch Probleme bereiten. Koaxialkabel werden zum Teil genutzt für die Anbindung lokaler Netze an Weitverkehrsnetze.

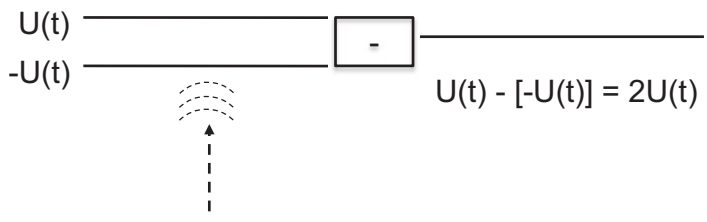
Symmetrische elektrische Kabel (◘ Abb. 14.17) arbeiten mit Adernpaaren, über die Stromstöße geschickt werden. Auch bei fehlender Schirmung des Adernpaares stören symmetrische Kabel kaum die Umgebung, Dies liegt daran, dass in beiden Adern die Stromrichtung entgegengesetzt ist (Hin- und Rückstrom) und sich die durch die Signalübertragung erzeugten elektromagnetischen Felder in größerem Abstand vom Adernpaar weitgehend auslöschen.

Bei Signalübertragungen in symmetrischen Kabeln (◘ Abb. 14.18) liegt an einer Ader die positive Signalspannung und an der anderen Ader die negative Signalspannung an. Beim Empfänger bildet ein Differenzverstärker die doppelte Signalspannung zur Signalverarbeitung. Der Vorteil gegenüber asymmetrischen Kabeln besteht darin, dass induktive Störeinflüsse auf beiden Leitungen additiv auftreten und deshalb durch die Differenzbildung (nahezu) ausgelöscht werden.

Die Störfestigkeit kann nochmals gesteigert werden, wenn die Adernpaare verdrillt sind (◘ Abb. 14.19). Dabei führen die



◘ **Abb. 14.17** Feldauslöschung bei symmetrischen Kabeln



◘ **Abb. 14.18** Eliminierung von Störfeldern durch Differenzverstärker bei symmetrischen Kabeln

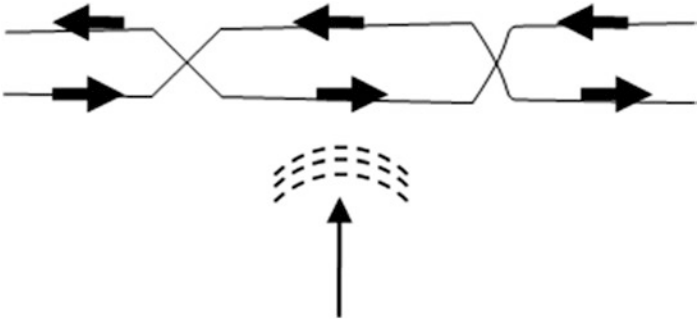


Abb. 14.19 Twisted-Pair-Kabel

Störspannungen in beiden Adern des Paares zu gegensätzlichen Störströmen, die sich (beinahe) auslöschen. Diese sog. TP-Kabel („Twisted Pair") werden sehr häufig in lokalen Rechnernetzen eingesetzt, wenn die Länge der Übertragungsstrecken unter 100 m liegt.

Elektrische Hohlleiter sind Rohrprofile, in deren Innenräumen sich elektromagnetische Wellen fortbewegen. Je nach Gestaltung des Profiles werden bestimmte Wellenlängen (Modi) bevorzugt übertragen. Hohlleiter besitzen gute Hochfrequenzeigenschaften und sind verbreitet in der Radartechnik, in Rechnernetzen spielen sie jedoch keine herausragende Rolle.

Lichtwellenleiter (Abb. 14.20) sind die leistungsstärksten Übertragungsmedien. Sie bestehen aus einer inneren Glasfaser (evtl. mehrere) mit Glaskern, -mantel und -beschichtung. Um die Faser befindet sich eine Schutzschicht (Sekundärbeschichtung), ein Kunststoffgarn als Zugentlastung und ein Kabelmantel.

Die Faser kann Lichtimpulse übertragen. Elektromagnetische Störfelder beeinflussen die Übertragung nicht. Die Leistungsdämpfung hängt vom Glasmaterial und von der Wellenlänge ab. Wegen besonders günstiger Dämpfungswerte und wegen der Verfügbarkeit geeigneter Sende- und Empfangsdioden wird überwiegend mit den Wellenlängen 850 nm, 1310 nm und 1550 nm gearbeitet („Sendefenster").

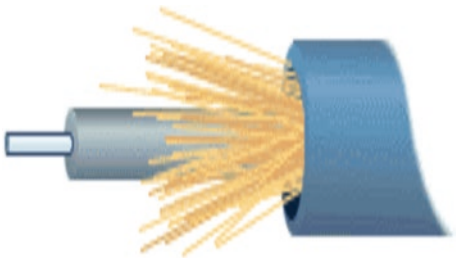


Abb. 14.20 Lichtwellenleiter

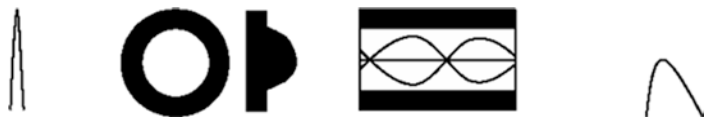
Lichtwellenleiter erlauben sehr hohe Datenraten. Es gibt mehrere Ausführungsformen, Multimode-Stufenindexfasern, Multimode-Gradientenfasern und Monomodefasern.

Multimode-Stufenindexfasern (◘ Abb. 14.21) haben einen inneren Kern (40 bis 100 µm Durchmesser), der von einem Mantel mit einem anderen Brechungsindex umgeben ist. Multimodefasern besitzen einen relativ großen Einstrahlwinkel (Apertur), deshalb können preiswerte LED-Dioden als Lichtquelle dienen. Die Lichtstrahlen bewegen sich auf verschiedenen Ausbreitungswegen (Modi). Der Mittelstrahl hat die kürzeste Laufzeit durch die Faser, die anderen schräg eingefallenen Strahlen benötigen eine längere Zeit. Dieser Effekt wird als Modendispersion bezeichnet und führt am Kabelausgang zu einer zeitlichen Verlängerung der Lichtimpulse. Dies kann bei größeren Kabellängen zu Beschränkungen der Pulsfrequenz und damit der erzielbaren Datenrate führen. Ein Maß für diese Beschränkungen ist das „min. Bandbreitenlängenprodukt". Dieses ist definiert als Produkt der maximal erreichbaren Pulsfrequenz mit der Kabellänge und wird in MHz*km gemessen.

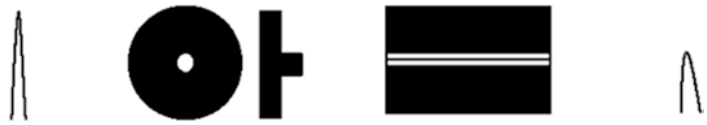
Eine Verringerung der Modendispersion kann durch Multimode-Gradientenindexfasern (◘ Abb. 14.22) erreicht werden, bei denen der Brechungsindex des Glaskerns variabel ist. Damit wird ein Linseneffekt erzielt, der die Variation der Laufzeiten der verschiedenen Strahlen reduziert.

Praktisch keine Modendispersion weisen Monomodefasern (◘ Abb. 14.23) auf, bei denen der Glaskern nur 5 bis 9 µm dick ist. Dadurch ist nur ein Ausbreitungsweg möglich und es findet keine Impulsverbreiterung statt. Dies ermöglicht

◘ **Abb. 14.21** Multimode-Stufenindexfaser



◘ **Abb. 14.22** Multimode-Gradientenindexfaser



◘ **Abb. 14.23** Monomodefaser

die Übertragung mit höchsten Datenraten auch über große Entfernungen. Allerdings müssen teure Laserdioden als Lichtquelle eingesetzt werden, um die erforderliche Lichtleistung durch den geringen Eingangsquerschnitt zu bringen.

Kabelgebundene Rechnernetze nutzen vorwiegend TP-Kabel auf Kupferbasis und Lichtwellenleiter.

TP-Kabel auf Kupferbasis sind preiswert und lassen sich sehr kostengünstig montieren und verlegen. Nachteilig sind evtl. gegenseitige Beeinflussungen über elektromagnetische Felder. Dieses sog. Nebensprechen muss durch hochwertige Produkte in Grenzen gehalten werden, um Abhörsicherheit und Störfestigkeit zu gewährleisten. TP-Kabel erlauben hohe Datenraten, allerdings nur über kurze Distanzen bis ca. 100 m wegen der starken Abhängigkeit der Dämpfung von Frequenz und Länge.

Lichtwellenleiter sind leistungsfähiger, besonders über längere Strecken. Außerdem weisen sie kein Nebensprechen auf und es gibt keine Probleme mit dem elektrischen Potentialausgleich. Glasfaserkabel besitzen aber auch einige Nachteile gegenüber TP-Kabeln. Die Kosten für Kabel und die erforderliche Messtechnik sind erheblich höher. Weiterhin gibt es einen wesentlich höheren Aufwand für Stecker- und Buchsenkonfektion und besonders für die Verlegearbeiten. Die Kabel sind sehr empfindlich, d. h. sie müssen sehr vorsichtig und mit großen Biegeradien verlegt werden, was höhere Baukosten zur Folge hat. Feuchtigkeit, Staub usw. können die Lebensdauer der Kabelinstallation erheblich reduzieren.

Wegen o. g. Eigenschaften dienen die TP-Kabel als Standardmedium in lokalen Rechnernetzen. Lichtwellenleiter dominieren bei Übertragungsstrecken über 100 m Länge. In Weitverkehrsnetzen werden sie fast ausschließlich verwendet.

14.3 Verkabelungstopologien

Optimal für die Informationsübertragung wäre ein vollvermaschtes Netz (◘ Abb. 14.24), d. h. jeder Rechner ist mit jedem anderen Rechner des Netzes über eine Duplexleitung verbunden. Dies ist jedoch nur in sehr kleinen Netzen möglich, da die Leitungsanzahl mit der Anzahl der Rechner im Netz sehr stark ansteigt.

Das andere Extrem ist die Verwendung eines Busses (◘ Abb. 14.25), d. h. eines gemeinsam genutzten Übertragungskabels („shared medium“), über das sich die Signale passiv in beide Richtungen ausbreiten. Busse lassen sich einfach realisieren. Sie sind aber für größere Systeme schlecht geeignet, da für die Nutzer meist nur eine geringe Nutzdatenrate zur Verfügung steht, weil die Bruttodatenrate des Netzwerkes auf alle aktiven Nutzer aufgeteilt wird.

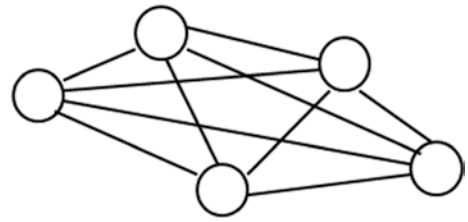


Abb. 14.24 Vollvermaschtes Netz

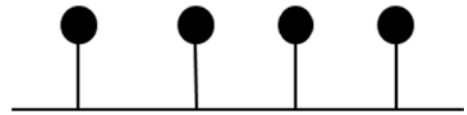


Abb. 14.25 Bus

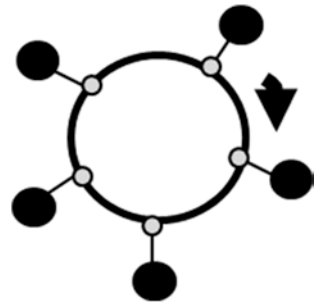


Abb. 14.26 Ring

Eine weitere einfache Topologie ist die Ringstruktur (Abb. 14.26). Hierbei erfolgt eine gerichtete Signalausbreitung über Ringsegmente. Zwischen jedem Segment erfolgt eine aktive Signalauffrischung. Der Ring kann als „shared medium" genutzt werden. Es ist aber auch möglich, große Ringe zu realisieren, in denen mehrere Signalfolgen gleichzeitig den Ring umlaufen.

Ebenfalls verbreitet ist eine Stern- bzw. Baumtopologie (Abb. 14.27), bei der die Nutzer mit Konzentratoren verbunden sind, die Signalströme passiv oder aktiv weiterleiten. Gegenwärtig dominiert diese Topologie den Bereich der lokalen Rechnernetze.

Die allgemeinste Topologie ist die der teilvermaschten Netze (Abb. 14.28), bei denen die Rechner mit einer Untermenge aller anderen Rechner verbunden sind. Da nicht jeder Rechner auf direktem Wege erreicht werden kann, müssen einige Rechner Vermittlungsaufgaben wahrnehmen. Diese Topologie ist in Weitverkehrsnetzen verbreitet.

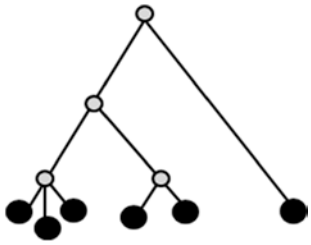


Abb. 14.27 Baum

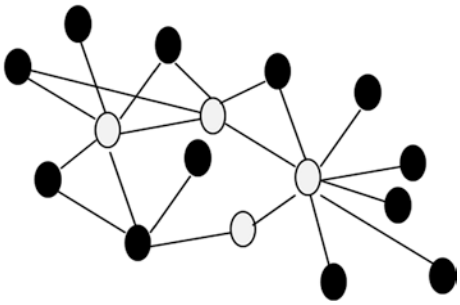


Abb. 14.28 Teilvermaschtes Netz

14.4 Bedarfsverkabelung

Die ersten technisch bedeutsamen lokalen Rechnernetze entstanden in den 1980-er Jahren. Der Kostenanteil der Kabelinfrastruktur an IT-Technik war gering. Die Standorte der Arbeitsstationen und Server bestimmen die Kabelführung.

Der wichtigste Vertreter war Ethernet IEEE 10Base5. Verwendet wurde eine Bustopologie mit einem dicken (1 cm) starren Koaxialkabel (Biegeradius 25 cm). An dieses wurden Transceiver angeklemmt, die über Stichleitungen mit den Teilnehmerrechnern verbunden waren (Abb. 14.29).

Die Ausmaße von 10Base5 waren erheblich (max. 2,5 km), die Stichleitungen konnten 50 m lang sein, die Länge eines Koaxialkabelsegments konnte bis 500 m betragen. Zudem konnten noch bis zu 5 Segmente über Signalverstärker (Repeater) verbunden werden (Abb. 14.30).

Für damalige Verhältnisse war 10Base5 ein leistungsfähiges LAN-Konzept. Die Verkabelung war jedoch sehr unzuverlässig. Wenn auch nur eine der vielen Verbindungsstellen durch ein Kontaktproblem ausfiel, kam es zum Totalausfall des Netzes. Die Fehlersuche gestaltete sich aufwendig, da die Verbindungsstellen über das ganze Gebäude verteilt waren.

Die kompatible Weiterentwicklung Ethernet IEEE 10Base2 arbeitete nach dem gleichen unzuverlässigen Verkabelungskonzept.

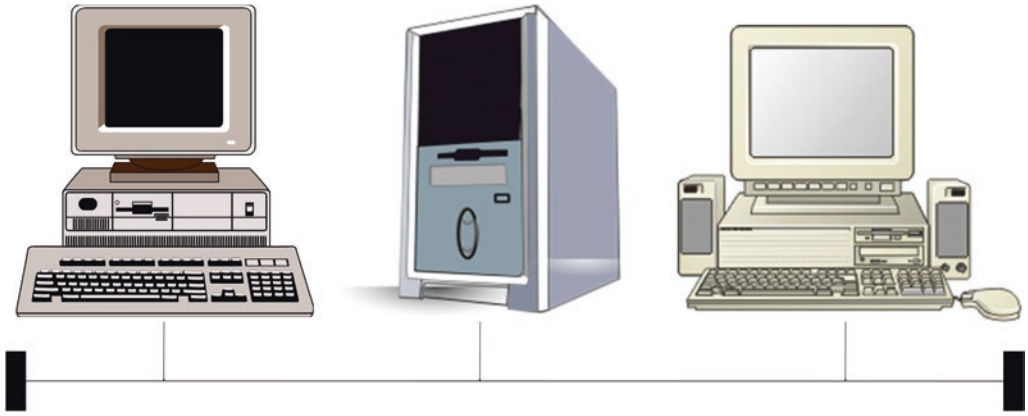


Abb. 14.29 IEEE 10Base-5

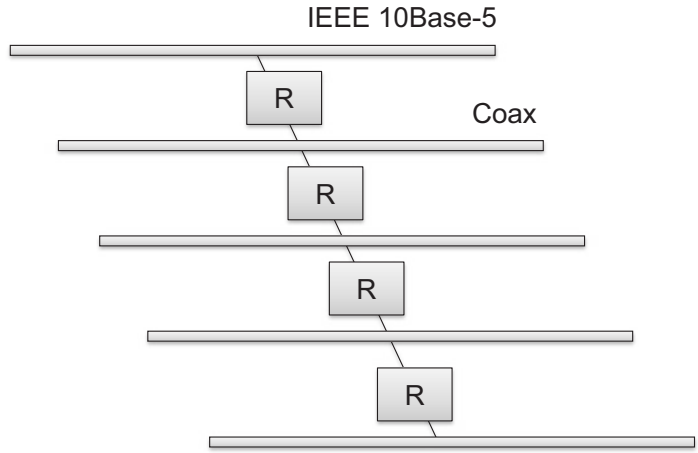


Abb. 14.30 IEEE 10Base-5: Segmentbildung

Es wurde lediglich ein anderes dünneres, leichter verlegbares Koaxialkabel verwendet, das direkt an die Netzteilnehmerrechner geführt wurde. Außerdem entfielen die Stichleitungen.

Zuverlässigere Nutzungseigenschaften versprach man sich von IEEE 10Base-T, das eine sternförmige Verkabelung vorsah. Das Verkabelungskonzept war auch mit dem Haustelefonnetz vereinbar. Die Teilnehmerrechner waren über leicht verlegbare TP-Kabel mit einem zentralen Signalverstärker (Hub) verbunden. Das Netzwerk war besser administrierbar, da es nur 2-Punkt-Leitungen gab mit weniger Verbindungstellen und alle Leitungen in einem Raum endeten. Fehlerhafte Strecken konnten vom Netzwerktechniker dadurch schnell entdeckt werden (Abb. 14.31).

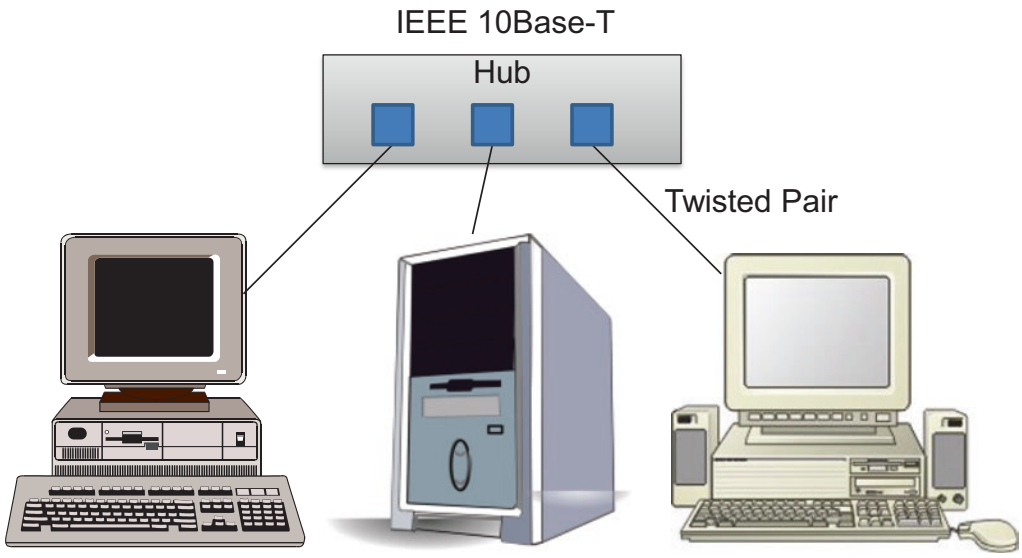


Abb. 14.31 IEEE 10Base-T

Neben den IEEE 802.3-Netzwerken waren auch andere Technologien verbreitet, z. B. IEEE 802.5 IBM Token Ring. In der Regel wurde TP-Kabel für die Verkabelung eingesetzt. Dieses Netzwerk konnte in Ringtopologie und auch in Sterntopologie realisiert werden. Die bei der Sterntopologie verwendeten Kabel hatten Adern in Hin- und Rückrichtung von einem zentralen Ringvermittler (Hub) zu den Teilnehmern. Vorteilhaft gegenüber einer physischen Ringtopologie war die geringere Fehleranfälligkeit. Im Fall eines defekten Ringteilnehmers wurde der Anschluss im Ringvermittler kurzgeschlossen und der Ring konnte weiterarbeiten (Abb. 14.32).

Die FDDI-Technologie (heute obsolete) eröffnete eine neue Qualität der LAN-Technologie in Bezug auf Datenraten und Ausdehnung. Es wurde für sog. Klasse-A-Stationen eine Ringtopologie mit zwei gegenläufigen Lichtwellenleitern realisiert. Im Falle einer Ringdurchtrennung konnten die beiden Ringe miteinander verbunden werden, sodass ohne Übertragungsausfall ein Ersatzring mit doppelter Länge gebildet wurde. Klasse-B-Stationen wurden in Sterntopologie an einen Kabelkonzentrator angeschlossen, der im Fehlerfall ebenfalls eine Rekonfiguration des Ringes vornehmen konnte (Abb. 14.33).

Bis Ende der 1980-er Jahre musste bei jeder neuen Netzwerktechnologie die Verkabelung erneuert oder modifiziert werden. Dies geschah mindestens im 5-Jahre-Rhythmus. Die Bedarfsverkabelung führte zu hohen Kosten und besonders im Falle der parallelen Nutzung alternativer Technologien zu relativ chaotische Strukturen mit verschiedenen Topologien und Kabeltypen.

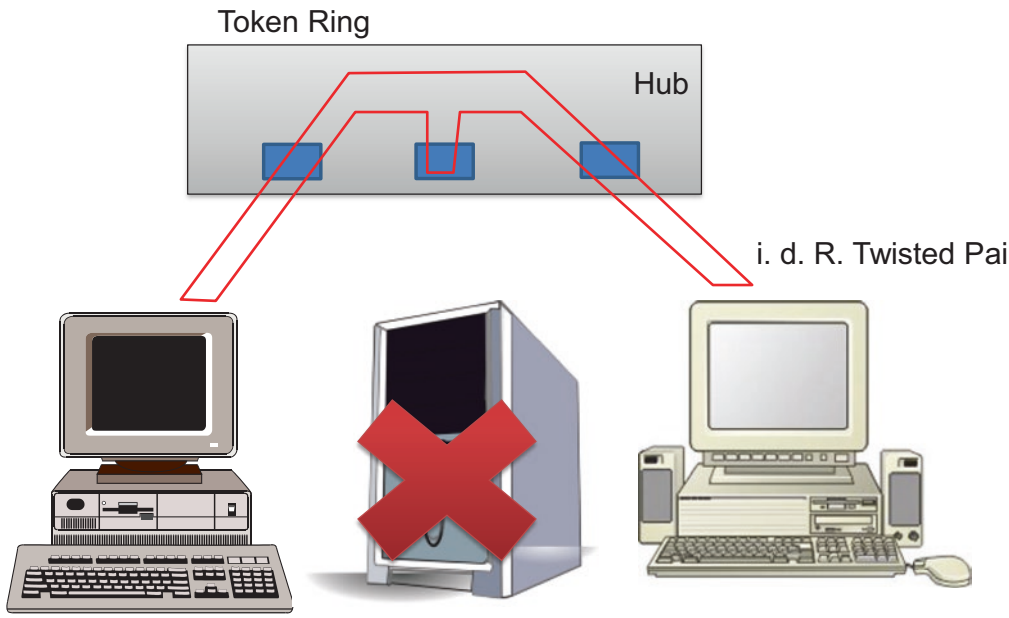


Abb. 14.32 Token Ring

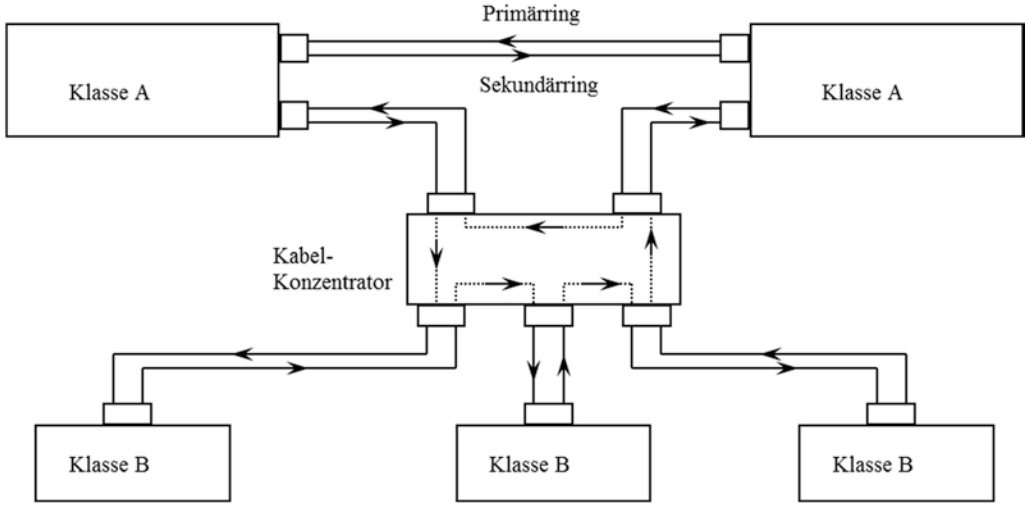


Abb. 14.33 FDDI

14.5 Strukturierte Verkabelung

Die Schlussfolgerungen aus den Problemen mit der Bedarfsverkabelung führten ab 1990 zum Prinzip der anwendungsneutralen Verkabelung.

Dabei soll die Netzwerkverkabelung als selbstverständlicher Teil der Gebäudeinfrastruktur geplant werden, wie beim Stromnetz und dem Wasserrohrnetz. Um die langfristigen Infrastrukturkosten gering zu halten soll dabei ein Zeithorizont von 10 bis 20 Jahren angestrebt werden.

Wichtige Prinzipien sind [5]:

- Verkabelung muss anwendungsunabhängig sein.
- Netztechnik muss sich an die Verkabelung anpassen, nicht umgekehrt.
- Netzwerkerweiterungen müssen möglich sein (Stationsanzahl, Übertragungsraten).
- Installation, Wartung, Fehlerkontrolle und einfaches Management müssen einfach sein.
- Hohe Zuverlässigkeit (ggf. Einplanung von Redundanz)
- Schutz vor unberechtigtem Zugriff.

1991 verabschiedeten die amerikanischen Standardorganisationen ANSI (American National Standard Institute), EIA (Electronics Industries Association) und TIA (Telecommunication Industry Association) den Standard EIA/TIA 568 „Commercial Building Telecommunications Wiring Standard“ zur sogenannten strukturierten Verkabelung.

Unter Leitung der ISO (International Organization for Standardization) schlossen sich andere Standardorganisationen im Wesentlichen dem Standard EIA/TIA 568 an. Für Europa relevant sind ab 1995 die Normen:

- ISO/IEC-11801 „General Cabling for Costumer Premises“
- EN 50173 „General Cabling Systems“.

In der Praxis sind noch außerordentlich viele Detailstandards zu beachten, u. a.:

EN 50310 - Gebäudemaßnahmen: Erdung, Potentialausgleich, …

EN 50173 - Planung der strukturierten Verkabelung

EN 50174-1 - Spezifikation/Qualitätssicherung

EN 50174-2 - Installation in Bürogebäuden

EN 50174-3 - Installation im industriellen Bereich

EN 50174-4 - Installation in Wohnungen

EN 50174-5 - Installation in Rechenzentren

EN 50288-X - Kabelnormen

EN 60603-7-X - Steckverbinder (RJ-45, …)

EN 50346 - Prüfvorschriften für installierte Verkabelung.

Weiterhin ist die elektromagnetische Verträglichkeit (EMV) zu beachten. Die EMV regelt die Begrenzung der „Störaussendung“ und Mindest-„Störfestigkeit“ von Geräten. Der Nachweis der EMV ist Pflicht und wird durch eine Konformitätserklärung

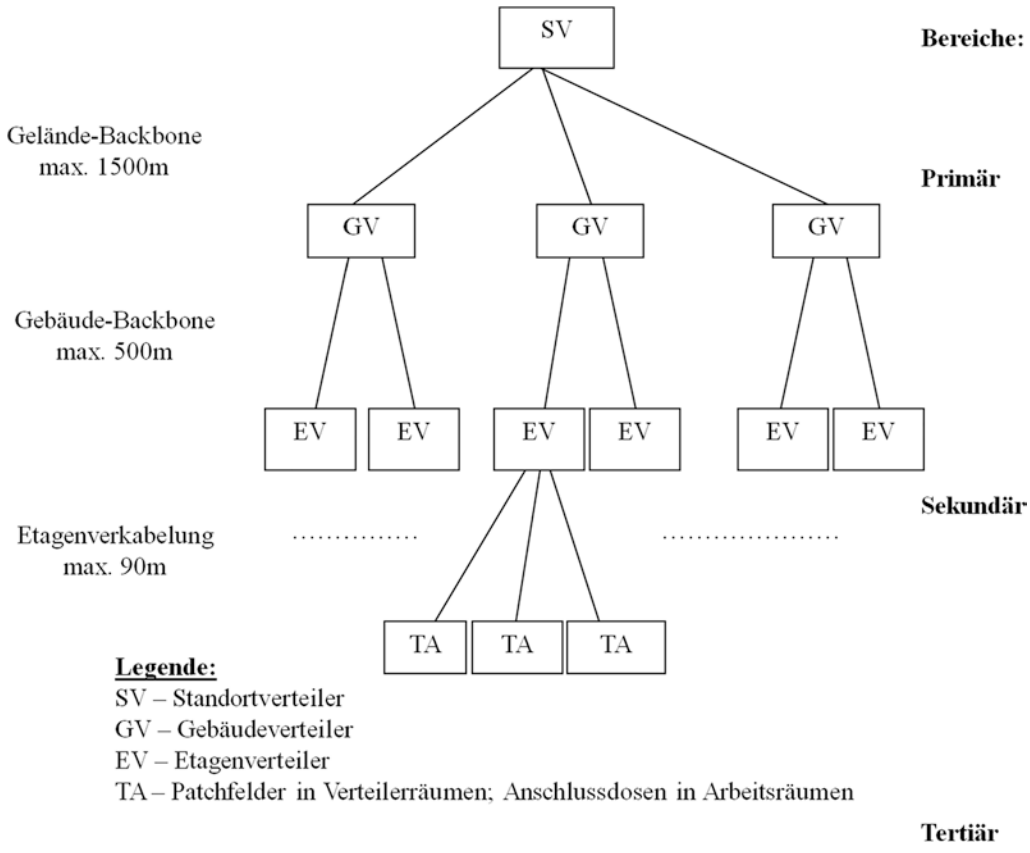
ausgewiesen, bzw. durch das CE-Zeichen (frz. „Conformité Européenne").

Wichtige Grundsätze regeln folgende Gesetze bzw. Normen:

- „Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln (EMVG)" vom 26.02.2008
- **EN 55022** - „Grenzwerte und Messverfahren für Funkstörungen von informationstechnischen Einrichtungen"
- **EN 5082** - „Fachgrundnorm Störfestigkeit".

Im Rahmen der o. g. Normen wird für die strukturierte Verkabelung eine Baumtopologie vorgeschlagen.

Ausgehend von einem Standortverteiler SV führt die Primärverkabelung (auch Arealverkabelung) sternförmig zu den Gebäudeverteilern GV. Von diesen führt die Sekundärverkabelung (auch Steigzonenverkabelung) sternförmig zu den Etagenverteilern EV. Von den Etagenverteilern geht die sternförmige Tertiärverkabelung (auch horizontale Verkabelung bzw. Etagenverkabelung) zu den Computeranschlüssen TA (◘ Abb. 14.34).



◘ **Abb. 14.34** Strukturierte Verkabelung nach EN 50173 und EIA/TIA 568

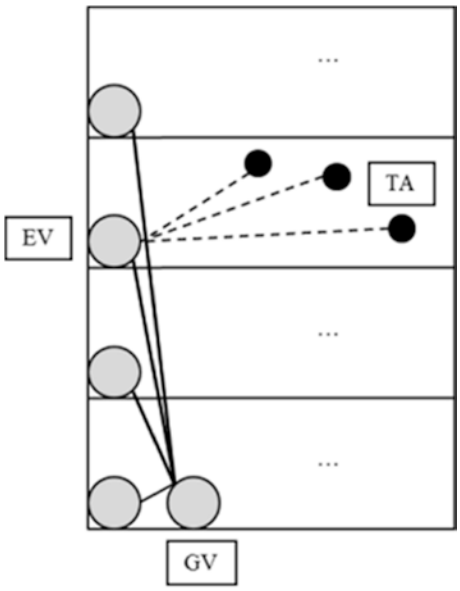
Die Primärverkabelung stellt hauptsächlich folgende Anforderungen:

- Sternförmige Trassenführung, evtl. mit Redundanz für Notfälle
- Potentialtrennung zwischen Gebäuden
- elektrische Störungsfestigkeit, Erweiterbarkeit, Abhörsicherheit
- Integrationsmöglichkeit für Subnetze beliebiger Technologie.

Realisiert wird die Primärverkabelung durch Lichtwellenleiter. Die max. Kabellänge beträgt 2000 m.

Für die Sekundärverkabelung werden in der Regel Multimode-Lichtwellenleiter verwendet. In der Gebäudegestaltung ist anzustreben, dass sich der Gebäudeverteiler in einem Etagenverteilraum befindet und dass alle anderen Etagenverteilerräume übereinander angeordnet sind. In sehr großen Gebäuden kann es ausgehend vom GV mehrere Steigleitungen geben. Durch die vertikale Verkabelung ergeben sich strenge Vorschriften für den Brandschutz (◘ Abb. 14.35).

Die Tertiärverkabelung (◘ Abb. 14.36) wird meist mit Cu-TP-Kabel realisiert. Dabei erfolgen feste Verlegungen (permanent link) jeweils zwischen einer Buchse in einem sog. Patchfeld (PP) im Etagenverteilerraum und einer Anschlussdose in einem Arbeitsraum. Die aktiven Komponenten, z. B. Arbeitsstationen, Switches usw., werden an die Buchsen angeschlossen mittels flexibler Anschlusskabel mit zwei Steckerenden.



◘ **Abb. 14.35** Sekundärverkabelung

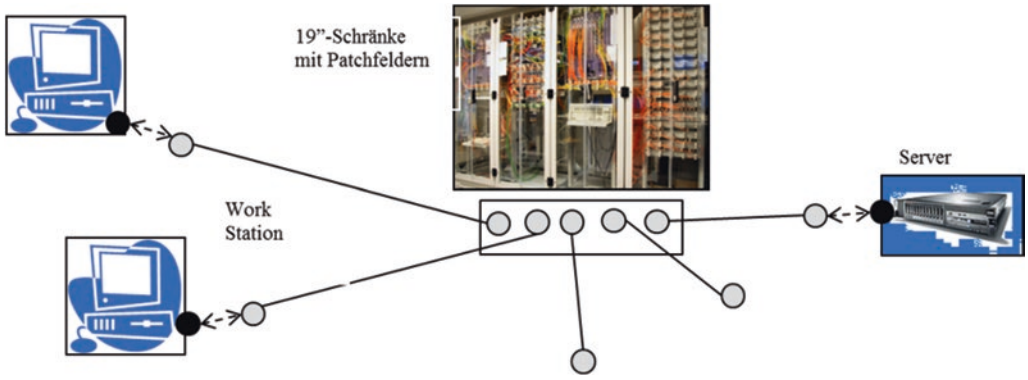


Abb. 14.36 Tertiärverkabelung

Seit 2002 erlaubt EN 50173 auch die Nutzung von Sammelpunkten CP (Consolidation Points) zwischen dem Patchfeld im Etagenverteilerraum und den Anschlussdosen TO (Abb. 14.37). Zwischen dem EV und dem CP liegt dabei eine Festverkabelung von mindestens 15 m Länge, zwischen dem CP und den TO ein hochwertiges flexibles Kabel (Consolidation Cable). Ein CP hat max. 12 Anschlüsse und muss zugänglich sein, z. B. in Zwischendecken oder Unterflursystemen. Vorteil der Sammelpunkt-Topologie ist eine größere Flexibilität der Gestaltung von Arbeitsplätzen in Großraumbüros.

Die Normen zur strukturierten Verkabelung verlangen, dass auf der Strecke zwischen zwei aktiven Geräten (Channel), die Anzahl der Steckübergänge auf maximal vier beschränkt wird, wobei die Steckverbindungen an den Geräten nicht mitgezählt werden. Dabei gibt es Längenrestriktionen für die einzelnen Abschnitte. Vereinfacht gelten als Maximallänge 100 m für den Channel und 90 m für den Permanent Link. Im Detail gehen in die Längenbeschränkungen weitere Angaben ein, wie Länge der einzelnen Abschnitte, Kabeltyp und Betriebstemperatur.

Die nachfolgende Abbildung (s. Abb. 14.38) zeigt ein Beispiel für 4 Steckübergänge (Interconnect-CP-TO-Modell).

Ein Switch ist über ein Kabel ohne Steckübergang fest mit einer Buchse in einem speziellen Patchfeld CC (Cross Connect Panel) verbunden. Ein Arbeitsplatzrechner besitzt eine Steckverbindung zur Netzwerkanschlussdose. Ein Konsolidationskabel ist an der Dose TO fest angeschlossen und hat einen zweiten Steckübergang am Konsolidationspunkt. Zwischen diesem und der zugehörigen Buchse im Patchfeld PP gibt es eine feste Verbindung. Zwischen den beiden Patchfeldern erfolgt eine Verbindung über ein Patchkabel mit zwei Steckübergängen.

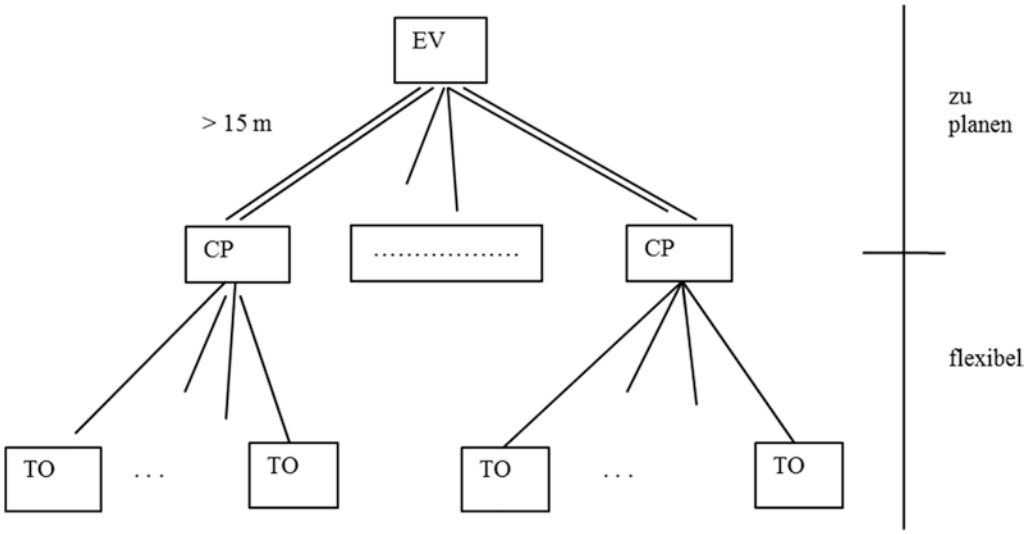


Abb. 14.37 EN 50173: Konsolidationspunkte

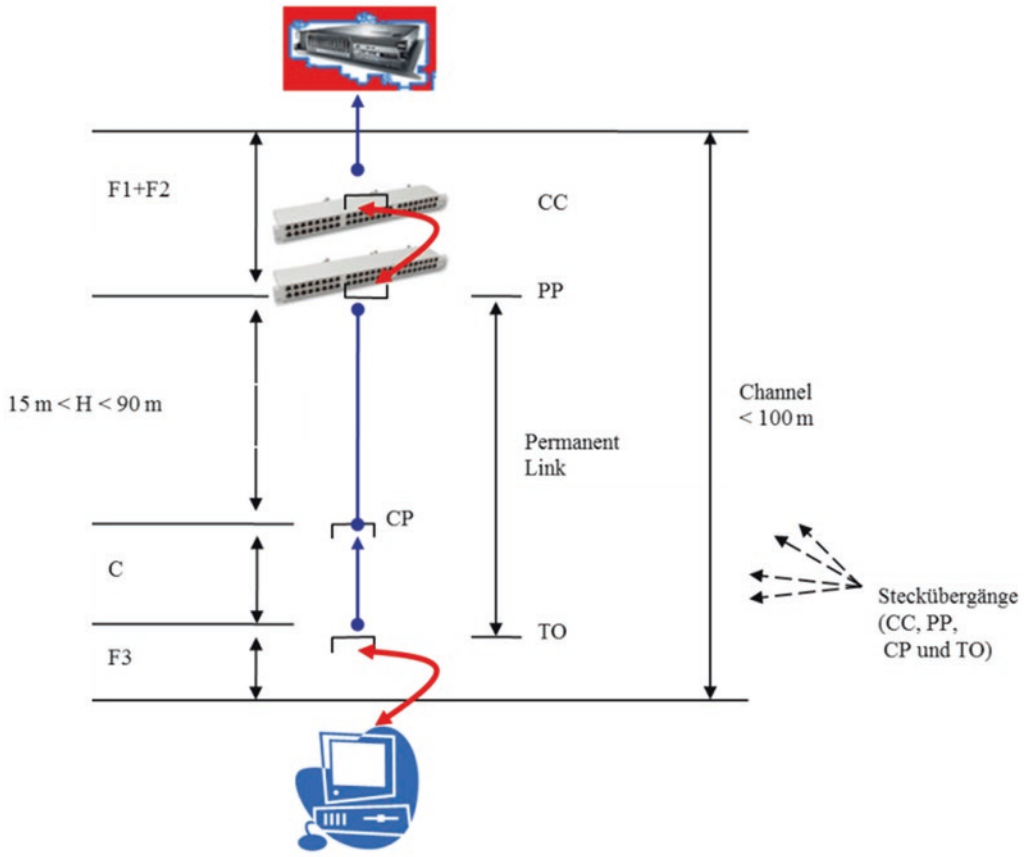


Abb. 14.38 Interconnect-CP-TO-Modell: Beispiel für 4 Stecküber

Neben Vorschriften zur Topologie beinhalten die Normen zur strukturierten Verkabelung auch Angaben zur Qualitätssicherung. In der EN 50173 sind die allgemeinen Anforderungen an Netzwerkinstallationen formuliert, in der EN 50174 werden unterschiedliche Stufen von Qualitätsplänen behandelt und die EN 50346 legt Messverfahren fest.

Es werden mehrere Stufen der Qualitätssicherung unterschieden. Der Aufwand zur Sicherung der Qualität und die damit verbundenen Kosten unterscheiden sich in den einzelnen Stufen erheblich.

Eine Referenzierung dient der Kalibrierung von Messgeräten und erfordert Untersuchungen im Labor. Dabei kann ein Kalibrierungszertifikat nach ISO 9000 erstellt werden.

Die Verifizierung ist die minimale Qualitätssicherung und besteht im Überprüfen der Verdrahtung, der Zuordnung von Anschlüssen und der Durchführung eines Durchgangstests.

Die Qualifizierung bzw. Validierung beinhaltet zusätzlich den Funktionsnachweis und die Überprüfung der in den Normen geforderten Bandbreite.

Unter Zertifizierung versteht man die Überprüfung der Konformität mit vorgegebenen Standards, z. B. Grenzwerteinhaltungen nach ISO/IEC 11801 und EN 50173 und die Erstellung einer detaillierten Dokumentation. Die Zertifizierung bietet eine Standardgarantie und vermeidet evtl. Gewährleistungsansprüche.

Die nachfolgende Tabelle (s. ◘ Tab. 14.3) enthält die wesentlichen Kontrollparameter, die typischerweise in einem Zertifikat enthalten sind.

14.6 Aktuelle Netzwerkklassen bzw. -kategorien

In den Normen EN 50173 ff. gibt es konkrete Vorgaben zu Kabelarten, Verdrahtung, Dämpfungsrestriktionen usw.

Zunächst sollen die Vorschriften zur Glasfaserverkabelung diskutiert werden. Die Lichtwellenleiter werden in verschiedene Kategorien unterteilt.

Multimodefasern sind preiswert, insbesondere bei Nutzung von LED-Strahlern. Allerdings schränkt die Modendispersion die erzielbaren Datenraten bei hohen Entfernungen ein. Je nach Qualität werden Multimodefasern in die Kategorien OM1 … OM3e eingeteilt. OM1-Fasern dürfen eine max. Dämpfung besitzen von 3,5 dB/km bei einer Wellenlänge von 850 nm und 1,5 dB/km bei 1300 nm und eine min. Bandbreitenlängenprodukt von 200 MHz * km bzw. 500 MHz * km. Die anderen Faserkategorien bis OM3e sind etwas hochwertiger.

Tab. 14.3 Kontrollparameter Zertifizierung bei nach ISO/IEC 11801 und EN 50173 [5]

Wert	Inhalt
Wiremap	Kontrolle der korrekten Verdrahtung
Impedance	Leitungswellenwiderstand des Kabels
Attenuation	Dämpfung
Length	Länge der Übertragungsstrecke
DC-Resistance	Ohmscher Widerstand
NEXT	(near end crosstalk) Nahübersprechen
FEXT	(far end crosstalk) Fernübersprechen
ACR-F (ELFEXT)	(equal level far end crosstalk) Verhältnis des übersprechenden Ausgangspegels zum eigentlichen Ausgangspegel
ACR	(Attenuation To Crosstalk Ratio) Dämpfung-Übersprech-Verhältnis
Powersum NEXT	Leistungssumme des Nahübersprechens
Powersum ELFEXT	Leistungssumme der elektromagnetische Koppelung am entfernten Kabelende
Powersum ACR	Leistungssumme des Dämpfung-Übersprech-Verhältnisses
Return Loss	Rückflussdämpfung
NVP	(nominal velocity of propagation) verzögerte Signallaufzeit gegenüber der Lichtgeschwindigkeit im Vakuum
Propagation Delay	Signallaufzeit
Delay Skew	Signallaufzeitunterschied auf verschiedenen Aderpaaren

Singlemodefasern besitzen die Kategorie OS1. Sie sind kostenintensiver, erlauben aber größere Datenraten und Kabellängen. Sie dürfen eine max. Dämpfung von 1,0 dB/km besitzen. Eine Modendispersion ist nicht vorhanden. Deshalb ist die Angabe eines min. Bandbreitenlängenproduktes nicht sinnvoll.

Im Weiteren werden die Vorschriften zur Kupferverkabelung diskutiert. Grundsätzlich werden TP-Kabel gefordert, die preiswert sind und sich leicht montieren lassen. Konkret sind die Kabel gekennzeichnet durch Kabelgeometrie, -material, den Durchmesser, die Zahl der Adernpaare, die Schlaglänge (Verdrillungen pro Länge), das Isolationsmaterial, die Schirmung, den zulässigen Temperaturbereich, das Gewicht usw. Der wichtigste Parameter ist die Angabe der Kabeldämpfung K für verschiedene Frequenzbereiche, angegeben in dB/100 m.

Wegen der Vielzahl der Kabelparameter wurden Qualitätsklassen in den Normen EN50173 ff. eingeführt, die durch eine Buchstabenangabe bezeichnet werden. Entsprechend gibt es Zahlenangaben für Qualitätskategorien bei EIA/TIA 568.

Es steht jedem Netzwerkbetreiber frei, welche Qualitätsklasse er installiert. Installationen mit niedriger Klasse sind preiswerter,

jedoch evtl. nicht zukunftssicher. Deshalb ist eine sorgfältige Abwägung der Netzwerkanforderungen für einen Zeithorizont von 15 Jahren sinnvoll.

Für die Gebäudeverkabelung werden TP-Kabel mit 4 farbig gekennzeichneten verdrillten Adernpaaren eingesetzt (Grün/Weiß-Grün, Blau/Weiß-Blau, Orange/Weiß-Orange, Braun/Weiß-Braun). Die verwendeten Buchsen und Stecker sowie die Pin-Belegung sind standardisiert. Meist wird das RJ-45-System nach EIA/TIA 568 verwendet (◘ Abb. 14.39).

Die auf den ersten Blick eigenartige Pin-Zuordnung erklärt sich durch Rücksichtnahme auf andere Standards, z. B. den Telefonstandard ISDN.

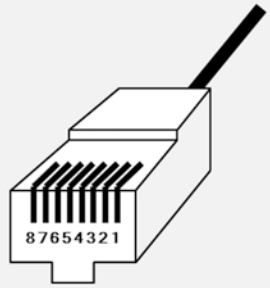
In einem Gebäude muss eine einheitliche Kodierung bei der Festinstallation verwendet werden. Bei flexiblen Kabeln gibt es normalerweise beidseitig gleich kodierte Kabel, aber für Sonderfälle auch unterschiedlich kodierte Cross-Over-Kabel. Diese können zur Verbindung zweier Computer ohne Switch verwendet werden.

Für die Kabel gibt es unterschiedliche Ausführungen. Alle Kabel sind 8-adrig und besitzen Cu-Adern mit ca. 1 mm Durchmesser. Sie sind paarweise verdrillt, besitzen aber eine unterschiedliche Schirmung.

UTP-Kabel (Unshielded Twisted Pair) bzw. U/UTP-Kabel haben Adernpaare ohne Schirmung und sind bis 100 MHz einsetzbar. Sie bieten optimale Verlegungseigenschaften, weil sie dünn und flexibel sind.

FTP-Kabel (Foiled Twisted Pair) bzw. U/FTP-Kabel besitzen Adernpaare in Metallfolie und sind bis 625 MHz geeignet.

S/UTP-Kabel (Screened unshielded TP) haben ungeschirmte Adernpaare plus eine Gesamtschirmung. Sie werden auch als F/UTP-Kabel (Folienschirmung) bzw. SF/UTP-Kabel (Schirmung durch Geflecht plus Folie) bezeichnet.

EIA/TIA 568 A			EIA/TIA 568 B	
1	Weiß-Grün		1	Weiß-Orange
2	Grün		2	Orange
3	Weiß-Orange		3	Weiß-Grün
4	Blau		4	Blau
5	Weiß-Blau		5	Weiß-Blau
6	Orange		6	Grün
7	Weiß-Braun		7	Weiß-Braun
8	Braun		8	Braun

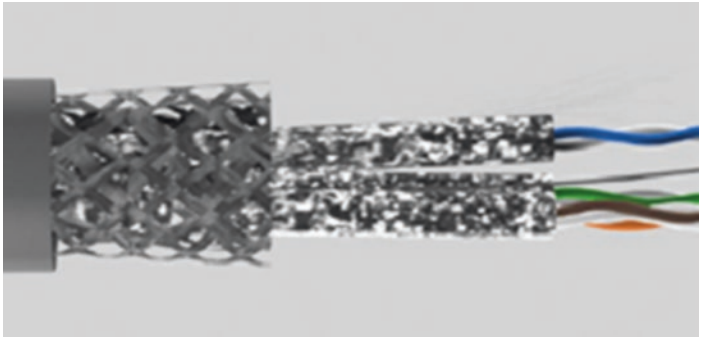
◘ **Abb. 14.39** RJ-45-Steckersystem

S/FTP-Kabel (Screened foiled TP) besitzen geschirmte Adernpaare plus eine Gesamtschirmung. Sie werden auch als F/FTP-Kabel (Folienschirmung) bzw. SF/FTP-Kabel (Schirmung durch Geflecht plus Folie) bezeichnet (◘ Abb. 14.40).

Die nachfolgende Tabelle (s. ◘ Tab. 14.4) enthält die Dämpfungsangaben für die unterschiedlichen Qualitätsklassen. Gegenwärtig vorherrschend sind Installationen der Klasse D bzw. Kategorie 5, die für Fast Ethernet und Gigabit-Ethernet geeignet sind. Zukünftige Installationen sollten mindestens mit Klasse E_A erfolgen, weil sonst kein Betrieb von 10-Gigabit-Ethernet möglich ist.

Normalerweise erfolgt die Stromversorgung für Endgeräte getrennt vom Rechnernetzwerk über das 220 V-Stromversorgungsnetz.

Zur strukturierten Verkabelung gehört auch die Planung der Stromversorgung über das Datennetzwerk. Die zugehörigen



◘ **Abb. 14.40** S/FTP-Kabel

◘ **Tab. 14.4** Dämpfungsgrenzwerte der Qualitätsklassen nach EN 50173 und EIA/TIA 568 [5]

Klasse EN 50173	Kategorie EIA/TIA 568	Anwendung	Datenrate	Grenzfrequenz (MHz)	Zulässige Dämpfung bei Grenzfrequenz
	3	Telefon/LAN	10 MBit/s	16	13,1 dB/100 m
C			20 MBit/s	16	14,4 dB/100 m
D		FastEthernet	100 MBit/s	100	24 dB/100 m
	5		100 MBit/s	100	22 dB/100 m
	6		1 GBit/s	200	23 dB/100 m
E		GbE	1 GBit/s	250	35,9 dB/100 m
E_A	(6_A)	10 GbE	10 GBit/s	500	49,3 dB/100 m
F			>10 GBit/s	600	54,6 dB/100 m
	7		>10 GBit/s	600	50 dB/100 m
F_A	(7_A)			1000	67,6 dB/100 m

Standards wurden im Standard IEEE 802.3af (Power over Ethernet) festgelegt. Dabei wird zwischen Stromquellen PSE (Power Sourcing Equipment) und Stromverbrauchern PD (Powered Device) unterschieden. Pro Kabel darf eine Leistung von max. 15 W bei einer Spannung von 44 … 57 V (typischerweise 48 V) zugeführt werden. Die Standardleistung reicht für VoIP-Telefone, aber nicht für Computer. Eine Erhöhung auf 30 W ist in Diskussion (IEEE 802.3at). Die Wärmeentwicklung pro Kabel ist unkritisch, bei Kabelbündeln muss aber eine Wärmebilanz berechnet werden. Es sind verschiedene Leistungsklassen vorgesehen (s. nachfolgende ◘ Tab. 14.5).

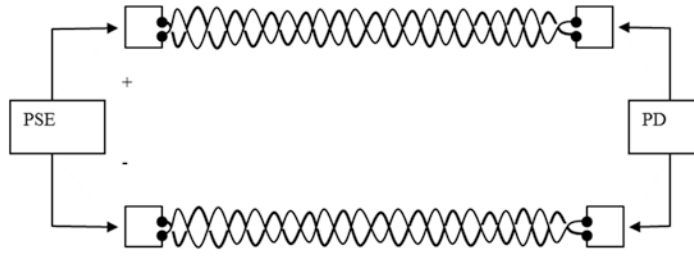
Es existieren zwei Varianten, die Phantomeinspeisung (über Datenübertragungspaare) und die Spare-Pair-Einspeisung (über ungenutzte Paare). Eine PSE kann das Verfahren wählen. Es muss aber im Netzwerk einheitlich sein. Die PD müssen alle Verfahren beherrschen, beim Anschließen erfolgt eine Erkennungsprozedur zwischen PSE und PD.

Bei der Spare-Pair-Einspeisung setzt die PSE die Adernpaare 4/5 und 7/8 auf unterschiedliche Potentiale. Die PD können dann die Spannungsdifferenz nutzen (◘ Abb. 14.41).

Die Spare-Pair-Einspeisung bereitet Probleme, da sie inkompatibel zu ISDN ist und ungeeignet für Netzwerke ist, in denen alle Adernpaare genutzt werden, z. B. Gbit-Ethernet.

◘ Tab. 14.5 PoE-Leistungsklassen nach IEEE 802.3af [5]

Leistungsklassen				
Klasse	**Typ**	**Max. Strom (mA)**	**Max. Leistung (PSE) (W)**	**Max. Leistung (PD) (W)**
0	Default	0–5	15,4	0,44–12,95
1	Optional	8–13	4,0	0,44–3,84
2	Optional	16–21	7,0	3,84–6,49
3	Optional	25–31	15,4	6,49–12,95
4	Reserviert	35–45	15,4	Reserviert



◘ Abb. 14.41 Power over Ethernet IEEE 802.3af: Spare-Pair-Einspeisung

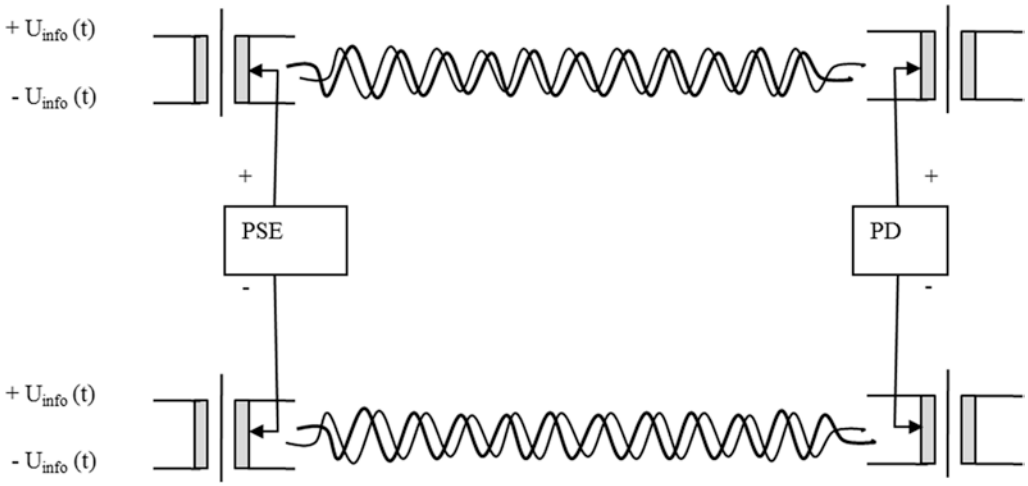


Abb. 14.42 Power over Ethernet IEEE 802.3af: Phantomeinspeisung

Bei der Phantomeinspeisung werden durch die PSE die Adernpaare 1/2 und 3/6 auf unterschiedliche Potentiale gesetzt. Es gibt zwei Verfahren MDI und MDI-X der Phantomeinspeisung, die sich durch die Polung unterscheiden. Die Stromverbraucher PD können dann die Spannungsdifferenz nutzen (Abb. 14.42).

14.7 Methodik der Qualitätsmessung und Zertifizierung, Fehlerdiagnostik

Installationsfehler lassen sich in höheren Protokollschichten eines Netzwerkes nicht mehr korrigieren.

Deshalb bestimmt die Kabelinstallation wesentlich die Qualität eines Netzwerkes mit.

Im Folgenden sollen typische Fehlerquellen in TP-Kabelinstallationen und die Methoden der Qualitätssicherung diskutiert werden [5].

Häufige Fehler sind **Fehlverdrahtungen** an Buchsen bzw. Steckern. Durch Sichtkontrollen können grobe Fehler erkannt werden, z. B. beschädigte Kabel, lose Drähte, angebrochene Stecker usw. Eine nachfolgende Durchgangsmessung zeigt an, ob die Pins 1–1 bis 8–8 elektrisch richtig verbunden sind (Zuordnung s. Abb. 4.39) und dass keine Kurzschlüsse vorliegen. Bei positivem Testergebnis kann trotzdem eine Kreuzung eines Adernpaares vorliegen. Dies ist z. B. der Fall, wenn auf beiden Seiten die grüne Ader auf Pin 4 und die blaue auf Pin 2 angeschlossen wurde. Die Durchgangsprüfung ist dann zwar positiv, aber das Hochfrequenzverhalten ist gestört. Nach

Standard müssen Pin 1 und 2 sowie Pin 4 und 5 jeweils mit einem Adernpaar verbunden sein, beim o. g. Installationsfehler ist dies aber nicht der Fall. Der Sinn der Verdrillung ist unterlaufen, die Folge ist stark erhöhtes Nebensprechen. Adernkreuzungen sind nur durch Hochfrequenzmessungen nachweisbar.

Sinnvoll ist auch eine Messung des **Gleichstromwiderstandes** aller Adern. Eine Überschreitung von Grenzwerten ist problematisch, niedrige Werte ermöglichen eine Fernstromversorgung.

Auch die **Kabelkapazität** sollte gemessen werden. Eine Grenzwertüberschreitung deutet auf Druckstellen oder Feuchtigkeit im Kabel hin. Außerdem dient der Messwert der Berechnung der Kabelimpedanz.

Die **Laufzeit** T_L der Signale im Kabel ist ebenfalls eine wichtige Messgröße. Diese hängt ab von der Länge des Kabels l_{kabel} und dem Verkürzungsfaktor **NVP (Nominal Velocity of Propagation),** der das Verhältnis der Ausbreitungsgeschwindigkeit im Kabel zur Lichtgeschwindigkeit c_{vakuum} angibt:

$$T_L = \frac{l_{\text{kabel}}}{c_{\text{kabel}}} = \frac{l_{\text{kabel}}}{\text{NVP} \cdot c_{\text{vakuum}}} \tag{14.1}$$

Der NVP-Wert liegt in der Regel um 0,6 und hängt ab vom Kabelmaterial und der Verdrillungsschlaglänge. In der Praxis wird die o. g. Formel meist umgekehrt benutzt, um aus der Laufzeitmessung die Kabellänge zu berechnen. Die Kabellänge ist wichtig für den Installateur, weil sie in seine Finanzabrechnung eingeht. Der Wert für NVP ist relativ ungenau, damit auch die errechnete Kabellänge. Die Fehler gleichen sich aber bei vielen Kabeln statistisch aus.

Aus technologischen Gründen schwankt der NVP-Wert über die Kabellänge. Deshalb gibt es Laufzeitdifferenzen zwischen den einzelnen Adernpaaren eines Kabels. Gekennzeichnet werden sie durch die Angabe eines DelaySkew-Wertes (Differenz zwischen Maximal- und Minimalwert):

$$\text{DelaySkew} = T_{L-\max} - T_{L-\min} \tag{14.2}$$

Dieser Wert ist wichtig für Technologien mit zeitparallelem Senden über mehrere Adern, z. B. bei 10- Gigabit-Ethernet. Bei dieser Technologie gibt es bidirektionale Übertragung mit 250 MBit/s über alle vier Adernpaare. Ein Delay Skew von 4 ns bedeutet bereits eine Zeitverschiebung um 1 Bitzeit!

Gemessen wird die Signallaufzeit durch Ausnutzung der Signalreflektion am offenen Kabelende (◘ Abb. 14.43). Es werden kurze Impulse von ca. 20 ns gesendet und die Zeitdifferenz bis zum Eintreffen des reflektierten Impulses gemessen. Die Laufzeit ergibt sich dann durch Halbierung.

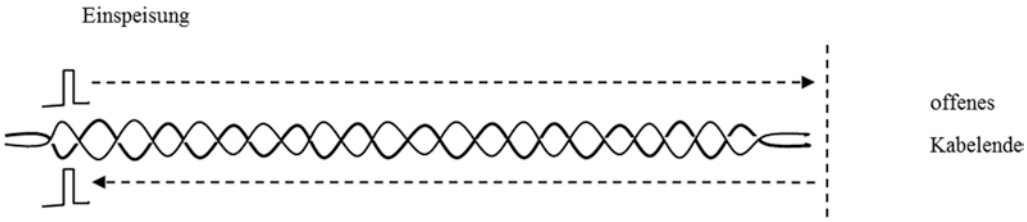


Abb. 14.43 Laufzeitmessung durch Ausnutzung der Signalreflexion am Kabelende

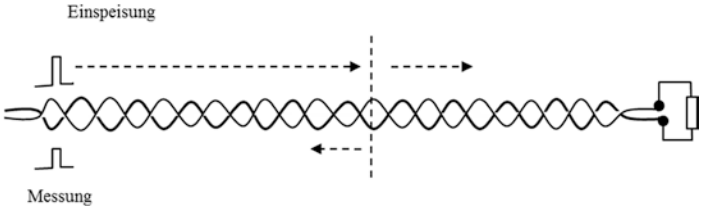


Abb. 14.44 Ermittlung von Störstellen durch Signalreflexion

Der Wellenwiderstand (Impedanz) eines Kabels Z_o bestimmt die Größe der Kabelabschlusswiderstände und wird aus Messungen der Laufzeit und der Kabelkapazität berechnet:

$$Z_0 = \frac{T_L}{C} \tag{14.3}$$

An Störstellen der Übertragungsstrecke können Signalreflexionen erfolgen, deren Ursache z. B. Kabelmontagefehler sein können. Die Prüfung erfolgt am abgeschlossenen Kabel. Beim Messvorgang werden kurze Impulse gesendet. Über die Messung der Laufzeit kann der Reflexionsort ermittelt werden (Abb. 14.44).

Dabei wird auch die Intensität des reflektierten Signales gemessen und die Kabelrückflussdämpfung A_r berechnet (Maßeinheit [dB]). Sie darf vorgeschrieben Grenzwerte nicht überschreiten:

$$A_r = 10 \cdot \log\left(\frac{\text{Sendeleistung}}{\text{reflektierte Leistung}}\right) \tag{14.4}$$

Sehr wichtig für die Qualitätseinschätzung sind die Messungen zum Hochfrequenzverhalten. Dabei ist eine hohe Anzahl von Messungen durchzuführen (48 pro Kabel).

Der wichtigste Wert ist die Kabeldämpfung A_i **(Insertion Loss),** die abhängig ist von der Kabellänge, der Frequenz, aber auch von Installationsfehlern (Biegungen, Quetschungen), der Temperatur und der Luftfeuchtigkeit. Gemessen und berechnet wird die Kabeldämpfung durch Einspeisen eines Impulses und dem Vergleich der Sende- und der Empfangsleistung. Die

Abb. 14.45 Messung der Kabeldämpfung (Insertion Loss)

Kabeldämpfung ist durch Verstärkung korrigierbar. Grenzwerte müssen unbedingt eingehalten werden (Abb. 14.45).

Die meisten HF-Messungen betreffen das Nebensprechen (Crosstalk), d. h. die gegenseitige Hochfrequenzbeeinflussung der Adern bzw. Kabel. Die Maßeinheit des Nebensprechens ist dB.

$$A_i = 10 \cdot \log \left(\frac{\text{Sendeleistung} - \text{fern}}{\text{Empfangsleistung} - \text{nah}} \right) \tag{14.5}$$

Beim Nahübersprechen *NEXT (Near End Crosstalk)* induzieren Signalströme im Paar A Störströme im Nachbar-Paar B. NEXT ist prinzipiell korrigierbar durch Gegensteuern im Adernpaar B. Die Messungen erfolgen am Kabelanfang. Auf ein Adernpaar wird ein Impuls gegeben und im Partnerpaar wird die empfangene Leistung gemessen. Der NEXT-Wert kann sich an den beiden Enden unterscheiden, deshalb sind zwei Messungen erforderlich (Abb. 14.46).

NEXT drückt den Vergleich von Sende- und Störleistung aus. Die Werte sind relativ längenunabhängig, aber stark frequenzabhängig und beeinflussbar durch die Kabelqualität. Hauptursachen für schlechte NEXT-Werte sind Montagefehler und zu geringe Qualität der Netzwerkkomponenten.

$$\text{NEXT} = 10 \cdot \log \left(\frac{\text{Sendeleistung} - \text{nah} - \text{A}}{\text{Störleistung} - \text{nah} - \text{B}} \right) \tag{14.6}$$

Nebensprechen erfolgt über die gesamte Länge eines Kabels. **FEXT (Far End Crosstalk)** beschreibt das Übersprechen am fernen Ende des Kabels.

$$\text{FEXT} = 10 \cdot \log \left(\frac{\text{Sendeleistung} - \text{fern} - \text{A}}{\text{Störleistung} - \text{nah} - \text{B}} \right) \tag{14.7}$$

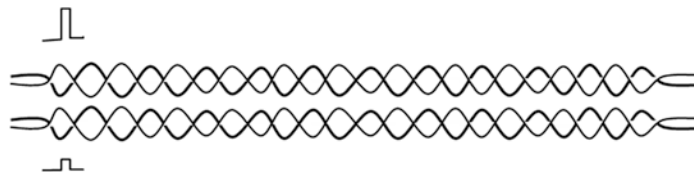


Abb. 14.46 Messungen von NEXT-Werten

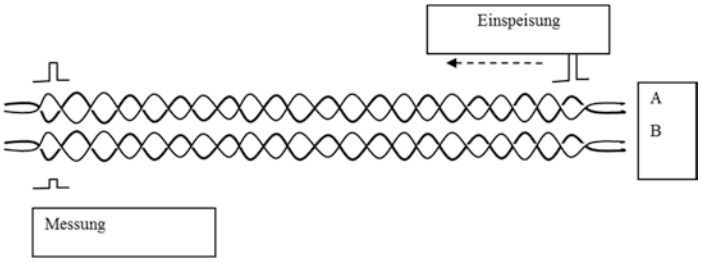


Abb. 14.47 Messungen von FEXT-Werten

Der FEXT-Wert ist längenabhängig und schwer messbar, da Einspeisung und Messung örtlich getrennt sind. Eine FEXT-Korrektur ist normalerweise nicht möglich (Abb. 14.47).

PSNEXT (Power Sum NEXT) stellt den Einfluss des Nebensprechens von allen anderen Paaren im Kabel dar. Die Größe ist bedeutsam für Kabel mit Parallel-Übertragung über mehrere Adernpaare.

Weitere Nebensprechgrößen sind: (14.8)

ACR (Attenuation Crosstalk Ratio)
- Verhältnis des Nebensprechens NEXT zur Dämpfung A
- ACR [dB] = NEXT [dB] – Dämpfung [dB]

ACR-F bzw. ELFEXT (Equal Level Far-end Cross Talk)
- Verhältnis des Nebensprechens FEXT zur Dämpfung A
- relativ längenunabhängig
- ACR-F [dB] = EXT [dB] – Dämpfung [dB]

PSACR und PSACR-F
- PSACR = PSNEXT minus Dämpfung des eigenen Paares
- PSACR-F = Summe ACR-F der anderen Paare

EMI (Eletromagnetic Interference) beschreibt die Störungen durch Emission fremder Geräte (Aliens).

So gibt es für die Größe des Übersprechens in Kabelbündeln zwischen Nachbarkabeln das **ANEXT (Alien NEXT)** und andere Alien-Werte **(PS ANEXT, PS AACR-F, …).**

Alien Nebensprechen stellt ein Problem dar bei Frequenzen über 500 MHz in UTP-Installationen. Auswege sind die Erhöhung der Kabelabstände, die Vergrößerung der Abstände zwischen Buchsen in Netzwerkdosen und Patchfeldern.

Kein Problem gibt es bei Verwendung von geschirmten S/FTP-Kabeln (Dämpfung des Alien AXTALK um 100 dB). Eine

Gütegarantie „per Design" ist bei Installation auf Niveau der Klasse F gegeben.

Nachfolgende ◘ Tab. 14.6 zeigt die Grenzwerte (Limits) einer Übertragungsstrecke der Klasse E (250 MHz) nach dem Standard EN 50173:2001.

Im Weiteren betrachten wir ein einfaches Beispiel bzgl. der aktuellen Planungsmethodik drahtgebundener Netzwerke.

Beispiel 14.1

Vernetzung in einem Studentenwohnheim

Für ein Studentenwohnheim mit 3 Geschossen (je 10 Zimmer) mit Anschluss an das Campusnetz und an das Internet sollte eine Netzkonzeption erarbeitet werden.

Dabei erfolgte eine konsequente Orientierung an den gültigen Standards zur strukturierten Verkabelung, d. h. der Normenfamilie nach EN/DIN 50173 (EU bzw. Bundesrepublik Deutschland) bzw. EIA/TIA 568 (USA, Nordamerika). Durch diesen modernen Ansatz wurde die Trennung aktiver und passiver Komponenten ermöglicht.

Am o.g. Studentenwohnheim werden die folgenden Maßnahmen vorgenommen:

- Zunächst wurden die baulichen Gegebenheiten des Gebäudes analysiert. Je Etage gab es einen kleinen Service-Raum von 10 m^2 Fläche. Alle drei Räume waren übereinander angeordnet und durch einen brandsicheren Kabelschacht verbunden. Diese Zimmer wurden als Verteilerräume umgewidmet.

◘ **Tab. 14.6** Grenzwerte einer Übertragungsstrecke der Klasse E nach EN 50173:2001 [5]

Messwerte Loss [dB] Delay [ns]	**Frequenz/MHz**								
	1	**4**	**10**	**16**	**20**	**31,25**	**100**	**200**	**250**
Insertion Loss	4,0	4,2	6,5	8,3	9,3	11,7	21,7	31,7	35,9
Delay	555								
Delay Skew	50,0	50,0	50,0	50,0	50,0	50,0	50,0	50,0	44,0
NEXT	65,0	63,0	56,6	53,2	51,6	48,4	39,9	34,8	33,1
PSNEXT	62,0	60,5	54,0	50,6	49,0	45,7	37,1	31,9	30,2
Return Loss	19,0	19,0	19,0	18,0	17,5	16,5	12,0	9,0	8,0
ACR-F	63,2	51,2	43,2	39,2	37,2	33,3	23,3	17,2	15,3
PSACR-F	60,3	48,3	40,3	36,2	34,3	30,4	20,3	14,2	12,3
ACR	62,8	58,9	50,0	44,9	42,3	36,7	18,2	3,0	−2,8
PSACR	58,0	56,3	47,5	42,3	39,7	34,0	15,4	0,2	−5,7

- Die Primärverkabelung war im Projekt nicht erforderlich. Die Sekundärverkabelung bestand im vertikalen Verlegen von drei Klasse-E-TP-Kabeln durch den Kabelschacht und die Tertiärverkabelung im horizontalen Verlegen von 10 TP-Kabeln zu den Studentenzimmern.
- Jeder Verteilerraum erhielt einen 19″-Schrank mit Platz für 12 Höheneinheiten HE (je 1,75 Zoll bzw. 4,45 cm).
- Für die Kabelinfrastruktur wurde ein Klasse-E-Patchfeld (1 HE, 24 Buchsen) eingebaut. Anschließend erfolgte das Anklemmen (Patchen) der Kabel an Patchfeld-Buchsen bzw. Anschlussdosen in den Studentenzimmern.
- Ergänzend soll die Realisierung der aktiven Komponenten beschrieben werden. Diese sind flexibel austauschbar.
- In jedem Schrank wurde eine unabhängige Stromversorgung USV (2 HE) mit einer Leistung von 2,2 KW und eine abschaltbare Steckdosenleiste (1 HE, 8 Steckdosen) eingebaut.
- Alle Schränke erhielten einen Gigabit-Ethernet-Switch (1 HE) mit 24 Ports und der Schrank im Erdgeschoss zusätzlich einen VDSL-Router (1 HE). Der Router realisiert die Internetanbindung (50 Mbit/s Datenrate) und die Verbindung zum LAN über einen integrierten schnellen 5-Port-Switch.
- Die restlichen Höheneinheiten in den 19″-Schränken dienen als Reserve für Servereinschübe (2 bis 4 HE, ca. 800 W Leistung).

Abb. 14.48 präsentiert die Belegung des 19″-Schrank im Erdgeschoss, die Verbindungen zwischen den Komponenten über flexible Patchkabel und die abgehenden fest verlegten Kabel.

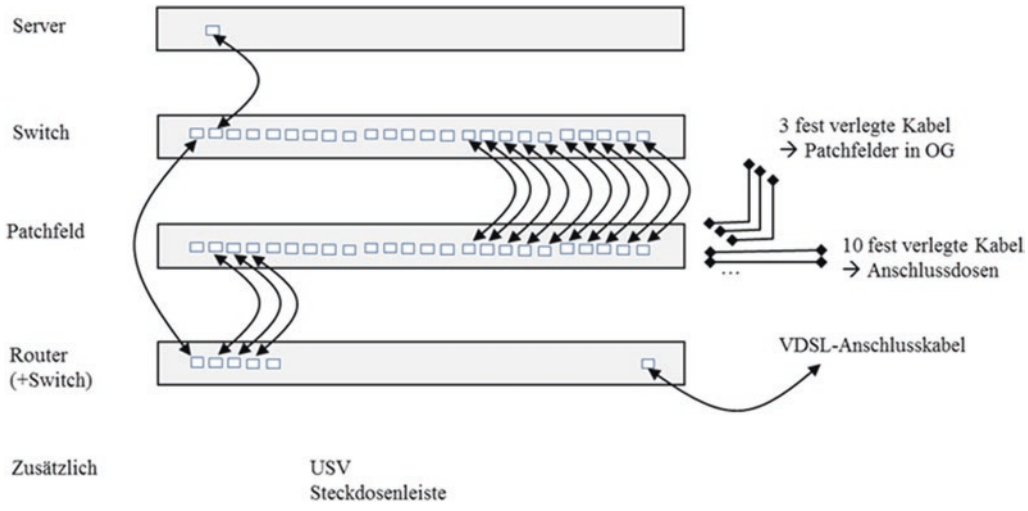


Abb. 14.48 Einschübe/Verkabelung: 19″-Schrank im Erdgeschoss-Verteilerraum

14.8 Zwischenfragen/Übungsaufgaben

14.8.1 Geräte zur Netzkopplung

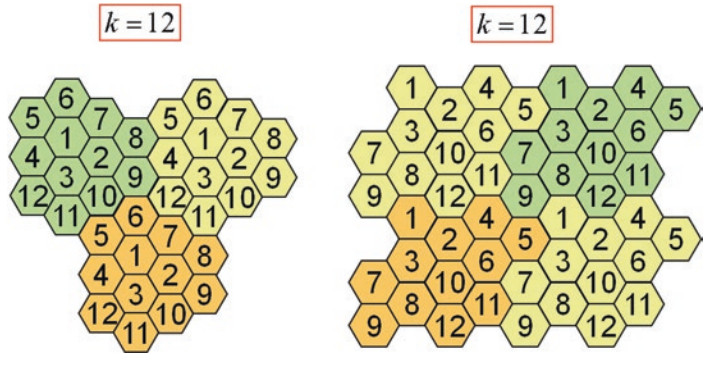
a. Welcher Schicht sind folgende Kopplungsgeräte zuzuordnen (Repeater, Bridge, Router, Cut-Through-Switch, Store-and-forward-Switch, IP-Switch, WLAN-AP, Application Gateway, Firewall)?
In welchen Fällen erfolgt eine Lasttrennung?
b. Können Ethernet-LANs unterschiedlicher Datenrate gekoppelt werden?
Stellen Sie die Ergebnisse in tabellarischer Form dar.

14.8.2 Switched Ethernet

a. Im angegebenen Szenario unterstützt jede Leitung (Port) die DRport = 100 MBit/s duplex. Die Durchschaltung von Verbindungen erfolgt innerhalb der Latenz Δt ($\Delta t = 80$ ms), die mittlere Framelänge beträgt FL = 1000 Byte. Berechnen Sie die Gesamtdatenrate DR [in Mbit/s] des Switches in dem unten aufgeführten Szenario (◘ Abb. 14.49):

14.8.3 Strukturierte Verkabelung

a. Vergleichen Sie die Eigenschaften von Lichtwellenleitern und TP-Kabeln.
b. Welche der nachfolgenden Größen ist längenabhängig
- NEXT
- FEXT
- ELFEXT



◘ **Abb. 14.49** Switch-Szenario

c. Wann tritt Alien NEXT auf und wie kann es verringert werden?
d. Welche Höchstdämpfung bei 100 MHz darf ein Netzwerk nach Klasse E erfüllen?
e. Berechnen Sie die Signallaufzeit für ein TP-Kabel mit 50 m Länge und einem NVP-Wert von 0,66.
f. In welchen Grenzen schwankt die Signallaufzeit, wenn herstellerbedingt der NVP-Wert um 10 % schwankt.
g. Welche Empfangsleistung ergibt sich bei einer Übertragungstrecke (50 m) mit einer Dämpfung von 18 dB/100 m bei einer Sendeleistung von 10 mW?

Ausblick Teil II

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_15

In diesem Teil wurden Ihnen weitere Details zur Nutzung von aktuellen Netzwerkmustern (Ethernet-Familie, MPLS, WLAN, 3G, 4G, 5G, Satellitenfunk, Pikonetze), zu den Konzepten zur strukturierten Verkabelung sowie der effizienter Vernetzung vermittelt.

Besonderer Wert wird dabei auf eine gute Strukturierung organisatorischer Bereiche in Netzwerken, Datensicherheit und sinnvollen Einsatz von aktiven Kopplungselementen gelegt. Dies ermöglicht die Wiederverwendbarkeit der Netzwerkfragmente und deren besseres Management.

Wir schätzen ein, dass Sie aufgrund dieser Kenntnisse die vereinfachten Aufgaben zur Planung von kostengünstigen, energiesparenden und effizienten Netzwerken selbständig lösen können.

Im Teil III erhalten Sie weitere Hinweise zu spezielleren Themen und werden dadurch befähigt, auch komplexere Arbeiten durchzuführen.

Da alle drei Teile eine Einheit bilden, verzichten wir in den ersten beiden Teilen auf ein Glossar und verweisen auf ein zusammenfassendes Glossar im Teil III.

Lösungen zu Zwischenfragen/Übungsaufgaben Teil II

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_16

Zu ► Abschn. 12.7

► Abschn. 12.7.1 Ethernet

a) Weshalb darf die Framelänge bei CDMA/CD-Ethernet einen bestimmten Wert nicht unterschreiten? Wie groß ist dieser bei IEEE 802.3?

Schlagen Sie je eine kostengünstige Ethernetversion vor für nachfolgende Anforderungen und nennen Sie die für diese Version vorgeschriebenen Medien:

- Datenrate mindestens 1 GBit/s, Streckenlängen mindestens 500 m
- Datenrate mindestens 10 GBit/s, Streckenlängen nur 10 m
- Datenrate mindestens 30 GBit/s, Streckenlänge mindestens 5 km

Zu ► Abschn. 12.7.1a)

Sender und(!) Empfänger sollen eine evtl. Kollision erkennen können!

Extremfall	2 Sender an den Enden des Übertragungsmediums (Länge l)
	Sender 1 sendet zum Zeitpunkt t
	Startsignal benötigt Zeitdauer tl bis zum Ort von Sender 2
	Sender 2 stellt mittels CS (Carrier Sense) bis zum Zeitpunkt (t + tl) fest: „Medium frei“.
	Gemäß CSMA könnte er noch senden.
	In diesem Zeitraum ist eine Kollision möglich,
	danach nicht mehr, und CS liefert: „Medium besetzt“

Sender 2 stellt immer zuerst fest, dass eine Kollision vorliegt, Sender 1 aber nur, wenn er mindestens die doppelte Signallaufzeit sendet (→ Framemindestgröße).

Sendezeit:	T = F/DR	Framegröße/Datenrate
Laufzeit:	tl = l/v	Länge/Ausbreitungsgeschwindigkeit

Mit Tmin = 2 * tl ergibt sich:

$$F > 2 * l * DR/v$$

Mit den Werten l = 2,5 km, v = 200.000 km/s und DR = 10 MBit/s ergibt sich:

$$F > 250 \text{ Bit}$$

IEEE 802.3	Festlegung auf 512 Bit, bzw. 64 Byte (ohne Präambel) Daraus ergibt sich ein Zeitslot von 51,2 µs bei 10 Mbit/s

Zu ► Abschn. 12.7.1b)
Mehrere Lösungen sind möglich durch Auswertung der ◘ Tab. 12.2 bis 12.6,
z. B.

– 1000Base-SX	monomode LWL
– 1000Base-CX	spezielles STP- bzw. Koax-Kabel
– 40GBase-LR4	monomode LWL

► Abschn. 12.7.2 WLAN

a) Welche grundlegenden Unterschiede und Gemeinsamkeiten bestehen zwischen leitungsgebundenen und drahtlosen LANs? Betrachten Sie dabei Betriebsarten, Management, Frequenzen, Fähigkeiten der Endgeräte, Dienstgüten, nationale/internationale Regulierung!
b) Vergleichen Sie Infrastrukturnetzwerke und Ad-hoc-Netzwerke hinsichtlich Planungsaufwand, Robustheit, Komplexität der Endgeräte, Übertragungsraten und Routing!
c) Vergleichen Sie die Eigenschaften der elektromagnetischen Wellen in den für WLAN IEEE 802.11a/b/g/n/ac/ad verwendeten Frequenzbereichen!
d) Welche Lösungsmöglichkeiten bestehen für die Abdeckung größerer geographischer Gebiete bzw. Gebäude mit WLAN?
e) Erläutern Sie die MIMO-Technik am Beispiel von neuen WLAN-Standards.

Zu ► Abschn. 12.7.2a)
Die Lösung lässt sich tabellarisch darstellen (◘ Tab. 16.1):

Zu ► Abschn. 12.7.2b)
Die Lösung lässt sich tabellarisch darstellen (◘ Tab. 16.2):

Zu ► Abschn. 12.7.2c)

–	2,4 GHz	ca. 10 cm Wellenlänge	→ Hindernisse >10 cm wirken abschattend
		Freies Frequenzband beschränkt	→ wenige Kanäle (3 überlappungsfrei)
		Dämpfung akzeptabel	→ in Gebäuden bis ca. 30 m
–	5 GHz	mehr verfügbare Bandbreite	→ Kanalbündelung möglich
		aber Konkurrenz zu Primärnutzern (Radar usw.)	
		stärkere Dämpfung	→ Reichweite reduziert
–	60 GHz	großzügige Bandbreite	→ sehr hohe Datenraten erzielbar
		sehr starke Dämpfung	→ massive Reichweitenprobleme

Tab. 16.1 Wichtige Eigenschaften leitungsgebundener und drahtloser Netze

Merkmal	Leitungsgebundene LANs	Drahtlose LANs
Betriebsart	Nur Infrastrukturmodus	Infrastruktur- und Ad-hoc Betrieb möglich
Management	Planung, aufwendige Kabelverlegung	Keine Kabelverlegung, im Ad-hoc Modus auch keine Planung
Frequenzen	Kupferkabel: 100 bis 1000 MHz, LWL: ca. 500 THz	Funk: 2,4 GHz, 5 GHz, mittelfristig: 60 GHz
Fähigkeiten der Endgeräte	Keine Mobilität Gerätegröße nach unten beschränkt durch notwendige Kabelverbindung	Mobilität wird i. a. unterstützt Kleinste Gerätegrößen möglich (Smartphones, Smartwatches usw.)
Dienstgüte	Datenrate bei drahtgebundenen LANs um Größenordnungen höher (bis 100 Gigabit/s).	Übertragungsfehlerrate bei drahtlosen LANs ebenfalls um Größenordnungen höher (10^{-8} statt 10^{-14})
Nationale/ Internationale Regulierung	Keine Regulierung notwendig, Standardisierte Technologie erhöht jedoch Interoperabilität	Nationale/internationale Regulierung aufgrund der bereits vollständig belegten Funkfrequenzen notwendig, Lizensierung i. d. R. langwieriger Prozess, deshalb Nutzung des lizenzfreien ISM-Bands (Industrial, Scientific and Medical), damit Einschränkung des Frequenzbereichs und der Sendeleistung

Tab. 16.2 Vergleich der Eigenschaften von Infrastruktur-WLAN und ad-Hoc-WLAN

	Infrastruktur	Ad hoc
Planungsaufwand	Planung erforderlich	keine Planung erforderlich
Robustheit	Geringer, da Kabel und Verbindungseinheiten zerstört werden können	Höher, da keine Kabel und Verbindungseinheiten
Komplexität der Endgeräte	Geringer, da komplexe Funktionalität von Verbindungseinheiten ausgeführt wird (z. B. Medienzugriff, Prioritätsmechanismen für Dienstgütegarantien)	Höher, da Geräte eigenständig die Funktionalitäten des Medienzugriffs, der Prioritäts-mechanismen für Dienstgütegarantien und der Vermittlung übernehmen müssen
Übertragungsraten	Höher	Geringer
Routing	Durch Infrastruktur (Zugangspunkte, Vermittlungsstellen)	Durch Endgeräte selbst, verschiedene Routingverfahren

Zu ► Abschn. 12.7.2d)
Einteilung in Versorgungsbereiche (Zellen) mit unterschiedlichen Frequenzen. Da es nur wenige Kanalfrequenzen zur Auswahl gibt (Interferenzgefahr → Rauschen), muss eine geschickte Planung erfolgen (Ausnutzen von Wänden mit hoher Dämpfung zur Zellabtrennung usw.).

Übergabe zwischen Zellen mittels Roaming (IEEE 802.11f. bzw. 802.11r) erhöht den Komfort für die Nutzung.

Durch WLAN ungenutzte Bereich müssen über kabelgebundene LAN überbrückt werden.

Zu ► Abschn. 12.7.2e)
◘ Abb. 12.13 illustriert den Einsatz der MIMO-Technik am Beispiel des WLAN-Standards IEEE 802.11n.

MIMO wird auch in anderen WLAN-Funktechnologien eingesetzt, z. B. bei IEEE 802.11ac und IEEE 802.11ad sowie auch bei der Mobilfunktechnologie LTE.

Zu ► Abschn. 13.5
► Abschn. 13.5.1 Zellulare Mobilfunknetze

a) Durch so genanntes Clustering werden geographische Bereiche in zellularen Funknetzen in Funkzellen mit unterschiedlichen Frequenzbändern strukturiert. Bezeichnet D den Abstand zweier Basisstationen mit derselben Sendefrequenz, R den Zellradius und k die Clustergröße, gilt folgender Zusammenhang:

$$D = R \cdot \sqrt{3k}$$

Wie sieht ein Cluster aus, das für Zellen gleicher Frequenzen einen Abstand $D = 6 \cdot R$ ermöglicht?

b) Was sind die Hauptunterschiede von GSM und UMTS und wie werden die höheren Datenraten erzielt? Was ist HSDPA und LTE?

Zu ► Abschn. 13.5.1a)
Es gelten - $D = 6 \cdot R$ und $D = 6 \cdot \sqrt{3k}$
Damit - $\sqrt{3k} = 6$
Ergebnis - k = 12

Es sind also mindestens 12 Frequenzen erforderlich.

Es gibt jedoch mehrere Realisierungsmöglichkeiten bei der Frequenzplanung. ◘ Abb. 16.1 zeigt zwei Varianten. In der links dargestellten Variante hat beispielsweise eine Zelle mit der Frequenz 1 keine Nachbarzelle mit der Frequenz 8, in der rechten Variante dagegen immer.

Eine weitere Schwierigkeit bei der Frequenzplanung besteht darin, dass komplexe Geländereliefs (mit Hindernissen) unterschiedlich große Zellen erfordern. Evtl. können auch extrem unterschiedliche Nutzerdichten (Anzahl der Nutzer pro Zelle) ebenfalls unterschiedlich große Zellen erforderlich machen.

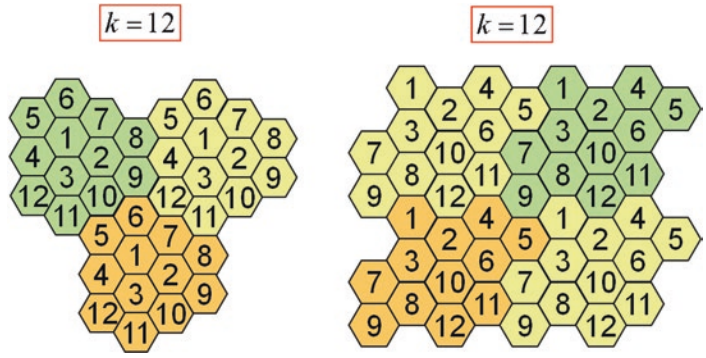


Abb. 16.1 Varianten zum Clusteraufbau bei k = 12

Zu ► Abschn. 13.5.1b)
Die Lösung der Aufgabe finden Sie in ► Abschn. 13.2.

Praktisch jedes Jahrzehnt erhöht sich die Datenrate des Mobilfunks um den Faktor 10 (s. Abb. 13.5). Generell gilt, dass es von den Generationen 2G bis 4G einen Übergang von der leitungsvermittelten zur paketvermittelten Kommunikation gibt. Weiterhin werden immer effizientere Kodierungsverfahren eingesetzt (Frequenz- und Zeitmultiplex → zusätzlich Code-Multiplex → zusätzlich OFDM).

Einen Vergleich der wichtigsten Technologien (Generationen) gibt Tab. 13.4.

Die neuesten Generationen des Mobilfunks haben hierarchische Zellstrukturen und sind mit weiteren drahtlosen Funknetzen sowie SAT-Funk interoperabel (Abb. 2.3).

Ab der 4G (LTE) ist neben Sprach- und Datenübertragung auch die komfortable Nutzung von Videotelefonie und die Nutzung sozialer Netzwerke möglich.

► Abschn. 13.5.2 In Richtung 5G
Die 5. Generation des Mobilfunks bezeichnet die nächste wichtige Phase der aktuellen Entwicklung von Mobilfunkstandards.

a) Welche Unterschiede bietet 5G hinsichtlich der Vorgänger 3G/4G!
b) Beschreiben Sie kurz die wichtigsten Netzwerktechnologien, die 5G-Einsatz künftig unterstützen sollen.
c) Analysieren Sie das Szenario in Abb. 13.18! Erklären Sie die Rollen jeweiliger Komponenten der Architektur.

Zu ► Abschn. 13.5.2a)
Die 5G (in Entwicklung) soll nochmals alle Übertragungsparameter wesentlich verbessern. Die wichtigsten Detailziele (Verbesserung um mehr als eine Größenordnung) sind in Abb. 13.13 dargestellt:

- Durchsatzerhöhung
- Laufzeitreduktion
- Vielfältige Sensoren
- Ausfallsicherheit
- Sicherheitsmaßnahmen
- Effizient Interoperabilität usw.

Die Erfüllung dieser Ziele soll die Voraussetzungen für neue Dienste (Telepräsenz, Internet of Things, Virtuelle Realität, Tactil Internet) schaffen.

Zu ► Abschn. 13.5.2b)
In ◘ Abb. 13.11 werden diese Technologien aufgezeigt.

Zu ► Abschn. 13.5.2c)
In ◘ Abb. 13.18 ist das Zusammenwirken verschiedenster Techniken dargestellt:

Interoperabilität der Netze 2G (GPRS, EDGE); 3G(UMTS, HSPA); 4G(LTE); WLAN usw.

Der Netzwerkkern wird per 5G SDN realisiert.

Zugangsgeräte aller Art sind zugelassen (Smartphones, Laptops, …). Cloudbasierte Applikationen und mobile Apps bestimmen die Nutzung.

Bereitgestellt werden diverse Dienste, wie z. B. hochwertige Telepräsenz, „Internet der Dinge“ und „intelligente Fertigung“.

► Abschn. 13.5.3 Satellitenfunk und Ortungssysteme

a) Geben Sie einige Beispiele von satelliten-basierten Kommunikationssystemen an! Welche Dienste realisieren diese?
b) Klassifizieren Sie die satelliten-basierte Systeme nach Orbithöhe (GEO, MEO, LEO). Vergleichen Sie diese bzgl. der DR, Sendeleistung, Distanz, Lebensdauer, Signalverzögerung!
c) Ein Satellit hat eine Entfernung zur Erde h = 20.200 km. Berechnen Sie die Periode T(r)! Zu welcher Klasse (Einsatzbereich) würden Sie diesen einordnen?
d) Vergleichen Sie die satelliten-basierte Ortungssysteme wie GPS, GALILEO usw.!

Zu ► Abschn. 13.5.3a)
Beispiele von satelliten-basierten Kommunikationssystemen entnehmen Sie ◘ Tab. 13.1.

Diese präsentiert die wichtigsten Kennwerte von Kommunikationssatelliten: SAT-Klassen, Dienste und Anwendungsbereiche, Frequenzbänder, Orbithöhen, Umlaufperioden, typische Datenraten.

Generell gilt:
Die satellitenbasierten Kommunikationssysteme bieten Dienste für Telefonie und Datentransfer an. Gegenüber terrestrischen Systemen haben sie eine höhere Latenz, was u. U. zu Problemen bei Echtzeitkommunikation führen kann.

Vorteilhaft ist, dass die Nutzer satellitenbasierter Kommunikationssysteme keine komplexe Infrastruktur am Boden benötigen. Deshalb sind sie gut geeignet für unzugängliche und auch für schwach besiedelte Gebiete.

Zu ► Abschn. 13.5.3b)
Im ► Abschn. 13.1 wurden verschiedene Satellitenklassen, die sog. GEO-, MEO-, LEO- und HEO-Satelliten (s. ◘ Abb. 3.2) vorgestellt. Als Legende zur Abbildung gilt: LEO – Low Earth Orbit; MEO – Medium Earth Orbit; HEO – Highly-Elliptical Orbit; GEO – Geostationary Earth Orbit.

Zur Lösung der Aufgabe werten Sie ◘ Tab. 13.2 aus.

Schwerpunkte:
- GEO-Satelliten sind langlebig, benötigen aber hohe Sendeleistungen und besitzen große Latenzen. Daher sind sie mehr für TV, Seeüberwachung, Air Traffic Control sowie Navigationsdienste geeignet.
  Außerdem ist in naher Zukunft zu erwarten, dass der Platz im Orbit für geostationäre Bahnen knapp wird.
- LEOs sind wegen ihrer geringen Latenz besser für die Telefonie geeignet, aber sie benötigen häufigen Handover und mehr Satellitentransponder pro Dienst usw.

Zu ► Abschn. 13.5.3c)

Geg.:	$R = 6370$ km	Erdradius
	$g = 9{,}81$ m/s^2	Erdbeschleunigung
	$h = 20.200$ km	
Ges.:	$T(r)$.	
Es gilt:	$r = h + R = 26.570$ km	Abstand zum Erdmittelpunkt
Weiterhin	$r^3 = g\,R^2\,T^2/(2\pi)^2$	Formel (13.9)

$$
\begin{aligned}
T(r) &= \mathrm{sqrt}[(r^{3*}(2\pi)^2)/g^*R^2] \\
&= \mathrm{sqrt}\left[\left(18{,}8 * 10^{12} * 39{,}5\right)/\left(9{,}81 * 40{,}6 * 10^6\right)\right]\ \mathrm{s} \\
&= \mathrm{sqrt}\left[1{,}864 * 10^9\right]\ \mathrm{s} \\
&= 43.174\ \mathrm{s} \\
&\text{ca. } 12\ \mathrm{h}
\end{aligned}
$$

16

Dieses Ortungssatellitensystem gehört konventionell zur Klasse MEO.

Die ergänzte Lösungstabelle sieht folgendermaßen aus (◘ Tab. 16.3):

Zu ► Abschn. 13.5.3d)
Die wichtigsten SAT-Ortungssysteme sind:

- GPS — globales USA-System zur Positionsbestimmung, seit Mitte der 90er voll in Betrieb, ursprünglich militärische Nutzung, zivile Nutzung (ca. 10 m Genauigkeit)
- GALILEO — globales EU-System, zivile Nutzung, seit 2016 nutzbar, vollständiger Ausbau bis 2018
- GLONASS — globales System aus der RF (ehemals UdSSR), Vollausbau 1996, danach Probleme, zivile Betriebsbereitschaft ab 2011
- Beidou — globales System (VR China), zivile Nutzung, seit 2004 für den asiatischen Bereich in Betrieb, weltweit verfügbares Netz befindet sich im Aufbau

Zu ► Abschn. 14.8

► Abschn. 14.8.1 Geräte zur Netzkopplung

a) Welcher Schicht sind folgende Kopplungsgeräte zuzuordnen (Repeater, Bridge, Router, Cut-Through-Switch, Store-and-forward-Switch, IP-Switch, WLAN-AP, Application Gateway, Firewall)?
In welchen Fällen erfolgt eine Lasttrennung?
Können Ethernet-LANs unterschiedlicher Datenrate gekoppelt werden?

◘ **Tab. 16.3** Zusammenhang Satellitenhöhe und Umlaufperiode

Typ	Satellitenhöhe h	Umlaufperiode T
GEO (Geo-stationary Earth Orbit Satellite)	Ca. 36.000 km (exakt 35.786 km)	24 h
MEO (Middle Earth Orbit Satellite)	7000 km	257 min = 4 h 17 min
LEO (Low Earth Orbit Satellite)	700 km	99 min
GPS (Global Positioning System, US NAVSTAR-Satellite)	**20.200 km**	**12 h**
ISS (International Space Station)	Ca. 400 km (exakt 371 km)	92 min

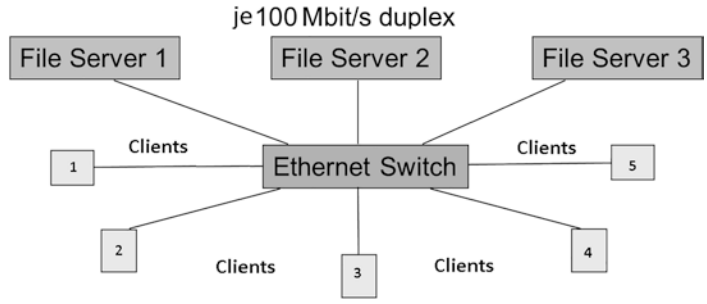


Abb. 16.2 Szenario Switched Ethernet

Stellen Sie die Ergebnisse in tabellarischer Form dar.

► Abschn. 14.8.2 Switched Ethernet

a) Im angegebenen Szenario (s. Abb. 16.2) unterstützt jede Leitung (Port) die DRport = 100 MBit/s duplex. Die Durchschaltung von Verbindungen erfolgt innerhalb der Latenz Δt ($\Delta t = 80$ Mikrosekunden), die mittlere Framelänge beträgt FL = 1000 Byte. Berechnen Sie die Gesamtnettodatenrate DR [in Mbit/s] des Switches in dem unten aufgeführten Szenario:

Zu ► Abschn. 14.8.1a + b)
s. Tab. 16.4.

Tab. 16.4 Einordnung von Geräten zur Netzkopplung

Gerät	OSI-Schicht	Lasttrennung	Kopplung unterschiedlicher Datenraten
Repeater	1 – Physical Layer	Nein	Nein
Bridge	2 – Data Link Layer	Ja	Ja
Router	3 – Network Layer	Ja	Ja
Cut-Through-Switch	2 – Data Link Layer	Ja	Nein
Store-and-forward-Switch	2 – Data Link Layer	Ja	Ja
IP-Switch	3 – Network Layer	Ja	Meist ja
WLAN-AP	2 – Data Link Layer	Ja	Meist nein
Application Gateway	7 – Application Layer	Ja	Ja
Firewall	Meist 4 – Transport Layer	Ja	Ja

Zu ► Abschn. 14.8.2a)
Die Auswertung von ◘ Abb. 16.2 ergibt für die Durchlaufzeit eines Frames durch den Switch:

$$\begin{aligned} T &= (FL/DRport) + \Delta t \\ &= (8 * 1000\ \text{Bit}/10^8\ \text{Bit/s}) + 80\ \mu s \\ &= 160\ \mu s \end{aligned}$$

Die Nettodatenrate ergibt sich dann zu:

$$\begin{aligned} \text{DRport-Netto}_{max} &= FL/T \\ &= 8 * 1000\ \text{Bit}/160 * 10^{-6}\ s \\ &= 50 * 10^6\ \text{Bit/s} = 50\ \text{Mbit/s} \end{aligned}$$

Insgesamt liegen 8 Duplexleitungen am Switch an. Dadurch ergibt sich eine maximale Bruttodatenrate von:

$$\text{DR-brutto}_{max} = 2 * 8 * \text{DRport-Netto}_{max} = 800\ \text{Mbit/s}$$

► Abschn. 14.8.3 Strukturierte Verkabelung

a) Vergleichen Sie die Eigenschaften von Lichtwellenleitern und TP-Kabeln.
b) Welche der nachfolgenden Größen ist längenabhängig
   - NEXT
   - FEXT
   - ELFEXT
c) Wann tritt Alien NEXT auf und wie kann es verringert werden?
d) Welche Höchstdämpfung bei 100 MHz darf ein Netzwerk nach Klasse E erfüllen?
e) Berechnen Sie die Signallaufzeit für ein TP-Kabel mit 50 m Länge und einem NVP-Wert von 0,66.
f) In welchen Grenzen schwankt die Signallaufzeit, wenn herstellerbedingt der NVP-Wert um 10 % schwankt.
g) Welche Empfangsleistung ergibt sich bei einer Übertragungstrecke (50 m) mit einer Dämpfung von 18 dB/100 m bei einer Sendeleistung von 10 mW?

Zu ► Abschn. 14.8.3a)

TP-Kabel - preiswert: Kabel, Anschlussdosen, Montagearbeit
Günstige Verlegung, robust, kleine Biegeradien, …
kurze Strecken – Bandbreite im GHz-Breich, geeignet bis 10 Gb Ethernet

LWL - hohe Kosten für Kabel, Anschlussdosen, Montagearbeit
Verlegung aufwendig, Biegeradien, Zugbelastung, …
sehr geringe Dämpfung
geeignet für höchste Übertragungsraten

Zu ► Abschn. 14.8.3b)
NEXT - längenunabhängig

FEXT - abhängig

ELFEXT - (relativ) unabhängig

Zu ► Abschn. 14.8.3c)

Alien NEXT - Übersprechen zwischen Nachbarkabeln

- Problem bei hohen Frequenzen bei UTP
- Abstände erhöhen
- Bessere Schirmung (S/FTP bringt 100 dB!!!)
- Installation Klasse F

Zu ► Abschn. 14.8.3d)
◘ Tab. 14.6 auswerten
Dämpfung max. 21,7 dB/100 m

Zu ► Abschn. 14.8.3e)

$$\text{TL} = \text{Länge-Kabel}/(\text{NVP} * \text{Lichtgeschwindigkeit})$$

$$\begin{aligned}\text{TL} &= 50\ \text{m}/(0{,}66 * 300.000\ \text{km/s}) \\ &= 50\ \text{m}/200.000\ \text{km/s} \\ &= 0{,}25\ \mu\text{s}\end{aligned}$$

Zu ► Abschn. 14.8.3f)
Annahme Fehler für Kabellänge vernachlässigbar, dann 10 % Fehler für Signallaufzeit

$$\text{TL} = 0{,}25\ \mu\text{s} \qquad \text{mit Genauigkeit 25 ns}$$

Zu ► Abschn. 14.8.3g)
Dämpfung = 10 lg (Sendeleistung/Empfangsleistung)

$$\begin{aligned}&18\ \text{dB/100 m} && \rightarrow\ 9\ \text{dB auf 50 m} \\ &9\ \text{dB} = 10\ \lg(\text{PS/PE}) && \rightarrow\ \text{PS/PE} = 10^{0{,}9} = 7{,}94 \\ &\text{PE} = 1{,}26\ \text{mW}\end{aligned}$$

Verarbeitungs-orientierte Schichten und Netzwerk-anwendungen

„Es ist nicht genug zu wissen – man muss auch anwenden.
Es ist nicht genug zu wollen – man muss auch tun".
(Johann Wolfgang von Goethe, 1749–1832, Dichter, Philosoph und Staatsmann)

Inhalte und kurzfassende Hinweise

Im Teil wird auf den bereits bekannten Begriffen und erworbenen Kenntnissen der Teile I und II wie Topologie, Protokolle, Dienste, Rechnernetzmuster, Switching und Routing sowie Basisprinzipien der Datenübetragung in Netzwerken aufgebaut.

Die Aufteilung im Teil III ist wie folgt:

- Abschnitt „Verarbeitungsorientierte Schichten"
- Abschnitt „Netzwerkanwendungen und mobile Apps"
- Abschnitt „Verteilte Systeme und Cloud Computing"

Abschließend werden Beispiele zu fortgeschrittenen Anwendungen und Netzwerkdiensten besprochen. Dabei wird auch auf die Portierbarkeit, Verschlüsselung, Komprimierung von Anwendungen in heterogenen Umgebungen, Betriebssystemen und Netzwerken eingegangen.

Inhaltsverzeichnis

Lernziele Teil III

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_17

17.1 Voraussetzungen Teil III

Das Teil III setzt voraus, dass Sie die Inhalte der Teile I und II beherrschen. Die Studierenden sind mit dem Aufbau und den Funktionen der relevanten Referenzmodelle (Internet, TCP/IP, OSI) vertraut und besitzen einen qualifizierten Überblick über aktuelle Protokolle lokaler Netzwerke sowie von Weitverkehrsnetzen, Zugangsnetzwerken, drahtlosen und Mobilfunknetzen.

Sie kennen die grundlegenden Eigenschaften der unterschiedlichen Netzkonzepte und können anhand gestellter Anforderungen eine geeignete Technologieauswahl vornehmen.

Die Kenntnisse der Teile I und II ermöglichen den Übergang zu den oberen Schichten des OSI-Referenzmodells, zu den verarbeitungsorientierten Schichten und zu den Netzwerkanwendungen. Des Weiteren werden die verteilten Systeme und die aktuellen Konzepte wie u. a. „IoS", „Cloud Computing" sowie „die hochverteilte Systeme" und „IoT" diskutiert.

17.2 Lernziele und vermitteltes Wissen

Teil III vermittelt Ihnen darüber hinaus Kenntnisse und Fertigkeiten, die benötigt werden, um in effizienter Weise von der Problemstellung zu den heutigen Rechnernetzanwendungen, mobilen Apps zu gelangen. Die klassischen Architekturen von Netzwerkservices und Verteilten Systemen erleben heutzutage signifikante Veränderungen, u. a. wie folgt:

- Ausbau von „Computing Power" und Vernetzung von Rechnern und Mobilfunkgeräte zu heterogenen Clustern und Grids
- Weitere Entwicklung des Internets der Dienste (IoS) bei weltweitem Cloud-Einsatz
- Ausbau des Internets der Dinge (IoT) bei der Unterstützung von Clouds und beim Übergang zum Fog Computing.

Im Teil III erwerben Sie Kenntnisse über die Techniken zu den fortgeschrittenen Rechnernetzanwendungen und mobilen Apps, von typischen Protokollen und Modellen der verarbeitungsorientierten OSI-Schichten (Layer 5–7) sowie zur Optimierung deren Performance und Effizienz.

Wir empfehlen Ihnen, unbedingt alle Zwischenfragen und Übungsaufgaben zunächst völlig selbständig zu lösen und erst danach die Lösungen im Anhang zur Überprüfung zu nutzen.

Den Abschluss des Teiles III bildet das zusammenfassende, gemeinsame Glossar zu den Teilen I, II und III.

WISSEN:
Sie beherrschen die wichtigsten Konzepte und Modelle zur Kommunikation in Netzwerken und kennen sich mit dem Aufbau von Netzwerkanwendungen aus. Sie können qualifiziert zu den aktuellen Konzepten, Weiterentwicklung der Netzwerkarchitekturen und Anwendungen Stellung nehmen.

Sie kennen die grundlegenden Eigenschaften der unterschiedlichen Netzkonzepte und können anhand gestellter Anforderungen eine geeignete Technologieauswahl vornehmen. Durch das Studium der Teile I–III sowie das Absolvieren des Begleitpraktikums besitzen sie erste praktische Erfahrungen im Aufbau von einfachen lokalen (drahtgebundenen und drahtlosen) Netzwerken sowie Pikonetzen.

Verarbeitungsorientierte Schichten

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_18

Im OSI-Referenzmodell werden die Schichten 5–7 als verarbeitungsorientierte Schichten bezeichnet (s. ◘ Abb. 18.1):

- Sitzungsschicht (L5)
- Darstellungsschicht (L6)
- Anwendungsschicht (L7).

Im Weiteren werden die folgenden Abkürzungen verwendet:
JVM – Java Virtual Machine
HW – Hardware
SW – Software
OS – Operating System
NW – Network
VM – Virtual Machine
VM – Virtual Machine Monitor
NAS – Network Attached Storage
SAN – Storage Area Network
VLAN – Virtual Local-area Network
VPN – Virtual Private Network (s. Glossar)

Implementierungstechnisch sind die Funktionalitäten der Schicht 5 jedoch meist in Mechanismen der Darstellungs- und Anwendungsschicht bzw. Internet-Dienste integriert [6, 16].

18.1 Verzahnung der Sitzungsschicht und Darstellungsschicht

Die Sitzungsschicht (Kommunikationssteuerung, L5) übernimmt die folgenden Aufgaben der Steuerung des Dialogs zwischen Benutzerprozessen, u. a.:

- Längerfristige Sitzungen über wechselnde Transportverbindungen (z. B. im Mobilumfeld)
- Interaktionsmodelle (z. B. die Modelle Client/Server, Peer-to-Peer in verteilten Systemen)
- Datensicherung (z. B. durch Einbau synchronisierter Sicherungspunkte zwecks Optimierung des Betriebsverhaltens, durch konsistente Durchführung von Transaktionen mit dem Commit-Verfahren).

Dabei werden die oben genannten Funktionalitäten in den Rechnernetzanwendungen schichtenübegreifend (L5-L6) einprogrammiert und untereinander stark und oft unerkennbar verzahnt!

Die Darstellungsschicht (L6) verrichtet die folgenden wichtigen Aufgaben:

- Konvertierung heterogener Datenformate
- Kompression multimedialer Daten
- Einsatz von Sicherheitsmechanismen und Abdeckung von Schutzzielen in den Netzwerkanwendungen.

18.1.1 Konvertierung und Anpassung von Formaten. Komprimierung und Codecs

Die Konvertierung heterogener Datenformate ist zwecks Heterogenitätsabbaus erforderlich.

Zum Beispiel in der Speicherstruktur für ein Frame bei der Videostreaming können die folgenden Probleme auftreten:

- Byteordnung und Bitordnung bei Client und Serveranwendung unklar
- interne Implementierung und Layout von Datentypen und Datenstrukturen (von Rechnerarchitektur stark abhängig, z. B. von der Wortbreite)

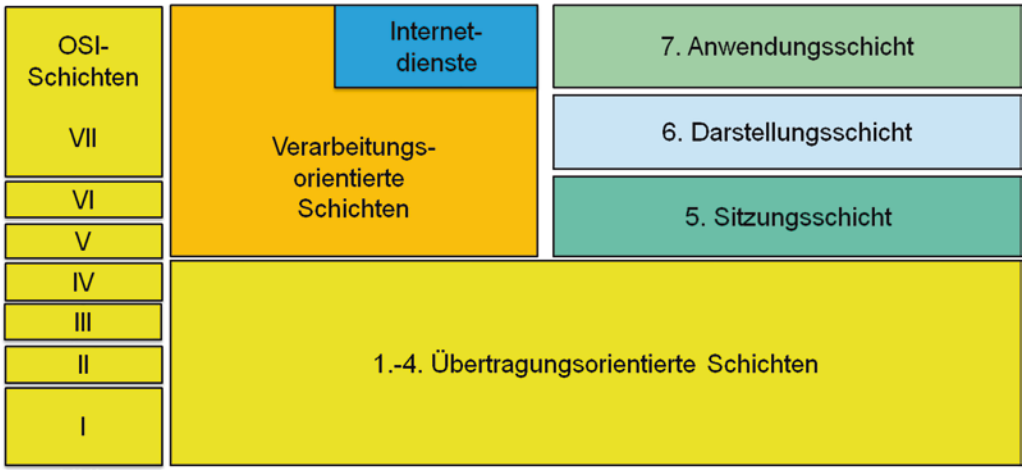


Abb. 18.1 Allgemeines zu den verarbeitungsorientierten Schichten

```
typedef struct {    // Speicherstruktur: Layout
unklar?
char *name;         //  String (evtl. Konvertierung
ASCII/EBCDIC)
int resolution;          // Byteordnung unklar?
char pixel [1024][1024]; // Bitordnung unklar?
} Image; // Speicherstruktur für ein  Frame  bei
der Videostreaming
```

Die übertragenen Daten müssen unter Umständen vor und/oder nach der Übertragung gewandelt werden, insbesondere bei der Übertragung von Binärdaten (Big-Endian- vs. Little-Endian-Darstellung ganzer Zahlen, Länge von int-Zahlen: 2, 4 oder 8 Byte, Layout von Datenstrukturen usw.). Um diese Probleme zu vermeiden, kommt eine einheitliche Transfersyntax zum Einsatz. Moderne Applikationen verwenden dazu eine XML-Notation oder portierbaren Java-Bytecode.

Als Transfersyntax bietet XML (eXtensible Markup Language) die folgenden wichtigen Funktionen:

- Abstrakte Beschreibung von Dokumenten und Datenstrukturen
- Vordefinierte Sammlung vielfältiger Basisdatentypen
- Abbildung auf Programmiersprachen mit XSL (eXtensible Stylesheet Language).

```
<!-- Datentyp (unabhängig von spezieller
Programmiersprache): -->
<element name="Bestellformular">
<complexType>
<element name="Kundenname" type="xsd:string"/>
<element name="Artikelnummer" type="xsd:int"/>
<element name="Betrag" type="xsd:amount"/>
</complexType>
</element>
<!-- Instanz dieses Datentyps: -->
<Bestellformular>
<Kundenname>Ralf Muster</Kundenname>
<Artikelnummer>17322</Artikelnummer>
<Betrag>99.95</Betrag>
</Bestellformular>
```

Eine einfache lösunung besteht in der Verwendung vorkompilierten Java-Bytecodes. Dieser ist übertragungs- und betriebssysystemunabhängig und wird nur über die hostspezifischen JVM (Java Virtual Machine) interpretativ ausgeführt.

Generell gilt: Die Konvertierung und die Vereinheitlichung der Transfersyntax (XML-Format, Java Bytecode, weitere Virtualisierungsverfahren wie bspw. die Server von Citrix, VMWare, …) reduzieren die Heterogenität der Datenformate und Komplexität der Transferroutinen zwecks Übertragungseffizienz (◘ Abb. 18.2):

Die Funktionalität der Darstellungsschicht wird oft per sog. Codecs implementiert. Als Codec (Kofferwort aus „Coder-Decoder“ im Englischen) bezeichnet man ein Verfahren, das multimediale Daten digital kodiert und dekodiert. Codecs ermöglichen direktes Umwandeln von einem Format in ein anderes (bspw. MPEG-2 zu MPEG-4) oder (BMP zu JPEG) oder (ASCII-Text zu PDF). Je nach Anwendungsart spricht man von Konvertierung bzw. Transcoding.

▪▪ Viele Codecs ermöglichen auch die zusätzliche Kompression von zu übertragenden Daten

Dies bringt Leistungsverbesserung und Gewinn in der Übertragungszeit. Die Kompressionsverfahren sind wesentlich für Multimedia- und für Mobilkommunikation (◘ Tab. 18.1).

Wir beschreiben nachfolgend einige typische Beispiele von Kompressionsverfahren (Codecs):

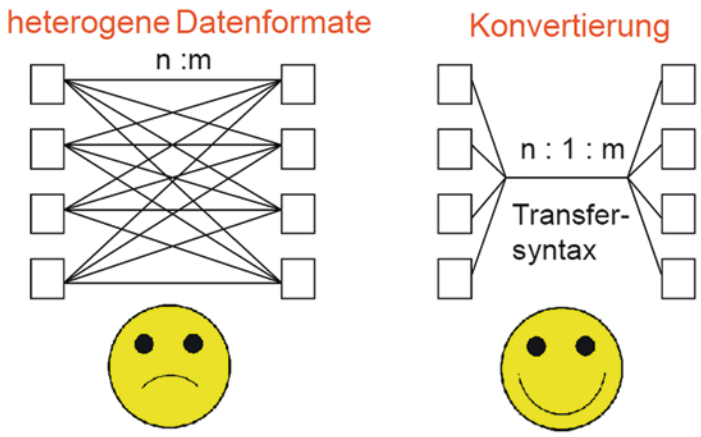


Abb. 18.2 Vereinheitlichung der Transfersyntax zwecks Übertragungseffizienz

Tab. 18.1 Kompressionsverharen in Rechnernetzen [16]

Medium	Größe unkomprimiert/ komprimiert, Byte	Kompressionsrate	Codecs	Kurze Beschreibung
1 Seite ASCII-Text oder Grafik	3…10 K/1…3 K	3:1	ZIP, RAR, 7z	Meist verlustfrei, Lauflängen- und Huffman-Kodierung
1 Seite Bitmap	0,5…8 M/10…160 K	50:1	JPEG, GIF, PNG	Verlustfrei sowie verlustbehaftet (hybride)
1 s Telefon oder 1 s Stereo	8/0,08 K	100:1	MP3 (MPEG-1 Layer 3), G.711	i. d. R. verlustbehaftet, Differentielles PCM oder Fast Fourier Transformation
1 s Video	30…300 M/0,1…1 M	300:1	MPEG-2, MPEG-4, H.264	Sehr effizient, daher verlustbehaftet, Fast Fourier oder Discrete Cos Transformation

a) **MPEG-2 (Weiterentwicklung des älteren MPEG-1-Standards):**
- Video- und Audiokodierung mit Kompression
- Sehr gute Videoqualität, Datenraten ca. bis ca. 50 Mbit/s
- Anwendung: DVDs und für digitales Fernsehen (DVB – Digital Video Broadcasting)

b) **H.264 (MPEG-4 Advanced Video Coding):**
   - Videokompression mit besonders hoher Kodiereffizienz
   - Optimierung durch Bildvorhersage (Prädiktion) und Bewegungskompensation
   - Anwendung bei Videokonferenzen und für mobile Endgeräte

c) **MP3 (MPEG-1 Audio Layer 3):**
   - Verlustbehaftete Audiokompression (Entfernung nicht hörbarer Frequenzen, lautstärkenabhängige Kodierung, Weglassen von Pausen), ca. 8–300 kbit/s
   - Anwendung im Internet (Online-Tauschbörsen und -Shops), MP3-Player.

18.1.2 Verschlüsselung und Datensicherheit

Eine wesentliche Rolle in Netzwerken spielen Kryptografie und Steganografie [10, 14, 15, 16]. **Die wichtigsten Schutzziele werden durch folgende eingebetteten Sicherheitsmechanismen abgedeckt:**

- Vertraulichkeit (per Verschlüsselung der Nachrichten bzw. Pakete)
- Integrität (Einbettung von Prüfdaten in den Nachrichten)
- Zugriffsschutz (per Authentisierung der Nachrichten bzw. Pakete)
- Zurechenbarkeit (mittels der Digitalen Unterschrift der Pakete/Nachrichten).

Die folgenden wichtigsten Kryptostandards sind aktuell und kommen meist zum Einsatz in den Rechnernetzanwendungen:

a) **AES, 1998–2003 eingeführt**
   - ***Advanced Encryption Standard***
   - entwickelt von Vincent Rijmen, Joan Daemen (Belgien)
   - standardisiert durch NIST
   - mit Schlüsseln der Länge 128/256 Bit

b) **RSA, 1977–1983 eingeführt**
   - ***Rivest-Shamir-Adleman-Chiffre,*** entwickelt von Ron Rivest, Adi Shamir, Leonard Adleman (USA-Israel)
   - standardisiert durch RSA Security, ANSI, IEEE
   - mit Schlüsseln der Länge 1024/2048 Bit

c) **DES, 1972–1977 eingeführt**
   - ***Data Encryption Standard***
   - entwickelt und standardisiert von IBM, NSA, NIST/ehemals NBS (USA)
   - mit Schlüsseln der Länge 56/168 Bit

d) **PGP/OpenPGP, ein offener Standard (seit 1991)**
   - „Ziemlich gute Privatsphäre", ***Pretty Good Privacy***
   - entwickelt von P. Zimmermann als freies Rahmenprogramm für zivile Zwecke.

PGP, Pretty Good Privacy (auf Deutsch: „Ziemlich Gute Privatsphäre“) ist ein offener Standard von P. Zimmermann, Pionier und Wegbereiter der Popularisierung von Kryptoverfahren für zivile Zwecke (▶ http://philzimmermann.com/EN/background/index.html). Im Jahre 1991 hat P. Zimmerman die aktuellen Kryptoverfahren als Software der Allgemeinheit zugänglich gemacht, u. a. DES, RSA, DH-Schlüsselaustausch, MD5, Elgamal, AES (Rijmen). Dabei nutzte er eine Schlüssellänge von 128 Bit (d. h. über die 56 Bit-Schranke), was einen mutigen Verstoß gegen USA-Rechtsvorschriften bedeutete. Als kurze Historie dazu:

- 1991: PGP-Veröffentlichung im Internet, Siegeszug rund um die Welt
- Gründung PGP Corp.
- aber 1993–1997: Gerichtsprozess der US-Regierung gegen P.Z. wegen illegalem Export militärisch nutzbarer Software
- Veröffentlichung von PGP bei MIT-Press Verlag als Theoriebuch mit sämtlichen Quelltexten, dadurch kein weiteres Gerichtsverfahren
- 1997: Einführung des IETF-Standards namens OpenPGP.

PGP ist ein typisches Verfahren der Kryptotechnik. Für alle diese Verfahren gelten nachfolgende Erläuterungen.

Die kryptografische Absicherung oder Verschlüsselung V(T, K) des Klartextes T erfolgt mit dem Einsatz eines geheimen Schlüssels K als Parameter zu dem wohluntersuchten und dokumentierten Kryptoverfahren V (laut der sog. KP1883, Prinzipien von A. Kerckhoffs).

Die Chiffre C bildet man als $C = V(T, K)$.

Die Entschlüsselung E ist zur Verschlüsselung reversibel: $E(V(T, K), K') = T$. (18.1)

Der Schlüssel für die Entschlüsselung K′ muss nicht gleich dem Verschlüsselungsschlüssel K sein:

$$\text{Symmetrische Verfahren: } K = K' \qquad (18.2)$$

$$\text{Asymmetrische Verfahren: } K\ != K'$$

Zur Verschlüsselung wird i. d. R. eine effiziente Kombination von symmetrischen und asymmetrischen Verfahren verwendet. Die Kombination beider Verfahren verfolgt das Ziel, Sicherheit und Effizienz zu integrieren (◘ Abb. 18.3):

- Symmetrisches Verfahren zur Verschlüsselung umfangreicher Meldungen
- Schlüssel wird aber für jede Meldung neu generiert und mit asymmetrischen
  Verfahren in verschlüsselter Form übertragen.

Das Prinzip der digitalen Unterschrift (s. ◘ Abb. 18.4) liegt darin, dass die Prüfsumme über den gesamten Nachrichteninhalt

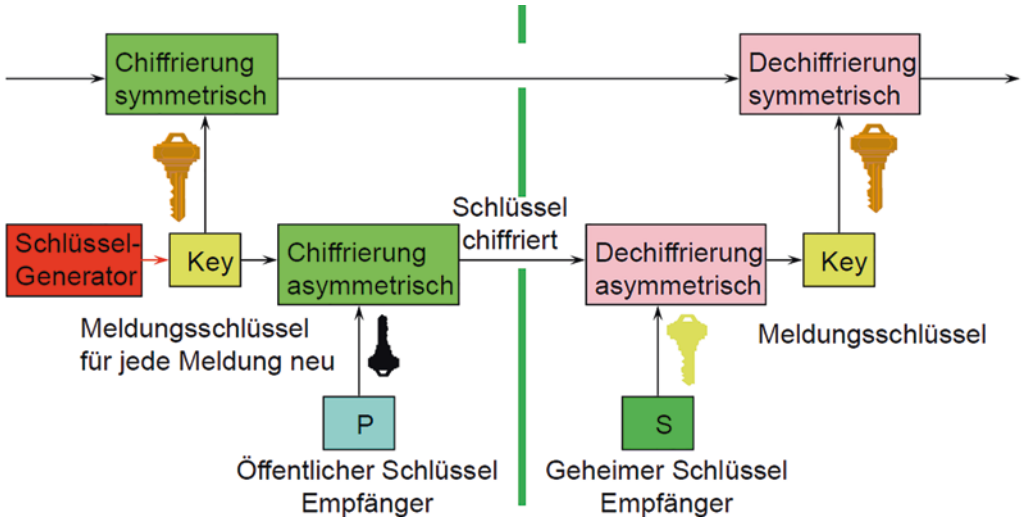


Abb. 18.3 Effiziente Kombination von symmetrischen und asymmetrischen Kryptoverfahren [16]

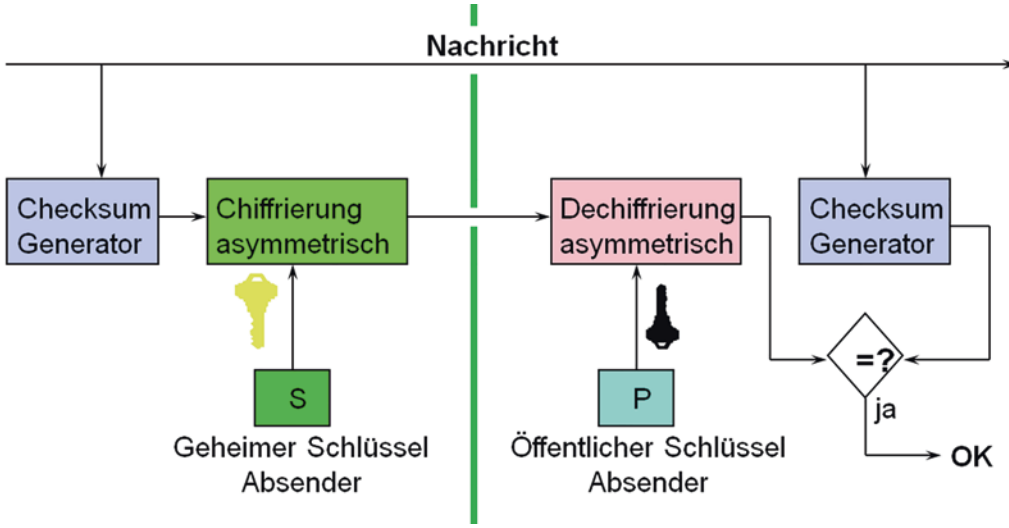


Abb. 18.4 Prinzip der Erzeugung und Verifikation der digitalen Signatur [16]

asymmetrisch mit dem privaten Schlüssel des Senders chiffriert wird (Umkehrung des asymmetrischen Verfahrens). Der Empfänger kann die Authentizität des Senders und Integrität der Nachricht prüfen (Verifikation der Digitalen Signatur).

Beispiel 18.1. Beschreibung des RSA-Verfahrens [16]

(Ronald Rivest (US), Adi Shamir (IL), Leonard Adleman (US) @ MIT):

1. Wähle Primzahlen p und q größer als 10^{100} (18.3)
2. Berechne $n = p * q$ und $z = (p - 1) * (q - 1)$

3. Wähle eine Zahl d teilerfremd zu z (Regel: $d > 2^{128}$)
4. Finde e, sodass gilt: e * d mod z = 1

Verschlüsseln (Klartextblock T): $C = T^e \bmod n$ (e, n öffentlich)
Entschlüsseln: $T = C^d \bmod n$ (d nicht aus e berechenbar)
Die Zahlenwerte (stark vereinfacht aus numerischen Gründen) sind wie folgt:
p = 3 und q = 11 → n = 33, z = 20
d = 7, e = 3 (e * d mod 20 = 3 * 7 mod 20 = 1)
Verschlüsseln T = 5 → $C = 5^3 \bmod 33 = 125 \bmod 33 = 26$
Entschlüsseln → $T = 26^7 \bmod 33 = 5$

18.2 Verzahnung der Anwendungsschicht und Standarddienste

Die Anwendungsschicht (Schicht 7) wird durch eine Vielfalt von Anwendungen, mobilen Apps und zugehörigen Diensten vertreten. U. a. gehören dazu:

- Anwendungsorientierte Internet-Dienste und –Protokolle (z. B. DNS, HTTP, FTP, Telnet/SSH, SMTP, POP3/IMAP etc.)
- Softwaretechnische Komponenten und Mechanismen zur Realisierung von Rechnernetz-Anwendungen (verteilte Systeme, Client/Server-Kommunikationsmodell, Fernaufrufe, wie Remote Procedure Call, CORBA Object Request Broker, Remote Method Invocation, Webservices und Komponentensoftware, Application Server und Middleware, virtuelle Maschinen und Ausführungsplattformen)
- Multimedia-Anwendungen und Groupware (Voice-over-IP, Skype, Videokonferenzen, Application Sharing durch P2P-Kommunikationsmodell).

Dabei sind die o. g. universellen Dienste, softwaretechnische Komponenten und Mechanismen sowie die Netzanwendungen und mobile Apps selbst meist schichtenübergreifend (L5-7) und untereinander verzahnt. Die Netzanwendungen und mobile Apps werden dann auf den host- und gerätespezifischen Plattformen durch verfügbare Applikation Server (seltener per CORBA – *Common Object Request Broker Architecture,* sehr oft per EJB – *Enterprise Java Beans,* .NET (Microsoft), im Embedded-Bereich per OSGi – *Open Services Gateway initiative*) ausgeführt.

Dabei sind die o. g. universellen Dienste, softwaretechnische Komponenten und Mechanismen sowie die Netzanwendungen und mobile Apps selbst meist schichtenübegreifend (L5-7) und untereinander verzahnt.

In der Vielfalt von sogenannten Standarddiensten im Internet sind die wichtigsten:

DNS (Domain Name System), WWW (World Wide Web, W3C), Email, File Transfer und Remote Login (oft über SSH – Secure Shell), Video- und Audiostreaming (über verschiedene Services, z. B. auch kostenlose wie YouTube oder

Spotify), Content Delivery und P2P (multimediale Tauschbörsen, Communities und soziale Netzwerke), VoIP- und Conferencingsysteme.

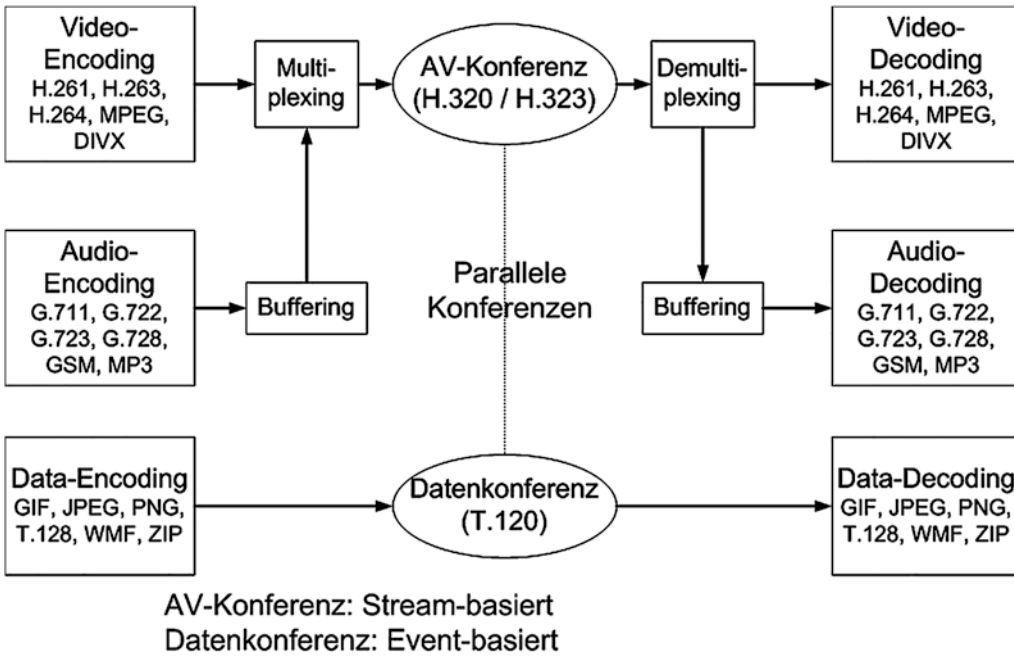
Viele von den oben genannten Services sind Ihnen gut bekannt durch den Alltag, jedoch diskutieren wir ein paar wichtige Aspekte im Weiteren in Form von Übungsaufgaben. Weiterhin konzentrieren wir uns auf die Darstellung von einigen dieser bekannten Konzepte: P2P und VoIP bzw. deren Kombination u. a. die Teleconferencingsysteme und Skype.

18.2.1 Teleconferencing und VoIP

■ **Teleconferencing**

Das Teleconferencing als Internetdienst bietet drei wesentliche Modi (◘ Abb. 18.5): Daten-, Audio- und Videoconferencing [16]. AV-Konferenzen sind streambasiert während Datenkonferenzen eventbasiert sind. Diese Modi nutzen unterschiedliche Codecs aufgrund diverser Anforderungen an die akzeptable Datenrate (1:10…1:50) und Komprimierungsrate (1:100…1:300).

Jedoch erfolgt im Protokoll-/Codecbereich die Ablösung von H.320/H.323 –Codecs, welche durch die ITU-T spezifiziert



◘ **Abb. 18.5** Breite Palette von Technologien und Codecs zum Teleconferencing. (Quelle: ► www.rn.inf.tu-dresden.de)

wurden, durch das Internet-basierte SIP (Session Initiation Protocol) mit der weiteren wesentlich verbesserten Anpassung von Videoströmen an unterschiedliche Datenraten und Endgeräte. Das Protokoll SIP ist aus der Internet-Technologie heraus erstanden und ähnelt im Aufbau und Struktur dem HTTP [6].

Der heutige Videokonferenzmarkt verwendet eine Reihe von Umsetzungsvarianten, deren Ausstattung im Wesentlichen vom Einsatzzweck abhängt:

- Desktop-Systeme und PCs: mit USB-Webcam, Mikrofon, Headset mithilfe der Clientsoftware wie NetMeeting, VNC, Skype, ooVoo, Viber etc.
- Settop-Boxen: Netzanschlüsse meist per DSL, LTE, WLAN und Ethernet-LAN
- Raumsysteme: leistungsstärkere Anlagen (Kameras, Raummikrofone, große Monitore, größere Räume).

IMS-basierte Videokonferenzen (IP Multimedia Subsystem, Bestandteil der LTE/4G-Systemarchitektur) erfolgen über Mobilfunknetze wie UMTS, HSDPA, LTE mit dem Einsatz einer Kommuniktionsanwendungssoftware, z. B. des Services Skypephone mit BREW OS.

■ Internet-Telefonie per VoIP

Die Übertragung von Telefongesprächen als Audio-Frames, die in IP-Pakete eingebettet sind, heißt „Voice-over-IP“ (VoIP). Durch VoIP bekamen die Nutzer viele Vorteile:

- breiter Einsatz bei IP-Netzwerken und bei 4G mit akzeptabler Sprachqualität
- oft kostenfreie Nutzung der Internet-Telefonie durch die DSL-Teilnehmer mit Internet-Flatrate
- kostengünstige Pauschaltarife (ebenfalls Flatrate) für den Übergang ins herkömmliche Telefonnetz (PSTN – Public Switched Telephone Network) und in die Mobilfunknetze
- in Software konfigurierbare Zusatzfunktionen (z. B. Rufweiterleitung, Rufblockierung, Rufnummernunterdrückung, Faxfunktion).

Das Protokoll H.323 für VoIP hat seinen Ursprung aus der digitalen Festnetz-Technologie heraus (ISDN). Das neuere SIP wurde durch die IETF spezifiziert und stellt ein großes Konkurrenzprotokoll zu H.323 bei VoIP dar.

SIP funktioniert als reines Signalisierungsprotokoll, welches ständige Weiterentwicklung bzw. Anpassung an marktspezifische Kriterien bietet (Quelle: ► http://www.voip-information.de).

18.2.2 Skype

Der Dienst Skype ist heutzutage der erfolgreichste Rivale zu zahlreichen VoIP-Services mit den gebräuchlichsten Protokollen SIP/RTP oder SIP/UDP. Der Service ist überwiegend nichtkommerziell und kostenfrei und ist daher sehr attraktiv im Privatbereich.

Skype verwendet eine hybride Architektur: Peer-to-Peer (P2P) und Client-Server-(C-S) werden untereinander kombiniert. Zugrunde liegt ein proprietäres Kommunikationsprotokoll Skype (vgl. SIP/RTP). Das System ist IPv4- und IPv6 –basiert und transparent für NAT, damit geeignet für Homeuser. Skype kann auch den TCP-Port 80 (vgl. WWW) und TCP-Port 443 zum Verbindungsaufbau verwenden, d. h. zur kryptografischen Absicherung des Datenverkehrs kommt das SSL-VPN (Kombination des Protokolls TLS und VPN über unsichere IP-Netze) zum Einsatz.

Kurze, aber aufschlussreiche Historie von Skype:
SW wurde von Ahti Heinla, Priit Kasesalu und Jaan Tallinn (Estland, 2003) entwickelt.
Die gleichnamige Firma wurde von Niklas Zennström/Janus Friis im Juli 2003 in Luxemburg gegründet.
Ab Sept. 2005 – Eigentum von eBay.
2007 entwickelte Skype sein eigenes Smartphone unter dem Brandnamen „Skypephone" mit dem BREW OS und Nutzung von UMTS, HSDPA und LTE.
An Okt. 2011 – Tochtergesellschaft von Microsoft.
Verfügbarkeit:
Windows 10, Mac OS X, Linux, sowie mobil – Apple iOS, OHA Android, Symbian, Maemo, MeeGo, Pocket PC, Windows 10, RIM BlackBerry

Die Datenkompression erfolgt nach effizienten Standardcodecs: SVOPC (16 kHz), AMR-WB (16 kHz), G.729 (8 kHz), G.711; seit 2009 kam der hauseigene proprietäre Audio-Codec SILK zum Einsatz.

Aufgrund der gewissen Ineffizienz des ursprünglichen Skype-Netzes (2003–2010) mit der P2P-Organisation (Probleme wie bei zahlreichen MM-Tauschbörsen und dabei häufig illegal) wurden die s. g. Nodes und Supernodes mit freiwilliger Umwidmung eigener privater Rechner zu stark ausgelastet. Gehäufte Ausfälle durch Überlastung von Peers erzeugten steigernde Kritik seitens der Privatuser.

Microsoft bereinigte die Skype-Struktur 2011–2012. Im Rahmen der Restrukturierung wurde das Skype-Netz von den Clientrechnern zu den eigenen Linux-Servern, also von P2P zum zentralisierten C-S-Aufbau, überführt. Die Servercluster wurden in gesicherten Datacentern (Clouds mit PaaS/IaaS) platziert, was eine verbesserte Skalierbarkeit und Sicherheit der Skype-Server mit sich brachte.

- **Bewertung von Skype**

Der Service bietet die folgenden gekapselten Dienste: VoIP, Videoconferencing, Chat, Instant Messaging, Screenshot- und Filetransfer und ist zur konventionellen Telefonie kompatibel. Es stehen die Gateways zu herkömmlichen Telefonnetzen (PSTN/ISDN/GSM) zur Verfügung (call via phone).

Gewisse Nachteile des Skype sind:

- Das Skype Protocol selbst: wurde nicht veröffentlicht, was Kritik seitens der User/Hersteller verursachte
- die P2P-Struktur, die das Mitnutzen der Kapazität der Nutzerrechner zum Weiterleiten von Anrufen anderer User bedeutet, deswegen musste die Security umfangreich überarbeitet und begutachtet werden
- mitunter niedrige Verständigungsqualität

Die expliziten Vorteile des Skype:
- keine Zusatzkosten für die User
- zahlreiche Desktop- und mobile Client-Versionen von Skype
- bereinigte und abgesicherte Struktur
- Anbindung von SIP-Telefonanlagen wie bspw. Asterisk an Skype möglich
- weltweite Skype-Anerkennung, bis ca. 300–500 Mio. User weltweit
- bestätigte Datensicherheit: AES mit 256-Bit-Key, RSA mit 2048-Bit-Key, PKI nach X.509

Die Entwicklung eigener Client-Anwendungen (◘ Abb. 18.6) unter Nutzung der Skype API ist auch möglich. Anbei ist für die Entwickler von Skypeclients die programmtechnische Basis von einigen Herstellern aufgeführt:
- **Win GUI wurde** - mit Pascal und Delphi entwickelt
- **Linux GUI – « – mit C ++**
- **Mac OS GUI – « – mit Objective**-C und Cocoa

Außerdem steht noch Internet Direct (Indy) in einer Open Source Socket-Bibliothek zur Verfügung.

18.2.3 Vitero: Online-Tutorien und Videokonferenzen an der HS OWL

Für die Online-Tutorien an der OWL werden die Videokonferenzen per Vitero-Software genutzt (► https://www.vitero.de/).

Das Tool bietet effektive Zusammenarbeit für seine Teilnehmer im Konzept „Virtual Telco Room“ durch die Webkonferenzen.

Der entscheidende Vorteil von Vitero gegenüber den klassischen Telekonferenzen (per Telefon, VoIP, Video, Web) ergibt sich aus der Ergonomie. Die folgenden Dienste stellt Vitero den Usern zur Verfügung:
- Audio (per Telefon und VoIP)
- Fotos und Livebilder (per Webcam)
- Application Sharing (gemeinsames Bearbeiten von Dokumenten, Groupware)
- Visualisierung und Interaktionen (Folien, Online-Abstimmungen, Untergruppen für die Teilnehmer, Kartenabfrage etc.).

Beispiel 18.2

Ein folgendes Szenario kann untersucht werden (s. ◘ Abb. 18.7).
Sie möchten eine Videokonferenz mit mehreren Partnern per Vitero aufbauen [16]. Sie nutzen ein Mehrpunktkonferenzsystem mit einer sternförmigen Architektur [16] und einer zentralen

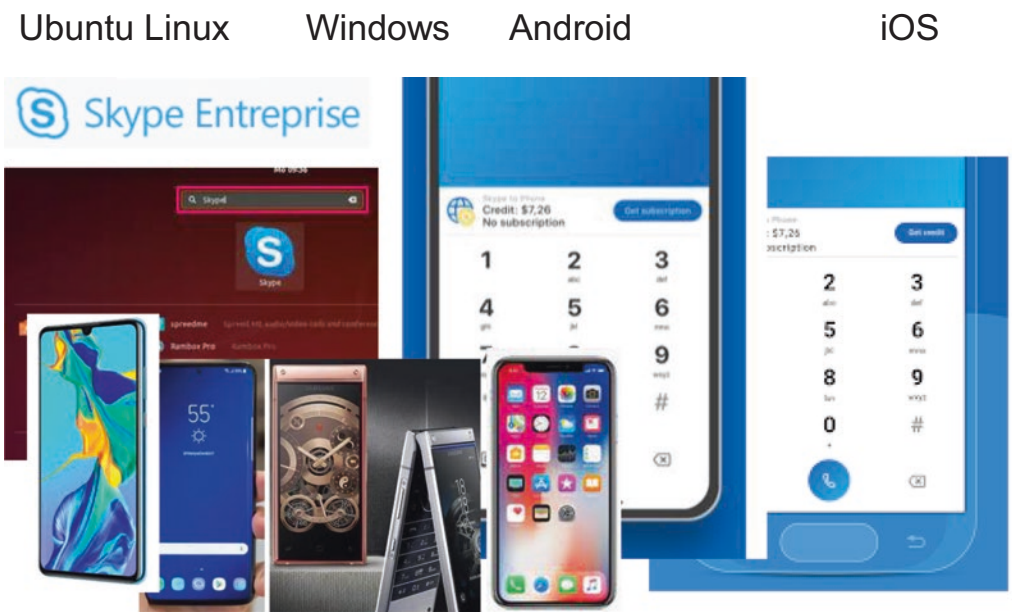


Abb. 18.6 Skype-Vielfalt: die Screenshots in verschiedenen Betriebssystemen

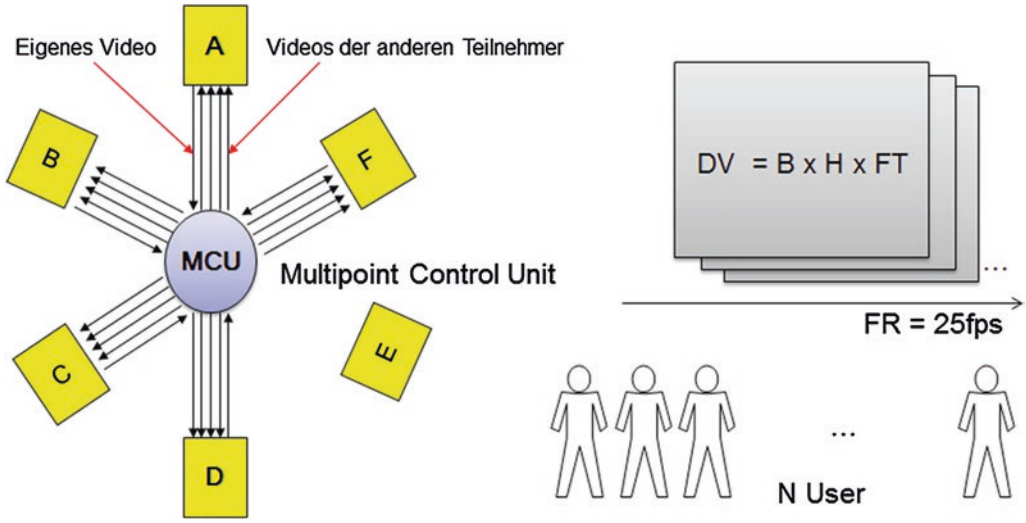


Abb. 18.7 Videokonferenzen per Vitero für N User bei angegebenen DV und FR

18

MCU-Einheit (Multipoint Control Unit). Vitero sendet ein Video mit der Auflösung A_1, A_2, A_3 (s. unten) mit einer Farbtiefe FT von 24 Bit/Pixel und einer Framerate FR von 25 fps:

- Videowiedergabe $A_1 = 480 \times 270$ Pixel
- Videowiedergabe $A_2 = 640 \times 360$ Pixel
- Videowiedergabe $A_3 = 1280 \times 720$ Pixel

Berechnungen:

a) Mit welchem Kompressionsfaktor müssen Sie ihr zu sendendes Videosignal komprimieren, wenn Sie einen DSL-Anschluss (Upstream: 5 MBit/s, Downstream: 100 MBit/s) nutzen?
b) Mit wie vielen Partnern N können Sie eine Videokonferenz aufbauen, wenn alle Partner Videos mit der gleichen Qualität mit dem Faktor fk = 111 (111:1) komprimiert senden und 20 % Overhead durch Protokoll-Header entsteht?
c) Im Regelfall sollte man aber nur maximal 60 % der zur Verfügung stehenden Bandbreite für die Videoübertragung nutzen. Wie kann die zu übertragene Datenmenge angepasst werden, damit Sie weiterhin mit allen Partnern kommunizieren können? Wie wirkt sich das auf die Qualität der Videos aus?
d) Welches maximales Datenvolumen V kann dabei pro User und pro Stunde T = 1 h bei der max. Übertragungseffizienz von k = 0,6 (60 %) transferiert werden?

Lösungen:

a) Mit welchem Kompressionsfaktor müssen Sie ihr zu sendendes Videosignal bei Vitero komprimieren, wenn Sie einen DSL-Anschluss (Upstream: 5 MBits/s; Downstream: 100 MBit/s) nutzen?

Gegeben:

- Farbtiefe FT = 24 bit/Pixel, Framerate FR = 25 fps

Auflösung:

- Videowiedergabe A_1 (480 × 270 Pixel)
- Videowiedergabe A_2 (640 × 360 Pixel)
- Videowiedergabe A_3 (1280 × 720 Pixel)

Farbtiefe FT = 24 bit/Pixel, Framerate FR = 25 fps
DSL-Anschluss: Upstream: 5 MBit/s, Downstream: 100 MBit/s
Gesucht: Kompressionsfaktor fk

Datenvolumen des unkomprimierten Videosignals:

$$\mathbf{DV = A_i * FT(i = 1, 2, 3)} \tag{18.4}$$

Datenrate des unkomprimierten Videosignals: $\mathbf{DR = DV * FR}$

- **Videowiedergabe mit A_1 (480 × 270 Pixel)** - 480 * 270 * 24 * 25 = 77,76 Mbit/s
- **Videowiedergabe mit A_2 (640 × 360 Pixel)** - 640 * 360 * 24 * 25 = 138,24 Mbit/s
- **Videowiedergabe mit A_3 (1280 × 720 Pixel)** - 1280 * 720 * 24 * 25 = 552,96 Mbit/s

Kanal zum Senden besitzt die $\mathbf{DR = 5MBit/s \quad fk = DR_{Videowiedergabe}/DR}$ (18.5)

fk = 78 Mbit/s / 5 Mbit/s = 16
fk = 139 Mbit/s / 5 Mbit/s = 28
fk = 553 Mbit/s / 5 Mbit/s = 111

Empfohlene Kompression sind - 16:1 oder 28:1 oder 111:1 je nach Auflösung A_1, A_2, A_3

b) Mit wie vielen Partnern N können Sie eine Videokonferenz aufbauen, wenn alle Partner Videos mit der gleichen Qualität mit dem Faktor fk = 111:1 komprimiert senden und 20 % Overhead durch Protokoll-Header entsteht?

Gegeben:
Videowiedergabe mit A_3 (1280 × 720 Pixel) - 1280 * 720 * 24 * 25 = 552,96 Mbit/s

Kompressionsfaktor fk = 111:1
DSL-Anschluss: Upstream: 5 MBit/s, Downstream: 100 MBit/s
Gesucht: Anzahl der Partner N
Benötigte Datenrate:

$$DR_{netto} = 552{,}96 \text{ Mbit/s} / 111 = 5 \text{ Mbit/s}$$

+20 % Overhead:

$$DR_{brutto} = 120\ \% * 5 \text{ Mbit/s} = 6 \text{ Mbit/s}$$

Kanal zum Empfangen (DSL-Downstream): 100 MBit/s
Anzahl der zu empfangenen Videostreams **N = 100 MBit/s: 6 MBit/s = 16 > 13 User** möglich
Kommunikation mit N = 13 Partnern möglich (Vitero-Tool unterszützt bis zu 13 User).

c) Im Regelfall sollte man aber nur maximal 60 % der zur Verfügung stehenden Datenrate DR für die Videoübertragung nutzen.
Wie kann die zu übertragene Datenmenge angepasst werden, damit Sie weiterhin mit allen Partnern kommunizieren können?
Wie wirkt sich das auf die Qualität der Videos aus?

Die Antwort entnehmen Sie in ◘ Tab. 18.2.

d) Welches maximales Datenvolumen V kann dabei pro User und pro Stunde T = 1 h bei der max. Übertragungseffizienz von k = 0,6 (60 %) transferiert werden?

Gegeben: DRbrutto = 6 MBit/s, k = 0,6, T = 1 h
Mögliche Voraussetzungen:
Audio über VoIP, Folienübetragung, Video per Webcam, Application Sharing
Gesucht: Datenvolumen V

$$\mathbf{V = k * T * DR_{brutto}} \tag{18.6}$$

V= 1/8 Bit/Byte * 0,6 * 3600 s * 6 MBit/s = 1/8 * 0,6 * 3600 * 6 = 1620 MByte

Tab. 18.2 Optimierungswege für Videoübertragung/Videokonferenzen

Reduzierung der Datenmenge durch	Auswirkungen auf die Qualität der Videos
Höhere Komprimierung	Verringerung der Bildqualität (größere Artefakte, „pixelig“)
Kleinere Framerate	Es werden weniger Bilder pro Sekunde gesendet. Bewegungen der Teilnehmer wirken ruckartig
Verringerung der Bildgröße DV = B * H	Kleineres Bild wird übertragen (z. B. 480 × 270 Pixel) (es gibt Videokonferenzsysteme, die nur den gerade Sprechenden größer, alle anderen Teilnehmer kleiner darstellen. Nachteil: Großer Rechenaufwand zur Überwachung, zu schneller Wechsel bei Diskussion zwischen mehreren Personen, nur für einseitigen Vortrag geeignet)
Verringerung der Farbtiefe	Bild wirkt blass
Reduzierung der Samplerate des Audios	Schlechte Tonqualität (klingt „dumpf“, „blechern“)

Die bei Vitero dokumentierten Werte sind:

- Modell: Audio über VoIP, keine Folien, eine Avatarwebcam, Application Sharing
- Teilnehmeranzahl N = 13, Auflösung $A_3 = 1280 * 720$ Pixel
- „Insgesamt kommt man in einer Sitzung dieser Art auf ca. 225 MByte Datenvolumen pro Stunde und Teilnehmer.“ (s. die Referenzenen zu Vitero unten).

Vitero-Referenzquellen:

1. Vitero-Konferenzsystem/Virtual Telco Room – Audio über VoIP/Telefon, Folien, Video per Webcam, Application Sharing (Online): ► https://www.vitero.de/de/anwendungsbereiche/e-learning.html
2. Viteros Technische Daten (Online): ► https://www.vitero.de/docs/vitero_datenvolumen.pdf

18.3 Sicherheit in Netzen

Als die Nutzung des Internets noch einem kleinen wissenschaftlichen Personenkreis vorbehalten war, kamen noch keine Absicherungsmaßnahmen für die Kommunikation zum Einsatz, da dafür kein Bedarf bestand. Nach der Kommerzialisierung des Internets und der größeren Verbreitung in allen Bevölkerungsschichten und Industrien wurden Maßnahmen nötig, die einen sicheren Datenverkehr ermöglichen. Hierfür wurden Kryptoverfahen/Kryptoprotokolle entwickelt, umgesetzt und stetig verbessert.

Die Einsatzgebiete (und es ist eine bei weitem nicht volle Liste!) für die Kryptoverfahren sind wie folgt:

- E-Commerce und Online-Banking
- Anwendungsorientierte Internet-Dienste und -Protokolle (z. B. WWW, Soziale Netzwerke, Clouds, Grids, VoIP/Skype, P2P-Systeme, sowie Anwendungen mit FTP, TELNET, SMTP, mobile Apps);
- Realisierung von Rechnernetz-Anwendungen und Apps (verteilte Systeme, Client/Server-Modell, Remote Procedure Call, Webservices, Komponentensoftware, Applikation Server);
- Multimedia-Anwendungen und Groupware (Videostreaming, Videokonferenzen, Application Sharing).

18.3.1 Kryptoprotokolle

Die folgenden Internet-Sicherheitsprotokolle kommen schichtenübergreifend zum Einsatz:

- IPsec (Secure IP) über Layer 3
- TLS/SSL (Transport Layer Security/Secure Socket Layer) über Layer 4
- PKI (Public Key Infrastructure zum TLS/SSL).

Die nachstehenden Protokolle zur kryptografischen Absicherung kommen oft zum Einsatz im Internet über die Schicht 6:

- S-HTTP (Secure Hypertext Transfer Protocol über TLS/SSL, URL: https://…)
- S-MIME (Secure MIME, multimediale Ergänzung zum Email-Dienst)
- Kerberos (Authentisierungsstruktur und Schlüsselverteilung in asym. Kryptoverfahren)
- SET (Secure Electronic Transactions von Verisign/MS, meist verzahnt mit TLS/SSL aus Kostengründen)
- PGP (Pretty Good Privacy).

Dabei erfolgt meist die Kombination asymmetrischer Kryptoverfahren (Schlüsselverteilung) mit symmetrischen Kryptoverfahren (Nachrichtenverschlüsselung) aus Effizienzgründen. Speziell für IPsec, bestehend aus AH (Authentication Header) und ESP (Encapsulating Security Payload), setzt die Realisierung direkt auf IP für virtuelle private Netze (VPN) auf und wird anwendungsübergreifend zwischen den Einwahlpunkten genutzt. Andere Verfahren funktionieren oberhalb der Transportschicht (L4), meist direkt mit der jeweiligen Anwendung (L5-7) verzahnt. Eine kompakte Übersicht über die Kryptoprotokolle ist unten aufgeführt (◘ Abb. 18.8):

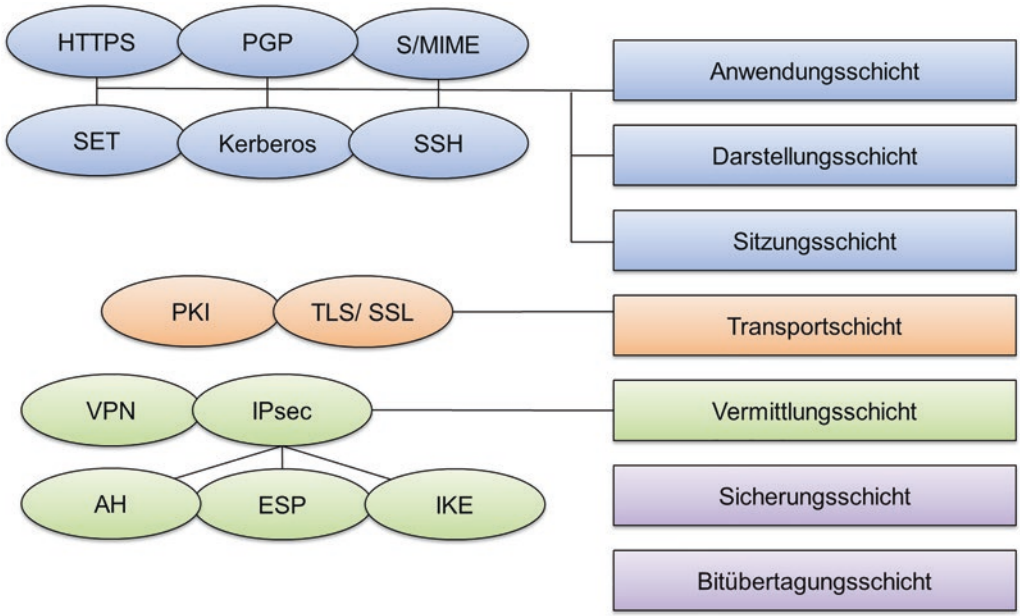


Abb. 18.8 Übersicht über die Kryptoprotokolle: übertragungs- und verarbeitungsorientierte Schichten

18.3.2 Einsatz von Firewalls

Eine Firewall (FW) ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt und ist auch ein Teilaspekt eines Sicherheitskonzepts des Unternehmens. Zuordnung der FW-Systeme (Filterung-Funktionalität) zu den OSI-Schichten ist wie folgt [11, 16]:

- PF (Layer 3)
- CR (Layer 4)
- AG (Layer 5–7).

Das Ziel einer FW ist die mehrseitige Filterung/Blockierung unberechtigter Zugriffe in privaten Netzwerken, zu den Anwendungen und Datenbeständen auf der Basis von IP-Adressen (PF, Paketfilter), TCP/IP-Portinformationen (CR, Circuit Relay) bzw. anwendungsbezogenen Informationen (AG, Application Gateway). Die Zusammenfassung der Filtermöglichkeiten einer Firewall ist wie folgt (Tab. 18.3):

Die Filtermöglichkeiten einer fortgeschrittener Firewall vom Typ SIF (Stateful Inspection) oder vom Typ NG-FW (New Generation Firewall) sind wie folgt:

- Kombination der Filterungsvermögen PF, CR und AG
- IDS/IPS (Intrusion Detection/Intrusion Prevention) -Systeme.

Tab. 18.3 Zusammenfassung der Filtermöglichkeiten einer Firewall

Filtermöglichkeiten einer Firewall	FW-Typen		
	PF	CR	AG
1. IP-Quell-/Zieladressen	x		
2. Domain Names (Quelle/Ziel)			x
3. Zugelassene/verbotene Protokolle bzw. TCP-Ports, z. B. http, ftp, SMTP	x		x
4. Beliebige inhaltsbezogene Schlüsselwörter (SPAM) ggf. auch anwendungsbezogene Authentisierung			x
5. Verschlüsselung			x
6. Schutz vor unberechtigten Remote-Login-Zugriffen			x
7. (distributed) Denial-of-Service-Attacken		x	
8. Ausführbare Makros, Skripte, Applets, Webservices			x

Öffentlich zugängliche Dienste (z. B. Web Server, ftp Server für File-Sharing etc.) [10, 11, 14, 16] werden in der DMZ (Demilitarized Zones) vor der eigentlichen Firewall platziert (Abb. 18.9).

- **Abgrenzung FW zu IDS/IPS [10, 16]**

Die Einsatzgebiete von Firewalls sind variabel. Die Funktion einer Firewall besteht aber nicht hauptsächlich darin, Angriffe zu erkennen. Die klassischen Firewalls sollen ausschließlich Regeln für die Netzwerkkommunikation umsetzen. Für das Aufspüren von Angriffen sind sogenannte IDS/IPS-Module ***(Intrusion Detection/IntrusionPrevention)*** zuständig, die durchaus auf einer Firewall aufsetzen können. Diese bauen zusammen mit dem Firewall-Modul ***fortgeschrittene Firewalls*** auf.

- **Intrusion Detection System (IDS):**
  - IDS beschreibt das Erkennen von Angriffen, die gegen ein Computersystem oder Netzwerk gerichtet sind und dient der Erhöhung der Sicherheit in einem Netzwerk.
- **Intrusion Prevention (IPS):**
  - diese Systeme sind erweiterte IDS, die im Falle eines entdeckten Angriffes zusätzlich Funktionalität zur Abwehr der Angriffe bereitstellen.

18.3.3 Collaborative Intrusion Detection Networks – CIDN

Die Angriffe (Threats, Attacks) wirken ganztags als Störung des Betriebs moderner Netze und Rechenzentren. Traditionelle IDS funktionieren isoliert und sind deswegen nicht richtig wirksam,

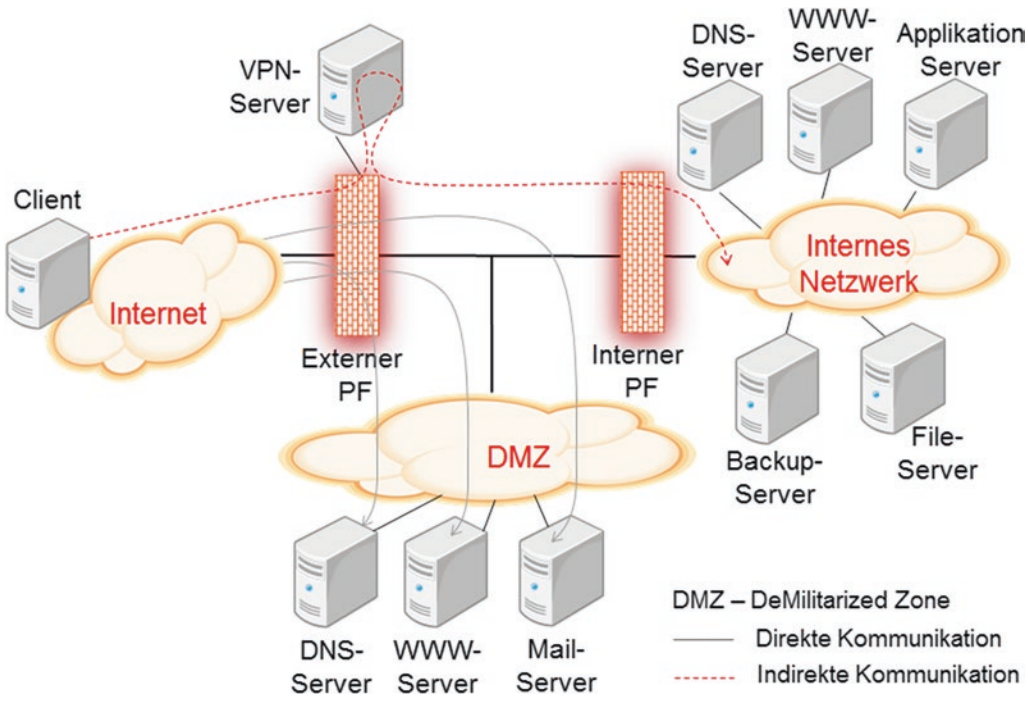


Abb. 18.9 DMZ: Öffentlich zugängliche und abgesicherte Dienste

weil sie unbekannte Bedrohungen, die immer weiter anspruchsvoller werden, nicht immer erkennen!

Ein CIDN (Collaborative Intrusion Detection Network) ist ein Kooperationsnetzwerk von einzelnen IDS, die paarweise ihr Wissen über Angriffe austauschen und damit die Verbesserung der Gesamtgenauigkeit und Effizienz von einzelnen IDS garantieren. Jedoch kann ein böswilliger Insider die Effizienz einzelner IDNs bspw. mittels Malware gefährden. Die wichtigsten CIDN-Funktionalitäten sind wie folgt [10]:

1. Auswahl von Peers (Collaborators) und Trust Management
2. Gemeinsames Entscheidungstreffen (Collaborative Intrusion Decision Making)
3. Ressourcenmanagement.

Die folgenden Anforderungen zu den CIDN sind am wichtigsten:

1. Leistungsfähigkeit
2. Robustheit
3. Skalierbarkeit
4. Kompatibilität vom einzelnen IDS.

Die traditionellen und die fortgeschrittenen Insider-Angriffe auf CIDN sind in Abb. 18.10 präsentiert.

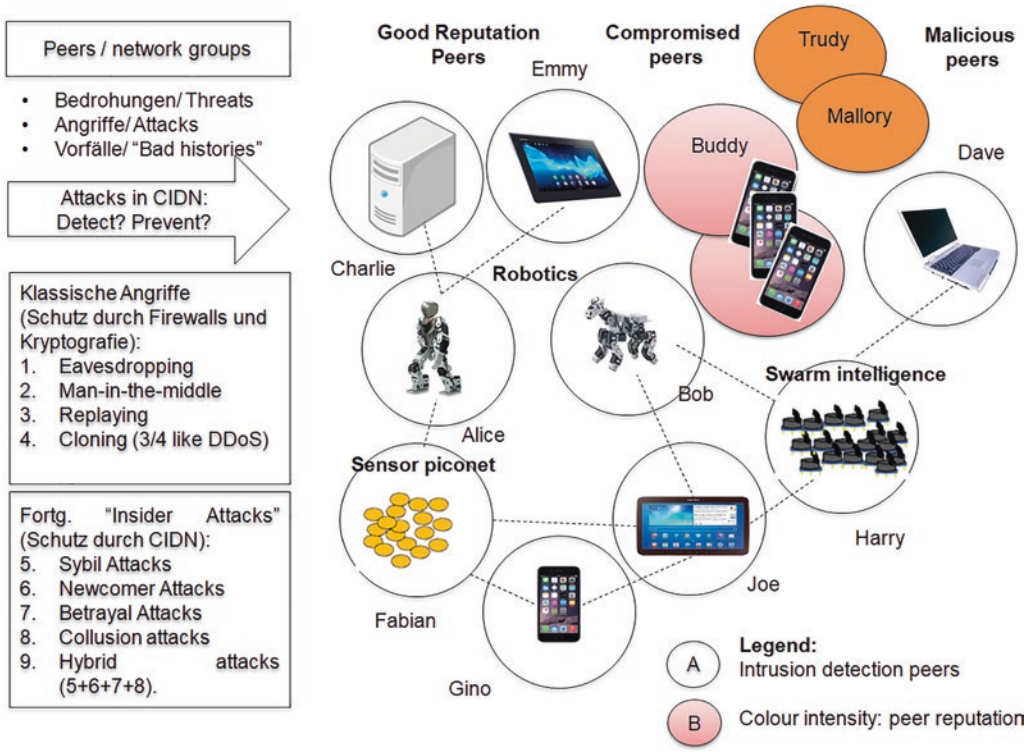


Abb. 18.10 Collaborative IDS-Netzwerke [10]

Die ersten vier Angriffstypen lassen sich trivial formulieren:

1. Lauschen-Angriffe: Eavesdropping
2. Verkleiden-Angriffe: Man-in-the-Middle, oder falsche Identität verwenden
3. Weiterleiten-Angriffe: d. h. Vermehren der „Malware" – Malicious Software – in Form von Viren, Trojanern, Würmen, Hoaxes, Greyware
4. Klonen-Angriffe: d. h. Vermehren sog. aktiver Denial-of-Service-Angriffe – DoS bzw. Distributed DoS, DDoS.

Die fortgeschrittenen Insider-Angriffe auf CIDN, die von Peers im CIDN durchgeführt werden, sind wie folgt:

5. Sybil-Angriffe (eine große Menge von Pseudonymen, gefälschten Identitäten, Fakes wird erzeugt)
6. Newcomer-Angriffe (die Peers mit „schlechter Reputation" löschen ihre schlechte Historien, die „X-Files" mit anderen Peers im Netzwerk)
7. Betrayal-Angriffe (der Vertrauensmechanismus ist robust und entspricht der sozialen Norm: „Es dauert eine lange Zeit und konsequent gutes Verhalten um hohes Vertrauen aufzubauen, während nur ein paar schlechte Handlungen es komplett ruinieren können"!

Tab. 18.4 Varianten eines kryptografisch abgesicherten Protokollstacks

Stack 1		Stack 2				Stack 3				Layer
Kerberos	HTTP, FTP, SMTP usw.	SSH (Port 443)		HTTPS (Port 465)	SPOP3 (995), IMAPS (991), IRCS (993)	HTTP, FTP, SMTP	S/MIME	PGP/ Open PGP	SET	Anwendung (L5–7)
		FTP	Telnet	HTTP	Weitere					
TCP/UDP		Sockets/TLS/SSL				TCP/UDP				Transport (L4)
		TCP								
AH	ESP	IP								Netzwerk (L3)
IPsec										
Netz-zugang	DSL	Ethernet	WLAN	WSN	VPN	3G–5G	…			PHY (1–2)

Wenn ein vertrauenswürdiger Peer unehrlich fungiert, wird sein Vertrauenswert katastrophal fallen. Daher ist es sich schwierig für diesen Peer, andere zu täuschen oder sein früheres Vertrauen innerhalb kurzer Zeit zurück zu gewinnen!)

8. Collusion-Angriffe treten auf, wenn eine Gruppe von kompromittierten oder bösartigen Peers agiert, um das CIDN zu kompromittieren.
9. Hybride Angriffe (5 + 6 + 7 + 8).

18.3.4 Kryptografisch abgesicherte Dienste und Protokollstacks

Die kryptografisch abgesicherten Dienste sind: SSH, HTTPS. Deren Positionierung in den kryptografisch abgesicherten Protokollstacks ist in ◘ Tab. 18.4 gezeigt.

18.4 Zwischenfragen/Übungsaufgaben

18.4.1 Kommunikationssteuerung

Über das Internet soll der Inhalt einer Festplatte (72 GByte) mit real 5 Mbit/s kopiert werden

(Hinweis: Speichergröße GigaByte als SI-Präfix).

a) Berechnen Sie die Dauer der Übertragung!
Wie hoch ist die Wahrscheinlichkeit w einer erfolgreichen Übertragung, wenn pro Stunde eine 10-%ige Ausfallwahrscheinlichkeit a der Transportverbindung existiert?
Wie kann das Betriebsverhalten gegenüber b) verbessert werden?

18.4.2 Datenaustausch zwischen heterogenen Computersystemen

In einem Netz mit 30 Computern existieren 3 verschiedene Systemarchitekturen.

a) Wie viele Import/Export-Routinen müssen programmiert und installiert werden, damit eine Verständigung zwischen allen Systemen möglich ist?
b) Welche Veränderungen ergeben sich, wenn ein weiterer Computer mit einer neuartigen Systemarchitektur in das Netz eingebunden wird?
c) Welche Vor- und Nachteile gegenüber b) ergeben sich bei Nutzung einer einheitlichen Transfersyntax?
d) Nennen Sie eine für einheitliche Transfersyntax geeignete Sprache.
e) Welche Vor- und Nachteile gegenüber a) und b) ergeben sich bei Nutzung von Java-Technologien?

18.4.3 Datenkomprimierung und Codecs

a) Wofür werden die Kompressionsverfahren bei den Netzwerken verwendet?
b) Wo werden ZIP, JPEG, MPEG-4 und MP3 eingesetzt? Nennen Sie jeweils mindestens ein Anwendungsgebiet!

18.4.4 Verschlüsselung

a) Vergleichen Sie den Einsatz von symmetrischen und asymmetrischen Verfahren bzgl. Performance und Schlüsselverteilung! Benennen Sie jeweils 2 konkrete Kryptoverfahren. Nennen Sie einige Vor- und Nachteile der asymmetrischen gegenüber den symmetrischen Kryptoverfahren!
b) Wie viel Zeit muss ein Angreifer für die Schlüsselermittlung durchschnittlich aufwenden (Durchprobieren – Angriff vom Typ Brute Force), wenn er lediglich weiß, dass eine symmetrische Verschlüsselung mit 5-Buchstabenschlüssel vorliegt und ein Dechiffrierungsversuch 10 ms dauert?
c) Beim RSA-Verfahren seien $p = 5$ und $q = 11$.
Geben Sie mögliche Werte für d und e an und verschlüsseln Sie die Zahlen 2, 3 und 4! Entschlüsseln Sie die chiffrierten Zahlen anschließend wieder!

Netzwerkanwendungen und mobile Apps

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_19

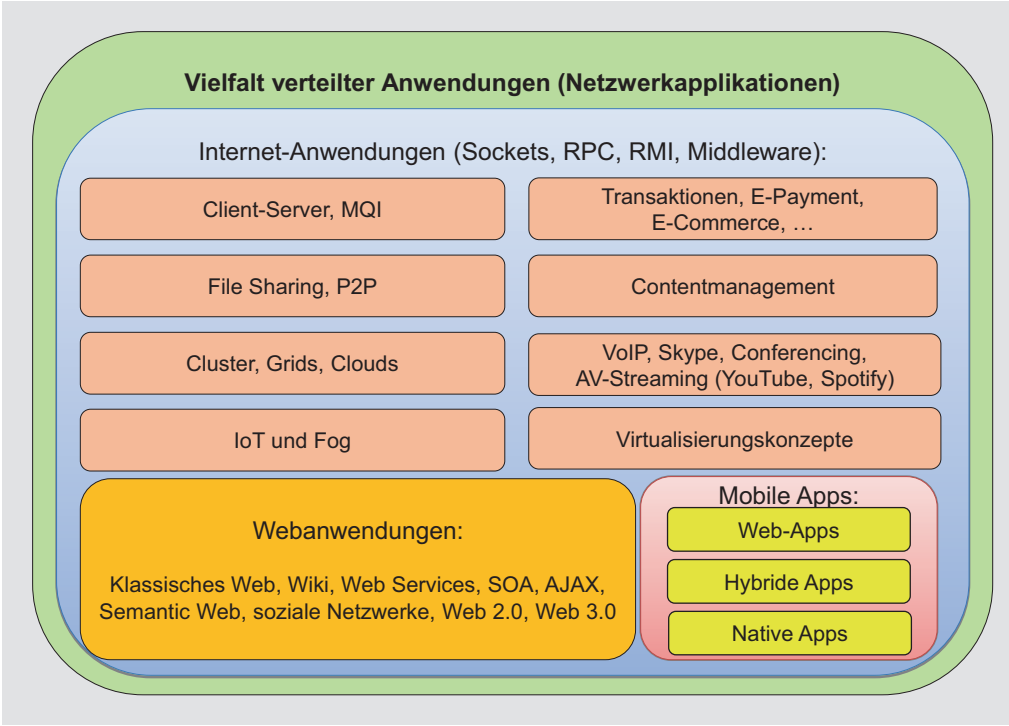


Abb. 19.1 Schematische Gesamteinordnung von aktuellen Netzwerkanwendungen

Die schematische Gesamteinordnung von aktuellen Netzwerkanwendungen ist in Abb. 19.1 repräsentiert. Aber wie Sie gleich erfahren werden, ist diese Kategorisierung nun sehr grob, aber eine genauere Kategorisierung ist aufgrund der Vielfältigkeit und Unmenge dern Einsatzgebiet und Eigenschaften kaum möglich!

19.1 Webanwendungen

19.1.1 „Klassisches" Web

Klassische Webanwendungen existieren seit etwa Anfang 1990er. Sir Timothy John Berners-Lee (geb. 1955 in London), britischer Physiker am CERN und berühmter Informatiker, hat damals die erste öffentliche Webpräsentation für ► info.cern.ch im Jahre 1990 entwickelt. Sir Berners-Lee ist Mitglied und Präsident of the World Wide Web Consortium (W3C) sowie Professor von Massachusetts Institute of Technology (MIT) und University of Southampton. Er gilt als Wegbereiter der Sprache HTML (Hyper-Text Markup Language) und Gründer des World Wide Web (1990). Auch für die erste Suchmaschine und das Betriebssystem (OS) NeXTSTEP gehört ihm die Urheberschaft.

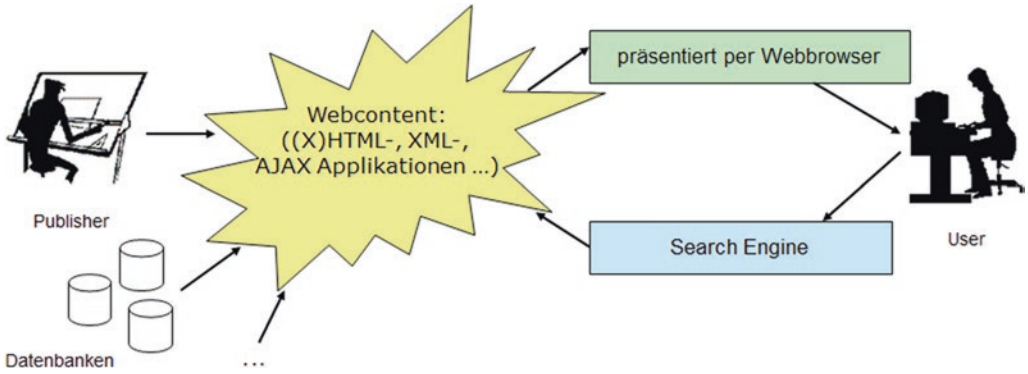


Abb. 19.2 Klassisches Szenario mit Webcontent [11, 16]

Die „Classical Web"-Applikationen und ihre Erweiterungen werden hauptsächlich zwecks Informationspräsentation in einer für Menschen lesbaren Form entwickelt und können nur beschränkt durch die Computerprogramme direkt weiter verarbeitet werden. Die Hypertext-Ressourcen werden durch Hyperlinks untereinander vernetzt. Diesbezüglich entstehen zwei Hauptprobleme (Abb. 19.2):

- Ein Suchprozess ist oft ineffizient und dessen Resultate sind häufig falsch oder nicht vollständig.
- Es gibt keine Möglichkeit einer simplen Automatisierung auf der Basis der im Web veröffentlichten Information

19.1.2 Suchmaschinen und Webcrawler

Webcrawler

Die so genannten „Spider" (Web Crawler) bauen einen Dokumentenbestand auf, indem er automatisch Dokumente aus dem WWW herunterlädt und deren Inhalte nach Referenzen auf weitere Dokumente durchsucht. Diesen Prozess („Crawling" genannt) setzt er mit den auf diese Weise gefundenen Dokumenten fort. Parallel dazu analysiert er den Inhalt der Dokumente und extrahiert ggfs. Metadaten und weitere Informationen. Das Crawling ist beendet, wenn keine neuen Referenzen gefunden wurden oder ein Abbruchkriterium erfüllt ist.

Die Aufgabe des Webcrawler liegt in [5, 14, 15, 16, 17]:

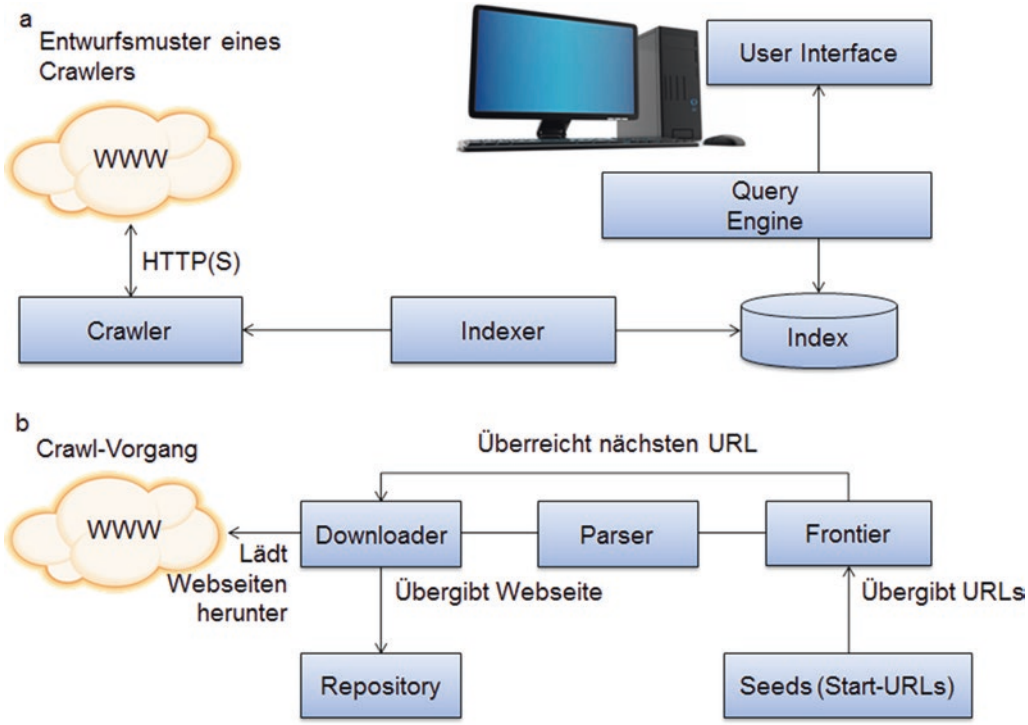
- Bestimmung von Schlüsselwörtern
- Auswertung so genannter Meta-Tags (semantische Seitenbeschreibungen), Eliminierung von Redundanz (z. B. Präpositionen, gleichartige Seiten)
- Gewichtung der Resultate, u. a. mit Kriterien wie Referenzierungshäufigkeit, Anfragehäufigkeit

- Aufbau und Komprimierung eines gewichteten Gesamtindex
- stark replizierte Speicherung zum Lastausgleich
- direkte Bedienung von Suchanfragen über diesen Index (Hash-Tabellen).

Ein solches Kriterium kann bspw. die Linktiefe bzw. die Anzahl der Crawling-Zyklen sein. Alternativ dazu ist auch ein dauerhaftes Crawling möglich, wodurch erreicht wird, dass der Dokumentenbestand immer aktuell gehalten wird. ◘ Abb. 19.3 präsentiert ein typisches Entwurfsmuster eines Crawlers nach R. Harbich (► http://www-e.uni-magdeburg.de/harbich/webcrawling/):

Der Frontier verwaltet noch nicht besuchte URLs. Vor dem Crawl-Vorgang wird ihr eine Menge von Start-URLs (auch Seeds genannt) hinzugefügt, von denen ausgehend die weiteren Dokumente gecrawlt werden. Der Frontier übergibt jede einzelne URL an den Downloader.

Der Downloader lädt den Inhalt des durch die übergebene URL bezeichneten Dokuments herunter und übergibt ihn



◘ **Abb. 19.3** Typischer Aufbau eines Crawlers nach R. Harbich (2008)

an das Repository und den Parser. Der Abruf des Dokuments erfolgt üblicherweise per HTTP(S)-Anfrage.

Der Betreiber einer Website kann dem Crawler Anweisungen erteilen, welche Seiten dieser nicht crawlen bzw. indexieren darf. Dies erfolgt über den Robots Exclusion Standard. Hierbei wird eine Datei mit dem Namen robots.txt im Wurzelverzeichnis der Website abgelegt. Diese enthält Regeln, die für bestimmte oder für alle Crawler gelten sollen. Es können einzelne Seiten oder ganze Verzeichnisse ausgeschlossen werden.

- **Suchmaschinen**

Die Suchmaschinen ermöglichen die Indexierung der Webseiten durch Webcrawler. Diese sind Suchprogramme, die ausgehend von populären Web-Seiten deren transitive Hülle bilden und die Inhalte durchsuchen. Jeweils mehrere hundert Millionen Indexierungsvorgänge existieren bei populären Suchmaschinen wie Google, Bing, Fireball, Lycos, Yahoo, Baidu.

19.1.3 Contentmanagment und Wikis. Web 2.0

Contentmanagment wird durch die Kollaborationswerkzeuge zum gemeinsamen Editieren von Dokumenten im WWW unterstützt. Diese sind oft leicht via Wiki-Server aufsetzbar.

Beispiel 19.1

Ein prominentestes Beispiel solcher Art ist die Wikipedia, die Online-Enzyklopädie. Deren Materialerstellung und Überarbeitung ist durch alle Benutzer möglich. Das System ist nichtkommerziell, lebt vom Engagement der Network Community. Umfangreiche Versionsverwaltung ist praktisch ohne „Edit Wars“ möglich ggf. erfolgt Rücksetzen auf frühere Versionen durch Administratoren bei Versuchen von Vandalismus mit dem evtl. Sperren von erwischten IP-Adressen. Die Auflösung von Meinungsverschiedenheiten wird über interaktive Diskussionsboards mit der Pflicht zur Einigung. 2003 kamen die ersten freiwilligen Beiträge und seit dieser Zeit weist die Wikipedia typischerweise sehr hohe Qualität und Aktualität der Informationen auf.

Der Einsatz von Wikis erspart den Aufwand bei der manuellen Administrierung vom Content erheblich und erhöht die Effizienz der Teamarbeit, auch bei steigender Autorenzahl im Vergleich zu CVS (Concurrent Versioning System, bspw. Git) und Groupware (Mehrbenutzereditoren), s. ◘ Abb. 19.4.

Web 2.0 ist ein gängiges Schlagwort zur Beschreibung neuer Anwendungsformen und Services, die durch Webbrowser zugänglich sind bspw. Wikis oder Weblogs. Diese Anwendungen

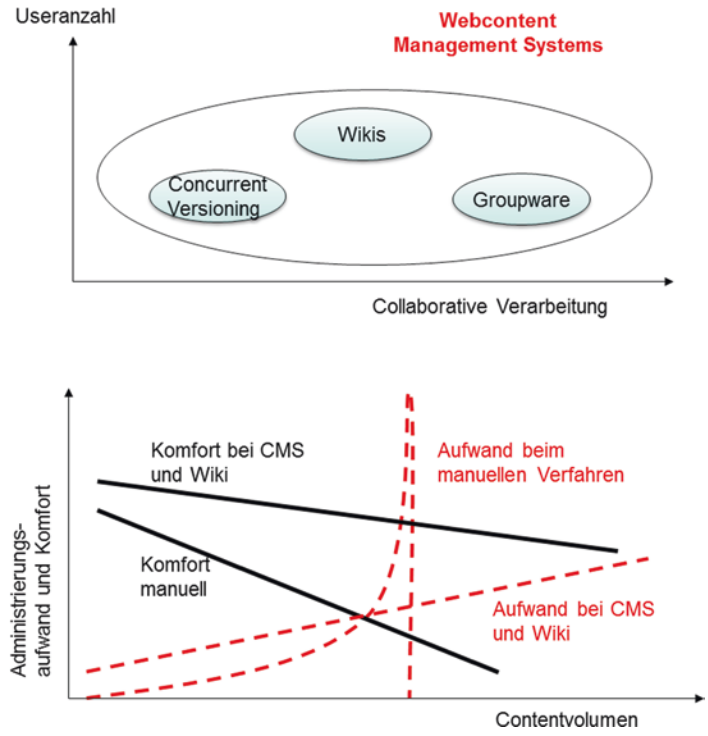


Abb. 19.4 Wikis im Vergleich zu den anderen Content Management Systemen

tragen generell eine hohe soziale Komponente, rufen GUIs auf und basieren auf den neuesten Interaktionsmodellen sowie Dokumentenrepräsentationen (XML, HTML5, CSS3, AJAX, Java,…). Die Autorenschaft des Begriffs gehört Tim O'Reilly (geb. 1954 in Cork), dem Gründer von O'Reilly Media Publishing sowie Anhänger der Freien Software und Open Source-Bewegung und Mitentwickler der Scriptsprache Perl.

Als Wegbereiter des Web 2.0 erklärte er 2005 den Begriff so: „Web 2.0 acts as a combination of classical web and other technical innovations like social networks and clouds":

$$\textbf{\textit{Web 2.0}} = \textbf{\textit{Klassisches Web}} + \textbf{\textit{soziale Netzwerke}} + \textbf{\textit{Clouds}} \tag{19.1}$$

19.1.4 Semantic Web und Web 3.0

Das semantische Web (Semantic Web) beinhaltet notwendige Architekturkomponenten zur Umwandlung eines komplexen Webcontents zur maschinen-bearbeitbaren Form mit Meta-informationen (Metategs). Diese erleichtern die standardisierte Suche mittels Webcrawlern (Abb. 19.5):

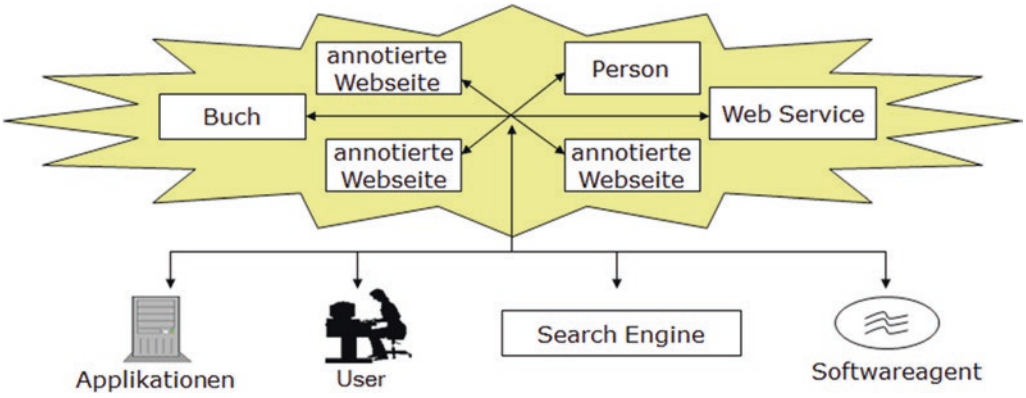


Abb. 19.5 Einfaches Szenario von Semantic Web [16]

Unter diesen Architekturkomponenten befinden sich die folgenden (Tab. 19.1):

Die Zusammenwirkung dieser Komponenten ist in Abb. 19.6 zu entnehmen:

Anschließend ist noch ein Beispiel angeführt:

Bespiel 19.2

Als Pendant zum Begriff „Web 2.0" wurde auch der Begriff „Web 3.0" durch J. Markoff (2008) eingeführt. Der Begriff addiert noch die Konzepte des Semantic Web dazu:

$$\textit{Web } \mathbf{3.0} = \textit{Web } \mathbf{2.0} + \textit{Semantic Web} \tag{19.2}$$

Tab. 19.1 Architekturkomponenten von Semantic Web [16]

Komponente	Abkürzungserläuterung	Begriffsbestimmung
XML	EXtensible Marup Language	Universelle Datenaustauschsprache
URIref	Uniform Resource Identifier Reference	Identifier für zahlreiche Ressourcen
RDF	Resource Description Framework	Standardisiertes Datenmodell zwecks Ressourcen- Beschreiben/Verlinken
RDF Schema, OWL	Web Ontology Language	Einige Mittel zur Definition verfügbarer Vokabulare und Restriktionen für das Datenmodell
SPARQL	SPARQL Protocol and RDF Query Language	Abfragemittel für die Webressourcen analog SQL (Resources Query)
Logische Reasoning		Kombination von Suchkriterien auf der Basis KI-Verfahren

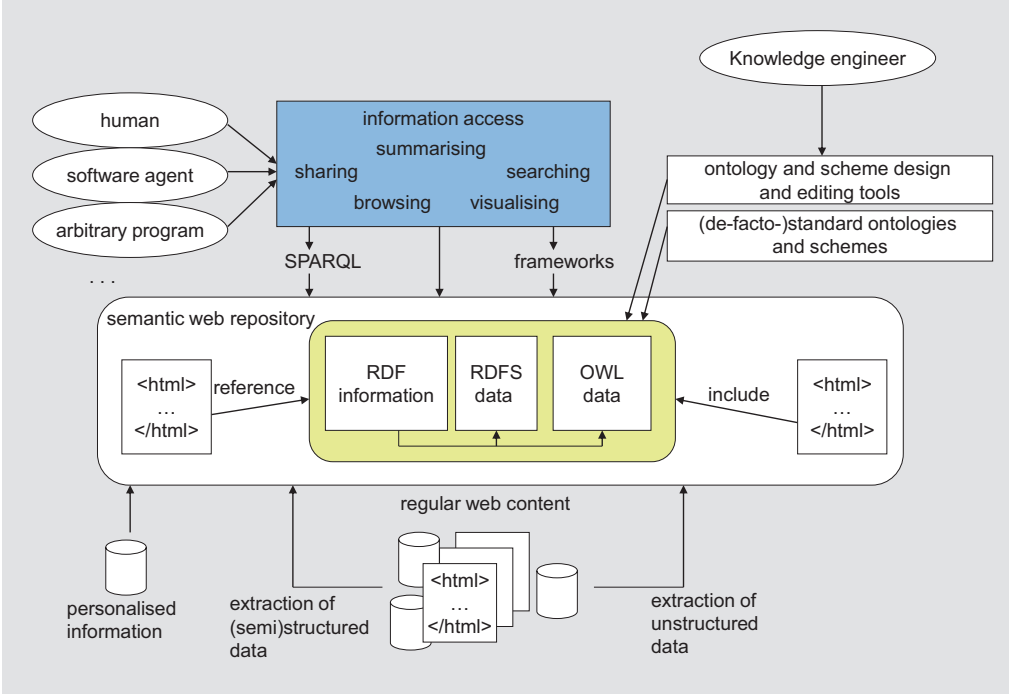


Abb. 19.6 Semantic Web [16]

19.2 Socket-basierte Anwendungen

Bei dem Socket-Konzept handelt es sich prinzipiell um eine Abstraktion von der tatsächlichen Netzwerkübertragung [17, 18]. Sockets bieten eine große Kontrolle über die Details der Kommunikation, bis hin zur Möglichkeit, beispielsweise IP-Pakete selbst zusammen zu setzen (so genannte Raw-Sockets). Ein Socket ist dabei vergleichbar mit einem File-Deskriptor, auf den mit normalen Lese- und Schreibaufrufen zugegriffen werden kann. Anstatt aber mit Dateien zu interagieren, verbirgt sich hinter einem Socket ein Kanal zu einem anderen Socket. Das zugrunde liegende Konzept ermöglicht, dass zwei miteinander verbundene Sockets sich in unterschiedlichen Prozessen und auch auf unterschiedlichen Rechnern befinden können. Die in einen Socket auf einem Rechner A geschriebenen Daten können dadurch aus einem Socket auf einem anderen Rechner B gelesen werden. Somit eignet sich das Konzept zur Interprozess- oder Netzwerkkommunikation.

Die konzeptionelle Anordnung eines Sockets innerhalb eines Kommunikationsvorgans zweier Instanzen ist in Abb. 19.7 dargestellt [16]:

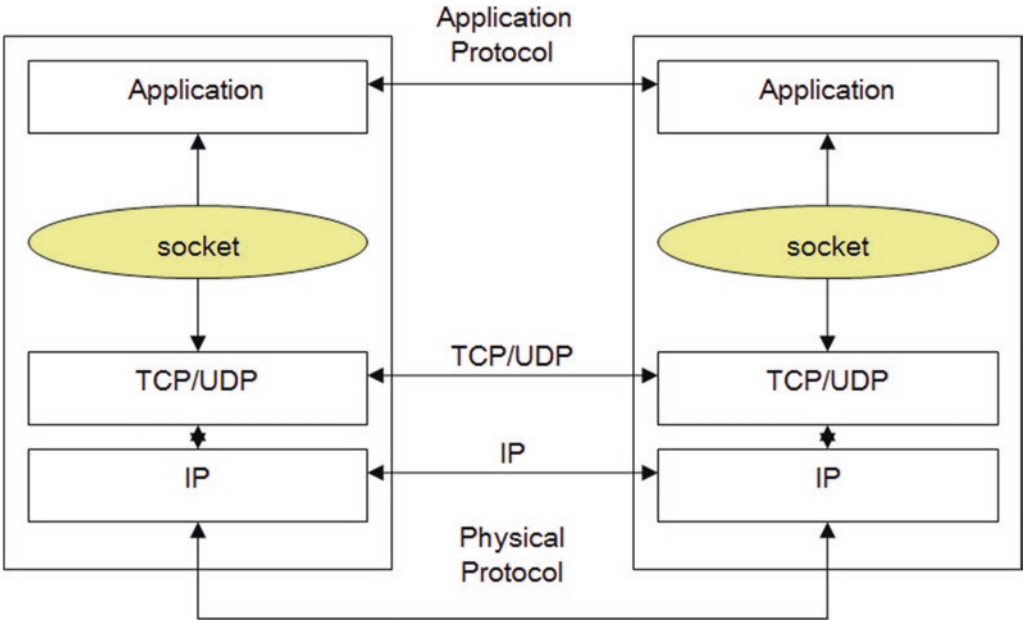


Abb. 19.7 Socket-Schnittstelle [16]

Wie in der Abbildung zu sehen ist, stellt ein Socket also nichts anderes dar als eine Schnittstelle zwischen der Applikation und dem gewählten Transportprotokoll (hier TCP oder UDP) über die Daten ausgetauscht werden können.

Die Vorteile einer Anwendung, die auf Basis dieses Konzeptes entwickelt werden, sind vor allem eine große Flexibilität und hohe Performance, wobei diesen Vorteilen ein hoher Aufwand bei der Entwicklung gegenübersteht.

19.2.1 Sockets: konzeptioneller Ablauf

Der Ablauf bei der Kommunikation lässt sich am einfachsten durch das open-close-read-write-Paradigma beschreiben. Dieses besagt, dass ein Socket zunächst „geöffnet“ werden muss und daraufhin in ihn geschrieben bzw. aus ihm gelesen werden kann. Nach Abschluss dieser Kommunikation wird der Socket wieder geschlossen. Der Begriff des Öffnens beschreibt dabei allerdings einen Vorgang, der abhängig vom verwendeten Transportprotokoll (UDP oder TCP) ist. Im Falle eines UDP-Sockets bedeutet das Öffnen lediglich, dass mithilfe eines Systemaufrufs ein Socket angelegt wird und dieser in der Folge für die Kommunikation verwendet werden kann. Da es sich bei UDP um ein verbindungsloses Protokoll handelt, muss bei jedem Sendevorgang die Adresse des Zielsystems angegeben werden [16, 18].

Im Falle eines Sockets, der auf TCP aufsetzt, gestaltet sich der Vorgang hingegen etwas aufwendiger. Bevor Daten über einen solchen Socket versendet werden können, muss dieser vom nicht verbundenen Zustand in den Zustand „verbunden" gebracht werden. Erst wenn eine Verbindung zwischen den Kommunikationspartnern besteht, ist der Socket für Lese- und Schreibzugriffe verfügbar. Für den Verbindungsaufbau werden alle relevanten Daten (IP-Adresse, Portnummer) in eine so genannte sockaddr_in-Struktur geschrieben und diese dann einer Funktion namens connect() übergeben. Bei den einzelnen Sendeschritten ist daraufhin die Angabe der Empfängeradresse nicht erforderlich, da das Betriebssystem die Zuordnung dieser Daten zum verbundenen Socket intern speichert.

19.2.2 Client-Server-Modell für Sockets

Einer Netzwerkanwendung auf Basis von Sockets liegt das klassische Client-/Server-Modell zugrunde. Es existiert somit eine klare Rollenverteilung zwischen einem Dienstanbieter, der auf eingehende Anfragen reagiert und einem Dienstnutzer, der eine Kommunikation initiiert. Dabei erfolgt die Vergabe der Rollen nicht für ganze Rechner bzw. Netzteilnehmer, sondern für Prozesse auf diesen Rechnern. Das bedeutet natürlich, dass nicht nur ein Host in einem Netzwerk über eine IP-Adresse adressierbar sein muss, sondern ein einzelner Prozess auf diesem Host. Diese Aufgabe erfüllen die beiden wichtigsten Transportprotokolle TCP und UDP mithilfe des Port-Konzepts. Die Protokollheader halten ein 16-Bit-Feld bereit, in das die Portnummer des anzusprechenden Prozesses eingetragen wird. Ein Prozess wird damit eindeutig durch die Angabe Host-Adresse:Port-Adresse identifiziert. Bei der Zuordnung der Port-Adresse zum Prozess muss zwischen Client- und Server-Prozess unterschieden werden. Der Server bindet meist mithilfe eines Systemaufrufs explizit eine Portnummer an sich selbst, bzw. genauer gesagt an den Socket, auf dem er auf eingehende Anfragen wartet, während einem Client-Prozess häufig eine solche Nummer vom Betriebssystem zugewiesen wird [16].

Ein Prozess kann prinzipiell sowohl die Rolle eines Servers, als auch eines Clients übernehmen. Denkbar ist zum Beispiel ein Szenario, bei dem ein Client im Rahmen einer Flugbuchung bei einem entsprechenden Server eine Anfrage stellt und dieser Server wiederum einen weiteren Server kontaktieren muss, um die Anfrage beantworten zu können. Die Benennung eines Servers und eines Clients bezieht sich daher immer auf eine Kommunikationsbeziehung und kann keine globale Gültigkeit haben.

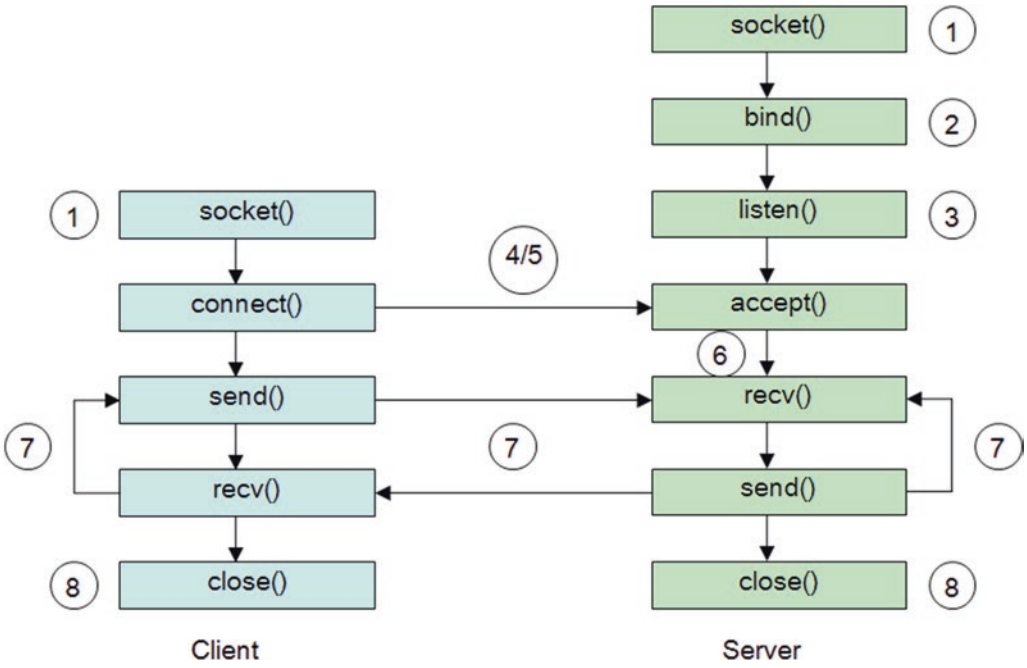
In der Praxis kommuniziert ein Server häufig gleichzeitig mit mehreren Clients, wie beispielsweise im Falle eines

hochfrequentierten Webservers, der in kürzester Zeit mehrere hunderte oder gar tausende Seitenanfragen erfüllen muss. Diese Möglichkeit wird durch parallele Prozesse oder Threads realisiert, worauf im Rahmen dieser Dokumentation allerdings nicht eingegangen werden soll.

19.2.3 Verbindungsorientierter Kommunikationsablauf

Für die Kommunikation über einen Socket müssen auf Client- und auf Serverseite unterschiedliche Vorarbeiten geleistet werden. Der Ablauf einer einfachen verbindungsorientierten Kommunikation ist in ◘ Abb. 19.8 dargestellt.

1. Sowohl der Client, als auch der Server fordern einen Socket an, der daraufhin als Schnittstelle zur Transportschicht dient. Das zu verwendende Transportprotokoll, hier TCP, muss angegeben werden.
2. Der Server bindet eine lokale Adresse (eine Portnummer) an den erstellten Socket. Über die Portnummer ist der Prozess in der Folge erreichbar.
3. Daraufhin wird durch den Aufruf von listen auf eingehende Verbindungsanträge gelauscht.



◘ **Abb. 19.8** Verbindungsorientierte Kommunikation

4. Der Client beantragt eine Verbindung durch Aufruf der Funktion connect. Dies bewirkt das Ende der Funktion listen beim Server.
5. Der Server akzeptiert den eingegangenen Verbindungsantrag durch den Aufruf von accept.
   Nun steht die Verbindung zwischen Client und Server. Dabei werden alle notwendigen Daten, wie IP-Adresse und Portnummer spezifiziert.
6. Auf Server-Seite wird eine eingehende Verbindung zunächst in eine Warteschlange eingehängt. Der vorherige Aufruf von accept bewirkt, dass diese Warteschlange abgearbeitet wird. Für jede eingegangene Anfrage wird dazu ein neuer, verbundener Socket erstellt. Damit ist zwischen den beiden Endpunkten ein Kommunikationskanal hergestellt.
7. Auf diesem Kanal können nun mithilfe entsprechender Systemaufrufe Daten geschrieben bzw. gelesen werden.
8. Nachdem alle Daten übertragen wurden müssen die Sockets geschlossen werden.

Das im 6. Schritt genannte automatische Anlegen eines neuen Sockets für jede eingegangene Verbindung mag ein wenig verwirren, könnte man doch den ursprünglich erstellten Socket für die eigentliche Kommunikation verwenden. Allerdings wird durch den dargestellten Ablauf eine sehr gute Aufgabenverteilung bewirkt. So kann der im 1. Schritt erzeugte Socket vom Serverprozess dazu verwendet werden, auf Verbindungen zu warten. Nach dem Herstellen einer Verbindung wird der neue Socket für die Zusammenarbeit mit dem Client verwendet. Der ursprüngliche Socket ist damit frei für weitere Verbindungsanträge. Dadurch ist die Grundlage für parallele Kommunikation geschaffen.

19.2.4 Verbindungsloser Kommunikationsablauf

Die einfachere der beiden hier diskutierten Interaktionsformen ist die verbindungslose Kommunikation mittels UDP. Ein typischer Ablauf ist in ◘ Abb. 19.9 dargestellt [16].

1. Client und Server fordern jeweils mit dem Systemaufruf einen Socket an. Dabei wird als Transportprotokoll UDP angeben.
2. Der Server bindet eine Portnummer an den erstellten Socket.
3. Durch den Aufruf von recvfrom blockiert der Server-Prozess und wartet auf eingehende Daten auf dem erstellten Socket.

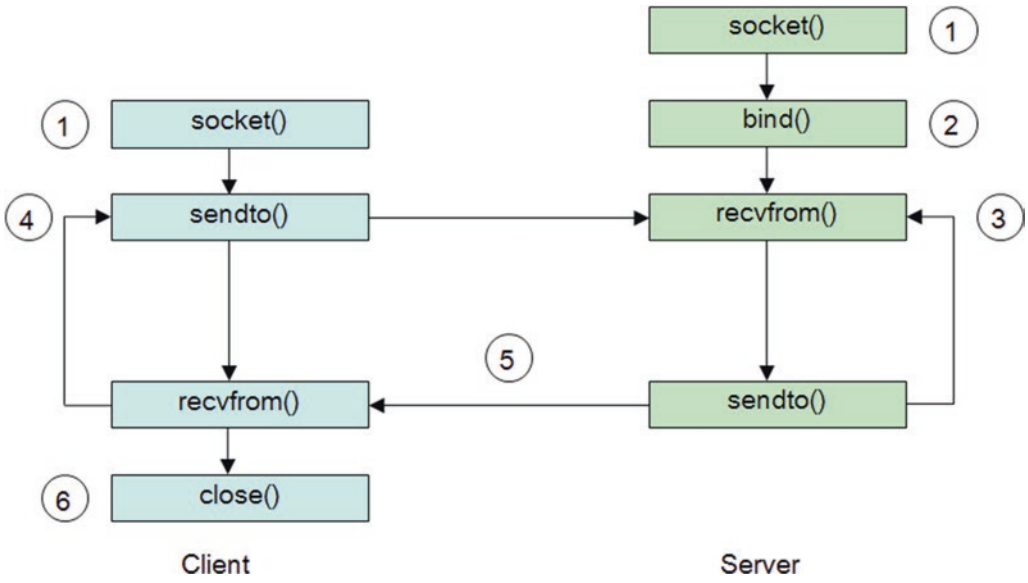


Abb. 19.9 Verbindungslose Kommunikation

4. Der Client versendet unter Angabe der Adressinformationen mithilfe von sendto Daten an den Server, die durch recvfrom von diesem entgegengenommen werden. Der Server antwortet auf gleiche Weise dem Client.
5. Der Socket auf Client-Seite wird nach abgeschlossener Kommunikation geschlossen.

19.2.5 Abgrenzung zur Middleware

Die Nutzung von Sockets zur Realisierung verteilter Anwendungen besitzt folgende Nachteile [16, 18]:

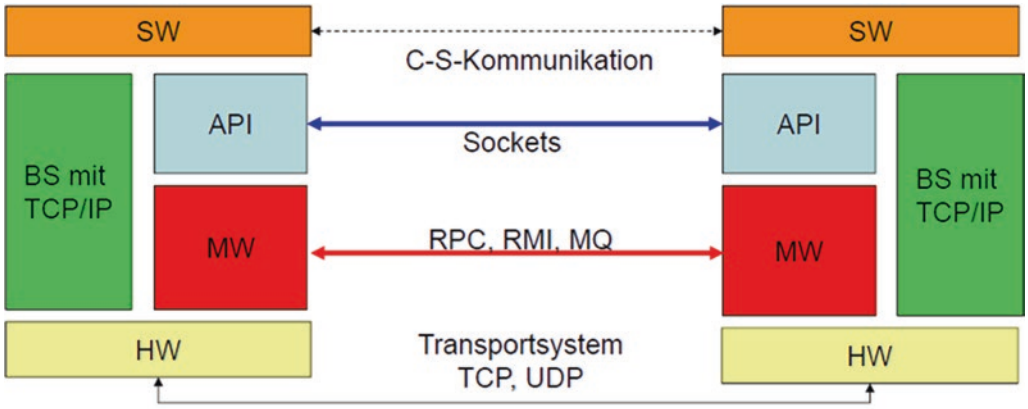
1. Da UDP unzuverlässig ist, müssen die obigen Programmstrukturen für den UDP-Server und -Client um Maßnahmen zur Erhöhung der Zuverlässigkeit (befristetes Warten auf eine Antwort, wiederholtes Senden des Auftrags usw.) erweitert werden.
2. Bei der Nutzung von TCP muss der Verbindungsauf- und -abbau jeweils explizit programmiert werden.
3. Da die Server von vielen Clients beauftragt werden, ist es ratsam, einen Server durch mehrere parallele Prozesse zu realisieren. Dies muss explizit programmiert werden.
4. Die übertragenen Daten müssen unter Umständen vor und/oder nach der Übertragung gewandelt werden, insbesondere bei der Übertragung von Binärdaten (Big-Endian- vs.

Little-Endian-Darstellung ganzer Zahlen, Länge von int-Zahlen: 2, 4 oder 8 Byte, Layout von Datenstrukturen usw.).

5. Beim modernen Software-Entwurf wird ein zu entwickelndes System in Module oder Objekte von Klassen aufgeteilt. Die Module interagieren über Prozedurfernaufrufe (RPC), die Objekte über Methodenfernaufrufe (RMI). Die Kommunikation über Sockets passt nicht zu diesem Paradigma [5, 16], die Socketkommunikation ist dabei transparent integriert.

19.3 Fernaufrufe: RPC und RMI. Middleware

Die Basiskommunikationsmechanismen in Verteilten Systemen sind die Fernaufrufe: RPC (Remote Procedure Call) und RMI (Remote Method Invocation). Diese sind mit den aktuellen programmatischen Paradigmen konform [10, 14, 15, 16]. Zusammen mit der MQI (Message Queuing Interfaces) für asynchronen Nachrichtenaustausch zählen diese Konzepte als Middleware (im Englischen „Zwischenanwendung"). Die MW (Middleware) wird zwischen Software und Hardware so angesiedelt [14, 18], dass die Komplexität der Applikationen und ihre Infrastruktur verborgen werden (◘ Abb. 19.10).



Legende:
BS – mit Unterstützung des TCP/IP-Protokollstack
API – Application Programming Interface
MW – Middleware
BS – Betriebssystem

◘ **Abb. 19.10** Was ist Middleware?

Beispiel 19.2

Die gängigen und hystorischen MW-Spezifikationen sind wie folgt [3, 4, 5, 7, 16]:

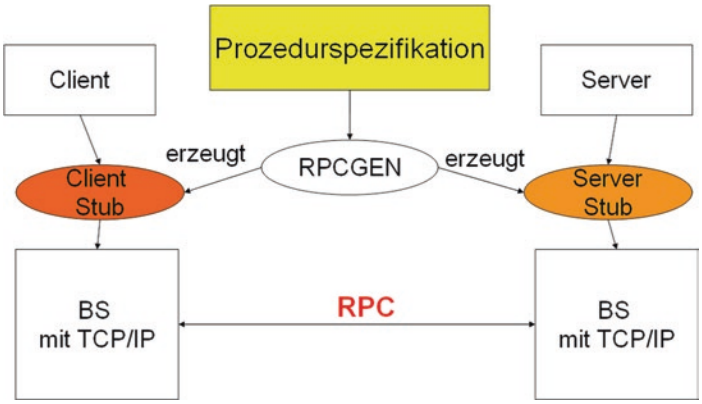
- CORBA (Common Object Brokering Interface, obsolete)
- EJB (Enterprise Java Beans, universell, geeignet für größere Systeme)
- MS.NET (proprietär und Microsoft-gebunden)
- OSGi (früher Open Services Gateway initiative, geeignet für Mobilumfeld und Embedded Systems)

Der Prozedurfernaufruf (Remote Procedure Call, RPC) ist ein Mechanismus, bei dem Anwendungsentwickler für die Kommunikation zwischen Prozessen auf unterschiedlichen Rechnern dasselbe Paradigma benutzen wie beim lokalen Prozeduraufruf. Der Programmierer muss dabei nur die Prozedurschnittstelle spezifizieren und die Anwendung programmieren; der Programmcode zur Kommunikation der Prozesse wird automatisch generiert.

Die wichtigsten RPCs sind [7, 15, 16]:

1. der von der Firma Sun Microsystems (derzeit Oracle) entwickelte Mechanismus
2. der RPC des DCE (Distributed Computing Environment), das von der OSF (Open Software Foundation) entwickelt wurde.

Da die Stubs C-Programmcode beinhalten, der zwischen der Anwendung und der Betriebssystem-Software angesiedelt ist, wird RPC als Middleware bezeichnet (◘ Abb. 19.11).



◘ **Abb. 19.11** Fernaufruf RPC als Middleware-Konzept (Client und Server in der Sprache C)

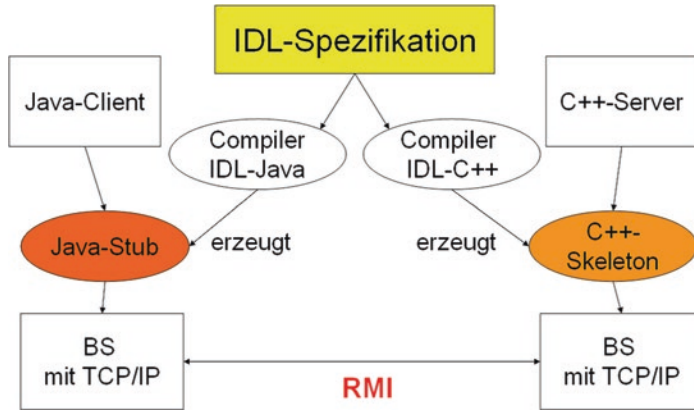


Abb. 19.12 Fernaufruf RMI als Middleware-Konzept (Client und Server in unterschiedlichen Sprachen)

Die Sockets spielen für die Fernaufrufe eine zusätzliche Hilfsrolle, wobei die codierten Schnittstelleninformationen mit dem Format für Ein- und Ausgabeparameter sowie mit dem Rückgabewert über die geöffneten Sockets übertragen werden (Marshalling- und Unmarshalling-Prozess genannt).

RMI (Remote Method Invocation) ist ein speziell für die Programmiersprache Java von der Firma Sun (seit 2009 Oracle) entwickeltes Middleware-Konzept. Aus einer IDL-Schnittstellenspezifikation (Interface Definition Language) können durch unterschiedliche IDL-Compiler Client-Stubs und Server-Skeletons in unterschiedlichen Programmiersprachen erzeugt werden (z. B. in C++, Java, C usw.). Im Beispiel wird der Client in der Sprache Java und der Server in C++ programmiert [7, 15, 16]. Entsprechend wird ein Java-Client-Stub und ein C++-Server-Skeleton aus der IDL-Spezifikation generiert. Der Java-Client kann somit auf verteilte Objekte, die in C++ implementiert sind, zugreifen (Abb. 19.12). Im Unterschied zu den Stubs ermöglicht Skeleton dynamische Anpassung der Interfaces zur Laufzeit.

Ein kurzer Vergleich von bekannten Middleware-Frameworks wird in Tab. 19.2. repräsentiert.

Tab. 19.2 Vergleich: OSGi vs. EJB vs. NET [7, 14, 16]

Merkmal	Middleware-Framework		
	OSGi	EJB	.NET
Implementierungs-sprachen	C++, Java	Java, JSP, Servlets	C, C++, C#, J#, ASP.NET, JS, VB
Entwicklungs-umgebung	Beliebig	Eclipse, Oracle NetBeans, JBuilder	MS Visual .NET mit Common Runtime Library – CLR
Einsatzbereich	Embedded-Bereich	Universell	Universell
Betriebssystem/Ver-fügbarkeit	Real-Time-BS, bspw. QNX	Alle wesentlichen	Microsoft
Preis/Lizenz	Kommerzielle, quelloffene	Kostenlose Basisdienste, allerdings spezielle Dienste per Lizenz	Kostenlose Basisdienste, allerdings spezielle Dienste per Lizenz
Abstraktionsniveau/ Granularität	Bundles als Dienste	Session Beans, Entities, Message Queuing Beans	Active-X, ADO.NET, weitere Komponenten bzw. Webservices
Eignung für komplexe Anwendungen	Einfach	Geeignet für sehr große verteilte Anwendungen	Geeignet für mittlere vert. Microsoft- Anwendungen

19.4 Asynchrone Nachrichtenübermittlung: MQI

Asynchrone Nachrichtenübermittlung wird mit dem Einsatz des MQI-Konzepts verwirklicht (Abb. 19.13). Das Ablegen und Herausnehmen von Nachrichten erfolgt im Rahmen einer Transaktion, wobei u. a. Nachrichten solange dauerhaft (persistent) gespeichert werden, bis sie entnommen werden. Es gibt kommerzielle und frei verfügbare Message-Queue-Systeme (die Message-Oriented-Middleware, MOM). Als eines der prominentesten Beispiele gilt IBM Websphere MQ (seit 1994, ehemals MQ Series):

- Die Anwendungen 1 und 2 können Informationen austauschen, ohne dass eine direkte Verbindung zwischen ihnen besteht (über Queue-Manager).

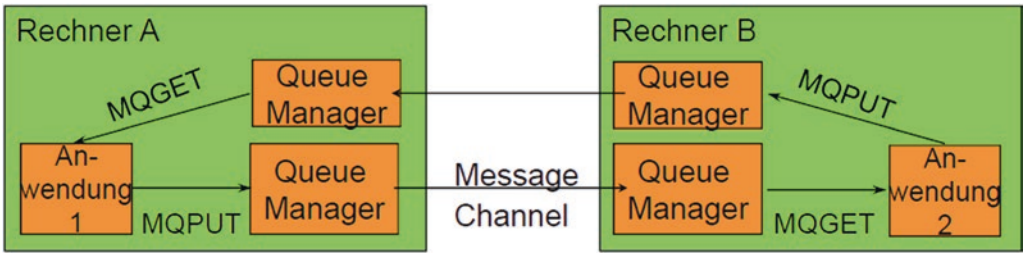


Abb. 19.13 Funktionsweise von MQI

- Die Kommunikation findet statt, indem die Programme ihre Nachrichten in Message-
  Queues ablegen und daraus entnehmen (Message Channel).
- MQI reiht Nachrichten in Queues (Warteschlangen) ein, von wo aus die Empfänger-
  Applikation sie asynchron abholen kann (i. d. R. FIFO).
- Entkopplung der Anwendungen durch Queue Manager: Nachrichtenweiterleitung auch
  bei nicht laufender Anwendung 1/2 möglich (geeignet für Mobile Computing).

Insgesamt unterstützt MQI die folgenden 12 Nachrichtentypen:

1. MQCONN – mit dem Queue-Manager verbinden
2. MQDISC – vom Queue-Manager trennen
3. MQOPEN – Message Queue öffnen
4. MQCLOSE – Message Queue schließen
5. MQGET – Lesen aus Message Queue
6. MQPUT – Schreiben in Message Queue
7. MQPUT1 – Öffnen, Schreiben & Schließen
8. MQBEGIN – Transaktion beginnen
9. MQBACK – Transaktion zurücknehmen
10. MQCMIT – Transaktion bestätigen
11. MQINQ – Attribute eines MQ-Objekts abfragen
12. MQSET – Attribute eines MQ-Objekts setzen.

MQI leistet den Austausch von Nachrichten zwischen heterogenen Anwendungen auf verschiedenen Plattformen bei der Unterstützung wesentlicher Betriebssystemen (Win, Linux, Mac OS, …). Aufgrund der Asynchronität ist die Schnittstelle insbesondere gut für das Mobile-Umfeld geeignet, wobei häufiges Handover/Abkoppeln/Wiederankoppeln möglich ist [16].

19.5 Weitere Techniken verteilter Anwendungen

Leistungsfähige Zusammenstellungen (Stacks) von freier Software zur Entwicklung verteilter Anwendungen sind u. a.:

1. LAMP = Linux + Apache + MySQL + PHP [/Perl/Python]
   Quelle: ► http://lamphowto.com/
2. WAMP = Windows + Apache + MySQL + PHP
   - Quelle: ► http://www.wampserver.com/
3. XAMPP = X(anyOS) + Apache + MySQL + PHP + Perl
   - Quelle: ► https://www.apachefriends.org/
4. MEAN = MongoDB + Express.js + Angular.js + Node.js
   - Quellen: ► http://meanjs.org/, ► http://mean.io/

- **MEAN-Konzept (seit 2009)**

MEAN vereinfacht und beschleunigt die Webentwicklung. Diese vier MEAN Stack Komponenten dienen zum Aufbau von fortgeschrittenen dynamischen Webseiten (alle JavaScript basiert):

- MongoDB, eine NonSQL-Datenbank (JSON-Format);
- Express.js, ein JavaScript-Framework für Webapplikationen;
- Angular.js, ein JavaScript MVC-Framework für Webapplikationen und Apps;
- Node.js, agile (asynchrone) Laufzeitplattform für skalierbare serverseitige Webapplikationen (CRUD, Steaming, Echtzeit etc.).

Akronym „CRUD" in den Anwendungen bzw. Webapplikationen bedeutet übliches Datenbankzugriffsparadigma: „Create, Read, Update, Delete".
Das Akronym umfasst die grundlegenden Operationen wie Create (Datensatz anlegen), Read (Datensatz lesen), Update (Datensatz aktualisieren), Delete (Datensatz löschen).

- **HTML5 (2014)**

HTML5 ist der Nachfolger von HTML 4 (1998) und XML als Kernsprachen. Die modifizierte Auszeichnungssprache ersetzt die Standards HTML 4.01, XHTML 1.0, DOM HTML Level 2 und bietet neue Funktionalitäten wie die Verwendung von Audio- und Videoquellen, Zugriff zum Filesystem, Verwaltung des lokalen Speichers und dynamischer 2D- und 3D-Grafiken. Ehemals wäre es nur mit zusätzlichen Plugins bspw. Adobe Flash möglich gewesen. HTML5 integriert die folgenden neuen Sprachelemente:

- Multimedia-Tags: <video>, <audio>, <canvas>.
- semantische Tags: <section>, <article>, <header>, <nav>.
- SVG-Bilder und mathematische Formeln.
- diverse APIs, DOM (XML Document Object Model)
- Canvas 2D API Specification: wie „Leinwand", gesteuert per JavaScript, CAPTCHA-Erkennung
- Web File System API, File API, Typed Arrays, Touch Events, Geo Location.
- Inter-operabilität mit Node.js, MVC JavaScript, JQuery etc.

19.6 Mobile Apps

Für viele Aufgaben ist es heutzutage einfacher und schneller ein Smartphone oder Tablet, als einen Computer oder Laptop zu verwenden. Mobile Applikationen (Apps) sind deshalb ein wichtiger Begleiter im Smartphone-Zeitalter. Nahezu für jede Lebenslage und jeden Sachverhalt gibt es heutzutage eine App.

Mobile Betriebssysteme und Apps kombinieren die typischen Features für den PC mit den neuen Feature für mobile Nutzung von diversen Netzwerken und Sensoren (im Sinne NW-Adaptern): Zellularnetze 3G-4G, Bluetooth, WLAN, GPS -Mobilenavigation, Touchscreen, Fotokamera, Videokamera, Spracherkennung und -Aufzeichnung (Speech Recognition, Voice Recorder), Musikplayer, Near Field Communication, Infrarotblaster.

Hersteller und viele Firmen ziehen es vor, ihre Apps nur für die am meisten genutzten Betriebssysteme – Google Android, Apple iOS, Windows – zur Verfügung zu stellen.

Die Unterschiede der Eigenschaften von Apps zu Desktop-Anwendungen und von spezialisierten mobilen Apps:

- Einsatz proprietärer JVM (wie Dalvik JVM), teilweise Intransparenz von Java Bytecode
- Sandboxing und abgeschottete Ausführung verhindert die Ausführung von Malware.
- Responsives Webdesign (RWD). Eine Webseite ist responsiv, wenn sie ihre Darstellung unterschiedlichen Geräten anpassen kann. Allerdings gehört mehr dazu, als ein paar Änderungen am CSS vorzunehmen. Themen wie „Mobile first" sind in aller Munde und bei Weitem nicht nur eine technische Herausforderung (Barrierefreiheit).

Durch den eingeschränkten Platz (in der Regel bietet ein Smartphone nur etwa 20 % der verfügbaren Fläche eines Desktops), sind die Designer gezwungen, sich auf das Wichtigste zu konzentrieren. Auch auf den kleinsten Geräten sollen die Kerninformationen der Webseite zur Verfügung stehen und vor allem einfach zu finden sein.

Trotzdem wird die Sparsamkeit in der Ressourcennutzung (Speichergröße, Bildschirmauflösung) eher zweitrangig, da es eine rasante Entwicklung der Leistungsfähigkeit der Hardware für Smartphones und Tablets gibt.

Neben den funktionalen Anforderungen zu den Apps müssen auch die nicht funktionalen Anforderungen erfüllt werden. Dazu gehören die Qualität, die Benutzerfreundlichkeit und die technische Umsetzung der Apps, u. a. die Verfügbarkeit unter diversen Betriebssystemen wie Google Android, Apple iOS und Microsoft Windows.

Die Verteilung von mobilen Apps wird durch die s. g. App Stores in den gängigen Betriebssystemen realisiert [7]. Es werden zwischen drei Typen mobiler Apps unterschieden: Webapps, native Apps und hybride Apps (◘ Abb. 19.14).

▪ Native Apps

Native Apps sind die typischen Apps, die die Nutzer aus dem App Store herunterladen und auf ihren Geräten installieren können. Sie werden in verschiedenen Programmiersprachen geschrieben, bspw. die bevorzugten Programmiersprachen für die größten Systeme sind:

- Java für Google Android
- Objective-C und Swift für Apple iOS
- C#, C und C++ für Microsoft Windows.

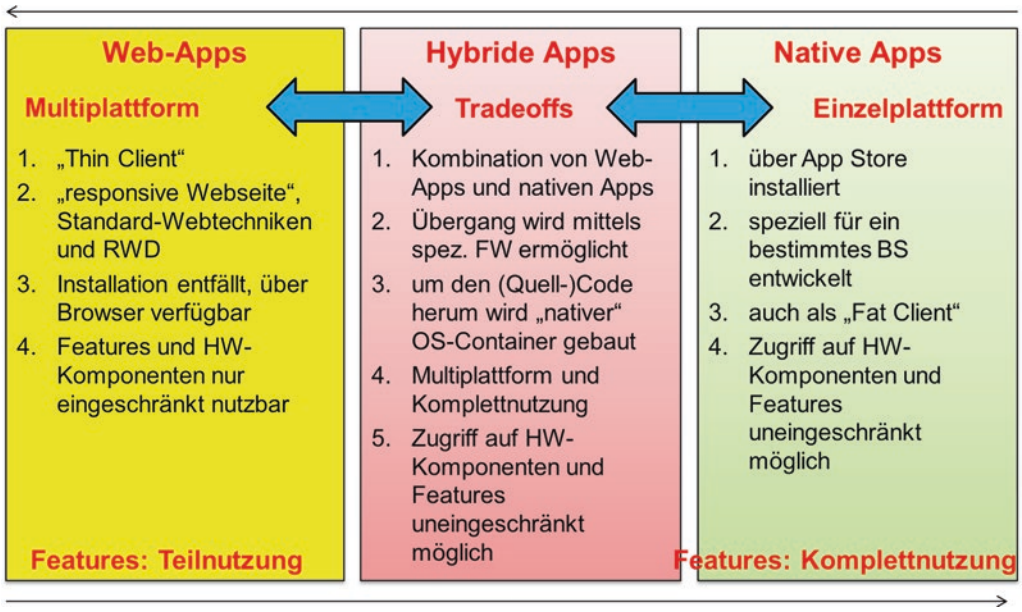


Abb. 19.14 Übergang zwischen drei Typen mobiler Apps [11]

Somit muss der Entwickler für jedes Betriebssystem eine andere Programmiersprache beherrschen. Aufgrund der verschiedenen Programmiersprachen können native Apps meistens nur auf Smartphones und Tablets mit dem Zielbetriebssystem installiert werden. Ein großer Vorteil nativer Apps ist die Möglichkeit auf Hardwarekomponenten des Smartphones zuzugreifen, bspw. der Kamera. Außerdem können native Apps in den Stores angeboten werden. Doch dafür muss meist für den Store, in dem die App erscheinen soll, eine Entwicklergebühr bezahlt werden. Bei der Entwicklung für iOS kommt noch der Überprüfungsprozess von Apple hinzu, der die Veröffentlichung der App ausbremst.

Das muss der Entwickler akzeptieren. Der Überprüfungsprozess gilt auch für Updates der Apps.

Mit nativen Apps können die verschiedensten Typen von Geräten auf einmal bedient werden, wenn alle auf einer Plattform basieren.

- **Web-Apps**

Web-Apps sind eigentlich Webseiten im Responsive Webdesign (RWD). Sie sind optisch genau auf mobile Zugangsgeräte angepasst und werden über eine URL im Browser aufgerufen und nicht auf dem Smartphone oder Tablet direkt installiert. Sie können somit auf jedem Gerät und mit jedem mobilen Betriebssystem genutzt werden. Zur Umsetzung einer Web-App

muss keine neue Programmiersprache gelernt oder spezielle Hardware (bspw. Mac) gekauft werden.

RWD benutzt die Web-Standards wie HTML5, CSS und JavaScript, damit sie auf beliebigen Endgeräten betrieben werden können. Im Gegensatz zu mobilen Apps, die für jede Plattform neu implementiert werden müssen, kann eine Implementierung von Web-Apps auf vielen verschiedenen Plattformen genutzt werden.

- **Hybride Apps**

Die dritte Art von Apps sind hybride Apps. Dabei werden native App und Web-App kombiniert. Es wird zuerst eine Web-App mit HTML, CSS und JavaScript erstellt. Diese wird dann von einem Container umgeben, der die App ähnlich wie ein Browser lädt. Mit diesem Container, der als nativer Wrapper bezeichnet wird, kann auch auf die Hardwarekomponenten des Smartphones zugegriffen werden. Hybride Apps können – nach dem Bezahlen der Entwicklergebühr und dem Überprüfungsprozess von Apple – in allen Stores zum Download angeboten werden.

Die speziellen Frameworks laden die Bibliotheken, die die Kommunikation zwischen JavaScript und der jeweiligen betriebssystemspezifischen Sprache herstellen. Dadurch können Hybrid-Apps auf diverse Hard- und Software-Komponenten des mobilen Endgerätes zugreifen. Ein Zugriff ist unter anderem auf Kontakte, Kamera, Bewegungssensor, GPS und Dateien möglich. Moderne Render-Engines erhöhen die Berechnungsgeschwindigkeit der Interpretation des HTML5-, CSS3- und JavaScript-Codes. Dadurch kann die Ausführungsgeschwindigkeit um ein Vielfaches erhöht werden.

Ein Vergleich zwischen Web-Apps, hybirden und nativen Apps ist in ◘ Abb. 19.15 aufgeführt.

Angesichts des wachsenden Dschungels unterschiedlicher mobiler Plattformen wird es immer wichtiger, Code zu schreiben, der sich in allen Welten nutzen lässt.

Zusammenfassend sind die Architektur und die wichtigsten Komponenten eines Frameworks für mobile Apps in ◘ Abb. 19.16 dargestellt. Die Arbeit mit HTML5, CSS3, JavaScript, den Komponenten des Betriebssystems, den Sensoren und Medien, den verfügbaren Plugins wird durch die Rendering Engine gewährleistet. Das Framework

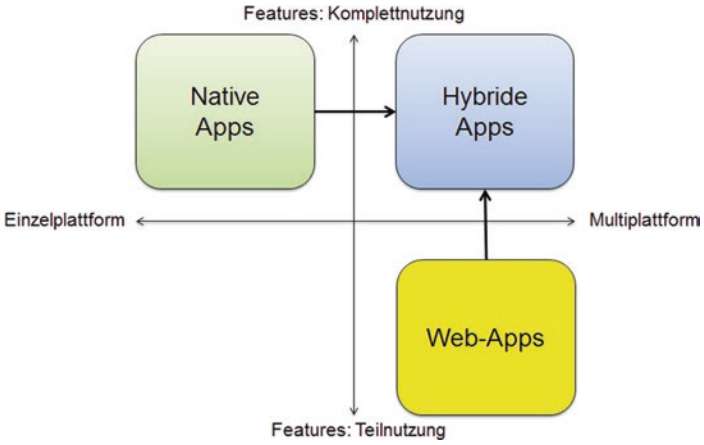


Abb. 19.15 Vergleich zwischen drei Typen mobiler Apps [7]

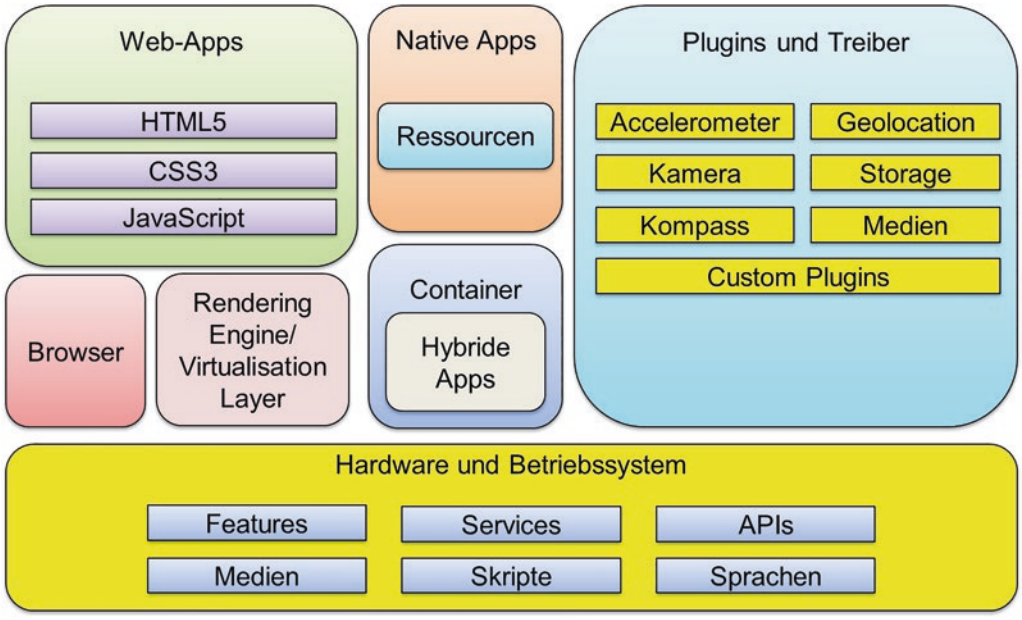


Abb. 19.16 Architektur eines Frameworks für mobile Apps [7]

dient zum Übergang zwischen Typen der Apps sowie für die Cross-Plattform-Entwicklung.

Die vergleichende Tabelle für die wichtigsten Tools und Frameworks zur Entwicklung von moblen Apps ist im Weiteren aufgeführt (Tab. 19.3):

Tab. 19.3 Vergleichende Tabelle für die wichtigsten Tools und Frameworks zur Entwicklung von moblen Apps

Tools und Frameworks	Cordova/ PhoneGap	Appcelerator Titanium	Intel XDK	Trigger.io	Ionic Lab
Einsatz und Anwendungs-virtualisierung	Webapps zu hybriden Apps	Cross-Plattform-Entwicklung, analog hybride, MBaaS (mobile backend as a service)	Cross-Plattform-Entwicklung, Überführung zu den native Apps	Hybride Apps, Überführung zu den native Apps	Open-Source-Webframework für Hybride Apps, Progressive Web Apps mit HTML5, CSS, JavaScript und AngularJS
Features zum Zugriff auf die Hardware-komponenten und Sensoren	Vorhanden für: – Beschleunigungssensor – Kamera – Kompass – Geolocation				
Verfügbarkeit	iOS, Android, Blackberry, Windows, webOS, Symbian	iOS, Android, BlackBerry, Windows	iOS, Android, Windows etc.	iOS, Android, Windows etc.	Interoperabel für iOS, Android, Windows 10 sowie Desktop Apps (Windows)
Zugriff auf die Komponenten von Betriebs-systemen	Vorhanden: – Netzwerke: WLAN, HSDPA, LTE, … – Speicher – Kontakte – Dateien und Filesystem – Medien (JPEG, MP3, MPEG2, …) – asynchr. Benachrichtigungen (Alarm, Ton, Vibration)				
Angebot der App im Store	Ermöglicht				
Sprachen für Auszeichnung und Programmierung	XML, HTML5, CSS, JavaScript, C, C++, Java, C#, Python, MEAN				
Dokumentationen und Communities	Dokumentation und Videotutorials vorhanden				

19.7 Zwischenfragen/Übungsaufgaben

19.7.1 Netzwerkanwendungen und mobile Apps

a) Worin unterscheiden sich native Apps, Web-Apps und hybride Apps?

Zwei Filialen eines Unternehmens sind über DSL-Internetlinks verbunden.

Eine Videoübertragung wird mit der Bildqualität von
V = 1000 * 1000 Punkten,
FT = 16-Bit-Farbkodierung und der Bildfrequenz
fps = 25 Bild/s vorgenommen.
Ist die Datenkompression für diesen Fall sinnvoll?
Berechnen Sie die erforderliche Datenrate für unkomprimierte Übertragung.

Moderne Verfahren/Codecs (wie bspw. ZIP, JPEG, MPEG etc.) ermöglichen eine Leistungsverbesserung/Ersparnis für die Datenrate durch die Kompression.

Bei welcher Mindestkompressionsrate KR (d. h. 1: KR) ist diese Übertragung bei einer verfügbaren Datenrate von DRv = 20 MBit/s möglich? (ggf. aufrunden!).

19.7.2 Sockets und Fernaufrufe

a) Erläutern Sie die Unterschiede zwischen Datagrammsockets und Streamsockets!
Erläutern Sie die Aufgaben der Socketprozeduren socket(), bind(), accept() und listen().
Wie unterscheiden sich jeweils die folgenden Paare der Socketprozeduren
   - sendto()/recvfrom(),
   - send()/recv()?

   Diskutieren Sie die Nachteile für die Programmierung unter Nutzung der Socketschnittstelle.
b) Die klassische Technologie zur Realisierung von Netzwerkanwendungen nennt sich „Prozedurfernaufruf“. Dieser besitzt wesentliche Unterschiede zu einem lokalen Aufruf (von-Neumann-Rechner).
Erläutern Sie den Ablauf eines RPC in Stichworten.
c) Nennen Sie drei Unterschiede des RPC zur RMI?
d) Nennen Sie je einen Einsatzfall für die Verwendung der Konzepte Socket, RPC und RMI?

19.7.3 WWW

a) Welche Aufgaben verrichtet ein WWW-Browser?
Beschreiben Sie den Vorgang, der nach einem Anklicken eines Links in einem WWW-Dokument abläuft!
b) Erklären Sie die Funktionsweise von Webservices und deren drei wichtigsten Aufbauprinzipien!
c) Beschreiben Sie die Funktionalitäten einer Suchmaschine und eines Webcrawler!
d) Erklären Sie die Unterschiede zwischen den Begriffen „Classical Web“ – „Web 2.0“ – „Web 3.0“?
Ist Web 3.0 heutzutage Ihrer Meinung nach schon komplett ausgebaut?
Welche Voraussetzungen braucht man dafür?

Verteilte Systeme und Cloud Computing

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_20

Verteilte Systeme werden vor allem für folgende Zwecke eingesetzt:

- gemeinsame Nutzung von Daten (z. B. verteilte Dateisysteme und World Wide Web), auch zur Erreichung von Fehlertoleranz durch Redundanz (z. B. Replikation von Daten einer Datenbank),
- gemeinsame Nutzung von Geräten (z. B. Drucker und Scanner)
- gemeinsame Nutzung von Rechenleistung (z. B. Zugriff auf Hochleistungsrechner),
- Kommunikation der Benutzer eines verteilten Systems (z. B. elektronische Post, gemeinsamer Terminkalender einer Arbeitsgruppe, Mehrbenutzeranwendungen wie Mehrbenutzertexteditoren oder Mehrbenutzergrafikeditoren, IP-Telefonie, Audio-Video-Konferenzen).

VS im Hintergrund

Neben solchen, für die Endanwender sichtbaren verteilten Anwendungen gibt es auch solche, die von anderen Komponenten intern benutzt werden und den Endanwendern verborgen bleiben wie bspw. Anwendungen zur Berechnung von Wegewahltabellen (OSPF, RIP, BGP usw.) und für Namensdienste (DNS), Konfigurationsdienste (DHCP) und Netzmanagement-Dienste (SNMP).

20.1 Verteilte Systeme: Transparenz, Architekturen und Leistungsoptimierung

20.1.1 Transparenzprinzip

Da die Nutzung verteilter Systeme i. d. R. komplizierter ist als die Nutzung eines einzelnen Programms, wurden auf unterschiedlichen Ebenen (Programmierebene, Benutzerebene usw.) Mechanismen eingeführt, die den Aspekt der Verteilung verbergen. Ein verteiltes System erscheint wie ein zentrales System. Man spricht von Verteilungstransparenz [15]. Sie bemerken allenfalls eine Leistungsveränderung. Folgende Arten der Verteilungstransparenz lassen sich unterscheiden (◘ Tab. 20.1):

20.1.2 Kommunikationsarten in Verteilten Systemen

Verteilte Systeme unterteilen sich nach der Art der Kommunikation:

1. **Client-Server-Kommunikation**
   - Kommunikation über Sockets (Transport: TCP/UDP)

Tab. 20.1 Die Arten der Verteilungstransparenz

Nr.	Art	Erklärung
1.	Zugriffstransparenz	Der Zugriff auf lokale und ferne Ressourcen erfolgt in derselben Weise
2.	Ortstransparenz	Der Zugriff auf Ressourcen ist ohne Kenntnis des Orts, an dem sich die Ressourcen befinden, durchführbar
3.	Namenstransparenz	Der Name einer Ressource ist für alle Rechner des verteilten Systems gleich
4.	Skalierungstransparenz	Die Erweiterung des Systems um weitere Rechner ist möglich, ohne dass die Gesamtstruktur oder die Anwendungsprogramme geändert werden müssen
5.	Replikationstransparenz	Falls das verteilte System zur Erhöhung der Verfügbarkeit und Fehlertoleranz mehrere Kopien von einer Ressource hält, so bleibt dies den Anwendungsprogrammen bzw. Usern verborgen
6.	Nebenläufigkeitstransparenz	Mehrere Anwendungsprogramme bzw. User können nebenläufig auf dieselben Ressourcen zugreifen, ohne dass es dabei zu Problemen kommt
7.	Ausführungs- bzw. Migrationstransparenz	Es ist für die Anwendungsprogramme bzw. User nicht erkennbar, auf welchem Rechner ein angeforderter Dienst ausgeführt wird. Es ist sogar möglich, dass ein laufendes Anwendungsprogramm während der Ausführung eines Dienstes auf einen anderen Rechner bewegt wird (Migration)
8.	Leistungstransparenz	Bei sich ändernden Belastungen kann das System umkonfiguriert werden, um die Leistung zu verbessern, ohne dass die Anwendungsprogramme bzw. User dies bemerken
9.	Ausfalltransparenz	Der Ausfall von Software- oder Hardwarekomponenten bleibt Anwendungsprogrammen bzw. Usern weitgehend verborgen

- Prozedurenfernaufruf (RPC, Remote Procedure Call)
- Methodenfernaufruf (RMI, Remote Method Invocation, und CORBA, Common Object Request Broker Architecture)
- Asynchrone Kommunikation (MQ, Message Queuing)

2. **Peer-to-Peer-Kommunikation (gleichberechtigte Partner, P2P)**
   - Peer – „Partner, kein Diener“
   - Dies sind hauptsächlich die Verteilten Systeme zur Realisierung von Tauschbörsen für Dateien (File-Sharing wie z. B. Napster, KaZaa usw.), mit denen vorwiegend Musik- und Videodateien (MP3, AVI, MPEG usw. nicht selten illegal) getauscht werden.

Vollkommen legale kombinierten P2P-Anwendungen sind, u. a.:
BOINC Grid, Conferencing-System Skype.

20.1.3 Skalierbarkeit und Verteilungsprinzipien

Alle verteilten Systeme basieren auf einem fundamentalen Konzept. Die Skalierbarkeit eines vert. Systems beschreibt dessen Laufzeitverhalten bei einer Änderung verschiedener Problemgrößen.

Die Skalierbarkeit der VS kann in den folgenden drei Dimensionen gemessen werden. Die ersten beiden sind für das heutige Cloud-Computing besonders relevant [9]:

1. Das System kann in Hinblick auf seiner Größe skalierbar sein. in diesem Fall kann dem System einfach weitere Ressourcen hinzugefügt werden, ohne dass die Leistung signifikant einbricht.
2. Das System kann unter dem Gesichtspunkt der geografischen Verteilung der Ressourcen skaliert werden. Dies bedeutet, dass die einzelnen Ressourcen weit verteilt auseinander liegen, ohne dass die Leistung des Systems stark beeinträchtigt wird.
3. Das System kann aufgrund seiner Verwaltung skalierbar sein. Ein administrativ skalierbares System erstreckt sich über viele unabhängige Organisationen, ohne dass die Komplexität der Verwaltung überproportional zunimmt.

Beispiel 20.1

Zum Thema der Größenskalierung wird in der vertikalen sowie in der horizontalen Skalierbarkeit unterschieden.

Vertikale Skalierung (Verteilung)

Im ersten Fall wird die Anzahl der Ressourcen pro Knoten variabel angepasst. Ein Beispiel für die vertikale Skalierung ist die Ersetzung eines normalen PC durch einen leistungsfähigen Cluster mit mehreren hochperformanten CPUs und mit der Summe von Arbeitsspeichern.

Horizontale Skalierung (Verteilung)

Im anderen Fall, der horizontalen Skalierung, wird das System erweitert, indem mehr Knoten hinzugefügt werden: n-tier-Anwendung. Man verteilt die Laufzeit auf mehr Schultern. Generell klassifiziert man ein skalierbares System, wenn es proportional von vertikaler oder horizontaler Skalierung profitiert. Die nachfolgenden Abbildungen sollen das Prinzip im Detail veranschaulichen [6].

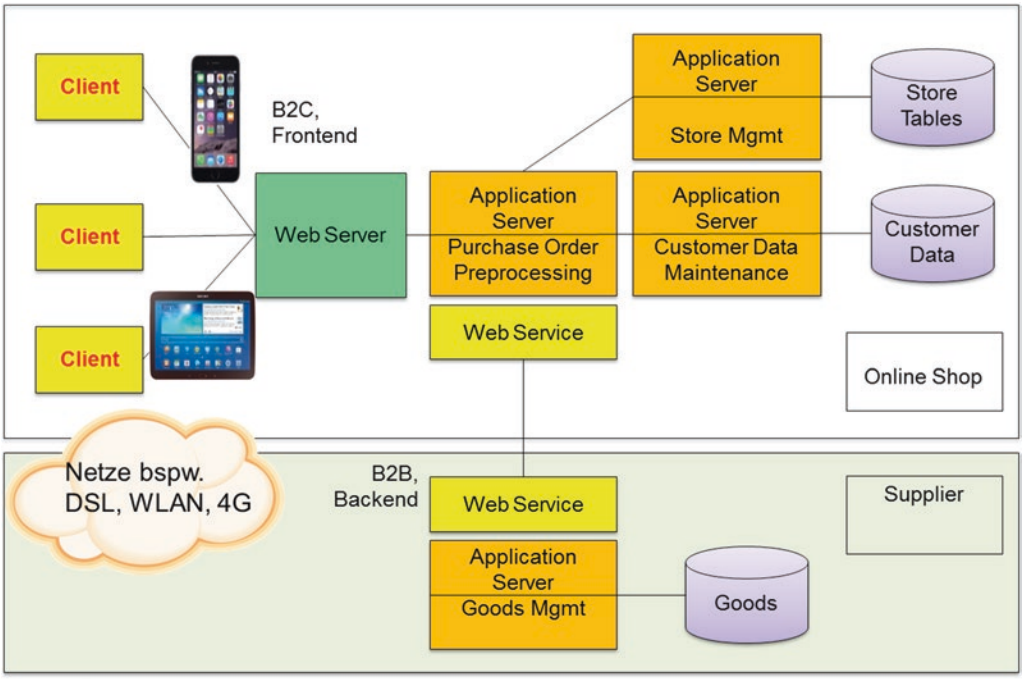
20.1.4 Wandel in Architekturen von Verteilten Systemen: Clustering und Clouds

Im C-S-Modell kommuniziert der Client mit dem Serverteil durch einen Nachrichtenaustausch zwecks der Verrichtung einer gemeinsamen Kooperationsaufgabe. Dabei wird eine längere

Kette von Schichten im n-tier-Modell bei mehreren vorhandenen Servern und deren Verbindungen aufgebaut. Lassen wir uns ein Beispiel anführen.

Beispiel 20.2

Eine verteilte Anwendung für E-Commerce hat öfters eine komplexere hierarchische Struktur (n-tier), welche zu den Zwecken der Performanceoptimierung verwendet wird. Ein Beispiel eines E-Commerce-Systems ist in ◘ Abb. 20.1 repräsentiert.
Die Anwendung 1 für einen Käufer (Client) interagiert mit dem virtuellen Shop, der Anwendung 2 für den Online-Shop. Die Anwendung 1 kommuniziert über einen Webserver mit dem beigefügten Applikationsserver. Der Applikationsserver stellt die Funktionalitäten zur Datenvorverarbeitung für die Kaufaufträge (Bestellung) zur Verfügung. Der Anwendungsserver für die Vorverarbeitung wird mit den nächsten zwei Applikationsservern verbunden. Einer von ihnen ist zur Lagerwartung, der andere für die Verwaltung von Kundendaten ausgerichtet. Die Anwendung 3 unterstützt die Kommunikation des Online-Shops mit den Lieferanten über einen eigenen Kommunikationskanal, der zu einem Anwendungsserver verbunden ist und zur Lieferantendatenbank. Die Kommunikation zwischen den Anwendungen 2



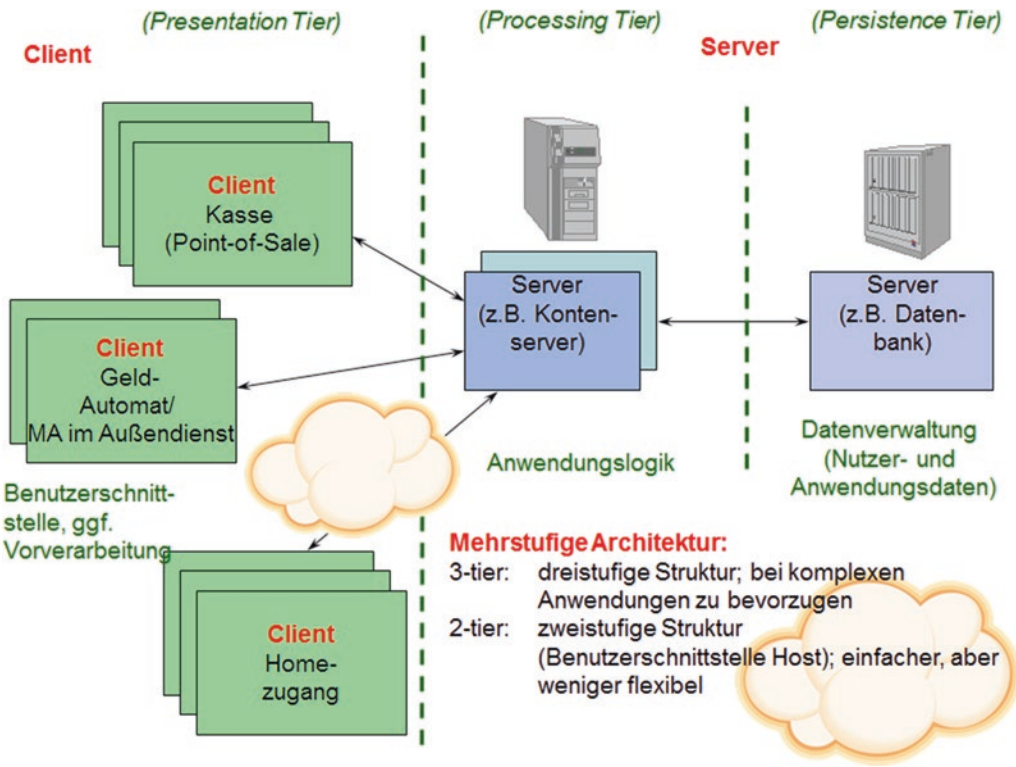
◘ **Abb. 20.1** Ein Beispielsystem für E-Commerce [16]

und 3, d. h. zwischen dem Online-Shop und dem Lieferanten wird unter Verwendung von Webservices durchgeführt.

Heutzutage sind solche Mehrschichtenarchitecturen stark in Verteilten Systemen verbreitet [4, 6]:

- 3-tier: diese Struktur ist ziemlich komplex und besitzt eine bessere Skalierbarkeit, d. h. sie ist für komplexere Applikationen zu bevorzugen;
- 2-tier: diese Struktur (bloße GUI und bloßer Host) ist einfacher, aber weniger flexibel (◘ Abb. 20.2).

Die Weiterentwicklung der typischen Anwendungsarchitekturen tendiert in verteilten Systemen mit herkömmlichen Client-Server- und n-Tier-Architekturen in Richtung von Clustering und Cloud Computing [154, 129, 153]. Der Serverteil wird durch leistungsfähige Cluster oder Clouds verstärkt und mehrfach repliziert. Effizienter Zugriff zu den gekapselten Services in den Cluster und Clouds erfolgt unter Nutzung von den im Internet verfügbaren Webservices, was unabdingbar zum Ausbau des IoS, (Internet of Services) führt.



◘ **Abb. 20.2** Architekturtyp: Client-Server und n-tier. (Quelle: [10, 16])

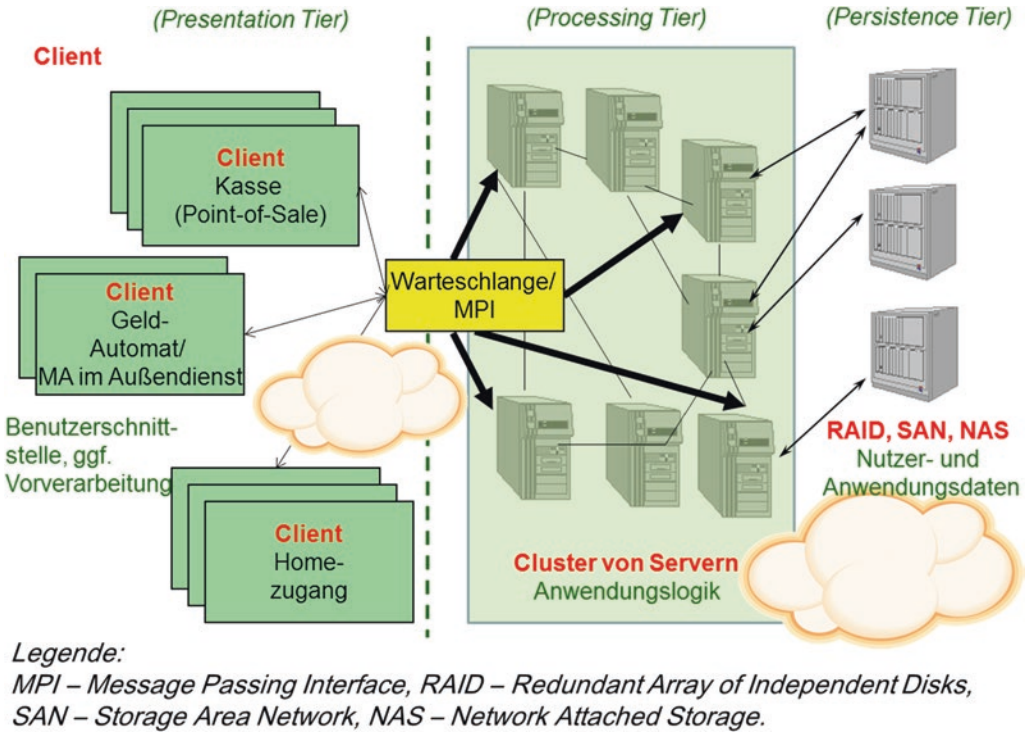
Der Einsatz leistungsfähigerer Serverteile charakterisiert den aktuellen Wandel der Architekturen von Verteilten Systemen:

C-S → n-tier → Clustering → IoS mit Cloud Computing (20.1)

Wesentliche architektonische Neuerungen werden über die Clustering-Architektur (◘ Abb. 20.3) abgebildet, indem jeder Dienst in mehreren Instanzen zur Verfügung gestellt wird (per Server- und Datenbankreplikation).

Die Cluster-Architektur ermöglicht eine Optimierung der QoS für verteilte Anwendungen via Replikation der Funktionalität zwischen mehreren Servern. Die Funktionalität für die Datenverarbeitung (Anwendungslogik) sowie für die Datenpersistenz wird über mehrere Server gleichzeitig oder parallelisiert realisiert. Unmittelbar vor der Replikation ist eine vorläufige Analyse der Datenkonsistenz erforderlich. Die Replikation der Funktionalitäten eines Servers wird durch einen Cluster von Servern mit folgenden Clusterfunktionen optimiert: Lastverteilung, fehlertolerantes Verhalten und feinere Parallelität bei der Verarbeitung (vgl. ◘ Abb. 20.2).

Ein wichtiges Pro-Argument für die Server-Replikationen in der Cluster-Architektur stellt die signifikante Verbesserung der



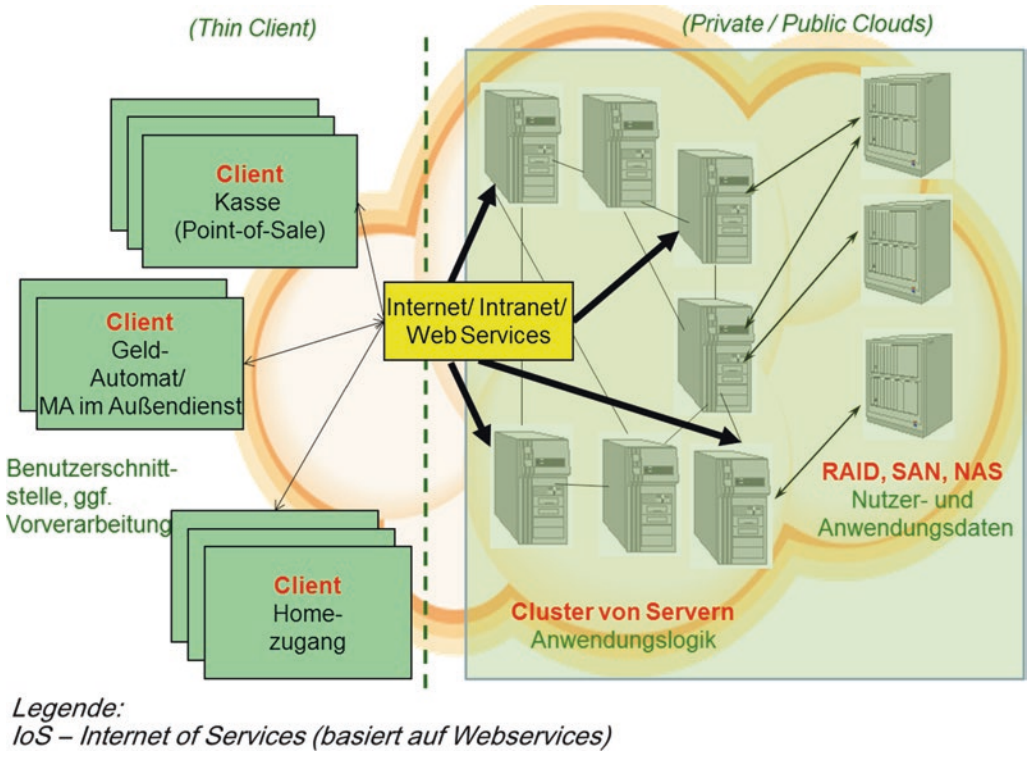
◘ **Abb. 20.3** Architekturtyp: Clustering. (Quelle: [10, 16])

Bearbeitungszeit dar. Gleichzeitig bleibt es dabei nachteilig, dass die zunehmende Komplexität das Konfliktmanagement und die Synchronisation erschwert [7].

Die qualitativ neuen Möglichkeiten haben sich seit 2011 in modernen Architekturen von verteilten Anwendungen etabliert, deren Serverteile in den Clouds gehostet werden (◘ Abb. 20.4).

Die Clouds als Architekturtyp einer verteilten Anwendung bietet die Einführung und Nutzung von „Rechenleistung" in ähnlicher Art und Weise wie bei der Lieferung von Wasser oder elektrischem Strom in modernen Versorgungsnetzen (in sogenannten „Utility Grids") geliefert werden. Es wird ein transparenter Betrieb in einer Cloud unter Nutzung von Internet of Services (basiert auf Webservices) aktiviert. Die wichtigsten Vorteile dieses Architekturtypes sind wie folgt [10, 16]:

1. Manchmal besitzen die Organisationen nicht genügend Ressourcen für die Datensicherung (Datenbackups) und die Lösung rechenintensiver Probleme. Dann bedeutet der Einsatz von Clouds eine gewisse Infrastruktur-Outsourcing
2. Außerdem unterstützt eine Cloud die Aggregation von Ressourcen von mehreren Organisationen, die durch die Provider erfolgt



◘ **Abb. 20.4** Architekturtyp: IoS und Clouds. (Quelle: [10, 16])

3. Unternehmen/Behörden können einen „On-Demand“ -Ressourcenzugriff bekommen
   als ideale Lösung bei schwankendem Bedarf
4. Die durch die Clouds entstehenden Ersparnisse bzgl. Verarbeitungszeit und Hardware-Kosten überwiegen i. a. den Nachteil wachsender Koordinations- und Synchronisationskomplexität.

Als ersten wesentlichen Nachteil kann jedoch die Uneinheitlichkeit der Datensicherheits- und Schutzaspekte vermerkt werden, insb. wenn die Datenverarbeitung organisatorische oder auch juristische Grenzen durchbricht. Des Weiteren fördert Cloud Computing die Heterogenität von Clients und die Herstellerbindung bei den Cloud-Services [10].

Es gibt heutzutage keine einheitliche Definition dessen, was ein Cloud-System ist [1]. Trotzdem lautet eine häufig verwendete Definition von NIST (National Institute of Standards and Technology, USA) 2011 folgendermaßen: „Cloud Computing ist ein Modell zur Ermöglichung eines allgegenwärtigen, bequemen, „On-Demand“-Netzwerkzugangs zu einem gemeinsamen Pool von konfigurierbaren Ressourcen (bspw. Netzwerke, Server, Speicher, Anwendungen und Services), die schnell bereitgestellt werden können und mit minimalem Verwaltungsaufwand oder Service-Provider Interaktionen freigegeben werden“. Laut NIST besteht das Cloud-Modell aus drei Servicemodellen (XaaS wie SaaS, PaaS und IaaS) und vier Bereitstellungsmodellen wie Public, Private, Hybrid und Community Clouds [1].

Im Gegensatz zu den Providerarten für die Clouds (Public, Private Clouds) gibt es die Clouds, die wissenschaftliche Gemeinschaften oder freiwillige Communities organisieren. Die freiwilligen Cloud-Systeme sind aber für jedermann zugänglich. Diese haben keine oder nur geringe Kosten, aber auch keine strengen SLA-Garantien! Die Beispiele dafür sind Guifi und ownCloud-Instanzen. Anderseits gibt es kommerzielle Cloud-Anbieter, die eine schnelle Bereitstellung und die Elastizität der Ressourcen in großem Umfang anbieten (bspw. Amazon EC2, MS Azure, IBM Softlayer, Bluemix, T-Systems Enterprise Cloud, Google Cloud Platform).

Beispiel 20.3

Die bekanntesten Beispielprojekte für die Grids sind [7, 10]:

- BOINC (The Berkeley Open Infrastructure for Network)
- SETI (Search for Extraterrestrial Intelligence)
- Rosetta (Krebs- und Alzheimerforschung per Grids)
- Earth System Grid
- Human Genome Research

Die bekanntesten kommerziellen Cloudprovider sind:

- Amazon EC2, IBM, SkyDrive, Wuala, T-Systems.

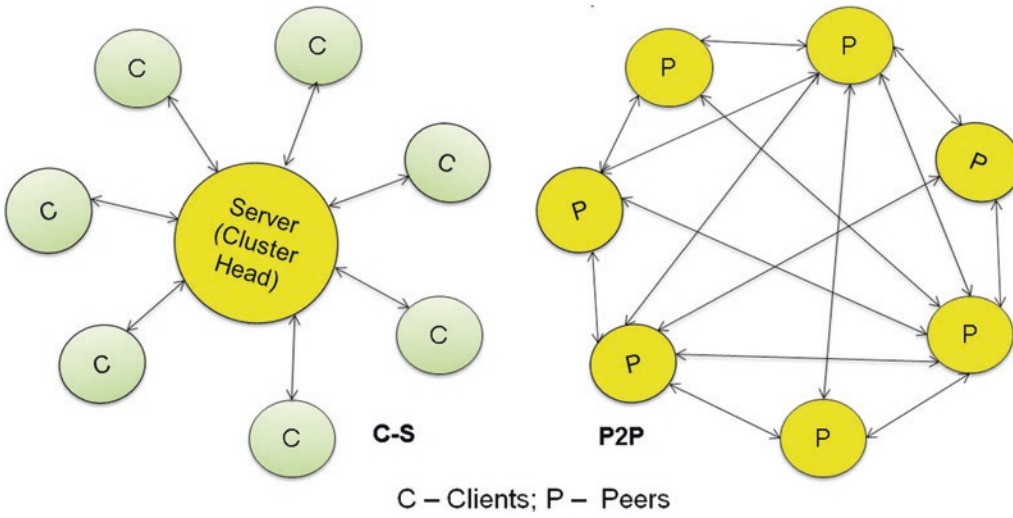
20.1.5 P2P-Systeme

Der Gegensatz zum Peer-to-Peer-Modell ist das Client-Server-Modell [17]. Bei diesem bietet ein Server einen Dienst an und ein Client nutzt diesen Dienst. In Peer-to-Peer-Netzen ist diese Rollenverteilung aufgehoben. Jeder Teilnehmer ist ein Peer, denn er kann einen Dienst gleichermaßen nutzen und selbst anbieten. P2P-Systeme werden charaktersiert durch (◘ Abb. 20.5):

- Direkte Kommunikation zwischen den Peers
- Keine Zentralisierung, evtl. optional
- Peers sind gleichzeitig Serviceprovider und User
- Mechanismus für Auffinden für Serviceprovider-Peers erforderlich!

P2P-Systeme lassen sich in unstrukturierte und strukturierte P2P-Systeme unterteilen. Die Typen von P2P-Systemen werden in ◘ Abb. 20.6 repräsentiert [10, 17]:

1. Typ A: zentralisiertes P2P-Modell
   - Ein Server dient für die Koordination und Suche
   - Beispiel: Napster.
2. Typ B: reines P2P-Modell
   - Hier ist keine zentralisierte Koordination vorhanden
   - Beispiel: Gnutella.
3. Typ C: hybrides P2P-Modell
   - Dynamisches Modell mit zentralen Entities, einige Peers agieren aber als Koordinatoren
   - Beispiele: Gnutella2, BitTorrent, Skype, WhatsApp.



◘ **Abb. 20.5** Vergleich von Kommunikationsmodellen: C-S- vs. P2P

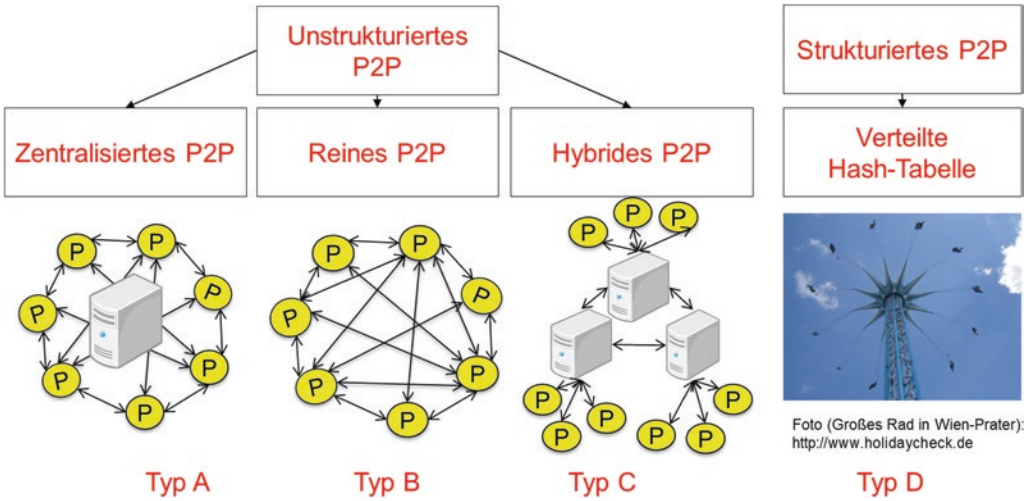


Abb. 20.6 Typen von P2P-Systemen

4. Typ D: verteiltes P2P-Modell mit vert. Hashtabelle
   - Eine DHT, Distributed Hash Table, wird eingesetzt. Die Zugriffs-IDs sind die Keys und werden auf einem Kreis platziert.
   - Das System ermöglicht die Überlappung fester Verbindungen (Fixed Connection Overlay), ähnlich wie beim Routingprinzip (verteiltes/hierarchisches Routing)
   - Beispiele: Chord, CAN, Pastry, Tapestry.

20.1.6 Leistungsoptimierung in Verteilten Systemen

Die Verfahren und Hilfsmittel zur Optimierung von Leistungskennwerten, wie bspw. Durchsatz [in Mbyte/s], Verzögerung oder Reaktionszeit [in ms], Anzahl von gleichzeitig angekoppelten Clients, abgesetzten Fernaufrufe oder ausgeführten SQL-Anfragen, sind wie folgt [16]:

1. Threads
2. Replikation
3. Caching
4. n-tier-Aufbau
5. Empirische Regeln.

Die ersten drei Paradigmen werden in Abb. 20.7 zusammengefasst. Die weiteren Paradigmen lassen sich in Abb. 20.8 anschauen [16]:

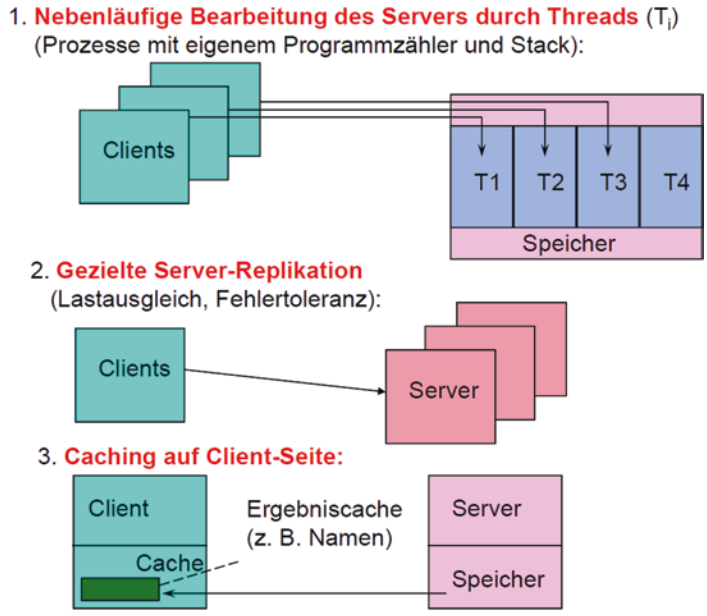


Abb. 20.7 Leistungsoptimierungsparadigmen (Threads – Replikation – Caching) [16]

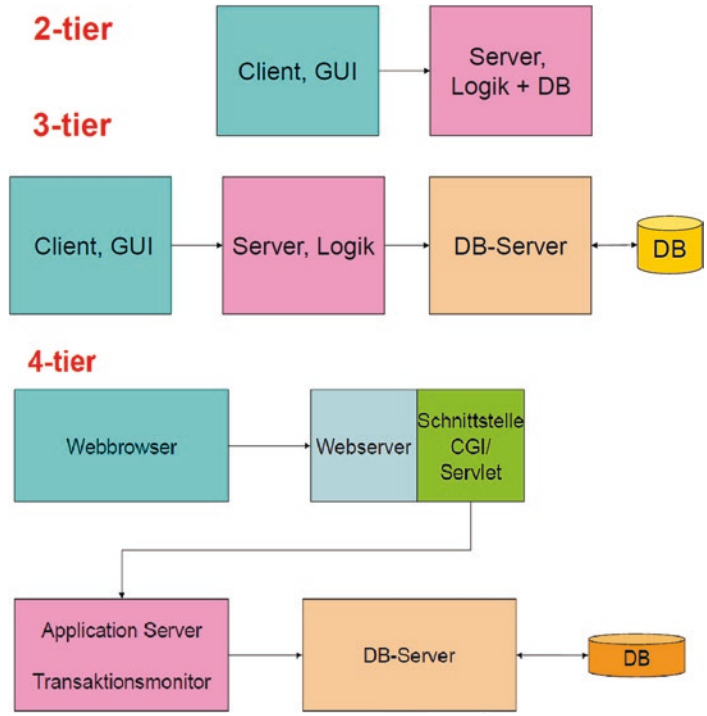


Abb. 20.8 Leistungsoptimierungsparadigmen (n-Tier)

1. Die Leistungsoptimierung von C-S-Systemen ist auf der Basis von nebenläufiger Bearbeitung des Servers durch Threads (Ti) primär möglich [18, 19]. Die Multithreading teilt die Verarbeitung durch den Hauptprozess in die nebenläufigen Subprozesse {T1, T2, T3, T4} im Speicher mit jeweils eigenem Programmzähler und Stack. Diese Subprozesse lassen nur minimalen Kontextaustausch zu (Registerübergabe des Programmzählers und Stackpointer). Die Clients profitieren durch bessere Skalierbarkeit und reduzierte Antwortszeit.
2. Die nächste Moglichkeit liegt an der gezielten Server-Replikation zwecks Lastausgleich und Fehlertoleranz. Auf redundante Verarbeitungskomponenten, Datenbanken, Dokumente und Files kann inklusiv/exklusiv zugegriffen werden. Die Clients profitieren durch feinere Parallelität und reduzierte Antwortszeit.
3. Caching im Speicher auf Client-Seite bringt operativen Zugriff auf die häufig benötigten Daten bspw. die Konfigurationsparameter oder die Namen zur Bindung bei Fernaufrufen RPC oder RMI.
4. Horizontale Verteilung der Anwendungen und Nutzung der N-tier-Architektur (mehrschichtige Architektur) bringt als Ergebnis erhöhte Fehlertoleranz, Flexibilität und Verfügbarkeit von verteilten Anwendungen [7].
5. Einhaltung dieser weiteren wichtigen empirischen Regeln spielt eine Rolle für Leistungsoptimierung in Verteilten Systemen, die nicht zu unterschätzen ist [16, 17]:
   - CPU-Leistung ist oft wichtiger als Netzleistung.
   - Software-Overhead durch Zusammenfassen von Paketen reduzieren.
   - Kontextwechsel zwischen Prozessen minimieren.
   - Kopiervorgänge minimieren, z. B. durch gemeinsamen Speicher (SAN/NAS).
   - Höhere Datenrate DR ist möglich, nicht aber eine geringere Verzögerung.
   - Überlastung vermeiden ist besser als beheben.
   - Timeouts vermeiden.

Beispiel 20.4

- NAS (Network Attached Storage): Einbindung unterschiedlicher Dateiserver über LAN-Technologien bei hoher Verfügbarkeit von Festplattenspeicher durch Redundanz.
- SAN (Storage Area Network): Weitergehendes Konzept mit blockorientiertem Datentransfer via FiberChannel (lokal eng begrenztes Hochleistungsnetz) oder Ethernet und Möglichkeit der Einbindung von Datenbanken und Bandgeräten.

20.2 Verteiltes Rechnen: Cluster und Grids

20.2.1 Verteiltes Rechnen: Einsatz und Leistungsmerkmale

Verteiltes Rechnen erfolgt über den gleichzeitigen Einsatz von „Computing Power" von Clustern oder Grids. Die Standard-Leistungskennwerte wie bspw. 100GFLOPS bei einem hausüblichen PC werden in diesem Falle bis zum Faktor $\times 10.000$ bis $\times 100.000$ multipliziert.

Verteiltes Rechnen wird aktuell in vielen wissenschaftlichen, gesellschaftlichen und kommerziellen Bereichen eingesetzt:

- in Genetik, Astronomie, bei physikalischer und chemischer Simulation
- in der Pharmaforschung
- in Statistik bei (e-Voting oder Volkszählung)
- in den Wirtschaftswissenschaften (Finanzmanagement und Risikoevaluiieruing)
- beim elektronischen Handel
- bei Automatisierung und Facility Management
- bei Webservices (Webdienste stellen i. d. R. den Zugang zu den Systemen für das Verteilte Rechnen bereit)
- zum Risikomanagement in der Baudynamik etc.

Der Begriff „FLOPS" kennzeichnet „Floating Point Operations Per Second" als üblichen Leistungswert. Häufig wird als FLOP eine Gleitkommazahlen-Operation (Floating-Point Operation) bezeichnet, wodurch vereinzelt auch die Variante FLOP/s auftaucht, beide Varianten sind allerdings gleichbedeutend. Die SI-konformen Präfixe (K, M, G, T, P, E, Z, Y) sind dabei wie folgt:

***KFLOPS** - KiloFLOPS = 10^3 FLOPS*

***MFLOPS** - MegaFLOPS = 10^6 FLOPS*

***GFLOPS** - GigaFLOPS = 10^9 FLOPS*

***TFLOPS** - TeraFLOPS = 10^{12} FLOPS*

***PFLOPS** - PetaFLOPS = 10^{15} FLOPS*

***EFLOPS** - ExaFLOPS = 10^{18} FLOPS*

***ZFLOPS** - ZettaFLOPS = 10^{21} FLOPS*

***YFLOPS** - YottaFLOPS = 10^{24} FLOPS*

Die leistungsstärksten Systeme für das Verteilte Rechnen (Computing Cluster und Grids) operieren heutzutage im Bereich ca. 1..10 PFLOPS. Zwecks Parellelisierung der Einzelanwendungen kommen nebenläufige Threads und das MPI-Konzept (Message Passing) zum Nachrichtenaustausch zwischen den nebenläufigen Threads zum Einsatz. Zur Parallelisierung nutzt man oft die folgenden Ansätze:

- Unabhängigkeit von Geschäftsprozessen (Workflow Parallelism) in einer C-S-Lösung
- Unabhängigkeit von Daten (Data Parallelism) in spezifischen Algorithmen in verteilten Anwendungen (wie bspw. Vektor-, Matrix-Kalkül)
- Unabhängigkeit von Abläufen (Blöcken und Prozessen) innerhalb eines Programms zur Ausführung auf einem Einzelrechner.

Die Nutzung der folgenden aktuellen Frameworks ermöglicht effiziente Parellelisierung von Netzwerkanwendungen:

- OpenMP (Open Multi-Processing), verwaltet durch OpenMP Architecture Review Board (ARB), Sprachen C/C++, FORTRAN, seit 1997 (Freeware)
- MPI (Message Passing Interface) von William Groupp and Erwin Lask, verwaltet durch MPI Forum, Sprachen C/C++, FORTRAN, seit 1994
- TBB (Intel Threading Building Blocks) – C++-Programmierbibliothek zur effizienten Nutzung von Mehrkernprozessoren, bietet auch einen Satz von Datenstrukturen und Algorithmen, die typische Probleme bei der Verwendung von Threads vermeiden helfen, seit 2006
- HPF (High Performance Fortran) – Schnittstelle für Ausführung parallelisierter Programme unter Nutzung des Datenunabhängigkeitsmerkmals (data parallelism model), nur FORTRAN-Algorithmen.

Beispiel 20.5

Die theoretische Spitzenleistung (TPP, Theoretical Peak Performance) eines einzelnen Rechenknotens eines CPU-basierten Hochleistungsrechners lässt sich wie folgt berechnen [19]:

$$\begin{aligned} GFLOPS = &(CPU{-}Takt\ in\ GHz) \times (Anzahl\ der\ CPU\text{-}Kerne) \\ &\times (CPU\text{-}Instruktionen\ pro\ Takt) \\ &\times (Anzahl\ der\ CPU\ im\ Rechenknoten). \end{aligned} \tag{20.2}$$

Dabei ist zu beachten, dass bei verschiedenen Rechnerarchitekturen die ausgeführten Instruktionen pro Zyklus variieren können. So haben z. B. Intel X5600 Series CPUs und AMD 6100/6200 Series CPUs vier Instruktionen per Zyklus und Intel E5-2600 Series CPUs acht Instruktionen per Zyklus.

Variante 1:

Zwei-Sockel-Server mit Intel X5675 (3,06 GHz, 6 Kerne, 4 Instruktionen pro Takt)

Performance = 3,06 × 6 × 4 × 2 = 146,88 GFLOPS

Variante 2:

Zwei-Sockel-Server mit Intel E5-2670 (2,6 GHz, 8 Kerne, 8 Instruktionen pro Takt)

Performance = 2,6 × 8 × 8 × 2 = 332,8 GFLOPS

Durch den FLOPS-Wert wird nicht die reine CPU-Geschwindigkeit abgebildet (von Taktfrequenz in GHz abhängig) sondern die reale Geschwindigkeit, die durch gesamte Rechnerarchitektur (bestehend aus Hauptspeicherorganisation, Registern, Bus, Maschinenbefehlen, Caches, Compiler etc.) charakterisiert wird.
Der FLOPS-Wert kann durch spezielle Software (die s. g. Benchmarks) ermittelt werden. Die Benchmarks bestimmen die typische Auslastung für einen Computer oder sogar einen Cluster, die aus einer statistisch repräsentativen Mischung von Gleitkommabefehlen (FLOP) besteht und lassen die Spitzengeschwindigkeit ausmessen.
Die Benchmarks können außerdem für bestimmte Arten von Applikationen zugeschnitten werden (Mathematik, Webkommunikation, Streaming,…). Auf diese Weise kann der maximale FLOPS-Wert eines Computers durch solches Programmpaket wie bspw. LINPACK, Livermore Benchmark, ermittelt werden.

Da es sich bei den Werten nur um die theoretische Spitzenleistung (Peak Performance) handelt und in einem Rechensystem noch ein gewisser Verwaltungsaufwand anfällt, wird zusätzlich die bereinigte Spitzenleistung (Adjusted Peak Performance, APP) ermittelt. Die APP liegt bei ca. 30 % der TPP.

20.2.2 Grids vs. Clustering

Einer der wichtigsten Teile der Cloud-Technologie sind die Grids. Der Begriff „GRID" wie „Global Resource Information Database" entstand im Jahre 1985 im Rahmen eines UNO-Programmes für Umweltschutz. Anderseits bedeutet der Begriff „Grid" auch das „Supply Network" [7, 10, 16, 17].

- Grid Computing ist eine Form des verteilten Rechnens, in dem ein „virtueller Supercomputer" aus einem Set lose gekoppelter heterogener und geografisch verteilter Computer, Tablets, Smartphones erzeugt wird.
- Im Gegensatz dazu wird ein Cluster aus einem Set effizient gekoppelter (i. d. R per LWL) homogener und in einem Ort konzentrierter „Computing Power" gebaut.

Von typischen Computerclustern unterscheidet sich Grid Computing in der wesentlich loseren Kopplung, der Heterogenität und der geographischen Zerstreuung der Computer. Des Weiteren ist ein Grid meistens bestimmt für eine spezielle Anwendung und nutzt häufig standardisierte Programmbibliotheken (API – Application Programming Interfaces), Middleware und Webservices.

Die Grids wurden mit dem Ziel entwickelt, die rechenintensive wissenschaftlichen und vor allem logisch-mathematischen kooperative Probleme zu lösen. Die folgenden Arten von Grids sind zu unterscheiden [7, 10]:

1. **Computer Grid**
   - Kombinierte Rechenleistung, die Zugriff auf verteilte Ressourcen erlaubt.
2. **Data Grid**
   - Das System ermöglicht gemeinsame Nutzung von enthaltenen Daten aus einer oder mehreren verteilten Datenbanken.
3. **Service Grid**
   - Vielzahl von Komponenten, von denen jede einzelne von einem anderen Ressource-Provider als Utility bereitgestellt wird.
4. **Application Grid**
   - Das System sorgt für eine verbesserte Auslastung des Betreibers und bietet ein breites Spektrum an Angeboten

durch eine organisationsübergreifende gemeinsame Nutzung von Ressourcen.

5. **Resource Grid**
   - Das System wird durch die Einführung eines Rollenmodells charakterisiert; die Rollen werden zwischen den Grid-Usern, einem Provider und einem Ressource-Provider abgegrenzt und klar differenziert.

Die Spitzenleistung einiger Cluster und Grids sind in ◘ Tab. 20.2 zusammengeführt (Quelle: wikipedia.de, eigene Zusammenstellung):

20.2.3 Beschleunigungsfaktoren

Die Beschleunigungsfaktoren im Verteilten Rechnen sind [10, 14, 18, 19]:

- Anzahl n der verfügbaren CPU oder GPU
- Anzahl n der verfügbaren Cores in den Prozessoren
- Anzahl n der verfügbaren Threads
- Speichergröße bei den Clustern
- Effiziente Kopplung zw. den Prozessoren (Fibre Channel 4…16 GBit/s) und minimierter Kommunikationsfaktor k zwischen diesen
- Effizienz der einzusetzenden SWT-Lösungen selbst (MPI, OpenMP, Intel TBB, HPF).

Das allerwichtigste Kriterium zur Parallelisierung der Netzwerkanwendungen ist der Faktor p – Parallelisierbarkeit (Verhältnis der Ausführungszeit einer CPU zur Dauer der parallelisierten Ausführung). Die Beschleunigung (Speedup A) im verteilten Rechnen ist somit:

$$A_n = A(n,\ p) = T_1 / T_n \tag{20.3}$$

Die Effizienz des Einsatzes von mehreren n CPUs wird in der Einheit En gemessen:

$$E_n = (A_n / n)\,100\,\%$$

◘ Abb. 20.9 mit der Tabelle illustriert [10] jeweils einige bekannten Speedup-Modelle (nach Amdahl, Grosch, Barsis-Gustafson, Karp-Flatt etc.) für das Verteilte Rechnen (Parallel Computing Speedup Models).

Die Beschleunigung (der Speedup-Faktor) ist in Abhängigkeit von $\{n, p = 1 - e, k\}$ angegeben (k – Kommunikationsfaktor, e – Anteil der nichtparallelisierbaren Abläufe in der Anwendung). Die Linien (3), (5) und (8) bilden jeweils einen optimistischen (idealen) Wert für die lineare Beschleunigung im Cluster oder Grid, einen realistischen Wert nach

Tab. 20.2 Spitzenleistung einiger Cluster und Grids [10]

Name	Standort	PFLOPS	Konfiguration	Energie-bedarf	Zweck
Summit	Oak Ridge National Laboratory (Tennessee, USA)	200	RAM 10PB, 4608 Knoten je 2x(22-core CPU + 6 GPU)	15 MW	Klimasimulation, relativistische Quantenchemie, Bio-, Astro- und Plasmaphysik, Computational Chemistry
Sunway TaihuLight	National Supercomputing Center, Wuxi, Jiangsu	93	40.960 CPU, 1,31 PB RAM	15.370 kW	Ganz neu, ohne Angabe
Tianhe-2	National University for Defense Technology, Changsha, China Finaler Standort: National Supercomputer Center (Guangzhou, China)	33,9	32.000 CPU, 1,4 PB RAM	17.808 kW	Chemische und physikalische Berechnungen (z. B. Untersuchungen von Erdölfeldern und Flugzeugentwicklung)
Titan	Oak Ridge National Laboratory (Tennessee, USA)	17,6	18.688 CPU + 18.688 GPU, 693,5 TB RAM	8209 kW	Physikalische Berechnungen
Sequoia	Lawrence Livermore National Laboratory (Kalifornien, USA)	16,3	98.304 CPU, 1,6 PB RAM	7890 kW	Simulation von Kernwaffentests
K computer	Advanced Institute for Computational Science (Japan)	10,5	88.128, 1377 TB RAM	12.660 kW	Chemische und physikalische Berechnungen
BOINC	Berkley Univ. (Kalifornien, USA), Berkeley Open Infrastructure for Network Computing	9…10	Grid, geografisch zerstreut und für PCs, Tablets und Smartphones zugeschnitten		Projekte wie SETI, RNA, ROSETTA, EINSTEIN usw.

(Fortsetzung)

Tab. 20.2 (Fortsetzung)

Name	Standort	PFLOPS	Konfiguration	Energie-bedarf	Zweck
Mira	Argonne National Laboratory (Illinois, USA)	8,2	49.152 CPU	3945 kW	Entwicklung neuer Energiequellen, Technologien und Materialien, Bio-informatik
Hazel Hen	Höchstleistungs-rechenzentrum Stuttgart	7,4	7712 CPU	3200 kW	Ohne Angabe
JUQUEEN	Forschungszentrum Jülich (Deutschland)	5,9	28.672 CPU, 448 TB RAM	2301 kW	Materialwissenschaft, theor. Chemie, Elementarteilchen-physik, Umwelt, Astrophysik
SuperMUC IBM	Leibniz-Rechenzentrum (LRZ) (Garching bei München, Deutschland)	2,9	18.432 CPU + 820 CPU, 340 TB RAM	3423 kW	Kosmologie über die Entstehung des Universums, Seismologie und Erd-bebenvorhersage
Stampede	Texas Advanced Computing Center (Texas, USA)	2,7	4870 CPUs, 185 TB RAM	4510 kW	Chemische und physikalische, biologische (z. B. Proteinstruktur-analyse), geologische (z. B. Erd-bebenvorhersage), medizinische Berechnungen (z. B. Krebswachstum)
Tianhe-1A	National Supercomputer Center (Tianjin, China)	2,3	14.336 CPU + 7168 GPU, 224 TB RAM	4040 kW	Chemische und physikalische Berechnungen (z. B. Untersuchungen von Erdölfeldern und Flugzeugent-wicklung)
Dawning Nebulae	National Supercomputing Center (Shenzhen, China)	1,3	55.680 CPU + 64.960 GPU, 224 TB RAM	2580 kW	Meteorologie, Finanzwirtschaft u. a.
IBM Roadrunner	Los Alamos National Laboratory (New Mexico, USA)	1,1	6000 CPU +, 13.000 CPU, 103 TB RAM	4040 kW	Physikalische Simulationen (z. B. Atomwaffen-simulationen)

Speedup factor $An=\frac{T_1}{T_n}$	Speedup Model	Conventions	Title of an empirical model
1.	$A_n=\sqrt{n}$	The type of math-log problem is not considered	Grosch's law (1965)
2.	$A_n=n^b$	The type of math-log problem is not considered	Generalized Grosch's law $0{,}5\le b\le 1$
3.	$A_n=n$	The type of math-log problem is not considered	Proportional Amdahl law for $p=1$ $s=0$
4.	$A_n=\log_2(n)$	The type of math-log problem is not considered	Logarithmic Law
5.	$A_n=\frac{1}{(1-p)+p/n}$	$0{,}5\le p\le 0{,}999\ldots$ $k=0$	Amdahl's Law (1967)
6.	$A_n=\frac{1}{(1-p)+p/n+k\cdot n}$	$0{,}5\le p\le 0{,}999\ldots$ $k\approx 10^{-4}..10^{-5}$	Corrected Amdahl's Model with inter-processor communication considering
7.	$A_n=2$ $n=70\%/r\%$	The type of math-log problem is not considered , $r=1\ldots 2\%$ characterizes inter-processor communication losses	Empirical law „69 - 70 – 72" for CPU-number n, which provides double speedup of computing time
8.	$A_n=(1-p)+p\cdot n$	$0{,}5\le p\le 0{,}999\ldots$ $k=0$	Barsis-Gustafson-Law (1988)
9.	$A_n>1$ $e(A_n,n)=1-p=\frac{1/A_n-1/n}{1-1/n}$	$e=1-p$ – the unknown part for sequential computing time; $0{,}5\le p\le 0{,}999\ldots$ $k=0$	Karp-Flatt-Metric (1990) for Amdahl's or Barsis-Gustafson-Law

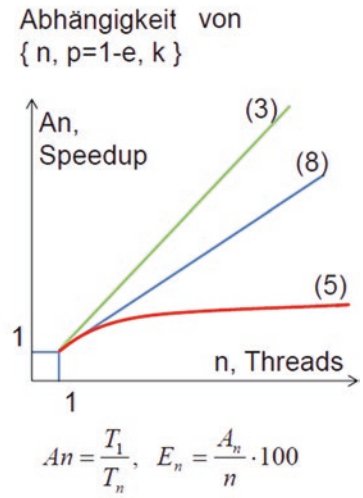


Abb. 20.9 Speedup-Modelle [10]

Gustafson-Barsis sowie einen pessimistischen Wert mit Asymptote nach Amdahl.

20.2.4 Allgemeine Architektur des Verteilten Rechnens

Generell gibt es die folgenden Arten von Verteilten Rechnen (im Englischen „Distributed Computing"):

- Cluster Computing (homogene Umgebung, zentralisierte Knoten, konsolidierte „Computing Power")
- Grid Computing (geographisch verteilte Knoten, heterogene)
- Cloud Computing (konsolidierte „Computing Power" und Speicherkapazität)
- Fog Computing (Peer-to-Peer-Systeme mit delegierter Intelligenz).

Die Arten von Distributed Computing und dazugehörende Systembeispiele von Clustern, Grids und Clouds wurden in Abb. 20.10 aufgeführt.

Die allgemeine Architektur des Verteilten Rechnens ist in Abb. 20.11 repräsentiert. Die Grids und Cluster interagieren mit

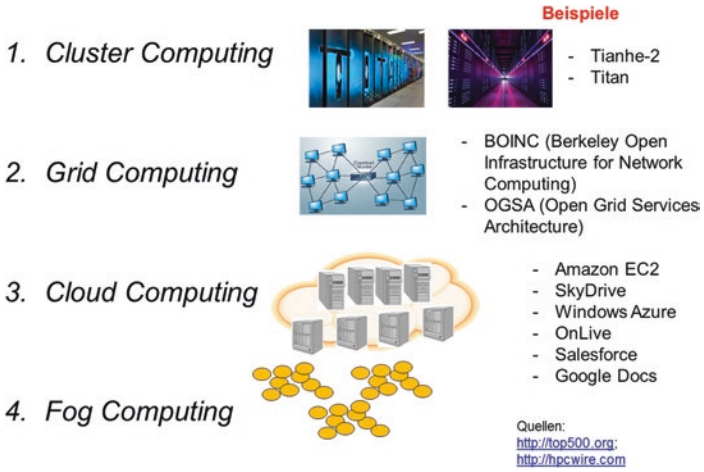


Abb. 20.10 Arten von Distributed Computing und dazugehörende Systembeispiele

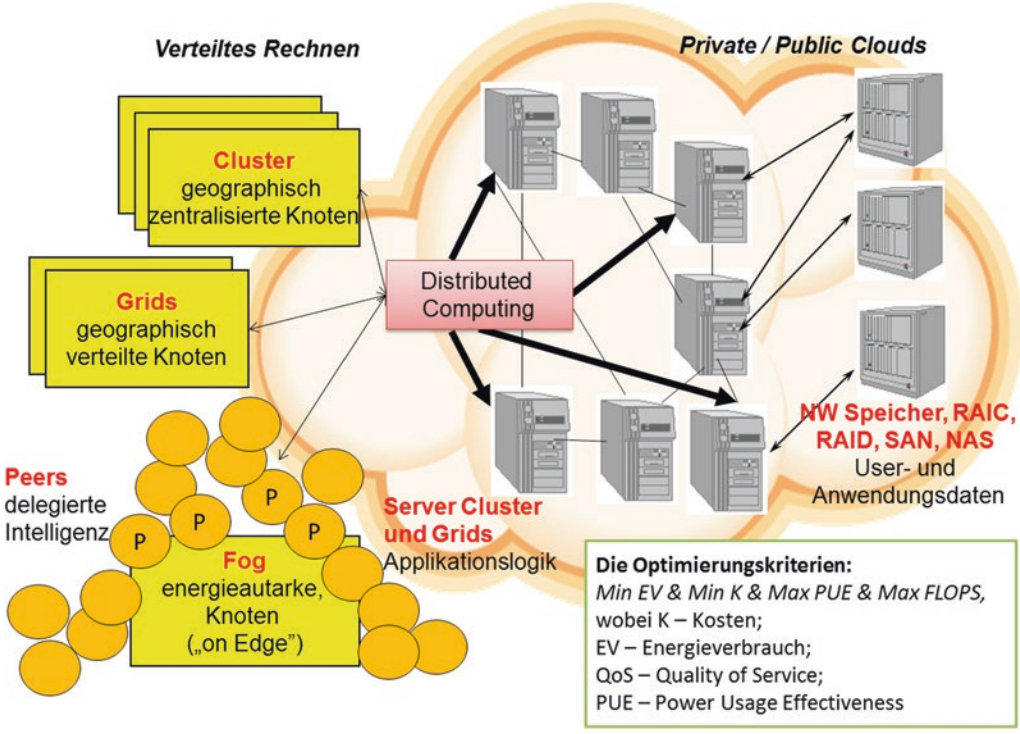


Abb. 20.11 Die allgemeine Architektur des Verteilten Rechnens

den Clouds und dem sog. Fog (mit energieautarken autonomen Knoten, deren Funktionalität „on Edge“ d. h. zum User delegiert wird). Genaueres über die Konzepte „Cloud Computing“ („Rechnen in den Wolken“) und „Fog Computing“ („Rechnen im Nebel“) erläutern die nachfolgenden Abschnitte dieses Teiles. Der Zugriff zu den Ressourcen in den Clouds (konsolidierte „Computing Power“ und Speicherkapazität) erfolgt mithilfe von „klassischen Techniken“ wie RPC, RMI, MPI, MQI oder mittels Webservices.

Die Optimierungskriterien zum Distributed Computing werden zu den verschiedenen Zielfunktionen kombiniert [10]:

$$\textbf{\textit{Min EV \& Min K \& Max PUE \& Max FLOPS}}, \tag{20.4}$$

wobei K – Kosten, EV – Energieverbrauch, QoS – Quality of Service, PUE – Power Usage Effectiveness.

Ein anderer abgeleiteter Wert ist PW (Performance per Watt):

$$PW = FLOPSc/EV, [FLOPS/W] \tag{20.5}$$

wobei FLOPSc die mittlere Clusterperformance darstellt. Bspw. können für die weltweit bekannten Cluster Tianhe-2 und Titan die folgenden Rechnungen vorgenommen werden (vgl. zur Tabelle mit den Angaben zur Performance und Energieverbrauch):

- ***für den Cluster „Tianhe-2“ (Volksrepublik China):***
  PW = 33,9 PFLOPS/17,808 MW
  = 1,9 PFLOPS/MW = 1,90 GFLOPS/W;
- ***für den Cluster „Titan“ (USA):***
  PW = 17,6 PFLOPS/8,209 MW
  = 2,14 PFLOPS/MW = 2,14 GFLOPS/W.

20.3 Webservices, SoA und IoS

20.3.1 Bausteine für die Webservices

Der Begriff „Webservices“ ist bereits seit 2003 im Einsatz. Ein Webservice ist eine gekapselte Softwarekomponente in beliebiger Programmiersprache, die zum Aufbau einer Webapplikation geeignet ist und über ein TCP/IP-Netzwerk und Protokolle der Schichten L5–7 (meistens HTTP, aber auch asynchron) für die direkte Maschine-zu-Maschine-Interaktion bereitgestellt wird. Somit agiert ein Webservice als eine Weiterentwicklung von MW-Komponenten. Die folgenden Bausteine werden dabei verwendet [14, 16]:

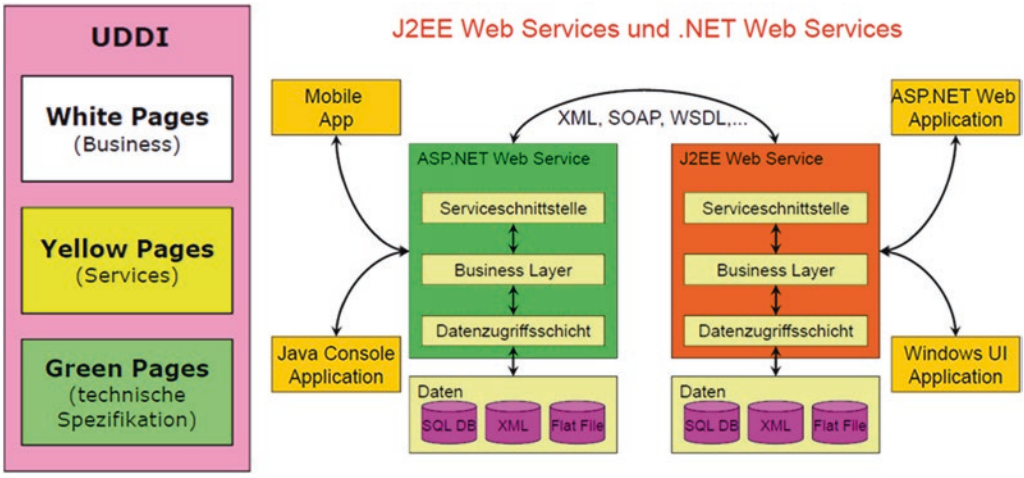
1. Jeder Webservice besitzt einen Uniform Resource Identifier (URI), über den er eindeutig identifizierbar ist, sowie eine Schnittstellenbeschreibung in XML-Format, die definiert, wie mit dem Webservice zu interagieren ist.

2. Für Webservices heißt der kombinierte Auskunfts- und Verzeichnisdienst UDDI (Universal Description, Discovery and Integration).
3. Die von UDDI angebotenen Webservices werden in dem XML-Dialekt WSDL (Webservices Description Language) beschrieben.
4. UDDI ist selbst ein Webservice und wird deshalb wie andere Webservices auch durch
5. SOAP (Service-Oriented Application Protocol, ursprünglich für Simple Object Access Protocol) in Anspruch genommen.

Es werden drei Zugriffsarten [14, 16] unterschieden (◘ Abb. 20.12):
- weiße Seiten (eine Art Telefonbuch): damit können Dienste anhand ihres Namens abgefragt werden;
- gelbe Seiten (eine Art Branchenbuch): damit können Dienste anhand unterschiedlicher Taxonomien abgefragt werden;
- grüne Seiten: damit können Dienste anhand unterschiedlicher technischer Details abgefragt werden.

20.3.2 Abgrenzung zur SOA

SOA (Service-Oriented Architecture) ist kein direkter Webservice. SOA beschreibt losgelöst von konkreten Implementierungstechnologien ein Architekturparadigma. Der SOA-Ansatz konnte auch schon vor 15 bis 20 Jahren mit den damals vorhandenen Technologien umgesetzt werden und fand unter anderem mit CORBA-Middleware seine Anwendung [14, 15, 16].



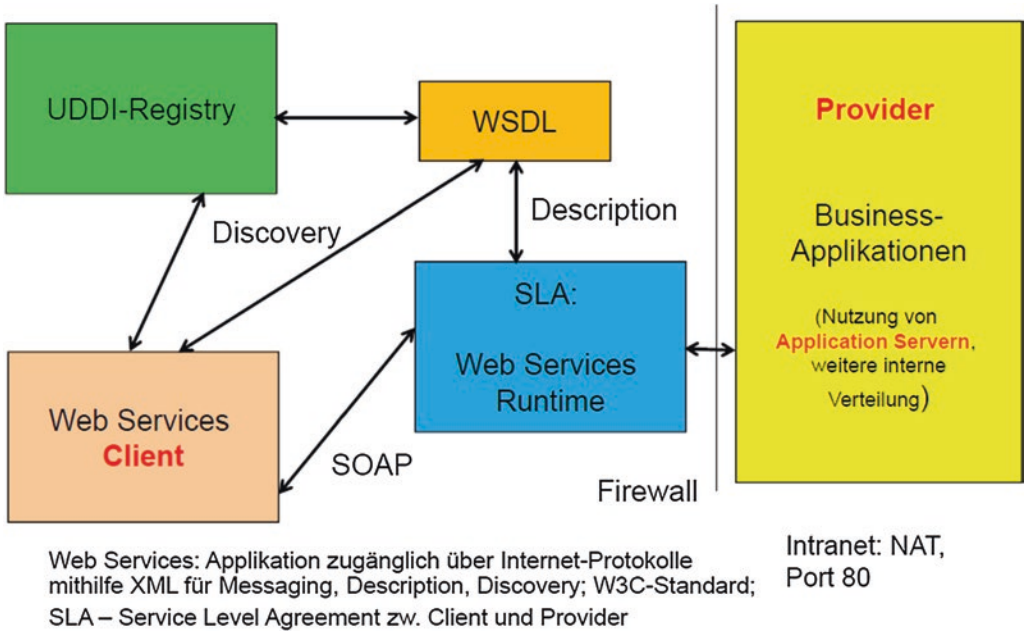
◘ **Abb. 20.12** UDDI-Service und beispielhafte Interoperabilität von Webservices

SOA ist keine Lösung für fachliche Probleme – als Architekturparadigma gibt SOA keine Empfehlung zur Behandlung von fachlichen Problemen. SOA ist individuell. Es gibt keine sog. „Standard-SOA". Ein Unternehmen muss eine SOA immer auf die eigenen Bedürfnisse zuschneiden.

1. Die Webservices basieren auf einer Service Oriented Architecture.
2. Zeit, Kosten und Komplexität von Softwareintegrationsprojekten lassen sich durch den Einsatz einer SOA deutlich reduzieren
3. Nutzung von Web Services führt nicht zwangsläufig zu einer SOA
4. Die wichtigste Neuerung bei SOA sind bewährte Webservice Standards.

Die Webservices sind seit 2005 einer der W3C-Standards. Die Webservices werden primär für Messaging, Description, Discovery verwendet. Weitere Webservices sind unter der Bezeichnung WS-* bekannt (Advanced Web Services) [14, 16].

Ein Einsatzszenario für Webservices ist in ◘ Abb. 20.13 aufgeführt. Web Services werden in die Webapplikation zwecks Vereinheitlichung der Kommunikation oder Ankopplung (EAI) integriert. Deren Ausführung erfolgt über Internet-Protokolle (HTTP/TCP, SMTP/UDP, REST/HTTP, …) mithilfe von XML. Die Laufzeitumgebung (Ausführungsplattform) wird über die



◘ **Abb. 20.13** Ein Einsatzszenario für Webservices [16]

Firewall (über Port 80) oder über die DMZ zugänglich. Die Verfügung über Webservices erfolgt i. d. R. im Rahmen eines Vertrages (SLA – Service Level Agreement) zw. Client und Provider von Webservices. Ein spezieller Fall ist der Zugang zu den internen Anwendungen oder Server im Intranet und NAT-Protokoll.

Die Webservices und die daraus ausgebaute SOA (auch die kommerziellen, die von SOA-Providern angeboten werden), bieten die Basis für das sog. Internet of Services, IoS. Beispiele sind Amazon AWS, OASIS, IETF, Ariba, OGSA – Open Grid Services Architecture. Der Einsatz von IoS bedeutet heutzutage massenhaftes Involvieren von Clouds (2010–2011) und den Ansatz, die Services und Infrastrukturen (bspw. „Computing Power" – Rechenkapazität, Sekundärspeicher, Ausführungsplattformen oder Software) über die speziellen Webservices zur Verfügung zu stellen ohne dass diese auf dem Clientrechner oder Mobilgerät installiert sein müssen.

20.3.3 Zusammenhang „Webservices, Grids, MW und Virtuelle Organisation"

Der Zusammenhang Grids, MW und Webservices lässt sich gut mit dem Konzept OGSA erklären. **Open Grid Services Architecture (OGSA)** ist eine mögliche Softwarearchitektur für die Grids. Diese hieß ehemals Open Grid Services Infrastructure (OGSI). Die Grundidee der OGSA ist die Darstellung von beteiligten Komponenten (Rechner, deren Hauptspeicher und Speichermedien, Mikroskope, …) als Grid-Services in einer offenen Komponentenarchitektur (u. a. als Middleware).

Durch die Standardisierung seitens W3C und Open Grid Forums (OGF) wurden diese Grid-Services auf die technische Ebene der Webservices portiert.

Die angesprochene Architektur OGSA kann bspw. mit dem Einsatz vom sog. WSRF (Web Services Resource Framework) als grundlegenden Baustein für die Griddienste erschaffen werden.

WSRF unterstützt zustandsbehaftete (stateful) Ressourcen (wie Dateien, Java-Objekte, Datensätze in einer Datenbank). Dies ermöglicht es, die Funktionalitäten auszuführen, die sich über mehrere Transaktionen erstrecken. Die Kombination eines Webservices mit einer solchen statusbehafteten Ressource bildet eine sogenannte WS-Ressource für die Grids.

Virtuelle Organisation (VO) ist ein zentrales und hardwareunabhängiges Konzept hinter der Grid-Philosophie. Dabei werden Ressourcen und Services einer VO dynamisch zugewiesen.

Implementierungen von Grid-Middleware und von Grid-zugeschnittenen Webservices sind bspw.:

- g-Eclipse
- Globus Toolkit v4
- Unicore
- gLite
- Sun Grid Engine.

20.4 Cloud Computing und XaaS

» „Cloud Computing beinhaltet Technologien und Geschäftsmodelle um IT-Ressourcen dynamisch zur Verfügung zu stellen und ihre Nutzung nach flexiblen Bezahlmodellen abzurechnen. Anstelle IT-Ressourcen, beispielsweise Server oder Anwendungen, in unternehmenseigenen Rechenzentren zu betreiben, sind diese bedarfsorientiert und flexibel in Form eines dienstleistungsbasierten Geschäftsmodells über das Internet oder ein Intranet verfügbar" (laut Microsoft).

Clouds ermöglichen den Einsatz und die Nutzung von „Computing Power" in analoger Art und Weise wie bei der Lieferung von Wasser oder Strom in modernen Versorgungsnetzen (s. g. Utility Grids): transparenter Betrieb in einer Cloud ist möglich [1, 10, 11, 16].

Vorteile:
- Einzelne Organisationen besitzen u. U. keine ausreichenden Ressourcen für
  Datenbackups und rechenintensive Probleme
- Aggregation Rechenressourcen von mehreren Organisationen (erfolgt durch die Provider)
  Unternehmen/Behörden können den „On-Demand" -Ressourcenzugriff bekommen
  (ideale Lösung bei schwankendem Bedarf)
- Ersparnisse in der Verarbeitungszeit und den Hardware-Kosten überwiegen das auf jeden
  Fall zu bemerkende Wachstum der Koordinations- und Synchronisationskomplexität

Nachteile:
- jedoch Uneinheitlichkeit der Datensicherheits-/Schutzaspekte!

Zahlreiche Beispielprojekte und Plattformen für Cloud Computing:
- Earth System Grid, Human Genome Research
- kommerzielle Cloudprovider (Windows Azure, OnLive, SkyDrive, T-Systems, IBM, Amazon EC2, Sun Cloud,..).

Geschichte [11]

- In der Entwicklung der Rechnernetzwerktechnik gab es immer wieder Vorstellungen, die Funktionalität der Arbeitsstationen auf eine reine Terminalfunktion (Thin Client) zu begrenzen und alle Verarbeitungsfunktionen transparent in das Netzwerk auszulagern. Beispielsweise versuchte die Firma Sun (derzeit Oracle) in den 90-er Jahren diese Vorstellung mit dem Konzept des Netzwerkcomputers, eines auf Java-Technologien orientierten Terminals, durchzusetzen (Motto = „Computer is a Network").
- Dieses Projekt scheiterte weitgehend, weil die damaligen Rechnernetze im dezentralen Zugriff weder leistungsfähig noch zuverlässig genug waren.
  In den letzten Jahren wurden aber enorme Fortschritte in der Netzwerktechnik bezüglich Übertragungsgeschwindigkeit, universeller Verfügbarkeit und hoher Zuverlässigkeit erreicht.

Cloud-Typen [1]

Neue Applikationen in den Clouds ermöglichen die Verlagerung von Kapazitäten und die Realisierung von hochverfügbaren Diensten wie Mail-, Akten- und Datenarchivierung (Cloud-Backups). Die Services der Clouds fördern das Hochleistungsrechnen und unterstützen multimediale Datenübertragungen von den verborgenen Clustern und Speichermedien nach außen. Unter Ausnutzung virtualisierter Rechen- und Speicherressourcen und moderner Web-Technologien stellt Cloud Computing skalierbare, netzwerk-zentrierte, abstrahierte IT-Infrastrukturen, Plattformen und Anwendungen als „on-demand"-Dienste zur Verfügung. Die Abrechnung dieser Dienste erfolgt nutzungsabhängig.

Man kann neben dem technischen Cloudstack auch zwischen verschiedenen Organisationsformen von „Clouds" unterscheiden, die je nach Anwendungsfall ihre Berechtigung haben (◘ Abb. 20.14):

- Private Clouds (unternehmensintern, hohes Maß an Datensicherheit!) – On Premises
- Public Clouds – Off Premises
- Hybride Clouds.
- Spezielle Art bilden s. g. Private Community Clouds [11].

Die organisatorischen Arten von Clouds sind in der ◘ Tab. 20.3. zusammengefasst:

Architektur und Dienstemuster

Die Cloud-Architektur laut Amazon lässt sich als Pyramidenmodell darstellen. Dienste haben ihre Muster und werden in drei unterschiedlichen Gruppen zwischen den Ebenen PHY (physikalische Ebene) und APL (Application-Ebene) aufgeteilt (vgl. ◘ Abb. 20.15). Die allgemeine Schablone nennt sich XaaS (Everything as a Service) und bezeichnet einen Ansatz, „alles"

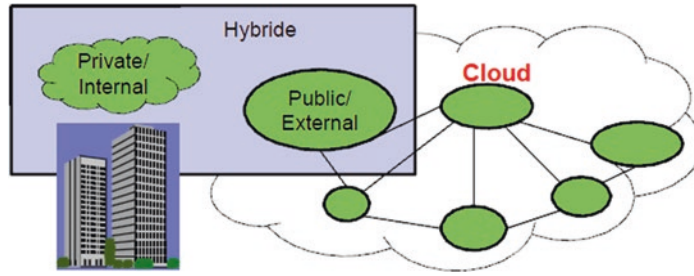


Abb. 20.14 Cloud-Typen

Tab. 20.3 Cloud-Typen (organisatorische Arten)

Private Cloud	**Public Cloud**
Kundeneigene, vom Kunden selbst betriebene Cloud-Umgebung	Zugang beschränkt (Kunde selbst, autorisierte Geschäfts-partner)
Im Eigentum eines IT-Dienst-leisters befindliche und von diesem betriebene Cloud-Umgebung	Zugriff über Intranet
Zugriff über Internet	
Flexible und schnelle Nutzung durch Subskription	
Hybrid Cloud	
Mischbetrieb von Private und Public Cloud	

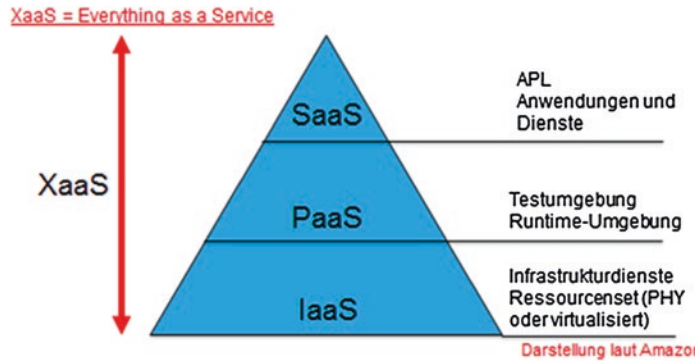


Abb. 20.15 XaaS-Servicemodell laut Amazon

als Service zur Verfügung zu stellen und zu konsumieren. Ansonsten heißen die ebenenspezifischen Services: SaaS (Software as a Service), IaaS (Infrastructure as a Service) und PaaS (Platform as a Service).

Die wesentlichen Eigenschaften des Cloud Computing sind wie folgt [7, 9, 11]:

- Service-oriented Internet (SOA, IoS)
- Diensterbringung auf Anforderung
- Netzwerkbasierter Zugang
- Ressourcen Pooling und Elastizität
- Messbare Dienstqualität QoS

Im Gegensatz zur Darstellung von Amazon bietet Microsoft eine detailliertere Architektur des Cloud Computing.

Die Last-/Funktionenverteilung zwischen Cloud Computing und herkömmlicher IT (laut Microsoft) ist in ◘ Abb. 20.16 repräsentiert. Auch an dieser Stelle kommt eine Mehrschichtenarchitektur zum Einsatz, jedoch sind diese Schichten im Unterschied zum OSI-Referenzmodell nur quasi-konsistent (zu den schichtenübergreifenen Funktionalitäten und Feedbacks):

Datensicherheit [11]

Bei dem Aufbau, dem Deployment und der Wartung von Cloud-Services bleibt die Data Security immer noch eine offene Frage. Cloud Computing wirft schwierige rechtliche Aspekte zwischen Endnutzern, Cloud-Anbietern und deren beteiligten Partnern auf. Für den Endnutzer ist die innere Cloudstruktur vollkommen

Herkömmliche IT	IaaS	PaaS	SaaS
Applikationen	Applikationen	Applikationen	Applikationen
Daten	Daten	Daten	Daten
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
Web Services	Web Services	Web Services	Web Services
BS	BS	BS	BS
Virtualisierung	Virtualisierung	Virtualisierung	Virtualisierung
Server	Server	Server	Server
Speicher	Speicher	Speicher	Speicher
Netzwerk	Netzwerk	Netzwerk	Netzwerk

Legende:

auf eigene Verantwortung

wird als Service von Cloud geliefert

◘ **Abb. 20.16** Quasi-konsistente Schichten: Servicemodell von Clouds laut Microsoft

Abgrenzung zu „Grid Computing“

Der Begriff Cloud Computing ist weiter gefasst als die Grids und Cluster: Bei den Grids geht es um gemeinsame freie oder vertragsgeregelte Verwendung der (virtualisierten) Ressourcen für das Verteilte Rechnen ohne zentrale Steuerung. Im Fall von „Cloud Computing“ hat man einen oder mehreren Cloud-Anbieter mit zentralisierter Steuerung von physikalischen und virtualisierten Ressourcen. Management von Ressourcen erfolgt ebenfalls zentral.

verborgen. Er muss den Cloud-Anbietern vertrauen. Es ergeben sich komplizierte Haftungsprobleme, da die Anbieter i.a. weltweit agieren, unterschiedlichen Gesetzgebungen unterliegen und u. U. ihrerseits von weiteren Anbietern Teildienstleistungen beziehen.

Im Allgemeinen sind rechtliche Vertragsbeziehungen in Clouds in der Bundesrepublik Deutschland durch die folgenden Gesetze und Rechtsvorschriften zu regeln (Quelle: Juris Bundesministerium der Justiz und Verbraucherschutz, BMJ Online: ► http://www.gesetze-im-internet.de/):

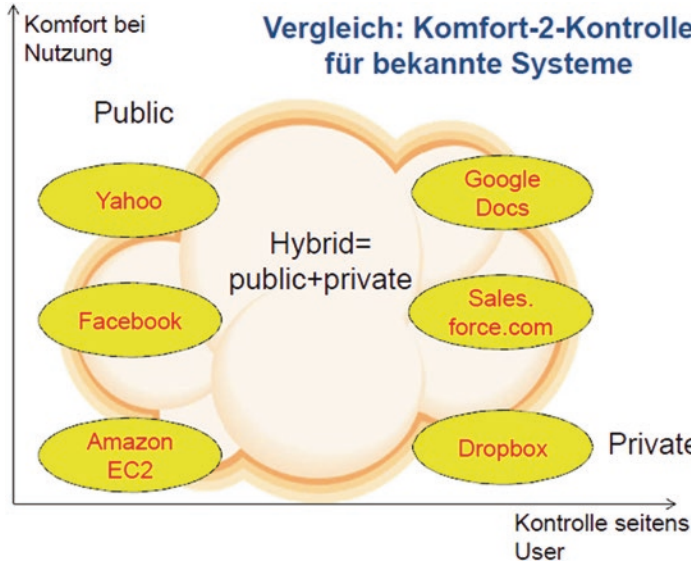
- BGB (Bürgerliches Gesetzbuch)
- TMG (Telemediengesetz) und TKG (Telekommunikationsgesetz).
- EU-Datenschutzgrundverordnung (ab Mai 2018) und BDSG (Bundesdatenschutzgesetz).

Welche Qualitätskriterien sind für Clouds anwendbar?

Die wichtigsten Kriterien sind wie folgt:

1. QoS und Performance.
2. Komfort bei Nutzung.
3. Kontrolle seitens der User.
4. Zuverlässigkeit und Datensicherheit.
5. Preis (per Dateneinheit und Zeit).

Die Kriterien-Projektion „Komfort zu Kontrolle“ für einzelne Systeme ist in ◘ Abb. 20.17 aufgeführt [10, 16].



◘ **Abb. 20.17** Welche Qualitätskriterien sind für Clouds anwendbar?

20.5 Netzwerkmanagement und Monitoring

Zur Planung, Überwachung und Koordinierung der Ressourcen eines Rechnernetzes werden Netzwerkmanagement und-Monitoring-Systeme genutzt (NWM).

Die folgende Klassifikation von NWM-Systemen kann angeboten werden [11, 16]:

- Konfigurationsmanagement (z. B. Netzstruktur)
- Fehlermanagement (z. B. bzgl. Transportprotokolls)
- Leistungsmanagement (z. B. Durchsatzmessung)
- Sicherheitsmanagement (z. B. Verschlüsselungsvarianten und ACL)
- Abrechnungsmanagement (z. B. bei DSL- oder Mobilzugang)
- Änderungsmanagement (z. B. bzgl. Systemanpassung)
- Dienstmanagement (z. B. bzgl. Dienstqualität).

Ziel des Netzwerkmanagements und Monitorings der vernetzten IT-Infrastruktur eines Unternehmens ist der problemfreie Betrieb von Hosts, Servern, Datenbanken, Softwaresystemen etc. (u. a. unterm Virtualisierungsaspekt), um eine höchstmögliche Fehlererkennung, -behebung zu ermöglichen, sowie höhere Verfügbarkeit zu gewährleisten [4, 20].

Ein Fehler, dessen Ursache korrekt erkannt und erfasst worden ist, kann für weitere Vorkommnisse als eine spezielle Regel definiert werden und gegebenenfalls durch automatisierte Gegenmaßnahmen oder das grundsätzliche Ausschließen der Fehlerquelle am erneuten Auftreten gehindert werden.

Netzwerkmanagement und Monitoring werden oft genutzt, um den SLA (Service Level Agreement, Dienstvertrag) automatisiert einzuhalten. Dafür werden die aussagekräftigen Leistungsindikatoren analysiert.

Unter Event Logging wird das Schreiben von Informationen über den Zustand eines Systems verstanden. NW-Management- und Monitoring-Software funktioniert oft in modernen, dynamischen Cloud-Umgebungen und ermöglicht außerdem die Konfiguration und Automatisierung der Anwendungsüberwachung in den Clouds.

Diese Informationen sind in erster Linie für Systemadministratoren gedacht und werden zur automatisierten Benachrichtigung von Systemadministratoren (per SMTP, SMS, Instant Messaging usw.) verwendet. Das Benachrichtigungssystem wird im Monitoring-System heutzutage oft eingebettet als eine unabdingbare Bedingung [3, 4].

Solche Monitoring-Software verwendet oft SNMP, MIB und Agent-Manager-Architektur (s. Teil I).

Das Protokoll SNMP kommt meist für lokale Netze/Firmennetze zum Einsatz. Mittels SNMP (◘ Abb. 20.18) funktionieren

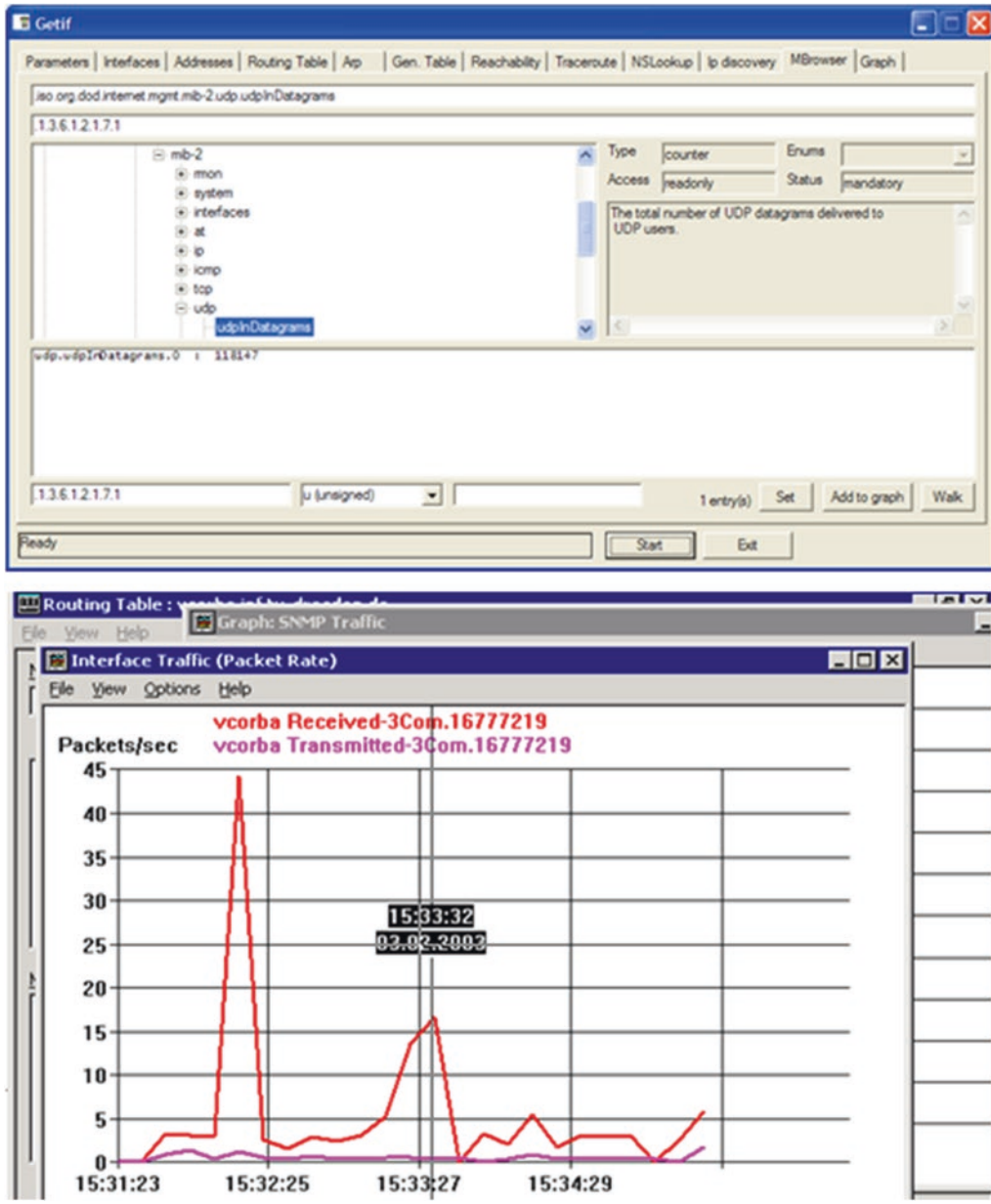


Abb. 20.18 Beispiele für die SNMP-Tools [11]

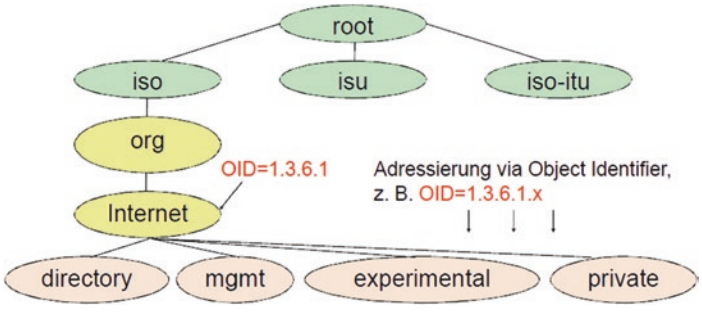
zahlreiche autonome Werkzeuge (Getif, MRTG, Nagios, TelemetryBox…) und insbesondere Management-Plattformen (MS SCOM, HP Sitescope etc.). Die NWM dienen außerdem zur Ergänzung von Sicherheitsmechanismen in Rechnernetzen (Authentisierung und Autorisierung) im aktuellen SNMPv3.

Im Vergleich zu den zahlreichen NWM- Plattformen gewinnen preisgünstigere Einzeltools und integrative Freware-Lösungen [3, 4, 11] immer mehr an Bedeutung (s. ◘ Tab. 20.4).

Der Einsatz von MIB (einer objekt-orientierten verteilten Datenbank mit Referenzieren von Agenten unterschiedlicher Hersteller und Provider) ist von besonderer Bedeutung in NWM. Im Allgemeinen unterstützen die aktuellen MIBs eine standardisierte ISO-Baumstruktur für Sammlung von Managed Objects MO. Die meisten MO sind durch feste Positionen (OIDs) im MIB-Baum gekennzeichnet [3, 4, 11]. Bei Tabellen ist die Anzahl der Elemente dynamisch (◘ Abb. 20.19).

◘ **Tab. 20.4** Beispielhafte Freewaretools zu Netzwerkmanagement

Tool	Funktionalität
Big Brother	Überwachungs-Framework, HTML-Ergebnisauslieferung, Administrierung, Monitoring, Message-Queuing-basiertes Tool (Emails, SMS- Nachrichten), Kern in C geschrieben, MIB-Browser: ► http://bb4.com
Getif	Grafischer MIB-Browser, unterstützt SNMPv1, v2 und v3: ► http://www.wtcs.org/snmp4tpc/getif.htm
MRTG (Multi Router Traffic Grapher)	Messen der Auslastung eines Netzwerks, grafische Darstellung, HTML-Ergebnis-auslieferung: ► http://www.mrtg.org
Nagios (ehemals Netsaint)	Modularer Aufbau, Benachrichtigung per E-Mail/SMS, HTML-Ergebnisaus-lieferung, industrieller Standard zum Monitoring einer IT-Infrastruktur: ► http://www.nagios.org
Net-SNMP (ehemals UCD-SNMP)	Primäres Tool, bekannt seit 1992, heute umfangreiche Suite, SNMP-Bibliotheken und -Agenten, MIB-Browser, Implementierung in C: ► http://www.netsnmp.org
Scotty	Tcl- Erweiterung für TMN (Tcl Network Managements), Unterstützung von SNMPv1, v2, Implementierung in C/Tcl, umfangreiches NM-Tool: ► http://wwwsnmp.cs.utwente.nl/
Telemetrybox	Ein Suite – All-in-one: ► http://www.telemetrybox.org



◘ **Abb. 20.19** MIB-Struktur mit OIDs

Die MIB-II stellt erste wichtige MIB-Erweiterung dar, da MIB-II Tabellenzugriff bietet. Viele Hersteller benötigen u. U. eigene MIBs. Die herstellerspezifischen MIBs verstehen unter sich Einbindung als Unterbaum in die MIB-II unter Knoten: „…private(4) enterprises(1) firma(x)“ (1.3.6.1.4.1.x).

Die folgenden OID-Beispiele können für MIB-II aufgeführt werden:

```
- 1.3.6.1.4.1.2 ibm Fa. IBM
- 1.3.6.1.4.1.9 cisco Cisco Systems, Inc.
- 1.3.6.1.4.1.11 hp Hewlett Packard
- 1.3.6.1.4.1.36 36 ehemals DEC
- 1.3.6.1.4.1.42 sun ehemals SUN Microsystems
(derzeit Oracle)
- 1.3.6.1.4.1.43 3Com 3Com
- 1.3.6.1.4.1.59 sgi Silicon Graphics, Inc.
- 1.3.6.1.4.1.63 63 Apple Computer, Inc.
- 1.3.6.1.4.1.71 71 NASA
- …
- 1.3.6.1.4.1.30000 30000 University of Western
Sydney.
```

Die folgenden SNMP-Protokollelemente [3, 4, 11] unterstützen das Netzwerkmanagement (◘ Abb. 20.20):

a) **Abwärts (ME → MA)**
   - SetRequest: Verändern Wert eines Attributes/eines MIB-Datensatzes (z. B. Änderung Puffergröße)
   - GetRequest: Lesen Wert/Abruf eines Datensatzes aus der MIB (z. B. Fenstergröße)
   - GetNextRequest: Anfordern Nachfolgeparameter/Abruf eines Datensatzes einer Liste (z. B. Zeile einer Routingtabelle)
   - GetBulk (ab SNMPv2): Anfordern mehrerer MIB-Werte/Abruf einer größeren Datenmenge (z. B. Routingtabelle)

b) **Aufwärts (MA → ME)**
   - GetResponse: Antwort auf Get…
   - Trap: unaufgeforderte Ausnahmemeldung des Agenten (z. B. Fehleranzeige)
   - Inform: wie Trap, muss aber durch Manager quittiert werden (ab SNMPv2)

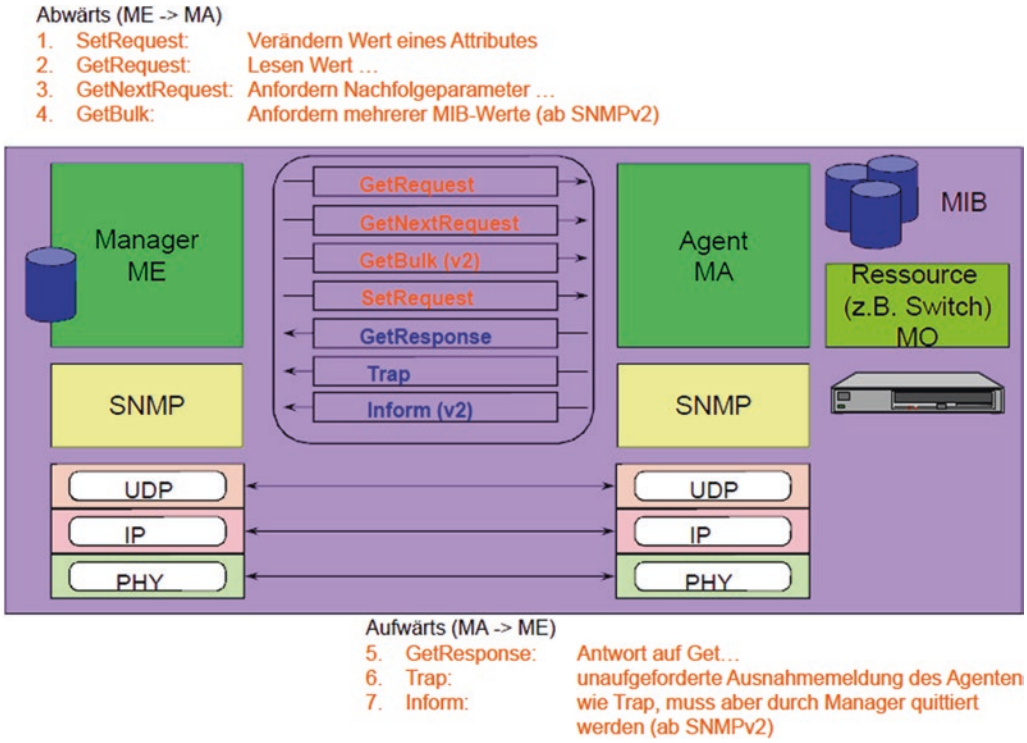


Abb. 20.20 Agent-Manager-Architektur

20.6 Virtualisierung in Rechnernetzen

Heutzutage wird Virtualisierung in diversen Formen [1, 5, 10, 11, 14, 15, 18, 19] für individuelle (Netzwerk-)Services, Applikationen und Ressourcen von Betriebssystemen (BS) eingesetzt. Weiterhin betrifft die Virtualisierung komplette BS, Mikrokontrollerarchitekturen, Speicher und Netzwerke sowie Multiprozessor- und Multicomputercluster [17–19]. Preisgünstige virtuelle Server können außerdem für Webhosting, Authentisierung und Enterprise Application Integration (EAI) angewandt werden. In manchen Fällen ersetzen virtuelle Server eines Dienstanbieters die gesamte IT-Infrastruktur eines KMU (Klein- oder Mittelstandsunternehmen, engl.: Small and Medium-sized enterprises, SME). Dieser Ansatz führt zu einer signifikanten Kostenreduktion und nennt sich IT-Outsourcing.

20.6.1 Virtualisierung als Abstraktionsverfahren

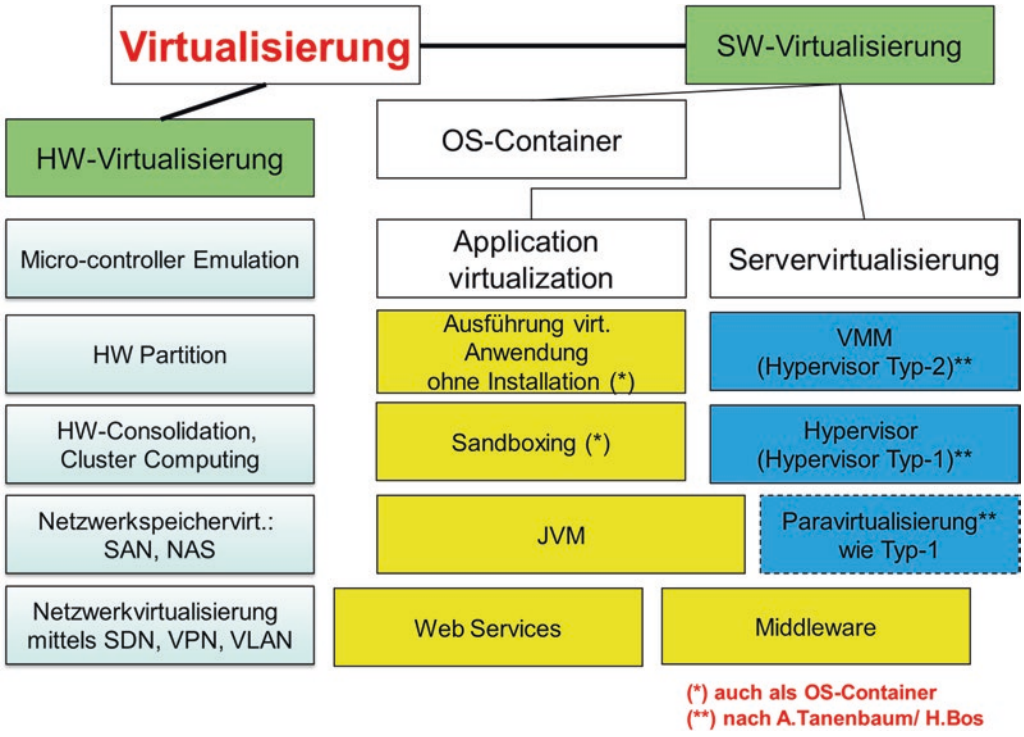
Unter Virtualisierung versteht man Methoden zur Abstraktion [15, 17, 18], die es erlauben, dem Nutzer scheinbar verfügbare

Ressourcen so bereitzustellen, als wären sie in der Realität vorhanden. Virtualisierung ist weiterhin eine der Hauptaufgaben moderner Betriebssysteme und wird eingesetzt, um Beschränkungen der realen Hardware/Software/Netzwerke zu verbergen (◘ Abb. 20.21).

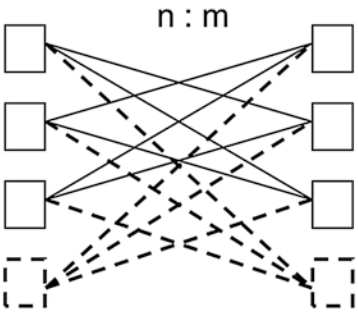
Die Virtualisierungskonzepte sind z. B. Multitasking/Multithreading, virtuelle Prozessoren (prozessorunabhängige Software-Entwicklung für Mikrocontroller), Java Virtual Machine (JVM, betriebssystemunabhängige Bytecode-Interpretation), plattformunabhängige Dienste (Webservices) und serviceorientierte Anwendungsarchitekturen, virtuelle Sekundärspeichersysteme (NAS oder SAN) und virtuelle Netzwerke (VLAN, VPN oder SDN).

Beispiel 20.6

In einem Betriebsnetz mit 30 Computern existieren 3 verschiedene Architekturen (◘ Abb. 20.22). Bei heterogenen Rechnerarchitekturen ist eine Verständigung der Computer nicht selbstverständlich, da sich die Datendarstellungen unterscheiden können, z. B. ist die Darstellung von Integer-Werten architekturabhängig. Im konkreten Beispiel müssen für jede der drei Rechnerarchitekturen zwei Import- und zwei Exportroutinen programmiert werden, also insgesamt 12 Routinen. Auf jedem Rechner müssen 4 Import- bzw. Exportroutinen



◘ **Abb. 20.21** Virtualisierungsarten [10, 11, 18]



a)

3 Architekturen;

jeder Rechner benötigt 2 Import- und 2 Export-Routinen

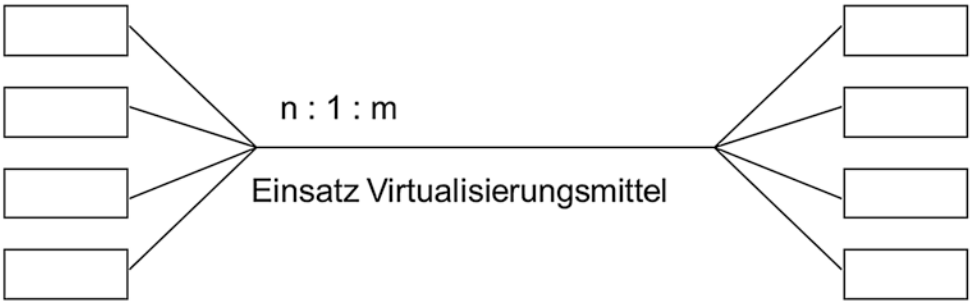
12 x programmieren; 120 x installieren

b)

4 Architekturen;

jeder Rechner benötigt 3 Import- und 3 Export-Routinen

24 x programmieren; 186 x installieren



c) je System nur noch 1 Import- und 1 Export-Routine

8 x programmieren; 62 x installieren

Abb. 20.22 Aufwand wird reduziert: ohne und mit Virtualisierung!

installiert werden, insgesamt sind es 120 Installationen. Bei einer Netzerweiterung muss erneut eine Vielzahl von Routinen programmiert und installiert werden. Falls im o. g. Beispiel nur ein Rechner mit einer neuen Architektur hinzukommt, sind insgesamt 24 Programmierungen von Routinen und 186 Installationen erforderlich. Die Netzerweiterung bedeutet damit einen Arbeitsaufwand von 12 Programmierungen und 62 Installationen. Dies stellt einen enormen Aufwand dar. Erschwerend kommt hinzu, dass es schwierig ist, für alle Rechnerarchitekturen geeignete Experten zu finden.

Durch Nutzung von virtuellen Maschinen kann der Aufwand wesentlich gesenkt werden, indem einheitliche Transferdarstellungen verwendet werden. Im o. g. Beispiel wären zum Ausgangszeitpunkt nur 3 Import- und 3 Exportroutinen zu programmieren und es müssten nur 60 Installationen vorgenommen werden. Die Netzerweiterung wäre vergleichsweise

einfach, da nur für jeden neuen Rechner eine Importroutine von der Transferdarstellung und eine Exportroutine in die Transferdarstellung programmiert werden muss und nur zwei Installationen durchgeführt werden müssen. Positiv ist weiterhin, dass für die Erweiterung keine Kenntnis über die anderen Rechnerarchitekturen erforderlich ist. Insgesamt ergibt sich eine erhebliche Einsparung an Kosten und Arbeitszeit.

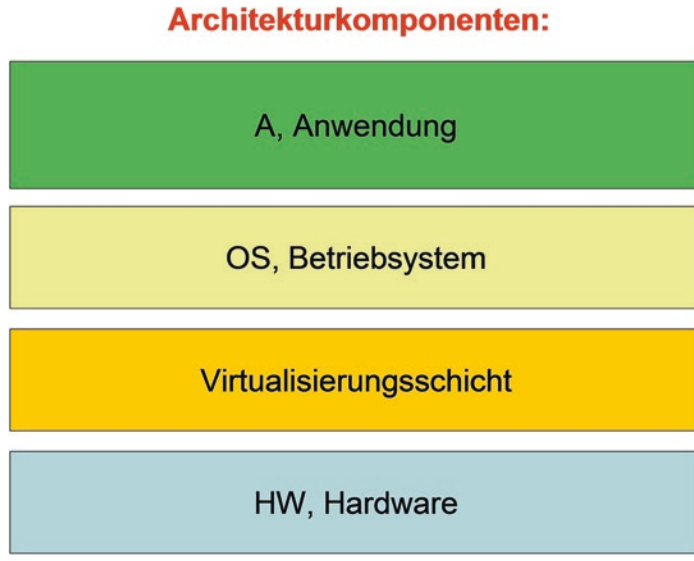
Mit Virtualisierung bezeichnet man die Methoden zur Schaffung einer logischen Abstraktionsschicht zwischen Ressourcen und Applikationen. Generell hat der Virtualisierungsansatz eine Schichtenarchitektur (◘ Abb. 20.23).

Die möglichen Virtualisierungstechniken zu den Betriebssystemen (BS bzw. OS) werden in ◘ Abb. 20.24 dargestellt. Diese sind [10, 11, 18]:

- OS-Container (effiziente Lösung bei eingeschränkter Funktionalität)
- VMM (Virtual Machine Monitor, oder manchmal auch ***Hypervisor Typ-2*** zur Verwaltung von ***VMs***)
- „reiner" Hypervisor (also***Typ – 1***).

20.6.2 Heterogene virtuelle Betriebsysteme

Die einfachste, aber ungenügend transparente Virtualisierungstechnik heißt OS-Container. Im Rahmen der Virtualisierung wird die ganze Laufzeitumgebung (Runtime Environment)



◘ **Abb. 20.23** Schichtenarchitektur zur Virtualisierung [11]

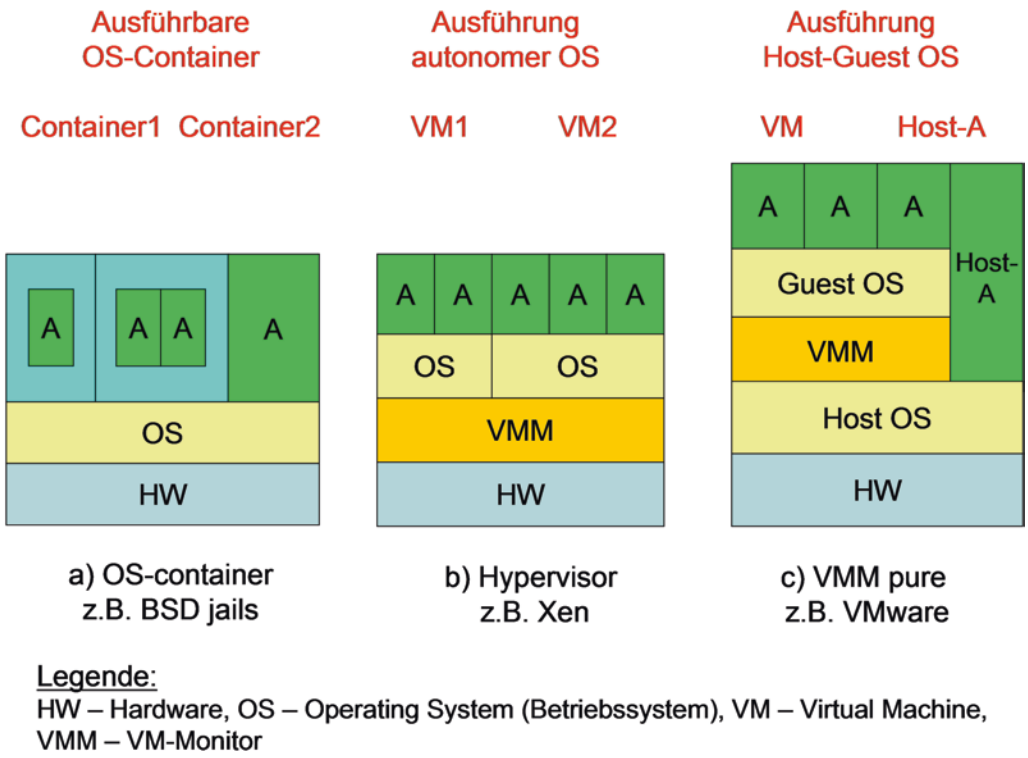


Abb. 20.24 Virtualisierung: OS-Container, VMM (Hypervisor Typ – 2) und Hypervisor (Typ – 1)

innerhalb eines geschlossenen Containers emuliert. Keine zusätzlichen BS müssen gebootet werden und es läuft nur ein OS-Kern (engl.: kernel). Der OS-Container ist somit Teil des Host-OS. Der Vorteil dieser Technik liegt in einer guten Integration von OS-Container und Gast-OS. Als Nachteil des Konzeptes kann man eine gewisse Verschlossenheit (engl.: jail = „Gefängnis“) vermerken, die es nicht erlaubt, Zusatztreibersoftware oder Kerne zu laden. Systembeispiele für OS-Container sind Open Solaris Zoning, BSD jails, OpenVZ, Virtuozzo, Linux-VServer [10, 11, 18].

Eine VMM-Lösung (Virtual Machine Monitors, oder Hypervisor Typ – 2 [18]) ermöglicht die Koexistenz diverser Gast-OS (z. B. UNIX, Linux und Windows) auf dem Host-OS. VMM wird durch zwei folgende Methoden implementiert,

- als Anwendung, die neben anderen Anwendungen auf dem Host-OS läuft und die die komplette reale Hardware für die Gast-Systeme emuliert, allerdings mit Leistungseinbußen (z. B. VMware Workstation, Microsoft Virtual PC)
- bzw. als Hypervisor Typ – 1 [18] („Meta-Betriebssystem“).

Wenn die Gastsysteme an den Hypervisor angepasst sind, spricht man von Paravirtualisierung, bspw. mittels Xen [18]. Dem Hypervisor ist der Typ 1 einzuordnen, wobei der Laufzeitverlust hier relativ gering ist. Vollständige Virtualisierung kostet im Allgemeinen etwas mehr Zeit, verlangt aber keine Anpassung der Gastsysteme [10, 11, 15, 18].

20.6.3 Servervirtualisierung. Dienste und dedizierte Server

Ein virtueller Server verhält sich den Nutzern gegenüber wie ein realer physikalischer Computer [11]. Ein virtueller Server ist ein Server, der seine Dienste für mehrere Bereiche/Domains anbietet. Er verhält sich dabei aus Anwendersicht wie ein echter Server, ist in Wirklichkeit jedoch kein eigenständiger Server sondern eine Instanz eines übergeordneten Servers (Gastgeber-System). I.d.R. residieren mehrere virtuelle Server (Gast-Systeme) auf einem Gastgeber-System. Man spricht in diesem Fall beim Gastgeber-System von einem Shared Server, also einem Server, den sich mehrere Gäste (Virtuelle Server) teilen. Prominente Beispiele sind Webserver, die mehrere hundert separate Webauftritte beherbergen können oder Mailserver, die Mails für mehrere Domains annehmen. Virtuelle Server erlauben den Betrieb mehrerer wenig belasteter Server auf einem Host, was die Host-basierten Kosten im Vergleich zu Servern auf dedizierten Hosts drastisch senken kann. Wenn die virtuellen Server nicht gleichzeitig Lastspitzen erfahren, ermöglicht dies zudem eine Überbuchung von Speicher und Prozessor.

Ein (virtueller) dedizierter Server ist ein Server, der nur für eine Tätigkeit abgestellt wird (dedicated service) oder nur einem Kunden zugeordnet ist (dedicated customer). Dedizierte (physikalische/virtuelle) Server (◘ Tab. 20.5) kommen zum Einsatz, wenn:

- die angebotenen Dienste für einen Shared Server zu viele Ressourcen in Anspruch nehmen.
- der Betrieb bestimmter Serverdienste die Betriebssicherheit anderer Shared Server auf dem Rechner gefährdet.
- der Server spezielle Sicherungsmaßnahmen erfordert.
- der Kunde eine Software nutzen will, welche vom Provider bzw. dessen Shared Servern nicht unterstützt wird.

Als Managed Server werden (virtuelle) Hosts bezeichnet, deren Betriebssysteme und Software SW (Server) von einem Dienstanbieter permanent überwacht und aktualisiert werden. Managed Server sind eine flexible und kostengünstige Lösung.

Tab. 20.5 Dienste und dedizierte Server [11]

Servertyp	Zugehörige Protokolle
Authentication Server	RADIUS
Chat Server	IRC
File Transfer Server	FTP
File Server	NFS
Datenbankserver	SQL
DHCP Server	DHCP, Intranet, IP, NAT, PAT und Mobile IP
Game Server	TCP/IP
Mailserver	SMTP, MIME, POP3, IMAP
Nameserver	DNS
Proxyserver	VPN, IPsec, SNMP, Intranet, FW
Streaming Server	SIP/RTP/Codecs
Time Server	NTP
Webserver	HTTP, HTTPS, SOAP, REST

20.6.4 Sandboxing

Eine virtuelle Produktgruppe, die in den letzten Jahren immer häufiger in Verbindung mit NW-Sicherheit und erweiterter Malware-Erkennung in Verbindung gebracht wird, ist Sandboxing. Ein ähnlicher Begriff ist „Sandboxie" für ein Computerprogramm, das eine sogenannte „Sandbox" (Container) bereitstellt, die es ermöglicht, Programme/Apps isoliert (virtualisiert) vom BS auszuführen.

Sandboxing ist eine Technologie, bei der eine Anwendung/App/Webdatei in einer abgesicherten und in sich geschlossenen Umgebung (Container) ausgeführt und auf schadhaftes Verhalten untersucht wird. Dies geschieht über aufeinanderfolgende Verfahren (Layering), die Schritt für Schritt abgearbeitet werden (s. Abb. 20.25):

1. Das initiale Scannen der Datei mittels eines Virenscanners (Malware-Engine) über signaturbasierende Verfahren.
2. Dynamische Codeanalyse (durch Browser, JVM etc.) sowie ein Reputationsabgleich.
3. Angeforderte Berechtigungen der Programme/Apps werden angezeigt und bedürfen der Zustimmung des Nutzers
4. Hier erfolgt eine Emulation des Codes, bei der im 1.Schritt eine statische und im 2. Schritt eine dynamische Code-Analyse vorgenommen wird. Hierbei wird untersucht, wie sich die SW auf einem Client verhalten würde und was das Programm (App) nach einer erfolgreichen

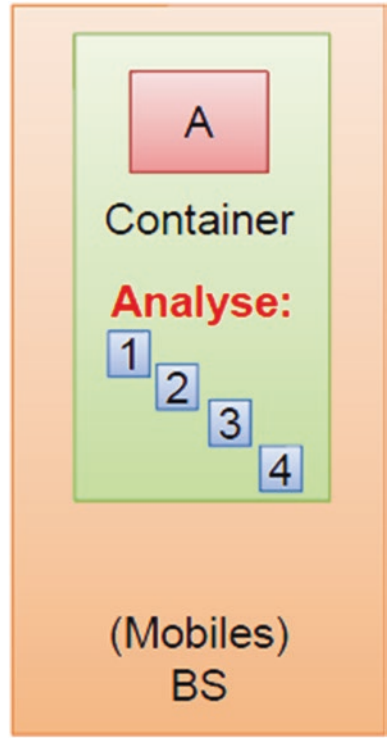


Abb. 20.25 Prinzip von Sandboxing

Ausführung bewirkt. Allerdings beansprucht diese Analyse Zeit, sodass Systeme, anders als bei Firewalls, Web Gateways oder Intrusion-Prevention-Systemen, nicht immer inline arbeiten.

Ein standardmäßiges Sandboxing unter Android und iOS bietet den Usern weitere Sicherheit, weil alle Apps in einem Container oder JVM/Dalvik VM abgetrennt und abgesichert laufen. Die aufgeforderten Berechtigungen für Apps werden angezeigt und bedürfen immer der Zustimmung des Nutzers.

20.6.5 Gegenüberstellung von Virtualisierungsprodukten. Fortgeschrittene Virtualisierungskonzepte

Äquivalent zur römischen Herrschaftsstrategie „Divide et Empera" sind bei der Virtualisierung die Konzepte der Ressourcenaufteilung (Partition) und -Vereinheitlichung (Consolidation) immer wichtig [18]. Außerdem sind die Virtualisierungsprodukte teilweise

Freeware und teilweise kostenpflichtig. Manche davon stellen in sich proprietäre Verfahren dar, die an bestimmte Techniken orientiert sind (Hyper-V).

Einige der darzustellenden Methoden und Produkte sind als physikalische Server einsetzbar (WMware Server, Hyper-V Virtual Server, Citrix Xen Hypervisor) [10, 11, 18]. Die Virtualisierungsprodukte werden auch für Cloudlösungen und SDN (Software-Defined Networking) eingesetzt.

Wesentlich leistungsfähiger ist die Produktklasse IBM LPAR mit Schnittstellen zu leistungsstarken Mainframes unter dem Betriebssystem z/OS (Memory/Processor Resources Partition). Virtual Machine Monitors wie z. B. Sun Virtual Box repräsentieren eine simple, jedoch meist nicht die effizienteste Lösung.

Die am Markt führenden Ansätze sind in ◘ Abb. 20.26 abgebildet.

Die fortgeschrittenen Virtualisierungskonzepte sind [10, 11, 18]:

1. Storage Virtualization (SAN, NAS sowie OpenStack- Software)
2. Application Virtualization (breites Spektrum: von JVMs bis zu Webservices).
3. Network Virtualization (neben „klassischen" VPN, MPLS kommt das SDN – Software Defined Network zu breitem Einsatz, OpenStack- Software sowie Software-Defined WAN).
4. Gemischtes Backup: gemeinsame Images von Daten und VMs, abwechselnder Betrieb von Vollbackup, differentiellem und Inkrementellem Backup, schnelleres VM-Deployment und VM-Migration).
5. Als Ergebnis: Bessere Integration von Clouds in die virtualisierte Landschaft und umgekehrt, von Virtualisierungskonzepten in den Clouds.

◘ Abb. 20.26 Wichtige Virtualisierungsprodukte am Markt. (Quelle: Wikipedia, eigene Zusammenstellung)

Einige Details dazu werden im Folgenden präsentiert. Im Bereich IT-Outsourcing und Cloud Computing sind die Produkte von VMware und Citrix unschlagbar.

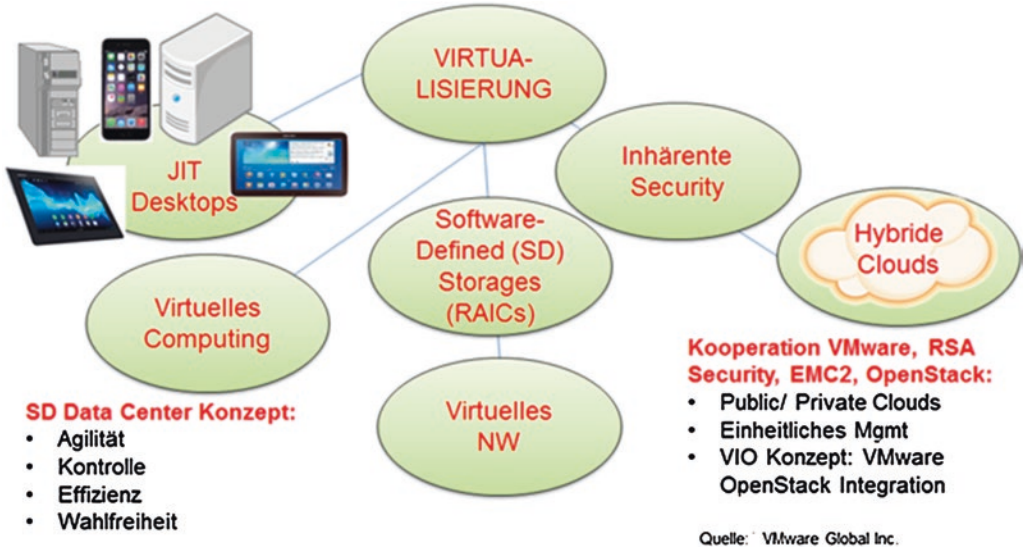
Beispiel 20.7. Citrix vs. VMWare

Das VMware-Konzept wurde in ◘ Abb. 20.27 repräsentiert und kann kurzfassend formuliert werden wie folgt (Quelle: ▶ http://www.vmware.com/):

- Jede Anwendung ist überall verfügbar; Entwicklung, Bereitstellung und Ausführung herkömmlicher und moderner Anwendungen; offenes Management
- Flexibilität beim Management der Cloud-Infrastruktur und Anwendungen
- Einheitliche Plattform
- Interne und externe Cloud mit einer gemeinsamen Software-Defined Data Center-Plattform basierend auf branchenführenden Computing-, Netzwerk- und Storage-Virtualisierungsverfahren.

Das „Citrix Motto" besteht aus den Positionen (Quelle: ▶ http://www.citrix.com):

- Virtualize Windows desktops and apps
- Secure apps and data
- Collaborate from anywhere
- Optimize the network
- Leverage the cloud.



◘ **Abb. 20.27** Konzept der Virtualisierung mit VMware

Integration mittels eines hybriden Hypervisors für diverse Server (u. a. Citrix, VMWare, Hyper-V, …) verschiedener Hersteller ist in ◘ Abb. 20.28 repräsentiert. Die Storage Snapshots ermöglichen sofortiges Backup oder Deployment mehrerer Ziel-VM, die für ein bestimmtes Virtualisierungskonzept zugeschnitten sind [10].

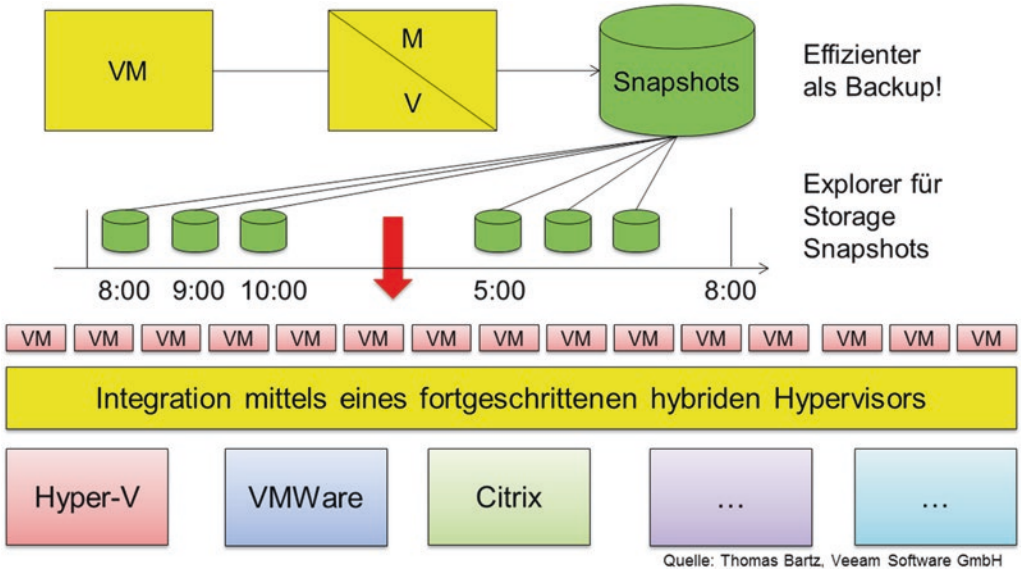
20.6.6 SDN – Software-Defined Networking

Wie erfolgt die Netzwerkvirtualisierung? Ähnlich wie BS-Virtualisierung, Server- oder APL/App-Virtualisierung!

Software-Defined Networking (SDN) bedeutet die Erzeugung von Computern, Netzwerk-Geräten und Software, wobei die APL und NW-Geräte voneinander abstrahiert werden [10]. Dabei verwendet man das Schichtenmodell für SDN (s. ◘ Abb. 20.29a) und für Netzwerk ohne Virtualisierung (s. ◘ Abb. 20.29b):

1. APL Plane: Anwendungsschicht
2. SDN Control Plane: Managementschicht
3. Infrastructure Plane: Datenebene mit NW-Geräten
4. i. d. R. OpenFlow-Protokoll: um L2/L3-Netze mit VMs zu verbinden und koordinieren. Als Alternative wird das VMware-spezifische Protokoll VXLAN (Virtual Extensible LAN).

Kurze Historie: Erste Konzepte stammen 2005 von der Stanford University. Seit 2013 wird SDN von mehreren Herstellern eingesetzt, sodass bereits von einer Hype-Periode gesprochen wird!



◘ **Abb. 20.28** Integration mittels eines hybriden Hypervisors

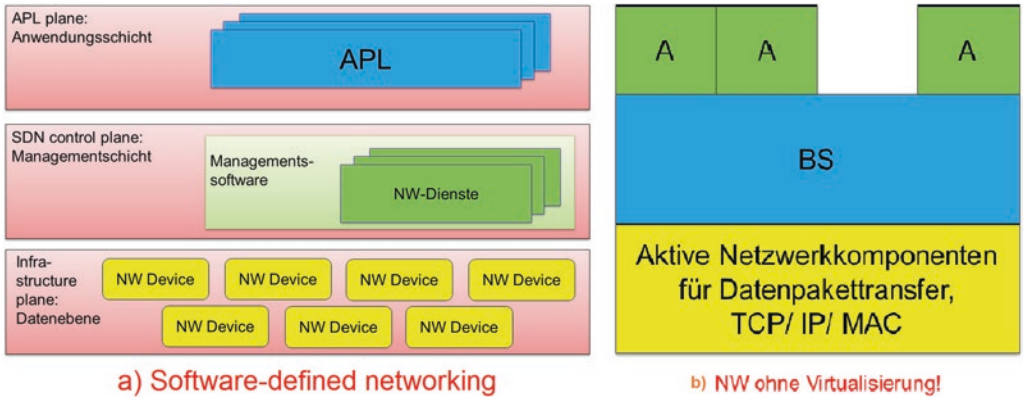


Abb. 20.29 Software-Defined Networking (**a**) im Vergleich zum physikalischen Netzwerk (**b**)

Die Wegbereiter sind die folgenden Firmen und Konsortien: VMware, EMC2, Cisco, HP, IBM, Juniper, Brocade, OpenStack etc. Die Zahl der SDN-Anbieter im Markt steigt mittlerweile rasant an. Das effiziente SDN-Verfahren ermöglicht ein einfacheres Low-Level-Management der Netzwerke durch ihre Abstraktion in die virtuellen Dienste. Die Motivation zum Ausbau von SDN läßt sich folgendermaßen erklären. Die Probleme von performanten physikalischen Netzwerken liegen heutzutage in:

- Inflexibilität von traditionellen PHY-Netzwerken
- mäßige Eignung zu den ständig ändernden Geschäfts-APL und Cloud-Services (IoS).
- Heterogenität: heutzutage werden die Anwendungen i. d. R. auf mehrere VMs verteilt, die untereinander intensiv kommunizieren.
- um die Arbeitslast von Servern zu optimieren (Load Balancing) migrieren die VMs oft, was die „Binding Points" für den NW-Verkehr heftig ändert.
- konventionelle Adressierungsschemata, feste logische Trennung in VLANs mit den VLAN-Verkehrsregeln sind in solchen dynamischen Umgebungen zu ineffizient!

Fazit: SDN-Einsatz mit der Verwendung der NW-Virtualisierungstechnologien ist hier erforderlich.

Beispiel 20.8

Durch Einsatz nur von einer neuen VM kann der Rekonfigurationsprozess für alle ACL auf allen Netzwerkgeräten und Ebenen in einem größeren Netzwerk mehrere Stunden dauern. Der Grund dafür besteht in der Ausrichtung von bestehenden Management-Tools auf konkrete Geräte aus einer Modellreihe von einem bestimmten Hersteller.

In software-definierten Netzwerken (SDN) lassen sich Zonen einrichten, die unter anderem für die Realisierung der User-abgrenzung/Mandantenfähigkeit (Multitenancy) eines Cloud Services erforderlich sind.

Trotz Diversität proprietärer Lösungen kommen OpenFlow und VXLAN zur engeren Protokollwahl [10].

- Zur Unterstützung des SDN verwendet OpenFlow-Protokoll die s. g. Flow Charts (Tabellen) zur Angabe von notwendigen Aktionen mit den Frames/Paketen bzw. zur Adressentranscoding (MAC, IP, Port) in einem virtualisierten Netzwerk von OpenFlow.
- VXLAN ist die Grundlage für die Einrichtung elastischer, portabler, virtueller Datacenter, die jedem Mandanten eine eigene Schutzzone bieten (VMware).
- VXLAN bietet zahlreiche Vorteile, die sich aus seiner speziellen Funktionsweise ergeben. VXLAN erstellt logische Layer-2-Netzwerke, die in Layer-3-Standard-IP-Paketen gekapselt werden. Durch diese Kapselung entstehen logische VXLAN-Netzwerke. Sie unterscheiden sich voneinander anhand einer Segment-Identität in jedem Frame, sodass keine VLAN-Tags erforderlich sind. Dies ermögliche die Koexistenz einer sehr großen Anzahl von isolierten Layer-2-VXLAN-Netzwerken in einer gemeinsamen Layer-3-Infrastruktur. Konkret handelt es sich bei dieser sehr großen Anzahl um 16,7 Millionen logische Netzwerke, die ein MSP einrichten könnte – eine ganze Menge Mandanten, die ein MSP (Managed Service Provider) verwalten könnte.

Fazit: SDN-Einsatz mit der Verwendung der NW-Virtualisierungstechnologien ist unbedingt erforderlich. Veranschaulichen wir noch ein folgendes Beispiel dazu.

Beispiel 20.9. SD-WAN – eine WAN-Virtualisierung (basierend auf den Materialien von R. Frenzel, IBH IT Service, Hausmesse am 16.03.2017)

Ein solches SD-WAN fasst mehrere PHY-Leitungen zu einer virtuellen zusammen und ermöglicht den Aufbau eines UDP-Tunnels für userspezifische Anwendungen. Die Virtualisierungssoftware NetScaler SD-WAN von Citrix überwacht die Verfügbarkeit, Latenzen und Jitter der PHY-Leitungen (◘ Abb. 20.30).

Fazit: Die Vorteile einzelner Leitungen (MPLS, LTE, DSL) sind hier zu kombinieren (◘ Tab. 20.6).

Die kombinierten Vorteile dieser Lösung mit SD-WAN sind wie folgt:

1. Priorisierung geschäftskritischer Anwendungen
2. Priorisierung von Verbindungen möglich
3. Funktionen wie TCP Flow Control und Datenkomprimierung

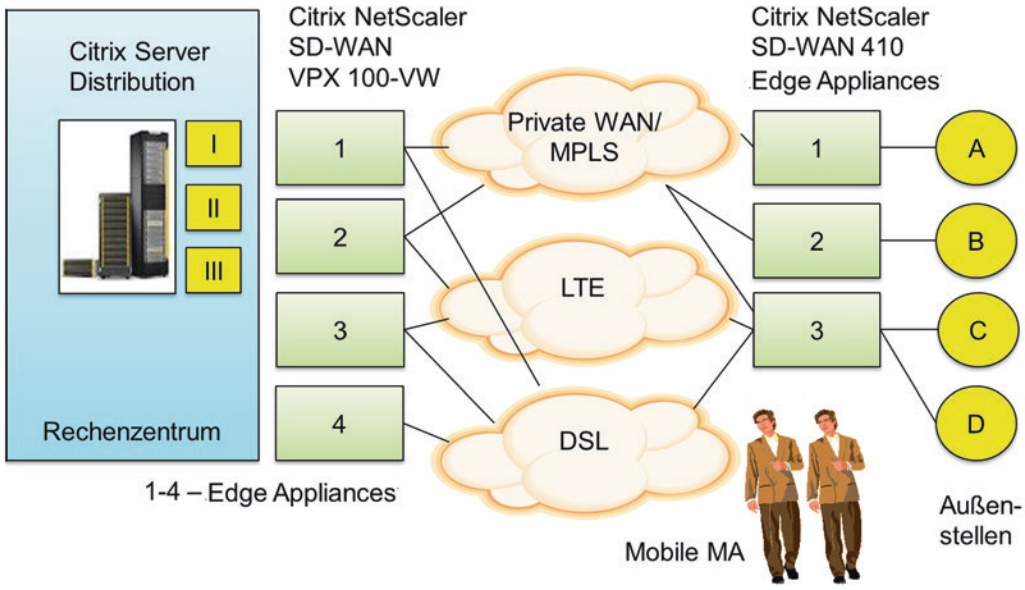


Abb. 20.30 WAN-Virtualisierung. (Quelle: R. Frenzel, IBH IT Service, Hausmesse am 16.03.2017)

Tab. 20.6 Virtuelles Weitverkehrsnetz (Software-defined Wide Area Network) mit MPLS, LTE, DSL (basierend auf den Materialien von R. Frenzel, IBH IT Service, Hausmesse am 16.03.2017)

Netzwerktyp	Vorteil	Nachteil
MPLS-Leitungen	Hohe Verfügbarkeit, QoS, konstantes Jitter	Aber: geringere DR, hohe Kosten
DSL-Leitungen	Hohe DR bei relativ geringeren Kosten	Aber: großes, schwankendes Jitter, schlechtere Verfügbarkeit
LTE-Verbindungen	Hohe DR	Aber: Kosten abhängig vom Provider und Nutzungsintensität (Tarif)

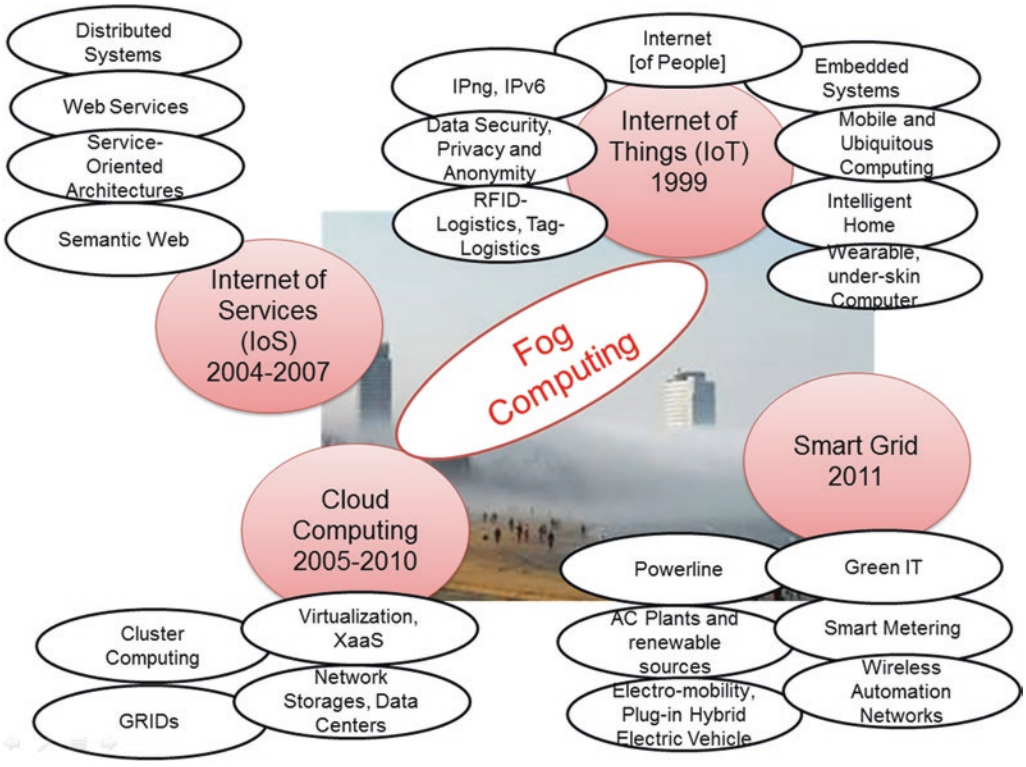
4. Protokolloptimierung und Dynamic Routing
5. Einfache Integration in die vorhandene Infrastruktur
6. Verschlüsselung für alle Datenpakete per IPsec mit AES 256 Bit
7. Einfaches Management mittels Citrix NetScaler Insight Center
8. Analyse durch AppFlow-Datenberichtsformate
9. Hochverfügbares und kostengünstiges virtuelles WAN

20.7 Fortgeschrittene Konzepte. Internet der Dinge und Fog Computing. Industrie 4.0. Blockchain

20.7.1 Begriffsklärung

Der Begriff „Internet der Dinge“ (Internet of Things, Kurzform: IoT) beschreibt, dass die per IP vernetzten Gadgets (Laptops, Tablets, Smartphones) zunehmend verschwinden und durch „intelligente Gegenstände“ ersetzt werden. Statt selbst Gegenstand der menschlichen Aufmerksamkeit zu sein, soll das IoT den Menschen bei seinen Tätigkeiten unmerklich unterstützen. Die immer kleineren eingebetteten Kontroller sollen Menschen im Alltag unterstützen, ohne abzulenken oder überhaupt aufzufallen.

So werden z. B. sogenannte Wearables direkt in Kleidungsstücke eingearbeitet. Weiterhin werden intelligente Gebäudetechnik (Intelligent Home), eingebettete Gerätschaften (Embedded) mit unterschiedlichen Sensoren (Bluetooth, RFID, 6LoWPAN, …) ausgerüstet (◘ Abb. 20.31). IoT ist außerdem die richtige Lösung bei



◘ **Abb. 20.31** Internet of Things in Zusammenhang mit Clouds, Webservices und Energieeffizienz

den Anwendungen, die Echtzeit voraussetzen, wie Industrie-Automatisierung, Transport, Video Streaming etc.

Laut der Vorhersage von Gartner Inc. wird Internet of Things (IoT) etwa 25 Mrd. Geräte im Jahre 2025 vernetzten. Aber schon heutzutage mit dem IoT in der Kindheitsphase konkurrieren zahlreiche vernetzte Geräte weltweit um die Datenpipelines in die Clouds aufgrund der großen Datenmenge („Big Data" Problematik).

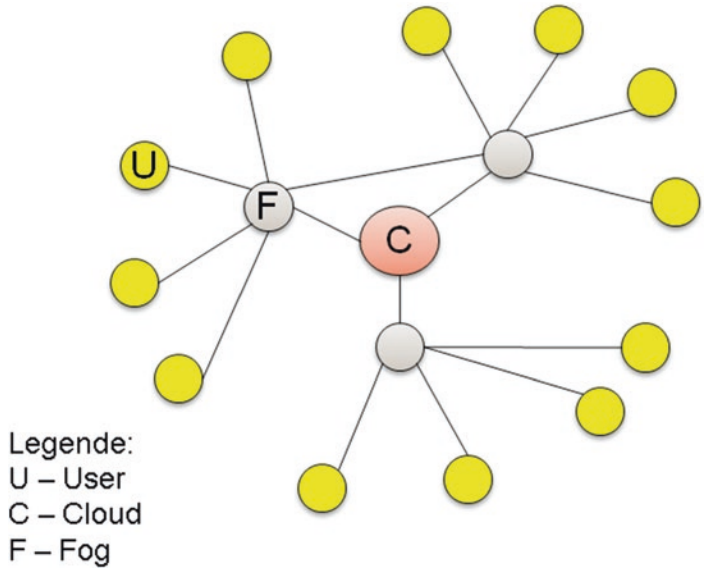
Mit anderen Worten bedeutet das: Myriaden von kleinen energieautarken Knoten werden unter einander vernetzt, so das eine „nebelige" Infrastruktur entsteht [10].

Viele Geräte sind fast permanent mit der Cloud verbunden und immer mehr wird in die Cloud verlagert. Dadurch entsteht das Problem mangelnder Bandbreite. Hier kommt das Fog Computing ins Spiel (◘ Abb. 20.32). Der Begriff „Fog Computing" wurde ursprünglich durch Cisco eingeführt.

„Nebel" agiert hauptsächlich wie eine Bridge zwischen IoT mit angekoppelten Geräten und Remote Datenzentren. Die Lösung zu diesen riesigen Datenvolumen, die in den Datenzentren geöffnet und verarbeitet werden, sind intelligente Kontroller und Gateways, die Daten von aktiven Geräten in deren unmittelbaren Nähe (laut Jack Pouchet, Emerson Network Power, 2016) vorverarbeiten.

20.7.2 Kooperation Fog-Cloud

Fog Computing („Fog" im Englischen „Nebel", „Trübheit") erweitert das Paradigma des Cloud Computing bis auf einen



◘ **Abb. 20.32** Architektur: User-Fog-Cloud

[intelligenten] Netzwerkknoten (Mikrokontroller auf Radio Network Edges) und erlaubt dadurch eine Reihe von neuen Anwendungen, Apps und Services. Die folgenden Merkmale von Fog Computing sind wesentlich [10]:

- Low-Latency, Location-Awareness (schnelle Reaktivierung von Knoten)
- weite geographische Verteilung
- sehr große Anzahl von Knoten und Mobilität, IPv6 empfohlen
- führende Rolle von „Wireless Access“
- Streaming- und Realtime-Anwendungen
- Knotenheterogenität.

Die wichtigsten Funktionalitäten von Fog Computing sind (alles anwenderseitig):

- Datenerfassung vor Ort
- Zwischenspeicherungen
- Kleine Anwendungen (Apps) ausführen
- Kleine Vorberechnungen vor Ort zu verrichten.

Fog Computing bietet eine passende Plattform für Weiterentwicklung von IoT-Diensten auf der Basis von den folgenden bekannten und neuen Netzwerktechnologien:

- Wireless Sensor and Actuator Networks (WSNs): ZigBee, Bluetooth, EnOcean
- RFID (Radio Frequency Identification, oder kontaktlose Funkkommunikation)
- WLAN (IEEE 802.11 ac, ad, ah – Wi-Fi HaLow)
- 6LoWPAN (als Weiterentwicklung von ZigBee)
- 5G-Mobilfunk mit sehr weit ausgelegter Interoperabilität aufgrund der NFV (Network Functions Virtualization).

Mit dem Fog Computing werden die Services und Berechnungen an den „Rand des Netzwerks“ verschoben (zum User hin). Dabei muss ein Kompromiss gefunden werden zwischen partiellem oder komplettem Verschieben. Fog Computing heißt auch „Edge Computing“.

Auch IBM versucht mit einer ähnlichen Initiative, das traditionelle Cloud-basierte Internet umzugestalten bzw. an „den Rand“ zu verschieben. Wenn über „Edge Computing“ gesprochen wird, ist damit wortwörtlich der Rand eines Netzwerkes gemeint, die Peripherie, wo das Internet endet und die reale Welt beginnt. Datenzentren sind die „Zentren“ des Netzwerkes; kleine Kontroller und typische Gadgets wie Laptops, Smartphones, Tablets, Multimediaplayer, Überwachungskameras stehen „am Rand“.

Der Vergleich von Fog und Clouds ist in ◘ Tab. 20.7 zu entnehmen:

Tab. 20.7 Vergleich von Fog und Cloud Techniken [10]

Herausforderungen einer Cloud oder eines NW-Speichers	Wie dabei Fog helfen kann
Latenz als größtes Problem	+ weniger Hops
Mobilität bei der Datenerfassung beschränkt	+ Datenlokalität und lokale Caches
Bandbreitenbegrenzung	+ Vor-Ort-Bearbeitung
Zuverlässigkeit und Robustheit akzeptabel aber angesichts Big Data fraglich	+ Fast Failover
Reiner Datenspeicher ohne Metainformationen für Suche	+ Location Awareness

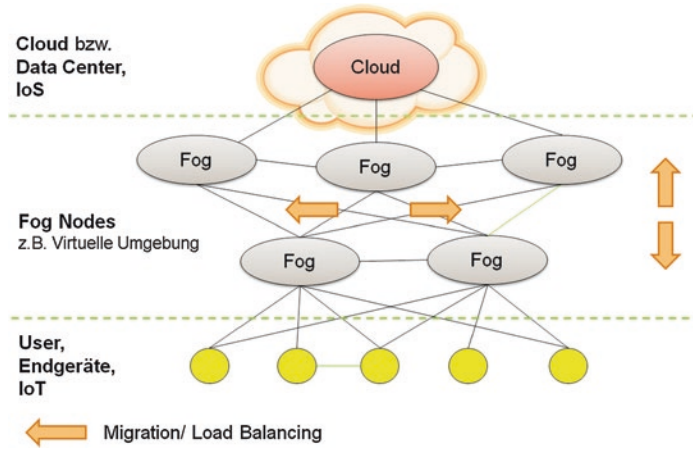


Abb. 20.33 Architektur von Fog Computing im Koexistenz zu Clouds: User + Fog + Cloud

Wie wird sich Fog Computing mittelfristig entwickeln? Der Nebel wird die Cloud nicht verdrängen. Die Frage ist nicht „Fog Computing vs. Cloud Computing", sondern es geht um die Koexistenz (Abb. 20.33).

Eine Beispielarchitektur für Fog Computing -Plattform und Applikationen repräsentiert Abb. 20.34.

Diese Architektur wird in fünf Layer (sog. Strata) eingegliedert. Die Clientapps für Endgeräte befinden sich auf der Layer 4 (Stratum 4) und verfolgen die Paradigmen von „Thin Client" (Cloud-centric), die für Smartphones und Tablets geeignet sind, bis zu „Fat Client" (Serverless Mobile Apps) für Robotik, Smart Stuff und Sensorpikonetze. Die Layer 3 (Stratum 3) bietet die Ausführungsplattformen und Web Services für

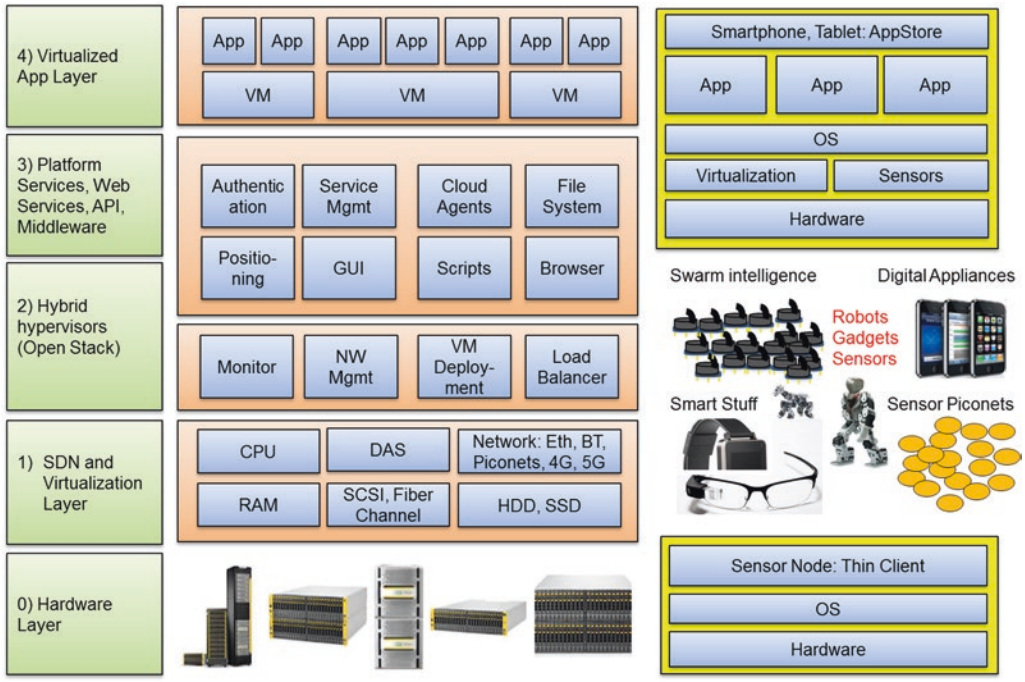


Abb. 20.34 Beispielarchitektur für Fog Computing -Plattform

einzelne Apps. Die Komponenten bauen auf Virtualisierung- und SDN-Technik auf (Layer 2/Stratum 2) sowie auf effizienter Hardware bzw. sog. „Composable Infrastructure", wie bspw. bei HPE-Produkten/HPE-Synergy: ► https://www.hpe.com.

Fog Computing weist viele Vorteile auf [10]:

- ermöglicht Big Data- und Echtzeitanalyse
- Energieeffizienz,
- Performance aufgrund physischer Nähe,
- geringere Datenströme über Internet als bei Cloud Computing,
- Sinkende Kosten bei der Datenverarbeitung (Big Data)
- Rechenleistung im Verhältnis zu Bandbreite immer günstiger (dank Raspberry Pi, Arduino Uno, Banana Pi, uvm.)
- Ersetzbarkeit bei Ausfällen
- geringere Transportkosten und geringere Latenzen
- verbesserte QoS,

aber der Datenschutz ist dabei fraglich. Die Verschlüsselung und der Einsatz von CIDN ist nachdrücklich zu empfehlen.

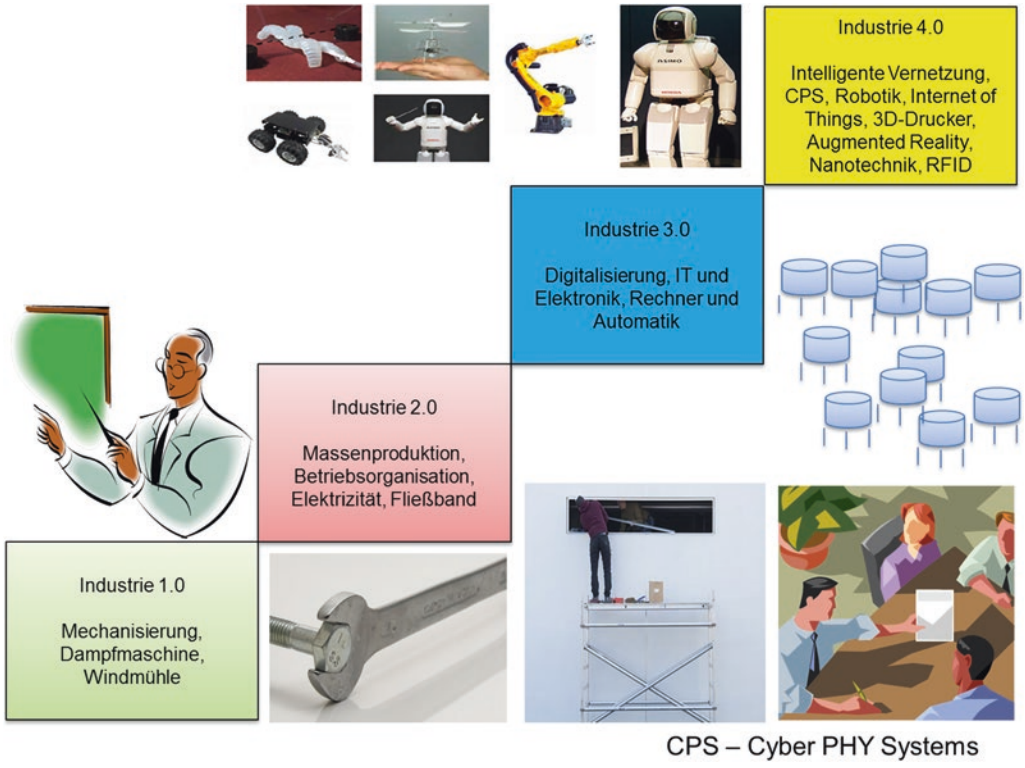
Dadurch wird Fog Computing zur treibenden Kraft für IoT. Mittelfristig wird IPv6 eingesetzt zur effizienteren Adressierung und zur Erhöhung der Datensicherheit. Die Security-Herausforderungen wachsen. Die Authentisierung

von angekoppelten Geräten in kombinierten Strukturen muss gewährleistet werden (User + Fog + Clouds). Die Verschlüsselung und digitale Signatur wird durch eine robuste Kombination von AES + RSA + PKI sowie den Einsatz von NG-FW und CIDN erreicht.

20.7.3 Industrie 4.0 und Blockchain

Industrie 4.0 (2011) ist ein zukünftiges wichtiges Ziel in der High-Tech-Strategie der Bundesregierung. Die treibende Kraft für die neue Generation der Industrie ist die weitere Automatisierung und Informatisierung von Produktionsprozessen (vgl. ◘ Abb. 20.35).

„In der Industrie 4.0 als Bundesregierungsprogramm werden Informations- und Kommunikations-, Automatisierungs-und Produktionstechnologien künftig stärker denn je miteinander verzahnt. Ziel ist es, den traditionellen Kern der deutschen Industrie mit seiner international herausragenden Position zu verteidigen und auszubauen!“ (nach VDMA-Projektmanager Jörn Lehmann. Wirtschaftsverbände arbeiten bei Industrie 4.0



◘ **Abb. 20.35** Kontext Industrie 4.0: „the four industrial revolutions“. (Eigene Darstellung)

eng zusammen, VDMA, id:979115, URL: ► http://www.vdma.org/article/-/articleview/979115).

Das Konzept setzt eine effiziente und energiesparende Vernetzung mit aktuellen Netzwerktechnologien (wie bspw. 6LoWPAN, 4G und 5G) voraus und verfolgt mehrere Ziele wie bspw. die Schaffung intelligenter Fabriken (Smart Factory) mit Adaptivität, Ressourceneffizienz und ergonomischen Arbeitsbedingungen. Die technologische Basis der Industrie 4.0 bilden die Cyber-Physical Systems (CPS) und das Internet der Dinge (IoT), vgl. ◘ Abb. 20.36.

Die Fertigungsprozesse werden nicht nur automatisiert (wie in Industrie 3.0) sondern die zu bearbeitenden Bauteile bekommen ihre zusätzliche „Intelligenz" durch die Ausrüstung mit preiswerten Chips (Prozessoren, Sensoren, drahtlosen Minisendern und RFIDs). Als weiteres Ziel geht es um die Integration von Kunden und Geschäftspartnern in einer optimierten Wertschöpfungskette durch deren weitgehende Vernetzung und unter der Berücksichtigung von Aspekten der Datensicherheit, Datenschutz und Anonymität [10] in diesen Ketten.

Ein weiterer wichtiger Trend in Rechnernetzen und Verteilten Systemen etwa seit dem Jahre 2010 ist der Einsatz der modernen Kryptotechnologie „Blockchain" (BC) unter Nutzung des Hash-Algorithmus SHA-256 von NIST zur Beschleunigung, Transparenz und Dezentralisierung von Finanztransaktionen sowie als vielversprechende digitale Zahlungsmittel (◘ Abb. 20.37) und Basis für die Kryptowährungen (vgl. Bitcoin, Monero, Ethereum).

Neben Kryptowährungen existieren heutzutage viele weitere BC-Anwendungen wie bspw. Smart Contracting. Für

◘ Abb. 20.36 Industrie 4.0 als Bundesregierungsprogramm. (Eigene Darstellung, Hintergrund: Google „Green Fabrics")

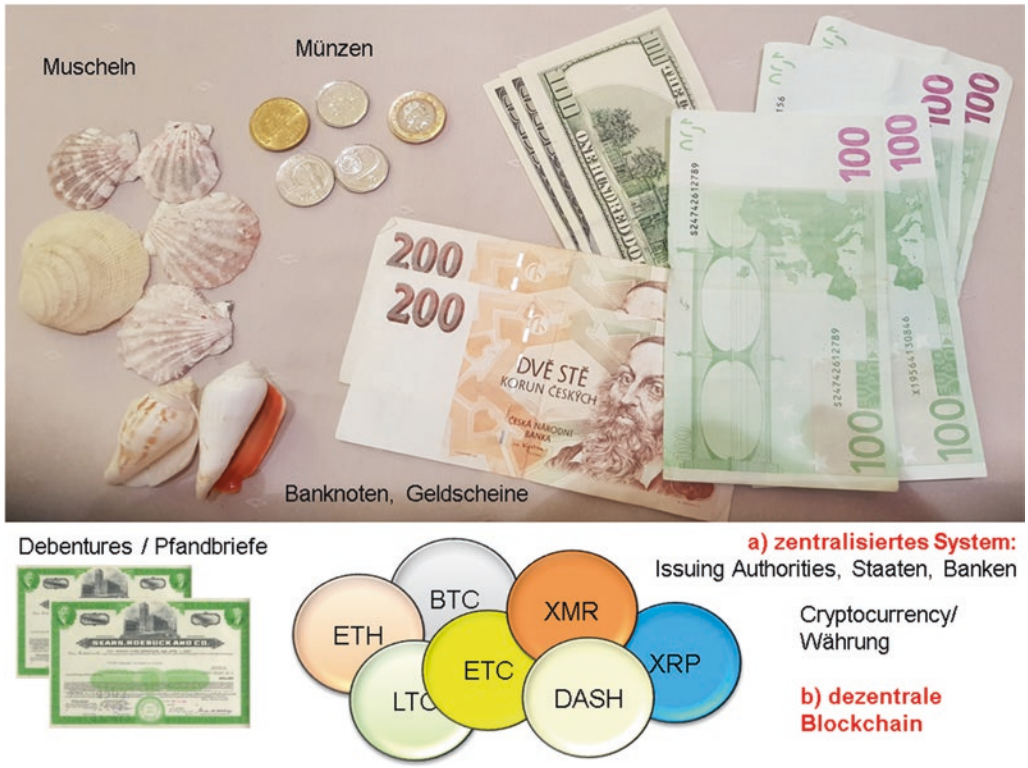


Abb. 20.37 Zentralisierte Zahlungsmittel und Blockchain-Kryptowährungen

die Smart Contracting (SC) gibt es die folgende Definition. Ein Smart Contract ist ein Vertrag auf der Software-Basis, bei dem unterschiedlichste Vertragsbedingungen hinterlegt werden können. Während des Vertragsverlaufs können bestimmte verknüpfte Aktionen selbsttätig ausgeführt werden, wenn ein entsprechender Auslöser vorliegt. Die Vorteile des Verfahren sind wie folgt:

- digital und rechtssicher
- basierend auf offener Digitalplattform
- transparent und zeitsparend
- ein rechtskonformer Vertrag wird in Blockchain angeboten und unterschrieben.

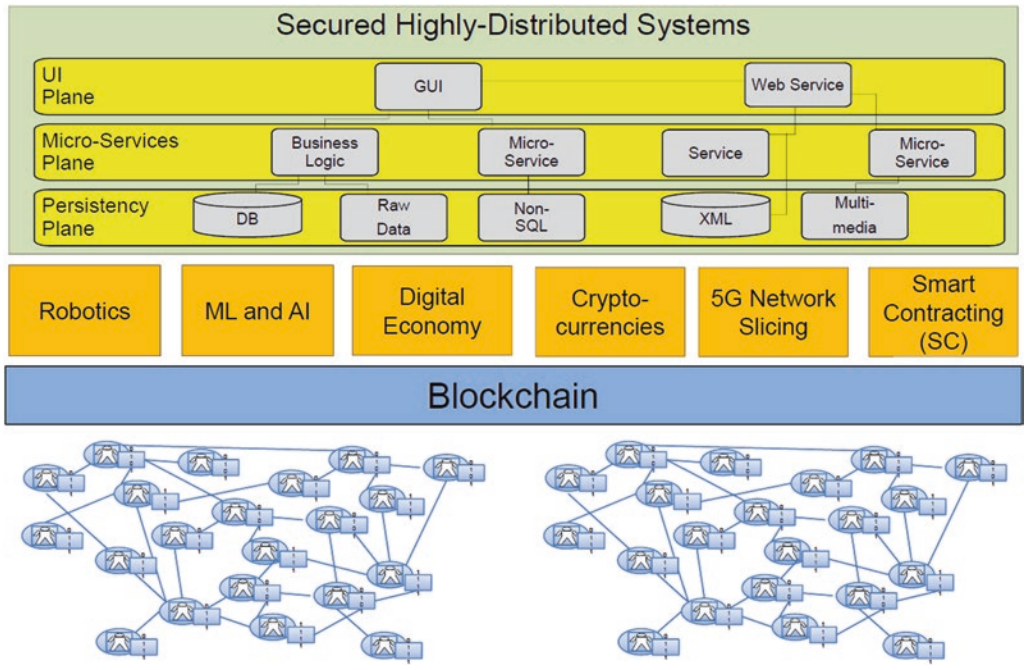
Wichtige Rolle wird die o. g. Technologie auch bei 5G-Applikationen und sog. hochverteilten Anwendungen (HDS, High-Distributed Systems) mittelfristig spielen. Die letzten haben oft eine sehr komplexe Struktur, die aus mehreren Funktionalitätsschichten (Planes) zusammengestellt und durch mehrere GUI, Komponenten und (Micro-)Services vertreten wird. HDS verwenden neben klassischen Algrorithmen auch die Ansätze der AI (Artificial

Intelligence) und ML (Machine Learning). Eine wichtige Rolle bei HDS spielt Energieeffizienz unter der Nutzung energiesparender Kommunikationsprotokolle und -Modelle (Cloud, Fog).

Die BC-basierten Frameworks ermöglichen profunde Blockchain-Integration in sog. HDS zwecks Erhöhung der Datensicherheit, insbesondere dort, wo Verbindlichkeit und Zurechenbarkeit bei der Ausführung von bestimmten Workflow-Schritten oder Komponenten, Moduln, Services zählt und garantiert werden muss (◘ Abb. 20.38). Mittlerweile existieren zahlreiche Open-Source-Implementierungen und Kryptoplattformen zur Unterstützung von BC-Transaktionen und -Anwendungen: MS Bletchley, Ethereum Classic, Codius für Ripple, Hyperledger Sawtooth etc.

Eine kurze Auswertung der Blockchain-Technologie kann unten entnommen werden:

1. **Vorteile**
   - Blockchain entwickelt sich dynamisch
   - IT-Großfirmen und Finanzinstitute engagieren sich zunehmend
   - Blockchain ist manipulationssicher und theoretisch unendlich lange nachvollziehbar
   - Viele Anwendungen und mobile Apps nutzen diese Kryptotechnologie: Kryptowährungen, Apps für Smart Contracting, hochverteilte Systeme sowie mittelfristige



◘ **Abb. 20.38** Effiziente und abgesicherte Hochverteilte Systeme

Applikationen zur Automatisierung von Bereichen, bei denen ehemals ein Vermittler (Mediator) erforderlich war.

2. **Nachteile**
   - Mittelfristige komplette Ablösung des zentralistischen Banksystems ist unwahrscheinlich, deshalb eher Nischenbusiness als Alternative zu zentralistischem Banksystem und Börsen
   - Rentabilität von Mining von Bitcoins und weiteren Kryptowährungen (ETH, LTC, XMR, XRP) ist aufgrund der Energieeffizienz fraglich
   - Die Lösung einiger BC-bezogener Probleme ist heute u. U. zu komplex und ressourcenaufwendig, langfristige Massendatenspeicherung (Big Data), massenweise Validitätsprüfungen, Verhinderung krimineller Machenschaften (Ransomware, Fraud).

20.8 Zwischenfragen/Übungsaufgaben

20.8.1 Verteilte Systeme

a) Zu welchen Zwecken werden Verteilte Systeme eingesetzt? Nennen Sie die fünf wesentlichen Merkmale der Verteilten Systeme!
b) Grenzen Sie die Begriffe „generisches VS“, „Cluster Computing“, „Grid Computing“ und“Cloud Computing” ab!
c) Entscheiden Sie, welche der folgenden Beispiele zu den Verteilten Systemen gehören und begründen Sie die getroffene Entscheidung!
   - Dezentral organisierte Büroumgebung auf Workstation-Netz
   - Zentralrechner einer Fluggesellschaft mit weltweit 10.000 sternförmig angeschlossenen einfachen Buchungsterminals
   - Multiprozessor-System
   - Fileserver
   - Grid-System
   - öffentliche Speichercloud
   - energieeffizienter Minicluster auf der Basis von 64 Raspberry Pi -Kontrollern
d) Welche Verteilten Systeme laufen beispielsweise im Hintergrund als Bestandteile des Betriebssystems?

20.8.2 Netzwerkmanagement mittels SNMP

a) Aus welchen Gründen ist die Management Information Base (MIB) international standardisiert worden?
b) Ein Rechnernetz werde mit SNMP verwaltet!
   - Der Manager möchte einen Parameter aus der vom Agenten verwalteten MIB lesen.
   - Der Manager möchte eine Tabelle lesen.
   - Der Agent will eine Ausnahmesituation melden.
   - Der Manager will einen MIB-Parameter ändern.

20.8.3 Client-Server-Modell und n-tier-Architekturen

a) Verteilte Systeme unterteilen sich nach der Art der zu unterstützenden Kommunikation:
   - Client-Server-Kommunikationsmodell (C-S);
   - Peer-2-Peer-Kommunikationsmodell (P2P).

   Vergleichen Sie die beiden Ansätze. Worin liegt der Unterschied zwischen C-S und P2P?
b) Für komplexe verteilte Systeme werden meistens n-tier-Architekturen benutzt. Die Entwicklung erfolgte von 2-tier- über 3-tier- hin zu n-tier-Applikationen.
   Welche Schichten würden Sie für einen WWW-Shop einsetzen? Skizzieren Sie Ihre Lösung!
   Beschreiben Sie die Funktionalitäten in einem WWW-Shop in Stichworten:
   - Einkaufskorb
   - Eingabeformulare zum Editieren von Kundendaten/Aufträge durch den User
   - Rabatt-Berechnungsmodul für Userdarstellung
   - Vorbereitung des Content für den User
   - Überprüfen von Zugriffsrechten des Users
   - Speichern von Kundendaten/Aufträge/History

20.8.4 Cloud Computing

In der Entwicklung der Rechnernetzwerktechnik gab es immer wieder Vorstellungen, die Funktionalität der Arbeitsstationen auf eine reine Terminalfunktion (Thin Client) zu begrenzen und alle Verarbeitungsfunktionen transparent in das Netzwerk auszulagern.

a) Definieren Sie den Begriff „Cloud Computing“? Nennen Sie Vorteile und Nachteile bei der Nutzung des Cloud Computing!

b) Welche Cloud-Modelle (Dienstmuster) hinsichtlich der erbrachten Dienste sind Ihnen bekannt? Verdeutlichen Sie die Unterschiede zwischen den Konzepten: SaaS, PaaS, IaaS.
c) Nennen Sie die Organisationsformen von Clouds, die je nach Anwendungsfall ihre Berechtigung haben!
d) Cloud Computing wirft schwierige rechtliche Aspekte zwischen Endnutzern, Cloud-Anbietern und deren beteiligten Partnern auf. Kommentieren Sie diese Aussage hinsichtlich der Aspekte Datenschutz und Datensicherheit!
e) Grenzen Sie die Begriffe „Cloud Computing“ und „Grid Computing“ ab!

Zusammenfassung

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_21

21

Wir hoffen, dass Sie durch das Studium der drei Teile „Rechnernetze“ zu einem „perfekten Netzwerker“ geworden sind (◘ Abb. 21.1).

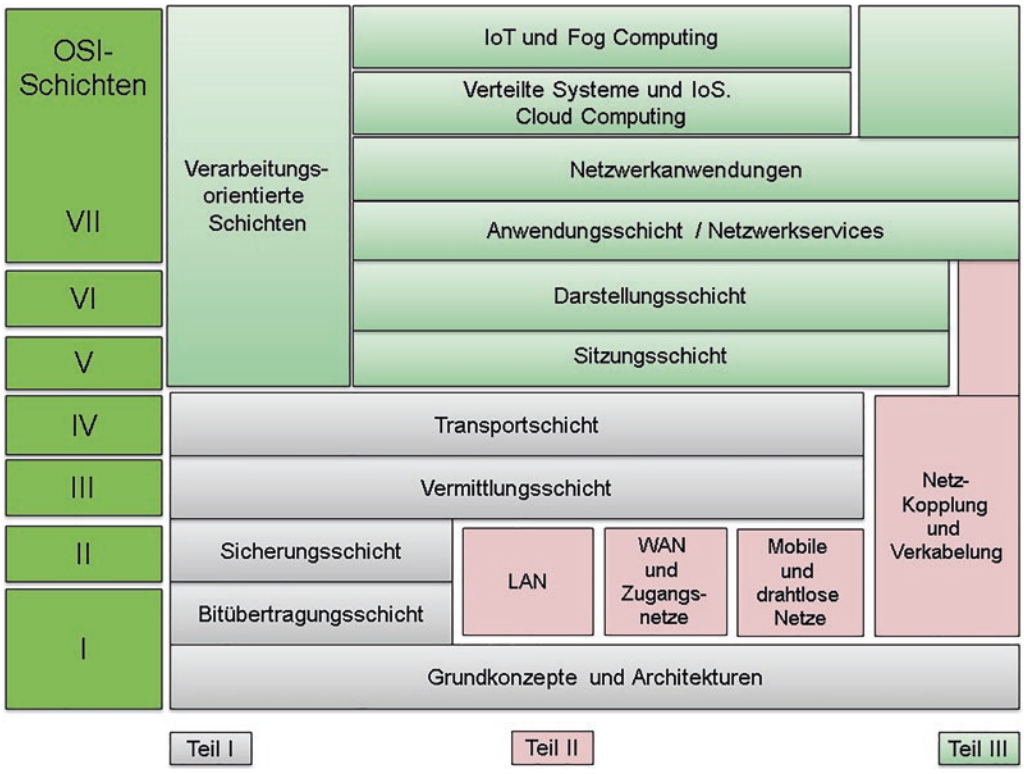
Die Teile I, II und III bieten Ihnen systematischen Überblick über Grundbegriffe der technischen Kommunikation, der geschichteten Protokollarchitekturen und des OSI-Referenzmodells. Mit den vorangegangenen Teilen haben Sie eine Grundübersicht zur Nutzung moderner heterogener Netzwerke unter IP erhalten.

Die Studierenden sind mit den Protokollfamilien: IEEE 802, TCP/IP, grundlegende Techniken für physikalische Schicht, Sicherungsschicht, Netzwerkschicht, einschließlich IP-Adressierung und Routing, sowie Transport- und Anwendungsschicht vertraut.

Fortgeschrittene Konzepte zu den Netzwerkservices und -anwendungen, mobilen Apps, verteilten Systemen und IoT wurden in diesem Teil vermittelt (s. das Konzept in ◘ Abb. 21.1).

Im Anschluss folgt noch ein Glossar zum Inhalt aller drei Teile.

Für zukünftige eigene Projekte haben Sie damit die Basis. Für spezielle Details empfehlen wir das klassische Werk von Andrew S. Tanenbaum und David J. Wetherall [17] als Nachschlagewerk und die unten aufgeführten weiteren Quellen [1, 2, 5–8, 10–16, 18, 19].



◘ **Abb. 21.1** Zur Struktur der Teile I, II, III

Lösungen zu Zwischenfragen/Übungsaufgaben Teil III

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_22

Zu ► Abschn. 18.4

► Abschn. 18.4.1 Kommunikationssteuerung

Über das Internet soll der Inhalt einer Festplatte (72 GByte) mit real 5 Mbit/s kopiert werden (Hinweis: Speichergröße GigaByte als SI-Präfix).

a) Berechnen Sie die Dauer der Übertragung!
b) Wie hoch ist die Wahrscheinlichkeit w einer erfolgreichen Übertragung, wenn pro Stunde eine 10-%ige Ausfallwahrscheinlichkeit a der Transportverbindung existiert?
c) Wie kann das Betriebsverhalten gegenüber b) verbessert werden?

Zu ► Abschn. 18.4.1a)

$$\begin{aligned}\text{Übertragungszeit T} &= \text{Datenvolumen/Übertragungsrate}\\ &= 72\ \text{GByte}/5\ \text{Mbit/s}\\ &= 115200\ \text{s} = 32\ \text{h}\end{aligned}$$

Zu ► Abschn. 18.4.1b)

$$\begin{aligned}w &= (1-a)^{t/h}\\ &= 0{,}9^{32} = 0{,}0343 = 3{,}43\,\%\end{aligned}$$

→erfolgreiche Übertragung nach durchschnittlich ca. 30 Versuchen (1000 h) !!!

Zu ► Abschn. 18.4.1c)

Sicherungspunkte setzen (Zwischenstand der Übertragung sichern),

z. B. Sicherung jede Stunde; max. 2 Wiederholungen einer Ü-Einheit

$$\begin{aligned}w &= [(1-a) + a*(1-a) + a^2*(1-a)]^{t/h}\\ &= [0{,}9 + 0{,}1*0{,}9 + 0{,}01*0{,}9]^{35{,}6}\\ &= 0{,}999^{35{,}6} = 0{,}965 = 96{,}5\,\%\end{aligned}$$

$$\begin{aligned}\text{Übertragungszeit T}' &= [1 + a + a^2] * \text{Datenvolumen/Übertragungsrate}\\ &= [1 + a + a^2] * T\\ &= 1{,}11 * 32\ \text{h} = 35{,}6\ \text{h}\end{aligned}$$

→96 %-ig-erfolgreiche Übertragung in 36 h !!!

► Abschn. 18.4.2 Datenaustausch zwischen heterogenen Computersystemen

In einem Netz mit n = 30 Computern existieren k = 3 verschiedene Systemarchitekturen.

a) Wie viele Import/Export-Routinen müssen programmiert und installiert werden, damit eine Verständigung zwischen allen Systemen möglich ist?
b) Welche Veränderungen ergeben sich, wenn ein weiterer Computer mit einer neuartigen Systemarchitektur in das Netz eingebunden wird?
c) Welche Vor- und Nachteile gegenüber b) ergeben sich bei Nutzung einer einheitlichen Transfersyntax?
d) Nennen Sie eine für einheitliche Transfersyntax geeignete Sprache.
e) Welche Vor- und Nachteile gegenüber a) und b) ergeben sich bei Nutzung von Java-Technologien?

Zu ► Abschn. 18.4.2a)
Für jede Architektur muss eine Input- und eine Output-Routine zu den anderen Architekturen programmiert werden.

Für Architekturen müssen $2 * k * (k - 1)$ Routinen programmiert werden.

Auf n Rechnern müssen $2 * (k - 1)$ Routinen installiert werden. Ingesamt also $n * 2 * (k - 1)$ Routinen.

Im vorliegenden Fall:

12 - Programmierungen

120 - Installationen

Zu ► Abschn. 18.4.2b)
Für $n = 31$ und $k = 4$ ergeben sich entsprechend die Werte:
24 - Programmierungen

186 - Installationen

Zu ► Abschn. 18.4.2c)
Es müssen nur noch $2 * k$ Routinen programmiert werden.
Es müssen nur noch $2 * n$ Routinen installiert werden.
Für $n = 31$ und $k = 4$ ergeben sich entsprechend die Werte:
8 - Programmierungen

62 - Installationen

Zu ► Abschn. 18.4.2d)
ASN.1 - (Abstract Syntax Notation One)

XML - (Extensible Markup Language)

Zu ► Abschn. 18.4.2e)
Java arbeitet nicht mit der lokalen Syntax des Computers, sondern mit einer eigenen Java-Syntax. Dadurch können sich alle Java-Instanzen in einem Netzwerk verstehen und es sind keine Import-/Export-Routinen erforderlich.

► Abschn. 18.4.3 Datenkomprimierung und Codecs

a) Wofür werden die Kompressionsverfahren bei den Netzwerken verwendet?
b) Wo werden ZIP, JPEG, MPEG-4 und MP3 eingesetzt? Nennen Sie mindestens ein Anwendungsgebiet.

Zu ► Abschn. 18.4.3a)

Kompressionsverfahren sind sinnvoll, um Datenübertragungsmengen zu verringern. Dies spart Übertragungskapazität und Übertragungszeit. Nachteilig ist der Aufwand zur Kompression und Dekompression.

Kompressionsverfahren bieten die größten Vorteile bei Multimediaübertragungen (Bilder, Sprache, Video).

Zu ► Abschn. 18.4.3b)

Hinweis: Vgl. ◘ Tab. 18.1.

ZIP - Kompression von Dateien und Archiven (verlustfrei)

JPEG - Kompression von Bildern (in der Regel verlustbehaftet, aber auch verlustfrei möglich)

MPEG-4 - Kompression von Videos (verlustbehaftet)

MP3 - Kompression von Audios (verlustbehaftet)

► Abschn. 18.4.4 Verschlüsselung

a) Vergleichen Sie den Einsatz von symmetrischen und asymmetrischen Verfahren bzgl. Performance und Schlüsselverteilung! Benennen Sie jeweils 2 konkrete Kryptoverfahren. Nennen Sie einige Vor- und Nachteile der asymmetrischen gegenüber den symmetrischen Kryptoverfahren!
b) Wie viel Zeit T muss ein Angreifer für die Schlüsselermittlung durchschnittlich aufwenden (Durchprobieren – Angriff vom Typ Brute Force), wenn er lediglich weiß, dass eine symmetrische Verschlüsselung mit 5-Buchstabenschlüssel vorliegt und ein Dechiffrierungsversuch $T_v = 10$ ms dauert?
c) Beim RSA-Verfahren seien $p = 5$ und $q = 11$.
Geben Sie mögliche Werte für d und e an und verschlüsseln Sie die Zahlen 2, 3 und 4! Entschlüsseln Sie die chiffrierten Zahlen anschließend wieder!

Zu ► Abschn. 18.4.4a)

Symmetrische Verfahren (s. ► Abschn. 18.1.2)

Performance - sehr gut

Schlüsselverteilung - nur sehr umständlich lösbar

Beispiel - AES

Asymmetrische Verfahren (s. ► Abschn. 18.1.2)

Performance - schlecht

Schlüsselverteilung - elegant und einfach lösbar

Beispiel - RSA

Zu ► Abschn. 18.4.4b)
Bei Anwendung eines beliebigen Schlüssels kann der dechiffrierte Text einer Häufigkeitsanalyse unterzogen werden. Für die Dauer des durchschnittlichen Probierens bei einer Schlüsselraumgröße SR gilt:

$$T = 1/2\ SR * T_v$$

Im Schlüsselraum existieren $SR = 26^5$ bzw. $SR = 11.881.376$ unterschiedliche Schlüssel.

Die Entschlüsselung dauert demnach max. 118.813,76 s bzw. etwa 33 h.

Durchschnittlich ist die Entschlüsselung nach 16,5 h beendet.

Zu ► Abschn. 18.4.4c)
Der Algorithmus des RSA-verfahrens wurde bereits im ► Abschn. 18.1.2 im Beispiel 18.1 beschrieben. An dieser Stelle rechnen wir mit anderen Werten.

Anwendung (vereinfacht, kleine Primzahlen für p, q).

1. $p = 5\ q = 11$
2. $n = p * q = 55$
   $z = (p - 1) * (q - 1) = 40$
3. $d = 3$ gewählt
   (40 nicht durch 3 teilbar)
4. Finde $e * d = 1 \bmod 40$
   (41, 81, 121, …)
   z. B. $e = 27$
   $(3 * 27 = 81)$,
   Werte {e,n} – öffentlich, Wert d – privater Schlüssel.

Verschlüsseln mit $C = T^e \pmod n = T^{27} \pmod{55}$

Klartext	T^e	Chiffretext	
	2	(134 217 728)	18
	3	7625597484 987	42
	4	18014398509481984	49

Entschlüsseln mit $T = C^d \pmod n = C^3 \pmod{55}$

Chiffretext	C^d	Klartext
48	5832	2
42	74 088	3
49	117649	4

Zu ► Abschn. 19.7
► Abschn. 19.7.1 Netzwerkanwendungen und mobile Apps

a) Worin unterscheiden sich native Apps, Web-Apps und hybride Apps?
b) Zwei Filialen eines Unternehmens sind über DSL-Internetlinks verbunden.

Eine Videoübertragung wird mit der Bildqualität von
V = 1000 * 1000 Punkten,
FT = 16-Bit-Farbkodierung und der Bildfrequenz
fps = 25 Bild/s vorgenommen.
Ist die Datenkompression für diesen Fall sinnvoll?
Berechnen Sie die erforderliche Datenrate für unkomprimierte Übertragung.

c) Moderne Verfahren/Codecs (wie bspw. ZIP, JPEG, MPEG etc.) ermöglichen eine Leistungsverbesserung/Ersparnis für die Datenrate durch die Kompression.
Bei welcher Mindestkompressionsrate KR (d. h. 1: KR) ist diese Übertragung bei einer verfügbaren Datenrate von DRv = 20 MBit/s möglich? (ggf. aufrunden!).

Zu ► Abschn. 19.7.1a)
Hinweis:
vgl. ◘ Abb. 19.14 und 19.15, sowie ◘ Tab. 19.3.

Native Apps
sind die für mobile Betriebssysteme typischen Apps, die die Nutzer aus dem App Store herunterladen und auf ihren Geräten installieren können (BS-spezifisch).

Web-Apps
Web-Apps sind Webseiten im Responsive Webdesign (RWD), die optisch genau auf mobile Zugangsgeräte angepasst und über eine URL im Browser aufgerufen werden. Sie sind nicht direkt auf dem Endgerät (Smartphone oder Tablet) installiert. Weiterhin kann durch RWD-Darstellungen Barrierefreiheit geboten werden.

Hybride Apps
stellen eine Kombination von nativen Apps und Web-Apps dar. Dabei wird zuerst eine Web-App mit HTML, CSS und JavaScript erstellt. Diese wird dann von einem Container umgeben, der die App ähnlich wie ein Browser lädt. Mit diesem Container, der als nativer Wrapper bezeichnet wird, kann auch auf die Hardwarekomponenten des Smartphones zugegriffen werden.

Spezielle Frameworks laden die Bibliotheken, die die Kommunikation zwischen JavaScript und der jeweiligen betriebssystemspezifischen Sprache herstellen. Dadurch können Hybrid-Apps auf diverse Hard- und Software-Komponenten des mobilen Endgerätes zugreifen. Ein Zugriff ist unter anderem auf Kontakte, Kamera, Bewegungssensor, GPS und Dateien möglich.

◘ Tab. 19.3 führt den Vergleich für die wichtigsten Tools und Frameworks zur Entwicklung von mobilen Apps vor. Zur Entwicklungsunterstützung sowie zur Erhöhung der Verfügbarkeit

mobiler Apps verwendet man i. d. R. folgende Tools und Frameworks:

- Cordova/PhoneGap
- Appcelerator
- Titanium
- Intel XDK
- Trigger.io
- Ionic Lab.

Die Architektur eines solchen Frameworks für mobile Apps wurde in ◘ Abb. 19.16 präsentiert.

Zu ► Abschn. 19.7.1b + c)

Gegeben - Bildqualität V = B × H = 1000 * 1000 Bildpunkte,
Farbtiefe FT = 16 Bit, Bildfrequenz fps = 25 Bild/s,
verfügbare Datenrate DRv = 20 MBit/s

Gesucht - Datenrate DR, Kompressionsrate KR

Geforderte Datenrate für unkomprimierte Übertragung ist zu hoch.

DR = V * FT * fps = 1000 * 1000 * 16 Bit * 25 1/s = 400 Mbit/s

→ Mindestkompressionsrate berechnen

KR = DR/DRv = 400 MBit/s/20 MBit/s = 20 (ggf.aufgerundet),

d. h.

Eine Mindestkompressionsrate von 1:20 ist zum Zweck der Bandbreitenersparung erforderlich.

► Abschn. 19.7.2 Sockets und Fernaufrufe

a) Erläutern Sie die Unterschiede zwischen Datagrammsockets und Streamsockets!
Erläutern Sie die Aufgaben der Socketprozeduren socket(), bind(), accept() und listen().
Wie unterscheiden sich jeweils die folgenden Paare der Socketprozeduren
   - sendto()/recvfrom(),
   - send()/recv()?

   Diskutieren Sie die Nachteile für die Programmierung unter Nutzung der Socketschnittstelle.
b) Die klassische Technologie zur Realisierung von Netzwerkanwendungen nennt sich „Prozedurfernaufruf“.
Dieser besitzt wesentliche Unterschiede zu einem lokalen Prozeduraufruf (von-Neumann-Rechner).
Erläutern Sie den Ablauf eines RPC in Stichworten.

c) Benennen Sie mindestens drei Unterschiede des RPC zur RMI?
d) Nennen Sie je einen Einsatzfall für die Verwendung der Konzepte Socket, RPC und RMI?

Zu ▶ Abschn. 19.7.2a)
Die Internet-Transportschicht realisiert zwei Übertragungsprotokolle, die jeweils eine Variante der Socket-Schnittstelle bieten (s. ◘ Abb. 19.7, 19.8 und 19.9),

- das verbindungslose UDP zur Übertragung von Einzelnachrichten (Datagrammen)
  mit den Socketfunktionen socket(), sendto(), recvfrom() und close().
- und das verbindungsorientierte TCP zur Übertragung von Streams (Datenströmen)
  mit den Socketfunktionen socket(), bind(), connect(), listen(), accept(), send(), recv() und close().

Aufgaben der Socketfunktionen

- socket()
  Prozedur bei TCP und UDP zum Anlegen einer Datenstruktur mit für lokale Portadresse und Partnerportadresse, sowie einem Speicherbereich für Ein- und Ausgabe von Daten
  Die lokale Portadresse wird durch socket() bereits initial belegt, die Partnerportadresse ist noch offen.
- bind()
  TCP-Prozedur zum Nutzen eines bestimmten lokalen Ports. Dies ist für Serverprozesse wichtig, da sie feste Portadressen verwenden müssen, z. B. benötigt ein Webserver den lokalen Port 80.
- listen()
  TCP-Prozedur für einen Server zum Warten auf einen Verbindungsantrag durch einen entfernten Client. Dieser muss dazu die Funktione connect() aufrufen.
  Nach Erhalt des Antrages beendet sich die Funktion listen(). Der Partnerport ist dann in der Socket-Struktur verfügbar.
- accept()
  TCP-Funktion mit der der Server einen Verbindungsantrag bestätigt.

Unterschiede zwischen recv()/recvfrom() bzw. zwischen send()/sendto()

- sendto()/recvfrom()
  Bei der UDP-Funktion sendto() gibt es keine Garantie der erfolgreichen Übertragung, weiterhin keine Garantie der richtigen Reihenfolge bei Mehrfachübertragungen. Eine

Überlastung des Empfängers durch zu hohe Senderaten ist möglich, ebenso ein Überlastung des Übertragungsnetzes.
- send()/recv()
  Bei der TCP-Funktion send() erfolgt eine Steuerung der Übertragung. Die Übertragung ist sicher, da verlorene Segmente durch Übertragungswiederholung trotzdem beim Zielrechner ankommen. Die korrekte Reihenfolge empfangener Segmente wird garantiert. Eine Überlastung des Empfängers (Fluss-Steuerung) bzw. des Netzes (Stauvermeidung) wird vermieden.

Abgrenzung zur Middleware
Die Nutzung von Sockets zur Realisierung verteilter Anwendungen besitzt folgende Nachteile [16, 18]:
- Da UDP unzuverlässig ist, müssen UDP-Server und -Client um Maßnahmen zur Erhöhung der Zuverlässigkeit (befristetes Warten auf eine Antwort, wiederholtes Senden des Auftrags usw.) erweitert werden.
- Bei der Nutzung von TCP muss der Verbindungsauf- und -abbau jeweils explizit programmiert werden.
- Da die Server von vielen Clients beauftragt werden, ist es ratsam, einen Server durch mehrere parallele Prozesse zu realisieren. Dies muss explizit programmiert werden.
- Die übertragenen Daten müssen unter Umständen vor und/oder nach der Übertragung umgewandelt werden, insbesondere bei der Übertragung von Binärdaten (Big-Endian- vs. Little-Endian-Darstellung ganzer Zahlen, Länge von int-Zahlen: 2, 4 oder 8 Byte, Layout von Datenstrukturen usw.).
- Beim Software-Entwurf wird heutzutage ein zu entwickelndes System in Module oder Objekte von Klassen aufgeteilt. Die Module interagieren über Prozedurfernaufrufe (RPC), die Objekte über Methodenfernaufrufe (RMI).
  Die Kommunikation über Sockets passt nicht zu diesem Paradigma [5, 16].

Zu ► Abschn. 19.7.2b)
Lokaler Prozeduraufruf (von-Neumann-Rechner)
Mittels eines Maschinekodebefehles „CALL“ erfolgt ein Sprung in die Befehlsfolgen eines „Unterprogrammes“, danach die Abarbeitung der Prozedurbefehle und abschließend mittels eines Maschinenkodebefehles „Return“ die Fortsetzung des aufrufenden Programmes.

Die Parameter des aufrufenden Programmes werden i.a. über den Programmstackspeicher entweder „Call-by-Value“ oder „Call-by-Reference“ übergeben.

Eine zeitparallele Arbeit zwischen Hauptprogramm und Unterprogramm erfolgt nicht. Die Arbeit des Hauptprogrammes

ist während der Zeit der Abarbeitung des Unterprogrammes unterbrochen.

Fernaufruf RPC

Die ◘ Abb. 19.11 zeigt die Komponenten, die für den Ablauf eines RPC von Bedeutung sind.

Bereits zur Übersetzungszeit werden die wichtigsten Voraussetzungen erfüllt. Das „Hauptprogramm" wird als Client, das „Unterprogramm" als Server konzipiert. Zur Verbindung der beiden werden durch einen speziellen Compiler (RPCGEN) sogenannte Stubs erzeugt, welche zur Laufzeit die Parameterübergabe organisieren sollen.

Ablauf zur Laufzeit:

1. Der Client-Stub nimmt die Inputparameter der Nutz-Prozedur entgegen.
2. Der Client-Stub sendet die Parameter in einer Nachricht zum Server-Stub.
3. Nachrichtenübertragung (i. a. über Socket-Schnittstelle)
4. Der Server-Stub nimmt die Nachricht entgegen und extrahiert die Inputparameter.
5. Der Server-Stub ruft die eigentliche Nutzprozedur auf.
6. Arbeit der Nutzprozedur
7. Der Server-Stub nimmt die Outputparameter der Prozedur entgegen, und sendet sie zurück zum Client-Stub.
8. Nachrichtenübertragung
9. Der Client-Stub nimmt die Nachricht entgegen und extrahiert die Outputparameter.
10. Der Client-Stub übergibt die Output-Parameter dem Client.

Zu ► Abschn. 19.7.2c)

Die folgende ◘ Tab. 22.1 zeigt einige Unterschiede zwischen RPC und RMI.

◘ **Tab. 22.1** Unterschiede zwischen RPC und RMI

Merkmal	RPC	RMI
Objektorientierung	Nein Fernaufruf einer Prozedur im Hauptspeicher des Servers	Ja Fernaufruf einer Methode im Hauptspeicher des Servers
Fixierung auf Programmiersprachen	Client- und Serverstubs werden in gleicher Sprache implementiert (meist in C, RPCGEN-Modul generiert die entsprechenden MW-Komponenten, d. h. den Client-und den Server-Stub)	Client und Server sowie die entsprechenden Middleware-Komponenten müssen nicht unbedingt in gleicher OO-Sprache implementiert werden
Parameterübergabe	„Call-by-Reference" ist problematisch	„Call-by-Reference" ist möglich
Schnittstellendefinition	Statisch, d. h. die Fernaufrufschnittstelle wird zur Übersetzungszeit vollständig definiert	Dynamisch, d. h. die definierte Schnittstelle kann zur Laufzeit vervollständigt werden!

Zu ► Abschn. 19.7.2d)
Die Einsatzfälle für die Verwendung der Konzepte Socket, RPC und RMI:
Sockets - klassische Applikationen basieren i. a. auf der TCP/IP-Schnittstelle (Sockets)

z. B. SMTP-Mailprogramme, einfache Chat-Dienste etc.

RPC - Die Fa. Sun realisierte auf der RPC-Basis bereits 1984 ein verteiltes Filesystem

(NFS, Network File System).

Weiterhin gibt es moderne Anwendungen auf der Basis der

XML-kodierten RPC-Aufrufe (sog. Webservices).

RMI - Java-RMI wird als wichtiger Grundmechanismus bspw.

im Middleware-Framework EJB (Enterprise Java Beans) verwendet

und damit auch für die mittels EJB entwickelten Applikationen

► Abschn. 19.7.3 WWW

a) Welche Aufgaben verrichtet ein WWW-Browser?
Beschreiben Sie den Vorgang, der nach einem Anklicken eines Links in einem WWW-Dokument abläuft!
b) Erklären Sie die Funktionsweise von Webservices und deren drei wichtigsten Aufbauprinzipien!
c) Beschreiben Sie die Funktionalitäten einer Suchmaschine und eines Webcrawler!
d) Erklären Sie die Unterschiede zwischen den Begriffen „Classical Web“ – „Web 2.0“ – „Web 3.0“?
Ist Web 3.0 heutzutage Ihrer Meinung nach schon komplett ausgebaut?
Welche Voraussetzungen braucht man dafür?

Zu ► Abschn. 19.7.3a)
Ein Webbrowser hat die Aufgabe, mittels des HTTP-Protokolls, Dateien von einem Webserver zu holen und diese nutzergerecht darzustellen. Die Adressierung erfolgt dabei über einen sog. URI (Uniform Resource Identifier). Die Dateien sind meist Dokumente in der Sprache HTML. Da diese Hypertextsprache interne Einbindungen anderer Dokumente (z. B. Bilder) erlaubt, müssen diese ebenfalls vom Server geholt und auf dem Client dargestellt werden. Der Browser muss auch interne Links in einem HTML-Dokument auf andere Dokumente anzeigen und bei Nutzerwunsch diese als Nachfolgedokument laden und darstellen.

Zu ► Abschn. 19.7.3b) Funktionsweise und Aufbauprinzipien von Webservices
Ein Webservice (WS) ist eine Software-Anwendung, die über einen URI eindeutig identifiziert wird. WS können mit anderen Software-Agenten interagieren unter Verwendung

XML-basierter Nachrichten durch den Austausch über internetbasierte Protokolle.

Intern kann ein WS in einer beliebigen Programmiersprache realisiert sein (vergleichbar Middleware-Komponenten). Die als WS-Trio bezeichneten Begriffe spielen bei der WS-Nutzung eine große Rolle:

- UDDI (Universal Description, Discovery and Integration)
  Auskunfts- und Verzeichnisdienst (UDDI ist selbst als WS realisiert)
  Informationen vom UDDI-Service können anhand des Dienstnamens abgefragt werden (white pages) oder über Angaben von Attributen (yellow pages; eine Art Branchenbuch) oder technischer Details (green pages).
- WSDL (Web Service Description Service)
  Beschreibung der Nutzerschnittstelle von WS (Ausführung ist transparent)
- SOAP (Protokoll)
  Übertragungsprotokoll für XML-orientierte Nachrichten

Man unterscheidet auch SOAP -Webservices und REST-Webservices [10, 14, 16], die REST-Services stellen eine leichtgewichtige Alternative zu SOAP dar.

Zu ► Abschn. 19.7.3c)
Suchmaschinen haben folgende Aufgaben:

- Verwaltung (Erstellung, Pflege) einer Übersicht zu den im WWW vorhandenen Informationen.
  Intern realisieren sie eine Indexstruktur mit Informationen über Inhalt und Ort von Dokumenten.
- Bearbeitung von Suchanfragen durch WWW-Browser
  Dazu muss eine Liste von Links zu interessanten Dokumenten erstellt werden. Die Qualität der Beantwortung und die Reaktionsschnelligkeit kennzeichnen die Güte einer Suchmaschine.
- Präsentation von kommerzieller Werbung, die möglichst gut auf die Bedürfnisse des Kunden zugeschnitten ist.

Intern nutzen sie die sogenannten Webcrawler zum automatischen durchsuchen des WWW.

Zu ► Abschn. 19.7.3d)
Classical Web (seit 1990), charakterisiert durch

- Übertragungsprotoll HTTP, Dokumentenbeschreibungssprache HTML,
  Suchmaschinen und wichtige Applikationen (Wikipedia, …)
- Semantic Web
  Das semantische Web (Semantic Web) beinhaltet notwendige Architekturkomponenten zur Umwandlung eines komplexen

Webinhaltes (Content) zur maschinenbearbeitbaren Form mit Metainformationen (Metatags). Diese erleichtern die standardisierte Verarbeitung von Dokumenten, z. B. durch Webcrawler (Spider).

Web 2.0 (2005)
Definition nach Tim O'Reilly (Anhänger der Freien Software und Open Source-Bewegung):
Web 2.0 = Klassisches Web + soziale Netzwerke + Clouds

Web 2.0 ist gegenwärtig in weiten Teilen realisiert.

Web 3.0 (?)
Definition nach J. Markoff (2008):
Web 3.0 = Web 2.0 + Semantic Web

Die Nutzung des WWW ist heutzutage viel schneller und effizienter als zur Gründerzeit. Wichtige Applikationen sind für jedermann komfortabel und schnell nutzbar, z. B. Google, Wiki, Webmail, YouTube, GoogleMaps, Amazon, ebay, Clouds …

Die Zielstellung des Web 3.0 erfordert die weitere Entwicklung von effizienten Crawlern, Suchmaschinen und Ontologien (Begriffsbäumen zum Ausbau von Metainformationen, sog. Metatags über aktuelle Webseiten).

Das Semantic Web erweitert das Web, um die universelle Datenaustauschbarkeit und Verarbeitungsmöglichkeit.

Das Web 3.0 befindet sich gegenwärtig noch in Entwicklung.

Das künftige Web ist konfrontiert mit neuen Herausforderungen:
- Anonymität und Schutz der Privatsphäre (bei Nutzung von sozialen Netzwerken und IoT)
- Datensicherheit angesichts des Cloud-Zugriffes
- Performance (Zugriffe zu sog. „Big Data", große Volumina wenig strukturierter akquirierter Daten).

Zu ► Abschn. 20.8

► Abschn. 20.8.1 Verteilte Systeme

a) Zu welchen Zwecken werden Verteilte Systeme eingesetzt? Nennen Sie die fünf wesentlichen Merkmale der Verteilten Systeme!
b) Grenzen Sie die Begriffe „generisches VS", „Cluster Computing", „Grid Computing" und"Cloud Computing" ab!
c) Entscheiden Sie, welche der folgenden Beispiele zu den Verteilten Systemen gehören und begründen Sie die getroffene Entscheidung!
   - Dezentral organisierte Büroumgebung auf Workstation-Netz

- Zentralrechner einer Fluggesellschaft mit weltweit 10.000 sternförmig angeschlossenen einfachen Buchungsterminals
- Multiprozessor-System
- Fileserver
- Grid-System
- öffentliche Speichercloud
- energieeffizienter Minicluster auf der Basis von 64 Raspberry Pi -Kontrollern

d) Welche Verteilten Systeme laufen beispielsweise im Hintergrund als Bestandteile des Betriebssystems?

Zu ► Abschn. 20.8.1a)
Verteilte Systeme (VS) werden vor allem für folgende Zwecke eingesetzt [15, 16]:

- gemeinsame Nutzung von Daten (z. B. verteilte Dateisysteme und World Wide Web), auch zur Erreichung von Fehlertoleranz durch Redundanz (z. B. Replikation von Daten einer Datenbank),
- gemeinsame Nutzung von Geräten (z. B. Drucker und Scanner)
- gemeinsame Nutzung von Rechenleistung (z. B. Zugriff auf Hochleistungsrechner),
- Kommunikation der Benutzer eines verteilten Systems (z. B. elektronische Post, gemeinsamer Terminkalender einer Arbeitsgruppe, Mehrbenutzeranwendungen wie Mehrbenutzertexteditoren oder Mehrbenutzergrafikeditoren, IP-Telefonie, Audio-Video-Konferenzen).

Die fünf wesentlichen Merkmale der Verteilten Systeme sind wie folgt [16]

1. Kopplung räumlich verteilter Rechner mittels Rechnernetz
2. Kooperation mit dem Ziel, eine bestimmte Anwendungsfunktionalität (Kooperationsaufgabe) zu erbringen
3. Kein gemeinsamer physikalischer Speicher, keine strikt synchronisierten Uhren
4. Dezentrale Organisation und Verwaltung
5. Häufig auch Fehlertoleranz und Lastausgleich durch Replikation.

Zu ► Abschn. 20.8.1b)
Eine schärfere Abgrenzung zwischen generischen VS, Cluster Computing, Grid Computing und dem heutigen Begriff „Cloud Computing“ gibt es nicht.

1. Clouds können die im Weiteren aufgelisteten Typen von VS integrieren
2. Bei Clustern wird „Computing Power“ in einem „virtuellen Supercomputer“ geografisch zentralisiert;
   Ein Cluster enthält i. d. R. Computer mit homogener Rechnerarchitektur.

3. Grid Computing ist eine Form des verteilten Rechnens, bei der ein „virtueller Supercomputer“ aus geographisch verteilter, heterogener und lose gekoppelter Computer erzeugt wird.
4. In einem verteilten System können unterschiedliche Transparenzaspekte mehr oder weniger stark ausgeprägt sein. Ein Beispiel für verteilte Systeme, bei denen besonders großer Wert auf Transparenz – insbesondere auf Ausführungstransparenz – gelegt wird, stellt das Grid Computing dar.

Während die historisch ersten Einsatzgebiete für das Grid Computing wissenschaftlicher Natur waren, wird es mittlerweile verstärkt auch im kommerziellen Umfeld eingesetzt.

Zu ► Abschn. 20.8.1c)
Die Lösung wurde in ◘ Tab. 22.2 zusammengefasst:

Zu ► Abschn. 20.8.1d)
Neben solchen Anwendungen, die für die User sichtbar sind, gibt es auch solche, die von anderen Komponenten intern benutzt werden und den Endanwendern verborgen bleiben, wie z. B. Anwendungen zur
- Berechnung von Wegewahltabellen (OSPF, RIP, BGP usw.),
- Namensdienste (DNS),
- Konfigurationsdienste (DHCP)
- und Netzmanagement-Dienste (SNMP).

◘ **Tab. 22.2** Szenarienanalyse

Szenario	Verteiltes System?	Kurze Begründung
Dezentral organisierte Büroumgebung auf Workstation-Netz	Ja	Kooperationsaufgabe, dezentral über Netzwerk, kein gemeinsamer Speicher
Zentralrechner einer Fluggesellschaft mit weltweit 10.000 sternförmig angeschlossenen einfachen Buchungsterminals	Nein	Kooperationsaufgabe, aber zentral
Multiprozessor-System	Nein	Verteilt über Netzwerk, ggf. gemeinsamer Speicher, zentral
Fileserver	Ja	Kooperationsaufgabe, dezentral über Netzwerk, kein gemeinsamer Speicher
Grid-System	Ja	Kooperationsaufgabe, dezentral über Netzwerk
Öffentliche Speichercloud	Ja	Kooperationsaufgabe, dezentral über Netzwerk
Energieeffizienter Minicluster auf der Basis von 64 Raspberry Pi -Kontrollern	Nein	Verteilt über Netzwerk, dezentral über Netzwerk, aber keine Kooperationsaufgabe

► Abschn. 20.8.2 Netzwerkmanagement mittels SNMP

a) Aus welchen Gründen ist die Management Information Base (MIB) international standardisiert worden?

b) Ein Rechnernetz werde mit SNMP verwaltet.
   - Der Manager möchte einen Parameter aus der vom Agenten verwalteten MIB lesen.
   - Der Manager möchte eine Tabelle lesen.
   - Der Agent will eine Ausnahmesituation melden.
   - Der Manager will einen MIB-Parameter ändern.

Zu ► Abschn. 20.8.2a)

Die einzelnen Geräte in einem Netzwerk stammen von verschiedenen Herstellern und unterscheiden sich teilweise erheblich in ihrer internen Funktionsweise, im Format und dem Inhalt von Steuertabellen, im Umfang der erhobenen Betriebsinformationen usw. (Heterogenität).

Damit ein Managerprogramm eine Übersicht der Betriebsparameter aller Netzwerkcomputer erstellen kann, müssen die Management-Agenten auf „allgemeine" Anfragen in einer „allgemeinen" Form antworten.

Durch eine standardisierte MIB wird dies garantiert.

Beispiel:
Durch Anforderung eines Objekts mit der ID „1.3.6.1.2.1.7" wird ein 32-Bitzählwert angefordert, der die Anzahl empfangener UDP-Sehmente anzeigt

Zu ► Abschn. 20.8.2b)

Durch Auswertung der ◘ Abb. 20.20 ergeben sich die Lösungen:
- Der Manager nutzt das Dienstelement „GetRequest".
  Der Agent antwortet mit „GetResponse".
- Der Manager nutzt die Dienstelemente „GetRequest" und „GetNextRequest"
  Der Agent antwortet mit „GetResponse".
- Der Agent nutzt das Dienstelement „Trap" ohne Aufforderung durch den Manager.
- Der Manager nutzt das Dienstelement „SetRequest".

► Abschn. 20.8.3 Client-Server-Modell und n-tier-Architektur

a) Verteilte Systeme unterteilen sich nach der Art der zu unterstützenden Kommunikation:
   - Client-Server-Kommunikationsmodell (C-S);
   - Peer-2-Peer-Kommunikationsmodell (P2P).
     Vergleichen Sie die beiden Ansätze. Worin liegt der Unterschied zwischen C-S und P2P?

b) Für komplexe verteilte Systeme werden meistens n-tier-Architekturen benutzt. Die Entwicklung erfolgte von 2-tier- über 3-tier- hin zu n-tier-Applikationen.
Welche Schichten würden Sie für einen WWW-Shop einsetzen? Skizzieren Sie Ihre Lösung!
Beschreiben Sie die Funktionalitäten in einem WWW-Shop in Stichworten:
- Einkaufskorb
- Eingabeformulare zum Editieren von Kundendaten/Aufträge durch den User
- Rabatt-Berechnungsmodul für Userdarstellung
- Vorbereitung des Content für den User
- Überprüfen von Zugriffsrechten des Users
- Speichern von Kundendaten/Aufträge/History

Zu ▶ Abschn. 20.8.3a)
Vergleich/Unterschiede:
Die Realisierung von VS erfolgt auf der Basis (vgl. ◘ Abb. 20.5):

1. des Client/Server-Modells:
   durch verteilte Objekte, Software-Komponenten, Webservices
   Der Client ist eine priorisierte auftraggebende Instanz (Initiator), während der Server die untergeordnete Instanz ist, die aber viel leistungsfähigere Hardware erfordert.
   Die Struktur ist i.a. zentralisiert.
   Die Rollen können jedoch auch vertauscht werden, bspw. meldet sich bei einem SNMP-Trap der Agent (normalerweise Server) selbst beim Manager an (in diesem Fall als Client).
2. des P2P-Modells:
   gleichberechtigte Kommunikationspartner, typisch für Grids, Skype, und (oft illegale) Tauschbörsen
   Die Struktur ist i.a. dezentralisiert.

Die beiden Konzepte werden auch erfolgreich kombiniert (vgl. ◘ Abb. 20.6).

Zu ▶ Abschn. 20.8.3b)
Für einen WWW-Shop ist die flexible 4-Tier-Architektur von Vorteil.
Die vier Schichten (Tiers) sind dabei wie folgt:
1 – Browser; 2 – Webserver; 3 – Applikation Server; 4 – Datenbank (s. ◘ Abb. 22.1).

Die zentrale Komponente der Architektur ist ein leistungsfähiger Application Server, der mittels zahlreicher Frameworks und mehrerer Skript- und Programmiersprachen unterstützt werden kann:

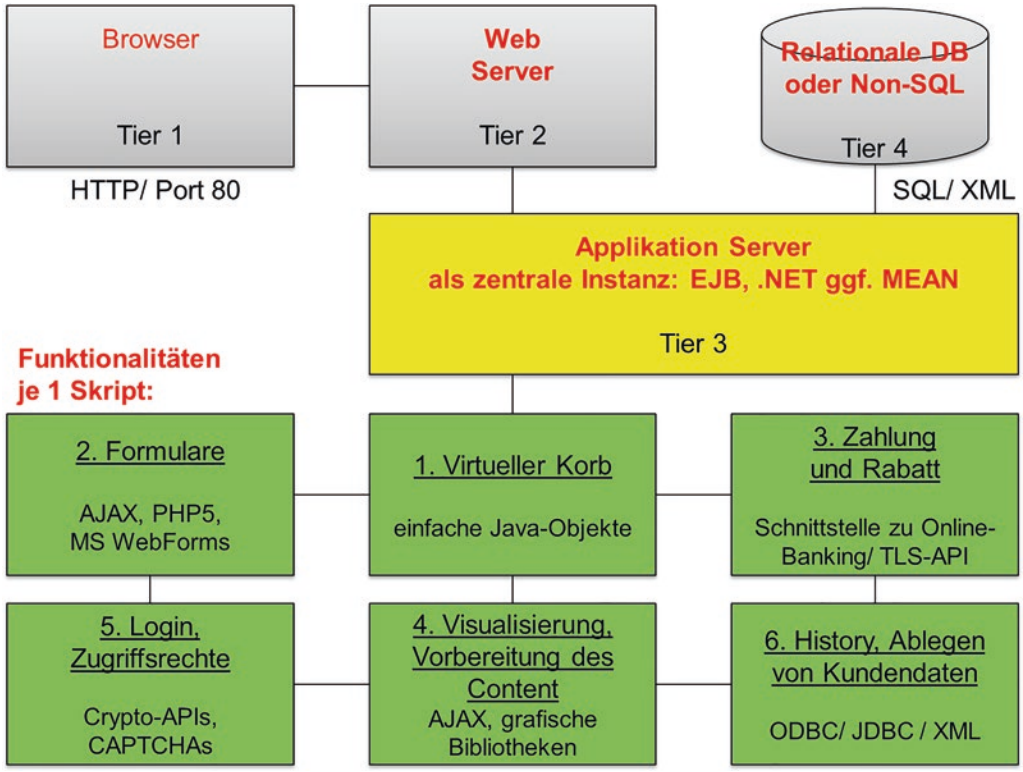


Abb. 22.1 n-tier-Architektur für einen Web-Shop

u. a. per EJB, .NET, MEAN (s. ► Abschn. 19.3 und 19.5).

Die o. g. sechs Module können in den folgenden gängigen Techniken implementiert werden (vgl. Abb. 22.1):

- Die Kernfunktionalitäten werden mittels einfacher Java-Objekte implementiert.
- AJAX ermöglicht asynchrone (abgekoppelte) Usereingabe ohne „Stop-Wait-Refresh"-Paradigma.
- Der Applikation Server erweitert die Funktionalitäten des Web Servers und bietet die ODBC/JDBC/XML- Schnittstelle zur Datenbank sowie spezielle aggregierte Kommunikationskomponenten (sog. „Beans" bei EJB oder ADO.NET bei MS.NET).
- Die Datenbank kann eine relationale Struktur haben („klassisch", SQL-getrieben) sowie „leichtgewichtig" sein wie bspw. MongoDB, eine NonSQL-Datenbank (per AJAX/JSON-Format getrieben).
- Spezielle Schnittstellen besitzen Modul 3 und Modul 5 zwecks kryptografischer Absicherung der Zahlung (TLS-Protokoll, s. ► Abschn. 18.3.1) und des Einloggens.

Bei dem oben beschriebenen Aufbau kann man die Schichten unabhängig von einander modernisieren und ggf. bei der Steigerung der Anzahl von Usern und Aufträgen skalieren.

► Abschn. 20.8.4 Cloud Computing
In der Entwicklung der Rechnernetzwerktechnik gab es immer wieder Vorstellungen, die Funktionalität der Arbeitsstationen auf eine reine Terminalfunktion (Thin Client) zu begrenzen und alle Verarbeitungsfunktionen transparent in das Netzwerk auszulagern.

a) Definieren Sie den Begriff „Cloud Computing"? Nennen Sie Vorteile und Nachteile bei der Nutzung des Cloud Computing!
b) Welche Cloud-Modelle (Dienstmuster) hinsichtlich der erbrachten Dienste sind Ihnen bekannt? Verdeutlichen Sie die Unterschiede zwischen den Konzepten: SaaS, PaaS, IaaS.
c) Nennen Sie die Organisationsformen von Clouds, die je nach Anwendungsfall ihre Berechtigung haben!
d) Cloud Computing wirft schwierige rechtliche Aspekte zwischen Endnutzern, Cloud-Anbietern und deren beteiligten Partnern auf. Kommentieren Sie diese Aussage hinsichtlich der Aspekte Datenschutz und Datensicherheit!
e) Grenzen Sie die Begriffe „Cloud Computing" und „Grid Computing" ab!

Zu ► Abschn. 20.8.4a)
Definition des Begriffs „Cloud Computing":
„Cloud Computing beinhaltet Technologien und Geschäftsmodelle um IT-Ressourcen dynamisch zur Verfügung zu stellen und ihre Nutzung nach flexiblen Bezahlmodellen abzurechnen. Anstelle IT-Ressourcen, beispielsweise Server oder Anwendungen, in unternehmenseigenen Rechenzentren zu betreiben, sind diese bedarfsorientiert und flexibel in Form eines dienstleistungsbasierten Geschäftsmodells über das Internet oder ein Intranet verfügbar" (laut Microsoft).

Clouds ermöglichen den Einsatz und die Nutzung von „Computing Power" in analoger Art und Weise wie bei der Lieferung von Wasser oder Strom in modernen Versorgungsnetzen (s. g. Utility Grids): transparenter Betrieb ist in einer Cloud möglich.

Vorteile:

- Einzelne Organisationen besitzen u. U. keine ausreichenden Ressourcen für
  Datenbackups und rechenintensive Probleme
- Aggregation Rechenressourcen von mehreren Organisationen (erfolgt durch die Provider)

Unternehmen/Behörden können den „On-Demand" -Ressourcenzugriff bekommen
(ideale Lösung bei schwankendem Bedarf)
Ersparnisse in der Verarbeitungszeit und den Hardware-Kosten überwiegen die Nachteile der bei Cloud-Lösungen größeren Koordinations- und Synchronisationskomplexität.

Nachteile:
- Komplexität/Probleme/Uneinheitlichkeit bei Datensicherheits-/Schutzaspekten!

Zu ► Abschn. 20.8.4b)
Dienstmuster
Die Cloud-Architektur laut Amazon lässt sich als Pyramidenmodell darstellen. Die Dienste haben ihre Muster und werden in drei unterschiedlichen Gruppen zwischen den Ebenen PHY (physikalische Ebene) und APL (Application-Ebene) aufgeteilt (vgl. ◘ Abb. 20.15).
- **XaaS (Everything as a Service)**
  allgemeine Schablone, die einen Ansatz bezeichnet, „alles" als Service zur Verfügung zu stellen und zu konsumieren.
- **SaaS (Software as a Service)**
  Die Software wird in der Cloud bereitgestellt
  bspw. ein virtuelles Betriebsystem oder Front-End für Onlinegamer
- **PaaS (Platform as a Service)**
  bspw. wird eine Testumgebung für einen Crossassembler zur Verfügung gestellt oder eine Produktivumgebung vieler leistungsfähiger VM oder ein Applikation Server zur Ausführung von Webservices im Modus „Business-to-Business".
- **IaaS (Infrastructure as a Service)**
  bspw. geht es um einen (virtuellen) Cloudspeicher für Nutzerdaten oder um einen Cluster leistungsfähiger Server, die für anspruchsvolle Simulationen in der Cloud angemietet werden können.

Zu ► Abschn. 20.8.4c)
Organisationsformen von Clouds
Es wird i. a. je nach Anwendungsfall eine Unterscheidung folgender drei Organisationsformen vorgenommen (s. ◘ Abb. 20.14).
1. Private Clouds (unternehmensintern, hohes Maß an Datensicherheit!) – „On Premises"
   - Kundeneigene, vom Kunden selbst betriebene Cloud-Umgebung
   - im Eigentum eines IT-Dienstleisters befindliche und von diesem betriebene Cloud
   - Zugriff über Internet, flexible und schnelle Nutzung durch internes Login.

2. Public Clouds – „Off Premises“
   - Beschränkter Zugang (Kunde selbst, autorisierte Geschäftspartner) über Intranet
3. Hybride Clouds.
   - Mischbetrieb von Private und Public Cloud
   - Manche Autoren definieren noch zusätzlich sog. „Private Community Clouds“. Unserer Ansicht nach zählen diese zu den hybriden Clouds.

Zu ► Abschn. 20.8.4d)

Datenschutz und Datensicherheit

Bei dem Aufbau, dem Deployment und der Wartung von Cloud-Services bleibt die Data Security immer noch eine offene Frage. Cloud Computing wirft schwierige rechtliche Aspekte zwischen Endnutzern, Cloud-Anbietern und deren beteiligten Partnern auf. Für den Endnutzer ist die innere Cloudstruktur vollkommen verborgen. Er muss den Cloud-Anbietern vertrauen. Es ergeben sich komplizierte Haftungsprobleme, da die Anbieter i.a. weltweit agieren, unterschiedlichen Gesetzgebungen unterliegen und u. U. ihrerseits von weiteren Anbietern Teildienstleistungen beziehen.

Im Allgemeinen sind rechtliche Vertragsbeziehungen in Clouds in der Bundesrepublik Deutschland durch die folgenden Gesetze und Rechtsvorschriften zu regeln (Quelle: Juris Bundesministerium der Justiz und Verbraucherschutz, BMJ Online: ► http://www.gesetze-im-internet.de/):

- BGB (Bürgerliches Gesetzbuch)
- TMG (Telemediengesetz) und TKG (Telekommunikationsgesetz).
- EU-Datenschutzgrundverordnung (ab Mai 2018) und BDSG (Bundesdatenschutzgesetz).

Zu ► Abschn. 20.8.4e)

Abgrenzung „Cloud Computing“ zu „Grid Computing“

Der Begriff Cloud Computing ist weiter gefasst als die Grids und Cluster:

- Bei den Grids geht es um gemeinsame freie oder vertragsgeregelte Verwendung der (virtualisierten) Ressourcen für das Verteilte Rechnen ohne zentrale Steuerung.
- Im Fall von „Cloud Computing“ hat man einen oder mehreren Cloud-Anbieter mit zentralisierter Steuerung von physikalischen und virtualisierten Ressourcen. Das Management von Ressourcen erfolgt ebenfalls zentral.

Aufgaben zum Komplex I – Übertragungsorientierte Schichten

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_23

23.1 Dienstelemente für einen abstrakten Telefondienst

a) Erstellen Sie ein folgendes Ablaufdiagramm für einen abstrakten Telefondienst, bei dem ein Initiatorprozess A eine Gesprächsverbindung zum Responderprozess B aufbauen will:
   - Zuerst hört der Prozess A bei einer ersten Verbindungsaufnahme ein Besetztzeichen und es kommt keine Verbindung zustande.
   - Beim zweiten Versuch wird die Verbindung zwischen Prozess A und Prozess B erfolgreich aufgebaut.
   - Die Daten werden übertragen (unbestätigter Datentransfer) und danach wird die Verbindung abgebaut.

b) Zeichen Sie das dazugehörige Zustandsdiagramm entsprechend den Vorgaben von Aufgabe a)!

23.2 Funkübertragungskanal nach Nyquist-Theorem

Über einen digitalen Funkübertragungskanal soll eine Datenrate von 160 MBit/s übertragen werden.

a) Wie groß sind Schrittgeschwindigkeit und minimale Bandbreite des (rauschfreien) Übertragungskanals, wenn pro Signalschritt 16 Bit kodiert werden können?

b) Auf welchen Wert erhöht sich die minimal erforderliche Bandbreite bei einem Signal-Rausch-Verhältnis auf dem Übertragungskanal von SNR = 1023?

23.3 Multiplexverfahren: Frequenzmultiplex vs. OFDM

a) Die Kanalbandbreite eines analogen Fernsehkanals beträgt 5,5 MHz. Wie viele Fernsehprogramme könnten durch ein Kabelverteilnetz im Frequenzmultiplex angeboten werden, wenn ein Frequenzband von 170–299 MHz nutzbar ist und zwischen den Kanälen ein Sicherheitsabstand von 1000 kHz einzuhalten ist?

b) Welche Vorteile bringt der Einsatz des OFDM-Konzepts im Vergleich zum Frequenzmultiplex?

23.4 Modulationsverfahren

a) Was ist ein Modulationsverfahren?

b) Stellen Sie die Übertragung der Bitfolge „0101100100100“ dar mit Amplitudentastung, Frequenztastung und Phasentastung!

23.5 IP-Adressen und Klassenbildung

a) Welche der vorgegebenen IPv4-Adressen sind falsch? Für richtige Adressen definieren Sie die Klassen (A, B, C, D) und tragen sie in die Tabelle ein!
b) Welche der Adressen sind Hostadressen (bitte vermerken)?
c) Welche der Adressen sind Netzwerkadressen (bitte vermerken)?
d) Welche der Adressen sind Broadcast/Multicast-Adressen (bitte vermerken)?

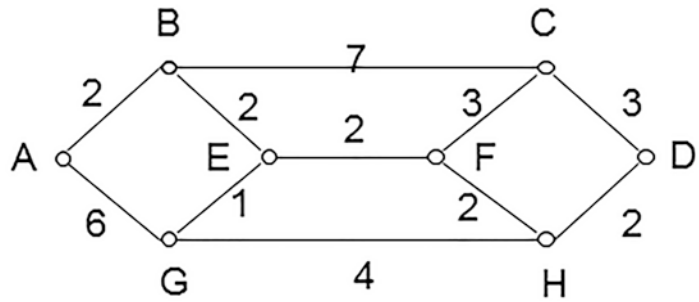
IP-Adresse	Klasse bzw. Typ oder fehlerhaft?
315.115.115.115	
117.117.117.117	
133.177.133.177	
115.0.0.0	
221.225.3.225	
155.122.0.0	
225.251.177.233	
235.225.235.735	

23.6 Distance Vector Routing

Gegeben sei folgendes Netzwerk (◘ Abb. 23.1):

Die Router sind in der Lage, die Übertragungskosten zu ihren Nachbarn zu bestimmen.

Im 30-s-Rhythmus senden sie ihre Distanzvektoren DV an ihre Nachbarn.



◘ **Abb. 23.1** Vermaschtes Netzwerk mit Knoten A, B, C, D, E, F, G, H

Hinweis:
Die Komponenten der Vektoren stellen die aktuelle Distanz vom Router zu den anderen Routern (Distanz zu A, Distanz zu B, …, Distanz zu H) dar.

e) Wie ändert sich die Routingtabelle des Knotens E, wenn dieser nach einem Systemausfall folgende Distanzvektoren von seinen Nachbarn erhält?
   von B (2, 0, 7, 8, 2, 4, 3, 6)
   von F (6, 4, 3, 4, 2, 0, 3, 2)
   von G (5, 3, 6, 6, 1, 3, 0, 4)
f) Nach wieviel Schritten ist der Inhalt der Routingtabelle stabil?
g) Überlegen Sie sich, ob der Inhalt der Tabelle bei zeitveränderlichen Metriken immer zu einem optimalen Ergebnis führt!

23.7 IP – Fragmentierung

Ein TCP-Segment mit 2048 Byte Nutzdaten wird an IP zur Auslieferung übergeben.

Der Übertragungsweg geht über zwei Netzwerke (Quellrechner → Router → Zielrechner).

Jedes Netzwerk hat eine Maximalgrenze MTU für die IP-Paketgröße.

Netzwerk 1 - MTU = 1024 Byte

Netzwerk 2 - MTU = 512 Byte

a) Geben Sie für die beim Empfänger ankommenden Fragmente jeweils die Größe und den Offset an.
b) Wie viele Fragmente würden erzeugt, wenn der Sender wüsste, dass die kleinste MTU auf den Pfad zum Empfänger 512 Byte beträgt?

23.8 Netto/Brutto-Datenrate in der Schichtenarchitektur

Ein Rechnernetz mit einer 7-Schichtenarchitektur habe pro Schicht einen Verlust der Datenrate von a = 15 % infolge Overhead. Wie hoch ist die Anwendungs-Übertragungsrate in einem 10Gigabit-Ethernet-LAN (10 GBit/s)?

23.9 Internet-Schichtenarchitektur und Netto-/Brutto-Verhältnis

a) Das Internet besitzt eine 4-Schichtenarchitektur und habe für die 2.Schicht einen Verlust der Datenrate von 10 % infolge Overhead. Jede nächste Schicht hat einen um 5 % höheren Overhead. Wie hoch ist die Anwendungs-Übertragungsrate (Schicht 4) in einem Gigabit-Ethernet-LAN (Netto-DR = 1000 Mbit/s)?
b) Wie groß ist das Netto-/Brutto-Verhältnis in diesem Fall?

23.10 Fehlerbehandlung durch Paritätskontrolle

Der ASCII-Basiskode ist ein Zeichendarstellungskode für Klein- und Großbuchstaben des englischen Alphabets, sowie für Ziffern, Sonder- und Steuerzeichen.

Auszug (hexadezimale Darstellung)

A	B	...	O	P	Q	...	Z
0×41	0×42		$0 \times 4F$	0×50	0×51		$0 \times 5A$

a) Notieren Sie zeichenweise untereinander die Zeichenkette „ABCDPQRS“ in binärer 7-bit-Darstellung.
b) Fügen Sie ein Kontrollbit für gerade Parität hinzu.
c) Welche Bitfehlersituationen können erkannt und welche korrigiert werden?
d) Wie hoch ist bei einer Bitfehlerwahrscheinlichkeit von 10^{-3} die Wahrscheinlichkeit eines fehlerhaften Zeichens und wie hoch ist die Wahrscheinlichkeit, dass der Fehler nicht erkannt wird?
e) Fügen Sie ein Kontrollzeichen für gerade Blockparität hinzu.
f) Welche Bitfehlersituationen können erkannt und welche korrigiert werden?
g) Für welche Anwendungen wäre ein solcher Kode geeignet?

23.11 Fehlerkorrigierende Codes

Folgende Tabelle enthält die Kodeabbildung für die Zeichen „A“, „B“, „C“ und „D“:

A	B	C	D
000000	111000	000111	111111

a) Wie würden Sie die folgenden, zum Teil gestörten Bitfolgen interpretieren?
   - 100000
   - 001111
   - 101111
   - 000111
   - 101010
b) Wie groß ist die Hamming-Distanz des Codes?
c) Wie viele Bitfehler lassen sich erkennen und wie viele korrigieren?

23.12 Cyclic Redundancy Check (CRC)

Um Übertragungsfehler erkennen zu können, wird mit den Daten noch eine redundante Bitfolge fester Länge, die sogenannte Sicherungssequenz (Frame Check Sequence), gesendet. Diese wird durch eine Polynomdivision ermittelt, bei der der Dateninhalt durch ein sogenanntes Generatorpolynom (bzw. Prüfpolynom) „dividiert" wird. Der Divisionsrest dient als Prüfsequenz und wird nach den letzten Informationsbits gesendet.

Die Informationsbits werden dabei sequentiell in einen Puffer (Größe = Polynomgrad plus 1) geschrieben und dann sequentiell gesendet. Im Puffer erfolgt bei jedem Takt ein bitweises Exclusiv-Oder (EXO) mit den Koeffizienten des Generatorpolynoms, falls das führende Bit im Puffer den Wert „1" besitzt.

Im folgenden Beispiel verwenden wir aus rechentechnischen Gründen eine sehr kurze Sendebitfolge und ein sehr kleines Polynom.

Zu übertragen seien die Daten (10 Bits) - 1010001101

Als Prüfmuster dient das Polynom - $x^3 + x + 1$

a) Berechnen Sie daraus die Sicherungssequenz!
b) Belegen Sie Ihr Ergebnis dadurch, dass Sie den Empfang des korrekt gesendeten Frames überprüfen!

Hinweis

Der „Quotient" muss nicht berechnet werden, da nur der Rest benötigt wird.

23.13 Protokolle der Sicherungsschicht

a) Vergleichen Sie die Protokolle HDLC und PPP miteinander!

23.14 Überlaststeuerung

Beim Choke-Verfahren wird an einem Router eine Messreihe von relativen „Lastwerten" ermittelt. Dieser Lastwert repräsentiert z. B. die Länge einer Warteschlange. Kurzzeitige Überschreitungen einer Grenzlast (Schwellwert) werden toleriert, aber bei dauerhafter Überschreitung wird ein sogenanntes Choke-Paket an den Quellknoten gesendet. Dieser muss dann die Sendeleistung verringern (Standard 50 %) und steigert sie dann langsam wieder.

So spielt sich ein vernünftiges Gleichgewicht der Paketsenderate ein.

Periodisch wird folgende Berechnung im Router ausgeführt.

$$\text{Last}_{\text{neu}} = a * \text{Last}_{\text{alt}} + (1 - a) * \text{Last}_{\text{aktuell}}$$

Dabei bedeuten:		
	Last_{neu}	Schätzung der Last für nächsten Zeitraum
	a	Anpassungsfaktor (Konstante des „Vergessens" der Historie)
	Last_{alt}	Last des vorherigen Zeitraumes
	$\text{Last}_{\text{aktuell}}$	Wert der momentanen Last

Im folgenden Beispiel wird an einem Gateway-Rechner eine Messreihe von relativen „Lastwerten" ermittelt: {1/5/8/9/9}. Als Schwellwert wird 7,9 verwendet, als Anpassungsfaktor 0,3.

Wann wird ein Choke-Paket gesendet?

23.15 Einsatz von IP: Adressen und Subnetze

Die Kommunikation in modernen Rechnernetzen erfolgt auf der Basis der Internet-Technologie (TCP/IP). Als universelle Adressen werden die IPv4-Adressen eingesetzt.

a) Erläutern Sie den Aufbau der IPv4-Adressen und die Aufteilung des Adressraums in die Klassen A–D, sowie die Aufteilung durch Netzmasken!
b) Welche Unterschiede sehen Sie in der Nutzung von MAC- und IP-Adressen?
c) Erläutern Sie den Einsatz von Subnetzmasken beim Routing! Welche Vorteile bringt die Maskierung (s. ◘ Abb. 23.2)?

Berechnen Sie für die gegebene Skizze:

d1) Die Knotenadresse im Subnetz S1 ist A1 = 129.44.0.7, die Subnetzmaske ist M1 = 255.255.128.0. Definieren Sie die Subnetzadresse S1! Wie hoch ist die maximale Knotenanzahl X in diesem Subnetz?

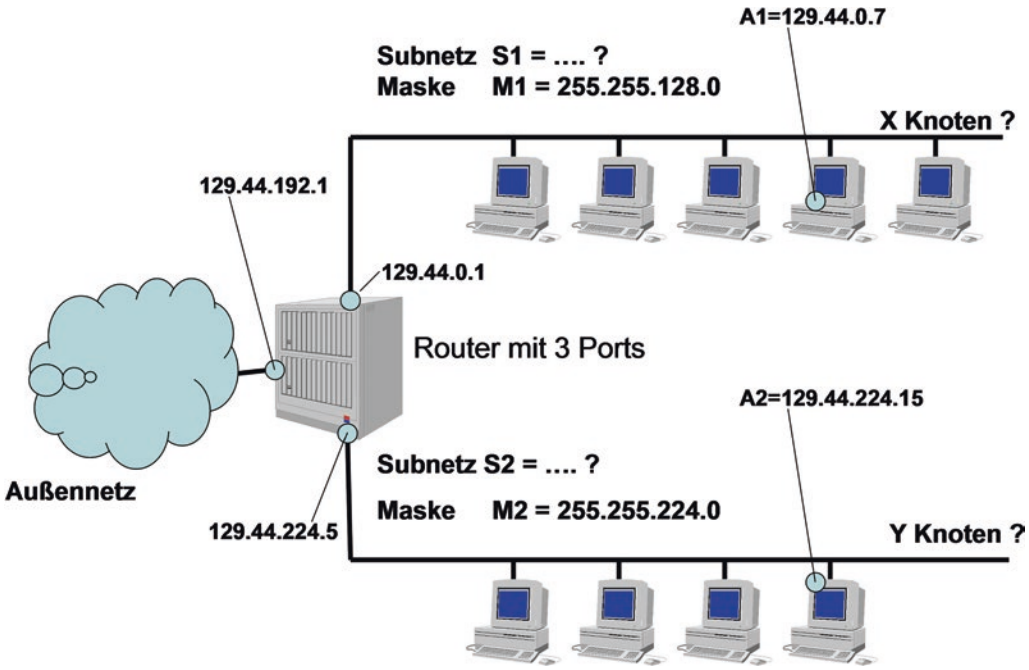


Abb. 23.2 Netzwerkszenario mit Router und Subnetting

d2) Die Knotenadresse im Subnetz S2 ist A2 = 129.44.224.15, die Subnetzmaske ist M2 = 255.255.224.0. Definieren Sie die Subnetzadresse S2! Wie hoch ist die maximale Knotenanzahl Y in diesem Subnetz?

23.16 Hilfsprotokolle zum Einsatz von IP

a) Erläutern Sie Aufgaben des Hilfsprotokolls ARP!
b) Erläutern Sie Aufgaben des Hilfsprotokolls DHCP!

23.17 Weiterentwicklung von IP: IPng

Als einige der wichtigsten Weiterentwicklungen von IP, oder IP Next Generation (IPng), gelten u. a. die Protokolle IPv6 und IPsec.

a) Diskutieren Sie Vor- und Nachteile von IPv6 im Vergleich zu IPv4!
b) IPsec stellt effiziente Sicherheitsmechanismen auf der Schicht 3 dar. Diskutieren Sie diese! Wie sehen die modifizierten IPsec-Pakete aus?

23.18 Quality of Service in der Transportschicht

Die Transportschicht lässt das Aushandeln von QoS-Parametern für die Kommunikation zwischen den Endsystemen in der Phase des Verbindungsaufbaues zu.

a) Welche Parameter kommen hierfür infrage? Diskutieren Sie diese!
b) Der Nutzer des Transportdienstes benötigt die folgenden QoS-Parameter:
kontinuierlich 1200 Byte/s, Verschlüsselung der zu übertragenden Daten.

Skizzieren Sie die Ablaufdiagramme für die nachfolgenden Szenarien:

b1) Der Responder kann die gewünschten Parameter erfüllen.
b2) Der Responder kann die Datenrate nur zu 75 % garantieren, nach Rücksprache mit der Anwendung akzeptiert der Initiator.
b3) Der Responder kann die Datenrate nur zu 75 % garantieren, der Initiator kann nicht akzeptieren und baut die Verbindung ab.
b4) Die Instanz zur Verschlüsselung beim Responder ist ausgefallen und es gibt keine Redundanz.

23.19 Ablauf- und Zustandsdiagramme für die Transportschicht

Ergänzen Sie die Aufgabe 23.1 um einen bestätigten Datentransfer für die Transportschicht.

Dienste müssen durch die untenstehenden Dienstprimitive realisiert werden.

Dienste	Zugehörige Dienstprimitive
Verbindungsaufbau	ConReq/ConInd/ConRsp/ConCnf
Datentransfer, bestätigt	DatReq/DatInd/DatRsp/DatCnf
Datentransfer, unbestätigt	DatReq/DatInd
Verbindungsabbau	DisReq/DisInd

a) Zeichnen Sie das Ablaufdiagramm für die Dienstfolge:

Verbindungsaufbau → Datentransfer, bestätigt → Verbindungsabbau!

b) Modellieren Sie die Aufgabe a) als Zustandsdiagramm!

23.20 Übersicht der Netzwerkfunktionen und Kommunikationsschichten

Ordnen Sie die Begriffe in der ersten Spalte der folgenden Tabelle den richtigen Kommunikationsschichten (Spalten 2–6) zu. In einigen Fällen kann ein Begriff mehreren Schichten zugeordnet werden. Als Schichten stehen die OSI-Schichten Bitübertragungsschicht, Sicherungsschicht, Vermittlungsschicht, Transportschicht und die Anwendungsschicht des TCP/IP-Referenzmodells zur Verfügung (◘ Tab. 23.1).

◘ **Tab. 23.1** Netzwerkfunktionen und Kommunikationsschichten. Tabelle zum Vervollständigen

Begriff	Bitübertragungsschicht	Sicherungsschicht	Vermittlungsschicht	Transportschicht	Anwendungsschicht
TCP als Bsp.	–	–	–	X	–
DHCP					
CSMA/CD					
BGPv4					
Client-Server-Anwendung					
DSL					
HTTPS					
IPv4					
UDP					
Koaxialkabel					
LWL					
Modem					
PPP					
Router					
Sockets					
Token Ring					
Twisted Pair					
WLAN					
Frequenzmultiplex					

Aufgaben zum Komplex II – Netzwerktechnologien und Mobile Kommunikation. Netzkopplung und Verkabelung

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_24

24.1 Multiprotocol Label Switching (MPLS)

a) Erläutern Sie den Aufbau eines MPLS-Tunnels! Wie setzt man die Labels?
(siehe Teil II Lehrbuch, ◘ Abb. 12.6)
b) Beschreiben Sie den Gesamtablauf zwischen dem Quell-Host, den Ingress/Egress-Routern und dem Ziel-Host in Stichworten!
c) Nennen Sie die wesentlichen Unterschiede zwischen MPLS und ATM!

24.2 Ethernet und ALOHA: stochastische Medienzugriffsverfahren

a) Geben Sie die Klassifikation von Medienzugriffsverfahren an!
Welche Medienzugriffsverfahren werden als „stochastisch" bezeichnet?
b) Wie groß ist die Mindestframelänge beim „klassischen Ethernet" IEEE 802.3?
c) Wie groß müssten die Frames bei einem busförmigen Netz der Länge 100 km, einer Datenrate von 100 Mbit/s und einer Signalausbreitungsgeschwindigkeit von 200.000 km/s mindestens sein?
d) Weshalb kann das CSMA/CD-Verfahren beim ALOHA-System nicht zum Einsatz kommen?

24.3 Netzwerktechnologien und WAN-Verbindungen

Im aufgeführten Beispiel (◘ Abb. 24.1) erfolgt der Zugriff zu den Diensten einer Cloud über „Thin Clients" mithilfe von Smartphones, Laptops oder PC/Desktops mit den folgenden Monatsdatenvolumina (V1, V2, V3, s. ◘ Tab. 24.1):
a) Welche Netzwerktechnologien ermöglichen diesen Zugriff? Nennen Sie 2–3 Beispiele!
b) Ergänzen Sie die unten aufgeführte Tabelle und kreuzen Sie zutreffendes an!
Konvention: 1 M = 1.000.000; 1 G = 10^9; 1 T = 10^{12}

Voraussetzungen Ein Monat hat im Schnitt 417 Arbeitsstunden, die durchschnittliche Auslastung der Verbindungen soll $\beta = 25\,\%$ nicht übersteigen, damit „burstartige" Belastungen abgefangen werden können (◘ Tab. 24.1).

Abb. 24.1 Netzwerkzugriff mithilfe von Smartphones, Laptops oder PC/Desktops

Tab. 24.1 Auswahl geeigneter Technologien zur Übertragung gegebener Volumina

Netzwerktyp	Typische DR, Mbit/s	$V_1 = 450$ TByte	$V_2 = 2{,}3$ TByte	$V_3 = 5$ TByte
ATM OC-3	155			
LTE	150			
DSL50	50			
HSDPA	14,4			
WLAN 802.11n	108…600			
10 GbE	10.000			

24.4 Netztechnologievergleich

Diskutieren Sie Vor- und Nachteile von MPLS, der Ethernet-Familie und ATM bei Einsatz als

- Last Mile Zugriff,
- Backbone,
- Lokales Netz

bezüglich

- Kosten,
- Dienstqualität (Anwendungen),
- Interoperabilität,
- Management,
- Datensicherheit.

Die Ergebnisse stellen Sie bitte tabellarisch dar!

24.5 Kopplungselemente: Transparent Bridges

Gegeben sei die folgende LAN-Topologie (◘ Abb. 24.2) mit den Rechnern A…E und den transparenten Bridges B1, B2:

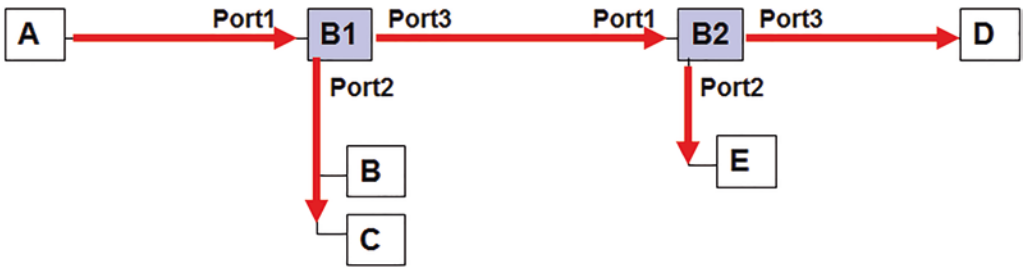
Wie werden die Wegewahltabellen bei transparenten Bridges aufgebaut?

a) Skizzieren Sie den Weg nacheinander gesendeter Frames mit folgenden Quell-/Zieladressen: (A/D), (B/A), (E/C), (B/E)!
b) Erfassen Sie in Tabellen, in welchen Schritten die Brücken ihre Kenntnisse über die Topologie des Netzes erwerben! Welche Informationen werten sie dazu aus?
c) Ergänzen Sie das Netz von b) um weitere Brücken, sodass alternative Wege möglich sind! Welche Probleme ergeben sich in diesem Fall für die Frameweiterleitung?
d) Benötigt man zur Lösung der Probleme von c) einen komplexen Routingalgorithmus (z. B. OSPF) oder gibt es einfachere Lösungen?

24.6 Strukturierte Verkabelung und Einsatz von Switches als Kopplungselemente (am Bsp. der Vernetzung eines Studentenwohnheims)

Für ein Studentenwohnheim mit 3 Etagen (je 10 Zimmer) mit Anschluss an das Campusnetz und an das Internet soll eine Netzkonzeption erarbeitet werden.

a) Diskutieren und vergleichen Sie mögliche Ansätze im Bereich der Verkabelung!
b) Was bedeutet der Begriff „Strukturierte Verkabelung“?
c) Wählen Sie geeignete Netztechnologien und dafür erforderliche Koppelelemente aus!



◘ **Abb. 24.2** LAN-Topologie mit Transparent Bridges

24.7 Firewall als Kopplungselement

a) Welche Basiskonzepte für die Firewalls sind Ihnen bekannt? Nennen Sie drei Firewallkonzepte und geben Sie ihre Zuordnung zu den OSI-Schichten an!
b) Nennen Sie Beispiele, bei denen die Verwendung eines Paketfilter-Firewalls ausreicht bzw. bei denen eine anwendungsbezogene Filterung erforderlich ist! Diskutieren Sie am Beispiel einer Schule.
c) Warum gibt es eine sog. demilitarisierte Zone (DMZ)?
d) In welcher Zone des Netzes können private Adressen eingesetzt werden? Welche Vorteile bringt dies?

24.8 Satellitenfunk

Wie lange dauert die Datenfunkübertragung eines Datenpakets mit Länge L = 1000 Byte zwischen einer terrestrischen Station und einem Satelliten (Uplink-Modus) auf der Orbithöhe h = 1200 km bei der maximalen Bitrate des Senders DR = 10 MBit/s?

a) Berechnen Sie die Gesamtzeit bei der Satellitenfunkkommunikation! Beachten Sie die korrekte und SI-konforme Umwandlung der Maßeinheiten!
b) Zu welcher Satellitenklasse (LEO, MEO, GEO) gehört der oben genannte Satellit? Welche Pro und Kontra haben Satelliten dieser Klasse?

24.9 Klassen von Satellitensystemen

Berechnen Sie die in der unten aufgeführten ◘ Tab. 24.2 fehlenden Angaben (ggf. Satellitenhöhe h oder Umlaufperiode T).

Hinweis

Die Umlaufperiode T ergibt sich zu $T = \text{sqrt}((R+h)^3/a)$ mit der Konstante

$$a = g * R^2/(2 * PI)^2$$

mit dem Erdradius R = 6378 km und der Konstante g = 9,81 N/kg (sqrt bedeutet Quadratwurzel).

Geben Sie Acht, dass Sie die richtigen Maßeinheiten verwenden!

Tab. 24.2 Zusammenhang Satellitenhöhe und Umlaufperiode. Tabelle mit fehlenden Angeben zum Ergänzen

Typ	Satellitenhöhe h	Umlaufperiode T
GEO (Geostationary Earth Orbit Satellite)	?	24 h
MEO (Middle Earth Orbit Satellite)	7000 km	?
LEO (Low Earth Orbit Satellite)	700 km	?
GPS (Global Positioning System, US NAVSTAR-Satellite)	20.200 km	?
ISS (International Space Station)	?	92 min

a) Berechnen Sie die lineare Geschwindigkeit v_{GPS} bei der gegebenen Satellitenhöhe h_{GPS} für GPS-Erdsatelliten mit der Umlaufperiode T_{GPS}!
b) Berechnen Sie die lineare Geschwindigkeit v_{ISS} bei der gegebenen Satellitenhöhe h_{ISS} für GPS-Erdsatelliten mit der Umlaufperiode T_{ISS}!

Hinweis zu a) und b)

$$v = (2PI/T)^{*}(R + h)$$

24.10 Frequenzspektrum und Funknetze

a) Werten Sie das nachfolgende Bild aus (Abb. 24.3). Geben Sie die Klassifikation von Frequenzbereichen und Wellenlängen an!
In welchem Frequenzbereich kommen die Funknetze zum Einsatz?
b) Welche Besonderheiten treten bei jeweiligen Wellentypen auf? Warum ist die LOS-Anforderung für Funkkommunikationssysteme von Bedeutung?
c) Typische Wellenlängen λ für Mobilfunkstandards sind nachfolgend aufgeführt:
   - GSM (890–960 MHz, 1710–1880 MHz), λ = 0,33 m (900 MHz)
   - WLAN IEEE 802.11b/g/n (2,4 GHz), λ = 0,125 m
   - WLAN IEEE 802.11a/n (5 GHz), λ = 0,06 m
   - WiMAX IEEE 802.16a (2–11 GHz), λ = 0,03 m (10 GHz)
   - WiMAX IEEE 802.16 (10–66 GHz), λ = 0,0045 m (66 GHz)

Wie hängen die Wellenlängen und Frequenzen zusammen?

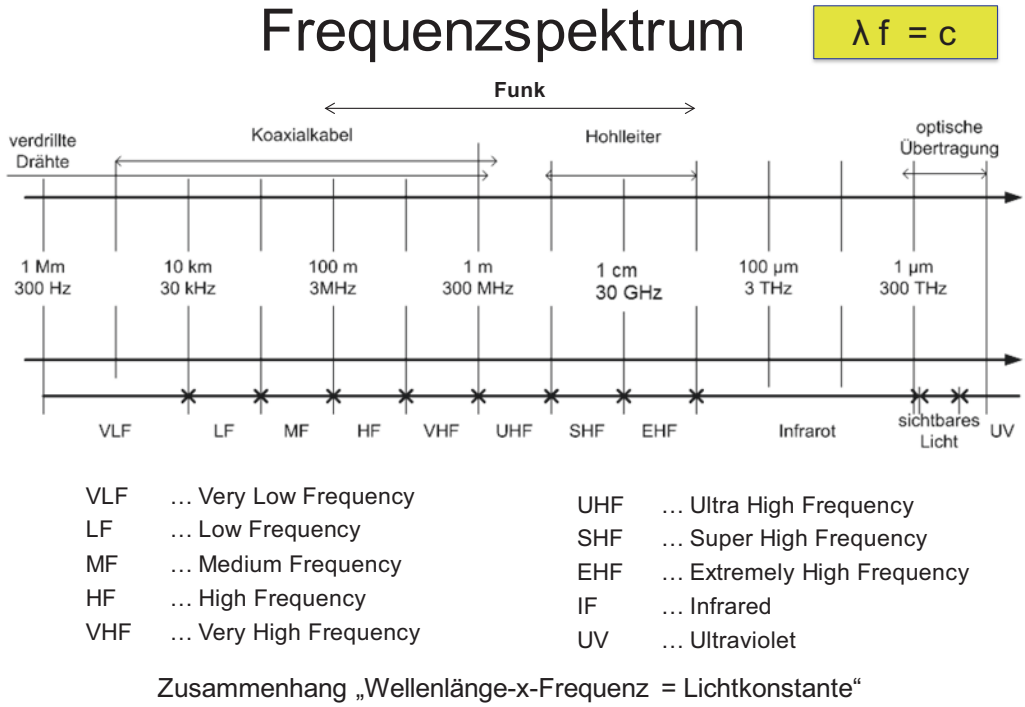


Abb. 24.3 EM-Schwingungen: Frequenzbereiche und Wellenlängen

24.11 Spektraleffizienz

a) Was versteht man unter dem Begriff „Spektraleffizienz“?
b) Wie errechnet sich maximale Spektraleffizienz eines Mobilfunksystems anhand der Nyquist- Theoreme?

24.12 Antennentechnik und Funknetze

a) Was ist eine Antenne? Welche Antennenarten kennen Sie? Welche Antennenarten kommen bei WLAN zum Einsatz? Welche Antennenarten kommen beim Mobilfunk zum Einsatz?
b) Diskutieren Sie Vorteile MIMO vs. SISO! Führen Sie entsprechende Systembeispiele an!
c) Diskutieren Sie die Unterschiede zwischen den Begriffen „Richtfunk“ vs. „Rundfunk“ vs. „Sektorantennen“!
d) Was ist Handover in Mobilfunknetzen? Verdeutlichen Sie den Begriff!

24.13 Freiraumdämpfung/EIRP

Das Freiraumdämpfungsmodell (FSL, oder Free Space Loss Model) stellt das einfachste aller denkbaren Simulationsmodelle für die Ausbreitung von elektromagnetischen Wellen dar. Dabei wird angenommen, dass sich das Sendesignal kugelförmig um die Sendeantenne verteilt (isotroper Kugelstrahler).

Zu einer ersten Abschätzung der Empfangsqualität kann das Modell genutzt werden, obwohl dämpfende Umgebungsobjekte (z. B. Wände) nicht berücksichtigt werden.

Die FSL-Dämpfung kann nach folgenden Formeln berechnet werden, wobei d den Abstand zwischen Sende- und Empfangsantenne bedeutet, λ die Wellenlänge und f die Frequenz.

$$\mathbf{FRD} = \mathbf{Sendeleistung/Empfangsleistung}$$
$$= (\mathbf{4}\pi * \mathbf{d}/\lambda)^{\mathbf{2}} = (\mathbf{4}\pi * \mathbf{f} * \mathbf{d}/\mathbf{c})^{\mathbf{2}}$$

In der Praxis verwendet man meist die logarithmierte Form (Angabe in dB)

$$\mathbf{FRD_{log}} = \mathbf{10} * \mathbf{log}(\mathbf{FRD}) = \mathbf{32{,}44} + \mathbf{20} * \mathbf{log}(\mathbf{f/MHz}) + \mathbf{20} * \mathbf{log}(\mathbf{d/km})$$

a) In einem WLAN ist ein Access Point im Außenbereich installiert mit der Sendefrequenz 2,4 GHz und der Sendeleistung Ptx = 30 mW. Wie groß ist die Empfangsleistung Prx in 35 m Abstand? (Wenden Sie das Modell der Freiraumdämpfung an.)
Vergleichen Sie die Ergebnisse nach den obigen zwei Formeln.

b) Ab welchem Abstand ist der Empfang nicht mehr möglich (Empfangsleistung unter 10^{-10} W)?

Der Gesetzgeber beschränkt die zulässige Sendeleistung, z. B. für WLAN 802.11b/g auf eine max. EIRP-Leistung von 100 mW. Für die Bestimmung der zulässigen Sendeleistung muss der Gewinn der verwendeten Antenne abgezogen werden.

c) Wie hoch darf die max. Sendeleistung bei IEEE 802.11g sein, wenn eine Sendeantenne mit einem Gewinn von 12 dBi eingesetzt wird?

24.14 FSL-Modelle im Mobilfunk

In der Mikrozelle eines Mobilfunknetzes im zugewiesenen Frequenzband von F = 2 GHz beträgt die minimale Empfangsfeldstärke den Wert PRx = 92,5 dB. Dies entspricht dem maximalen Pfadverlust PL (Path Loss) im Freien (s. Free Space Loss Model bzw. vorige Aufgabe!).

a) Schätzen Sie die maximale Reichweite d bzw. Zellradius für das Mobilfunknetz ab!
   Betrachten Sie das FSL-Ausleuchtungsmodell (Freiraumdämpfung) zum Modellieren der Pfadverluste!
b) Lösen Sie die Aufgabe bei dem minimal zulässigen Wert PRx = 72,5 dB.
   Schätzen Sie die maximale Reichweite in diesem Fall ab.
   Wie ändert sich das Ergebnis?

Hinweis
Basierend auf dem Teil II Lehrbuch bzw. Buch [11]:
Vorsicht ist bei den Maßeinheiten geboten, z. B. liefert die Frequenzangabe in GHz und die Distanzangabe in km:

$$\mathbf{FRD_{log} = 10 * log(FRD) = 92{,}44 + 20 * log(f/GHz) + 20 * log(d/km)}$$

24.15 Weitere Ausbreitungsaspekte in Funknetzen

a) Welche Funksignalausbreitungsaspekte soll man bei Aufbau von Funkkommunikationssystemen berücksichtigen? Geben Sie entsprechende Szenarien an.
b) Diskutieren Sie die wichtigsten Effekte der Wellenausbreitung je nach Wellenlänge!

Aufgaben zum Komplex III – Verarbeitungsorientierte Schichten und Netzwerkanwendungen

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze,* https://doi.org/10.1007/978-3-658-25617-3_25

25.1 Klassische Internetapplikationen

a) Warum ist es sinnvoll, dass einige Anwendungen anstelle des Transportprotokolls TCP das weniger leistungsfähige Protokoll UDP nutzen?
b) In welchen Fällen ist es sinnvoll, Dateien mittels des SMTP-Protokolls zu verschicken und in welchen Fällen eignet sich das Protokoll FTP besser?
c) Welche Gefahren entstehen bei Nutzung des TELNET-Protokolls?
Zeigen Sie mögliche Maßnahmen zum Schutz auf!

25.2 Cloud Computing

In der Entwicklung der Rechnernetzwerktechnik gab es immer wieder Vorstellungen, die Funktionalität der Arbeitsstationen auf eine reine Terminalfunktion (Thin Client) zu begrenzen und alle Verarbeitungsfunktionen transparent in das Netzwerk auszulagern.

a) Vergleichen Sie die Unterschiede in der Last-/Funktionenverteilung zwischen Cloud Computing und herkömmlicher IT vs. SaaS vs. PaaS vs. IaaS!
b) Ordnen Sie die Cloud-Einsatzszenarios in der ersten Spalte der folgenden ◘ Tab. 25.1 den richtigen Mustern von Cloud-Diensten (Spalten 2–4) zu. In einigen Fällen kann ein Begriff mehreren Mustern/Spalten zugeordnet werden:

◘ **Tab. 25.1** Cloud-Einsatzszenarien

Dienstmuster	IaaS	PaaS	SaaS
– Cloud Backup			
– Data Center			
– VM Migration			
– Market Place			
– Hochleistungscluster für paralleles Rechnen			
– SOA Plattform			
– Test-Umgebung			
– Frontend			

25.3 Multimediale Netzwerkanwendungen und Mobilfunk

Eine Videostreaming wird mit dem Standard UXGA verwirklicht. Dieser ermöglicht die Bildauflösung von $V = 1600 \times 1200$ Pixel. Dabei wird die Farbkodierung $FT = 24$ Bit genutzt sowie die Bildfrequenz $fps = 25$ Bild/s. Diese Übertragung wird

a) zuerst ohne Kompression per Festnetzmietleitung vorgenommen.
   Wie groß muss die verfügbare Datenrate sein, wenn keine Kompression möglich ist?
b) Welche Netzwerktechnologien sind für diese Videostreaming ohne Kompression am besten geeignet?
c) Die beschriebene Videoübertragung wird per Mobilfunk mit Kompressionsverfahren vorgenommen. Bei welchen Kompressionsraten KR ist diese Übertragung möglich, wenn die folgenden maximalen Datenraten bei Mobilfunk mittlerweile verfügbar sind. Bereichen Sie diese Werte und ergänzen Sie die angegebene Tabelle (ggf. aufrunden!):

Mobilfunknetz	Max. DR	Die zu berechnende Kompressionsrate KR
HSDPA	14,4 MBit/s	?
LTE	150 MBit/s	?

25.4 SNMP-Management

a) Angegeben seien ein Server mit installierter Managersoftware und ein Switch mit einem Agenten, zwischen denen SNMP-Nachrichten verkehren. Die beiden verweisen auf eine MIB. Ergänzen Sie das in ◘ Abb. 25.1 vorgegebene Weg-Zeit-Diagramm (Ablaufdiagramm).

25.5 Architekturwandlung in modernen Verteilten Systemen

Unsere Zeit wird durch die signifikante Architekturwandlung in Netzwerkservices und verteilten Systemen charakterisiert. Die Verarbeitungs-, Persistenz- und Anwendungsdaten werden von mehreren Servern oder Peers bereitgestellt.

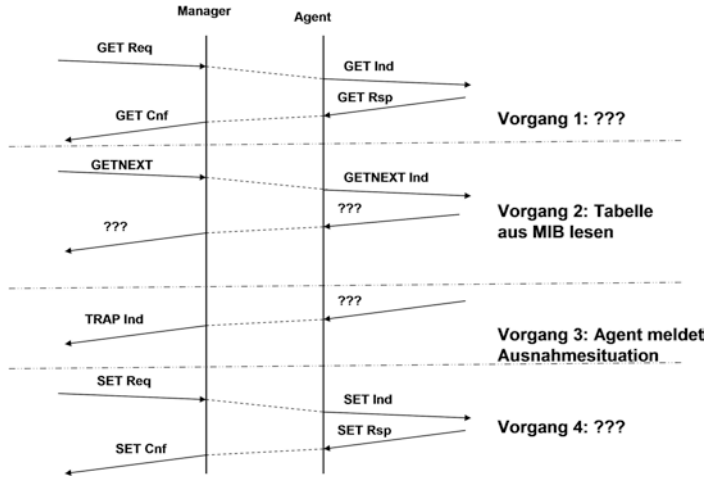


Abb. 25.1 SNMP-Ablaufdiagramm zum Vervollständigen

a) Ergänzen Sie das unten aufgeführte Organigramm!
Vergleichen Sie die Client-Server- und Peer-To-Peer-Architekturen (C-S/P2P) in Abb. 25.2.
Führen Sie jeweils 2–3 Beispiele an!
b) Erklären Sie die Funktionsweise von hybriden P2P/C-S-Systemen in Stichworten!
Nennen Sie jeweils drei Systembeispiele zu jedem der aufgeführten Architekturtypen mit der Erläuterung des Einsatzgebietes (s. Abb. 25.3)!

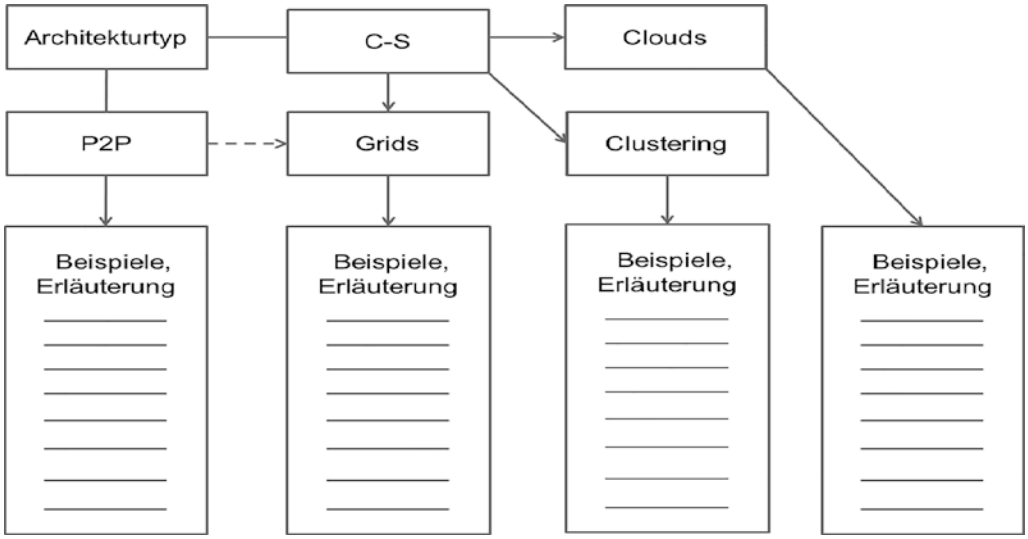


Abb. 25.2 Client-Server- und Peer-To-Peer-Architekturen

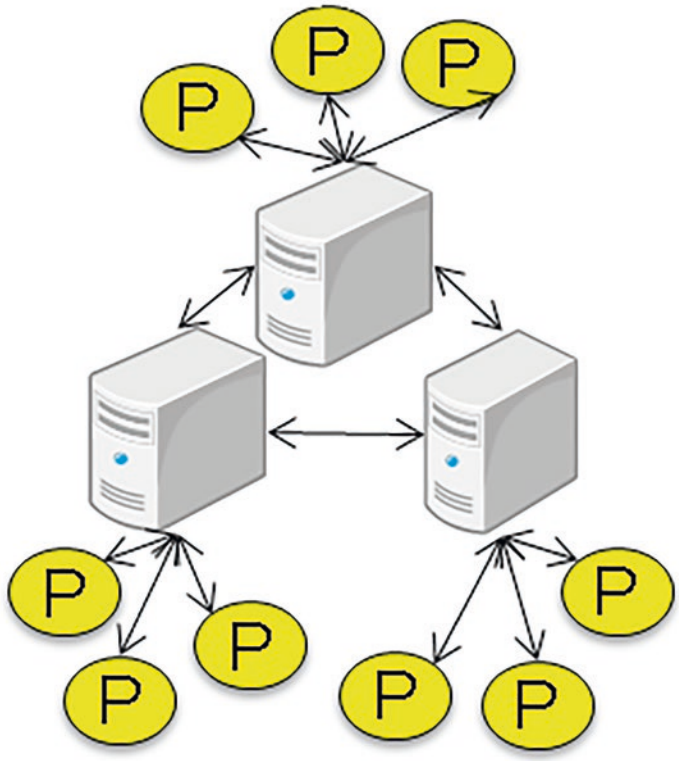


Abb. 25.3 Hybrides P2P

25.6 Videokonferenzen

Folgendes Szenario ist gegeben (s. Abb. 18.7, Teil III Lehrbuch): Sie möchten mit mehreren Partnern eine Videokonferenz aufbauen. Sie nutzen ein Mehrpunktkonferenzsystem mit einer sternförmigen Architektur und einer zentralen MCU (Multipoint Control Unit). Sie senden Ihr Video mit der Auflösung CIF mit einer Farbtiefe von 24 Bit/Pixel und einer Framerate von 15 fps.

a) Mit welchem Kompressionsfaktor müssen Sie ihr zu sendendes Videosignal komprimieren, wenn Sie einen Internetanschluss (Upstream: 192 kbit/s, Downstream: 2048 kbit/s) nutzen?
b) Mit wie vielen Partnern können Sie eine Videokonferenz aufbauen, wenn alle Partner Videos mit der gleichen Qualität mit dem Faktor 200:1 komprimiert senden und 10 % Overhead durch Protokoll-Header entsteht?

c) Im Regelfall sollte man aber nur maximal 60 % der zur Verfügung stehenden Bandbreite für die Videoübertragung nutzen. Wie kann die zu übertragene Datenmenge angepasst werden, damit Sie weiterhin mit allen Partnern kommunizieren können? Wie wirkt sich das auf die Qualität der Videos aus?

25.7 Fortgeschrittene Sicherheit in Netzwerken: Firewalls und CIDN

Eine Firewall ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt und ist auch ein wichtiger Teilaspekt eines Netzwerks.

a) Vergleichen Sie die IDS/IPS-Module (Intrusion Detection und Intrusion Prevention Systems) mit „klassischen" Firewalls! Verdeutlichen Sie die Unterschiede!
b) Nennen Sie Beispiele, bei denen die Verwendung eines Paketfilter-Firewalls ausreicht bzw. bei denen eine anwendungsbezogene Filterung erforderlich ist!
c) Wofür dient ein Circuit Relay?
d) Ergänzen Sie die folgende Tabelle (◘ Tab. 25.2) der Filtermöglichkeiten von Firewallsystemen. Ordnen Sie die Filterungsmöglichkeiten in der ersten Spalte der folgenden Tabelle den richtigen FW-Konzepten (Spalten 2–5) zu. In einigen Fällen kann ein Begriff mehreren Mustern/Spalten zugeordnet werden:
e) Warum gibt es eine mehrstufige Firewall-Strategie? Diskutieren Sie anhand des unten aufgeführten Diagramms (◘ Abb. 25.4)!
f) Was ist CIDN?
Welche Arten von Angriffen verhindern diese?

25.8 Kryptografische Absicherung in den Rechnernetzapplikationen

a) Kann es sinnvoll sein, in mehreren Netzarchitektur-Schichten Verschlüsselungsalgorithmen einzusetzen? Nennen Sie Beispiele!
b) Kann der Empfänger einer digital signierten Nachricht den Nachrichteninhalt verändern und eine passende Signatur erzeugen?
c) Wie kann man die folgende Aussage kommentieren: „TLS/SSL bietet stärkere Feingranularität bei der Absicherung für die Rechnernetzapplikationen als VPN/IPsec".
Aus welchem Grund kann man dies behaupten?

Tab. 25.2 Filtermöglichkeiten von Firewallsystemen. Tabelle zum Vervollständigen

Filterungsmöglichkeiten	PF (Paketfilter)	CR (Circuit Relay)	AG (Application Gateway)	Fortgeschrittenes FW-System
Zeitfensterkontrolle				
IP-Adressen und DMZ (Demilitarized Zone)				
Intrusion Detection und Intrusion Prevention Systems: IDS/IPS				
Zugelassene/verbotene Protokolle				
Malware-Blockierung, SPAM-Filter und Antiphishing				
Anwendungsbezogene Authentisierung und Verschlüsselung				
Proxy für bestimmte Dienste, Proxyserver				
Ausführbare Skripte, Applets, Web Services				
Web Application Firewall				
TCP-Ports und Blockierung von DDoS				
Bitte „X" falls zutreffend!				

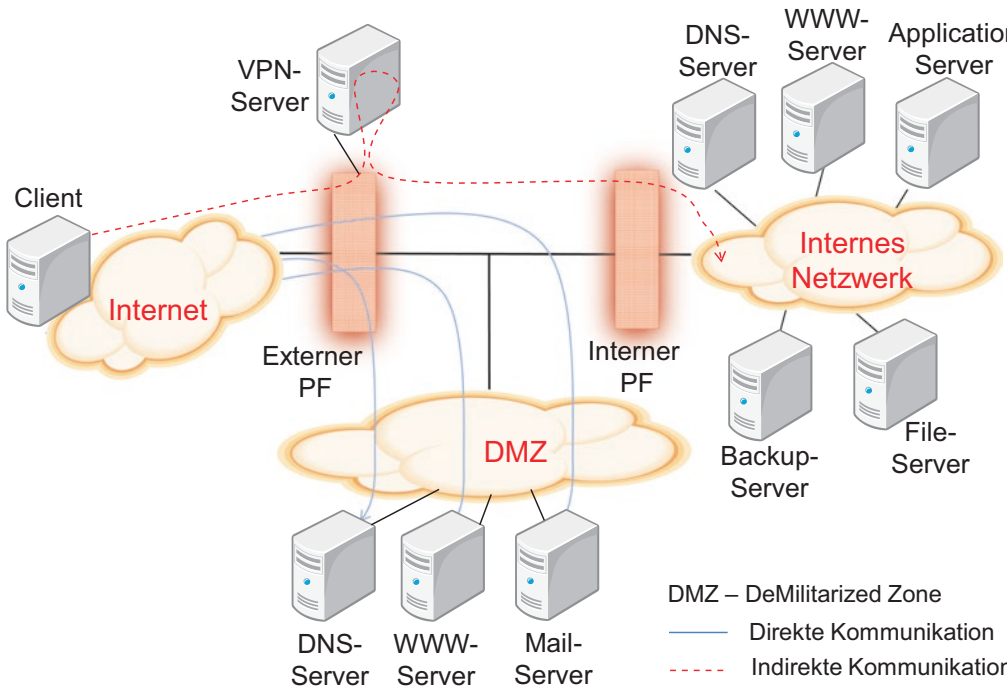


Abb. 25.4 DMZ und mehrstufige Firewall-Strategie

25.9 Kryptoprotokolle

Kryptoprotokolle sind Netzwerkprotokolle (i. d. R. Layer 3 bis 7), die die verschlüsselte und authentifizierte Datenübertragung über ein Computernetzwerk für die Verteilten Anwendungen garantieren.

a) Ergänzen Sie das Bild!
Definieren Sie die fehlenden Kryptoprotokolle (Abb. 25.5)!

b) Ordnen Sie die folgenden Kryptoprotokolle in der ersten Spalte der folgenden Tabelle (alphabetisch sortiert) den richtigen Kommunikationsschichten (Spalten 2–5) zu.
Vermerk: In einigen Fällen kann ein Begriff mehreren Schichten zugeordnet werden, außerdem sind manche Begriffe gar keine Kryptoprotokolle! Als Schichten stehen die OSI-Schichten und die Schichten des TCP/IP-Referenzmodells zur Verfügung (Tab. 25.3):

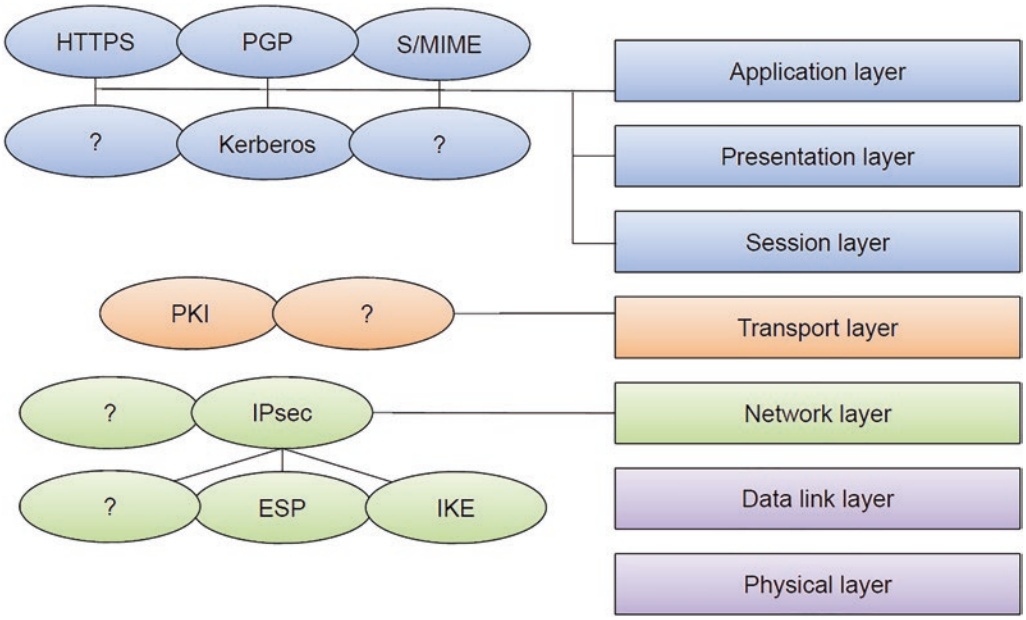


Abb. 25.5 Ausgewählte Kryptoprotokolle mit OSI-Schichtenzuordnung zum Vervollständigen

Tab. 25.3 Einordnung von Kryptoprotokollen. Tabelle zum Vervollständigen

Begriff	Vermittlungsschicht L3	Transportschicht L4	Anwendung L5–L7
AH			
ESP			
HTTPS			
IKE			
IPsec			
IRC			
IRCS			
PGP			
POP3			
PKI			
RSVP			
S/MIME			
SET			
Socket			
VPN			
VoIP			
TLS/SSL			

25.10 Backup und Cloud Backup

In einem Modellbetrieb bzw. KMU (Klein- und Mittelstandsunternehmen) erfolgt die Datenvollsicherung bzw. Cloud Vollbackup über die bestehenden VDSL und MPLS-Netzwerkverbindungen immer freitags um ca. 21 h. Außerdem finden weitere regelmäßige Backups statt.

Dafür werden zwei folgenden Verfahren eingesetzt:

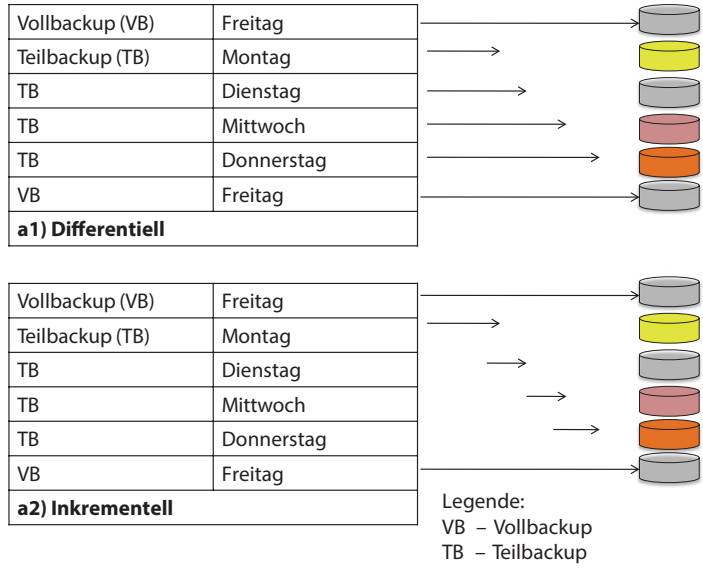
- IB, steht für Inkrementelles Backup;
- DB, steht Differentielles Backup.

a) Ordnen Sie die Begriffe IB und DB den unten aufgeführten Bildern zu (◘ Abb. 25.6)!

b) Diskutieren Sie jeweils zwei Pro- und zwei Contra-Argumente für die beiden Verfahren. Vergleichen Sie die beiden Verfahren anhand der angegebenen Tabelle. Die unten angegebene Tabelle ist auszufüllen!

Backup/Datensicherungsverfahren	IB	DB
Vorteile	1. 2.	1. 2.
Nachteile	1. 2.	1. 2.

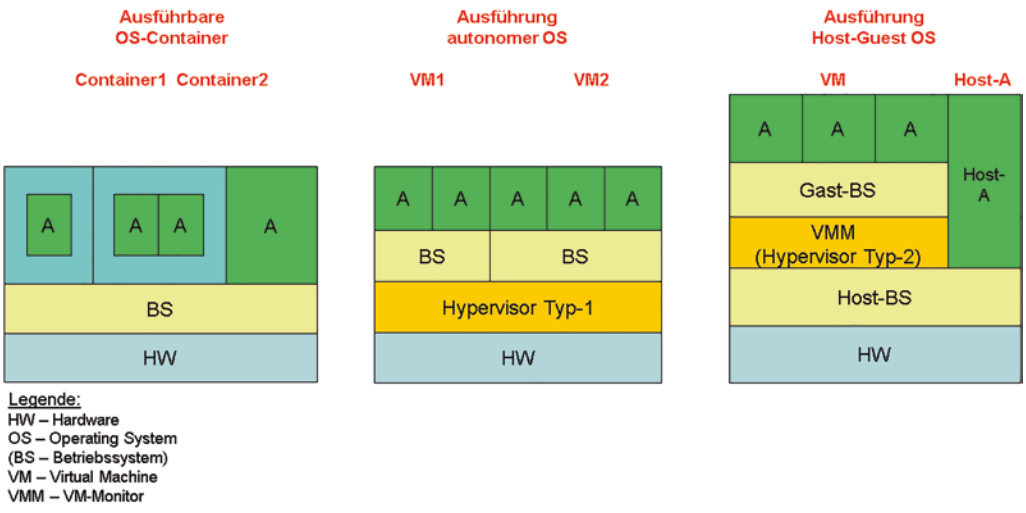
c) Nennen Sie die wesentlichen Nachteile der Cloud Backup Lösung (mind. 2)?



◘ **Abb. 25.6** Backup-Strategien

25.11 Virtualisierungsverfahren in Rechnernetzen

a) Was bedeutet der Begriff „Virtualisierung“ in aktuellen Rechnernetzen und Verteilten Systemen (Rechnerarchitekturen, Betriebssystemen und Applikationen)?
b) Existierende Virtualisierungsverfahren ermöglichen den Heterogenitätsabbau in aktuellen Rechnernetzen und im Mobilfunkumfeld (s. ◘ Abb. 25.7).
Dafür kommen die folgenden Konzepte zum Einsatz: OS-Container, Hypervisor (Typ-1) und VM-Monitor (Hypervisor Typ-2).
Welche Vorteile haben OS-Container bzw. im Mobilfunkumfeld gegenüber Hypervisor Typ-1 oder Typ-2?
Nennen Sie wichtige Systembeispiele zum Konzept OS-Container!
c) Warum bietet ein Hypervisor Typ-1 eine günstigere Alternative zu einem VM-Monitor (Typ-2)? Nennen Sie mind. 2 Argumente diesbezüglich!
d) Nennen Sie mind. 3 Systembeispiele der Betriebssystemvirtualisierung (bedeutende Produkte am Markt)!
e) Ein leistungsstarker physikalischer Server in einem Mittelstandsunternehmen trägt 40 VM je mit dem Hauptspeicher 4 GB und der Festplatte 6 TB (s. ◘ Abb. 25.8)
Welche Mindestkapazitätsanforderungen und wieviel Reserve muss der Server haben? Begründen Sie den Vorschlag!



◘ **Abb. 25.7** Vergleich von Virtualisierungskonzepten: OS-Container, Hypervisor (Typ-1), VM-Monitor (Hypervisor Typ-2)

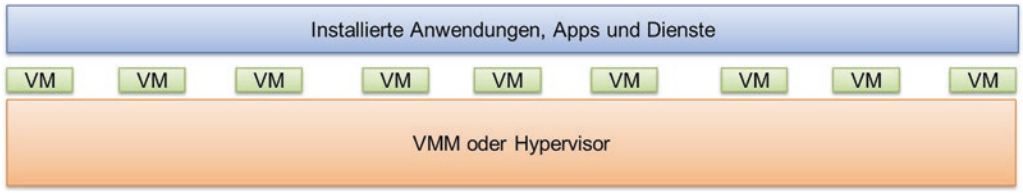


Abb. 25.8 Virtualisierungsszenario: Hypervisor oder Monitor, virtuelle Maschinen, installierte Anwendungen, Apps und Dienste

f) Wieviel Hauptspeicher insgesamt und welche gesamte Festplattenkapazität kann der phys. Server in dem Falle haben, um einen einwandfreien Betrieb von diesen 50 VM mit 10 %-Reserve zu gewährleisten? Begründen Sie den Vorschlag!

25.12 Entwicklungstrends in Rechnernetzen

a) Verdeutlichen Sie die Unterschiede zwischen IoT und IoS!
b) Was ist Fog Computing!
Beschreiben Sie kurz die wichtigsten Netzwerktechnologien, die Fog Computing unterstützen!
c) Verdeutlichen Sie die Unterschiede zwischen Clouds und Fog Computing?
Wie wird die Koexistenz gewährleistet?

Serviceteil

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze*, https://doi.org/10.1007/978-3-658-25617-3

Glossar zu den Teilen I-II-III

Begriff, Abkürzung	Kurzname	Erläuterung
1. AMPS/1G, auch NMT/A-Netz	Advanced Mobile Phone System, auch Nordic Mobile Telephone	Analoges Mobilfunknetz in den USA der „1G“ sowie NMT: Skandinavien, nordische Länder, A-Netz: Deutschland
2. GSM/2G	GSM (Global System for mobile Telecommunication)	2.Generation des Mobilfunks: GSM und GSM-Erweiterungen weltweit, u. a. GPRS – General Packet Radio Service (der paketvermittelnde Dienst für Datenübertragung)
3. 2G–5G	Generationen des digitalen Mobilfunks	Migration von leitungsvermittelnden zu den paketvermittelnden Systemen mit der Tendenz zum Datenratenwachstum um Faktor 10–100 pro Jahrzehnt
4. UMTS/3G	IMT2000 (in Europa: Universal Mobile Telecommunications System)	International Mobile Telecommunications by the year 2000 (Datenrate ca. 2 Mbit/s)
5. 4G, LTE, LTE-II	Long Term Evolution, versch. Release	Aktueller Standard des Mobilfunks, 4.Generation mit paketvermittelnden Daten- und Sprachservices, erhöhten Datenraten ab 150 Mbit/s und kürzeren Latenzen bei 5 ms
6. 5G	IMT2020	International Mobile Telecommunications by the year 2020, künftiger Standard für 5G, Vernetzung per SDN, Netzwerksfunktionalitätsvirtualisierung (NFV), Interoperabilität mit LTE, WLAN, Sensorpikonetzen und Satellitenfunk, Latenz unter 1 ms und Datenraten bis 10 GBit/s
7. 6LoWPAN	IPv6 over Low power Wireless Personal Area Network	IPv6 für WPAN mit niedrigem Energieverbrauch, ein Kommunikationsprotokoll für drahtlose Pikonetze mit dem Header-Kompressionsverfahren für IPv6-Pakete über IEEE-802.15.4/ZigBee
8. AES	Advanced Encryption Standard, 1998–2003 eingeführt	Entwickelt von Vincent Rijmen und Joan Daemen (Belgien) und durch NIST (USA) mit Schlüsseln der Länge 128/256 Bit standardisiert
9. AJAX	Asynchronous Java and XML	Teil der Java-Technik für abgekoppelte Kommunikation des Webbrowsers mit dem Webserver
10. ATM	Asynchronous Transfer Mode	Kommunikationsprotokoll in breitbandigen (optischen) Netzwerken, geeignet zur Übertragung von Daten, Sprache und Video mit QoS-Garantien, jedoch Produkte und Management sind verhältnismäßig teuer im Vgl. zu MPLS und DSL
11. B2B	Modus „Business-to-Business“ bei EAI	Integration von Rechnernetzanwendungen zwischen den Unternehmen (oft mittels MW und WS)

Begriff, Abkürzung	Kurzname	Erläuterung
12. B2C	Modus „Business-to-Consummer“ bei EAI	Integration von Rechnernetzanwendungen und Apps zwischen Unternehmen und Endusern (oft mittels MW und WS)
13. BYOD	„Bring Your Own Device!“	Integrationskonzepte privater mobiler Endgeräte in den Netzwerken von Unternehmen
14. Caching	Performanceoptimierung in vert. Anwendungen	Betriebsystem oder Software belässt gewisse häufig genutzte Ressourcen im (Client-) Arbeitsspeicher (im Cache), auch nach dem Ende deren Benutzung
15. CBC	Cipher Block Chaining Mode	Sicherere Betriebsart mit Verkettung der Chiffreblöcke per XOR, in der Blockchiffren betrieben werden können
16. CDMA	Code Division Multiple Access	Codemultiplexverfahren für die gleichzeitige Übertragung verschiedener Datenströme im gemeinsamen Frequenzbereich, Übertragungskanälen werden verschiedene Codes dauerhaft zugewiesen
17. CIDN	Collaborative Intrusion Detection Network	Netzwerk aus den Knoten mit IDS (Intrusion Detection System) zum kooperierendem Entdecken und Verhindern von Malware und untersagten Aktivitäten
18. Cloud Computing	„Rechnen in den Wolken“	Ressourcennutzung und Datenspeicherung in einem entfernten Rechenzentrum (in einer Cloud)
19. DES	Data Encryption Standard, 1972–1977 eingeführt	Entwickelt und standardisiert von IBM, NSA, NIST/ ehemals NBS (USA) mit Schlüsseln der Länge 56/168 Bit, wird durch AES ersetzt
20. DSL, xDSL	„Digital Subscriber Line“: S – Symmetric, A – Asymmetric, VH – Very High Speed	Reihe von Übertragungsstandards der Bitübertragungsschicht, effizientes Zugangsnetz, nutzt FDM und OFDM-Verfahren zur Datenübertragung
21. DSSS	Direct Sequence Spread Spectrum	Bandspreizverfahren mit Verwendung einer Chipping-Bitsequenz als Spreizcode im zu übertragenden Code
22. EAI	Enterprise Application Integration	Anpassung und Integration von Anwendungen im Unternehmen nach ihren Schnittstellen, Austauschformaten, Protokollen, (Middleware-)Komponenten und erbrachten (Web-)Services
23. EnOcean	Drahtlose Pikosensornetze mit Energy Harvesting, EU-Standard	Herstellerübergreifende Spezifikation für batterielose Pikosensornetze (Energy Harvesting) in der Gebäudeautomation
24. Ethernet	Verbreitete Technologie für LAN	Vom klassischen busförmigen Ethernet mit „Shared Medium“ bis zum 100 GBit/s – schnellem Switched Ethernet mit individueller Kopplung nach dem Standard IEEE 802.3
25. FDM, FDMA	Frequency Division Multiple Access	Frequenzmultiplex, Übertragungskanälen werden verschiedene Frequenzen dauerhaft zugewiesen
26. FHSS	Frequency Hopping Spread Spectrum	Bandspreizverfahren durch Frequenzsprünge, Frequenz wird um Median variiert

Begriff, Abkürzung	Kurzname	Erläuterung
27. Fog Computing	„Rechnen im Nebel“, i. d. R. in der Kooperation mit Clouds	System mit energieautarken autonomen Knoten, deren Funktionalität „on Edge“ d. h. zum User delegiert wird
28. GALILEO	EU-Satellitennavigations-system	Europäisches ziviles Satellitennavigations- und Zeitgebungssystem
29. GEO	Geostationary Earth Orbit	Geostationäres Satellitensystem mit der Orbithöhe bei ca. 35.786 km
30. GLONASS	Globales Navigations-system	Navigationssystem der RF (nur in Kooperation mit GPS und Galileo funktionsfähig)
31. GPRS	General Packet Radio Service	Paketorientierter Dienst zur Datenübertragung in GSM-Netzen
32. GPS	Global Positioning System, Globales Satellitennavigations-system, NAVSTAR GPS	Globales Positionsbestimmungssystem (Inbetrieb-nahme seit 1985 in den USA)
33. GSM	Global System for Mobile Communications	Erster weltweiter Standard für volldigitale, zellulare Mobilfunknetze, 10 kbit/s im Schnitt, Standard der „2G“
34. HSDPA/HSUPA	High Speed Downlink/ Uplink Packet Access	Beschleunigte Datenübertragungsverfahren für Mobilfunkstandard UMTS „3G“ bei der Downlink/ Uplink-Kommunikation (Datenrate ca. 14 Mbit/s)
35. IDL	Interface Definition Language	C-konforme Schnittstellensprache bei den RMI-Methodenfernaufrufen
36. IDS	Intrusion Detection System	Systeme zum Entdecken und Verhindern von Malware und untersagten Aktivitäten als Firewall-Ergänzungen
37. IEEE	Institute of Electrical and Electronics Engineers	Weltweiter Berufsverband für Standardisierung und Normungen von Netzwerktechniken, Hardware und Software
38. IEEE 802.11	WiFi/WLAN	„Wireless Fidelity“-Consortium zur Entwicklung von WLAN, Wireless Local Area Network (internationaler Standard für drahtlose lokale Netze)
39. IEEE 802.15	WPAN	Wireless Personal Area Network (Internationaler Standard für drahtlose Pikonetze)
40. IEEE 802.15.1	Bluetooth, WPAN	Wireless Personal Area Network, drahtlose Ver-netzung im Nahbereich (Pikonetze)
41. IEEE 802.15.4	WSN	Wireless Sensor Network, drahtlose Pikonetze
42. IEEE 802.16	WiMAX	„Worldwide Interoperability for Microwave Access“-Consortium zur Entwicklung des int. Standards für drahtlose Netze im städtischen und Weitverkehrs-bereich
43. IEEE 802.20	MBWA	Mobile Broadband Wireless Access (Standard für drahtlosen, mobilen Internetzugang in Netzwerken)

Begriff, Abkürzung	Kurzname	Erläuterung
44. IEEE 802.3	Ethernet-Familie mit der Bezeichnungen von 10Base-X bis zu 100000Base-X	Inkludiert gängige Standards wie Ethernet, Fast Ethernet, Gigabit Ethernet, 10 GbE, 40 GbE und 100 GbE
45. Industrie 4.0 (2011)	4.-te industrielle Revolution	Industrie 4.0 (2011) ist ein zukünftiges wichtiges Ziel in der High-Tech-Strategie der Bundesregierung. Weiterentwicklung der industriellen Automatisierung mit Einsatz von RFIDs, intelligenter Vernetzung und IoT, sowie der Techniken der virtuellen Realität und 3D-Druckers
46. IoS	Internet of Services	Beschreibt, wie die Funktionalitäten in die Clouds massenhaft portiert werden; Zugriff erfolgt mithilfe von (Web-)Services
47. IoT	Internet of Things (Internet der Dinge)	Konzept beschreibt, wie Rechner zunehmend verschwinden und durch kleine „intelligente Gegenstände“ mit IP-basierter Kommunikation ersetzt werden
48. IPsec	IP Security	Kryptografisch abgesichertes IP, die IP-Pakete werden per AH-Subprotokoll authentisiert und per ESP-Protokoll (Encapsulation Security Payload) verschlüsselt. Die Protokollheader werden entsprechend modifiziert
49. ISDN	Integrated Service Digital Network	Internationaler Standard für digitales Telekommunikationsnetz
50. ISM	Industrial, Scientific and Medical Band	Lizenzfrei Frequenzbereiche, die durch Hochfrequenz-Geräte genutzt werden können, z. B. 2,4 GHz-Band
51. JSP	Java Server Pages	Teil der Java-Technik zur Implementierung serverseitiger Skripte in Webanwendungen
52. JVM	Java Virtual Machine	Ausführungsumgebung je Betriebssystem für universellen Java Bytecode, ermöglicht weitgehende Portierbarkeit der Java-Quellcodes
53. LAN	Local-Area Network	Lokales Netzwerk (drahtlos/drahtgebunden)
54. LEO	Low Earth Orbit	Niedrige Erdumlaufbahn, Höhe 200–2000 km, energieärmste Bahnen
55. LOS/NLOS	Line-of-Sight/Non-Line-of-Sight	Anforderung des Vorhandenseins einer Sichtlinie in Funkkommunikation bei den Hochfrequenzen (GHz/Microwave)
56. LTE	Long Term Evolution	Mobilfunkstandard der 4G, beinhaltet Grundschema von UMTS, Übergang zur 5G
57. MEO	Medium Earth Orbit	Mittlere Erdumlaufbahn, Höhe 2000–36.000 km, zwischen GEO und LEO, genutzt (bspw. für Navigationssysteme GPS, GALILEO etc.)

Begriff, Abkürzung	Kurzname	Erläuterung
58. Middleware Components	Middleware-Komponenten	Middleware-Komponente verrichtet eine Kommunikationsaufgabe unter Nutzung von Fernaufrufmechanismen wie PRC oder RMI. Intern kann eine Middleware-Komponente in einer beliebigen Programmiersprache realisiert sein
59. MPLS	Multiprotocol Label Switching	Integrationstechnik für die Vorläufertechniken wie ATM, Frame Relay, sowie DSL, VPN, ermöglicht effiziente Übertragung von Datenpaketen in einem verbindungslosen Netz entlang eines zuvor reservierten Pfade
60. MW	Middleware	Middleware ist eine Verteilungsplattform zur Ausführung und ein Protokollset von höheren OSI-Schichten zur Unterstützung der Kommunikation zwischen Clients und Servern; eines der grundlegenden Konzepte von Verteilter Systemen und in der Informatik. Unter Middleware versteht man Komponenten der Kommunikationssoftware, die zwischen der Anwendungssoftware (dem Client und Server) sowie dem Betriebssystem angesiedelt werden; Middleware dient der vereinfachten und standardisierten Kommunikation der Komponenten einer vert. Anwendung oder App. Ein Webservice ist lediglich eine spezifische dienstorientierte Middleware-Komponente mit Webschnittstelle
61. NAS, SAN	Network Attached Storage und Storage-Area-Network	SAN und NAS sind verwandte Konzepte für Speichernetzwerk mit schnellem Zugriff durch optische Links wie bspw. Fibre Channel
62. NFC	Near Field Communication	Drahtlose Vernetzung im Nahbereich
63. ODFMA	OFDM Access	OFDM-basiertes Protokoll der 2.Schicht mit der Zuweisung der Trägerfrequenzen und breitem Einsatz bspw. bei DSL, LTE, WLAN, Bluetooth und 5G, nutzt das Modulationsverfahren mit mehreren orthogonalen Trägern zur digitalen Datenübertragung
64. OFDM	Orthogonal Frequency Division Multiplex	Aktuelles Frequenzmultiplex- sowie Fourier-Transformation-basiertes Codierungsverfahren mit der Auswahl von leicht-überlappenden Spektren mit minimaler Interferenz und maximaler Spektraleffizienz
65. PGP/OpenPGP	„Pretty Good Privacy", eine ziemlich gute Privatsphäre	Ein offener Standard (seit 1991), ursprünglich von P. Zimmermann entwickelt als freies kryptografisches Rahmenprogramm für zivile Zwecke
66. PKI	Public Key Infrastructure: X.509 oder Kerberos	Vergabe der öffentlichen Schlüssel per Zertifikate, die von den vertrauenswürdigen Zertifizierungsstellen ausgestellt wurden; Überprüfung der Integrität öffentlicher Schlüssel und Nachweis der Zuordnung von Benutzernamen und Schlüssel für digitale Unterschrift

Begriff, Abkürzung	Kurzname	Erläuterung
67. PSTN	Public Switched Telehone Network	Festnetz, Gesamtheit aller öffentlichen leitungsgebundenen Telefonnetze
68. QoE	Quality of Experience, Dienstgüte in der Praxis	Praktische positive Anwenderserfahrungen mit einem Kommunikationsdienst (Websurfing, Telefonie, Fernsehebroadcasting, Call Center, Cloud etc.); Robustheit der Dienstgüte bei der Entfernung zur Basisstation, zum Data Center oder zur Cloud sowie an der Peripherie des Netzwerks
69. QoS	Quality of Service, Dienstgüte	QoS beschreibt die Güte eines Kommunikationsdienstes aus der Sicht der Anwender (Datenrate, Latenz, Jitter, Verlustrate etc.), QoS wird per Dienstvertrag ausgehandelt
70. Replikation	Performanceoptimierung in vert. Anwendungen durch Redundanz	Vermehrung, mehrfache Reservierung der Ressourcen in vert. Anwendungen zwecks deren erhöhter Verfügbarkeit und Skalierbarkeit mit integrierten Synchronisationsmechanismen für Datenkonsistenz
71. RFID	Radio-Frequency Identification	Berührungslose Identifizierung und Lokalisieren von Objekten und Lebewesen mit Radiowellen
72. RMI	Remote Method Invocation (1990er)	Fernaufruf der Methode in einem verteilten Objekt, gängiger Mechanismus zur Client-Server-Kommunikation in verteilten Anwendungen und Apps (Middleware und Webservices)
73. RPC	Remote Procedure Call (1980er)	Fernaufruf einer Prozedur, Mechanismus zur Client-Server-Kommunikation in verteilten Anwendungen und Apps (Middleware und Webservices)
74. RSA	Rivest-Shamir-Adleman-Chiffre, 1977–1983 eingeführt	Entwickelt von Ron Rivest, Adi Shamir, Leonard Adleman (USA-Israel) und standardisiert durch RSA Security, ANSI, IEEE mit Schlüsseln der Länge 1024/2048 Bit
75. SDH	Synchronous Digital Hierarchy	Multiplextechnik im Bereich der Telekommunikation, erlaubt das Zusammenfassen von niederratigen Datenströmen zu einem hochratigen, wichtige Grundlage für SONET, ATM etc
76. SDMA	Space Division Multiple Access	Raummultiplex bei Rundfunksendern und im analogen Telefonsystem
77. SDN	Software-Defined Network	Organisation der virtuellen Providernetzwerke verschiedener Art über spezielle Controller-Software für Clouds und Cluster, oft unter Nutzung der Protokolle OpenFlow oder VXLAN
78. SET	Secure Electronic Transactions	Schwergewichtiges Kryptoprotokoll zur Absicherung der Transaktionen mit Kreditkarten, wird in der Praxis oft mit TLS/SSl kombiniert

Begriff, Abkürzung	Kurzname	Erläuterung
79. Smart Grid	Intelligentes Stromnetz	Kommunikative und energieeffiziente Vernetzung und Steuerung von Stromerzeugern und -Speichern, intelligente und energieeffiziente Netzdienste über vorhandene Stromnetzeinfrastuktur („Delivery Grids"), Interoperabilität mit DSL und Powerline sowie energieeffiziente Cluster („Green IT")
80. SOA	Service-Oriented Architecture	Architektur objektorientierter verteilter Anwendungen unter Nutzung von Webservices und -Komponenten zur effizienten Kommunikation zwecks EAI und Ankopplung „Business-to-Business"
81. SOAP	Service-Oriented Application Protocol (ursprünglich „Simple Object Access Protocol")	Netzwerkprotokoll für XML-kodierte Fernaufrufe (XML-RPC) in Webservice-Technik
82. TCP	Transmission Control Protocol	Verbindungsorientiertes Transportschichtprotokoll mit Paketbestätigung, Fehlerbehandlung und Flusssteuerung
83. TDM, TDMA	Time Division Multiple Access	Zeitmultiplexverfahren, jedem zu übertragenden Datenstrom wird entsprechender Timeslot (oder bei Bedarf mehrere Timeslots) zugewiesen
84. TLS/SSL	Transport Layer Security/ Secure Socket Layer	Kryptografisch abgesichertes verbindungsorientiertes Protokoll zur Kommunikation über die Socket-Schnittstelle per TCP mit gegenseitiger Authentisierung von Kommunikationspartnern und Schlüsselverteilung per PKI X.509
85. UDDI	Universal Description Discovery and Integration für Webservices	Auskunfts- und Verzeichnisdienst (UDDI ist selbst als WS realisiert); Informationen vom UDDI-Service können anhand des Dienstnamens abgefragt werden (white pages) oder über Angaben von Attributen (yellow pages; eine Art Branchenbuch) oder technischer Details (green pages)
86. UDP	User Datagram Protocol	Verbindungsloses Transportschichtprotokoll ohne Fehlerbehandlung und Flussteuerung
87. UMTS	Universal Mobile Telecommunications System	Europäischer Mobilfunkstandard „3G", digital, leitungs- und paketvermittelnd
88. URI, URL	Uniform Resource Locator/Identifier	Universelle DNS-konforme Adressenbezeichner für Webressourcen und Webservices
89. VLAN	Virtual Local-Area Network	Virtualisiertes LAN zwecks Abgrenzung und Absicherung organisatorischer Bereiche im LAN, kann als Teil des SDN betrachtet werden
90. VM	Virtual Machine	Virtuelle Ausführungsumgebung für ein Betriebssystem (Linux, Windows, mobile OS) oder einen spezifischen rechnerunabhängigen Code (Java Bytecode)
91. VPN	Virtual Private Network	Ein kryptografisch abgesichertes Tunnel-Netzwerk über die öffentliche Weitverkehrsnetze

Begriff, Abkürzung	Kurzname	Erläuterung
92. VS	Verteiltes System bzw. vert. Anwendung setzt eine Rechnernetzinfrastruktur voraus	Verteilte Systeme werden vor allem für folgende Zwecke eingesetzt [15, 16]: – gemeinsame Nutzung von Daten – gemeinsame Nutzung von Geräten – gemeinsame Nutzung von Rechenleistung – Kommunikation der Benutzer eines VS Die fünf wesentlichen Merkmale der Verteilten Systeme sind wie folgt [16]: – Kopplung räumlich verteilter Rechner mittels Rechnernetz – Kooperation mit dem Ziel, eine bestimmte Anwendungsfunktionalität (Kooperationsaufgabe) zu erbringen – Kein gemeinsamer physikalischer Speicher, keine strikt synchronisierten Uhren – Dezentrale Organisation und Verwaltung – Häufig auch Fehlertoleranz und Lastausgleich durch Replikation Eine schärfere Abgrenzung zwischen „generischen VS“, „Cluster Computing“, „Grid Computing“ und „Cloud Computing“ gibt es nicht
93. WAN	Wide-Area-Network	Weitverkehrsnetz wie MPLS, ATM, DSL sowie 3G, 4G
94. WS	Webservice, Webdienst	Software-Anwendung, die über einen URI eindeutig identifiziert wird. WS können mit anderen Software-Agenten interagieren unter Verwendung XML-basierter Nachrichten durch den Austausch über internetbasierte Protokolle. Intern kann ein WS in einer beliebigen Programmiersprache realisiert sein (vergleichbar Middleware-Komponenten)
95. WSDL	Web Service Description Service	Beschreibung der Nutzerschnittstelle von WS (Ausführung ist transparent)

Begriff, Abkürzung	Kurzname	Erläuterung
96. XaaS	Everything as a Service	Allgemeine Schablone, die einen Ansatz bezeichnet, „alles" als Service zur Verfügung zu stellen und zu konsumieren: a) SaaS (Software as a Service) Die Software wird in der Cloud bereitgestellt bspw. ein virtuelles Betriebsystem oder Front-End für Onlinegamer b) PaaS (Platform as a Service) bspw. wird eine Testumgebung für einen Cross-assembler zur Verfügung gestellt oder eine Produktivumgebung vieler leistungsfähiger VM oder ein Applikation Server zur Ausführung von Webservices im Modus „Business-to-Business" c) IaaS (Infrastructure as a Service) bspw. geht es um einen (virtuellen) Cloud-speicher für Nutzerdaten oder um einen Cluster leistungsfähiger Server, die für anspruchsvolle Simulationen in der Cloud angemietet werden können
97. XML	Extensible Markup Language, die erweiterbare Auszeichnungssprache	Auszeichnungssprache zur Darstellung verschiedener objektorientierter Dokumentenmodelle mit dem Mapping zu den existierenden Software, Programmier- und Darstellungssprachen, ist gut für den plattformunabhängigen Austausch geeignet
98. ZigBee	Drahtlose Pikosensornetze nach IEEE-802.15.4	Spezifikation für drahtlose Pikosensornetze mit geringem Datenaufkommen in der Gebäudeautomation, baut auf IEEE 802.15.4 auf

Literatur

1. Blokland, K., J. Mengerink, M. Pol, und D. Rubruck. 2016. *Cloud-Services testen. Von der Risikobetrachtung zu wirksamen Testmaßnahmen*, 1. Aufl. Heidelberg: dpunkt (ISBN 978-3864903496).
2. Diskreter Event Network Simulator für das Internet NS-3. 2017. ► https://www.nsnam.org/. Zugegriffen: 25. Mai 2020.
3. Gütter, Dietbert. 2017. Netzwerkpraxis für Lehramt, Manuskript der TU Dresden (Print).
4. Gütter, Dietbert. 2017. Betriebssysteme und Rechnernetze, Manuskript der TU Dresden (Print).
5. Kersken, Sascha. 2007. *IT-Handbuch für Fachinformatiker. Der Ausbildungsbegleiter*, 3., aktualisierte und erweiterte Aufl., 1014. Bonn: Galileo Computing (ISBN 978-3-8362-1015-7).
6. Luntovskyy, Andriy. 2017. Rechnernetze im 4.Semester, Manuskript der BA Dresden (Print). Wiesbaden: Springer Vieweg.
7. Luntovskyy, Andriy. 2017. Verteilte Systeme im 5.Semester, Manuskript der BA Dresden (Print).
8. Luntovskyy, Andriy. 2017. Mobile Kommunikation und Telematik im 5.Semester, Manuskript der BA Dresden (Print).
9. Luntovskyy, Andriy. 2017. Netzwerkpraxis und neue Technologien. Wandel in Architekturen von Netzwerken undVerteilten Systemen und Telematik im 6.Semester, Manuskript der BA Dresden (Print).
10. Luntovskyy, Andriy, und Josef Spillner. 2017. *Architectural transformations in network services and distributed systems: Service vision. Case studies*, XXIV, 344. Springer (ISBN: 978-3-658-14840-9, 238 color pict.).
11. Luntovskyy, Andriy, Dietbert Guetter, und Igor Melnyk. 2011. *Planung und Optimierung von Rechnernetzen: Methoden, Modelle, Tools für Entwurf, Diagnose und Management im Lebenszyklus von drahtgebundenen und drahtlosen Rechnernetzen*, 435. Wiesbaden: V+T/Springer Fachmedien Wiesbaden GmbH (ISBN: 978-3-8348-1458-6).
12. OMNeT++ Discrete Event Simulator: Objective Modular Network Testbed in C++ and Simulations-Framework. 2017. ► https://omnetpp.org/. Zugegriffen: 25. Mai 2020.
13. Peterson, L. L., und B. S. Davie. 2011. *Computer networks. A system approach*, 5. Aufl., 920. Burlington, Massachusetts: Morgan Kaufmann (ISBN: 978-0-12-385059-1).
14. Schill, Alexande, und Thomas Springer. 2012. *Verteilte Systeme – Grundlagen und Basistechnologien*, 2. Aufl., 433. Heidelberg: Springer Verlag (ISBN: 978-3-642-25795-7).
15. Schneider, U., Hrsg. 2012. *Taschenbuch der Informatik*, 7. Aufl., 736. München: Carl-Hanser Verlag (ISBN: 978-3-44642638-2).
16. Skripte der Professur Rechnernetze. 2017. ► http://www.rn.inf.tu-dresden.de/. Zugegriffen: 25. Mai 2020.
17. Tanenbaum, Andrew S., und David J. Wetherall. 2012. *Computernetzwerke*, 5., aktualisierte Aufl., 1040. München: Pearson Studium (ISBN: 978-3-8689-4137-1).
18. Tanenbaum, Andrew S., und Herbert Bos. 2016. *Moderne Betriebssysteme*, 4., aktualisierte Aufl., 1313. München: Pearson Studium (ISBN 978-3-8632-6766-7).
19. Tanenbaum, Andrew S., und Todd Austin. 2014. *Rechnerarchitektur: Von der digitalen Logik zum Parallelrechner*, 6., aktualisierte Aufl., 802. München: Pearson Studium (ISBN 978-3-8632-6687-5).
20. Wireshark Homepage. 2017. ► https://www.wireshark.org/. Zugegriffen: 25. Mai 2020.