UNIVERSITÄT LEIPZIG

Scriptum zur Lehrveranstaltung

Rechnernetze

(Architektur, Schichten, Protokolle, Internet und WWW,
ausgewählte Netze und Dienste)

Teil 1
(Architektur von Rechnernetzen)

wird gegenwärtig aktualisiert
Stand: 22.11.2011

Studiengang Informatik, Kernfach Rechnernetze (UL)
Studiengang Praktische Informatik (BA)
Umfang: 2 SWS
15 Wochen

Prof. Dr.-Ing. habil. Klaus Irmscher
Universität Leipzig
Institut für Informatik
Lehrstuhl Rechnernetze und Verteilte Systeme (em.)

Dresden, den 11. September 2011

Gliederung
Teil 1 (Architektur von Rechnernetzen): Kap. 1 ... 9
Teil IntW3 (Internet und WWW): Kap. 10 ... 11
Teil 2 (Ausgewählte Netze): Kap. 12 ... 18
Teil 3 (Übertragungssysteme): Kap. 19 ... 22

Teil 1: Architektur von Rechnernetzen

1 Einführung zu Rechnernetzen

1.1 Rechnernetze und Verteilte Systeme

Information und Kommunikation

Information:

Grundelemente der Kybernetik: Stoff, Energie, Information (an materielle Träger gebunden). Aspekte der Information: syntaktisch (Grammatik), semantisch (Inhalt), pragmatisch (Bedeutung). Träger der Information: elektrische bzw. optische Signale (Kupferkabel, Glasfaser, Funkwelle). Funk: elektromagnetische Wellen

Kommunikation:

Austausch bzw. Übertragung von Informationen (IPC und Telekommunikation).
Kommunikationsmedien:

- Kabelgebunden (wired): Kupferkabel / Koaxialkabel / Lichtwellenleiter
- Kabellos (wireless): Elektromagnetische Wellen (Funk) / Infrarot / Satellitenfunk

Rechtsträgerschaft:

- Öffentliche Netze (i.allg. Telefon- u. Datennetze, ISDN, B-ISDN, Backbones, Satelliten)
- Privatnetze (LAN, MAN, HS-LAN, WAN, Mobilfunknetze, WLAN, WPAN)

Zielstellungen und Merkmale der Kommunikation

- Datentransfer, z.B. FTP, downloads
- Zugriff auf (entfernte) Informationen: Daten (DBS), Informationen (WWW, News), neue Internet-Technologien, u.a. Web 2.0; Programme (RJE, telnet)
- Nachrichtenaustausch: asynchron (SMS, E-Mail), synchron (Audio/Videokonferenz)
- allseitige Erreichbarkeit: Kabel, kabellos (Modem, Funk, Satellit): ubiquitous, nomadic
- Verteilkommunikation (vs. Individualkommunikation): Rundfunk, Fernsehen
- Neue Einsatzformen, z.B. Teleworking (CSCW: Computer Supported Cooperative Work), Teleteaching (Distance Learning), Telepräsenz (Steuerung entfernter Prozesse), Grid-Computing, Social Networks, Cloud-Computing

Ursprung der Datenübertragung (Nachrichtentechnik, Datennetze) - Auswahl -

1833	Gauß, Weber	elektromagnetischer Telegraf	)
1840	Morse	Einführung Telegraf in Praxis (Behörde)	)
1861	Reiss	) Telefon	) Individual-
1876	Bell, Gray	) (erste Individualkomm.)	) kommunikation
1877	1. Fernsprechvermittlung in Deutschland (von Hand)		)
1892	Strowger	elektromagnetischer Wähler	)
1900	Funktelegraphie	elektromagnet. Wellen („Funken“)	)
1923	Hörfunk		) Verteil-
1936	Fernsehen		) kommunikation
1958	öbl A (analoges Mobilfunknetz)		)
1969	ARPA		)
1964	Satellitenkommunikation		)
1976	Ethernet (Gigabit-Ethernet 1998)		) Rechnernetze,
1983	Internet (NCP -> TCP/IP)		) Mobilfunknetze
1988	ISDN, B-ISDN (ATM, 1992)		)
1992	GSM (digitales Mobilfunknetz), X.25 -> IP		)
2000	GPRS, SDH/WDM -> optische Netze		)

Kommunikationsformen
Austausch/Übertragung von Informationen. Unterscheidung je übermittelter Information:
Textkommunikation:
- Austausch von Informationen (Symbole einer natürlichen oder künstlichen Sprache)
- für das menschliches Verständnis bestimmt und verfügbar auf Papier oder Display

Datenkommunikation:
- Austausch binärcodierter Informationen
- Komm.-Partner: Geräte zum Senden/Empfangen binärcodierter Daten (Computer ...)
- Anwendungen, u.a. Daten- und Rechnernetze, DFV, Teledienste, Informationssysteme, Büroautomatisierung

Sprachkommunikation (audio):
- Austausch auditiver Medien (Sprache, Musik, Geräusche),
- analoge / digitale Übertragung (Telefonie, Handy, VoIP)

Bild- und Videokommunikation (video)
- Austausch visueller Medien (Standbild, Bewegtbild (Videosequenz), Film, Animation)
- grau-skaliert, farbig; analog / digital
- Anwendungen: u.a. Multimedia, Videokonferenzsysteme, WWW, Podcasting

Klassifikation
Fernschreib- und Fernsprech-typische Netze (niederratig)
- Netze für Telefon, Telefax, Telex, Teletext, ...
- analog / digital (z.B. PSTN, ISDN); kabelgebunden

Mobilfunknetze
- Zellularfunknetze (2G ... 4G: GSM, UMTS, LTE), Bündelfunk, Funkruf, Satelliten
- WLAN, W-ATM, WPAN (Infrarot, Bluetooth), RFID, NFC

Datennetze
- i.allg. öffentlich verwaltete Netze; digital, mit Signalisierungssystem (z.B. SS7)
- Paketvermittlung (z.B. X.25, Frame Relay, IP), Access Network (z.B. xDSL, WLL)

Rechnernetze
- LAN / MAN / WAN -> Schwerpunkt IP (Internet)
- Novell-Ethernet, Gigabit-Ethernet, Internet, B-ISDN/ATM, optische Netze (SDH/WDM)

Verbund von Rechnernetzen
- Internetworking (Repeater, Bridges, Switches, Router, Gateway)
- Backbones (z.B. WiN, TEN-34/155, GÉANT, Ebone, Abilene/NGnet)

Rechnerverbundsysteme
Bis zur Mitte der 80er Jahre dominierten **zentralisierte Rechner**, die über lokale oder entfernte Terminals genutzt wurden (Datenfernverarbeitung). Zwei grundlegende Entwicklungen führten zur Abkehr von dieser Richtung: preiswerte, leistungsfähige Arbeitsplatzrechner und allseitige Vernetzung derselben über Kabel und Funk.

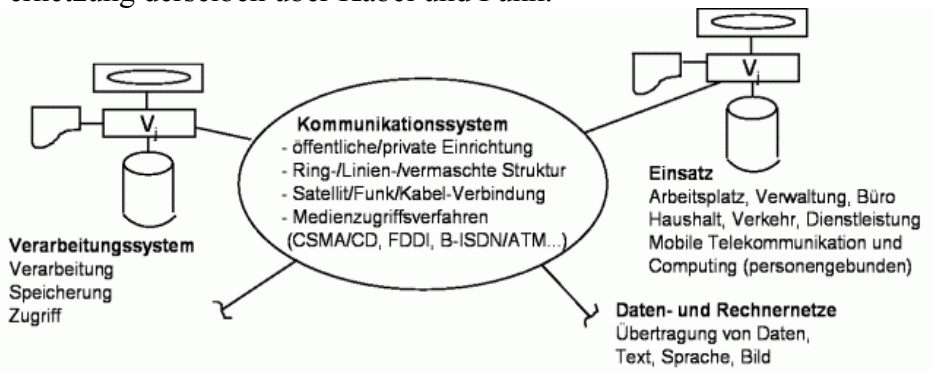


Abbildung 1.1: Verteiltes Rechnersystem / Rechnernetz

Es entstanden **Rechnerverbundsysteme**, die aus autonomen Rechnern und einem Kommunikationssystem („Rechnernetz“) bestehen (Philip Enslow jr., 1977). Wichtige Merkmale dieser Systeme sind die Aufteilung der Ressourcen (Hardware und Software), Verbundfunktionen, wie Nachrichten, Last, Verfügbarkeit und ihr heterogener Aufbau, der zusammen mit einer Ressourcenverwaltung die Basis bildet.

Begriffe **Verteiltes System** und **Rechnernetz** (z.T. synonym gebraucht). Rechnernetz: Transportsystem, Verteiltes System: Verteilte Anwendung (Basis Rechnernetz, Verteilungsplattform, ...). Rechnernetz transparent, unabhängig, auf welchem Rechner die Anwendung installiert ist. Verteiltes System als Menge autonomer Subsysteme, die koordiniert kooperieren, um gemeinsame Aufgabe zu bearbeiten und über Kommunikationseinrichtungen verbunden sind ~> siehe auch Script zu Verteilte Systeme!

1.2 Grundbegriffe

1.2.1 Verbundsysteme

Datennetze: i.allg. öffentlich bzw. privat (Regulierung), paketvermittelt (vs. Telefonnetze: leitungsvermittelt); bilden Trägerdienst für Rechnernetze bzw. Teledienste.

Rechnerverbundsysteme („Rechnernetze“): Verbund mehrerer Rechner, die Informationen austauschen und autonom bzw. gemeinsam eine Aufgabe bearbeiten. Verschiedene Formen:

- *Mehrrechnersysteme*:
  Loser Verbund, starke gegenseitige Abhängigkeit, Master/Slave-Prinzip (kein “verteiltes System”). Beispiele: Doppelrechner (Sicherheit), Asynchrones Mehrrechnersystem (HASP), Cluster-Systeme (Ausfallsicherheit)
- *Rechner- / Computer- Netze*
  Mehrere miteinander verbundene, unabhängige Rechner (Autonomie), Realisierung von Verbundfunktionen. Kabelgebundene/kabellose Netze ~> WAN, LAN, MAN (HS-LAN). Beispiele: Internet, Gigabit-Netze, B-ISDN/ATM, SDH/WDM, optische Netze.
- *Netze von Rechnernetzen*
  Verbindung (heterogener) Netze über Repeater, Bridges, Switches, Router, Gateways (je nach Kopplungsschicht) ~> Internetworking. Beispiele: Backbone-Netze, Zugangsnetze.
- *Infrastrukturnetze / Ad-hoc-Netze*

Konfiguration eines Rechnerverbundsystems (Beispiel):

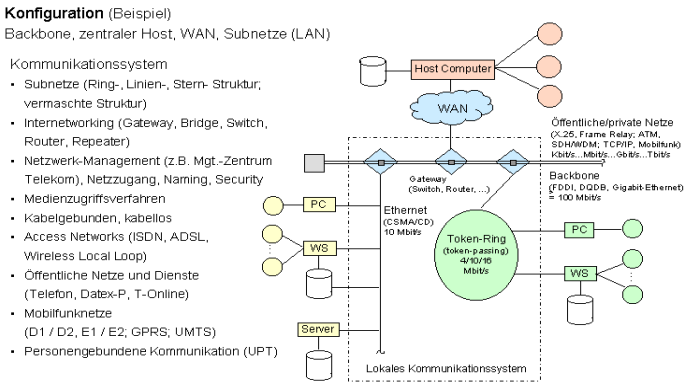


Abbildung 1.2: Konfiguration Rechnerverbundsystem (Beispiel)

Rechnernetz
Ein Rechnernetz ist ein verteiltes System miteinander verbundener, autonomer (unabhängiger), programmierbarer Computer. Die Computer arbeiten autonom oder im Verbund an der Lösung einer Aufgabe. Der Informationsaustausch erfolgt über ein Kommunikationssystem.

Rechnernetze stellt Dienste für Nutzer bereit:
- Verarbeitungs- und Speicherleistungen (z.B. Cloud)
- Rechnernetz-gebundener Nachrichtenaustausch
- Verfügbarkeit über im RN vorhandenen Daten bzw. Programme und Dienste (z.B. Web).

Komponenten eines Rechnernetzes:
- Computer (“Teilnehmercomputer”, ”Host”)
- Nachrichtenkanäle bzw. Datennetz für die Verbindung der Teilnehmercomputer
- System von Steuer- und Kommunikationskomponenten (ermöglichen wechselseitige Inanspruchnahme von Diensten).

Architektur von Rechnernetzen: Satz von Protokollen, Diensten und Schichten.

Verbundfunktionen

Alle Computer sind logisch erreichbar, keine physische Direktverbindung erforderlich. Realisierung von Verbundfunktionen:

Lastverbund: Verteilung Arbeitslast (infolge Nutzeraufträge) auf Gesamtsystem.
Ziel: Lastausgleich => kürzere Reaktion- bzw. Verarbeitungszeiten.

Ressourcenverbund: Zugriff auf die im Verbund verfügbaren Betriebsmittel (Ressourcen), u.a. Programme, Daten, Speicher, Prozessoren.

Kommunikationsverbund: Trägersystem für computergestützten Informationsaustausch zwischen Mensch und Maschine. Nutzung von Telekommunikations- und Telematikdiensten (z.B. Mail, FTP, VoD).

Verfügbarkeitsverbund: Sicherung gegen Ausfall (Defekt bzw. Wartung).

Steuerungsverbund: Dezentralisierte und koordinierte Steuerung von Prozessen (PPS, ...).

Kommunikationskanal

Verbindendes Element zwischen den Kommunikationspartnern:

Drahtgebunden
- metallische Leiter: Kupferkabel (z.B. Telefon-Leitung, ISDN, xDSL)
- Koaxialkabel (z.B. TV-Kabel)
- Optische Leiter (Lichtwellenleiter): Glasfaserkabel

Drahtlos -> Funkübertragung (elektromagnetische Wellen), u.a.
- terrestrisch (Zellularfunk, Bündelfunk), Nahbereich (WLAN, Infrarot, Bluetooth, RFID)
- Satellitenübertragung, u.a. ARPAnet/Internet (USA-Hawaií), USA-Europa, Europa, GPS.

Wichtige Maße des Kommunikationskanals:
- Kanalkapazität: Übertragungseinheiten je Zeiteinheit (z.B. bit/s)
- Bandbreite: Festlegung der Signalfrequenzen für die Informationsübertragung (kHz)

Kommunikationseinrichtungen
- öffentlich (public): Telefonnetze, Datennetze; genormte Schnittstellen (z.B. V-/X-Serien der CCITT) bzw. Internet TCP/IP; Paket- oder Leitungsvermittelt.
- privat (eigene Leitungen, u.a. Energienetz, Bahnnetz; Inhouse-Netze)

1.2.2 Trends in Rechner- und Datenkommunikation

Bereitstellung einer Kommunikationsinfrastruktur (kabelgebunden und kabellos)

Telefon- und Datennetze (Kupferkabel -> max. 50 Mbit/s)

Telefon (28.8 kbit/s) Analog -Technik
ISDN (64 kbit/s) Digital - Technik
[Datex-L,] Datex-P (48 kbit/s, X.25-Protokoll -> IP) Digital - Technik
xDSL (z.B. Access NW ADSL: downstream 8 Mbit/s, uplink 768 kbit/s; T-DSL: 25 Mbit/s

Hochgeschwindigkeitsnetze (Datennetze, Backbones; Glasfaserkabel -> n Tbit/s)

B-ISDN/ATM - Technologie: (2...34) .... 155 .... 622 .... 2 488 Mbit/s, z.B.
DFN: 34/155 Mbit/s: B-WiN-Backbone (Basis: ATM, Förderung DFN e.V. u. BMBF)

TEN-34/155: 34/155 Mbit/s (Europäischer Multiprotokoll-Backbone: X.25 / IP)
SDH/WDM - Technologie: (622 Mbit/s) ... 2.5 ... 10.5 ... 16*2.5 Gbit/s ... n Tbit/s
Basis: Optische Netze; Protokolle SDH/WDM, DWDM; Dienste: IP [, ATM]), z.B.
G-WiN: 622 Mbit/s ... 2.5 ... 10.5_{2004} Gbit/s (UL: 622 Mbit/s), dark fiber
X-WiN, GÉANT2: 10 Gbit/s ... 100 $Gbit/s_{2012}$
ANSnet (NSFnet): 90 Mbit/s ... 140 Mbit/s ... 10 Gbit/s
vBNS (USA, Internet 2): 622 Mbit/s, Abilene / NGnet: 2.5 / 10 Gbit/s

Lokale Netze (LAN) - Koaxialkabel
Ethernet (10 Mbit/s), Token-Ring (10....16 Mbit/s)

High-Speed-LAN (Koaxialkabel bzw. Glasfaser)

FDDI	100 Mbit/s
DQDB	2 * 150 Mbit/s (DATEX-M)
Fast-Ethernet	100 Mbit/s
Gigabit-Ethernet	1_{1998} / 10_{2001} / 40_{2003} / 100_{2010} Gbit/s ("100GET"-Netz)

Zugangsnetze (Access Networks) - Kupferkabel bzw. Glasfaser
ADSL (8 Mbit/s), SDSL (2 Mbit/s), VPON (50 Mbit/s), PON.

Mobilkommunikation (drahtlos, elektromagnetische Welle: Funk bzw. Infrarot)
Zellularfunk: GSM (D1/2), DCS (E1/2): 9.6 kbit/s; GPRS: 60 ... 115 kbit/s
UMTS: 384 kbit/s, HSDPA: 7,2 Mbit/s; LTE: 100 Mbit/s ... 1 Gbit/s
Bündelfunk, Mobile IP, W-ATM (Mobile Broadband System), Wimax (50 Mbit/s)
WLAN (54/108 Mbit/s), Nahbereichsfunk (IR, Bluetooth), Sensornetze
Satellitenfunk

Innovation *Glasfasertechnik* (LWL, neue Lasertechnik – Nobelpreis Kao_{2009}):
Leitungsgebundene Kommunikation (Festnetze): 100 Mbit/s ... 400 Gbit/s ... n Tbit/s.
Optische Übertragungstechnik (Modulation der Signale zur DÜ auf einer Wellenlänge):
DWDM-Technik (Dense Wavelength Division Multiplexing), dark fibre.
Weitverkehrsnetze (long haul): bisher 10 Gbit/s pro Wellenlänge (am wirtschaftlichsten).
Bündelung bis zu 160 opt. DÜ-Kanäle (X-WiN, GÈANT) -> mehrere Terabit/s pro Glasfaserpaar.
In Entwicklung: 100 Gbit/s auf einer einzelnen Wellenlänge.
Zunahme nichtlinearer Effekte -> Ü-Störungen. Router, freie Kanäle in existierenden Glasfasern. Testbeds (2010):
Verbindung NREN $X\text{-}WiN_{de}$ – $RENATER_{fr}$ (im X-WiN generell nicht vor 2012)
Verbindung Uni-RZ TU Dresden – TU Bergakademie Freiberg
Lokale Netze: Gigabit-Ethernet (1 / 10 / 40 / 100 Gbit/s ("100GET")).
Standardisierung: IEEE 802.3ba 2010: für ein Optical Transport Network (OTN)
40 / 100 Gbit/s, Entfernung: wenige Meter ... 10 (40) km.

Globalisierung

Vernetzung aller Bereiche

- Hochgeschwindigkeitsnetze, Backbone, Trend Gigabitnetze (SDH/WDM vs. ATM)
  High-Speed-Internet (Next Generation Internet)
- Optische („photonische") Netze (LWL, WDM, Lichtfarben; dark fiber)
- Einbezug LAN und Mobilkommunikation (ubiquitous: Smartphone und Tablet PC)
- Web 2.0, Cloud-Computing

=> Aufbau einer Datenautobahn (Information Super Highway) ~> >= 100 Gbit/s.
Vision Al Gore (ehem. US-Vizepräsident): Global Information Infrastructure (GII)
Verbindung von WAN, LAN, Kabelfernsehen und weiteren Netzwerken und Satellit

Übertragung von Text, Sprache, Bild

Multimedia, Videokonferenz, Virtual Reality, ...

Digitalisierung analoger Signale
Telefon: PSTN -> ISDN; B-ISDN; analoge -> digitale MFN (GSM);
Internet-Telefonie (VoIP).

Anwendungen und Technologien
- Verteilte Systeme und Anwendungen
  - Verteilungsplattformen (DCE, CORBA, RMI, DCOM, .Net, EJB, ..., SOA)
  - Anwendungen, u.a. (gekoppelt mit Internet/WWW ~> Web Services)
    Client/Server-Systeme, WfMS-Systeme, e-Commerce, CSCW, Teleworking
    Peer-to-Peer (P2P): Musiktauschbörse (wie Gnutella, Napster), File-Sharing
  - Standardisierung: ODP, TINA -C; OSF, OMG, Microsoft, W_3C
- Neue Kommunikationstechnologien / -dienste (u.a. ad-hoc-Netze, ubiquitous computing)
- Internet und WWW (CGI/PHP, Perl, XML, AJAX, HTML5) => Internet-Technologien.
  Anwendungen: Web 2.0: RSS-Feeds, Facebook, Twitter ...; Cloud-Computing.
- Visualisierungen => Virtual Reality (VRML, Web3D), Audio/Video-Conferences
  Hochleistungsrechnen/Übertragen => Grid-Computing
- Objektorientierung: CORBA, Java --> Komponentenarchitektur: EJB, DCOM, CCM
- Einsatz neuer Medien in Aus- / Weiterbildung (Distance Learning, Teleteaching)
- Embedded Systems: z.B. intelligente Lichtschalter, Verkehrstelematik

1.3 Netzwerkstrukturen

1.3.1 Strukturen von Rechnernetzen

Allgemeiner Aufbau eines Rechnernetzes

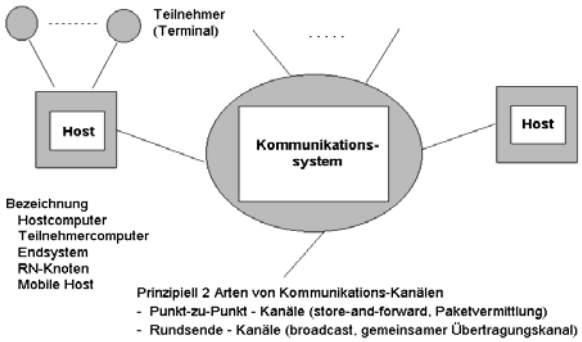


Abbildung 1.3: Verallgemeinerter Aufbau eines Rechnernetzes

Daraus leiten sich allgemein folgende Arten von Rechnernetzen ab:
- WAN („long haul“, flächendeckend, paketvermittelt), Backbone, Internet
- LAN, MAN, HS-LAN (lokal, shared media)
- wired / wireless (Festnetz, Mobilfunk)
- Infrastrukturnetze / Ad-hoc-Netze
- Photonische Netze (SDH/WDM), Kernnetze (u.a. ATM, Internet), Zugangsnetze (xDSL)

Strukturen von Rechnernetzen
Logische Struktur:
Beschreibung der Funktionsweise eines Rechnernetzes und der Realisierung der Steuerung (Architektur eines Rechnernetzes).
Fundamentales Architekturprinzip von Rechnernetzen: Hierarchische Mehrschichtenstruktur. Menge logischer Schichten, die auf gleicher Ebene Protokolle austauschen und über Dienste die Kommunikations-Funktionen der nächst niedrigen Schicht in Anspruch nehmen (Dienstnutzer, Diensterbringer). Standard-Referenzmodelle, u.a.

ISO/OSI (ISO 7498), DoD (Internet, TCP/IP), B-ISDN (SDH, ATM).

Topologische Struktur

Zuordnung der Teilnehmer-Computer zu den Kommunikationskanälen. Aufgabe der Planung ~> Leitungen, Cluster, Konzentratoren. Keine Darstellung der Arbeitsweise.

Physische Struktur

Beschreibt die konkreten HW/SW-Komponenten eines Rechnernetzes. Verschiedene Rechnernetz-Arten, unterschieden nach topologischen Strukturen / Entfernung zwischen den Teilnehmer-Computern / Datenübertragungstechniken / Nutzungsformen der Übertragungskanäle. Unterteilung in (historisch bedingt, verschwindend):

- **WAN** (Wide Area Networks): Globale, flächendeckende Netze (Weitverkehrsnetze), i.allg. vermascht, Paketvermittlung, große territoriale Ausdehnung („long haul“)..
- **LAN** (Local Area Networks): Inhouse-Netze (Lokale Rechnernetze): Geringe Entfernungen (100 m ... einige km), HS-LAN / MAN im 100 km-Bereich
  (HS-LAN: High-Speed Local Area Network, MAN: Metropolitan Area Network)

Kabelgebundene Netze / kabellose Netze (Mobilkommunikation). Infrastrukturnetze / Adhoc-Netze (spontane Vernetzung).

1.3.2 Netzwerk-Topologien

Topologische Strukturen

Netztopologien können klassifiziert werden als

- **broadcast / multicast** (sog. Rundsendekanäle):
  I.allg. LAN (MAN, HS-LAN). Alle Stationen an gemeinsamen Übertragungsmedium angeschlossen, d.h. Nachricht (von 1 Station ausgesandt) kann alle anderen Stationen erreichen; Empfänger nimmt Nachricht vom Medium.
  Bei multicast: Menge von ausgewählten Stationen (z.B. WAN Overlay-NW MBone).
- **store-and-forward** (sog. Punkt-zu-Punkt-Netze):
  Nachricht / Paket im Zwischenknoten gespeichert, Weitertransport in Richtung Zielknoten. Leitweglenkung (Routing), Realisierung einer Pkt-zu-Pkt-Verbindung, i.allg. bei WAN.

Danach kann man topologische Strukturen formulieren

- *Vollständig vermaschtes Netzwerk*
  Jede Station über dedizierte Punkt-zu-Punkt-Verbindung verbunden. Verbindungsleitungen können parallel arbeiten ~> hoher Durchsatz, geringe Wartezeiten (nur wenige Zwischenknoten bis Endknoten). Einfache Kommunikations-SW, kein Routing erforderlich. Hohe Zuverlässigkeit, geringe Ausfall-Wkt. Teuer: Anzahl der Verbindungsleitungen: n (n-1)/2.

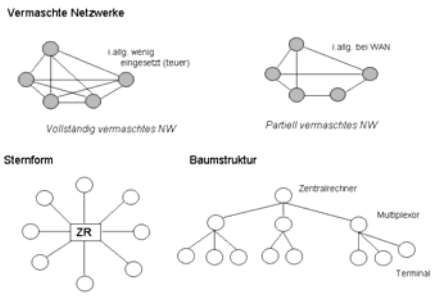


Abbildung 1.4: Netzwerk-Topologien (1)

- *Partiell vermaschtes Netzwerk*
  Punkt-zu-Punkt-Verbindung (nicht alle Stationen verbunden), i.allg. Zwischenspeicherung (store-and-forward). Kostengünstiger, aber auch anfälliger. Verbindungsleitungen können den Verkehrsanforderungen angepasst werden. Routing (Leitweglenkung) erforderlich.

- *Sternform*
  Alle Stationen mit zentralen Vermittlungsknoten verbunden. Beispiele: Sternkoppler, ATM-Switch. Einfaches Routing (Tabellen), aber schlechte Zuverlässigkeit und hohe Redundanz. Anwendung, z.B. Rechenzentren, Terminals an Zentralrechnern, ATM-Netze.
- *Baum- oder Hierarchisches Netzwerk*
  Erweiterung der Sternform, Einsatz häufig im Terminal-NW und zur Prozess-Steuerung (Leitstand-Systeme in der Automatisierungstechnik).
- *Gemeinsames Übertragungsmedium: Shared Media, Rundsende-Kanal (Broadcast)*
  i.allg. für LAN. Falls mehrere Stationen gleichzeitig übertragen wollen, ist Kontrollmechanismus für Zugriff auf Medium erforderlich (Medienzugriffsverfahren).
  - Serieller Bus (Sammelleitung, "Highway"): Verbindung: Broadcast, paarweise erdrillte Leitungen, Koaxialkabel oder LWL. Gesamtzusammenbruch bei Busausfall. Bidirektionale Verbindung.
  - Ring (Schleife): unidirektionale Verbindung: Verbindung: i.d.R. Punkt-zu-Punkt (ggf. Broadcast). Kupferkabel, LWL. Zusammenbruch bei Auftrennung des Rings (Abhilfe: doppelter Ring, wie FDDI)
- *Drahtloses Netzwerk*
  Konzept entspricht einer Sammelleitung (Highway), benutzt aber Funk- oder Satellitenübertragung (elektromagnetische Wellen) statt Kabel.

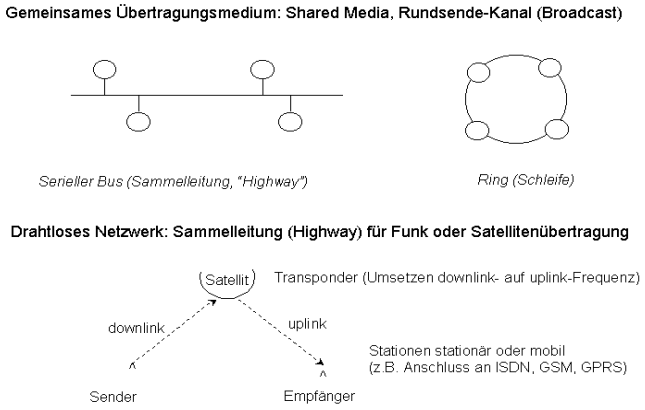


Abbildung 1.5: Netzwerk-Toplogien (2)

Mobilfunknetze: Clusterbildung (cellular networks), Raummultiplexing
- Zellularfunknetze, z.B. C / D / E - Netze, AMPS, USCD; Sprache, Daten
  Standard (ETSI): GSM (Global System for Mobile Communication)
  bzw. DCS (Digital Communication System)
  Paketfunk (Modacom, Ardis), GSM à GPRS; UMTS à HSDPA, EDGE à LTE
- Bündelfunk (TETRA), Cordless Telephony (DECT), FemToCell, MBS (W-ATM)

Arten von Kommunikations-Subnetzen

1. ***Punkt-zu-Punkt-Kanäle***
   Nachricht (Paket, Message) von Punkt zu Punkt weitergeleitet. Bezeichnung als Punkt-zu-Punkt-Netz (point-to-point), Teilstrecken-Netz (store-and-forward), Paketvermittlungs-Netz (packet switching)
   Typisch für Weitverkehrsnetze (WAN). Topologien: vermascht (voll, partiell), Stern, Baum, Ring. Wichtig:: Routing (Leitweglenkung) der Pakete auf Grund von Adressen.

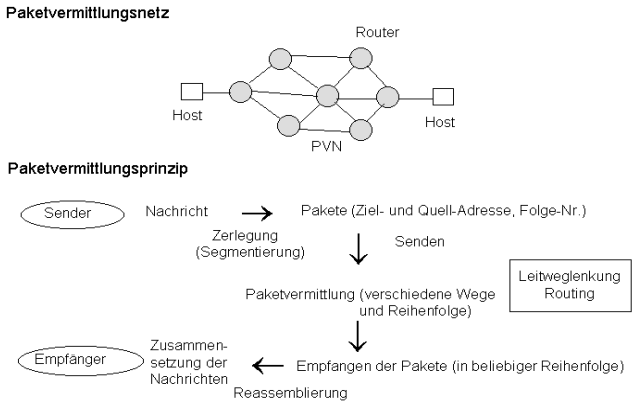


Abbildung 1.6: Prinzip der Paketvermittlung

2. ***Rundsende-Kanäle***
   Benutzung eines gemeinsamen (einzigen) Kommunikationskanals, den alle Hosts (Knoten) benutzen (Shared Media). Nachricht enthält Empfängeradresse, Empfänger nimmt Nachricht vom Kanal. Formen:
   Broadcasting (an alle Teilnehmer),
   Multicasting (an ausgewählte Teilnehmer).
   Typisch für lokale Netze (LAN) und Stadt-Netze (MAN). Topologien: Bus, Ring, Satellit.

1.3.3 Vermittlungstechniken

Vermittlung
Die Stationen können physikalisch (galvanische Kopplung) oder logisch (nicht direkt) verbunden sein. Das Netz muss die Daten zwischen den Endpunkten vermitteln, um einen sog. Ende-zu-Ende-Pfad (ISO: ”Relay”) zwischen den Stationen bereitzustellen.
Wichtigste Vermittlungstechniken:
Leitungsvermittlung (circuit switching)
Leitungsvermittlung errichtet einen dedizierten Kanal oder Leitung zwischen 2 Stationen (analog klassisches Telefonnetz, POTS). Bei Mobilfunknetze: „kanal“vermittelt.
Vermittlung nur bei Aufbau der Verbindung, dann kann Datenübertragung erfolgen (feste Verbindung). Hohe Datenübertragungs-Raten, aber uneffektive Leitungsausnützung (keine Sharing mit anderen Teilnehmern). Kosten pro Verbindungsdauer ermittelt.
Paketvermittlung (packet switching)
Nachrichten werden in Fragmente (Pakete, Zellen) segmentiert, versehen mit Zieladresse. Pakete werden entsprechend der Adressinformation durch Netz vermittelt. Somit Multiplexe Nutzung der Leitungen, bessere Ausnutzung (insbesondere bei teueren Leitungen und hoher Last). Falls Empfänger nicht erreichbar, werden Nachrichten im Netz gespeichert. Bei Empfänger werden Nachrichten wieder zusammengesetzt (Reassemblierung). Routing (Leitweglenkung) erforderlich. Langsamere Übertragung (Aufbau - Übertragung - Abbau einer Verbindung). Kosten pro Paket (nicht nach Verbindungsdauer, „allways online“) berechnet.
Nachrichtenvermittlung (message switching)
Im Prinzip eine Paketvermittlung für lange Nachrichten (store-and-forward). Diese in Hintergrundspeichern von Vermittlungsknoten zwischengespeichert, bis der Zielrechner die Nachricht abfordert. Typische Anwendung: E-Mail (Electronic Mail).

1.4 Typen von Rechnernetzen

Daten- und Rechnernetze
- Telefonnetze (analog (PSTN), digital (ISDN))
- Datennetze (Paketvermittlungsnetze (PVN): X.25, Frame Relay, IP; B-ISDN/ATM)
- Rechnernetze (WAN (z.B. Internet), LAN, MAN), Access Networks (z.B. xDSL)
- Mobilfunknetze (flächendeckend, lokal, Nahbereich)
- Infrastrukturnetze / Ad-hoc-Netze

WAN: Wide Area Networks (long haul networks)
Flächenüberdeckend, umfassend Länder und Kontinente (Kabel, Funk/Satellit). I.allg. öffentliche Trägereinrichtungen (Träger- und Teledienste), als Basis von WAN.
I.d.R. genehmigungs- und gebührenpflichtig.
Provider und Aufgaben:
- Telekom, AT&T, British Telecom, Telenor, ...
- Bereitstellung der Kommunikationsinfrastruktur (Kabel, Vermittlungseinrichtung, ...)
- i.w. Paket- und Leitungsvermittlung (Pkt-zu-Pkt-Verbindung, store-and-forward)

Kommunikationsnetz
- Vermaschte Struktur bzw. Stern; Routing (Leitweglenkung)
- PVN, z.B. [X.25 -> DATEX-P] IP -> "Internet-PVN", GSM -> GPRS -> EDGE -> UMTS
- Trend: B-ISDN -> ATM -> Gigabitnetze (SDH/WDM, dark fiber) -> NG Internet (IPv6)

Leistungsdaten
Mehrere 1000 km; Kupferdoppelader -> Lichtwellenleiter (Photonische Netze)
Datenraten: 100 Kbit/s ... 155 Mbit/s ... 10.5 Gbit/s ... 16*10.5 Gbit/s ... Tbit/s
(K=1024) (M=1024K) (G=1024M) (T=1024G)
1999/2000: Fujitsu (1.04 Terabit/s, 10 000 km Teststrecke),
Nortel (80 Gbit/s, 640 km Teststrecke, Multiplexen 80 Kanäle à 6.4 Tbit/s)
Architektur (Protokolle):

Standard:	OSI	7 Schichten
Quasi-Standard:	DoD (TCP/IP, Internet)	4 Schichten

Bekannte WAN:

Basis X.25 (OSI):	IXI (1.paneuropäischer Backbone), S-WiN
Basis TCP/IP:	Internet, CSNET, EUnet
Unix-orientiert:	USENET
"IBM-Protokoll"-orientiert:	BITNET (EARN)
Mobilfunknetze:	Zellularfunk: GSM (D/E-Netze), GPRS, UMTS; HSDPA, LTE

Backbones (i.w. Forschungsnetz-Backbones):
NSFnet (USA), Ebone (Europa): amerikanische/europäische Internet-Backbones (IP)
NorduNET (Skandinavien): X.25, IP
DFN: WiN (X.25), B-WiN (B-ISDN/ATM), G-WiN (SDH/WDM: IP-Dienst)
IXI (X.25), EuropaNET (X.25 / IP), TEN-34/155 (ATM / IP), GÉANT (WDM): Europa
MONET (Washington D.C), METON (Stockholm)
Internet 2 (vBNS, Abilene/NGnet: SDH/WDM)

LAN (Local Area Networks, lokale Netze)
Verbindung innerhalb eines Hauses/Fabrik ("Inhouse"-Netz) und Zubringer- (Access-) NW. Entfernung 2 ... 10 km (Repeater für Leitungs-Verlängerung). Gemeinsamer Übertragungskanal, keine Bandbreitenreservierung. Hohe Bandbreiten (> 1 Mbit/s, M=1024K, aber nicht Multimedia-fähig). Einfachere Protokolle (d.h. abgerüsteter Protokollstack). Beispiele:
- Ethernet 2 ... 10 Mbit/s (Kollision)
- Fast- (100 Mbit/s), Gigabit-Ethernet (1/10/40 Gbit/s) (Switch)
- Token-Ring 2 ... 16 Mbit/s (Delay)

Private Kabelverbindungen (Kupfer, Koaxial), Rundsendekanäle (Bus, Ring)
Bekannte LAN:
Ethernet (z.B. NetWare, AppleTalk): CSMA/CD
IBM-Token-Ring, 100GET
FunkLAN (WLAN: IEEE 802.11), z.B. System WaveLAN
WPAN (Infrarot-Netze, Bluetooth), schnurlose Nebenstellenanlagen (DECT), RFID

MAN (Metropolitan Area Networks)
Spezifische, LAN-ähnliche Architekturen; Ausdehnung >= 100 km-Bereich.
Basis: Breitband-Kommunikationsmechanismen, HS-LAN (Hochgeschwindigkeits-LAN)
- FDDI 100 Mbit/s
  DQDB 2 * 150 Mbit/s
  PCI-Fast-Ethernet, VG-Any LAN: 100 Mbit/s
  Gigabit-Ethernet 1 / 10 / 40 / 100 Gbit/s ...
- B-ISDN: STM 150 Mbit/s, ATM 155 ... 622 Mbit/s ... 2488 Mbit/s
- Gigabit-Netze: 2.5 ... 10.5 Gbit/s ... 16 * 10.5 Gbit/s ... (1 ... 6.5 Tbit/s)

Übertragungs-Medium: Breitband-Kabel, Lichtwellenleiter ~> optische Netze.
Hohe Übertragungsraten: 100 Mbit/s ... 10.5 Gbit/s ... 100 Gbit/s ...

Mobilfunknetze
Mobile Computing
2 Komponenten
- Mobile (portable) Computer; u.a. Notebook, Notepad, Palmtop ~> Smartphone, Tablet PC
  leicht, tragbar, energiearm; neuartige Bedienoberflächen (Stift, Sprache)
- Mobilkommunikation (Mobilfunknetze)
  Funk (WAN, LAN, WPAN): im terrestrischen, lokalen und körpernahen Bereich
  Satellitennetze: im erdfernen Bereich (GEOS, LEOS)

Mobilfunknetze
Telefon (Sprach-) / Datenverkehr, Ubiquitous/Nomadic Computing (mobile distributed)
Verschiedene Mobilfunknetze (Zellularfunk), u.a.
- *Mobiltelefonie*: GSM- bzw. DCS-Netze (D1/2, E1/2): 2G, UMTS, EDGE: 3G, LTE: 4G
  GSM: Global System for Mobile Communications (Europe), 900 MHz
  DCS: Digital Cellular System (World), 1800 MHz
  UMTS: Universal Mobile Telecommunications Service, 2000 MHz
  LTE: Long Term Evolution
- *Daten-Paketfunk:* Modacom (DE), Ardis (USA): 1G, Bündelfunk (TETRA)
  GPRS (Nutzung GSM-Infrastruktur): 2.5G, HSDPA (Datendienst in UMTS): 3G, LTE
  GPRS: General Packet Radio Service
  HSDPA: High Speed Downlink Packet Access

Beispiel: *Zellularfunknetz*
Raummultiplex: Aufteilung in Zellen (Wiederverwendbarkeit Frequenzen, Dämpfung)

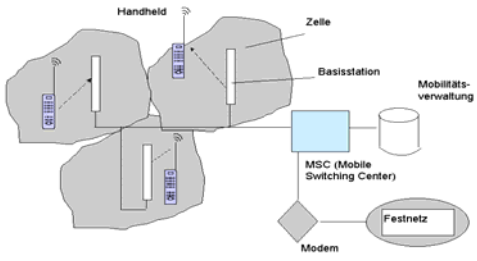


Abbildung 1.7: Aufbau Mobilfunknetz nach ETSI/GSM

Wichtige Leistungen im MFN:
- Roaming: automatisches Erkennen der aktuellen Funkzelle
- Handover: automatisches Wechseln der Funkzelle
- Mobiltätsverwaltung (MSC-DBn)

Satellitenübertragungssysteme
- GEOS (Geostationary Earth Orbit Satellits): Stationäre Position (ca. 3 Stück); Höhe: 36000 km; Inmarsat. Leistungsstarke Endgeräte, ständige Funkverbindung.
- LEOS (Low Earth Orbit Satellits): Erdumkreisend (ca. 70 Stück, als NW); Höhe: 700 - 1500 km; Erdball-überdeckend. Sprach- und Datendienste: 2 - 4 kbit/s; Iridium, Globalstar Leistungsschwache Endgeräte (Handhelds).
- GAN (Global Area Network): z.B. LEOS (Satelliten projizieren während Umlauf Funkzellen zur Erde; analog zum terrestrischen zellularen Mobilfunknetz)

Vernetzung der Satelliten bzw. mit terrestrischen Systemen. Vinton Cerf: Planung interplanetares System (Mars, ca. 2010).

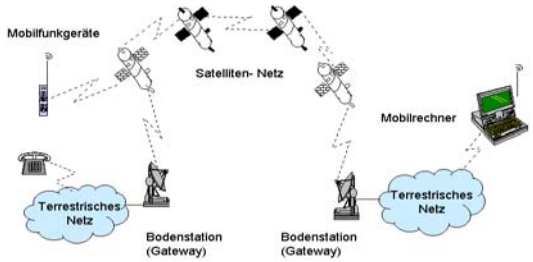


Abbildung 1.8: Satellitenübertragungssystem

Datenautobahn (Information Highway, Data Super Highway)
Schnelle landesumfassende Verbindung (digital). Verbindung Städte, ... Haushalte (auch länderübergreifend). Bereitstellung neuer Kommunikationstechnologien, Hochgeschwindigkeit (B-ISDN/ATM, SDH/WDM, dark fiber (Gbit/s)) 100GET; drahtlose Netze und neuer Kommunikationsdienste (Teledienste), u.a.
* Multimedia, Videokonferenz, Bildtelefonie, Hypermedia, Multimedia-Mail (MIME)
* Auskunfts- und Bestelldienste, Informationsdienste (Gopher ... WWW/Hypertext)
* Neue Internet-Technologien: Web 2.0 und soziale Netze (Blogs, Wiki, RSS-Feeds, Facebook, Twitter, ...), Cloud-Computing ~> siehe WebTrendMap (iA)
* Video-on-Demand (Videofilme auf Bestellung), neue Fernsehkanäle (interaktiv), Internet über Kabel / Satellit, e-Commerce (e-cash, Home-Banking, e-Bay)
* Neue Tele-Technologien, u.a.
  Teleteaching, Distance Learning; Tele-Universität, Bildungsportal/Sa.
  Telekooperation (CSCW), z.B. Telearbeit (Teleworking), Telemedizin; Grid-Computing
  Simultaneous Engineering (z.B. gemeinsame Texterstellung, CAD), Telepräsenz
  Electronic Publishing, Automatische Spracherkennung/verarbeitung/ausgabe
* Interaktives Fernsehen (500 TV-Kanäle, 3D, Mediabox, Entertainment-Technologie)

Initiativen in USA :
NII (National Information Infrastructure): Nationales Programm (4/94), Clinton / Al Gore zum Aufbau eines Information Highway
1. Schritt: Teleshopping, Video-on-Demand, Fernlernen (> 500 Fernsehkanäle). Im Anschluss: Professionelle Nutzung zur Telearbeit, Telekooperation, Simultaneous Engineering. Schwerpunkte: Teleteaching/Distance Learning (beste Lehrer für alle) und Gesundheitswesen (verbesserter Zugriff für alle)

1996: Konzentration des Programmes auf Nutzung Internet und Bereitstellung von Hochgeschwindigkeits-Backbones:
- NSFnet (ANSnet, MCI, Sprint, ...): 45 / 90 / 140 Mbit/s, 2.5 / 10 … Gbit/s, Backbone (TCP/IP).
- Entwicklung Gigabit-Netze, u.a. vBNS (622 Mbit/s), Abilene / NGnet (2.5 -> 10 Gbit/s).
- Gründung NSFnet NSF(1985, National Science Foundation, USA): Zugang zum Internet, insbes. für amerikanische Universität. NSFnet übernimmt 1989 die Funktion des ARPAnet (ARPAnet wird vom DoD aufgelöst), Weiterführung im ANSnet, NREN; kommerziell WorldCom, Sprint, MCI, ...

Initiativen in Europa
Koordinierung der europäischen Forschungs-Institutionen für schnelle Kommunikation in Europa (u.a. EU Weißbuch „Bangemann"-Bericht).
Gründung RARE (Koordinierung der Kommunikation in der Forschung)
DFN-Verein (im Auftrage des BMFT ~> BMB+F)
DANTE Ltd. (Betreibergesellschaft)
Europäische Forschungs-Backbones
IXI (Basis X.25), EuropaNET (Basis: IP und X.25), NorduNET, WiN
TEN-34/155 (Basis: ATM, IP-Dienste)
GÉANT (SDH/WDM, IP-Dienste): optische Netze, dark fiber

Initiativen in Deutschland
DFN - Verein (Berlin, 1984; im Auftrag des BMFT)

S-WiN:	ab 1990	X.25
B-WiN:	ab 1996	ATM (ATM- und IP-Dienste)
G-WiN:	ab 06/2000	SDH/WDM (IP-Dienste, optional ATM)
X-WiN:	ab 2006	dark fiber (IP-Dienst), 10.5 Gbit/s ~> 100 Gbit/s $_{2012}$

Anbindung an TEN-155, GÉANT, Ebone, US-Internets (direkter Link)

2 Netzwerkarchitekturen

2.1 Hierarchische Schichtenstruktur

Komplexität bei Rechnernetzen analog zu Betriebssystemen und Anwendungsprogrammen.
Netzwerk-Architektur: *Satz von Schichten, Protokollen und Diensten.*
Hierarchisch angeordnete Schichten: Aufteilung der Funktionen, Überschaubarkeit. Unterschiedliche Schichtenanzahl bei den verschiedenen Rechnernetzen. --> *Schichtenmodelle:*
- Logische Strukturierung, keine Implementierungsvorschrift.
- Verschiedene Referenzmodelle, u.a. OSI (ISO), Internet (TCP/IP), B-ISDN (ISO), GSM, UMTS (ETSI), WAP/WAE (1998, WAP-Forum), Bluetooth (Ericsson).

Schichtenmodell
Logische Struktur für die Kommunikation zwischen zwei entfernten Partnern A und B.
Begriffe:
- Instanz, Entity: Aktive HW- oder SW-Komponente, Kommunikationspartner: Host A, B
- Protokolle: Logische Verbindung zum Austausch von Nachrichten (horizontale Verbindung, je Schicht). Festlegung zu Formate, Codes, Ablauf, Fehlerbehandlung, ...
- Dienste (Dienstprimitive): Realisierung der Protokolle durch die Dienste der darunter liegenden Schicht (vertikale Verbindung, je Kommunikationspartner)
- Dienstzugriffspunkte: Schnittstelle zur Dienstbereitstellung (SAP: Service Access Point).

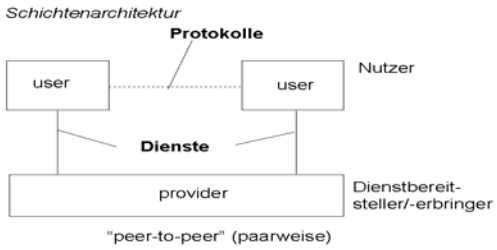


Abbildung 2.1: Service-Convention-Modell

Nachrichtenkopf (Header)
Zur Identifikation der Nachricht fügt Schicht N an die aus Schicht N+1 erhaltene Nachricht einen Nachrichtenkopf (Header) an. Dieser enthält Steuerinformationen, u.a. laufende Nr., Adressen, ggf. Größe, Zeiten. Die Nachricht (Header + Information) wird an die darunter folgende Schicht übergeben, die wiederum ihren Header anfügt. Am Zielknoten werden schichtenweise in umgekehrter Folge die Header wieder entfernt.

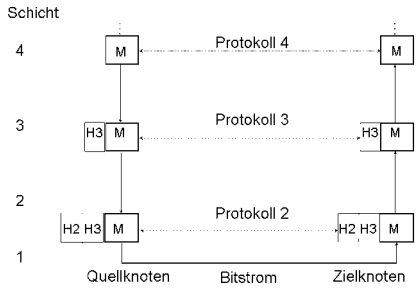


Abbildung 2.2: Verwaltung Nachrichtenkopf (Header)

Netzwerkarchitektur (Satz von Schichten, Protokollen und Diensten)
Protokoll (horizontale Verbindung):
Satz von Regeln (semantisch und syntaktisch) zum Informationsaustausch zwischen zwei Kommunikationspartnern, u.a. Nachrichtenformat, Code, Algorithmen bei normaler und gestörter Übertragung ... I.d.R. eine logische Verbindung (lediglich unterste Schicht liefert einen physikalischen Pfad zwischen Sender und Empfänger).
Schicht:
Paarweise Kommunikation zwischen Instanzen (Peer-Entities) einer Schicht (peer-to-peer-Verbindung). Zuordnung bestimmter Funktionen im Kommunikationsvorgang. Hierarchische Schichten-Referenzmodelle (OSI, TCP/IP).
Dienst (vertikale Verbindung):
Realisierung der Funktionen. durch Dienste der darunter liegenden Schicht (Dienstprimitive). Dienstbereitstellung an sog. Dienstzugriffspunkten *(Service Access Point, SAP).*

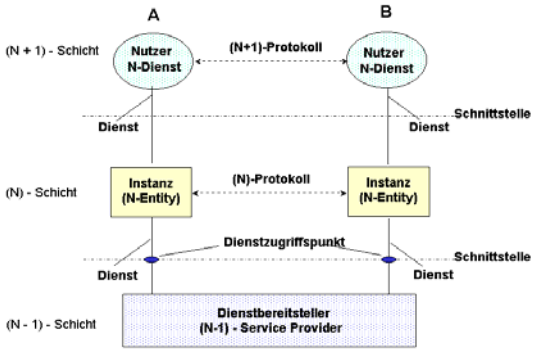


Abbildung 2.3: Allgemeines Dienstmodell (Protokolle, Primitive)

2.2 Schnittstellen und Dienste

Dienstarten

Je Schicht können 2 verschiedene Dienstarten angeboten werden:

Verbindungsorientierter Dienst (connection-oriented service, CO)

3 Phasen:Verbindungsaufbau, Datentransfer, Verbindungsabbau.
Gesicherter Übertragungsdienst (Reihenfolgetreue der Dateneinheiten).

Verbindungsloser Dienst (connectionless service, CL)

Jede Nachricht erhält vollständige Adresse und Folge-Nr. Nur Datentransferphase.
Unsicherer, aber schneller Dienst (keine Reihenfolgetreue). Speziell:
Datagram-Dienst: unzuverlässiger, nicht quittierter Dienst (Analogie: Telegramme)
Betätigter Datagram-Dienst: mit Quittierung (Analogie: eingeschriebene Post)
Anfrage/Antwort-Dienst: senden 1 Datagram, mit Antwort (Analogie: DB-Abfrage)

Funktionalität

Funktionen, die in allen Schichten auftreten können:

Verbindungsaufbau / abbau
Adressierung
Übertragungsrichtung (Simplex- / Halbduplex- / Vollduplex-Übertragung)
Fehlerbehandlung (Erkennung / Behebung)
Fluss-Steuerung (Geschwindigkeitsausgleich): Flow Control
Überlaststeuerung (Überlaufbehandlung: Pufferung, Ratenkontrolle): Congestion Control
Multiplexing / Demultiplexing (Parallelität)

Ausgetauschte Nachrichten

Schicht (Bezug OSI)		Instanz
7 ... 5	Anwendungsschichten	Nachricht (A-, P-, S-PDU)
4	Transportschicht	TPDU (Transport-PDU, OSI), Segment (TCP)
3	Vermittlungsschicht	Paket, Datagram (bei verbindungslos)
2	Sicherungsschicht	Rahmen (Frame)
1	Bitübertragungsschicht	Bitstrom

Dienstprimitive

4 Klassen (angeboten je Protokolloperation und Schicht):

Anfrage (request)	Instanz fordert Dienst an, um bestimmte Aufgabe auszuführen
Anzeige (indication)	Instanz wird über ein Ereignis informiert
Antwort (response)	Instanz antwortet auf das Ereignis
Bestätigung (confirm)	Bestätigung auf vorherige Dienstanforderung

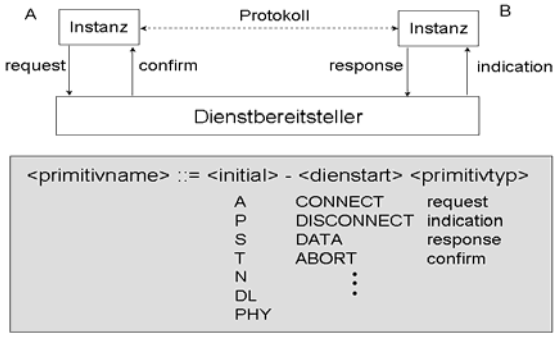


Abbildung 2.4: Spezifiktion der Dienstprimitive

Beispiel eines verbindungsorientierten Dienstes (CO):
(CONNECT: bestätigter Dienst, DISCONNECT: unbestätigter Dienst)

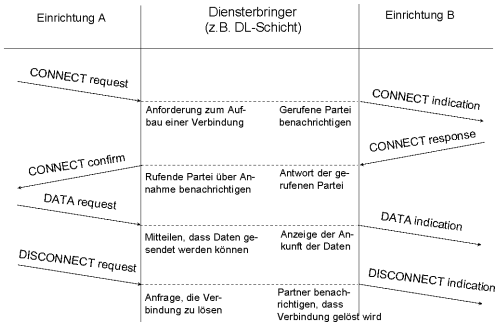


Abbildung 2.5: Weg-Zeit-Diagramm für CO-Dienst

Referenzmodelle für Telekommunikation (Rechnernetze)
Standardisiert, international (ISO)
OSI-Referenzmodell (Open System Interconnection)
B-ISDN (Broadband-ISDN)
Weltweit, ISO/IETF (nicht ISO)
DoD-Referenzmodell (TCP/IP, Internet)
Industrie-Standards
SNA / IBM (System Network Architecture)
[DNA / DEC (Digital Network Architecture)]
NetWare (Novell, LAN / Ethernet)

Referenzmodelle für Verteilte (Verarbeitungs-) Systeme
Standardisiert (ISO)
ODP-Referenzmodell (Open Distributed Processing)
Internationale Konsortien
OSF (Open Software Foundation) --> DCE
OMG (Open Management Group) --> CORBA
Industrie-Standards
ANSA, TINA-C, DCOM (Microsoft), EJB (Sun, Java), Web (W3C, WHATWG) ...

2.3 OSI-Referenzmodell

2.3.1 Basis-Referenzmodell

OSI Basis Reference Model (ISO / IS 7498)
OSI: Open System Interconnection. Mehrschichtenarchitektur. Standardisierung (ISO) für offene Systeme. Abstraktes logisch-funktionelles Architekturmodell für RN. Internationaler Standard (IS 7498).
7-Schichten-Architektur
Mehrschichtenarchitektur offener Systeme (offen: Nutzung, Zugänglichkeit, Weiterentwicklung). Festlegung der allgemeinen Kommunikations- und Kooperationsbeziehungen.
Je Schicht definierte Funktionen (international genormte Protokolle, z.B. ITU-TS: T-, V-, X-Serien, ...), keine Implementierungsvorschriften. Dokumentation: Day / Zimmermann (1983).

7 - Schichten - Architektur

7: Application Layer (Anwendungsschicht)	
6: Presentation Layer (Darstellungsschicht)	Anwendungssystem
5: Session Layer (Sitzungsschicht)	
4: Transport Layer (Transportschicht)	Transportsystem
3: Network Layer (Netzwerk- / Vermittlungsschicht)	

2: Data Link Layer (Verbindungs- / Sicherungsschicht)
bei LAN: Subschichten 2a: LLC (Logical Link Layer) Übertragungssystem
2b: MAC (Medium Access Layer)
1: Physical Layer (Physikalische / Bitübertragungsschicht)
0: Physikalisches Übertragungsmedium (nicht Bestandteil OSI-Modell)

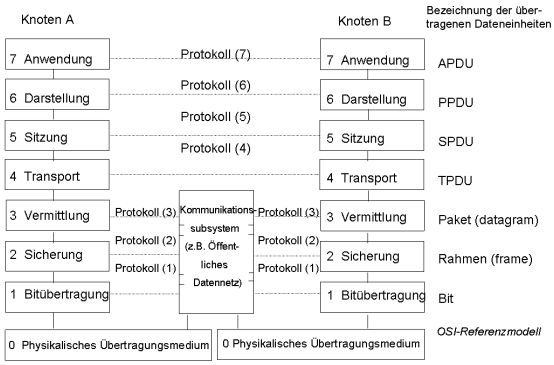


Abbildung 2.6: OSI-Referenzmodell (Schichten)

Dienstmodell
(N) - Einrichtung (peer entity)
Informationsaustausch über Kommunikationsprotokolle (ITU-TS), u.a. Regeln zum Austausch der PDU, Übertragungssteuerung (PCI), Quittierung, Fensterbreite, Code, ...
Realisierung der Kommunikation über Dienste der nächst niedrigeren Schicht Dienstprimitive
Informationsaustausch zwischen Dienstbenutzer- und bereitsteller

REQUEST:	Anforderung eines Kommunikationsdienstes
INDICATION:	Anzeige einer Kommunikationsanforderung
RESPONSE:	Reaktion Kommunikationspartner auf Kommunikationsanforderung
CONFIRM:	Bestätigung der Kommunikationsanforderung

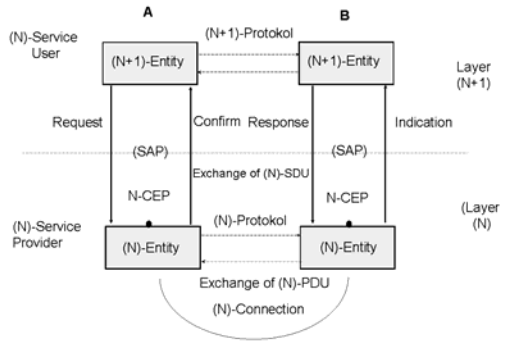


Abbildung 2.7: OSI-Referenzmodell (Dienstprimitive)

(N) - Verbindung (N-connection)
Logischer Pfad zwischen Sender/Empfänger für Zeit des Nachrichtenaustausches
(verbindungsorientierter bzw. verbindungsloser (N) - Dienst)
Verbindungsdienst (Kommunikationsablauf, Phasen)
- Verbindungsorienter Dienst:
  Zuverlässiger Übertragungsdienst
  3 Phasen: Verbindungs-Aufbau (establishment), Übertragung (transfer), Abbau (release)
  Übertragene Informationen:
  horizontal: PDU Protokolldateneinheit (Header + SDU)
  vertikal: IDU Schnittstellendateneinheit (ICI + SDU)
  ICI (Interface Control Information),
  SDU (Service Data Unit, Dienstdateneinheit)

- Verbindungsloser Dienst:
  Unzuverlässiger Übertragungsdienst; nur Transfer-Phase
  Keine feste Sender/Empfänger-Verbindung
  Informationseinheiten enthalten vollständige Zieladresse

2.3.2 Funktionen der Schichten im OSI-Modell

Bitübertragungsschicht

Aufgaben

Physische Übertragung von **Bits** über einen Kommunikationskanal (Bitstrom). Bereitstellung der mechanischen, elektrischen und funktionellen, prozeduralen Hilfsmittel zum Aufbau, Betrieb und Abbau der physischen Verbindung. Bitstromübertragung erfolgt in der Reihenfolge der eintreffenden Bits, ohne Einschränkung hinsichtlich Codes und inhaltliche Bedeutung. Physisches Medium (drahtgebunden, drahtlos; "Schicht 0") gehört nicht zum OSI-RM.

Typische Probleme der PHY-Schicht

Sicherung der Bits (was als 1 weggeht, muss auch als 1 ankommen). Dauer der Bitübertragung. Übertragungsrichtung; lt. CCITT: Simplex: nur in 1 Richtung, Duplex: gleichzeitig in beide Richtungen. Steckerkompatibilität: Pin-Anzahl, Belegung der Endsysteme, ...
In den höheren Schichten werden die Bits zu Informationseinheiten (Frame, Paket, Nachricht) zusammengefasst.

Bekannte Protokolle: V.24, X.21 (CCITT)

Sicherungsschicht

Charakterisitik

Zusammenfassung der von Bitübertragungsschicht übertragenen Bitströme zu Datenreihen (**Frames**, Rahmen) und Weitergabe (falls fehlerfrei) an die Vermittlungsschicht. Sender teilt die Eingangsdaten in einen Datenübertragungsrahmen ein, z.B. einige 100 Bytes, und überträgt diese sequentiell. Analog ist der vom Empfänger erzeugte Quittungsrahmen zu verarbeiten

Aufgaben der Sicherungsschicht

Aktivieren / Deaktivieren von Verbindungen.
Erkennung/-behebung von Übertragungsfehlern (z.B. Anzeige des Fehlers an Vermittlungsschicht). Steuerung von beschädigten, verloren gegangenen bzw. duplizierten Rahmen.
Steuerung des Datenstroms (asynchrone / synchrone Übertragung, Rahmenerkennung).
Sicherung / Angleichung bei ungleichen Sende / Empfänger-Leistungen (Flusssteuerung, z.B. Bereitstellung entsprechender Pufferbereiche).
Steuerung bei Übertragung in beiden Richtungen (z.B. für Quittungen) --> dazu spezielle Verfahren, u.a. Huckepackverschickung (piggy packing).

Bekannte Protokolle

HDLC: High Level Data Link Control (Teil der X.25-Empfehlung, ISO-Standard)
SLIP: Serial Link Internet Protocol
PPP: Point-to-Point-Protocol (IETF/Internet, Wählverbindung)
ATM, TC-Teilschicht (Transmission Convergence)

Problem bei Broadcast-Netzen: Mehrfachzugriffsprotokolle wegen gemeinsamen Übertragungsmediums (*Shared Media*), insbes. bei LAN ~> Unterteilung in 2 Subschichten:

MAC (Medium Access Control): benachbart zur PHY-Schicht, verschiedene Medienzugriffsverfahren (z.B. Ethernet, Token-Ring).

LLC (Logical Link Control): benachbart zur Vermittlungsschicht, restliche Funktionen der Sicherungsschicht, insbes. Anpassung an Vermittlungsschicht

MAC (Medium Access Control, Subschicht 2a)

Kanalzuordnung: statisch (z.B. Telefon, Frequenzmultiplex)
dynamisch --> LAN, MAN

Mehrfachzugriffsprotokolle, u.a.

WAN Mobilfunknetze (-> Raummultiplex, zusammen mit FDM, TDM bzw. CDM):
Digitaler Zellularfunk (GSM, GPRS, CPDP, USCD, IS-95-CDMA)

LAN ALOHA, CSMA/CD (Ethernet) Token-Ring / Bus
Drahtlose LAN (wireless LAN): MACA / MACAW

HS-LAN FDDI (Fibre Distributed Digital Interface)
DQDB (Distributed Queueing Dual Bus)
HIPPI (High Performance Parallel Interface), Nachfolger Fibre Channel
Fast/Gigabit-Ethernet

Satellitennetze, z.B. ACTS (Advance Communication Technology Satellite)
SDM (Raummultiplexing, z.B. bei LEOS)
FDM (Frequenzmultiplexing)
TDM (Zeitmultiplexing)
CDMA (Code Division Multiple Access)

Vermittlungsschicht

Aufgaben

Realisierung Datentransport über mögliche Zwischenknoten.
Paket-Leitweglenkung (**Routing**) von Quelle zu Ziel: statisch: über Tabellen (nur selten geändert), dynamisch: vor jeder Sitzung neu geänderte Tabellen, adaptive Anpassung.
Steuerung eines möglichen Paketstaus (Fluss-Steuerung).
Abrechnungs-Funktion für Paketübertragung (insbes. Länder überschreitender Verkehr).
Identifikation der Knoten (Netzwerk-Adresse).
Internetworking zwischen verschiedenen Subnetzen (Netze unterschiedlicher Dienstgüte).
Bereitstellung eines einheitlichen Netzdienstes an der Schnittstelle zur Transportstation.
Dateneinheit: **Paket** (bzw. Datagram, falls verbindungslos).
Auf- und Abbau logischer Verbindungskanäle. Unterstützung durch
Wegsteuerung (Routing, Leitweglenkung),
Fluss-Steuerung (Steuerung der Flussmenge).

Typische Protokolle (Paketvermittlungsnetze), u.a.

X.25 in öffentlichen Datennetzen (veraltet), PVN, CCITT
Frame Relay analog X.25, aber schneller (einfachere Fehlerbehebung)
IP Internet Protocol (ARPA / Internet, PVN, dominierend)
XTP eXpress Telecommunication Protocol (Gigabit-Netze)

Wichtige Anwendungen: Durchschaltevermittlung: Telefonnetz
Paketvermittlung: WAN (z.B. Internet)

Logische Verbindungen

- Leitungsdurchschaltung (Circuit Switching)
- Virtuelle Kanäle (“Virtual Circuit”, Virtual Call): Auf- und Abbau virtueller Kanäle. Store-and-Forward, Paketvermittlung, Sicherung der Paketreihenfolge.
- Datagramtechnik: Vereinfachte Form, keine eigene Verbindungsaufnahme. Keine Reihenfolgesicherung; Pakete mit vollständiger Zieladresse. Pakete über verschiedene Wege zum Empfänger.

Bei Broadcast-Netzen vereinfachtes Routing, oft nur verdünnte oder keine Schicht 3.

Transportschicht

Aufgaben

Übernahme der Daten von Schicht 3 bzw. Paketisierung der Nachrichten für Schicht 3. Realisierung eines transparenten Datentransports für die darüber liegende (Sitzungs-) Schicht, d.h. unabhängig von Kommunikationsschichten 1... 3.
Sicherung eines zuverlässigen und kosteneffizienten Datentransfers zwischen den logischen Endpunkten. Sicherung einer **End-to-End-Verbindung**, d.h. Verbindung zw. Endknoten (darunterliegende Protokolle realisieren Protokolle zwischen ihren unmittelbaren Nachbarn). Dabei optimale Nutzung vorhandener Kommunikationsressourcen
5 Standard-Transportdienstklassen in ISO/OSI (TS0 ... TS4, z.B. ISO 8072, 8073)

* Berücksichtigen Art des Informationsverkehrs, z.B. Dialog-, Stapel- oder Echtzeitbetrieb
* Charakterisiert werden diese Dienstklassen durch Parameterwerte für u.a. Durchsatz, Zulässige Transportverzögerungszeit, Verbindungsaufbauzeit, Restfehler-Wkt.

Höchste übertragungsorientierte Schicht des Transportsystems.

Funktionen

Multiplexing von End-to-End-Transportverbindungen in Netzen (Mehrfachnutzung eines Kanals, mehrere Verbindungen zw. den Hosts).
Auf- und Abbau von Netzverbindungen.
Adressenzuordnung (Mapping).
End-to-End-Reihenfolgesteuerung der zu übermittelnden Daten.
Segmentierung und Blockung der Daten (Dekomposition / Aggregation).
End-to-End-Flußsteuerung auf den Verbindungen.
Flussregulierung zwischen Hosts unterschiedlicher Geschwindigkeiten.

Bekannte Protokolle

TCP Transmission Control Protocol (verbindungsorientiert)
UDP User Datagram Protocol (verbindungslos)
mit Socket-Programmierschnittstelle (IP-Adresse, Port-Nr.)
OSI, Transportklassen 0 ... 4 (verbindungsorientiert ... verbindungslos)

Sitzungsschicht

Aufgaben

Realisierung einer Sitzung, d.h. einer Kooperation von Anwendungsprozessen (auf homogenen bzw. heterogenen Systemen). Realisierung Datentransport (wie Transportschicht), mit zusätzlichen Diensten, u.a.

- *Dialogsteuerung.*
- *Kommunikation in eine oder beideRichtungen* (Regelung der maßgeblichen Richtung).
- *Token-Management:* die Seite, die über das Token verfügt, kann eine bestimmte Operation ausführen; diese Operation könnte z.B. nicht von beiden gleichzeitig ausgeführt werden.
- *Synchronisation* bei Systemabstürzen.

Unterste Schicht des Anwendungssystems: Abwicklung, Organisation und Synchronisation des Nachrichtenaustauschs zwischen logischen Benutzern. Ermöglicht die gleichzeitige Kommunikation mehrerer logischer Benutzer.
In homogenen Systemen kann Darstellungsschicht (6) entfallen, die Sitzungsschicht sollte vorhanden sein. Bei LAN fehlen oftmals die Schichten 5, 6 (wegen der Broadcast-Funktion).

Darstellungsschicht

Aufgaben

Kommunikation zwischen Anwendungsprozessen auf heterogenen Rechnersystemen. *Einheitliche Darstellung* und *Behandlung* der strukturierten Daten mit syntaktisch verschiedenen Datentypen sowie verschiedenen Darstellungsformaten, unter Beibehaltung der Bedeutung des Inhaltes.
Syntaktische Kompatibilität wird erreicht durch

- Transformation der Datenformate einschließlich Anweisungsstruktur in eine Standardform
- Code-Konvertierung
- Handhabung mittels abstrakter Datentypen,

d.h. Konvertierung zwischen interner Darstellungsform eines Rechners in die Standard-Darstellung des Netzes. Weitere Funktionen: Datenkompression, Kryptographie wegen Vertraulichkeit und Authentizität.
Formale Beschreibungssprache: ASN.1 der ISO (Abstract Syntax Notation)

Anwendungsschicht

Aufgaben

Oberste Schicht des OSI-Referenzmodells. Stellt Dienste für die Benutzung eines RN bereit.

Wichtige Dienste der Anwendungsschicht

Identifizierung der Kommunikationspartner (über deren Namen bzw. Adresse).
Angaben der logischen Erreichbarkeit der gewünschten Kommunikationspartner.
Gewährleistung von Zugriffsrechten bzw. Schutz vor unerlaubter Systembenutzung.
Gewährleistung bestimmter Dienstqualitäten, wie Antwortzeit, Durchsatz, zulässige Fehlerrate (wenn nicht bereits auf IP-Ebene, wie RSVP, DiffServ).
Synchronisation kooperierender Applikationsprozesse.
Überwachung der zugelassenen Syntax (Zeichenmenge und Datenstruktur).
Informationstransfer.

Schicht 7 kann in 2 Subschichten unterteilt werden:
Schicht 7a: benachbart zu Schicht 6 mit Netzverwaltung und Standard-Anwendungsdienste;
Schicht 7b: Anwendungen

Netzverwaltung (Management) - gemäß OSI

Beide Teile (Applikations- und System-Management) beziehen sich auf das ganze Netz, nicht auf lokale Systemkomponenten (--> Schichten-Management)

Applikations-Management:

Steuerung und Verwaltung der OSI-Applikationsprozesse, u.a.

* Parameterinitialisierung der Applikationsprozesse
* Initialisierung, Betrieb und Beendigung von Applikationsprozessen
* Ressourcenzuweisung / -nutzung zu Applikationsprozessen
* Feststellung und Verhinderung von Ressourcen-Zugriffskonflikten
* Integritätssteuerung
* Wiederanlaufsteuerung von Applikationsprozessen

System-Management:

Steuerung und Verwaltung von Ressourcen in allen OSI-Schichten, u.a.

* Aktivierungsfunktionen (Programme, logische Verbindungen, Leitungen)
* Programmlade-Funktionen, Parameterinitialisierung
* Überwachungsfunktionen (Statusmeldung der Systemressourcen)
* Fehlerkontrolle (Fehlererkennung / -diagnose, Systemrekonfigurierung, Neustart)

Anwendungsdienste

Bereitstellung von Protokollen und Diensten zur Unterstützung der Anwendungen, u.a.

- Filetransfer: Dateiübertragung zw. verschiedenen Dateisystemen (Konvertierung der Daten, Dateiname)
- Verzeichnisdienst: Lokalisierung verteilter Ressourcen
- Virtueller Terminaldienst: Abbildung realer Terminals auf abstraktes Terminal
- Elektronische Post: Nachrichtenaustausch, MHS, E-Mail
- Remote Job Entry (entfernter Jobaufruf, Stapelbetrieb)

Angebot von Standard-Dienstleistungen (genutzt zum Aufbau oben genannter Dienste)

ISO-CASE (Common Application Service Elements): Satz von Dienstleistungen, die von Anwendungen genutzt werden können, insbes. in verteilten Anwendungen
CCITT-RTS (Reliable Transfer Service) für X.400-Empfehlung (E-Mail)

CCITT-ROS (Remote Operation Service) für X.400-Empfehlung
ISO-FTAM (File Transfer, Access and Management) für automatischen Dateitransfer
ECMA-VTP (Virtual Terminal Protocol): Terminals unterschiedlicher Hersteller als NW-Terminals
CCITT-MHS (Message Handling System): Meldungsvermittlung, z.B. Electronic Mail (X.400)
CCITT-Directory Service (X.500): Globaler Dienst zur Ortsbestimmung von Daten und Programmen
ECMA-RDA (Remote Database Access): Verteilter, entfernter Datenbankzugriff

2.4 TCP/IP-Referenzmodell

2.4.1 DoD-Basisreferenzmodell

Ausgangspunkt
ARPAnet Forschungs- und Militärnetz. Förderung durch DoD (Department of Defense)
Internet: Herauslösen Milnet aus ARPA, Ersetzen NCP durch TCP/IP, zivile Nutzung
4-schichtiges Referenzmodell (Version IPv4): Protokollpaar TCP/IP, ergänzt durch UDP und andere Protokolle.

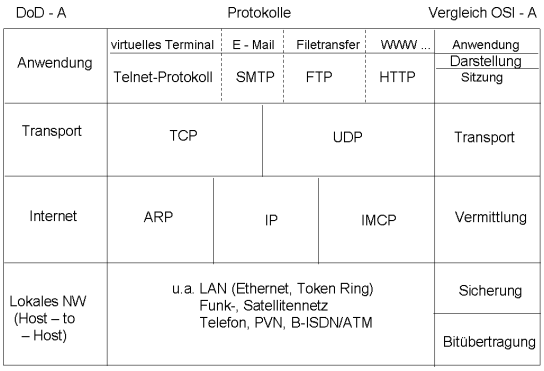


Abbildung 2.8: DoD-Referenzmodell TCP/IP (IPv4)

Zielstellungen im Internet:
Verbindung unterschiedlicher Netze (Kabel, Funk, Satellit). Sicherung gegenüber Zerstörung (insbes. militär. Bereich, Westküste) flexible Architektur. Ursprünglich: rein Daten (Texte, Daten, Bilder). Nun: Sprache, Video (Multimedia), Gruppenkommunikation, Echtzeit; all IP.

2.4.2 Funktionen der Schichten des DoD-Referenzmodells

Lokales Netzwerk (Host-to-Host-Schicht)
Hierzu keine Festlegungen. Beliebige Netze zugelassen.
Rückbezug auf OSI-Schichten 1 und 2
Internet-Schicht
Paketvermitteltes Netz auf Basis verbindungsloser Dienst (keine Reihenfolgetreue). "Sicherheitsnadel" des Internet: soll Pakete über jedes beliebige Netz befördern.
Wichtige Protokolle, u.a.
Internet Protocol (IP)
Verbindungslos, nach Prinzip "best effort". Paketformat ("Datagramme"). Routing (Leitweglenkung). Unzuverlässiger Dienst, d.h. Pakete verlustig bzw dupliziert oder in anderer Reihenfolg. Fluss-Steuerung (Vermeidung Überlast).
Adressierung: netz-id | host-id
Versionen: IPv4: 32-bit-Adresse
IPv6: 128-bit-Adresse (+ Priorität + Flow Label für QoS u. verschiedene Nachrichtenströme)
ARP: Address Resolution Protocol (Umkehrung: RARP)
Abbildung IP-Adresse <==> Ethernet-Adresse für LAN
ICMP: Internet Control Message Protocol (z.B. Ping)

Transport-Schicht
2 Protokolle zur Adressierung von Ende-zu-Ende-Prozessen: TCP, UDP (auf Basis IP)
TCP: Transmission Control Protocol
Zuverlässiger (verbindungsorientierter) Transport-Dienst über IP. Nachrichten fehlerfrei übergeben, keine Paket-Verluste / Duplikate. Fehlerkorrektur (Paket-Wiederholung, Sliding-Window-Verfahren).
Flusssteuerung (Geschwindigkeitsregulierung zwischen Sender und Empfänger).
Segmentierung der Benutzerdaten: Segmente bzw. Pakete. TCP bietet Bytestrom-Übertragung --> damit Nachrichtengrenzen nicht eingehalten. Mehrere Anwendungen gleichzeitig, keine Multicast- und Broadcast-Adressierung
UDP: User Datagram Protocol
Unzuverlässiger (verbindungsloser) Datagram-Dienst über IP, d.h. keine Reihenfolgetreue, keine Vermeidung doppelter Nachrichtenzustellung, keine Filterung. Ablauffolge und Flusskontrolle ist durch Anwendungsprozess zu realisieren.
Nachrichtengrenzen immer eingehalten (d.h. empfangene Nachricht = gesendeter). Mehrere Anwendungen gleichzeitig unterstützt, auch Multicast- u. Broadcast-Adressen.
Schnelles Protokoll, u.a. für einmalige Abfragen, Client/Server-Anwendungen, Unix.

Realisierung der Adressierung von Ende-zu-Ende-Prozessen für IP-basierte Netze:

Internet-Schicht	Transport-Schicht	Anwendungs-Schicht
IP verbindungslos	TCP verbindungsorientiert	Zuverlässigkeit, Reihenfolgetreue usw. durch TCP/IP gesichert
	UDP verbindungslos	Zuverlässigkeit, Reihenfolgetreue usw. durch UDP/IP nicht gesichert Diese Merkmale sind (falls erfordert) durch Anwendungsprozess zu sichern

Anwendungsschicht
Anwendungen und anwendungsspezifische Protokolle. Sitzungs- und Darstellungsschicht exisitieren im Internet nicht (keine Notwendigkeit; Datensicherheit in Anwendungsschicht des Internet integriert).
Basis-Dienste
Telnet (virtuelles Terminal, Remote Login): Virtuelles Terminal-Protokoll (Telnet-Protokoll)
File-Transfer: FTP (File Transfer Protokoll)
Electronic Mail: SMTP (Simple Mail Transfer Protocol), POP (Post Office Protocol)
Erweiterte Dienste, u.a.
DNS (Domain Name Service): zum Konventieren von Hostnamen in Netzadressen
MIME: Multimedia-Mail
NetNews für Diskussionsdienst: NNTP (Network User Transport Protocol)
WWW (World Wide Web) Informationssystem: HTTP (HyperText Transfer Protocol)

2.5 Beispiele (Rechnernetze, Datenübertragungsdienste)

Flächendeckende Netze (Internet: Basis TCP/IP, WAN)
ARPAnet: 1969/71 (Dienste: Telnet, FTP, E-Mail; Basis: NCP, später TCP/IP)
NSFNET: NSF: National Science Foundation
CSNET (TCP/IP) → NSFNET (1990) → ANSnet (Advanced Network and Services)
→ NREN (National Research and Educational Network, 1991): Ziel: 2.5 Gbit/s -> Tbit/s
Backbone-Networks:
USA: NSFNET, ANS, MCI-Net, Sprint, ...

Europa: EBone, WiN (DFN), TEN/GÉANT (10 -> 100 Gbit/s)
Internet: TCP/IP (IPv4, IPv6); Dienste: E-Mail, News, FTP, Remote Login, WWW
Gigabit-Netze: Aurora (MIT), G-WiN (DFN, 10 Gbit/s), X-WiN (DFN -> 100 Gbit/s,
Abilene/NGnet (Nordamerika: 2.5 / 10 -> 100 Gbit/s)
Entwicklung der wichtigsten Nutzungsformen des Internet
- Ursprünglich FTP (Fileübertragung)
- Email
- Nutzung Web 1.0 (konventionelles WWW) ~> Ablösung X.25 in Europa durch IP
- Peer-to-Peer-Übertragungen (downloads von Videos)
- Nutzung Web 2.0, insbes. Abonnementsdienste (RSS-Feeds) und Wikis, Online-Portale (Facebook, StudiVZ, Google+ ...), Nachrichtenorientierte Dienste (Twitter ...)
- Zukünftig Cloud-Computing: Speicher- und Verarbeitungsdienste im Internet, Zugriff über Web-Browser (auch mobil per Smartphone oder Tablet PC), Unterstützung durch Betriebssysteme wie MS Azure, Windows 8 udgl.

Datenübertragungsdienste
Bereitstellung durch öffentliche / private Telekommunikationsgesellschaften, u.a.
Telefonnetz: analog (PSTN, 14,4 kbit/s) bzw. digital (ISDN, 64 kbit/s)
ADSL: Asynchronous Digital Subscriber Line (über vorhandene Kupferleitungen)
downstream: bis zu 8 Mbit/s, upstream: bis zu 800 kbit/s
Erweiterungen: T-DSL (bis 25 Mbit/s), SDSL (2 Mbit/s), VDSL (bis 50 Mbit/s, Glasfaser
DQDB (Telekom: Datex-M): HS-LAN, 2 * 150 Mbit/s
Gigabit-Ethernet: 1 / 10 / 40 /100 Gbit/s ("100GET") -> Standard für HS-LAN
SMDS: Switched Multimegabit Data Service
für Zusammenschluss mehrerer LAN's; Entwicklung durch Bellcore (Anfg. 80er)
erster leitungsvermittelter Breitbandübertragungsdienst (45 / 90 Mbit/s)
SMDS-Basisanschluss: verbindungsloser Paketdienst
Basis für Multicast-Backbones in DE (z.B. Mbone)
X.25-Netze: älterer, verbindungsorientierter Paketdienst
sowohl Paketvermittlung als auch virtuelle permanente Leitungen
Protokolle: X.21, HDLC, PAD ("Triple X": X.3 / X.28 / X.29)
geringere Datenübertragungsraten: 48 kbit/s
~> Ablösung durch verbindungslosen Paketdienst auf Basis IP
Frame Relay: analog X.25, aber ohne aufwendige Fehlersicherung --> DÜ i.allg. 1.5 Mbit/s
B-ISDN / ATM bzw. Photonische Netze
SDH, ATM, WDM, ..., Echtzeit, Dienstgüte, Reservierungen, DÜ >= 155 Mbit/s
B-ISDN / ATM (SDH, ATM)
Echtzeit, Dienstgüte, Reservierungen, DÜ: (34) 155 Mbit/s ... 2,5 Gbit/s.
Netze: Forschungs-Backbones B-WiN (DFN), TEN34/155 (Danté Ltd.)
Optische Netze (SDH / WDM, DWDM, ...)
Glasfasernetze, Basis IP (TCP/UDP); oft dark fiber. DÜ: 2.5/10/100 Gbit/s ... Tbit/s
Netze (NREN): X-WiN, Renater, GÉANT, US-Internets

3 Bitübertragungsschicht (Physical Layer)

3.1 Aspekte der Datenübertragung

Bitübertragungsschicht
ISO/OSI-Modell: Schicht 1 (Physikalische Schicht)

Abbildung 3.1: Schichtenmodell (OSI, Schicht 1)

Problemstellungen
- Datenübertragung (Bitstrom)
- Übertragungsmedien:
  drahtgebunden: Kupferkabel, Koaxialkabel, Glasfaserkabel (Lichtwellenleiter)
  drahtlos: Funkwellen, Mikrowellen, Infrarot, Lichtwellen (Laser)
- Datenübertragungsnetze (Auswahl):
  Telefonnetz (Sprachübertragung bzw. Zugangsnetz, analog / digital), u.a.
  POTS, PSTN, ISDN, xDSL
  Datennetze (digital, kabelgebunden), u.a. PDH, SONET, SDH, WDM, DWDM
  Datennetze (digital, kabelgebunden):
  PDH, SONET, SDH (SDH/WDM, DWDM)
  Kabellose Netze (Sprach- und Datenübertragung, seit 90er digital):
  Mobilfunknetze (Telefon, Datenpaketfunk, zellulär), Bündelfunk, Satellitennetze
  Wireless LAN (W-LAN), W-ATM, HomeRF, FemToCell
  WPAN (Infrarot, Bluetooth), RFID, NFC

Datenübertragungstechnologie
- Übertragungseinheit: **bit** (**bi**nary **d**igit) -> Bitstrom
- Informationsträger: elektrische oder optische Signale (Lichtfarben)
  Funk: elektromagnetische Wellen
- Informationen werden über Drähte/Kabel oder elektromagnetische Wellen durch Variieren bestimmter Eigenschaften (z.B. Spannung, Strom bzw. Laser (Lichtfarben)) übertragen.

Übertragungsstörungen (Modell: Shannon - gestörter Übertragungskanal)

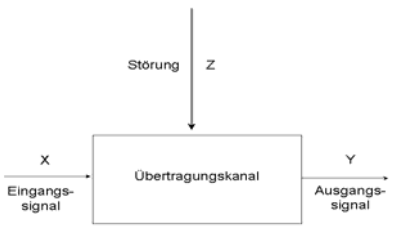


Abbildung 3.2: Kanalmodell (Shannon)

- Dämpfung: Energieverlust bei Ausbreitung des Signals.

- Laufzeitverzerrung: Unterschiedliche Ausbreitungsgeschwindigkeiten (vorauseilende / einholende / überholende Bits).
- Rauschen: unerwünschte Energien anderer Quellen.

Digitalisierung analoger Signale: Signalabtastung, 8-Bit-Muster (Puls-Code-Modulation, PCM)

Modulation/Demodulation

Aufbringen des Signals auf Trägermedium (bzw. Herunternehmen)

- Amplitudenmodulation: Nutzung 2er verschiedener Spannungspegel für 0 und 1
- Frequenzmodulation: Nutzung verschiedener Töne (Frequenzen)
- Phasenmodulation: Trägerwelle um n Grad versetzt (jeder Versatz überträgt 2 Datenbit)

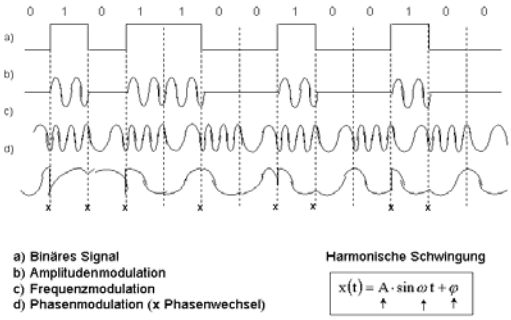


Abbildung 3.3: Signalmodulation (Beispiele)

Zugehöriges Gerät: **Modem** (**Mo**dulation / **Dem**odulation)

Oftmals kombinierte Modulationstechniken, z.B. Quadraturmodulation (QAM): Kombination von Amplituden- und Phasenmodulation. Sog. Konstellationsmuster kennzeichnen die zulässigen Kombinationen von Amplitude und Phase. Verfahren, z.B. ITU-Standard

V.21		300 bit/s-Modems	FDM
V.22		1 200 bit/s-Modems	FDM
V.32	für	9 600 bit/s-Modems	QAM
V.32bis		14 400 bit/s-Modems (Faxmodems)	TCM (Trellis)
V.34		28 800 bit/s-Modems	TCM

Zur Verringerung der Fehler-Wkt. fügen viele Modems ein Paritätsbit ein -> Aufgabe der sog. Trellis-Codierung (TCM).

Multiplexing

Mehrere Übertragungen gleichzeitig über gleichen Übertragungskanal. Wichtigste Verfahren:

Frequenz-Multiplexverfahren (FDM: Frequency Division Multiplexing)

- Gesamtes Frequenzspektrum in einzelne logische Kanäle aufgeteilt (mit Sicherungsband), jeder Benutzer erhält den exklusiven Besitz eines einzelnen Frequenzbandes.
- Typische Anwendung: Telefonnetz

Zeit-Multiplexverfahren (TDM: Time Division Multiplexing)

- Frequenzband zeitlich aufgeteilt. Jeder Benutzer erhält vorübergehend die gesamte Bandbreite über eine bestimmte Zeitdauer zugeteilt.
- Benutzer wechseln sich ohne gegenseitige Kenntnis ab.
- *Typische Netze: Paketvermittlungsnetze (X.25, IP, ATM).

Raum-Multiplexing (SDM: Space Division Multiplexing)

- Nutzung gleicher Frequenz in benachbarten Räumen.
- Typisches Netze: Zellularfunk (Ausnützen Dämpfungseigenschaften der Funkwellen).

Code-Multiplexing (CDM: Code Division Multiplexing)

- Nutzung unterschiedlicher Codes zur Übertragung mehrerer Vorgänge. Empfänger kennt Code, andere Codes nur noch als Rauschen erkannt und herausgefiltert.

- Frequenzband auf gesamte Breite des Frequenzbereiches aufgespreizt (Verwendung sog. Spreizcodes (Chips), die Sender und Empfänger auch bekannt sind).
- Anwendung im Zellularfunk (IS-95-CDMA, UMTS Phase 2+) und in Militärtechnik (Abhörsicherheit).

Wellenlängen-Multiplexverfahren (WDM: Wavelength Division Multiplexing)

- In Glasfaserkabel werden verschiedene Frequenz-Multiplexverfahren kombiniert angewandt => genannt: Wellenlängen-Multiplexing (WDM).
- Informationssignal auf Wellenfarben aufmoduliert. Verschiedene Lichtfarben (Wellenlängen) parallel übertragen.
- Einsatz in optischen Netzen (Glasfasernetze), $v_{ü} > 2.5$ Gbit/s.

3.2 Übertragungsmedien

Kategorien von Übertragungsmedien

- magnetische Medien (Band, Platte)
- terrestrische Medien (Kupferkabel, Koaxialkabel, Glasfaser/Lichtwellenleiter)
  Unterseekabel (Kupferkabel -> Glasfaserkabel)
- aerische Medien (Funk, Infrarot, Laserstrahl): Satelliten, Funksysteme

3.2.1 Magnetische Medien (incl. opt. Speicherung)

Medium: Magnetband, festplatte,Diskette, CD-ROM (bzw. RW),
bzw. mit optischer Speicherung: DVD, Blu-Ray, USB-Stick
Merkmale: sequentieller bzw. wahlfreier Zugriff, offline-Verbindung, hohe Übertragungskapazität, z.B.
8 mm-Videoband: 7 Gbyte, CD-RW: 800 MB, Blu-Ray: 54 GB dual layer
Geschwindigkeit vglb. ATM, aber < WDM/SDH. Für große Datenmengen ggf. akzeptable Lösung, aber keine online-Verbindung, keine Interaktionen.
Heutiger Standard $_{2011}$: CD, DVD, USB

3.2.2 Drahtgebundene Übertragung

Verdrilltes Kupferkabelpaar

Online-Verbindung, häufigste Anwendung (insbes. im Netzzugangsbereich). 2 Kabel, i.allg. Durchmesser 1 mm. Verdrillung --> Reduzierung der elektromagnetischen Störungen.
Wichtigste Anwendung: *Telefonnetz* (--> Realisierung FTTH-Paradigma). Bei längeren Strecken: Verstärkung durch *Repeater.* Geeignet für analoge und digitale Signale.
Verschiedene Ausführungen, u.a.
Telefonnetz:
Sternvierer: 4 Adern, um sich selbst verdrillt, mit Kunststoffhülle (sog. Kategorie 3) .
Rechnernetz:
Kategorie 5: analog Kategorie 3, aber stärker verdrillt und mit Teflonbeschichtung. Damit bessere Isolation und größere Entfernung. 2 Typen

- Unshielded Twisted Pair (UTP): unabgeschirmte verdrillte Kabelpaare, jeweils 2 Adernpaare verdrillt.
- Shielded Twisted Pair (STP): ähnlich UTP; aber außerhalb IBM nicht durchgesetzt.

Koaxialkabel

Bessere Abschirmung als verdrillte Kabelpaare.Für größere Geschwindigkeit und Entfernungen geeignet.

- Basis-Koaxialkabel
  50 ohmig: i.allg. für digitale Übertragung.

75 ohmig: i.allg. für analoge Übertragung (siehe Breitband-Koaxialkabel)

- Breitband-Koaxialkabel
  Für analoge Übertragung im Kabelfernsehen, 300 bzw. 450 MHz, 100 km Länge.
  Aufteilung i.allg. in 6-MHz-Kanäle für TV-Übertragung. Diese Kanäle unabhängig voneinander für analoges TV, Audio in CD-Qualität (1.4 Mbit/s), digitale Datenübertragung (z.B. 3 Mbit/s). Breitband-Koaxialkabel benötigen Analogverstärker.

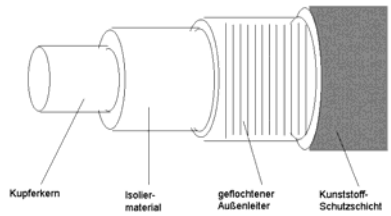


Abbildung 3.4: Aufbau Koaxialkabel

Lichtwellenleiter

Lichtsignale als Träger der Informationen --> optische Netze (Glasfasernetze)
Voraussetzung: genaue Laserquellen
Übertragungsraten: 2.5 Gbit/s ... 400 Gbit/s ... mehrere Tbit/s
Komponenten eines optischen Übertragungssystems:
Lichtquelle, Übertragungsmedium (Glasfaser), Detektor
Lichtquelle: nimmt elektrisches Signal an und wandelt es in Lichtimpulse (Modulation).
LED (Licht Emitierende Dioden) 20 ... 50 Mbit/s für Multimode
Laser-Diode bis zu 10 Gbit/s für Monomode
Licht => 1-Bit
Kein Licht => 0-Bit
Übertragungsmedium: dünne Glasfaser. I.allg. mehrere Fasern gebündelt und durch Außenhülle geschützt.
Multimode-Faser: dickerer Kern, viele Lichtstrahlen schwirren in der Faser (mehrere Wellenlängen). Faserdurchmesser a = 50 ... 70 μ ; a = 50 λ (λ: Wellenlänge des Lichts)
Monomode-Faser: dünner Kern, nur eine einzige Wellenlänge. Teuer, aufwendige Installation
Faserdurchmesser a = 1 ... 2 μ ; a ~ λ (λ: Wellenlänge des Lichts)
Detektor: wandelt Lichtimpulse wieder in elektrische Signale um.

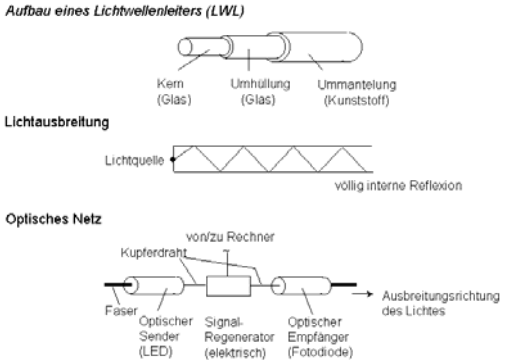


Abbildung 3.5: Aufbau Lichtwellenleiter und optisches Netz

Netze mit Lichtwellenleitern
Nutzung von 2 Schnittstellenarten:

- passive Schnittstellen: angeschweißt.

- aktive Repeater: Umwandlung Licht in elektrisches Signal, ggf. verstärkt und wieder als Licht abgesendet.

Neuere LWL-Netze: Verwendung optischer Schalter (Add/Drop), optische Verstärker und Regeneratoren, keine Wandlung in elektrische Signale ~> Performancesteigerung (siehe Kap. „Optische Netze“). Topologien: Ring (für LAN), Stern (für HW-Broadcasting)

3.2.3 Drahtlose Übertragung

Elektromagnetisches Spektrum und seine Verwendung in der Telekommunikation
Nationale und internationale Vereinbarungen über die Nutzung der Frequenzen
international: ITU-R (WARC) ITU: International Telecommunications Union
USA: FCC (nicht an WARC gebunden) FCC: Federal Communications Commission

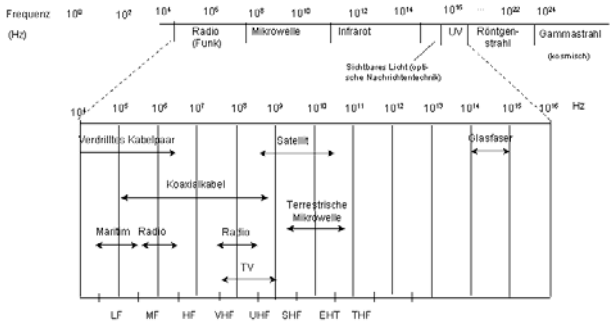


Abbildung 3.6: Elektromagnetisches Frequenzspektrum

Die meiste Übertragungen nutzen schmales Frequenzband, um optimalen Empfang zu sichern. Im Militärbereich und Satellitenübertragung oft Sprung zwischen schmalen und breiten Frequenzband (Frequency Hopping, Streuspektrum, Sicherheit gegen Abhören und gegen Schwingungen). Im kommerziellen Bereich u. WLAN: *Direct Sequence Spread Spectrum* (echtes Streuspektrum; Spreizcode: Signal auf gesamte Bandbreite aufgepreizt ~> verbesserte spektrale Effizienz).

Radiowellen
Elektromagnetische Wellen, sind rundstrahlend (omnidirektional), d.h. keine Ausrichtung zwischen Sender und Empfänger erforderlich --> geeignet für Verteilkommunikation (TV). Sie sind leicht erzeugbar, für große Entfernungen, Eindringen in Gebäude=> für Kommunikation im Inneren und Äußeren geeignet.
Merkmale der Radiowellen:
Frequenzabhängig, bei niedrigen Frequenzen leicht durch Hindernisse hindurchdringend, Leistung aber mit $1/r^3$ in Luftentfernung abfallend (Dämpfung). Problem der Störungen, insbesondere bei großen Entfernungen.
In *niedrigem Frequenzband* (VLF, LF, MF) folgen die Radiowellen der Erdoberfläche und dringen mühelos in Gebäude ein (z.B. AM-Hörfunk). Problem für Datenkommunikation: geringe Bandbreite.
In *höherem Frequenzband* (HF, VHF) werden bodennahe Wellen von Erde absorbiert. Die in Höhe gerichteten Wellen werden von Ionosphäre gebrochen.

Richtfunk (Mikrowellenübertragung)
Wellen bei > 100 MHz verlaufen geradlinig und können eng gebündelt werden. Sende- und Empfangsantennen müssen genau aufeinander ausgerichtet sein.

Vor Glasfaser bildete Mikrowellen-Übertragung das Kernnetz für Ferngespräche (z.B. MCI aus Microwave Communications Inc. hervorgegangen). Bei größeren Entfernungen sind Repeaterstationen erforderlich (Erdkrümmung). Mikrowellen können schlecht durch Gebäude dringen. Routinemäßiger Frequenzbereich bis zu 10 GHz (bei 8 GHz kommt Absorption durch Wasser hinzu => Regenproblem).
Mikrowellenkommunikation stark verbreitet im Telefonsystem, Funktelefonie, Fernsehen. Vorteile gegenüber Glasfaser: keine reglementiertes Vorrecht (z.B. Mikrowellenturm in kleinem Grundstück -> kein extra Drahtnetz; Bsp.: im Campusnetz Universität Leipzig).
MCI: Mikrowellen-Telefonnetz (MCI Microwave), dagegen Sprint: Nutzung Glasfaser neben Eisenbahnschiene (Gründerfirma: Southern Pacific Railroad).
Anwendungen:
- Langstreckenkommunikation
- Campusnetze
- ISM-Band: Industrie / Wissenschaft / Medizin (Bereich 2.400 ... 2.484 GHz)
- Bänder 902 - 928 MHz bis 5,725 - 5,850 GHz: für drahtlose Telefone, Garagentoröffner, drahtloser HiFi-Lautsprecher.

Zur Beachtung für spezielle Funkbereiche:
Freigabe von Frequenzen in Deutschland $_{2010}$, insbes. für die Internet-Breitbandanbindung des ländlichen Raumes (sog. „Surfen auf dem Dorf“) und für Mobiltelefonie (u.a. LTE). Schwerpunkt: digitale Dividende (engl. *digital dividend*) -> durch Digitalisierung des Rundfunks frei werdenden Frequenzbänder (insbes. durch Umstellung terrestrisches TV von PAL auf DVB-T).
Für die im Bereich 850 MHz betriebenen Funkmikrofone (Headsets, Lavalier- und Hand-Mikrofone) der Veranstaltungstechnik sollen alternative Frequenzbereiche bereitgestellt werden.

Infrarot- und Millimeterwellen
Für Kurzstreckenkommunikation (Nahbereichsanschluss).
Leistung: Infrared (IR): 0,115 Mbit/s (SIR), 4 Mbit/s (FIR), 16 Mbit/s (VFIR)
Standard und Konsortium: IrDA (Infrared Data Association).

1994: 1. Standard IrDA 1.0 (sog. SIR, Serial Infrared): Datenraten bis 115,2 kbit/s.
1995: Erweiterung IrDA 1.1 (sog. FIR: Fast Infrared): Datenraten bis 4 Mbit/s.
1999: Erweiterter Standard (sog. VFIR: Very Fast Infrared). Datenraten bis 16 Mbit/s.

Anwendungen:
Kopplung peripherer Geräte an PC bzw. PDA (Personal Digital Assistant) mit PC.
Fernsteuerung von TV-Geräten, Videorecordern, Stereogeräten.
Gerätetreiber in Betriebssystemen des PC, PDA und Handys.

Preisgünstig, aber IR-Wellen können keine festen Gegenstände durchdringen (Eigenschaft wie Licht). Jedoch Vorteil gegenüber Abhören (Sichtentfernung). Somit Infrarot gut für interne drahtlose LAN, insbesondere in einem Raum.
Infrarot und Bluetooth (Funkübertragung im 2.4 GHz-Band) sind Basis für Nahbereichskommunikation, sog. *WPAN (Wireless Personal Area Networks).*

Lichtwellenübertragung
Übertragung mit Laserstrahlen.
Schon seit Jahrhunderten zur *aerischen optischen Zeichengabe* genutzt (Licht).
Moderne Anwendung: Laserstrahlen - optische Zeichenübergabe über Laser (unidirektional).
Nachteile von Laserstrahlen:
- exakte Ausrichtung zwischen Sender und Empfänger erforderlich.
- Laserstrahlen können Regen oder dichten Nebel nicht durchdringen

Glasfaserübertragung
Glasfasernetz (LWL-Netz): optische Netze (Übertragung und Vermittlung).
- Leicht installierbar, kostengünstig, hohe Bandbreite. Keine FCC-Lizens erforderlich.
- Übertragungsleistung: > 2.5 Gbit/s (neue LWL- und genaue Lasertechniken).

Unterseekabel
Kontinente überspannende Übertragung. Erstmalig 1851 Telegraphie an Ostküste der USA (Kupferkabel); heute Glasfaserkabel. Verbindung der Kontinente untereinander: Europa, Afrika, Amerika, Australien, Neuseeland, Mikronesien.
I.allg. im Bestand der nationalen Telekommunik.-Konzerne (z.B. Telekom: TAT12 / 13 $_{WiN}$).
Gegenstück zu Satellitenkommunikation (Kommunikationssatelliten).
Gefahren für Unterseekabel:
- Haie fressen Kabel an
- Niveauunterschiede: Kontinentalsockel – tiefer Graben
- Fischernetze, Raubfische, Boote (in seichten Gewässern 3 m tief eingegraben)

Installations- und Wartungsschiff
- Atlantic Guardian (Stapellauf 2001, van-Giesen-Werft)
- Heimathafen Baltimore (Nationalhymne der USA);
- Gesetzlich eng geregelte Reparaturzeiten.

3.3 Netze für Datenübertragung (Anwendungsnetze)

Nachrichtennetze (Auswahl)
Telefonnetz (Basis: Kupferkabel): Sprachübertragung (+ Daten)
- POTS: Plain Old Telephone Service
- PSTS: Public Switched Telephone System

ISDN (Schmalband-ISDN, S-ISDN; Basis Kupferkabel) Sprache (+ Daten)
Hochgeschwindigkeitsnetze (Basis: LWL): Daten (Paketdatenübertragung)
- PDH (Plesiochronous Digital Hierarchy)
- SONET (Synchronous Optical Network)
- SDH (Synchronous Digital Hierarchy)

Mobilfunknetze (Basis: elektromagnetische Welle): Sprache (+ SMS + Daten)
- Zellularfunknetze (Basis: Funkwellen): 2G -> 2.5G -> 3G

Satellitenkommunikation (Basis: Funkwellen): Sprache + Daten

3.3.1 Telefonsystem

Öffentliches Fernsprechwählnetz (Public Switched Telephone Network - PSTN)
Wichtigste Komponenten
- Ortsvermittlung (verdrillte Kabelpaare, analoge Zeichengabe bzw. digital/ISDN)
- Fernvermittlungen (LWL oder Mikrowelle, digitale Zeichengabe)
- Vermittlungsämter

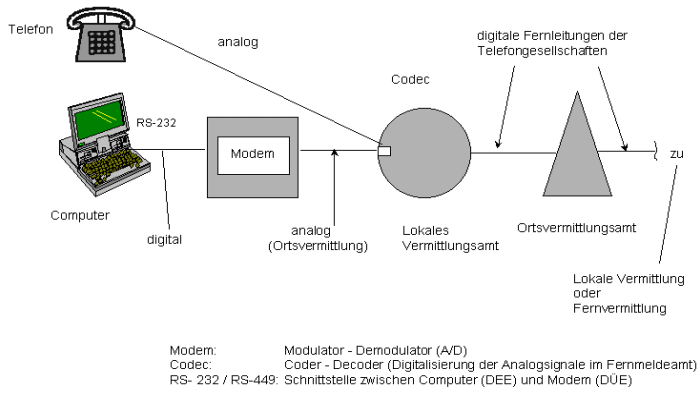


Abbildung 3.7: Telefonsystem

Ortsvermittlung: z.T. noch (infolge Tradition) analog Zeichengabe. A/D-Wandlung über sog. Modems.

Multiplexen und Fernvermittlung
Multiplexen := mehrere Kommunikationskanäle gleichzeitig über gleiche physische Leitung
Wichtigste Verfahren in Telefonsystemen:
Frequenz-Multiplexverfahren (FDM: Frequency Division Multiplexing)
- Frequenzspektrum auf die logischen Kanäle aufgeteilt.
- Jeder Benutzer erhält ausschließlichen Besitz eines Frequenzbandes.
  (Anmerkung: bei Glasfaserkanälen verschiedene FDM-Verfahren kombiniert angewandt => sog. Wellenlängen-Multiplexing (WDM: Wavelength Division Multiplexing)

Zeit-Multiplexverfahren (TDM: Time Division Multiplexing)
- Zeitliche Aufteilung der Übertragungsbandbreite.
- Jeder Benutzer erhält vorübergehend für bestimmte Zeitdauer die gesamte Bandbreite.
  TDM kann vollständig digital realisiert werden (im Gegensatz zu FDM).

Fernvermittlung: vollständig digital

Übertragung im Sprachbereich
Dazu sind Analogsignale zu digitalisieren:
- Geräte Codec (im Fernmeldeamt, Ortsamtstechnik). Digitalisierung der Analogsignale.
- Zugehöriges Verfahren: PCM (Pulscodemodulation)
  8000 Abtastungen pro Sekunde, 125 ms-Rahmen (Sample)
  Abtastung := Modulation eines unstetigen Signals (0 | 1)
  Nyquist-Theorem: Abtastung mit doppelter Frequenz (Sprache 4 kHz --> 8000 Abtastungen/s) ermöglicht genau eine verlustfreie Darstellung des analogen Signals als digitales Signal.

ITU-T konnte PCM international nicht standardisieren -> viele inkompatible Systeme.

Digitale Übertragung
Im digitalen Bereich wurde in Nordamerika und Japan der sog. T1-Träger entwickelt
(exakt: **DS1**-Format)
T1: 24 Sprachkanäle, die gemultiplext werden. Je Kanal: 8 Bit
- 7 Bit Nutzdaten
- 1 Bit zur Steuerung

Somit je Kanal 7 * 8000 Abtastwerte (Daten) + 1 * 8000 Abtastwerte (Zeichengabe-Information)
T1-Rahmen besteht aus 24 * 8 = 192 Bit + 1 Bit zur Rahmenbildung = 193 Bit pro 125 ms
Insgesamt Bruttodatenrate von 1.544 Mbit/s (sog. primary rate):
193 bit / 125 ms = 193 * 8000 bit/s = 1.544 Mbit/s.

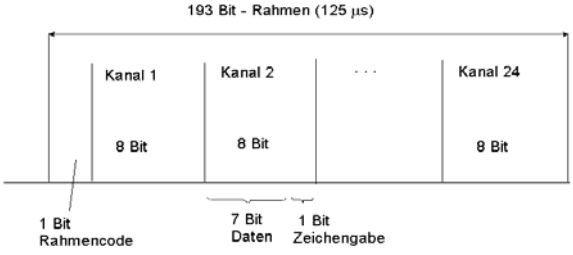


Abbildung 3.8: Aufbau T1-Träger (1.544 Mbit/s)

Wird T1-Träger ausschließlich für Daten verwendet, werden nur 23 Kanäle benutzt (24. Kanal dient zur speziellen Synchronisation). Zeitmultiplexing TDM erlaubt auch, mehrere T1-Träger in höherwertige T1-Träger (T2, T3, ...) zu multiplexen.
=> ***PDH: Plesiochrone Digitale Hierarchie***

3.3.2 ISDN (Integrated Services Digital Network)

Schmalband (Narrow-Band) - ISDN (S-ISDN):
- Aufbau eines digitalen, leitungsvermittelten Telefonsystems
- Vorrangig Sprachdienste, auch Datenübertragung (z.B. audio/video, u.a. Audio-Video-Conference Systems, Bildtelefon).

Von CCITT *standardisierte Kanalkombinationen*
1. **Basisanschluss** 2 B + 1 D
2. **Primärmultiplexanschluss** 23 B + 1 D (USA, Japan)
   30 B + 1 D (Europa)
3. **Hybridanschluss** 1 A + 1 C

   mit A - analoger Telefonkanal (4kHz)
   B - digitaler PCM-Kanal für Sprache oder Daten (64 kbit/s)
   C - digitaler Kanal (8 oder 16 kbit/s)
   D - digitaler Kanal für bandexterne Zeichengabe (16 bzw. 64 kbit/s)
   E - digitaler Kanal für bandinterne ISDN-Zeichengabe (64 kbit/s)
   H - digitaler Kanal (384, 1.536 oder 1.920 kbit/s)

Max. Datenraten: Basisanschluss: 2 * 64 + 16 = 144 kbit/s
Primärmultiplex: 1.544 Mbit/s (USA, sog. Primary Rate)
2.048 Mbit/s (Europa)

Basisanschluss -> Ablösung des konventionellen Telefondienstes (POTS: Plain Old Telephone Service) für Haushalte und kleine Betriebe ~> Realisierung FTTH-Paradigma.

3.3.3 Hochgeschwindigkeitsnetze

Basis für Hochgeschwindigkeitsnetze
- i.allg. Lichtwellenleiter (Glasfaserkabel; optische Übertragung).
- verschiedene Übertragungsrahmen auf Bitübertragungsschicht.

PDH - Plesiochrone Digitale Hierarchie
Synchrones Zeitmultiplexverfahren (STM, Rahmen im ÜK immer an gleicher Stelle, d.h. Rahmen ggf. auch leer übertragen).
Basis T1; durch Multiplexen T2, T3, usw.
insbes. Einsatz in Nordamerika, Japan; noch heute Basis für einige WAN.

T1 - Kanal: 1.544 Mbit/s
T2 - Kanal: 6.312 Mbit/s (4 T1-Ströme)
T3 - Kanal: 44.736 Mbit/s (6 T2-Ströme)
T4 - Kanal: 274.176 Mbit/s (7 T3-Ströme)

CCITT definierte das Multiplexen von 4 in einem Strom auf jeder Ebene.

Somit CCITT-Hierarchie: Anzahl Kanäle	Geschwindigkeit (Mbit/s)
32	2,048
128	8,848
512	34,304
2048	139,264
8192	565,148

SONET
Zielstellung eines **synchronen TDM** für LWL (Zeitmultiplex), insbesondere:
- Zusammenführung verschiedener Netzbetreiber (Zeichengabe, Zeittakt, Rahmenstruktur)

- Vereinheitlichung der digitalen Systeme in Nordamerika, Japan, Europa: alle mit 64 kbit/s Kanäle
- Multiplexen mehrerer digitaler Kanäle (insbes. höher als T3 = 44.736 Mbit/s --> bis Gbit/s)
- Unterstützungen für Betriebsabläufe, Administration und Wartung (OAM) bereitstellen

1985: Bellcore Forschungslabor: Entwicklung des Standards SONET (Synchronous Optical Network)
1989: Eintreten CCITT in diese Bemühungen
=> Verschiedene Empfehlungen (G.707, G. 708, G.709)
=> Empfehlungsreihe: *SDH (Synchronous Digital Hierarchy)*
SONET-Basisrahmen: Block von 810 Byte alle 125 ms übertragen.
Da SONET synchron, werden Rahmen immer ausgegeben (mit Nutzdaten oder leer).
8000 Rahmen/s = Abtastrate von PCM-Kanäle (alle digitale Telefonsysteme).
Somit 8 * 810 = 6.480 Bit, die 8000 mal pro Sekunde zu übertragen sind => Bruttodatenrate.
STS-1 : 51,84 Mbit/s (STS: Synchronous Transport Signal).
Alle SONET-Bündel sind ein Vielfaches von STS-1 (STS-1, ... , STS-48).

SDH – Synchrone Digitale Hierarchie
Standard der CCITT (1989). Zugehörige Empfehlungen: G.707, G.708, G.709.
Basis für Breitband-ISDN-Architektur (B-ISDN/ATM) sowie für SDH/WDM-Technologie.
=> **ATM: Asynchronous Transfer Mode** (spezielles Cell-Relay der CCITT; Pakete konstanter Größe).
Als Unterscheidung zum synchronen Betrieb bei SONET werden bei ATM auch unregelmäßige (asynchrone) Zellenankünfte erlaubt.

Vermittlungstechniken in Hochgeschwindigkeitsnetzen
- Leitungsvermittlung (Durchschaltevermittlung): für analoge Übertragung (Telefon)
- Paketvermittlung: in Datenkommunikation
- Crossbar / Switches: für ATM-Technologie

SONET		SDH	Datenrate [Mbit/s]	
elektrisch	optisch	optisch	Brutto	Nutzerdaten
STS - 1	OC - 1		51,84	49,536
STS - 3	OC - 3	STM - 1	155,52	148,608
STS - 9	OC - 9	STM - 3	466,56	445,824
STS - 12	OC - 12	STM - 4	622,08	594,432
STS - 18	OC - 18	STM - 6	933,12	891,648
STS - 24	OC - 24	STM - 8	1244,16	1188,864
STS - 36	OC - 36	STM - 12	1866,24	1783,296
STS - 48	OC - 48	STM - 16	2488,32	2377,728

OC: Optischer Träger (LWL)
STS: Elektrischer Träger
STM: Synchronous Transfer Mode (LWL)
ATM beginnt ab 155 Mbit/s (Basiskanal STM-1)

Abbildung 3.9: Zusammenstellung SONET – SDH

3.3.4 Mobilfunknetze

Mobile Computing
Komponenten: Portable Computer: Notebooks ... Handhelds (Smartphone, Tablet PC)
Drahtlose Netze (Funkübertragung, wireless)
Ausprägungen: ubiquitous / nomadic / pervasive Computing

Netzstrukturen: Infrastrukturnetze / mobile ad-hoc-Netze (spontane Vernetzung)
Kooperationsmodelle: Client/Server, Peer-to-Peer (P2P)

Klassifikation

Funknetze

Flächendeckende Funknetze (Wireless WAN, Mobilfunk):

- Zellularfunknetze: Ausgang Mobiltelfonie, nun verstärkt Datenfunktechnik
  Kanalvermittelt (Sprache, u.a. GSM, EDGE, UMTS), Paketvermittelt (GPRS, HSDPA))
- Bündelfunk, Funkruf, schnurlose Telefonie (auch als W-LAN, DECT), Satellitennetze
- Internet: mobile / cellular IP

Lokale Funknetze (Wireless Radio Networks):

- W-LAN nach Standard IEEE 802.11 bzw. ETSI / HIPERLAN, HomeRF
- W-ATM (wireless broadband communications, Trend zu IP ~> "all IP"), Wimax

Drahtlose Nahbereichskommunikation (Raumnetze, WPAN):

- Infrarot, Bluetooth, RFID, NFC

Personensuchsysteme (Paging-Systeme)

Endgeräte: Lautsprecher (in Gebäuden) bzw. kleine Handgeräte (Piepser).
Moderne Piepser an Computer ansteckbar und somit Info's an Festnetz weiterleitbar. Falls ein Piepser vom Sender ein Signal erhält und seine Nummer kennt, gibt er ein akustisches Signal. I.allg. unidirektional. Wenig Bandbreite erforderlich (nur geringe Anzahl von Bytes übertragen). Frequenzband 150 - 174 MHz, neuere Systeme 930 - 932 MHz.

Drahtlose Telefone (schnurlos, cordless)

2 Teile: Basisstation (ans Festnetz angeschlossen)
1 ... n Telefone (drahtlos verbunden)

Entwicklungen:
- CT-1 (USA), CEPT-1 (Europa) 1. Generation
- CT-3 DECT - Standard (1993), sog. 3. Generation
  (DECT: Digital Enhanced Cordless Telephone)
- PHS (Japan): Personal Handyphone System
- IS.134 (USA)

Massenmarkt; auch für FemToCell (Anm.: CT nicht mehr betrieben).

Analoge Funktelefonsysteme

1964 (USA): erste Autotelefone
1960er: **IMTS** (Improved Mobile Telephone System): Unterstützung von 23 Kanäle im Bandbereich 150 - 450 MHz
1982: **AMPS** (Advanced Mobile Phone System): Einsatz in USA ("AMPS"), UK ("TACS") und Japan ("MCS-L1"). Aufteilung des Bereiches in Zellen (zugehörige Frequenzen). Wiederverwendbarkeit der Frequenzen in entfernten Zellen.
In Deutschland: **A- , B- , C- Netze** (öbl: öffentlicher beweglicher Landfunk): A-Netz (1958), B-Netz (1972), C-Netz (1986, 1996 abgeschaltet). Aufbau als Zellularfunknetze (ab C-Netz: Handover, Roaming) ~> Ablösung durch digitale Netze.

Aufbau einer Zelle (ca. 10 km): Clusterisierung des Versorgungsbereiches (Dämpfung)

- enthält eine Basisstation (Antenne für Endgerät und Computer)
- alle Basisstationen sind angeschlossen an MTSO (Mobile Telephone Switching Office) oder MSC (Mobile Switching Center). MTSO / MSC kommunizieren über öffentliche Telefon- oder Paketvermittlungsnetze.

Beispiele Zellularnetze AMPS (American Mobile Phone System), öbl C-Funk (DE).
Realisierung:

- *Handover*: -Automatisches Wechseln der Funkzelle (Messung Funkintensität, Zuordnung

Funkkanal), Verwalten der aktuellen Ortskoordinaten, Location Update.
- Roaming: Auffinden des Teilnehmers (Strategie: "Information folgt dem Teilnehmer"). Freizügiger Ortswechsel, d.h. Teilnehmer anrufbar, wenn er seinen Ort wechselt (auch internationales Roaming).
- *Mobilitätsverwaltung*: Datenbank, mit Aufenthaltskoordinaten und Nutzerprofil (Home- und Visitor Location Register, Authentisierung, Geräteidentifikation).

Digitale zellulare Funknetze
Digitalisierung der Funknetze
USA:
AMPS --> Standards IS-54 und IS-135 (sog. Frequenzzuteilungsschemata)
und --> Standard IS-95 (sog. Frequenzverteilungsspektrum, Nutzung CDMA)
Frequenzband: 1.9 GHz (**D-AMPS**)
Europa:
GSM: Global System for Mobile Communications (Standard durch ETSI):
GSM nutzt die Multiplexverfahren FDM (Frequenz Division Multiplexing), TDM (Time Division Multiplexing) und Raummultiplexing SDM
Frequenzband: 900 MHz
Betreibersysteme: D1 (Telekom, T-Mobile), D2 (Mannesmann, Arcor, Vodafone)

DCS-1800 (Standard durch ETSI):
Frequenzband: 1.8 GHz
Betreibersystem: E1 (E-Plus, o.tel.o), E2 (Viag Interkom, O2)

Weitere Entwicklungen:
Weiterentwicklung der 2G-Netze (GSM, DCS) durch Anwendung Kanalbündelung (HSCSD) und Pakettechnik --> GPRS und EDGE (2.5G): 115 ... 384 kbit/s
- **PCS** (USA, Personal Communications Services) bzw. PCN (weltweit, Personal Communications Network); Aufbau von hot-spots.
  Mikrozellen (Durchmesser 50 ... 100 Meter), erlaubt auch leichtere Telefone. Mehrfachverwendung der Frequenzen (~> Aufbau von **hot spots**) -> Ausbau zur sog. 3. und 4. Generation der Zellularfunknetze.
- **UMTS** (Universal Mobile Telcommunications System, 3G): Integration der wichtigen Funknetze und Satellitenkommunikation, 384 kbit/s ... 2 Mbit/s, mit HSDPA 1,8 ... 7,2 Mbit/s (speziell bis 28 Mbit/s.)
  MBS (Mobile Broadband System): **W-ATM** / AAL2: 100 Mbit/s (--> IP-Technik), Wimax
- **LTE** (Long Term Evolution): Verbesserungen in Funkvermittlung, sog. MFN 4G
  Leistung 100 Mbit/s $_{2011}$ ... 1 Gbit/s $_{2014}$. UPT (Universal Personal Telecommunication),
- mobile und cellular IP, Adressierung und Service-Discovery, Einsatz DHCP.

3.3.5 Satellitenkommunikation

Kommunikationssatellit
- großer Mikrowellenverstärker am Himmel.
- enthält 1 ... n Transponder für verschiedene Frequenzbereiche, die das eingehende Signal verstärken und Signal auf anderen Frequenzen an Erde zurücksenden.

Geostationäre Satelliten (GEOS: Global Earth Orbit Satellite)
Frequenzbänder: 4 ... 30 GHz, FDM-Multiplexverfahren.
Erdferne Satelliten ~> erfordern aber leistungsstarke Sende-/Empfangseinrichtungen.
Entwicklung kostengünstiger Mikrostationen (VSAT: Very Small Aperture Terminal):
19.2 kbit/s aufwärts (upstream)
512 kbit/s abwärts (downstream)

System **INMARSAT**
3 geostationäre Satelliten, 36 000 km Höhe
seit 1982 in Betrieb (insbes. für Schiff-Schiff-Kommunikation und TV).

Erdnahe Satelliten (LEOS: Low Earth Orbit Satellite)
Leistungschwächere Sende-/Empfangseinrichtungen, z.B. Satelliten-Handys (Motorola).
Schnell umlaufende Satelliten projizieren Funkzellen auf Erdoberfläche („Zellularsystem“).

***Motorola Iridium** Project (1990):*
Globales Netzwerk für Personal Communication.
77 Satelliten (Element 77: Iridium) - nur 66 Satelliten realisiert (~> Iridium-System).
Iridium - System
66 Satelliten, 750 km Höhe; inges. 283 272 Kanäle (je Satellit max. 48 Punktstrahlen mit insges. 1 628 Zellen über Erdoberfläche)
1.6 GHz - Band (auf- und abwärts). 1999/2000 abgeschaltet (kommerzielle Gründe)
Satellitenprojekte:

Inmarsat-2	10 Satelliten	10 000 km
Globalstar	24 Satelliten	1 400 km
Iridium	66 Satelliten	860 km
Teledesic	840 Satelliten	600 km

4 Sicherungsschicht (Data Link Layer)

4.1 Architektur DLL-Schicht

4.1.1 Dienste für Vermittlungsschicht

Sicherungsschicht (Data Link Layer, DLL)
OSI-Referenzmodell: Schicht 2
DoD-Referenzmodell: Host-to-Host-Schicht (Lokales Netzwerk)

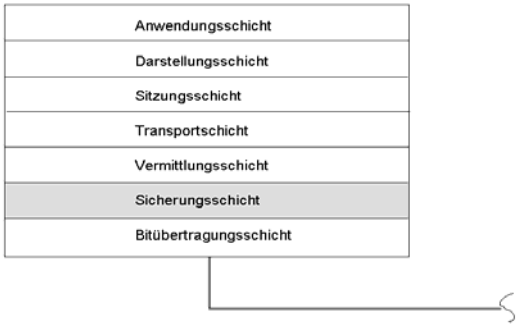


Abbildung 4.1: Schichtenmodell (OSI, Schicht 2)

Aufgaben der Sicherungsschicht:
- Bereitstellung von Diensten für die übergeordnete Vermittlungsschicht
- Aufteilung der Daten in Rahmen (Frames) und Begrenzung der Rahmen
- Flusssteuerung (Richtung, Reihenfolge, Geschwindigkeitsabgleich)
- Fehlererkennung und Fehlerkorrektur

Hauptaufgabe für DLL: Übertragung von Daten der Vermittlungsschicht (Schicht 3).
Über SAP’s (Service Access Points) können der Schicht 3 folgende Dienste angeboten werden (Q: Quelle, S: Senke):
1. unbestätigter verbindungsloser Dienst: Q --> S, ohne Bestätigung und ohne feste logische Verbindung.

2. bestätigter verbindungsloser Dienst: Q --> S, keine feste logische Verbindung, aber Empfang jedes Rahmens wird bestätigt (bei Fehler: Sendewiederholung).
3. verbindungsorientierter Dienst: Q --> S, mit fester logischer Verbindung (Verbindungsaufbau, Transfer, Verbindungsabbau).

4.1.2 Rahmenerstellung

Bitstromübertragung

Dazu benutzt die Data Link Layer die Dienste der Bitübertragungsschicht.
Bitübertragungsschicht: unbearbeiteter Bitstrom. Dabei können Fehler auftreten (Verlust, unterschiedliche Anzahl).
Sicherungsschicht muss diese Fehler aufdecken (Fehlererkennung) und ggf. korrigieren (Wiederholung bzw. automatische Fehlerkorrektur).
Dazu: Bitstrom aufgeteilt in diskrete Rahmen (Frame), mit Prüfsumme (~> Prüfsummenalgorithmen). Wenn beim Empfänger bei der *Prüfsummenkontrolle* Abweichungen auftreten ~> Behebung veranlassen.

Unterteilung des Bitstroms (Rahmenabgrenzung)

Einfachste Form:

- Einfügen von Leerstellen. Aber problematisch: Netze liefern keine Garantie für Zeitabläufe, zu riskant.

Andere, am häufigsten angewandte Möglichkeiten (oft auch in Kombination):

- Zeichenzählung (Längenfeld im Header)
- Anfangs- und Endezeichen (mit Zeichenstopfen)
- Anfangs- und Endflags (mit Bitstopfen)
- Verstöße gegen Kodierregel der Bitübertragungsschicht (sog. illegale Signalübergänge).

Rahmenabgrenzung (Synchronisation zwischen Sender und Empfänger)

1. *Zeichenzählung*
   Einfügen eines Längenfeldes im Header des Rahmens (Anzahl der Zeichen).
   Problem: bei Veränderung des Zeichenzählfeldes während der Übertragung kann Empfänger den Anfang des nächsten Rahmens nicht erkennen ~> keine Synchronisation; heute weniger angewandt.

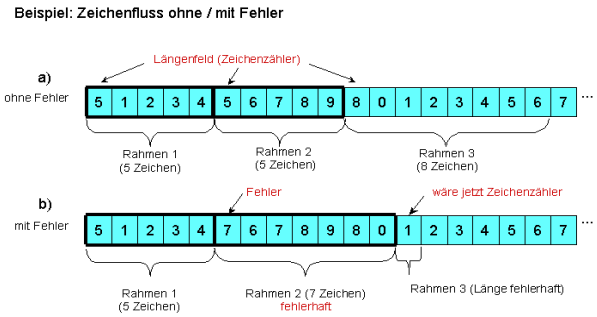


Abbildung 4.2: Rahmenabgrenzung durch Zeichenzählung

2. *Anfangs- und Endezeichen (mit Zeichenstopfen, character stuffing)*
   Synchronisation durch ASCII - Zeichenfolgen
   Rahmenanfang: DLE STX (hex 10 02) mit: DLE: Data Link Escape, STX: Start of Text
   Rahmenende: DLE ETX (hex 10 03) mit: ETX: End of Text
   Empfänger braucht zur Synchronisation nur nach dieser Zeichenfolge zu suchen.

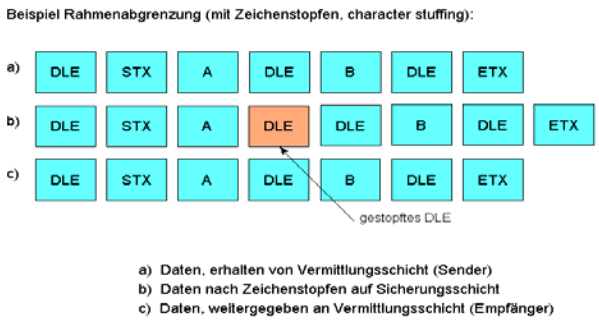


Abbildung 4.3: Rahmenabgrenzung durch Anfangs- und Endezeichen

Problem: Bei der Übertragung von Binärdaten kann die Zeichenfolge DLE STX oder DLE ETX auch als Daten enthalten sein ~> Synchronisationsproblem beim Empfänger.
Abhilfe: Sende-DLL fügt vor einem DLE noch ein zweites DLE ein (sog. *Zeichenstopfen, character stuffing*). Empfänger-DLL entfernt das 2. DLE vor Weiterleitung an ihre Vermittlungsschicht
Nachteile: enge Anbindung an 8-Bit-Zeichen und ASCII-Zeichensatz für Rechnernetz nicht vorteilhaft ~> Ziel: beliebige Anzahl Bits/Zeichen.

3. *Anfangs- und Endflags (mit Bitstopfen, Bit stuffing)*
Rahmenanfang und -ende: durch bestimmtes Bitmuster (Flag) gekennzeichnet (z.B. SDLC: 01111110 hex 7E). Bei Binärdaten ist auch diese Bitfolge in den „Nutzdaten" zu übertragen.
Lösung: Entdeckt Sender 5 aufeinanderfolgende "1", stopft er automatisch eine "0" hinzu. Der Empfänger nimmt entsprechend die "0" heraus, sobald er 5 aufeinanderfolgende "1" mit einer folgenden "0" erhält.

a) . . . . 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0 . . .
b) . . . . 0 1 1 0 1 1 1 1 1 **0** 1 1 1 1 1 **0** 1 1 1 1 1 **0** 1 0 0 1 0 . . .
c) . . . . 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0 . . .

a) Originaldaten
b) Übertragene Daten (mit gestopften Bits 0)
c) Daten beim Empfänger zur Weiterleitung an Vermittlungsschicht

4. *Verstöße gegen die Kodierregel*
- Anwendungen in Netzen bei Kodierung im physikalischen Medium mit Redundanz. Vorteil: kein Stopfen erforderlich; sie ist Teil der IEEE 802-Norm für LAN.
- Rahmenbegrenzung durch unzulässige Folgen von Signalübergängen.

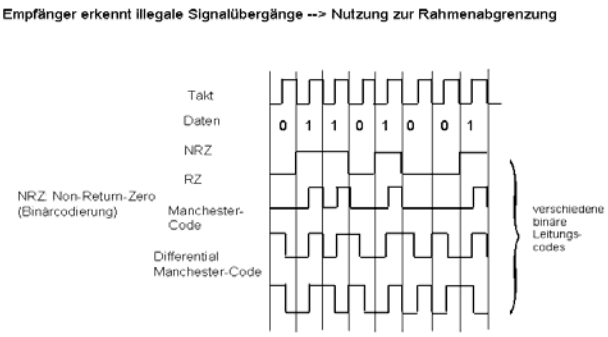


Abbildung 4.4: Rahmenabgrenzung durch Kodierregelverstoss

4.1.3 Fehlerüberwachung und Flusssteuerung

Fehlerüberwachung
Aufgaben:
- Sicherung, dass Rahmen fehlerfrei übertragen und wirklich an Vermittlungsschicht übertragen werden,
- Einhaltung der Reihenfolge.

Lösung:
- durch positive / negative Bestätigung (ACK, NAK),
- Timer-Kontrollen (falls Bestätigungen ausbleiben bzw. nicht möglich sind),
- Einführung von Folgenummern.

Flusssteuerung
Problem: Empfänger langsamer als Sender
Lösung:
- Flusssteuerung (flow control)
- Drosselmechanismus (erfordert Rückmeldeinformationen), Ratenkontrolle.

Realisierung über Protokolle: Protokoll definiert, wann ein Sender den nächsten Rahmen absenden darf (ansonsten ausdrücklich verboten).

4.2 Fehlererkennung und –korrektur

4.2.1 Fehler

Gründe:
- Thermisches Rauschen) gestörter Übertragungskanal,
- Impulse)
- Frequenzabhängige Übertragung,
- Nebensprechen,
- Echos (falls Echosperren in Telefonsystem abgeschaltet sind),
- Fading bei Mikrowellen (phasenverschoben eintreffende Mikrowellen),
- Synchronisierung bei PCM, ...

Häufigkeit:
- analoge Systeme (Ortsvermittlung): häufig
- digital: selten
- drahtlos: häufige Fehler

Fehlerbehandlung:
- Fehlererkennung, Fehlerbehebung (Fehlerkorrektur)
- In einigen Medien treten Fehler massenweise (gebündelt) auf --> Bündelfehler schwieriger erkenn- und korrigierbar.

Verfahren zur Fehlerbehebung
Mitsenden von redundanten Informationen (2 Grundstrategien):
- Fehlerkorrektur-Codes (genug redundante Informationen)
- Fehlererkennungs-Codes (wenig redundante Informationen)

4.2.2 Fehlerkorrekturcodes

Bei Fehlerkorrekturcodes werden genügend redundante Informationen mitgesendet, so dass Empfänger den Fehler erkennt und korrigiert (erkennt, wie Zeichen im Urzustand aussehen müsste):
- Prüfsummenbildung
- Bestimmung Hammingabstand
- Mitsenden Paritätsbit

Was ist ein Fehler ?

Rahmen (Nachricht): m Datenbits
Redundanz: r Prüfbits
n-Bit - Codewort: n = m + r

Vergleicht man 2 Codewörter (Exclusives OR), so kann man zählen, wie oft ein 1-Bit im Ergebnis vorkommt. Die Anzahl der Bitpositionen, in denen sich 2 Codewörter unterscheiden, wird als *Hamming-Abstand d* (Hamming, 1950) bezeichnet. Mittels Hamming-Codes lassen sich Fehler erkennen und korrigieren:

- Einzelfehler
- Fehlerbündel (mit Tricks)

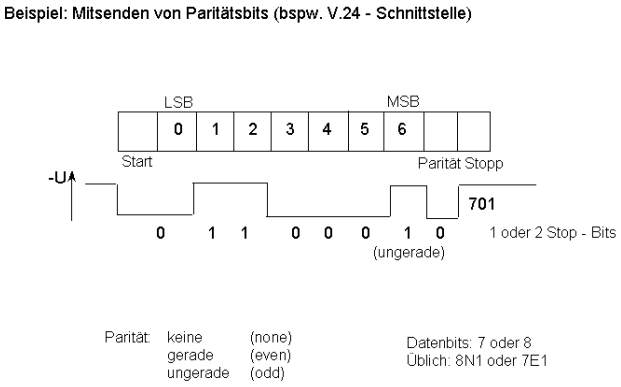


Abbildung 4.5: Paritätsbit

4.2.3 Fehlererkennungscodes

Polynomcode

Es werden nur soviele redundante Informationen mitgesendet, dass Empfänger zwar das Auftreten eines Fehlers erkennt, nicht aber seine Art. Behebung nur durch Aufforderung zur nochmaligen Übertragung.

Fehlererkennung und nochmalige Sendewiederholung ist bei Rechnernetzen i.allg. effizienter als Fehlerkorrektur. Bei Übertragung isochroner Medien (audio/video) und Echtzeitkommunikation ist Fehlerkorrektur erforderlich (z.B. FEC Forward Error Correction bei Mobilfunknetzen).

Praktisch angewandtes Verfahren: **Polynomcode**, auch zyklischer Redundanzcode oder **CRC (Cyclic Redundancy Code)** genannt.

Er basiert darauf, dass man Bitketten als Polynome mit den Ketten 0 und 1 behandelt. Polynomberechnungen erfolgen nach Regeln der algebraischen Feldtheorie Modulo 2. Dazu müssen sich Sender und Empfänger vor Übertragung auf ein Generatorpolynom G(x) einigen (werthöchstes und wertniedrigstes Generatorbit muss 1 sein).

$G(x) = x^{k-1} + ... x^{k-n} + ... x^0$ (Grad k)

International genormte Polynome

CRC - 12	$x^{12} + x^{11} + x^3 + x^2 + x^1 + 1$	für Zeichenlänge 6 bit
CRC - 16	$x^{16} + x^{15} + x^2 + 1$	für Zeichenlänge 8 bit
CRC - CCITT	$x^{16} + x^{12} + x^5 + 1$	für Zeichenlänge 8 bit

Fehlererkennung durch Prüfsummenbildungen. Hardwaremäßige Realisierung mit einfachen Schieberegistern (Peterson, Brown, 1961) -> fast immer eingesetzt.

4.3 Wichtige Protokolltypen der Sicherungsschicht

4.3.1 Aufgabenstellung

Rahmenaufbau

Die DLL erhält Daten (Paket) von der Vermittlungsschicht. Dieses Paket erhält einen Header (Steuerinformationen). Paket und Header werden in Rahmen (Frame) der DLL eingeschlossen und so der Sicherungsschicht übergeben, die dann für die Bitübertragungschicht bereitgestellt werden (analog umgekehrt).

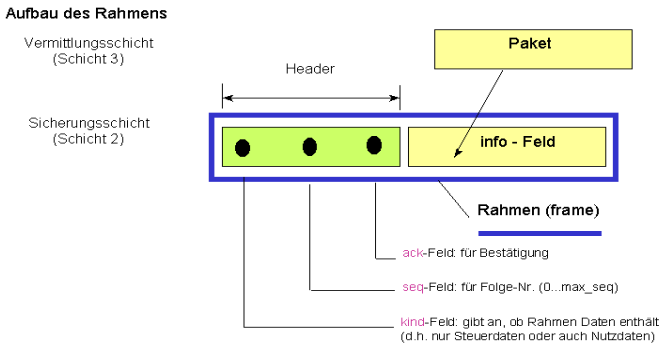


Abbildung 4.6:Rahmenaufbau (DLL-Schicht)

Richtung der Datenübertragung

- Simplex-Übertragung: nur 1 Richtung, 2-Drahtleitung
- Halbduplex-Übertragung: wechselseitig (abwechselnd), auf gleicher Leitung, 2-Draht
- Duplex-Übertragung: in beiden Richtungen, 4-Drahtleitung
  Vorwärtskanal: Daten; Rückkanal: Statusmeldungen

Realisierung über entsprechende Protokolle:

Simplex-Protokolle (u.a. Stop-and-Wait),
Duplex-Protokolle (variable Fenstergrößen, Sliding-Windows)

4.3.2 Simplex-Protokolle

Uneingeschränktes Simplex-Protokoll

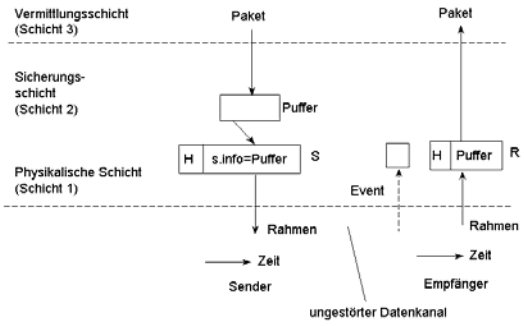


Abbildung 4.7: Uneingeschränktes Simplex-Protokoll

Daten nur in 1 Richtung übertragen, Sender und Empfänger jederzeit bereit. Puffer unendlich groß, Datenübertragungskanal ungestört. Allerdings obige Vorgaben unrealistisch.
Nachteile: keine Synchronisation zwischen Sender und Empfänger, keine Fehlererkennung.

Simplex-Protokoll mit Stop-and-Wait
Annahme: Empfangene Seite ist *nicht immer empfangsbereit* bzw. endliche Puffergröße; Datenübertragungskanal sei weiterhin ungestört.
Der Sender ist deshalb davon abzuhalten, den Empfänger schneller mit Daten zu beliefern als dieser Verarbeiten kann. Eine Lösung ergibt sich nur dann, wenn Empfänger eine *Bestätigung an den Sender* zurückgibt. Nach Weitergabe des Paketes an Schicht 3 schickt Empfänger einen kleinen Leer-Rahmen an Sender (mit Erlaubnis zum Senden des nächsten Rahmens). Im Sendeprotokoll ist deshalb eine Wartezeit für den Empfang des Leer-Rahmens vorgesehen. Protokolle, bei denen Sender auf Bestätigung wartet, nennt man Stop-and-Wait-Protokolle.

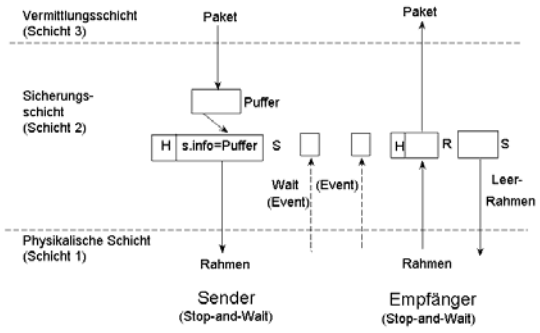


Abbildung 4.8: Simplex-Protokoll mit Stop-and Wait

Simplex-Protokoll für gestörte (rauschende) Kanäle
Es können Rahmen verlustig gehen oder gestört sein, HW soll Übertragungsfehler erkennen.
Lösung:
1. Timer (Setzen Time-Out für Wiederholungen): Empfänger eines Rahmens sendet Bestätigung nur dann, wenn Daten korrekt angekommen sind; ansonsten werden die Daten verworfen. Sender wiederholt die Übertragung nach Ablauf eines Time-Out.
2. Folge - Nr.: Timer allein nicht ausreichend (Duplikate möglich). Mittels einer Folge-Nr. im Header jedes gesendeten Rahmens kann Empfänger prüfen, ob es sich um einen neuen Rahmen oder um ein Duplikat handelt.

Protokolle, bei denen Sender auf positive Bestätigung wartet:
- PAR - Protokolle (Positive Acknowledgement with Retransmission)
- ARQ - Protokolle (Automatic Repeat reQuest)

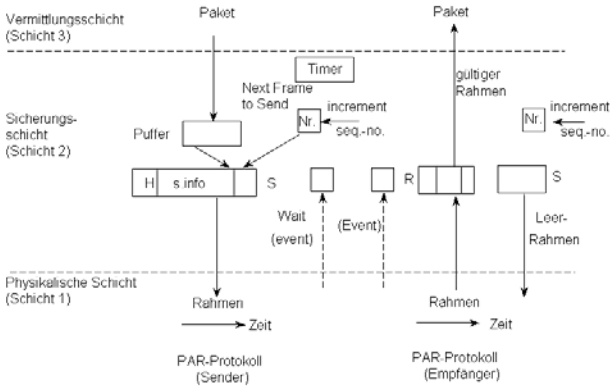


Abbildung 4.9: Simplex-Protokoll für gestörte (rauschende) Kanäle

4.3.3 Protokolle mit variablen Fenstergrößen

Duplexübertragung
In der Praxis wird Datenübertragung in beiden Richtungen benötigt (Duplex):
Vollduplex: Vorwärtskanal (Daten), Rückwärtskanal (Steuerinformationen), 2 Kanäle separat
Halbduplex: Überlappung von Daten und Steuerinformationen auf gleicher Leitung erbringt bessere Ausnutzung gegenüber Vollduplex.
Weitere Verbesserung: **Huckepacktransport** (Piggy packing)

- Gleichzeitige Datenübertragung von A --> B und B --> A. Rahmen enthalten ack-Feld (genutzt für Bestätigungsmeldung).
- Wenn A einen Rahmen nach B sendet, so verzögert B die Rücksendung des leeren Prüfrahmens. Die Bestätigung wird an den Rahmen der Sendung von B nach A angehängt (im Feld ack des Headers). Somit wird Bestätigung als Freifahrt auf dem nächsten Datenrahmen mitgesendet. Nur wenn B nichts selbst sendet, wird eine Empfangsbestätigung als Steuerrahmen an A gesendet.
- Vorteil: bessere Kanalauslastung.

Sliding-Window-Protokolle
(Schiebefensterprotokolle bzw. Protokolle mit variabler Fenstergrößen)
Es ist eine weitere Gruppe von Protokollen, die sehr *robust* sind und unter schlechten Bedingungen funktionieren.
Bei allen Schiebefensterprotokollen enthält jeder zu sendende Rahmen eine Folge-Nr.: 0 bis zu einem beliebigen Maximum (im allg. $2^n - 1$ für ein n-Bit-Feld). *Hauptmerkmal*
Sender führt Liste von Folge-Nr.'n, die die Anzahl schickbarer Rahmen enthält. Diese Rahmen passen genau in das sog. Sendefenster. Analog enthält der Empfänger ein Empfangsfenster mit Anzahl der annehmbaren Rahmen. Die Fenster enthalten Ober- und Untergrenzen.
Falls von Schicht 3 ein neues Paket eintrifft, erhält es die nächst höhere Folge-Nr. und die Fensterobergrenze wird um eins verschoben. Falls eine Bestätigung eintrifft, wird auch die Untergrenze um eins weitergerückt. Jeder Rahmen, der nicht im Fenster aufgenommen wird, wird kommentarlos zerstört.

Spezielle Schiebefensterprotokolle

- Schiebefensterprotokolle mit n = 1 (1 Bit): arbeitet nach **Stop-and-Wait**
- Protokolle mit „Gehe n zurück" **(go back n):** Sender darf bis zu W Rahmen abschicken (anstatt nur 1), bevor er blockiert wird. W ist sinnvoll zu wählen, ohne dass das Fenster gefüllt wird. Diese Technik nennt man auch Pipelining.

Pipelining kann große Probleme bei gestörtem Übertragungskanal erbringen, z.B.:

- Rahmenverlust,
- was soll Empfänger mit den vorhergehenden bzw. nachfolgenden Rahmen anfangen.

Zwei Ansätze für Fehlerbehandlung bei Pipelining:

1. „gehe n zurück" (go back n):
   Empfänger verwirft bei Fehler alle nachfolgenden Rahmen und schickt keine Bestätigungen. Strategie entspricht dem Empfangsfenster der Größe 1.
   Nach Ablauf des Sende -Timers sendet Sender alle unbestätigten Rahmen nochmals, beginnend mit dem fehlerhaften Rahmen. Hoher Bandbreitenverlust.
2. Selektive Wiederhohlung (Selective Repeat):
   Hierbei speichert die empfangende Sicherungsschicht alle korrekte Rahmen, die auf den fehlerhaften folgten. Wenn Sender merkt, dass etwas nicht o.k., so schickt er nur den fehlerhaften Rahmen (und nicht auch die nachfolgenden neu). Strategie entspricht Empfangsfenster der Größe > 1.

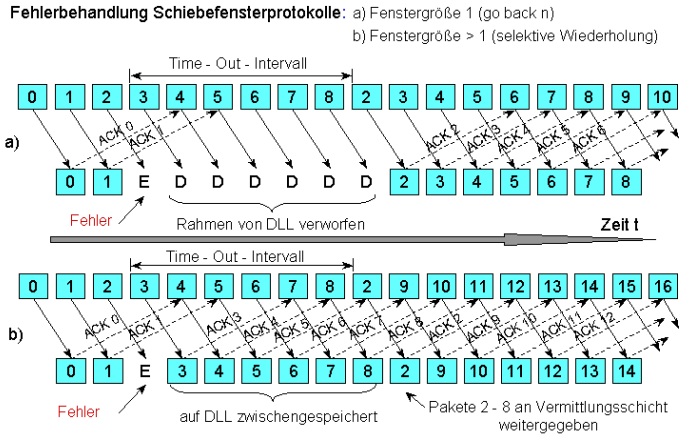


Abbildung 4.10: Fehlerbehandlung bei Schiebefensterprotokollen

4.4 Protokollbeispiele der Sicherungsschicht

Punkt-zu-Punkt - Übertragung (store-and-forward) --> WAN
HDLC, SDLC
SLIP, PPP (Internet)
TC - Teilschicht von ATM
Rundsendekanäle (Broadcast, Shared Media) --> LAN, MAN
Gemeinsames Übertragungsmedium
Dazu speziell die Sicherungsschicht (DLL) in 2 Subschichten unterteilt:
2a - MAC: Medium Access Control
2b - LLC: Logical Link Control (insbes. für Umsetzung in kompatible Rahmenformate).

HDLC – High-Level Data Link Control
Synchrones Übertragungsprotokoll der Schicht 2, abgeleitet von SDLC / IBM
Protokollentwicklung:

Protokoll		Institutionen
SDLC	(Synchronous Data Link Control)	IBM/SNA (System Network Architecture)
ADCCP	(Advanced Data Communication Control Procedure)	ANSI (modifiziertes SDLC)
HDLC	(High-Level Data Link Control)	ISO / CCITT
LAP	(Link Access Procedure)	CCITT (Übernahme HDLC als Teil der X.25-Norm)
LAP B	(Link Access Procedure, Vers. B)	CCITT (abgeändertes LAP für Kompatibilität zu späteren HDLC-Versionen)

Alle genannten Protokolle arbeiten auf gleichem Prinzip;
- bitorientiert,
- Anwendung Bitstopfverfahren für Datentransparenz,
- nur geringe Unterscheidungen.

Rahmenformat bitorientierter Protokolle

Bits	8	8	8	0	16	8
	01111110	Adresse	Steuerung	Daten	Prüfsumme	01111110

Legende:	Feld Steuerung:	u.a. für Folge - Nr, Bestätigungen
	Feld Daten:	beliebige Informationen
	Feld Prüfsumme:	für zyklische Redundanzcode-Anwendung (CRC-CCITT-Generatorpolynom)
	Begrenzende Flags:	01111110

Internet-Protokolle der Sicherungsschicht

Internet:

Vorwiegend Punkt-zu-Punkt-Netze, aber auch LAN - LAN möglich. Einwahl über entsprechende Router eines Internet-Providers (DFN, XLINK, Online, AOL, CompuServ, ...)

Zur Verbindung

HOST (im allg. PC, WS) und Router (Wählleitung) bzw.
Router - Router (Mietleitung)

stellt das Internet 2 Protokolle bereit, die am häufigsten benutzt werden:

SLIP: Serial Line Internet Protocol (älteres Protokoll),
PPP: Point-to-Point-Protocol (von IETF standardisiert).

Viele Internet-Provider unterstützen SLIP und PPP. Zukunft liegt bei PPP (sowohl für Wähl- als auch für Mietleitungen).

SLIP – Serial Line IP

Es ist das ältere der beiden Protokolle; häufig angewandt, aber problematisch. Entwicklung: *Rick Adams*, 1984 (RFC 1055). Damit HOST über Wählleitung und Modem an Internet anschließbar.

SLIP ist ein einfaches Punkt-zu-Punkt – Rahmenprotokoll. Unbestätigter Dienst (Steuerung über höhere Schichten). Ethernet- oder Tokenring- Rahmen werden in HDLC-Rahmen durch Sonderzeichen unter Benutzung von Zeichenstopfen verpackt

0X EB = Start Übertragung
0X C0 = Ende Übertragung

SLIP auch für Übertragung von TCP/IP - Paketen geeignet. Neuere SLIP-Versionen (RFC 1144) unterstützen TCP- und IP-Kompressionen

Nachteile SLIP:

- Keine Fehlererkennung und Fehlerkorrektur (--> höhere Schichten).
- Unterstützt nur IP (Probleme für Novell - LAN's).
- Jede Seite muss die IP-Adresse kennen (keine dynamische Zuweisung bei Verbindungsaufbau).
- Keine Authentifikations-Versionen (Teilnehmer weiß nicht, mit wem er korrespondiert).
- Kein zugelassener Internet-Standard.

PPP – Point-to-Point-Protocol

Entwicklung durch IETF: Reihe von Protokollen der Internet-Sicherungsschicht: RFC 1661 (und RFC 1662, 1663).

PPP unterstützt

- Fehlererkennung
- mehrere Protokolle, u.a. TCP/IP (Internet), IPX/SPX (Netware), ...
- Dynamische Vergabe von IP-Adressen (zum Zeitpunkt des Verbindungsaufbaus)
- Authentifikation usw.

Merkmale von PPP

- Rahmenerstellung: Kennzeichnung Ende des Rahmens und Anfang des nächsten (mit Fehlererkennung).
- Verbindungssteuerungsprotokoll LCP (Link Control Protocol): Zum Anschalten und Testen von Leitungen, Optionsverhandlung, Verbindungsabbau.
- Möglichkeit zur Aushandlung von Optionen, die unabhängig vom benutzten Vermitt-

lungsschicht-Protokoll sind. Vorgesehen ist, dass auf jeder unterstützten Vermittlungsschicht ein anderes NCP (Network Control Protocol) läuft (vorhanden für TCP/IP, IPX - andere in Vorbereitung).

Verbindungsaufbau über PPP:
PC ruft über Modem den Service-Provider an. Dabei physische Verbindung aufgebaut. Dann sendet PC mehrere LCP-Pakete im Nutzerdatenfeld vom PPP-Rahmen. Danach werden mehrere NCP-Pakete versendet, um die Vermittlungsschicht zu konfigurieren, insbes. zur Nutzung von TCP/IP --> dazu IP-Adresse erforderlich.
Funktion von NCP:
Beispielsweise kann NCP für das IP genutzt werden, um IP-Adressen zuzuweisen (da es nicht genügend IP-Adressen gibt, können diese dynamisch für jeden neu beim Provider angeschlossenen PC für die Dauer der Sitzung zugewiesen werden). Jeder Internet-Provider erhält einen Block von Adressen. Nach Sitzungsende wird über NCP die Verbindung zur Vermittlungsschicht abgebaut und IP-Adressen freigegeben. Dann wird das LCP benutzt, um die Verbindung auf Sicherungsschicht zu beenden. Anschließend wird das Modem angewiesen, Verbindung zur Bitübertragungsschicht abzubauen.
PPP-Rahmenformat
PPP ähnlich HDLC (Pkt-zu-Pkt), aber zeichenorientiert (HDLC bitorientiert). PPP und SLIP nutzen Zeichenstopfungsverfahren bei Wählleitung über Modems (je Rahmen ganzzahlige Byteanzahl - im Gegensatz zu HDLC). Somit können PPP-Rahmen nicht nur über Wählleitungen des Telefonnetzes, sondern auch über SONET, SDH oder echte bitorientierte HDLC-Leitungen (z.B. Router/Router-Verbindungen) gesendet werden. Dazu wird PPP in HDLC-Rahmen enkapsuliert.
PPP bietet protokollübergreifenden Mechanismus für

- Einsatz mit Modems (Telefon, Wählleitungen).
- Bitorientierte HDLC-Leitungen.
- SONET und andere DLL-Schichten.
- Unterstützung von Fehlererkennung, Optionsverhandlungen, Headerkompression und wahlweise eine zuverlässige Übertragung mit Hilfe der HDLC-Rahmenerstellung.

ATM-Sicherungsschicht
Funktionalität der Sicherungsschicht in *TC-Teilschicht (Transmission Control)*. ATM-Zellen (5 Byte Header, 48 Byte Payload) werden auf Basis SONET, SDH, PDH, FDDI und anderer Träger übertragen. ATM hat keine Flusssteuerung.
Senden: TC-Teilschicht erzeugt für den Header das **HEC-Feld** (Header Error Control, 1 Byte, Prüfsummenbildung).
Damit Zelle für Übertragung fertig: sie wird in den Bitstrom des physikalischen Übertragungssystems eingepasst.
Empfangen: Ermittlung Zellengrenzen des eingehenden Bitstroms (Verwendung HEC).

Sub-Schichten in LAN
Bei LAN / MAN Schicht 2 in 2 Subschichten aufgeteilt
MAC: Medium Access Control - Zugriffsverfahren, wie
Ethernet, Token-Ring, ...
FDDI, DQDB, ...
Fast-Ethernet, Gigabit-Ethernet, VG-Any-LAN, ...
HiPPi, HyperChannel, Segment Switching, ...
LLC: Logical Link Control - Restliche Funktionen der Schicht 2 (insbesondere Umsetzung in kompatible Rahmenformate).

5 Medienzugriffsverfahren (Media Access Control)

5.1 Sub-Schichten der Data Link Layer

Problemstellung
Netze können in 2 Kategorien unterteilt werden:
- **Punkt-zu-Punkt-Netze** (store-and-forward):
  i.allg. Paketvermittlung, vorwiegend bei WAN.
- **Broadcast-Netze** (Rundsende-Netze, Shared Media)
  Gemeinsamer Übertragungskanal -> Problem bei gleichzeitiger Benutzung; vorwiegend bei LAN, MAN, Satellitennetze.
  Lösung: Mehrfachzugriffsprotokolle (Multi Access oder Random Access Protocols);
  Anordnung in einer spezifischen Teilschicht der Schicht 2: MAC.

Subschichten der Sicherungsschicht (DLL, Schicht 2)
- MAC (Medium Access Control)
  Medienzugriffsverfahren
- LLC (Logical Link Control)
  insbes. zum Abgleichen der
  unterschiedlichen Rahmenformate

3	Vermittlung	
2b	LLC	Sicherung
2a	MAC	
1	Bitübertragung	

Mediumzugriffs-Teilschicht (MAC)
Rundsenden erbringt
* Kanäle mit Vielfachzugriff
* Kanäle mit wahlfreiem Zugriff (stochastisch vs. deterministisch)

Problem: Aufteilung des gemeinsamen Übertragungskanals auf mehrere Benutzer .

Untergliederung der Zugriffsmethoden auf gemeinsamen Übertragungskanal
nach Topologie

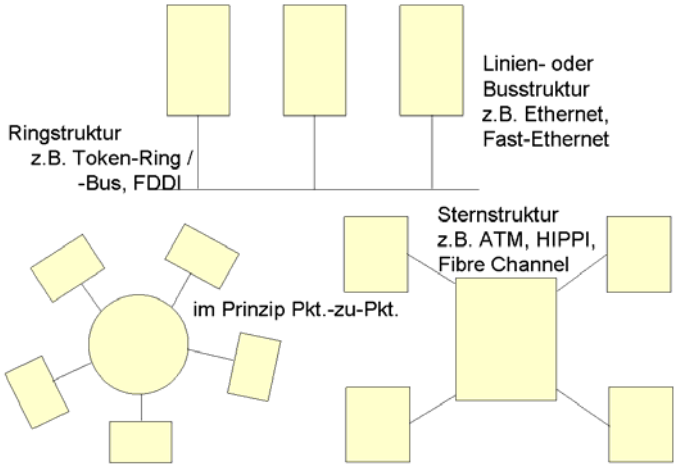


Abbildung 5.1: Topologische Strukturen LAN (Shared Media)

nach Zeitverhalten

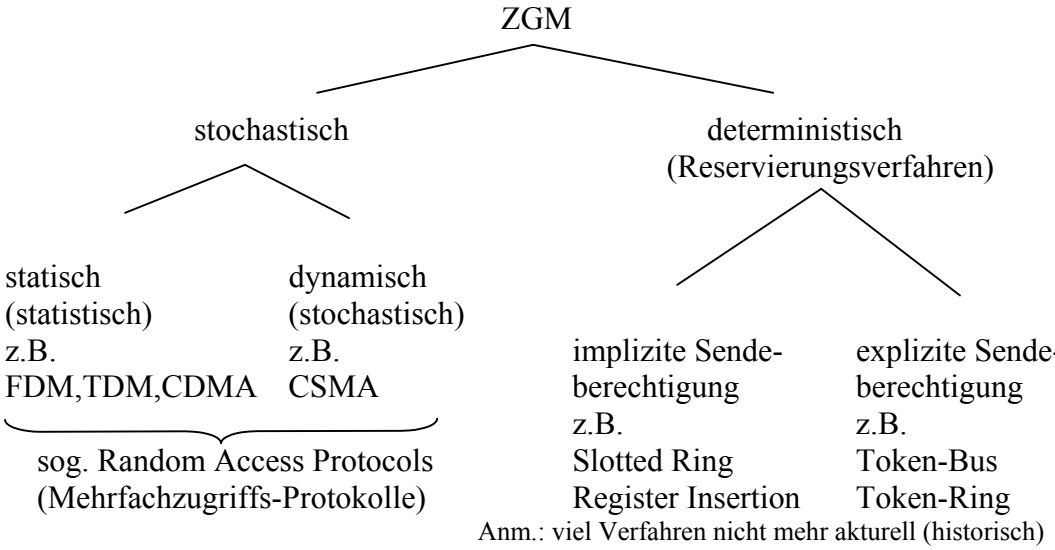


Abbildung 5.2: Shared-Media-Zugriffsmethoden (Zeitverhalten)

5.2 Kanalzuordnung bei MAC

Kanalzuordnungsprinzipien
Aufgabe: Einzelner Broadcast-Kanal ist mehreren Benutzern gleichzeitig zur Verfügung zu stellen (Shared Media).

Statische Kanalzuordnung in LAN und MAN ~> Multiplexing **FDMA, TDMA, CDMA**
a) Frequenzmultiplexverfahren (FDMA: Frequency Division Multiple Access)
Klassischer Weg, um einen Kanal auf mehrere Nutzer aufzuteilen: **FDM** Frequenzmultiplexverfahren (FDM - Frequency Division Multiplexing).
Einzelner Kanal (z.B. Telefonleitung): verfügbare Bandbreite wird bei N Nutzern in N gleich große Teile zerlegt und jedem Benutzer ein Teil zugewiesen.
Jeder Benutzer hat sein eigenes Frequenzband => keine Überschneidung.
FDM gut - für konstante Zahl von Nutzern (einfacher und effizienter Algorithmus)
schlecht - falls weniger Nutzer (als bei Aufteilung), wird Bandbreite verschenkt
- falls mehr Nutzer, muss Zugang verweigert werden
- bei Rechnernetzen sehr starke Schwankungen in Last und Anzahl
=> Großteil der Bandbreite ungenutzt.

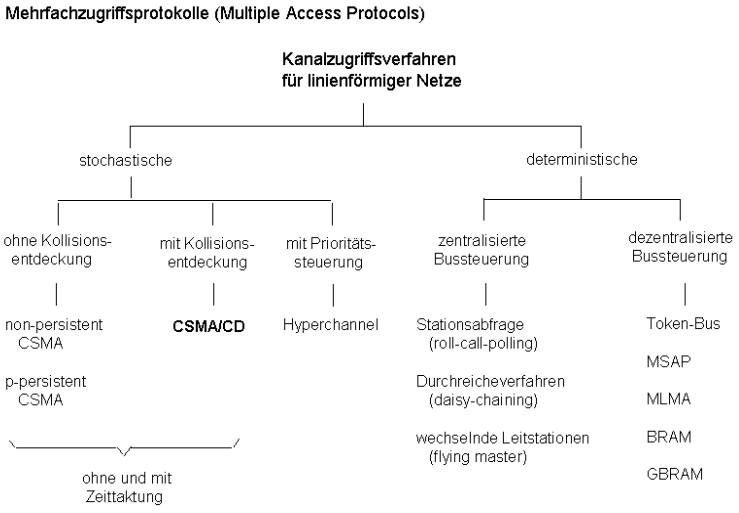
b) Zeitmultiplexverfahren (TDMA: Time Division Multiplex Access):
Gesamter Kanal wird zeitlich aufgeteilt (Zeitschlitz, Slot). Jedem Nutzerpaar wird ein Slot zur exklusiv Nutzung bereit gestellt.
Einschätzung für *synchrones Zeitmultiplexen* (STM-Modus) analog wie bei FDM.
Jeder Nutzer wird immer mit jedem N-tem Zeitschlitz verbunden. Falls Nutzer diesen nicht beansprucht, liegt Kapazität brach ~> STM vs. ATM
Asynchrones Zeitmultiplexen (ATM-Modus): hierbei keine permanente Zuordnung von Zeitschlitz und Nutzer ~> bessere Kanalauslastung.
c) Codemultiplexverfahren (CDMA: Code Division Multiplex Access)
Einsatz unterschiedlicher Codierungen je Übertragungskanal, wobei Sender und Empfänger die für sie gültigen Codes kennen. Verwendung von Spreizcodes.
Trotz Überlagerungen können die Empfänger die Signale herausfiltern (bis zu einer Rauschgrenze). Einsatz: Militärfunk (Abhörsicherheit), vermehrt auch in MFN.

Dynamische Kanalzuordnung in LAN und MAN
Dazu nachfolgende Methoden vorgestellt, die auf folgenden *5 Grundannahmen* beruhen (Anwendung bei Verfahren wie CSMA):

1. *Stationen-Modell:*
   N unabhängige Stationen, die Rahmen erzeugen mit der Wkt. $\lambda * \Delta t$
   λ : Ankunftshäufigkeit ($1/T_A$)
   Δt : Intervall-Länge, in der der Rahmen erzeugt wird
   Ist Rahmen erstellt, bleibt Station blockiert, bis der Rahmen erfolgreich übertragen wurde.
2. *Einzelkanal-Annahme*: Nur 1 Kanal verfügbar
3. *Kollisionen-Annahme*: Wenn 2 Rahmen gleichzeitig übertragen werden, werden die Rahmen entstellt (zerstört) = Kollision. Ein kollidierter Rahmen muss später erneut übertragen werden.
4. *Zeitunterteilung*
   a) nicht unterteilte Zeit (continous time): Übertragung eines Rahmens kann zu jeder Zeit beginnen (kein Haupttakt, der die Zeit in einzelne Intervalle unterteilt).
   b) unterteilte Zeit (slotted time): Zeit in einzelne Intervalle (*Schlitze*) unterteilt. Übertragung eines Rahmens beginnt immer am Anfang eines Schlitzes. Ein Schlitz kann 0, 1, ... , n Rahmen enthalten, was einem untätigen Kanal, einer erfolgreichen Übertragung oder einer Kollision entspricht .
5. *Träger*
   a) Trägererkennung (Carrier Sense): Stationen können erkennen, ob Kanal in Gebrauch ist. Falls Kanal als besetzt erkannt wird, wird kein Sendeversuch gestartet.
   b) keine Trägererkennung (No Carrier Sense):
   Stationen können Kanal vor Benutzung nicht überprüfen (z.B. Satelliten, WLAN).
   Erst anschließend feststellbar, ob Übertragung erfolgreich war oder ist.

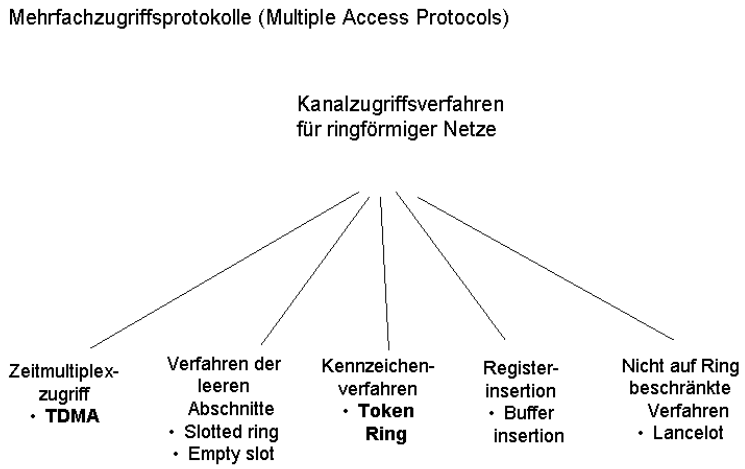
5.3 Mehrfachzugriffsprotokolle

5.3.1 Einteilung



Anm.: Verfahren z.T. nicht mehr aktuell (historisch)

Abbildung 5.3: Kanalzugriffsverfahren für linienförmige Netze



Anm.: Verfahren z.T. nicht mehr aktuell (historisch)

Abbildung 5.4: Kanalzugriffsverfahren für ringförmige Netze

5.3.2 ALOHA-Protokolle

ALOHA - Protokolle
Norman Abramson, Universität Hawaií (1970)
Eigentlich für bodengestützten Rundfunk entwickelt, aber Grundidee allgemein nutzbar, wenn unkoordinierte Benutzer um einen einzelnen Kanal konkurrieren.
2 Versionen
- reines ALOHA keine globale Zeitsynchronisation
- unterteiltes ALOHA Zeit in Schlitze aufgeteilt, in die alle Rahmen passen müssen

Reines ALOHA
Abramson, 1970; für Satellitenkommunikation und terrestrische Funkübertragung. Jeder Benutzer kann zu willkürlichen Zeiten senden. Es treten Kollisionen auf, die kollidierten Rahmen werden zerstört. Sender hört Kanal ab und ermittelt, ob sein Rahmen zerstört wurde (bei LAN erfolgt Bestätigung unmittelbar, bei Satelliten um ca. 270 ms verzögert). Nach Warten einer zufälligen Zeit erneutes Senden (zufällige Wartezeit, sonst kollidieren immer die gleichen Rahmen). Alle Rahmen haben gleiche Länge, um Durchsatz zu maximieren.

Unterteiltes ALOHA (slotted ALOHA)
Roberts, 1972; auch für Satellitenkommunikation und terrestrische Funkübertragung. Methode zur Verdopplung der Kapazität. Zeit in Intervalle eingeteilt, wobei jedes Intervall einem Rahmen entspricht. Somit Synchronisation zwischen Benutzern möglich.
Bei slotted ALOHA darf nicht sofort gesendet werden, sobald ein Zeilenrücklauf (Sendeauftrag) eingegeben wurde. Es muss auf den nächsten Zeitschlitz gewartet werden. Dadurch wird gefährliche Zeitspanne für Kollision um die Hälfte gekürzt.

5.3.3 Mehrfachzugriffsprotokolle (CSMA, WDMA, MACA)

CSMA - Protokolle (CSMA: Carrier Sense Multiple Access)
Kanalauslastung bei ALOHA: $\eta_{max} = 1/e$
Kanalauslastung bei LAN: Verbesserung durch entsprechende Protokolle.
Trägererkennungsprotokolle (Carrier Sense Protocols):

Stationen können Träger (Carrier) abhören. Dazu verschiedene Versionen, geeignet für terrestrische Funkübertragung und leitungsgebundene Übertragung (im Gegensatz zu ALOHA und WLAN). Anm.:

ALOHA: Ergebnis der Trägererkennung zu spät (>= 270 ms). Kollsion erfolgt beim Empfänger, aber durch CSMA nur bei Sender feststellbar.

WLAN: keine Kollisionserkennung identifizierbar, da mehrere Signale im Sendebereich möglic (Abhilfe: kurze Rahmen RTS/CTS ~> Kollosionsvermeidung CSMA/CA).

Ständiges (persistent) und ununterbrochenes CSMA

Protokolle:

1-persistent - CSMA:

Station hört Kanal ab. Wenn frei, kann sie senden - sonst warten ("1 - persistent", weil Station mit Wkt. 1 sendet, wenn ein Kanal frei). Bei Kollision warten zufällige Zeit bis erneutes Senden ~> besser als reines ALOHA und unterteiltes ALOHA (dort willkürliches Senden).

Non-persistent - CSMA:

Vor Senden wird Kanal überprüft. Falls frei, Sendebeginn. Falls belegt, wird nicht ständig (non-persistent) die Kanalbelegung geprüft (Sendevorgang nach zufälliger Spanne wiederholt) ~> Bessere Kanalauslastung und längere Wartezeiten als 1-Persistent-CSMA.

p-persistent - CSMA: (persistent := dauerhaft, ständig)

Gehört zu den getakteten Kanälen. Vor Senden Kanal geprüft. Falls frei, sendet Station mit Wkt. p: mit Wkt 1-p wartet sie auf nächsten Zeitschlitz (senden bzw. warten); Vorgang wiederholt, bis Rahmen übertragen. Bei Kollision erneuter Versuch nach zufälliger Zeitspanne.

CSMA mit Kollisionserkennung (CSMA/CD)

CSMA: Verbesserung gegenüber ALOHA, da keine Station sendet, wenn Kanal als belegt erkannt. Verbesserung dadurch noch, wenn Übertragung abgebrochen wird, sobald eine Kollision erkannt wird (nicht erst Rahmenübertragung beenden; Rahmen wird ohnehin zerstört).
Anm.: Übertragung wurde begonnen, da 2 Stationen den Kanal als frei erkannten aber dann Kollision

=> Protokoll: **CSMA/CD (Carrier Sense Multiple Access with Collision Detection).**

Einsatz in LAN's (MAC-Teilschicht), z.B. Ethernet (IEEE 802.3). Alle CSMA-Protokolle sind unzuverlässig und wegen Kollisionen nicht für Multimedia geeignet.

CSMA/CD kann sich in *3 Zuständen* befinden: frei (Leerlauf), Übertragung, Konkurrenz (in dieser Phase sind Kollisionen möglich).
Falls eine Station einen freien Kanal erkennt, beginnt sie mit Übertragung. Bei Erkennen der Kollision wird Übertragung abgebrochen und nach zufälliger Zeit wird die Sendung wiederholt (unter Annahme, dass keine andere Station begonnen hat). Somit besteht das Modell aus Konkurrenz- und Übertragungsperioden und Leerlauf, falls keine Station sendet.

CSMA/CD - Konkurrenzintervall

Problem: Bestimmung der Zeit, um eine Kollision zu erkennen. Länge der Konkurrenzperiode ist wichtig für die Abschätzung von Verzögerungen und Datendurchsatz. Minimale Zeit zur Kollisionsentdeckung ist die Zeit, die ein Signal benötigt, um von einer Station zur nächsten zu gelangen.
Größe des Konkurrenzintervalls (ALOHA-Modell): Beispiel
Verzögerungszeit für Signal von S1 nach S2 (1 km) sei $\tau = 5$ ms (10 Mbit/s). Kurz vor Ankunft des Signals an entferntesten Station 2 (Zeit t - ε) beginnt Station 2 zu senden --> Kolli-

sion, Entdeckung an Station 2, Abbruch Übertragung Station 2. Erkennung der Kollision an Station 1 nach Zeit 2τ - ε. Daraus folgt für die Größe des Konkurrenzslots im Beispiel:
(10 Mbit/s - LAN, 2 500 m Entfernung, = 4 Repeater zwischen 2 Stationen):

max. Distanz zwischen 2 Stationen: 2,5 km
Signalausbreitungsgeschwindigkeit: 5 ms/km
min. Zeit für Kollisionsentdeckung: 25 ms (für 2* 2,5 km = 5 km)
4 Repeater zwischen 2 Stationen (lt. IEEE 802.3) ergibt kleinste zulässige Rahmendauer: 51,2 ms. Dies entspricht bei 10 Mbit/s einer Slotlänge 512 Bit = 64 Byte

Technische Realisierung: Ethernet.

Weitere Mehrfachzugriffsprotokolle

Kollisionsfreie Protokolle. Verhinderung Kollision auch in der Konkurrenzphase (bei CSMA/CD hierbei noch Kollisionen möglich). Verfahren:

Bitmustermethode (Basic Bit-Map Method)

Jede Konkurrenzperiode besteht aus genau N Schlitzen, in den jede Station eine 1 (für Senden) einträgt. Somit vereinbart, wer als nächstes senden darf (dadurch keine Kollision). Solche Protokolle als *Reservierungsprotokolle* (*Reservation Protocols*) bezeichnet.

Binäres Countdown (Binary Countdown)

Verwendung binärer Stationsadressen, in denen der Sendewunsch im High-Order-Bit der Adresse vermerkt ist (~> „Ankündigung eines Sendens“). Dadurch Overhead reduziert. Anwendung: Datakit (Fraser, 1987).

Protokolle mit eingeschränkter Konkurrenz

Bisher 2 Grundstrategien zur Kanalakquisition:

Konkurrenzmethode (CSMA): gut geeignet für niedrige Last
Kollisionsfreie Methode: gut geeignet für hohe Last

Nun: Kombination beider, je nach Last. Solche Protokolle nennt man Protokolle mit eingeschränkter Konkurrenz (*Limited Contention Protocols*). Anwendung des sog. Adaptive Tree Walk Protocols, um effektiv den Stationen die Zeitschlitze dynamisch zuzuordnen.

WDMA-Protokolle (Wavelength Division Multiple Access)

Ein anderer Ansatz zur Kanalzuordnung ist Wellenlängenmultiplexing (WDMA)
- die Aufteilung des Kanals in Teilkanäle mittels FDM, TDM oder beiden und
- die dynamische Zuordnung dieser Teilkanäle nach Bedarf.

Vorwiegende Anwendung: LWL-LAN (optische Übertragung) und WAN (SDH/WDM).
Bei WDMA werden jeder Station 2 Kanäle zugeordnet:
- schmaler Kanal: als Steuerkanal (Signalisierung)
- breiter Kanal: für Datenrahmen

Es gibt verschiedene WDMA-Protokolle, mit unterschiedlicher Anzahl von Steuerkanälen, Skalierbarkeit, Durchsatz u.a. (siehe Chen (1994), Levine/Akyildiz (1995) ...).
Wichtige Anwendung WDMA für photonische Netze (SDH/WDM bzw. dark fiber).
Beispiele: G-WiN (SDH / WDM), GÉANT, X-WiN.

Einfache Art eines optischen LANs durch Verwendung eines passiven Sternkopplers: 2 Fasern von jeder Station werden zu einem Glaszylinder verschmolzen. Eine Faser dient für die Ausgabe in den Zylinder, die andere für Eingabe vom Zylinder. Eine Lichtausgabe von einer Station beleuchtet den Zylinder und kann von allen anderen Stationen erkannt werden.
Passive Sterne können Hunderte von Stationen bedienen.
Um mehrere Übertragungen gleichzeitig zu unterstützen, wird das Spektrum in Kanäle (Wellenlängenbänder) aufgeteilt. Beim WDMA-Protokoll werden jeder Station 2 Kanäle zugeordnet. Ein schmaler Kanal dient als Steuerkanal, um die Stationen zu signalisieren; ein breiter Kanal dient den Stationen dazu, die Datenrahmen auszugeben.

Jede Station hat 2 Sender und 2 Empfänger:
1. einen Empfänger mit fester Wellenlänge zum Abhören seines eigenen Steuerkanals.
2. einen einstellbaren Sender zum Senden auf dem Steuerkanal der anderen Station.
3. einen Sender mit fester Wellenlänge zum Ausgeben von Datenrahmen.
4. einen einstellbaren Empfänger zum Auswählen eines abzuhörenden Datensenders.

5.3.4 Drahtlose LAN

Mehrfach-Zugriffsprotokolle für drahtlose LAN
Mobilität: portable Computer über Funksignale (oder Infrarot) verbunden (sog. drahtlose LAN, wireless LAN, W-LAN bzw. WPAN). W-LAN haben andere Eigenschaften als konventionelle LAN's und setzen spezielle Protokolle in der MAC-Subschicht voraus.
Ein naiver Ansatz für ein drahtloses LAN wäre CSMA: Man hört einfach auf andere Übertragungen und sendet nur, wenn kein anderer sendet. Protokoll aber nicht geeignet, weil die Störung am Empfänger, nicht am Sender eine Rolle spielt. Problem:
- Station muss vor Beginn einer Übertragung wissen, ob es beim Empfänger Aktivitäten gibt oder nicht (CSMA teilt lediglich Aktivitäten in unmittelbarer Umgebung der Station mit).
- Da kein Kabel sondern Radiokurzwellen, können mehrere Übertragungen für andere Ziele laufen, sofern diese Ziele nicht innerhalb gegenseitiger Bereiche liegen.

Lösung durch spezifische Protokolle (z.B. MACA, MACAW).

MACA (Multiple Access with Collision Avoidance)
Früheres Protokoll für drahtlose LAN (Karn, 1990). Bildet Grundlage für den IEEE-Standard 802.11 (drahtlose LAN).
Prinzip: Sender regt Empfänger zur Ausgabe eines kurzen Rahmens an, so dass nahe gelegene Stationen diese Übertragung erkennen und für die Dauer des bevorstehenden (großen) Datenrahmens nichts übertragen.
Protokollablauf : A -----> RTS-Rahmen (kurzer Rahmen 30 Byte) B
(Request to Send) enthält Länge des folgenden Rahmens
<---------- CTS-Rahmen (Clear to Send)
Datenlänge aus RTS-Rahmen kopiert
----------> Datenübertragung
Wenn Stationen nicht im "Hör"-Bereich der RTS / CTS - Nachrichten liegen, kann es zu Kollisionen kommen. Bei Kollision nach zufälliger Zeit wird erneut gesendet -> angewandter Algorithmus: *Binäres exponentielles Backoff* (=> siehe IEEE 802.3).

MACAW (Multiple Access with Collision Avoidance for Wireless Networks)
Verbesserung MACA durch Bharghavan u.a. (1994), insbesondere bei verlorenen Rahmen (Reaktion erst auf Ebene der Transportschicht: Lösung durch zusätzliche ACK-Rahmen nach jedem erfolgreichen Datenrahmen) und weitere Maßnahmen. Verbesserte Fairness des Protokolls und erhöhte Systemleistung.

5.3.5 Digitale Zellularfunknetze

Digitale Zellularfunknetze (Cellular Radio Networks)
Digitale Zellfunknetze vordergründig auf Telefonie ausgerichtet (Verlängerung ISDN) --> somit andere Protokolle als in drahtlosen LAN nach IEEE 802.11.
Da die Verbindung Minuten (nicht Millisekunden) dauert, wird hierbei die Kanalzuordnung *pro Verbindung* und nicht pro Rahmen durchgeführt (im Gegensatz zum Datenpaketfunk, wie Modacom bzw. GPRS: hierbei *pro Paket*). Dennoch gelten die gleichen Techniken für den Datenverkehr.
Vorläufer: analoge zellulare Funktelefonsysteme: AMPS (Advanced Mobile Phone System), USA ab 1982, in Deutschland öbl-A (1958), öbl-B (1972), öbl-C (1986).

Standards für digitale Mobilfunksysteme/netze (ETSI, 3GPP / 3GPP2, ...), u.a.
MFN 2G: GSM, DCS, CDPD, D-AMPS, PDC -> MFN 2.5: GPRS
MFN 3G: EDGE, UMTS, CDMA2000
MFN 4G: LTE
Verschiedene Lösungen zur Kanalzuordnung für digitale Funksysteme, u.a.:
Vermittlung: - Leitungsvermittlung („Kanalvermittlung“, LVM), z.B. GSM
- Paketvermittlung (PVM), z.B. GPRS
Multiplextechniken zur gleichzeitigen Übertragung mehrerer Vorgänge:
- SDMA: Raummultiplexing (Space Division Multiple Access)
- FDMA: Frequenzmultiplexing (Frequency Division Multiple Access)
- TDMA: Zeitmultiplexing (Time Division Multiple Access)
- CDMA: Codemultiplexing (Code Division Multiple Access)
- und Kombinationen, u.a. bei

GSM (Global System for Mobile Communications, ETSI): LVM; SDM, FDM, TDM
DCS (Digital Cellular System, ETSI): LVM; SDM, FDM, TDM
CDPD (Cellular Digital Packet Data): PVM; SDM, TDM, FDM
IS-95-CDMA, UMTS, CDMA2000: PVM; SDM, TDM, CDM

GSM: Global System for Mobile Communications
Heutige Zellularfunktelefonie (GSM, DCS) ist digital und kanalvermittelt (MFN 2G). Erweiterung durch paketvermittelten Funk (GPRS, MFN 2.5G).
Vorteile der digitalen gegenüber analogen mobilen Kommunikation:
- Integration von Sprache, Daten und Fax in einem System,
- bessere Sprachkompressionsalgorithmen ~> weniger Bandbreite pro Kanal benötigt,
- Anwendung Fehlerkorrekturcodes (FEC) ~> Verbesserung der Übertragungsqualität,
- digitale Signale können verschlüsselt werden (Datenschutz, Sicherheit),
- höhere Übertragungsleistungen, insbes. für Datenübertragung (Internet-Zugang),
- neue Übertragungskanäle im Frequenzspektrum (z.B. Digital Dividend).

Leistungsdaten (Auswahl):
GSM: 9,6 kbit/s (bzw. 14,4 kbit/s) GPRS: max. 171 kbit/s EDGE: 345 kbit/s
UMTS: 384 kbit/s HSDPA: 7,2 Mbit/s (HSDPA+: 28 Mbit/s)
LTE: 100 Mbit/s (-> 1 Gbit/$_{s\ 2014}$)
Entwicklungslinien:
GSM-Standard: Meilenstein in der Entwicklung der drahtlosen Kommunikation. Vorlage auch für viele andere Systeme und Netzgenerationen. Wünschenswert: weltweit einheitlicher Standard - leider nicht der Fall. Europäisches System GSM völlig neu und als digitales System entwickelt, ohne Kompromiss bezüglich Abwärtskompatibilität (z.B. Benutzung vorhandener Zeitschlitze). GSM weiterentwickelt als US-System und in mehr als 50 inner-/außereuropäischen Ländern eingesetzt.
GSM (2G) + HSCSD + PVM ~> GPRS (2.5G) ~> EDGE.
US-System IS-54 und japanisches System JDC (Vorläufer des PDC) wurden kompatibel zum vorhandenen analogen System des jeweiligen Landes ausgelegt, so dass jeder AMPS-Kanal sowohl für analoge als auch digitale Kommunikation benutzt werden kann.
Analoge Diskrepanz auch bei den MFN 3G:
UMTS (3GPP – GSM-lastig) und CDMA2000 (3GPP2 – CDMA-lastig).
Merkmale GSM:
Standard durch ETSI, ursprünglich für 900 MHz-Band, später auf 1800 MHz zugewiesen (anderes System ETSI/DCS 1800, ~GSM). GSM verwendet zur Kanalzuordnung eine Kombination von ALOHA, TDM, FDM. GSM hat bis zu max. 200 Vollduplexkanäle pro Zelle, je Kanal eine Downlinkfrequenz und Uplinkfrequenz von je 200 kHz:
Downlink-Frequenz (von Basisstation zu mobilen Stationen),

Uplink-Frequenz (von mobilen Stationen zur Basisstation).
GSM innerhalb und außerhalb Europa (weniger in USA), leistungsfähiger als US-Systeme wie IS-54/USDC (Nachfolgesysteme UMTS / IMT-2000), International Roaming Verträge zwischen den Betreiberländern, Europa: GSM-900, USA/Canada: GSM-800.
GSM ist grundsätzlich leitungsvermittelt ("kanalvermittelt").
Grundproblem aller MFN: Aufteilung der (begrenzten) Funkfrequenzen auf viele Teil-nehmer zur gleichzeitigen Benutzung (Millionen-Teilnehmersysteme).

124 Frequenzkanäle, jedes Frequenzband ist 200 kHz breit. Jede der 124 Frequenzkanäle unterstützt 8 getrennte Verbindungen mittels Zeitmultiplexverfahren (TDM-System mit 8 Schlitzen). Jede aktive Station erhält einen Zeitschlitz auf einem Kanal.

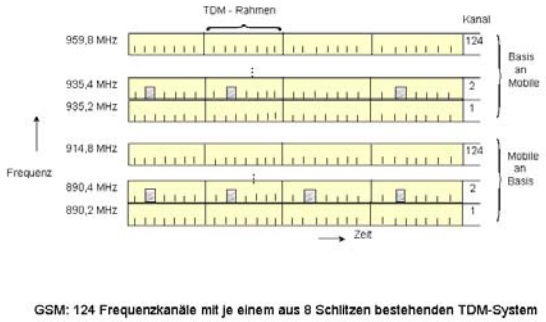


Abbildung 5.5: GSM-Frequenzkanäle

Die in Abbildung 5.5 dargestellte 8 Zeitschlitze gehören zum gleichen Kanal, je 4 in eine Richtung. Die zu sendenden Daten sind in diese Schlitze einzufüllen, bis alle Daten versendet sind. Die dargestellten TDM-Schlitze sind Teil einer komplexen Rahmenhierarchie.

Protokollhierarchie in GSM

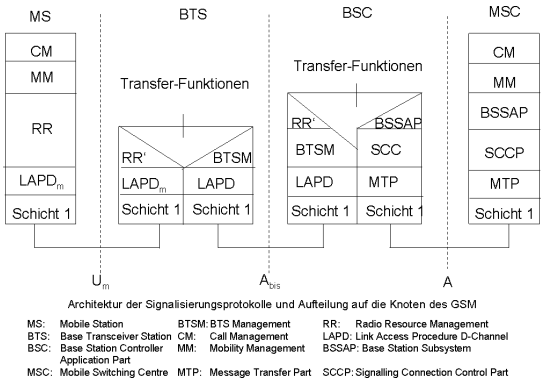


Abbildung 5.6: Signalisierungsprotokolle der GSM-Sicherungsschicht

CDPD - Cellular Digital Packet Data
CDPD ist verbindungsloser Datagramdienst, Datenpaketfunk (gut für IP-Pakete). GSM leitungsvermittelt (Sprache), hohe Fehlerraten möglich; Abrechnung: Verbindungsdauer.
GPRS (General Paket Radio Service): paketvermittelt; Abrechnung: Anzahl Pakete.
Für Übertragung von Daten: Lösung mittels paketvermittelten digitalen Datagrammdienstes: CDPD - Cellular Digital Packet Data. CDPD ist kompatibel zu AMPS (d.h. setzt auf AMPS auf). Ein träger 30-kHz-Kanal kann zum Senden von Datenrahmen mit Bruttorate von 19,2 kbit/s benutzt werden. Wegen des CDPD-Overheads liegt Nettorate bei 9,6 kbit/s.
Kanalzuordnung durch *Non-persistent-CSMA* (~> für Übertragung jedes Einzelrahmens) und zwar speziell: *DSMA - Digital Sense Multiple Access*.

CDMA - Code Division Multiple Access
Weitere Form der Zuordnung eines drahtlosen Kanals, bisher dominierend FDM, TDM (GSM):
CDMA ermöglicht jeder Station, jederzeit über das gesamte Frequenzspektrum zu übertragen (Aufspreizung des Funkkanals, Spreizcode („Chips“)). CDMA ermöglicht mehrere gleichzeitige Übertragungen durch Trennung über Kodierschemata, d.h. verschieden Kodierungen.
Ursprung: Miltärtechnik. Anwendung *Code-Multi-plexing*-Verfahren (CDMA). Kollidierte Rahmen werden durch lineare Addition von Mehrfachsignalen nicht als verstümmelt betrachtet ~> Empfänger kann entsprechendes Signal dekodieren. CDMA besitzt die Fähigkeit, das gewünschte Signal herauszuziehen und alles andere als Nebengeräusch abzulegen.
CDMA wird in drahtlosen Systemen mit einer festen Basisstation und vielen mobilen Stationen eingesetzt, die in unterschiedlicher Entfernung zur Basisstation sind.
Anwendung *Code-Multiplexing*-Verfahren (CDMA): in US-Systemen wie IS-95-CDMA, CDMA2000, zunehmend auch in UMTS (Phase 2).

5.4 IEEE-Norm 802 für LAN

5.4.1 Architekturkonzept

IEEE - Norm 802 für LAN
Architekturkonzept
Zur Umsetzung der Kanalzuordnung und Protokolle auf LAN (und MAN) wurden von der IEEE mehrere Normen unter Bezeichnung IEEE 802 herausgebracht, u.a.

IEEE 802.3	**CSMA/CD - Netze**	(ISO 8802/3)
IEEE 802.4	**Token-Bus - Netze**	(ISO 8802/4)
IEEE 802.5	**Token-Ring - Netze**	(ISO 8802/5)

Norm IEEE 802.2 beschreibt obere Sublayer der Sicherungsschicht, zugehöriges Protokoll: LLC-Protokoll (Logical Link Control Protocol). ISO 8802/2
Norm IEEE 802.11 für drahtlose LAN (W-LAN, wireless LAN).
Die Normen unterscheiden sich in der Bitübertragungsschicht (PHY) und MAC-Teilschicht, sind aber kompatibel zur Sicherungsschicht.
Die Normen IEEE 802 wurden übernommen von
- ANSI als nationale US-Normen (IEEE 802),
- ISO als internationale Norm (ISO 8802).

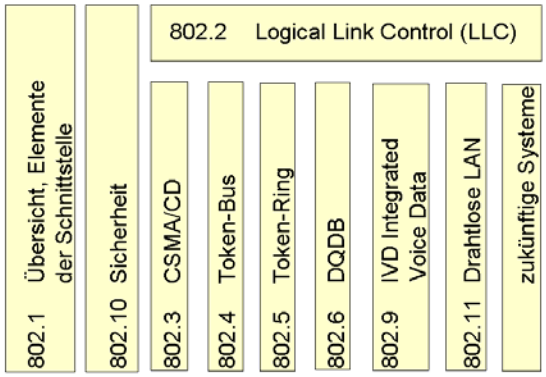


Abbildung 5.7: IEEE 802 LAN-Standards (Überblick)

Anm.:
- Token-Bus und Token-Ring heute weitgehend proprietär bzw. verdrängt.
- Ethernet: Klassisches Ethernet (Basis CSMA/CD) ergänzt durch kollisionsfreie Switch-Technologien, Fast-Ethernet (100 Mbit/s) und Gigabit-Ethernet (1 / 10 / 100 Gbit/s).

Eingliederung IEEE 802.2 / 802.3 in OSI-Referenzmodell

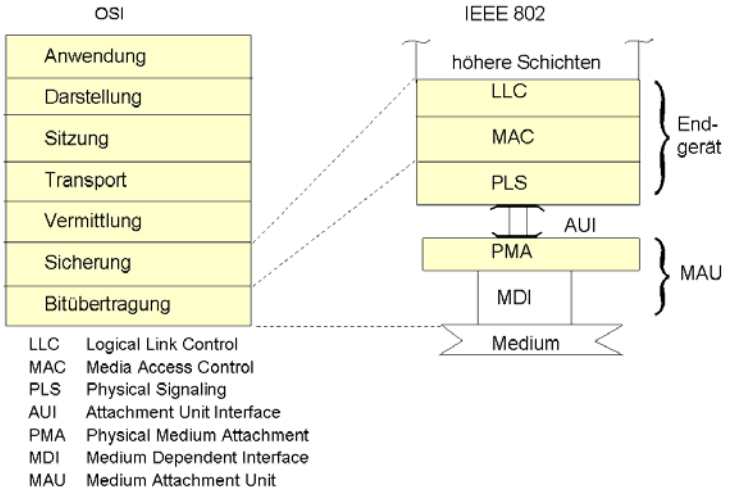


Abbildung 5.8: IEEE 802.2 und IEEE 802.3 im OSI-Referenzmodell

Funktionen der LLC-, MAC- und PHY-Schicht (IEEE 802-Norm)

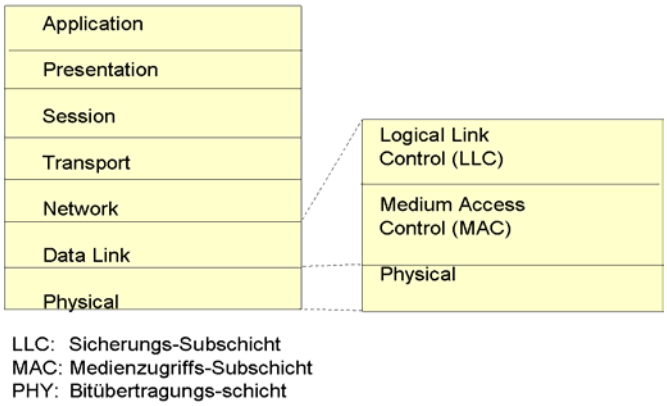


Abbildung 5.9: LLC-, MAC- und PHY-Schicht in LAN

Schicht	Funktionen
LLC	Unquittierter, verbindungsloser Dienst (LLC1) Verbindungsorientierter Dienst (LLC2) Quittierter, verbindungsloser Dienst (LLC3)
802.2	bei verbindungsorientiertem Dienst: - Verbindungsaufbau/abbau - Reihenfolgesicherung - Datenflusssteuerung - Fehlererkennung und -behebung
MAC	Empfang MA-PDU's (MAC-Rahmen)
802.3	Medienzugriff für MA-PDU's einschl. Konfliktauflösung
:	Erzeugung der Frame Checking Sequence (FCS)
:	Auswertung der FCS
802.5	Pufferung von MAC-Rahmen
PHY	Aktivierung/Deaktivierung Codierung/Decodierung von Leitungssignalen Präambel-Erzeugung Bitsynchronisation Übertragung von unstrukturierten Bitströmen

5.4.2 IEEE-Norm 802.3 und Ethernet

CSMA/CD
Zugriffsverfahren: CSMA/CD: Carrier Sense Multiple Access / Collision Detection (Trägererkennung / Kollisionsentdeckung) ~> für 10-Mbit/s-Ethernet.
Grundkonzept:
- wenn eine Station übertragen will, hört sie das Kabel (Kanal) ab.
- wenn Kanal belegt, wartet Station, bis er frei ist, ansonst sendet sie sofort (1-persistent).
- wenn 2 oder mehrere Stationen gleichzeitig auf einen freien Kanal zugreifen ~> Kollision.
- jede der Stationen unterbricht dann die Übertragung, wartet eine zufallsgesteuerte Zeitspanne und wiederholt den ganzen Vorgang.

Auf Grund endlicher Signal-Ausbreitungsgeschwindigkeit können trotz Abhören Kollisionen auftreten.

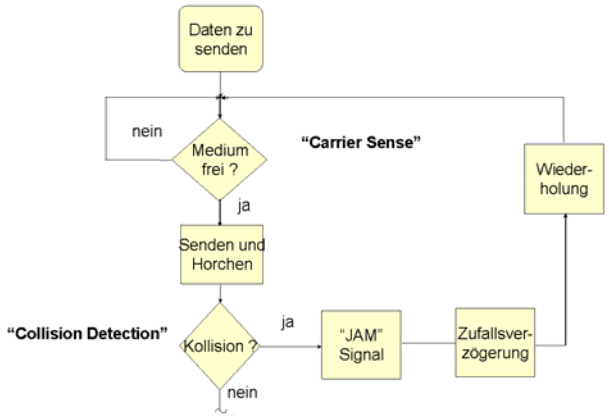


Abbildung 5.10: Ablauf CSMA/CD

Jamming (Bündelstörung):
Alle Stationen beobachten die Leitung. Entdeckt eine Station eine Kollision, dann sendet sie ein "Jamming"-Signal.
Jamming-Signal unterscheidet sich in seiner Signalform deutlich von anderen Signalen. Sendende Stationen brechen Übertragung nach Wahrnehmung des Jamming-Signals sofort ab.

Kollisionen und Jamming
Auf Grund endlicher Signal-Ausbreitungsgeschwindigkeit können trotz Abhören des Kanals Kollisionen auftreten ~> Jamming (Bündelstörung):

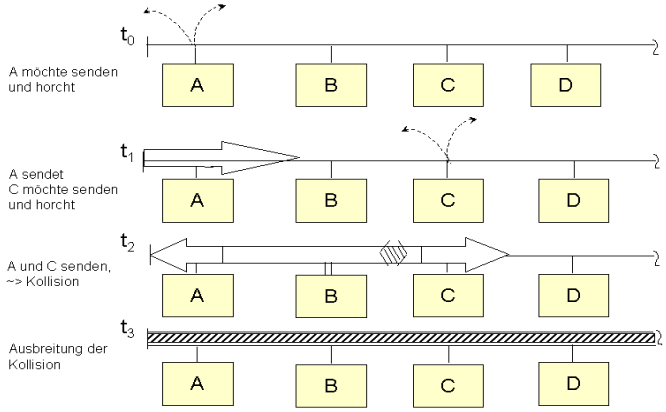


Abbildung 5.11: Kollision (Beispiel)

- Alle Stationen beobachten die Leitung.
- Entdeckt eine Station eine Kollision, dann sendet sie ein "Jamming"-Signal.

- Jamming-Signal unterscheidet sich in seiner Signalform deutlich von anderen Signalen.
- Sendende Stationen brechen Übertragung nach Wahrnehmung des Jamming-Signals sofort ab (ohne die gestörte Übertragung noch zu beenden).

Ethernet ("Äther")
Ethernet ist ein spezielles CSMA/CD-Protokoll, basierend auf Norm IEEE 802.3.
Entwicklung: Metcalf und Boggs (1976)
Literatur: "Ethernet: Distributed Packet Switching for Local Computer Networks", Communications of the ACM, July 1976, pp. 395-404
Ergänzung des ALOHA (Abramson) durch Trägererkennung (Carrier Sense). Daraus erarbeiteten Xerox, DEC und Intel einen 10 Mbit/s-Ethernet-Standard => bildet die Basis für die Norm IEEE 802.3 (IEEE 802.3 beschreibt Familie von 1-persistent CSMA/CD-Systemen).
Ursprünglicher Standard: 10 Mbit/s Basisband für Koaxialkabel mit 50 W (Ohm).
Norm IEEE 802.3
- gilt für ein LAN mit 1-persistent CSMA/CD.
- Familie von 1-persistent-CSMA/CD-Systemen mit Geschwindigkeiten von 1 ... 10 Mbit/s für verschiedene Medien.

Ethernet-Kabel
Bekannte Kabeltypen:

10 Base 5	Thick Ethernet (dickes Koaxialkabel)
10 Base 2	Thin Ethernet (dünnes Koaxialkabel)
10 Base-T	HUB und verdrillte Kabelpaare
10 Base-F	Glasfaser

Analog im Bereich von MAN

100 Base-T4	Verdrilltes Kabelpaar, Kategorie 3 (Cat-3)
100 Base-TX	Verdrilltes Kabelpaar, Kategorie 5 (Cat-5)
100 Base-F bzw. FX	Glasfaserkabel, Multimode

10 Base 2: "Thin Ethernet".
Dünnes Koaxialkabel (RG 58, 50 W Wellenwiderstand). Kostengünstig, gut verlegbar. Maximale Segmentlänge: 200 m. Knoten/Segment: 30.
Anschlüsse über sog. BNC-Stecker (statt TAP-Schraubanschluss). Transceiver-Elektronik befindet sich hier auf dem Controller, jede Station hat ihren eigenen Transceiver.
Heutige Ethernet-Karten haben in der Regel sowohl 15-poligen Stecker für Thick Ethernet Kabel (10 Base 5) bzw. Koaxial-Stecker für Thin Ethernet Kabel (10 Base 2) als auch RJ45-Stecker (HUB)

10 Base-T: Verwendung HUB und verdrillte Kabelpaare zu den Hosts

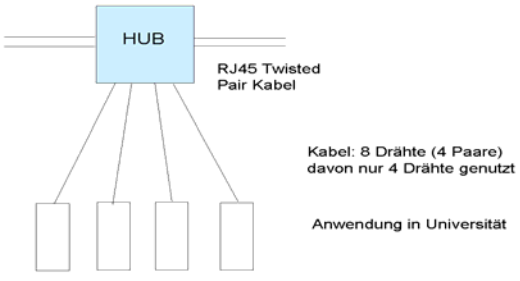


Abbildung 5.12: Ethernet-Kabel 10 Base-T und RJ45

Nutzung verdrillter Kabelpaare (Kupfer, Telefon)
UTP: Unshielded Twisted Pair, Verwendung von RJ45-Stecker (Plastik)
STP: Shielded Twisted Pair (IBM, teuer), verwendet RJ45-Stecker (metallisches Gehäuse)

Maximale Segmentlänge zw. HUB und Rechner: 100 m (bzw. 150 m)
Knoten/Segment: 1024
Einfache Wartung (einfaches Hinzufügen/Abkoppeln). Von allen Stationen geht ein Kabel zu einer zentralen Buchse (HUB). Schnelle Ausführung: 100 Base-T (Fast-Ethernet).

10 Base-F: Anschluss von Glasfasern
Max. Segmentlänge: 2000 m. Knoten/Segment: 1024. Gut für Verkabelung zwischen Gebäuden; teuer

Verkabelungstopologien:
Repeater (Verstärker): zur Ausweitung der Netzentfernungen; arbeitet auf Ebene Bitübertragungsschicht, Repeater verstärkt, aber verursacht auch eine Verzögerung.

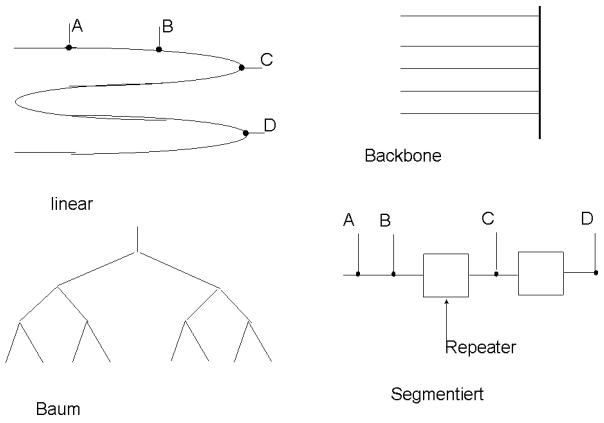


Abbildung 5.13. LAN-Toplogien (Auswahl)

IEEE 802.3 / Ethernet
Manchester-Kodierung
Kollision von 2 Null-Volt-Signalen ist nicht zu erkennen (Zweideutigkeit). Empfänger muss Anfang, Ende oder Mitte jedes Bits ohne Bezug auf einen externen Takt eindeutig erkennen.
Ansätze hierzu: Manchester-Kodierung und differentielle Manchester-Kodierung.
Jede Bitperiode wird in 2 gleiche Intervalle unterteilt. Binäres 1-Bit wird gesendet, indem die Spannung im 1. Intervall hoch und im 2. niedrig gesetzt wird. Eine binäre 0 umgekehrt: zuerst Low, dann High. Dieser Übergang in Mitte der Bitperiode erleichtert Synchronisation zwischen Sender und Empfänger. Nachteil: gegenüber direkter binärer Kodierung wird doppelte Bandbreite vorausgesetzt.

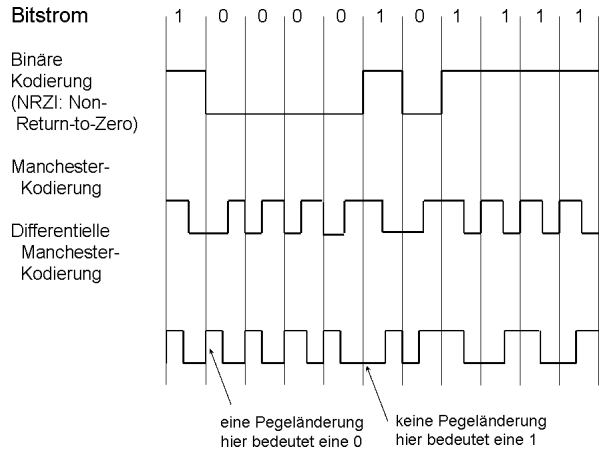


Abbildung 5.14: Manchester-Kodierung

Differentielle Manchester-Kodierung
Variation der Manchester-Kodierung. Höhere Rauschbeständigkeit, aber komplexer. Alle Basissysteme verwenden Manchester-Kodierung mit -0,85 Volt, CSMA/CD.
Ethernet arbeitet mit Manchester-Kodierung (Rahmenerkennung).

MAC-Protokoll nach IEEE 802.3

Rahmenformat nach IEEE 802.3

7	1	2 oder 6	2 oder 6	2	0 ... 1500	0 ... 46	4 Byte
Präambel		Zieladresse	Quelladresse		Daten	Pad	Prüf-Σ

Beginn des Rahmenbegrenzers

Länge des Datenfeldes

Präambel: Rahmenbeginn
Bitfolge 10101010 --> über Manchester-Kodierung wird aus dieser Bitfolge für die Dauer von 5,6 ms eine 10 MHz-Schwingung erzeugt. Diese dient zur Synchronisation der Taktgeber zwischen Empfänger und Sender.
Rahmenstartbyte: 10101011 - markiert den Anfang des Rahmens
Ziel / Quelladresse: i.d.R. 6 Byte im 10 MHz-Basisband benutzt
- Höherwertiges Bit in Zieladresse (Bit 47):
- für normale Adressen (Unicast) für Gruppenadresse (Multicast:
- Sender, Adresse hex FFFF (alles 1): Broadcast. mehrere Empfänger)
- Bit 46: Kann zur Unterscheidung in lokale und globale Adresse verwendet werden.
  Lokale Adressen: vom jeweiligen Netzverwalter vergeben, gelten nur im lokalen Netz.
  Globale Adressen: von IEEE vergeben.
  Somit 48 - 2 = 46 verfügbare Adressbits --> ca. $7 * 2^{13}$ globale Adressen.
  Vermittlungsschicht muss nun ermitteln, wo sich das Ziel befindet (Nutzung ARP/RARP).

Längenfeld: Anzahl Bytes des Datenfeldes (0 ... 1500).
IEEE 802.3 legt Mindest-Rahmenlänge von 64 Byte fest, um ungültige Rahmen bzw. Bruchteile zu erkennen; d.h. Datenteil = 46 Bytes. Falls Datenteil < 46 Bytes, füllt Pad-Feld den Rahmen bis zum Minimum auf.
Festlegung einer minimalen Rahmenlänge soll auch verhindern, dass eine Station die Übertragung eines kurzen Rahmens beendet, bevor sein erstes Bit das andere Ende des Kabels erreicht und dort ggf. mit anderem Rahmen kollidiert.

Rahmenformat (Rahmenlänge)
Kollisionserkennung kann bis zu 2τ dauern (τ: Verteilungszeit für Übertragung A -> B)

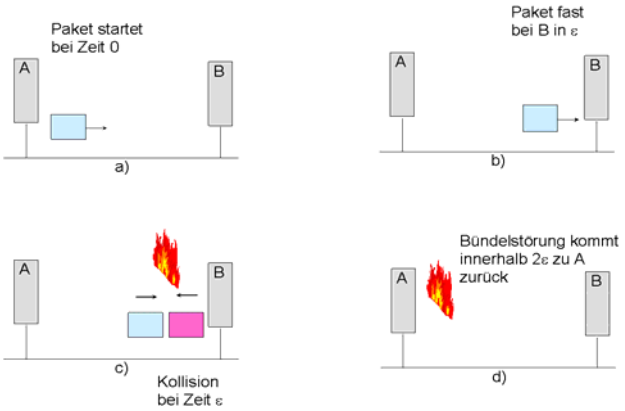


Abbildung 5.15: Kollisionserkennung (Rahmenlänge)

Legende zur Abbildung:
- Station A sendet zur Zeit 0 einen Rahmen (Zeit zum Erreichen von B sei τ, B sei die am weitesten entfernte Station).
- Kurz vor Erreichen von B (Zeit τ - e) beginnt B selbst eine Übertragung --> Kollision --> B bricht Übertragung ab, sendet 48-Bit-Signal (Jamming), um alle Stationen zu warnen.
- Zur Zeit 2τ erkennt Sender A das Warnsignal und bricht seine Übertragung ab (Wiederholung nach zufälliger Zeitspanne).
- Versucht eine Station einen sehr kurzen Rahmen zu übertragen, kann eine Kollision stattfinden, aber Übertragung wird beendet, bevor das Warnsignal in 2t zurückkommt.
- Sender denkt fälschlicherweise, dass der Rahmen erfolgreich gesendet wurde. Zu dessen Vermeidung muss Übertragung aller Rahmen > 2τ dauern.
- Bei einem 10 Mbit/s-LAN mit einer maximalen Länge von 2 500 m und 4 Repeatern (nach 802.3-Spezifikation) muss der kleinste zulässige Rahmen 51,2 ms (= 64 Byte) dauern. Rahmen mit weniger Byte werden auf 64 Byte aufgefüllt.

Prüfsumme: 32 Bit langer Hashcode der Daten.
Prüfsummenalgorithmus: zyklische Redundanz.

Rahmenlänge (mind. 64 Byte, max. 1518 Byte)

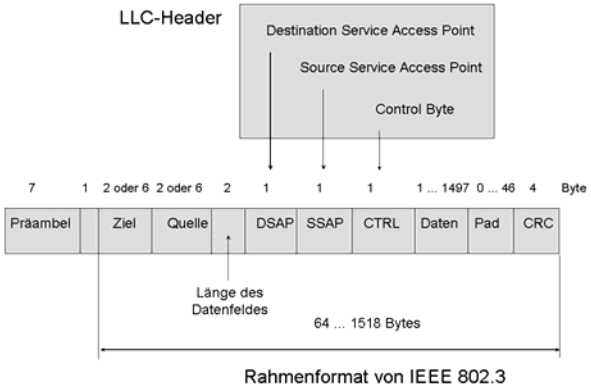


Abbildung 5.16: Rahmenformat IEEE 802.3 und LLC-Header

Adressen und Namen
Name: identifiziert ein Objekt, z.B. Adapterkarte für Ethernet, Token-Ring, FDDI, ATM ...
Adresse: Ort des Objekts, z.B. T-Stecker eines 10 Base 2 Ethernets Kabels, an den eine Ethernet-Adapterkarte angeschlossen ist.
Adressfelder eines Ethernet- oder Token-Ring-Rahmens enthalten somit Namen und keine Adressen, da sie sich auf Werte beziehen, die in den Adapterkarten fest verdrahtet sind.

Binärer exponentieller Backoff - Algorithmus (Binary Exponential Backoff)
Zufallssteuerung im Falle einer Kollision (siehe CSMA/CD)
- Nach eine Kollision wird die Zeit in einzelne Schlitze (Slots) unterteilt, deren Länge der vollen Übertragungszeit 2τ entspricht.
- Um den längsten nach 802.3 zulässigen Pfad zu verwenden (2,5 km und 4 Repeater), wurde die Schlitzzeit auf 512 Bitzeiten bzw. 51,2 ms gesetzt.

Nutzung Konkurrenzintervall, bestehend aus diskreten Slots (Slotgröße: 512 Bit, Slotzeit: 51,2 ms).
Annahme: es sind bisher i Kollisionen aufgetreten

nach 1. Kollision:	0 oder 1 Slotzeit warten bis wieder senden
nach 2. Kollision:	0,1,2 oder 3 Slotzeiten warten (0 ... 22 -1)
nach 3. Kollision:	Zufallszahl zwischen 0 ... 23 -1
.....	

nach i. Kollision: Zufallszahl zwischen 0 ... 2i -1 (für i <= 10)
für i = 11 ... 16: Zufallszahl zwischen 0 ... 1023
nach 16 Versuchen: Abbrechen --> Fehlermeldung an höhere Schicht

Zugehörigen Algorithmus ~> *Binary Exponential Backoff* (binäre Unteraussteuerung):

- Dynamische Anpassung an die Anzahl n der sendebereiten Stationen. Versuchen nur wenige Stationen zu senden, dann ist ein kleines Zufallsintervall günstig.
- Versuchen viele Stationen zu senden, dann ist ein Zufallsintervall ==> 1023 Slots günstig (Kollisions-Wkt. dann verschwindend gering).

Fast-Ethernet

FDDI für Hochgeschwindigkeits-LAN (100 Mbit/s): kein Massenprodukt geworden, keine Multimedia-Übertragung, keine isochrone Übertragung (-> Nischenprodukt). Erweiterung 10-Mbit/s-Ethernet auf Fast-Ethernet (100 Mbit/s).

Normierungsausschuss des 802.3: Norm 802.3u, 1995 von IEEE zugelassen.

* kein neues Konzept gegenüber Ethernet.
* Beibehaltung aller Paketformate, Schnittstellen, Prozeduren und Regeln.
* Lediglich Bitzeit von 100 ns auf 10 ns gesenkt.

Somit Abwärtskompatibilität zu den riesigen LAN - Installationen gesichert. Kostenvorteile für Fast-Ethernet.

Verkabelung

* Nutzung der Vorteile der 10 Base T-Verkabelung (HUB)
  (somit Vampirabzweige oder BNC-Stecker nicht zulässig ~> Twisted Pair, RJ45).
* Dennoch mussten Veränderungen gewählt werden.

Zulässige Verkabelungen:

100 Base-T4 Verdrilltes Kabelpaar
4 Paare UTP Kategorie 3 (25 MHz): 3 Paare für Daten, 1 Paar für Kollisionssignalisierung. Max. Segment: 100 m

100 Base-TX Verdrilltes Kabelpaar
2 Paare Kategorie 5 (100 W) oder STP (150 W). Max. Segment: 100 m. Weitgehend identisch mit 100 Mbit/s FDDI-Kupfer Standard. Vorteil: Vollduplex bei 100 Mbit/s.
RJ-45 Stecker

100 Base-F (bzw. -FX) 2 Multimode Glasfasern
Identisch mit Glasfaser FDDI-Standard. Max. Segment: 2 000 m. Vorteile: Vollduplex bei 100 Mbit/s, lange Strecken.

Anm.: HUB's mit 100 Base-T4 und 100 Base-TX werden als 100 Base-T bezeichnet.

Isochrones Ethernet

Erweiterungen für Multimedia-Übertragungen.

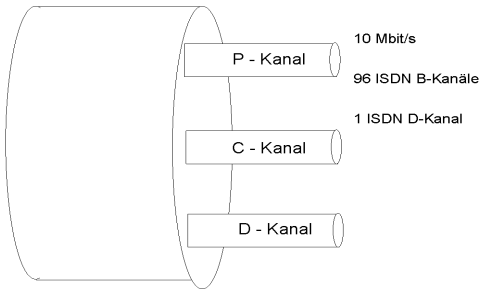


Abbildung 5.17: Subkanäle bei isochronem Ethernet

Auf vorhandenen 10 Base-T Kabel werden im Zeitmultiplex-Verfahren 3 Subkanäle 4/5 Code statt Manchester Code. Über den C- und D- Kanal wird (ähnlich wie bei ISDN) eine 6,144 Mbit/s Verbindung geschaltet. Ablösung durch Gigabit-Ethernet.

Vermittelte LAN's nach 802.3 (Switched Ethernet)
Engpass, wenn zu viele Stationen an einem 802.3-LAN angeschlossen sind.
Möglichkeiten zur Abhilfe:
- 100 Mbit/s Fast-Ethernet --> Problem: Austausch 10 Mbit/s Adapterkarten (Kosten).
- Vermitteltes 802.3-LAN (Switched Ethernet: 1- / 10- / (100-) Gbit/s-Ethernet).

Anm.: 100/1000 Mbit/s-Ethernet heute Standard.
Kern des Switched Ethernet:
Vermittler, mit Hochgeschwindigkeitsplatine (> 1 Gbit/s, herstellerspezifische Protokolle) und Platz für 4 ... 32 Steckkarten mit je 1 ... 8 Anschlüssen. Meist hat jeder Stecker einen 10 Base-T - Anschluss an einem Host.

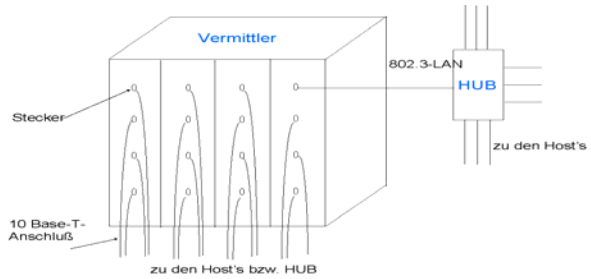


Abbildung 5.18: Ethernet Switch

Switched Ethernet
- Klassisches Ethernet (z.B. 10BASE5, 10BASE2) mit Kabel als gemeinsames Übertragungsmedium (collision domain / shared medium) arbeitet gut bei geringem Verkehrsaufkommen. Bei Auslastung > 50 % vermehrt Staus (Congestion), dadurch Übertragungsleistung drastisch reduziert.
- Trotz CSMA/CD-Bezeichnung spielt Kollisionsauflösung heute nur geringe Rolle. Heutige Netzwerke werden im Vollduplexmodus betrieben, bei dem Switches für die Zugriffsauflösung sorgen und keine Kollisionen mehr entstehen. Dennoch blieb das Frame-Format (insbes. Frame-Header) und die für die Kollisionserkennung vorgeschrie-bene minimale Frame-Länge bis hinauf zu 10-Gbit/s-Ethernet unverändert.
- Bei Switched Ethernet gibt es kein HDX (halbduplex) bei Netzwerkkarten, Hubs sind nicht mehr zugelassen. Diese sind durch Switches zu ersetzen, die durch ihre FDX- (full duplex) Fähigkeit mit ausschließlichen Punkt-zu-Punkt-Verbindungen die Collision Domains eliminieren und somit absolut kollisionsfrei arbeiten.

100-Gbit/s-Ethernet
(Projekt 100GET: 100 Gbit/s Carrier-Grade Ethernet Transport Technologies)
Entwicklung von Technologien für ein schnelles, zuverlässiges und sicheres Internet der Zukunft sowie Vorbereitung eines Standards für ein 100-Gbit/s-Ethernet. Zielstellungen: Übertragungskapazität (Datenvolumen, Geschwindigkeit), Sicherheit, Robustheit, Qualität der Netzverbindungen ~> NG eines superschnellen Internet.
Führende europäische Unternehmen und Forschungseinrichtungen aus Deutschland, Finnland, Frankreich, Schweden und Spanien. Durchgängige Grundlage für Datenverkehr im Kern- und Metronetz auf Basis Ethernet, mit 100 Milliarden Bit pro Sekunde bei hoher Qualität (technischer Ausfall < 5 min/Jahr). Störungsfreier Betrieb, gesichert gegen unbefugten Zugriff. DÜ-Rate mit 100 Gbit/s pro Kanal nur mit Glasfasertechnik erreichbar. Das erfordert völlig neue optische Komponenten und angepasste Elektronik.
Anwendungen: Downloads (Musik, Video), Medizin, Videokonferenzen, Teleteaching, ...

5.4.3 IEEE-Norm 802.5: Token Ring

Wird ergänzt

5.4.4 IEEE-Norm 802.2: Logical Link Control (LLC)

Dienste der IEEE 802-LAN
802-LAN's und 802.6-MAN (DQDB) bieten einen (unzuverlässigen) Datagram-Dienst. Falls von IP-Paketen genutzt, ist eine garantierte Übertragung nicht vorausgesetzt (ein IP-Paket kann lediglich in das 802-Nutzdatenfeld eingefügt und gesendet werden; Verluste sind in höheren Schichten zu behandeln). Falls in Schicht 2 eine Fehlerüberwachung und Flusssteuerung gewünscht ist, kann auf alle 802-LAN und -MAN-Protokolle das LLC-Protokoll (Logical Link Control) aufgesetzt werden.
LLC verbirgt auch die Unterschiede zwischen verschiedenen 802-Netzen durch Bereitstellung eines universellen Formats und eine Schnittstelle zur Vermittlungsschicht. LLC-Protokolle, Format und Schnittstellen basieren auf OSI.
LLC bietet 3 Dienstoptionen:

* unzuverlässigen Datagram-Dienst
* bestätigten Datagram-Dienst
* verbindungsorientierten Dienst

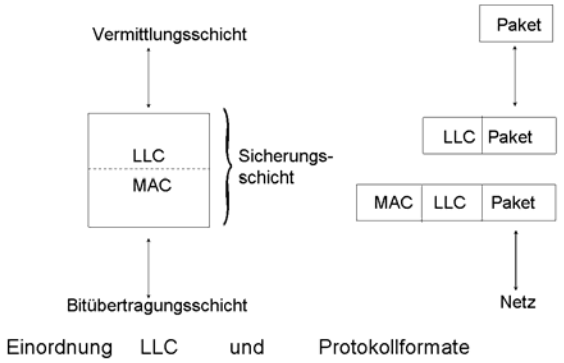


Abbildung 5.19: Formate in LLC

LLC-Header basiert auf dem älteren HDLC-Protokoll. Für Daten und Steuerung werden verschiedene Formate benutzt:

- *bestätigter Datagram-Dienst* und *verbindungsorientierter Dienst*: Datenrahmen enthalten Quelladresse, Zieladresse, Folge-Nr., Bestätigungs-Nr. und andere Bits.
- *unzuverlässiger Datagram-Dienst*: hierbei Folge- und Bestätigungs-Nr. weggelassen.

6 Vermittlungsschicht

6.1 Aufgaben, Designaspekte und Organisation

Aufgabenstellungen
Paket-Transport vom Ursprung zum Ziel, i.allg. über Zwischenknoten (sog. **Router,** Vermittlungsknoten, "store-and-forward", "Punkt-zu-Punkt"), insbes.
- Routing der Pakete (Pfadauswahl, Leitwegbestimmung),
- Überlaststeuerung (congestion control),
- Flußsteuerung (Geschwindigkeitsregulierung).
- Internetworking (Protokoll-Ausgleichen zwischen verschiedenen Netzen).

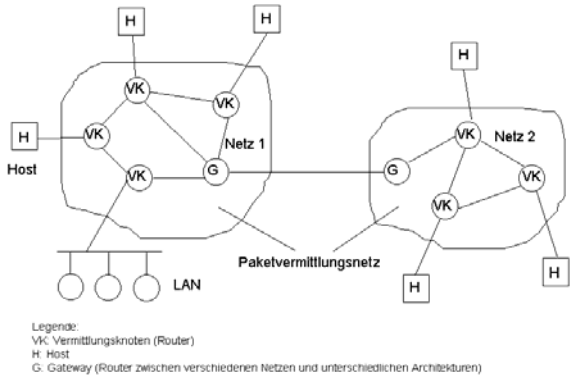


Abbildung 6.1: Paketvermittlungsnetz (Beispielkonfiguration)

Designaspekte der Vermittlungsschicht
Zielstellungen an Dienstleistung der Vermittlungsschicht: unabhängig von Netztechnologie, transparent für Transportschicht und die der Transportschicht bereitgestellten Netzadressen müssen ein einheitliches Nummerierungsschema darstellen (auch zwischen WAN und LAN).
Wichtige Fragestellung: **Paketvermittlungsnetz**, *verbindungsloser (CL)* oder *verbindungsorientierter (CO)* Dienst ? und damit auch: auf welcher nachfolgenden Schicht wird bei verbindungsloser DÜ ein verbindungsorientierter Dienst bereitgestellt ?

Interessenlager 1 (insbesondere Internet): **verbindungslos** (CL: connectionless)
- Teilnetz soll *nur Bits* transportieren,
- Erfahrung damit seit 1970 (ARPAnet) ~> dominierende Technologie durch Internet, vor allem bedingt durch die Internet-Anwendungen, insbes. WWW.
- Fehlerüberwachung (Korrektur, Erkennung) und Flusssteuerung sollen *Hosts* übernehmen,
- Jedes Paket muss bei verbindungslos die *volle Zieladresse* erhalten (Datagram),
- *Schnelligkeit* wichtiger als Genauigkeit (Internet: keine Dienstgüte, nur "best effort").

  IP-Netze überlassen die CO/CL-Frage den höheren Protokollschichten.
  Damit aber keine Reihenfolgetreue der Pakete auf Ebene der VMS (IP).

Meisten Anwendungen erfordern aber eine verbindungsorientierte Kommunikation: Regelung auf einer nächsthöheren Protokollschicht (z.B. TCP bei IP), ggf. in Anwendungsschicht bzw. durch Anwendung selbst (z.B. Auskunftssysteme).

Interessenlager 2 (insbes. Betreiber klassischer ISO/OSI-PVN): **verbindungsorientiert** (CO: connection oriented)
- Hundertjährige Erfahrung mit Telefonnetz und Postsystem.
- Vor Übertragung ist eine *Verbindung* mit der gleichen Schicht der Empfängerseite aufzubauen. Diese Verbindung erhält eine spezielle Kennung und bleibt bestehen, bis alle Daten übertragen sind. Danach explizit abgebaut.

- Kommunikation in beiden Richtungen (duplex); Pakete werden *in Reihenfolge* zugestellt.
- *Flusssteuerung* (flow control) wird automatisch bereitgestellt (damit schneller Sender einen langsamen Empfänger nicht überschwemmt).
- Optional: garantierte Zustellung, explizite Empfangsbestätigung, Pakete mit hoher Priorität.
- Damit Nutzer von komplexen Protokollen auf Transport-Schicht befreit. Außerdem auf verbindungsorientierter Vermittlungsschicht besser *Echtzeit-Audio/Video* aufsetzbar.
- Markante Vertreter: X.25, Frame Relay, ATM ~> rückläufige Bedeutung.

Interne Organisation der Vermittlungsschicht
Unabhängig von dem für die Transport-Schicht bereitgestellten Dienst (verbindungsorientiert oder verbindungslos) wird der interne Ablauf realisiert durch
- eine virtuelle Verbindung (Telefon, X.25, ATM) *oder*
- Datagrame (Internet) für die unabhängigen Pakete des verbindungslosen Aufbaus.

Virtuelle Verbindung
Im allgemeinen für verbindungsorientierte Dienste. Beim Verbindungsaufbau wird eine *Route* zwischen Quelle und Ziel gewählt, die dann für die gesamte Übertragung unverändert bleibt (analog Telefonnetz: virtual call); Wird Verbindung getrennt, endet die virtuelle Verbindung. Zur Erkennung des Weges führen die Router eine *Tabelle,* in der jeweils ein Eintrag für jede offene virtuelle Verbindung erfolgt.
Jedes Paket muss außer den üblichen Steuerdaten ein *Nummernfeld* im Header führen*,* das die virtuelle Verbindung bezeichnet => dadurch leitet Router das ankommende Paket an die richtige Ausgabeleitung weiter (diese virtuellen Nr. haben nur lokale Bedeutung für den Router). Wenn eine Verbindung beendet, werden Eintragungen aus den Router-Tabellen entfernt.

Datagram
Hierbei werden *keine Routen voraus festgelegt* (auch bei verbindungsorientierten Dienst), Routen ständig neu ermittelt. Jedes Paket wird unabhängig vom Vorgänger transportiert; nachfolgende Pakete können auf anderen Routen verlaufen.
Jedes Datagramm muss *volle Zieladresse* (sog. große Adresse) und *Reihenfolge-Nr.* enthalten. Router sucht für jedes Paket die Ausgangsleitung und überträgt dieses. Damit sind diese Netz robuster, trotz vieler Ablaufhandlungen.
Beide internen Ablaufformen haben Vor- und Nachteile. Verschiedene Kombinationen in Verbindung mit verbindungslosen bzw. verbindungsorientierten Diensten möglich.

6.2 Routing-Algorithmen

6.2.1 Routing (Leitweglenkung)

Routing
Flächendeckende Computernetzen sind i.d.R. paketvermittelt, d.h. Rechner nicht direkt miteinander verbunden (Pkt.-zu-Pkt.). Austausch der Pakete zwischen entfernten Hosts erfolgt mit Hilfe von Vermittlungsknoten (sog. Router), die die Pakete entsprechend Zieladresse weiterleiten (*store-and-forward*). Dazu Entscheidung erforderlich, an welchen nächsten Nachbarn ein Paket geschickt werden muss, um einen bestimmten Zielrechner zu erreichen. Lösung über Verfahren zur Wegeauswahl (*Leitweglenkung,* engl.: *Routing,*).
Dabei nicht nur Wegeauswahl zwischen Sender und Empfänger, sondern Weg sollte unter bestimmten Gesichtspunkten *optimal* sein, z.B. möglichst wenig Zwischenschritte (“Hops“), Gesamtdauer für alle Schritte sollte minimal sein oder geringe “Kosten”.
-> Verschiedene Routing-Verfahren: statisch / dynamisch bzw. reaktiv / proaktiv.
Routing-Verfahren: Bestimmung des Weges der Pakete von Quelle zu Ziel (über Teilknoten)
- bei Datagram: Entscheidungen je Paket neu.

- bei virtueller Verbindung: Entscheidung nur bei Verbindungsaufbau, danach folgen alle Pakete dieser Route (sog. “Sitzungsrouting, Session Routing”).

Kriterien eines Routing-Algorithmus
- genau und einfach,
- robust: gegenüber Änderungen der Topologie, SW-Upgrads, Datenverkehr, HW / SW-Fehler, Leitungsauswechslungen, ...
- stabil (viele Routing-Algorithmen erreichen keinen stabilen Zustand),
- fair und optimal (oft gegensätzlich zueinander).

Optimierungskriterien, u.a. durchschnittliche Paketverzögerung, Maximum des gesamten Netzdurchsatzes, Minimieren der Paket-Teilstrecken.

Klassifikation von Routing-Verfahren:
Erste Unterscheidung in nichtadaptive und adaptive Routing-Verfahren (Hauptgruppen):
- *Nichtadaptive Verfahren* sind statisch: Routing anhand fester Tabellen.
- *Adaptive Routing-Verfahren* stellen sich automatisch auf eine veränderte Netzwerktopologie ein. Bekannte adaptive Routing-Verfahren:
  in IP-Netzen: Distance-Vector-Verfahren und Link-State-Verfahren,
  Routing in Ad-hoc-Netzen erfolgt ausschließlich adaptiv.

Weitere Unterteilung der Routing-Verfahren in proaktive (engl.: table-driven) und reaktive (engl.: on-demand) Verfahren:
- *Proaktive Verfahren:* halten Routing-Tabellen zu allen denkbaren Knoten im Netz, selbst wenn zum entsprechenden Ziel nie ein Paket geschickt wird.
- *Reaktive Verfahren:* Route zu einem Ziel erst dann berechnet, wenn ein Paket versendet werden soll.

2 Hauptgruppen von Routing-Algorithmen
1. **Nichtadaptive Algorithmen**: Leitweg wird voraus bestimmt (Festlegung beim Booten des Netzes auf allen Routern) => sog. “statisches Routing”.
2. **Adaptive Algorithmen** => sog. “dynamisches Routing”:
   - ändern Routing-Entscheidungen entsprechend Änderungen in Topologie und Verkehr,
   - nutzen Messungen und Schätzungen zum Verkehr und zur Topologie,
   - unterscheiden sich nach
     - Quelle der Informationen (lokal, vom Nachbar-Router oder allen Routern),
     - Zeitpunkt der Routenänderung (nach Δt oder Last- bzw. Topologieänderung),
     - Optimierungsmetrik (Entfernung, Anzahl Teilstrecken, geschätzte Übertragungszeit),
     - Implementierungsprinzip: zentral / dezentral.

6.2.2 Statisches Routing (Beispiele)

Shortest Path Routing
Bestimmung des Leitweges als “kürzesten” Weg: Ermittlung des kürzesten Pfades mittels graphentheoretischer Methode und Optimierung. Einfaches Konzept, häufig angewandt.
Verschiedene Metriken zur Optimierung -> verschiedene Algorithmen (Dijkstra, 1959), z.B.
- Länge der Teilstrecken,
- Bogenbeschriftung (Länge, Bandbreite, durchschnittlicher Verkehr, Übertragungskosten, mittlere Warteschlangenlänge, gemessene Verzögerungen).
- Wichtungen.

Flooding (“Fluten”)
Jedes ankommende Paket wird über mehrere Ausgangsleitungen gesendet (außer auf der Ankunftsleitung). Bewirkt große Zahl von Paketduplizierungen. Eindämmungsmöglichkeiten:
- Streckenzähler, Merken der gefluteten Pakete (über eingefügte Folge-Nr.),

- selektives Flooding: nicht jedes Paket an jede Ausgangsleitungen, sondern nur auf Leitungen, die in die richtige Richtung laufen (z.B. entsprechend Topologie).

Anwendung im militärischen Bereich (robust), im DB-Bereich (wenn alle Datenbanken zu aktualisieren sind), bei Ad-hoc-Netzen.

Flußbasiertes Routing (flow-based Routing)
Hierbei Topologie und Last berücksichtigt. Datenverkehr wird gemessen und sei über bestimmte Zeit konstant. Ermittlung mittlerer Paketverzögerungzeit per Warteschlangen-Theorie --> effektiver statischer Routing-Algorithmus.

6.2.3 Dynamisches (adaptives) Routing (Beispiele)

Distance-Vector-Routing
Jeder Router verwaltet eine Tabelle (Vektor), auf deren Grundlage er die am besten bekannte Entfernung zu jedem Ziel und die zu benutzende Leitung ermittelt ("*Distances*"). Tabellen werden aktualisiert durch Informationsaustausch zwischen benachbarten Routern (periodisch). Einsatz im Internet.
Election-Algorithmus zur Ermittlung der Distances: **Heartbeat** (Herzschlag)-Verfahren.
Andere Bezeichnungen

- verteiltes Bellmann-Ford - Routing (1957),
- Ford-Fulkerson - Routing (1962). Ursprüngliches Routing im ARPAnet und Internet (Protokoll: **RIP**: Routing Information Protocol).

Heute in vielen Cisco-Routern (modifiziertes Distance-Vector-Routing). Jeder Router führt eine Routing-Tabelle, die für jeden Teilnetz-Router einen Eintrag enthält. Dieser Eintrag umfaßt: bevorzugte Ausgangsleitung, geschätzte Zeit oder Entfernung (Distances sind die "Kosten", ausgedrückt in Entfernung, Bandbreite, Puffergrößen, ...).
Eingesetzte Metriken:

- Zahl der Teilstrecken,
- Zeitverzögerungen (über ECHO-Pakete gemessen),
- Gesamtzahl von Paketen.

Distance-Vector-Routing angewandt in den Internet-Protokollen
RIP (Routing Information Protocol) und
EGP (Exterior Gateway Protocol, leicht modifiziertes Distance-Vector-Routing).
Spezifische Varianten:

- Count-to-Infinity (um auch schnell auf schlechtere Nachrichten zu reagieren).
- Split Horizon Hack (Trick zur Erhöhung Geschwindigkeit des Distance-Vector-Routings).

Link-State-Routing
Es ist der andere wichtige adaptive Routing-Algorithmus. Einsatz im Internet. Ersetzt seit 1979 das Distance-Vector-Routing im ARPA / Internet, weil im DV-Routing

- Leitungsbandbreite unberücksichtigt
  (ARPA: 56 kbit/s ~> 230 kbit/s ~> > 1.544 Mbit/s, Internet 2,5 ~> 10 ~> 100 Gbit/s),
- Distance-Vector-Algorithmus zu langsam (Link-State-Routing kennt vollständige Netz-Topologie und konvergiert schneller).

Election-Algorithmus zur Ermittlung der Distances im ges. Netz: **Probe/Echo**-Verfahren.
Link-State-Routing umfaßt 5 Schritte:

1. Ermittlung aller Nachbar-Router und deren Netzadressen
   - dazu HELLO-Pakete auf jede Punkt-zu-Punkt-Leitung.
2. Ermittlung der Leitungskosten bzw. der Verzögerungen
   - Einbezug eines Timers.
3. Erstellung von Link-State-Paketen (LSP)

   - nach Ermittlung und Austausch der Informationen muss jeder Router ein Paket mit allen Daten zusammenstellen: Identität Sender, Folge-Nr., Alter, Liste der Nachbarn mit den entsprechenden Verzögerungen.
4. Verteilen von Link-State-Paketen (LSP)
   - Paket ist an alle Router zuverlässig zu verteilen (Problem: Router ändern ihre Routen),
   - Basiskonzept ist der Flooding-Algorithmus zur Verteilung.
5. Berechnung des kürzesten Pfades zu allen anderen Routern (z.B. mittels Dijkstra-Algorithmus: shortest Path).

~> Jeder Router kennt nun die vollständige Netztopologie.

Anwendungsbeispiele des Link-State-Algorithmus

OSPF-Protokoll im Internet (**Open Shortest Path First**),

Link-State-Protokoll **IS-IS** (**Intermediate System**)

- Basis für DECnet und für verbindungsloses OSI-Protokoll **CLNP,**
- Internet-Backbones (NSFnet, X-WiN, GÉANT, ...),
- digitaler Zellfunk CDPD,
- Novell Netware (Routing in IPX-Paketen).

6.2.4 Weitere Routing-Algorithmen

Hierarchisches Routing

Anwachsen der Teilnetze ~> Anwachsen der Routing-Tabellen der Router. Unterteilung (hierarchisch) in Regionen; mehrstufig (Regionen, Cluster, Zonen, Gruppen, ...).

Routing mobiler Host's

Mobilitätsverwaltung für Teilnehmer in Zellen / Cluster (handover/off, Roaming, Location Update). Dynamische Adressvergabe: für Internet DHCP (z.B. mobile IP).

- Je Bereich:
  - Fremdagent (visitor agent (bei mobile IP) / visitor location register (bei Zellularfunknetzen)): verwaltet alle sich in seinem Bereich aufhaltenden mobilen Teilnehmer.
  - Heimagent (home agent / home location register): verwaltet mobile Teilnehmer seines Bereiches, auch wenn sie sich momentan außerhalb aufhalten.
- Periodische Meldung der Bewegung der mobilen Teilnehmer (Registrierung).
- Nutzung von Tunneling-Technologien.

Broadcast-Routing (Rundsende-Routing)

Anwendung, wenn Hosts *an alle anderen Host* Nachrichten versenden wollen (z.B. Aktualisierung von DB, Echtzeitanwendungen). *Methoden:*

- bestimmtes Paket an jedes Ziel (--> Verschwendung),
- Flooding,
- Multidestination-Routing (auf Basis einer Liste von Zielen oder Bitmuster),
- Spanning-Tree-Algorithmus (Router weiß, welche Leitungen zu seinen Spanning-Tree gehören),
- Reverse-Path-Forwarding (verbessertes Spanning-Tree: Router braucht Spanning-Tree dann nicht mehr zu kennen, keine Ziellisten erforderlich, einfache Implementation).

Spanning-Tree (überspannender Baum):

Es ist eine Untermenge eines Teilnetzes, das alle Knoten enthält, aber *keine Schleifen* aufweist. Die schleifenlose Topologie kennzeichnet immer genau 1 Pfad zu dem entsprechenden Knoten.

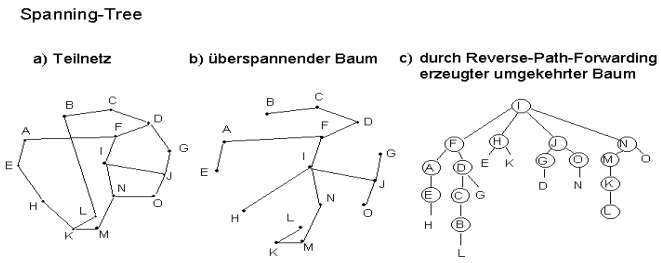


Abbildung 6.2: Spanning-Tree

Multicast-Routing
Übertragung der Nachricht an eine Gruppe ("Multicasting"). Voraussetzung für Multicasting: Gruppen-Management (Anlegen, Löschen von Gruppen und deren Teilnehmern).
Anwendung: Audio/Video-Konferenz: Übertragung nur einfach im Netz an Gruppe; am entsprechenden Multicast-Router erfolgt die Auftrennung an die Mitglieder der MC-Gruppe.
Im Multicast-Routing berechnet jeder Router einen Spanning-Tree, der alle im Teilnetz vorhandenen Router abdeckt. Multicasting mehr für NG Internet maßgeblich.
Spezielle Variante: Core-based-Trees (Ballardie u.a., 1993).

6.3 Überlastüberwachung

6.3.1 Überlaststeuerung (congestion control)

Überlastüberwachung
Bei ausreichender Leitungskapazität werden alle Pakete zugestellt. Bei Überlastung kommt es zum Zustand, dass mehr und mehr Pakete verloren gehen ... , bis keine Leistung mehr erbracht wird. Dazu Überlastüberwachung (**congestion control**) erforderlich => globale Aufgabe aller Knoten (zweite wichtige Aufgabe der Vermittlungsschicht).

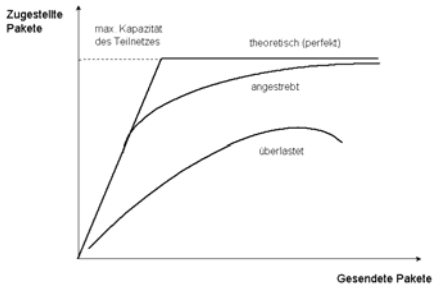


Abbildung 6.3: Überlastüberwachung

Anm.: Flußsteuerung (Schicht DLL) verhindert, dass Sender mehr Daten schickt, als Empfänger aufnehmen kann => Punkt-zu-Punkt - Aufgabe einzelner Sender / Empfänger.
Gründe für Netzüberlastung ("Stau")
- Hohe Paketankunft für gleiche Ausgangsleitung ~> Paketverlust bei geringem Speicher,
- Langsame Prozessoren,
- Niedrige Bandbreiten,
- Kein freier Puffer für neu ankommende Pakete ~> Pakete werden ignoriert (~> Verlust).

Methoden zur Überlaststeuerung
- *Vorab-Zuweisung von Puffern:* Beim Aufbau einer virtuellen Verbindung werden nicht nur Leitweg-Tabellen generiert, sondern auch Pufferbereiche in jedem Router fest zugeordnet (Zeitgeberdienste für Puffer).
- *Freie Zuordnung von Puffern, Verwerfen von Paketen;* Je 1 Puffer pro Eingangsleitung (Huckepack-Rückmeldung). Paket verworfen, wenn kein Puffer verfügbar.
- *Systematisches Verwerfen von Paketen*, die noch nicht weit gekommen sind.
- *Router weist Pakete von benachbarten Quellen zurück*, wenn Anzahl der belegten Puffer einen Grenzwert überschreitet.
- *Choke-Pakete* (zur Verkehrsreduzierung).

Allgemeine Prinzipien der Überlastüberwachung
Aus Sicht der Steuerungstheorie (Automatisierungstechnik) kann man die Lösung in 2 Gruppen unterteilen:
Lösung mit offener Schleife: d.h. Problem soll durch gutes Design von vornherein ausgeklammert werden oder Lösung mit geschlossener Schleife (Korrektur während des Betriebes).
Die Überlastüberwachung untergliedert sich in 3 Teile
1. Überwachung des Systems, um zu erkennen, wann und wo Überlastungen entstehen.
   Parameter: Speicherplatz, verworfene Pakete, Warteschlangen-Länge, Paketverzögerungen, erneut übertragene Pakete, ...
2. Übertragung der Informationen vom Erkennungspunkt an die Stelle, wo Überlastungen behoben werden können,
   z.B. - Informationspakete --> führen aber zur Erhöhen der Last,
   - spezifisches Bit in jedem Paket,
   - periodische Abtastpakete.
3. Behebung der Überlastungssituation: dazu viele Algorithmen
   - offene Schleifen (agieren an Quelle oder Ziel).
   - geschlossene Schleifen (mit expliziter oder impliziter Bestätigung).
     Explizit: hierbei Pakete vom Überlastungs-Pkt. an Quelle zurückgesandt, um zu warnen.
     Implizit: Ableitung aus lokalen Beobachtungen

Überlast := Last > Ressourcen. Behebung durch Erhöhung der Ressourcen (z.B. Bandbreite oder Reserve-Router) bzw. Reduzierung der Last (z.B. Verweigerung des Dienstes, Senkung der Dienstqualität).

Vermeidung von Überlastungen
In offenen Schleifen: Minimierung der Überlast.
Dazu Maßnahmen auf Sicherungs-, Vermittlungs- und Transportschicht (Reduzierung, aber z.T. auch Erhöhung der Last)
Sicherungsschicht:
- Erneute Übertragung (abhängig von Timeout eines Senders; kann zu schwerer Überlast führen).
- Zwischenspeicherung von außer der Reihe gesendeten Paketen (wenn Empfänger zu viele außerplanmäßige Pakete verwirft, müssen diese später erneut übertragen werden => Erhöhung der Belastung).
- Bestätigungen (Bestätigungspakete erhöhen Last; Huckepack und Sammlungen von Bestätigungen können erneute Übertragung veranlassen).
- Flusssteuerung (Anpassung Senderate an Empfangsrate reduziert Datenrate und senkt die Überlastung).

Vermittlungsschicht:
- Wahl zwischen virtuellen Verbindungen und Datagramen (viele Algorithmen funktionieren nur bei virtuellen Verbindungen).
- Warteschlangen und Dienste für Pakete (abhängig, ob Warteschlange je Ein / Ausgangsleitung vorhanden).
- Verwerfen von Paketen (Problem: welche Pakete zu verwerfen, wenn ungenügend Platz).
- Routing-Algorithmus (Verteilung der Last auf alle Leitungen).
- Verwaltung der Lebensdauer von Paketen (bis es verworfen wird; falls Dauer zu lang => Timeout => erneute Übertragung erforderlich).

Transportschicht:
- Maßnahmen wie auf Sicherungsschicht: Erneute Übertragung, Zwischenspeichern von außer der Reihe gesendeten Paketen, Bestätigungen, Flusssteuerung.
- zusätzlich: Timeout (schwierig vorhersagbar, da nicht nur zwischen benachbarten Routern).

6.3.2 Algorithmen zur Überlastüberwachung (Auswahl)

Traffic-Shaping (Verkehrs-Anpassung)
- Ausgleichen der Verkehrsspitzen, in dem die Stationen gezwungen werden, in besser vorhersagbaren Raten zu übertragen,
- Anwendung in ATM-Netzen und im NG Internet (IPv6) ~> zur Realisierung von QoS,
- Regulierung der durchschnittlichen Rate, d.h. Begrenzung der Übertragungs-Rate, nicht der Datenmenge (wie bei Schiebefenster),
- Wichtig für Echtzeitdaten (z.B. audio / video),
- Für Netzbetreiber ist das Einhalten der Shaping-Vereinbarungen durch das Traffic-Policing wichtig,
- Bekannte Algorithmen (Auswahl):
  - *Leaky-Bucket-Algorithmus:*
    Leaky-Bucket-Algorithmus erzielt Durchschnittsrate, unabhängig von Verkehrsspitzen. Realisierung über Warteschlangentechnik.

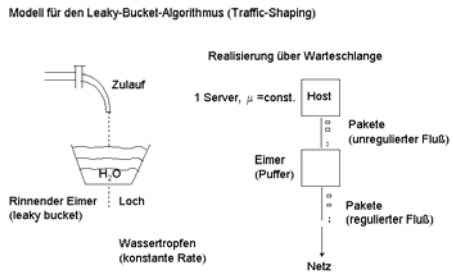


Abbildung 6.4: Leaky-Bucket-Algorithmus

  - *Token-Bucket-Algorithmus:*
    Ermöglicht beschleunigte Ausgaben bei Verkehrsspitzen. Dazu erhält Eimer alle Δt ein *Token.* Falls Token, dann Übertragung. Falls Eimer voll, werden Token weggeworfen (aber keine Pakete) - im Gegensatz dazu verwirft der Leaky-Bucket-Algorithmus Pakete, wenn Eimer voll ist. Falls Eimer voll, dürfen keine Pakete mehr gesendet werden.

Flussspezifikation
Übereinkunft zwischen Sender, Empfänger und Teilnetz für Verkehrsausgleichung (Traffic Shaping). Es ist eine Datenstruktur, die den eingespeisten Verkehr und auch die Dienstequali-

tät beschreibt. Anwendung bei virtuellen Verbindungen und Folgen von Datagrammen. Parameter der Spezifikation:
- maximale Paketgröße (Byte)
  Token-Bucket-Rate (Byte/s) und Token-Bucket-Größe (Byte)
  Maximale Übertragungsrate (Byte/s)
- Dienstqualität (Verluste, Verzögerungen, Abweichungen).

Überlastüberwachungen mit virtuellen Verbindungen (dynamische Überlastkontrolle)
2 Verfahren:
- Admission Control (Zugangssteuerung)
  - Regelung der Verbindungsaufnahme. Wenn Überlast angezeigt, dann keine weiteren virtuellen Verbindungen mehr aufgebaut.
  - Anwendung beispielsweise im Telefonsystem.
- Verhandlung einer Vereinbarung
  - zwischen Host und Teilnetz,
  - zum Aufbau einer virtuellen Verbindung.

Preis dieser Überlast-Überwachung: ungenutzte Bandbreite.

Choke-Pakete
Gültig für virtuelle Verbindungen und Datagramme. Jeder Router überwacht seine Ausgangsleitungen und Ressourcen (z.B. Schwellbereich für Auslastung). Falls Überschreitung, wird Choke-Paket an Quellhost geschickt. Dieser reduziert Verkehr um X %.

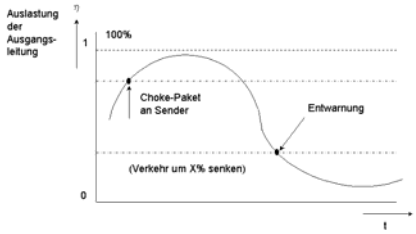


Abbildung 6.5: Choke-Pakete

Variationen:
- *Weighted Fair Queueing* (Nagle, 1987): Router haben für jede Quelle eine Warteschlange (Anwendung: ATM-Vermittlung). Falls eine Leitung frei, werden Warteschlangen ringsum abgefragt und das 1. Paket aus nächster Warteschlange entnommen.
- *Hop-by-Hop - Choke-Pakete:* Bei hohen Geschwindigkeiten und großen Entfernungen ist Versenden Choke-Paket nicht geeignet, weil Reaktion zu langsam. Deshalb Hop-by-Hop - Choke-Paket: wird auf jeder Teilstrecke wirksam.

Weitere Algorithmen
- *Load Shedding:* Verwerfen von Paketen, die nicht bewältigt werden, durch den Router (z.B. bei ATM).
- *Jitter-Kontrolle*: Pakete transportiert innerhalb eines Verzögerungsbereiches, Berechnung der erwarteten Übertragungszeiten für jede Teilstrecke ~> Entscheidung auf Grund der berechneten Übertragungszeiten.
- *Resource Reservation Protocol (RSVP)*
  Senden an Empfangsgruppen, Aufbau Spanning-Trees, Problem: Skalierbarkeit. Anwendung bei Multicasting (Zhang, 1993), Next Generation Internet (IPv6).
- Neue Dienste:
  IntServ (Integrated Services ~> RSVP)

DiffServ (Differentiated Services)
PHB: Per-Hop Forwarding Behavior – Weiterleitungsstrategie des Datenstroms durch Router ~> End-to-End-Dienste als Expedited bzw. Assured Forwarding PHB, ähnlich den IntServ-Diensttypen ...
Realisierungen im Q-WIN bzw. CoS (Class-of-Services $_{\text{UniLeipzig/DFN}}$)

-Bandbreiten-Management
Verwaltung der Bandbreite
SLS (Service Level Specification),
MPLS (Multi Protocol Layer Switching), ... Projekt Alabama $_{\text{UniLeipzig, RNVS}}$
Überdimensionierung (Overprovisioning)

6.4 Protokolle der Vermittlungsschicht

Protokolle und Netze der Vermittlungsschicht (Auswahl)

X.25	OSI-Standard, i.allg. für öffentlich/staatliche Paketvermittlungsnetze (PVN) (in DE: PVN Datex-P, Betreiber: Deutsche Telekom AG).
Frame Relay	Öffentliches PVN (~ X.25), mit reduzierter Fehlerbehandlung.
SNA	IBM-Netz
Internet:	IP (IPv4, IPv6), Steuerprotokolle ICMP, ARP, RARP Internet Multicasting, Mobile IP / Cellular IP Gateway-Protokolle: OSPF Internes Gateway Routing Protokoll BGP Externes Gateway Protokoll

6.4.1 Protokollfamilie X.25

Merkmale

Charakteristik X.25
- Netzwerk-Architektur für Schicht 3 (bzw. 1 ... 3) OSI.
- Standard der ISO / CCITT (ITU-TS).
- Weltweiter Standard für Paketvermittlungsnetze, analog zu den Standards für Telefon /Telefax-Netze.
- Weitgehend zurückgedrängt durch IP (Internet), insbes. durch WWW.

Dienstklasse (in X.25 - Schicht 3): Verbindungsorientiert
- Virtuelle Verbindung (switched virtual circuits, SVC, “Virtual Call”).
- Permanente virtuelle Verbindungen (permanent virtual circuits, PVC).

X.25 - Paketvermittlungsnetze (Auswahl)
Deutschland (Datex-P), Frankreich (Transpac), Spanien (CTNE), Kanada (Datapac).

Protokollhierarchie

Protokoll-Architektur:

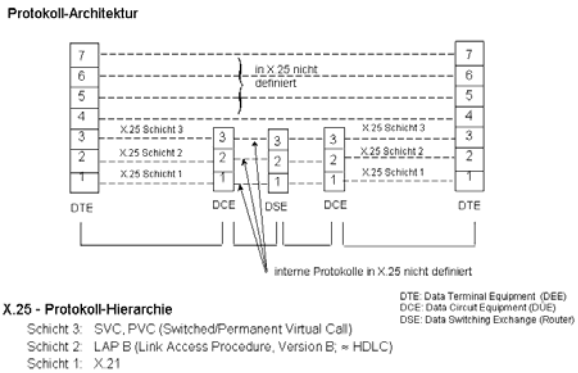


Abbildung 6.6: X.25-Protokollfamilie

X.25-Verbindung:

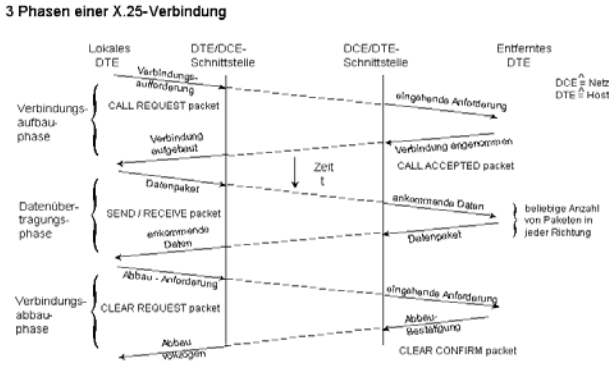


Abbildung 6.7: Phasen einer X.25-Verbindung

X.25 Paketformate:

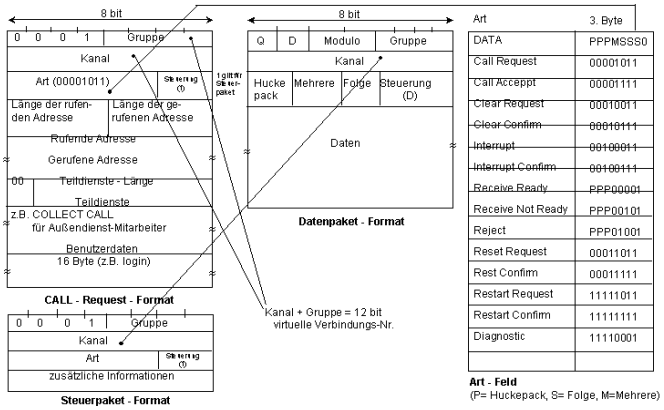


Abbildung 6.8: X.25 Paketformate

Datex-P
Flächendeckendes X.25 - PVN (Paketvermittlungsnetz) der Deutschen Telekom AG.
DÜ-Raten: 300 bit/s ... 64 kbit/s (ab Mitte 90er: 1.92 Mbit/s).
1994: 160 Datex-P-Knoten
PAD-Anschluss für Nicht-X.25-Geräte
X.25-Einsatz: IXI/EuropaNET, NorduNET, Basis für S-WiN
1996: B-WiN (X.25 -> ATM), 2000: G-WiN (ATM -> SDH/WDM), 2006: X-WiN (dark fibre)

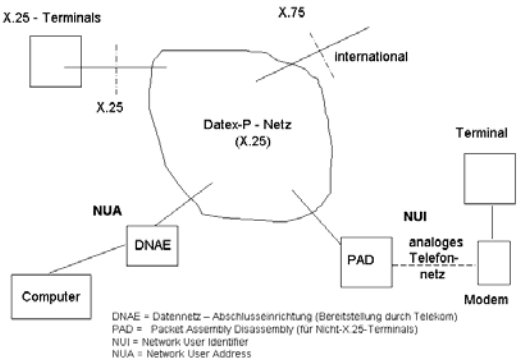


Abbildung 6.9: Datex-P

PAD-Anschluss: Telekom stellt dem Nutzer eine NUI (Teilnehmererkennung) bereit; darüber werden auch die Gebühren abgerechnet.
Rechner-Direktanschluss: über Datenadresse NUA (Network User Address).
Wählt man sich über eine PAD ein, muss anschließend die NUA eingegeben werden. Vorgang: PAD anwählen, eigene NUI und Passwort eingeben, NUA eingeben.

6.4.2 Frame Relay

Aufgabe: Verbindung von LAN's über große Entfernungen, $DÜ_{FR} > DÜ_{X.25}$.
Nachteil X.25: Aufbau des LAN-WAN-Verbindungspaketes ist sehr zeitaufwendig. Daher LAN-X.25 Verbindungen häufig auf 64 kbit/s begrenzt.

Merkmale Frame Relay

- Netzzugangsprotokoll (--> Access Network).
- Anschlussgeschwindigkeit: 56 kbit/s ..... 2 048 kbit/s (--> 45 Mbit/s).
- Verbindungsorientiert, PVC (permanent virtual circuit).
- X.25 ähnlich, aber weniger Fehlersicherungsmaßnahmen (infolge verbesserter Netze nicht mehr unbedingt erforderlich):
  - keine automatische Rahmenwiederholung (ack),
  - keine Fehlererkennung,
  - kein Schiebefenstermechanismus,
  - keine Flusskontrolle,
- Verlorengegangene Rahmen müssen von Schicht 4 ... 7 behandelt werden.
- Ausgelegt für hochwertige Übertragungsleitungen.
- Verwendung von Q.922 - Rahmen (Weiterentwicklung von LAP B).
- Rahmengröße 5 . . . 8 192 Bytes (verträglich mit ATM).
- Nur für asynchrone Datenverbindungen geeignet (keine Sprache, keine isochrone Dienste).

Einsatzvergleich X.25 – Frame Relay

- X.25 wurde für stark fehlerbelastete Leitungen entwickelt (z.B. analoges Telefon-Netz). Führende Rolle von Deutschland und Europa.
- Bei Umstellung auf digitale Leitungen war X.25 in USA noch wenig verbreitet => daher leichtere Einführung von Frame Relay.
- Frame-Relay-Angebot der Telekom erst seit Mitte 1995. Telekom setzt auf ADSL (<--> "Concert" FR - NW der VIAG Interkom).
- S-WiN: X.25; keine Umstellung auf Frame Relay, da B-WiN-Netz ATM (34 Mbit/s, 1996).

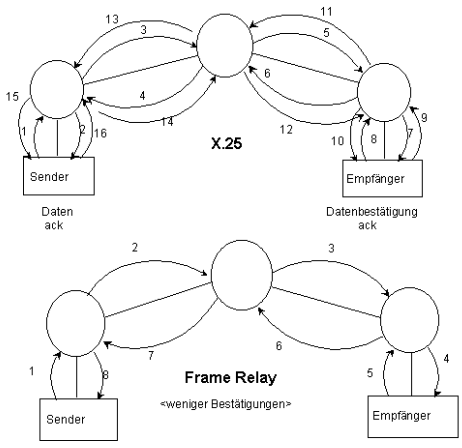


Abbildung 6.10: Ablauf-Vergleich X.25 und Frame Relay

6.5 Vermittlungsschicht im Internet

6.5.1 Das Internet

Internet im Überblick

Internet := zusammengeschlossene Sammlung vieler Netze auf Basis TCP/IP, die miteinander verbunden sind (sog. "TCP/IP"-Netze):

- es gibt keine echte Struktur,
- viele Backbones, gebildet aus Leitungen hoher Bandbreite und schnellen Routern,
- daran regionale Netze, LAN / MAN von Universitäten, Forschungseinrichtungen, ..., Internet-Service-Provider angeschlossen,
- das alles zusammenhaltende Protokoll ("sog. Klebstoff") ist das Protokoll der Vermittlungsschicht: das **IP (Internet Protocol)**.

Ursprung und Entwicklung:

- ARPAnet (Advanced Research Project Agency, Department of Defense)
  - Inbetriebnahme 1969 (4 Knoten), L. Kleinrock
  - Basisdienste: Telnet, FTP, SMTP (Email, RFC 822 Postformat),
- Steuerprogramm NCP --> TCP/IP (--> Begriff "Internet", Organisation durch IETF),
- NSF (National Science Foundation): Backbone NSFnet (~> ANSnet ~> Worldcom ...).

Keine zentrale Verwaltung/Steuerung (Adressenvergabe durch IETF/remote und IEEE/lokal).

Arbeitsweise

- Dominierende Protokolle:
  - Vermittlungsschicht (OSI/3): IP
  - Transportschicht (OSI/4): TCP, UDP
- Die Transportschicht des Internet (Protokolle TCP, UDP) nimmt von Anwendung die Datenströme entgegen und teilt sie in Datagrame (sog. Segmente) auf:
  Datagramgröße: i.d.R. ca. 1 500 Byte, max. 64 KByte
- Schnittstellen:
  - zwischen Anwendung und Transportschicht: T-SAP (SAP: Service Access Point)
    Bereitstellung einer Socket-Schnittstelle (Socket-Nr., IP-Adresse).
  - zwischen Transport- und Vermittlungsschicht: N-SAP (Datagram).
- Jedes Segment wird mit TCP-Header versehen und an IP-Schicht übergeben (mit IP-Adresse) bzw. vorbereitet.
- IP-Schicht fügt IP-Header an und übergibt dies der Schicht 2, die ihrerseits ihren Header anfügt (z.B. Ethernet-Header).

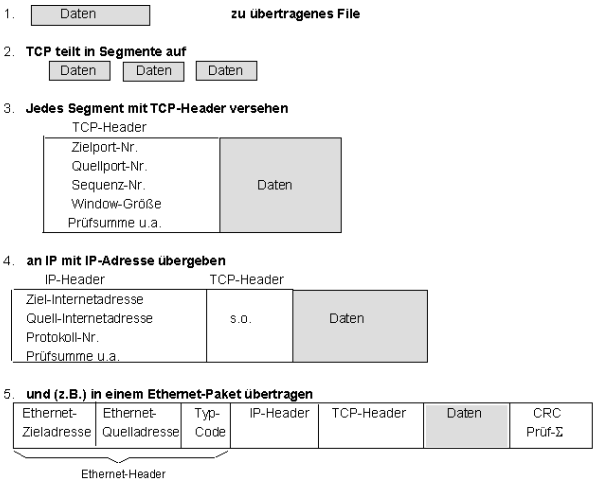


Abbildung 6.11: Datenstrukturierung

Internet-Protokolle

Schicht 4: TCP - Transmission Control Protocol
UDP - User Datagram Protocol

Schicht 3: IP - Internet Protocol (IPv4 -> IPv6, Migration fortlaufend)
Steuerprotokolle (IPv4): ICMP, ARP, RARP, BOOTP
Gateway-Routing – Protokolle: OSPF (Nachfolge für RIP), BGP
Internet - Multicasting
Mobile IP
CIDR - Classless InterDomain Routing

Schicht 2: Protokolle der DLL, u.a. Ethernet, HDLC, ATM, . . .
Für Wählzugang (Modem): SLIP, PPP

6.5.2 IP (Internet Protocol)

Internet Protocol Version IPv4

- Verbindungsloses Protokoll (RFC 791),
- Zerlegung (Fragmentierung) der Segmente in Pakete bei Bedarf,
  Paketgröße: max. 65 535 Byte (64 KByte), i.d.R. 1 500 Byte, Default 576 Byte
- Adressierung: 32 Bit Internet Adresse (IPv4) 128 Bit (IPv6),
- Prüfsumme: lediglich Kopfprüfsumme, keine Datenprüfsumme,
- Endliche Lebensdauer eines Paketes (time-to-life),
- Zustellung: Best Effort
  * Pakete können verloren gehen, in falscher Reihenfolge oder dupliziert ankommen,
  * Keine Fehlerbehandlung (im Gegensatz zu X.25), sondern ist durch höhere Schichten zu realisieren (i.d.R. durch TCP).

OSI-Äquivalent: CLNP (Connectionless Network Protocol): Verbindungsloses OSI-Protokoll als Äquivalent zum X.25-Standard (nicht durchgesetzt), Datagram-Protokoll des OSI.

Aufbau IP-Datagram

IP Header: fester Teil: 20 Byte, optionaler Teil: variable Länge

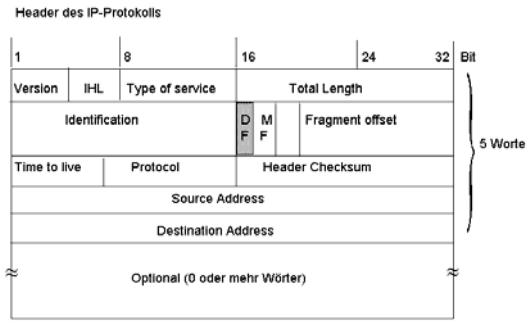


Abbildung 6.12: Aufbau IP-Datagram (IPv4)

Versionsfeld: Versions-Nr. des IP-Protokolls (z.B. Nr. 4 für IPv4), zu dem das Datagram gehört

IHL: Header-Länge in 32-bit-Wörtern (mind.: 5, max.15)

Service: Gewünschter Dienst (zuverlässig, Geschwindigkeit, Durchsatz)

Length: Gesamtlänge des Datagramms (max. 64 KByte)

Identification: für Zielhost, um Fragmente zu identifizieren

Protocol: Kennzeichnung des zugehörigen Transportprotokolls, z.B. Weitergabe an TCP (=6) oder UDP (=17), ICMP (=1); ca. 30 Protokolle definiert.

DF, MF, Fragmentabstand: erlaubt, IP-Datagramm in mehrere Teile aufzuteilen, durchzunummerieren und am Ziel wieder zusammenzusetzen.

IP-Adresse
Jeder Host und Router im Internet hat eine (eindeutige) IP-Adresse.
Aufbau:

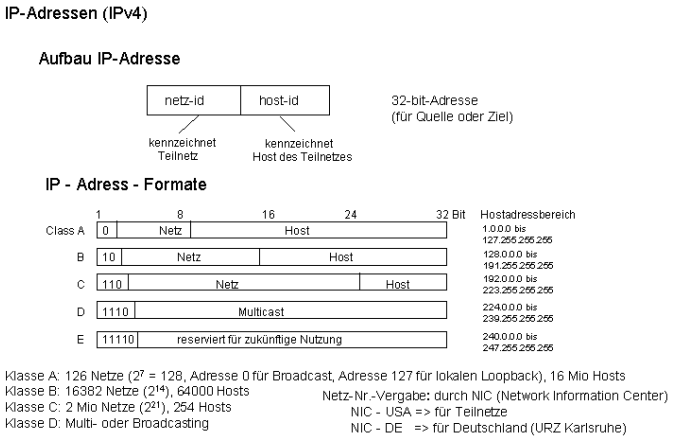


Abbildung 6.13: Aufbau IP-Adresse

Adressbildung IPv4
Darstellung (am Beispiel):
bitweise 10010110 11001000 01100100 00100001
hexadezimal 9 6 C 8 6 4 2 1
üblicherweise in 4 gepunkteten Dezimalzahlen (dotted decimal notation): 150.200.100.33
Übertragung:
Adresse wird in sog. "**Network Byte Order**" übertragen (werthöchste Stelle zuerst). Für TCP/IP gilt als Network Byte Order das sogenannte "**Big Endian Format**", d.h. das werthöchste Byte / Bit wird zuerst gesendet.

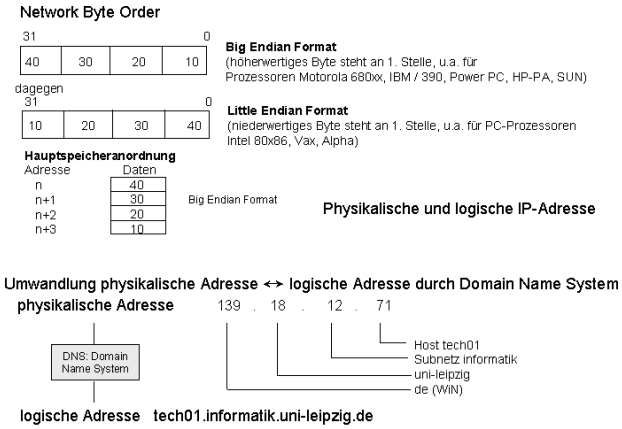


Abbildung 6.14: Adressbildung

Physikalische und logische Adresse:
Umwandlung physikalische Adresse <--> logische Adresse erfolgt mit Hilfe des DNS (**Domain Name System**) - Bestandteil der Anwendungsschicht.
Eine Netzadresse ist einem Teilnetz (z.B. Ethernet-Segment) zugeordnet. Alle Host eines Segments haben gleiche Netz-Adresse (net-id). Jeder an das Teilnetz angeschlossene Host hat eine eindeutige Host-Adresse (host-id). Falls Host (z.B. Router) an mehrere Netze angeschlossen ist, hat er mehrere Netz-Adressen.

IP-Adressen sind unabhängig von physikalischen HW-Adressen (z.B. Kabeladressen). IP-Konventionen sind in RFC-Dokumenten (Request for Comments) definiert. Zur Adressabbildung auf physikalische HW-Adressen existieren RFC-Dokumente für Ethernet, Token-Ring, FDDI, HDLC, ATM-Zellen u.a.

Subnetze und Subnetz-Adressierung
Problem: Anzahl der Host im Netz begrenzt, z.B. C-Netz: 254 Host. Wenn Anzahl Host steigt, ist neue Netzkonfiguration erforderlich (komplizierter administrativer Vorgang: NIC, Konfigurierung, Bekanntgabe IP-Adressen). Abhilfe: Dynamische Vergabe von IP-Adressen (DHCP) oder Teilnetze (Subnetzadressierung).
Subnetzadressierung:
Host-id (z.B. 16 bit) aufgeteilt in Subnet-id (z.B. 6 bit) und Host-id (z.B. 10 bit). Außerhalb des Netzes ist die Netzbildung nicht erkennbar, es muss vom NIC keine neue IP-Adresse eingeholt werden.
Wenn IP-Paket eintrifft, wird seine Zieladresse in Routing-Tabelle nachgeschlagen:
- falls lokaler Host: Paket direkt weitergereicht,
- falls entfernter Host: an nächsten Router weitergereicht,
- falls das Netz nicht vorhanden: dann an Vergabe-Router (besitzt ausführliche Tabelle).

Bei Subnetzen werden die Routing-Tabellen geändert. Adresserkennung erfolgt durch ein boolesches AND mit der Subnetz-Maske im Router. Damit leichte Lokalisierung möglich.
Moderne IP Routing-Protokolle (aber nicht RIP, EGP) erlauben eine solche Adressierung von Subnetzen. Hierbei besteht die IP-Adresse aus der eigentlichen 32 Bit-Adresse und einer 32 Bit-Subnetzmaske 111 . . . 11 00 . . . 0

6.5.3 Protokoll IPv6

Ausbau des Internet zum Next Generation Internet
Ausgangspunkt: klassisches Internet (IPv4). Internet-Gurus wollen dies unverändert lassen ("keep simple", reines Transportnetz). Vollkommene Zielstellungen noch nicht endgültig definiert; verschiedene Vorschläge von IETF diskutiert, u.a.
- IPv6: vergrößerte Adressbreite, Prioritäten usw.
- Dienstgüte und Reservierungsstrategien, wie RSVP, IntServ, DiffServ, ...
- Sicherheitskonzepte, Mobilität, Prioritäten
- Hochgeschwindigkeitsbackbone.

Protokoll IPv6
- größere Adresse: 16 Byte / 128 Bit (statt 4 Byte / 32 Bit wie bei IPv4),
- vereinfachter Header --> effektivere Abarbeitung,
- Unterstützung durch Optionen,
- Sicherheit (Authentification und Security),
- Dienstgüte (Prioritäten, Flow Label),

⇨ Zielstellung für Hochgeschwindigkeitsnetze mit IP-Diensten (Gigabit, SDH/WDM, Internet-2).

Bei der Schaffung des Internet war explosionsartiges Anwachsen nicht vorhersehbar. Hauptproblem: fehlende Adressen. Classless Inter Domain Routing (CIDR) schafft zwar etwas Luft. Aber mit kommerzieller Nutzung des Internet sind die Tage von IPv4 gezählt.
Die IETF begann 1990 mit Entwicklungsarbeiten für das neue Internet Protocol IP, das insbesondere für Echtzeitanwendungen, Video- und Gruppenkommunikation geeignet sein sollte.
Verschiedene Lösungsvorschläge (1992), u.a

- TCP auf **CLNP** aufsetzen (Connectionless Network Protocol). 160-bit-Adresse wäre für "ewig" ausreichend, aber "OSI"-Lösung, und schlechte Dienstarten-Unterstützung für Multimedia-Daten.
- **SIPP** (Simple Internet Protocol Plus) nach Deering / Francis (1995). Als IPv5 bereits experimentell genutzt. Dieses wurde dann als **IPv6** bezeichnet.

6.5.4 Internet-Steuerprotokolle

IPv4 durch verschiedene Steuerprotokolle begleitet, u.a. ICMP, ARP, RARP, BOOTP, DHCP.

ICMP (Internet Control Message Protocol)
Definiert in RFC 792, als Protokoll zum Senden von Nachrichten (i.allg. durch Router), falls bestimmte Ereignisse auftreten (z.B. Fehler). Auch für Testzwecke nutzbar, u.a. ping (z.B. MS-DOS> ping adler).
ca. 15 ICMP-Nachrichten definiert, z.B. Paket nicht zustellbar, Choke-Paket, ...

ARP (Address Resolution Protocol)
Definiert in RFC 826. Aufgabe: Adressenabbildung IP --> Ethernet
Geg.: IP-Adresse (32-bit-Adresse, nicht an HW gebunden, Verwaltung durch ISOC/NIC),
Ges.: Ethernet-Adresse (48-bit-Adresse, an HW (Ethernet-Karte) gebunden, Verwaltung durch IEEE)
Zuordnung beider Adressen erfolgt durch SW-Routine und ARP-Protokoll:
- Zuordnung befindet sich in ARP-Tabelle;
- Fehlt der Eintrag, sendet ARP eine Rundsendeanfrage an alle Ethernet-Adressen des Netzes. Diese Nachricht wird von IP bearbeitet und an den entsprechenden Knotenrechner zurückgemeldet.

ARP ist vorteilhafter als Konfigurationsdateien und i.d.R. in allen IP-Knoten vorhanden. Damit auch einfacher ein Austausch einer Ethernet-Karte möglich.
Einem Rechner mit einer einzigen Ethernet-Adresse können mehrere IP-Adressen zugeordnet werden. ARP-Einträge befinden sich in einem *Cache*, normalerweise im Hauptspeicher. Die Einträge werden nach vorgegebener Zeit gelöscht. Dann ist Adressauflösung durch wiederholte Aufrufe des ARP-Protokolls erneut durchzuführen. Hierdurch werden die Adresszuordnungen automatisch immer auf den neuesten Stand gehalten.

RARP (Reverse Address Resolution Protocol)
RARP (RFC 903) ist die Umkehrung zur ARP (Geg: Ethernet, Ges: IP). Ermittlung IP-Adresse für eine bestimmte Ethernet-Adresse. IP-Adresse ist i.allg auf externen Plattenspeicher oder im Betriebssystem abgespeichert. Somit Adresse erst suchen -> RARP-Server erforderlich.
Verbesserung durch Bootstrap-Protokoll BOOTP (RFC 951, 1048 und 1084):
- Benutzt UDP-Nachrichten,
- Liefert die IP-Adresse des Dateiservers, auf dem sich die IP-Adresse des Vergabe-Routers befindet.

Alternativen zu RARP:

BOOTP Bootstrap Protocol
Anwendung in Schicht 7, Nutzung Schicht-4-UDP, leichte Implementierung (RARP wird mit Schicht-3-IP integriert).

DHCP Dynamic Host Configuration Protocol
Dynamische Zuordnung von IP-Adressen, Vergabe freier IP-Adresse (ggf. zeitbedingte Zuordnung, "Lease"), Automatische Konfigurierung,

DHCP-Discovery: suche nach DHCP-Server im Einzugsbereich, Bereitstellung zusätzlicher Konfigurierungsparameter.
Einsatz DHCP im mobile IP.

Internet Multicasting
Verwendung der Adressklasse D (Internet-Adresse Klasse D): Senden an Gruppe adressierter Mitglieder. Für Gruppen: 28 Bit => über 250 Mio. Gruppen.
2 Gruppenadressen:
permanente Adressen (existieren immer) und
temporäre Adressen (Gruppen immer neu zu erstellen).
Multicasting erfolgt durch spezielle Multicast-Router.
Für Anfragen / Antwort - Pakete steht das *IGMP (Internet Group Management Protocol)* zur Verfügung (etwa ähnlich dem ICMP): RFC 1112.
Multicast-Routing erfolgt über Spanning-Trees. Jeder Multicast-Router tauscht mit seinem Nachbarn Informationen über ein modifiziertes Distance-Vector-Protocol aus. Dabei Nutzung von Tunneling-Verfahren, um Knoten zu umgehen, die nicht im Spanning-Tree enthalten sind.

CIDR - Classless Inter Domain Routing
Problem: exponentielles Wachstum des Internet, insbes. durch kommerzielle Nutzung: Email, Web ~> bald keine freien IP-Adressen mehr verfügbar. Vergeudung von IP-Adressen, insb. in Klasse-B-Netzen (für viele Unternehmen zu groß).
Verschiedene Lösungen entwickelt, die aber wieder neue Probleme schaffen. Ein wenig Atemfreiheit bringt das CIDR (RFC 1519).
Basiskonzept:
Die verbleibenden Klasse-C-Netze (~ 2 Mio.) werden in Blöcke mit variablen Längen zugewiesen. Dabei Verwendung von Blöcken aufeinanderfolgender Klasse-C-Netze.
Zusätzlich: Aufteilung des Adressraums der Klasse-C in Zonen

Adressen	194.0.0.0	bis	195.255.255.255	für Europa
	198.0.0.0	bis	199.255.255.255	für Nordamerika
	200.0.0.0	bis	201.255.255.255	für Mittel- und Südamerika
	202.0.0.0	bis	203.255.255.255	für Asien und Pazifik

Somit für jede Region ca. 32 Mio. Adressen, weitere 320 Mio. Adressen der Klasse C in Reserve (204 .... 223).
Einfacheres Routing: Routing-Tabellen werden mit 32-Bit Maske erweitert. Mittels CIDR werden die alten Netze der Klasse A, B, C nicht mehr zum Routing verwendet.
Alternative Lösung: DHCP.

6.5.5 Mobilität im Internet

mobile IP
Nutzung IP-Protokoll zum Anschluss portabler Endgeräte über Funkverbindung. Problem liegt im Adressierungsschema des IP.
Jede IP-Adresse hat 3 Felder: Netz - Klasse, Netz - Nr., Host - Nr.
Bei Ortswechsel sind damit mobile Rechner nicht erreichbar. Nutzt man die vollständige IP-Adresse für das Routing, wären zu viele Einträge zu verwalten. IETF-AG stellte Ziele:
- jeder mobile Host muss seine Heimat-IP-Adresse in jedem beliegen Ort nutzen können,
- SW-Änderungen in festen Hosts, Routern, Tabellen nicht zulässig.

Lösung:
- Jeder Standort, der seinen Benutzern einen mobilen Anschluss gewähren will, muss einen Heimagenten erstellen.

- Jeder Standort, der einen Besucher zulassen will, muss einen Fremdagenten erstellen.
- Beide Agenten kontaktieren miteinander (Nutzung ARP: spezielles Gratuitous ARP).

Verschiedene Lösungsvorschläge für mobile IP-Protokolle (gemäß Columbia-Proposal).
Ziel: Transparenz für feste und mobile Stationen bzgl. Teilnehmer und Anwendung.
~> Realisierung durch Configuration and Resource Management.
Unterstützung durch folgende Maßnahmen:

1. Mobile Internet Protocol (mobile IP)
   - *Erweiterung des Festnetz*-IP (Netzwerk-Schicht, Layer 3) durch mobile IP: mobiler Teilnehmer behält seine IP-Adresse auch bei Wechsel des Subnetzes bei (Transparenz zu höheren Schichten und zu stationärer / mobiler Rechner).
   - Klassische IP-Adresse für *Zieladressierung* (Subnetz) und *Routing* (Host) im Festnetz. IP-Adresse dient für den Festnetz-Rechner zur
     - *Lokalisierung / Adressierung* (location identifier),
     - *Charakterisierung / Name* (endpoint identifier).

     Keine Probleme bei gleichzeitiger Verwendung der IP-Adresse als Adresse und Name.
   - Mobilstation (Migration zwischen Subnetzen): IP-Adresse nicht mehr gleichzeitig als Adresse und Name für den Rechner verwendbar, da sich Aufenthaltsort (Subnetz) verändert (insbes. wenn Dienst zu adressieren ist). Lösungsvarianten für Mobilstation (Fortsetzung)
     - 1. Lösungsmöglichkeit: Mobiler Rechner erhält je Subnetz eine neue Adresse dynamisch zugewiesen (z.B. DHCP):
       -> häufige Aktualisierung aller Name-Server, Informierung aller höheren Schichten.
       -> Transparenz-Verlust.
     - 2. Lösungsmöglichkeit:
       Mobiler Rechner behält IP-Adresse, unabhängig vom Subnetz, in dem er sich befindet -> Vielzahl von Realisierungsvorschlägen, z.B.: Columbia-Proposal.
2. Ressourcen - Management
   - Gleiche Arbeitsumgebung für mobilen Teilnehmer, unabhängig vom aktuellen Aufenthaltsort.
   - Mitbewegen der Dienste (Service-Mobilität), z.B. DB-Zugriffszeiten unabhängig vom Ort. Erreicht dadurch dass Prozesse, Daten oder Arbeitsumgebung dem TN folgen.
   - Dynamische Replizierung wichtiger Informationen (Synchronisation, Datenkonsistenz), ermöglicht Nutzung lokal vorhandener Ressourcen durch mobilen TN (z.B. Drucker).

mobile IP (Lösungsansatz nach Columbia Proposal)
Mobiler Rechner behält IP-Adresse, unabhängig vom Subnetz, in dem er sich befindet:

- Die MH in Umgebung eines MSR bilden ein virtuelles Subnetz.
- MSR verbinden MH und bilden Gateway zwischen mobilen Subnetzen und Festnetz.
- MSR senden Datenpakete an MHs (übernehmen Adressierungs- und Routing-Fktn.).

Legende: MH:Mobile Host (Mobilrechner); MSR: Mobile Support Router ; FH: Fixed Host

Lösung: Vertreter des mobilen Rechners im Heimnetz ist der Heimagent (HA, über seine IP-Adresse erreichbar) ~> verwaltet Aufenthalt im Fremdnetz (Fremdagent) über Care-of-Adresse; diese muss im HA registriert sein. Air Interface zwischen Fremdagent und MH.
Arbeitsschritte: Agent Discovery, Registrierung, Tunneling.

* Anmeldung MH beim nächstliegenden MSR, periodische Bestätigung (Fremdagent, Care-of-Adresse, Heimagent; Signalisierung).
* Senden Daten von Festnetzrechner an MH über nächstliegenden MSR:
  - falls MH dort registriert ist (*Registrierung*), erfolgt sofortige Auslieferung.
  - ansonsten Bestimmung des aktuellen Aufenthaltsortes (über MSR) durch Befragung aller MSR (*Agent Discovery*).

* Falls dann Ziel-MSR bekannt, wird Datenpaket gekapselt und zum MSR geschickt (*"IP-Tunneling"*). MSR entkapselt Datenpaket und Auslieferung an MH.
* Senden MH an Festnetzrechner direkt über Internet, nicht über Heimagent.
* Verringerung des Suchaufwandes durch folgenden Mechanismus: falls MH sich von einem Subnetz zum anderen bewegt (d.h. zu anderem MSR), meldet neuer MSR automatisch den neuen Ort an vorherigen MSR (--> Einsparung von Lokalisierungsanfragen).

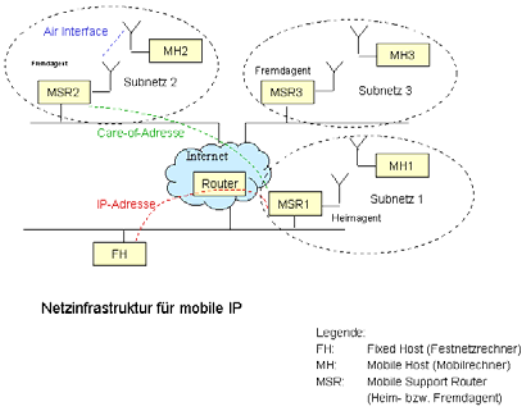


Abbildung 6.15: Mobile IP (Columbia Proposal)

Günstiges Verfahren für Bewegungen in engerer Umgebung, weniger ideal für große Versorgungsbereiche (ggf. Kombination mit Cellular IP).

Versionen von mobile IP
Mobile IP für viele Anwendungen mit mobilen Rechnern geeignet, z.B. Email, DB-Zugriff. Andere Anwendungen benötigen noch zusätzliche Maßnahmen in den höheren Schichten (z.B. Transportschicht: Indirect TCP) und in der Infrastruktur.
Verschiedene Mobile-IP - Vorschläge (Standardisierungen):

* Mobile*IP
* Short Cut Routing - Protocol (IBM - MHP)
* Virtual Internet Protocol (VIP)
* Transparent Internet Routing for mobile Hosts (MRHP)
* RoamAbout Mobile IP
* Internet Mobile Host Protocol (IMHP)
* IP Mobility Support - IETF Draft

Reduktion der Signalisierungsvorgänge zwischen Heim- und Fremdagent bei Wechsel der Funkzelle durch Kombination mobile IP / cellular IP. Gateway (Care-of-Adresse) des Zugangsnetzes kennt Aufenthalt der MH in den Funkzellen (Routen in Cache-Speichern gehalten). Heimagent führt Gateway-Adresse. Signalisierung zum Heimagent (Globales Netz) nur bei Wechsel des Zugangsnetzes.

6.5.6 Inter/Intra-Domain-Routing

Struktur des Internet
Internet besteht aus einer großen Zahl autonomer Systeme. Ein **Autonomes System (AS)** besteht aus einer Gruppe von Netzen und Routern, die als Einheit administriert werden. Es kann intern einen eigenen Routing-Algorithmus verwenden => dazu internes Gateway-Protokoll.
Interne Gateway - Protokolle (IGP), z.B.
RIP Routing Information Protocol ~> Basis: Distance-Vector-Protocol
OSPF Open Shortest Path First ~> Basis: Link-State-Protocol

Das Routing zwischen autonomen Systemen erfolgt über ein Externes Gateway Protokoll.
Externe Gateway - Protokolle, z.B.
EGP Exterior Gateway Protocol bzw. sein Nachfolger
BGP Border Gateway Protocol

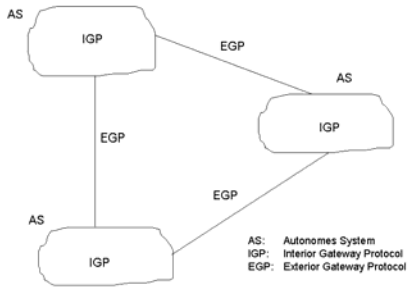


Abbildung 6.16: Routing-Protokolle in IP-Teilnetzen

IP-Routing und Metrik
Routing-Metrik = Maß für Qualität einer Route: Kosten, Länge, Durchsatz, Fehlerrate
Linke State Routing (LS): dynamisches Routing, berücksichtigt den derzeitigen Zustand der Route. Link-State-Protokoll sind: OSPF (TCP / IP) - dagegen RIP: Dist.Vect.-Protocol
IS - IS (OSI) IS: Intermediate System
NLSP (Netware)
IP-Routing erfolgt zwischen Subnetzen, nicht zwischen einzelnen Knoten (Hosts). Mit Brücken verbundene LAN's werden als ein einziges Subnetz angesehen.

OSPF (Open Shortest Path First)
Internes Gateway – Protokoll. Uursprünglich: RIP-Routing Information Protocol (Basis: Distance-Vector-Protocol, Ford / Bellmann).
1979 abgelöst durch ein Link-State-Protocol.1990 als Standard: OSPF (RFC 1247)
Vorteile: Offene Architektur, Mehrere Entfernungsparameter, Dynamischer Algorithmus, Realisierung von Diensten (Feld: Typ of Service), Lastausgleich, Unterstützung hierarchischer Systeme, Sicherheit.
OSPF unterstützt 3 Arten von Netzen und Verbindungen:

1. Punkt-zu-Punkt zwischen 2 Routern,
2. Mehrfachzugriffsnetze mit Broadcasting (i.allg. LAN),
3. Mehrfachzugriffsnetze ohne Broadcasting (i.allg. PVN - WAN).

Einsatz OSPF: Internes Gateway Protokoll (IGP):
Mehrfachzugriffsnetz: an dieses sind mehrere Router angeschlossen, von denen jeder mit allen anderen kommunizieren kann.
OSPF unterscheidet 4 Router-Klassen:

1. Interne Router, die gänzlich zu einem Bereiche gehören.
2. Router an Bereichsgrenzen, die 2 oder mehrere Bereich verbinden.
3. Backbone-Router, die sich am Backbone befinden (jedes autonome System (AS) hat einen Backbone).
4. AS-Grenz-Router, die zwischen mehreren AS vermitteln (Verbindung AS über EGP).

BGP - Border Gateway Protocol
Externes Gateway-Protokoll für Routing zwischen autonomen Systemen. Ein internes Gateway Protokoll muss nur die Routing-Algorithmen erfüllen, BGP muss dagegen weitere Regeln befolgen, z.B.

- kein Transitverkehr durch AS,
- kein Datenverkehr über Irak (vom Pentacon aus, zumindest z.Zt. Saddam Hussein),
- IBM-Datenverkehr darf nicht bei Microsoft enden, ...

Diese Maßnahmen sind nicht Bestandteil des Protokolls; sie werden im Router installiert. Aus der Sicht eines BGP-Routers besteht die Welt nur aus BGP-Routen und den vorhandenen Leitungen.

Kategorien für Autonome Systeme:
1. Stub-Netze (Stummel-Netze): nur 1 Verbindung,
   Können nicht zum Transit genutzt werden, da nur 1 Seite.
2. Mehrfachanschlussnetze (Multiconnected Networks): für Transitverkehr nutzbar.
3. Transitnetze: z.B. Backbones.

BGP ist grundsätzlich ein Distance-Vector-Protocol. Dabei teilt jeder BGP-Router seinen Nachbarn die benutzten Pfade mit.

6.6 Routing in Ad-hoc-Netzen

6.6.1 Ad-hoc-Netze

Infrastrukturnetze und Ad-hoc-Netze
Typen von Netzen:
- Infrastrukturnetze: stationäre Netze mit Routern, Servern, hierarchische Struktur und zentrale Diensteanbieter. Typisch: Client/Server-Architektur.
- Ad-hoc-Netze: spontane Vernetzung, kurzfristig, ohne aufwendige Konfiguration. Keine feste Kommunikationsinfrastruktur, verteilte Diensteanbieter.
  Typische Anwendung: Peer-to-Peer Networking (P2P).
  Bekannte Ad-hoc-Netze: Mobile Ad-hoc-Netze (MANET).
  Andere Begriffe: Instant Infrastructure bzw. Mobile-mesh Networking.

Topologie:
Unterschiedliche Topologien von Ad-hoc-Netzen und stationären Netzen ~> Auswirkungen auf Wegeauswahl (Routing).
- *Infrastrukturnetze* i.allg. hierarchisch gegliedert. Direkt miteinander kommunizierende Rechner werden zu Subnetzen zusammengefasst. Knoten, die nicht denselben Subnetzen angehören, kommunizieren über *Router.*
- Computer in *Ad-hoc-Netzen* müssen Routingaufgaben selbst übernehmen.

Leitweglenkung
Drei Netzwerkklassen bezüglich topologischer Änderungsraten (-> für Auswahlkriterium):
1. Netze mit *sehr hoher Änderungsrate* erlauben keine strukturierten Ansätze zur Wegeauswahl. Ändert sich die Topologie noch während der Wegeauswahlprozesse, müs-sen Wegeentscheidungen neu getroffen werden. Hoher Verwaltungsaufwand ~> oft nur Ausweg, Nutzdaten über Fluten an alle Knoten zu verteilen ~> ineffizienter Nachrichtentransport. Bei sehr dynamischen Netzwerken ist Fluten oftmals nur die einzige Möglichkeit.
2. Ist *Änderungsrate* der Netzwerktopologie *sehr klein*, können Verfahren zur Wegeauswahl von traditionellen Netzwerken verwendet werden.
3. Die dritte Klasse von Netzen liegt mit der Änderungsrate zwischen diesen Extremen (*mittlere Änderungsrate*). Solche Netzwerke ändern ihre Topologie zu selten, um strukturierte Ansätze zur Wegeauswahl zuzulassen, jedoch zu häufig, um klassische Verfahren einzusetzen.

6.6.2 Routing-Algorithmen (Auswahl)

Leitweglenkung in Ad-hoc-Netzen
Ein Unterschied zwischen stationären und Ad-hoc-Netzen besteht in der Rolle von Routern. In Infrastrukturnetzen werden bevorzugt Router für die Paketweiterleitung eingesetzt, obwohl in stationären Netzen dies auch Arbeitsplatzrechner realisieren könnten (und in bestimmten Situationen auch tun). Die Weiterleitung von Paketen wird damit nicht den Arbeitsplatzrechnern auferlegt, sondern von spezialisierten Vermittlungsrechnern durchgeführt.
In Add-hoc-Netzen stehen nur die Endgeräte selbst zur Verfügung, d.h. es gibt keine Knoten, die ausschließlich für das Routing eingesetzt werden. Jedes am Ad-hoc-Netz beteiligte Gerät muss daher Routingaufgaben übernehmern, um Pakete weiterzuleiten.

Adaptive Routing-Verfahren in Ad-hoc-Netzen
Für Ad-hoc-Netze sind dynamische Routing-Verfahren erforderlich. Adaptive Routing-Algorithmen, die modifiziert in ad-hoc-Netzen eingesetzt werden:

- Distance-Vector-Verfahren (*Heartbeat-Algorithmus*):
  Knoten tauscht Distanzinformationen *nur mit Nachbarknoten* aus. Dabei auch Distanzinformationen über Knoten ausgetauscht, die sich nicht in Nachbarschaft befinden. Da Distanzinformationen von Nachbar zu Nachbar weitergegeben werden, kann sich im Verlaufe des Verfahrens jeder Knoten ein Bild des gesamten Netzes machen.
- Link-State-Verfahren (*Probe/Echo-Algorithmus*):
  Jeder Knoten ermittelt die Distanzen *zu den unmittelbaren Nachbarn*. Diese Informationen werden *an alle Knoten* des Netzwerks weiter vermittelt.
  Link-State-Verfahren sind anspruchsvoller in der Implementierung, fordern höhere Rechenleistung und haben einen höheren Speicherbedarf als Distance-Vector-Verfahren, aber die Algorithmen konvergieren schneller. Link-State-Verfahren führen zu besseren Ergebnissen, da jeder Knoten nach einer gewissen zeitlichen Verzögerung ein exaktes Bild vom Netzwerk erhält.

Topologie-Einfluss
Unterschiedliche topologische Eigenschaften von Ad-hoc-Netzen und stationären Netzen
~> Auswirkung auf Wegeauswahl.
Kommunikationswege in stationären Netzen:
Stationäre Netze i.allg. hierarchisch gegliedert. Rechner, die direkt miteinander kommunizieren, werden zu Subnetzen zusammengefasst (in Abb. a: N1, N2 , N3). Knoten, die nicht denselben Subnetzen angehören, kommunizieren über *Router* (in Abb. a: N4 bis N7).

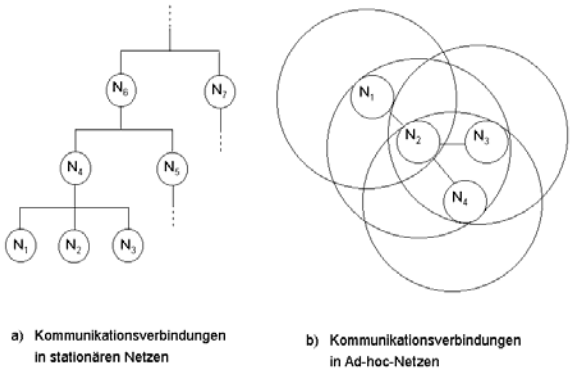


Abbildung 6.17: Kommunikationswege in stationären und Ad-hoc-Netzen

Damit die Wegeauswahl auch für große Anzahl von Knoten effektiv funktioniert (beim Internet einige Millionen Knoten), spiegeln Netzadres sen häufig die Topologie des Netzes wieder. So verwendet Vermittlungsprotokoll IP des Internet für Rechneradressen desselben Subnetzes dasselbe Adress-Präfix. Damit Wegeauswahl wesentlich erleichtert.
In Ad-hoc-Netzen (üblicherweise drahtlos) ist Netzstruktur durch den Standort und die Kommunikationsreichweite der beteiligten Rechner gegeben (Abb. b). Man kann aber nicht durch eine geeignete Vergabe von Netzadressen den Wegeauswahlprozess unterstützen, da sich nach der Vergabe der Adressen die Netzwerktopologie ändern kann. Zusätzlich ist Struktur wesentlich dynamischer, da die Rechner sich ständig räumlich bewegen. Die Wegeauswahl muss sich daher auf häufige Änderungen der Netzwerktopologie einstellen.

Auswahl von Ad-hoc-Routing-Verfahren

- DBF (Distributed Bellmann-Ford)
- DSDV (Destination-Sequenced Distance-Vector)
- DSR (Dynamic Source Routing)
- OLSR (Optimized Link State Routing)
- Link-Reversal-Routing
  - Full-Reversal-Routing
  - Partial-Reversal-Routing
  - LMR-Verfahren (Lightweight Mobile Routing)
  - TORA-Verfahren (Temporally-Ordered Routing Algorithm)

DBF und DSDV

Eines der ersten Routing-Verfahren, das speziell für Ad-hoc-Netze konzipiert wurde, ist *DSDV (Destination-Sequenced Distance-Vector)*. Verfahren geht auf ein älteres Verfahren zurück, das für stationäre Netze eingesetzt wurde: *DBF (Distributed Bellmann-Ford)*.
DBF und DSDV sind proaktive Verfahren, gehörig zur Klasse Distance-Vector-Verfahren.

DBF (Distributed Bellmann-Ford-Algorithmus)

DBF-Verfahren bildet Basis für DSDV (Distance-Vector-Verfahren).
Kurze Erläuterung zu DBF:
Jeder Knoten verfügt über eine Routing-Tabelle, die für jeden Netzknoten angibt,
- über welchen Nachbarn das Paket weitergeleitet werden muss (*Hop*) und
- welche Gesamtdistanz bis zum Ziel zurückgelegt werden muss (*Metrik*).

Als Metrik wird in diesem und in den folgenden Beispielen die Anzahl der Zwischenschritte bis zum Ziel benutzt.
Beispiel zur Arbeitsweise von Distance-Vector-Verfahren, insbes. DBF:

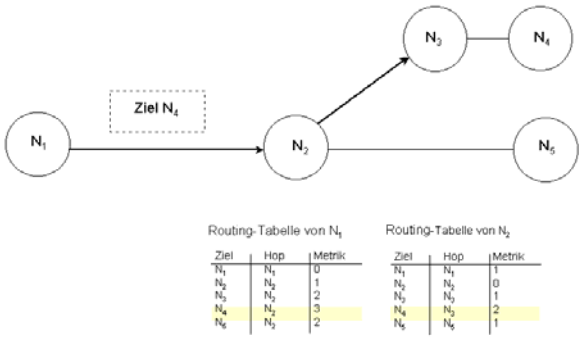


Abbildung 6.18: Distributed Bellmann-Ford-Algorithmus (Beispiel)

- Knoten N_1 sendet ein Paket an Knoten N_4.
  N_1 sucht in Routing-Tabelle nach Eintrag zu N_4 und ermittelt N_2 als nächstes Ziel. N_2 findet nun N_3 als nächstes Ziel usw. Weiterleitung so lange durchgeführt, bis Zielknoten erreicht wird.
- Distance-Vector-Verfahren dadurch ausgezeichnet, dass Sender eines Paketes nicht gesamten Weg zum Ziel kennen muss. Der Weg wird vielmehr auf der Reise ermittelt.
- DBF-Verfahren legt fest, wie Routing-Tabellen entstehen. Hierzu tauscht jeder Knoten mit seinem Nachbarknoten *Distanzvektoren* aus. Distanzvektoren geben zu jedem Ziel im Netz an, welche Entfernung zum jeweiligen Knoten besteht, d.h. der Distanzvektor entspricht der Spalte *Metrik* der Routing-Tabelle.

DSDV (Destination-Sequenced Distance-Vector)
Für Ad-hoc-Netze ist Verhalten bei *unterbrochenen Verbindungen* besonders problematisch (tritt verhältnismäßig häufig auf). Routing-Verfahren muss sich hinreichend schnell auf die neue Situation einstellen. Deshalb Weiterentwicklung DBF zum DSDV.
Prinzip des DSDV-Verfahrens:

- Periodisch oder falls ein Knoten eine Topologieänderung erkannt hat, werden Distanzinformationen an alle Nachbarknoten versendet. Hierbei kann ein Knoten entweder alle Distanzeinträge (*Full Dump*) oder nur die geänderten Einträge senden, je nachdem, wie groß die Änderungen seit der letzten Sendung waren.
- DSDV erweitert die Routing-Tabellen um eine Spalte *Sequenznummer*. Diese wird benötigt, um Aktualität einer Nachricht erkennen zu können. Die Sequenznummer wird i.d.R. von dem Knoten vergeben, zu dem die Distanz gemessen wurde. Sie wird bei jedem Verbreiten von Distanzinformationen erhöht.
- Empfängt ein Knoten neue Distanzinformationen, so wird Eintrag nur *aktualisiert*, wenn entweder die Sequenznummer sich erhöht hat oder die Sequenznummer gleich geblieben ist und sich zusätzlich die Gesamtdistanz verringert hat.
- Das Verfahren setzt voraus, dass alle Verbindungen *bidirektional* sind. Diese Voraussetzung wird in Ad-hoc-Netzen nicht immer erfüllt.

7 Transportschicht

7.1 Dienste der Transportschicht

Transportschicht
Schicht 4 (OSI-Modell) bzw. Schicht 3 (TCP/IP-Modell). Sie bildet zusammen mit Vermittlungsschicht (insbesondere IP) den Kern der gesamten Protokollhierarchie:
- bietet Dienste für die daraufsitzenden Schichten (Sitzungsschicht ... Anwendungsschicht), verbindungslos / verbindungsorientiert.
- nutzt Dienstleistungen der Vermittlungsschicht.

Aufgaben / Zielstellungen:
- Datentransport von Quelle zu Ziel (Ende-zu-Ende-Protokoll: End-to-End-Relay),
- unabhängig vom physischen Netz,
- zuverlässig und kostengünstig.

Dienste für die oberen Schichten
Transportschicht (TSP) soll Benutzern einen effizienten, zuverlässigen und kostengünstigen Dienst anbieten. Benutzer sind Prozesse der Verarbeitungsschichten.
Angeboten werden 2 Arten von Transportdiensten, die denen der Vermittlungsschicht ähnlich sind (incl. Adressierung, Flusssteuerung): *verbindungsorientiert* (connection-oriented) bzw. *verbindungslos* (connectionless).

Dienstqualität der Transportschicht
Hauptfunktionen der TSP-Schicht:
- Bereitstellung eines verbindungslosen oder verbindungsorientierten Dienstes (bei End-to-End-Relay),
- Verbesserung der Dienstqualität, die von der Vermittlungsschicht bereitgestellt wird (~> QoS: Quality of Service).

Parameter für Dienstgüte auf Transport-Schicht
- Dauer des Verbindungsaufbaus (Connection Establishment Delay): möglichst geringe Verzögerung.
- Ausfall-Wkt. bei Verbindungsaufbau (Connection Establishment Failure Probability): falls Verbindung nicht innerhalb einer Aufbaudauer aufgebaut ist.
- Durchsatz (Throughput): Übertragene Informationseinheiten je Zeiteinheit [Byte/s].
- Übertragungsverzögerung (Transit Delay): Zeit Quelle -> Ziel
- Restfehlerrate (Residual Error Ratio): Anzahl verlorener bzw. zerstörter Nachrichten im Vergleich zu den gesamten Nachrichten.
- Schutz (Protection): Schutz vor unerlaubten Lesen oder Verändern (Hacker)
- Priorität (Priority): z.B. bei Überlastungen.
- Störausgleichsverhalten (Resilience): Wkt., dass Transportschicht spontan die Verbindung beendet (bei Überlastung oder interne Probleme).

Parameter werden bei Verbindungsaufbau ausgehandelt: sog. *Optionsverhandlung* (Option Negotiation). Parameter bleiben für Dauer der Verbindung unverändert. Bessere Dienstqualität ist teurer.

Dienstoperationen der Transportschicht
Vermittlungsschicht:
X.25: verbindungsorientiert, zuverlässig ==> für stark gestörte Übertragungskanäle
IP: verbindungslos, unzuverlässig ==> Normalfall (z.B. Paketverluste)
Transportschicht:
i.allg. zuverlässig (TCP, OSI-TP-Klasse 4),
auch unzuverlässiger Dienst unterstützt (Datagramme, UDP, OSI-TP-Klasse 0)

Transportdienst von vielen Programmen genutzt ~> muss nutzerfreundlich und einfach sein.
Nachrichten zwischen Transportinstanzen: *TPDU (Transport Protocol Data Unit)*
- TPDU sind (von Vermittlungsschicht ausgehend) in *Paketen* enthalten,
- Pakete sind (von Sicherungsschicht ausgehend) in *Rahmen* enthalten.

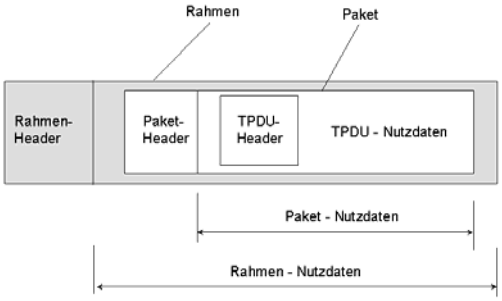


Abbildung 7.1: Verschachtelung TPDU

Berkeley-Sockets
Gruppe von Transportoperationen, die im Berkeley-UNIX für Zugriff auf TCP bzw. UDP benutzt werden. Heute in allen Betriebssystemen (u.a. Windows) bzw. Programmierumgebungen (z.B. DCE, Java) angeboten

Berkeley-Sockets

Operationen werden in dieser Reihenfolge von Servern ausgeführt

Operationen	Bedeutung
SOCKET	Erzeugt neuen Kommunikations-Endpunkt; weist Tabellenplatz in Transport-Instanz zu Festlegung Adressen-Format, gewünschter Dienst und Protokolle Neue Sockets haben keine Adresse
BIND	Hängt lokale Adresse an Socket an
LISTEN	Kündigt Bereitschaft zur Annahme von Verbindungen an; weist Platz in Warteschlange zu
ACCEPT	Blockiert den Rufenden, bis ein Verbindungsversuch von einem Client ankommt
CONNECT	Client muss auch Socket (mit Operation SOCKET) erzeugen (BIND nicht erforderlich, da Adresse für Server uninteressant) CONNECT blockiert den Rufenden und startet Verbindungsprozess => somit aktiver Versuch, eine Verbindung aufzubauen
SEND	Sendet Daten über eine Verbindung
RECEIVE	Empfängt Daten über eine Verbindung (bei Vollduplex können beide Seiten mit SEND und RECEIVE arbeiten)
CLOSE	Abbau einer Verbindung (verläuft symmetrisch für beide Seiten)

Abbildung 7.2: Berkeley Sockets

Elemente der Transportschicht
Protokolle der Transportschicht
Sie ähneln den Protokollen der Sicherungsschicht, insbes. zur Fehlerüberwachung, Folgesteuerung und Flusssteuerung. Wichtiger Unterschied:
DLL: 2 Knoten (Router) kommunizieren direkt über physischen Kanal;
TSP: Kommunikation über ganzes Teilnetz, d.h. in Transport-Schicht muss Ziel ausdrücklich adressiert werden (End-to-End).
Adressierung
- bezüglich Anwendungsschicht: TSAP: Transport Service Access Point (allgemein)
  * im Internet: IP-Adresse + lokale Port-Nr. (sog. „Socket“)
  * im ATM: AAL-SAP’s
- bezüglich Vermittlungsschicht: NSAP: Network Service Access Point (z.B. IP-Adresse)

7.2 Internet-Transportprotokolle

7.2.1 Einordnung

2 Protokollarten der Internet-Transportschicht:

- zuverlässig, verbindungsorientiert (TCP: Transmission Control Protocol)
- unzuverlässig, verbindungslos (UDP: User Datagram Protocol)

Schichtenzuordnung

Anwendung	Anwendung und anwendungsspezifisches Protokoll (z.B. WWW/HTTP)
Transport	TCP oder UDP
Vermittlung	IP
Netzwerk	OSI-Schichten 1 - 2

7.2.2 Transmission Control Protocol (TCP)

Zuverlässiger Bytestrom (Ende-zu-Ende-Verbindung)

TCP: Bereitstellung eines zuverlässigen Dienstes, um Bytestrom von Ende-zu-Ende in einem unzuverlässigen Netzwerk (IP) zu übertragen (dynamische Anpassung an unterschiedliche Netzwerk-Merkmale). Definiert in RFC 793 (Verbesserungen in RFC 1122 und 1223).
Jede Maschine mit TCP hat eine Transportinstanz, die entweder ein Benutzerprozess oder Teil des Kernels ist.

Funktion:			
lokaler Prozess		Bytestrom	
TCP-Transport-instanz	Zerlegung in Segmente i.d.R. 1500 Byte (max. 64 KByte)		Zusammensetzung als Bytestrom
IP		IP-Datagramm (Paket)	

IP sichert keine Reihenfolge der Datagramme. TCP muß deshalb nach Timeout bei Bedarf erneut übertragen.

Merkmale des TCP - Protokolls

- Verbindungsorientiert (Verbindungsaufbau, Datentransfer, Verbindungsabbau);
- Partner sind über virtuelle, vollduplex-fähige, bidirektionale Leitungen verbunden;
- Sicherer Nachrichtentransport, reihenfolgerichtig.
  Fehlererkennung durch Sequenz-Nummer, Bestätigungs-Nummer (Quittung), Prüfsumme, Zeitüberwachung; Segmentwiederholung bei Datenverlust;
- Segmentierung der Benutzerdaten (Anwendungsprogramme erzeugen nur Datenstrom, ohne Strukturierung in Segmente bzw. Pakete);
- Flusssteuerung (sichert, dass Empfänger nicht mit Daten überflutet wird);
- Zeitüberwachung (Timer); Prioritätssteuerung, Sicherheitsklassen;
- Überlastüberwachung (Überlastfenster, Schwellwert).

TCP-Dienstmodell

Sockets

Bereitstellung eines TCP- Dienstes an speziellen Endpunkten, den sogenannten Sockets.
Jeder Socket hat eine Socket-Nr. (die sog. Socketadresse), bestehend aus
IP - Adresse des Hosts und **lokaler Port** (16 - Bit - Nr., **TSAP**).
Port ~> TCP-Name für TSAP (Transport Layer Service Access Point)

Socketaufrufe

Erzeugen Socket (Datenstruktur):	SOCKET
Binden, Verbindungsauf/abbau:	BIND, LISTEN, ACCEPT, CONNECT, CLOSE
Übertragen:	SEND, RECEIVE

Ein Socket kann für mehrere Verbindungen gleichzeitig benutzt werden, d.h. mehrere Verbindungen enden auf gleichem Socket.

Ports

Ein Port definiert den Zugang zwischen TCP (oder UDP) und der nächst höheren Schicht. Jeder Anwendung ist eindeutig ein Port (oder mehrere) zugeordnet. Ein Port identifiziert eindeutig die gewünschte Anwendung.
Auswahl von Portnummern:

1 - 255	reserviert für Internetdienste
256 - 1023	reserviert für privilegierte Benutzer (z.B. Superuser in UNIX)
1024 - 5000	transienter Bereich; Port-Nummern werden dynamisch generiert
5001 - 65553	Port-Nummern frei für Anwendungen

Well-known Ports für reservierte Ports (Vergabe durch IANA).
Eingerichtet für offizielle Dienste, u.a.

ftp	21 / tcp	definiert in RFC 1700
telnet	23 / tcp	(Datei etc/services)
time	37 / udp	

Nachrichten beliebiger Länge werden zu Ports gesendet und von Ports empfangen. Ports werden dynamisch eingerichtet und zerstört.
Port-Zugriff über “Capabilities” gesteuert: Sende-, Empfang-, Besitz- Capabilities:
- Anwendung generiert Port, besitzt alle 3 Capabilities;
- Capabilities können in Nachrichten an andere Prozesse weitergereicht werden;
- Sender von Empfangs- und Besitz-Capabilities verliert Empfangs- und Besitzrecht.

TSP-Kopf enthält nur Port-Nummern, nicht die vollständige IP-Adresse, die z.B. Bestandteil eines Socket ist. Diese Information wird von der Transportschicht an die Vermittlungsschicht über einen “Pseudoprotokollkopf” übergeben. Dieser wird von der Vermittlungsschicht ausgewertet, um Quell- und Zieladresse zu bestimmen. Der Pseudoprotokollkopf wird nicht an den Empfänger weitergegeben. Die Prüfsumme im TSP-Protokoll schließt den Pseudoprotokollkopf ein.
TCP-Verbindungen sind immer
- vollduplex: Verkehr kann gleichzeitig in beide Richtungen fließen;
- Punkt-zu-Punkt: Jede Verbindung hat genau 2 Endpunkte.

TCP unterstützt kein Multicasting und kein Broadcasting.

TCP-Bytestrom-Verbindung

TCP-Verbindung ist ein Bytestrom, kein (strukturierter) Nachrichtenstrom. Anwendungsprozess überträgt an TCP für die Dauer der Verbindung einen kontinuierlichen Strom von Bytes.
TCP teilt Bytestrom in Segmente variabler Länge auf und gibt sie an IP weiter (TCP sammelt genügend Bytes von dem Byte-Strom, um einen Puffer vernünftiger Größe zu füllen, ehe Daten (Segment) an IP übermittelt werden).
Beim Verbindungsaufbau handeln Sender und Empfänger die maximale Segmentgröße (Maximum Segment Size, MSS) aus: Segment := TCP-Header + Daten.
Jedes Segment hat mindestens 40 Byte (TCP + IP Kopf) und Daten, IP-Default = 536 - (TCP + IP Kopf). Segmentgröße kann bei Sender und Empfänger unterschiedlich sein.

Push-Mechanismus

Einfacher Steuerungsmechanismus, gesteuert von Anwendung. Damit kann Anwendung TCP auffordern, die Daten an IP sofort weiterzugeben, obwohl Puffer noch nicht gefüllt ist. Auf Empfängerseite gibt TCP ebenfalls die Daten ohne Verzögerung an Anwendung weiter.
Steuerung über PUSH-Flag im TCP-Protokoll. Anwendung: z.B. Abbruch eines Kommandos.

Urgent-Mechanismus

Damit kann Anwendungsprogramm Daten schnell übertragen, ohne den Transfer aller bereits im Bytestrom befindlicher Daten abzuwarten.
Beispiel: Abbruch eines entfernten Programms über Kill-Kommando; Durch dieses Ereignis hört TCP mit Ansammeln von Daten auf und überträgt sofort alles, was für die betreffende Verbindung anliegt.
Die Anwendung spezifiziert dann die Daten als urgent (URG-Bit im TCP-Header). TCP überträgt diese Daten außerhalb der Reihenfolge. TCP auf Zielmaschine informiert seine Anwendung, in den Urgent-Modus überzugehen.
Urgent := grober Signalisierungsmechanismus und überlässt alles andere der Anwendung.

Aufbau TCP-Protokoll

TCP tauscht Daten in Form von Segmenten aus.
Segment: - fester 20-Byte - Header + optionaler Teil
- gefolgt von Daten.

Segmentgröße wird durch TCP festgelegt.
2 Faktoren bestimmend:

- Jedes Segment (incl. TCP-Header) muss in das IP-Nutzdatenfeld von 65 535 Byte passen.
- Jedes Netz hat eine maximale Transfereinheit (MTU: Maximal Transfer Unit), in die jedes Segment passen muss. MTU i.allg. einige 1000 Byte groß (= obere Segment-Größe); bei Netzübergängen können unterschiedliche MTU auftreten -> Router müssen dann die Segmente fragmentieren.

Schiebefensterprotokoll (Sliding Window) in TCP

TCP-Einheiten benutzen das Schiebefenster-Protokoll (Sliding Window) unter Nutzung der Folge- und Bestätigungs-Nummer: Überträgt ein Sender ein Segment, wird gleichzeitig ein Timer gestartet. Kommt Segment am Ziel an, sendet Empfänger-TCP ein Segment (Segment-Nr. / Folge-Nr.) mit Bestätigungs-Nr. zurück. Diese Nummer entspricht der nächsten erwarteten Folge-Nr. Läuft Sender-Timer ab, ehe Bestätigung eintrifft, überträgt Sender das Segment erneut (Sender entscheidet, ob nur das 1. ausstehende oder alle Segmente neu zu übertragen sind).
Sliding Window wird von TCP über 3 Zeiger verwaltet (beinhalten Byte-Adressen relativ zum Anfang der Übertragung). Protokoll arbeitet auf Byte-Ebene. Bestätigung (ack) durch Empfänger erfolgt ebenfalls auf der Byte-Ebene.
Fenstergröße

- variabel (dynamisch veränderlich).
- Empfänger kann neue Fenstergröße mitteilen, zusammen mit Bestätigung (piggyback).

Die dynamisch veränderliche Fenstergröße wird von TCP zur Flusssteuerung zwischen Sender / Empfänger eingesetzt. Z.B. Fenstergröße 0 besagt:
Bytes (incl. ack Nr.1) wurden empfangen, aber Empfänger will vorläufig keine Daten mehr; Erlaubnis zum Fortsetzen des Senders erfolgt dann mit Segment gleicher Bestätigungs-Nr. und Windows-Feld 0;
Zur Steuerung / Vermeidung von Staus dienen andere Mechanismen.

TCP-Verbindungsmanagement

TCP-Verbindungen werden über das sog. Drei-Wege-Handshake aufgebaut.

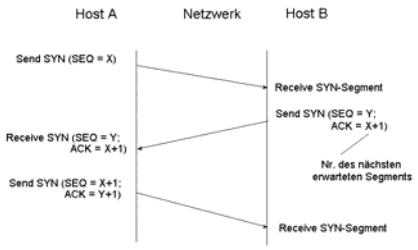


Abbildung 7.3: Drei-Wege-Handshake

TCP-Timer-Management

TCP nutzt mehrere Timer, u.a.

- Retransmission-Timer: wichtigster Timer (Sende-Wiederholungs-Intervall)
  Timer für Sendewiederholung (RTO: Retransmission Time Out). RTO läuft ab, wenn Zeitraum zwischen Senden eines TCP-Segments und seiner Bestätigung überschritten wird. Zeitraum ist dynamisch veränderlich.
- Persistence-Timer: zur Verklemmungs-Verhinderung
- Keepalive-Timer: Beenden einer Verbindung, wenn diese über längere Zeit inaktiv ist.

TCP-Segmentkopf (Header)

Segment:

- 20-Byte-Header mit festem Format;
- dem können Header-Optionen folgen;
- diesem können bis zu 65 535 - 20 - 20 = 65 495 Datenbytes folgen (Segmente ohne Daten werden für Steuernachrichten und Bestätigungen genutzt).

Quell / Zielport: Lokaler Endpunkt der Verbindung (Port: max 256)
Port + IP-Adresse --> eindeutiger TSAP (48 bit)
$TSAP_{TCP}$ = (IP-Adresse, TCP-Port), z.B. 134.60.77.243 , 80
Damit Anwendung bezeichnet, die auf der entsprechenden IP-Adresse läuft.

Folge-Nr. (Sequence-No.): Nr. des 1. Oktetts der Daten im Segment.

Bestätigungs-Nr. (Acknowledge-No.): Nr. der zu erwarteten Daten bei unkorrektem Empfang.

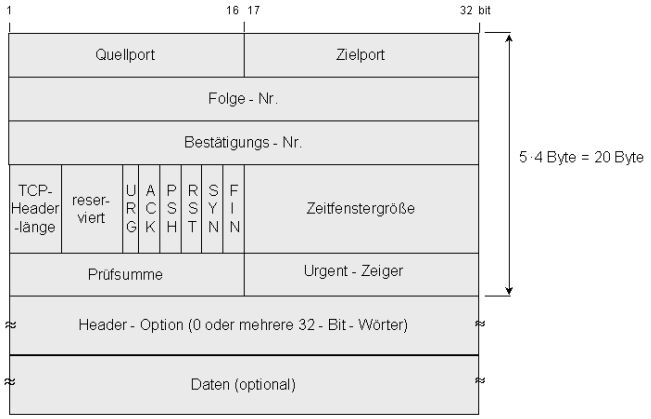


Abbildung 7.4: TCP-Header

Header-Länge: Anzahl der 32-bit-Wörter imTCP-Header.

Flags: URG: 1, wenn Urgent-Zeiger (Dringend-Zeiger) gesetzt (-> Byteversatz der aktuellen Folge-Nr. bei dringlichen Daten).
ACK: 1, wenn Bestätigung-Nr. gültig
0: Segment enthält keine Bestätigung.
PSH: PUSH-Daten => Empfänger aufgefordert, die Daten der Anwendung ohne Zwischenspeicherung sofort bereitzustellen.
RST: um Verbindung zurückzusetzen (z.B. Absturz eines Hosts).
SYN: für Aufbau einer Verbindung.
FIN: für Abbau einer Verbindung (Sender soll keine weiteren Daten mehr übertragen).

Zeitfenstergröße: Fenster variabler Größe
- bezeichnet Anzahl der Bytes, die ab dem bestätigten Byte gesendet werden können;
- Nutzung zur Flusssteuerung (Windowfeld 0 und ACK-Nr. 1 => Empfänger verlängert Verschnaufpause).

Prüfsumme: für extreme Zuverlässigkeit (Prüfung Header, Daten und Pseudo-Header)

Urgent-Flag: um Daten schnell übertragen, ohne den Transfer aller bereits im Bytestrom befindlicher Daten abzuwarten ~> Daten außerhalb der Reihenfolge übertragen (TCP setzt Zielmaschine in Urgent-Modus = grober Signalisierungsmechanismus)

Optionen: für zusätzliche Funktionen, z.B.
- Spezifikation der max. TCP-Nutzdaten;
- Fenstergrößen (RFC 1323);
- Selektive Wiederholung statt Protokoll “go back n” (RFC 1106).

7.2.3 User Datagram Protocol (UDP)

Verbindungsloser Transportdienst

UDP - User Datagram Protocol
- Verbindungsloses Transportprotokoll im Internet, definiert in RFC 768;
- Kein Verbindungsaufbau / abbau;
- Nur Datentransfer Quelle --> Ziel (ohne auf Rückmeldung des Empfängers zu achten).

UDP überträgt gekapselte rohe IP-Datagramme. Merkmale von UDP:
- keine Kontrollmechanismen;
- keine Reihenfolgeüberwachung der Pakete ~> damit keine Sicherung einer erfolgreichen Übertragung;
- keine Fehlerbehebung;
- keine Zeitüberwachung;
- zustandslos (stateless);
- minimale Protokollmechanismen, wenig Overhead --> sehr effektiv;
- Einhaltung der Nachrichtengrenzen wird garantiert --> Multi- und Broadcasting möglich (empfangene Nachricht = gesendete Nachricht).

Anwendung
- in vielen Client/Server-Anwendungen, die auf der Basis Anfrage/Antwort laufen;
- UNIX-Kommandos / Anwendungen;
- Network File System (NFS);
- X-Window;
- NS-Protokoll (Domain Name Server).

UDP ermöglicht Angabe von Multicast- und Broadcast-Adressen.

UDP-Segment

Bestehend aus
- 8-Byte-Header,
- gefolgt von Daten.

Im Prinzip entspricht dies dem IP-Paket, ergänzt durch die Port-Nr.
$TSAP_{UDP}$ = (IP-Adresse, UDP-Port), z.B. 134.60.77.243 , 53
Die Rechneradressen befinden sich im vorgeschalteten IP-Header
UDP-Header:

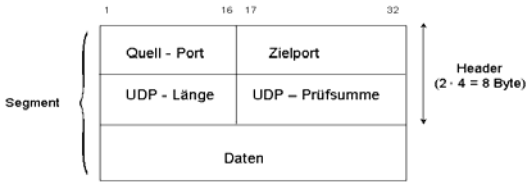


Abbildung 7.5: UDP-Header

Quellport / Zielport	Endpunkte der Quell-/Zielmaschinen (Programme)
UDP - Länge:	8-Byte-Header und Daten
Prüfsumme:	Prüfsumme über Pseudo-Header, UDP-Header, UDP-Daten Prüfsumme ist optional

7.3 Netzwerkprogrammierung (Sockets)

7.3.1 Socket-Programmierschnittstelle

Netzwerkprogrammierung
Von „Netzwerk"programmierung spricht man, falls die verteilte Anwendung direkt auf kommunikationsorientierten Protokollstack aufsetzt, z.B. Internet (TCP/IP ~> Sockets). Gute Steuerbarkeit, hohe Performance, gültig für viele Plattformen. Aber: native Programmierung, wenig Anwendungsunterstützung, sehr aufwendig, da viele Aktivitäten selbst vorgenommen werden müssen, z.B. Datenformate, Synchronisation, CPU-Architektur (little/big endian). I.allg. nur für kleine Anwendungen geeignet.
Erweiterung durch Verteilungsplattformen/Middleware (LVA „Verteilte Systeme"):
- *kommunikationsorientiert*: RPC (Remote Procedure Call), RMI (Remote Method Invocation), MQSeries ...
- *anwendungsorientiert*: CORBA, EJB, WCF, SOA ...

Alternativ: „Internet-Technologien": W3, Web Services, AJAX, ... Cloud Computing

Sockets im Internet
Fragestellung: wie TCP bzw. UDP nutzbar ? Zu den Internet-Transport-Protokollen TCP und UDP sind keine Programmierschnittstellen vorgeschrieben.
Verbreitetste Schnittstelle: Socket-Interface des BSD UNIX (Berkeley).
Ursprünglich unter Unix zur Inter-Prozess-Kommunikation eingesetzt, entwickelte sich das Konzept der Sockets zum de facto Standard für TSAP Implementationen (TSAP: Transport Layer Service Access Point). Unter Unix ist ein Socket eine Ressource des Betriebssystems und wird wie eine Datei behandelt. Andere Betriebssysteme stellen Socket-Funktionalität über gesonderte Bibiliotheken zur Verfügung. Eine Anwendung, die Sockets als Kommunikations-Schnittstelle verwendet, ist weitgehend unabhängig vom verwendeten Transportmechanismus und muss beim Austausch des Protokolls nur geringfügig verändert werden.
Socket
- Abstraktion des Transportsystems in Form einer Betriebssystem-Ressource (z.B. Datei);
- Bereitstellung der TCP / UDP - Dienste am Socket;

- Vollständige TCP / UDP - Adresse, bestehend aus IP-Adresse, Port-Nr. (~> als “Socket” bezeichnet).

Socket-Merkmale:

- Jede Kommunikation eines Prozesses mit einem anderen (entfernten) Prozess verwendet Sockets als Zugangspunkt zum Transportsystem (TCP / UDP).
- Sockets können mit 1 oder mehreren Prozessen verbunden sein.
- Sockets für lokale Interprozesskommunikation (z.B. AF_UNIX) oder entfernte Kommunikation über Netz (z.B. AF_INET).
- Semantik der Kommunikations-Endpunkte sind auf Basis - E/A - Funktionen des Betriebssystems abgebildet.
- Sockets wie Variable in einem Programm verwendbar, Namensgebung deshalb möglich.
- Je Kommunikations-Art muss Typangabe verwendet werden:
  für verbindungslose Kommunikation (UDP): Typ Datagram
  für verbindungsorientiert Kommunikation (TCP): Typ Stream.
- Sockets können aktiv (z.B. für Clients) oder passiv sein (z.B. für Server).

7.3.2 Prozesskommunikation über Sockets

Socket-Implementierung

Socket: Endpunkt einer Kommunikationsverbindung (sowohl lokal als auch entfernt). Für remote Verbindung: Socket verbindet die Anwendung mit dem Transportmechanismus (TCP und UDP). Für TCP- oder UDP-Protokolle ist die Socketadresse durch Kombination IP-Adresse und Port-Nr. definiert (TSAP).

Socket analog zum Filedeskriptor durch einen Socketdeskriptor als Integerwert definiert. Socketdeskriptor als Pointer auf Deskriptortabelle ~> Descriptor-Tabellen-Einträge enthalten jeweils einen Pointer, der auf eine Socketstruktur zeigt.

Verallgemeinerung des Open - Read/Write - Close – Paradigmas: Verbindung erlaubt einfachen Datenaustausch als Bytefolge --> Daten werden nicht interpretiert.

Ursprünglich Teil des 4BSD Unix; Generalisierung des Unix-Mechanismus für E/A. Außerhalb BSD Unix sind Sockets als System-Bibliotheksroutinen in anderen Betriebssystemen implementiert (z.B. WinSock). De-Facto-Standard als Schnittstelle für TCP/IP und Internet. Sockets sind keine Protokolle.

Das UNIX Open – Read / Write – Close – Paradigma

Der Systemaufruf *socket* erzeugt (ähnlich dem Aufruf *open*) einen Deskriptor, der im Gegensatz zu Datei-Deskriptoren nicht an eine spezifische Adresse gebunden ist.

Es handelt sich dabei um einen Integer-Wert, der als Pointer interpretiert auf eine Deskriptor-Tabelle zeigt. In dieser Tabelle findet sich dann ein Zeiger auf eine Socket-Struktur.

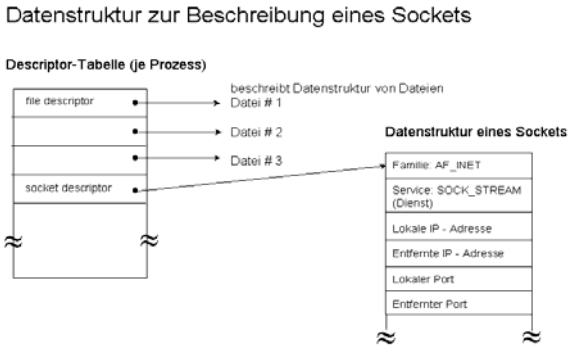


Abbildung 7.6: Descriptor-Tabelle und Socket-Struktur

Um eine Verbindung über Sockets herzustellen, werden die entsprechenden Befehle für den Socket(-Deskriptor) aufgerufen, wobei er wie eine Variable verwendet und als Parameter übergeben wird.

Aufrufe zur Socket-Programmierung:

Bedeutung		**Befehl**
1.	Socket erzeugen (Datenstruktur innerhalb des Adressraums für Datenbereich des Betriebssystems)	socket (...)
2.	Socket mit einem nach außen sichtbaren Namen versehen (mit einer TSAP - Adresse). Danach kann der Name bekannt gegeben und verteilt werden	bind (...)
3.	Warteschlange erstellen, um eingehende Nachrichten zu speichern (Verbindungsaufnahme ankündigen)	listen (...)
4.	Auf Nachricht warten (Server wartet auf Verbindungswunsch), Socket Descriptor an Kind-Prozess weitergeben	accept (...)
5.	Verbindung zwischen zwei Sockets herstellen (C -> S)	connect (...)
6.	Daten senden, empfangen	send (...) sendto (...) recv (...) recvfrom (...)
7.	Beenden (Abbau der Verbindung)	close (...)

Eine Verbindung über einen Socket hat drei Kennwerte, die IP-Adresse, das Protokoll und den Port. Des Weiteren gibt es drei Typen von Sockets. Stream Sockets (**SOCK_STREAM**) für zuverlässige, verbindungsorientierte Duplex-Verbindungen werden im Internet-Bereich durch TCP/IP unterstützt. Datagram Sockets (**SOCK_DGRAM**) für verbindungslose, nicht garantierte Nachtrichtenübertragung werden durch UDP unterstützt. Als Mechanismus für selbst programmierte höhere Protokolle stehen Raw Sockets (SOCK_RAW) zur Verfügung.

Die in Klammern angegebenen symbolischen Konstanten können über vordefinierte Header (z.B. /sys/types.h, /sys/socket.h bei BSD UNIX) eingebunden werden. Entsprechend werden auch die folgenden Symbole für Adressfamilien verwendet, über die dem Socket ein Transportmechanismus zugeordnet wird (sog. Domain bzw. **Address Family**):

- **AF_UNIX** lokale Verbindung über Dateisystem
- **AF_IUCV** lokale Verbindung im MVS und VM über die IUCV-Domains (Inter User Communication Vehicle)
- **AF_INET** entfernte Verbindung über TCP / IP
- **AF_APPLETALK** entfernte Verbindung über Apple Computer Incorporated Appletalk Network

7.3.3 Sockets in der Programmiersprache C

A: Allgemein (d.h. TCP oder UDP)

In der Programmiersprache C werden Sockets über einen Aufruf von socket erzeugt, z.B.:

```
int s;                    - - socket descriptor
s = socket (
        int  family,      - -  family = AF_UNIX | AF_INET | . . .
        int  type,        - -  type = SOCK_DGRAM | SOCK_STREAM | . . .
        int  protocol);   - -  protocol = Version bzw. 0 (default)
```

Die Funktion vergibt einen willkürlichen freien Deskriptor, der innerhalb der Datei-Deskriptor-Tabelle des Prozesses allokiert wird. Die Datenstruktur bleibt dabei zunächst ungefüllt. Beispiel: s=socket (AF_INET, SOCK_STREAM, 0).

In einem weiteren Schritt müssen dieser Struktur Daten zugewiesen werden. Bspw. in UNIX:

```
struct sockaddr_in  {
        u_short sin_family;   - -  AF_INET
        u_short sin_port;     - -  Portnummer
        u_long  sin_addr;     - -  IP - Adresse
        char    sin_zero [8]; - -  nicht verwendet
};
```

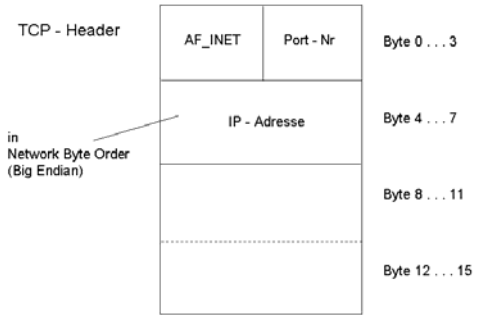


Abbildung 7.7: Parameterstrukturierung TCP-Header

Danach kann die Namensbindung des Sockets erfolgen.

```
retcode = bind (
        int  socket,
        sockaddr_in    * localaddr,
        int  addrlen);
```

Dazu werden folgende Daten benötigt, die anschließend der Funktion bind übergeben werden:

int socket:	Socket Identification (sockid)
localaddr:	Struktur enthält
	Address Family = 2 für TCP / IP
	Protocol Port
	IP Address
addrlen:	Länge der Struktur localaddr

Der erstellte Socket wird mit bind mit der in sockaddr_in befindlichen Adressinformation versehen und somit eine well-known Port-Nr. dem Socket zugewiesen. I.allg. ist der Aufruf nur beim Server notwendig, um die so gewonnene eindeutige Socketadresse den Clients mitteilen zu können.

Mit der Funktion close wird ein Socket gelöscht bzw. deallokiert, falls der aufrufende Prozess der letzte Prozess war, der ihn verwendet:

```
retcode = close (int  socket);
```

Weitere Kommandos: Sie werden in Abhängigkeit der Dienste unterschiedlich verwendet:

- Socket mit einer Empfänger - Adresse verbinden
  connect (sockid, destaddr, addrlen)
- Daten senden

sendto (sockid, buffer, length, ...)UDP
write (sockid, buffer, length) TCP

- Daten empfangen
  recvfrom (sockid, buffer, length, ...) UDP
  read (sockid, buffer, length) TCP
- Anzahl von Verbindungen, die über den Socket geknüpft werden können
  listen (sockid, queuelen)
- Warten auf eine Verbindung
  accept (sockid, clientaddr, addrlen)

B: Datagram-Kommunikation mit UDP

Für UDP-Kommunikation von Client zu einem Server gibt es jeweils entsprechende Sende- und Empfangsaufrufe (Socketspezifikation mit SOCK_DGRAM).

Senden von Datagramen:

```
retcode = sendto (
        int  socket,          - - socket descriptor
        char  *  msg,         - - Zeiger auf Nachricht
        int  msglen,          - - Nachrichten-Länge in Bytes
        int  flags,           - - Kontrollbits
        sockaddr_in  * to,    - - Zeiger auf Zieladresse
        int  tolen);          - - Adresslänge in Bytes
```

Mit *sendto* verschickt der Client eine Nachricht an den Server, der die Nachricht mit *recvfrom* aus dem Nachrichten-Puffer abholt.

Empfangen von Datagramen:

```
retcode = recvfrom (
        int  socket,          - - socket descriptor
        char  buf,            - - Zeiger auf Nachricht
        int  buflen,          - - Nachrichtenlänge
        int  flags,           - - Kontrollbits
        sockaddr_in  from,    - - Senderadresse
        int  fromlen);        - - Adresslänge
```

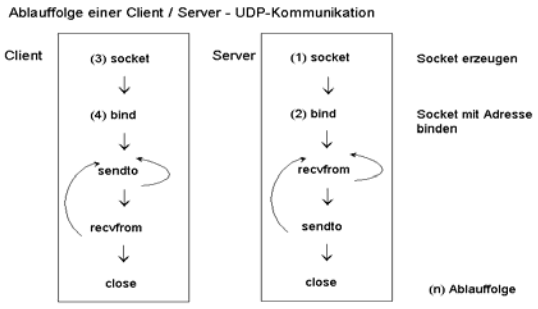


Abbildung 7.8: Ablauf einer Client/Server-UDP-Kommunikation

C: Stream-Kommunikation mit TCP

Für eine sichere Verbindung ist etwas mehr Aufwand nötig und dafür werden weitere Aufrufe verwendet. Neben **socket** und **bind** ist zusätzlich ein Verbindungsaufbau zu realisieren (**listen, accept, connect**). TCP-Verbindungen oder auch Stream-Kommunikation erfordern, dass

der Server an dem entsprechenden Port auf Verbindungsanfragen wartet. Um keine Blockierung des Servers nötig zu machen, werden Warteschlangen eingesetzt.

Ein Aufruf von listen legt sie Länge der Warteschlange fest und initialisiert sie:

```
retcode = listen (
        int  socket,          - -  Socket, der als Anlaufstelle definiert ist
        int  queue_length);   - -  Anzahl der aktiv möglichen Verbindungen

        RETURN:  0   erfolgreicher Aufruf;
                -1   Fehler
```

Dafür wird ein passiver Socket verwendet. Über diesen können nun keine Daten mehr ausgetauscht werden, da er ausschließlich für Verbindungswünsche verwendet wird.

Ein Aufruf von accept nimmt den nächsten Verbindungswunsch aus der Warteschlange und erzeugt einen neuen aktiven Socket, über den anschließend die eigentliche Kommunikation läuft.

```
new_socket = accept (
        int  socket,
        sockaddr_in  *  clientaddr,
        int  *   addrlen);
```

new_socket: implizit erzeugter neuer Socket, repräsentiert die neue TCP-Verbindung.
clientaddr: damit steht dem Server die Client-Adresse zur Verfügung (Puffer, in den die Client-Adressen kopiert werden).
addrlen: Länge des Pufferbereiches.

Der Aufruf von *accept* ist jedoch blockierend, wenn die Warteschlange leer ist.

Auf der Client-Seite stehen diesen Aufrufen beim Server (listen, accept) der aktive Verbindungsaufbauwunsch **connect** gegenüber (Socket mit Empfängeradresse verbinden)

```
retcode = connect (
        int  socket,              - -  sockid
        sockaddr_in  *  server,   - -  destaddr
        int  addrlen);
```

Die anschließende Verbindungsaufnahme wird mit einem Drei-Wege-Handshake Protokoll abgewickelt. Steht die Verbindung, kann mit read/write aus dem Socket gelesen bzw. auf ihm geschrieben werden, wie auf jedem anderen Stream (gepufferte E/A Operationen).

Senden / Empfangen über aufgebaute Verbindung: nach listen, accept, connect kann mit read und write über die Verbindung von beiden Seiten aus kommuniziert werden.

```
retcode = read (int  socket, char    buf, int  buflen);
retcode = write (int  socket, char    buf, int  buflen);
```

In retcode wird jeweils die Anzahl der gelesenen bzw. gesendeten Bytes zurückgegeben.
read / write analoges Verhalten wie bei Dateioperationen.
Insbesondere beim Lesen gilt:

- Puffergröße und Pufferfüllstand prüfen,
- Empfänger liest Nachrichten als Bytestrom und muss auf End-of-File- Bedingung achten.

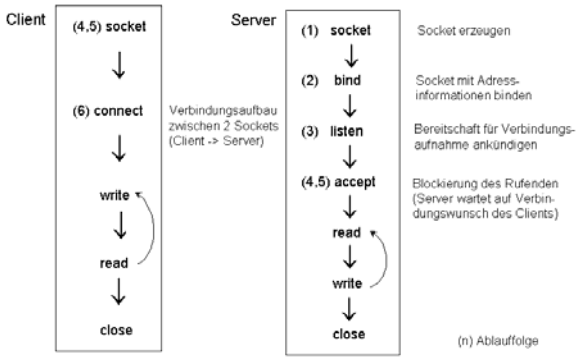


Abbildung 7.9: Ablauf Client/Server-TCP-Kommunikation

Selektives Warten
Ein Serverprozess kann auch *asynchron*, d.h. *nicht blockierend*, auf mehreren Sockets, auf mehreren Verbindungen bzw. Datagramme warten. Dies unterstützt der Aufruf

select: int sock1, sock2;
fd_set refds, wrfds, exfds;
sock1 = socket (AF_INET, ...);
sock2 = socket (AF_INET, ...);
FD_SET (sock1, &refds); - - setzt entsprechendes Bit in
FD_SET (sock 2, &refds); - - Menge der Filedeskriptoren
retcode = select (numfds, - - Anzahl der Filedeskriptoren
&refds, - - Lesedeskriptoren
&wrfds, - - Schreibdeskriptoren
&exfds, - - Deskriptoren für Ausnahmen
time out);

In retcode steht, an wievielen Sockets in der Menge der Deskriptoren ein Verbindungswunsch anliegt.
refds fungiert dabei als Bitvektor, d.h. für jeden Socket wird ein Bit gesetzt, sobald ein Verbindungswunsch für diesen Socket ankommt.
Durch entsprechende Interpretation des Bitvektors (z.B. Makro IS_SET) kann der Server herausfinden, welchen Socket er bedienen soll.

8 Sicherheit in Rechnernetzen

8.1 Sicherheit und Schutz (Problemstellung)

Angriffsarten
Verteilte Systeme besitzen zahlreiche Angriffspunkte für gewollte oder ungewollte Störungen des Betriebes. Die Bedrohung erfolgt in Quelle, Senke (Dateien, Ports, Speicherinhalte) und auf dem Weg von Quelle zu Senke (Datenpakete).

Unterbrechen:
Bewusste Störung des Übertragungssystems, indem z.B. das Netz aufgetrennt wird. Dies ist ein Angriff auf die **Verfügbarkeit** des Systems.

Abhören und Mitschneiden:
Erfolgt dies durch nicht autorisierte Teilnehmer, so handelt es sich um einen Angriff auf die **Vertraulichkeit** der Informationen.

Fälschen:
Werden Nachrichten während des Transports verändert, findet ein Angriff auf die **Integrität der Informationen** statt.

Hinzufügen, Generieren:
Ahmt ein nicht autorisierter Teilnehmer das Verhalten eines autorisierten Teilnehmers nach und erzeugt falsche Daten, so ist das ein Angriff auf die **Glaubwürdigkeit** des Systems.

Angriffsformen
Besitzt jemand Zugang zum System über einen Kommunikationskanal, so kann er auf fünf Wegen unautorisiert auf das System zugreifen (1 passiv, 4 aktiv):
Lauschangriff (eyesdropping):
Dies ist eine **passive Angriffsform**, die die Daten nicht verändert. Unbemerktes Abhören und Mitschneiden von Informationen zählt dazu. Der Inhalt bleibt unverändert.
Maskerade (masquerading):
Der Angreifer gibt sich als jemand anderes aus, z.B. als eine andere **Person** unter Zuhilfenahme eines falschen Passwortes oder ein **Prozess** verwendet eine falsche ID, um einen anderen Prozess **nachzuahmen**.
Intrigieren (tampering):
Nachrichten können bei der Übertragung verfälscht werden, so dass beim Empfänger ein **anderes Verhalten bewirkt** wird als vom Absender beabsichtigt ist.
Wiederholen (replay):
Nachrichten können (z.B. durch Lauschen oder Maskerade) **mitgeschnitten** und später unverändert erneut **gesendet** werden. Der Angreifer muss die Nachricht (z.B. übertragenes Zugangspasswort) nicht entschlüsseln können und kann sich unautorisiert Zugang zum System verschaffen. Notwendigkeit von Zeitstempel und Frische-Marken.
Verweigerung (denial of service):
Eine eingeschleuste Komponente verhindert angeforderte Diensterbringungen, weil sie Nachrichten nicht weiterleitet oder umleitet oder verfälscht. Auch die Netzüberflutung (flooding) mit willkürlichen Nachrichten (Überlast) kann zur Dienstverweigerung führen.

Für die vier **aktiven Angriffsformen** muss ein attackierendes Programm in das System gebracht werden, bevor es aktiv werden kann. Dazu kann ein dem Angreifer **bekanntes Passwort** oder eine **Umgehung der Autorisierung** eingesetzt werden. Ebenfalls möglich ist das Tarnen eines Programms als legitimes Programm und das Einbringen über legale Wege (z.B. Email). Diese nennt man dann auch **Virus-Programme**. Diese Programme können (für den Angreifer) sinnvolle Aufgaben ausführen oder einfach Zerstörung anrichten, z.B. indem sie sich immer weiter vervielfältigen und selbst weiter verbreiten. In diese Kategorie fallen auch so genannte **Würmer** (z.B. Internet-Wurm, 1988, Morris). Eine vierte Variante sind **Trojanische Pferde**, die als oft normales funktionsfähiges Programm auftreten, im Hintergrund aber noch anderer Funktionen ausführen. Sie öffnen Hintertüren im System oder täuschen Anmeldevorgänge vor (spoof login), um den Angreifer mit Zugangsinformationen zu versorgen.

Vertrauenswürdiges System
Es werden folgende Minimal-Anforderungen gestellt:
Abgesicherte Kommunikationskanäle:
Diese verhindern das unautorisierte Abhören und sind durch Kryptographie (Verschlüsselung) realisierbar.
Gegenseitiges Misstrauen:
Es findet immer eine Authentifizierung der Kommunikationspartner statt, um zu sichern, dass der Client ein rechtmäßiger Vertreter seiner Klasse ist und ob Server authentisch ist.
Frische (Aktualität) der Nachrichten:
Es ist sicherzustellen, dass Nachrichten nicht unbemerkt veraltet sein können, um Replay-Angriffe zu verhindern. **Zeitstempel**, **Tickets** oder sog. **Nonces** (angehängte Zufallszahlen, anhand derer sich Nachrichten bestimmten Sitzungen zuordnen lassen) leisten das.

Hauptsächlich drei Mechanismen eingesetzt, um die obigen Anforderungen zu erfüllen:

Verschlüsselung:
Nachrichten werden verschlüsselt und nicht im Klartext übertragen. Diese Methode wird auch verwendet, um Nachrichten digital zu signieren und somit sowohl den Autor eindeutig zu identifizieren als auch die Nachricht vor unbemerkter Veränderung zu schützen.

Authentisierung:
Hierfür wird eine vertrauenswürdige Basis eingesetzt, die **Schlüssel** (Passworte) verteilt und verwaltet, sowie z.B. Tickets generiert.

Zugriffskontrollmechanismen:
Hier werden Rechte für bestimmte Klassen von Teilnehmern (roles) geregelt. Zugriffe auf Ressourcen des verteilten Systems sind nur bestimmten Teilnehmern gestattet. Die Relation wird in Form von **Zugriffskontroll-Listen** (access lists) bzw. **Capabilities** verwaltet.

Verschlüsselungsverfahren (Kryptographie)

Verschlüsselung bildet die Basis der Sicherheitsstrategien in Rechnernetzen und verteilten Systemen. Verschlüsselung einer Information erfolgt durch eine Verschlüsselungsfunktion und einen Schlüssel. Schreibweise:

$F(K,M) \rightarrow \{M\}_K$

F: Verschlüsselungsfunktion
K: Schlüssel
M: unverschlüsselte Nachricht
$\{M\}_K$: mit Schlüssel K verschlüsselte Nachricht M

Schlüssel K:
- müssen sicher verteilt, sicher gespeichert sein.
- Vergabe und Verteilung durch vertrauenswürdigen *Schlüsseldienst.*
- Unterscheidung in Verschlüsselungsverfahren unter Verwendung
  - geheimer Schlüssel (private key, **symmetrische Verschlüsselung**) oder
  - öffentlicher Schlüssel (public key, **asymmetrische Verschlüsselung**).

Grundprinzip herkömmlicher (sog. symmetrischer) Verfahren
- Verschlüsselungsprinzip: Klartext -> Chiffre -> Klartext; viele herkömmliche Verfahren.
- Ver- und Entschlüsselung mit gleichem Schlüssel (geheim, private key).
- Schlüssel muss Sender und Empfänger bekannt sein.
- Vorbehaltlos sichere Verschlüsselungsverfahren, falls folgendes Kriterium erfüllt: Erzeugter chiffrierter Text enthält nicht genügend Informationen, um den Ausgangstext eindeutig zu bestimmen, unabhängig, wieviel chiffrierter Text zur Verfügung steht (einziges Verfahren: One-Time Pad).
- Berechnungssichere Verschlüsselungsverfahren, falls folgende Kriterien erfüllt: Aufwand zum Code-Knacken übersteigt den Wert der verschlüsselten Informationen; Die zum Knacken der Chiffre benötigte Zeit übersteigt die Brauchbarkeitsdauer der Informationen.

8.2 Symmetrische Verschlüsselung

8.2.1 Verschlüsselungsfunktion Schlüssel und Chiffrierer

Verschlüsselung

Verschlüsselung erfolgt durch eine Funktion, die auf die Daten und den Schlüssel angewendet wird. Eine dazugehörige Funktion zur Entschlüsselung liefert entsprechend die Daten zurück. **Symmetrische** Verfahren haben nur einen Schlüssel, der für beide Funktionen verwendet wird, **asymmetrische** besitzen jeweils einen eigenen Schlüssel.
Wichtig ist auf jeden Fall der Schutz des Schlüssels. Aus diesem Grund werden Schlüssel durch einen vertrauenswürdigen Schlüsseldienst verteilt und sicher gespeichert. Die Schlüssel

müssen nicht unbedingt alle geheim gehalten werden. Verfahren mit öffentlichen Schlüsseln (asymmetrische Verfahren) veröffentlichen jeweils einen der beiden Schlüssel, wohingegen Verfahren mit geheimen Schlüsseln (symmetrisch) dies verbieten.

Verfahren mit geheimen Schlüssel
Beide Kommunikationspartner A und B verwenden den gleichen, **geheimen** Schlüssel K (**private key**) -> sog. Symmetrische oder Private-Key - Verschlüsselungsverfahren.
Mit diesem Schlüssel verschlüsselt A seine Nachricht für B und verschickt sie. B entschlüsselt die erhaltene Nachricht mit dem gleichen Schlüssel K. Der Schlüssel K darf nur den Kommunikationspartnern bekannt sein. Also muss ein geheimer Schlüsselaustausch erfolgen.
Schlüssel sind nur dem Sender und dem Empfänger bekannt. Kodier- und Dekodierfunktionen können öffentlich sein (Kodier- und Dekodierfunktionen oft zu sich selbst invers).
Einsatz von Blockchiffrierer (wie CBC, DES, IDEA) und Stromchiffrierer (wie A5, RC4).

Blockchiffrierer
Verfahren teilen den Klartext in **gleich große Blöcke** und verschlüsseln diese, ohne die Blockgröße zu ändern. Es gibt vier Betriebsarten, Electronic Code Book (ECB) Modus, Cipher Block Chaining (CBC) Modus, Cipher Feedback Chaining (CFC) Modus und Output Feedback (OFB) Modus. Beispiele für solche Verfahren sind Data Encryption Standard (DES, 1973), Triple DES, Blowfish (1993) oder Cast (1996). Sie finden Anwendung in großem Umfang und gelten als sicher.
Prinzipiell lässt sich die Verschlüsselung rückberechnen durch Überprüfung aller Kodierungsmöglichkeiten, abhängig von Schlüssellänge und verwendeter Computer-Hardware. Ebenso schnelles Computing erforderlich. Bedeutsam ist bei diesen Verfahren vor allem die **Schlüssellänge**. Früher wurden Schlüssel mit 40 oder 56 Bit eingesetzt (z.B. bei DES), heute sind 168 Bit (bei Triple DES) Standard.
Tabelle (Preise 1998):

Schlüssellänge	Langsamer Pentium (ca. 1.000 $)	Dedizierte Hardware (ca. 100.000 $)	Dedizierte Hardware (ca. 1.000.000 $)
40 Bit	1 Monat	0,3 Sekunden	0,02 Sekunden
56 Bit	5000 Jahre	6 Stunden	35 Minuten
dabei ausgeführte Tests pro Sekunde	200.000	255.000.000	$3 * 10^{13}$

Stromchiffrierer
Einsatz bei symmetrischen Verschlüsselungsverfahren (geheime Schlüssel). Arbeitsweise:
- Aus einem geheimen Schlüssel wird ein Bitstrom erzeugt.
- Geheimtext = Klartext <*XOR*> Schlüsselstrom (Verschlüsselung).
- Klartext = Geheimtext <*XOR*> Schlüsselstrom (Entschlüsselung).

Beispiele:
A5: schneller, in Hardware implementierter Algorithmus, Verwendung im GSM-Netz.
SEAL: berechnet aus einem 160 Bit Schlüssel und einem 32-Bit-Index einen Zufallsstring, der dann den Schlüsselstrom bildet.
RC4: Verfahren nach Rivest.

8.2.2 Traditionelle Verschlüsselung

Überblick
- Ersetzungschiffre: Ersetzung von Buchstaben bzw. Buchstabengruppen unter Beibehaltung der Reihenfolgen der Klartextsysmbole. Verschiedene Chiffre-Verfahren:
  * Cäsarchiffre
  * Monoalphabetische Chiffre (u.a. DES)
  * Verschlüsselung mehrerer Buchstaben (Playfair)

  * Polyalphabetische Chiffre
  * Rotormaschinen
- Versetzungschiffre: Umstellung der Reihenfolge, keine Ersetzungszeichen.
- One-Time-Pads: Ausarbeitung einer nicht-brechbaren Chiffre.

Ersetzungschiffre
Jeder Buchstabe oder Buchstabengruppen wird durch einen anderen Buchstaben oder Buchstabengruppe ersetzt. Beibehalten der Reihenfolgen der Klartextsysmbole, diese werden nur verschoben. Bekannte Ersetzungschiffre:
Cäsarchiffre
- Ältester Ersetzungschiffre; Verschiebung um 3 Zeichen, wie a -> D, b -> F, ..., z -> C
- Verallgemeinerung: Verschiebung um k Zeichen.
- Chiffre leicht zu knacken: nur 26 Schlüsselkombinationen probieren.

Monoalphabetische Chiffre (u.a. DES)
- Jedes Symbol auf anderen Buchstaben abgebildet.
- Anwendung einer willkürlichen Ersetzung erweitert Schlüsselbereich drastisch.
- Chiffre erscheint sicher (26! Kombinationen probieren). Dennoch unsicher wegen der statischen Eigenschaften der natürlichen Sprache.

Verschlüsselung mehrerer Buchstaben
- Bekanntester Code: Playfair.
  Playfair-Algorithmus: Basiert auf 5*5 Matrix von Buchstaben, erstellt mittels eines Schlüsselwortes. Matrixerstellung: Buchstaben des Schlüsselwortes von links nach rechts und von oben nach unten eingetragen und dann übrige Matrix mit den verbleibenden Buchstaben in alphabetischer Reihenfolge gefüllt.
- Der Ausgangstext wird in Gruppen zu je zwei Buchstaben nach bestimmten Regeln verschlüsselt.

Polyalphabetische Chiffre
- Verbesserung der einfachen monoalphabetischen Technik durch Einsatz verschiedener monoalphabetischer Ersetzungen.

Rotormaschinen
- Maschine besteht aus einer Reihe voneinander unabhängig drehbarer Zylinder, durch die elektrische Impulse fließen.
- Jeder Zylinder hat 26 Anschlüsse zur Eingabe und 26 zur Ausgabe, die so verdrahtet sind, dass jeder Eingabeanschluss mit einem Ausgabeanschluss verbunden ist.
- Ein Zylinder entspricht einem polyalphabetischen Ersetzungsalgorithmus.

Versetzungschiffre
Während Ersetzungschiffre die Reihenfolge der Klartextsymbole beibehalten und diese nur verschleiern, stellen Versetzungschiffre die Buchstaben um, verwenden jedoch keine Ersetzungszeichen. Chiffre durch ein Wort verschlüsselt, das keine Buchstabenwiederholungen enthält. Durchführung in mehr als einer Stufe der Transposition macht diese Chiffre sicherer.

One-Time-Pads
Ausarbeitung einer nicht-knackbaren Chiffre ist relativ einfach:
- Zuerst Auswahl einer zufälligen Zeichenkette als Schlüssel.
- Danach Klartext in eine Zeichenkette konvertiert, z.B. anhand seiner ASCII-Darstellung.
- Dann Berechnung des EXCLUSIVE OR dieser zwei Ketten Bit für Bit.

Daraus resultierender Chiffretext kann nicht gebrochen werden (-> vorbehaltlos sicher). Zugehörige Methode: als One-Time-Pad bezeichnet (gilt als einzig bekanntes Verfahren).
Nachteile der Methode:
1. Schlüssel läßt sich nicht merken.

2. Verkürzung des zur Übertragung verwendbare Nutzdatenumfang durch den Schlüssel.
3. Methode ist empfindlich gegenüber verlorenen oder eingefügten Zeichen.

8.2.3 DES – Data Encryption Standard

DES – Verfahren

Eines der bekanntesten Verfahren mit geheimen Schlüsseln (1977: National Institute of Standards and Technology, USA), Blockchiffrier-Verfahren.
Eingabe zum DES: 64-bit Klartext und 56-bit Schlüssel. In 16 schlüsselabhängigen Runden werden Bitrotationen und zusätzlich 3 schlüsselunabhängige Transpositionen durchgeführt.
Ausgabe des DES: 64-bit verschlüsselter Text. Mit dem gleichen Schlüssel kann die Entschlüsselung erfolgen.
DES insbesondere für eine Umsetzung auf HW-Bausteine konzipiert. Für DES gibt es spezielle VLSI-Chips für die NW-Karte, um Daten in Echtzeit zu ver- und entschlüsseln.
DES-Schlüssel läßt sich ermitteln oder zurückrechnen, indem man zu einem bekannten chiffrierten und dechiffrierten Text alle $2^{56} = 7{,}2 \cdot 10^{16}$ Möglichkeiten überprüft. Dauer bei Test von 1 Mio. Schlüssel pro Sekunde: immerhin 1142 Jahre im Mittel.
Weitere Sicherheit: Schlüssel kann für jedes Nachrichtenpaket nach für beide Seiten bekannten Schema gewechselt werden, so dass Rückrechnungsaufwand nochmals wächst.
Mit *massiv paralleler Spezial-HW* lassen sich DES-verschlüsselte Informationern in Minuten entschlüsseln. Deshalb Verfahren mit längeren Schlüsseln entwickelt, wie

- Triple DES mit 168-bit Schlüssel für 64-bit Daten (Stallings, 1995).
- International Data Encryption Algorithm (IDEA; Lai / Massey, 1990) mit 128-bit-Schlüssel für 64-bit Daten.

Nachteile geheimer Schlüssel: Sender und Empfänger benötigen den Schlüssel; es muss Austausch des Schlüssels stattfinden -> anfällig gegen Angriffe.

DES-Verschlüsselung

Ausgangstext wird zunächst in Blöcken von 64 Bit verschlüsselt. Ergebnis: Chiffretext mit einer Länge von 64 Bit.
Algorithmus, parametrisiert von einem 56-Bit-Schlüssel, ist in 19 Einzelschritte aufgeteilt

- 1. Stufe: schlüsselunabhängige Versetzung des 64-Bit-Ausgangstextes.
- Vorletzte Stufe: die 32 Bit auf der linken Seite werden mit den 32 Bit auf der rechten Seite vertauscht.
- Restliche 16 Stufen: Funktionsweise identisch, jedoch von verschiedenen Funktionen des Schlüssels parametrisiert .
- Letzte Stufe: genaue Umkehrung des ersten Schritts.

Algorithmus so, dass die Nachricht mit dem Schlüssel entschlüsselt werden kann, mit dem sie verschlüsselt wurde. Dabei laufen die einzelnen Schritte in der umgekehrten Reihenfolge ab.

DES-Betriebsarten

DES (Data Encryption Standard) ist ein monoalphabetischer Ersetzungschiffre. Er arbeitet mit einem 64-Bit-Zeichen Blockchiffrierer. Bekannte Verfahren (Blockchiffrierer):

- ECB: Electronic Code Book Mode
- CBC: Cipher Block Chaining
- CFB: Cipher Feedback Block Mode
- OFM: Output Feedback Mode

Grundlegende Probleme bei DES:

- 56 Bit-Schlüssel viel zu kurz --> Brute-Force-Angriff möglich.
- Implementierungen von S-Boxen nicht bekannt --> könnte möglicher Angriffspunkt sein.

Abhilfe: **Triple DES**: Schlüssellänge 164 Bit mit 64 Bit Daten (Stallings, 1995)

8.2.4 IDEA – International Data Encryption Algorithm

IDEA: International Data Encryption Algorithm
- Verwendung Blockchiffrierer.
- Grundstruktur des Algorithmus IDEA ähnelt dem von DES dahingehend, dass Eingabeblöcke aus 64-Bit-Klartext in einer Folge parametrisierter Iterationen vermengt werden, um Ausgabenblöcke aus 64-Bit-Chiffretext zu erzeugen.
- Wegen der umfangreichen Bitmischung genügen 8 Iterationen.

8.2.5 Netzsicherheit

Probleme bezüglich Netzsicherheit -> Einteilung in 4 miteinander verflochtene Bereiche:
1. Geheimhaltung: Schutz vor unberechtigtem Zugriff.
2. Authentifikation: Ermittlung des Partners (mit wem man es zu tun hat).
3. Autorisierung (Nichtanerkennung): digitale Unterschriften
4. Integrität: Vertrauenswürdigkeit der Informationen

Die meisten Angriffe auf existierende Systeme sind absichtlich und bösartig.
Angriffsmotivationen (Beispiele):

Angreifer	Absicht
Student	Hat Spass daran, in den Emails anderer Leute zu schnüffeln
Hacker	Will Sicherheit auf Probe stellen und Daten klauen
Geschäftsmann	Interesse am Marketingplan der Konkurrenz

Aufgaben der Schichten (ist im Komplexen zu erbringen, nicht Einzelaufgabe):
* Bitübertragungsschicht: Verhinderung des Leitungsanzapfens bspw. dadurch, dass Übertragungsleitungen in Kabelkanälen mit Argongas unter Hochdruck gesetzt sind.
* Sicherungsschicht: Versendung kodierter Pakete in einer Punkt-zu-Punkt-Leitung ist möglich. Problem, wenn Pakete mehrere Routern durchlaufen; dann müssen sie in jedem decodiert werden.
* Vermittlungsschicht: Installation von Firewalls möglich.
* Transportschicht: Verschlüsselung kompletter Verbindungen von Ende zu Ende möglich. Lösung gültig hinsichtlich Geheimhaltung, aber ungenügend zu Authentisierung und Autorisierung.
* Verarbeitungsschicht: Vollständige Lösung der Probleme muss im Verarbeitungsprozess erfolgen.

Einschätzung und Resumé zu symmetrischen Verschlüsselungsverfahren
- Traditionelle symmetrischen Verschlüsselungsverfahren, insbes. DES und IDEA.
- Anwendung in vielen Protokollen (z.B. SSL und SHTTP).
- Anwendungsbeispiel: PGP (Pretty Good Privacy): Verwendung IDEA zur Verschlüsselung von Daten.
- Vorteil symmetrischer Verfahren gegenüber asymmetrischen: weniger rechenintensiv.
- Deswegen oft in Zusammenarbeit mit asymmetrischen Verfahren (z.B. RSA) eingesetzt. Beispiel: SSL-Protokoll (Secure Socket Layer). Daten werden mit Triple DES verschlüsselt, und Schlüssel mit dem asymmetrischen Verfahren RSA an Empfänger geschickt.

8.3 Asymmetrische Verfahren

8.3.1 Verfahren mit öffentlichen Schlüsseln

Öffentliche und private Schlüssel

Viele Daten in unverschlüsselter Form über Internet übertragen (allerdings stehen neue Techniken der sicheren Übertragung von Informationen zur Verfügung). Techniken basieren i.allg. auf Verschlüsselungsverfahren mit bestimmten Eigenschaften:

* Verschlüsselungsalgorithmen: öffentlich zugänglich (eine Verschlüsselung, in der nur das Verfahren geheim ist, gilt als unsicher).
* Öffentliche und private Schlüssel: mit öffentlichem Schlüssel kann jeder ein Dokument so verschlüsseln, dass es nur der Empfänger entschlüsseln kann, der den passenden privaten Schlüssel besitzt (jeder Anwender erzeugt seinen öffentlichen und privaten Schlüssel selbst).
* Voraussetzung: Algorithmen ungemein rechenaufwendig, um Zahlen in Primfaktoren zu zerlegen (Verschlüsselung nicht in sinnvollen Zeiträumen brechbar).

Für die Übertragung von vertraulichen Daten müssen moderne Verschlüsselungsverfahren angewendet werden.

Symmetrische Kryptosysteme: EIN Schlüssel, mit dem verschlüsselt und danach wieder entschlüsselt wird. Nachteile:

* beide Seiten müssen den Schlüssel besitzen,
* der Schlüssel muss zuerst ausgetauscht werden,
* Probleme bei Netzwerken --> die Übertragung kann abgehört werden.

Asymmetrische Kryptosysteme: ZWEI Schlüssel S und P.

* P (Public Key): öffentlicher Schlüssel - zum Verschlüsseln,
* S (Secure Key): geheimer Schlüssel - zum Entschlüsseln.

Mit P verschlüsselte Nachricht kann nur mit S entschlüsselt werden.

8.3.2 Grundlagen asymmetrischer Verfahren

Asymmetrische Verschlüsselungsverfahren

Mit der Anwendung öffentlicher und privater Schlüssel ist die nötige Sicherheit gegeben:

da S geheim ist, kann nur der Besitzer von S die Nachrichten entschlüsseln, die mit P (öffentlich) verschlüsselt wurden.

Damit ist sichergestellt, dass nur der gewünschte Empfänger die Daten erhält. Der Sender hat keine Schwierigkeiten, an den nötigen Schlüssel P zu kommen, da dieser sowieso öffentlich bekannt und damit nicht durch Abhören bedroht ist. Umgekehrt kann eine Nachricht nur dann mit P entschlüsselt werden, wenn sie mit S verschlüsselt wurde. Damit kann man die Identität des Absenders überprüfen.

Will man beides kombinieren, so muss man die Nachricht doppelt verschlüsseln: mit dem geheimen Schlüssel des Absenders und mit dem öffentlichen Schlüssel des Empfängers.

Bei der asymmetrischen Verschlüsselung kommen somit zwei Schlüssel zum Einsatz:

P (Public Key): öffentlich, zum Verschlüsseln
S (Secure Key): privat, zum Entschlüsseln

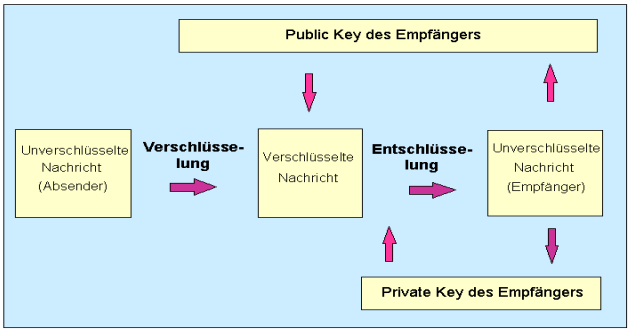


Abbildung 8.1: Asymmetrische Verschlüsselung

Nachteile asymmetrischer Kryptosysteme:
Asymmetrische Kryptosysteme sind viel langsamer als die symmetrischen. Deshalb werden beide Verfahren häufig kombiniert:

* Zuerst Erzeugung eines Schlüssels für ein symmetrisches Verfahren (sog. Session Key). Dieser Schlüssel nur für Dauer der Übertragung gültig.
* Dann asymmetrisches Verfahren für den Session Key-Austausch zwischen beiden Enden der Verbindung.
* Eigentliche Datenübertragung findet unter der Verwendung des symmetrischen Verfahrens statt --> hohe Effizienz.

Sicherheitsprobleme bei asymmetrischen Kryptosystemen:
Integrität des P/S-Schlüsselpaares: Öffentlicher Schlüssel gehört zwar zu einem bestimmtem Schlüssel S, aber unsicher, dass dieses Schlüsselpaar wirklich zu der Person gehört, die geheime Nachricht senden will. Problem: Integrität des Schlüssels, z.B. kann Schlüssel unter falschem Namen veröffentlicht werden. ~> deshalb ist Herkunft des Schlüssels zu überprüfen. Einfachste Methode: selbst überzeugen durch offline-Austausch des Schlüssels (Diskette, Briefpost) - aber auch problematisch (Entfernung, Kosten, mehrere Partner).
Abhilfe über ein **Zertifikat** (Beglaubigung) und eine 3. (vertrauenswürdige) Instanz: **Zeritifizierungsstelle**.
Digital: jeder öffentliche Schlüssel benötigt ein Zertifikat. Dazu Zertifizierungsstelle (**KCA: Key Certification Authority**): Unterzeichnung des öffentlichen Schlüssels mit eigenem geheimen Schlüssel. Digitale Unterschrift kann jeder mittels des öffentlichen Schlüssels der KCA auf ihre Gültigkeit überprüfen.

Algorithmen mit öffentlichen Schlüsseln (public key)
Um auf das Vertrauen zwischen Sender und Empfänger (wie bei geheimen Schlüsseln) verzichten zu können, wurde Prinzip der öffentlichen (public key) Schlüssel entwickelt (Deering / Hinden, 1995; im Zusammenhang mit IPv6).
Verfahren: Asymmetrische oder Public-Key - Verschlüsselungsverfahren:

* Verwendung eines Schlüsselpaares, bestehend aus einem öffentlichen und einem privaten Schlüssel.
* Der private Schlüssel bleibt beim Besitzer, der öffentliche muss “verbreitet” werden.
* Man darf den privaten nicht aus dem öffentlichen Schlüssel berechnen können.

Mathematische Basis öffentlicher Schlüssel: Produkt zweier sehr großer Primzahlen ($>10^{100}$) und Fakt, dass Zerlegung in Primfaktoren sehr aufwendig ist und lange dauert.

1. Ein potentieller Empfänger bildet Schlüsselpaar (K_e, K_d)
   K_e: öffentlicher Schlüssel (e: encryption)
   K_d: privater Schlüssel (d: decryption)
   Mit K_e können die Sender Nachrichten kodieren, die nur der Besitzer des privaten Schlüssels (K_d) dekodieren kann.
   Die beiden Schlüssel werden durch Verwendung einer Einwegfunktion (engl.: one-way-function) gebildet => aus Kenntnis eines Schlüssels läßt sich der andere Schlüssel nur extrem aufwendig herleiten.
2. Kodierfunktion E und Dekodierfunktion D dürfen ebenfalls öffentlich bekannt sein. Eine mit E und dem öffentlichen Schlüssel K_e verschlüsselte Nachricht läßt sich nur mit D und dem passenden Dekodierschlüssel K_d entpacken.

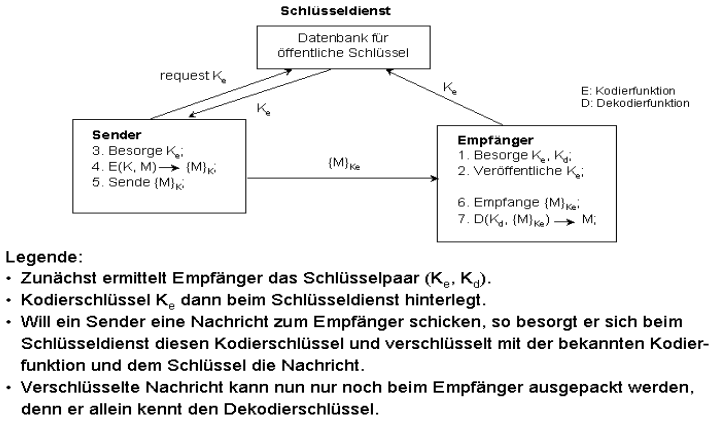


Abbildung 8.2: Verfahren mit öffentlichen Schlüsseln

8.3.3 RSA-Algorithmus

Anhand des **RSA**-Algorithmus wird die Funktionsweise von Verfahren beschrieben, deren Sicherheit auf dem Faktorisierungsproblem von großen Zahlen basiert. RSA ist benannt nach den Entwicklern **R**ivest, **S**hamir und **A**dleman und verwendet **Blockchiffrierung**. Die Grundidee ist, dass es sehr leicht ist, das Produkt zweier Primzahlen zu berechnen, jedoch sehr schwierig, eine große Zahl in Primfaktoren zu zerlegen (Faktorisierung).

Algorithmus:

Erster Schritt:

Auffinden zweier Zahlen e und d, die als Kodier- und Dekodierschlüssel dienen.

Algorithmus:

1. Wähle 2 Primzahlen P und Q (jeweils > 10^{100}) und bilde
   $N = P \cdot Q$ und $Z = (P - 1) \cdot (Q - 1)$
2. Wähle d frei als eine Zahl, die relativ prim zu Z ist, d.h. wähle d so, dass
   ggT (d, Z) = 1 ggT: größter gemeinsamer Teiler
3. Bestimme e aus Lösung der Gleichung
   $e \cdot 1 = 1 \mod Z$ mit e > Z d h . auch e muss relativ prim zu Z sein

Daraus 2 neue Schlüssel: Kodierschlüssel $K_e = < e, N >$
Dekodierschlüssel $K_d = < d, N >$

Zugehörige Funktionen: Kodierfunktion $E(e, N, M) := M^e \mod N = \{M\}$
Dekodierfunktion $D(d, N, \{M\}) := \{M\}^d \mod N = M$

Kodiert werden dann Nachrichtenblöcke, deren ganzzahlige Repräsentation kleiner N ist, d.h. ein Block mit k Bit kann kodiert werden, wobei $2^k < N$.

Praxiseinsatz von RSA

Als **Konzealationssystem** (concealation: Verbergung, Verheimlichung):
Jeder kann mit öffentlichen Schlüsseln c und n einen Klartext verschlüsseln und einen codierten Text an Inhaber der geheimen Schlüssel schicken. Nur dieser ist in der Lage, den Text mit Hilfe des geheimen Dechiffrierschlüssels wieder zu entschlüsseln; Vertraulichkeit der mitgeteilten Daten bleibt gewahrt.

Als **Signatursystem** (signature: Unterschrift):
öffentlich: Testschlüssel t (entspricht c) und n; geheim: p und q, sowie der Signaturschlüssel s (entspricht d). Um sich auszuweisen, verschlüsselt man einen Klartextblock mit Hilfe des geheimen Schlüssels und schickt den Klartext gemeinsam mit der Signatur (= dem verschlüsselten Text) an Empfänger. Dieser codiert die Signatur mittels des öffentlichen Testschlüssels und vergleicht den geschickten Klartext mit dem der Decodierung. Wenn diese identisch, ist Übersender der Botschaft derjenige, für den er sich ausgibt.

Sicherheitserhöhung für RSA
Alle bekannten Angriffe auf RSA bauen auf die multiplikative Struktur von RSA auf. Sicherheitserhöhung durch zusätzliche Einbindung einer nicht-multiplikativen Hashfunktion --> somit erhält man ein relativ sicheres Konzealations- bzw. Signatursystem:
Anwendung des Verfahrens bei **PGP (Pretty Good Privacy)**.

Zusammenfassung zu RSA
RSA zählt zu den "wohluntersuchten" Systemen, kann aber nicht als "*kryptographisch stark*" eingestuft werden, da noch keinen Beweis für die Sicherheit von RSA existiert.
RSA ist den anderen Systemen dann vorzuziehen, wenn weniger Wert auf absolute Sicherheit als vielmehr auf Effizienz und Geschwindigkeit gelegt wird.
Die Sicherheit von RSA beruht auf der Annahme, dass die Faktorisierung von n in die Primzahlen p und q mit heutigen Rechnern sehr schwer und zeitaufwendig ist.
Ein 429 Bit langer RSA-Schlüssel wurde bereits geknackt, ein 512-Bit Schlüssel wird deshalb angewendet, im Finanzsektor sogar ein 768-Bit-Schlüssel.
Heute wird ein 1024-Bit-Schlüssel als sicher angesehen. Jede Vergrößerung des Schlüssels um 10 Bit vergrößert die zu entschlüsselnden Zahlen um den Faktor 1000.

8.3.4 Weitere Verfahren mit öffentlichen Schlüsseln (DSS, Diffie-Hellmann)

DSS (Digital Signature Scheme)
Verfahren *Digital Signature Scheme* beruht auf einer Exponentialfunktion: Geeignet für Konstruktion von sicheren Authentisierungssystemen, dank der mathematischen Eigenschaften.
Problem der Berechnung des diskreten Logarithmus -> Umkehrung ist sehr schwierig, verhindert die Entschlüsselung. Denn zur Verschlüsselung wird eine zuvor gefundene Zahl mit dem Zeilencode der Nachricht potenziert; der Nachrichtencode stellt den Exponenten dar.
Die Wiedergewinnung des Exponenten äußerst schwierig, selbst wenn Basis der Expotentiation bekannt ist. DSS offiziell standardisiertes Verfahren.

Diffie-Hellmann-Protokoll
Schlüsselaustauschprotokoll von Diffie und Hellman basiert auf einer exponentiellen Einwegfunktion (analog zum DSS-Verfahren, Digital Signature Scheme):
- Jeder Teilnehmer wählt sich eine Zufallszahl als Basis und berechnet die Exponentialfunktion zu einer bekannten Grundzahl.
- Übergabe des Ergebnisses der Berechnung an die Kommunikationspartner.
- Partner benutzt dieses als Grundzahl und potenziert des Ergebnisses mit der jeweiligen Zufallszahl --> Gewinnung des Schlüssels.
- Wegen der Kommutativität der Expotentialfunktion --> beide Schlüssel der Partner damit gleich. Da für eine Entschlüsselung ein Unbeteiligter den diskreten Logarithmus berechnen müsste, ist dieses System als sicherer Schutz der Vertraulichkeit anzusehen.

8.3.5 Anwendungen (PGP, SSL)

PGP - Pretty Good Privacy
PGP ist eines der bekanntesten Verschlüsselungssysteme, die auf RSA aufsetzen. Es dient als Verschlüsselungsalgorithmus für signierte Nachrichten.

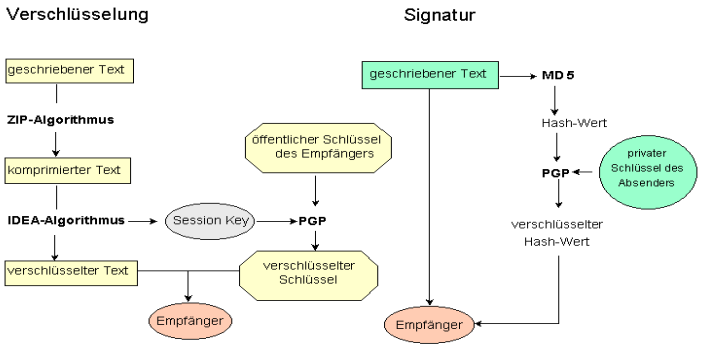


Abbildung 8.3: PGP (Pretty Good Privacy)

PGP arbeitet mit drei Verschlüsselungsmethoden:

- Austausch der Schlüssel unter Verwendung von RSA (asymmetrisch).
- Verschlüsselung der Nachricht selbst mit der symmetrischen Chiffre IDEA (International Data Encryption Algorithm); der Schlüssel wird zufällig erzeugt (Session Key, Sessionschlüssel).
- Zur Authentisierung / Signierung einer Nachricht wird MD5 verwendet (damit Erzeugung eines eindeutigen 128-Bit-Hashwertes der Nachricht).

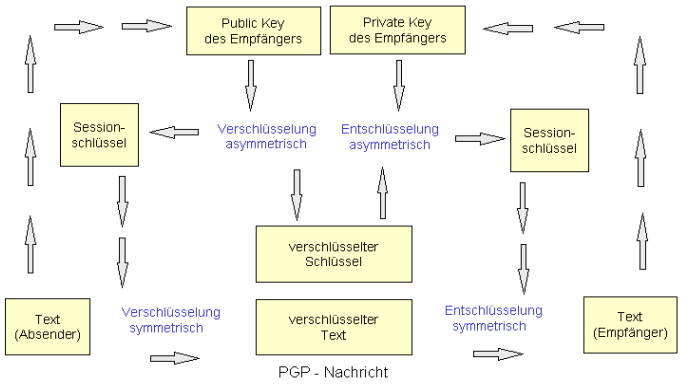


Abbildung 8.4: Verschlüsselungsalgorithmen bei PGP

SSL - Secure Socket Layer

Secure Socket Layer (SSL): weitere Anwendung, die die RSA-Verschlüsselung nutzt. Entwickelt von Netscape, stellt Verschlüsselung und Authentifikation ursprünglich für HTTP zur Verfügung:

- Vereinbarung eines Session-Schlüssels mittels eines Public-Key-Verfahrens (RSA) vor dem Verbindungsaufbau.
- Ermittlung eines Schlüssels für ein Private-Key-Verfahren, mit dem die eigentlichen Datenpakete verschlüsselt werden.
- Gewährleistung von Authentizität der verwendeten Public Keys mittels X.509-Zertifikaten.

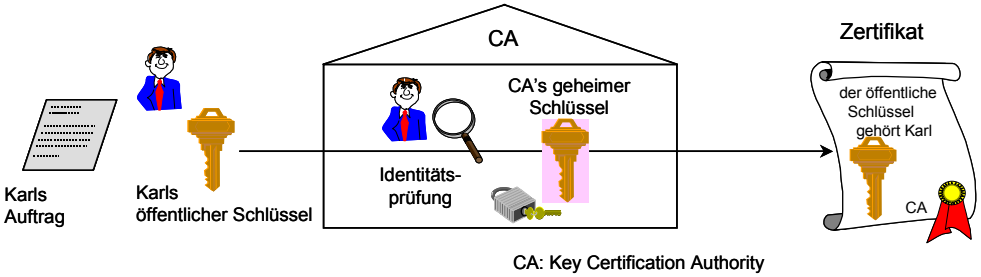


Abbildung 8.5: Zertifikat-Übergabe

X.509-Zertifikat:

- Enthält neben dem Namen des Inhabers Angaben zu Unternehmen oder Organisation, seine Email-Adresse und eine Gültigkeitsdauer.
  Eventuell noch einen beliebigen Kommentar und den Verwendungszweck, beispielsweise sichere Email, sichere Online-Verbindungen mit SSL, Signatur von Objekten (z.B. Java-Applets) oder anderen Zertifikaten.
- Wird einem Benutzer nur auf Antrag, und nachdem er sich gegenüber der CA (Key Certification Authority) nach einem genau festgelegten Prozess (CPS: Certificate Practice Statement) authentifiziert hat, zugeschickt.
- Verfahren nicht standardisiert. Es gibt Klassen von Zertifikaten (Abstufung der Verläßlichkeit), mit unterschiedlichen Authentisierungsprozessen und Kosten.

SSL ist eine Technik zur sicheren Datenübertragung über unsichere Verbindungen. Entwickelt wurde sie von Netscape und findet hauptsächlich in Web-Browsern Anwendung. Die Verbindung ist dann geheim, authentisch (über Zertifikate) und die Integrität der Datenpakete kann sichergestellt werden. In Zukunft soll das SSL Protokoll von IPng ersetzt werden.
Im OSI-Modell wird SSL über der Transportschicht und unter der Anwendungsschicht eingeschoben und in zwei Unterschichten eingeteilt, das SSL-Handshake-Protokoll und das SSL-Record-Protokoll.

Zusammenfassung
Alle genannten Verschlüsselungsmethoden werden heute auch in vielen anderen Programmen, Plugins und Applets benutzt. Allerdings können alle Programme, die in USA geschrieben wurden, nicht als sehr sicher angesehen werden, denn die NSA (National Security Authority) begrenzt den Export der sicheren Verschlüsselungsprogramme, z.B. wurde die zulässige Länge des RSA-Schlüssels auf 512 Bit grenzt, obwohl diese Verschlüsselung erst ab einer Länge von 768 Bit wirklich sicher ist.
Deshalb ist heutzutage die Entwicklung von neuen Verschlüsselungssystemen in Europa sehr gefragt, die nicht den US-amerikanischen Exportbedingungen unterliegen.

9 Aspekte der Anwendungsschicht

9.1 Dienste im Überblick

Dienste der Schicht 7 (Application Layer, Anwendungsschicht)
Subschichten Schicht 7b (Anwendung), Schicht 7a (Dienste zur Anwendung), insbes. zu
- Netzverwaltung (Management-Dienste) und
- Anwendungsunterstützung und -dienste

Standard-Dienstleistungen in ISO/OSI:
ISO - CASE (Common Application Service Elements): Satz von Dienstleistungen, die in anderen (verteilten) Anwendungen nutzbar
CCITT - RTS (Reliable Transfer Service), für CCITT-Empfehlung X.400 (E-Mail)
CCITT - ROS (Remote Operation Service)
OSI - Dienstelemente
ACSE (Association Control Service Element) zur Assoziationssteuerung

CCR (Commitment, Concurrency, Recovery) zur Festwertübergabe, Mehrfachbearbeitung, Wiederherstellung

Standard-Dienste/Protokolle im Internet: FTP, SMTP, Telnet, SNMP, HTTP

Anwendungsdienste (ITU-TS)

- Filedienste: Dateitransfer, - zugriff, -verwaltung
  ISO - FTAM (File Transfer, Access and Management), automatischer Dateitransfer
- Terminaldienst: ECM -VTP (Virtual Terminal Protocol)
  Verwendung Terminals unterschiedlicher Hersteller als NW-Arbeitsstationen
- Elektronische Post (Electronic Mail, Mailbox):
  u.a. CCITT - MHS (Message Handling System)
  CCITT - X.400 (Ositel)
  OSI - MOTIS (ISO/OSI); seit 1988 starke Annäherung MOTIS u. X.400 E-Mail-Dienste in TCP/IP-Netzen, u.a. elm, pine (i.w. POP: Post Office Protocol)
- Verzeichnisdienst: CCITT-Directory Service (X.500)
- Dienste für entfernte Auftragsbearbeitung: RJE (Jobtransfer- und -verwaltung)
- Bildspeicherung und Übertragung
- Telematikdienste: Teletext, Bildschirmtext (Viewdata), E-Mail, Telepräsenz, WfMS, EDI
  Teleconferencing (interaktiv: Audio/Video, Chat; nicht-interaktiv: textuell)
  Teleteaching ... Tele-Universität, Kollaborationssysteme

Dienste in anderen Rechnernetzen

- *Internet* (Übernahme aus ARPAnet)
  FTP File Transfer Protocol
  NETBLT NetWork Block Transfer, für schnelle Übertragung (direkt auf IP, ohne TCP)
  SMTP Simple Mail Transfer Protocol: für Email mit Postformat RFC 822 (POP, IMAP), Adressierungsschema: name @ domäne
  z.B. meier@informatik.uni-leipzig.de (andere Subdomains: uk, edu, com, ...)
  TELNET Anwendungsdienst bzw. Protokoll für virtuelle Terminals
  => verwendet für “Entferntes Einloggen”
  Übernahme FTP, Telnet in viele andere Systeme, die TCP/IP als Grundlage für Kommunikation haben, z.B. UNIX, MS-Windows
  HTTP HyperText Transfer Protocol: Basis für WWW
  LDAP Lightweight Directory Access Protocol: Basis für Verzeichnisdienst
- *MAP (Manufacturing Automation Protocol, General Motors)*
  - MAC: Token-Bus
  - ACSE, FTAM, Verzeichnisdienst (nicht CCR, JTM), VTP nur teilweise
  - statt X.400 Verwendung des Nachrichtensystems MMS (Manufacturing Message System, Fertigungs-Nachrichtennorm: für Kommunikation zwischen Maschinen)
- *TOP (Technical Office Protocol, Boeing)*
  - MAC: Ethernet
  - ACSE, FTAM, Verzeichnisdienst, VTP (nicht CCR, JTM)
  - X.400 - Mailbox
- *USENET*
  - Maildienst (kompatibel zu ARPA-Postsystem auf Basis SMTP)
  - News-Dienst (UsenetNews, News): weltweiter Diskussionsdienst, “schwarzes” Brett, Teilnehmer jeder Nachrichtengruppe können alle dort abgelegten Nachrichten lesen.

9.2 Filedienste

Virtueller Filedienst

Filedienste ermöglichen Zugriff zu lokalen und entfernten Dateien und Dateitransfer. Filedienst ist Funktion der OSI-Schicht 7, nutzt aber zu Filedienst-Erbringung (wegen Heterogenität der Computer) die Hilfe der OSI-Schicht 6 (Datenkonvertierung).
Im Internet: Schicht 4, mit anwendungsspezifischem Protokoll FTP.
Filedienste gestatten
* Herstellen und Übertragen von Filekopien (Filekopierdienst)
* Arbeit mit lokalen und entfernten Dateien (Zugriff für beide gleich gestaltet).

Wegen Inhomogenität der Dateisysteme (Datenstrukturen, Codes, Zugriffstechniken, Dateiverwaltung) werden sog. virtuelle Filedienste (virtual file store, virtuelle Dateispeicher) eingerichtet. Aufgabe: Vereinheitlichen des Verhaltens der im RN enthaltenen Dateisysteme.
Realisierung des virtuellen Filedienstes mittles eines virtuellen Dateiverwaltungssystems:
- standardisierte Festlegungen zur Darstellung der realen Dateiverwaltungssysteme (Standard-Protokolle)
- Zugriff mit Netzfile-Zugriffsmethode (Abbildung der Zugriffsoperationen auf die einzelnen Operationen der einzelnen Computer)

Für die einzelnen Filedienste existieren in jedem Rechner spezielle Filezugriffs- bzw. Fileübertragungsprotokolle, z.B. FTP (File Transfer Protocol) im Internet
und verteilte Dateisysteme, z.B. NFS (Network File System) SUN
RFS (Remote File System) OSI
DFS (Distributed File System) DCE
Prospero (im Internet), zusammen mit Archie

FTAM (File Transfer, Access and Management)
- Standardisierter Filedienst in OSI-Strukturen: ISO 8571
- Beruhend auf Initiator-Responder-Prinzip (identisch zu Client-Server-Prinzip)

Auf Benutzung der FTAM-Dienstleistungen beruhen die meisten Anwendungsdienste in Rechnernetzen sowie ISO-Anwendungsdienste, die nicht zum Definitionsbereich des OSI-Referenzmodells gehören, z.B. ODA/ODIF (MM-Dokumente), EDI/EDIFACT (elektronischer Dokumentenaustausch im Büro).

9.3 Virtuelles Terminal

Terminaldienste
Problemstellungen
- Vielzahl unterschiedlicher Terminals,
- Nicht einheitliche Verwendung sog. ESCAPE-Folgen (Zeichenfolgen zur Kursorsteuerung, Inversmodus, Einfügemodus, ...).

Normierung durch OSI: Virtuelles Terminal (VT)
Ziele:
* Gestattung der Variantenvielfalt (Bildschirm, Tastatur, Drucker) realer Terminals,
* Einheitliche Anschlussbedingungen,
* Abbildung des Funktions-Vorrats der realen Terminals auf Funktionen eines virtuellen Terminals.

Ein Virtuelles Terminal ist eine Datenstruktur, die den abstrakten Zustand des realen Terminals darstellt. Computer realisiert die Abbildungen zwischen realer und abstrakter Datenstruktur. Zum Virtuellen Terminal gehören
- Spezifikation der Schnittstelle für Virtuelles-Terminal - Dienste und
- Virtuelles Terminalprotokoll (VTP) zur Festlegung der Kommunikation zwischen Mensch und Applikation.

9.4 Telematik-Dienste

Telematik
Telematik: Kunstwort aus **Tele**kommunikation und Infor**matik.**

Telematikdienste: Kommunikationsdienste, gestützt auf Rechnernetze, Nutzung der nachrichten- und rechentechnischen Mittel.
Typische Merkmale:
- Übermittlung codierter Textdaten, Sprache, Bild und Videosequenzen (multimedial)
- Kommunikation mit Endgeräten, die das elektronische Erstellen, Aufbereiten und Senden/Empfangen von Dokumenten gestatten (Text, Audio/Video).
  (Prinzipiell auch Teletex und Faksimile --> dies sind aber Standarddienste der öffentlichen Datennetze)

Bekannte Anwendungen:
- Elektronische Post
- Telekonferenz (nicht-interaktiv)
- Audio/Videokonferenz (interaktiv)

Elektronische Post (Mailbox-Service)
Realisierung einer asynchronen Kommunikation zwischen Mensch und Computer über dialogfähige Terminals. Basiert auf der sog. "Briefkastenmethode":
- Nachricht in Briefkasten (Mailbox) hinterlegt, Adressat muss nicht aktiv eingeloggt sein,
- Adressat kann zu späterer Zeit auf diese Nachricht zugreifen und darüber verfügen,
- Jeder Teilnehmer (mit eigenem Account) erhält seine eigene Mailbox, auf die nur er selbst Zugriff erhält.

Ausgangspunkt: ARPAnet mit SMTP (Mail-Protokoll) und Postformat RFC 822 (POP: Post Office Protocol). Maildienst ist nicht nur eine Sonderform des Dateitransfers, sondern eine Form der Mensch-Maschine-Kommunikation:
- es sind strukturierte Dateien (Texte), Ergänzung durch MIME (Audio (wave) und Video),
- sie enthalten Sender- und Empfängeradressen,
- enthalten weitere Informationen, u.a. Sender- und Empfänger-Namen (ggf. Namensliste, Kopien), Versanddaten, Bezug zum Inhalt (Subject).

Viele private und staatliche Telefongesellschaften haben elektronische Post in ihr Dienstaufgebot aufgenommen. Zur Vermeidung eines Chaos wurde 1984 von der CCITT die Protokollserie X.400 als Empfehlung für sog. MHS (Message Handling Systems, Nachrichtenbehandlungssysteme) definiert. ISO versuchte, dies unter der Bezeichnung MOTIS (Message-Oriented Text Interchange System, nachrichtenorientiertes Textaustauschsystem) zu übernehmen. Probleme wegen fehlender Struktur in X.400. 1988 glich CCITT X.400 mit MOTIS ab. MOTIS/X.400 entwickelte sich zur Standardform der CCITT
Dem gegenüber stehen die E-Mail-Systeme in TCP/IP-Netzen, u.a. elm, pine, Mailbox-Dienste in WWW-Browsern (wie Mosaic, Netscape, Mozilla Thunderbird, Internet Explorer).
Aufbau eines Mailbox-Systems:

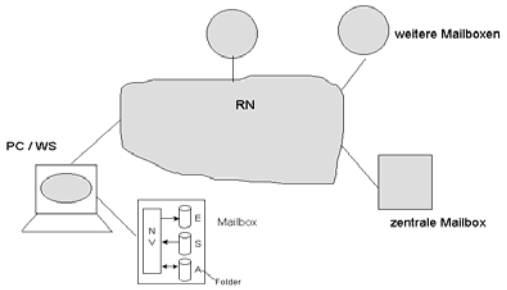


Abbildung 9.1: Aufbau Mailbox-System

Komponenten:
- Speicher (Folder)

für empfangene Nachrichten (lesen: Inbox)
zu sendene Nachrichten (schreiben: Sentbox)
Entwurfsnachrichten (Draft), gelöschte Nachrichten (Thrash)
zu archivierende Nachrichten

- Nachrichtenverwalter für
  Verwaltung der Nachrichten (Senden, Empfangen, Löschen, ...)
  Verwaltung der Nachrichten-Speicher
  Koordinierung der Wechselwirkungen mit anderen Teilnehmern

Weitere Funktionen des Mailbox-Services:

Lokale Funktionen:
- Systemunterstützung für Zugriff auf eigene Mailbox (Abfragen, Auswahl von Nachrichten, Löschen, ...)
- Editorfunktionen

Entfernte Funktionen:
- Systemunterstützungen für Kommunikation mit anderen Mailboxen
- Zuschalten einer Mailbox zur aktiven Teilnahme
- Abschalten
- Explizites Quittieren von Nachrichten

Service-Funktionen: Weitere Hilfs-Funktionen, u.a.
- Ändern Zugriffsrechte
- Anzeige der erreichbaren Teilnehmer
- Nachrichtenaufbereitung (Header, ...)

MIME: Multimedia-Erweiterung für Mail im Internet (Erweiterung für Audio, Video, Nicht-ASCII-Zeichen, Binärdaten)

Telekonferenz

Neue Form der Mensch-Maschine-Kommunikation auf Basis von Rechner-Nachrichten. Rechnernetz dient als Kommunikationsmittel / system. Zusammenführen geographisch getrennter Kommunikationspartner.

Nicht-interaktive Telekonferenzsysteme

- Verfahren: Briefkastenmethode (asynchrone Kommunikation)
- Textinformationen
- Teilnehmer müssen nicht gleichzeitig anwesend sein

Heute weitestgehend verdrängt durch interaktive (synchrone) Telekonferenzsysteme.

Interaktive Telekonferenzsysteme (Audio/Videokonferenzsystem)

- synchrone Kommunikation
- Übertragung Text, Audio, Images (Bilder), Videosequenzen
- Auswahl von Telekonferenzsystemen
  Internet: MBone (Multicast-Backbone) und MBone-Tools (vic, vat, wb, ...)
  Microsoft: Netmeeting (Basis H.361)
  verschiedene ISDN-basierte Systeme (Basis H. 320), u.a. PictureTel, ProShare, Hicom
  Visitphone: Entwicklung Uni Leipzig / RN & VS (Basis ATM)
  DFNVC: DFN Video Conferencing - Dienst

Spezieller “Telekonferenz”-Dienst: Chat-Dienst: Textaustausch im Dialog.

Anwendung Multimedia

- Übertragung von Texten, auditiven Medien (Sprache, Musik, Geräusche) und visuellen Medien (Standbilder, Bewegtbilder, Videosequenzen),
  Synchrone Kommunikation zwischen 2 oder mehreren Partnern;
- Hochgeschwindigkeits-Übertragung (Bewegtbilder, TV-Qualität: $v_{ü} > 20$ Mbit/s), Datenkompressionen (JPEG, M-JPEG, MPEG, H.261), Bandbreitenreservierung, CPU-Power

Nutzungsszenarien

- Konferenzschaltung zw. 2 oder mehreren Teilnehmern: Adresse: <nutzer>@<domain>
- Konferenzteilnehmer können sich sehen und hören

- Shared Applications (z.B. Zeichenblatt, Whiteboard)
- Ergänzung durch asynchrone Kommunikation: Multimedia-Mail (mit MIME-Erweiterung)

9.5 Entfernte Auftragsbearbeitung

Jobfernverarbeitung

Entfernte Verarbeitung von Computeraufträgen (Jobfernverarbeitung). Ursprung aus Datenfernverarbeitungs (DFV)-Technologie; heute: Bedeutung in Supercomputer-Nutzung.
Typische Dienste: ROS: Remote Operation Service, RJE: Remote Job Entry
RJE: Entfernte Abarbeitung von Jobs in Stapelverarbeitungs-Betriebsweise: Übergabe Job an (entfernten) Zielrechner, Rückführung der Ergebnisse.
Zusätzlicher Services im RJE-Dienst:
Information über aktuellen Stand der Jobverarbeitung, ggf. Abbruch der Jobverarbeitung (cancellation), Übermittlung von Systemnachrichten, Transfer von Nutzer-Dateien, Operator-Operator-Kommunikation.
Protokoll: RJE-Protokoll (JCL: Job Control Language)
Verarbeitungsweisen:

- nutzergesteuert: Teilnehmer wählt Zielrechner aus (JCL)
- vollautomatisch: RJE-Dienst wirkt als virtuelle Maschine (keine JCL-Spezifikation der einzelnen Maschinen).

Teil IntW3: Internet und WWW

Teil 2: Ausgewählte Netze

Teil 3: Übertragungssysteme

24 Literatur

Berghoff, J.; Wittmann,R.: Multicast. Protokolle, Programmierung, Anwendung. dpunkt,1997
Braun, T.: Zitterbart, M.: Hochleistungskommunikation, Bd. I und II. Oldenburg, 1996
Häckelmann, H.; Petzold, H.J.; Strahringer, S.: Kommunikationssysteme. Springer, 2000
Huitema, C.: IPv6: The New Internet Protocol. Prentice-Hall, Englewood Cliffs, 1996
Lockemann,P.; Krüger,G.; Krumm,H.: Telekommunikation u. Datenhaltung. Hanser,1993
Kurose, J.F.; Ross, K.W.: Computernetze (Top-Down-Ansatz mit Schwerpunkt Internet). Pearson Education/Addison Wesley, München, 2002
Kyas, O.: ATM Netzwerke. Datacom, 1996
Müller, G.; Eymann, T.; Kreutzer, M.: Telematik- und Kommunikationssysteme in der vernetzten Wirtschaft. Oldenbourg Verlag München/Wien, 2003
Perlman, R.: Interconnections: Bridges and Routers. Addison-Wesley, Reading, 1993
Peterson, L.L.; Davie, B.S.: Computernetze. dpunkt, 2000
Proakis, J.G.; Salehi, M.: Grundlagen der Kommunikationstechnik. Pearson Studium, München, 2004
Rose, M.T.: TCP/IP-Netze. Carl-Hanser, München, 1994
Schäfer, G.: Netzsicherheit. Algorithmische Grundlagen und Protokolle. dpunkt, Heidelberg, 2003
Sinz, W.: Lokale Netze. dpunkt, Heidelberg, 1996
Stevens, D.L.: Netzwerkprogrammierung. Prentice-Hall, 1994
Tanenbaum, A.S.: Computer-Netzwerke. Pearson Studium, München, 2003
Walke, B.: Mobilfunknetze und ihre Protokolle 1/2. Teubner, 2000