Lernskript
„Technisch-angewandte Informatik“

Kerngebiete:

Technische Informatik

Angewandte Informatik

Vertiefungsgebiet:

A1 (Methoden der Informatik für spezielle Anwendungen)

DATENÜBERTRAGUNGSTECHNIKEN
UND -SYSTEME

nach Tanenbaum: „Computernetzwerke“

Einleitung

- Rechnernetz:
  eine Anzahl miteinander verbundener eigenständiger Hosts. Der Anwender hat genau Kontrolle darüber, was wo abläuft.
- verteiltes System:
  der Benutzer benutzt ein virtuelles System. Welche physikalischen Ressourcen dabei angesprochen werden, ist für ihn nicht sichtbar.

SAP (service access point) = Zieladresse eines Partners (Frequenz, Rufnummer, IP-Adresse o.ä.)

Warum Rechnernetze?

- Unternehmen können Informationen überall verfügbar machen.
- Ressourcen können gemeinsam benutzt werden (ein Farblaserdrucker für eine Person wäre übertrieben).
- Erhöhung der Verfügbarkeit durch mehrere Systeme.
- Viele kleine Systeme sind billiger als wenige Großrechner.

Wie hat sich die Vernetzung zeitlich verändert?

Früher hatte man Terminals an einem Großrechner. Heute hat man viele selbstständige Workstations und aufgabenbezogene Server (Fileserver, Mailserver).

Adressierungsmöglichkeiten

- **Broadcast**
  Ein Datenpaket wird (in einem gewissen Bereich – also nicht über das ganze Internet) an alle angeschlossenen Empfänger geschickt. Ein Broadcast-Code kann die Empfängergruppe angeben. Wer sich dafür nicht interessiert, erhält die Nachricht zwar, kann sie aber ignorieren.
- **Point-to-Point**
  Eine Kommunikation mit einem adressierten Ziel. Das Datenpaket kann aber über mehrere Systeme geroutet werden, bevor es beim Empfänger ankommt.

Reichweite von Netzen

	Entfernung	Übertragungstechnik	Topologie
LAN (local area network)	10m - 1km	Kupfer, 10/100 MBit	Bus IEEE 802.3 (=Ethernet)
MAN (metropolitan area network)	10km		
WAN (wide area network)	100km - 1000km	Satellitenfunk, Bodenfunk	Router
Wireless LAN	- 500m	Funk	
„Wireless WAN“	∞	Funk	Miteinander verbundene Funkzellen

Bei MANs (Stadtnetzen) hat man meist zwei Leitungen. Eine Leitung für jede Flussrichtung.

Zu Funknetzen:

- drahtlos: Funkverbindung zum Netz
- mobil: tragbarer Computer (z.B. Notebook oder PDA)

Nachteil bei Funknetzen:

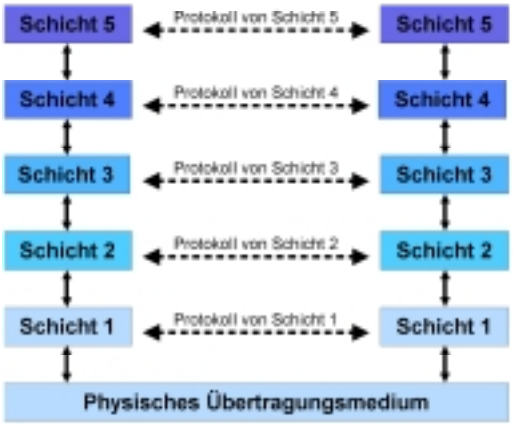
- langsamer als verdrahtete Netze
- fehleranfälliger

Netzkopplungen

- **Router**:
  Verbindungspunkte zwischen gleichartigen Netzen

- **Gateways**:
  Verbindungspunkte zwischen inkompatiblen Netzen

Schichtenmodell



Netzarchitektur = Gruppe von Schichten und Protokollen

Das Schichtenmodell hat den Vorteil, dass man eine Applikation entwickeln kann, ohne sich um die unteren Schichten Gedanken machen muss. Außerdem kann man z.B. das Übertragungsmedium von Kupfer auf Glasfaser umstellen, ohne dass sich was an den Anwendungsprotokollen ändern muss. Protokolle der unteren Schichten können die Datenpakete auch zerlegen oder kodieren. Wichtig ist nur, dass die Pakete auf der Gegenseite (Peer) in der umgekehrten Reihenfolge nach denselben Konventionen dekodiert wird. Jede Schicht kann unabhängig von jeder anderen geändert werden, solange die Änderung auf beiden Seiten vorgenommen wird. Es werden immer Header bei jeder Schicht hinzugefügt und beim Empfänger wieder entfernt.

Multiplexen = mehrere Verbindungen werden zu einer Verbindung zusammengefasst (Beispiel: einige tausend Telefongespräche über eine Glasfaserverbindung).

Verbindungsorientierung

- **verbindungorientiert**:
  Es wird eine logische Verbindung zwischen zwei Peers aufgebaut, über die dann Pakete in der richtigen Reihenfolge übertragen werden können. (Analogie: Telefonsystem)
  Beispiel: Telnet-Sitzung, Voice-over-IP
- **verbindungslos**:
  Ein Datenpaket wird adressiert und losgeschickt. Der Empfänger erhält es (hoffentlich). Die Reihenfolge der Pakete kommen aber nicht garantiert in der gesendeten Reihenfolge an. (Analogie: Postsystem)
  Beispiel: Datenbankanfrage, Nameserveranfrage

Dienstqualität (Quality of Service = QoS)

Manchmal möchte man ein schnelles Protokoll (Datengramm-Dienst) für Echtzeitanwendungen haben (Telefonie, Video), wo mal ein paar Bits verlorengehen können. Manchmal braucht man aber auch gesicherte Dienste (Dateidienst, Email), die lieber sicher und dafür langsamer sind.

Referenzmodelle

ISO OSI (Open Systems Interconnection)

- **7 - Anwendungsschicht** (application layer):
  Anwendungsprotokolle (Email, Jobverwaltung...).
- **6 - Darstellungsschicht** (presentation layer):
  Kodierung (ASCII, Unicode, Fließkommazahlen).
- **5 - Sitzungsschicht** (session layer):
  Synchronisation, Dialogsteuerung, Duplex/Simplex-Verbindungen
- **4 - Transportschicht** (transport layer):
  Aufbau von Punkt-zu-Punkt-Verbindungen.
- **3 - Vermittlungsschicht** (network layer):
  Routing der Datenpakete, um das Netz optimal auszulasten.
- **2 - Sicherungsschicht** (data link layer):
  Datenmengen werden in Rahmen aufgeteilt, Fehlerkorrektur
- **1 - Bitübertragungsschicht** (physical layer):
  Ein Bit mit 0 oder 1 muss einwandfrei übertragen werden. Wieviel Volt ist 1? Wieviele Mikrosekunden dauert ein Bit?

- Ebene 1-3:
  Punkt-zu-Punkt. Hier schalten sich auch Relais während der Übertragung ein.
- Ebene 4-7:
  Ende-zu-Ende. Diese Ebenen werden nur von den Peers benutzt.

Konzepte

- **Dienst**:
  Wie funktioniert eine Schicht? Was bietet sie an? Wie können andere Schichten darauf zugreifen?
- **Schnittstelle**:
  Verbindung zwischen zwei Schichten
- **Protokoll**:
  Semantische Beschreibung der ausgetauschten Daten

TCP/IP

TCP/IP ist das Protokoll des Internets, das auf dem ARPANET basiert, das im Auftrag des amerikanischen Verteidigungsministeriums entwickelt wurde. Das ARPANET sollte so konstruiert werden, dass auch bei Kriegseinwirkung an einem Netzknoten alle anderen Knoten weiter kommunizieren könnten (Routing). Außerdem sollte TCP/IP die verschiedenen benutzten Protokolle durch ein einheitliches Protokoll ersetzen.

1. **Bitübertragungsschicht**:
   Ethernet, Satellitenfunk
2. **Internetschicht (IP)**:
   Zustellung von IP-Paketen an den Empfänger. Ungesichert. Nicht unbedingt korrekte Reihenfolge.
3. **Transportschicht**:
   TCP (transmission control protocol = verbindungorientiert, zuverlässig)
   UDP (user datagram protocol = verbindungslos, unzuverlässig)
4. **Anwendungsschicht**:
   TELNET (Terminal)
   FTP (Dateitransfer)
   SMTP (Mailtransfer)

Vergleich OSI und TCP/IP

OSI	TCP/IP	Beispiele bei TCP/IP	Aufgaben
Anwendungsschicht	Anwendungsschicht	SMTP, DNS, TELNET, FTP	verschiedene Anwendungen
Darstellungsschicht			
Sitzungsschicht			
Transportschicht	Transportschicht	TCP, UDP	Verwaltung von Verbindungen, direkt Peer-To-Peer, QoS
Vermittlungsschicht	Internetschicht	IP	Routing, Überwachung der Auslastung
Sicherungsschicht	Bitübertragungsschicht	SLIP, PPP	Rahmen erstellen, Fehlerkorrektur
Bitübertragungsschicht		Ethernet (802.3), SATNET	Spezifikation der physikalischen Schnittstellen

Nachteile von OSI

- ist sehr komplex und schwer zu implementieren
- viele Entscheidungen wurden politisch und nicht technisch getroffen
- TCP/IP war im Berkeley UNIX schon integriert und funktionsfähig
- vergleichsweise langsam durch unnötige Schichten (5 und 6)
- schlechtes Image (OSI wurde zwangweise durch die Regierungen gefördert)

Nachteile von TCP/IP:

- OSI ist allgemeingültig für alle Protokolle (man kann IBMs SNA mit OSI beschreiben), TCP/IP ist kein Modell
- TCP/IP unterscheidet nicht zwischen Schicht 1 und 2
- viele Protokolle wurden spontan für einen Anwendungsfall zusammengestrickt

Datenübertragungsdienste

DQDB (distributed queue dual bus – DATEX-M)

Aussterbender Standard bei MANs. Man hat je einen Bus pro Datenflussrichtung. Datenraten bis 45 Mbps. Wird langsam abgelöst durch...

Breitband-ISDN / ATM

B-ISDN ist ein Netzdienst, der parallel zum vorhandenen Telefonsystem aufgebaut wird. Auf B-ISDN können zukünftig das Telefonnetz, das Kabelfernsehen und die Datendienste basieren. B-ISDN basiert auf ATM (asynchronous transfer mode) und überträgt Daten mit 155 Mbps (demnächst im Gigabit-Bereich). Bei ATM kann man eine Bandbreite anmelden und hat die dann virtuell zur Verfügung. Man ist always-online.

80% der Backbones des ISP und das interne Netz der Telekom basieren auf ATM. Es laufen erste Versuche mit TV-Sendungen über MPEG-2.

X.25 (DATEX-P)

Alter Standard für öffentliche paketvermittelnde Dienste. Die Bitübertragungsschicht läuft über X.21 (digitale Datenübertragung). X.25 kennt Leitungsvermittlung wie SMDS, aber kann auch **permamente virtuelle Leitungen** aufbauen, die für den Kunden wie Standleitungen aussehen.

SMDS (switched multimegabit data service)

Verbindungsloser (!) Breitbanddienst (45 Mbps) der Telcos. Jede Niederlassung einer Firma hat ein LAN. Man kann über SMDS die LANs verbinden. Man muss keine Standleitung halten, sondern rechnet nach Datenvolumen ab.

Frame-Relay

Benutzt keine komplizierten Fehlerkorrekturen und braucht deshalb zuverlässige Übertragungsmedien. Arbeitet im Bereich 1,5 Mbps. Frame-Relay ist völlig ungesichert und braucht deshalb sichere Medien wie Glasfaser.

Bitübertragungsschicht

Physikalisches

Fourier-Analyse

Man kann ein analoges Signal mittels einer Fourier-Analyse in seine reinen Frequenzen zerlegen (demodulieren). Fourier sagt, dass jedes Signal durch eine Summe von Cosinus- und Sinusfunktionen dargestellt werden kann. (Ähnliches passiert auch beim menschlichen Ohr.) Man kann ein Signal so darstellen:

$$g(t)=\frac{1}{2}\cdot c+\sum_{n=1}^{\infty} a_n \cdot \sin(2\pi n f t)+\sum_{n=1}^{\infty} b_n \cdot \cos(2\pi n f t)$$

a_n und b_n sind die Amplituden für Sinus und Cosinus der n-ten „Harmonischen".

Baudrate: „Signalgeschwindigkeit" (wieviele Signale pro Sekunde)

Bitrate: „Datengeschwindigkeit" (wieviele Bits pro Sekunde)

Nyquist-Formel

Man kann ein Signal wieder samplen (abtasten), wenn die Samplefrequenz genau doppelt so hoch ist wie die Bandbreite der (rauschfreien!) Leitung.

Bandbreite: Differenz zwischen höchster und niedrigster Frequenz (80MHz-100MHz ist ein Bereich mit 20MHz Bandbreite).

$$\text{maximale Datenrate} = 2 \cdot \text{Bandbreite} \cdot \log_2 \text{Stufen} \quad \frac{\text{bit}}{\text{sec}}$$

Beispiel: Wenn man also binäre Signale (=2 Stufen) über eine Leitung mit 3kHz Bandbreite schickt, kann man maximal 6kps übertragen.

Übertragungsmedien

	Technologie	**Übertragungskapazität**	**Reichweite**	**Bemerkung**
Magnetbänder	Magnetbänder	hoch	beliebig	für Echtzeitbetrieb absurd
Twisted Pair	CAT 3 (verdrillte Kupferleitungen mit 1mm Durchmesser)	1-10 MBit	???	
Twisted Pair	CAT 5 (stärker verdrillte Kupferleitungen)	10-100 MBit	150m	
Koaxialkabel	dicker Kupferkern mit geflochtener Abschirmung	1Gbit	1km	
Lichtwellenleiter	Multimode-Glaskern mit reflektierender Hülle (mehrere Lichtstrahlen werden immer wieder in den Kern zurückgeworfen)	10GBit	30km	
Funkübertragung	Radiowellen			durchdringen Wände
	Mikrowellen			werden von Wänden blockiert
	Lichtwellen (Laserlink)			nur bei direkter Sichtlinie

Glasfaser ist weniger störanfällig. Elektronen stoßen sich ab und beeinflussen sich damit (thermisches Rauschen). Photonen überlagern sich einfach nur.

Bei Lichtwellenleitern gibt es aktive Verbinder (mit Fotodiode und Laser) und passive Verbinder (Glasfasern werden verschmolzen). Passive Verbinder verlieren mehr Licht, sind aber deutlich schneller.

Modems (Modulator/Demodulator): wandelt Digitalsignale in Analogsignale (für analoge Telefonleitungen)

Codec (Coder/Decoder): wandelt Analogsignale in Digitalsignale (für Sprachdaten auf digitalen Kanälen)

Dämpfung

Energieverlust auf einer Leitung (hängt von der Frequenz ab)

$$\text{Dämpfung} = 10 \cdot \log_{10} \frac{\text{übertragene Leistung}}{\text{empfangene Leistung}}$$

Modulation (analoges Kodieren digitaler Informationen):

- **Amplitudenmodulation** (Sinus=1, nichts=0)
- **Frequenzmodulation** (hohe Frequenz=1, niedrige Frequenz=0)
- **Phasenmodulation** (je nach Phasenwinkel eines Sinus hat man 0 oder 1)

Wenn man diese Modulationen kombiniert, erreicht man bei **Quadraturamplitudenmodulation** 4 Bit/Baud.

Mit **Kompression** (z.B. MNP5) erreicht man noch höhere Datenraten je nach Inhalt (Texte sehr gut, JPG kaum).

Multiplexen: Zusammenfassen von „schmalbandigen" Datenströmen zu einem „breitbandigen" (z.B. in der Fernvermittlung)

- **Frequenzmultiplexen**: mehrere sauber getrennte Frequenbänder werden zusammengefasst (Kupferkabel)
- Wellenlängenmultiplexen: wie Freqenzmultiplexen aber über Glasfaser (Prismen unterteilen die Frequenzbänder wieder)
- **Zeitmultiplexen**: auf jeder Zeitscheibe darf immer einer senden (geht nur digital)

Vermittlung:

- **Leitungsvermittlung** (veraltet)
  (dedizierte Kupferleitung)
- **Paketvermittlung**
  (Pakete werden als digitale Daten in einem festgelegten Format zum Ziel geroutet)

ISDN (integrated services digital network): digitaler Telefondienst (man kann direkt digitale Informationen ohne Modem übertragen)

Mit ISDN hat man beim Basisanschluss zwei B-Kanäle (64kBit) für Daten und einen D-Kanal (16Kbit) für Steuerinformationen.

Man kann auch Primärmultiplexanschlüsse mit 30 B-Kanälen (64Kbit) und einem D-Kanal (64Kbit) nehmen.

ISDN ist für den Internet-Bereich zunehmend weniger interessant (die Bandbreite ist auch bei Kanalbündelung zu gering). Da nimmt man lieber ADSL über Kupferleitungen oder ATM über Cat5 oder Glasfaser. Außerdem geht der Trend zu mobiler Kommunikation...

Mobilfunk / Zellfunk

Pager: unidirektionale Systeme für Numerik oder Alphanumerik (kein bestätigter Empfang)

GSM (global system for mobile communication) auf 900MHz und 1800MHz

Früher gab es nur analoge Funktelefone, die leicht abzuhören waren und schlechte Qualität hatten. Heute nutzt man digitale Funktelefone (GSM).

Geostationäre Satelliten sind 36.000km über dem Äquator und für einen Bezugspunkt auf der Erde fix. Man braucht also die Antenne nur einmal auszurichten. Die Satelliten senden im GHz-Bereich auf verschiedenen Frequenzen. Die Übertragungszeit ist 0,25 Sekunden. Für Mobilfunk gab es das legendäre Iridium. ;) Satelliten haben den Vorteil, dass man nur eine Schüssel installieren muss (die Kabelkanäle sind meistens schon voll). Allerdings muss das Wetter mitspielen.

Sicherungsschicht (2)

Die Sicherungsschicht zerhackt Datenströme in einzelne Rahmen und kümmert sich um deren gesicherte Übertragung (Prüfsumme). Außerdem gibt es eine Flusssteuerung, um den Empfänger nicht zu überfluten.

Es gibt hier drei Möglichkeiten:

1. unbestätigte verbindungslose Dienste
   Es wird keine Verbindung aufgebaut. Geht etwas verloren, müssen sich die höheren Schichten darum kümmern.
   Beispiel: UDP, Sprachdaten
2. bestätigte verbindungslose Dienste
   Es wird keine Verbindung aufgebaut. Der Empfänger bestätigt nur den Erhalt der Rahmen.
3. verbindungsorientierte Dienste
   Es wird eine von beiden seiten bestätigte Verbindung aufgebaut
   Beispiel: TCP mit 3-Way-Hanshaking

Rahmenerstellung

Es werden Rahmen aus dem Datenstrom erzeugt. Dabei ist die Begrenzung zwischen den Rahmen ein DLE-Zeichen (data link escape) und STX (start of text) oder ETX (end of text). Kommt tatsächlich ein DLE im Datenstrom vor, wird DLE-DLE gesendet. Das geht nur bei 8-Bit-Übertragungen.

Bit-Stuffing: jeder Rahmen beginnt mit 01111110. Soll wirklich 0111110 übertragen werden, wird 011111010 genommen (eine Null „reingestopft“).

Fehlerkorrektur

Der Sender verschickt jeden Rahmen mit einer Nummer und einer Prüfsumme. Außerdem lässt er sich den Empfang vom Empfänger quittieren. Bekommt der Sender während einer Timerzeit keine Bestätigung, sendet er das Paket noch einmal.

- Fehlererkennungcodes: es ist gerade mal soviel Redundanz in den Daten, dass man einen Übertragungsfehler erkennen kann
  - **CRC** (cyclic redundancy check):
    Jedem Rahmen wird eine Prüfsumme zugewiesen, die durch ein Polynom errechnet wird. Die Datenbits sind die Koeffizienten des Polynoms. Man muss sich vorher auf ein Polynom einigen. [...]
- Fehlerkorrekturcodes: es ist soviel Redundanz in den Daten, dass der Empfänger einen Übertragungsfehler selbst korrigieren kann (z.B. Hamming-Code)
  - **Hamming-Abstand**: Anzahl der Bits, in denen sich zwei Byte/Wörter unterscheiden. Mit einem Paritätsbit kann man einen 1-Bit-Fehler direkt korrigieren.
  - **Hamming-Code**: Codewörter (z.B. Bytes oder Wörter) die alle einen minimalen Hamming-Abstand haben. Dadurch kann man einzelne Bitfehler direkt korrigieren. Beispiel: 1-Bit-Fehler ist korrigierbar, 2-Bit-Fehler wird erkannt, 3-Bit-Fehler wird fehlinterpretiert. Um x Fehler beheben zu können, braucht man einen Hamming-Code mit Mindestabstand $2 \cdot x + 1$.

Flusssteuerung (flow control)

Damit ein langsamer Empfänger nicht überflutet wird, muss man die Sendegeschwindigkeit koordinieren (z.B. Stop-And-Wait, wenn der Empfänger „Halt“ schreit).

Simplex: nur Senden in jeweils eine Richtung möglich

Duplex: Senden gleichzeitig in beide Richtungen möglich

Schiebefensterprotokoll: es werden immer nur x Pakete gesendet bis eine Bestätigung erfolgen muss. Bei einem Fehler kann selektiv das defekte Paket neu geschickt werden.

HDLC (high-level data link control)

HDLC ist ein bitorientiertes Protokoll, das mit Bit-Stuffing arbeitet. Es arbeitet vollduplex. Um die Effizienz der Übertragung zu erhöhen, wartet HDLC nicht ständig auf die Erlaubnis, ein Paket senden zu dürfen. Es sendet eine bestimmte Anzahl an Paketen auf einmal los. Diese Anzahl ist das **Window**. Sie wird durch die Kapazität des Empfangspuffers begrenzt. Der Empfänger bestätigt auch immer diese Anzahl von Rahmen. Gibt es einen Übertragungsfehler, so werden alle Rahmen seit der letzten Bestätigung noch einmal gesendet. HDLC benutzt zwar den 8-Bit-Code 01111110 als Kennung für einen Rahmen, aber ist ansonsten codeunabhängig.

Sicherungsschicht im Internet

Point-to-Point-Verbindungen braucht man meistens zur Netzkopplung. Man hat in einem Gebäude ein LAN, das man mittels eines Netzkopplung mit dem Internet über einen ISP verbindet. Wenn man sich von zuhause ins Internet einwählt, benutzt man auch ein Point-to-Point-Protokoll.

SLIP (serial line IP): veraltetes Protokoll zur Verbindung einer Workstation mit dem Internet über ein Modem. SLIP hat keine Fehlererkennung und kann nur IP. Es gibt auch keinen Authentifizierung. Bitstuffing wie bei HDLC.

PPP (point to point protocol): weit verbreitetes Protokoll für Internet-Verbindungen. Es gibt eine Authentifizierung, einer Fehlerkontrolle und die Möglichkeit, auch andere Protokolle wie IPX oder AppleTalk zu routen. Dazu gibt es das **LCP** (link control protocol), mit dem Verbindungen auf und abgebaut werden und das festlegt, wieviele Bytes als Nutzdaten in jedem Paket übertragen werden. Bitstuffing wie bei HDLC.

MAC-Teilschicht

MAC = Medium Access Control

Hier geht es um Broadcast-Netze. Das gehört mit zur Sicherungsschicht.

Statische Kanalzuordnung

Es macht keinen Sinn, einen breitbandigen Kanal in feste kleinere Kanäle aufzuteilen. Überträgt ein Benutzer nichts, so ist die Kapazität für andere Anwender nicht nutzbar, die am Limit sind und seine Bandbreite gut gebrauchen könnten.

Dynamische Kanalzuordnung

- man hat variabel viele Computer
- alle Computer übertragen über einen gemeinsamen Kanal
- es kann zu Kollisionen kommen, wenn mehrere Computer gleichzeitig senden
- entweder jeder Computer kann zu jeder Zeit senden (es gibt keinen Takt) oder es gibt festgelegte Intervalle (Slots)
- entweder es gibt einen erkennbaren Träger (Carrier) oder man sendet einfach blind

ALOHA

Unkoordiniertes/chaotisches Senden. Überschneidungen irgendwo in einem Paket führen zum Verlust beider Pakete. Um den potentiellen Schaden in Grenzen zu halten, gibt es eine feste Paketgröße.

Reines ALOHA ist sehr ineffizient. Der Kanal kann zu höchstens 18% ausgelastet werden.

Unterteiltes ALOHA

Pakete dürfen immer nur in vorbestimmten (synchronisierten) Intervallen gesendet werden. Dadurch erhöht sich die maximal mögliche Auslastung auf immerhin 36%.

CSMA (carrier sense multiple access)

Ein Träger (Carrier) macht deutlich, ob der Kanal frei ist oder nicht. Die Sender hören diesen Carrier ab.

- 1-persisent CSMA:
  Sobald ein Kanal frei ist, sendet der Computer mit Wahrscheinlichkeit 1.
- p-persistent CSMA:
  Sobald ein Kanal frei ist, sendet der Computer mit Wahrscheinlichkeit p. Je kleiner die Wahrscheinlichkeit, um so höher ist der Durchsatz (und die „Höflichkeit“ der Sender, andere vorzulassen).
- Non-persistent CSMA:
  Sobald ein Kanal frei ist, wartet man noch eine zufällige Zeit und nutzt ihn dann erst (falls er dann noch frei ist). Das ist die „höfliche“ Variante.

CSMA/CD (carrier sense multiple access – collision detection)

Sobald ein Kanal frei ist (durch Träger erkannt), dann kann eine Station senden. Senden zwei Stationen gleichzeitig, dann erkennen sie die Kollision und brechen noch während der Übertragung ab.

Bei einer Kollision wartet eine Station eine zufällige Zeit und sendet wieder.

Reservierungsprotokolle

Es gibt eine Konkurrenzperiode, während der alle Sender anmelden, ob sie etwas senden möchten. Jeder Sender hat dazu einen „Konkurrenz“-Slot, wo er seinen Wunsch „eintragen kann“. Ist die Konkurrenzperiode vorbei, senden die Sender in der vereinbarten Reihenfolge. Danach beginnt eine neue Konkurrenzperiode.

Das klappt nur, wenn die Verzögerungszeit so gering ist, dass man bitweise in die Kommunikation eingreifen kann!

Man kann auch jedem Sender eine binäre Adresse zuordnen. Alle Stationen, die etwas senden möchten, schicken zeitgleich ihre Adressen an alle anderen. Erkennt eine Station eine 1, wo sie eine 0 gesendet hat, dann hat eine andere Station eine höhere Adresse und darf vorher senden. Dieser Algorithmus beseitigt zwar den Overhead der ersten Methode, ist nicht fair.

Adaptive Tree Walk Protocol

Wave Division Multiple Access

Protokolle für Funk-LANs

Es ist schwer herauszubekommen, ob man senden darf, weil vielleicht mein Partner noch in meinem Bereich ist, aber er sich mit jemandem unterhält, den ich aufgrund der Entfernung nicht mehr empfangen kann (**Hidden-Station-Problem**).

MACA (multiple access with collision avoidance)

Um das Hidden-Station-Problem zu umgehen, sendet der Sender erst ein RTS (request to send) an den Empfänger. Der bestätigt die Übertragung mit einem CTS (clear to send). Wenn eine dritte Station also RTS oder CTS hört, muss sie schweigen, bis die Übertragung beendet ist. Die Länge der Daten steht im RTS- und CTS-Paket drin. Das ganze ist sinnvoll, weil RTS und CTS nur ca. 30 Bytes lang sind.

Digitales Zellfunknetz

Beim drahtlosen LAN gibt es nur ein Protokoll. Beim Zellfunknetz gibt es mehrere Protokolle. Deshalb muss man etwas vorsichtiger sein.

GSM (global system for mobile communications)

GSM ist der europäische (und sich weltweit verbreitende) Standard für Mobilfunk. GSM arbeitet bei 900 MHz und 1800 MHz. Jede Zelle kann theoretisch knapp 1000 Verbindungen gleichzeitig managen (dank Frequenzmultiplexen und Zeitmultiplexen). Jeder Kanal kann etwa 9600 bps senden.

Mittlerweile setzen sich digitale Datendienste durch, denn die Minutenpreise sind hoch und 9600 bps sind nicht viel. Man arbeitet an HSCSD und UMTS.

IEEE 802.3 (Ethernet)

802.3 ist ein Protokoll zur Übertragung in einem LAN mittels 1-persistent CSMA/CD.

Ethernet ist die Weiterentwicklung. 802.3 ist der Original-Standard auf einem 50-Ohm-Koaxialkabel mit 10 Mbps.

Typische Kabeltypen sind:

- 10Base5 (Thicknet) – Vampirabzweige
- 10Base2 (Thinnet/Cheapnet) – T-stücke
- 10BaseT (Twisted Pair) – direkte Verbindung mit Hubs/Switches
- 10BaseF (Glasfaser)

Manchester-Code

Am besten überträgt man eine Schwingung auf dem Ethernet. So kann man schnell unterscheiden, ob man bei 0 Volt lauter Null-Bits empfängt oder aber gar keine Verbindung hat. Deshalb ist 1 z.B. High/Low und 0 ist Low/High. Und man nicht nicht 0V und 5V, sondern -0,85V und +0,85V.

Token-Bus, Token-Ring, DQDB

Bridge

Verbindungselement auf der Sicherungsschicht. Mann kann z.B. über ISDN auch IPX bridgen.

LANs mit hohen Bitraten

FDDI (fiber distributed data interface)

FDDI ist ein Token-Ring-LAN über Multimode-Lichtwellenleiter (mit LEDs als Sendern aus Sicherheitsgründen für neugierige Anwender), mit dem man 100MBit über bis zu 200km übertragen kann.

Man benutzt zwei Ringe. Auf einem überträgt man linksherum – im anderen rechtsherum. Brechen beide Ringe an einer Stelle (wegen Brand o.ä.), dann kann man immer noch den restlichen Ring nutzen.

FDDI nutzt man heutzutage höchstens noch im Backbone-Bereich.

Fast-Ethernet

Fast-Ethernet läuft mit 100 MBit und man kann es über 100BaseTX (Twisted Pair – Vollduplex) oder 100BaseF (Glasfaser) nutzen. Ansonsten ist es identisch mit normalem 802.3-Ethernet.

Satellitennetze

Vermittlungsschicht

Die Vermittlungsschicht soll Pakete von einer Quelle zu einem Ziel bringen und arbeitet Ende-zu-Ende-mäßig.

Im Internet ist die Vermittlungsschicht (IP) verbindungslos.

Virtuelle Verbindung: zwischen zwei Computern wird eine Route ausgehandelt und benutzt (logische Verbindungsnummer)

Datagramm: Datenpaket, das ohne expliziten Verbindungsaufbau übertragen werden kann

Routing-Algorithmen

Statisches Routing

Es gibt eine feste Routing-Tabelle, die der Admin festgelegt hat.

Dynamisches Routing

Shortest Path: es wird der kürzeste Pfad im Netz zum Zielsystem ermittelt (gewichteter Graph). Die Gewichtung können Leitungskosten, die geografische Entfernung,die Bandbreite oder die Leitungsverzögerung sein.

Flooding: es wird über alle Kanäle ein Paket mit einer eindeutigen Nummer geschickt. Es kommt immer das schnellste zuerst an.

Flussbasiertes Routing, ...

Hierarchisches Routing

Mobiles Routing

Hierarchisches Routing benutzt man vor allem für mobile Computer benutzt. Ein mobiler Computer hat eine Heimat-Adresse und eine mobile Adresse. Wird er gesucht, so wird im ersten Schritt nach seiner festen Heimat-Adresse gesucht. Dort kann man dann abfragen, wo sich der Computer zuletzt eingebucht hat.

Entweder routet man erst zur Heimat-Adresse und dann weiter. Oder es wird die Zieladresse an der Heimat-Adresse abgefragt und direkt geroutet.

Broadcast

Man kann auch weiter als im lokalen Teilnetz Broadcast-Pakete versenden. Dann benutzt man Spanning-Tree.

Multicast

Pakete werden gezielt an mehrere Systeme gleichzeitig gesendet.

Überlastungsüberwachung

Verbundnetze

Repeater: verstärkt ein Signal über größere Strecken (physikalisch)

Bridge: speichert ein Datenpaket, überprüft es und leitet es weiter

Router: ein Datenpaket wird über ein anderes Medium oder Netz geschickte (z.B. ISDN-IP-Router)

Tunneling: man verschickt ein Datenpaket über ein anderes Protokoll oder Netz (IPX-Tunneln über IP oder HTTP über DNS)

Paketfilter/Firewall: filtert den Datenverkehr

Vermittlungsschicht im Internet

IP = internet protocol

IP-Adresse = 4 Bytes

Class A, B, C... (gähn)

Netzmaske für Teilnetze... (obergähn)

ARP: (address resolution protocol) Die Hardware auf der Sicherungsschickt kennt nur Hardware-Adressen (bei Ethernet: MAC). ARP setzt IP-Adressen lokal auf Hardware-Adressen um.

RIP: Protokoll, dass Routern untereinander mitteilt, wer wohin routen kann

OSPF: (open shortest path first) besseres Protokoll als RIP (schneller bei Ausfällen, kann Subnetze)

BGP: (border gateway protocol) wie OSPF, aber man kann das Routing genauer festlegen