

8.Vorlesung Grundlagen der Informatik

Dr. Christian Baun

Hochschule Darmstadt
Fachbereich Informatik
christian.baun@h-da.de

1.12.2011

Wiederholung vom letzten Mal

- Klassifikationen von Betriebssystemen
 - Betriebsarten (Stapelbetrieb, Dialogbetrieb)
 - Singletasking und Multitasking
 - Einzelbenutzerbetrieb und Mehrbenutzerbetrieb
 - Ein-Prozessor- und Mehr-Prozessor-Betriebssysteme
 - Echtzeitbetriebssysteme
- Prozesskontext
 - Benutzerkontext
 - Hardwarekontext
 - Systemkontext
- Prozessmodelle
- Prozesstabellen und Prozesskontrollblöcke
- Zustandslisten

Heute

- Grundlagen der Computervernetzung
 - Netzwerkdienste und Rollen
 - Übertragungsmedien
 - Einteilung der Netzwerke
 - Formen der Datenübertragung
 - Richtungsabhängigkeit der Datenübertragung
 - Topologien von Computernetzwerken
 - Frequenz
 - Datensignal
 - Fourierreihe
 - Bandbreite
 - Zugriffsverfahren
- Kommunikation in Netzwerken
 - Protokolle und Protokollschichten
 - TCP/IP-Referenzmodell
 - Hybrides Referenzmodell
 - OSI-Referenzmodell

Zwingend nötige Elemente für Computernetzwerke

- Für den Aufbau und Betrieb eines Computernetzwerks sind mindestens 3 Elemente nötig:
 - 1 **Mindestens 2 Rechner mit Netzwerkdiensten**
 - Die Rechner wollen miteinander kommunizieren oder gemeinsam eine Ressource nutzen
 - Der Netzwerkdienst stellt einen Dienst (Service) bereit, um zu kommunizieren oder gemeinsame Ressourcen zu nutzen
 - 2 **Übertragungsmedium**
 - Dient dem Austausch von Daten
 - 3 **Netzwerkprotokolle**
 - Regeln, die festlegen, wie Rechner miteinander kommunizieren können

Die Regeln (Netzwerkprotokolle) sind zwingend nötig. Ansonsten können sich die Kommunikationspartner *nicht verstehen*. Man stelle sich einen Telefonanruf ins Ausland vor. Die Verbindung kommt zustande, aber kein Teilnehmer versteht die Sprache des anderen. Nur wenn beide Kommunikationspartner die gleiche Sprache sprechen, kommt eine Kommunikation zustande.

- Dr. Christian Baun – 8.Vorlesung Grundlagen der Informatik – Hochschule Darmstadt – WS11/12 5/52

Übertragungsmedien

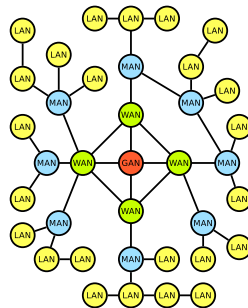
- Es existieren verschiedene Übertragungsmedien, um Computernetzwerke aufzubauen
 - ① **Leitungsgebundene Übertragungsmedien**
 - **Elektrischer Leiter:** Daten werden über Twisted-Pair-Kabel (verdrehte Kabel) oder Koaxialkabel in Form elektrischer Impulse übertragen
 - **Lichtwellenleiter:** Daten werden als Lichtimpulse übertragen
 - ② **Nicht-leitungsgebundene Übertragung** (Drahtlose Übertragung)
 - **Funktechnik:** Daten werden in Form elektromagnetischer Wellen im Radiofrequenzbereich (Radiowellen) übertragen
 - **Infrarot:** Daten werden in Form elektromagnetischer Wellen im Spektralbereich übertragen

Netzwerkprotokolle

- In Netzwerkprotokollen sind die Regeln festgelegt, die die Kommunikation (also den Informationsaustausch) zwischen den Kommunikationspartnern ermöglichen
⇒ **Protokollschichten** und **Referenzmodelle**

Einteilung der Netzwerke nach räumlicher Ausdehnung

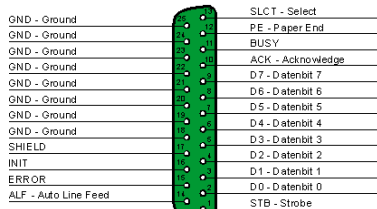
- ❶ **Local Area Network (LAN)** – 10 bis 1.000 m
 - Erstreckt sich über eine Wohnung, ein Gebäude oder ein Firmengelände
 - Technologien: Ethernet, WLAN, Token Ring (früher)
- ❷ **Metropolitan Area Network (MAN)** – 10 km
 - Erstreckt sich über das Gebiet einer Stadt oder eine Ballungsgebiet
 - Technologien: Lichtwellenleiter (Glasfaser), WiMAX (IEEE 802.16)
- ❸ **Wide Area Network (WAN)** – 100 bis 1.000 km
 - Verbindet mehrere Netzwerke über einen großen geografischen Bereich
 - Technologien: Ethernet (10 Gbit/s) Asynchronous Transfer Mode (ATM)
- ❹ **Global Area Network (GAN)** – 10.000 km
 - Kann über unbegrenzte geographische Entfernungen mehrere WANs verbinden
 - Häufig Satelliten- oder Glasfaserübertragung
 - Das Internet ist ein GAN



Parallele Datenübertragung

- Kommunikation zwischen Rechnern ist mit **paralleler** und **serieller** Datenübertragung möglich
- Neben den Steuerleitungen ist bei **paralleler Datenübertragung** für jedes Datenbit eine eigene Datenleitung vorhanden
- Beispiel für parallele Datenübertragung: Parallele Schnittstelle zum klassischen Anschluss von Druckern
 - Über diese parallele Schnittstelle kann pro Zeiteinheit ein komplettes Byte an Daten übertragen werden
- Vorteil: Hohe Geschwindigkeit
- Nachteil: Es sind viele Leitungen nötig
 - Das ist bei großen Distanzen kostenintensiv und aufwändig
- Anwendung: Lokale Bus-Systeme

Das Bild zeigt die parallele Schnittstelle (25-polig)

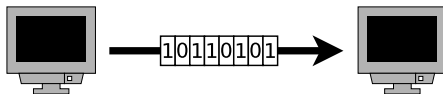


SUB-D 25-polig weiblich
Ansicht auf Buchsen Seite

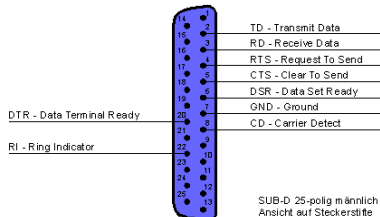
Bildquelle: <http://www.elektron-bbs.de>

Serielle Datenübertragung

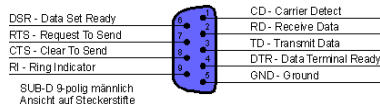
- Bei **serieller Datenübertragung** werden die Bits auf einer Datenleitung nacheinander übertragen
- Für den Transfer eines Bytes sind 8 Zeiteinheiten nötig
- Vorteil: Auch für große Distanzen geeignet, da nur wenige Leitungen nötig sind
- Nachteil: Geringerer Datendurchsatz
- Anwendung: Lokale Bus-Systeme und **Netzwerkverbindungen**



Das Bild zeigt die serielle Schnittstelle (25-polig)



Das Bild zeigt die serielle Schnittstelle (9-polig)



Bildquelle: <http://www.elektron-bbs.de>

Synchrone und asynchrone Datenübertragung (1/2)

- Um Daten aus einem Bitstrom auszulesen, muss der eingehende Datenstrom über ein **Zeitfenster** abgetastet werden
 - Das Zeitfenster wird über eine **Taktquelle** gewonnen
- **Synchrone Datenübertragung**
 - Die Kommunikationspartner synchronisieren die Übertragung zeitlich mit einem Taktsignal
 - Das Taktsignal kann über eine eigene Schnittstellenleitung gesendet werden oder wird vom Empfänger aus dem Datensignal zurückgewonnen
 - Diesen Vorgang nennt man **Taktrückgewinnung**
- Vorteil:
 - Die Daten müssen nicht regelmäßig neu synchronisiert werden
- Nachteil:
 - Aufwändige Realisierung

Synchrone und asynchrone Datenübertragung (2/2)

● Asynchrone Datenübertragung

- Die Kommunikationspartner verwenden voneinander unabhängige Taktquellen
- Werden Daten übertragen, wird vor die Daten ein Startbit gesetzt
 - Dieses Startbit signalisiert dem Empfänger, dass er seine Taktquelle starten soll
 - Am Ende der Daten folgt ein Stopbit, mit dem die Datenübertragung beendet wird
- Vorteil:
 - Es ist keine Synchronisation der Taktquellen nötig
- Nachteile:
 - Weil die Taktquellen voneinander abweichen können, ist die maximale Größe der übertragbaren Daten relativ klein
 - Startbit und Stopbit stellen einen Overhead dar

Datenübertragung im Netzwerkbereich

- Im Netzwerkbereich gibt der Sender den Takt vor und liefert ihn immer mit dem Datenstrom
 - Darum findet über Computernetzwerke prinzipiell immer **synchrone Datenübertragung** statt
- Man kann aber dennoch Computernetzwerke in synchron und asynchrone unterscheiden
 - **Synchronen Computernetzwerke:** Die Verbindung zwischen den Kommunikationspartnern bleibt bestehen und damit ist die Verbindung dauerhaft synchronisiert
 - **Asynchronen Computernetzwerken:** Zwischen den Phasen des Datentransfers besteht keine Verbindung
 - Die Kommunikationspartner müssen sich beim Verbindungsaufbau immer wieder neu synchronisieren

Richtungsabhängigkeit der Datenübertragung

• Simplex

- Der Informationstransfer funktioniert nur in einer Richtung
- Nach dem Ende der Übertragung kann der Kommunikationskanal von einem anderen Sender verwendet werden
- Beispiel: Pager, Radio, Fernsehen

• Duplex (Vollduplex)

- Der Informationstransfer funktioniert in beide Richtungen gleichzeitig
- Beispiel: Netzwerke mit Twisted-Pair-Kabel (hier gibt es separate Leitungen für Senden und Empfangen)

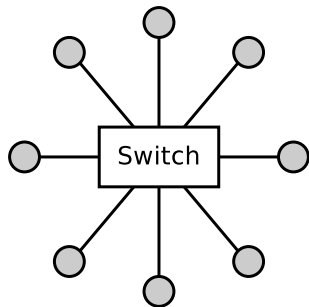
• Wechselbetrieb (Halbduplex)

- Der Informationstransfer funktioniert in beide Richtungen, aber nicht gleichzeitig
- Beispiel: Glasfaserkabel, Netzwerke mit Koaxialkabel (hier gibt es nur eine Leitung für Senden und Empfangen)

Topologien von Computernetzwerken

- Es existieren unterschiedliche Topologien von Computernetzwerken
- Die Topologie legt fest, wie die Kommunikationspartner miteinander verbunden sind
- Unterschieden werden:
 - **Physische Topologie:** beschreibt den Aufbau der Netzverkabelung
 - **Logische Topologie:** beschreibt den Datenfluss zwischen den Endgeräten
 - Die logische Topologie beschreibt, in welcher logischen Beziehung die Rechner beim Datenaustausch zueinander stehen
- Die physische und die logische Topologie können sich unterscheiden
- Topologien werden grafisch mit Knoten und Kanten dargestellt
- Die Struktur großer Netze ist oftmals aus mehreren unterschiedlichen Topologien zusammensetzt
- Die Topologie ist entscheidend für seine Ausfallsicherheit

Stern-Topologie

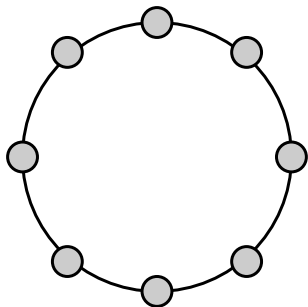


- Alle Knoten sind direkt an einer zentralen Komponente (Hub oder Switch) angeschlossen
- Ausfall der zentralen Komponente führt zum Ausfall des kompletten Netzes
 - Die zentrale Komponente kann redundant ausgelegt werden
- Leicht verständlich und erweiterbar
- Ausfall eines Knotens führt nicht zum Ausfall des Netzes

- Beispiele:

- Fast Ethernet: 10 Mbit/s, 100 Mbit/s, 1 Gbit/s, 10 Gbit/s
- Token Ring (physisch): 4-16 Mbit/s
- Fibre Channel (Speichernetzwerke): 2-16 Gbit/s
- InfiniBand (Cluster): 10-40 Gbit/s

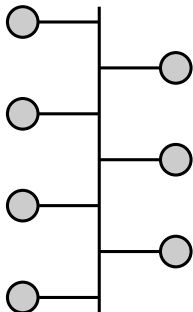
Ring-Topologie



- Jeweils 2 Knoten sind direkt miteinander verbunden
- Die zu übertragende Information wird von Knoten zu Knoten weitergeleitet, bis sie ihren Bestimmungsort erreicht
- Fällt ein Knoten aus, fällt der komplette Ring aus

- Jeder Teilnehmer ist gleichzeitig ein Signalverstärker (Repeater)
 - Große Ringlängen (abhängig vom Medium) sind möglich
 - Maximale Ringlänge bei Token Ring 800 m
- Beispiele:
 - Token Ring (logisch): 4-16 Mbit/s
 - Fiber Distributed Data Interface (FDDI): 100-1000 Mbit/s

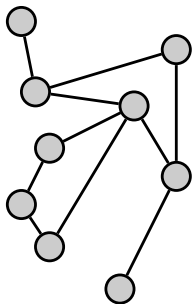
Bus-Topologie



- Alle Knoten sind mit demselben Übertragungsmedium (dem Bus) verbunden
- Keine aktiven Komponenten zwischen Knoten und Medium
- Ausfall einzelner Knoten führt nicht zum Ausfall des Netzes
- Geringe Kosten für Aufbau
 - Switches waren mal teuer!
- Störung des Übertragungsmediums blockiert den gesamten Bus
- Zu jedem Zeitpunkt kann nur eine Station Daten senden. Ansonsten kommt es zu Kollisionen
- Beispiele:
 - 10BASE2 (Thin Ethernet): 10 Mbit/s

Maschen-Topologie

- In einem vermaschten Netzwerk ist jeder Teilnehmer mit einem oder mehreren anderen Teilnehmern verbunden
- Ist jeder Teilnehmer mit jedem anderen Teilnehmer verbunden, spricht man von einem **vollständig vermaschten Netz**
- Fällt ein Teilnehmer oder eine Verbindung aus, ist die Kommunikation durch Umleiten (Routing) der Daten im Regelfall weiter möglich



- Vorteile:
 - Ausfallsicher (abhängig vom Verkabelungsaufwand)
- Nachteile:
 - Hoher Verkabelungsaufwand und Energieverbrauch
 - Komplexes Routing für nicht vollständig vermaschte Netze nötig
- Beispiele:
 - Logische Topologie zwischen Routern
 - Ad-hoc-(Funk-)Netze

Baum-Topologie

- Von einer Wurzel gehen eine oder mehrere Kanten aus
 - Jede Kante führt zu einem Blattknoten oder zu Wurzeln weiterer Bäume
- Mehrere Netze der Sterntopologie sind hierarchisch verbunden
- Vorteile:
 - Ausfall eines Endgeräts hat keine Konsequenzen
 - Gute Erweiterbarkeit und große Entfernungen realisierbar
 - Gute Eignung für Such- und Sortieralgorithmen
- Nachteile:
 - Beim Ausfall einer Wurzel ist der komplette davon ausgehende (Unter)Baum nicht mehr erreichbar
 - Bei großen Bäumen können die Wurzeln zu Engpässen werden, da die Kommunikation von der einen unteren Baumhälfte in die andere Hälfte immer über die Wurzel gehen muss



- Beispiel:
 - Verbindungen zwischen den Verteilern (Hub, Switch) werden mittels eines Uplinks hergestellt

Zellen-Topologie

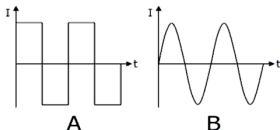
- Kommt hauptsächlich bei drahtlosen Netzen zum Einsatz
- **Zelle:** Bereich (Reichweite) um eine Basisstation (z.B. WLAN Access Point), in dem eine Kommunikation zwischen den Endgeräten und der Basisstation möglich ist
- Vorteile:
 - Keine Störung durch Ausfall von Teilnehmern möglich
- Nachteile:
 - Störanfällig abhängig von der Qualität der Basisstation(en))
 - Begrenzte Reichweite der Basisstationen (abhängig von deren Anzahl)
- Beispiele:
 - Wireless LAN (IEEE 802.11)
 - Global System for Mobile Communications (GSM)
 - Bluetooth-Hotspots als Funkzellen

Heutiger Stand

- Heute ist Ethernet (1-10 Gbit/s) mit Switches und damit die Stern-Topologie der Standard für Netzwerkverbindungen im LAN-Bereich
- Miteinander verbundene Verteiler realisieren eine Baum-Topologie, wenn es keine Schleifen in der Verkabelung gibt
- Die Zell-Topologie ist bei Funknetzen Standard
- Die Maschen-Topologie ist ein möglicher Anwendungsfall von Funknetzen und die logische Topologie zwischen Routern
- Bus- und Ring-Topologien spielen keine bedeutende Rolle mehr
 - Im Mai 2004 hat IBM seine Token-Ring-Produktpalette abgegeben

Frequenz

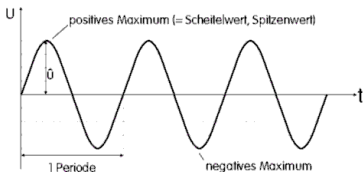
- Die Elektrotechnik unterscheidet 2 Spannungsarten:
 - Gleichspannung:** Höhe und Polarität der Spannung sind immer gleich
 - Wechselspannung:** Höhe und Polarität ändern sich periodisch



Bildquelle: <http://www.dj4uf.de>

- Abb. A: *Rechteckförmiger* theoretischer Wechselstrom
- Abb. B: *Sinusförmiger* Wechselstrom in der Praxis

- Periodendauer:** Zeit, die der periodische Spannungsverlauf benötigt
- Frequenz:** Anzahl der Schwingungen pro Sekunde
- Je niedriger die Periodendauer, desto höher ist die Frequenz



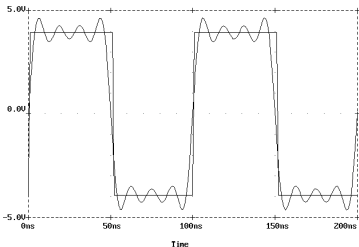
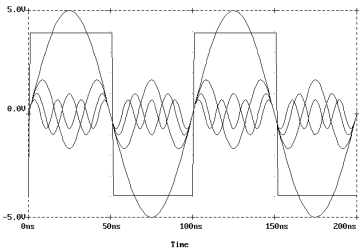
$$\text{Frequenz} = \frac{1}{\text{Periodendauer}}$$

- Frequenzen gibt man in der Einheit Hertz (Hz) an
- 1 Hertz = 1 Schwingung pro Sekunde
- Beispiel: Wechselspannungsversorgung mit 50 Hz

Datensignal

- Datenaustausch erfolgt durch den Austausch binärer Daten
 - Obwohl auf ein Netzkabel ein digitales Signal gegeben wird, handelt es sich um ein analoges Signal
- Signale unterliegen physikalischen Gesetzmäßigkeiten (z.B. Dämpfung)
 - Die **Dämpfung** schwächt die Höhe eines Signals ab
 - Unterschreitet die Höhe eines Datensignals einen bestimmten Wert, kann es nicht mehr eindeutig erkannt werden
 - Je höher die Frequenz, desto höher die Dämpfung
 - Die Dämpfung begrenzt die maximal überbrückbare Distanz

Fourierreihe

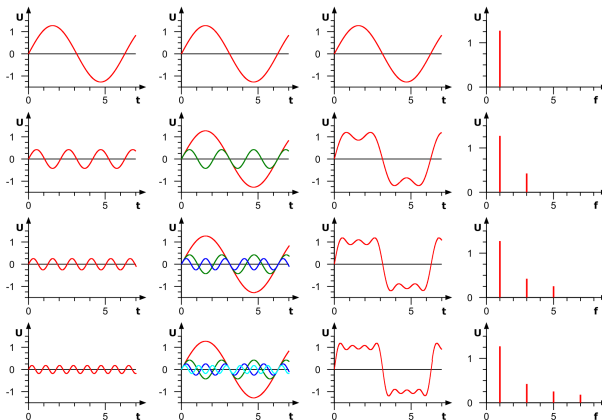


- Laut der **Fourierreihe** nach Jean Baptiste Joseph Fourier setzt sich ein Rechtecksignal – also auch ein Binärsignal – aus einer Überlagerung von harmonischen Schwingungen zusammen
 - Ein Rechtecksignal besteht aus einer **Grundfrequenz** und aus Oberwellen
 - Diese **Oberwellen** sind ganzzahlige Vielfache der Grundfrequenz und nennt man **Harmonische**
 - Man spricht von Oberwellen der 3., 5., 7., usw. Ordnung
 - Je mehr Harmonische berücksichtigt werden, umso näher kommt man einem idealen Rechtecksignal

Fourierreihe und Bandbreite

- Die Fourierreihe gibt Auskunft über folgende für die Netzwerktechnik wichtige Punkte
 - **Verformung des Datensignals**
 - **Nötige Bandbreite des Übertragungsmediums**
- Um ein Rechtecksignal eindeutig zu übertragen, müssen mindestens die Grundfrequenz und die 3. und 5. Oberwelle übertragen werden
 - Die 3. und 5. Oberwelle sind nötig, damit das Rechtecksignal noch seine rechteckige Form behält und nicht abgerundet aussieht
- Das Übertragungsmedium muss also nicht nur die Grundfrequenz, sondern auch die 3. und 5. Oberwelle – also die 3- und 5-fache Frequenz – fehlerfrei übertragen
 - In der Praxis werden die Oberwellen immer stärker gedämpft als die Grundfrequenz
- Die **Bandbreite** ist der Bereich von Frequenzen, der über ein Übertragungsmedium ohne Beeinflussung übertragen werden kann
 - Die Dämpfung des Datensignals steigt mit der Frequenz

Fourier-Synthese einer Rechteckschwingung



Quelle: Wikipedia

- Die Diagramme der ersten Spalte zeigen diejenige Schwingung, die in der jeweiligen Zeile hinzugefügt wird. Die Diagramme in der zweiten Spalte zeigen alle bisher berücksichtigten Schwingungen, die dann in den Diagrammen der dritten Spalte addiert werden, um dem zu erzeugenden Signal möglichst nahe zu kommen. Je mehr Harmonische (Vielfache der Grundfrequenz) berücksichtigt werden, umso näher kommt man einem idealen Rechtecksignal. Die vierte Spalte zeigt das Amplitudenspektrum normiert auf die Grundschiwingung.

Zugriffsverfahren

- In Netzwerken greifen alle Teilnehmer auf ein Übertragungsmedium gemeinsam zu
 - Man spricht in diesem Zusammenhang auch von *Shared Media*
- Es muss über ein **Zugriffsverfahren** sichergestellt sein, dass innerhalb eines Zeitraums immer nur ein Teilnehmer Daten sendet
 - Nur dann können die Daten fehlerfrei übertragen werden
- Bei Shared Media unterscheidet man zwischen 2 Zugriffsverfahren
 - ① **Deterministisches Zugriffsverfahren**
 - ② **Nicht-deterministisches Zugriffsverfahren**

Deterministisches Zugriffsverfahren

- Konventionen regeln den Zugriff auf das gemeinsam genutzte Medium
 - Der Zugriff erfolgt zu einem bestimmten Zeitpunkt in Übereinstimmung mit den anderen Teilnehmern
- Beispiel: **Token-Passing-Verfahren** bei Token Ring und FDDI
 - Das Senderecht wird über ein Token realisiert
 - Der Teilnehmer, der das Token hat, ist berechtigt, Daten zu versenden
 - Ist ein Teilnehmer mit dem Senden fertig, gibt er das Senderecht an einen anderen Teilnehmer weiter
 - Dieser Teilnehmer darf durch den Erhalt des Senderechts ebenfalls über einen bestimmten Zeitraum Daten senden
 - Macht der Teilnehmer von seinem Senderecht keinen Gebrauch, gibt er das Senderecht direkt an einen anderen Teilnehmer weiter
 - Die Sendezeit für jeden Teilnehmer ist nach dem Erhalt des Token beschränkt und jeder Teilnehmer erhält irgendwann das Token
 - Darum ist das Token-Passing-Verfahren ein **faies Zugriffsverfahren**
 - Kein Teilnehmer wird bei der Weitergabe des Token übergangen
 - Es ist garantiert, dass jeder Teilnehmer nach einer bestimmten **Wartezeit**, deren **maximale Dauer vorhersehbar** ist, Daten senden darf

Nicht-deterministisches Zugriffsverfahren

- Alle Teilnehmer stehen (bzgl. Medienzugriff) in direktem Wettbewerb
- Die **Wartezeit** des Zugriffs auf das Übertragungsmedium und die **Datenmenge**, die nach einem bestimmten Zeitpunkt übertragen werden kann, sind **nicht vorhersagbar**
 - Dauer der Wartezeit und Datenmenge hängen von der Anzahl der Teilnehmer und der Datenmenge ab, die die einzelnen Teilnehmer versenden
- Beispiel: Carrier Sense Multiple Access Collision Detection (CSMA/CD) bei Ethernet (mit Koaxialkabeln)
 - Will ein Teilnehmer senden, prüft er ob das Medium frei ist
 - Ist es frei, kann der Teilnehmer senden
 - Wollen 2 oder mehr Teilnehmer zur selben Zeit senden, gehen die Teilnehmer von einem freien Medium aus und es kommt zu einer **Kollision**
 - Durch das Kollisionserkennungsverfahren werden Kollisionen erkannt, worauf die sendenden Teilnehmer das Senden abbrechen
 - Die Teilnehmer versuchen (nach einer Wartezeit) erneut zu Senden
 - Die Wartezeit ermittelt jeder Teilnehmer nach dem Zufallsprinzip um eine erneute Kollision zu vermeiden

Protokolle

- Ein **Protokoll** ist die Menge aller vorab getroffenen **Vereinbarungen** zwischen Kommunikationspartnern
- Zu den Vereinbarungen gehören:
 - Welche Station sendet an wen und aus welchem Anlass?
 - Was ist die maximale Länge einer Nachricht?
 - Was geschieht bei Fehlern?
 - Wie erkennt man das letzte Bit einer Nachricht?
 - Wie erkennt man, dass eine Nachricht verloren wurde?
 - Wie kann man eine verlorene Nachricht erneut anfordern?
- Protokolle definieren...
 - **Syntax**: Das Format gültiger Nachrichten
 - **Grammatik**: Genaue Abfolge der Nachrichten
 - **Semantik**: Vokabular gültiger Nachrichten und deren Bedeutung

Protokollschichten

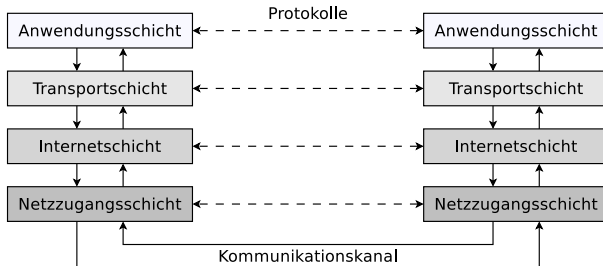
- 2 **Schichtenmodelle** als Designgrundlage von Kommunikationsprotokollen in Rechnernetzen:
 - ① **TCP/IP-Modell** bzw. **DoD-Schichtenmodell**
 - ② **OSI-Referenzmodell**
- Zusätzlich behandeln wir das **Hybride Referenzmodell**
 - Eine Erweiterung des TCP/IP-Modells von Andrew S. Tanenbaum
- Für alle Schichtenmodelle gilt:
 - Jede **Schicht** (*Layer*) behandelt einen bestimmten Aspekt der Kommunikation
 - Jede Schicht bietet eine **Schnittstelle** zur darüberliegenden Schicht
 - Jede Schnittstelle besteht aus einer Menge von **Operationen**, die zusammen einen **Dienst** definieren
- In den Schichten werden die Daten gekapselt (\implies **Datenkapselung**)

TCP/IP-Referenzmodell bzw. DoD-Schichtenmodell

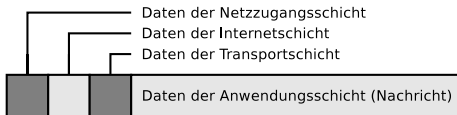
- Wurde ab 1970 vom Department of Defense (DoD) entwickelt
- Die Aufgaben der Kommunikation wurden in 4 aufeinander aufbauende Schichten unterteilt
- Nach dem DoD-Referenzmodell wurde das Internet aufgebaut
 - Ziel: Ein militärisches Netz, das durch eine dezentrale Struktur vor Ausfällen geschützt sein sollte
- Für jede Schicht ist festgelegt, was sie zu leisten hat
- Diese Anforderungen müssen Kommunikationsprotokolle realisieren
 - Die konkrete Umsetzung wird nicht vorgegeben und kann sehr unterschiedlich sein
 - Daher existieren für jede der 4 Schichten zahlreiche Protokolle

Nummer	Schicht	Beispiele
4	Anwendung	HTTP, FTP, SMTP, POP , DNS, SSH, Telnet
3	Transport	TCP, UDP
2	Internet	IP (IPv4, IPv6), ICMP, IPsec
1	Netzzugang	Ethernet, ATM, FDDI, PPP, Token Ring

TCP/IP-Referenzmodell – Paketaufbau



- Jede Ebene des TCP/IP-Referenzmodells fügt einer Nachricht zusätzliche Informationen als Header hinzu
- Diese werden beim Empfänger auf der gleichen Ebene ausgewertet



Schichten des TCP/IP-Referenzmodells (1/4)

- **Netzzugangsschicht**
- Physischer Anschluss
- Umsetzung der Daten in Signale
- Platzhalter für verschiedene Techniken zur Datenübertragung von Punkt zu Punkt Datenübertragung über verschiedene...
 - Übertragungsmedien (Kupferkabel, WLAN, Lichtwellenleiter,...),
 - Leitungscode (RZ-Code, NRZ-Code,...) und
 - Zugriffsprotokolle (Ethernet, Token Ring, FDDI,...)
- Die physischen Adresse (MAC-Adresse) legt den Empfänger fest
- Zerlegung des Bitstroms in **Rahmen** (engl. Frames)
- Sicherung des Datentransfers durch Fehlererkennung und -behebung



Schichten des TCP/IP-Referenzmodells (2/4)

- **Internetschicht**
- Aufgabe: Weitervermittlung von **Paketen** und Wegewahl (Routing)
 - Für empfangene Pakete wird hier das nächste Zwischenziel ermittelt und die Pakete dorthin weitergeleitet
 - Kern ist das Internet Protocol (IP) Version 4 oder 6, das einen Paketauslieferungsdienst bereitstellt
- Netzwerkweite Adressierung ist hier notwendig
- Jedes Netzwerkgerät erhält eine (logische) Netzwerkadresse
 - Logische Netzwerkadressen dienen der Verwaltung von Netzwerken



Schichten des TCP/IP-Referenzmodells (3/4)

- **Transportschicht**
- Ermöglicht den Transport von Daten (**Segmenten**) zwischen Prozessen auf unterschiedlichen Geräten über sog. Ende-zu-Ende-Protokolle
- Es existieren 2 Ansätze der Informationsübertragung
 - Verbindungslose Übertragung (UDP)
 - Es gibt keine Kontrolle, das ein Paket ankommt
 - Die Kontrolle muss in der Anwendungsschicht erfolgen
 - Verbindungsorientierte Übertragung (TCP)
 - Vor der Übertragung wird eine logische Verbindung aufgebaut und aufrechterhalten (auch wenn keine Daten übertragen werden)
 - Ermöglicht eine Kontrolle der Paketreihenfolge und des Datenflusses



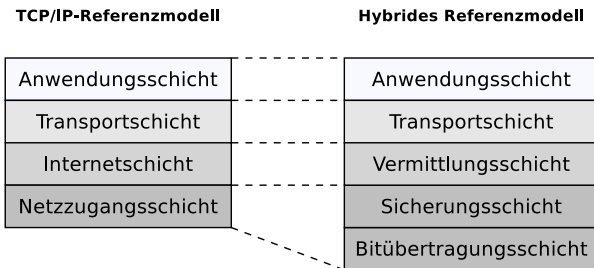
Schichten des TCP/IP-Referenzmodells (4/4)

- **Anwendungsschicht**
- Macht den Benutzern Dienste verfügbar
- Enthält alle Protokolle, die mit Anwendungsprogrammen zusammenarbeiten und das Netzwerk für den Austausch anwendungsspezifischer Daten nutzen
 - Beispiele: HTTP, FTP, Telnet, SMTP, DNS, ...



Hybrides Referenzmodell

- Gelegentlich wird das TCP/IP-Referenzmodell als fünfschichtiges Modell dargestellt
- Dieses Modell nennt man hybrides Referenzmodell



Ein Grund für das hybride Referenzmodell

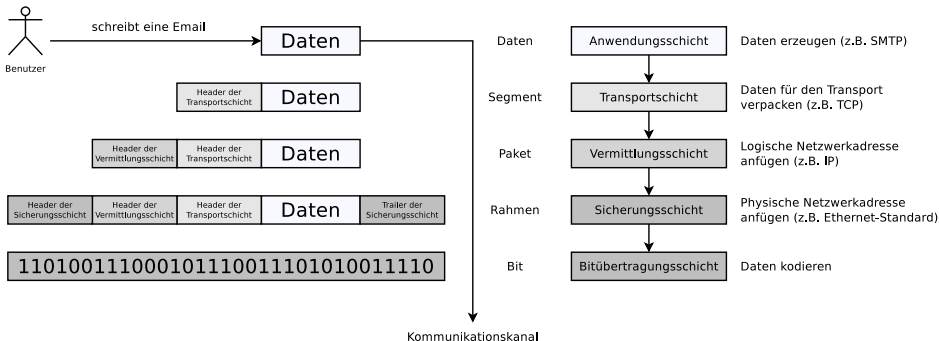
- Das TCP/IP-Referenzmodell unterscheidet nicht zwischen den Bitübertragungs- und Sicherungsschicht, dabei sind diese Schichten völlig unterschiedlich
 - Die **Bitübertragungsschicht** hat mit den Übertragungsmerkmalen von Kupferdarht, Glasfaser und drahtlosen Kommunikationsmedien zu tun
 - Hier findet der physische Anschluss und die Umsetzung der Daten in Signale statt
 - Die **Sicherungsschicht** ist darauf beschränkt, den Anfang und das Ende von Rahmen abzugrenzen und sie mit der gewünschten Zuverlässigkeit von einem Ende zum anderen zu befördern
 - Hier findet die Zerlegung des Bitstroms in Rahmen (engl. Frames) und die Sicherung des Datentransfers durch Fehlererkennung und -behebung statt
- Ein korrektes Modell sollte beides als separate Schichten beinhalten
 - Das TCP/IP-Modell tut das nicht

Quelle: **Computernetzwerke**, Andrew S. Tanenbaum, Pearson (2000)

Ablauf der Kommunikation (1/2)

• Vertikale Kommunikation

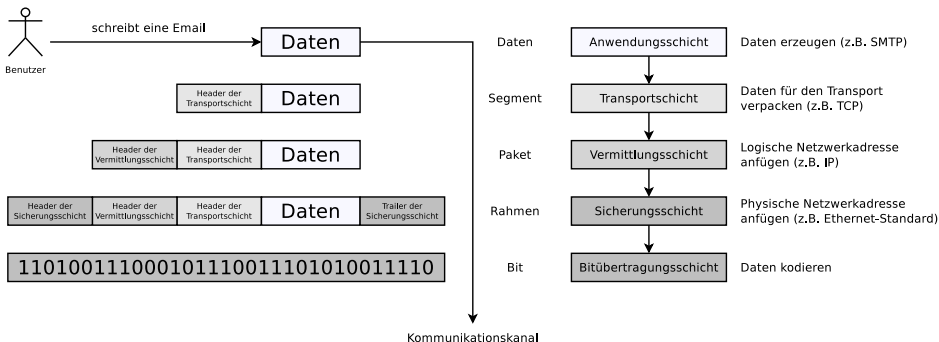
- Eine Nachricht wird von oben nach unten Schicht für Schicht verpackt und beim Empfänger in umgekehrter Schichtreihenfolge von unten nach oben wieder entpackt
- **Data Encapsulation** (Datenkapselung) und **De-encapsulation**



Ablauf der Kommunikation (2/2)

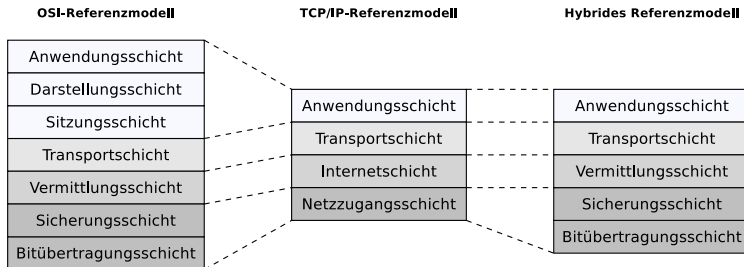
• Horizontale Kommunikation

- Auf den gleichen Schichten von Sender und Empfänger werden jeweils die gleichen Protokollfunktionen verwendet
- Die Schichten können jeweils den der Schicht entsprechenden Zustand des Datenpakets verstehen



OSI-Referenzmodell

- Einige Jahre nach dem TCP/IP-Referenzmodell (1970) wurde das OSI-Referenzmodell ab 1979 entwickelt und 1983 von der Internationalen Organisation für Normung standardisiert
 - OSI = Open Systems Interconnection
- Der Aufbau ist ähnlich zum TCP/IP-Referenzmodell
- Das OSI-Modell verwendet aber 7 statt nur 4 Schichten



Schichten des OSI-Referenzmodell (1)

① Bitübertragungsschicht

- Wird auch **Physische Schicht** genannt
- Ist für das Übertragen der Einsen und Nullen zuständig
- Das Protokoll bestimmt unter anderem:
 - Wie viele Bits können pro Sekunde gesendet werden?
 - Kann die Übertragung in beide Richtungen gleichzeitig stattfinden?
- Treten bei der Übertragung der einzelnen Bits durch die Bitübertragungsschicht Fehler auf (ist in der Realität die Regel), ist ein Verfahren notwendig um diese Fehler zu erkennen und zu korrigieren
 - Das ist die Hauptaufgabe der Sicherungsschicht

Schichten des OSI-Referenzmodell (2)

② Sicherungsschicht

- Soll fehlerfreien Datenaustausch gewährleisten
- Regelt den Zugriff auf das Übertragungsmedium
- Adressierung der Geräte mit physischen Adressen (MAC-Adressen)
- Gruppirt die Bits in Einheiten (sog. Rahmen bzw. Frames)
- Fügt zur Fehlererkennung jedem Rahmen eine Prüfsumme an
 - So können fehlerhafte Rahmen vom Empfänger erkannt und entweder verworfen oder sogar korrigiert werden
 - Ein erneutes Anfordern verworfener Rahmen sieht die Sicherungsschicht nicht vor
- Im Header ist eine laufende Nummer zur Unterscheidung der Rahmen

Schichten des OSI-Referenzmodell (3)

③ Vermittlungsschicht bzw. Netzwerkschicht

- Sorgt für den eigentlichen Datentransfer zwischen den Rechnern
 - Wählt den Pfad (besten Weg) im Netzwerk (Vermittlung bzw. Routing)
- Der kürzeste Weg ist nicht immer auch der Beste
 - Die Verzögerung auf einer gegebenen Route ist entscheidend
 - Die Verzögerungen ändern sich je nach Auslastung der Strecke
- Die beiden darunterliegenden Schichten ermöglichen nur die Kommunikation zwischen angrenzenden Rechnern
 - Die Vermittlungsschicht ermöglicht Kommunikation über die Grenzen eines Netzwerks hinaus
 - Die Daten werden mit Ziel- und Quelladressen versehen, über die das zielgerichtete Routing möglich ist
- Das am weitesten verbreitete Netzwerkprotokoll ist das verbindungslose IP (Internet Protocol)
 - Jedes IP-Paket wird unabhängig an sein Ziel vermittelt (*geroutet*)
 - Der Pfad wird nicht aufgezeichnet
- Adressierung der Geräte mit logischen Adressen (IP-Adressen)

Schichten des OSI-Referenzmodell (4)

④ Transportschicht

- Sorgt dafür, dass die Daten der Vermittlungsschicht korrekt an die richtigen Anwendungen ausgeliefert werden
- Zwischen Sender und Empfänger können Pakete verloren gehen
- Die Transportschicht sichert die verlustfreie Lieferung der Nachrichten
 - Garantiert die korrekte Reihenfolge der Nachrichtenpakete
- Sorgt für zuverlässigen Datentransfer und ermöglicht den gleichzeitigen Zugriff mehrere Anwendungen auf dieselben Netzwerkdienste
 - Stellt einen transparenten Datenkanal zur Verfügung
- Teilt die Daten beim Sender mit Transportprotokollen in kleine Teile auf, so dass sie von der Vermittlungsschicht weitergeleitet werden können
 - Beim Empfänger werden Sie in der korrekten Reihenfolge wieder zu einem Datenblock zusammengesetzt
- Baut auf verbindungsorientierten oder -losen Netzwerkdiensten auf
- Die zwei wichtigsten Transportprotokolle:
 - TCP (Transport Control Protocol): verbindungsorientiert
 - UDP (Universal Datagram Protocol): verbindungslos
- Kombination TCP/IP ist De-facto Standard für Netzwerkkommunikation

Zwei wesentliche Arten von Protokollen

- Man unterscheidet 2 Protokollarten
- **Verbindungsorientierte Protokolle**
 - Analog zum Telefon
 - Eine Verbindung zwischen Sender und Empfänger wird aufgebaut, dann werden Daten ausgetauscht und handeln das zu verwendende Protokoll aus. Anschließend wird die Verbindung abgebaut
 - Es gibt eine Zustellungsgarantie
 - Diese ist aber zeitaufwendig
- **Verbindungslose Protokolle**
 - Analog zum Briefkasten
 - Kein Verbindungsaufbau notwendig
 - Nachrichten werden vom Sender verschickt, wenn Sie vorliegen, ohne eine Verbindung aufzubauen
 - Keine Zustellungsgarantie, dafür schneller

Schichten des OSI-Referenzmodell (5)

5 Sitzungsschicht

- Erweiterte Version der Transportschicht
 - Ist für Aufbau, Überwachung und Beenden einer Sitzung verantwortlich
- Eine Sitzung ist die Grundlage für eine virtuelle Verbindung zwischen 2 Anwendungen auf physisch unabhängigen Rechnern
- Bietet Funktionen zur Dialogkontrolle (welcher Teilnehmer gerade spricht)
 - Sorgt für Verbindungsaufbau und Verbindungsabbau
 - Sorgt für die Darstellung der Daten in einer für die darüberliegende Schicht unabhängigen Form
- Bietet u.a. Funktionen zur Synchronisierung
 - Kontrollpunkte können in längeren Übertragungen eingebaut werden
 - Kommt es zum Verbindungsabbruch, kann zum nächsten Kontrollpunkt zurückgekehrt werden und die Übertragung muss nicht von vorne beginnen

Die Sitzungsschicht wird in der Praxis kaum benutzt

Schichten des OSI-Referenzmodell (6)

6 Darstellungsschicht

- Enthält Regeln zur Formatierung (Präsentation) der Nachrichten
 - Der Sender kann den Empfänger informieren, dass eine Nachricht in einem bestimmten Format vorliegt
 - Datensätze können hier mit Feldern (z.B. Name, Matrikelnummer. . .) definiert werden
 - Art und Länge des Datentyps kann definiert werden
 - Komprimierung und Verschlüsselung können hier eine Rolle spielen

Die Darstellungsschicht wird in der Praxis kaum benutzt

Schichten des OSI-Referenzmodell (7)

7 Anwendungsschicht

- Bindeglied zwischen Benutzer und Anwendungsprozessen
- Sollte ursprünglich eine Sammlung von Standard-Netzwerkanwendungen enthalten
- Es werden hauptsächlich Anwendungsprotokolle eingesetzt
- Aus Sicht des OSI-Modells sind alle verteilten Systeme lediglich Anwendungen in der Anwendungsschicht
- Populäre Protokolle: HTTP, FTP, Telnet, SSH, NFS, SMTP, LDAP

Nächste Vorlesung

Nächste Vorlesung:
8.12.2011