Zusammenfassung Kommunikationstechnik

Kommunikationssystem:
physikalisches und logisches System zur Realisierung der datentechnischen Verbindung zweier Prozesse

Offenes System:
jeder, der Hard- und Softwareprotokolle anerkennt darf als Kommunikationspartner am Prozess teilnehmen
Endsysteme sind nicht an bestimmten Hersteller oder Architektur gebunden
Endsysteme stellen selbständige Rechnersysteme dar und arbeiten automatisch
können in Kommunikation mit anderem Rechnersystem treten
Endgerät ist für ordnungsgemäße Durchführung der Kommunikation selbst zuständig

Verbundsysteme:
arbeiten mittels einer physikalischen und logischen Vorschrift miteinander

Parameter:
= Veränderliche
-> beschreibt Abhängigkeit einer (physikalischen) Größe von einer anderen
= unterscheidende Wert
= funktionaler mathematischer Zusammenhang
-> durch Parameteränderung kann Funktionalität des Systems geändert werden

Schnittstelle (Interface)
Definition:
= definierte, normierte Verbindung zwischen zwei unabhängigen Systemen
grenzt technische Funktionen und/oder administrative Zuständigkeiten bei Geräten und Netzen voneinander ab
Normung:
fest vorgeschriebenen Inhalte:

- elektrische Signale auf den Schnittstellenleitungen
- Betriebsweise (zeitliche Aufeinaderfolge von Signalen und deren Bedeutung)
- mechanische Strukturen der Schnittstelle (Buchse-Stecker, Materialien...)

Normung der Schnittstellensoftware:
X/open – Group:
Zusammenschluss 10 namhafter Computerproduzenten:
-> Ziel: Vereinheitlichung von Unix und Festlegung von Standards

Das Kommunikationssystem

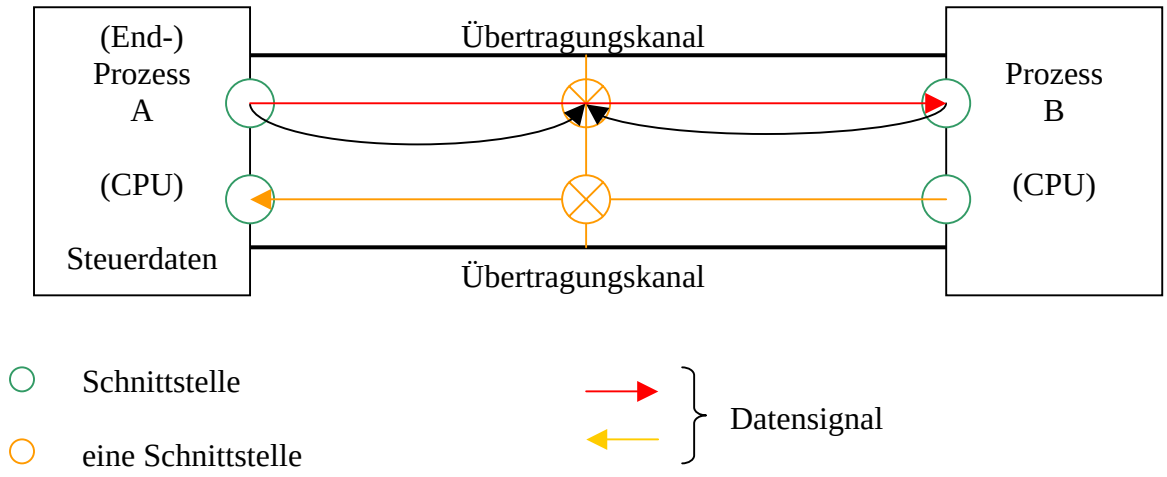
Kommunizieren von Prozessen

- nur aktive Prozesse kommunizieren miteinander
- nur zwei Prozesse kommunizieren miteinander
- einfaches Senden ist keine Kommunikation

Verbindungsarten:
Ein Sender zu einem Empfänger -> unicast-Verbindung (Punkt-zu-Punkt-Verbindung)
Ein Sender zu mehreren Empfängern -> multicast-Verbindung
Ein Sender mit Rundspruch an alle Empfänger -> broadcast-Verbindung
=> jede Verbindungsart lässt sich durch andere implementieren -> unicast-Verbindungen realisieren multicast-Verbindung und broadcast-Verbindungen

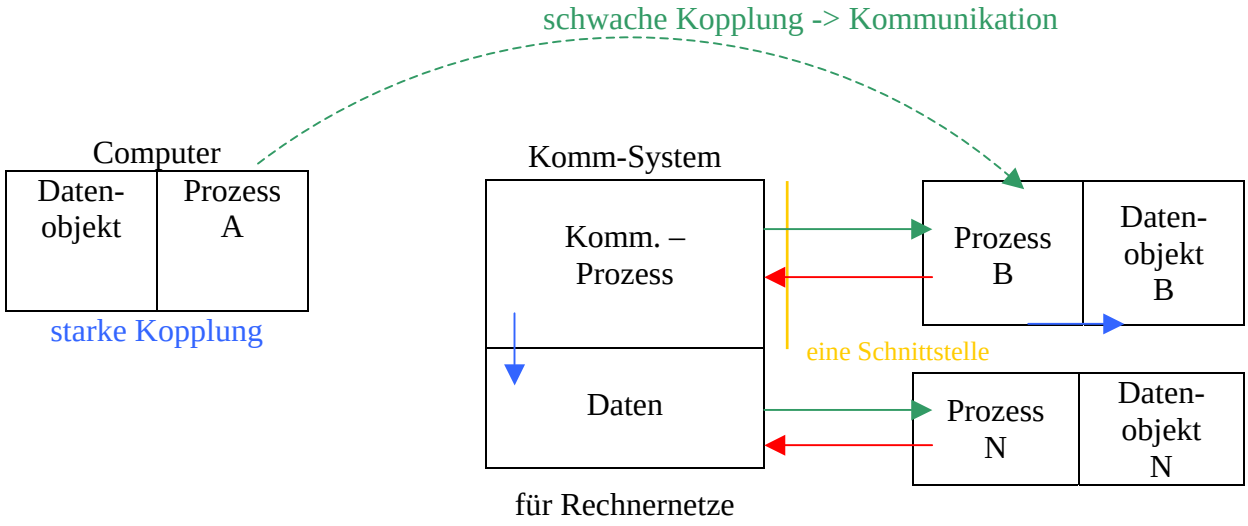
Elemente eines Kommunikationssystems

1. Teilnehmer A: DV-Prozess A, je eine Datenquelle mit Tor und Datensenke mit Tor
2. Teilnehmer B: äquivalent zu A
3. Übertragungskanal: = Kanal mit vermittelndem Medium; Übertragungsverfahren: Simplex-, Halbduplex- oder (Voll-) duplex



Übertragungskanal und Kopplungsarten

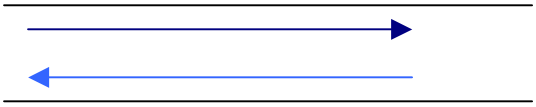
- Teilnehmer A und B immer über Übertragungskanal miteinander verbunden
- Bei Kommunikation will Prozess auf Objekte des anderen Prozesses zugreifen
- Zugriff nur durch Einwilligung möglich
- auf eigenes DV-Objekt kann der eigene Prozess immer direkt zugreifen -> starke Kopplung – keine Kommunikation
- Zugriff auf DV-Objekt eines entfernten zweiten Rechners -> schwache Kopplung – Kommunikation
- bei indirekter schwacher Kopplung kommunizieren nacheinander drei Prozesse:
  1. Prozess A mit Kommunikationsprozess des Kommunikationssytems
  2. Kommunikationsprozess mit Prozess B
- bei direkter schwacher Kopplung erfolgt Austausch ohne aktives Kommunikationssystem
- Übertragungskanal ist bei allen Kommunikationsprozessen passives System



Simplex:

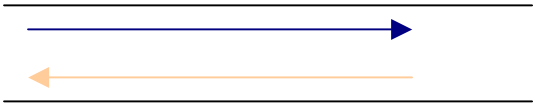
Datenfluss ⟶ Nur eine Richtung

Halbduplex:



zu Zeitpunkt T nur eine Ü-Richtung

Vollduplex:



Übertragung in beiden Richtungen
zur gleichen Zeit

- logischer Übertragungskanal arbeitet mit drei verschiedenen Betriebsarten.
  1. Simplex-Verfahren
  2. Halbduplex-Verfahren
  3. Vollduplex- oder Duplex-Verfahren
- bei Simplex-Verfahren werden Daten nur in eine Richtung transportiert
- Halbduplex ist Modus mit Zweirichtungsverbindung – es kann aber nicht gleichzeitig in beide Richtungen gesendet werden – z.B. bidirektionaler Bus (= Zweirichtungsbus bei Mikrocomputern)
- Vollduplex: es kann gleichzeitig in beide Richtungen gesendet werden
- Kommunikationskanal = logische und physische Verbindung zweier unabhängiger, abgegrenzter und selbständig arbeitender Systeme; physische und logische Schnittstelle zwischen zwei dynamischen Systemen
- nur eine logische Schnittstelle existiert, kann unterschiedlich physisch ausgebildet sein, es kann eine oder mehrere Steckerverbindungen geben

Topologie	Anzahl Verbindungen bei n Netzknoten	Aufwand für das Betreiben	Sicherheit
Stern	n-1	i. A. Netzwerksteuerung durch zentrale Knoten; kostengünstig, einfach	Bei Ausfall des Hub keine Verbindung mehr möglich
vollvermascht	n(n-1) / 2	Steuerung im Allgemeinen nicht zentral, sondern bei den einzelnen Netzpunkten hoher Aufwand	sehr hohe Sicherheit wegen hoher Redundanz
Ring	n	Steuerung i. A. nicht bei einem Knoten, hoher Aufwand	relativ hohe Sicherheit, bei Ausfall einer Strecke oder eines Knotens immer noch jede Verbindung möglich
Linie (Bus)	n-1	Steuerung i.A. nicht bei einem Knoten, hoher Aufwand	sehr geringe Sicherheit, bei Ausfall einer Strecke oder eines Knoten nicht mehr alle Verbindungen möglich

Übertragungsverfahren in LAN

- Es existiert nur ein Übertragungskanal -> wird von allen angeschlossenen Stationen anteilig genutzt
- Übertragungskanal eines Signals über gesamte Bandbreite des Übertragungsmediums
- Bandbreite (Kanal) $\geq$ Bandbreite Signal
- Frequenz = 0 (Signalpegel ist constant) => Gleichanteil im Signal
- Telefonleitung nur über Modem nutzbar, Datensignal wird einem Träger aufmoduliert (dessen Frequenz liegt innerhalb Bandbreite des Kanals)
- nur für kürzere Distanzen geeignet wegen hoher Flankensteilheit => hohe Forderungen an Kabelqualität
- Modem: Modulationsverfahren zur Übertragung von Datensignalen
- zu Zeitpunkt t nur ein Informationsstrom übertragbar
- Breitbandübertragung: Bildung unterschiedlich koexistenter Übertragungskanäle auf Übertragungsmedium
- Frequenzband von 10 bis 450 MHz wird in Teilbänder zersplittet, Teilbänder mit verschiedenen Nutzungsarten (Daten, Audio, Video, ...)
- Ansteuerung unterschiedlicher Informationskanäle durch Frequenzmodulationsverfahren
- Frequenzmodulationsverfahren erfordert Modulation und Demodulation -> Arbeitsaufgabe des Modems
- Breitbandtechnik arbeitet nur mit unidirektionalen Kanälen
- für bidirektionalen Verkehr muss Sende- und Empfangsteil installiert sein
- Trägersignal = eigene Trägerfrequenz des Signals (Trägerfrequenzrtechnik)
- Modem = Modulator/Demodulator

Internettechnologie

Standards:

- Standards => Abmachungen zwischen zwei Partnern oder mehr (Konventionen)
- deren Einhaltung soll Kompatibilität unterschiedlicher Systeme sicherstellen
- verschiedene Standards:
  internationale, nationale, Industrie - Standards
- Konsequenzen bei Verzicht auf Normen und Standards:
  1. Offene Systeme entstehen nicht -> freie Kommunikation nicht möglich
  2. es entstehen Herstellerinseln -> können nicht, oder nur sehr aufwendig in Verbindung verbracht werden
  3. Stärkere Bindungen an einzelnen Hersteller -> Wechsel des Herstellers nicht oder nur mit hohem Aufwand möglich

Repeater:

- Verknüpft mehrere Segmente eines LAN
  -> sind auf physischer Ebene (Schicht 1) identisch
  => Leitungsverstärker

Bridge:

- Verbindung zweier LAN auf Ebene 2
- Voraussetzung: Nutzen gleicher Protokolle
- transparent aus Sicht der kommunizierenden Endsysteme
- ohne eigene Stationsadresse

Router:

- verbindet zwei Netzsegmente auf Schicht 3
- besitzt eigene Stationsadresse
- weiterzugebende Nachrichten werden anhand der Zielnetzwerkadresse heraus gefiltert
- Wegefindung in einem vermaschten System möglich

Gateway:

- Intelligente Schnittstelle
- verbindet LAN's auf kleinster gemeinsamer Ebene (oberhalb Schicht 3)
- Protokollumsetzung

Kommunikationssysteme

Das Internetprotokoll

IP-Header und –Pakete, Datagramme

- Das ISO/OSI-Äquivalent für IP ist Schicht 3
- IP-Header ist "Umschlag" für IP-Paket
- Prüfsumme dient Überprüfung von gelungenen und misslungenen Übertragungen des Kopfes
- wenn Prüfsumme beim Empfänger ungleich des dazu empfangen IP-Headers, wird Paket verworfen
- Nutzdaten des Pakets werden nicht überprüft -> Verfälschung während des Transport durch das Netz
- keine Quittierung -> erst TCP quittiert Empfang
- Weg des einzelnen Pakets einer Gesamtsendung kann unterschiedlich sein -> Pakete werden durchnumeriert
- Zusammenfassung
  1. keine Garantie , dass Paket Empfänger erreicht
  2. keine Anforderung an den Absender für fehlerhafte Pakete
  3. keine Quittierung des Empfängers
- solche Sendungen werden Datagramme genannte

IP-Adressierung

- im Internet werden nur Host-Computer adressiert
- weiter Angaben im Datenpaket -> Angaben interessiert IP nicht
- 32 Bit für IP-Adresse -> theoretisch 4 Milliarden Hosts
- Darstellung als Oktet (4x8 Bit) – getrennt durch einen Punkt
- Vergabe durch NIC
- praktischen IP-Adressen werden 5 Gruppen zugeordnet (A-E) -> beinahe alle Hosts sind Bestandteil eigenständiger Subnetze
- a b c sind adressierbare Subnetze, h mögliche Hostadresse
- Große Netze der Klasse A kann es weltweit nur 128 geben, aber 16 Millionen Hosts
- Mittlere Netze der Klasse B können es 16.384 sein, 65.536 Computer
- Kleine Netze der Klasse C können es 2.097.152 sein, 256 Rechner
- Begründung damals: Effizienz der IP-Routings
- -> es gehen die Internetadressen aus

Domain Name Server (DNS)

- mit *domain name lookup* wird aus Domänennamen gültige IP-Adresse erzeugt
- Datenbanken auf DNS liefern zum Domänennamen IP-Adress und umgekehrt
- Alle DNS sind miteinander verbunden -> nicht jeder muss alle Adressen vorhalten
- IP-Adresse bereits abgefragte Domäns werden durch DNS im lokalen Cache gespeichert -> Erhöhung der Effizienz (nicht alle DB müssen durchsucht werden)
- hierarchische Struktur für Domänennamen -> definiert zahlreiche organisatorische und geografische Hauptbereiche
- oberste Ebene dieser Hierarchie ist Toplevel-Domän

Transmission Control Protocol (TCP)
Aufbau des TCP :

- TCP benutzt nur IP-Pakete Pakete bestehen aus Header und Nutzdaten Nutzdaten werden vom TCP aufgeteilt in: TCP-Header
  2. Nutzdaten
  oder umgekehrt:
  Nutzdaten+TCP-Header = IP-Nutzdaten
- Stabiler und sicherer Verbindungsaufbau nach dem handshake-Verfahren

Aufbau einer TCP-Verbindung:

- Drei Schritte:
  1. Host A sendet Host B IP-Paket mit Absichtserklärung zum Aufbau einer TCP-Verbindung
  2. wenn Verbindung akezptiert wird sendet Host B Host A IP-Paket mit *positiv acknowledgement* -> Quittung an Host A zum Weitermachen
  3. wenn für Host A Verbindung steht, sendet Host A Host B IP-Paket mit positiv acknowledgement

Datenaustausch:

- TCP_Pakete erhalten fortlaufende Nummern
- Host B muss jedes Paket unter Angabe dieser Nummer quittieren
- Host A hat nach Timeout keine Quittung -> Sendung wird wiederholt
- Host A und B müssen über Sendung und Empfang genau Buch führen (automatisches Routing lässt Pakete ungeordnet, beschädigt oder gar nicht ankommen)
- Ausbleibende Sendungen und Quittungen führen zu Dopplungen
- Prüfsumme des TCP-Headers gibt an, ob Paket fehlerhaft ist
- TCP garantiert fehlerfreie und sichere Verbindung zwischen Kommunikationspartnern
- TCP-Schichten haben mit ihren Protokollen festen, logischen Verbindungsaufbau geschaffen
- Vermischung der Pakete, wenn einer der beiden Kommunikationspartner Verbindung zu einem Dritten aufbaut -> Lösung: Vergabe von TCP-Portnummern
- TCP-Portnummern stehen im TCP-Header als logische Portnummer mit 16 Bit
- soll Verbindung zustande kommen, muss sendende Host richtige Portnummer des empfangenden Hosts (neben der IP-Adresse) angeben
- Wahl der Portnummer in den Host frei
- wichtige Internetadressen haben bestimmte Standardnummern (Webserver: Port 80; E-Mails: Port 110)

TCP-Portnummern, Sockets, Winsocks

- zwei Computer können über 1 TCP-Verbindung für z.B. ftp-Download (an Port 20), eine WWW (an Port 80) und Newsgroup-Artikel-Abholung (an Port 119) gleichzeitig unterhalten
- Socket = Kombination von IP-Adresse und TCP-Portnummer
- Jede Kommunikation im Net findet über diese beiden Elemente statt
- Internet-Programm sendet und empfängt Daten über ein Objekt vom Datentyp Socket
- jeweiliges BS stellt Sockets bereits fertig zur Vefügung -> muss sich nicht um IP-Adressen und Ports kümmern
- Übertragung dieses Konzepts in Microsoft-Welt => Winsock
- in den Winsocks-DLLs stehen notwendige Basisroutinen
- Alle Internet-Programme kommunizieren via TCP
- Portieren von Netzwerksoftware (z.B. Unix) auf Windows-Maschine dank weitgehender Standardisierung relativ einfach

Netzwerkanbindung unter UNIX

Netzwerksoftware

- dominierende Low-Level-Netzwerksoftware war TCP/IP-Protokoll (und ist heute)
- Komponenten:
  1. IP (Internet Protokoll): transportiert Rohdaten
  2. ICMP (Internet Control Message Protokoll): stellt für IP mehrere Low-Level-Unterstützungen bereit z.B. Fehlermeldungen, Routing-Hilfen, Echo-Anforderungen
  3. ARP (Address Resolution Protocol): wandelt logische Netzwerk in physische Hardwareadressen um
  4. UDP (User Datagram Protocol): transportiert nicht geprüfte Meldungen unter Verwendung von IP von einem Programm zum anderen
  5. TCP (Transmission Control Protocol): transportiert Daten zuverlässig und verbindungsorientiert unter Verwendung von IP von einem Programm zum anderen
- TCP/IP ist einheitliche Programmierschnittstelle -> Systeme mit verschiedenen Netzwerkhardware können Daten austauschen
- Mit TCP/IP können physikalisch separate Netzwerke über Software größere und flexiblere "logische Netzwerke" bilden

Netzwerkarchitekturen

ISO-OSI-Modell

- 7 Schichten-Architektur
- Probleme sind aufgetreten:
  1. OSI-Protokolle basieren auf unrealistischen Konzepten, die in aktuellen Netzwerken nicht mehr benötigt werden
  2. Spezifikation teilweise unvollständig
  3. OSI-Protokolle sind industriellen Standards unterlegen
  4. 7 Schichten haben schlechte Performance
- OSI hat heute nur noch theoretischen Wert
- Folge: Computersysteme mit Industrie entwickeln lassen

TCP/IP-Modell

- Industriestandards mit 4 Schichten
- Protokoll einer Schicht basiert auf Protokoll der darunterliegenden Schicht

- Daten werden im Protokollsack der sendenden Maschine nach unten gereicht, bei der empfangenen Maschine nach oben
- Standardprotokoll für Kommunikation zwischen unterschiedlichen DV-Systemen
- IP = Internet Protocol => Ebene 3 des ISO/OSI – Modell)
- TCP = Transfusion Control Protocol => Ebene 4
- UDP = Quittungsloser Diagrammaustausch möglich
- Standarddienste TCP:
  1. Telnet (Virtual Terminal Protocol): User-Terminal am Host
  2. FTP (File Transfer Protocol): Dateisendungen
  3. SMTP (Simple Mail Transfer Protocol): einfacher Postdienst

NFS von SUN
- NFS = Network File System
- Dienste:
  1. Einrichtung von Directories durch den User
  2. Zugriff auf Daten in entfernten Servern
- Kopplung von Servern in einem Netz
- transparenter Datenaustausch in heterogenen Netzen
- Weitere Protokolle unter NFS:
  1. XDR = External Data Representation: stellt maschinen-, betriebssytem- und Netz unabhängige Datenstruktur zur Verfügung
  2. RPC = Remote Procedure Call: entfernter Dienstaufruf

Ethernet-Paket und Adressierung
- BS UNIX unterstützt verschiedenen physikalische Netzwerke: Ethernet, Token Ring, modembasierte Systeme
- in Verbindungsschicht wird Hardware verwaltet; Protokolle der höheren Schichten wissen nichts davon
- Netzwerkschnittstelle = Verbindung einer Maschine zum Netzwerk
- bei mehreren Netzwerkschnittstellen können Netzwerkkarten miteinander verbunden werden -> Router, Routing!
- Gateway = Router mit Protokollkonvertierung
- Transfer von Rohdaten findet in Form von Paketen statt
- Paket (Frame) besteht aus Header und Nutzlast
- Jede Schicht fügt Header dazu und betrachtet Paket der darüberliegenden Schicht als Nutzlast -> stetige Zunahme der Paketlänge
- TCP verwendet unterschiedliche Adressierungsschemen:
  1. Netzwerkhardware wird mit 6 Byte adressiert
  2. IP-Adresse jedes Netzwerkgerätes ist 4 Byte lang
  3. Verbindungsschicht des TCP/IP-Modells realisiert Verbindung von IP-Adresse und Hardwareadresse
- ARP ordnet bestimmter IP-Adresse eine Hardwareadresse zu

Routing
- Routing Dämonen setzen Routingprotokolle zur Realisierung des Informationsaustauschs ein
- gebräuchlisten Routingprotokolle:
  1. RIP = Routing Information Protokoll
  2. OSPF = Open Shortest Path First
  3. IGRP = Interior Gateway Routing Protocol
  4. EGP = Exterior Gateway Protocol

5. BGP = Border Gateway Protocol
6. DVMRP = Distance Vecot Multicast Routing Protocol

- Interne Protokolle: RIP, OSPF, IGRP
- Externe Protokolle: EGP, BGP
- IP-Multicast mit DVMRP

Einrichtung eines Netzwerks

- 6 Etappen zum Aufbau
  1. Planung: festlegen der physischen und logischen Struktur
  2. Adressenzuweisung: aktiven Netzwerkkomponenten werden eindeutige IP-Adressen zugewiesen
  3. Hardwareinstallation: Einrichtung der Netzwerkhardware
  4. Hosteinrichtung: Hosts müssen bei Bootfolge Konfigurieren der Netzwerkschnittstellen ermöglichen
  5. Routing: Routing-Dämonen und/oder statische Routes einrichten
  6. Debugging: Fehlersuche
- physische Struktur ist heute Ethernet, beginnend mit 3 Mbit/s; als Standard mit 10 Mbit/s, 100 Mbit/s, 500 Mbit/s und 1 Gbit/s
- Zugriffsverfahren ist CSMA/CD:
  1. CS = Carrier Sense: erkennen, ob jemand spricht
  2. MA = Multiple Access: jeder kann sprechen
  3. CD = Collision Detection: erkennen, ob jemand ins Wort gefallen ist
- Im Internet ist jede zugewiesene IP-Adresse eindeutig
- Zuweisung erfolgt für eine Netzwerkschnittstelle
- Kommando ifconfig aktiviert/deaktiviert Netzwerkschnittstelle, setzt IP-Adresse, überträgt Adressen und setzt Operationen und Parameter
- route definiert statische Routen -> Einträge in der Routing-Tabelle werden vorgenommen
- Weg durchs Netzwerk ist statisch
- Weg wird auf der IP-Schicht in der Routing-Tabelle gesucht -> gibt es einen, geht es über diesen; gibt es keinen, wird Standardroute verwendet oder an Sender zurückgegeben
- Dämonen routed und gated setzen die Routes
- gated ist generische Routing-Shell für unterschiedliche Protokolle
- durch editieren dieser Shell wird Dämon für spezifische Aufgaben fit gemacht

Das Ethernet

Historisches

- Metcalfe entwickelt Aloha-System
- Funktionsweise:
  1. Alle Stationen konnten senden, wenn sie Quittung vom Empfänger erhalten, war Übertragung erfolgreich
  2. Kam keine Quittung zurück, musste von Kollision mit der Sendung ausgegangen werden
  3. Wiederholung der Sendung nach Wartezeit
- Gravierender Nachteil:
  Totales Versagen bei erhöhtem Sendeaufkommen im Netz -> Entwicklung eines Verfahrens zur Kollisionserkennung
- Zufalls-Zugriffsverfahren kann nur anwendungsbereit gemacht werden, wenn Kanal ständig abgehört wird und bei "Ruhe" gesendet wird
- Folge: CSMA/CD ist entstanden
- CSMA/CD = Trägermedium frei -> Horchen, Mutiple Access – bei Mehrfachzugriff -> alle Senden, Collision Detect – Kollision erkennen
- Collision Detection ist Kollisionserkennungsverfahren, mit dessen Hilfe die sendende Station prüft, ob Daten kollisionsfrei versendet wurden

Position im Schichtenmodell

- Ethernet-Protokolle definieren ISO-OSI-7-Schichtenmodelle und TCP/IP-Kommunikationsmodell die Schichten 1 und 2
- Ersetzen der proprietären Herstellerlösungen durch offene, herstellerunabhängige Standard-Systeme
- Normierung der Datennetze durch:
  1. ANSI (American National Standards Institute)
  2. CCITT (Comité Consultatif International Télégraphique et Téléphonique)
  3. DIN (Deutsches Institut für Normierung)
  4. ECMA (European Computer Manufacturers Association)
  5. ISO (International Standards Organization)
  6. IEEE (Institute of Electrical and Electronic Engineers) -> IEEE-Konsortium definiert Übertragungsmechanismen der unteren zwei Schichten des OSI-Referenzmodells
     IEEE-Standards für CSMA/CD, Token Ring, Token Bus

Physical Layer

- Ethernet arbeitet mit Koaxialkabel
- verschiedene bestehende Versionen bauen alle auf 10Base5 auf
- 10Base5 folgt aus:
  erste Teil ist Übertragungsrate (10Mbit/s)
  zweite Teil ist Übertragungsverfahren (Basis- (Base) oder Breitband(Broad)) -> da hohe Kosten gibt es bisher nur Broad-Standard
  dritte Teil zeigt 100-fache maximale Segmentlänge bei Koaxialkabel (5*100 =500m), oder nennt die anderen Medien (LWL und Twisted-Pair-Kabel)
- physial Layer wird in 4 Bereiche geteilt:
  1. Physical Line Signaling (PLS): Signalisieren (auf) der physikalischen (Übertragungs-)linie
  2. Attachment Unit Interface (AUI): Befestigungsstück der Schnittstelle
  3. Physical Medium Attachment (PMA): Befestigung am physikalischen (Übertragungs-)medium

4. Medium Dependent Interface (MDI): (Übertragungs-)medium-abhängige Schnittstelle

- Diese Teile bereiten Daten auf -> Datenkodierung, elektrische/physikalische Anpassung

Physical Line Signaling (PLS)

- PLS verbindet MAC-Ebene mit unteren Teilschichten
- Hauptaufgabe: bestimmte Zustände des vorhandenen Ü-medium an MAC-Ebene weiter zu geben
- Statusmeldungen wie
  1. Medium ist belegt
  2. Medium ist frei
  3. Kollision auf dem Übertragungsmedium

  werden an MAC-Ebene weitergegeben
- Auf MAC-Ebene werden vom Zugriffsverfahren CSMA/CD entsprechende Entscheidungen abgeleitet (z.B. "Daten senden" oder "erneutes Versenden der Daten wegen Kollision")

Attachment Unit Interface (AUI)

- beim 1. Ethernet (10Base5) wurde starres Koaxialkabel verwendet -> Endgeräte wurden über flexibles Verbindungskabel an Ü-medium angeschlossen
- Physical Layer wurde in zwei Bereiche (AUI+MAU) unterteilt und mit Drop Cable oder AUI-Kabel verbunden
- AUI-Kabel darf max. 50 m lang sein; Definition eines 15-poigen Subminiatur-D-Steckverbinder mit Schiebeverriegelung
- An AUI können verschiedene Transceiver angeschlossen werden

Media Access Unit (MAU)

- Media Access Unit wird beim Ethernet Tranceiver genannt, der eigentlichen Zugriff auf Ü-medium sowie Datenübertragung realisiert
- MAU definiert sich aus Physical Medium Attachment und Medium Dependent Interface
- Bei erster Implementierung des Ethernet (10Base5) war MAU separat dargestellt
- nachfolgende Versionen haben MAU auf Netzwerkkarte oder anderen Ethernet-Komponenten integriert

Physical Medium Attachment (PMA)

- PMA ist funktionelle Schnittstelle zwischen oberen und unteren Schichten -> beinhaltet logische Schaltung der MAU
- Hauptfunktion: Wandlung des eintreffenden Datenformats aus den höheren Schichten in ein serielles Format (-> für Koaxialkabel-Übertragung geeignet)
- Auf Empfängerseite für Rückgewinnung des Taktes aus empfangenen seriellen Signal verantwortlich -> notwendig für Synchronisation zwischen Sender und Empfänger

Medium Dependent Interface (MDI)

- MDI ist Bestandteil der MAU
- ist medienabhängige Schnittstelle zwischen Endgerät und gegebenen Ü-mediums (z. B. Koaxialkabel, LWL, TP)
- unterschiedliche technische Ausführungen garantieren unterschiedlichen Anschluss der Ethernet-Varianten an Ü-Medium
- MDI realisiert physikalische Anpassung und mechanische Anpassung

- Ethernet-Standard definiert jeweils eigener Abschnitt das entsprechende medienabhängige MDI

Kommunikation zwischen AUI und MAU

- über MAU sind zum einen Nutzdaten (Data-In-Out-Leitungen), zum anderen Statusdaten (Control-In-Out-Leitungen) zu übertragen
- Conrol-In-Leitungen realisieren Datenaustausch von MAU zum Endgerät; Contro-Out-Leitungen realisieren Datenaustausch vom Endgerät zur MAU
- acht signifikante Signale
  1. Control In A: Statusinformation Kanal A von MAU zum Endgerät
  2. Control In B: Statusinformation Kanal B von MAU zum Endgerät
  3. Control Out A: Kanal A Signalisierung der Betriebszustände
  4. Control Out B: Kanal B Signalisierung der Betriebszustände
  5. Data In A: Kanal A für Dateneingang
  6. Data In B: Kanal B für Dateneingang
  7. Data Out A: Kanal A für Datenausgang
  8. Data Out B: Kanal B für Datenausgang
- Kommunikation über Conrol-Signale erfolgt mittels einfachem Verfahren, dass nur drei Zustände kennt
- Von MAU zum Endgerät => Steuerung des Datenstroms
  1. Control Signal 0 (CS0) => Fehler während Datensendung
  2. Control Signal 1 (CS1) => MAU (noch) nicht sendebereit für Daten
  3. IDL-Signal (idle) => MAU sendebereit für Daten
- Vom Endgerät zur MAU => Senden von Anweisungen an die MAU:
  1. IDL-Signal => MAU geht in normalen Betriebszustand ("reset")
  2. CS0 => MAU geht in Monitor-Mode -> sendet keine Daten mehr
  3. CS1 => MAU geht in normalen Betriebszustand zurück

SQE-Testsignal und Jabber-Schutzfunktion

- SQE-Signal im 10-MBit-Ethernet-Standard definiert
- Signal-Quality-Error-Testsignal wird im AUI-Transceiver bzw. in der MAU dargestellt (mit Funktionalität einer Kollisionserkennung)
- AUI-Transceiver mit SQE-Testfunktion zum Ein- und Ausschalten ausgerüstet
- Funktion: Nach Aussenden des Nutzdatenframes wird Testsignal auf CI-Signalpfad des AUI verschickt -> gleicht dem Signal für erkannte Kollision
- Viele 10 MBit-Ethernetadapter erwarten so ein Signal -> Heartbeat für Erhöhung der Funktionssicherheit -> garantierte Sendeunterbrechung und erneute stochastische Senderauswahl
- SQE-Testsignal wird zwischen den Frames gesendet -> keine Performance-Einbußen
- Bei Verbindung des AUI-Transceivers mit Repeater muss SQE-Testfunktion ausgeschaltet sein -> für Repeater kann es nur "wahre" Kollisionen geben
- Defekte Ethernet-Komponenten, die ständig Daten senden werden mit Jabber-Schutzfunktion "ruhig" gestellt
- Zeitraum für Datensendung beträgt 20-150 ms -> bei Überschreitung erzeugt MAU mit Hilfe der Jabber-Schutzfunktion ein SQE-Signal über CI-Pfad des AUI

10BaseX-Strukturen

1. 10Base5:
   Keine Neuinstallation,
   Koaxialkabel Typ RG 8, max 500m,
   danach Repeater,
   Yellow Cable,
   Busstruktur,
   Basisband,
   Manchester-Codierung,
   Netzanbindung über Taps und Drop Cable

2. 10Base2:
   dünneres Koaxialkabel Typ RG 58A/U oder RG 58C/U, 185m,
   Netzanbindung über T-Stück,
   oft fertig konfektioniert,
   Basisband
   Manchester-Codierung

3. 10Broad36:
   Breitband -> hat sich nicht durchgesetzt
   LWL
   Baumstruktur
   Koaxialkabel
   1800m Segmentlänge
   Netzanbindung direkt über F-Stecker

4. 10BaseT:
   Twisted-Pair-Kabel
   Sternstruktur
   Basisband max. 100m
   Manchester-Codierung
   Anschluss über RJ-45-Stecker

5. 10BaseF:
   Fiber Cable -> LWL, zwei grundsätzliche Varianten im 10MBit-Ethernetstandard
   a) Fiber Optic Inter-Repeater Link für Hub-Verbindungen
   b) neuere 10BaseFL – Variante
   FOIRL: 1000m
   850nm
   Multimode-Fiber mit d = 62,5/125µm
   immer Faser-Paar

6. 10BaseFL:
   Ersetzt FOIRL,
   max. 2000m
   Vielzahl von Netzwerkkomponenten erhältlich -> heute Standard LWL

7. 10BaseFB:
   spezielle Variante des glasfaserbasierten 10-MBit-Ethernet
   für Bereich des Backbone entwickelt

8. 10BaseFP:
   Fiber Passiv -> passiver Sternverteiler für 33 Stationen mit Segmentlänge von 500 m
   Verteiler ist kein Hub oder Repeater
   sollte eigentlich 10BaseFP-Star heißen, gibt keine Produkt am Markt
   Protokoll von einem Hersteller nie umgesetzt

Manchester-Codierungsverfahren

- beschreibt, wie Daten über das serielle Übertragungsmedium transportiert wird
- in Digitaltechnik ist Spannungspegel 0V (logische 0) und +5V (logische 1)
- Darstellung für serielle Übertragung ungeeignet -> es lässt sich wegen des möglich hohen Gleichanteils keine Taktfrequenz zurückgewinnen
- Lösung: Parallel zur Datenleitung muss Taktleitung verlegt sein
  oder
  Auswahl eines geeigneten Codierungsverfahren, dass systemimmanent reichlich Taktinformation beinhaltet -> Manchester-Codierungsverfahren
- Funktionalität: Manchester-Code überträgt Taktinformation kombiniert mit Dateninformation -> Taktinformation befindet sich in der Mitte einer Bitperiode
- Alle Ethernet-Varianten benutzen Manchester-Codierung -> Sicherstellung der Synchronisation zwischen Sender und Empfänger
- Manchester-codierte Signal besitzt genügend Taktinformation -> empfangende Station kann eigentliche Dateninformationen herausfiltern
- im Manchester-Code wird sichergestellt, dass bei einer Folge von gleichen Bits kein gleichförmiges Signal entsteht -> 1. Hälfte der Bitperiode stellt komplementären Wert dar, 2. Hälft den wahren Wert
- innerhalb jeder Bitperiode findet ein Pegelwechsel statt
- dies garantiert:
  1. Gewinnung des Clock-Signals zur Synchronisation
  2. Erreichung einer absoluten Gleichspannungsfreiheit
- Gleichspannungsfreiheit ist notwendig zur Vermeidung eines Gleichspannungsanteil im Datenstrom
- Gleichspannung bewirkt beim Empfänger eine Verschiebung der Arbeitspunkte -> Informationen können nicht mehr aus Signal herausgelesen werden
- Manchester-Code arbeitet bis zu einer Frequenz von 10 MHz und Bitperiode dauert 100ns

Media Access Control (MAC)

- funktionelle Beschreibung auf dem Physical Layer entspricht keiner Netzwerktechnologie
- zielgerichtete Übertragung macht funktionellen Teil aus
- auf MAC-Ebene wird Zugriffsverfahren mit Kollisionserkennung und Umgang mit der Kollision beschrieben
- außerdem werden beschrieben:
  Format (auf das die einzelnen Datenbytes zu bringen sind) und Adressierungsschema (Format der Ethernet-Adressen)
- Funktion des MAC-Layer ist völlig unabhängig von der Physical Layer
- Vorteil:
  Zusammenspiel der verschiedenen Ü-medien sehr eifnach realisierbar
  Zugriffsverfahren und Datenformat sind (über gesamter Evolution des Ethernet) gleich geblieben
- Data Terminal Equipment (DTE) ist unabhänige und adressierbare Einheit
- DTE ist unabhängiger und adressierbarer Endpunkt für Versendung von Daten

- Beim Ethernet tut dies der MAC-Layer
- aber: Endpunkt ist nicht der Übergang vom Netzwerkkabel zum Interface einer Ethernet-Komponente, sondern die obere Ebene des MAC-Layers

Media Access Control (MAC)
Zugriffsverfahren:

- Zugriff: sende willige Station verlangt Alleinbesitz des Ü-mediums
- weil nur einer allein ungestört Daten senden kann, ist Alleinbesitz notwendig
- Alleinbesitz und Zugriff kann gesteuert werden oder sich selbständig regeln
- Teilnehmer teilen sich Kabel und Bandbreite (Koaxialkabel an alle Stationen direkt angeschlossen)
- Diese Multipunktverbindung auf gemeinsam genutztes Ü-medium macht Zugriffsverfahren erforderlich
- Mehrfachzugriff wird erlaubt -> Multipunktverbindung zu einer Überlagerung der Dateninformation auf dem Bus; Folge: Kollision im Ethernet-Standard
- CSMA/CD trägt Rechnung für Multipunkt und Kollision
- CS = Carrier Sense -> Abhören des Trägers
- MA = Multiple Access -> trotz Abhören kann es zu Mehrfachzugriff kommen
- CD = Collision Detection -> Erkennung einer Kollision und Abbruch der Datensendung
- CS kann Kollision nicht verhindern -> zwei Stationen beginnen gleichzeitig mit Aussenden von Daten
- Wahrscheinlichkeit wächst mit zunehmender Anzahl aktiver Stationen
- Zugriffsverfahren erkennt, ob Signal übertragen wird -> Erkennung eines Trägers (carrier)
- da kein tatsächlicher Träger vorhanden ist (Datensignale sind nicht aufmoduliert) wird Erkennung über Datensignale selbst vorgenommen -> Daten sind Träger
- relevante Parameter:
    1. Slot Time:
       Größte mögliche (Lauf-)Zeit, die der kleinste Frame noch zur Erkennung auf der entferntesten Station in einer Kollisionsdomäne haben darf
    2. Inter Frame Gap:
       Zeitraum nach dem CS und vor Aussenden der Daten -> für Erholung der Empfänger
    3. Attempt Limit:
       Maximale Anzahl erlaubter Kollisionen, bis zu der versucht wird, das Frame erneut zu senden
    4. Backoff Limit:
       Zeitraum vor dem wiederholten Aussenden der Daten nach stochastischen Bestimmung der Wartezeit
    5. Jam Size:
       Signal mit 32-48 Datenbits, das sendende Station nach Erkennen als "Störsignal" zum Geltendmachen der Kollision aussendet (Kollisionserkennung durch Gleichspannungsverschiebung)
    6. Minimale Paketgröße:
       64 Byte
    7. Maximale Paketgröße:
       1518 Byte
    8. Frame Header:
       14 Byte

- Zur Taktsynchronisation und zum Einschwingen geht jedem Frame eine 7 Byte lange Präambel und ein 1 Byte langer Start-of-Frame-Delemiter voraus
- wird außerhalb der Slot-Time nach 576 Bitzeiten = Late-Collision
- Late-Collision kann nur im Netzwerk auftreten, dessen Ausdehnung größer als erlaubt ist -> auf genaue Dimensionierung achten
- Backoff-Prozess beschreibt Generieren der Wartezeit nach Kollision nach dem Zufallsprinzip -> kein gleichzeitiges erneutes Starten -> Zahl der Wiederholungsversuche (Ethernet-Standard erlaubt) 1024 Stationen in einer Kollisionsdomäne)