Netzwerktechnik Grundlagen

Sebastian Mahr

9. September 2001

Inhaltsverzeichnis

1 Einführung in die Netzwerktechnik

1.1 Überblick

1.2 Zentrales/Dezentrales Konzept

- Downsizing - Übergang Großrechner zum PC
- Rightsizing - Einbindung eines Großrechners in Client-/Server-Architektur

1.2.1 Zentrales Konzept

Zentraler Großrechner, Terminals an Arbeitsplätzen

1.2.2 Dezentrales Konzept

- Verteilung der Rechen- und Speicherleistung auf verschiedene System
- feinere Skalierung ist möglich

1.2.3 Vor-/Nachteile der Dezentralisierung

- Fehlertoleranz
- Individuelle Gestaltung
- Kosten
- besere Anpassungsfähigkeit an steigende Bedarf
- Möglichkeit des modularen Aufbaus

1.2.4 Nachteile und Probleme

- aufwendigere Softwareverwaltung
- Datensicherheit ist gefährdeter
- Gefahr einer Vireninfizierung
- mögliche Inkombatibilitäten
- schlechter Support, da kein zentraler Hersteller
- Produkttest wegen Vielfalt nicht mehr sorgfältig genung
- guter Systemadministrator wird benötigt
- höherer Verwaltungs- und Wartungsaufwand
- Kommunikation untereinander wird durch unterschiedliche Systeme erschwert

- unterschiedliche Datenformate aus unterschiedlichen Softwarepaketen
- größerer Schulungsbedarf bei den Anwendern

1.3 Ziele beim Aufbau von Rechnernetzen

Man kann die Ziele aus folgenden Sichtweisen betrachten:

- Funktionssicht (Teilhabe am Netz), aus Sicht eines Einzelnutzers
- weitere Nutzungsmöglichkeiten durch Blick auf das Gesamtsystem

1.3.1 Einzelziele

- Informationsbeschaffung
- elektronische Kommunikation: Email, Newsgroups, Bulletin Boards, spezielle Konferenzsysteme
- Rechnernutzung, Benutzung von Mainframes im Dialogmodus
- Remote Job Entries, Ausführen von Computerprogrammen auf entfernten Rechnern, Remote Terminal, Terminalemulation
- Datenzugriff (Redundanz, Inkonsistenz), Vermeidung von Verteilungsabreit
- Programmnutzung, zentrale Installation, dezentrale Nutzung
- Ressourcenteilung, Total Cost of Ownership (TCO, *Microsoft ownes Windows, you just licensed it*), Peripherie-Sharing mit anderen Rechnern im Netz

1.3.2 Gesamtziele

- Datenverbund, unabhängig vom Ort der Speicherung stehen Daten als Gesamtheit oder nach anwendungsbezogenen Kriterien gegliedert an den einzelnen Datenstationen zur Verfügung, das Netzwerk bietet eine sicherere Umgebung für die Daten
- Funktionsverbund, auf einzelnen Arbeitsstationen werden (virtuelle) Funktionen bereitgestellt, die diese selbst nicht erbringen können
- Verfügbarkeitsverbund, damit beim Ausfall von Teilkomponenten das Netzwerk zwar mit verminderter Leistungsfähigkeit, jedoch vollem Funktionsumfang betriebsfähig bleibt (Prioritätenregelung)
- Leistungsverbund, das Netzwerk tritt mit allen beteiligten Stationen als einheitliches System auf, das nach sachlichen Kriterien einzelne Komponenten an verschiedenen Stellen positioniert
- Lastverbund, an einzelnen Stationen entstehende Arbeitslasten werden nach bestimmten Kriterien auf alle Stationen verteilt

- Verteilte Anwendungen

Standardfunktionen in Netzwerken

- Remote Terminal
- Remote Job Entry
- Remote Special Devices
- Filetransfers
- Ditributed Filesystems
- Mailing/Messaging
- Distributed Databases
- Distributed Applications

1.4 Netzwerkarten A

- Clients
- Peers
- Server

Die Aufgabe, die ein Computer übernimmt, hängt vom verwendeten Betriebssystem ab:

- Netzwerkbetriebssystem (WinNT, Novell Server, UNIX)
- Client-Betriebssystem (DOS, OS/2)
- Peer-Netzwerkbetriebssystem (Win9x, MacOS)

Je nachdem, welche Computer an einem Netzwerk teilnehmen, unterscheidet man folgende Arten:

- Server-Netzwerke (oder Client-/Server-Netzwerke)
- Peer- oder Peer-to-Peer-Netzwerke
- Hybridnetzwerke

1.4.1 Servernetzwerke und Domänen

In Server-Netzwerken sorgen Server für die Sicherheit und Verwaltung. Domänen sind Zusammenfassungen von Netzwerken und Clients, die die gleichen Sicherheitsinformationen verwenden. Diese werden von den Domänencontrollern (besondere Server) verwaltet. Es gibt:

- PDC - Primary Domain Controller
- BDC - Backup Domain Controller

Auf dem PDC liegt die Benutzerkonten-Datenbank. Es kann niemand auf die Ressourcen der Server einer Domäne zugreifen, bevor er von einem Domänencontroller erkannt und von diesem dazu autorisiert wurde.

Vorteile Servernetzwerke

- zentrale Sicherheitsfunktionen
- zentrale Datenhaltung
- Bündelung der Hard- und Software, Kostensenkung
- gemeinsame Nutzung teurer Geräte
- optimierte dedizierte Server
- wenig aufwendige Sicherheitsabfragen (???)
- keine gemeinsame Verwaltung von gemeinsamen Ressourcen von Seiten der Anwender
- einfache Verwaltung von vielen Anwendern
- Verhinderung von Datenschwund

Nachteile Servernetzwerke

- teure dedizierte Hardware
- teure Software und Lizenzen (für NW-OS)
- Netzwerkverwalter muß vorhanden sein

1.4.2 Peer-Netzwerke

- keine zentrale Kontrolle
- Organisation in Arbeitsgruppen (Workgroups)
- derjenige, dessen Computer Ressourcen zur Verfügung stellt, vergibt auch die Paßwörter dafür

Vorteile Peer-Netzwerke

- keine Investitionen nötig
- kein Netzwerkverwalter notwendig
- Anwender entscheiden über Nutzen der Ressourcen
- man muß sich nicht auf die Arbeitsfähigkeit von anderen Computern verlassen
- geringe Kosten für kleine Netzwerke

Nachteile Peer-Netzwerke

- zusätzliche Beanspruchung der Computer
- Peers nicht so leistungsfähig wie Server
- Fehlen einer zentralen Organisation
- keine zentrale Datenarchivierung
- Anwender muß selbst Verwalter spielen
- schwache und unzuverlässige Sicherheitsfunktionen
- erschwertes Arbeiten in größeren Peer-Netzen

1.4.3 Hybridnetze

Hybrid-Netzwerke enthalten alle drei Arten von Rechnern.

Vorteile Hybrid-Netze

- Vorteile von Server-Netzwerken
- Viele Vorteile von Peer-Netzwerken
- verschiedene Bereiche können unterschiedlich verwaltet werden (unkritische - Benutzer, kritische - Systemverwalter)

Nachteile Hybrid-Netze

Hybrid-Netze haben die gleichen Nachteile wie Server- und Peer-Netzwerke.

1.4.4 Server-Typen

- Datei-Server (Fileserver)
- Drucker-Server (Printserver)
- Anwendungs-Server (Applicationserver)
- Message-Server
- Datenbank-Server

Im folgenden werden die einzelnen Server-Arten näher erläutert.

1.4.5 Datei-Server

Mit Hilfe der Netzwerk-Dateidienste können Anwender Dateien und die darin enthaltenen Daten austauschen, lesen und schreiben sowie gemeinsam genutzte Dateien verwalten. Folgende Datei-Dienste werden unterschieden:

- Dateitransfer
- Dateispeicherung und Dateimigration
- Dateisynchronisation
- Dateiarchvierung

Dateitransfer

3 Arten von Speichermedien:

- Online-Medien

  z.B. Festplatten, RAID-Systeme (Redundant Array of Inexpensive/Independend Disks, RAID 0-7), insgesamt sind Online-Speichermedien als teuer zu bewerten und lohnt sich für einen großen Teil der Daten, die nicht ständig zur Verfügung stehen müssen, nicht

- Offline-Medien

  Dazu zählen z.B. Bandlaufwerke oder MO-Laufwerke mit Wechseldatenträgern. Hohe Speicherkapazität mit relativ geringen Kosten

- Near-line-Speicher

  Mischung aus Online- und Offline-Medien, das Wechseln der Medien entfällt, da Jukebox- oder Bandkarussel-System eingesetzt werden

Datenmigration

Der Begriff bezeichnet den Prozeß, bei dem Daten von einem Medium der oben aufgeführten Kategorie auf ein anderes gespielt werden. Die Dateien, die für die Datenmigration in Frage kommen, können nach den unterschiedlichsten Kriterien ausgesucht werden.

Datensynchronisation bzw. Replikation

Die Dateisynchronisation versucht sämtliche Veränderungen, die an Dateien vorgenommen wurden, in eine chronologische Reihenfolge zu bringen und sicherzustellen, daß jeder Anwender mit der aktuellsten Version einer Datei arbeitet.

Dateiarchivierung

Dateiarchivierung ist die Datensicherung von Dateien auf Offline-Speicher.

Drucker-Server

- mehrere Anwender teilen sich einen Drucker
- Drucker müssen nicht mehr direkt am Computer stehen
- die Leistung der Arbeitsplatzrechner wird durch hohe Übertragungsraten, Druckerwarteschlangen und Druckerpuffer erhöht
- vielfacher gleichzeitiger Zugriff auf einen Drucker durch Druckerwarteschlagen auf dem Server
- Anwender können sich Fax-Dienste teilen

Anwendungsserver

- die Anwendung selber läuft auf dem Server, die Arbeit geschieht an den Terminals
- die Daten bleiben in der Nähe der Anwendung (z.B. Datenbank) und werden zentral an einer bestimmten Stelle gespeichert

Message-Server

Vier Haupttypen:

- E-Mail
  - Nachrichten werden an andere Netzteilnehmer versendet, auch über Internet
  - neue Funktionen erlauben die Einbettung von Videos, Tönen, Grafiken und sonstigen Mist, der nichts darin verloren hat
  - Die Kommuniktationssysteme Telefon und Computer wachsen langsam zu einem einzigen System zusammen

- Workgroup-Anwendungen
  - Workflow-Management-Anwendungen
  - Dokumente mit verknüpften Objekten

  Anwendungen, deren Erledigung Eingaben von mehreren Netzwerkbenutzern verlangen, lassen sich mit derartigen Anwendungen wesentlich leichter erledigen.

- Objektorientierte Anwendungen
  - komplexe Aufgaben werden durch die Kombination von kleineren Anwendungen gelöst, die als Objekte bezeichnet werden
  - Message-Dienste erleichtern die Kommunikation zwischen den Objekten, indem sie als Vermittler fungieren

- Directory-Services
  - Directory Service Server helfen dabei, Infomrationen im Netzwerk aufzufinden, zu speichern und zu sichern.
  - der Server merkt sich, welche Ressourcen welchen Anwendern und Clients in der Domäne zur Verfügung stehen

Datenbank-Server

Die meisten Datenbanksysteme arbeiten auf Client-/Server-Basis.

- die Client-Komponente der Anwendung läuft auf einem Client mit geringen (ausreichendem) Funktionsumfang
- die Server-Komponente umfaßt den gesamten Funktionsumfang der möglichen Datenbankoperationen, läuft auf dem Datenbank-Server und bearbeitet die Anfragen.

Aus Sicht der Endanwender erscheint die Datenbank als eine Einheit

1.5 Netzwerkarten B

Die Netzwerke werden nach geografischen Aspekten eingeteilt.

1.5.1 VLAN - Very Local Area Network

- Entfernung zwischen den Rechnern nur sehr begrenzt (auch innerhalb eines Gehäuses möglich)
- hohe Übertragungsgeschwindigkeiten im GBit-Bereich

1.5.2 LAN - Local Area Network

- lokal beschränkt (innerhalb von Grundstücksgrenzen)
- LAN steht unter der Kontrolle des Benutzers (<-> Betreiber)
  - Betreiber stellt physikalische Übertragungswege zur Verfügung
  - der Benutzer nimmt diesen Dienst gegen Entgelt in Anspruch
- in einem LAN ist der Betreiber auch gleichzeitig Benutzer und umgekehrt -> volle Kontrolle

1.5.3 WAN - Wide Area Network

Sie dienen der Verbindung verteilter Rechnersystemeund stützen sich in der Regel auf Kommunikationsnetze und -dienste öffentlicher bzw. privater TK-Unternehmen (Standleitung). Die Funktion des Betreibers und des Benutzers sind hier wieder klar getrennt.

1.5.4 MAN - Metropolitan Area Network

- auf ein Ballungsgebiet begrenztes WAN
- es basiert auf speziellen Hochfrequenzkabeln (z.B. Glasfaser)

1.5.5 GAN - Global Area Network

Verbindung von Rechnersystemen auf unterschiedlichen Kontinenten, z.B. über Satellit.

1.6 Aufbau eines WAN

- bei großen Entfernungen, z.B. zwischen Kontinenten, kann man die Standorte nur noch mit hohem finanziellen Aufwand per Standleitung miteinander verbinden (z.B. sternförmig oder vermascht)
- einfacher ist es, die Standorte über das Internet miteinander zu verbinden
  - diese Lösung ist unsicher, da die Performance der Verbindung stark vom Datenaufkommen im Internet abhängig ist (Datenstaus)
  - jeder Benutzer muß in der Firewall administriert werden, was bei großen Anwenderzahlen nicht mehr wartbar ist
  - sehr großes Sicherheitsrisiko, wird normalerweise sowieso von Firewalls geblockt
- Lösung bieten die VPN (Virtual Private Networks)
  - logische Trennung der im Internet geführten Kanäle des Firmennetzes vom allgemeinen Internet

  - jeder Mitarbeiter kann von überall Zugang zum Firmennetz bekommen, aus seiner Sicht ist es ein lokales LAN
  - VPNs sind preiswerter als herkömmliche Standleitungen
  - Servicequalität eines ISPs definiert sich durch
    * garantierte Verfügbarkeit
    * Reaktionszeiten
    * Laufzeiten
    * Datendurchsatz u.v.m
  - Sicherheitsprobleme werden druch Anwendung des RADIUS-Protokolls vermieden (Remote Authentication Dial-In User Service)
  - Nachteil ist, daß ein ISP gefunden werden muß, der in den erforderlichen Ländern Dial-In-POPs hat

2 Netzwerktopologien

2.1 Begriff Topologie und Überblick

- die Art und Weise, in welcher die physische Verbindung zwischen Knoten eines Netwerkes hergestellt wird, nennt man Netzwerk-Topologie; es gibt:
  - Knoten (nodes)
  - Verbindungen (connections)
- die Topologie ist primär vom Einsatzzweck des Netzes abhängig
- jedes verwendete Gerät im Netz ist ein Knoten, z.B.
  - intelligente Arbeitsstationen
  - Datenverarbeitungsanlagen
  - zentrale Großrechner
  - Netzwerk-Server
  - Gateways
  - aktive Vermittlungsknoten (Repeater, Bridges, Router, Hubs)
  - passive Vermittlungsknoten (z.B. Leitungs-Splitter, passive Hubs)
  - Drucker mit direktem Netzwerkanschluß
  - als Verbindung versteht man die physikalische Verknüpfung zwischen Knoten in einem Netz

Es werden im weiteren folgende Topologien erläutert:

- Grundformen

  - Bus
  - Stern
  - Ring
- kombinierte Formen
  - Stern-Bus
  - Stern-Ring
- erweiterte Formen
  - Masche
  - Baum
- Formen nach Art der DÜ
  - Diffusionsnetz
  - Teilstreckennetz

2.2 Bus-Topologie

- wird häufig in kleinen, einfachen oder vorübergehenden Netzen eingesetzt
- das Kabel (der Bus) besteht aus einem oder mehreren Drähten und hat keine aktiven elektronischen Vorrichtungen, die das Signal verstärken
- Bus-Topologie -> passive Topologie
- wird ein Signal gesendet, so geht es an alle Rechner, die mit dem Bus verbunden sind; nur der Rechner mit der richtigen Adresse kann das Paket empfangen, alle anderen ignorieren die Nachricht
- es kein nur ein Computer zur Zeit eine Nachricht senden, jeder Rechner muß warten, bis das Netz frei ist, um zu senden (gilt auch für Stern- und Ringnetze)
- das Signal geht über die gesamte Länge des Kabels, deshalb muß es am Ende absorbiert werden, um Reflexionen zu vermeiden; dies erfolgt mit Terminatoren
- auf einem nicht-terminierten Bus kann ein Signal wie ein Echo hin- und herwandern, dies nennt man Klingeln bzw. Ringing
- gängige Varianten von Bus-Netze:
  - 10Base2 - Thinnet
  - 10Base5 - Thicknet
  - Norm IEEE802.3

Vorteile

- einfacher Aufbau und Zuverlässigkeit
- preisgünstige Verkabelung
- einfach zu erweitern
- Einsatz eines Repeaters möglich, um größere Entfernungen zu überbrücken
- Ausfallsicherheit (fällt ein Knoten aus, ist nicht das komplette Netz betroffen)

Nachteile

- geringe Performance
  - es kann nur ein Computer zur gleichen Zeit senden
  - ein Teil der Bandbreite wird für Übertragungsfunktionen verwendet
- jedes BNC-Verbindungsstück schwächt das Signal
- schwierige Lokalisierung von Fehlern

2.3 Stern-Topologie

- sämtliche Kabelverbindungen laufen zu einer zentralen Stelle, wo entweder ein Computer (z.B. Großrechner) oder ein reines Vermittlungsgerät (Hub oder Sternkoppler) steht
- die Stern-Topologie wird in konzentrierten Netzen eingesetzt, deren Endpunkte direkt von einer zentralen Stelle aus erreichbar sind
- jeder angeschlossen Computer kommuniziert mit einem zentralen Hub, der die Nachricht entweder
  - an alle Computer des Netzwerkes weiterleitet (Broadcast-Stern-Netzwerk), der Hub kann aktiv oder passiv sein
  - oder nur an einen bestimmten Computer (Switched-Stern-Netzwerk) weiterleitet
- ein aktiver Hub verstärkt das elektrische Signal und leitet es an alle angeschlossen Rechner weiter (Multiport-Repeater)
- einfache Erweiterung durch Anschluß eines weiteren Stern-Hubs anstelle eines Computers

Vorteile

- einfache Erweiterung
- gute Wartbarkeit durch Zentralisierung, intelligente Hubs stellen auch Funktionen zur Überwachung und Verwaltung bereit
- Ausfall von einem Rechner beeinträchtigt nicht das gesamte Netz, der Hub kann den Fehler diagnostizieren und entsprechend behandeln
- Hubs können unterschiedliche Kabeltypen akzeptieren
- ein Stern-Netzwerk ist der flexibelste Netzwerktyp und im Falle eines Netzwerkfehlers einfach zu reparieren

Nachteile

- bei Ausfall des zentralen Hubs ist das ganze Netzwerk funtkionsunfähig
- viele Stern-Netzwerke benötigen an zentraler Stelle einen Signal-Verstärker
- großer Kabelbedarf

2.4 Ring-Topologie

- jeder Computer wird mit dem nächsten verbunden, wobei das letzte Gerät wieder mit dem ersten verbunden wird
- jeder Computer übertragt das weiter, was er vom Vorgänger empfangen hat (bis das Paket den Zielrechner erreicht)
- die Daten werden in eine Richtung übertragen (unidirektional), daher Ring-Topologie
- jeder Rechner verstärkt das Signal beim Weiterleiten (aktives Netzwerk)
- keine Terminatoren notwendig, da geschlossener Kreis
- einige Ring-Netzwerke leiten Tokens weiter
  - ein Token ist eine kurze Nachricht, die im Netz weitergeleitet wird, bis ein Computer Informationen an einen anderen senden möchte
  - möchte ein Computer nun senden, verändert er das Token und leitet es weiter
  - stimmt die Empfängeradresse des Tokens mit der Adresse eines Rechners überein, nimmt dieser das Paket an und erstellt eine Empfangsbestätigung an den Absender
  - der sendende Computer erstellt ein weiteres Token und leitet es ins Netz, damit andere Computer darüber kommunizieren können (dieses zirkuliert solange, bis ein Computer es aufgreift und sendet

  - kehrt das Token an den Ausgangspunkt zurück, ist der Zielrechner nicht gefunden worden
  - schnelle Netze lassen mehrere Tokens gleichzeitig zirkulieren

Varianten der Ring-Topologie:

- doppelter Ring, die Stationen sind mit einem zweiten (leistungsschwächeren Ring) miteinander verbunden, Backup-Ring
- Zweifach-Ring, außer dem Hauptknoten existiert eine Verbindung jedes Knotens mit dem übernächsten
- Stern-Ring

Vorteile

- jeder Computer hat gleichen Zugriff auf das Token, daher keine Monopolisierung des Netzwerkes
- werden immer mehr Rechner angeschlossen, bleibt das Netz funktionfähig, die Leistungsfähigkeit nimmt aber über einen kalkulierbaren Betrag ab

Nachteile

- der Ausfall eines Computers kann das gesamte Netz lahmlegen
- die Fehlersuche ist in einem Ring-Netzwerk sehr schwierig
- Hinzufügen und Entfernen eines Rechner unterbricht das Netzwerk

2.5 Stern-Bus- und Stern-Ring-Topologie

Die Topologien Bus, Stern und Ring werden häufig kombiniert.

- Stern-Bus
  - mehrere Stern-Hubs werden über einen Bus miteinander verbunden
  - bei Ausfall eines Computers kann ein Hub ihn isolieren
  - bei Ausfall eines Hubs können die angeschlossenen PCs nicht mehr miteinander kommunizieren, das Netzwerk zerfällt in zwei Teile
- Stern-Ring
  - ähnliche Verkabelung wie in einem Stern
  - die Kabel sind mit dem zentralen Ringleitungsverteiler über einen Ring verbunden
  - ist eine Station nicht aktiv, wird durch Schließen eines Schalters der Ring aufrechterhalten

2.6 Maschen-Topologie

- es existieren redundate Verbindungen ziwschen den einzelnen Knoten
- jeder Knoten ist mit allen anderen Knoten im Netz direkt verbunden (vollständiges Netz
- die meisten Maschen-Netze sind Hybrid-Netze, die nur ein paar redundante Verbindungen haben
- die Anzahl der Verbindungen errechnet sich durch: Bsp. 6 Geräte $= 6+5+4+3+2+1 = 15$ Verbindungen

Vorteile

- Maschen-Netze lassen sich leicht nach Fehlern durchsuchen
- sie sind sehr fehlertolerant
- geringe Auswirkungen bei Medienfehlern
- unterschiedliche Routen durch redundante Verbindungen

Nachteile

- schwierige Installation
- hohe Kosten

2.7 Baum-Topologie

- Erweiterung der Stern-Topologie mit hierarchischer Struktur
- Großrechnernetze werden oft als Baum aufgebaut (oberste Ebene Mainframe, weiter unten Terminals und Peripherie)
- Beispiel: ARCnet von Datapoint
- Vorteil ist die leichte Erweiterbarkeit, weshalb es sich besonders für komplexe Netze eignet
- der Ausfall von Knoten kann ganze Äste blockieren

2.8 Diffusions- und Teilstrecken-Topologie

Die Topologien werden anhand der Übermittlungsweise unterschieden.

2.8.1 Diffusionsnetz

- Sendeprinzip: Broadcasting, gesendete Nachrichten breiten sich im gesamten Netz aus
- alle Stationen sind an ein gemeinsames Medium angeschlossen
- passive Knoten horchen das Zentralmedium ständig nach Nachrichten ab
- zu Diffusionsnetzen zählen die Bus-Netze sowie einige drahtlose Netze

2.8.2 Teilstreckennetz

- die Nachrichten gelangen über eine oder mehrere Teilstrecken zum Empfänger
- es entstehen Zwischenknoten, die aktiv an der Weiterleitung teilnehmen
- Beispiele sind Maschennetze und Ringnetze, außerdem einige drahtlose Netze wie Richtfunk, Mikrowellenübertragung

3 Netzwerkkomponenten

3.1 Signalübertragung

- Signalübertragung = Art und Weise, in der Daten über ein Medium üertragen werden
- die Nachricht muß so umgeformt werden, daß Empfänger und Sender sich verstehen -> diesen Vorgang nennt man Kodierung (Encoding), das ursprünglche Signal wird so verändert, daß es Daten darstellen kann
- Information kann analog oder digital übertragen werden
  - digitale Signalübertragung
  - analoge Signalübertragung

3.1.1 Digitale Signalübertragung

- die Umwandlung von Daten in ein digitales Signal bezeichnet man als Kodierungs-Schemata
- man unterscheidet zwei Kategorien:
  - Spannungszustands-Kodierung (Current State Encoding)
    Ein Zustand wird durch das Fehlen oder Vorhandensein einer Signalcharakteristik kodiert. Folgende Kodierungs-Schemata werden u.a. bei der Spannungszustands-Kodierung verwendet:

- Unipolar
  - Bipolar
  - Return-To-Zero (RZ)
  - Biphase
- Spannungswechsel-Kodierung (State Transition Encoding)

  Zur Kodierung von Daten wird der Spannungswechsel des Signals genommen. Als Kodierungs-Schemata werden u.a. verwendet:
- Manchester (z.B. in Ethernet-LANs), Darstellung durch Spannungswechsel
  - Differential Manchester (z.B. in Token-Ring-LANs), der Spannungswechsel dient hier für die Taktung
  - Non-Return-To-Zero (NRZ), ähnlich wie Differntial Manchester, allerdings ohne Spannungswechsel in der Mitte eines Intervalls

3.1.2 Analoge Signalübertragung

- analoge Signale bestehen aus elektromagnetischen Wellen; eine anloge Welle ändert sich fortlaufend
- analoge Signale haben folgende Charakteristika:
  - Amplitude - Stärke des Signal oder Höhe einer Welle; eine Amplitude liefert folgende Informationen:
    * elektrische Spannung in Volt
    * elektrische Stärke in Ampere
    * elektrische Leistung in Watt
    * und das Stärkeverhältnis von Signalen zueinander in Dezibel
  - Phase - bezeichnet den relativen Zustand einer Welle zu einer anderen, die als Referenzwelle dient (-> Phasenverschiebung)
  - alle drei Charakteristika können für die Kodierung analoger Signale eingesetzt werden
    * Amplitudenverschiebung: zur Kodierung wird die Amplitude des Signals verändert
    * Frequenzverschiebung: hier wird die Frequenz verändert
    * Phasenverschiebung: zur Kodierung werden die Wechsel von einer Phase zur anderen verwendet

3.1.3 Vergleich Signalübertragungsmethoden

- Vorteile der digitalen Signalübertragung gegenüber der analogen:
  - weniger Übertragungsfehler durch Rauschen oder elektromagnetischen Störungen
  - kostengünstig
- Nachteil: digitale Signale, die über über die gleiche Entfernung geschickt werden wie analoge, werden wesentlich stärker abgeschwächt
- Vorteile der analogen Signalübertragung
  - geringere Dämpfung als bei digitalen Signalen
  - erhöhen der Bandbreite ist möglich (Multiplex)
- Nachteil ist die höhere Fehleranfälligkeit durch Rauschen und elektromagnetischen Störungen

3.1.4 Bit-Synchronisation

Die vorher erläuterten Kodierungs-Schemata modulieren eine bestimmte Eigenschaft des Signals, welche das empfangende Gerät interpretieren muß. Hierbei spielt der Zeitfaktor eine große Rolle. Die Abstimmung der zeitlichen Abstimmung der Signalmessung nennt man Bit-Synchronisation.

Asynchrone Bit-Synchronisation

- die Nachricht beginnt mit einem Start-Bit, um die internen Taktgeber der beiden kommunizierenden Geräte zeitlich miteinander abzustimmen
- werden keine Daten übergeben, laufen die internen Taktgeber asynchron
- asynchrone Übertragungen sind im allgemeinen sehr kurz und enden mit einem Stop-Bit

Synchrone Bit-Synchronisation

Folgende drei Mechanismen werden für die Synchronisation verwendet:

- garantierter Statuswechsel

  Die Synchronisationsinformation ist Teil des Datensignals. Der Empfänger hat die Garantie, daß Statuswechsel in bestimmtem Abständen erfolgen und er seinen internen Taktgeber darauf abstimmen kann

- Seperate Taktsignale

  Hier wird ein seperater Kanal für die Synchronisation verwendet. Diese Methode benötigt also die doppelte Kanalkapaazität und ist recht uneffektiv, außer für kurze Entfernungen

- Oversampling

  Der Empfänger sampelt (nimmt Stichproben) des Signals mit einer wesentlich höheren Rate als die Datenrate (Bsp.: jeder 10. Takt Information, alle anderen 9 zur Synchronisation). Hier kann eine Kodierungsmethode verwendet werden, die auf das Hinzufügen eines Taktsignals verzichtet

3.1.5 Takt

- unter dem Takt versteht man ein Signal, das zwei verschiedene Werte annehmen kann oder das einen sinusförmigen Verlauf hat. Der Wert wechselt in periodischen Abständen
- die Taktdauer/Taktzeit entspricht der Zeit zwischen zwei ab- oder aufsteigenden Flanken
- die Zeit zwischen zwei Nulldurchgängen bezeichnet man die Taktperiode
- die Taktfrequenz ist der Kehrwert der Taktperiode, die Einheit ist Hertz (Hz)
- der Takt wird durch den Taktgenerator erzeugt (Schrittaktgeber)
- die Schrittgeschwindigkeit in Baud (Bd) gibt die Anzahl der von Taktgenerator ausgeführten Schritte in einer Sekunde an

Unterschied Baud und Bit

- die Übertragungsgeschwindigkeit wird in Bit/s angegeben
- die Schrittgeschwindigkeit gibt die Anzahl der Signalwechsel innerhalb einer Sekunde an und wird in Baud gemessen
- wird mit Hilfe eines Signalwechsels ein Bit dargestellt, so entspricht 1 Bit/s einem Baud
- bei mehreren Signalwechseln pro Bit oder umgekehrt stimmt die Gleichsetzung nicht mehr

3.1.6 Übertragungssicherung

Damit die Daten den Empfänger unverfälscht erreichen, fügen alle Sicherungsverfahren den versendeten Daten Zusatzinformation hinzu.

- Paritätsprüfung

  - aus den Daten werden Gruppen gebildet, die aus einer Reihe Datenbits und einem Paritätsbit bestehen. Die Anzalh der gesetzten Bits muß entweder
    * gerade (even parity)
    * ungerade (odd parity)

    sein. Außerdem kann die Bildung der Paritätsbits

- zeichenweise (Querparität)

  - über mehrere Zeichen hinweg (Längsparität)

übertragen werden. Bei einer Längsparität wird nach den gesicherten Zeichen ein weiteres mit den Paritätsinformationen übertragen.

- der Nachteil bei beiden Verfahren ist, daß zwei gleichzeitige Fehler sich aufheben können und nicht bemerkt werden.

- daher verwendet die Blocksicherung (Kreuzsicherung) beide Verfahren gleichzeitig

- Zyklische Blocksicherung

  - CRC - cyclic redundancy check
  - eine auf der Polynomrechnung basierende Prüfsumme wird über eine größere Anzahl von Bits geprüft
  - hohe Fehlererkennungsrate

3.1.7 Basis- und Breitband-Übertragungen

- Die Gesamtkapazität eines Mediums, die Bandbreite, kann auch in mehrere Kanäle unterteilt werden.

- Basisband

  - die gesamte Bandbreite wird für einen Kanal genutzt
  - die meisten LANs arbeiten mit einer Basisband-Technik

- Breitband

  - die gesamte Bandbreite wird in unterschiedliche Kanäle aufgeteilt
  - jeder Kanal kann ein unterschiedliches analoges Signal transportieren

3.2 Netzwerkmedien

Es gibt unterschiedliche Art und Weisen, in einem Netzwerk Verbindungen herzustellen:

- Kabel
  - Koaxialkabel
  - verdrillte Zweidrahtleiter (twisted pair)
  - Glasfaserkabel
- kabellose Medien
  - Einsatz von höheren elektromagnetischen Frequenzen
  - Funkwellen
  - Mikrowellen
  - Infrarotlicht

Der physikalische Weg, über den die Daten gesendet werden, wird als Übertragungsmedium bezeichnet. Jedes Medium kann man nach folgenden Faktoren unterscheiden:

- Kosten
- Installation
- Bandbreite
  - die Kapazität wird normalerweise als Bandbreite angegeben (Megibit pro Sekunde, Mbps)
  - die Bandbreite gibt an, wieviele Bits ein Medium in einer Sekunde übertragen kann
- Knoten-Kapazität
  - jedes Netzwerk-Kabelsystem hat eine natürliche Obergrenze, bis zu der eine bestimmte Anzahl an Rechnern angeschlossen werden können
  - eine Erweiterung über diese Grenze ist nicht oder nur sehr kostspielig möglich
- Dämpfung
  - elektromagnetische Signale werden während der Übertragung abgeschwächt -> Dämpfung
  - zu lange Kabel führen zu Übertragungsfehlern und Netzwerkausfällen, die maximale Länge eines Kabels ist daher begrenzt

- Anfälligkeit gegenüber elektromagnetischen Störungen (EMV)
  - elektromagnetische Störungen werden auch als Rauschen bezeichnet
  - elektromagnetische Störungen werden durch von außen eindringende elektromagnetischen Wellen verursacht, die das Signal beeinflussen
  - derselbe Effekt erlaubt es, das Kabelsignal von außen abzuhören

3.2.1 Kabeltypen

Verdrillte Zweidrahtleiter

- ein verdrehter Zweidrahtleiter besteht aus einem oder mehreren miteinander verdrehten Paaren Kupferdraht (z.B. Telefonkabel)
- eine Störung eines Drahtes durch einen anderen wird als Überlagerung/Übersprechen bezeichnet
- durch die Verdrillung werden die Störungen ausgeglichen, sie bewirkt eine Abschrimung außen

Twisted-Pail-Kabel gibt es mit und ohne Abschirmung:

- UTP - unshielded twisted pair, nicht abgeschirmte Zweidrahtleiter
  - mehrere verdrillte Paare, die sich in einer einfachen Plastikummantelung befinden
  - UTP-Kabel wurden von der EIA (Electrical Industries Association) in Qualitätsstufen eingeteilt:
    * Kategorie 1 und 2: niedrige Datenübertragungsraten < 4 Mbps, Einsatz in älteren Telefonnetzen
    * Kategorie 3: Datenübertragunsrate bis zu 16 Mbps, Standard für Telefonanlagen
    * Kategorie 4: bis 20 Mbps
    * Kategorie 5: gegenüber Kategorie 3 haben sie eine bessere Isolation, mehr Verdrillungen pro m, dafür sind aber Zusatzgeräte nötig und Installation ist teurer
  - für Computernetzwerke sind Kabel der Kategorien 3, 4 und 5 geeignet, sie bestehen aus vier oder acht Drähten (zwei- bzw vierpaarig)
  - UTP-Kabel sind ursprünglich für Telefonnetze gedacht, ein Computernetzwerk kann darüber laufen
  - Folgende Eigenschaften haben UTP-Kabel
    * Kosten: gering
    * Installation: einfach

    * Kapazität der Bandbreite: 1- 155 Mbps bis 100 m, Standard: 10 Mbps
    * Knotenkapazität: maximale Obergrenze 1024
    * Dämpfung: vorhanden, daher maximale Länge 100 m
    * EMV: sehr anfällig, leicht abzuhören

- STP - shielded twisted pair, abgeschirmte verdrillte Zweidrahtleiter

  - Abschirmung besteht aus Aluminium und Polyester (zwischen Plastikmantel und Drähten)
  - Eigenschaften:
    * Kosten: relativ teuer
    * schwierigere Installation, da spezielle Stecker notwendig sind (zusätzliche Erdung)
    * Kapazität der Bandbreite: bei 100 m 16 - 500 Mbps, Standard ist 16 Mbps bis 155
    * Knotenkapazität: maximal 270
    * Dämpfung: wie UTP-Kabel
    * EMV: die Abschirmung blockt einen Großteil der elektromagnetischen Störungen ab, allerdings sind sie immer noch nicht abhörsicher

Koaxialkabel

- sie bestehen aus einem Innen- und einem Außenleiter, die auf der gleichen Achse liegen
- der Innenleiter besteht as Kupferdraht oder einer Litze, der Außenleiter aus einem geflochtenen Draht oder einer Metallfolie (Abschirmung)
- Koaxialkabeltypen:

  - RG-8, RG-11: 50 Ohm, 1 cm Durchmesser, Thick Ethernet (10Base5)
  - RG-58: 50 Ohm, 0,5 cm, Thin Ethernet (10Base2)
  - RG-95: 75 Ohm, Kabelfernsehen
  - RG-62: 93 Ohm, ARCNet

- Eigenschaften:

  - Kosten: mittlere Preislage
  - Installation: BNC-T-Stecker oder Vampirklemmen und Terminatoren werden benötigt, Einsatz meist im Ehternet oder im Stern (ARCNet)
  - Kapazität der Bandbreite: Standard: 10 Mbps, die Bandbreite steigt mit dem Durchmesser des Innenleiters

  - Knotenkapazität: dünne Kabel max. 30, dicke Kabek max. 100 Knoten
  - Dämpfung: maximale Länge liegt bei mehreren Kilometern
  - EMV: Abschirmung bietet guten, aber keinen vollkommenen Schutz vor Störungen

PVC- und Plenum-Kabel

- PVC - Polyvinylchlorid, flexibler, preiswerter Kunststoff, wird oft für Isolation bei Koaxialkabeln verwendet
- Plenum ist der Bereich zwischen richtiger und abgehängter Decke
- für die Verlegung von Kabeln im Plenum gibt es Bestimmungen
- die Brandschutzbestimmung verbietet die Verwendung von PVC im Plenum

Exkurs: x-BASE-x, x-BROAD-x

- die erste Zahl gibt die maximale Datenübertragungsrate in MBit/s an
- der Begriff in der Mitte steht für die Art der Datenübertragung
  - BASE - Basisband
  - BROAD - Breitband
- die letzte Zahl gibt die maximale Länge des Kabels in 100 m an
  - 2 - Segmentlänge 200m
  - T - Twisted Pair
  - F - Fibre

Beispiele:

- 10BASE5 - Thick-Ethernet, Yellow Cable, starr, Verwendung im Backbone-Bereich (Verbindung zentraler Netzbestandteile)
- 10BASE2 - Thin-Ethernet, Cheapernet (schwarze Kabel), Koaxialkabel mit BNC-Steckern, Mindestabstand zwischen zwei Knoten 0,5 m
- 10BASE-T, 100BASE-T - Verkabelung mit UTP/STP bei 10 oder 100 Mbit/s
- 100BROAD-F - Verkabelung von Glasfasern (FDDI)

Glasfaserkabel

- statt elektrischer Signale werden Lichtsignale übertragen
- eine Faser besteht aus einem Kern aus Glas oder Plastik, der das Licht leitet
- die Innenschicht ist mit einer Hülle umgeben, die das Licht zurück zum Kern reflektiert
- jede Faser ist von einer Plastikummantelung umgeben (eventuell mit Verstärkungsdrähten oder mit einem Gel gefüllter Zwischenraum)
- es werden meisten mehrere Fasern zu einem Kabel zusammengefaßt
- es gibt zwei Varianten:
  - monomodale Glasfasern: es gibt nur einen einzigen Pfad für das Licht (für Laser-Signale)
  - multimodale Glasfasern: es existieren unterschiedliche Lichtpfade (aufgrund unterschiedlicher Einfallswinkel der Lichtstrahlen), beim Empfänger kommen alle Teile zur gleichen Zeit an und erscheinen als ein Signal; es entstehen Laufzeitunterschiede, die sogenannte Moden-Dispersion
- monomodale Glasfasern haben eine höhre Bandbreite und könne länger sein als multimodale, sind aber noch sehr teurer
- die Daten werden über eine optische Schnittstelle in Lichtimpulse und wieder zurück umgewandelt; als Lichtquelle kann ein Injektionslaser (monomodale Faser) oder LEDs eingesetzt (multimodal), aufgefangen werden die Lichtimpulse durch Photodioden
- Eigenschaften:
  - Kosten: zur Zeit noch sehr teuer, ebenso wie das nötige Zubehör
  - Installation: sehr schwierig, es gilt auch kleinste Unterbrechungen, die das Signal brechen könnten zu vermeiden (an den Schnittstellen)
  - Kapazität der Bandbreite: sehr hoch, da Licht eine höhere Frequenz als Strom hat, 100 Mbps bis 2 Gbps; die Übertragungsrate ist abhängig von:
    * Zusammensetzung der Glasfaser
    * Modus
    * Wellenlänge/Frequenz des übertragenen Lichts

    Die Entfernung geht über mehrere Kilometer.
  - Knotenkapazität: in der Regel sind nur wenige Geräte eines Netzwerkes direkt mit Glasfaser miteinander verbunden; sie dienen als Backbones zwischen an sich langsameren LANs

  - Dämpfung: so gut wie keine Dämpfung, da kein elektrischer Strom fließt, dafür allerdings chromatische Streuung, d.h. Licht wird leicht reflektiert und in verschiedene Farben gebrochen (Datenverlust). Bei monomodalen Kabeln wird nur eine bestimmte Lichtfrequenz transportiert, daher keine chromatische Streuung, d.h. diese Kabel sind für sehr große Strecken geeignet
  - EMV: es fließt kein Strom, daher sind Glasfaserkabel immun gegen elektromagnetische Störungen und gegen Abhörmaßnahmen

3.2.2 Drahtlose Medien

Es gibt drei Medien:

- Funkwellen
  - Frequenzen zwischen 10 kHz und 1 GHz (Funk-/Radiofrequenz)
  - Arten:
    * Kurzwelle - Funkverkehr, Radio
    * Mittelwelle - Fernsehn, Radio
    * Ultrakurzwelle - Fernsehen, Radio
  - für die meisten Sendefrequenzen wird eine Sendelizenz benötigt
  - nicht-genehmigungspflichtige Sendefrequenzen sind stark eingeschränkt, Sendeleistung unter 1 Watt
  - Funkwellen können
    * omnidirektional, d.h. in alle Richtungen übertragen werden
    * oder direktional in eine Richtung
  - Arten von Antennen:
    * Funktürme (omnidirektional)
    * Halbwellen-Dipole
    * Wurfantennen
    * Strahler
  - zur Verwendung in Computernetzen gibt es folgende Einteilung:
    * niedrige Leistung, Einzelfrequenz, Reichweite von Einzelfrequenz-Receivern ca. 20 bis 30 m
    * hohe Leistung, Einzelfrequenz, vor allem für Fernverbindungen, auch über den Horizont hinaus, da die Atmosphäre das Funksignal reflektiert
    * Mehrfachfrequenz, es werden mehrere Frequenzen gleichzeitig benutzt
- Mikrowellen
  - es werden die niedrigen GHz-Frequenzen des elektromagnetischen Spektrums verwendet, daher großer Datendurchsatz und hohe Leistung

- Arten der Mikrowellenübertragung:
  - terrestrische Mikrowellensysteme: Parabolantennen werden zum Senden und Empfangen benutzt, es muß eine Sichtlinie zwischen den Kommunikationspartnern geben (z.B. zwischen zwei Gebäuden)
  - Satellitenübertragungssysteme: Mikrowellensignale werden zwischen ausgerichteten Parabolantennen übermittelt, als Zwischenvermittler dient ein Satellitensystem (Sichtlinie ist immer gewährleistet) in z.B. geostationärer Umlaufbahn (ca. 50.000 km); es kann allerdings zu Übertragungsverzögerungen zwischen 0,5 und 5 sek. kommen

- Infrarot
  - Infrarotlicht wird von LEDs ausgestrahlt und von Photozellen wieder aufgefangen
  - die Daten werden mit Wellen aus dem TeraHertz-Bereich übertragen
  - Infrarotsignale können keine festen Objekte durchdringen und werden von Lichtquellen abgeschwächt
  - die Übertragung erfolgt
    - über eine Sichtlinienverbindung
    - omnidirektional, d.h. das Licht wird nach allen Seiten ausgestrahlt und von Wänden und Decken reflektiert
  - Sichtlinienverbindungen erlauben höhere Übertragungsraten, omnidirektionale Verbindungen sind flexibler
  - Infrarotstrahlen lassen sich stark bündeln und auf ein Ziel richten (bis zu mehreren tausend m Entferung mit Laser)
  - Infrarotverbindungen sind nicht genehmigungspflichtig
  - durch die PPP-Verbindung sind sie relativ abhörsicher

3.3 Netzwerk-Karten

- Netzwerk-Karten - NICs - Network Interface Cards
- sie stellen die physikalische Verbindung eines Rechners mit dem Netzwerk her
- Anwendungsporgramme kommunizieren über Netzwerkkarten-Treiber mit den Netzwerkkarten bzw. mit dem Netzwerk
- Arbeitsweise einer Netzwerk-Karte:
  - die Daten werden in einen Puffer geschrieben
  - ein Chip berechnet für die gepufferten Daten eine Prüfsumme und fügt Adressierungsdaten hinzu -> dies wird nun als Frame bezeichnet

  - die Hardware-Adresse der Karte wird schon vom Hersteller vergeben und ist weltweit eindeutig
  - in einem Ethernet überwacht die Karte das Netzwerk und wartet, bis sie die Daten übertragen kann
  - die Umwandelung der Daten in ein Form, die über das gewählte Medium transportiert werden kann, nennt man Transceiver

4 Netzwerkprotokolle

4.1 Begriff und Überblick

4.2 ISO/OSI-Referenzmodell

- ISO - Internationale Standardisierungs-Organisation
- OSI - Open Systems Interconnection
- Computer benötigen feste Regeln, die vorschreiben, wie sie miteinander zu kommunizieren haben unabhängig vom verwendeten Betriebssystem -> Protokolle
- Aufgabenbereiche:
  - gegenseitige Kommunikation
  - ein Gerät muß wissen, wann es Daten übertragen kann und wann nicht
  - korrekte Übertragung der Daten muß gewährleistet sein
  - Nutzung der physikalischen Übertragungsmedien
  - Aufrechterhaltung eines akzeptablen Datenflusses zwischen den Geräten
  - Übertragung der Bits über verschiedene Medien
- das OSI-Modell ist ein Denkmodell, daß die wechselseitigen Beziehungen und Prozesse zwischen verschiedenen Geräten eines Netzwerkes nachvollziehbar macht
- die eigentliche Arbeit wird von entsprechender Hard- und Software erledigt
- das OSI-Modell unterteilt die Kommunikationsaufgaben (Tasks) in kleinere Unteraufgaben (Subtasks)
- die verwendeten Protokolle beziehen sich auf diese Subtasks
- eine Gruppierung von Protokollen, um eine komplette Kommunikationsaufgabe durchzuführen, nennt man Protokoll-Stack
  - Gruppe oder Reihe von Protokollen, die als Teil eines Tasks übereinandergelagert worden sind
  - zu jeder Schicht des OSI-Modells gehören unterschiedliche Protokolle

- jede Schicht im Protokollstack empfängt Dienste von der darunterliegenden Schicht und versorgt die darüberliegende Schicht ebenfalls mit Diensten
- auf zwei Computern, die miteinander kommunizieren wollen, müssen die selben Protokollstacks laufen, da jede Schicht des Stacks des einen Computers mit der entsprechenden Schicht des Stacks des anderen Computers kommuniziert
- jede Schicht bis auf die unterste fügt einer zu sendenden Nachricht einen Header hinzu, beim empfangenden Computer entnimmt jede Schicht den ihr zugehörigen Header

Es werden sieben Schichten unterschieden, die im nachfolgenden näher betrachtet werden:

1. Bitübertragungschicht - Physical Layer
2. Sicherungsschicht - Data Link Layer
3. Vermittlungsschicht - Network Layer
4. Transportschicht - Transport Layer
5. Kommunikationssteuerungsschicht - Session Layer
6. Darstellungsschicht - Presentation Layer
7. Anwendungsschicht - Application Layer

4.2.1 Schicht 1: Physikalische Schicht

- der physical layer ist für das Verschicken der Bits von einem Rechner auf den anderen verantwortlich, also die physikalische Verbindung zum Netzwerk zum Senden/Empfangen von Daten
- die physikalische Schicht erledigt folgende Aufgaben:
  - Anpassung an die Arten der Netzwerkverbindung
  - Umwandelung analoger Signale in digitale und umgekehrt
  - Bit-Synchronisation
  - bestimmt, welche Methoden zur Nutzung der Bandbreite verwendet wird (Basis- oder Breitband)

4.2.2 Schicht 2: Verbindungsschicht

- der data link layer gewährleistet den Datenfluß, der über eine Verbindung von einem Gerät zum anderen geht
- Datenpakete werden von der Netzwerkschicht übernommen und in Datenrahmen (Frames) verpackt

- es werden Kontrollinformationen hinzugefügt, z.B.
  - Frame-Typ
  - Routing-Informationen
  - Informationen über die Datenteilung
- außerdem wird eine zyklische Redundanzprüfung vorgenommen (CRC - Cyclic Redundancy Check)
- die Verbindungsschicht wird in zwei weitere Schichten unterteilt:
  - Media Access Control, MAC
  - Logical Link Control, LLC

4.2.3 Schicht 3: Netzwerkschicht

- der network layer kümmert sich um den Weg von einer Adresse zu anderen (Routing)
- entweder über direkte Kommunikation zwischen zwei Geräten oder in großen Netzwerken über ein Zwischensystem (intermediate system)
- die Netzwerkschicht übersetzt logische Netzwerkadressen in physikalische
- diese Schicht legt auch die Priorität einer Nachricht fest (Qualität)
- Zwischensystem, die nur Routing- und Verbindungsaufgaben haben und keine Umgebung für ausführbare Programme bereitstellen, führen nur die beiden ersten Schichten des OSI-Modells aus (von unten her gesehen)
- Router und Gateway arbeiten auf der Netzwerkschicht
- die Netzwerkschicht dient der Unterstützung logische getrennter Netzwerke
- Aufgabe:
  - Adressierung
  - Spannungs-, Nachrichten- und Datenpaketeaustausch
  - Streckenfindung und -auswahl
  - Verbindungsdienste
    - Steuerung des Datenflusses
    - Steuerung der Fehlerkontrolle
    - Datenpaketfolge
  - Gateway-Dienste

4.2.4 Schicht 4: Transportschicht

- der transport layer sorgt dafür, daß Datenpakete fehlerfrei, in Folge und ohne Datenveluste oder Duplikaten übertragen werden
- Nachrichten von der Kommunikationsschicht werden in kleinere Datenpakete verpackt zum versenden oder umgekehrt
- die Transportschicht sendet normalerweise eine Eingangsbestätigung für die empfangenen Nachrichten an den Absender-Computer

4.2.5 Schicht 5: Kommunikationsschicht

- Aufgabe des session layers ist es, Anwendungen, die auf unterschiedlichen Computern laufen, innerhalb einer Verbindung (Sitzung, Session) miteinander arbeiten zu lassen
- es werden weitere Dienste angeboten, z.B. damit zwei Programme sich finden und eine Kommunikationsverbindung aufbauen können, sowie die Datensynchronisation und Kontrollpunktvergabe
- außerdem steuert diese Schicht den Dialog zwischen zwei Prozessen und entscheidet, wann wer übertragen und empfangen darf

4.2.6 Schicht 6: Darstellungsschicht

- der presentation layer übersetzt Daten aus den Formaten, die das Netzwerk benötigt, in die Formate, die der Computer braucht und umgekehrt
- Aufgaben:
  - Konvertierung von Protokollen
  - Datenübersetung
  - Datenkompression und -verschlüsselung
  - Zeichensatzumwandelung
  - Interpretation grafischer Befehle
- der Netzwerk-Redirector arbeitet ebenfalls in dieser Schicht und hat folgende Aufgaben:
  - sorgt dafür, daß Dateien, die sich auf einem Datei-Server befinden, für Client-Computer sichtbar sind
  - bindet Netzwerkdrucker so ein, als wären sie lokal vorhanden

4.2.7 Schicht 7: Anwendungsschicht

- der application layer bietet Dienste, die Anwendungsprogramme direkt unterstützen, wie z.B.
  - Datenbankzugriff
  - Email
  - Dateiübertragung
- Anwendungsprogramme können so auf mehreren Rechnern verteilt arbeiten, als wären sie lokal auf einem Rechner installiert

4.3 IEEE-802

- IEEE - Institute for Electrical and Electronic Engineers, Ingenieurs-Vereinigung, USA
- IEEE-802 - Festlegung bestimmter LAN-Standards, seit Februar 1980 (02 - 80 -> 802)
- IEEE-802 legt Netzwerkaspekte in Bezug auf die unteren drei ISO/OSI-Schichten fest
- IEEE-802 und das OSI-Modell wurden gleichzeitig und in Zusammenarbeit entwickelt, sie haben viele Gemeinsamkeiten und harmonisieren gut

4.4 Protokoll-Stacks

In modernen Netzwerken werden unterschiedliche Protokoll-Stacks eingesetzt. Gebräuchlich sind:

- ISO/OSI Protokoll-Suite
- IBM Systems Network Architecture (SNA)
- Digital DECNet
- Novell Netware
- Apple AppleTalk
- Internet-Protokoll-Suite TCP/IP

In Netzwerken werden Datenpakete gesendet und empfangen. Für die Zusammenstellung und die Interpretation (auspacken) sowie die Änderung der Pakete sind die Netzwerkprotokolle notwendig. Sie bewegen die Datenpakete quasi auf dem Protokollstack rauf und runter. Datenpakete haben folgende Komponenten:

- Quell-Adresse
- Ziel-Adresse
- Anweisungen zum Weiterleiten der Daten
- Informationen zum Zusammenfügen der Daten
- die eigentlichen Daten, die übertragen werden sollen
- Informationen für die Fehlerprüfung

Die Komponenten werden in drei Teilen zusammengefaßt:

- Header
  - Alarmsignal (zeigt an, daß Daten übertragen werden)
  - Quell- und Ziel-Adresse
  - Zeitinformationen zur Synchronisation
- Daten (die größe der Daten liegt üblicherweise zwischen 48 Bytes und 4 KBytes)
- Trailer (meist CRC)

Jede Schicht des OSI-Modells fügt dem Datenpaket Informationen hinzu, die für die entsprechende Schicht des anderen Computers gedacht sind. Um Informationen von einem LAN zu einem anderen, eventuell über mehrere Pfade (Zwischensysteme) herzustellen, müssen routing-fähige Protokolle eingesetzt werden.

Um einen Protokoll-Stack mit dem Treiber der Netzwerk-Karte zu verbinden, wird ein besonderer Verbindungsprozeß notwendig (binding process). Es lassen sich auch mehrere Protokolle mit der gleichen Netzwerk-Karte verbinden, außerdem kann ein Protokoll an mehrere Netzwerk-Karten gebunden werden.

Eine grobe Einteilung der Netzwerk-Protokolle:

- Netzwerkprotokolle (OSI-Schicht 1-3)
- Transportprotokolle (OSI-Schicht 3, 4)
- Anwendungsprotokolle (OSI-Schicht 5-7)

Die Netzwerkprodukte von Microsoft (666) werden mit mehreren Netzwerkprotokollen ausgeliefert:

- NetBEUI für kleine Netzwerke mit einem Server
- NWLink für mittelgroße Netze bzw. Netze mit Zugriff auf die Novell NetWare-Welt
- TCP/IP für weltumspannende Netze
- DLC für SNA-Mainframes von IBM oder zu älteren HP-Druckern

4.5 NetBIOS

- Network Basic Output System, IBM
- NetBIOS nutzt NetBEUI auf der Transportschicht und reicht über die Schichten 3 - 5
- alternativ kann NetBIOS als anwendungsorientiertes Protokoll der Schicht 5 auf andere Transportprotokolle aufsetzen (SPX/IPX, TCP/IP)

4.6 NetBEUI

- NetBIOS Extended User Interface
- NetBEUI wurde für den Datenaustausch von 2 bis 200 Computern entwickelt, daher ist es auf kleine LANs beschränkt
- es kann nicht für den Datenaustausch zwischen zwei Netzwerken eingesetzt werden
- NetBEUI 3.0 ist das Microsoft-Update von IBMs NetBEUI und ist in Windows NT enthalten
- es erstreckt sich über die OSI-Schichten 3 und 4 und setzt die Schicht 5 greift es auf NetBIOS zurück
- Vorteile:
  - hohe Geschwindigkeit in kleinen Netzen
  - Verwaltung von mehr als 254 Sitzungen
  - hohe Leistung bei langsamen seriellen Verbindungen
  - einfache Einrichtung
  - automatische Tuning-Funktion
  - guter Schutz vor Fehlern
  - geringer Speicherbedarf
- Nachteile:
  - kein Routing zwischen Netzwerken
  - sehr wenig Software-Tools
  - keine Unterstützung für andere Plattformen

4.7 NWLink

- Kleinweich Umsetzung von Novells IPX/SPX-Stack (Novell Netware)
  - IPX - Internetwork Packet Exchange
  - SPX - Sequenced Packet Exchange
- NWLink ist IPX für Windows NT, wobei IPX das Protokoll und NWLink die Netzwerkkomponente ist, die das Protokoll zur Verfügung stellt.
- es erleichtert die Migration zwischen Plattformen, da man nun mit NetWare-Servern kommunizieren kann.
- NWLink enthält außerdem Verbesserungen gegenüber der Programmierschnittstelle von Novells Version von NetBIOS. Daher kann Windows NT sowohl als Client als auch als Server in Novells IPX/NetBIOS Client-Server-Anwendungen eingesetzt werden.
- Vorteile:
  - leichtes Setup
  - Routing zwischen Netzwerken möglich
  - höhere Geschwindigkeit als TCP/IP (unter Win NT)
  - gute NetWare-Unterstützung (erleichtert die Migration)
- Nachteile:
  - kein zentrales IPX-Adressierungsschema (keine zentrale Netzwerknumerierung) macht es bei großen Netzwerken nicht mehr einsetzbar
  - langsame serielle Verbindungen sind langsamer als bei NetBEUI
  - keine Unterstützung von Standardprotokollen für die Systemverwaltung
  - keine große Toolauswahl wie bei TCP/IP

4.8 TCP/IP

- TCP/IP soll die Kommunikation zwischen einer Reihe unterschiedlicher Rechnersysteme mittels eines Standardprotokolls gewährleisten
- die Protokoll-Suite enthält Regeln
  - für den Kommunikationsauf- und abbau innerhalb eines Netzes
  - für die Kommunikation in unterschiedlichen Netzen, die miteinander verbunden sind
- auf der Basis einer TCP/IP-Verbindung können dann weitere Protokolle aufsetzen

4.8.1 Entstehung

- die Entwicklung von TCP/IP ist eng mit der Entstehung des Internets verbunden und mit UNIX-Betriebssystemen
- Mitte der 70er Jahre begann TCP/IP als Experimentalprojekt des amerikanischen Verteidigungsministeriums (Departement of Defense, DoD, Projektgruppe ARPA)
- Ziel war die Entwicklung eines herstellerunabhängigen Standards für die Kommunikation zwischen Computersystemen und wird heute von allen gängigen Plattformen unterstützt
- TCP/IP ist mittlerweile ein Standardprotokoll
- TCP/IP arbeitet zur Zeit noch mit 32 Bit Adreßraum (IPv4), wird aber bald erweitert (IPv6)

4.8.2 DoD-4-Schichten-Modell

TCP/IP wurde vor dem OSI-Modell entwickelt, hält sich aber trotzdem daran. Es existiert jedoch ein eigenes Modell, das DoD-4-Schichten-Modell:

- Host-to-Host-Layer
  - TCP - Transmission Control Protocol, Protokoll für eine gesicherte Verbindung zwischen zwei Systemen
    Die Sicherung besteht in der Bestätigung für empfangene Nachrichten. Fehlt diese Bestätigung nach einer gewissen Zeit, wird das Paket erneut gesendet. Die TCP-Kommunikation stellt eine logische Verbindung zwischen zwei Systemen her. Es können auch mehrere Verbindungen gleichzeitig hergestellt werden, da diese über verschiedene Port-Adressen laufen
  - UDP - User Datagram Protocol, ungesicherter, verbindungsloser Dienst, daher hat er weniger Overhead als TCP
- Internet-Layer
  - IP - Internet Protocol, übernimmt die Daten aus einer oberen Ebene und versendet diese über das Netzwerk, Hauptaufgabe ist dabei das Routing
  - ICMP - Internet Control Message Protocol, Austausch von Service-Meldungen (ping, traceroute)
  - ARP - Address Resolution Protocol, übersetzt IP-Adressen in (Hardware-) MAC-Adressen mit Hilfe einer Tabelle
  - RARP - Reverse ARP, übersetzt Hardware-Adressen in IP-Adressen (bei Microsoft DHCP)
- Network Access Layer

Class	Network-Anteil	Host-Anteil
A	1	3
B	2	2
C	1	3

- bei Verwendung bestimmter Netzwerk-System (z.B. Ehternet oder Toter Ring) wird eventuell die Verwendung einer bestimmten Protokollvariante vorgeschrieben (z.B. Ethernet II oder Ehternet SNAP)
- PPP/SLIP - Point-to-Point-Protocol / Serial-Line-Internet-Protocol, wird immer dann genutzt, wenn anstatt LAN-Leitung analoge (z.B. Telefonleitungen) genutzt werden

4.8.3 Adressen und TCP/IP

- MAC-Adresse oder Hardware-Adresse (Media Access Control), eine weltweit eindeutige Adresse der Netzwerkkarte; Modems etwa kommunizieren direkt auf IP-Ebene
- IP-Adresse, Software-Adresse, die aus vier Bytes gebildet wird und eindeutig sein muß, sobald ein Netzwerk an einem anderen (z.B. dem Internet) hängt
- Port-Adresse, Aufgabe ist die Trennung einzelner TCP-Verbindungen voneinander, außerdem können gezielt Verbindungen auf einem anderen Host aufgebaut werden; bestimmte Dienste haben fest zugeordnete Ports (well-known-ports zwischen 1 und 255)

4.8.4 Network und Host

- IP-Adressen werden in einen Netzwerkanteil und einen Hostanteil an den Bytegrenzen aufgeteilt
- der Host-Anteil bezeichnet einen einzelnen Rechner in einem bestimmten Netzwerk
- der Netzwerkanteil wird auch als Domain bezeichnet
- pro Anteil muß mindestens immer ein Byte verwendet werden

4.8.5 Subnet-Mask

- kleinstes Netz (Class C) hat maximal 255 Hosts. Der Host-Anteil kann netzintern weiter aufgeteilt werden mit Hilfe der Subnet-Mask -> Subclassing
- die Subnet-Mask muß auf allen Rechnern des Netzes gleich eingestellt sein

4.8.6 Domain Name Service

- IP-Adressen sind unhandlich, deshalb werden Namen vergeben (Kommunikation Mensch - Maschine)
- da Rechner intern nur mit IP-Adressen arbeiten, müssen entsprechende Übersetzungsmechanismen bereitgestellt werden
  - DNS
    - Domain Name Service
    - für jede Domaine wird ein Rechner konfiguriert, der auf Anforderung die Adressen in Namen umsetzt und umgekehrt mit Hilfe einer Datenbank, in denen alle Rechner registriert sind
    - jedes Netzwerk hat eine primary und einen secondary DNS
  - Konfigurationsdateien
    - für die Konfiguration von TCP/IP auf einem Rechner gibt es vier Dateien, deren Aufbau bei allen Systemen gleich ist (hosts, networks, services, protocol) und die reine ASCII-Dateien sind
    - unter Linux finden sich diese Dateien in /etc

4.8.7 Struktur von Domain-Namen

- Domain-Namen bezeichnen einen Abschnitt in einem Netzwerk
- DNS-Server sind für die Namensauflösung innerhalb einer Domain zuständig
- ist ein Netz mit dem Internet verbunden, so werden auch die DNS-Server in die globale DNS-Struktur eingereiht
- die Struktur ähnelt einem Dateiverzeichnis:
  - an der Spitze befindet sich die Root-Domain
  - direkt unterhalb sind die Top-Level-Domains
  - die wiederum auf einzelne Domämen verweisen
- mißlingt eine Namensauflösung, wird sie an einen höher liegenden DNS-Server delegiert

Top-Level-Domains gibt es in zwei Arten:

- geografische Domänen: jeder Staat der Erde hat seine eigen Domain
- organisatorische Domänen: sie beschreiben innerhalb der USA eine Zugehörigkeit zu verschiedenen Organisationen

Da jeder Domain-Name eindeutig sein muß, werden diese zentral verwaltet in sogenannten NICs (Network Information Center). In den meisten Länder gibt es eine Filiale, wo man sich einen Namen registrieren lassen kann. Wurde eine Domain registriert, so übernimmt eine verantwortliche Person die Einteilung in Sub-Domänen.

Der Name für einen Rechner bzw. eine Domain wird aus der hierarchischen Struktur abgeleitet:

- der Name der Top-Level-Domain steht ganz rechts
- durch Punkte getrennt folgen die Namen der untergeordneten Sub-Domänen
- ganz links folgt der Name des Rechners

4.8.8 DHCP

- ab einer gewissen Menge wird es schwierig, den Überblick zu behalten
- das DHCP-Protokoll (dynamic host configuration protocol) ermöglicht einem Host, beim Start des TCP/IP zuerst nach einer freien Adresse zu fragen
- dazu verwaltet ein Server eine Liste mit einem IP-Adressenpool und teilt diese auf Anforderung zu
- die Adresse des DNS-Servers muß allerdings auf jeder Station konfiguriert werden

4.8.9 Vorteile TCP/IP

- weitreichende Verbindungsmöglichkeiten, d.h. Plattformunabhängigkeit (horizontal und vertikal)
- direkter Zugriff auf das Internet
- leistungsstarkes Routing
- SNMP - Simple Network Management Protocol
- DHCP
- WINS - Windows Internet Name Service
- Unterstützung für die meisten Internet-Protokolle (POP3, HTTP, ...)
- zentrale Zuweisung von TCP/IP-Domänen, was die Verbindung mit Netzwerken anderer Unternehmen erlaubt

4.8.10 Nachteile TCP/IP

- zentrale Zuweisung von Domänen verursacht Verwaltungsaufwand und Kosten
- mitlerweile ist die Verfügbarkeit einzigartiger Domänen-Nummer stark eingeschränkt
- relativ großer Overhead
- langsamere Geschwindigkeit als NWLink und NetBEUI

4.9 Exkurs: Adressierung in Netzen

4.9.1 Internet Protocol, Version 4 (IPv4)

- die 32bittige Adresse wird in 4 Oktette eingeteilt
- ein Nameserver verwaltet mit Hilfe einer Datenbank die Domain-Namen und wandelt sie bei Bedarf in eine IP-Adresse um
- die IP-Adresse besteht aus einer netid und einer hostid
- eine Unterteilung erfolgt in Adreßklassen:
  - Class-A-Adressen
    * das erste Oktett bildet die Netzwerkadresse
    * Class-A-Adressen beginnen mit einer 0 (Null) im ersten Oktett (Netzwerkanteil)
    * die restlichen drei Oktette bilden den Hostanteil
    * es können 2^7 Netze und 2^{24} Hosts adressiert werden, also 128 Netze mit maximal 16.777.216 - 2 Hosts
    * steht in allen Bits eine 1, so wird diese Adresse als Broadcast-Adresse für Nachrichten ins eigene Netz verwendet
    * für Adressen ist der Adreßraum 1.0.0.0 bis 126.255.255.255 reserviert
    * 127.0.0.0 ist für das Loopback-Device vergesehen
  - Class-B-Adressen
    * die ersten beiden Oktette bilden die Netzadresse
    * Class-B-Adressen beginnen mit 10 im ersten Oktett, die restlichen 14 bilden die Netzadresse
    * die letzten zwei Oktette bilden den Hostanteil
    * es können 2^{14} Netze mit 2^{16} Hosts adressiert werden, also 16.384 Netze und 65.536 - 2 Hosts
    * für Adressen ist der Adreßraum 128.0.0.0 bis 191.255.255.255 reserviert
  - Class-C-Adressen
    * die ersten drei Oktette bilden die Netzadresse

        * Class-C-Adressen beginnen mit 11 im ersten Oktett, die restlichen 22 Bits kennzeichnen die Netzadresse
        * Oktett 4 bildet die Hostadresse
        * es können 2^{21} Netze mit 2^8 Hosts adressiert werden, d.h. 2.097.152 Netze mit 256 - 2 Hosts
        * für Adressen ist der Adreßraum 192.0.0.0 bis 223.255.255.255 reserviert
    - Class-D: wird zur Adressierung einer Gruppe von Hosts verwendet
    - Class-E: ist für zukünftige Erweiterungen reserviert

- Class-A-Adressen werden mittlerweile so gut wie nicht mehr vergeben, Class-B-Adressen sind auch rar

4.9.2 Internet Protocol, Version 6 (IPv6)

- durch die neue Adreßstruktur mit 128-Bit-Adressen ist es zu einer Erweiterung des Adreßraumes gekommen, Anzahl möglicher Adressen: $3,402823 * 10^{38}$
- hinzugekommen sind außerdem zusätzliche Funktionen für Multimedia und Sicherheit
- eine Adresse gemäß IPv6 baut sich aus acht durch Doppelpunkt getrennte Hexadezimalziffer-Tetraden auf
- Adressen nach IPv4 können in IPv6 abgebildet werden, indem die letzten 32 Bit die alte Adresse enthalten und alle anderen Bits auf Null gesetzt werden (kann durch zwei Doppelpunkte vereinfacht dargestellt werden)
- anstelle von Knoten werden nun Schnittstellen definiert:
    - Unicast: eine einzelne Schnittstelle
    - Anycast: Set von Schnittstellen, wobei Datenpakete immer an der Schnittstelle abgeliefert werden, die der Quelle am nächsten ist
    - Multicast: Set von Schnittstellen, ein Datenpaket wird an alle weitergereicht
- die Art der Adresse wird durch ein Präfix, das durch die führenden Bits einer Adresse gebildet wird, angezeigt
- die Vergabe von Adressen wird vereinfacht, da z.B. die geografische Lage eines Netzwerkes berücksichtigt werden kann (optimiertes Routing)

5 Netzwerkpraxis

5.1 Einführung

Die Informationen aus dem c't-Artikel sind im nächsten Kapitel mit aufgeführt.

5.1.1 Rahmenformate

- ein Datenrahmen im DIX-Ethernet (Digital, Intel, Xerox), der Urform des Ethernets, ist folgendermaßen aufgebaut:
  - Preamble, Vorspann, 8 Bytes
  - Destination, Ziel, 6 Bytes
  - Source, Ursprung, 6 Bytes
  - Protocol, Protokoll, 2 Bytes
  - Data, Daten (Nutzdaten), n Bytes
  - FCS, Prüfsumme, 4 Bytes
- ein Datenrahmen nach IEEE 802.3 (MAC-Rahmenformat) hat folgenden Aufbau:
  - Preamble, 8 Bytes
  - SFD, Rahmenanfang, 1 Byte
  - Destination, 6 Bytes
  - Source, 6 Bytes
  - Length, Länge, 2 Bytes
  - Logical Link Control
    - DSAP, 1 Byte
    - SSAP, 1 Byte
    - CTL, 1 (2) Byte, alle drei gehören zur Schicht-2-Steuerung
    - Data and PAD Field, Datenfeld, Füllbytes, n Bytes
  - FCS, 4 Bytes

Die Felder haben unterschiedliche Funktionen:

Preamble: wird vom Empfänger zur Synchronisation genutzt

SFD: das Feld kennzeichnet den Rahmenbeginn

Destination: Zieladresse

Source: Ursprungsadresse

Protocol: verwendetes Protokoll

Length: Anzahl der Oktette im LLC-Feld (Logical Link Control)

DSAP: Destination Service Access Point

SSAP: Source Service Access Point

CTL: Control-Feld

FCS: Frame Check Sequence, enthält das Ergebnis der CRC-Prüfung

Die maximale Rahmenlänge eines 802.3-LANs beträgt 1.518 Oktette, die minimale Rahmenlänge beträgt 64 Oktette. Wird die minimale Rahmenlänge nicht erreicht, wird ein Feld mit *PAD-Bytes* aufgefüllt (wird später noch erklärt).

5.1.2 Segmentierung

- Übertragen viele Geräte in einem Netzwerk Daten, kommt es zu Datenkollisionen, das Netzwerk verstopft und die Gesamtleistung läßt merklich nach. Es kann sogar zu mehr Kollisionen als tatsächlichen Übertragungen kommen.
- Dies kommt daher, daß sich viele Geräte ein Medium teilen.
- Durch die *Segmentierung* wird ein großes Ethernet in zwei oder mehrere Teilstücke (Segmente) unterteilt, die über Bridges oder Router miteinander verbunden werden.
- Bridges und Router übertragen nur Daten in andere Segmente, wenn dies wirklich nötig ist.

5.1.3 Twisted-Pair Spezifikationen

Kategorie	Linkklasse	max. Frequenz	Beispiele
1	A	100 KHz	ISDN-Basisanschluss
2	B	1 MHz	ISDN-Primärmultiplexanschluss
3	C	16 MHz	10BaseT, Token Ring
4	-	20 MHz	16 MBit Token Ring
5	D	100 MHz	100 MBit Ethernet, CDDI
6	E	200 MHz	155 MBit-ATM
7	F	66 MHz	622 MBit-ATM, Gigabit Ethernet

Diese Normen entstanden Dank Mithilfe folgender fröhlicher Organisationen:

EIA: Electronic Industry Association

TIA: Telecommunication Industry Association

IEC: International Electronical Commission

Außerdem gibt es noch viele bunte europäische und volksdeutsche Normen, deren Nummern sich keine (M)Sau merken kann.

Die Linkklassen enthalten Angaben über:

- Kabelmerkmale

- Wanddose
- Patchfelder
- Anschlußdose

Die Linkklassen sind abwärtskompatibel.

5.2 Ethernet

5.2.1 10 Mbps-Ethernet

Zur Geschichte:

- Entwicklung in den 60ern an der Uni Hawai (ALOHA-Projekt) als Paketfunk-Netz mit CSMA/CD-Protokoll
- als Grundlage für die *IEEE 802.3-Norm* benutzten die Firmen Digital, Intel und Xerox (DIX) eine Spezifikation, die im Xerox PARC weiterentwickelt wurde (erstes richtiges Ethernet)

Um einen reibungslosen Datenverkehr in einem Ethernet zu gewährleisten, muß sichergestellt werden, daß immer nur ein Rechner das Netz benutzen kann und es nicht zu *Kollisionen* kommt. Dies wird durch das *CSMA/CD-Verfahren* (Carrier Sense Multiple Access with Collision Detection, ein *Medienzugriffsverfahren*) gewährleistet.

- jeder Rechner im Netz verschickt Datenpakete
- kommt es zu einer Kollision der Datenpakete, hören alle Rechner, die gerade am senden sind, damit auf und versuchen es nach einer gewissen Zeit wieder
- somit kämpfen die Rechner um die Datenübertragung, weshalb das ganze auch als *contentionbased system* bezeichnet wird

Ethernet arbeitet mit einer maximalen Übertragungsrate von *10 Mbps*, die praktisch nicht erreicht wird (realistisch sind *1 bis 4 Mbps*). Ethernet unterstützt verschiedene Kabeltypen, weshalb man von *Verkabelungssystemem* spricht. Folgende haben sich durchgesetzt:

1. Thicknet-Ethernet, 10Base5
   - als Kabel werden RG-8 oder RG-11 Koaxkabel verwendet, auch *Yellow Cable* genannt, 50 Ohm
   - mit Hilfe von Krokodilklemmen werden *Transceiver* an den Hauptbus angeklemmt
   - über ein AUI-Kabel (attachement universal interface) wird der Transceiver mit einem DIX-Stecker (Digital, Intel, Xerox) an die Netzwerkkarte angeschlossen
   - der Hauptbus muß an beiden Enden terminiert sein

- Spezifikationen:
  - maximale Segmentlänge 500 m
  - maximale Anzahl Anschlüsse 100 [1]
  - maximal 5 Segmente
  - maximal 4 Repeater[2]
  - maximal 3 Segmente mit Knoten
  - mindesten 2,5 m Abstand zwischen den Anschlüssen
  - maximale Länge mit Repeatern: 2.500 m
  - maximale Länge Hauptbus - Stationen: 50 m (das sogenannte AUI-Drop-Kabel)
- im Thicknet gilt die *5:4:3-Regel*, d.h. es gibt
  - 5 Segmente,
  - die durch 4 Repeater verbunden sind,
  - wobei an 3 Segmenten Stationen angeschlossen sind

  So ergibt sich eine maximale Länge von 2.500 m.
- als Nachteile sind die hohen Kosten und die umständliche Verkabelung durch das starre Koaxkabel zu nennen

2. Thinnet-Ethernet, 10Base2

- hier werden als Kabel ein dünneres Koaxkabel verwendet (ähnlich Fernseh-antennenkabel, RG-59), RG-58A/U, RG-58C/U, jeweils 50 Ohm; RG-58A/U (Kupferkern als Litze ausgeführt) wird am häufigsten verwendet
- um einen Rechner an den Bus anzuschließen, werden *T-Stücke* verwendet, der Anschluß an der Netzwerkkarte ist ein *BNC-Anschluß*
- der Bus muß immer noch an jedem Ende terminiert werden
- der Transceiver ist nun Teil der Netzwerkkarte
- Spezifikationen:
  - maximale Segmentlänge: 185 m
  - maximal 5 Segmente
  - maximal 4 Repeater
  - maximal 3 Segmente mit Knoten
  - maximal 30 Geräte pro Segment
  - maximale Gesamtlänge mit Repeatern 925 m

[1] pro Segment???

[2] sobald Repeater in einem Ethernet benutzt werden, dürfen diese keine eigenen Signale wie SQE (Signal Quality Error) oder einen Heart Beat versenden, da es ansonsten zu Kollisionen kommt

- Nachteile sind die immer noch hohen Kabelkosten, da man mehr Kabel braucht, um den Bus direkt an die Stationen zu legen, als bei Thicknet; auch die Störanfälligkeit steigt, da nun ein ganzes Segment bzw. Netzwerk bei Kabeldefekten an Knoten ausfallen kann.
- Daher wird oft Thicknet und Thinnet kombiniert verwendet. Thicknet dient für Backbone-Aufgaben und Thinnet für die Verkabelung zwischen den Stationen

3. Twisted-Pair-Ethernet, 10BaseT

   - anstatt Koaxkabeln werden nicht abgeschirmte Zweidrahtleiter (UTP) verwendet (Twisted-Pair-Kabel, Kategorie 3), welches oft in Telefonanlagen eingesetzt wurde
   - die Verkabelung erfolgt mit Hilfe von Hubs in Sternform, obwohl es logisch als Bus aufgebaut ist
   - dadurch können Fehler in einem Segment (jeder Knoten hat sein eigenes) sich nicht auf andere Segmente bzw. das gesamte Netzwerk ausdehnen; fehlerhafte Geräte können durch Entfernen des Kabels vom Hub vom Netz getrennt werden, ohne dieses zu stören
   - intelligente bzw. aktive Hubs besitzen Verwaltungsfunktionen und können fernbedient werden, z.B. um Geräte abzuklemmen
   - als Stecker werden normalerweise RJ-45-Stecker verwendet, alternativ kann auch ein Transceiver mit DIX-Buchse oder AUI-Stecker, oder eine Twisted-Pair-Access Unit (TPAU) eingesetzt werden
   - Spezifikationen:
     - maximal 1024 Segmente
     - maximal 1024 Segmente mit Knoten
     - maximale Länge eines Segmentes 100 m
     - pro Segment maximal 2 Knoten
     - maximal 1024 Knoten pro Netzwerk
     - maximal 4 Hubs in einer Kette
   - UTP-Kabel sind wesentlich billiger als Koaxkabel und sind wesentlich flexibler; der UTP-Standard ist unter IEEE 802.3 festgelegt

4. 10BaseFL-Ethernet

   - die Signale werden über Glasfaserkabel übertragen
   - da 10BaseFL auf dem Broadcast-Prinzip beruht, wird ein Netzwerkhub benötigt, um die Lichtsignale zu verteilen und an alle Stationen weiterzuleiten; daher ist die Sternform zwingend erforderlich
   - der Hub kann passiv oder aktiv sein (Concentrator)

  - ein passiver Hub splittet die Signale optisch und leitet sie mit geringerer Intensität weiter; ein passiver Hub bietet auch keine Verwaltungs- und Fehlererkennungsfunktionen
  - ein aktiver Hub verstärkt und leitet das Signal elektronisch weiter, die Lichtintensität wird nicht beeinträchtigt
- Spezifikationen:
  - maximal 1024 Segmente
  - maximal 1024 Segment mit Knoten
  - maximale Länge eines Segmentes 2.000 m
  - maximal 2 Knoten pro Segment
  - maximal 1024 Knoten pro Netzwerk
  - maximal 4 Hubs in einer Kette
- Da 10BaseFL sehr große Entfernungen überbrücken kann, wird es oft für Backbone-Lösungen verwendet.

5.2.2 100 Mbps-Ethernet

Hier existieren zwei konkurrierende Standards:

1. 100VG-AnyLAN
   (oder 100BaseVG, VG, AnyLAN)

   - teilt sich Eigenschaften von Ethernet und Token Ring, z.B. die Unterstützung von Ethernet- und Token-Ring-Datenpakete
   - 100 Mbps DÜ-Rate mit Telefonqualität (VG = Voice Grade)
   - die Verkabelung erfolgt entweder über UTP-Kabel ab Kategorie 3 oder über Lichtwellenleiter
   - es verwendet eine Sterntopologie
   - der Hub regelt den Zugang und die Priorität des Datentransfers; hier wird kein CSMA/CD verwendet -> Demand Priority Access-Protokoll, dabei werden mindesten vier Adernpaare benötigt
   - die Hubs bieten eine große Datensicherheit, da sie aktive sind und z.B. adressierte Datenrahmen ausfiltern können

2. Fast Ethernet, 100BaseT

   - verwendet wie 10BaseT das CSMA/CD-Protokoll
   - es ist für unterschiedliche Medien spezifiziert:
     - 100BaseT4: vierpaariges UTP der Kategorie 3, 4, 5 oder STP
     - 100BaseTX: zweipaariges UTP der Kategorie 5 oder STP
     - 100BaseFX: zweifaseriges Glasfaserkabel

Typ, Faser	Wellenlänge	Segmentlänge	Kabeltyp
1000BaseSX	830 nm	220 m	multimodal
1000BaseSX	830 nm	275 m	multimodal
1000BaseSX	830 nm	500 m	multimodal
1000BaseSX	830 nm	550 m	multimodal
1000BaseLX	1.270 nm	550 m	multimodal
...	...	...	...
1000BaseLX	1.270 nm	5.000 m	monomodal
1000BaseCX	Impedanz: 150 Ohm	25 m	Kupfer, Twinax

Tabelle 1: in der IEEE-Norm 802.3z spezifizierte Kabeltypen

- 100BaseT verwendet einen sternförmig verkabelten Bus, ist also physisch Stern und logisch Bus
- 10BaseT wird unterstützt, es gelten die selben Vor- und Nachteile wie bei 10BaseT

5.2.3 1000 Mbps-Ethernet

- Gigabit-Ethernet ist für Kupferkabel (Twinax) und Glasfaserkabel ausgelegt, TP folgt im Jahr 2.000 (IEEE 802.3az)
- das S in der Bezeichnung steht für *short*, das L für *long*, und das C für *Kupfer*
- die Faserdicke der Glasfasern wird von oben nach unten hin immer dünner
- Gigabit-Ethernet kann mit allen anderen Ethernet-Standards verwendet werden, da die Zugriffsverfahren größtenteils gleich sind. Die Komponenten (vom GB-Ethernet) können zwischen 10, 100 und 1000 Mbps umschalten (*Autonegotiation*).
- Jeder Ethernet-Standard versendet die Daten in einem Format, dem verschiedene Informationen hinzugefügt werden. Die OSI-Schicht 2, der MAC-Layer, verpackt dazu die Daten in einen Rahmen (Frame) und die zusätzlichen Informationen in einen *Frame-Header*. Die Daten werden auch vom MAC-Layer wieder entpackt (auf der Empfänger-Station).
- Mit Hilfe des *Padding-Verfahrens* wird das Datenfeld eines Frames, das aus den Nutzdaten und Protokollinformationen der höheren OSI-Schichten besteht, auf die erforderliche Mindestgröße gebracht, falls es diese nicht schon erreicht hat. Die Mindestgröße beträgt 46 Byte, die maximale 1.500 Bytes. Die restlichen Informationen sind 18 Bytes groß (der Header).
- Längenproblematik: Damit die Erkennung einer Kollision von der sendenden Station überhaupt noch möglich ist, muß bei der Verwendung des CSMA/CD-Verfahrens auf die maximale Länge einer Ethernet-Strecke aufgepaßt

werden. Wird diese zu lang, braucht auch das Datenframe länger auf dem Weg durch das Netz, was zu Kollisionen führt, da andere Stationen laut Carrier Sense das Medium als frei betrachten und selber anfangen zu senden.

  - der Sender stellt die Überwachung von Kollisionen nach 576 Bit-Zeiten ein; dies setzt sich zusammen aus 512 Bit für ein minimales Datenpaket und einer Sperrzeit für die Kollisionserkennung von 64 Bit.
  - ist die Kabelstrecke zwischen den Stationen zu groß, registriert der Sender die Kollision zu spät und versendet das entsprechende Paket nicht neu (Backoff-Prozeß); das Paket ist unerkannt verschollen (*Late Collision*)
  - der Zeitraum, nach dem keine Kollisionen mehr auftreten dürfen, wird als *Slot Time* bezeichnet und beträgt 512 Bit-Zeiten (bei 10 und 100 Mbps-Ethernet)
  - die restliche *Sperrzeit* von 64 Bit dient der Verhinderung von Überschwingungen, die eine Kollisionserkennung unmöglich machen
  - damit sich das Signal einschwingen kann, wird eine 7 Byte große *Präambel* und ein 1 Byte großer *Start Frame Delimiter* vorausgeschickt, der den Paketanfang durch ein eindeutiges Bit-Muster kennzeichnet; die Präambel dient auch der Taktsynchronisation
  - die festgelegten 576 Bit-Zeiten (maximale Laufzeit eines Signals zwischen den am weitesten auseinanderliegenden Stationen eines LANs) werden auch als *Round Trip Delay, RTD* bezeichnet

- die Signale breiten sich in Kupfer- und Glasfasermedien mit einer Geschwindigkeit von 200.000km/s aus (keine Lichtgeschwindigkeit, da Dämpfung); daher gibt es folgende theoretische Werte zu lernen:

  - Ethernet mit 10Mbps, Bit-Dauer 0,1 μs, bis 2.000 m
  - Fast Ethernet mit 100Mbps, Bit-Dauer 0,01 μs[3], bis 200 m
  - Gigabit Ethernet mit 1.000 Mbps, Bit-Dauer 0,001 μs, bis 20 m ohne Zusatzstoffe

- um die maximale Ausdehnung von Gigabit-Ethernet zu erhöhen, wurde die Länge der Datenframes geändert

  - es wurde dafür gesorgt, daß jede Station mindestens so viele Bits sendet, die benötigt werden, um die weiteste Strecke zwischen zwei Stationen sicher zu überbrücken
  - dazu werden MAC-Frames (64bis 511 Byte) mit speziellen Symbolen auf eine Mindestlänge von 512 Byte verlängert (Extension)

[3] immer der Kehrwert der DÜ-Rate

- damit kann eine sendende Station Kollisionen erkennen; genauso wie alle anderen Stationen die mögliche Belegung des Netzes nun erkennen können

- die Verlängerung der MAC-Frames ist nur im *Halbduplexmodus* nötig, im *Vollduplexmodus* treten keine Kollisionen auf, da gleichzeitig gesendet und empfangen werden kann

- ein *Flow-Control-Verfahren* sorgt durch Steuerung der Größe des Datenflusses dafür, daß kein Datenstau entsteht; andere Teilnehmer regulieren ihren Datenfluß, bis ein reibungsloser Verkehr erreicht ist

- Gigabit-Ethernet arbeitet meistens mit Glasfaserkabeln oder Koaxkabelstrecken mit Repeatern (da Zweifachführung -> Quadaxkabel)

5.3 Token Ring

- Token Ring wurde von Big Blue entwickelt
- entspricht dem IEEE 802.5-Standard
- physikalisch ein Stern, logisch ein Ring
- die Workstations werden über Kabel mit dem Hub oder Ringverteiler (die alte MSAU) verbunden
- Bezeichnungen für den Token-Ring-Hub:
  - MAU, Media Attachement Unit, Multistation Access Unit
  - MSAU, Multistation Access Unit
  - Ringverteiler
- an jeder verdammten MSAU können bis zu acht kleine Workstationferkelchen ihre Milch ziehen (!!!geniales Wörterspielchen!!!)
- untereinander werden die MSAUs mit *Patch-Kabeln* verbunden; jede MSAU hat folgende Anschlüsse:
  - Ring In (RI)
  - Ring Out (RO)
- die Netzwerkkarten werden über ein Token-Ring-Kabel mit der MSAU verbunden
  - an einem Ende ist ein *9-Pin-Stecker*, der an die Netzwerkkarte kommt (D-Sub-Stecker)
  - am anderen Ende ist ein IBM-Datenstecker
- zu den Netzwerkkarten:

  - jede Token-Ring-Karte hat eine herstellerseitig festgelegte eindeutige Adresse, die eventuell mit Konfigurationssoftware geändert werden kann
  - jede Workstation kann höchstens zwei Karten aufnehmen, wovon eine primär und die andere sekundär ist
  - die Karten werden über DIP-Schalter konfiguriert
  - es gehen insgesamt vier Drähte an eine Karte
  - in einem Segment dürfen die Geschwindigkeiten nicht gemischt werden, also entweder 4 oder 16 Mbps

- bei der Verkabelung werden die Stationen mit einer MSAU und diese untereinander verbunden; zur Varkabelung gibt es IBM-Standardkabel:

  - Typ 1: STP-Kabel (zweipaariger Zweidrahtleiter), für Terminals und Schalttafeln
  - Typ 2: STP-Kabel, wie Typ 1, jedoch mit zusätzlich vier Zweidrahtleitern für Telefonverkehr
  - Typ 3: vierpaariges UTP-Kabel, sehr störanfällig
  - Typ 5: optisches Kabel, nur für den Hauptringpfad verwendbar
  - Typ 6: STP-Kabel, wird als Patch-Kabel oder Verlängerungskabel in Schaltschränken verwendet, für Kurzstrecken, zwei verdrillte Kupferdrähte mit Drahtfaserkern und Abschirmung, sehr biegsam
  - Typ 8: wie Typ-6-Kabel, zum Verlegen unter Teppichen
  - Typ 9: wie Typ 6, feuerresistent

- Spezifikationen von Token Ring:

  - verschiedene Kabeltypen nutzbar
  - maximal 33 MSAUs
  - maximal 260 Knoten
  - maximale Entfernung Knoten und MSAU:
    * UTP: 45,5 m
    * STP oder Glasfaser: bis 100m
  - maximale Länge des Patch-Kabels (zur Verbindung der MSAUs)
    * UTP: 45,5 m
    * STP: 200 m
    * Glasfaser: 1000 m
  - minimale Länge des Patch-Kabels: 2,5 m
  - maximale Länge aller Patch-Kabel:

    * UTP: 112,2 m
    * Glasfaser: mehrere Kilometer

- zur Arbeitsweise eines Token-Ring-Netzwerkes:
  - die Netzwerkkarten sind physikalisch in Form eines Rings an die MSAUs angeschlossen, arbeiten jedoch logisch in einem Ring
  - in diesem Ring kreist nun ein freier Token von 3 Bytes in einer Richtung
  - ein Knoten kennt folgende Stationen:
    * Nearest Active Upstream Neighbour, NAUN: nächster aktiver Nachbar im Netz (datenstromaufwärts), von diesem empfängt der Knoten solche Tokens
    * Nearest Active Downstream Neighbour: NADN: nächster aktier Nachbar im Netz (datenstromabwärts), an diesen werden Tokens weitergeleitet
  - empfängt ein Knoten ein frei zirkulierendes Token, weiß er, daß niemand am Senden ist und er Daten an dieses Token anhängen kann, um diese weiterzutransportieren
  - dieses besetzte Token wird an den NADN weitergeleitet, bis dieser den Knoten erreicht, an den die im Token transportierten Daten adressiert sind
  - die Empfänger-Station empfängt das Token, leitet die Daten an höhere Schichten weiter;
  - der nun leere Datenrahmen des Tokens wird entsprechend gekennzeichnet[4] und wieder in den Ring geleitet (zur Ausgangsstation, die das Paket gesendet hat)
  - empfängt die Ausgangsstation das Token, weiß sie, daß die Daten empfangen wurden (dieser Vorgang wird auch Feedback genannt)
  - Nun beginnt die Prozedur von vorne.
- jedes Gerät im Ring arbeitet auch als Repeater, die die Daten weiterleiten und empfangen, bis sie den Kreis wieder geschlossen haben
- die Stationen in einem Token-Ring-Netzwerkes werden auch als *Monitore* bezeichnet:
  - es gibt einen *aktiven Monitor* pro Ring
  - alle anderen sind damit *Standby-Monitore*, die bei Ausfall des aktiven Monitors einspringen
  - Aufgabe des aktiven Monitors ist die Durchführung einer Art Systemprüfung, die alle sieben Sekunden erfolgt

[4] durch zwei Bits

  - aktiver Monitor im Ring ist immer der Rechner, der als erster im Netz präsent war und somit das erste Token sendete

- die Systemprüfung läuft folgendermaßen ab:

  - alle sieben Sekunden sendet der aktive Token einen Token zur nächsten Station im Ring (NADN)
  - damit kennt die Empfangsstation die Adresse des aktiven Monitors
  - dann geht das Token wieder weiter im Ring zur nächsten Station und informiert dort ebenfalls über den aktiven Monitor
  - der Prozeß wiederholt sich solange, bis der Token wieder beim aktiven Monitor eintrifft
  - dadurch hat jeder Monitor im Netz folgende Informationen erhalten:
    * die Adresse des aktiven Monitors im Ring
    * die Adresse des jeweiligen NAUN
    * die Adresse des jeweiligen NADN
  - hört eine Station innerhalb der sieben Sekunden nichts von seinem NAUN, schickt es eine Nachricht den Ring hinunter mit folgenden Informationen:
    * seine eigene Netzwerkadresse
    * die Adresse des NAUN
    * Fehlerhinweis, z.B. keine Reaktion vom Knoten
  - diese Informationen werden auch als *Warnsignal* oder *Beaconing* bezeichnet
  - dieses Warnsignal hilft, den Fehler in einem Ring zu lokalisieren
  - der Bereich, in dem der Fehler auftritt, wird als *Fehler-Domäne* oder *Fault-Domain* bezeichnet
  - nach Lokalisierung der Fault-Domain filtert die Workstation, die den Fehler erkennt hat, die Datenpakete ihres fehlerhaften NAUNs aus, das Netzwerk bleibt stabil