Kommunikations-systeme und Netzwerke 3.JG

Horst Weißenbrunner
01.03.2022
Version 0.0

KOMMUNIKATIONSSYSTEME UND NETZWERKE

Netzwerk Grundlagen:

Rechnernetz

Ein Rechnernetz ist eine Anzahl einzelner miteinander verbundener Rechner.

Wirtschaftlicher Nutzen

- schneller Datenaustausch untereinander
- Daten können zentral erfasst und verarbeitet werden
- Zuverlässigkeit
  - in der Flugsicherung
  - im Bankenwesen
  - in militärischen Bereichen
- Vorhandene Ressourcen gemeinsam nutzen

Begriffe:

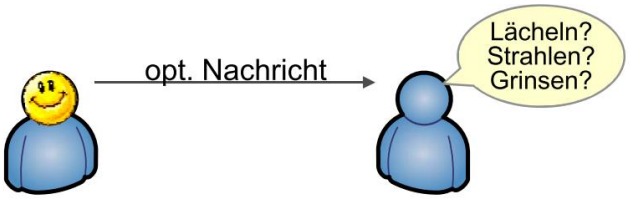
Kommunikation -> Gemeinsamkeit:

Kommunikation ist Austausch von Nachrichten zwischen Teilnehmern/Anwendungen. Nachrichten kann man senden und/oder empfangen

Nachrichten:

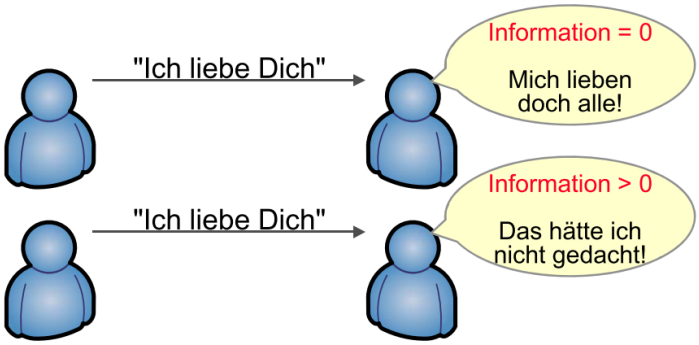
Nachrichten sind Bedeutungen, die ein K.-Teilnehmer bestimmten Ereignissen zuordnet.

Kommunikation ist nur möglich, wenn die am Prozess beteiligten Teilnehmer demselben Ereignis die gleiche (oder annähernd oder teilweise gleiche) Bedeutung zuordnen.



Information bezeichnet den qualitativen Aspekt einer Nachricht.

Information ist neues Wissen über ein Ereignis oder einen Sachverhalt,
Information ist Beseitigung von Ungewissheit.



Medien:

- Zwischenmenschliche Kommunikation basiert auf Sinnesorganen und Artikulation.
- Ereignisklassen zwischenmenschlicher Kommunikation werden Medien genannt.
- Beispiele: Sprache (Audio)-> Bild (Video) -> Text, Schrift (Daten).
- Aber, uneinheitliche Verwendung:
  -> Übertragungs-Medien (Koax, LWL, CuDA, Funk
  -> „Die Medien“ (Rundfunk/Presse).

Multimedia

Gleichzeitige Verwendung mehrerer Medien beim gleichen Kommunikationsprozess.
Multimedia wird oft an das Endgerät „Rechner“ gebunden.

Protokolle:

Protokolle sind Regeln, die den Nachrichtenaustausch regeln. Beispiel Funktechnik (Roger - Over - Out)

Auf Grund der hohen Komplexität werden die Aufgaben von einer Reihe von Protokollen, mit verschiedenen Teilaufgaben, abgewickelt.

Netzwerk-Protokolle regeln den Datenaustausch in Computernetzen. Sie definieren die erforderlichen Regeln für Aufgaben wie das Adressieren von Datenpaketen, die Vermittlung von Datenpaketen, den Transport von Datenpaketen, den Verbindungsaufbau oder die Fehlerüberprüfung. Wichtige Netzwerk-Protokolle für das Internet sind in der IP-Protokollfamilie zu finden.

Internet:

Das **Internet** (von englisch internetwork, zusammengesetzt aus dem Präfix inter und network ‚Netz' oder kurz net ‚Netz'), umgangssprachlich auch Netz, ist ein weltweiter Verbund von Rechnernetzwerken, den autonomen Systemen. Es ermöglicht die Nutzung von Internetdiensten wie WWW, E-Mail, Telnet, SSH, XMPP, MQTT und FTP. Dabei kann sich jeder Rechner mit jedem anderen Rechner verbinden. Der Datenaustausch zwischen den über das Internet verbundenen Rechnern erfolgt über die technisch normierten Internetprotokolle. Die Technik des Internets wird durch die RFCs der Internet Engineering Task Force (IETF) beschrieben.

Die Verbreitung des Internets hat zu umfassenden Umwälzungen in vielen Lebensbereichen geführt. Es trug zu einem Modernisierungsschub in vielen Wirtschaftsbereichen sowie zur Entstehung neuer Wirtschaftszweige bei und hat zu einem grundlegenden Wandel des Kommunikationsverhaltens und der Mediennutzung im beruflichen und privaten Bereich geführt. Die kulturelle Bedeutung dieser Entwicklung wird manchmal mit der Erfindung des Buchdrucks gleichgesetzt.

Die Übertragung von Daten im Internet unabhängig von ihrem Inhalt, dem Absender und dem Empfänger wird als Netzneutralität bezeichnet.

Quelle: https://de.wikipedia.org/wiki/Internet

Entwicklung und Betrieb

1969 wurde das ARPANET (Advanced Research Project Agency Network) aufgebaut.

Drei Universitäten wurden über 56 kbit-Netz verbunden
Initiiert und bezahlt vom Department of Defense (DoD). Ziel: robustes, leistungsfähiges und bezahlbares Netz.

1971: Email, Das Arpanet besitzt 15 Knoten

1973: TCP|UDP-IP-´Transportprotokolle

1983: Trennung in Milnet und Arpanet

Begriff Internet wird eingeführt

Einführung des Domain Name Service (DNS).

1988: erste Internetprovider in DE

1989: Verbreiterung der Nutzung (Kommerzialisierung)

wissenschaftlichen Einrichtungen, Schulen, Privathaushalte, Firmen, Organisationen

1992: Einführung des Internetdienstes WWW (world wide web).

Einfach zu nutzender Dienst für Text Bilder Audio Video

Internet wird zum Massennetz

1992 Gründung der Internet Society (ISOC)

Innerhalb der ISOC ist das Internet Architecture Board (IAB) für die technische Weiterentwicklung zuständig.

1997 Es sind rund sechs Millionen Computer mit dem Internet verbunden.

2002 Als Folge der Terroranschläge vom 11. September 2001 werden in vielen Ländern neue Gesetze eingeführt, die die Anonymität der Internetbenutzung erheblich einschränken.

Quelle: Entwicklung des Internet https://www.dvdh.de/internet/chronologische-entwicklung-des-internet.html

Organisationen in der Netzwerktechnik:

An der Entwicklung der Kommunikations- und Netzwerktechnik sind verschiedene nationale und internationale Organisationen beteiligt. Sie nehmen Normungen vor und entscheiden so über den Einsatz neuer Entwicklungen.

Es folgt ein Auszug der wichtigsten internationalen Organisationen, die eine besondere Relevanz besitzen.

IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
IEEE	Institute of Electrical and Electronics Engineers
IEC	International Electrotechnical Commission
ITU	International Telecommunication Union

Quelle: https://www.elektronik-kompendium.de/sites/net/1912011.htm

Netzwerk Topologien

Die Topologie eines Netzwerkes ist die Art der Leitungs- bzw. Kabelführung.

- Linien-Topologie
- Bus-Topologie
- Baum-Topologie
- Ring-Topologie
- Stern-Topologie
- Maschen-Topologie (dezentrales Netzwerk)

Quelle:
https://www.elektronik-kompendium.de/sites/net/0503281.htm
https://www.giga.de/extra/netzwerk/tipps/netzwerktopologien-in-der-it-was-warum-und-welche/

Linien-Topologie

- Alle Teilnehmer sind nacheinander in Reihe geschaltet.
- Es gibt einen Anfangs- und einen End-Teilnehmer.
- Teilnehmer können auf die übertragenen Informationen zugreifen, wenn sie diese durchlaufen.

Nachteile:

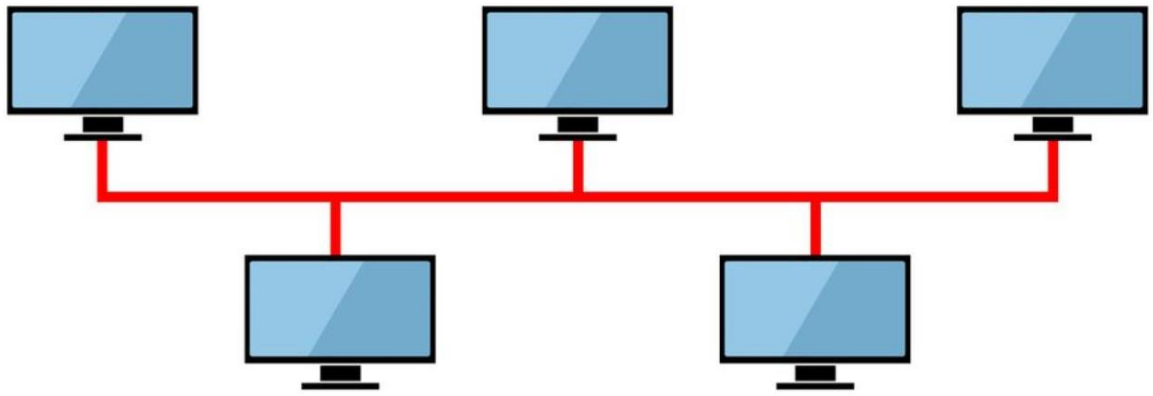
- Teilnehmer-Ausfall

Bus-Topologie

- Alle Teilnehmer sind über die gleiche Leitung (Bus) miteinander verbunden.
- Alle Teilnehmer können auf das Übertragungsmedium und die übertragenen Informationen zugreifen.
- Um Störungen auf der Leitung zu verhindern und die physikalischen Bedingungen zu verbessern, werden die beiden Kabelenden mit einem Abschlusswiderstand versehen.
- Soll der Bus erweitert werden oder Hosts hinzugefügt oder entfernt werden, kann das Netzwerk für die Zeit der Arbeiten ausfallen.

Nachteile:

- Teilnehmer-Ausfall (Coax)

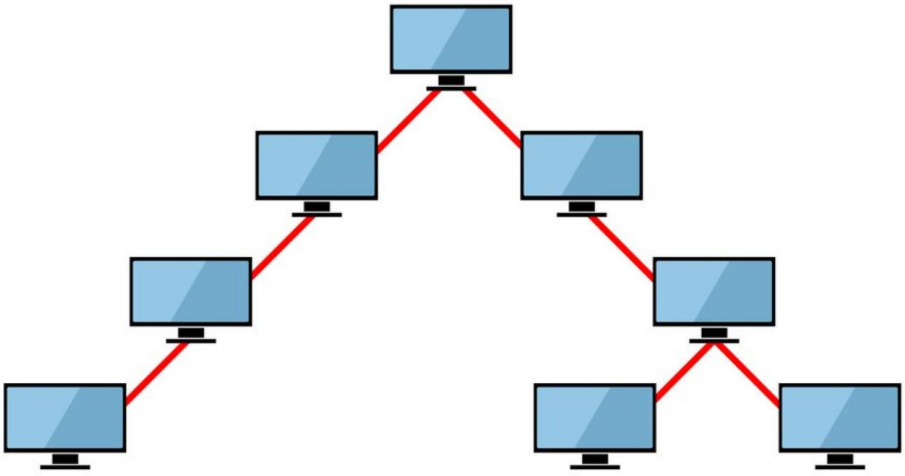


Baum-Topologie

- Ein Teilnehmer ist die Wurzel, von der aus sich andere Teilnehmer weiter „verzweigen“ können.
- Es ergibt sich eine Hierarchie.

Nachteile:

- Funktioniert weiterhin bei Teilnehmer-Ausfall (Redundanz) - Variabel (je näher der Ausfall an der Wurzel, desto schlimmer)

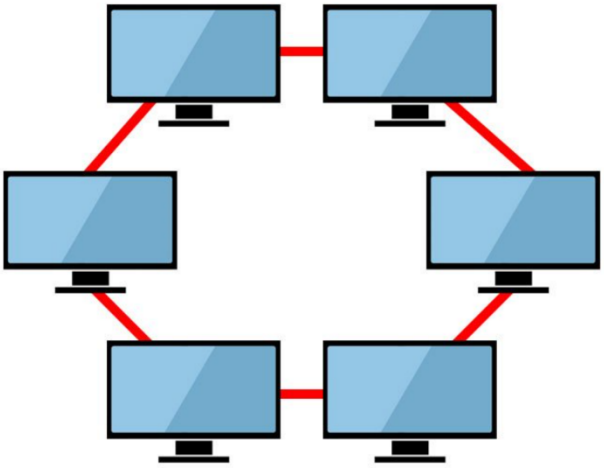


Ring-Topologie

- Teilnehmer werden zu einem Ring zusammengeschlossen.
- Die zu übertragende Information wird bis zu ihrem Bestimmungsort durch die anderen Teilnehmer durchgereicht.
- Durch Protection-Umschaltung kann der Ausfall des ganzen Rings bei Ausfall eines Teilnehmers verhindert werden.
- Kann in einen Bus-Betrieb umgeschaltet werden.

Eigenschaften:

- Redundanzmanager notwendig

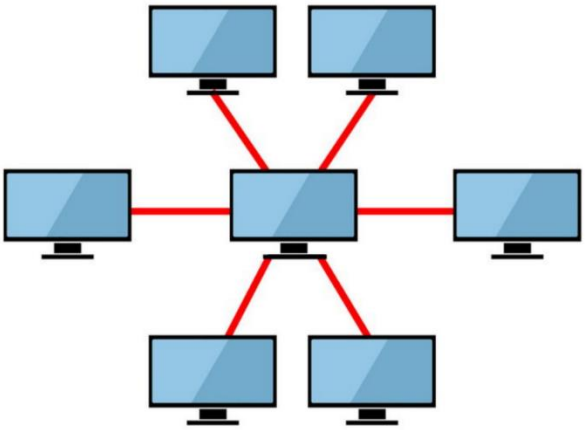


Stern-Topologie

- Alle Teilnehmer sind über einen zentralen Teilnehmer miteinander verbunden (Switch, Hub).
- Zentraler Teilnehmer übernimmt die Datensteuerung

Eigenschaften:

- Funktioniert weiterhin bei Teilnehmer-Ausfall - es sei denn der Zentral-Teilnehmer fällt aus.



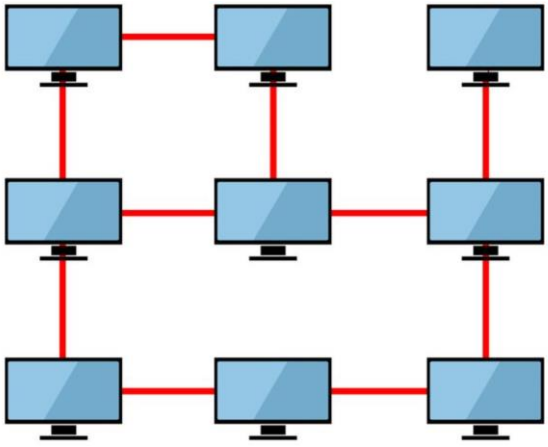
Maschen-Topologie

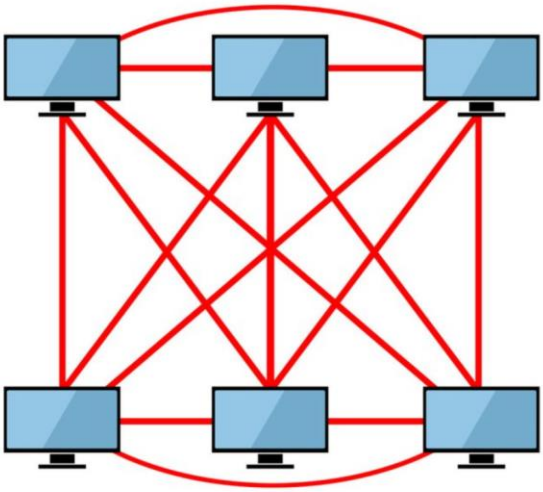
Teil:

- Jeder Teilnehmer ist mit einem oder mehreren Teilnehmern verbunden.
- Komplexes Routing nötig

Voll:

- Jeder Teilnehmer ist mit jedem anderen Teilnehmer verbunden.
- Benötigt kein Routing, da es nur Direktverbindungen gibt.





Vor und Nachteile (Übersicht)

Topologie	Vorteile	Nachteile
Bus-Topologie	• einfach installierbar • kurze Leitungen	• Netzausdehnung begrenzt • bei Kabelbruch fällt Netz aus • aufwändige Zugriffsmethoden
Ring-Topologie	• verteilte Steuerung • große Netzausdehnung	• aufwendige Fehlersuche • bei Störungen Netzausfall • hoher Verkabelungsaufwand
Stern-Topologie	• einfache Vernetzung • einfache Erweiterung • hohe Ausfallsicherheit	• hoher Verkabelungsaufwand • Netzausfall bei Ausfall oder Überlastung des Hubs
Maschen-Topologie	• dezentrale Steuerung • unendliche Netzausdehnung • hohe Ausfallsicherheit	• aufwendige Administration • teure und hochwertige Vernetzung

Quelle: https://www.elektronik-kompendium.de/sites/net/0503281.htm

Netzwerktypen

Je nach Größe und Reichweite des Rechnerverbunds werden verschiedene Netzwerkdimensionen unterschieden.

- Personal Area Networks (PAN)
  Unter diesem Netzwerktyp versteht man ein Netz, das aus Kleingeräte wie PDAs oder Mobiltelefone besteht.
  z. B. Bluetooth
- Local Area Networks (LAN)
  Unter LAN versteht man ein Computernetz, das Flächenmäßig auf 1 km² begrenzt ist.
  z. B. Ethernet und WLAN
- Metropolitan Area Networks (MAN)
  MANs sollen in einer Stadt, meist verschiedene Bürozentren verbinden.
- Wide Area Networks (WAN)
  WANs erstrecken sich über einen sehr großen geografischen Bereich, es erstrecket sich über Länder oder sogar Kontinente.
  z. B. DSL und Mobilfunk
- Global Area Networks (GAN)
  Unter einem GAN versteht man ein Netz das weltweit mehrere WANs verbindet.
  z. B. das Internet

Grundbegriffe Netzwerk:

Link

Ein physikalisches Netzwerk bezeichnet man manchmal auch als Link, was Verbindung bedeutet. Zu diesem Netzwerk gehören alle Nodes, die an dem selben Link angeschlossen sind bzw. die direkt miteinander verbunden sind.

Host

Ein Host ist ein Node ohne Router-Eigenschaft, die damit eine Endstelle in einem Netzwerk darstellt. Typischerweise wird ein Client oder Server als Host bezeichnet.

Knoten

Allgemein formuliert ist ein Knoten ein Verzweigungspunkt in einem Kommunikationsnetzwerk, an dem mehrere Verbindungen zusammenlaufen. Knoten sind im Telefonnetz die Vermittlungsstellen oder auch Telefonanlagen. In einem IP-Netzwerk sind Router und in einem Ethernet-Netzwerk sind Switche die Knoten.

Zugangspunkte zu einem Netzwerk, z. B. WLAN-Access-Points, werden häufig auch als Knoten bezeichnet.

Client

Ein Client ist ein Endgerät oder auch nur eine Software-Komponente, die von einer zentralen Stelle Dienste oder Daten anfordert oder über einen zentralen Zugang am Netzwerk teilnimmt. Der Client ist als Teil der Client-Server-Architektur in größere Zahl in allen Netzwerken zu finden.

Typische Hardware-Clients sind PCs, Smartphones, Tablets und Notebooks. Auf diesen laufen dann mehrere Software-Clients für unterschiedliche Dienste. WWW, E-Mail, Messaging, usw.

Server

Ein Server ist ein Computer, der Rechenleistung, Speicher, Daten und Dienste in einem Netzwerk bereitstellt und Zugriffsrechte verwaltet. Auf dem Server laufen mehrere Dienste und Anwendungen, die von anderen Netzwerk-Teilnehmern mit einem Software-Client über das Netzwerk angefordert werden.

Gateway

Ein Gateway ist eine Hardware oder Software oder eine Kombination daraus, die eine Schnittstelle zwischen zwei inkompatiblen Netzwerken darstellt. Das Gateway kümmert sich darum, dass die Form und Adressierung der Daten in das jeweilige andere Format oder Protokoll des anderen Netzes konvertiert werden.

Bridge

Eine Bridge bzw. Netzwerkbrücke verbindet zwei Teilnetze, die auf der Schicht 1 und 2 des OSI-Schichtenmodells arbeiten. Für die Hosts im Netzwerk ist die Bridge transparent, sie können sie nicht sehen.

In den Anfangszeiten von lokalen Netzwerken mit Ethernet stand der Begriff Bridge für ein Gerät zur Kopplung zweier Ethernet-Segmente. Die Bridge war eine wichtige Komponente, um große lokale Netzwerke zu betreiben. Die Segmentierung begrenzt die Größen der Kollisions-Domänen und das Risiko einer Schleifenbildung.

Einen Switch kann man auch als Multiport-Bridge betrachten.

Port

In der Netzwerktechnik kann ein Port eine Steckverbindung an einem Switch, Router, etc. oder eine logische Assoziation sein. Zum Beispiel der Zugang zum Netzwerk für einen WLAN-Client an einem WLAN-Access-Point.

Der Port bei den Protokollen TCP und UDP ist eine Art Adresse, die die Zuordnung zwischen einem Protokoll und einer Anwendung oder zwischen einem Datenstrom und einer Anwendung definiert.

Ein Port, egal ob logisch oder physisch, wird häufig durch eine Nummer oder Adresse gekennzeichnet.

Backbone

Backbone ist eine Bezeichnung für die Hauptübertragungsstrecke in einem Netzwerk. Der Backbone verbindet in der Regel mehrere Netzknoten. Die Netzknoten sind die Zugangspunkte zum Backbone. Man spricht in dem Zusammenhang auch vom Kernnetz oder Core Network.

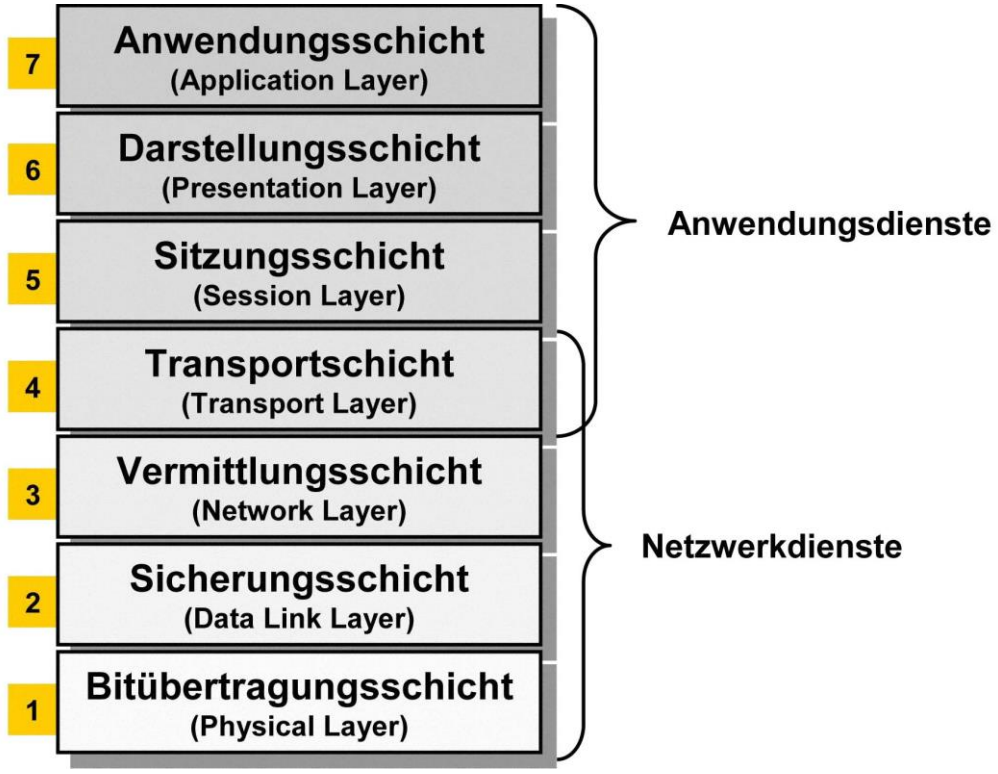
Bei größeren Vernetzungen mit mehreren Netzwerkstrukturen bildet ein Backbone die Infrastruktur im Hintergrund. Zum Beispiel um lokale Netze und Hochleistungssysteme miteinander zu verbinden. Ein Backbone wird dabei redundant ausgelegt.

Quelle: https://www.elektronik-kompendium.de/sites/net/1710111.htm

ISO/OSI 7-Schichten Modell:

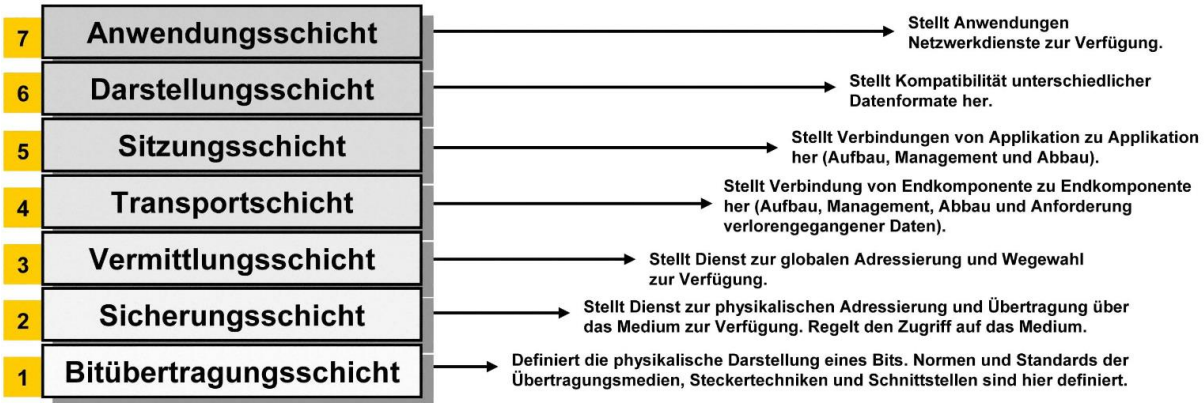
1984 wurde das ” Reference Model for Open Systems Interconnection“ oder kurz OSI-Modell veröffentlicht.

Die Schichtung beruht auf dem Prinzip, dass jede Schicht der ihr Übergeordneten Schicht bestimmte Dienstleistungen anbietet. Die Schicht, die Dienstleistungen in Anspruch nimmt, braucht keinerlei Kenntnisse darüber haben, die diese Dienste erbracht werden.



Eselsbrücke:

Please Do Not Throw Salami Pizza Away



Layer 1: Physical Layer, Bitübertragungsschicht

Maßnahmen und Verfahren zur Übertragung von Bitfolgen

Der Physical Layer regelt die Übertragung von Bits über das Übertragungsmedium, die Festlegungen betreffen also die Eigenschaften des

Übertragungsmediums. wie z.B.: physikalische Steckverbindungen, Spannungs- bzw. Strompegeln, Übertragungsgeschwindigkeit, usw.

Layer 2: Data Link Layer, Sicherungsschicht

Logische Verbindungen mit Datenpaketen und elementare Fehlererkennungsmechanismen

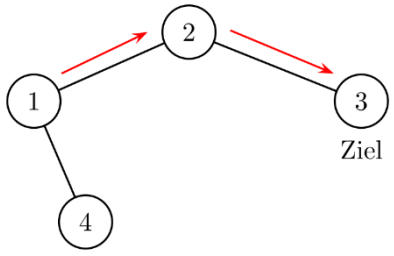
Die Aufgabe des Data Link Layers besteht darin, aus der unsicheren Übertragung des Physical Layers (elektrische Störungen!) eine sichere Übertragung zu machen. Zu diesem Zweck werden die Daten in Rahmen (frames) aufgeteilt und mit Zusätzen zur Fehlererkennung versehen. Protokollbeispiele: HDLC (high-level data link control), SLIP (serial line IP), PPP (point-to-point protokol)

Layer 3: Network Layer, Vermittlungsschicht

Routing und Datenflusskontrolle

Die Netzwerkschicht stellt die Verbindung zwischen Knoten her. Die wichtigste Aufgabe ist die Auswahl der Paket-Routen, also das Routing von Sender zum Empfänger. Auf dieser Schicht erfolgt erstmals die logische Adressierung der Endgeräte.

Das Internet Protokoll (IP) ist in dieser Schicht einzuordnen.
In der Skizze ist der Knoten 3 nicht direkt mit Knoten 1 verbunden. Sollen nun Daten von 1 nach 3 gesendet werden, so ist der Network Layer von Knoten 1 verantwortlich die Daten an Knoten 2 zu senden. Dessen Network Layer ist wiederum verantwortlich die Daten nicht an seine darüberliegenden Schichten, sondern weiter an Knoten 3 zu senden, der das Ziel darstellt.



Layer 4: Transport Layer, Transportschicht

Logische Ende-zu-Ende-Verbindungen

Der Transport Layer stellt aus den Daten der darunterliegenden Schichten eine zuverlässige end-to-end Verbindung her. Dazu gehört vor allem das Herstellen der richtigen Reihenfolge der einzelnen Pakete, denn diese werden nicht garantiert in derselben Reihenfolge empfangen wie sie gesendet wurden. Protokollbeispiele: TCP (Transmission Control Protocol),UDP (User Data Protocol)

Die Transportschicht ist das Bindeglied zwischen den transportorientierten und anwendungsorientierten Schichten. Hier werden die Datenpakete einer Anwendung zugeordnet.

Layer 5: Session Layer, Sitzungsschicht

Prozeß-zu-Prozeß-Verbindungen

Die Sitzungsschicht ermöglicht den Verbindungsauf- und abbau, und regelt den Austausch von Nachrichten auf der Transportverbindung .z.B. Kann ein Transfer in nur einer Richtung stattfinden, regelt die Sitzungsschicht, wer an der Reihe ist.

Layer 6: Presentation Layer, Darstellungsschicht

Ausgabe von Daten in Standardformate

Der Presentation Layer beschäftigt sich mit den high-level Datenstrukturen die benötigt werden um dieselben Daten in verschiedensten Umgebungen gleich darzustellen. z.B. die Behandlung unterschiedlicher Zeichensätzen (ASCII, ISO-Latin-1, EBCDIC, etc.)

Layer 7: Application Layer, Anwendungsschicht

Dienste, Anwendungen und Netzmanagement

Die Anwendungsschicht enthält eine große Zahl häufig benötigter Protokolle, die einzelne Programme zur Erbringung ihrer Dienst definiert haben. Protokollbeispiele: ftp, telnet, mail

Auf dieser Ebene findet auch die Dateneingabe und -ausgabe statt.

Quelle: https://www.elektronik-kompendium.de/sites/kom/0301201.htm

OSI-Schichtenmodell in der Netzwerktechnik

<table>
<tr><th>OSI</th><th>Einordnung</th><th>DoD</th><th>Protokolle</th><th>Einheiten</th><th>Behandlung</th><th>Komponenten</th></tr>
<tr><td>Anwendung</td><td rowspan="3">anwendungs-
bezogen</td><td rowspan="3">Anwendung</td><td rowspan="3">DNS
HTTP
SMTP
IMAP</td><td rowspan="3">Daten</td><td>Kapselung</td><td rowspan="3">Gateway
Server
Proxy</td></tr>
<tr><td>Darstellung</td><td>Codec
Dateiformat</td></tr>
<tr><td>Kommunikation</td><td>Verschlüsselung</td></tr>
<tr><td>Transport</td><td rowspan="4">übertragungs-
bezogen und
transport-
orientiert</td><td>Transport</td><td>TCP UDP</td><td>Segment
(TCP)
Datagram
(UDP)</td><td></td></tr>
<tr><td>Vermittlung</td><td>Internet</td><td>IPv4 IPv6</td><td>Datagram</td><td></td><td>Router
L3-Switch</td></tr>
<tr><td>Sicherung</td><td rowspan="2">Netzzugang</td><td rowspan="2">Ethernet
WLAN</td><td rowspan="2">Rahmen
Frame
Bit
Symbol</td><td></td><td>Switch
Bridge</td></tr>
<tr><td>Bitübertragung</td><td></td><td>Hub
Repeater</td></tr>
</table>

Datenübertragung und Adressierung

Zum Verständnis der Funktionsweise von Protokollen in Schichtenmodelle ist es hilfreich zwischen der Adressierung und der Datenübertragung zu unterscheiden.

<table>
<tr><th>Schichten</th><th colspan="2">Datenverarbeitung und -übertragung</th><th colspan="2">Adressierung und Verbindungsaufbau</th></tr>
<tr><td>Anwendung
OSI-Schicht
5 + 6 + 7</td><td>HTTP, FTP,
IMAP, SMTP</td><td>SMB (Windows)
Samba (Unix/Linux)
↓
NetBIOS (Windows)</td><td>URL:
www.das-elko.de</td><td>NetBIOS-Name
(Computername)
↓
lmhosts / WINS</td></tr>
<tr><td>Übertragung
OSI-Schicht
3 + 4</td><td colspan="2">Transport: TCP / UDP (Datenpakete)
↓
Adressierung: IP / ICMP (Adresse)</td><td colspan="2">IP-Adresse und TCP/UDP-Port</td></tr>
<tr><td>Netzzugang
(physikalisch)
OSI-Schicht
1 + 2</td><td colspan="2">NDIS
Treiber
Netzwerkkarte (NIC)</td><td colspan="2">ARP
MAC-Adresse
Ethernet</td></tr>
</table>

Quelle: https://www.elektronik-kompendium.de/sites/net/0706101.htm

Links und Videos:

Links:

Grundlagen:

https://www.elektronik-kompendium.de/sites/net/0503271.htm

https://dev-supp.de/netzwerk-anonymitaet/rechnernetze

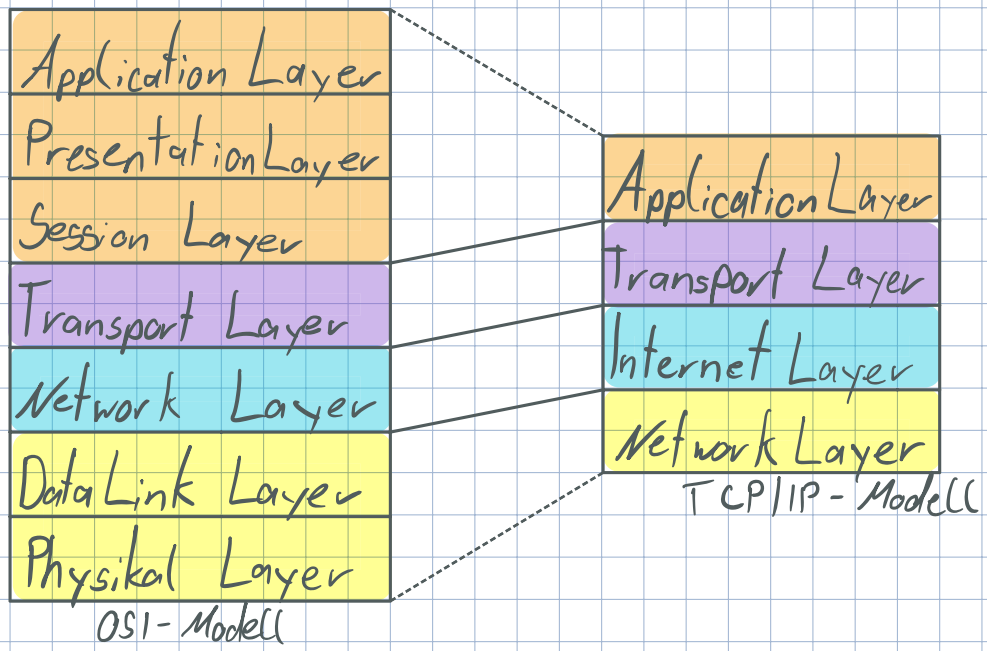
https://dbs.uni-leipzig.de/buecher/mrdbs/mrdbs-15.html

https://userpages.uni-koblenz.de/~unikorn/lehre/gdrn/ws16/01%20Einf%81hrung%20(leer).pdf

Grundlagen:

- Rechnernetz:
  - Ein Rechnernetz ist eine Anzahl einzelner miteinander verbundener Rechner.
- Wirtschaftliche Nutzen
  - schneller Datenaustausch untereinander
  - Daten können zentral erfasst und verarbeitet werden
  - Zuverlässigkeit:
    - in der Flugsicherung
    - im Bankenwesen
    - in militärischen Bereichen
  - Verhandene Ressourcen gereinsam nutzen

TCP/IP-Referenzmodell (cfd.tu-berlin.de)



Adressierung:

Benötigt beim Durchlauf der 4 TCP/IP-Schichten

1) MAC-Adresse (Media Access-Control-Adr) 48bit ≙ 6bytes

Hex: 00:80:FA:20:CB:01 (00:80:FA = Hersteller, 20:CB:01 = Lfd. Nr)

Hardwareadresse jedes Netzwerkadapters eindeutig

2) (IP-Adresse) Internet Adr. 10.0.0.99

3) Transport-Protokoll Adresse (6 → TCP / 17 → UDP)

4) Port

Fach: KSN 3 V1.1

Subnetting

Horst Weißenbrunner

Grundlagen

IP-Adresse

IP-Adressen bestehen bei IPv4 aus 32 Bit und bei IPv6 aus 128 Bit.

Jedes Gerät innerhalb eines Datennetzwerkes braucht eine Adresse, damit es eindeutig identifiziert werden kann. Das gilt sowohl fürs kleine Heimnetzwerk als auch für das Internet. Nur so ist gesichert, dass der Datenstrom beim richtigen Gerät ankommt. Beim Aufruf einer Internetseite überträgt der Browser stets auch die IP-Adresse Ihres Geräts mit. Denn nur so weiß der Web-Server, wohin er das gewünschte Datenpaket senden soll.

Sie besteht aus 32 Bits, sind technisch gesehen also eine 32-stellige Binärzahl wie z. B. 11000000 10101000 10110010 00011111. Um dieses Ziffernmonster zu bändigen, wird es in der Regel als eine Kombination aus vier Dezimalzahlen mit Werten von 0 bis 255 dargestellt, die mit Punkten voneinander getrennt sind. Unser Beispiel sieht in diesem Format wie folgt aus: 192.168.178.31.

Subnet Mask

Das zweite, für TCP/IP erforderliche Element ist die Subnetzmaske. Die Subnetzmaske wird vom TCP/IP-Protokoll verwendet, um zu bestimmen, ob sich ein Host im lokalen Subnetz oder in einem Remotenetzwerk befindet.

11000000.10101000.01111011.10000100 -- IP address (192.168.123.132)
11111111.11111111.11111111.00000000 -- Subnet mask (255.255.255.0)

Netzadresse

Bei einer IPv4-Adresse ist der vordere Teil die Netzadresse und der hintere Teil die Hostadresse. Die Teilung findet typischerweise an einem Punkt (".") statt. Aber nicht immer. An welcher Stelle genau die IPv4-Adresse in Netz und Host geteilt wird, dass entscheidet die Netzklasse oder die Subnetzmaske.

Broadcast Adresse

Datenpakete mit der Broadcast-Adresse als Zieladresse werden in dem jeweiligen Subnetz an alle Hosts geschickt. Eine Broadcast-Adresse innerhalb eines Netzwerks dient dazu, alle Hosts innerhalb eines Netzwerks zu erreichen.

IPV4-Netzwerkklassen

Typischerweise werden IP-Adressen in Klassen eingeteilt.

Netzklasse	Präfix	theoretischer Adressbereich	Netzmaske	Netze	Hosts im Netz
Klasse A	0	0.0.0.0 – 127.255.255.255	255.0.0.0	128	16 777 216
Klasse B	10	128.0.0.0 – 191.255.255.255	255.255.0.0	16 384	65 536
Klasse C	110	192.0.0.0 – 223.255.255.255	255.255.255.0	2 097 152	256
Klasse D	1110	224.0.0.0 – 239.255.255.255	Multicast-Anwendungen		
Klasse E	1111	240.0.0.0 – 255.255.255.255	reserviert für zukünftige Anwendungen		

Subnetting

Subnetting unterteilt ein Netzwerk in mehrere kleinere Unternetze. Das Gegenteil davon wäre Supernetting. Beim Supernetting wird mit anderen Worten die Anzahl der maximalen Hosts im Netzwerk erhöht oder mehrere Netze zusammengefasst.

Beim Subnetting können dem eigentlichen Subnetz z.B. der Klasse B (255.255.0.0) Bits vom Hostanteil für Sub-Subnetze gegeben werden.

Herkömmliches Subnetting ersetzt das 2-Teiligen IP Adressierungsschema durch ein 3-Teiliges. Neben dem Host- und Netzwerkteil, die in der IP-Adresse enthalten sind, kommt zusätzlich nun auch noch eine Subnetmaske hinzu.

<- 32 BIT ->		
Netzwerknummer	**Hostnummer**	
Netzwerknummer	**Subnetznummer**	**Hostnummer**

Beispiel:

Das vorhandene Netz soll in 4 Subnetze unterteilen.

IP-Adresse: 192.168.168.0

Subnetzmaske: 255.255.255.0

Lösung:

Netzadresse **192.168.168.**0 — Alle Bits der IP-Adresse mit Subnet Mask Binär AND verknüpfen

Hostanteil 192.168.168.**0** — alle Stellen bei denen die Subnet Mask (Binär) 0 ist

192.168.168.**0000 0000**

Anzahl von bits:	1	2	3	4	5	6	7	8	...
Anzahl der Subnetze:	2	4	8	16	32	64	128	256	...

Mit 1 bit können 2^1 = 2 Subnetze aufgebaut werden.
Es sind aber 4 Subnetze notwendig.

Mit 2 bits können 2^2 = 4 Subnetze aufgebaut werden.

Der Netzteil soll also um 2 bits erweitert werden.

Netzanteil | Hostanteil

Ip-Adresse: 192.168.168.00|**000000**

Netzmaske: 255.255.255.11|**000000**

6 bits

Der Netzanteil wurde um 2 bits in der Netzmaske erweitert. (Von links nach rechts)

Dadurch verschiebt sich die Grenze zwischen dem Hostanteil und Netzanteil nach rechts. (D.h. der Netzanteil ist nun größer geworden)

Der Hostanteil besteht nun aus 6 bits .

D.h jedem Subnetz stehen 2^6 = 64 IP Adressen zur Verfügung:

Subnetzadresse (1 IP)	Host- IP-Range (62 IP)			Broadcast (1 IP)
192.168.168.0	192.168.168.1	-	192.168.168.62	192.168.168.63
192.168.168.64	192.168.168.65	-	192.168.168.126	192.168.168.127
192.168.168.128	192.168.168.129	-	192.168.168.190	192.168.168.191
192.168.168.192	192.168.168.193	-	192.168.168.254	192.168.168.255

Links:

https://www.heise.de/netze/tools/netzwerkrechner/

https://www.elektronik-kompendium.de/sites/net/0907201.htm

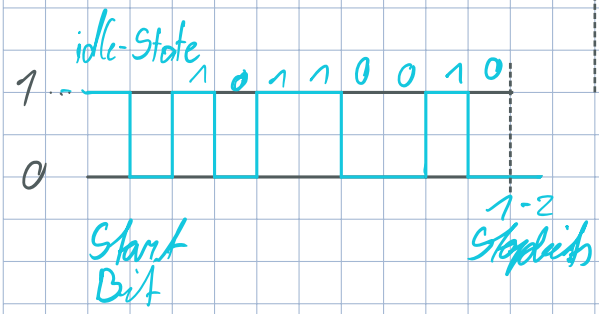
Videos:

https://www.youtube.com/watch?v=BbWtW1jHkBM

Übertragungsmethoden

Asynchrone DÜ

- Leitung meiste Zeit im Leerlauf (Idle)
- Hin und wieder werden kleine Blöcke übertragen
- bis 115200 Baud



Synchrone DÜ

schneller!!

- Clock Pulse (dauernd)
  (Sender + Empfänger synchron)