1st Slide Set
Computer Networks

Prof. Dr. Christian Baun

Frankfurt University of Applied Sciences
(1971–2014: Fachhochschule Frankfurt am Main)
Faculty of Computer Science and Engineering
christianbaun@fb2.fra-uas.de

Organizational Information

- **E-Mail:** `christianbaun@fb2.fra-uas.de`

!!! Tell me when problems exist at an early stage !!!

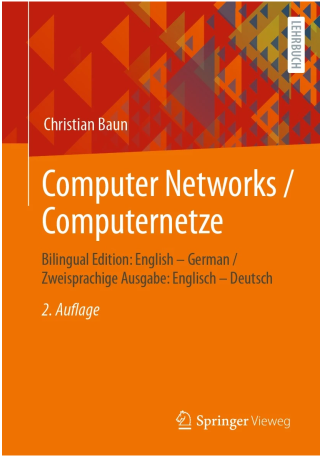
- **Homepage:** `http://www.christianbaun.de`

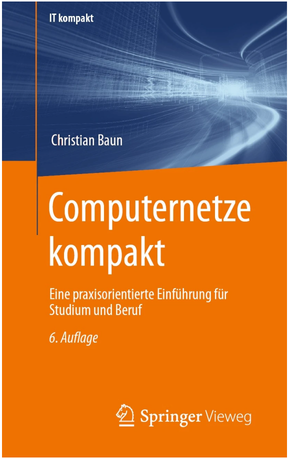
!!! Check the course page regularly !!!

- The homepage contains among others
  - **Presentation slides** in English and German language
  - **Exams**
  - **Sample solutions**
- Participating the exercises is not a precondition for exam participation
  - But it is recommended to participate the exercises

The content of the English and German slides is identical, but please use the English slides for the exam preparation to become familiar with the technical terms

Literature





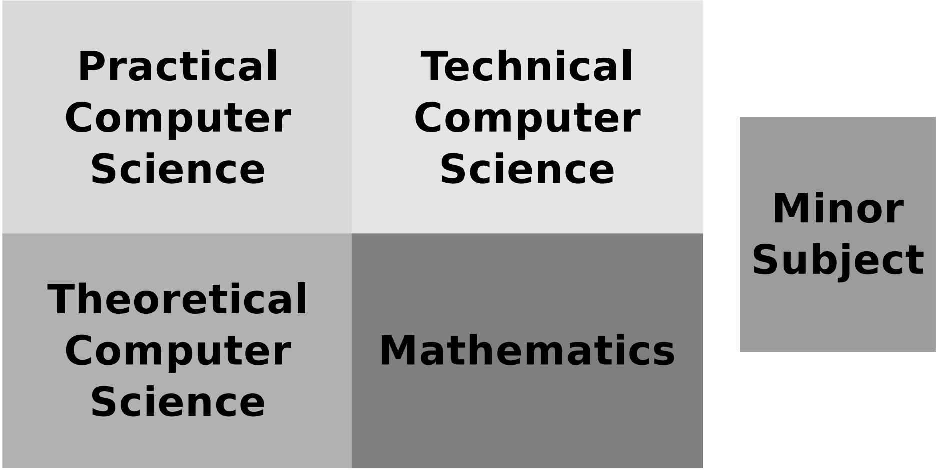
- My slide sets were the basis for these books
- The two-column layout (English/German) of the bilingual book is quite useful for this course

You can download both books for free via the FRA-UAS library from the intranet

Learning Objectives of this Slide Set

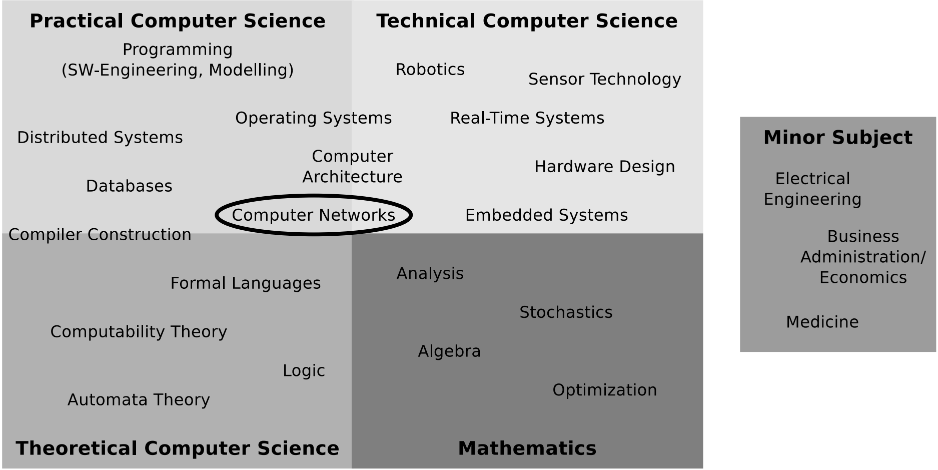
- Organizational Information
- Fundamentals of computer networks
  - Network services, roles, transmission media and network protocols
  - Classification of networks
  - Parallel/ serial data, synchronous/asynchronous data transmission
  - Directional dependence (anisotropy) of data transmission
  - Topologies
  - Frequency, data signal and fourier series
  - Bit rate, baud rate, bandwidth and latency
- Protocols
  - TCP/IP reference model
  - Hybrid reference model
  - OSI reference model

Computer Networks in Computer Science (1/2)



Where would you place the computer networks?

Computer Networks in Computer Science (2/2)



Computer networks belong to practical computer science and technical computer science

Required Components to set up a Computer Network

- For setting up and running a computer network, these components are required:
  1. ≥ 2 **terminal devices with network services running**
     - The devices are intended to communicate with each other or access shared resources
     - A network service provides a service for communication or shared resources usage
  2. **Transmission medium** to send and receive data (see slide set 2)
     - Common used transmission media are based of copper wires (e.g. twisted pair cables or coaxial cables) and fiber-optic cables
     - Wireless data transmission is also possible
  3. **Network protocols** (see slide 30)
     - Rules that specify, how computers can communicate

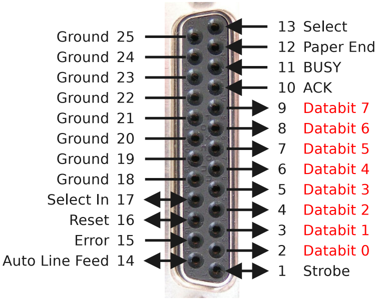
The rules (network protocols) are mandatory. Without them, the communication partners cannot *understand each other*. Just imagine a phone call to a foreign country. The connection is established, but no participant understands the other's language. Only if all participants speak the same language, communication becomes possible

Parallel Data Transmission

- Communication between computers is possible via **parallel** and **serial** data transmission
- With **parallel data transmission**, in addition to the control lines, multiple data lines exist
- Example: Parallel port which was the standard interface to connect printers until it was replaced by USB
  - Via this interface, an entire byte of data can be transferred per time unit
- Benefit: Higher throughput
- Drawback: Lots of lines are necessary
  - This is cost-intensive for long distances
- Usage: Local bus systems

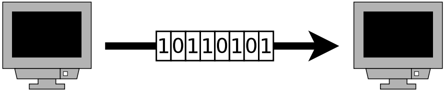
(e.g. ATA, SCSI, ISA, PCI, Front Side Bus, IEEE-1284 "printer port")

The image shows the parallel port (DB25 = 25 pins)

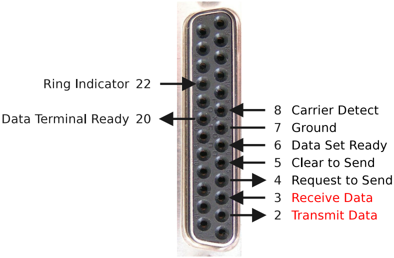


Serial Data Transmission

- When **serial data transmission** is used, the bits are transmitted one after another via the bus
  - Transferring a byte takes 8 times longer compared to parallel data transmission (when using 8 data lines)
- Benefit: Can be used for long range distances, because only few wires are required
- Drawback: Lesser throughput
- Usage: Local bus systems and **computer networks**



The image shows the serial port RS-232 (DB-25 = 25 pins)



Some serial network technologies

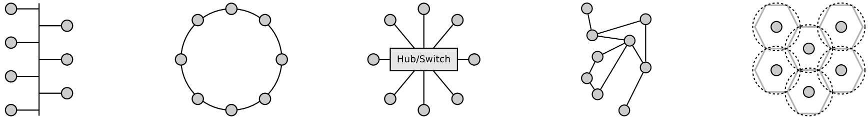
Ethernet, USB, CAN, FireWire, Fibre Channel (for SAN), InfiniBand

Directional Dependence (Anisotropy) of Data Transmission

- **Simplex**
  - The information transfer only works in one direction
  - After the end of a transmission, the communication channel can be used by another sender
  - Examples: Radio, TV, Pager
- **Duplex (Full-duplex)**
  - The information transfer works in both directions simultaneously
  - Examples: Phone, networks with twisted pair cables because they provide separate wires for send and receive
- **Half-duplex**
  - The information transfer works in both directions, but not simultaneously
    - Only one direction at a time
  - Examples:
    - Networks with fiber-optic cables or coaxial cables, because there exists just a single line to sending and receiving
    - Wireless networks with just a single channel

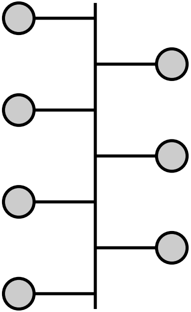
Topologies of Computer Networks

- The topology of a computer network...
  - determines how the communication partners are connected with each other
  - affects its reliability a lot
- The structure of large-scale networks is often a combination of different topologies
- Physical and logical topology may differ
  - **Physical topology**: Describes the wiring
  - **Logical topology**: Describes the flow of data between the terminal devices
- Topologies are graphically represented with nodes and edges



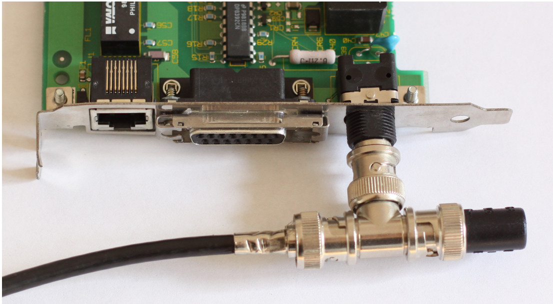
Bus Network

- All terminal devices are connected via a shared cable – the bus

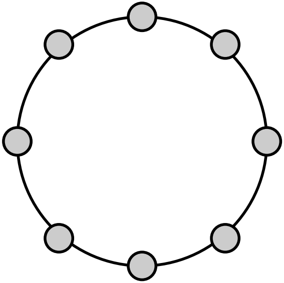


- No active components between the terminal devices and the shared cable
  - If a node fails, it does not affect the network itself
- Advantage: Cheap to implement
  - In the past, Hubs and Switches have been expensive
- Drawback: Shared cable fails $\Longrightarrow$ network fails
- Only a single node can send data at each point in time $\Longrightarrow$ otherwise, collisions will occur
  - A media access control method like CSMA/CD is required (see slide set 6)
- Examples:
  - 10BASE2 (Thin Ethernet) and 10BASE5 (Thick Ethernet): 10 Mbps
  - PowerLAN (Powerline Communication) uses the power grid as shared transmission medium: 1200 Mbit/s

10BASE2 (A Journey into the Past)



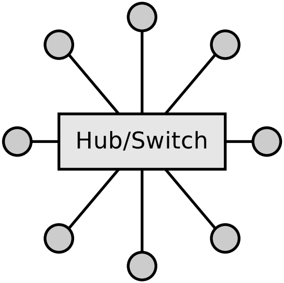
Ring Network



- Connects node to node
- All data is transferred from nodes to nodes until the destination is reached
- Disruption of a single link $\Longrightarrow$ network failure

- Each node is also a repeater, which amplifies the signal
  - For that reason, large-sized rings (transmission medium dependent) are possible
  - Maximum ring length for Token Ring: 800 m
- Examples:
  - Token Ring (**logical**): 4-16 Mbps
  - Fiber Distributed Data Interface (FDDI): 100-1000 Mbps
    - FDDI implements 2 rings
    - One is a secondary backup, in case the primary ring fails

Star Network



- All nodes are connected directly with a central component (Hub or Switch)
- Failure of the central component leads to a failure of the network itself
  - The central component can be implemented in a redundant way
- Failure of a node do not cause a failure of the network itself
- Advantages: Expandability and stability
- Examples:
  - Ethernet: 10 Mbps, 100 Mbps, 1-40 Gbps
  - Token Ring (**physical**): 4-16 Mbps
  - Fibre Channel (storage networks): 2-16 Gbps
  - InfiniBand (cluster): 10-40 Gbps

Media Access Unit

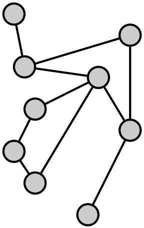
Image source: Raymangold22. Wikimedia (CC0)

- Token Ring demonstrates that the physical and logical topology of a network can be different
  - Token Ring implements a logical ring network
  - Wiring is mostly done equal to a star network
- Using a Media Access Unit (MAU) was common
  - Each device is connected with just a single cable with the MAU
  - **Implements a star network from a technical point of view**
    - **Still a ring network from a logical point of view**
  - A MAU is a *ring in a box*

- If a node is not connected or does its connection fail, then the MAU bypasses this node and the ring is still properly functioning

Mesh Network

- Each node is connected with one or more other nodes
  - In a **fully connected mesh network**, the nodes are all connected to each other
- If nodes or connections fail, communication inside the network is typically still possible because the frames are redirected



- Benefit: Failure safe (depends on the cabling effort)
- Drawbacks: Cabling effort and energy consumption
- Furthermore, in not fully connected mesh networks, it is complex to identify the best way from sender to receiver during packet forwarding
- Examples:
  - Logical topology between Routers
  - Ad-hoc (wireless) networks

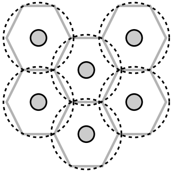
Tree Network

- One or more edges are connected with the root
  - Every edge leads to a leaf node or to the root of another tree
- Several star topology networks are hierarchically connected
- Benefits:
  - Failure of a terminal device (leaf node) has no consequences
  - Good expandability and long distances are possible
  - Well suited for searching and sorting algorithms
- Drawbacks:
  - When a node fails, the complete (sub-)tree behind is no longer accessible
  - In a large tree, the root may become a bottleneck because the communication from one half of the tree to the other half always needs to pass the root

- Example:
  - Connecting Hubs or Switches via an uplink port

Cellular Network

- Implemented by wireless networks
- **Cell**: Area where the nodes can communicate with the base station
- Advantage: Failure of nodes do not affect the network itself
- Drawback: Maximum dimension is limited by the number of base stations and their positions



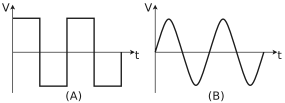
- Only one node can send data at each point in time $\Longrightarrow$ otherwise, collisions will occur
  - A media access control method like CSMA/CA is required (see slide set 6)
- Examples:
  - Wireless LAN = WiFi (IEEE 802.11)
  - Global System for Mobile Communications (GSM)
  - Bluetooth hotspots

Current Situation

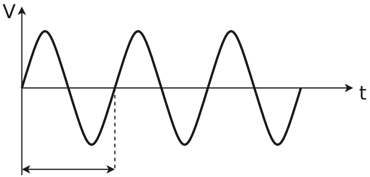
- **Bus** and **ring topology** are seldom used nowadays
  (⟹ see slide set 2)
  - 10BASE2/5 (Thin/Thick Ethernet) are outdated since the mid/end-1990s
  - May 2004: IBM sells his complete Token Ring product lineup
  - PowerLAN (Powerline Communication) is a niche technology
- Today, Ethernet (1-40 Gbit/s) with Switches (⟹ **star topology**) is standard for wired LAN
  (⟹ see slide set 4)
- Connecting Hubs and Switches implements a **tree topology**, if there are no loops in the cabling
  (⟹ see slide sets 3+4)
- **Cell topology** is the standard for wireless networks
  (⟹ see slide set 2)
- **Mesh topology** is one possible use case of wireless networks and it is the logical topology between Routers
  (⟹ see slide sets 2+7+8)

Frequency

- Electrical engineering distinguishes between 2 types of voltage:
  1. **Direct current voltage**: Polarity of voltage and voltage level remain constant
  2. **Alternating current voltage**: Polarity of voltage and voltage level change periodically



- Fig. A: *Rectangular shaped* alternating current voltage in theory
- Fig. B: *Sinus shaped* alternating current voltage in practice
- **Period**: The time it takes for the periodic voltage curve
- **Frequency**: Number of oscillations per second
- The lower the period, the higher is the frequency



$$\text{Frequency [Hz]} = \frac{1}{\text{Period [s]}}$$

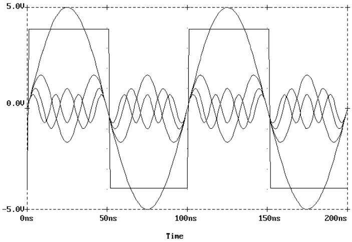
- The unit for frequency is the hertz (Hz)
- 1 Hz = 1 event (oscillation) per second
- Example: Alternating current voltage in Europe with 50 Hz

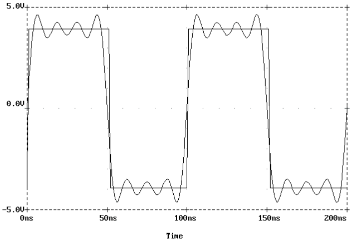
Data Signal

- Data exchange takes place through the exchange of **binary data**
  - But the transmission media always transmit **analog signals**
- The signals are subject to physical laws
  - This includes the **attenuation** (signal weakening)
  - Attenuation weakens the amplitude of a signal more and more over distance on all transmission media
    - If the amplitude of a data signal has dropped below a certain value, it can no longer be clearly interpreted
  - Thus, the attenuation limits the maximum bridgeable distance for all transmission media
  - The **higher** the **frequency**, the **higher** is the **attenuation**

Fourier Series

Image source: Jörg Rech. Ethernet. Heise



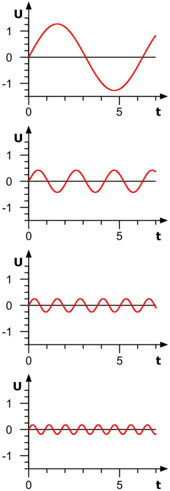


- According to the **fourier series**, which is named in honour of Jean Baptiste Joseph Fourier (1768-1830), a square-wave signal (e.g. a binary signal), consists of the sum of a set of oscillating functions
  - A square wave signal consists of a fundamental frequency and harmonics
  - Harmonics are integer multiples of the fundamental frequency
    - They are often referred to as harmonics of the 3rd, 5th, 7th, etc. order
  - The more harmonics are taken into account, the more similar becomes the result with a square wave signal

Fourier Series and Bandwidth

Image Source: René Schwarz. Wikipedia (CC-BY-SA-1.0)

- To **transmit a square-wave signal** clearly via the transmission medium, at least the **fundamental frequency** and the **harmonics of the 3rd and 5th order** need to be transmitted bug-free
  - The harmonics of the 3rd and 5th order are necessary for keeping the square wave its rectangular shape and preventing that it looks rounded (see next slide)
  - In practice, the harmonics are more attenuated than the fundamental frequency
- The **bandwidth**, from the viewpoint of the transmission medium, is the range of frequencies which can be transmitted via the transmission medium without interferences



We already know...

The attenuation of the signal increases with the frequency

Fourier Synthesis of a square-wave Signal

Source: Wikipedia

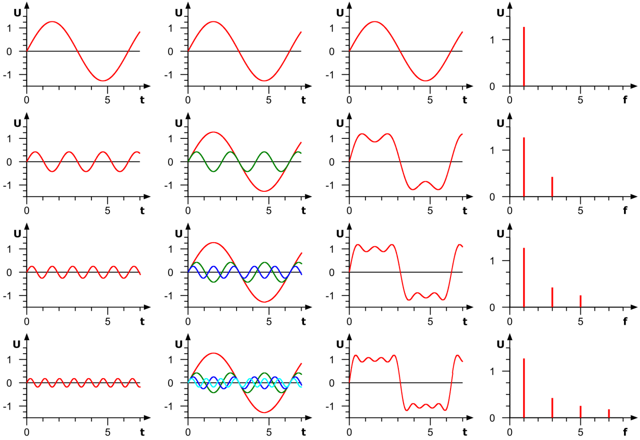
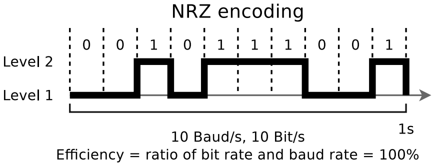


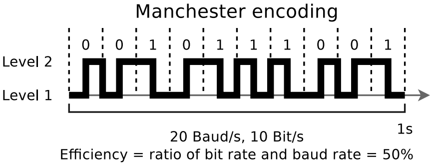
Image source: René Schwarz. Wikipedia (CC-BY-SA-1.0)

- The graphs in the 1st column show the oscillation, which is added in the respective row. The graphs in the 2nd column show all so far recognized oscillations, which are then added to the diagrams of the 3rd column, to reach as close as possible the signal which shall be generated. The more harmonics (multiples of the fundamental frequency) are taken into account, the more we get an ideal square-wave signal. The 4th column shows the amplitude spectrum, normalized to the fundamental frequency

Bit Rate and Baud Rate

- **Bit rate**: Number of transferred bits per time unit (bit/s or bps)
- **Baud rate**: Number of transferred symbols per time unit.
  - Initially, the baud rate indicated the signaling rate of a telegraph, thus the number of Morse code characters per second
- The ratio between bit rate and baud rate depends on the **line encoding scheme** used
  - Two examples. . .





- The line code specifies in computer networks the maximum number of signals that can be transmitted via the transmission media used
- The line code of a network technology is specified by the layer protocol used
- More information about line codes provides slide set 3

Bandwidth and Latency (1/2)

- Main factors, influencing the performance of a computer network:
  - **Bandwidth** (**throughput**)
  - **Latency** (**delay**)
- The **bandwidth** specifies how many bits can be transmitted within a period via the network
  - If a network has a bandwidth (throughput) of 1 Mbit/s, one million bits can be transmitted per second
    - Thus, a bit has a *width* of 1 μs
    - If the bandwidth is doubled, the number of bits that can be transmitted per second doubles too

Bandwidth and Latency (2/2)

- The **latency** of a network is the time, a message needs to travel from one end of the network to the most distant end

$$\text{Latency} = \text{Propagation delay} + \text{Transmission delay} + \text{Waiting time}$$

$$\text{Propagation delay} = \frac{\text{Distance}}{\text{Speed of light} * \text{Velocity factor}}$$

- Distance: Length of the network connection
- Speed of light: 299, 792, 458 m/s
- Velocity factor: Vacuum = 1, twisted pair cables = 0.6, optical fiber = 0.67, coaxial cables = 0.77

$$\text{Transmission delay} = \frac{\text{Message size}}{\text{Bandwidth}}$$

Transmission delay = 0, if the message consists only of a single bit

- Waiting times are caused by network devices (e.g. Switches)
  - They need to cache received data first before forwarding it

Waiting time = 0, if the network connection between sender and destination is just a single line or a single channel

Source: Larry L. Peterson, Bruce S. Davie. Computernetzwerke. dpunkt (2008)

Bandwidth-Delay Product

- Calculates the **volume of a network connection**
  - Signals cannot be transmitted with infinite speed via the transmission media
    - The propagation speed is in any event limited by the speed of light and it depends on the velocity factor of the transmission medium
  - The product of bandwidth and delay (latency) corresponds to the maximum number of bits that can reside inside the line between sender and receiver
- Example: A network with 100 Mbit/s bandwidth, and 10 ms latency

$$100,000,000\,\text{Bits/s} \times 0.01\,\text{s} = 1,000,000\,\text{Bits}$$

- There are a maximum number of 1,000,000 Bits inside the network line
  - This is equivalent to 125,000 Bytes (approx. 123 kB)

Protocols

- A **protocol** is the set of all previously made **agreements** between communication partners
  - These agreements include:
    - Rules for connection establishment and clearing
    - Method of synchronization between sender and receiver
    - Measures for the detection and treatment of transmission errors
    - Definition of valid messages (vocabulary)
    - Format and encoding of messages
- Protocols specify...
  - the **syntax** (= format of valid messages)
  - the **semantics** (= vocabulary and meaning of valid messages)

Reference Models

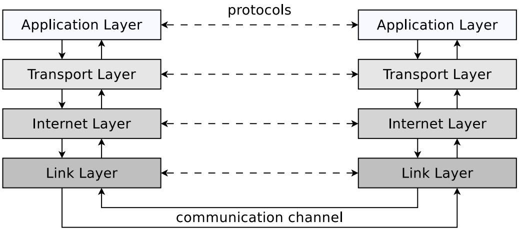
- Communication in computer networks is subdivided into **reference models**
- Each **layer** of a reference model handles a particular aspect of communication and offers **interfaces** to the overlying layer and underlying layer
- Each interface consists of a set of **operations**, which together define a **service**
- In the layers, the data is encapsulated ($\Longrightarrow$ **encapsulation**)
- Because each layer is complete in itself, single protocols can be modified or replaced without affecting all aspects of communication
- The most popular reference models are...
  - the **TCP/IP reference model**,
  - the **OSI reference model**
  - and the **hybrid reference model**

TCP/IP Reference Model or DoD Model

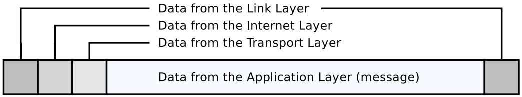
- Developed from 1970 onwards by the Department of Defense (DoD) in the Arpanet project
- Divides the required functionality to realize communication into 4 layers
- For each layer, it is specified, what functionality it provides
  - These requirements are implemented by communication protocols
    - Concrete implementation is not specified and can be implemented in different ways
    - Therefore, for each of the 4 layers, multiple protocols exist

Number	**Layer**	**Protocols (Examples)**
4	Application Layer	HTTP, FTP, SMTP, POP3, DNS, SSH, Telnet
3	Transport Layer	TCP, UDP
2	Internet Layer	IP (IPv4, IPv6), ICMP, IPsec, IPX
1	Link Layer	Ethernet, WLAN, ATM, FDDI, PPP, Token Ring

TCP/IP Reference Model – Message Structure

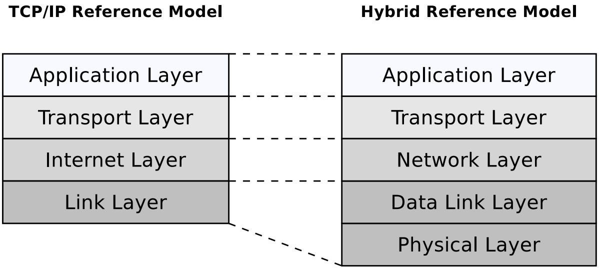


- Each layer adds additional information as **header** to the message
  - Some protocols (e.g. Ethernet) add in the link layer not only a header but also a **trailer** at the end of the message
  - The receiver analyzes the header (and trailer) on the same layer



Hybrid Reference Model

- The TCP/IP reference model is often presented in the literature (e.g. by Andrew S. Tanenbaum) as a 5-layer model
  - Reason: It makes sense to split the **Link Layer** into 2 layers, because they have different tasks
- This model is an extension of the TCP/IP model and is called **hybrid reference model**



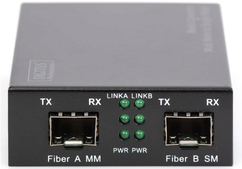
The objects of the individual layers will be discussed on the basis of the hybrid reference model

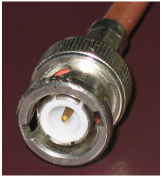
Physical Layer (see Slide Sets 2+3)

- **Transmits the ones and zeros**
  - **Physical connection** to the network
  - **Conversion of data in signals**
- Protocol and transmission medium specify among others:
  - How many bits can be transmitted per second?
  - Can transmission take place simultaneously in both directions?
- Devices: **Repeater**, **Hub** (Multiport Repeater)

Hybrid Reference Model

Hybrid Reference Model
Application Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer





Data Link Layer (see Slide Sets 4+5+6)

- Ensures error-free data exchange of **frames** between devices in physical networks
  - Detects transmission errors with **checksums**
  - Controls the access to the transmission medium (e.g. via CSMA/CD or CSMA/CA)
- Specifies physical network addresses (**MAC addresses**)

Hybrid Reference Model

Application Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

- At sender site: Packs the Network Layer packets into frames and transmits them (in a reliable way) via a physical network from one device to another
- At receiver site: Identifies frames in the bit stream from the Physical Layer
- Devices: **Bridges**, **Layer-2-Switches** (Multiport Bridges) and **Modems** connect physical networks

Network Layer (see Slide Sets 7+8)

- Forwards (*routes*) **packets** between logical networks (over physical networks)
    - For this *internetworking*, the Network Layer defines **logical addresses** (**IP addresses**)
    - Each IP packet is *routed* independently to its destination and the path is not recorded
- At sender site: Packs the segments of the Transport Layer in packets
- At receiver site: Unpacks the packets in the frames from the Data Link Layer
- **Routers** and **Layer-3-Switches** connect logical networks
- Usually the connectionless Internet Protocol (IP) is used
    - Other protocols (e.g. IPX) have been replaced by IP

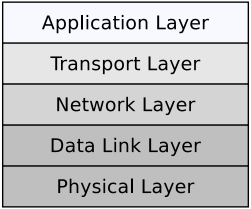
Hybrid Reference Model

Application Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Transport Layer (see Slide Set 9)

- Transports **segments** between processes on different devices via so-called end-to-end protocols
- At sender site: Packs the data of the Application Layer into segments
- At receiver site: Unpacks the segments inside the packets from the Network Layer

Hybrid Reference Model



- Addresses processes with **port numbers**
  - Data Link Layer and Network Layer implement physical and logical addressing of the network devices
- Transport protocols implement different forms of communication
  - UDP (User Datagram Protocol): Connectionless communication
  - TCP (Transport Control Protocol): Connection-oriented communication
    - Combination of TCP/IP = de facto standard for computer networks

Different Forms of Communication (see Slide Set 9)

- **Connectionless communication**
  - Analogous to a mailbox
  - Sender transmits messages without prior connection establishment
  - Disadvantage: No validation that a segment arrives at the destination
    - If validation is wanted, it must be implemented in the Application Layer
  - Benefit: Better throughput, because of lesser overhead
- **Connection-oriented communication**
  - Analogous to a telephone
  - Prior data exchange, a connection is established between sender and receiver
    - The connection is not terminated, even if no data is transmitted
  - After all data is exchanged, the connection becomes terminated by one of the communication partners
  - Implements flow control and congestion control
    - Ensures lossless segment delivery in the correct order
      $\Longrightarrow$ Successful delivery is guaranteed

Application Layer (see Slide Set 10)

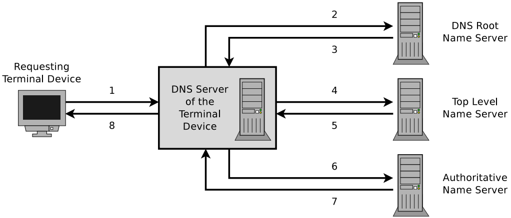
- Contains all protocols, that interact with the application programs (e.g. browser or email program)
- Here are the messages (e.g. HTML pages or emails), formated according to the used application protocol
- Some Application Layer protocols: HTTP, FTP, SMTP, POP3, DNS, SSH, Telnet

Hybrid Reference Model

Hybrid Reference Model
Application Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

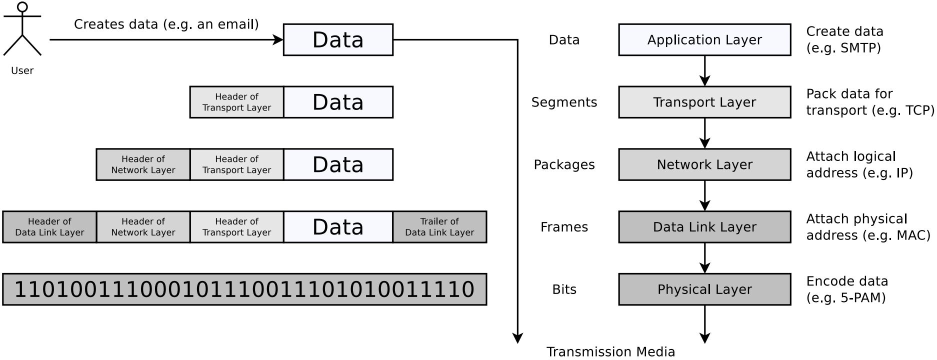
wikipedia.org (CC0)

pixabay.com (CC0)



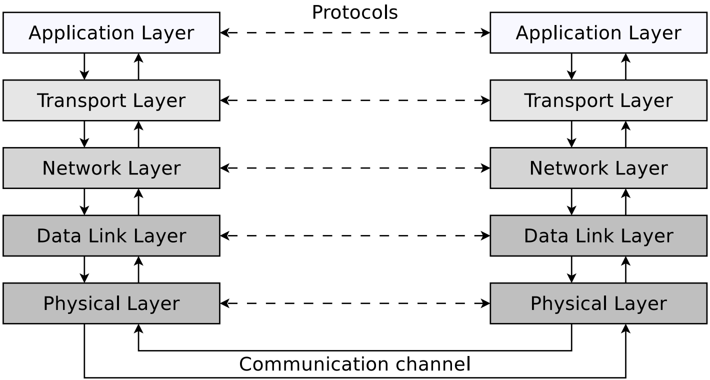
How Communication works (1/2)

- **Vertical communication**
  - Messages are packed from top to bottom layer by layer and extracted at the receiver in the reverse layer sequence
  - **Data encapsulation** and **de-encapsulation**



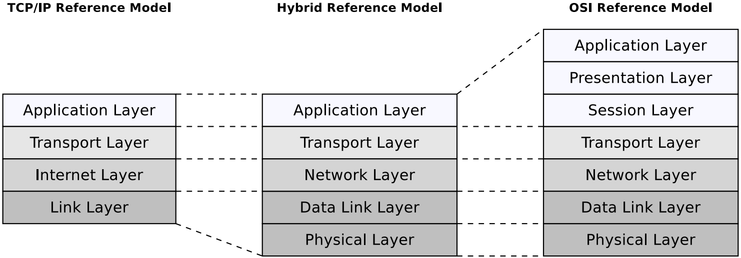
How Communication works (2/2)

- **Horizontal communication**
  - Equal protocol functions are used in the equivalent layers by sender and receiver



OSI Reference Model

- Some years after the TCP/IP reference model (1970s), the OSI reference model was developed from 1979 onwards
  - 1983: Standardized by the Intern. Organization for Standardization (ISO)
  - OSI = Open Systems Interconnection
- The structure is similar to the TCP/IP reference model
  - The OSI model implements 7 layers
- In contrast to the hybrid reference model, the Application Layer functionality is distributed across 3 layers in the OSI reference model



Session Layer

- **Controls the dialogues** (connections) between processes
  - Controls which node is allowed to send next
- Provides checkpointing which is useful for longer data transmissions to enable **synchronization**
  - If the connection fails, returning to a checkpoint avoids starting the transmission from the beginning
- Protocols that meet the required capabilities of the Session Layer are **Telnet** for remote controlling computers and **FTP** for file transmission
  - These protocols can be assigned to the Application Layer too
    - The Application Layer includes the protocols, used by the users' applications
  - FTP and Telnet are used directly by the relevant programs and not by abstract protocols of upper levels
    - Thus, it makes sense to assign these Session Layer protocols to the Application Layer

The Session Layer is seldom used in practice, because all tasks intended to this layer are fulfilled by Application Layer protocols today

Presentation Layer

- Contains rules for setting the **format (presentation) of messages**
  - The sender can notify the receiver that a message has a specific **format** (e.g. ASCII) to make conversion happen, which is perhaps necessary
  - Data records can be specified here with fields (e.g. name, student ID number...)
  - **Data types and their length** can be defined here
  - **Compression and encryption** could be implemented by this layer

The Presentation Layer is seldom used in practice, because all tasks intended to this layer are fulfilled by Application Layer protocols today

Reference Models – Summary

- Conclusion: The hybrid reference model illustrates the functioning of computer networks in a realistic way
  - It distinguishes between the Physical Layer and Data Link Layer
    - This is useful, because the objectives differ a lot
  - It does not subdivide the Application Layer
    - This is not useful and does not take place in practice
    - Functionalities, which are intended for Session Layer and Presentation Layer, are provided by Application Layer protocols and services
  - It combines the advantages of the TCP/IP reference model and the OSI reference model, without taking over their drawbacks