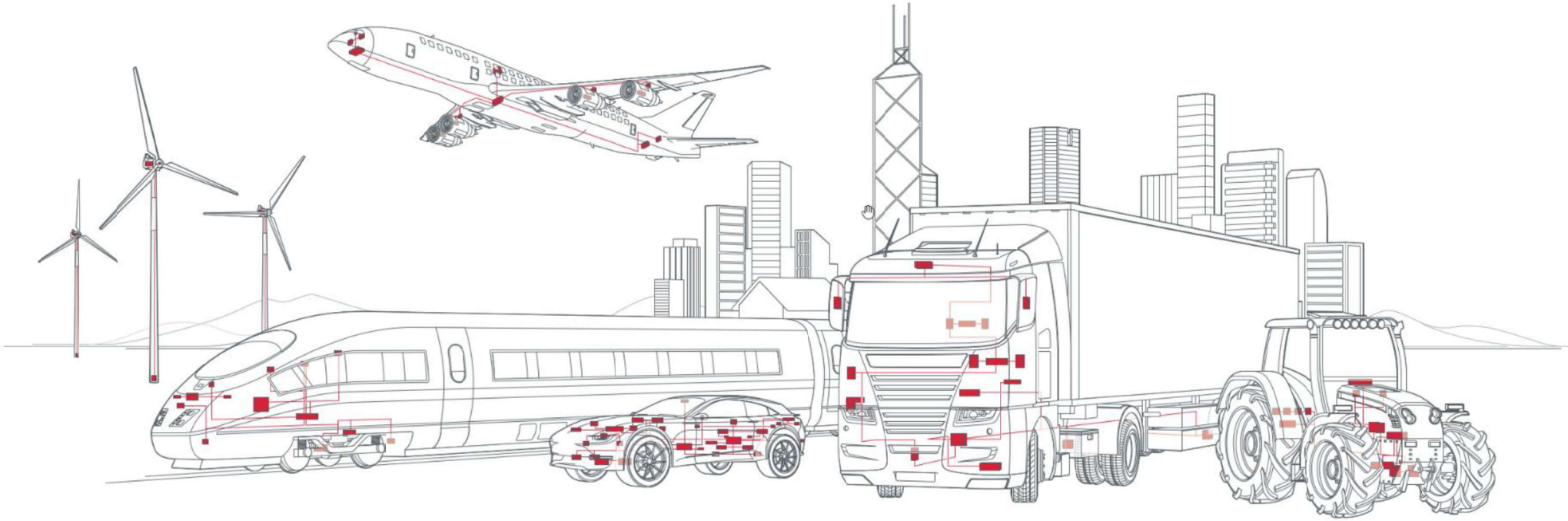


Fortgeschrittene Kommunikationssysteme (FKS)

A.1 – Fundamentals

V1.3 | 2022-03-26

Section 1 - Fundamentals

- **Introduction & Scope**
- Definitions
- OSI Model
- Summary

M2M (Machine-to-Machine)

M2M communication provides machines the ability to connect with each other via network and automatically exchange data over the network, often primarily in order to fulfill their basic purpose

- M2M networks are often closed networks or closed user groups and serve one specific application
- Often, domain specific protocol standards are used, designed to perfectly fulfill the need of the specific application case

Industry

- Energy
  - Metering
- Transportation
  - Automotive
  - Avionics
  - Logistics
- Production
  - Factory
  - Robotics

Public/Private

- Healthcare
  - Medical Machines
  - Body Sensors
- Telecommunication
  - Infrastructure
- Building
  - Security
  - Network
  - Automation

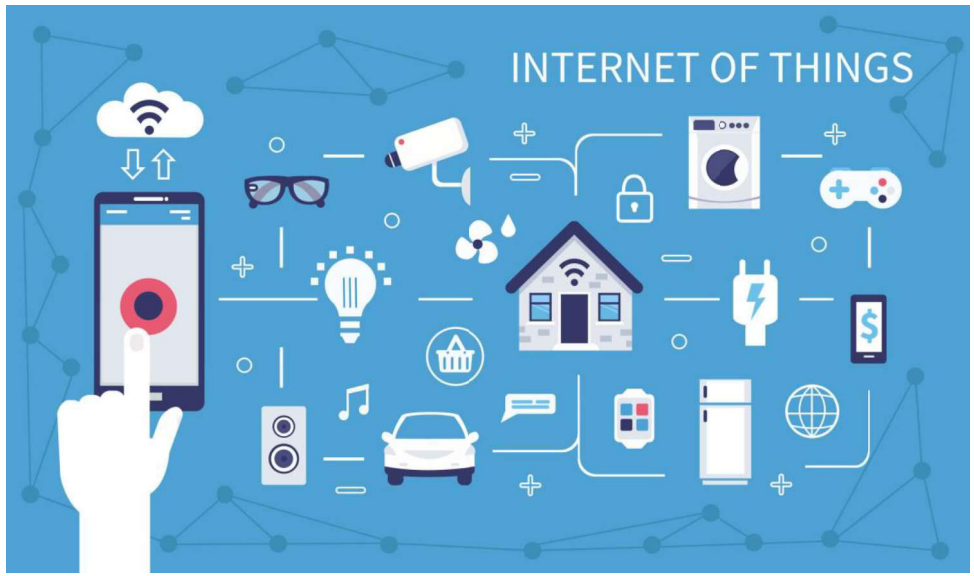
Other

- Space
  - Satellite
  - Rockets
- Consumer Electronics
  - Mobile Devices
  - Audio

IoT (Internet of Things)

IoT refers to a wider concept, which enables to interconnect physical and virtual objects with each other and making devices become more sophisticated and useful, often transforming their function entirely

- This networking may include a variety of equipment and devices, e.g. personal devices, consumer electronics, business machines or vehicles
- Communications can be established using a range of public technologies, from mobile networks (3G/4G) and WIFI, to Bluetooth and even wired Internet access
- Examples are fitness trackers, home automation (Alexa etc.), but also industrial automation, sensors, connected vehicles etc.



M2M is a subset of IoT, whereby …
→ **M2M** solutions are often narrowly defined for a specific function using dedicated or cellular networks, while
→ **IoT** based systems have much more flexibility and connectivity options

Distance Scaling of M2M Communication

Near Field Communication

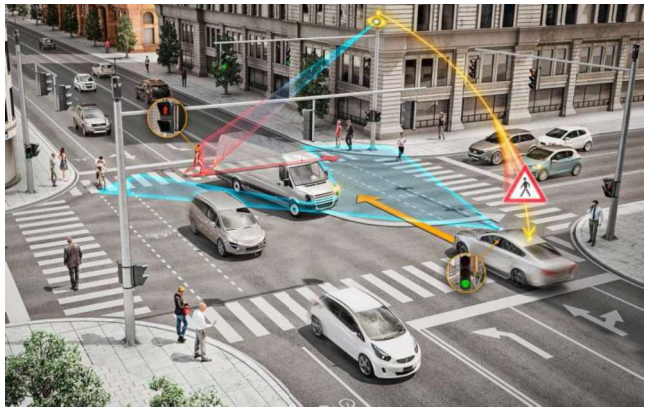
Distances: ~0,05 m

Medium: Electromagnetic, 13,56 MHz

Transmission Rate: 424 kBit/s (~10^5)

Technology: HF-RFID-Tags

Standard: ISO/IEC 14443 or ISO/IEC 15693



Car2x Communication (real-time)

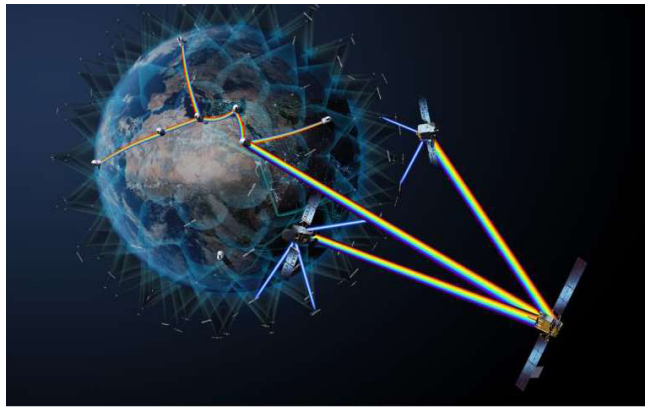
Distances: 100 m (real-time)

Medium: Electromagnetic, 5.85–5.925 GHz

Transmission Rate: 3 - 27 Mbit/s (~10^7)

Technology: ~WLAN

Standards: 802.11p - Wireless Access for Vehicular Environment (WAVE)



Orbit Communication

Distances: ~50.000 km

Medium: Optic

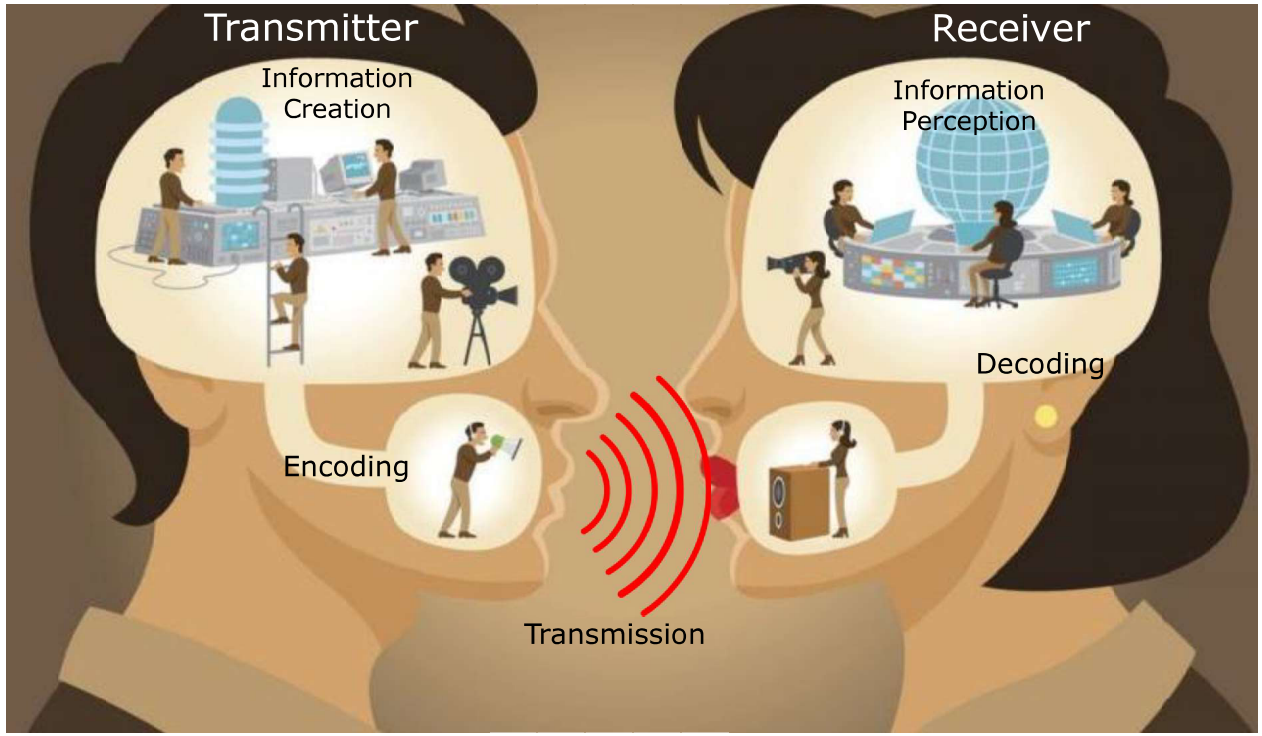
Transmission Rate: ~1 Tbit/s (10^12)

Technology: Laser

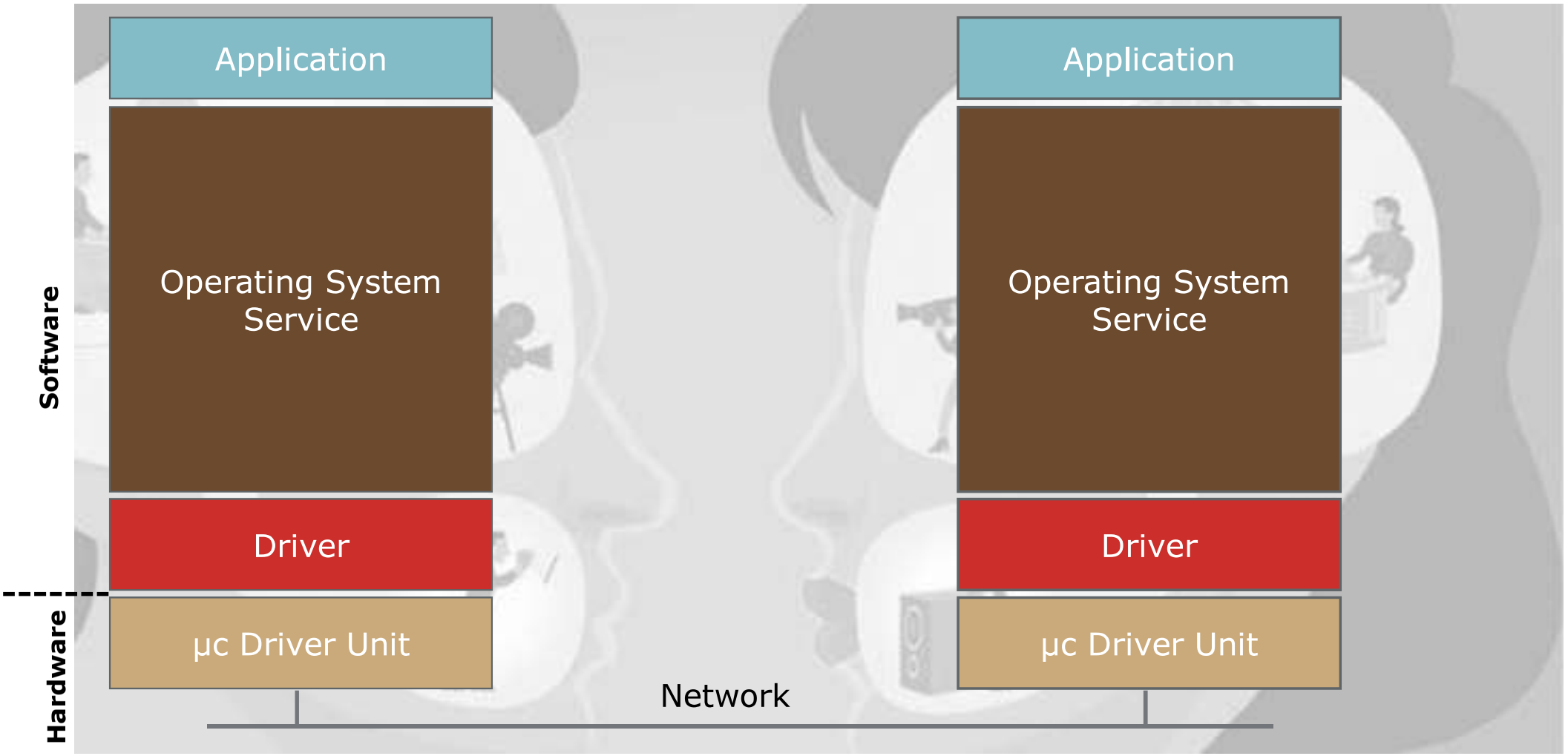
Reference: Research Project - ESA HydRON Project (2021)

Decomposition of Communicating Systems

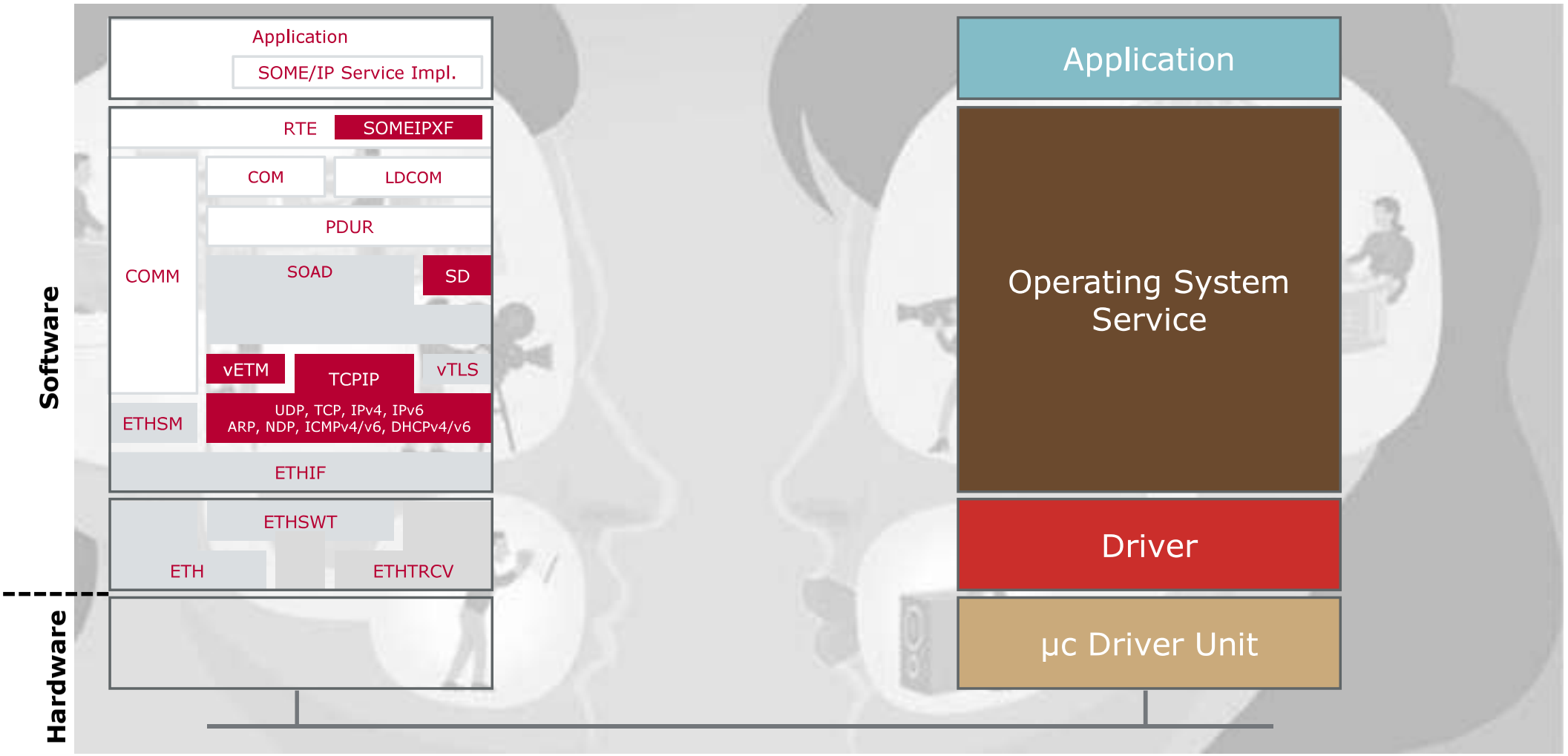
- **Transmitter**: Has an information that should be passed on
- **Information Creation**: Logical information is transferred from high-level/application control to communication driver
- **Encoding**: Information is transduced in a commonly agreed Protocol
- **Transmission**: Code is transferred as message via a physical medium from Transmitter to Receiver
- **Decoding**: Code is converted back from „Code" to logical information
- **Information Perception**: Information is processed by Receiver



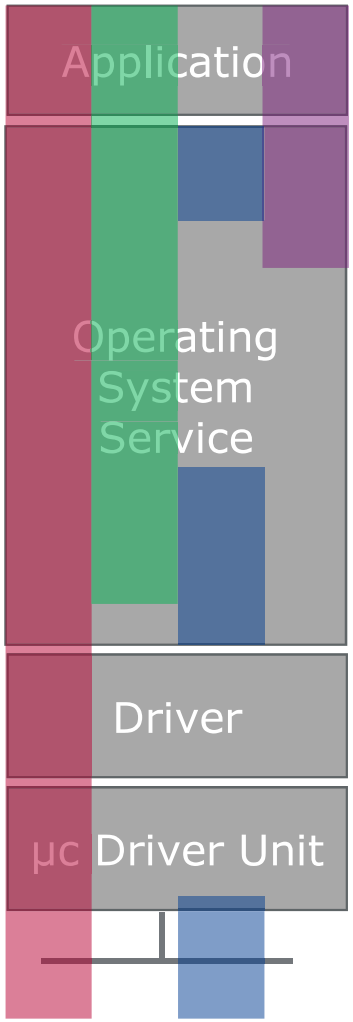
Example – Automotive Communicating Systems



Example – Automotive Ethernet Communicating Systems



Technical Scope / Schedule of this Lecture



Chapter A - Principles of Communication

- A1: Foundation of communication technology [MD]
- A2: Communication between Machines (Machine Networks) [MD]
- A3: Signal Encoding [MD]
- A4: Communication in Machines (Data Communication) [MD]
- A5: Safety & Security [AE]

Chapter B - Timing of Communication

- B1: Timing Concepts [AE]
- B2: Timing Analysis of Communication [AE]

Chapter C - Communication Protocols (Automotive)

- C1: CAN [AE]
- C2: Automotive Ethernet [MD]

Chapter D - Application in Vehicle Industry

- D1: Vehicle Communication [MD]
- D2: Communication in AUTOSAR Control Units [AE]
- D3: Safety in Vehicle Communication [AE]
- D4: Security in Vehicle Communication [TJ]
- D5: Gateways in Vehicle Communication [TJ]

MD = Michael Deubzer, AE = Arlinda Elmazi, TJ = Tobias Jennewein

Sommersemester 2022

Semesterzeitraum: 15.03.2022 - 30.09.2022

	Mo	Di	Mi	Do	Fr	Sa	So	KW
März		15	16	17	18	19	20	11
	21	22	23	24	25	26	27	12
	28	29	30	31				13
April					1	2	3	
	4	5	6	7	8	9	10	14
	11	12	13	14	15	16	17	15
	18	19	20	21	22	23	24	16
	25	26	27	28	29	30		17
Mai							1	
	2	3	4	5	6	7	8	18
	9	10	11	12	13	14	15	19
	16	17	18	19	20	21	22	20
	23	24	25	26	27	28	29	21
	30	31						22
Juni			1	2	3	4	5	
	6	7	8	9	10	11	12	23
	13	14	15	16	17	18	19	24
	20	21	22	23	24	25	26	25
	27	28	29	30				26
Juli					1	2	3	
	4	5	6 AW	7 RSDS	8 SLNZ	9	10	27
	11	12	13	14	15	16	17	28
	18	19	20	21	22	23	24	29
	25	26	27	28	29	30	31	30
	August							
	September							

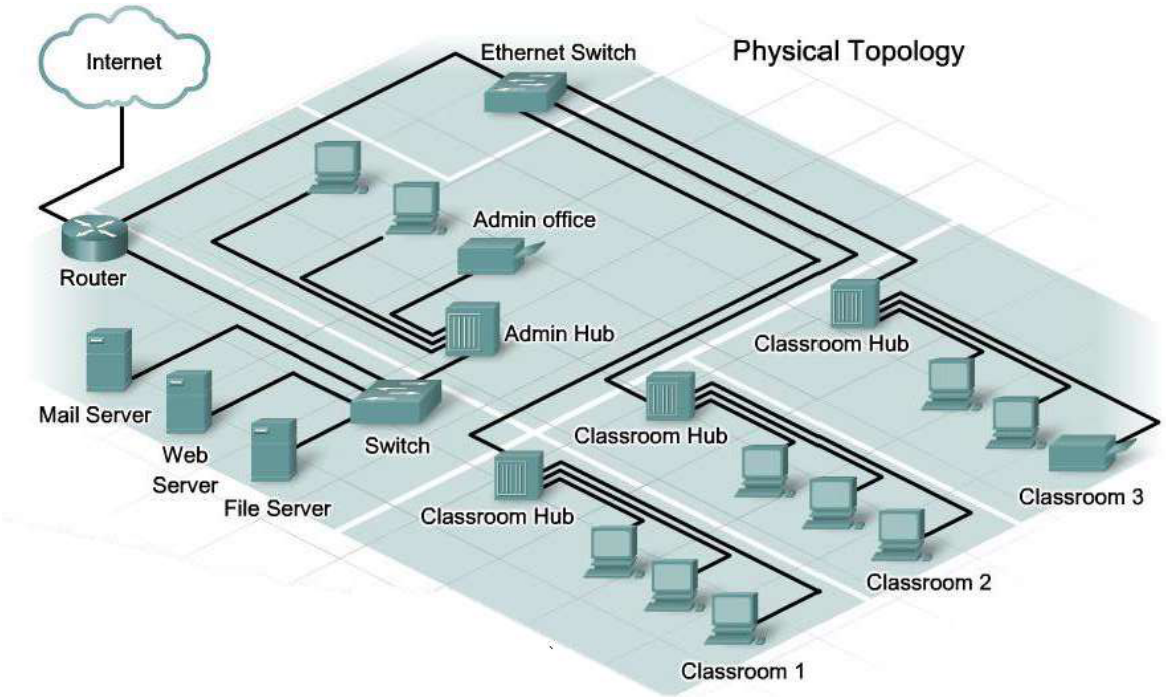
Summe Vorlesungstage							
14	15	17	14	14	-	-	
		(-1)	(-1)	(-1)			

Lecture unit assignment is only an orientation and is subject to change!

Section 1 - Fundamentals

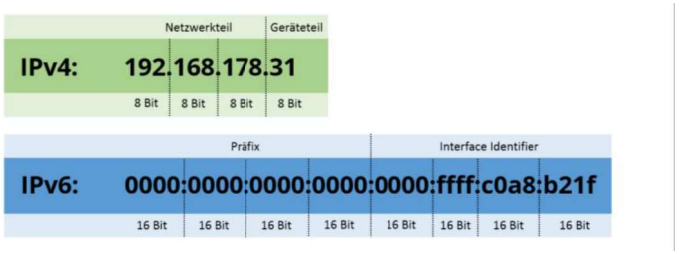
Physical Network Diagram

- Describes the physical **layout** of the network devices
- Consists of
  - Communicating Devices (Sender/Receiver)
  - Interconnection Devices (Switch, Router, …)
  - Cabling
- Purpose
  - Providing a bird's eye view of the network in its physical space, like a floorplan

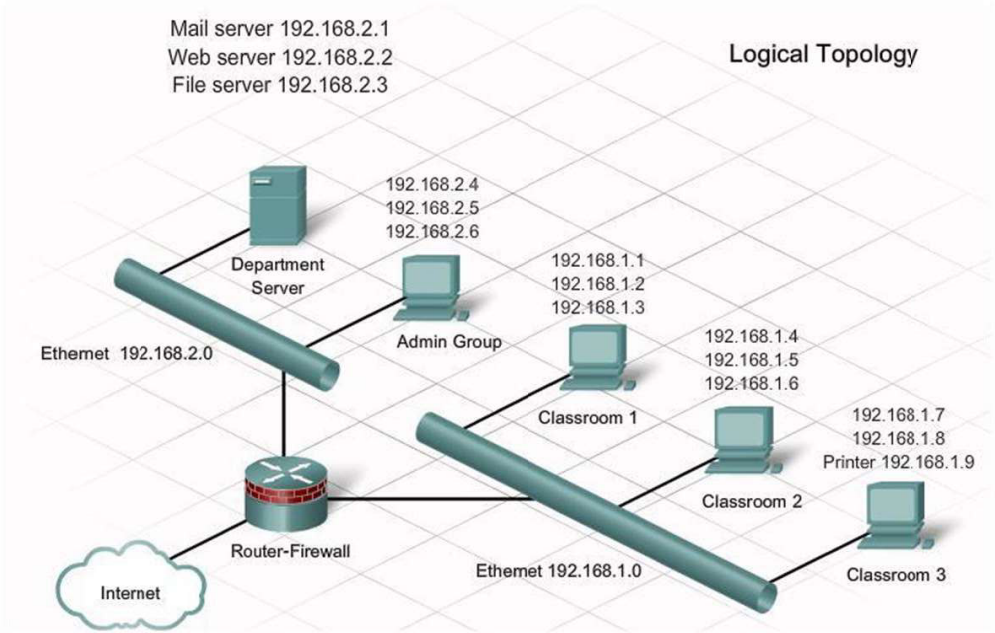


Logical Network Diagram

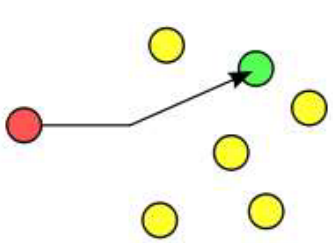
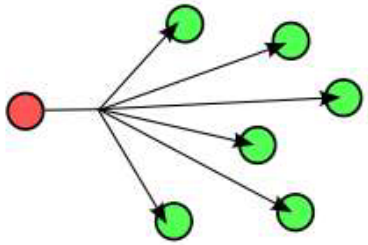
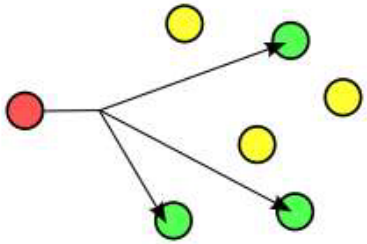
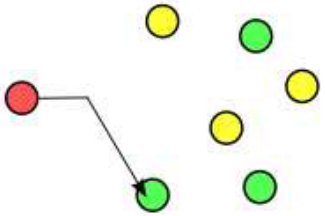
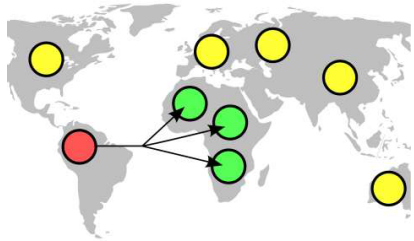
- Describes the way **information flows** through a network
- Shows subnets (including VLAN IDs, masks, and addresses), network devices like routers and firewalls, and routing protocols
- Logical Network Diagram correlates with Layer 3 of OSI Model (*see next sub section*)
- Showing IP Addresses of network devices
  - IPv4 or IPv6



- Purpose
  - Understanding the dataflow in a network system and finding the correct IP-Address

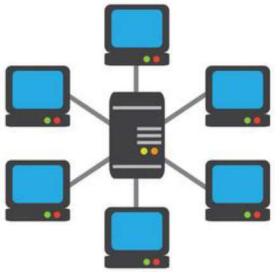


Routing Schemas

	Unicast	Broadcast	Multicast	Anycast	Geocast
					
Description	▸ One-to-one transmission ▸ Only uniquely identified endpoint receives the data	▸ One-to-all transmission ▸ all possible endpoints associated with the broadcast address	▸ One-to-N transmission ▸ Specific group of notes have expressed interest and receive the data	▸ One-to-one-of-N transmission ▸ Only one out of a group of notes receives the data – often the nearest to sender	▸ One-to-all-in-on-region transmission ▸ Only receiver in a certain geographical region receive the data
Typical Use	▸ TCP, UDP	▸ Message Passing Interface (MPI)	▸ IPv6	▸ Protecting Distributed-Denial-of-Service-Attacks	▸ IPv6

Topologies (1)

Star



A centralized node is located at the core of the network topology, in which all other nodes must communicate through. One of the most used topology.

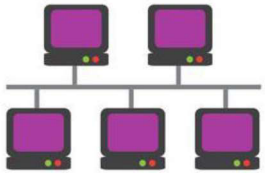
Advantages

- Installation and changes are easy
- Diagnosis: troubleshooting & detection of problems is easy
- Robustness: a failing device doesn't affect other devices
- Centralized management & monitoring

Drawbacks

- Single point of failure (centralized node)
- Performance depends on centralized node
- Cabling costs

Bus



Nodes make use of a single line for data transmission, where all are connected to. Often used in early age of network communication & small networks.

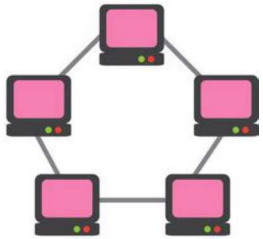
Advantages

- Simple installation - single communication line is shared
- Setup and expandability is easy
- Less costly - low cabling effort

Drawbacks

- Message Collision: medium has to be shared across all communication participants
- Diagnosis: identify a problem is hard
- Not efficient: All devices receiver all signals

Ring



Similar to bus topology, but closed loop. Not often used nowadays.

Advantages

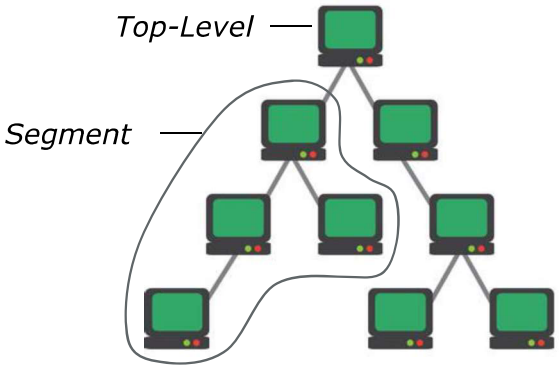
- Very orderly network - Less package collision
- Better throughput than Bus topology

Drawbacks

- Single point of failure – a link failure can fail the entire network
- Bad expandability – Changing a device can affect the network

Topologies (2)

Tree



Combination of Bus (Top-Level) and Star topology (Segments). Ideal, when one device acts as root device, e.g. network of diff. departments in one organization.

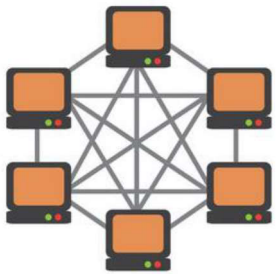
Advantages

- Good robustness – failing of one Segment doesn't lead to affect the rest of the network
- Easy fault identification
- Expandability – Scaling via adding secondary notes

Drawbacks

- Multiple points of failure – star & bus topology needs to be functional all times
- Difficult installation, maintenance & configuration
- High security standards are posed

Fully Connected



Each devices (n) is connected to all other devices of the network. Used for mission-critical network environments. Connections number $= n(n-1)/2$.

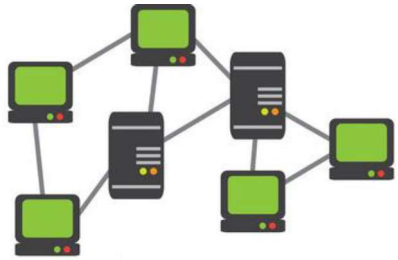
Advantages

- Very good Fault Tolerance due to redundant links
- Very good robustness – one failing device, doesn't affect the other devices
- Expandability – adding further devices doesn't affect the existing devices

Drawbacks

- Cost of implementation (Cabling, Ports)
- Complicated implementation and maintenance

Mesh



Similar to Fully Connected topology, but only a part of devices is connected to each other. Often used in high-availability environments.

Advantages

- Good Fault Tolerance – slightly lower as when Fully Connected
- Expandability is easy
- Lower costs as Fully Connected

Drawbacks

- Complex structure
- Complicated implementation and maintenance

RAM(S) (EN 50126) for Computer Networks

- **Maintainability**

*Ability to be **timely and easily** maintained (including servicing, inspection and check, repair and/or modification)*

  - Measure: probability in which a product / system can be repaired following a failure within a specific time frame

- **Reliability**

*Ability of a communication system to **function** under stated conditions for a specified **period of time***

  - Measure: probability in which a system will not experience an unplanned outage

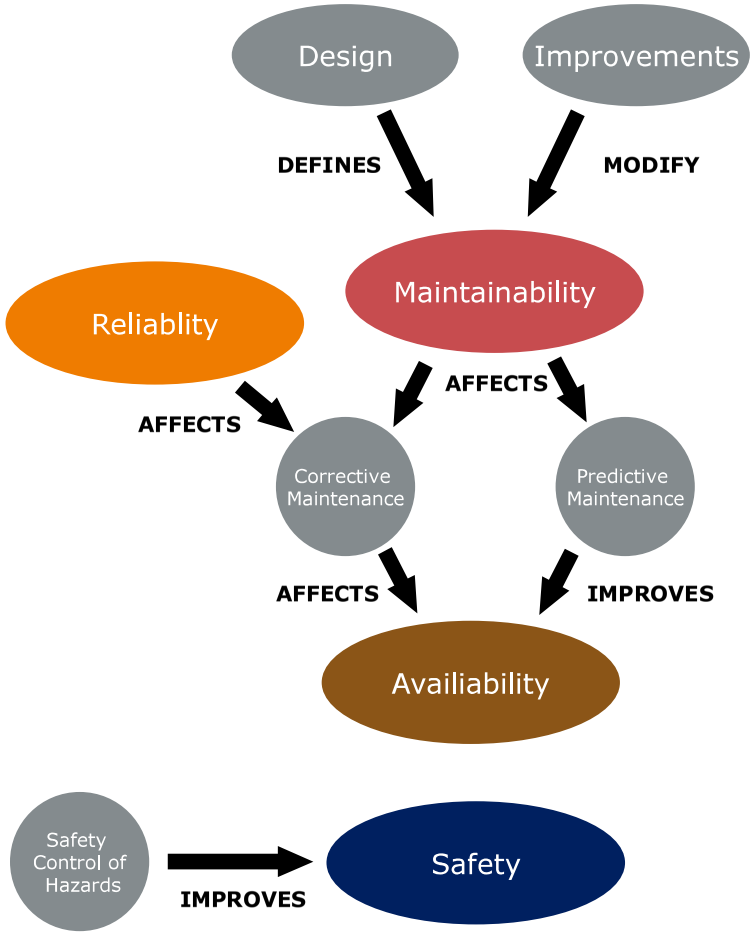
- **Availability**

*Ability to keep a **functioning state** in the given environment*

  - Measure: probability in which the system is working in a functioning state when required, including both planned and unplanned outages

- **Safety**

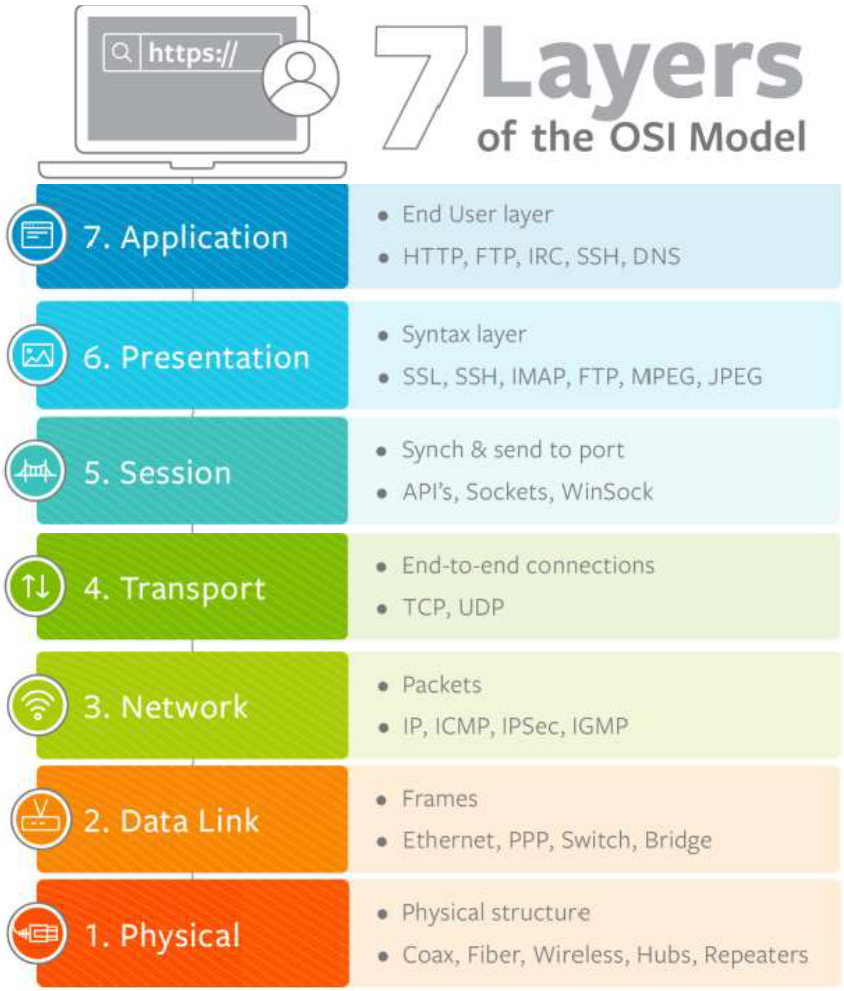
*Ability **not to harm people**, the environment, or any assets during a whole life cycle.*



Section 2 - Coding

OSI Reference Model (7 Layer Model)

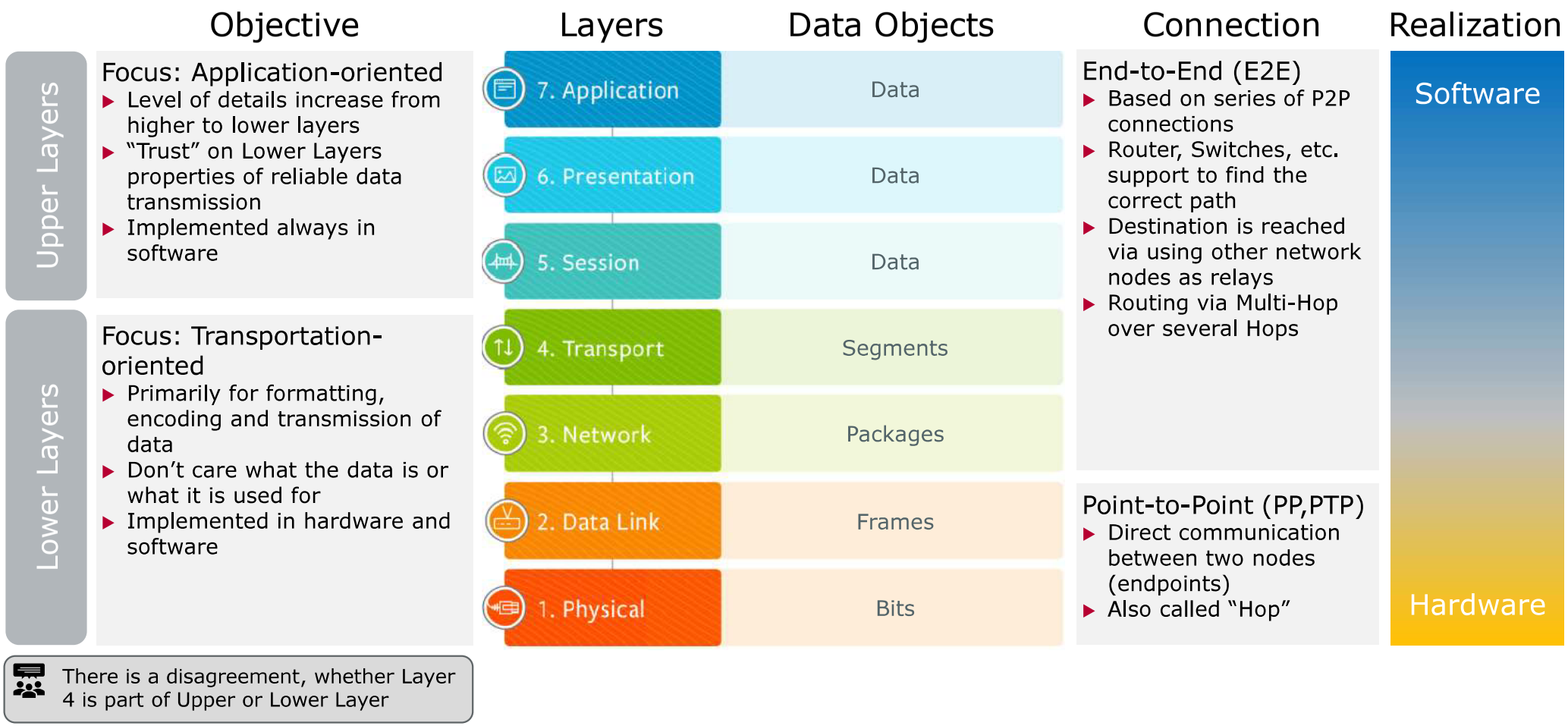
- Open Systems Interconnection (OSI) model is a **reference model** for network protocols
- It was developed in 1977 and **since 1984**, it's maintained by the International Organization for Standardization (**ISO**) as standard
- Objective is to describe communication across any technical systems in a **standardized schema**
- As there are various **functional** (correctness, order, …) and **non-functional** (safety, security, timing, efficiency) **requirements**, the OSI model is divided in a **Layer Model**, addressing different competences of a communication channel
- Each of the **7 layers** is well defined in regard of objectives and interfaces, which allows to realize one layer via different technologies
- Each layer relies on the next lower layer and provides services to the next higher layer



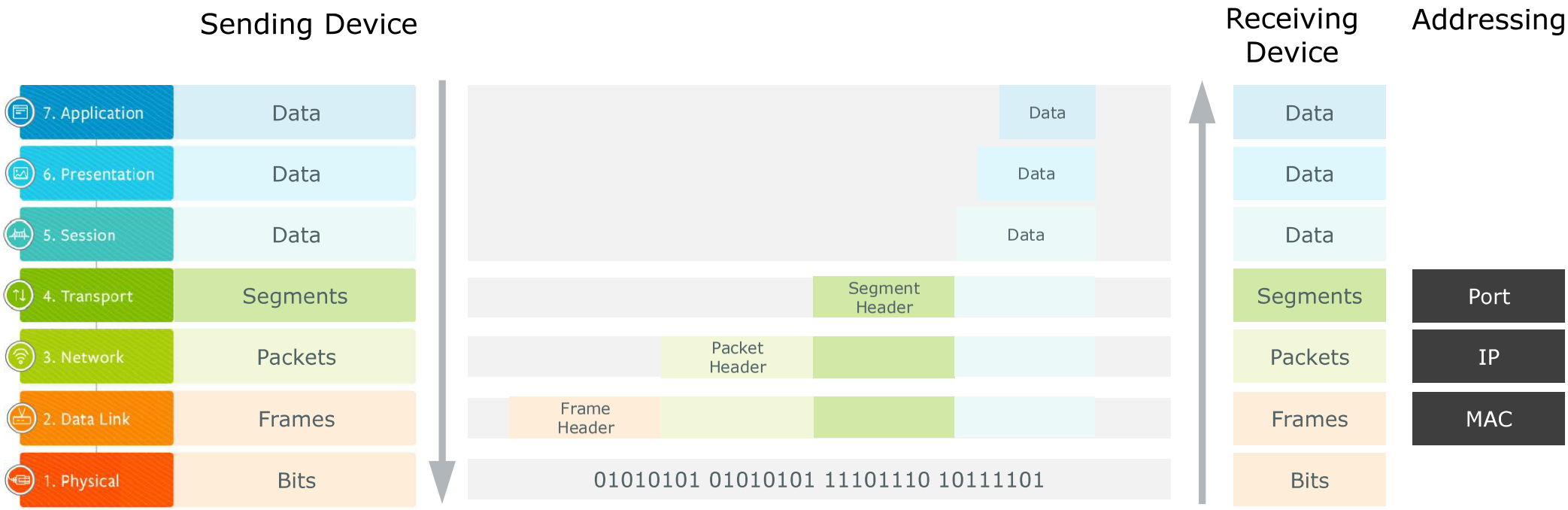
Further Information https://osi-model.com/

*„**P**lease **D**o **N**ot **T**hrow **S**alami **P**izza **A**way!"*

Structure


Objective
Layers
Data Objects
Connection
Realization
Upper Layers
Focus: Application-oriented
Level of details increase from higher to lower layers
"Trust" on Lower Layers properties of reliable data transmission
Implemented always in software
Lower Layers
Focus: Transportation-oriented
Primarily for formatting, encoding and transmission of data
Don't care what the data is or what it is used for
Implemented in hardware and software
7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical
Data
Data
Data
Segments
Packages
Frames
Bits
End-to-End (E2E)
Based on series of P2P connections
Router, Switches, etc. support to find the correct path
Destination is reached via using other network nodes as relays
Routing via Multi-Hop over several Hops
Point-to-Point (PP,PTP)
Direct communication between two nodes (endpoints)
Also called "Hop"
Software
Hardware
There is a disagreement, whether Layer 4 is part of Upper or Lower Layer

Transmission



- Sender encodes application data from high level abstract information to low level binary data
- Data is packed in different **Protocol Data Units** (PDU), each design to fulfill the purpose of the corresponding layer
- Receiver decodes the application information from low level binary data to high level abstract information

(0) Medium (non official OSI Layer)

Objective

- Physical realization of information transmission via electric, electromagnetic, optic or acoustic medium

Requirements on Medium

- Good quality of signal transmission
- Flexibility or scalability over time
- Easy and non-time consuming adds and changes
- Easy maintenance

Physical Components

- e.g. Cable, Connector, Transceiver, T-Piece, Terminating Resistors, Antenna, Hub

Examples

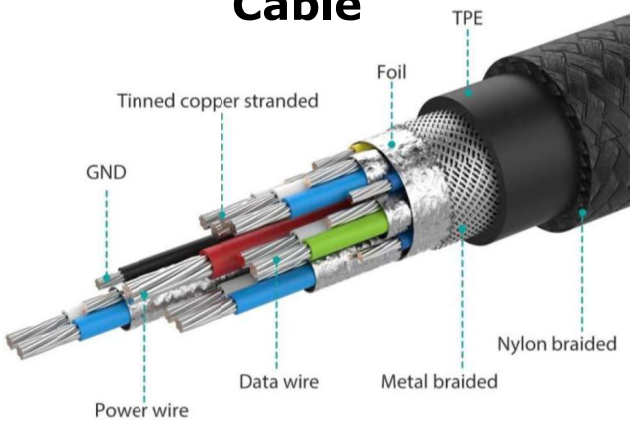
- Electric Connectors: USB-* Connector

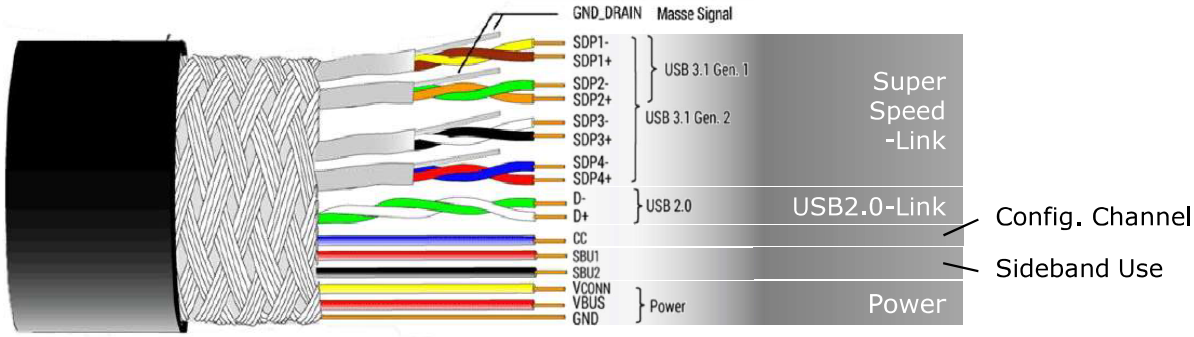
Connector Guide:
www.cablestogo.com/learning/connector-guides

Connector Electronic Basics:
https://learn.sparkfun.com/tutorials/connector-basics/all

(0) Examples of an Electrical Medium: USB-C

Cable



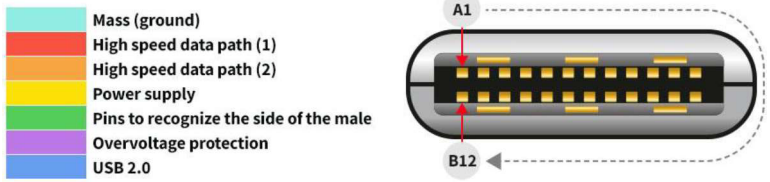


- **USB3.x - SuperSpeed-Link**
  - Pair(s) of shielded Twisted-Pair / Coaxial cable
  - Data transfer in Dual Simplex-Mode
- **USB2.0**: Downwards compatibility
- **Configuration Channel**: Identifying connection & orientation, …
- **Sideband Use**: Analog audio signals
- **Power**: Up to 5A charging current

Connector

Duplication of pins for reverse polarity protection

A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12
GND	TX1+	TX1-	VBUS	CC1	D+	D-	SBU1	VBUS	RX2-	RX2+	GND
GND	RX1+	RX1-	VBUS	SBU2	D-	D+	CC2	VBUS	TX2-	TX2+	GND
B12	B11	B10	B9	B8	B7	B6	B5	B4	B3	B2	B1



USB3.1 Article (dt.): https://kompendium.infotip.de/usb_3.1_gen_2_usb_typ-c_verbinder.html

(1) Physical Layer (dt. Bitübertragungsschicht)

Objective

- Physical transmission of raw bit information

Actions/Tasks

- Activating, maintaining, deactivating a physical connection between sender and receiver
- Executing the transport of bits

Mechanisms

- Encoding and decoding dynamic behavior of the physical medium for transferring information from one sender to receiver
  - Modulation of Frequency, Amplitudes, Phase Shift, …

Physical Components

- Transmission: e.g. Repeater, Hub, Amplifier

Examples

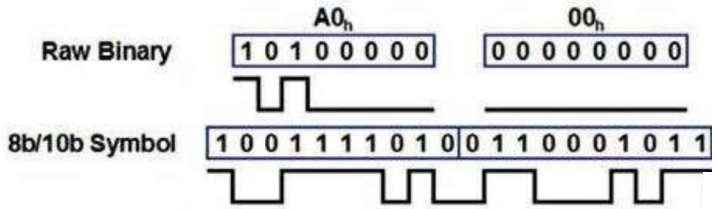
- Electric Connectors: RS 232, RJ45

(1) Examples of a Physical Layer: USB 3.0

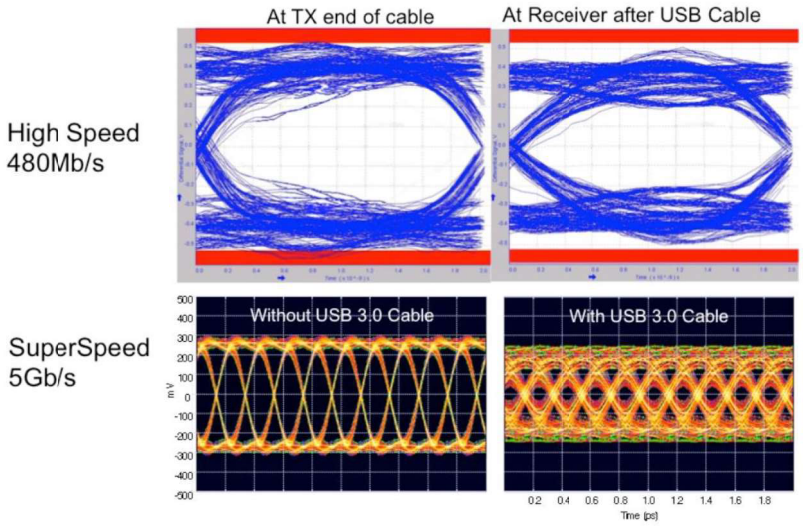
Physical Medium

- Data line realized via two data pairs (e.g. SDP1+, SDP1-)
  - Transmit path
  - Receive path
- Data Link Layer provides 8 bit information, which is transformed via 8b10b encoding to 10 bit information (25% Overhead), for the purpose of
  - DC balancing (dt. Gleichspannungsausgleich) – Relation between "0" and "1" is exactly 50% in long term consideration
  - Clock recovery (dt. Taktrückgewinnung) - Reconstructing the transmission frequency of Sender at Receiver side from sequence of bit changes
- Transmitter functions of the Physical Layer include
  - Data scrambling
    - Rearrangement of bit sequence in order to meet the physical requirements of the channel
  - 8b10b encoding Serialization
- Receiver functions of the Physical Layer include
  - De-serialization
  - 8b10b decoding
  - Data descrambling
  - Receiver clock
  - Data recovery
- Signal modulation in practice
  - 1.000 mV **peak-to-peak** (pk-pk) signal at Sender source; 100 ps Pulse Width
  - 600 mV pk-pk without USB cable
  - 500 mV pk-pk with USB cable -> only 100 mV pk-pk / 100ps wide eye opening

Example: 8b10b Encoding



Example: Eye pattern (dt. Augendiagramm) with different cables



(2) Data Link Layer (dt. Sicherungsschicht)

Objective

- **Physical addressing** of connected devices
- **Scheduling** the access to the physical medium
- Enabling a **reliable transmission** (free of failure)

Actions/Tasks

- Framing: Aggregating Bits to **Frames** with a defined **Source & Destination**
- Multiplexing: **Routing** different Protocols over one Physical Layer
- Flow Control: **Acknowledgement** mechanism between Receiver and Sender
- Error Control: Adding Checksums for **identifying data corruption** of Frames

Sub-Layers

- Layer 2a: Media Access Control (MAC)
- Layer 2b: Logical Link Control (LLC)

Physical Components

- e.g. Switch, Bridge

HUB vs. SWITCH vs. ROUTER (einfach erklärt)
https://youtu.be/zFfattg5gd8

Examples

- HDLC (used for ISDN, GSM), IEEE 802.5 (Token Ring)

(2.A) Data Link Sub-Layer: MAC

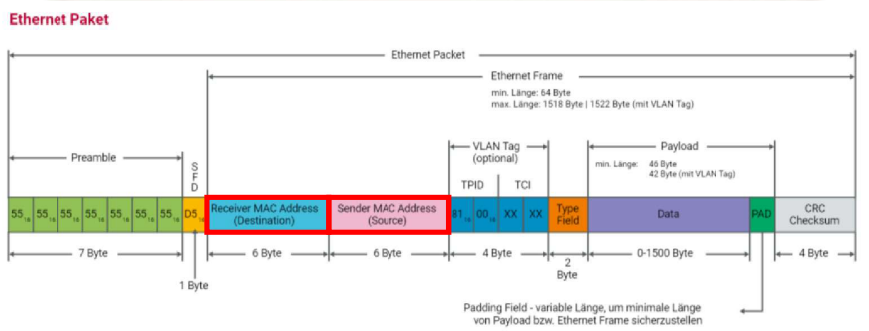
2. Data Link

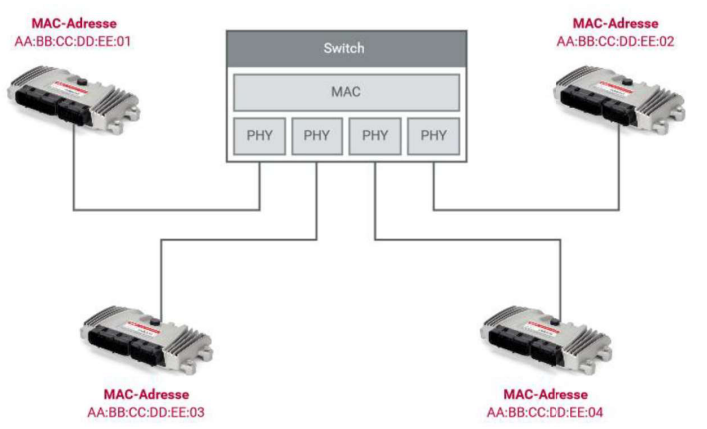
Media Access Control (MAC)

*Unique identifier, "burned" into hardware of a network interface controller. Also called **Physical Address** or **Device Address**.*

- Each device, connected to a network has a unique MAC address per interface
- MAC-address is sent at the beginning of each data frame
  - Frames include information on Source [1] and Destination [1…n] MAC address
  - Unicast-, Multicast- or Broadcast-Addresses are possible
- Data-Link layer enables with MAC addressing a point-to-point connection between devices
- Switch has a table {network-interface; MAC address}
- Device filters relevant data frames
- Protection against errors, e.g. by generating and checking frame check sums
- Control of access to the physical transmission medium
  - Collision Recovery

Identifying your MAC Address at Windows system
CMD -> „ipconfig /all" (Physical Address)





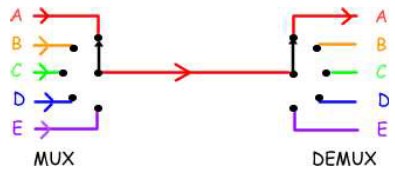
(2.B) Data Link Sub-Layer: LLC

Logical Link Control (LLC)

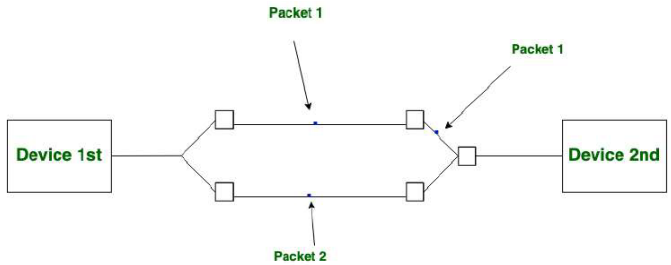
Responsible for Multiplexing and Flow Control and implemented in software.

- **Multiplexing** of protocols
  - A) **Aggregating multiple digital signals** to **one combined signal**, which can be transferred over one shared medium
  - B) **Decomposing** the combined signal to its individual signals
- Providing **Flow Control Services** for (3) Network Layer
  - A) **Un**acknowledged connection**less** services
    - **No connection is established** between the two stations in advance
    - Sender transmits frames **without waiting for confirmation** of receiver
    - **Data lost is not corrected** → Fast transmission
      - (if required) higher OSI Levels have to correct incorrect data
  - B) Acknowledged connection**less** services
    - **Receiver confirms** each received frame
    - **Sender waits for this acknowledge** of receiver before sending further frames
  - C) **Connection-oriented** services
    - **Virtual circuit** between sender and receiver is established
      - This path stays for the complete duration of the connection
    - Receiver confirmation received frames / Sender transfers next frames after receiving acknowledgement
    - Connection is terminated at end of communication

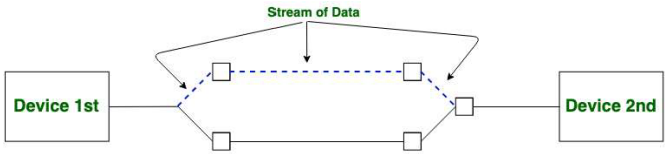
Multiplexing



Connectionless Service



Connection-oriented Service



(3) Network Layer (dt. Vermittlungsschicht)

Objective

- Enabling **different networks** to connect with each other

Actions/Tasks

- Switching connections and providing packet-orient services for relaying of data packets

Mechanisms

- Routing: Determining suitable route from source to destination
- Logical Addressing: Unique addressing for identifying each device (Sender, Receiver)
  - In extension to Layer 2 **across different networks**
  - IP address is unique inside one network, but is non-unique across all networks

Physical Components

- e.g. Router, Layer-3-Switch

Examples

- Internet Protocol (IPv4/IPv6)
- Open Shortest Path First (OSPF)

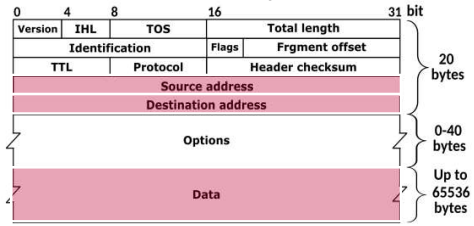
(3) Principles of Network Layer: Routing

3. Network

Package

- Device sends Package (e.g. IPv4) to Router, including
  - Source
  - Destination (of different network)
  - Data
  - Further Information

Example: IPv4 Package

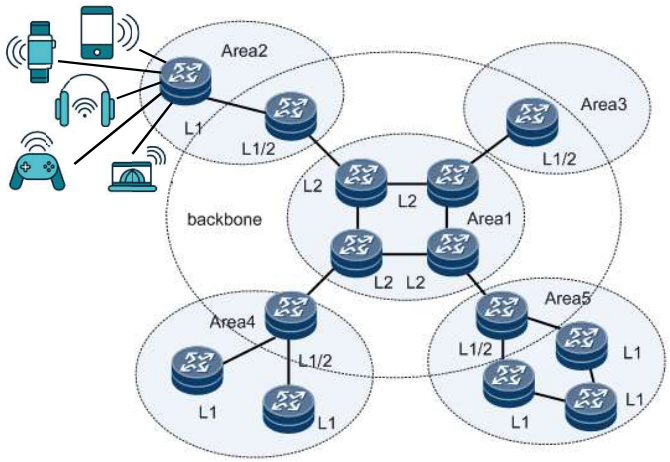


Routing

- Routing Table defines the path for connecting a device with another device or network via a Hop
  - A table entry provides for an IP Address-range of destination device(s) which router and interface has to be used
  - Additionally, each entry includes a metric on the cost of the Hop
- Router Levels
  - Level-1 (L1): intra-area routing
    - Establishing of neighborship only with L1 or L1/2 routers
    - Default route for pointing towards nearest L1/2 router
  - Level-2 (L2): inter-area routing
  - Level-1-2 (L1/2): intra- and inter-area routing
- Router determines best path to destination
  - e.g. Dijkstra-Algorithm

Example: Routing Table

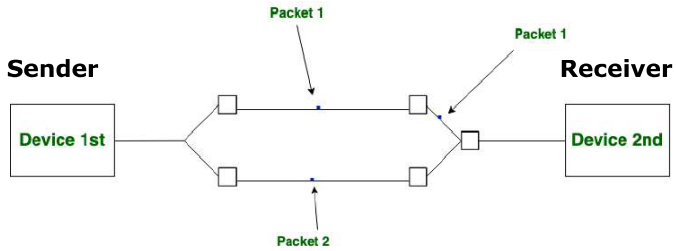
Network destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.100	10
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.0.0	255.255.255.0	192.168.0.100	192.168.0.100	10
192.168.0.100	255.255.255.255	127.0.0.1	127.0.0.1	10
192.168.0.1	255.255.255.255	192.168.0.100	192.168.0.100	10



Der DIJKSTRA ALGORITHMUS
https://youtu.be/KiOso3VE-vI

(3) Principles of Network Layer: Connection Services

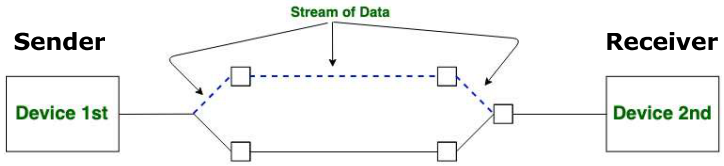
Connectionless Services



Virtual circuit between Sender and Receiver is established in advance

- For "bursty" communication
- Congestion (dt. *Stau*) is not possible
- No guarantee of reliability
- Overload is possible
- Packet may follow different paths

Connection-oriented Services



No connection is established between the Source and Destination stations in advance

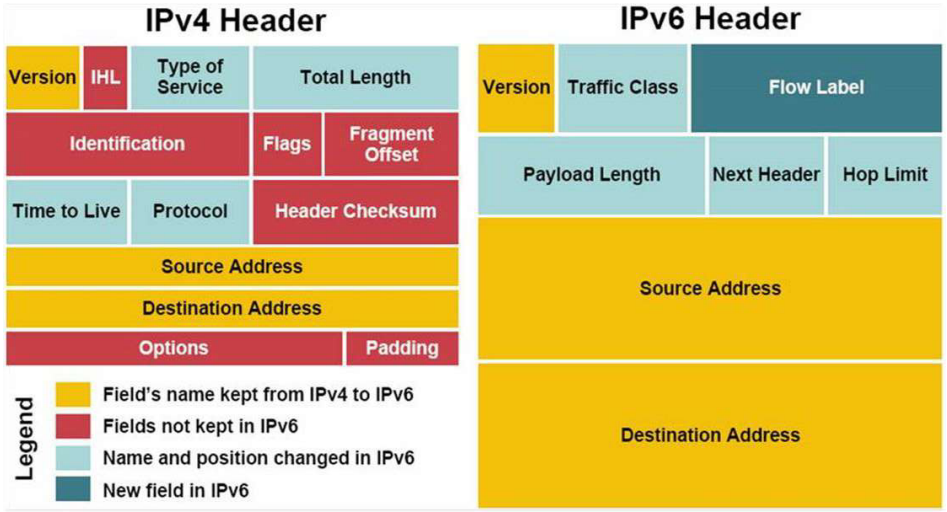
- For long and steady communication
- Congestion is possible
- Guarantee of reliability
- No overload possible
- All packets follow the same path

(3) Examples of Network Layer: IPv4, IPv6

IPv6 replaces IPv4

IPv6 brings some key features to improve the limitations exposed by IPv4. The new IP standard extends IPv4 in several important aspects:

- Upgrade from 32 to 128-bit addressing
  - 3,4·10^38 instead of 4,3·10^9 addresses
- 6-to-4 tunnel (allows IPv6 nodes to connect to outside IPv6 services over an IPv4 network)
- New, simplified IPv6 header format
- Built-in security
- Better support for QoS
- New protocol for neighboring node interaction
- Extensibility for new features using extension headers



IPv4 vs. IPv6 - Wo liegen die Unterschiede und was ist "besser"?
https://youtu.be/OjBJvXcuE-I

(4) Transportation Layer (dt. Transportschicht)

Objective

- **Ensuring transfer** of a **variable-length** data sequences (Segments) from a source to a destination host while maintaining **Quality of Service** (QoS)

Actions/Tasks

- Segmentation / Reassembly: Slicing application data packages into transferable frames and re-connecting them
- Control the reliability of a given connection
  - Reliable/Unreliable data transfer (Depending on Connection Mode)

Mechanisms

- Flow control: How much data should be sent where and at what rate between sender and receiver
- Error control: Acknowledgement of successful data transmission / Re-send in case of errors
- Load Balancing and Congestion Avoidance

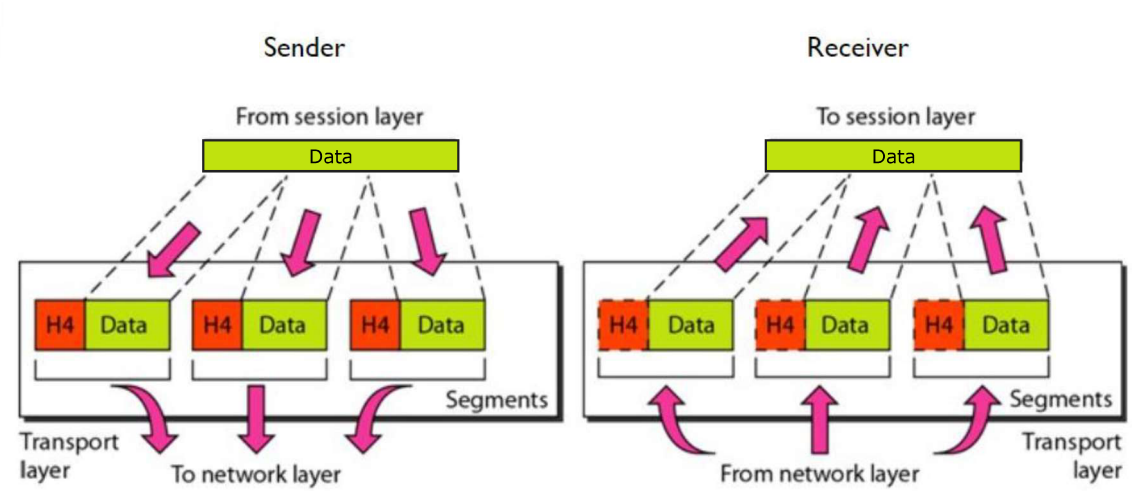
Examples

- Ports / TCP, UDP

(4) Examples of Transportation Layer: Segmentation / Reassembly

4. Transport

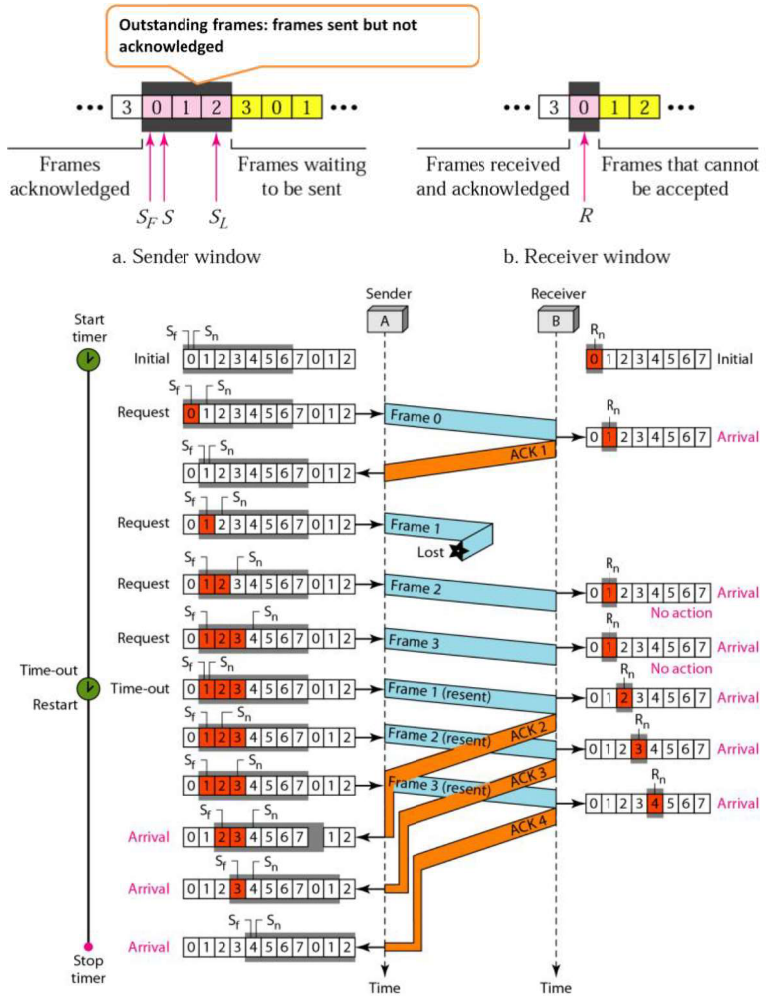
- Segmentation
  - Transportation Layer protocol breaks data unit form Session Layer down into transferable size (Segment)
  - **Maximum Transmission Unit** (MTU) – defines largest Frame size a given network will carry
- Reassembly
  - Receiver reconstructs data unit from correctly transmitted Segments



(4) Examples of Transportation Layer: Flow Control

Examples

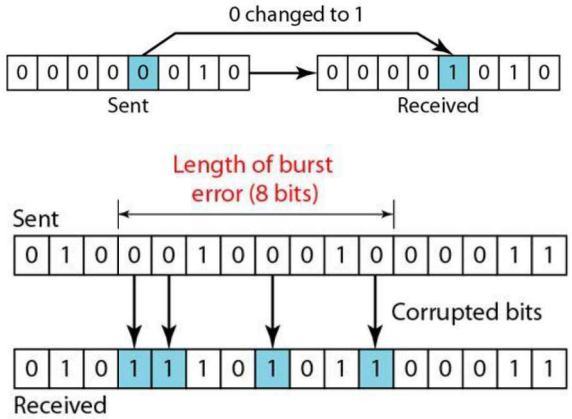
- *Stop-and-Wait*
  - Transmitting frame-by-frame, and waiting for ACK **of each individual frame** before sending the next one
- *Go-Back-N ARQ*
  1. The **Sender** (A) starts sending Frames with the **First Frame** (SF) from a **Sender Window** till **Last Frame** (SL) and starts a timer with each **Sent Frame** (S)
  2. The **Receiver** (B) sends a positive **Acknowledge** (ACK) if a **Received Frame** (R) has arrived safe and in order
  3. If a Frame is damaged or out of order, the **Receiver** is **silent** and will **discard all subsequent Frames**
  4. When the timer of an unacknowledged Frame at the Sender site is **expired**, the **Sender goes back** and **resents all Frames**, beginning with the one with expired timer (that is why the protocol is called Go-Back-N ARQ)
  5. The **Receiver** doesn't have to acknowledge each Frame received, but it can send cumulative ACK for several Frames
  6. (Thus, the receive window is an abstract concept defining an imaginary box of size 1 with one single variable Rn.)
  7. The window slides when a correct frame has arrived; sliding occurs one slot at a time



(4) Examples of Transportation Layer: Error Control

Examples of Error Types

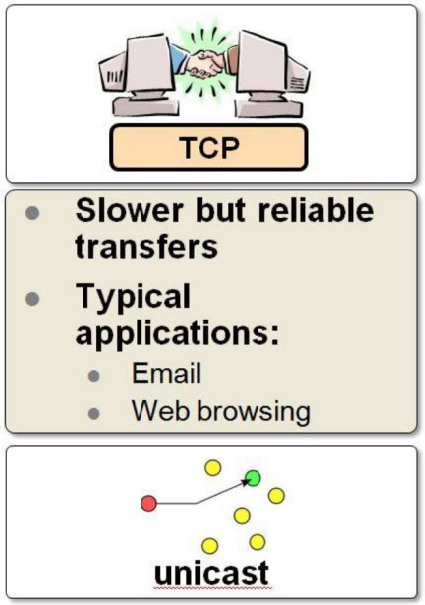
- *Single Bit Error*
  - When there is a change in only one bit of the sender's data then it is called a single bit error
- *Burst Error*
  - When there is a change in two or more bits of the sender's data then it is called a burst error

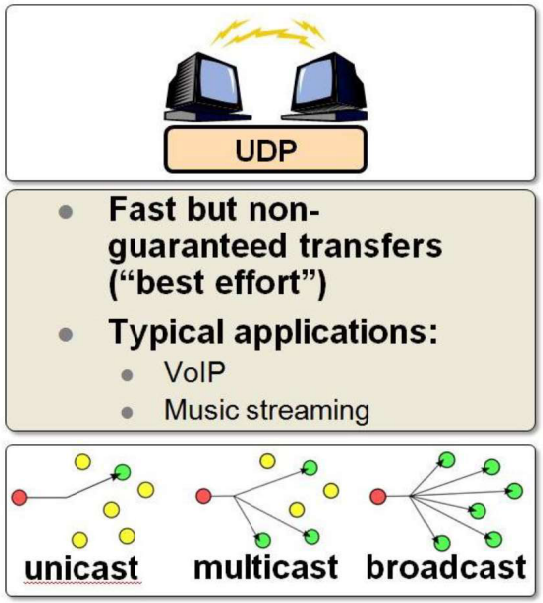


Phases in Error Control

- **Error Detection**
  - Detecting at the Receiver that the data received has an error or not
  - (Concepts shown in FKS Chapter "Signal Encoding").
- **Acknowledgement**
  - If any error is detected the Receiver sends a negative acknowledgement(NACK) to the Sender
- **Error Handling**
  - **Retransmission:** When the Sender receives a negative acknowledgement or if any acknowledgement is not received from the Receiver, Sender retransmits the data again. Resending is repeated until a message arrives that the Receiver believes is error-free (usually, not all errors can be detected).
  - **Error Correction:** Forward error correction is the process in which the receiver tries to guess the message by using redundant bits. This is possible, as we see later, if the number of errors is small.

(4) Examples of Transportation Layer: TCP vs. UDP





TCP

- Connection-oriented
- No loss: Error-affected Frames are re-sent
- No duplication
- First In First Out (FIFO): Correct order is persisted
- Timeout: Data has to be transferred in time

UDP: Packet-oriented protocol

- Connectionless
- No guarantee on complete delivery
- No guarantee on duplication
- No guarantee on correct order
- Lower overhead → faster

(5) Session Layer (dt. Sitzungsschicht)

Objective

- Creating the **logical connection** between two systems and their application processes

Actions/Tasks

- Logical connection Management
  - Initialization
  - Maintenance
  - Termination

Mechanisms

- Authentication and Authorization
- Creation of check points for re-synchronization of connection in order to preventing complete re-transmission

Components

- Commonly implemented in application environments using Remote Procedure Calls (RPCs)

Examples

- RPC, Structured Query Language (SQL), AppleTalk Session protocol

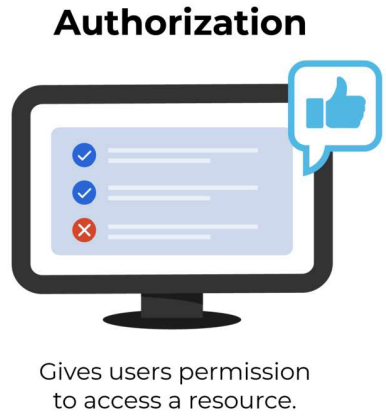
(5) Examples of Session Layer: Authentication and Authorization

Authentication

- Is the act of validating that users/machines are whom they claim to be and is the first step in any security process
- Authentication process requires one to n factors
  - **Passwords**: most common factor
  - **One-time Pins**: e.g. number key which is sent by SMS
  - **Authentication Apps**: generating security codes via outside party granting access
  - **Biometrics**: e.g. fingerprint, eye scan

Authorization

- Is the process of giving the user/machine permission to access a specific resource or function
- Term is often used interchangeably with access control or client privilege
- Authorization must always follow authentication
- Authorization areas and user settings are maintained by security teams



(6) Presentation Layer (dt. Darstellungsschicht)

Objective

- Converting data between application and network in order to guarantee compatibility across different type of systems
- Also called "Syntax Layer" – mapping semantics and syntax of the data in a way it can be consumed by every distinct network entity.

Actions/Tasks

- Transforming data into a processable form of the application or lower levels
  - Formatting from "Transfer Syntax" to "System's Syntax" *(see table right)*
  - Data De-compression
  - Decryption
- Transforming data into network transmission format
  - Formatting from "System's Syntax" to "Transfer Syntax", e.g. Abstract Syntax Notation One (ASN.1)
  - Data compression
  - Encryption

Example: Formats

Data Type	Example Formats
Text	ASCII
Images	JPEG, GIF, BMP
Video	MPEG, QuickTime
Audio	MP3, WAV

Description of ASN.1
https://youtu.be/EccHushRhWs

Mechanisms

- Formatting, Compression, Encryption

Examples

- Video Compression

(6) Examples of Presentation Layer: Compression/Decompression

- Data elements For efficient transmission of data elemets
- Compression Ratio

$$\text{Compression Ratio} = \frac{Uncompressed\ Size}{Compressed\ Size}$$

- Two types of compression

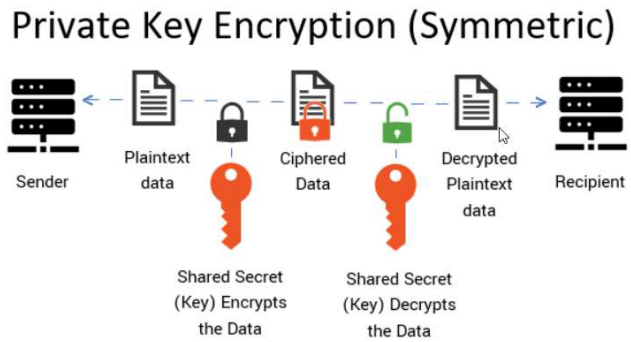
	Lossy Compression	Lossless Compression
Data Elimination	**Eliminates** those bytes which are considered as **not-noticeable**	**Keeps** even those bytes which are not-noticeable
Restoration	A file **cannot be completely restored** to its original form	A file **can be restored** to its original form
Quality	Leads to **lower quality**	**No quality degradation** happens
Size	**Reduces** the size of file to large extent	**Lower reduction** of size
Capacity	**Higher** data holding capacity	**Lower** data holding capacity
Usage	Mainly used to compress **raw data**, e.g. audio, video, images	Mainly used to compress **generated data**, e.g. text, numeric data, executable code
Examples	Transform coding, Discrete Cosine Transform, Discrete Wavelet transform, fractal compression, Sliding Window Lempel-Ziv (LZ77), etc.	Run length encoding, Huffman Coding, Lempel-Ziv-Welch, Arithmetic encoding, etc.

Example: Compression in JEPG

low ——— high

(6) Examples of Presentation Layer: Encryption/Decryption

- Security by encryption exists, when following is guaranteed
  - Read along the data **confidentiality** is prevented by "simple encryption"
  - Change of data **integrity** is prevented by a digital signature
  - Repetition of data **authenticity** is prevented by clearly marking (counter) the data
- Encryption algorithms can be divided in two general types
  - Symmetric: Private Key for encryption and decryption is equal (right figure)
  - Asymmetric: Public key for encryption and private key for decryption
- Encryption methods and keys are only exchanged between communicating devices
  - Only sender and receiver can properly encode and decode data into readable format
- Important metrics of encryption algorithms are
  - Encryption/Decryption time
  - Throughput
  - Level of Security
  - Key Length
  - Avalanche effect (*dt. Lawineneffekt*)
  - Possible Attacks
- *(More details on Data Security will follow in Chapter "Safety & Security")*



Survey on the Cryptographic Encryption Algorithms
https://www.researchgate.net/publication/321587376_A_Survey_on_the_Cryptographic_Encryption_Algorithms

(7) Application Layer (dt. Anwendungsschicht)

Objective

- Interfacing lower layer network services with the software application / end user

Actions/Tasks

- Verifying the **availability** of communication **partners**
- Determining **resource availability**
- **Synchronizing** communication
- Managing application-specific **networking requirements**
- Identifying **constraints from application level**
  - e.g. authentication, privacy, quality of service, networking devices and data syntax
- Interacting with the **user-interface**

Mechanisms

- Providing **Application Service Elements** (ASE)
  - **Common Application Service Elements** (CASE)
    - e.g. remote operations, support recovery from failure, rollback steps
  - **Special Application Service Elements** (SASE)
    - e.g. file transfer, message handling, database access

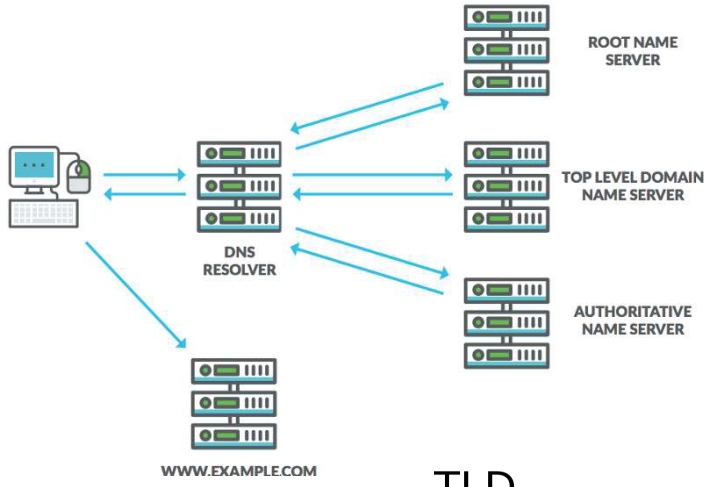
Examples

- DNS, FTP, HTTP, IMAP, POP, SMTP

(7) Examples of Application Layer: DNS

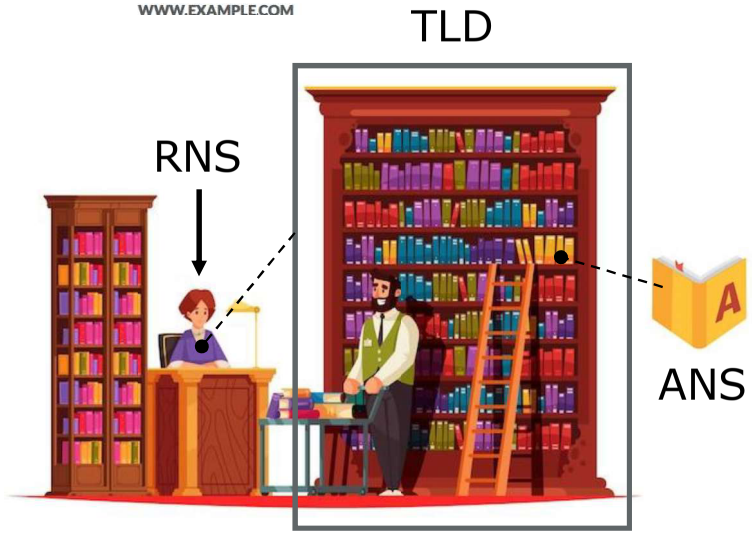
DNS

- Domain Names System (DNS) is the „phonebook" of the internet
- DNS provides easy to remember names (Link) for Internet Protocol (IP) addresses
- DNS Resolver has a local cache on history of found websites and returns the IP address
  - In case the IP address for the requested website is not available, a DNS lockup is performed



Procedure of a DNS lockup

1. User enters a website name in DNS format, e.g. „www.oth-regensburg.de"
2. Website name is sent to **DNS Resolver**, which checks local caches on entered website or requests following servers
   - **Root Name Server** (RNS) checks for each zone
     - e.g. zones like .org, .com, **.de**, .net
   - **Top Level Domain Name Server** (TLD) checks for pages within one zone
     - e.g. for .de including: **oth-regensburg.de**, amazon.de, google.de …)
   - **Authoritative Name Server** (ANS) for specific information on certain pages
     - e.g. oth-regensburg.de: 194.95.104.101
3. Once an IP was found for a website, this IP is stored in a local cache



Websites With Most Visits

What are the Websites with the most search queries (from Germany)?

— Folgende Daten gelten für Dezember 2021

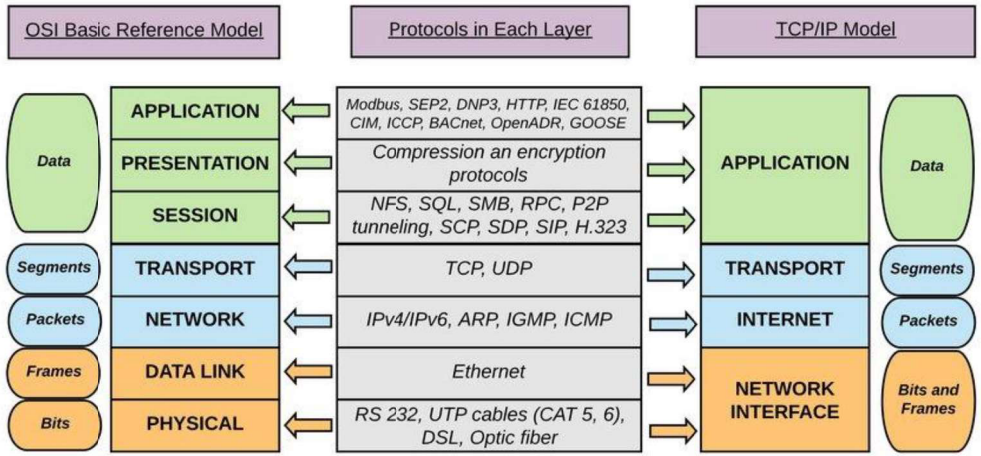
TOP 10 der meistbesuchten Websites in Deutschland

Platz	Domain	Besucher
1	google.com	934,70 Mio.
2	youtube.com	358,56 Mio.
3	amazon.de	311,17 Mio.
4	facebook.com	316,66 Mio.
5	wikipedia.org	239,43 Mio.
6	google.de	199,55 Mio.
7	bild.de	167,09 Mio.
8	ebay.de	140,52 Mio.
9	instagram.com	106,61 Mio.
10	t-online.de	91,95 Mio.

Aligning TCP/IP to OSI Model

TCP/IP

- The purpose of TCP/IP model is to allow communication **over large distances** with a **high reliability** over an **unreliable network**
- **Internet Protocol** (IP)
  - Obtains the address to which data is sent
- **Transmission Control Protocol** (TCP)
  - Responsible for data delivery, after IP address has been found



Comparison

- **OSI Model**, as pure **reference model**, is developed in order to enable a **standardized inter-operability** across the protocols of the different layers and therefore enables the **selection of a certain protocol** which fits the needs of the dedicated system und development in the best way.
- **TCP/IP Model/Protocol**, as a **certain implementation** of the OSI model, was developed to build a **robust and automatically recovering** phone line on the battlefield which connects various devices over a common network (Internet).

	OSI	TCP/IP
Number of Layers	7	4
Meta-Level	Reference model – **generic**, **protocol independent** standard	Implementation – Uses standard protocols
Quantity Services	Yes	No
Complexity	higher	Lower
Developed by	International Standard Organization (ISO)	Defense Advanced Research Projects Agency (DARPA)

Evaluation

Pro

- **Good guidance tool** to develop any network model
- Changes one layer **do not affect other layers**
- It is **flexible** in nature, protocols in each layer can be replaced very conveniently

Con

- It is purely a **theoretical model** that does not consider the availability of appropriate technology
- It has an inherent **implementation complexity** that renders networking operations inefficient and slow
- Some of the layers have **very little functionality** when practically deployed, e.g. Session and Presentation Layer

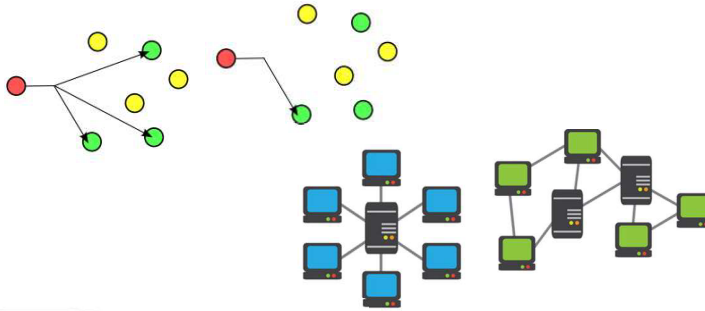
The launching timing of the OSI model was inappropriate. When OSI appeared, the TCP/IP protocols were already implemented. TCP/IP model was very much preferred by the academia. It was believed that OSI was a product of the European communities and the US government, who were trying to force an inferior model to researchers and programmers. Hence, there was considerable resistance in adopting it.

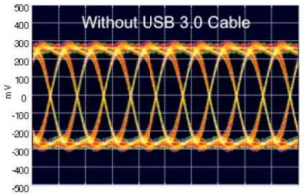
Section 2 - Coding

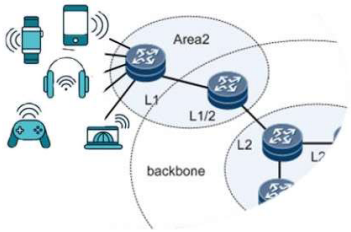
Summary

In Network Communication …

- … there are different **Routing Schemas** required, so a sender can distribute the information to the **desired receiving device**
- … there are different **Topologies** for interconnecting the devices of a network according to the **system requirements** (bandwidth, robustness, expandability, costs, …)
- … the **OSI Reference Model** is an internal standard for **classifying communication protocols** according to a well defined and exchangeable service layer
- … the **OSI-Layer 1** is responsible for the **bit transmission** and takes care that the binary signal is transferred over the communication channel correctly by considering the **physical effects** of the transmission medium
- … the **OSI-Layer 2** manage the physical addressing of any device in a network and handles the **point-to-point connection** between two direct devices, as well as the **multiplexing** and **flow control**, for the purpose of exchanging data **frames**
- … the **OSI-Layer 3** enables the **routing of packages** across different networks via offering **connection-less** or **connection-oriented** services for transfer of data **packages**



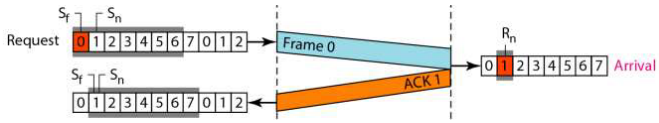




Summary

In Network Communication …

- … the **OSI-Layer 4** ensures the transmission of **variable length data**, which is transmitted as Segments, by maintaining the **QoS**

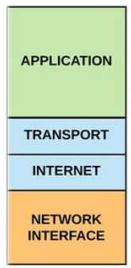


- … the **OSI-Layer 5** creates a **logical Session** between two systems and is responsible for **Authentication** and **Authorization** as well as the **re-synchronization** in case of connection loss

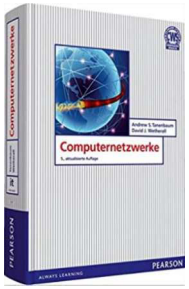
- … the **OSI-Layer 6** guarantees the **compatibility** on application data level by **formatting** data elements between transfer syntax and system syntax and provides **compression** and **encryption** services

- … the **OSI-Layer 7** interfaces with the application or end user by providing **network data/services** for the application

- … the **TCP/IP Protocol** is one **implementation** of the OSI Model, and enables a **robust** and **automatically recovering** communication between devices



Literature



Computernetzwerke

Authors: Andrew S. Tanenbaum , David J. Wetherall

ISBN: 978-3868941371

Content: OSI Model

Quiz

- Next Lecture Unit

End

- Introduction & Scope
- Definitions
- OSI Model
- Summary