Networks:-

To avoid confusion: 1 Kibibyte (KiB) = 2^{10} bytes = 1024 bytes (sometimes also called "large Kilobyte" (KKB)) ⟹ 1024 KiB = mebibyte.

American Standard Code for Information Interchange (ASCII): using 7 bits per character, whereas Extended ASCII uses 8 bits.
The non-printable characters from 0x00 to 0x20 and 0x7F are used as control characters, Therefore ASCII can be used not only to store data, but also to control data transmission for example:
- Start of Text (STX)
- End of Text (ETX)
- ACKnowledge (ACK)
- Negative ACKnowledge (NAK)

Unicode: To avoid problems caused by diff. character encoding.

Code length		Format	The 1st bit(s) indicates the length of the character encoding.
1 byte	7 bits	0x------	
2 bytes	11 //	110x----	10------
3 //	16 //	1110----	10------ 10------
4 //	21 //	11110---	10------ 10------ 10------
5 //	26 //	111110--	-------- -------- -------- --------
6 //	31 //	1111110-	-------- -------- -------- -------- --------

UTF-8: The most popular Unicode coding.

UTF-16: * Variable-length encoding (16 or 32 bits)
* Optimized for Commonly used characters from Basic Multilingual Plane (BMP)
* Used mainly for internal representation of characters in frameworks like .NET, Java, or Tcl.

UTF-32:
* Fixed-length encoding (32 bits)
* Used mainly in APIs.

Data Transmission:

Serial: Data is transmitted over a single line, one bit at a time. Ex. of serial: USB, Ethernet, Serial ATA, CAN

Parallel: Several bits are sent as a whole on the bus. It has not only data lines, but control lines as well.
Ex. of parallel: PCI, Compact Flash.

Synchronous transmission: It always have a clock signal or a way to recover the transmission by the receiver.
Sender & receiver are always synchronized. Ex.: SPI, & I2C buses.

ASynchronous: Communication partners use independent clock sources. If data is transferred, a start bit is set before the data. This signals the receiver that it should start its clock source.
Disadv: Because the clock can (slightly) differ, maximum size of the data that can be transmitted in one piece is limited. Examples: RS-232, RS-485

Simplex: Information is transfered only in one direction (Unidirectional).
Ex.: Radio & TV, GPS, Radio clock signal.

Full-duplex: transmission works in both directions simultaneously (bidirectional)
Ex.: Walkie-Talkie.

Half-duplex: Transmission in both directions (bidirectional), but not simultaneously. Examples of Half-duplex: Ethernet (via twisted pair cables), and Telephone.

Topologies of Computer network: Determines how communication partners are connected / Physical topology: Wirings.

Logical topology: describes the flow of data between the terminal devices.

Ring network: Two nodes are directly connected.
Information to be transmitted is forwarded until destination
An interruption of the ring causes network failure.

Bus Network: Connected via a shared transmission medium.
No active components between the nodes & the medium.
means ⟹ If any node fails, the network doesn't fail.
But an interruption of the bus causes network failure.

Star: All nodes directly connected to a central Hub.
Good expandability & stability. If any node fails neither affect other nodes, nor the network.
disadv: Considerable effort for cabling, and dependence on the the Central hub.

Mesh: If nodes or connections fail, communication still possible via other routes. & High level of reliability.
High cabling effort,
& increased electric power consumption.

Tree: Several star topology networks are hierarchically connected.
Failure of leaf node has no big effect on network's functionality
Expandability is excellent & long distances can be realized.
Suited for search & sort algorithms.
If a node or even the root fails, the entire (sub-)tree behind can no longer be reached.

Cellular: Wireless network use this topology.
Failure of a node doesn't effect the functionality of the network.
Limited range of the base stations, depending on their number & position.

Fourier Series: A square-wave signal (also binary signal) Can be represented by a Fourier series as the sum of a set of oscillating functions. Consists of a fundamental frequency & harmonics.

If you have a certain binary signal with a given max. frequency, the bandwidth of your transmission line must be at least 5 times higher than the base frequency of the transition.
Baud rate: num. of transferred
Bandwidth: Is the range of frequencies which can be transmitted via the medium without interference.
Bit rate: num. of transmitted payload in bits per time ⟹ [b/s]. | Symbol per time ⟹ Symbol rate ⟹ [Symbol/time unit]

TCP/IP Reference Model (DoD): 1- End-to-End principle. 2- Robustness Principle (You should be conservitive in what you do).

Layer Name	Protocols (examples)
Application Layer	HTTP, FTP, SMTP, POP3, DNS, SSH, Telnet
Transport //	TCP, UDP
Internet //	IP (IPv4, IPv6), ICMP, IPsec, IPX
Link //	Ethernet, WLAN, ATM, FDDI, PPP, Token Ring

Starting from application layer, every layer adds additional data to the message before submitting it. The receiver stars reading from link layer (or physical layer).

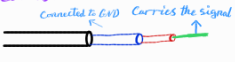
Hybrid Reference Model:

TCP/IP Reference Model → Hybrid Reference Model

Application Layer	Application Layer
Transport Layer	Transport Layer
Internet Layer	Network Layer
Link Layer	Data Link Layer
	Physical Layer

Physical Layer: Responsible for the transfer of ones & zeros. The Physical Connection & the conversion of the data into signals takes place.
Protocoles of this layer define how many bits can be sent per second & whether the transmission can take place simultaneously in both directions.

Ethernet: The most widely used LAN technology. Standards differ in the data rate & the transmission medium. Versions of cables up to 40 Gb/s.
Baseband transmission method (BASE). No carrier Frequencies → Transmitted directly.

Coaxial Cables:


Twisted Pair cables: Assures that the wires are on average the interfering source are affected equally. The noise produces a common mode signal which can be cancelled by the receiver by only regarding the differential signal level.

Fiber-Optics cables: typically from plastics or glass. Consists of light-transmitting core. **Adv.**: 1) you can transfer diff. (high) wave-length easily in it, therefore you get multiple channels. 2- They are immune to electromagnatic interference & radio freq. interference. 3- Low allenuation ⟶ long distance can be realized.

WLAN: **Challenges**: 1- Interference with other sources. 2- Multipath propagation. 3- Hidden Terminal. 4- Fading.
↳ need collision detection & avoidance to avoid it.

Bluetooth: Is a wireless network system for data transmission over short distances to replace short cables.
The freq. levels are changing up to 1600 times per second. Organized in so called Piconet. A Piconet consists of max. 255 participants, of which a max. of 8 may be active. One active node is the master and the remaining 7 active nodes are slaves.

Baseline Wander: We usually take the mean value between High & Low to know the threshold voltage. When transmitting long sequences of zero- or one-bits, the average may shift so much that it becomes difficult to detect a significant change of the signal. To prevent a shift of the average (Baseline Wander) when using a line code With two signal levels, the usage of both signal levels must be evenly distributed.

Clock Recovery (Synchronization): If the clocks of the Sender and the receiver drift apart, the receiver may become confused during a long sequence of logic zero- or one-bits.

NRZ-M: 1-bit = signal change ⟶ 0-bit = no change.
NRZ-I: 0-bit = signal change ⟶ 1-bit = no change.
MLT-3: 3 signal levels (+1, 0, and -). Same as NRZ-M.

Manchester: Each data bit is encoded by a combination of high/low or low/high bit sequence. Because of not more than two consecutive bits which have the level, the clock synchronisation is possible. As the number of low and high values are the same, the code result is balanced for any input data and no baseline wander can occur.
* It doubles the necessary data bandwidth. (means 50% efficiency)

Linecode	Signal level	Baseline Wander possible	Signal level change	Self-synchronizing possible	Efficiency	Directly transferable	Additional encoding
NRZ	2	yes	at changes	no	100%	no	
NRZI	2	yes	for 1-bits	no	75%	no	
MLT-3	3	yes	for 1-bits	no	100%	no	
RZ	3	yes	always	yes	50%	no	
Unip. RZ	2	yes	for 1-bits	no	75%	no	
Manchester	2	no	always	yes	50%	yes	
4B5B	2 or 3, depending on additional encoding	no	–	yes	80%	no	NRZI or MLT3
8B10B	2	no	–	yes	80%	no	NRZ
8B6T	3	no	–	yes	100%	yes	

Data Encoding: Why self-synchronous?
* To avoid clock draft, and therefore to avoid a wrong bit sampling.
* For short packets and if the sampling point is in the middle of a bit, a small clock drift doesn't shift the sampling point that much, and the bits are still correctly sampled.

Data link Layer: Main tasks: Error detection, & if possible error correction. Also, the protocols control the access to the transmission medium (for example, via CSMA/CD or CSMA/CA)

Error-detection codes are used instead of error-correction codes in many applications, Why? = It is often more efficient to re-transmit an erroneous message than to add the necessary additional bits for the error-correction in every single transmitted message.
Example of useful error-correction usage? = Simplex communication apps. With no possibility for re-transmission, data storing.

Why do we use Hybrid not the others?
The Hybrid reference model illustrates the functioning of Computer networks in a more realistic way compared to:
- The TCP reference model:
As it comes up with different functionalities and tasks of the Physical layer and data link layer by splitting the link layer in TCP/IP reference model.
- The OSI reference model:
Because the functionalities, which are intended for session layer and presentation layer are implemented today by the Application layer Protocols in most cases.

Advantages of layered Reference Models: Changes on one layer don't affect the other layers, Provided that the interfaces between the layers don't Change. The diff. layers seperate services, interfaces, and protocols, so they are more flexible and less complex than a network Combining all Characteristics and functionalities in one.

Bit Stuffing: If HDLC (High-Data-Link-Layer) Protocol of the receiver discovers a five consecutive one-bits, followed by a zero-bit in the bitstream from the physical layer, the stuffed zero-bit is removed.

Byte (character) Stuffing: If STX (02) or ETX (03) occurs in the Payload (body), it must be escaped (quoted) by a stuffed DLE (10) (Data Link Escape) in the Data link layer. If DLE appears in the payload, it is also escaped by an additional stuffed DLE.
We add DLE (0x10) before the byte (character) we want to stuff!

WLAN uses CSMA/CA instead of CSMA/CD, because with WLAN it is not possible to detect all collisions. Why not possible?
= Because of decreasing signal strengths, in some cases a node intending to transmit a message and therefore sending the carrier, can not receive messages from other nodes outside it's reception range. So, a hidden station problem might occur.

For which conditions, we use CSMA/CA RTS/CTS instead of CSMA/CA?
= Transmission of long packets / high payloads.

What drawback of CSMA/CA RTS/CTS compared to CSMA/CA?
= The exchange of the RTS & CTS messages adds additional payload to the network and decreases the overall latency of a data transmission.

CRC Calculation:
Example: $x^5 + x^2 + x$
100110

```
1 1 1 0 1 0 0 1 1 1 0 0 1 0 0 0 0 0
1 0 0 1 1 0                          XOR
0 1 1 1 0 0 0                        operation
  1 0 0 1 1 0
  0 1 1 1 0 1
    1 0 0 1 1 0
    0 1 0 0 0 1 1
      1 0 0 1 1 0
      0 0 0 1 0 1 0 0 1
        1 0 0 1 1 0
        0 0 1 1 1 1 0 0
          1 0 0 1 1 0
          0 1 1 0 1 0 0
            1 0 0 1 1 0
            0 1 0 0 1 0 0
              1 0 0 1 1 0
              0 0 0 0 1 0 0
                ↙
```

must be added to the right end of the data before sending it.

Network layer: Called internet layer in TCP/IP reference model. Its task is to forward packets between logical networks over physical network segements. The network layer defines logical addresses (IP addresses). Gateways, or routers are used to forward packets on their way from the send to the distination.

Usually, the connectionless Internet Protocol (IP) is used. **Advantages of IP**: Low overhead, allow multicast and broadcast operations

Disadvantages of IP: No acknowledgement from the receiver, that the packet has been received, risk of packet loss.

	Network length (without prefix)	Host length (no. of devices)
Class A	7 bit (⇒ 128 nets)	24 bit (⇒ 16.777.214)
Class B	14 bit (⇒ 16384 nets)	16 bit (⇒ 65534 hosts)
Class C	21 bit (⇒ 2.097152 nets)	8 bit (⇒ 254 host)

Why since $2^8 = 256$? 2 address always reserved.
- broadcasting ID (set to 0)
- Identifying the host ID

Why **UDP** is often used for video telephony? and **TCP** for Webserver?

= **UDP** is connectionless. Its Low overhead makes it ideal for time-sensitive applications like Video-telephony, where single erroneus messages are not critical.
(It is better to ignorge a package if it didn't arrive)

= **TCP** is connection-oriented. It guarantees the correct transport between a send and a receiver, like it is necessary for a website.

IP address: 153. 213.11. 213 /27 (Host)
- Network (doesn't change)
- /27 → how many ones in the Subnet mask (Netmask)

Subnet (network) address: 153. 213.11. XXX
- this e.g. 192
- by taking the first n-num. of bits from the last 8-bits (host) from the IP address. (in this case n = 27-24 = 3)
- +1 for the first host address

Broadcast address: 153. 213.11. XXX (same; 223)
- The rest of the 8-bits to the right are ones.
- -1 for the last host address.

Differences between an IP address, a port, and a socket?

= IP addresses are used on the network layer by the internet protocol for addressing, whereas ports are used on the transport layer for addressing. A socket is a combination of an IP address and a port number.

193.99.144.85 : 8080
IP address | Port
Socket

Application Layer (highest layer): Contains all protocols that interact with the user application programs (e.g., browser or email client). The messages (e.g., HTML pages or emails) are located according to the respective Application Layer Protocol.

Transport layer: (End-to-End protocols)
- Connection-oriented communication. (Receiver has to acknowledge)
- Reliability
- Flow control

} Services

How to avoid physical layer collision?
= Only the bit with a Token can send data (all nodes are equal)

CAN Bus: In the Controller Area Network (CAN) bus arbitration process, the node with lowest indentifier will win the bus and be able to transmit the message. The lower the ID, the higher the priority of the message.

Why can't have 2 nodes with the same ID?
= If both nodes starts transmitting at the same time, the arbitration process will fail. In addition, if a message with acknowledgement does not work properly (as a dominant ACK will "overwrite" a recessive NACK).

Bit Stuffing: CAN uses NRZ coding with bit stuffing (after five equal bits, an inverse bit is added) to allow the synchronization of nodes without stable oscillators. (Start of fram bit is not counted from the five)