Summary Computer Networks

John

July 8, 2017

Contents

1 Motivation

1.1 Communication Metaphors

- Phase 1: Person to person
- Phase 2: Person to machine
- Phase 3: Machine to machine/Network of computers
- Phase 4: The internet of Things

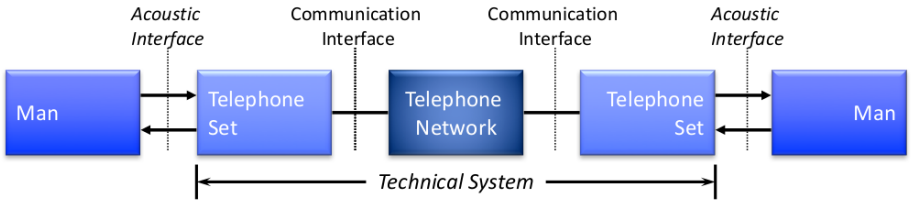
1.2 History

- 1837: Samuel Morse develops the telegraph
- 1953: First transatlantic Telephone line
- 1876: Alexander Graham Bell patents the telephone (tele=distant, phone=voice)

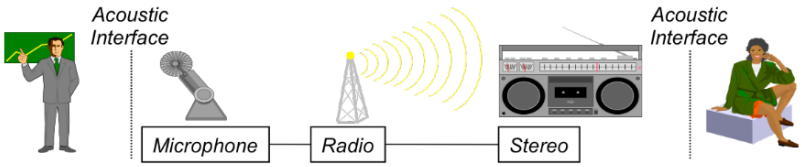
1.3 Telephone Network

Existing networks are going to be integrated

- **Model of telecommunication**



- **Model of broadcasting**



1.4 The Internet

The internet consists of

- a set of computers, which
  - use the TCP/IP protocols
  - are somehow (directly or indirectly) connected
  - offer or use particular services
- a set of users, which have access to these services
- a set of other networks, which (somehow) are accessible

Design Principles

- Minimalism and autonomy - The network operates by itself , does not require internal changes when new networks are added
- Best-effort service model
- Soft-state (stateless) - The routers do not need to maintain end-to-end communication information
- Decentralization

2 Introduction

2.1 Data Communication

Data communication is the processing and the transport of digital data over connections between computers (generally over large distances).
Data communication comprises two areas: Computer Networks and Communication Protocols

2.2 What is Digital Data?

- Data: Representation of facts in a formal way, processable by humans and machines, e.g. a language
- Information: is whatever contributes to a reduction in the uncertainty of the state of a system, can only be handled by humans
- Signal: is the physical representation of data by spatial or timely variation of physical characteristics
- Example: Sounds of a language (Data) during speaking are acoustic waves (Signals)

2.3 Data Communication

- Sharing resources saves costs
- Exchange of information

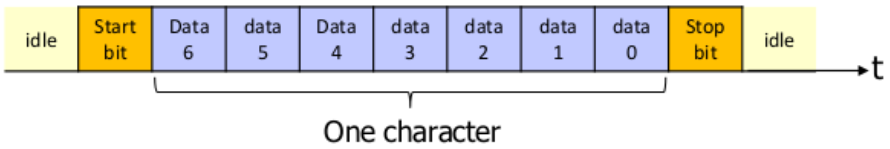
2.4 Networking Principles

Communication Peers

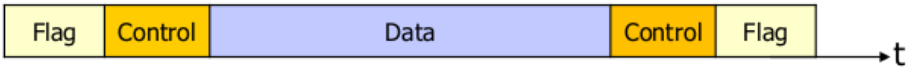
- Unicast: Two communication peers communicate over a Point-to-Point connection.
- Multicast: One sender communicates to several receivers, which are known.
- Broadcast: One sender transmits to all other peers. Typically the other peers are (partially) unknown.
- Others: Anycast, Geocast, etc.

Transmission

- Serial Transmission
- Parallel Transmission (Problem: synchronisation of the data)
- Asynchronous Transmission: Transmission in which each block (character) is individually synchronized



- Synchronous Transmission: Transmission in which the time of occurrence of each signal representing a bit is related to a fixed time frame



Connection Properties

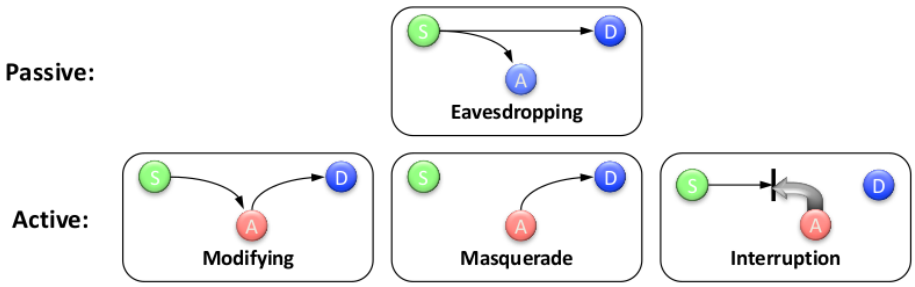
- Simplex
- Duplex
- Half-Duplex

Multiplexing: Combining multiple data channels into a single data channel at the source

Quality

- Technical Performance (Delay-Bandwidth-Product = Store capacity of the line)
  - Delay [s]
  - Jitter [s]
  - Throughput [bit/s]
  - Data rate [bit/s] (wird vorgegeben)
- Costs
- Reliability
- Security and Protection

Safety measures: Encryption, Trustworthy systems



The Client/Server Principle

- Client → Server: Request
- Server → Client: Reply
- Advantages
  - Cost reduction
  - Better usage of resources
  - Modular extensions
  - Reliability by redundancy
- Server: Program (process) which offers a service over a network.
- Client: Program (process) which uses a service offered by a server.

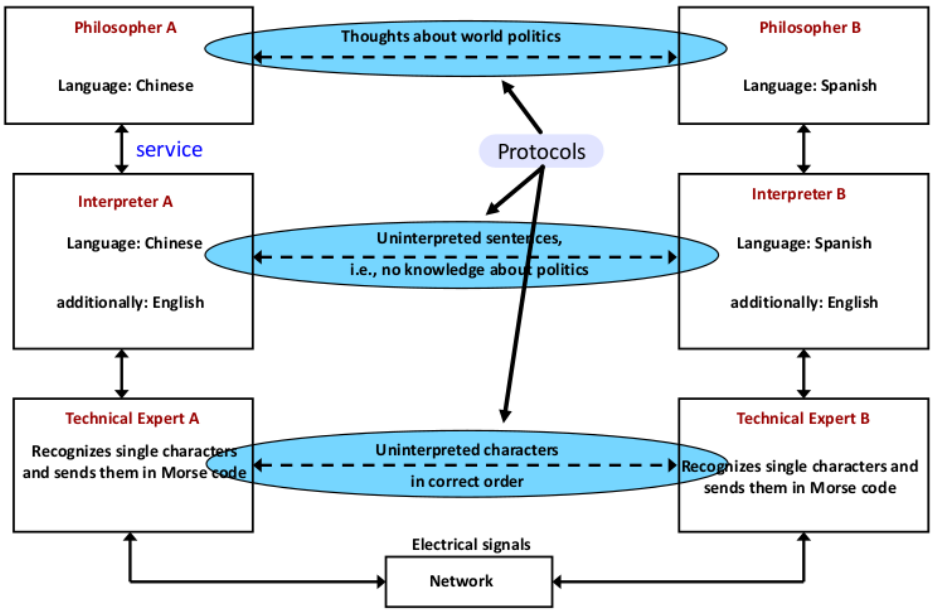
Peer-to-Peer Principle (ursprüngliche Kommunikation im Internet)

- Equal partners, no fixed client and server roles
- Connections between any pair of computers
- Establishment of a whole network of connections
- Best example: File Sharing, e.g., Napster, Gnutella

2.5 Communication Protocols

A protocol is the set of agreements between (application) processes with the purpose of communication.
To enable understanding in communication, all communication partners have to speak the same language.

- Data formats and their semantics
- Control over media access
- Priorities
- Handling of transmission errors
- Sequence control
- Flow control mechanisms
- Segmentation and composition of long messages
- Multiplexing
- Routing



→ communication between horizontal layers

Peer of a Layer

- use one service (except the bottom)
- offer a service (except the top)
- do not need to know other than the next lower one
- talk according to the rules

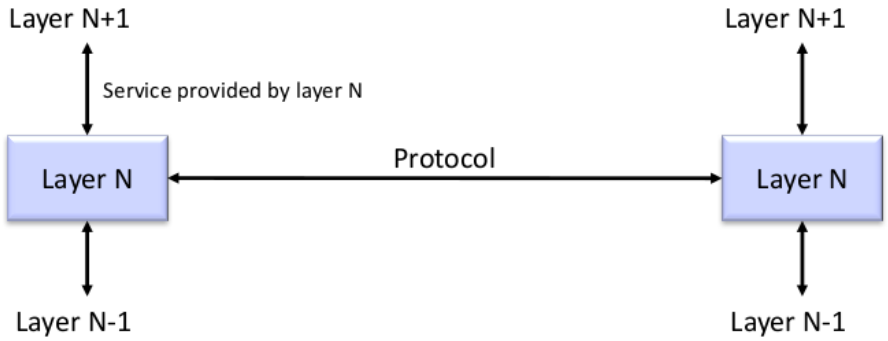
Communication architectures are based on

- Service = Communication Service
- Rules = Communication Protocol

A service is offered from a service provider at a service interface to service users.

Types of services are:

- Request
- Indication
- Response
- Confirmation

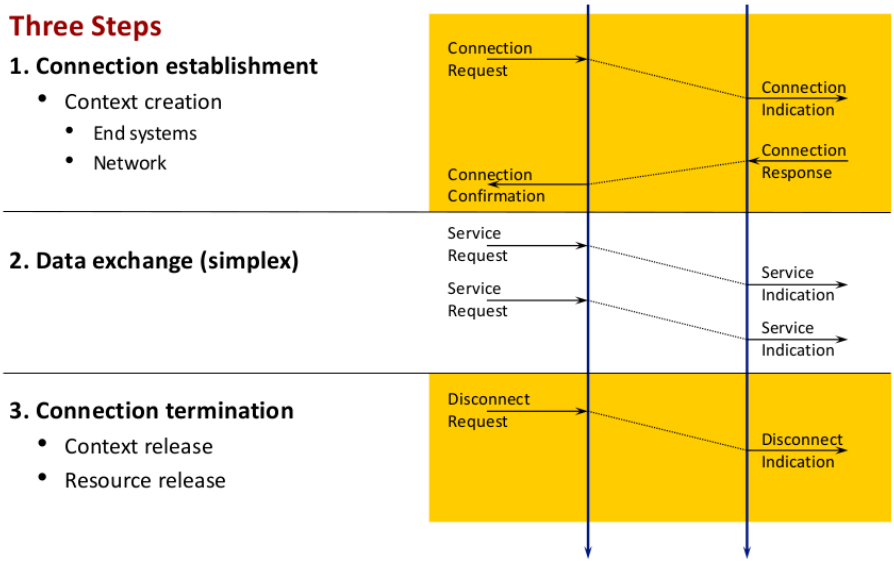


Types of Services

- Unacknowledged Service
  - Modeled after the postal service
  - Initiated by the service user
- Acknowledged Service (Transaction)
- Connection-oriented Service
  - Modeled after the telephone system
  - Before the instances on Layer-(N) can exchange data, a connection on Layer-(N-1) has

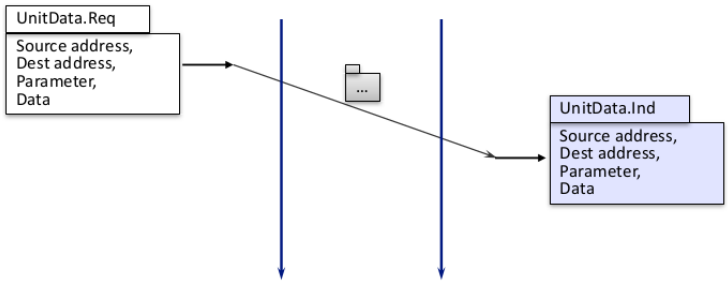
to be established
  - Negotiation of protocol parameters
    → Communication context
- Connectionless Service
  - Modeled after the postal service
  - No establishment of connection on a lower layer required
    → No communication context

Connection-oriented Service



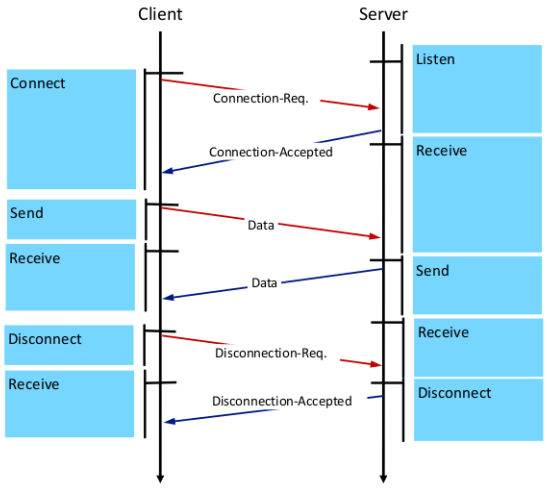
Connectionless Service

- **Connectionless Service is also called Datagram Service**
  - Does not provide relationship between transmissions
  - Does not guarantee the sequence of send data
  - Does not provide reliability
    - No acks!

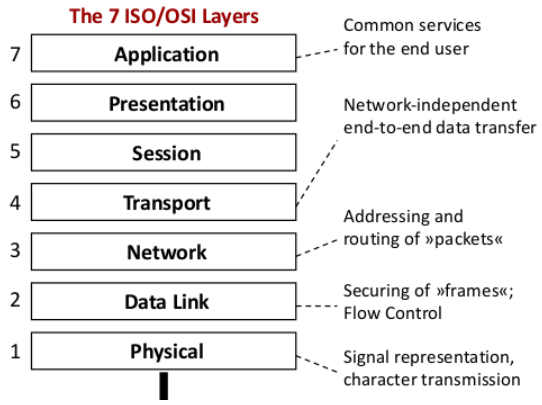


Service primitives

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection



2.6 ISO/OSI Reference Model



Critics on the model

Layer 5 and 6 are rarely implemented

Generally too much overhead – some details are unnecessary, some layers are overloaded

1. Physical Layer
   - Responsible for single bit transmission
   - Details are defined: type of cables, meaning of pins of network connectors, transmission direction on the cable
2. Data Link Layer
   - Ensures an error-free data transmission between two directly connected devices → segmented into frames (transmitted separately)
   - Receiver checks the correctness (checksum)
   - flow control is used to control the re-transmission of corrupt frames and protect the receiver from overload.
   - control of medium access (prevent address conflict)
3. Network Layer
   - Data-transmission over large distances and between heterogeneous sub-networks
   - uniform addressing of hosts
   - routing: select a path through the network.
   - Quality of Service (QoS) issues, i.e., if too many packets are present at the same time in the network, they may form bottlenecks. (congestion, maximum size of the transferred data units (MTU), delay, jitter, transit time, etc.)
4. Transport Layer
   - end-to-end communication between two processes
   - Ensure that the data are receipt complete and in correct order
   - current network state is monitored to adapt to the receiver and to the network capacity
5. Session Layer

- manages reliable data transport
- offers dialogue control, i.e., define the direction of the transmission.
- token management (allows operation)
- set synchronization points in the communication process

6. Presentation Layer
   - Represent the data to be transmitted in a way, that they can be handled from different computer systems
   - Data are encoded in an abstract (and commonly recognized) data format before the transmission and are coded back by the receiver into its own data format.
7. Application Layer
   - standard protocols are provided, that can be used from applications
   - interface to file transfer

Interplay between the Layers

- Layer (N-1) offers its functionality to layer N as a communication service.
- Layer N enhances the data to be sent with control information (Header) and sends the data together with the header as Protocol Data Units (PDU).
- Depending on the protocol, N-PDUs can be segmented into several (N-1)-PDUs before transmission

2.7 The TCP/IP Reference Model

1. Host-to-Network Layer (1+2)
   - Not defined exactly
   - host must be connected to the network via a protocol in a way that it is able to send and receive IP datagrams
2. Internet Layer (3)
   - interworking of different networks
   - enables communication between hosts over the own network borders (transmission is connectionless)
   - Router takes over the forwarding
   - Path can be dynamic
   - In contrast to ISO, only one packet format is defined, together with a connectionless protocol, the Internet Protocol (IP)
3. Transport Layer (4)
   - covers the communication between the end systems
   - TCP (Transmission Control Protocol) is a reliable, connection-oriented protocol for the transmission of a byte stream between two hosts.
   - UDP (User Datagram Protocol) is an unreliable and connectionless protocol (best effort).
4. Application Layer (7)
   - defines common communication services (HTTP, FTP,..)

2.8 OSI vs. TCP/IP

1. Time - The TCP/IP protocols were already widely used before OSI had finished the standardization activities.
2. Freedom from obligation (defines what not how) → incompatibility of products
3. Complicatedness
4. Political reasons (Europe)
5. Hurriedly product implementation

2.9 Standardization

Two types of standards
- De facto standards
- De jure standards

Organisationen:
- ISO
- Internet Engineering Task Force
- Institute of Electrical and Electronic Engineers (IEEE)

2.10 Evolution of Computer Networks

- First generation: via mainframe in computer center
- Connection via LAN, router → rest of the world
- computer centers via router connected to backbone → rest of the world

2.11 Classification of Computer Networks

- Personal Area Network (PAN) - 1m
- Local Area Network (LAN) - 10-100m
- Metropolitan Area Network (MAN) - 1-10km
- Wide Area Network (WAN) - 100-1000km
- Internet - 10000km

3 Physical Layer

3.1 Theoretical Basis for Data Communication

- Spectrum of a signal is the range of frequencies it contains
- The absolute bandwidth of the signal is the width of the spectrum
- Bandwith of a medium: Frequency range which can be transmitted over a medium

Transmission of information can take place on
- Baseband (information is transmitted over the medium as it is)
  → discrete (digital) signals
- Broadband (The information is transmitted analogous by modulating onto a carrier signal) used in optical and radio networks
  → continuous (analogous) signals

Nyquist- und Shannon-Theorem
max. data rate $= 2 \cdot B \cdot log_2(n)$ vs. $B \cdot log_2(1 + SNR)$

3.2 Analog Data and Digital Signals

Pulse Code Modulation (PCM) is based on the sampling theorem by Shannon and Raabe: If a signal is sampled at regular intervals of time and at a rate higher than twice the highest significant signal frequency, then the samples contain all the information of the original signal.

3.3 Data Encoding

see exercise

3.4 Transmission Media

see exercise

3.5 The Last Mile Problem

connect private homes to the Internet without installing many new cables → Use existing telephone lines: re-use them for data traffic

Examples: Modem, ISDN, DSL

Modulation:
- Amplitude Modulation
- Frequency Modulation
- Phase Modulation

3.6 Multiplexing

Sharing of an expensive resource, e.g., transmit multiple connections over the same line
Frequency Division Multiplexing, Time Division Multiplexing

3.7 Digital Subscriber Line (DSL)

Combination of usual phone service (analog/ISDN) and data service: simply use the whole spectrum a copper cable can transfer, not only the range up to 3.4 kHz!

4 Data Link Layer

- provides a well-defined service interface to the network layer
- deals with transmission errors regulates the flow of data, the access to the medium, that a slow receiver is not swamped by a fast sender

Parts:
- Logical Link Control (LLC)
  - Organization of the data to be sent into frames
  - Guarantee (if possible) an error free transmission between neighboring nodes by ...
  - Detection (and recovery) of transfer errors
  - Flow Control (avoidance of overloading the receiver)
  - Buffer Management
- Medium Access Control (MAC)
  - Access control to the communication channel in broadcast networks

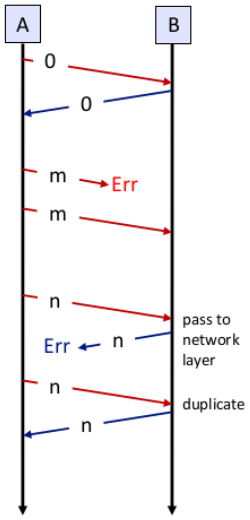
4.1 Error Detection and Correction

Compute a short checksum of the data and send it together with the data to the receiver.
CRC, Hamming Code → exercise

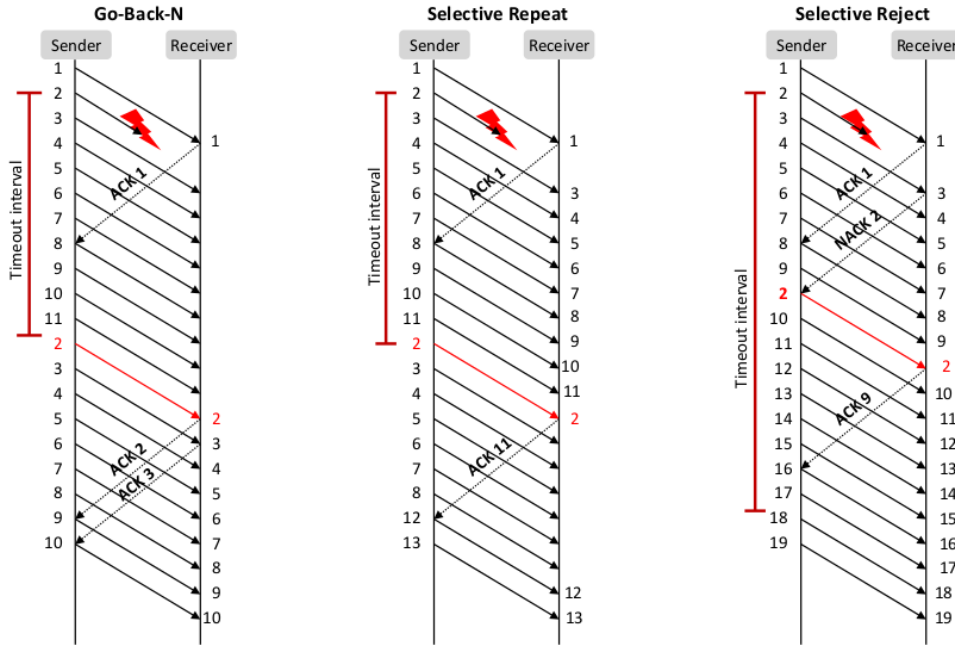
4.2 Elementary Data Link Protocols

- **Requirement**
  - The sender needs a guarantee that the frame was correctly received
    - ➢ Acknowledgement from receiver
- **How to distinguish original and retransmitted frame?**
  - Solution: Put a sequence number into each frame
  - What is the minimum number of bits needed for the sequence number?
  - Enough to distinguish between frame m and frame m+1
    - ➡ 1 bit sequence number sufficient
- **Receiver expects a particular sequence number**
  - If arriving frame has correct sequence number accept, otherwise reject

➡ **Automatic Repeat reQuest (ARQ)**



Sliding Window: Allow sender to transmit up to W frames before blocking
→ exercise



4.3 High Level Data Link Control (HDLC)

Three types of stations

- Primary station: responsible for controlling the operation of the link.
- Secondary station: operates under the control of the primary station.
- Combined station

Bit stuffing: Sender inserts a zero after each sequence of five ones. The receiver removes this zero.
frame: 01111110 Address Control Data Checksum 01111110
Control: 0 Seq P/F Next

4.4 Point-to-Point Protocol (PPP)

Establish a direct connection between two nodes
Features:

- Framing method with error detection

- Link Control Protocol
- is character oriented and uses byte-stuffing

4.5 Protocol Verification

- Finite state machines
- Petry nets

5 Medium Access Control Sublayer

Two kinds of connections in networks
- Point-to-point connections
- Broadcast (Multi-access channel, Random access channel)

In a network with broadcast connections → Who gets the channel?

5.1 The Channel Allocation Problem

Static Channel Allocation
- Time Division Multiple Access (TDMA)
- Frequency Division Multiple Access (FDMA)

→ works only for fixed number of users, data traffic is bursty

5.2 Multiple Access Protocols

ALOHA
- Stations are sending completely uncoordinated (random)
- All stations use the same frequency
- When two (or more) stations are sending at the same time, a collision occurs: all messages are destroyed.
- repeat after a random time
- Improvement: Slotted ALOHA → The time axis is divided into time slots

Carrier Sense Multiple Access (CSMA)
- each station, which wants to send, first examines whether already another station is sending
- p-persistent CSMA : If channel idle, station transmits with probability p in current slot and with probability (1-p) it defers until next slot.
- CSMA with Collision Detection: CSMA/CD
  - Basis of Ethernet
  - A station who detects a collision stops immediately transmitting
  - Afterwards it waits a random time and tries again

5.3 Multiple Access Protocols - Collision-Free Protocols

Split into reservation phase and transmission phase.
- Bit-Map Protocol
  - without connection: set k-th bit in reservation frame
  - with connection: try to write your station number in one contention slot
- Binary Countdown: Compare addresses, 1 wins

5.4 Multiple Access Protocols - Limited Contention Protocols

- Adaptive Tree Walk Protocol
- Coordination by using a Token

5.5 Multiple Access Protocols - MAC for Wireless Networks

Multiple Access with Collision Avoidance (MACA)

- Idea: Inform stations in the neighborhood about the transmission
- Ready To Send (RTS)
- Clear To Send (CTS)
- Extension of MACA by an acknowledgement → MACAW

5.6 Ethernet

Resolving Collisions in Ethernet: Binary Exponential Backoff

5.7 Network Infrastructure

- Transparent Bridges: Address Learning
- Preventing loops: compute a spanning tree from all connected bridges

5.8 Virtual LANs

Decoupling of the logical topology from the physical topology

5.9 Summary

Layer 1 defines transmission medium and bit representation on this medium, transmission mode, data rate, pin usage of connectors, ...
Layer 2 protects against transmissions errors (mostly CRC) and receiver overload (flow control, sliding window)
Layer 2 also defines medium access coordination for broadcast networks
Both layers together define how to transfer data from one computer to a directly connected one, thus both are implemented in one piece of software: the network interface card driver.

6 Network Layer

- Boundary between network carrier and customer
- Control of global traffic
  - Coupling of sub-networks
  - Global addressing
  - Routing of data packets
  - Initiation, management, and termination of connections through the whole network
  - Global flow control

Routers in the network receive frames from layer 2, extract the layer 3 content (packet) and decide based on the global address to which outgoing connection (port) the packet has to be passed on. Accordingly the packet becomes payload of a new frame and is sent.

6.1 Routing principles

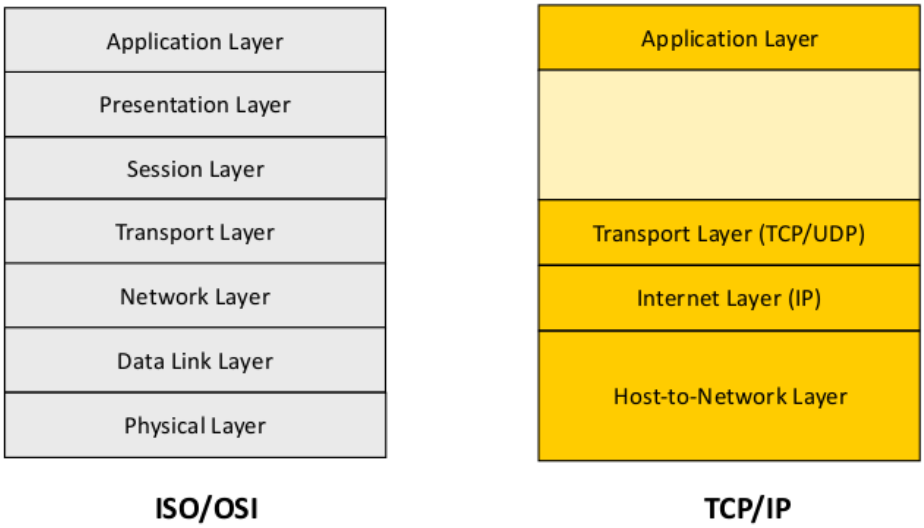
- Connectionless communication (e.g. Internet, packets can take different ways)
- Connection-Oriented Communication (e.g. telephony, virtual connection)

Routing: determine most favorable route from the source node to the destination node
Routing tables: can be determined statically or dynamically, can be one-, two- or multidimensional (optimization goals)

6.2 Internet

Goal:Interconnection of computers and networks using uniform protocols

- ARPANET (predecessor of today's Internet)
- All networks had different protocols → TCP/IP networks



6.3 Internet Protocol (IP)

Raw division into three tasks

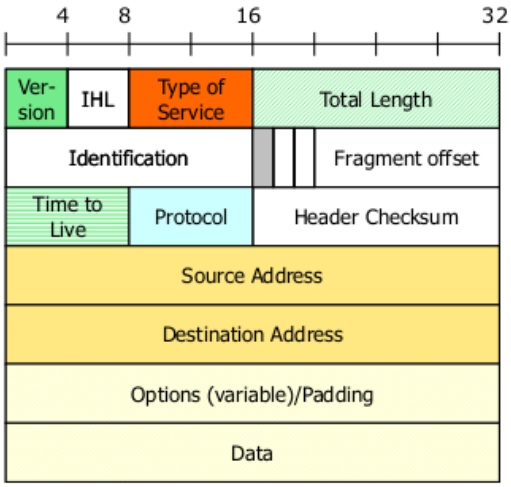
- Data transfer over a global network
- Route decision at the sub-nodes
- Control of the network or transmission status

connectionless, unreliable transmission of datagrams/packets → Best Effort Service

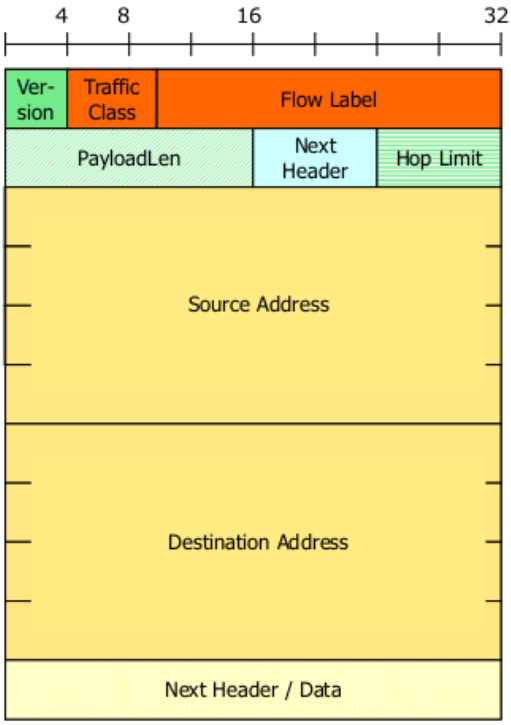
Subnets: Some bits of the host address are used as network ID, A Subnet Mask identifies the "abused" bits
Classless Inter-Domain Routing (CIDR): Form of an IP address: a.b.c.d/x (The first x bits are the network identification)

6.4 IPv6

- Simpler structure of the headers
- More automatism
- Simpler configuration
- Performance improvements
- Migration strategies
- More security
- Larger address space (128 bit)
- Flow label: virtual connection with certain characteristics/requirements



The IPv6 header is longer, but this is caused by the longer addresses. Otherwise it is "better sorted" and thus faster to process by routers.



Three types of addresses:

- Unicast
- Anycast
- Multicast (no broadcast)

Coexistence:

- Header Conversion (Router translates an incoming IPv6 packet into a IPv4 packet, receiving router retranslates)
- Tunneling (encapsulates an incoming IPv6 packet into a new IPv4 packet)

6.5 Network Address Translation

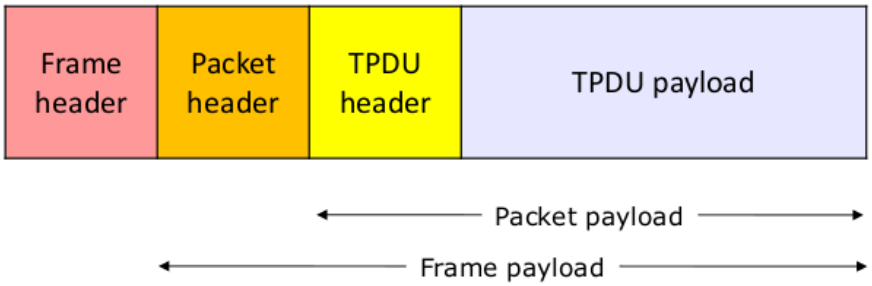
- Private address blocks (10.0.0.0, 172.16.0.0, 192.168.0.0)
- Router attached to the external world also need a global address
- Basic NAT (also: Static NAT)
  - Each private IP address is translated into one certain external IP address
  - disadvantage: need as many official IP addresses as you have computers
- Hiding NAT
  - Translates several local addresses into the same external address
  - uses different ports

6.6 Auxiliary Protocols

- Address Resolution Protocol (ARP)
  - With ARP, IP is mapped to the hardware address and vice versa
  - ARP Request → ARP Response
- Reverse Address Resolution Protocol (RARP)
  - makes it possible that a booted machine broadcasts its hardware address and gets back by a RARP server the appropriate IP address.
  - But: RARP-server in each local network required
- Dynamic Host Configuration Protocol (DHCP)
  - A computer sends a DHCP DISCOVER packet. In each subnet a DHCP Relay Agent is placed, who passes such a message on to the DHCP server.
- Internet Control Message Protocol (ICMP)

  - control protocol of layer 3 if something unexpected happens (e.g.TTL=0)
  - transmits error and control messages in an IP packet
- Internet Group Management Protocol (IGMP)

7 Network Layer



Messages from transport entities: Transport Protocol Data Unit (TPDU)

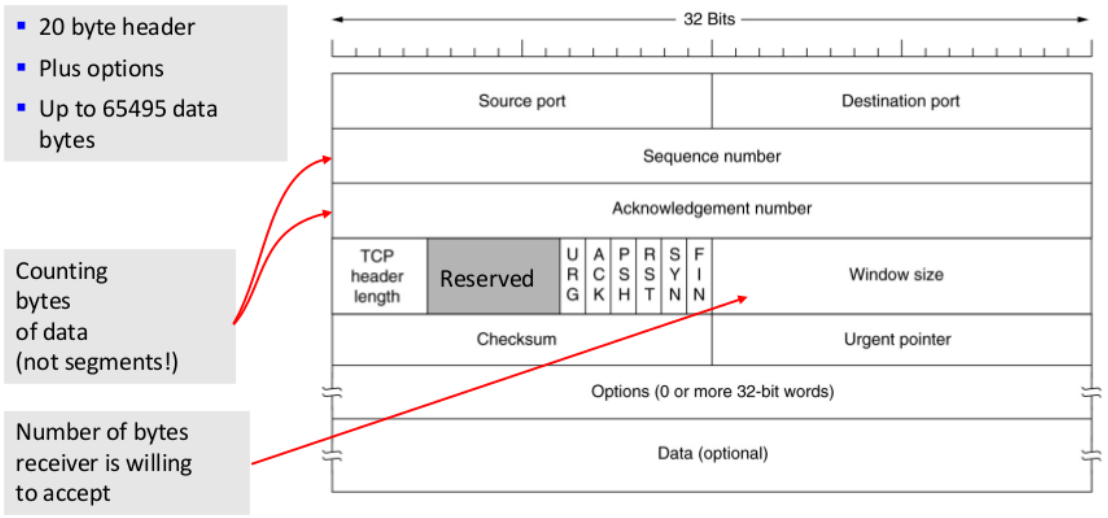
7.1 User Datagram Protocol (UDP)

- Like IP: Connectionless and unreliable
- No acknowledgement
- Use in multicast
- Not reliable but fast
- Addressing of the applications by **port numbers**

7.2 Transport Control Protocol (TCP)

- Connection-oriented and reliable (error-free, keeps packet order, without duplicates)
- Byte stream, not message stream
- Error handling, acknowledgements, flow control
- Urgent messages
- Addressing of the application by port numbers
- Establishes logical connections between two **Sockets**
- TPDUs are called segments
- Send and receive buffers

Ports:
- 0-1023 System
- 1024-49151 User
- 49152-65535 Private



TCP Connection Management:

1. SYN, Seq=x
2. SYN, Seq=y, ACK=x+1
3. Seq=x+1, ACK=y+1