

MVŠO

MORAVSKÁ VYSOKÁ ŠKOLA OLMOUC 

Computer Networks

Vít PÁSZTO

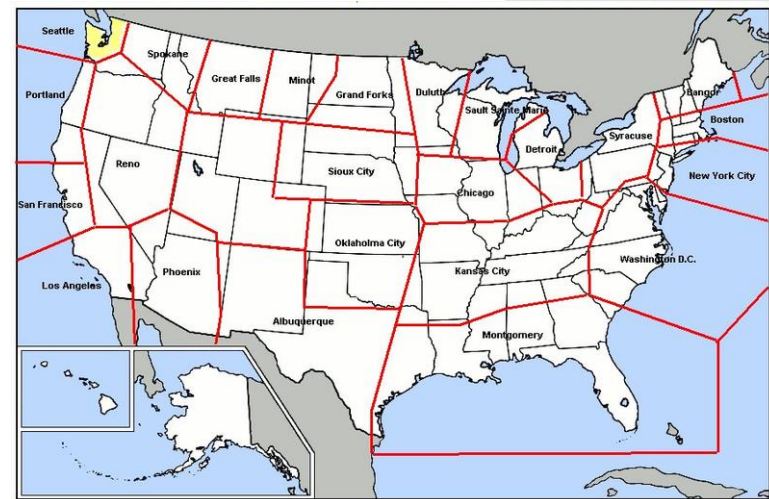
21.3.2023

Computer Networks

- Set of technologies allowing transfer and exchange of information among computers
- Allows users to communicate (following some rules) in order to share and exchange data (resources/information)
- History goes back to the second half of 20th century (US Air Force WAN for semi-automatic ground envi (radar))
- Internet (WWW), storage services, printers/faxes (peripheral devices), email, instant communication (messengers, VoIP and others)

Computer Networks

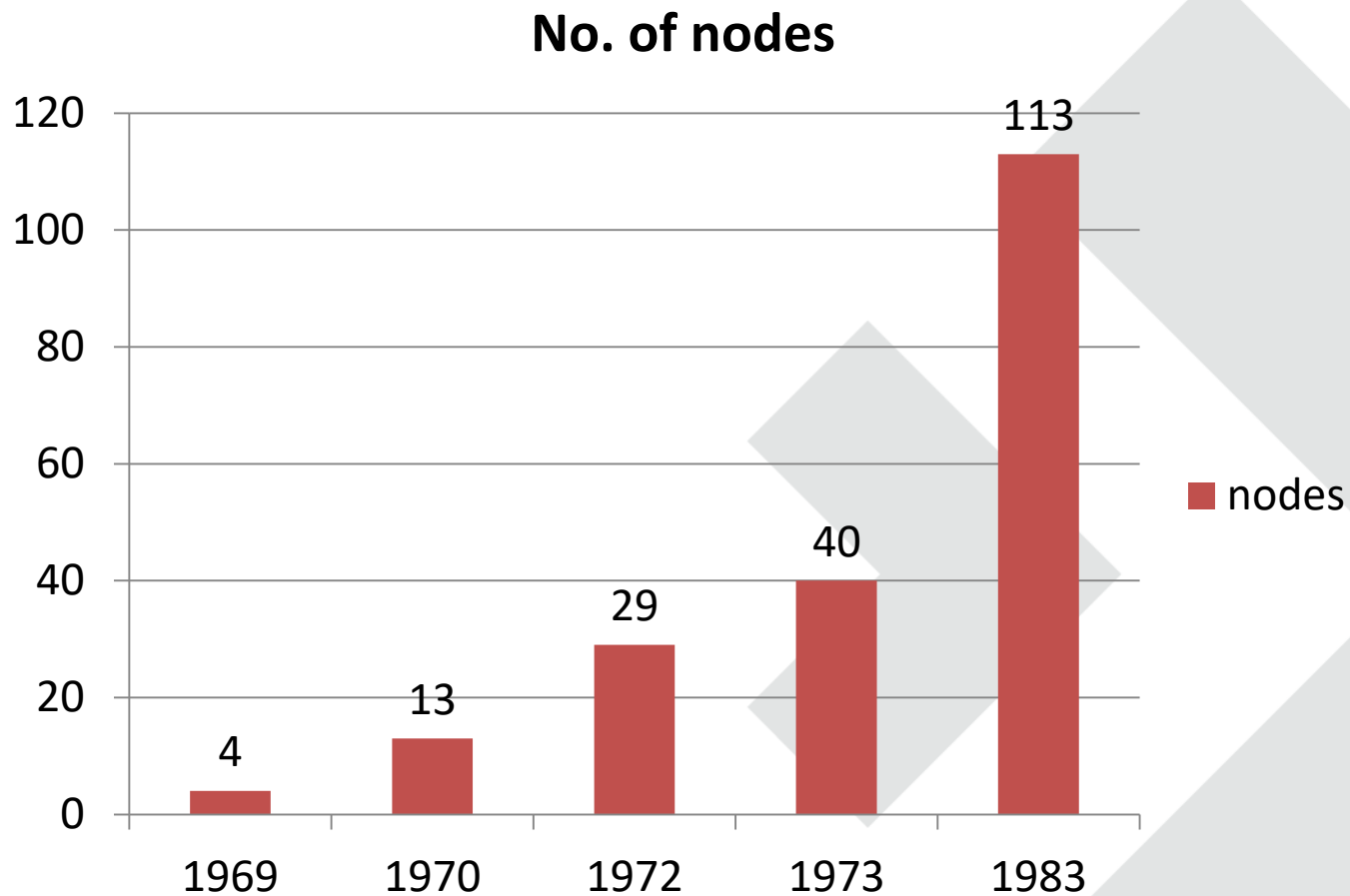
- History goes back to the second half of 20th century (US Air Force WAN for semi-automatic ground envi (radar))



ARPANET

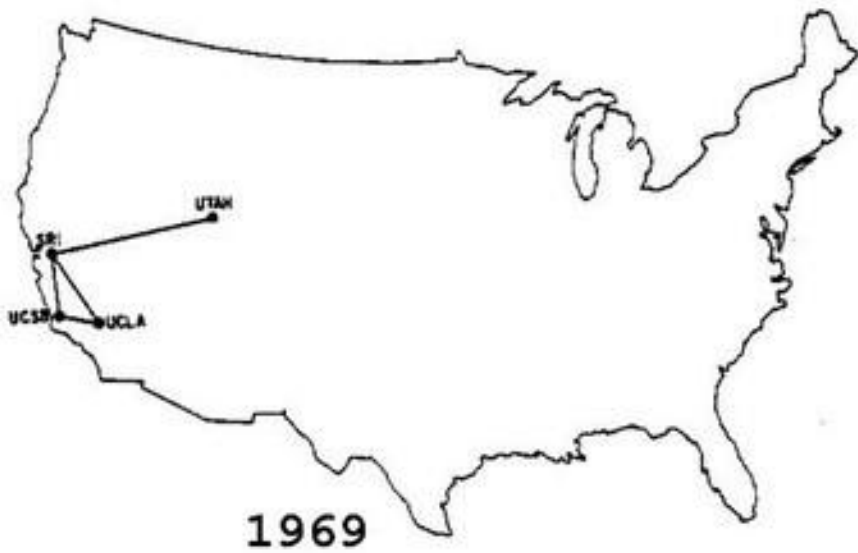
- The first „modern“ computer network (1969)
- U.S. Ministry of Defence (ARPA) – Larry Roberts
- Testing network for packet switching
- No central unit because of destruction of any part
- Four initial members:
 - UCLA, SCRI (Stanford Central Research Institute), UCSB (University of California Santa Barbara), University of Utah
- First packet sent on 29th Oct 1969
- Network Control Protocol (NCP)

ARPANET

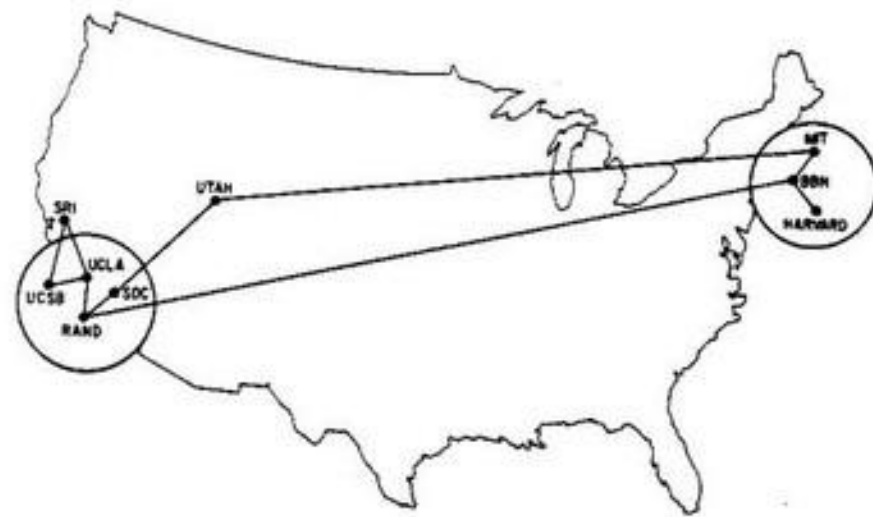


ARPANET

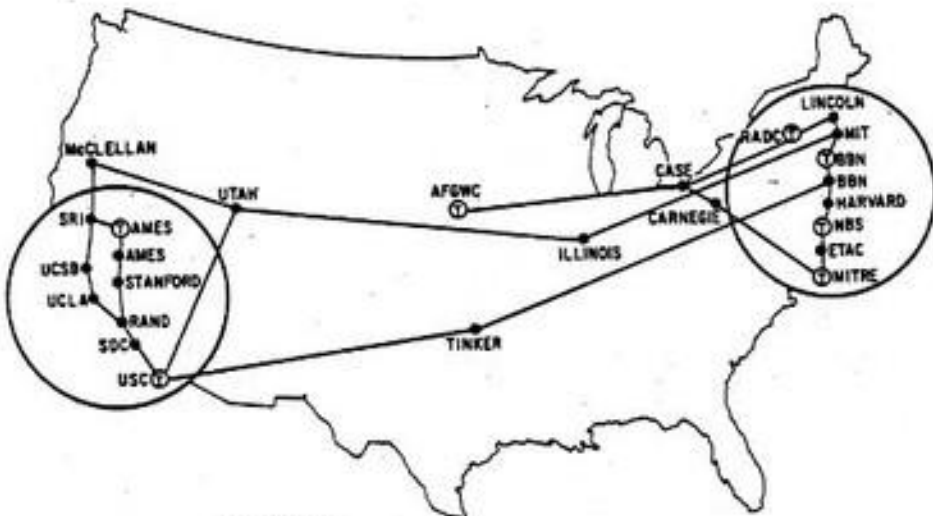
- 1973 – Europe joined the network
 - Norway and UK („emails“)
 - 1976 – Queen Elizabeth used the network
- 1983 – Separation of ARPANET → MILNET → 68 nodes lost from ARPANET
- 1983 – NCP replaced by TCP/IP
- Establishments of LANs (NSFNET) → ARPANET as backbone network
- Disconnected in 1990



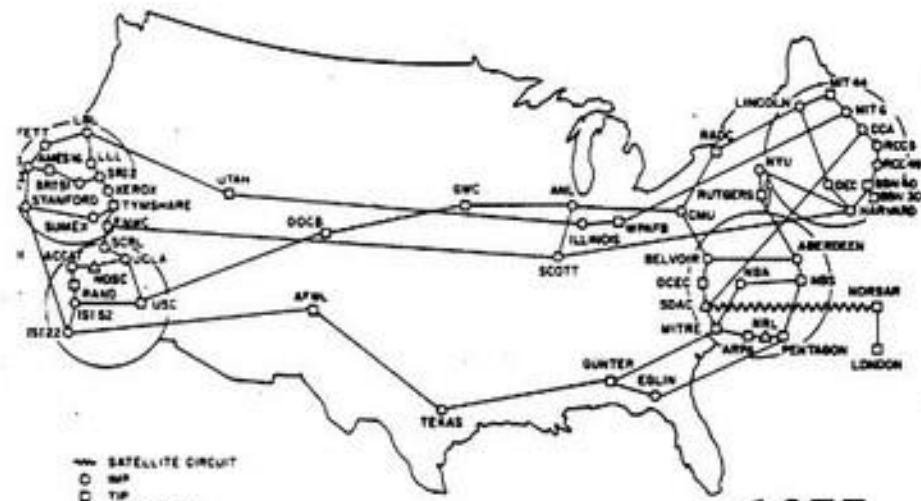
1969



1970



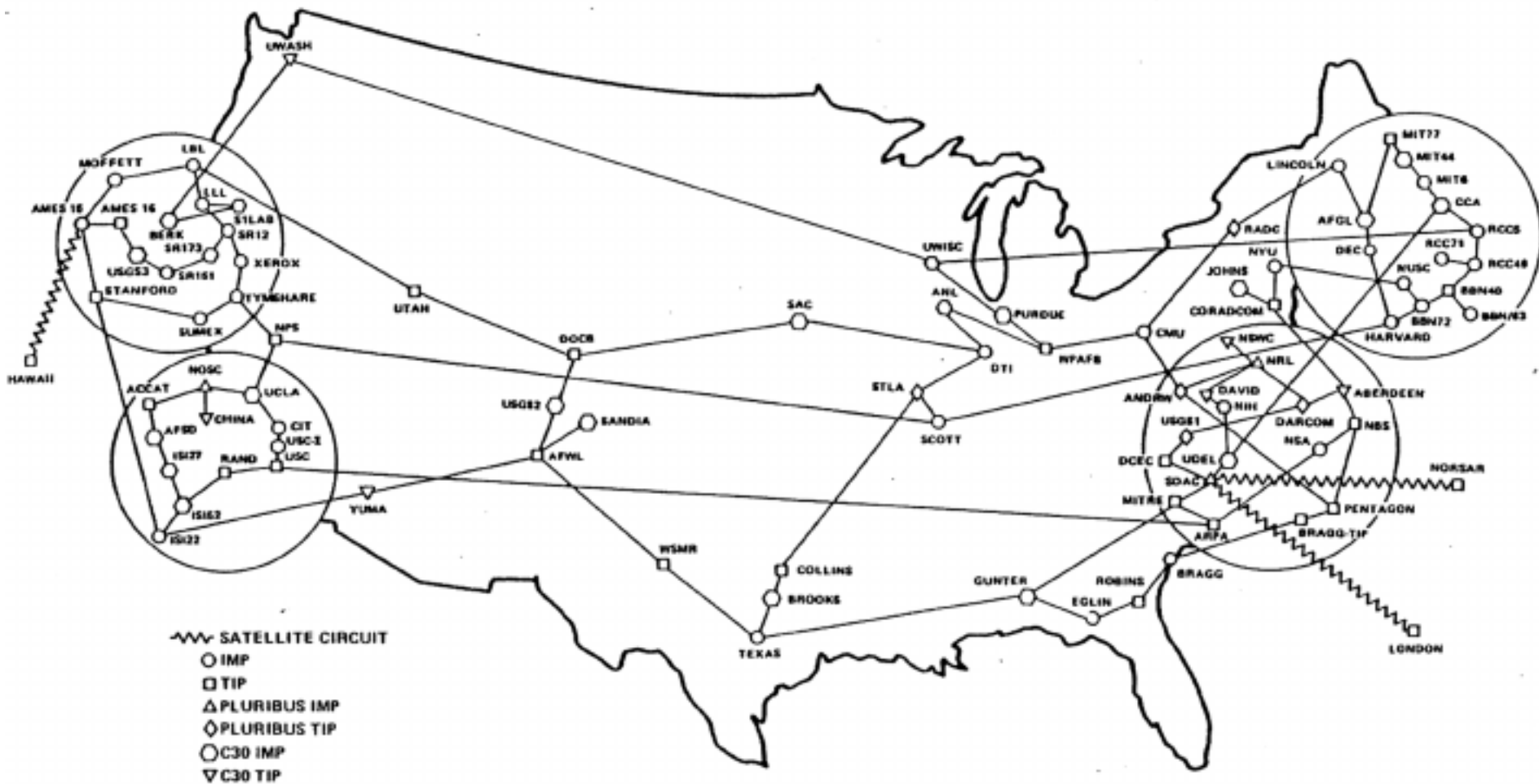
1972



1977

--- SATELLITE CIRCUIT
 ○ IMP
 □ TIP
 ⊕ PLURIBUS IMP
 (NOTE: THIS MAP DOES NOT SHOW ARPANET (EXPERIMENTAL SATELLITE CONNECTIONS))
 NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

ARPANET GEOGRAPHIC MAP, JANUARY 1982



(NOTE: THIS MAP DOES NOT SHOW ARPA'S EXPERIMENTAL SATELLITE CONNECTIONS)
 NAMES SHOWN ARE IMP NAMES. NOT (NECESSARILY) HOST NAMES

Computer Networks

- Computers
 - Multi-users with limited communication
- Computer network
 - Computers are connected and cooperating
 - They keep their identity
- Distributed operating system
 - Cluster of computers, which is compact unit
 - Inner structure is transparent to the user

Computer Networks

- Sharing resources
 - Data sets and files (programs, data)
 - Technical resources (peripherals, capacities)
- Communication
 - Between users – email, messaging, social networks
 - Between programs – distributed apps

Computer Networks

- Higher reliability
 - Back-ups
 - Redundant infrastructures
- Costs savings
 - Network of rather small computers is cheaper than one super-computer
 - Nowadays we have computer clusters and grids

Computer Networks - classification

- Switching
- Node connection
- Signal type
- Geographical scale
- Property/ownership

Computer Networks – classification (Switching)

- Circuit switched network
 - Oldest technology (telegraphy, telephony, ISDN)
 - Connection established for two nodes
 - Communication channel open as long as the „call“ lasts (bit stream)
 - Connection via operator's exchange/switchboard
 - The link remains reserved even if no communication
 - Virtual circuit switched network

Computer Networks – classification (Switching)

- Circuit switched network

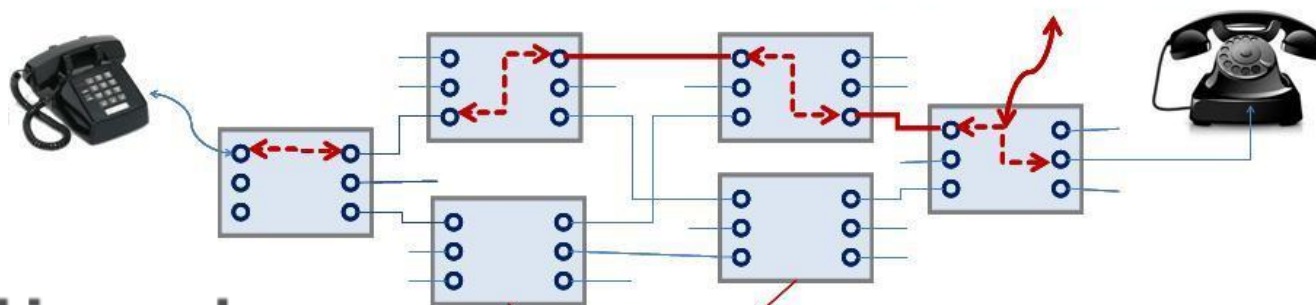
–cons & pros:

- reduced communication speed, comm. between 2 nodes, set up
- + „low“ acquisition, running costs, reliability (fast, errorless)

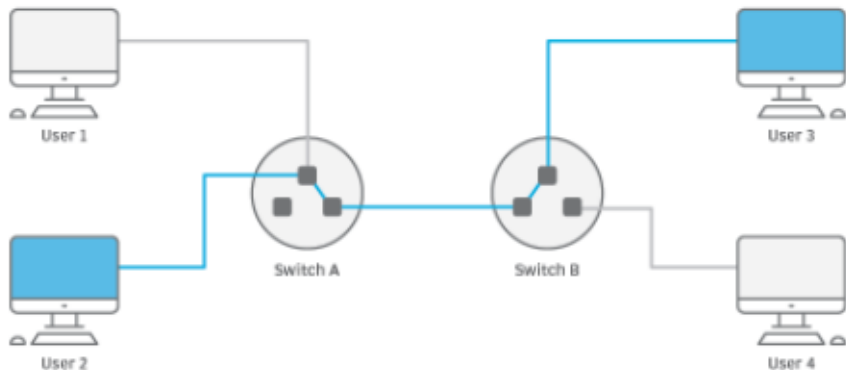
Computer Networks – classification (Switching)

- Circuit switched network

Physical Connection is setup
When call connection is made



How circuit switching works

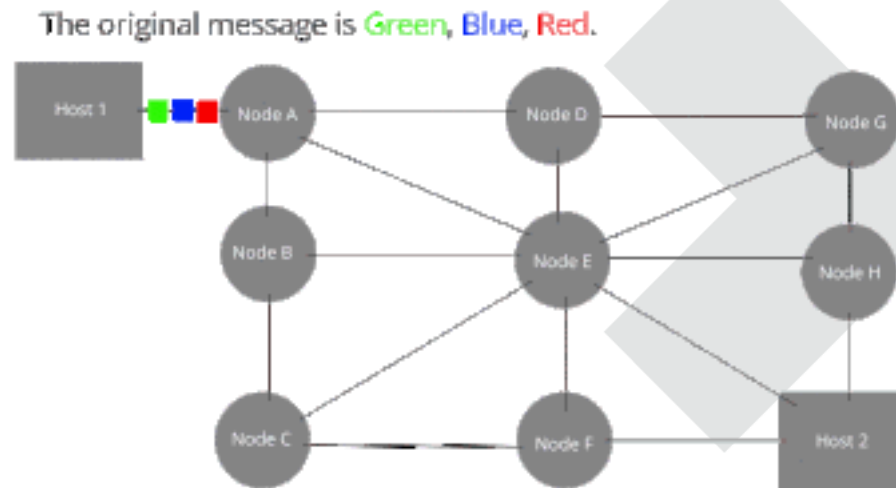


Computer Networks – classification (Switching)

- Packet network
 - Most of data is transmitted in packets
 - Packet is formatted unit of data (~10B to kB long)
 - Packet = control information and data (payload)
 - Topology and active network nodes (routers, switches, usually FIFO)
 - Basis for the Internet communication
 - Used in mobile-phone comm. (GSM vs. GPRS/XG)

Computer Networks – classification (Switching)

- Packet network
 - Bandwidth is shared among users (the packet route is not known „a priori“)



IP version 4 packet

Cor

• P

I

I

I

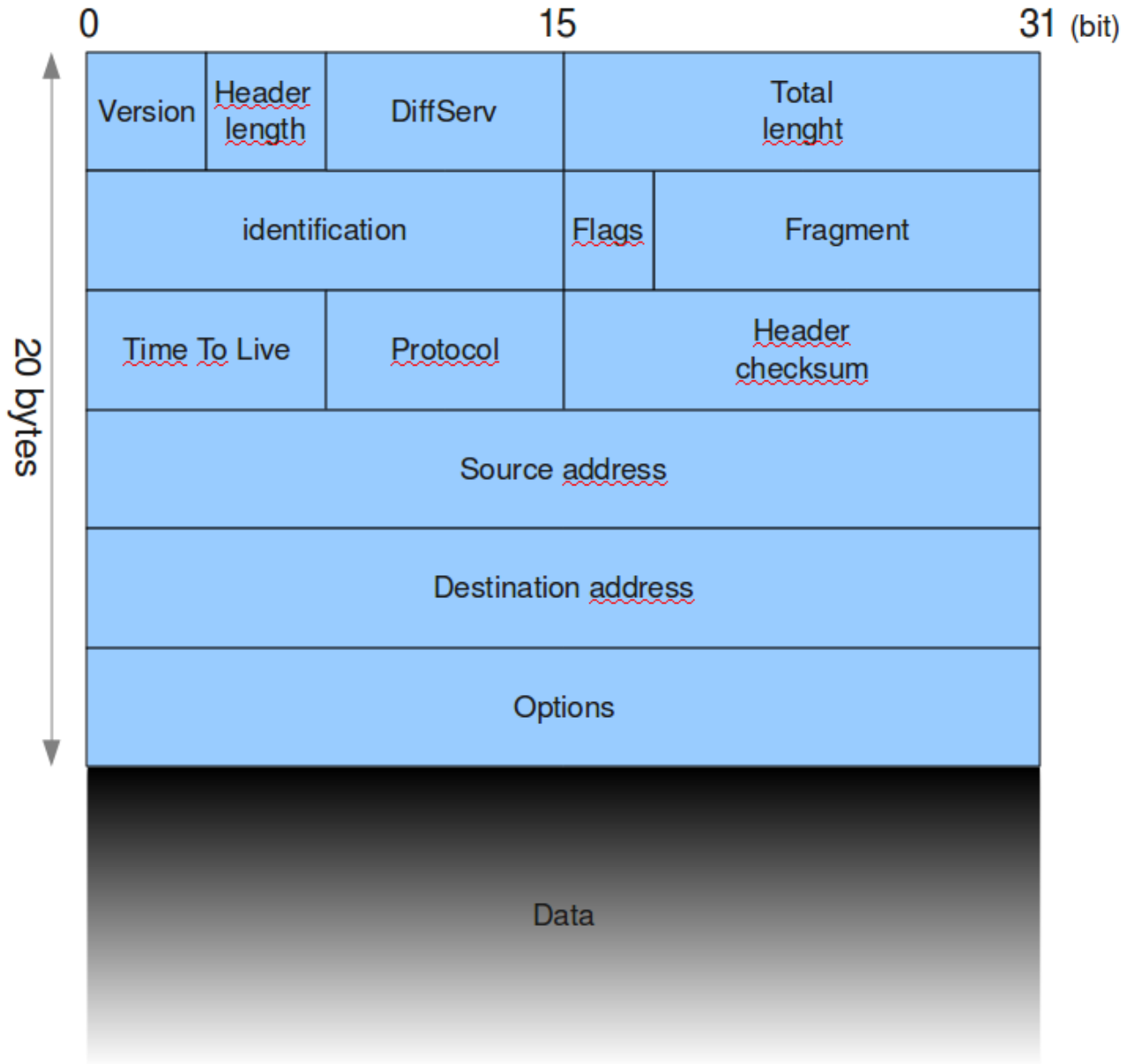
I

2

I

I

I



ing)

ng)

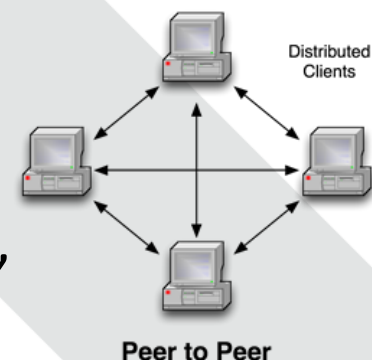
d)

3G)

Computer Networks – classification (node conn.)

- Peer-to-peer (P2P)

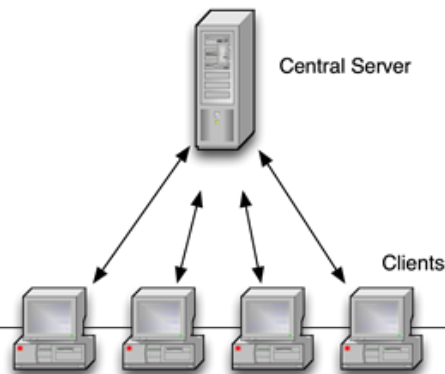
- all nodes are equal (no central coordination)
- all computers can share their resources (memory, peripherals, files etc...)
- common for data sharing/exchange
- + more users --> overall available speed increases
- - (i)legality – authors rights, attacks („infections“, spams, viruses, Troys), terrorism
- example – BitTorrent, Napster (music), DC, Bitcoin...



Computer Networks – classification (node conn.)

- Client-server

- One (or more) computer (servers) is superior to another one (or more) computer (clients)
- Server offers services to others „common“ computers (workstations)
- example – file, email, print, WWW server etc.



Client / Server

Computer Networks – classification (signal type)

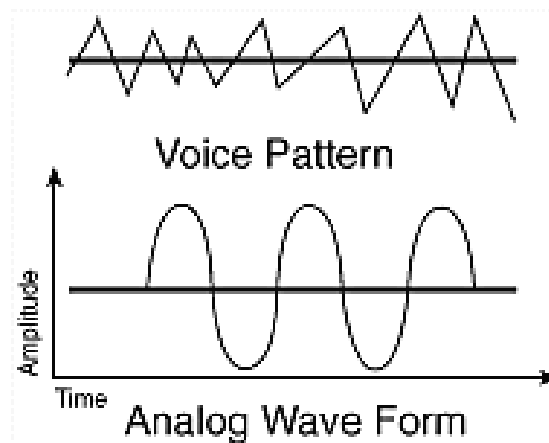
- Analogue network

- Works with analogue (continuous) signal

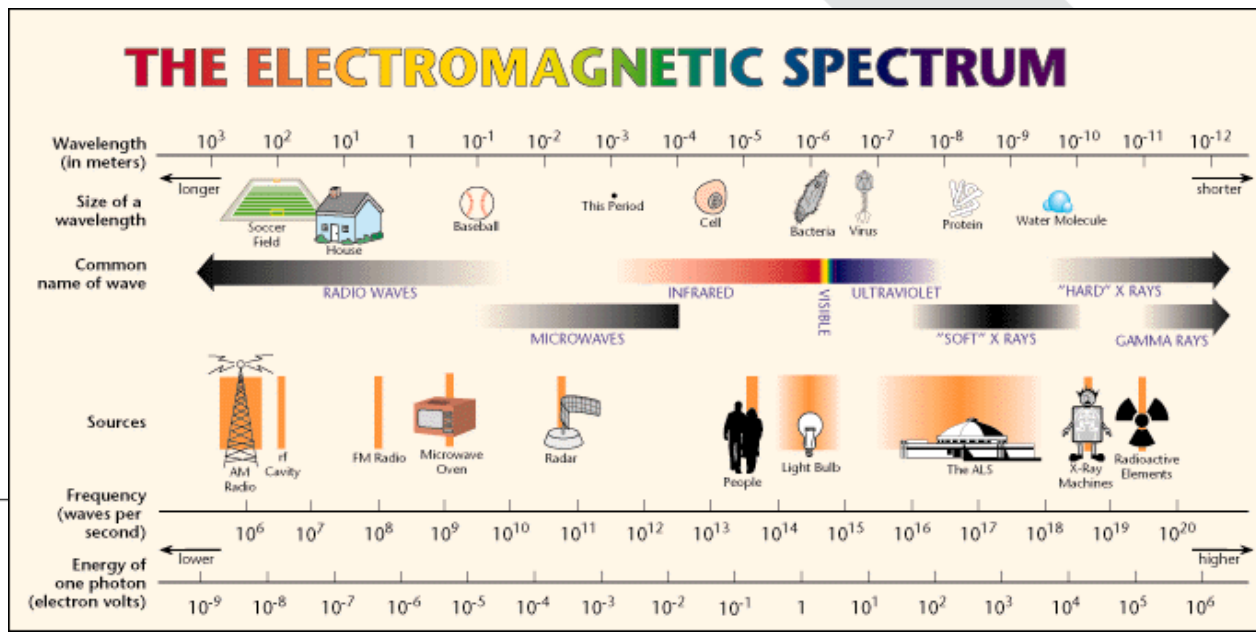
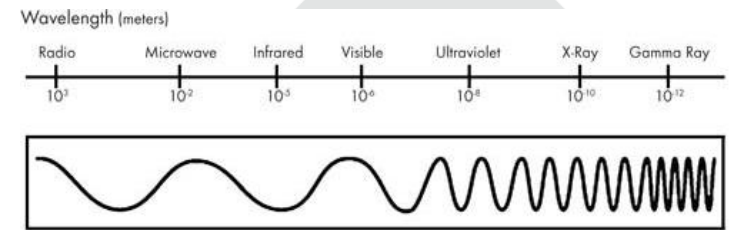
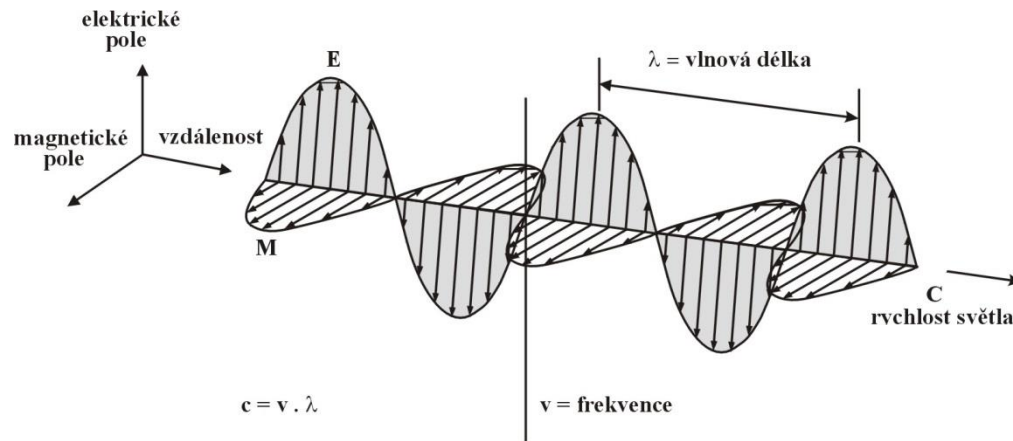
- Amplitude and frequency

- Example:

- you speak to handset – change in air pressure – collected by a handset -- amplified and then converted into current, or voltage fluctuations:



Computer Networks – classification (signal type)



Computer Networks – classification (signal type)

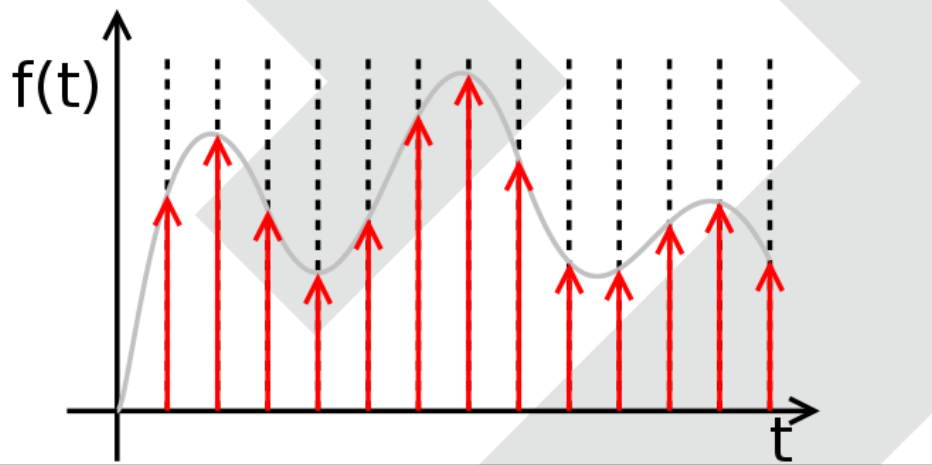
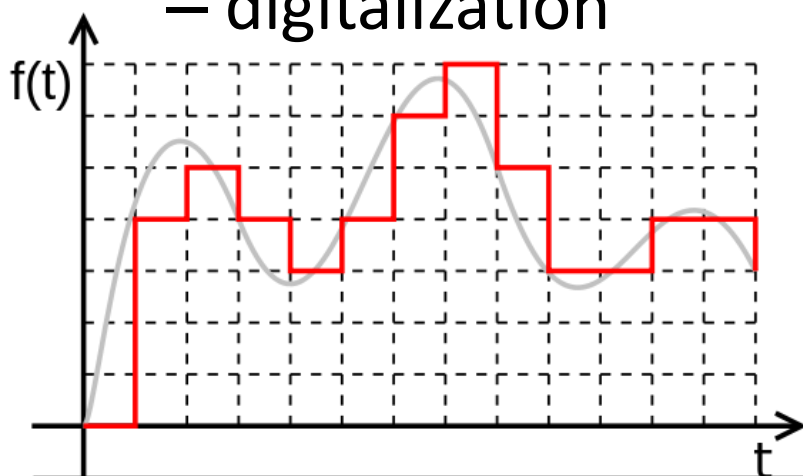
- Digital network
 - Works with digital (discrete) signal pulses (1/0)
 - All techniques valid with analogue signal (amplifying, filtering etc.) could be applied on digital
 - Analogue signal is chopped to form digital one
 - advantages - ?

Computer Networks – classification (signal type)

- Digital signal

- sampling - continuous-valued discrete-time signal
- quantization (replaces each sample value by an approximation selected from a given discrete set)

– digitalization



Computer Networks – classification (signal type)

Feature	Analog Characteristics	Digital Characteristics
Signal	Continuously variable, in both amplitude and frequency	Discrete signal, represented as either changes in voltage or changes in light levels
Traffic measurement	Hz (for example, a telephone channel is 4KHz)	Bits per second (for example, a T-1 line carries 1.544Mbps, and an E-1 line transports 2.048Mbps)
Bandwidth	Low bandwidth (4KHz), which means low data transmission rates (up to 33.6Kbps) because of limited channel bandwidth	High bandwidth that can support high-speed data and emerging applications that involve video and multimedia

Computer Networks – classification (signal type)

Feature	Analog Characteristics	Digital Characteristics
Network capacity	Low; one conversation per telephone channel	High; multiplexers enable multiple conversations to share a communications channel and hence to achieve greater transmission efficiencies
Network manageability	Poor; a lot of labor is needed for network maintenance and control because dumb analog devices do not provide management information streams that allow the device to be remotely managed	Good; smart devices produce alerts, alarms, traffic statistics, and performance measurements, and technicians at a network control center (NCC) or network operations center (NOC) can remotely monitor and manage the various network elements
Network capacity	Low; one conversation per telephone channel	High; multiplexers enable multiple conversations to share a communications channel and hence to achieve greater transmission efficiencies

Computer Networks – classification (signal type)

Feature	Analog Characteristics	Digital Characteristics
Power requirement	High because the signal contains a wide range of frequencies and amplitudes	Low because only two discrete signals—the one and the zero—need to be transmitted
Security	Poor; when you tap into an analog circuit, you hear the voice stream in its native form, and it is difficult to detect an intrusion	Good; encryption can be used
Error rates	High; 10^{-5} bits (that is, 1 in 100,000 bits) is guaranteed to have an error	Low; with twisted-pair, 10^{-7} (that, is 1 in 10 million bits per second) will have an error, with satellite, 10^{-9} (that is, 1 in 1 billion per second) will have an error, and with fiber, 10^{-11} (that is only 1 in 10 trillion bits per second) will have an error

Computer Networks – classification (geo scale)

- PAN
- LAN (WLAN)
- MAN
- WAN

- others – HAN (Home), SAN (Storage), CAN (Campus), GAN (Global), RAN (radio) VPN, Ambient network

Computer Networks – classification (geo scale)

- **PAN – Personal area network**
- Using devices such as mobile phone, PDA, laptop/notebook, tablet, smart watches, printers, video games consoles etc.
- Transfer via USB/FireWire, IrDA, Bluetooth
- Short distances (few meters – up to 10 meters)

Computer Networks – classification (geo scale)

- PAN – Personal area network



Computer Networks – classification (geo scale)

- **LAN – Local area network**
- smaller scale (room/building/block of buildings)
- own cabling and equipment (e.g. optical fiber, active network nodes,...)
- runs at 10 Mb/s to 10 Gb/s
- low error rate (wired networks)
- formerly for resources sharing
- example: MVSO + Tesco SW

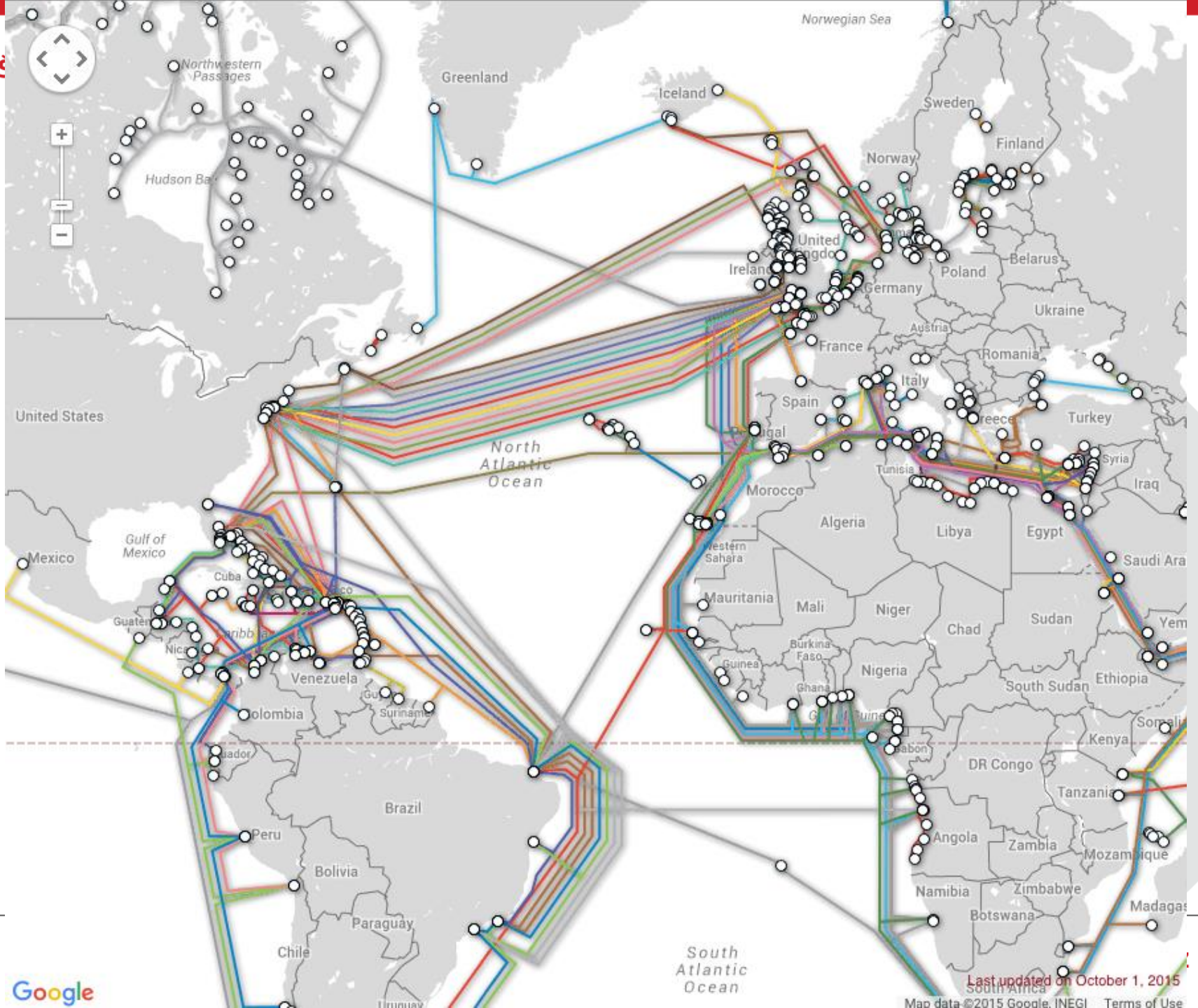
Computer Networks – classification (geo scale)

- **MAN – Metropolitan area network**
- covering the whole city/town (or several blocks)
- operated by one institution (company or local authority), but...
- ... cabling and network equipment is rent/leased
- technically – more LANs wirelessly connected
- example: DQDB – up to 100 km (two nodes max 2km), up to 155 Mb/s

Computer Networks – classification (geo scale)

- **WAN – Wide area network**
- broad area – up to international scale
- leased cabling and infrastructure (optical fibres, microwave channels, satellites)
- great variety of bandwidth (65 kb/s to 100 Gb/s)
- formerly for remote access and communication among users
- WAN is being replaced by VPN





Last updated on October 1, 2015

Computer Networks – classification (ownership)

- PDN – Public data network
 - operated by a telecommunications administration, or a recognized private operating agency
- PN – Private network
 - uses private IP address space, „private“ packets cannot be transmitted via public Internet
- VPN – Virtual private network
 - connection to private computers via public network
 - establishes access to intranet (security issues)

Computer Networks – classification (others)

- Ambient network
 - combination of PAN, LAN/WLAN and mobile networks
 - concept of „not disconnected“ communitation (joining networks) --- EU FP6

- Example:

Laptop → (Bluetooth) → Mobile → (GPRS) → mobile signal provider → Internet

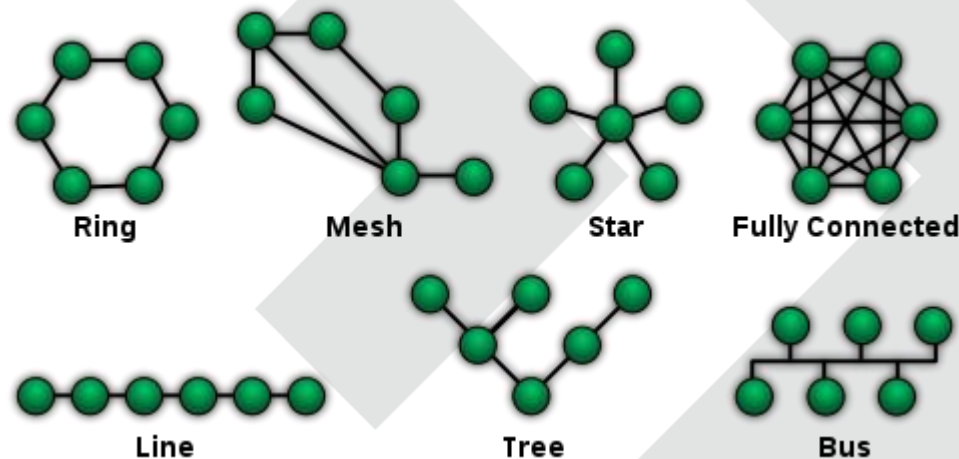
PDA → (bluetooth) → Laptop → (WLAN) → AP

Computer Networks – classification (others)

- Ambient network
 - combination of PAN, LAN/WLAN and mobile networks
- HAN – Home area network
 - communication among home digital devices
- SAN – Storage area network
 - connection to storage capacity of various devices, which appear like locally attached to the operating system

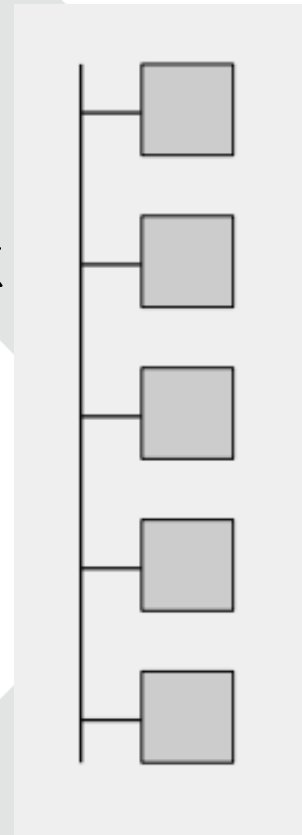
Computer Networks – topology

- Arrangement of various elements in computer network (mainly cabling and active components)
- Basic types:
 - Point-to-point
 - Bus network
 - Star network
 - Ring network
 - Tree network
 - Mesh network



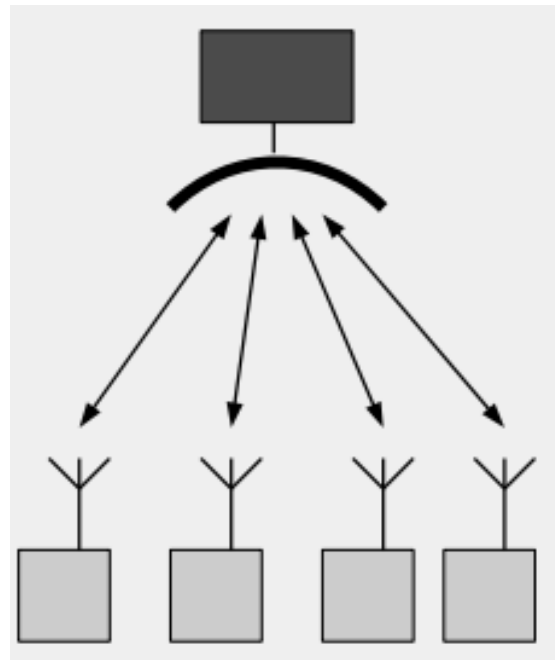
Computer Networks – topology (Bus network)

- one transmitting medium
- data are sent in one direction (async.)
- if a single node is damaged – all network transmission ceased
- every station receives all network traffic
- equal transmission priority
- + easy to connect, less cabling, small net
- - if something breaks, all net. collapse



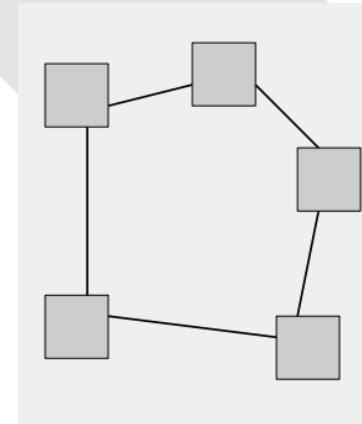
Computer Networks – topology (Bus network)

- with one central station
- used for WLAN



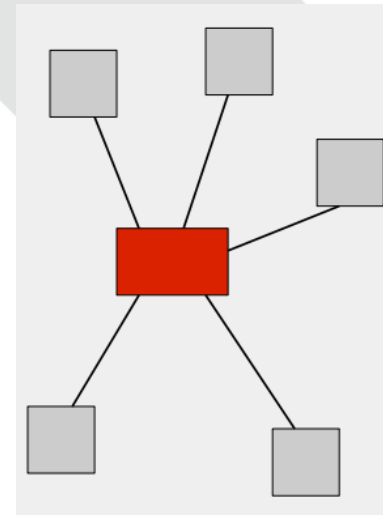
Computer Networks – topology (Ring network)

- every node (computer) is connected to another two (to form a circle)
- data have to pass through every single node between start/end node
- + easy-to-transmit, minimal delay time, no packets collision, highest bandwidth
- - if failure, then problem



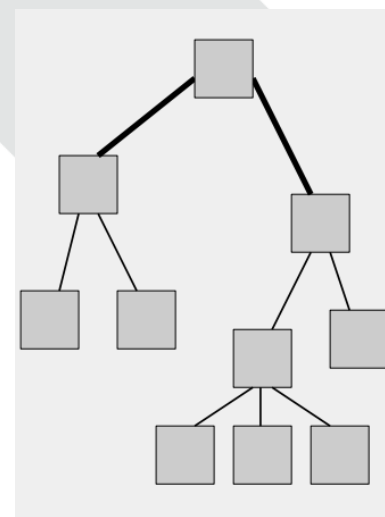
Computer Networks – topology (Star network)

- most used network topology
- computers are connected to the central point (hub or switch)
- one link between central point and computer
- + if failure of one computer, it works; no packets collision, easy to expand
- - many cables, special hw (central p.)



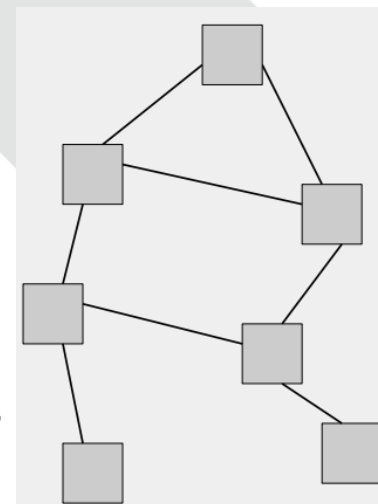
Computer Networks – topology (Tree network)

- combination of Bus and Star
- broad area networks
- in most cases B-tree types
- + scalable, point-to-point connection, easier fault identification and isolation
- - many cables, hard to maintain, if backbone fails, the entire network falls



Computer Networks – topology (Mesh network)

- connection among nodes
- no central feature
- represented by a general graph
- shortest path bridging
- + scalable, lower sensitivity to failures, decentralized
- - ???



Computer Networks – classification

VIDEO

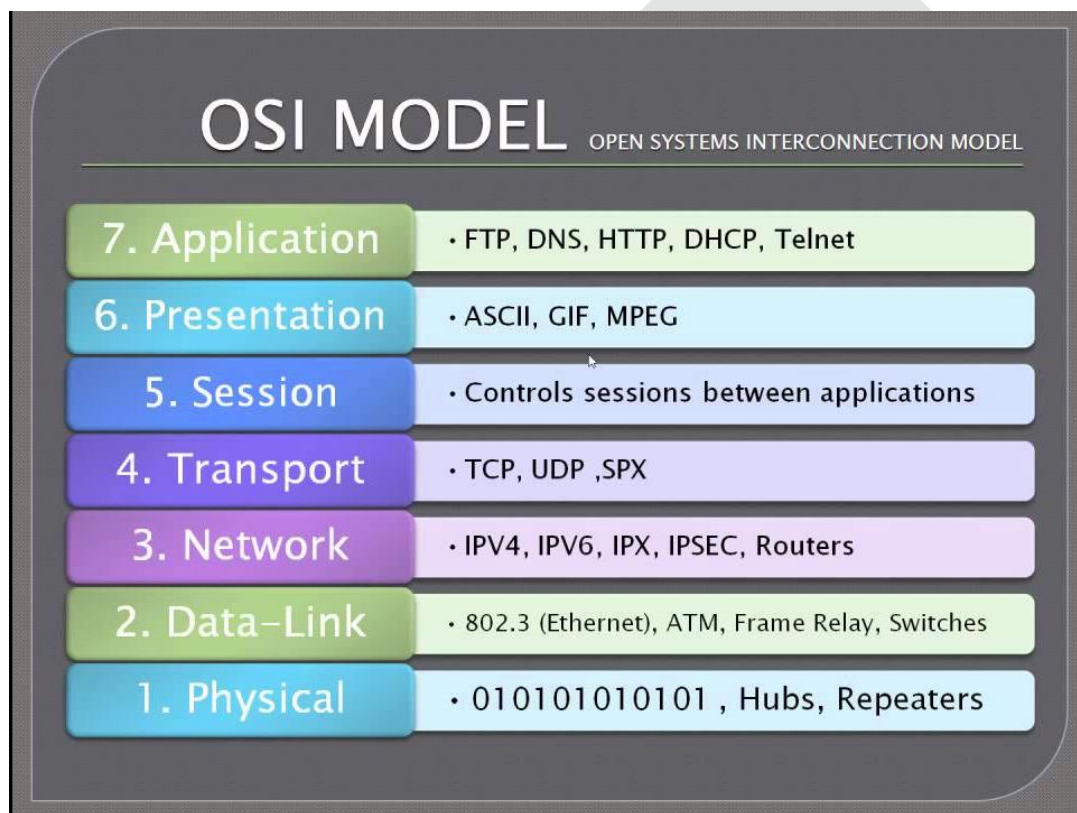
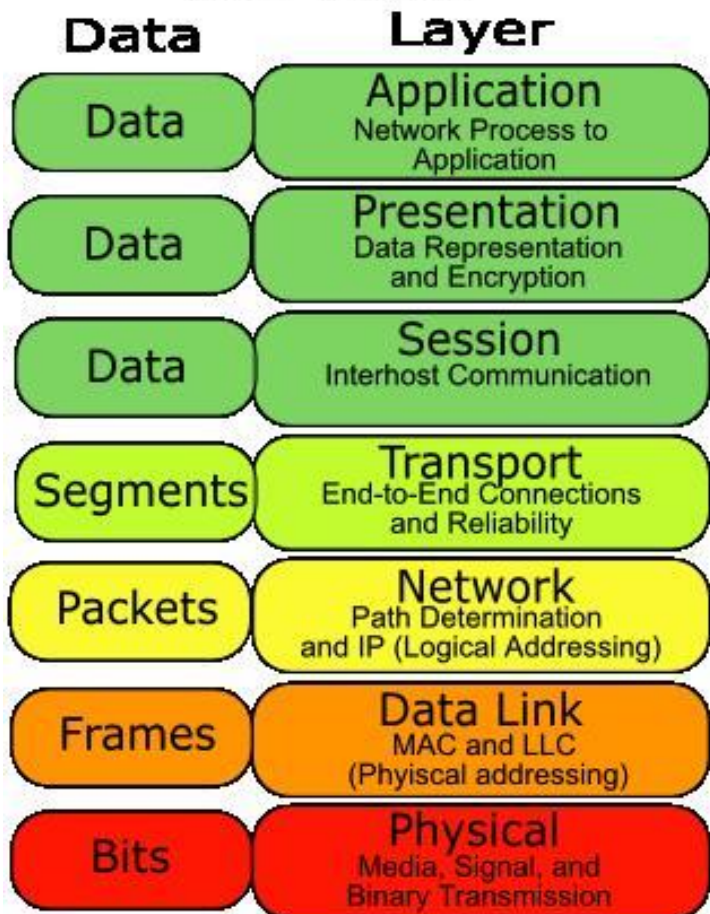
ISO/OSI model

Computer Networks – former heterogeneity

- Experimental networks (ARPANET, CYCLADES, SNA from IBM, DNA from DEC)
- Need for mutual inter-connection
- Layer architecture (main ideas):
 - individual layer for different abstraction degree
 - each layer should provide exactly specified functions
 - interface should minimize data-flow
 - number of layers should be optimized

Computer Networks – ISO OSI model

OSI Model

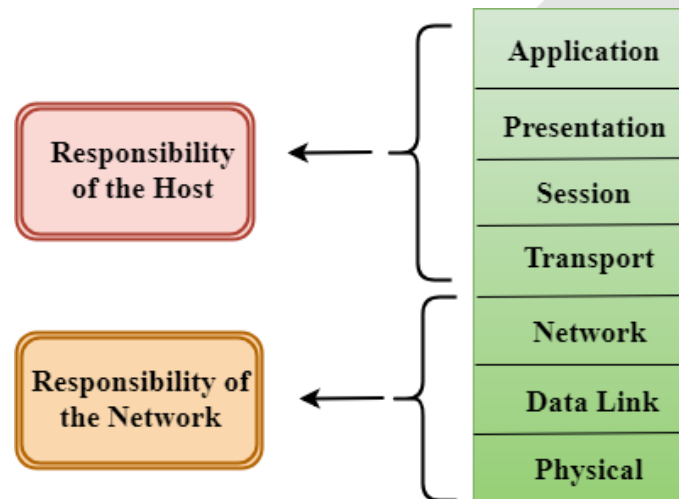


Computer Networks – ISO OSI

- Reference model OSI (Open Systems Interconnection)
 - Specified by ISO (International Organization for Standardization)
 - Needed for standardization of internet communication
 - ISO 7498 (y. 1984); ITU-T (X.200)
 - Layer-scheme describing the communication
 - Layers are independent and substitutable
 - Model objective = standards development
 - Implementation is not specified – but principles
 - Main aim = decomposition of the communication

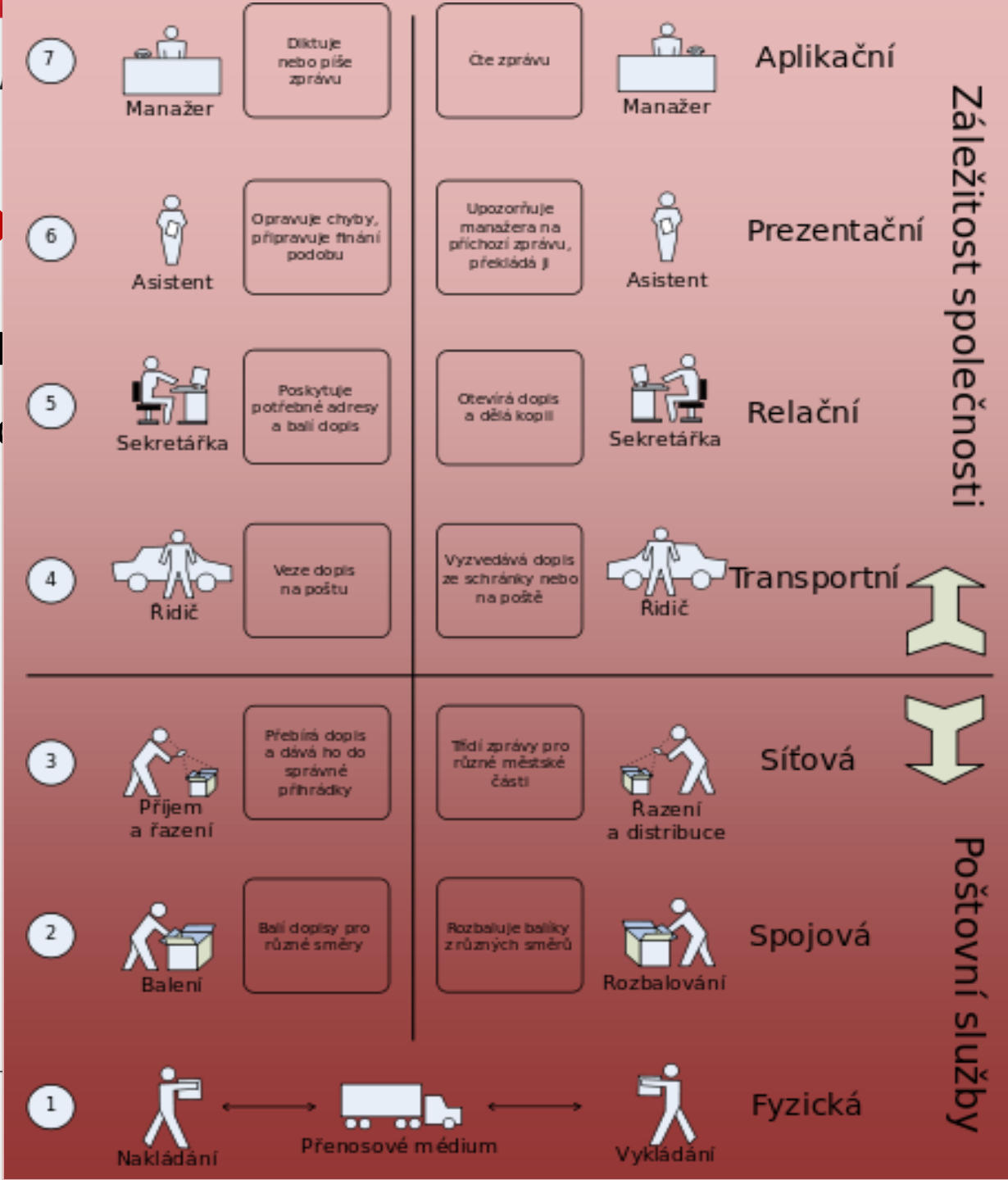
Computer Networks – ISO OSI

- Example:
 - Communication between companies' management
 - From UP to BOTTOM
 - Individual layers have communication „interface“



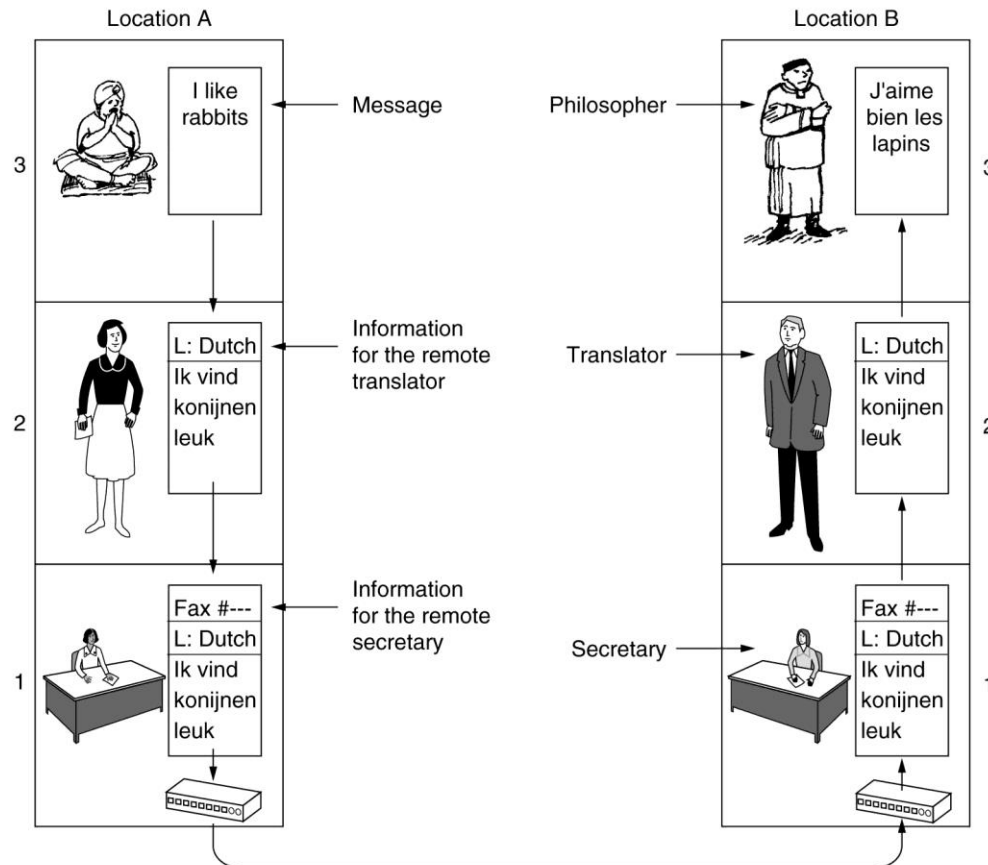
Comp

- Exa
- C



Computer Networks – ISO OSI

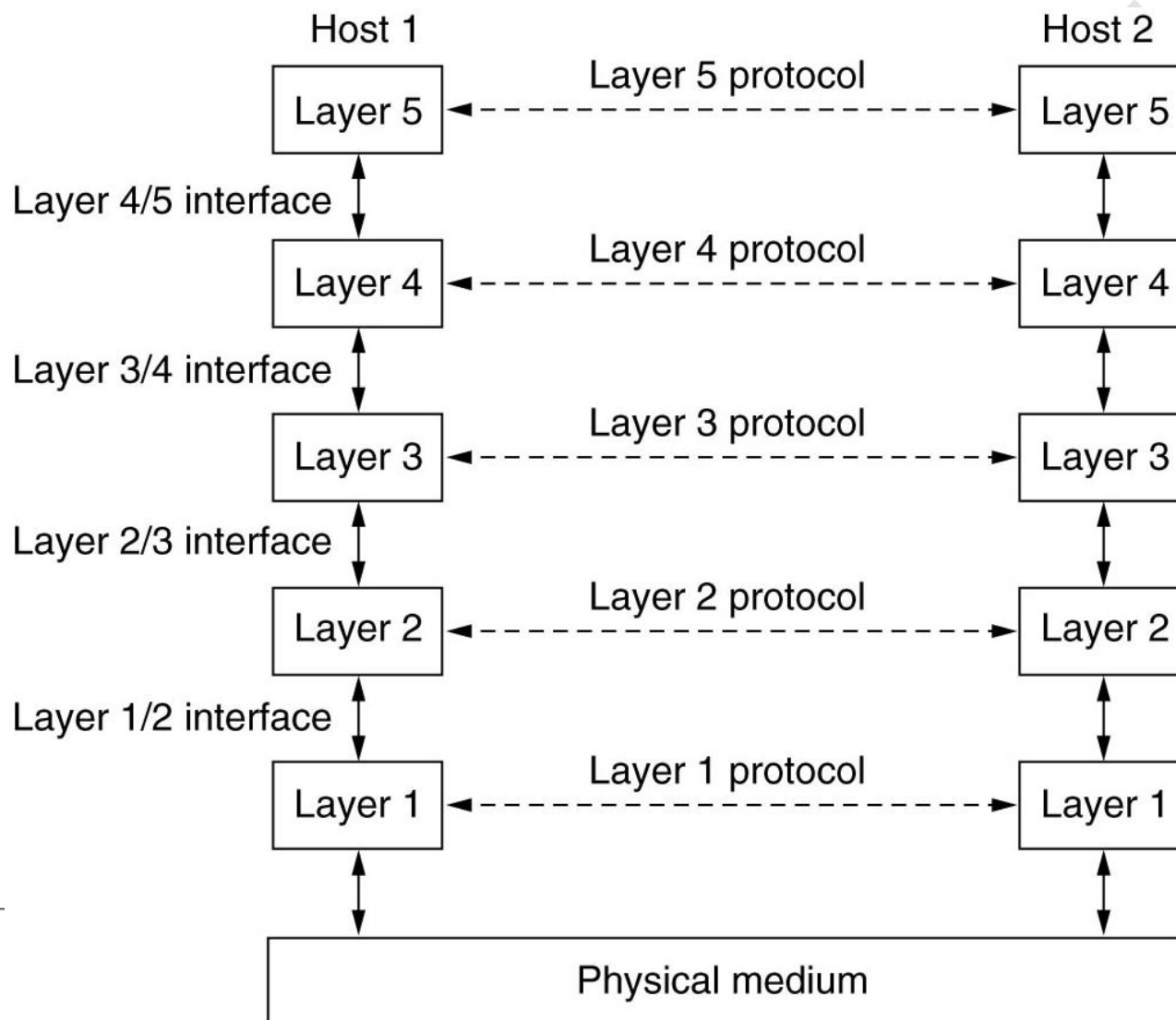
- Example (simplified):
 - Communication between two entities (people)



Computer Networks – ISO OSI

- Layer provides services to a higher-level layer
- Layer does not „bother“ higher layer
- Data are sent in packets and in each layer is enriched with new information (formatting, addresses etc.)
- If any layer is not active = it is null/transparent layer
- No layer can be skipped
- Communication:
 - Vertically -> via interface
 - Horizontally -> via protocols

ISO OSI – Communication



ISO OSI – Entities

- Entities:
 - are active objects of a layer
 - set of entities = layer
 - communicate with other system entities
 - carry functions and offer services (and consume services from preceding layer)
 - function = providing specified service
 - interact directly only with neighbouring layers' entities
 - example (at lower layers) – hardware devices (I/O ports)

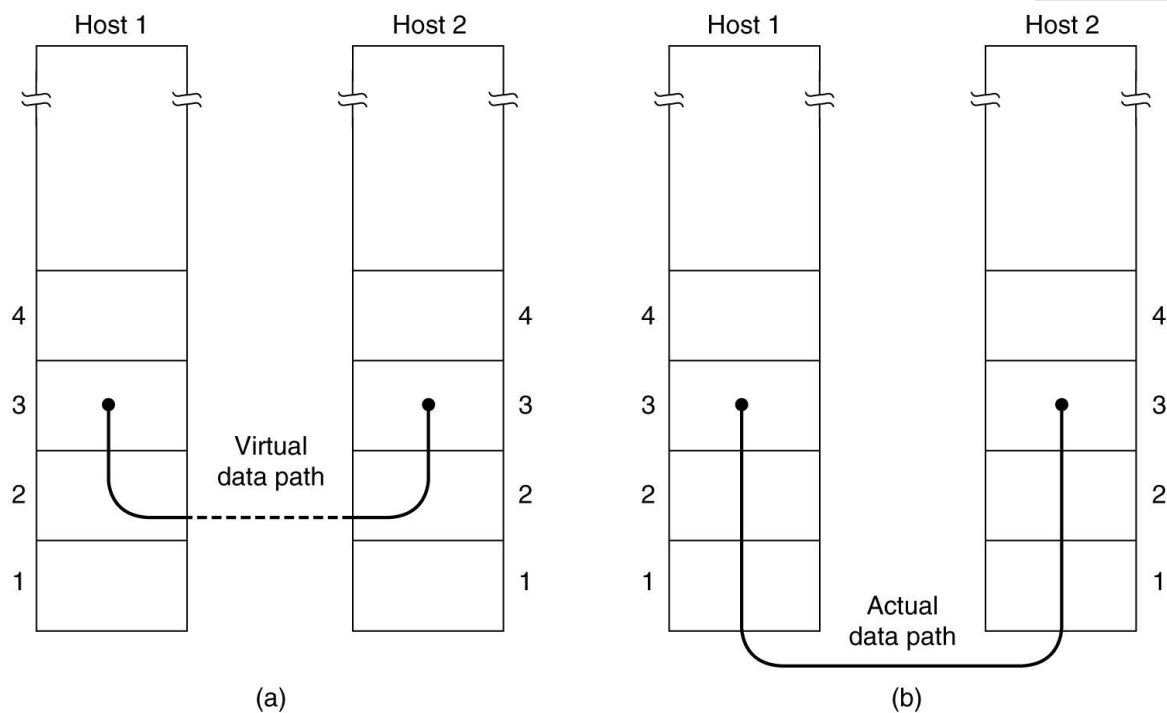
ISO OSI – Protocols & Services

- Protocol:
 - set of rules for communication of entities in the same layer
- Service:
 - for higher-level layer; using lower-level layer
 - offered in Service Access Points (SAP) having their addresses
 - interaction:
 - request (request for lower-level layer service)
 - confirm (no comment)
 - indication (info for higher-level layer to cause some action)
 - response (user reaction/action-end to indication)

ISO OSI – Protocols & Services

- Protocol:

- set of rules for communication of entities in the same layer



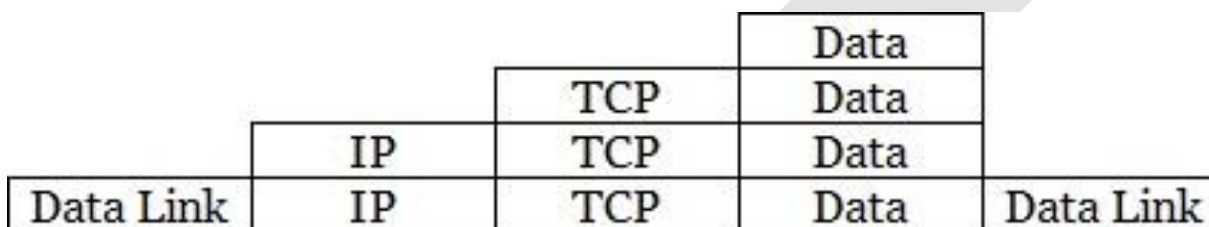
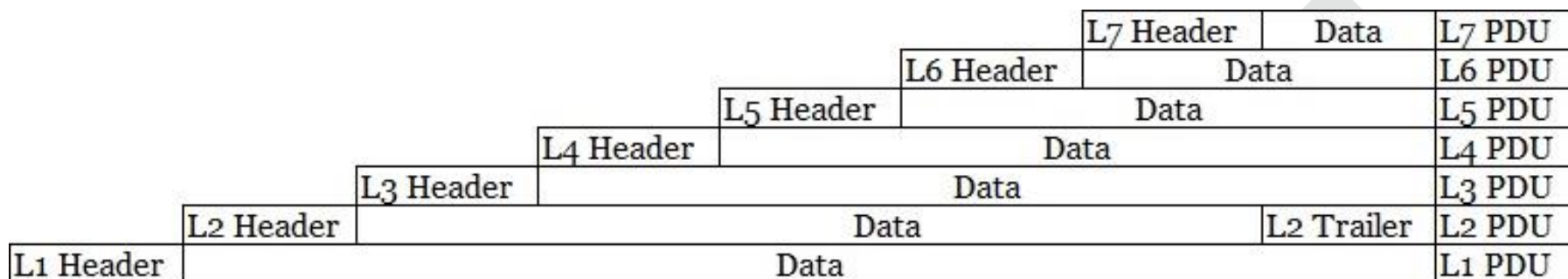
ISO OSI – Protocols & Services

- Protocol:
 - set of rules for communication of entities in the same layer
- Service:
 - for higher-level layer; using lower-level layer
 - offered in Service Access Points (SAP) having their addresses
 - interaction:
 - request (request for lower-level layer service)
 - confirm (no comment)
 - indication (info for higher-level layer to cause some action)
 - response (user reaction/action-end to indication)

ISO OSI – Services

- Services:
 - Connection-oriented services
 - connection – transmission – termination
 - connection is to be identified, both sides are communicating
 - example – telephony (classic, ISDN) or virtual connections (ATM)
 - Connectionless services
 - data are sent as a packets with end-point addresses (more than 1)
 - multicast (group of end-points) or broadcast (anyone could get it)
 - packets are independent to each other
 - example – link layer (LAN), IP protocol
 - Reliable (confirmation messages) or unreliable services

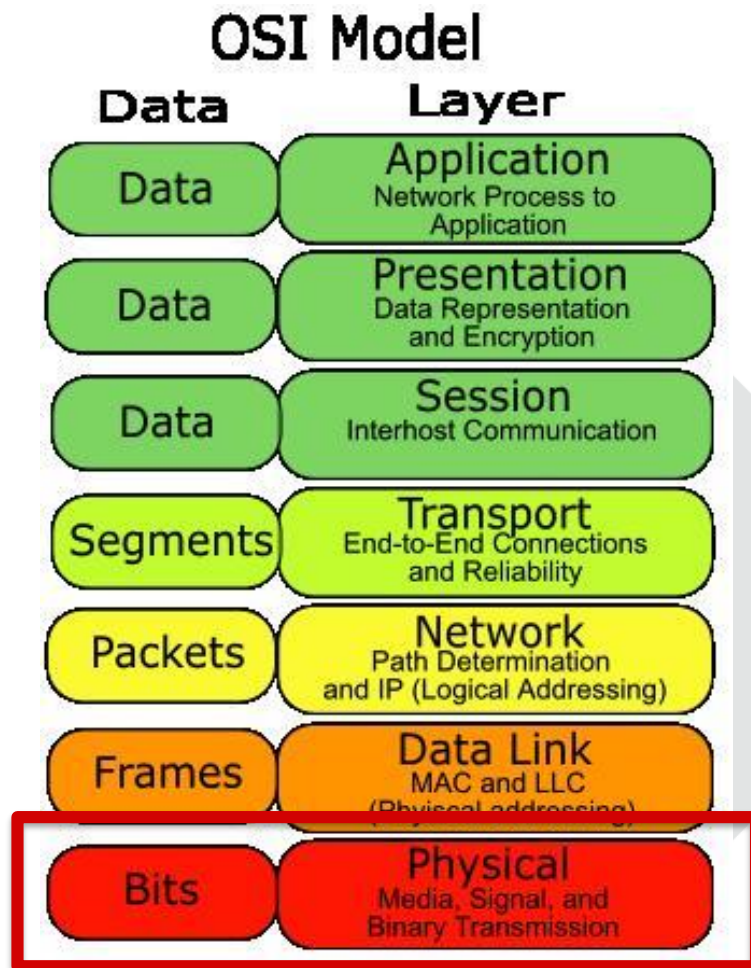
ISO OSI – Encapsulation



Computer Networks

Vít PÁSZTO

Network Layer



Physical layer

- Guarantee physical tasks
 - transforms bits into physical signal (and vice versa)
- Ensures electrical properties of a network:
 - voltage, frequency, modulation, speed, timing, synchronization, coding etc.
- And also mechanical properties of connectors:
 - shape, size and connectors
- Works with signal => via hardware
- All about physical elements in a network

Physical layer

- Activation, sustaining and deactivation physical connection for bits transmission
- Half or full duplex
- Services:
 - open/close physical connection
 - bits arranging into serial current
 - error messages for link layer
- example: RS232, V.35

Physical layer

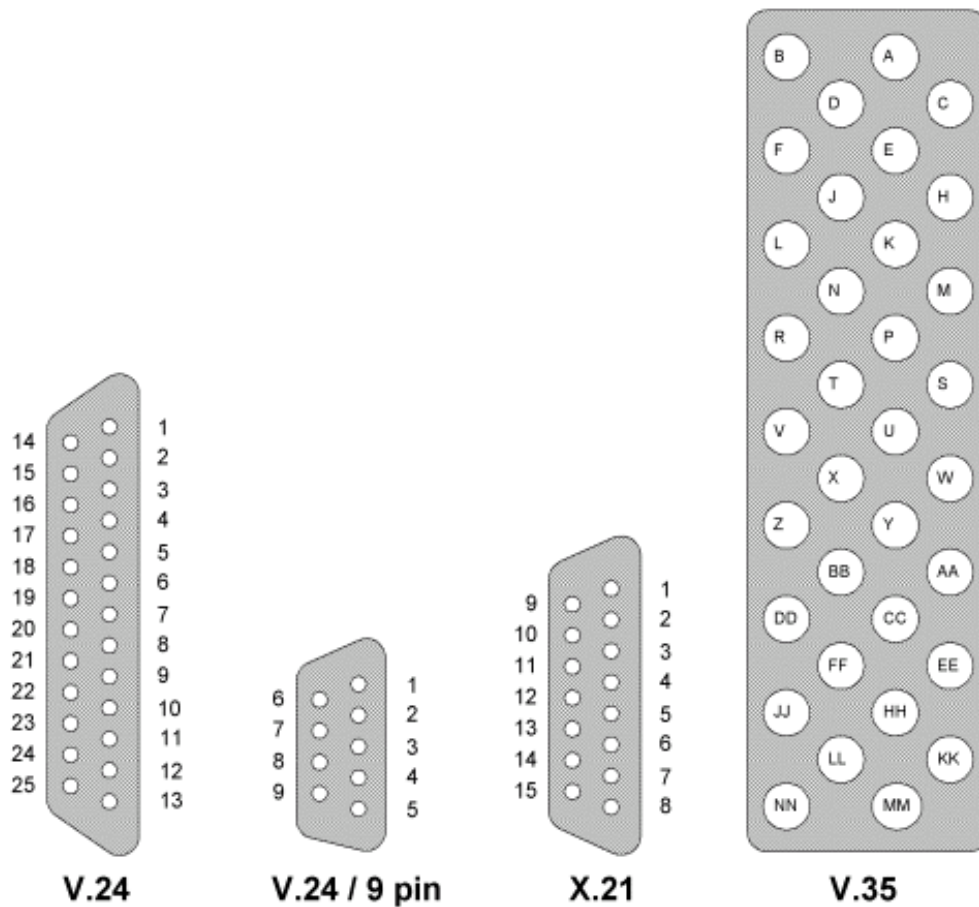
- What is it about?
 - modems
 - standards for communication
 - ISDN, DSL
 - cables
 - transmission technologies (Bluetooth, IrDA etc.)
 - connectors
 - active nodes

Physical layer

- Modem (<http://goo.gl/SriaSc>) - V.21, V.22, V.22bis, V.26bis, V.27ter, V.32, V.32bis, V.34, V.90, V.92, V.44
- Group of EIA standards – RS-232, RS-485 and RS-422
- ISDN (Integrated Services Digital Network)
- DSL (Digital Subscriber Line) / ADSL



Physical layer

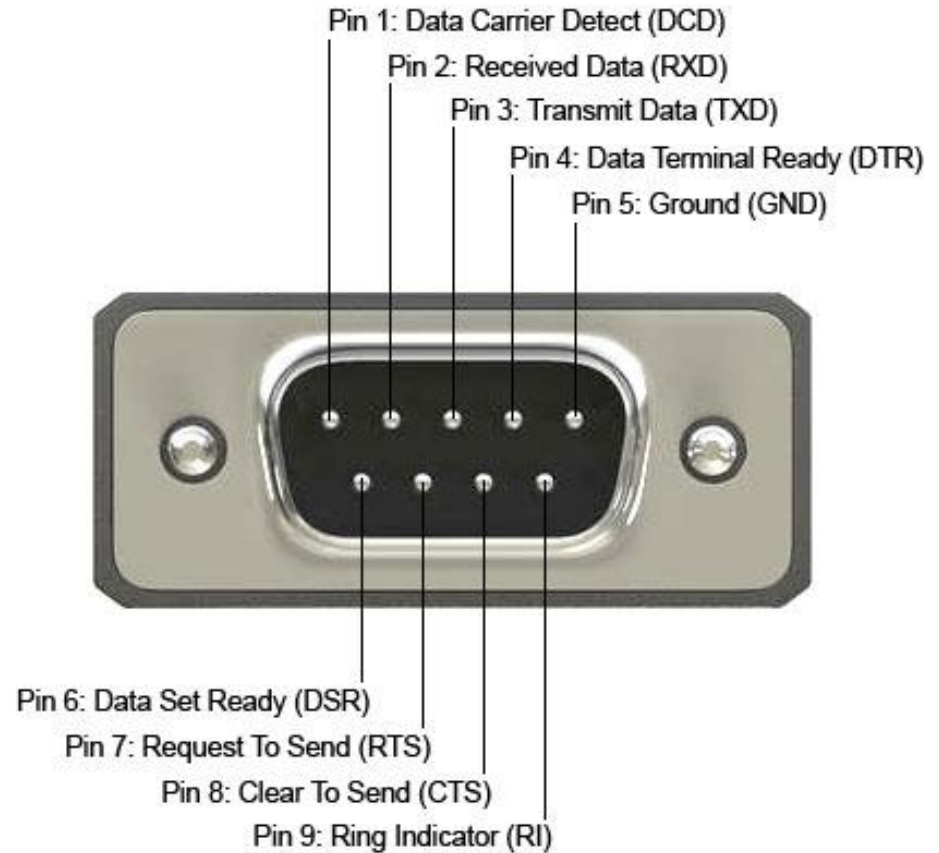


ITU	Kb/s
V.32	9,6
V.32bis	14,4
V.34	28, 8
V.34+	33,6
V.90	56 (switchboard to modem) 33,6 (modem to switchboard)

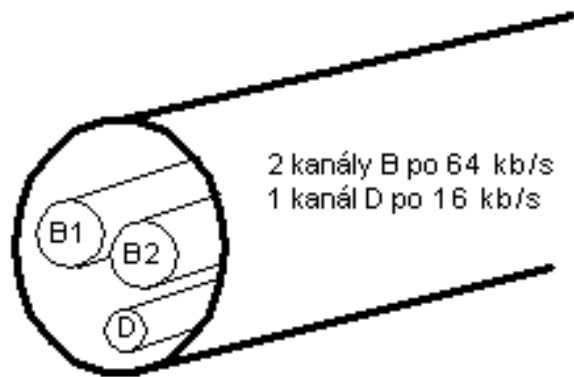
Physical layer



RS232 Pinout

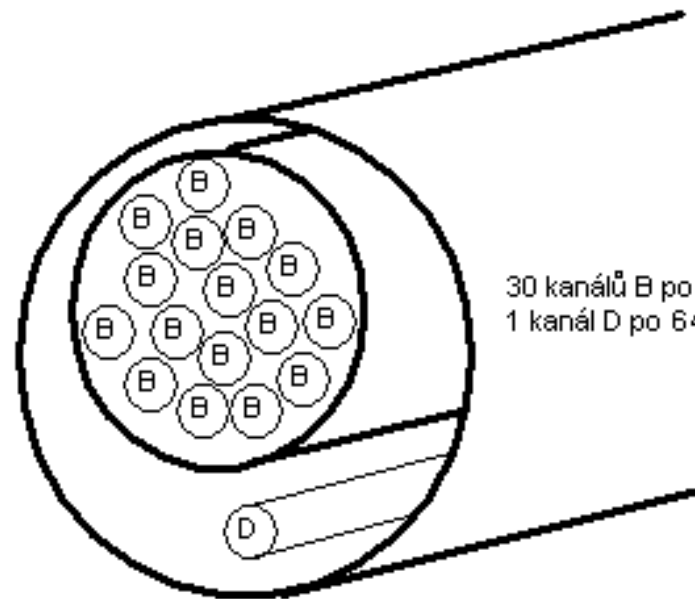


Physical layer



2 kanály B po 64 kb/s
1 kanál D po 16 kb/s

euroISDN2
(Basic Rate)

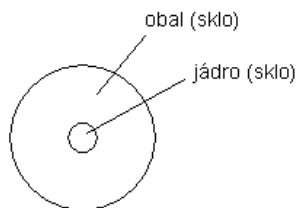
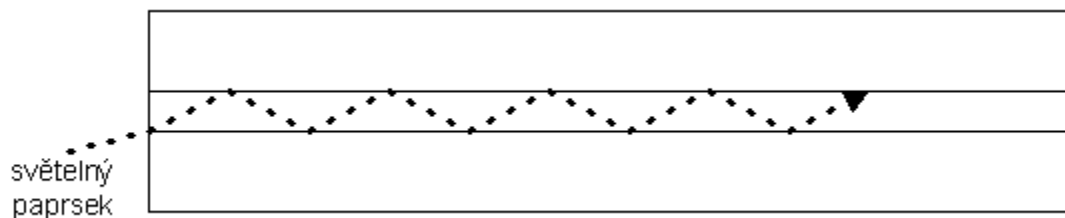


30 kanálů B po 64 kb/s
1 kanál D po 64 kb/s

euroISDN30
(Primary Rate)

Physical layer

- T1, E1 (multiplex digital data transmission)
- SONET/SDH (Synchronous Digital Hierarchy) – optical transmission
- 10Base2 (thin Ethernet) and 10Base-T (twisted pair cable)

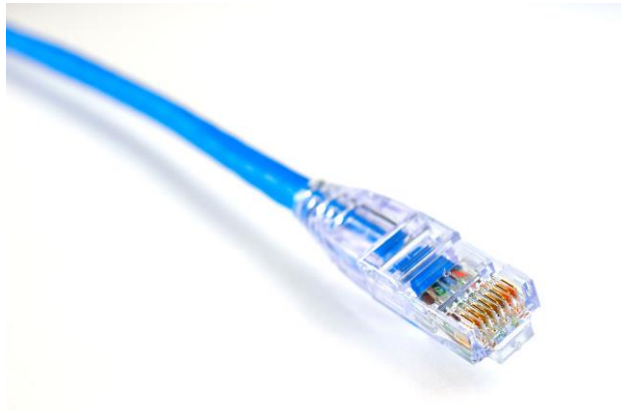


Signal	Speed
E0	64 kbit/s
E1	2,048 Mbit/s
E2	8,448 Mbit/s
E3	34,368 Mbit/s
E4	139,264 Mbit/s

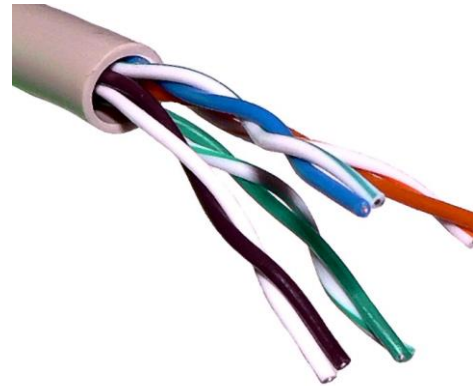
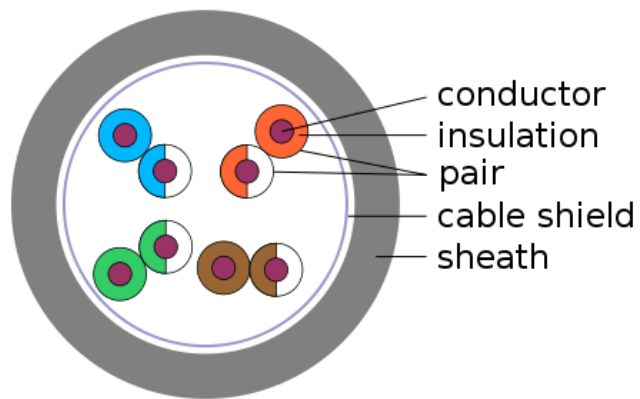
Physical layer



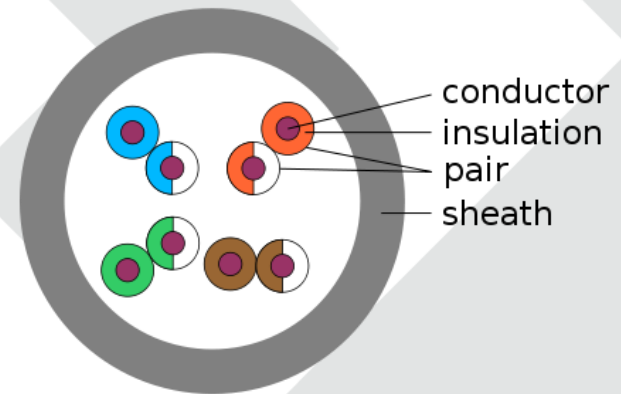
Physical layer





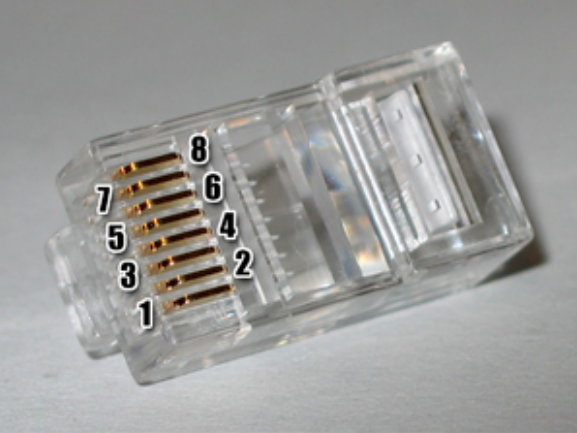














S/UTP



UTP



Physical layer

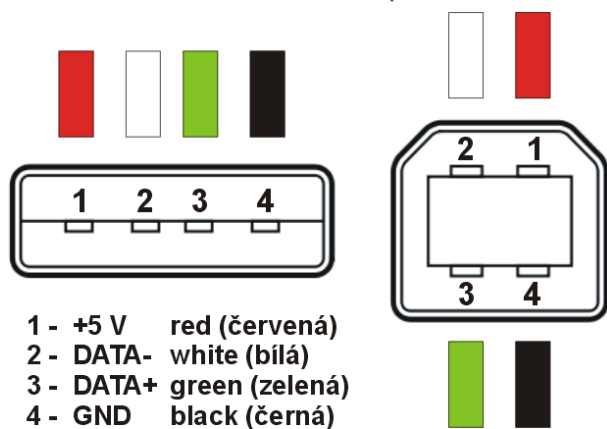
Pin	T568A Pair	T568B Pair	1000BASE-T Signal ID	Wire	T568A Color	T568B Color	Pins on plug face (socket is reversed)
1	3	2	DA+	tip	 white/green stripe	 white/orange stripe	
2	3	2	DA-	ring	 green solid	 orange solid	
3	2	3	DB+	tip	 white/orange stripe	 white/green stripe	
4	1	1	DC+	ring	 blue solid	 blue solid	
5	1	1	DC-	tip	 white/blue stripe	 white/blue stripe	
6	2	3	DB-	ring	 orange solid	 green solid	
7	4	4	DD+	tip	 white/brown stripe	 white/brown stripe	
8	4	4	DD-	ring	 brown solid	 brown solid	

Physical layer

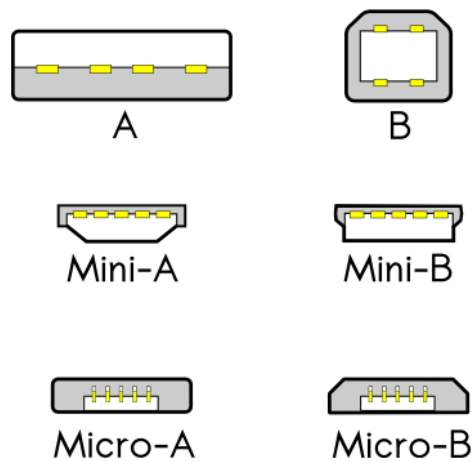
- Bluetooth
- IEEE 802.11
- FireWire
- IrDA
- USB

Physical layer

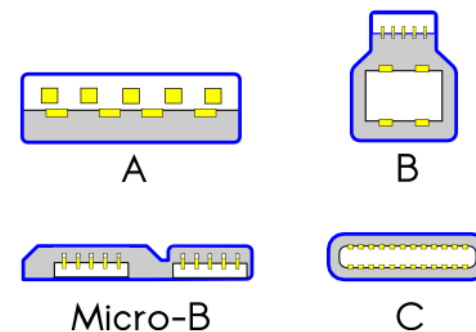
Schéma zapojení konektorů USB (na panelu - ♀)



USB 1.0 - 2.0



USB 3.0 - 3.1



Physical layer



USB camera Lumix, * mini USB, * type B, * female type A, * type A

connectors	USB 1.0 1996	USB 2.0 2001	USB 2.0 Revised	USB 3.0 2011	USB 3.1 2014	USB 3.2 2017	USB4 2019
Data rate	1.5 Mbit/s (<i>Low Speed</i>)	480 Mbit/s (<i>High Speed</i>)		5 Gbit/s (<i>SuperSp eed</i>)	10 Gbit/s (<i>SuperSp eed+</i>)	20 Gbit/s (<i>SuperSp eed+</i>)	40 Gbit/s (<i>SuperSp eed+</i>)

Physical layer

Pin	Color	Signal name		Description
		A	B	
Shell	N/A	Shield		Metal housing
1	Red	VBUS		Power
2	White	D-		USB 2.0 differential pair
3	Green	D+		
4	Black	GND		Ground for power return
5	Blue	StdA_SSRX-	StdB_SSTX-	SuperSpeed receiver differential pair
6	Yellow	StdA_SSRX+	StdB_SSTX+	
7	N/A	GND_DRAIN		Ground for signal return
8	Purple	StdA_SSTX-	StdB_SSTX-	SuperSpeed transmitter differential pair



Physical layer



USB 3.0 host, VGA connector, DisplayPort connector, USB 2.0 host.

Physical layer

- HDMI
- High-Definition Multi-media Interface
- uncompressed transmission (video and sound)



Physical layer

- Repeater:
 - signal correction (amplification), one input – one output
 - if different cables = transceiver
- Hub:
 - signal is multiplied (multiport repeater)
 - collision detection
 - sending signal to all (no addressing)
 - has been replaced by switches (but it is „faster“ than switch)

Physical layer - homework

- 3 slides presentation about one of the technologies here:

1-Wire

ARINC 818 Avionics Digital Video Bus

Bluetooth physical layer

CAN bus (controller area network) physical layer

DSL

EIA RS-232, EIA-422, EIA-423, RS-449, RS-485

Etherloop

Ethernet physical layer Including 10BASE-T, 10BASE2,

10BASE5, 100BASE-TX, 100BASE-FX, 100BASE-T,

1000BASE-T, 1000BASE-SX and other varieties

G.hn/G.9960 physical layer

GSM Um air interface physical layer

IEEE 802.15.4 physical layers

IEEE 1394 interface

IRDA physical layer

ISDN

ITU Recommendations: see ITU-T

I²C, I²S

LoRa

Low-voltage differential signaling

Mobile Industry Processor Interface physical layer

Modulated ultrasound

Optical Transport Network (OTN)

SMB

SONET/SDH

SPI

T1 and other T-carrier links, and E1 and other E-carrier links

Telephone network modems — V.92

TransferJet physical layer

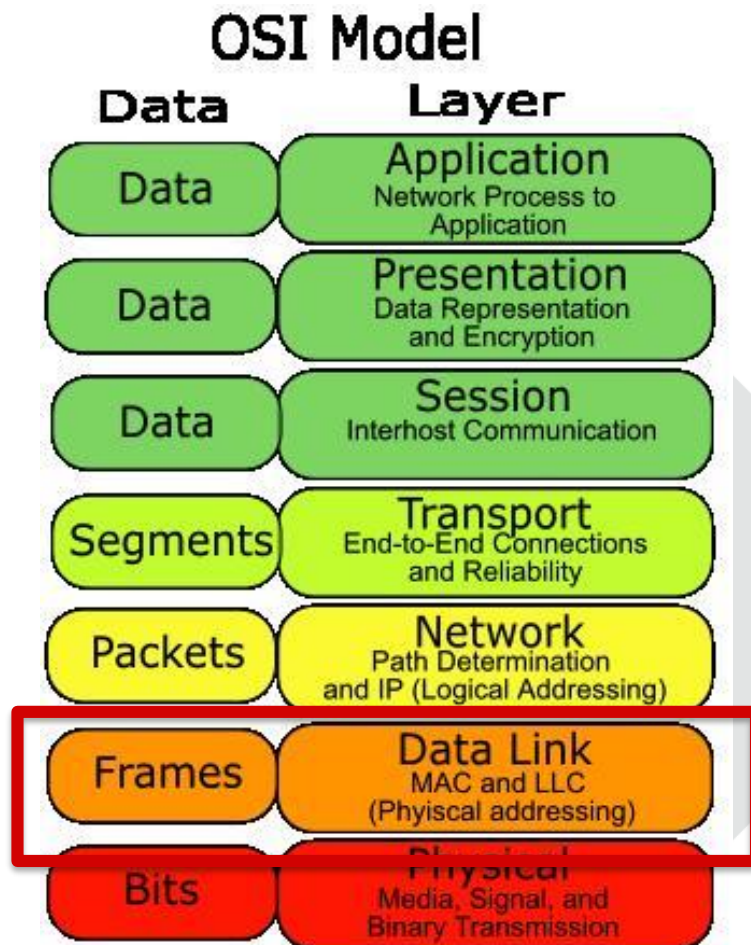
USB physical layer

Varieties of 802.11 Wi-Fi physical layers

Visible light communication co-ordinated under IEEE 802.15.7

X10

Network Layer



Data-link layer

- Differences:
 - **Data link layer** -> larger data-blocks transfer -> frames
 - **Physical layer** -> bit transfer

 - **Data link layer** -> bits interpretation (distinguish what is info part – header – and what is the data itself payload)
 - **Physical layer** -> does not recognize bits (just sending them)

Data-link layer

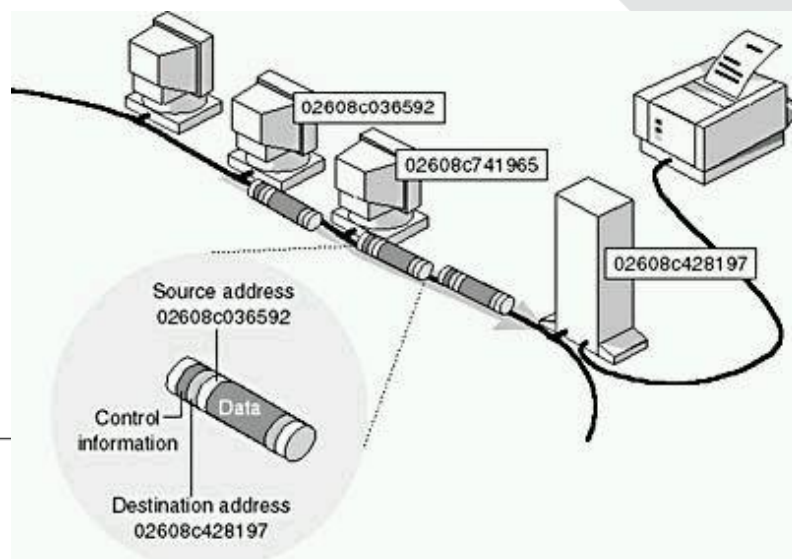
- Main task:
 - packet preparation for transport
 - access control to medium
- Creates data frames and receives data from network layer
- Creates connection/interface between programme processes and physical devices (IN/OUT)
- When data goes through different types of network (LAN vs. WAN) -> data frame is modified and adjusted to a specific network (no change of content)

Data-link layer

- Access control to a medium using several methods
- Source node (network device connected with transport medium) -> Network interface controller (NIC) -> using router to pass in between networks (e.g. LAN to WAN)
- Router unpacks a data frame (gets network address) -> makes routing decision -> pack a data into different data frame -> sends it to WAN

Data-link layer

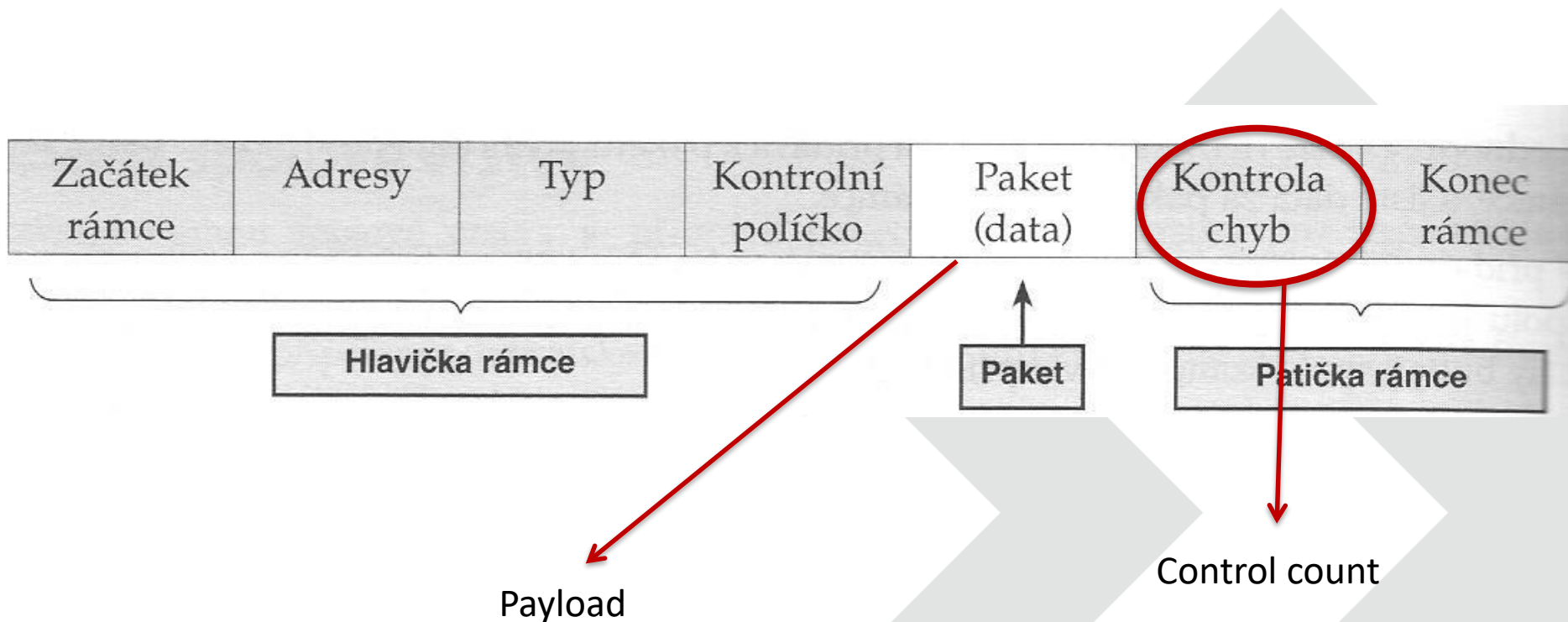
- Data-link layer adds a header and footer to a data:
 - Info about devices
 - Timing information
 - Transmission errors
 - Which nodes will be communicating next time



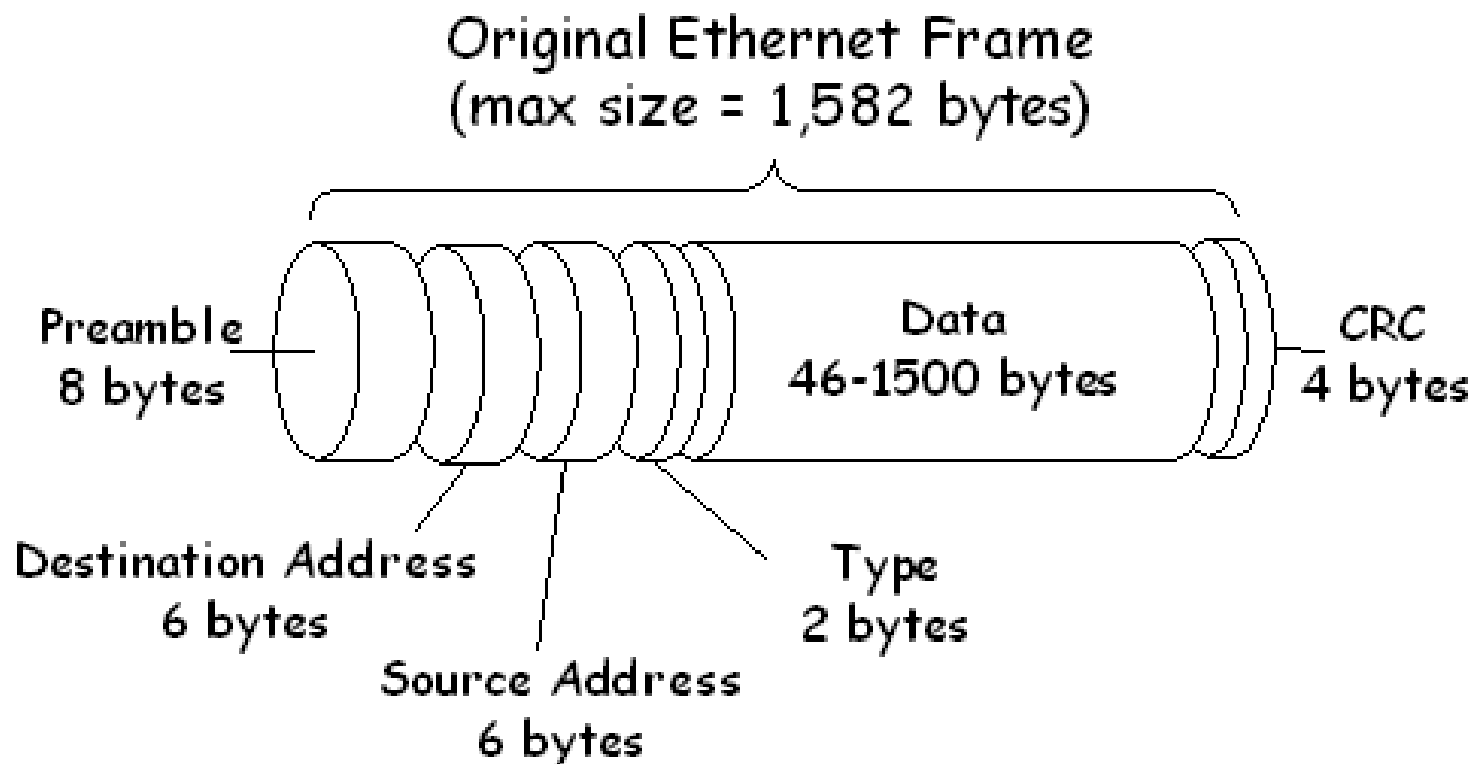
Data-link layer – data frame

- Data are sent in 1/0 (bits)
- Destination device recognizes Start and End delimiter (special sample of 1/0)
- Data frame structure is changing with a network type
- Typical fields (excluding a data/payload):
 - Start and End
 - addresses (MAC)
 - data type in a frame
 - control field

Data-link layer – data frame



Data-link layer – data frame



Data frame – header

- Start flag
- Physical address (MAC) of destination device
 - Set by a manufacturer (1st three) + unique address
- MAC is important within one LAN
- If data frame is transmitted out -> router -> reads IP and generates MAC of the opposite device
- After receiving a data frame, node reads MAC addresses and decides, if A) receives a data frame or B) discard a data frame

Data frame – header

- If A), data frame is unpacked, modified (using protocols) and passed to higher level layer (network layer)
- If a data frame is not addressed to a receiving node, it could be passed via broadcast to others
- This is typical for LANs -> MAC is in the form of FF:FF:FF:FF:FF:FF
- Header also contains info about a data type

Data frame – footer

- Info about a data frame status:
 - if a data frame arrived with no change or errors
- Control field = FCS (Frame Check Sequence)
- Source node makes a logical count on sending data = CRC (Cyclic Redundancy Check), which is stored in FCS
- When data arrives, CRC is executed and is compared with FCS
- If a count does not match -> a frame is discarded

Data-link layer – Protocols

- Most typical – Ethernet, PPP (Point-to-Point), ATM (Asynchronous Transfer Mode), HDLC etc.
- Every protocol is for specific network (e.g. Ethernet and IEEE 802 LAN; PPP and HDLC for WAN)
- Umbrella organizations ISO, IEEE, ANSI, ITU-T
- Protocols working on sw as well as on hw (network devices)
- More protocols = more methods of medium access control

Access control to shared medium

- Deterministic method
 - Every nodes has set an access time (on network)
 - Access is controlled and ruled = during transmission, no other node can transmit -> transmission link (network) might not be used effectively
 - e.g. Token Ring

Access control to shared medium

- Non-deterministic method (stochastic method)
 - nodes are „competing/fighting“ of transmission to shared medium (I have something to send, so I try)
 - In order not to overload a link -> CSMA (Carrier sense multiple access)
 - node is listening whether there is transmission -> waits or sends
 - but transmission collision/conflict in the same moment => collision and discard all data frames

CSMA/CD and CSMA/CA

- CSMA addition of CD (Collision Detection) and CA (Collision Avoidance)
- CSMA/CD:
 - Ethernet, collision detection; device is waiting, then sends a data frame. If collision, then resends
- CSMA/CA:
 - WLAN, tries to avoid collision; node listens and if OK, sends an information that the node is about to transmit => avoids collision
 - But there could be a collision of information message

Access control to non-shared medium

- There is no need to avoid collision (example PPP)
- Protocol decides to send a data in modes:
 - simplex
 - half-duplex
 - full-duplex (PC-PC, PC-switch, switch-switch)
- In case of full-duplex and UTP cable (100 Mbps Ethernet) one is receiving, second is transmitting (both in the same moment)
- Before transmission – „agreement“ of what mode will be used

Ethernet

- Technology/protocol used on LANs
- Many types according to speed (10 Mbps - 10 Gbps)
- Ethernet data frame is similar in all cases (differences are in the data placement system)
Standard 802.2 and 802.3, method CSMA/CD -> frame has to contain source and destination address (MAC)
- On TCP/IP networks - protocol Ethernet II

Ethernet

- Using IEEE 802.3 there are 4 Ethernet variants:
 - 10 Mbps – Ethernet 10Base-T
 - 100 Mbps – fast Ethernet
 - 1 Gbps – gigabite Ethernet
 - 10 Gbps – 10 gigabite Ethernet
- Values stands for maximal theoretical bandwidth
- Transfer medium – optical or metallic fibres/cabels
- Many connectors for data transmission

Wireless transmission

- Radio and microwave frequency
- Used in open space (air transmission)
- Could be used by third-parties => security and encryption
- Advantages & Disadvantages
- Not so fast (max. hundreds of Mbps)
- 4 basic types:
 - 802.11 (WLAN)
 - 802.15 (WPAN)
 - 802.16 (WiMAX)
 - GSM (using GPRS protocol)

Wireless transmission

- 802.11 (WLAN)
 - Wi-Fi, local networks, CSMA/CA
 - sends a frame -> waits for confirmation -> if does not come, sends a frame again
 - supports authenticity (verification of communicating sides), association with access-point and transmission security/encryption
- 802.15 (WPAN)
 - Wireless PAN, typically Bluetooth
 - Transmission range from 1 to 100 meters

Wireless transmission

802.11 network PHY standards [hide]								
802.11 protocol	Release date ^[8]	Fre- quency	Band- width	Stream data rate ^[7]	Allowable MIMO streams	Modulation	Approximate range ^[citation needed]	
		(GHz)	(MHz)	(Mbit/s)			Indoor	Outdoor
802.11-1997	Jun 1997	2.4	22	1, 2	N/A	DSSS, FHSS	20 m (66 ft)	100 m (330 ft)
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM	35 m (115 ft)	120 m (390 ft)
		3.7 ^[A]						5,000 m (16,000 ft) ^[A]
b	Sep 1999	2.4	22	1, 2, 5.5, 11	N/A	DSSS	35 m (115 ft)	140 m (460 ft)
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM	38 m (125 ft)	140 m (460 ft)
n	Oct 2009	2.4/5	20	Up to 288.8 ^[B]	4	MIMO-OFDM	70 m (230 ft)	250 m (820 ft) ^[8]
			40	Up to 600 ^[B]				
ac	Dec 2013	5	20	Up to 346.8 ^[B]	8		35 m (115 ft) ^[9]	
			40	Up to 800 ^[B]				
			80	Up to 1733.2 ^[B]				
		160	Up to 3466.8 ^[B]					
		0.054-0.79 ^[C]	6-8	Up to 568.9 ^[10]	4			
ad	Dec 2012	60	2,160	Up to 6,757 ^[11] (6.7 Gbit/s)	N/A	OFDM, single carrier, low-power single carrier	3.3 m (11 ft) ^[12]	
ah	Dec 2016	0.9	1-16	Up to 347 ^[13]	4	MIMO-OFDM		
aj	Est. Jul 2017	45/60						
ax	Est. Dec 2018	2.4/5		Up to 10.53 Gbit/s		MIMO-OFDM		
ay	Est. Nov 2019	60	8000	Up to 20,000 (20 Gbit/s) ^[14]	4	OFDM, single carrier,	10 m (33 ft)	100 m (328 ft)
az	Est. Mar 2021	60						

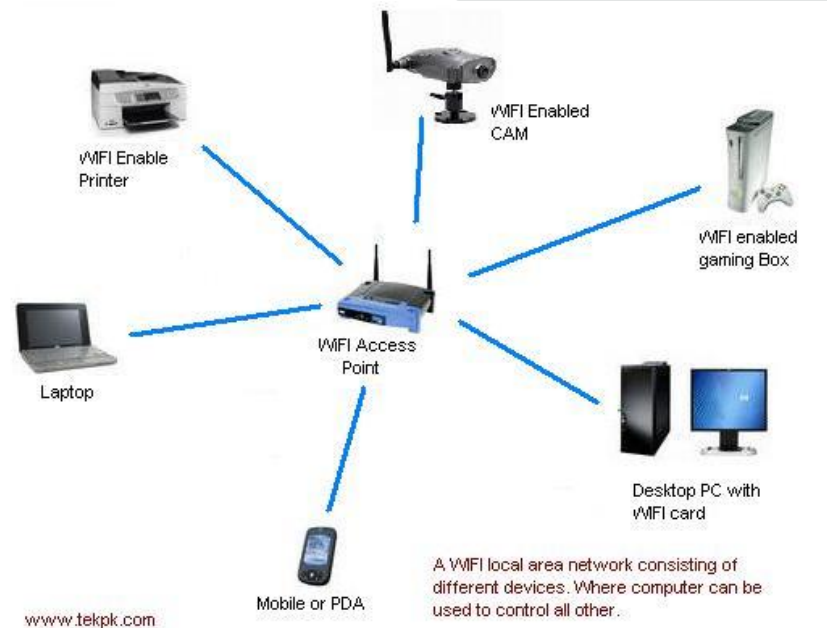
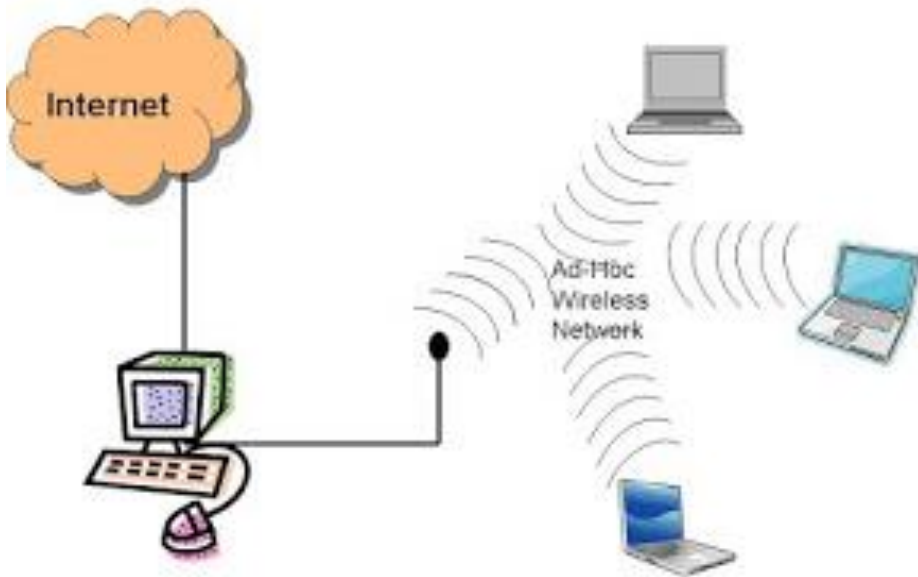
Transmission range from 1 to 100 meters

Wireless transmission

- 802.16 (WiMAX)
 - Worldwide Interoperability for Microwave Access
 - Broadband wireless internet access
 - Outdoor networks, supplement to Wi-Fi (which is more or less indoor)
 - Range up to 50 km
- GSM (Global System for Mobile Communication)
 - Digital transmission (voice call, SMS, MMS, ...)
 - protocol GPRS
 - Range up to hundreds km (depending on antennas type and height, terrain, etc.)

Wireless transmission

- Structure:
 - ad hoc networks (peer to peer)
 - access point (client-server type networks)



Wireless transmission – security issues

- Protection from „eavesdropping “ or unauthorized use
- For user – there’s no need to be connected via wire-based devices (switch, HUB, router, ...)
- It is sufficient to be in WiFi range
- Protection possibilities:
 - MAC addresses filtering (list of permitted MACs)
 - transmission encryption

Wireless networks - encryption

- WEP (Wired Equivalent Privacy)
 - from 1999, authenticity of workstations and transmission encryption, algorithm RC4 and security key of 40 or 104 bits + 24 bit initiation vector
 - vulnerability of RC4 => is not safe anymore
- WPA (WiFi Protected Access)
 - substitution of WEP, in 2002, RC4 again but + 128 bit key and 48 bit initiation vector
 - fundamental improvement via dynamic key (TKIP)
 - hard to break through

Wireless networks - encryption

- WPA 2 (WiFi Protected Access 2)
 - in 2004
 - protocol CCMP (used for 802.11i)
 - AES encryption (Advanced Encryption Standard)
 - high security
 - needs higher computer performance => older devices could not work with WPA2