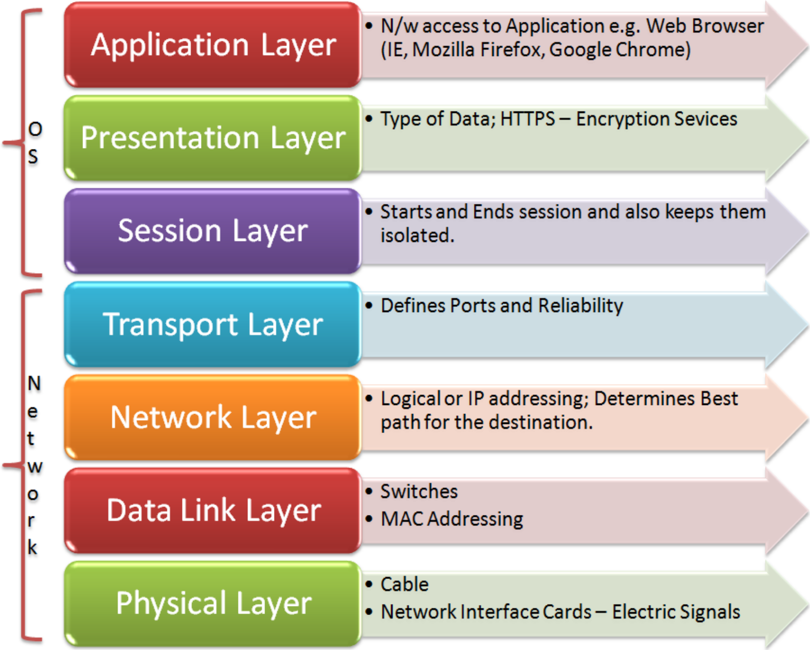
# Link layer, medium access control

Ing. Yelena Trofimova

Department of Computer Systems
Faculty of Information Technology
Czech Technical University in Prague

Computer networks, BIE-PSI
SS 2020/21, Lecture 2

https://courses.fit.cvut.cz/BIE-PSI/



OS

Application Layer

- N/w access to Application e.g. Web Browser (IE, Mozilla Firefox, Google Chrome)

Presentation Layer

- Type of Data; HTTPS – Encryption Sevices

Session Layer

- Starts and Ends session and also keeps them isolated.

Network

Transport Layer

- Defines Ports and Reliability

Network Layer

- Logical or IP addressing; Determines Best path for the destination.

Data Link Layer

- Switches
- MAC Addressing

Physical Layer

- Cable
- Network Interface Cards – Electric Signals

# Contents

- Link layer
  - types of services
  - errors detection and correction
- MAC and LLC sublayers
  - medium access control
  - logical link control
- Implementation
  - wired: Ethernet
  - wireless: Wi-Fi, Bluetooth

# Reliability of services

Reliability: reaction of layer to lost/corrupted block of data.

Types of services:

- unacknowledged connectionless service
- acknowledged connectionless service
- acknowledged connection-oriented service

# Link layer protocols

Link layer protocols ensure communication between neighboring devices:

- framing
- link access

Other possible services:

- insurance of reliable transfer
  - guaranteed frame delivery
  - elimination of frame duplication
  - correct frame ordering
- flow and error control
- addressing in the scope of network segment
  - end-stations have assigned address
  - mapping of the network address to the link layer address

# Error Detection and Correction

Type of data encoding depends on the medium at the physical layer.

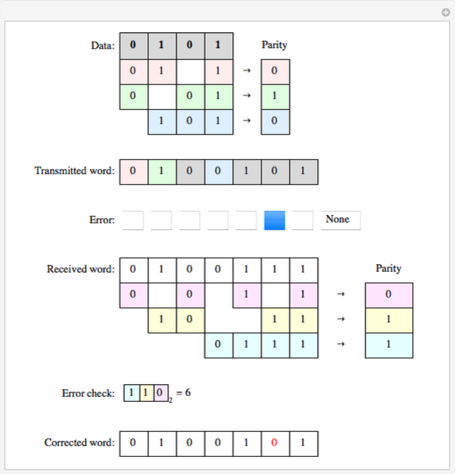
- Bit error rate (BER) - number of bit errors per unit time
  - could vary significantly: cca $10^{-3} - 10^{-12}$
  - exceptional and accidental errors in optical link
  - frequent errors in wireless link
- The basic principle is the redundancy of transmitted information $\Rightarrow$ channel capacity is reduced.

# Error Detection

- Parity bit (even or odd): added for the total number of 1-bits to be even or odd
- Checksum: sum of all bytes (words) values in the message
- CRC (Cyclic Redundancy Check)
  - key G(x)
  - the CRC is the remainder after division of the message M(x) by the key G(x)

# Error Correcting Codes

- All of these codes add redundancy to the information that is sent.
- Examples:
  - Hamming code (7,4) encodes 4 bites into 7 bites, which allows to correct one error and detect two
  - Binary Convolution Code and Reed – Solomon Code are used in satellite communication



| Data: | 0 | 1 | 0 | 1 | | Parity |
|---|---|---|---|---|---|---|
| | 0 | 1 | | 1 | → | 0 |
| | 0 | | 0 | 1 | → | 1 |
| | | 1 | 0 | 1 | → | 0 |

| Transmitted word: | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
|---|---|---|---|---|---|---|---|

| Error: | □ | □ | □ | □ | □ | ■ | □ | None |
|---|---|---|---|---|---|---|---|---|

| Received word: | 0 | 1 | 0 | 0 | 1 | 1 | 1 | | Parity |
|---|---|---|---|---|---|---|---|---|---|
| | 0 | | 0 | | 1 | | 1 | → | 0 |
| | | 1 | 0 | | | 1 | 1 | → | 1 |
| | | | | 0 | 1 | 1 | 1 | → | 1 |

Error check: $\boxed{1}\boxed{1}\boxed{0}_2 = 6$

| Corrected word: | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
|---|---|---|---|---|---|---|---|

Source: Wolfram Demonstrations Project, Hamming (7,4)

# Data in link channel

Problem of "$bandwidth \times delay$"

- product of bandwidth and delay gives the amount of data "on the way"
- influences the selection of frame acknowledgment and resend methods

Examples:

- Ethernet (10BaseT) in local network
  - 10 Mb/s * 0.5 ms = 625 Byte
  - less than 1 frame
- long international optical link 10 Gb/s
  - 10 Gb/s * 5 ms = 6.25 MByte
  - thousands of frames in the communication channel

# Link Layer Sublayers

Link layer is too general.
2 sublayers:

- MAC (Medium Access Control) – controls the access to shared medium, defines frame address (MAC address)
- LLC (Logical Link Control) – supports the coexistence of different network layer protocols in the same link, flow control and error control

# Medium Access Control Methods

are implemented on MAC sublayer, have sense only in case of shared medium

- deterministic access
  - static allocation
  - centralized allocation management. For example: based on permission from management station to transmit
  - distributed allocation
- random access

# Random Access Methods

- ALOHA
- Slotted ALOHA
- CSMA
- CSMA/CD
- CSMA/CA

# ALOHA, slotted Aloha

- developed in the 1970s for a packet radio network by Hawaii University
- whenever a sender has data, it transmits
- transmission can be successful or not (collisions or channel errors)
- in case of error (higher layer), sender retransmits his message after some random time
- slotted Aloha – improvement: time is slotted and a packet can only be transmitted at the beginning of one slot (it can reduce the collision duration)

# CSMA

Carrier Sense Multiple Access

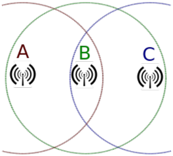
- based on the Aloha system
- collisions are not detected
- before the station starts transmission, it listens to the link, if no transmission is ongoing
- if channel is idle, station transmits
- if channel is not idle, three variants:
  - 1-persistent: wait for finish and send right away with probability 1
  - non-persistent: wait for random time
  - p-persistent: wait until the next slot and send with probability p
- problem: non-zero signal propagation time between stations

# CSMA with Collision Detection

- during the transmission station listens to the channel
  - could be implemented on the wire
- in case of collision detection (receives something different than transmits), stops transmitting
- better medium utilization in compare with CSMA – does not continue with sending of corrupted frame

# CSMA with Collision Avoidance

- CSMA/CD could not be used for radio networks
  - could not listen during transmitting
  - so called "hidden terminal" effect



- RTS/CTS algorithm
  - station sends RTS – Request To Send packet
  - central station respond with CTS – Clear To Send
    - thus other stations know about planning transmission
  - used in Wi-Fi

# Frames

Stream of bits is divided into frames

Problem is to determine the frame boundaries

- frame length is defined explicitly
  - frames are of equal length
  - at the beginning of the frame there is an information about length
- gap at the end of the frame
- byte stuffing: start and stop flags
- bit stuffing: analogous to byte stuffing for protocols that do framing on bit level

# PPP

Point to Point Protocol
RFC 1661, 1662

- most commonly used for WAN connection
- byte oriented protocol
- supports different authentication protocols (EAP, PAP, CHAP)
- is used over serial cable, phone line, cellular telephone, fiber optics, ethernet
- 0x7E is a flag (frame delimiter)
  - 0x7E ⇒ 0x7D 0x5E
  - 0x7D ⇒ 0x7D 0x5D

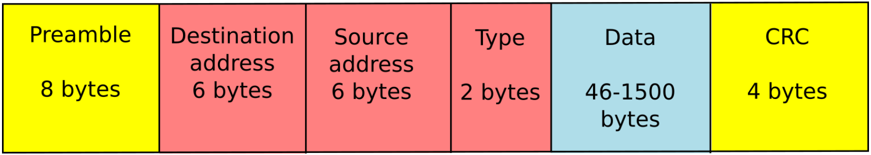
# Ethernet

- 2 standards:
  - Ethernet II (DIX: consortium Digital, Intel, Xerox)
  - IEEE 802.3 (ISO 8802-3), more general version by IEEE
- in Internet, Ethernet II is obligatory
- frames can be distinguished
- both standards can co-exist on the same segment

# Ethernet II

- Preamble: 1010101010....1011
- Address: 3 bytes prefix (manufacturer) + 3 bytes suffix
- XXXXXXFB
  - F: 0 – global, 1 – local
  - B: 0 – unicast, 1 – multicast
- FF:FF:FF:FF:FF:FF is broadcast

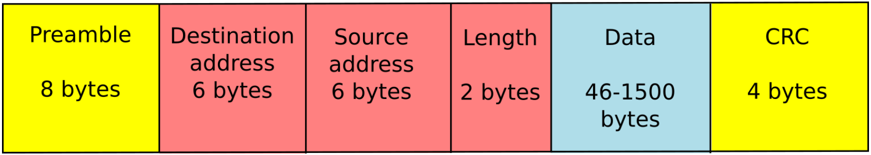
- Type = ID of network protocol
  - 0x0800 = IPv4
  - 0x0806 = ARP
  - 0x86DD = IPv6



| Preamble | Destination address | Source address | Type | Data | CRC |
|---|---|---|---|---|---|
| 8 bytes | 6 bytes | 6 bytes | 2 bytes | 46-1500 bytes | 4 bytes |

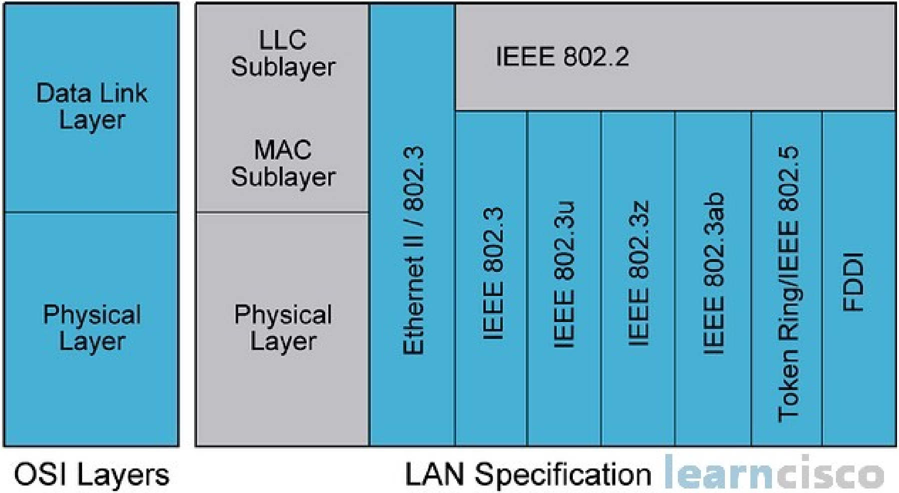
# Ethernet 802.3

- Length 0 – 1500 bytes (0–0x5DC)
- Data:
  - IEEE 802.3 Novell IPX
  - IEEE 802.2 LLC
  - IEEE 802.2 SNAP



| Preamble | Destination address | Source address | Length | Data | CRC |
|---|---|---|---|---|---|
| 8 bytes | 6 bytes | 6 bytes | 2 bytes | 46-1500 bytes | 4 bytes |

# Ethernet Standards



Data Link Layer

Physical Layer

OSI Layers

LLC Sublayer

MAC Sublayer

Physical Layer

Ethernet II / 802.3

IEEE 802.2

IEEE 802.3

IEEE 802.3u

IEEE 802.3z

IEEE 802.3ab

Token Ring/IEEE 802.5

FDDI

LAN Specification

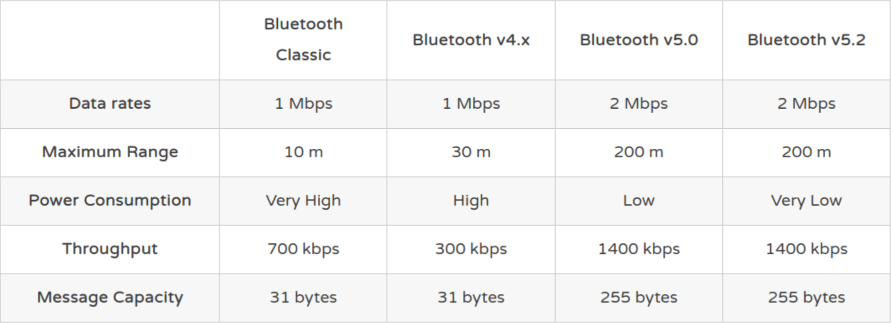
learncisco

# WiFi (802.11)

- types of nodes: clients and Access Points (AP)
- communication modes: infrastructure, ad-hoc
- support for data encryption
- authentication protocols:
    - free access (no authentication)
    - WEP
    - WPA, WPA2
- variants:
    - 802.11a (5GHz, 54 Mbps)
    - 802.11b (2.4GHz, 11 Mbps)
    - 802.11g (2.4GHz, 54 Mbps)
    - 802.11n (5GHz or 2.4GHz, 100 Mbps)
    - 802.11ac (5GHz, 500 Mbps)
    - 802.11ax (2.4GHz or 5GHz, up to 11Gbps)

# Bluetooth (802.15.1)

- PAN (Personal Area Networks)
- Topology:
  - piconet: 7 active clients, max 255 (active and non-active) clients
  - scatternet: piconets connected through the common client
  - star-bus



| | Bluetooth Classic | Bluetooth v4.x | Bluetooth v5.0 | Bluetooth v5.2 |
|---|---|---|---|---|
| Data rates | 1 Mbps | 1 Mbps | 2 Mbps | 2 Mbps |
| Maximum Range | 10 m | 30 m | 200 m | 200 m |
| Power Consumption | Very High | High | Low | Very Low |
| Throughput | 700 kbps | 300 kbps | 1400 kbps | 1400 kbps |
| Message Capacity | 31 bytes | 31 bytes | 255 bytes | 255 bytes |