Computer network architectures and protocols

theory

Imre Varga
University of Debrecen, Faculty of Informatics

04 September 2017

General information

Subject, course:

Computer network architectures and protocols
INHK721 (Computer Science Engineering BSc)
Computer networks (Architectures and protocols)
INJK711-K5 (Business Information BSc)

Wednesday 10:00-12:00, TEOKJ II/106B room (Lecture, I.V.)
Tuesday 12:00-14:00, IF03 room (Practice, INJK711L, I.V.)
Tuesday 16:00-18:00, IF03 room (Practice, INHK721L, A.K.)

subject credit: 5 (INJK711-K5), 4 (INHK721)

General information

Teachers:

Dr. Varga, Imre (Tuesday 10, Tuesday 12)
Department of Informatics Systems and Networks
email: varga.imre@inf.unideb.hu
www: irh.inf.unideb.hu/user/vargai
room: IF13

Karsai, Andrea (Tuesday 16)
Network and Telecommunication Supplier Unit
email: karsai.andrea@it.unideb.hu
room: Chemistry Building, C stairway 4/3

General information

Requirements, conditions for **practice** (INJK711L):

maximum number of absences: 3

late arrival (more than 20 minutes) means absent from class

2 midterm tests (+1 retake)

to pass a test: reach **at least 50%**

if a test failed: retake is necessary with extra conditions

retake test: covers the whole semester

result overwrites the worse test result

General information

Requirements, conditions for **lecture** (INJK711-K5):

written exam

to pass: reach **at least 50%**

signature + passed theoretical test: suggested grade

theoretical and practical results together determine the final grade (50%-50%)

Readings:

Andrew S. Tanenbaum: *Computer Networks*, Prentice-Hall, 2003.

Topics

- Concepts of network
- Layered network architecture
- Protocols and services
- Transmission mediums
- Ethernet
- IP addressing
- Routing
- Network configuration
- Applications (DNS, web, e-mail, ftp, …)
- *Many more things…*

Basics of computer networks

Computer Networks

Definition:

Two or more computers linked together with some software and hardware tools for an information transmission related purpose.

Purposes:

- Human communication.
- Sharing resources.
- Increasing reliability.
- Increasing speed.
- etc.

Computer Network Nodes

Node:

Device with own network address. It can communicate independently (e.g. computer, printer, router).

In a communication a node can act either as a transmitter (source) or as a receiver (sink).

Categories of network devices and tools:

- End user node: computer, printer, scanner, and any other devices that provide services directly to the user
- Network linking/connecting tools: devices that enable communication between end user nodes by connecting them to each other

Classification of Computer Networks

Based on their sizes:

- Personal Area Network (PAN)
- Local Area Networks (LAN)
- Metropolitan Area Networks (MAN)
- Wide Area Networks (WAN)

Based on switching technology:

- Packet switching
- Circuit switching
- Message switching

Classification of Computer Networks

Personal Area Network

- For one person
- Size: few meters
- E.g.: USB, Bluetooth

Local Area Network

- For a building
- Size: max few 100 m
- Ethernet, Wi-Fi

Metropolitan Area Network

- Covers a city
- Size: few 10 km
- Connect LANs

Wide Area Network

- Covers countries and more
- Size: more 100 km

Classification of Computer Networks

Circuit switching

- Establish a dedicated communications channel (circuit) before the nodes may communicate, they remains connected during communication

Message switching

- The whole information (message) travels from node to node (store-and-forward technique)

Packet switching

- Message is cut into smaller units (packet) which are transmitted independently

Packet switching

Advantages

- Don’t need large memory/disk in routers (cheaper)
- No continually busy lines for long time (interactive)
- While 2nd packet is arriving 1st can be sent (faster)
- Fault tolerant (re-routing, partial retransmission)
- Efficient (not occupied line, if no transmission)
- Charging/fees are based on the amount of sent information (not the time of connection)

Internet is (mostly) packet switched.

Transmission Speed

Transmission speed
(network speed, bandwidth, bit rate):

Amount of information transmitted during a time unit. Measure of unit: bit/sec, b/s, bps.

The throughput measured in applications is always lower than the physical bandwidth.

Larger units:

- 1 kbps = 1000 bps
- 1 Mbps = 1000 Kbps
- 1 Gbps = 1000 Mbps

Directions of Information Transmission

One way (simplex) connection:

The transmission of information allowed only one way is called a one way (simplex) connection (eg. radio broadcasting).

Alternate way (half duplex) connection:

The transmission allowed both directions, but only one direction at a time is called a half duplex connection (eg. CB radio).

Two way (full duplex) connection:

The traffic allowed in both directions simultaneously is called a full duplex connection (eg. telephone).

Connections of Data Transmission

Point-to-point connection:

The propagation of information performed between two points (a transmitter and a receiver) is called a peer-to-peer connection.

Multiple nodes connection, broadcasting:

A transmitter provided information to multiple receivers is called a multiple nodes connection. Broadcasting is a multiple nodes connection, where all receivers get the information inside a given range (e.g. radio broadcasting).

Basics of Addressing

Unique address (Unicast):

An identifier, assigned to a network interface of a node.

Everyone address (Broadcast):

An address, identifying all nodes (and interfaces of nodes) in a so called broadcast domain.

Not a list of unique addresses.

Computer Network Protocol

Protocol:

The formal description of all rules and conventions which determines the communication of network devices (nodes) (set of communication rules).

Syntax, semantics, timing, etc.

Examples:

HTTP, FTP, IP, DHCP, TCP, UDP, SMTP, POP3, IMAP, ARP, RARP, ICMP, RIP, EIGRP, OSPF, IPSEC, …

Server-Client Architecture

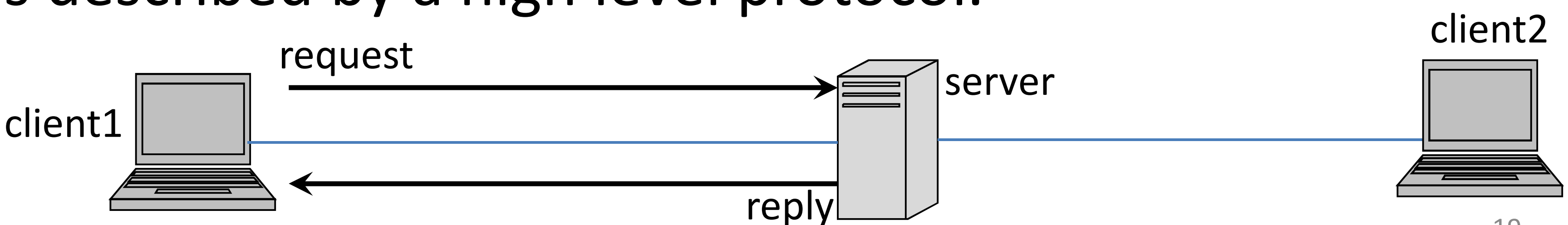
Server:

A network node (and software) which provides services for other nodes. The service of a server is ensured by a server-software (e.g. a web-server).

Client:

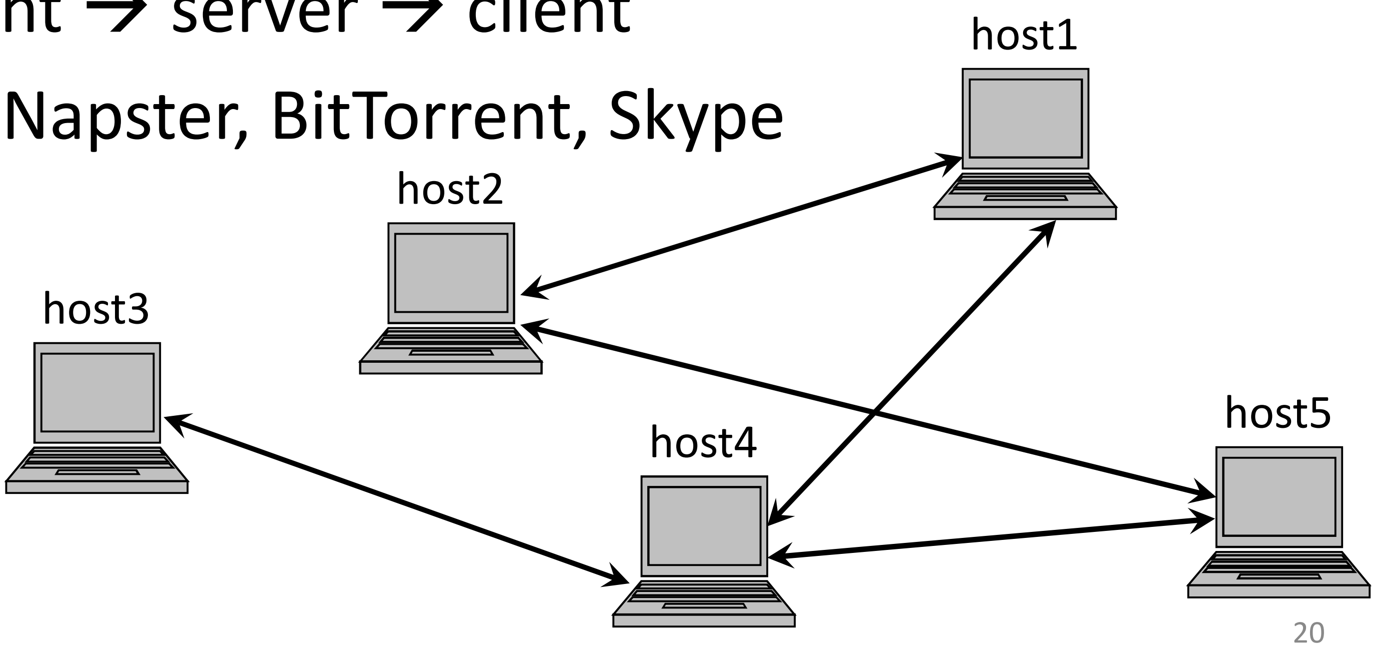
A network node (and software) which has some kind of network service demand. For recourse to the service the client uses a client-software (e.g. web browser).

The communication between the server and the client is described by a high level protocol.



Peer-to-peer architecture

- No fixed client/serves roles
  - Equivalent hosts
- Anyone in the group can communicate with anyone else directly
  - No client → server → client
- Example: Napster, BitTorrent, Skype



Transmission Media, Channel, Collision

Transmission media:

Device or material on which the transmission of information (signal) is performed. (Eg. twisted-pair cable, coaxial cable, fiber-optic cable, or air).

Transmission channel:

Data path, frequency band for transmitting signals. Usually, in a transmission media multiple channels (data path) are formed.

Collision:

A collision occurs when two (or more) nodes transmit information at the same time on a common transmission channel.

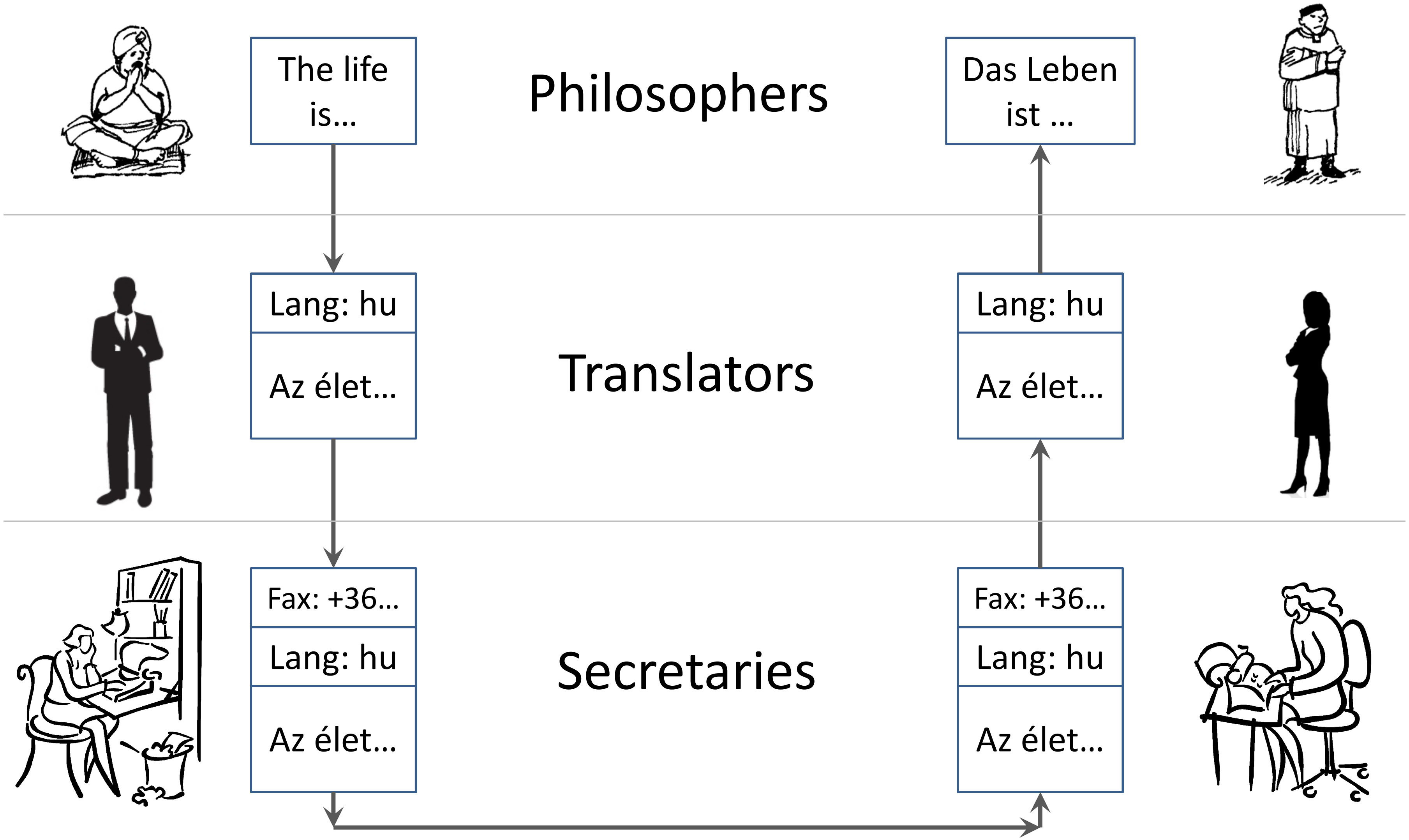
Layered Network Architecture

Layered Network Architecture

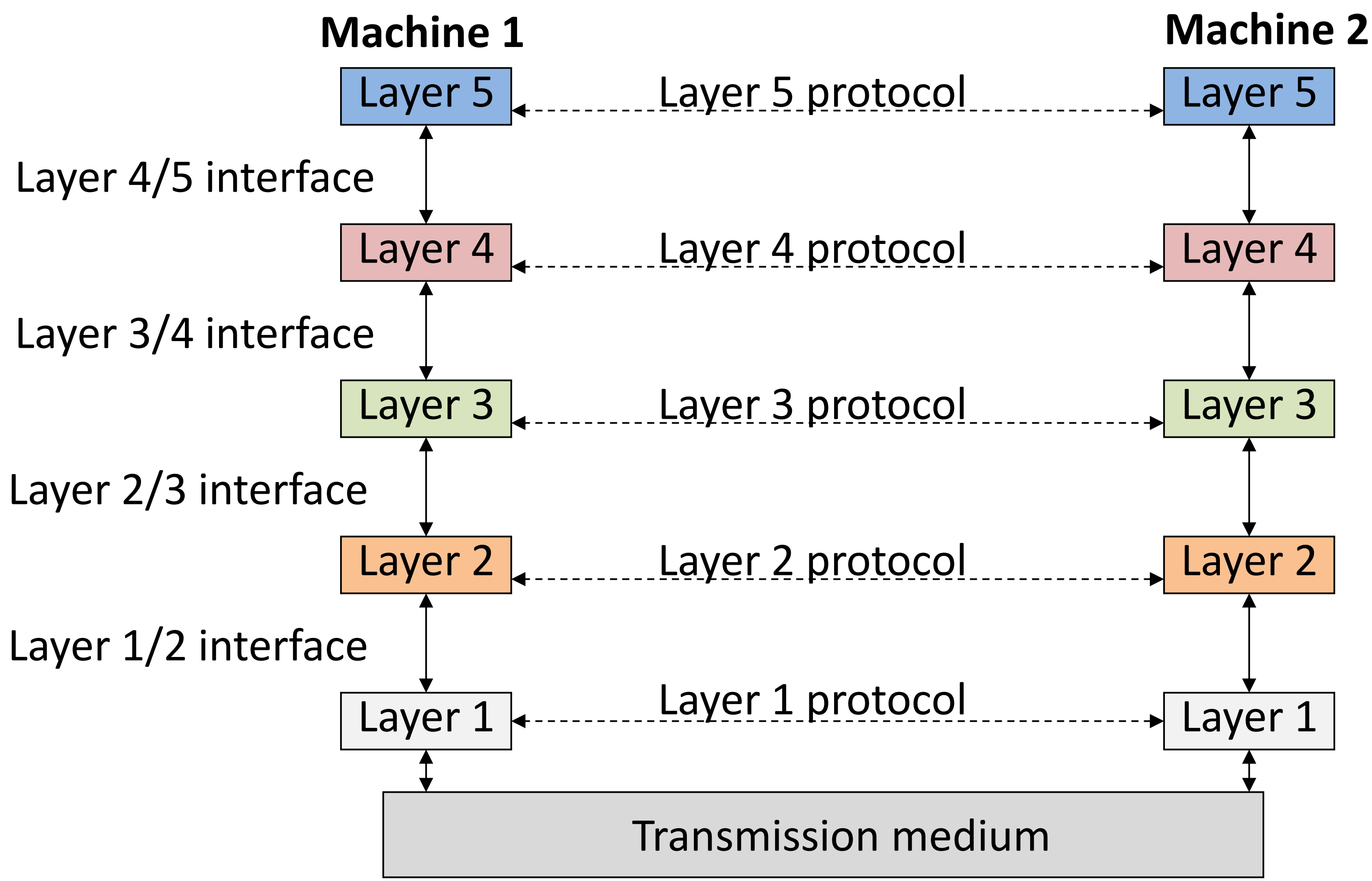
Why we use layered network architecture?

- To describe a huge protocol is complex and difficult.
- A hierarchical protocol system can be easier implemented.
- The change tracking is easier.
- Layers can cooperate also in case of different producers.

Philosopher-translator-secretary architecture



Layers (Levels), Protocols, Interfaces



Concepts of Layered Architecture

Layer N protocol:

A protocol which describes the specifications of layer N.

Peers:

Entities which located on the same level of the two communication endpoints (nodes). In some logical way the peers communicate each other by the help of the corresponding layer protocol.

Layer N/N+1 interface:

Connection of boundary surface of layers N and N+1.

Service of Layer N:

Set of actions (service) which are provided to layer N+1 by layer N (through the interface).

Encapsulation

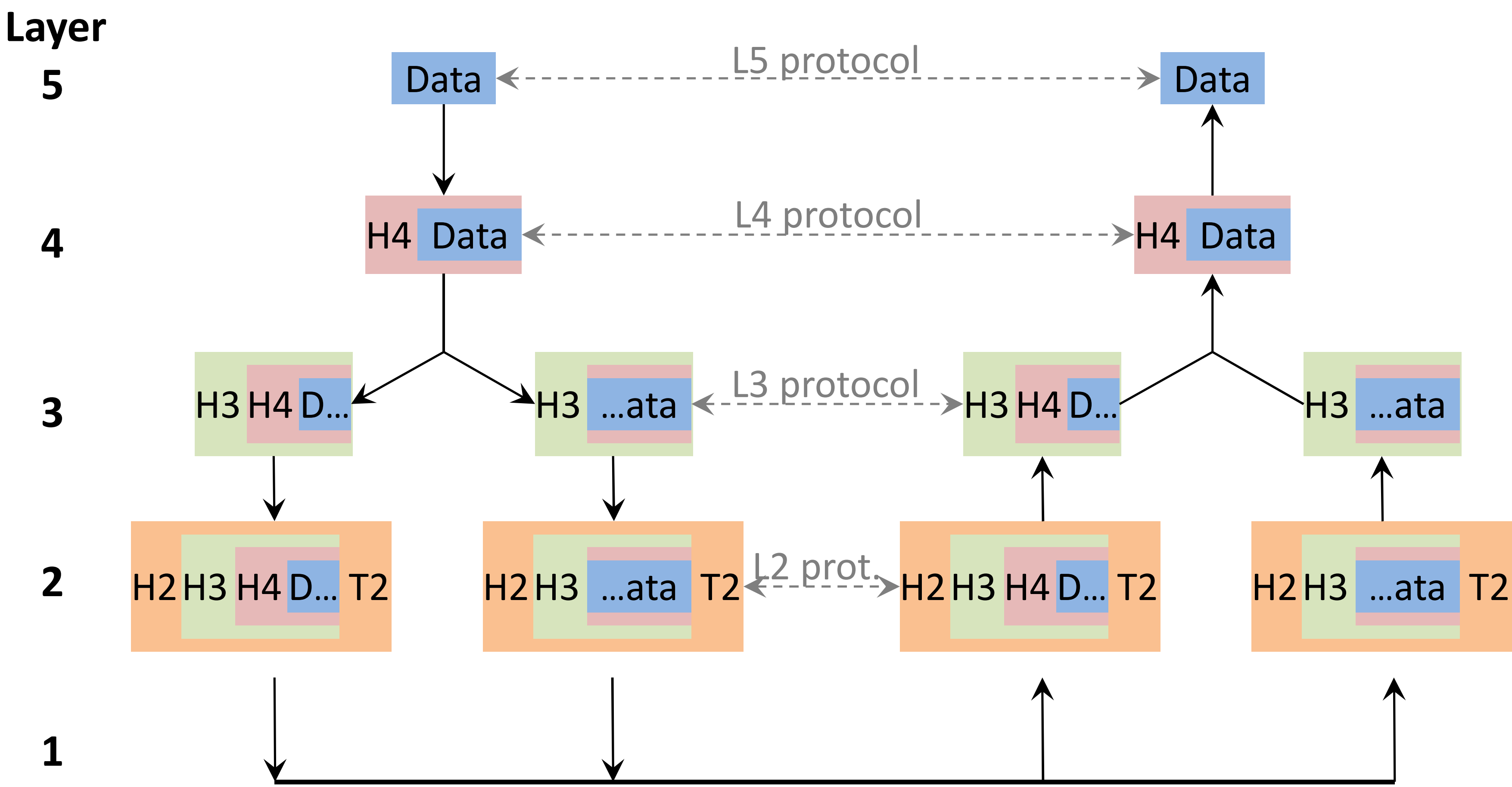
Encapsulation:

Packaging the information arrived from a higher level with a header of a specific protocol (it is similar when a traditional mail letter is put in an envelope and the envelope is addressed).

Protocol Data Unit (PDU):

Entity (contains header and data) handled by the considered protocol. (It is frequently mentioned as packet.)

Scheme of Network Communication



OSI Reference Model

Layer		Name of PDU
7	Application Layer	APDU
6	Presentation Layer	PPDU
5	Session Layer	SPDU
4	Transport Layer	TPDU, Segment
3	Network Layer	Packet
2	Data Link Layer	Frame
1	Physical Layer	Bit

Layers of OSI model

Physical Layer (L1):

Specification and properties of different transmission mediums in order to implement signal transmission.

- Cables, connectors, modulation, signal coding, etc.

Data Link Layer (L2):

Reliable transmission between two directly connected devices. Two sublayers: LLC, MAC.

- Physical addressing, media access, logical topology, acknowledging, etc.

Layers of OSI model

Network Layer (L3):

Connection between any two network nodes (not just dirrectly connected).

- Routing, traffic control, network addressing, etc.

Transport Layer (L4):

Reliable connection between softwares on two nodes. Protocols may connectionless or connection-oriented.

- Data stream, error detection/correction, order guarantee, etc.

Layers of OSI model

Session Layer (L5):

Relationship-treating between applications during the dialog, establishing sessions between hosts.

Presentation Layer (L6):

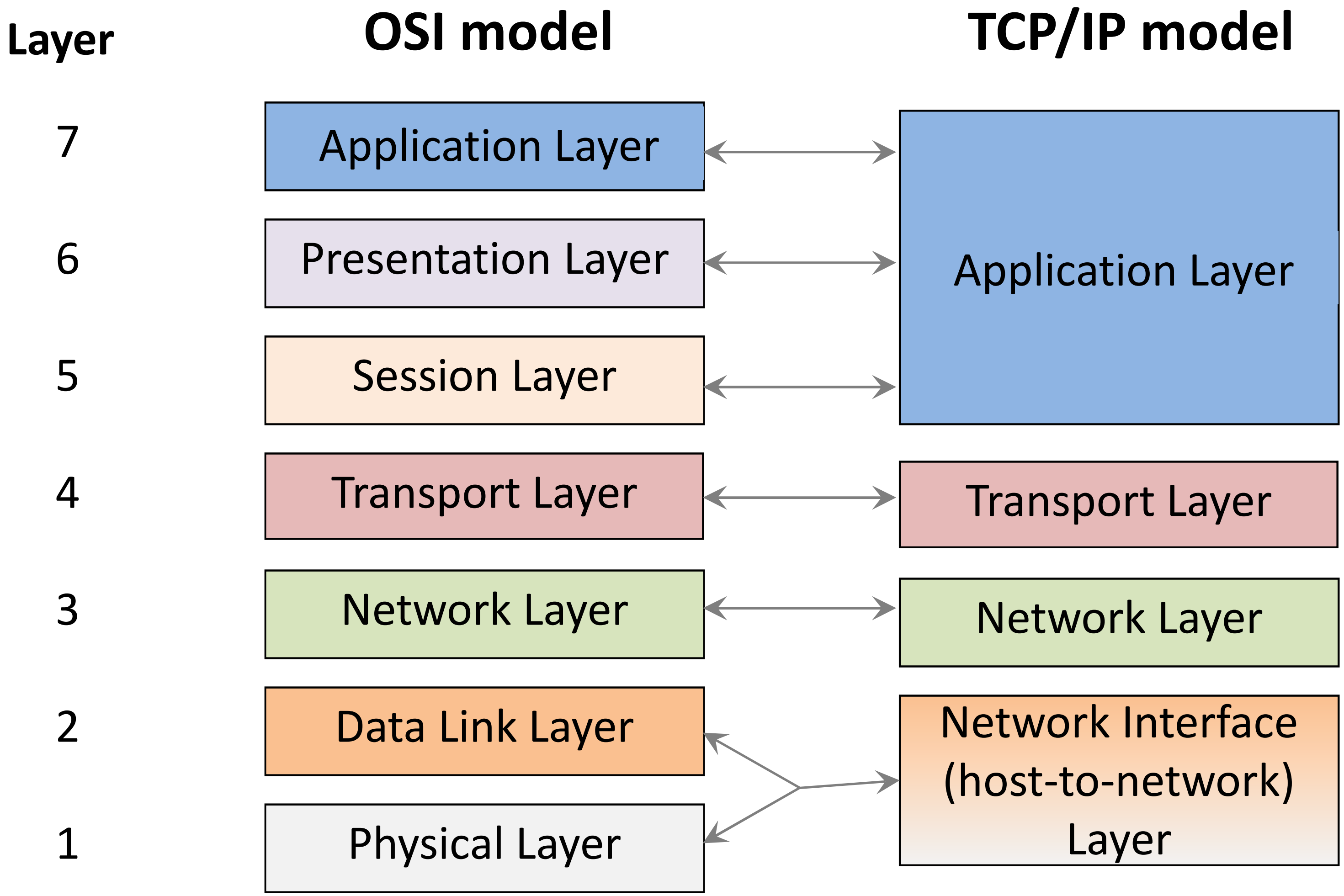
Provides same interpretation of information (different nodes can use different data structures, data representation). Encryption, compression, etc.

Application Layer (L7):

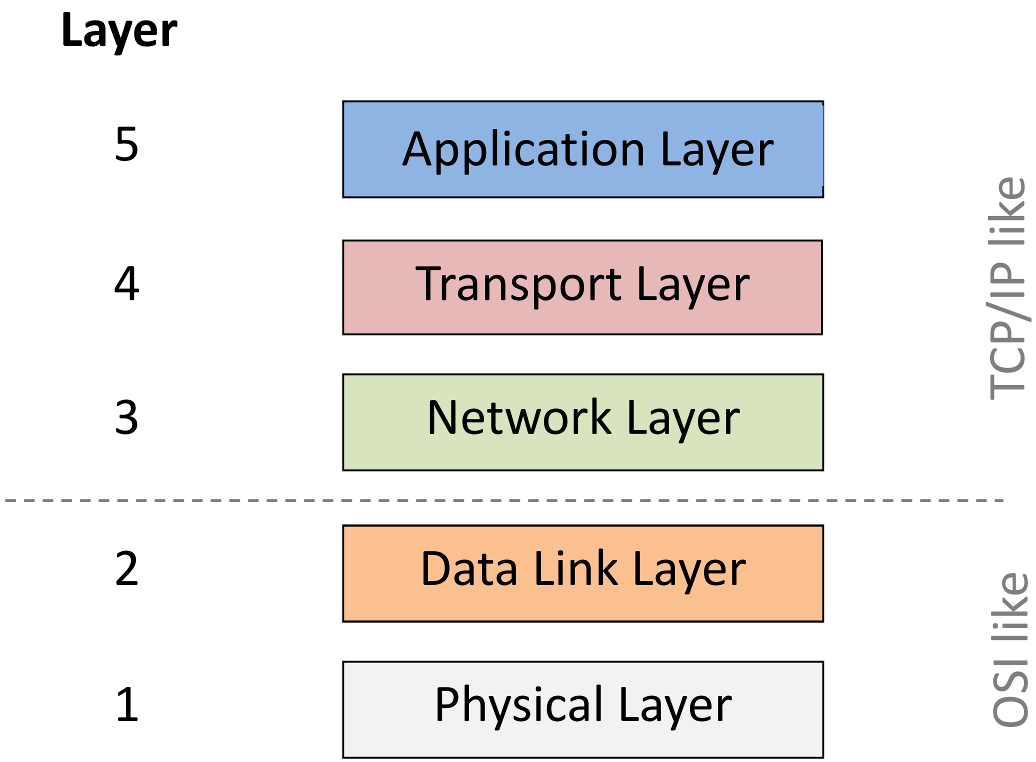
Interface between applications and users.

- DNS, web, e-mail, ftp, bittorrent, etc.

Mapping of TCP/IP - OSI Model



Hybrid Reference Model



Network interconnection

Network Interconnection - Basics

Collision domain; Bandwidth domain:

Part of a network, where collisions can be detected (a common communication channel that is shared by multiple nodes).

In a collision domain only one information transmission can be performed at a time.

Broadcast domain:

Part of a network, where information transmitted with a broadcast address can be detected.

Interconnected networks

Problems with interconnected networks

- Too large distances between nodes
- Too large collision domain: low efficiency, frequent collisions
- Too large broadcast domain: congestion, too much packets
- Connected networks can have different
  - cabling
  - signals
  - speed
  - packet size
  - address space
  - protocols

Network Interconnection Devices

Repeater:

Amplifies and repeats the signals sent on transmission media.

Does not separate the connected subnetworks.

Repeaters with multiple ports is called a HUB.

Bridge:

Working in Data Link Layer it performs selective connection („Only those packets goes through the bridge, who tends to other side”).

The interconnected subnets form separate collision domains.

Usually transmits the broadcasting towards all interconnected subnets.

Network Interconnection Devices

Switch:

A multiple port device with bridge functionality between any two ports.

Router:

Working in Network Layer it performs selective connection, routing, and traffic control.

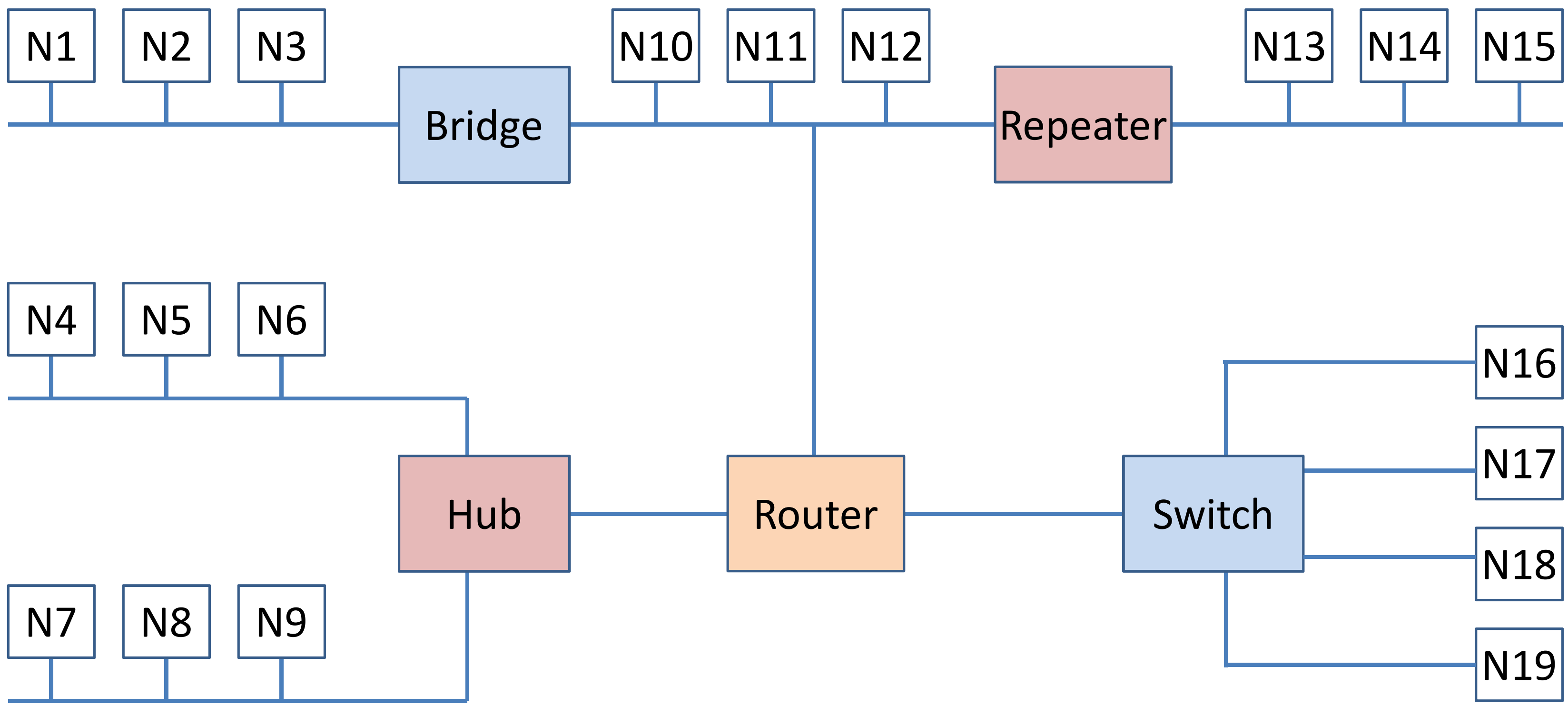
The interconnected subnets form separate collision domains and separate broadcast domains.

It is a node with own IP address.

It is also called a gateway in Network Layer (default gateway).

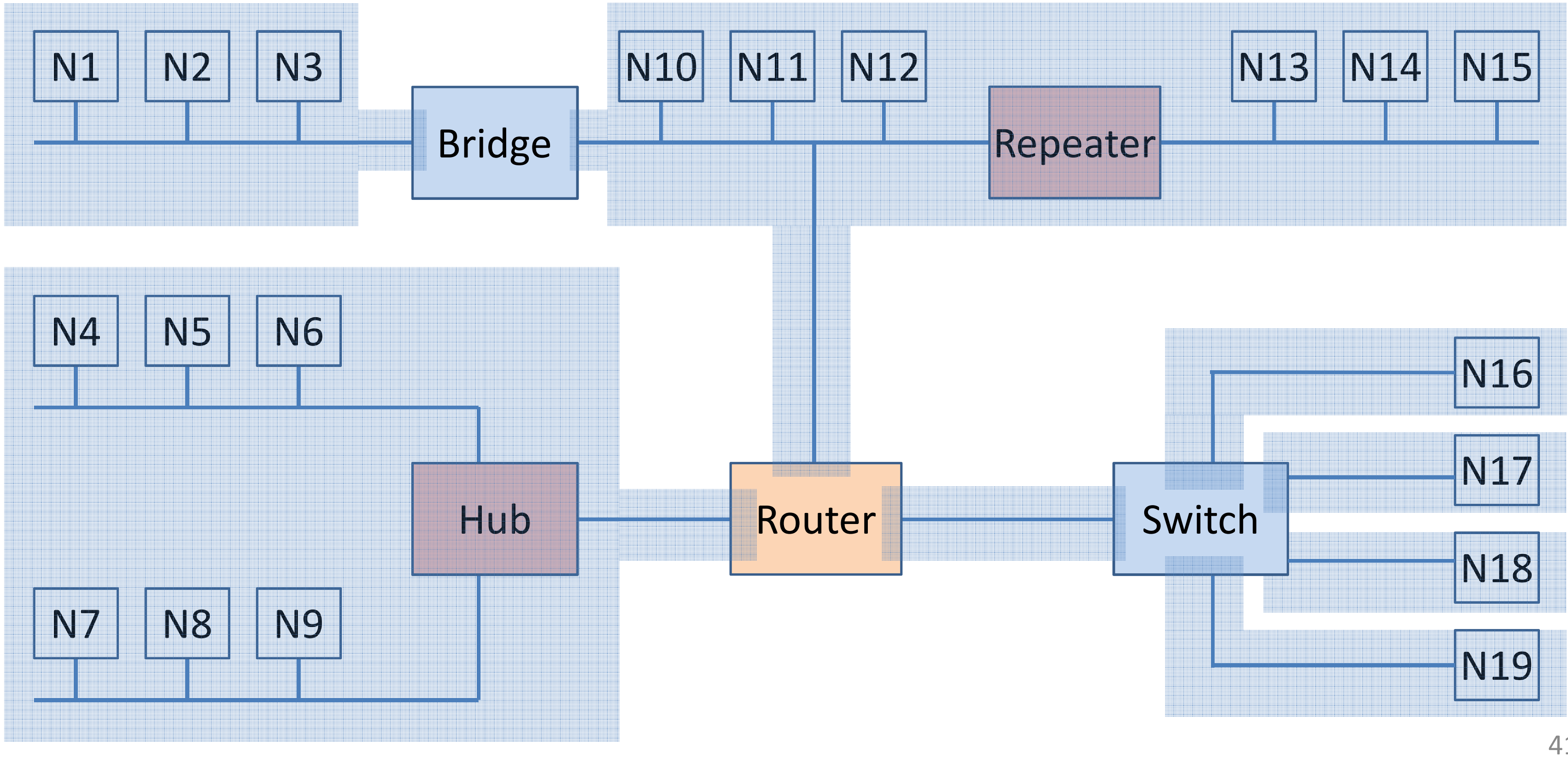
Network Interconnection Devices

- Which node-pairs don't disturb each other?
- Who is available form where by broadcast?



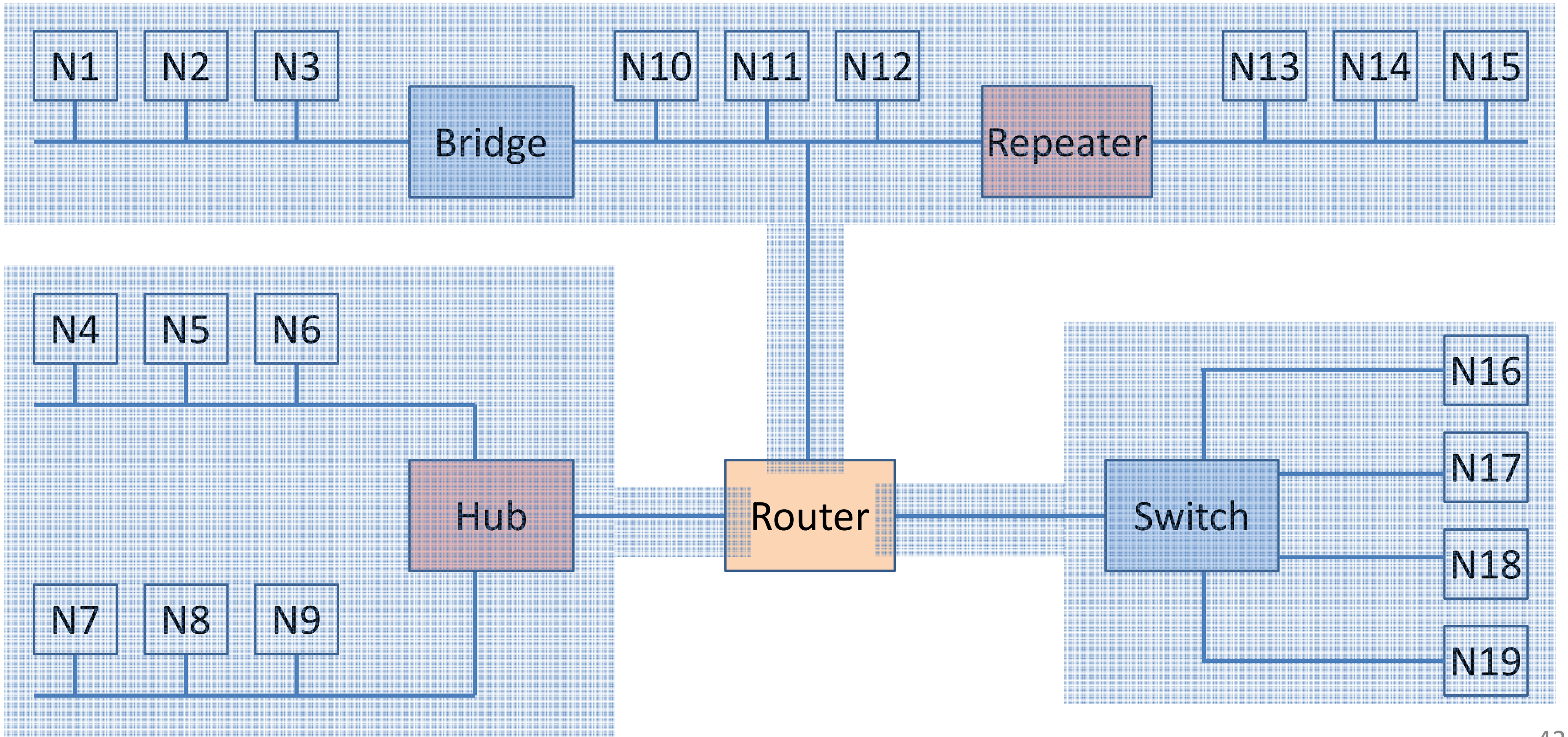
Network Interconnection Devices

- Which node-pairs don't disturb each other?
- Collision domains:



Network Interconnection Devices

- Who is available form where by broadcast?
- Broadcast domains:

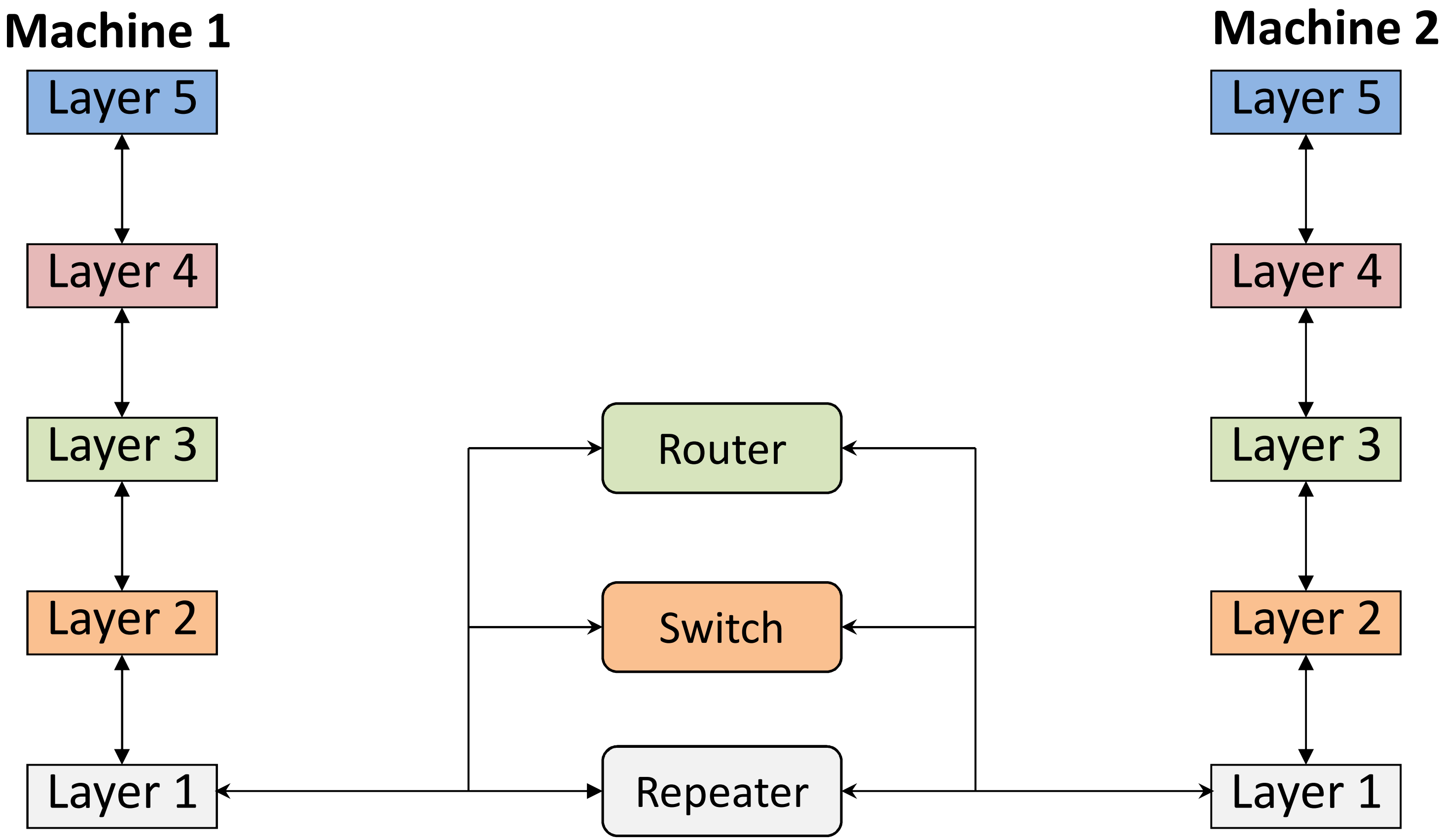


Network Interconnection Devices

Subnetworks – based on the functionality of network interconnection devices – can be connected in different OSI Layers.

OSI layer	**Connector item**
Transport Layer and above	gateway
Network Layer	router
Data Link Layer	bridge, switch
Physical Layer	repeater, hub

Repeater, switch, router



Physical layer

Physical layer

First layer of hybrid model (L1)

Specification and properties of different transmission mediums in order to implement signal transmission.

Topics

- Cables and connectors
- Topology
- Modulation and signal coding,
- etc.

Theoretical basis of communication

Fourier analysis

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_n \sin(2\pi nft) + \sum_{n=1}^{\infty} \mathrm{b_n}\cos(2\pi nft)$$

Frequency band limits the bitrate

- Larger signal frequency range
- Larger bandwidth
- More detailed signal
- More coded information
- Faster transmission speed
- (More noise in the channel decrease the bitrate)

Attenuation

The amplitude of a signal is decreasing during its way in a transmission media.

The length of a transmission media is determined such a way that the signal should be interpreted securely by the receiver.

If large distance has to be covered, the signal has to be restored by the help of amplifiers (repeaters).

The attenuation depends on frequency (bandwidth important), thus the amplifiers have to compensate this with frequency dependent amplification.

Physical transmission and cables

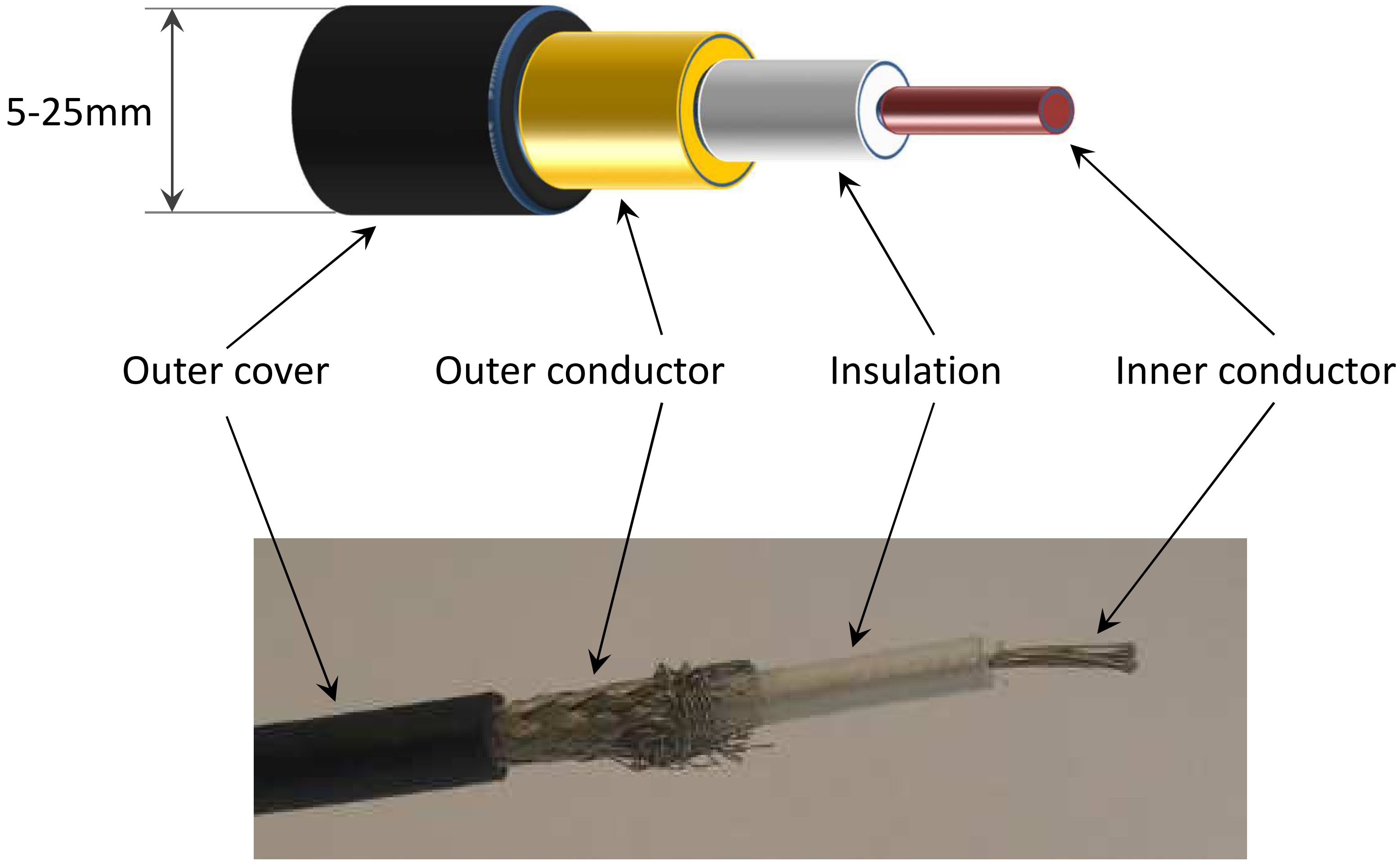
Wired

- Coaxial cable (electric signal)
  - Thin, thick
- Twisted pair (electric signal)
  - UTP, FTP, STP
- Optical fibre (light)
  - Multimode, single mode

Wireless

- Air (electromagnetic waves)
  - Radio wave, microwave, infrared

Coaxial cable



Coaxial cable

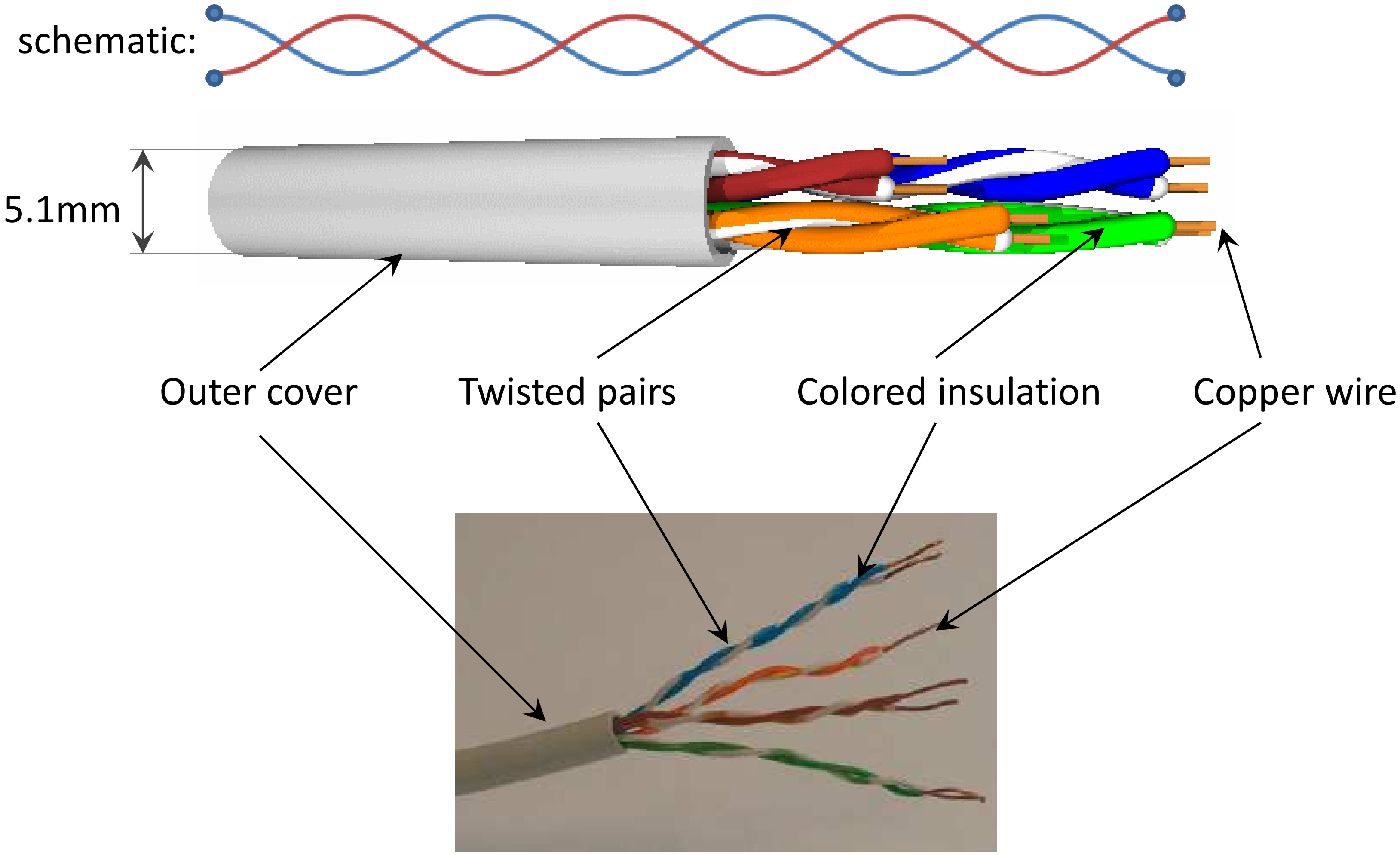
Transmission characteristics:

- Due to the concentric structure of conductors, it is not sensitive for interference and crosstalk
- In case of digital transmission amplifiers are required in every km
- In case of analog transmission, amplifiers are required in every several km

Applications:

- Transmission of television broadcasting
- Large distant telephone transmission
- Connection of computers

Unshielded Twisted Pair



Unshielded Twisted Pair

Characteristics:

- It is the cheapest media
- Data transmission speed (100Mbps) and the distance (100m) to be covered are highly limited
- Two isolated copper conductors are twisted and four such pairs are grouped without shield (UTP)
- Foiled Twisted Pair (FTP): pairs has a common shield cover
- Shielded Twisted Pair (STP): pairs are shielded separately

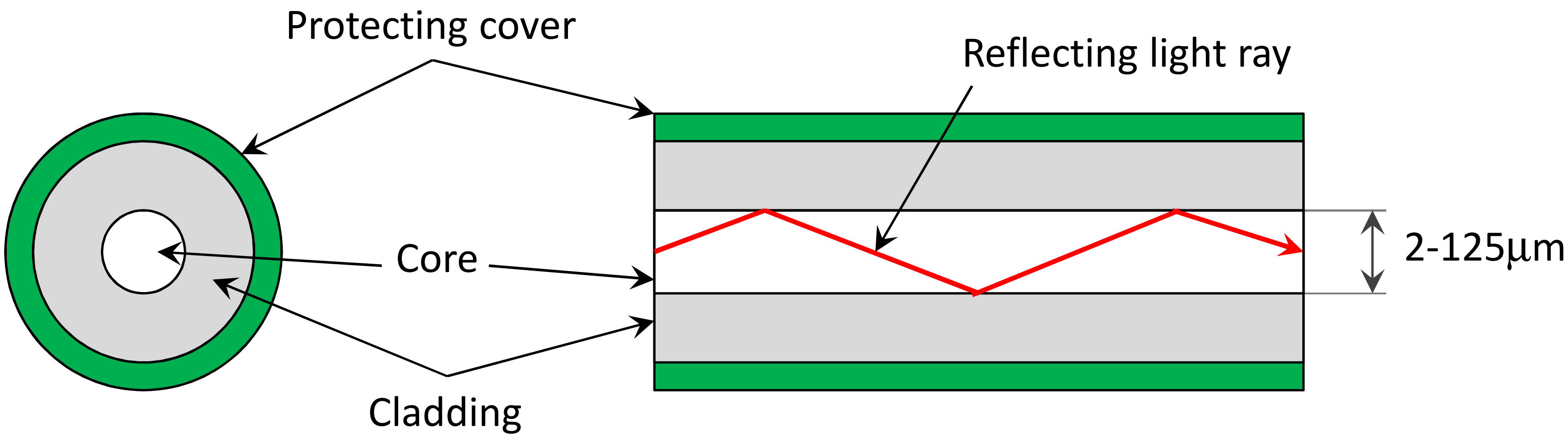
Common twisted-pair cables

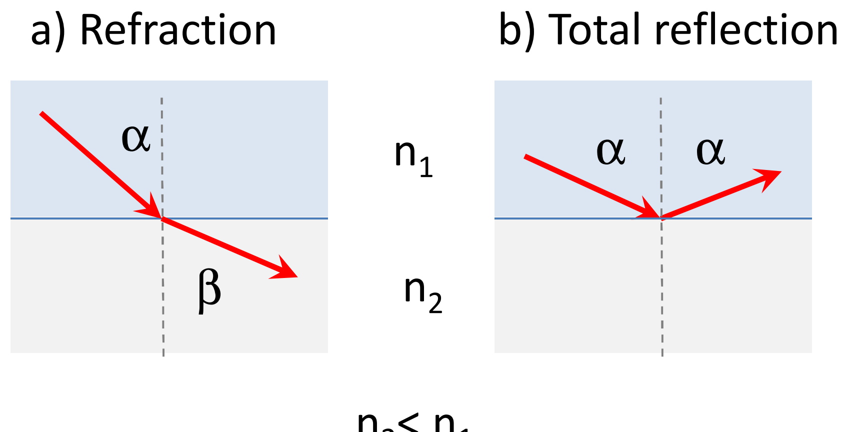
Name	Typical construction	Bandwidth	Application
CAT. 1	UTP	0.4 MHz	phone
CAT. 3	UTP	16 MHz	10Base-T
CAT. 5	UTP	100 MHz	100Base-T
CAT. 5e	UTP	100 MHz	1GBase-T
CAT. 6	UTP	250 MHz	10GBase-T
CAT. 7	FTP / STP	600 MHz	10GBase-T

Terminated in 8P8C (RJ45) connector

Maximum length: 100 m (90+4+6 or 90+10)

Optical fiber



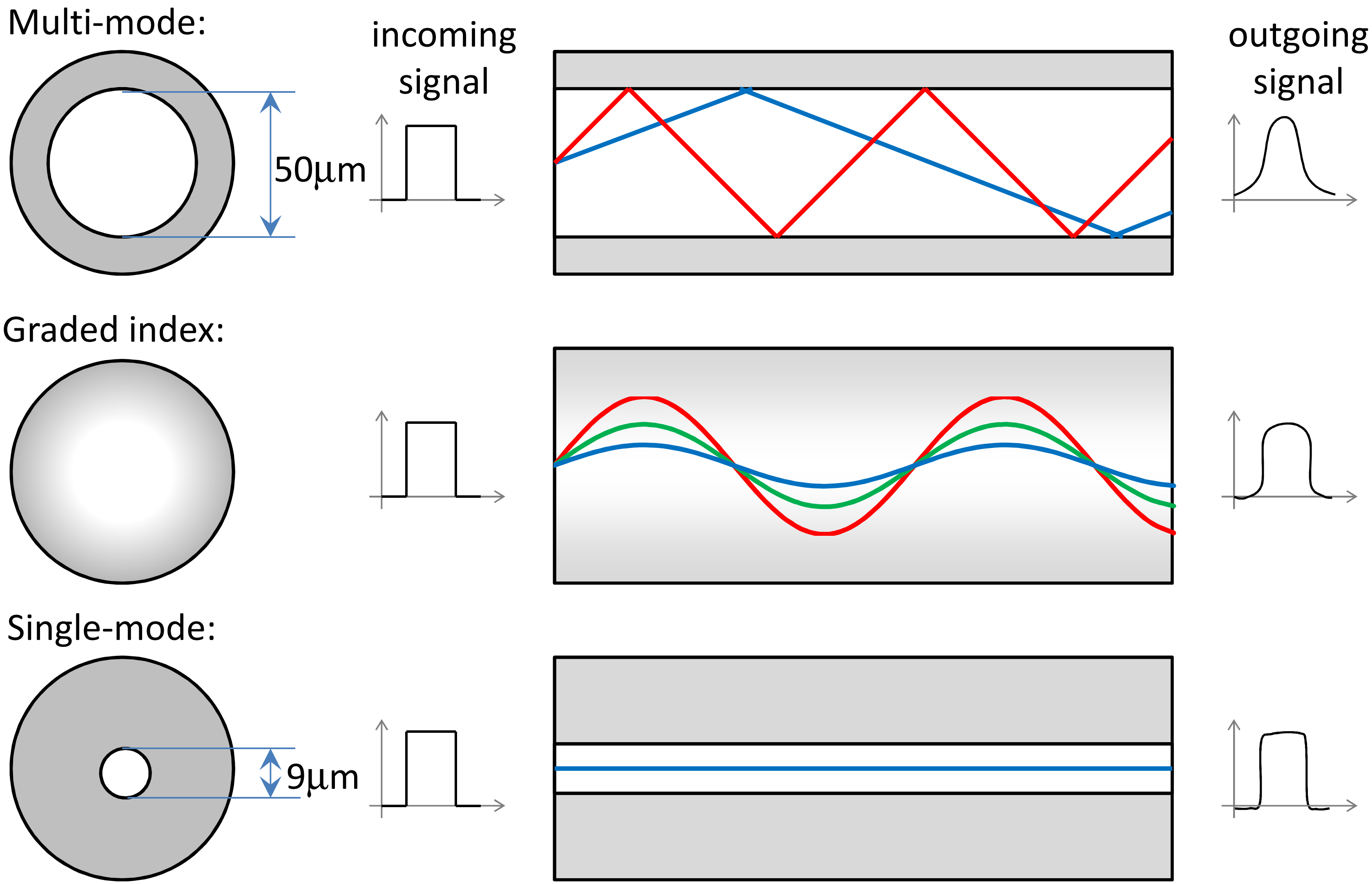


Optical fiber

Characteristics:

- Core and cladding: glass or plastic with different reflective index
- Works in 10^{14} - 10^{15} Hz (infrared) domain
- 3 versions are used: multi mode, single mode, multi mode graded index
- Light sources: LED, laser diode
- Connectors: ST, SC, FC, MT-RJ, LC, MU, MDI, …

Types of optical fibers



Optical fiber

Advantages:

- **Larger capacity**: High transmission speed can be achieved (2 Gbps in 10x km).
- **Smaller size and weight**
- **Smaller attenuation**: The attenuation is smaller, and it is constant at a wide frequency range.
- **Electromagnetic isolation**: Not sensitive for outer electromagnetic effects, there is no crosstalk.
- **Larger repeating distance**: Smaller the number of repeaters is, smaller the possibilities of errors and the costs are.

Signal, Signal Coding, Modulation

Signal: Physical quantities, depending on place and time, and carrying information. Information carrier on the communication channel, it could be analog or digital.

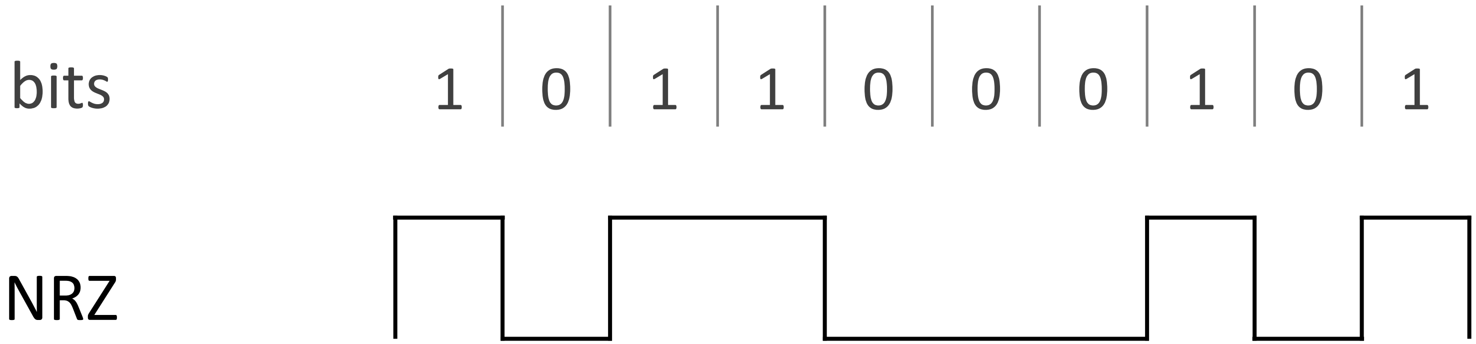
Signal Coding: Mapping the (digital) information onto the digital carrier signal (e.g. voltage levels, changing of voltage levels). It is also called line coding.

Modulation: Mapping onto analog carrier signal. The process of creating the (modulated) signal to be transmitted through the channel from the modulating signal coming from the source and the analog carrier signal. Inverse process is the demodulation. A **modem** performs modulation and demodulation, as well.

NRZ signal coding

Non Return to Zero

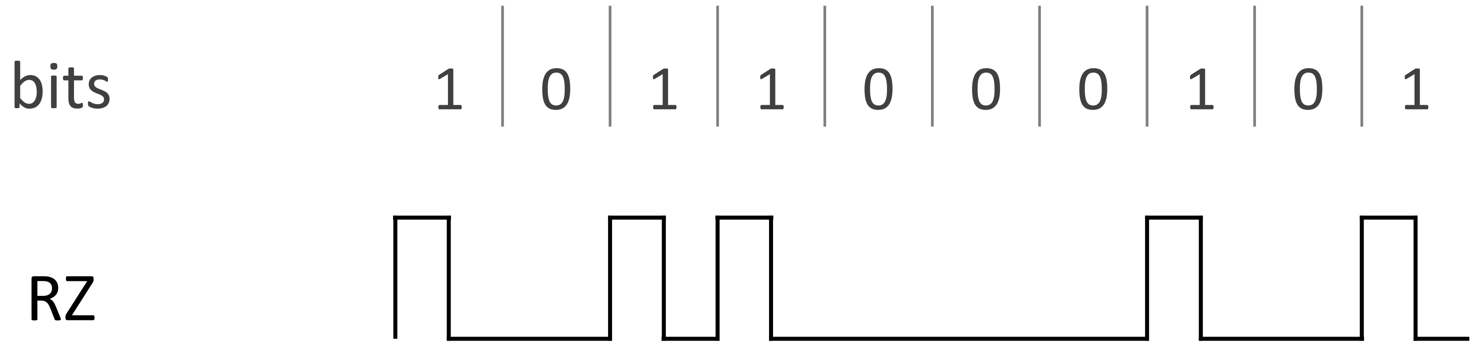
- ‚0’ bit represented by one signal level (-1)
- ‚1’ bit represented by an other signal level (+1)
- Easy implementation
- No synchronization in case of (several) same bits



RZ signal coding

Return to Zero

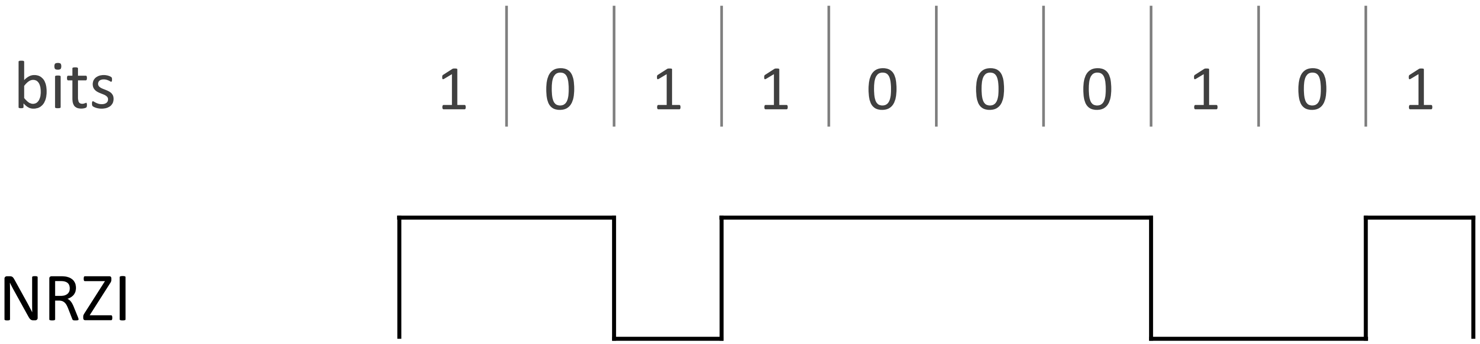
- ‚0’ bit represented by one signal level (-1)
- ‚1’ bit represented by half bit-time (+1) and half bit-time (+1)
- Double frequency needed
- No synchronization in case of several ‚0’ bits



NRZI signal coding

Non Return to Zero Inverted

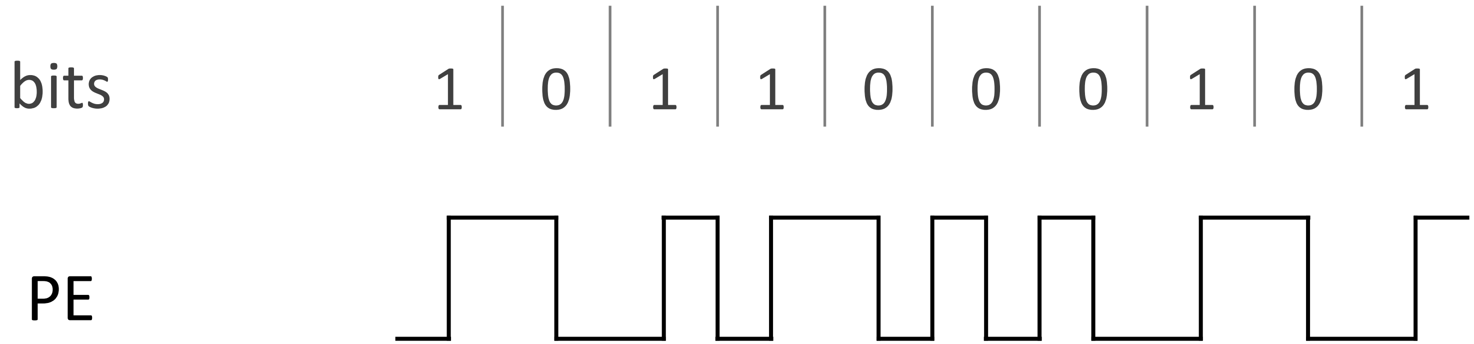
- ‚0’ bit represented by keeping the previous signal level
- ‚1’ bit represented by changing the previous signal level
- No synchronization in case of several ‚0’ bits



Manchester signal coding

Also called Phase Encoding (PE)

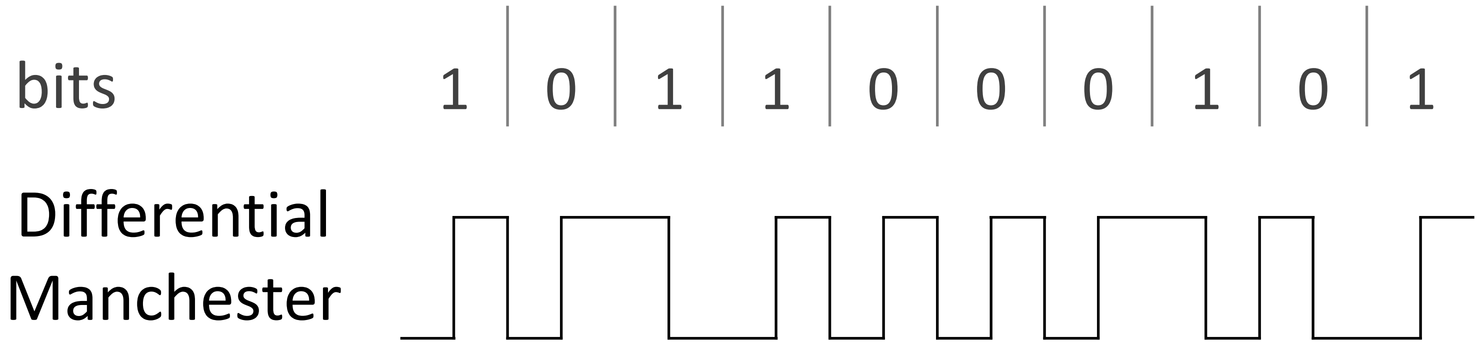
- ‚0’ bit represented by high-low level change at the middle of bit-time
- ‚1’ bit represented by low-high signal sequence
- Double frequency needed
- Synchronized



DM signal coding

Differential Manchester

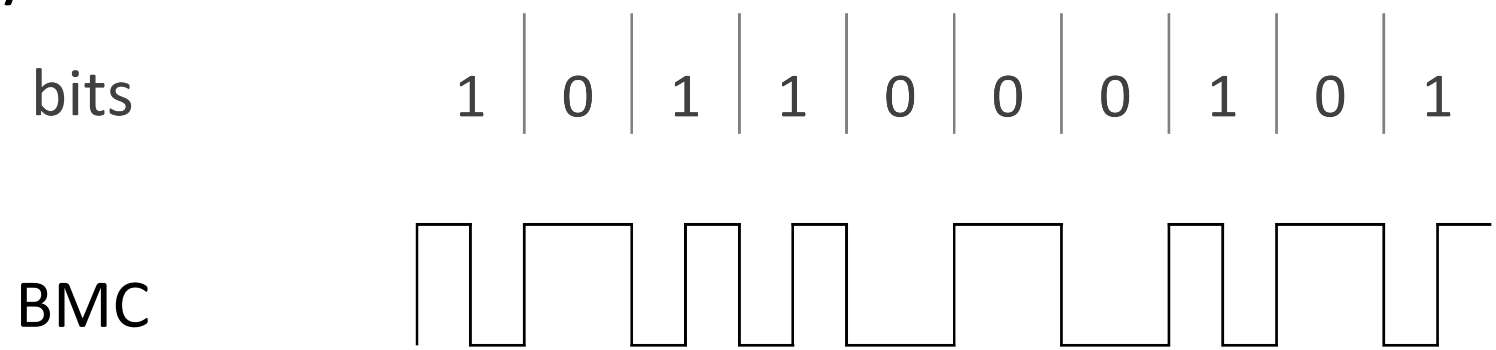
- ‚0’ bit represented by the same level change at the middle of bit-time as previously
- ‚1’ bit represented by opposite level change at the middle of bit-time as previously
- Double frequency needed, synchronized



BMC signal coding

Biphase Mark Coding

- ‚0’ bit represented by changing level for full bit-time
- ‚1’ bit represented by changing level for half bit-time, then changing level again for half bit-time
- Double frequency needed
- Synchronized



4B5B coding

4bit-5bit coding

- Maps group of 4 bits onto group of 5 bits
- Uses a conversion table
- Max 3 „0” bits are next to each other
- There are special and unused 5-bit groups
- Further coded by e.g. NRZI

bits	0000 0110 1100 0001
4B5B	11110 01110 11010 01001

Modulation

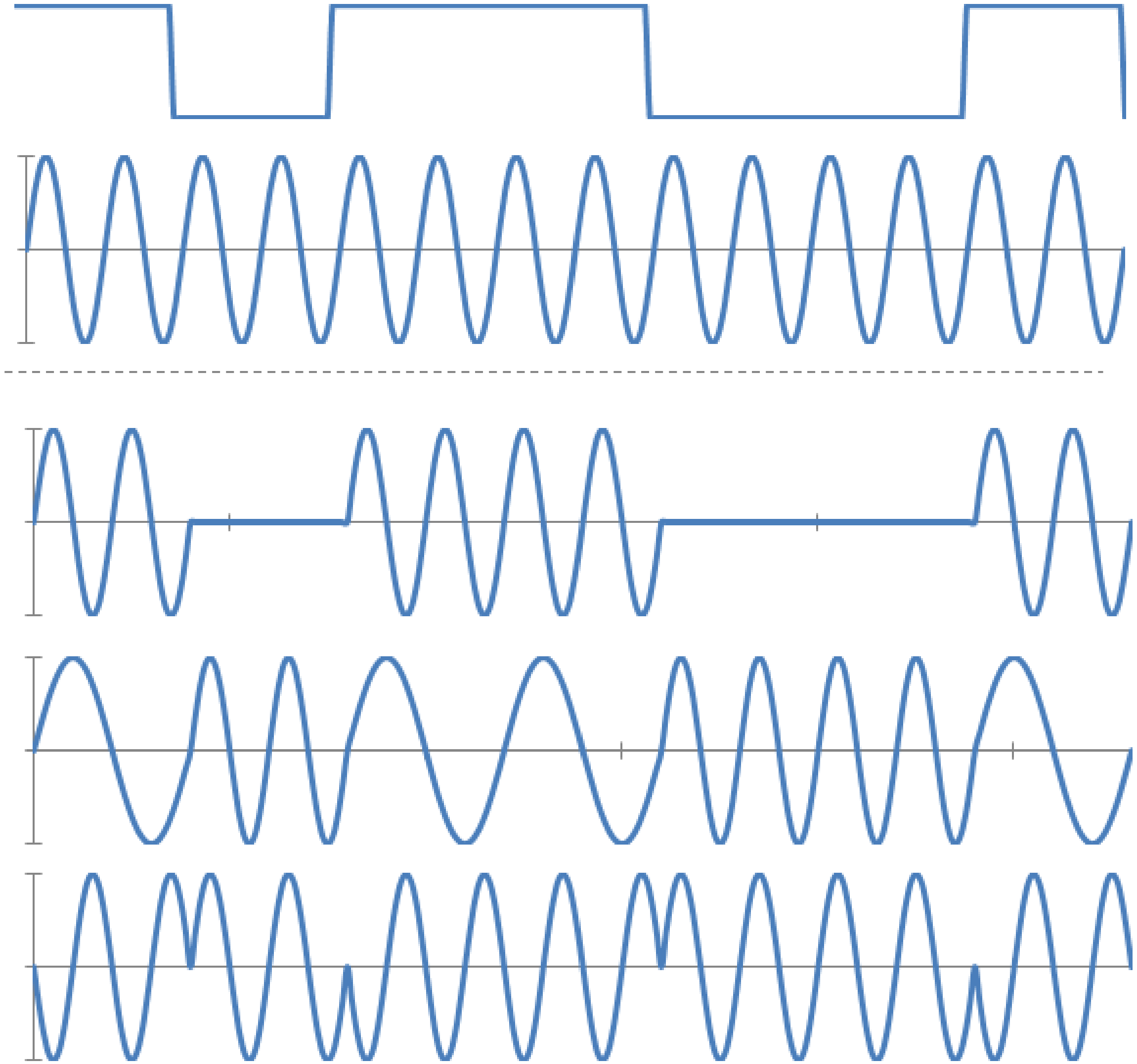
Digital signal

Carrier signal

Amplitude
modulation (AM)

Frequency
modulation (FM)

Phase
modulation (PM)



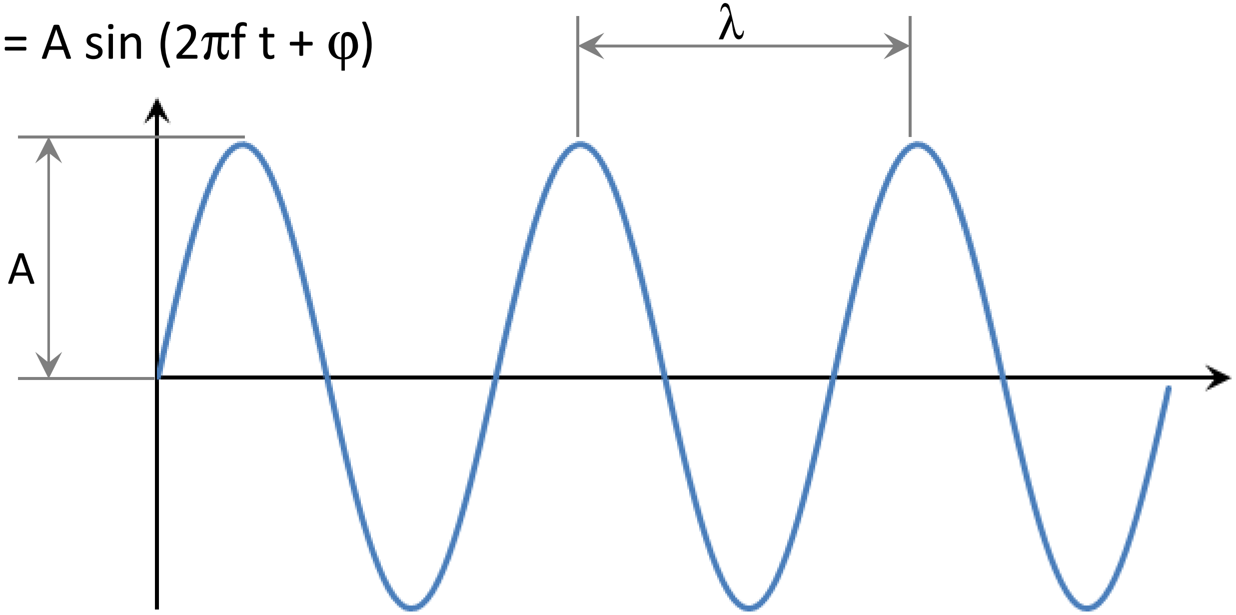
Bases of Wireless Communication

- **Wave:** A kind of changing, which results point-to-point (cyclic) energy transfer.
- **Amplitude:** Distance between the zero and the maximum signal height.
- **Frequency (f):** Number of cycles in one second.
- **Time of period (T):** The time of one cycle $T = 1/f$.
- **Wave length** (λ): Distance between two identical signal height values.
- **Speed of light (c):** velocity of an electromagnetic ray

  $C = f\,\lambda$

Bases of Wireless Communication

$x(t) = A \sin(2\pi f\, t + \varphi)$



Example (Wi-Fi):

f = 2.4 GHz = $2.4 * 10^{9}$ Hz

λ = 125 mm = $0.125 * 10^{-3}$ m

T = 41.7 ns = $4{,}17 * 10^{-10}$ s

c = 300 000 km/s = $1.08 * 10^{9}$ km/h

Wireless transmission

Propagation and detection of electromagnetic signals are performed by antennas.

The two ways of transmitting:

- **Directed**: focused electromagnetic ray. Antennas should be positioned very precisely.
- **Omnidirectional** (not directed) : radiation can be received with multiple antennas

Three frequency ranges for wireless transmission:

- 2 - 40 GHz (microwave transmission) (directed)
- 30 MHz - 1 GHz (radio frequency) (omnidirectional)
- $3\ 10^{11}$ - $2\ 10^{14}$ Hz (infrared)

Communication satellites

Relaying/forwarding either in space or on the ground

- Geostationary satellites (Arthur C. Clarke)
  - Altitude 35800km
- Medium-Earth orbit satellites
  - Altitude 5000-20000km
  - Global Positioning System (GPS)
- Low-Earth orbit satellites
  - Altitude 150-2000km
  - Iridium, Globalstar, Teledesic

Topologies

Physical topology:

Investigates the placement of nodes and their connection possibilities. (Cable topologies).

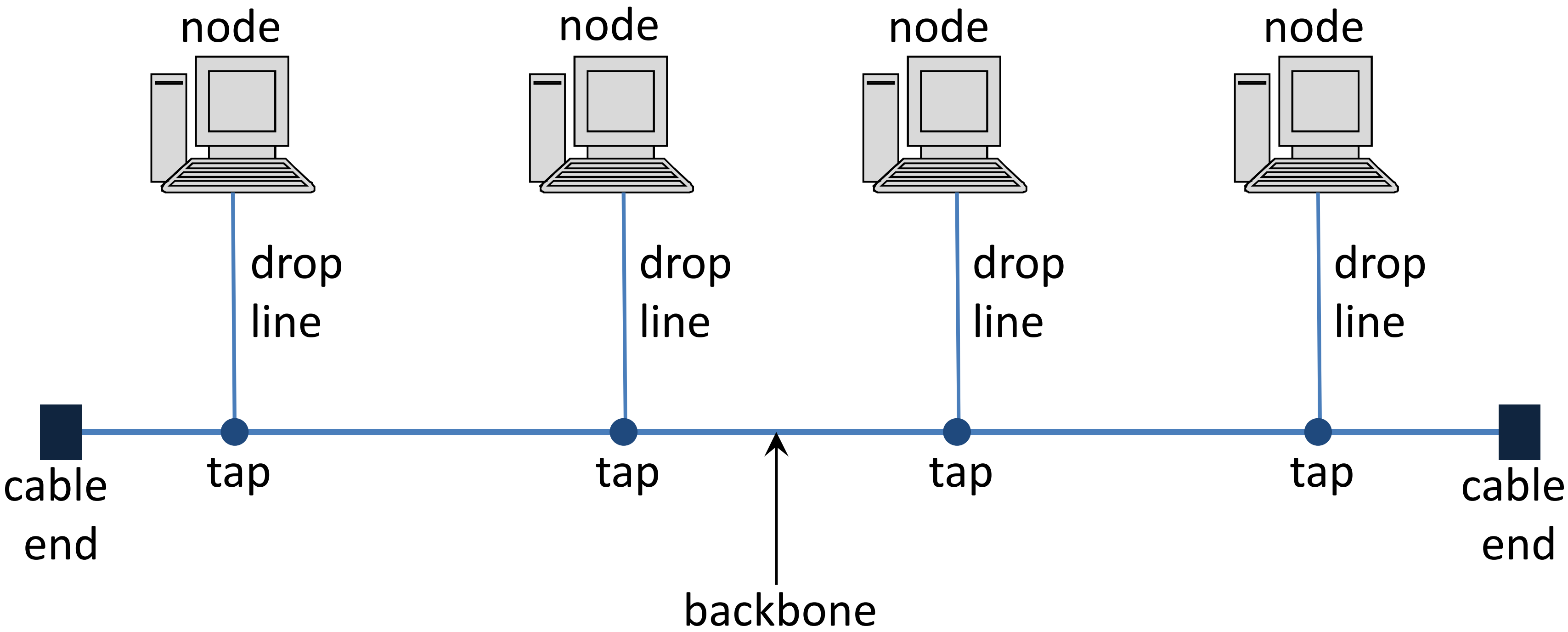
Logical topology:

Investigates the logical sequence and order of nodes.

Topologies:

- Bus
- Ring
- Mesh
- Star

Bus topology



Bus topology

One long cable acts as a backbone to link all the devices in the network. Nodes are connected to the common main cable by drop lines and taps.

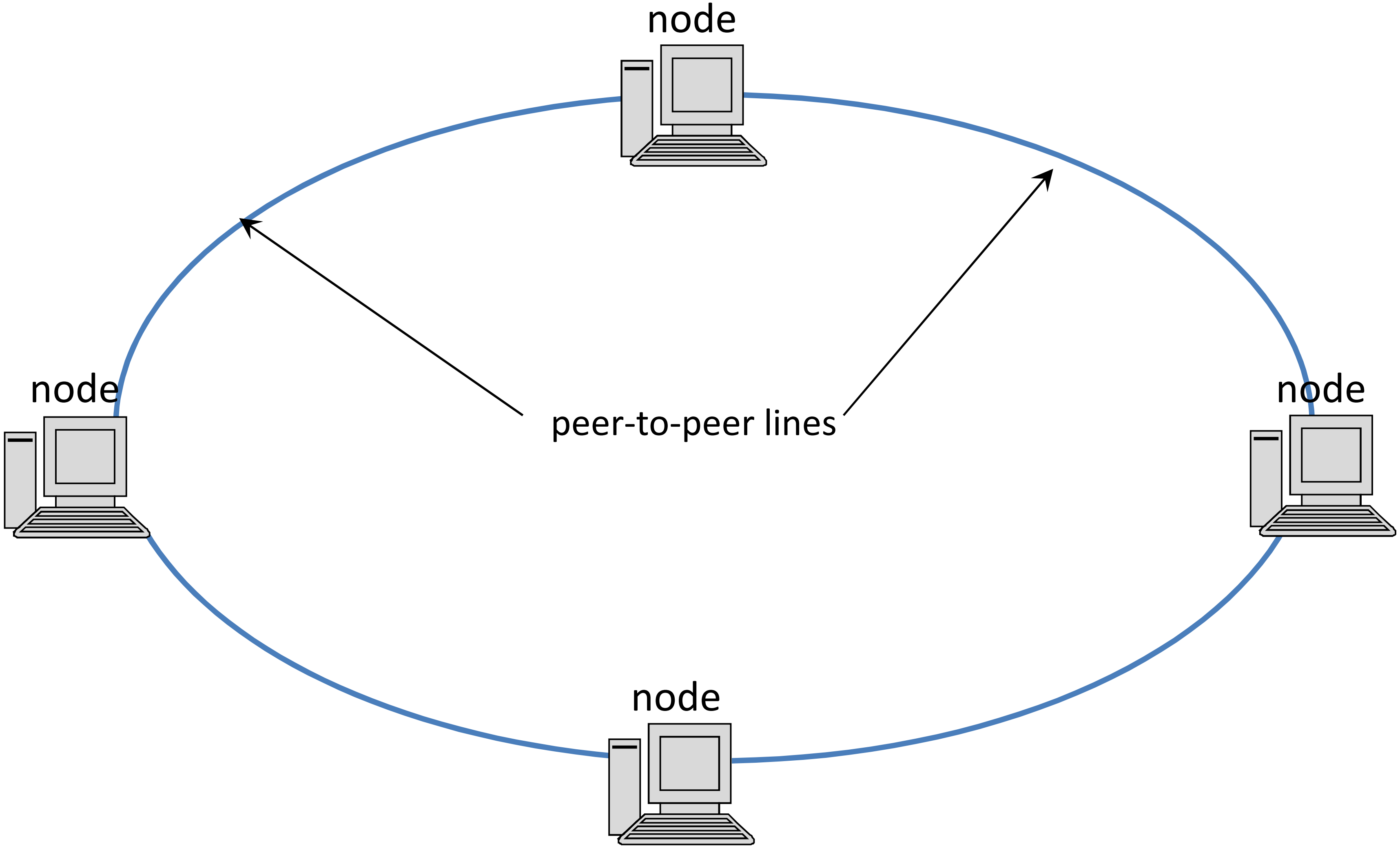
Advantage:

- Easy installation
- Simple and cheap

Disadvantage:

- Difficult fault isolation
- Bandwidth is shared on all links

Ring topology



Ring topology

Each device has a dedicated point-to-point line connected only to the two devices on both sides.

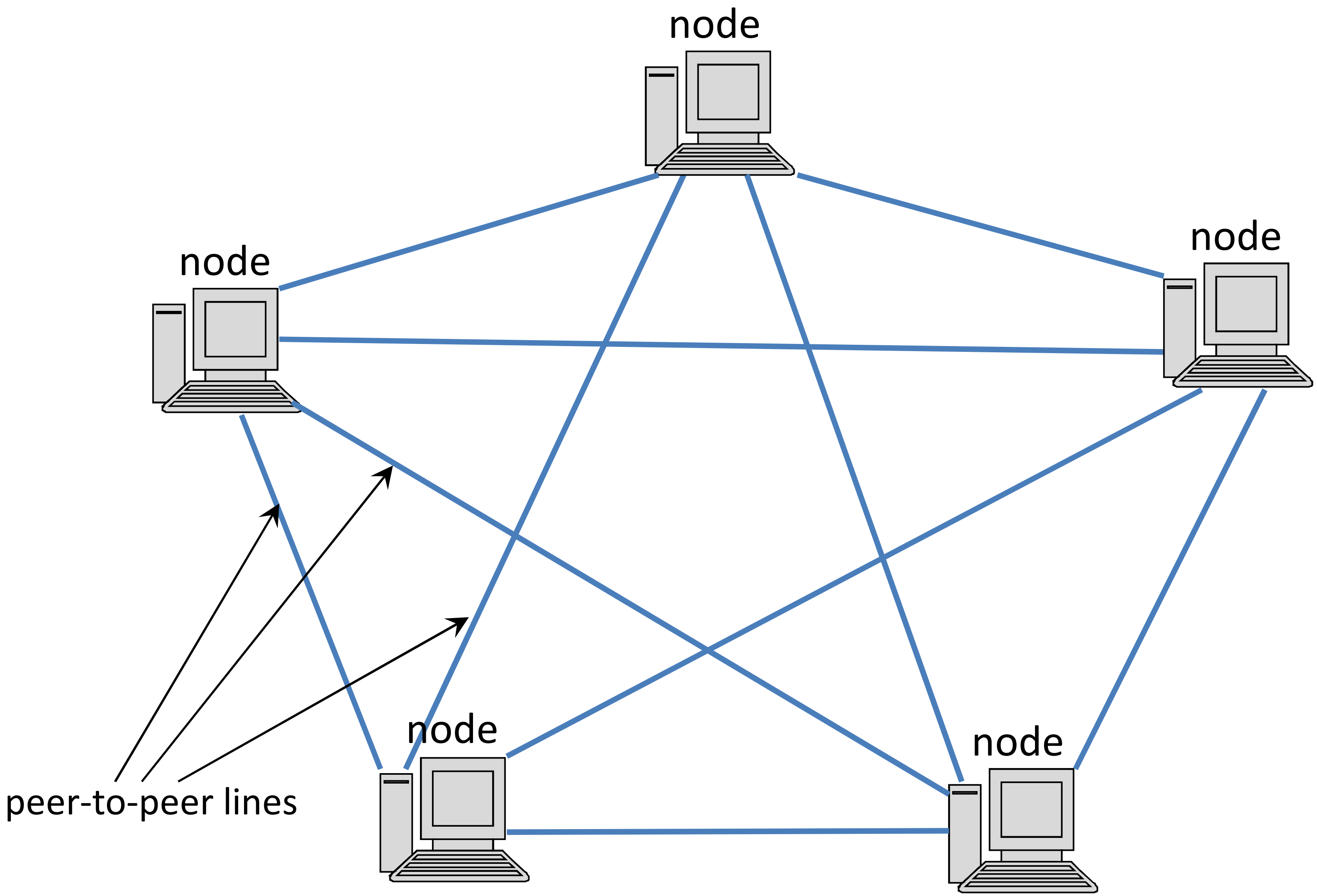
Advantage:

- Easy installation
- Fault isolation is simplified

Disadvantage:

- Changing a devices can affect the network
- Bandwidth is shared on all links

Mesh topology



Mesh topology

Every device has a dedicated point-to-point link to (almost) every other device.

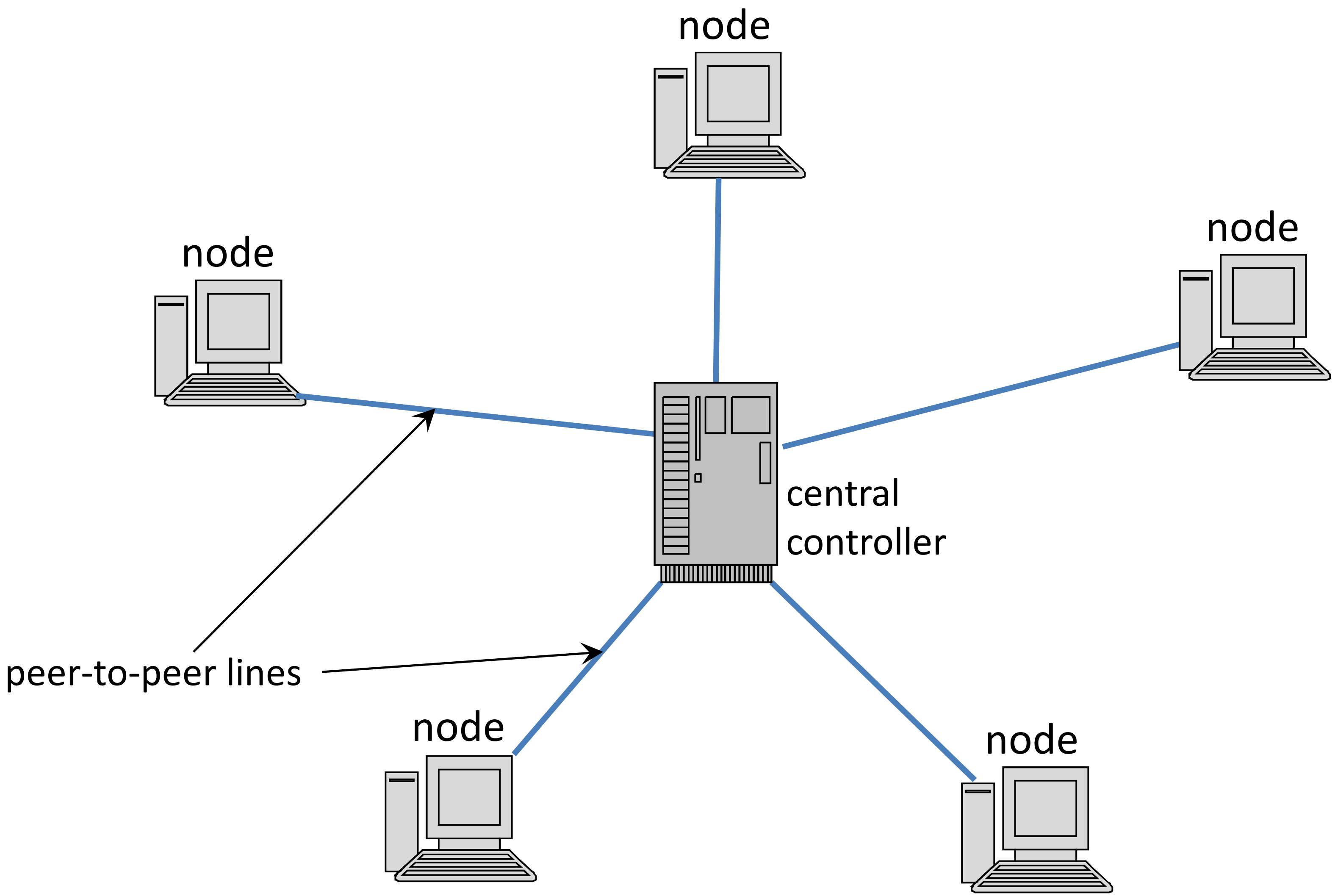
Advantage:

- Mesh topology is robust
- Lines are not shared (in most of cases)

Disadvantage:

- A fully connected mesh network therefore has N(N-1)/2 physical channels to link N devices

Star topology



Star topology

Each device has a dedicated point-to-point link only to a central controller (usually a switch).

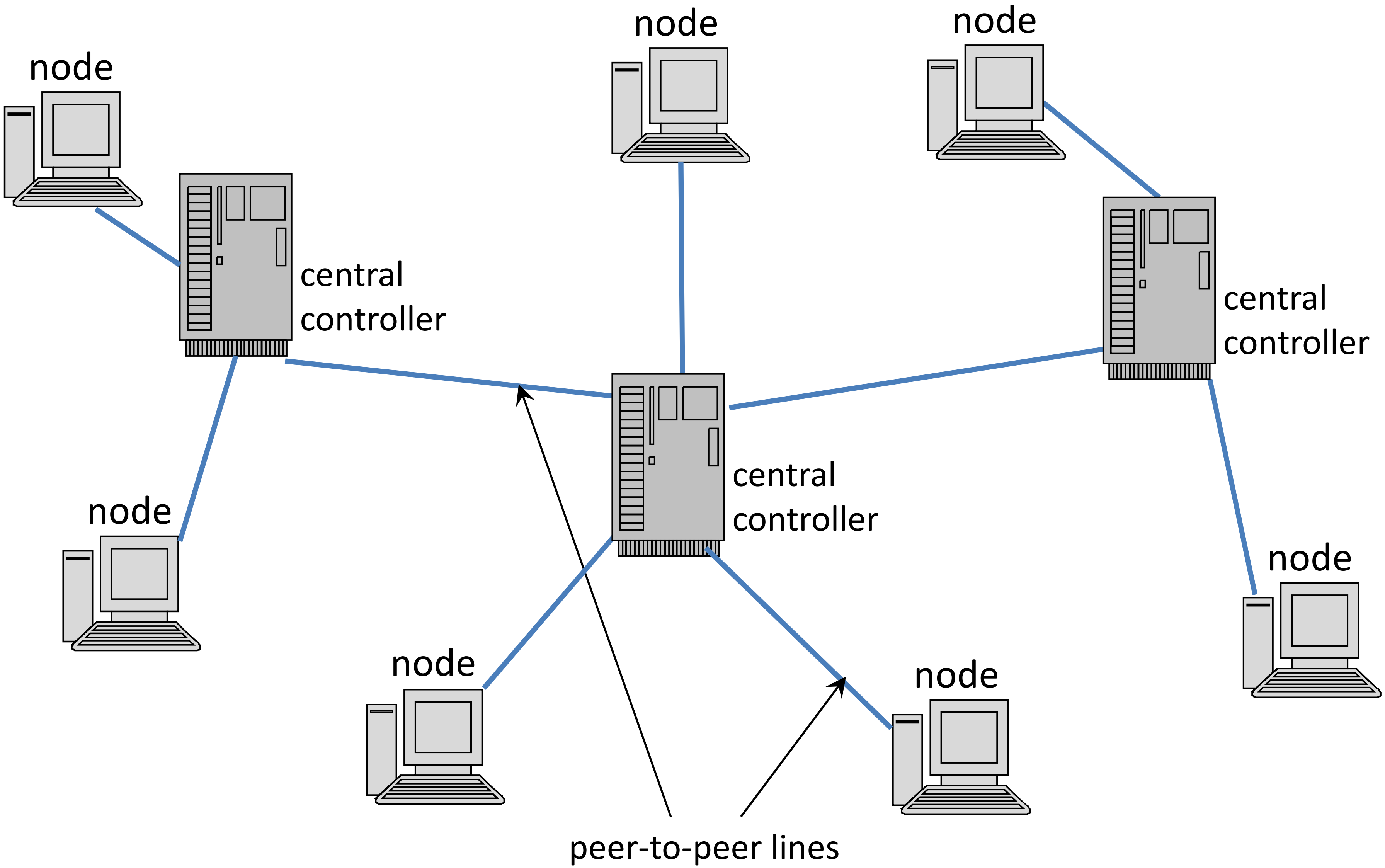
Advantage:

- if a link fails, only that link is affected
- Lines are not shared

Disadvantage:

- Failure of the central hub renders the network unserviceable

Extended star (tree) topology



Data link layer

Data link layer

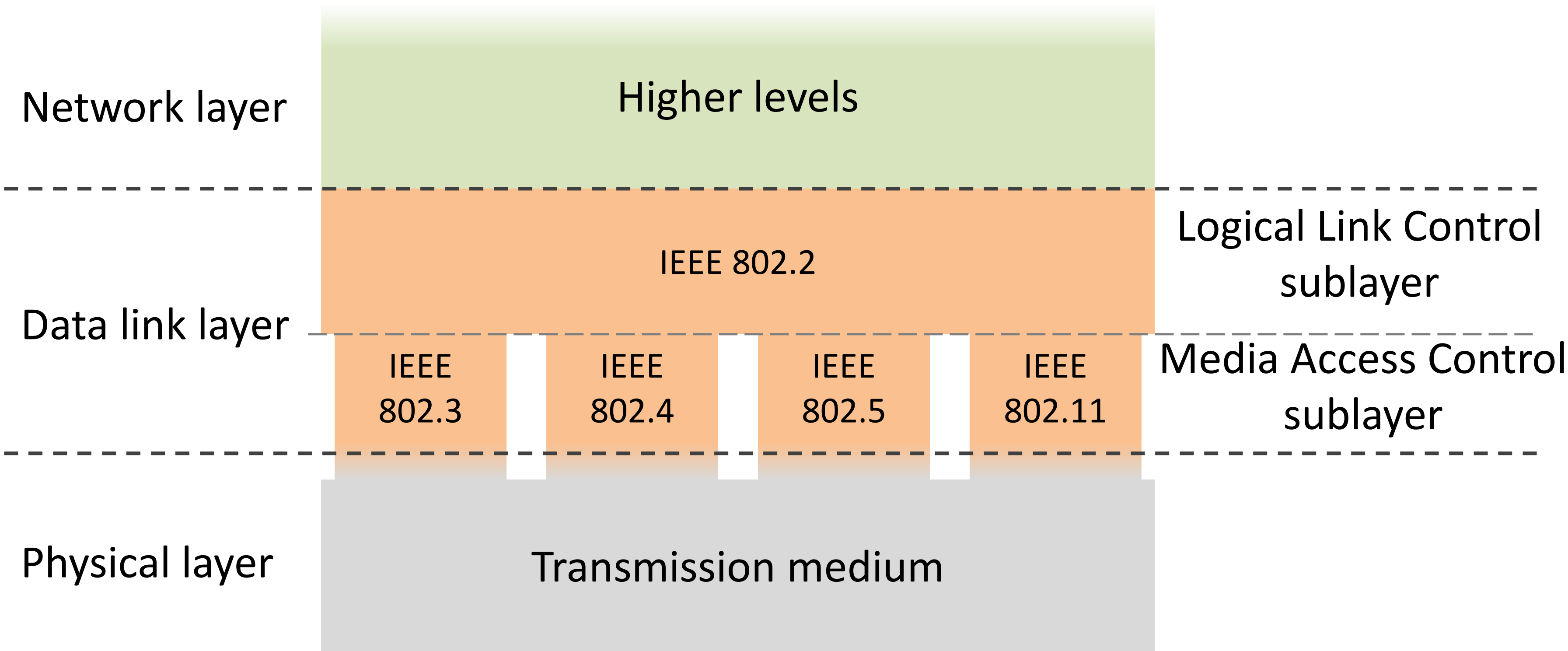
Second layer of hybrid model (L2)

Reliable transmission between two directly connected devices. Two sublayers: LLC, MAC.

Topics

- Physical addressing (identification)
- Media access
- Logical topology
- etc.

Data link Layer



IEEE 802.2 = Logical Link Control (LLC) protocol

IEEE 802.3 = CSMA/CD
IEEE 802.4 = Token bus
IEEE 802.5 = Token ring
IEEE 802.11 = Wi-Fi

Media Access Control (MAC) protocols

Framing

Breaking the bit stream into frames

- Character count

5 5 1 3 6	4 0 2 3	7 4 3 5 9 6 4	4 6 9 1	without error

5 5 1 3 6	6 0 2 3 7 4	3 5 9	6 4 4 6 9 1	with error

- Byte/character stuffing (starting/end flag byte)

F | t o t a l   f r a m e   c o n t e n t | F

F | T o t a l   @ F r a m e   C o n t e n t | F

F | B i g . @ F r a n k @ @ g m a i l . c o m | F

- Bit stuffing

Similar to byte stuffing just special bit pattern is stuffed.

Error detection and correction

- Checksum: A special value calculated based on the frame content and attached to the end of the frame before sending
- After receiving the frame it is calculated again and compared by the original/attached value
- If the two values are different, an error occurred during transmission.
- Examples
  - Parity bit
  - Cyclic Redundancy Check (CRC)

Data-link technologies

WAN

- SLIP
- PPP
- ATM
- X.25
- Frame-relay
- ISDN
- ADSL

LAN (MAN)

- Aloha
- Ethernet
- Wi-Fi
- Token-ring
- Token-bus
- FDDI
- DQDB

Media access

Static (suitable, if node number is small and constant)

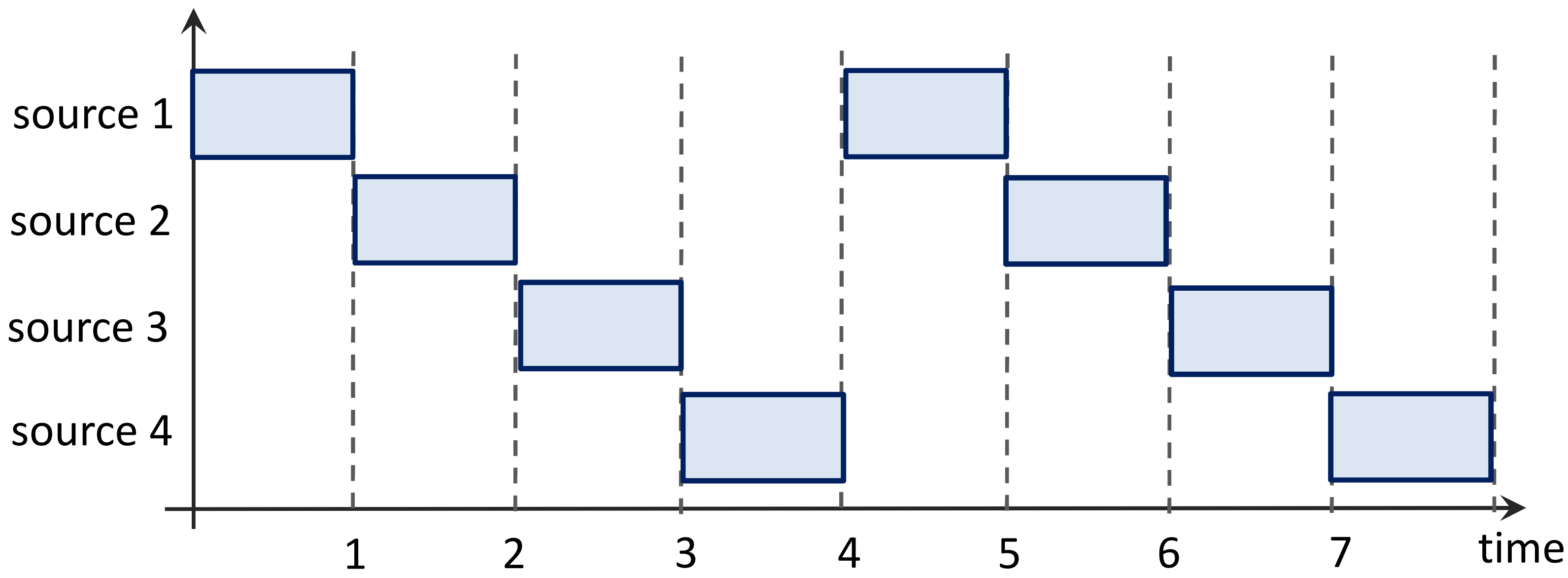
- Time-Division Multiplexing (TDM)
- Frequency-Division Multiplexing (FDM)

Dynamic (suitable, if node number is large or changing)

- No carrier sense
- Time-slotted
- Token
- Carrier Sense Multiple Access (CSMA)
- Collision Detection (CD) / Collision Avoidance (CA)
- Code Division Multiple Access (CDMA)

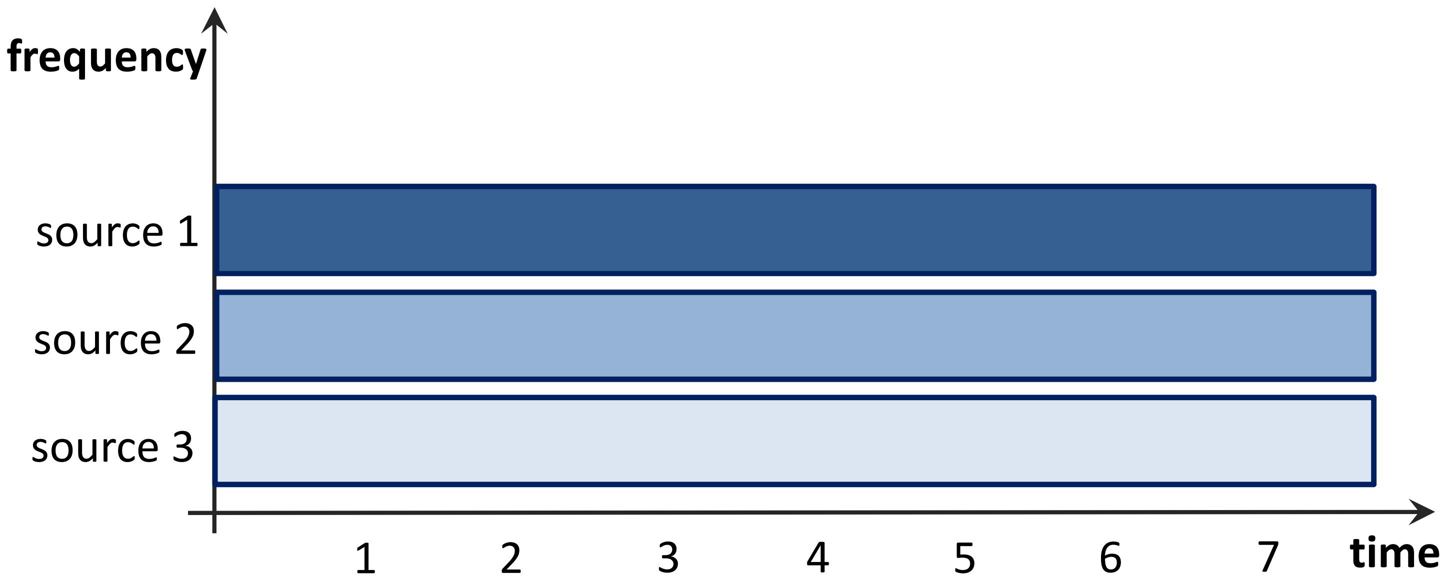
TDM

- Each source can send periodically only in a given time interval
- Low speed sources, high speed channel



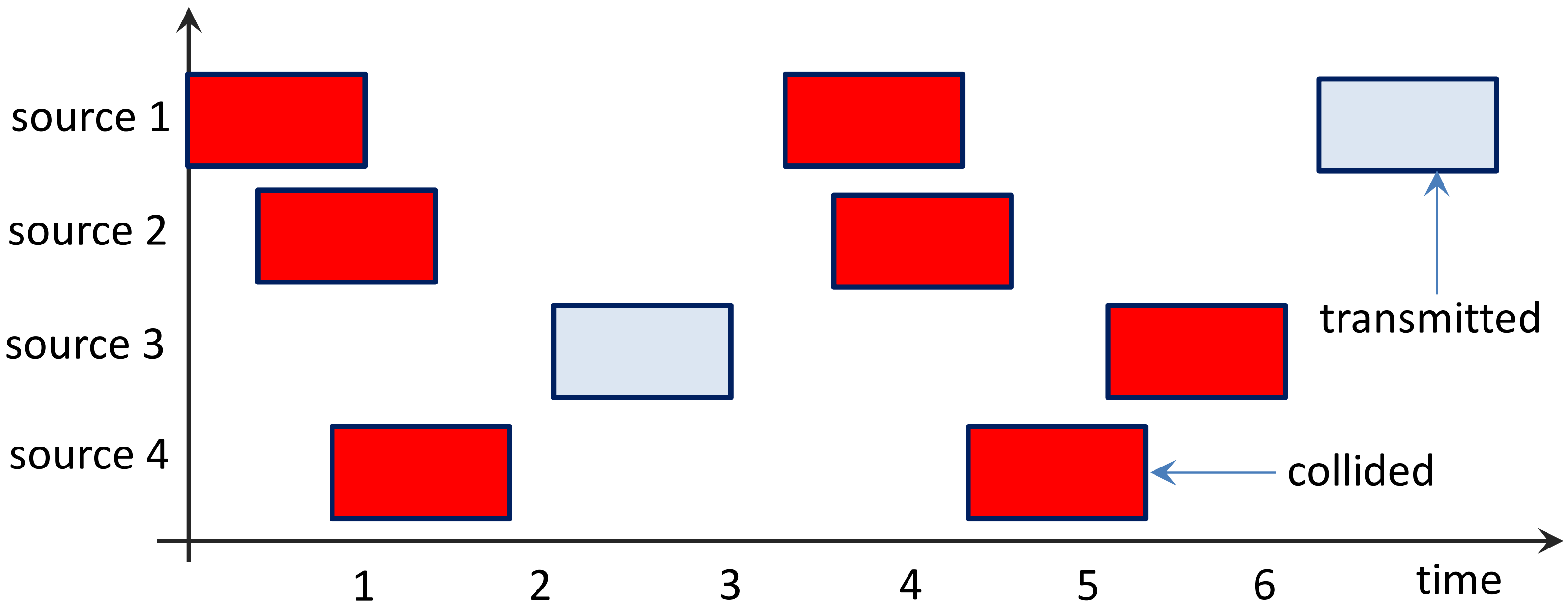
FDM

- Each source use a separate (not overlapping) frequency sub-band to modulate signals
- Example: radio and TV broadcasting
- In case of optical signals it is also referred Wave-length Division Multiplexing (WDM)



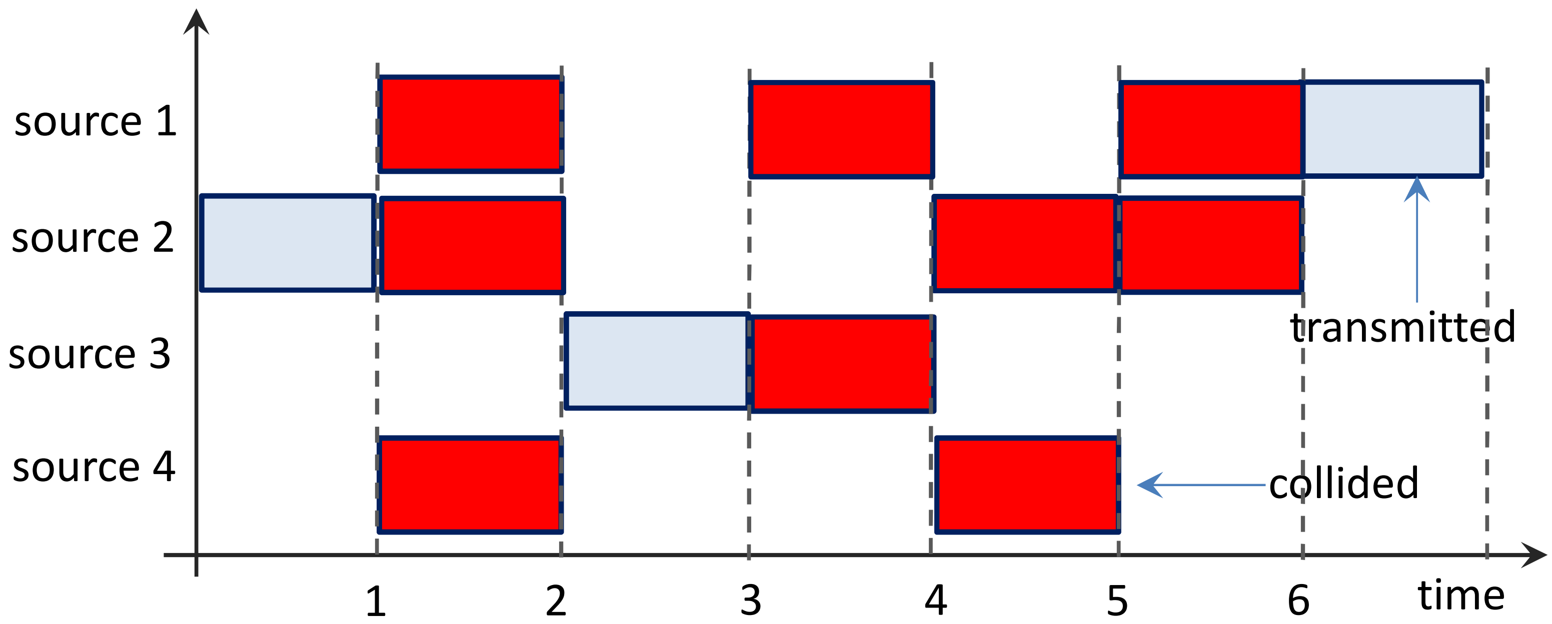
Pure ALOHA

- Wireless communication between Hawaiian islands
- Anybody can send a frame anytime
- Many collisions occur (max efficiency 18.4%)



Slotted ALOHA

- Time slot is applied
- A source can start sending only at beginning of slot
- Many collisions occur (max efficiency 36.8%)



Token-ring

- Logical topology: ring (physical topology: star)
- Special frame (token) always orbits in the network
- Device can transmit only if it has control of the token
- Who has the token send a data-frame, it is forwarded from node to node
- Destination gets data-frame and forward an acknowledgement
- Source gets acknowledgement, removes the frame, passes the token to the next node
- No collision occurs

Carrier sense multiple access

The same channel is used by several nodes

If the channel is busy no one else starts transmission

- 1 persistent CSMA: if the channel become idle/free, waiting/ready node starts sending immediately
- p-persistent CSMA: if the channel become idle, ready node starts sending with *p* probability or waits the next time slot with *1-p* probability
- non-persistent CSMA: if the channel is in use, node wait (immediately, before channel become idle) a random time period

Ethernet

The most popular technology for wired LANs based on **Carrier Sense Multiple Access with Collision Detection** (CSMA/CD) media access method.

version	standard	year	speed
'Classical' Ethernet	IEEE 802.3	1980	10 Mbps
Fast Ethernet	IEEE 802.3u	1995	100 Mbps
Gigabit Ethernet	IEEE 802.3ab	1999	1.000 Mbps
10Gigabit Ethernet	IEEE 802.3ae	2002	10.000 Mbps
100Gigabit Ethernet	IEEE 802.3ba	2010	100.000 Mbps

Ethernet cabling

Name	Cable	Max. segment	Speed	
10Base5	Thick coax	100 m	10 Mbps	Classical Ethernet
10Base2	Thin coax	185 m	10 Mbps	
10Base-T	Twisted pair	100 m	10 Mbps	
10Base-F	Fiber optics	2000 m	10 Mbps	
100Base-T4	Twisted pair	100 m	100 Mbps	Fast Ethernet
100Base-TX	Twisted pair	100 m	100 Mbps	
100Base-FX	Fiber optics	2000 m	100 Mbps	
1000Base-SX	Fiber optics	550 m	1000 Mbps	Gigabit Ethernet
1000Base-LX	Fiber optics	5000 m	1000 Mbps	
1000Base-CX	2 pairs of STP	25 m	1000 Mbps	
1000Base-T	4 pairs of UTP	100 m	1000 Mbps	

Ethernet frame format

Direction of transmission

	Preamble	7 bytes (7 x ‘10101010’ for synchronization)
	Start of Frame	1 byte (‘10101011’)
Header	**Destination address**	6 bytes
Header	**Source address**	6 bytes
Header	**Length/Type**	2 bytes (IEEE/Ethernet)
Data	**Data/Payload**	0 - 1500 bytes
Tail	**Pad (if necessary)**	0 - 46 bytes (minimum frame length is 64 bytes)
Tail	**CRC checksum**	4 bytes

Ethernet (MAC) address

6 bytes wide identifier of network cards written in hexadecimal number system separated per bytes.

Example: 00-26-9E-93-75-AA

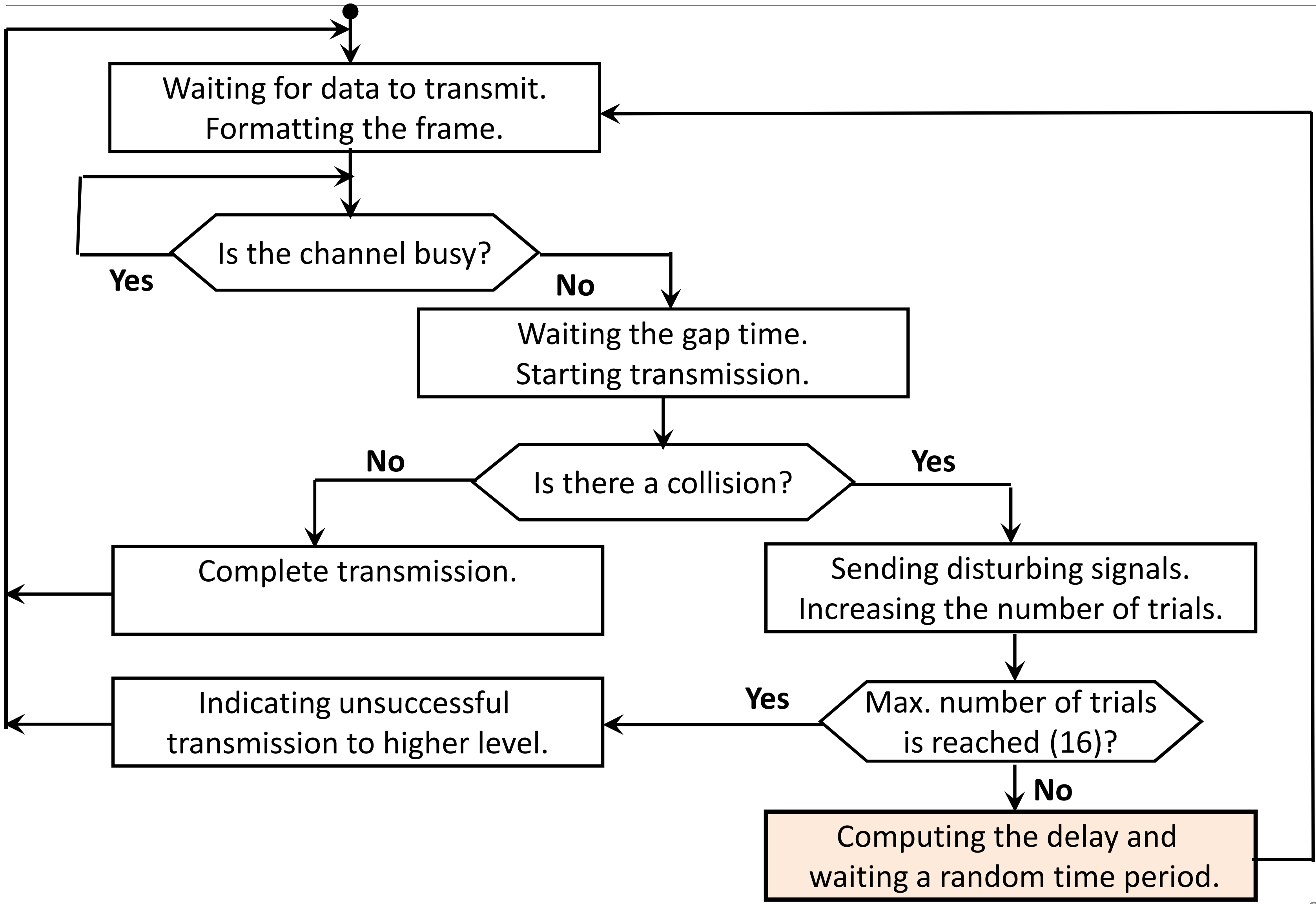
UOI: ID of manufacturer (3 bytes)

serial number (3 bytes)

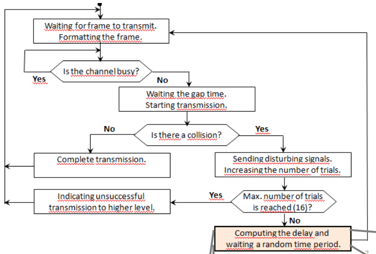
MAC address is ‘burned’ into the network interface.
There are no network cards in the world with same MAC address.

Broadcast address: FF-FF-FF-FF-FF-FF

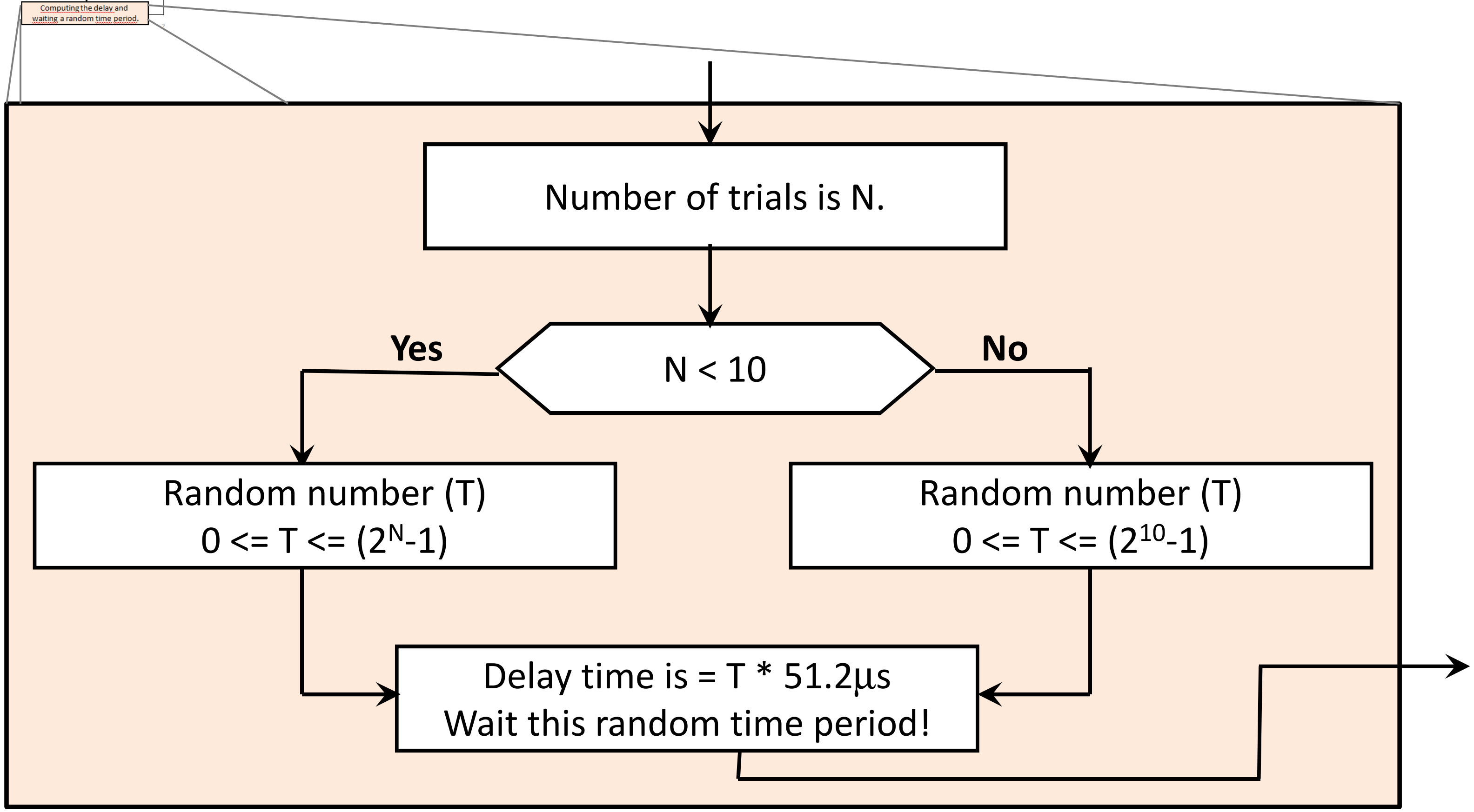
Ethernet frame transmission (CSMA/CD)



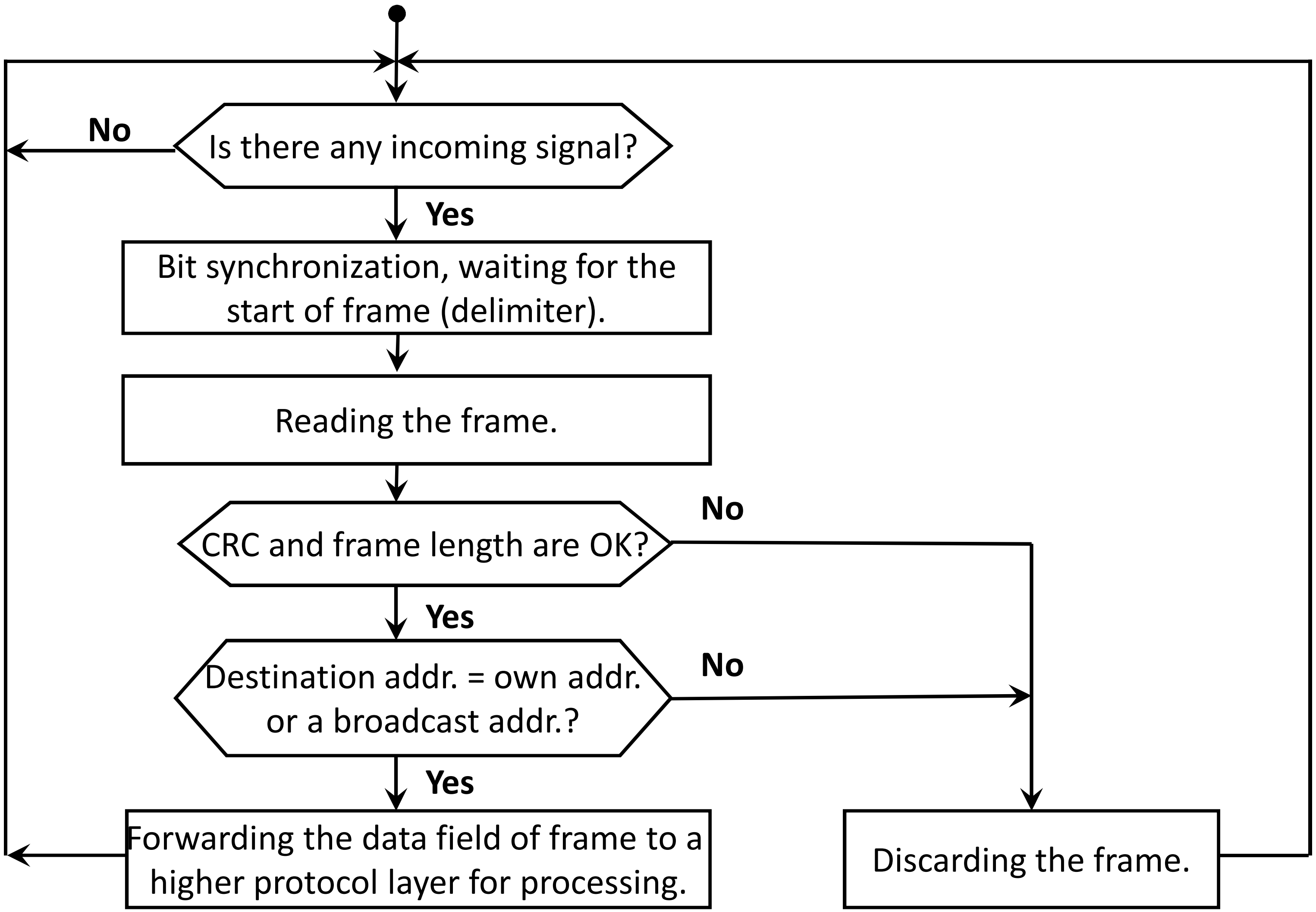
Computing the delay and wait



Binary Exponential Backoff algorithm



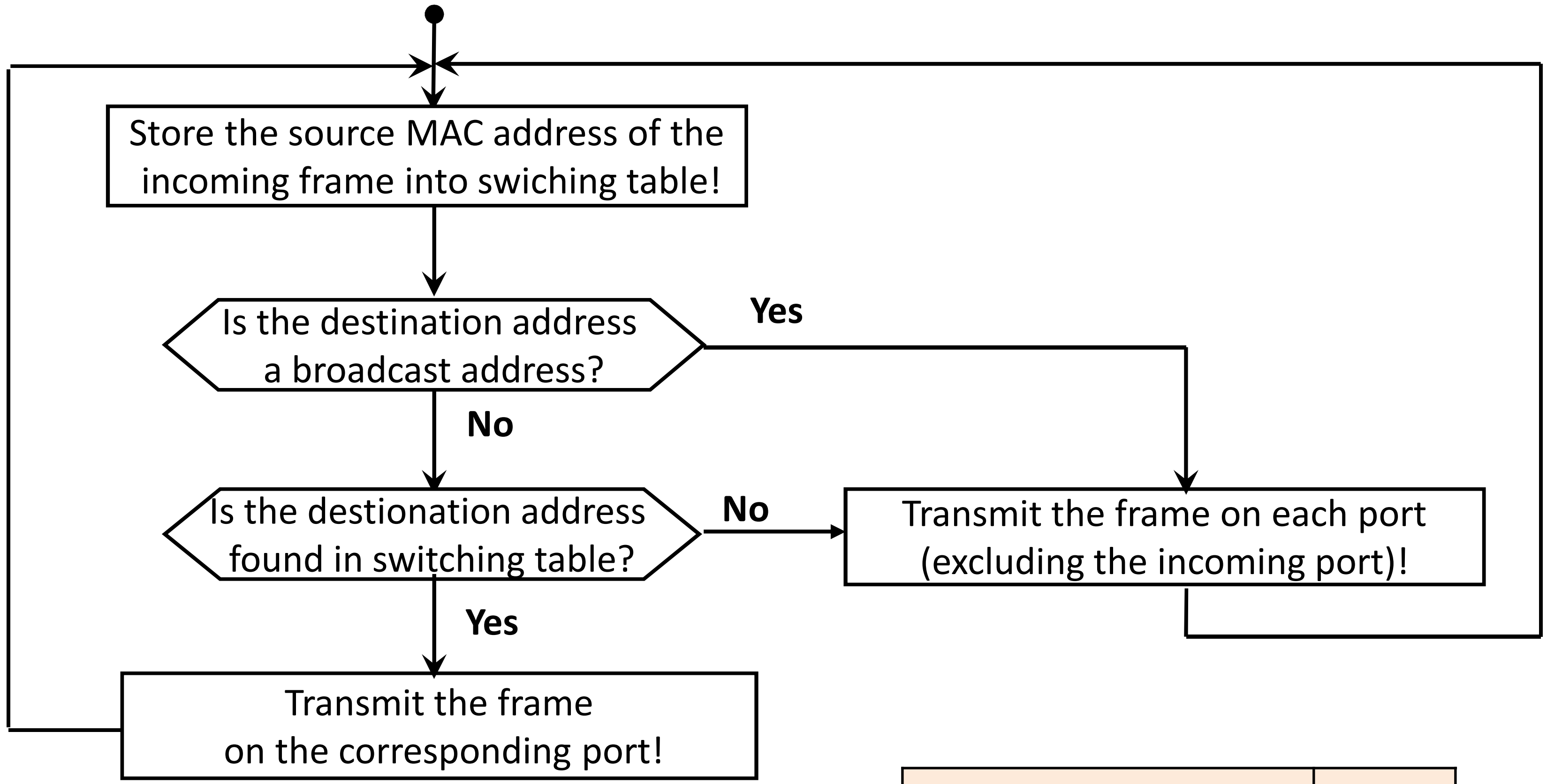
Receiving an Ethernet frame



Ethernet switching

- A collision domain occurs when multiple computers are connected to the single, shared transmission media (line).
- Devices in second layer (bridge or switch) provide switching divide the collision domains.
- Each port of a switch forms a separate collision domain.
- These devices control the transmission of frames by MAC-addresses assigned to the Ethernet devices.
- Switches for each port stores the MAC addresses of the accessible devices from that port in a switching table.
- Switches upload and maintain their switching tables (cache) dynamically.

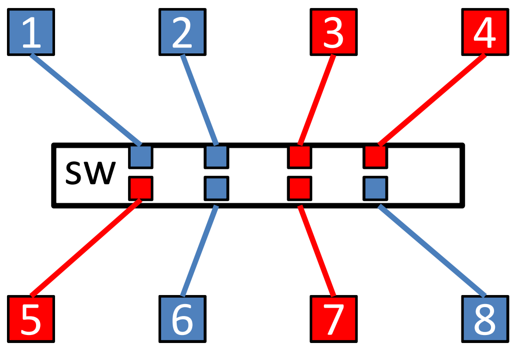
Ethernet switching



MAC address	Port
00-26-9E-93-75-AA	1
00-1E-64-60-0E-B0	2
08-00-27-00-FC-E1	3

Virtual LANs

- Goal: decoupling the logical topology from the physical topology
  - Migration has not got wiring effects
  - Redefinition of broadcast domain
- Based on VLAN-aware switches
- Each MAC addresses or each ports of a switch belongs to a given VLAN
  - Tagged by VLAN name
- IEEE 802.1Q supports VLAN on Ethernet



Wi-Fi

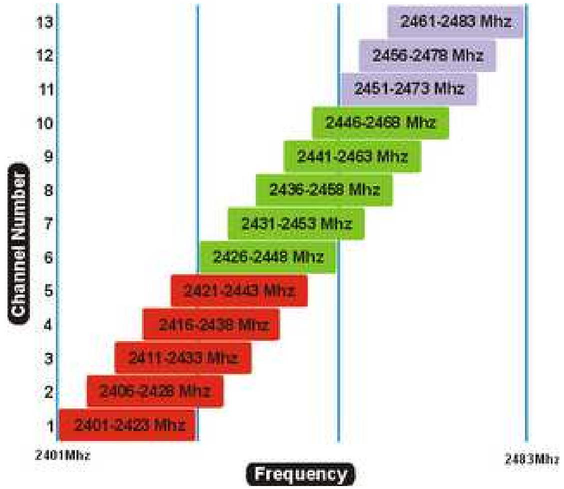
A set of standards for implementing Wireless Local Area Network (WLAN) computer communication.

Located in Physical and Data link layer.

More important standards:

- IEEE 802.11a (1999)
- IEEE 802.11b (1999)
- IEEE 802.11g (2003)
- IEEE 802.11n (2009)

Wi-Fi



IEEE 802.11b:

- 13 overlapping channels (EU) with 5 MHz bandwidth on 2.4 GHz.
- Maximum 11 Mbps speed.
- Different coding/modulating technologies.

IEEE 802.11a:

- Technology working on 5 GHz (light-like propagation).
- Maximum 54 Mbps data transmission speed.
- Requires a separate radio frequency (RF) unit (5 GHz).

Wi-Fi

IEEE 802.11g:

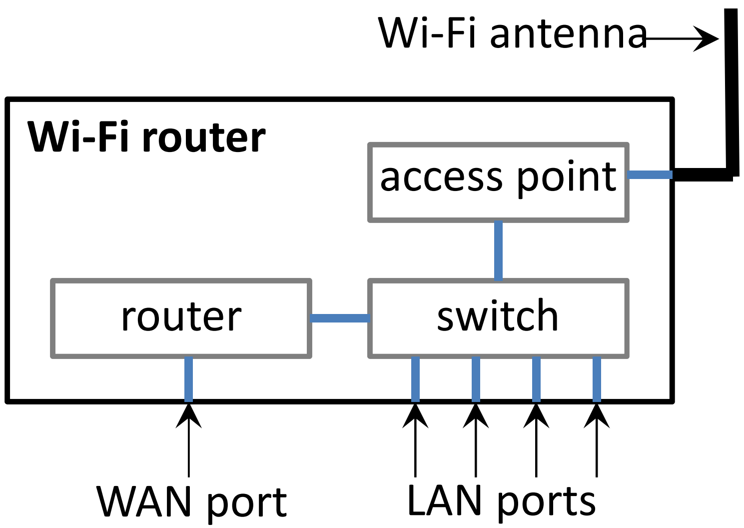
- New coding and modulating technology on 2.4 GHz (PBCC, OFDM).
- 54 Mbps maximum data transmission speed.
- Retain frequency (2.4 GHz) provides a backward compatibility for 802.11b systems.

IEEE 802.11n:

- Technology working on both 2.4 GHz and 5 GHz.
- 600 Mbps maximum data transmission speed.
- More antennas.

Wi-Fi

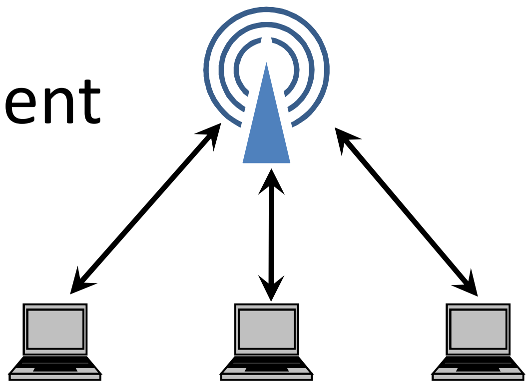
- Access point (AP): network device allows a Wi-Fi device to connect the wired network (bridge between IEEE 802.11 and IEEE802.3)
- Wi-Fi router: complex device
  - Router
  - Switch
  - Access point
  - Other
    - Storage
    - web/ftp server



Wi-Fi

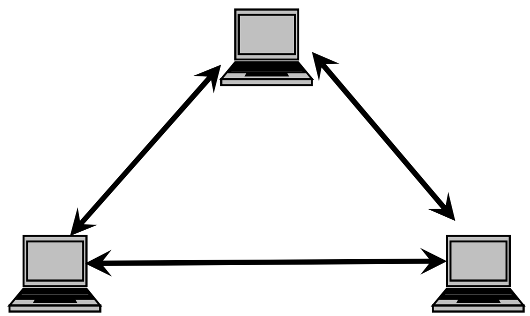
Infrastructure mode

- Wi-Fi devices directly connect only to a base station (access point)
- Multiple access point can be present (roaming)



Ad-hoc mode

- No base station (AP)
- Wireless devices directly connect to each other (peer-to-peer)
- Wi-Fi Direct



Wi-Fi

SSID: ‚name’ of the network

Security solutions:

- Open access
  - Encryption free
- SSID is hideable
- Wired Equivalent Privacy (WEP)
  - Easily breakable, week encryption
- Wi-Fi Protected Access (WPA)
  - Temporal Key Integrity Protocol (TKIP; 128 bit)
- Wi-Fi Protected Access 2 (WPA2)
  - Advances Encryption Standard (AES; 128/256 bit)

FDDI

- Fiber Distributed Data Interface
- MAN (or LAN) media access
- Dual ring topology
- Multi-mode optical cables
- 100Mbps data rate
- Up to 200km
- Up to 1000 nodes
- Fault tolerance
- 4B5B signal coding

PPP

- Point-to-Point Protocol (RFC 1661)
- WAN data-link layer protocol
- Establish direct connection between two nodes
- Used for costumer dial-up internet access (ISP to home)
- Authentication, compression, encryption, error detection
- Used over serial line, trunk line, cellular phone, optic link
- Directives: PPP over Ethernet, PPP over ATM
- Parts
  - LCP: link establish, configure, testing
  - NCP: supports L3 protocols: IP, IPX, AppleTalk, etc.

PPP

Working scheme

- Costumer PC calls provider’s router via a modem
- Router’s modem answering, establishing physical connection
- PC sends LCP packets to configure PPP
- NCP packets configure network layer (e.g. IP address)
- Normal Internet traffic
- NCP frees up IP address, close network layer
- LCP shuts down data-link layer connection
- Modem hang up the phone releasing physical layer

N-ISDN

(Narrowband) Integrated Service Digital Network

Network services over PSTN (Public Switched Telephone Network).

Standard channel types:

- A: 4KHz analog (telephone)
- B: 64kbps digital (voice and data)
- C: 8/16kbps digital
- D: 16/64kbps digital (signaling)

N-ISDN

Standard channel combinations:

- Basic Rate Interface (BRI)
  - 2B + $1D_{(16)}$ channels
- Primary Rate Interface (PRI)
  - 23B + $1D_{(64)}$ channels (USA)
  - 30B + $1D_{(64)}$ channels (EU)
- Hybrid Rate Interface
  - 1A + 1C channels

Its bandwidth is not enough today.

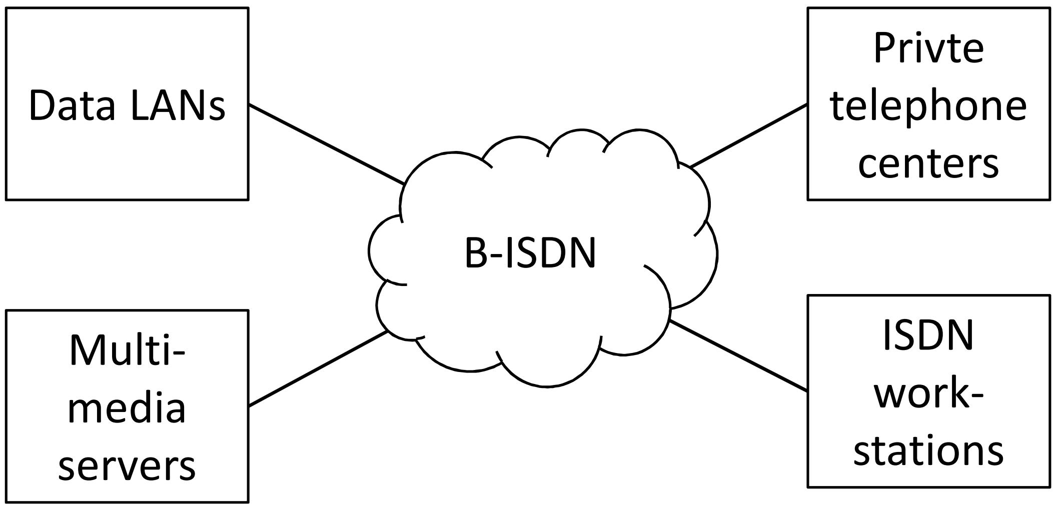
B-ISDN

(Broadband) Integrated Service Digital Network

Network service demands:

- Data-, voice-, video-, multimedia transfer, interactive communication (different bandwidth needs)

Computers using this services are connected by B-ISDN.



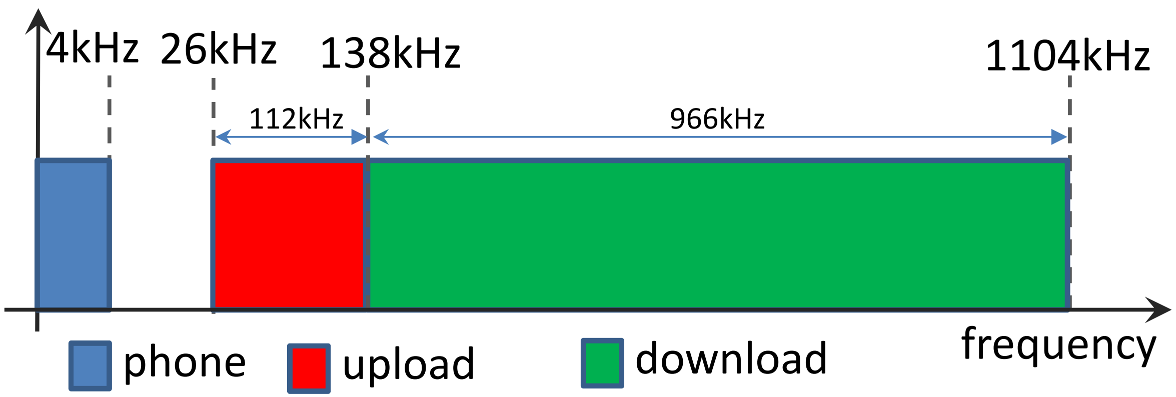
ATM

- Asynchronous Transfer Mode (ATM)
- Different media have different needs (low latency, constant bitrate, nothing special, etc.)
- Protocol over ISDN, PSTN, SONET/SDH network
- Fixed-sized frames (cell: 5+48 bytes)
- In OSI data-link (L2) and physical (L1) layer
- Connection-oriented (VC: virtual circuit)
- Similar to both circuit switching and packet switching networks
- Uses asynchronous (no clock) TDM

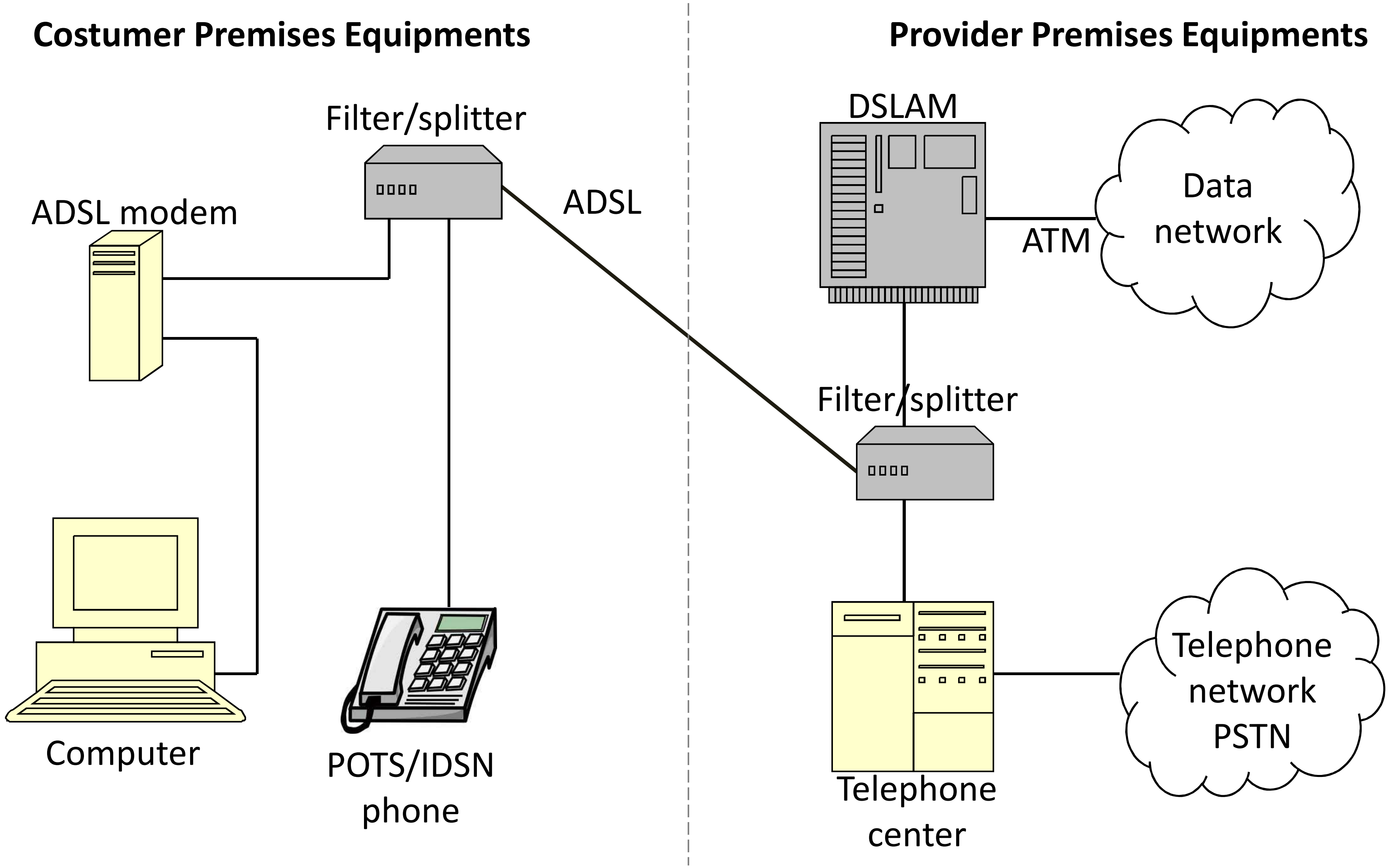
ADSL

- Asymmetrical Digital Subscriber Line
- Most user: large download, but small upload
- Digital communication on twisted pair

	max. download	max. upload
ADSL	8.0 Mbps	1.0 Mbps
ADSL2	12.0 Mbps	1.0 Mbps
ADSL2+	24.0 Mbps	1.0 Mbps

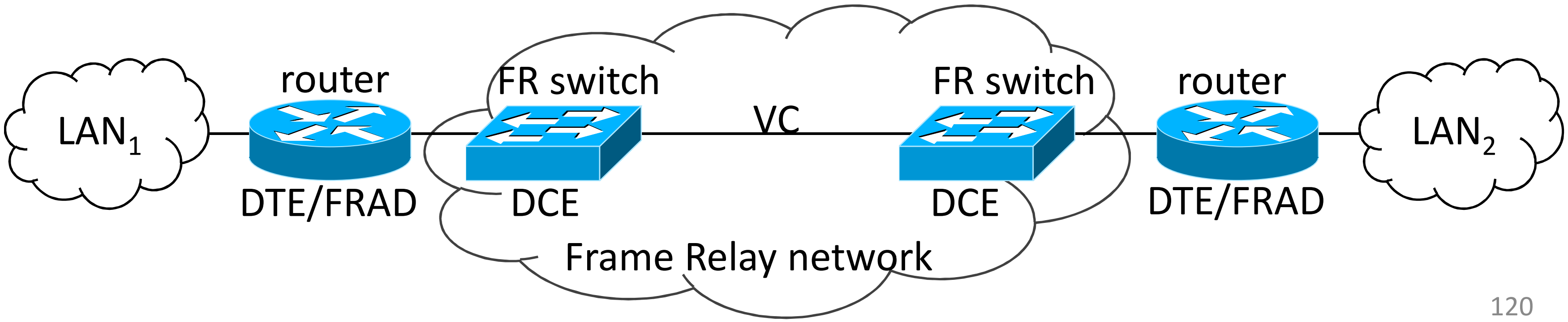


ADSL reference model



Frame Relay

- Standardized WAN technology
- It uses a packet switching methodology
- FR specifies the physical and logical link layers of digital telecommunications channels
- Data is encapsulated in variable-size units (frames)
- Nodes are connected by virtual circuits (VC)



Network layer

Network layer

Third layer of hybrid model (L3)

Connection between any two network nodes (not just dirrectly connected).

Topics

- Network addressing
- Routing
- Subnetting
- etc.

The **IP** network protocol

IP (Internet Protocol) (*RFC 791*)

- The network layer protocol of TCP/IP reference model.
- Widely used, it is the basic element of Internet.
- Most important characteristics:
  - Structure of IP header.
  - IP addressing, address classes.
  - Fragment supporting.
  - **Datagram** services towards Transport Layer.

Structure of IP header

Consists of 32-bit words.

Length: Minimum 5, maximum 15 words.

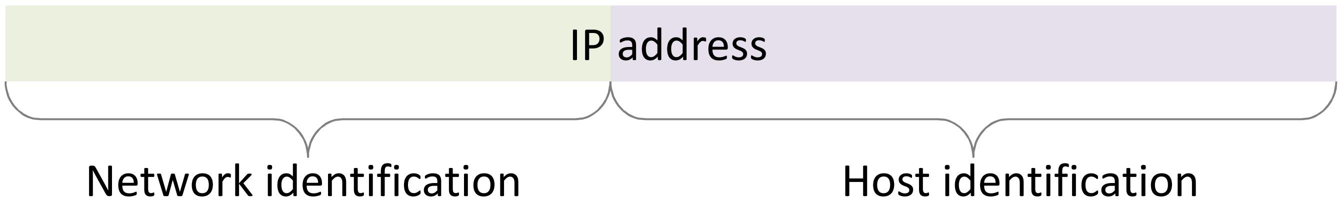
<table>
<tr><td colspan="4">Version</td><td colspan="4">IHL</td><td colspan="8">Type of service</td><td colspan="16">Whole length</td></tr>
<tr><td colspan="16">Identifier</td><td colspan="1"></td><td colspan="1">DF</td><td colspan="1">MF</td><td colspan="13">Fragment offset</td></tr>
<tr><td colspan="8">Time To Live</td><td colspan="8">Transport layer prot.</td><td colspan="16">Header checksum</td></tr>
<tr><td colspan="32">Sender (source) IP address</td></tr>
<tr><td colspan="32">Receiver (destination) IP address</td></tr>
<tr><td colspan="32">Optional field(s) [0-10 words]</td></tr>
</table>

IP addresses

- Identifies the node in Network Layer.
- 32 bit (4 byte) long.
- **Dotted decimal notation**
  - eg. 157.45.190.57
- Managing identifiers
  - InterNIC
  - IANA
- For organisations not unique addresses but address domains (network identifiers) are assigned.

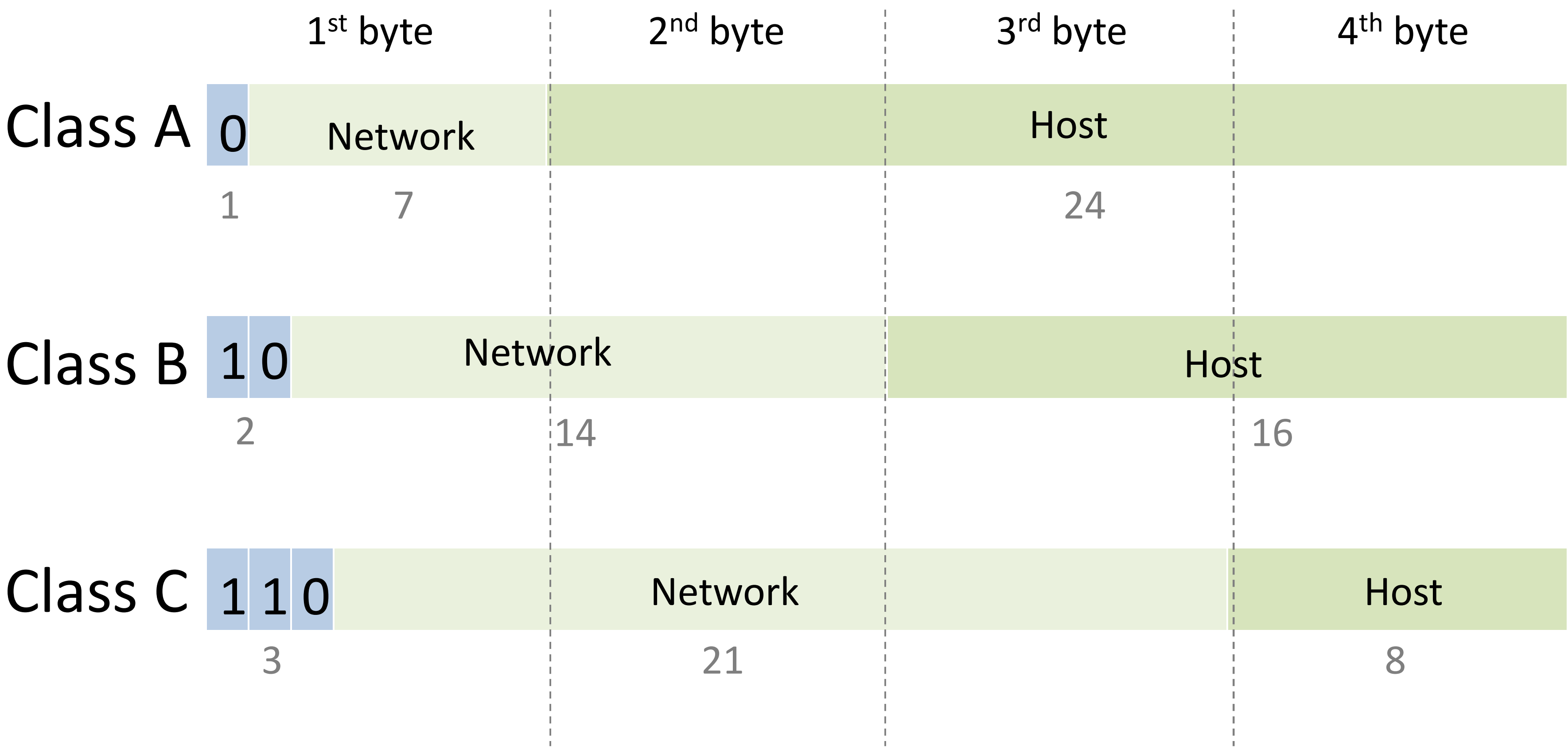
IP addresses

- The first part on an IP address identifies the network, the second part identifies the node (inside the network).



- The IP routing based on the network identifiers.
- How many bits should be in network IDs?
  – If too small, the large domains will be unused.
  – If too large, only small subnetworks can be handled.

Classes of IP addresses



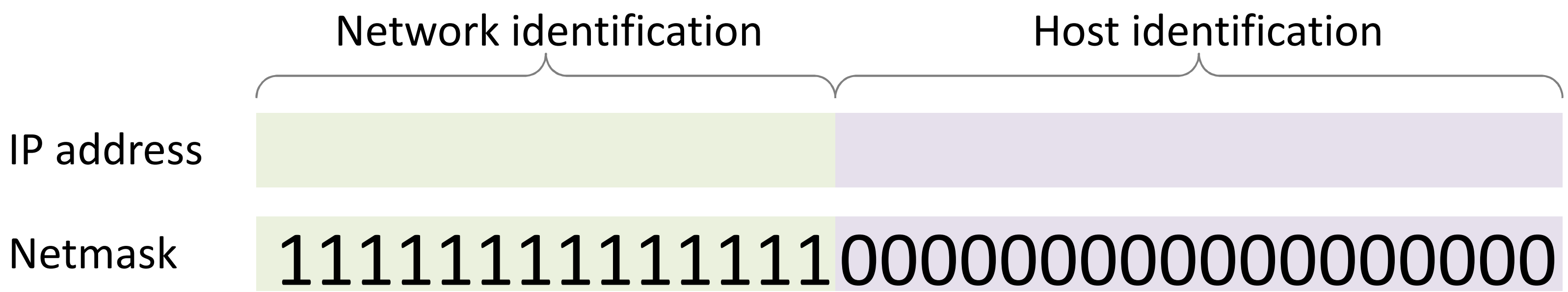
Network mask

Network mask (netmask):

- A 32 bit mask, which contains bits with values of 1 in place of network and subnetwork identifiers, and bits with values of 0 in place of host identifiers.

Prefix length:

- The number of value 1 in netmask (number of binary places in netmask).



Law of First Byte

Class	Leading bit(s)	First byte	Netmask	Prefix
A	0	0-127	255.0.0.0	8
B	10	128-191	255.255.0.0	16
C	110	192-223	255.255.255.0	24

Special IP addresses

- Not specificated host

00000000	000000000000000000000000

- ID of the specific network (network ID)

Network	000000000000000000

- Broadcast on the specific network

Network	111111111111111111

- Loopback address

01111111	Anything

Fragmentation

- Cutting the packet/datagram into pieces at 8-bytes units
- Nodes do it due to datalink MTU
- Sometimes fragments are also fragmented at internal nodes (routers)
- Only the destination merges the fragments
- In the IP header „Fragment offset” field tells the position of the fragment in the original packet
- DF and MF header bits are also used

Fragmentation example

- Sending a packet of 1900 bytes

- „Original" packet:

  DF=0, MF=0, offset=00000 00000000

- From source to router

  DF=0, MF=1, offset=00000 00000000 (0 =0 /8)
  DF=0, MF=0, offset=00000 10000000 (128=1024/8)

- From router to destination

  DF=0, MF=1, offset=00000 00000000 (0 =0 /8)
  DF=0, MF=1, offset=00000 01000000 (64 =512 /8)
  DF=0, MF=1, offset=00000 10000000 (128=1024/8)
  DF=0, MF=0, offset=00000 11000000 (192=1536/8)

Problems of Dual Address systems

In Network and Data Link Layers two independent address systems (IP addresses and Ethernet addresses) are considered.

- For encapsulation of Data Link Layer (forming an Ethernet frame) the physical address (MAC address) belonging to the IP address has to be determined.
- In certain cases it could be necessary to determine the IP address by the help of Ethernet address.

Network Address –> Physical Address

ARP (Address Resolution Protocol):

- Each node records physical addresses belonging to the network addresses in a table (ARP table).
- How get a new data (pair of addresses) into the table?

1. ARP question:
   Who knows the physical address of the network address X?
2. Each node of subnet receives and processes the frame of the question by a broadcast message.
3. If a node ‘identifies itself’ with network address X, sends an answer to the ARP question with own physical address.

Physical Address –> Network Address

RARP (Reverse Address Resolution Protocol)

- RARP servers stores network addresses of given physical addresses
- Servers replays to (broadcast) queries

BOOTP (BOOTstrap Protocol)

- Its operation is similar to RARP
- It works not just in a broadcast domain
  - using BOOTP relay agents

Physical Address –> Network Address

DHCP (Dynamic Host Configuration Protocol):

- Allows assignment of IP address domain.
- In case of more DHCP servers, the handled address domains should not overlap (in default).
- Clients get the IP address (and other network setup) for a renewable time period.
- If client and server are in different network it uses relay agents.

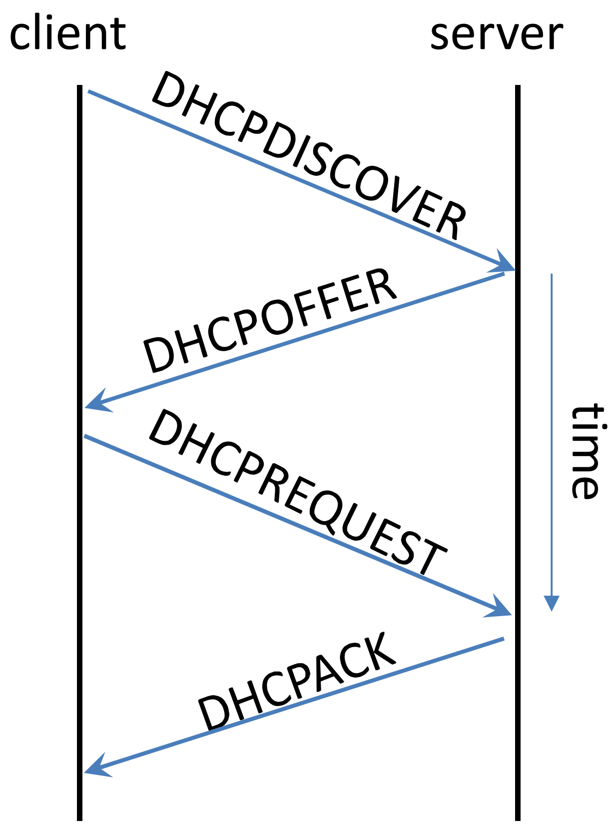
Physical Address –> Network Address

DHCP scheme of functioning :

1. DHCP question: Who can give me an IP address?
2. Each node of subnet receives the frame of the question by a broadcast message.
3. A DHCP servers process the question: If there is a free IP address in the handled address domain, then send an answer to DHCP question with that IP address.
4. The client chooses one from the received DHCP answers, and sends a feedback of its choice to the corresponding DHCP server.
5. The DHCP server books the choice of address (the address became occupied), and confirms client on booking.

Physical Address –> Network Address

DHCP scheme of functioning :



Problems with classful IP networks

- Class A networks are to large, Class C networks are to small, Class B networks are full.

Solutions:

- Private IP domains (e.g. 192.168.0.0/16) with Network Address Translation (NAT)
- Classless IP addressing: the border between network and host ID is shiftable (e.g. netmask 255.240.0.0)
- IPv6, new version of Internet Protocol

IPv6

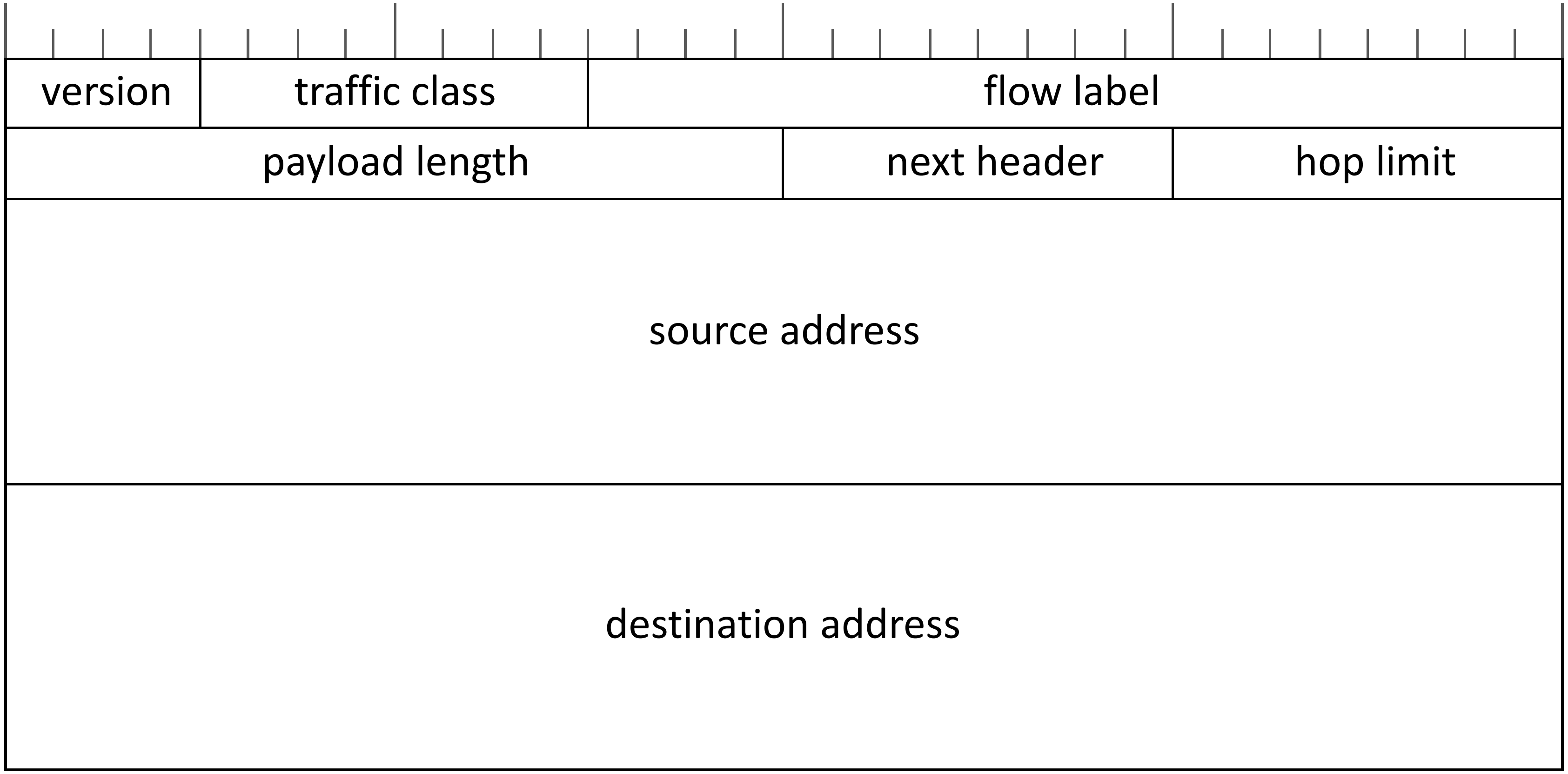
- Continuous lunching (from 1994)
  - Long coexists with IPv4
  - Dual stack (IPv4 vs IPv6)
  - Tunneling (IPv6 inside IPv4)
- 128 bits long addresses
  - Network prefix (first 64 bits)
  - Interface ID (last 64 bits)
- Large address space (approx. 10^{38} address)

IPv6

- Representation: 8 groups of 4 hexadecimal digits
  FE80:0000:0000:0000:32E4:00DF:FE27:8D3F
- Shorter form
  FE80::32E4:DF:FE27:8D3F
- Special addresses
  - 2000::/3 global unicast
  - FD00::/8 local unicast (IPv4 private)
  - FE80::/10 link-local unicast (valid only locally)
  - FF00::/8 multicast
  - ::1 loopback

IPv6

- Header structure (fix 40 bytes)

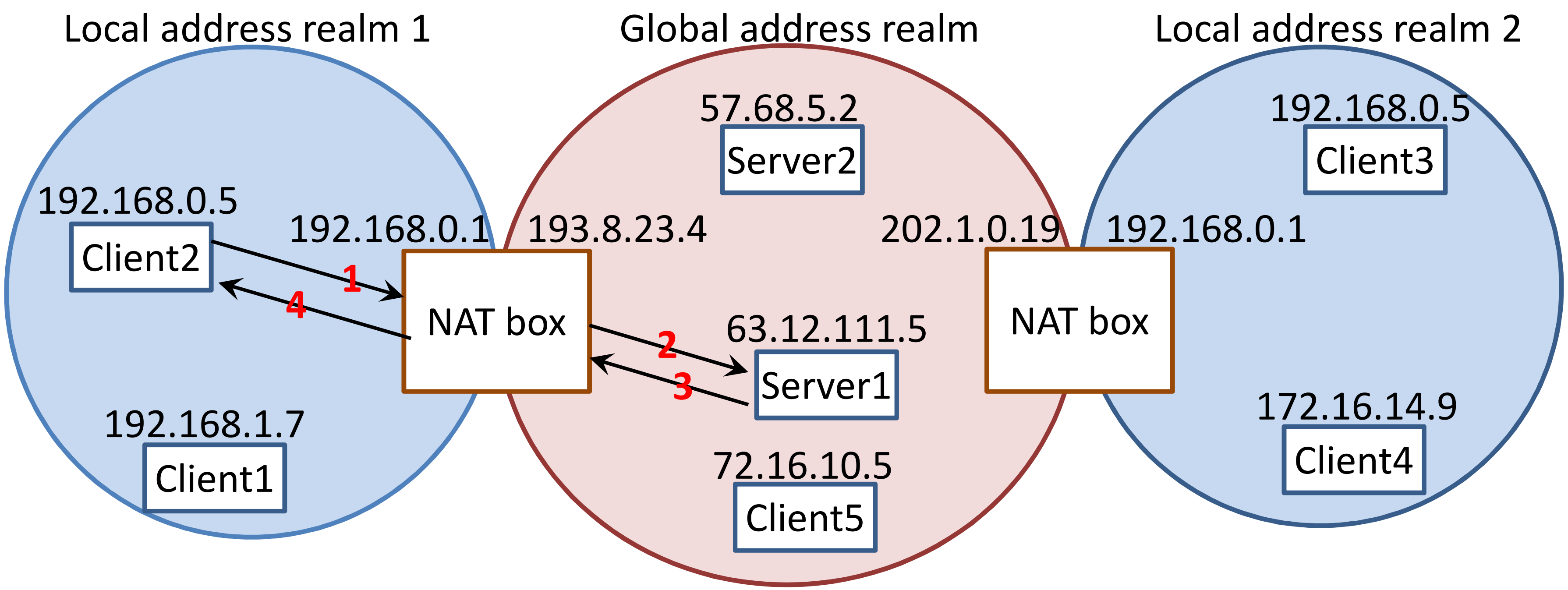


- +Extension headers

Private IP networks

- Network that uses private IP address space
- Commonly used for home and office LANs, when globally routable addresses are not necessary
- Must use a network address translator (NAT)
- Private domains:
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16

Network Address Translation



- 1: Source 192.168.0.5 Destination 63.12.111.5
- 2: Source 193.8.23.4 Destination 63.12.111.5
- 3: Source 63.12.111.5 Destination 193.8.23.4
- 4: Source 63.12.111.5 Destination 192.168.0.5

CIDR

Classless Inter-Domain Routing

Main problem:

We want to divide a network to different sized subnets. (Original subnetting results same subnet size.)

Not the number of subnets is important, but the number of nodes in a given subnet.

IP classes are not so important.

Network-host border can be shifted.

The result depends on the arriving time of demands.

IP subnets

Why is it necessary to create subnets?

- The logical functionality of the institute can be a reason.
- On an IP network more than one broadcast domains (usually with the same size) have to be created.

How can we create a subnet?

- Some of the higher position bits of host ID of an IP address will be used identifying the subnet.
- The new network-node boundary is denoted with the network mask (longer prefix is used).

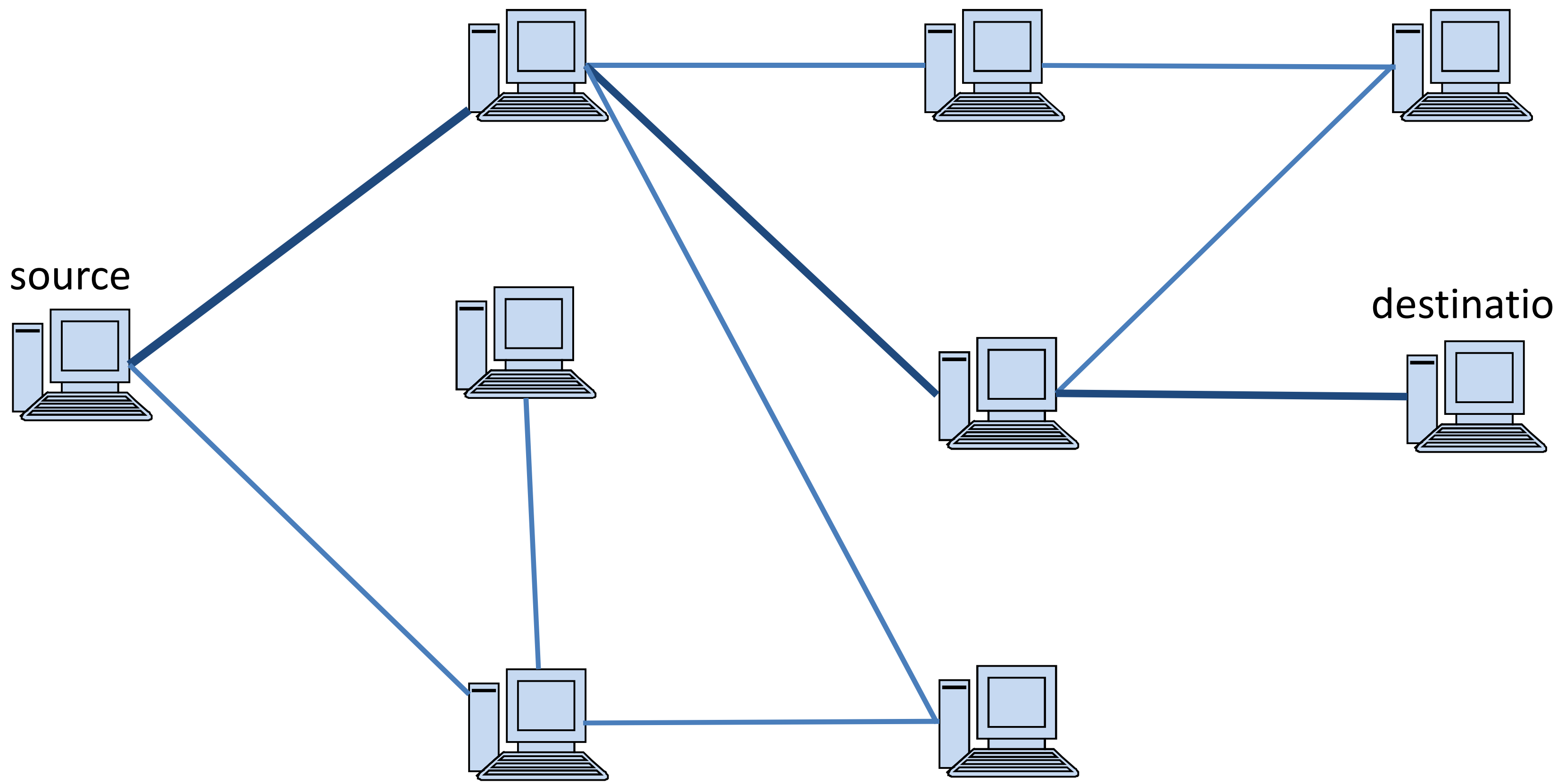
ICMP

Internet Control Message Protocol (RFC 792)

- Implemented together with IP
- When an unexpected event happens it is reported by ICMP messages
- Encapsulated into IP packet (8-bytes header)
- Several network utilities based on ICMP
- Examples:
  – Destination unreachable (routing)
  – Time exceeded (TTL)
  – Echo request (ping)
  – Echo reply (ping)

Routing

- How to find the destination?



Routing table

Each node have a „list” about its (direct) connections and knows who is the „best informed” of them.

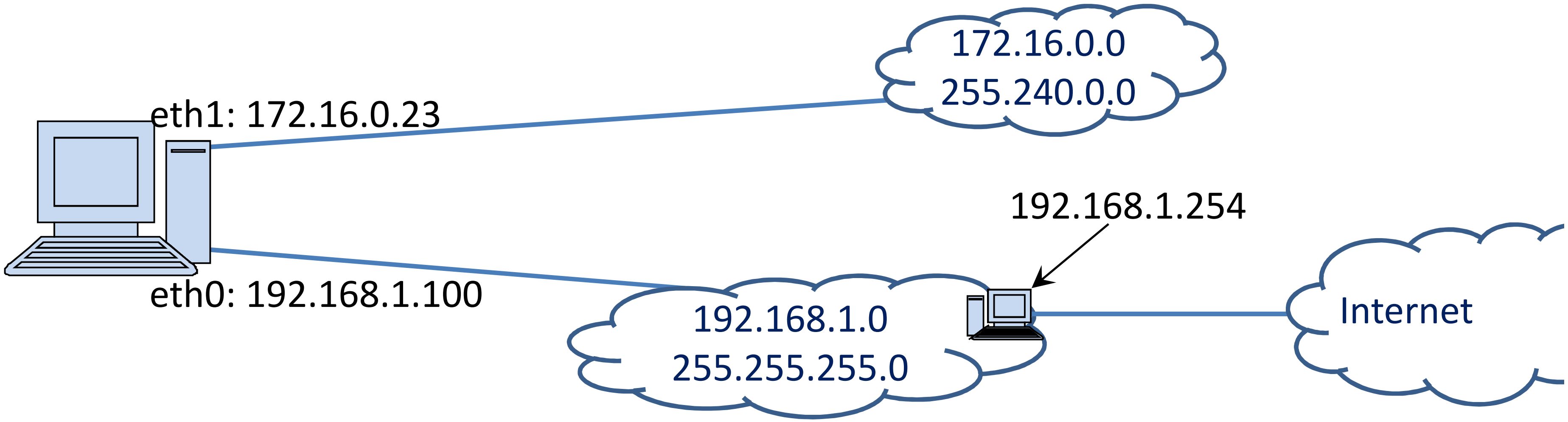
This „list” is called **routing table**.

The „best informed” node in a network called **default gateway**.

If a node wants to send a packet to an other, it searches for the destination in its connection list. If it is in the list, the sender can know how to reach it, else it sends the packet to default gateway (as a next hop) maybe it can forward the packet to the addressee.

Routing table example

Computer with 2 network interfaces



Destination Network ID	Gateway	Netmask (genmask)	Interface
192.168.1.0	0.0.0.0	255.255.255.0	eth0
172.16.0.0	0.0.0.0	255.240.0.0	eth1
0.0.0.0	192.168.1.254	0.0.0.0	eth0

Routing process

How the routing works in case of sending to an given IP:

- *Step 1*: See the first row of routing table.
- *Step 2*: Make AND operation between the given destination IP and the netmask in the row.
- *Step 3*: If the result equal to Network ID in the row, send the packet on your interface written at the end of row. (If gateway given send to the gateway, else directly to destination on the link.) Ready.
- *Step 4*: Otherwise see the next row (if exists) and go to *Step 2*. If no further row stop with error.

Routing example

Sending a packet to 193.6.128.5. Via which interface?

First row	193. 6.128. 5	
	& 255.255.255. 0	
	193. 6.128. 0	≠ 192.168.1.0
Second row	193. 6.128. 5	
	& 255.240. 0. 0	
	193. 0. 0. 0	≠ 172.16.0.0
Third row	193. 6.128. 5	
	& 0. 0. 0. 0	
	0. 0. 0. 0	= 0.0.0.0

Send the packet to gateway 192.168.1.254
(this is the **next hop**) via the interface eth0 (192.168.1.100).

Maintenance of routing tables

Static (nonadaptive) routing

- The routing tables are treated by the system administrator (root).

Dynamic (adaptive) routing

- Routers automatically change information between each other to update their routing tables.
  - Internal: finding optimal route
  - External: finding trusted route

Routing concepts

- Autonomous system: Administrative routing unit with same routing strategy
- Metrics: Describes the quality of routes (distance, cost, bandwidth)
- Routed protocols: General protocols controlled by routers (IP, ICMP, etc.)
- Routing protocols: Controls the routing process
  - Distance vector routing: RIP, EIGRP, BGP
  - Link-state routing: OSPF, IS-IS, etc.

Distance Vector Routing

Operation:

- Routers store the shortest distance to all nodes and the next node on the shortest path
- Routers exchange this information between neighbors periodically and automatically
- Routers check (based on the new information) whether there is better path than the stored one.

Examples:

- RIP, EIGRP, etc.

Mathematical background

- Direct cost (distance)

$$d(i,j) = \begin{cases} cost, \text{ if } i \text{ and } j \text{ in the same network} \\ \infty, \text{ otherwise} \end{cases}$$

- Distance on the shortest path

$$\mathrm{D}(i,j) = \begin{cases} 0, \text{ if } i = j \\ \min\limits_{k}\{d(i,k) + D(k,j)\}, \text{ otherwise} \end{cases}$$

where k runs over the neighbors of i

Composition of routing table

- Initial state: $D(i,j) = \begin{cases} 0, if\ i = j \\ \infty, otherwise \end{cases}$

  All i node knows *d(i,k)* to all *k* neighbors.

- Algorithm (Bellman-Ford):

1. All *i* node get *D(k,j)* from *k* neighbors.
2. Node *i* calculates *D(i,j)* based on Step 1.
3. If the new *D(i,j)* smaller then its previous value store it and the shortest path to *j* goes through *k*.
4. Continue at Step 1.

After finite iteration we get the optimal routes.

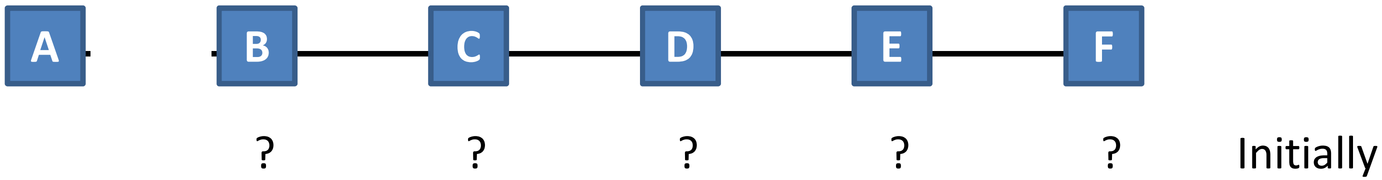
Problems with DV-routing

- Count to infinity:
  The method slowly respond to topological changes. After any change in the network longer time needed to find the optimal path.
- Too small initial value:
  If optimal path damaged available longer path can’t overwrite it.
  Solution: longer distance arrives from the direction of optimal path overwrite it.

Examples of problems

Slow convergence (after turn on)

- How far is router 'A' from a given router?

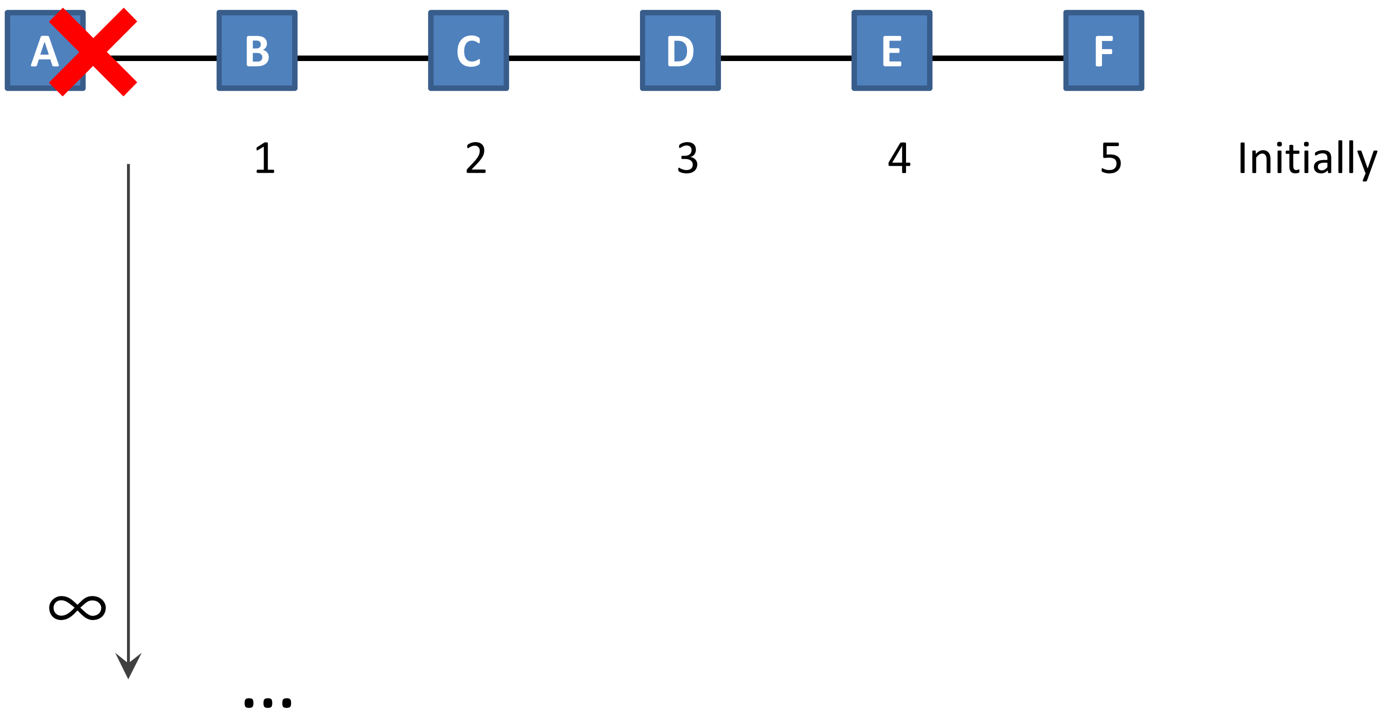


Several exchange needed to discover changes.

Examples of problems

Count to infinity (after break down)

- How far is router 'A' from a given router?



Never said: 'A' unreachable

RIP

Routing Information Protocol (RFC 1058)

- Distance vector based internal routing protocol
- Old, but continuously developed
- Maximum 15 router long paths
- Information sending in each 30 seconds
- If topology has changed immediate sending
- The second version (RIP v2) is CIDR compatible

EIGRP

Enhanced Interior Gateway Routing Protocol

- Developed and used by CISCO
- Routing update in every 90 seconds
- CIDR compatible
- Default metric is bandwidth
- Other metrics: delay, MTU, reliability, load
- Stores potential substitute paths

Link-state routing

Operation:

1. Discover neighbors
2. Measuring the cost of accessing neighbors
3. Composing packets from measure results
4. Sending the packet to all routers
5. Routers knows the topology and can calculate the optimal paths to all other router (by **Dijkstra's algorithm**)

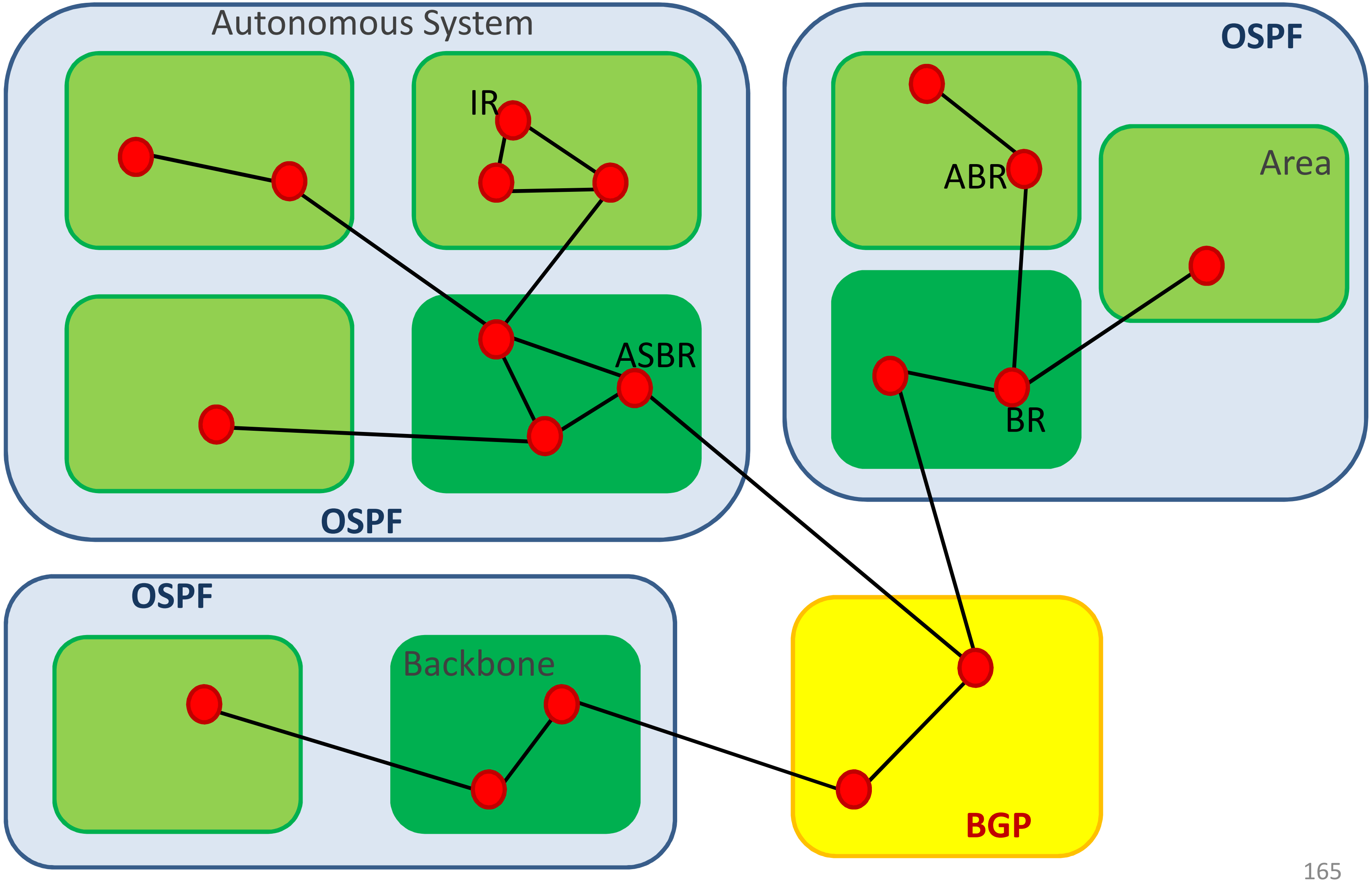
Example: OSPF, IS-IS

OSPF

Open Shortest Path First

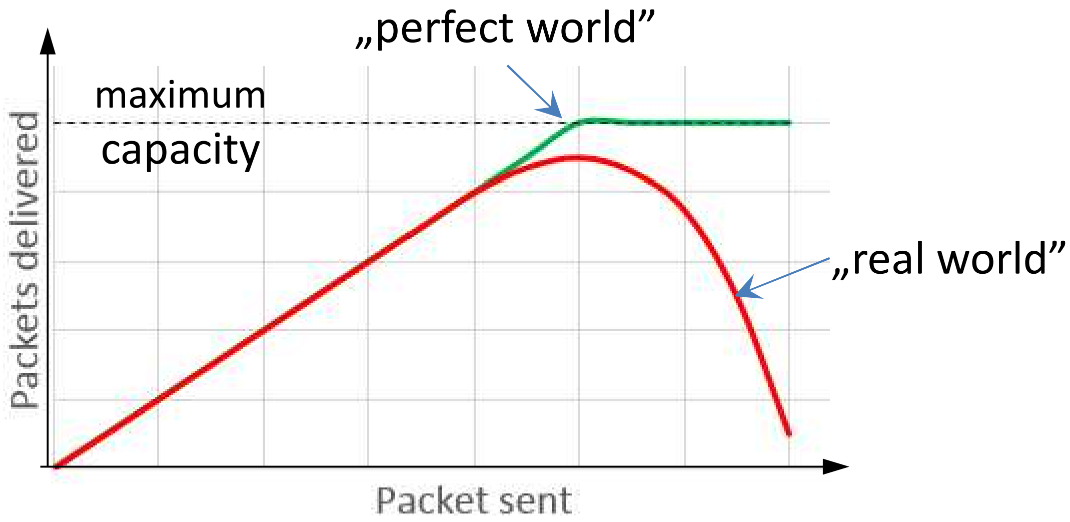
- Link-state interior routing
- Default from 90’s
- Use ‚areas’ (smaller units than AS)
- Different classes of routers:
  – IR: Internal Router (inside area)
  – ABR: Area Border Router
  – BR: Backbone Router
  – ASBR: Autonomous System Boundary Router
- Multipath routing

OSPF


Autonomous System
IR
ASBR
OSPF
OSPF
ABR
Area
BR
OSPF
Backbone
BGP

Congestion control

- If too many packets are present in the subnet the performance degrades.
- Network layer have to manage this situation
  - Several algorithm is used
- Different of flow control in data-link layer



QoS

Quality of Service

- Different services have different requirements

services/needs	**Reliability**	**Delay**	**Jitter**	**Bandwidth**
E-mail	High	Low	Low	Low
Web access	High	Medium	Low	Medium
Audio stream	Low	Low	High	Medium
Video stream	Low	Low	High	High
Telephony	Low	High	High	Low
Video conference	Low	High	High	High

- Solutions: buffering, resource reservation, traffic shaping, leaky bucket, etc.

Transport layer

Transport layer

Fourth layer of hybrid model (L4)

Reliable connection between software on two nodes. Protocols may connectionless or connection-oriented.

Topics

- Error detection/correction
- Order guarantee
- Identifying programs on a node
- Flow control
- etc.

Port

Problem:

- IP address (and DNS name) identifies the node only.
- A node has more different connections, it executes more network applications.
- A program has to know which segment (data unit in L4) belongs to it

Solution: **port**

- It identifies network programs or services on a node.
- It is a 16bits long number in decimal form.
- Range: 0 - 65535

Port

Range: 0 – 65535 (since it is 16bits long)

- **Well-known ports**: 0 – 1023
  Used by system processes that provide widely used types of network services
- Registered ports: 1024 - 49151
- Private ports: 49152 – 65535
  Used freely

Stored in files:

- linux: /etc/services
- windows: C:/WINDOWS/system32/drivers/etc/services

Well-known ports

- 21: **FTP** (File Transfer Protocol)
  used for down/up loading files
- 22: **SSH** (Secure SHell)
  used for secure login to remote computer
- 25: **SMTP** (Simple Mail Transfer Protocol)
  used for e-mail routing to mail servers
- 53: **DNS** (Domain Name System)
  used for eg.: www.unideb.hu → 193.6.128.25
- 67: **DHCP** (Dynamic Host Configuration Protocol)
  automatic network configuration of host

Well-known ports

- 80: **HTTP** (HyperText Transfer Protocol)
  used by web browsers
- 110: **POP3** (Post Office Protocol v3)
  used for downloading e-mails from servers
- 143: **IMAP** (Internet Message Access Protocol)
  used for downloading e-mails from servers (newer)
- 443: **HTTPS** (HyperText Transfer Protocol over SSL)
  used by web browsers for secured sites
- 995: **POP3** (Post Office Protocol v3 over SSL)
  used for secured downloading e-mails from servers

Transport layer protocols

UDP: User Datagram Protocol

- Connection free
- Non-reliable

TCP: Transmisson Control Protocol

- Connection based
- Reliable

UDP

- The UDP (User Datagram Protocol) is the connection free transport protocol of the TCP/IP protocol set.
- Transmission of datagrams without any guarantee (without confirmation).
- Failure management is to higher level (applications) protocols.
- The UDP protocol is suitable for applications which do not need to concatenate sequences of segments. E.g. DHCP, DNS .
- Short header, fast transmission.

TCP

- The TCP (Transmission Control Protocol) is the connection based transfer protocol of the TCP/IP protocol set. It provides a reliable (receipted) bit stream for applications.
- Before starting data transmission, the two nodes build up a TCP connection (Three-way handshake).
- The destination node receipts the segment(s).
- If a segment is missing, the TCP protocol ensures retransmission of the missing segment.
- Long header, slow transmission.

Headers

UDP:

Source port number	Destination port number
Length (byte)	Checksum

TCP:

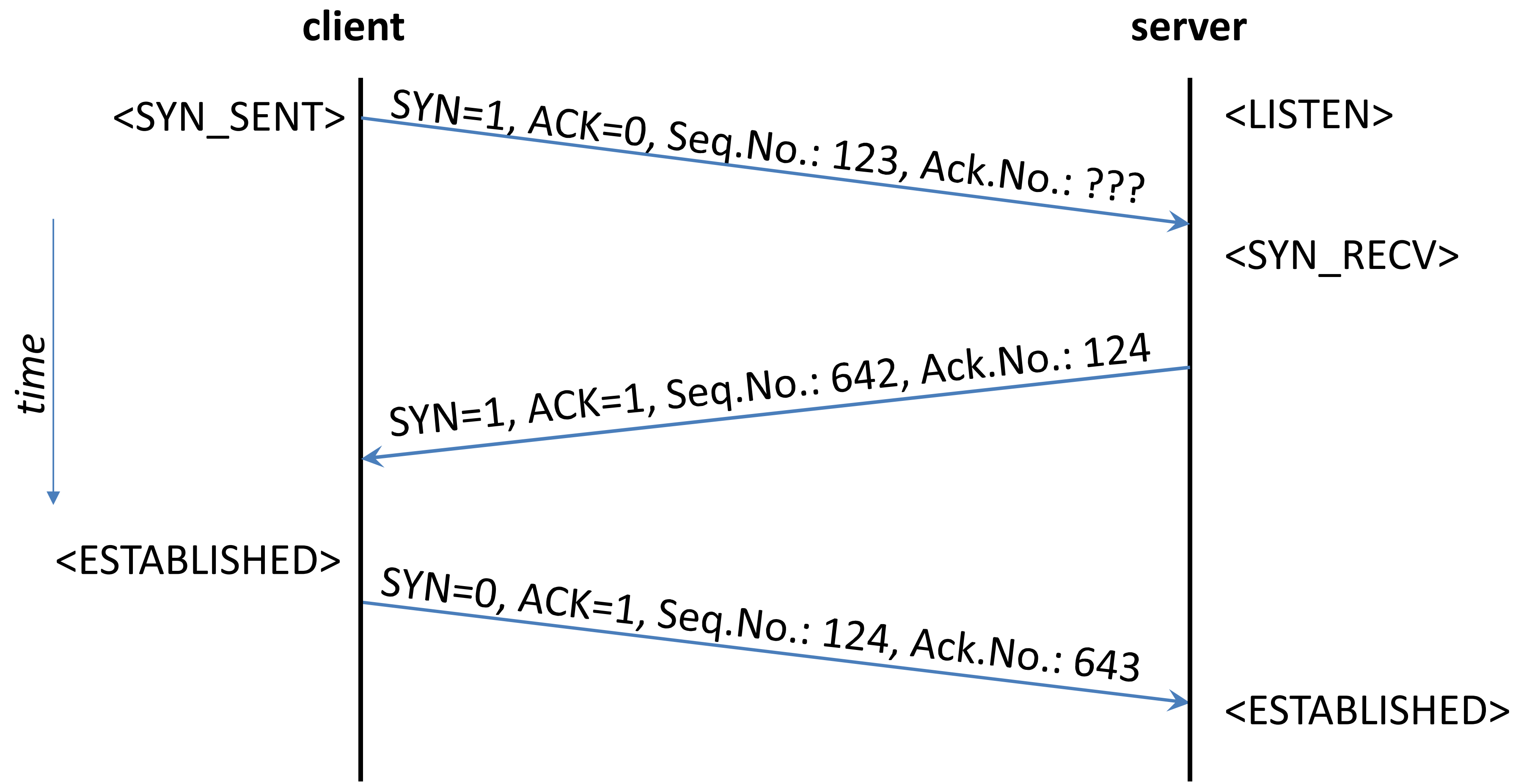
<table>
<tr><td colspan="8">Source port number</td><td colspan="2">Destination port number</td></tr>
<tr><td colspan="10">No. of sequence (SEQ No.)</td></tr>
<tr><td colspan="10">No. of acknowledgement(ACK No.)</td></tr>
<tr><td>Data Offset</td><td>Reserved</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td colspan="2">Window size</td></tr>
<tr><td colspan="8">Checksum</td><td colspan="2">URG pointer</td></tr>
<tr><td colspan="9">Options</td><td>Filling</td></tr>
</table>

Three-way handshake

TCP need to create a connection (session) before transmission, in 3 steps:

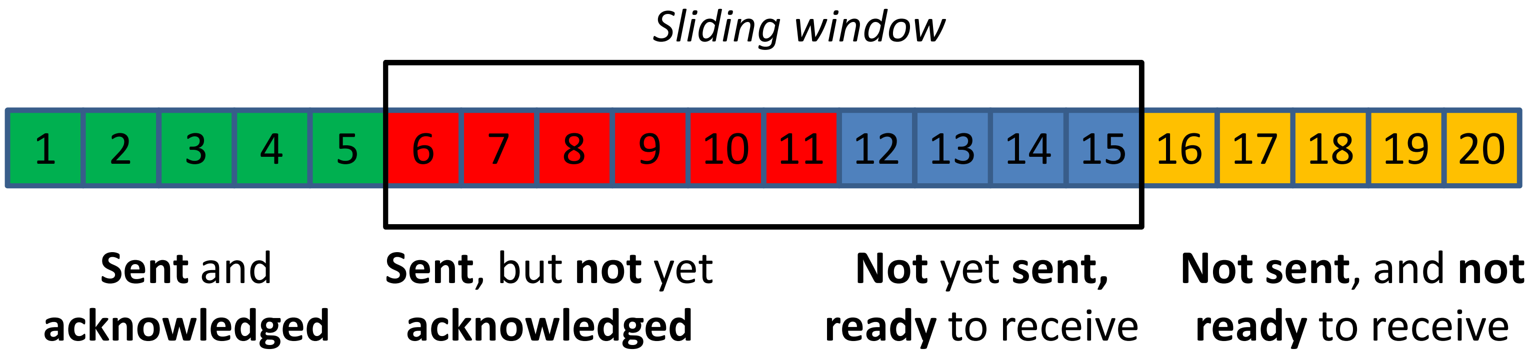
1. Client to Server: (SYN)
   „I want to talk with you."
2. Server to Client: (SYN, ACK)
   „Ok, I am ready to talk with you."
3. Client to Server: (ACK)
   „Ok, I have heard that you are ready to talk with me"
4. Client to Server:
   „I want to say that…"

Three-way handshake

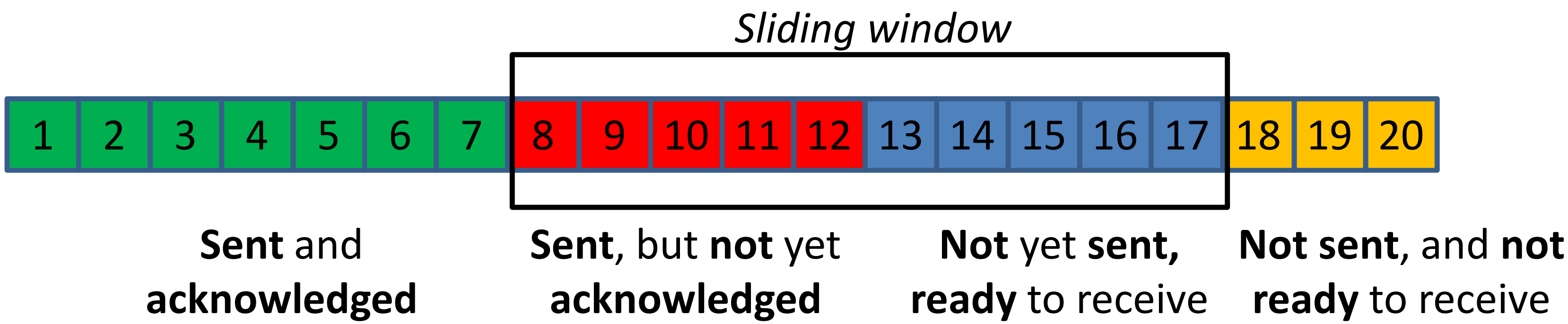


Sliding window

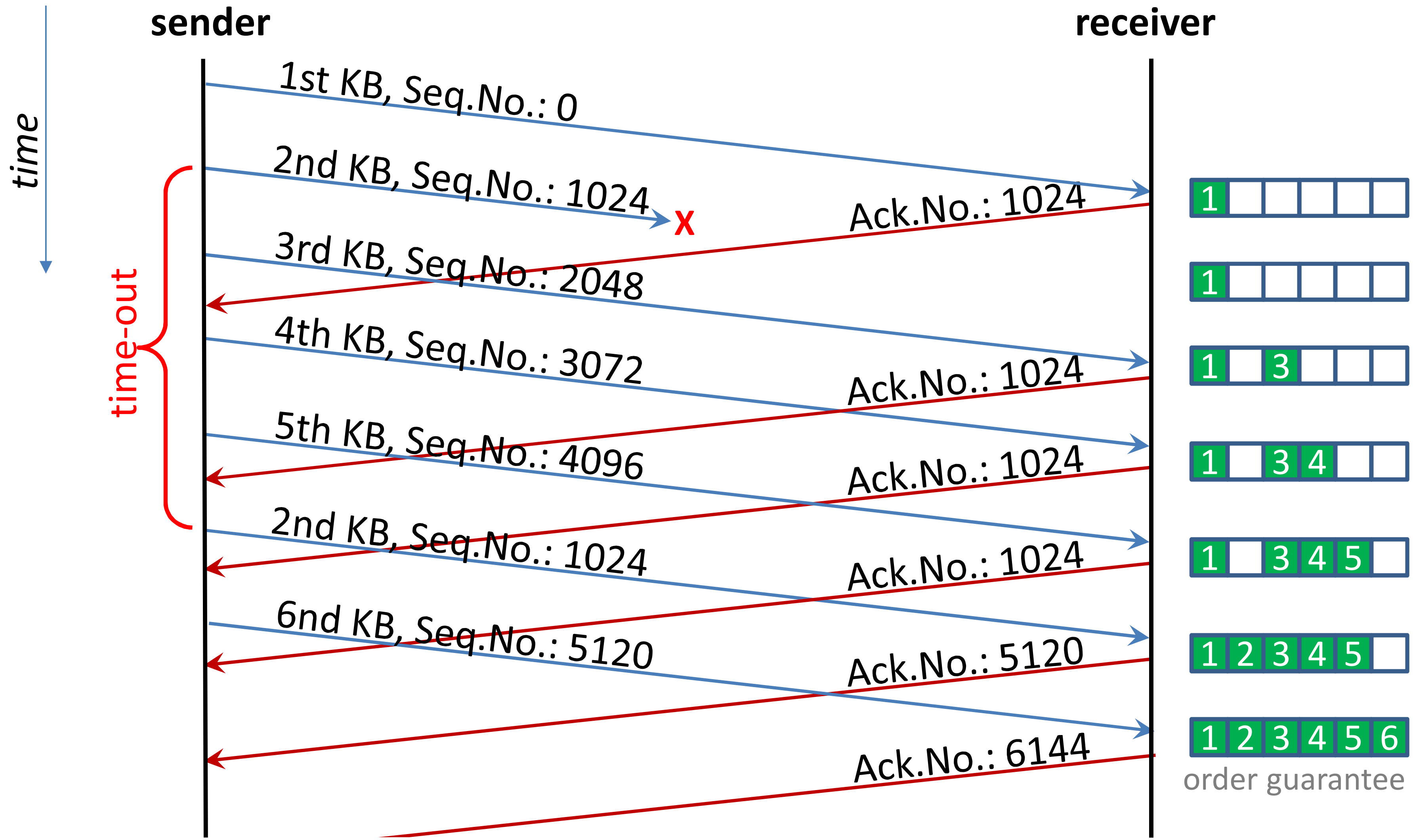
Sender: 11 sent and 5 receipted TCP segments, window size 10



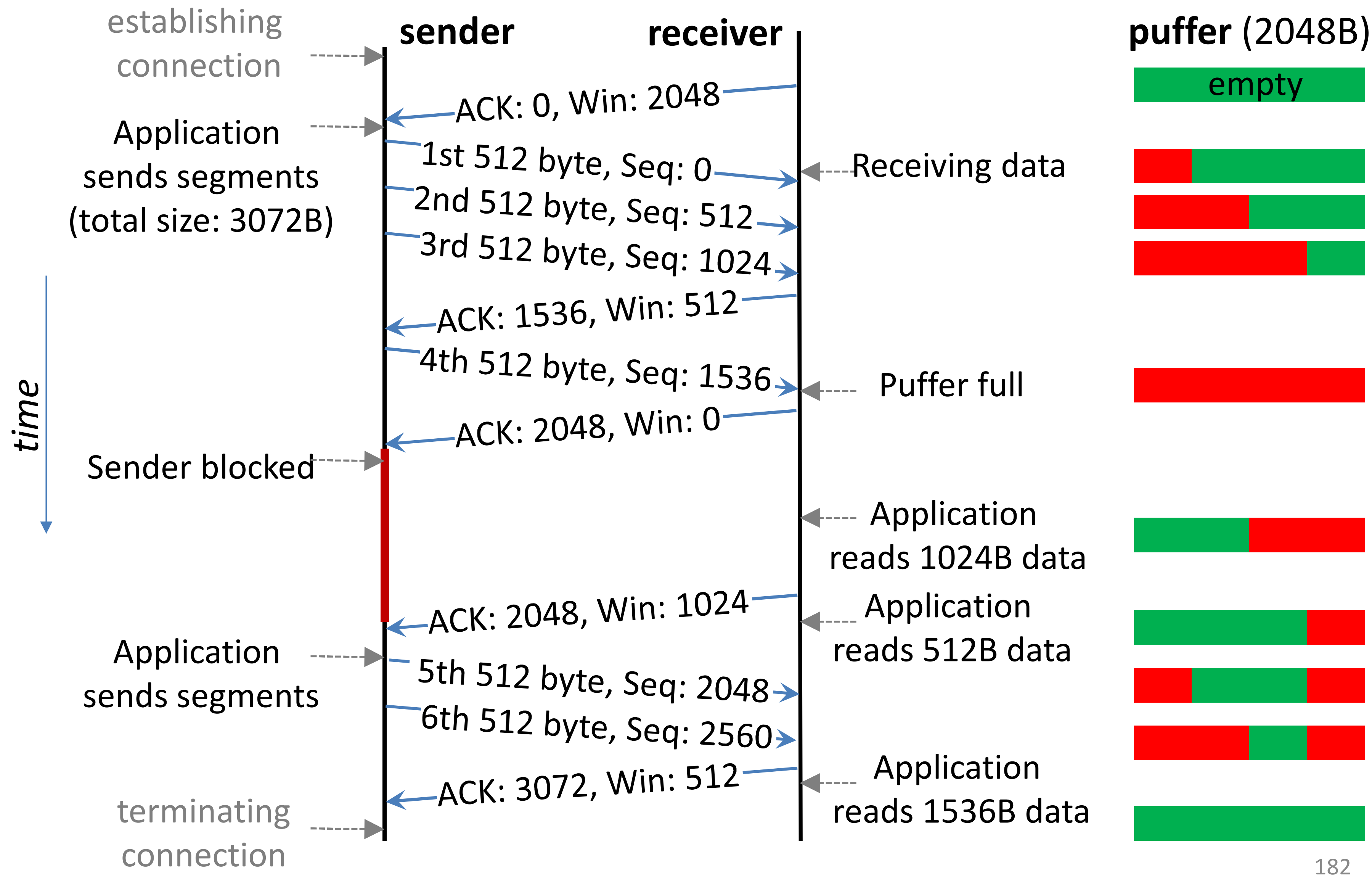
Sender: 12 sent and 7 receipted TCP segments, window size 10



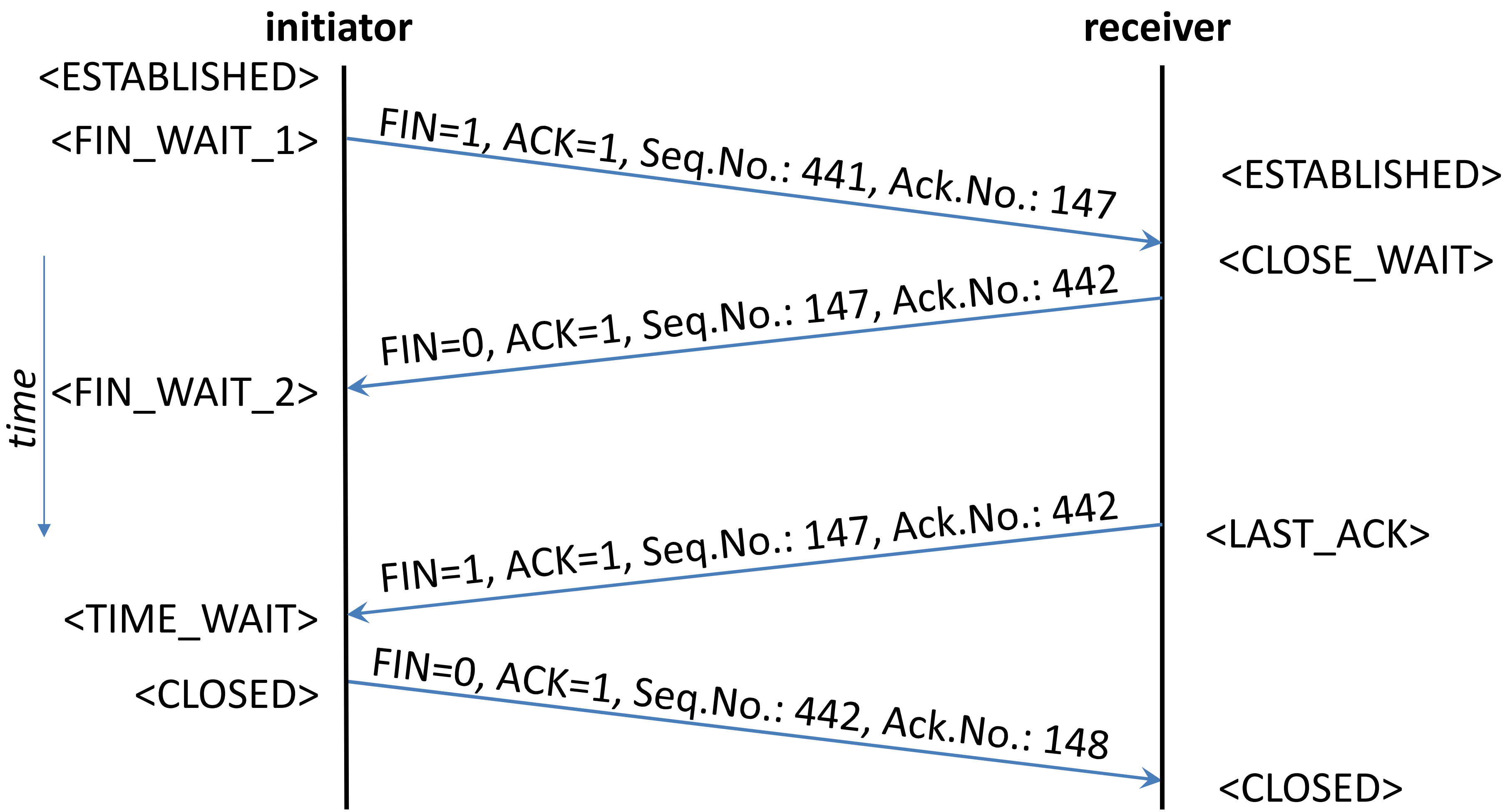
Lost segment retransmission



Flow control



Connection termination



Use of TCP and UDP

TCP is used when the reliability is important

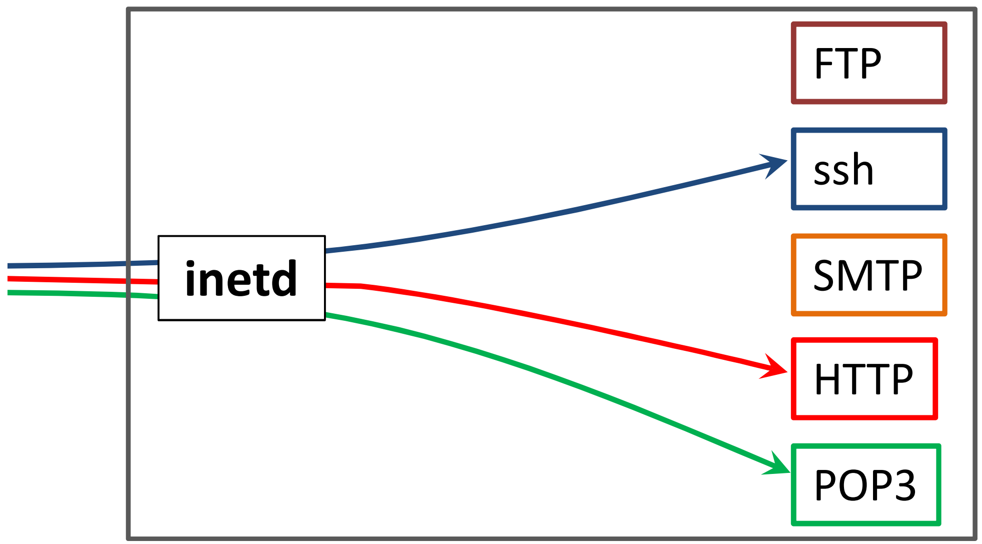
- We nees all bytes precisely even if the speed is slow
- Eg: downloading file, browsing web, reading email

UDP is used when the speed is important

- We need fast, continuous transmission even if some segments are lost.
- Eg: IP phoning (eg: Skype), watching live video

Super-server: inetd

- If all server programs (daemons) always listen to packet, it is not efficient (too much processes).
- Incoming packets first goes to *inetd*
- *inetd* decide which server program belongs to this packet (based on port number).
- *inetd* launches the *demon* (servicing program), delivers the packet.



Access control

tcpd: Access control for internet services

Operation

- Request arrives
- The i*netd* launches *tcpd*, not the service daemon
- The *tcpd* logs the request
- It checks the rights
  - by pattern-based access control configuration files
- Either starts the requested daemon or don’t respond

Configuration and commands

- /etc/protocols
- /etc/services
- /etc/inetd.conf
- /etc/hosts.allow, /etc/hosts.deny
- telnet
- netstat
- nmap
- netcat (nc)

Application layer

Application layer

Top layer of OSI and TCP/IP models.

Interface between network and users.

Ensures the communication required by the users.

Contains protocols needed by end users.

Main topics

- Domain names (DNS)
- World Wide Web (www, HTTP, HTML, URL)
- E-mail (SMTP, POP3, IMAP)
- File transfer (FTP, BitTorrent)
- etc.

Network addresses and hostnames

Problem:

- Users like alphabetical names (texts) instead of numbers.
- Computers identify each other by IP address (which is numerical information).
- Need of decupling names and network addresses.

Solution:

- Mapping IP addresses to names
  - Central `hosts.txt` file (ARPANET)
  - **Domain Name System** (DNS)

Domain Name System

- **Hierarchical, domain-based naming scheme**
- **Implemented in distributed database system**
- **Client-server architecture**
- Decentralization and scalability
- Platform independence
- General purpose realization
  - Support latter applications
- Specified in RFC 1034 and RFC 1035 (etc.)
- In use since 1980s
- E.g.: www.unideb.hu ⟷ 193.6.128.25

Components of DNS

Domain namespace and **resource record**s

- The names and information about them.
- Nodes of the graph represents resources.

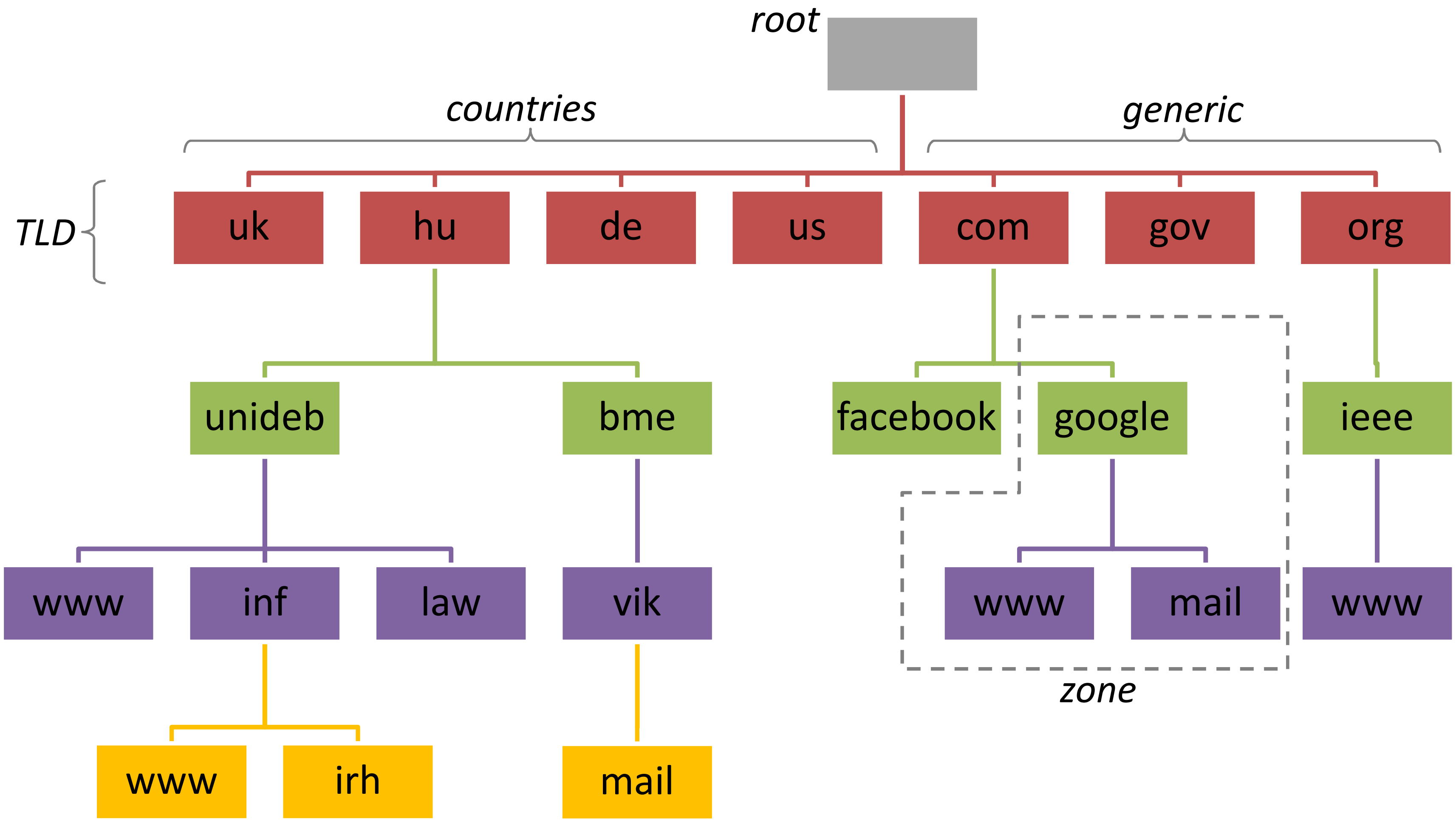
Name servers

- Store resource records.
- Answers queries.

Resolver applications

- Ask name servers,
  for example if IP address is needed, but a name is given.

Domain Namespace



Domain Namespace

Tree graph, where each node represents a set of resource (e.g. computer).

Each node has a **label** (a kind of name).

- Subset of ASCII (a-z, A-Z, 0-9, -)
  - Internationalized characters (Punycode)
- Max length of labels is 63 characters.
- No case sensitivity.
- No equal labels with same parent node.
- Label of root is a string with length 0 (null label).

Domain Namespace

Fully Qualified Domain Name (FQDN)

- Nodes can be identified by the series of labels from the node to the root.
- Absolute domain name.
- User representation (max 253 characters):
  `irh.inf.unideb.hu.`
- Binary representation (max 255 bytes):
  `3irh3inf6unideb2hu0`

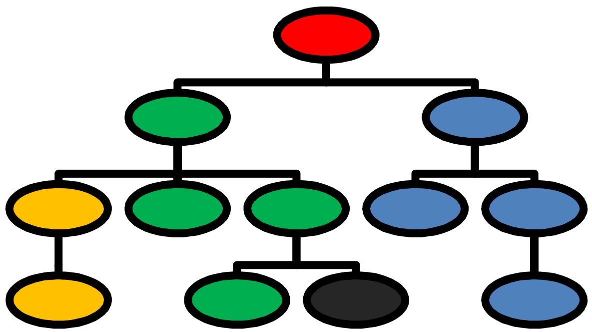
Partially Qualified Domain Name

- Relative domain name.

Domain Namespace

Zone

- Administrative unit of domain namespace.
- A contiguous sub-graph
  - – May consist of a domain and sub-domains.
- Zones does not overlap.
- Belongs to organizations/institutions responsible for a set of domain names.
- Contains name servers.
- Referred by its ‚highest' domain name.



Reverse lookup

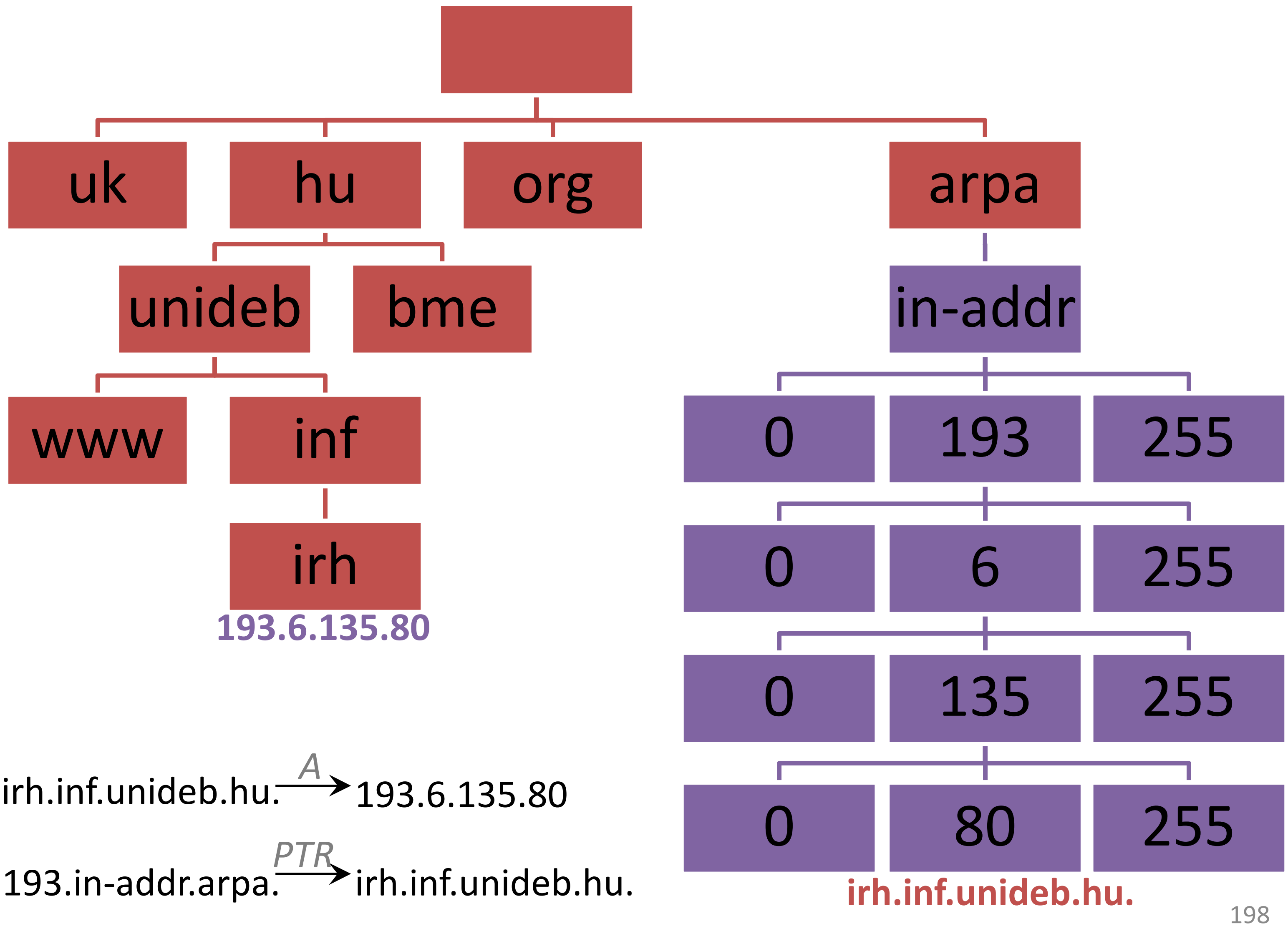
The namespace has a special subgraph

- under the in-addr.arpa. domain.
- for mapping IP to domain name.
- its subdomains belongs to bytes of IP addresses.
- its Resource Records contains domain names (PTR).

Example:

- 25.128.6.193.in-addr.arpa. refers to the domain name of node has IP address 193.6.128.25 (www.unideb.hu)

Reverse Namespace



irh.inf.unideb.hu. $\xrightarrow{A}$ 193.6.135.80

80.135.6.193.in-addr.arpa. $\xrightarrow{PTR}$ irh.inf.unideb.hu.

Resource Record

A domain name specify a node of the graph.

A node related to resource set.

Information resources are stored in resource records.

Resource records (RR) stored in **zone file**.

The order of RRs is not important.

Examples of resource records:

- What is the IP address of a computer given by name?
- Which computer is a name server in a zone?
- Which computer is a mail-exchanger?
- etc.

Resource Record

Structure:

`[domain_name] [TTL] [class] type data`

- domain_name: domain to which this record applies
- TTL: how ‚stable' is the record (or validity in seconds) volatile → low value, quasi constant → high value
- class: practically always IN (Internet)
- type: what kind of information is stored in data field
- data: value with type specific format/content

In case of blank optional field last record or zone file directives are used.

Resource Record

Frequently used RR types:

- `SOA`: authoritative information about the zone
- `NS`: authoritative name server of the domain
- `A`: network address of the domain (hostname)
- `AAAA` : IPv6 address of the domain
- `MX`: mail exchanger (or MTA) of the domain
- `CNAME`: alias name of the canonical domain
- `HINFO`: info about the host hardware/operating system
- `PTR`: pointer to reverse DNS lookup
- `TXT`: arbitrary human-readable text about domain

Resource Record

Values of different types:

- `SOA`: complex record
  (primary name server, email of responsible person, serial number, timing details of refreshing)
- `NS`: domain name of a host
- `A`: IPv4 address (if class is IN)
- `AAAA` : IPv6 address of the domain
- `MX`: priority and a domain name of mail server
- `CNAME`: a (canonical) domain name
- `PTR`: domain name of a host

Example zone file

```
$TTL                43200               ;default TTL
$ORIGIN             example.org.        ;base name
@  IN    SOA        dns1.example.org.              root.example.org. (
   2009100501       ; serial <2009-Okt-05, update 1>
   86400            ; refresh <1 day>
   3600             ; retry <1 hour>
   1209600          ; expire <2 weeks>
   10800 )          ; minimum TTL <3 hours>
example.org.        86400   IN      NS      dns1.example.org.
example.org.        86400   IN      NS      dns2.example.org.
example.org.        86400   IN      MX      10      mail.example.org.
dns1.example.org.           IN      A       192.168.0.1
dns2.example.org.           IN      A       192.168.0.2
mail.example.org.           IN      AAAA    2001:503:ba3e::2:30
server.example.org.         IN      A       192.168.0.4
host.example.org.           IN      A       192.168.0.101
e2.example.org.             IN      A       192.168.0.102
ftp.example.org.            IN      CNAME   server.example.org.
```

Resolver

A software, which means interface between user network applications and name servers.

Client side of the DNS (usually platform dependent).

If a program needs IP address but domain name is given address resolver do the address mapping.

It sends a request to name server and gives the reply based on resource records to the user application.

Results:

- an RR-based answer (www.unideb.hu →193.6.128.25)
- name error
- data not found

Name server

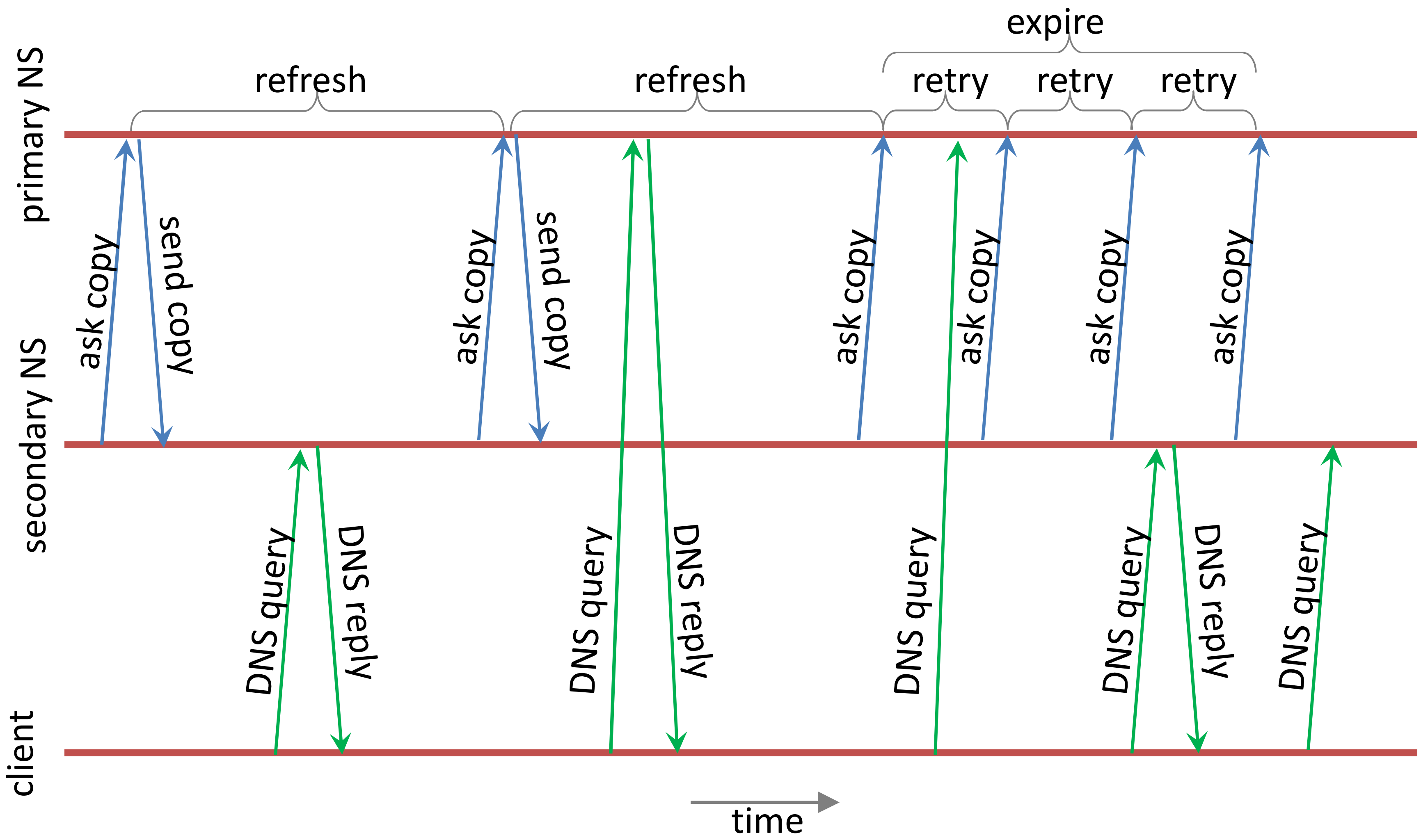
The name server is a software on a computer, which

- stores resource records of a zone (zone file)
- knows connections to neighboring zones
- temporarily stores some RRs of other zones
  - **Cache**: based on TTL fields of RRs
- replies to resolver query.

Each zone has name servers

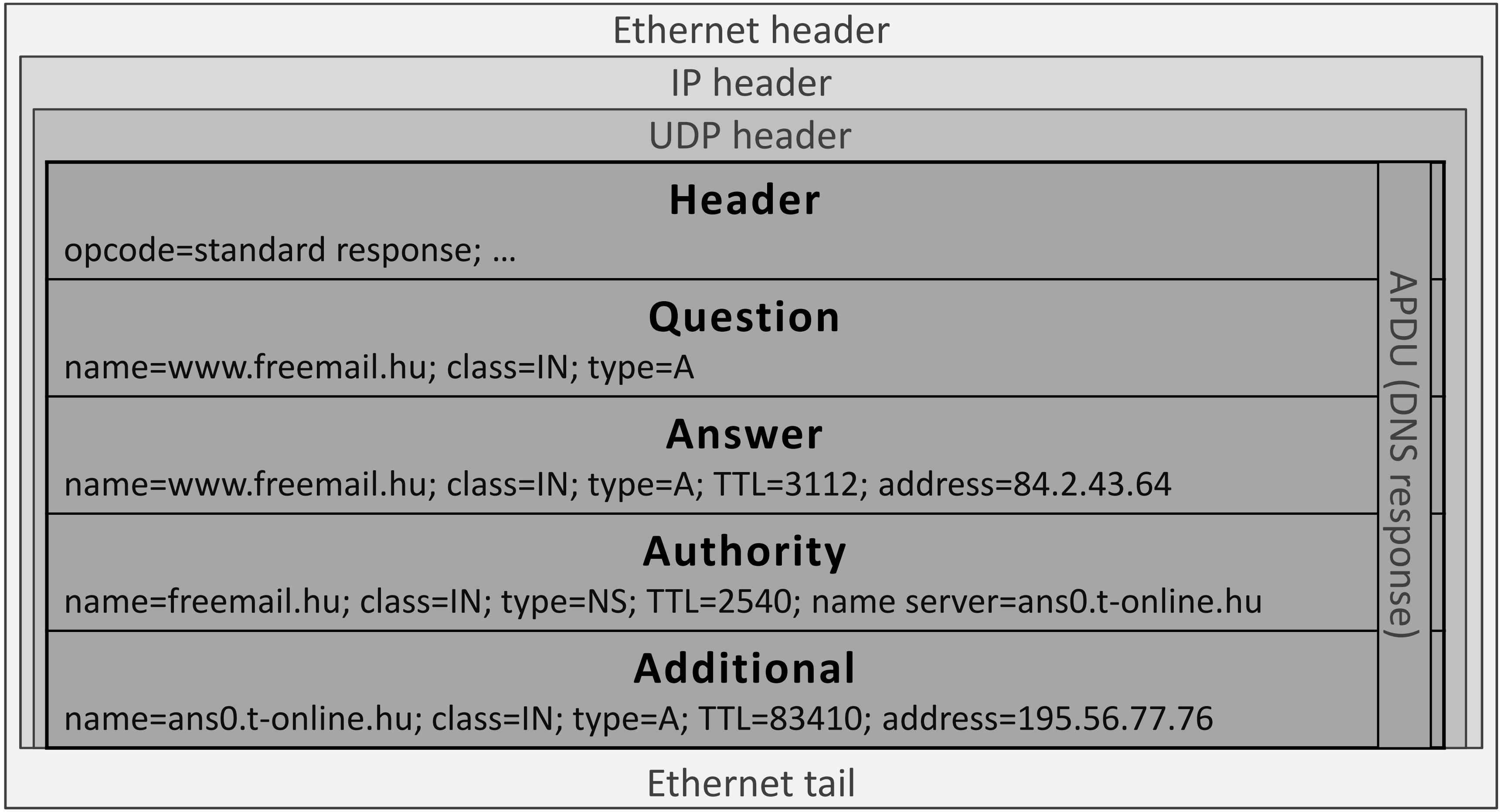
- **primary** name server
  authoritative zone file managed by administrator
- **secondary** name server
  automatic copy from primary NS (see SOA record)

Primary and secondary servers



Query

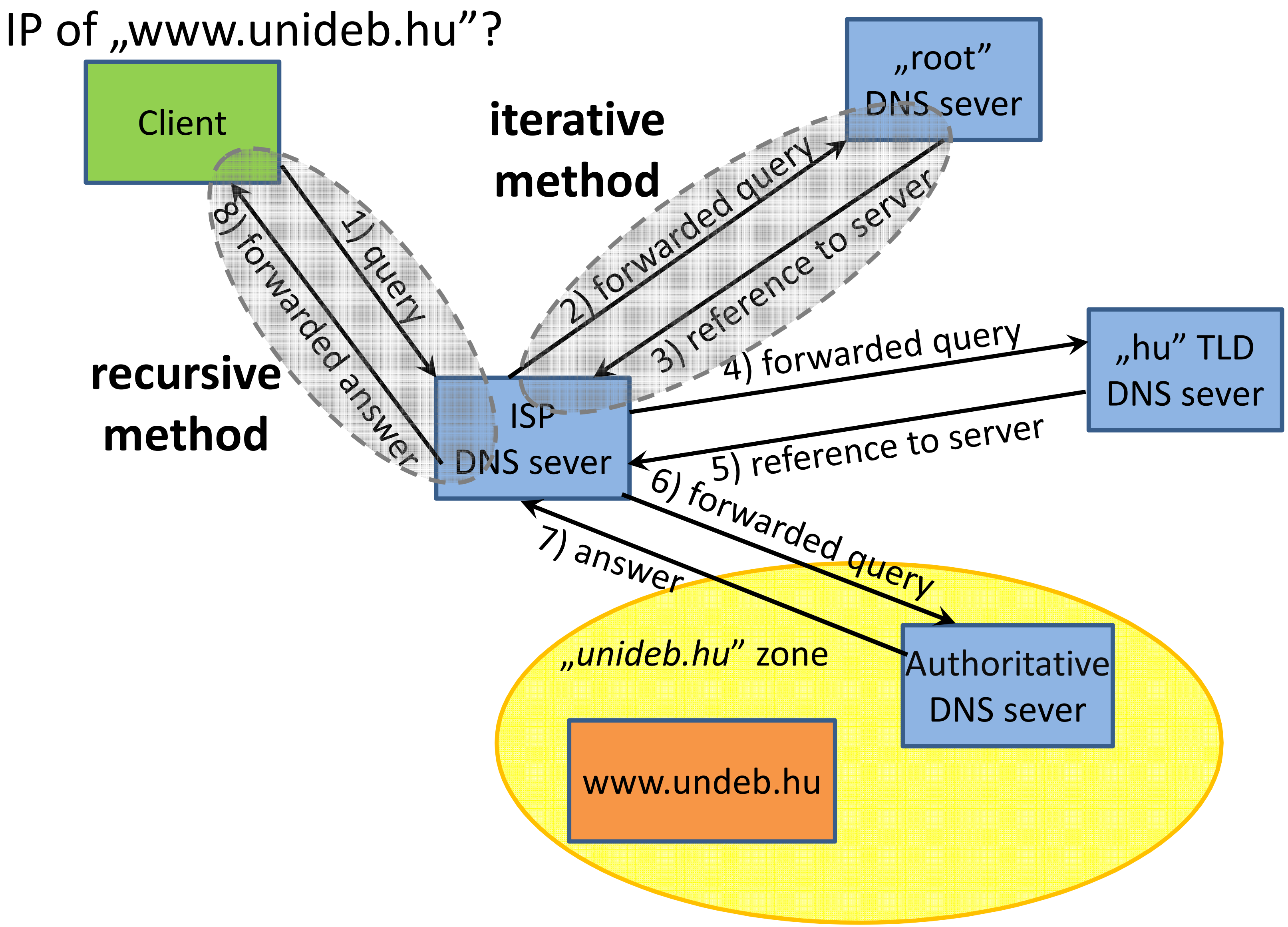
- Structure of query and answers are the same



DNS lookup process

- Client's resolver asks the name server
  (send a query in UDP segment, destination port 53)
- Server looks for answer
  - in temporary memory (cache)
  - in own Resource Records
  - ask other servers
    - Iterative query
    - Recursive query
- Other servers' answer is stored in cache for a while
- Name server response to client

Iterative and recursive query



Iterative and recursive query

Iterative method

- Easy implementation on server
- Implemented on all name server
- Answer can be a reference to other servers

Recursive method

- Easy implementation on client
- Must be implemented on both side
- Special flag bits in query/response header
- Answer allways the asked information (or error)

Configuration and commands

- **`/etc/hosts`**
  `192.168.0.23    RedLaptop`
- **`/etc/nsswitch.conf`**
  `host:  dns  files`
- **`/etc/resolv.conf`**
  `domain       unideb.hu`
  `nameserver 193.6.128.5`
- **`nslookup`**
  - Interactive mode
  - Non-interactive mode
- **`host`**

World Wide Web

The most widely used and most quickly spreading part of Internet.

Concept: Tim Berners-Lee (CERN, 1989)

We can navigate among **website**s by hyperlink.

Based on:

- URL (Uniform Resource Locator)
- HTML (HyperText Markup Language)
- HTTP (HyperText Transfer Protocol)

URL

Known as **web address**.

All webpage can be refered by URL.

Its parts:

- Scheme (protocol)
- Domain name or IP address
- Port number
- Path and name of file on server
- Query string
- Fragment identifier (bookmark)

URL examples

- http://www.example.org:80/index.html?lang=eng#top
- http://www.unideb.hu
- ftp://152.66.115.246/.banner
- http://neptun.unideb.hu/?page=studhun
- https://hu-hu.facebook.com/login.php
- http://en.wikipedia.org/wiki/HTML#History
- mailto:varga.imre@inf.unideb.hu

Legend:

- Scheme
- Domain name
- Port
- Path
- Query
- Fragment ID

HTML

A desription language to create websites.

Standardized by W3C (World Wide Web Consortium).

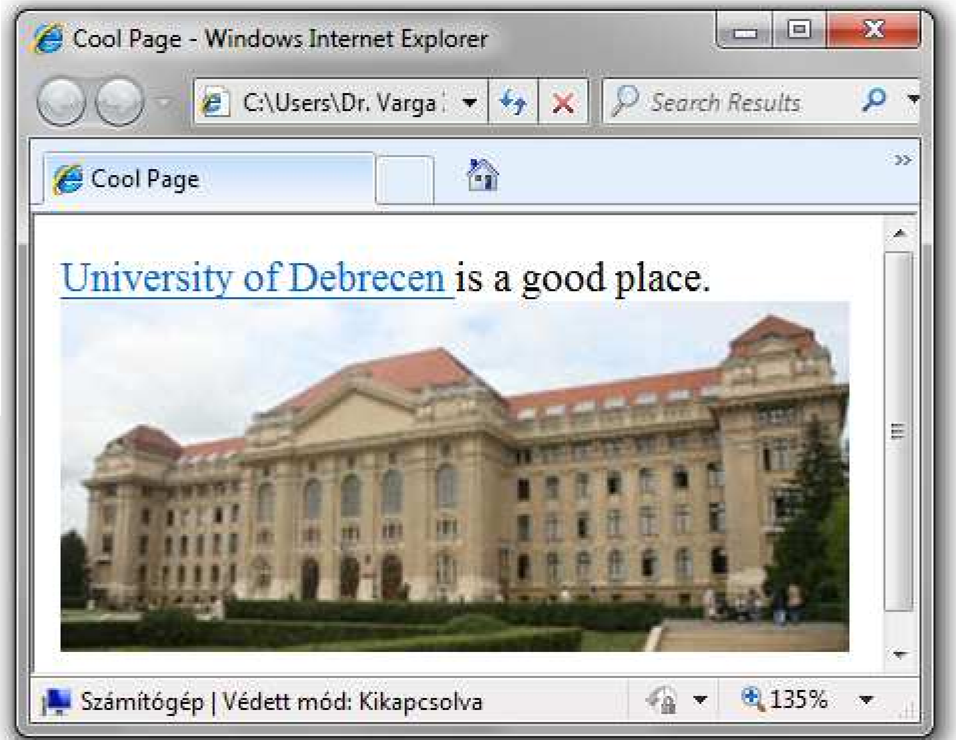
Websites are text-based files (contains only characters) which is represented (in visual form) by **browser**s.

Popular browsers:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Netscape Navigator
- Opera
- Safari
- Konqueror
- etc.

Example HTML file

```
<html>
  <head>
    <title>
      Cool Page
    </title>
  </head>
  <body>
    <a href="http://www.unideb.hu">
       University of Debrecen
    </a>
    is a good place. </br>
   <img src="UD.jpg">
  </body>
</html>
```



Hyperlink

A (hyper)link is a reference to data that the reader can directly follow (by a click).

A hyperlink points to

- a whole website or an element within a page,
- different media (picture, audio, video).

Hipermedia is a media with hiperlink.

- Media can be text, picture or video.

Hyperlink based on URL.

Example:

```
<a href="http://www.google.hu"> Google </a>
```

HTTP

HTTP is a request-response (client-server) information transmission protocol of application layer. (RFC 1945)

Client: web browser which visualize web pages for user.

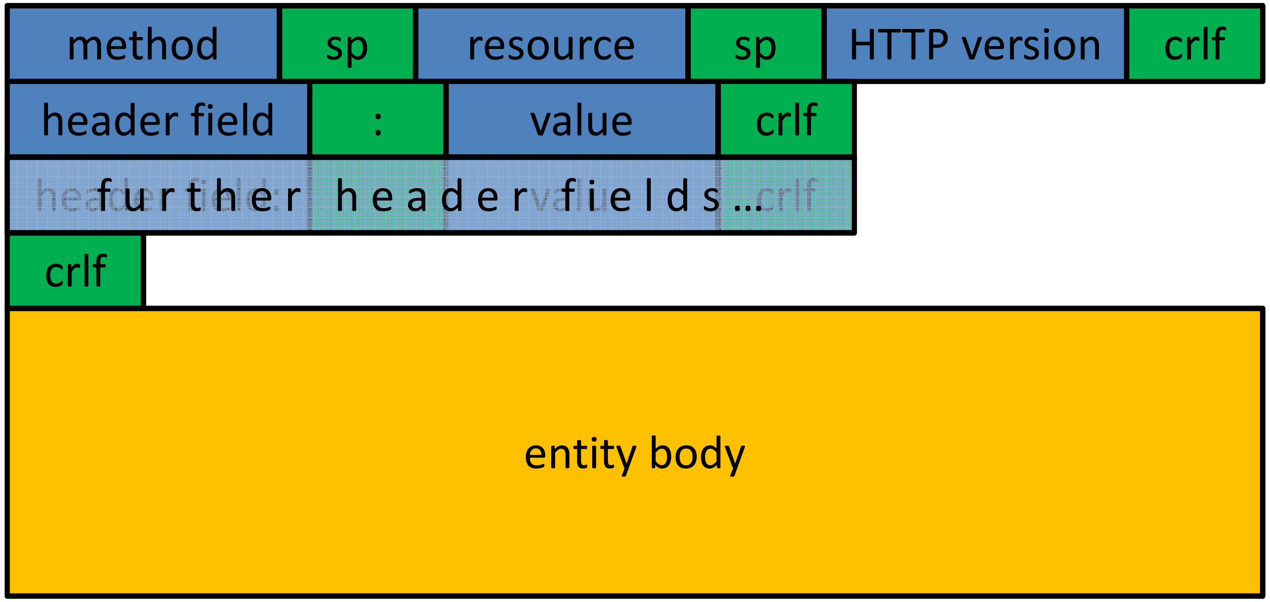
Server: computer (webserver) which stores webpages.

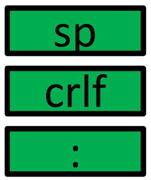
Usually it uses TCP connection (in Transport layer)

Safer solution: HTTPS (HTTP Secure)
HTTP over SSL/TLS protocol

HTTP

- Request format

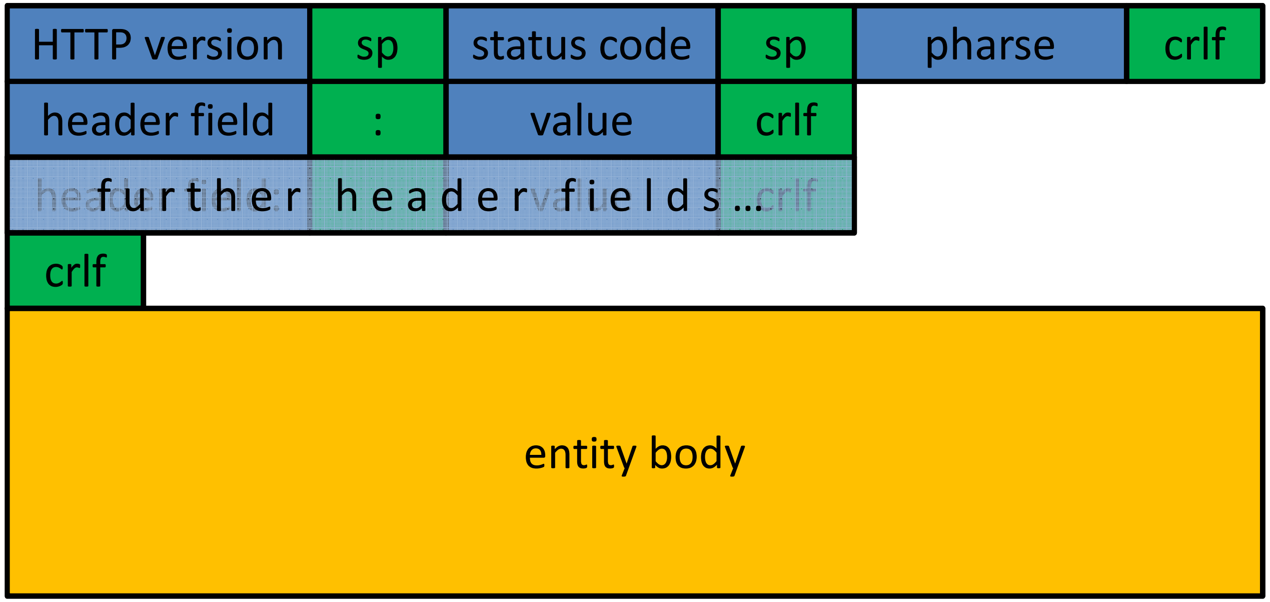




space character
carriage return + line feed characters
colon character

HTTP

- Response format



sp space character

crlf carriage return + line feed characters

: colon character

HTTP Status Codes

- 1xx: Request received, continuing process.
- 2xx: Indicates the action requested by the client was received, accepted and processed successfully.
- 3xx: The client must take additional action to complete the request.
- 4xx: In cases when the client seems to have erred.
- 5xx: The server failed to fulfill a valid request.

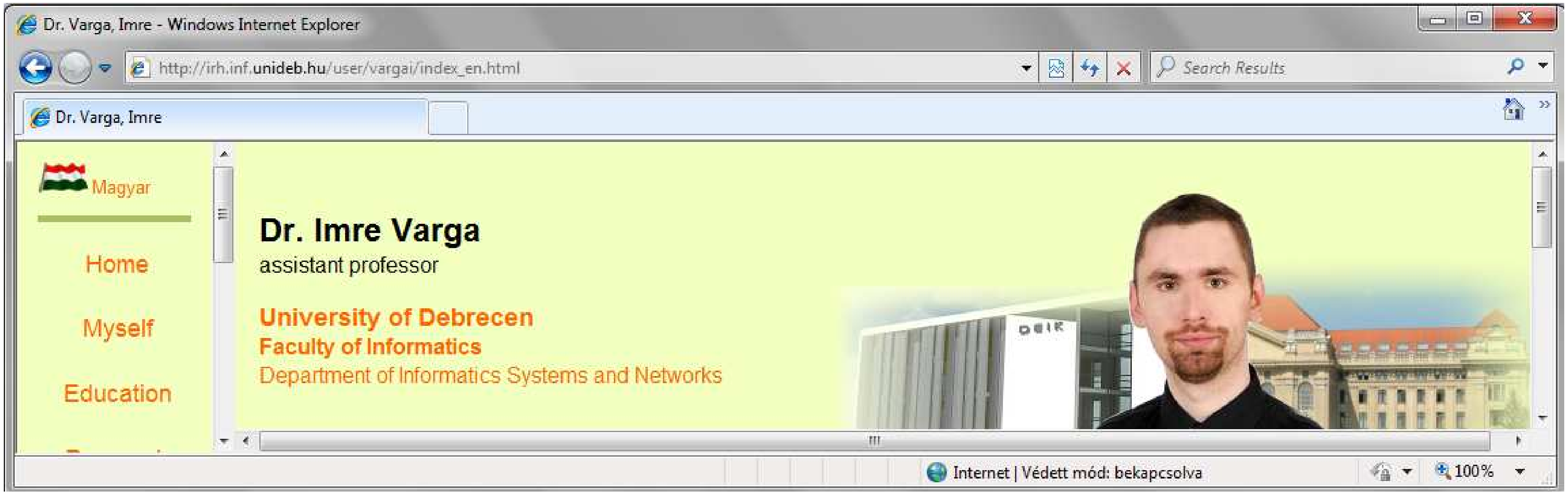
Browsing web

1. The user gives the URL in the address bar of browser.
2. The web browser determines the protocol from URL (eg. http://...).
3. It determines the (IP) address of web server from domain name in URL via DNS (eg. www.unideb.hu).
4. It builds up a session with web server (via TCP usually using port 80).
5. A request sent to HTTP server giving the name of the folder (and the HTML file) containing the web page (eg. /index.html).

Browsing web

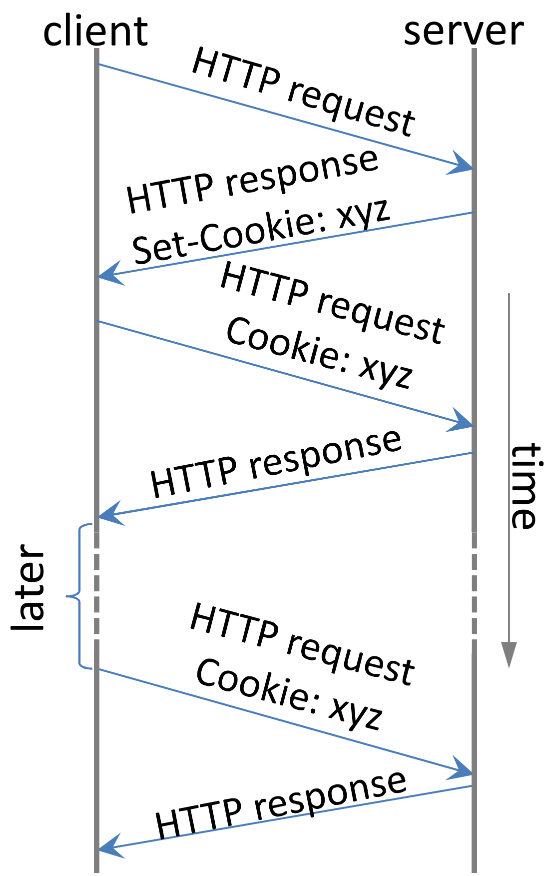
6. The server responds the request by sending to client the text or other medias (pictures, sounds, clips, etc.) defined in the HTML page.

7. The browser (client) composes files, displays the web page to user, and closes the session.



Cookie

- Name and value pair to ensure stateful operation
- Browser sends a usual request
- Server sends a „Set-Cookie” header field
- Client saves the cookie (information)
- Later when the browser requests the same site it sends the cookie.
- Server sends „personalized” site based on the cookie value



Browsing in terminal

linux$> telnet irh.inf.unideb.hu 80
Trying 193.6.135.80...
Connected to erlang.inf.unideb.hu.
Escape character is '^]'.
GET /index.htm HTTP/1.1
Host: irh.inf.unideb.hu

HTTP/1.1 200 OK
Date: Wed, 12 Feb 2014 11:26:45 GMT
Server: Apache/2.2.17 (Fedora)
Last-Modified: Sun, 20 Jan 2013 11:22:30 GMT
ETag: "1440c6d-135d-4d3b68f634980"
Accept-Ranges: bytes
Content-Length: 4957
Connection: close
Content-Type: text/html; charset=iso-8859-1

<html><head>
<title>DE IK IRH</title> ...

Command

Request

Reply header

Reply: requested page

E-mail

Electronic mail (E-mail, email, eMail)

A method of exchanging digital messages from an author to one or more recipients. (RFC 821)

E-mail address:

local_part@domain_part

user@provider

E-mail contains 2 sections

- Header:

  It has several fields (sender, addressee, subject, …)

- Body:

  The ‘message’.

E-mail header fields

- From:
  Sender’s e-mail address
- To:
  The e-mail address(es) of the recipient(s)
- Subject:
  Topic of the message
- Date:
  The local time and date when the message was written
- Message-ID:
  Automatically generated to identify the message

E-mail header fields

- Cc:
  E-mail addresses who will get copies of message.
- Bcc:
  E-mail addresses of recipients who won't see eachother in the header of their message.
- Reply-To:
  Address that should be used to reply to the message.
- Content-Type:
  Information about how the message is to be displayed, usually a MIME type.
- and much more…

Body of e-mail

Originally it contains only characters (text).

Modern graphic email clients allow the use of either plain text or HTML.

Multipurpose Internet Mail Extensions (**MIME**, RFC 2045) is an Internet standard that extends the format of email to support:

- Text in character sets other than ASCII (eg.: áíűŁäšş)
- Non-text attachments (jpg, pdf, mp3, avi)
- Message bodies with multiple parts
- Example: *text/plain, text/html, image/jpeg*

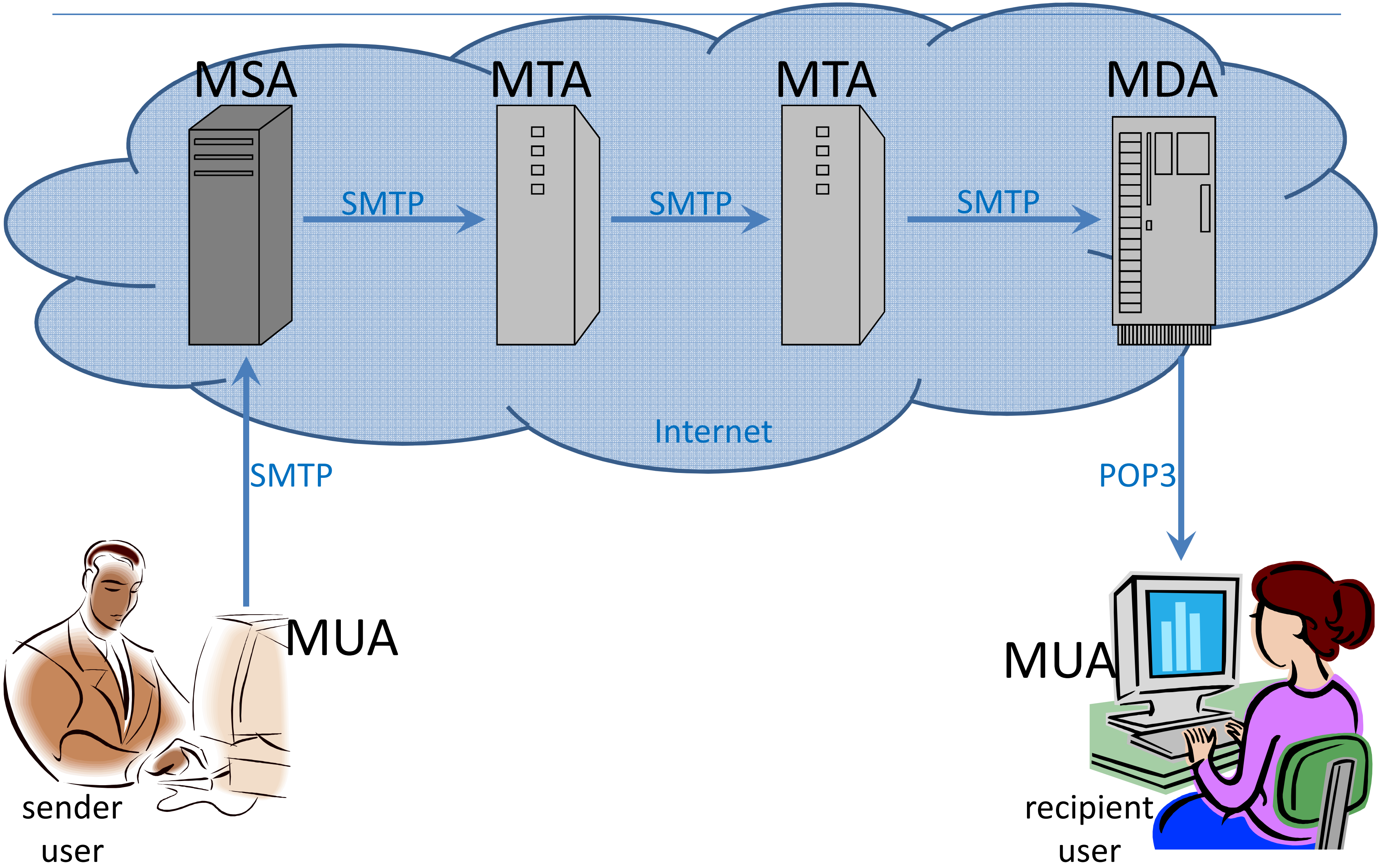
Mail servers and clients

- Programs used by users for managing e-mails are called Mail User Agents (MUA).
- MUA submit the e-mail to Mail Submission Agent (MSA) who will forward it.
- Messages are exchanged between hosts using the Simple Mail Transfer Protocol (SMTP) with software programs called Mail Transfer Agents (MTA).
- Messages are delivered to a mail store by programs called Mail Delivery Agents (MDA). Users can retrieve their messages from servers using standard protocols such as POP3 or IMAP.

Process of e-mailing

1. Sender composes the message and hits „Send” button.
2. Senders MUA formats the e-mail and sends it to MSA by SMTP.
3. MSA forwards the e-mail to recipients MDA (and perhaps to some internal MTA) by SMTP.
4. The MDA delivers e-mail to the recipients mailbox.
5. Recipient presses the "get mail" button in own MUA, which download the e-mail from MDA by POP3 or IMAP.

Process of e-mailing



Process of e-mailing

1. Email header contains the destination email address
2. MSA asks the MX record of domain name after @
3. Name server answers the name of mail exchanger server of the destination domain
4. MSA asks the IP address of mail exchanger from DNS
5. The email is sent to the port 25 of the given IP address by SMTP
6. MDA receives the message and gets the username (destination email address part before @)
7. MDA puts the mail to the user's inbox mail folder
8. Recipient's MUA download mails from MDA by POP3

Connect to SMTP server

```
linux$> telnet mail.server.com 25
Trying 193.6.138.45...
Connected to delfin.unideb.hu.
Escape character is '^]'.
220 delfin.unideb.hu ESMTP Postfix (Ubuntu)
helo mail
250 delfin.unideb.hu
mail from: nobody@nowhere.com
250 2.1.0 Ok
rcpt to: varga.imre@unideb.hu
250 2.1.0 Ok
data
354 Enter mail, end with "." on a line by itself
Subject: test

This is a test e-mail.
.
250 2.0.0 Message accepted for delivery
Connection closed by foreign host.
```

Connect to POP3 server

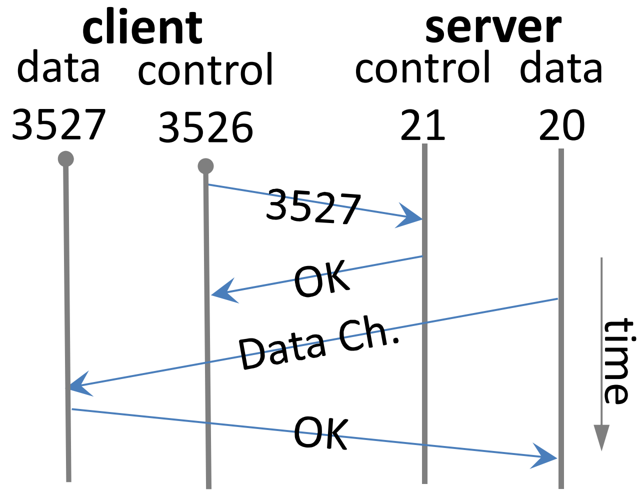
```
linux$> telnet freemail.hu 110
Trying 195.228.245.1...
Connected to freemail.hu.
Escape character is '^]'.
+OK <6245.1392286988@freemail.hu>
USER proglabor
+OK
PASS proglabor
+OK
LIST
+OK
1 2442
2 12658
.
RETR 1
+OK
Message-ID: <df14a185b13857ef027324fdb8561cd.squirrel@mail.unideb.hu>
Subject: Important mail to you
From: "Dr. Varga Imre" <varga.imre@unideb.hu>
To: proglabor@freemail.hu

Dear Friend, …
```

FTP

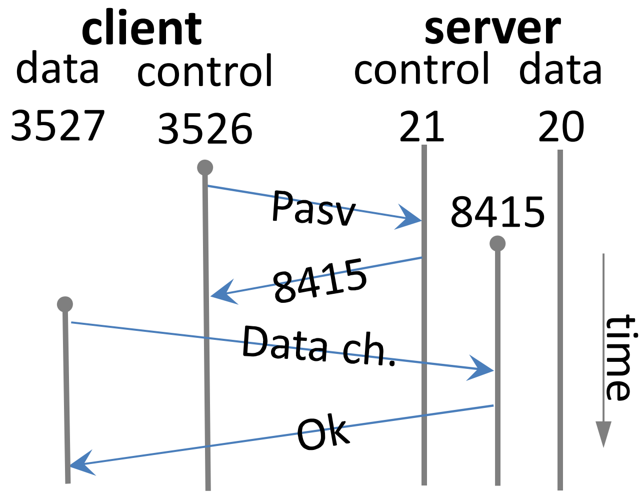
- File Transfer Protocol
- Details in RFC 959
- Client-server architecture
- Down/upload files from/to servers
- 2 channels (Control & Data)
- FTP server codes (e.g. 220 Service ready for new user.)
- Anonymous FTP
- Browsers support it
- Much popular solution is the peer-to-peer BitTorrent

Active and passive modes

- Client connects to port 21 of server (control channel)
- Active mode:
  - Client opens a port (to data channel)
  - Server connect to it



- Passive mode:
  - Server opens a new port (to data channel)
  - Client connect to it



FTP

Download the `rfc0959.txt` file which is in `documents/rfc` folder of `ftp.bme.hu` server!

- In browser: ftp://ftp.bme.hu/documents/rfc/rfc0959.txt
- In terminal:

```
linux$> ftp ftp.bme.hu
Name (ftp.bme.hu:user): anonymous
Password:
ftp> passive
ftp> cd documents/rfc
ftp> get rfc0959.txt
ftp> quit
```

Connect to FTP server

Terminal 1 (Control channel)

```
linux$> telnet ftp.bme.hu 21
Trying 2001:738:2001:2001::c1ca...
Connected to ftp.bme.hu.
Escape character is '^]'.
220--- Welcome to Pure-FTPd ---
USER anonymous
331- Welcome to ftp.bme.hu FTP service.
PASS
230 Any password will work
EPSV
229 Extended Passive mode OK (|||62282|)
RETR ReadMe.txt
150 Accepted data connection
226-File successfully transferred
QUIT
221 Logout.
Connection closed by foreign host.
```

Terminal 2 (Data channel)

```
linux$> telnet ftp.bme.hu 62282
Trying 2001:738:2001:2001::c1ca...
Connected to ftp.bme.hu.
Escape character is '^]'.

This is the content of ReadMe.txt

Connection closed by foreign host
```

ssh

Secure Shell

- Remote command-line login
- Encrypted data communication

```
linux$> ls
a.out   Desktop   prog.c   program.log
linux$> ssh user@irh.inf.unideb.hu
user@irh.inf.unideb.hu's password:
Last login: Thu Feb 13 12:49:32 2014 from
erlang.inf.unideb.hu
[remote]$ ls
Desktop  inetd.conf  readme.txt  run.sh
[remote]$ exit
logout
Connection to irh.inf.unideb.hu closed.
linux$>
```

Other parts of Application layer

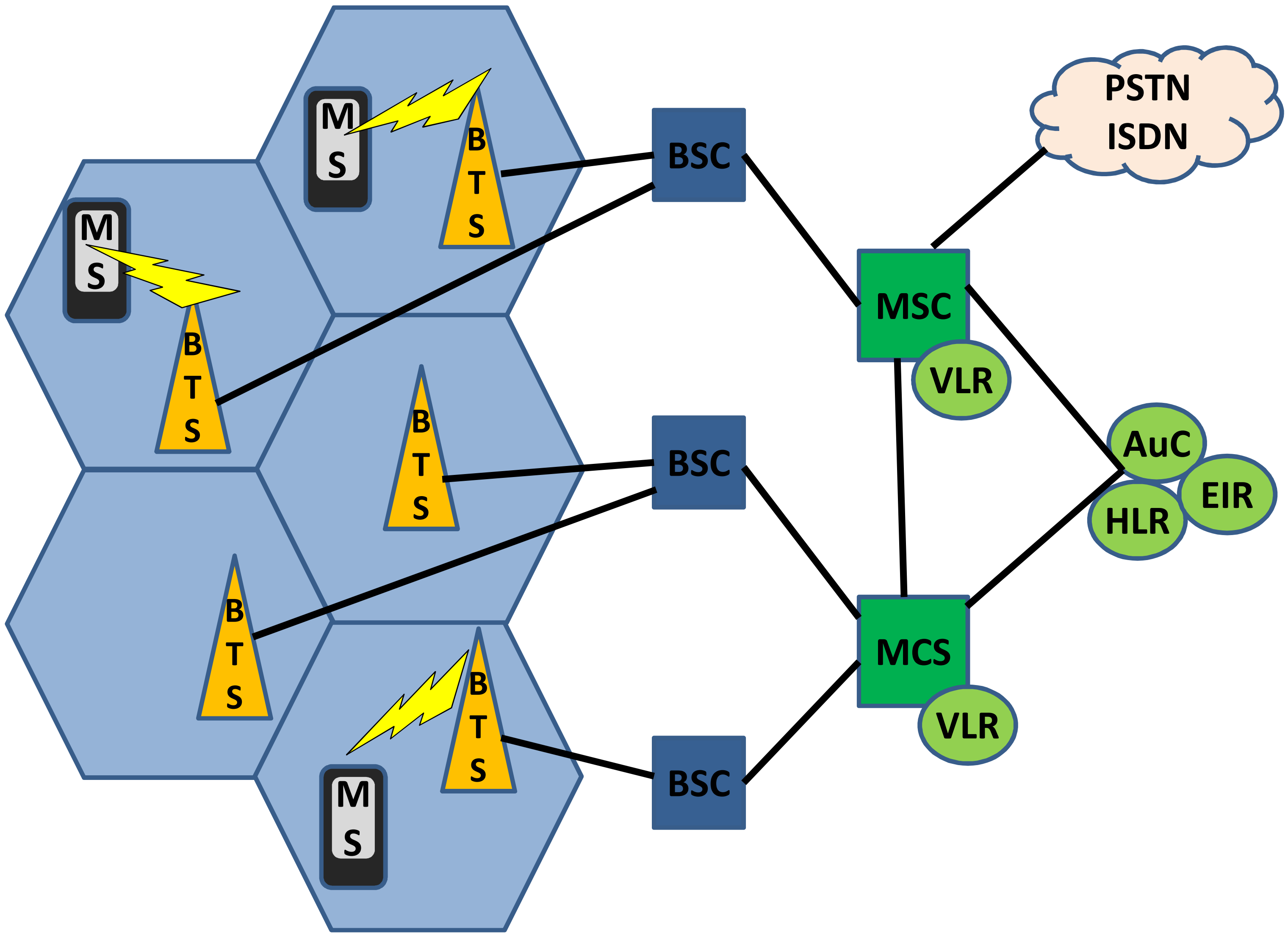
- Remote login (telnet, ssh)
- Down/uploading files (scp, FTP, bittorent)
- Voice over IP (VoIP) (Skype, MSN)
- IPTV (UPC)
- Distributed databeses
- Online games
- etc.

Mobile telephone systems

Cellular wireless network

- 1G: NMT (analog voice)
- 2G: GSM (ca. 0.01 Mbps)
- 2.5G: GPRS (ca. 0.1 Mbps)
- 2.75G: EDGE (ca. 0.5 Mbps)
- 3G: UTMS (ca. 1 Mbps)
- 3.5G: HSDPA/HSUPA (ca. 10 Mbps)
- 4G: LTE, WiMax (ca. 100 Mbps)
- 5G: coming soon… (ca. 1000 Mbps)

GSM architecture



GSM architectures

- Mobile Equipment (ME)
- Subscriber Identity Module (SIM)

Mobile station (MS)

- Base Transceiver Station (BTS)
- Base Station Controller (BSC)

Base Station Subsystem (BSS)

- Mobile Switching Center (MSC)
- Home Location Register (HLR)
- Visitor Location Register (VLR)
- Authentication Center (AUC)
- Equipment Identity Register (EIR)

Network Switching Subsystem (NSS)

Network setup & commands on Windows

Network setup

4 necessary properties to use network on a computer:

- IP address
- Netmask
- Gateway
- DNS server

They are given by the Internet Service Provider (ISP).

Either the user do their setup or use DHCP (if possible).

The user can use ‘command-line’ or GUI (Graphical User Interface) to do setup process.

Network setup by Control Panel*

1. Go to Start Menu
2. 'Control Panel'
3. 'View network status and tasks' in 'Network and Internet' block
4. 'Change adapter settings'
5. Right mouse click on the adapter, choose 'Properties'
6. Choose 'Internet Protocol Version 4 (TCP/IPv4)' and push button 'Properties'
7. Choose automatic configuration (DHCP) or give the four datas.

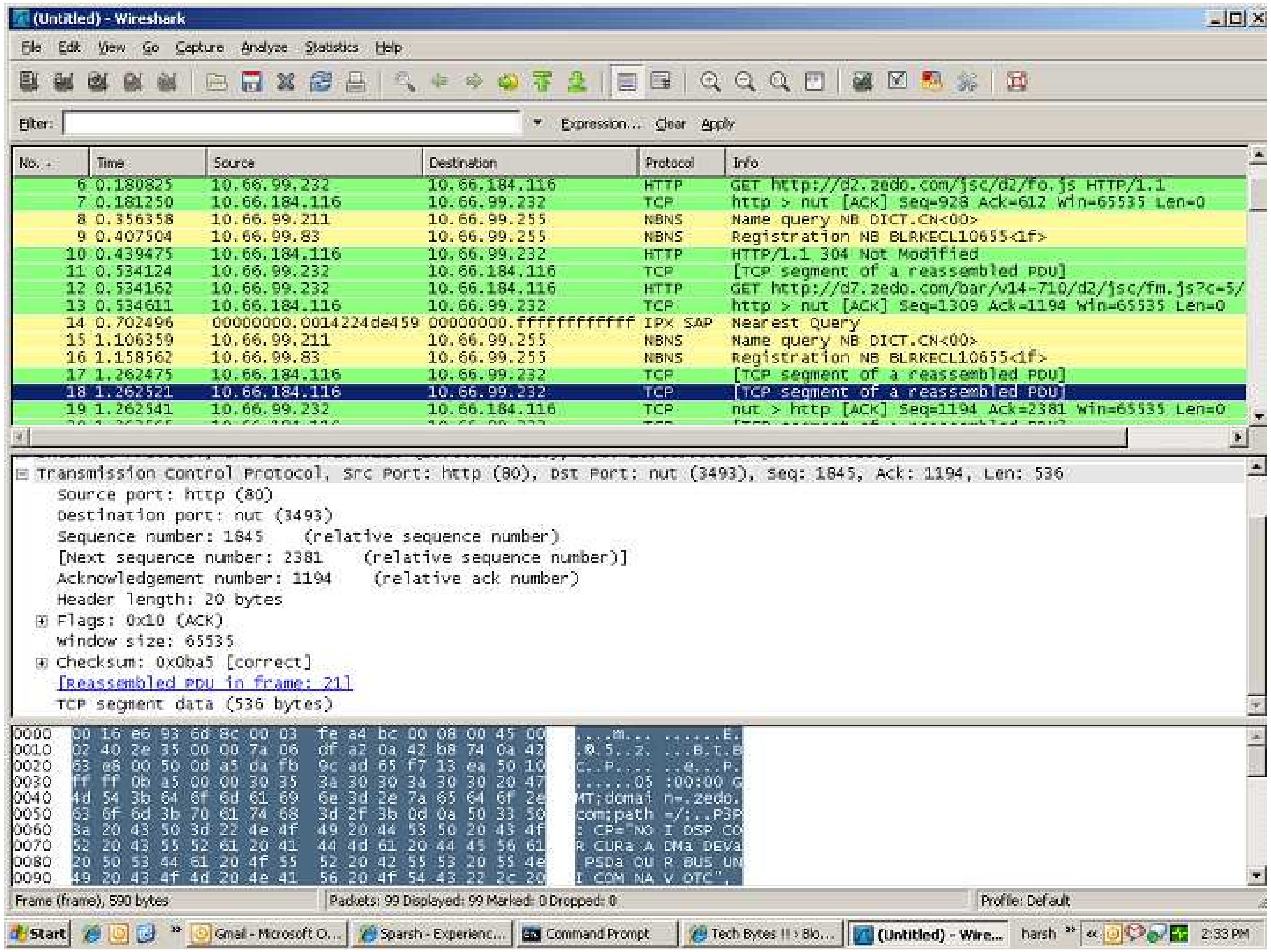
* on Windows 7 operating system

Useful network commands on Windows

- `ipconfig`: Shows the setups of network adapters.
- `ipconfig /all`: Shows the detailed setups of network adapters.
- `route print`: Shows the routing table of the computer.
- `ping <node>`: Check connection to other computers.
- `arp -a`: Shows ARP table.
- `tracert <node>`: Show the hops to a computer.
- `netstat -s`: Shows network statistics (IP, TCP, UDP).

Wireshark

- Free and open-source packet analyzer



References & further readings

- Andrew S. Tanenbaum: *Computer Networks*, Prentice-Hall, 2003
- Wikipedia, http://en.wikipedia.org
- Béla Almási: Számítógép hálózatok, University of Debrecen