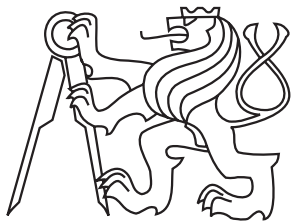
# Network layer, network address, IPv4.

Ing. Yelena Trofimova

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


Computer networks, BIE-PSI
SS 2020/21, Lecture 3

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



# Contents

# Link layer x network layer

- Link layer
  - data transfer between "neighboring" devices
  - medium access control
  - flow control
  - error checking
- Network layer
  - data transfer between the source and destination addresses
  - host addresses
  - routing between networks
  - services of varying quality (QoS - Quality of Services)

# Services of the Network Layer

Goals to be achieved to provide service for the transport layer:

- independence of the forwarding method
- independence of network topology
- provide network numbering schema

- connection-oriented services
- connectionless services - connection is carries out at the transport layer

# Conectionless service

- block of data from the transport layer is divided into packets
- functions of the end-device: SEND PACKET, RECEIVE PACKET
- packets ("datagrams") are routed individually
- packet header contains address
- router implements some routing algorithm, usually uses the routing table with rows: $\{$ *dest_addr, link* $\}$
- example: IP

# Connection-oriented service

- virtual circuits
  - first stage: circuit registration on all routers on the path
  - all data then is transferred throw this path
  - last stage: deletion of information about the circuit on all routers on the path
- packet header contains a virtual circuit identifier
- row of the routing table: { *(link_in, label_in) (link_out, label_out)* }
- example: MPLS

# Comparison

| | Datagram network | Virtual circuits |
|---|---|---|
| path registration | no | yes |
| addressing | src/dest addr | label |
| state information on the router | no | yes |
| routing | individual | only during the path registration |
| router failure | small problem | big problem |
| QoS & flow control | difficult | easy |
| congestion control | difficult | easy |

# Addressing

Unique addresses across the network

Network

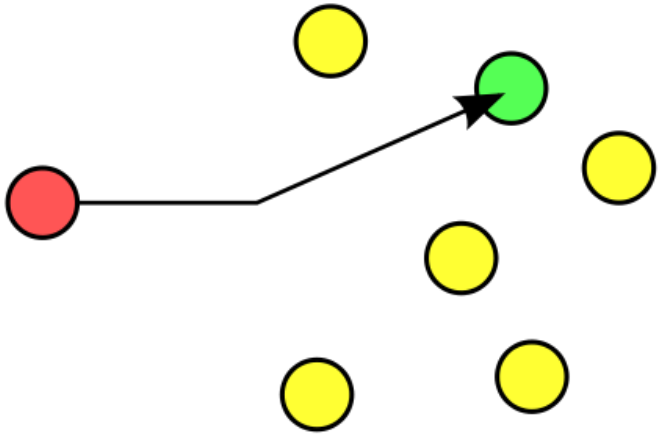
- continuous group of addresses
  - disjoint with another network
- division of address space
  - example: national telephone prefix
- simplification of routing
  - the entire network is represented by a single address from outside
- multilevel layout – subnets

# Types of addressing

- unicast
- broadcast
- anycast
- multicast

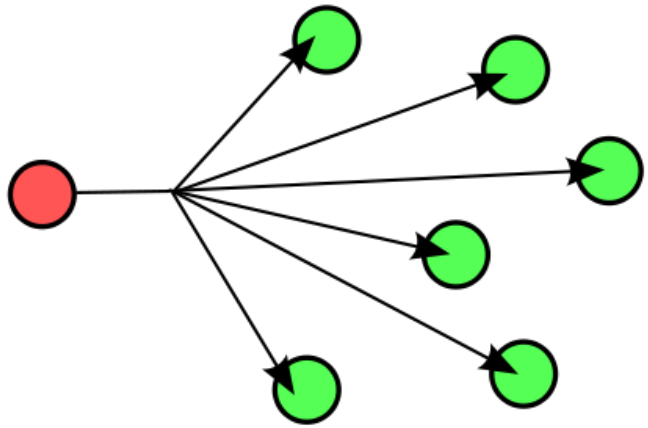
# Unicast

- destination: 1 host
- standard in IPv4/IPv6



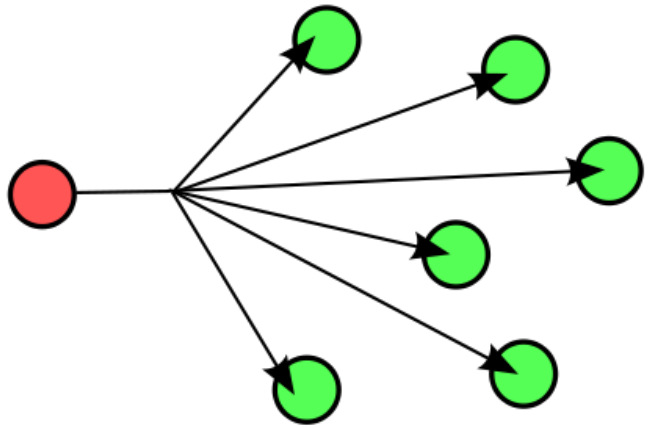
# Broadcast

- destination: all hosts in the local network
- is not routed outside the local network
- uses link layer broadcast addresses:
  Ethernet: FF:FF:FF:FF:FF:FF
- destination IP address contains all 1s in host part of the IP address
- Example: IP address 192.113.147.16/25
  mask 255.255.255.128
  net address 192.113.147.0
  broadcast ???



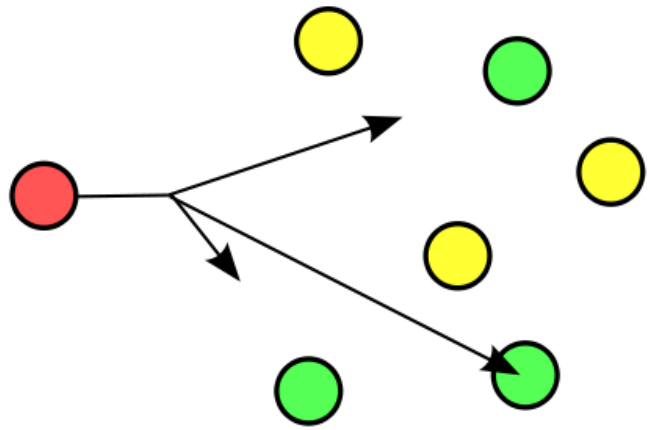
# Broadcast

- destination: all hosts in the local network
- is not routed outside the local network
- uses link layer broadcast addresses:
  Ethernet: FF:FF:FF:FF:FF:FF
- destination IP address contains all 1s in host part of the IP address
- Example: IP address 192.113.147.16/25
  mask 255.255.255.128
  net address 192.113.147.0
  broadcast 192.113.147.127



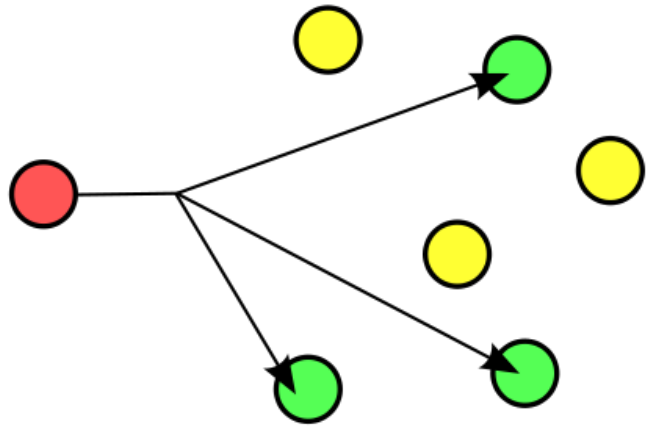
# Anycast

- addressing and routing strategy when several devices have the same address but the the real recipient is just one device within the group
- destination: 1 host in a group
- benefits:
  - load balancing
  - lower latency
- examples:
  - DNS root servers
  - content delivery networks



# Multicast

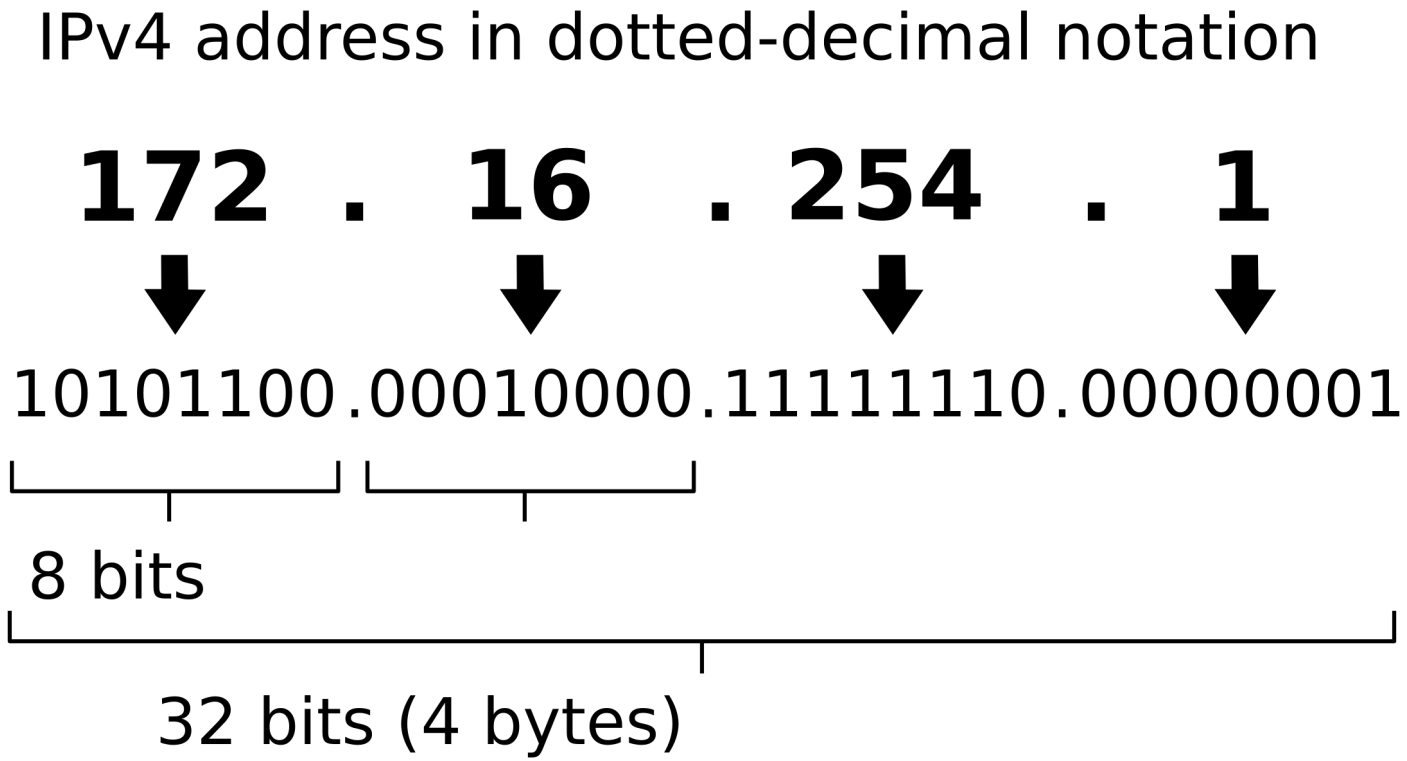
- destination: group of hosts
- multicast addresses: IPv4 class D 224.0.0.0 – 239.255.255.255
- IGMP protocol (Internet Group Management Protokol) for hosts registration
- PIM protocol (Protocol Independent Multicast) for multicast routing



# IPv4 address

32-bit number

- dot-decimal notation: 4 groups of 8 bits=octet(byte)




Source: Wikipedia

# IPv4 address classes

- classful design is a history, is not used today
  - A,B,C = normal IP addresses (unicast)
  - D = multicast
  - E = reserved

| class | prefix | network address | networks | hosts | first address |
|---|---|---|---|---|---|
| A | 0 | 8 bits | 128 | $2^{24}$ | 0.0.0.0 |
| B | 10 | 16 bits | 16384 | $2^{16}$ | 128.0.0.0 |
| C | 110 | 24 bits | 2097152 | $2^{8}$ | 192.0.0.0 |
| D | 1110 | | | | 224.0.0.0 |
| E | 1111 | | | | 240.0.0.0 |

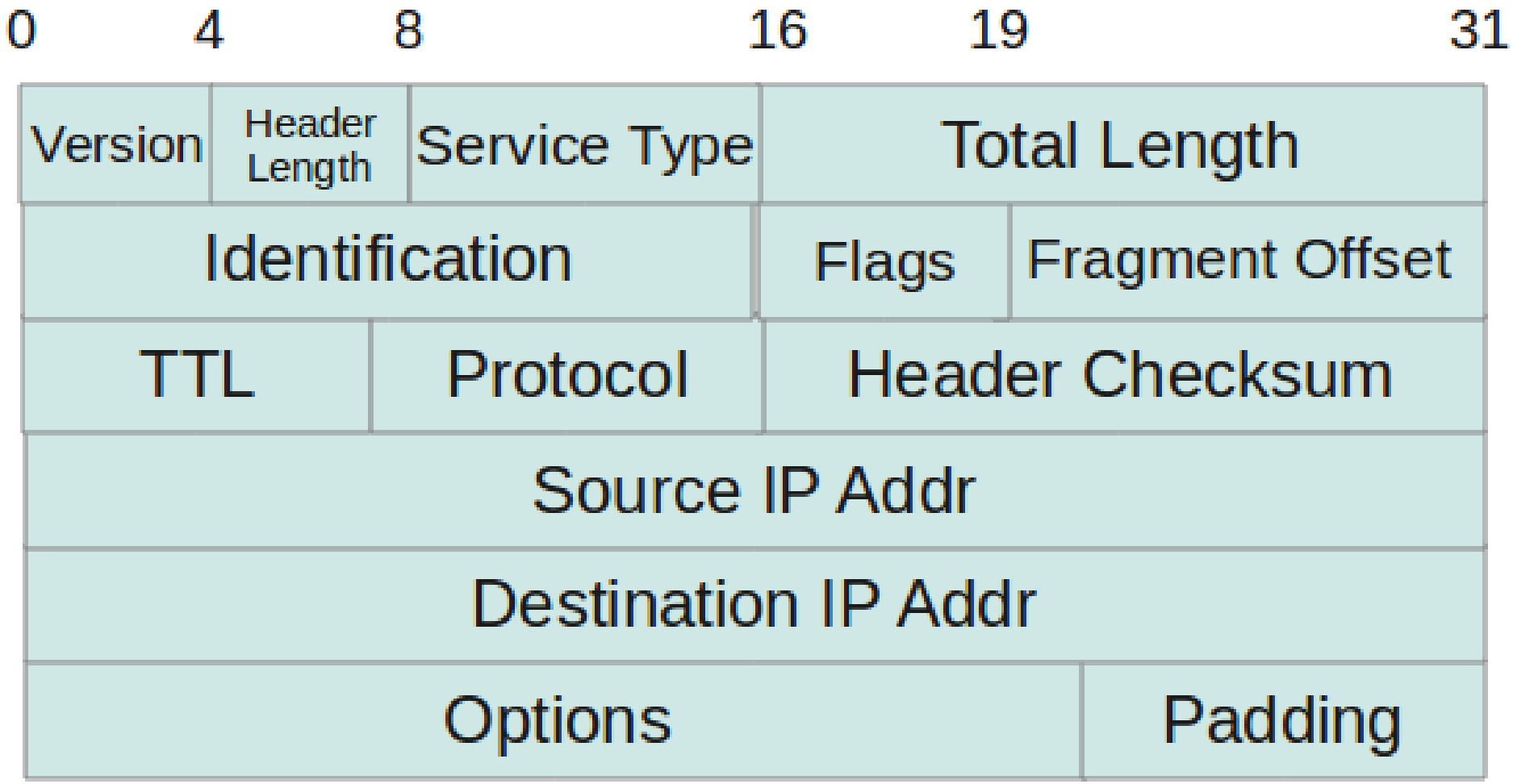
# IPv4 address - CIDR

- CIDR schema (Classless Inter-Domain Routing) – RFC1518, RFC1519
- network prefix length is arbitrary – classful prefix scheme can only be 8, 16 or 24 bits
- withdrawal of classes A, B and C
- mask is expressed by the number of bits in network part
- example: network prefix = 18 of "1" bits:
  11111111.11111111.11000000.00000000
  CIDR format: /18 = mask 255.255.192.0

# Private IP addresses

- free to use in private networks
- not routed in the Internet
- useful for NAT:
  - we have few IPv4 public addresses
  - network isolation
  - router performs translation of a large number of private addresses to a single (or several) public addresses
- 10.0.0.0/8 16777216 addrs / 1x class A
  172.16.0.0/12 1048576 addrs / 16x class B
  192.168.0.0/16 65537 addrs / 256x class C

# IPv4 packet header




Source: https://portunreachable.com/tagged/ip

# IPv4 packet header fields I

- version: 4 (IP version 4)
- header length: in 32-bit words
- type of service: for basic QoS
- total length: packet length in bytes
- packet identification: for identification of fragments
- flags: different flags, used for fragmentation
- fragment offset: relative offset of the fragment
- time to live: counter of the hops over routers

# IPv4 packet header fields II

- protocol: transport protocol identification
- header checksum: checksum control
- source address: IPv4 address of the source host
- destination address: IPv4 address of the destination host
- options: not often used, some special purposes
- padding: alignment of the header length to 32 bits

# Fragmentation

- by MTU (Maximal Transmission Unit), defined by link layer
- packet with length $>$ MTU will be divided to more smaller packets
- fragments are delivered independently
- packet completion (defragmentation) is made on destination host

# Recall: ARP

- Address Resolution Protocol – RFC826
- resolution of network layer addresses into link layer addresses
  - sending a query: "Who has the IP address x.x.x.x?"
  - response contains the MAC address
- ARP cache on every host
- automatic records expiration
- is used today for IPv4, but was designed to operate with any type of network/link address

# ICMP

Internet Control Message Protocol

- send error/information messages
  - type: 4 bits
  - code: 4 bits
- for example:
  - requested service is not available
  - that host or router could not be reached
- types of relevant messages:

| Type | Code | Description |
|---|---|---|
| 0 – Echo Reply | 0 | Echo reply |
| 3 – Destination Unreachable | 0 | Destination network unreachable |
| | 1 | Destination host unreachable |
| | 2 | Destination protocol unreachable |
| | 3 | Destination port unreachable |
| | 4 | Fragmentation needed and DF flag set |
| | 5 | Source route failed |
| 5 – Redirect Message | 0 | Redirect datagram for the Network |
| | 1 | Redirect datagram for the host |
| | 2 | Redirect datagram for the Type of Service and Network |
| | 3 | Redirect datagram for the Service and Host |
| 8 – Echo Request | 0 | Echo request |
| 9 – Router Advertisement | 0 | Use to discover the addresses of operational routers |
| 10 – Router Solicitation | 0 | |
| 11 – Time Exceeded | 0 | Time to live exceeded in transit |
| | 1 | Fragment reassembly time exceeded |
| 12 – Parameter Problem | 0 | Pointer indicates error |
| | 1 | Missing required option |
| | 2 | Bad length |
| 13 – Timestamp | 0 | Used for time synchronization |
| 14 – Timestamp Reply | 0 | Reply to Timestamp message |