U.PORTO
FEUP FACULDADE DE ENGENHARIA UNIVERSIDADE DO PORTO

Arquiteturas da Computação Industrial

Industrial Computing Architectures

Lecture 22 – **The Internet Protocol (network layer)**

Slides by Luís Almeida (lda@fe.up.pt)

(based on previous slides from Paulo Portugal;
some changes by Pedro Santos)

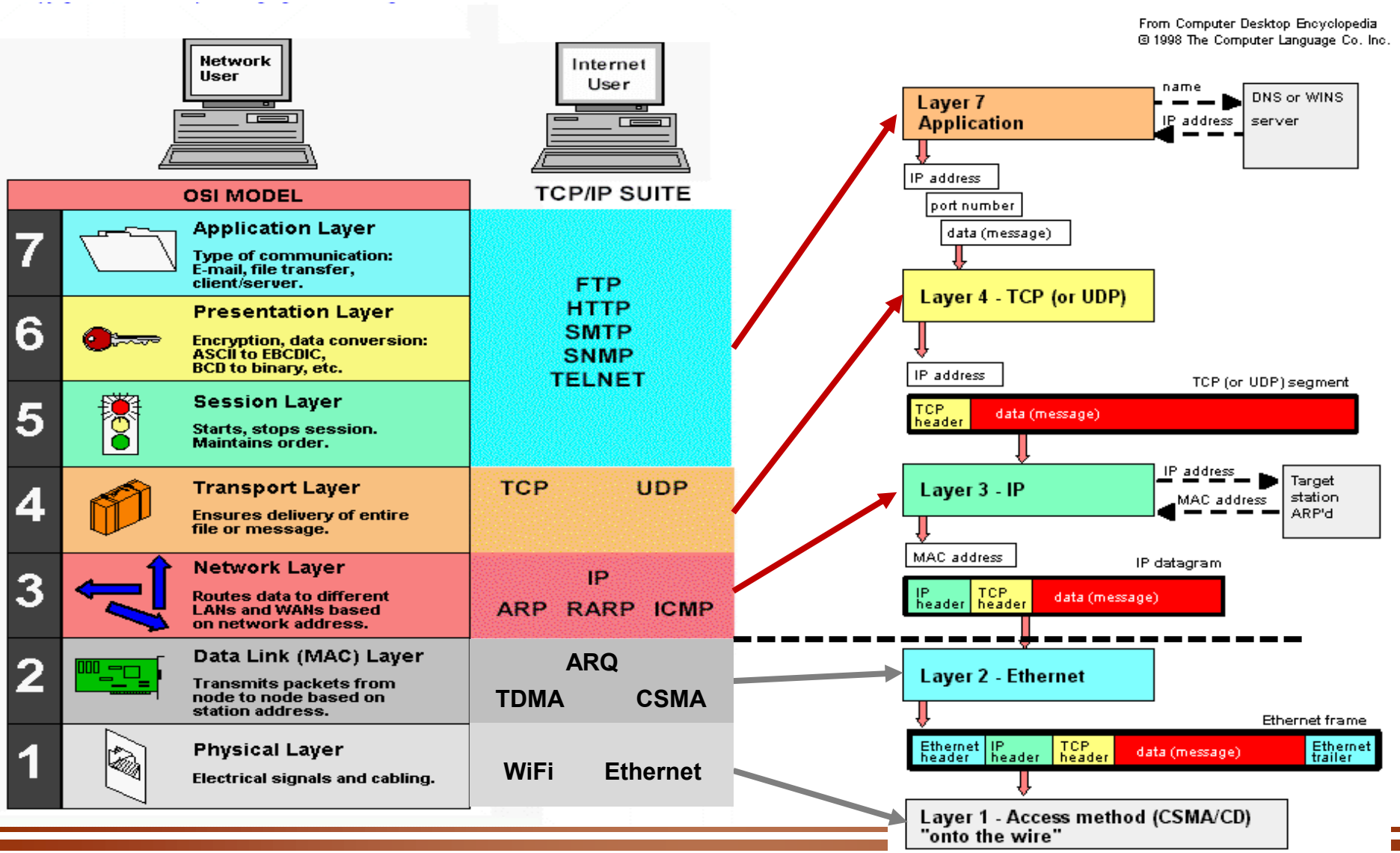
Previous 4 lectures

- **Introduction to wireless communications in industry**
  - Motivation, problems/solutions; Technologies
- **IEEE 802.11**
  - Architecture, protocol stack; Physical and Data link layers; MAC
- **IEEE 802.15.4**
  - Architecture, protocol stack; Physical and Data link layers; MAC
- **Industrial protocols** over IEEE 802.15.4
  - ZigBess; WirelessHART; ISA100
- **Preparation to second test + Second test**

This lecture

- **The Internet Protocol stack**
  - Motivation, problems/solutions
- **The IP network layer**
  - Routing packets
  - The IP PDU
  - Fragmentation for lower layer packets
  - The IP header
  - IP addressing
  - Interface configuration
  - Address resolution protocol - ARP
  - Internet Control Messaging Protocol – ICMP

The IP protocol stack



U.PORTO
FEUP FACULDADE DE ENGENHARIA
UNIVERSIDADE DO PORTO

The IP network layer

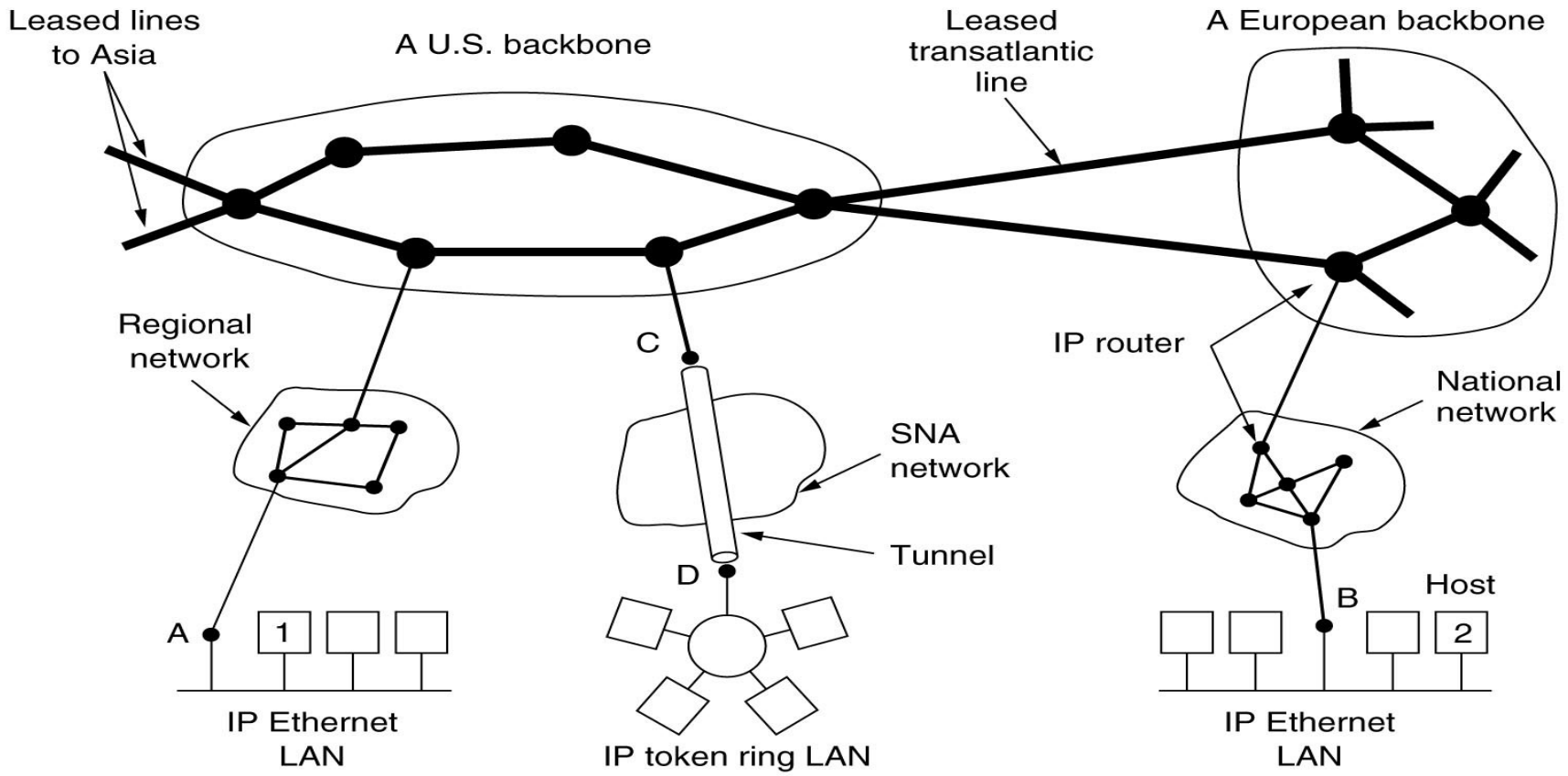
IP – network layer

- **IPv4**: IETF **RFC 791** (sept 1981)
- **End-to-end principle**
  - **simplify** the network ➔ push network intelligence to the end nodes
  - Quality of Service (**QoS**) is **best effort** (no guarantees)

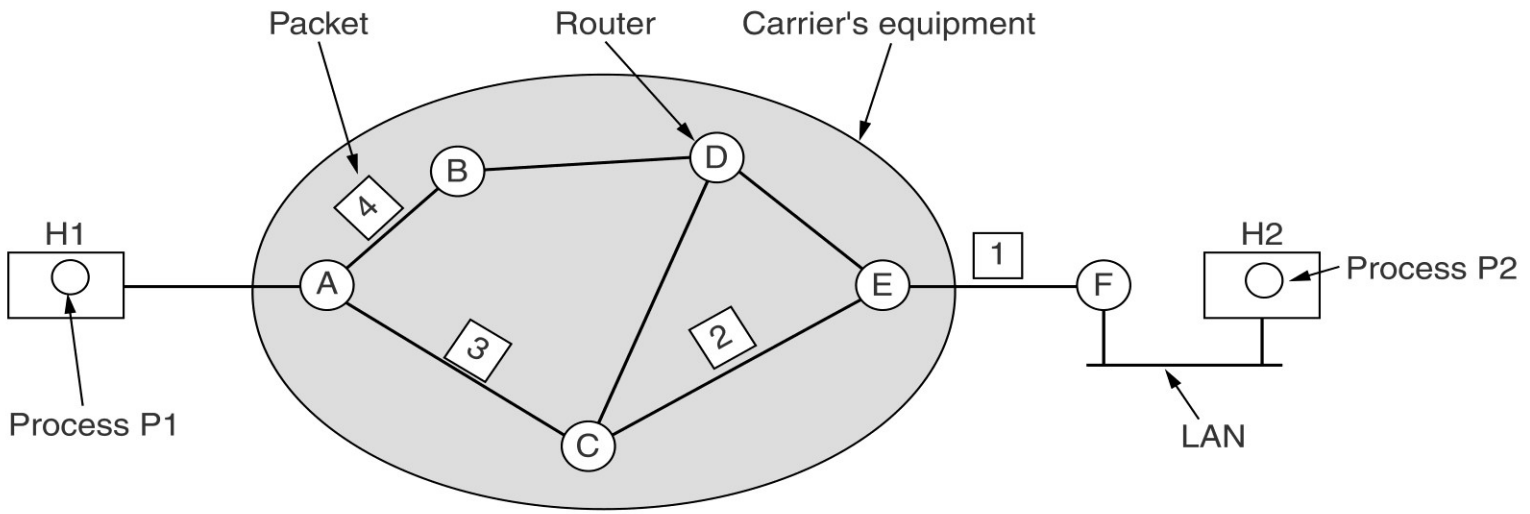
- **Network layer**
  - Provides an upper interface in **IP packets** (i.e. datagrams)
    - » **Max. 64KBytes** (frequently less than 1500 Bytes in practice)
  - **Routing** of datagrams across networks
    - » **Based on Internet addresses**
  - **Fragmentation** and **re-assembly** of datagrams to fit the packets offered by the lower interface (part of L4 in OSI model)
    - » **ex. Ethernet** offers 1500 Bytes packets

IP - packet routing

- **Internet**: interconnection of multiple heterogeneous networks
  - Packets generally have to cross multiple networks in their path



IP - packet routing



A's table

initially		later	
A	–	A	–
B	B	B	B
C	C	C	C
D	B	D	B
E	C	E	B
F	C	F	B

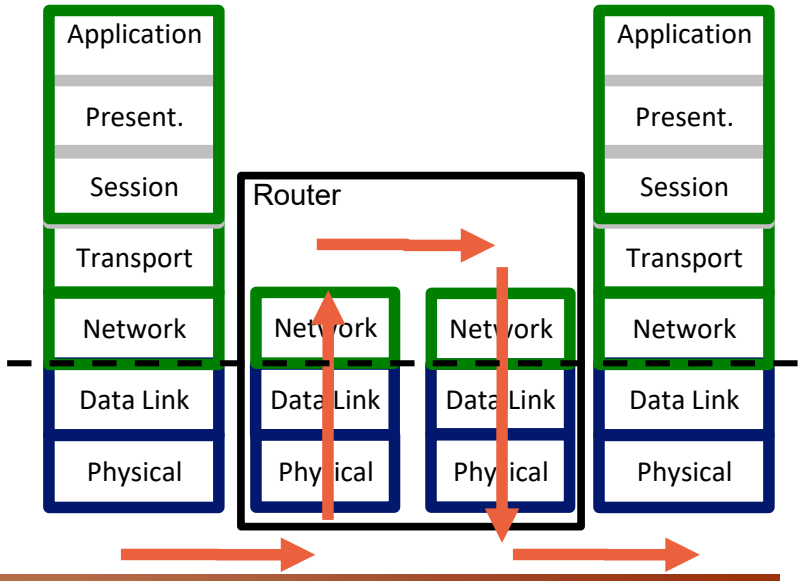
Dest. Line

C's table

A	A
B	A
C	–
D	D
E	E
F	E

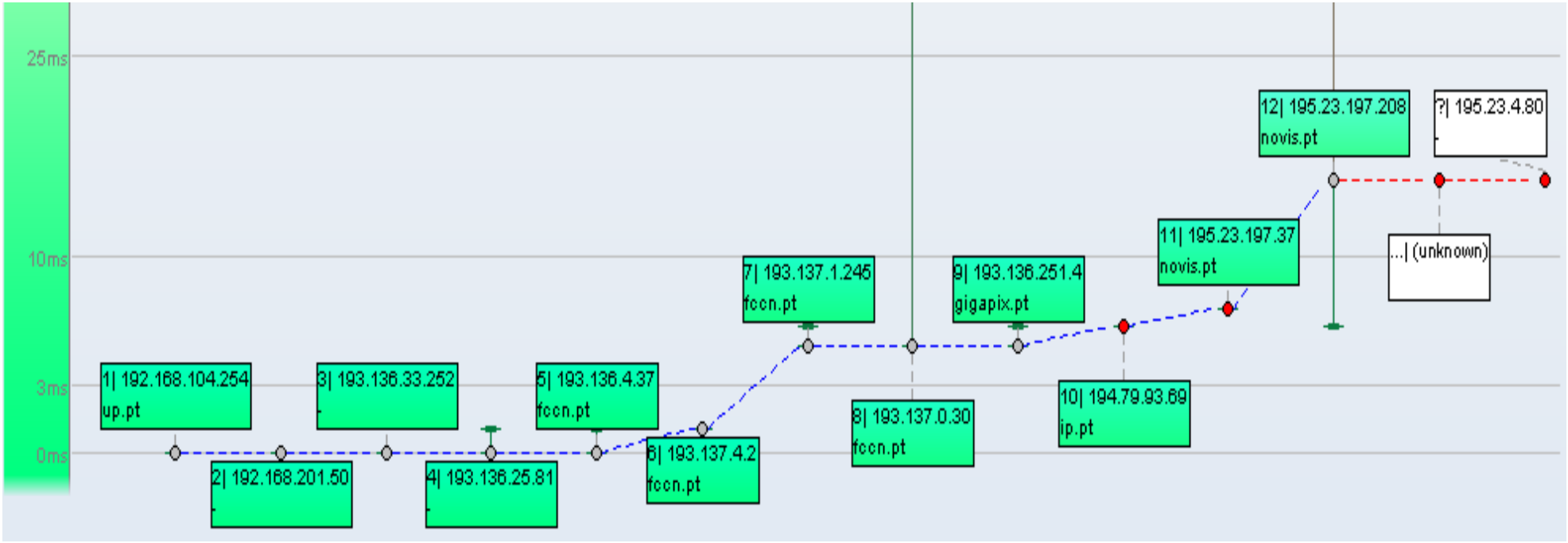
E's table

A	C
B	D
C	C
D	D
E	–
F	F

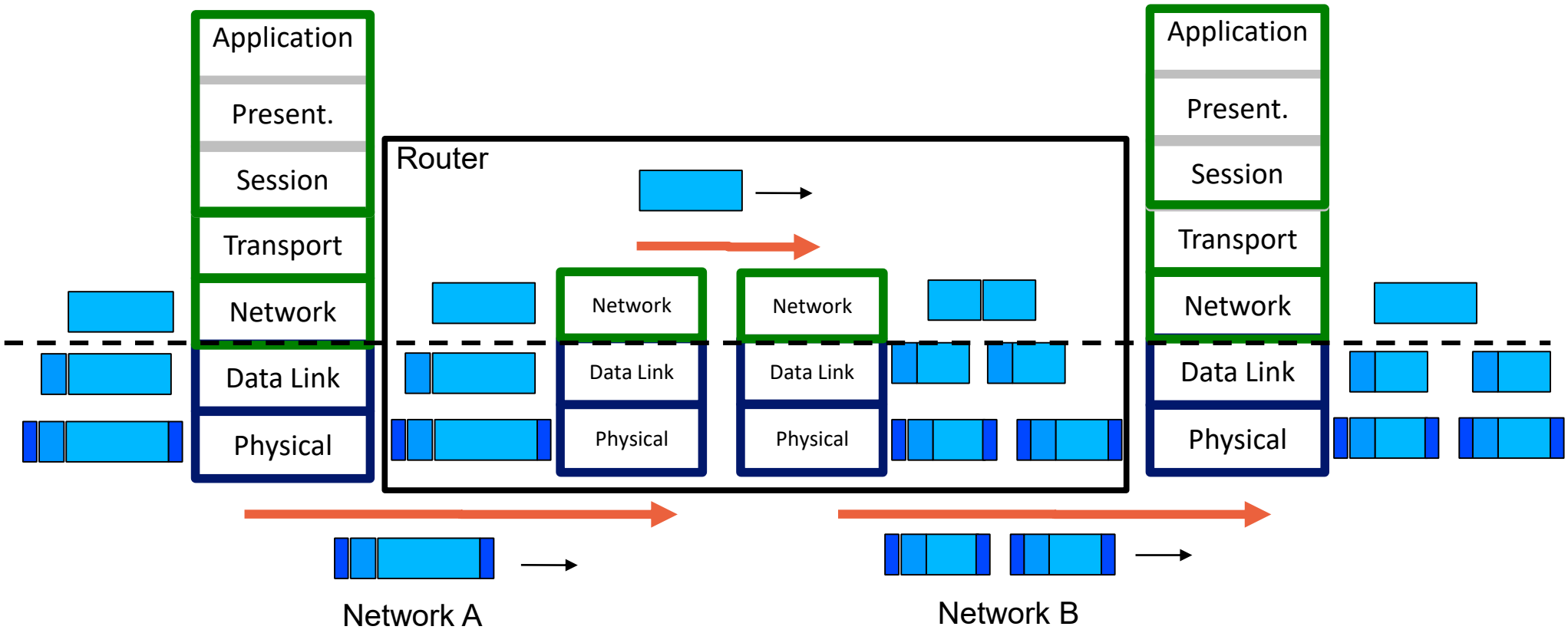


IP – packet routing

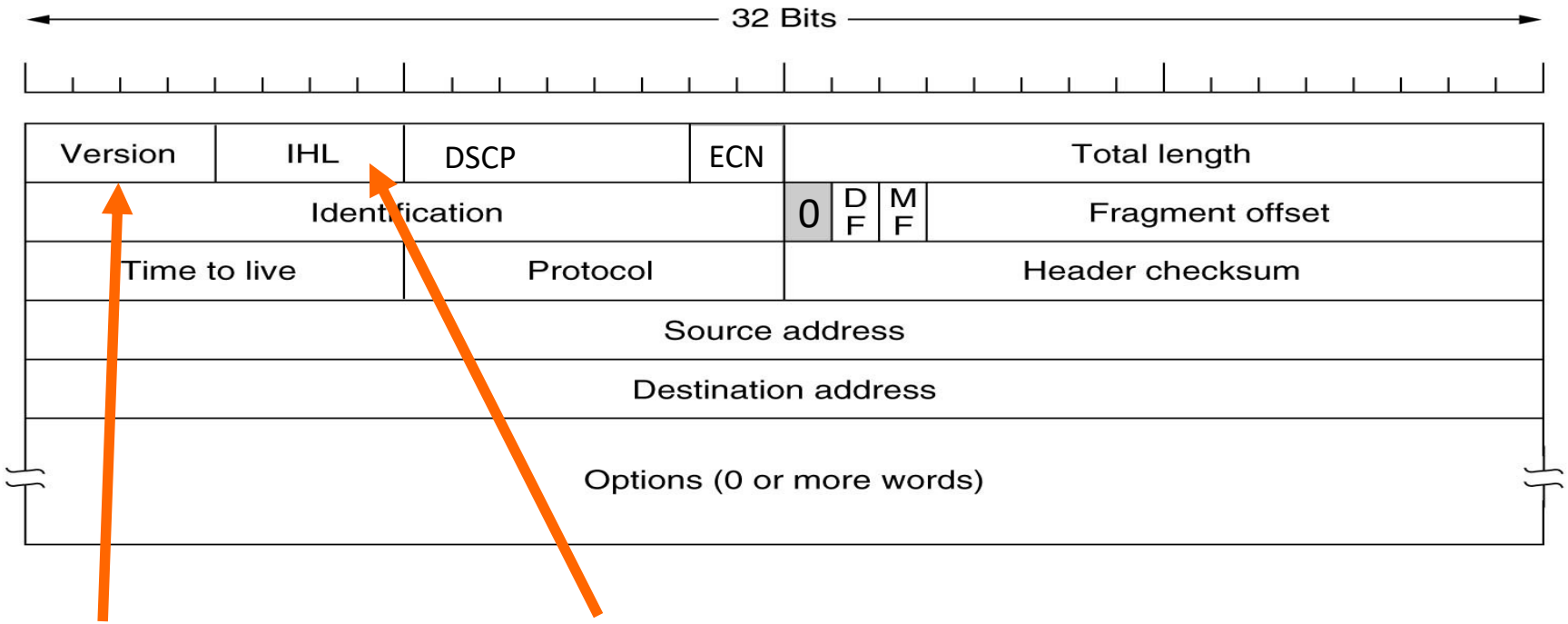
- Example:
  Linux-> /usr/sbin/**traceroute** www.publico.pt
  Windows-> **tracert** www.publico.pt



IP - packet fragmentation / re-assembly



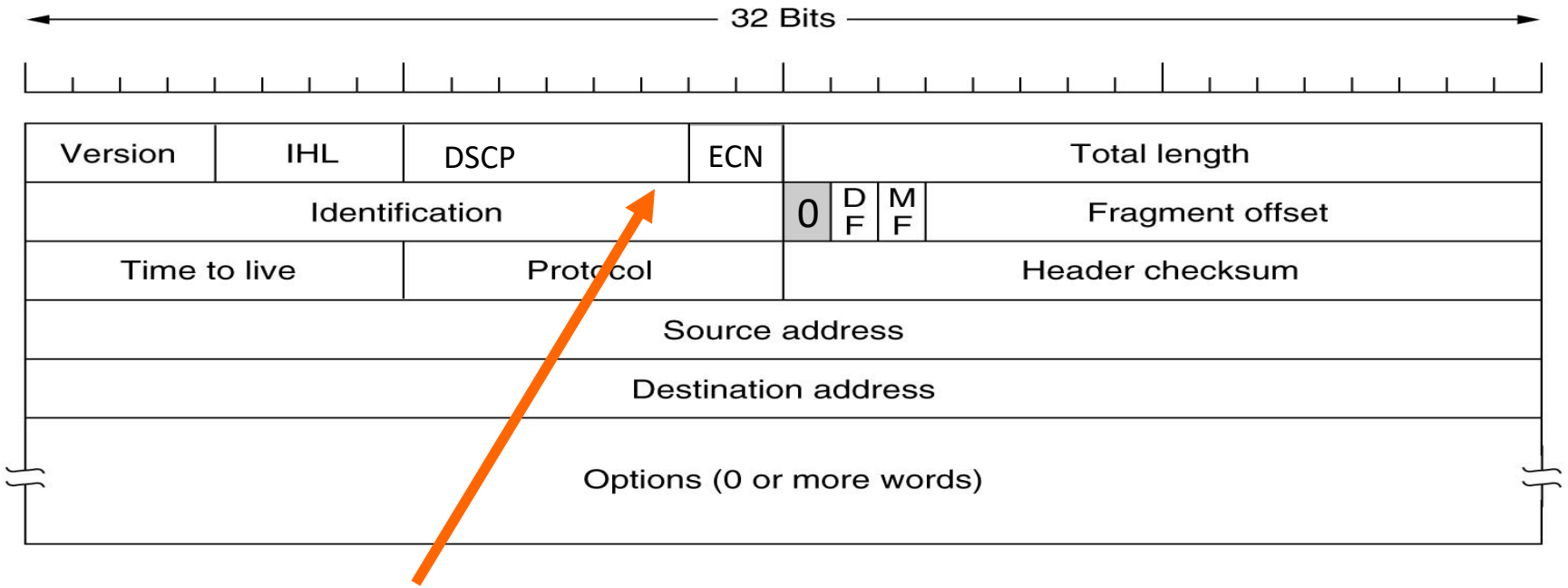
The IP packet



Version: IPv4, IPv6

IHL (Internet Header Length):
multiples of 4 Bytes → $5 \leq IHL \leq 15$ (20-60 Bytes)

The IP packet



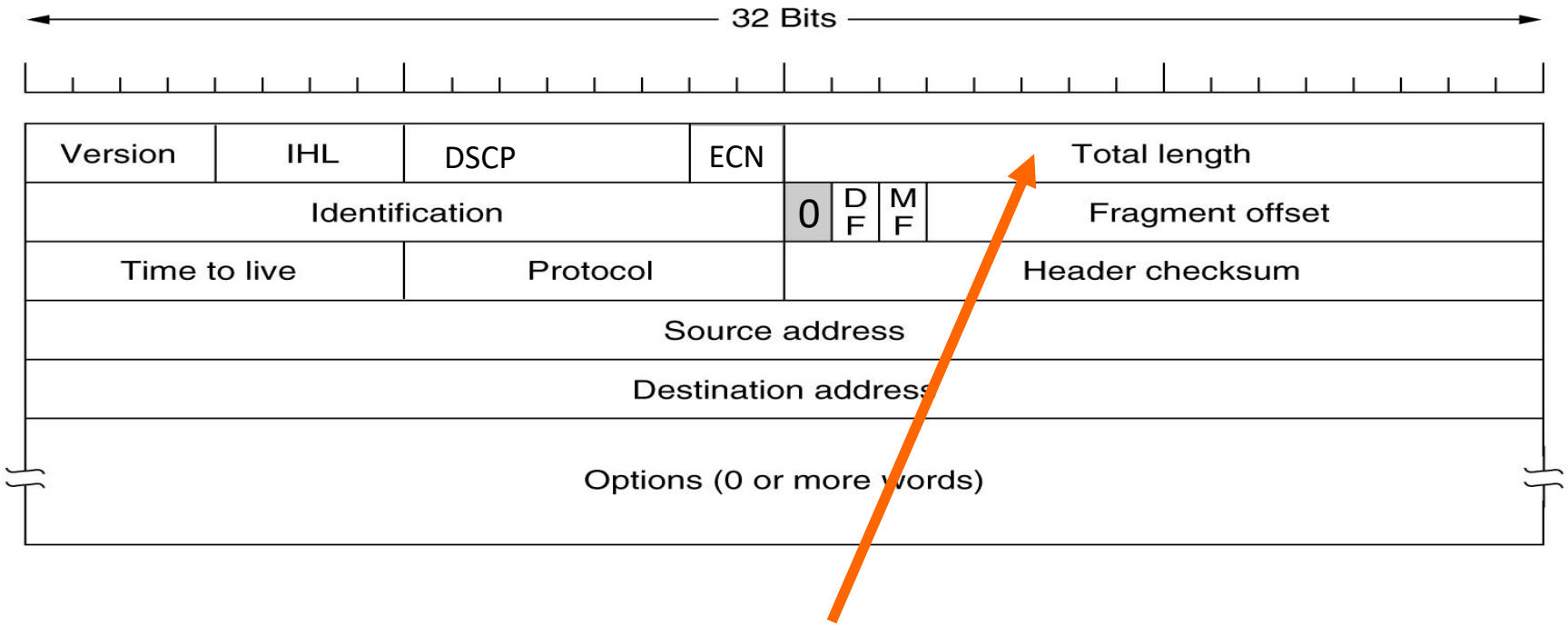
Differentiated Service Code Point (DSCP):

Allows defining up to **64 QoS classes** (voice, video, email, files)

Explicit Congestion Notification (ECN):

Signals congestion without dropping packets

The IP packet

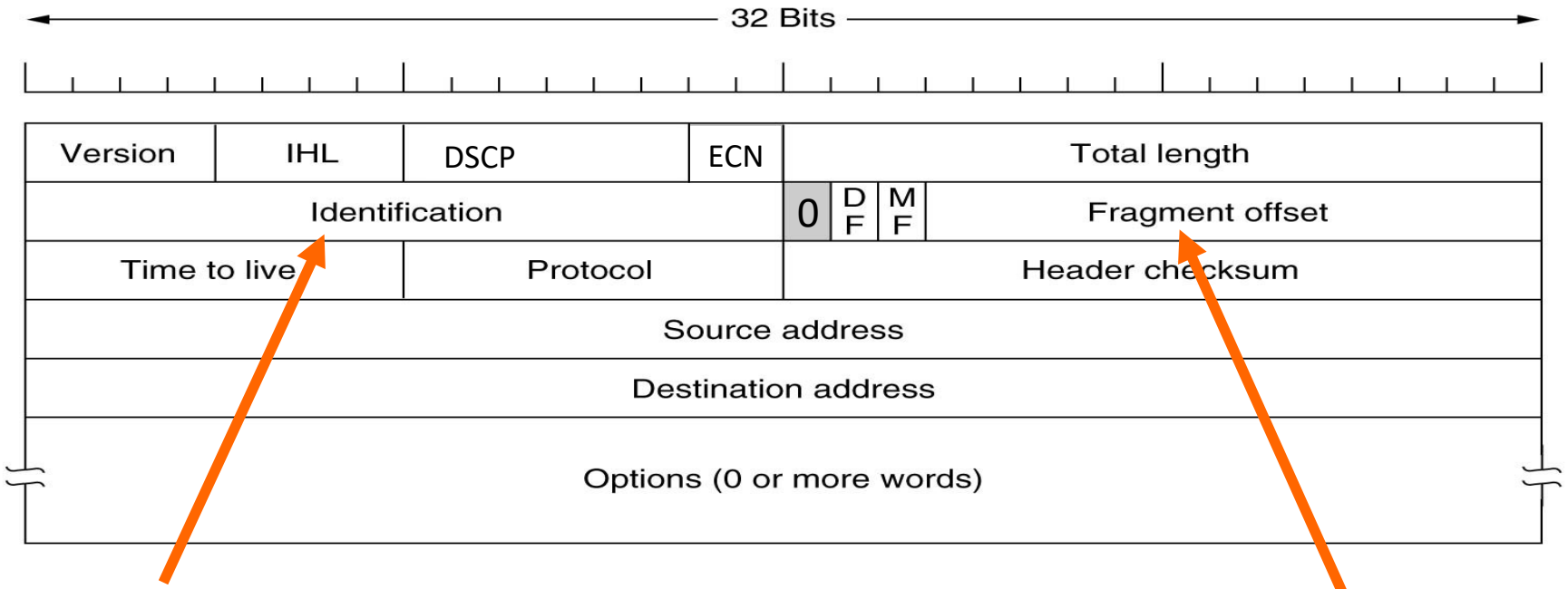


Total Length:

Total packet length including header

IP packets 20 B – 65535 B

The IP packet



Identification:

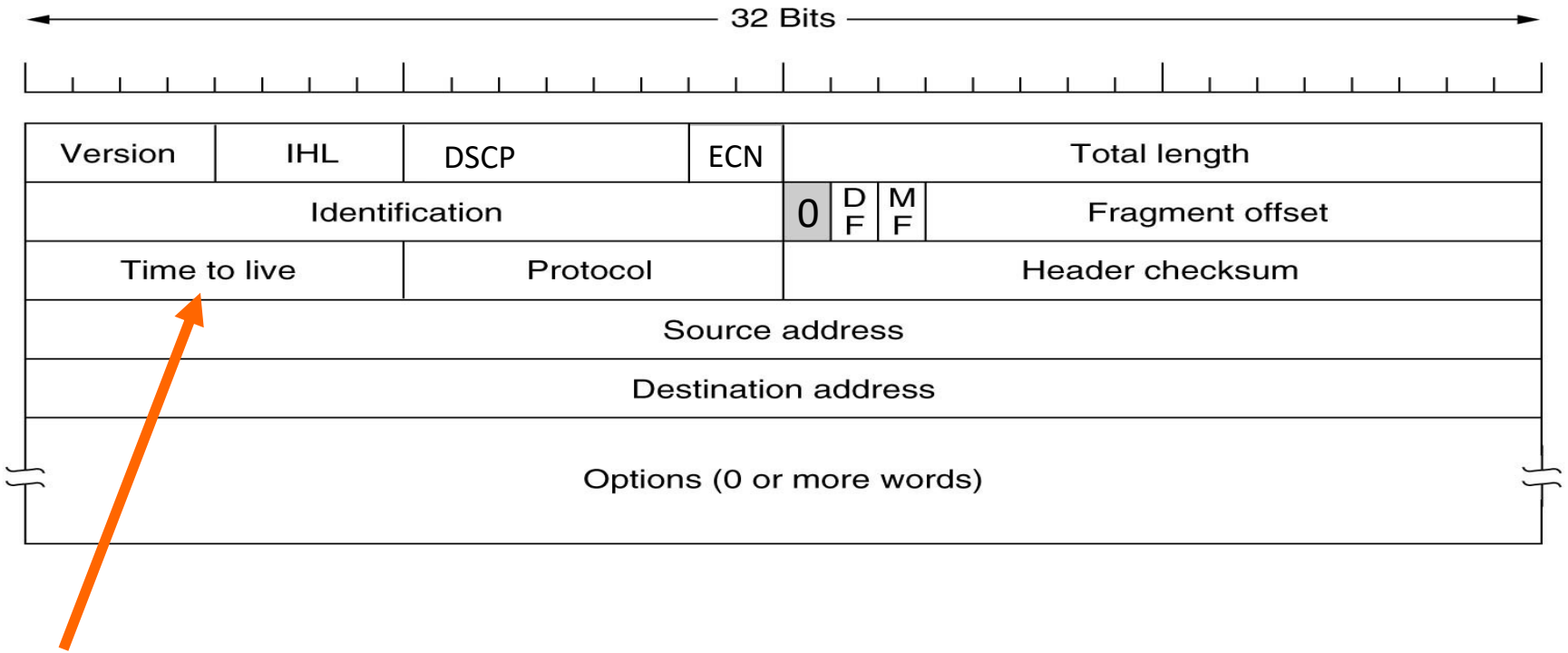
Numbers the original datagrams to identify its fragments

Fragment offset:

With fragmentation → offset of this fragment in the data of the original datagram

DF – Don't Fragment ; MF – More Fragments

The IP packet

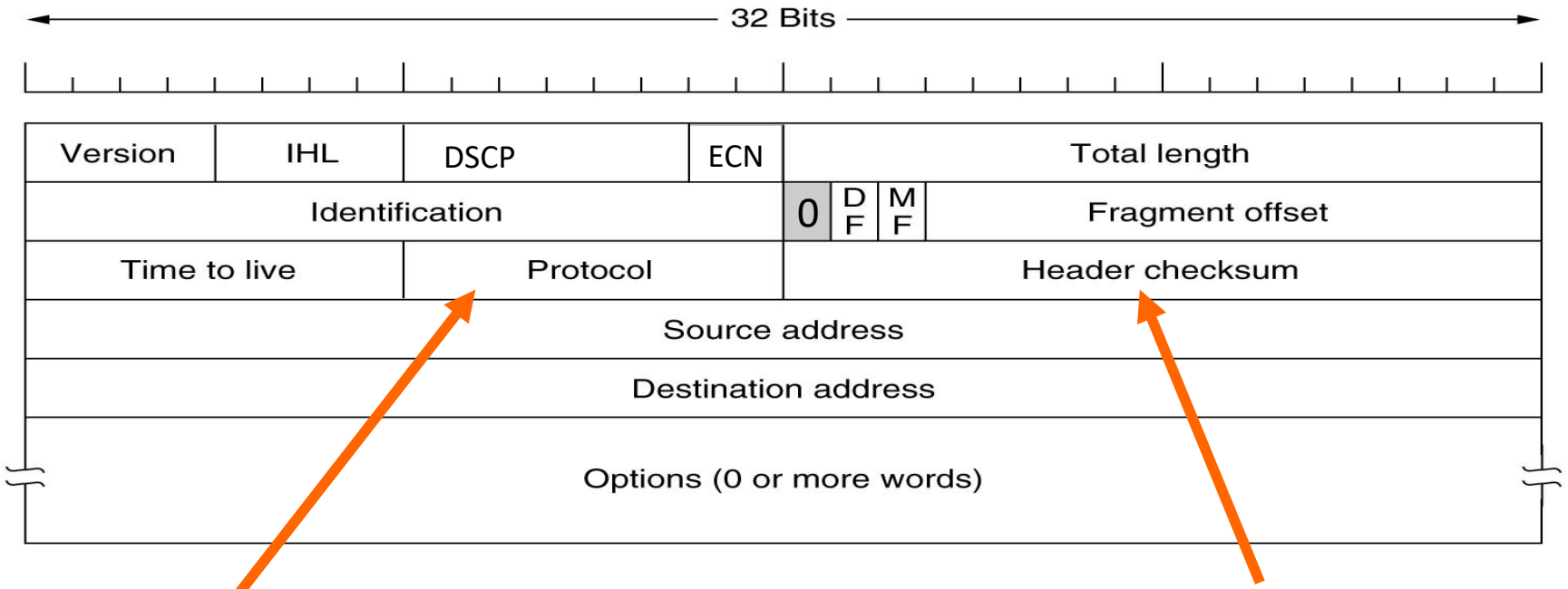


Time-To-Live (TTL):

Despite the name “time”, this is a counter of routing hops (“-1” in each router)

When reaching 0, the packet is dropped (the sender is signaled)

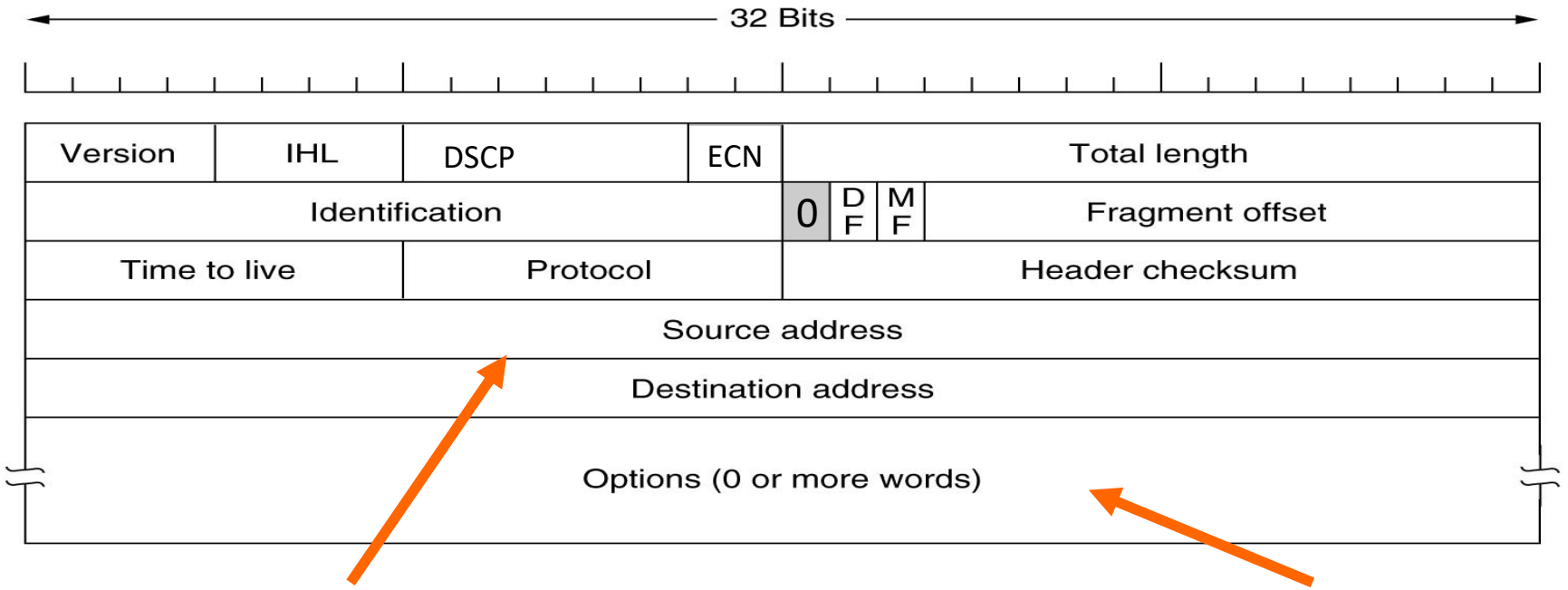
The IP packet



Protocol:
Identifies the higher layer protocol that should handle this packet
ex. TCP 0x06, UDP 0x11…

Header Checksum:
Cyclic Redundancy Check (CRC) of the packet header

The IP packet



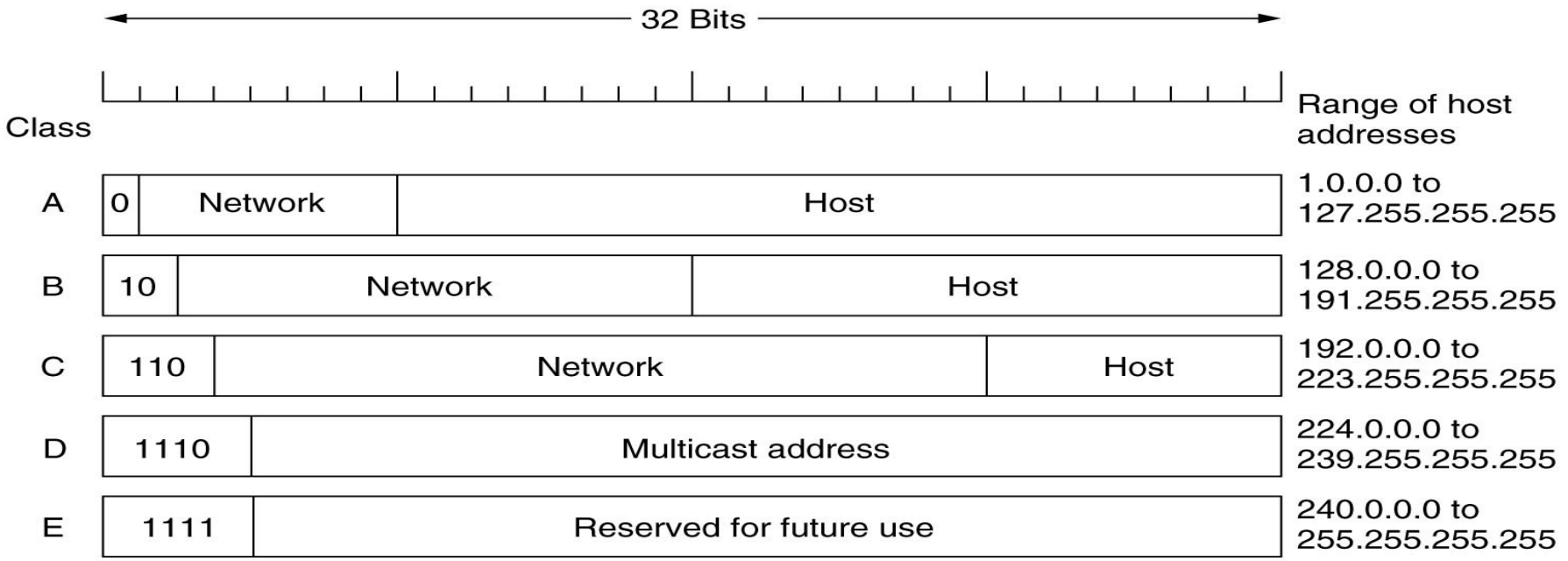
Source / Destination Addresses:
IP addresses of the end-to-end stations

Options:
Frequently unused or
1B Option Type (plus 3B padding)

Note: when communicating through routers, the IP addresses are kept but the DLL addresses (MAC) are updated to the respective interfaces

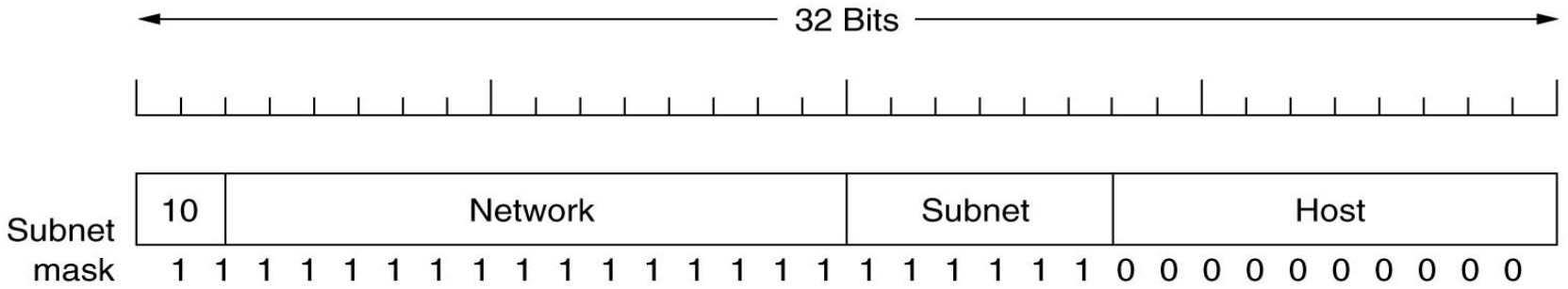
IP addresses

- **IPv4-** 32 bit addresses; **IPv6**- 128 bit addresses
- **One address** ⇔ one network **interface**
- **Classes** of addresses (A, B, C, D and E)
  - for a more efficient use of the address space (although not so used)

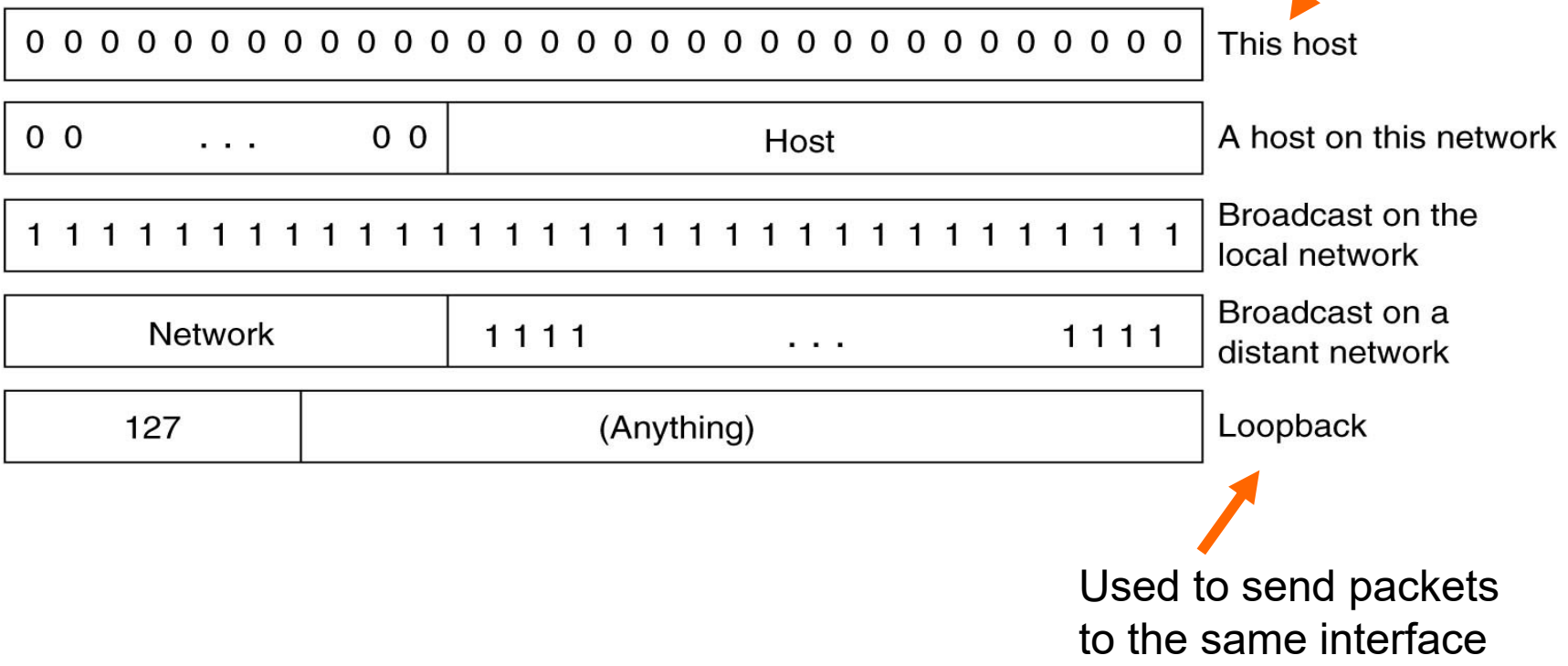


Sub-networks

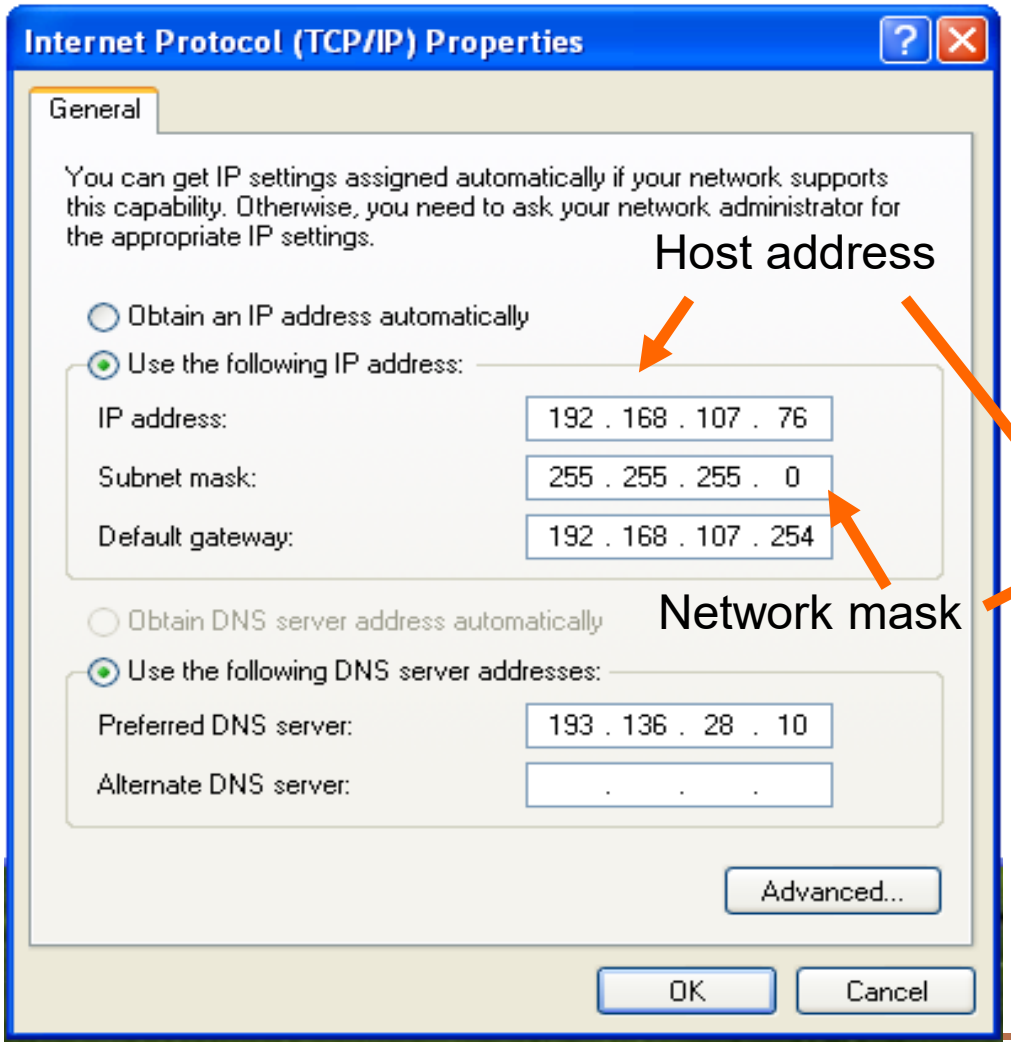
- **Variable Length Subnet Mask**
  - Any number of bits can be used to defined a sub-network
    - » Better control of the sub-network size
    - » Particularly useful in the allocation of addresses by ISPs to client organizations
  - Currently extended with **Classless Inter-Domain Routing (CIDR)**
  - Ex. 255.255.252.0 → 4 times more hosts than a class C

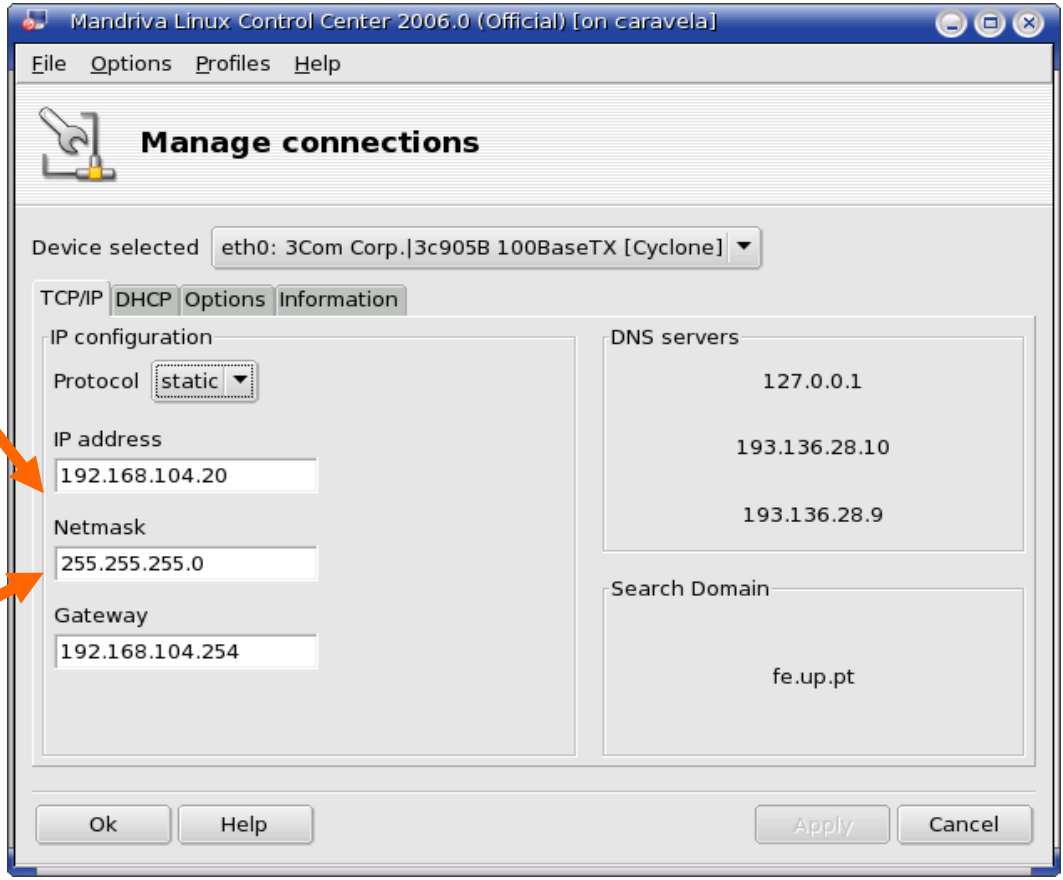


Special IP addresses



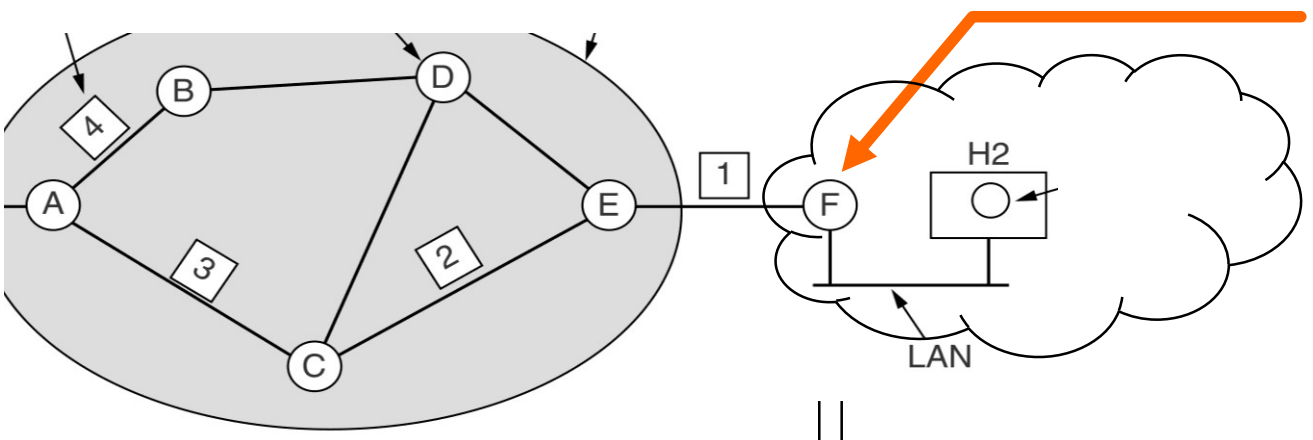
Configuring an interface





Default Gateway

- **Local communications**
  - Destination address AND network mask = Source address AND network mask
  - Ex: 192.168.113.28 && 255.255.255.0 = 192.168.113.50 && 255.255.255.0
- **External communications**
  - Destination address AND network mask ≠ Source address AND network mask
    - » **Destination in a different network ➔ send packet to *Default Gateway***

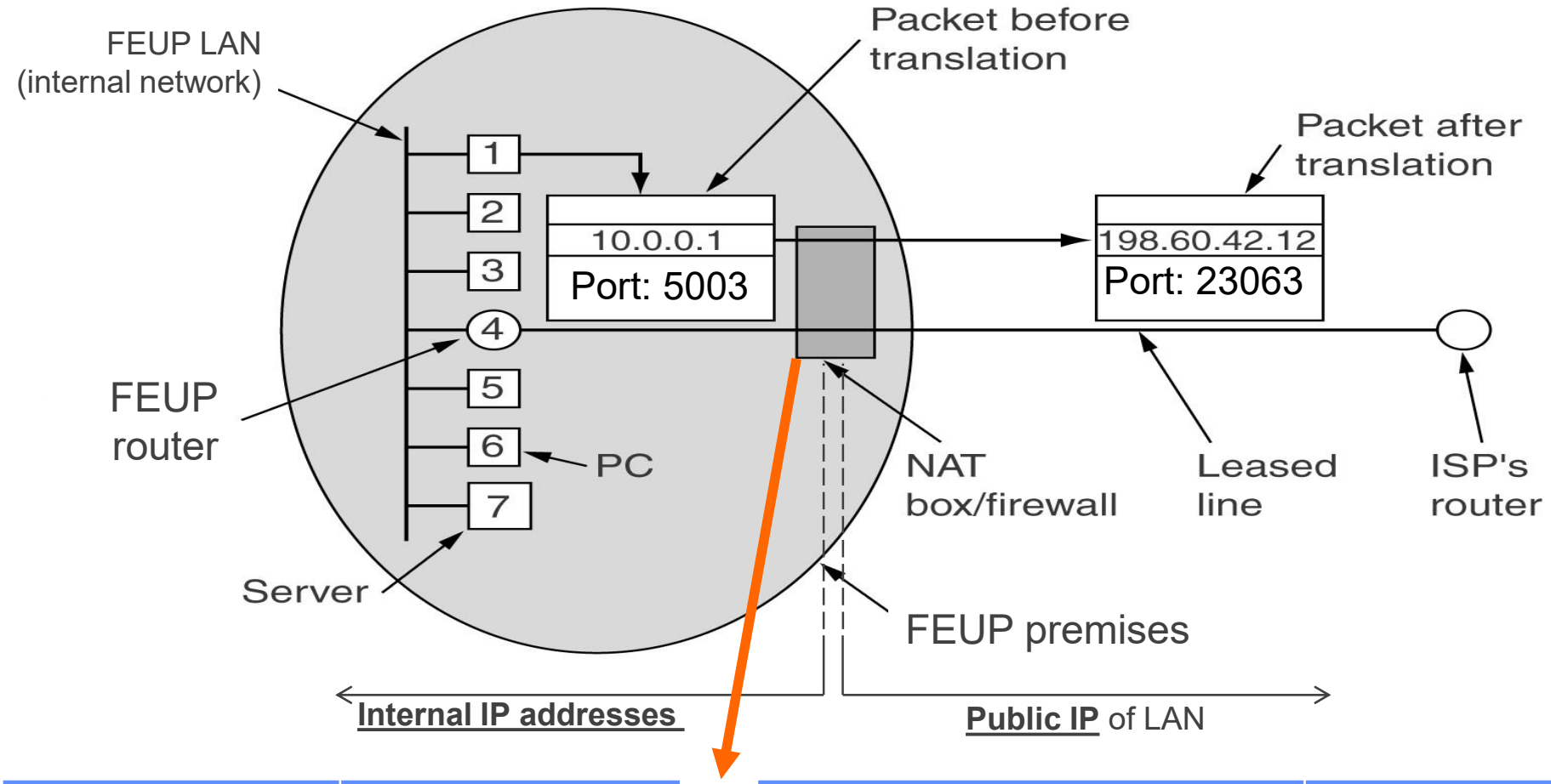


Gateway:
router that connects a network to the Internet

Public IP of LAN

Internal IP addresses
(separate from rest of Internet)

NAT - Network Address Translation

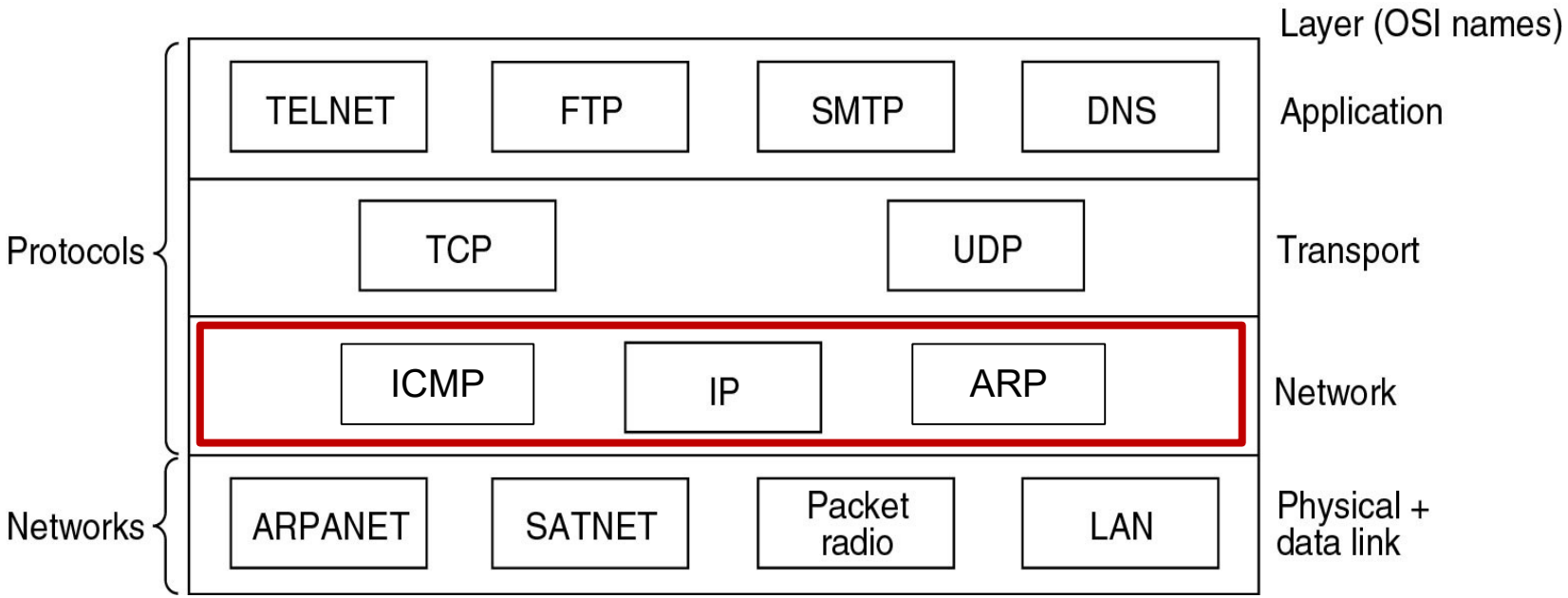


Internal Src IP	Internal Src Port	↔	Public IP	Public Port
10.0.0.1	5003	↔	192.60.42.12 (**FEUP's public IP**)	23063

NAT - Network Address Translation

- **Private Networks**
  - 10.0.0.0 **/8** ← Number of bits of the network mask (compact representation) (10.0.0.0 - 10.255.255.255)
  - 172.16.0.0 **/12** (172.16.0.0 - 172.31.255.255)
  - 192.168.0.0 **/16** (192.168.0.0 - 192.168.255.255)
- NAT allowed reusing addresses in large scale
  - Salvation of IPv4 ! Otherwise the address space would have been exhausted long ago
- Disadvantages
  - Hosts under NAT cannot be servers
  - Breaks the end-to-end principle and the layers isolation

Internet network layer protocols



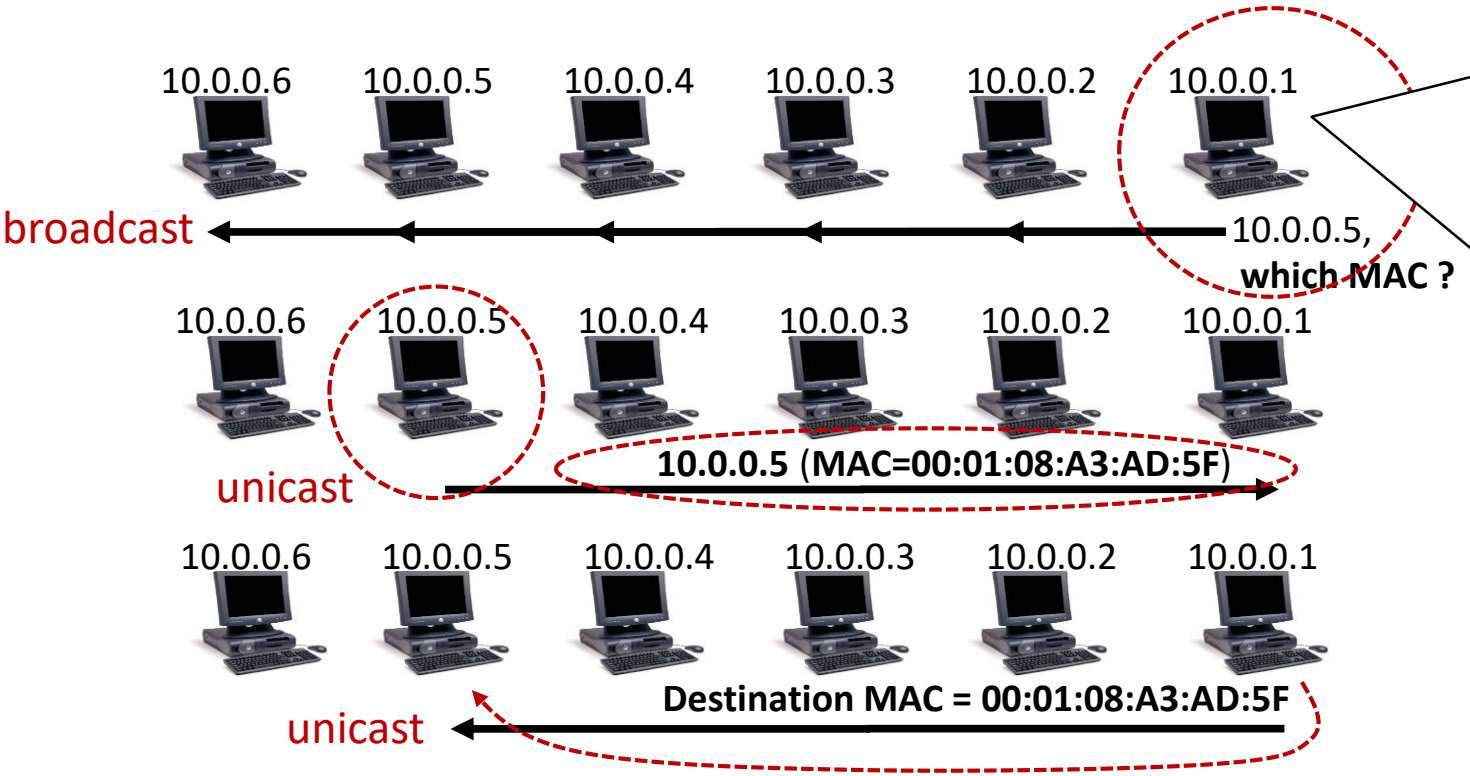
ICMP - Internet Control Message Protocol

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

Ping

ARP - Address Resolution Protocol

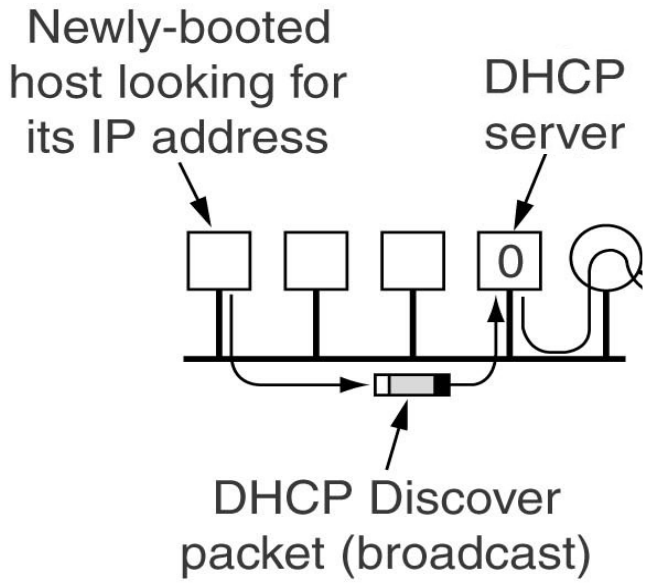
- MAC addresses are needed for Data Link Layer exchanges
- ARP – keeps IP addresses separated from MAC addresses
  - Carries out the correspondence dynamically when needed (using broadcast)



1. I just came in to this local network.
2. I was told to to talk to 10.0.0.5, but don't know its Level 2 (data link) address.
3. If I broadcast, everyone will spend time and resources decapsulating the packet and checking if the Level 3 (IP) destination address is theirs.
4. If I learn the MAC, this can be avoided!

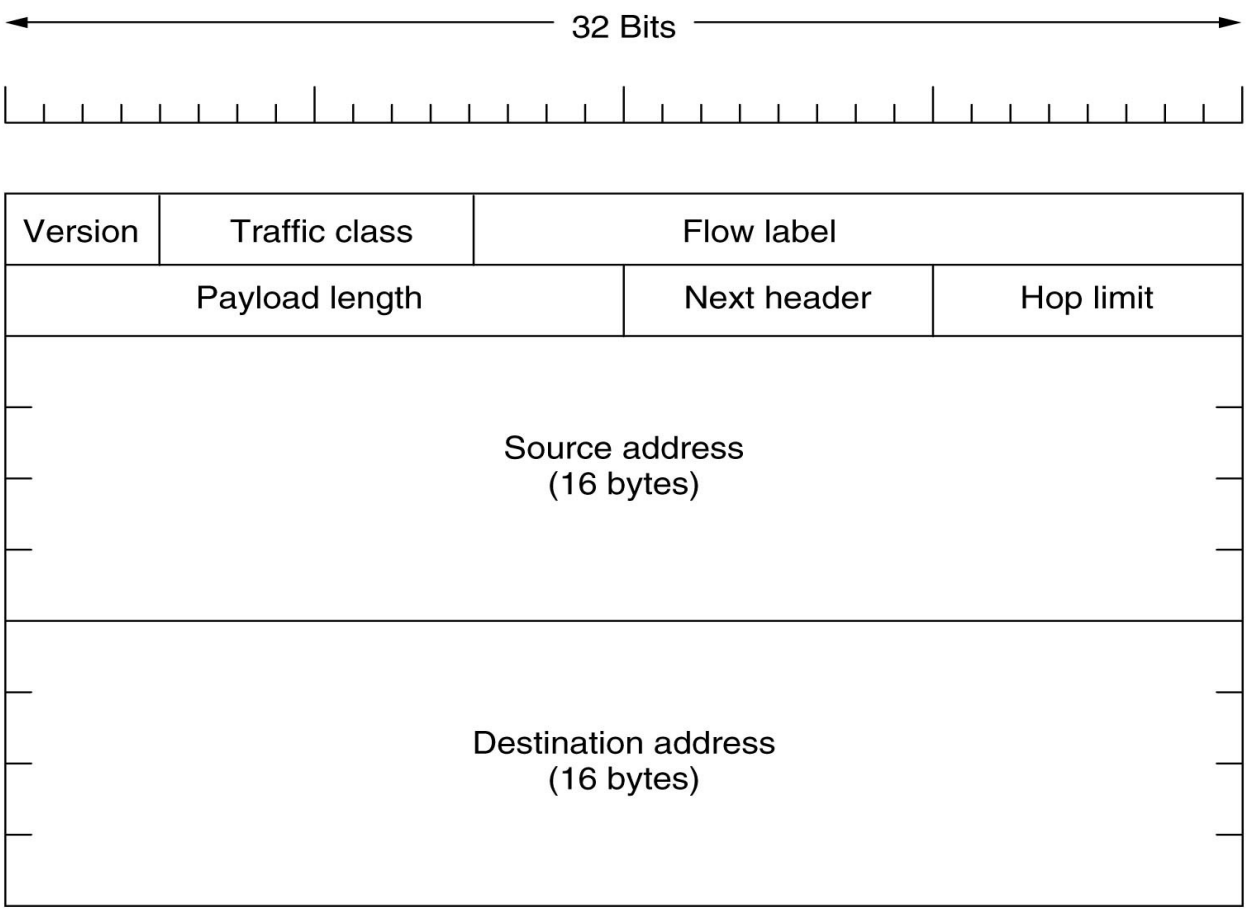
RARP – BOOTP - DHCP

- **RARP**: Reverse Address Resolution Protocol *(obsolete)*
- **BOOTP**: BOOTstrap Protocol
- **DHCP**: Dynamic Host Configuration Protocol (uses BOOTP)



IPv6

- **16Byte addresses !**
  - ~7k addresses/m2 of Earth surface!!!
  - Elimination of NATs
  - Enabling of semantic-rich addresses



Bibliography

- Many **online resources**
- **Data and Computer Communications**, W. Stallings, Prentice Hall, 2007 (library)
  - Chapter on "Internetwork Protocols"
- **Computer Networking – A top-down approach**, J. Kurose, K. Ross, Pearson, 2010 (library)
  - Chapter on "Network Layer": sections: 4.1, 4.2 and 4.3
- Use **WireShark**, capture some **IP packets** and observe their **struture**. Also, observe the packets exchanged by **ARP, ICMP and DHCP**.