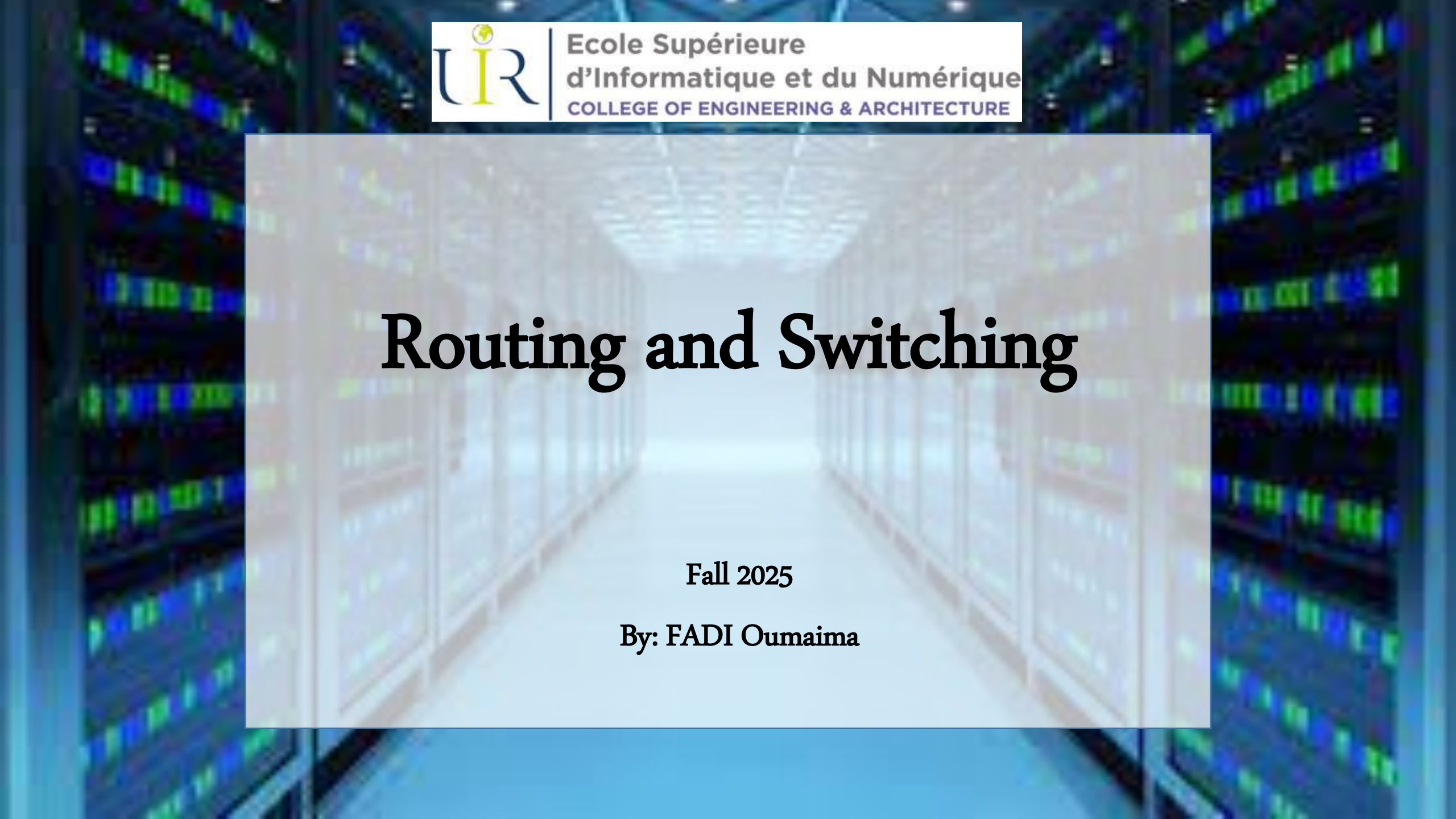


Routing and Switching

Fall 2025

By: FADI Oumaima

Chapter 2 : IP Addressing (IPv4) & ICMP/ARP

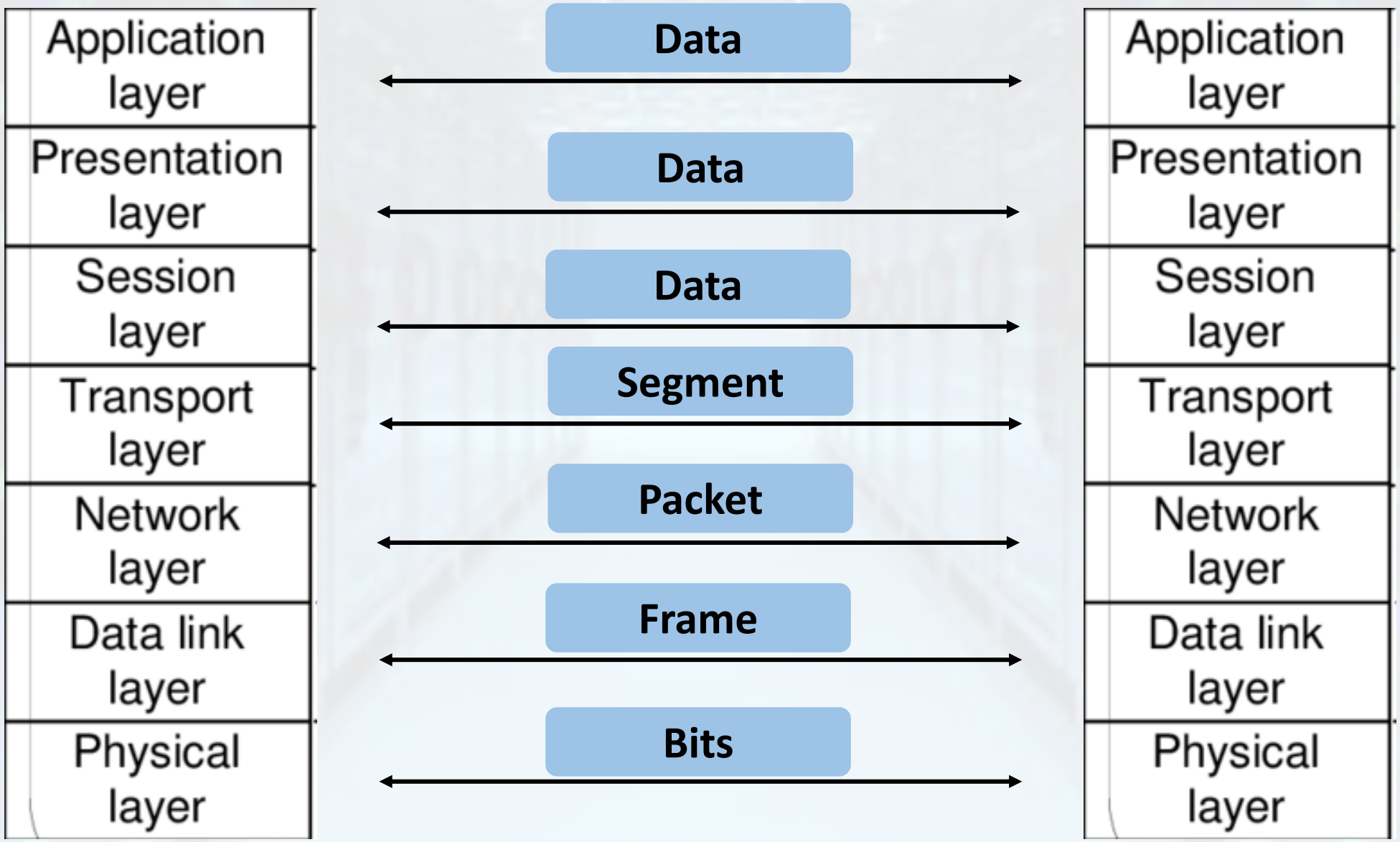
Topics:

- ✓ IPv4 address classes, private vs. public addresses
- ✓ Subnet mask and network/broadcast addresses
- ✓ ICMP basics (ping, traceroute)
- ✓ ARP operation

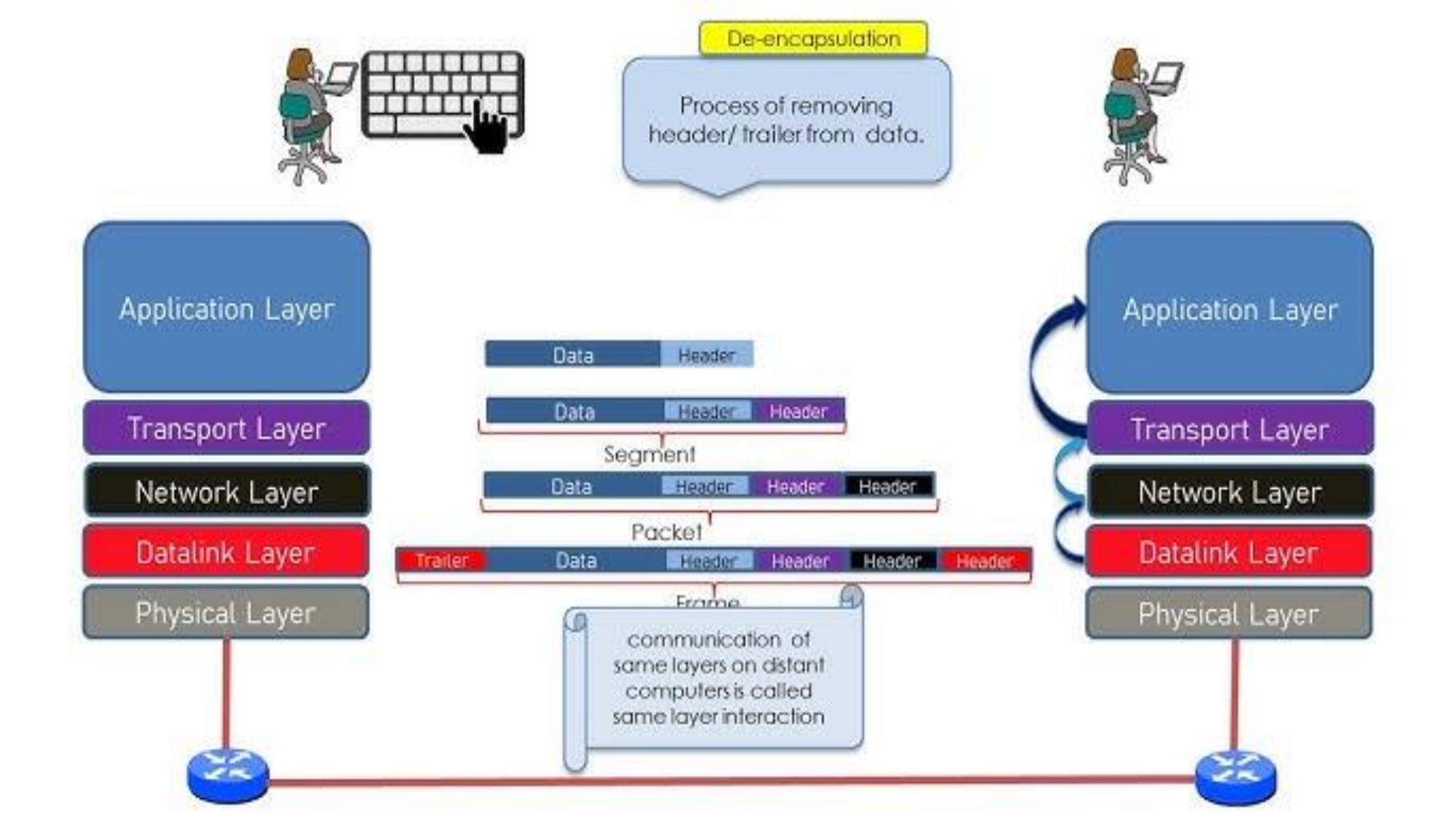
Goals:

- ✓ Explore OSI layers in details
- ✓ Understand IPv4 structure and key Layer 3 protocols.
- ✓ Introduction to Subnet mask and network/broadcast addresses.
- ✓ Grasp the ARP and ICMP protocols mechanisms.

OSI Reference Model (7 layers)



Encapsulation/De-encapsulation and Data Units



Encapsulation/De-encapsulation and Data Units

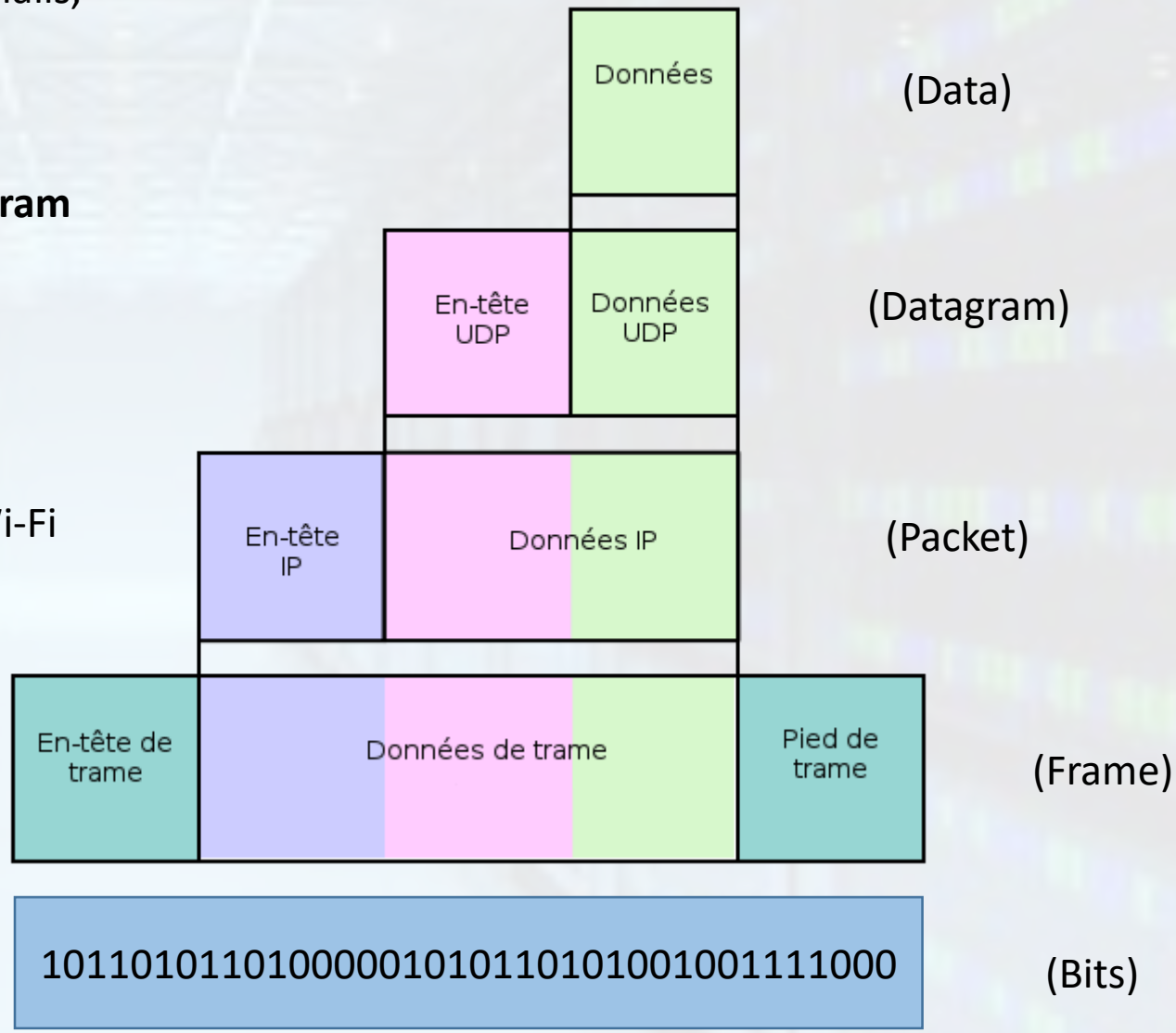
Application Layer: just called **Data** (messages, files, emails, web pages, etc.).

Transport Layer: becomes a **Segment** (TCP) or a **Datagram** (UDP).

Network Layer: becomes a **Packet** (IP packet).

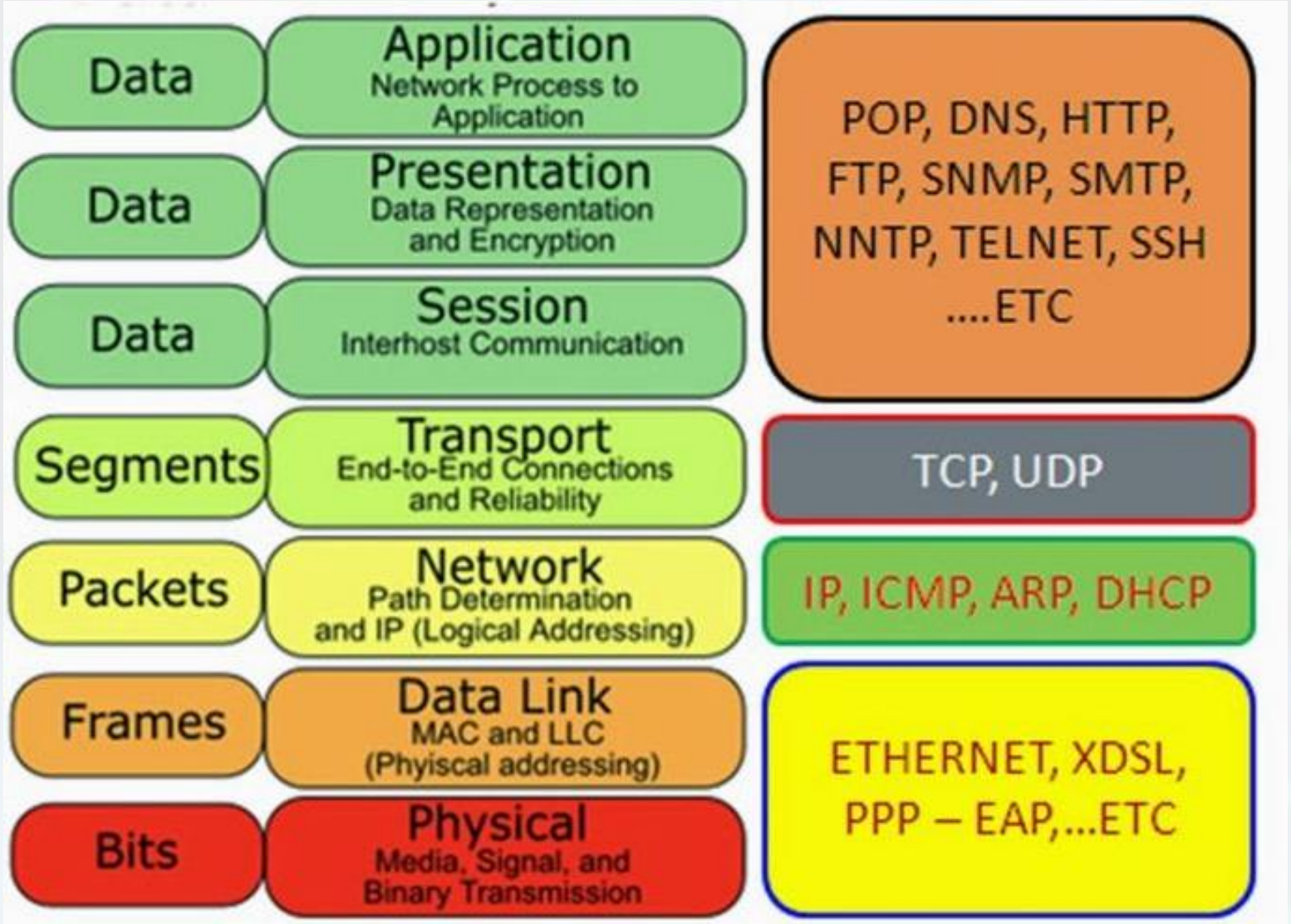
Data Link Layer: becomes a **Frame** (Ethernet frame, Wi-Fi frame).

Physical Layer: becomes **Bits** (0s and 1s sent across the medium).



PS: « Trame » is the frensh word for frame

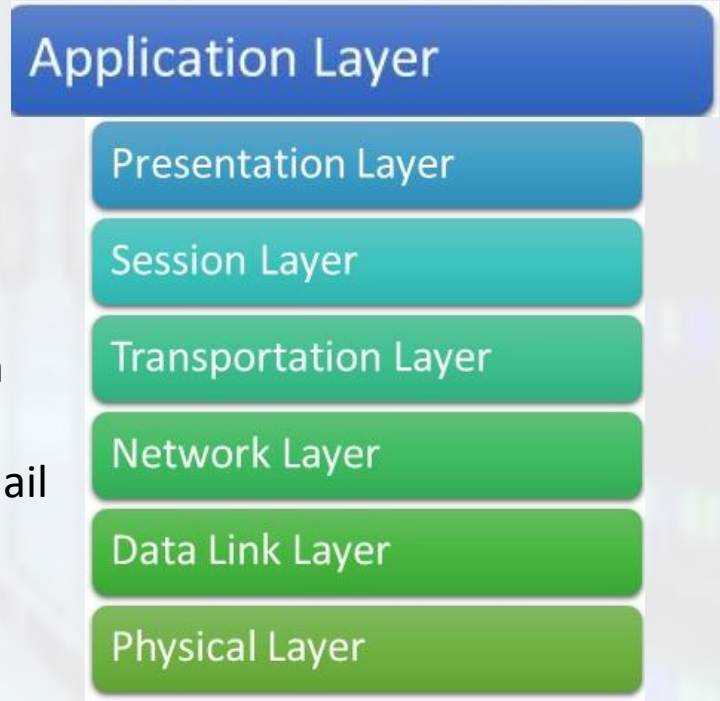
OSI stacks protocols



OSI: Application layer

Acts as an **interface for application access to the network**
This layer contains all the high-level protocols.
This layer transmits messages to the lower layer.
The first protocols to be developed were:

TELNET (virtual terminal protocol): allows a user to remotely log in to a machine to work on it.
FTP (File Transfer Protocol): provides an efficient way to transfer data from one machine to another.
SMTP (Simple Mail Transfer Protocol): enables the sending of electronic mail between two users.
DNS (Domain Name System): allows the assignment and management of domain names.
HTTP (Hypertext Transfer Protocol): used to load web pages on the World Wide Web.



OSI: Transportation layer

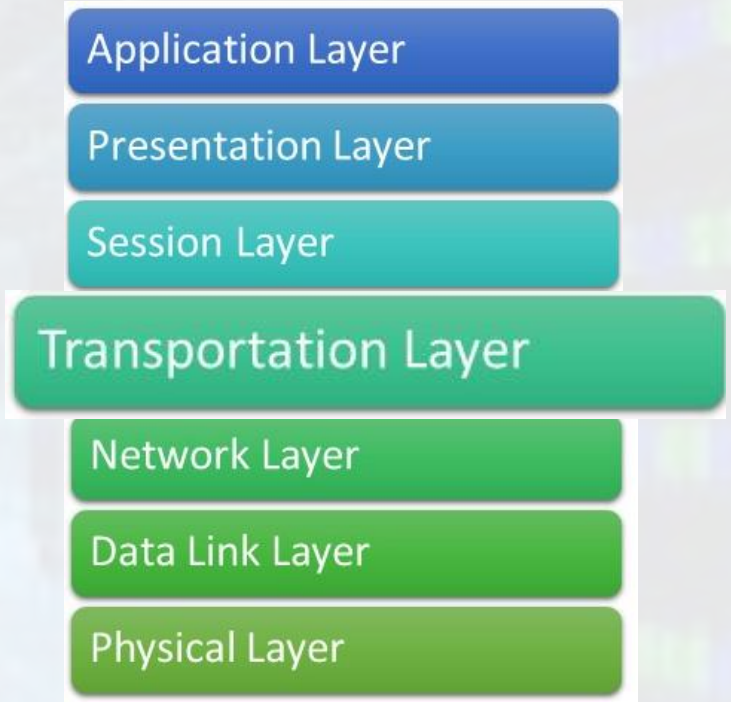
The **Transportation layer** is responsible for establishing a **point-to-point connection** with the remote computer.

Two end-to-end protocols have been defined for this layer:

TCP (Transmission Control Protocol)

UDP (User Datagram Protocol)

At a minimum, it must ensure that the data transmitted to the remote host is properly delivered to the correct application.



OSI: Nework layer

This layer contains the **IP protocol**, responsible for communicating with other machines using **packet switching**.

The Network layer must provide:

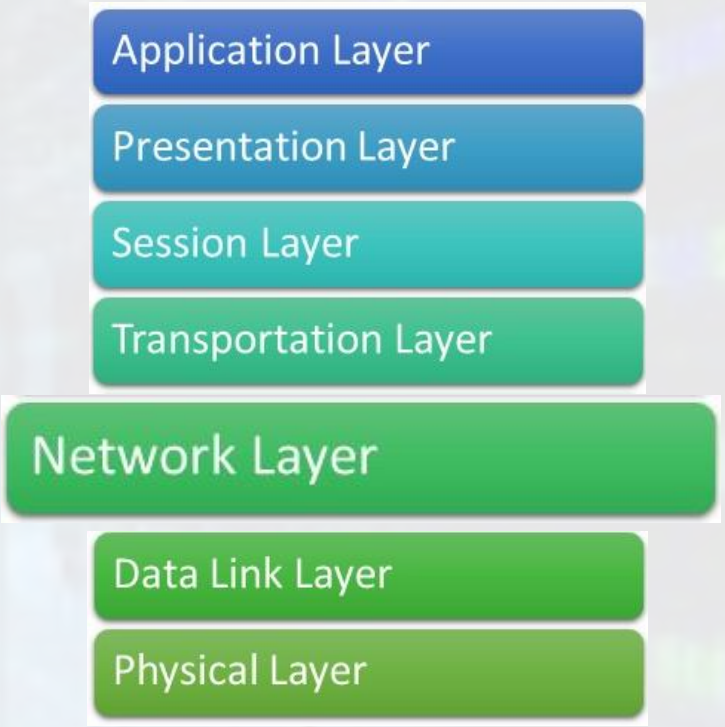
Addressing of packets: via the **IP protocol**.

Address resolution: using **ARP/RARP protocols**.

Packet injection into any type of network: by handling **fragmentation (MTU)**.

Support for control messages: with the **ICMP protocol**.

Independent routing of packets toward their destination: using **routing protocols** such as **RIP, OSPF**, etc.



OSI: Data link layer

Ensures the transmission of **frames** over a **point-to-point link** → no routing at this level.

Provides **secure exchanges** between directly connected devices.

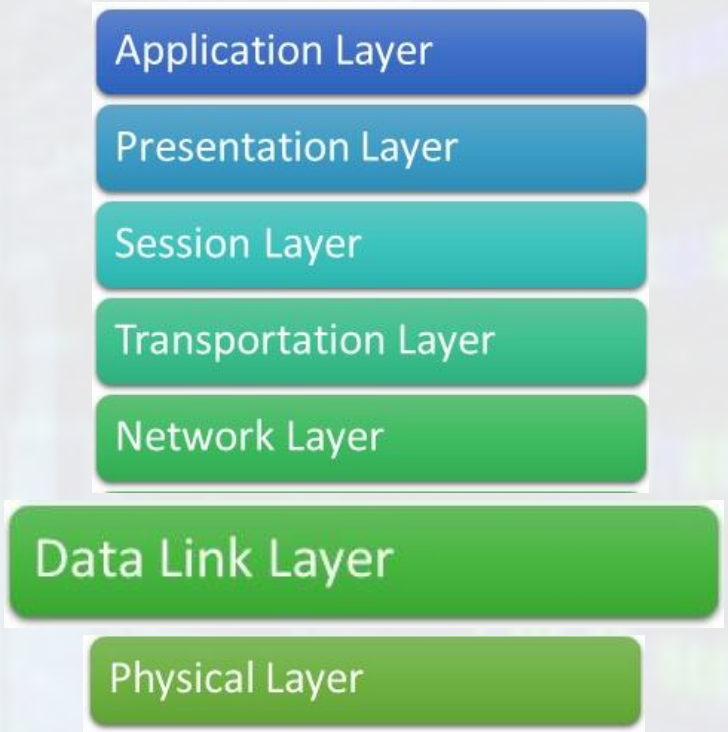
Manages **access to the transmission medium**.

Converts a raw stream of bits into **frames** that can be processed efficiently (including error detection, loss detection, and dialogue synchronization).

For **LANs**, the Data Link Layer is divided into two sublayers:

LLC (Logical Link Control): manages flow control, error detection, and communication with the Network Layer.

MAC (Medium Access Control): manages how devices share and access the transmission medium (e.g., Ethernet, Wi-Fi).



OSI: Data link Sub layers

The Data Link Layer in LANs is divided into two sublayers:

LLC (Logical Link Control): handles communication with the Network layer and provides flow/error control.

MAC (Medium Access Control): controls how devices access and share the transmission medium.

The **MAC sublayer** has been the subject of three IEEE standards:

802.3: Bus network using **CSMA/CD** (Carrier Sense Multiple Access with Collision Detection) → basis for Ethernet.

802.4: Token Bus (less common today).

802.5: Token Ring (IBM networks, now obsolete).

Protocols assigning

- ✓ A computer always runs multiple programs (**processes**)
- ✓ A process waiting for network data is called:

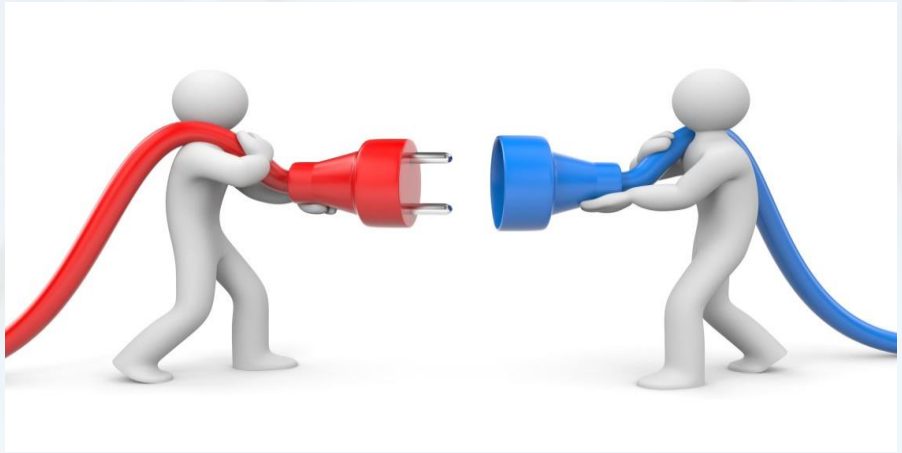
Daemon (on Unix)

Service (on Windows)

- ✓ The process **“listens”** on the network for connections
- ✓ The **Transport layer** must deliver data to the **correct process**

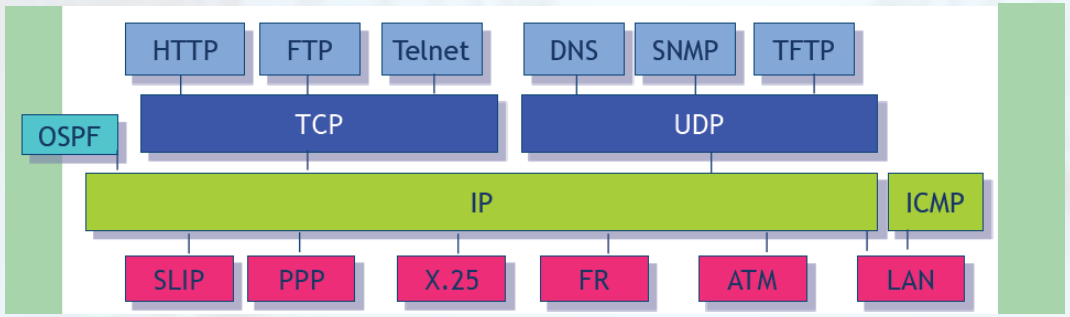
Protocols assigning

- ✓ A process is located in the system by a port
- ✓ Identified by a 16-bit number → **65 535** possible ports
- ✓ Each process is assigned a unique port number
- ✓ To reach a process, its port number must be specified
- ✓ The **Transport** layer assigns the port number to a connection



Protocols assigning

- In general, the well-known port numbers are between **1 and 1023**.
- The list of port numbers is recorded under Unix in the file **/etc/services**.
- Some port numbers are fixed and always assigned to the same application. These are called **“well-known ports.”**
- The well-known ports are managed by the **IANA** (Internet Assigned Numbers Authority)
- Examples: **FTP: 21 ; Telnet: 23 ; SMTP (mail): 25 ; HTTP: 80 ; POP: 110**

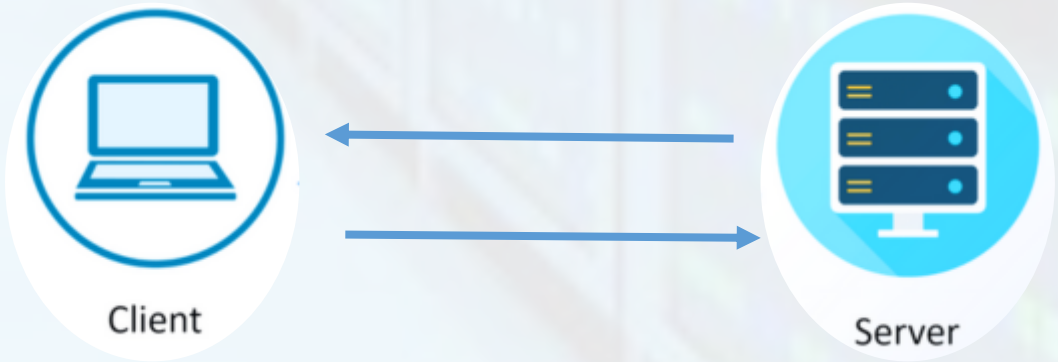


Socket

- In a symmetrical way, to connect to a given server, you must use a **client**.
- The client will open a connection on the client computer also using a **port number**.
- To establish a client/server connection, at least **4 parameters** are required:

1. The IP address of the client
2. The port number of the client
3. The IP address of the server
4. The port number of the server

- The association: **{protocol, destination IP address, source port, source IP address}** is called a **socket**.
- A socket describes a connection between two machines.



Frame: Ethernet (IEEE 802.3): Mac @

Format:

Six numbers coded in hexadecimal, separated by “ : ”

Example: 00 : D3 : FF : 17 : 1E : 03

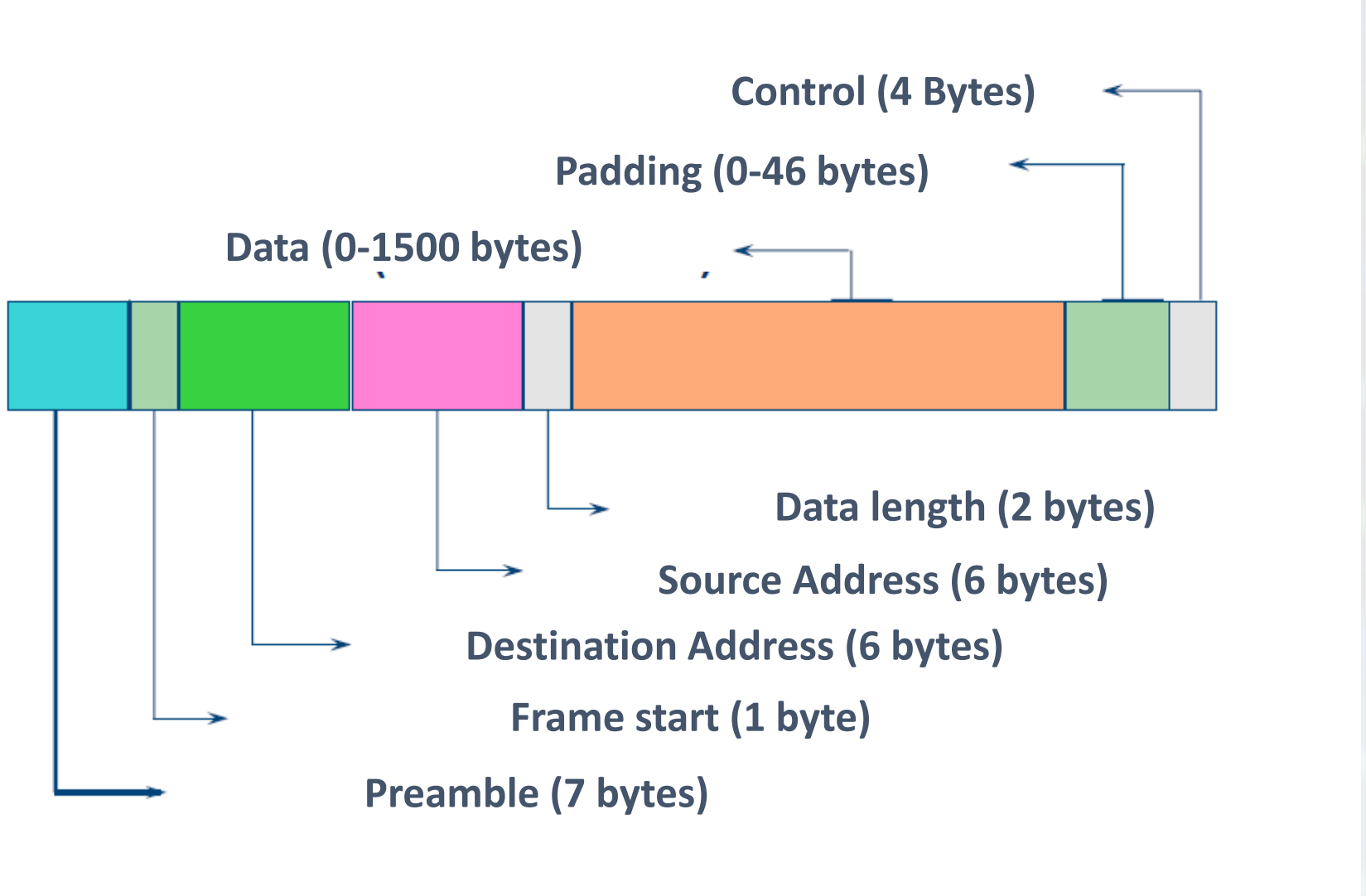
Characteristics:

48 bits or 6 bytes

Global uniqueness

The first 3 bytes indicate the manufacturer

Frame: IEEE 802.3



Frame: IEEE 802.3

As with IP addresses, Ethernet addresses can be:

– **Unicast**: station address, individual address

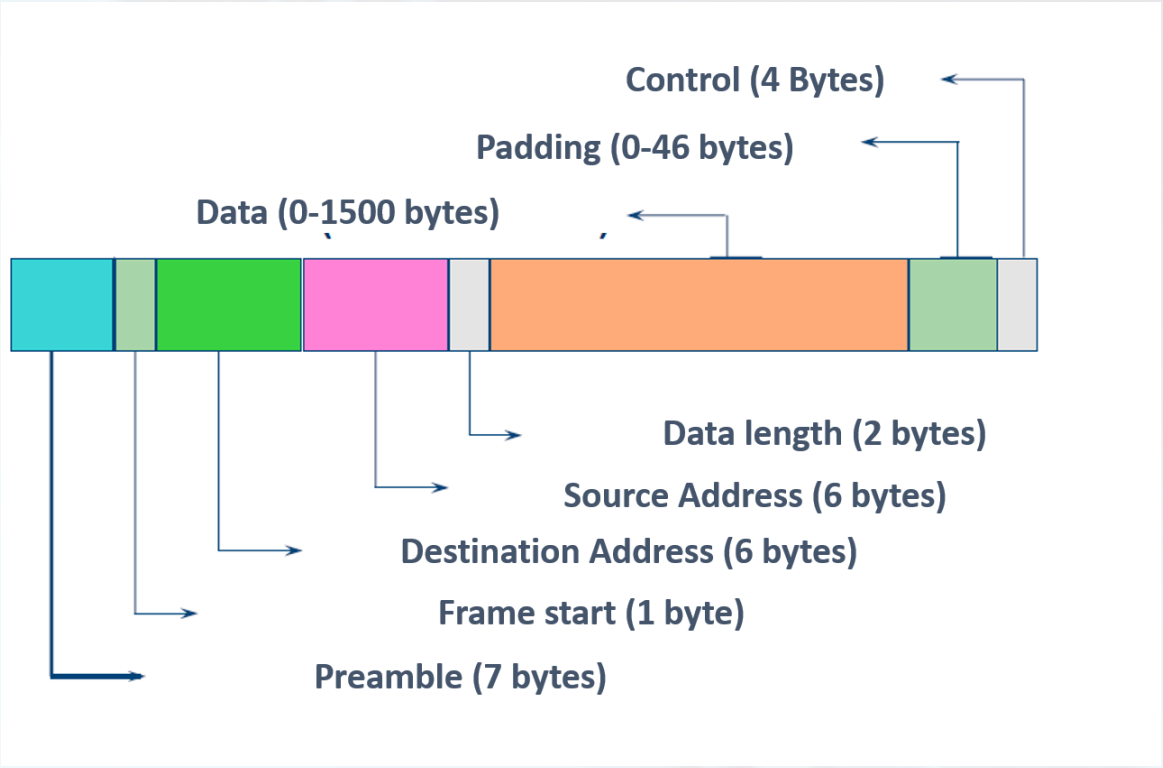
– **Broadcast**: generalized broadcast address to all machines

! The broadcast address in Ethernet networks, as with IP addressing, is composed entirely of 1s:

– FF:FF:FF:FF:FF:FF

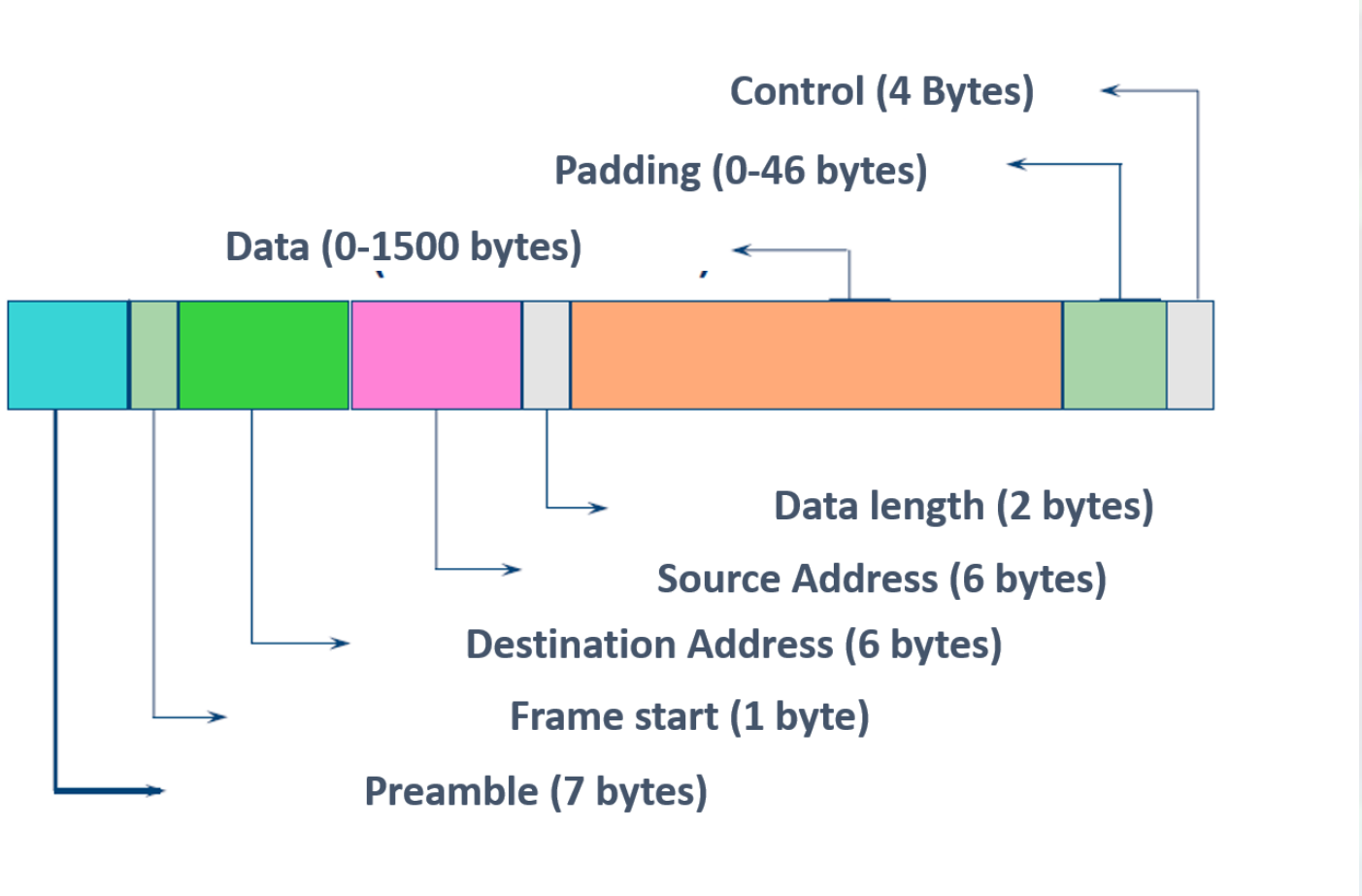
– **Multicast**: group address

– Ranges: 01-00-5E-00-00-00 to 01-00-5E-7F-FF-FF



Frame: IEEE 802.3

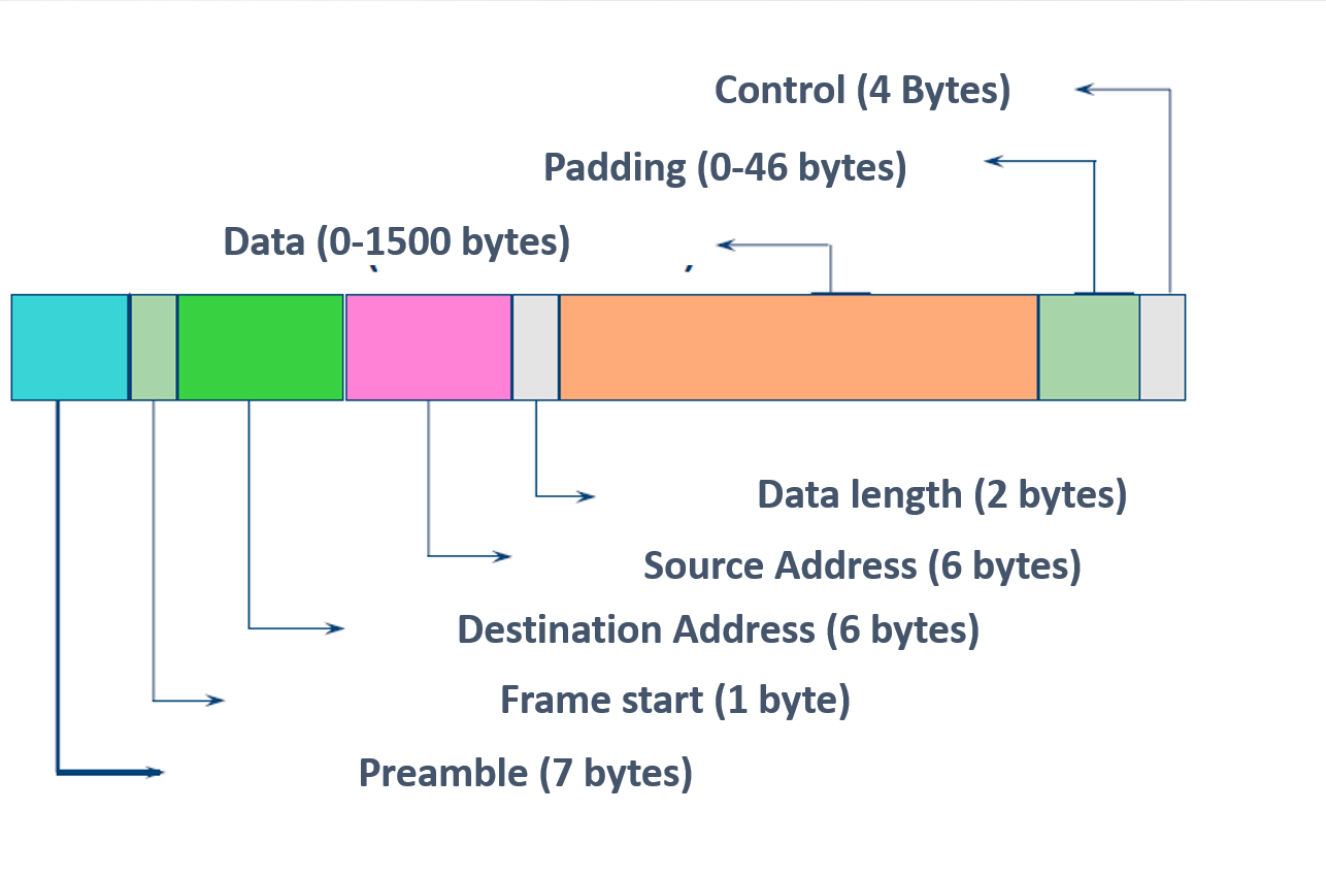
Preamble:
56 bits = 7 × (10101010)
Synchronization bit
Start of frame delimiter (SFD)
8 bits = 10101011



Frame: IEEE 802.3

Ethernet or MAC Addresses
Destination address:
- Unicast address
- Multicast address
- Broadcast address

Source address: Unicast address
Length of the data field:
- Between 1 and 1500 **bytes**



Frame: IEEE 802.3

Data

Padding (bunch of 0 s)

Exists if data < 46 bytes

Completes the frame length to 64 bytes

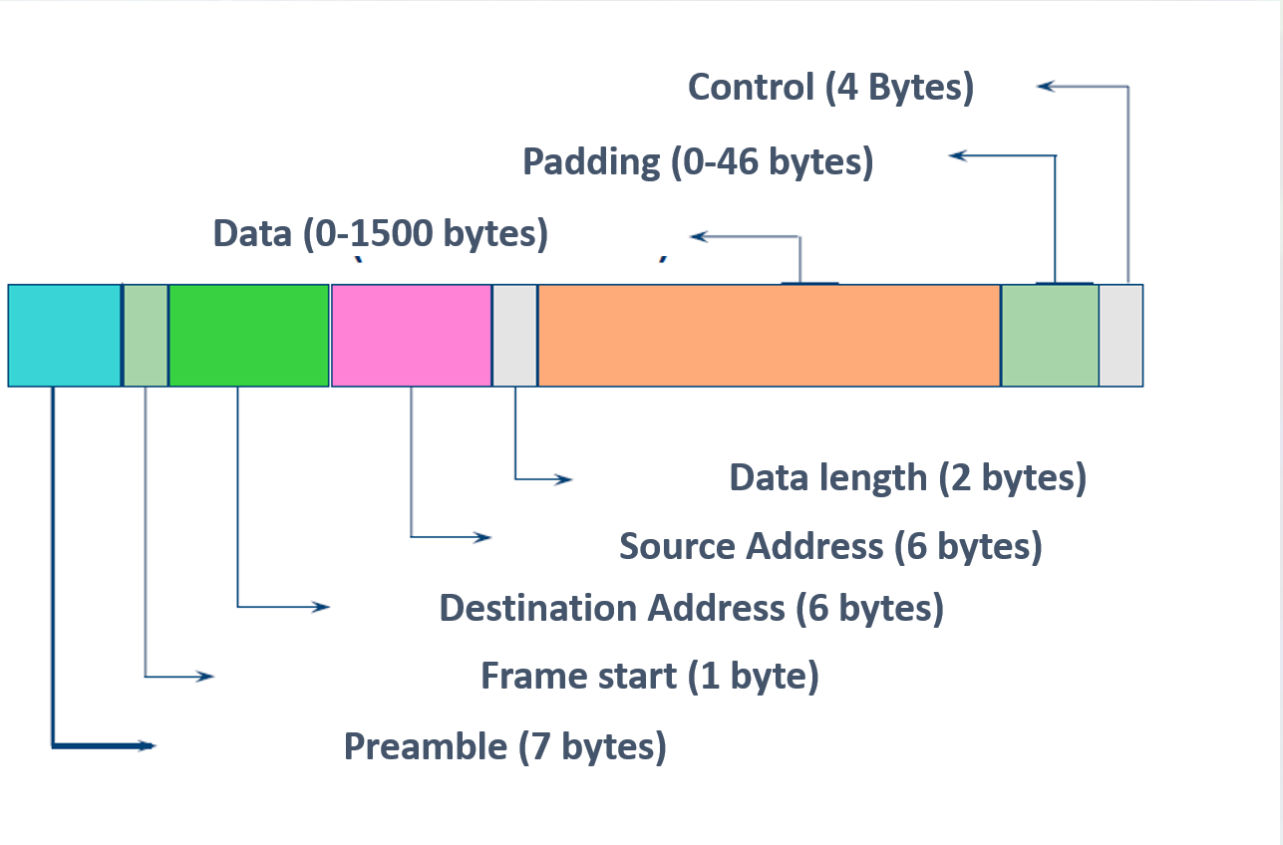
Valid frame:

46 ≤ (data + padding) ≤ 1500

64 ≤ (MAC addresses + length + data + padding + control) ≤ 1518

Control:

Control sequence = 32-bit CRC (Cyclic Redundancy Check) polynomial



Frame: Ethernet

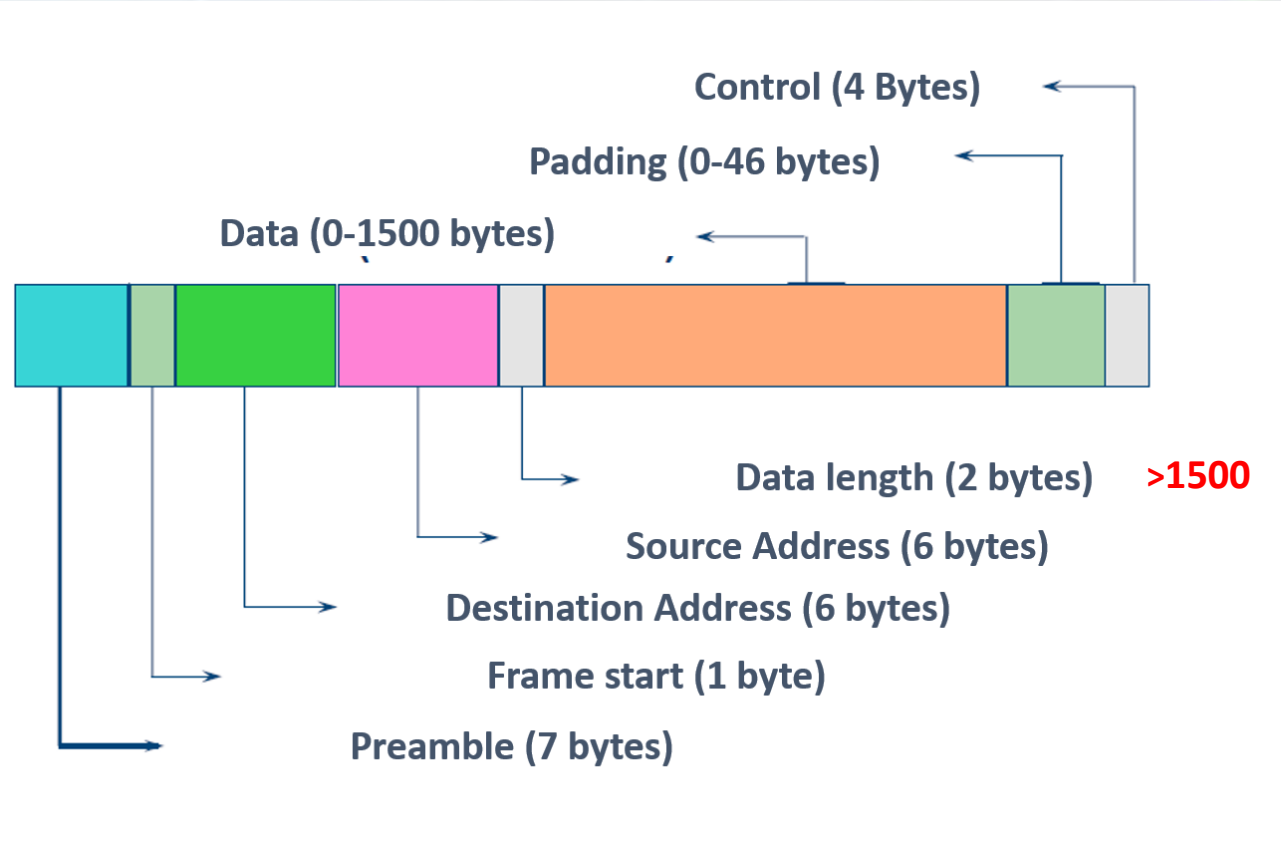
The Ethernet frame was created by a consortium of companies to meet certain needs.

It can travel on the same network as the 802.3 frame.

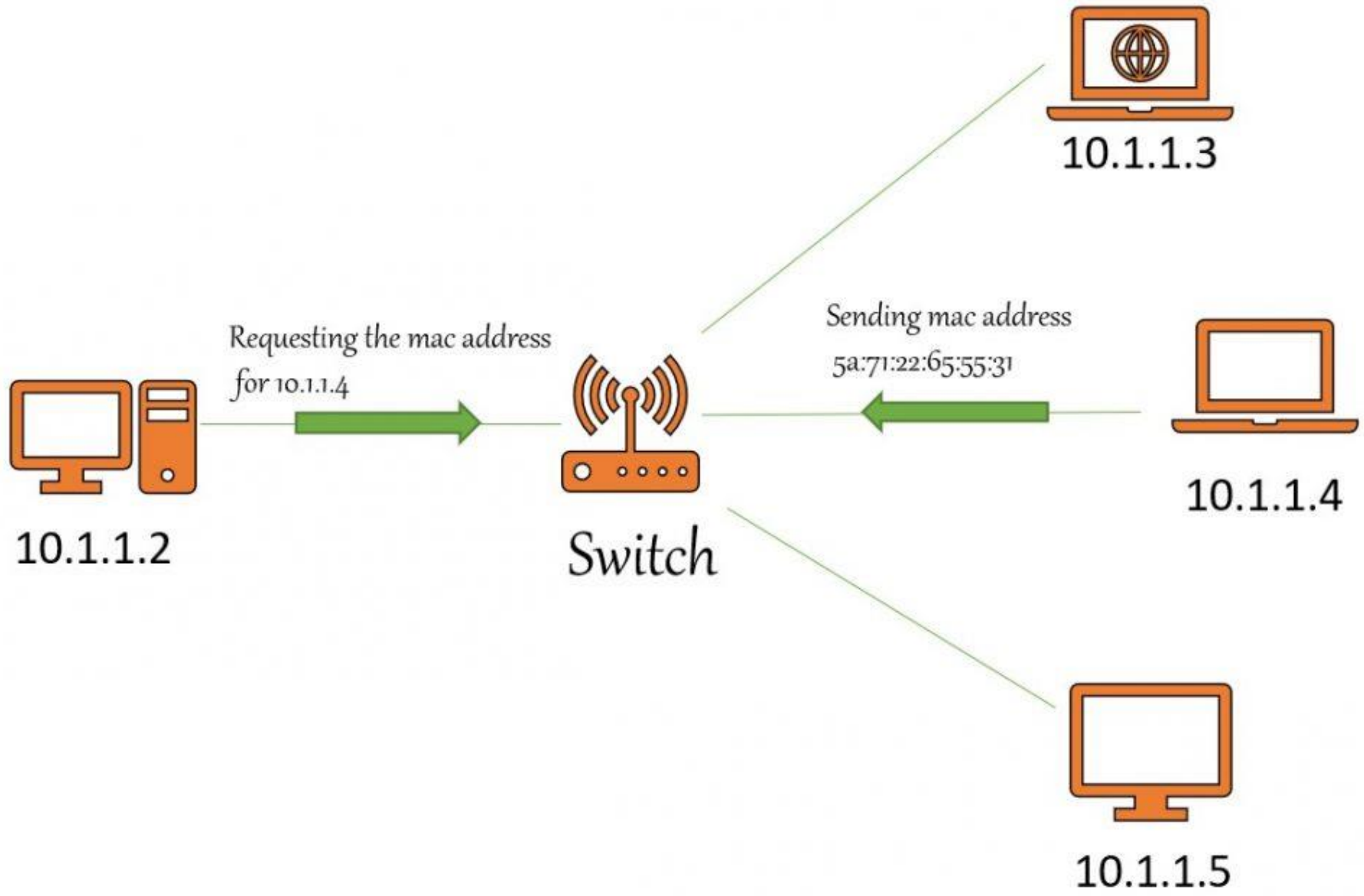
The difference between an Ethernet frame and an IEEE 802.3 frame lies in the value of the **5th field**:

-If this value is **less than 1500** (length), it is an IEEE 802.3 frame.

-If this value is **greater than 1500** (type), it is an Ethernet frame



ARP: Address Resolution Protocol



ARP: Address Resolution Protocol

Address resolution is the process of mapping a host's IP address to its physical (hardware) address.

The **ARP protocol** obtains the hardware address of hosts located on the same physical network.

Process:

- Broadcast an ARP request to all hosts, asking for the hardware address corresponding to the IP address IPx.
- Each host receives the request and compares its own IP address with IPx.
- If IP = IPx, the host sends its hardware address to the requester, who updates an **ARP table**.
- Otherwise, the host ignores the request.

Each machine contains an **ARP cache** storing recent requests (limited number of entries).

*To view on Windows: arp -g

RARP: Reverse ARP

RARP performs the **inverse operation of ARP**:

Determines the **IP address** from a **hardware (MAC) address**.

Example:

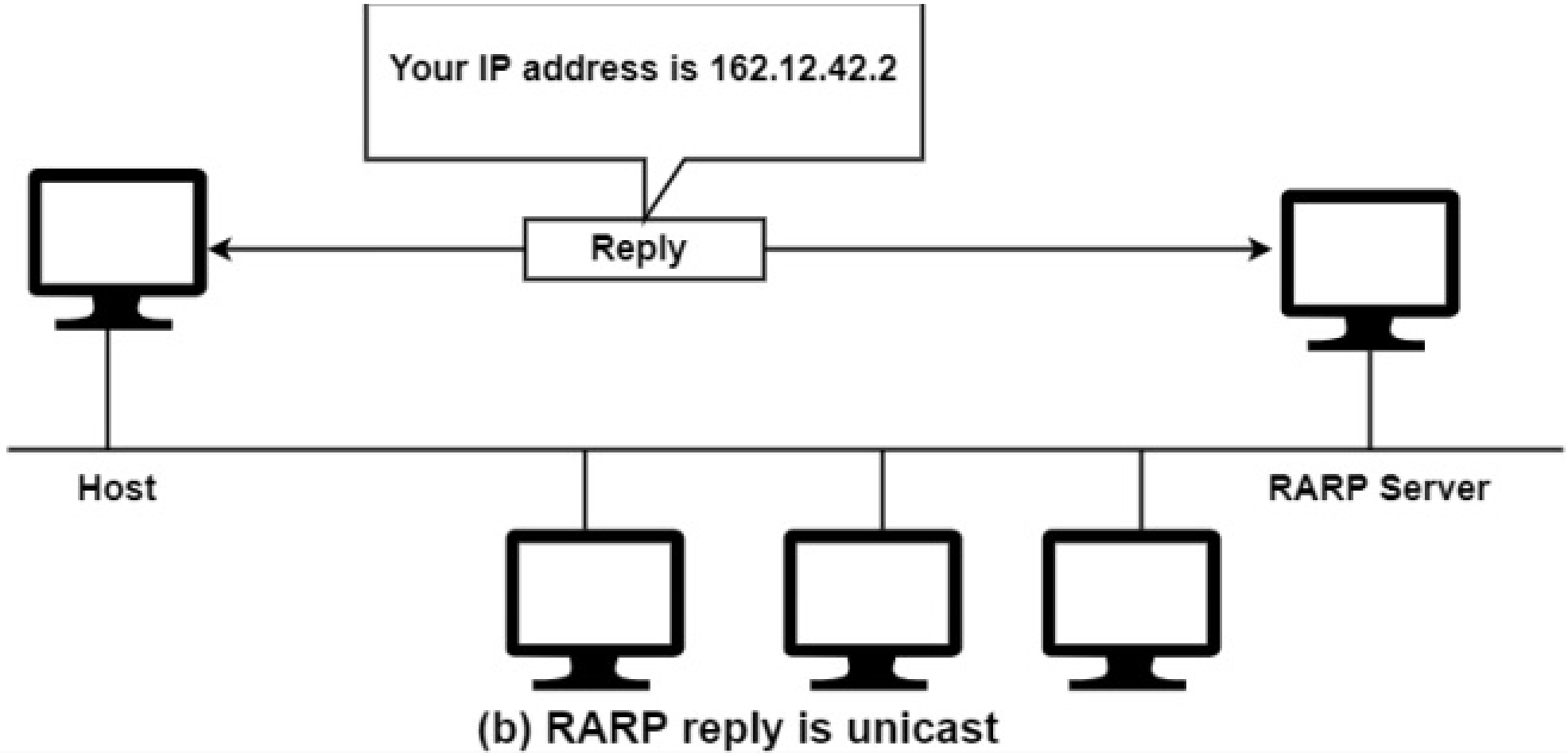
-A diskless computer, when starting up, must contact a server to obtain its IP address before it can use TCP/IP.

-It broadcasts a **RARP request**, identifying itself as the recipient.

-The request reaches a server that maintains a database mapping physical addresses to IP addresses.

-The server responds directly to the requesting machine, providing its IP address.

RARP: Reverse ARP



(b) RARP reply is unicast

ICMP

Internet Control Message Protocol (ICMP)

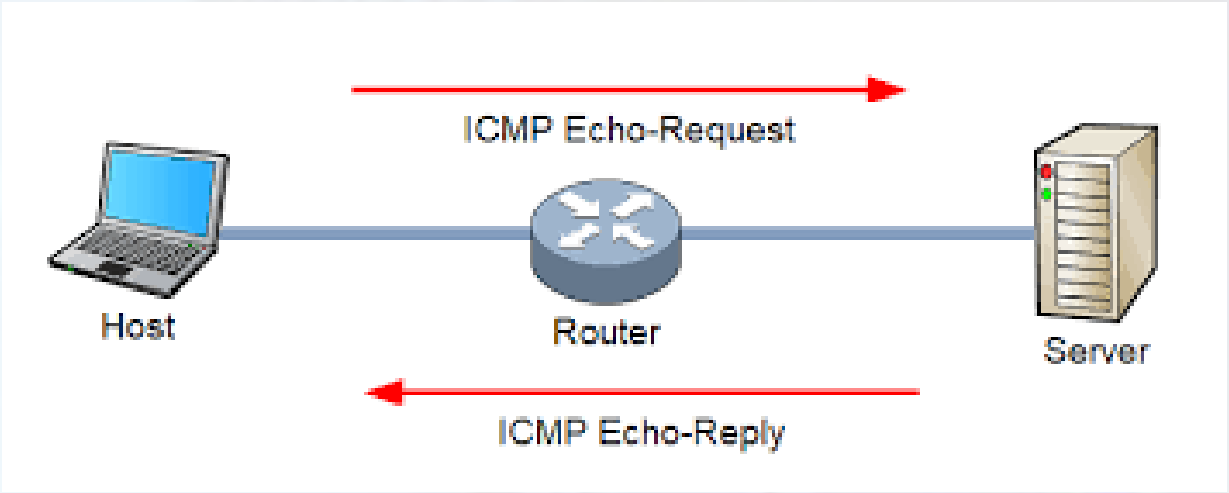
Provides a set of services for the internal needs of IP networks

Measures transit times (**PING – Packet Internet Gopher**)

Indicates errors, including:

- Destination unreachable
- Time exceeded
- Parameter problem

ICMP messages are carried within IP packets



IPv4

An IP address or "Internet Protocol Address" or "IP Address" is a 32-bit integer made up of a pair (netid, hostid), where **netid** identifies a network and **hostid** identifies a machine on that network.

IP Address size = 32 bits → 2^{32}, which corresponds to about 4 billion possible addresses.

Two types:

Private addresses, which any network administrator can freely assign as long as they are not routed on the Internet:

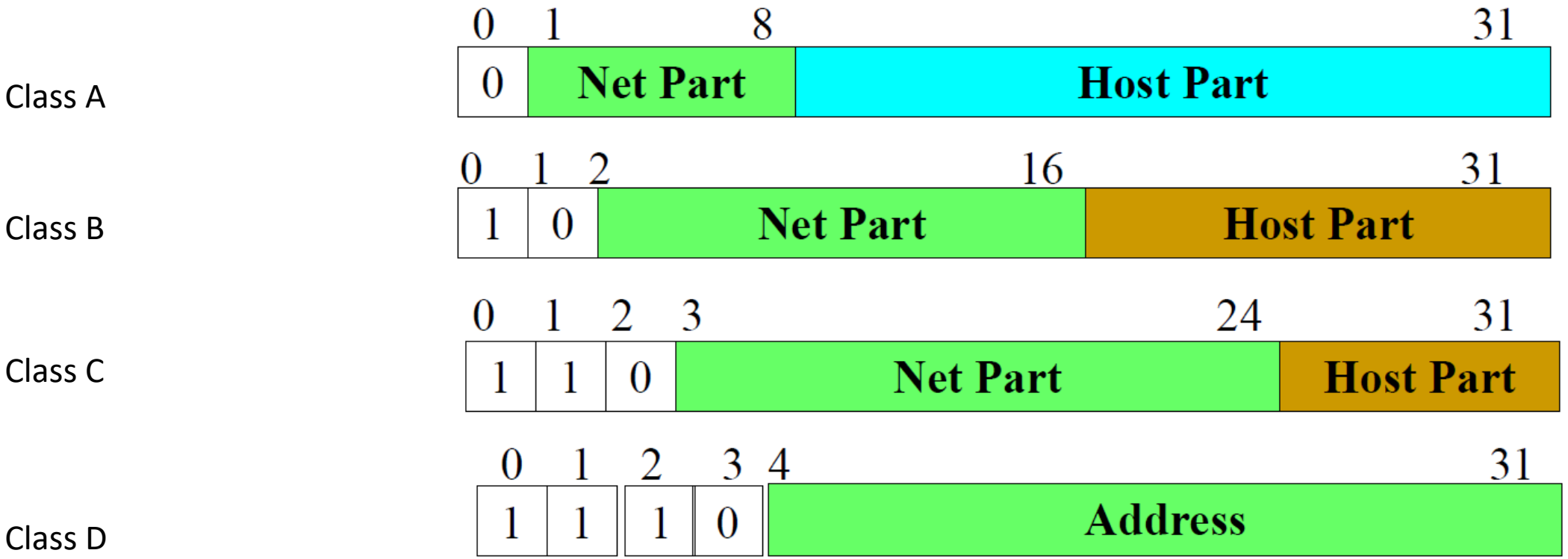
10.0.0.0 → 10.255.255.255 (former ARPANET!)

172.16.0.0 → 172.31.255.255

192.168.0.0 → 192.168.255.255

Public addresses, assigned by a global organization that ensures their uniqueness

IPv4 addresses classes



Class D: Multicast

Class E: Reserved

IPv4 addresses classes

Class A

First bit: 0 → Range: 0.0.0.0 – 127.255.255.255

Default subnet mask: 255.0.0.0 (/8)

Networks: 128 possible networks

Hosts per network: ~16 million ($2^{24} - 2$)

Use case: Very large networks

Note: 127.x.x.x reserved for loopback

Class B

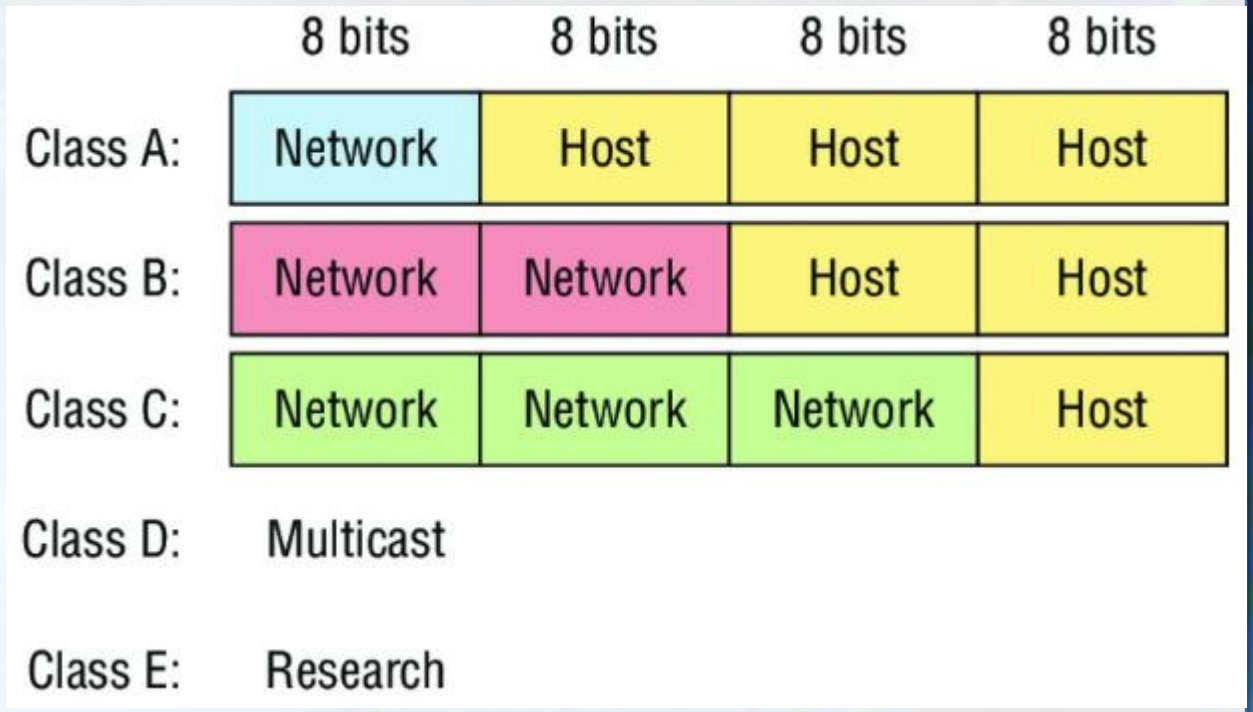
First two bits: 10 → Range: 128.0.0.0 – 191.255.255.255

Default subnet mask: 255.255.0.0 (/16)

Networks: 16,384

Hosts per network: ~65,000 ($2^{16} - 2$)

Use case: Medium to large organizations



IPv4 addresses classes

Class C

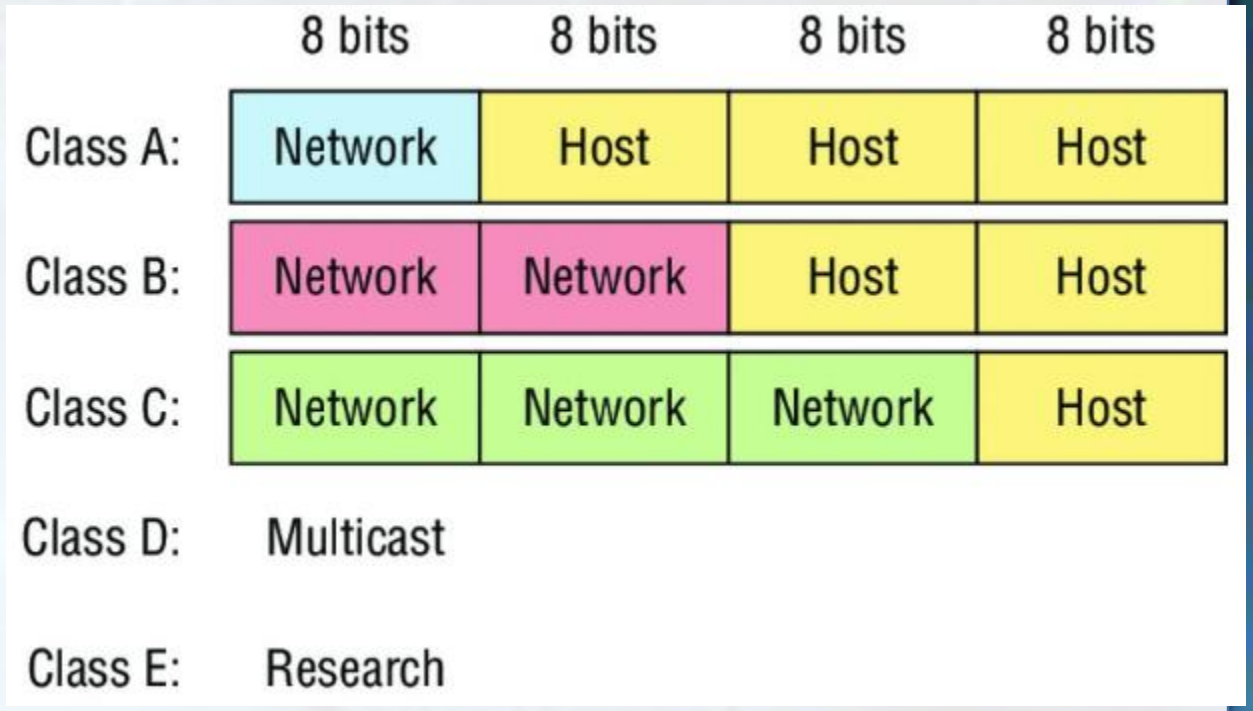
First three bits: 110 → Range: 192.0.0.0 – 223.255.255.255

Default subnet mask: 255.255.255.0 (/24)

Networks: Over 2 million

Hosts per network: 254 ($2^8 - 2$)

Use case: Small networks (LANs, SMEs)



Class D (Multicast)

First four bits: 1110 → Range: 224.0.0.0 – 239.255.255.255

Use case: Multicast groups (e.g., streaming, routing updates)

Not for host addressing.

IPv4 addresses classes

Class E (Experimental)

First four bits: 1111 → Range: 240.0.0.0 – 255.255.255.255

Reserved for experimental/research use

Not used in practice.

Special Addresses

Private ranges:

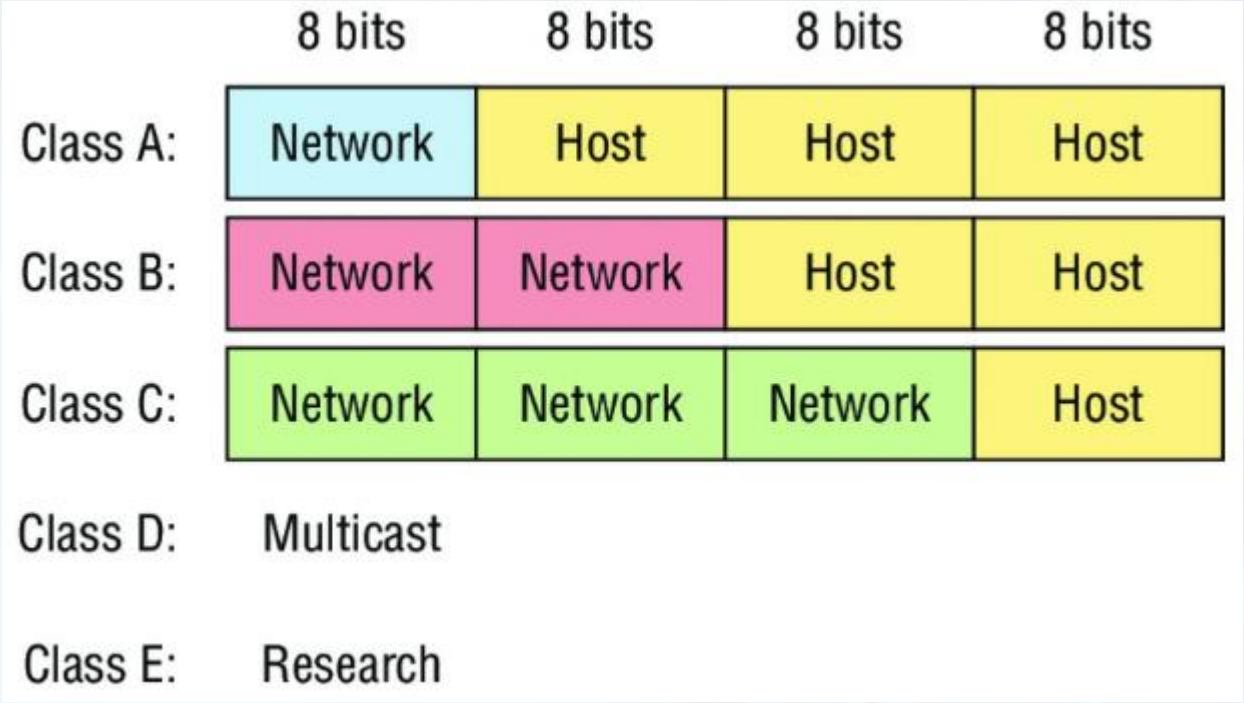
Class A: 10.0.0.0 – 10.255.255.255

Class B: 172.16.0.0 – 172.31.255.255

Class C: 192.168.0.0 – 192.168.255.255

Loopback: 127.0.0.1 (localhost)

Broadcast: 255.255.255.255



The notion of the mask

- The mask is a 32-bit integer, made up of a sequence of 1s followed by a sequence of 0s.
- By applying a logical AND between any IP address and its associated mask, we obtain the network part of the address (the network address).
- For example, the mask associated with a class A address is:
  1111 1111 0000 0000 0000 0000 0000 0000, which corresponds in decimal notation to 255.0.0.0.
- Another notation consists of writing an address followed by the number of bits set to 1 in the mask.
- Example: 193.194.64.0 with the mask 255.255.255.0 corresponds to 193.194.64.0/24.

The notion of the mask

Class A: 255.0.0.0 or /8

Class B: 255.255.0.0 or /16

Class C: 255.255.255.0 or /24

Special addresses

Network address: host part = 0

1100 0001 1100 0010 0100 0000 0000 0000

→ **193.194.64.0**

Local machine address: network part = 0

0000 0000 0000 0000 0000 0000 0100 0111

→ **0.0.0.71**

Directed broadcast address (Net-directed broadcast): host part = 1

1100 0001 1100 0010 0100 0000 1111 1111

→ **193.194.64.255 or 193.194.64.0/24**

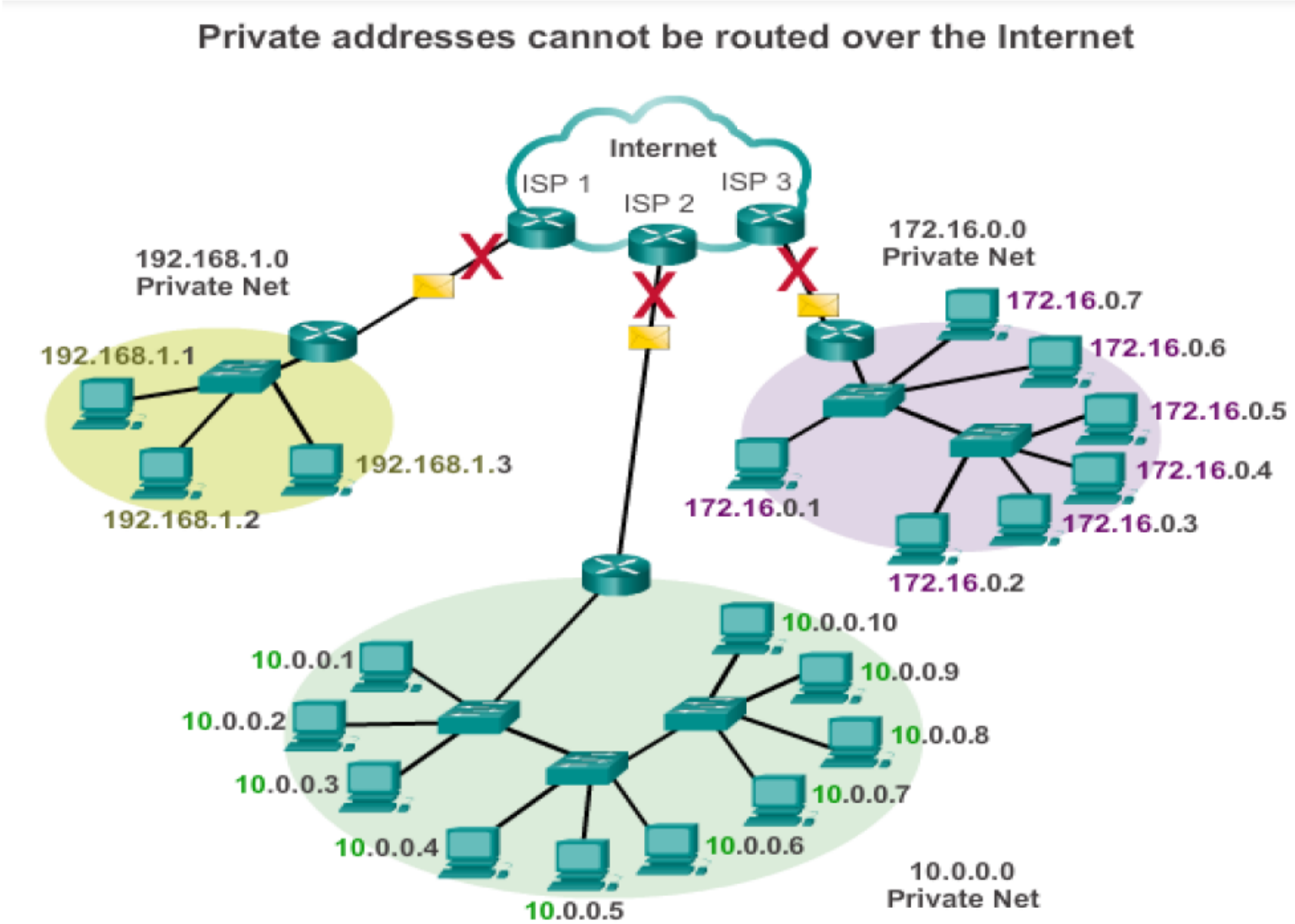
Limited broadcast address: all bits set to 1

→ **255.255.255.255**

Loopback address: all addresses starting with 127 (loopback)

→ **127.X.X.X, for example 127.0.0.1 (localhost)**

Public Vs private address



Public Vs private address

- **Public IP Address**

Unique, globally routable on the Internet

Assigned by ISPs or regional registries

Example: 102.45.23.7

- **Private IP Address**

Used only inside local/private networks

Not routable on the public Internet

Defined ranges:

Class A: 10.0.0.0 – 10.255.255.255

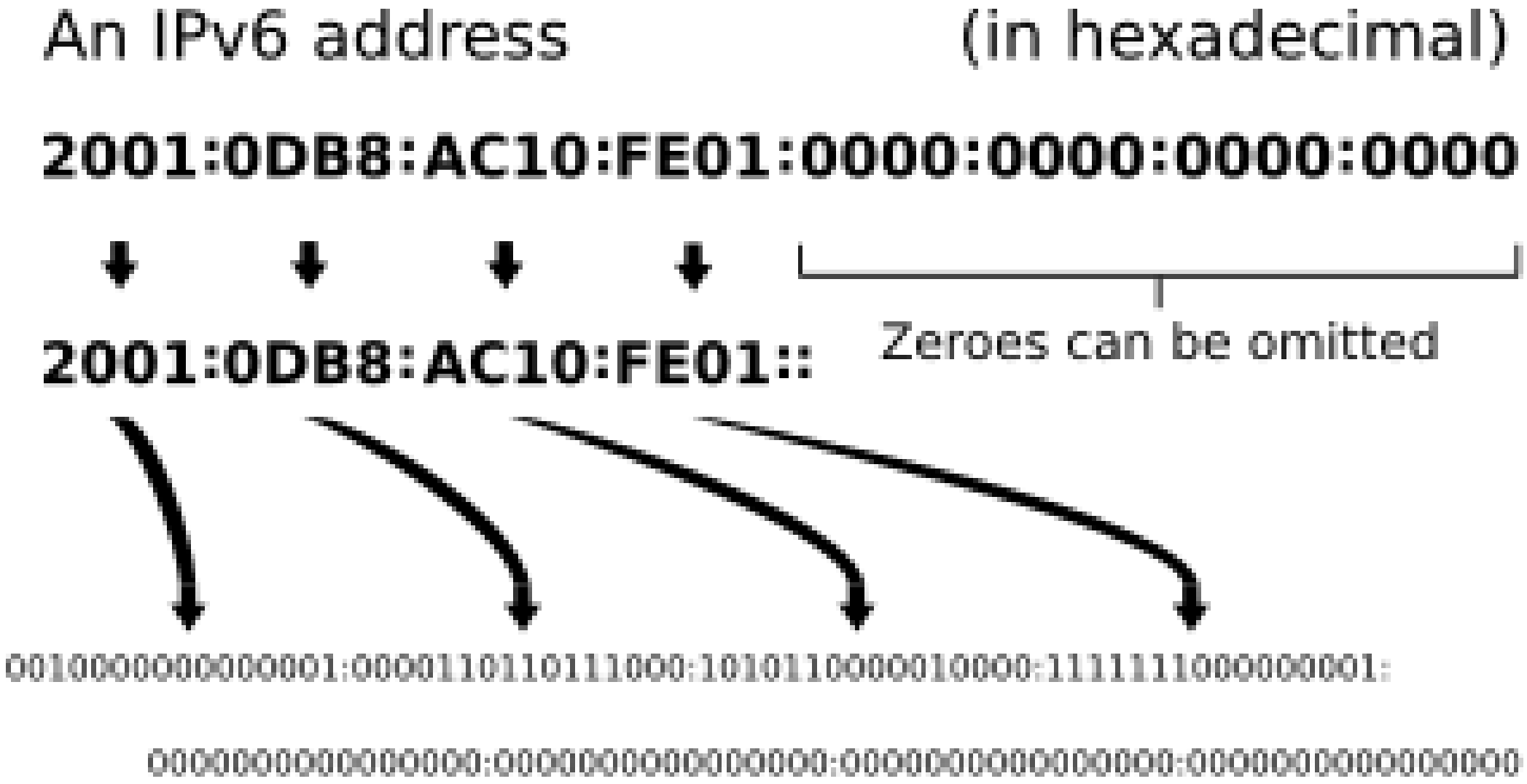
Class B: 172.16.0.0 – 172.31.255.255

Class C: 192.168.0.0 – 192.168.255.255

IPv6

- The address space has been expanded from 4 bytes (32 bits) to 16 bytes (128 bits).
- Simplified datagram headers, with only 7 fields instead of 14.
- Plug and Play configuration, thanks to machine auto-configuration mechanisms.
- More efficient routing, with reduced routing tables.
- Flow identification for integrated services.
- Standard security mechanisms.
- Mobility.
- An almost unlimited number of IP addresses.

IPv6


An IPv6 address (in hexadecimal)
2001:0DB8:AC10:FE01:0000:0000:0000:0000
2001:0DB8:AC10:FE01::
Zeroes can be omitted
0010000000000001:0000110110111000:1010110000010000:1111111100000001:
0000000000000000:0000000000000000:0000000000000000:0000000000000000

IPv4 vs IPv6

IPv4

Address Size:
32-bit number

Address Format:
Dotted Decimal Notation:
192.168.1.1

Prefix Notation:
255.255.255.0
/24

Number of addresses:
2**32 = 4,294,967,296

Vs

IPv6

Address Size:
128-bit number

Address Format:
Hexadecimal Notation:
fe80::94db:946e:8d4e:129e

Prefix Notation:
/64

Number of addresses:
2**128 =
340,282,366,920,938,463,463,374,607,
431,768,211,456

IPv6 Categories

Unicast: refers to an identifier associated with a single interface.

Multicast: refers to a group identifier; interfaces that are members receive the multicast ID.

Anycast: designates the “closest” interface in a group, based on the routing metric.