REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
الجمهورية الجزائرية الديمقراطية الشعبية

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

ECOLE SUPERIEUREEN EN SCIENCES APPLIQUEES
--T L E M C E N--

وزارة التعليم العالي والبحث العلمي

المدرسة العليا في العلوم التطبيقية
-تلمسان-

HIGHER SCHOOL OF APPLIED SCIENCES OF TLEMCEN

SECOND-CYCLE DEPARTMENT

LECTURE HANDOUT

Computer Networks

Prepared by:

Dr BRAHAMI Mustapha Anwar

Contents

List of Figures

Preface

Mastering computer networks and communication protocols is now an essential skill for any engineer in applied sciences. In an era of interconnected systems, where the fast, reliable, and secure transmission of data has become a necessity, understanding the underlying mechanisms of networks is crucial for designing, operating, and maintaining high-performance infrastructures.

This textbook, entitled “Computer networks”, is intended for third-year Electronics students at the École Supérieure en Sciences Appliquées de Tlemcen (ESSA-Tlemcen), where it has been taught since 2023. This course requires prior knowledge in computer tools, computer system architecture, and communication systems.

The primary objective of this course is to provide students with a comprehensive understanding of computer networks, their architectures, and the protocols that govern communication between systems. The course addresses not only theoretical concepts but also their implementation in real environments to ensure both conceptual and practical training.

The course particularly emphasizes:

- The layered architecture of networks and how each layer interacts with the others,
- The protocols that ensure various functions (addressing, routing, error control, reliability),
- The current technologies and standards used in wired and wireless networks,
- Practical application through case studies to develop operational skills.

The course content is structured into several progressive chapters, allowing a coherent skill-building approach:

- **Chapter 1: Introduction to Computer Networks**

  This first chapter introduces the fundamental concepts: definitions, objectives, a historical overview of communications and the evolution of the Internet. It also presents the

different classifications of networks (by geographic scope, topology, speed, and transmission mode), providing a global view of current architectures.

- **Chapter 2: Layered Architecture and the OSI Model**

  This chapter introduces the principle of layered structuring, the notions of protocol, service, and interface, as well as the advantages of hierarchical architectures. A detailed analysis of the OSI model and its seven functional layers is carried out, highlighting their roles and interactions.

- **Chapter 3: The Physical Layer**

  This chapter covers the general characteristics of physical transmission, transmission modes, bandwidth and speed, as well as transmission media (cables, optical fibers, wireless links). This part provides the essential hardware foundations for understanding binary communication over a channel.

- **Chapter 4: The Data Link Layer**

  This chapter highlights the crucial role of this layer in ensuring reliable exchanges. It addresses data encapsulation into frames, error control mechanisms, media access control (CSMA/CD, CSMA/CA, token passing), and physical addressing (MAC). Major protocols such as Ethernet are studied.

- **Chapter 5: The Network Layer**

  This section deals with logical addressing (IPv4), subnetting concepts, IP routing principles and mechanisms, as well as routing protocols (static and dynamic). This chapter is essential for understanding how data travels through multiple interconnected networks.

- **Chapter 6: The Transport Layer**

  This part focuses on the TCP and UDP protocols, their characteristics, segmentation concepts, multiplexing/demultiplexing, as well as flow control and transmission reliability.

- **Chapter 7: Session, Presentation, and Application Layers**

  Finally, this chapter explores the upper layers of the OSI model: session management, data translation, encryption and compression, as well as application services and protocols such as HTTP, FTP, SMTP, DNS.

Each chapter is accompanied by practical examples to consolidate understanding through the manipulation of studied concepts (frame analysis, IP address configuration, network architecture studies, protocol testing, etc.).

This textbook combines theory and practice. Concepts are introduced progressively and illustrated with explanatory diagrams, concrete examples, and exercises. The practical aspect is strongly emphasized, enabling students to apply the concepts studied.

In short, this course aims to provide future engineers with a global vision of computer networks while developing their ability to design, configure, and secure interconnected systems.

Chapter 1

Introduction to computer networks

1.1 Introduction

Computer networks have become an essential part of our daily and professional lives. They enable not only the rapid exchange of information but also the sharing of hardware and software resources on a large scale. However, behind this apparent simplicity of use lies a rich history and a variety of technical concepts.

In this first chapter, we will define what a computer network is, trace the major stages of its evolution, in particular the emergence of the Internet, and then present the different classifications of networks according to several criteria.

1.2 Definitions

A computer network can be defined as a set of autonomous computer systems, called nodes, connected to each other by hardware (cables, fibres, waves, etc.) and software (protocols, network operating systems). This interconnection allows computers to communicate, exchange data and share resources, either directly or indirectly via intermediaries.

In practice, two connected computers are sufficient to constitute a computer network. Of course, modern networks are much larger and more diverse, ranging from small domestic interconnections to the global Internet.

Having defined what a network is, it is worth looking back at the historical evolution of the means of communication that made the emergence of modern networks possible.

1.3 Historical overview of communications

Some important milestones include [1]:

- 1837: William Cooke and Charles Wheatstone develop the electric telegraph in
- England. In the same year, Samuel Morse and Alfred Vail develop a similar system in the United States.
- 1866: The first functional transatlantic cable is laid, connecting Europe to America.
- 1876: Alexander Graham Bell invents the telephone.
- 1901: Guglielmo Marconi successfully completes the first wireless telegraph transmission at cross the Atlantic.
- 1907: Édouard Belin achieves the first transmission of a photograph.
  1923: John Baird develops the first mechanical television.

These innovations, by increasing the means of remote transmission, gradually paved the way for the creation of computer networks.

1.4 Birth and evolution of the Internet

This technical evolution found its natural extension in the creation of the Internet, which is now the world's largest network [1].

- 1959–1968: The ARPA programme — a project by the US Department of Defence aimed at creating a resilient network.
- 1969: Birth of ARPANET, the ancestor of today's Internet.
- 1970s–1982: International expansion with the first connections in Europe (Norway, London). Emergence of UseNet and BitNet.
- 1983: Adoption of the TCP/IP protocol, giving rise to the modern Internet.
- 1986: The NSF deploys supercomputers to increase network capacity.
- 1987–1992: Rapid expansion thanks to commercial access providers.

The Internet thus established itself as a "network of networks", connecting universities, businesses, institutions and individuals on a global scale. Its management is based on a decentralised organisation and a constantly expanding community.

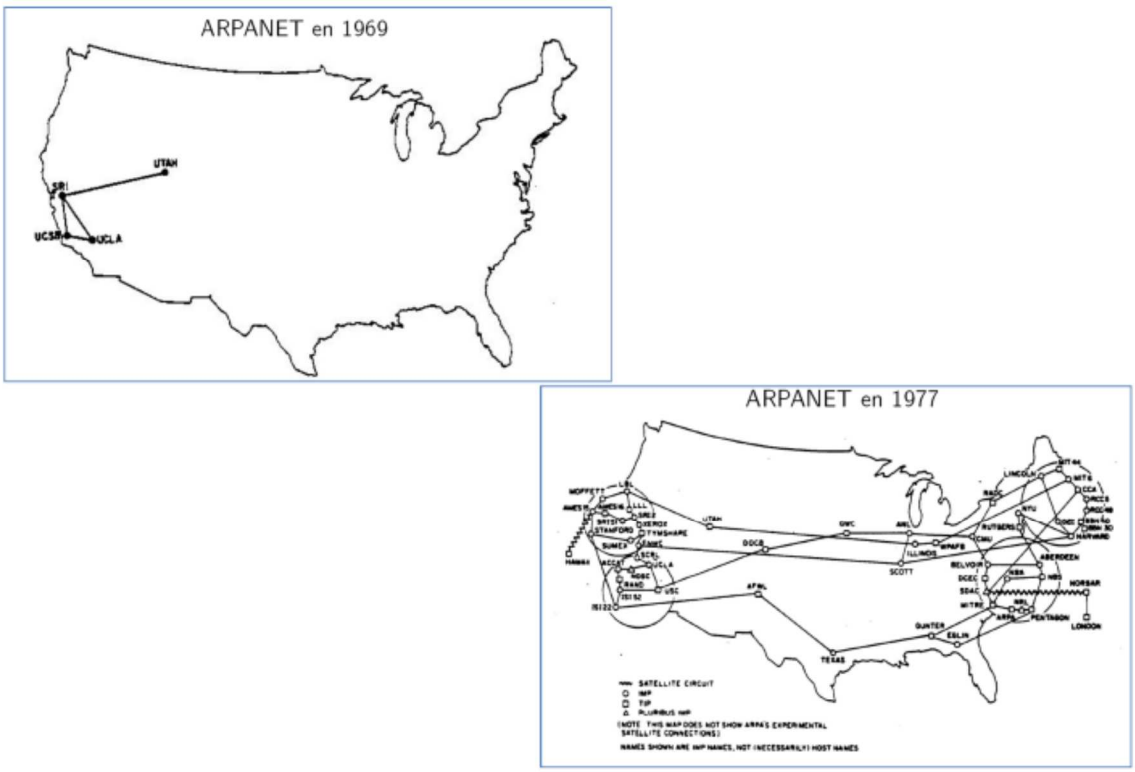

Figure 1.1 Evolution of ARPANET [1]

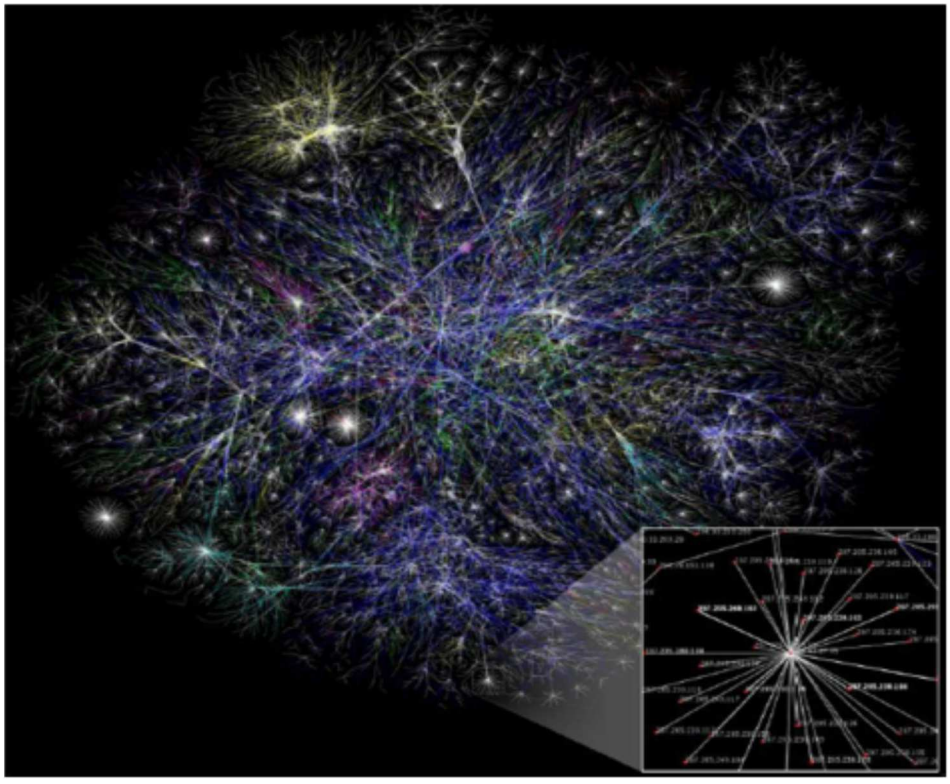

Figure 0.2 Internet : a network of networks [1]

Now that we understand how the Internet was born and developed, we need to better characterise computer networks by classifying them according to different criteria.

1.5 Classification of networks

The diversity of computer networks makes their classification complex. However, they can be grouped according to several criteria [2].

1.5.1 According to distance or geographical extent

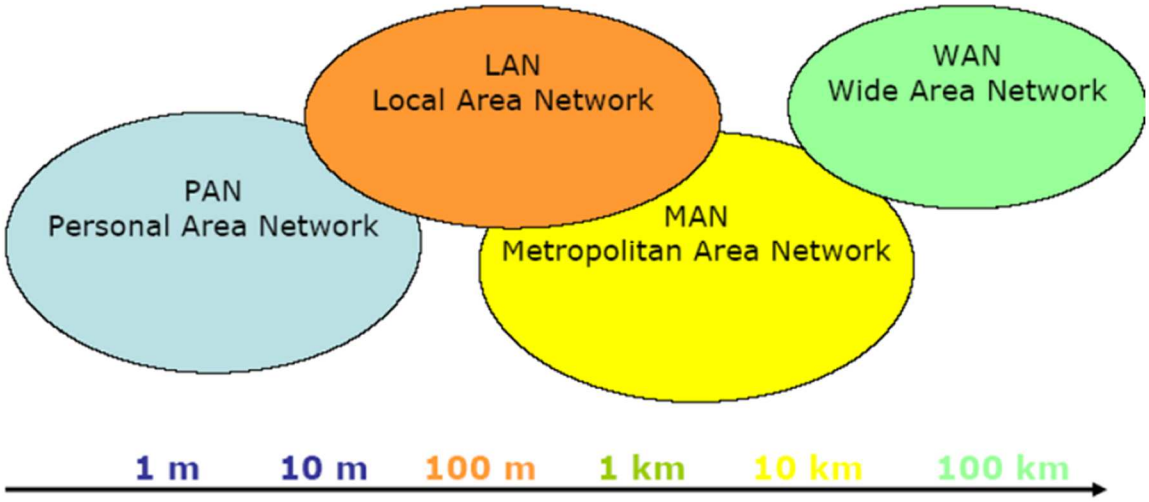

Figure 0.3 Classification of networks according to distance or geographical extent [2]

(a) Personal Area Networks (PANs)

These cover a range of a few metres and interconnect personal devices such as personal computers, laptops, printers, domestic appliances, etc.

Figure 0.4 Personal Area Networks (PAN)

- These cover a range of several hundred metres and interconnect IT equipment within a single company or university
- Their speed ranges from a few Mbit/s to a few Gbit/s.
- The most commonly used technology: Ethernet.

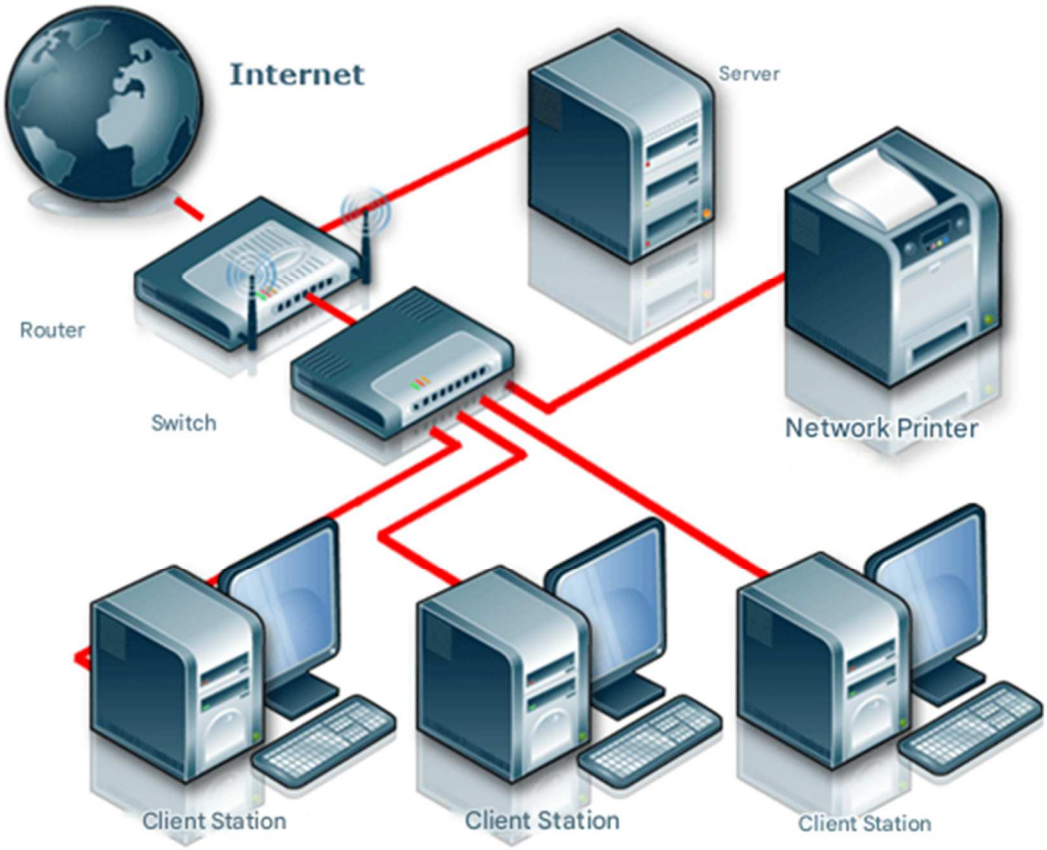

Figure 0.5 Local Area Networks (LAN) [2]

(b) Metropolitan Area Networks (MANs)

These interconnect several sites within the same city, as well as local area networks located in distant buildings.

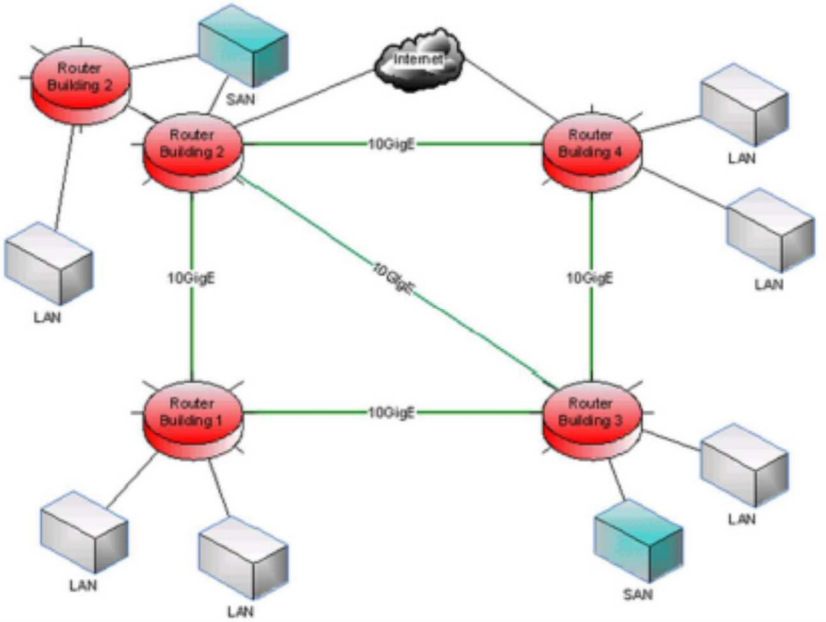

Figure 0.6 Metropolitan Area Networks (MAN) [3]

(c) Wide area networks (WANs)

They consist of interconnections between LANs and even MANs. Wide area networks are capable of transmitting information over thousands of kilometres across the globe. They are either terrestrial or satellite-based.

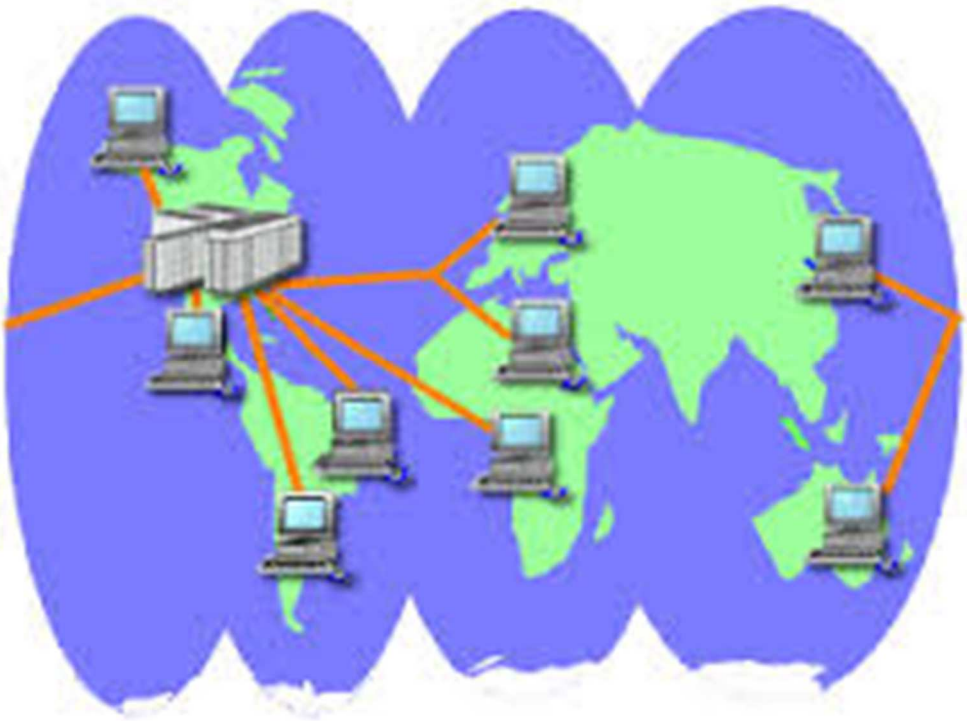

Figure 0.7 Wide Area Networks (WAN) [3]

1.5.2 According to topology

Network topology describes how the elements of a network are arranged in relation to each other.

The most commonly used topologies are:

- Bus
- Ring
- Star
- Tree
- Mesh

(a) Bus topology

The word “bus” refers to the physical line that connects the machines in the network.

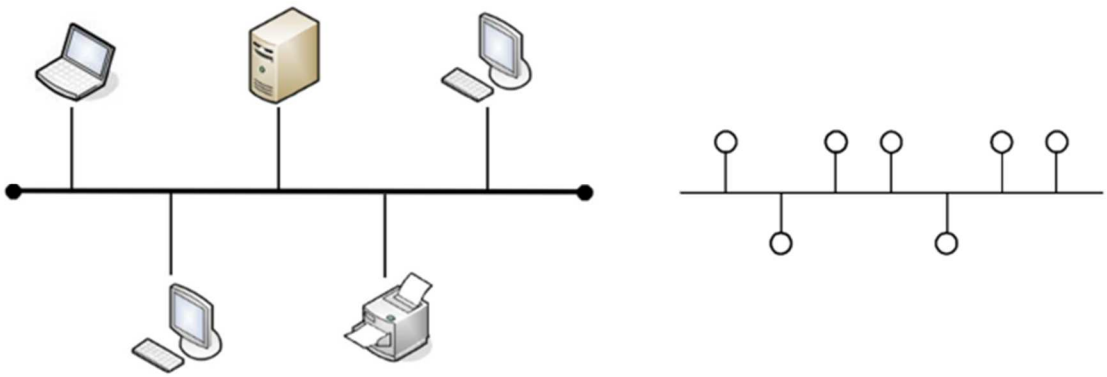

Figure 0.8 Bus topology [3]

(b) Ring topology

Computers are located on a loop and communicate in turn. Each node acts as a repeater in the flow of information. Information flows in only one direction in the ring.

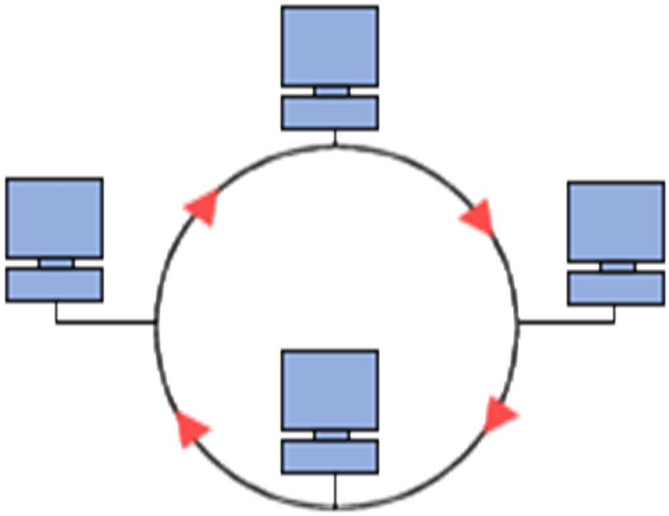

Figure 0.9 Ring topology [3]

(c) Star topology

The computers in the network are connected to a central node, which is usually a hub or switch. The role of this node is to ensure communication between the different nodes. Most current local area networks are based on this topology.

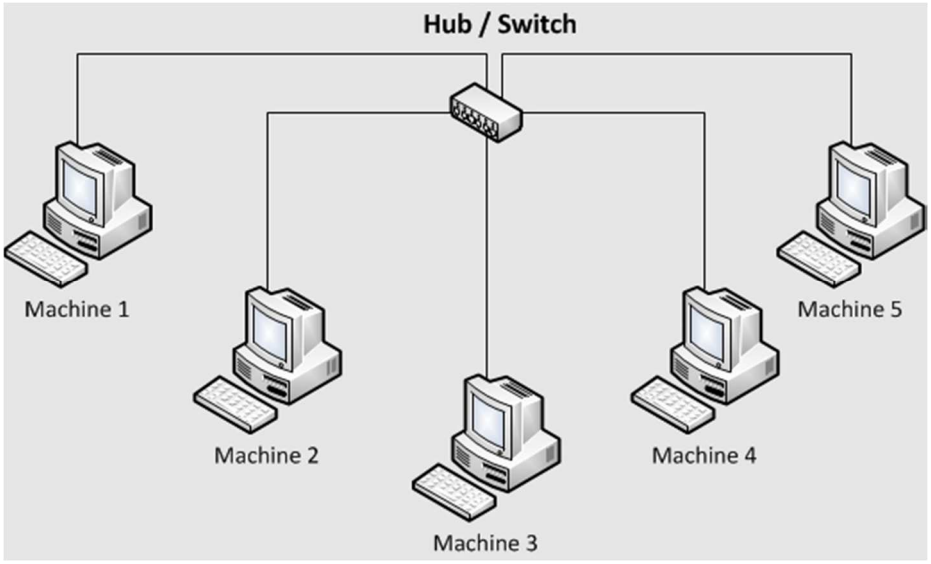

Figure 0.10 Star topology [4]

(d) Tree topology

This topology allows a network to be divided into hierarchical subnetworks.

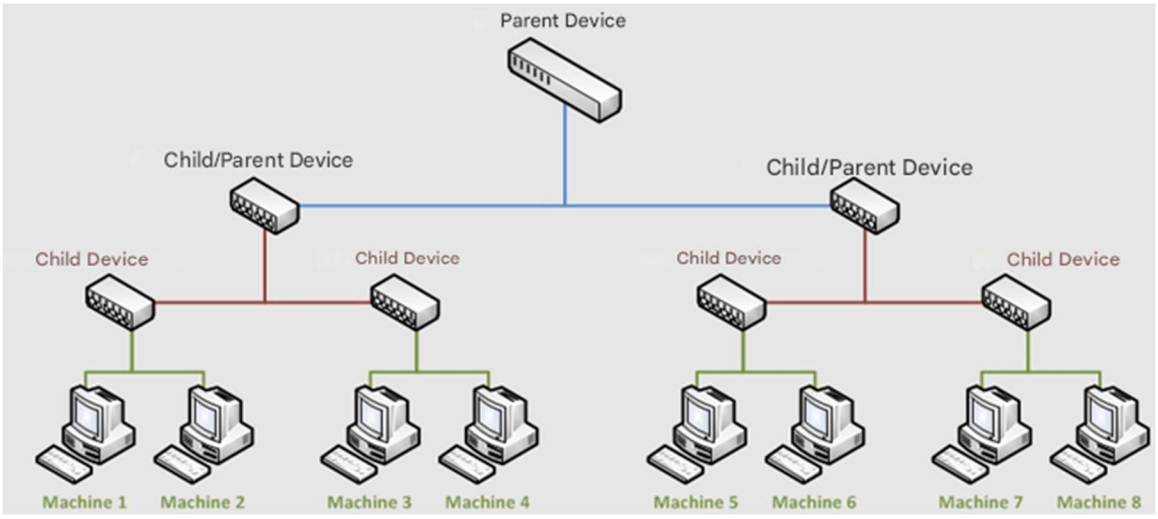

Figure 0.11 Tree topology [4]

(e) Mesh topology

In a mesh network, each node is connected to one or more other nodes without any particular logic, generally offering several different paths between any two nodes, which increases the reliability of the network.

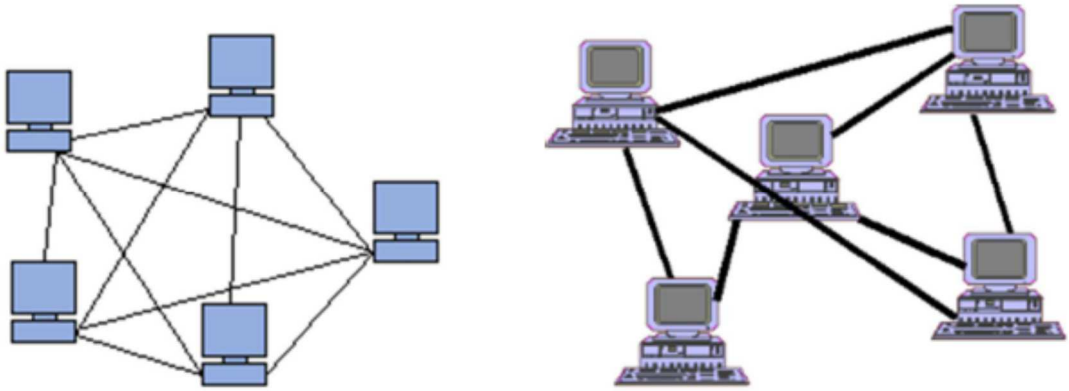

Figure 0.12 Mesh topology [3]

1.5.3 According to speed

- Ethernet (100 Mbit/s)
- ATM (up to 622 Mbit/s)

1.5.4 By transmission mode

- Wired (e.g. Ethernet)
- Wireless (e.g. Wi-Fi, GSM)
- Fibre optic (e.g. FDDI, ATM)

These different classifications show that there are many types of computer networks, adapted to a variety of contexts, from simple personal networks to the global Internet.

1.6 Conclusion

Computer networks are now an essential part of the infrastructure of our connected societies. Their emergence is the result of a long technological evolution, from the telegraph to the global Internet. Classifying them according to size, topology, speed or transmission mode provides a better understanding of their diversity and uses.

This first chapter has laid the foundations: definition, history and types of networks. In the following chapters, we will explore the technical aspects in greater depth, particularly the protocols, architecture and management of these networks.

Chapter 2
The OSI model

2.1 Introduction

In the design and operation of computer networks, it is essential to have a methodological framework for structuring exchanges and clarifying the responsibilities of each component. Layered architecture meets this need by, dividing communication into several levels, each fulfilling a well-defined role.

The OSI (Open Systems Interconnection) model, proposed by the ISO in 1984, has established itself as a reference model. Although it has not been implemented as such in real networks, it remains a fundamental basis for understanding communication mechanisms and locating protocols.

2.2 Layered architecture [5]

The concept of layers is a common method in computer science when it comes to subdividing the tasks of a system. It is found in operating systems, software and, of course, networks.

In telecommunications, layered architecture consists of segmenting a system into several stacked levels. Each layer has a specific function (service) and communicates with the two adjacent layers through an interface:

- the lower layer provides services to the upper layer,
- the upper layer uses the services of the lower layer.

Actual communication takes place between physical layers, while exchanges between layers of the same level of two nodes are referred to as logical or virtual.

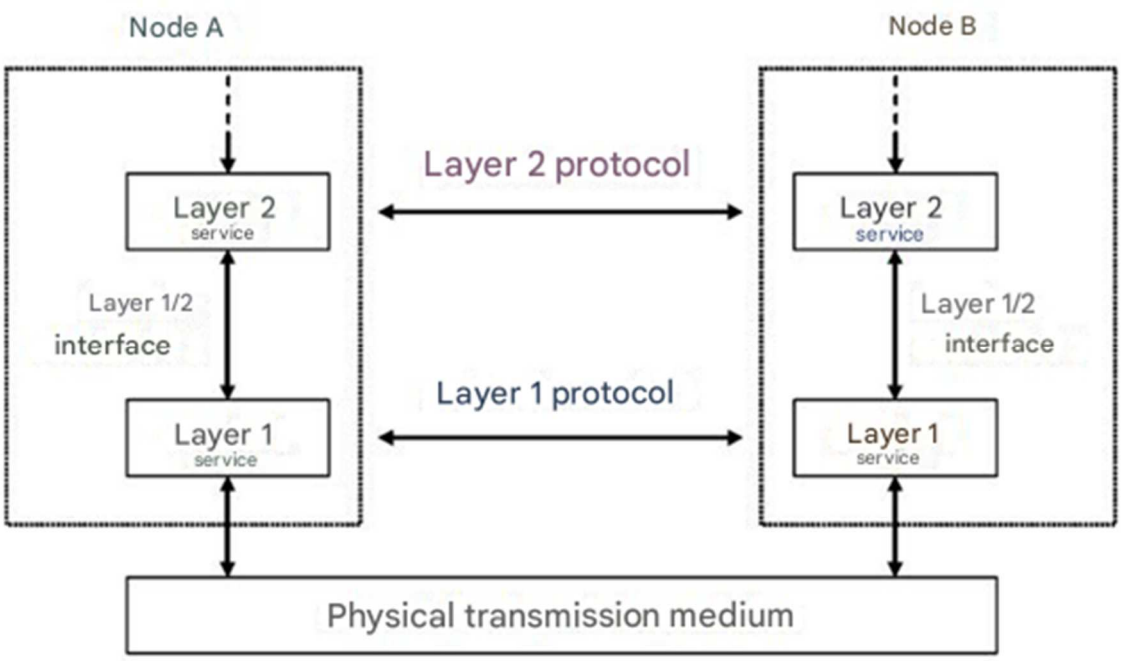

Figure 2.1 General principle of a layered architecture [5]

Before detailing the OSI model, it is necessary to clarify the concepts of protocol, service and interface, which are the fundamental elements of this approach.

2.3 Protocol, service and interface

- Protocol: set of rules and conventions that define the structure and meaning of messages exchanged between two communicating entities.
- Service: implementation of the specifications imposed by a protocol, realised through the available functions.
- Interface: access point to a service. In software, this usually involves function calls or libraries; in hardware, it may correspond to registers accessible by the user.

These concepts provide a better understanding of the benefits of a modular organisation. Let us now look at the advantages of a layered architecture.

2.4 Advantages of layered systems

The principle of layer decomposition offers several benefits [6]:

- Simplicity: each problem is dealt with separately.
- Modularity: each layer is relatively independent.
- Flexibility: a layer can evolve without requiring a complete overhaul of the system.

- Abstraction: it is not necessary to understand all the technical details to grasp how the system works as a whole.
- Easier maintenance: corrections and improvements are localised.

Based on these advantages, the ISO proposed a standardised theoretical model: the OSI model.

2.5 The OSI model [6]

The OSI (Open Systems Interconnection) model is a seven-layer reference model published in 1984 by the ISO (International Organisation for Standardisation).

- It is a theoretical model that does not correspond to any particular network technology.
- It provides a universal framework for understanding network protocols and services.
- Each layer of the model performs a specific function and communicates with adjacent layers.

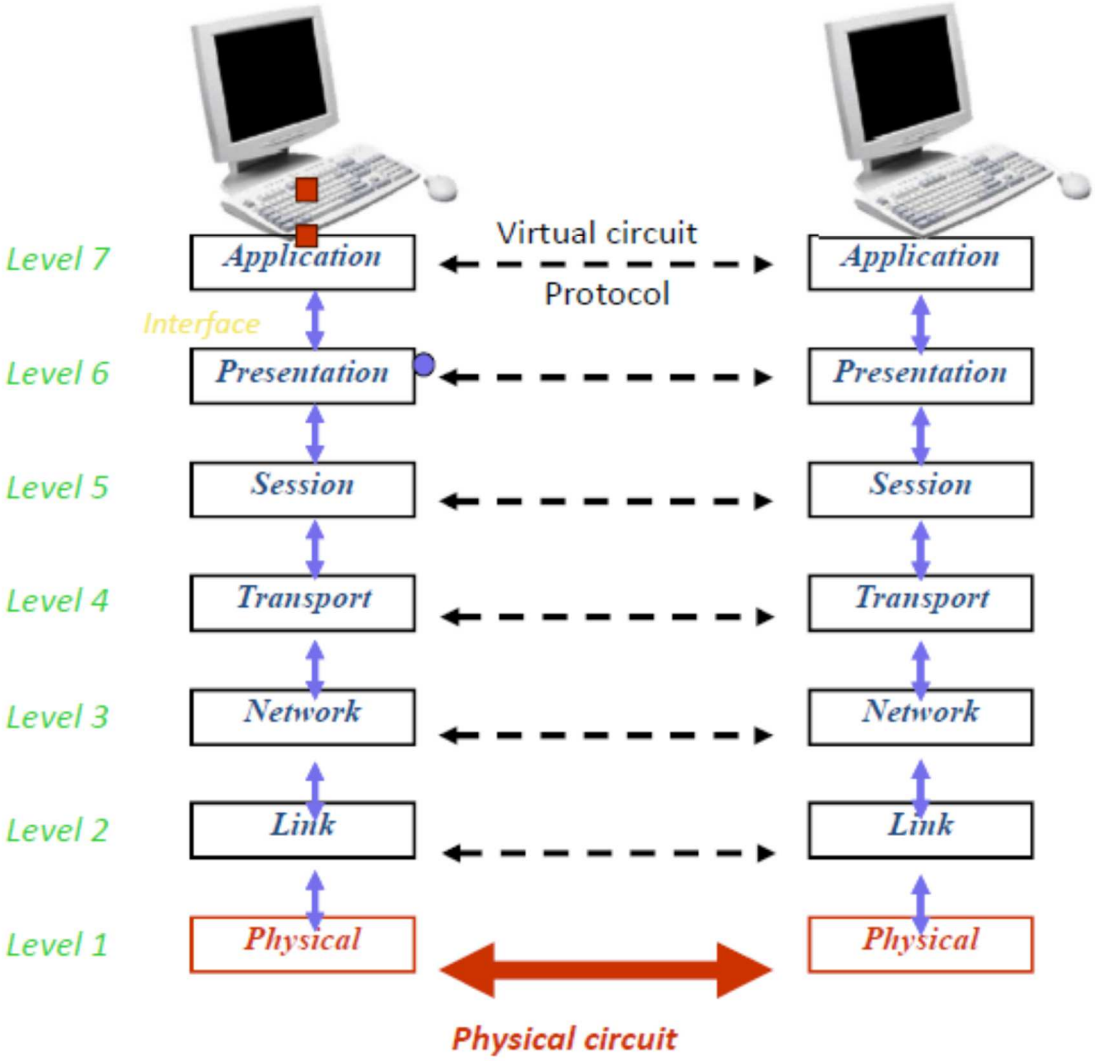

Figure 2.2 The OSI model and its 7 layers [6]

Let us now examine the role of each layer in detail.

2.6 The seven layers of the OSI model [7]

2.6.1 Physical layer (Level 1)

This layer corresponds to the hardware level of the network. It ensures the transmission of bits via a physical medium (twisted pairs, fibre optics, radio waves).

It manages signal encoding and modulation (NRZ, Manchester, AM, FM).

The unit of exchange is the bit.

Without this layer, no communication is possible, as it forms the hardware basis for all other layers.

2.6.2 Data link layer (Level 2)

The data link layer organises data into frames and ensures error-free transmission above the physical layer.

It manages synchronisation, error detection and sometimes correction (CRC, parity), as well as physical addressing (MAC addresses).

It also controls shared access to the medium (CSMA/CD, etc.).

It plays a crucial role in the reliability of direct communications between two neighbouring devices.

2.6.3 Network layer (Level 3)

The role of the network layer is to route data from one point to another, even if the two machines are not directly connected.

It chooses the path to follow using routing and manages logical addressing (e.g. IP addresses).

Its exchange unit is the packet.

It also handles congestion control.

Protocols emblematic of this layer are IP and X.25.

2.6.4 Transport layer (Level 4)

The transport layer serves as an interface between the upper layers (application processing) and the lower layers (transmission).

It divides messages into numbered segments, reassembles them in the correct order and guarantees the reliability of communications.

It also manages quality of service and flow control.

The two best-known protocols are:

- TCP: connection-oriented, reliable;
- UDP: connectionless, faster but less reliable.

2.6.5 Session layer (Level 5)

This layer establishes, manages and terminates sessions between applications.

It enables a logical dialogue to be maintained, for example during an FTP connection or a web session.

It is useful for managing prolonged exchanges, where simple data transmission is not sufficient.

2.6.6 Presentation layer (Level 6)

The presentation layer is responsible for translating, encrypting and compressing data.
It ensures interoperability between heterogeneous systems by transforming data into a format that can be understood by all.
For example, it can convert ASCII character encoding to Unicode, or compress a stream before transmission.

2.6.7 Application layer (Level 7)

The application layer is the one that is directly visible to the end user. It offers a variety of services that enable the exchange of information across the network. Among the best known are:

- HTTP/HTTPS: web protocol for viewing pages and secure information transfer.
- FTP (File Transfer Protocol): file transfer between machines.
- SMTP (Simple Mail Transfer Protocol), POP3 and IMAP: protocols used for sending and receiving emails.
- DNS (Domain Name System): name resolution service, enabling the translation of a domain name into an IP address.
- Telnet and SSH (Secure Shell): remote access to computer systems.
- SNMP (Simple Network Management Protocol): management and supervision of network equipment.

This layer is at the top of the OSI model and corresponds to the point of contact between the user and the network, as it provides the applications and services that use the data transported by the underlying layers.

2.7 Conclusion

Although the OSI model has not been implemented as such, it remains an essential conceptual framework for understanding the structure of computer networks. By breaking down the network into seven layers, it clarifies the functions of each level, promotes interoperability and facilitates technological evolution.

This chapter has presented layered architecture, the fundamental concepts of protocol, service and interface, the advantages of this approach, and then the OSI model and its seven layers.

In the following chapters, we will detail the characteristics, roles, and objectives of each of these layers of the OSI model in order to deepen our understanding.

Chapter 3
The physical layer

3.1 Introduction

The physical layer is the first level of the OSI model. It represents the hardware part of the network and defines how bits (0s and 1s) are actually transmitted between two remote systems. This layer does not deal with the content of the data, but only with its transport through a given medium (cable, fibre optic, radio waves, etc.).

It forms the essential basis for all communications: without the physical layer, no data can be transmitted.

3.2 General characteristics of the physical layer

The physical layer performs several essential functions [8]:

- Binary transmission of data via physical media (twisted pairs, fibre optics, radio waves, lasers, etc.).
- Definition of the electrical and mechanical characteristics of transmission media.
- Definition of binary transmission techniques (bit duration, signal shape, etc.).
- Definition of connector properties and pinout standards.
- Defining the capacity of a line to support unidirectional or bidirectional communications.

These characteristics form the technical foundations necessary for the upper layers of the OSI model.

3.3 Transmission line operating modes

Before studying transmission techniques, it is important to understand the different operating modes of a transmission line:

- Simplex communications between two devices only allow data to flow in one direction. The transmitter and receiver are two separate entities, and it is the transmitter that controls the transmission.

- Half-duplex communications allow data to travel in both directions on a single physical medium, but not simultaneously. The first transmitter initiates the communication.

- Full-duplex communications allow simultaneous bidirectional transfers on a line.

These modes directly influence the efficiency and speed of exchanges.

3.4 Signal transmission over the medium

Regardless of the transmission medium used, the constraint remains the same: digital information must be transmitted over an analogue medium in the most optimal way possible.

There are two transmission techniques [9]:

- Baseband transmission
- Broadband transmission

This distinction is important because it determines the range and efficiency of the transmission.

3.4.1 Baseband transmission

Binary data (digital signal) is transmitted directly over the cable without changing the frequency band used (baseband). It is used over short distances (local area networks).

The digital signal is transmitted directly without modulation. This mode is used over short distances, for example in local area networks (LANs).

Two distinct fixed voltage levels are matched, each corresponding to a logic level (1 or 0); this is called a coding operation [10].

When a digital signal is transmitted in baseband, it can be represented using different types of coding:

(a) ***RZ (Return to Zero) coding***

- Simple coding that consists of matching bit 1 to an electrical signal with a voltage of n volts and bit 0 to a signal with zero voltage.
- Problem: a zero voltage corresponds to the transmission of a binary 0 but can also correspond to the absence of data transmission.

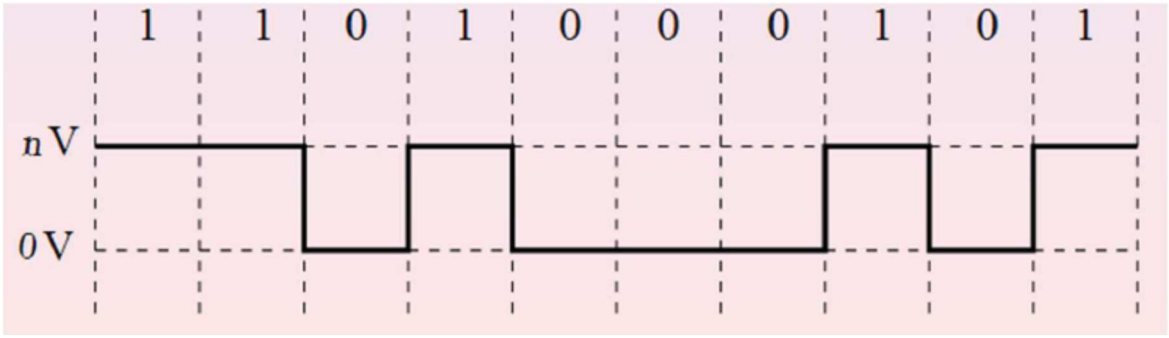

Figure 3.1 RZ coding [10]

(b) NRZ (No Return to Zero) coding

- Bit 1 is encoded by an n-volt signal and bit 0 by an opposite voltage of -n volts.
- Resolution of the problem of no signal on the cable.
- Problem: if a binary sequence contains several consecutive binary 0s or 1s, the transmitter and receiver must be perfectly synchronised for decoding to be performed correctly.

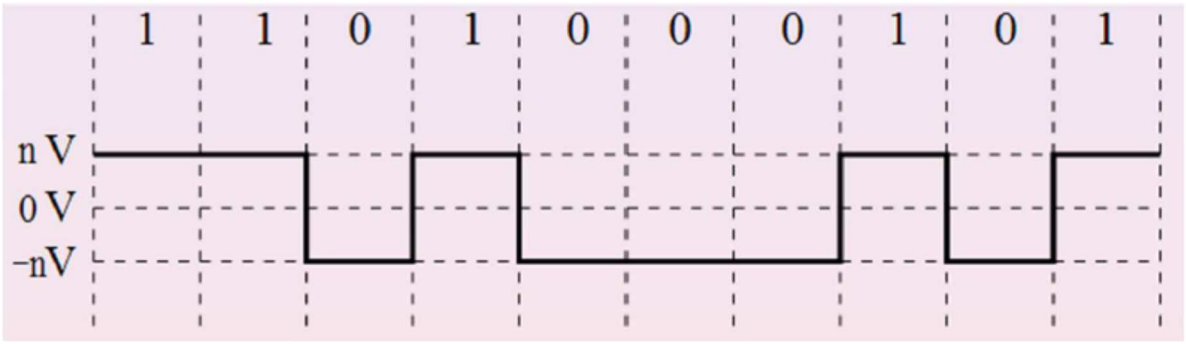

Figure 3.2 NRZ coding [10]

(c) Manchester coding

- This is a code based on signal variations: it is no longer the voltage that is important, but the signal difference.
- Bit 1 is encoded by a transition from voltage n to -n and bit 0 by the reverse transition.
- It offers a solution to the problem of detecting long strings of 0s or 1s.

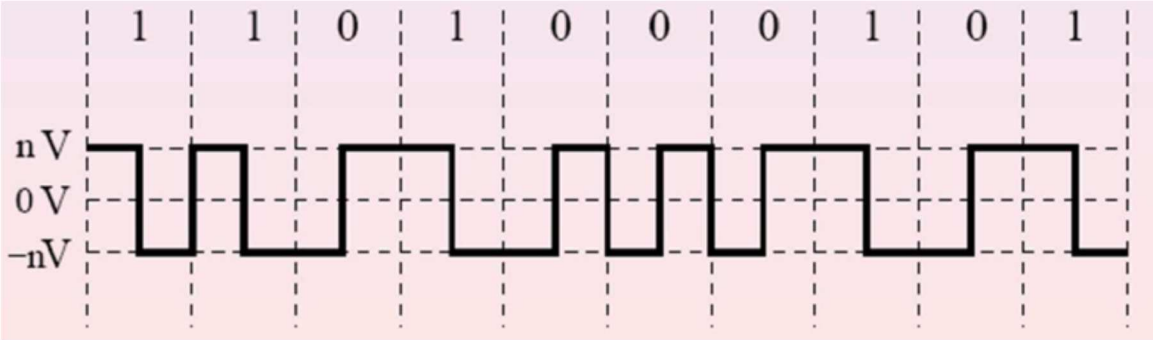

Figure 3.3 Manchester coding [10]

3.4.2 Broadband transmission

This involves transforming the digital signal into an analogue signal by modulation; this produces a single analogue signal that carries information through changes in its characteristics over time (frequency, amplitude, phase) [9].

This technique is used for high-speed transmissions over long distances (telephone lines, microwave links, etc.).

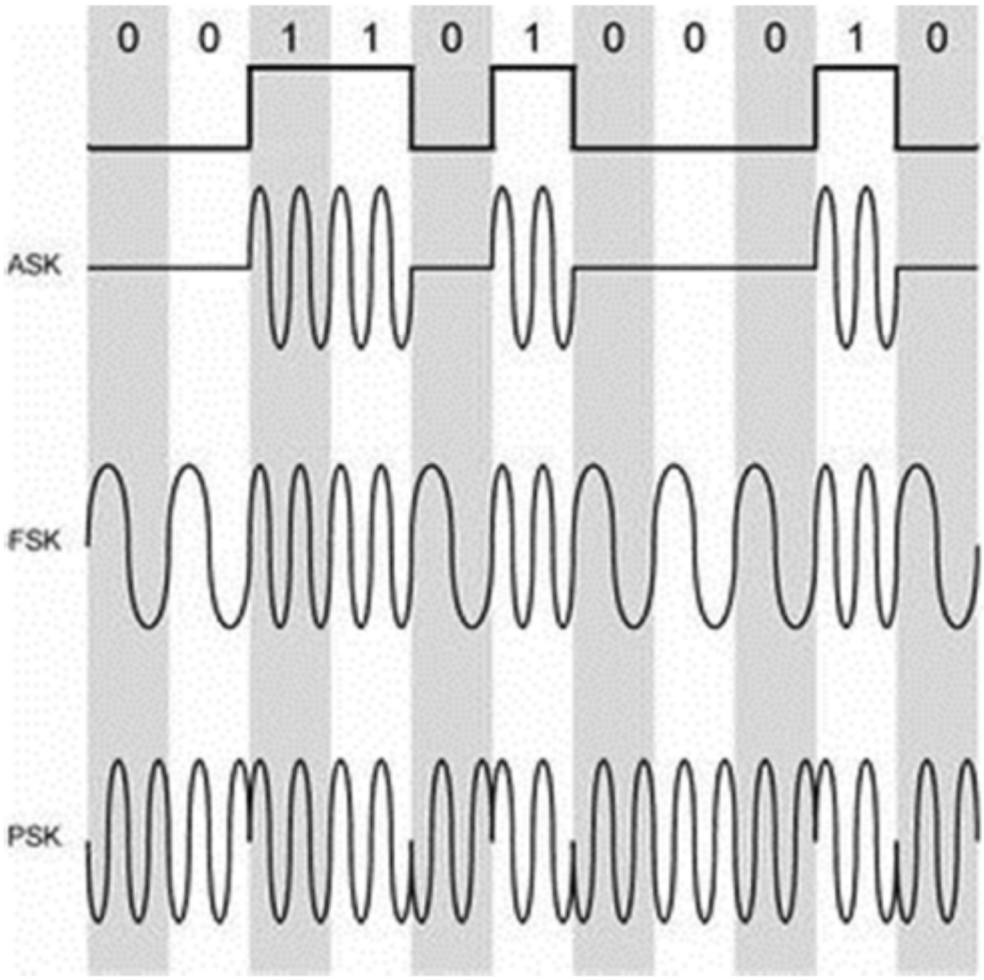

Figure 3.4 Different types of modulation [10]

3.4.3 Examples of transmissions

- RS-232 serial link: NRZ;
- USB: NRZI;
- Ethernet: Manchester;
- Token Ring: differential Manchester;
- Fibre optics: amplitude modulation;
- Telephony, ADSL: frequency modulation.

3.5 Bandwidth and speed

- Two fundamental concepts must be distinguished:
- **Bandwidth**: bandwidth represents the amount of information (in bits/s) that can be transmitted over a transmission medium (maximum possible amount).

- **Speed**: throughput is the amount of data that passes through a network during a given period of time (actual amount).

A medium may have a high theoretical bandwidth but a throughput limited by noise, interference or the protocols used.

Unit of Bandwidth	Abbrev.	Equivalence
Bits per second	bps	1 bps = fundamental unit of bandwidth
Kilobits per second	kbps	1 kbps = 1,000 bps = 10^3 bps
Megabits per second	Mbps	1 Mbps = 1,000,000 bps = 10^6 bps
Gigabits per second	Gbps	1 Gbps = 1,000,000,000 bps = 10^9 bps

Figure 3.5 Speed and bandwidth units [11]

3.6 Transmission media

There are different types of data transmission media. In computer networks, there are several types of transmission media:

- copper media: twisted pair cables and coaxial cables,
- fibre optics,
- radio waves for wireless networks.

3.6.1 Twisted pair cables

This is currently the most widely used physical medium. It is used in several cases:

- connecting a workstation to the network hub (hub, switch, etc.).
- interconnecting various types of active components (hubs, switches, repeaters, etc.).

The structure of this type of cable is simple, consisting of several copper wires twisted in pairs (to reduce crosstalk).

Generally, it consists of four twisted pairs (computer networks) and two pairs for telephone cables.

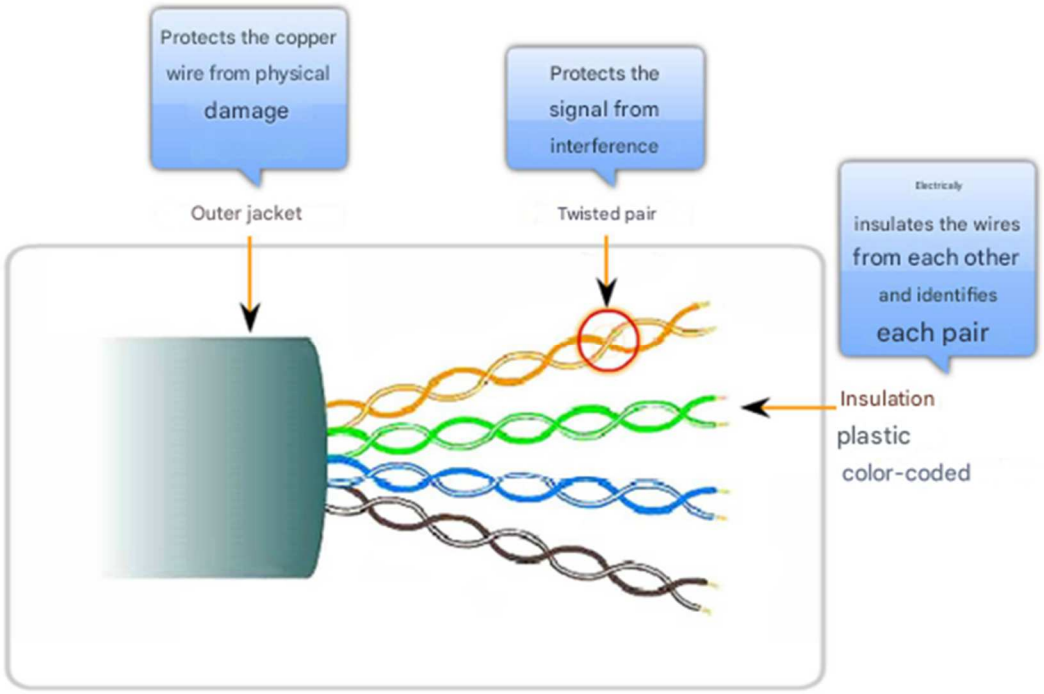

Figure 3.6 Twisted pair cable [11]

To limit interference, twisted pairs are often shielded. The type of cable depends on the shielding used:

1- Unshielded twisted pair (UTP) cable, the simplest and therefore least expensive medium.

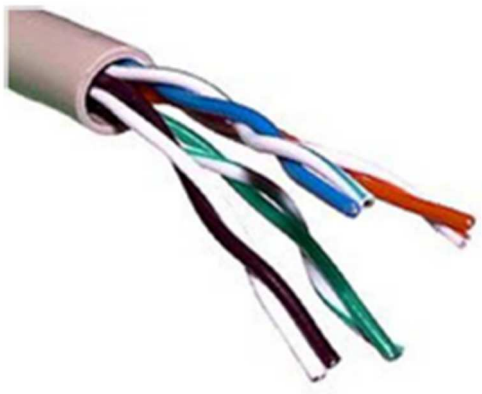

Figure 3.7 UTP cable [11]

2- Shielded cable, FTP (Foiled Twisted Pairs). The shield is a simple aluminium foil placed between the wires and the PVC sheath.

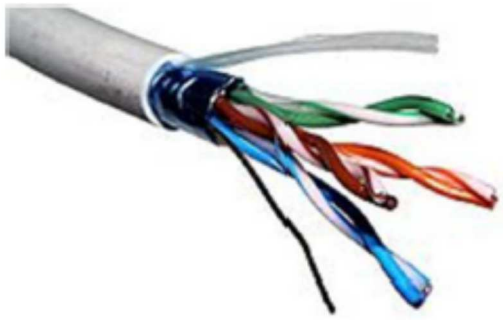

Figure 3.8 FTP cable [11]

3- Shielded cable, STP (Shielded Twisted Pair), each pair is protected from interference by a shield (aluminium foil or metal braid).

Figure 3.9 STP cable [11]

(a) Connectors and cabling standards

Connector: cabling termination→ RJ45 (8 pins).

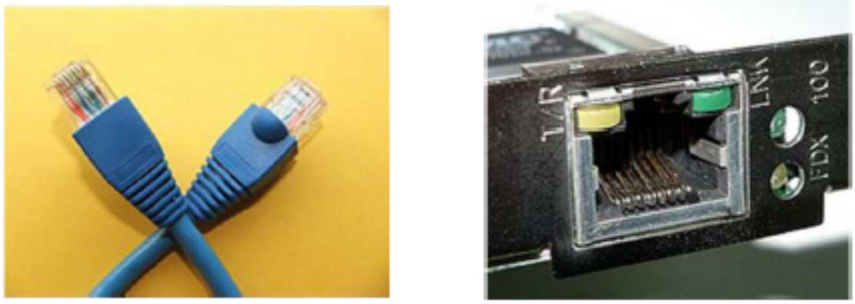

Figure 3.10 Connectors [11]

Two main cabling standards:

- T568A
- T568B

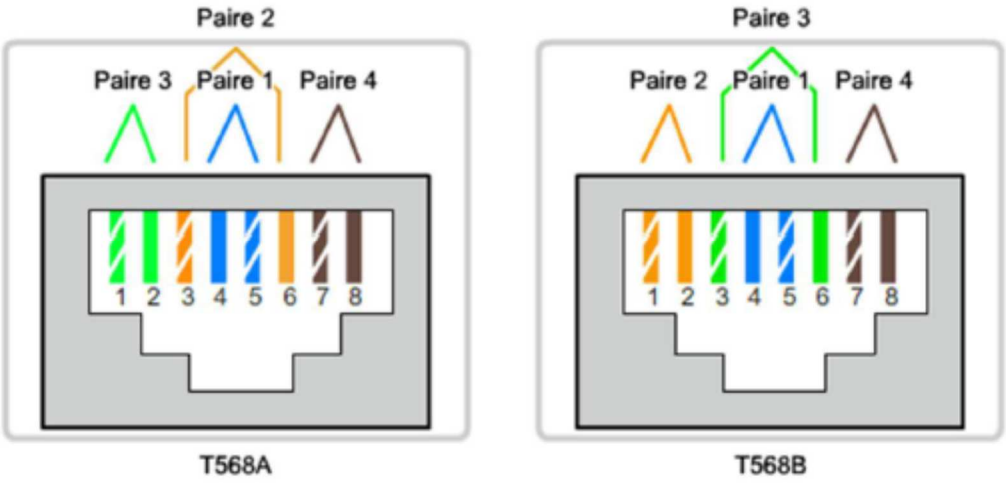

Figure 3.11 Wiring standards [11]

(b) Straight cables and crossover cables

Switches and hubs are identified as DCE (Data Connection Equipment), while terminal stations and routers are DTE (Data Terminal Equipment) devices. Identical DTE/DTE or DCE/DCE devices are connected using a crossover cable (which crosses the transmit and receive pairs). Different types of equipment are connected using a straight cable because the transmission and reception positions on their interfaces are already reversed.

New ranges of network equipment automatically adapt to cables by recognising the signal positions (transmission and reception) [11].

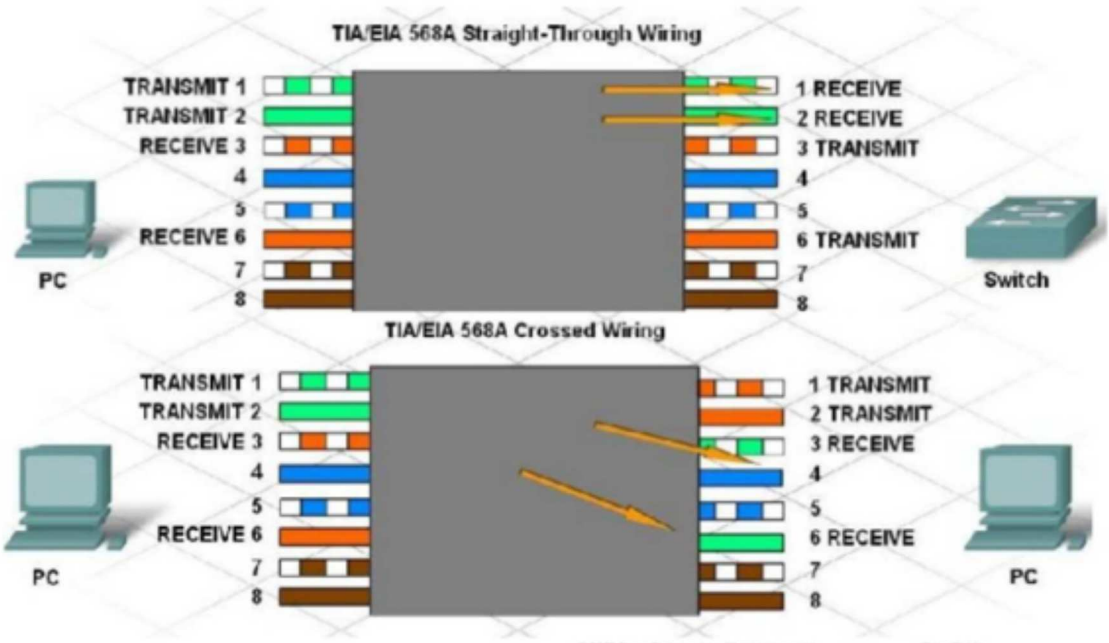

Figure 3.12 Straight cables and crossover cables [11]

(c) Advantages and disadvantages of twisted pair cables

Advantages: low cost, flexibility.

Disadvantages: range limited to 100 m, sensitive to electromagnetic interference.

3.6.2 Coaxial cable

Central copper conductor surrounded by insulation and a metal sheath. It is used in bus topologies. It uses a standard BNC connector.

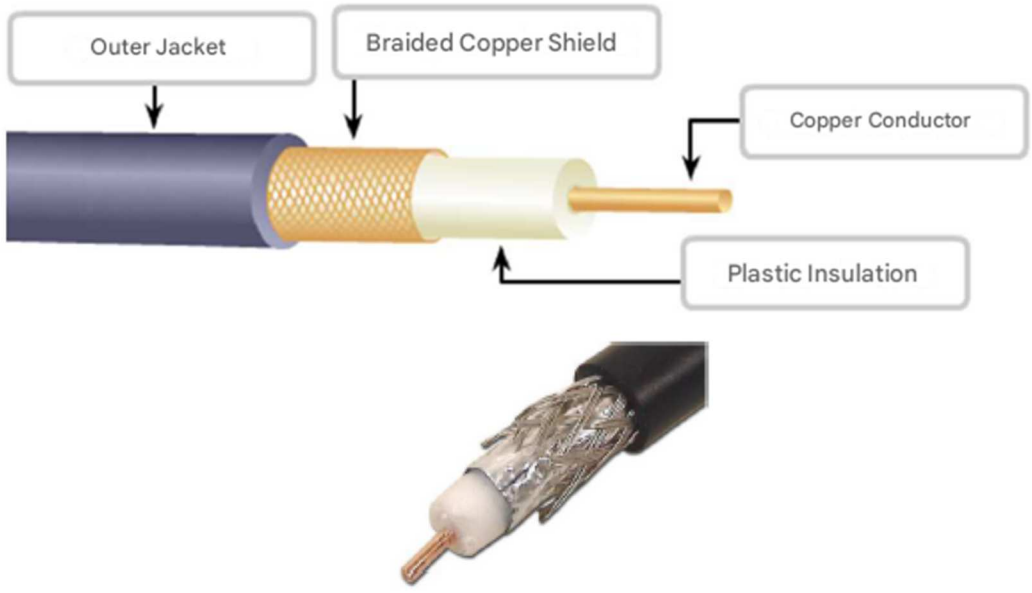

Figure 3.13 Structure of a coaxial cable [11]

Figure 3.14 BNC connectors [11]

(a) Advantages and disadvantages of coaxial cables

Advantages: maximum distance can reach 500 metres, good resistance to interference.

Disadvantages: rigidity, weight, obsolescence in modern networks.

3.6.3 Optical fibre

Optical fibre is a very thin glass or plastic wire that conducts light. It enables high-speed data transmission using optical rays.

The fibre connection is made by an optical transmitter that converts an electrical signal into a light signal. Its use is beneficial even in low-speed networks to reduce transmission error rates and the number of retransmissions.

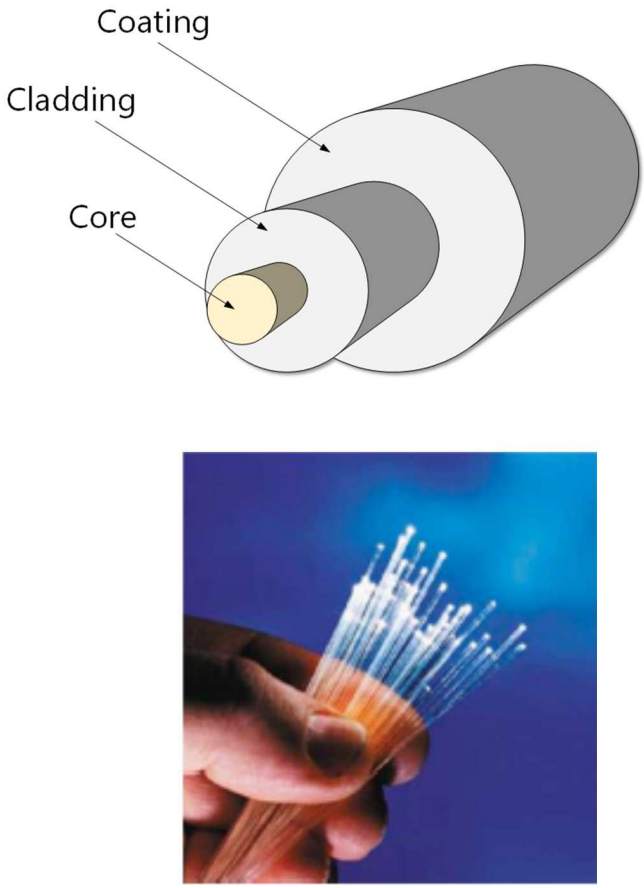

Figure 3.15 Structure of fibre optics [11]

There are two types of optical fibre [8]:

(a) Multimode fibres:

- The light beam is transmitted by successive refractions.
- Performance of approximately 1 Gbit/s over a maximum distance of one kilometre.
- Suitable for high-speed local area networks.
- The least expensive cable for optical fibres.

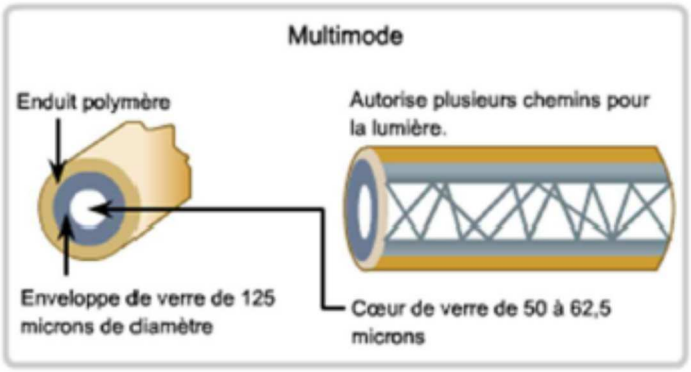

Figure 3.16 Structure of multimode optical fibre [11]

(b) Single-mode fibres

- Only transmits rays whose trajectory is the axis of the fibre.
- A laser beam is required at both ends.
- Data rates can exceed several tens of Gbit/s over long distances (wide area networks).
- Very high implementation cost, particularly due to the laser beams.

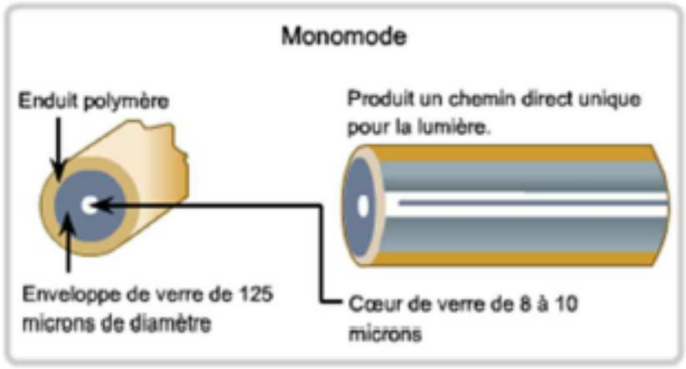

Figure 3.17 Structure of single-mode optical fibre [11]

(c) Advantages and disadvantages of optical fibres

Advantages: very high speed, low attenuation, insensitivity to electromagnetic interference.

Disadvantages: high cost, delicate installation.

3.6.4 Wireless networks

Wireless networks use media such as air or vacuum as a medium for transmitting electromagnetic waves: the airwaves.

Several types of electromagnetic waves are used, as shown in the figure below.

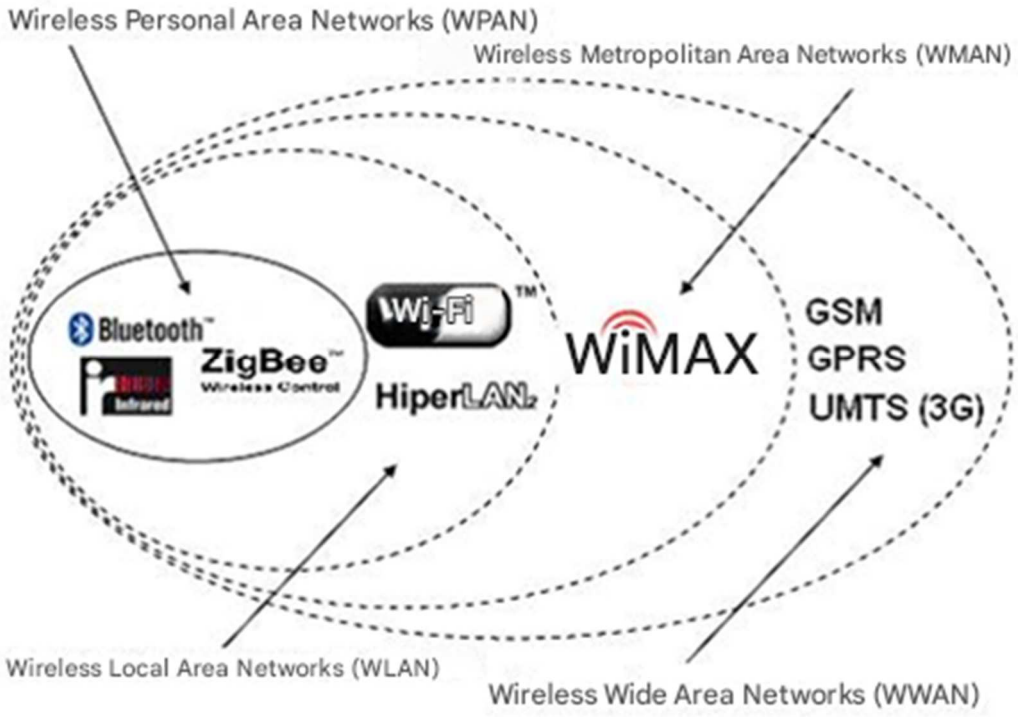

Figure 3.18 Types of wireless networks [9]

(a) Advantages and disadvantages of wireless networks

Advantages: mobility, flexibility and ease of deployment

Disadvantages: susceptibility to interference, more complex security.

3.7 Conclusion

The physical layer is the hardware foundation of the OSI model. It defines how binary data flows through a network via different media: twisted pairs, coaxial cables, fibre optics or electromagnetic waves.

This chapter has presented the main characteristics of the physical layer, its transmission modes, coding techniques and different media.

In the next chapter, we will discuss the data link layer, which uses the physical layer's service- to ensure reliable transmission, detect errors and organise exchanges between two nodes in a network.

Chapter 4
The data link layer

4.1 Introduction

After studying the physical layer, which deals with the raw transfer of bits over the medium, we now turn to the data link layer. This layer occupies the second position in the OSI model, just above the physical layer, and plays a fundamental role in ensuring reliable communication between two systems connected by a physical link.

Unlike the physical layer, which is limited to transmitting electrical or optical signals, the data link layer organises these bits into frames that can be understood by the upper layers. It manages error detection, flow control and access to the medium. In other words, it transforms a raw service into a structured and reliable service.

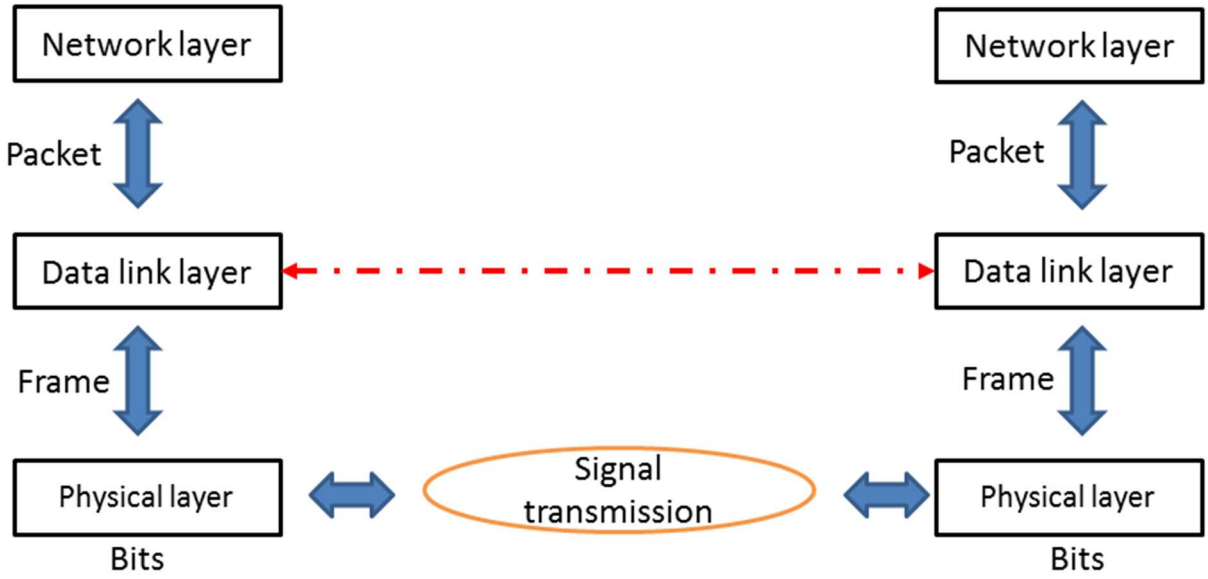

Figure 4.1 Location of the data link layer in the OSI model [12]

4.2 Role of the data link layer

The main role of this layer is to ensure the reliability of communications between two directly connected nodes. To do this, it must provide the following services:

- Frame segmentation: delimiting data from the network layer.
- Transmission media access control: which machine has the right to use the medium to send data.

- Addressing: physical identification of machines.
- Error control: ensuring error-free data transfer.
- Flow control: ensuring reliable data transfer.

Concrete example: if a PC sends a file to a printer via Ethernet, the link layer divides the file into frames, adds a control code (CRC) to detect errors, and then transmits them to the physical layer.

After these services, let's examine how the layer is organised to perform these functions.

4.3 Organisation of the data link layer

According to the IEEE 802 standard, this layer is divided into two sublayers [12]:

- LLC (Logical Link Control): provides services to the upper layers.
- MAC (Media Access Control): controls access to the physical medium and manages MAC addressing.

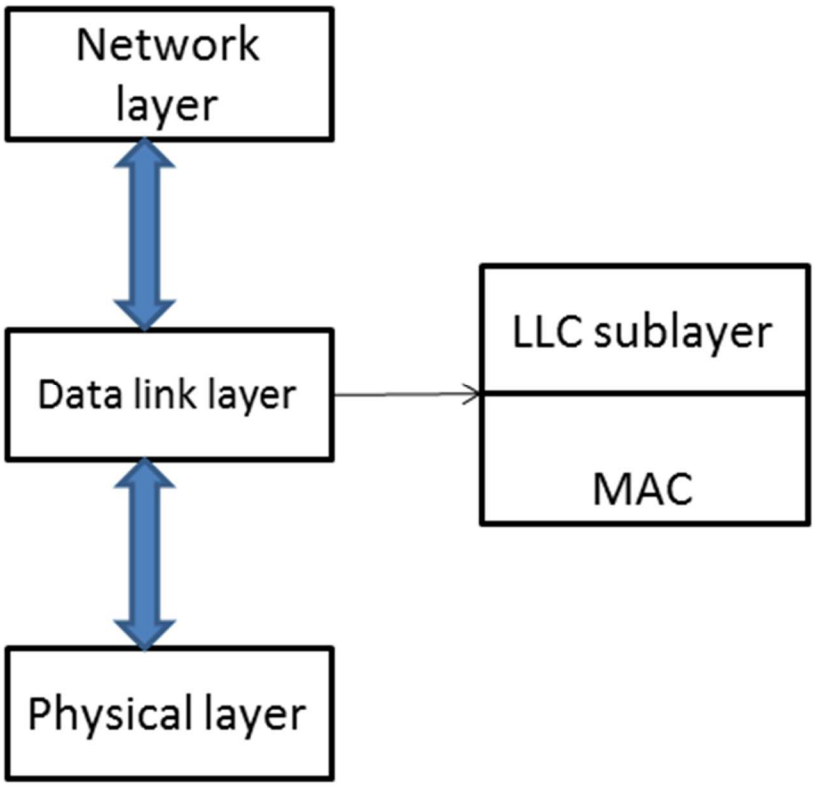

Figure 4.2 Organisation of the data link layer into sublayers [12]

Once this organisation has been understood, let us see how data is encapsulated in the form of frames.

4.4 Encapsulation and frames

The data link layer encapsulates data from the network layer into units called frames. A typical frame consists of:

- Preamble: a sequence of bits used for synchronisation.
- Source and destination physical addresses.
- Data field.
- CRC (Cyclic Redundancy Check) to detect errors.

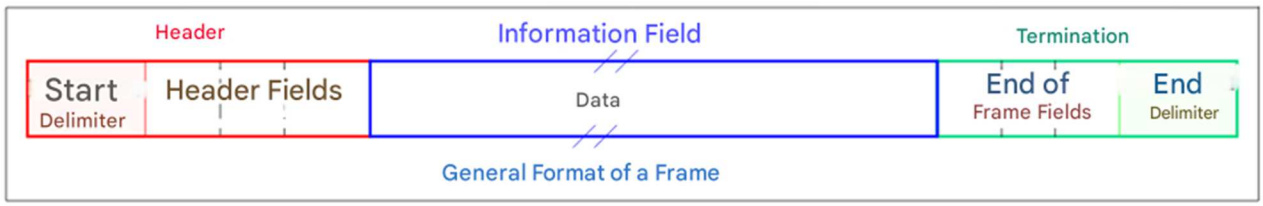

Figure 4.3 General format of a frame [10]

The start and end of a frame are often identified by delimiters consisting of a certain number of bits, each with a specific meaning.

Several delimiter techniques are possible:

- Special characters (IBM BSC protocol)
- Flags (HDLC protocol)
- Encoding violation (Ethernet protocol)

4.4.1 Special characters [10]

- Three characters are taken from the character set: DLE, STX and ETX
- The start is marked by the sequence DLE STX
- The end is marked by DLE ETX

- DLE is used for transparency: added before each DLE of data.

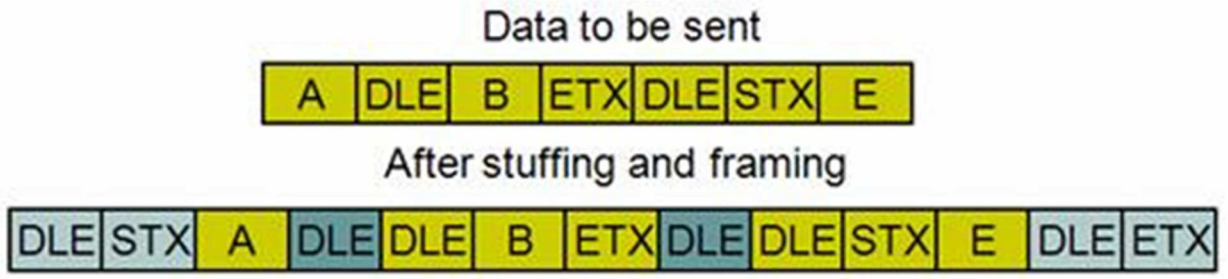

Figure 4.4 Delimiters: Special characters [10]

4.4.2 Flags

- A sequence of bits (flag) is the delimiter.
- Generally equal to 01111110
- A bit set to 0 is added after any sequence of 5 bits set to 1 in the data to ensure transparency.

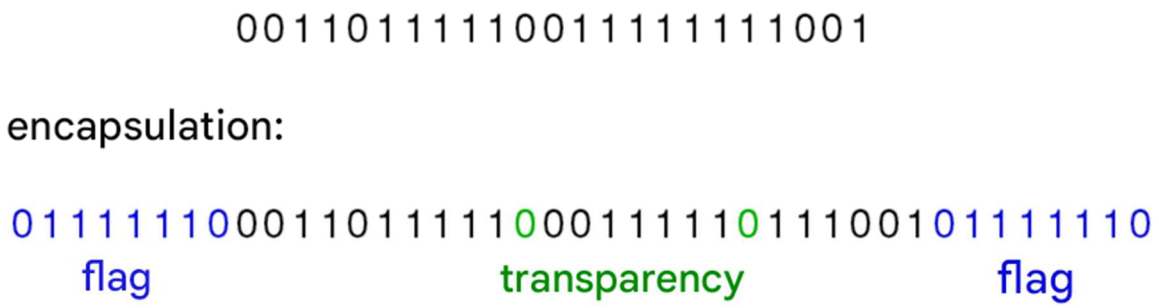

Figure 4.5 Delimiters: Flags

4.4.3 Encoding violation

Like the Ethernet protocol, which uses a frame start marker and performs a Manchester coding violation to detect the end of the frame.

Once the frames have been defined, let's see how to prevent multiple machines from sending simultaneously on a shared medium [12].

4.5 Media access control

In a multipoint link, several stations use the same transmission medium. When two (or more) stations send data (frames) simultaneously on the same medium, there is inevitably a collision (interference).

Physically, a collision means that the signals representing the data are mixed up and the information cannot be recognised. The data must be retransmitted at a later time.

There are several media access control protocols, the most commonly used being CSMA.

4.5.1 The CSMA method

The CSMA (Carrier Sense Multiple Access) method is based on listening to the transmission medium before sending a frame [12]:

- If the channel is free: transmit the frame.
- If the channel is busy: delay transmission.

CSMA reduces the number of collisions.

Problem: collisions may still occur during transmission:

- When two stations transmit their data simultaneously.
- When the transmitter listens to the medium, it may not detect the presence of a signal because the distance is too great.

4.5.2 The CSMA/CD method [11]

- CSMA/CD (Collision Detection) is CSMA with collision detection.
- After transmitting the frame, the transmitter remains listening to the medium in order to detect any collisions.
- In the event of a collision, the frame is then retransmitted after a random waiting period.

Now that we have seen how access is regulated, let's talk about the physical addressing that identifies each machine.

4.6 MAC address

A MAC address is a 6-byte encoded number that defines the physical address (hardware address) of a network card. The IEEE defines the format and assignment of MAC addresses, as they must be unique.

The MAC address is made up of two parts. The first part identifies the network card manufacturer (OUI - Organisationally Unique Identifier) and the second part is a number that has never been used by that same manufacturer (UAA - Universally Administered Address) [11]:

- Manufacturer ID (24 bits) (0-23)
- Serial number (24 bits) (24-47)

The MAC address is represented in hexadecimal form (example: 00:1A:2B:3C:4D:5E).

Below are some examples of OUI (Organisationally Unique Identifier):

- 00:00:0C Cisco
- 00:05:5D D-Link
- 00:06:BC 3Com
- 00:09:5B Netgear
- 00:90:69 Juniper
- 00:00:B4 Edimax

Commands to find the MAC address:

- Windows: ipconfig /all
- Linux: ifconfig (Hwaddr field)

4.7 Transmission error management

Errors are mainly related to transmission media. One or more bits of information may be changed during data transmission. Data may be corrupted or lost.

Errors are caused by interference (noise) or distortion [12].

4.7.1 Preventing transmission errors

To reduce interference, you must:

- Shield the wires.
- Ensure that cables are kept away from sources of interference (noise).

To reduce distortion, you must:

- Adjust transmission equipment and improve connection quality.
- Use amplifiers and repeaters.
- Use higher quality cables.

The risk of errors always exists, but it must not exceed a certain threshold of 10^{-8} to 10^{-10}

4.7.2 Error control

- It must be possible to detect and correct errors.
- In general, to transmit k bits of information, r bits known as check bits are added.
- This is referred to as code(n, k) or code word.
- The check bits are calculated based on the information bits.
- In total, n= k + r bits are transmitted.
- Upon reception, the check bits are recalculated to ensure that the information has been received correctly.

4.7.3 Error checking

There are several error control methods [12]:

- Detection (detector code): This type of code can detect changes in one or more information bits. However, it cannot correct these errors.
- Detection and correction (correction code): This type of code can detect changes in one or more information bits. In addition, it has the ability to correct these errors.

The most commonly used detection techniques are:

- VRC (Vertical Redundancy Check): Vertical parity.
- LRC (Longitudinal Redundancy Check): Longitudinal parity.
- CRC (Cyclic Redundancy Check): Polynomial check.

(a) Vertical parity: VRC

- The oldest mechanism.
- Calculate parity and add a bit to the information sent:
  - **Even parity**: if the number of 1s in the information is even, then the parity bit is equal to 1, otherwise 0
  - **Odd parity**: if the number of 1s in the information is odd, then the parity bit is equal to 1, otherwise 0

Example:

  - If we use odd parity for the information **1100100,** we add **1**
  - The information to be sent is: **11001001**
- Error detection with CRC consists of:
  - **recalculating** the parity bit upon reception and comparing it with the received parity bit.
- The information received is **11001001**
  - The parity bit corresponding to the information: **1100100** is equal to **1,** so the information received is correct.

Disadvantages:

  - The error is detected, but it is not possible to know which bit has changed.
  - If the number of bits that change is even, then it is impossible to detect the error. (1100100→ **1110000**)

(b) Longitudinal parity: LRC

This involves applying the principle of parity (even or odd) to the columns of a data block.

Character	ASCII code
D	1000100
A	1000001
T	1010100
A	1000001
LRC	**1101111**

Figure 4.6 LRC parity (Example: sending the DATA message) [12]

The LRC technique is more effective than the VRC technique.

It is impossible to detect the error if two bits are changed at the same time in the same column.

For greater efficiency, add a check on the lines.

Character	ASCII	Parity bit
D	1000100	1
A	1000001	1
T	1010100	0
A	1000001	1
LRC	1101111	1

Figure 4.7 Enhanced LRC [12]

(c) CRC: Polynomial verification

Binary information can be written in polynomial form according to powers of 2.

$$(1110)_2 = 1*2^3 + 1*2^2 + 1*2^1 + 0*2^0$$

In the general case:

$$(u_k u_{k-1} \ldots\ldots\ldots u_1 u_0)_2 = u_k.X^k + u_{k-1}.X^{k-1} + \ldots\ldots\ldots + u_1.X^1 + u_0.X^0 \text{ avec } u_i \in [0,1]$$

Example:

The sequence 1100101 is represented by the polynomial

$$\begin{aligned} 1100101 &= 1.X^6 + 1.X^5 + 0.X^4 + 0.X^3 + 1.X^2 + 0.X^1 + 1.X^0 \\ &= X^6 + X^5 + X^2 + 1 \end{aligned}$$

Calculation of the CRC

- A polynomial called the generator polynomial **G(X)** of degree **n** is chosen
- Example: generator polynomial $\mathbf{X^4 + X^2 + X}$ of degree **4**
- Let us consider **m** bits of information represented in the form of a polynomial **M(X)** of degree **m**
- To calculate the CRC:
    - multiply the polynomial **M(X)** by $\mathbf{X^n}$ (n is the degree of the generator polynomial)
    - divide $\mathbf{X^n}$ **.M(X)** by **G(x)**
    - to obtain the quotient **Q(X)** and the remainder **R(X)**

$$X^n\ M(X) = Q(X).G(X) + R(X)$$

    - The CRC corresponds to the remainder of the division **R(X)**
- Therefore, the information to be sent is equal to: **M(X).R(X)**

Calculation of the CRC by successive additions

- Let **G(X)** be a generator polynomial of degree **n**. We transform it into a binary word.

Example:

  - With the generating polynomial $\mathbf{X^4 + X^2 + X}$, we obtain **10110**
  - We add **n** zeros to the binary word to be transmitted, where **n** is the degree of the generator polynomial.
  - We want to transmit the word **11100111** using the generator polynomial $\mathbf{X^4 + X^2 + X}$, which gives us **111001110000**

- We will iteratively add (or successively exclude) to this word the word corresponding to the generator polynomial until the resulting word is less than the generator polynomial.
- This word corresponds to the CRC to be added to the word before it is transmitted.

CRC example

- Let us take the information 11100111 and the generating polynomial $X^4 + X^2 + X$
- $G(X) = X^4 + X^2 + X$
- $M(X) = X^7 + X^6 + X^5 + X^2 + X^1 + 1$
- Multiply M(X) by X^4
- $M(X).X^4 = X^{11} + X^{10} + X^9 + X^6 + X^5 + X^4$

  = **111001110000**

The solution to this example is illustrated in Figure 4.8.

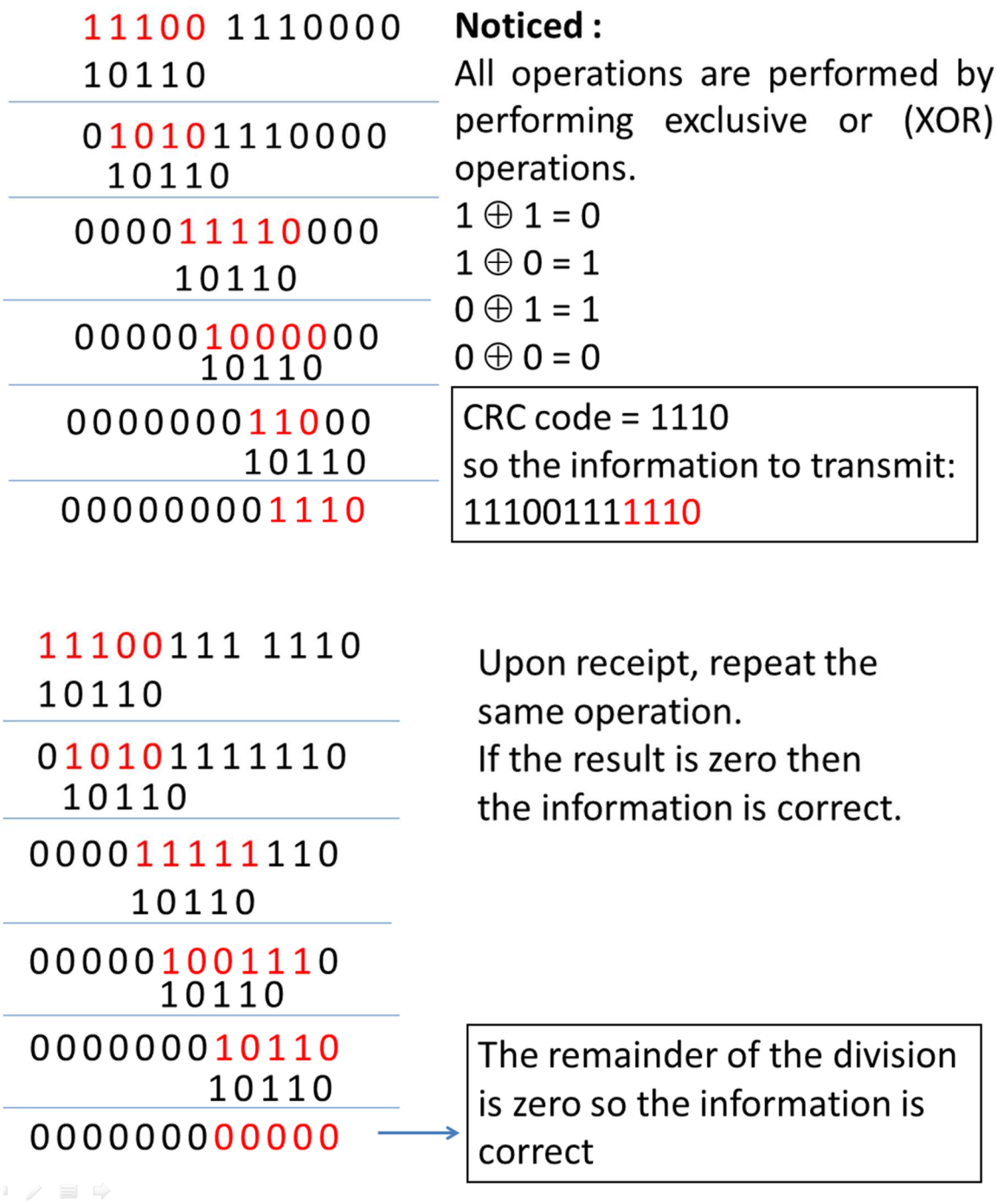

Figure 4.8 CRC example solution

4.8 Some data link layer protocols

- Ethernet (IEEE 802.3): dominant in wired networks.
- Wi-Fi (IEEE 802.11): for wireless local area networks.
- PPP: for direct connections.

- HDLC: for serial connections.
- Frame Relay: used in older WAN networks.

4.8.1 Ethernet

Ethernet is currently used in almost all corporate local area networks (LANs).

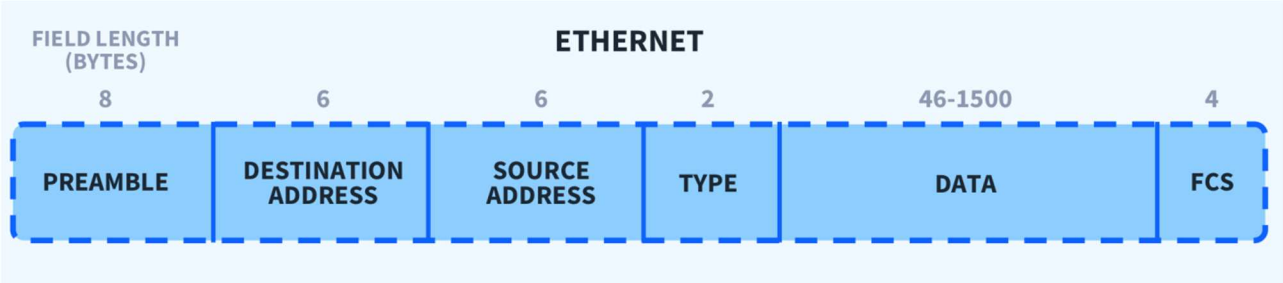

Figure 4.9 Ethernet frame format [14]

The different fields of the Ethernet frame are as follows:

- Preamble (8 bytes): announces the start of the frame and allows receivers to synchronise. It contains 8 bytes with a value of **10101010** (alternating 1s and 0s), except for the last byte, where the last 2 bits are 1.
- Destination and Source Address (6 bytes): MAC address of the Ethernet interface (network card) receiving (or sending) the frame.
- EtherType (2 bytes): frame type, indicates the network layer protocol encapsulated in the frame.
- Data (46 to 1500 bytes): the data carried by the frame.
- CRC (Cyclic Redundancy Code): error checking is performed by a CRC code based on the CRC-32 generator polynomial.

4.9 Conclusion

The data link layer is an essential part of the OSI model. It provides a reliable service by organising transmission into frames, detecting errors and controlling access to the medium. Without it, communications would be chaotic and prone to frequent data loss.

In the next chapter, we will study the network layer, which handles data routing between separate networks, introducing the concepts of logical addressing and routing.

Chapter 5
Network Layer

5.1 Introduction

In the OSI model, the network layer occupies a central position: it sits above the data link layer and below the transport layer. This layer plays an essential role in communication between remote systems, as it enables data to be routed from its source to its destination, even if the two systems are on different networks.

Unlike the previous layers, which manage local or physical connections, the network layer introduces a global view of the network. It is no longer limited to transmitting frames between two directly connected machines, but handles the passage of data through intermediate equipment called routers.

In other words, the network layer is the starting point for the concept of network interconnection, which is the basis for the functioning of the Internet and wide area networks. It is responsible for choosing the most appropriate path for the data and ensures its transport from one end of the network to the other, regardless of the media and technologies used.

Now that we have located the network layer in the OSI model and explained its importance, let's examine its specific role and responsibilities.

5.2 Role of the network layer

Routes data packets between the sender and the recipient across different networks (network meshing).

The network layer offers two basic functions:

- Logical addressing (machine identification): each machine must have a unique logical address within a network.
- Routing: the network layer allows a machine to be found in a network using a route specifying how the machine can be reached.

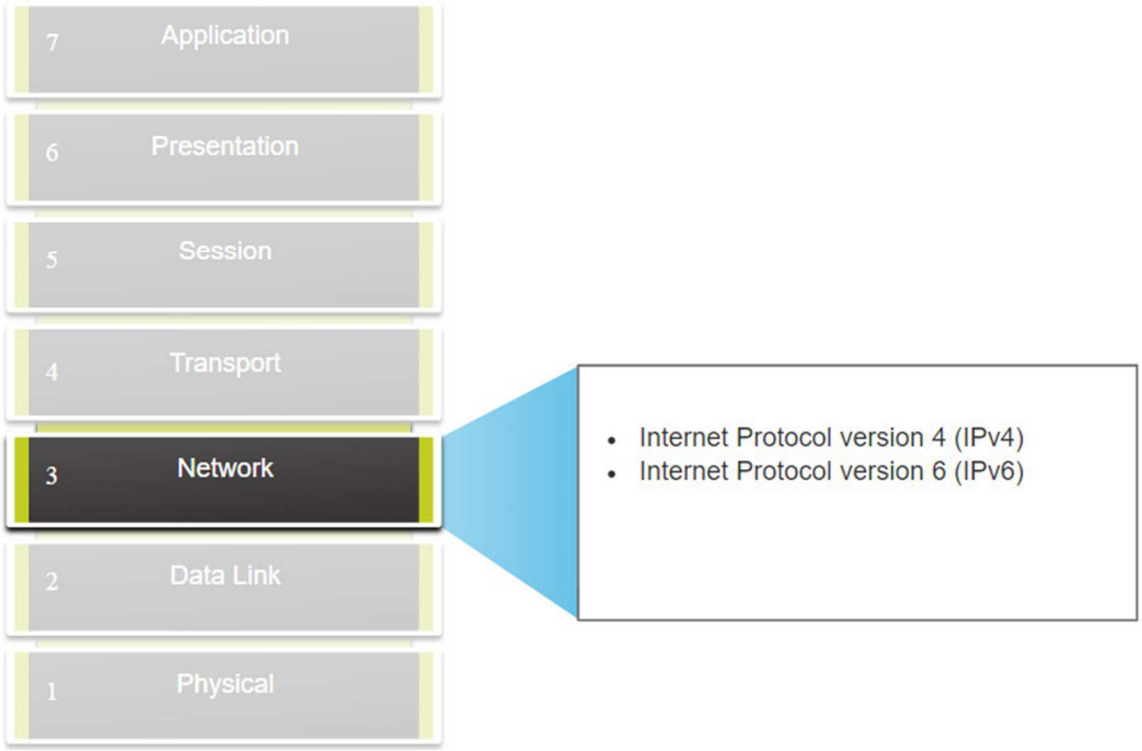

Figure 5.1 Network layer [11]

Now that we have presented the general functions, let's take a look at how the network layer performs logical addressing.

5.3 Logical addressing (IPv4)

- Each host (machine) has a unique address.
- The address is a logical address, not a physical one (it can be changed).
- Addresses are grouped according to the network number (network address).

5.3.1 IP address

- An IP address is encoded on 32 bits (4 bytes).
- Each combination (2^{32} combinations) represents an address.

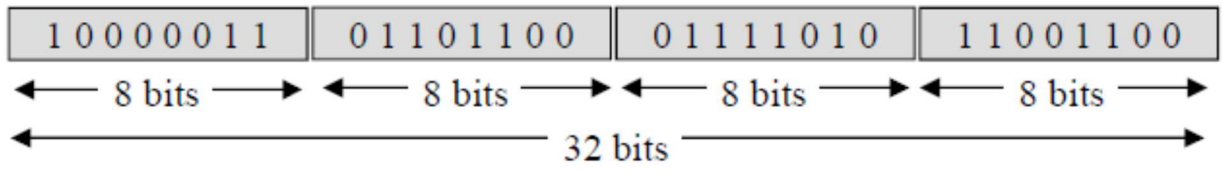

Figure 5.2 IP address in binary [3]

– It is practically impossible to memorise 32 bits→ , an IP address is represented in decimal format with 4 numbers separated by dots.

– This is known as “dot decimal notation”.

(a) Decimal dotted notation for IP addresses

– Each 8 bits of the address represents a decimal number.

– This decimal number represents a value between 0 and 255.

Example 1

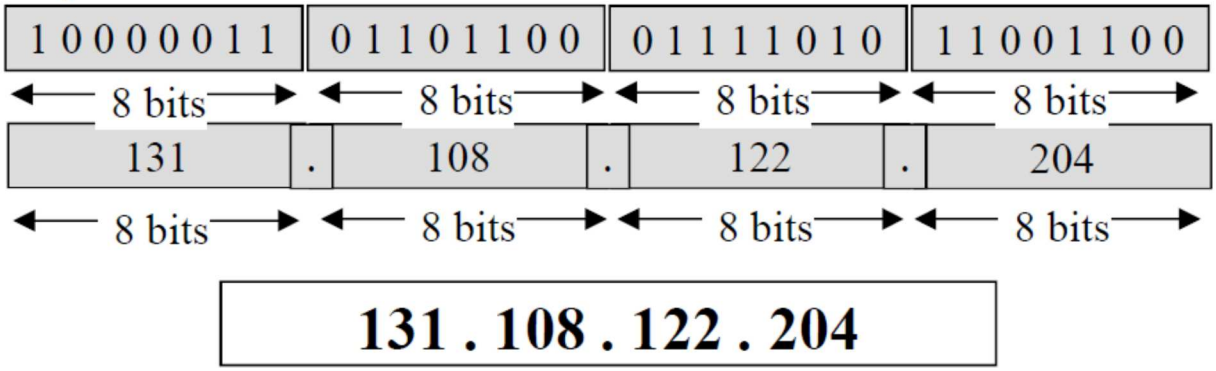

Figure 5.3 Dotted decimal notation [3]

Example 2

The address **131.108.122.264** is invalid because the last number is greater than 255.

5.3.2 Fields of an IP address

An IP address consists of two parts:

– A **network number (NET-ID)**: a global address to identify a network; this address is common to all machines on that network.

– **A machine (host) number**: identifies a machine on a network.

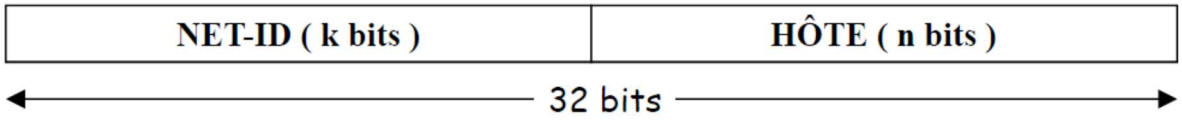

Figure 5.4 Fields of an IP address [3]

Example

Consider the network with the number **192.168.1.0.** The machines on this network have the following addresses: **192.168.1.1, 192.168.1.2, 192.168.1.3, 192.168.1.4, 192.168.1.5, 192.168.1.6**

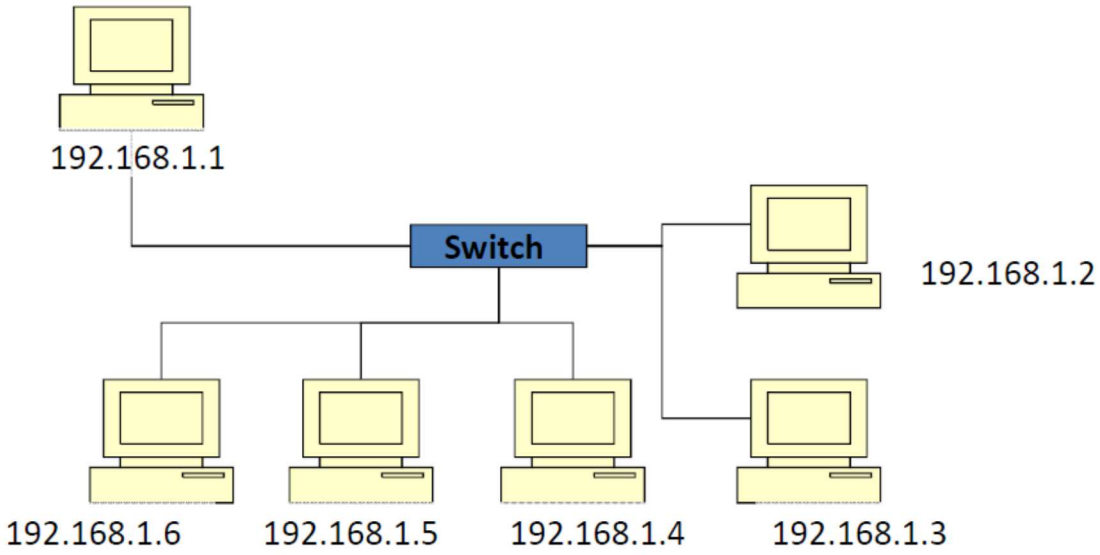

Figure 5.5 Example IP network [3]

5.3.3 IP address classes

The size of the network portion (net-id) determines the class of the IP address. IP addresses are classified into three classes (Figure 5.6)

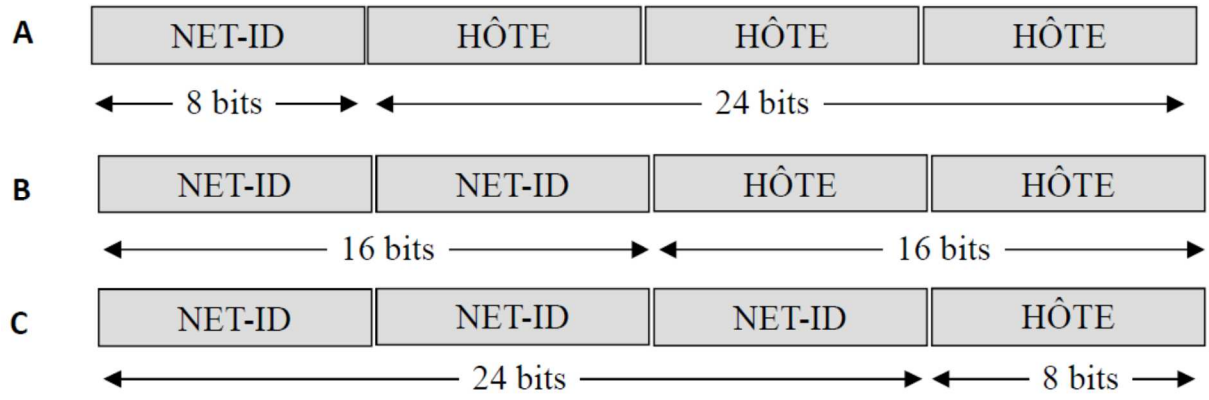

Figure 5.6 The three classes of IP addresses [3]

5.3.4 Class A IP address

- The first octet is reserved for the network, and the next three octets (24 bits) are reserved for hosts.
- The first octet of a Class A IP address always starts with bit **0** (7 bits remain).

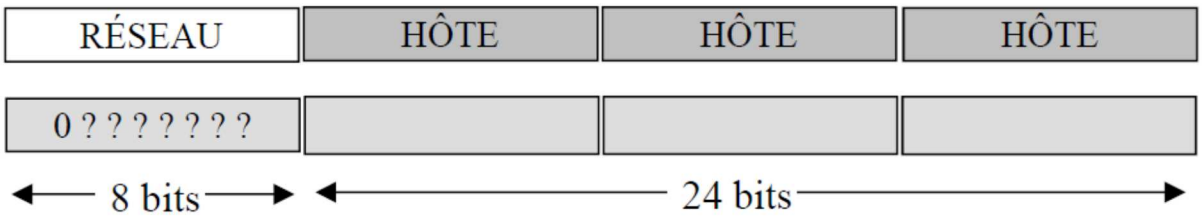

Figure 5.7 Class A IP address [3]

- **Number of available networks**: 2^7 = 128 networks.
- **Number of available hosts**: 2^{24} - 2 = 16,777,214 hosts.

Example

90.25.48.10 corresponds to a Class **A** address.

01011010 00011001 00110000 00001010

5.3.5 Class B IP address

- The first 2 bytes are reserved for the network, the next 2 bytes (16 bits) are reserved for hosts.
- The first byte of a Class B IP address always begins with the bit sequence **10** (14 bits remain).

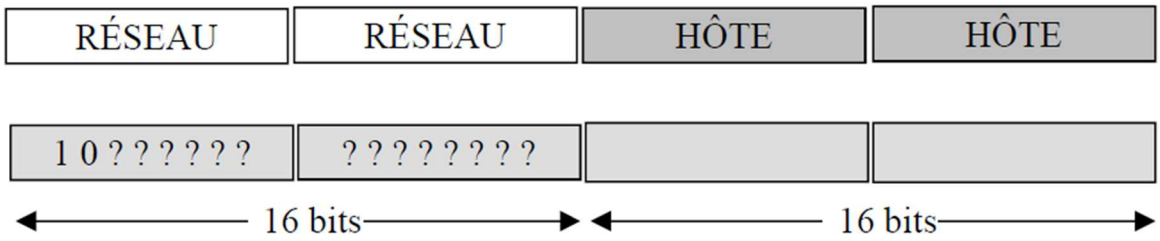

Figure 5.8 Class B IP address [3]

- **Number of available networks**: 2^{14} = 16,384 networks.
- **Number of available hosts**: 2^{16} - 2 = 65,534 hosts.

Example

130.100.20.10 corresponds to a class **B** IP address.

10000010 01100100 00010100 00001010

5.3.6 Class C IP address

- The first 3 bytes are reserved for the network, the next byte (8 bits) is reserved for hosts.
- The first octet of a class C IP address always begins with the bit sequence **110** (21 bits remain).

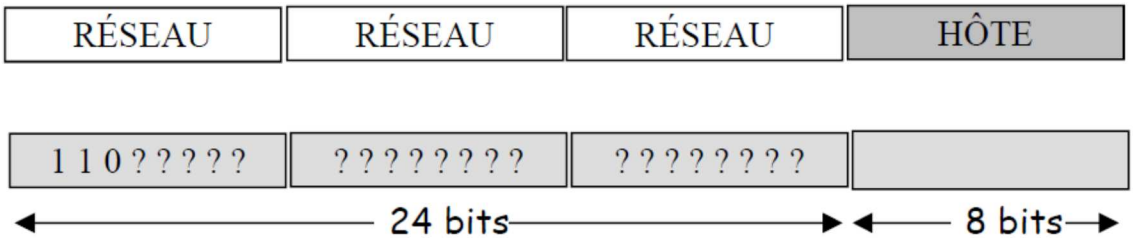

Figure 5.9 Class C IP address [3]

- **Number of available networks**: 2^{21} = 209,752 networks.
- **Number of available hosts**: 2^{8} - 2 = 254 hosts.

Example

192.5.5.11 corresponds to a class **C** address.

11000000 00000101 00000101 00001011

5.3.7 Special IP address classes

There are two other special IP address classes:

- Class D: reserved for multicast communications (group communications)
- Class E: Class E addresses are reserved for experimentation.

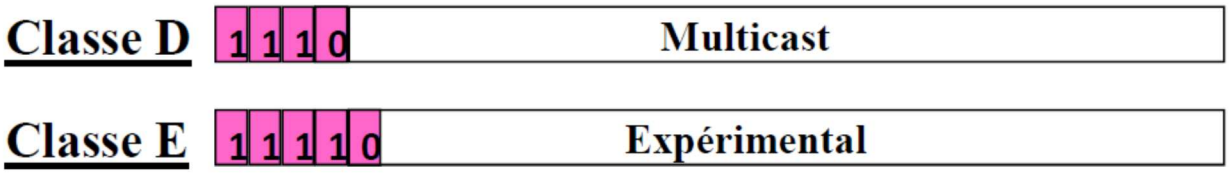

Figure 5.10 Class D and E IP classes [3]

Example

The address 226.5.5.11 is class D

11100010 00000101 00000101 00001011

The address 242.5.5.11 is class E

11110010 00000101 00000101 00001011

5.3.8 Class A IP address range

- from **0**0 00 00 01 . 00 00 00 00 . 00 00 00 00 . 00 00 00 00
- to **0**1 11 11 11 . 11 11 11 11 . 11 11 11 11 . 11 11 11 11
- The range of possible addresses: **1.0.0.0** to **126.255.255.255**

Note:

- The address **0.b.c.d** does not exist.
- The address **127.b.c.d**, where b, c and d are numbers between 0 and 255, represents a loopback address. In this case, the packet is sent to the same host without being transmitted over the network. It is used even if there is no physical network interface on the machine.

5.3.9 Class B and C IP address ranges

Class B:

- from **10** 00 00 00 . 00 00 00 00 . 00 00 00 00 . 00 00 00 00
- **10** 11 11 11 . 11 11 11 11 . 11 11 11 11 . 11 11 11 11
- The range of possible addresses: from **128.0.0.0** to **191.255.255.255**

Class C:

- from **11 0**0 00 00 . 00 00 00 00 . 00 00 00 00 . 00 00 00 00
- to **11 0**1 11 11 . 11 11 11 11 . 11 11 11 11 . 11 11 11 11
- The range of possible addresses: from **192.0.0.0** to **223.255.255.255**

5.3.10 Network address

If the host part consists solely of **zeros,** then this address corresponds to the network address (network identity). A network address cannot be assigned to a machine (invalid address).

Example

- In the class A address:
  90.25.48.10: the address **90.0.0.0** corresponds to a network address.
- In the class B address:
  130.100.20.10: the address **130.100.0.0** corresponds to a network address.
- In a Class C address:
  192.5.5.11: the address **192.5.5.0** corresponds to a network address.

An address that only contains 0s in the network and host parts (**0.0.0.0**) refers to all networks (default route, see routing).

5.3.11 Broadcast address

- Broadcast address: Broadcasting occurs when a source sends data to all units on a network.
- All machines on the same network receive the data packet.
- When an address contains only **1** in the host part, it is called a broadcast address.
- A broadcast address cannot be assigned to a machine (invalid address).

Example

- The broadcast address corresponding to Class A address **90.25.48.10** is **90.255.255.255**

- The broadcast address corresponding to the Class B address **130.100.20.10** is **130.100.255.255**
- The broadcast address corresponding to the Class C address **192.5.5.11** is **192.5.5.255**

5.3.12 Network mask

This is a combination of bits used to describe the portion of an address that designates the network and the portion that designates the host.

It is calculated as follows:

- Express the IP address in binary format.
- Replace all bits in **the network portion of the address with 1**.
- Replace all bits in **the host portion of the address with 0**.
- Finally, convert the binary address to decimal format.

The default mask for:

- Class A: 255.0.0.0➔ /8
- Class B: 255.255.0.0➔ /16
- Class C: 255.255.255.0➔ /24

Example 1: Class A

Let's say the IP address is **12.30.10.2** with the network mask **255.0.0.**0 → **12.30.10.2/8**

Network information

- Class: **A**
- Number of bits for the network portion: **8**
- Number of bits for the host portion: **24**
- Network address (network identity): **12.0.0.0**

- Broadcast address: **12.255.255.255**
- Valid address of the first host on the network: **12.0.0.1**
- Valid address of the last host on the network: **12.255.255.254**

Example 2: Class B

Let's take the IP address: **172.30.10.2** with the network mask: **255.255.0.0→ 172.30.10.2/16**

Network information

- Class: **B**
- Number of bits for network: **16**
- Number of host bits: **16**
- Network address (network identity): **172.30.0.0**
- Broadcast address: **172.30.255.255**
- Valid address of the first host on the network: **172.30.0.1**
- Valid address of the last host on the network: **172.30.255.254**

Example 3: Class C

Let's take the IP address: **192.130.10.2** with the network mask: **255.255.255.0→ 192.130.10.2/24**

Network information:

- Class: **C**
- Number of bits for network: **24**
- Number of host bits: **8**
- Network address (network identity): **192.130.10.0**
- Broadcast address: **192.130.10.255**
- Valid address of the first host on the network: **192.130.10.1**

– Valid address of the last host on the network: **192.130.10.254**

5.3.13 Public IP addresses

– Public IP addresses are assigned to companies and organisations by **ICANN** (Internet Corporation for Assigned Names and Numbers) to ensure **that these addresses are unique**.

– These IP addresses are known as **public (visible on the Internet)**.

– Public addresses are unique.

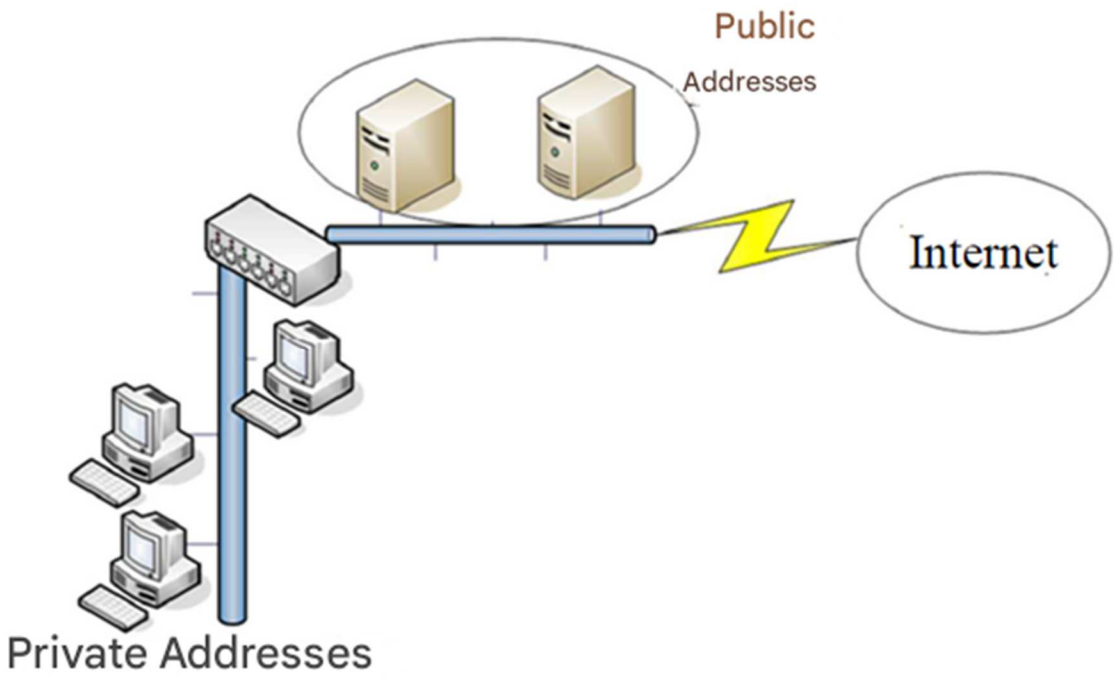

Figure 5.11 Public and private IP addresses [4]

5.3.14 Private IP addresses

– Used in a private (local) network.

– If the machines on a network do not need to be visible from the outside (Internet).

– This does not require a public IP address, so private addresses (which can be reused in other networks) can be used.

– Private IP address ranges:

- **1** Class A network: **10.0.0.0** to **10.255.255.255**
- **16** class B networks: **172.16.0.0** to **172.31.0.0**
- **256** class C networks: **192.168.0.0** to **192.168.255.0**

5.3.15 Static/dynamic IP address allocation

- There are several ways to assign an IP address to a computer:
- Some machines always have the same address (static address): this address is assigned manually (using a command or via a graphical interface):
  - Linux: ***ifconfig eth0 192.168.0.5 netmask 255.255.255.0***
- Some machines have an address that changes each time they start up (dynamic address): this address is assigned dynamically and automatically by another machine (DHCP server: Dynamic Host Configuration Protocol):
  - Linux: ***iface eth0 inet dhcp***

5.4 Subnets

5.4.1 Creating subnets

- The main problem with IP addresses is the waste of address space→ s of reserved but unassigned addresses.
- For example:
  - If there are 50 machines in a network→ , this requires 50 addresses.
  - The most appropriate class is class C (e.g. 193.220.12.0), which has 254 hosts→ using only 50 addresses.
  - However, the remaining addresses (204 addresses) are unused and cannot be assigned elsewhere since the network address is already allocated.
- So why not use the addresses of a network with a capacity that meets your needs without wasting addresses? This is equivalent to taking part of the global network instead of taking all the addresses offered by that network.

5.4.2 Problems

- How to determine subnets (how to determine the address of each subnet).
- How to calculate the subnet mask.
- How to calculate the range of valid addresses for each subnetwork.
- How to calculate the broadcast address of each subnetwork.

5.4.3 Principle of subnet division

To perform this division:

- Take **n** bits from the **host** part→ . These bits must be reassigned to the **network part** in the address.
- The number of bits borrowed depends on the number of **subnets** you want to have and the number **of hosts** in each subnet.

Example

- If you want to have two subnets, borrow 1 bit (2^1).
- If you want to have 4 subnets, borrow 2 bits (2^2).
- If you want to have 7 subnets, borrow 3 bits (2^3 = subnets)→ , use only 7.

5.4.4 Principle of subnet division

- This operation is often referred to as "borrowing" bits.
- Bits are always borrowed from the leftmost host bit.
- Each combination of borrowed bits represents a subnet (2^n subnets).
- The number of bits remaining determines the number of addresses that can be used in the subnet.
- ($2^{\text{number of remaining host bits}}$) – 2 = usable addresses (number of hosts).
- The subtraction corresponds to the two reserved addresses, which are the network address and the network broadcast address.

Example

- Let's take the address of a class C network: **192.55.12.0**
- In binary: **11000000.00110111.00001100.00000000**
- Assuming we want to have 4 subnets:
    - In this case, we take two bits from the host part (each subnet will have $2^6 - 2 = 62$ hosts)
    - The first subnet: **11000000.00110111.00001100.<u>00</u>000000**

      192.55.12.0
    - The second subnet: **11000000.00110111.00001100.<u>01</u>000000**

      192.55.12.64
    - The third subnet: **11000000.00110111.00001100.<u>10</u>000000**

      192.55.12.128
    - The fourth subnet: **11000000.00110111.00001100.<u>11</u>000000**

      192.55.12.192

5.4.5 Subnet mask

- When using subnets, **the default network mask is no longer valid**, as we have added **additional bits to the net-id (network part)**.
- The new mask value for subnets is calculated as follows:
    - Take the default mask of the initial network
    - Fill in the borrowed bits of the host portion with **1s**
    - and leave the remaining bits of the host portion at **0**

Example

- With two subnets, for the class C address: **192.55.12.0**
- Default mask (255.255.255.0): **11111111.11111111.11111111.00000000**

- The mask for the new subnets: **11111111.11111111.11111111.**10000000→ **255.255.255.128** or just indicate the number of bits set to **1→ /25**
- So the first subnet: **192.55.12.0 /25**
- The second subnet: **192.55.12.128 /25**

Example

- Let's take the address of the class C network: **192.55.12.0**
- Assuming we want to have 4 subnets:
    - Number of bits borrowed = 2 bits
    - The new mask: 11111111.11111111.11111111.11000000→ 255.255.255.192
    - The first subnet: **192.55.12.0 /26**
    - The second subnet: **192.55.12.64 /26**
    - The third subnet: **192.55.12.128 /26**
    - The fourth subnet: **192.55.12.192 /26**

5.4.6 Broadcast address for subnets

- The broadcast address is an address whose host part contains only 1.
- In the case of subnets, the broadcast address is not the same for all subnets.
- To calculate the broadcast address of a subnet:
- Write the address of this subnetwork in binary
- Fill in the host part with only 1
- Then convert to decimal

Example

- The first subnet 192.55.12.0

  11000000.00110111.00001100.**00**000000

The broadcast address 11000000.00110111.00001100.00**111111** → 192.55.12.63

- The second subnet 192.55.12.64 :

  11000000.00110111.00001100.**01**000000

  The broadcast address 11000000.00110111.00001100.01**111111** → 192.55.12.127

- The third subnet 192.55.12.128 :

  11000000.00110111.00001100.**10**000000

  The broadcast address 11000000.00110111.00001100.10**111111** → 192.55.12.191

- The forth subnet 192.55.12.192 :

  11000000.00110111.00001100.11000000

  The broadcast address 11000000.00110111.00001100.11**111111** → 192.55.12.255

5.3.6 Valid address range

- Let's take the address of the Class C network: **192.55.12.0**
- Assuming we want to have 4 subnets:
  - In this case, we take two bits from the host part (each subnet will have $2^6 - 2$ = 62 hosts)
  - The first subnet: **11000000.00110111.00001100.00000000**

    192.55.12.0 (valid addresses: 192.55.12.1→ 192.55.12.62)
  - The second subnet: **11000000.00110111.00001100.01000000**

    192.55.12.64 (valid addresses: 192.55.12.65→ 192.55.12.126)

- The third subnet: **11000000.00110111.00001100.10000000**

  192.55.12.128 (valid addresses: 192.55.12.129→ 192.55.12.190)

- The fourth subnet: **11000000.00110111.00001100.11000000**

  192.55.12.192 (valid addresses: 192.55.12.193→ 192.55.12.254)

Exercise 1

- Your organisation's network address is **150.193.0.0**
- You need **50** subnets. Each subnet has **750** hosts.
- What is the address class?
- What is the default mask?
- How many bits must be borrowed from the host portion of the network address to create at least 50 subnets, each with at least 750 hosts?
- What will the subnet mask be?
- For the first 4 subnets, give the range of machine addresses and the broadcast address.

Exercise 2

- Let us consider three machines, A, B and C, with the following addresses:
  - A: 192.168.0.133 / 25
  - B: 192.168.0.200 / 27
  - C: 192.168.0.220 / 26
- Give the subnet address of each machine and indicate the value of the subnet mask in decimal form.
- How many machines are there in the network of machines A, B and C?

Now that we have studied logical addressing, let's look at the basic principles of routing.

5.5 IP routing

5.5.1 Routing issues

– **Objective**: Route IP packets from source machine A to destination machine B.

– **Problem**: How can machine B be reached when its IP address is known?

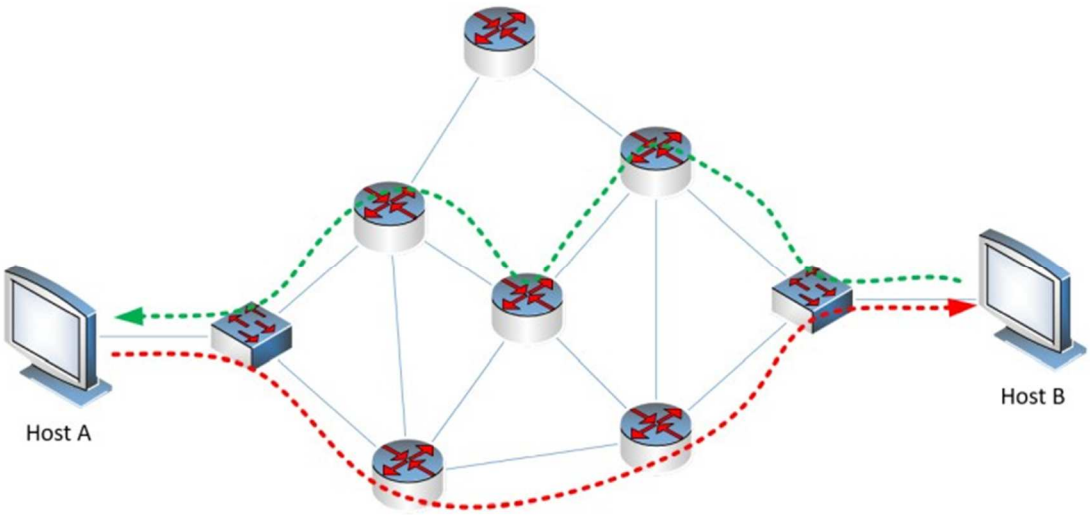

Figure 5.12 Routing issues [8]

5.5.2 IP routing: Definition

Routing consists of determining (choosing) the route by which packets are transmitted from the source to the destination using equipment called **routers.** This process is based on an IP routing table containing information about the various possible destinations and how to reach them.

5.5.3 IP packet

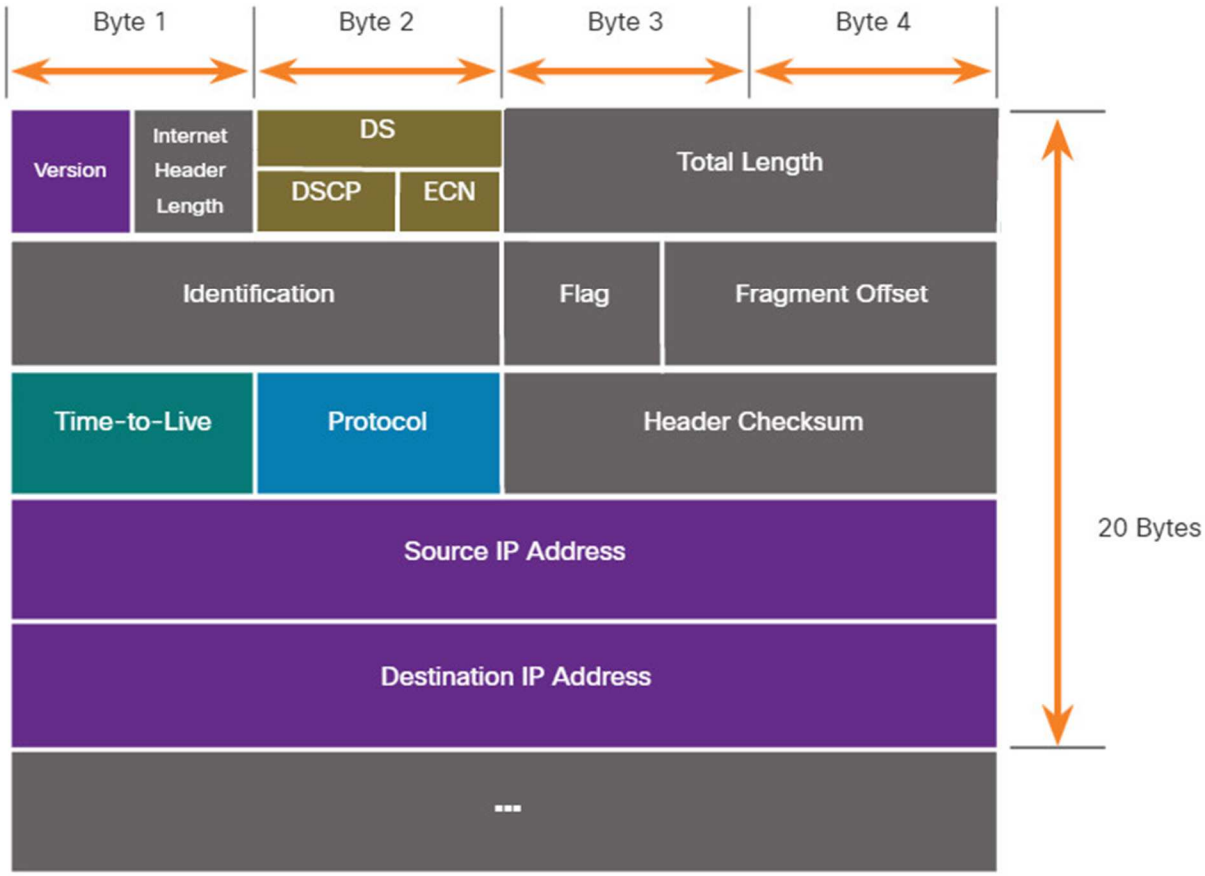

Figure 5.13 Structure of an IP packet [15]

5.5.4 What is a router?

A router is a piece of hardware and software (layer 3) that ensures that packets sent by a machine on one network can reach a destination machine on a different network. Packets can only travel between different networks if those networks are connected by one or more routers.

Figure 5.14 Cisco routers [16]

Figure 5.15 Router symbol [16]

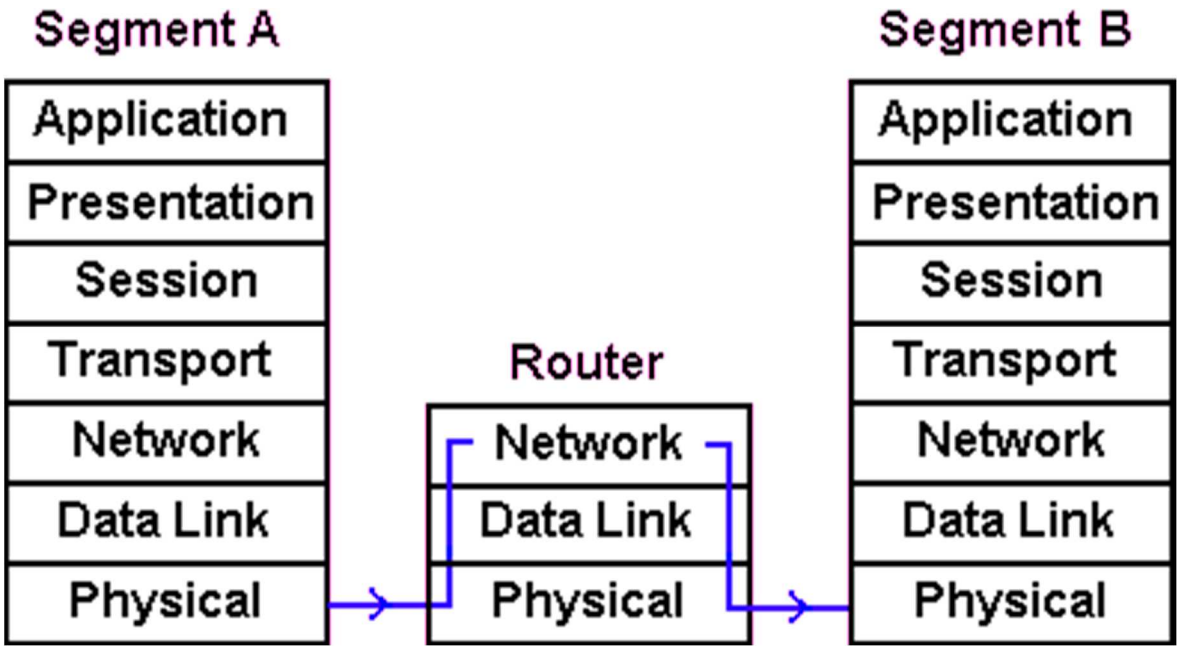

Figure 5.16 The router and the OSI model [9]

5.5.5 Role of the router

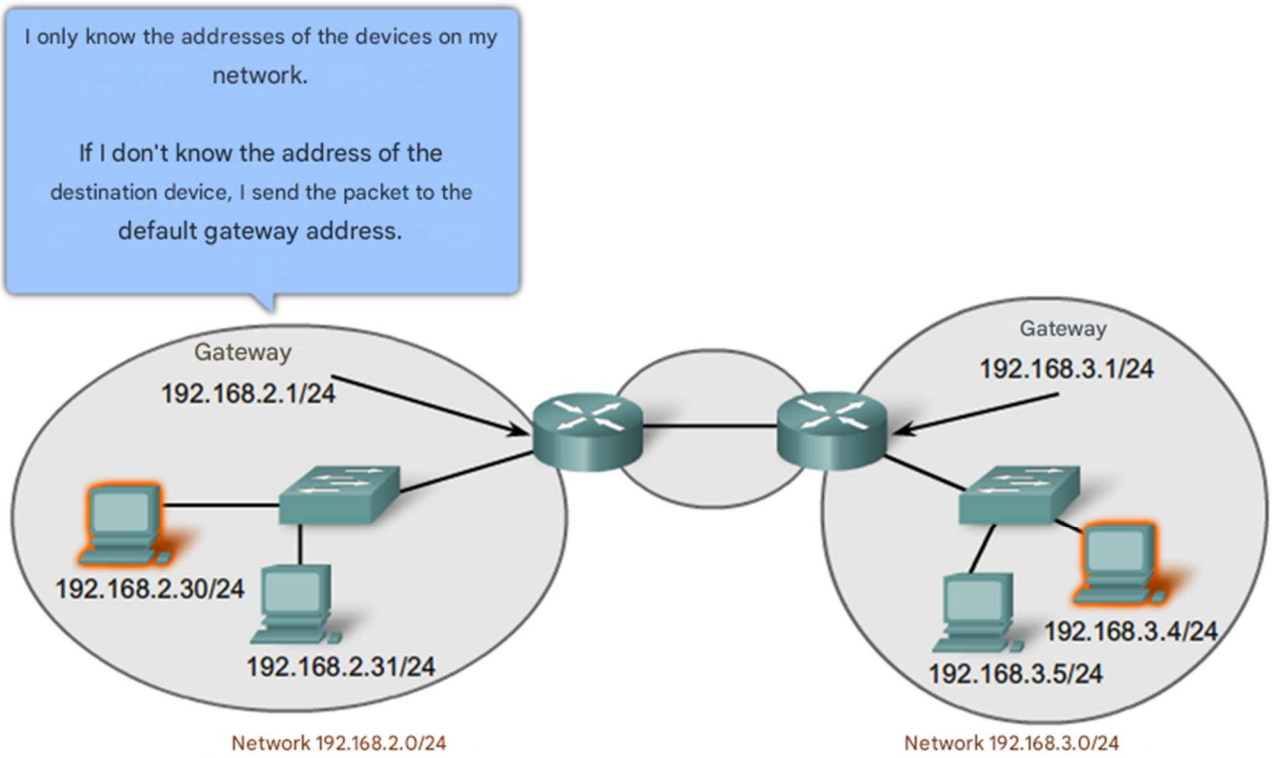

Figure 5.17 Role of a router [16]

5.5.6 Routing table

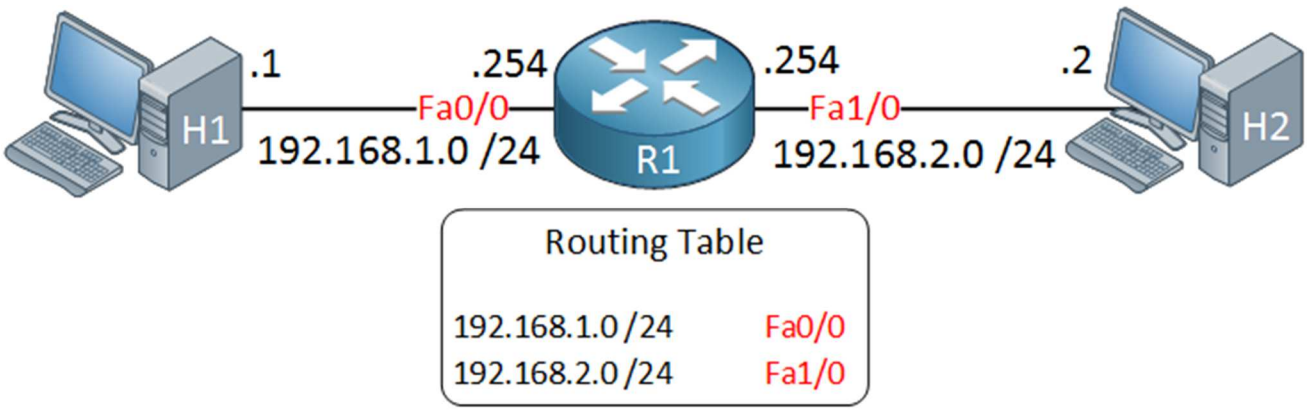

Figure 5.18 Routing table [14]

5.5.7 Default route

– This is a route that corresponds to all destination networks.

– The default route is used to direct packets addressed to networks that are not explicitly mentioned in the routing table.

– The address **0.0.0.0** corresponds to the default route.

Example routing table (CISCO router)

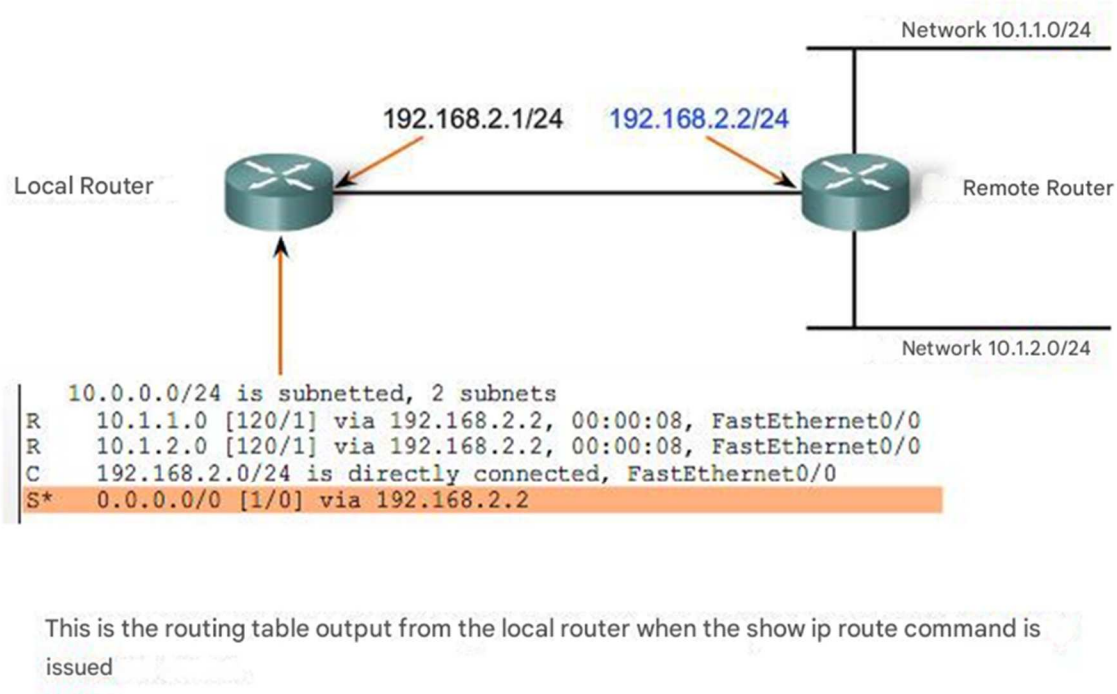

Figure 5.19 Example of a routing table [14]

5.5.8 IP routing: basic algorithm

- Extract the destination IP address (**IPDest**) from the packet.
- Calculate the destination network address (**IPRes**) by applying an **AND** between **IPDest** and the **subnet mask**.
- If this IPRes address corresponds to the local network address:
    - IPdest is directly accessible from the router.
    - The router will transmit the packet to the destination using the ARP protocol.
- Otherwise (if it is not a directly accessible address, the local IP routing table must be consulted):
    - If IPres is in the table, then: Route the packet according to the table.
    - Otherwise, if IPres is not in the table, then: Take the default route indicated in the table.
    - If the default route is not configured, the packet will be destroyed.

5.5.9 Static routing

- The administrator configures the routes for each router manually.
- Advantages:
    - Bandwidth savings.
    - Security.
- Disadvantages:
    - Complex configuration for large networks.
    - Difficult to update.

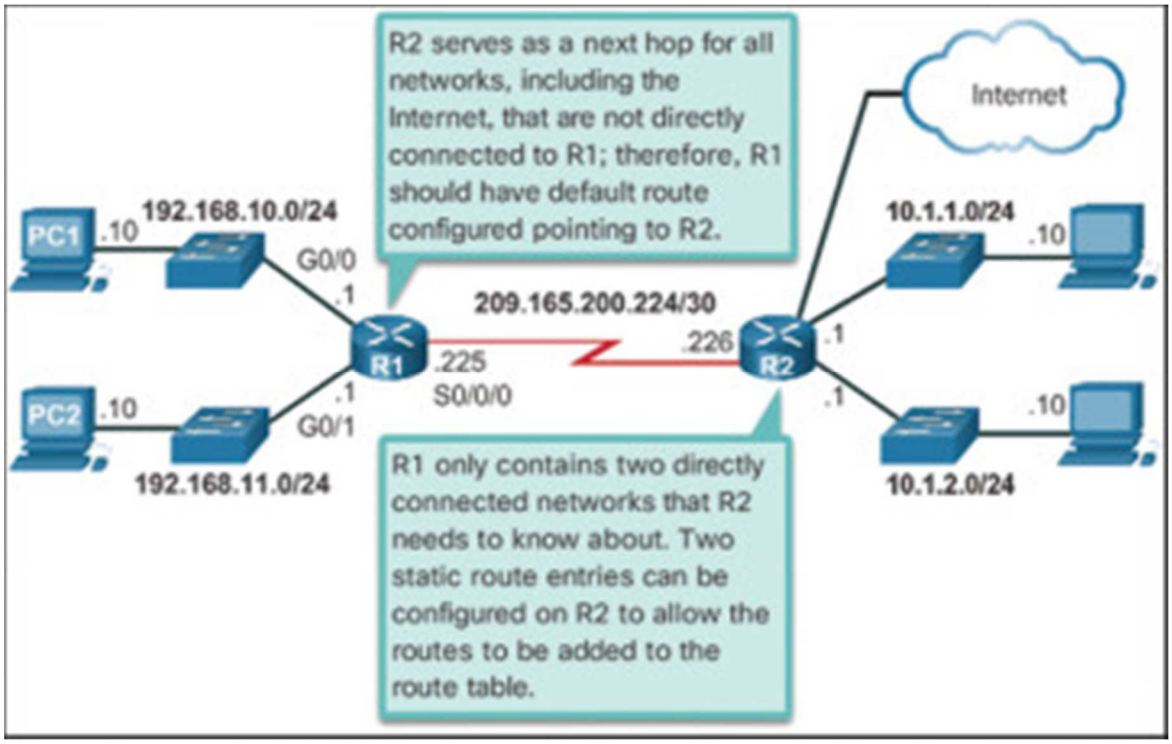

Figure 5.20 Static routing [14]

5.5.10 Dynamic routing

- Routes are updated automatically.
- A **routing protocol** is used to enable routers to communicate with each other and exchange information periodically or on an event-driven basis, so that each router is aware of changes in the network without manual intervention by the network administrator.
- Advantages:
  - Easy updating (automatic).
  - Better performance.
- Disadvantages:
  - Bandwidth consumption.
  - Vulnerable to attacks.
  - Additional consumption of physical resources (CPU and RAM) on routers.

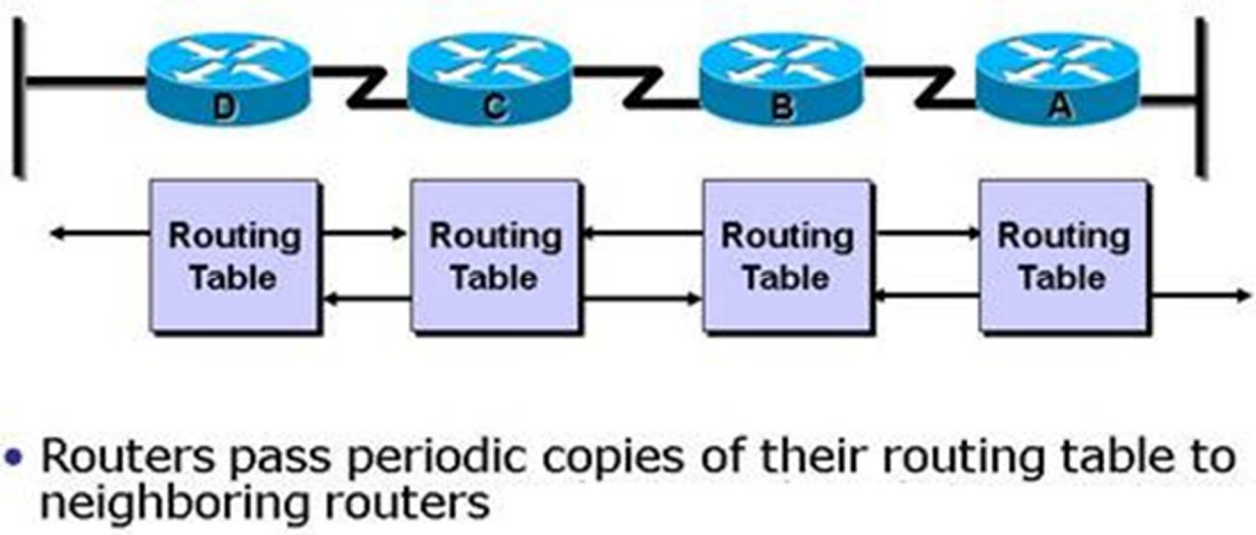

Figure 5.21 Dynamic routing [14]

5.5.11 Different types of routing protocols

- **Distance vector routing protocol:** uses a routing algorithm that adds up distances to find the best routes (Bellman-Ford algorithm). They often send their entire routing table to neighbours. (Examples: RIP and IGRP).

- **Link state routing protocol:** uses a more efficient algorithm (Dijkstra or Shortest Path First). Routers collect all link costs and construct a tree of all paths from their point of view. The best routes are then integrated into the routing table. (Examples: OSPF and ISIS).

- **A hybrid routing protocol:** is a distance vector routing protocol that incorporates link state concepts. One example is EIGRP.

5.6 Conclusion

The network layer plays a fundamental role in the OSI model by ensuring the forwarding of packets between systems located on separate networks. It introduces essential mechanisms such as logical addressing, which allows hosts to be identified globally, and routing, which chooses the optimal path to reach the destination.

It relies on several key protocols such as IP for addressing and routing, as well as routing protocols such as. Without these functions, it would be impossible to ensure reliable and efficient communication in an interconnected environment.

The next chapter will focus on the transport layer, which guarantees the reliability and integrity of data between applications.

Chapter 6
Transport Layer

6.1 Introduction

The transport layer is an essential component of the OSI model, located above the network layer and below the session layer. Its fundamental role is to ensure reliable and efficient data transfer between two applications running on different systems.

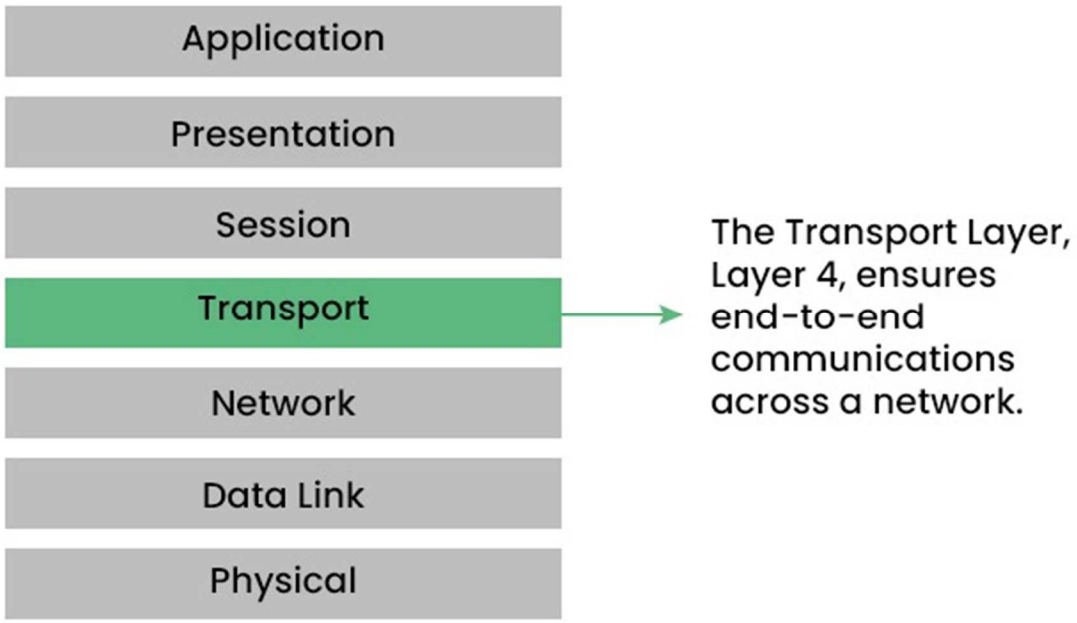

Figure 6.1 Transport layer [2]

Unlike the network layer, which focuses on routing packets between machines, the transport layer establishes end-to-end communication between application processes. It ensures that the data sent by the source application arrives correctly and in the right order at the destination application.

It offers two modes of communication:

- **Connection-oriented**: as in the TCP protocol, where a logical connection is established before the transfer.
- **Connectionless**: as in the UDP protocol, where data is sent without establishing a connection beforehand.

The transport layer provides a transparent service to applications, masking the imperfections of the underlying network.

Now that we have presented the general function of the transport layer, let's detail its main responsibilities.

6.2 Definition and role

The transport layer ensures complete, reliable and orderly delivery of data between applications, regardless of the characteristics of the underlying networks. Its role is to:

- **Segment** application **data** into units called segments, which will be encapsulated in network packets.
- **Multiplexing and demultiplexing**: identifying the different applications using the same network connection via port numbers.
- **Ensure error control and reassembly** of segments upon receipt.
- **Guarantee data integrity and correct sequencing** to avoid loss or duplication.
- **Connection management**: establishing, maintaining and releasing connections for connection-oriented protocols.

Unlike lower layers, which offer an unreliable (best-effort) service, the transport layer adds correction and reliability mechanisms that are essential for critical applications.

6.3 Network layer vs. transport layer

– The network layer provides communication between hosts, while the transport layer provides communication between applications.

– The network layer provides only a minimum level of service quality, so application requirements must be met by the transport layer.

– Improve the reliability of network layer transmissions from sender to receiver.

Now that we have presented the services, let us examine the functions provided by the transport layer.

6.4 Multiplexing

- The primary role of the transport layer is multiplexing:
    - For each host, there are several applications running in parallel.

- But hosts have a single address (IP), so a second value is used to identify the process on a machine: the port number.
- A (logical) connection is therefore represented by four values: (source address, source port) – (destination address, destination port).

6.5 Demultiplexing

- Demultiplexing is performed at the destination:
  - The recipient receives the different segments.
  - Each segment has a source port number and a destination port number.
  - The recipient uses the destination port number to direct the segment to the appropriate application.

Now that we have detailed the main functions of the transport layer, let's look at the two main protocols used in this layer, namely UDP and TCP

6.6 UDP (User Datagram Protocol) [4]

- Connectionless mode
- Unreliable transport
- Direct sending of information
- No flow control
- No sequencing guarantee
- Optional error detection
- Usage: Multimedia applications

6.7 TCP (Transport Control Protocol) [4]

- Connection-oriented service:
  - Connection/data transfer/disconnection phase
- Sequencing guarantee:

    - Segment numbering

- Reliable transport:
    - Error control + acknowledgements + retransmission
- Flow control:
    - The transmitter does not overwhelm the receiver.
- Usage: Critical applications

6.8 UDP characteristics

- Advantages:
    - Simplest transport protocol:
        - Simple exchanges of short client/server messages
            - DNS (Domain Name Service):

              Question: "What is the address of google.com?"

              Answer: "google.com is at 72.14.221.104"
    - No connection time
    - Small header
- Disadvantages:
    - Lack of reliability (not necessary for video streaming or VoIP applications)
    - No congestion management (routers are the only solution to reduce this effect)
- Applications using UDP: DNS, SNMP, DHCP, etc.

6.8.1 UDP segment format

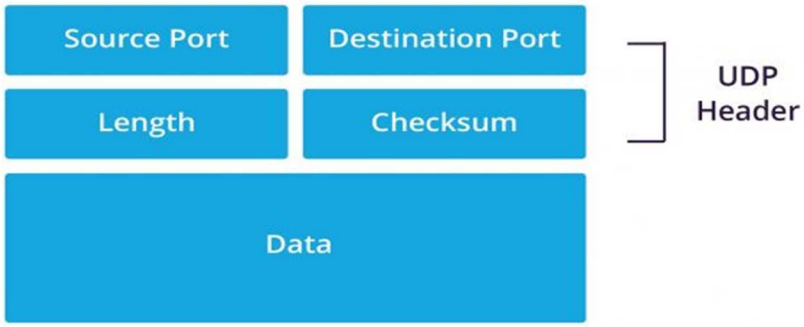

Figure 6.2 UDP segment format [4]

6.8.2 UDP: standard ports [2]

No port	Mot-clé	Description
7	ECHO	Echo
11	USERS	Active Users
13	DAYTIME	Daytime
37	TIME	Time
42	NAMESERVER	Host Name Server
53	DOMAIN	Domain Name Server
67	BOOTPS	Boot protocol server
68	BOOTPC	Boot protocol client
69	TFTP	Trivial File transfert protocol
123	NTP	Network Time Protocol
161	SNMP	Simple Network Management prot.

6.9 TCP characteristics

- Communication:
  - Reliable: data lost by the network is retransmitted.
  - Connected mode: Connection phase / data transfer phase / disconnection phase
- Congestion control
- Quite difficult to implement (much more so than UDP)

6.9.1 Principle of TCP segments

- Reliability is achieved through a segment acknowledgement mechanism:
  - When a segment is sent, an alarm is triggered.
  - It is deactivated when the corresponding acknowledgement is received.
  - If it expires, the segment is resent.
- Each segment has a sequence number:
  - To preserve order and avoid duplicates.
  - Acknowledgements are identified by an ACK marker.
  - Transport in the same segment: data and data acknowledgement.

6.9.2 TCP segment format

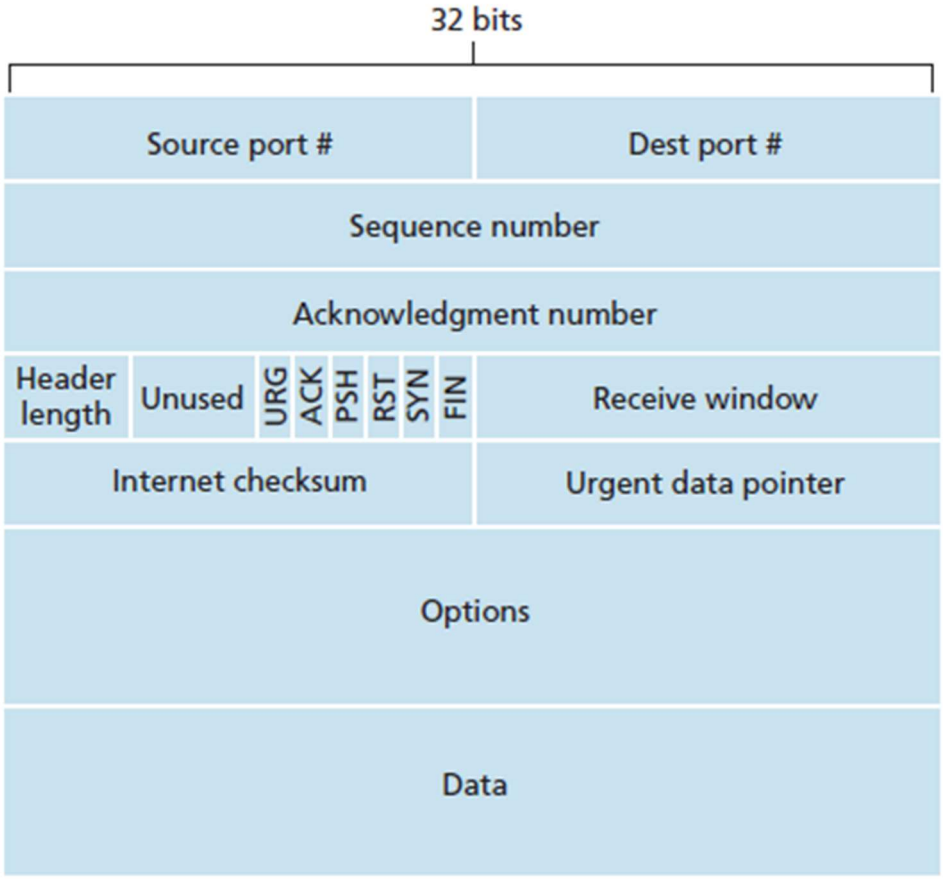

Figure 6.3 TCP segment format [4]

- Field Size: in number of 32-bit words

- Markers:
    - URG: urgent data
    - ACK: acknowledgement
    - PSH: forces immediate transmission
    - RST: connection refusal
    - SYN: synchronisation for connection
    - FIN: connection termination
- Checksum: use of polynomial verification (CRC)
- Options: max. segment size …

6.9.3 TCP: standard ports [2]

No port	Mot-clé	Description
20	FTP-DATA	File Transfer [Default Data]
21	FTP	File Transfer [Control]
23	TELNET	Telnet
25	SMTP	Simple Mail Transfer
37	TIME	Time
42	NAMESERVER	Host Name Server
43	NICNAME	Who Is
53	DOMAIN	Domain Name Server
79	FINGER	Finger
80	HTTP	WWW
110	POP3	Post Office Protocol - Version 3
111	SUNRPC	SUN Remote Procedure Call

6.10 Conclusion

The transport layer is a key element of the OSI model, as it establishes end-to-end communication between applications and guarantees the integrity of the data exchanged. It differs from the lower layers in its ability to provide a reliable service, despite network uncertainties.

It combines several essential mechanisms: segmentation and reassembly, error control, flow control and, if necessary, connection management. Thanks to these mechanisms, the transport layer ensures that the information transmitted by the source application is delivered without loss and in the correct order.

Finally, its two main protocols, TCP and UDP, address different needs: reliability and control on the one hand, speed and simplicity on the other.

The next chapter will focus on the upper layers of the OSI model, namely the session, presentation and application layers.

Chapter 7

Session, presentation and application layers

7.1 Introduction

After studying the lower layers of the OSI model (physical, link, network and transport), we will now look at the upper layers, which are directly involved in communication between applications. These layers are:

- The Session layer: manages dialogue and synchronisation between two applications.
- The Presentation layer: handles data translation, compression and encryption.
- The Application layer: provides network services directly to users and applications.

These three layers are essential to ensure that data is not only transmitted correctly, but also interpreted and used appropriately by applications. They make communication intelligible, secure and user-oriented.

Let's start by looking at the session layer, which establishes and manages dialogues between communicating applications.

7.2 Session layer

The session layer manages communication sessions between applications. A session is an organised interaction between two communicating entities. This layer:

- Establishes the session;
- Keeps the session active during communication;
- Releases the session at the end of the exchange.

It is therefore closely linked to the following concepts:

- Authentication: logging in with a username/password.
- Permissions: rights granted to the user during the session.

It also provides synchronisation mechanisms, for example by inserting checkpoints so that transmission can be restarted in the event of an interruption.

Having looked at the role of the session, let's move on to the presentation layer, which deals with data format.

7.3 Presentation layer

The presentation layer is responsible for translating data between the format used by the application and the format used for transmission. It acts as a universal translator between heterogeneous systems. Its functions are:

- **Translation:** conversion between different data formats (e.g. EBCDIC to ASCII).
- **Compression:** reducing data size to optimise transmission.
- **Encryption:** securing data during transfer.

Examples of use:

- Compression of JPEG images or MP3 audio files.
- SSL/TLS encryption to secure web exchanges.

Now that we have looked at data presentation, let's move on to the final layer, the application layer, which is closest to the user.

7.4 Application layer

The application layer provides network services to user applications. It allows programmes such as web browsers, email clients, and FTP software to access network resources.

Its functions are:

- **User interface**: this is the only layer directly visible to the end user.
- **Provision of network services**: such as email, file transfer, and web access.
- **Management of application protocols**: which ensure communication between applications.

The application layer is the top layer of the OSI model. It is the source and final destination of all data exchanged between users. This layer provides the interfaces for communication between users.

Application layer protocols run on terminal equipment. The application layer is not implemented at the core network equipment (intermediate equipment) level [17].

7.5 Application classes

- Consumer: email, web, instant messaging, file sharing (P2P, etc.), online gaming, video streaming, VoIP (telephony), file transfer, videoconferencing.

- IT for IT professionals: remote terminal use, distributed file systems, network management.

- Specialised: stock market, industry, healthcare, transport, nuclear, space, weather, scientific computing.

7.6 Application architectures

7.6.1 Client-server architecture

- The server is an application hosted by a host machine that is always on, with permanent and fixed access.

- The client communicates with the server intermittently.

- Clients do not communicate directly with each other, but go through the server.

- Example: browser – web server.

7.6.2 Peer-to-peer (P2P)

- No server.

- Terminal equipment communicates directly with each other and exchanges services.

- Good performance, but complicated to manage because the devices are constantly changing.

- Example: torrent.

Let's move on to explaining a few application layer protocols:

7.7 The HTTP protocol: HyperText Transfer Protocol

- Uses the concept of hypertext, where a document contains links to other objects or documents.

- A web page consists of a file written in HTML (Hypertext Markup Language), which references several objects.

- Each web page is identified by a URL (Universal Resource Locator):

  http://www.essa-tlemcen.dz/emploi-du-temps.html

- The objects (files) are stored on an HTTP server (commonly referred to as a web server).

- Even if other languages are used to manage the application on the server (PHP: dynamic pages, etc.), the pages and syntax follow HTML and HTTP standards.

- HTTP runs on TCP and uses port 80.

7.8 Email

- The most widely used application on networks, due to its simplicity and speed of execution, has revolutionised the way we communicate.

- Use of an email client that provides the functionality of two protocols, SMTP and POP:

  - SMTP: to send emails to the mail server (TCP port number 25).

  - POP: to receive email from the mail server (TCP port number 110).

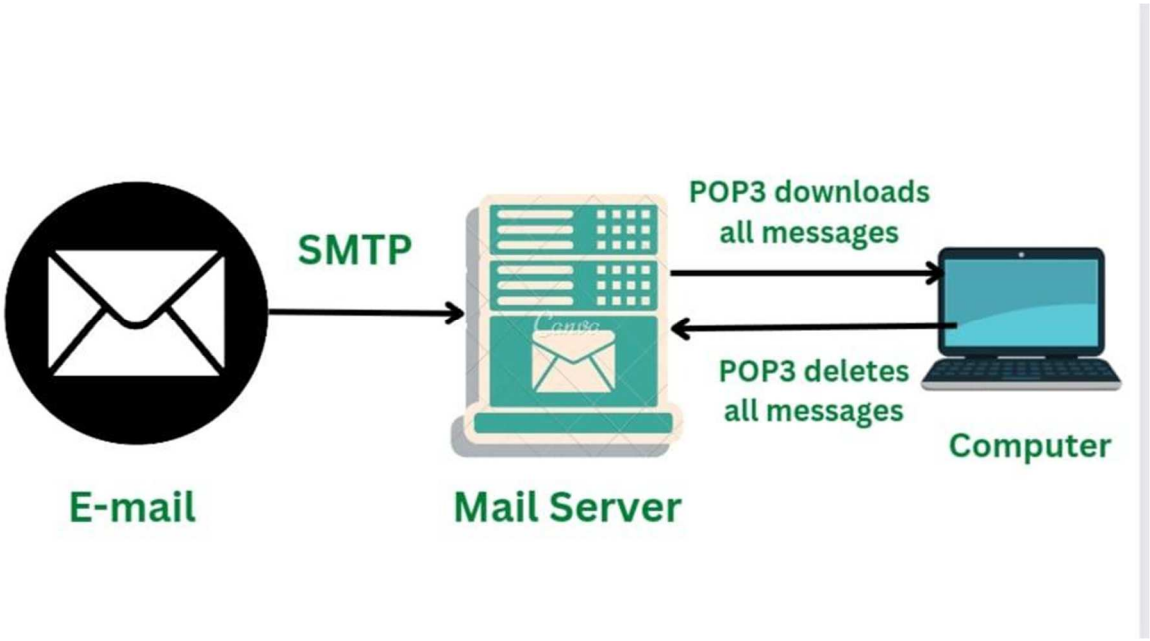

Figure 7.1 Email [17]

7.9 The FTP protocol: File Transfer Protocol

- Used for transferring/downloading files.
- It allows users to:
    - connect to an FTP server and then disconnect when the download is complete.
    - to transfer files, regardless of their nature, between both ends of the connection and in both directions.
- Access is granted with a login and password.
- FTP operates over TCP and uses port 21 for commands and port 20 for data.

7.10 Telnet: Terminal network

- Telnet: is a remote command utility that offers a range of features enabling interactive command execution in the remote environment.
- A Telnet connection is established in two phases:
    - an authentication phase.
    - a remote work phase.
- Operates in connected mode (TCP) on port 23.

7.11 DHCP protocol: Dynamic Host Configuration Protocol

- DHCP: Automatically assigns an IP address to a machine that connects to the network.
- Facilitates the management of machine addresses in large networks that change frequently.
- The assignment is done in several phases:
    - The client sends a DHCPDISCOVER broadcast packet using the address 255.255.255.255
    - If a DHCP server receives such a message, it responds to indicate that it is available.

    - The server consults its database to see if the client's physical address corresponds to a fixed IP address. If this is not the case, it chooses an available IP address and sends it to the client.

- DHCP operates on UDP and uses port 67.

7.12 The DNS protocol: Domain Name System

- Allows symbolic names (easy to remember) to be associated with numerical addresses, usually IP addresses.

- DNS structure:

    - Distribution of information across multiple DNS servers.

    - A DNS is both a client and a server.

    - Based on a hierarchical structure at the top of which are ROOT servers (there are 13 for the entire Internet).

7.13 Conclusion

The session, presentation and application layers constitute the interface between the user and network services. They are essential for ensuring that the data exchanged is properly organised, understandable and secure.

- The session layer ensures continuity of exchanges by managing dialogues and synchronisation.

- The presentation layer ensures that data is interpreted correctly through translation, compression and encryption.

- The application layer provides essential network services (web, messaging, file transfer, name resolution) via protocols such as HTTP, SMTP, FTP and DNS.

These three layers rely on the lower layers to provide comprehensive, reliable communication tailored to the needs of applications. They mark the transition between the world of networks and that of users.

Conclusion

Throughout this textbook, we have explored the fundamental concepts that govern computer networks and communication protocols. The study was conducted following a hierarchical approach based on the OSI model, which allowed us to understand the role and interactions of each layer, from the physical transmission of signals to the application services intended for the end user.

The first chapters introduced the basic concepts, the history of communications, and the different classifications of networks. We then analyzed in detail the lower layers (physical, data link, and network), focusing on their essential mechanisms: signal encoding, frame encapsulation, physical and logical addressing, routing, and error control.

Subsequently, we addressed the upper layers (transport, session, presentation, and application), which ensure reliability, dialogue management, data translation, and security, while providing network services adapted to applications. Major protocols such as Ethernet, IP, TCP, UDP, HTTP, and DNS were studied to illustrate these mechanisms concretely.

The entire content was complemented by practical examples aimed at strengthening the understanding of concepts and developing the skills necessary to implement them in real-world environments.

This textbook thus constitutes a solid reference for engineering students, enabling them to master the fundamentals of computer networks and protocols, and to acquire the knowledge required to analyze, design, and manage reliable and efficient communication systems.

Bibliography

[1] LOHIER S. PRESENT D. (2020). Réseaux et transmissions : Protocoles, infrastructures et services. Dunod. ISBN : 9782100811830

[2] KUROSE J. F., ROSS K. W. (2024). Computer Networking: A Top-Down Approach (8th Edition). Pearson. ISBN : 9780136681557

[3] DORDOIGNE, J. (2025). Réseaux informatiques - Notions fondamentales (10th edition). ENI. ISBN : 978-2-409-04826-5

[4] SCHALKWIJK, L. (2020). CISCO - Introduction aux réseaux : 1er module de préparation à la certification CCNA 200-301. ENI. ISBN : 978-2-409-02619-5

[5] Réseaux informatiques, modèle OSI, protocole TCP/IP. http://info.arqendra.net/Files/_Rsx+OSI+TCPIP_cours.pdf

[6] BENNADA, B. Réseaux informatiques. Université de Tlemcen

[7] DE MEY, L. Structure en couches : Le modèle de référence OSI. courstechinfo.be/Reseaux

[8] FERRAND P. Réseaux. INSA de Lyon. http://www.ferrand.cc/pdfs/cours_reseaux.pdf

[9] FRABOULET, A. Introduction aux réseaux. INSA de Lyon. http://docinsa.insa-lyon.fr/polycop/download.php?id=173834&id2=0

[10] PARET D. and REBAINE H. (2018). Réseaux multiplexés pour systèmes embarqués : CAN, LIN, FlexRay, Safe by Wire (Second edition). Dunod. ISBN : 9782100582891

[11] CISCO Systems (2020). Networking Essentials. Cisco Networking Academy.

[12] Xavier Buche. Liaison de données. L3-S6 INFO/MIAGE, Réseaux. Université de Lille

[13] FOROUZAN B. A. (2019). Data Communications and Networking. McGraw-Hill

[14] CISCO Systems (2020). Introduction to Networks (CCNA v7). Cisco Networking Academy

[15] ZHANG Tuo. Routage Dynamique RIP sur CISCO, M2103.IUT Dijon-Auxerre

[16] Cisco (2020). Switching, Routing, and Wireless Essentials (CCNA v7)

[17] Christian Bulfone. Quelques protocoles applicatifs, Licence "Mathématiques et Informatique Appliquées aux Sciences Humaines et Sociales" (MIASHS). Université Grenoble Alpes