Chapter 1
Networking Fundamentals

What is a Computer Network?

What is a Computer Network?

A **computer network** (or communication network) is a set of interconnected **devices** (both hardware and software components) that are **linked together** to **exchange information and share resources**.

These devices can be connected through **wired connections** (such as Ethernet cables) or **wireless links** (such as Wi-Fi or radio signals).

Advantages of Computer Networks?

Advantages of Computer Networks

Computer networks offers many advantages, including

- **Data sharing**: easy exchange of files and information between users.
- **Resource sharing**: access to shared computing power, storage capacity, printers, and other devices.
- **Information access**: ability to search and retrieve data (from the Internet, etc.).
- **Cloud storage/services**: centralized and scalable storage accessible from anywhere.
- **Remote communication**: supports email, video conferencing, and other forms of online collaboration.
- **Scalability and flexibility**: easy to expand or modify as needs evolve.

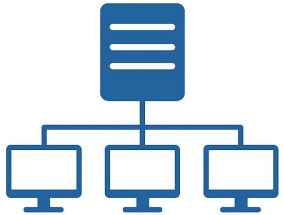
Types of Computer Networks?

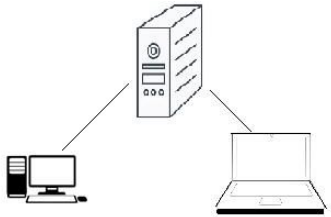
Types of Computer Networks

- **Client–Server Network (More Secure, distributed)**

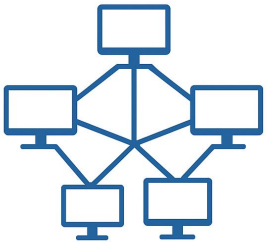
- **Peer-to-Peer (P2P) Network (Less Secure, decentralized)**

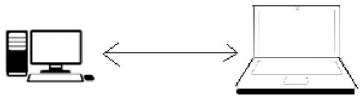
Client–Server Network
(More Secure)



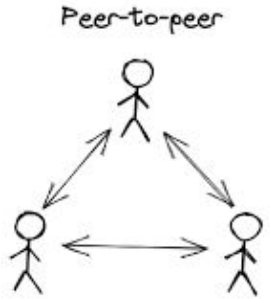


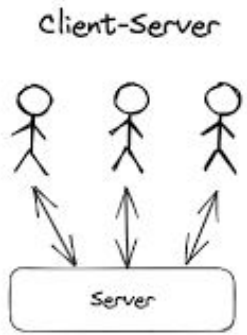
Peer-to-Peer (P2P) Network
(Less Secure)





Types of Computer Networks





- **Client–Server Network (More Secure, distributed)**
  - Centralized model where **clients** request services and **servers** provide them.
  - Offers **better security**, **centralized control**, and **easier management** of resources and user access.
  - Common in enterprises and organizations.

- **Peer-to-Peer (P2P) Network (Less Secure, decentralized)**
  - Decentralized model where **each device acts as both client and server**.
  - Easier to set up but **harder to secure and manage**.
  - Suitable for **small or temporary networks** (e.g., file sharing among a few devices).

Problem Statement

Problem Statement

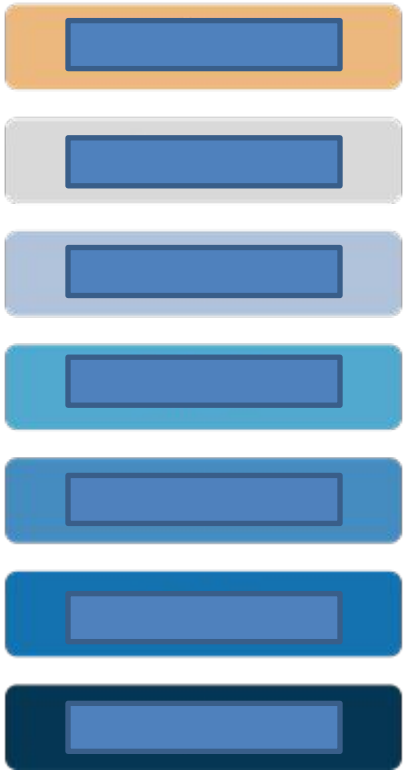
- To create a computer network and connect different machines/devices to it, it is essential to **consider the differences between these machines**.
- The machines to be connected to a network are often **built by different manufacturers and** use **different hardware** and software/**operating systems**.
- This diversity creates challenges in ensuring **interoperability**, **communication compatibility**, and **network reliability**.

Problem Statement

How can we make a network work properly so that all nodes can communicate with each other (regardless of their differences in hardware or software)?

Solution

OSI (Open System Interconnection) Model



Each **layer** communicates only with:

- its **adjacent layers** (either above or below)
- the **corresponding layer** on another system

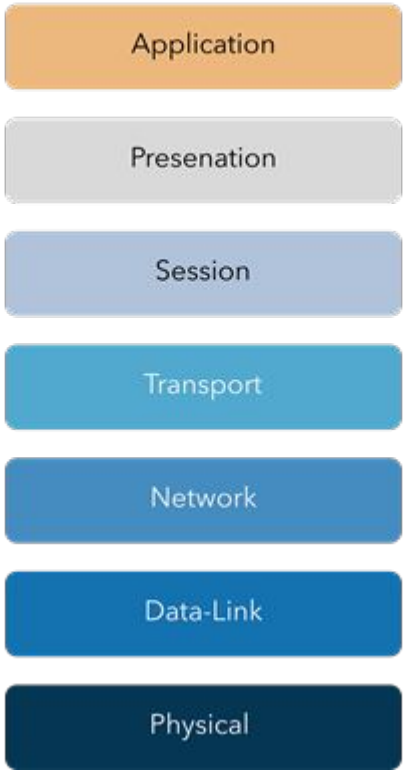
Questions

1. **Name these layers (OSI model** layers)

2. **Which one is Layer 1?**

3. **What do we call data at each layer?**

OSI (Open System Interconnection) Model



Each **layer** communicates only with:

- its **adjacent layers** (either above or below)
- the **corresponding layer** on another system

Questions

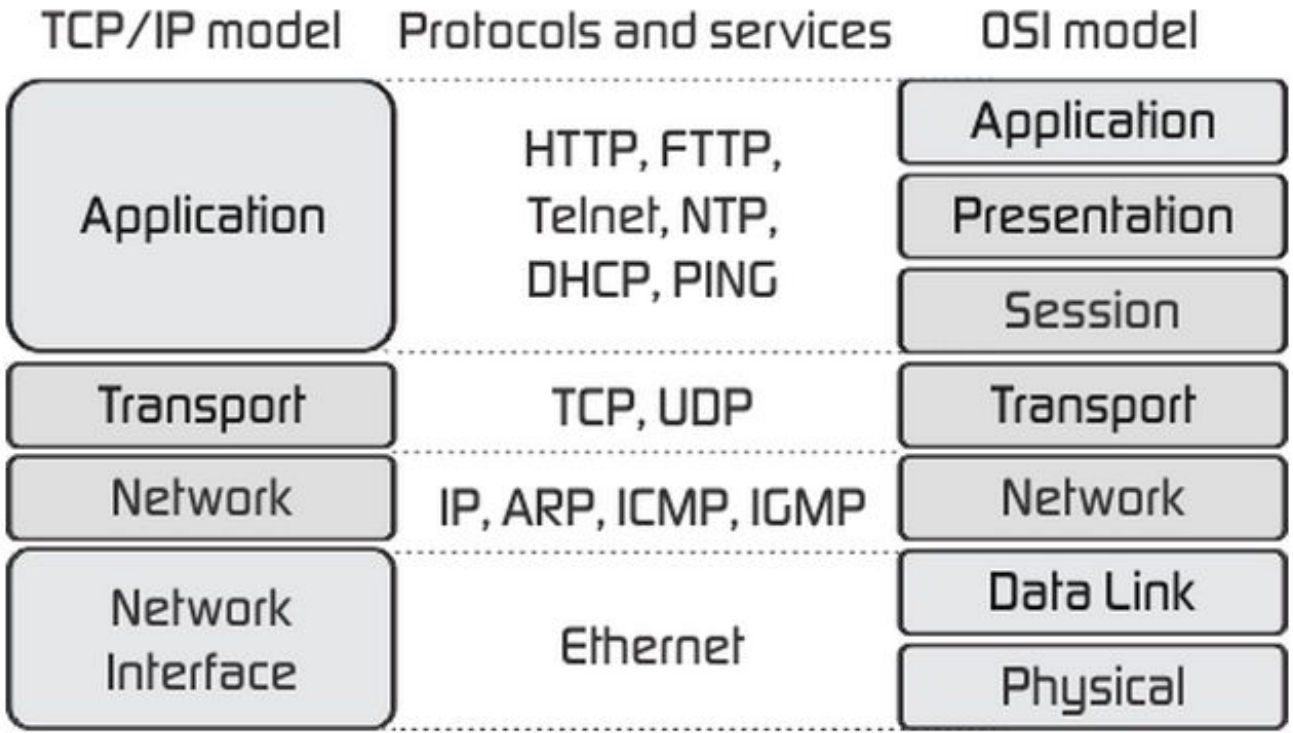
1. **Name these layers (OSI model** layers)

2. **Which one is Layer 1?**

3. **What do we call data at each layer?**

OSI vs TCP/IP

OSI vs. TCP/IP


TCP/IP model
Protocols and services
OSI model
Application
HTTP, FTTP, Telnet, NTP, DHCP, PING
Application
Presentation
Session
Transport
TCP, UDP
Transport
Network
IP, ARP, ICMP, IGMP
Network
Network Interface
Ethernet
Data Link
Physical

OSI Model Layers

OSI Model Layers—What Interests Us the Most?

In this course, we focus on the key networking concepts that are essential for **security engineering** and **system configuration**

- **Protocols**: such as the **TCP 3-way handshake**, which ensures reliable communication between hosts.
- **IP addressing**: including **address classes**, **ranges**, and **subnet masks**, fundamental for **firewall rules** and **network configuration**.
- **Services and Ports**: understanding which ports are used by different services is crucial for **monitoring**, **filtering**, and **defense**.

OSI Model Layers

1. Physical Layer

1. Physical Layer

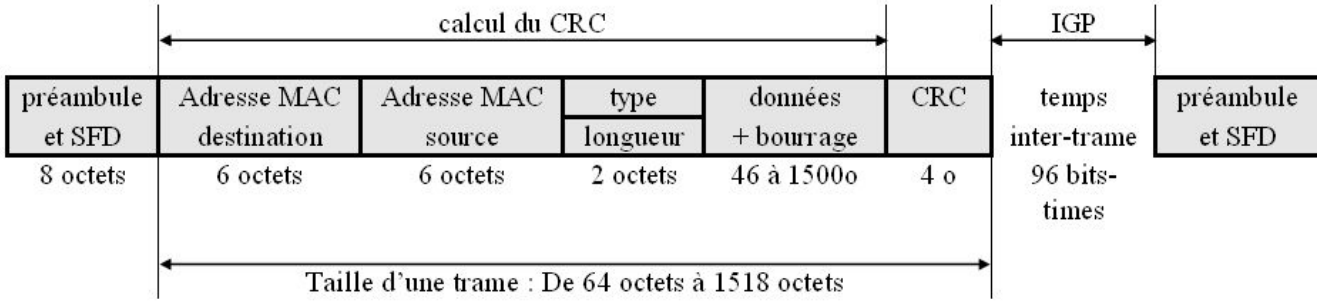
- The lowest (first) layer of the OSI model.
- Responsible for transmitting data **bits** from the sender to the receiver.
- The information traveling through the transmission medium can be **discrete** (e.g., text, image) or **continuous** (e.g., sound).
- To transmit a continuous signal (also called an analog signal), it must undergo three phases known as signal normalization:
  - **Sampling phase:** divides the signal into regular time intervals.
  - **Quantization phase:** establishes a correspondence between certain values (called quantization levels) and the amplitude of a sample.
  - **Encoding phase:** enables the transmission of binary data.
  -
- Discrete information requires only the encoding phase.

OSI Model Layers

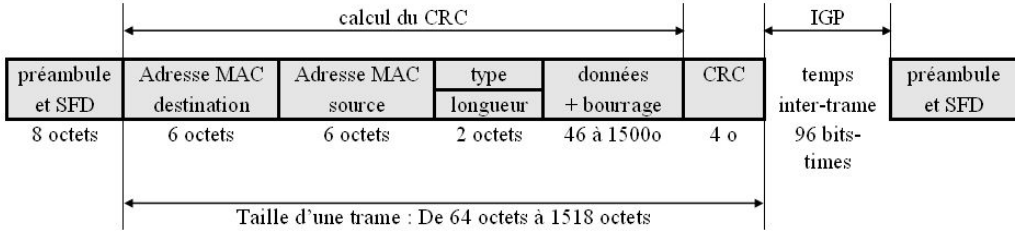
2. Data link Layer

2. Data Link Layer

- The second layer of the OSI model manages the **physical addresses** of machines (**MAC addresses)**.
- In addition, it is responsible for error detection, correction, and retransmission.
- At this layer, the transmitted data are called **frames**.



2. Data Link Layer



- The different fields of a frame and their meanings are as follows:
  - **Destination MAC address:** MAC address of the destination machine.
  - **Source MAC address:** MAC address of the source machine (the one sending the frame).
  - **Data:** information coming from Layer 3, in the case of Ethernet.
  - **Padding (PAD):** padding bytes inserted if the length of the data is insufficient (less than 46 bytes).
  - **CRC (FCS):** field used for error checking.
    - Cyclic Redundancy Check and Frame Check Sequence

- **MAC Address**
  Its length is 6 bytes, represented in hexadecimal.

  Example: 00:1B:44:11:3A:B7

OSI Model Layers

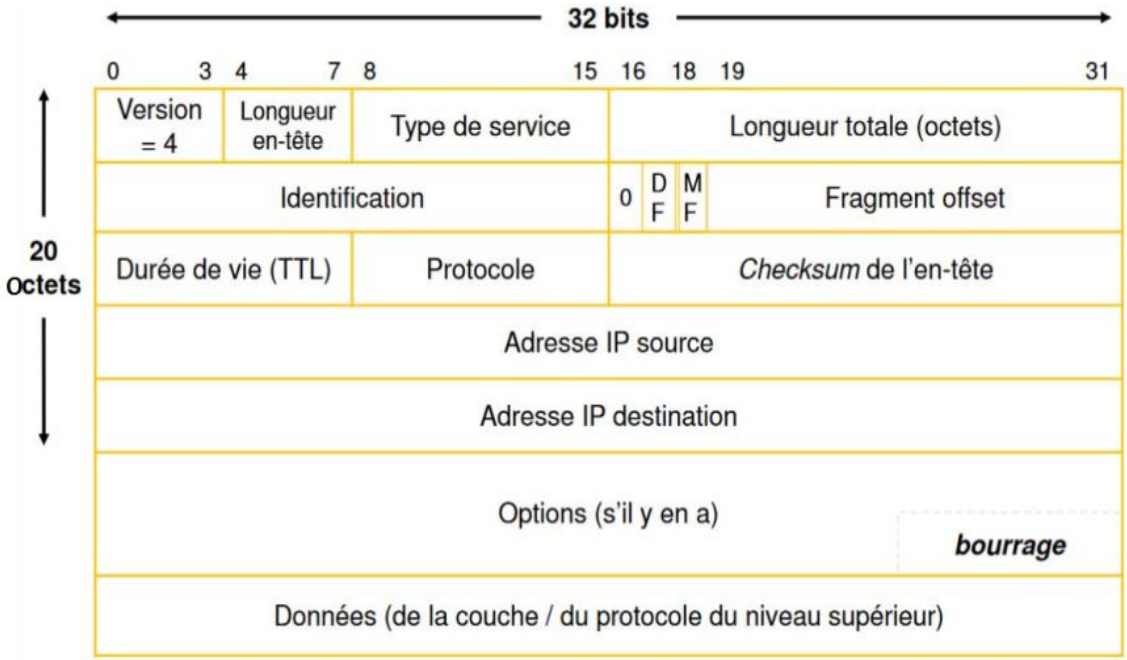
3. Network Layer

3. Network Layer

- The third layer of the OSI model.
- Responsible for determining how packets are routed from point A to point B.
- The information transmitted at this stage is called a **packet**, and the addresses used are called **logical addresses** (**IP addresses**).

3. Network Layer

- The different fields of a frame and their meanings?



3. Network Layer

- An **IP address** is unique within a computer network and has a length of **4 bytes (32 bits)**.

  Example: **XXX.XXX.XXX.XXX**, where each X is a digit.

- Each part of the IP address ranges from 0 to 255.
  Thus, **192.168.14.10** or **122.32.1.0** are examples of **IPv4 addresses**.

- An IP address consists of two parts:
  - one identifying the network (called **netID**) and
  - the other identifying the host (called **hostID**).

The Net 1995

3. Network Layer

IP Address Classification

- There are mainly two classes of IP addresses
  - **Private IP addresses** are used only within a local network (LAN) and cannot be routed on the Internet. Below are the private IP address ranges:
    - **10.0.0.0/8**, i.e., from **10.0.0.0 to 10.255.255.255**
    - **172.16.0.0/12**, i.e., from **172.16.0.0 to 172.31.255.255**
    - **192.168.0.0/16**, i.e., from **192.168.0.0 to 192.168.255.255**
  - **Public IP addresses** are routable on the Internet and are assigned, for example, by an Internet Service Provider (ISP).

3. Network Layer

IP Address Classification

- There are mainly two classes of IP addresses
  - **Private IP addresses** are used only within a local network (LAN) and cannot be routed on the Internet. Below are the private IP address ranges:
    - **10.0.0.0/8**, i.e., from **10.0.0.0 to 10.255.255.255**
    - **172.16.0.0/12**, i.e., from **172.16.0.0 to 172.31.255.255**
    - **192.168.0.0/16**, i.e., from **192.168.0.0 to 192.168.255.255**
  - **Public IP addresses** are routable on the Internet and are assigned, for example, by an Internet Service Provider (ISP).

3. Network Layer

3. Network Layer

Specific IP Addresses

- **Subnet Mask (Netmask)**
  - The subnet mask is used to separate the network portion from the host portion of an IP address.
  - It allows checking whether two machines belong to the same network or not.
  - If they do not, a router must be used to route information from one network to another.

  Example

  - 192.168.30.0 : 255.255.255.0 → network 192.168.30.0/24
  - 192.168.65.0 : 255.255.255.0 → network 192.168.65.0/24

3. Network Layer

Specific IP Addresses

- **Loopback Address**
  This is a self-referencing address used for testing, e.g., **127.0.0.1**.

- **Broadcast Address**
  In this case, all the bits in the host portion are set to 1. **Example: 192.168.65.255**

- **Network Address**
  All the bits in the host portion are set to 0. **Example: 192.168.65.0**

- **0.0.0.0:** When all bits of the IP address are set to 0, it indicates the **default route** or is used by a machine during boot to discover its own IP address.

- **255.255.255.255:** When all bits of the IP address are set to 1, it represents **all hosts on the local network** (broadcast on the local network).

OSI Model Layers

4. Transport Layer

4. Transport Layer

- The fourth layer of the OSI model, its main role is to ensure **logical communication between applications**.

- It is also responsible for the **fragmentation** of data from the upper layers (called SDU, Service Data Units) into several smaller units called PDU (Protocol Data Units), which are then sent to the network layer.

- Once these PDUs are received by the destination, the transport layer reads their headers and **reassembles** them into a single data unit.

4. Transport Layer

The main services provided by the transport layer include

- **Connection-oriented communication (TCP):** ensures that a logical connection is established before data transmission.

- **Order of delivery:** the transport layer manages sequencing and ensures that data is received **in the same order** as it was sent (using sequence numbers).

- **Reliability:** ensures that the receiver has successfully received all segments; missing or corrupted segments are **retransmitted** (TCP).

- **Multiplexing/Demultiplexing:** allows multiple applications to send and receive data simultaneously over the same network connection.

4. Transport Layer

Port Number

- The port number in the transport layer is used to **identify an application**.
- It is a 16-bit integer (2 bytes) and can have a value ranging from **0 to 65,535**.
- Each type of application is associated with a specific port number.

There are three categories of ports:

- **Well-known ports (0–1023):** reserved for common and standardized services (e.g., web, file sharing, email, etc.).

- **Registered ports (1024–49151):** assigned for use by proprietary or user applications.

- **Dynamic or private ports (49152–65535):** available for temporary or custom use by applications.

4. Transport Layer

TCP and UDP Protocols

- The transport layer uses two essential protocols: **TCP** and **UDP**.

- **UDP (User Datagram Protocol)**
  - UDP is a **connectionless transport protocol** that does not guarantee that data will reach its destination.
  - It does **not provide retransmission mechanisms** in case of packet loss, making it faster but less reliable.

- **TCP (Transmission Control Protocol)**
  - TCP is a **connection-oriented transport protocol** that enables **two-way communication** between two endpoints using the **3-Way Handshake** procedure.
  - It is a **reliable protocol**, meaning it ensures that all transmitted data successfully reach their destination.
  - If transmission errors occur, TCP automatically **retransmits lost data**.

4. Transport Layer

OSI Model Layers

5. Session Layer

5. Session Layer

The session layer allows users on different machines to **establish sessions**.

A session provides various services, including

- **Dialog management:** keeps track of whose turn it is to transmit.
- **Token management:** prevents two participants from attempting the same critical operation simultaneously.
- **Synchronization:** manages **recovery points** so that long transmissions can resume from where they stopped after an interruption.

OSI Model Layers

6. Presentation Layer

6. Presentation Layer

- Unlike the lower layers, which mainly deal with the transmission of bits, the presentation layer focuses on the **syntax and semantics** of the transmitted information.

- To enable communication between computers using **different data representations**, the exchanged data structures must be defined in an **abstract way** and linked to a **standard encoding system** used during transmission.

- This layer is responsible for **managing these data structures** and allows the **definition and exchange of higher-level structures** (for example, banking records).

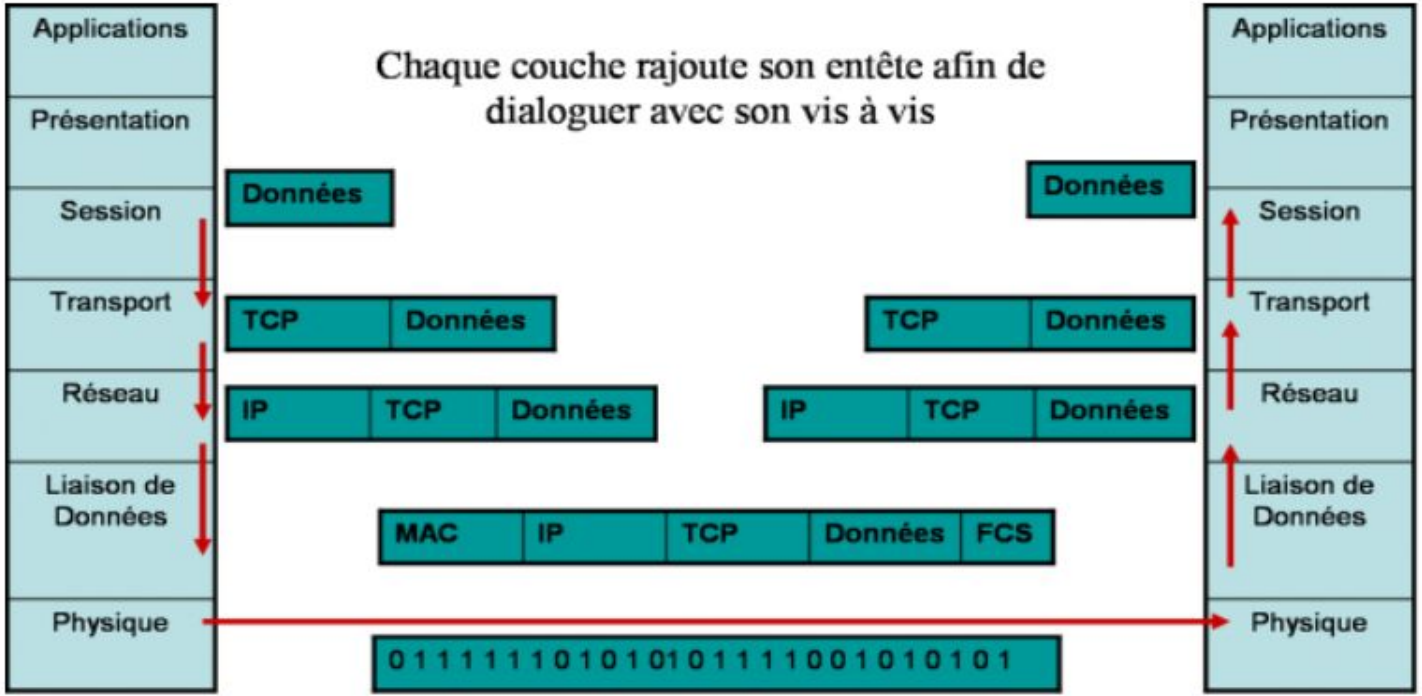
OSI Model Layers

7. Application Layer

7. Application Layer

- The application layer contains a variety of **protocols useful to end users**.
- **HTTP (HyperText Transfer Protocol)**, which forms the foundation of the **World Wide Web**, is one of the most widely used application protocols.
- When a browser needs to display a web page, it sends the page name to the server using the **HTTP/HTTPS** protocol.
- The server then responds by sending back the requested web page.
- Other application protocols are used for **file transfer**, **email communication**, and various other services.

Principle of Encapsulation / De-encapsulation



Quizz Time

Quiz 1 - IP Addressing

What is the main purpose of a subnet mask?

A. To identify the network and host portions of an IP address

B. To encrypt IP packets

C. To assign MAC addresses

D. To route data between networks

Quiz 2 - TCP Protocol

What are the three steps of the TCP three-way handshake?

A. SYN → ACK → SYN-ACK

B. SYN → SYN-ACK → ACK

C. ACK → SYN → FIN

D. FIN → ACK → SYN

Quiz 3 - OSI Model: Data Units

Each layer of the OSI model uses a specific type of data unit (PDU).

Match each data unit to the correct OSI layer.

Option	Layers
A. Bit	1️⃣ Layer 5
B. Frame	2️⃣ Layer 4
C. Packet	3️⃣ Layer 3
D. Session	4️⃣ Layer 2
E. Datagram	5️⃣ Layer 1
F. Data	

Quiz 4 – IP Addressing

Which of the following is a *private IP address*?

A. 8.8.8.8

B. 172.16.5.10

C. 200.10.5.6

D. 150.20.0.2

Quiz 5 – Common ports

Match the following **ports** with the correct **services**.

- 21 → ? NAS SAN OWASP
- 22 → ?
- 23 → ?
- 25 → ?
- 80 → ?
- 443 → ?
- 53 → ?
- 3389 → ?

Quiz 6 – Subnetting Concept

How many hosts can a `/24` network support?

A. 254
B. 256
C. 512
D. 128

Quiz 7 – Protocols in Security

What is the purpose of **ARP** (Address Resolution Protocol)?

A. Converts IP addresses to MAC addresses
B. Converts MAC addresses to IP addresses
C. Routes packets between networks
D. Encrypts data packets

Quiz 8 – Protocols & Security Risks

Some network protocols are inherently insecure if used without encryption.
Match the following **protocols** to their **secure or insecure equivalents**.

Insecure Protocol	Secure Alternative
FTP	?
Telnet	?
HTTP	?
POP3	?
LDAP	?

Quiz 9 – IP Addressing and Subnetting

For each of the following networks:

- `172.16.0.0/16`
- `192.168.20.3/24`
- `192.168.67.34/19`

Indicate the following:

- subnet mask
- network address
- first usable host address
- last usable host address
- broadcast address

Q & A

amine.merzoug@univ-batna2.dz

https://staff.univ-batna2.dz/merzoug-amine

https://github.com/amine-merzoug