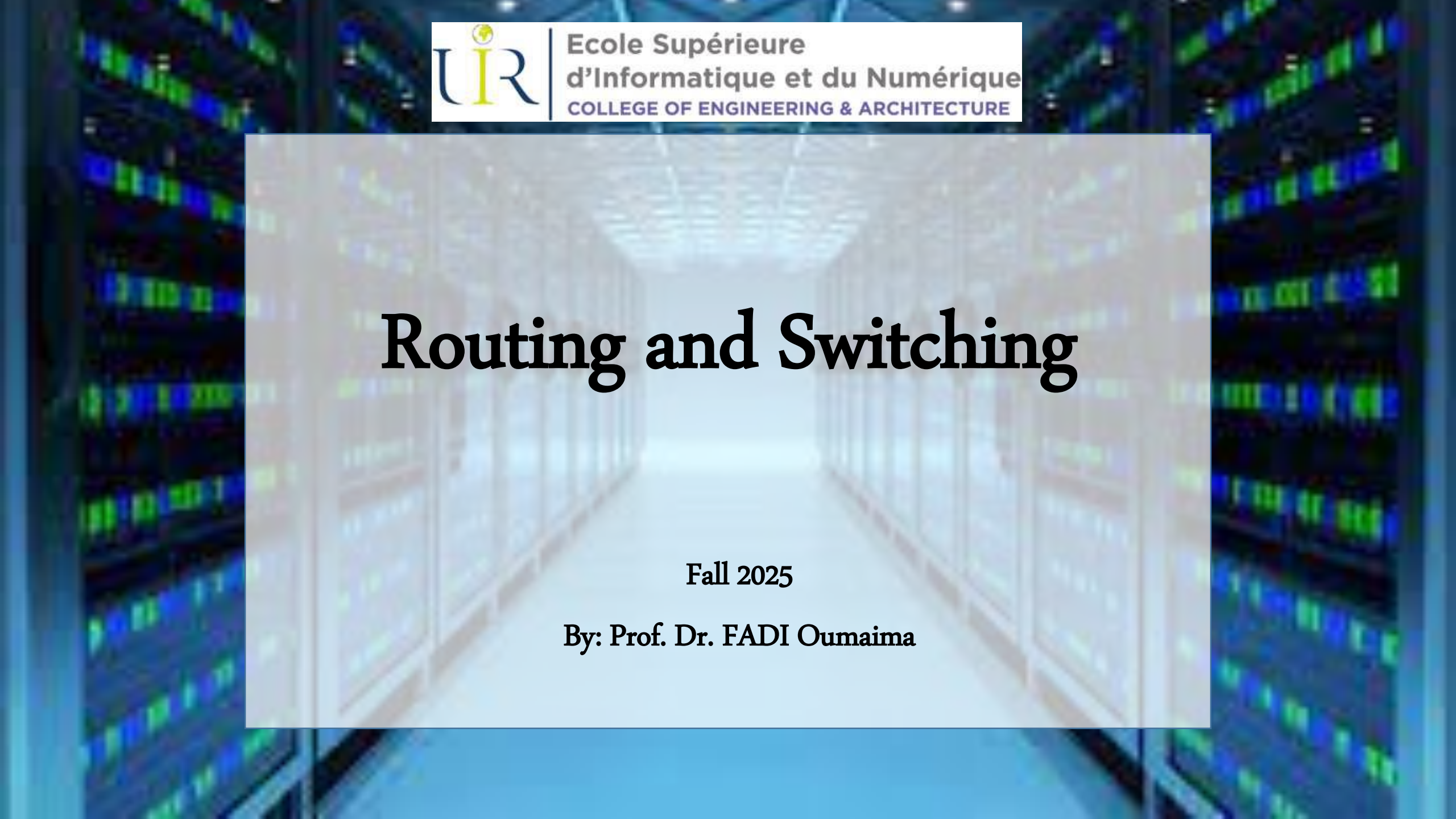


Routing and Switching

Fall 2025

By: Prof. Dr. FADI Oumaima

Lecture: Prof. Dr. Fadi Oumaima

Email: oumaima.fadi@uir.ac.ma

Evaluation

Lab Report+ Quiz:**10%**

CC: **20%**

CF: **50%**

HCIA-certification: **20%**

Chapter1: Networking Fundamentals & OSI/TCP-IP Models

Topics:

- Networking basics: LAN, WAN, Internet, intranets
- Physical vs. logical topologies
- Copper, fiber, wireless media
- OSI Reference Model
- TCP/IP model

Goals:

- ✓ Understand what a network is and what constitues it.
- ✓ Identify the network components
- ✓ Describe the primary mechanisms of communication over a network

What's a network?

A **network** is an interconnected system that allows the flow of:

- Continuous or discontinuous streams (water, air, oil…)
- Discrete elements (goods, information, people…

Computer Network (Réseau Informatique)

A **communication system** (hardware + software)
Enables a set of computers (in the broad sense) to exchange information

A **digital telecommunications network** that enables resource sharing among **nodes**

Nodes = communication devices using a common telecom technology
Broad sense: access points, phones, sensors, etc

What's a network?

Data Transmission
Ensured through **data links**, using:

- **Wired media**: twisted pair cables, fiber optics
- **Wireless methods**: Wi-Fi, microwave transmission, free-space optical communication

Purpose of Networks
Information exchange is not the final goal → networks enable **services**
Services are:

- Accessible from any device connected to the network
- Implemented by a set of computers on the network

Examples of services:
Email (SMTP)
File transfer (FTP)
Remote access (Telnet, SSH)

What’s a communication protocol?

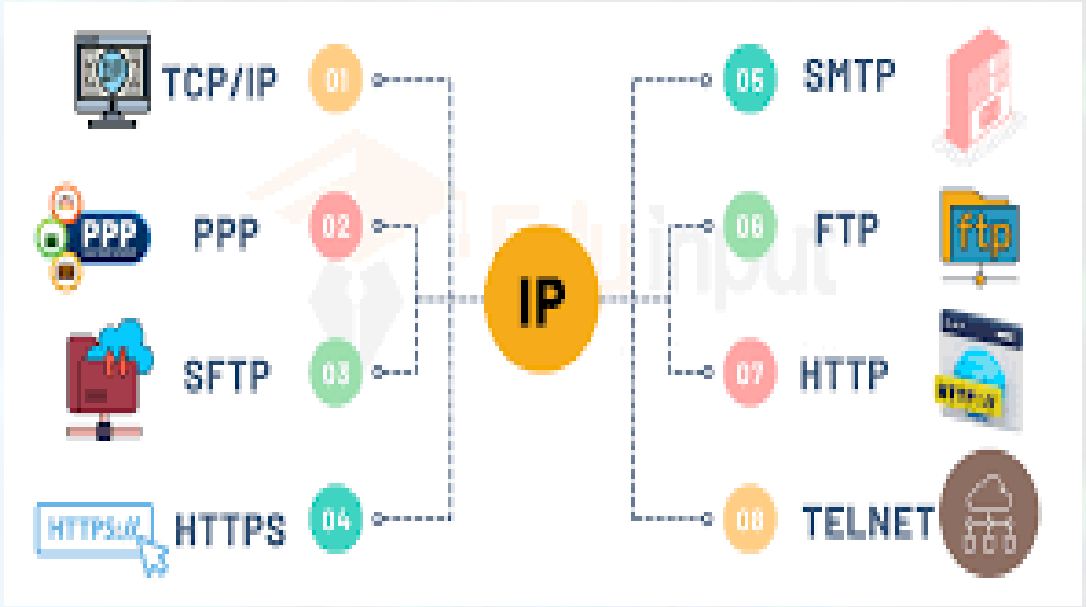
Communication Protocol

A communication protocol = **set of rules & procedures** defining a type of communication

Protocols are **organized in layers** to decompose and order tasks

Several protocol families/models exist, each as a suite of layered protocols

Examples: **OSI, TCP/IP, IBM ASN, AppleTalk**



Network History

1926 • Phone

1974 • The internet was born

1985 • First domain name

1991 • First Website

1999 • IoT introduced

2015 • 15 B connected devices

2020 • 50B connected devices

Networks support the way we learn

- Virtual Classrooms
- On-demand Video
- Collaborative Learning Spaces
- Mobile Learning

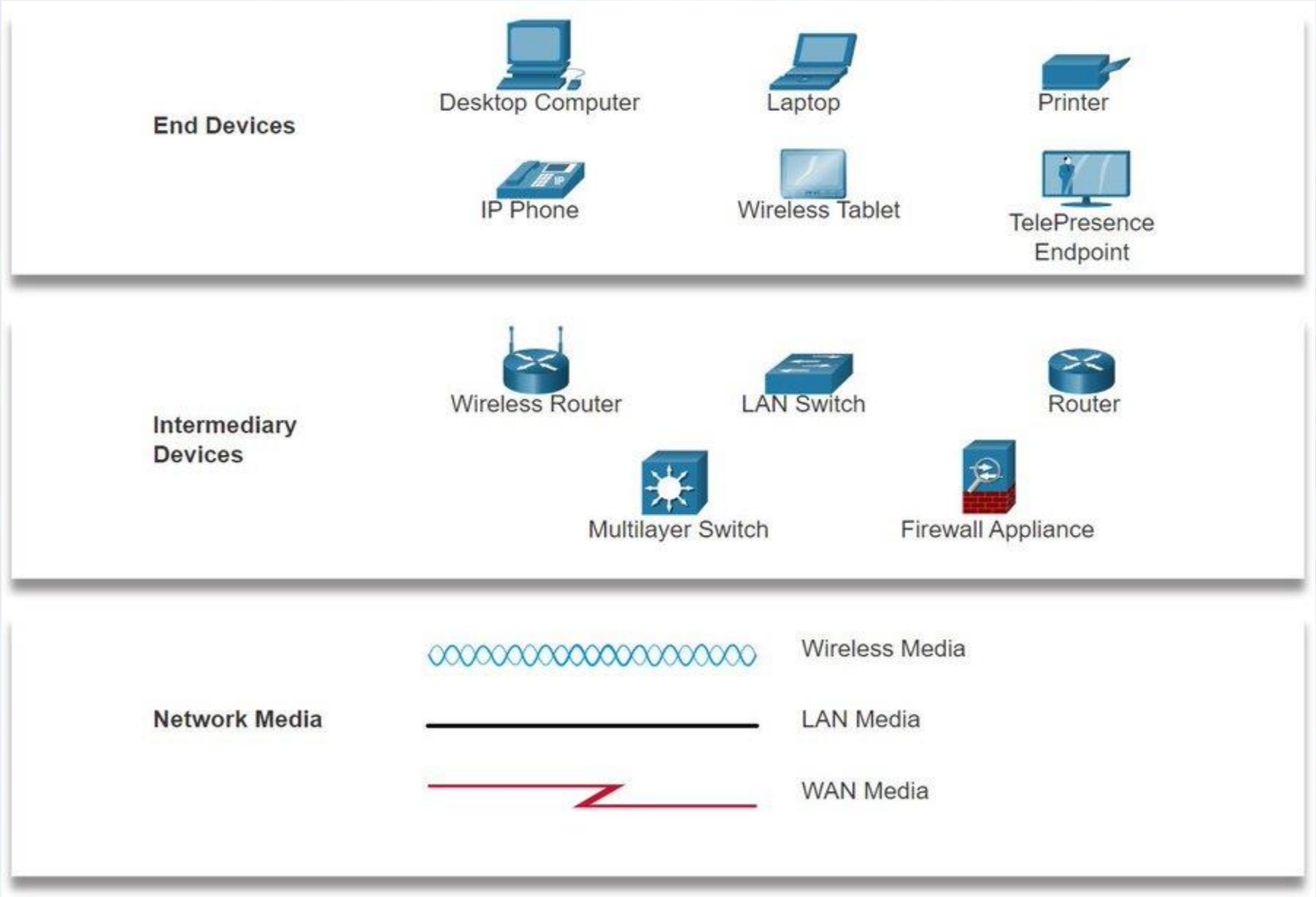
Networks support the way we communicate

- Instant Messaging (IM)
- Social Media
- Weblogs
- Podcasting
- P2P File Sharing

Networks support the way we play/ do business

- Online Gaming
- Online Shopping
- Online Entertainment

Networks Components



Networks Components

- Router

- A router connects two or more networks together
- Forwards packets based on **IP addresses** (Layer 3 – Network Layer)

✓ Uses routing tables and routing protocols (RIP, OSPF, BGP)

✓ Determines the **best path** for data transmission

✓ Provides NAT (Network Address Translation) and DHCP services

✓ Can filter traffic (basic security)

Example: Connects a home/office LAN to the Internet

Networks Components

- Switch

- A switch interconnects multiple devices inside a LAN

- Forwards frames based on **MAC addresses** (Layer 2 – Data Link Layer)

- ✓ Creates separate **collision domains** (unlike hubs)
- ✓ Learns MAC addresses and builds a switching table
- ✓ Provides full-duplex communication
- ✓ Supports VLANs and Quality of Service (QoS) in advanced models

Use Case: Connecting PCs, printers, and servers within the same LAN

Networks Components

- Firewall

- A firewall is a **security barrier** between trusted and untrusted networks

- Controls incoming/outgoing traffic based on **security rules**

Types:

Packet-filtering firewalls (Layer 3)

Stateful inspection firewalls (track connections)

Next-Generation Firewalls (NGFW – includes IDS/IPS, deep packet inspection)

- ✓ Blocks unauthorized access
- ✓ Protects against malware, attacks, and data leaks
- ✓ Enforces network security policies

Use Case: Protecting enterprise LANs from Internet threats

Networks Components

- Hub

- A hub is a simple device operating at **Layer 1 (Physical Layer)**

- Broadcasts data to **all ports**, regardless of destination

- ✓ No intelligence (cannot filter or learn addresses)
- ✓ Half-duplex → prone to collisions
- ✓ All devices share the same collision and broadcast domain

Disadvantage: Very inefficient, replaced by switches

Use Case: Was used in early LANs (10Base-T Ethernet)

Network Media

Definition: Network media are the **physical or wireless paths** that carry data signals

- Wired (LAN):

Unshielded Twisted Pair (UTP)

Consists of two **copper conductors**, insulated from each other

The conductors are twisted **helically** around a longitudinal symmetry axis

Twisting reduces the effects of **electromagnetic interference (EMI)** from the environment

Widely used in Ethernet and telephone networks

Most common use: **connecting subscribers to the telephone central office**

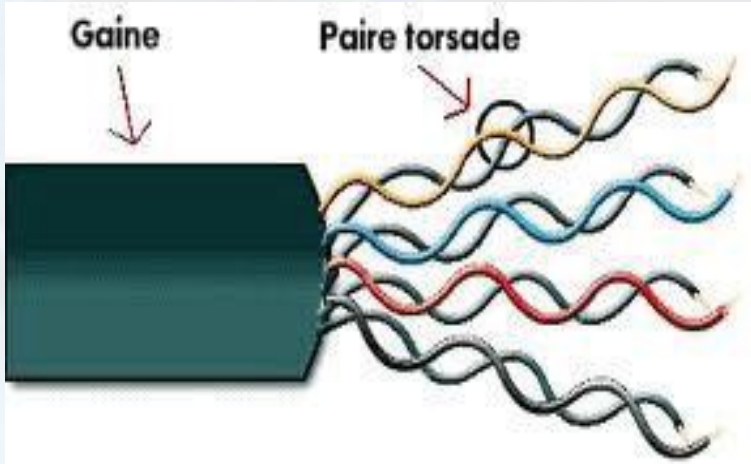
Main drawback: signal attenuation, especially when conductor diameter is small

Solution: use of **repeaters**

Recommended for **short distances** (a few kilometers)

Low cost medium

Easy to connect and add new equipment



Network Media

Coaxial Cables

To avoid interference from external noise, coaxial cables use **two cylindrical metallic conductors** with the same axis, separated by an insulator

Provide **better performance** than twisted pair:

Lower signal attenuation

Support for higher-frequency signal transmission

Greater resistance to external disturbances

Commonly used in cable TV, broadband Internet, and early Ethernet networks

Capacity depends on:

- **Length** of the cable
- **Physical characteristics** of conductors and insulation
- Performance:
- Up to **tens of Mbit/s** over 1 km
- **Higher bitrates** possible over shorter distances
- Over **10 km**, transmission rates drop below **10 kbit/s**

Network Media

Optical Fiber Cable

Very thin glass fiber composed of:

Core: Light propagates here, emitted by an LED or laser source

Cladding: Has a refractive index ensuring the light signal stays within the fiber

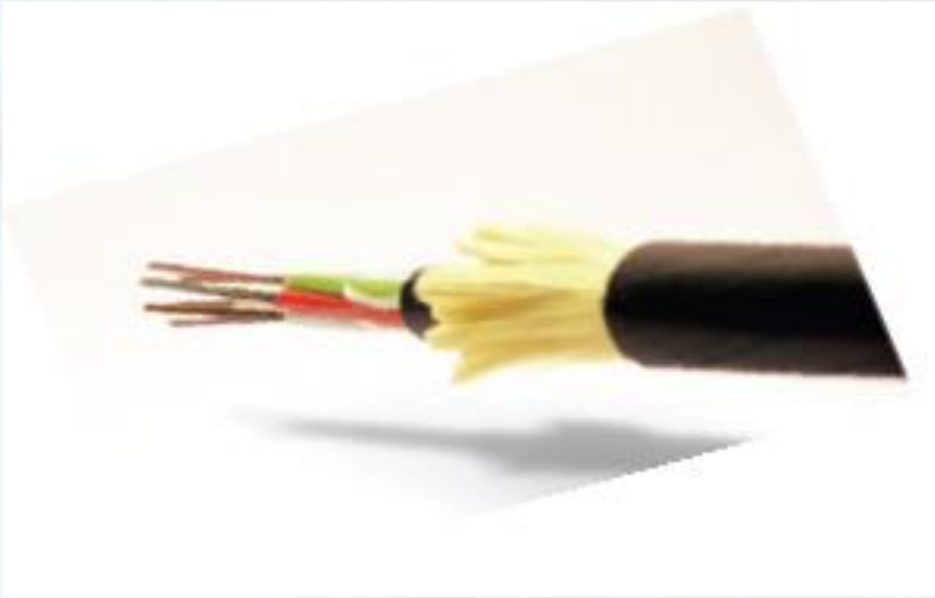
Advantages of Optical Fiber

Very small external diameter (~0.1 mm)

Extremely lightweight (a few grams per kilometer)

Very high capacity – allows simultaneous transmission of many TV and telephone channels

Resistant to interference from nearby radio transmitters



Network Media

Wireless:

- Wi-Fi (802.11 standards)
- Bluetooth (short range)
- Microwave links
- Satellite communication
- Free-Space Optical (laser-based)

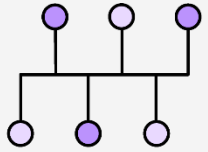
WAN Media:

- Leased lines (E1/T1)
- MPLS (Multi-Protocol Label Switching)
- 4G/5G Cellular
- Satellite links for remote locations

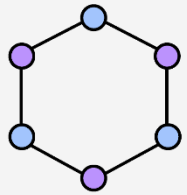
Impact: Media type affects **speed, cost, distance, and reliability**

Network topologies

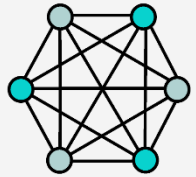
Bus



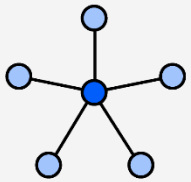
Ring



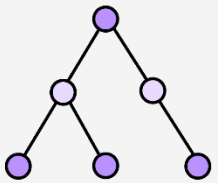
Mesh



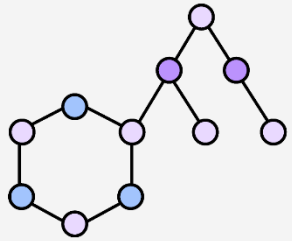
Star



Tree

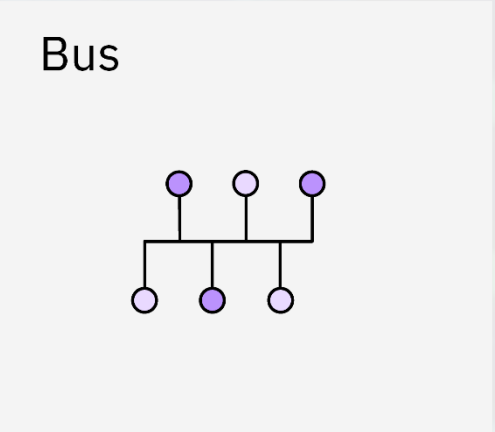


Hybrid



Network topologies

Bus Topology
All devices share a single backbone cable



✓ **Advantages:**
- Easy to implement and cost-effective for small networks
- Requires less cable than star or mesh

X **Disadvantages:**
- Entire network fails if backbone breaks
- Difficult to troubleshoot and isolate issues
- Performance decreases as more devices are added

Collision issue: CSMA/CD

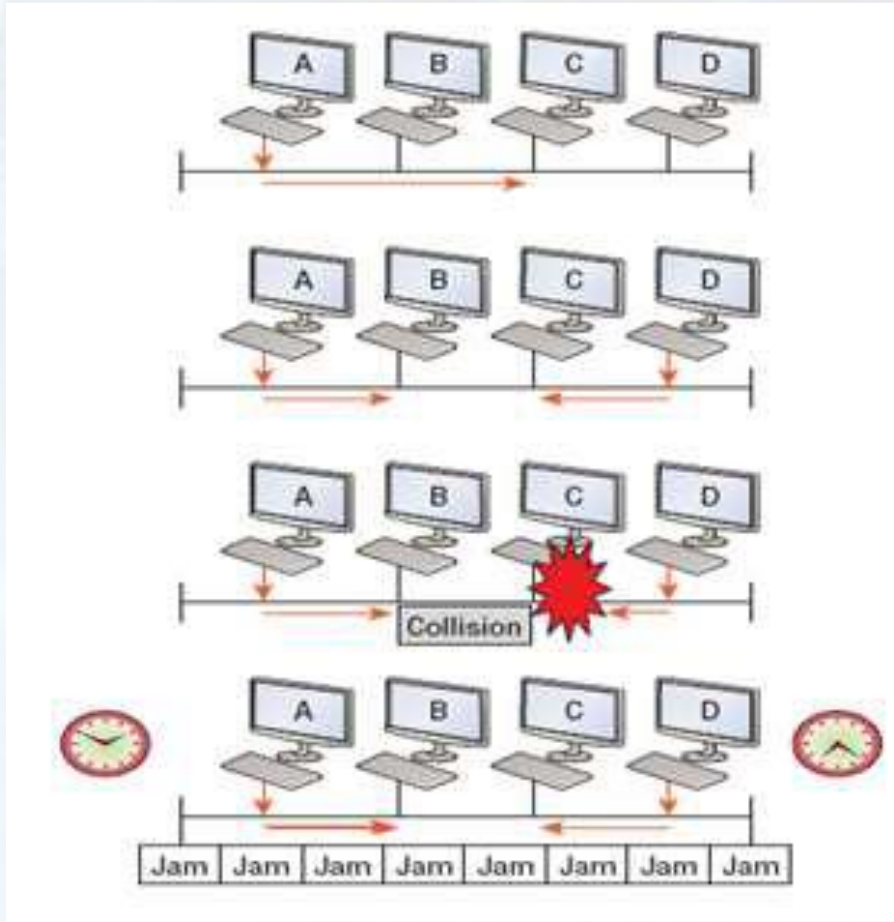
Ethernet networking uses a protocol called **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)**, which allows devices to share bandwidth evenly while preventing two devices from transmitting simultaneously on the same network medium. CSMA/CD was created to overcome the problem of **collisions** that occur when packets are transmitted from different nodes at the same time.

So, how does the CSMA/CD protocol work?

Collision issue: CSMA/CD

When a collision occurs on an Ethernet LAN, the following events take place:

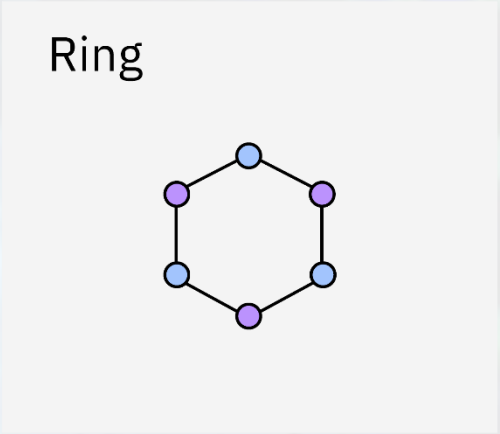
1. A **jam signal** informs all devices that a collision has occurred.
2. The collision triggers a **random backoff algorithm**.
3. Each device on the Ethernet segment **stops transmitting** for a short period until its waiting timer expires.
4. All hosts then have **equal priority** to transmit once their timers expire.



Network topologies

Ring Topology

Each device connected to exactly two others, forming a closed loop



✓ **Advantages:**

Easy to install and reconfigure

Equal access to the network (no central control)

Performs better than bus under heavy load

X **Disadvantages:**

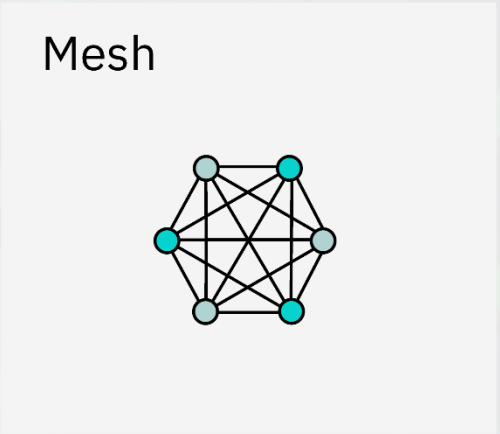
A single break can disrupt the whole network

Troubleshooting is difficult

Adding/removing nodes can affect the entire ring

Network topologies

Mesh Topology
Every device connected to every other device (full or partial mesh)



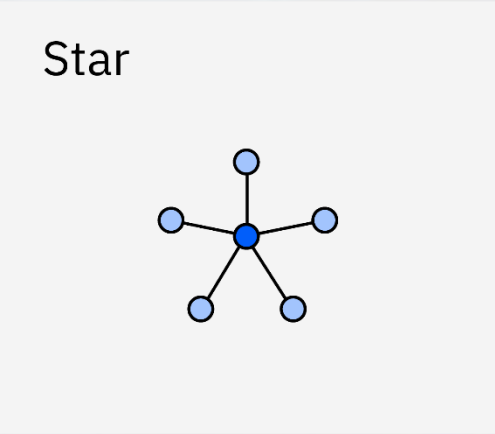
✓ **Advantages:**
High redundancy and fault tolerance
Data can take multiple paths → very reliable
High performance, no congestion

X **Disadvantages:**
Very expensive (lots of cabling and ports required)
Complex installation and management
Not scalable for very large networks

Network topologies

Star Topology

Definition: All devices connect to a central device (hub or switch)

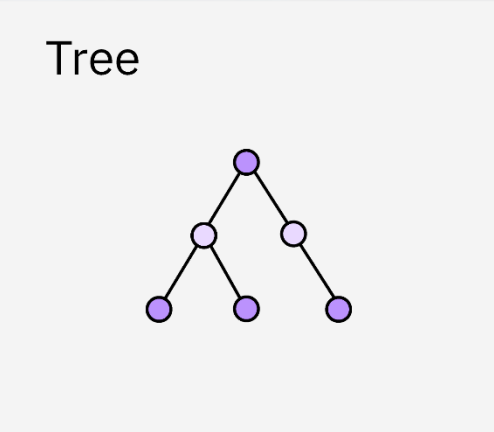


✓ **Advantages:**
- Easy to install and manage
- Easy to add or remove devices
- A single cable failure affects only one node

X **Disadvantages:**
- Failure of the central device brings down the entire network
- Requires more cable length than bus or ring
- Central device adds cost

Network topologies

Tree Topology
A hybrid of star and bus; devices are connected in a tree-like structure with levels

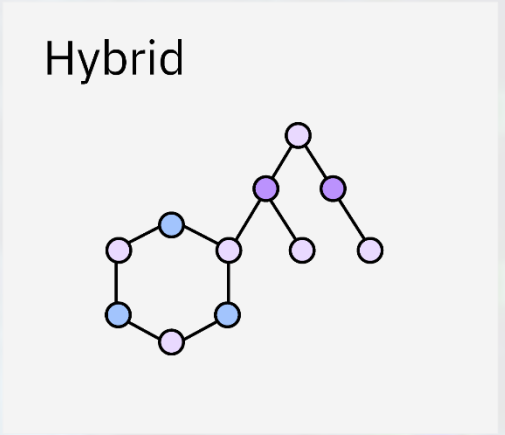


✓ **Advantages:**
- Supports large networks with structured management
- Easier to expand than bus or ring
- Isolation of groups possible

✗ **Disadvantages:**
- If backbone/root node fails, the whole segment is affected
- Complex configuration compared to star or bus
- More expensive cabling and management

Network topologies

Hybrid Topology
Combination of two or more different topologies (e.g., star-bus, star-ring)



✓ **Advantages:**
- Flexible and adaptable to different needs
- Inherits strengths of combined topologies
- Scalable for large, complex networks

X **Disadvantages:**
- Design and management can be complex
- More expensive than simple topologies
- Failure in one part may affect others depending on the structure

Network topologies: Sum up

Topology	Advantages	Disadvantages	Best Use Case
Ring	Equal access, better under load	One break disrupts whole ring	Small closed networks
Bus	Low cost, simple to set up	Backbone failure = total failure, poor scalability	Small networks, labs
Star	Easy to manage, single failure only affects one device	Central device failure = total failure, more cabling	LANs, offices
Hierarchical (Tree)	Scalable, structured	Backbone failure affects whole segment, costly	Large organizations, ISPs
Mesh	Very reliable, fault-tolerant	Very expensive, complex	Critical networks (military, financial)
Hybrid	Flexible, scalable, combines strengths	Complex design, high cost	Enterprise, large data centers

Networks types

Personal Area Network (PAN)

A PAN is a network used for communication among devices close to one person, typically within a range of a few meters.

Use Cases:

- Connecting personal devices like smartphones, tablets, and wearables.
- Enabling hands-free communication through Bluetooth headsets.
- Synchronizing data between a computer and a smartphone.

Local Area Network (LAN)

A LAN is a network that connects computers and devices within a limited area such as a home, office, or building.

Use Cases:

- Sharing resources like printers and file servers within an office.
- Facilitating communication and collaboration among employees.
- Providing internet access within a home or small business.

Network types

Metropolitan Area Network (MAN)

A MAN covers a larger geographic area than a LAN but smaller than a WAN, typically spanning a city or a large campus.

Use Cases:

- Connecting multiple campuses of a university.
- Providing high-speed internet access across a city.
- Linking local government offices within a metropolitan area.

Wide Area Network (WAN)

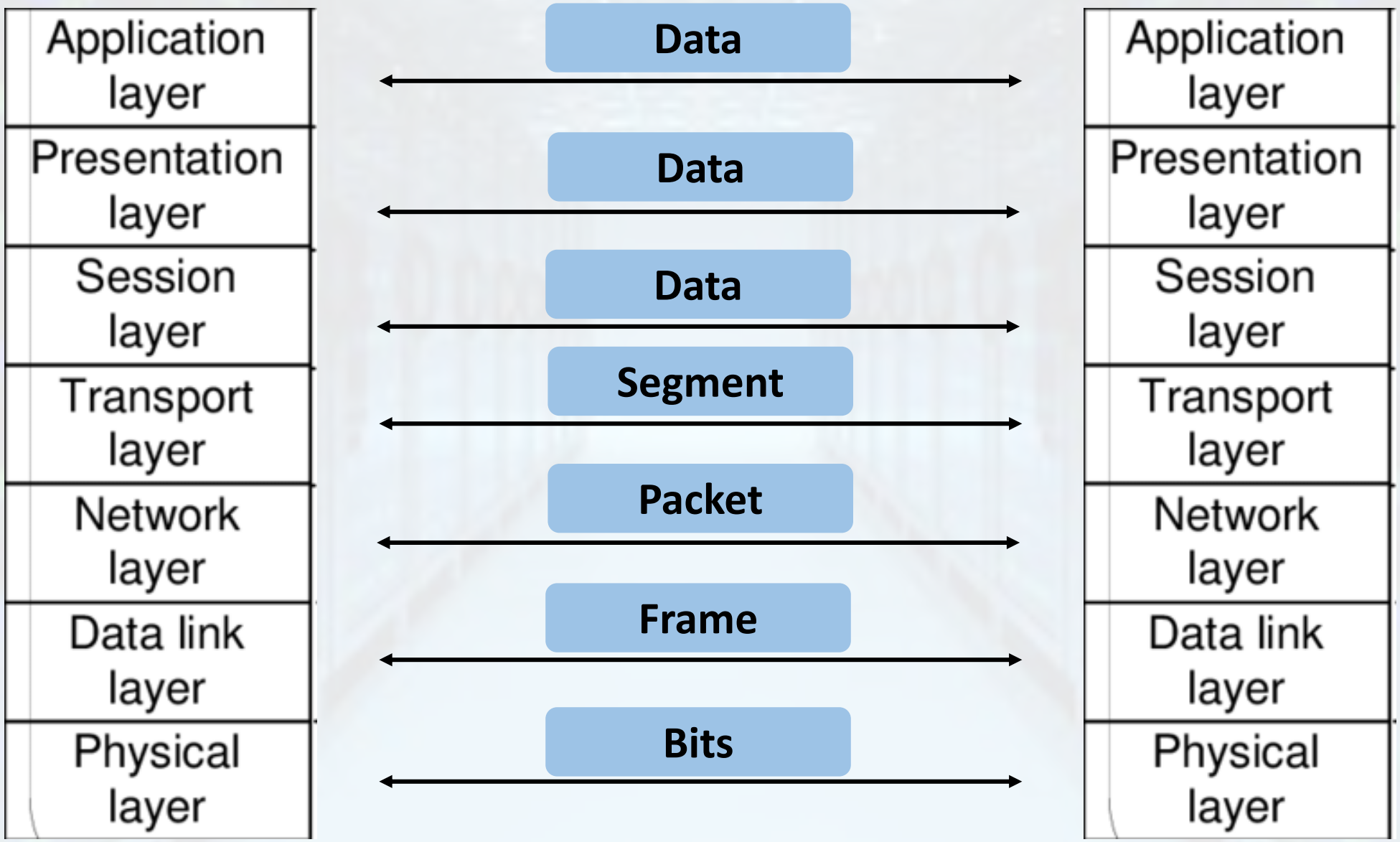
A WAN spans a large geographic area, often a country or continent.

The most prominent example of a WAN is the Internet.

Use Cases:

- Connecting branch offices of multinational companies.
- Facilitating global communication and data exchange.
- Enabling remote access to central resources.

OSI Reference Model (7 layers)



OSI Reference Model (7 layers)

Application Layer

Manages the interface between the machine and the users

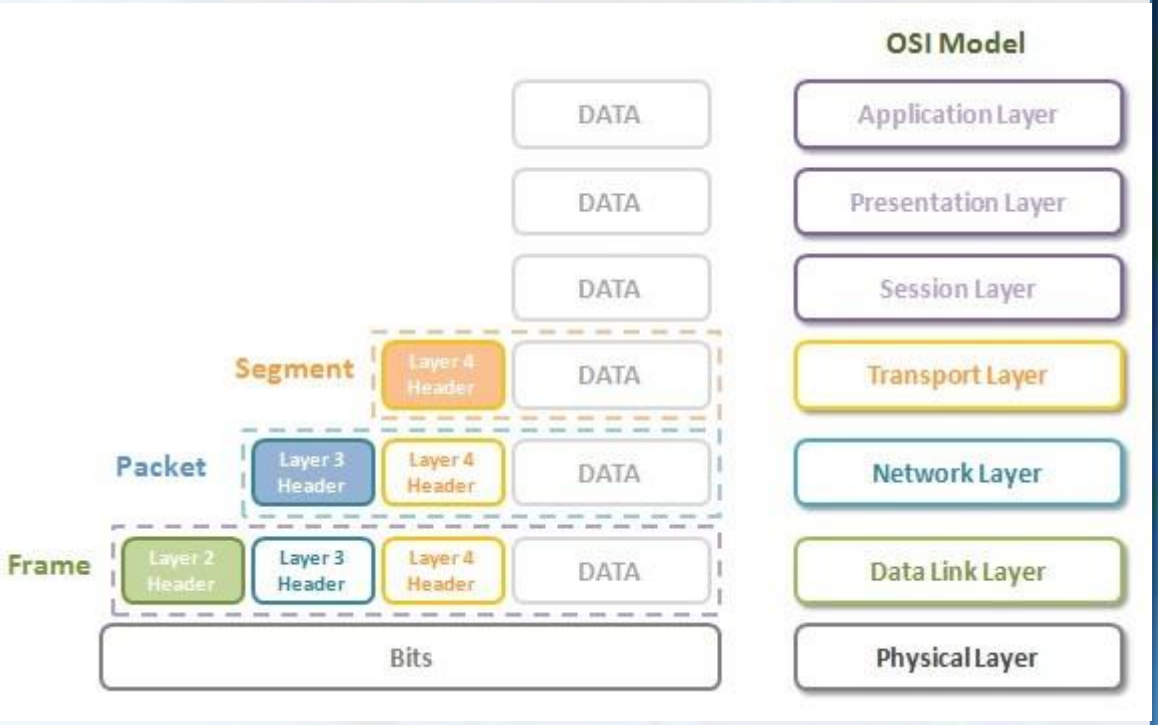
Presentation Layer

Ensures consistency and independence of transmitted data

Session Layer

Establishes and releases connections

Manages synchronization of user tasks



OSI Reference Model (7 layers)

Transport Layer

Segments long messages into smaller segments

Delivers segments **error-free and in sequence**

Provides **flow control**

Network Layer

Responsible for addressing and routing of packets

Divides segments into packets

Manages network traffic

Data Link Layer

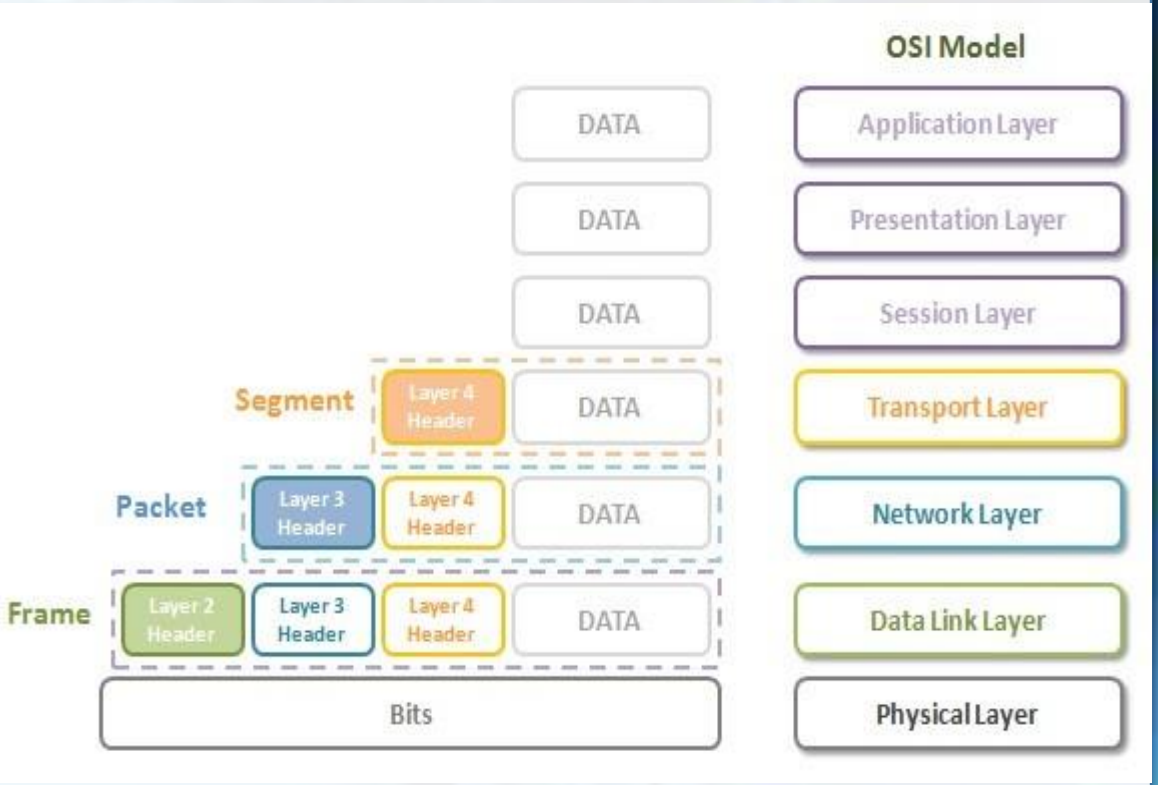
Divides packets into frames

Ensures transmission quality (error detection and correction)

Physical Layer

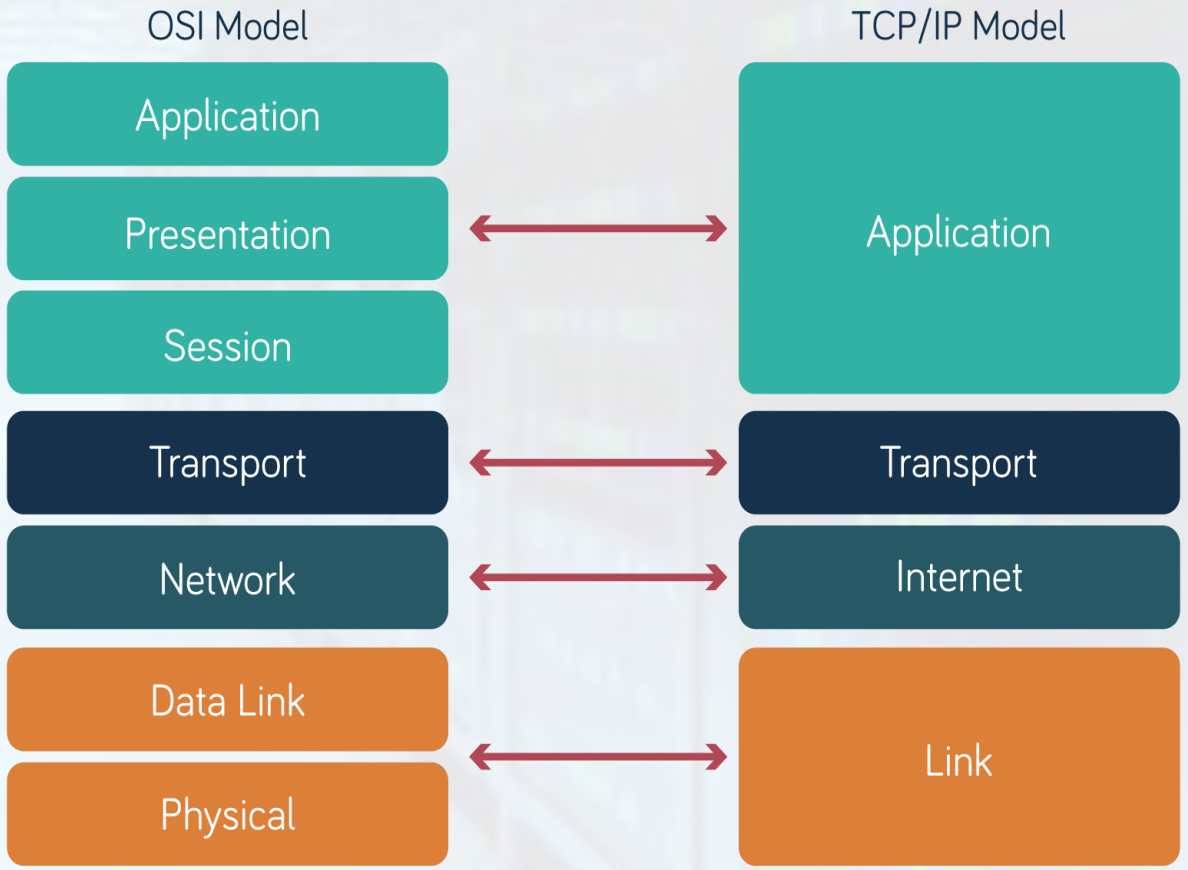
Transmits binary data over the physical medium

Adapts binary signals to the transmission medium



TCP/IP model (4 layers)

- ✓ The **Internet model (TCP/IP)** was created to solve a **practical problem**, while the **OSI model** represents a more **theoretical approach**, developed earlier in networking history.
- ✓ The OSI model is **easier to understand**, but the **TCP/IP model** is the most widely used in practice.



TCP/IP model

TCP (Transmission Control Protocol)

- A connection-oriented, end-to-end protocol
- Provides flow control and congestion control
- Ensures data integrity (checksum)
- Guarantees reliable transmission (loss detection and retransmission)

A TCP connection is uniquely identified by:

- ✓ Source IP address
- ✓ Destination IP address
- ✓ Source TCP port
- ✓ Destination TCP port

Why TCP is Used?

Known for its robustness

Applications:

- ✓ Terminal emulation
- ✓ File transfer
- ✓ Web browsing
- ✓ Email

Supports **client-server communication**