Lecture 5

Learning outcomes:

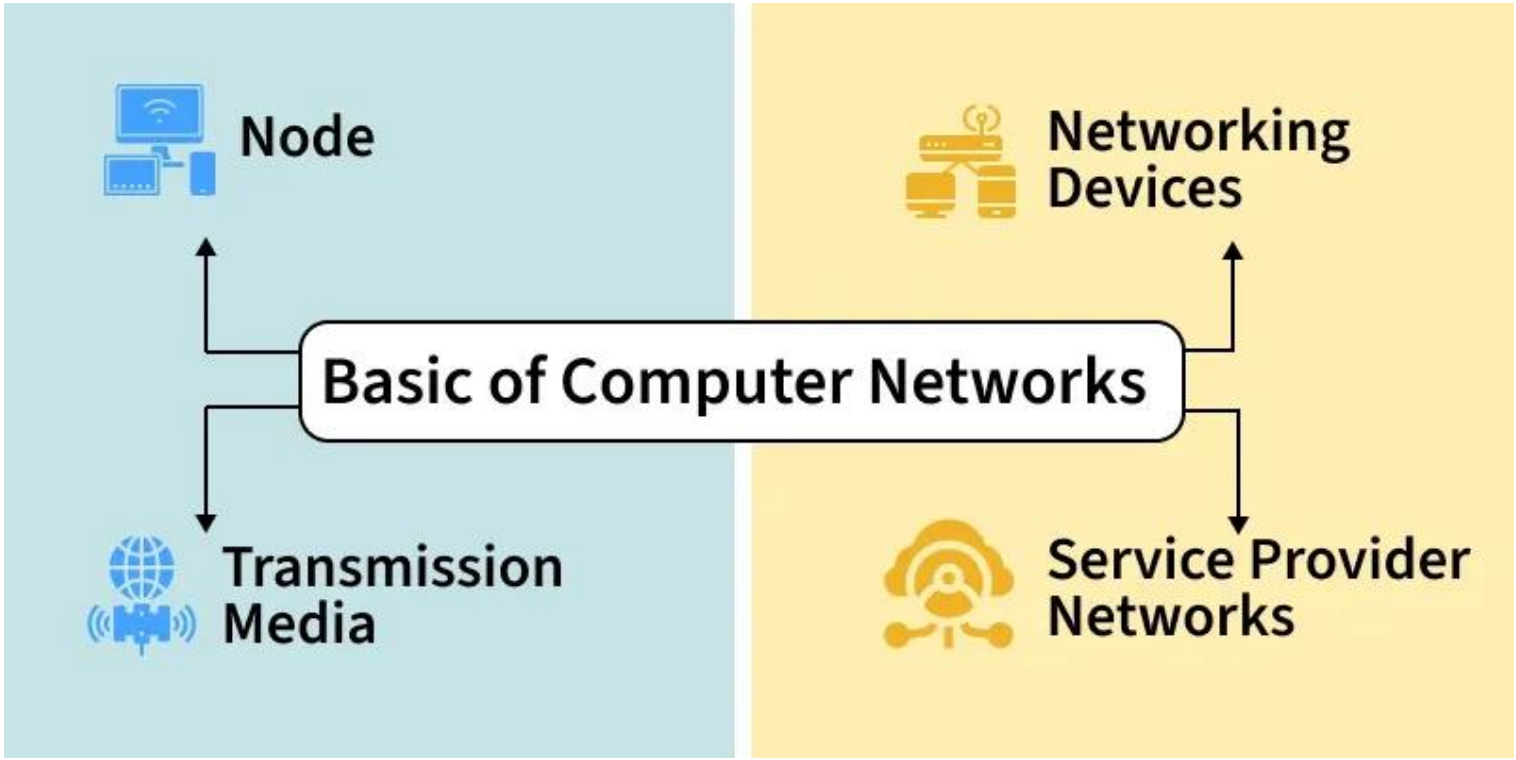
- *Computer Network.*

Computer Network

- A computer network is a collection of interconnected devices that can communicate and share resources and information with each other. These devices can include computers, servers, printers, and other hardware.

- Networks allow for the efficient exchange of data, enabling various applications such as email, file sharing, and internet browsing.

Basic Terminologies of Computer Networks



- **Node:** Any device that can send, receive, or forward data in a network. This includes laptops, mobiles, printers, servers, etc.

- **Networking Devices:** Devices that manage and support networking functions. This includes routers, switches, hubs, and access points.

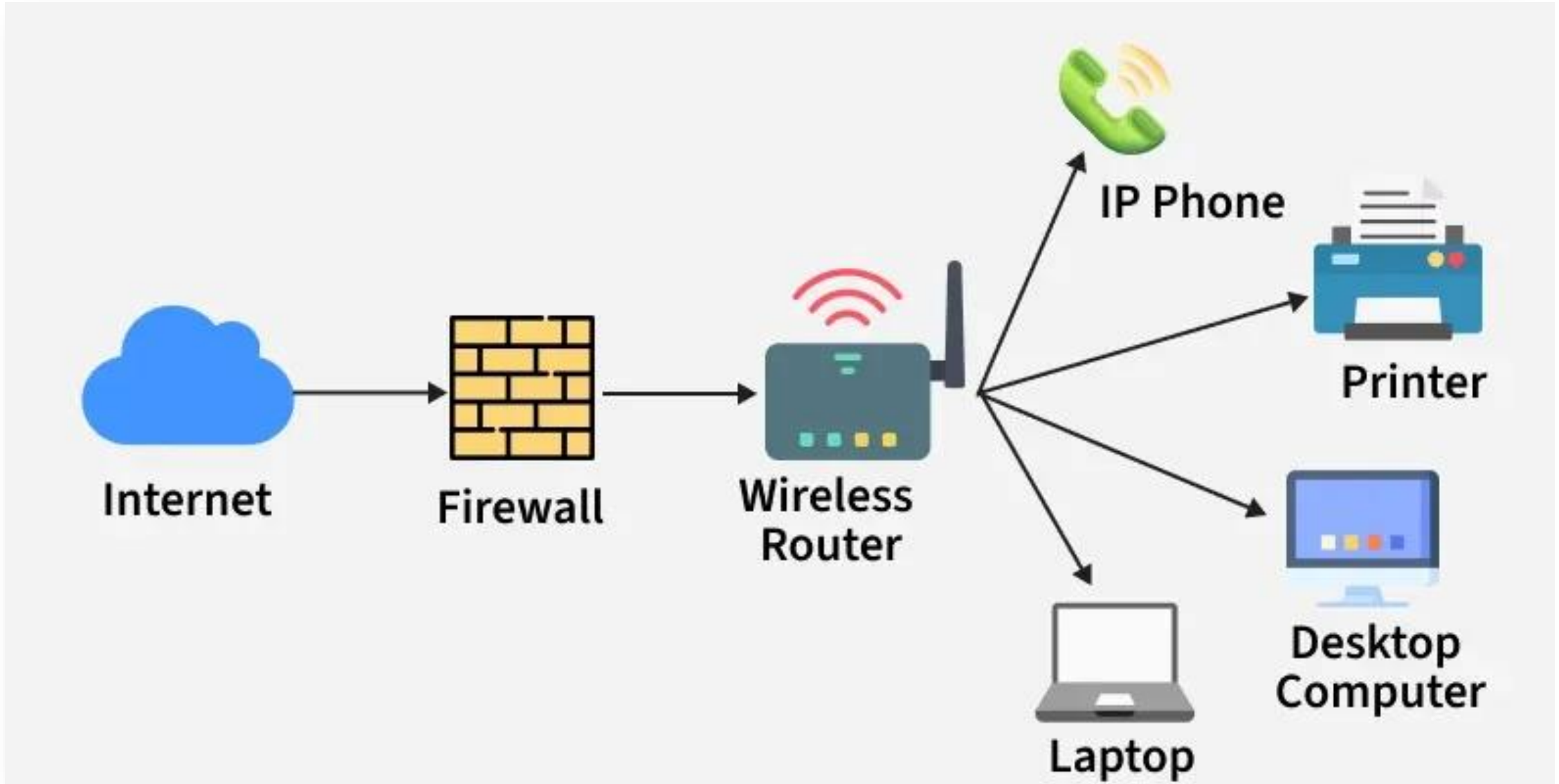
- **Transmission Media:** The physical or wireless medium through which data travels between devices. This includes wired media such as Ethernet cables and optical fiber, or wireless media such as Wi-Fi, Bluetooth and infrared.

- **Service Provider Networks:** Networks offered by external providers that allow users or organizations to lease network access and capabilities. This includes internet providers or mobile carriers, for example, major telecommunications companies like AT&T, Verizon, T-Mobile, CenturyLink (Lumen Technologies), and Comcast (Xfinity), as well as international companies such as Deutsche Telekom, China Telecom, NTT, Orange, and Tata Communications.

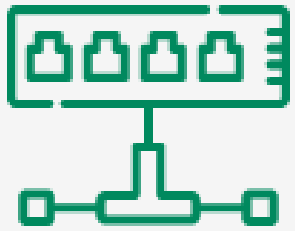
How Does a Computer Network Work

❑ Basics building blocks of a Computer network are Nodes and Links.

- A Network Node can be illustrated as Equipment for Data Communication.
- Link in Computer Networks can be defined as wires or cables or free space of wireless networks.
- The working of Computer Networks can be simply defined as rules or protocols which help in sending and receiving data via the links which allow Computer networks to communicate.
- Each device has an IP Address, that helps in identifying the device.
- A firewall is a network security device either hardware or software-based which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects, or drops that specific traffic.

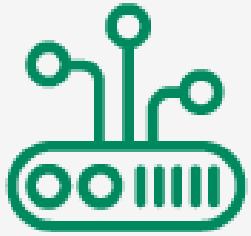

IP Phone
Printer
Internet
Firewall
Wireless
Router
Desktop
Computer
Laptop

Common Types of Network Devices

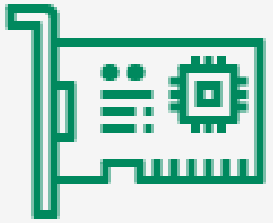


Hub

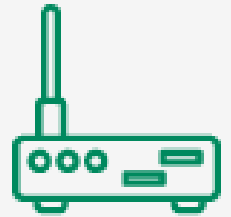
Router



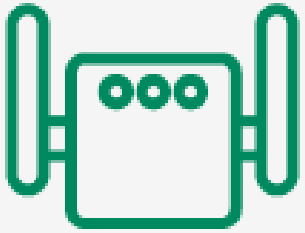
Gateway



NIC

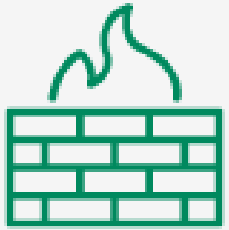


Modem



Repeater

WAP



Firewall

IDPS

VPN

Network Devices

- Network devices are physical devices that allow hardware on a computer network to communicate and interact with each other.

- Network devices like hubs, repeaters, bridges, switches, routers and gateways help manage and direct data flow in a network.

- They ensure efficient communication between connected devices by controlling data transfer, boosting signals, and linking different networks.

- Each device serves a specific role, from simple data forwarding to complex routing between networks.

Functions of Network Devices

- Network devices help to send and receive data between different devices.
- Network devices allow devices to connect to the network efficiently and securely.
- Network devices improves network speed and manage data flow better.
- It protects the network by controlling access and preventing threats.
- Expand the network range and solve signal problems.

Types of Computer Networks

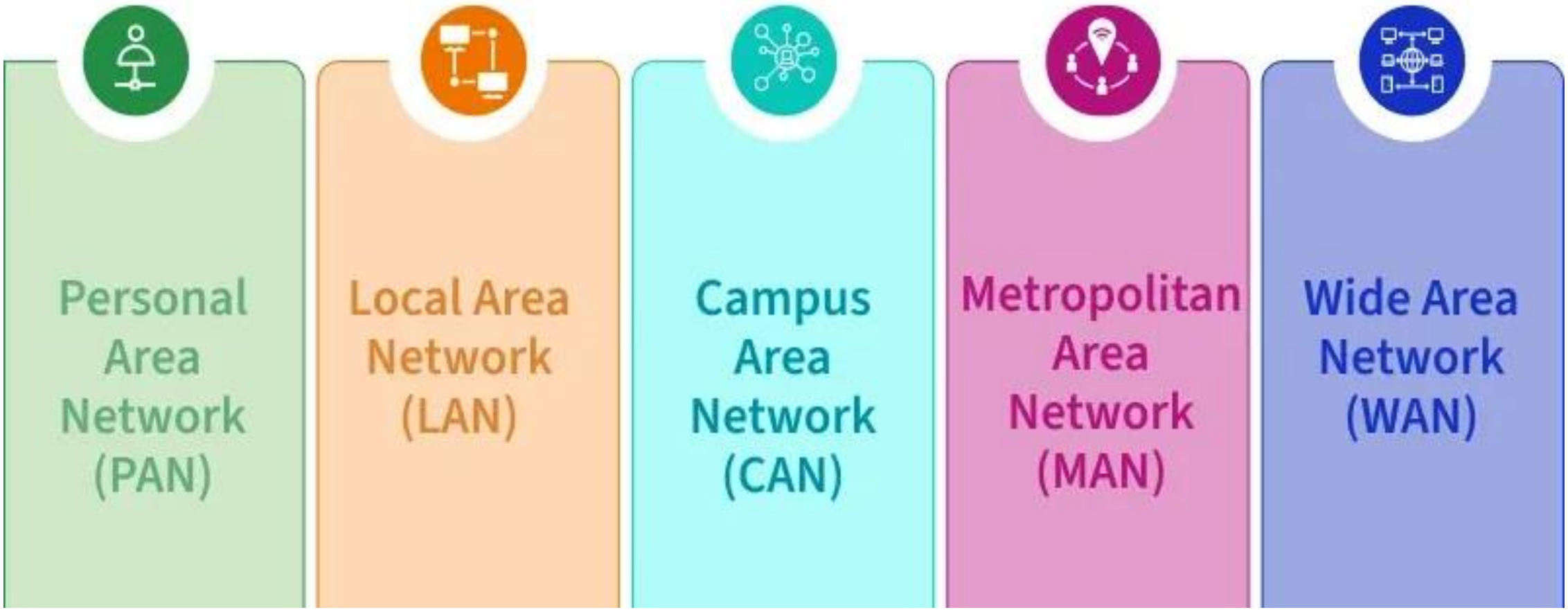
❖ Computer networks are classified based on several factors, such as architecture, geographical area, topology, etc.

❑ Types of Computer Network Architecture:

- Client-Server Architecture: Client-Server Architecture is a type of Computer Network Architecture in which Nodes can be Servers or Clients. Here, the server node can manage the Client Node Behaviour.

- Peer-to-Peer Architecture: In P2P (Peer-to-Peer) Architecture, there is not any concept of a Central Server. Each device is free for working as either client or server.

Classification Based on Geographical Area

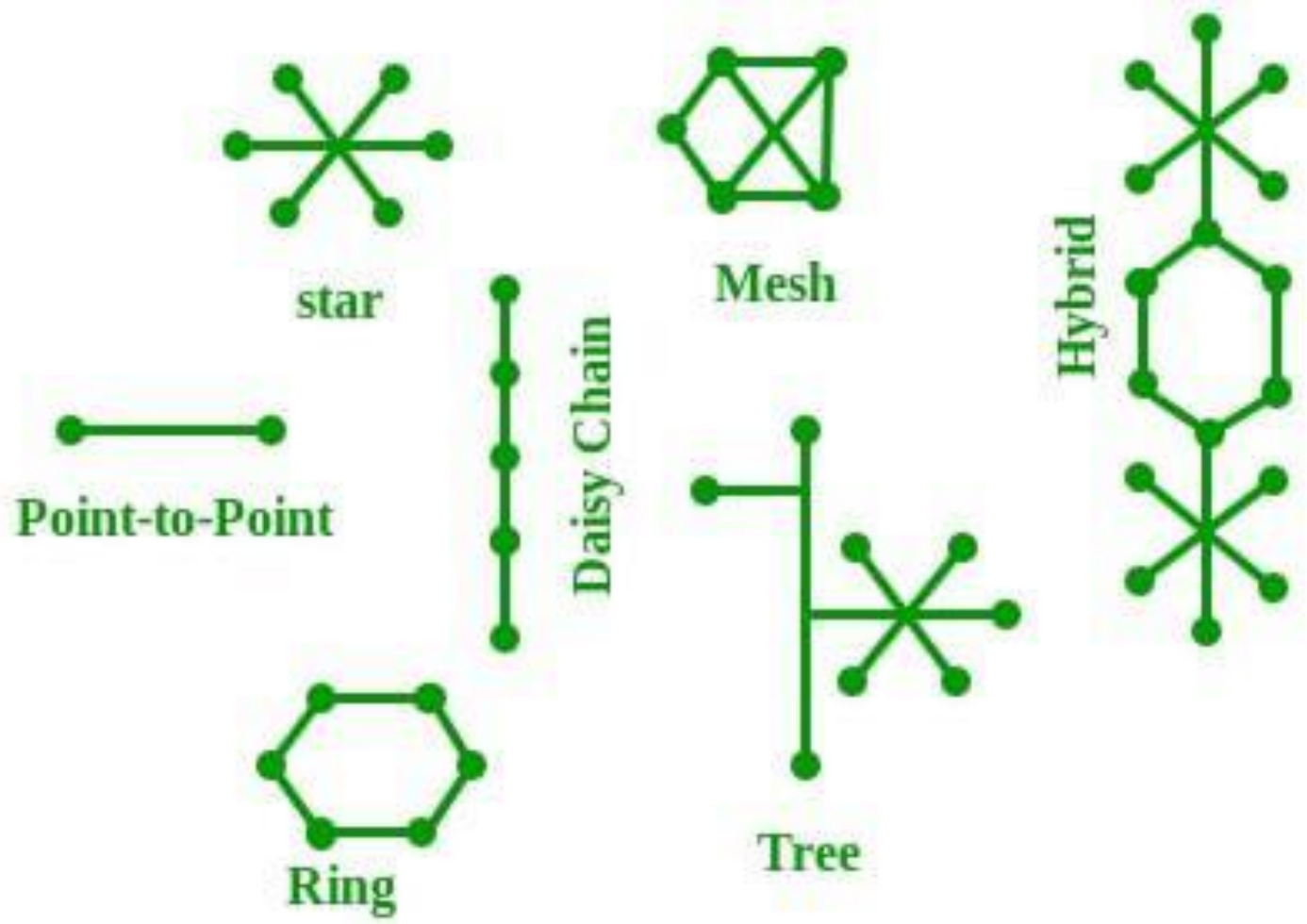


Network Topology

❖The Network Topology is the layout arrangement of the different devices in a network. Some types of network topologies are:

- **Bus Topology:** In bus topology all devices are connected to a single central cable called a bus.
- **Star Topology:** In star topology all devices are connected to a central node called hub or switch.
- **Ring Topology:** In ring topology devices are connected in a circular loop with each device connected to two others. Data travels in one direction (or sometimes both) passing through each device until it reaches its destination.
- **Mesh Topology:** In mesh topology every device is connected to every other device in the network.
- **Tree Topology:** Tree topology is the combination of star and bus topology. Tree topology is good for organizing large networks and allows for easy expansion.
- **Hybrid Topology:** Hybrid topology is the combination of two or more different topologies (like star and mesh).
- **Point-to-point topology:** It is a network setup where two devices are directly connected with a single dedicated link for communication.

Network Topology



Network Protocols

- A protocol is a set of rules or algorithms which define the way how two entities can communicate across the network.

- **Transmission Control Protocol/Internet Protocol (TCP/IP):**TCP/IP is the foundational protocol suite of the internet, enabling reliable communication. TCP Ensures data is delivered reliably and in order and IP routes data packets to their destination based on IP addresses.
- **Hypertext Transfer Protocol (HTTP) and HTTPS:** HTTP and HTTPS protocols used for transmitting web pages. In HTTP communication is unsecured and in HTTPS secured communication using SSL/TLS encryption.
- **Simple Mail Transfer Protocol (SMTP):** SMTP protocol used to send email.
- **File Transfer Protocol (FTP):** FTP protocol used for transferring files between computers. Includes commands for uploading, downloading, and managing files on a remote server.
- **Dynamic Host Configuration Protocol (DHCP):** The DHCP protocol automatically assigns IP addresses to devices on a network. Reduces manual configuration and IP address conflicts.

Computer Network Models

- Designing and managing networks is a challenging process that requires integrating various technologies such as software, hardware, firmware and electrical systems. To simplify this task, the concept of layering was introduced. Layers isolate specific tasks, operate independently and rely on one another only for data exchange, ensuring the network functions as a cohesive system.
- Layered architecture is a design framework used in networking to organize and simplify the complexities of communication systems. It divides the networking process into different layers, with each layer assigned a specific set of tasks and responsibilities. This structured approach ensures modularity, flexibility and easier troubleshooting.
- The most commonly used architectures are:

- **OSI Model**
- **TCP/IP Model**

OSI Model

- The **OSI (Open Systems Interconnection)** Model is a set of rules that explains how different computer systems communicate over a network. OSI Model was developed by the **International Organization for Standardization (ISO)**.
- The **OSI** Model consists of 7 layers and each layer has specific functions and responsibilities. This layered approach makes it easier for different devices and technologies to work together.
- The **OSI** Model provides a clear structure for data transmission and managing network issues.
- The **OSI** Model is widely used as a reference to understand how network systems function.

Layers of the OSI Model

- There are 7 layers in the OSI Model and each layer has its specific role in handling data. All the layers are mentioned below:

1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

Layer 1: Physical Layer

- The lowest layer of the OSI reference model is the Physical Layer. It is responsible for the actual physical connection between the devices.
- Physical Layer is responsible for transmitting individual bits from one node to the next.
- When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.
- Common physical layer devices are Hub, Repeater, Modem, and Cables.

Layer 2: Data Link Layer (DLL)

- The data link layer is responsible for the node-to-node delivery of the message.
- The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer.
- When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its Media Access Control (MAC) address.
- Switches and Bridges are common Data Link Layer devices.

Layer 3: Network Layer

- The network layer works for the transmission of data from one host to the other located in different networks.
- It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available.
- The sender and receiver's IP address are placed in the header by the network layer.
- The network layer is implemented by networking devices such as routers and switches.

Layer 4: Transport Layer

- The transport layer provides services to the application layer and takes services from the network layer.
- It is responsible for the end-to-end delivery of the complete message.
- The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.
- Protocols used in Transport Layer are TCP, UDP NetBIOS, PPTP.

Layer 5: Session Layer

- Session Layer in the OSI Model is responsible for the establishment of connections, management of connections, terminations of sessions between two devices.
- It also provides authentication and security.
- Protocols used in the Session Layer are NetBIOS, PPTP.

Layer 6: Presentation Layer

- The presentation layer is also called the Translation layer. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.
- Protocols used in the Presentation Layer are TLS/SSL (Transport Layer Security / Secure Sockets Layer).
- JPEG, MPEG, GIF, are standards or formats used for encoding data, which is part of the presentation layer's role.

Layer 7: Application Layer

- At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data to be transferred over the network.
- This layer also serves as a window for the application services to access the network and for displaying the received information to the user.
- Protocols used in the Application layer are SMTP, FTP, DNS, etc.

OSI Model

07 Application Layer	→	The closest layer to the user; provides application services.
06 Presentation Layer	→	Encrypts, encodes and compresses usable data.
05 Session Layer	→	Establishes, manages, & terminates sessions between end nodes.
04 Transport Layer	→	Transmits data using transmission protocols including TCP & UDP.
03 Network Layer	→	Assigns global addresses to interfaces and determines the best routes through different networks.
02 Data link Layer	→	Assigns local addresses to interfaces, delivers information locally, MAC method
01 Physical Layer	→	Encodes signals, cabling and connectors, physical specifications.

How Data Flows in the OSI Model?

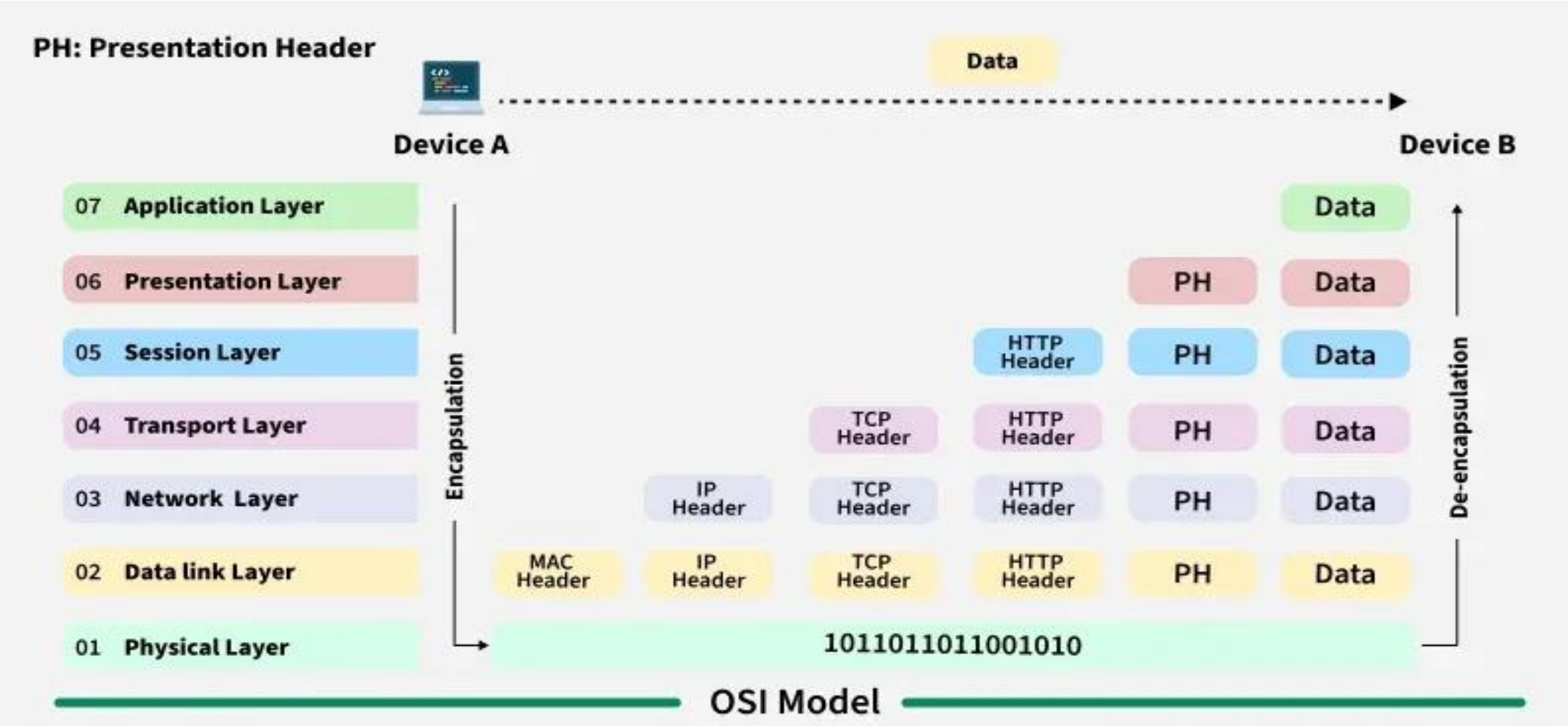
- When we transfer information from one device to another, it travels through 7 layers of OSI model.
- First data travels down through 7 layers from the sender's end and then climbs back 7 layers on the receiver's end.

Data flows through the OSI model in a step-by-step process:

- Application Layer: Applications create the data.
- Presentation Layer: Data is formatted and encrypted.
- Session Layer: Connections are established and managed.
- Transport Layer: Data is broken into segments for reliable delivery.
- Network Layer: Segments are packaged into packets and routed.
- Data Link Layer: Packets are framed and sent to the next device.
- Physical Layer: Frames are converted into bits and transmitted physically.

❖Each layer adds specific information to ensure the data reaches its destination correctly, and these steps are reversed upon arrival.

OSI Model


PH: Presentation Header
Data
Device A
Device B
07 Application Layer
06 Presentation Layer
05 Session Layer
04 Transport Layer
03 Network Layer
02 Data link Layer
01 Physical Layer
Encapsulation
De-encapsulation
Data
PH
HTTP Header
TCP Header
IP Header
MAC Header
1011011011001010
OSI Model

- We can understand how data flows through OSI Model with the help of an example mentioned below.

➢ Let us suppose, Person A sends an e-mail to his friend Person B.

- Step 1: Person A interacts with e-mail application like Gmail, outlook, etc. Writes his email to send. (This happens at Application Layer).

- Step 2: At Presentation Layer, Mail application prepares for data transmission like encrypting data and formatting it for transmission.

- Step 3: At Session Layer, there is a connection established between the sender and receiver on the internet.

- Step 4: At Transport Layer, Email data is broken into smaller segments. It adds sequence number and error-checking information to maintain the reliability of the information.

- Step 5: At Network Layer, addressing of packets is done in order to find the best route for transfer.

- Step 6: At Data Link Layer, data packets are encapsulated into frames, then MAC address is added for local devices and then it checks for error using error detection.

- Step 7: At Physical Layer, Frames are transmitted in the form of electrical/ optical signals over a physical network medium like ethernet cable or WiFi.

- After the email reaches the receiver i.e. Person B, the process will reverse and decrypt the e-mail content. At last, the email will be shown on Person B email client.

Why Does the OSI Model Matter

- The OSI Model matters because it provides the user a clear structure of "how the data moves in the network?".
- As the OSI Model consists of 7 layers, each layer has its specific role, and due to which it helps in understanding, identifying and solving the complex network problems easily by focusing on one of the layers not the entire network.
- As the modern Internet does not prefer the OSI Model, but still, the OSI Model is still very helpful for solving network problems. It helps people understanding network concepts very easily.

Advantages of OSI Model

- The OSI Model defines the communication of a computing system into 7 different layers. Its advantages include:

- It divides network communication into 7 layers which makes it easier to understand and troubleshoot.
- It standardizes network communications, as each layer has fixed functions and protocols.
- Diagnosing network problems is easier with the **OSI model.**
- It is easier to improve with advancements as each layer can get updates separately.

Disadvantages of OSI Model

- The OSI Model has seven layers, which can be complicated and hard to understand for beginners.

- In real-life networking, most systems use a simpler model called the Internet protocol suite (TCP/IP), so the OSI Model is not always directly applicable.

- Each layer in the OSI Model adds its own set of rules and operations, which can make the process more time-consuming and less efficient.

TCP/IP Model- Home work