Afternoon session

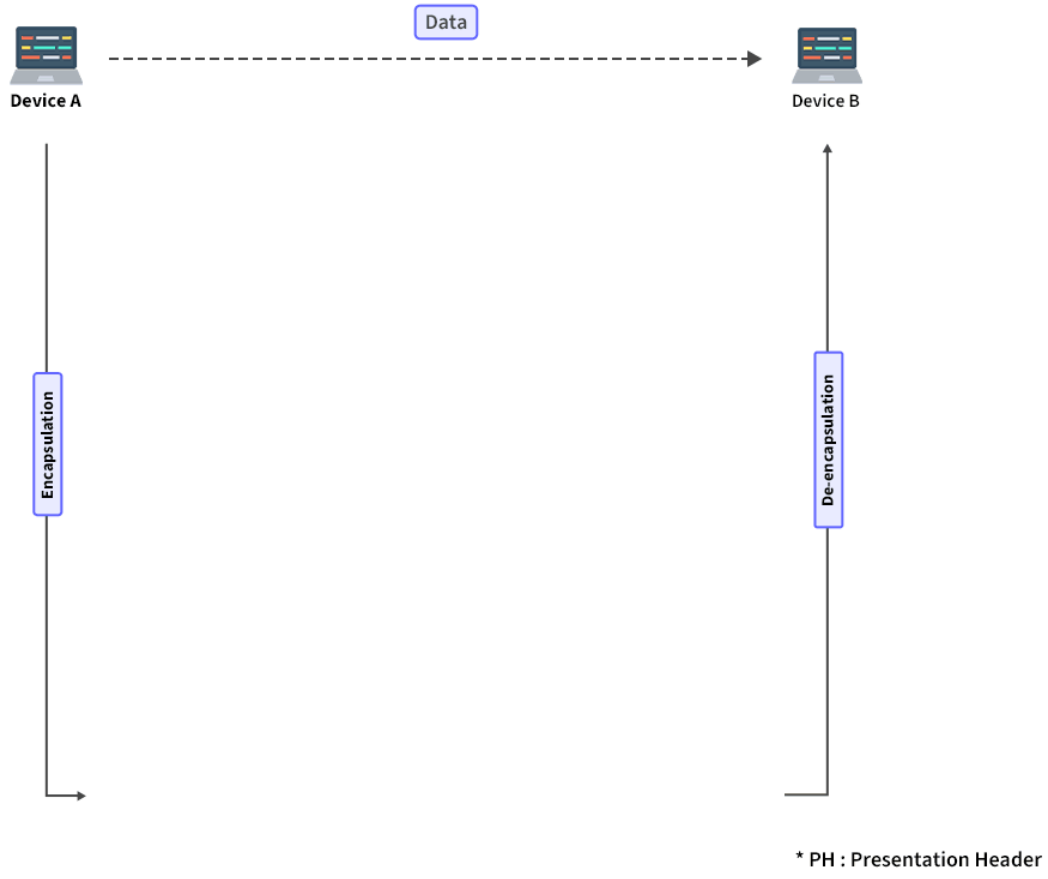
What is OSI Model? – Layers of OSI Model

-

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. 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.

In this article, we will discuss the OSI Model and each layer of the OSI Model in detail. We will also discuss the flow of data in the OSI Model and how the **OSI Model** is different from the **TCP/IP Model.**



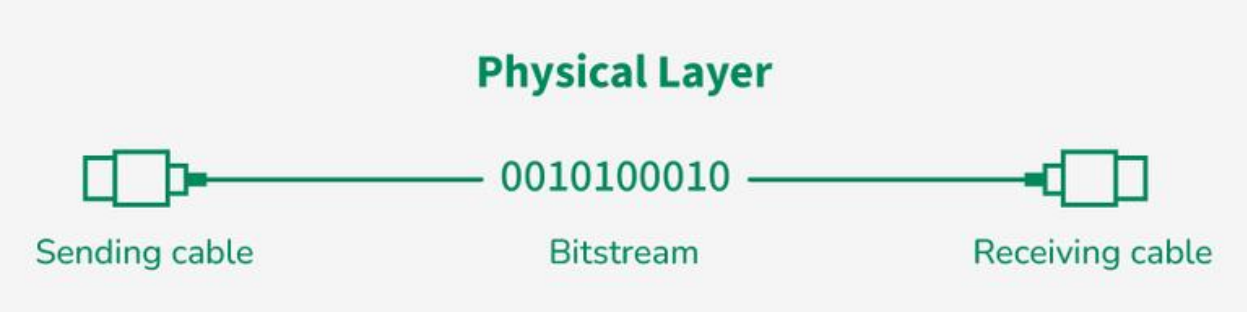
Layers of the OSI Model

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

- Physical Layer
- Data Link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- 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. The physical layer contains information in the form of **bits.** 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.



Physical Layer

Functions of the Physical Layer

- **Bit Synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at the bit level.

- **Bit Rate Control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
- **Physical Topologies:** Physical layer specifies how the different, devices/nodes are arranged in a network i.e. bus topology , star topology , or mesh topology .
- **Transmission Mode:** Physical layer also defines how the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex .

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 MAC address. Packet in the Data Link layer is referred to as **Frame.** Switches and Bridges are common Data Link Layer devices.

The Data Link Layer is divided into two sublayers:

- Logical Link Control (LLC)
- Media Access Control (MAC)

The packet received from the Network layer is further divided into frames depending on the frame size of the **NIC(Network Interface Card)**. DLL also encapsulates Sender and Receiver's MAC address in the header.

The Receiver's MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.

Functions of the Data Link Layer

- **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
- **Physical Addressing:** After creating frames, the Data link layer adds physical addresses (**MAC addresses**) of the sender and/or receiver in the header of each frame.
- **Error Control:** The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.

- **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving an acknowledgment.
- **Access Control:** When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

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. Segment in the Network layer is referred to as **Packet.** Network layer is implemented by networking devices such as routers and switches.

Functions of the Network Layer

- **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
- **Logical Addressing:** To identify each device inter-network uniquely, the network layer defines an addressing scheme. The sender and receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

Layer 4 – Transport Layer

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as **Segments**. 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.

At the sender's side, the transport layer receives the formatted data from the upper layers, performs **Segmentation**, and also implements **Flow and error**

control to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.

- Generally, this destination port number is configured, either by default or manually. For example, when a web application requests a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default ports assigned.

At the Receiver's side, Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

Functions of the Transport Layer

- **Segmentation and Reassembly:** This layer accepts the message from the (session) layer, and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
- **Service Point Addressing:** To deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

Services Provided by Transport Layer

- Connection-Oriented Service
- Connectionless Service

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.

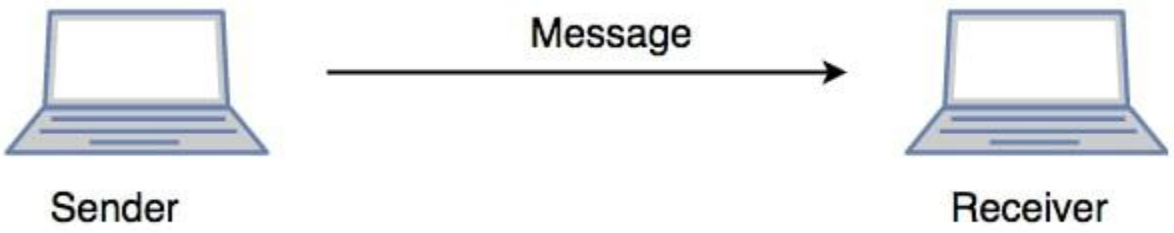
Functions of the Session Layer

- **Session Establishment, Maintenance, and Termination:** The layer allows the two processes to establish, use, and terminate a connection.

- **Synchronization:** This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
- **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

Example

Let us consider a scenario where a user wants to send a message through some Messenger application running in their browser. The "**Messenger**" here acts as the application layer which provides the user with an interface to create the data. This message or so-called **Data** is compressed, optionally encrypted (if the data is sensitive), and converted into bits (0's and 1's) so that it can be transmitted.



Communication in Session Layer

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 JPEG, MPEG, GIF, TLS/SSL, etc.

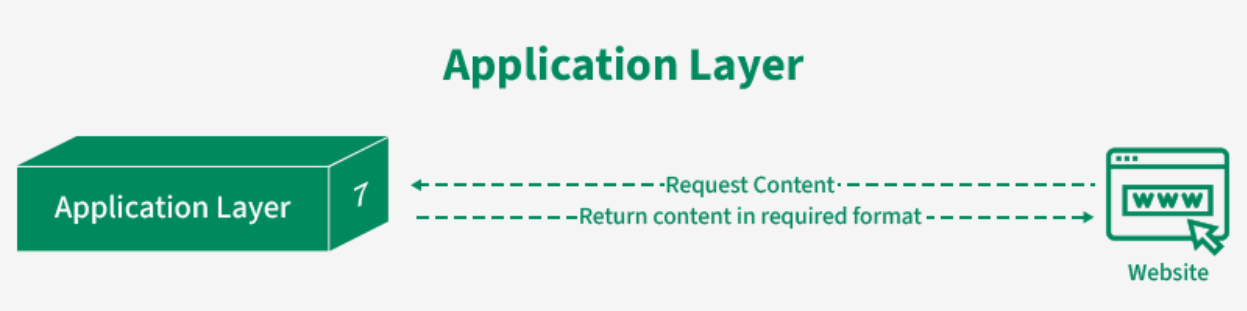
Functions of the Presentation Layer

- **Translation:** For example, ASCII to EBCDIC .
- **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.

- **Compression:** Reduces the number of bits that need to be transmitted on the network.

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.



Application Layer

Functions of the Application Layer

The main functions of the application layer are given below.

- **Network Virtual Terminal(NVT):** It allows a user to log on to a remote host.
- **File Transfer Access and Management(FTAM):** This application allows a user to access files in a remote host, retrieve files in a remote host, and manage or control files from a remote computer.
- **Mail Services:** Provide email service.
- **Directory Services:** This application provides distributed database sources and access for global information about various objects and services.

How Data Flows in the OSI Model?

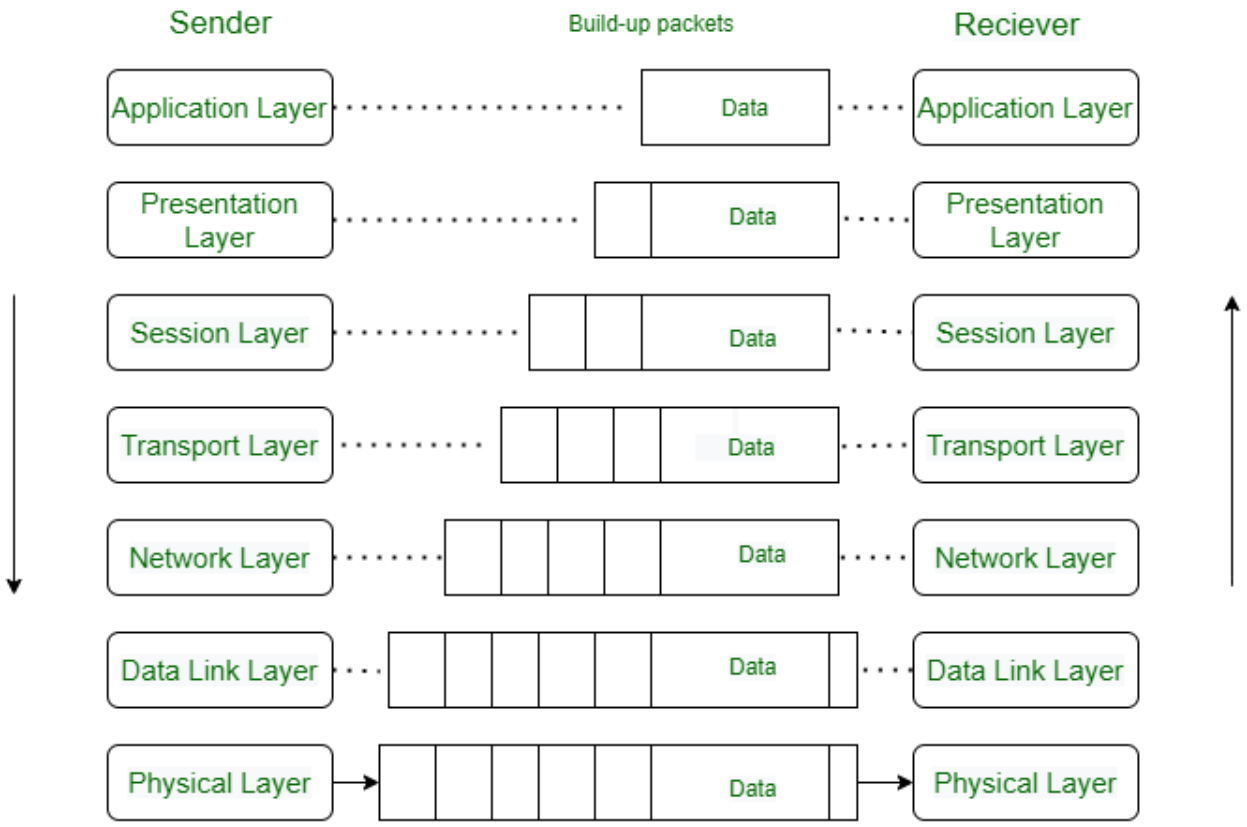
When we transfer information from one device to another, it travels through 7 layers of OSI model. First data travels down through 7 layers from the sender's end and then climbs back 7 layers on the receiver's end.

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.



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.
Protocols Used in the OSI Layers

Layer	Working	Protocol Data Unit	Protocols
1 – Physical Layer	Establishing Physical Connections between Devices.	Bits	USB, SONET/SDH, etc.
2 – Data Link Layer	Node to Node Delivery of Message.	Frames	Ethernet, PPP, etc.
3 – Network Layer	Transmission of data from one host to another, located in different networks.	Packets	IP, ICMP, IGMP, OSPF, etc.

Layer	Working	Protocol Data Unit	Protocols
4 – Transport Layer	Take Service from Network Layer and provide it to the Application Layer.	Segments (for TCP) or Datagrams (for UDP)	TCP, UDP, SCTP, etc.
5 – Session Layer	Establishes Connection, Maintenance, Ensures Authentication and Ensures security.	Data	NetBIOS, RPC, PPTP, etc.
6 – Presentation Layer	Data from the application layer is extracted and manipulated in the required format for transmission.	Data	TLS/SSL, MIME, JPEG, PNG, ASCII, etc.
7 – Application Layer	Helps in identifying the client and synchronizing communication.	Data	FTP, SMTP, DNS, DHCP, etc.

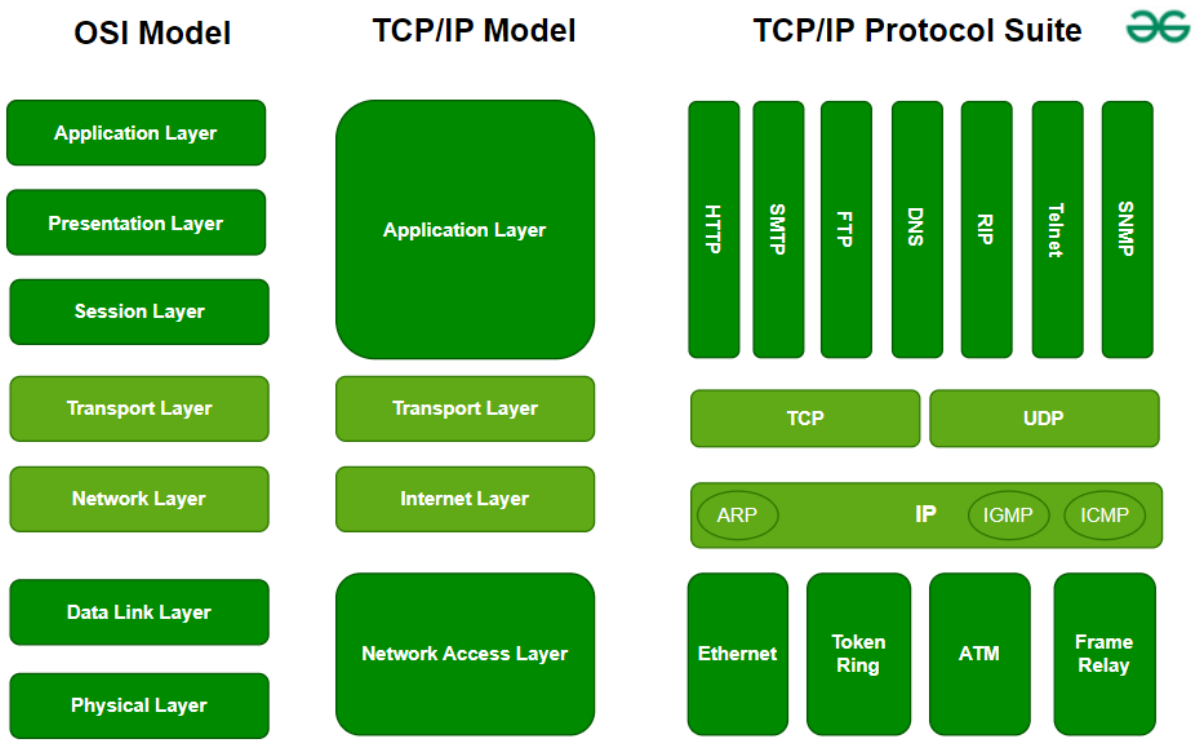
Why Does The OSI Model Matter?

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.

Difference Between OSI and TCP/IP Model

OSI Model	TCP/IP Model
OSI stands for Open Systems Interconnection.	TCP/IP stands for Transmission Control Protocol/Internet Protocol.
OSI model has 7 layers.	TCP/IP model consists of 4 layers.
Package delivery is guaranteed in OSI Model.	Package delivery is not guaranteed in the TCP/IP Model.
In the OSI model, Only layers 1,2 and 3 are necessary for data transmission.	All layers of the TCP/IP model are needed for data transmission.
Protocols at each layer is independent of the other layer.	Layers are integrated, some layers are required by other layers of TCP/IP model.
OSI Model is a conceptual framework, less used in practical applications.	Widely used in actual networks like Internet and Communication Systems.



OSI vs TCP/IP

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.
- The OSI Model is more of a theoretical framework, meaning it's great for understanding concepts but not always practical for implementation.

Conclusion

In conclusion, the OSI (Open Systems Interconnection) model helps us understand how data moves in networks. It consists of seven distinct layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application. Each layer has specific responsibilities and interacts with the layers directly above and below it. Since it is a conceptual model, but the OSI framework is still widely used to troubleshoot and understand networking issues.

what is internet ?

The internet is a vast network of computers and servers that allows people to communicate and share information with each other.

It's like a giant web that connects billions of devices around the world.

Internet as a web

How does it work?

When you want to access something on the internet, like a website or your email, your computer sends a request through a series of cables and routers. These routers act like traffic cops, directing your request to the right destination.

Internet routers

The destination is usually a server, which is a powerful computer that stores information. The server processes your request and sends back the information you need.

Internet server

What can you do with the internet?

The internet has revolutionized the way we live, work, and play. Here are just a few things you can do with it:

- **Communicate with others:** Send emails, chat with friends, and make video calls.
- **Access information:** Research topics, read news articles, and watch videos.
- **Shop online:** Buy products and services from all over the world.
- **Learn new skills:** Take online courses and tutorials.
- **Play games:** Compete with friends or strangers from around the globe.
- **Stay connected:** Follow your favorite celebrities and brands on social media.

People using internet for various activities

The internet is a powerful tool that can be used for good or bad. It's important to be aware of the risks and to use it responsibly.

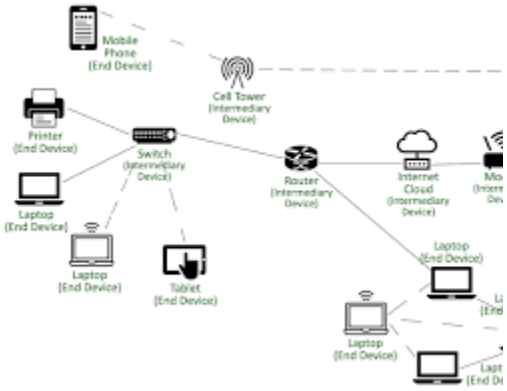
write some network terminologies ?

Network Terminologies Explained with Images

Basic Networking Concepts

1. Node:

- Any device connected to a network.
- Examples: Computers, printers, servers, routers, switches.

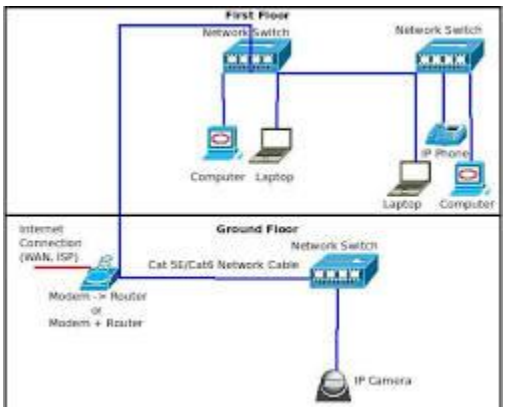


Network Node

2. Link:

- A connection between two nodes.

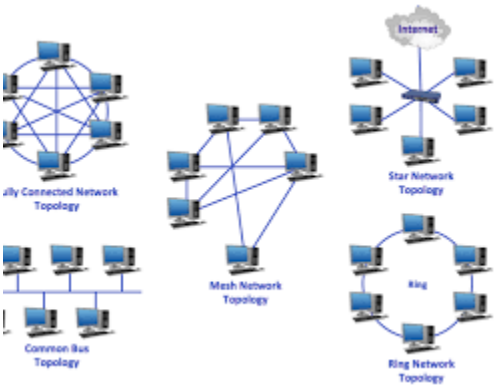
- Can be physical (cables) or wireless.



Network Link

3. Network:

- A collection of interconnected devices that can communicate with each other.
- Examples: LAN, WAN, MAN.



Network Topology

Networking Devices

1. Router:

- Forwards data packets between networks.
- Determines the best path for data transmission.

Router

2. Switch:

- Connects devices within a network.
- Forwards data packets to the intended recipient.

Switch

3. Hub:

- Connects multiple devices in a network.
- Broadcasts data to all connected devices.

Hub

4. Modem:

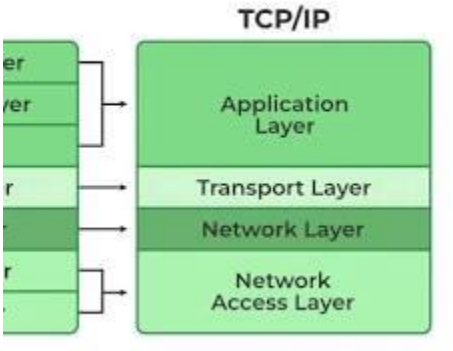
- Modulates and demodulates signals for data transmission over analog lines.
- Used for internet connections.

Modem

Network Protocols

1. TCP/IP:

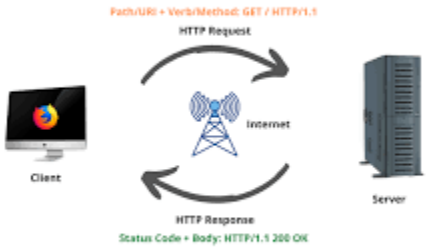
- A suite of protocols used for communication over the internet.
- TCP: Transmission Control Protocol (reliable, connection-oriented)
- IP: Internet Protocol (unreliable, connectionless)



TCP/IP Model

2. HTTP:

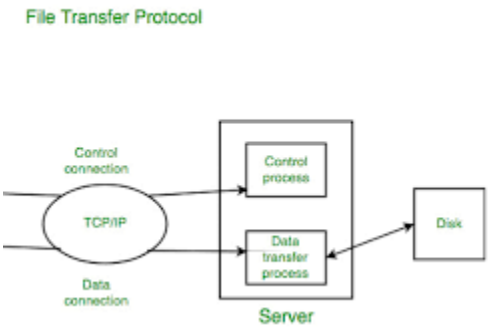
- Hypertext Transfer Protocol
- Used for communication between web browsers and servers.



HTTP RequestResponse Cycle

3. FTP:

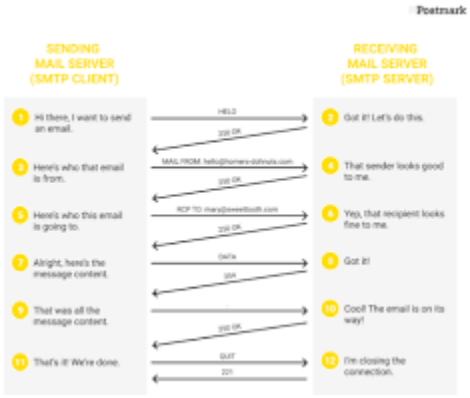
- File Transfer Protocol
- Used for transferring files between computers.



FTP Process

4. SMTP:

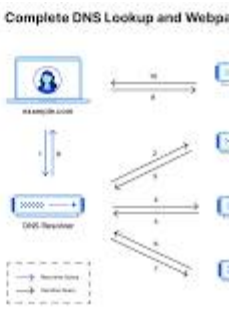
- Simple Mail Transfer Protocol
- Used for sending emails.



SMTP Process

5. DNS:

- Domain Name System
- Translates domain names (e.g., [invalid URL removed]) into IP addresses.

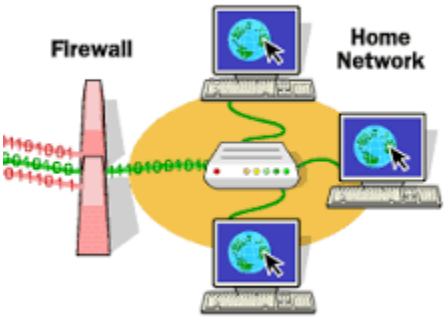


DNS Lookup Process

Network Security Concepts

1. Firewall:

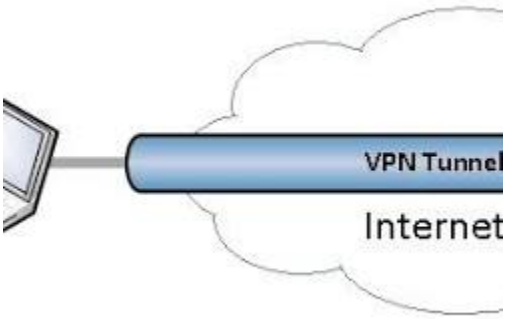
- A security system that monitors and controls incoming and outgoing network traffic.



Firewall

2. VPN:

- Virtual Private Network
- Creates a secure, encrypted connection over a public network.



VPN Tunnel

3. Encryption:

- The process of converting plain text into ciphertext.
- Used to protect sensitive data.

Encryption Process

Note: To visualize these concepts better, you can search for images on Google Images or use online tools like diagrams.net to create your own diagrams.

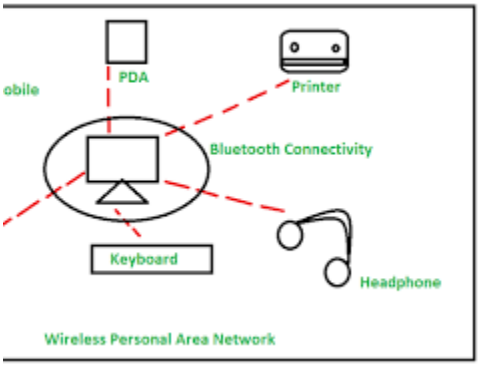
Different types of networks explanation with images

Types of Networks

Networks are classified based on their geographical scope and the devices they connect. Here are the primary types:

1. Personal Area Network (PAN)

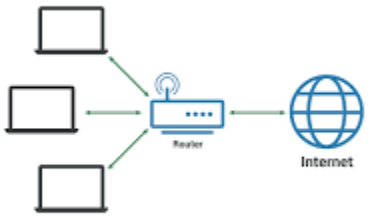
- **Scope:** Smallest type of network, typically within a 10-meter radius.
- **Devices:** Personal devices like smartphones, tablets, laptops, and printers.
- **Connection:** Usually wireless (Bluetooth or Wi-Fi).



Personal Area Network (PAN)

2. Local Area Network (LAN)

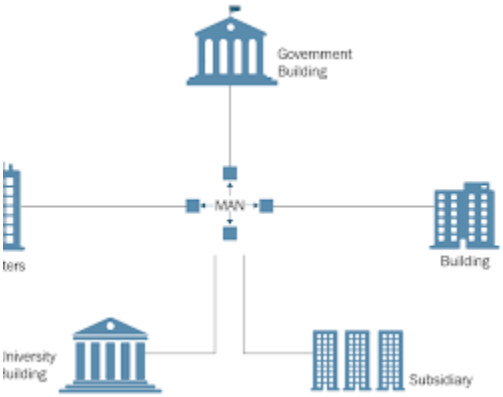
- **Scope:** Covers a small geographical area, such as a home, office, or school building.
- **Devices:** Computers, printers, servers, and other network devices.
- **Connection:** Wired (Ethernet cables) or wireless (Wi-Fi).



Local Area Network (LAN)

3. Metropolitan Area Network (MAN)

- **Scope:** Covers a larger geographical area, such as a city or campus.
- **Devices:** Multiple LANs connected together.
- **Connection:** Leased lines, fiber-optic cables, or wireless technologies.



Metropolitan Area Network (MAN)

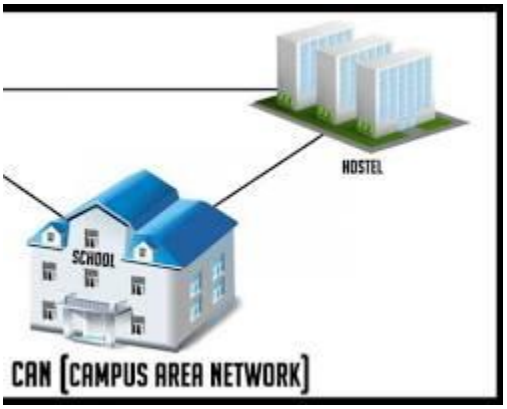
4. Wide Area Network (WAN)

- **Scope:** Covers a large geographical area, such as a country or continent.
- **Devices:** Multiple LANs and MANs connected together.
- **Connection:** Leased lines, satellite links, or the public internet.

Wide Area Network (WAN)

5. Campus Area Network (CAN)

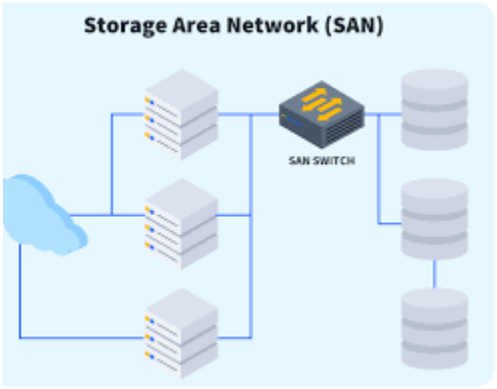
- **Scope:** Covers a specific campus or corporate area.
- **Devices:** Multiple LANs connected together.
- **Connection:** High-speed fiber-optic cables.



Campus Area Network (CAN)

6. Storage Area Network (SAN)

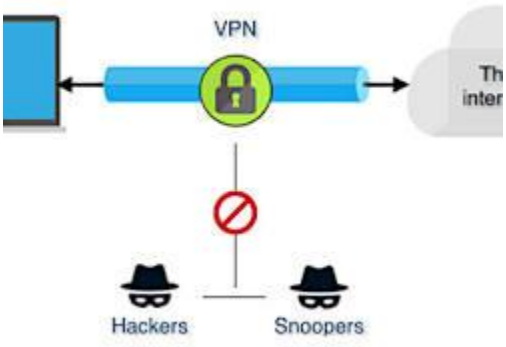
- **Scope:** Dedicated network for storage devices.
- **Devices:** Storage devices like disk arrays and tape libraries.
- **Connection:** High-speed fiber-optic cables.



Storage Area Network (SAN)

7. Virtual Private Network (VPN)

- **Scope:** Creates a secure, private network over a public network (like the internet).
- **Devices:** Computers, servers, and other network devices.
- **Connection:** Encrypted connection.



Virtual Private Network (VPN)

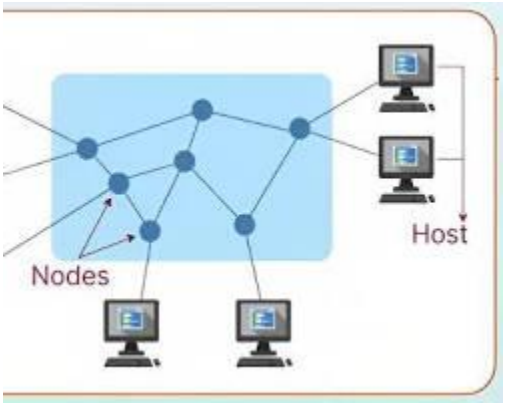
These network types differ in terms of their size, geographic scope, and the technologies used to connect devices. Understanding these distinctions is essential for effective network design and management.

What is a Computer Network?

A computer network is a collection of interconnected devices that can communicate and share resources. These devices can be computers, printers, servers, and more. Networks allow us to share files, send emails, browse the internet, and collaborate with others, regardless of physical location.

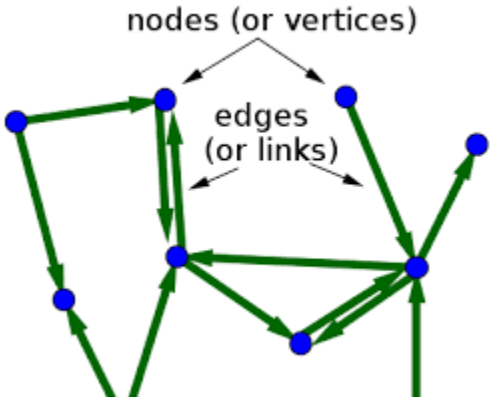
Key Components of a Computer Network:

1. **Nodes:**
   - Individual devices connected to the network.
   - Examples: Computers, servers, printers, smartphones.



network nodes

2. **Links:**
   - The connections between nodes.
   - Can be physical (cables) or wireless (radio waves).



network links

3. **Network Devices:**
   - Devices that facilitate communication between nodes.
   - **Routers:** Direct data packets between networks.

router

- **Switches:** Connect devices within a network.

switch

- **Modems:** Modulate and demodulate signals for data transmission over analog lines.

modem

- **Hubs:** Connect multiple devices in a network.

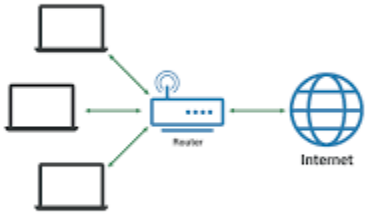
hub

Types of Computer Networks:

1. **Personal Area Network (PAN):**
    - Small network, typically within a 10-meter radius.
    - Connects personal devices like smartphones, tablets, and laptops.

PAN

2. **Local Area Network (LAN):**
    - Covers a small geographic area, like a home, office, or school.
    - Connects devices within a building or campus.

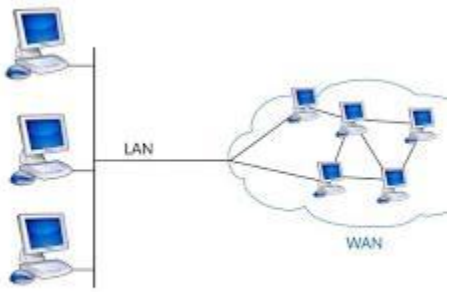


LAN

3. **Metropolitan Area Network (MAN):**
    - Covers a larger area, like a city or campus.
    - Connects multiple LANs.

MAN

4. **Wide Area Network (WAN):**
    - Covers a large geographic area, like a country or continent.
    - Connects multiple LANs and MANs.
    - The internet is a global WAN.



WAN

How Computer Networks Work:

1. **Data Transmission:** Data is broken into packets and sent across the network.
2. **Routing:** Routers determine the best path for data packets to reach their destination.
3. **Transmission Medium:** Data is transmitted through physical media like cables or wireless signals.
4. **Network Protocols:** Protocols like TCP/IP define the rules for communication.

By understanding the basic concepts and components of computer networks, you can appreciate how they have revolutionized the way we live and work.