Computer Networks

Computer Networks Notes

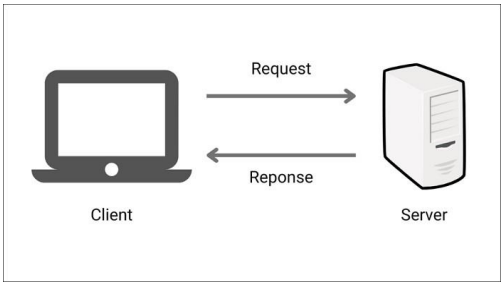
BASICS

1. What is Computer Networking?

Computer networking refers to connected computing devices (such as laptops, desktops, servers, smartphones, and tablets) and an ever-expanding array of IoT devices (such as cameras, door locks, doorbells, refrigerators, audio/visual systems, thermostats, and various sensors) that communicate with one another.

2. Basic terms:

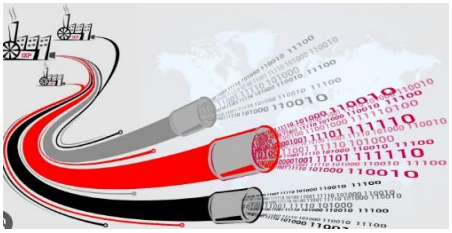
a. **Client**: A client is a computer program or device that requests services or resources from a server. It's usually part of a client-server architecture where the client initiates requests, and the server responds to those requests.



b. **Server**: A server is a computer or system that provides resources, services, or data to other computers, known as clients, over a network. Servers respond to requests from clients and can store and manage data or perform specific tasks.

c. **Peer**: In networking, a peer refers to a computer or device that shares the same level of functionality and responsibility with others. Peers communicate with each other in a peer-to-peer network without a central server.

d. **Host**: A host is any device connected to a network, such as a computer or a server, capable of sending or receiving data. It can be a client, server, or both.



e. **Bandwidth**: Bandwidth refers to the capacity of a communication channel to transmit data. It is often used to describe the data transfer rate of an internet connection and is measured in bits per second (bps) or a similar unit.

f. Throughput : Throughput is the term given to the number of packets that are processed within a specific period of time.

g. **Jitter**: Jitter is the variation in the delay of received data packets in a network. It can lead to inconsistent packet delivery times, which may affect the quality of real-time applications like voice or video.

h. **Packet**: Packets are used at the network layer of the OSI model. A packet is a small unit of data transmitted over a network. It contains both the actual data being sent and the necessary control information, such as source and destination addresses.

i. **Frame**: In networking, a frame is a data transmission unit at the data link layer of the OSI model. A frame is a data transmission unit that includes both the data being sent and the necessary control information for reliable transmission within a local network segment.

j. **Local Host**: Local host typically refers to the computer or device you are currently using. It's often identified by the loopback address (127.0.0.1), allowing a device to communicate with itself.

k. **Bit Rate**: Bit rate is the number of bits processed or transmitted in a unit of time, often measured in bits per second (bps). It represents the speed of data transfer in a network.

l. **Noise**: In the context of networking, noise refers to unwanted electrical or electromagnetic interference that can disrupt the transmission of data signals.

m. **Attenuation**: Attenuation is the reduction in signal strength as it travels through a medium, such as a cable or fiber optic. It can affect the quality and integrity of the transmitted data.

n. **Distortion**: Distortion in networking refers to any alteration or corruption of the signal during transmission, leading to errors in the received data.

3. Difference between Web and Internet?

Internet:

- Definition: The internet is like a giant network that connects millions of smaller networks worldwide.
- Example: Think of the internet as a massive library. Each book in the library is like a website or online service. The library itself is the internet, connecting all these books (websites) together.

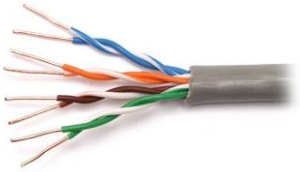
Web:

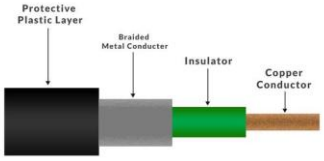
- Definition: The web (or World Wide Web) is a part of the internet where you access information using websites and web browsers.

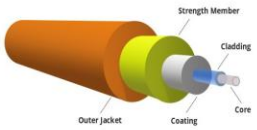
- Example: Imagine a book in the library (internet). When you open the book and read its pages, that's like using a website on the web. The pages of the book are like different web pages you navigate through.

In short, the internet is a vast network, and the web is a way to access information on that network through websites.

4. Types of Transmission Media







Physical Transmission Media:

- Twisted Pair Cable: Copper wires twisted for local networks. Eg: Telephone lines and LANs
- Coaxial Cable: Central conductor for cable connecting TV and broadband.
- Fiber Optic Cable: Glass fibers transmit data using light for high-speed internet and long-distance communication.

Wireless Transmission Media:

- Microwave Transmission: High-frequency radio waves for long-distance.
- Satellite Communication: Orbits relay signals globally. Satellite TV broadcasting signals from a satellite to a home dish.
- Infrared Transmission: Short-range, like TV remote controls.

5. Unicast, BroadCast and Multicast

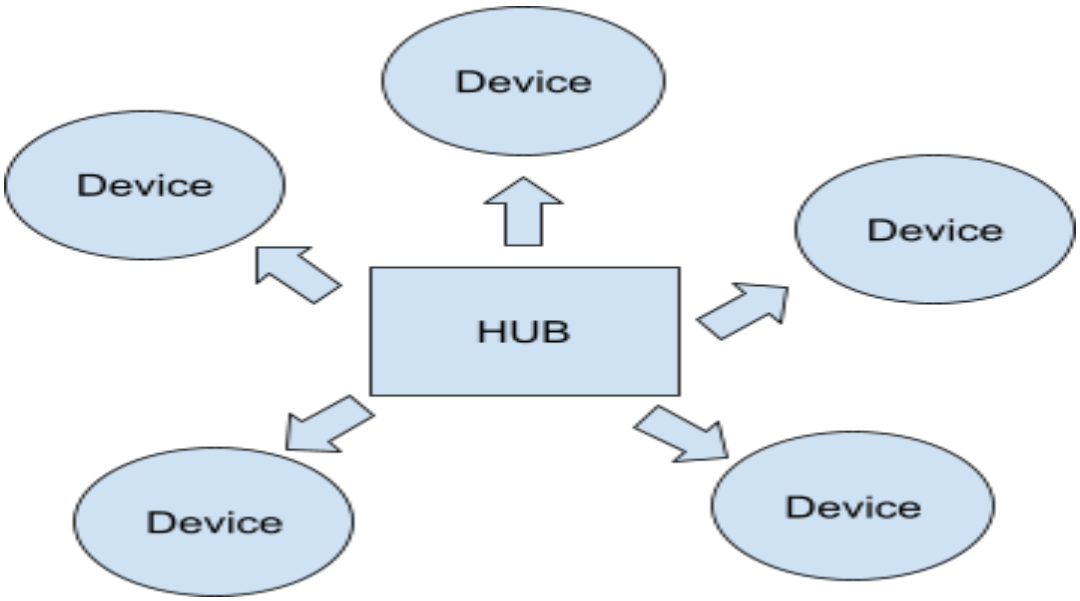
a. **Unicast**: One-to-one communication (e.g., sending an email to a friend).

b. **Broadcast**: One-to-all communication (e.g., TV broadcasting to all TVs in range).
c. **Multicast**: One-to-many communication to specific receivers (e.g., video conference call to a specific group).

6. Computer Network Devices

a. **Repeater:** (Physical Layer)
Signals lose strength as they travel through cables or airwaves. A repeater steps in, amplifies those weakened signals, and sends them on their way with renewed energy.
Eg: Use a Wi-Fi repeater to strengthen the signal in areas where the Wi-Fi from the router is weak or has to travel a long distance.

b. **Hub:** (Physical layer)
Connects multiple devices in a network. It broadcasts data to all connected devices, making it less efficient than a switch.



c. **Switch**: (Data Link Layer)
Connects devices within the same network. It intelligently forwards data only to the intended recipient, improving network efficiency.
d. **Bridge**: (Data Link Layer)
Connects and filters traffic between two different LANs.

e. **Routers**: (Network Layer)
Connects different networks at the network layer, directing data

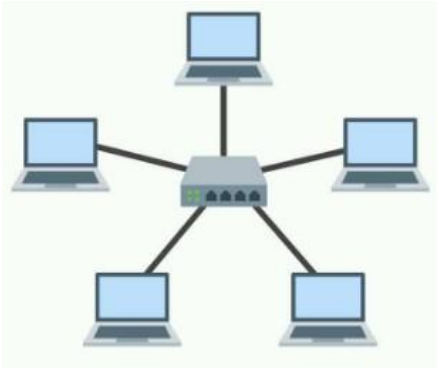
between them based on IP addresses. It makes decisions based on logical addressing.

Example: Home router connecting devices to the internet.

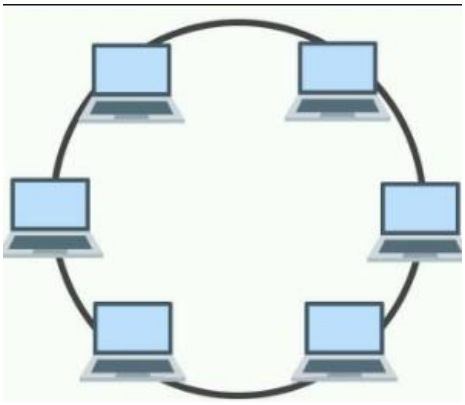
- **Network** : A network is a set of devices that are connected with a physical media link. In a network, two or more nodes are connected by a physical link or two or more networks are connected by one or more nodes. A network is a collection of devices connected to each other to allow the sharing of data.

- **Network Topology** : Network topology specifies the layout of a computer network. It shows how devices and cables are connected to each other.

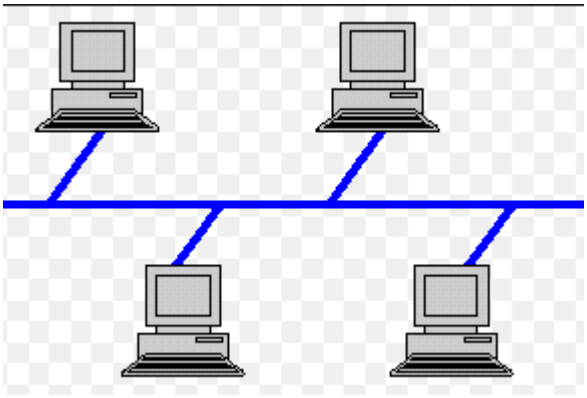
  Types of Network Topology :
  - **Star :**
    - Star topology is a network topology in which all the nodes are connected to a single device known as a central device.
    - Star topology requires more cable compared to other topologies. Therefore, it is more robust as a failure in one cable will only disconnect a specific computer connected to this cable.
    - If the central device is damaged, then the whole network fails.
    - Star topology is very easy to install, manage and troubleshoot. It is commonly used in office and home networks.



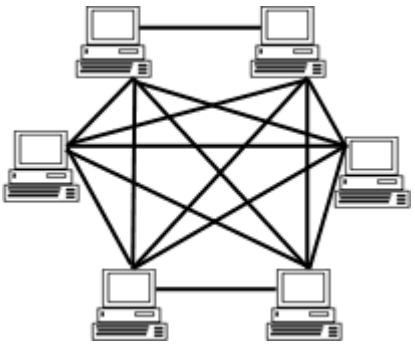
- **Ring** :
  1. Ring topology is a network topology in which nodes are exactly connected to two or more nodes and thus, forming a single continuous path for the transmission.
  2. It does not need any central server to control the connectivity among the nodes.
  3. If the single node is damaged, then the whole network fails.
  4. Ring topology is very rarely used as it is expensive, difficult to install and manage.
  5. Examples of Ring topology are SONET network, SDH network, etc.



- **Bus :**
    1. Bus topology is a network topology in which all the nodes are connected to a single cable known as a central cable or bus.
    2. It acts as a shared communication medium, i.e., if any device wants to send the data to other devices, then it will send the data over the bus which in turn sends the data to all the attached devices.
    3. Bus topology is useful for a small number of devices.
    4. As if the bus is damaged then the whole network fails.



- **Mesh** :
    1. Mesh topology is a network topology in which all the nodes are individually connected to other nodes.
    2. It does not need any central switch or hub to control the connectivity among the nodes.
    3. **Mesh topology is categorized into two parts**: Fully connected mesh topology: In this topology, all the nodes are connected to each other. Partially connected mesh topology: In this topology, all the nodes are not connected to each other.
    4. It is robust as a failure in one cable will only disconnect the specified computer connected to this cable.
    5. Mesh topology is rarely used as installation and configuration are difficult when connectivity gets more.
    6. Cabling cost is high as it requires bulk wiring.



- **Tree** :
    1. Tree topology is a combination of star and bus topology. It is also known as the expanded star topology.
    2. In tree topology, all the star networks are connected to a single bus.
    3. Ethernet protocol is used in this topology.
    4. In this, the whole network is divided into segments known as star networks which can be easily maintained. If one segment is damaged, there is no effect on other segments.
    5. Tree topology depends on the "main bus," and if it breaks, then the whole network gets damaged.

    Example: Large organizational networks, where individual departments have their own star topology, connected to a central bus serving the entire organization.

- **Hybrid** :
    1. A hybrid topology is a combination of different topologies to form a resulting topology.
    2. If star topology is connected with another star topology, then it remains a star topology. If star topology is connected with different topology, then it becomes a Hybrid topology.
    3. It provides flexibility as it can be implemented in a different network environment.

- **<u>Different Types of Networks</u>** : (Imp) - Networks can be divided on the basis of area of distribution. For example:

- **PAN (Personal Area Network)**: Its range limit is up to 10 meters. It is created for personal use. Generally, personal devices are connected to this network. For example computers, telephones, fax, printers, etc.
- **LAN (Local Area Network)**: It is used for a small geographical location like office, hospital, school, etc.
- **HAN (House Area Network)**: It is actually a LAN that is used within a house and used to connect homely devices like personal computers, phones, printers, etc.
- **CAN (Campus Area Network)**: It is a connection of devices within a campus area which links to other departments of the organization within the same campus.
- **MAN (Metropolitan Area Network)**: It is used to connect the devices which span to large cities like metropolitan cities over a wide geographical area.
- **WAN (Wide Area Network)**: It is used over a wide geographical location that may range to connect cities and countries.
- **GAN (Global Area Network)**: It uses satellites to connect devices over the global area.

- **VPN (Virtual Private Network)** : VPN or the Virtual Private Network is a private WAN (Wide Area Network) built on the internet. It allows the creation of a secured tunnel (protected network) between different networks using the internet (public network). By using the VPN, a client can connect to the organization's network remotely.
- **Advantages of VPN** :
    1. VPN is used to connect offices in different geographical locations remotely and is cheaper when compared to WAN connections.
    2. VPN is used for secure transactions and confidential data transfer between multiple offices located in different geographical locations.
    3. VPN keeps an organization's information secured against any potential threats or intrusions by using virtualization.
    4. VPN encrypts the internet traffic and disguises the online identity.
- **Types of VPN** :

- **Access VPN:** Access VPN is used to provide connectivity to remote mobile users and telecommuters. It serves as an alternative to dial-up connections or ISDN (Integrated Services Digital Network) connections. It is a low-cost solution and provides a wide range of connectivity.
- **Site-to-Site VPN:** A Site-to-Site or Router-to-Router VPN is commonly used in large companies having branches in different locations to connect the network of one office to another in different locations. There are 2 sub-categories as mentioned below:
- **Intranet VPN:** Intranet VPN is useful for connecting remote offices in different geographical locations using shared infrastructure (internet connectivity and servers) with the same accessibility policies as a private WAN (wide area network).
- **Extranet VPN:** Extranet VPN uses shared infrastructure over an intranet, suppliers, customers, partners, and other entities and connects them using dedicated connections.

- **IPv4 Address** : An IP address is a 32-bit dynamic address of a node in the network. An IPv4 address has 4 octets of 8-bit each with each number with a value up to 255. IPv4 classes are differentiated based on the number of hosts it supports on the network. There are five types of IPv4 classes and are based on the first octet of IP addresses which are classified as Class A, B, C, D, or E.

IPv4 Class	IPv4 Start Address	IPv4 End Address	Usage
A	0.0.0.0	127.255.255.255	Used for Large Network
B	128.0.0.0	191.255.255.255	Used for Medium Size Network
C	192.0.0.0	223.255.255.255	Used for Local Area Network
D	224.0.0.0	239.255.255.255	Reserved for Multicasting
E	240.0.0.0	255.255.255.254	Study and R&D

- **IPv6 Address:**

  -An **IPv6 address** is a **128-bit dynamic address** used to identify a node in the network. Unlike IPv4, which uses 4 octets, **IPv6 uses 8 groups (or blocks)** of 4 hexadecimal digits, separated by colons (:). Each group represents **16 bits**, making up the total of **128 bits**.

  IPv6 is designed to overcome the **address limitations of IPv4** and provides **an almost unlimited number of unique addresses**, suitable for the growing number of internet-connected devices, including IoT.

  ☑ **IPv6 Address Format:**

  -Written as: 2001:0db8:0000:0000:0000:ff00:0042:8329

  -Can be compressed as: 2001:db8::ff00:42:8329

  -Each section is 16 bits (4 hex digits), total 8 sections → 8 × 16 = 128 bits

---

☑ **Key Characteristics of IPv6:**

Property	Description
Bit Size	128-bit address
Representation	Hexadecimal, colon-separated
Example	2001:db8::1
Total Addresses	2^{128} ≈ 340 undecillion
Broadcasting	Not supported (uses multicast/anycast instead)
Security	Built-in support for IPSec
Configuration	Supports auto-configuration (SLAAC) and DHCPv6
Fragmentation	Performed only by the sender, not routers
Routing	More efficient than IPv4
NAT	Not required (sufficient addresses available)

☑ **IPv6 Address Types (like IPv4 classes):**

- While IPv6 doesn't use classes like IPv4 (Class A, B, C...), it supports **address types** for different use cases:

Address Type	Purpose
Unicast	One-to-one communication (specific device)
Multicast	One-to-many communication
Anycast	One-to-nearest (best route) communication
Broadcast	❌ Not available in IPv6

☑ **IPv6 Prefixes (instead of classes):**

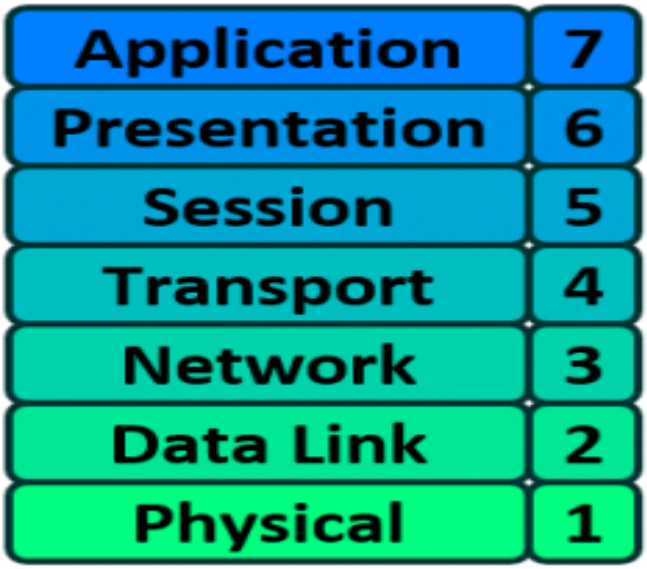
- IPv6 uses **prefixes** to indicate the **network portion** (similar to subnetting in IPv4):

Common Prefix	Type	Example Use
::/0	Default route	All IPv6 addresses
::1/128	Loopback address	Local host (like 127.0.0.1 in IPv4)
FE80::/10	Link-local addresses	Used in local network only
2000::/3	Global unicast	Routable addresses
FF00::/8	Multicast	Group communication

☑ **Summary Comparison: IPv4 vs IPv6**

Feature	IPv4	IPv6
Address Length	32 bits	128 bits
Address Format	Decimal (e.g. 192.168.0.1)	Hexadecimal (e.g. 2001::1)
Address Classes	A, B, C, D, E	No classes (uses address types)
NAT Required	Yes	No
Broadcast	Yes	No (uses multicast)
Security	Optional	Mandatory (IPSec)

- **OSI (Open System Interconnections)** (Imp) : It is a network architecture model based on the ISO standards. It is called the OSI model as it deals with connecting the systems that are open for communication with other systems. **The OSI model has seven layers.** The principles used to arrive at the seven layers can be summarized briefly as below:
    1. Create a new layer if a different abstraction is needed.
    2. Each layer should have a well-defined function.
    3. The function of each layer is chosen based on internationally standardized protocols.
- **Seven Layers** :

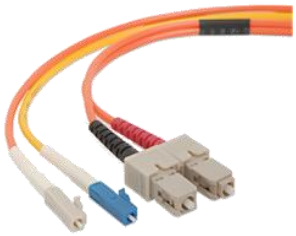


---

1. **Physical Layer**
    - It is the lowest layer of the OSI reference model.
    - It is used for the transmission of an unstructured raw bit stream over a physical medium.
    - Physical layer transmits the data either in the form of electrical/optical or mechanical form.
    - The physical layer is mainly used for the physical connection between the devices, and such physical connection can be made by using twisted-pair cable, fibre-optic or wireless transmission media.

    The Physical layer of the OSI model is responsible for the transfer of bits the 1's and 0'which make up all computer code. It encompasses the physical medium, like Ethernet cables or Serial Cables. Despite its name, it includes wireless technologies like WiFi.
    Simply put, Layer fi is anything that carries fi's and 0's between two nodes. Ethernet uses electric pulses, WiFi uses radio waves, and Fiber uses light pulses. Repeaters and Hubs also function at this layer.



2. DataLink Layer:

   Layer 2 is responsible for putting 1's and 0's on the wire, and pulling 1's and 0's from the wire.

The Network Interface Card (NIC) that you plug your Ethernet wire into handles the Layer 2 functionality. It receives signals from the wire, and transmits signals on to the wire.

Layer 2 will then group together those fi's and 0's into chunks known as Frames.

There is an addressing system that exists at Layer 2 known as the Media Access Control address, or MAC address. **The MAC address uniquely identifies each individual NIC**.

A **Switch** also operates at this layer. **The role of Layer 2 is to deliver packets from *hop to hop***.

- It is used for transferring the data from one node to another node.
- It receives the data from the network layer and converts the data into data frames and then attaches the physical address to these frames which are sent to the physical layer.
- It enables the error-free transfer of data from one node to another node.

Functions of Data-link layer:

- **Frame synchronization**: Data-link layer converts the data into frames, and it ensures that the destination must recognize the starting and ending of each frame.
- **Flow control**: Data-link layer controls the data flow within the network.

- **Error control**: It detects and corrects the error occurred during the transmission from source to destination.
- **Addressing**: Data-link layers attach the physical address with the data frames so that the individual machines can be easily identified.
- **Link management**: Data-link layer manages the initiation, maintenance and termination of the link between the source and destination for the effective exchange of data.

3. *Network Layer: The Network layer of the OSI model is responsible for packet delivery from end to end.*

   The Internet achieves this by employing another addressing scheme— the Internet Protocol address, commonly known as the IP Address. This system provides a logical identification for each node connected to the Internet.

   Routers operate at this layer.

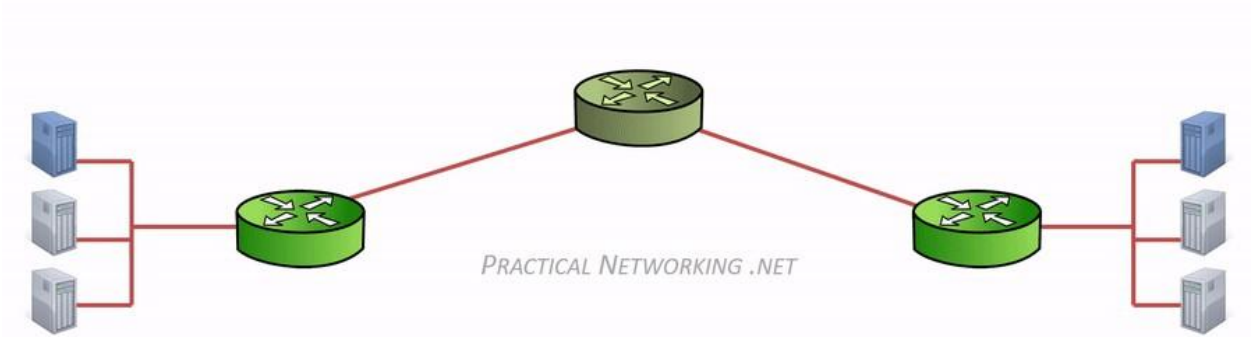
Q. If we already have a unique L2 addressing scheme on every NIC (like MAC addresses), why do we need yet another addressing scheme at L3 (like IP addresses)? Or vice versa?

- **Layer 2** uses **MAC addresses** and is responsible for packet delivery from **hop to hop**.
- **Layer 3** uses **IP addresses** and is responsible for packet delivery from *end to end.*

When a computer has data to send, it encapsulates it in an IP header which will include information like the Source and Destination IP addresses of the two “ends” of the communication.

The IP Header and Data are then further encapsulated in a MAC address header, which will include information like the Source and Destination MAC address of the current “hop” in the path towards the final destination.

Here is an illustration to drive this point home:



Notice between each Router, the MAC address header is stripped and regenerated to get it to the next hop. The IP header generated by the first computer is only stripped off by the final computer, hence the IP header handled the “end to end” delivery, and each of the four *different* MAC headers involved in this animation handled the “hop to hop” delivery.

Think of your home network as a neighborhood, and each device in your home (like your computer, phone, or smart TV) as a house in that neighborhood. In this analogy, MAC addresses are like unique house numbers. They help devices on the same street communicate with each other efficiently. For instance, if your computer wants to send a message to your printer, it can use the MAC address to find it quickly within the local network (neighborhood).

Now, let's extend the analogy to the broader internet. Imagine your neighborhood is just one of many in a city, and each city is a part of a vast country. If you want to send a letter to a friend in a different city or

country, you wouldn't just use your house number; you'd need a more comprehensive address, including the city, state, and country. This is where IP addresses come in.

- Network layer converts the logical address into the physical address.
- The routing concept means it determines the best route for the packet to travel from source to the destination.

  Functions of network layer :

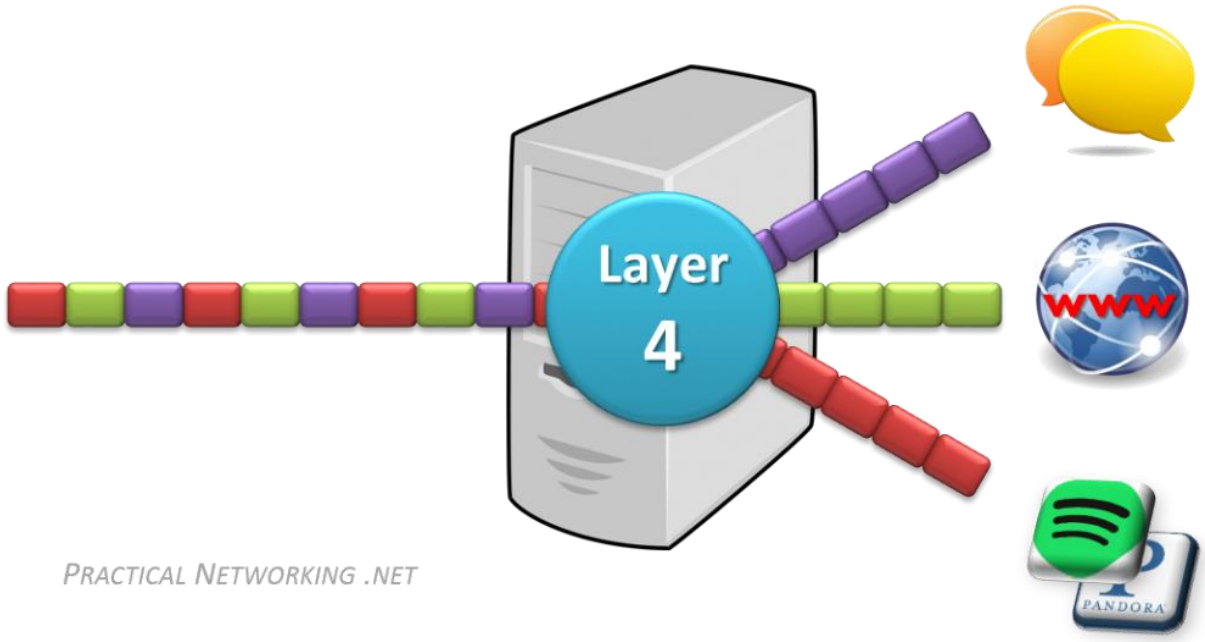
- **Routing**: The network layer determines the best route from source to destination. This function is known as routing.
- **Logical addressing**: The network layer defines the addressing scheme to identify each device uniquely.
- **Packetizing**: The network layer receives the data from the upper layer and converts the data into packets. This process is known as packetizing.
- **Internetworking**: The network layer provides the logical connection between the different types of networks for forming a bigger network.
- **Fragmentation**: It is a process of dividing the packets into fragments..

4. Transport Layer

- It delivers the message through the network and provides error checking so that no error occurs during the transfer of data.
- **It provides two kinds of services**:
  - **Connection-oriented transmission**: In this transmission, the receiver sends the acknowledgement to the sender after the packet has been received.

- **Connectionless transmission**: In this transmission, the receiver does not send the acknowledgement to the sender.

At any given time on a user's computer there might be an Internet browser open, while music is being streamed, while a messenger or chat app is running. Each of these applications are sending and receiving data from the Internet, and all that data is arriving in the form of 1's and 0's on to that computer's NIC. Something has to exist in order to distinguish which 1's and 0's belong to the messenger or the browser or the streaming music. That "something" is Layer 4:



Layer 4 accomplishes this by using an addressing scheme known as Port Numbers.

Specifically, two methods of distinguishing network streams exist. They are known as the Transmission Control Protocol (TCP), or the User Datagram Protocol (UDP).

5. Session Layer

- The main responsibility of the session layer is beginning, maintaining and ending the communication between the devices.
- Session layer also reports the error coming from the upper layers.
- Session layer establishes and maintains the session between the two users.

6. Presentation Layer

- The presentation layer is also known as a Translation layer as it translates the data from one format to another format.
- At the sender side, this layer translates the data format used by the application layer to the common format and at the receiver side, this layer translates the common format into a format used by the application layer.

  Functions of presentation layer:
  - Character code translation
  - Data conversion
  - Data compression
  - Data encryption

7. Application Layer

- Application layer enables the user to access the network.
- It is the topmost layer of the OSI reference model.
- Application layer protocols are file transfer protocol (FTP), simple mail transfer protocol (SMTP), domain name system, etc.
- The most widely used application protocol is HTTP (Hypertext transfer protocol). A user sends the request for the web page using HTTP.

  Example: Facebook, Youtube, Gmail etc.

- **TCP/IP Reference Model** : It is a compressed version of the OSI model with only **4 layers**. It was developed by the US Department of Defence (DoD) in the 1860s. The name of this model is based on 2 standard protocols used i.e. TCP (Transmission Control Protocol) and IP (Internet Protocol).
    1. **Link** : Decides which links such as serial lines or classic Ethernet must be used to meet the needs of the connectionless internet layer. Ex - Sonet, Ethernet
    2. **Internet** : The internet layer is the most important layer which holds the whole architecture together. It delivers the IP packets where they are supposed to be delivered. Ex - IP, ICMP.
    3. **Transport** : Its functionality is almost the same as the OSI transport layer. It enables peer entities on the network to carry on a conversation. Ex - TCP, UDP (User Datagram Protocol)
    4. **Application** : It contains all the higher-level protocols. Ex - HTTP, SMTP, RTP, DNS.

- **HTTP and HTTPS** :

HTTP is the HyperText Transfer Protocol which defines the set of rules and standards on how the information can be transmitted on the World Wide Web (WWW). It helps the web browsers and web servers for communication. It is a 'stateless protocol' where each command is independent with respect to the previous command. **HTTP is an application layer protocol built upon the TCP. It uses port 80 by default.**

i. **Definition**: HTTP is the foundation of data communication on the World Wide Web. It is an application layer protocol that enables the transfer of hypertext, which are text-based documents containing hyperlinks and multimedia content. Get, post, put and delete are some types of requests.

ii. **Example**: When you enter a URL in your browser, it typically uses HTTP to request the web page from the server. However, data transferred using HTTP is not encrypted,

making it susceptible to interception and tampering.

i. **HTTPS is the HyperText Transfer Protocol Secure or Secure HTTP.** It is an advanced and secured version of HTTP. On top of HTTP, SSL/TLS protocol is used to provide security. **It enables secure transactions by encrypting the communication and also helps identify network servers securely. It uses port 443 by default.**
Example: When you visit a website with an "https://" URL, such as "https://www.example.com," the communication between your browser and the server is encrypted, making it more difficult for third parties to intercept or manipulate the data.

- **DNS (Imp)** :
    1. DNS is an acronym that stands for Domain Name System.DNS was introduced by Paul Mockapetris and Jon Postel in 1983.
    2. It is a naming system for all the resources over the internet which includes physical nodes and applications. It is used to locate resources easily over a network.
    3. DNS is an internet which maps the domain names to their associated IP addresses.

4. Without DNS, users must know the IP address of the web page that you wanted to access.

- **Working of DNS** (**Imp**)**:** If you want to visit the website of "shaurya", then the user will type "https://www.shaurya.com" into the address bar of the web browser. Once the domain name is entered, then the domain name system will translate the domain name into the IP address which can be easily interpreted by the computer. Using the IP address, the computer can locate the web page requested by the user.

- **DNS Forwarder** : A forwarder is used with a DNS server when it receives DNS queries that cannot be resolved quickly. So it forwards those requests to external DNS servers for resolution. A DNS server which is configured as a forwarder will behave differently than the DNS server which is not configured as a forwarder.

- **SMTP Protocol** : SMTP is the **Simple Mail Transfer Protocol**. SMTP sets the rule for communication between servers. This set of rules helps the software to transmit emails over the internet. It supports both End-to-End and Store-and-Forward methods. It is in always-listening mode on port 25.

Q. How a packet travels(V.V.V Important)

1. Key Players
2. Host to Host Communication
3. Host to Host through a Switch
4. Host to Host through a Router
5. Final Video

2. Common Networking commands

a. **ping**: Tests the reachability of a host on a network using Internet Control Message Protocol (ICMP) echo requests.

b. **netstat**: Displays information about network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.

c. **tracert (traceroute on Unix-like systems)**: Traces the route that packets take to reach a destination, showing the IP addresses of routers in the path.

d. **ipconfig (Windows) / ifconfig (Unix-like systems)**: Displays the configuration of network interfaces on a system, including IP addresses, subnet masks, and gateway addresses.

e. **nslookup**: Allows you to query Domain Name System (DNS) servers to obtain domain name or IP address information.

f. **route**: Displays and manipulates the IP routing table, showing the routing information used by the system.

g. **pathping**: Combines features of ping and tracert, providing information on packet loss at each hop along the route.

h. **netDiag (Windows)**: A network diagnostic tool that can be used to troubleshoot various network issues.

i. **hostname**: Displays the name of the current host or sets the host name.

j. **arp**: Displays and modifies the ARP (Address Resolution Protocol) cache, which maps IP addresses to MAC addresses on a local network.

3. What is an API?

An API, or Application Programming Interface, is a set of rules and protocols that allows one piece of software or application to interact with another. It defines the methods and data formats that applications can use to request and exchange information.

In a hotel setting, envision a scenario where you place an order with a servant, who then communicates the order to the kitchen. Subsequently, the servant returns with the prepared food to serve the customer. Here the servant acts like an API.

Eg. Google maps API, Weather API, News API.

4. What is SSL (Secure Socket Layer)/TLS (Transport Layer Security)?

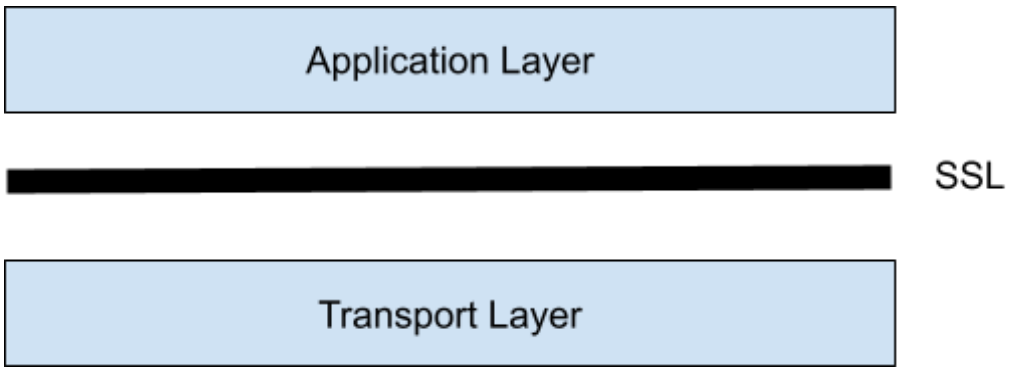
To provide security between client and server while transferring data we use SSL.

It mainly has 3 important features:

a. **Integrity**: The message should be sent without tampering to the client.

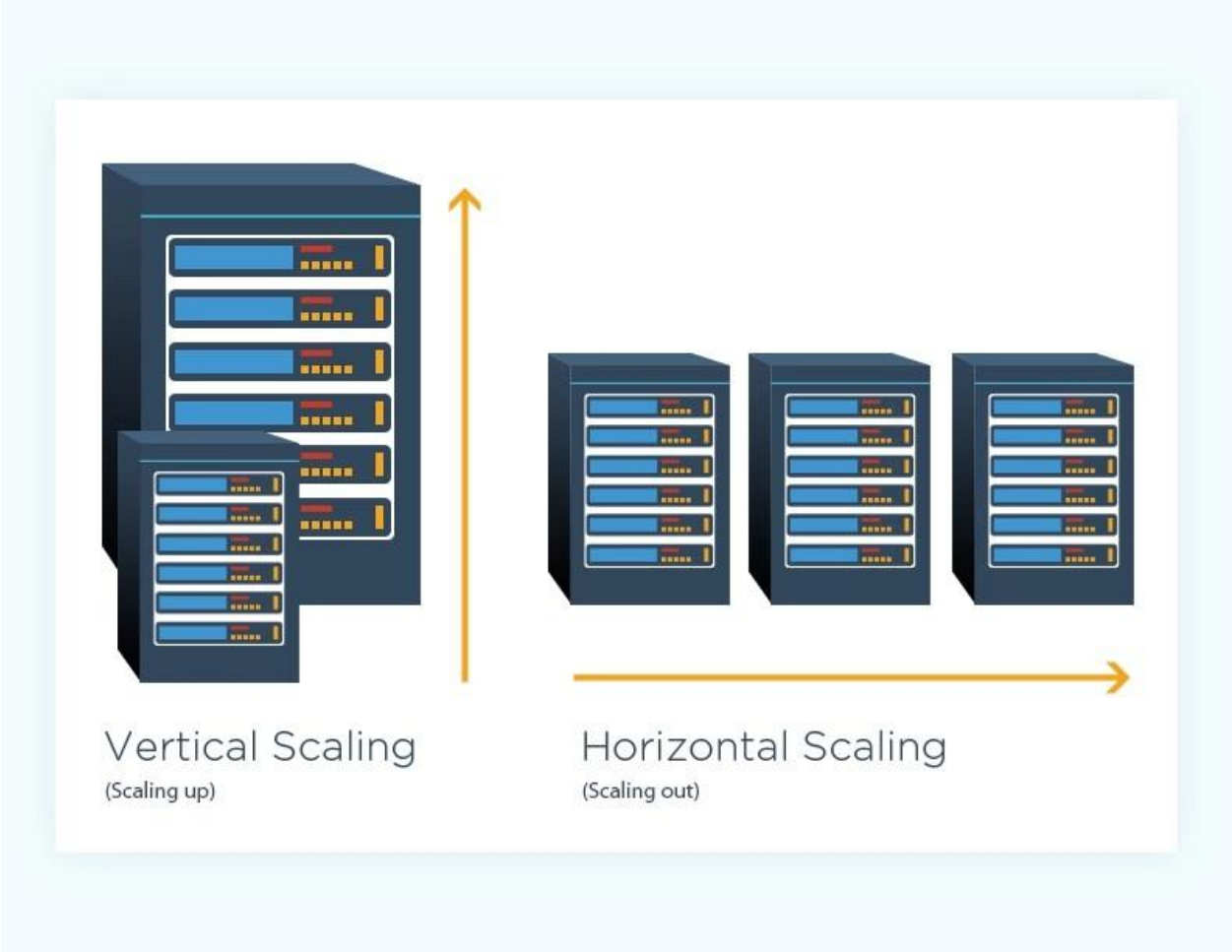
b. Authentication/Authorization

c. **Confidentiality**: Encrypting the data before transferring.



5. Horizontal Vs Vertical Scaling

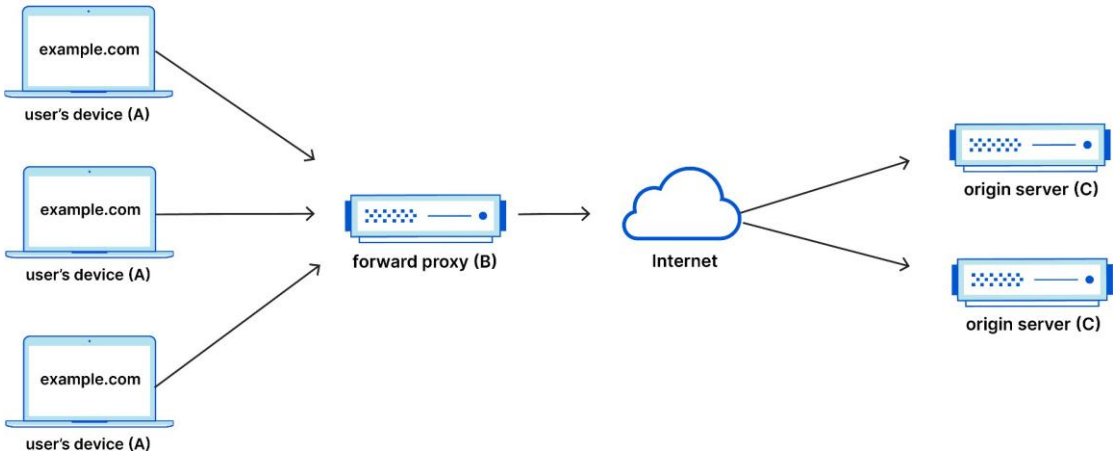
Horizontal scaling, also known as scaling out, involves adding more machines or nodes to your system. This approach distributes the workload across multiple machines. **Vertical scaling**, on the other hand, also called scaling up, means increasing the power of a single machine by adding more resources like CPU, RAM, or storage. Horizontal scaling is typically more cost-effective and provides better fault tolerance, while vertical scaling may have limitations and can be more expensive as you reach the upper bounds of a single machine's capacity.



6. Forward Proxy and Reverse Proxy

a. **Forward Proxy**: (On Client Side)
   - Protects the client's online identity
   - To avoid state or institutional browsing restrictions
   - To block access to certain content (School network might be configured to connect to the web through a proxy with certain rules)

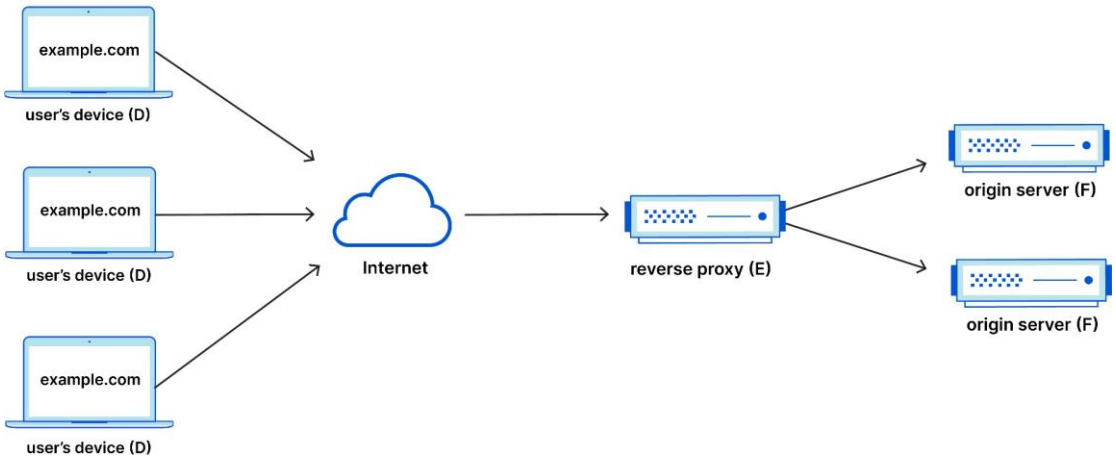
Forward Proxy Flow



b. **Reverse Proxy**: (On Server side)

- Load Balancing
- Protection from attacks to a server
- Caching

Reverse Proxy Flow



- **<u>Difference Between TCP (Transmission Control Protocol) and UDP (User Datagram Protocol)</u>**:
    1. **TCP** is a connection-oriented protocol, whereas **UDP** is a connectionless protocol. A key **difference between TCP and UDP** is speed, as **TCP** is comparatively slower than **UDP**. Overall, **UDP** is a much faster, simpler, and efficient protocol, however, retransmission of lost data packets is only possible with **TCP**

2. TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data. UDP has only the basic error checking mechanism using checksums.

Important Protocols

A protocol is a set of rules which is used to govern all the aspects of information communication.The main elements of a protocol are:

- **Syntax**: It specifies the structure or format of the data. It also specifies the order in which they are presented.
- **Semantics**: It specifies the meaning of each section of bits.
- **Timing**: Timing specifies two characteristics: When data should be sent and how fast it can be sent.

- **DHCP**: DHCP is the **Dynamic Host Configuration Protocol**. It is an application layer protocol used to auto-configure devices on IP networks enabling them to use the TCP and UDP-based protocols. The DHCP servers auto-assign the IPs and other network configurations to the devices individually which enables them to communicate over the IP network. It helps to get the subnet mask, IP address and helps to resolve the DNS. It uses port 67 by default.
- **FTP** : FTP is a **File Transfer Protocol.** It is an application layer protocol used to transfer files and data reliably and efficiently between hosts. It can also be used to download files from remote servers to your computer. It uses port 27 by default.
- **ICMP** : ICMP is the **Internet Control Message Protocol.** It is a network layer protocol used for error handling. It is mainly used by network devices like routers for diagnosing the network connection issues and crucial for error reporting and testing if the data is reaching the preferred destination in time. It uses port 7 by default.
- **ARP** : ARP is **Address Resolution Protocol**. It is a network-level protocol used to convert the logical address i.e. IP address to the device's physical address i.e. MAC address. It can also be used to get the MAC address of devices when they are trying to communicate over the local network.
- **RIP** :RIP stands for Routing Information Protocol. It is accessed by the routers to send data from one network to another. RIP is a dynamic protocol which is used to find the best route from source to the destination over a network by using the hop count

algorithm. Routers use this protocol to exchange the network topology information. This protocol can be used by small or medium-sized networks.

- **MAC address and IP address** (Imp) :

  1. Both MAC (Media Access Control) Address and IP Address are used to **uniquely define a device on the internet.** NIC Card's Manufacturer provides the MAC Address, on the other hand Internet Service Provider provides IP Address.

  2. **The main difference between MAC and IP address** is that MAC Address is used to ensure the physical address of a computer. It uniquely identifies the devices on a network. While IP addresses are used to uniquely identify the connection of a network with that device taking part in a network.

- **Ipconfig and Ifconfig :**

  1. Ipconfig : Internet Protocol Configuration, It is a command used in Microsoft operating systems to view and configure network interfaces

  2. Ifconfig : Interface Configuration, It is a command used in MAC, Linux, UNIX operating systems to view and configure network interfaces

- **Firewall :** The firewall is a network security system that is used to monitor the incoming and outgoing traffic and blocks the same based on the firewall security policies. It acts as a wall between the internet (public network) and the networking devices (a private network). It is either a hardware device, software program, or a combination of both. It adds a layer of security to the network.

Important Key Points

1. **What happens when you enter google.com in the web browser? (Most Imp)**

Steps :

- Check the browser cache first if the content is fresh and present in the cache display the same.
- If not, the browser checks if the IP of the URL is present in the cache (browser and OS) if not then requests the OS to do a DNS lookup using UDP to get the corresponding IP address of the URL from the DNS server to establish a new TCP connection.
- A new TCP connection is set between the browser and the server using three-way handshaking.
- An HTTP request is sent to the server using the TCP connection.
- The web servers running on the Servers handle the incoming HTTP request and send the HTTP response.
- The browser processes the HTTP response sent by the server and may close the TCP connection or reuse the same for future requests.
- If the response data is cacheable then browsers cache the same.
- Browser decodes the response and renders the content.

2. **Hub:** Hub is a networking device which is used to transmit the signal to each port (except one port) to respond from which the signal was received. Hub is operated on a Physical layer. In this packet filtering is not available. It is of two types: Active Hub, Passive Hub.

   Switch: Switch is a network device which is used to enable the connection establishment and connection termination on the basis of need. Switch is operated on the Data link layer. In this packet filtering is available. It is a type of full duplex transmission mode and it is also called an efficient bridge.

3. A **subnet** is a network inside a network achieved by the process called subnetting which helps divide a network into subnets. It is used for getting a higher routing efficiency and enhances the security of the network. It reduces the time to extract the host address from the routing table.

4. **<u>The reliability of a network</u> can be measured by the following factors**:

- Downtime: The downtime is defined as the required time to recover.
- Failure Frequency: It is the frequency when it fails to work the way it is intended.
- Catastrophe: It indicates that the network has been attacked by some unexpected event such as fire, earthquake.

5. There are mainly two criteria which make a **<u>network effective and efficient</u>**:

- <u>Performance</u> : performance can be measured in many ways like transmit time and response time.
- <u>Reliability:</u> reliability is measured by frequency of failure.
- <u>Robustness</u>**:** robustness specifies the quality or condition of being strong and in good condition.
- <u>Security:</u> It specifies how to protect data from unauthorized access and viruses.

6. **<u>Node and Link</u>** : A network is a connection setup of two or more computers directly connected by some physical mediums like optical fiber or coaxial cable. This physical medium of connection is known as a link, and the computers that it is connected to are known as nodes.

7. CDN (Content Delivery Network)

A content delivery network (CDN) is a geographically distributed group of servers that caches content close to end users. A CDN allows for the quick transfer of assets needed for loading Internet content, including HTML pages, JavaScript files, stylesheets, images, and videos.

7. *<u>Modem</u>:*
A modem is short for modulator-demodulator. In simpler terms, it connects your home network to the internet service provider (ISP) by converting digital data from your devices into a form that can be transmitted over the ISP's network and vice versa.

8. **Gateway and Router**: A Router is a device that directs data traffic between different networks. In a home network, it typically manages the flow of data between your local devices and the internet. Routers use a system called Network Address Translation (NAT) to assign local IP addresses to devices within your home network, allowing them to share a single public IP address when accessing the internet.

   A gateway is a device that connects two different networks and facilitates communication between them. It acts as a bridge between your local network and the internet.In the context of home networking, a gateway often combines the functionality of a modem and a router in a single device. It serves as the entry point to the internet and manages both the connection to the ISP and the local network.

9. **NIC (Imp)** : NIC stands for **Network Interface Card**. It is a peripheral card attached to the PC to connect to a network. Every NIC has its own MAC address that identifies the PC on the network. It provides a wireless connection to a local area network. NICs were mainly used in desktop computers.

10. **POP3 stands for Post Office Protocol version3**. POP is responsible for accessing the mail service on a client machine. POP3 works on two models such as Delete mode and Keep mode.

11. **Private IP Address** - There are three ranges of IP addresses that have been reserved for IP addresses. They are not valid for use on the internet. If you want to access the internet on these private IPs, you must use a proxy server or NAT server. Public IP addresses are distinct and registered on the internet, assigned by your Internet Service Provider (ISP) for a fee. Routers typically receive public IP addresses.

    Public IP Address - A public IP address is an address taken by the Internet Service Provider which facilitates communication on the internet.

12. **RAID** (Redundant Array of Inexpensive/Independent Disks): It is a method to provide Fault Tolerance by using multiple Hard Disc Drives.

13. **Netstat :** It is a command line utility program. It gives useful information about the current TCP/IP setting of a connection.

14. **Ping** : The "ping" is a utility program that allows you to check the connectivity between the network devices. You can ping devices using its IP address or name.

15. The processes on each machine that communicate at a given layer are called **peer-peer processes. (P2P).**

16. **Unicasting:** If the message is sent to a single node from the source then it is known as unicasting. This is commonly used in networks to establish a new connection.

Anycasting: If the message is sent to any of the nodes from the source then it is known as anycasting. It is mainly used to get the content from any of the servers in the Content Delivery System.

Multicasting: If the message is sent to a subset of nodes from the source then it is known as multicasting. Used to send the same data to multiple receivers.

Broadcasting: If the message is sent to all the nodes in a network from a source then it is known as broadcasting. DHCP and ARP in the local network use broadcasting.

17. What is Firewall? Types of Firewall.

A firewall is like the security guard of your computer network, determining what can enter or exit. It acts as a barrier between your internal network and external networks (like the internet), filtering and controlling traffic based on predetermined security rules.

a. *Packet Filtering Firewall:*
   As the data is sent in packets, this firewall checks the header of each packet. As it doesn't check the payload data it is not that secure.
b. *Proxy Firewall:*
   It hides the IP address of the computer and acts as a proxy. It also checks the payload of the data that's why it is very secure. It is slower compared to Packet Filtering Firewalls.

c. *Hybrid Firewall:*

Combination of both Packet Filtering Firewall and Proxy Firewall. It offers highest security.

18. Basic Network Attacks in Computer

- *Man-in-the-Middle (MitM) Attack:*

  The attacker intercepts communication between two parties, gaining unauthorized access to sensitive information.

- *Denial of Service (DoS) Attack:*
  Overwhelms a system or network with a flood of traffic, rendering it unauthorized to legitimate users.

- *Spoofing Attacks:*
  Attackers manipulate their identity or IP address to appear as a trusted entity.

- *Phishing Attacks:*
  Deceptive attempts to trick individuals into revealing sensitive information through emails, messages, or websites.

- *SQL Injection:*
  Exploiting vulnerabilities in web applications to manipulate or gain unauthorized access to a database.

19. Various terms in cryptography.

- *Hash function:*
  It is a function which converts a plain text into a cipher text. It is really difficult to convert the cipher text back to plain text.
  Eg: MD5 and SHA256.

- *Encryption:*
  It's like putting a message into a secret language that only those with the right "key" can understand.
  - *Symmetric Encryption:*
    In this type, the same key is used for both the encryption and decryption of the data.
  - *Asymmetric Encryption:*
    Also known as public-key cryptography, it involves a pair of keys – a public key and a private key. The public key is used for encryption, while the private key is used for decryption.

20. Process of end-to-end encryption using asymmetric encryption

- *Key Generation:*
    i. Both the sender and receiver generate a pair of cryptographic keys: a public key and a private key.
    ii. The public key is shared openly, while the private key is kept secret.

- *Sender Encrypts Message:*
    i. The sender obtains the recipient's public key.
    ii. Using the recipient's public key, the sender encrypts the message. Only the recipient's private key can decrypt this message.

- *Transmission of Encrypted Message:*
    i. The sender transmits the encrypted message to the recipient.

- *Receiver Decrypts Message:*
    i. The recipient uses their private key to decrypt the received message.
    ii. Since the private key is known only to the recipient, it's assumed that only the intended recipient can successfully decrypt the message.

21. Digital Signatures

- A digital signature is a cryptographic technique used to verify the authenticity and integrity of a digital message, document, or transaction.

- It involves the use of asymmetric cryptography, where the sender uses their private key to encrypt a hash of the message, creating a digital signature.
- The recipient, using the sender's public key, can decrypt the signature to obtain the original hash.
- By hashing the received message and comparing it with the decrypted hash, the recipient can verify both the sender's identity and that the message has not been altered during transmission.

22. Pipelining in Computer Networks

🔹 What is Pipelining?

Definition:
Pipelining is a technique in computer networks where **multiple packets are sent without waiting for the acknowledgment of previous ones**, improving overall throughput and efficiency.

It's used in **reliable data transfer protocols** to **send multiple frames** before needing an acknowledgment, avoiding idle time.

🔹 Why is Pipelining Important?

- Improves **network utilization**
- Reduces **idle time**
- Allows **parallelism** in sending and receiving
- Increases **throughput** (data transfer rate)

🧠 Types of Pipelining Protocols

Protocol	Description
Stop-and-Wait	Sends 1 frame at a time, waits for ACK (no pipelining)
Go-Back-N (GBN)	Sender can send N frames before waiting for ACK
Selective Repeat (SR)	Sender sends N frames, and retransmits **only the lost** or **corrupted ones**

🔹 **1. Stop-and-Wait Protocol**

- Only one frame is in transit at a time.
- Next frame is sent **only after** receiving an acknowledgment (ACK).
- **Inefficient** in high-latency networks.

No pipelining

🔹 **2. Go-Back-N (GBN) Protocol**

- Sender can send **up to N frames** before waiting for ACK.
- If an error occurs, all subsequent frames are **discarded** and resent.

Pipelined but less efficient than Selective Repeat.

🔹 **3. Selective Repeat Protocol**

- Similar to GBN but more efficient.
- Sender retransmits **only the specific frame** that was lost or corrupted.
- Receiver buffers out-of-order frames.

Most efficient pipelining technique

---

23. CSMA/CD (Used in Wired Ethernet)

Carrier Sense Multiple Access with Collision Detection

✅ **How it works:**

1. **Carrier Sense:** Check if the medium (cable) is idle.
2. **Multiple Access:** Multiple devices can attempt to use the same channel.
3. **Collision Detection:** If two devices send at once → collision occurs → they stop, wait random time, and retry.

⚙️ **Used In: Wired Ethernet (legacy versions, like 10BASE-T)**

❌ **Not used in modern full-duplex networks, because collisions don't occur there.**

---

24. CSMA/CA (Used in Wireless Networks)

Carrier Sense Multiple Access with Collision Avoidance

✅ **How it works:**

1. **Carrier Sense:** Listen before sending.
2. **Collision Avoidance:** Use techniques like random back-off and RTS/CTS (Request to Send / Clear to Send) to **avoid** collisions before they happen.

⚙️ **Used In: Wireless networks like Wi-Fi (IEEE 802.11)**

🔁 **No collision detection possible in wireless, because devices can't listen while transmitting.**

25. QoS (Quality of Service)

✅ **Definition:**

QoS refers to the overall performance of a network or service, especially the ability to provide guaranteed service levels such as bandwidth, delay, jitter, and packet loss.

🧠 **Used In:**

- **VoIP (Voice over IP)**
- **Video conferencing**
- **Streaming services**
- **Real-time applications**

🎯 **QoS Parameters:**

Parameter	Description
Bandwidth	Max data transfer rate
Latency	Delay in data delivery
Jitter	Variation in latency
Packet Loss	Packets lost in transit
Reliability	Consistency of packet delivery

📌 **Techniques to Achieve QoS:**

- **Traffic shaping**
- **Resource reservation**
- **Priority queuing**

- Congestion control

---

26. ARQ (Automatic Repeat Request)

✅ **Definition:**

ARQ is an error-control protocol used in data communication where the receiver detects errors and asks the sender to resend the corrupted data.

🔁 **Types of ARQ:**

Type	Description
Stop-and-Wait ARQ	Sender waits for ACK before sending next frame
Go-Back-N ARQ	Sender can send N frames; resends all after error
Selective Repeat ARQ	Resends only the specific erroneous frames

🎯 **Purpose:**

To ensure reliable data transmission over unreliable networks.

---

27. RARQ (Reverse Automatic Repeat Request)

✅ **Definition:**

RARQ is a variation of ARQ where the receiver requests retransmission only when needed, instead of the sender checking for acknowledgment.

📌 **Key Point:**

- It is receiver-driven, unlike ARQ which is sender-driven.
- More common in certain wireless and error-prone transmission systems.

---

28. Definition:

Term	Description
Pure ALOHA	A simple communication protocol where stations transmit anytime they have data, without checking the channel.
Slotted ALOHA	An improved version of Pure ALOHA where time is divided into equal slots, and stations can only transmit at the beginning of a time slot.

🔹 **Working Principle:**

Feature	Pure ALOHA	Slotted ALOHA
Time Synchronization	❌ Not required	✅ Required
Transmission Time	Anytime	Only at start of predefined time slots
Collision Window	2 × Frame Time	1 × Frame Time
Probability of Success	Lower (more chance of collision)	Higher (less chance of collision)