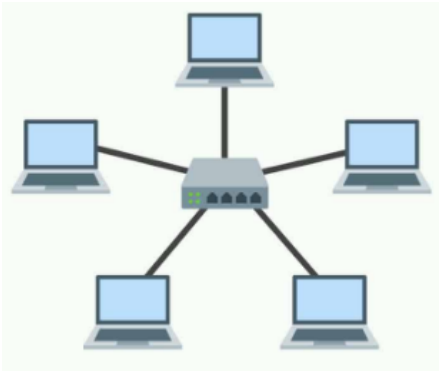
Computer Networks

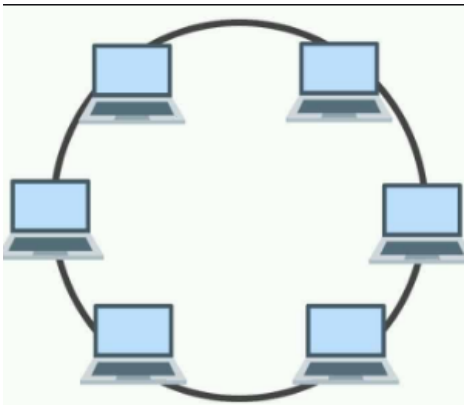
- **Network** : A network is a set of devices that are connected with a physical media link. In a network, two or more nodes are connected by a physical link or two or more networks are connected by one or more nodes. A network is a collection of devices connected to each other to allow the sharing of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

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

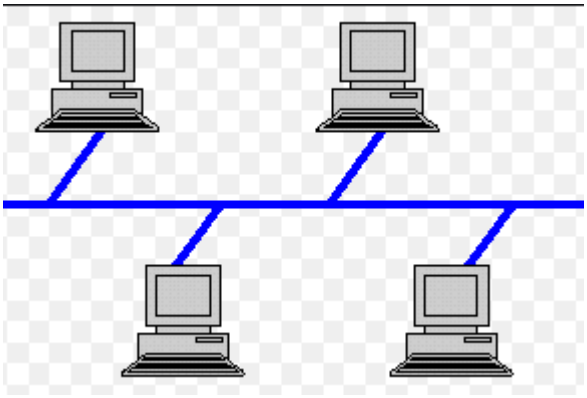
  Types of Network Topology :
  - **Star :**
    - Star topology is a network topology in which all the nodes are connected to a single device known as a central device.
    - Star topology requires more cable compared to other topologies. Therefore, it is more robust as a failure in one cable will only 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.



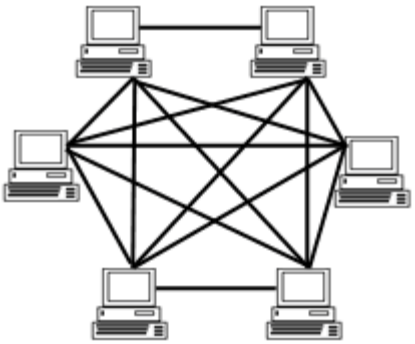
- **Ring** :
  1. Ring topology is a network topology in which nodes are exactly connected to two or more nodes and thus, forming a single continuous path for the transmission.
  2. It does not need any central server to control the connectivity among the nodes.
  3. If the single node is damaged, then 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

- **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

- **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.

2. **DataLink Layer**
    - 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

- 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.

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, simple mail transfer protocol, 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.

- **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.**

  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.**

- **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.

- **Difference Between TCP (Transmission Control Protocol) and UDP (User Datagram Protocol)**:
    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. **<u>Gateway and router</u>** : A node that is connected to two or more networks is commonly known as a gateway. It is also known as a router. It is used to forward messages from one network to another. **Both the gateway and router regulate the traffic in the network**. **Differences between gateway and router**: A router sends the data between two similar networks while gateway sends the data between two dissimilar networks.

8. **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.

9. **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.

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

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

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

13. **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.

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

15. **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.