Computer Network :

Two or more than two computers are connected to each other to share data and resources is called computer network.

Network Motivation

- Sharing of Resources
- Facilitate Communications

The main goals of computer networks are as follows –

Resource Sharing:

The main goal of the computer network is Resource Sharing. It is to create all the programs, data and hardware accessible to anyone on the network without considering the resource's physical area and the client.

Saving Money:

The second goal of a computer network is saving money. Small computers have a much excellent value proportion than higher ones. Mainframes are approximately a method ten times quicker than the quickest single-chip microprocessors, but they cost a huge number of times more. This imbalance has made numerous system designers build systems, including dynamic personal computers, one per customer, with data kept on at least one shared document server machines. This objective prompts networks for specific computers situated in a similar building, including a network is known as LAN (Local Area Network).

High Reliability:

The third goal is to support high reliability by acquiring a different authority of supply. For example, all **files can be recreated on a few machines**, and thus if one of them is non-existent, the additional copies could be available.

Improve Performance:

The fourth goal of a computer network is to improve accessibility and the performance of the system. A system's performance can be improved by inserting one or more processors into it as its workload grows.

For example, if the system is full, replacing it with a larger one at a large expense, it is better to add more processors to it at less cost and less disruption to the user. This improves both accessibilities as well as the performance of a system.

Communication Medium:

The fifth goal of the computer network offers a powerful communication medium. The different user on the network can immediately identify a document that has been refreshed on a network.

Applications of computer networks

1. Resource Sharing:

Resource sharing is an application of a computer network. Resource sharing means you can share one Hardware and Software among multiple users. Hardware includes printers, Disks, Fax Machines, etc. Computing devices. And Software includes Atom, Oracle VM Virtual Box, Postman, Android Studio, etc.

2. Information Sharing:

Using a computer network, we can share Information over the network, and it provides Search capabilities such as WWW. Over the network, a single information can be shared among the many users over the internet.

3. Communication:

Communication includes email, calls, message broadcast, electronic funds transfer system etc.

4. Entertainment Industry:

In Entertainment industry also uses computer networks widely. Some of the Entertainment industries are Video on demand, Multiperson real-time simulation games, movie/TV programs, etc.

5. Access to Remote Databases:

Computer networks allow us to access the Remote Database of the various applications by the end-users. Some applications are Reservation for Hotels, Airline Booking, Home Banking, Automated Newspaper, Automated Library etc.

6. Home applications:

There are many common uses of the computer network are as home applications. For example, you can consider user-to-user communication, access to remote instruction, electronic commerce, and entertainment. Another way is managing bank accounts, transferring money to some other banks, paying bills electronically. A computer network arranges a robust connection mechanism between users.

7. Business applications:

The result of business application here is resource sharing. And the purpose of resource sharing is that without moving to the physical location of the resource, all the data, plans, and tools can be shared to any network user. Most of the companies are doing business electronically with other companies and with other clients worldwide with the help of a computer network.

8. Mobile users

The rapidly growing sectors in computer applications are mobile devices like notebook computers and PDAs (personal digital assistants). Here mobile users/device means portable device. The computer network is widely used in new-age technology like smartwatches, wearable devices, tablets, online transactions, purchasing or selling products online, etc.

9. Social media

Social media is also a great example of a computer network application. It helps people to share and receive any information related to political, ethical, and social issues.

Types of computer network:

PERSONAL AREA NETWORK (PAN):

This is the smallest and most basic network that you'll find. It's meant to cover a very small area (typically a single room or building). A PAN is most commonly used for one individual and to connect just a handful of devices such as a computer, smart phone, and printer. Probably the most well-known PAN technology is Bluetooth connection. So, next time you connect your phone to your car to play music, you can thank your Personal Area Network!

LAN : (LOCAL AREA NETWORK):

Limited to office, building

College building

LOCAL AREA NETWORK (LAN)

This is an extremely common and well-known type of network. LAN connects a group of computers or devices together across a local area. This type of network can be utilized to connect devices throughout one building or even 2-3 buildings depending on the proximity to each other. Whether your office location utilizes wired or wireless connection, it's almost surely using a LAN connection.

MAN : (METROPOLITAN AREA NETWORK) :

Limited to city,e.g. cable tv network

METROPOLITAN AREA NETWORK (MAN)

Larger than a LAN but smaller than a WAN, a MAN incorporates elements of both types of networks. It connects multiple LANs together and spans an entire geographical area such as a city or town (or sometimes a campus). Ownership and management can be handled by a single person, but it's more likely done by a larger company or organization.

WAN :(WIDE AREA NETWORK)

Geographical unlimited, world wide, e.g. internet, telephone system

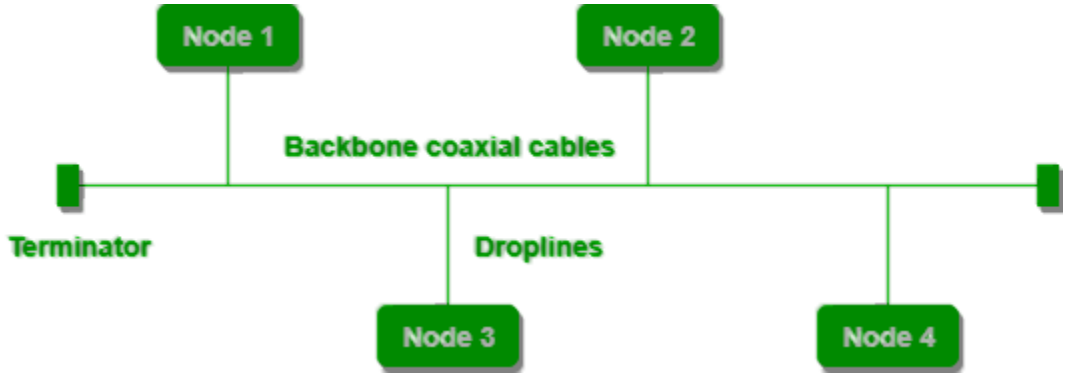
WIRELESS LOCAL AREA NETWORK (WLAN)

A WLAN is simply a LAN that does not rely on cables to connect to the network. So, when you're using WiFi, you're using a WLAN. WLANs are typically used in the same scenario as LANs, it just depends on whether you'd prefer an on premises or remote cloud solution (wires or wireless).

Network Topology :

Geographically / Geometrically arrangement of nodes (Computers) in the network is called as network topology.

Bus topology



Bus Topology:
Bus topology is a network type in which every computer and network device is connected to a single cable. It transmits the data from one end to another in a single direction. No bi-directional feature is in bus topology. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

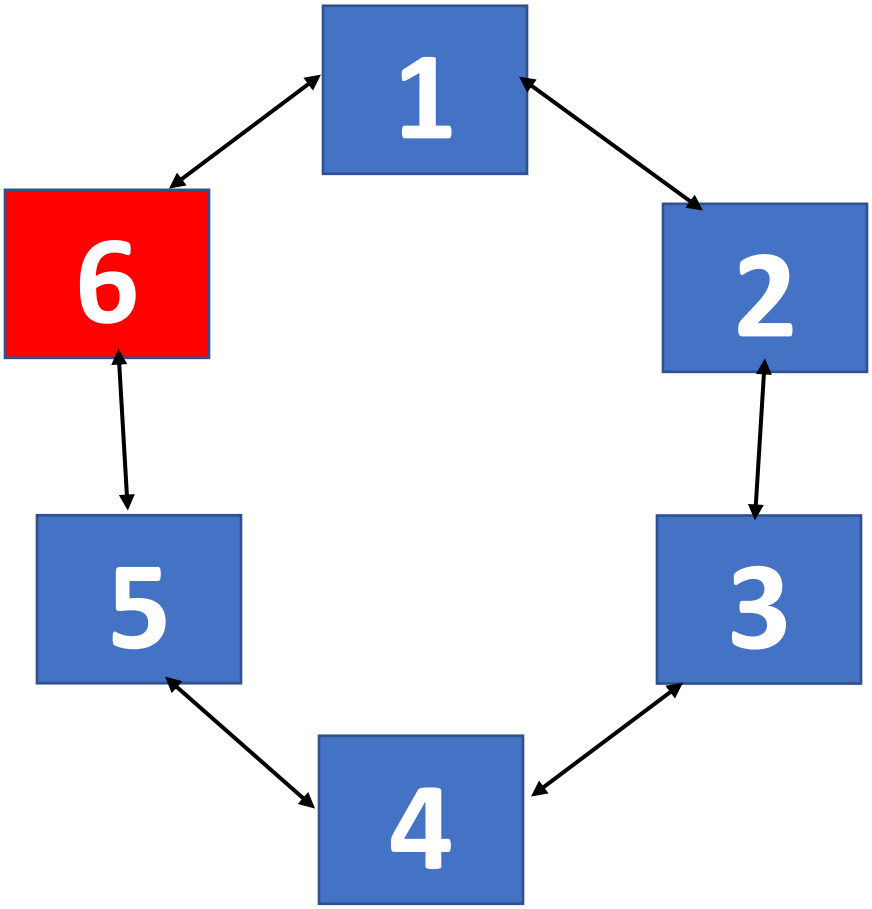
Advantages of this topology:

- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, which is known as backbone cable, and N drop lines are required.
- The cost of the cable is less compared to other topologies, but it is used to build small networks.

Disadvantages of Bus Topology :

- Bus topology is not great for large networks.
- Identification of problems becomes difficult if the whole network goes down.
- Troubleshooting individual device issues is very hard.
- Need terminators are required at both ends of the main cable.
- Additional devices slow the network down.
- If the main cable is damaged, the whole network fails or splits into two.
- Packet loss is high.
- This network topology is very slow as compared to other topologies.

Ring Topology



Ring Topology:

In this topology, it forms a ring connecting devices with exactly two neighbouring devices.

A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the

ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.

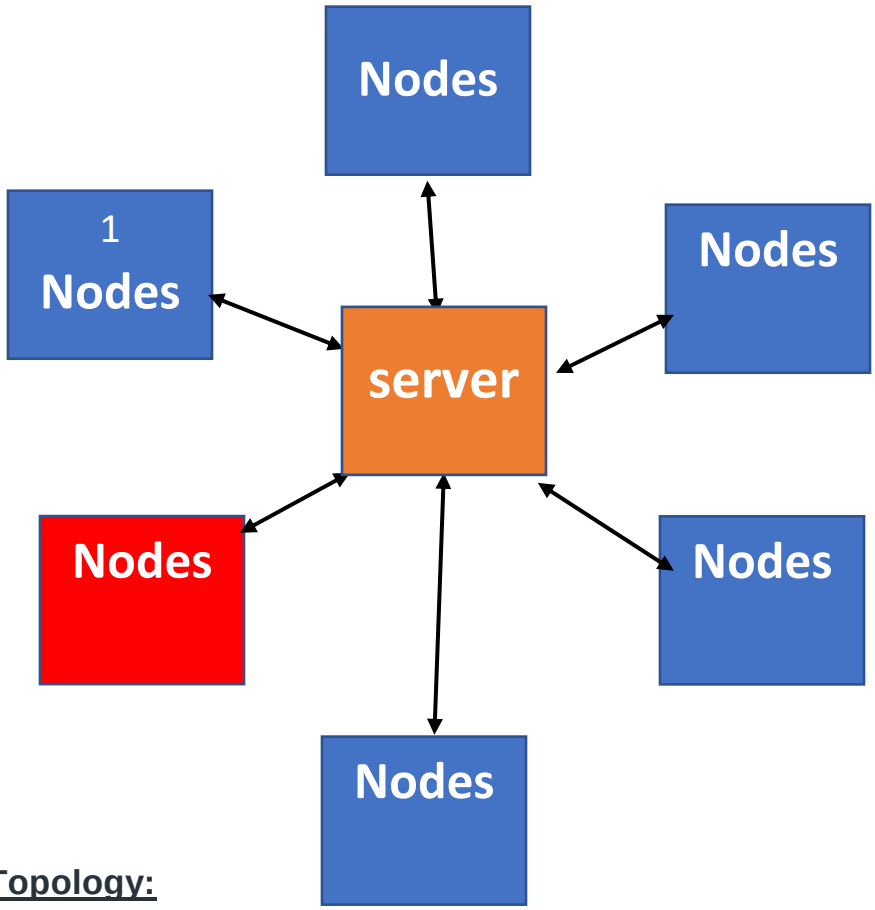
Advantages:

- In this data flows in one direction which reduces the chance of packet collisions.
- In this topology additional workstations can be added after without impacting performance of the network.
- Equal access to the resources.
- There is no need of server to control the connectivity among the nodes in the topology.
- It is cheap to install and expand.
- Minimum collision.
- Speed to transfer the data is very high in this type of topology.
- Due to the presence of token passing the performance of ring topology becomes better than bus topology under heavy traffic.
- Easy to manage.
- Ring network is extremely orderly organized where every device has access to the token and therefore the opportunity to transmit.

Disadvantages of Ring topology :

- Due to the Uni-directional Ring, a data packet (token) must have to pass through all the nodes.
- If one workstation shuts down, it affects whole network or if a node goes down entire network goes down.
- It is slower in performance as compared to the bus topology
- It is Expensive.
- Addition and removal of any node during a network is difficult and may cause issue in network activity.
- Difficult to troubleshoot the ring.
- In order for all the computer to communicate with each other, all computer must be turned on.
- Total dependence in on one cable.
- They were not Scalable.

Star Topology



Star Topology:

In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them. In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc.

Advantages of Star Topology

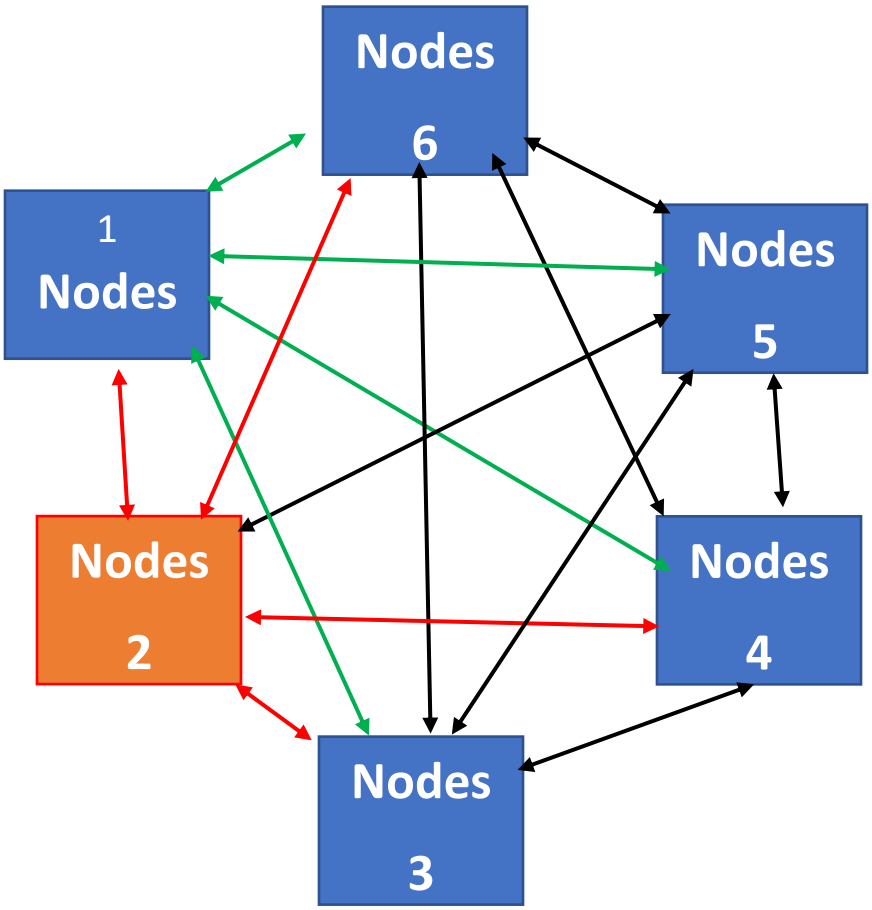
- It is very reliable – if one cable or device fails then all the others will still work

- It is high-performing as no data collisions can occur
- Less expensive because each device only need one I/O port and wishes to be connected with hub with one link.
- Easier to put in
- Robust in nature
- Easy fault detection because the link are often easily identified.
- No disruptions to the network when connecting or removing devices.
- Each device requires just one port i.e. to attach to the hub.
- If N devices are connected to every other in star, then the amount of cables required to attach them is N. So, it's easy to line up.

Disadvantages of Star Topology

- Requires more cable than a linear bus .
- If the connecting network device (network switch) fails, nodes attached are disabled and can't participate in network communication.
- More expensive than linear bus topology due to the value of the connecting devices (network switches)
- If hub goes down everything goes down, none of the devices can work without hub.
- Hub requires more resources and regular maintenance because it's the central system of star .
- Extra hardware is required (hubs or switches) which adds to cost
- Performance is predicated on the one concentrator i.e. hub.

Mesh /completely connected Topology



Mesh Topology:

In a mesh topology, every device is connected to another device via a particular channel. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.

Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure 1, there are 6 devices connected to each other, hence the total number of ports required by each device is 5.

Advantages of Mesh Topology :

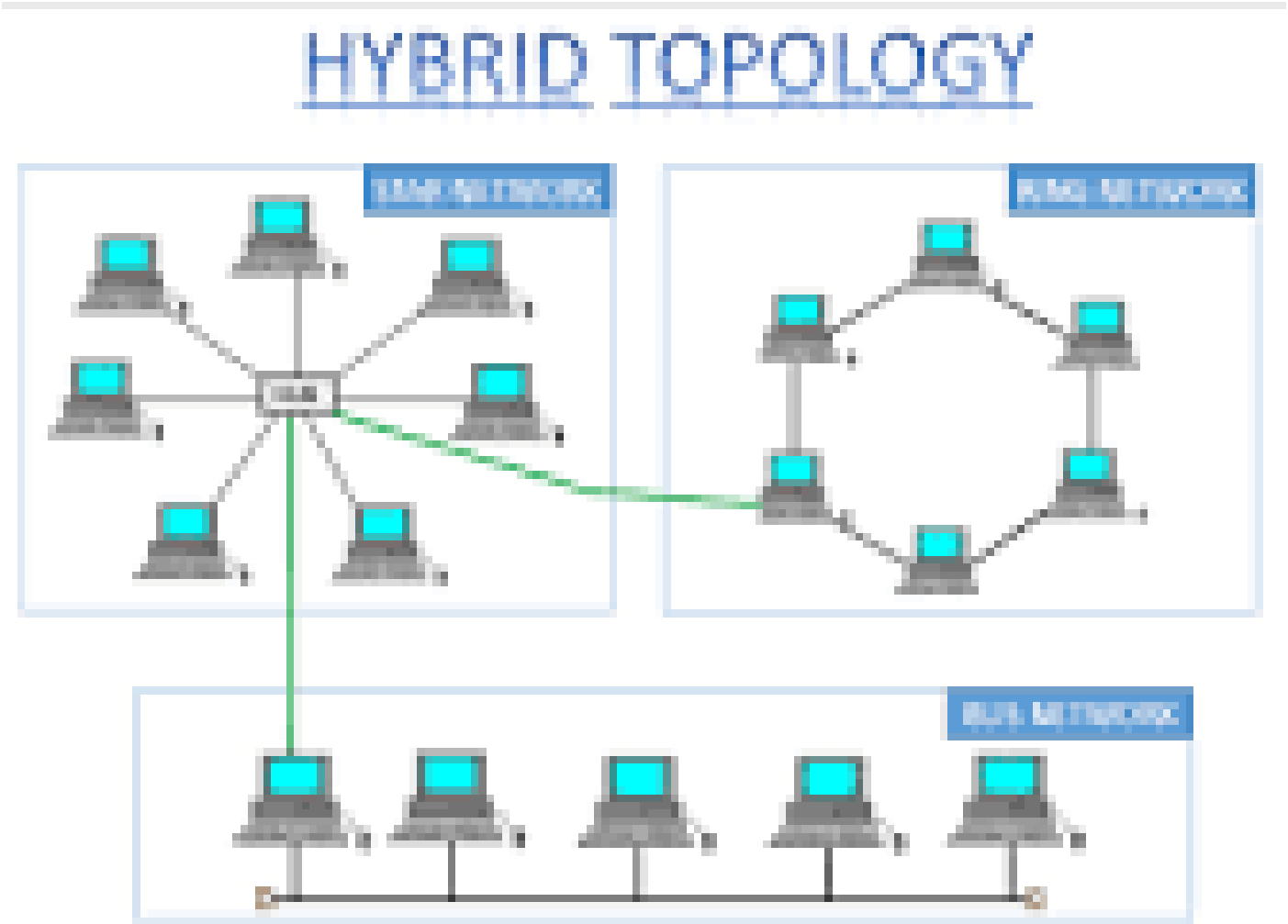
- Failure during a single device won’t break the network.
- There is no traffic problem as there is a dedicated point to point links for every computer.
- Fault identification is straightforward.
- This topology provides multiple paths to succeed in the destination and tons of redundancy.
- It provides high privacy and security.
- Data transmission is more consistent because failure doesn’t disrupt its processes.
- Adding new devices won’t disrupt data transmissions.
- This topology has robust features to beat any situation.
- A mesh doesn’t have a centralized authority.

Disadvantages of Mesh Topology :

- It’s costly as compared to the opposite network topologies i.e. star, bus, point to point topology.
- Installation is extremely difficult in the mesh.
- Power requirement is higher as all the nodes will need to remain active all the time and share the load.
- Complex process.
- The cost to implement mesh is above other selections.
- There is a high risk of redundant connections.
- Each node requires a further utility cost to think about.
- Maintenance needs are challenging with a mesh.

Hybrid Topology:

Combination of two or more different topologies to make a resultant topology that has good points(as well as weaknesses) of all constituent basic topologies instead of having characteristics of only one specific topology. this mix of topologies is completed consistent with the wants of the organization. for instance if in an office in one of the department's ring topology is employed and another star, topology is employed, connecting these topologies will end in Hybrid Topology (ring topology and star topology).



Advantages of Hybrid Topology:

- This type of topology combines the benefits of different types of topologies in one topology.
- Can be modified as per requirement.
- It is extremely flexible.
- It is very reliable.
- It is easily scalable as Hybrid networks are built in a fashion which enables easy integration of new hardware components.
- Error detecting and troubleshooting are easy.
- Handles a large volume of traffic.
- It is used to create large networks.
- The speed of the topology becomes fast when two topologies are put together.

Disadvantages of Hybrid Topology:

- It is a type of network expensive.
- The design of a hybrid network is very complex.
- There is a change in the hardware to connect one topology with another topology.
- Hybrid architectures are larger in scale so they require a lot of cables in the installation process.
- Hubs which are used to connect two distinct networks are very costly. And hubs are different from usual hubs as they need to be intelligent enough to work with different architectures.
- Installation is a difficult process.

Network Protocols:

A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network.

Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure or design.

List of Network Protocols

There are thousands of different network protocols, but they all perform one of three primary actions:

- Communication
- Network management
- Security

- **Hypertext Transfer Protocol (HTTP)**: This Internet Protocol defines how data is transmitted over the internet and determines how web servers and browsers should respond to commands. This protocol appears at the beginning of various URLs or web addresses online.

- **Secure Socket Shell (SSH)**: This protocol provides secure access to a computer, even if it's on an unsecured network. SSH is particularly useful for network administrators who need to manage different systems remotely.

- **Short Message Service (SMS)**: This communications protocol was created to send and receive text messages over cellular networks. SMS refers exclusively to text-based messages. Pictures, videos or other media require Multimedia Messaging Service (MMS), an extension of the SMS protocol.

1. DHCP: Dynamic Host Configuration Protocol

DHCP is a communication protocol that enables network administrators to automate the assignment of IP addresses in a network. In an IP network, every device connecting to the internet requires a unique IP. DHCP lets network admins distribute IP addresses from a central point and automatically send a new IP address when a device is plugged in from a different place in the network. DHCP works on a client-server model.

Advantages of using DHCP

- Centralized management of IP addresses.
- Reuse of IP addresses, reducing the total number of IP addresses required.

Disadvantages of using DHCP

- Tracking internet activity becomes tedious, as the same device can have multiple IP addresses over a period of time.
- Computers with DHCP cannot be used as servers, as their IPs change over time.

2. DNS: Domain Name System protocol

The DNS protocol helps in translating or mapping host names to IP addresses. DNS works on a client-server model, and uses a distributed database over a hierarchy of name servers.

Hosts are identified based on their IP addresses, but memorizing an IP address is difficult due to its complexity. IPs are also dynamic, making it all the more necessary to map domain names to IP addresses. DNS helps resolve this issue by converting the domain names of websites into numerical IP addresses.

Advantages

- DNS facilitates internet access.
- Eliminates the need to memorize IP addresses.

Disadvantages

- DNS queries don't carry information pertaining to the client who initiated it. This is because the DNS server only sees the IP from where the query came from, making the server susceptible to manipulation from hackers.

- DNS root servers, if compromised, could enable hackers to redirect to other pages for phishing data.

3. FTP: File Transfer Protocol

File Transfer Protocol enables file sharing between hosts, both local and remote, and runs on top of TCP. For file transfer, FTP creates two TCP connections: control and data connection. The control connection is used to transfer control information like passwords, commands to retrieve and store files, etc., and the data connection is used to transfer the actual file. Both of these connections run in parallel during the entire file transfer process.

Advantages

- Enables sharing large files and multiple directories at the same time.
- Lets you resume file sharing if it was interrupted.
- Lets you recover lost data, and schedule a file transfer.

Disadvantages

- FTP lacks security. Data, usernames, and passwords are transferred in plain text, making them vulnerable to malicious actors.
- FTP lacks encryption capabilities, making it non-compliant with industry standards.

4. HTTP: Hyper Text Transfer Protocol

HTTP is an application layer protocol used for distributed, collaborative, and hypermedia information systems. It works on a client-server model, where the web browser acts as the client. Data such as text, images, and other multimedia files are shared over the World Wide Web using HTTP. As a request and response type protocol, the client sends a request to the server, which is then processed by the server before sending a response back to the client.

HTTP is a stateless protocol, meaning the client and server are only aware of each other while the connection between them is intact. After that, both the client and server forget about each other's existence. Due to this phenomenon, the client and server can't both retain information between requests.

Advantages

- Memory usage and CPU usage are low because of lesser concurrent connections.
- Errors can be reported without closing connections.
- Owing to lesser TCP connections, network congestion is reduced.

Disadvantages

- HTTP lacks encryption capabilities, making it less secure.
- HTTP requires more power to establish communication and transfer data.

5. IMAP and IMAP4: Internet Message Access Protocol (version 4)

IMAP is an email protocol that lets end users access and manipulate messages stored on a mail server from their email client as if they were present locally on their remote device. IMAP follows a client-server model, and lets multiple clients access messages on a common mail server concurrently. IMAP includes operations for creating, deleting, and renaming mailboxes; checking for new messages; permanently removing messages; setting and removing flags; and much more. The current version of IMAP is version 4 revision 1.

Advantages

- As the emails are stored on the mail server, local storage utilization is minimal.
- In case of accidental deletion of emails or data, it is always possible to retrieve them as they are stored on the mail server.

Disadvantages

- Emails won't work without an active internet connection.
- High utilization of emails by end users requires more mailbox storage, thereby augmenting costs.

6. POP and POP3: Post Office Protocol (version 3)

The Post Office Protocol is also an email protocol. Using this protocol, the end user can download emails from the mail server to their own email client. Once the emails are downloaded locally, they can be read without an internet connection. Also, once the emails are moved locally, they get deleted from the mail server, freeing up space. POP3 is not designed to perform extensive manipulations with the messages on the mail server, unlike IMAP4. POP3 is the latest version of the Post Office Protocol.

Advantages

- Read emails on local devices without internet connection.
- The mail server need not have high storage capacity, as the emails get deleted when they're moved locally.

Disadvantages

- If the local device on which the emails were downloaded crashes or gets stolen, the emails are lost.

7. SMTP: Simple Mail Transfer Protocol

SMTP is a protocol designed to transfer electronic mail reliably and efficiently. SMTP is a push protocol and is used to send the email, whereas POP and IMAP are used to retrieve emails on the end user's side. SMTP transfers emails between systems, and notifies on incoming emails. Using SMTP, a client can transfer an email to another client on the same network or another network through a relay or gateway access available to both networks.

Advantages

- Ease of installation.
- Connects to any system without any restriction.
- It doesn't need any development from your side.

Disadvantages

- Back and forth conversations between servers can delay sending a message, and also increases the chance of the message not being delivered.
- Certain firewalls can block the ports used with SMTP.

8. Telnet: Terminal emulation protocol

Telnet is an application layer protocol that enables a user to communicate with a remote device. A Telnet client is installed on the user's machine, which accesses the command line interface of another remote machine that runs a Telnet server program.

Telnet is mostly used by network administrators to access and manage remote devices. To access a remote device, a network admin needs to enter the IP or host name of the remote device, after which they will be presented with a virtual terminal that can interact with the host.

Advantages

- Compatible with multiple operating systems.
- Saves a lot of time due to its swift connectivity with remote devices.

Disadvantages

- Telnet lacks encryption capabilities and sends across critical information in clear text, making it easier for malicious actors.

- Expensive due to slow typing speeds.

9. SNMP: Simple Network Management Protocol

SNMP is an application layer protocol used to manage nodes, like servers, workstations, routers, switches, etc., on an IP network. SNMP enables network admins to monitor network performance, identify network glitches, and troubleshoot them. SNMP protocol is comprised of three components: a managed device, an SNMP agent, and an SNMP manager.

The SNMP agent resides on the managed device. The agent is a software module that has local knowledge of management information, and translates that information into a form compatible with the SNMP manager. The SNMP manager presents the data obtained from the SNMP agent, helping network admins manage nodes effectively.

Currently, there are three versions of SNMP: SNMP v1, SNMP v2, and SNMP v3. Both versions 1 and 2 have many features in common, but SNMP v2 offers enhancements such as additional protocol operations. SNMP version 3 (SNMP v3) adds security and remote configuration capabilities to the previous versions.

. TCP: Transmission Control Protocol

TCP is a transport layer protocol that provides a reliable stream delivery and virtual connection service to applications through the use of sequenced acknowledgement. TCP is a connection-oriented protocol, as it requires a connection to be established between applications before data transfer. Through flow control and acknowledgement of data, TCP provides extensive error checking. TCP ensures sequencing of data, meaning the data packets arrive in order at the receiving end. Retransmission of lost data packets is also feasible with TCP.

Advantages

- TCP ensures three things: data reaches the destination, reaches it on time, and reaches it without duplication.
- TCP automatically breaks data into packets before transmission.

Disadvantages

- TCP cannot be used for broadcast and multicast connections.

2. UDP: User Datagram Protocol

UDP is a connection-less transport layer protocol that provides a simple but unreliable message service. Unlike TCP, UDP adds no reliability, flow control, or error recovery functions. UDP is useful in situations where the reliability mechanisms of TCP are not necessary. Retransmission of lost data packets isn't possible with UDP.

Advantages

- Broadcast and multicast connections are possible with UDP.
- UDP is faster than TCP.

Disadvantages

- In UDP, it's possible that a packet may not be delivered, be delivered twice, or not be delivered at all.
- Manual disintegration of data packets is needed.

Network layer protocols

1. IP: Internet Protocol (IPv4)

IPv4 is a network layer protocol that contains addressing and control information, which helps packets be routed in a network. IP works in tandem with TCP to deliver data packets across the network. Under IP, each host is assigned a 32-bit address comprised of two major parts: the network number and host number. The network number identifies a network and is assigned by the internet, while the host number identifies a host on the network and is assigned by a network admin. The IP is only responsible for delivering the packets, and TCP helps puts them back in the right order.

Advantages

- IPv4 encrypts data to ensure privacy and security.
- With IP, routing data becomes more scalable and economical.

Disadvantages

- IPv4 is labor intensive, complex, and prone to errors.

2. IPv6: Internet Protocol version 6

IPv6 is the latest version of the Internet Protocol, a network layer protocol that possesses addressing and control information for enabling packets to be routed in the network. IPv6 was created to deal with IPv4 exhaustion. It increases the IP address size from 32 bits to 128 bits to support more levels of addressing.

Advantages

- More efficient routing and packet processing compared to IPv4.
- Better security compared to IPv4.

Disadvantages

- IPv6 is not compatible with machines that run on IPv4.
- Challenge in upgrading the devices to IPv6.

3. ICMP: Internet Control Message Protocol

ICMP is a network layer supporting protocol used by network devices to send error messages and operational information. ICMP messages delivered in IP packets are used for out-of-band messages related to network operation or misoperation. ICMP is used to announce network errors, congestion, and timeouts, as well assist in troubleshooting.

Advantages

- ICMP is used to diagnose network issues.

Disadvantages

- Sending a lot of ICMP messages increases network traffic.
- End users are affected if malicious users send many ICMP destination unreachable packets.

Data link layer network protocols

1. ARP: Address Resolution Protocol

The Address Resolution Protocol helps map IP addresses to physical machine addresses (or a MAC address for Ethernet) recognized in the local network. A table called an ARP cache is used to maintain a correlation between each IP address and its corresponding MAC address. ARP offers the rules to make these correlations, and helps convert addresses in both directions.

Advantages

- MAC addresses need not be known or memorized, as the ARP cache contains all the MAC addresses and maps them automatically with IPs.

Disadvantages

- ARP is susceptible to security attacks called ARP spoofing attacks.
- When using ARP, sometimes a hacker might be able to stop the traffic altogether. This is also known as ARP denial-of-services.

2. SLIP: Serial Line IP

SLIP is used for point-to-point serial connections using TCP/IP. SLIP is used on dedicated serial links, and sometimes for dial-up purposes. SLIP is useful for allowing mixes of hosts and routers to communicate with one another; for example, host-host, host-router, and router-router are all common SLIP network configurations. SLIP is merely a packet framing protocol: It defines a sequence of characters that frame IP packets on a serial line. It does not provide addressing, packet type identification, error detection or correction, or compression mechanisms.

Advantages

- Since it has a small overhead, it is suitable for usage in microcontrollers.
- It reuses existing dial-up connections and telephone lines.
- It's easy to deploy since it's based on the Internet Protocol.

Disadvantages

- SLIP doesn't support automatic setup of network connections in multiple OSI layers at the same time.
- SLIP does not support synchronous connections, such as a connection created through the internet from a modem to an internet service provider (ISP).

OSI Model : (Open System Interconnection)

- OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- The Main Purpose of OSI Model is to connect heterogenous systems.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.

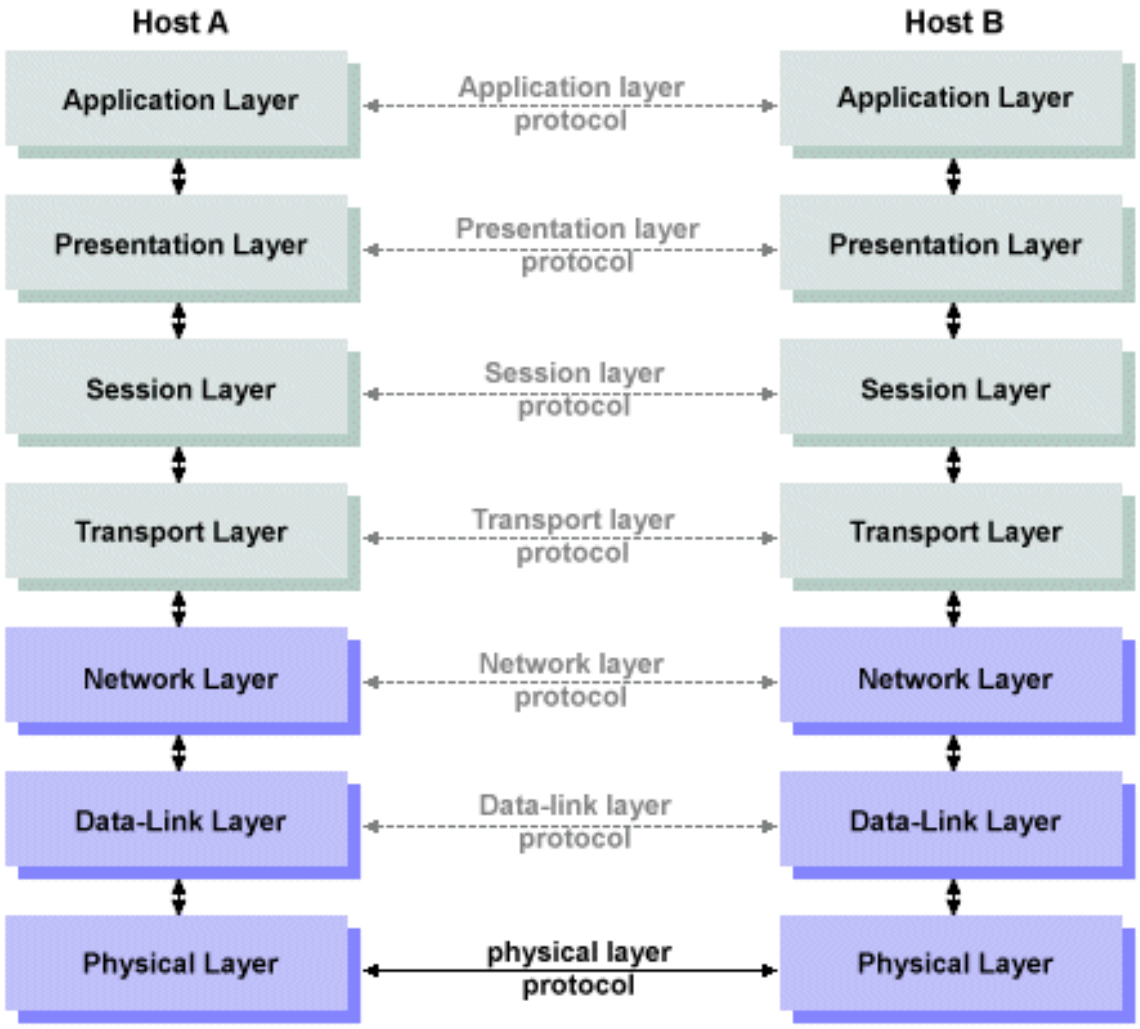


Fig. OSI Model

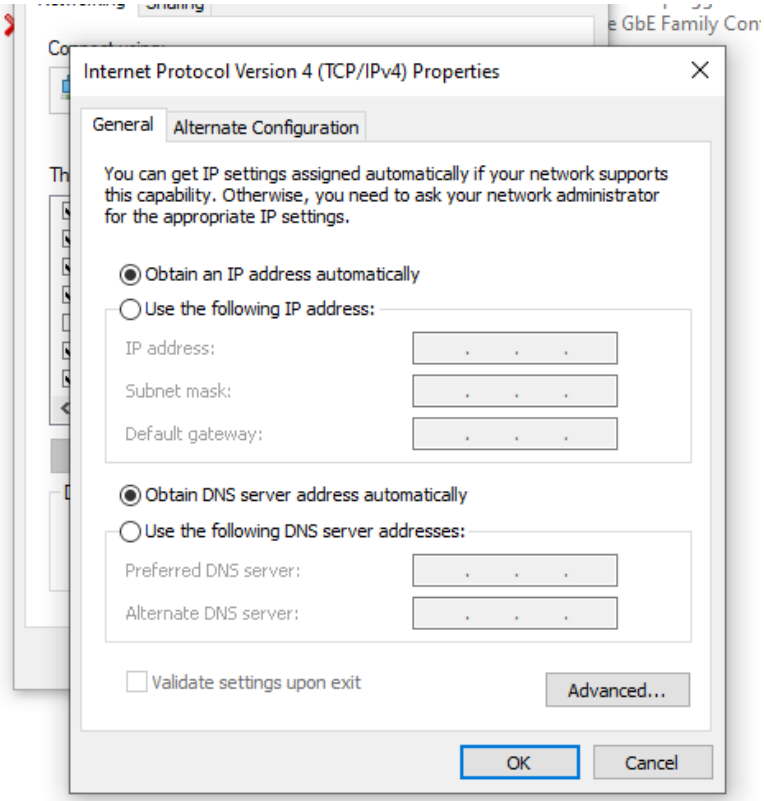
These are the seven layers of the OSI model −

- **Physical layer** −It is the first layer that physically connects the two systems that need to communicate. It transmits data in bits and manages simplex or duplex transmission by modem. It also manages Network Interface Card's hardware interface to the network, like cabling, cable terminators, topography, voltage levels, etc.

- **Data link layer** − It is the firmware layer of Network Interface Card. It assembles datagrams into frames and adds start and stop flags to each frame. It also resolves problems caused by damaged, lost or duplicate frames.
- **Network layer** − It is concerned with routing, switching and controlling flow of information between the workstations. It also breaks down transport layer datagrams into smaller datagrams.

- **Transport layer** − Till the session layer, file is in its own form. Transport layer breaks it down into data frames, provides error checking at network segment level and prevents a fast host from overrunning a slower one. Transport layer isolates the upper layers from network hardware.

- **Session layer** − This layer is responsible for establishing a session between two workstations that want to exchange data.

- **Presentation layer** − This layer is concerned with correct representation of data, i.e. syntax and semantics of information. It controls file level security and is also responsible for converting data to network standards.

- **Application layer** − It is the topmost layer of the network that is responsible for sending application requests by the user to the lower levels. Typical applications include file transfer, E-mail, remote logon, data entry, etc.