Computer Network

A computer network is a collection of interconnected devices that share resources and information.

- **Network:** A network is a collection of computers and devices that are connected together to enable communication and data exchange.
- **Nodes:** Nodes are devices that are connected to a network. These can include computers, Servers, Printers, Routers, Switches, and others
- **Protocol:** A protocol is a set of rules and standards that govern how data is transmitted over a network. Examples TCP/IP, HTTP, and FTP.
- **Topology:** Network topology refers to the physical and logical arrangement of nodes on a network. The common network topologies include bus, star, ring, mesh, and tree.
- **Service Provider Networks:** These types of Networks give permission to take Network Capacity and Functionality on lease from the Provider. Service Provider Networks include Wireless Communications, Data Carriers, etc.
- **IP Address**: An IP address is a unique numerical identifier that is assigned to every device on a network. IP addresses are used to identify devices and enable communication between them.
- **DNS:** The Domain Name System (DNS) is a protocol that is used to translate human-readable domain names (such as www.google.com) into IP addresses that computers can understand.
- **Firewall:** A firewall is a security device that is used to monitor and control incoming and outgoing network traffic. Firewalls are used to protect networks from unauthorized access and other security threats.
- **LAN:** A Local Area Network (LAN) is a network that covers a small area, such as an office or a home. LANs are typically used to connect computers and other devices within a building or a campus.
- **WAN:** A Wide Area Network (WAN) is a network that covers a large geographic area, such as a city, country, or even the entire world. WANs are used to connect LANs together and are typically used for long-distance communication.
- **Cloud Networks:** Cloud Networks can be visualized with a Wide Area Network (WAN) as they can be hosted on public or private cloud service providers and cloud networks are available if there is a demand. Cloud Networks consist of Virtual Routers, Firewalls, etc.

Types of Physical Components

1. NIC(Network Interface Card)

NIC or Network Interface Card is a network adapter used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique ID that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and the router or modem. NIC card is a layer 2 device, which means it works on the network model's physical and data link layers.

2. HUB

A hub is a multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through hub remains one. Hub does not have any routing table to store the data of ports and map destination addresses., the routing table is used to send/broadcast information across all the ports.

Types of HUB

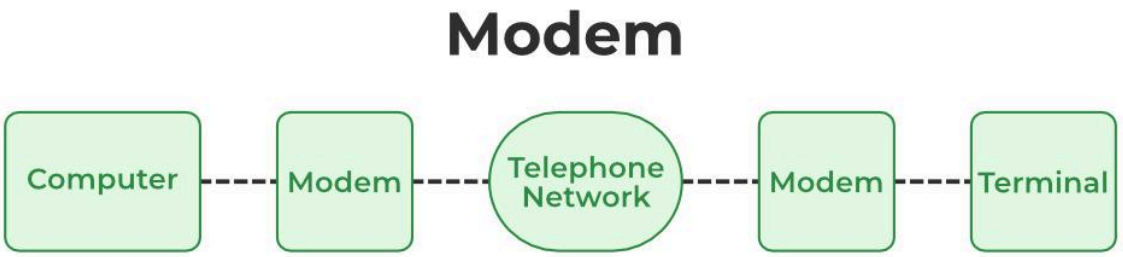
- **Active HUB:** Active HUB regenerates and amplifies the electric signal before sending them to all connected device. This hub is suitable to transmit data for long distance connections over the network.
- **Passive HUB:** As the name suggests it does not amplify or regenerate electric signal, it is the simplest types of Hub among all and it is not suitable for long-distnace connections.
- **Switching HUB:** This is also known as intelligent HUB, they provide some additional functionality over active and passive hubs. They analyze data packets and make decisions based on MAC address and they are operated on DLL(Data Link Layer).

3. Router

A Router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.

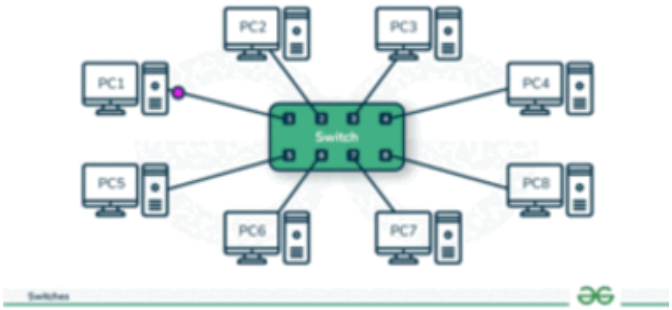
4. Modem

A Modem is a short form of Modulator/Demodulator. The Modem is a hardware component/device that can connect computers and other devices such as routers and switches to the internet. Modems convert or modulate the analog signals coming from telephone wire into a digital form that is in the form of 0s and 1s.



5. Switch(datalink)

A Switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports implies less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only.



6. Nodes

Node is a term used to refer to any computing devices such as computers that send and receive network packets across the network.

7. Media

It is also known as Link which is going to carry data from one side to another side. This link can be Wired Medium (Guided Medium) and Wireless Medium (Unguided Medium). It is of two types:

8. Repeater

Repeater is an important component of computer networks as it is used to regenerate and amplify signal in the computer networks. Repeaters are used to improve the quality of the networks and they are operated on the Physical Layer of the OSI Model.physical layer.

9. Server

A server is a computer program that provides various functionality to another computer program. The server plays a vital role in facilitating communication, data storage, etc. Servers have more data storage as compared to normal computers. They are designed for the specific purpose of handling multiple requests from clients.

10. Bridge – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

Types of Computer Networks

1. Personal Area Network (PAN)

It is a type of network designed to connect devices within a short range, typically around one person.PAN offers a network range of 1 to 100 meters from person to device providing communication. Its transmission speed is very high with very easy maintenance and very low cost. This uses Bluetooth, IrDA, and Zigbee as technology. Examples of PAN are USB, computer, phone, tablet, printer, PDA, etc.

2. Local Area Network (LAN)

A LAN is a computer network that connects computers through a common communication path, contained within a limited area, that is, locally. A LAN encompasses two or more computers connected over a server. The two important technologies involved in this network are Ethernet and Wi-fi. It ranges up to 2km & transmission speed is very high with easy maintenance and low cost. Examples of LAN are networking in a home, school, library, laboratory, college, office, etc.

3. Campus Area Network (CAN)

This network covers a limited geographical area that is, it spreads across several buildings within the campus. CAN mainly use Ethernet technology with a range from 1km to 5km. Its transmission speed is very high with a moderate maintenance cost and moderate cost. Examples of CAN are networks that cover schools, colleges, buildings, etc.

4. Metropolitan Area Network (MAN)

This is the type of computer network that connects computers over a geographical distance through a shared communication path over a city, town, or metropolitan area. This network mainly uses FDDI, CDDI, and ATM as the technology with a range from 5km to 50km. Its transmission speed is average.

5. Wide Area Network (WAN)

WAN is a type of computer network that connects computers over a large geographical distance through a shared communication path. It is not restrained to a single location but extends over many locations. WAN can also be defined as a group of local area networks that communicate with each other with a range above 50km. Here we use Leased-Line & Dial-up technology.

Parameters	PAN	LAN	CAN	MAN	WAN
Full Name	Personal Area Network	Local Area Network	Campus Area Network	Metropolitan Area Network	Wide Area Network
Technology	Bluetooth, IrDA,Zigbee	Ethernet & Wifi	Ethernet	FDDI, CDDi. ATM	Leased Line, Dial-Up
Range	1-100 m	Upto 2km	1 – 5 km	5-50 km	Above 50 km
Transmission Speed	Very High	Very High	High	Average	Low
Ownership	Private	Private	Private	Private or Public	Private or Public
Maintenance	Very Easy	Easy	Moderate	Difficult	Very Difficult
Cost	Very Low	Low	Moderate	High	Very High

Local Area Network

A router serves as the hub where the majority of LANs connect to the Internet. Home LANs often utilise a single router, but bigger LANs may also use network switches to transmit packets more effectively.

Types of LAN

- **Client/Server LANs:** Multiple devices (the clients) are connected to a main server in a client/server LAN. The server controls network traffic, device access, application access, and file storage. Any connected device that runs apps or accesses the Internet qualifies as a client. Clients can use wired or wireless connections to connect to the server.
- **Peer-to-Peer LANs:** Peer-to-peer LANs are commonly smaller because they shortage a central server and can't support huge workloads like client/server LANs can. Every device on a peer-to-peer LAN collaborates equally to the network's operation. Through wired or wireless connections to a switch or router, the devices share data and resources. Peer-to-peer networks are the norm in homes.
- **Ethernet:** It is most widely used archetecture. ethernet specifies the network speed, cable type and network interface adapters. This type of architecture used in both wired or wireless networks.
- **Token ring:** Token ring is a type of local area network (LAN) setup that was once widely used but is now less common. It manages network access through the use of tokens and has an operating speed of 100 megabits per second.
- **Cloud-managed:** A cloud-managed LAN depend on a centralized cloud service to handle tasks such as access control, policy enforcement, network setup, and various security and performance issues. This approach simplifies management in diverse network environments, making it ideal for businesses.
- **Virtual LAN**

Imagine establishing two independent LANs in the same room, each with its own router and Internet connection. Similar to that, but with only one router and one Internet connection required, VLANs divide networks virtually rather than physically.

Equipment is Needed to Set up a LAN

- **Router:-** This is the central device that is used to connect the LAN to the internet.
- **Modem:-** This it required only if connecting to the internet. Modem convert the signals from your Internet Service Provider (ISP) to a router usable.
- **Switch (optional for larger networks):-** Used to expands the number of devices that can be connected to the LAN.
- **Ethernet Cables:-** It is used to connect devices to the router or switch.
- **Network Interface Cards (NICs)**:- It is required for each devices that is connect to the LAN through Ethernet.
- **Wireless Access Point (if wireless connectivity is needed):-** Allows wireless devices to connect to the LAN.
- **Devices**:- Device you want to connect like Laptop, Computers, smartphones, tablets, smart TVs, and other devices.

MAN

LANs are connected using the single-mode optical fiber lines, which results in the creation of metropolitan area network(MAN) to provide the interconnection of LANs efficiently.The purpose of MAN is to provide a communication link between two independent LANs

Process of MAN Network Constructed

1. Network infrastructure

- Core Layer
  The core of MAN is usually designed using high-capacity fiber optic cables.They form the central hub of the network interconnecting several parts and powerful router and parts and switches are used to control data flow and routing within the MAN.

2. Connection to local area network (LANs)

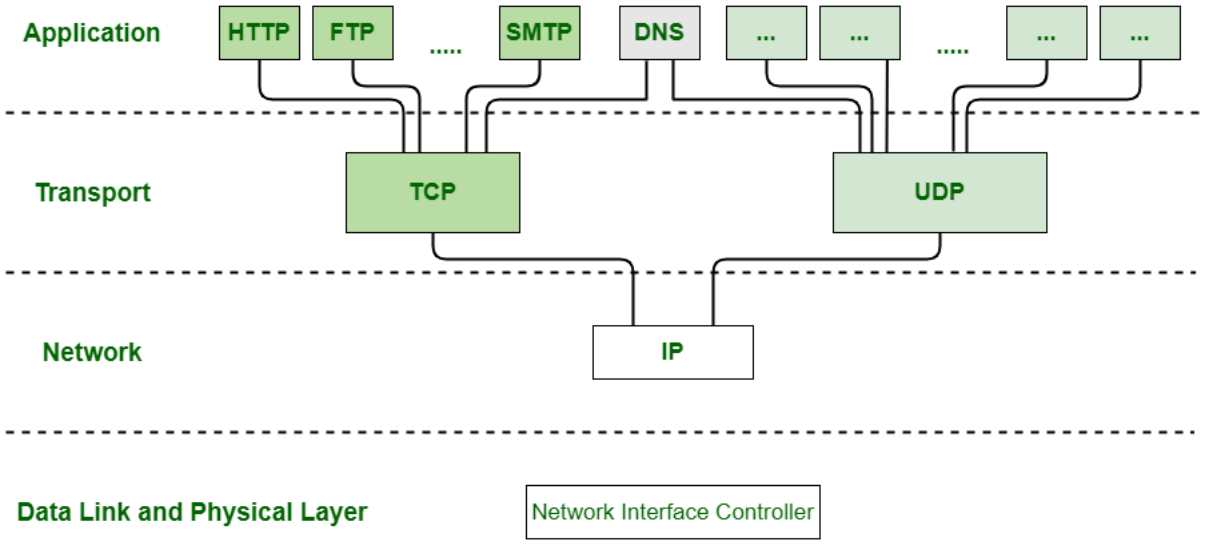
WAN

A WAN (Wide Area Network) is to connect multiple smaller Local Area Networks (LANs) or MANs.

Internetworking

Internetworking is combined of 2 words, inter and networking which implies an association between totally different nodes or segments.Internetworking is enforced in Layer three (Network Layer) of the OSI-ISO model.

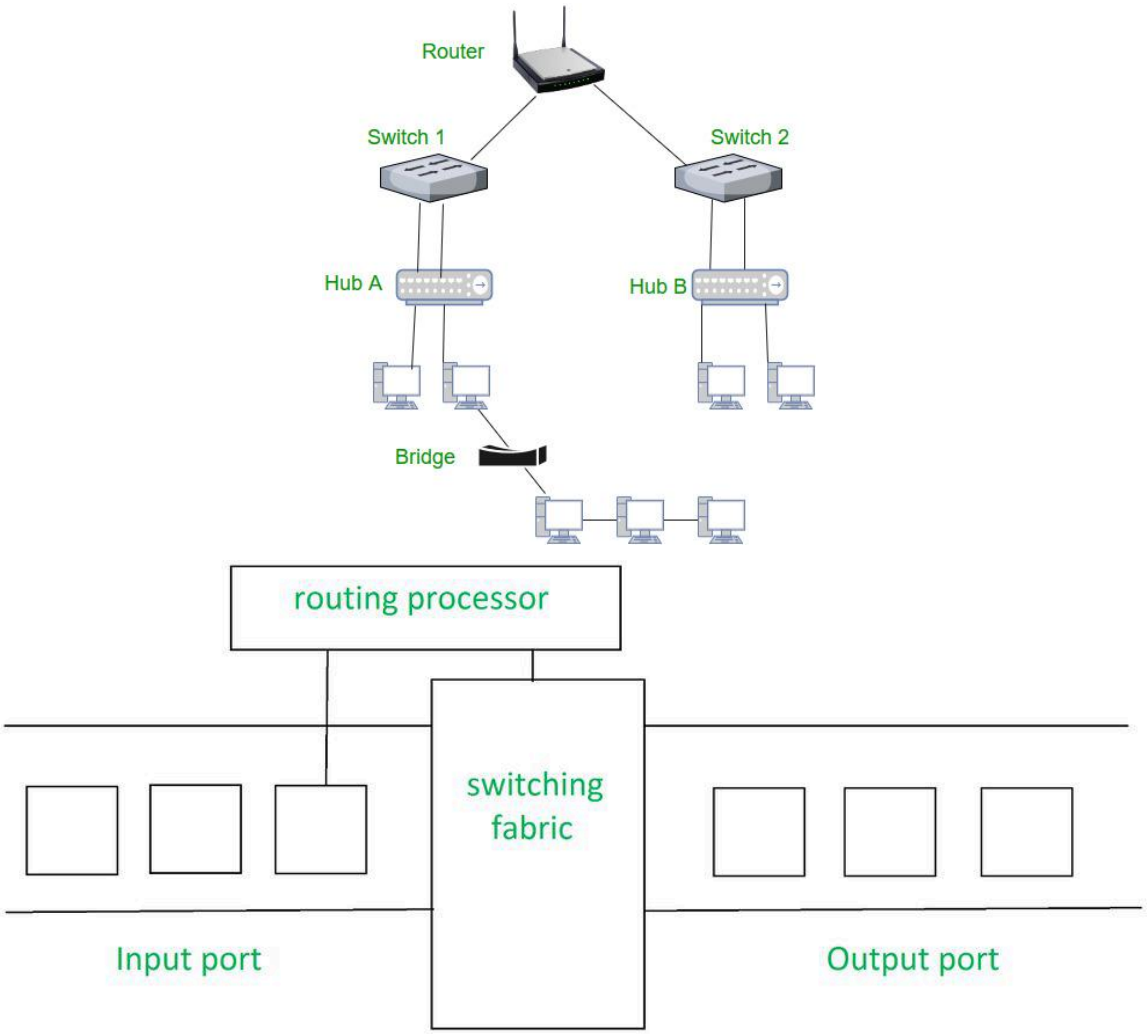
- **Internet:**
  A public network that connects computers worldwide, allowing people to access websites, send emails, and share information.
- **Intranet:**
  A private network within an organization, used for internal communication and sharing resources like documents.
- **Extranet:**
  A private network that allows limited access to external partners, enabling secure collaboration between businesses.



Router

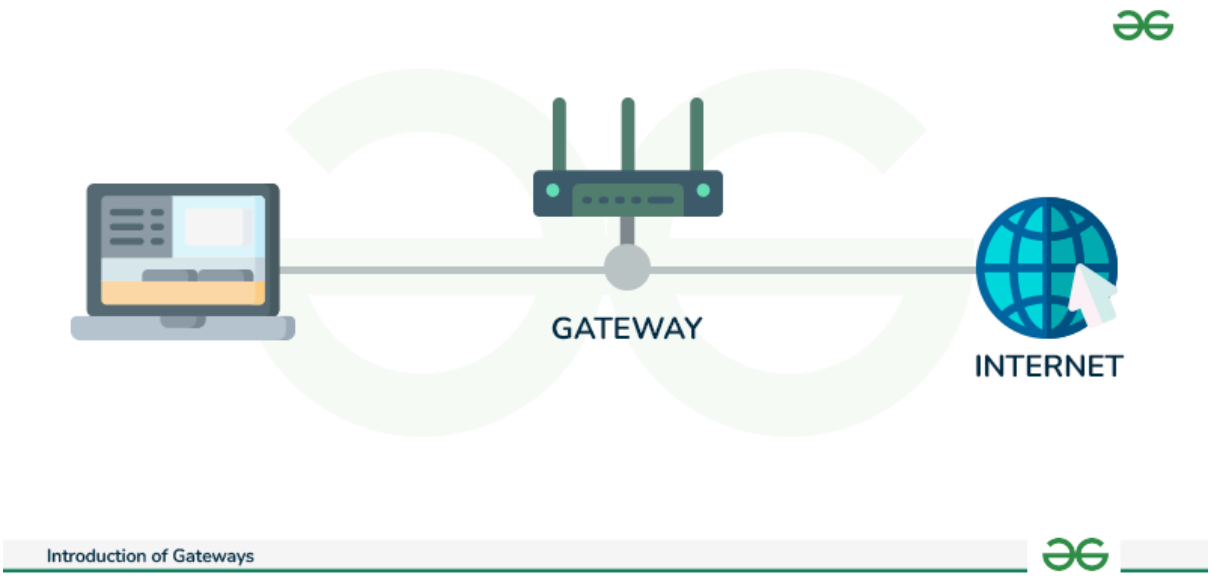
A Router is a networking device that forwards data packets between computer networks. One or more packet-switched networks or subnetworks can be connected using a router. By sending data packets to their intended IP addresses, it manages traffic between different networks and permits several devices to share an Internet connection.

A router determines a packet's future path by examining the destination IP address of the header and comparing it to the routing database. The list of routing tables outlines how to send the data to a specific network location. They use a set of rules to determine the most effective way to transmit the data to the specified IP address.



Gateways

A network gateway is a device that connects different networks by translating messages from one protocol into another protocol. The gateway monitors and controls all the incoming and outgoing network traffic.



Network Switch

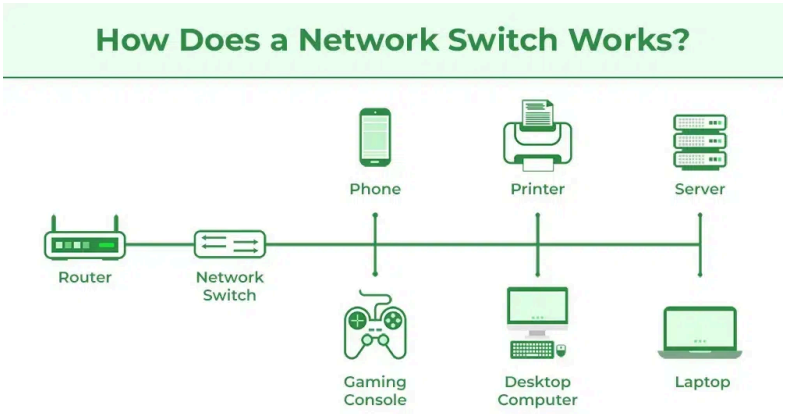
- The Switch is a network device that is used to segment the networks into different subnetworks called subnets or LAN segments. It is responsible for filtering and forwarding the packets between LAN segments based on MAC address.
- Switches are one of the most important things for transferring information between different endpoints.
- Switches are having full-duplex communication which helps in making effective use of bandwidth.

Layer 2 Switch

A Layer 2 switch operates at Layer 2 of OSI model, which is the Data Link Layer. The switch forwards data packets depending on the devices' MAC (Media Access Control) addresses that are in its network.

Layer 3 Switch

A Layer 3 Switch is identical to an ordinary switch in its operation with a router at the same time, working at both data link layer (Layer 2) and network layer (Layer 3) under the Open Systems Interconnection model. Layer 3 switches can route packets between diverse subnets or VLANs (virtual LANs) with the application of IP addresses



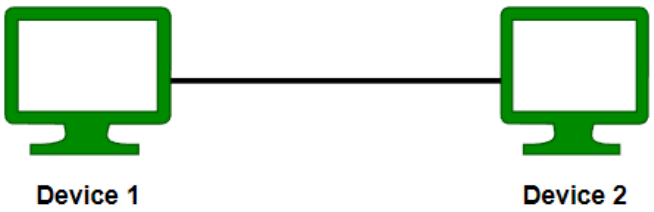
When the source wants to send the data packet to the destination, the packet first enters the switch and the switch reads its header and finds the MAC address of the destination to identify the device then it sends the packet out through the appropriate ports that lead to the destination devices.

Switch establishes a temporary connection between the source and destination for communication and terminates the connection once the conversation is done

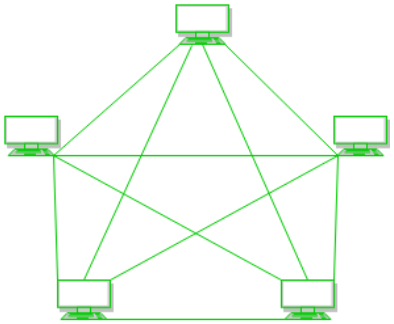
Network Topology

Network topology refers to the arrangement of different elements like nodes, links, or devices in a computer network. It defines how these components are connected and interact with each other.

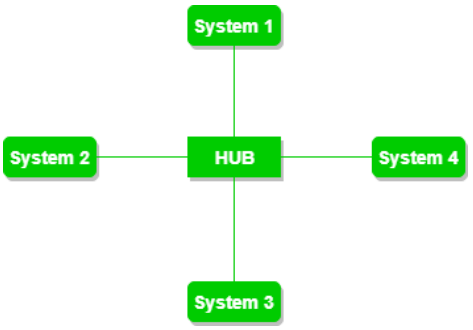
Point to Point Topology



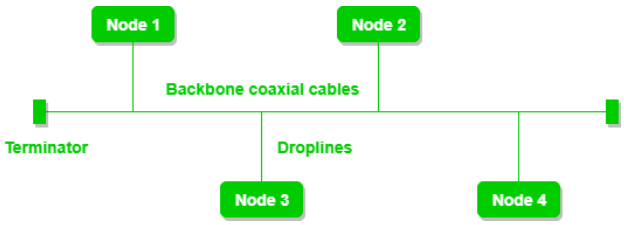
Mesh Topology



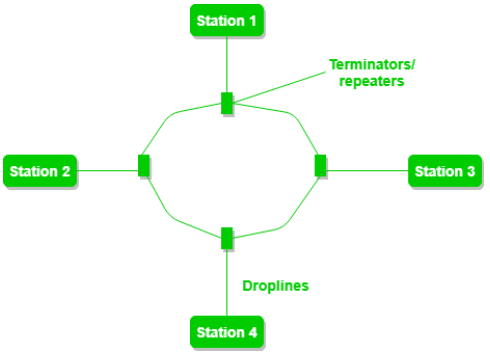
Star Topology



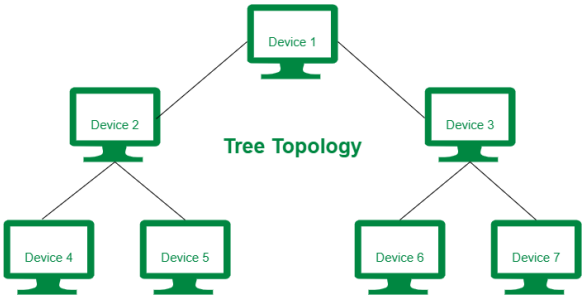
Bus Topology



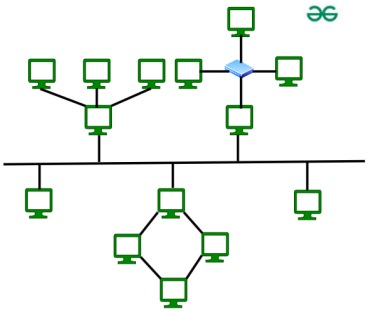
Ring Topology



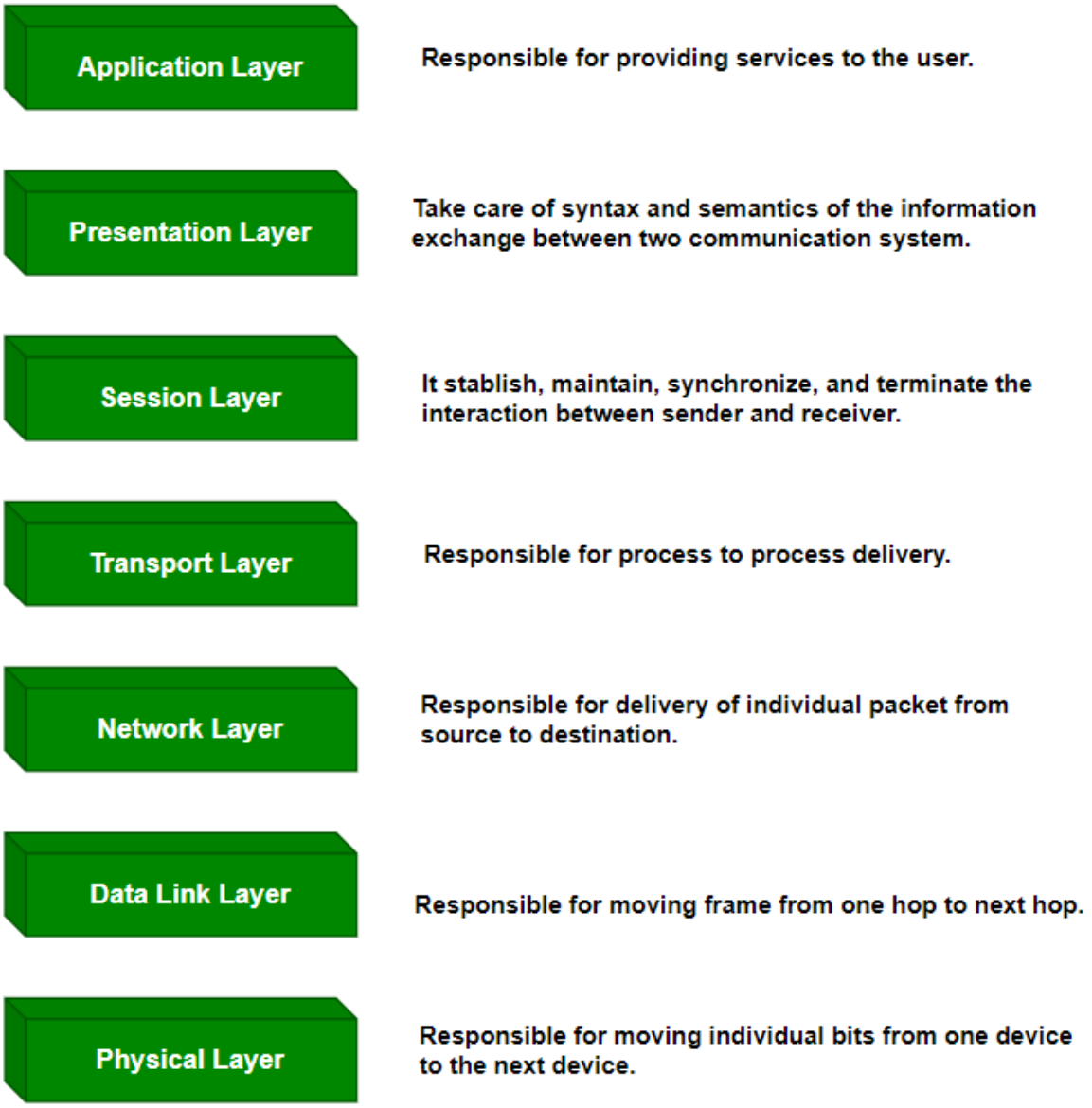
Tree Topology



Hybrid Topology



OSI Model



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

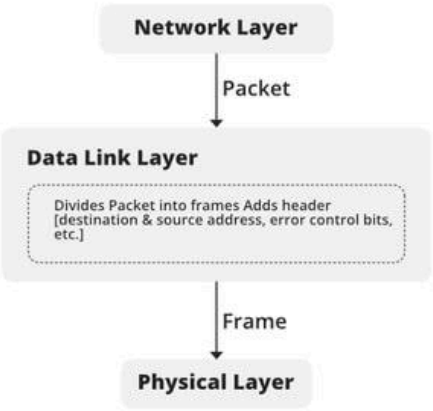
Physical Layer

It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.** It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

Functions of the Physical Layer Bit Synchronization , Bit Rate Control , Physical Topologies , Transmission Mode

Data Link Layer

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address .The packet received from the Network layer is further divided into frames depending on the frame size of the NIC(Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.



Network Layer

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP address es are placed in the header by the network layer.

Functions

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

Transport Layer

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as *Segments* . It is responsible for the end-to-end delivery of the complete message. The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

At the sender's side: The transport layer receives the formatted data from the upper layers, performs **Segmentation** , and also implements **Flow and error control** to ensure proper data transmission. It also adds Source and Destination port number s in its header and forwards the segmented data to the Network Layer.

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

Functions of the Transport Layer

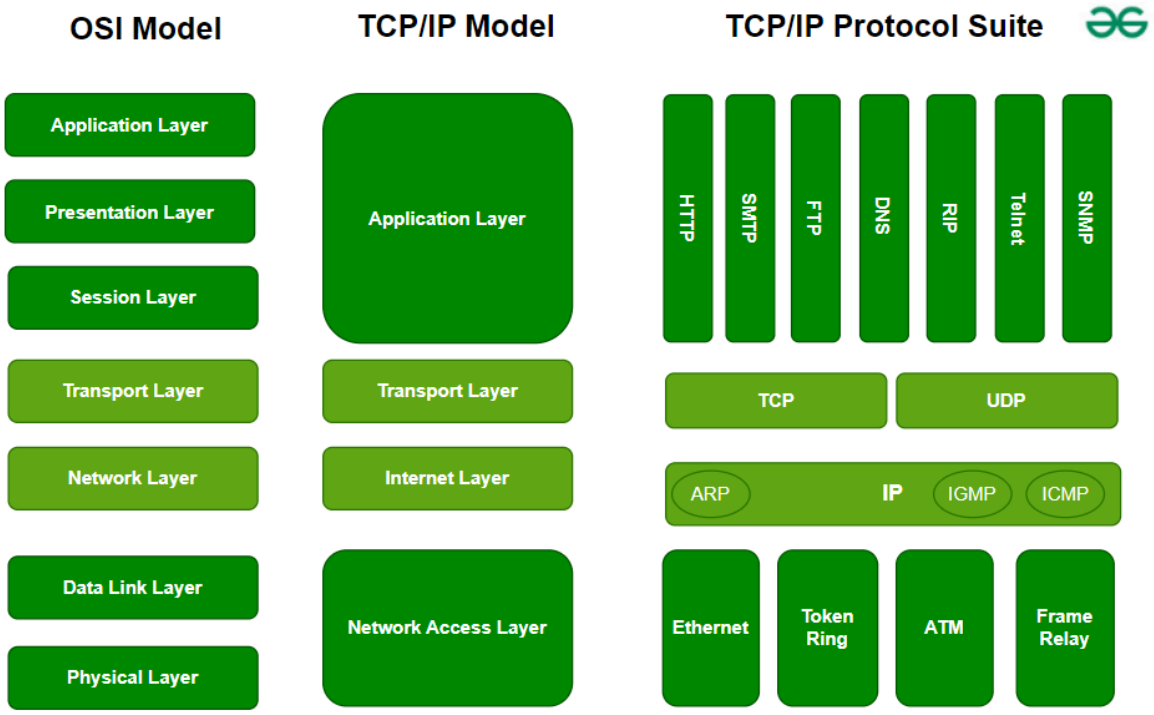
- **Segmentation and Reassembly:** This layer accepts the message from the (session) layer, and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
- **Service Point Addressing:**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

1. Connection-Oriented Service: It is a three-phase process that includes: Connection Establishment , Data Transfer , Termination/disconnection
In this type of transmission, the receiving device sends an acknowledgment, back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.

2. Connectionless service: It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

Layer No	Layer Name	Responsibility	Information Form (Data Unit)	Device or Protocol
7	Application Layer	Helps in identifying the client and synchronizing communication.	Message	SMTP
6	Presentation Layer	Data from the application layer is extracted and manipulated in the required format for transmission.	Message	JPEG , MPEG , GIF
5	Session Layer	Establishes Connection, Maintenance, Ensures Authentication and Ensures security.	Message (or encrypted message)	Gateway
4	Transport Layer	Take Service from Network Layer and provide it to the Application Layer.	Segment	Firewall

3	Network Layer	Transmission of data from one host to another, located in different networks.	Packet	Router
2	Data Link Layer	Node to Node Delivery of Message.	Frame	Switch , Bridge
1	Physical Layer	Establishing Physical Connections between Devices.	Bits	Hub , Repeater , Modem , Cables



Physical Layer

1. The physical layer maintains the data rate
2. It helps in Physical Topology (Mesh, Star, Bus, Ring) decisions
3. It helps in providing Physical Medium and Interface decisions.
4. It provides two types of configuration Point Point configuration and Multi-Point configuration.It has a protocol data unit in bits.
5. Hubs, Ethernet, etc. device is used in this layer.
6. This layer comes under the category of Hardware Layers
7. It provides an important aspect called Modulation, which is the process of converting the data into radio waves by adding the information to an electrical or optical nerve signal.
8. It also provides a Switching mechanism wherein data packets can be forwarded from one port (sender port) to the leading destination port.

Line Configuration

- **Point-to-Point configuration:** In Point-to-Point configuration, there is a line (link) that is fully dedicated to carrying the data between two devices.
- **Multi-Point configuration:** In a Multi-Point configuration, there is a line (link) through which multiple devices are connected.

Modes of Transmission Medium

1. **Simplex mode:** In this mode, out of two devices, only one device can transmit the data, and the other device can only receive the data. Example- Input from keyboards, monitors, TV broadcasting, Radio broadcasting, etc.
2. **Half Duplex mode:** In this mode, out of two devices, both devices can send and receive the data but only one at a time not simultaneously. Examples- Walkie-Talkie, Railway Track, etc.
3. **Full-Duplex mode:** In this mode, both devices can send and receive the data simultaneously. Examples- Telephone Systems, Chatting applications, etc.

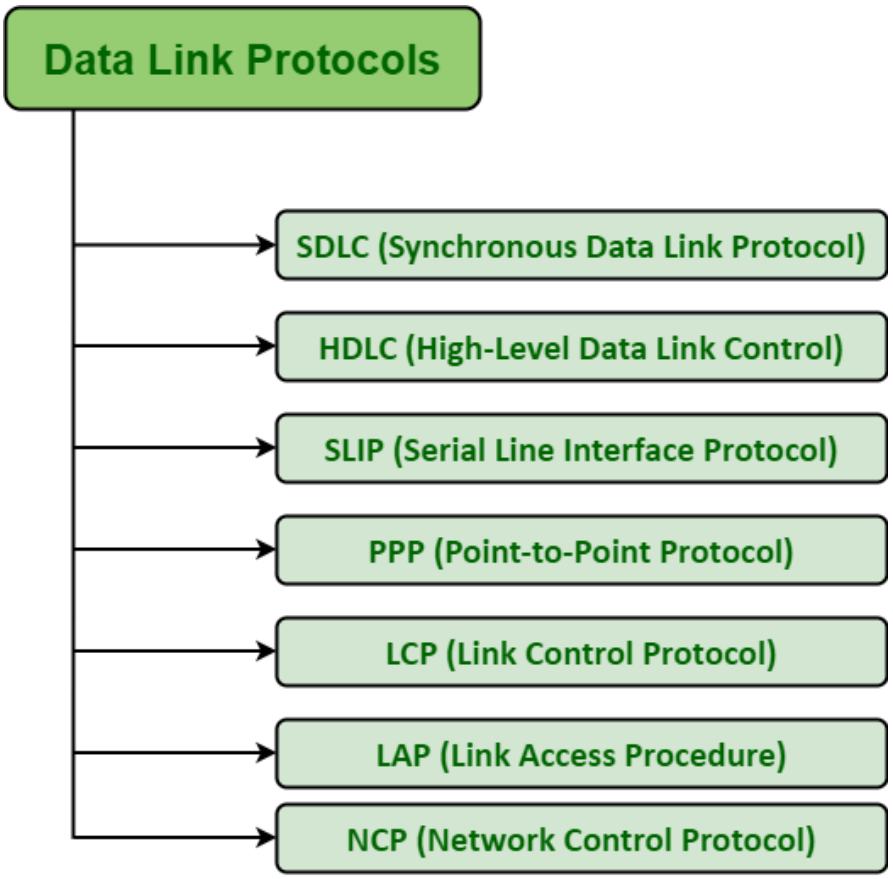
Data Link Layer

Framing

The packet received from the Network layer is known as a frame in the Data link layer. At the sender's side, DLL receives packets from the Network layer and divides them into small frames, then, sends each frame bit-by-bit to the physical layer. It also attaches some special bits (for error control and addressing) at the header and end of the frame. At the receiver's end, DLL takes bits from the Physical layer organizes them into the frame, and sends them to the Network layer.

Addressing

The data link layer encapsulates the source and destination's MAC address/ physical address in the header of each frame to ensure node-to-node delivery. MAC address is the unique hardware address that is assigned to the device while manufacturing.



Protocol

A protocol is a set of rules that determines how data is sent and received over a network.

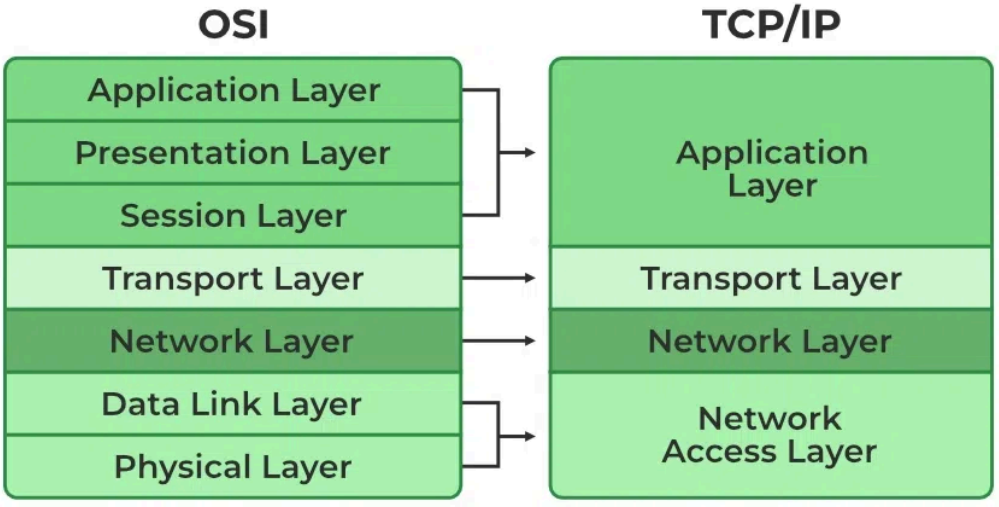
- **TCP (Transmission Control Protocol):** Ensures data is sent and received accurately by breaking it into packets, sending them, and reassembling them at the destination.
- **IP (Internet Protocol):** Addresses and routes the packets to make sure they reach the right destination.
- **HTTP/HTTPS (HyperText Transfer Protocol/Secure):** HTTP used for transferring web pages on the internet. When you browse a website, your browser uses HTTP to request and display web pages. And HTTPs is a secure version of HTTP that encrypts data to protect it from being intercepted.
- **FTP (File Transfer Protocol):** Used for transferring files between computers on a network. It allows users to upload and download files.
- **SMTP (Simple Mail Transfer Protocol):** Used for sending emails. It transfers emails from a client to a server or between servers.
- **DNS (Domain Name System):** It is used to translates human-readable domain names (like www.example.com) into IP addresses that computers use to identify each other on the network.
- **DHCP (Dynamic Host Configuration Protocol):** Automatically assigns IP addresses to devices on a network, ensuring each device has a unique address.
- **SSH (Secure Shell):** Provides a secure way to access and manage devices over a network. It encrypts the data, making it safe from eavesdropping.
- **SNMP (Simple Network Management Protocol):** Used for managing and monitoring network devices like routers, switches, and servers. It collects and organizes information about these devices

TCP/IP Model Transmission Control Protocol/Internet Protocol

This model defines how data is transmitted over networks, ensuring reliable communication between devices. It consists of four layers: the Link Layer, the Internet Layer, the Transport Layer, and the Application Layer.

Whenever we want to send something over the internet using the TCP/IP Model, the TCP/IP Model divides the data into packets at the sender's end and the same packets have to be recombined at the receiver's end to form the same data, and this thing happens to maintain the accuracy of the data.

Layers



1. Network Access Layer

It is a group of applications requiring network communications. This layer is responsible for generating the data and requesting connections. It acts on behalf of the sender and the Network Access layer on the behalf of the receiver.

2. Internet or Network Layer

It defines the protocols which are responsible for the logical transmission of data over the entire network.

- **IP:** IP stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions: IPv4 and IPv6. IPv4 is the one that most websites are using currently. But IPv6 is growing as the number of IPv4 addresses is limited in number when compared to the number of users.
- **ICMP:** ICMP stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
- **ARP:** ARP stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP, and Inverse ARP.

3. Transport Layer

The TCP/IP transport layer protocols exchange data receipt acknowledgments and retransmit missing packets to ensure that packets arrive in order and without error.Transmission Control Protocol (TCP) and User Datagram Protocol are transport layer protocols at this level (UDP).

- **TCP:** Applications can interact with one another using TCP as though they were physically connected by a circuit. TCP transmits data in a way that resembles character-by-character transmission rather than separate packets. A starting point that establishes the connection, the whole transmission in byte order, and an ending point that closes the connection make up this transmission.

- **UDP:** The datagram delivery service is provided by UDP, the other transport layer protocol. Connections between receiving and sending hosts are not verified by UDP. Applications that transport little amounts of data use UDP rather than TCP because it eliminates the processes of establishing and validating connections.

4. Application Layer

It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The three main protocols present in this layer are:

- **HTTP and HTTPS:** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser needs to fill out forms, sign in, authenticate, and carry out bank transactions.
- **SSH:** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
- **NTP:** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it's out of sync.

The physical layer is not covered by the TCP/IP model because the data link layer is considered the point at which the interface occurs between the TCP/IP stock and the underlying network hardware. Also, it is designed to be independent of the underlying physical media. This allows TCP/IP to be flexible and adaptable to different types of physical connections

TCP/IP Ports

A port is the logical address of any protocol; alternatively, we might think of a port as a special door for each protocol, through which all packets are routed.

Types of Port

By using ports, the computer is able to distinguish between all incoming traffic, including web pages and emails that flow to separate ports. Let's now examine several port number ranges after determining the port number.

1. Well Known Port

- Known as system ports or well-known ports, ports 0 through 1023 are specifically linked to specific services.
- It is set aside for frequently utilised and specific services.
- Certain commonly used protocols and services, such as HTTP (port 80), HTTPS(port 443), DNS (port 53), and SSH (port 22), use it.

2. Registered Port

- The Internet Assigned Numbers Authority allows ports in the range of 1024 to 49151 to be registered for a particular purpose.
- These ports are referred to as registered ports.These are utilised by fewer apps or services, but they are utilised by those that need the particular port.
- Organisations can request any specific port number in this range from IANA (Internet Assigned Number Authority).

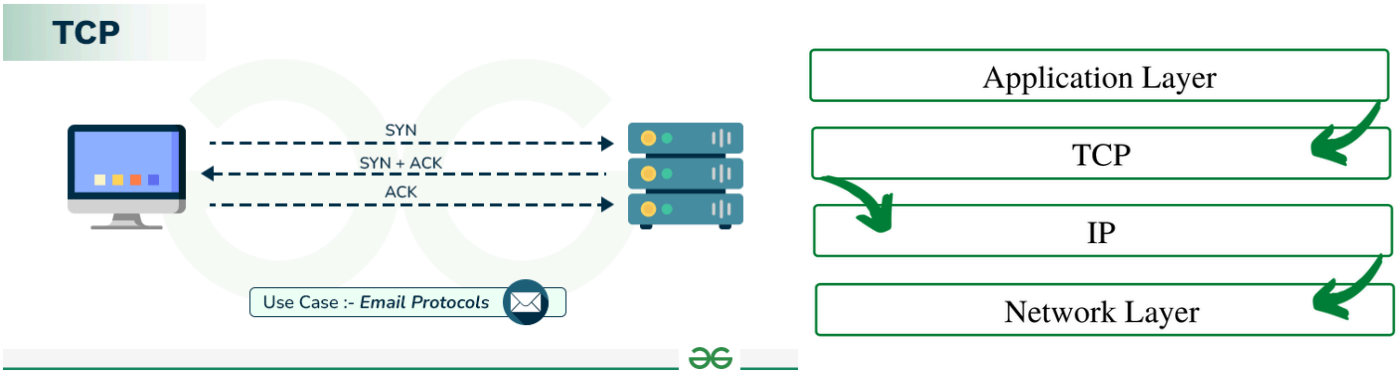
3. Dynamic Port

- Unassigned ports, often known as dynamic or ephemeral ports, are those that range from 49152 to 65535 and can be used for any kind of service.
- It is employed for transient or fleeting connections.
- It can be utilised by any process and is not registered nor assigned.

Transmission Control Protocol (TCP)

Transmission Control Protocol (TCP) is a **connection-oriented protocol for communications** that helps in the exchange of messages between different devices over a network. The Internet Protocol (IP), which establishes the technique for sending data packets between computers, works with TCP.The position of TCP is at the transport layer of the OSI model.

Transmission Control Protocol (TCP) model breaks down the data into small bundles and afterward reassembles the bundles into the original message on the opposite end to make sure that each message reaches its target location intact. Sending the information in little bundles of information makes it simpler to maintain efficiency as opposed to sending everything in one go.

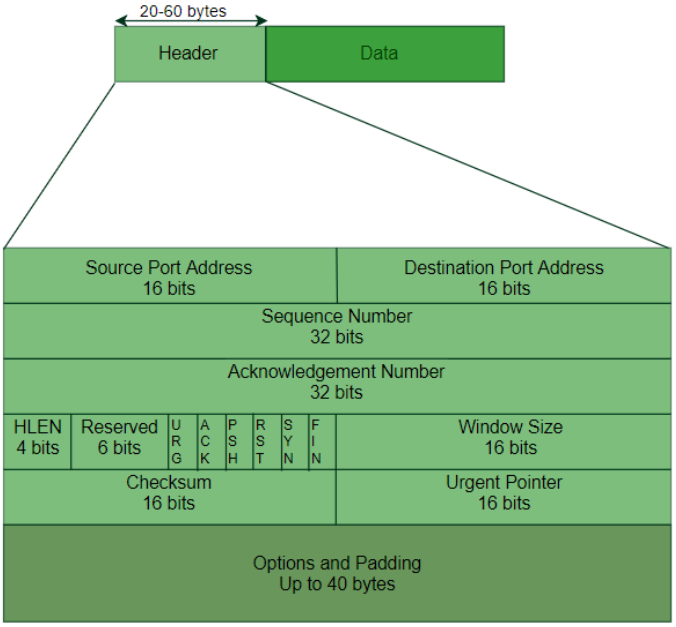


Internet Protocol (IP)

Internet Protocol (IP) is a method that is useful for sending data from one device to another from all over the internet. It is a set of rules governing how data is sent and received over the internet. It is responsible for addressing and routing packets of data so they can travel from the sender to the correct destination across multiple networks. Every device contains a unique IP Address that helps it communicate and exchange data across other devices present on the internet.

TCP 3-Way Handshake Process

The TCP 3-Way Handshake is a fundamental process that establishes a reliable connection between two devices over a TCP/IP network. It involves three steps: SYN (Synchronize), SYN-ACK (Synchronize-Acknowledge), and ACK (Acknowledge). During the handshake, the client and server exchange initial sequence numbers and confirm the connection establishment.

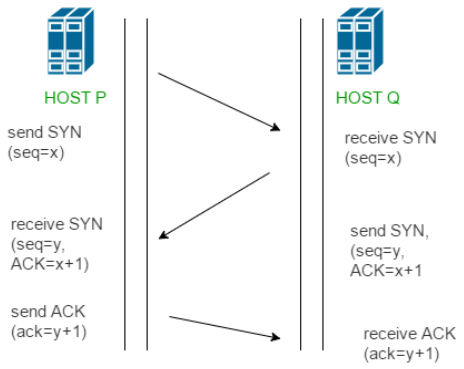


The header of a TCP segment can range from 20-60 bytes. 40 bytes are for options. If there are no options, a header is 20 bytes else it can be of upmost 60 bytes. Header fields:

- **Source Port Address:** A 16-bit field that holds the port address of the application that is sending the data segment.
- **Destination Port Address:** A 16-bit field that holds the port address of the application in the host that is receiving the data segment.
- **Sequence Number:** A 32-bit field that holds the sequence number , i.e, the byte number of the first byte that is sent in that particular segment. It is used to reassemble the message at the receiving end of the segments that are received out of order.
- **Acknowledgement Number:** A 32-bit field that holds the acknowledgement number, i.e, the byte number that the receiver expects to receive next. It is an acknowledgement for the previous bytes being received successfully.

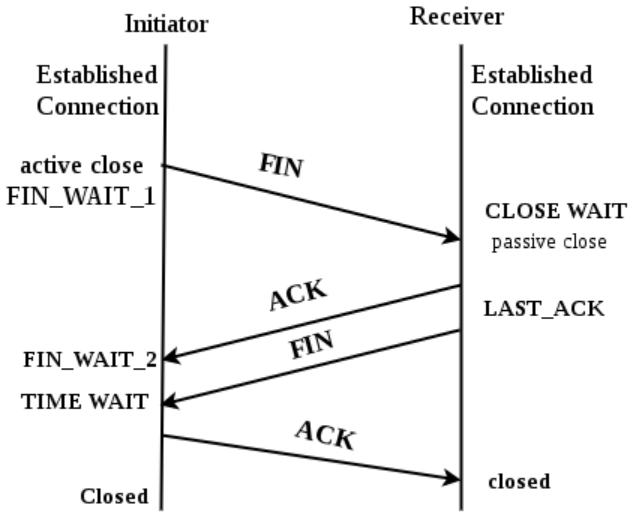
- **Header Length (HLEN):** This is a 4-bit field that indicates the length of the TCP header by a number of 4-byte words in the header, i.e if the header is 20 bytes(min length of TCP header), then this field will hold 5 (because 5 x 4 = 20) and the maximum length: 60 bytes, then it'll hold the value 15(because 15 x 4 = 60). Hence, the value of this field is always between 5 and 15.
- **Control flags:** These are 6 1-bit control bits that control connection establishment, connection termination, connection abortion, flow control, mode of transfer etc. Their function is:
    - URG: Urgent pointer is valid
    - ACK: Acknowledgement number is valid(used in case of cumulative acknowledgement)
    - PSH: Request for push
    - RST: Reset the connection
    - SYN: Synchronize sequence numbers
    - FIN: Terminate the connection
- **Window size:** This field tells the window size in bytes.
- **Checksum:** This field holds the checksum for error control .
- **Urgent pointer:** This field (valid only if the URG control flag is set) is used to point to data that is urgently required that needs to reach the receiving process at the earliest. The value of this field is added to the sequence number to get the byte number of the last urgent byte.

- **Step 1 (SYN):** In the first step, the client wants to establish a connection with a server, so it sends a segment with SYN(Synchronize Sequence Number) which informs the server that the client is likely to start communication and with what sequence number it starts segments with
- **Step 2 (SYN + ACK):** Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segments with
- **Step 3 (ACK):** In the final part client acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer



TCP supports two types of connection releases like most connection-oriented transport protocols:

1. **Graceful connection release –**
   In the Graceful connection release, the connection is open until both parties have closed their sides of the connection.



2. **Abrupt connection release –**
   In an Abrupt connection release, either one TCP entity is forced to close the connection or one user closes both directions of data transfer.
   An abrupt connection release is carried out when an RST segment is sent. An RST segment can be sent for the below reasons:
   1. When a non-SYN segment was received for a non-existing TCP connection.
   2. In an open connection, some TCP implementations send an RST segment when a segment with an invalid header is received. This will prevent attacks by closing the corresponding connection.
   3. When some implementations need to close an existing TCP connection, they send an RST segment. They will close an existing TCP connection for the following reasons:
      - Lack of resources to support the connection
      - The remote host is now unreachable and has stopped responding.

TCP Timers

- **Retransmission Timer** – When TCP sends a segment the timer starts and stops when the acknowledgment is received. If the timer expires timeout occurs and the segment is retransmitted. RTO (retransmission timeout is for 1 RTT) to calculate retransmission timeout we first need to calculate the RTT(round trip time).
- **Persistent Timer** – To deal with a zero-window-size deadlock situation, TCP uses a persistence timer. When the sending TCP receives an acknowledgment with a window size of zero, it starts a persistence timer. When the persistence timer goes off, the sending TCP sends a special segment called a probe. This segment contains only 1 byte of new data. It has a sequence number, but its sequence number is never acknowledged; it is even ignored in calculating the sequence number for the rest of the data. The probe causes the receiving TCP to resend the acknowledgment which was lost.
- **Keep Alive Timer** – A keepalive timer is used to prevent a long idle connection between two TCPs. If a client opens a TCP connection to a server transfers some data and becomes silent the client will crash. In this case, the connection remains open forever. So a keepalive timer is used. Each time the server hears from a client, it resets this timer. The time-out is usually 2 hours. If the server does not hear from the client after 2 hours, it sends a probe segment. If there is no response after 10 probes, each of which is 75 s apart, it assumes that the client is down and terminates the connection.
- **Time Wait Timer** – This timer is used during tcp connection termination. The timer starts after sending the last Ack for 2nd FIN and closing the connection.

Fast Recovery Technique For Loss Recovery in TCP

When there is a packet loss detected, the TCP sender does 4 things:

1. Reduces the cwnd by 50%.
2. Reduces the ssthresh value by 50% of cwnd.
3. Retransmit the lost packet.
4. Enters the Fast Recovery phase.

Fast Recovery Phase:

This comprises of two parts:

1. The half window of silence
2. Maintain the inflight=cwnd until a new ACK arrives at the sender side.

The half window of silence is the amount of time the sender becomes silent(inactive) and waits for inflight to become equal to cwnd. Because cwnd is reduced to its half when packet loss is detected. Before that inflight was exactly equal to cwnd, but now inflight is approximately double of cwnd value. So, the sender doesn't transmit any new packet neither it increases its cwnd by 1 per ACK. The sender will keep on getting DUP-ACK until the receiver receives the retransmitted packet.

After the inflight becomes equal to cwnd, the half window of silence ends here, now also DUP-ACK will keep coming, so the sender doesn't increase its cwnd but it will maintain an inflight value equal to cwnd. When one DUP-ACK comes, the inflight becomes 1 less than the previous value, so to maintain inflight=cwnd sender transmits one new packet into the network. When finally the receiver gets the retransmitted packet and it sends a new ACK to the sender, then the sender will come out of the Fast Recovery phase and immediately enter the AIMD phase. The sender comes out of the recovery phase because it has confirmed that the lost packet is received by the receiver and thus the network is no longer congested. But, it has to carefully increase the cwnd to avoid subsequent congestion too early, thus entering AIMD hereafter.

MAC

MAC refers to Media Access Control,MAC is a series of rules through which devices can transfer data among them in a network. When a device is connected to a network, it obtains a unique MAC address. It identifies a device connected to a network. The MAC address, also known as the hardware address, is hard-wired to the network interface card of any device.In a network MAC addresses help direct data packets to intended destinations hence they are considered crucial for communication purposes. While sending a message, a specific device includes the recipient's MAC address on the packet.The total length MAC address in **byte is 6 (or 48 bits)**.

used formats:

- Six two-digits hexadecimals separated by hyphens (-) like 45-67-89-AB-12-CD .
- Six two-digits hexadecimals separated by colons (:) like 45:67:89:AB:DE:23 .
- Three four-digits hexadecimals separated by dots (.) like ABCD.4567.1238 .

The left 24 bits (3 bytes) of the address is termed as **Organizationally Unique Identifier (OUI) number.** This globally unique OUI number will always remain the same for NICs manufactured by the same company. The right 24 bits (3 bytes) of the address is termed as **Network Interface Controller Specific (NICS),** which is responsible for communication either by using cables or wirelessly over a computer network.

Channel Allocation Problem

Channel allocation is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks. There are user's quantity may vary every time the process takes place. If there are N number of users and channel is divided into N equal-sized sub channels, Each user is assigned one portion. If the number of users are small and don't vary at times, then Frequency Division Multiplexing can be used as it is a simple and efficient channel bandwidth allocating technique.

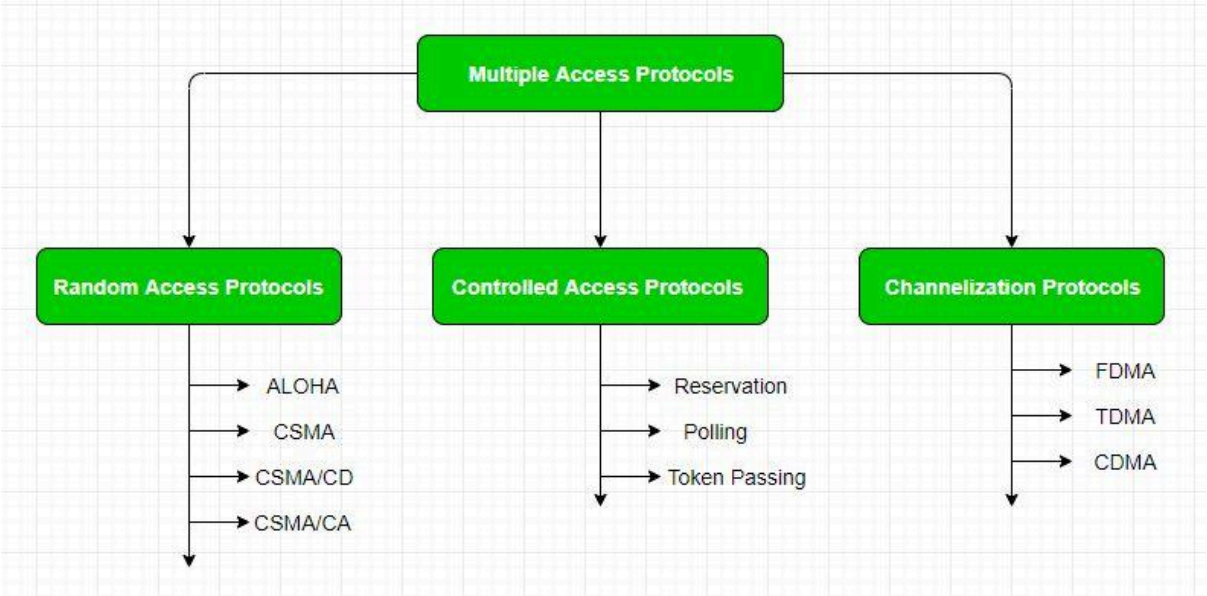
Channel allocation problem can be solved by two schemes: Static Channel Allocation in LANs and MANs, and Dynamic Channel Allocation.

Multiple Access Protocols

Multiple Access Protocols are methods used in computer networks to control how data is transmitted when multiple devices are trying to communicate over the same network. These protocols ensure that data packets are sent and received efficiently, without collisions or interference. They help manage the network traffic so that all devices can share the communication channel smoothly and effectively.

Data Link Control

The data link control is responsible for the reliable transmission of messages over transmission channels by using techniques like framing, error control and flow control. For Data link control refer to – Stop and Wait ARQ.



1. Random Access Protocol

In this, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium's state(idle or busy). It has two features:

- There is no fixed time for sending data
- There is no fixed sequence of stations sending data

The Random access protocols are further subdivided as: aloha and csma

ALOHA

- **Pure ALOHA**
  When a station sends data it waits for an acknowledgement. If the acknowledgement doesn't come within the allotted time then the station waits for a random amount of time called back-off time (Tb) and re-sends the data. Since different stations wait for different amount of time, the probability of further collision decreases.
- **Slotted ALOHA**
  It is similar to pure aloha, except that we divide time into slots and sending of data is allowed only at the beginning of these slots. If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.

CSMA

Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However there is still chance of collision in CSMA due to propagation delay.

- **1-Persistent:** The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally(with 1 probability) as soon as the channel gets idle.
- **Non-Persistent:** The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.
- **P-Persistent:** The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it send with p probability. This repeat continues until the frame is sent. It is used in Wifi and packet radio systems.
- **O-Persistent:** Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.

CSMA/CD

Carrier sense multiple access with collision detection. Stations can terminate transmission of data if collision is detected

CSMA/CA

Carrier sense multiple access with collision avoidance. The process of collisions detection involves sender receiving acknowledgement signals. If there is just one signal(its own) then the data is successfully sent but if there are two signals(its own and the one with which it has collided) then it means a collision has occurred.

CSMA/CA Avoids Collision By

- **Interframe Space:** Station waits for medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called Interframe space or IFS. After this time it again checks the medium for being idle. The IFS duration depends on the priority of station.
- **Contention Window:** It is the amount of time divided into slots. If the sender is ready to send data, it chooses a random number of slots as wait time which doubles every time medium is not found idle. If the medium is found busy it does not restart the entire process, rather it restarts the timer when the channel is found idle again.
- **Acknowledgement:** The sender re-transmits the data if acknowledgement is not received before time-out.

2. Controlled Access

Controlled access protocols ensure that only one device uses the network at a time. Think of it like taking turns in a conversation so everyone can speak without talking over each other.

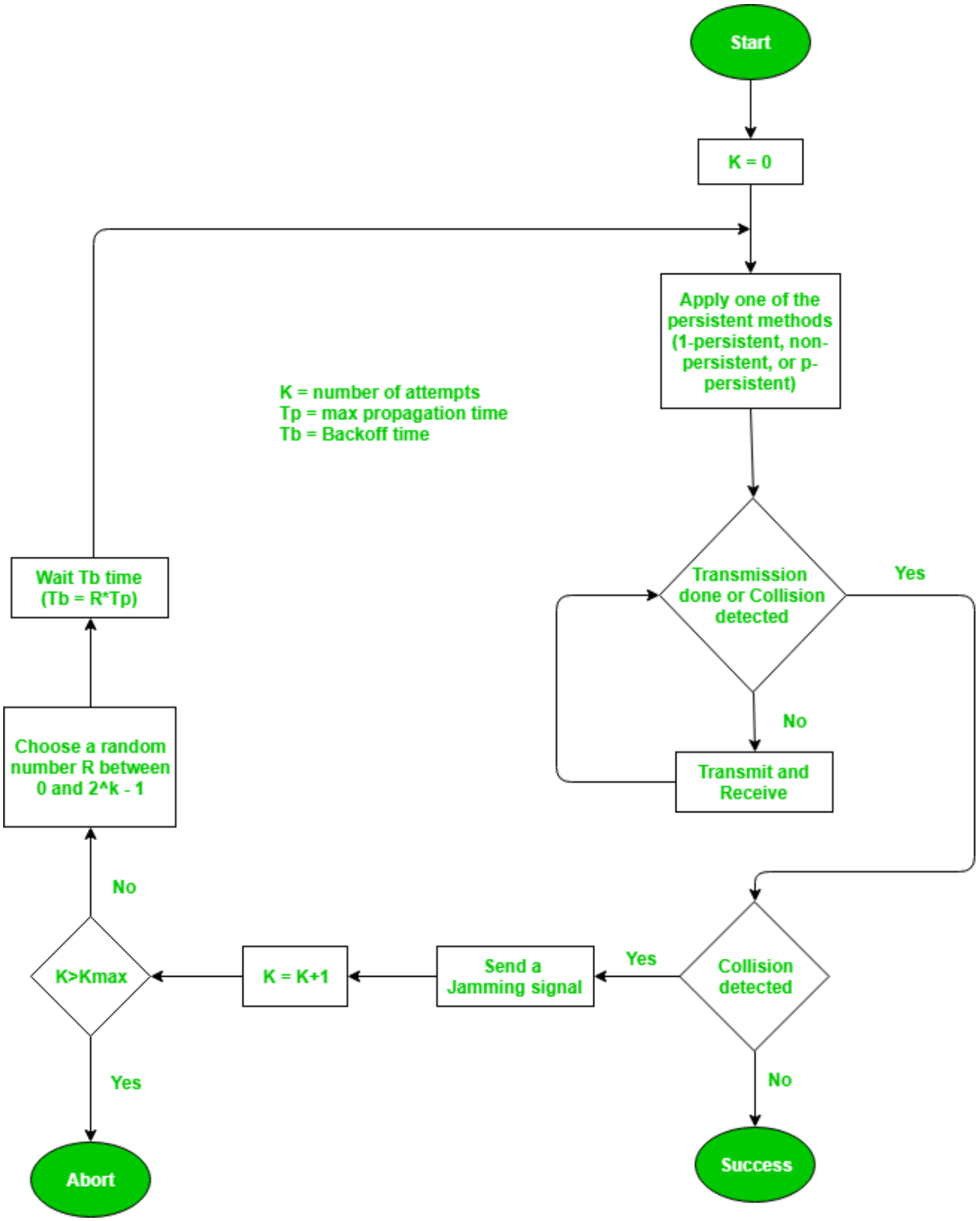
3. Channelization

In this, the available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.

- Frequency Division Multiple Access (FDMA)
- Time Division Multiple Access (TDMA)
- Code Division Multiple Access (CDMA)
- Orthogonal Frequency Division Multiple Access (OFDMA)

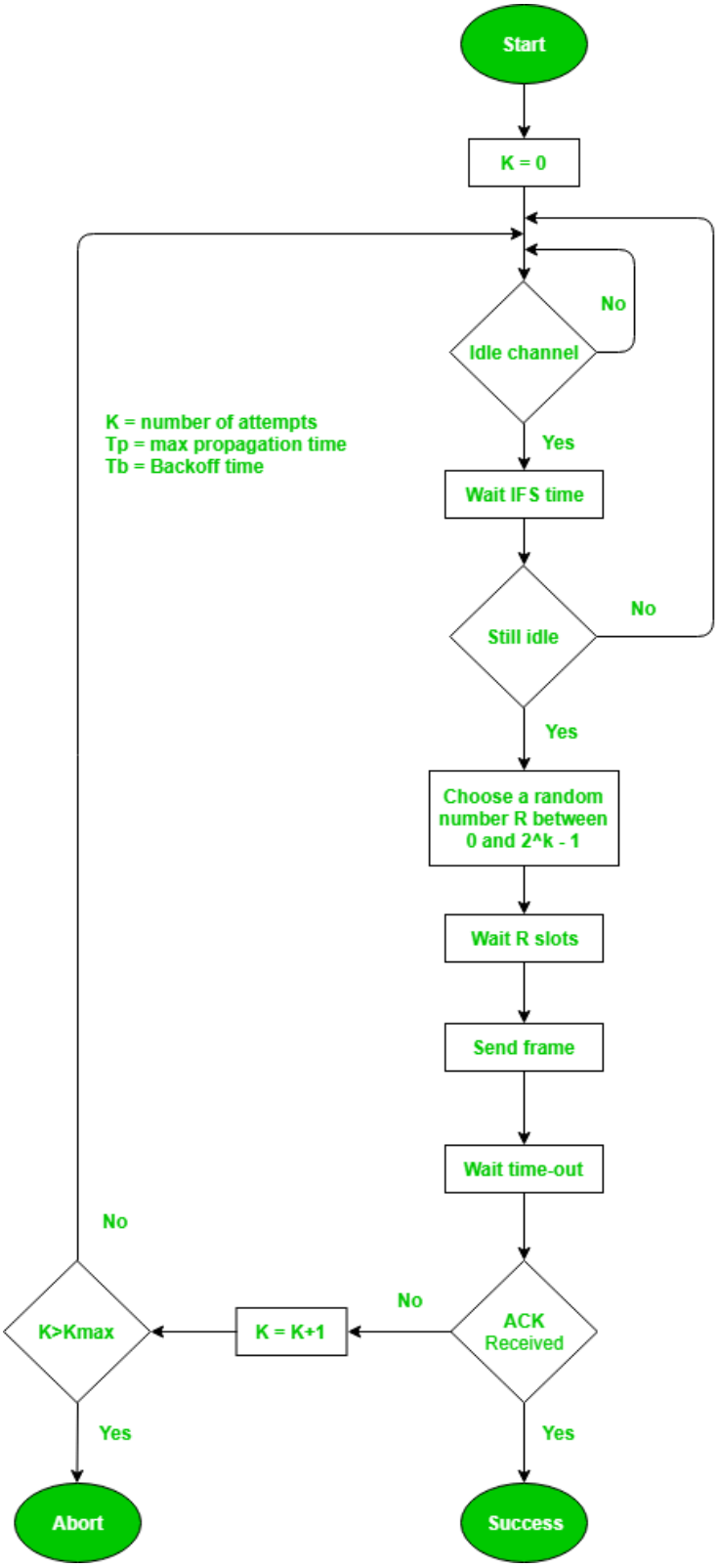
Carrier Sense Multiple Access (CSMA)

1. Carrier Sense Multiple Access with Collision Detection (CSMA/CD):



2. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

Ifs - interframe space



CSMA/CD is used in Ethernet networks, while CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is used in wireless networks. CSMA/CA aims to avoid collisions altogether by scheduling transmissions based on network conditions and using acknowledgments to confirm successful data transmission

Controlled Access Protocols

1. Reservation

- In the reservation method, a station needs to make a reservation before sending data.
- The timeline has two kinds of periods:
    - Reservation interval of fixed time length
    - Data transmission period of variable frames.
- If there are M stations, the reservation interval is divided into M slots, and each station has one slot.
- Suppose if station 1 has a frame to send, it transmits 1 bit during the slot 1. No other station is allowed to transmit during this slot.
- In general, i th station may announce that it has a frame to send by inserting a 1 bit into i th slot. After all N slots have been checked, each station knows which stations wish to transmit.
- The stations which have reserved their slots transfer their frames in that order.
- After data transmission period, next reservation interval begins.
- Since everyone agrees on who goes next, there will never be any collisions.

2. Polling

- Polling process is similar to the roll-call performed in class. Just like the teacher, a controller sends a message to each node in turn.
- In this, one acts as a primary station(controller) and the others are secondary stations. All data exchanges must be made through the controller.
- The message sent by the controller contains the address of the node being selected for granting access.
- Although all nodes receive the message the addressed one responds to it and sends data if any. If there is no data, usually a “poll reject”(NAK) message is sent back.

3. Token Passing

- In token passing scheme, the stations are connected logically to each other in form of ring and access to stations is governed by tokens.
- A token is a special bit pattern or a small message, which circulate from one station to the next in some predefined order.
- In Token ring, token is passed from one station to another adjacent station in the ring whereas incase of Token bus, each station uses the bus to send the token to the next station in some predefined order.
- In both cases, token represents permission to send. If a station has a frame queued for transmission when it receives the token, it can send that frame before it passes the token to the next station. If it has no queued frame, it passes the token simply.
- After sending a frame, each station must wait for all N stations (including itself) to send the token to their neighbours and the other N – 1 stations to send a frame, if they have one.

Stop and Wait Protocol

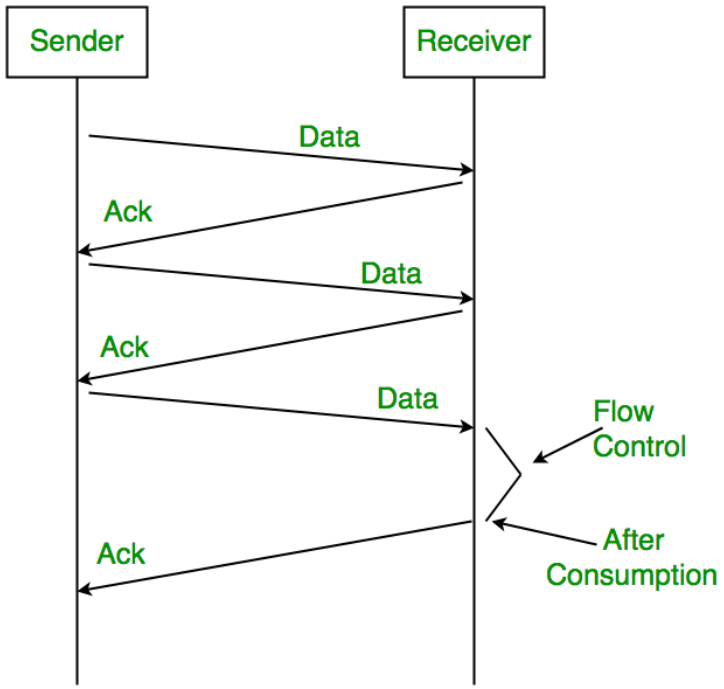
Stop and Wait ARQ is a Sliding Window Protocol method used for the reliable delivery of data frames. The stop-and-wait ARQ is used for noisy channels or links to handle flow and error control between sender and receiver. The Stop and Wait ARQ protocol sends a data frame and then waits for an acknowledgment (ACK) from the receiver.

At Sender

- Rule 1: Send one data packet at a time.
- Rule 2: Send the next packet only after receiving acknowledgment for the previous.

At Receiver

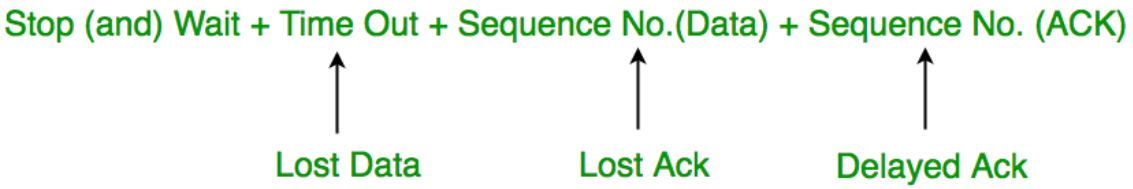
- Rule 1: Send acknowledgement after receiving and consuming a data packet.
- Rule 2: After consuming packet acknowledgement need to be sent (Flow Control)



Problems

1. Lost Data
2. Lost Acknowledgement
3. Delayed Acknowledgement/Data

Stop and Wait for ARQ (Automatic Repeat Request)



1. Time Out

Timeout refers to the duration for which the sender waits for an acknowledgment (ACK) from the receiver after transmitting a data packet. If the sender does not receive an ACK within this timeout period, it assumes that the frame was lost or corrupted and retransmits the frame.

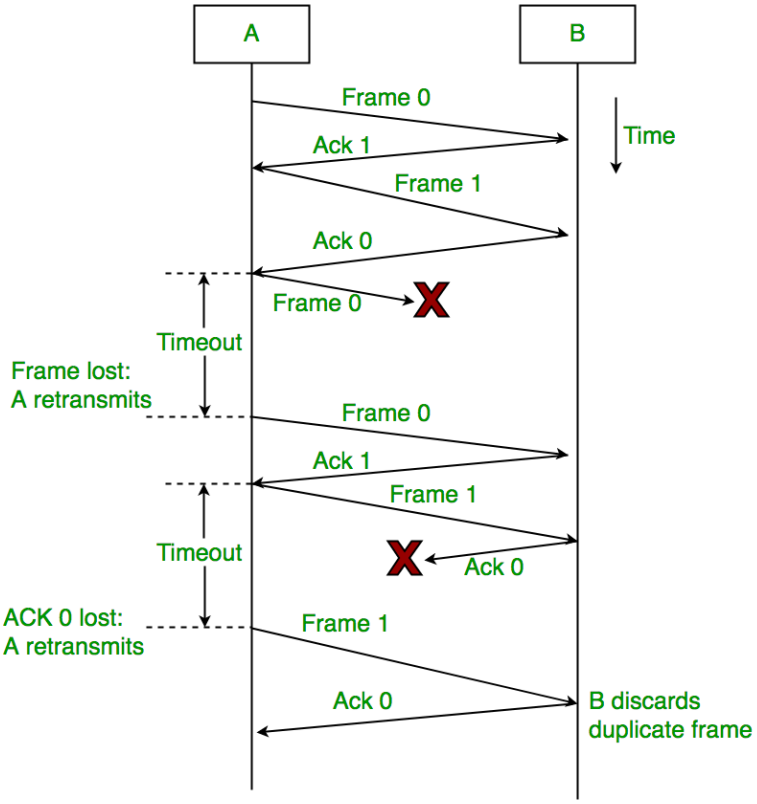
2. Sequence Number (Data)

In Stop-and-Wait ARQ, the sender assigns sequence numbers to each data frame it sends. This allows the receiver to identify and acknowledge each frame individually, ensuring reliable delivery of data packets. After sending a frame, the sender waits for an acknowledgment before sending the next fram

3. Sequence Number(Acknowledgement)

Similarly, sequence numbers are also used in acknowledgments (ACKs) sent by the receiver to acknowledge received data frames. When the receiver successfully receives a data frame, it sends an ACK back to the sender, indicating the sequence number of the next expected frame. The sender uses this ACK to determine whether the transmission was successful and whether it can proceed to send the next frame.

- Sender A sends a data frame or packet with sequence number 0.
- Receiver B, after receiving the data frame, sends an acknowledgement with sequence number 1 (the sequence number of the next expected data frame or packet)
  There is only a one-bit sequence number that implies that both sender and receiver have a buffer for one frame or packet only.



Stop and Wait ARQ has very less efficiency , it can be improved by increasing the window size. Also , for better efficiency , Go back N and Selective Repeat Protocols are used. The Stop and Wait ARQ solves the main three problems but may cause big performance issues as the sender always waits for acknowledgement even if it has the next packet ready to send. Consider a situation where you have a high bandwidth connection and propagation delay is also high

Selective Repeat Protocol

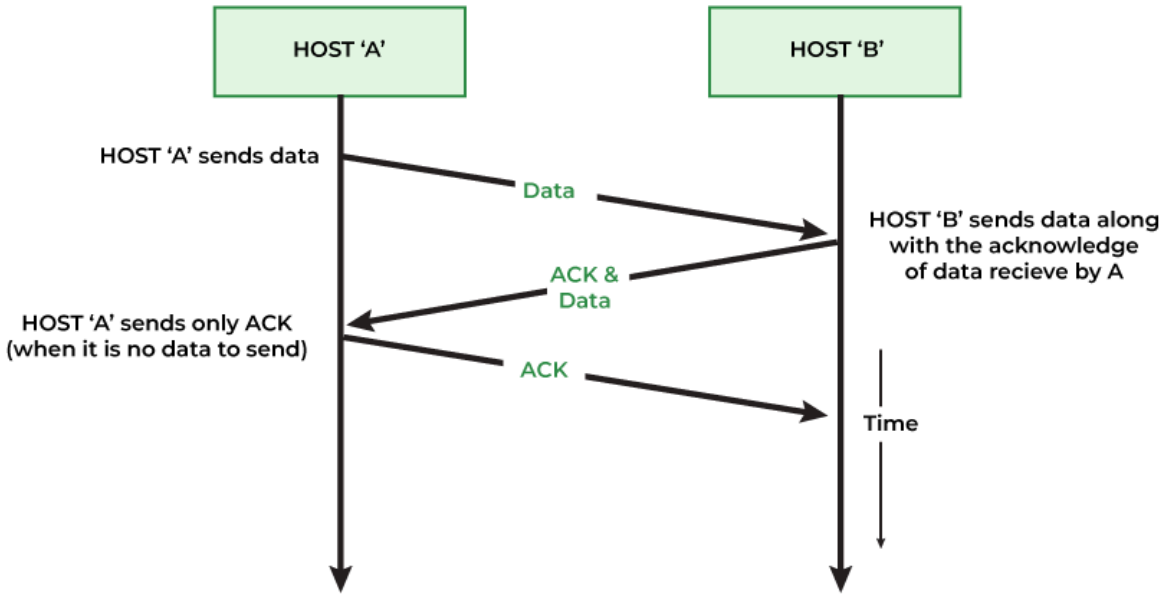
This protocol(SRP) is mostly identical to GBN protocol, except that buffers are used and the receiver, and the sender, each maintains a window of size. SRP works better when the link is very unreliable. Because in this case, retransmission tends to happen more frequently, selectively retransmitting frames is more efficient than retransmitting all of them. SRP also requires full-duplex link. backward acknowledgements are also in progress.

- Sender's Windows (Ws) = Receiver's Windows (Wr).
- Window size should be less than or equal to half the sequence number in SR protocol. This is to avoid packets being recognized incorrectly. If the size of the window is greater than half the sequence number space, then if an ACK is lost, the sender may send new packets that the receiver believes are retransmissions.
- Sender can transmit new packets as long as their number is with W of all unACKed packets.
- Sender retransmit un-ACKed packets after a timeout – Or upon a NAK if NAK is employed.
- Receiver ACKs all correct packets.
- Receiver stores correct packets until they can be delivered in order to the higher layer.
- In Selective Repeat ARQ, the size of the sender and receiver window must be at most one-half of 2^m.

Piggybacking

Piggybacking is the technique of delaying outgoing acknowledgment and attaching it to the next data packet.

When a data frame arrives, the receiver waits and does not send the control frame (acknowledgment) back immediately. The receiver waits until its network layer moves to the next data packet. Acknowledgment is associated with this outgoing data frame. Thus the acknowledgment travels along with the next data frame. This technique in which the outgoing acknowledgment is delayed temporarily is called Piggybacking.



IPv4

It uses a set of four numbers, separated by periods (like 192.168.0.1), to give each device a unique address. This address helps data find its way from one device to another over the internet.
IPv4 addresses consist of three parts:

- **Network Part**: The network part indicates the distinctive variety that's appointed to the network. The network part conjointly identifies the category of the network that's assigned.
- **Host Part**: uniquely identifies the machine on your network. This part of the IPv4 address is assigned to every host. For each host on network, the network part is same, the host half must vary.
- **Subnet Number**: This is the nonobligatory part of IPv4. Local networks that have massive numbers of hosts are divided into subnets and subnet numbers are appointed to that.

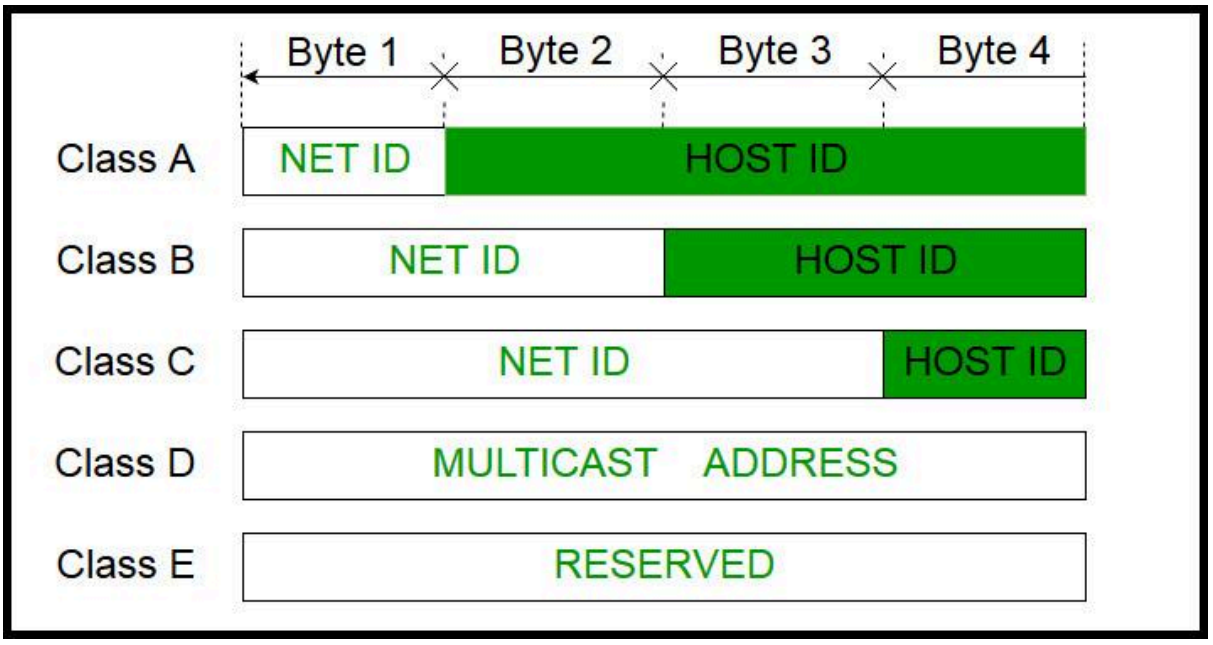
IPv6

This new IP address version is being deployed to fulfil the need for more Internet addresses. With 128-bit address space, it allows 340 undecillion unique address space.The first 48 bits represent Global Routing Prefix. The next 16 bits represent the student ID and the last 64 bits represent the host ID.

IPv6	IPv4
It supports Auto and renumbering address configuration	It Supports Manual and DHCP address configuration
produce 3.4×1038 address space	generate 4.29×109 address space
Hexadecimal representation	Decimal representation
In IPv6 checksum field is not	In IPv4 checksum field is available
IPv6 has a header of 40 bytes	IPv4 has a header of 20-60 bytes.
IPv6 does not support VLSM.	IPv4 supports VLSM.

Classful IP Addressing

Classful IP addressing is a way of organizing and managing IP addresses, which are used to identify devices on a network.
The 32-bit IP address is divided into five sub-classes.



CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Host IDs are used to identify a host within a network. The host ID is assigned based on the following rules:

- Within any network, the host ID must be unique to that network.
- A host ID in which all bits are set to 0 cannot be assigned because this host ID is used to represent the network ID of the IP address.
- Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broadcast address to send packets to all the hosts present on that particular network.

The problem with this classful addressing method is that millions of class A addresses are wasted, many of the class B addresses are wasted, whereas, the number of addresses available in class C is so small that it cannot cater to the needs of organizations. Class D addresses are used for multicast routing and are therefore available as a single block only. Class E addresses are reserved.

Classless Addressing in IP Addressing

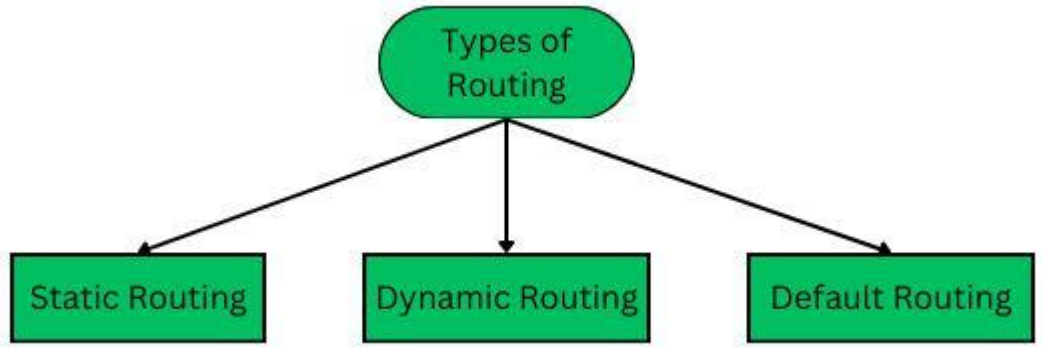
To reduce the wastage of IP addresses in a block, we use sub-netting. What we do is that we use host id bits as net id bits of a classful IP address. We give the IP address and define the number of bits for mask along with it (usually followed by a '/' symbol), like, 192.168.1.1/28. Here, subnet mask is found by putting the given number of bits out of 32 as 1, like, in the given address, we need to put 28 out of 32 bits as 1 and the rest as 0, and so, the subnet mask would be 255.255.255.240. A classless addressing system or classless interdomain routing (CIDR or supernetting) is the way to combine two or more class C networks to create a/23 or a /22 supernet. A classless addressing system or classless interdomain routing (CIDR) is an improved IP addressing system. In a classless addressing system the block of IP address is assigned dynamically based on specific rules.

Supernetting in Network Layer

Supernetting is the opposite of Subnetting. In subnetting, a single big network is divided into multiple smaller subnetworks. In Supernetting, multiple networks are combined into a bigger network termed a Supernetwork or Supernet.

Routing

Routing is the process of determining paths through a network for sending data packets. Routing ensures that data moves effectively from source to destination, making the best use of network resources and ensuring consistent communication. Routing is a process that is performed by layer 3 (or network layer) devices



1. Static Routing

Static routing is also called as “non-adaptive routing”. In this, routing configuration is done manually by the network administrator. Let’s say for example, we have 5 different routes to transmit data from one node to another, so the network administrator will have to manually enter the routing information by assessing all the routes.

2. Default Routing

This is the method where the router is configured to send all packets toward a single router (next hop). It doesn’t matter to which network the packet belongs, it is forwarded out to the router which is configured for default routing. It is generally used with stub routers. A stub router is a router that has only one route to reach all other networks.

3. Dynamic Routing

Dynamic routing makes automatic adjustments of the routes according to the current state of the route in the routing table. Dynamic routing uses protocols to discover network destinations and the routes to reach them. RIP and OSPF are the best examples of dynamic routing protocols.

Unicast Routing

Unicast means the transmission from a single sender to a single receiver. It is a point-to-point communication between the sender and receiver. There are various unicast protocols such as TCP, HTTP, etc.

Major Protocols of Unicast Routing

1. **Distance Vector Routing:** Distance-Vector routers use a distributed algorithm to compute their routing tables.
2. **Link-State Routing:** Link-State routing uses link-state routers to exchange messages that allow each router to learn the entire network topology.
3. **Path-Vector Routing:** It is a routing protocol that maintains the path that is updated dynamically.

Routing Strategies :

1. Fixed Routing
2. Flooding
3. Dynamic Routing
4. Random Routing
5. Flow-based Routing

Fixed Routing –

- A route is selected for each source and destination pair of nodes in the network.
- The route is fixed; changes only if the topology of the network changes.

Flooding –

- Requires no network information like topology, load condition, cost of diff. paths
- Every incoming packet to a node is sent out on every outgoing like except the one it arrived on.(sending to all connecting nodes).

Link State Routing

link-state routing uses link-state routers to exchange messages that allow each router to learn the entire network topology. Based on this learned topology, each router is then able to compute its routing table by using the shortest path computation. Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router i.e. the internet work.

1. **Knowledge about the neighborhood**: Instead of sending its routing table, a router sends the information about its neighborhood only. A router broadcast its identities and cost of the directly attached links to other routers.
2. **Flooding:** Each router sends the information to every other router on the internetwork except its neighbors. Every router that receives the packet sends the copies to all the neighbors. Finally each and every router receives a copy of the same information.
3. **Information Sharing**: A router send the information to every other router only when the change occurs in the information.

Link state routing has two phase:

1. **Reliable Flooding: Initial state**– Each node knows the cost of its neighbors. Final state- Each node knows the entire graph.
2. **Route Calculation**: Each node uses Dijkstra' s algorithm on the graph to calculate the optimal routes to all nodes. The link state routing algorithm is also known as Dijkstra's algorithm which is used to find the shortest path from one node to every other node in the network.

Distance Vector Routing (DVR) Protocol

Distance Vector Routing (DVR) Protocol is a method used by routers to find the best path for data to travel across a network. Each router keeps a table that shows the shortest distance to every other router, based on the number of hops (or steps) needed to reach them. Routers share this information with their neighbors, allowing them to update their tables and find the most efficient routes.

Each router maintains a Distance Vector table containing the distance between itself and All possible destination nodes.

```
Dx(y) = min { C(x,v) + Dv(y), Dx(y) } for each node y ? N
```

Firewall

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules accepts, rejects, or drops that specific traffic.

- **Accept:** allow the traffic
- **Reject:** block the traffic but reply with an “unreachable error”
- **Drop:** block the traffic with no reply .

Types of Firewall

1. Packet Filtering Firewall

Controls network access by monitoring outgoing and incoming packets and allowing them to pass or stop based on source and destination IP address, protocols, and ports. transport layer. Packet filtering firewall maintains a filtering table that decides whether the packet will be forwarded or not.

2. Stateful Inspection Firewall

Tracks the state of network connections and makes filtering decisions based on connection history and defined rules.

3. Software Firewall

Installed locally or on a cloud server, it controls data inflow and outflow but can be time-consuming to manage.

4. Hardware Firewall

A physical appliance that blocks malicious data before it reaches vulnerable network endpoints.

5. Application Layer Firewall

Inspects packets at the application layer and can block specific content and misuse of protocols like HTTP and FTP.

6. Next-Generation Firewall (NGFW)

Combines deep packet inspection, application inspection, and other advanced features to protect against modern threats.

7. Proxy Service Firewall

Acts as a gateway between networks for specific applications, filtering communications at the application layer.

8. Circuit-Level Gateway Firewall

Operates at the session layer, allowing TCP connections but doesn't inspect individual data packets, making it less secure against malware.

Congestion Control

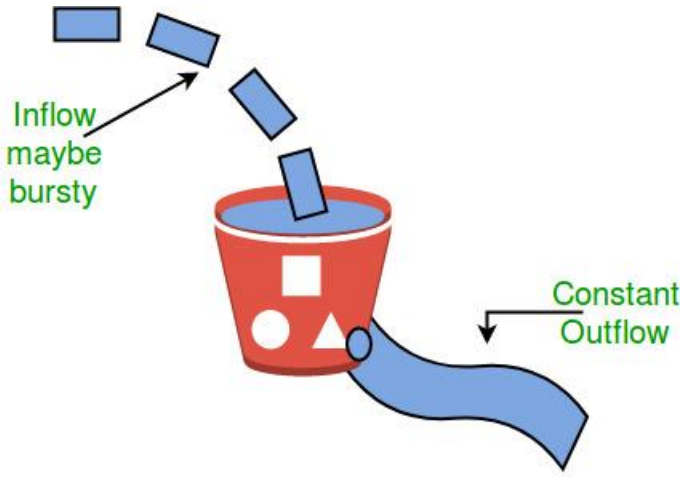
Congestion control is a crucial concept in computer networks. It refers to the methods used to prevent network overload and ensure smooth data flow. When too much data is sent through the network at once, it can cause delays and data loss.

Congestion Control Algorithm

- Congestion Control is a mechanism that controls the entry of data packets into the network, enabling a better use of a shared network infrastructure and avoiding congestive collapse.
- **Congestive-avoidance algorithms** (CAA) are implemented at the TCP layer as the mechanism to avoid congestive collapse in a network.

Leaky Bucket Algorithm

The leaky bucket algorithm discovers its use in the context of network traffic shaping or rate-limiting.Let us consider an example to understand Imagine a bucket with a small hole in the bottom. No matter at what rate water enters the bucket, the outflow is at constant rate. When the bucket is full with water additional water entering spills over the sides and is lost.



- When host wants to send packet, packet is thrown into the bucket.
- The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
- Bursty traffic is converted to a uniform traffic by the leaky bucket.
- In practice the bucket is a finite queue that outputs at a finite rate.

Token Bucket Algorithm
In some applications, when large bursts arrive, the output is allowed to speed up. This calls for a more flexible algorithm, preferably one that never loses information.It is a control algorithm that indicates when traffic should be sent. This order comes based on the display of tokens in the bucket. The bucket contains tokens. Each of the tokens defines a packet of predetermined size. Tokens in the bucket are deleted for the ability to share a packet.When tokens are shown, a flow to transmit traffic appears in the display of tokens. No token means no flow sends its packets. Hence, a flow transfers traffic up to its peak burst rate in good tokens in the bucket.

- In regular intervals tokens are thrown into the bucket. *f*
- The bucket has a maximum capacity. *f*
- If there is a ready packet, a token is removed from the bucket, and the packet is sent.
- If there is no token in the bucket, the packet cannot be sent.

Congestion Policy in TCP

- **Slow Start Phase:** Starts slow increment is exponential to the threshold.
- **Congestion Avoidance Phase:** After reaching the threshold increment is by 1.
- **Congestion Detection Phase:** The sender goes back to the Slow start phase or the Congestion avoidance phase.

Open Loop Congestion Control:
Definition: Open loop congestion control involves policies and techniques aimed at preventing network congestion before it happens. Control measures are implemented either by the source or destination to avoid overloading the network.

1. **Retransmission Policy**: Optimizes retransmissions to avoid network congestion by using appropriate timers.
2. **Window Policy**: Adopts Selective Repeat window to resend only specific lost packets, reducing congestion.
3. **Discarding Policy**: Routers discard less sensitive packets to prevent congestion while maintaining data quality.
4. **Acknowledgment Policy**: Reduces network load by sending acknowledgments for multiple packets at once or upon timer expiry.
5. **Admission Policy**: Controls traffic by denying connections when resources are insufficient, preventing further congestion.

Closed Loop Congestion Control:
Definition: Closed loop congestion control refers to techniques used to manage and alleviate congestion after it occurs. These methods work by monitoring network traffic and adjusting the flow of data in response to congestion.

1. **Backpressure**: Congested nodes stop receiving data, causing upstream nodes to slow down, preventing further congestion.
2. **Choke Packet Technique**: Congested nodes send a packet to the source to reduce traffic, alleviating congestion.
3. **Implicit Signaling**: Source detects congestion based on lack of acknowledgment or other inferred signs.
4. **Explicit Signaling**: Congested nodes send signals in data packets to warn the source or destination about congestion.

Circuit Switching

Circuit Switching is a type of switching, in which a connection is established between the source and destination beforehand. This connection receives the complete bandwidth of the network until the data is transferred completely.

Phases of Circuit Switching

- **Circuit Establishment:** A dedicated circuit between the source and destination is constructed via a number of intermediary switching center's. Communication signals can be requested and received when the sender and receiver communicate signals over the circuit.
- **Data Transfer:** Data can be transferred between the source and destination once the circuit has been established. The link between the two parties remains as long as they communicate.
- **Circuit Disconnection:** Disconnection in the circuit occurs when one of the users initiates the disconnect. When the disconnection occurs, all intermediary linkages between the sender and receiver are terminated.

Message switching techniques

Message switching is a switching mechanism in which a message is sent as a single unit and routed to intermediary nodes where it is stored and forwarded. The message-switching approach does not provide a dedicated path between the sender and receiver. In message switching, end-users communicate by sending and receiving *messages* that include the entire data to be shared. Messages are the smallest individual unit. Also, the sender and receiver are not directly connected. Several intermediate nodes transfer data and ensure that the message reaches its destination. Message-switched data networks are hence called hop-by-hop systems.

Packet Switching

Packet Switching in computer networks is a method of transferring data to a network in the form of packets.

1. Connection-oriented Packet Switching (Virtual Circuit)

Before starting the transmission, it establishes a logical path or virtual connection using a signaling protocol, between sender and receiver and all packets belongs to this flow will follow this predefined route.

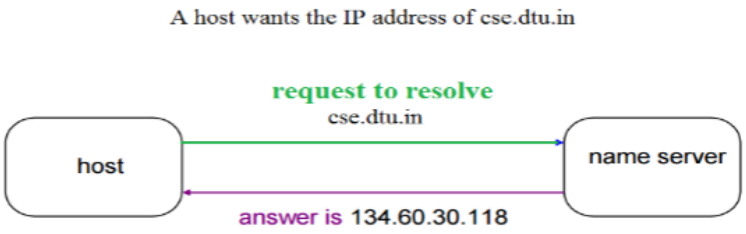
2. Connectionless Packet Switching (Datagram)

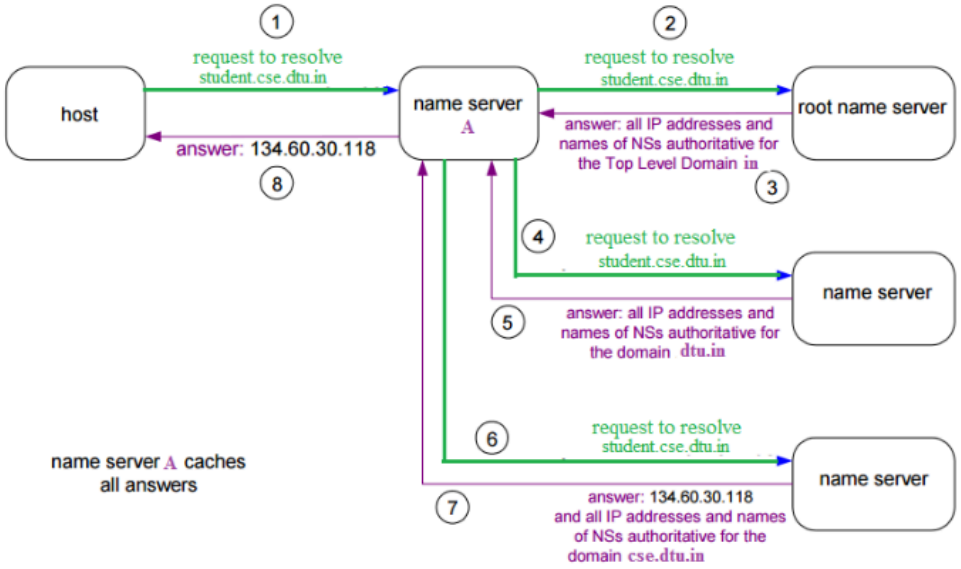
Unlike Connection-oriented packet switching, In Connectionless Packet Switching each packet contains all necessary addressing information such as source address, destination address, port numbers, etc. Packets belonging to one flow may take different routes because routing decisions are made dynamically, so the packets that arrived at the destination might be out of order. It has no connection setup and teardown phase, like Virtual Circuits.
Packet delivery is not guaranteed in connectionless packet switching, so reliable delivery must be provided by end systems using additional protocols.

Domain Name System (DNS)

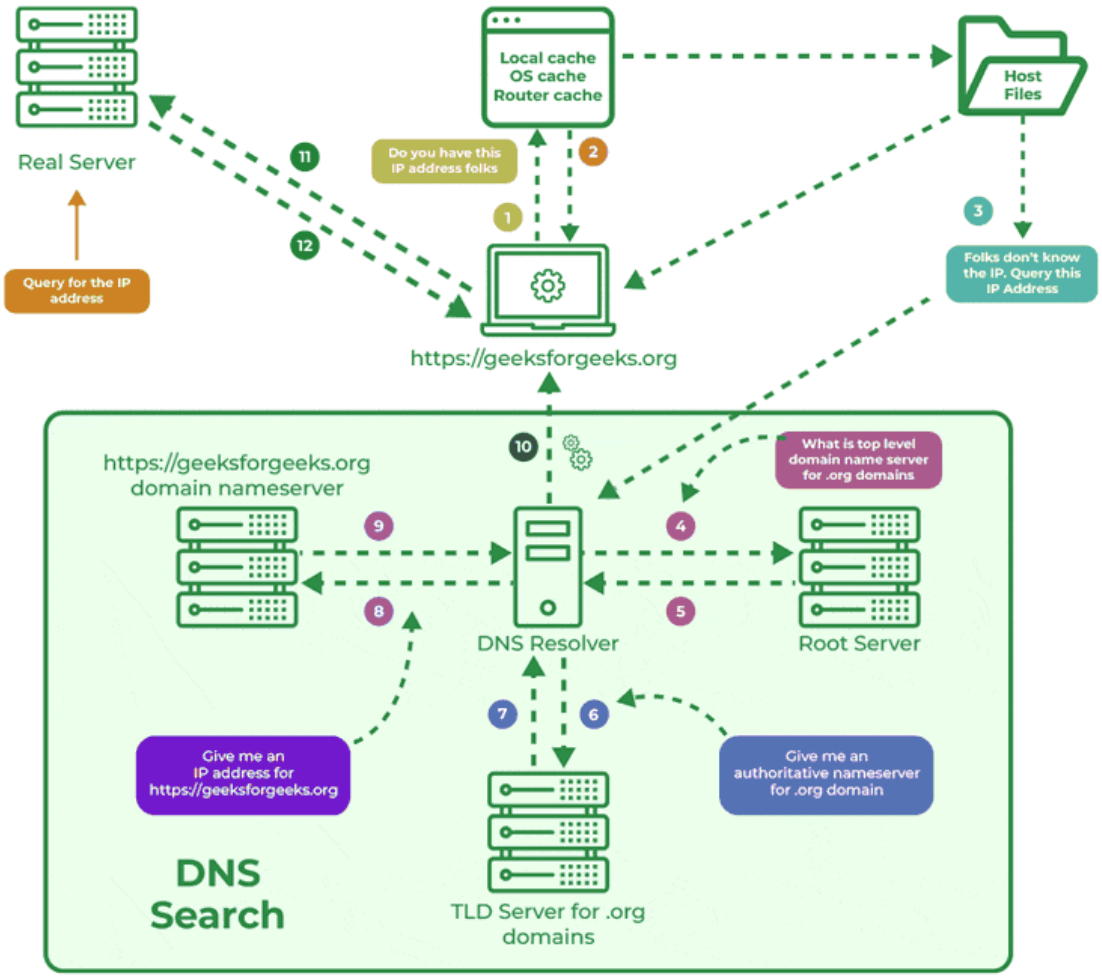
The Domain Name System (DNS) is like the internet's phone book. It helps you find websites by translating easy-to-remember names (like www.example.com) into the numerical IP addresses (like 192.0.2.1) that computers use to locate each other on the internet.

- **Country Domain:** .in (India) .us .uk
- **Generic Domains:** .com(commercial), .edu(educational), .mil(military), .org(nonprofit organization), .net(similar to commercial) all these are generic domains.
- **Inverse Domain:** if we want to know what is the domain name of the website. IP to domain name mapping.





How Does DNS Works

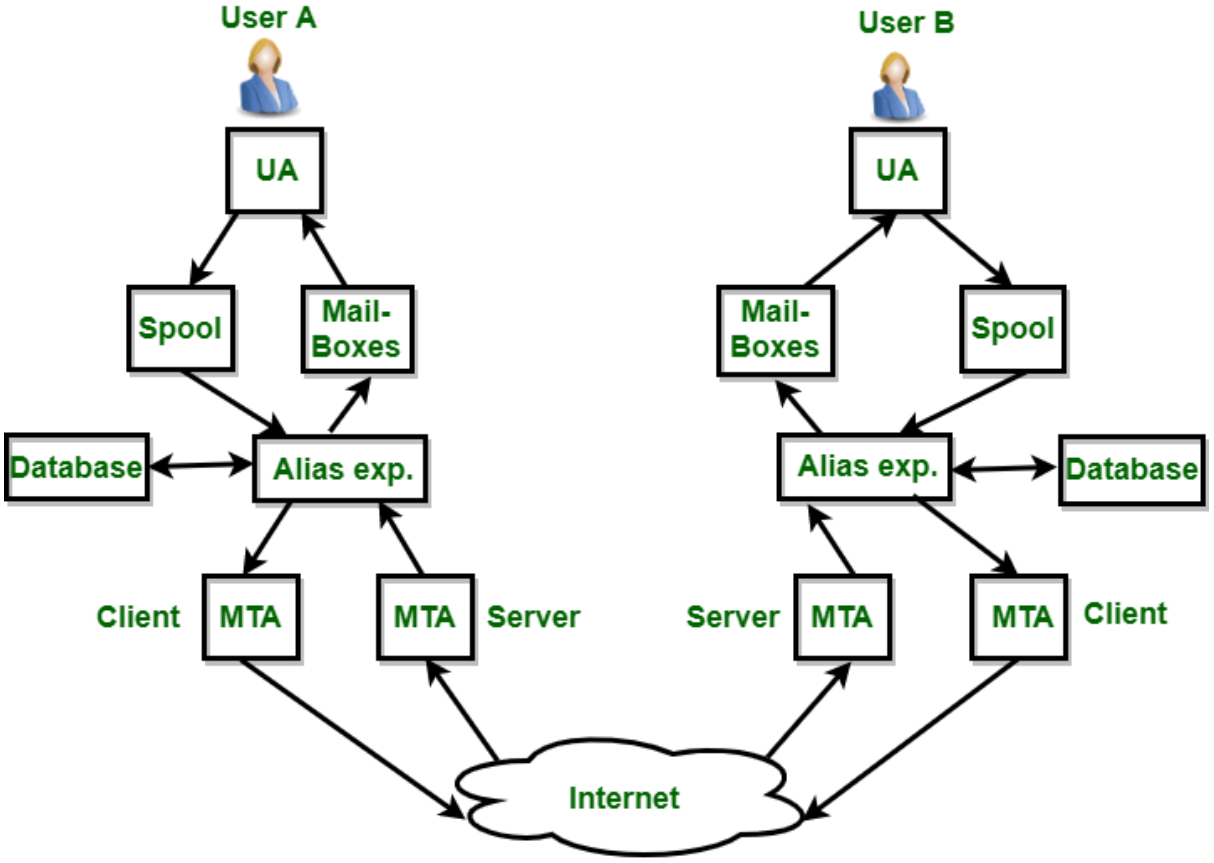


1. A user types “example.com” into a web browser.
2. The request goes to a DNS resolver.
3. The resolver asks a root server where to find the top-level domain (TLD) server for .com.
4. The root server tells the resolver to contact the .com TLD server.
5. The resolver then asks the .com TLD server for the IP address of “example.com.”
6. The .com TLD server gives the resolver the IP address of the domain’s nameserver.
7. The resolver then asks the domain’s nameserver for the IP address of “example.com.”
8. The domain’s nameserver returns the IP address to the resolver.

Here is the list of main DNS servers involved in loading a Webpage.

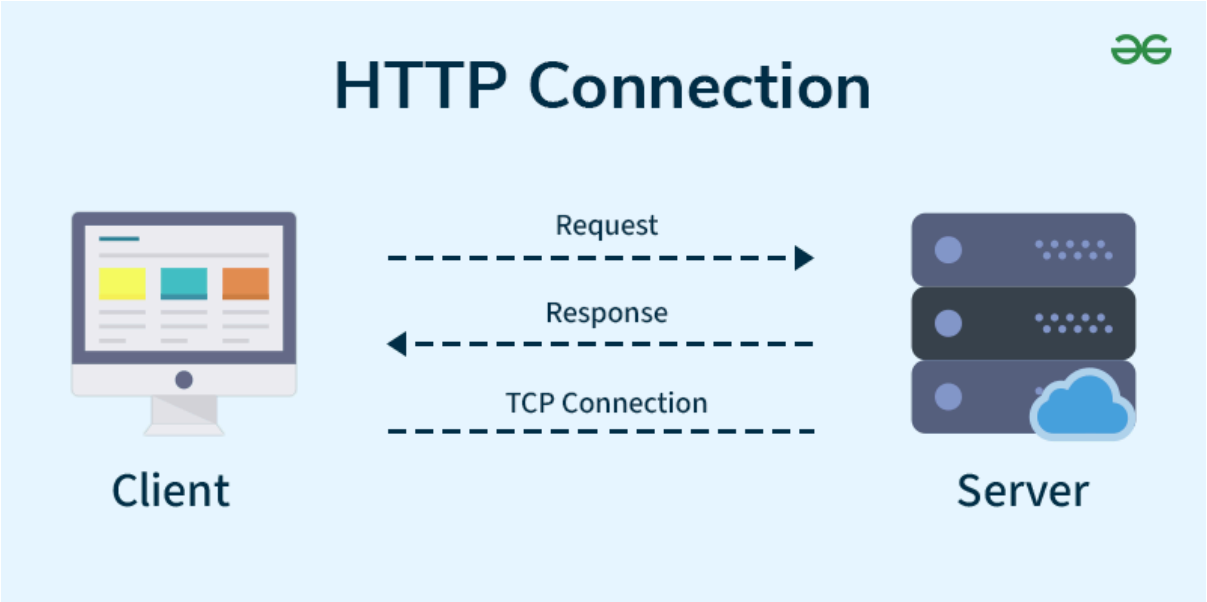
- Local DNS Resolver
- Root DNS Servers
- Top-Level Domain (TLD) DNS Servers
- Authoritative DNS Servers
- Web Server

Electronic Mail



HTTP

HTTP stands for “Hypertext Transfer Protocol.” It is a set of rules for sharing data on the World Wide Web (WWW).



HTTP status code

Three-digit codes known as HTTP status codes are most frequently used to show if an HTTP request has been fulfilled successfully. The five blocks below represent the breakdown of status codes:

- 1x Informative
- 2xx Achievement
- 3xx Reorientation
- 4xx Client Mistake
- 5xx Error on the Server