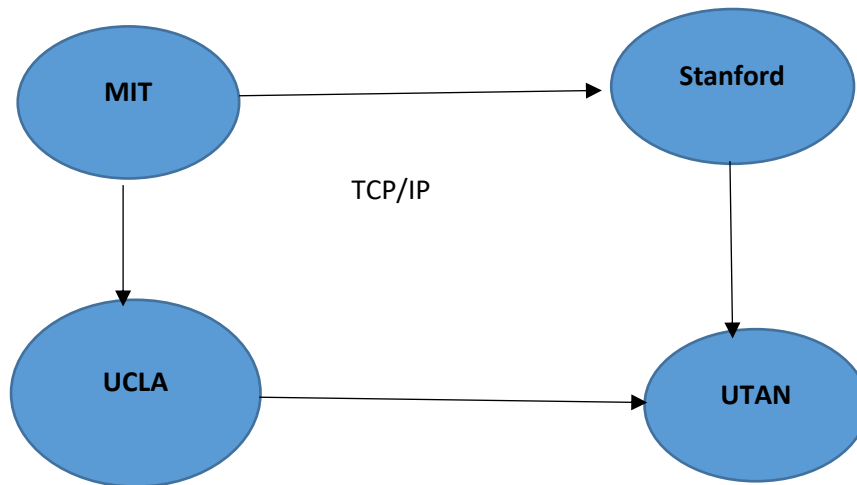# COMPUTER NETWORKING

COMPUTER: (Commonly Oriented Machine Particularly Used for Training, Education and Research)

Very First Network→**ARPA** net (Research purpose in earlier days)

```
    MIT  ───────────────▶  Stanford
     │                        │
     │        TCP/IP          │
     ▼                        ▼
   UCLA  ───────────────▶   UTAN
```

World first Web page→ **WWW (World Wide Web)**

* Collection of pages (here we don't have search engine for searching)

Website: https://info.cern.ch/hypertext/WWW/TheProject.html

Internet Society decides the protocols for internets in this RFC (Request for Comments) comes.

Website: https://www.internetsociety.org/

Our Computer can act as a server and also a client

```
                    Request
  ┌────────────┐  ───────────▶  ┌────────────┐
  │ google.com │                │   Server   │
  │            │  ◀───────────  │            │
  └────────────┘   Response     └────────────┘
     Client                       google server
```
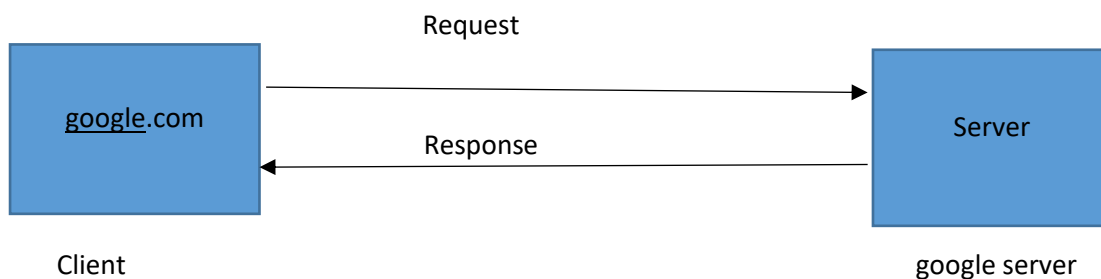
Different Types of Protocols are there:

1. TCP(Transmission Control Protocol)
2. UDP(User Datagram Protocol)
3. HTTP(Hyper Text Transfer Protocol)
4. SMTP(Simple Mail Transfer Protocol)
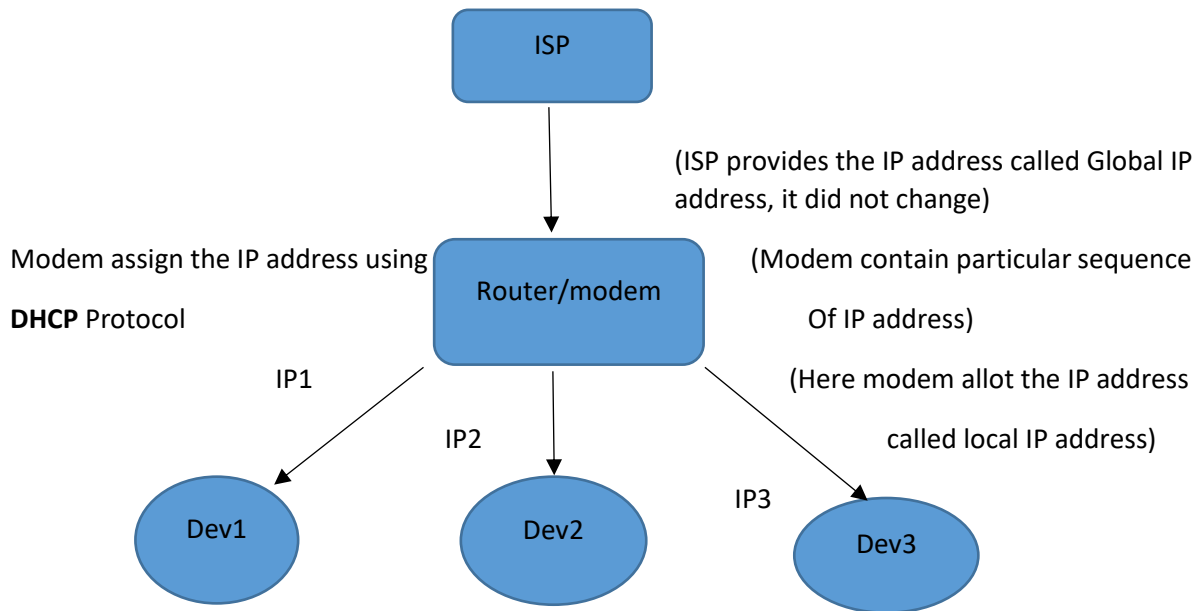5. DHCP(Dynamic Host Configuration Protocol)

These protocols are set by the internet society members.

If you send the data or file to server these are not directly transfer the total file, it split the files into chunks (small) and transfer the file or data called Packets.

IP (Internet Protocol) ADDRESS: Decides which device to send the data

Every machine has its own IP which means if you search for something that IP will goes to server and give back the response. Format: xx.xx.xx.xx (x to range 0-255)

Example:

ISP

(ISP provides the IP address called Global IP address, it did not change)

Modem assign the IP address using

DHCP Protocol

Router/modem

(Modem contain particular sequence

Of IP address)

IP1

(Here modem allot the IP address

IP2

called local IP address)

IP3

Dev1

Dev2

Dev3

NAT (Network Access Translator)→It forward the data , who want the request and send back the response.

PORTS: Decides which application to send the data in that device.

It is a 16 bit number→Total =2^16 = 65000   port numbers are available.

HTTP use the port 80 →all the searches in the web browser hit this port number.

0-1023 ports are reserved ports

1024-49152 ports are application (e.g.: SQL-1433)

Remaining we can use.

How it's connected?

It connected through two ways:

Physically: Fibre optic cables, Coaxial cables (under water-submarines)

Wireless: 3G, 4G, LTE, 5G

TYPES OF NETWORK:

LAN (Local area Network):

It is a collection of devices connected together in one physical location, such as a building, office, or home.

MAN (Metropolitan Area Network):

It is a computer network that connects computers within a metropolitan area, which could be a single large city, multiple cities and towns, or any given large area with multiple buildings. A MAN is larger than a local area network (LAN) but smaller than a wide area network (WAN).

WAN (Wide Area Network):

It is the technology that connects your offices, data centres, cloud applications, and cloud storage together. It is called a wide-area network because it spans beyond a single building or large campus to include multiple locations spread across a specific geographic area, or even the world.

It use Optical Fibre Cable. In this two main methods are there:

1. SONET(Synchronised Optical Networking): It connect through the optical fibre
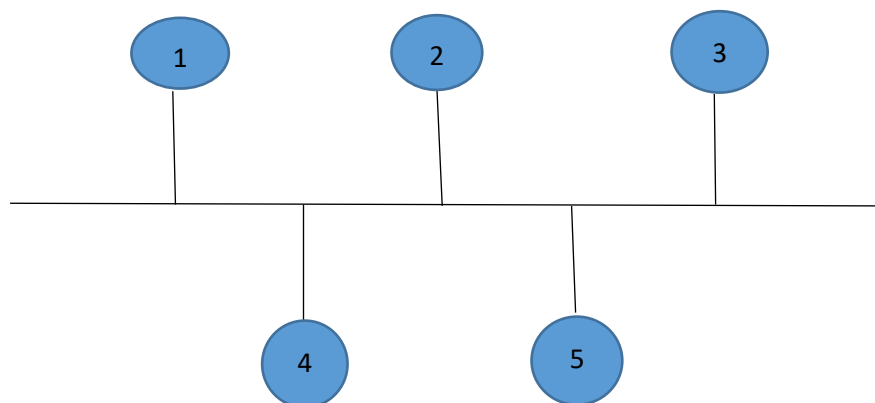2. Frame Relay: It connect LAN to the WAN

The Collection of types of network form the internet.

MODEM:

It is used to convert analog signal into digital signal and vice versa.
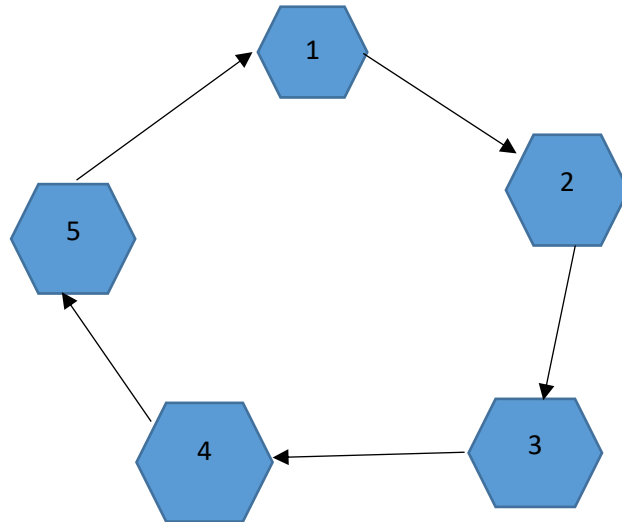
TOPOLOGIES:

BUS TOPOLOGY:

- In this network topology all the computers are connected with single cable.
- If the wire will break the next connection will be lost.
- Only one system can communicate at the same time.

RING TOPOLOGY:

- In this topology all the computers are connected together.
- If one connection is failed all the computer will lost the connection, any other information did not transfer.
- Once the data is transfer it takes the data to all the computer, it will affect the security of information.
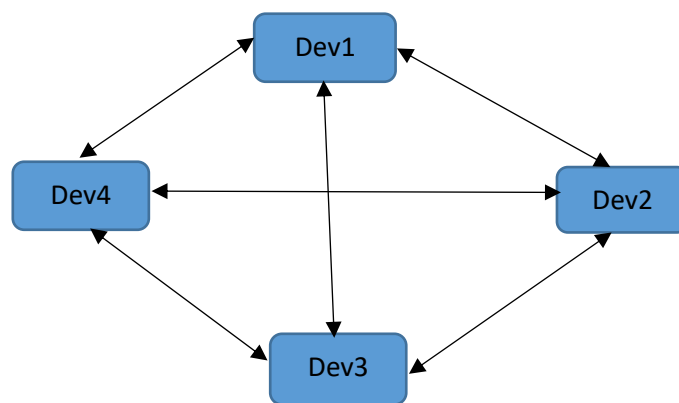
STAR TOPOLOGY:
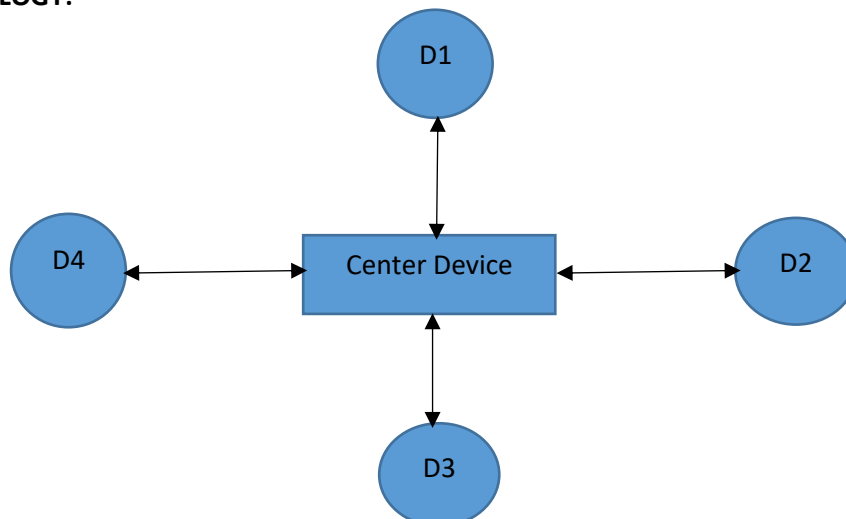
- In this topology all the computers are connected in one centralised device.
- If Centralised device fails none of the computer transfer the data, all the connection are lost.

TREE TOPOLOGY:
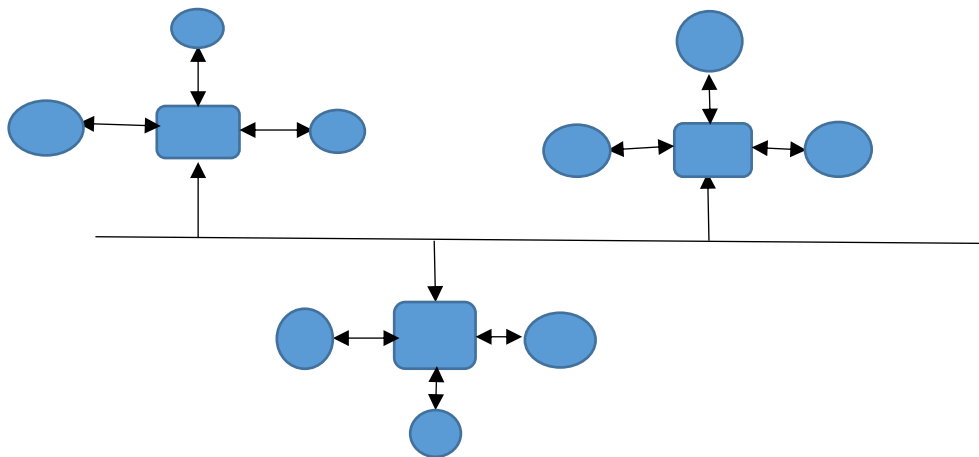
- The Combination of bus and star topology is called tree topology.
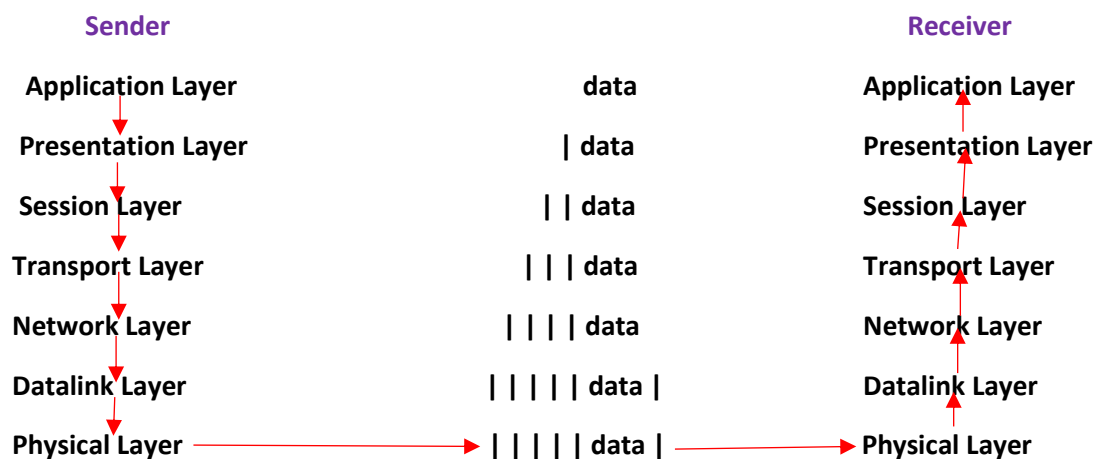- The path is connected in bus and the data's are transferred in star.

MESH TOPOLOGY:

- Each Computer is connected to another computer.
- It is most Expensive Compared with other topology.
- It has Scalability Issues because of many number of cables are needed.

How the internet works?

OSI MODEL: (Structure of the Network) (Open System Interconnection)

Sender		Receiver
Application Layer	data	Application Layer
Presentation Layer	| data	Presentation Layer
Session Layer	| | data	Session Layer
Transport Layer	| | | data	Transport Layer
Network Layer	| | | | data	Network Layer
Datalink Layer	| | | | | data |	Datalink Layer
Physical Layer	| | | | | data |	Physical Layer

1. APPLICATION LAYER:

These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

Example: Application – Browsers, Skype Messenger, etc.
Note: 1. the application Layer is also called Desktop Layer.
2. **Device or Protocol Use:** SMTP

2. PRESENTATION LAYER:

The presentation layer is also called the **Translation layer**. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

Functions of the Presentation Layer:

- **Translation:** For example, ASCII to EBCDIC.

- **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.

- **Compression/Decompression:** Reduces the number of bits that need to be transmitted on the network.
Note: **Device or Protocol Use:** JPEG, MPEG, GIF

3. SESSION LAYER:

This layer is responsible for the establishment of connection, maintenance of sessions, and authentication, and also ensures security.

Functions of the Session Layer

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

Note: These 3 layers is done by the network application itself. These are also known as **Upper Layers or Software Layers. Device or Protocol Use:** NetBIOS, PPTP.

4. TRANSPORT LAYER:

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

At the sender's side: The transport layer receives the formatted data from the upper layers, performs **Segmentation**, and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port numbers 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:**
- **Service Point Addressing:**

    1. **Connection-Oriented Service**
    2. **Connectionless service**

1. Connection-Oriented Service: It is a three-phase process that includes
- Connection Establishment
- Data Transfer
- Termination/disconnection

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.

Note:
1. Data in the Transport Layer is called **Segments**.
2. The transport layer is called as **Heart of the OSI** model.
3. The sender needs to know the port number associated with the receiver's application.
4. **Device or Protocol Use:** TCP, UDP, NetBIOS, PPTP.

For the past four layer used by networking device like Gateway.

5. 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 addresses are placed in the header by the network layer.

Functions of the Network Layer

- **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.

- **Logical Addressing:** To identify each device on Internetwork 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.

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

6. DATALINK 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 Data Link Layer is divided into two sublayers:

1. Logical Link Control(LLC)
2. Media Access Control(MAC)

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

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

Functions of the Data Link Layer

- **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.

- **Physical addressing:** After creating frames, the Data link layer adds physical addresses (MAC addresses) of the sender and/or receiver in the header of each frame.

- **Error control:** The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.

- **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving an acknowledgment.

- **Access control:** When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.
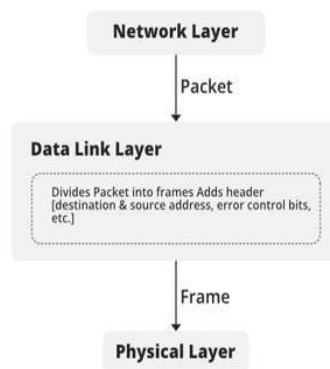
Note:
1. Packet in the Data Link layer is referred to as **Frame.**
2. Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.
3. Switch & Bridge are Data Link Layer devices.

7. PHYSICAL LAYER:

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.** 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:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at the bit level.

- **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.

- **Physical topologies:** Physical layer specifies how the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.

- **Transmission mode:** Physical layer also defines how the data flows between the two connected devices. The various transmission modes possible are simplex, half-duplex and full-duplex.

Note:
1. Hub, Repeater, Modem, and Cables are Physical Layer devices.
2. Network Layer, Data Link Layer, and Physical Layer are also known as **Lower Layers** or **Hardware Layers**.

TCP/IP (Another Model): It is used in transport layer protocol.

It is also have the layer level:

1. Application layer
2. Transport layer
3. Network layer
4. Datalink layer
5. Physical layer

A. Client- Server Architecture:
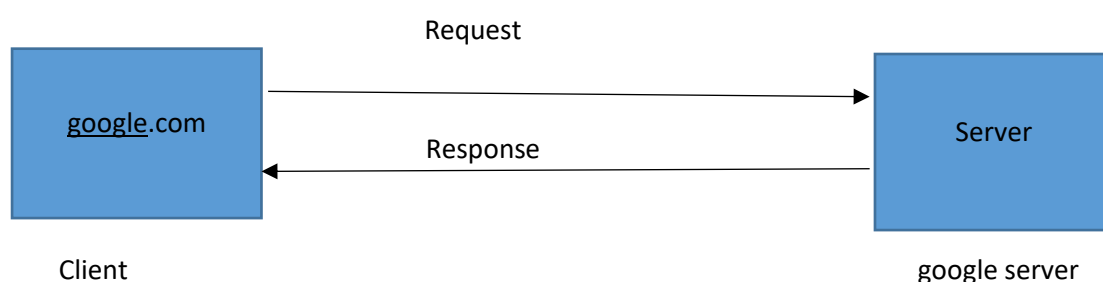
The client (eg.youtube.com) send the **request** to the youtube website, it goes to the youtube server and the server send back the **response** to the client.

B. Point to Point Architecture (Peer to Peer):

Five PCs at two different Locations
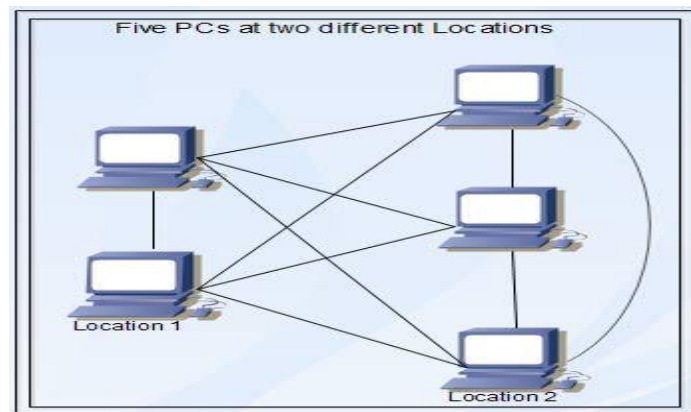
In this architecture the computer act as a client as well as server.eg: torrent

The computer act as a centralized device.

Network Devices:

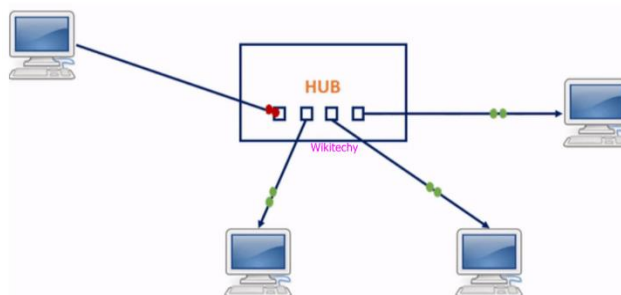**1. Repeaters:**

- ➢ Physical layer device.
- ➢ Regenerates and retransmit the incoming weak signal/data in a signal LAN.
- ➢ 2 port device. One port is getting the week (attenuated) signal and another port regenerate the signal.
- ➢ It does not amplify signal or increase the signal strength, It just regenerate the week signal/data.
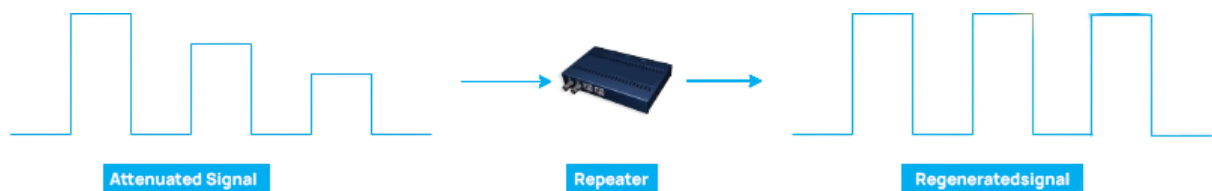
2. Hub

- ➢ Physical layer device.
- ➢ Used to connect multiple device in a single LAN.
- ➢ It broadcast the received signal/data to all other ports of the hub.
- ➢ Half duplex mode of transmission.ie one device is completely transfer the data after that another device transfer the data. In this hub data is transfer to all the connected devices

Two types of hub:

A. passive hub: It broadcasts the received signal/data to all other ports of the hub.

B. Active hub: It regenerates the received signal and broadcasts to all other ports of the hub. * It is a multiport repeater.

3. Switch:

➢ Datalink layer device.
➢ Used to connect multiple devices in a single LAN.
➢ It examines the destination MAC Address of the received signal/data and retransmits the signal/data to the corresponding device.
➢ Full duplex mode of transmission. It transfer the data simultaneously to the other device.
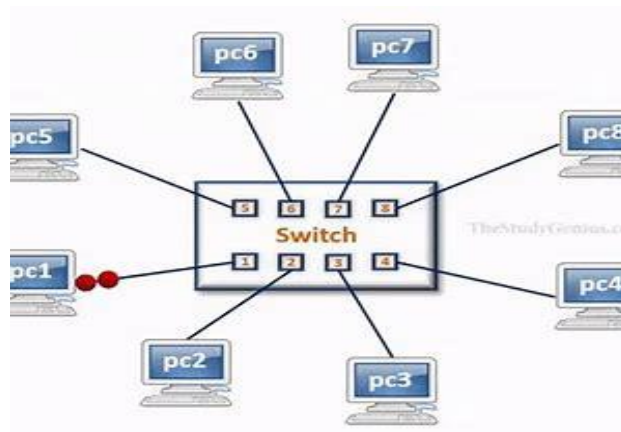
4. Bridge:

➢ Datalink layer device.
➢ Used to connect 2 LAN working on a same protocol.
➢ Used to divide a large network into smaller segments.
➢ Has MAC address reading capability.
➢ Can also regenerate a week signal like repeater.
➢ It reduce the data traffic.
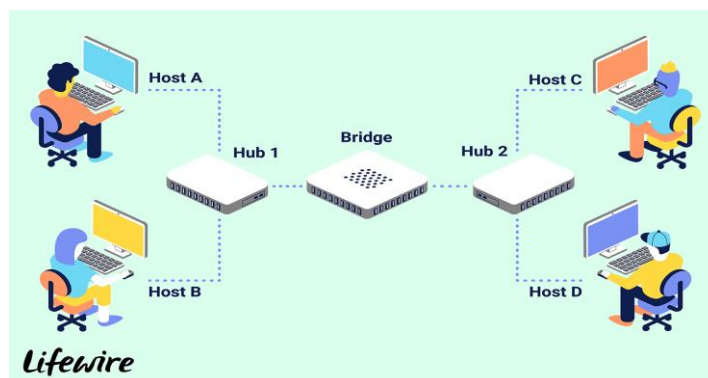
5. Router:

- ➢ Network Layer device.
- ➢ Used to connect multiple LAN and WAN together working on same protocols.
- ➢ Forward data packets based on IP address.
- ➢ To forwards data packets, routers always maintain routing table.
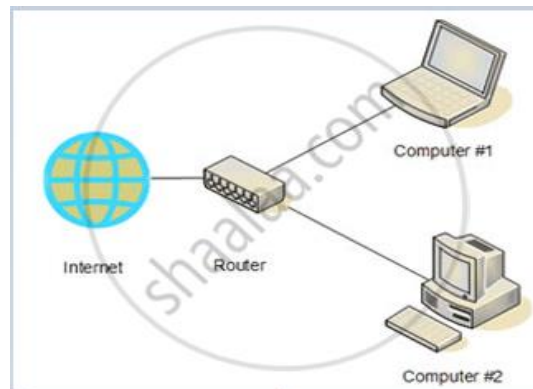
6. Gateway:

- ➢ Works on upper layer of the OSI model.(Application, Session, Presentation and Transport layer)
- ➢ Used to connect dissimilar networks together working on different set of protocols.
- ➢ Also called protocol converters.
- ➢ Depending on the functionality, a gateway can operate at the any of the 7 layers of OSI model.
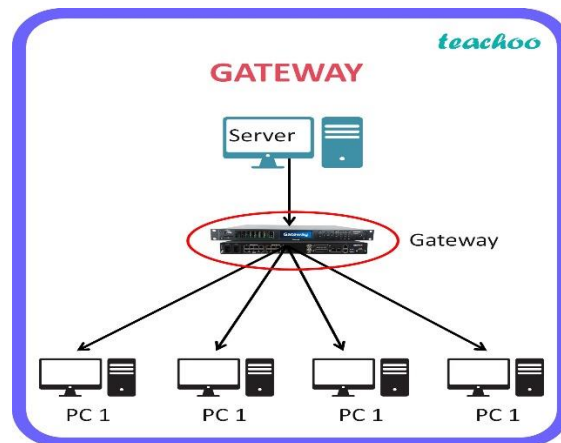
Socket: It is the combination of port and IP address. It is used to identify both a machine and a service within the machine.

HTTP (Hyper Text Transfer protocol):

It is used in the Application layer protocol. (SMTP, POP3-post office protocol)

It is used to getting request and response from the website or particular server.

It is stateless protocol.

Cookies: It is the text files with small pieces of data — like a username and password — that are used to identify your computer as you use a network. Specific cookies are used to identify specific users and improve their web browsing experience. It is a unique String. It contain Third Party Cookies used for other member don't access our stored information.
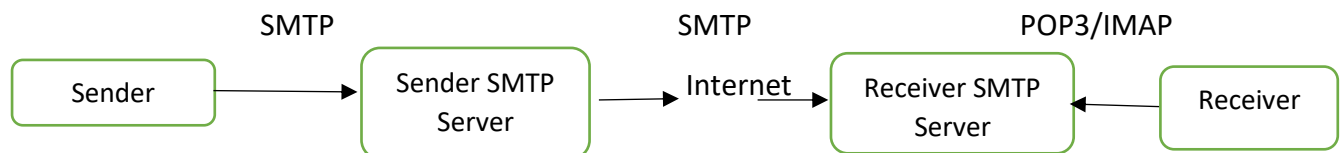
It has many methods like get, post, put, delete etc. these are used to find which operation is done by the server.
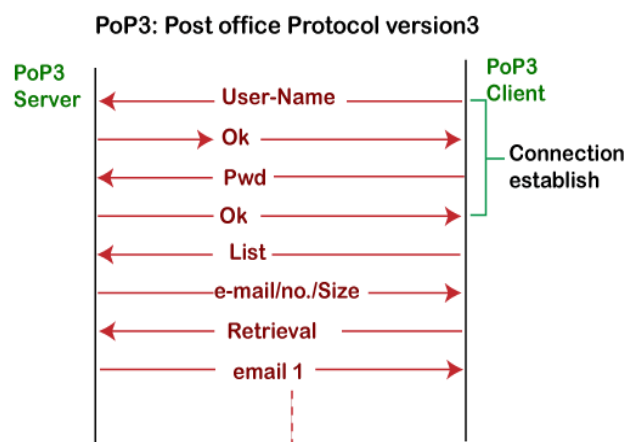
Status code:

- ✓ **1xx** → Informational
- ✓ **2xx** → Success message
- ✓ **3xx** → Redirecting
- ✓ **4xx** → Client Error
- ✓ **5xx** → Server Error

How mail works?

Simple Mail Transfer Protocol (SMTP):

1. POP3:

2. IMAP (Internet Message Access Protocol):

Internet Message Access Protocol (IMAP) is a protocol for accessing email or bulletin board messages from a (possibly shared) mail server or service. IMAP allows a client e-mail program to access remote message stores as if they were local. Email stored on an IMAP server can be manipulated from a workstation at the office, a desktop computer at home or a notebook computer while traveling, without requiring the transfer of messages or files back and forth between these computers.

DNS (Domain Name System):

It helps Internet users and network devices discover websites using human-readable hostnames, instead of numeric IP addresses. It is used by UDP because it is fast.
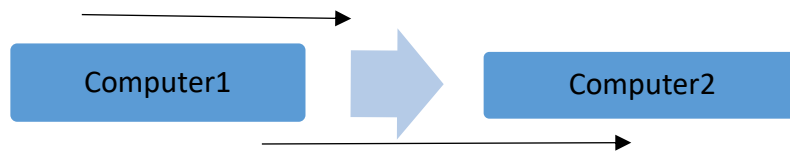
E.g.: mail.google.com [mail→Sub domain, google→Second level domain, .com→Top level domain]
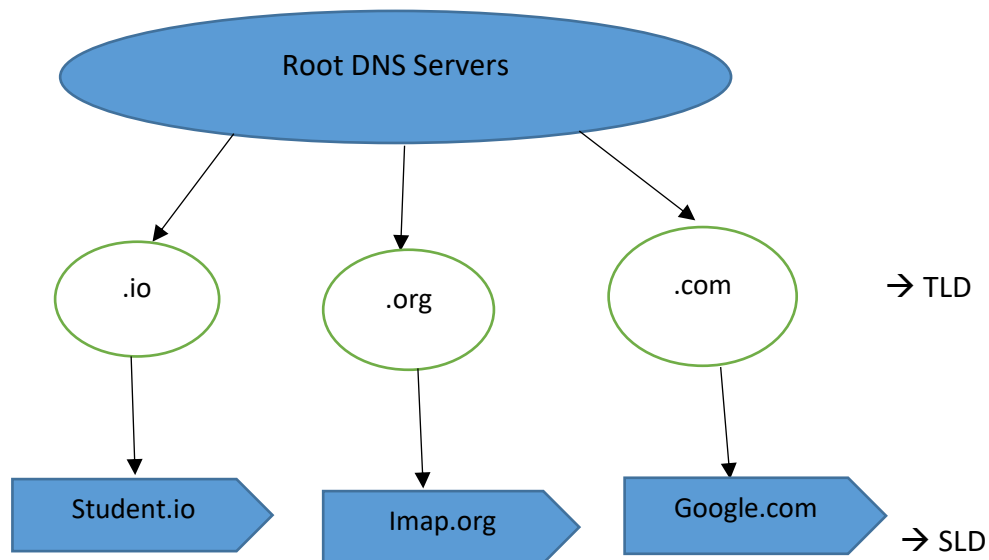
.io, .com, .org → this databases are stored and managed by ICANN (Internet Corporation for Assigned Names and Numbers).
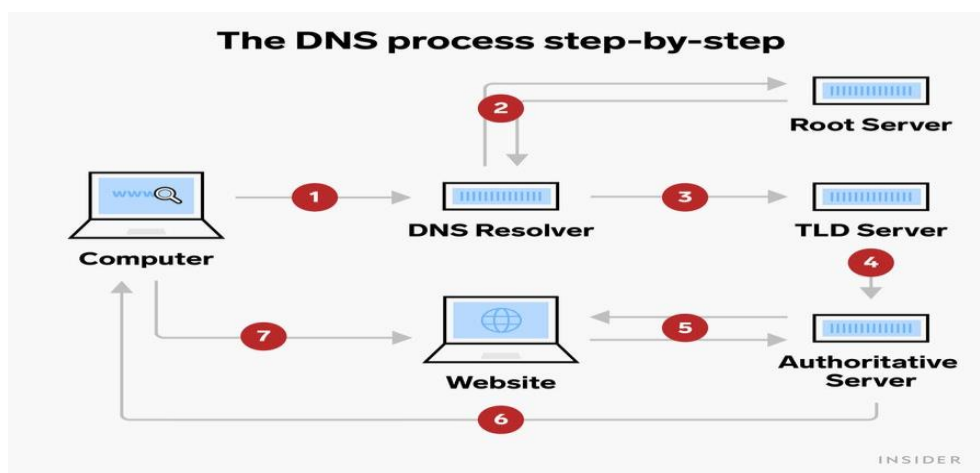
Transport layer→ within device take the information from the network to the application

Network layer→ it transfer the data from one device to another device.

Transport layer contain **multiplexer** and **demultiplexer** within the device for transferring the various types of data's in one format called multiplexer and vice versa called demultiplexer. In this intermediate the socket is connected which is stored port number.

Transport layer use TCP/UDP protocol.

Congestion control: It occurs when a network is overrun with more data packet traffic than it can cope with.

Checksum: It is a value that represents the number of bits in a transmission message and is used by IT professionals to detect high-level errors within data transmissions. It is used to check the data's are corrupted or not.

Timers:

TCP sets the timer when it sends the data segment and expects an ACK from receiver for this data segment before the time expires. To identify the data we use sequence number.

> ➤ If ACK arrives before timer goes off, TCP believes the segment has been successfully delivered.
> ➤ If timer goes off and ACK has not arrived yet, TCP assumes segment has been lost and it retransmit the same segments.
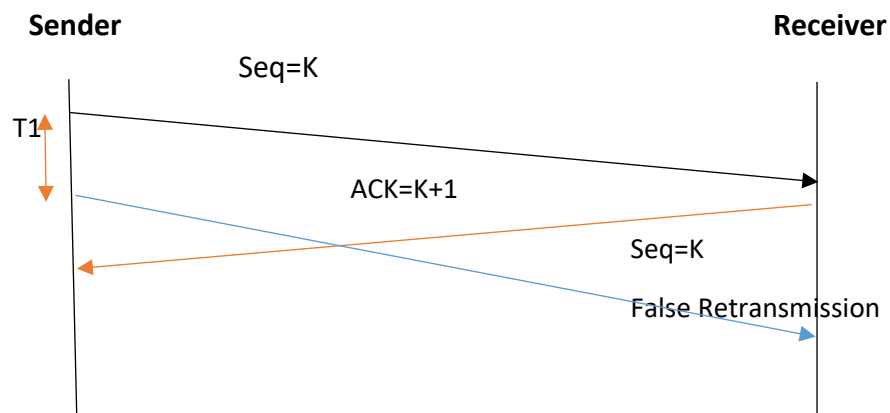
1. Too long RTO
   Network under Utilization
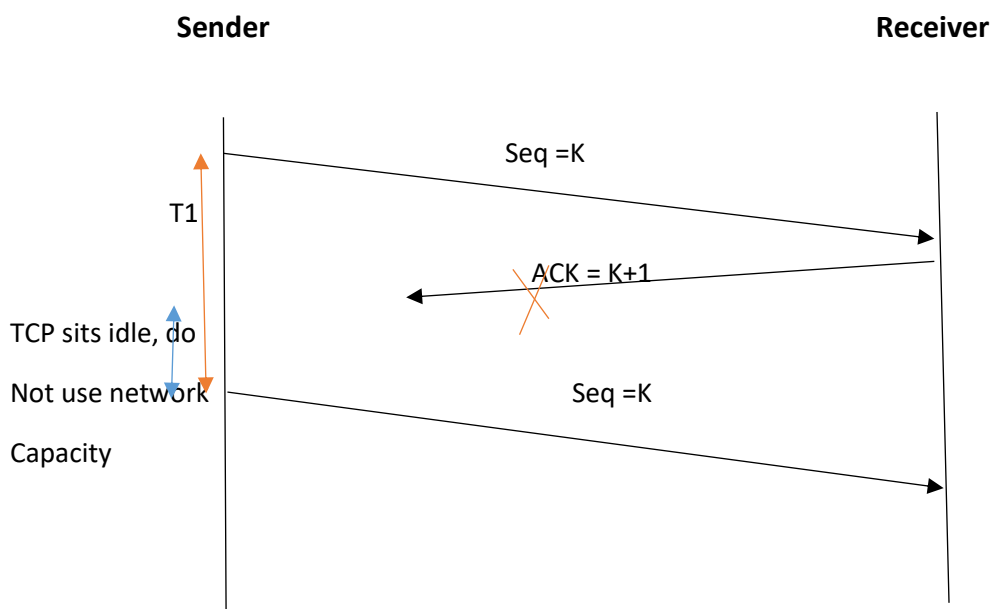
2. Too short RTO

Unnecessary Retransmission

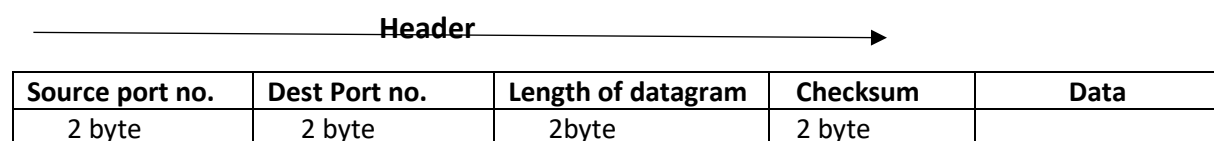Network Congestion

UDP (User datagram Protocol):

➢ Data may or may not be delivered.

➢ Data may change on the way.

➢ Data may not be in the order.

➢ It is a connectionless protocol. It also uses Checksum.

UDP Packet:

Header ──────────────────────────────→

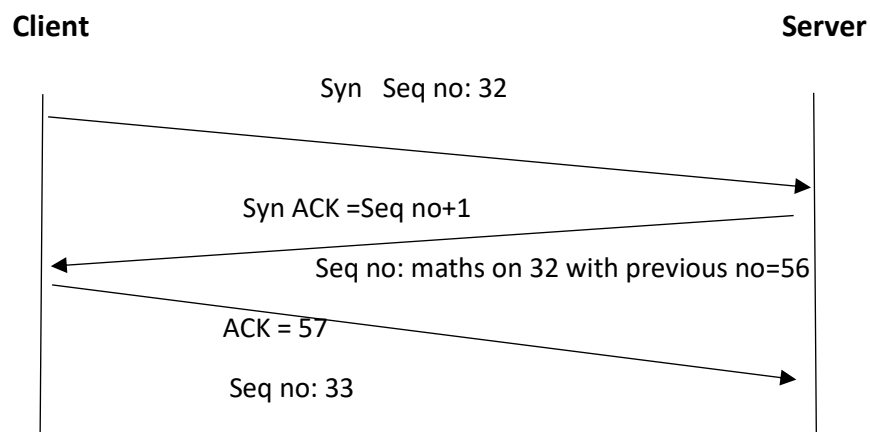| Source port no.	Dest Port no.	Length of datagram	Checksum	Data
2 byte	2 byte	2byte	2 byte	

Total size =2^16 → 2^16 – 8 = 65,536 bytes.

TCP (Transmission Control Protocol):

➢ Application layer sends lots of raw data to TCP which is in transport layer, that TCP segments this data (divide in chunks) and add header. It may also collect the data from the network layer. In this the data packet contain sequence number and acknowledge number.

➢ TCP protocol only connects between two computers.

➢ It take care of two things:

1. When data does not arrive.
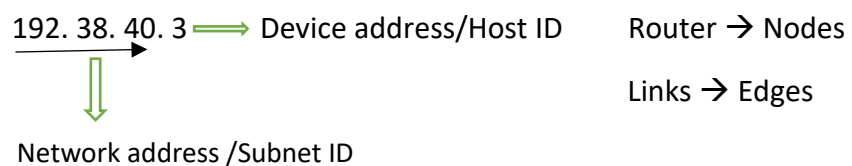2. Maintains the order of the data.

Features:

➢ Connection Oriented.

➢ Error Control.

➢ Congestion Control.

➢ Full Duplex.

3 way handshake:

Client   Server

Syn   Seq no: 32

Syn ACK =Seq no+1

Seq no: maths on 32 with previous no=56

ACK = 57

Seq no: 33

Network layer use IP address:

192. 38. 40. 3 ⟹ Device address/Host ID   Router → Nodes

Links → Edges

Network address /Subnet ID

   It uses Router which is managed by routing table. This routing table are controlled by Control plane, two types of Routing:

1. Static Routing → Manually
2. Dynamic Routing → It use different algorithm
   190.89.9.0/31 →subnet mask (obtain 31 bits remaining 1 bit consider as 0)

IP address:

IPv4 → 32 bits, 4 words → 192(8 bit).42(8 bit).1(8 bit).2(8 bit)

Classes of IP address:

Class A →   0.0.0.0   127.255.255.255

Class B →   128.0.0.0   191.255.255.255

Class C →   192.0.0.0   223.255.255.255

Class D →   224.0.0.0   239.255.255.255

Class E →   240.0.0.0   255.255.255.255

Reserved Address: 127.0.0.0/8 → e.g.: localhost 127.0.0.1 loopback address

Packets contain IP version, length, Identification number, Protocols, Checksums, address, TTL (Time to Live), etc.

IPv6 → 128 bits =2^128 =3.4* 10^38 e.g. a: a: a: a: a: a: a: a (each value contain 16 bit hexadecimal).

Datalink Layer uses DHCP protocol.

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

Middle Boxes:

➢ A middlebox is a computer networking device that transforms, inspects, filters, and manipulates traffic for purposes other than packet forwarding.
➢ Examples of middleboxes include firewalls, network address translators (NATs), load balancers, and deep packet inspection (DPI) devices.

Firewall:

➢ It is a device used for network security. It monitors network traffic – both incoming and outgoing – to either allow or block data packets based on its security rules.
➢ Its purpose is to create a barrier between your internal networks and traffic that flows in from external sources – like the rest of the internet. This blocks hackers, viruses and other malicious traffic.

Firewalls protect your website against the following:

1. Brute Force Attacks
2. DDoS Attacks
3. Malware