__/__/____

COMPUTER NETWORKS.

A computer network is a set of devices connected through links. A node can be computer, printer, or any other device.

The links connecting the nodes are known as communication channels.

It is a group of computers connected with each other wires, optical fibres or optical links so that various devices can interact with each other through a network.

* Major Components of a Computer Network.

- **Hub**

It is a central device that splits the network connection into multiple devices. When computer requests for information from a computer, it sends the request to the Hub.

Hub distributes this request to all the interconnected computers.

- **Switches**

Switch is a networking device that groups all the devices over the network to transfer the data to another device. A switch is better than Hub as it does not broadcast the message over the network i.e. it sends the message to the device for which it belongs to.

Switch send messages directly from S → D.

- Cables and Connectors.

Cable is a transmission media that transmits the communication signals.

1) Twisted pair cable :- It is a high-speed cable that transmits data over 1GBPS or more

2) Coaxial Cable :- Coaxial cable resembles like a TV installation cable. Coaxial cable is more expensive than twisted pair.

3) Fibre optic Cable :- It is a high speed cable that transmits the data using light beams. It provides high data transmission speed as compared to other cables. It is more expensive compared to other cables.

- Router

Router is a device that connects the LAN to the internet.

The router is mainly used to connect the distinct networks or connect the internet to multiple computers.

__/__/____

- Modem

Modem connects the computer to the internet over the existing telephone line. A modem is not integrated with the computer motherboard.

A modem is a separate part on the PC slot found on the motherboard.

- NIC (National Interface Card)

It is a device that helps the computer to communicate with another device.

NIC contains hardware addresses, the data link layer protocol use this address to identify the system on the network so that it transfers the data to the correct destination.

1) Wireless NIC 2) Wired NIC

* Features of Computer Network

1) Communication Speed.

2) File sharing.

3) Back up and Roll back is easy.

4) Software and Hardware sharing.

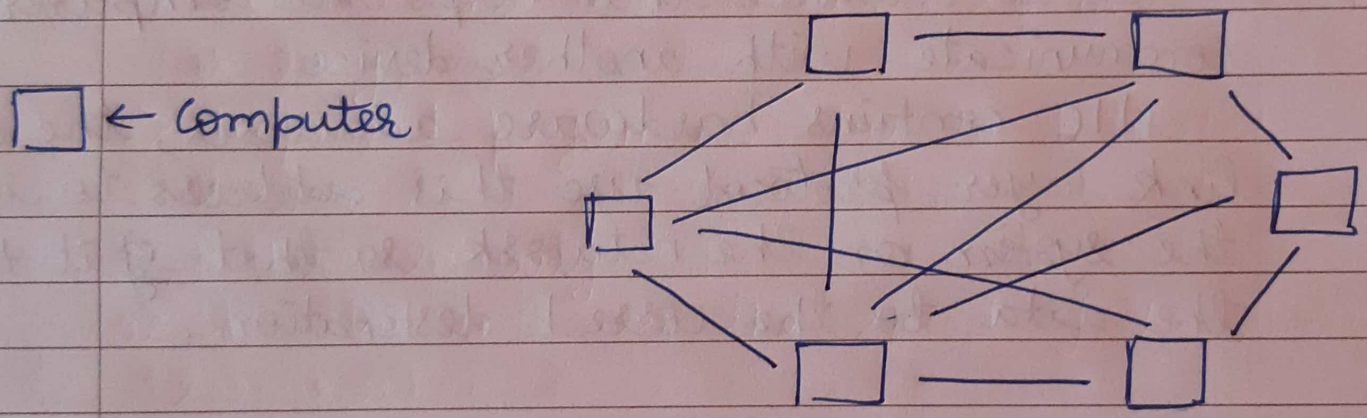
5) Security.

6) Scalability.

7) Reliability.

* Architecture

1) Peer-to-Peer Network.



- It is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data. (Upto 10 computers)

- It has no dedicated server

- Special permissions are assigned to each computer for sharing the resources.

__/__/__

- Advantages.

i) It is less costly as it does not contain any dedicated server.
ii) If one computer stops working, others won't.
iii) It is easy to set up and maintain as each computer manages itself.

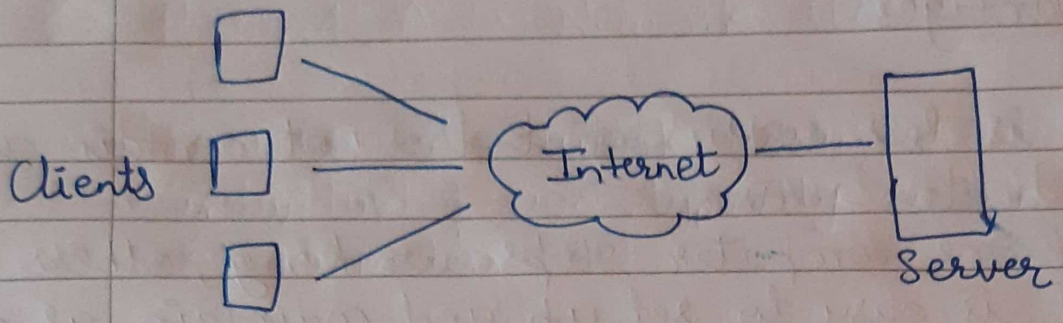
- Disadvantages

i) Data is in different locations. So, no backup of data.
ii) It does not contain a centralized system.
iii) It has a security issue as the device is managed by itself.

2) Client/Server Network.

- Client/Server network is a network model designed for the end users called clients, to access the resource such as songs, videos from a central computer known as Server.

- The central controller is known as Server while all other are called clients.



-Advantages

1) It contains the centralized system. So, backup is easy.
2) Improved performance due to dedicated server.
3) Better security.
4) It also increases the speed of the sharing resources.

-Disadvantages

1) Expensive as it requires the server with large memory
2) The server has a Network Operating System (NOS) to the provide the resources to the clients, but cost of NOS is very high.

3) It requires a dedicated network administrator to manage all the resources.

__/__/____

* Computer Network Types.

1) LAN (Local Area Network)

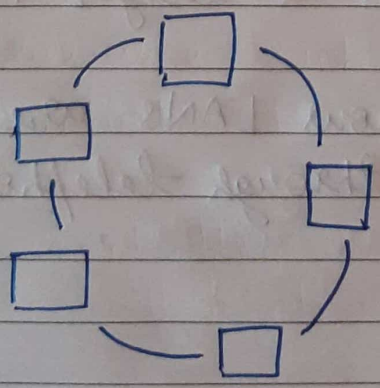
- Local Area ~~Netw~~ Network is a group of computers connected to each other in a small area such as building, office, etc.

- It is used for connecting two or more PCs through a communication medium such as twisted pair, coaxial cable, etc.

- It is less costly as it built with inexpensive hardware such as hubs, network adaptors, and ethernet cables.

- The data is transferred at an extremely ~~fear~~ faster rate in LAN.

- It provides higher security.



2> Personal Area Network (PAN)

- PAN is a network arranged within an individual person, typically within a range of 10 meters.

- It covers an area of 30 feet.

- Personal devices that are used to develop the network are the laptop, mobile phones, media player and play stations.

Wireless PAN - Developed by WiFi, Bluetooth.
Wired PAN - Developed by using the USB.

3> Metropolitan Area Network (MAN).

- It is a network that covers a large geographic area by interconnecting a different LAN to form a larger network.

- In MAN, various LANs are connected to each other through telephone exchange line.

__/__/____

4) ~~Wired~~ Wide Area Network (WAN)

- A wide area network is a network that extends over a large geographical area such as states or countries.

- The internet is one of the biggest WAN in the world.

- Advantages

1) Geographical Area.
2) Centralized data.
3) Get ~~upded~~ updated files.
4) Exchange messages
5) Sharing of softwares and resources.
6) High bandwidth.

- Disadvantages

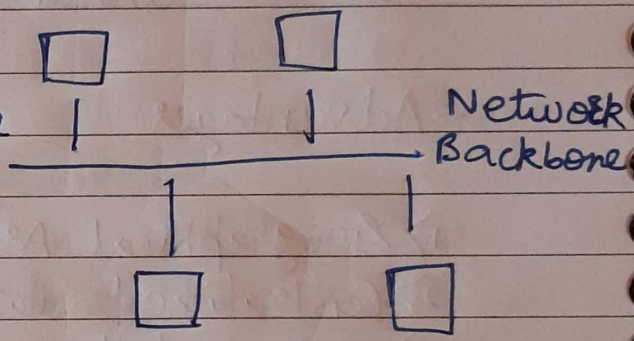
1) Security issue.
2) Needs firewall & antivirus software.
3) High setup cost
4) Troubleshooting problems.

* Topology

Topology defines the structure of the network of how all the components are inter-connected to each other.

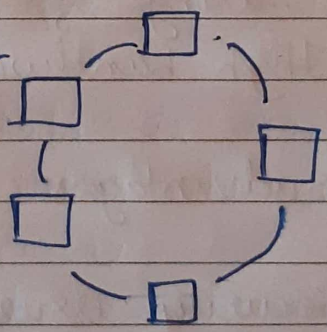
1) Bus Topology

Stations are connected to the network backbone through a single cable.



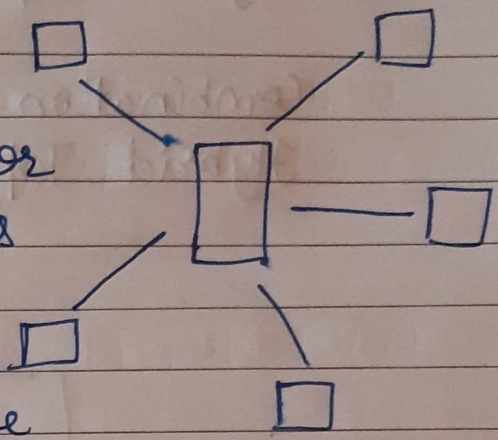
2) Ring Topology.

It is like bus topology but with connected nodes.
The data flows in only one direction.



The most common acess of ring topology is token passing.
Token is a frame that circulates around the network.

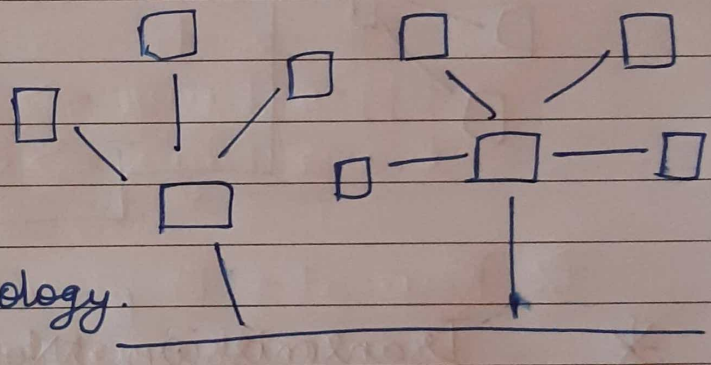
3) Star Topology



Here, every node is connected to the central hub, switch or a central computer known as server.

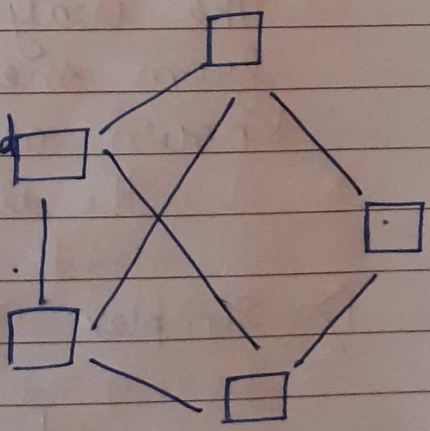
Coaxial cables or RJ-45 cables are used to connect the computers.

4) Tree topology



It combines the characteristics of bus topology and star topology.

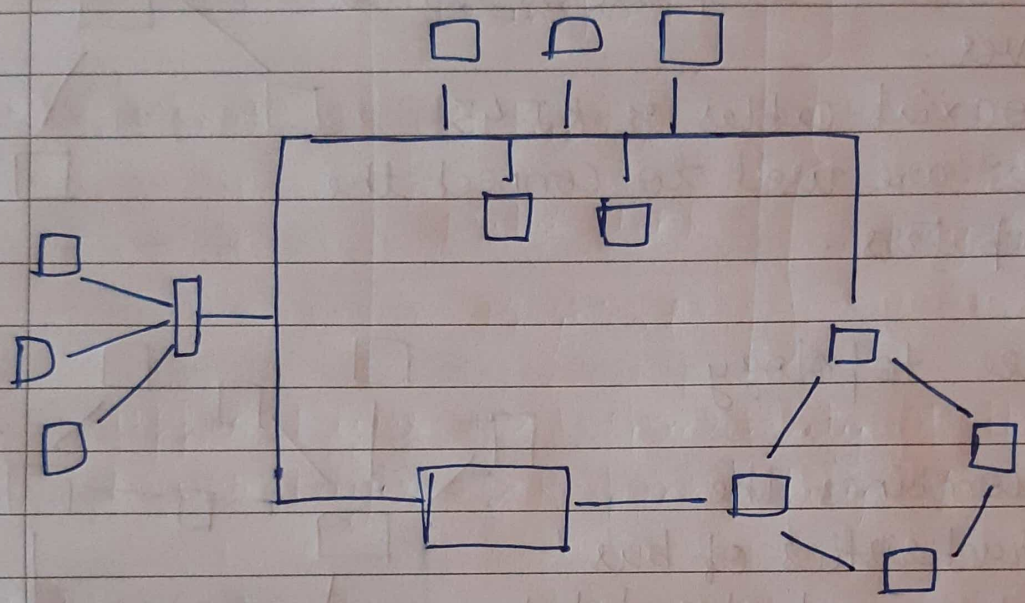
5) Mesh topology



Here, the nodes are interconnected with each other through various redundant connections.

6> Hybrid Topology

Combination of various topologies is known as Hybrid Topology.

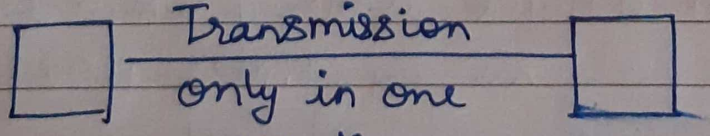


* Transmission ~~Modes~~ Modes

The way in which data is transmitted from one device to another device is known as transmission mode.

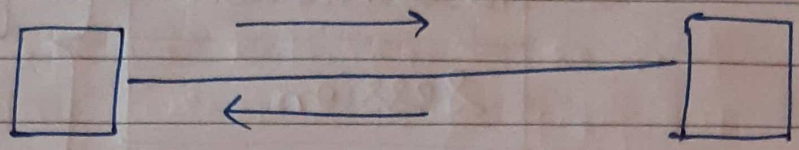
It is defined in the to physical layer.

1> Simplex Mode



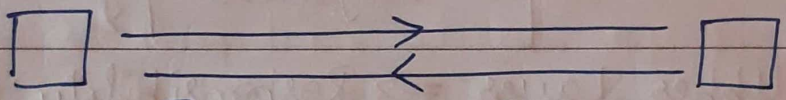
__/__/____

2) Half duplex mode.



Transmission in either direction, but not simultaneously.

3) Full Duplex Mode.



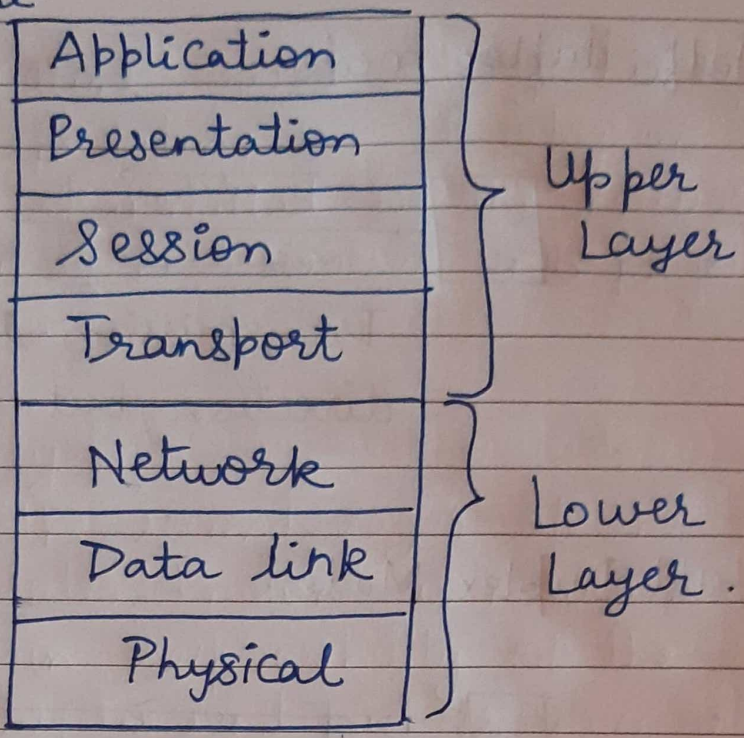
Transmission in both the directions simultaneously.

* OSI MODEL

- Open System Interconnection.
- Seven-Layer Model.
- The model is divided into two layers: Upper and Lower layers
- The upper layer of the OSI model mainly deals with the application related issues, and are implemented only in the software.
- The lower layer of the OSI model deals with transport related issues.

__/__/____

Architecture



Upper Layer ⇒ Responsibility of the Host
Lower Layer ⇒ Responsibility of the Network

1) Physical - It provides a physical medium through which bits are transmitted.

2) Data link - It is used for error free transfer of data frames.

3) Network - It is responsible for moving the packets from source to destination.

4) Transport - It provides reliable message delivery from process to process.

5) Session - It is used to establish, manage and terminate the sessions.

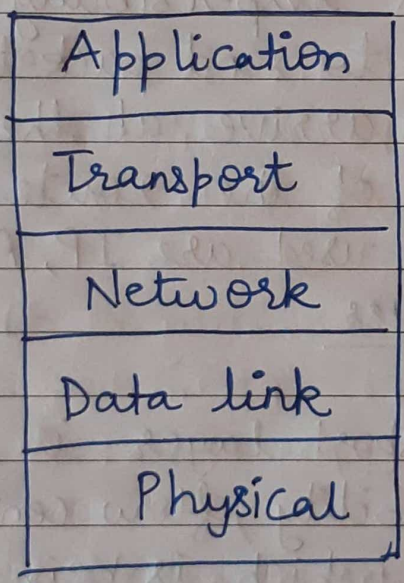
__/__/____

6) Presentation - It is responsible for translation, compression's encryption.

7) Application - This layer provide the services to the user.

* TCP/IP MODEL

- 5 Layer Model



1) Network Access Layer
- It is the lowest layer of the TCP/IP Model
- It is the combination of the Physical Layer and the Data Link Layer defined in the OSI Model.
- It defines how the data should be sent physically through a network.

- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.

2) Internet Layer

- It is the second layer of the model.
- It is also known as network Layer.
- The main responsibility of the internet layer is to send packets from any network, and they arrive at the destination irrespective of the route that take.
  Protocols used are IP, ARP, ICMP.

3) Transport Layer

- The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.
- The two protocols used in this layer are UDP and TCP.

4) Application Layer

- Topmost layer in the TCP/IP model.
- It responsible for handling high-level protocols, issues of representation.

__/__/____

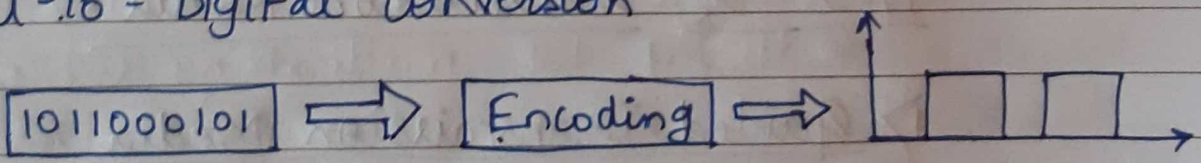
- This layer allows the user to interact with the application.
- When one application layer wants to forward its data to another application layer, it ~~com~~ forwards it data to the transport layer.
- Protocols in the Application Layer are HTTP, SNMP, SMTP, DNS, TELNET, FTP.

* PHYSICAL LAYER

→ Digital Transmission

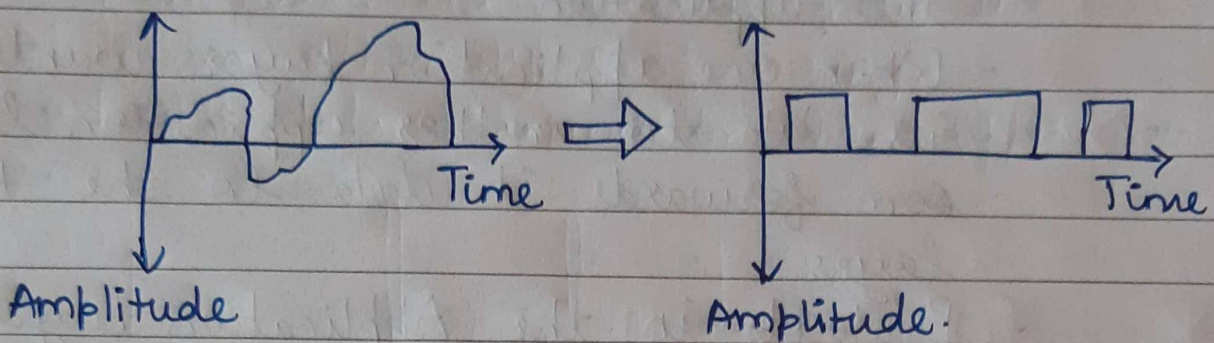
Data can be represented either in analog or digital form. Therefore, the data needs to be converted in digital form so that it can be used by a computer.

i) Digital-to-Digital Conversion



Types of encoding
- Unipolar
- Polar
- Bipolar.

2> Analog-to-Digital Conversion.



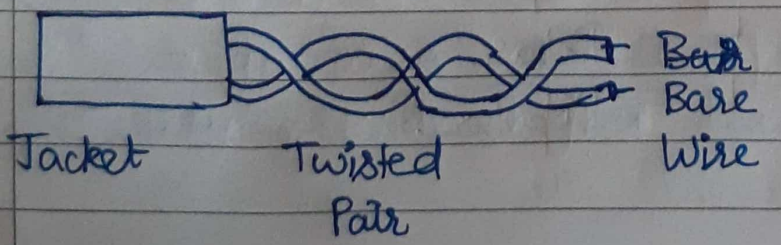
→ Transmission Media

-Transmission Media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through electromagnetic signals.
-The main functionality of the transmission media is to carry the information in the form of bits through LAN (Local Area Network)

Types of Transmission Media :-

1> Guided Transmission Media

• Twisted Pair cable

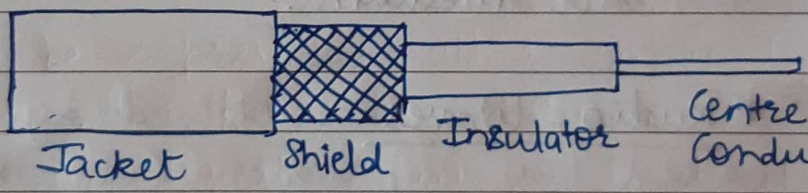


It is made up of a pair of cables twisted with each other.

NOTE → Copper-based network, bits are in the form of electrical signals.
Fibre-based network, bits are in the form of light pulses.

• Coaxial Cable

- The name of the cable is coaxial as it contains two conductors parallel to each other.
- The inner conductor is made up of copper mesh. The middle core is made up non-conductive cover that separates the inner conductor from the outer.
- The middle core is responsible for the data transferring whereas the copper mesh prevents from the EMI (Electromagnetic interference).



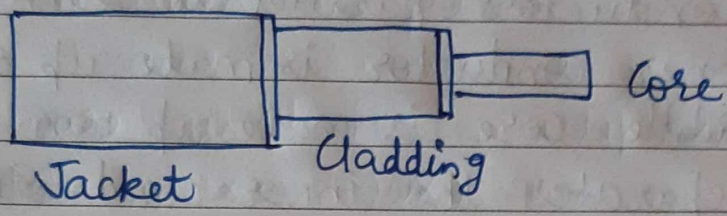
Types of Coaxial Cable

- Baseband transmission - single signal at high speed
- Broadband transmission - Multiple signals simultaneously.

• Fibre optic Cable

- Uses electrical signals for communication.
- It is a cable that holds the optical fibres coated in plastic that are used to data by pulses of light.

- The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring.
- Faster data transmission than copper wires.



2> Unguided Transmission Media

- Wireless transmission.
- Air medium.

• Radio Waves

- Omnidirectional i.e. signals are propagated in all directions.
- Range is from 3KHz - 1GHz (Frequency)
- Useful for multicasting when there is one sender and many receivers.
  Eg. FM, Television, cordless phones.
- It is mainly used for wide area networks and mobile cellular phones. They cover a large area, and can penetrate the walls.
- They provide higher transmission rate.

__/__/____

- **Microwaves.**

  - Travel in straight line, so the transmitter and receiver should be accurately aligned to each other i.e. unidirectional.
  - Frequency range is from 1GHz to 300GHz.
  - Cannot pass through buildings.
  - Communication over ocean can be achieved through microwaves.

- **Infrared Waves**

  - It is a wireless technology used for communicat-ion over short ranges.
  - The frequency is from 300GHz to 400THz.
  - Data transfer between two cell phones, TV remote operation, data transfer between computer and cellphone
  - Supports high bandwidth.
  - ~~For~~ Cannot penetrate walls.
  - Provides better security with minimum interference.

→ Multiplexing and Demultiplexing

- Multiplexing is a technique used to combine and send the multiple data streams over a single medium. The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as Multiplexer (MUX)

- Multiplexer combines n input lines to generate a single output line. Multiplexing follows ~~One~~ many-to-one i.e. n input lines and one output line.

- Demultiplexing is achieved by using a device called Demultiplexer ~~(OE~~ (DEMUX) available at the receiving end. Demux separates a signal into its component signals i.e. 1 input and n outputs

- Therefore, ~~we~~ Demultiplexing follows one-to-many approach.

- If there are multiple signals to share one medium, then the medium must be divided in such a way that each signal is given some portion of the available bandwidth.

__/__/____

- When multiple signals share the common medium, there is a possibility of collision. Multiplexing concept is used to avoid such collision.

Techniques for Multiplexing

- Frequency-Division Multiplexing (FDM)
- Wavelength-Division Multiplexing (WDM)
- Time-division Multiplexing (TDM)

→ Switching

- When a user accesses the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information from one computer network to another network is known as switching.

- Switching in a computer network is achieved by using switches. A switch is a small hardware device which is used to join multiple computers together with one local area network (LAN).

- Switches are used to forward the packets based on MAC Addresses.

- A switch is used to transfer the data only to the device that has been addressed. It verifies the destination address to route the packet appropriately.

- It is operated in full duplex mode.

- Package collision is minimum as it directly communicates between source & destination.

- Switch increases the bandwidth of the network.

* DATA LINK LAYER

- The main responsibility of the Data Link Layer is to transform the datagram across an individual link.

- The Data link layer protocol defines the format of the packet exchanged accross the nodes as well as the actions such as Errors, detection, retransmission, flow control, random access.

- The Data Link Layer protocols are Ethernet, token ring, FDDI, PPP.

__/__/____

Services provided by Data link layer :-

→ Framing and Link access.
→ Reliable Delivery.
→ Flow control.
→ Error Detection.
→ ~~Error~~ Error Correction.
→ Half Duplex & Full Duplex.

* NETWORK LAYER

- The main role of the network layer is to move packets from sending host to the receiving host.

- It handles the service requests from the transport layer and further forwards the service request to the data link layer.

- The network layer translates the logical addresses into physical addresses.

- It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.

__/__/____

→ Routing

- A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.

- Routing is a process of selecting path along which the data can be transferred from source to the destination.

- A router works at the network layer in the OSI model and internet layer in TCP/IP.

- A routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.

- The routing protocols use the metric to determine the best path for the packet delivery. The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path, etc. used by the routing algorithm to determine the optimal path to the destination

Types of Routing
- Static Routing
- Dynamic Routing
- Default Routing.

NOTE :- MAC address is used to identify the actual device.
IP address is used to locate a device on network.
MAC → Media Access Control.

→ Protocols

1) ARP (Address ~~Resolut~~ Resolution Protocol)
- It is a network layer protocol which is used to find the physical address from the IP address.

Reply – Request Type of Protocol
Request - When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.

Reply - Every device attached to the network will accept the ARP request and process the request but only recipient recognizes the IP address and sends back its physical address in the form of ARP reply.

2) RARP (Reverse Address Resolution Protocol)

- It The protocol which is used to Obtain the IP address from a server is RARP.

- If a host wants to know its IP address, then it broadcast the RARP query packet that contains its physical address to the entire network. A RARP server on the network recognizes the RARP packet and responds back with the host IP address.

- The message format of the RARP protocol is similar to the ARP protocol.

3) ICMP (Internet control Message Control).

- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.

- A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disable links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.

ICMP protocol uses two terms:

ICMP Test :- It is used to whether the destination is reachable or not.

ICMP Reply :- It is used to check whether the destination device is responding or not.

- The core responsible of ICMP protocol is to report the problems, not correct them. The responsibility of correction lies with the sender.

__/__/____

* TRANSPORT LAYER.

- The main role of the transport layer is to provide the communication services directly to the application processes running on different hosts.

- The application processes on different hosts are not physically connected, application processes use the logical communication provided by the transport layer to send the messages to each other.

- TCP and UDP are 2 transport layer protocols that provide a different set of services to the network layer.

- All transport layer protocols provide multiplexing / demultiplexing service. It also provides other services such as reliable data transfer, bandwidth guarantees, and delay guarantees.

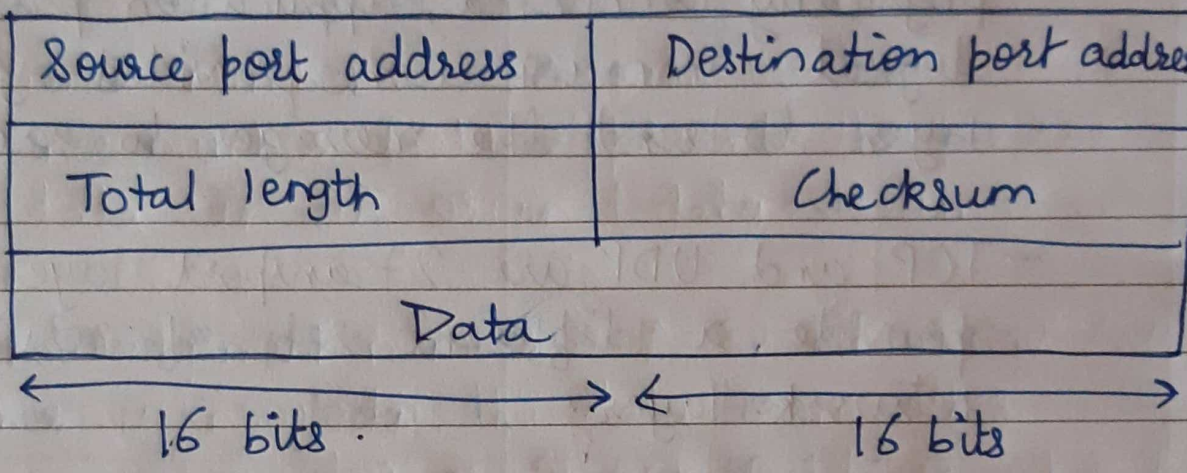
→ Protocols

i) UDP (User Datagram Protocol)
- UDP is a simple connectionless protocol and it provides non-sequenced transport functionality.

- UDP is used when reliability and security are less important than speed and size.

- UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.

- The packet produced the UDP protocol is known as a user datagram.



- Source port address: It defines the address of the application ~~layer~~ process that has delivered a message. (16 bit address)

- Destination port address: It defines the address of the application process that will receive the message. (16-bit address)

- Total length: It defines the total length of the user datagram in bytes. (16-bit field)

- Checksum: The checksum is a ~~bit~~ 16 bit-field which is used in error detection.

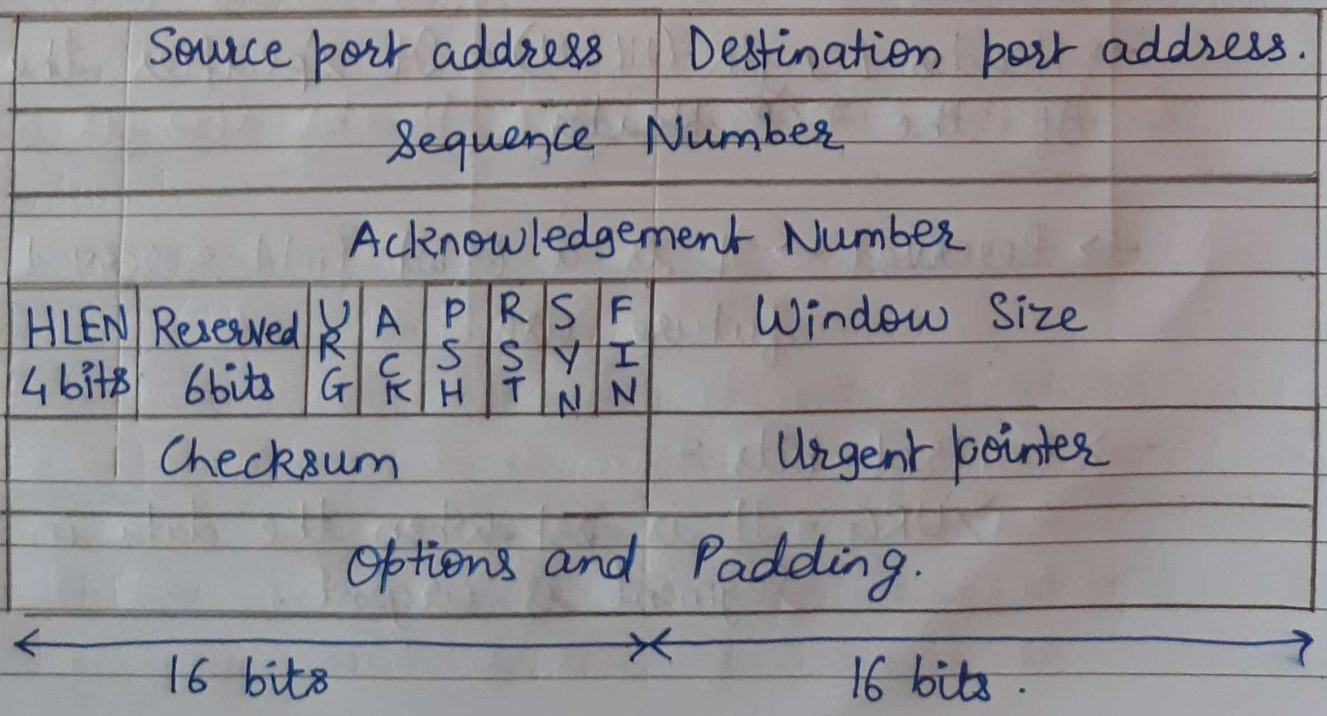
2) TCP (Transmission Control Protocol)

- It provides full transport layer services to applications.

- It is a connection-oriented protocol means the the connection established between ~~the~~ both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.

- Features of TCP → Stream data transfer, Reliability, Flow control, Multiplexing, Logical Connections, Full Duplex.

TCP Segment Format



→ Source port address :- It is used to define the address of the application program in a source computer. It is a 16-bit field.

→ Destination port address :- It is used to define the address of the application program in a destination computer. It is a 16-bit field.

→ Sequence number :- ~~A stream of data~~ The 32-bit sequence number field represents the position of the data in an original data stream.

→ Acknowledgement number :- A 32-bit acknowledgement number acknowledge the data from other communicating devices. If ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive.

→ Header Length (HLEN) - It specifies the size of the TCP Header.

→ Reserved → It is a 6-bit field reserved for future use.

→ Control bits :-

i) URG - It is set when the data in the Segment is urgent.

__/__/____

2> ACK - When this field is set, it validates the acknowledgment number.

3> PSH - The PSH field is used to inform the sender that higher throughput is needed so if possible, data must be pushed with higher throughput.

4> RST - The reset bit is used to reset the TCP connection when there is any confusion in the sequence numbers.

5> SYN - The SYN field is used to synchronize the sequence number in 3 types of segments: connection request, connection confirmation and confirmation acknowledgement.

6> FIN - The FIN field is used to inform the receiving TCP module that the sender has finished sending data.

→ Window Size - 16-bit field which defines the size of the window.

→ Checksum - 16-bit field used in error detection.

→ Urgent pointer - If URG flag is set to 1, then this 16-bit field is an offset from the sequence number indicating that is last urgent data byte.

→ Options and padding - It defines the optional fields that convey the additional information to the receiver.

TCP	UDP
TCP establishes a virtual circuit before transmitting the data	UDP transmits the data directly to the destination computer, without verifying whether the receiver is ready to receive or not.
Connection-Oriented Protocol.	Connectionless Protocol.
Speed is slow.	Speed is high.
Reliable protocol	Unreliable protocol.
Header size is 20 bytes	Header size is 8 bytes.

__/__/____

* APPLICATION LAYER.

- The application layer programs are based on clients and servers.

- Functions of the Application Layer are
  i. Identifying communication partners.
  ii. Determining resource availability.
  iii. Synchronizing communication.

→ Protocols

1) DNS - Domain Name System.

- It is a directory service that provides a mapping between the name of the host on the network and its numerical addresses.
- DNS is required for functioning of the internet.
- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
- DNS is a client/server network communication protocol. DNS clients send requests to the server while DNS servers send responses to the client.
- Client requests contain a name which is converted into an IP address known as a forward DNS lookups and the same is for reverse DNS lookups in opposite manner.

2) FTP - File Transfer Protocol

- It is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.

- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.

- It is also used for downloading the files to computer from other servers.

- It provides the sharing of files.

- It transfers the data more reliably and efficiently.

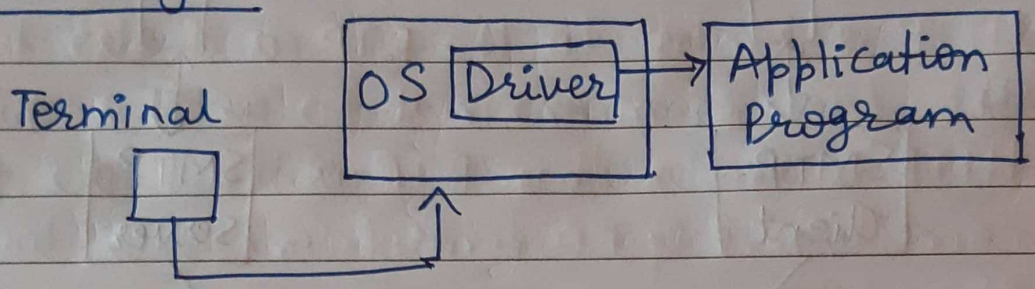
3) TELNET - Terminal Network

- TELNET is a client-server program that provides a user access any application program on a remote computer.
- It is a program that allows a user to log on a remote computer.
- It provides a connection to the remote computer in such a way that a local terminal appears to be at the

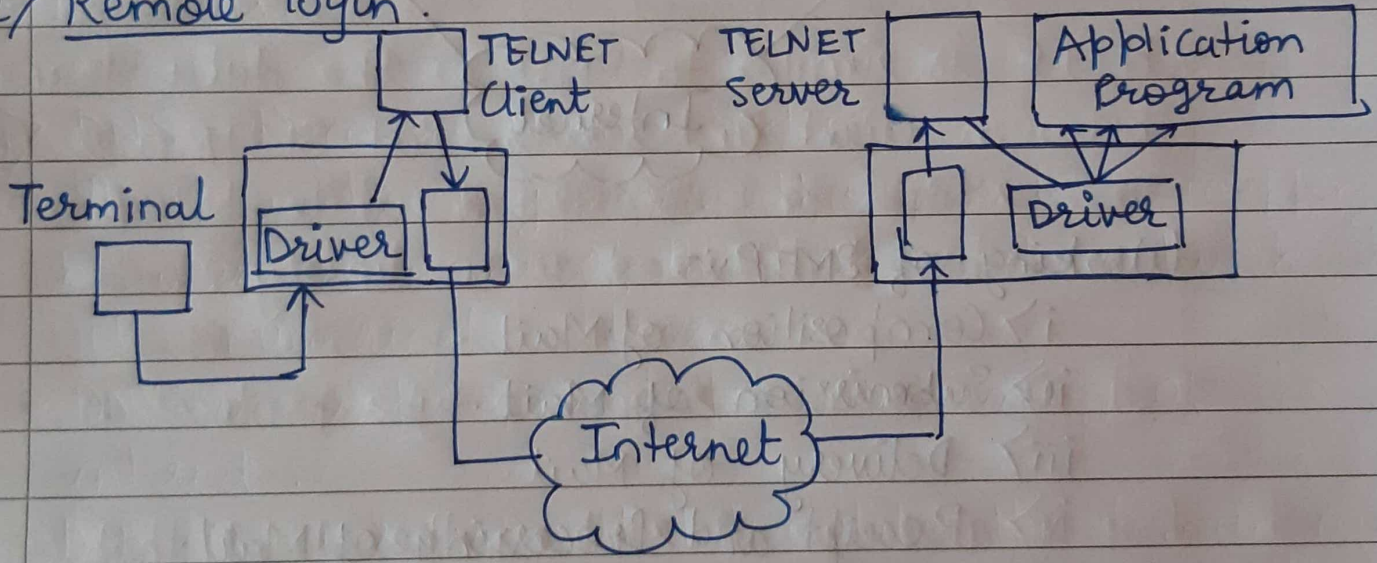
remote side.

There are two types of Login

1) Local login.



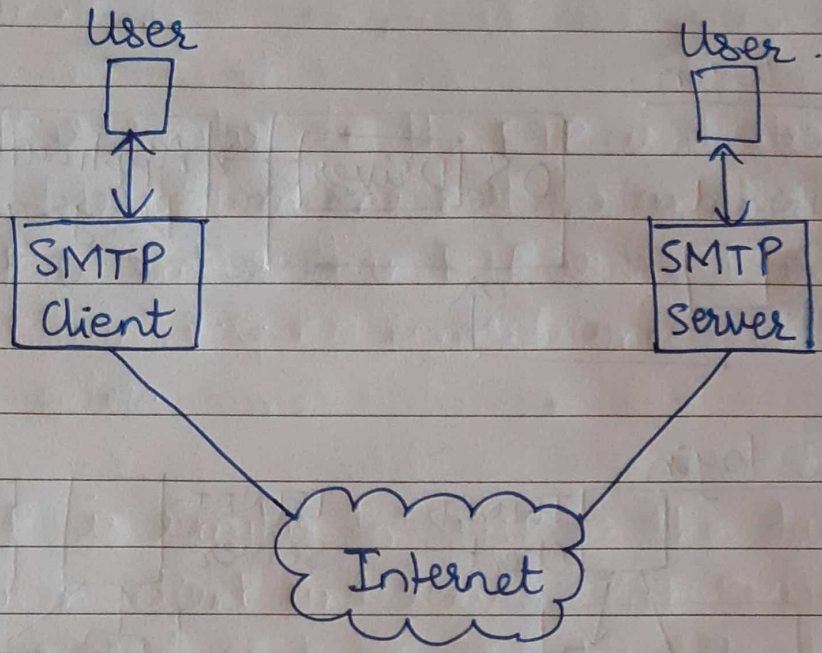
2) Remote login.



4) SMTP - Simple Mail Transfer Protocol

+ It is a set of communication guidelines that allow software to transmit an electronic mail over the internet. It is a service program used for sending messages to other computer users based on email addr.

- It can send a single message to one or more recipients ~~with~~ which can include text, voice, video or graphics.



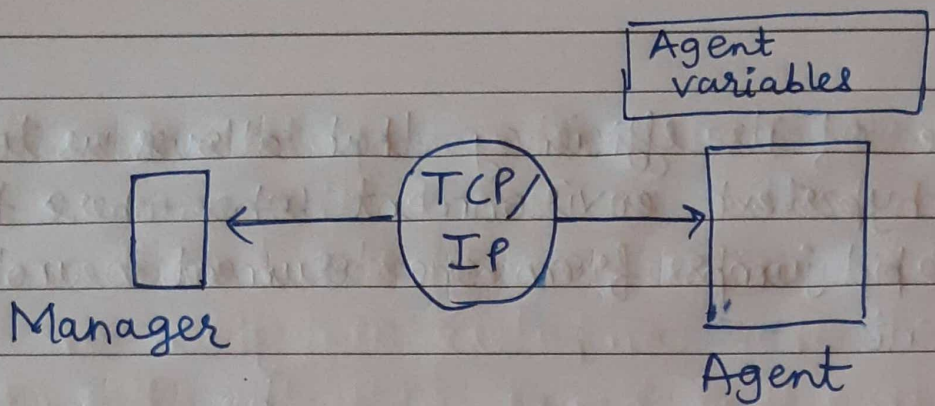
Working of SMTP :-

i) Composition of Mail.
ii) Submission of Mail.
iii) Delivery of Mail.
iv) Receipt and Processing of Mail.
v) Access and retrieval of Mail.

5) SNMP - Simple Network Management Protocol.

- It is a framework used for ~~mang~~ managing devices on the internet.
- It has two components: Managers and agents. Manager is a host that controls and monitors a set of agents such as routers.

__/__/____



- The protocol designed at the application level can monitor the devices made by different manufacturers and installed on different physical networks.

- Manager is a host that runs SNMP client Program while the agent is a router than runs SNMP Server Program.

- The agent is used to keep the information in a database while the manager is used to access the values in the database.

6) HTTP - Hyper Text Transfer Protocol.

- It is a protocol used to access the data on the World Wide Web (WWW)

- It can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.

- Connectionless, media-independent, stateless protocol.

- The protocol is known as Hyper Text Transfer Protocol.

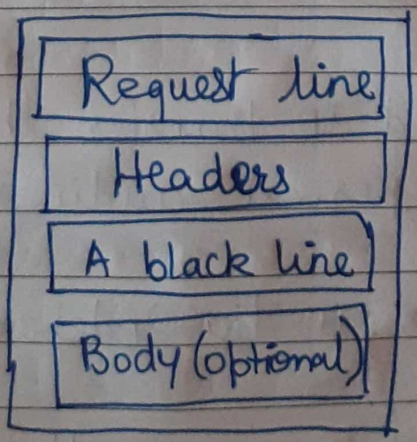
because of its efficiency that allows us to use in a hypertext environment ~~when~~ where there are rapid jumps from one document to another document.

- HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e. no control connection to transfer the files.

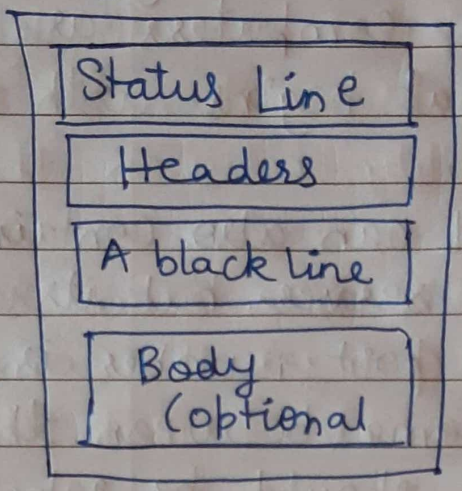
- HTTP is similar to SMTP as the data transferred between client and server. But SMTP messages are stored and forwarded while HTTP messages are ~~delwered~~ delivered immediately.

- It is a request response type protocol.

Request message is sent by the client that consists of a ~~re~~ request line, headers, and sometimes a body



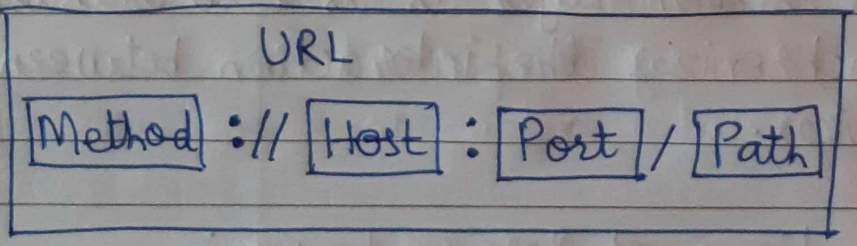
The response message is sent by the server to the client that consists of a status line, headers, and sometimes a body.



→ Uniform Resource Locator (URL)

- The client wants to access the documents in an internet needs an address and facilitate the access of documents, the HTTP uses the concept of Uniform Resource ~~Allocator~~ Locator.

- The URL is a standard way of specifying any kind of information on the internet.



Method : The method is the protocol used to retrieve the document from a server.

Host : The host is the computer where the information is stored. ~~the comman~~ Webpages are mainly stored in the computers and the computers are given an alias name that begins with the characters "www"

Port : The URL can also contain the port number of the server, but its an optional field. If the port number is included, then it must come between the host and path and it should be separated from the host by a colon.

Path : Path is the pathname of the file where the information is stored. The path itself contain slashes that separate the directories from the subdirectories and files.

* SESSION LAYER.

The session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session Layer :

a) Dialog control : Session layer acts as a dialog controller that creates a dialog between two processes

__/__/____

or we can say that it allows the communication between two processes which can be either half-duplex or full duplex.

b) Synchronization: Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This is ~~pra~~ called as Synchronization and recovery.

* PRESENTATION LAYER

- The Presentation Layer is mainly concerned with the syntax and the semantics of the information exchanged between the two systems.

- It acts as a data translator ~~of a~~ for a network.

- The layer is part of the operating system that converts the data from presentation format to another format.

- It is also known as syntax layer.

Functions of Presentation Layer

1) Translation
Different computers ~~used~~ use different encoding methods. The presentation layer handles the interoperability between the different encoding methods.
It converts the data from sender-dependent format and changes the common format into receiver-dependent format at the receiving end.

2) Encryption.
Encryption is the process of converting the sender-transmitted information into another form and sends the ~~maintain~~ resulting message over the network. It is needed to maintain privacy.

3) Compression.
Data compression is a process of compressing of data i.e. it reduces the numbers of bits to be transmitted.
It is very important in multimedia such as text, audio, video, etc.

__/__/____

* Miscellaneous

IPV4	IPV6.
It is a 32-bit address	It is a 128-bit address.
Numeric address with 4 fields seperated by dot (.)	Alphanumeric address with 8 fields separated by colon.
5 different classes (A to E)	Does not contain classes.
It generates 4 billion unique addresses.	It generates 340 undecillion unique addresses.
End-to-end connection integrity is unachievable	End-to-end connection integrity is achievable.
Checksum field available	Checksum field unavailable.
IpV4 is broadcasting	IpV6 is multicasting.
It does does not provide encryption and authentication	It provides encryption and authentication.
It consists of 4 octets	It consists of 16 octets.
Address is represented in decimal.	Address is represented is hexadecimal.

HTTP	HTTPS
Hyper Text Transfer Protocol.	Hyper Text Transfer Protocol Secure.
It is written in address bare as http://	It is written in address bar as https://
The HTTP transmits the data over port number 80.	The HTTPS transmits data over port number 443.
It is unsecured as plain text is sent	It is secured as encrypted data is sent.
It is an application layer protocol.	It is a transport layer protocol.
It does not use SSL	It provides SSL that uses encryption of data.
Page ~~lodin~~ loading is fast	Page loading is slow because of additional feature i.e. security.
Mainly used for websites like blog-writing	It is used for websites containg bank account details