MODULE 5 (NETWORKING)

A computer network is a set of devices connected through links. A node can be computer, printer, or any other device capable of sending or receiving the data. The links connecting the nodes are known as communication channels.

TOPIC 1:DATA COMMUNICATION

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.

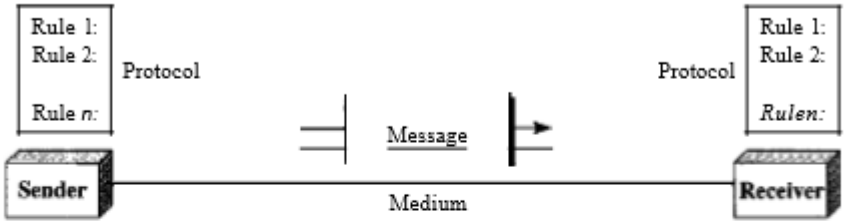
For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

- Delivery. The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
- Accuracy. The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
- Timeliness. The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind ofdelivery is called real-time transmission.
- Jitter. Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery ofaudio or video packets. For example, let us assume that video packets are sent every 3D ms. Ifsome ofthe packets arrive with 3D-ms delay and others with 4D-ms delay, an uneven quality in the video is the result.

TOPIC 2: COMPONENTS OF DATA COMMUNICATION

A data communications system has five components (see Figure 1.1).

Figure 1.1 *Five components of data communication*



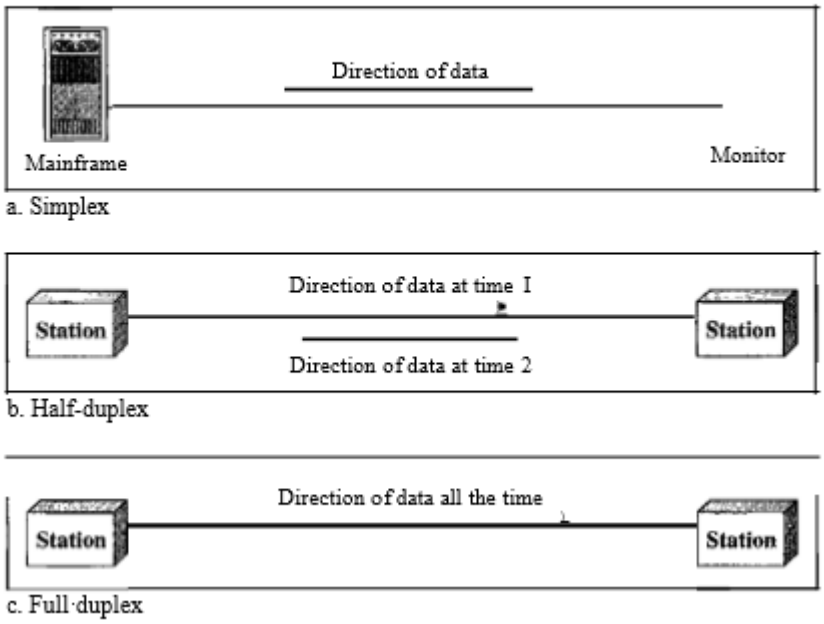
1. Message. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
2. Sender. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. Receiver. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
4. Transmission medium. The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

5. Protocol. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

TOPIC 3: Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplex as shown in Figure 1.2.

Figure 1.2 *Dataflow (simplex, half-duplex, andfull-duplex)*



- **Simplex**

In simplex mode, the communication is unidirectional, as on a one-way street. Only one ofthe two devices on a link can transmit; the other can only receive (see Figure 1.2a). Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity ofthe channel to send data in one direction.

- **Half-Duplex**

In half-duplex mode, each station can both transmit and receive, but not at the same time. : When one device is sending, the other can only receive, and vice versa (see Figure 1.2b).

The half-duplex mode is like a one-lane road with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) radios are both half-duplex systems.

- **Full-Duplex**

  In full-duplex (alsO called duplex), both stations can transmit and receive simultaneously (see Figure 1.2c). The full-duplex mode is like a tWo way street with traffic flowing in both directions at the same time.

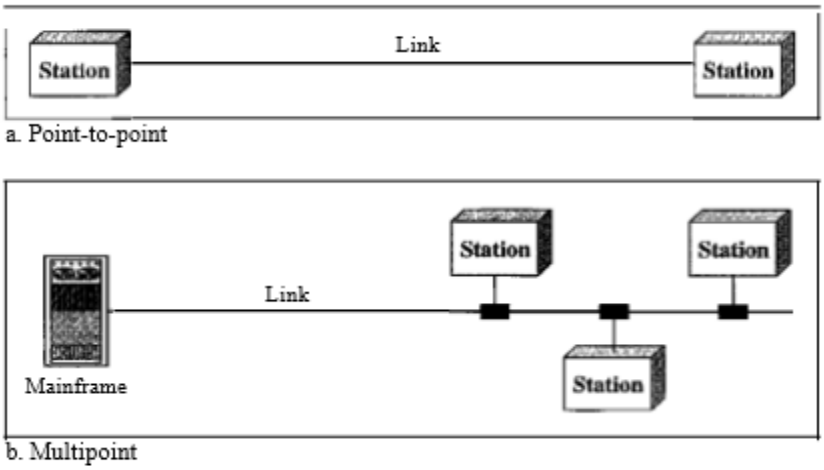
  One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time.

TOPIC 4: Type of Connection

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For visualization purposes, it is simplest to imagine any link as a line drawn between two points. For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections: point-to-point and multipoint.

- **Point-to-Point:** A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible (see Figure 1.3a). When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.
- **Multipoint:** A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link (see Figure 1.3b).

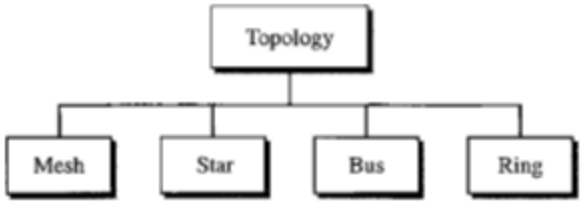
Figure 1.3 *Types of connections: point-to-point and multipoint*



TOPIC 5 : Physical Topology

The term physical topology refers to the way in which a network is laid out physically.: Two or more devices connect to a link; two or more links form a topology.

Figure 1.4 *Categories oftopology*

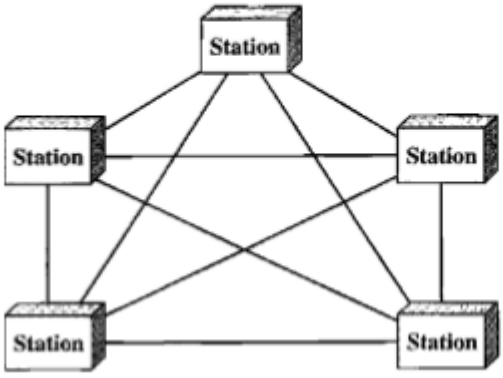


Mesh

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects.

A mesh offers several advantages over other network topologies. First, the use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices. Second, a mesh topology is robust. Ifone link becomes unusable, it does not incapacitate the entire system. Third, there is the advantage ofprivacy or security. When every message travels along a dedicated line, only the intended recipient sees it.

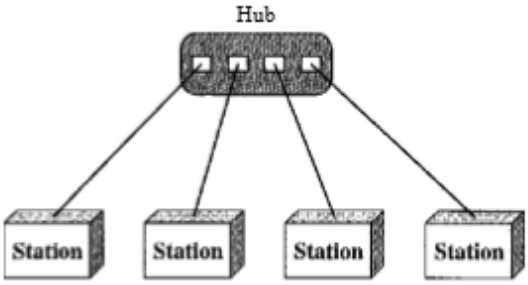
Figure 1.5 *A fully connected mesh topology (five devices)*



Star Topology

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: Ifone device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device (see Figure 1.6) . A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure. Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub. Other advantages include robustness. Ifone link fails, only that link is affected. All other links remain active.

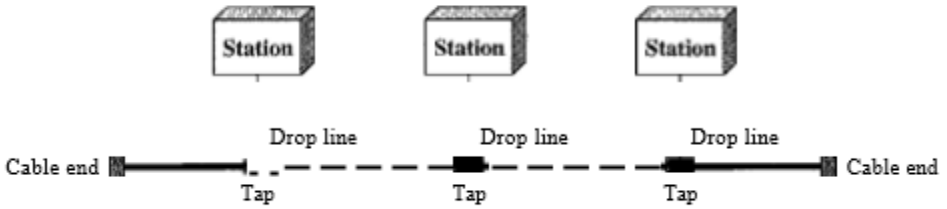
Figure 1.6 *A star topology connecting four stations*



Bus Topology

A bus topology, on the otherhand, is multipoint. One long cable acts as a backbone to link all the devices in a network (see Figure 1.7).

Figure 1.7 *A bus topology connecting three stations*

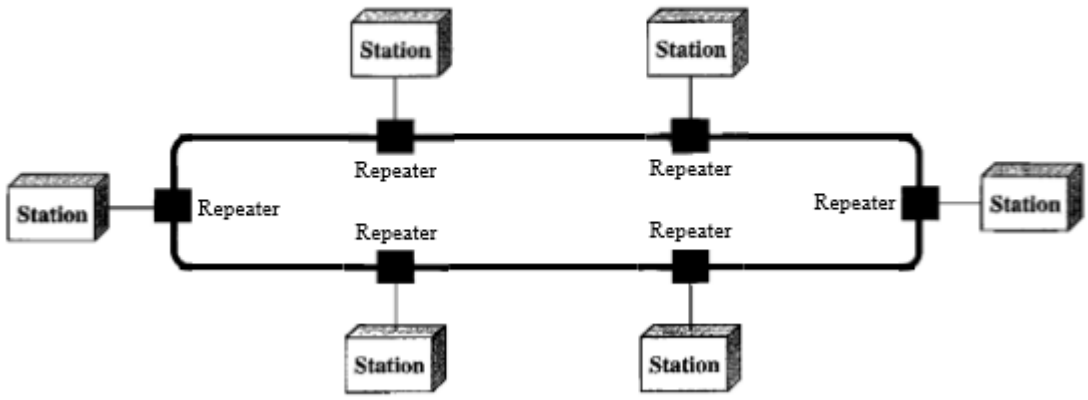


Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable.

Ring Topology

In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along (see Figure 1.8).

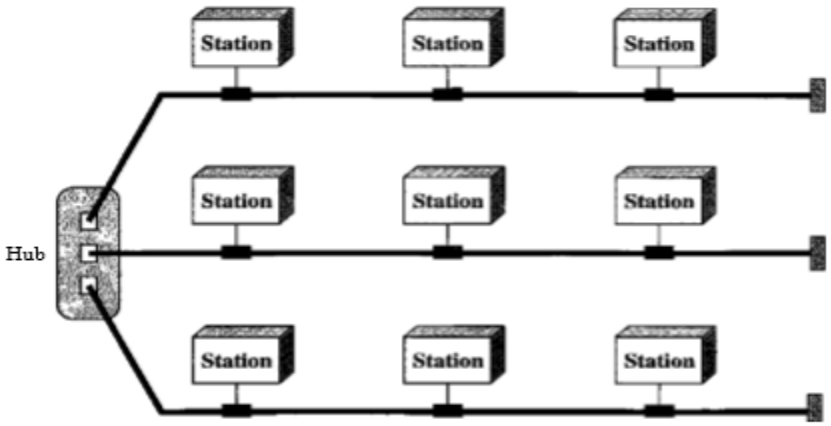
Figure 1.8 *A ring topology connecting six stations*



Hybrid Topology

A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown inFigure 1.9.

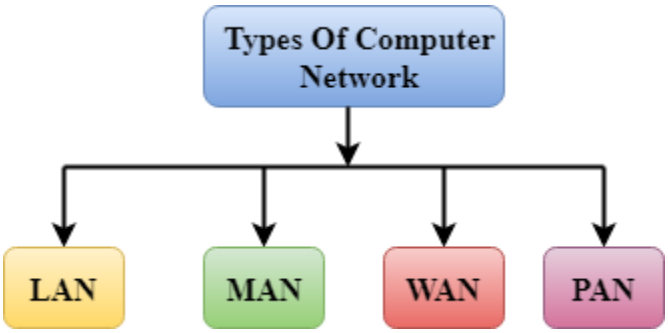
Figure 1.9 A *hybrid topology: a star backbone with three bus networks*



TOPIC 6: TYPES OF NETWORK

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

A computer network can be categorized by their size. A **computer network** is mainly of **four types**:



- LAN(Local Area Network)
- PAN(Personal Area Network)

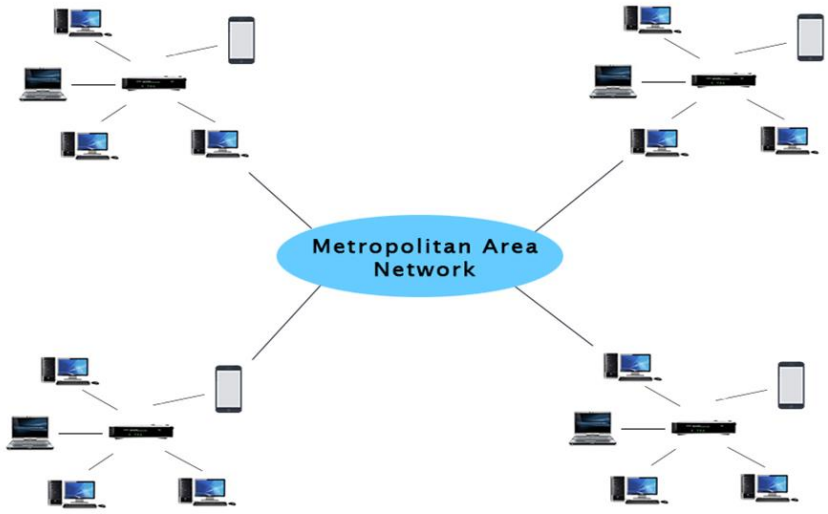
- MAN(Metropolitan Area Network)
- WAN(Wide Area Network)

LAN(Local Area Network)

- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.

MAN(Metropolitan Area Network)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- It has a higher range than Local Area Network(LAN).

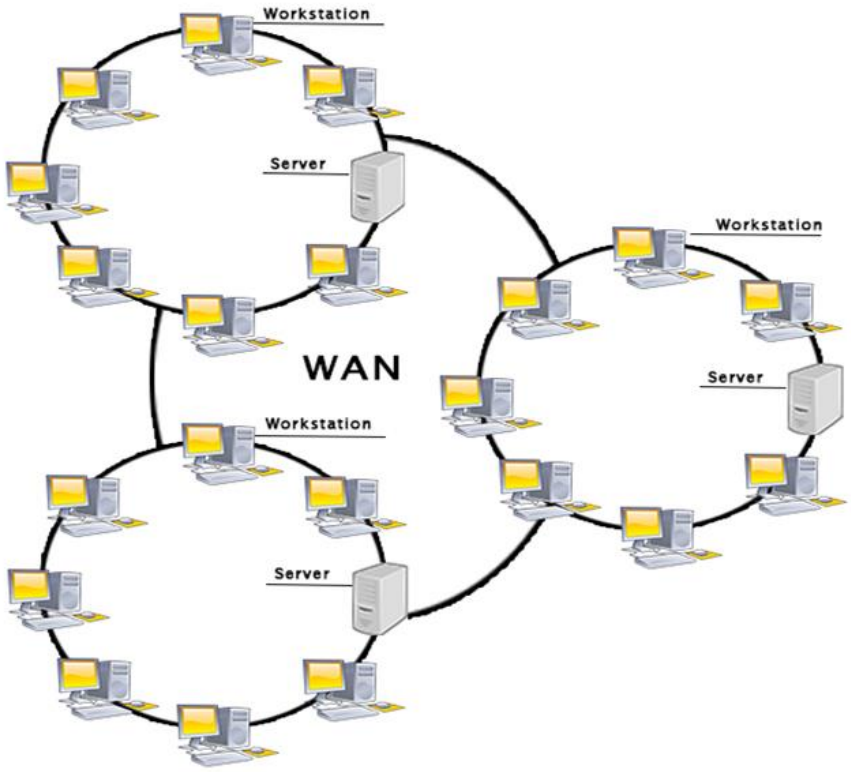


Uses Of Metropolitan Area Network:

- MAN is used in communication between the banks in a city.
- It can be used in an Airline Reservation.
- It can be used in a college within a city.
- It can also be used for communication in the military.

WAN(Wide Area Network)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.



Examples Of Wide Area Network:

- **Mobile Broadband:** A 4G network is widely used across a region or country.
- **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

INTERNET

The **Internet** (or **internet**)[a] is the global system of interconnected computer networks that uses the Internet protocol suite (TCP/IP) to communicate between networks and devices.

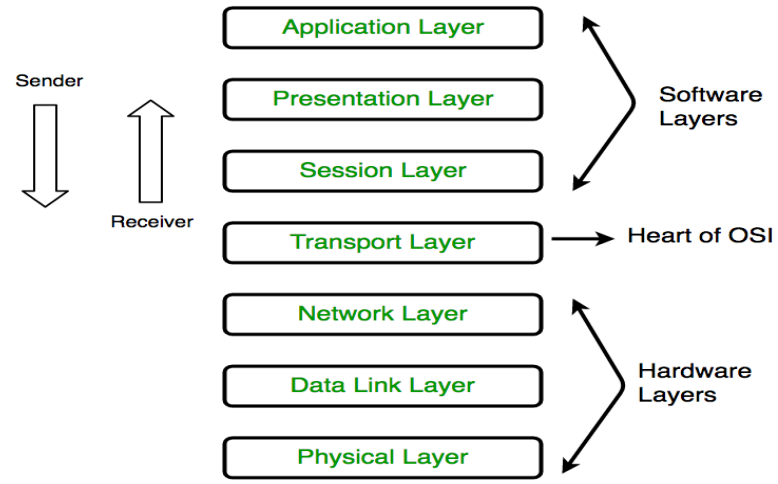
The basic distinction between network and net is that the **Network** consists of pcs that area unit physically connected and may be used as a private computer yet on share data with one another. Conversely, the **Internet** could be a technology that links these little and huge networks with one another and builds a additional in depth network.

PROTOCOLS AND STANDARDS

In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. A protocol is a set ofrules that govern data communications. A protocol defines what is communicated, how it is communicated, and when itis communicated.

OSI MODEL

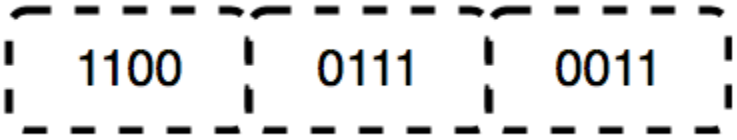
OSI stands for **Open Systems Interconnection**. It has been developed by ISO – '**International Organization of Standardization**', in the year 1984. It is a 7 layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.



1. Physical Layer (Layer 1) :

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.



The functions of the physical layer are :

1. **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 bit level.
2. **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
3. **Physical topologies:** Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.
4. **Transmission mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex.

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

2. Data Link Layer (DLL) (Layer 2) :

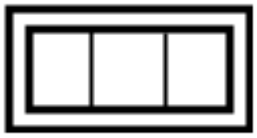
The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.
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 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.



The functions of the Data Link layer are :

1. **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.
2. **Physical addressing:** After creating frames, the Data link layer adds physical addresses (MAC address) of the sender and/or receiver in the header of each frame.
3. **Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
4. **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 acknowledgement.
5. **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.

** Packet in Data Link layer is referred to as **Frame**.*

*** Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.*

*** *Switch & Bridge are Data Link Layer devices.*

3. Network Layer (Layer 3) :

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.
The functions of the Network layer are :

1. **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
2. **Logical Addressing:** In order 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.

* *Segment* in Network layer is referred to as **Packet**.

** Network layer is implemented by networking devices such as routers.

4. Transport Layer (Layer 4) :

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 acknowledgement of the successful data transmission and re-transmits the data if an error is found.

• **At sender's side:**

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.

Note: The sender needs to know the port number associated with the receiver's application. Generally, this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default ports assigned.

- **At 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.

The functions of the transport layer are :

1. **Segmentation and Reassembly:** This layer accepts the message from the (session) layer, 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.
2. **Service Point Addressing:** In order to deliver the message to the correct process, the transport layer header includes a type of address called 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.

The services provided by the transport layer :

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 acknowledgement, 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.

** Data in the Transport Layer is called as **Segments**.*
*** Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.*
*Transport Layer is called as **Heart of OSI** model.*

5. Session Layer (Layer 5) :

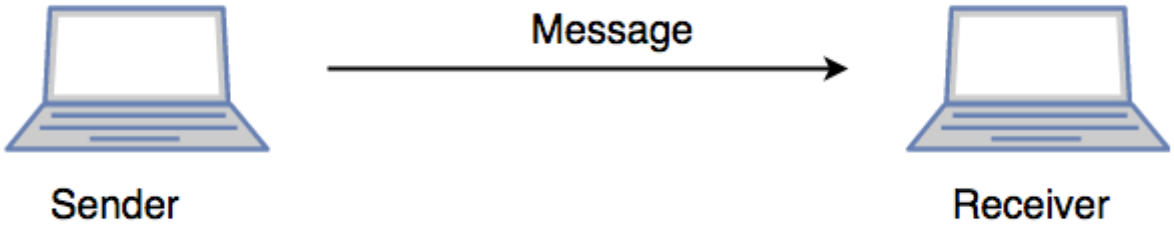
This layer is responsible for the establishment of connection, maintenance of sessions, authentication, and also ensures security.
The functions of the session layer are :

1. **Session establishment, maintenance, and termination:** The layer allows the two processes to establish, use and terminate a connection.
2. **Synchronization:** This layer allows a process to add checkpoints which are considered synchronization points into 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.
3. **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

***All the below 3 layers(including Session Layer) are integrated as a single layer in the TCP/IP model as "Application Layer".*
***Implementation of these 3 layers is done by the network application itself. These are also known as **Upper Layers** or **Software Layers**.*

SCENARIO:

Let's consider a scenario where a user wants to send a message through some Messenger application running in his browser. The "Messenger" here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data), and converted into bits (0's and 1's) so that it can be transmitted.



6. Presentation Layer (Layer 6) :

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. The functions of the presentation layer are :

1. **Translation:** For example, ASCII to EBCDIC.
2. **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
3. **Compression:** Reduces the number of bits that need to be transmitted on the network.

7. Application Layer (Layer 7) :

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. 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. Ex: Application – Browsers, Skype Messenger, etc. ***Application Layer is also called Desktop Layer.*

The functions of the Application layer are :

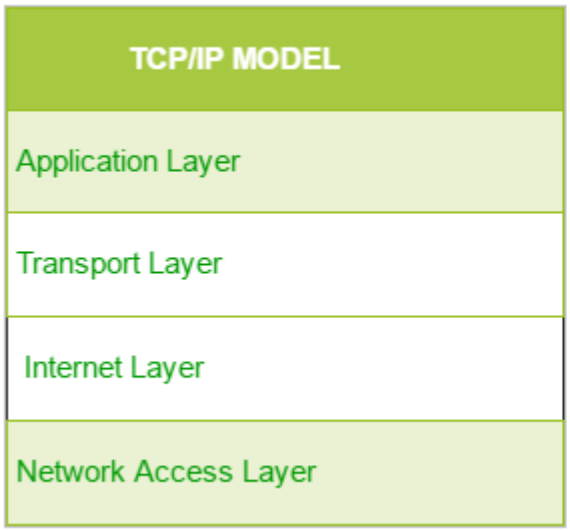
1. Network Virtual TerminalIU
2. FTAM-File transfer access and management
3. Mail Services
4. Directory Services

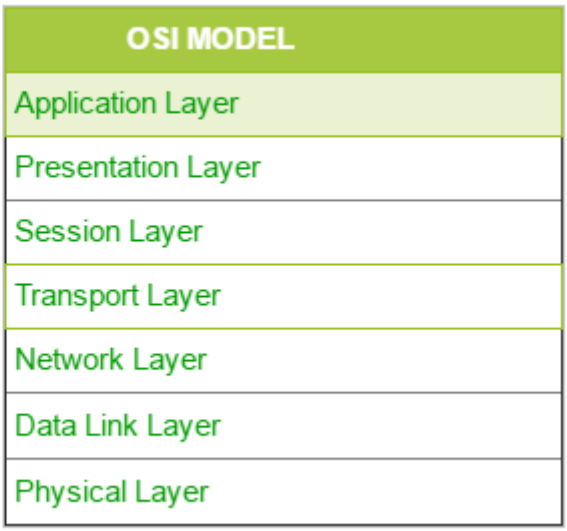
TCP/IP MODEL

The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

The diagrammatic comparison of the TCP/IP and OSI model is as follows :





Difference between TCP/IP and OSI Model:

TCP/IP	OSI

TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable	OSI is less reliable
TCP/IP does not have very strict boundaries.	OSI has strict boundaries
TCP/IP uses both session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.

The first layer is the Process layer on the behalf of the sender and Network Access layer on the behalf of the receiver. During this article, we will be talking on the behalf of the receiver.

1. Network Access Layer –

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.
We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

2. Internet Layer –

This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

1. **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 of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.

2. **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
3. **IGMP**

   The Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group ofrecipients
4. **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.
5. **RARP**

   The Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when itknows only its physical address. It is used when a computer is connected to a network for the first time orwhen a diskless computer is booted

3. Transport Layer –

This layer is analogous to the transport layer of the OSI model. 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 two main protocols present in this layer are :

1. **Transmission Control Protocol (TCP) –** It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
2. **User Datagram Protocol (UDP) –** On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.
3. **SCTP**

The Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet. It is a transport layer protocol that combines the best features of UDP and TCP.

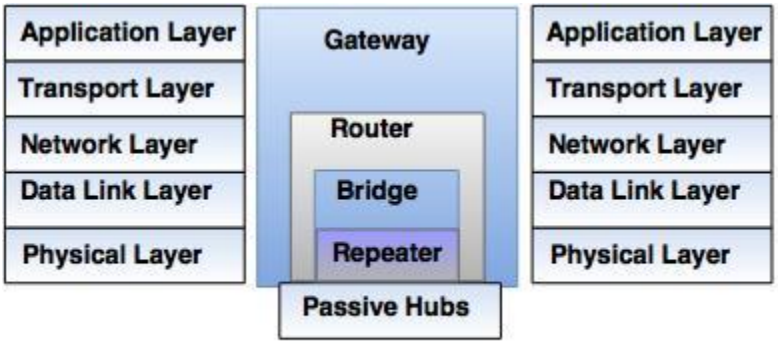
4. Application Layer –

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at Protocols in Application Layer for some information about these protocols. Protocols other than those present in the linked article are :

1. **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 need to fill out forms, sign in, authenticate and carry out bank transactions.

CONNECTING DEVICES

Connecting devices are divided into five different categories on the basis of layers in which they operate in the network.



Types of Connecting Devices

1. Devices which operate below the physical layer.

For example: Passive hub.

2. Devices which operate at the physical layer.

For example: Repeater.

3. Devices which operate at the physical and data link layers.

For example: Bridge.

4. Devices which operate at the physical layer, data link layer and network layer.

For example: Router.

5. Devices which operate at all five layers.

For example: Gateway.

LETS DISCUSS THEM IN DETAIL

1. **HUB**

   Hubs connect multiple computer networking devices together. hub is the simplest in the family of network connecting devices because it connects LAN components with identical protocols. Hubs do not perform packet filtering or addressing functions; they just send data packets to all connected devices. Hubs operate at the Physical layer of the Open Systems Interconnection (OSI) model.

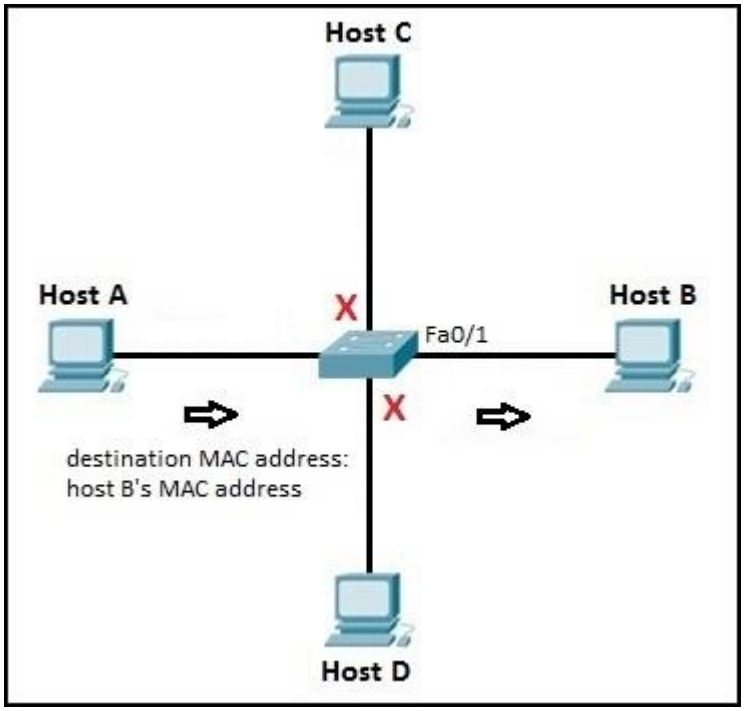
   Passive hub is just a connector which connects wire coming from other devices. **Active hub** is multi-point repeater with capability of regeneration of signals. **Active hub can process and monitor information while passive hub cannot** do this.

2. Repeater

A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.

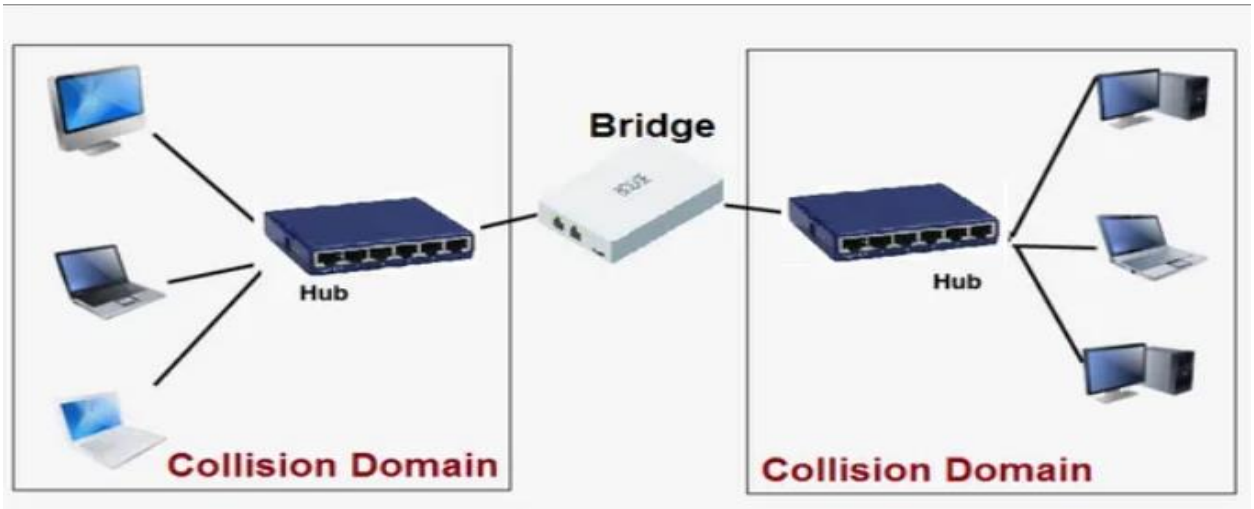
3. SWITCH

Switches generally have a more intelligent role than hubs. A switch is a multiport device that improves network efficiency. Generally, switches can read the hardware addresses of incoming packets to transmit them to the appropriate destination.



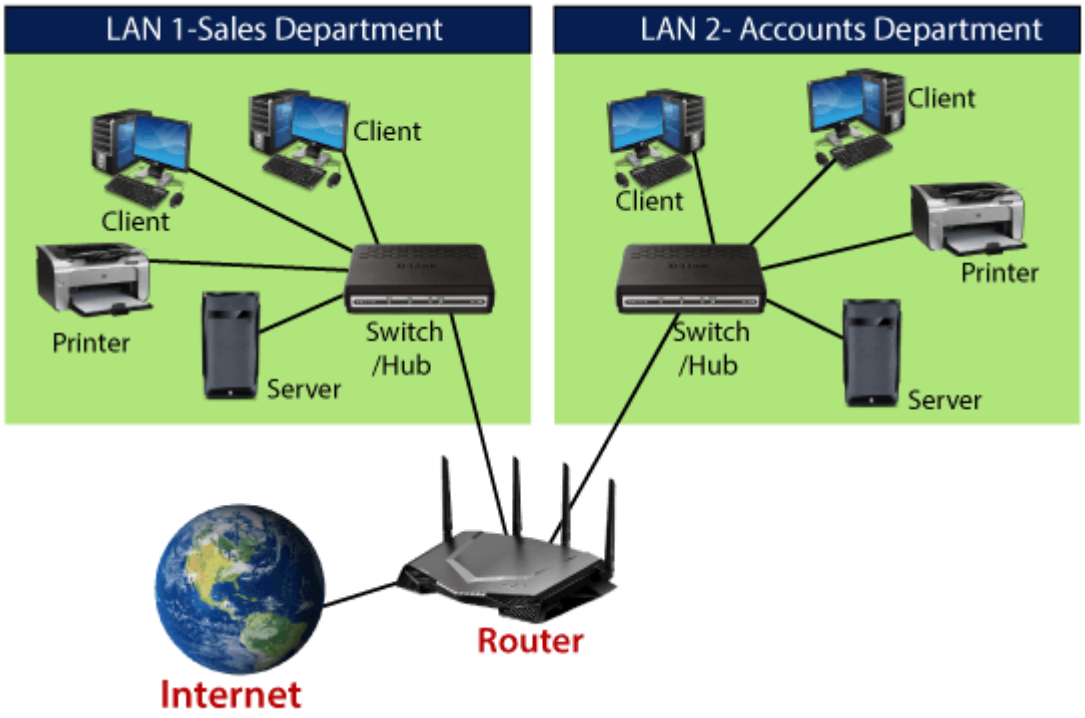
4. BRIDGES

A bridge is a computer **network hardware device** that works at the **data link layer of OSI model,** and it also helps to make interconnection in between multiple networks with using of same protocol.



5. Routers

   Routers are devices that join networks, as display in the figure. Routers are used in internetworking between LANs with different protocols. It is the simplest function that accepts packets from a connected network and passes them to another connected network. The router includes a mixture of hardware and software. The hardware can be a computer server, a disconnected computer. The hardware contains the physical link to several networks in the internetwork.



6. GATEWAY

A gateway is a network node that forms a passage between two networks operating with different transmission protocols.

- Gateway is located at the boundary of a network and manages all data that inflows or outflows from that network.
- It forms a passage between two different networks operating with different transmission protocols.
- A gateway operates as a protocol converter, providing compatibility between the different protocols used in the two different networks.
- The feature that differentiates a gateway from other network devices is that it can operate at any layer of the OSI model.

TOPIC : WEB BROWSER

A **web browser** (commonly referred to as a **browser**) is application software for accessing the World Wide Web. When a user requests a web page from a particular website, the web

browser retrieves the necessary content from a web server and then displays the page on the user's device.

A web browser is not the same thing as a search engine, though the two are often confused.[1][2] A search engine is a website that provides links to other websites. However, to connect to a website's server and display its web pages, a user must have a web browser installed.[3]

A web browser is a software program that allows a user to locate, access, and display web pages. In common usage, a web browser is usually shortened to "browser."

Web browsers are used primarily for displaying and accessing websites on the internet

SEARCH ENGINE

A **search engine** is software accessed on the Internet that searches a database of information according to the user's query. The engine provides a list of results that best match what the user is trying to find. Today, there are many different search engines available on the Internet, each with its own abilities and features. The first search engine ever developed is considered Archie, which was used to search for FTP files, and the first text-based search engine is considered Veronica. Currently, the most popular and well-known search engine is Google. Other popular search engines include AOL, Ask.com, Baidu, Bing, DuckDuckGo, and Yahoo.

WEB BROWSER VS SEARCH ENGINE

Search Engine: A search engine is a kind of website through which users can search the content available on the Internet. For this purpose, users enter the desired keywords into the search field. Then the search engine looks through its index for relevant web pages and displays them in the form of a list. The Internet is a huge source of information & resources and to access the resource from the Internet there are some kinds of software, this softwares are known as Search Engine. Some of the popular ones are: Google, Bing, Yahoo, Duck duck go, Baidu, etc.

There are three main components of the Search engine:

- Crawler: Crawlers are software programs sometimes referred to the bots. It regularly scans the websites automatically for URLs, keywords, and links in order to discover the new updates. The crawler can follow the links present on some other webpage.
- Index: As we know, the Crawler continuously scans the websites, it develops an index of URLs, links and keywords to make the search results more effective.
- Search Algorithm: The search algorithm is the complete mechanism behind the whole searching process. It is working by searching for the index and finding for the most suitable webpages by matching keywords that are searched by the users.

Web Browser: The web browser is an example of application software that is developed to retrieve and view the information from web pages or HTML files present on the web servers. The first web browser was invented by Sir Tim Berners-Lee in 1990 and the very first graphical web browser was developed in 1993 which is named the mosaic. After that, various web browsers were developed. Some of them are navigator which is developed by Netscape communication, Microsoft's internet explorer, Google Chrome, Mozilla Firefox, Opera and Apple safari.

The main characteristics of Web Browser are:

- It consists of Graphical User Interface.
- It contains the search box where the user can type the address or URL.
- Page style can be static or dynamic. It depends upon the interactivity and the formatting.
- TCP/IP and HTTP protocols are used by the web browsers.

TOPIC : SHARED SERVICES: FORMS, DOCS, SHEETS, MEET,DRIVE

Google Forms is a survey administration software included as part of the free, web-based Google Docs Editors suite offered by Google.

The app allows users to create and edit surveys online while collaborating with other users in real-time. The collected information can be automatically entered into a spreadsheet.[1]

Google Forms lets you collect information from people via personalized quizzes or surveys. You can then connect the info to a spreadsheet on Sheets to automatically record the answers. The spreadsheet then populates with the responses from the quiz or survey in real-time. This makes Google Forms one of the easiest ways to save data directly into a spreadsheet.

With Forms, you can collect RSVPs, start surveys, or create quizzes for students with a simple online form. You can share your form via email, a direct link, or on social media and ask everyone to participate.

DOCS

Google Docs is an online word processor included as part of the free, web-based Google Docs Editors suite offered by Google, which also includes Google Sheets, Google Slides, Google Drawings, Google Forms, Google Sites, and Google Keep. Google Docs is accessible via an internet browser as a web-based application and is also available as a mobile app on Android and iOS and as a desktop application on Google's Chrome OS.

Google Docs allows users to create and edit documents online while collaborating with other users in real-time. Edits are tracked by user with a revision history presenting changes. An editor's position is highlighted with an editor-specific color and cursor and a permissions system regulates what users can do.

SHEET

Google Sheets is a spreadsheet program included as part of the free, web-based Google Docs Editors suite offered by Google. The app allows users to create and edit files online while collaborating with other users in real-time. Edits are tracked by user with a revision history presenting changes. An editor's position is highlighted with an editor-specific color and cursor and a permissions system regulates what users can do.

MEET

Google Meet is a video-communication service developed by Google.

DRIVE

Google Drive is a file storage and synchronization service developed by Google. Launched on April 24, 2012, Google Drive allows users to store files in the cloud, synchronize files across devices, and share files.

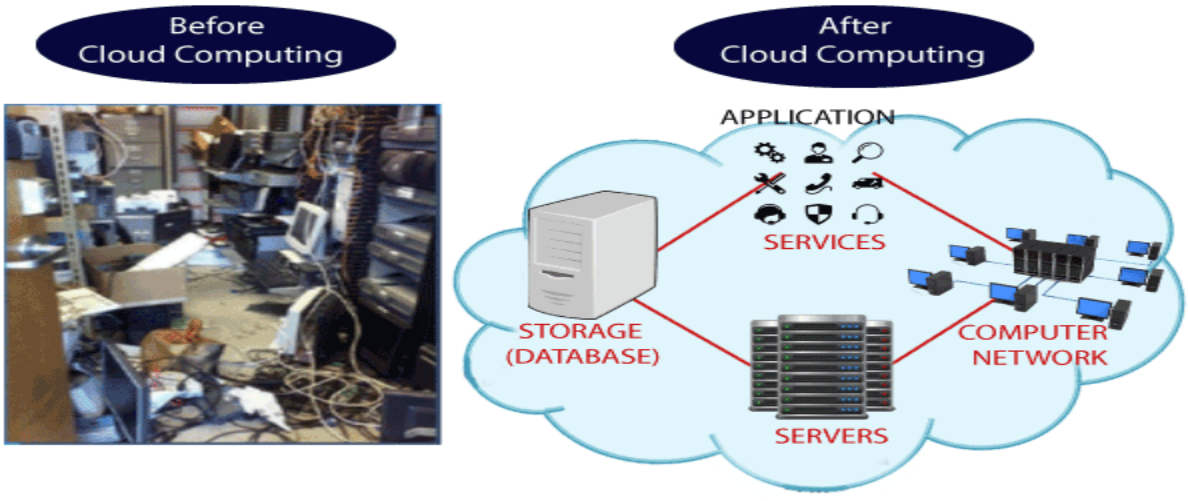
CLOUD COMPUTING

Cloud computing is a virtualization-based technology that allows us to create, configure, and customize applications via an internet connection. The cloud technology includes a development platform, hard disk, software application, and database.

It is a technology that uses remote servers on the internet to store, manage, and access data online rather than local drives. The data can be anything such as files, images, documents, audio, video, and more.

There are the following operations that we can do using cloud computing:

- Developing new applications and services
- Storage, back up, and recovery of data
- Hosting blogs and websites
- Delivery of software on demand
- Analysis of data
- Streaming videos and audios



Characteristics of Cloud Computing

The characteristics of cloud computing are given below:

1) Agility

The cloud **works in a distributed computing environment**. It shares resources among users and works very fast.

2) High availability and reliability

The availability of servers is high and more reliable because the **chances of infrastructure failure are minimum**.

3) High Scalability

Cloud offers **"on-demand" provisioning of resources on a large scale**, without having engineers for peak loads.

4) Multi-Sharing

With the help of cloud computing, **multiple users and applications can work more efficiently** with cost reductions by sharing common infrastructure.

5) Device and Location Independence

Cloud computing enables the users to access systems using a web browser regardless of their location or what device they use e.g. PC, mobile phone, etc. **As infrastructure is off-site** (typically provided by a third-party) **and accessed via the Internet, users can connect from anywhere**.

6) Maintenance

Maintenance of cloud computing applications is easier, since they **do not need to be installed on each user's computer and can be accessed from different places**. So, it reduces the cost also.

7) Low Cost

By using cloud computing, the cost will be reduced because to take the services of cloud computing, **IT company need not to set its own infrastructure** and pay-as-per usage of resources.

8) Services in the pay-per-use mode

Application Programming Interfaces **(APIs) are provided to the users so that they can access services on the cloud** by using these APIs **and pay the charges as per the usage of services**.

Types of Cloud

There are the following 4 types of cloud that you can deploy according to the organization's needs

- Public Cloud

  Private Cloud

  Hybrid Cloud

  Community Cloud

Public Cloud

Public cloud is **open to all** to store and access information via the Internet using the pay-per-usage method.

In public cloud, computing resources are managed and operated by the Cloud Service Provider (CSP).

Example: Amazon elastic compute cloud (EC2), IBM SmartCloud Enterprise, Microsoft, Google App Engine, Windows Azure Services Platform.

Private Cloud

Private cloud is also known as an **internal cloud** or **corporate cloud**. It is used by organizations to build and manage their own data centers internally or by the third party.

Hybrid Cloud

Hybrid Cloud is a combination of the public cloud and the private cloud. we can say:

Hybrid Cloud* = *Public Cloud* + *Private Cloud

Hybrid cloud is partially secure because the services which are running on the public cloud can be accessed by anyone, while the services which are running on a private cloud can be accessed only by the organization's users.

Example: Google Application Suite (Gmail, Google Apps, and Google Drive), Office 365 (MS Office on the Web and One Drive), Amazon Web Services.

Community Cloud

Community cloud allows systems and services to be accessible by a group of several organizations to share the information between the organization and a specific community. It is owned, managed, and operated by one or more organizations in the community, a third party, or a combination of them.