

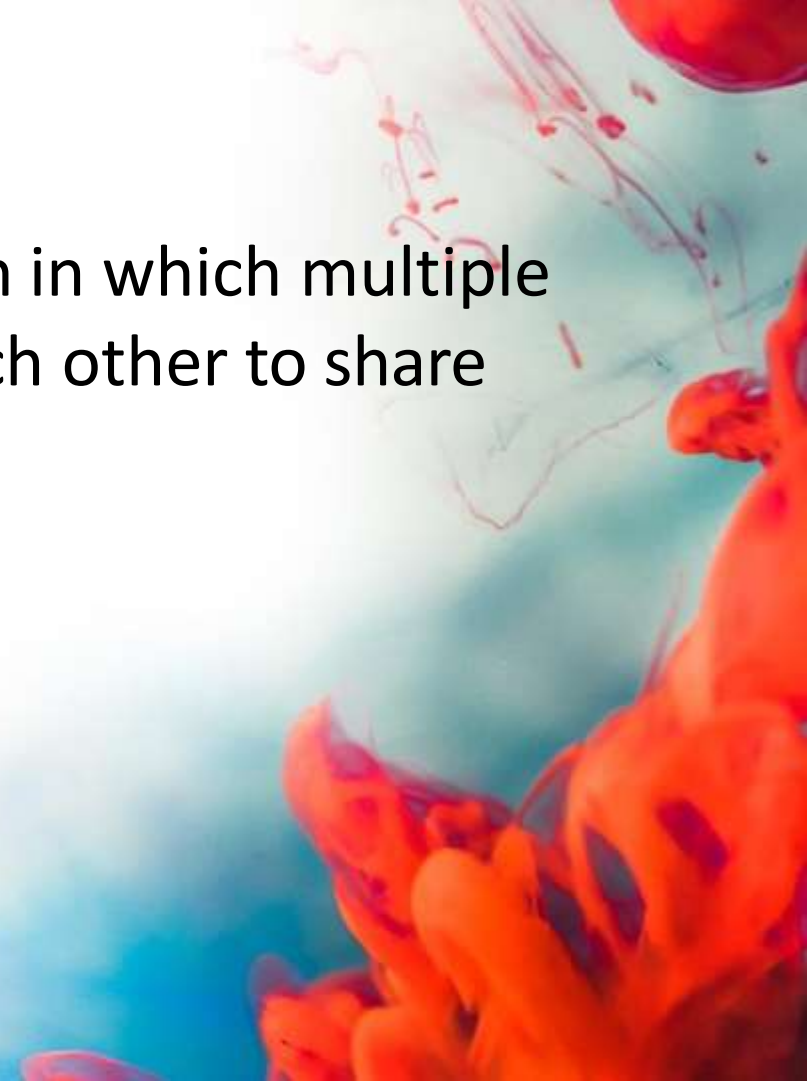


IWPD(Internet and Webpage Design)

By Atul Bhatt

Network

- A **computer network** is a system in which multiple computers are connected to each other to share information and resources.



Characteristics of a Computer Network

- Share resources from one computer to another.
- Create files and store them in one computer, access those files from the other computer(s) connected over the network.
- Connect a printer, scanner, or a fax machine to one computer within the network and let other computers of the network use the machines available over the network.

Internet

- It is a worldwide/global system of interconnected computer networks. It uses the standard Internet Protocol (TCP/IP). Every computer in Internet is identified by a unique IP address. IP Address is a unique set of numbers (such as 110.22.33.114) which identifies a computer's location.

Intranet

- Intranet is the system in which multiple PCs are connected to each other. PCs in intranet are not available to the world outside the intranet. Usually each organization has its own Intranet network and members/employees of that organization can access the computers in their intranet.

Differences between Internet and Intranet

- Internet is general to PCs all over the world whereas Intranet is specific to few PCs.
- Internet provides a wider and better access to websites to a large population, whereas Intranet is restricted.
- Internet is not as safe as Intranet. Intranet can be safely privatized as per the need.

Features Of Computer network

A list Of Computer network features is given below.

- Communication speed
- File sharing
- Back up and Roll back is easy
- Software and Hardware sharing
- Security

Communication speed

Network provides us to communicate over the network in a fast and efficient manner. For example, we can do video conferencing, email messaging, etc. over the internet. Therefore, the computer network is a great way to share our knowledge and ideas.

File sharing

File sharing is one of the major advantage of the computer network. Computer network provides us to share the files with each other.

Back up and Roll back is easy

Since the files are stored in the main server which is centrally located. Therefore, it is easy to take the back up from the main server.

Software and Hardware sharing

We can install the applications on the main server, therefore, the user can access the applications centrally. So, we do not need to install the software on every machine. Similarly, hardware can also be shared.

Security

Network allows the security by ensuring that the user has the right to access the certain files and applications.

ARPANET

- **Advanced Research Projects Agency Network, ARPANET or ARPAnet** began development in 1966 by the United States ARPA. ARPANET was a Wide Area Network linking many Universities and research centers, was first to use packet switching, and was the beginning of what we consider the Internet today. ARPANET was created to make it easier for people to access computers, improve computer equipment, and to have a more effective communication method for the military.

World Wide Web (WWW)

- The World Wide Web (WWW) is a network of online content that is formatted in HTML and accessed via HTTP. The term refers to all the interlinked HTML pages that can be accessed over the Internet. The World Wide Web was originally designed in 1991 by Tim Berners-Lee.

Netiquette

- Netiquette is short for "Internet etiquette." Just like etiquette is a code of polite behavior in society, netiquette is a code of **good behavior on the Internet**. This includes several aspects of the Internet, such as email, social media, online chat, web forums, website comments, multiplayer gaming, and other types of online communication.

- Avoid posting inflammatory or offensive comments online [flaming](#).
- Respect others' privacy by not sharing personal information, photos, or videos that another person may not want published online.
- Never [spam](#) others by sending large amounts of unsolicited email.
- Show good sportsmanship when playing online games, whether you win or lose.
- Don't [troll](#) people in web forums or website comments by repeatedly nagging or annoying them.
- Stick to the topic when posting in online forums or when commenting on photos or videos, such as [YouTube](#) or [Facebook](#) comments.
- Don't swear or use offensive language.
- Avoid replying to negative comments with more negative comments. Instead, break the cycle with a positive post.
- If someone asks a question and you know the answer, offer to help.
- Thank others who help you online.

5 Positive Effects of the Internet

- 1. It is easier to do research**
- 2. Communication with family, friends and relatives is faster**
- 3. There is a great possibility to earn while working from home**
- 4. Faster business transactions and cheaper products**
- 5. Savings on travel cost**

Packet Switching

- Packet switching is a digital network transmission process in which data is broken into suitably-sized pieces or blocks for fast and efficient transfer via different network devices. **When a computer attempts to send a file to another computer, the file is broken into packets so that it can be sent across the network in the most efficient way.** These packets are then routed by network devices to the destination.



• In connectionless packet switching, each packet has the following information written in its **header** section:

- The destination address
- The source address
- Total number of pieces
- The sequence number (Seq#) needed to enable reassembly

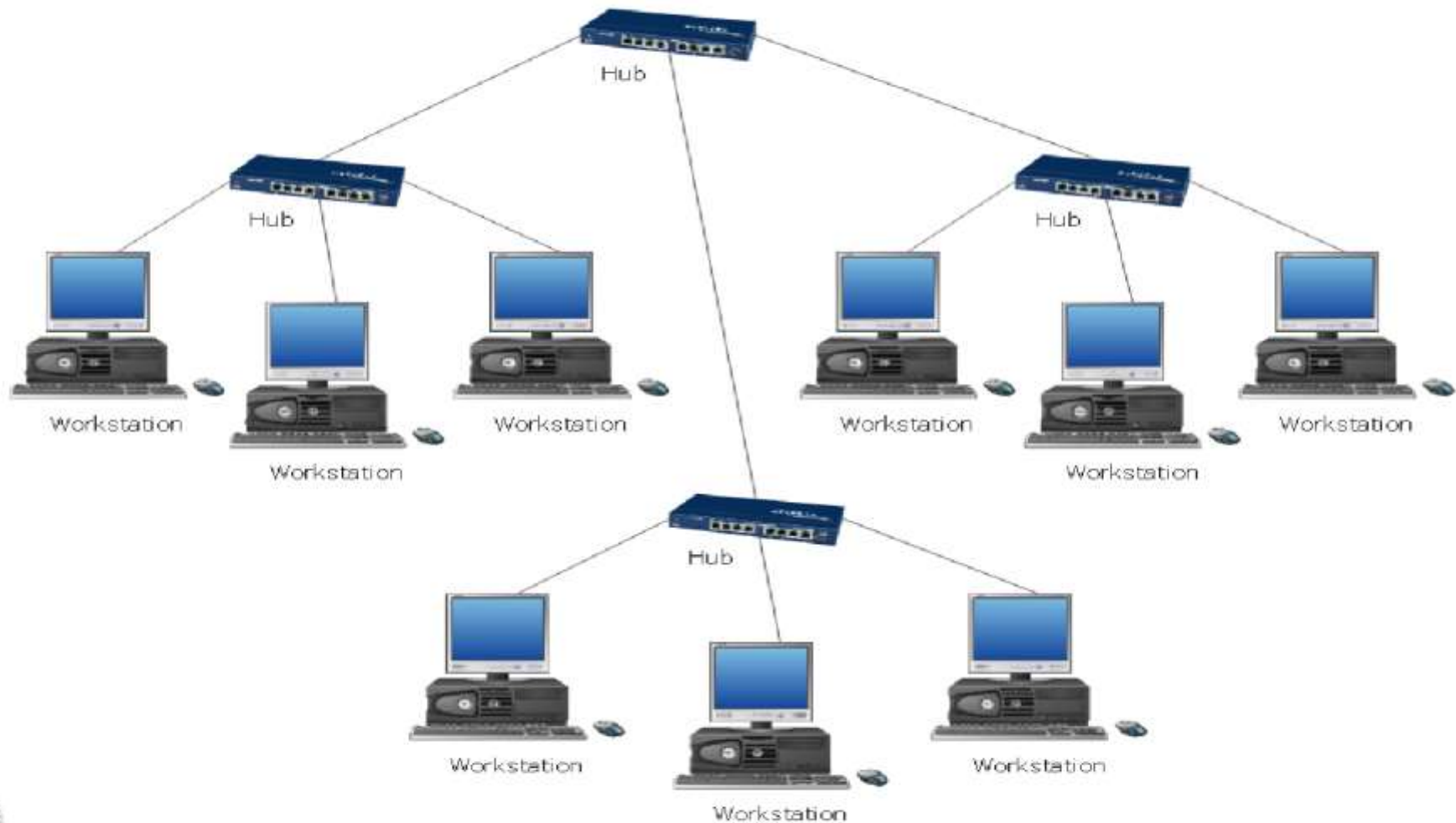
After reaching the destination through different routes, the packets are rearranged to form the original message.

Internet Protocol (IP)

- Internet Protocol (IP) is the principal set (or communications protocol) of digital message formats and rules for exchanging messages between computers across a single network or a series of interconnected networks, using the Internet Protocol Suite (often referred to as TCP/IP). Messages are exchanged as datagrams, also known as data packets or just packets.

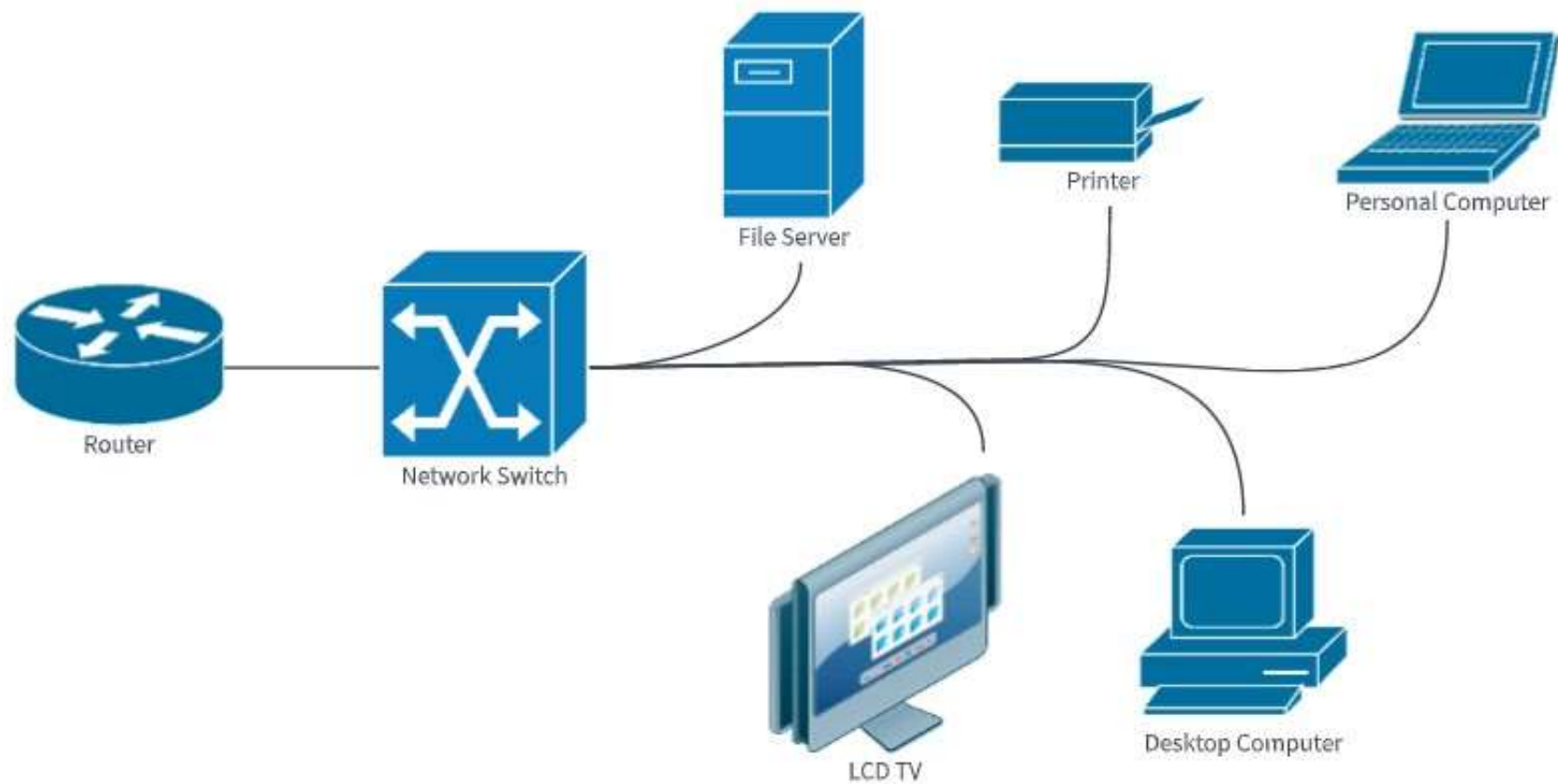
Hub

- A Hub is a hardware device that divides the network connection among multiple devices. When computer requests for some information from a network, it first sends the request to the Hub through cable. Hub will broadcast this request to the entire network. All the devices will check whether the request belongs to them or not. If not, the request will be dropped.
- The process used by the Hub consumes more bandwidth and limits the amount of communication. Nowadays, the use of hub is obsolete, and it is replaced by more advanced computer network components such as Switches, Routers.



Switch

- A switch is a hardware device that connects multiple devices on a computer network. A Switch contains more advanced features than Hub. The Switch contains the updated table that decides where the data is transmitted or not. Switch delivers the message to the correct destination based on the physical address present in the incoming message. (**manageable switch**)
- A Switch does not broadcast the message to the entire network like the Hub. It determines the device to whom the message is to be transmitted. Therefore, we can say that switch provides a direct connection between the source and destination. It increases the speed of the network.





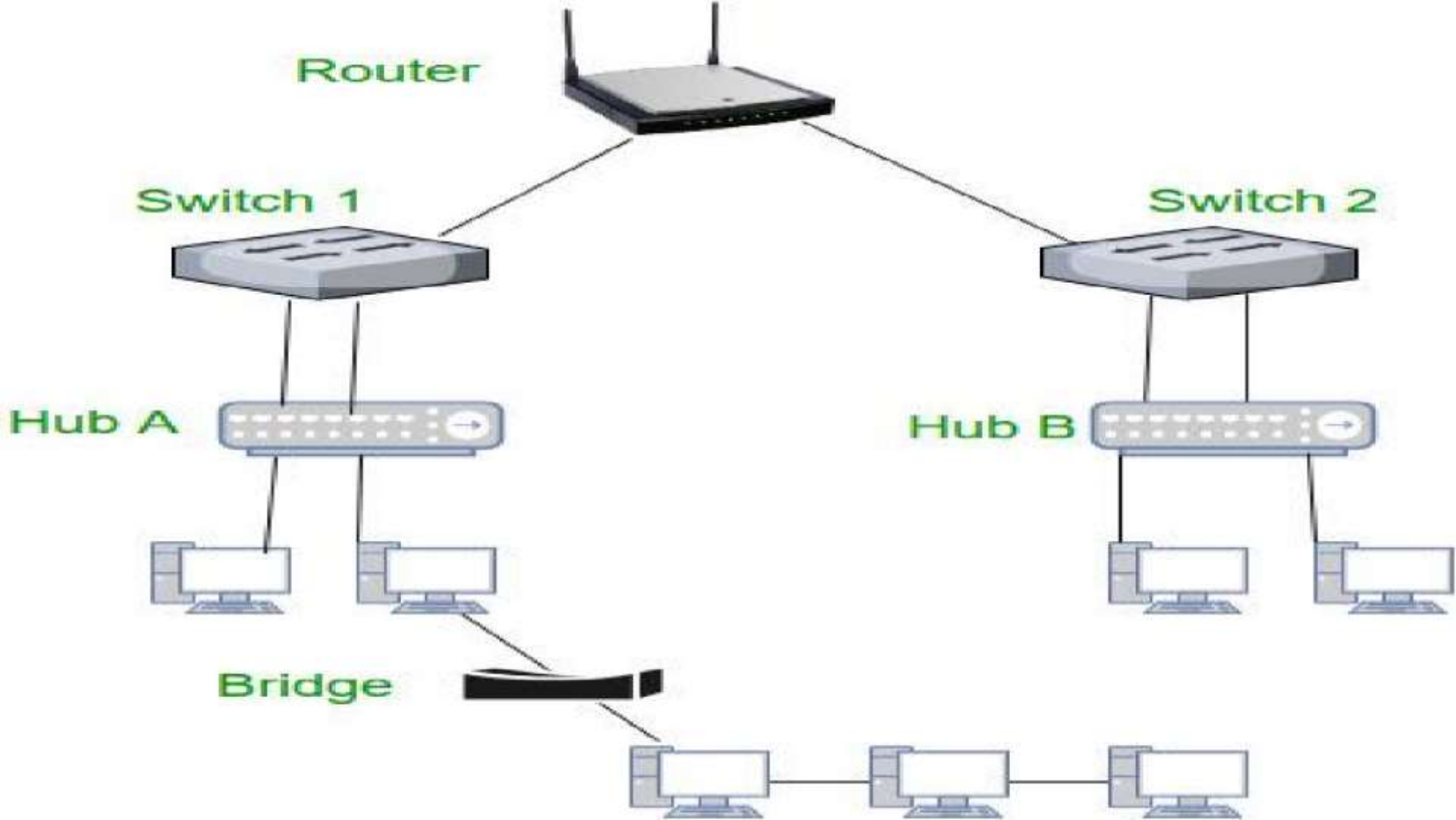
Modem



Desktop

Router

- A router is a hardware device which is used to connect a LAN with an internet connection. It is used to receive, analyze and forward the incoming packets to another network.
- A router works in a **Layer 3 (Network layer)** of the OSI Reference model.
- A router forwards the packet based on the information available in the routing table.
- It determines the best path from the available paths for the transmission of the packet.



What is HTML?

- HTML is the standard markup language for creating Web pages.
- HTML stands for Hyper Text Markup Language
- HTML describes the structure of a Web page
- HTML consists of a series of elements
- HTML elements tell the browser how to display the content
- HTML elements are represented by tags
- HTML tags label pieces of content such as "heading", "paragraph", "table", and so on
- Browsers do not display the HTML tags, but use them to render the content of the page

Modem

- A modem is a hardware device that allows the computer to connect to the internet over the existing telephone line.
- A modem is not integrated with the motherboard rather than it is installed on the PCI slot found on the motherboard.
- It stands for Modulator/Demodulator. It converts the digital data into an analog signal over the telephone lines.

Computer Network Types

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.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.

LAN(Local Area Network)



PAN(Personal Area Network)

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- Personal Area Network covers an area of **30 feet**.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

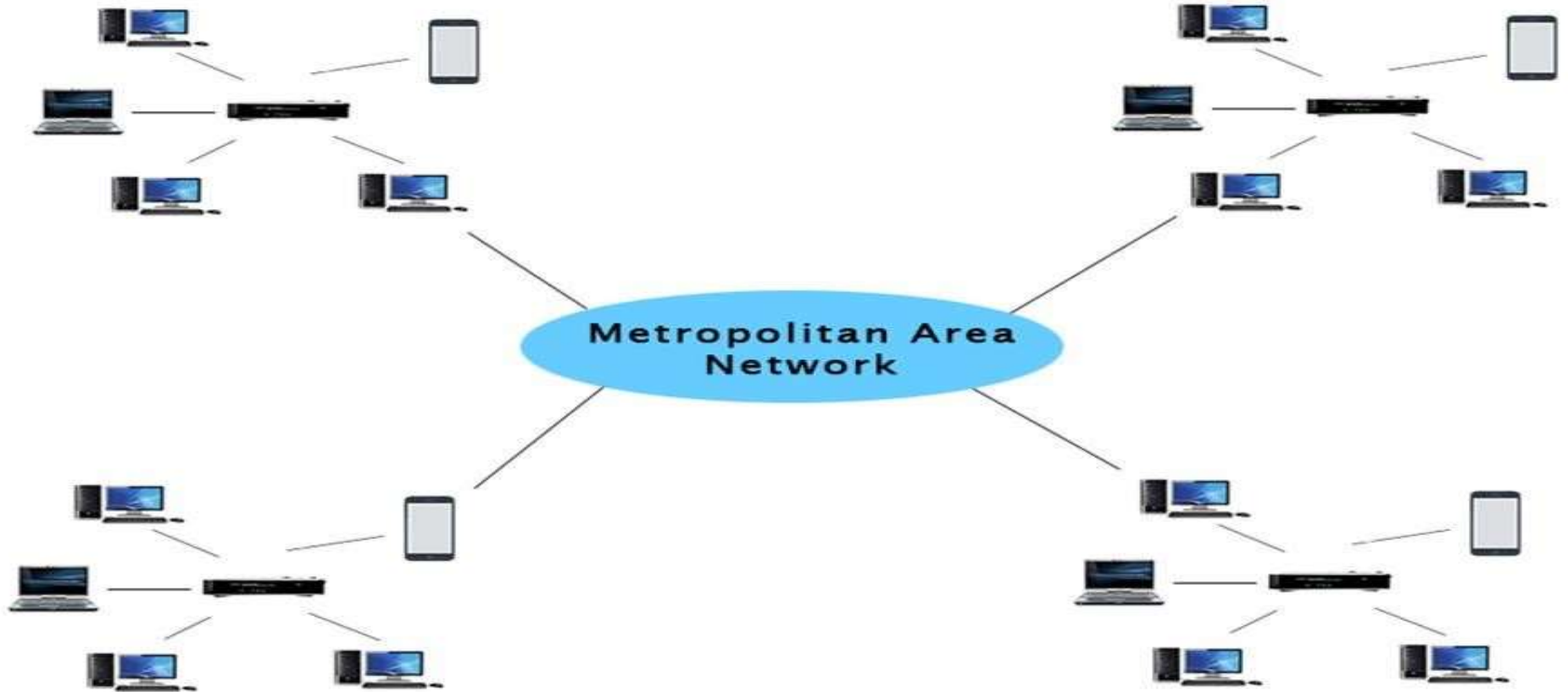
PAN(Personal Area Network)



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).**

MAN(Metropolitan Area Network



Uses Of Metropolitan Area Network:

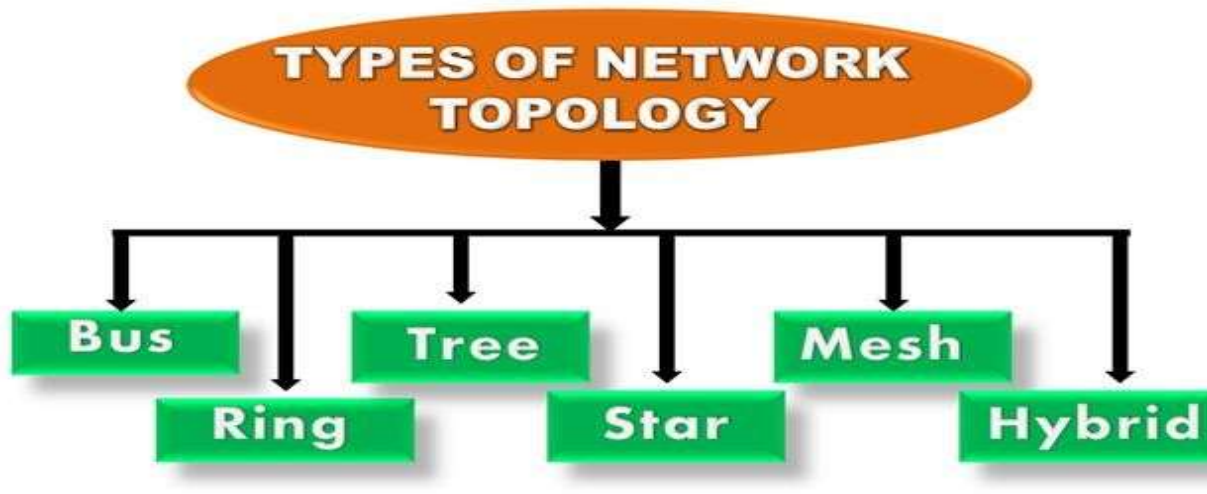
- MAN is used in communication between the banks in a city.
- It can be used in an Airline Reservation.
- It can be used in a college within a city.
- It can also be used for communication in the military.

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.

What is Topology?

- Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.



Bus Topology



- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.

Advantages of Bus topology:

- **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.

Disadvantages of Bus topology:

- **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.

Ring Topology



- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.

Advantages of Ring topology:

- **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- **Product availability:** Many hardware and software tools for network operation and monitoring are available.

Disadvantages of Ring topology:

- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Failure:** The breakdown in one station leads to the failure of the overall network.

Star Topology

- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.



Advantages of Star topology

Network control: Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.

Limited failure: As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.

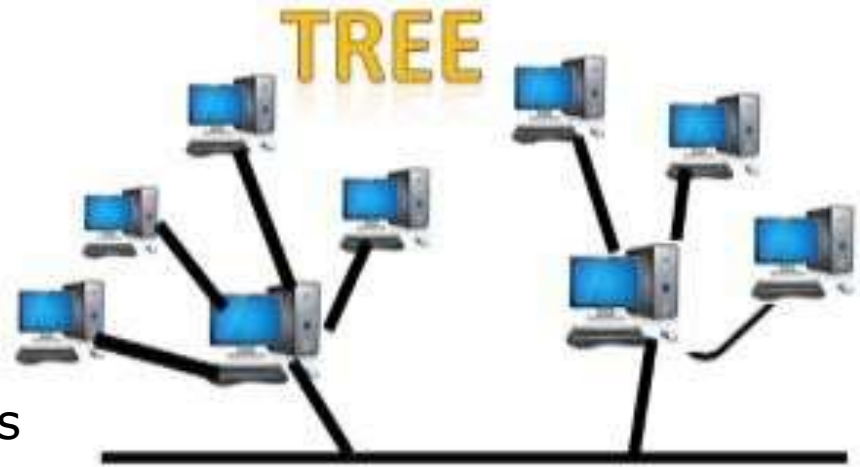
Disadvantages of Star topology

• **A Central point of failure:** If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.

• **Cable:** Sometimes cable routing becomes difficult when a significant amount of routing is required.

Tree topology

- Tree topology combines the characteristics of bus topology and star topology.
- A tree topology is a type of structure in which all the computers are connected with each other in **hierarchical fashion**.
- **The top-most node in tree topology is known as a root node**, and all other nodes are the descendants of the root node.
- There is only one path exists between two nodes for the data transmission. Thus, it forms a **parent-child hierarchy**.



Advantages of Tree topology

- **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.

Disadvantages of Tree topology

- **High cost:** Devices required for broadband transmission are very costly.
- **Failure:** A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.

Mesh topology

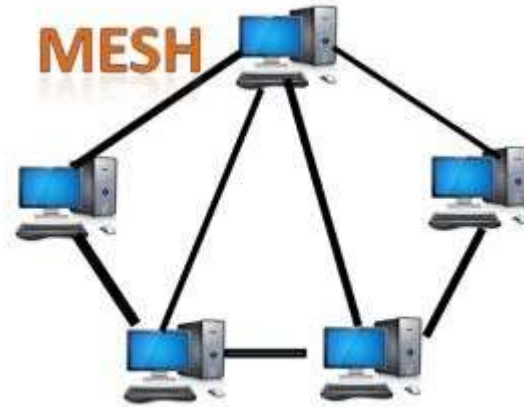
- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.

- There are multiple paths from one computer to another computer.

- It does not contain the switch, hub or any central computer which acts as a central point of communication.

- The Internet is an example of the mesh topology.

- Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.



Advantages of Mesh topology:

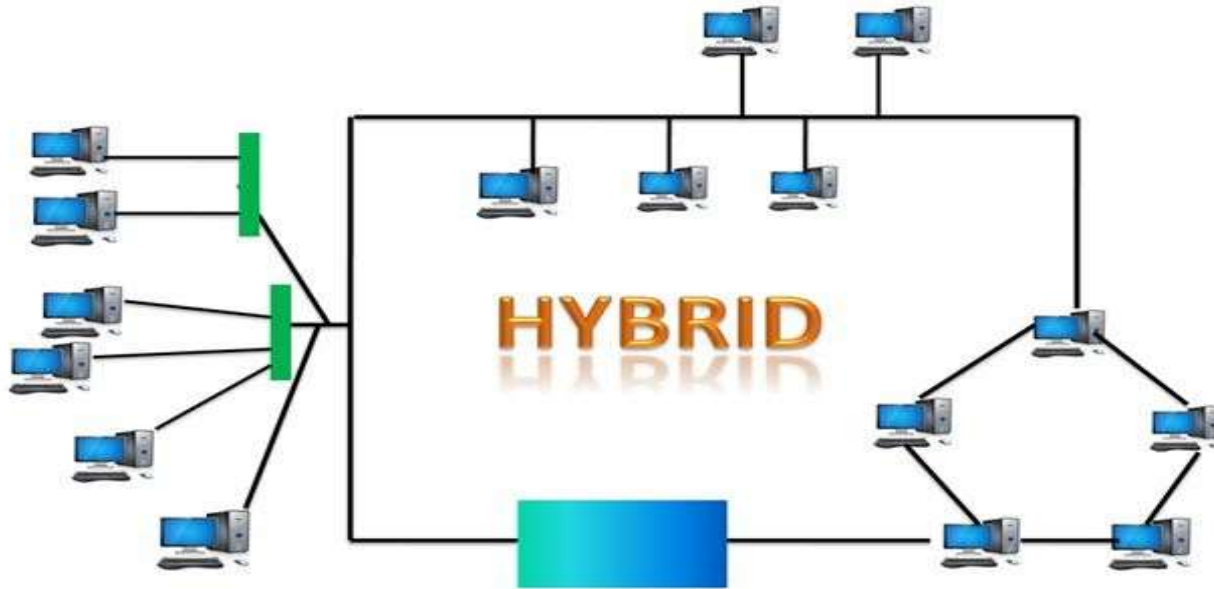
Reliable: The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.

Fast Communication: Communication is very fast between the nodes.

Disadvantages of Mesh topology

- **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
- **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication link failure goes undetected.

Hybrid Topology



- The combination of various different topologies is known as **Hybrid topology**.
- A Hybrid topology is a connection between different links and nodes to transfer the data.
- When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.

Advantages of Hybrid Topology

- **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
- **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.

Disadvantages of Hybrid topology

- **Complex design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
- **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.

IP address

An Internet Protocol address (IP address) is a logical numeric address that is assigned to every single computer, printer, switch, router or any other device that is part of a TCP/IP-based network.

The IP address is the core component on which the networking architecture is built; no network exists without it. An IP address is a logical address that is used to uniquely identify every node in the network. Because IP addresses are logical, they can change. They are similar to addresses in a town or city because the IP address gives the network node an address so that it can communicate with other nodes or networks, just like mail is sent to friends and relatives.

- Addresses in **IPv4** are 32-bits long. This allows for a maximum of 4,294,967,296 (2^{32}) unique addresses.
- Addresses in **IPv6** are 128-bits, which allows for 3.4×10^{38} (2^{128}) unique addresses.

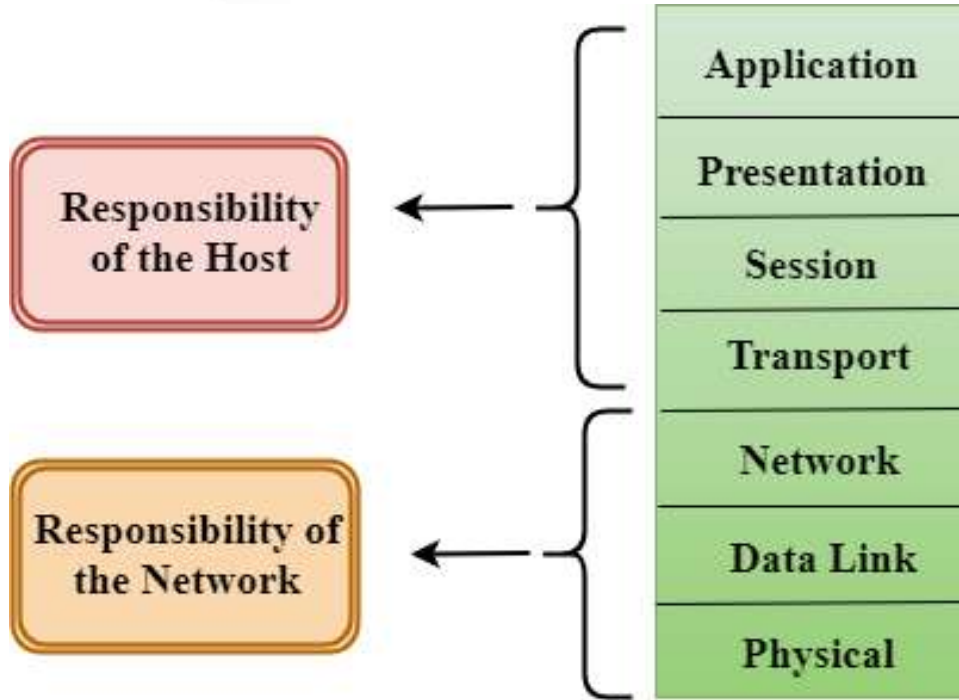
(MAC) Address

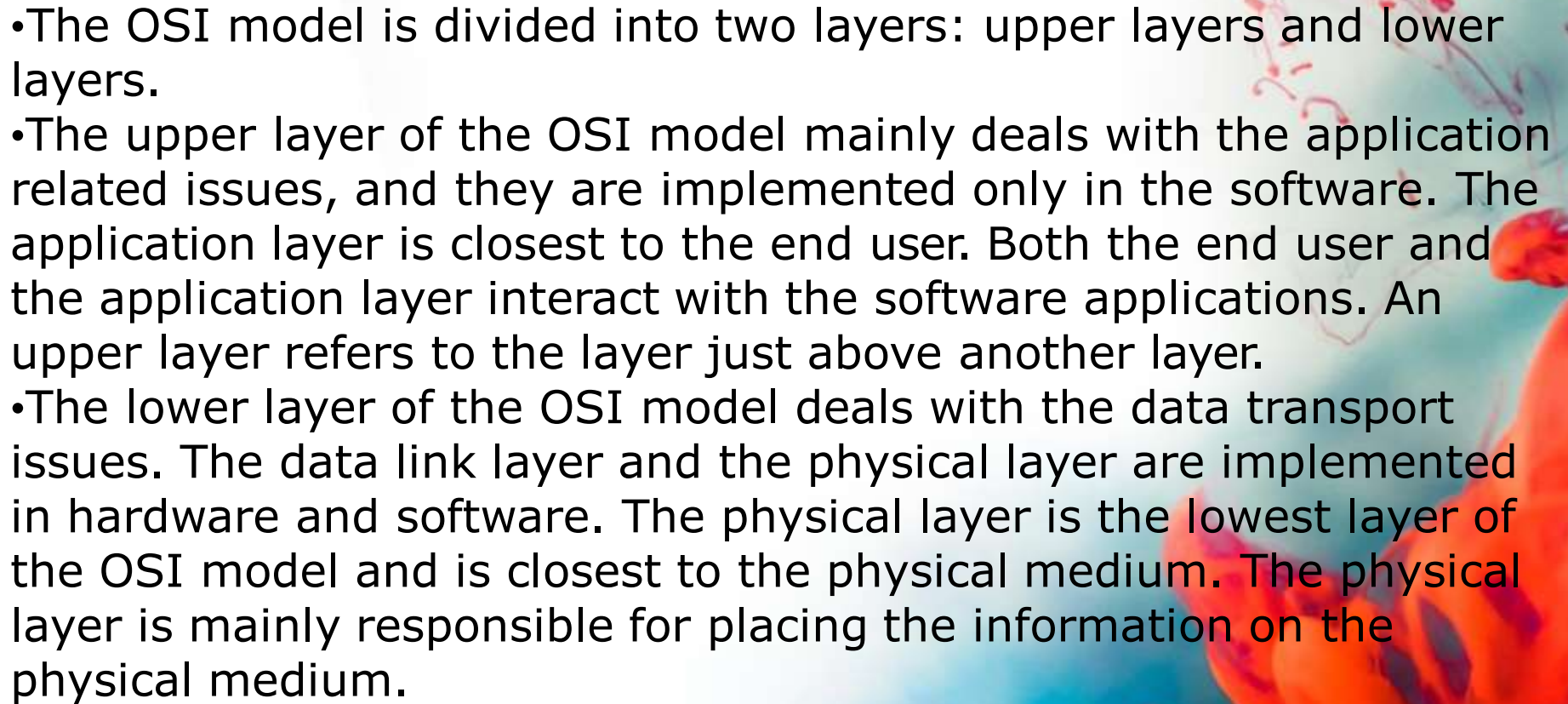
MAC Addresses are unique **48-bits** hardware number of a computer, which is embedded into network card (known as **Network Interface Card**) during the time of manufacturing. MAC Address is also known as **Physical Address** of a network device.

OSI Model

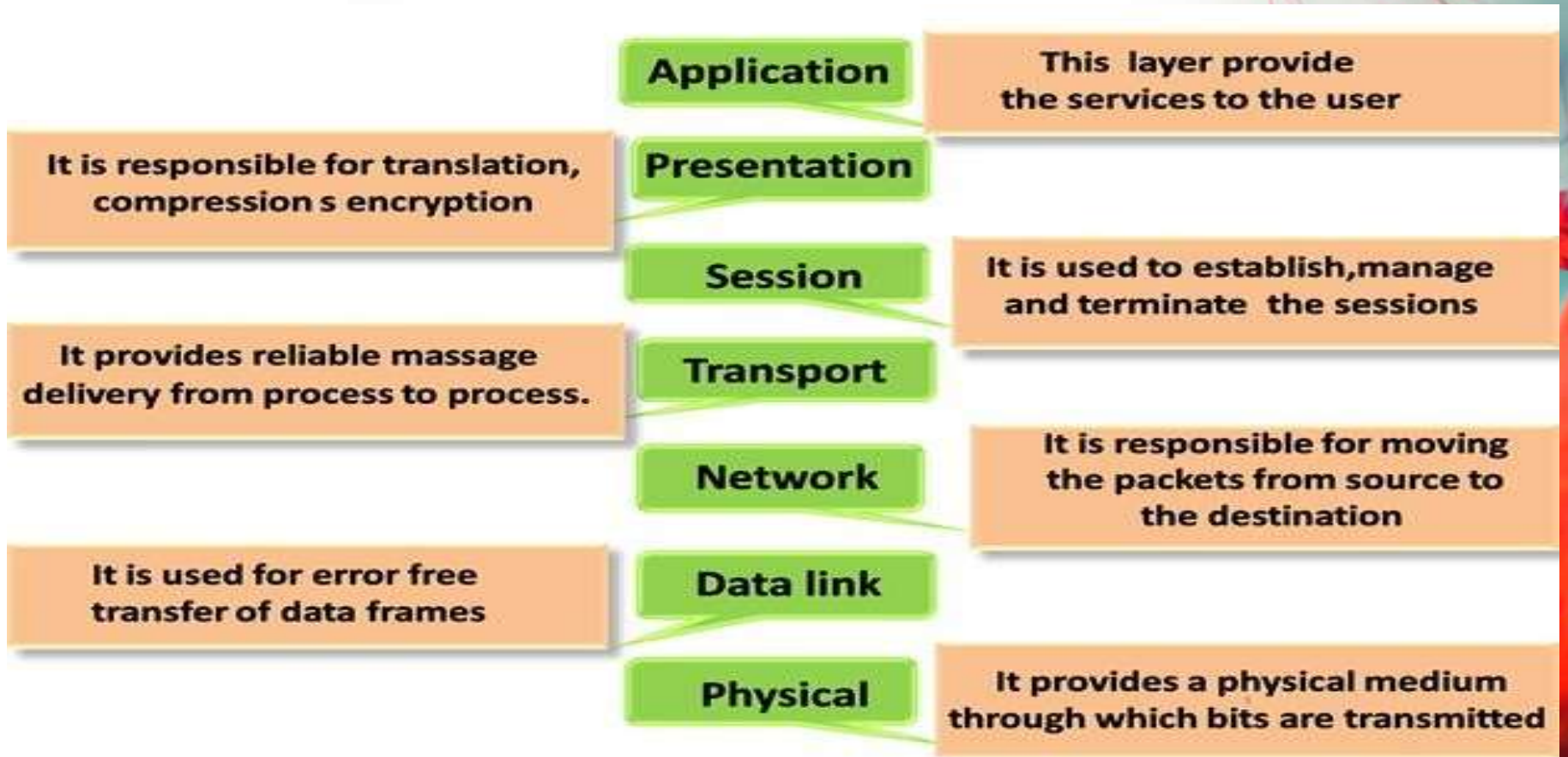
- OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network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

Characteristics of OSI Model:



- 
- The OSI model is divided into two layers: upper layers and lower layers.
 - The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
 - The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

Functions of the OSI Layers



Physical layer

- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- Physical Layer: This layer defines the hardware, cabling wiring, power output, pulse rate etc.

Functions of a Physical layer :

•**Line Configuration:** It defines the way how two or more devices can be connected physically.

Topology: It defines the way how network devices are arranged.

•**Signals:** It determines the type of the signal used for transmitting the information.

Data-Link Layer

- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- It contains two sub-layers:

- **Logical Link Control Layer**

- It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
- It identifies the address of the network layer protocol from the header.
- It also provides flow control.



- **Media Access Control Layer**

- A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
- It is used for transferring the packets over the network.

Functions of the Data-link layer

• **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

Network Layer

- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

- **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- **Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
- **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

Transport Layer

- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

Session Layer

- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

•**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.

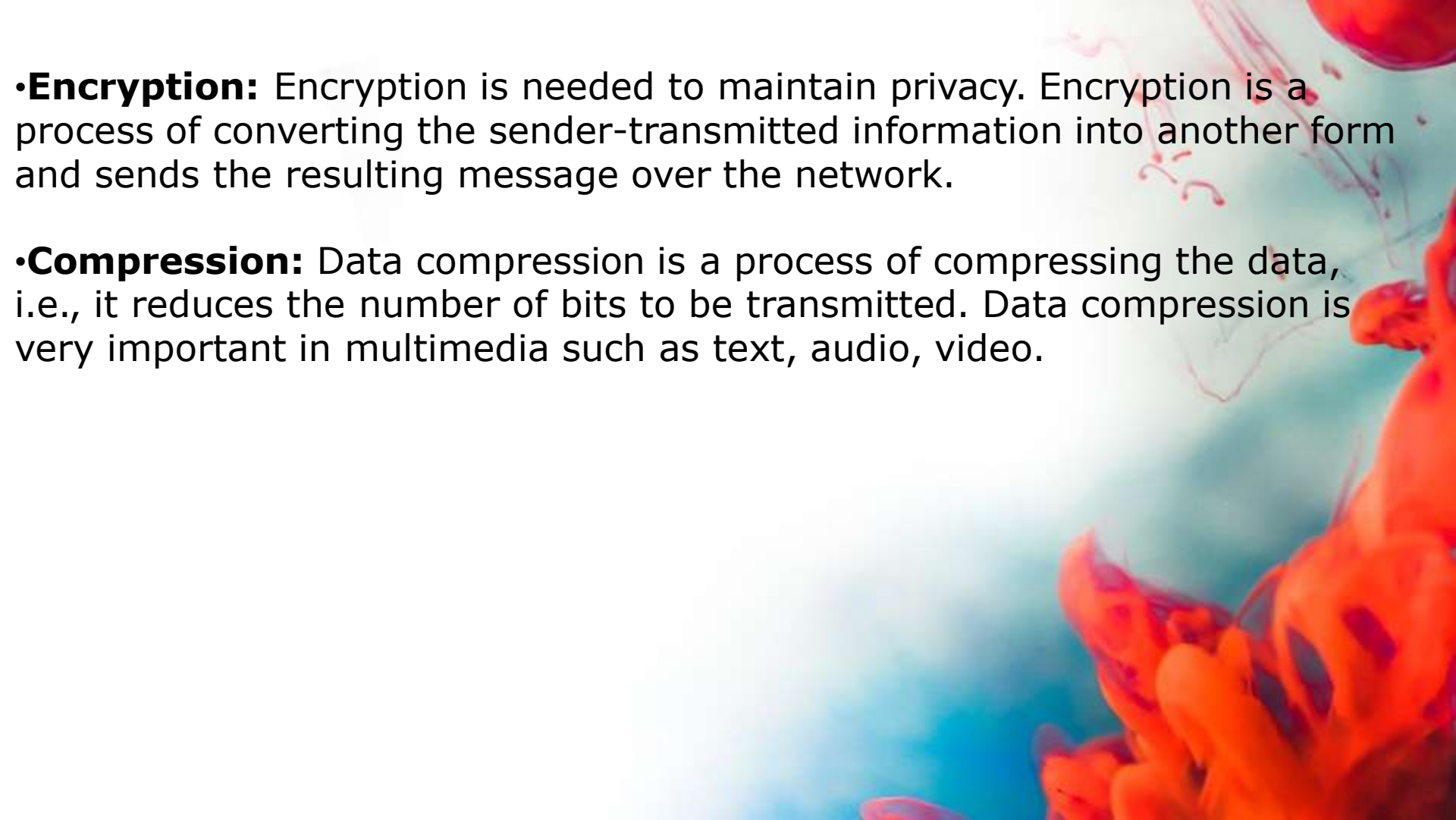
•**Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

Presentation layer

- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation layer is also known as the syntax layer.

Functions of Presentation layer:

•**Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.



•**Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.

•**Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

Application layer

- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application layer is not an application, but it performs the application layer functions.
- This layer provides the network services to the end-users.

Functions of Application layer:

- File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- Mail services:** An application layer provides the facility for email forwarding and storage.
- Directory services:** An application provides the distributed database sources and is used to provide that global information about various objects.

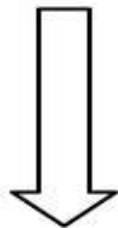
Deep In OSI Layers

The background of the slide features a vibrant underwater scene. In the upper right, a jellyfish with long, thin, pinkish-purple tentacles is visible against a light blue background. Below it, a coral reef with bright orange and red corals extends towards the bottom right corner. The overall lighting is bright and clear, suggesting a shallow reef environment.

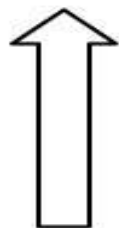
OSI Model

- OSI stands for **Open Systems Interconnection**. It has been developed by ISO – ‘**International Organization of Standardization**’, in the year 1974. 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.

Sender



Receiver



Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

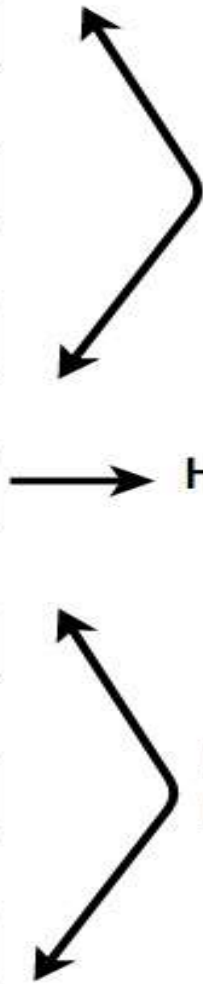
Data Link Layer

Physical Layer

Software Layers

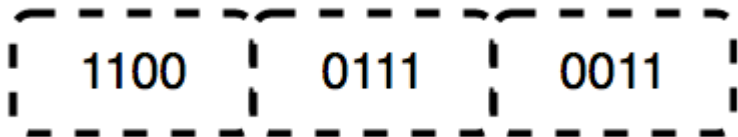
Heart of OSI

Hardware Layers



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 the actual physical connection between the devices. 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.



1100 0111 0011

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.

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.



- The packet received from 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 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, Data link layer adds physical addresses (MAC address) of 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 that amount of data that can be sent before receiving acknowledgement.

5.Access control: When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

*Packet in Data Link layer is referred 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) :

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

2.Logical Addressing: In order to identify each device on internet network uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

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

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

4. Transport Layer (Layer 4) :

- Transport layer provides services to application layer and takes services from 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. Transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

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 segment 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 correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.

The services provided by transport layer :

- 1.Connection Oriented Service:** It is a three-phase process which include
- Connection Establishment
 - Data Transfer
 - Termination / disconnection

In this type of transmission, the receiving device sends an acknowledgment, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.

2.Connection less 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 connection less 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 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 as synchronization points into the data. These synchronization point 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 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**.*

6. Presentation Layer (Layer 6) :

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 cipher text 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 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 as Desktop Layer.*

The functions of the Application layer are :

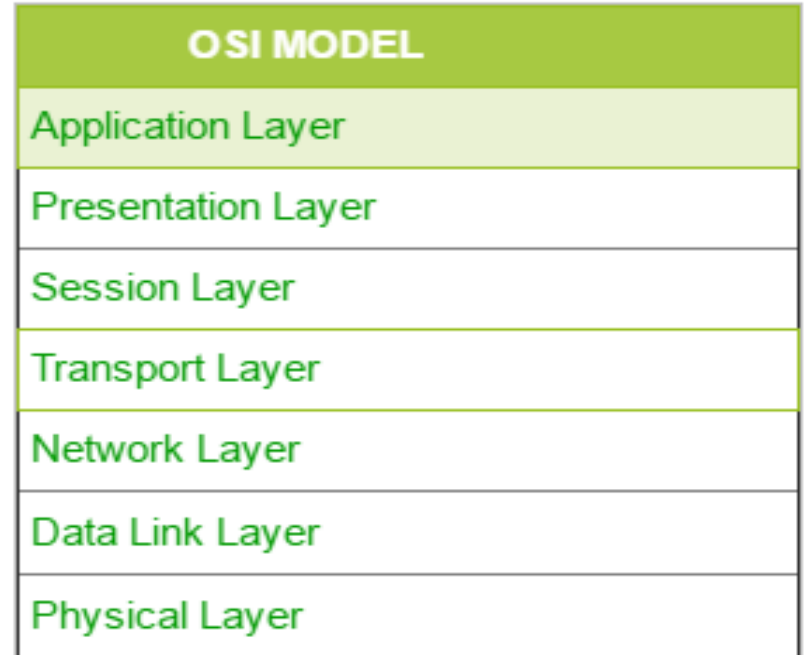
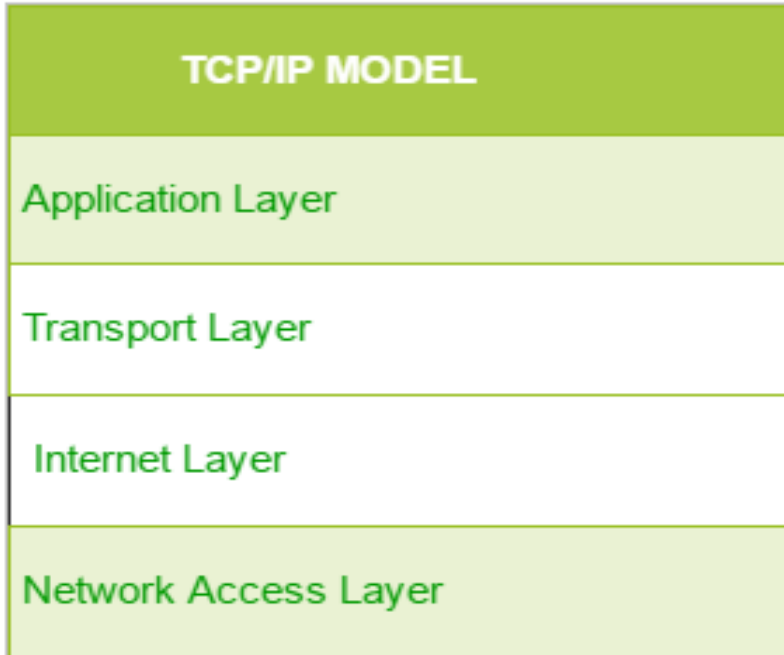
1. Network Virtual Terminal
2. FTAM-File transfer access and management
3. Mail Services
4. Directory Services

OSI model acts as a reference model and is not implemented in Internet because of its late invention. Current model being used is the TCP/IP model.

TCP/IP Model

- The **OSI Model** we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. 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



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 follow a horizontal approach.

OSI follows a vertical approach.

OSI uses different session and presentation layers.

OSI developed model then protocol.

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 –

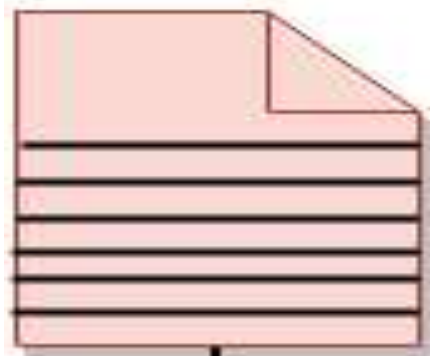
This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

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.

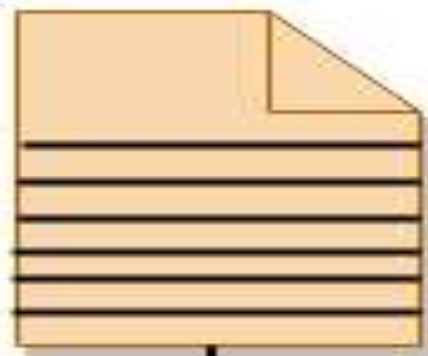
Client and Server model

- A client and server networking model is a model in which computers such as servers provide the network services to the other computers such as clients to perform a user based tasks. This model is known as client-server networking model.
- The application programs using the client-server model should follow the given below strategies:

Client



Server



Internet



Client

A client is a program that runs on the local machine requesting service from the server. A client program is a finite program means that the service started by the user and terminates when the service is completed.

Server

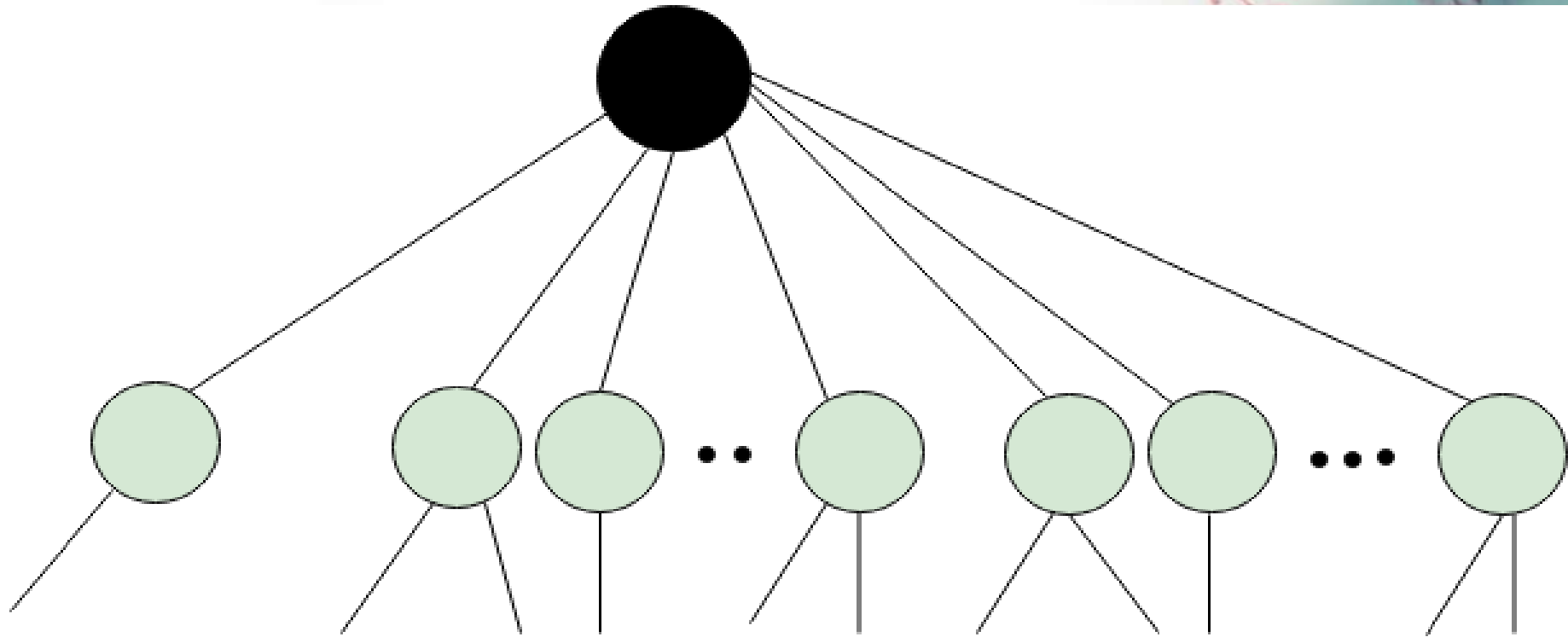
A server is a program that runs on the remote machine providing services to the clients. When the client requests for a service, then the server opens the door for the incoming requests, but it never initiates the service.

A server program is an infinite program means that when it starts, it runs infinitely unless the problem arises. The server waits for the incoming requests from the clients. When the request arrives at the server, then it responds to the request.

DNS Domain Name System.

- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- **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 TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.



Inverse domain

Generic domains

Country domains

<u>Label</u>	<u>Description</u>
aero	Airlines and aerospace companies
biz	Businesses or firms
com	Commercial Organizations
coop	Cooperative business Organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International Organizations
mil	Military groups
museum	Museum & other nonprofit organizations
name	Personal names
net	Network Support centers
org	Nonprofit Organizations
pro	Professional individual Organizations

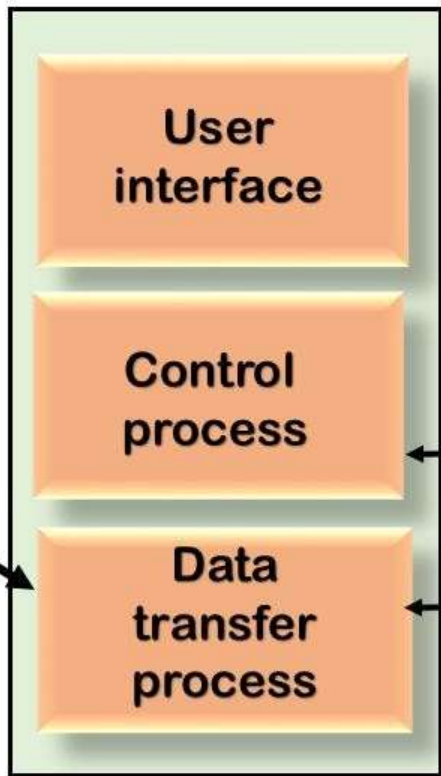
Working of DNS

- 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 lookup while requests containing an IP address which is converted into a name known as reverse DNS lookup.
- DNS implements a distributed database to store the name of all the hosts available on the internet.

FTP File transfer protocol.

- FTP stands for File transfer protocol.
- FTP 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.

User 

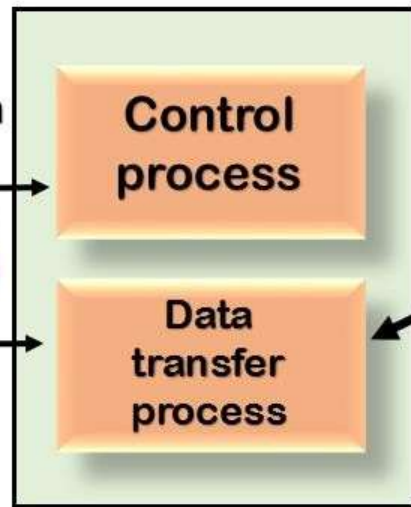


Client

Control connection



Data connection



Server

FTP Clients

- FTP client is a program that implements a file transfer protocol which allows you to transfer files between two hosts on the internet.
- It allows a user to connect to a remote host and upload or download the files.
- It has a set of commands that we can use to connect to a host, transfer the files between you and your host and close the connection.
- The FTP program is also available as a built-in component in a Web browser. This GUI based FTP client makes the file transfer very easy and also does not require to remember the FTP commands.

Telnet

- The main task of the internet is to provide services to users. For example, users want to run different application programs at the remote site and transfers a result to the local site. This requires a client-server program such as FTP, SMTP. But this would not allow us to create a specific program for each demand.
- The better solution is to provide a general client-server program that lets the user access any application program on a remote computer. Therefore, a program that allows a user to log on to a remote computer. A popular client-server program Telnet is used to meet such demands. Telnet is an abbreviation for **Terminal Network**.
- Telnet provides a connection to the remote computer in such a way that a local terminal appears to be at the remote side.

Simple Mail Transfer Protocol (SMTP)

- Email is emerging as one of the most valuable services on the internet today. Most of the internet systems use SMTP as a method to transfer mail from one user to another. SMTP is a push protocol and is used to send the mail whereas POP (post office protocol) or IMAP (internet message access protocol) are used to retrieve those mails at the receiver's side.

SMTP

- SMTP is an application layer protocol. The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is always on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection on that port (25). After successfully establishing the TCP connection the client process sends the mail instantly.

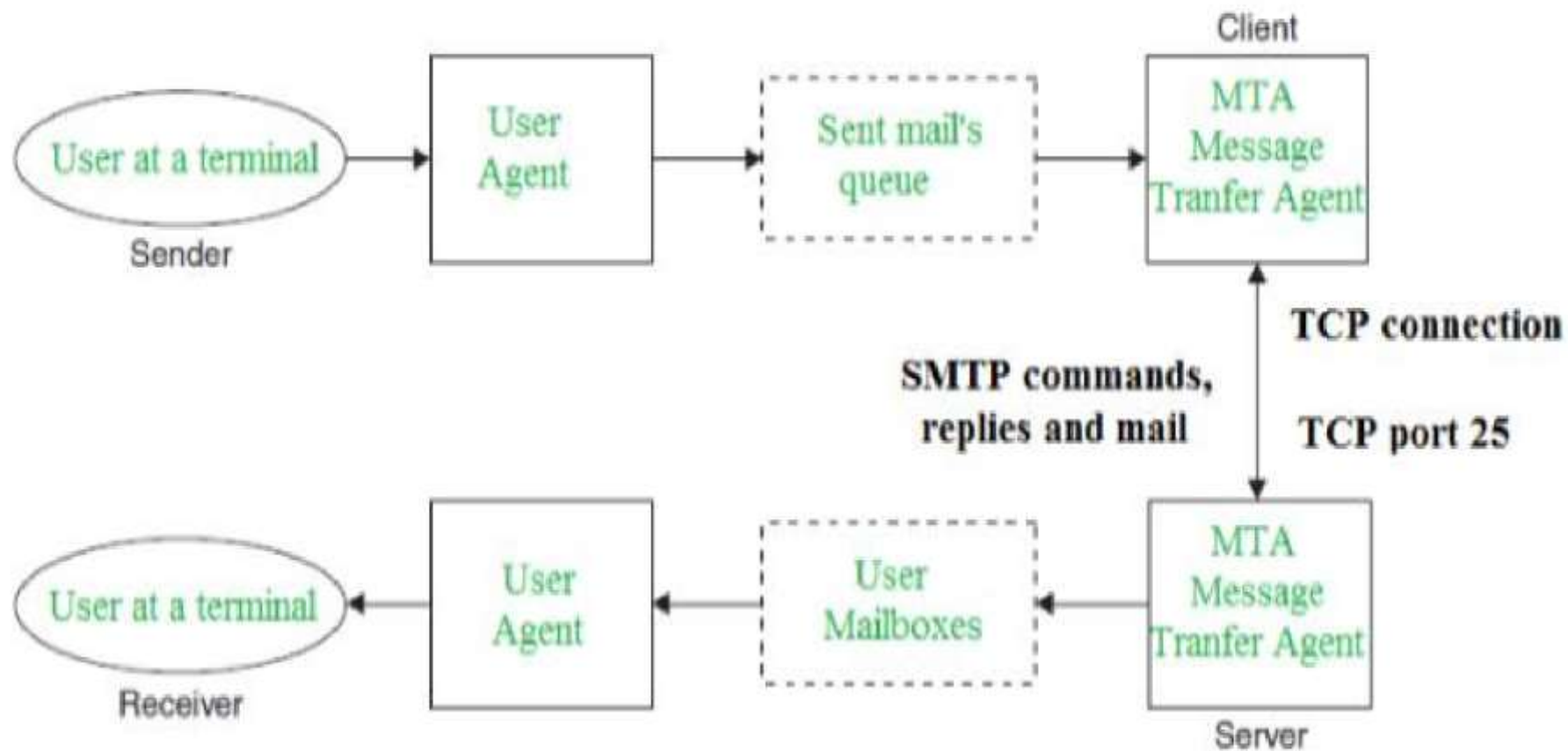
SMTP Protocol

The SMTP model is of two type :

- 1.End-to- end method
- 2.Store-and- forward method

Model of SMTP system

In the SMTP model user deals with the user agent (UA) for example Microsoft Outlook, Netscape, Mozilla, etc. In order to exchange the mail using TCP, MTA is used. The users sending the mail do not have to deal with the MTA it is the responsibility of the system admin to set up the local MTA. The MTA maintains a small queue of mails so that it can schedule repeat delivery of mail in case the receiver is not available. The MTA delivers the mail to the mailboxes and the information can later be downloaded by the user agents.



Both the SMTP-client and MSTP-server should have 2 components:

1. User agent (UA)
2. Local MTA

Post Office Protocol (POP)

Post Office Protocol (POP) is a type of computer networking and Internet standard protocol that extracts and retrieves email from a remote mail server for access by the host machine.

POP is an application layer protocol in the OSI model that provides end users the ability to fetch and receive email.

Post Office Protocol is the primary protocol behind email communication. POP works through a supporting email software client that integrates POP for connecting to the remote email server and downloading email messages to the recipient's computer machine.

POP3 stands for Post Office Protocol Version3 (Current Version). POP is a protocol which listens on port 110 and is responsible for accessing the mail service on a client machine. POP3 works in two modes such as Delete Mode and Keep Mode.

a) Delete Mode: A mail is deleted from the mailbox after successful retrieval.

b) Keep Mode: The Mail remains Intact in the mailbox after successful retrieval.

Difference between SMTP and POP3

- For sending and receiving messages, we use two protocols one is SMTP (Simple Mail Transfer Protocol) and another is POP3 (Post Office Protocol version 3). They are also called as PUSH and POP protocols respectively. They are agents, Message Transfer Agent and Message Access Agent respectively to send and retrieve the messages.

S.NO	SMTP	POP3
1.		
2.		
3.	The port number of SMTP is 25.	The port number of POP3 is 110.
4.	It is a MTA (Message Transfer Agent) for sending the to the receiver.	It is MAA (Message Access Agent) for accessing the messages from mail box.
5.		It has also two MAAs one is client MAA (Message Access Agent) and another is server is server (Message Access Agent). MAA
6.		POP3 is also known as POP protocol.

IMAP (Internet Message Access Protocol)

- IMAP (Internet Message Access Protocol) is a standard email [protocol](#) that stores email messages on a mail server, but allows the end user to view and manipulate the messages as though they were stored locally on the end user's computing device(s). This allows users to organize messages into folders, have multiple client applications know which messages have been read, flag messages for urgency or follow-up and save draft messages on the server.

IMAP can be contrasted with another [client/server](#) email protocol, Post Office Protocol 3 ([POP3](#)). With POP3, mail is saved for the end user in a single mailbox on the server and moved to the end user's device when the mail client opens. While POP3 can be thought of as a "store-and-forward" service, IMAP can be thought of as a remote [file server](#).

Multipurpose Internet Mail Extension (MIME) Protocol

- **Why do we need MIME?**

Limitations of Simple Mail Transfer Protocol (SMTP):

- SMTP has a very simple structure
- It's simplicity however comes with a price as it only send messages in NVT 7-bit ASCII format.
- It cannot be used for languages that do not support 7-bit ASCII format such as- French, German, Russian, Chinese and Japanese, etc. so it cannot be transmitted using SMTP. So, in order *to make SMTP more broad we use MIME*.
- t cannot be used to send binary files or video or audio data.

Purpose and Functionality of MIME –

Growing demand for Email Message as people also want to express in terms of Multimedia. So, MIME another email application is introduced as it is not restricted to textual data.

MIME *transforms non-ASCII data* at sender side to NVT 7-bit data and delivers it to the client SMTP. The message at receiver side is transferred back to the original data. As well as we can send video and audio data using MIME as it transfers them also in 7-bit ASCII data.

Features of MIME –

It is able to send multiple attachments with a single message.

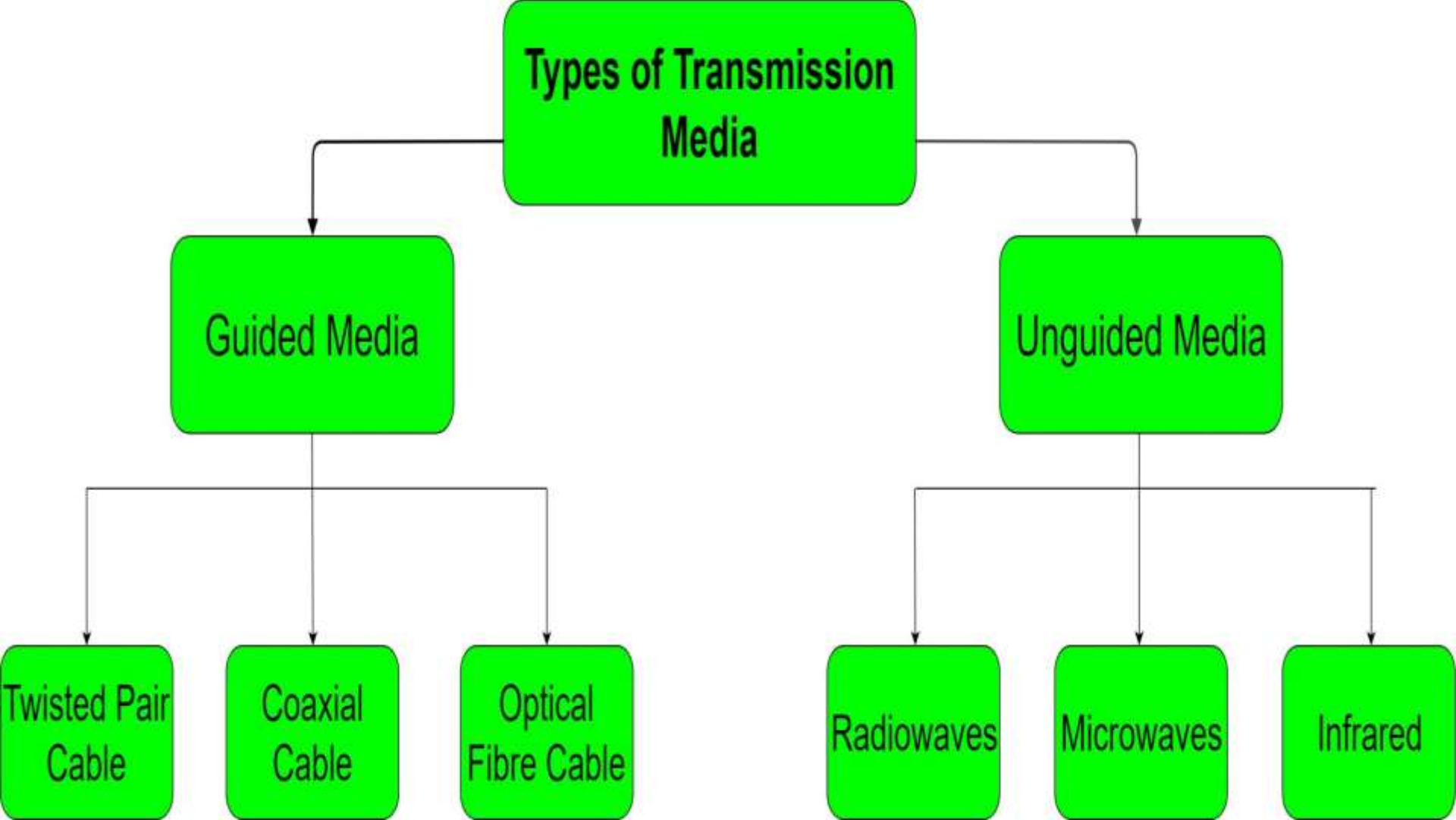
Unlimited message length.

Binary attachments (executables, images, audio, or video files) which may be divided if needed.

MIME provided support for varying content types and multi-part messages.

Types of Transmission Media

- In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e it is the channel through which data is sent from one place to another.
Transmission Media is broadly classified into the following types:



Types of Transmission Media

Guided Media

Unguided Media

Twisted Pair Cable

Coaxial Cable

Optical Fibre Cable

Radiowaves

Microwaves

Infrared

1. Guided Media:

It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

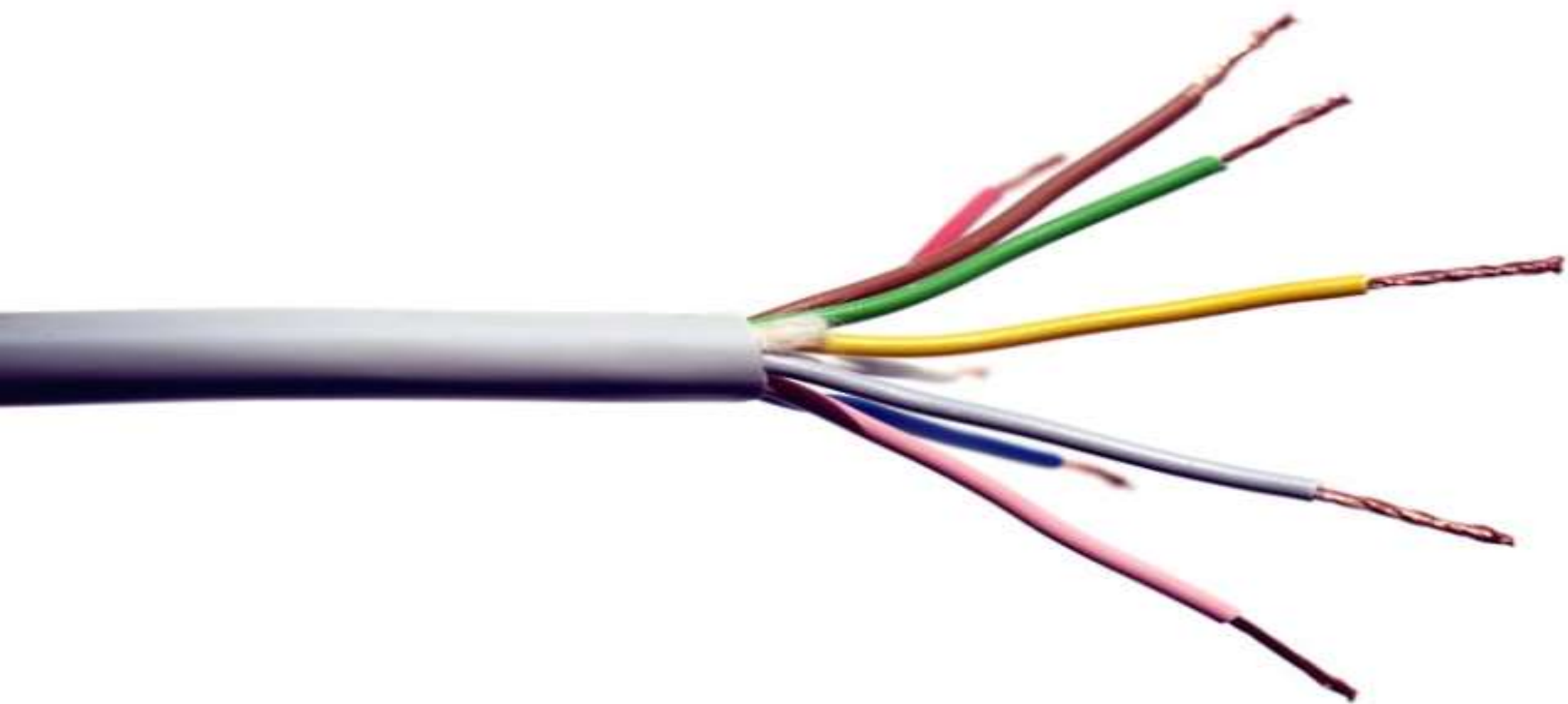
Features:

- High Speed
- Secure
- Used for comparatively shorter distances

There are 3 major types of Guided Media:

(i) Twisted Pair Cable –

It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:



Unshielded Twisted Pair (UTP):

This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.

Shielded Twisted Pair (STP):

This type of cable consists of a special jacket to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.

(ii) Coaxial Cable –

It has an outer plastic covering containing 2 parallel conductors each having a separate insulated protection cover. Coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.

Advantages:

- High Bandwidth
- Better noise Immunity
- Easy to install and expand
- Inexpensive

Disadvantages:

- Single cable failure can disrupt the entire network

Protective Plastic Cover

Inner Insulator

Braided Outer Conductor

Inner Conducting Core



(iii) Optical Fiber Cable –

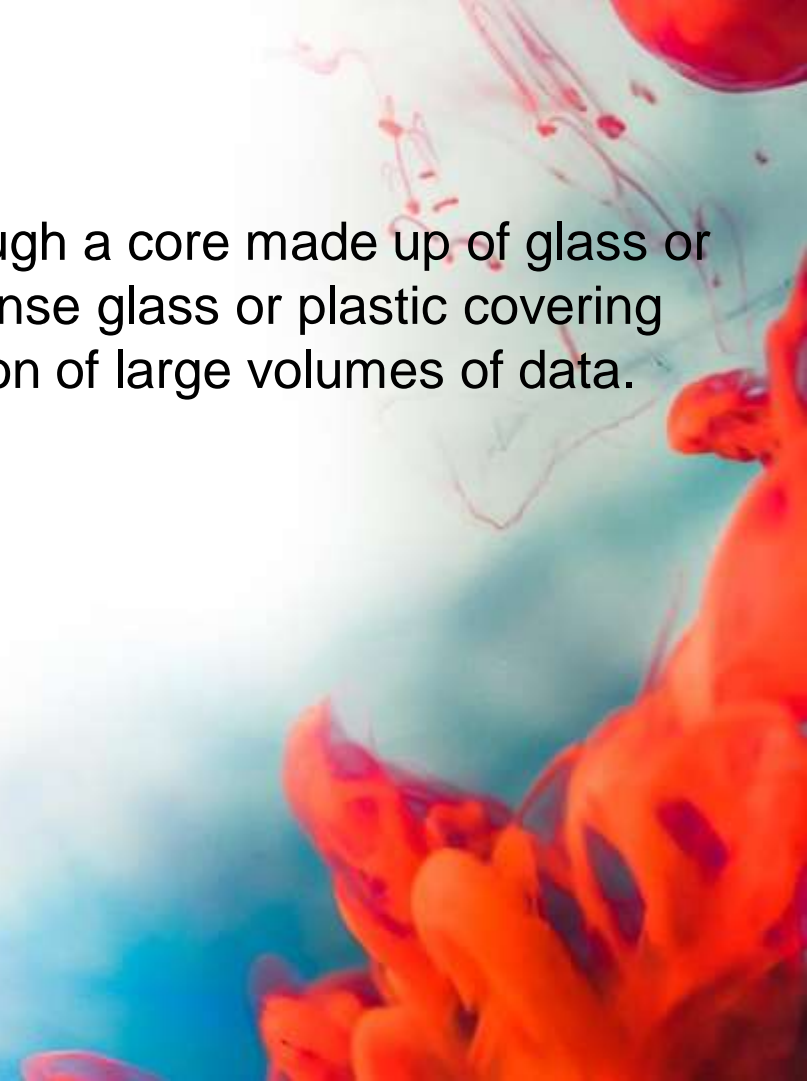
It uses the concept of reflection of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for transmission of large volumes of data.

Advantages:

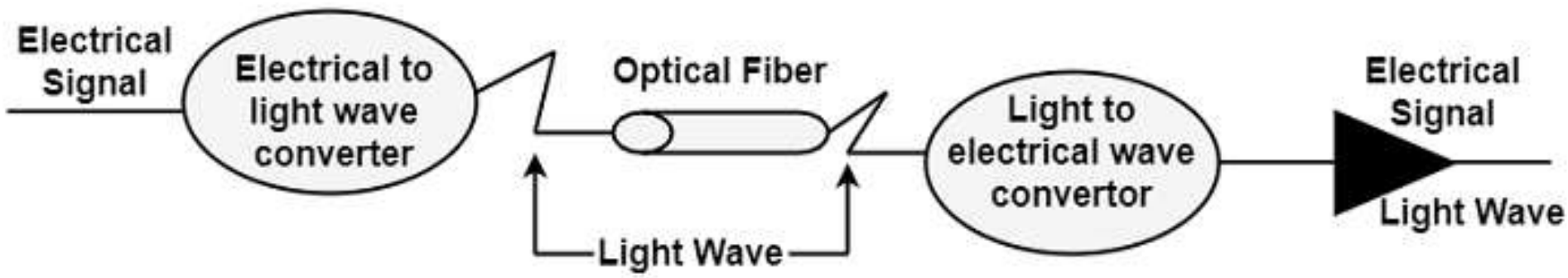
- Increased capacity and bandwidth
- Light weight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials

Disadvantages:

- Difficult to install and maintain
- High cost



Construction of Optical Fiber Cable



2. Unguided Media:

It is also referred to as Wireless or Unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals.

Features:

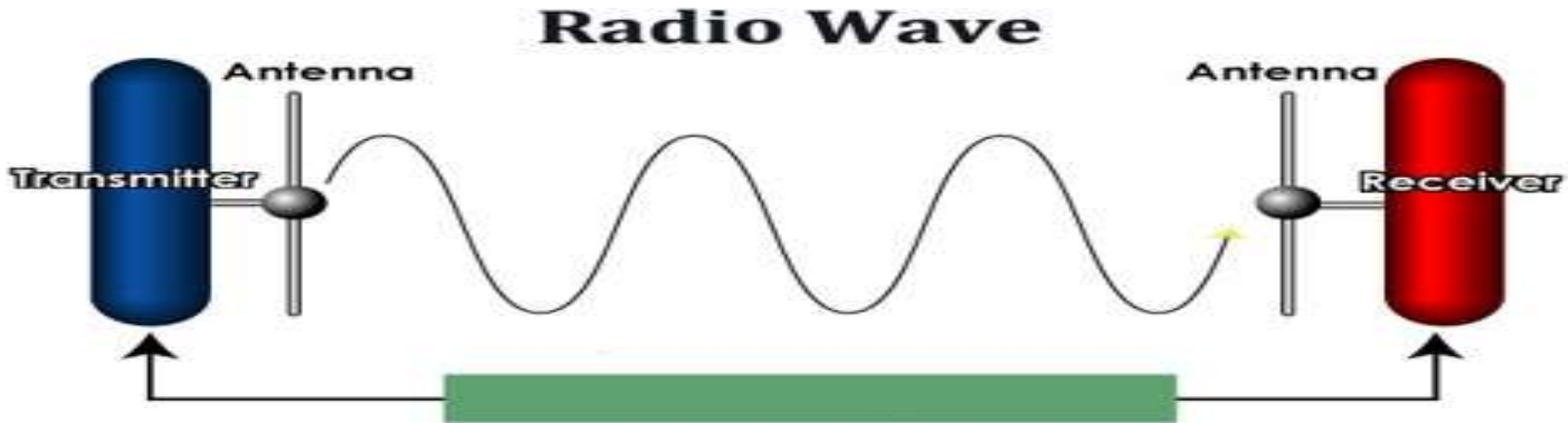
- Signal is broadcasted through air
- Less Secure
- Used for larger distances

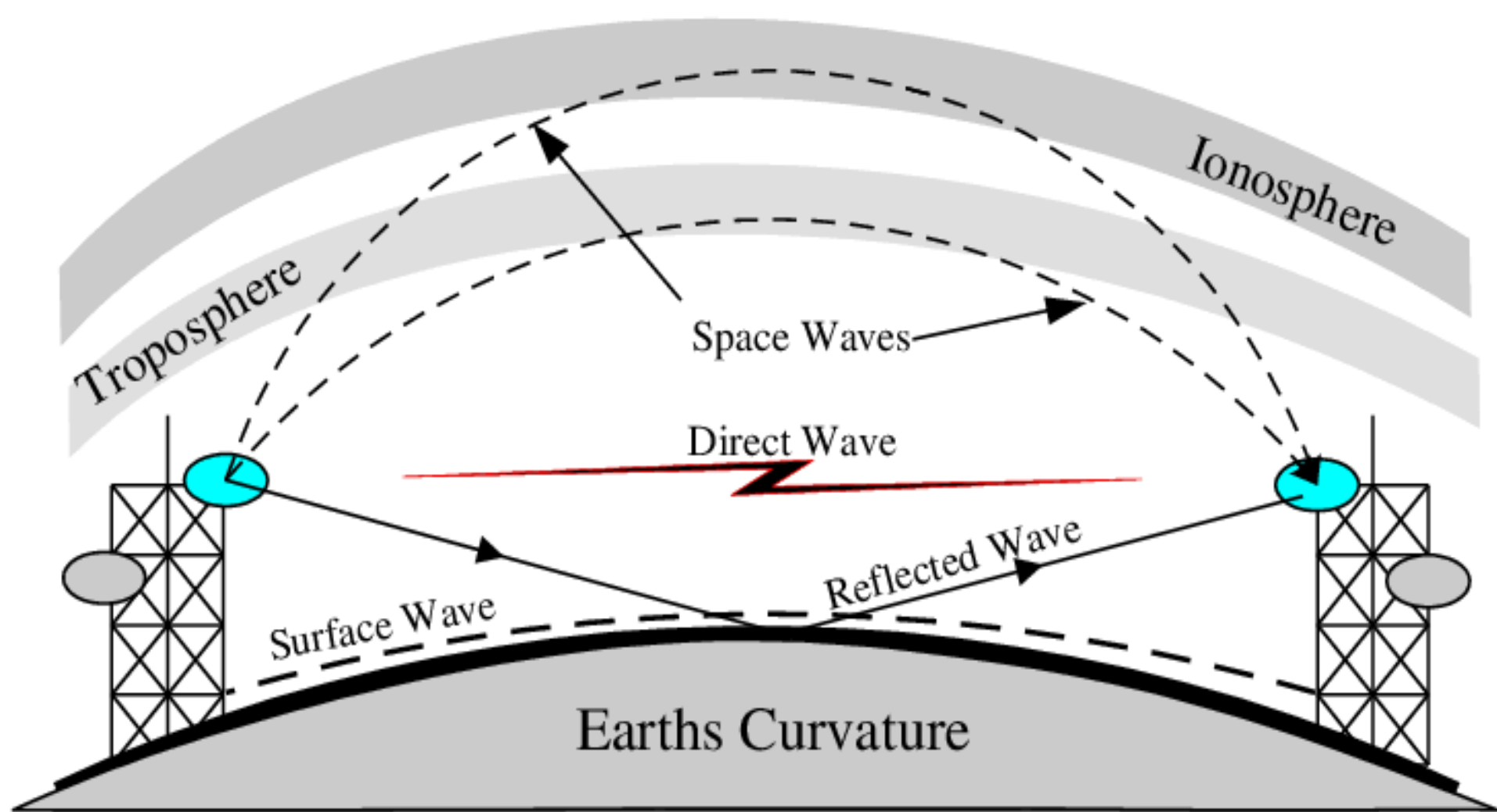
There are 3 major types of Unguided Media:



(i) Radiowaves –

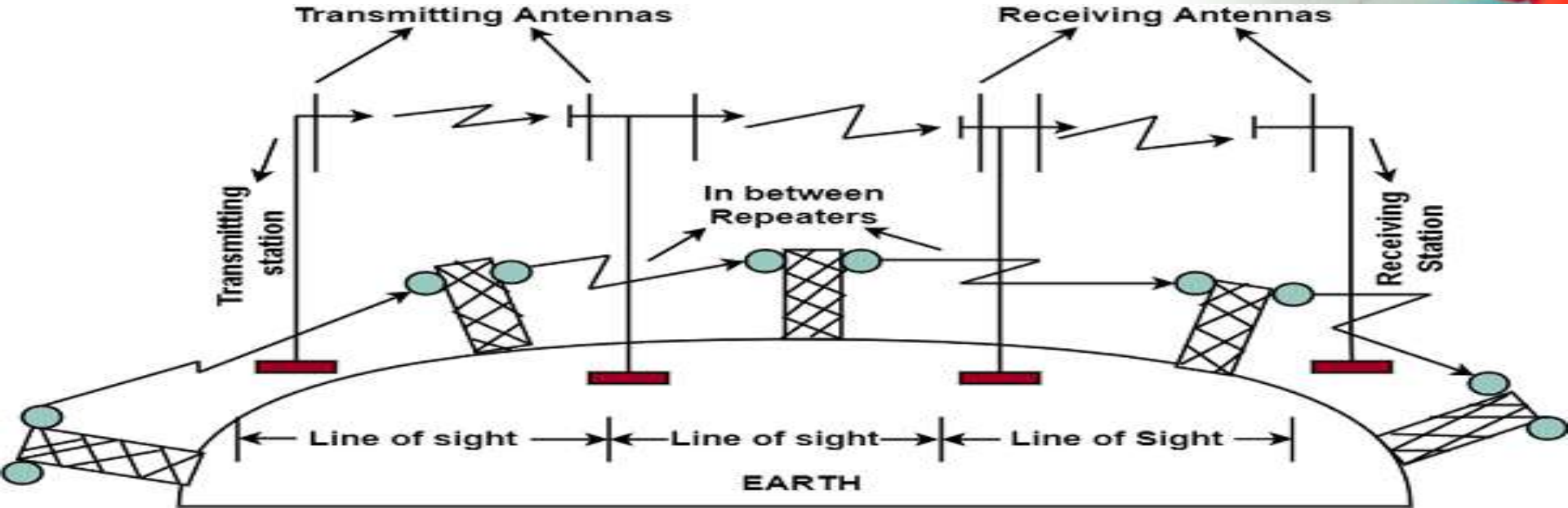
These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range: 3KHz – 1GHz. AM and FM radios and cordless phones use Radiowaves for transmission. Further Categorized as (i) Terrestrial and (ii) Satellite.





ii) Microwaves –

It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range: 1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.



(iii) Infrared –

Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range: 300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.



Web Hosting

Web hosting is a service that allows organizations and individuals to post a website or web page onto the Internet. A web host, or web hosting service provider, is a business that provides the technologies and services needed for the website or webpage to be viewed in the Internet. Websites are hosted, or stored, on special computers called servers. When Internet users want to view your website, all they need to do is type your website address or domain into their browser. Their computer will then connect to your server and your webpages will be delivered to them through the browser.

Meta Search Engine

- A meta search engine is a type of search engine that gives results based on a combination of results from other search engine databases. It specializes in concatenating databases from a variety of search engines and linking search results to relevant sources. To put it simply, a meta search engine submits your query to several other search engines and returns a summary of the results. Therefore, the search results you receive are an aggregate result of multiple searches.

JavaScript

- [JavaScript](#) is a lightweight programming language (“scripting language”) and used to make web pages interactive. It can insert dynamic text into HTML. JavaScript is also known as browser’s language. JavaScript(JS) is not similar or related to Java. Both the languages have a C like a syntax and are widely used in client-side Web applications, but there are few similarities only. JavaScript is mainly used to make web pages more interactive.

Java

- Java is an object-oriented programming language and have virtual machine platform that allows you to create compiled programs that run on nearly every platform. Java promised, “Write Once, Run Anywhere”. Java is used in a wide range of places, including Android apps, credit card programming and in the creation of desktop applications and web enterprise applications.

Authentication

- **Authentication** is the process of verifying who you are. When you log on to a PC with a user name and password you are authenticating, Authentication is about validating your credentials like User Name/User ID and password to verify your identity. The system determines whether you are what you say you are using your credentials. In public and private networks, the system authenticates the user identity via login passwords. Authentication is usually done by a username and password, and sometimes in conjunction with factors of authentication, which refers to the various ways to be authenticated.

Authorization

- **Authorization** the process of verifying that you have access to something. Gaining access to a resource (e.g. directory on a hard disk) because the permissions configured on it allow you access is authorization. Authorization, on the other hand, occurs after your identity is successfully authenticated by the system, which ultimately gives you full permission to access the resources such as information, files, databases, funds, locations, almost anything.

Automated Teller Machine (ATM)

- An ATM, which stands for automated teller machine, is a specialized computer that makes it convenient to manage a bank account holder's funds. It allows a person to check account balances, withdraw or deposit money, print a statement of account activities or transactions, and even purchase stamps.

HTTP

- HTTP stands for **HyperText Transfer Protocol**.
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment 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 used to carry the data in the form of MIME-like format.

Ethernet

- Ethernet is an array of networking technologies and systems used in local area networks (LAN), where computers are connected within a primary physical space.
- Systems using Ethernet communication divide data streams into packets, which are known as frames. Frames include source and destination address information, as well as mechanisms used to detect errors in transmitted data and retransmission requests.

What is Ecommerce?

- Ecommerce, also known as electronic commerce or internet commerce, refers to the buying and selling of goods or services using the internet, and the transfer of money and data to execute these transactions. Ecommerce is often used to refer to the sale of physical products online, but it can also describe any kind of commercial transaction that is facilitated through the internet.
- Whereas e-business refers to all aspects of operating an online business, ecommerce refers specifically to the transaction of goods and services.

Cookie

- A cookie is a small amount of data generated by a website and saved by your web browser. Its purpose is to remember information about you, similar to a preference file created by a software application.
- While cookies serve many functions, their most common purpose is to store login information for a specific site. Some sites will save both your username and password in a cookie, while others will only save your username. Whenever you check a box that says, "**Remember me on this computer**," the website will generate a login cookie once you successfully log in. Each time you revisit the website, you may only need to enter your password or you might not need to log in at all.

Session

- In the computing world, a session refers to a limited time of communication between two systems. Some sessions involve a client and a server, while other sessions involve two personal computers.
- A common type of client/server session is a Web or HTTP session. An HTTP session is initiated by a Web browser each time you visit a website. While each page visit constitutes an individual session, the term is often used to describe the entire time you spend on the website

proxy server

- Represent some else
- Authorized to act on behalf of another
- A proxy server verifies and forwards incoming client requests to other servers for further communication. A proxy server is located between a client and a server where it acts as an intermediary between the two, such as a Web browser and a Web server. The proxy server's most important role is providing security



Common Gateway Interface (CGI)

- The **Common Gateway Interface (CGI)** provides the middleware between WWW servers and external databases and information sources. The World Wide Web Consortium (W3C) defined the Common Gateway Interface (CGI) and also defined how a program interacts with a Hyper Text Transfer Protocol (HTTP) server. The Web server typically passes the form information to a small application program that processes the data and may send back a confirmation message. This process or convention for passing data back and forth between the server and the application is called the common gateway interface (CGI).

Private key and Public key

- Cryptography is the science of secret writing with the intention of keeping the data secret. Cryptography is classified into symmetric cryptography, asymmetric cryptography and hashing.
- Private Key:
In Private key, the same key (secret key) is used for encryption and decryption. In this key is symmetric because the only key is copy or share by another party to decrypt the cipher text. It is faster than the public key cryptography.
- **Public Key:**
In Public key, two keys are used one key is used for encryption and another key is used for decryption. One key (public key) is used for encrypt the plain text to convert it into cipher text and another key (private key) is used but receiver to decrypt the cipher text to read the message.

1.

2.

3.

In private key cryptography, the key is kept secret.

In public key cryptography, one of the two keys is kept secret.

4.

Private key is **Symmetrical** because there is only one key that is called secret key.

Public key is **Asymmetrical** because there is two type of key: private and public key.

5.

In this cryptography, sender and receiver met to share a key.

In this cryptography, sender and receiver does not need to met.

6.

In this cryptography, public key can be public and private key is private.

Cyber Law (IT Law)

- **Cyber Law** also called IT Law is the law regarding Information-technology including computers and internet. It is related to legal informatics and supervises the digital circulation of information, software, information security and e-commerce.
- IT law does not consist a separate area of law rather it encloses aspects of contract, intellectual property, privacy and data protection laws. Intellectual property is a key element of IT law. The area of software license is controversial and still evolving in Europe and elsewhere.

Importance of Cyber Law:

1. It covers all transaction over internet.
2. It keeps eyes on all activities over internet.
3. It touches every action and every reaction in cyberspace.

Area of Cyber Law:

Cyber laws contain different types of purposes. Some laws create rules for how individuals and companies may use computers and the internet while some laws protect people from becoming the victims of crime through unscrupulous activities on the internet.



Difference between MAC Address and IP Address

- Both [MAC Address](#) and [IP Address](#) are used to uniquely defines a device on the internet. NIC Card's Manufacturer provides the MAC Address, on the other hand Internet Service Provider provides IP Address.
- The main difference between MAC and IP address is that, MAC Address is used to ensure the physical address of computer. It uniquely identifies the devices on a network. While IP address are used to uniquely identifies the connection of network with that device take part in a network.

1.

2.

MAC Address is a six byte hexadecimal address.

IP Address is either four byte (IPv4) or six byte (IPv6) address.

3.

A device attached with MAC Address can retrieve by ARP protocol.

A device attached with IP Address can retrieve by RARP protocol.

4.

NIC Card's Manufacturer provides the MAC Address.

Internet Service Provider provides IP Address.

5.

IP Address is the logical address of the computer.

User Datagram Protocol (UDP)

- **User Datagram Protocol (UDP)** is a Transport Layer protocol. UDP is a part of Internet Protocol suite, referred as UDP/IP suite. Unlike TCP, it is **unreliable and connectionless protocol**. So, there is no need to establish connection prior to data transfer.
- Though Transmission Control Protocol (TCP) is the dominant transport layer protocol used with most of Internet services; provides assured delivery, reliability and much more but all these services cost us with additional overhead and latency. Here, UDP comes into picture.
- For the Realtime services like computer gaming, voice or video communication, live conferences; we need UDP. Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets. There is no error checking in UDP, so it also save bandwidth.

TRANSMISSION CONTROL PROTOCOL (TCP)

USER DATAGRAM PROTOCOL (UDP)

TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.

UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission.

TCP is reliable as it guarantees delivery of data to the destination router.

The delivery of data to the destination cannot be guaranteed in UDP.

TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data.

UDP has only the basic error checking mechanism using checksums.

Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in-order at the receiver.

There is no sequencing of data in UDP. If ordering is required, it has to be managed by the application layer.

TCP is comparatively slower than UDP.

UDP is faster, simpler and more efficient than TCP.

Retransmission of lost packets is possible in TCP, but not in UDP.

There is no retransmission of lost packets in User Datagram Protocol (UDP).

TCP has a (20-80) bytes variable length header.

UDP has a 8 bytes fixed length header.

TCP is heavy-weight.

UDP is lightweight.

TCP doesn't supports Broadcasting.

UDP supports Broadcasting.

Internet Service Provider (ISP)

- An Internet service provider (ISP) is a company that provides customers with Internet access. Data may be transmitted using several technologies,
- Typically, ISPs also provide their customers with the ability to communicate with one another by providing Internet email accounts, usually with numerous email addresses at the customer's discretion. Other services, such as telephone and television services, may be provided as well. The services and service combinations may be unique to each ISP.
- An Internet service provider is also known as an Internet access provider (IAP).

Search Engine

- Search engine is a service that allows Internet users to search for content via the World Wide Web (WWW). A user enters keywords or key phrases into a search engine and receives a list of Web content results in the form of websites, images, videos or other online data.
- The list of content returned via a search engine to a user is known as a search engine results page

What is a Firewall?

- A firewall is a type of cybersecurity tool that is used to filter traffic on a network. Firewalls can be used to separate network nodes from external traffic sources, internal traffic sources, or even specific applications. Firewalls can be software, hardware, or cloud-based, with each type of firewall having its own unique pros and cons.
- The primary goal of a **firewall is to block malicious traffic requests and data packets** while allowing legitimate traffic through.

Software Firewalls

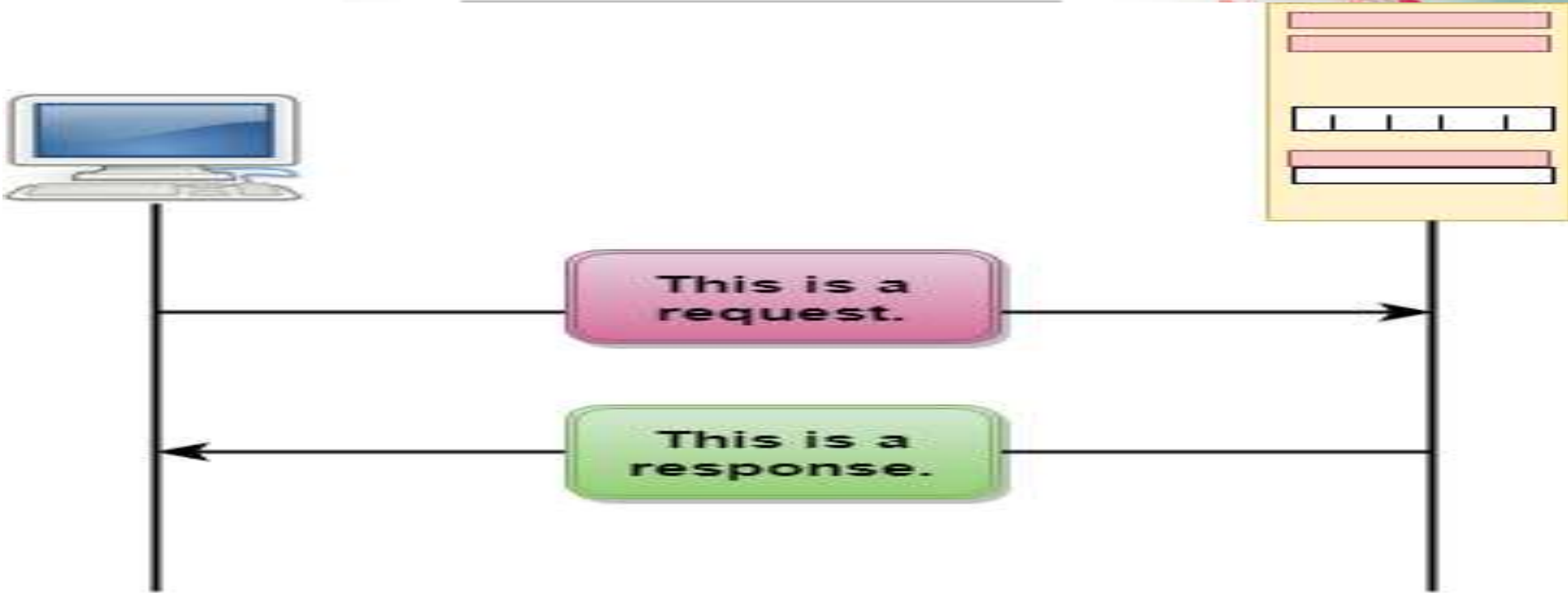
Software firewalls include any type of firewall that is installed on a local device rather than a separate piece of hardware (or a cloud server). The big benefit of a software firewall is that it's highly useful for creating defense in depth by isolating individual network endpoints from one another.

However, maintaining individual software firewalls on different devices can be difficult and time-consuming. Furthermore, not every device on a network may be compatible with a single software firewall, which may mean having to use several different software firewalls to cover every asset.

Hardware Firewalls

Hardware firewalls use a physical appliance that acts in a manner similar to a traffic router to intercept data packets and traffic requests before they're connected to the network's servers.

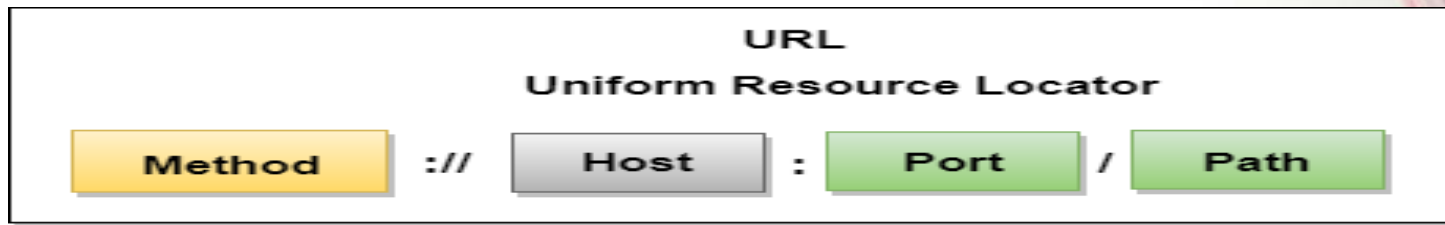
HTTP Transactions



The above figure shows the HTTP transaction between client and server. The client initiates a transaction by sending a request message to the server. The server replies to the request message by sending a response message.

Uniform Resource Locator (URL)

- A client that wants to access the document in an internet needs an address and to facilitate the access of documents, the HTTP uses the concept of Uniform Resource Locator (URL).
- The Uniform Resource Locator (URL) is a standard way of specifying any kind of information on the internet.
- The URL defines four parts: method, host computer, port, and path.



- **Method:** The method is the protocol used to retrieve the document from a server. For example, HTTP.
- **Host:** The host is the computer where the information is stored, and the computer is given an alias name. Web pages are mainly stored in the computers and the computers are given an alias name that begins with the characters "www". This field is not mandatory.
- **Port:** The URL can also contain the port number of the server, but it's 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.

Computer Network Security

- Computer network security consists of measures taken by business or some organizations to monitor and prevent unauthorized access from the outside attackers.
- Different approaches to computer network security management have different requirements depending on the size of the computer network. For example, a home office requires basic network security while large businesses require high maintenance to prevent the network from malicious attacks.
- Network Administrator controls access to the data and software on the network. A network administrator assigns the user ID and password to the authorized person.

What is Cryptography?

- Cryptography is used to secure and protect data during communication. It is helpful to prevent unauthorized person or group of users from accessing any confidential data. Encryption and decryption are the two essential functionalities of cryptography.
- A message sent over the network is transformed into an unrecognizable encrypted message known as data encryption. At the receiving end, the received message is converted to its original form known as decryption.

Encryption

- Encryption is a process which transforms the original information into an unrecognizable form. This new form of the message is entirely different from the original message. That's why a hacker is not able to read the data as senders use an encryption algorithm. Encryption is usually done using key algorithms.
- Data is encrypted to make it safe from stealing. However, many known companies also encrypt data to keep their trade secret from their competitors.



Decryption?

- Decryption is a process of converting encoded/encrypted data in a form that is readable and understood by a human or a computer. This method is performed by un-encrypting the text manually or by using keys used to encrypt the original data.



Decryption process

Secure Socket Layer (SSL)

- Secure Socket Layer (SSL) provide security to the data that is transferred between web browser and server. SSL encrypt the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

What Is a Blockchain?

A blockchain is a distributed database or ledger that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format. Blockchains are best known for their crucial role in cryptocurrency systems, such as [Bitcoin](#), for maintaining a secure and decentralized record of transactions. The innovation with a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party.

BLOCK 1

BLOCK 2

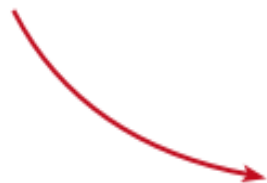
BLOCK 3



Hash: 6U9P2

Previous hash:

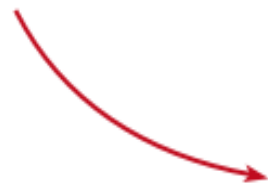
00000



Hash: 8Y5C9

Previous hash:

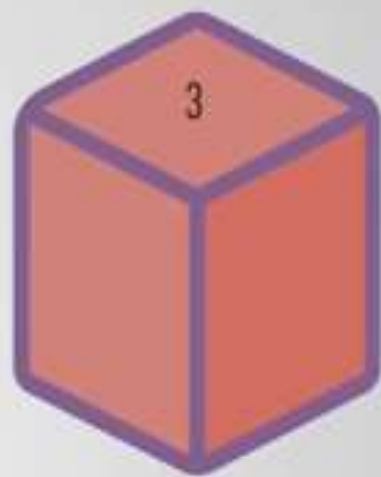
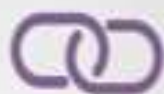
6U9P2



Hash: 9L4Z1

Previous hash:

8Y5C9



Hash: **1Z8F**

Previous hash: **0000**

Hash: **6BQ1**

Previous hash: **1Z8F**

Hash: **3H4Q**

Previous hash: **6BQ1**



Cloud Hosting

- The method of outsourcing an enterprise's processing and storage capabilities to a service provider that provides its networking services in a utility model is cloud hosting.
- The cloud vendor supervised the setup, cloud storage, protection and management, while customers will configure hardware and applications and scale servers online. Computing and storage services are dispersed in a cloud computing configuration through hundreds of virtual machines according to the load balance I / O demand.

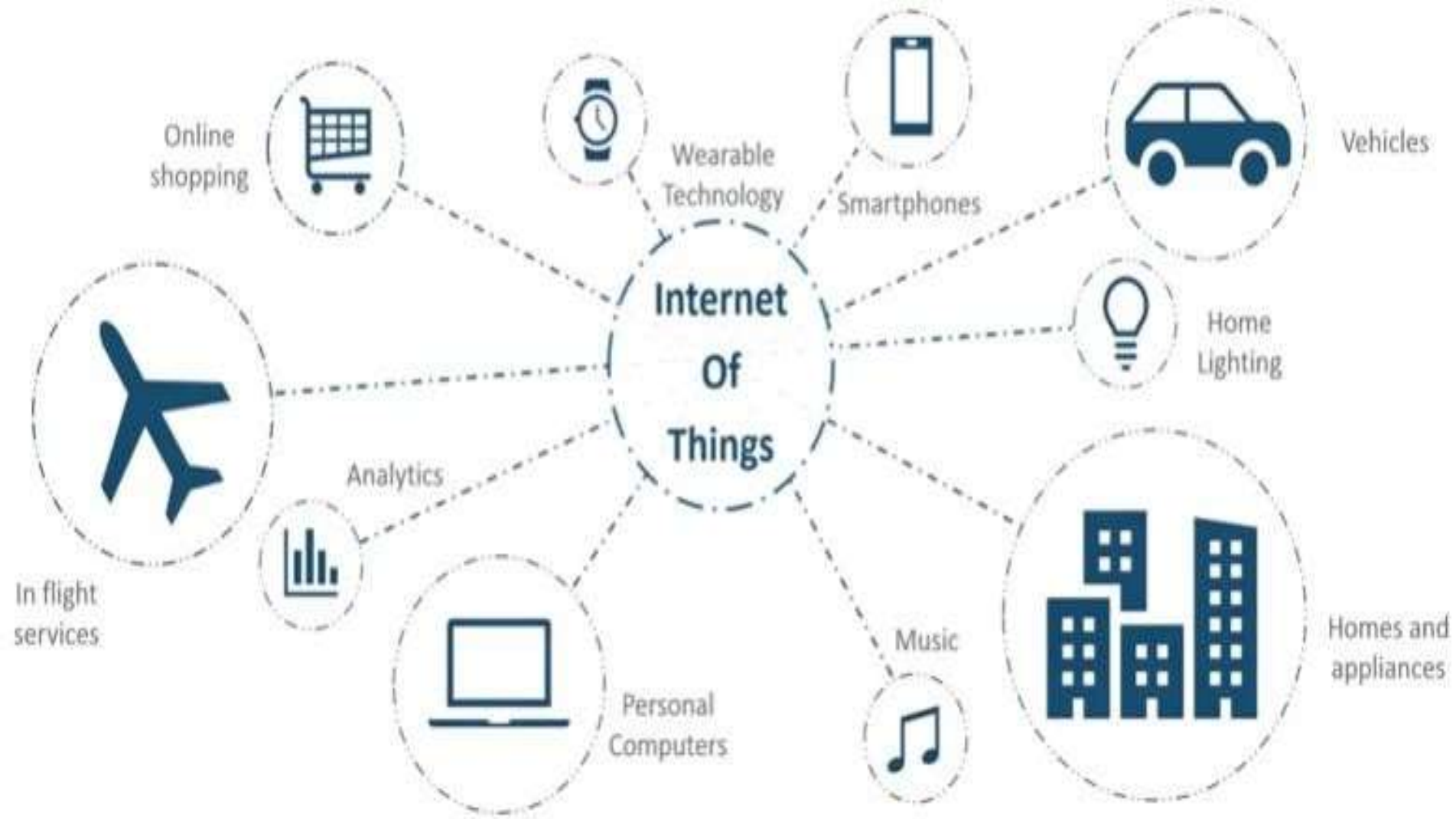
- Top vendors/providers
- As a technology model, cloud computing systems have fuelled a growth in the infrastructure under which a third-party vendor, usually with a pay-per-use system, provides a customer with the hardware, applications, servers, storage and networking facilities.
- [Amazon Web Services](#), the Google Cloud Portal, [IBM](#) Cloud and [Microsoft Azure](#) are common providers who offer cloud hosting. AWS, which provides comprehensive storage facilities and more areas and zones than most cloud vendors, is the leading competitor in the market. In recent years, Azure and Google have gained momentum.

What is the GPU?

- GPU stands for **Graphics Processing Unit**. GPUs are also known as video cards or graphics cards. In order to display pictures, videos, and 2D or 3D animations, each device uses a GPU. A GPU performs fast calculations of arithmetic and frees up the [CPU](#) to do different things. A GPU has lots of smaller cores made for multi-tasking, while a CPU makes use of some cores primarily based on sequential serial processing. In the world of computing, graphics processing technology has advanced to offer specific benefits. The modern GPUs enables new possibilities in **content creation, machine learning, gaming**, etc.

IoT (Internet of Things) Tutorial

- Let's us look closely at our mobile device which contains GPS Tracking, Mobile Gyroscope, Adaptive brightness, Voice detection, Face detection etc. These components have their own individual features, but what about if these all communicate with each other to provide a better environment? For example, the phone brightness is adjusted based on my GPS location or my direction.
- Connecting everyday things embedded with electronics, software, and sensors to internet enabling to collect and exchange data without human interaction called as the Internet of Things (IoT).
- The term "Things" in the Internet of Things refers to anything and everything in day to day life which is accessed or connected through the internet.



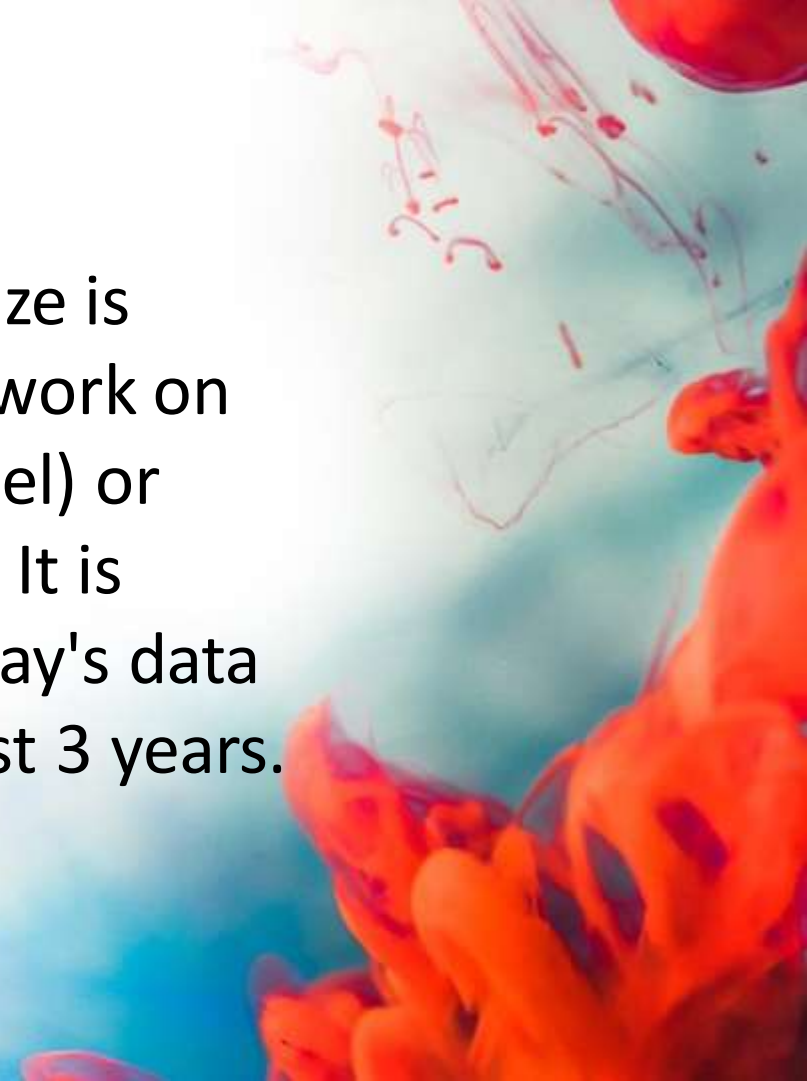
- IoT is an advanced automation and analytics system which deals with artificial intelligence, sensor, networking, electronic, cloud messaging etc. to deliver complete systems for the product or services. The system created by IoT has greater transparency, control, and performance.
- As we have a platform such as a cloud that contains all the data through which we connect all the things around us. For example, a house, where we can connect our home appliances such as air conditioner, light, etc. through each other and all these things are managed at the same platform. Since we have a platform, we can connect our car, track its fuel meter, speed level, and also track the location of the car.



- If there is a common platform where all these things can connect to each other would be great because based on my preference, I can set the room temperature. For example, if I love the room temperature to to be set at 25 or 26-degree Celsius when I reach back home from my office, then according to my car location, my AC would start before 10 minutes I arrive at home. This can be done through the Internet of Things (IoT).

What is Big Data

- Data which are very large in size is called Big Data. Normally we work on data of size MB(WordDoc ,Excel) or maximum GB(Movies, Codes) It is stated that almost 90% of today's data has been generated in the past 3 years.

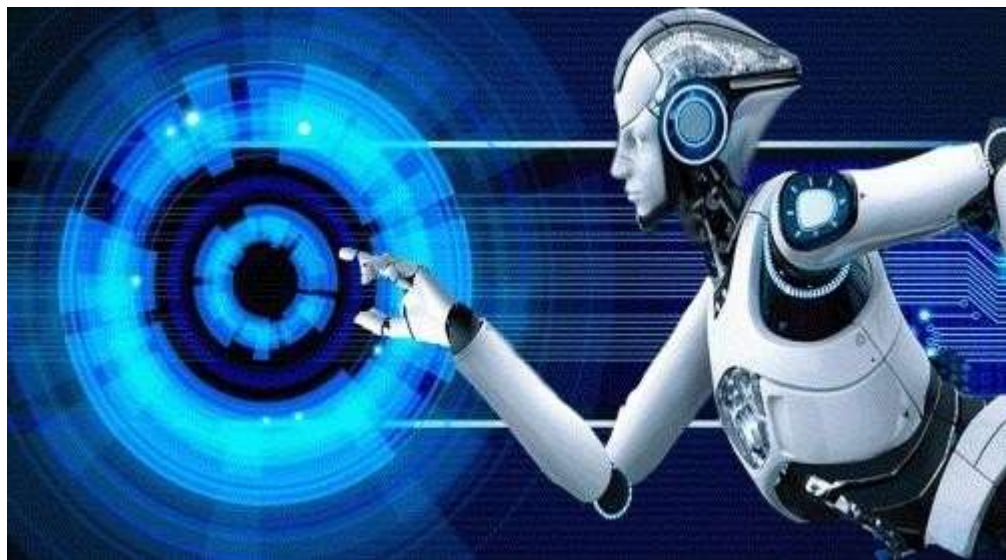


Sources of Big Data

- These data come from many sources like
- **Social networking sites:** Facebook, Google, LinkedIn all these sites generates huge amount of data on a day to day basis as they have billions of users worldwide.
- **E-commerce site:** Sites like Amazon, Flipkart, Alibaba generates huge amount of logs from which users buying trends can be traced.
- **Weather Station:** All the weather station and satellite gives very huge data which are stored and manipulated to forecast weather.
- **Telecom company:** Telecom giants like Airtel, Vodafone study the user trends and accordingly publish their plans and for this they store the data of its million users.
- **Share Market:** Stock exchange across the world generates huge amount of data through its daily transaction.

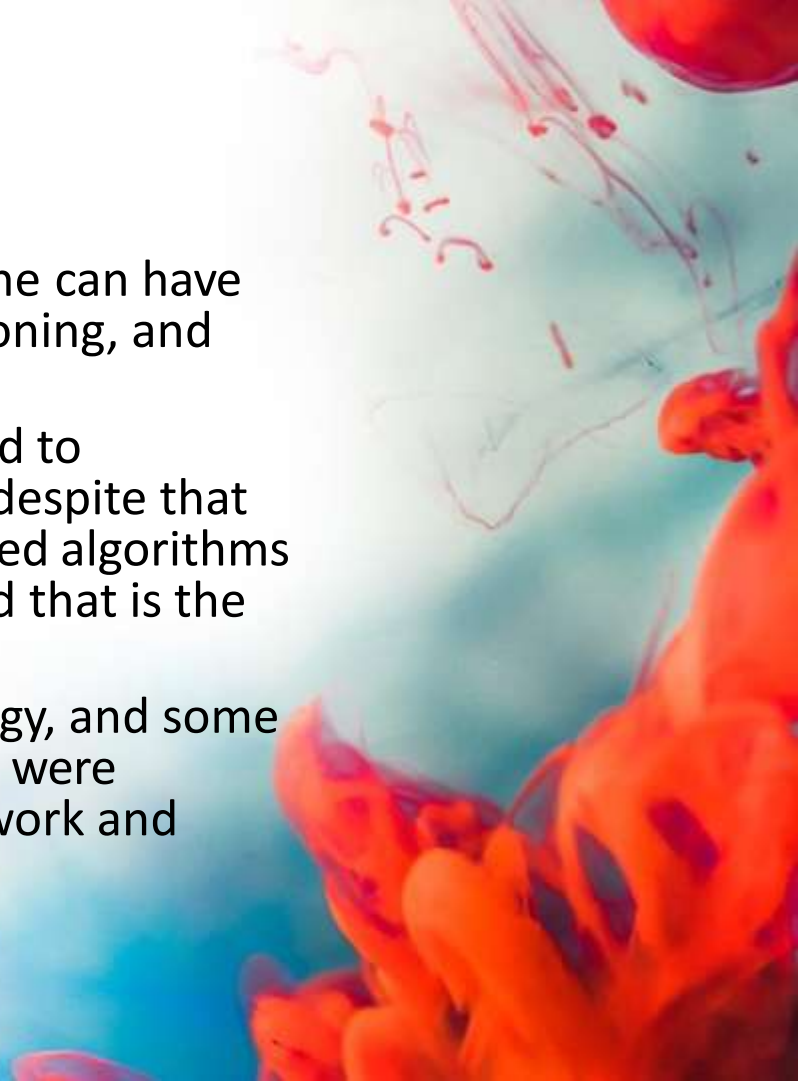
Artificial Intelligence

- In today's world, technology is growing very fast, and we are getting in touch with different new technologies day by day. Here, one of the booming technologies of computer science is Artificial Intelligence which is ready to create a new revolution in the world by making intelligent machines. The Artificial Intelligence is now all around us. It is currently working with a variety of subfields, ranging from general to specific, such as self-driving cars, playing chess, proving theorems, playing music, Painting, etc.
- AI is one of the fascinating and universal fields of Computer science which has a great scope in future. AI holds a tendency to cause a machine to work as a human.



- Artificial Intelligence is composed of two words **Artificial** and **Intelligence**, where Artificial defines "*man-made*," and intelligence defines "*thinking power*", hence AI means "*a man-made thinking power*."
- So, we can define AI as:
- **"It is a branch of computer science by which we can create intelligent machines which can behave like a human, think like humans, and able to make decisions."**

- Artificial Intelligence exists when a machine can have human based skills such as learning, reasoning, and solving problems
- With Artificial Intelligence you do not need to preprogram a machine to do some work, despite that you can create a machine with programmed algorithms which can work with own intelligence, and that is the awesomeness of AI.
- It is believed that AI is not a new technology, and some people says that as per Greek myth, there were Mechanical men in early days which can work and behave like humans.



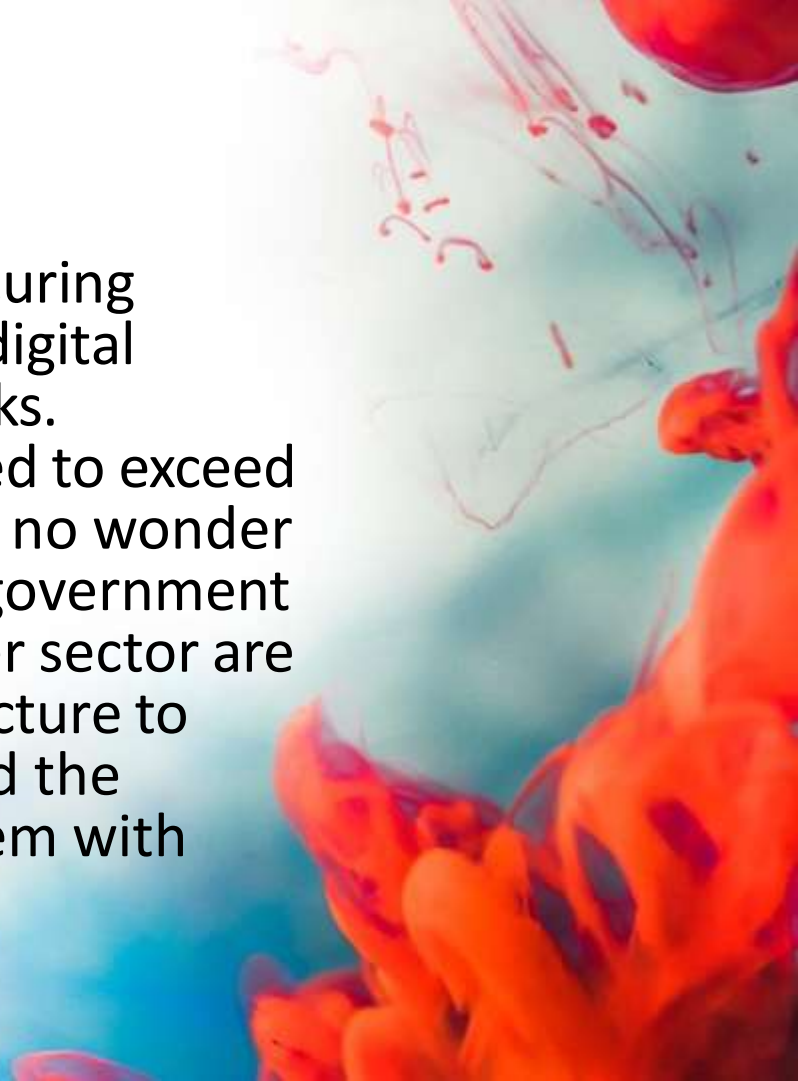
Automation

- Automation is the creation and application of technologies to produce and deliver goods and services with minimal human intervention. The implementation of automation technologies, techniques and processes improve the efficiency, reliability, and/or speed of many tasks that were previously performed by humans.
- Automation is being used in a number of areas such as manufacturing, transport, utilities, defense, facilities, operations and lately, information technology.



What Is Cybersecurity?

- Cybersecurity is the practice of securing networks, systems and any other digital infrastructure from malicious attacks. With [cybercrime damages](#) projected to exceed a staggering \$6 trillion by 2021, it's no wonder banks, tech companies, hospitals, government agencies and just about every other sector are investing in cybersecurity infrastructure to protect their business practices and the millions of customers that trust them with their data.



What is IMPS?

- Immediate Payment Service (IMPS) is a service provided by banks to ensure real-time interbank funds transfer. Unlike NEFT, funds can be transferred on any day of the week including holidays and weekends using IMPS.
- IMPS aims to make electronic funds transfer easy and convenient for customers and to support the RBI's goal of electronification of retail payments. IMPS has built the foundation for a full range of mobile banking services.
- **Transaction Limits**
- Generally, the transaction limit for IMPS transfer is set to be Rs.2 lakh.

Real-Time Gross Settlement (RTGS)

- Real-time gross settlement (RTGS) was launched in the year 2004 by the Reserve Bank of India. It is a system that performs continuous real-time fund transfers. Here, 'real-time' means that the instructions are processed at the very moment when they are received rather than any sort of delay. Similarly, gross settlement means the fund transfer instructions will be handled on an instruction by instruction basis.
- This money transfer technique is primarily meant for large value transactions. The Reserve Bank of India has waived off charges for RTGS transactions only to boost the popularity among the citizens. The apex bank has asked the commercial banks to pass on the benefits to customers. About 1,40,000 bank branches are RTGS-enabled in the country.
- **Visit the nearest bank branch and fill the RTGS form to initiate a fund transfer.**

UPI: Unified Payments Interface – Instant mobile payments

- UPI is a single platform that merges various banking services and features under one umbrella. A UPI ID and PIN are sufficient to send and receive money. Real-time bank-to-bank payments can be made using a mobile number or virtual payment address (UPI ID). Online payments are simplified.
- Pay for your hailing services, food delivery services, and shopping sites with UPI payments for instant fund transfer.
- Pay at the nearest restaurants, grocery stores, and departmental stores online.
- Rent, mobile recharge, and utility bill payments can be done online instantly.

What is NEFT?

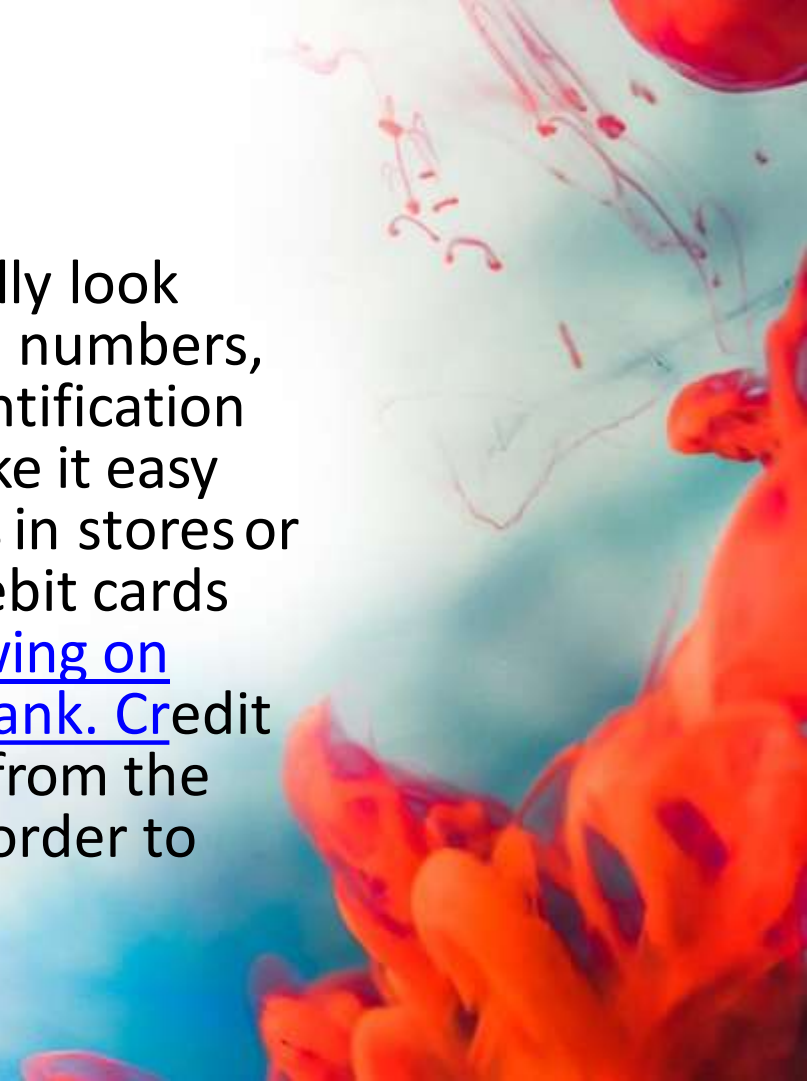
- National Electronic Funds Transfer (NEFT) is a mode of online funds transfer that is introduced by the Reserve Bank of India (RBI). It quickly transfers money between banks throughout India. A bank branch must be NEFT-enabled for a customer to be able to transfer the funds to another party.
- **What are the permitted timings to make an NEFT transaction?**
- Earlier, the NEFT clearance would take place subject to specified slots:
- Monday-Friday: 8 a.m. to 7 p.m.
- Saturday: 8 a.m. to 12 p.m.
- You can initiate an NEFT fund transfer starting from Re.1. On the other hand, RBI has not set any maximum limit for the same. When it comes to cash transactions, you can transfer up to Rs.50,000 per transaction. Also, there is no limit on the total amount you can transfer. Few banks have set their own upper limit, such as HDFC Bank has set the upper limit of Rs.25 lakh per day per customer ID via online NEFT.

Transfer Amount (in ₹)	Transaction Charges (in ₹)
10,000-1 lakh	5 + GST
1 lakh-2 lakh	15 + GST
Above 2 lakh	25 + GST



Credit cards

- Credit cards and debit cards typically look almost identical, with 16-digit card numbers, expiration dates, and personal identification number (PIN) codes. Both can make it easy and convenient to make purchases in stores or online, with one key difference. Debit cards allow you to spend money by drawing on funds you have deposited at the bank. Credit cards allow you to borrow money from the card issuer up to a certain limit in order to purchase items or withdraw cash.



What Is a Debit Card?

- A debit card is a payment card that makes payments by deducting money directly from a consumer's checking account, rather than on loan from a bank. Debit cards offer the convenience of credit cards and many of the same consumer protections when issued by major payment processors like Visa or Mastercard.



E-wallets

- E-wallet is a type of electronic card which is used for transactions made online through a computer or a smartphone. Its utility is same as a credit or debit card. An E-wallet needs to be linked with the individual's bank account to make payments.

Descriptions: E-wallet is a type of pre-paid account in which a user can store his/her money for any future online transaction. An E-wallet is protected with a password. With the help of an E-wallet, one can make payments for groceries, online purchases, and flight tickets, among others.

E-wallet has mainly two components, software and information. The software component stores personal information and provides security and encryption of the data. The information component is a database of details provided by the user which includes their name, shipping address, payment method, amount to be paid, credit or debit card details, etc.

What is DigiLocker

- Available both on websites and mobile apps, DigiLocker is nothing but a digital locker to store all your documents. Linked to both Aadhaar card and cellphone numbers, DigiLocker eliminates the use of physical documents as part of the government's Digital India drive, since all data is stored in the cloud.
- You can upload scanned copies of your documents (PDF, JPEG or PNG format) and access it anywhere you want. You can also e-sign these uploaded documents, which works like self-attestation of physical documents.

UMANG App

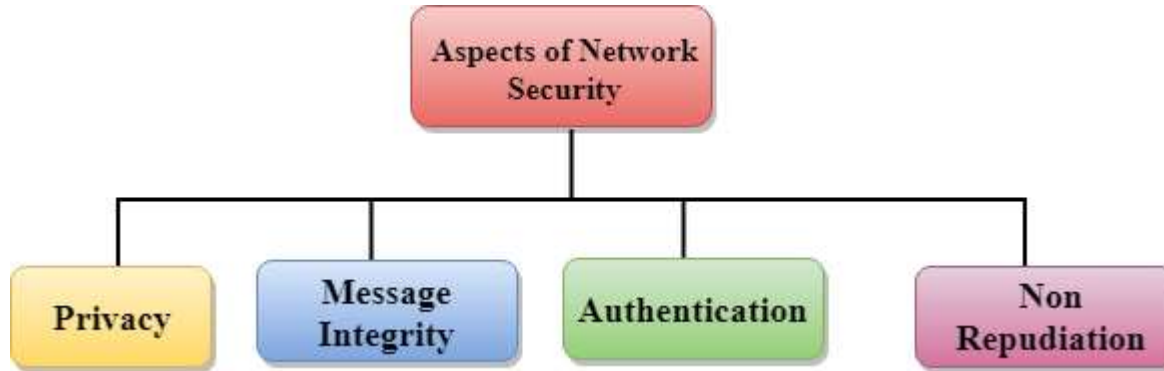
- The Umang Application offers the following benefits to its users-
- You can avail over 150 different services offered by the central and state governments easily
- Simple categorisation of services as Recently Viewed, New and Updated, Trending, Top Rated and Suggested has been made to enhance the app interface
- You can easily search for a specific State or Central Government service using the in-app filter
- The application is available in 12 regional languages such as Hindi, Marathi, Tamil, Assamese, Gujarati, Bengali, Kannada, Odia, Punjabi, Malayalam, Marathi, Telugu and Urdu, apart from English
- You can even make easy online payment of various utility bills such as gas, water, electricity, etc.
- The application also offers key integration services including Digilocker and Aadhaar

Computer Network Security

- Computer network security consists of measures taken by business or some organizations to monitor and prevent unauthorized access from the outside attackers.
- Different approaches to computer network security management have different requirements depending on the size of the computer network. For example, a home office requires basic network security while large businesses require high maintenance to prevent the network from malicious attacks.
- Network Administrator controls access to the data and software on the network. A network administrator assigns the user ID and password to the authorized person.

Aspects of Network Security:

Following are the desirable properties to achieve secure communication:

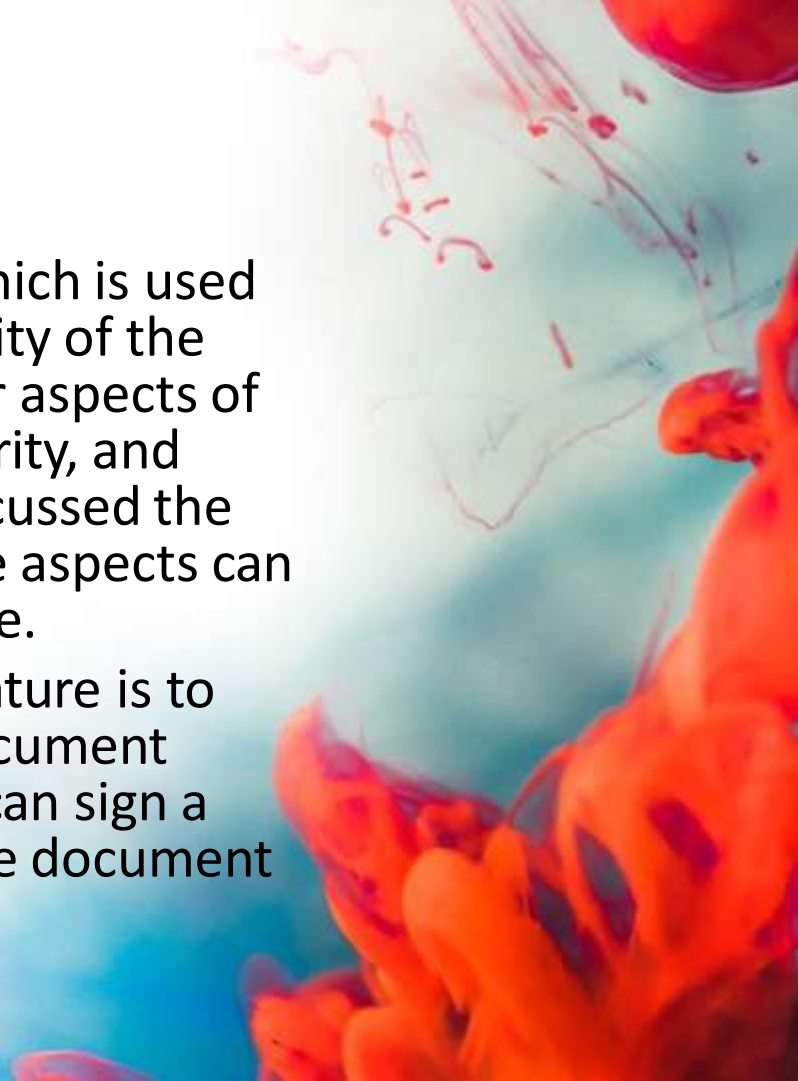


- **Privacy:** Privacy means both the sender and the receiver expects confidentiality. The transmitted message should be sent only to the intended receiver while the message should be opaque for other users. Only the sender and receiver should be able to understand the transmitted message as eavesdroppers can intercept the message. Therefore, there is a requirement to encrypt the message so that the message cannot be intercepted. This aspect of confidentiality is commonly used to achieve secure communication.
- **Message Integrity:** Data integrity means that the data must arrive at the receiver exactly as it was sent. There must be no changes in the data content during transmission, either maliciously or accident, in a transit. As there are more and more monetary exchanges over the internet, data integrity is more crucial. The data integrity must be preserved for secure communication.

- **End-point authentication:** Authentication means that the receiver is sure of the sender's identity, i.e., no imposter has sent the message.
- **Non-Repudiation:** Non-Repudiation means that the receiver must be able to prove that the received message has come from a specific sender. The sender must not deny sending a message that he or she send. The burden of proving the identity comes on the receiver. For example, if a customer sends a request to transfer the money from one account to another account, then the bank must have a proof that the customer has requested for the transaction.

Digital Signature

- The Digital Signature is a technique which is used to validate the authenticity and integrity of the message. We know that there are four aspects of security: privacy, authentication, integrity, and non-repudiation. We have already discussed the first aspect of security and other three aspects can be achieved by using a digital signature.
- The basic idea behind the Digital Signature is to sign a document. When we send a document electronically, we can also sign it. We can sign a document in two ways: to sign a whole document and to sign a digest.



- The term HTTP stands for?
 - Hyper terminal tracing program
 - Hypertext tracing protocol
 - Hypertext transfer protocol
 - Hypertext transfer program



- A proxy server is used as the computer?
 - with external access
 - acting as a backup
 - performing file handling
 - accessing user permissions



- Which one of the following is a valid email address?
 - javat@point.com
 - gmail.com
 - tpoint@.com
 - javatpoint@books

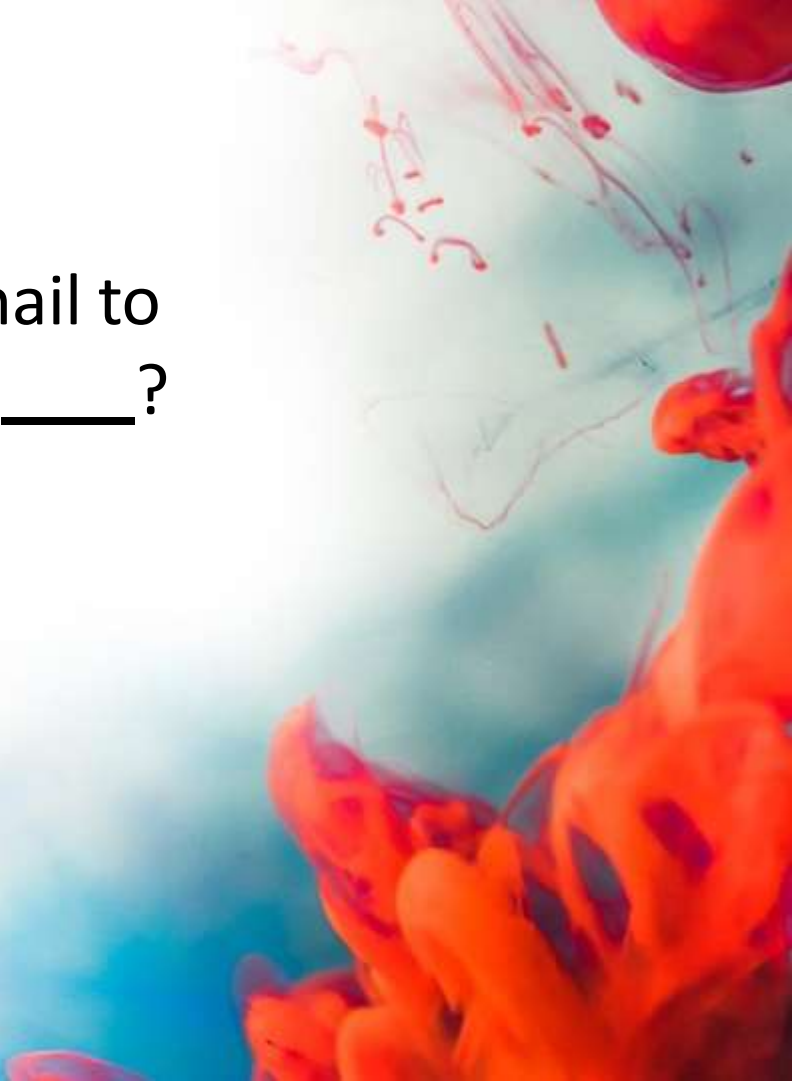
- The term FTP stands for?
 - File transfer program
 - File transmission protocol
 - File transfer protocol
 - File transfer protection



- Which one of the following is not a network topology?
 - Star
 - Ring
 - Bus
 - Peer to Peer



- When the mail server sends mail to other mail servers it becomes ____?
 - SMTP client
 - SMTP server
 - Peer
 - Master



- The length of an IPv6 address is?
 - 32 bits
 - 64 bits
 - 128 bits
 - 256 bits



- The term WAN stands for?
 - Wide Area Net
 - Wide Access Network
 - Wide Area Network
 - Wide Access Net



- Which layer of the TCP / IP stack corresponds to the OSI model transport layer?
 - Host to host
 - Application
 - Internet
 - Network Access



- The term IPv4 stands for?
 - Internet Protocol Version 4
 - Internet Programming Version 4
 - International Programming Version 4
 - None of these



- The term LAN stands for?
 - Local Area Net
 - Local Aera Network
 - Local Array Network
 - Local Array Net



- Which of the through is share the data of two computer?
 - Library
 - Network
 - Grouping
 - Integrated system



- 1) A process is a_____.
 - single thread of execution.
 - program in the execution
 - program in the memory
 - task



- What is the decimal equivalent of the binary number 10111?
 - 21
 - 39
 - 42
 - 23



- Which of the following is the smallest visual element on a video monitor?
 - Character
 - Pixel
 - Byte
 - Bit



- Which of the following is an output device?
 - Keyboard
 - Mouse
 - Light pen
 - VDU



- Which of the following is an input device?
 - Plotter
 - Printer
 - VDU
 - Mouse



- BIOS is used?
 - By operating system
 - By compiler
 - By interpreter
 - By application software



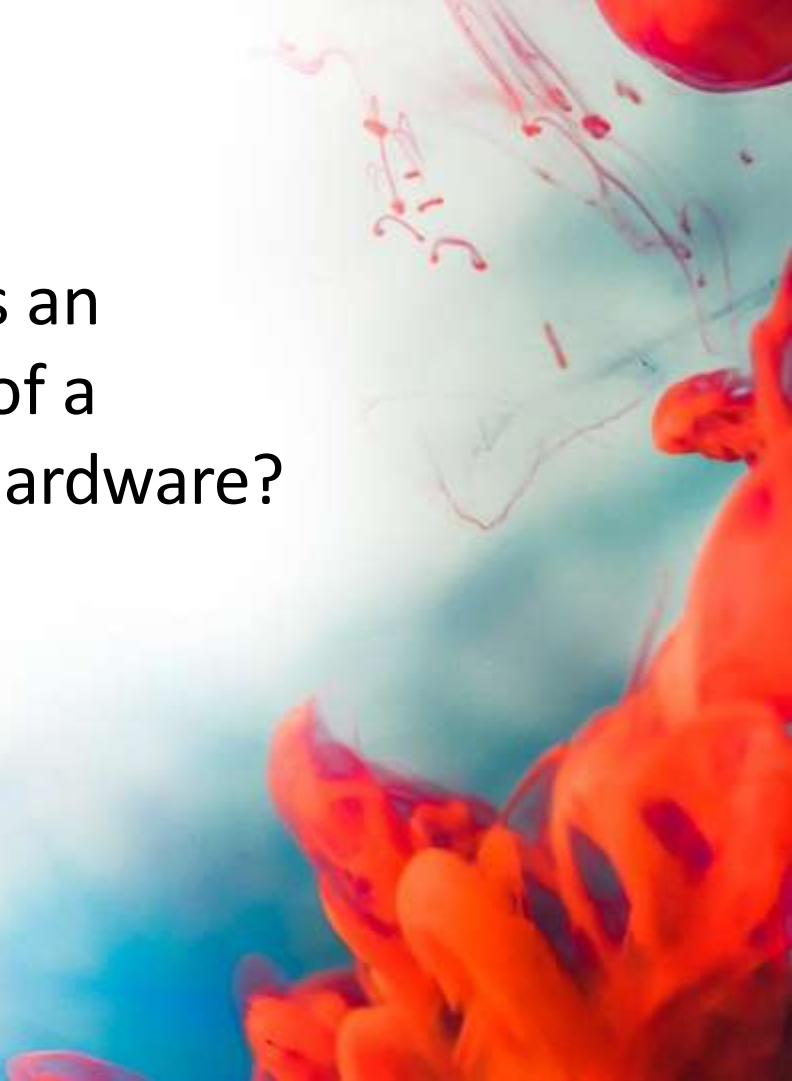
- What is the mean of the Booting in the system?
 - Restarting computer
 - Install the program
 - To scan
 - To turn off



- The central processing unit is located in the _____.
 - Hard disk
 - System unit
 - Memory unit
 - Monitor



- Which type of program acts as an intermediary between a user of a computer and the computer hardware?
 - Operating system
 - User thread
 - Superuser thread
 - Application program



- What kind of language can computer understand?
 - Normal language
 - Computer language
 - Assembly language
 - High-level language



- What is the speed of computer measured in?
 - Nanoseconds
 - Kilo-seconds
 - Gigahertz
 - Megabytes



- What is the full form of RAM?
 - Remote Access Memory
 - Random Access Memory
 - Remote Access Memory
 - Random Access Memory



- What is the full form of DRAM?
 - Dynamic Remote Access Memory
 - Dynamic Random-Access Memory
 - Dependent Remote Access Memory
 - Dependent Random-Access Memory

- Which of the following is not considered hardware?
 - Operating system
 - CPU
 - Keyboard
 - Hard disk



- Which of the following is exclusively a sequential access storage device?
 - Hard disk
 - Floppy disk
 - Magnetic tape
 - DVD



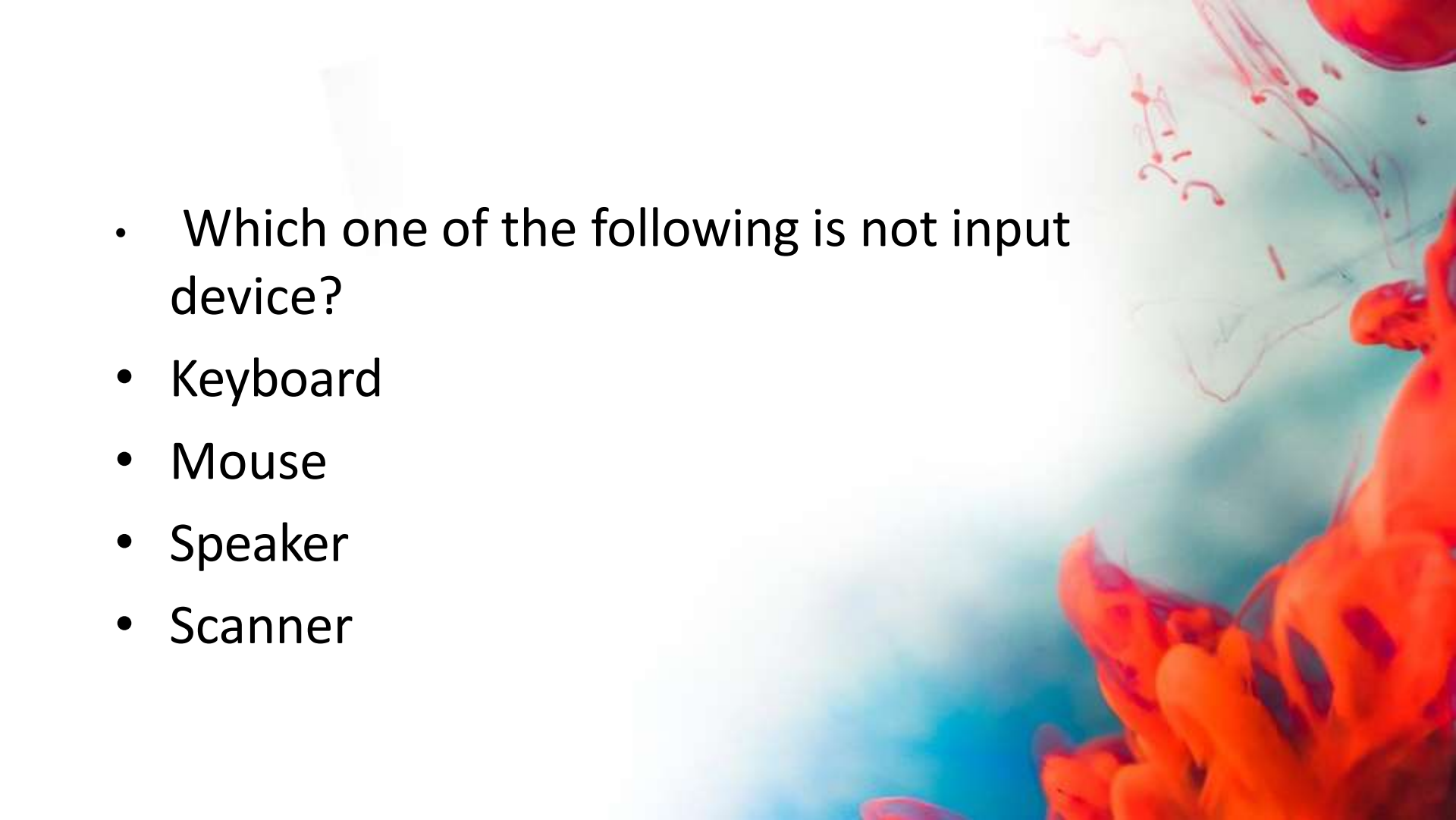
- What is the full form of USB?
 - Unshielded System Board
 - Universal System Board
 - Unidentified System Bus
 - Universal System Bus



- Which one of the following is not a form of data storage media?
 - A database
 - Magnetic tape
 - Magnetic disc
 - Optical disc



- What is five main components of a computer system?
 - CPU, CD-ROM, Mouse, Keyboard, Sound card
 - Memory, Video card, Monitor, Software, Hardware
 - Modem, Keyboard, Word Processor, Printer, Screen
 - CPU, Memory, System bus, Input, Output

- 
- Which one of the following is not input device?
 - Keyboard
 - Mouse
 - Speaker
 - Scanner

- Which one of the following is an example of the browser software?
- Microsoft Word
- Notepad
- Internet navigator
- Internet explorer



