Unit 1: Introduction to computer network

Content

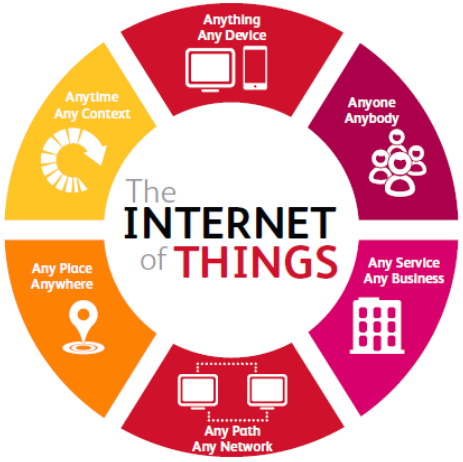
1.1 Communicating in a network centric world
1.2 Network as a platform
1.3 Architecture of internet
1.4 Classification of networks
1.5 Components of a network
1.6 Network topology and transmission
1.7 Layered models

Communicating in a network centric world

- Networks in Our Daily Lives
- Technology Then and Now
- The Global Community
- Networks Support the Way We Learn
- Networks Support the Way We Communicate
- Networks Support the Way We Work
- Networks Support the Way We Play

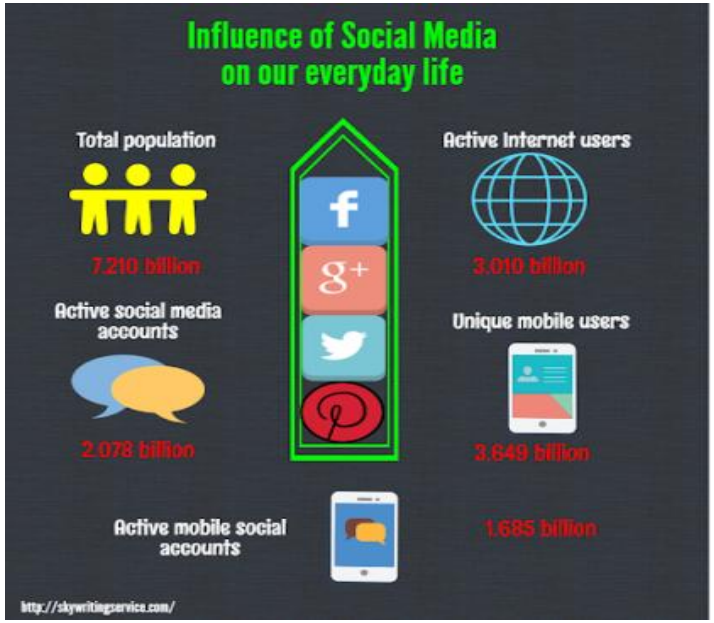
Networks in Our Daily Lives

- Communication is almost as important to us as our reliance on air, water, food, and shelter.
- The methods that we use to communicate are constantly changing and evolving. Whereas we were once limited to face-to-face interactions, breakthroughs in technology have significantly extended the reach of our communications.



Networks in Our Daily Lives

- Networks connect people and promote unregulated communication.
- The Internet is the largest network in existence. In fact, the term *Internet* means a network of networks. It is actually a collection of interconnected private and public networks.



Technology Then and Now

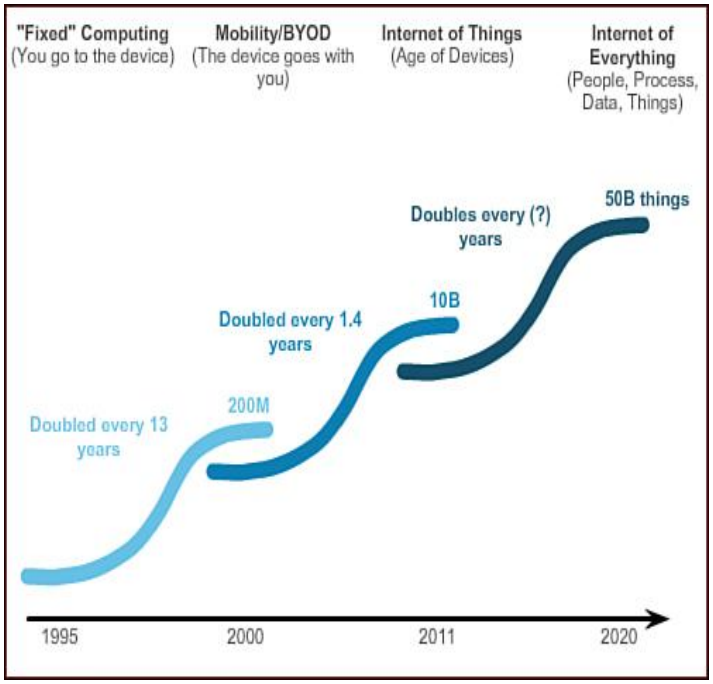
- Imagine a world without the Internet.
  - No more Google, YouTube, instant messaging, Facebook, Wikipedia, online gaming, Netflix, shopping online, or quickly looking up phone numbers and map directions to various locations at the click of a finger.
  - How different would our lives be without all of this?
  - Time would go back to the 80's!

Technology Then and Now

- A whole new world with the Internet!
  - Innovators are figuring out new ways to use the Internet more every day.
  - Consider the changes that have happened within the last couple of decades.

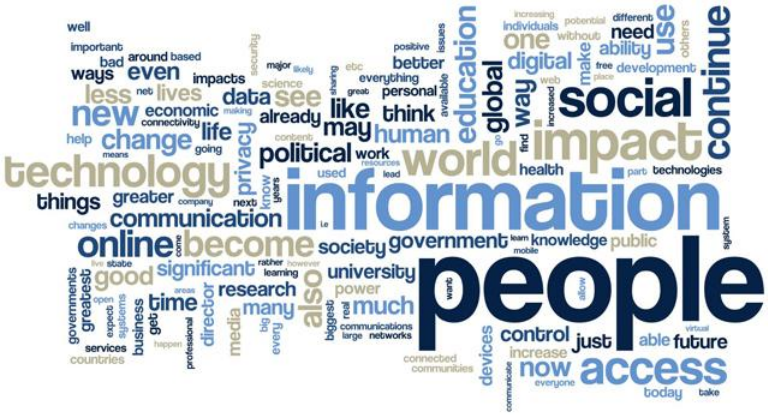
Technology Then and Now

- A whole new world with the Internet!
  - Now consider what changes will happen within the next decade.
  - What else do you think we will be able to do using the network as the platform?



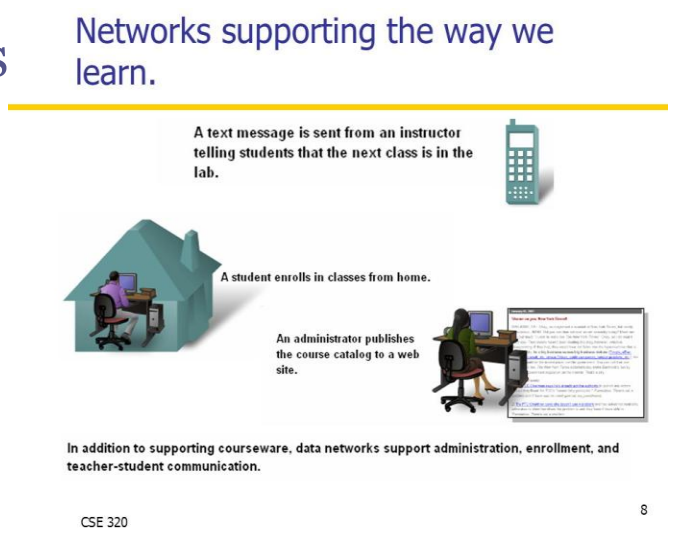
The Global Community

- The human network
  - The internet has changed the manner in which social, commercial, political, and personal interactions occur.
  - The Internet encourages the creation of global communities.
  - Global communities allow for social interaction that is independent of location or time zone.
  - We refer to this as the *human network*.



Networks Support the Way We Learn

- Changing the way we learn.
  - Robust and reliable networks support and enrich student learning experiences. They deliver learning material in a wide range of formats, including interactive activities, assessments, and feedback. Networks now
    - Support the creation of virtual classrooms
    - Provide on-demand video
    - Enable collaborative learning spaces
    - Enable mobile learning



Networks Support the Way We Communicate

- Changing the Way We Communicate
  - The globalization of the Internet has ushered in new forms of communication that empower individuals to create information that can be accessed by a global audience.
  - Some forms of communications include:
    - Instant messaging (IM) and texting
    - Social media
    - Collaboration tools
    - Weblogs (blogs)
    - Wikis
    - Podcasting
    - Peer-to-peer (P2P) file sharing

Networks Support the Way We Work

- Changing the Way We Work
  - Data networks were initially used by business world.
  - These business networks evolved to enable the transmission of many different types of information services, including email, video, messaging, and telephony.

Networks Support the Way We play

- Changing the Way We Play
  - The widespread adoption of the Internet by travel industries enhances the ability to enjoy and share many forms of recreation.
  - In addition, the Internet is used for traditional forms of entertainment. Live sporting events and concerts can be experienced as they are happening, or recorded and viewed on demand.
  - Networks enable the creation of new forms of entertainment, such as online games.

Network as a platform

- The Converging Network:
  - The network has become a platform for distributing a wide range of services to end users in a reliable, efficient, and secure manner.
  - Advances in technology are enabling us to consolidate these different kinds of networks onto one platform, referred to as the ***converged network***.
  - Unlike dedicated networks, converged networks are capable of delivering voice, video streams, text, and graphics among many different types of devices over the same communication channel and network structure.

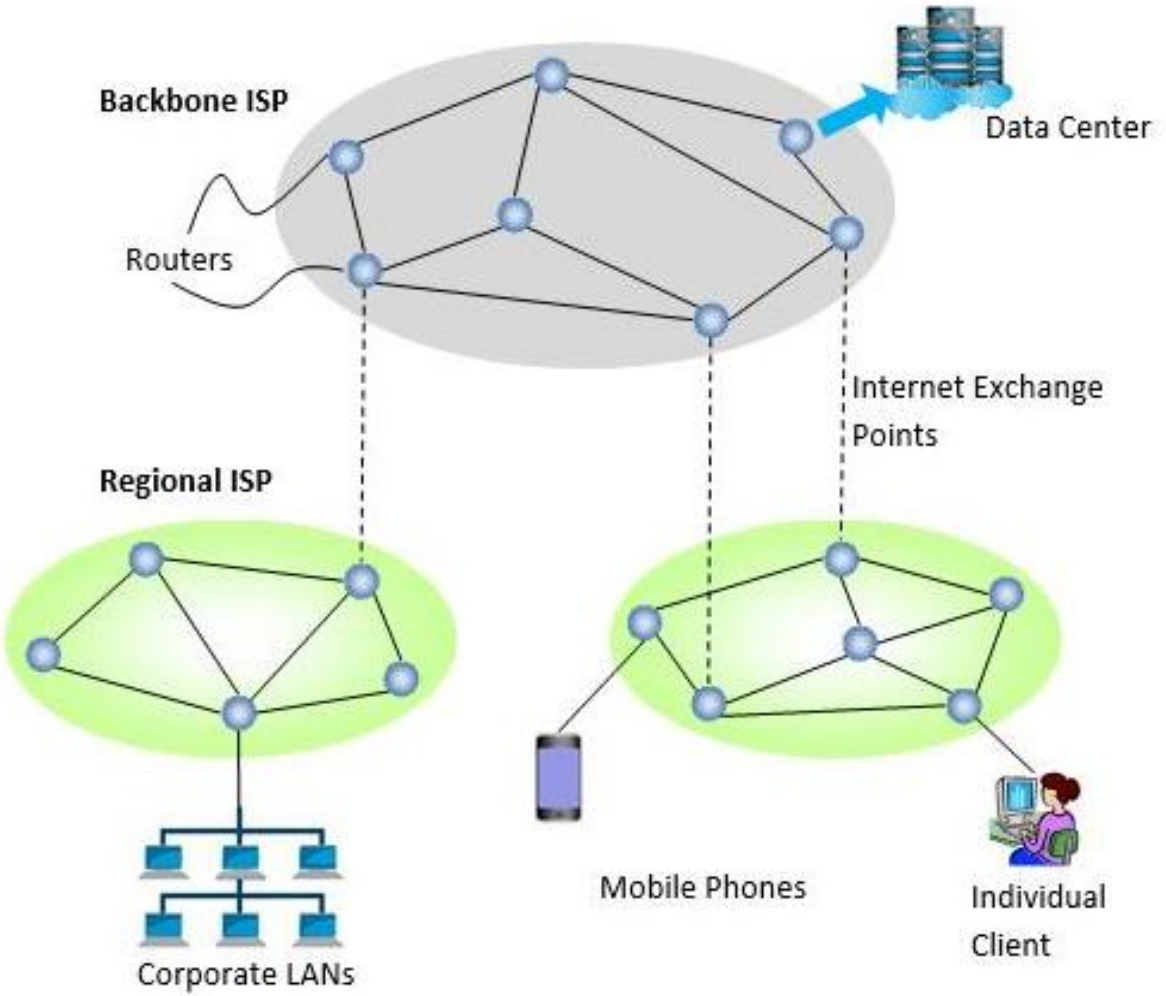
Network as a platform

- Previously separate and distinct communication forms have converged onto a common platform.
- In a converged network, there are still many points of contact and many specialized devices, such as personal computers, phones, TVs, and tablet computers, but there is one common network infrastructure.
- This network infrastructure uses the same set of rules, agreements, and implementation standards.

Architecture of internet

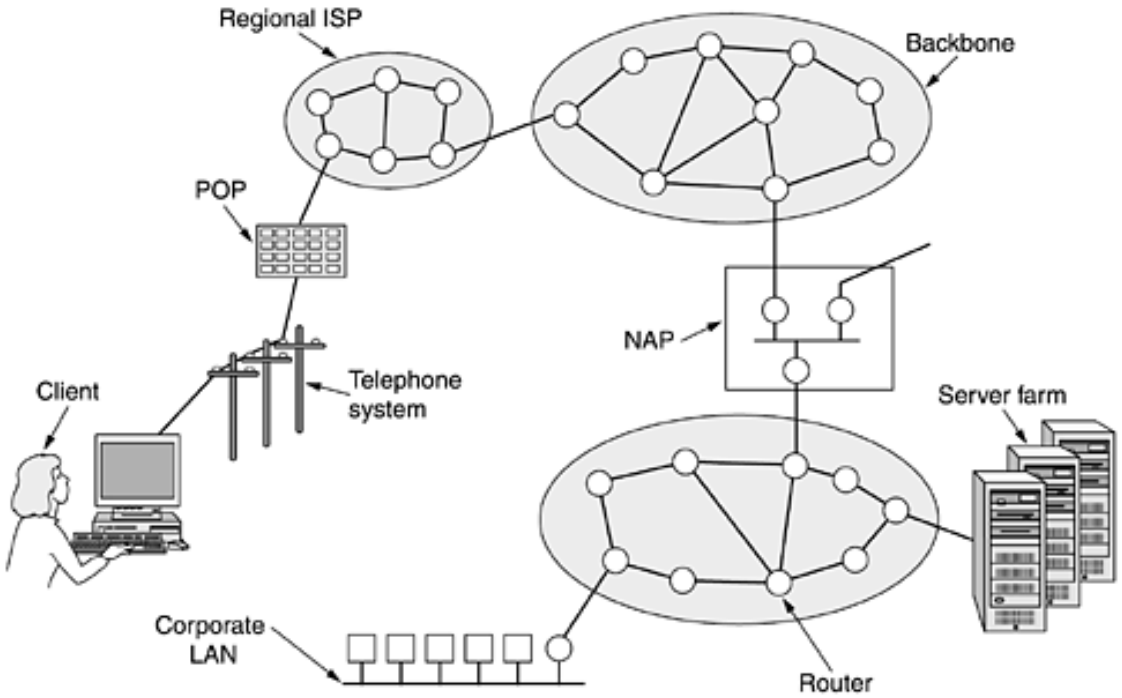
- The architecture of the Internet is ever-changing due to continuous changes in the technologies as well as the nature of the service provided.
- The heterogeneity and vastness of the Internet make it difficult to describe every aspect of its architecture.
- The overall architecture can be described in three levels –
  - Backbone ISP (Internet Service Provider)
  - Regional ISPs
  - Clients

- The following diagram shows the three levels –



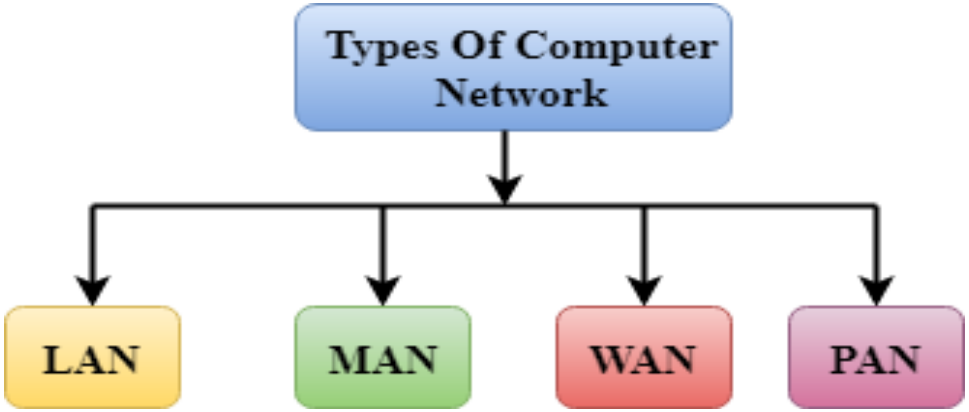
- Backbone ISP (Internet Service Provider) – Backbone ISPs are large international backbone networks. They are equipped with thousands of routers and store enormous amounts of information in data centers, connected through high bandwidth fiber optic links.
- Everyone needs to connect with a backbone ISP to access the entire Internet.
- There are different ways through which a client can connect to the ISP. A commonly used way is DSL (Digital Subscriber Line) which reuses the telephone connection of the user for transmission of digital data.
- The user uses a dial-up connection instead of the telephone call.

- For high-speed Internet access, the connectivity can be done through FTTH (Fiber to the Home), that uses optical fibers for transmitting data.
- Nowadays, most Internet access is done through the wireless connection to mobile phones from fixed subscribers, who transmit data within their coverage area.



Classification of networks

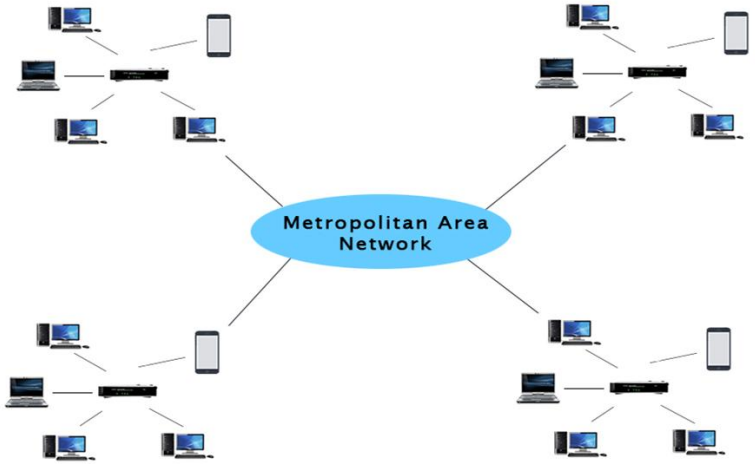
- The network can be classified in following manner:
- There are many different network protocols, each has its own characteristics and application domain.
  - Personal area network (PAN)
  - Local area network (LAN)
  - Metropolitan area network (MAN)
  - Wide area network (WAN)



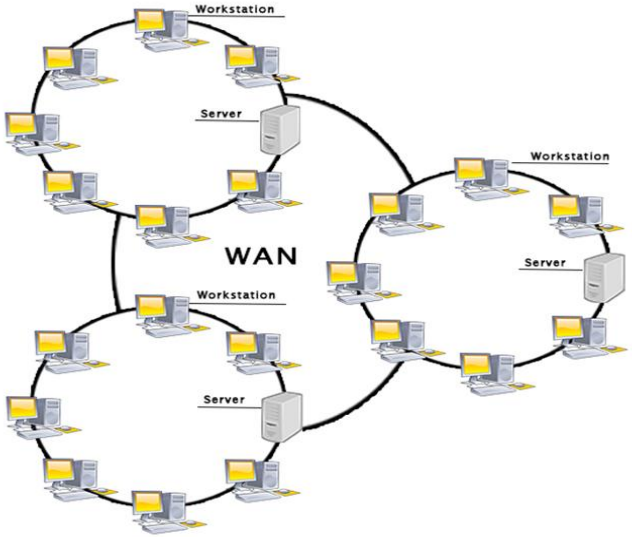
- Personal area network (PAN):
  - The PAN provides interconnection of devices within the range of an individual person, typically within a range of 10 meters.
  - Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
    - Example of wired PAN: Infrared, Bluetooth etc
    - Examples of wireless PAN: Cell phone headsets, wireless keyboards, wireless mice, printers, bar code scanners etc

- Local area network (LAN):
  - 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.
    - Example: Networking in the home, school, library, laboratory, college/ university campus, or office.

- Metropolitan area network (MAN):
  - A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
  - MAN or Metropolitan area Network covers a larger area than that of a LAN and smaller area as compared to WAN.
  - Uses Of Metropolitan Area Network:
    - MAN is used in communication between the banks in a city.
    - It can be used in a college within a city.



- Wide area network (WAN):
  - A Wide Area Network is a network that extends over a large geographical area such as states or countries.
  - A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fiber 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.



Components of a network

- Computer network components are the major parts which are needed to install the software.
- Computer networks components comprise both physical parts as well as the software required for installing computer networks.
- Some important network components are:
  - NIC
  - Hub
  - Switch
  - Router
  - Modem
  - Cable

- Network interface card (NIC):
  - Each system or computer in a computer network must have a card called network interface card (NIC).
  - The main purpose of NIC is to format the data, send the data and receive the data at the receiving node.

- 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.
  - 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.

- Router:
  - When we talk about computer network components, the other device that used to connect a LAN with an internet connection is called Router.
  - When you have two distinct networks (LANs) or want to share a single internet connection to multiple computers, we use a Router.
  - There are two types of Router: wired and wireless. The choice depends on your physical office/home setting, speed and cost.

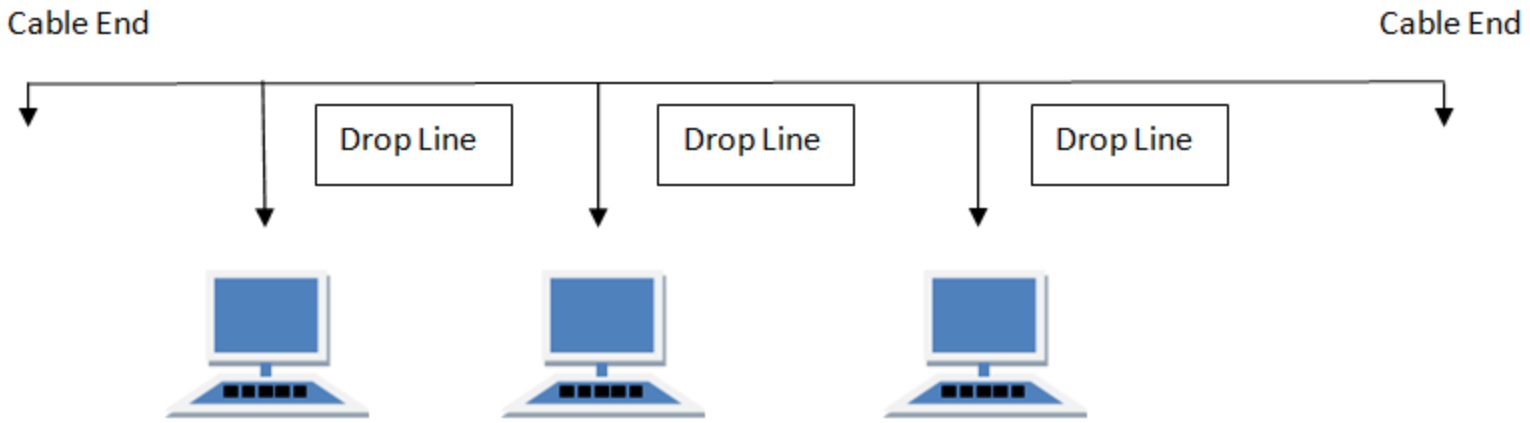
- Modem:
  - A modem is a hardware device that allows the computer to connect to the internet over the existing telephone line.
  - A modem is not integrated with the motherboard rather than it is installed on the PCI slot found on the motherboard.
  - It stands for Modulator/Demodulator. It converts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

- LAN Cable:
  - A local area Network cable is also known as data cable or Ethernet cable which is a wired cable used to connect a device to the internet or to other devices like computer, printers, etc.

Network topology and transmission

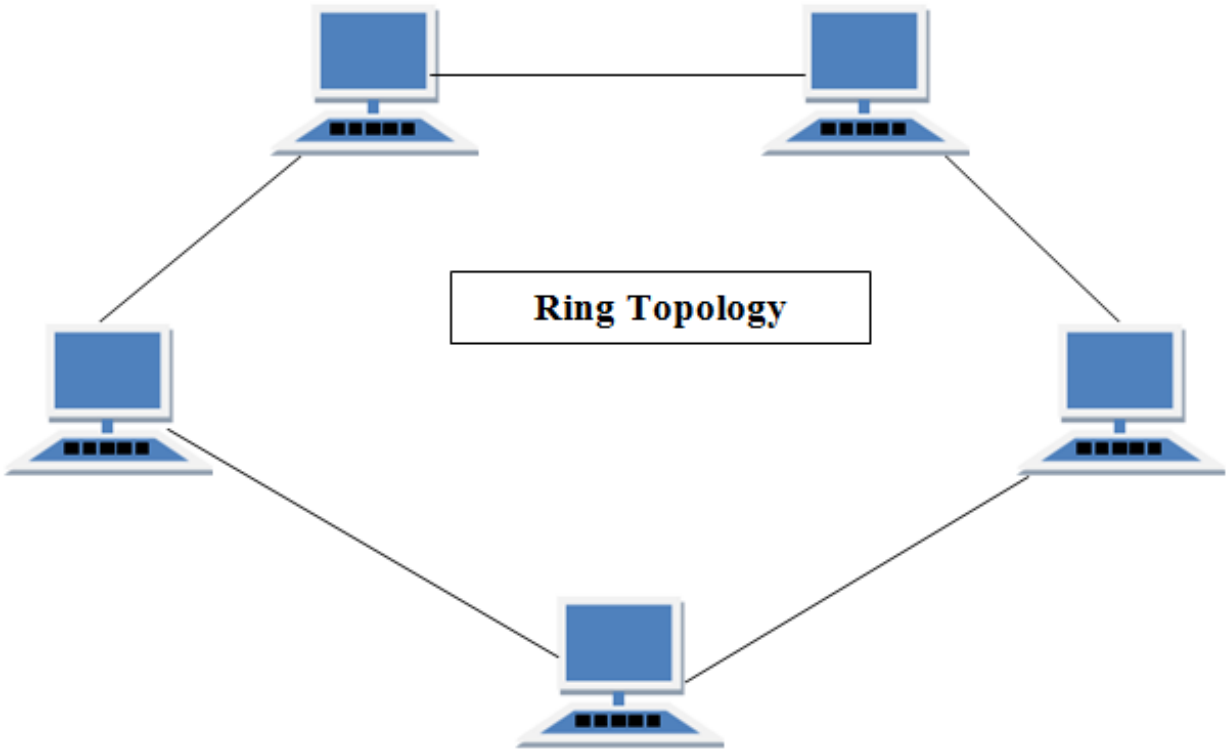
- Geometric representation of how the computers are connected to each other is known as topology.
- Topologies may define both physical and logical aspect of the network.
- There are six types of topologies–
- Bus
- Ring
- Mesh
- Star
- Tree
- Hybrid

- Bus Topology:
  - In bus topology there is a main cable and all the devices are connected to this main cable through drop lines.
  - There is a device called tap that connects the drop line to the main cable.
  - Since all the data is transmitted over the main cable, there is a limit of drop lines and the distance a main cable can have.

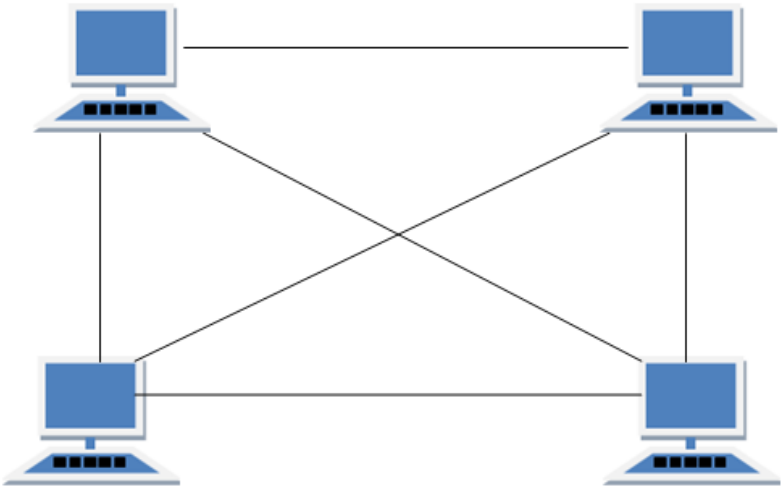


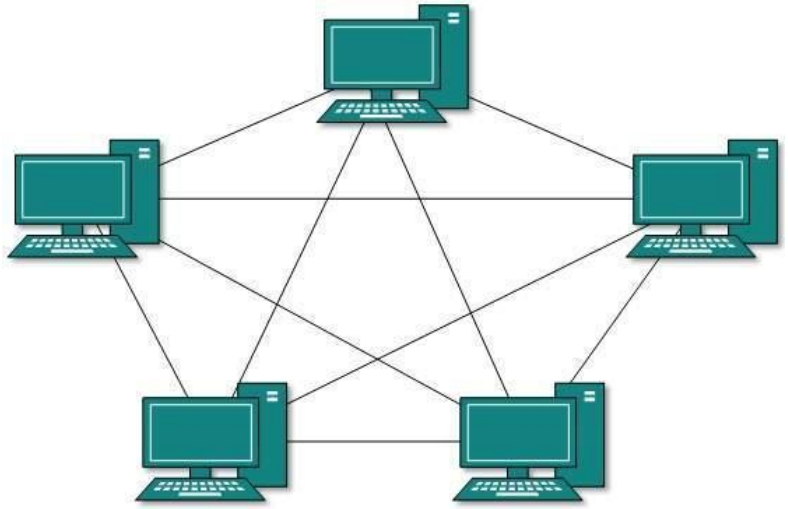
- Ring Topology:
  - In ring topology each device is connected with the two devices on either side of it.
  - There are two dedicated point to point links a device has with the devices on the either side of it.
  - This structure forms a ring thus it is known as ring topology.
  - If a device wants to send data to another device then it sends the data in one direction.

- Ring Topology:
  - Each device in ring topology has a repeater, if the received data is intended for other device then repeater forwards this data until the intended device receives it.

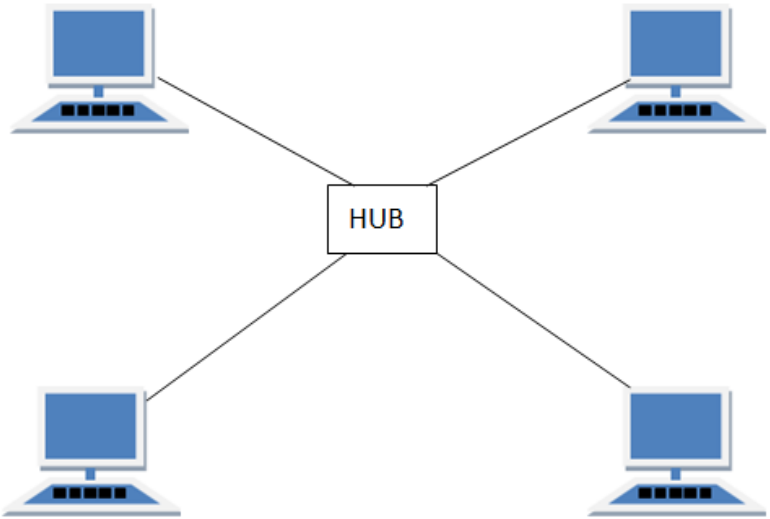


- Mesh Topology:
  - In mesh topology each device is connected to every other device on the network through a dedicated point-to-point link.
  - When we say dedicated it means that the link only carries data for the two connected devices only.
  - Lets say we have n devices in the network then each device must be connected with (n-1) devices of the network.
  - Number of links in a mesh topology of n devices would be n(n-1)/2.

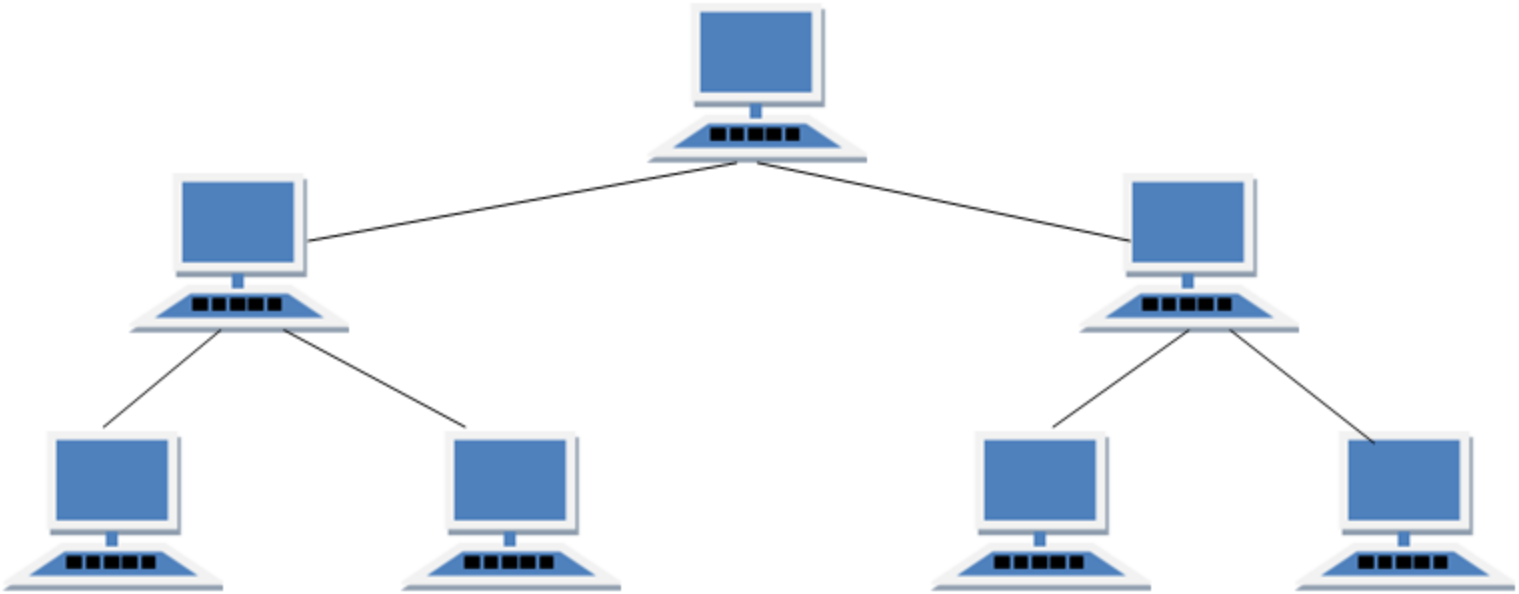




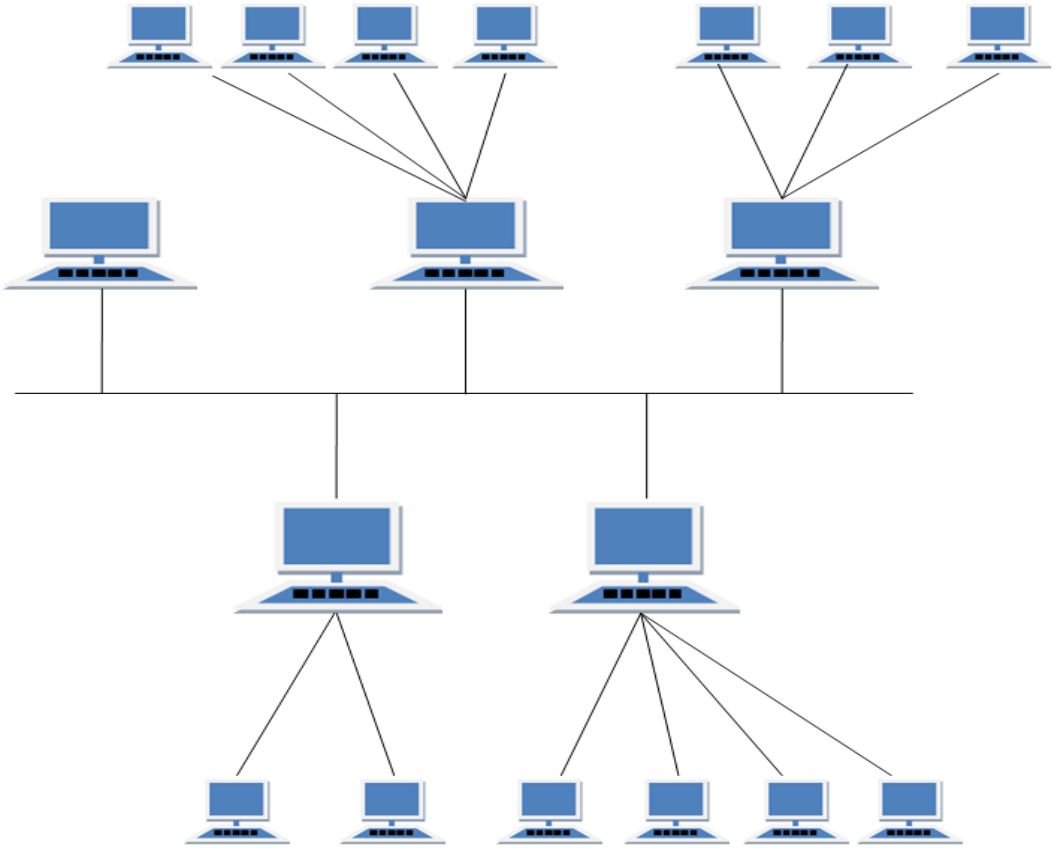
- Star Topology:
  - In star topology each device in the network is connected to a central device called hub.
  - Unlike Mesh topology, star topology doesn't allow direct communication between devices, a device must have to communicate through hub.
  - If one device wants to send data to other device, it has to first send the data to hub and then the hub transmit that data to the designated device.



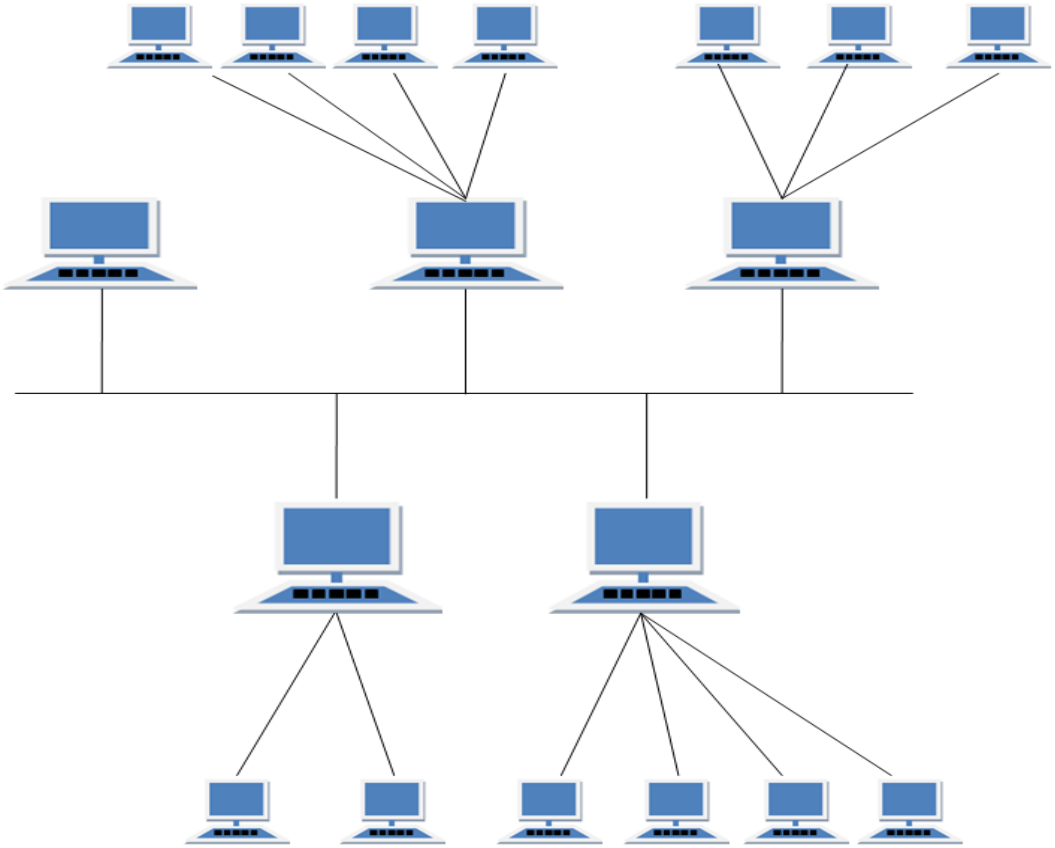
- Tree Topology:
  - This is also known as Hierarchical Topology, this is the most common form of network topology in use presently.
  - This topology imitates as extended Star topology and inherits properties of bus topology.
  - This topology divides the network in to multiple levels/layers of network.



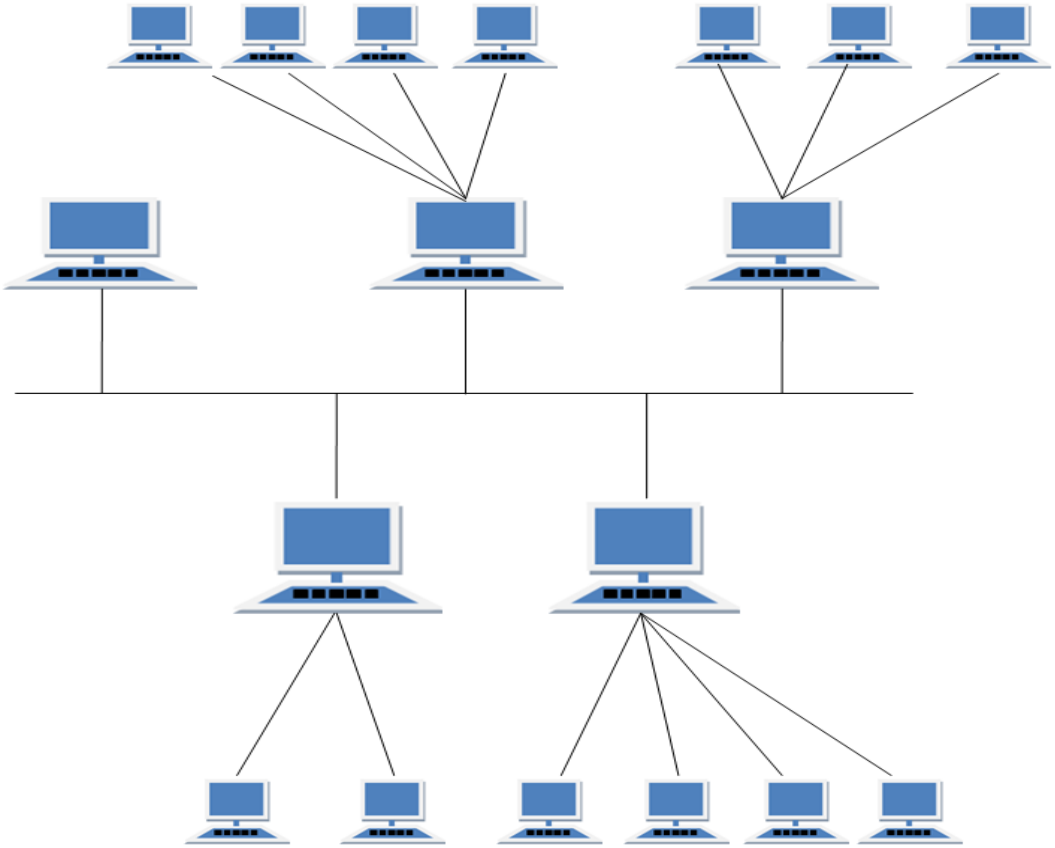
- Hybrid Topology:
  - A combination of two or more topology is known as hybrid topology.
  - For example a combination of star and mesh topology is known as hybrid topology.



- Hybrid Topology:
  - A combination of two or more topology is known as hybrid topology.
  - For example a combination of star and mesh topology is known as hybrid topology.



- Hybrid Topology:
  - A combination of two or more topology is known as hybrid topology.
  - For example a combination of star and mesh topology is known as hybrid topology.

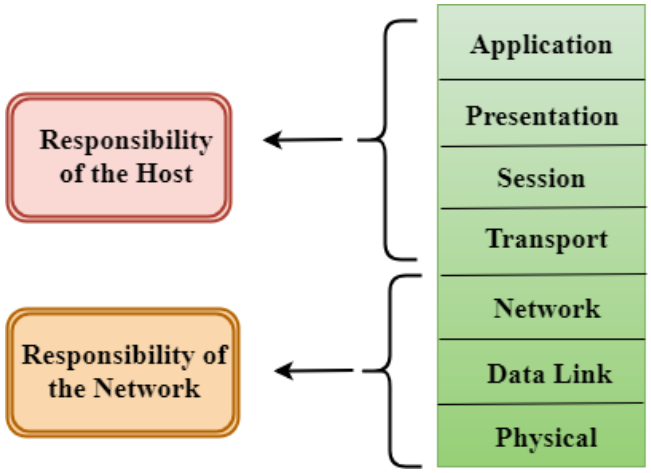


Layered models

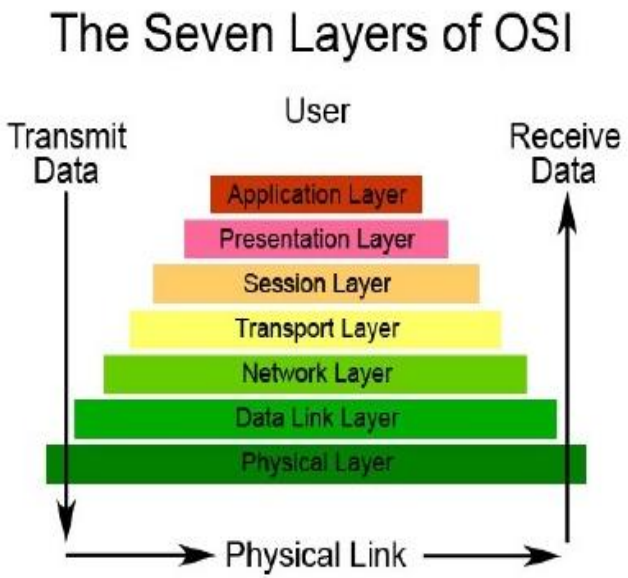
- In computer science, the concept of network layers is a framework that helps to understand complex network interactions.
- There are two models that are widely referenced today: OSI and TCP/IP.
- The concepts are similar, but the layers themselves differ between the two models.
- While TCP/IP is the newer model, the Open Systems Interconnection (OSI) model is still referenced a lot to describe network layers.

- OSI Reference 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.

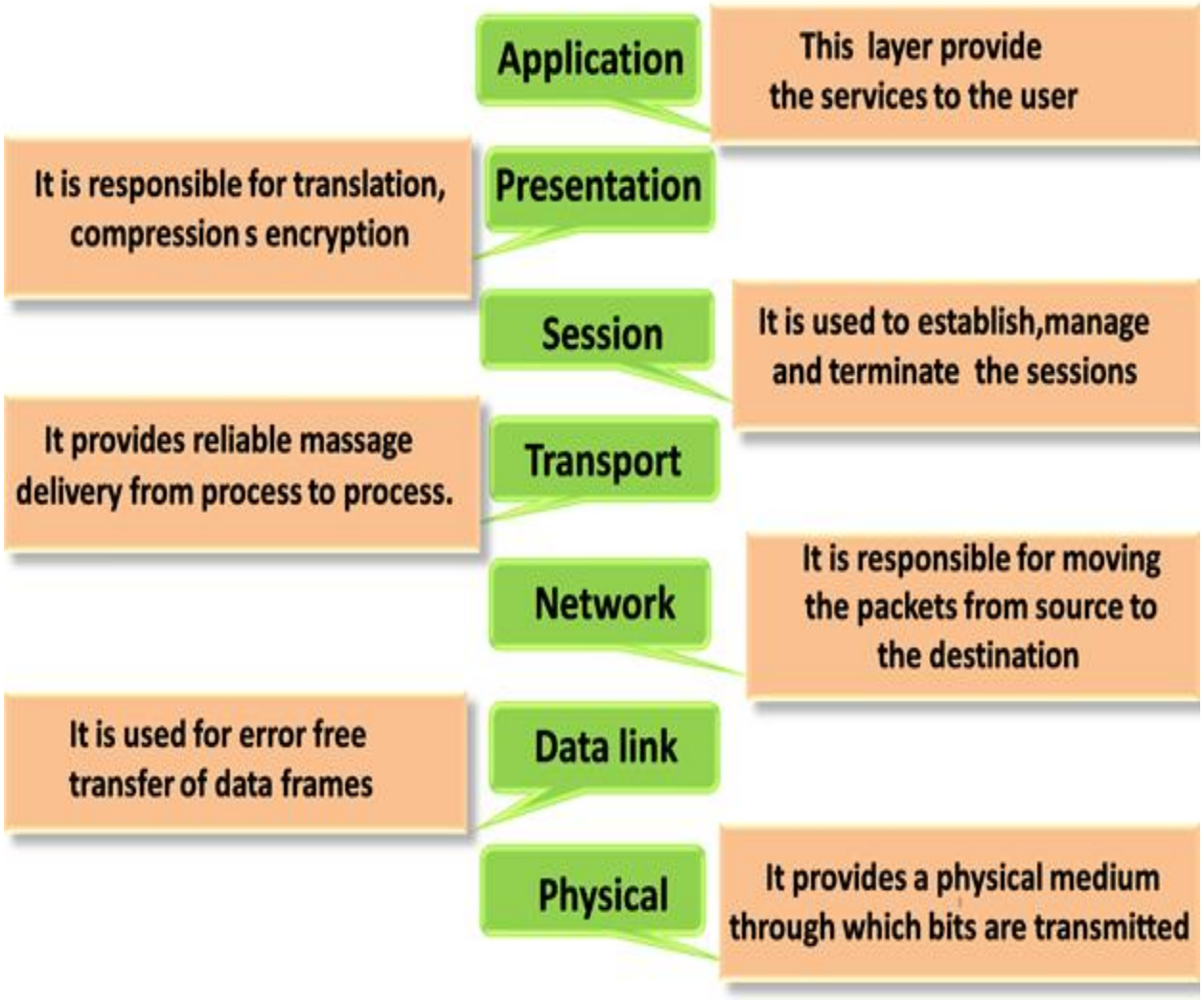
- The OSI model is divided into two layers: Upper layers and Lower layers.
- The upper layer:
  - This layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user.
- The lower layer:
  - This 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.



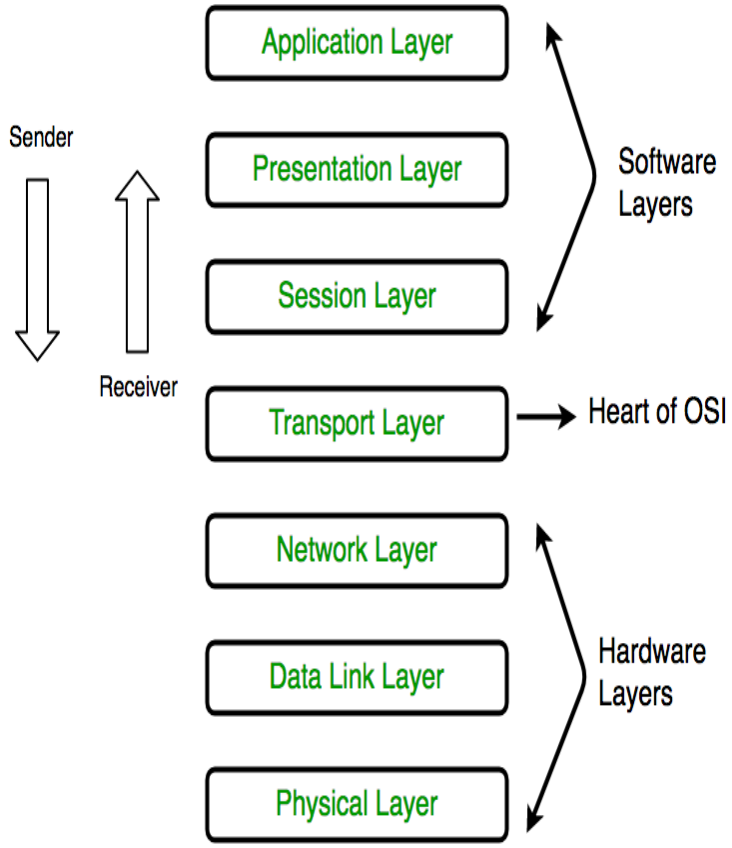
- There are the seven OSI layers. A list of seven layers are given below:
  1. Physical Layer
  2. Data-Link Layer
  3. Network Layer
  4. Transport Layer
  5. Session Layer
  6. Presentation Layer
  7. Application Layer



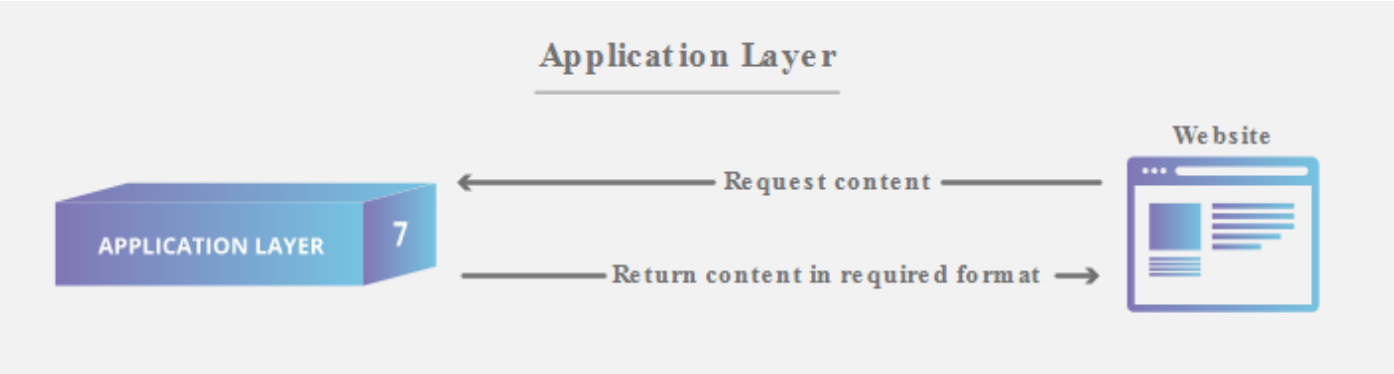
- Functions of the OSI Layers:
  - Each layer in the OSI model has a different function:



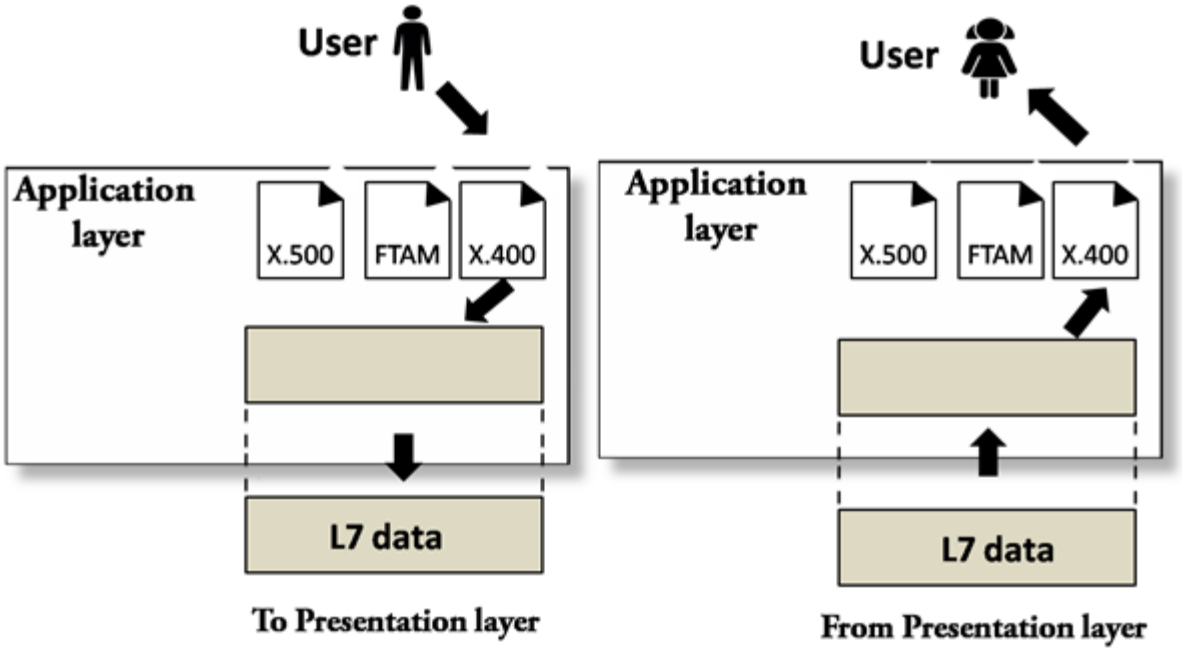
- Functions of the OSI Layers:
  - The seven abstraction layers of the OSI model can be explained as follows:
  - For the OSI model, let's start at the top (Application layer) and work our way down to bottom (Physical layer):



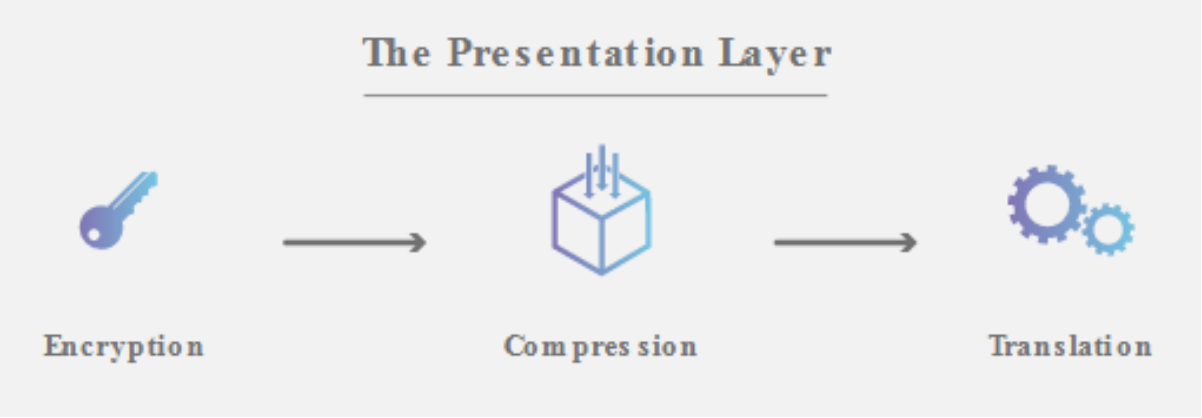
- 7. The Application Layer:
  - This is the only layer that directly interacts with data from the user.
  - Software applications like web browsers and email clients rely on the application layer to initiate communications.
  - But it should be made clear that the application layer is responsible for the protocols and data manipulation that the software relies on to present meaningful data to the user.



- 7. The Application Layer:
  - Application layer protocols include HTTP as well as SMTP (Simple Mail Transfer Protocol is one of the protocols that enables email communications).

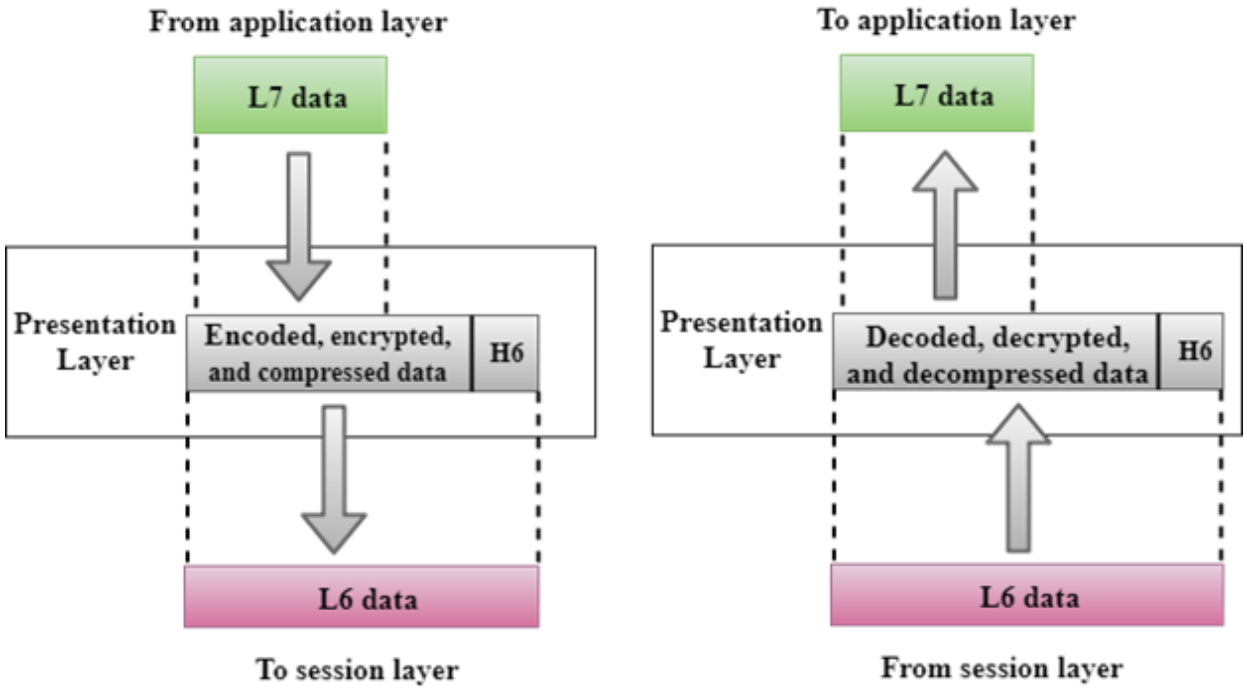


- 6. The Presentation Layer
  - This layer is primarily responsible for preparing data so that it can be used by the application layer; in other words, layer 6 makes the data presentable for applications to consume.
  - A Presentation layer is mainly concerned with the syntax and semantics of the information 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.



- 6. The Presentation Layer
  - The presentation layer is responsible for translation (Encoding/Decoding), Encryption/Decryption, and Compression/Decompression of data.
  - Translation:
    - Two communicating devices communicating may be using different encoding methods, so layer 6 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/Decryption:
    - Encryption is needed to maintain privacy.
    - If the devices are communicating over an encrypted connection, layer 6 is responsible for adding the encryption on the sender's end as well as converting the encryption on the receiver's end so that it can present the application layer with decrypted readable data.

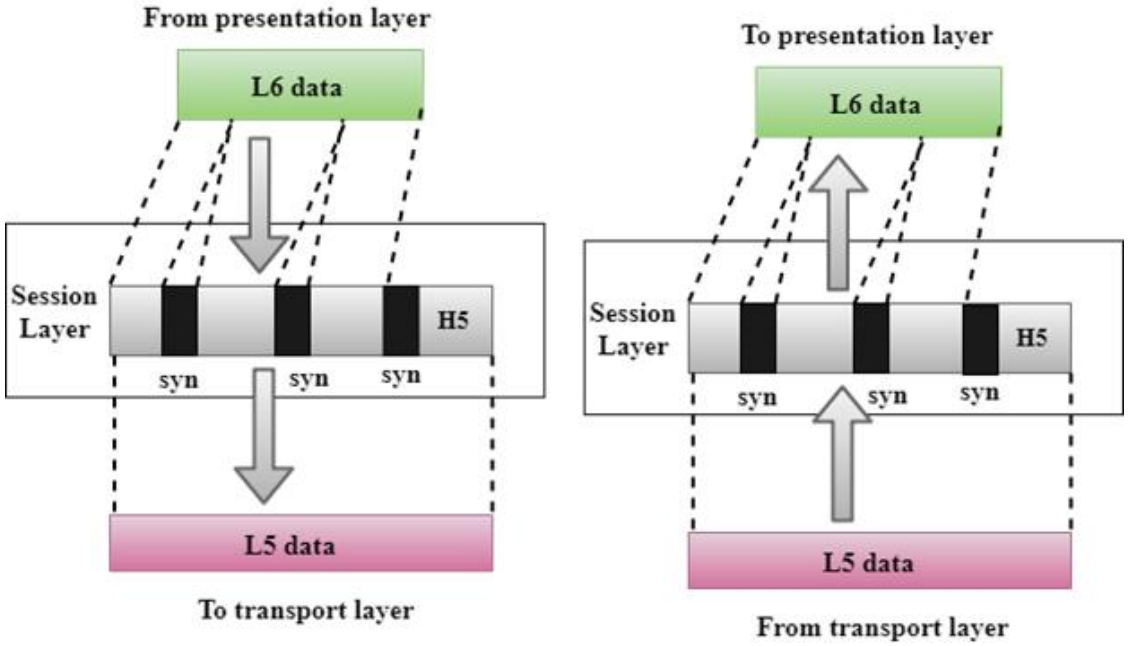
- 6. The Presentation Layer
  - Compression/Decompression:
    - Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted.
    - The presentation layer is also responsible for compressing data it receives from the application layer before delivering it to layer 5 and decompressing while transferring the data to layer 7.
    - This helps improve the speed and efficiency of communication.



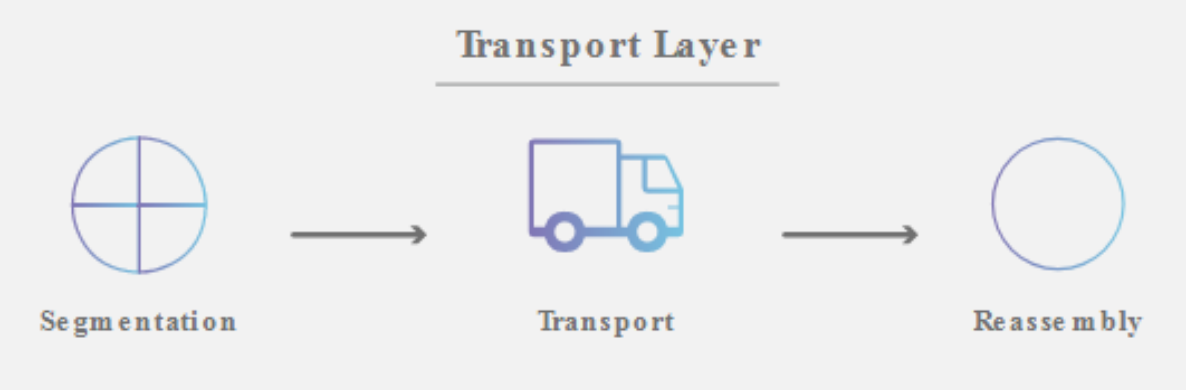
- 5. The Session Layer:
  - The Session layer is used to maintain and synchronizes the interaction between communicating devices.
  - This is the layer responsible for opening and closing communication between the two devices.
  - The time between when the communication is opened and closed is known as the session.
  - The session layer ensures that the session stays open long enough to transfer all the data being exchanged, and then promptly closes the session in order to avoid wasting resources.

- 5. The Session Layer:
  - The session layer also synchronizes data transfer with checkpoints.
  - This means, it adds some checkpoints in between 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.

- 5. The Session Layer:
  - For example, if a 100 megabyte file is being transferred, the session layer could set a checkpoint every 5 megabytes. In the case of a disconnect or a crash after 52 megabytes have been transferred, the session could be resumed from the last checkpoint, meaning only 50 more megabytes of data need to be transferred. Without the checkpoints, the entire transfer would have to begin again from scratch.

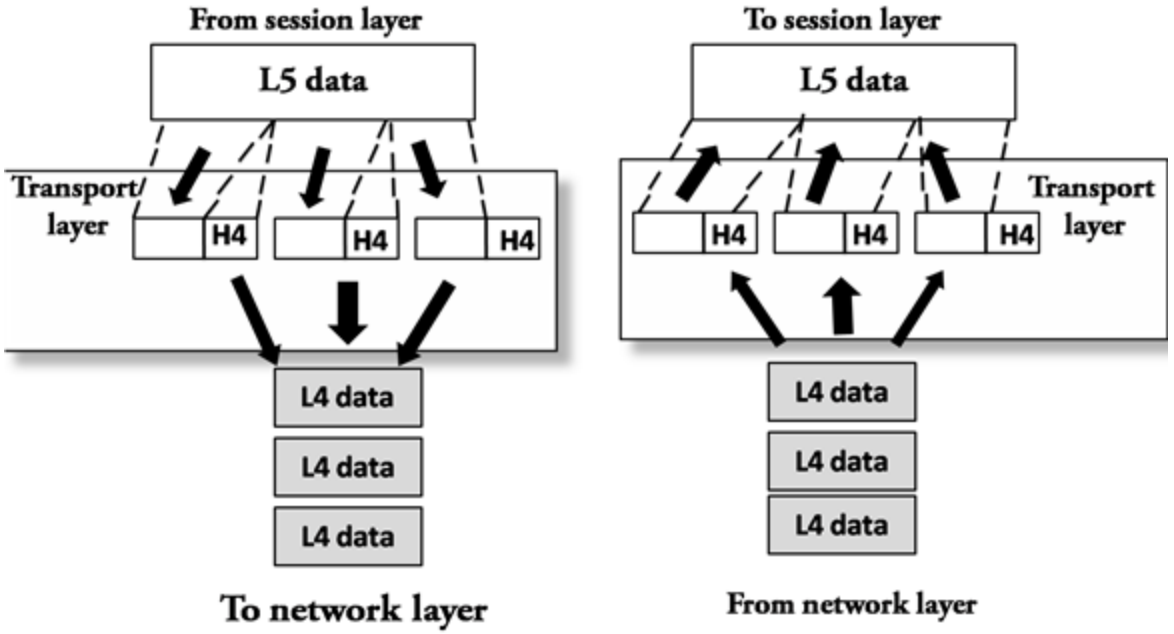


- 4. The Transport Layer
  - The Transport layer ensures that messages are transmitted in the order in which they are received and there is no duplication of data.
  - The main responsibility of the transport layer is to transfer the data completely.
  - It receives the data from the upper layer and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

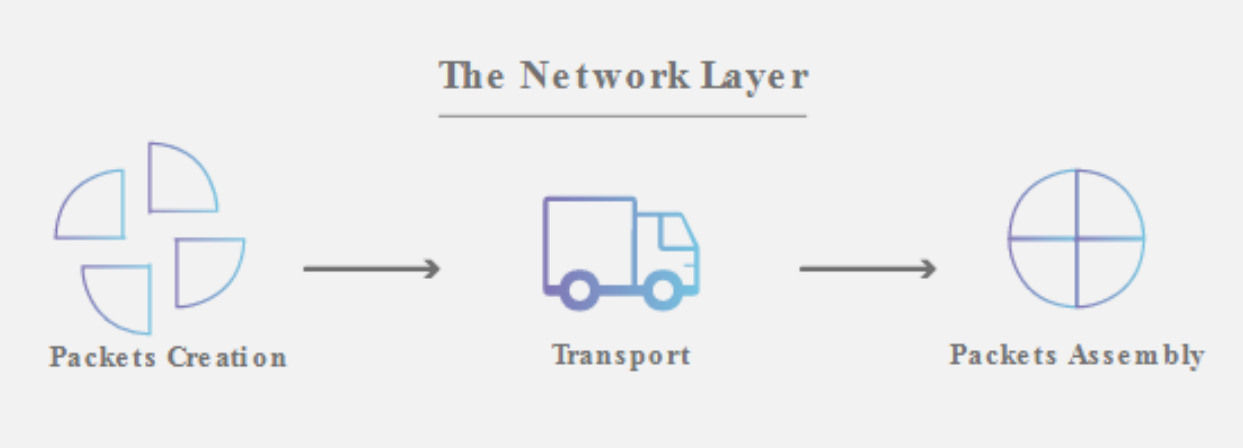


- 4. The Transport Layer
  - The Layer 4 is responsible for end-to-end communication between the two devices.
  - This includes taking data from the session layer and breaking it up into chunks called **segments** before sending it to layer 3.
  - The transport layer on the receiving device is responsible for **reassembling** the segments into data which the session layer can consume.
  - Computers run several programs simultaneously due to this reason, the transport layer adds the **header** to each segment that contains the address known as a **service-point address**.
  - The transport layer is also responsible for flow control and error control.

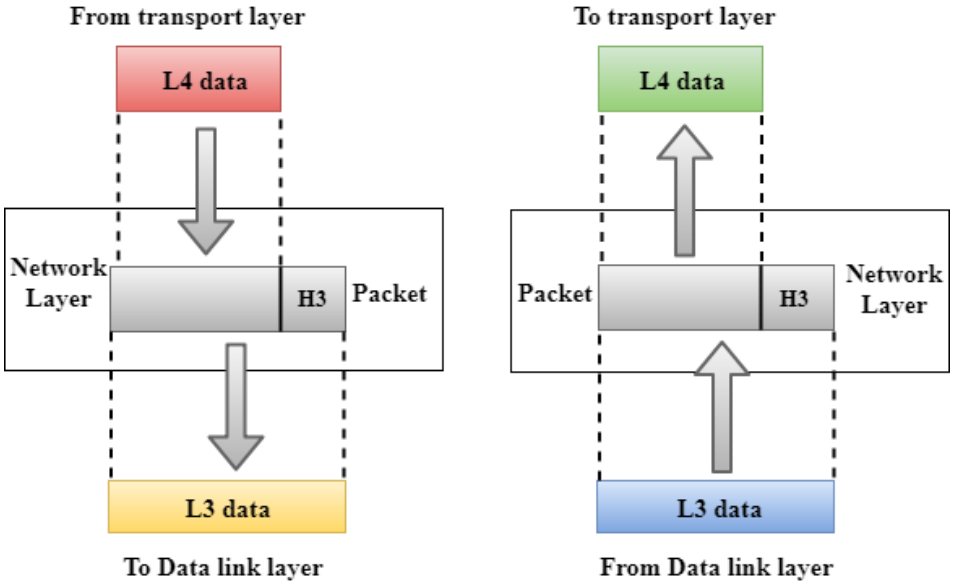
- 4. The Transport Layer
  - The flow control determines an optimal speed of transmission to ensure that a sender with a fast connection doesn't overwhelm a receiver with a slow connection.
  - The transport layer performs error control on the receiving end by ensuring that the data received is complete, and the sender transport layer ensures that message reach at the destination without any error.



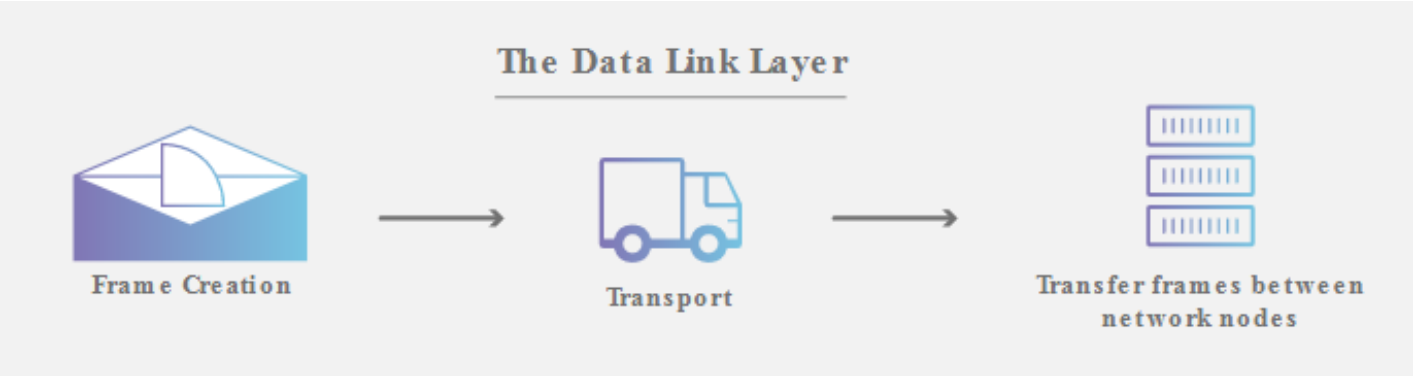
- 3. The Network Layer
  - This layer manages device addressing and keeps a track of the location of devices on the network.
  - The network layer is also responsible for facilitating data transfer between two different networks. If the two devices communicating are on the same network, then the network layer is unnecessary.
  - 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.



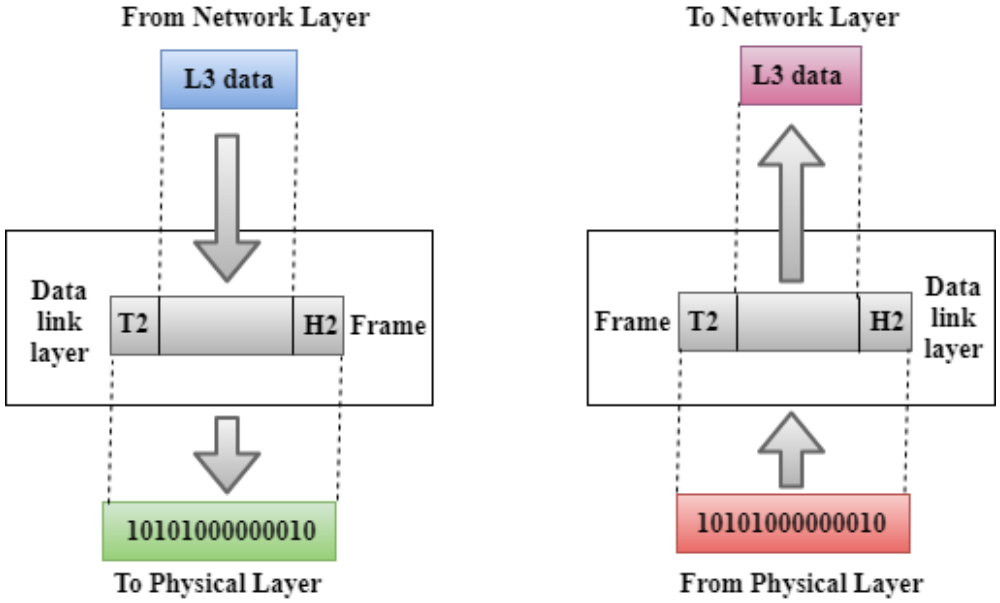
- 3. The Network Layer
  - A Network Layer receives the segments from the transport layer and converts them into packets.
  - This process is known as Packetizing.
  - A Network layer adds the source and destination address to the header of the packet. This address is used to identify the device on the internet.
  - The network layer also finds the best physical path for the data to reach its destination; this is known as routing.



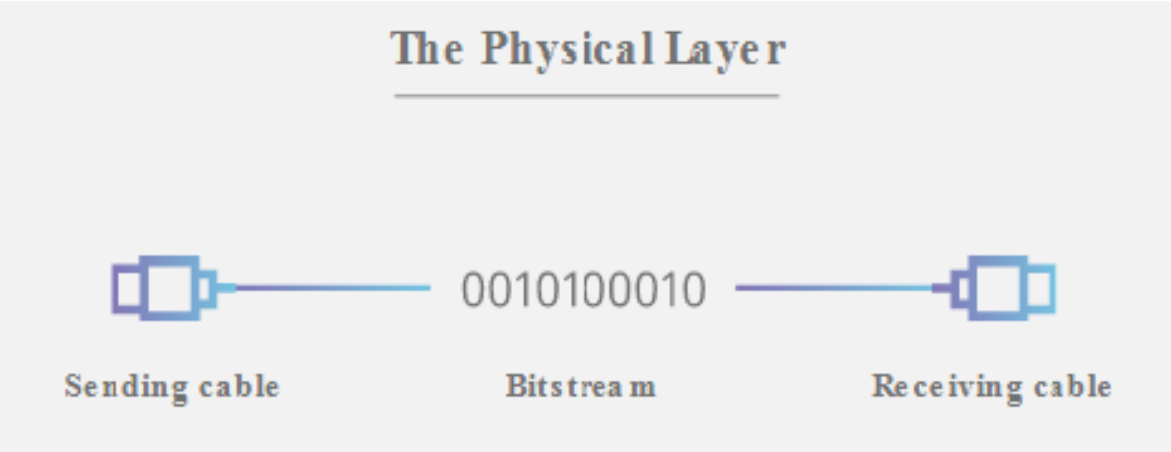
- 2. The Data Link Layer
  - The data link layer is very similar to the network layer.
  - This layer is responsible for the error-free transfer of data.
  - It provides a reliable and efficient communication between two or more devices.
  - The data link layer takes packets from the network layer and breaks them into smaller pieces called frames. This is called as framing.
  - The Data link layer adds a header and a trailer to the frame.
  - The header which is added to the frame contains the hardware destination and source address.



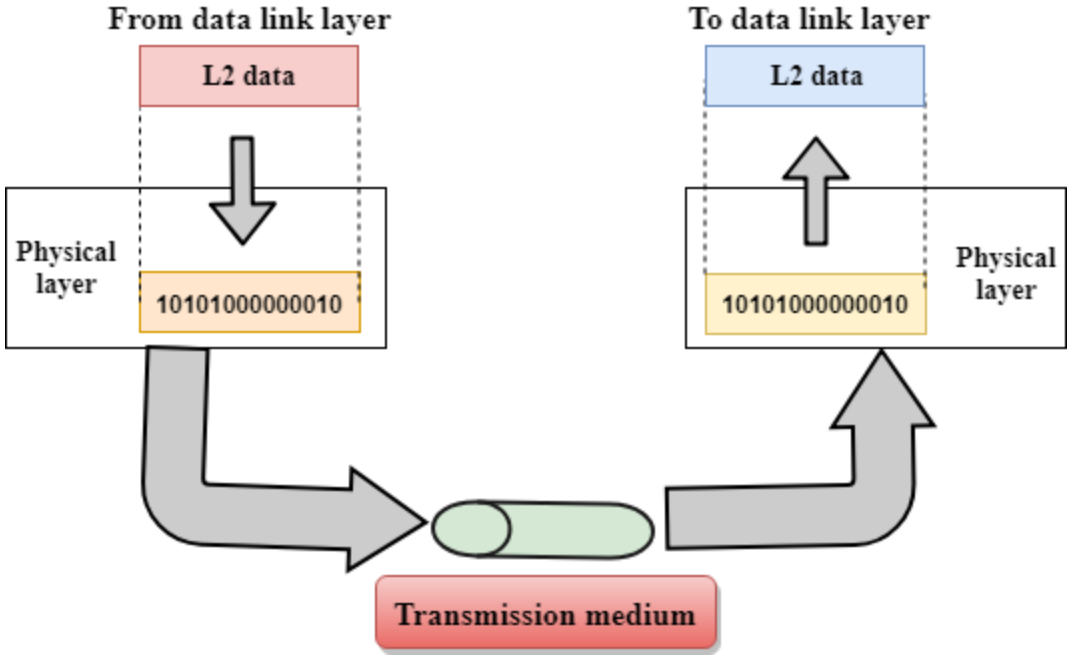
- 2. The Data Link Layer
  - The trailer which is added to the message frame before it is sent to the physical layer controls the errors in the frame.
  - If any error seems to occur, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
  - The data link layer is also responsible for flow control. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted.



- 1. The 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.
  - This layer includes the physical equipment involved in the data transfer, such as the cables and switches

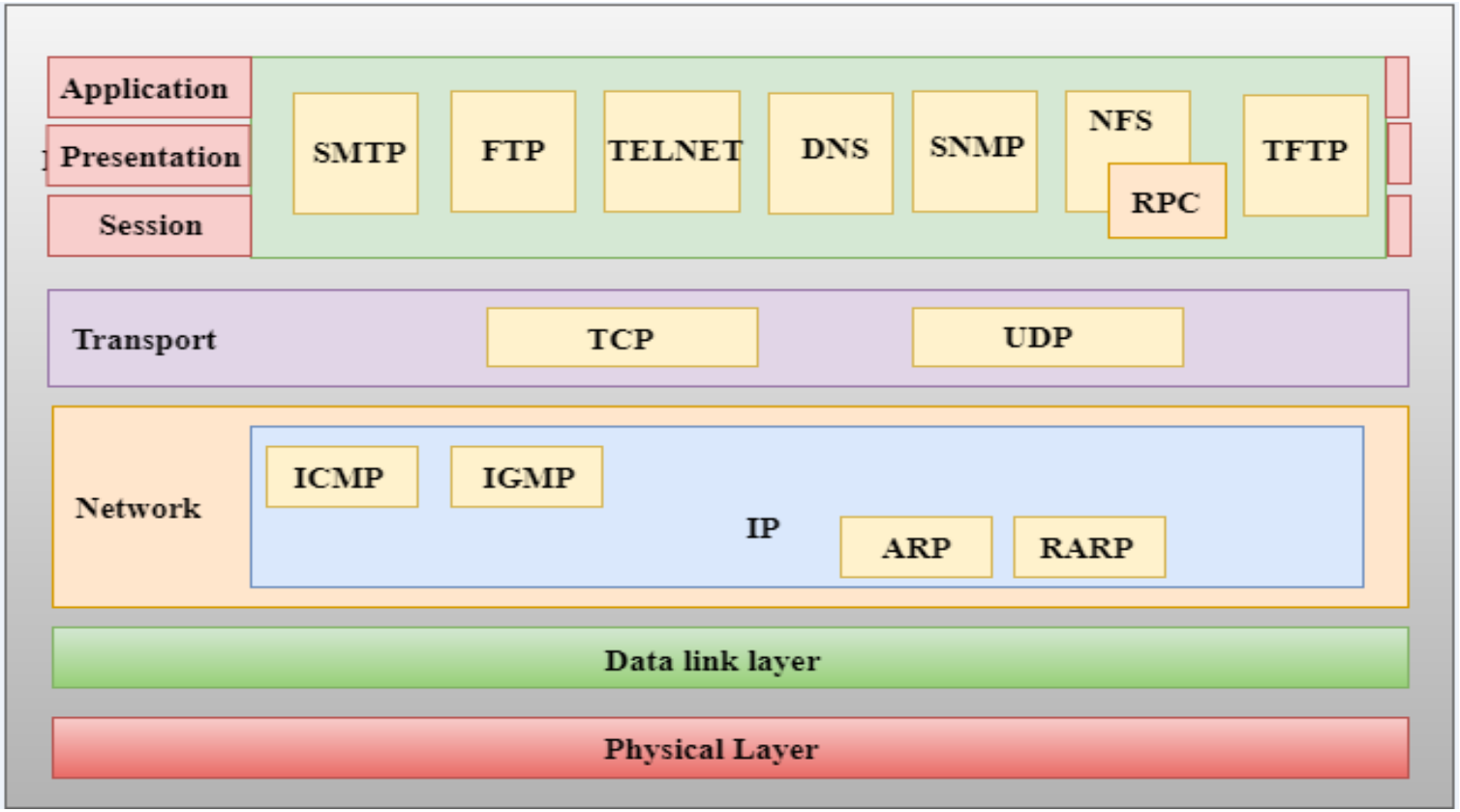


- 1. The Physical Layer
  - It defines the way how two or more devices can be connected physically.
  - This is also the layer where the data gets converted into a bit stream, which is a string of 1s and 0s.
  - The physical layer of both devices must also agree on a signal convention so that the 1's can be distinguished from the 0's on both devices.



- TCP/IP Reference Model:
  - The TCP/IP model was developed prior to the OSI model.
  - The TCP/IP model is not exactly similar to the OSI model.
  - The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
  - The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
  - TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.
  - Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

- Layers in TCP/IP Model:
  - The TCP/IP Model has four layers:
    - Physical Layer and data link layer – combined known as host-to-network layer
    - Network layer
    - Transport
    - Application



- 1. Physical and Data Link Layer
  - Physical and Data Link Layers in TCP/IP model does not define any protocols, they support all the standard protocols.
  - They are combined known as host-to-network layer.
  - A network in TCP/IP internetwork can be LAN or WAN.

- 2. Network Layer
  - In the network layer, the TCP/IP model supports internetworking protocol in short known as IP.
  - The IP uses four protocols internally: ARP, RARP, ICMP & IGMP.
  - Internetworking protocol(IP):
    1. It is an unreliable connectionless protocol used by TCP/IP Model.
    2. This protocol is used for data transmission.
    3. This protocol doesn't do error checking or tracking of data, thus we cannot be sure that the data is actually reached its destination. This is why it is also known as best effort delivery service which means this protocol tries it best to send the data to its destination but doesn't take an guarantee.
    4. IP protocol transmits the data in form of small packets known as datagrams. Each of these datagrams are transmitted separately, thus they can take different routes and sometime duplicate datagrams can be reached to destination, also they are reached in no particular order at the destination.

- 2. Network Layer
  - Four protocol the Internetworking protocol(IP) uses:
  - Address Resolution Protocol (ARP)
    - ARP finds the physical address by using the IP address.
    - In a network, each device is known as physical address usually imprinted on Network interface card (NIC).
    - ARP protocol is used to find the physical address of a device whose internet address (IP address) is known.
  - Reverse Address Resolution Protocol (RARP)
    - RARP protocol helps to find the internet address of a device whose physical address is known.

- 2. Network Layer
  - Internet Control Message Protocol (ICMP)
    - IP in network layer sends data in form of small packets known as datagrams. ICMP protocol sends the datagrams problems back to sender. It is used for query and error reporting messages.
  - Internet Group Message Protocol (IGMP)
    - This protocol is used for simultaneous transmission of a message to a group of recipients.

- 3. Transport Layer
  - Transport layer in TCP/Model can be represented by three protocols:
    - Transmission control protocol (TCP), User data gram protocol (UDP) and Stream Control Transmission Protocol (SCTP).
    - These three protocols in transport layer are responsible for delivery of messages from one process to another.
    - The SCTP protocol was later introduced to meet the needs of newer applications.

- 3. Transport Layer
  - User Datagram protocol (UDP):

    1. UDP is a process to process protocol used for data transmission.
    2. It takes the data from upper layer of TCP/IP Model and adds following information to the data:
       a) Port Address – Source port address of 16 bits and destination port address of 16 bits added to the data so that it reaches to correct destination and displays the correct source of data.
       b) Checksum error control – 16 bits of checksum data is added to the data received from upper layer, this is used for error control.
       c) Length of data – Length defines the total bytes of data present in datagram.
    3. Although this protocol finds the error in the transmission of data, it doesn't specify the error which makes it hard to identify the actual error in transmission.

- 3. Transport Layer
  - Transmission control protocol (TCP)
    1. Unlike UDP which is a connectionless protocol, the TCP is a connection oriented protocol.
    2. A connection must be made between sender and receiver before the transmission of data.
    3. TCP protocol divides the data in small units called segments. Each segment contains the sequence number which makes it possible to rearrange the segments in correct order at the receiver side to make the complete data.
    4. It also adds acknowledgement number to the segments to verify that the data is actually reached its destination or not.
    5. Unlike UDP which is unable to specify the exact error in transmission, this protocol does error control and specifies the exact error which makes TCP a reliable protocol.

- 3. Transport Layer
  - Stream Control Transmission Protocol (SCTP)
    1. The SCTP protocol was later introduced to meet the needs of newer applications.
    2. This protocol combines the best features of TCP and UDP protocols.
    3. It was discovered later to support newer applications such as voice data transmission over the internet.

- 4. Application Layer
  1. This is the top most layer of TCP/IP model.
  2. It is used for interaction between user and application.
  3. There are several protocols used by the application layer for user interaction such as: HTTP, SNMP, SMTP, DNS, TELNET, FTP etc.
  - HTTP:
    - HTTP stands for Hypertext transfer protocol, it allows the user to interact with world wide web through the browser application.
    - HTTP can be used to transfer various types of data such as plain text, audio, video etc.
  - FTP:
    - FTP stands for File Transfer Protocol.
    - This protocol is used for transmitting files from one system to another system.

- 4. Application Layer
  - TELNET:
    - TELNET is a client-server protocol. It is a reliable connection oriented protocol.
    - This protocol is used on internet or on LAN to provide a bidirectional (both ways) text based communication through a virtual terminal connection.
  - DNS:
    - DNS stands for Domain Name System.
    - Each computer on a network has different IP address, a computer is known by its IP address.
    - DNS provides a mapping to a name to the IP Address so a name can be used to identify a system on network rather than IP address itself.

- 4. Application Layer
  - SNMP:
    - SNMP stands for Simple Network Management Protocol.
    - It managers the devices connected to the internet using TCP/IP protocol.
  - SMTP:
    - SMTP stands for Simple mail transfer protocol.
    - It is used for email services, using this protocol a email containing data can be sent to another email address.

Thank you