**STUDY NOTES**

## UNIT –I

## Introduction to Computer networks

## Network goals and motivation

## Application of Networks

## Network Topologies

## Classification of Networks

## Network protocols and hierarchies

## Design issues for the layers

## Connection oriented and connectionless services

## Service primitives

## Relation of services to protocol

## Network models- OSI and TCP/IP

## Comparison of OSI and TCP/IP

## A critique of OSI and TCP/IP

## Examples of Network

## Introduction to Computer networks

## Definition - 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 is a set of connected computers. Computers on a network are called nodes. The connection between computers can be done via cabling, most commonly the Ethernet cable, or wirelessly through radio waves. Connected computers can share resources, like access to the Internet, printers, file servers, and others. A network is a multipurpose connection, which allows a single computer to do more.

## Network goals and motivation

1. **Resource Sharing**   
   Many organization has a substantial number of computers in operations, which are located apart. Eg. A group of office workers can share a common printer, fax, modem, scanner etc.
2. **High Reliability**   
   If there are alternate sources of supply, all files could be replicated on two or, machines. If one of them is not available, due to hardware failure, the other copies could be used.
3. **Inter-process Communication**   
   Network users, located geographically apart, may converse in an interactive session through the network. In order to permit this, the network must provide almost error-free communications.
4. **Flexible access**   
   Files can be accessed from any computer in the network. The project can be begun on one computer and finished on another.  
     
   Other goals include Distribution of processing functions, Centralized management, and allocation of network resources, Compatibility of dissimilar equipment and software, Good network performance, Scalability, Saving money, Access to remote information, Person to person communication etc.

## Applications of Networks

1. **Information and Resource Sharing:** Computer networks allow organizations having units which are placed apart from each other, to share information in a very effective manner. Programs and software in any computer can be accessed by other computers linked to the network. It also allows sharing of hardware equipment, like printers and scanners among varied users.
2. **Retrieving Remote Information:** Through computer networks, users can retrieve remote information on a variety of topics. The information is stored in remote databases to which the user gains access through information systems like the World Wide Web.
3. **Speedy Interpersonal Communication:** Computer networks have increased the speed and volume of communication like never before. Electronic Mail (email) is extensively used for sending texts, documents, images, and videos across the globe. Online communications have increased by manifold times through social networking services.
4. **E-Commerce:** Computer networks have paved way for a variety of business and commercial transactions online, popularly called e-commerce. Users and organizations can pool funds, buy or sell items, pay bills, manage bank accounts, pay taxes, transfer funds and handle investments electronically.
5. **Highly Reliable Systems:** Computer networks allow systems to be distributed in nature, by the virtue of which data is stored in multiple sources. This makes the system highly reliable. If a failure occurs in one source, then the system will still continue to function and data will still be available from the other sources.
6. **Cost–Effective Systems:** Computer networks have reduced the cost of establishment of computer systems in organizations. Previously, it was imperative for organizations to set up expensive mainframes for computation and storage. With the advent of networks, it is sufficient to set up interconnected personal computers (PCs) for the same purpose.
7. **VoIP:** VoIP or Voice over Internet protocol has revolutionized telecommunication systems. Through this, telephone calls are made digitally using Internet Protocols instead of the regular analog phone lines.

## Network Topologies

## The arrangement of a network which comprises of nodes and connecting lines via sender and receiver is referred as network topology. The various network topologies are :

## Bus Topology :

​ Bus topology is a network type in which every computer and network device is connected to single cable. It transmits the data from one end to another in single direction. No bi-directional feature is in 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.
* The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
* The configuration of a bus topology is quite simpler as compared to other topologies.
* The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.
* The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).



### 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.
* **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
* **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
* **Limited failure:** A failure in one node will not have any effect on other nodes.

### Disadvantages of Bus topology:

* **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.
* **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.
* **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
* **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
* **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.

## Star Topology :

​ In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node. The hub can be passive ​in nature i.e. not intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as active ​hubs. Active hubs have repeaters in them.

* 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**.
* Coaxial cable or RJ-45 cables are used to connect the computers.
* Hubs or Switches are mainly used as connection devices in a **physical star topology**.
* Star topology is the most popular topology in network implementation.



### Advantages of Star topology

* **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator has to go to the single station to troubleshoot the problem.
* **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.
* **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
* **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
* **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
* **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

### 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.

## Ring Topology :

​ In this topology, it forms a ring connecting a devices with its exactly two neighbouring devices.

* 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.
* The most common access method of the ring topology is **token passing**.
  + **Token passing:** It is a network access method in which token is passed from one node to another node.
  + **Token:** It is a frame that circulates around the network.

### Working of Token passing

* A token moves around the network, and it is passed from computer to computer until it reaches the destination.
* The sender modifies the token by putting the address along with the data.
* The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.
* In a ring topology, a token is used as a carrier.



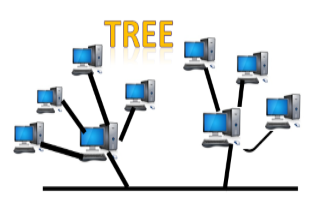
### Advantages of Ring topology:

* **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.
* **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
* **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

### 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.
* **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
* **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

## 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

* **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
* **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
* **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.
* **Error detection:** Error detection and error correction are very easy in a tree topology.
* **Limited failure:** The breakdown in one station does not affect the entire network.
* **Point-to-point wiring:** It has point-to-point wiring for individual segments.

### Disadvantages of Tree topology

* **Difficult troubleshooting:** If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
* **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.
* **Reconfiguration difficult:** If new devices are added, then it becomes difficult to reconfigure.

## Mesh Topology :

In mesh topology, every device is connected to another device via particular channel.

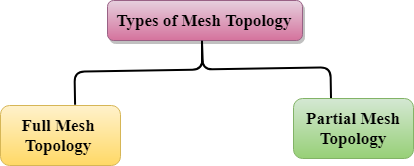


* Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
* There are multiple paths from one computer to another computer.
* It does not contain the switch, hub or any central computer which acts as a central point 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.
* Mesh topology is mainly used for wireless networks.
* Mesh topology can be formed by using the formula:  
  **Number of cables = (n\*(n-1))/2;**

Where n is the number of nodes that represents the network.

**Mesh topology is divided into two categories:**

* Fully connected mesh topology
* Partially connected mesh topology



* **Full Mesh Topology:** In a full mesh topology, each computer is connected to all the computers available in the network.
* **Partial Mesh Topology:** In a partial mesh topology, not all but certain computers are connected to those computers with which they communicate frequently.

### 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.

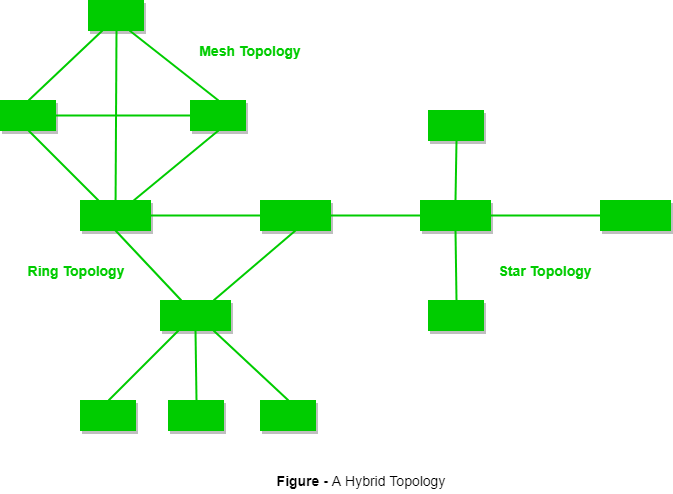
**Easier Reconfiguration:** Adding new devices would not disrupt the communication between other devices.

### 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.
* **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.

## Hybrid Topology :

This topology is a collection of two or more topologies which are described above. This is a scalable topology which can be expanded easily. It is reliable one but at the same it is a costly 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.
* **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
* **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

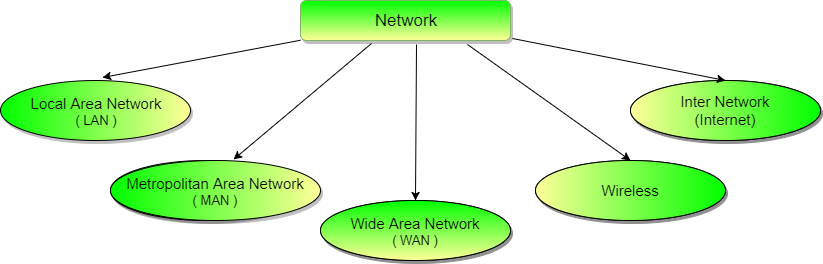
### Disadvantages of Hybrid topology

* **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.
* **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

## Classification of Networks

Networks can be of following 5 types:

1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide Area Network (WAN)
4. Wireless
5. Inter Network (Internet)

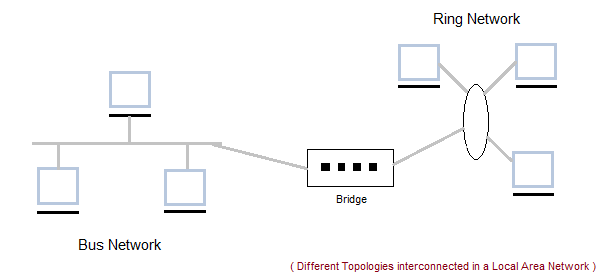


## Local Area Network (LAN)

It is also called LAN and designed for small physical areas such as an office, group of buildings or a factory. LANs are used widely as it is easy to design and to troubleshoot. Personal computers and workstations are connected to each other through LANs. We can use different types of topologies through LAN, these are Star, Ring, Bus, Tree etc.

LAN can be a simple network like connecting two computers, to share files and network among each other while it can also be as complex as interconnecting an entire building.

LAN networks are also widely used to share resources like printers, shared hard-drive etc.



### Characteristics of LAN

* LAN's are private networks, not subject to tariffs or other regulatory controls.
* LAN's operate at relatively high speed when compared to the typical WAN.
* There are different types of Media Access Control methods in a LAN, the prominent ones are Ethernet, Token ring.
* It connects computers in a single building, block or campus, i.e. they work in a restricted geographical area.

### Applications of LAN

* One of the computer in a network can become a server serving all the remaining computers called clients. Software can be stored on the server and it can be used by the remaining clients.
* Connecting Locally all the workstations in a building to let them communicate with each other locally without any internet access.
* Sharing common resources like printers etc are some common applications of LAN.

### Advantages of LAN

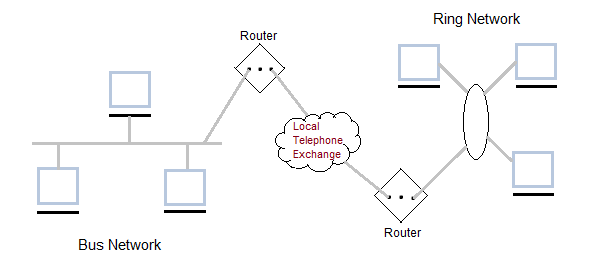
* **Resource Sharing:** Computer resources like printers, modems, DVD-ROM drives and hard disks can be shared with the help of local area networks. This reduces cost and hardware purchases.
* **Software Applications Sharing:** It is cheaper to use same software over network instead of purchasing separate licensed software for each client a network.
* **Easy and Cheap Communication:** Data and messages can easily be transferred over networked computers.
* **Centralized Data:** The data of all network users can be saved on hard disk of the server computer. This will help users to use any workstation in a network to access their data. Because data is not stored on workstations locally.
* **Data Security:** Since, data is stored on server computer centrally, it will be easy to manage data at only one place and the data will be more secure too.
* **Internet Sharing:** Local Area Network provides the facility to share a single internet connection among all the LAN users. In Net Cafes, single internet connection sharing system keeps the internet expenses cheaper.

### Disadvantages of LAN

* **High Setup Cost:** Although the LAN will save cost over time due to shared computer resources, but the initial setup costs of installing Local Area Networks is high.
* **Privacy Violations:** The LAN administrator has the rights to check personal data files of each and every LAN user. Moreover he can check the internet history and computer use history of the LAN user.
* **Data Security Threat:** Unauthorised users can access important data of an organization if centralized data repository is not secured properly by the LAN administrator.
* **LAN Maintenance Job:** Local Area Network requires a LAN Administrator because, there are problems of software installations or hardware failures or cable disturbances in Local Area Network. A LAN Administrator is needed at this full time job.
* **Covers Limited Area:** Local Area Network covers a small area like one office, one building or a group of nearby buildings.

## Metropolitan Area Network (MAN)

It was developed in 1980s.It is basically a bigger version of LAN. It is also called MAN and uses the similar technology as LAN. It is designed to extend over the entire city. It can be means to connecting a number of LANs into a larger network or it can be a single cable. It is mainly hold and operated by single private company or a public company.



### Characteristics of MAN

* It generally covers towns and cities (50 km)
* Communication medium used for MAN are optical fibers, cables etc.
* Data rates adequate for distributed computing applications.

### Advantages of MAN

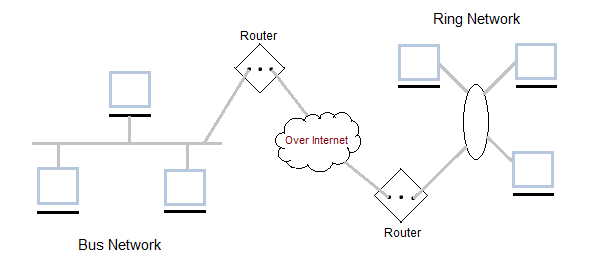
* Extremely efficient and provide fast communication via high-speed carriers, such as fibre optic cables.
* It provides a good back bone for large network and provides greater access to WANs.
* The dual bus used in MAN helps the transmission of data in both directions simultaneously.
* A MAN usually encompasses several blocks of a city or an entire city.

### Disadvantages of MAN

* More cable required for a MAN connection from one place to another.
* It is difficult to make the system secure from hackers and industrial espionage(spying) graphical regions.

## Wide Area Network (WAN)

It is also called WAN. WAN can be private or it can be public leased network. It is used for the network that covers large distance such as cover states of a country. It is not easy to design and maintain. Communication medium used by WAN are PSTN or Satellite links. WAN operates on low data rates.



### Characteristics of WAN

* It generally covers large distances(states, countries, continents).
* Communication medium used are satellite, public telephone networks which are connected by routers.

### Advantages of WAN

* Covers a large geographical area so long distance business can connect on the one network.
* Shares software and resources with connecting workstations.
* Messages can be sent very quickly to anyone else on the network. These messages can have picture, sounds or data included with them(called attachments).
* Expensive things(such as printers or phone lines to the internet) can be shared by all the computers on the network without having to buy a different peripheral for each computer.
* Everyone on the network can use the same data. This avoids problems where some users may have older information than others.

### Disadvantages of WAN

* Need a good firewall to restrict outsiders from entering and disrupting the network.
* Setting up a network can be an expensive, slow and complicated. The bigger the network the more expensive it is.
* Once set up, maintaining a network is a full-time job which requires network supervisors and technicians to be employed.
* Security is a real issue when many different people have the ability to use information from other computers. Protection against hackers and viruses adds more complexity and expense.

## Wireless Network

Digital wireless communication is not a new idea. Earlier, **Morse code** was used to implement wireless networks. Modern digital wireless systems have better performance, but the basic idea is the same.

Wireless Networks can be divided into three main categories:

1. **System interconnection**
2. **Wireless LANs**
3. **Wireless WANs**

### System Interconnection

System interconnection is all about interconnecting the components of a computer using **short-range radio**. Some companies got together to design a short-range wireless network called **Bluetooth** to connect various components such as monitor, keyboard, mouse and printer, to the main unit, without wires. Bluetooth also allows digital cameras, headsets, scanners and other devices to connect to a computer by merely being brought within range.

In simplest form, system interconnection networks use the master-slave concept. The system unit is normally the **master**, talking to the mouse, keyboard, etc. as **slaves**.

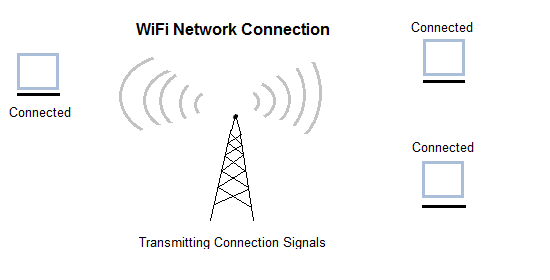
### Wireless LANs

These are the systems in which every computer has a **radio modem** and **antenna** with which it can communicate with other systems. Wireless LANs are becoming increasingly common in small offices and homes, where installing **Ethernet** is considered too much trouble. There is a standard for wireless LANs called **IEEE 802.11**, which most systems implement and which is becoming very widespread.

### Wireless WANs

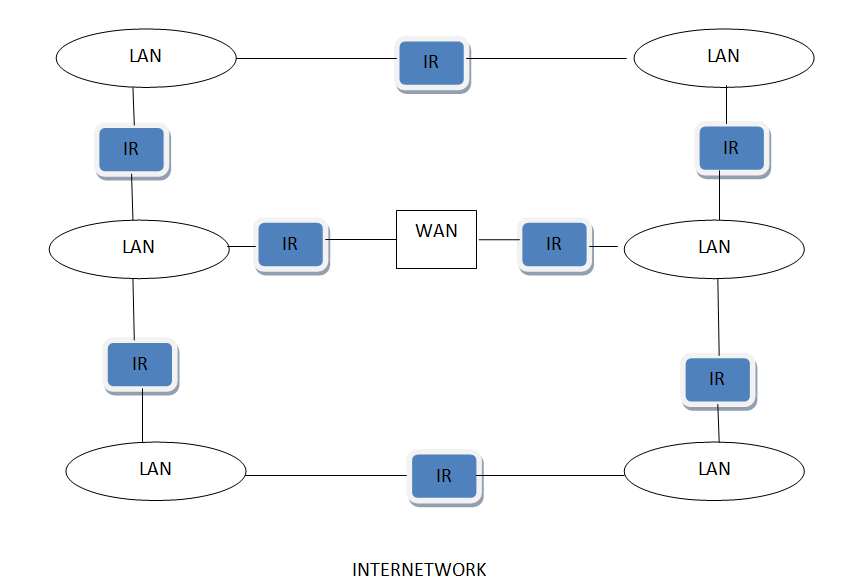
The radio network used for cellular telephones is an example of a low-bandwidth wireless WAN. This system has already gone through three generations.

* The first generation was analog and for voice only.
* The second generation was digital and for voice only.
* The third generation is digital and is for both voice and data.



## Inter Network

Inter Network or Internet is a combination of two or more networks. Inter network can be formed by joining two or more individual networks by means of various devices such as routers, gateways and bridges.

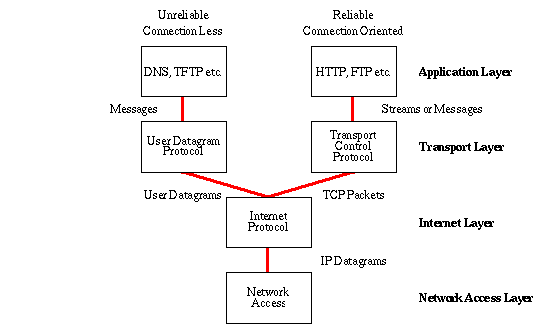


## Network protocols and hierarchies

A protocol is a set of rules that governs the communications between computers on a network. These rules include guidelines that regulate the following characteristics of a network: access method, allowed physical topologies, types of cabling, and speed of data transfer.

## Types of Protocols

* **TCP-** Transmission control protocol is used for communication over a network. In TCP data is broken down into small packets and then sent to the destination. However, IP is making sure packets are transmitted to the right address.
* **Internet Protocol (IP)** - IP is also working with TCP. It is an addressing Protocol. IP addresses packets route them and show different nodes and network Unless it reaches its right destination. The IP protocol is developed in 1970.
* **FTP**- File transfer protocol is basically used for transferring files to different networks. There may be a mass of files such as text files, multimedia files, etc. This way of file transfer is quicker than other methods.
* **SMTP-** Simple mail transfer protocol manages the transmission and outgoing mail over the internet.
* **HTTP**- HTTP is based on client and server model. HTTP is used for making a connection between the web client and web server. HTTP shows information in web pages.
* **Ethernet**- Ethernet is a most important for LAN communication. Ethernet transmits the data in digital packets. If any computer wants to use this protocol they should contain Ethernet Network Interface Card (NIC). The card is implemented with unique address code fixed in the microchip.
* **Telnet**- Telnet is an established with some rules which are used to connect to another computer. Telnet is mainly used for the remote login process. The computer which is requesting for a connection that is a local computer and which is accepting the connection that is a remote computer. If you give a command in a local computer that command is executed in the remote computer. Telnet is also based on client and server model.
* **Gopher**- Gopher is an application layer protocol, which is used for searching and retrieving documents from remote sites. This is possible to start an online connection with other computers through gopher.
* **Network hierarchies**



## Design issues for the layers

A number of design issues exist for the layer to layer approach of computer networks. Some of the main design issues are as follows:

#### 1. Reliability

Network channels and components may be unreliable, resulting in loss of bits while data transfer. So, an important design issue is to make sure that the information transferred is not distorted.

#### 2. Scalability

Networks are continuously evolving. The sizes are continually increasing leading to congestion. Also, when new technologies are applied to the added components, it may lead to incompatibility issues. Hence, the design should be done so that the networks are scalable and can accommodate such additions and alterations.

#### 3. Addressing

At a particular time, innumerable messages are being transferred between large numbers of computers. So, a naming or addressing system should exist so that each layer can identify the sender and receivers of each message.

#### 4. Error Control

Unreliable channels introduce a number of errors in the data streams that are communicated. So, the layers need to agree upon common error detection and error correction methods so as to protect data packets while they are transferred.

#### 5. Flow Control

If the rate at which data is produced by the sender is higher than the rate at which data is received by the receiver, there are chances of overflowing the receiver. So, a proper flow control mechanism needs to be implemented.

#### 6. Resource Allocation

Computer networks provide services in the form of network resources to the end users. The main design issue is to allocate and deallocate resources to processes. The allocation/deallocation should occur so that minimal interference among the hosts occurs and there is optimal usage of the resources.

#### 7. Statistical Multiplexing

It is not feasible to allocate a dedicated path for each message while it is being transferred from the source to the destination. So, the data channel needs to be multiplexed, so as to allocate a fraction of the bandwidth or time to each host.

#### 8. Routing

There may be multiple paths from the source to the destination. Routing involves choosing an optimal path among all possible paths, in terms of cost and time. There are several routing algorithms that are used in network systems.

#### 9. Security

A major factor of data communication is to defend it against threats like eavesdropping and surreptitious alteration of messages. So, there should be adequate mechanisms to prevent unauthorized access to data through authentication and cryptography.

## Connection oriented and connectionless services

These are the two services given by the layers to layers above them. These services are:

1. Connection Oriented Service
2. Connectionless Services

## Connection Oriented Services

There is a sequence of operation to be followed by the users of connection oriented service. These are:

1. Connection is established.
2. Information is sent.
3. Connection is released.

In connection oriented service we have to establish a connection before starting the communication. When connection is established, we send the message or the information and then we release the connection.

Connection oriented service is more reliable than connectionless service. We can send the message in connection oriented service if there is an error at the receivers end. Example of connection oriented is TCP (Transmission Control Protocol) protocol.

## Connection Less Services

It is similar to the postal services, as it carries the full address where the message (letter) is to be carried. Each message is routed independently from source to destination. The order of message sent can be different from the order received.

In connectionless the data is transferred in one direction from source to destination without checking that destination is still there or not or if it prepared to accept the message. Authentication is not needed in this. Example of Connectionless service is UDP (User Datagram Protocol) protocol.

### Difference: Connection oriented and Connectionless service

1. In connection oriented service authentication is needed, while connectionless service does not need any authentication.
2. Connection oriented protocol makes a connection and checks whether message is received or not and sends again if an error occurs, while connectionless service protocol does not guarantees a message delivery.
3. Connection oriented service is more reliable than connectionless service.
4. Connection oriented service interface is stream based and connectionless is message based.

## Service primitives

A service is formally specified by a set of primitives (operations) available to a user process to access the service. These primitives tell the service to perform some action or report on an action taken by a peer entity. If the protocol stack is located in the operating system, as it often is, the primitives are normally system calls. These calls cause a trap to kernel mode, which then turns control of the machine over to the operating system to send the necessary packets. The set of primitives available depends on the nature of the service being provided. The primitives for connection-oriented service are different from those of connection-less service. There are five types of service primitives :

1. **LISTEN :**When a server is ready to accept an incoming connection it executes the LISTEN primitive. It blocks waiting for an incoming connection.
2. **CONNECT :**It connects the server by establishing a connection. Response is awaited.
3. **RECIEVE:**Then the RECIEVE call blocks the server.
4. **SEND :**Then the client executes SEND primitive to transmit its request followed by the execution of RECIEVE to get the reply. Send the message.
5. **DISCONNECT :** This primitive is used for terminating the connection. After this primitive one can't send any message. When the client sends DISCONNECT packet then the server also sends the DISCONNECT packet to acknowledge the client. When the server package is received by client then the process is terminated.

#### Connection Oriented Service Primitives

There are 5 types of primitives for Connection Oriented Service :

|  |  |
| --- | --- |
| LISTEN | Block waiting for an incoming connection |
| CONNECTION | Establish a connection with a waiting peer |
| RECEIVE | Block waiting for an incoming message |
| SEND | Sending a message to the peer |
| DISCONNECT | Terminate a connection |

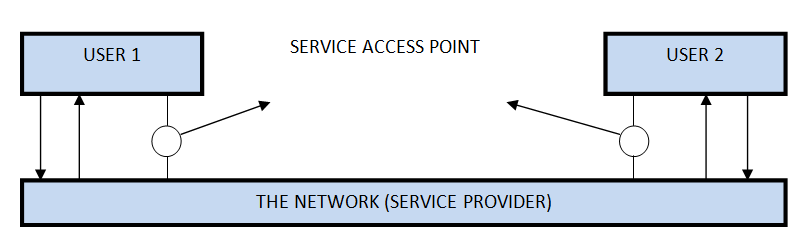
#### Connectionless Service Primitives

There are 4 types of primitives for Connectionless Oriented Service:

|  |  |
| --- | --- |
| UNIDATA | This primitive sends a packet of data |
| FACILITY, REPORT | Primitive for enquiring about the performance of the network, like delivery statistics. |

## Relation of services to protocol

**Service Definition -** These are the operations that a layer can provide to the layer above it in the OSI Reference model. It defines the operation and states a layer is ready to perform but it does not specify anything about the implementation of these operations.



#### Protocols Defination

These are set of rules that govern the format and meaning of frames, messages or packets that are exchanged between the server and client.

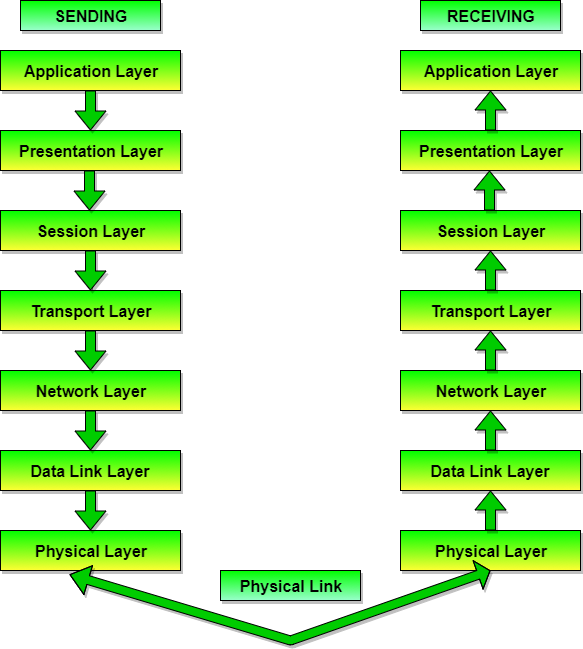
## Network models- OSI and TCP/IP

The most important reference models are:

1. OSI reference model.
2. TCP/IP reference model.

## Introduction to ISO-OSI Model

There are many users who use computer network and are located all over the world. To ensure national and worldwide data communication ISO (ISO stands for International Organization of Standardization.) developed this model. This is called a model for open system interconnection (OSI) and is normally called as OSI model.OSI model architecture consists of seven layers. It defines seven layers or levels in a complete communication system.

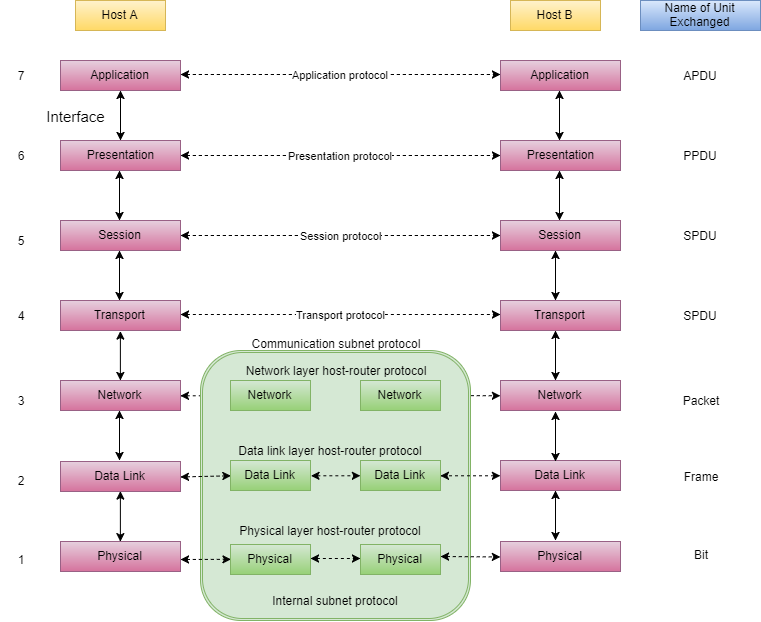


There are n numbers of users who use computer network and are located over the world. So to ensure, national and worldwide data communication, systems must be developed which are compatible to communicate with each other ISO has developed a standard. ISO stands for **International organization of Standardization**. This is called a model for **Open System Interconnection** (OSI) and is commonly known as OSI model.

The ISO-OSI model is a seven layer architecture. It defines seven layers or levels in a complete communication system. They are:

1. Application Layer
2. Presentation Layer
3. Session Layer
4. Transport Layer
5. Network Layer
6. Datalink Layer
7. Physical Layer

**The complete representation of the OSI model, showcasing all the layers and how they communicate with each other.**



## Feature of OSI Model

1. Big picture of communication over network is understandable through this OSI model.
2. We see how hardware and software work together.
3. We can understand new technologies as they are developed.
4. Troubleshooting is easier by separate networks.
5. Can be used to compare basic functional relationships on different networks.

## Principles of OSI Reference Model

The OSI reference model has 7 layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

1. A layer should be created where a different abstraction is needed.
2. Each layer should perform a well-defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that architecture does not become unwieldly.

## Functions of Different Layers

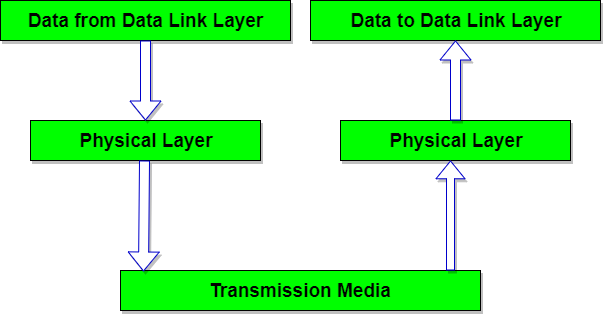
# Physical Layer - OSI Reference Model

Physical layer is the lowest layer of the OSI reference model. It is responsible for sending bits from one computer to another. This layer is not concerned with the meaning of the bits and deals with the setup of physical connection to the network and with transmission and reception of signals.

## Functions of Physical Layer

Following are the various functions performed by the Physical layer of the OSI model.

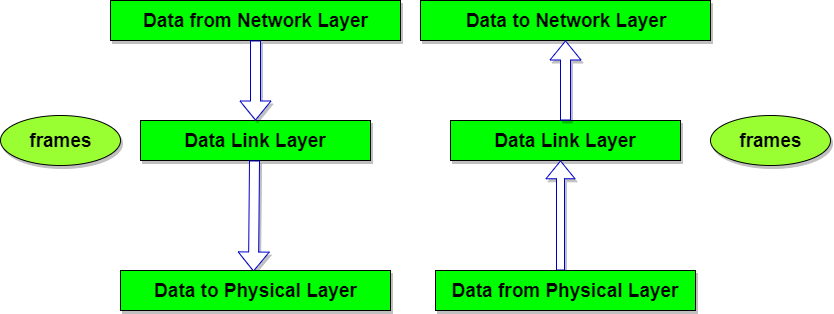
1. **Representation of Bits:** Data in this layer consists of stream of bits. The bits must be encoded into signals for transmission. It defines the type of encoding i.e. how 0's and 1's are changed to signal.
2. **Data Rate:**This layer defines the rate of transmission which is the number of bits per second.
3. **Synchronization:**It deals with the synchronization of the transmitter and receiver. The sender and receiver are synchronized at bit level.
4. **Interface:**The physical layer defines the transmission interface between devices and transmission medium.
5. **Line Configuration:**This layer connects devices with the medium: Point to Point configuration and Multipoint configuration.
6. **Topologies:**Devices must be connected using the following topologies: Mesh, Star, Ring and Bus.
7. **Transmission Modes:**Physical Layer defines the direction of transmission between two devices: Simplex, Half Duplex, Full Duplex.
8. Deals with baseband and broadband transmission.



# Data Link Layer - OSI Model

## Functions of Data Link Layer

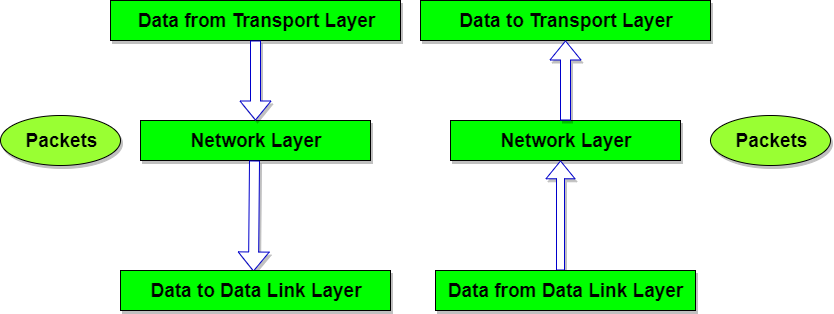
1. **Framing:** Frames are the streams of bits received from the network layer into manageable data units. This division of stream of bits is done by Data Link Layer.
2. **Physical Addressing:**The Data Link layer adds a header to the frame in order to define physical address of the sender or receiver of the frame, if the frames are to be distributed to different systems on the network.
3. **Flow Control:**A flow control mechanism to avoid a fast transmitter from running a slow receiver by buffering the extra bit is provided by flow control. This prevents traffic jam at the receiver side.
4. **Error Control:**Error control is achieved by adding a trailer at the end of the frame. Duplication of frames are also prevented by using this mechanism. Data Link Layers adds mechanism to prevent duplication of frames.
5. **Access Control:**Protocols of this layer determine which of the devices has control over the link at any given time, when two or more devices are connected to the same link.



# Network Layer - OSI Model

## Functions of Network Layer

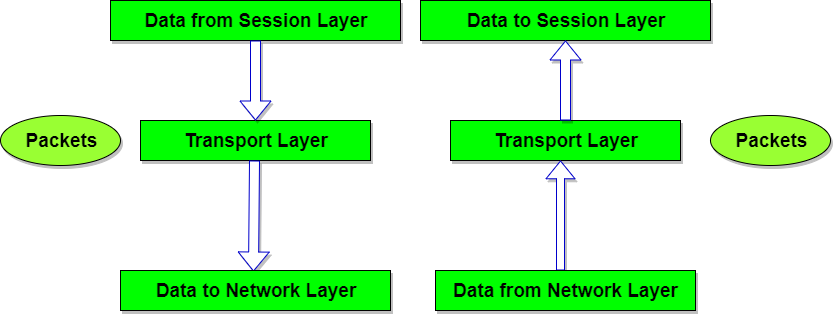
1. It translates logical network address into physical address. Concerned with circuit, message or packet switching.
2. Routers and gateways operate in the network layer. Mechanism is provided by Network Layer for routing the packets to final destination.
3. Connection services are provided including network layer flow control, network layer error control and packet sequence control.
4. Breaks larger packets into small packets.



# Transport Layer - OSI Model

## Functions of Transport Layer

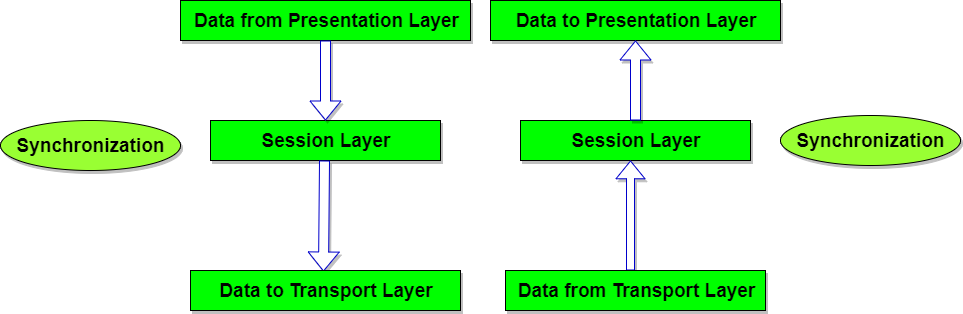
1. **Service Point Addressing:** Transport Layer header includes service point address which is port address. This layer gets the message to the correct process on the computer unlike Network Layer, which gets each packet to the correct computer.
2. **Segmentation and Reassembling:** A message is divided into segments; each segment contains sequence number, which enables this layer in reassembling the message. Message is reassembled correctly upon arrival at the destination and replaces packets which were lost in transmission.
3. **Connection Control:** It includes 2 types:
   * Connectionless Transport Layer : Each segment is considered as an independent packet and delivered to the transport layer at the destination machine.
   * Connection Oriented Transport Layer : Before delivering packets, connection is made with transport layer at the destination machine.
4. **Flow Control:** In this layer, flow control is performed end to end.
5. **Error Control:** Error Control is performed end to end in this layer to ensure that the complete message arrives at the receiving transport layer without any error. Error Correction is done through retransmission.



# Session Layer - OSI Model

## Functions of Session Layer

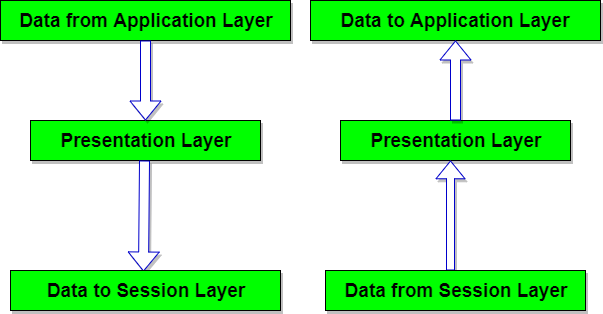
1. **Dialog Control :**This layer allows two systems to start communication with each other in half-duplex or full-duplex.
2. **Token Management:**This layer prevents two parties from attempting the same critical operation at the same time.
3. **Synchronization :**This layer allows a process to add checkpoints which are considered as synchronization points into stream of data. Example: If a system is sending a file of 800 pages, adding checkpoints after every 50 pages is recommended. This ensures that 50 page unit is successfully received and acknowledged. This is beneficial at the time of crash as if a crash happens at page number 110; there is no need to retransmit 1 to100 pages.



# Presentation Layer - OSI Model

## Functions of Presentation Layer

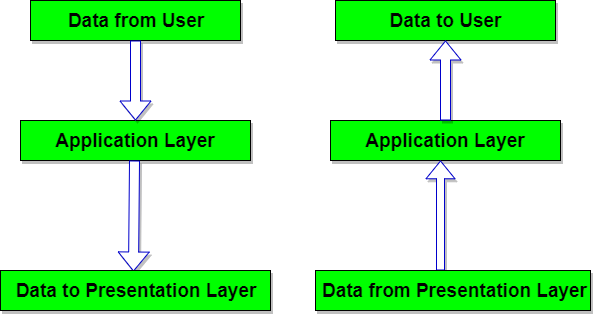
1. **Translation:** Before being transmitted, information in the form of characters and numbers should be changed to bit streams. The presentation layer is responsible for interoperability between encoding methods as different computers use different encoding methods. It translates data between the formats the network requires and the format the computer.
2. **Encryption:** It carries out encryption at the transmitter and decryption at the receiver.
3. **Compression:** It carries out data compression to reduce the bandwidth of the data to be transmitted. The primary role of Data compression is to reduce the number of bits to be 0transmitted. It is important in transmitting multimedia such as audio, video, text etc.



# Application Layer - OSI Model

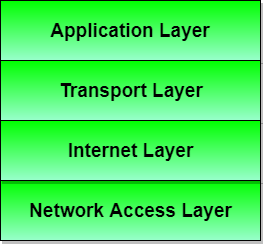
## Functions of Application Layer

1. **Mail Services:** This layer provides the basis for E-mail forwarding and storage.
2. **Network Virtual Terminal:** It allows a user to log on to a remote host. The application creates software emulation of a terminal at the remote host. User's computer talks to the software terminal which in turn talks to the host and vice versa. Then the remote host believes it is communicating with one of its own terminals and allows user to log on.
3. **Directory Services:** This layer provides access for global information about various services.
4. **File Transfer, Access and Management (FTAM):** It is a standard mechanism to access files and manages it. Users can access files in a remote computer and manage it. They can also retrieve files from a remote computer.

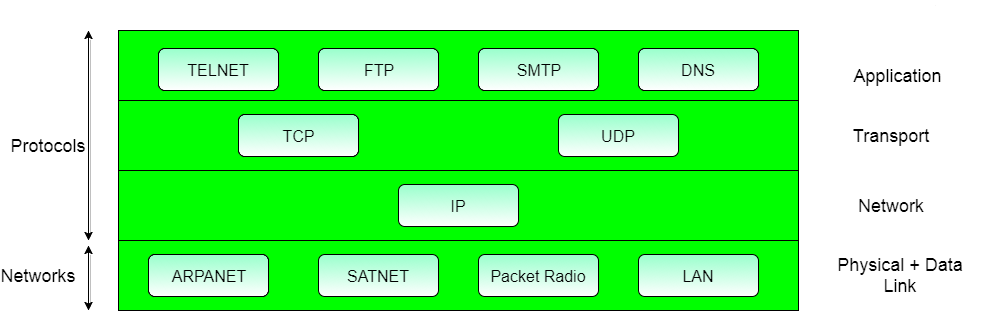


# The TCP/IP Reference Model

TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. **Protocols** are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination or the internet. They also offer simple naming and addressing schemes.



Protocols and networks in the TCP/IP model:



## Different Layers of TCP/IP Reference Model

Below we have discussed the 4 layers that form the TCP/IP reference model:

### Layer 1: Host-to-network Layer

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network.

### Layer 2: Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.
6. The various functions performed by the Internet Layer are:
   * Delivering IP packets
   * Performing routing
   * Avoiding congestion

### Layer 3: Transport Layer

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.

### Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. **TELNET** is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
2. **FTP**(File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. **SMTP**(Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. **DNS**(Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.
5. It allows peer entities to carry conversation.
6. It defines two end-to-end protocols: TCP and UDP
   * **TCP(Transmission Control Protocol):** It is a reliable connection-oriented protocol which handles byte-stream from source to destination without error and flow control.
   * **UDP(User-Datagram Protocol):** It is an unreliable connection-less protocol that do not want TCPs, sequencing and flow control. Eg: One-shot request-reply kind of service.

## Merits of TCP/IP model

1. It operated independently.
2. It is scalable.
3. Client/server architecture.
4. Supports a number of routing protocols.
5. Can be used to establish a connection between two computers.

## Demerits of TCP/IP

1. In this, the transport layer does not guarantee delivery of packets.
2. The model cannot be used in any other application.
3. Replacing protocol is not easy.
4. It has not clearly separated its services, interfaces and protocols.

# Comparison of OSI and TCP/IP Reference Model

Now it's time to compare both the reference model that we have learned till now. Let's start by addressing the similarities that both of these models have.

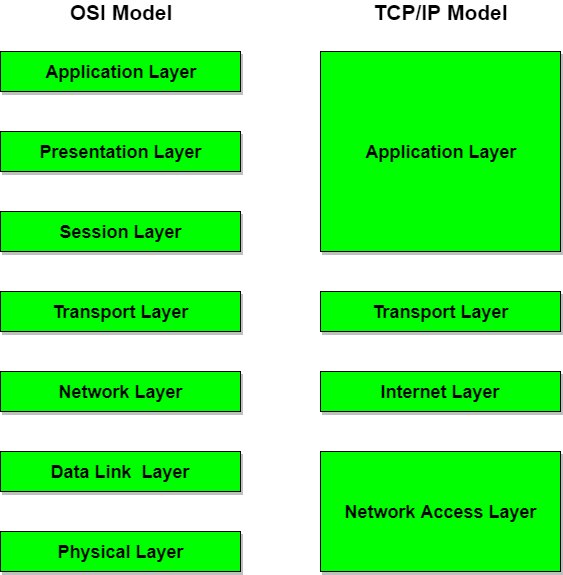
Following are some **similarities** between OSI Reference Model and TCP/IP Reference Model.

* Both have layered architecture.
* Layers provide similar functionalities.
* Both are protocol stack.
* Both are reference models.

## Difference between OSI and TCP/IP Reference Model

|  |  |
| --- | --- |
| **OSI(Open System Interconnection)** | **TCP/IP(Transmission Control Protocol / Internet Protocol)** |
| 1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user. | 1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network. |
| 2. In OSI model the transport layer guarantees the delivery of packets. | 2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable. |
| 3. Follows vertical approach. | 3. Follows horizontal approach. |
| 4. OSI model has a separate Presentation layer and Session layer. | 4. TCP/IP does not have a separate Presentation layer or Session layer. |
| 5. Transport Layer is Connection Oriented. | 5. Transport Layer is both Connection Oriented and Connection less. |
| 6. Network Layer is both Connection Oriented and Connection less. | 6. Network Layer is Connection less. |
| 7. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool. | 7. TCP/IP model is, in a way implementation of the OSI model. |
| 8. Network layer of OSI model provides both connection oriented and connectionless service. | 8. The Network layer in TCP/IP model provides connectionless service. |
| 9. OSI model has a problem of fitting the protocols into the model. | 9. TCP/IP model does not fit any protocol |
| 10. Protocols are hidden in OSI model and are easily replaced as the technology changes. | 10. In TCP/IP replacing protocol is not easy. |
| 11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent. | 11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent. |
| 12. It has 7 layers | 12. It has 4 layers |

### Diagrammatic Comparison between OSI Reference Model and TCP/IP Reference Model



* **A critique of OSI and TCP/IP**

The OSI Model is often criticised as being overly complex, offering too many choices. It is usually contrasted with the Internet, or TCP/IP protocol suite by such critics. It is hard to separate the implementation from the specification when analysing these criticisms. For example, the idea that there are <#1644#>*too many*<#1644#> layers, simply does not hold water. A TP4/CLNP (the ISO Connection Oriented Transport Protocol in its appropriate class for running over the ISO datagram network protocol) implementation could be almost exactly as efficient as a TCP/IP one. Indeed there exist implementations that are. The model has its use as a reference to compare different protocol systems, and should be considered a major success as that model. The ISO protocols that instantiate the model in ISO stacks are a completely separate matter. The concept of layers introduced in the OSI model has two motivations:

1. Primarily technically, but secondarily politically, it is a modularisation technique, taken from software engineering, and re-applied to the systems engineering of communications architectures (a term used instead of model).
2. Secondarily technically, but primarily politically, each layer (module) can be implemented by a different supplier, to a service specification, and must only rely on the service specifications of other layers(modules)

* **Examples of network**

Internet

Internet is defined as an Information super Highway, to access information over the web. However, It can be defined in many ways as follows:

* Internet is a world-wide global system of interconnected computer networks.
* Internet 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 location.
* A special computer DNS (Domain Name Server) is used to give name to the IP Address so that user can locate a computer by a name.
* For example, a DNS server will resolve a name **http://www.tutorialspoint.com** to a particular IP address to uniquely identify the computer on which this website is hosted.
* Internet is accessible to every user all over the world.

