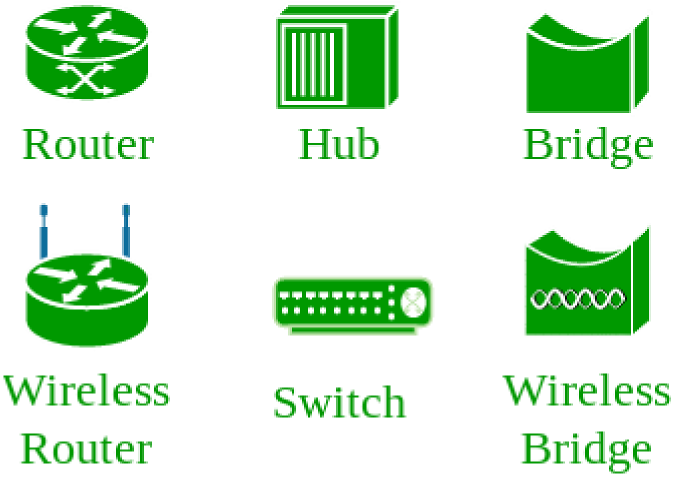
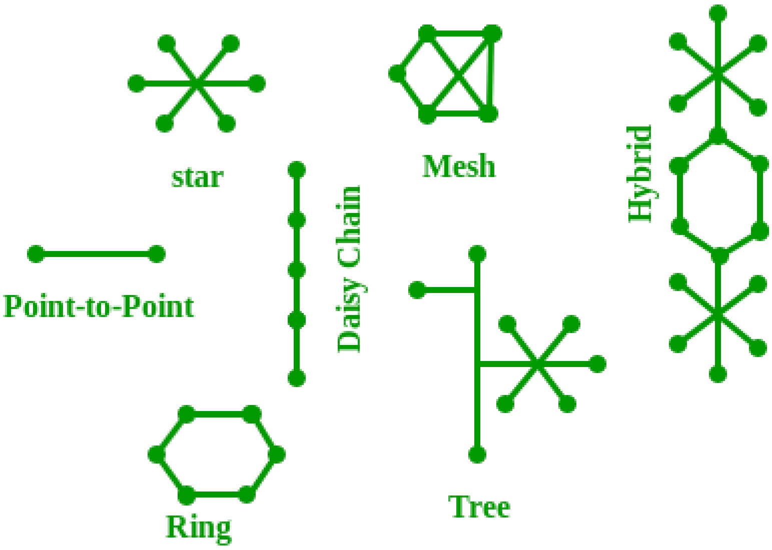
Basics of Computer Networking

Open system:
A system which is connected to the network and is ready for communication.
Closed system:
A system which is not connected to the network and can't be communicated with.
Computer Network:
An interconnection of multiple devices, also known as hosts, that are connected using multiple paths for the purpose of sending/receiving data or media. Computer networks can also include multiple devices/mediums which help in the communication between two different devices; these are known as **Network devices** and include things such as routers, switches, hubs, and bridges.



Network Topology:
The layout arrangement of the different devices in a network. Common examples include: Bus, Star, Mesh, Ring, and Daisy chain.



OSI:

OSI stands for **Open Systems Interconnection**. It is a reference model that specifies standards for communications protocols and also the functionalities of each layer.

Protocol:

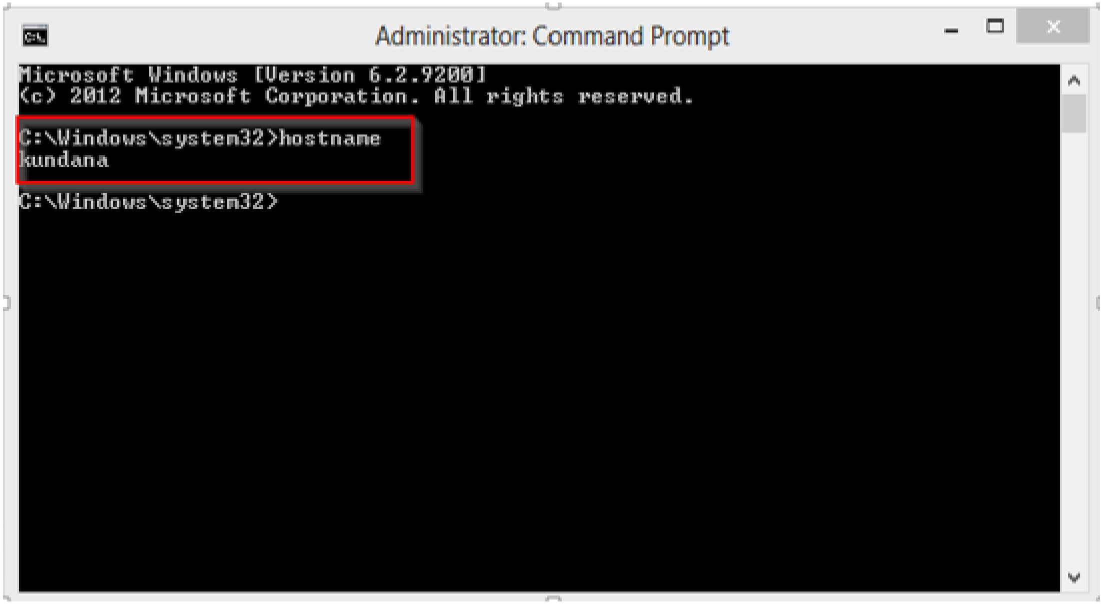
A protocol is the set of rules or algorithms which define the way how two entities can communicate across the network and there exists different protocol defined at each layer of the OSI model. Few of such protocols are TCP, IP, UDP, ARP, DHCP, FTP and so on.

UNIQUE IDENTIFIERS OF NETWORK

Host name:

Each device in the network is associated with a unique device name known as Hostname.

Type “hostname” in the command prompt(Administrator Mode) and press ‘Enter’, this displays the hostname of your machine.



```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\system32>hostname
kundana

C:\Windows\system32>
```

IP Address (Internet Protocol address):

Also known as the Logical Address, the IP Address is the network address of the system across the network.

To identify each device in the world-wide-web, the Internet Assigned Numbers Authority (IANA) assigns an IPV4 (Version 4) address as a unique identifier to each device on the Internet.

The length of an IPv4 address is 32-bits, hence, we have 2^{32} IP addresses available. The length of an IPv6 address is 128-bits.

Type "ipconfig" in the command prompt and press 'Enter', this gives us the IP address of the device.

MAC Address (Media Access Control address):

Also known as physical address, the MAC Address is the unique identifier of each host and is associated with its NIC (Network Interface Card).

A MAC address is assigned to the NIC at the time of manufacturing.

The length of the MAC address is : 12-nibble/ 6 bytes/ 48 bits

Type "ipconfig/all" in the command prompt and press 'Enter', this gives us the MAC address.

Port:

A port can be referred to as a logical channel through which data can be sent/received to an application. Any host may have multiple applications running, and each of these applications is identified using the port number on which they are running.

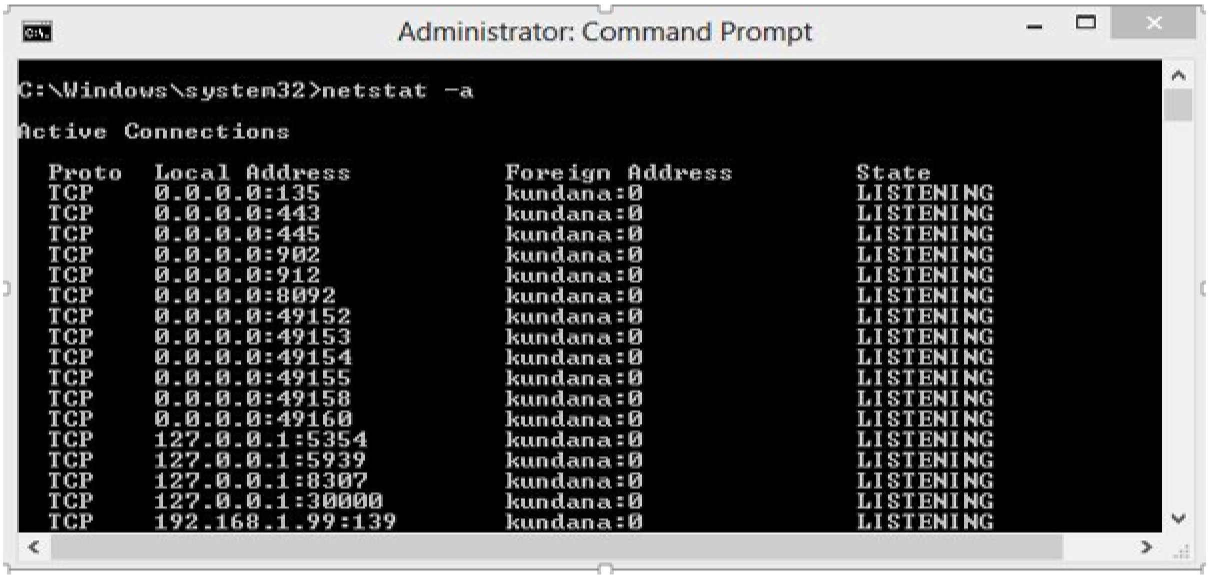
A port number is a 16-bit integer, hence, we have 2^{16} ports available which are categorized as shown below:

Port Types	Range
Well known Ports	0 – 1023
Registered Ports	1024 – 49151
Ephemeral Ports	49152 – 65535

Number of ports: 65,536

Range: 0 – 65535

*Type "**netstat -a**" in the command prompt and press 'Enter', this lists all the ports being used.*



```
C:\Windows\system32>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            kundana:0              LISTENING
  TCP    0.0.0.0:443            kundana:0              LISTENING
  TCP    0.0.0.0:445            kundana:0              LISTENING
  TCP    0.0.0.0:902            kundana:0              LISTENING
  TCP    0.0.0.0:912            kundana:0              LISTENING
  TCP    0.0.0.0:8092           kundana:0              LISTENING
  TCP    0.0.0.0:49152          kundana:0              LISTENING
  TCP    0.0.0.0:49153          kundana:0              LISTENING
  TCP    0.0.0.0:49154          kundana:0              LISTENING
  TCP    0.0.0.0:49155          kundana:0              LISTENING
  TCP    0.0.0.0:49158          kundana:0              LISTENING
  TCP    0.0.0.0:49160          kundana:0              LISTENING
  TCP    127.0.0.1:5354         kundana:0              LISTENING
  TCP    127.0.0.1:5939         kundana:0              LISTENING
  TCP    127.0.0.1:8307         kundana:0              LISTENING
  TCP    127.0.0.1:30000        kundana:0              LISTENING
  TCP    192.168.1.99:139       kundana:0              LISTENING
```

Socket:

The unique combination of IP address and Port number together are termed as Socket.

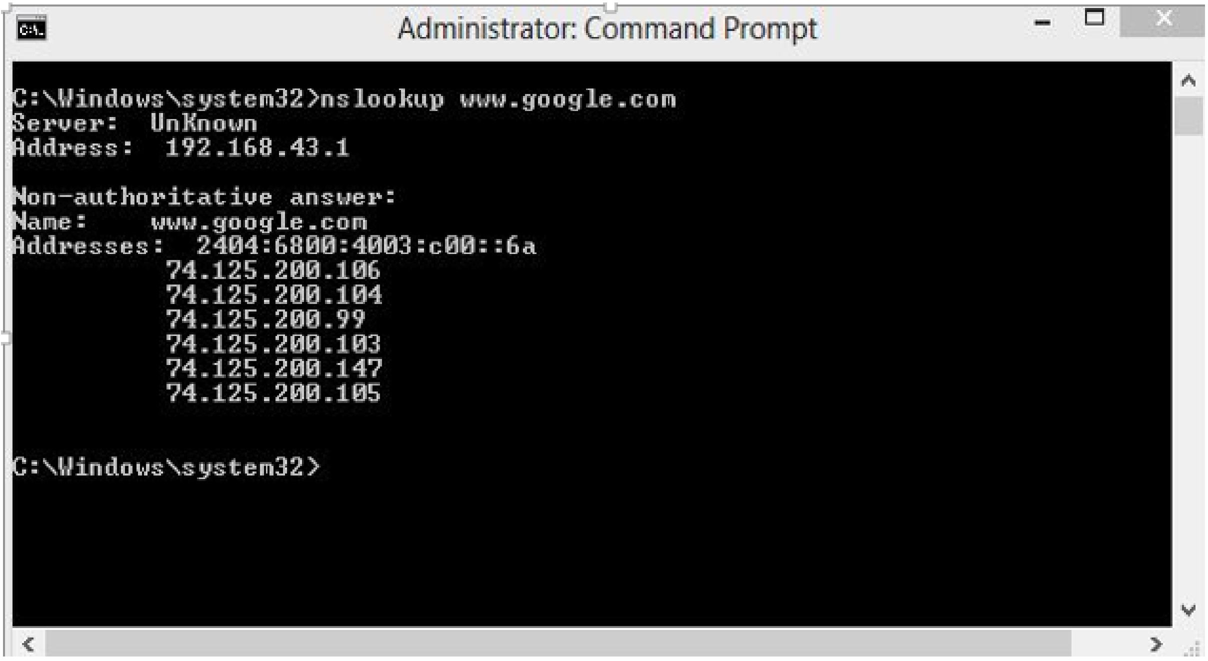
<u>Other related concepts</u>

DNS Server:

DNS stands for **Domain Name system**.

DNS is basically a server which translates web addresses or URLs (ex: www.google.com) into their corresponding IP addresses. We don't have to remember all the IP addresses of each and every website.

The command '**nslookup**' gives you the IP address of the domain you are looking for. This also provides the information of our DNS Server.



```
C:\Windows\system32>nslookup www.google.com
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4003:c00::6a
          74.125.200.106
          74.125.200.104
          74.125.200.99
          74.125.200.103
          74.125.200.147
          74.125.200.105


C:\Windows\system32>
```

ARP:

ARP stands for **Address Resolution Protocol**.

It is used to convert an IP address to its corresponding physical address(i.e., MAC Address).
ARP is used by the Data Link Layer to identify the MAC address of the Receiver's machine.
RARP:
RARP stands for **Reverse Address Resolution Protocol**.
As the name suggests, it provides the IP address of the device given a physical address as input. But RARP has become obsolete since the time DHCP has come into the picture.

The Internet and the Web

1. The Internet:
In simplest terms, the Internet is a global network comprised of smaller networks that are interconnected using **standardized** communication protocols. The Internet standards describe a framework known as the Internet protocol suite. This model divides methods into a *layered system of protocols.*
These layers are as follows:

1. **Application layer (highest) –** concerned with the data(URL, type, etc.). This is where HTTP, HTTPS, etc., comes in.

2. **Transport layer –** responsible for end-to-end communication over a network.

3. **Network layer –** provides data route.

The Internet provides a variety of information and communication facilities; contains forums, databases, email, hypertext, etc. It consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies.

2. The World Wide Web:
The Web is a only way to access information through the Internet. It's a system of Internet servers that support specially formatted documents. The documents are formatted in a markup language called **HTML**, or "HyperText Markup Language", which supports a number of features including links and multimedia. These documents are interlinked using hypertext links and are accessible via the Internet.
To link hypertext to the Internet, we need:

1. The markup language, i.e., HTML.
2. The transfer protocol, e.g., HTTP.
3. Uniform Resource Locator (URL), the address of the resource.

We access the Web using **Web browsers**.
Difference between Web and Internet:

Internet	Web
The Internet is the network of networks and the network allows to exchange of the data between two or more computers.	The Web is a way to access Information through the Internet.
It is also known as Network of Networks.	The Web is a model for sharing information using Internet.
The Internet is a way of transporting information between devices.	The protocol used by the web is Http.
	The Web is accessed by the Web Browser.

URI:
URI stands for **'Uniform Resource Identifier'** . A URI can be a name, locator, or both for an online resource whereas a URL is just the locator. URLs are a subset of URIs. A URL is human-readable text that was designed to replace the numbers (IP addresses) that computers use to communicate with servers.
A URL consists of a protocol, domain name, and path (which includes the specific subfolder structure where a page is located) like-

protocol://WebSiteName.topLevelDomain/path

1. Protocol – Http or Https.
2. WebSiteName – geeksforgeeks, google etc.
3. topLevelDomain- .com, .edu, .in etc.

4. path- specific folders and/or subfolders that are on a given website.

Who governs the Internet?
The Internet is not governed and has no single authority figure. The ultimate authority for where the Internet is going rests with **the Internet Society**, or ISOC.
ISOC is a voluntary membership organization whose purpose is to promote global information exchange through Internet technology.

- ISOC appoints the **IAB- Internet Architecture Board**. They meet regularly to review standards and allocate resources, like addresses.

- **IETF- Internet Engineering Task Force**. Another volunteer organization that meets regularly to discuss operational and technical problems.

Internet and Web programming

The Internet is a vast network of computers, and server's, which communicate with each other. The internet connect's with the whole wide world together. How does it actually work at a very low level?

Client side:
First when we type a url like www.google.com, the browser converts it into a file containing:

1. GET /HTTP/1.1 (where GET means we are requesting some data from the server and HTTP refers to protocol that we are using, 1.1 refers to version of HTTP request)
2. Host: www.google.com
3. And some other information

Now this file is converted to binary code by the browser and it is sent down the wires if we are connected through Ethernet and if we are using WiFi, first it converts it to radio signal which is decoded by router in a very low level. It is converted to binary and then sent to the servers.

This information or 'binary codes' go to the destination and respond if it is received by the sender only because of the IP address.

One router will send the information to another and this keeps on going until the binary codes reach the destination.

Server side:

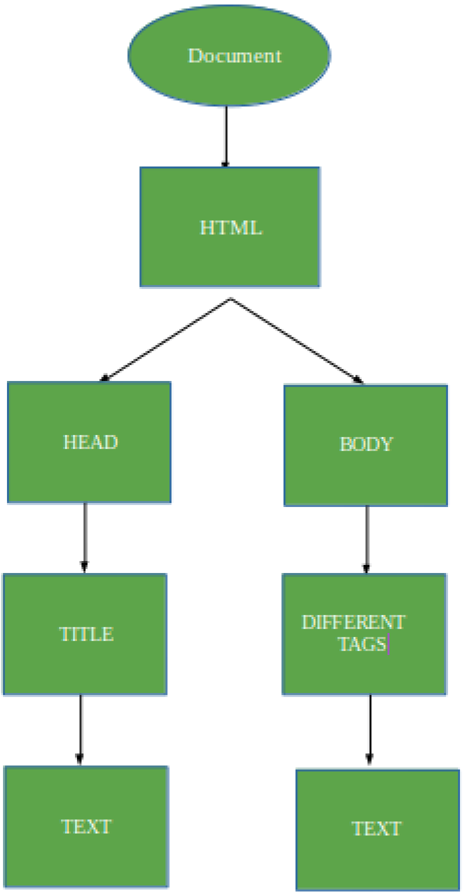
Now the server receives the binary code and decodes it and sends the response in the following manner:

1. HTTP/1.1 200 ok (where 200 ok is the status)
2. Content-type:type/html
3. Body of page

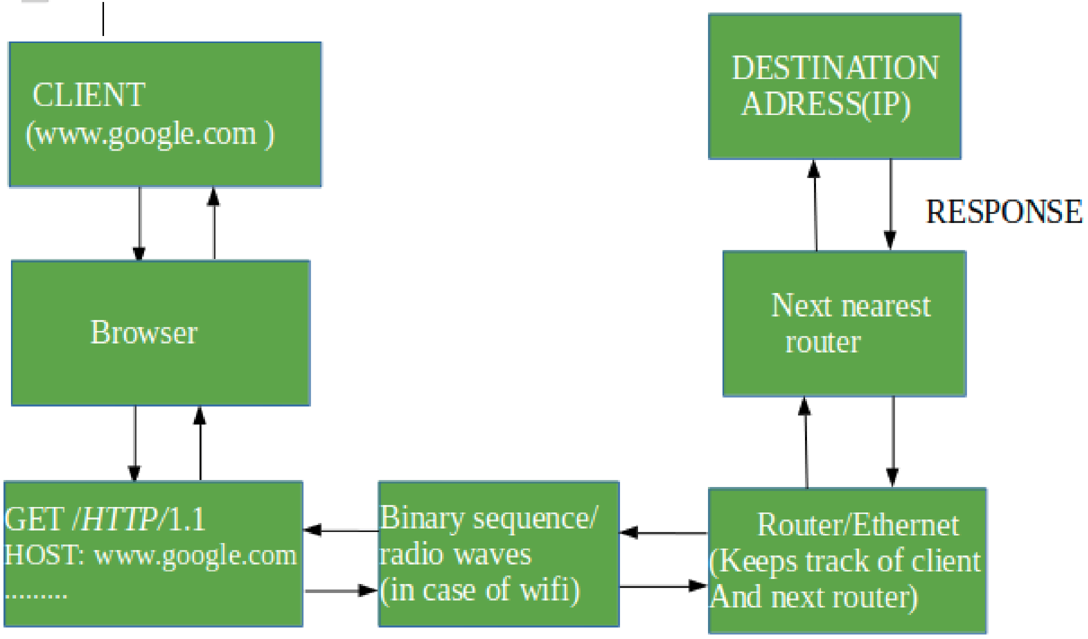
Now this is converted back to binary by the server and sent to the IP address that is requesting it. Once the codes are received by the client, the browser again decodes the information in the following way:

1. First it checks the status
2. It starts reading the document from html tag and constructs a Tree like structure.
3. The html tree is then converted to corresponding binary code and rendered on the screen.
4. In the end we see the website front-end.

Below is the tree structure of html document:



The following diagram show the whole process:



Internet of Everything

Internet Of Everything (IoE) has been the one of the trendiest topic lately and it's here, IoE is the upcoming most innovative and Ubiquitous technology advancement which is going to make networked connections more relevant and valuable than ever before. Turning information into action that creates new capabilities, richer experiences and unprecedented economic opportunities for businesses, individuals and countries.

Technically IoE refers to billions of devices and consumer products connected to the internet in an intelligent networked environment with expanded digital features.

It is basically a philosophy in which our technology future is compromised of different types of appliances, devices, and things connected to the global internet. As of now the internet connection is only restricted to Phone's/Tablet's, PC's and a handful of other devices but the idea behind IoE is that in the future, Machines will become more intelligent and cognitive by having more access to data and expanded network opportunities.

In simpler terms IoE is the intelligent connection of *people, process, data and things* that will be transforming our world in such a way that there will be billions of connected devices having sensors to detect, measure and access their status all of which will be connected over public or private network built over standard protocols like TCP/IP.

So how is the; *Internet of Everything* any different from the Internet of Things? Well, the difference is the **intelligent connection**. IoT is mostly about physical devices and objects communicating with each other but IoE brings with it the network intelligence to bind all these concepts together into a cohesive system.

IOT has been limited to only machines thus achieving Machine to Machine Communication but IoE brings together people, process, data, and things and adds them into the network therefore not just Phone's/Tablet's and PC's but People. Health Fitness band's, Coffee Pot's, Marine Container's all become a Node in an intelligent network communicating with each other. The more expansive IoE concepts include, besides M2M communication, M2P, and technology-assisted P2P communication.

The IoE Economy will profoundly effect four major Aspects of our lives:

1. **People –**
   People will be connected to the internet in more relevant ways and will be generating data and interacting with devices by not only through Mobile's/Tablet's, PC's and Social Network but also through Sensors placed on human skins or sewn into clothing which will provide a person's vital signs. In this way, people will themselves becomes Nodes on the internet.
   A good example is Nike's wearable fitness band's which read a person's vital signs and sports apparel's and gears embedded with chips which track the performance of Athletes.

2. **Things –**
   Things and physical items such as sensors, industry devices, consumer products, enterprise assets will be connected to the internet or to each other, also fetching information from its surrounding's, will be more context-aware, more cognitive, more intelligent, often so-called the internet of things.
   As of 1984, only 1000 devices were connected to the internet which increased to about 1 million in 1992 and shot across 10 Billion in 2010 and as Cisco predicts there will be around 50 Billion devices connected to the internet by 2020. These devices will be fetching data from its environment internally or externally and sending it back to the server for analyzing and making much more intelligent decisions.

3. **Data –**
   Rather than simply collection Raw data, these connected devices will be sending higher level, more processed data back to respective servers for faster evaluation or more intelligent decision making.
   Here the data is more about insightful information and action plan than just random chunk. Figuring out a way to decipher the right flow of

information is the key to making the best use of Big Data and as the types of data and sources increase, in order to draw useful insight's there will be a need to classify information and analyze it.

4. **Process –**
   With the equivalent to IOE process, the right information will be delivered to the right person at the right time in an appropriate way. Technology-based Businesses will be relying on data to make further decisions and advance their workflow processes and strategies and will be therefore competing to leverage the data faster than their competitors for an agile and faster decision making.

General Electrics predicts that IoE can add 15 trillion dollars to the Global Domestic Product while Cisco estimates 19 trillion in savings and profits for companies that can leverage IoE. But as the number of devices connected to the internet increase and therefore collect more data, privacy is put at risk which increases security concerns but as these devices grow more intelligent, hopes is that the device and network will grow knowledgeable enough to detect, stop and prevent any harmful threats. IoE is here and is inevitable, we should embrace ourselves to adapt our lives to the changes that it brings with it.

Goals of Networks

Computer Network means an interconnection of autonomous (standalone) computers for information exchange. The connecting media could be a copper wire, optical fiber, microwave, or satellite.

Networking Elements – The computer network includes the following networking elements:

1. At least two computers
2. Transmission medium either wired or wireless
3. Protocols or rules that govern the communication
4. Network software such as Network Operating System

Network Criteria:

The criteria that have to be met by a computer network are:

1. Performance – It is measured in terms of transit time and response time.

- Transit time is the time for a message to travel from one device to another
- Response time is the elapsed time between an inquiry and a response.

Performance is dependent on the following factors:

- The number of users
- Type of transmission medium

- Capability of connected network
- Efficiency of software

2. Reliability – It is measured in terms of

- Frequency of failure
- Recovery from failures
- Robustness during catastrophe

3. Security – It means protecting data from unauthorized access.

Goals of Computer Networks: The following are some important goals of computer networks:

1. **Resource Sharing –**
   Many organization has a substantial number of computers in operations, which are located apart. Ex. 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 more 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.

Line Configuration in Computer Networks

A network is two or more devices connected through a link. A link is a communication pathway that transfer data from one device to another. Devices can be a computer, printer or any other device that is capable to send and receive data. For visualization purpose, imagine any link as a line drawn between two points.
For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections:

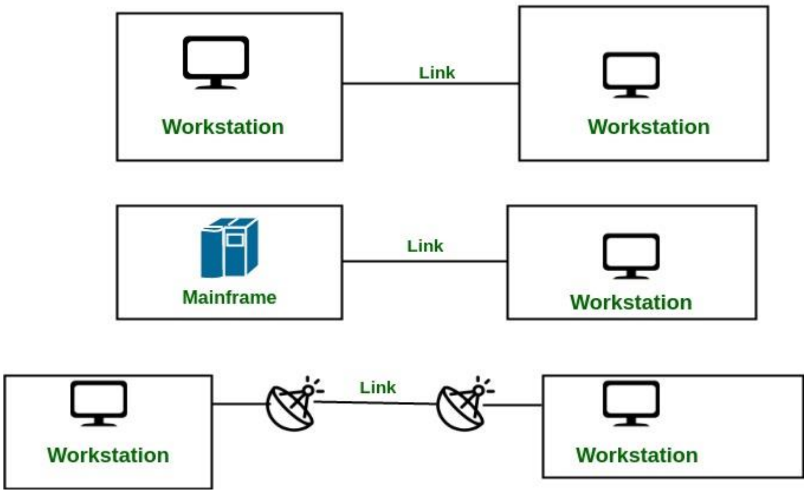
1. **Point-to-Point Connection**

2. **Multipoint Connection**

Point-to-Point Connection :

1. A point-to-point connection provides a dedicated link between two devices.
2. The entire capacity of the link is reserved for transmission between those two devices.
3. Most point-to-point connections use a actual length of wire or cable to connect the two end, but other options such as microwave or satellite links are also possible.
4. Point to point network topology is considered to be one of the easiest and most conventional network topologies.
5. It is also the simplest to establish and understand.

Example: Point-to-Point connection between remote control and Television for changing the channels.

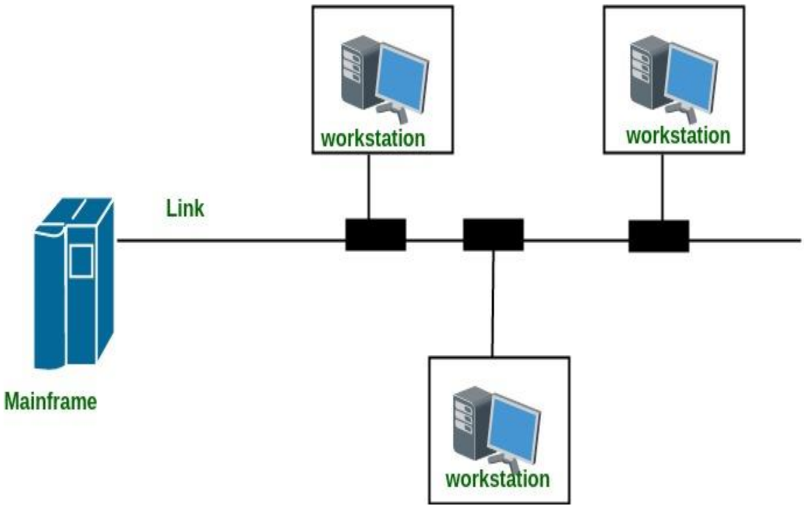


Multipoint Connection :

1. It is also called Multidrop configuration. In this connection two or more devices share a single link.
2. More than two devices share the link that is the capacity of the channel is shared now. With shared capacity, there can be two possibilities in a Multipoint Line configuration:

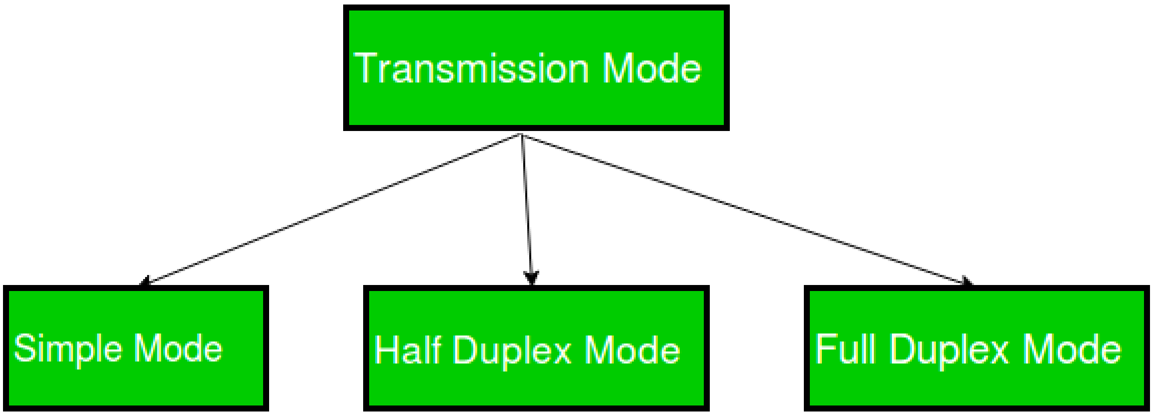
Spatial Sharing: If several devices can share the link simultaneously, its called Spatially shared line configuration.

Temporal (Time) Sharing: If users must take turns using the link , then its called Temporally shared or Time Shared Line configuration.



Transmission Modes in Computer Networks (Simplex, Half-Duplex and Full-Duplex)

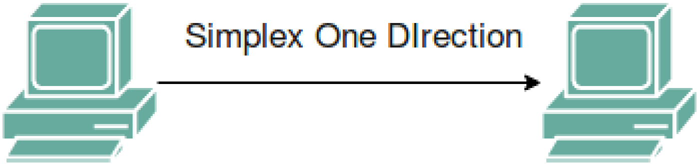
Transmission mode means transferring of data between two devices. It is also known as communication mode. Buses and networks are designed to allow communication to occur between individual devices that are interconnected. There are three types of transmission mode:-



These are explained as following below.

1. Simplex Mode –
In Simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit, the other can only receive. The

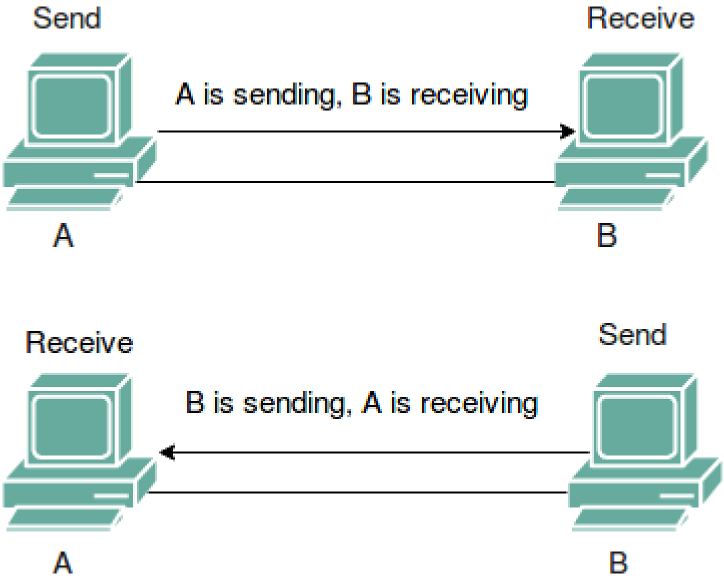
simplex mode can use the entire capacity of the channel to send data in one direction.
Example: Keyboard and traditional monitors. The keyboard can only introduce input, the monitor can only give the output.



2. Half-Duplex Mode –

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is used in cases where there is no need for communication in both direction at the same time. The entire capacity of the channel can be utilized for each direction.
Example: Walkie- talkie in which message is sent one at a time and messages are sent in both the directions.

```
Channel capacity=Bandwidth * Propagation Delay
```



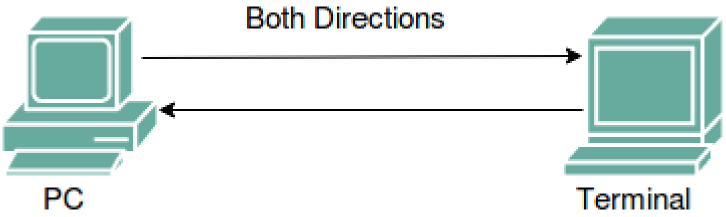
3. Full-Duplex Mode –

In full-duplex mode, both stations can transmit and receive simultaneously. In full_duplex mode, signals going in one direction share the capacity of the link with signals going in other direction, this sharing can occur in two ways:

- Either the link must contain two physically separate transmission paths, one for sending and other for receiving.
- Or the capacity is divided between signals travelling in both directions.

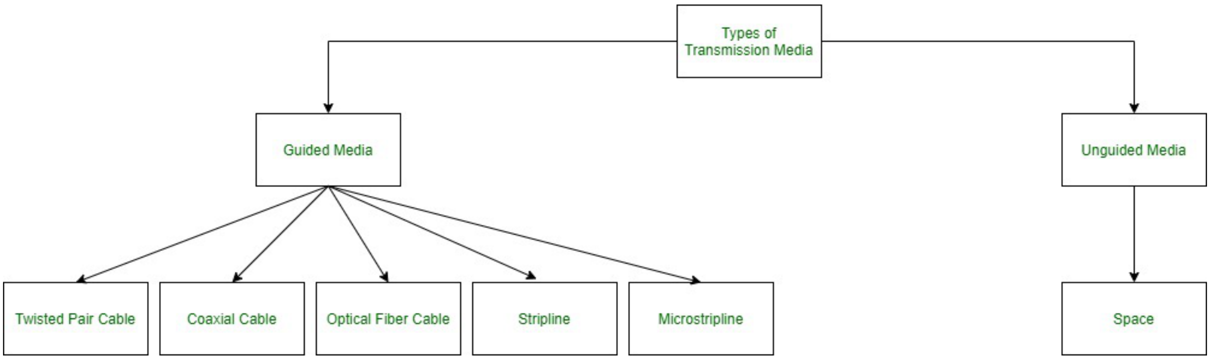
Full-duplex mode is used when communication in both direction is required all the time. The capacity of the channel, however must be divided between the two directions.
Example: Telephone Network in which there is communication between two persons by a telephone line, through which both can talk and listen at the same time.

```
Channel Capacity=2* Bandwidth*propagation Delay
```



Types of Transmission Media

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



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

- High Speed
- Secure
- Used for comparatively shorter distances

There are 3 major types of Guided Media:

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

1. **Unshielded Twisted Pair (UTP):**
   This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.
   Advantages:
   - Least expensive
   - Easy to install
   - High-speed capacity
   - Susceptible to external interference
   - Lower capacity and performance in comparison to STP
   - Short distance transmission due to attenuation
2. **Shielded Twisted Pair (STP):**
   This type of cable consists of a special jacket to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.
   Advantages:
   - Better performance at a higher data rate in comparison to UTP
   - Eliminates crosstalk
   - Comparatively faster
   - Comparatively difficult to install and manufacture
   - More expensive
   - Bulky

(ii) Coaxial Cable –

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

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

Disadvantages:

- Single cable failure can disrupt the entire network

(iii) Optical Fibre Cable –

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

The cable can be unidirectional or bidirectional. The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bidirectional mode.

Advantages:

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

Disadvantages:

- Difficult to install and maintain
- High cost
- Fragile

(iv) Stripline

Stripline is a transverse electromagnetic (TEM) transmission line medium invented by Robert M. Barrett of the Air Force Cambridge Research Centre in the 1950s. Stripline is the earliest form of the planar transmission line. It uses a conducting material to transmit high-frequency waves it is also called a waveguide. This conducting material is sandwiched between two layers of the ground plane which are usually shorted to provide EMI immunity.

(v) Microstripline

In this, the conducting material is separated from the ground plane by a layer of dielectric.

2. Unguided Media:

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

- The signal is broadcasted through air
- Less Secure
- Used for larger distances

There are 3 types of Signals transmitted through unguided media:

(i) Radiowaves –

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

(ii) Microwaves –

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

(iii) Infrared –

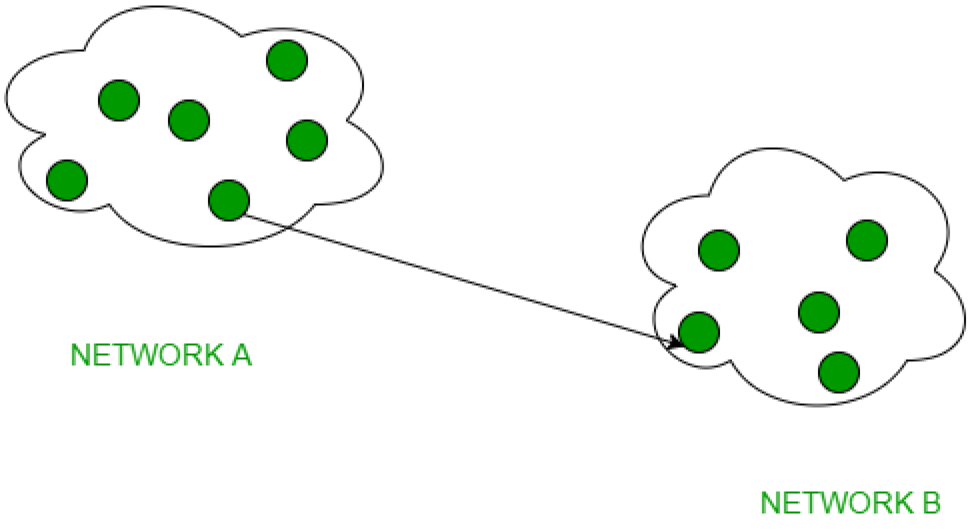
Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

Difference between Unicast, Broadcast and Multicast in Computer Network

The **cast** term here signifies some data(stream of packets) is being transmitted to the recipient(s) from client(s) side over the communication channel that helps them to communicate. Let's see some of the "cast" concepts that are prevailing in the computer networks field.

1. Unicast –

This type of information transfer is useful when there is a participation of single sender and single recipient. So, in short, you can term it as a one-to-one transmission. For example, a device having IP address 10.1.2.0 in a network wants to send the traffic stream(data packets) to the device with IP address 20.12.4.2 in the other network, then unicast comes into the picture. This is the most common form of data transfer over the networks.

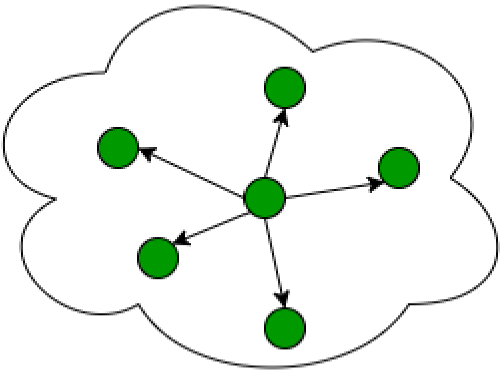


UNICAST EXAMPLE

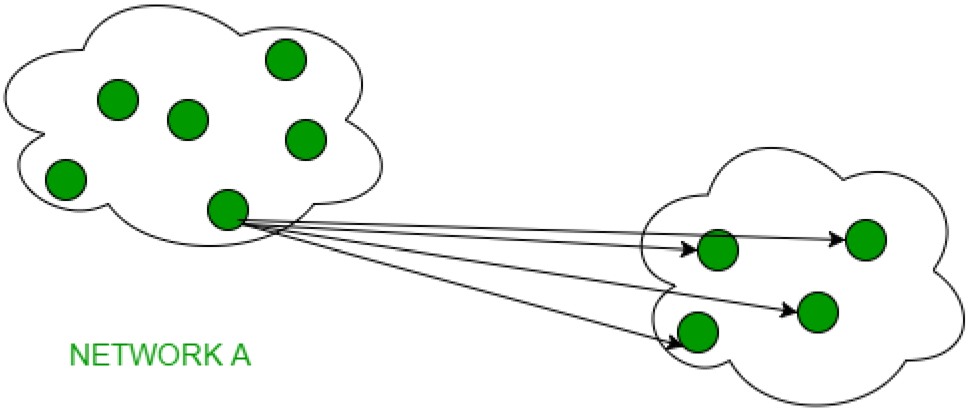
2. Broadcast –

Broadcasting transfer (one-to-all) techniques can be classified into two types :

- **Limited Broadcasting –**
  Suppose you have to send stream of packets to all the devices over the network that you reside, this broadcasting comes handy. For this to achieve, it will append 255.255.255.255 (all the 32 bits of IP address set to 1) called as **Limited Broadcast Address** in the destination address of the datagram (packet) header which is reserved for information transfer to all the recipients from a single client (sender) over the network.



- **Direct Broadcasting –**
  This is useful when a device in one network wants to transfer packet stream to all the devices over the other network. This is achieved by translating all the Host ID part bits of the destination address to 1, referred as **Direct Broadcast Address** in the datagram header for information transfer.



This mode is mainly utilized by television networks for video and audio distribution.
One important protocol of this class in Computer Networks is Address Resolution Protocol (ARP) that is used for resolving IP address into physical address which is necessary for underlying communication.

3. Multicast –

In multicasting, one/more senders and one/more recipients participate in data transfer traffic. In this method traffic recline between the boundaries of unicast (one-to-one) and broadcast (one-to-all). Multicast lets server's direct single copies of data streams that are then simulated and routed to hosts that request it. IP multicast requires support of some other protocols like **IGMP (Internet Group Management Protocol), Multicast routing** for its working. Also in Classful IP addressing **Class D** is reserved for multicast groups.
Questions Corner –
Practicing the following questions will help you test your knowledge. It is highly recommended that you practice them.

1. Direct Broadcast Address
2. Direct Broadcast Address
3. Direct Broadcast Address

Introduction to basic Networking terminology

For a specific purpose if things are connected together, are referred as a **NETWORK**. A network can be of many types, like a telephone network, television network, computer network or even a people network.
Similarly, a **COMPUTER NETWORK** is also a kind of setup, where it connects two or more devices to share a range of services and information in the form of **e-mails and messages**, **databases**, **documents**, **web-sites**, **audios and videoes**, **Telephone calls and video conferences** etc among them.
A **PROTOCOL** is nothing but set of defined **rules**, which has to be followed by every connected devices across a network to communicate and share information among them. To facilitates **End to End** communication, a number of protocols worked together to form a **Protocol Suites or Stacks**.
Some basic Protocols are:

- **IP** : Internet Protocol
- **FTP** : File Transfer Protocol
- **SMTP** : Simple Mail Transfer Protocol
- **HTTP** : Hyper Text Transfer Protocol

The **Network reference models** were developed to allow products from different manufacturers to interoperate on a network. A network reference model serves as a blueprint, detailing standards for how protocol communication should occur.
The most widely recognized reference models are, the **Open Systems Interconnect** (OSI) Model and **Department of Defense** (DoD, also known as TCP/IP) model.

Network Typesare often categorized by their size and functionality. According to the size, the network can be commonly categorized into**Three**types.

- **LANs (Local Area Networks)**
- **MANs (Metropolitan Area Networks)**
- **WANs (Wide Area Networks)**

An Internetwork is a general term describing multiple networks connected together. The Internet is the largest and most well-known internetwork.

Some networks are categorized by their function, as opposed to their size. For example:

- SAN **(Storage Area Network)**: A SAN provides systems with high-speed, lossless access to high-capacity storage devices.
- VPN **(Virtual Private Network)**: A VPN allows for information to be securely sent across a public or unsecure network, such as the Internet. Common uses of a VPN are to connect branch offices or remote users to a main office.

In a network, any connected device is called as***host***. A host can serve as following ways:

- A host can acts as a ***Client***, when he is requesting information.
- A host can acts as a ***Server***, when he provides information.
- A host can also request and provide information, is called ***Peer***.

Types of Network Topology

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 :

a) Mesh Topology :

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

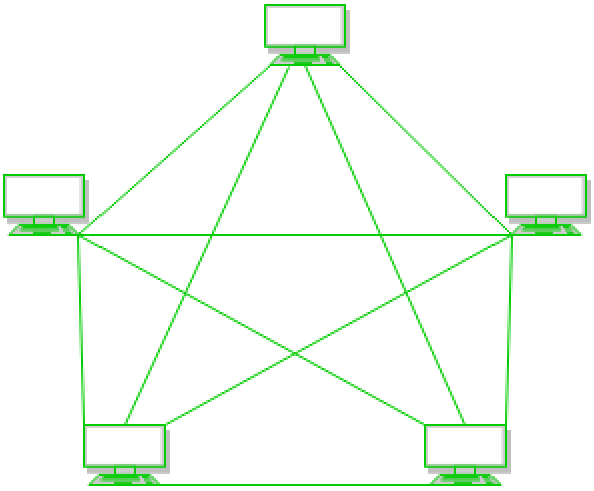


Figure 1 : Every device is connected with another via dedicated channels. These channels are known as links.

- If suppose, N number of devices are connected with each other in mesh topology, then total number of ports that is required by each device is ? N-1. In the Figure 1, there are 5 devices connected to each other, hence total number of ports required is 4.
- If suppose, N number of devices are connected with each other in mesh topology, then total number of dedicated links required to connect them is $^NC_2$ i.e. N(N-1)/2. In the Figure 1, there are 5 devices connected to each other, hence total number of links required is 5*4/2 = 10.

Advantages of this topology :

- It is robust.
- Fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

Problems with this topology :

- Installation and configuration is difficult.
- Cost of cables are high as bulk wiring is required, hence suitable for less number of devices.
- Cost of maintenance is high.

b) 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.

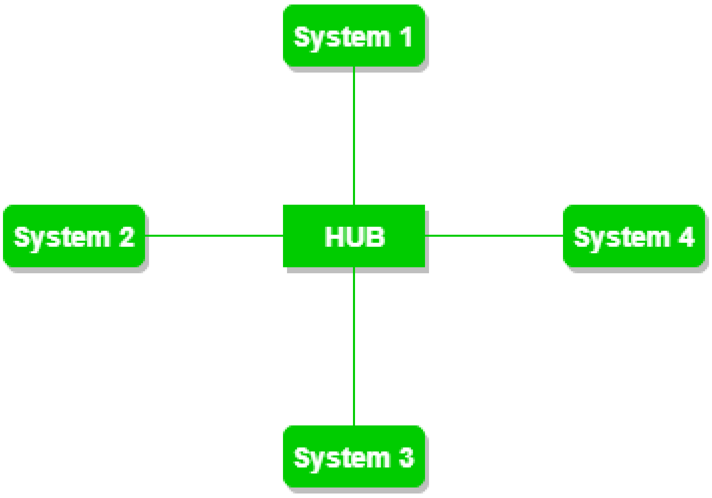


Figure 2 : A star topology having four systems connected to single point of connection i.e. hub.

Advantages of this topology :

- If N devices are connected to each other in star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device require only 1 port i.e. to connect to the hub.

Problems with this topology :

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- Cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

c) 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. It is multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

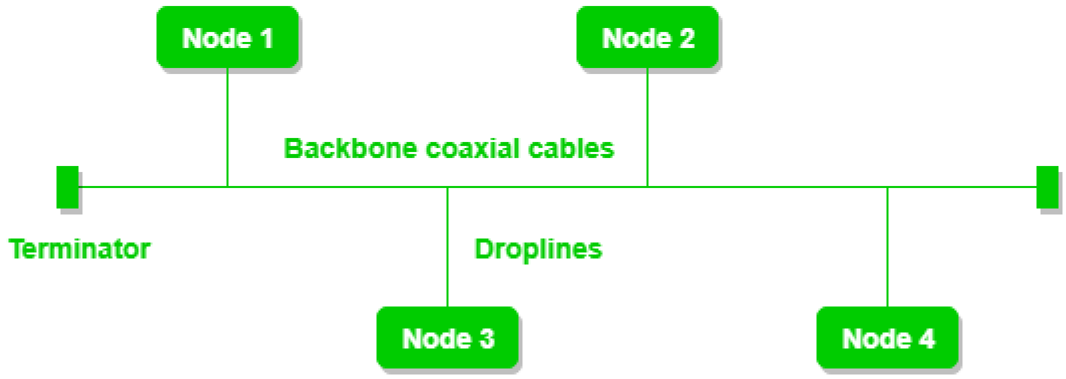


Figure 3 : A bus topology with shared backbone cable. The nodes are connected to the channel via drop lines.

Advantages of this topology :

- If N devices are connected to each other in bus topology, then the number of cables required to connect them is 1 ?which is known as backbone cable and N drop lines are required.
- Cost of the cable is less as compared to other topology, but it is used to built small networks.

Problems with this topology :

- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD etc.

d) Ring Topology :

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

A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.

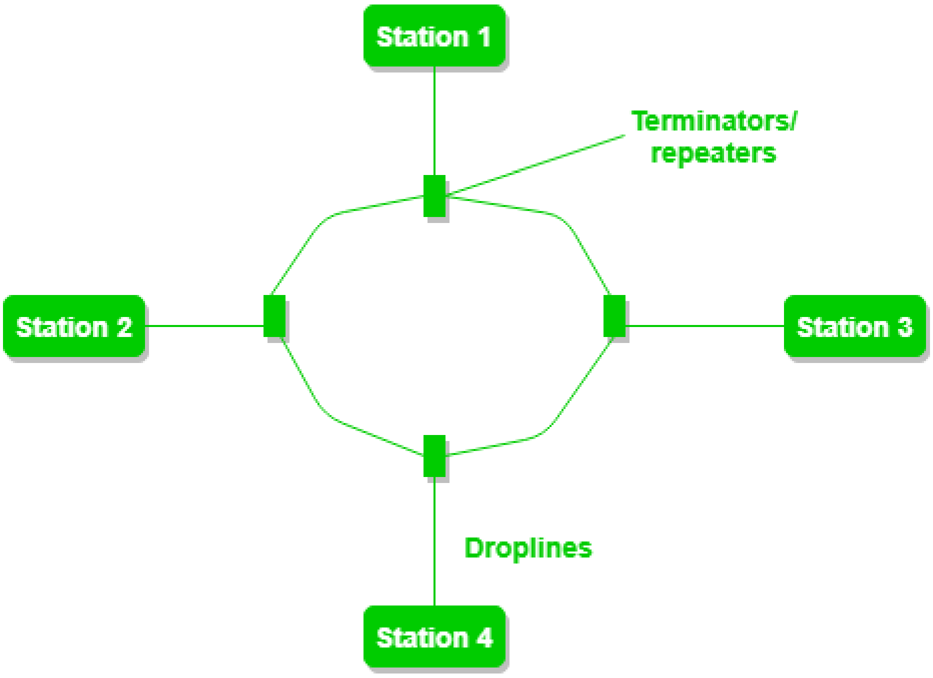


Figure 4 : A ring topology comprises of 4 stations connected with each forming a ring..

The following operations takes place in ring topology are :

1. One station is known as **monitor** station which takes all the responsibility to perform the operations.
2. To transmit the data, station has to hold the token. After the transmission is done, the token is to be released for other stations to use.
3. When no station is transmitting the data, then the token will circulate in the ring.
4. There are two types of token release techniques : **Early token release** releases the token just after the transmitting the data and **Delay token release** releases the token after the acknowledgement is received from the receiver.

Advantages of this topology :

- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.

Problems with this topology :

- Troubleshooting is difficult in this topology.
- Addition of stations in between or removal of stations can disturb the whole topology.

e) Tree Topology :

? This topology is the variation of Star topology. This topology have hierarchical flow of data.

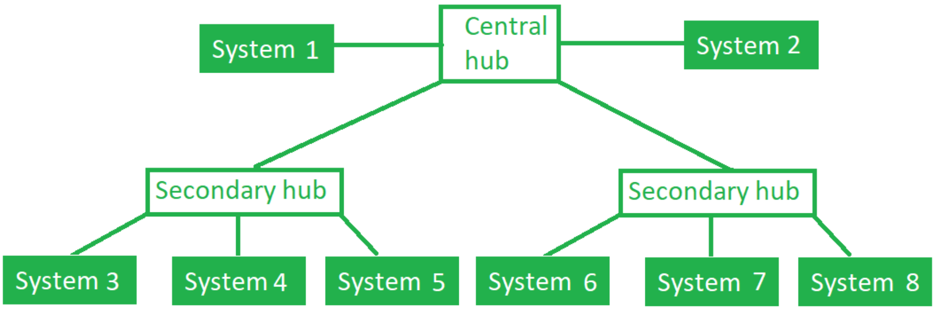


Figure 5 : In this the various secondary hubs are connected to the central hub which contains the repeater. In this data flow from top to bottom i.e from the central hub to secondary and then to the devices or from bottom to top i.e. devices to secondary hub and then to the central hub. It is multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

Advantages of this topology :

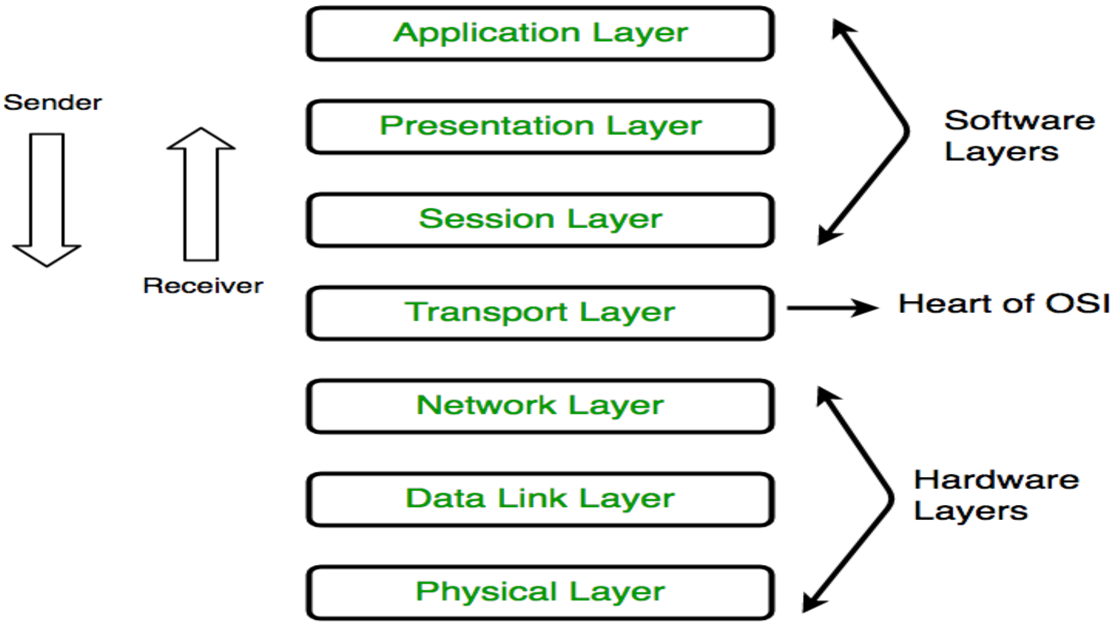
- It allows more devices to be attached to a single central hub thus it increases the distance that is travel by the signal to come to the devices.
- It allows the network to get isolate and also prioritize from different computers.

Problems with this topology :

- If the central hub gets fails the entire system fails.
- The cost is high because of cabling.

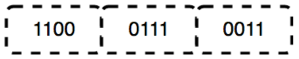
Layers of OSI Model

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



1. Physical Layer (Layer 1) :

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.** It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.



The functions of the physical layer are :

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

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

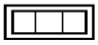
2. Data Link Layer (DLL) (Layer 2) :

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

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

The packet received from Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver’s MAC address in the header.

The Receiver’s MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking “Who has that IP address?” and the destination host will reply with its MAC address.



The functions of the data Link layer are :

1. **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
2. **Physical addressing:** After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
3. **Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
4. **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus , flow control coordinates that amount of data that can be sent before receiving acknowledgement.
5. **Access control:** When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

** Packet in Data Link layer is referred as **Frame**.*
*** Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.*
**** Switch & Bridge are Data Link Layer devices.*

3. Network Layer (Layer 3) :

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

1. **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.
2. **Logical Addressing:** In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

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

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

4. Transport Layer (Layer 4) :

Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

- **At sender's side:**

Transport layer receives the formatted data from the upper layers, performs **Segmentation** and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.

Note: The sender need to know the port number associated with the receiver's application.

Generally, this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default port assigned.

- **At receiver's side:**

Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

The functions of the transport layer are :

1. **Segmentation and Reassembly:** This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the

segment produced has a header associated with it. The transport layer at the destination station reassembles the message.

2. **Service Point Addressing:** In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.

The services provided by the transport layer :

1. **Connection Oriented Service:** It is a three-phase process which include
   – Connection Establishment
   – Data Transfer
   – Termination / disconnection
   In this type of transmission, the receiving device sends an acknowledgement, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.
2. **Connection less service:** It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

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

5. Session Layer (Layer 5) :

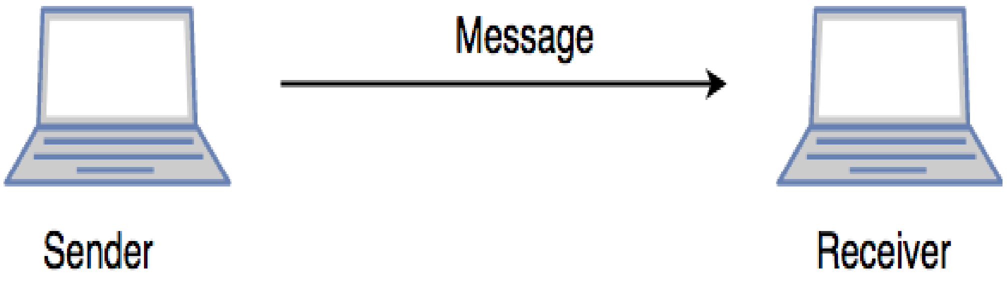
This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.
The functions of the session layer are :

1. **Session establishment, maintenance and termination:** The layer allows the two processes to establish, use and terminate a connection.
2. **Synchronization :** This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
3. **Dialog Controller :** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

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

SCENARIO:

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



6. Presentation Layer (Layer 6) :

Presentation layer is also called the **Translation layer**.The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

The functions of the presentation layer are :

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

7. Application Layer (Layer 7) :

At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

Ex: Application – Browsers, Skype Messenger etc.

***Application Layer is also called as Desktop Layer.*

The functions of the Application layer are :

1. Network Virtual Terminal
2. FTAM-File transfer access and management

3. Mail Services
4. Directory Services

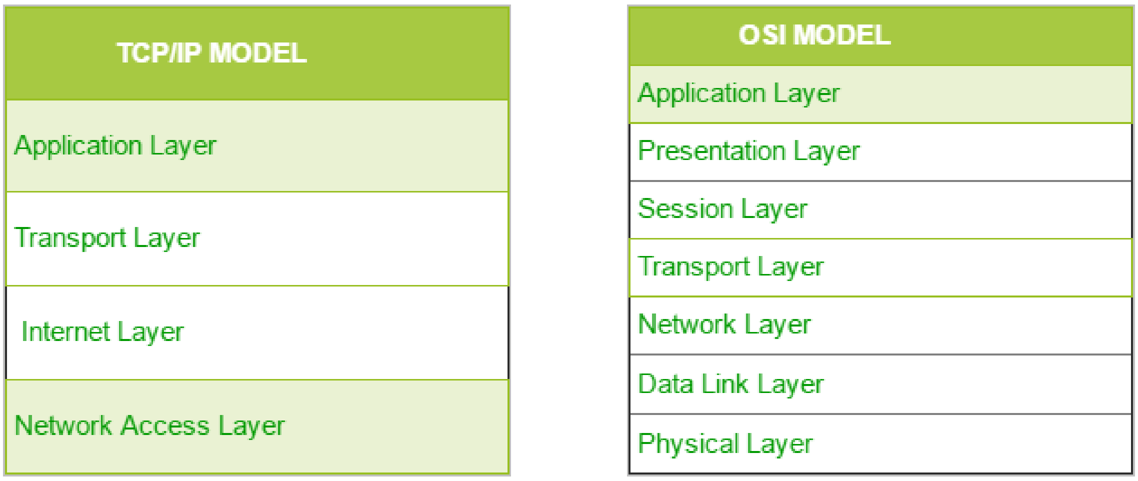
OSI model acts as a reference model and is not implemented in the Internet because of its late invention. Current model being used is the TCP/IP model.

TCP/IP Model

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

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

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



TCP/IP MODEL
Application Layer
Transport Layer
Internet Layer
Network Access Layer

OSI MODEL
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Difference between TCP/IP and OSI Model:

TCP/IP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.

TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable	OSI is less reliable
TCP/IP does not have very strict boundaries.	OSI has strict boundaries
TCP/IP follow a horizontal approach.	OSI follows a vertical approach.
TCP/IP uses both session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP developed protocols then model.	OSI developed model then protocol.
Transport layer in TCP/IP does not provide assurance delivery of packets.	In OSI model, transport layer provides assurance delivery of packets.
TCP/IP model network layer only provides connection less services.	Connection less and connection oriented both services are provided by network layer in OSI model.
Protocols cannot be replaced easily in TCP/IP model.	While in OSI model, Protocols are better covered and is easy to replace with the change in technology.

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

1. Network Access Layer –

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

2. Internet Layer –

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

1. **IP –** stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions:
   IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
2. **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
3. **ARP –** stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

3. Host-to-Host Layer –

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :

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

4. Application Layer –

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

1. **HTTP and HTTPS –** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.
2. **SSH –** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
3. **NTP –** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it's out of sync.

We always encourage you to explore further, this is only for basic interview preparation, but it will vary company to company. So, which company you are focusing, please explore e.g. cisco if you are targeting such type of company, please explore previous year questions from glassdoor or gfg.