Course: 503: Network Technologies

Course Code	503
Course Title	Network Technologies
Credit	3
Teaching per Week	3 Hrs
Minimum weeks per Semester	15 (Including Class work, examination, preparation etc.)
Review / Revision	June 2019
Purpose of Course	With extensive use of Internet and Network at offices, it has now become quite essential for students of IT and Computer Science to acquire basic knowledge of Computer Networks. The purpose of this course is to provide basic knowledge of Computer Networks.
Course Objective	Making students aware of 1. Layering Models. 2. Various Network Topologies. 3. Computer Network parlance. 4. Network Security.
Pre-requisite	Prior knowledge of Operating Systems, LAN
Course Out come	After studying this subject, students will be aware of Layering Models, Different types of Computer Networks, Networking terms, Networking Topologies, Networking protocols and Networking Security.

Course Content	**Unit 1. An Introduction to Networks, Network Topologies, and Types** 1.1 Data Communication [Analog, Digital] 1.2 Introduction: Networking 1.3 Information Exchange, Sharing, Preserving & Protecting 1.4 Hardware and Software Resource Sharing 1.5 Need Uses and Advantages of Network 1.6 Clients, Servers, Peers based and Hybrid Networks 1.7 Server types 1.8 Network Topologies (Bus, Star, Ring, Star Bus, Star Ring & Physical Mesh) 1.9 Defining Network Protocols (H/W Protocols, S/W Protocols H/W-S/W Interface) 1.10 Introduction to Wireless Network, Ad-hoc Wireless and Sensor Wireless Network **Unit 2. The Layering Models and Data Communication** 2.1 Introduction to OSI model with all layers 2.2 Differences between OSI Model & TCP/IP model 2.3 Data Communication Model, Digital and Analog data and signals, bit rate, baud, bandwidth, Nyquist bit rate **Unit 3. Networking Hardware** 3.1 Introduction to Guided Transmission Media-Twisted Pair, Coaxial cable, Optical Fibre 3.2 Wireless transmission-Radio waves, microwaves, infrared waves, Satellite Communication. 3.3 Networking devices (repeater, hub, switch, router, bridge, modem) **Unit 4. Basic of TCP/IP Model** 4.1 Introduction to TCP/IP Model 4.2 Network Access Layer – MAC Address 4.3 Internet Layer – IP Address, IP Subnetting 4.4 Transport Layer - TCP, UDP, Port number 4.5 Application Layer **Unit 5. Network Security: Introductory Concepts and Terminologies** 5.1 Various Types of Securities 5.2 Security with Certificates 5.3 Firewalls

Unit 1. An Introduction to Networks, Network Topologies, and Types

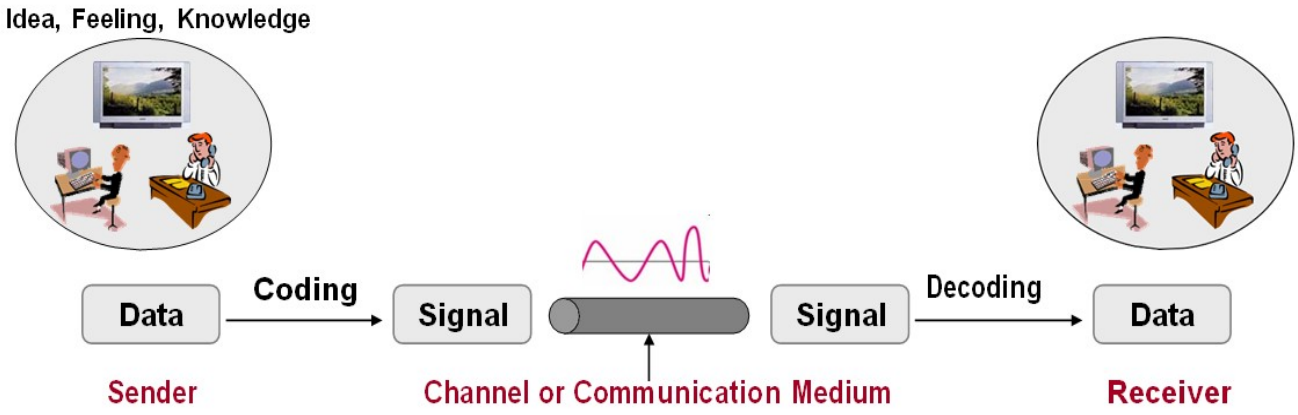
Analog and Digital Signals, Time and Frequency Representation of Signals

Data vs. Signal

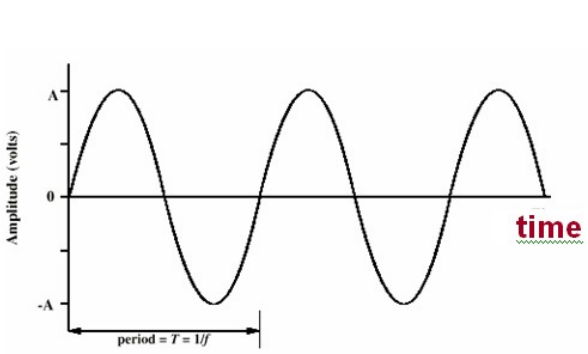
Data–information formatted in human/machine readable form examples: voice, music, image, file

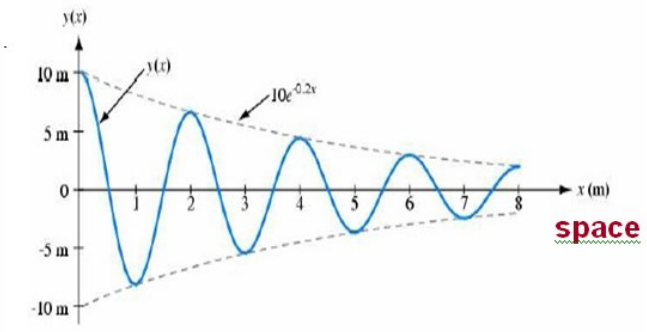
Signal–electric or electromagnetic representation of data transmission media work by conducting energy along a physical path; thus, to be transmitted, data must be turned into energy in the form of electro-magnetic signals.

Transmission–communication of data through propagation and processing of signals



Signal Representation–typically in 2D space, as a function of time, space or frequency when horizontal axis is time, graph displays the value of a signal at one particular point in space as a function of time when horizontal axis is space, graph displays the value of a signal at one particular point in time as a function of space.





The time- and space- representation of a signal often resemble each other, though the signal envelope in the space-representation is different (signal attenuates over distance).

Analog vs. Digital Data

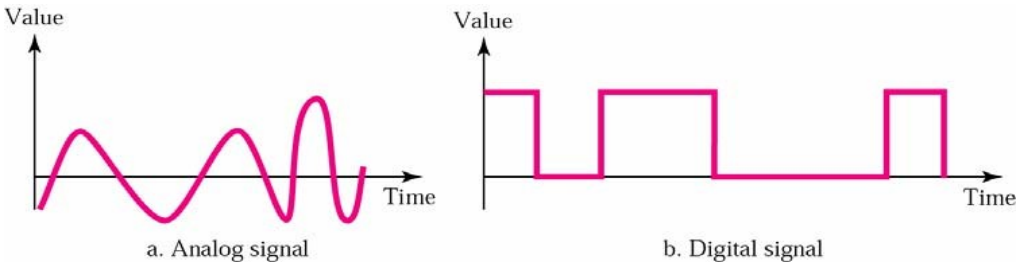
analog data – representation variable takes on continuous values in some interval, e.g. voice, temperature, etc.

digital data – representation variable takes on discrete (a finite & countable number of) values in a given interval, e.g. text, digitized images, etc.

Analog vs. Digital Signal

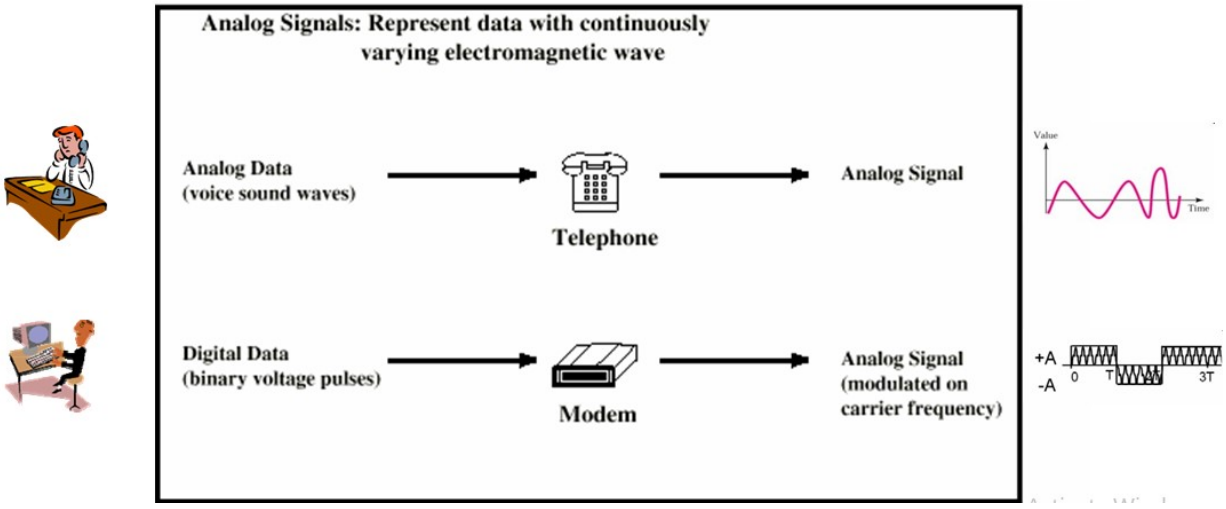
analog signal – signal that is continuousin time and can assume an infinite number of values in a given range (continuous in time and value)

discrete (digital) signal – signal that is continuous in time and assumes only a limited number of values (maintains a constant level and then changes to another constant level)



a. Analog signal b. Digital signal

Both analog and digital data can be transmitted using either analog or digital signals.



example: analog signaling of analog and digital data

Classification of Analog Signals

Simple Analog Signal – cannot be decomposed into simpler signals

sinewave – most fundamental form of periodic analog signal – mathematically described with 3

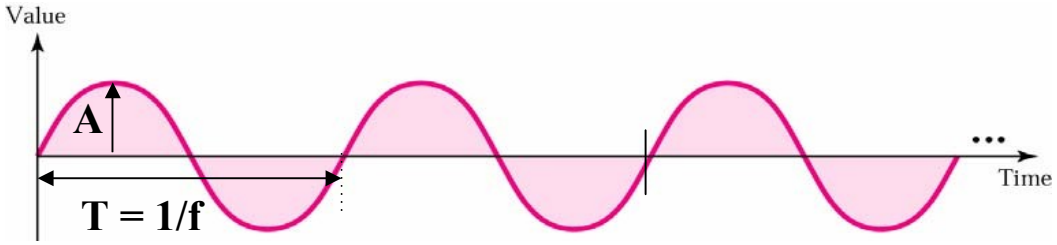
parameters

$s(t) = A \cdot \sin(2\pi ft + \varphi)$

peak amplitude (A) – absolute value of signal's highest intensity – unit: volts [V]

frequency (f) – number of periods in one second – unit: hertz [Hz] = [1/s] – inverse of period (T)!

phase (φ) – absolute position of the waveform relative to an arbitrary origin – unit: degrees [º] or radians [rad]



Composite Analog Signal – composed of multiple sinewaves

Unit	Equivalent	Unit	Equivalent
seconds (s)	1 s	hertz (Hz)	1 Hz
milliseconds (ms)	10^{-3} s	kilohertz (KHz)	10^{3} Hz
microseconds (μs)	10^{-6} s	megahertz (MHz)	10^{6} Hz
nanoseconds (ns)	10^{-9} s	gigahertz (GHz)	10^{9} Hz
picoseconds (ps)	10^{-12} s	terahertz (THz)	10^{12} Hz

What Is Networking?

Networking is the exchange of information and ideas among people with a common profession or special interest, usually in an informal social setting.

A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

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

Characteristics of a Computer Network

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

Following is the list of hardware's required to set up a computer network.

- Network Cables
- Distributors
- Routers
- Internal Network Cards
- External Network Cards

Network Cables

Network cables are used to connect computers. The most commonly used cable is Category 5 cable RJ-45.

Distributors

A computer can be connected to another one via a serial port but if we need to connect many computers to produce a network, this serial connection will not work.

The solution is to use a central body to which other computers, printers, scanners, etc. can be connected and then this body will manage or distribute network traffic.

Router

A router is a type of device which acts as the central point among computers and other devices that are a part of the network. It is equipped with holes called ports. Computers and other devices are connected to a router using network cables. Now-a-days router comes in wireless modes using which computers can be connected without any physical cable.

Network Card

Network card is a necessary component of a computer without which a computer cannot be connected over a network. It is also known as the network adapter or Network Interface Card (NIC). Most branded computers have network card pre-installed. Network cards are of two types: Internal and External Network Cards.

Internal Network Cards

Motherboard has a slot for internal network card where it is to be inserted. Internal network cards are of two types in which the first type uses Peripheral Component Interconnect (PCI) connection, while the second type uses Industry Standard Architecture (ISA). Network cables are required to provide network access.

External Network Cards

External network cards are of two types: Wireless and USB based. Wireless network card needs to be inserted into the motherboard, however no network cable is required to connect to the network.

Universal Serial Bus (USB)

USB card is easy to use and connects via USB port. Computers automatically detect USB card and can install the drivers required to support the USB network card automatically.

Why we need computer networks? Need for Computer Networking

Computer networks help users on the network to share the resources and in communication. Can you imagine a world now without emails, online newspapers, blogs, chat and the other services offered by the internet?

The following are the important uses and benefits of a computer network.

File sharing: Networking of computers helps the network users to share data files.

Hardware sharing: Users can share devices such as printers, scanners, CD-ROM drives, hard drives etc. Without computer networks, device sharing is not possible.

Application sharing: Applications can be shared over the network, and this allows to implement client/server applications

User communication: Networks allow users to communicate using e-mail, newsgroups, and video conferencing etc.

Network gaming: A lot of network games are available, which allow multi-users to play from different locations.

Voice over IP (VoIP): Voice over Internet Protocol (IP) is a revolutionary change in telecommunication which allows to send telephone calls (voice data) using standard Internet Protocol (IP) rather than by traditional PSTN.

Advantages and Disadvantages of Computer Network

Computer networking has become one of the most successful ways of sharing information, where all computers are wirelessly linked together by a common network. Now, businesses and organizations heavily rely on it to get messages and information across to essential channels. Not only has that it benefited establishments, but also individuals, as they also need to share important information every day. But no matter how useful computer networking is, it does not come without drawbacks. Here are its advantages and disadvantages:

List of Advantages of Computer Networking

1. It enhances communication and availability of information. Networking, especially with full access to the web, allows ways of communication that would simply be impossible before it was developed. Instant messaging can now allow users to talk in real time and send files to other people wherever they are in the world, which is a huge boon for businesses. Also, it allows access to a vast amount of useful information, including traditional reference materials and timely facts, such as news and current events.

2. It allows for more convenient resource sharing. This benefit is very important, particularly for larger companies that really need to produce huge numbers of resources to be shared to all the people. Since the technology involves computer-based work, it is assured that the resources they wanted to get across would be completely shared by connecting to a computer network which their audience is also using.

3. It makes file sharing easier.

Computer networking allows easier accessibility for people to share their files, which greatly helps them with saving more time and effort, since they could do file sharing more accordingly and effectively.

4. It is highly flexible.

This technology is known to be very flexible, as it gives users the opportunity to explore everything about essential things, such as software without affecting their functionality. Plus, people will have the accessibility to all information they need to get and share.

5. It is an inexpensive system.

Installing networking software on your device would not cost too much, as you are assured that it lasts and can effectively share information to your peers. Also, there is no need to change the software regularly, as mostly it is not required to do so.

6. It increases cost efficiency.

With computer networking, you can use a lot of software products available on the market which can just be stored or installed in your system or server, and can then be used by various workstations.

7. It boosts storage capacity.

Since you are going to share information, files and resources to other people, you have to ensure all data and content are properly stored in the system. With this networking technology, you can do all of this without any hassle, while having all the space you need for storage.

List of Disadvantages of Computer Networking

1. It lacks independence.

Computer networking involves a process that is operated using computers, so people will be relying more of computer work, instead of exerting an effort for their tasks at hand. Aside from this, they will be dependent on the main file server, which means that, if it breaks down, the system would become useless, making users idle.

2. It poses security difficulties.

Because there would be a huge number of people who would be using a computer network to get and share some of their files and resources, a certain user's security would be always at risk. There might even be illegal activities that would occur, which you need to be careful about and aware of.

3. It lacks robustness.

As previously stated, if a computer network's main server breaks down, the entire system would become useless. Also, if it has a bridging device or a central linking server that fails, the entire network would also come to a standstill. To deal with these problems, huge networks should have a powerful computer to serve as file server to make setting up and maintaining the network easier.

4. It allows for more presence of computer viruses and malware.

There would be instances that stored files are corrupt due to computer viruses. Thus, network administrators should conduct regular check-ups on the system, and the stored files at the same time.

5. Its light policing usage promotes negative acts.
It has been observed that providing users with internet connectivity has fostered undesirable behavior among them. Considering that the web is a minefield of distractions—online games, humor sites and even porn sites—workers could be tempted during their work hours. The huge network of machines could also encourage them to engage in illicit practices, such as instant messaging and file sharing, instead of working on work-related matters. While many organizations draw up certain policies on this, they have proven difficult to enforce and even engendered resentment from employees.

6. It requires an efficient handler.
For a computer network to work efficiently and optimally, it requires high technical skills and know-how of its operations and administration. A person just having basic skills cannot do this job. Take note that the responsibility to handle such a system is high, as allotting permissions and passwords can be daunting. Similarly, network configuration and connection is very tedious and cannot be done by an average technician who does not have advanced knowledge.

7. It requires an expensive set-up.
Though computer networks are said to be an inexpensive system when it is already running, its initial set up cost can still be high depending on the number of computers to be connected. Expensive devices, such as routers, switches, hubs, etc., can add up to the cost. Aside from these, it would also need network interface cards (NICs) for workstations in case they are not built-in.

Exchange of Information

The first stage of any negotiation is the exchange of information. Both parties convey their views on the problems in a non-confronting manner. The trick here is to decide what to show and what to hide. The information you share with your counterparts will familiarize themselves with a certain fraction of your position. However, it would be like cutting the branch you are sitting on, if you give away too much information.

It is a wise move to have a little chat with the other counterparts in the negotiation, before revealing your cards. This will set a positive vibe. You might find some things in common, such as likes and dislikes between you and the others.

If you jump straight into negotiating, then others might think you to be hasty and aggressive. Some people may actually desire negotiating in this style. However, an informal conversation would come in handy when it comes to negotiations.

Of course, in case of introductions and preliminaries, it is advisable to stick to formality. The best way to introduce yourself is to present yourself in a relaxed and friendly manner with some formal restraint. It would be too foolish of you if you seem to try to bleed your opponent dry. This sort of an approach will make them defensive, which will go against the negotiation.

Information Sharing

Information sharing describes the exchange of data between various organizations, people and technologies. There are several types of information sharing:

- Information shared by individuals (such as a video shared on Facebook or YouTube)
- Information shared by organizations (such as the RSS feed of an online weather report)
- Information shared between firmware/software (such as the IP addresses of available network nodes or the availability of disk space)

The advent of wide distributed networks, intranets, cross-platform compatibility, application porting and standardization of IP protocols have all facilitated the huge growth in global information sharing. When it comes to personal information however, no matter how easy it is to port the actual data, there are laws in most countries prohibiting the sharing of personal data without explicit permission being granted. In the U.S. and Europe it is a criminal offense to share any personal data about anyone without such explicit permission. There is plenty of other information sharing that does not fall under the law and information sharing is increasing as more networks and organizations connect and information becomes easier to share across the internet.

digital preservation

Digital preservation is the active safekeeping of digitally stored information. As a part of the formalized efforts of library and archival sciences, digital preservation includes the practices required to ensure that information is safe from medium failures as well as software and hardware obsolescence.

In the digital age, preserving information, entertainment and other material involves not only backing up desired content but also caring for and maintaining the storage media upon which the data is stored. Digital preservation is essential to modern history, not least because much information is not stored in any type of hard copy.

Network protection - methods for protecting your network and data

Networks are the essential system of information technology. All communication between computer systems and terminals takes place in local (LAN) and wide area networks (WAN). Various information and resources are exchanged on a daily basis. The individual nodes in the network are connected to each other via cables, radio connections, dial-up or leased lines. Precisely these need special protection. Network Protection means any activity to protect against manipulation of your network and your data. This includes hardware and software technologies as well as corresponding security strategies. This primarily includes first and foremost preventing intrusion into the network in order to prevent the subsequent spread and further damage to the network. Several types of network protection shall be mentioned here:

- Antivirus software
- Application security
- Behavioral analysis
- Avoidance of data loss
- Firewalls (web application firewalls)
- Mobile Security
- VPN
- Browser/Web Security

RESOURCE SHARING

Computer-communication networks allow the sharing of specialized computer resources such as data bases, programs, and hardware. Such a network consists of both the computer resources and a communications system interconnecting them and allowing their full utilization to be achieved.

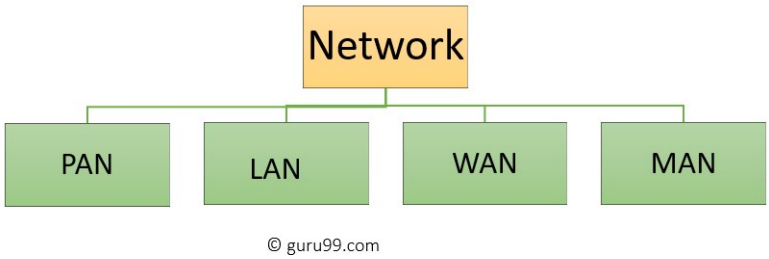
Computer Hardware includes the physical, tangible parts or components of a computer, such as the cabinet, central processing unit, monitor, keyboard, computer data storage, graphic card, sound card, speakers and motherboard. By contrast, software is instructions that can be stored and run by hardware. Hardware is so-termed because it is "hard" or rigid with respect to changes or modifications; whereas software is "soft" because it is easy to update or change. Intermediate between software and hardware is "firmware", which is software that is strongly coupled to the particular hardware of a computer system and thus the most difficult to change but also among the most stable with respect to consistency of interface. The progression from levels of "hardness" to "softness" in computer systems parallels a progression of layers of abstraction in computing. Hardware is typically directed by the software to execute any command or instruction. A combination of hardware and software forms a usable computing system, although other systems exist with only hardware components.

Types of Computer Networks: LAN, MAN, WAN, VPN

What Are the Important Types of Computer Networks?

There are various types of computer networks available. We can categorize them according to their size as well as their purpose.

The size of a network should be expressed by the geographic area and number of computers, which are a part of their networks. It includes devices housed in a single room to millions of devices spread across the world.



Some of the most popular network types are:

- PAN
- LAN
- MAN
- WAN

What is PAN (Personal Area Network)?

PAN is a computer network formed around a person. It generally consists of a computer, mobile, or personal digital assistant. PAN can be used for establishing communication among these personal devices for connecting to a digital network and the internet.

Characteristics of PAN

- It is mostly personal devices network equipped within a limited area.
- Allows you to handle the interconnection of IT devices at the surrounding of a single user.
- PAN includes mobile devices, tablet, and laptop.
- It can be wirelessly connected to the internet called WPAN.
- Appliances use for PAN: cordless mice, keyboards, and Bluetooth systems.

Advantages of PAN

Here, are important pros/benefits of using PAN network:

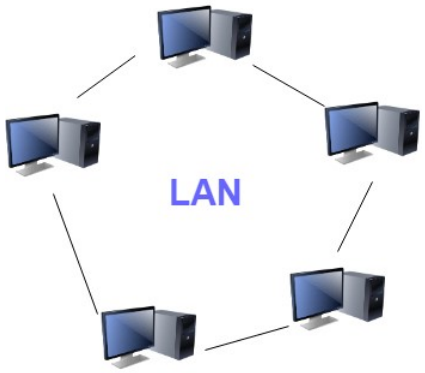
- PAN networks are relatively secure and safe
- It offers only short-range solution up to ten meters
- Strictly restricted to a small area

Disadvantages of PAN

Here are important cons/ drawback of using PAN network:

- It may establish a bad connection to other networks at the same radio bands.
- Distance limits.

What is LAN?



A **L**ocal **A**rea **N**etwork (LAN) is a group of computer and peripheral devices which are connected in a limited area such as school, laboratory, home, and office building. It is a widely useful network for sharing resources like files, printers, games, and other application. The simplest type of LAN network is to connect computers and a printer in someone's home or office. In general, LAN will be used as one type of transmission medium.
It is a network which consists of less than 5000 interconnected devices across several buildings.

Characteristics of LAN

Here are important characteristics of a LAN network:

- It is a private network, so an outside regulatory body never controls it.
- LAN operates at a relatively higher speed compared to other WAN systems.
- There are various kinds of media access control methods like token ring and ethernet.

Advantages of LAN

Here are pros/benefits of using LAN:

- Computer resources like hard-disks, DVD-ROM, and printers can share local area networks. This significantly reduces the cost of hardware purchases.
- You can use the same software over the network instead of purchasing the licensed software for each client in the network.
- Data of all network users can be stored on a single hard disk of the server computer.
- You can easily transfer data and messages over networked computers.
- It will be easy to manage data at only one place, which makes data more secure.

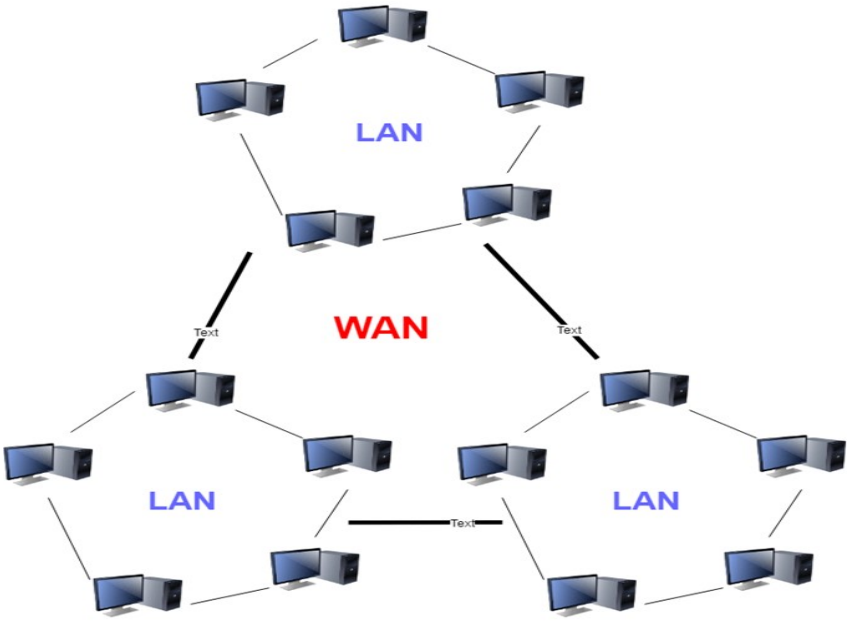
- Local Area Network offers the facility to share a single internet connection among all the LAN users.

Disadvantages of LAN

Here are the important cons/ drawbacks of LAN:

- LAN will indeed save cost because of shared computer resources, but the initial cost of installing Local Area Networks is quite high.
- The LAN admin can check personal data files of every LAN user, so it does not offer good privacy.
- Unauthorized users can access critical data of an organization in case LAN admin is not able to secure centralized data repository.
- Local Area Network requires a constant LAN administration as there are issues related to software setup and hardware failures

What is WAN?



WAN (Wide Area Network) is another important computer network that which is spread across a large geographical area. WAN network system could be a connection of a LAN which connects with other LAN's using telephone lines and radio waves. It is mostly limited to an enterprise or an organization.

Characteristics of LAN:

- The software files will be shared among all the users; therefore, all can access to the latest files.
- Any organization can form its global integrated network using WAN.

Advantages of WAN

Here are the benefits/ pros of using WAN:

- WAN helps you to cover a larger geographical area. Therefore business offices situated at longer distances can easily communicate.

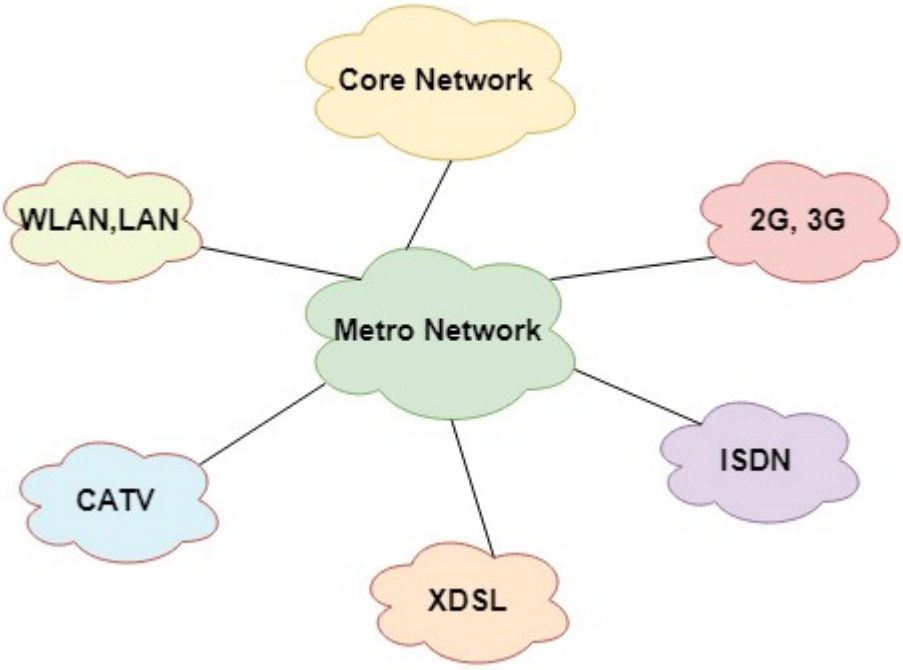
- Contains devices like mobile phones, laptop, tablet, computers, gaming consoles, etc.
- WLAN connections work using radio transmitters and receivers built into client devices.

Disadvantage of WAN

Here are drawbacks/cons of using WAN:

- The initial setup cost of investment is very high.
- It is difficult to maintain the WAN network. You need skilled technicians and network administrators.
- There are more errors and issues because of the wide coverage and the use of different technologies.
- It requires more time to resolve issues because of the involvement of multiple wired and wireless technologies.
- Offers lower security compared to other types of networks.

What is MAN?



A Metropolitan Area Network or MAN is consisting of a computer network across an entire city, college campus, or a small region. This type of network is large than a LAN, which is mostly limited to a single building or site. Depending upon the type of configuration, this type of network allows you to cover an area from several miles to tens of miles.

Characteristics of MAN

Here are important characteristics of the MAN network:

- It mostly covers towns and cities in a maximum 50 km range
- Mostly used medium is optical fibers, cables

- Data rates adequate for distributed computing applications.

Advantages of MAN

Here are pros/benefits of using MAN system:

- It offers fast communication using high-speed carriers, like fiber optic cables.
- It provides excellent support for an extensive size network and greater access to WANs.
- The dual bus in MAN network provides support to transmit data in both directions concurrently.
- A MAN network mostly includes some areas of a city or an entire city.

Disadvantages of MAN

Here are drawbacks/ cons of using the MAN network:

- You need more cable to establish MAN connection from one place to another.
- In MAN network it is tough to make the system secure from hackers

11 Types of Networks in Use Today

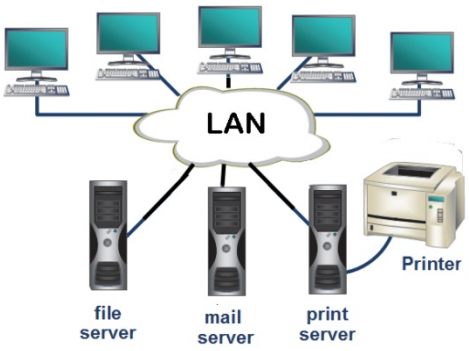
1. Personal Area Network (PAN)

The smallest and most basic type of network, a PAN is made up of a wireless modem, a computer or two, phones, printers, tablets, etc., and revolves around one person in one building. These types of networks are typically found in small offices or residences, and are managed by one person or organization from a single device.

2. Local Area Network (LAN)

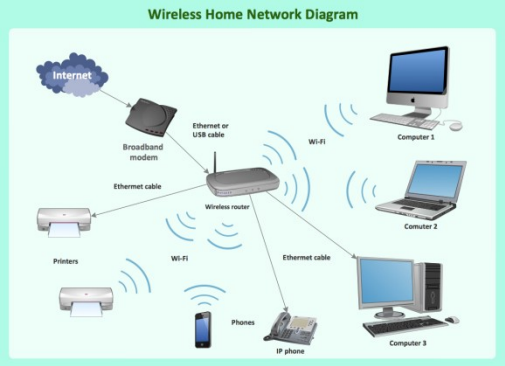
We're confident that you've heard of these types of networks before – LANs are the most frequently discussed networks, one of the most common, one of the most original and one of the simplest types of networks. LANs connect groups of computers and low-voltage devices together across short distances (within a building or between a group of two or three buildings in close proximity to each other) to share information and resources. Enterprises typically manage and maintain LANs.

Using routers, LANs can connect to wide area networks (WANs, explained below) to rapidly and safely transfer data.



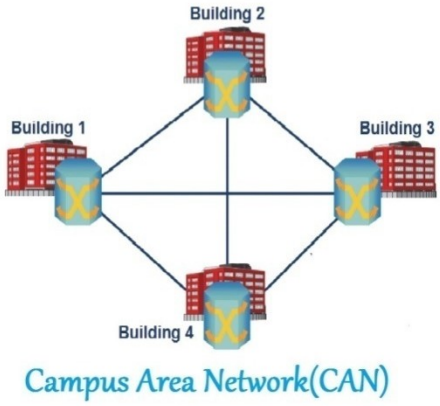
3. Wireless Local Area Network (WLAN)

Functioning like a LAN, WLANs make use of wireless network technology, such as Wi-Fi. Typically seen in the same types of applications as LANs, these types of networks don't require that devices rely on physical cables to connect to the network.



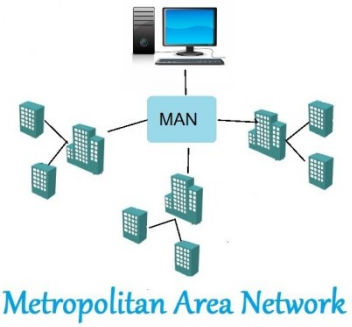
4. Campus Area Network (CAN)

Larger than LANs, but smaller than metropolitan area networks (MANs, explained below), these types of networks are typically seen in universities, large K-12 school districts or small businesses. They can be spread across several buildings that are fairly close to each other so users can share resources.



5. Metropolitan Area Network (MAN)

These types of networks are larger than LANs but smaller than WANs – and incorporate elements from both types of networks. MANs span an entire geographic area (typically a town or city, but sometimes a campus). Ownership and maintenance is handled by



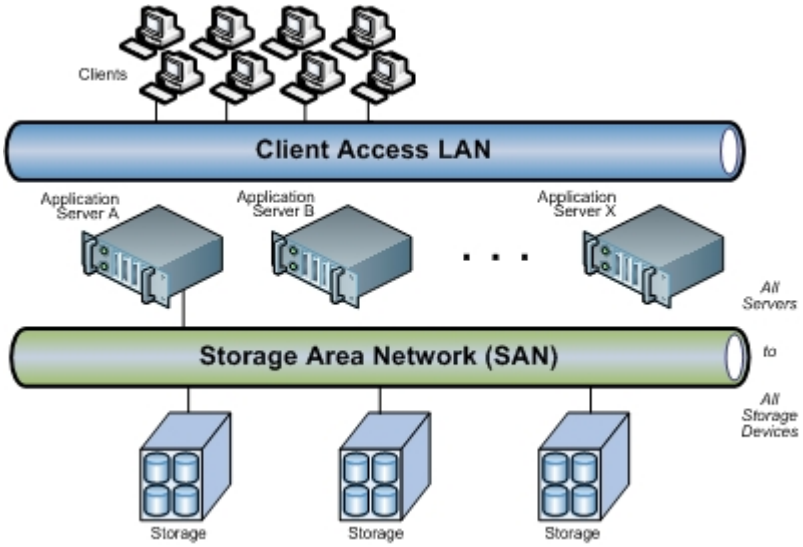
either a single person or company (a local council, a large company, etc.).

6. Wide Area Network (WAN)

Slightly more complex than a LAN, a WAN connects computers together across longer physical distances. This allows computers and low-voltage devices to be remotely connected to each other over one large network to communicate even when they're miles apart.
The Internet is the most basic example of a WAN, connecting all computers together around the world. Because of a WAN's vast reach, it is typically owned and maintained by multiple administrators or the public.

7. Storage-Area Network (SAN)

As a dedicated high-speed network that connects shared pools of storage devices to several servers, these types of networks don't rely on a LAN or WAN. Instead, they move storage resources away from the network and place them into their own high-performance network. SANs can be accessed in the same fashion as a drive attached to a server. Types of storage-area networks include converged, virtual and unified SANs.



8. System-Area Network (also known as SAN)

This term is fairly new within the past two decades. It is used to explain a relatively local network that is designed to provide high-speed connection in server-to-server applications (cluster environments), storage area networks (called "SANs" as well) and processor-to-processor applications. The computers connected on a SAN operate as a single system at very high speeds.

9. Passive Optical Local Area Network (POLAN)

As an alternative to traditional switch-based Ethernet LANs, POLAN technology can be integrated into structured cabling to overcome concerns about supporting traditional Ethernet protocols and network applications such as PoE (Power over Ethernet). A point-to-multipoint LAN architecture, POLAN uses optical splitters to split an optical

signal from one strand of singlemode optical fiber into multiple signals to serve users and devices.

10. Enterprise Private Network (EPN)

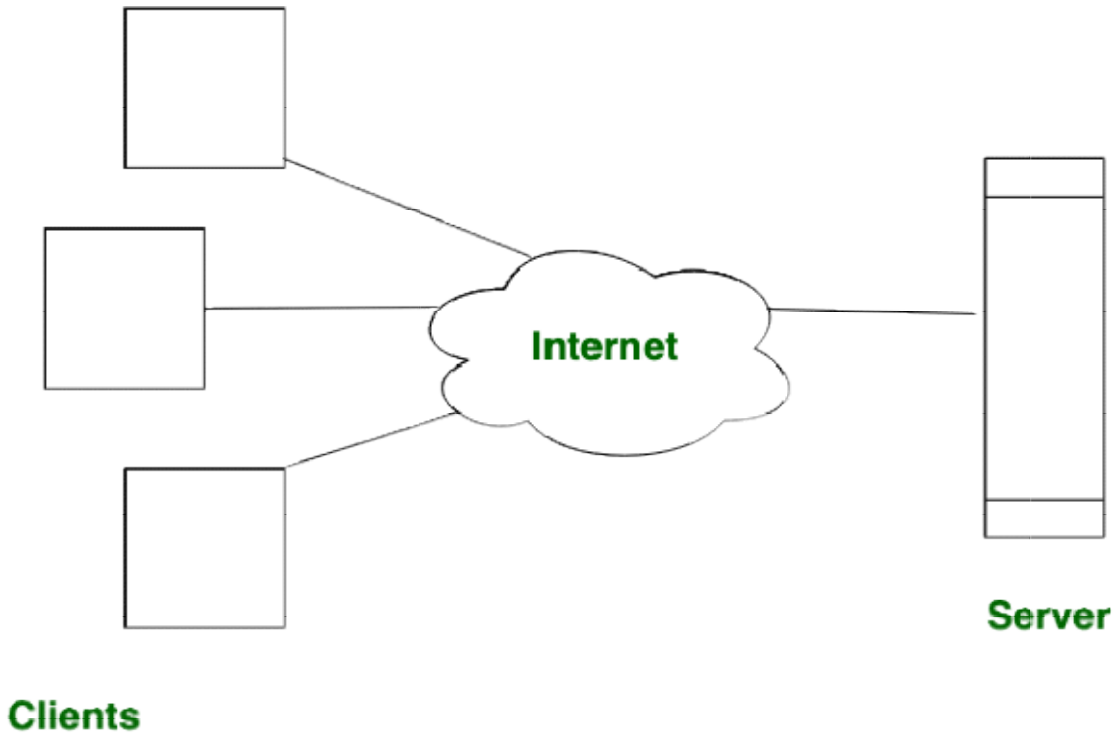
These types of networks are built and owned by businesses that want to securely connect its various locations to share computer resources.

11. Virtual Private Network (VPN)

By extending a private network across the Internet, a VPN lets its users send and receive data as if their devices were connected to the private network – even if they're not. Through a virtual point-to-point connection, users can access a private network remotely.

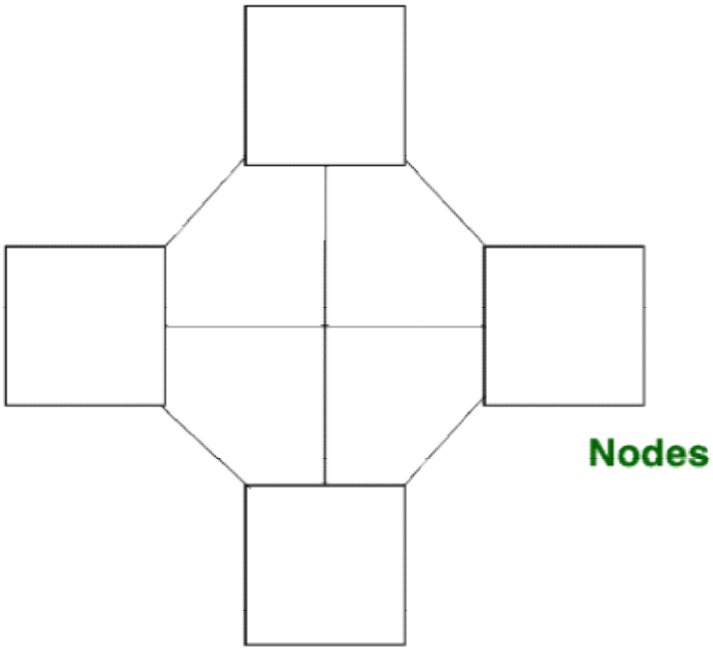
Difference between Client-Server and Peer-to-Peer Network

Client-Server Network:
This model are broadly used network model. In Client-Server Network, Clients and server are differentiated, Specific server and clients are present. In Client-Server Network, Centralized server is used to store the data because its management is centralized.In Client-Server Network, Server respond the services which is request by Client.



Client-Server Network Model

Peer-to-Peer Network:
This model does not differentiate the clients and the servers, In this each and every node is itself client and server. In Peer-to-Peer Network, Each and every node can do both request and respond for the services.



Peer-to-Peer Network Model

Difference between Client-Server and Peer-to-Peer Network:

S.NO	CLIENT-SERVER NETWORK	PEER-TO-PEER NETWORK
1.	In Client-Server Network, Clients and server are differentiated, Specific server and clients are present.	In Peer-to-Peer Network, Clients and server are not differentiated.
2.	Client-Server Network focuses on information sharing.	While Peer-to-Peer Network focuses on connectivity.

3.	In Client-Server Network, Centralized server is used to store the data.	While in Peer-to-Peer Network, Each peer has its own data.
4.	In Client-Server Network, Server respond the services which is request by Client.	While in Peer-to-Peer Network, Each and every node can do both request and respond for the services.
5.	Client-Server Network are costlier than Peer-to-Peer Network.	While Peer-to-Peer Network are less costlier than Client-Server Network.
6.	Client-Server Network are more stable than Peer-to-Peer Network.	While Peer-to-Peer Network are less stable if number of peer is increase.
7.	Client-Server Network is used for both small and large networks.	While Peer-to-Peer Network is generally suited for small networks with fewer than 10 computers.

P2P(Peer To Peer) File Sharing

Introduction

In Computer Networking, P2P is a file sharing technology, allowing the users to access mainly the multimedia files like videos, music, e-books, games etc. The individual users in this network are referred to as **peers**. The peers request for the files from other peers by establishing TCP or UDP connections.

How P2P works(Overview)

A peer-to-peer network allows computer hardware and software to communicate without the need for a server. Unlike client-server architecture, there is no central server for processing requests in a P2P architecture. The peers directly interact with one another without the requirement of a central server.

Now, when one peer makes a request, it is possible that multiple peers have the copy of that requested object. Now the problem is how to get the IP addresses of all those peers. This is decided by the underlying architecture supported by the P2P systems. By

means of one of these methods, the client peer can get to know about all the peers which have the requested object/file and the file transfer takes place directly between these two peers.

Three such Architectures exist:

1. Centralized Directory
2. Query Flooding
3. Exploiting Heterogeneity

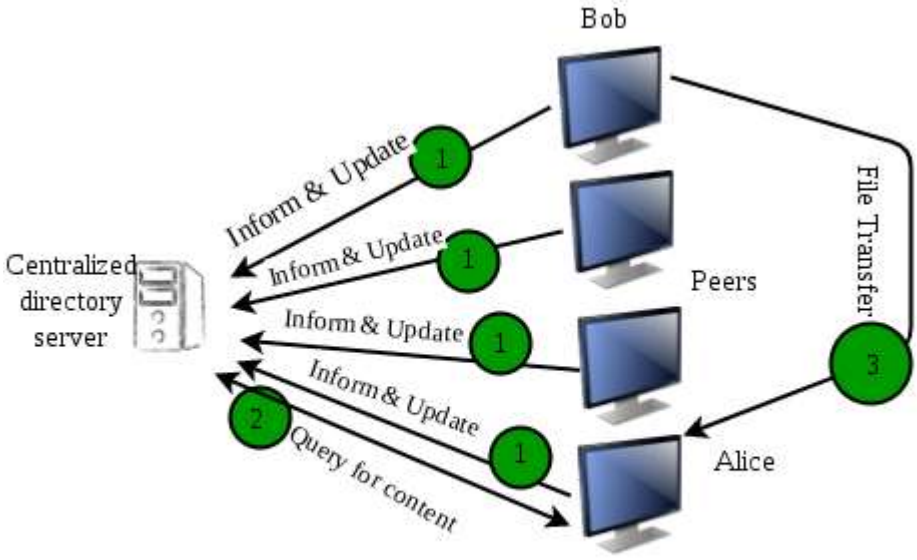
1. Centralized Directory

- It is somewhat similar to client server architecture in the sense that it maintains a huge central server to provide directory service.
- All the peers inform this central server of their IP address and the files they are making available for sharing.
- The server queries the peers at regular intervals to make sure if the peers are still connected or not.
- So basically this server maintains a huge database regarding which file is present at which IP addresses.

Working

- Now whenever a requesting peer comes in, it sends its query to the server.
- Since the server has all the information of its peers, so it returns the IP addresses of all the peers having the requested file to the peer.
- Now the file transfer takes place between these two peers.

The first system which made use of this method was **Napster**, for the purpose of Mp3 distribution.



P2P paradigm with a centralised directory

The major problem with such an architecture is that there is a single point of failure. If the server crashes, the whole P2P network crashes. Also, since all of the processing is to be done by a single server so a huge amount of database has to be maintained and regularly updated.

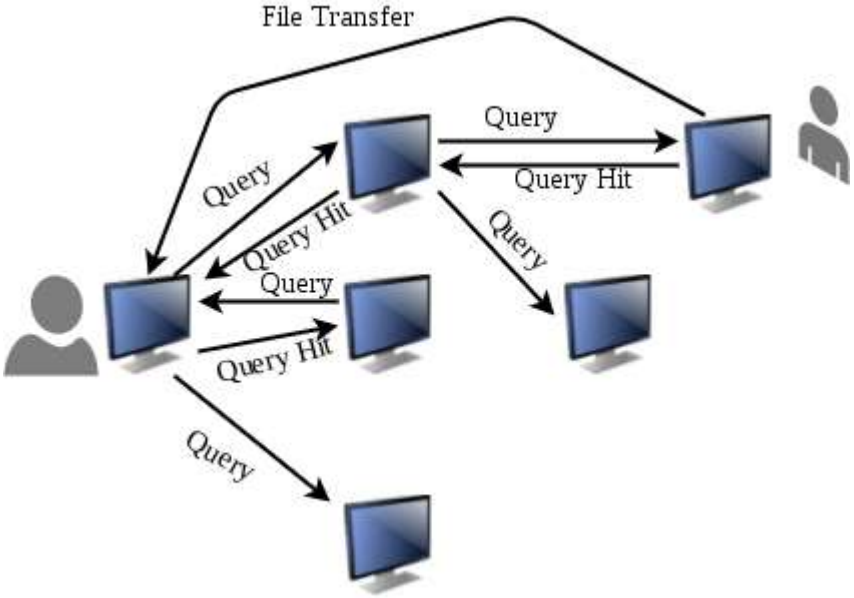
2. Query Flooding

- Unlike the centralized approach, this method makes use of distributed systems.
- In this, the peers are supposed to be connected into an overlay network. It means if a connection/path exists from one peer to other, it is a part of this overlay network.
- In this overlay network, peers are called as nodes and the connection between peers is called an edge between the nodes, thus resulting in a graph-like structure.

Working

- Now when one peer requests for some file, this request is sent to all its neighboring nodes i.e. to all nodes which are connected to this node. If those nodes don't have the required file, they pass on the query to their neighbors and so on. This is called as query flooding.
- When the peer with requested file is found (referred to as query hit), the query flooding stops and it sends back the file name and file size to the client, thus following the reverse path.
- If there are multiple query hits, the client selects from one of these peers.

Gnutella was the first decentralized peer to peer network.



This method also has some disadvantages like, the query has to be sent to all the neighboring peers unless a match is found. This increases traffic in the network.

3. Exploiting heterogeneity

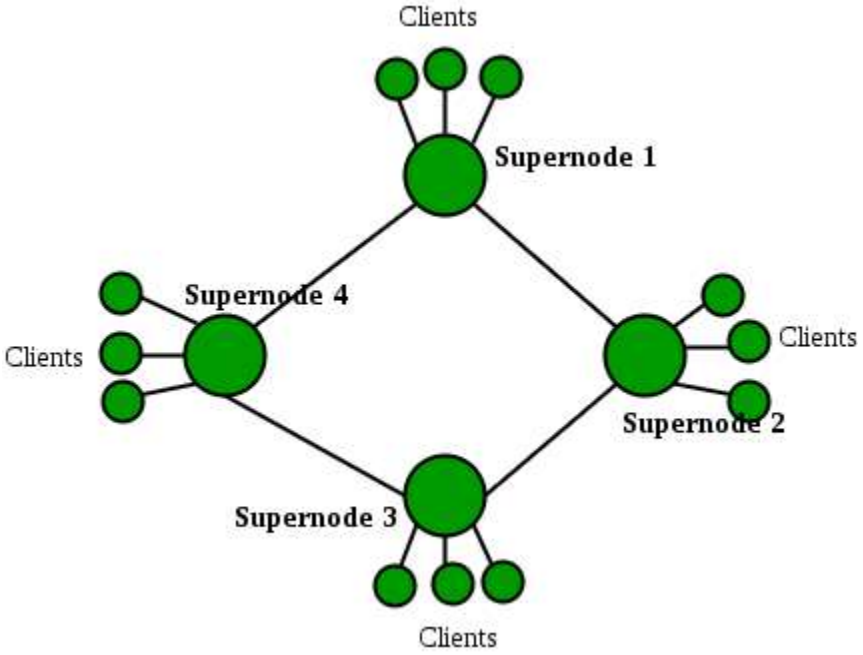
- This P2P architecture makes use of both the above discussed systems.
- It resembles a distributed system like Gnutella because there is no central server for query processing.
- But unlike Gnutella, it does not treat all its peers equally. The peers with higher bandwidth and network connectivity are at a higher priority and are called as **group leaders/super nodes**. The rest of the peers are assigned to these super nodes.

- These super nodes are interconnected and the peers under these super nodes inform their respective leaders about their connectivity, IP address and the files available for sharing.

KaZaA technology is such an example which makes use of Napster and Gnutella both. Thus, the individual group leaders along with their child peers form a Napster-like structure. These group leaders then interconnect among themselves to resemble a Gnutella-like structure.

Working

- This structure can process the queries in two ways.
- The first one is that the super nodes could contact other super nodes and merge their databases with its own database. Thus, this super node now has information of a large number of peers.
- Another approach is that when a query comes in, it is forwarded to the neighboring super nodes until a match is found, just like in Gnutella. Thus query flooding exists but with limited scope as each super node has many child peers. Hence, such a system exploits the heterogeneity of the peers by designating some of them as group leaders/super nodes and others as their child peers.



What Are Hybrid Networks?

A hybrid network is any computer network that uses more than one type of connecting technology or topology. For example, a home network that uses both Wi-Fi and

Ethernet cables to connect computers is a hybrid. In the early years of computer networking, hybrid networks often consisted of Token Ring or Star technologies, however these were quickly antiquated by Ethernet. While textbooks often refer to these types of hybrids, they are basically extinct in 2014.

Home Network Hybrids

Although Ethernet and Wi-Fi usually use the same router in a home network, this doesn't mean that the technology behind them is identical. Both have different specifications developed by the IEEE Standards Association. Ethernet cable networks use the 802.3 standards, while Wi-Fi networks use 802.11. These standards have different rules about how data is transferred. A home WiFi Ethernet router is a hybrid device that brings these two different technologies together. Without such a hybrid device, there would be no way to connect an Ethernet-based desktop to a Wi-Fi-based tablet on the same network.

Advantages of Hybrids

The two main advantages of a hybrid network are cost-savings and accessibility. If you have an Ethernet network at home and buy a tablet, rather than replacing all of your Ethernet components with Wi-Fi, you can simply add a Wi-Fi router to your existing network. The same is true for business networks, but on a larger scale. Few businesses have the budget to replace an entire network all at once. Hybrids allow a business to bring in new networking technologies, while phasing out old technologies over the course of several years.

Disadvantages of Hybrids

The main disadvantage of hybrids are security and support costs. Each network technology introduces new security concerns. Having a router with a good firewall becomes meaningless, for example, if you add a Wi-Fi access point that hasn't been encrypted with a strong password. In business networks, supporting different types of network technologies can become expensive, since they usually need someone with expertise in each technology. Business hybrid networks are always the result of balancing the need for a fast, accessible network with the need for data security.

What is a server?

A server is a computer or system that provides resources, data, services, or programs to other computers, known as clients, over a network. In theory, whenever computers share resources with client machines they are considered servers. There are many types of servers, including web servers, mail servers, and virtual servers.

An individual system can provide resources and use them from another system at the same time. This means that a device could be both a server and a client at the same time.

Some of the first servers were mainframe computers or minicomputers. Minicomputers were much smaller than mainframe computers, hence the name. However, as technology progressed, they ended up becoming much larger than desktop computers, which made the term microcomputer somewhat farcical.

Initially, such servers were connected to clients known as terminals that did not do any actual computing. These terminals, referred to as dumb terminals, existed simply to accept input via a keyboard or card reader and to return the results of any computations to a display screen or printer. The actual computing was done on the server.

Later, servers were often single, powerful computers connected over a network to a set of less-powerful client computers. This network architecture is often referred to as the client-server model, in which both the client computer and the server possess computing power, but certain tasks are delegated to servers. In previous computing models, such as the mainframe-terminal model, the mainframe did act as a server even though it wasn't referred to by that name.

As technology has evolved, the definition of a server has evolved with it. These days, a server may be nothing more than software running on one or more physical computing devices. Such

servers are often referred to as virtual servers. Originally, virtual servers were used to increase the number of server functions a single hardware server could do. Today, virtual servers are often run by a third-party on hardware across the Internet in an arrangement called cloud computing.

A server may be designed to do a single task, such as a mail server, which accepts and stores email and then provides it to a requesting client. Servers may also perform several tasks, such as a file and print server, which both stores files and accepts print jobs from clients and then sends them on to a network-attached printer.

How a server works

To function as a server, a device must be configured to listen to requests from clients on a network connection. This functionality can exist as part of the operating system as an installed application, role, or a combination of the two.

For example, Microsoft's Windows Server operating system provides the functionality to listen to and respond to client requests. Additionally installed roles or services increase which kinds of client requests the server can respond to. In another example, an Apache web server responds to Internet browser requests via an additional application, Apache, installed on top of an operating system.

When a client requires data or functionality from a server, it sends a request over the network. The server receives this request and responds with the appropriate information. This is the request and response model of client-server networking, also known as the call and response model.

A server will often perform numerous additional tasks as part of a single request and response, including verifying the identity of the requestor, ensuring that the client has permission to access the data or resources requested, and properly formatting or returning the required response in an expected way.

Types of servers

There are many types of servers that all perform different functions. Many networks contain one or more of the common server types:

File servers

File servers store and distribute files. Multiple clients or users may share files stored on a server. In addition, centrally storing files offers easier backup or fault tolerance solutions than attempting to provide security and integrity for files on every device in an organization. File server hardware can be designed to maximize read and write speeds to improve performance.

Print servers

Print servers allow for the management and distribution of printing functionality. Rather than attaching a printer to every workstation, a single print server can respond to printing requests from numerous clients. Today, some larger and higher-end printers come with their own built-in print server, which removes the need for an additional computer-based print server. This internal print server also functions by responding to print requests from a client.

Application servers

Application servers run applications in lieu of client computers running applications locally. Application servers often run resource-intensive applications that are shared by a large number of users. Doing so removes the need for each client to have sufficient resources to run the applications. It also removes the need to install and maintain software on many machines as opposed to only one.

DNS servers

Domain Name System (DNS) servers are application servers that provide name resolution to client computers by converting names easily understood by humans into machine-readable IP addresses. The DNS system is a widely distributed database of names and other DNS servers, each of which can be used to request an otherwise unknown computer name. When a client needs the address of a system, it sends a DNS request with the name of the desired resource to a DNS server. The DNS server responds with the necessary IP address from its table of names.

Mail servers

Mail servers are a very common type of application server. Mail servers receive emails sent to a user and store them until requested by a client on behalf of said user. Having an email server allows for a single machine to be properly configured and attached to the network at all times. It is then ready to send and receive messages rather than requiring every client machine to have its own email subsystem continuously running.

Web servers

One of the most abundant types of servers in today's market is a web server. A web server is a special kind of application server that hosts programs and data requested by users across the Internet or an intranet. Web servers respond to requests from browsers running on client computers for web pages, or other web-based services. Common web servers include Apache web servers, Microsoft Internet Information Services (IIS) servers and Nginx servers.

Database servers

The amount of data used by companies, users, and other services is staggering. Much of that data is stored in databases. Databases need to be accessible to multiple clients at any given time and can require extraordinary amounts of disk space. Both of these needs lend themselves well to locating such databases on servers. Database servers run database applications and respond to numerous requests from clients. Common database server applications include Oracle, Microsoft SQL Server, DB2, and Informix.

Virtual servers

Virtual servers are taking the server world by storm. Unlike traditional servers that are installed as an operating system on machine hardware, virtual servers exist only as defined within specialized software called hypervisor. Each hypervisor can run hundreds, or even thousands, of virtual servers all at once. The hypervisor presents virtual hardware to the server as if it were real physical hardware. The virtual server uses the virtual hardware as usual, and the hypervisor passes the actual computation and storage needs onto the real hardware beneath, which is shared among all the other virtual servers.

Proxy servers

A proxy server acts as an intermediary between a client and a server. Often used to isolate either the clients or servers for security purposes, a proxy server takes the request from the client. Instead of responding to the client, it passes the request on to another server or process. The proxy server receives the response from the second server and then replies to the original client as if it were replying on its own. In this way, neither the client nor the responding server needs to directly connect to each other.

Monitoring and management servers

Some servers exist to monitor or manage other systems and clients. There are many types of monitoring servers. Several of them listen to the network and receive every client request and

server response, but some do not request or respond to data themselves. In this way, the monitoring server can keep track of all the traffic on the network, as well as the requests and replies of clients and servers, without interfering with those operations. A monitoring server will respond to requests from monitoring clients such as those run by network administrators watching the health of the network.

What Is Network Topology?

The configuration, or topology, of a network is key to determining its performance. Network topology is the way a network is arranged, including the physical or logical description of how links and nodes are set up to relate to each other.

There are numerous ways a network can be arranged, all with different pros and cons, and some are more useful in certain circumstances than others. Admins have a range of options when it comes to choosing a network topology, and this decision must account for the size and scale of their business, its goals, and budget. Several tasks go into effective network topology management, including configuration management, visual mapping, and general performance monitoring. The key is to understand your objectives and requirements to create and manage the network topology in the right way for your business.

What Is Network Topology?

Network topology refers to how various nodes, devices, and connections on your network are physically or logically arranged in relation to each other. Think of your network as a city, and the topology as the road map. Just as there are many ways to arrange and maintain a city—such as making sure the avenues and boulevards can facilitate passage between the parts of town getting the most traffic—there are several ways to arrange a network. Each has advantages and disadvantages and depending on the needs of your company, certain arrangements can give you a greater degree of connectivity and security.

There are two approaches to network topology: physical and logical. Physical network topology, as the name suggests, refers to the physical connections and interconnections between nodes and the network—the wires, cables, and so forth. Logical network topology is a little more abstract and strategic, referring to the conceptual understanding of how and why the network is arranged the way it is, and how data moves through it.

Why Is Network Topology Important?

The layout of your network is important for several reasons. Above all, it plays an essential role in how and how well your network functions. Choosing the right topology for your company's operational model can increase performance while making it easier to locate faults, troubleshoot errors, and more effectively allocate resources across the network to ensure optimal network health. A streamlined and properly managed network topology can increase energy and data efficiency, which can in turn help to reduce operational and maintenance costs.

The design and structure of a network are usually shown and manipulated in a software-created network topology diagram. These diagrams are essential for a few reasons, but especially for how they can provide visual representations of both physical and logical layouts, allowing administrators to see the connections between devices when troubleshooting.

The way a network is arranged can make or break network functionality, connectivity, and protection from downtime. The question of, "What is network topology?" can be answered with an explanation of the two categories in the network topology.

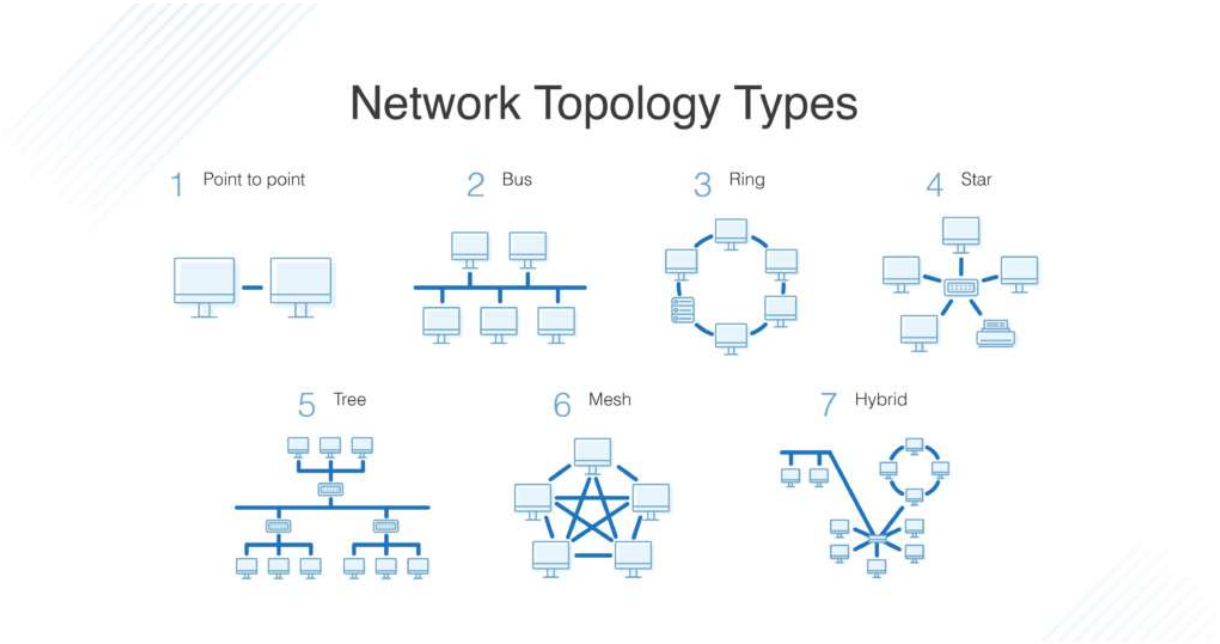
1. **Physical** – The physical network topology refers to the actual connections (wires, cables, etc.) of how the network is arranged. Setup, maintenance, and provisioning tasks require insight into the physical network.
2. **Logical** – The logical network topology is a higher-level *idea* of how the network is set up, including which nodes connect to each other and in which ways, as well as how data is transmitted through the network. Logical network topology includes any virtual and cloud resources.

Effective network management and monitoring require a strong grasp of both the physical and logical topology of a network to ensure your network is efficient and healthy.

What's the Most Common Type of Network Topology?

Building a local area network (LAN) topology can be make-or-break for your business, as you want to set up a resilient, secure, and easy-to-maintain topology. There are several different types of network topology and all are suitable for

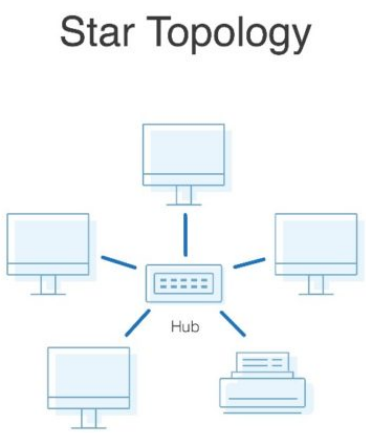
different purposes, depending on the overall network size and your objectives.



As with most things, there's no "right" or one-size-fits-all option. With this in mind, I'll walk you through the most common network topology definitions to give you a feel for the advantages and disadvantages of each.

What Is Star Topology?

A star topology, the most common network topology, is laid out so every node in the network is directly connected to one central hub via coaxial, twisted-pair, or fiber-optic cable. Acting as a server, this central node manages data transmission—as information sent from any node on the network has to pass through the central one to reach its destination—and functions as a repeater, which helps prevent data loss.



Advantages of Star Topology

Star topologies are common since they allow you to conveniently manage your entire network from a single location. Because each of the nodes is independently connected to the central hub, should one go down, the rest of the network will continue functioning unaffected, making the star topology a stable and secure network layout.

Additionally, devices can be added, removed, and modified without taking the entire network offline.

On the physical side of things, the structure of the star topology uses relatively little cabling to fully connect the network, which allows for both straightforward setup and management over time as the network expands or contracts. The simplicity of the network design makes life easier for administrators, too, because it's easy to identify where errors or performance issues are occurring.

Disadvantages of Star Topology

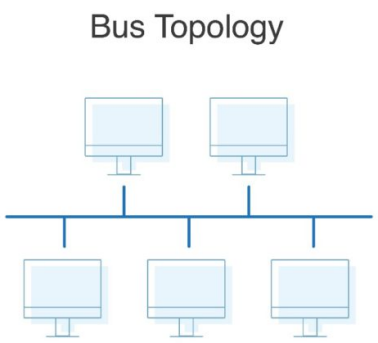
On the flipside, if the central hub goes down, the rest of the network can't function. But if the central hub is properly managed and kept in good health, administrators shouldn't have too many issues.

The overall bandwidth and performance of the network are also limited by the

central node's configurations and technical specifications, making star topologies expensive to set up and operate.

What Is Bus Topology?

A bus topology orients all the devices on a network along a single cable running in a single direction from one end of the network to the other—which is why it's sometimes called a "line topology" or "backbone topology." Data flow on the network also follows the route of the cable, moving in one direction.



Advantages of Bus Topology

Bus topologies are a good, cost-effective choice for smaller networks because the layout is simple, allowing all devices to be connected via a single coaxial or RJ45 cable. If needed, more nodes can be easily added to the network by joining additional cables.

Disadvantages of Bus Topology

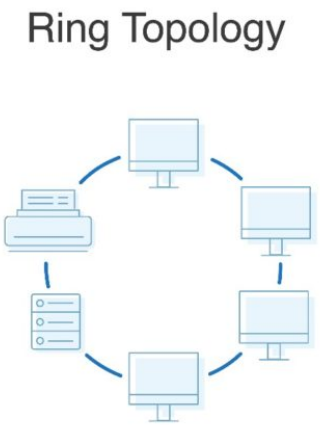
However, because bus topologies use a single cable to transmit data, they're somewhat vulnerable. If the cable experiences a failure, the whole network goes down, which can be time-consuming and expensive to restore, which can be less of an issue with smaller networks.

Bus topologies are best suited for small networks because there's only so much bandwidth, and every additional node will slow transmission speeds.

Furthermore, data is “half-duplex,” which means it can’t be sent in two opposite directions at the same time, so this layout is not the ideal choice for networks with huge amounts of traffic.

What Is Ring Topology? Single vs. Dual

Ring topology is where nodes are arranged in a circle (or ring). The data can travel through the ring network in either one direction or both directions, with each device having exactly two neighbors.



Pros of Ring Topology

Since each device is only connected to the ones on either side, when data is transmitted, the packets also travel along the circle, moving through each of the intermediate nodes until they arrive at their destination. If a large network is arranged in a ring topology, repeaters can be used to ensure packets arrive correctly and without data loss.

Only one station on the network is permitted to send data at a time, which greatly reduces the risk of packet collisions, making ring topologies efficient at transmitting data without errors.

By and large, ring topologies are cost-effective and inexpensive to install, and the

intricate point-to-point connectivity of the nodes makes it relatively easy to identify issues or misconfigurations on the network.

Cons of Ring Topology

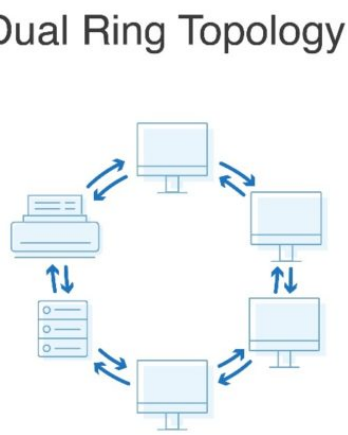
Even though it's popular, a ring topology is still vulnerable to failure without proper network management. Since the flow of data transmission moves unidirectionally between nodes along each ring, if one node goes down, it can take the entire network with it. That's why it's imperative for each of the nodes to be monitored and kept in good health. Nevertheless, even if you're vigilant and attentive to node performance, your network can still be taken down by a transmission line failure.

The question of scalability should also be taken into consideration. In a ring topology, all the devices on the network share bandwidth, so the addition of more devices can contribute to overall communication delays. Network administrators need to be mindful of the devices added to the topology to avoid overburdening the network's resources and capacity.

Additionally, the entire network must be taken offline to reconfigure, add, or remove nodes. And while that's not the end of the world, scheduling downtime for the network can be inconvenient and costly.

What Is Dual-Ring Topology?

A network with ring topology is half-duplex, meaning data can only move in one direction at a time. Ring topologies can be made full-duplex by adding a second connection between network nodes, creating a dual ring topology.

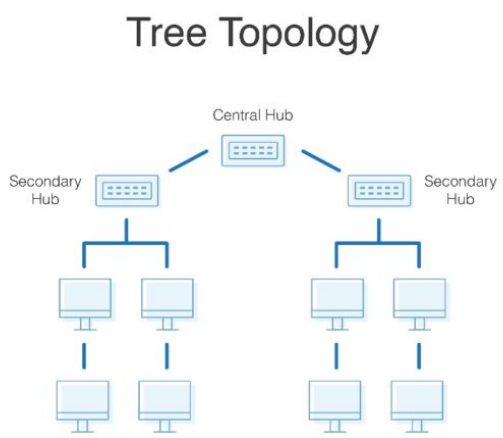


Advantages of Dual-Ring Topology

The primary advantage of dual ring topology is its efficiency: because each node has two connections on either side, information can be sent both clockwise and counterclockwise along the network. The secondary ring included in a dual-ring topology setup can act as a redundant layer and backup, which helps solve for many of the disadvantages of traditional ring topology. Dual ring topologies offer a little extra security, too: if one ring fails within a node, the other ring is still able to send data.

What Is Tree Topology?

The tree topology structure gets its name from how the central node functions as a sort of trunk for the network, with nodes extending outward in a branch-like fashion. However, where each node in a star topology is directly connected to the central hub, a tree topology has a parent-child hierarchy to how the nodes are connected. Those connected to the central hub are connected linearly to other nodes, so two connected nodes only share one mutual connection. Because the tree topology structure is both extremely flexible and scalable, it’s often used for wide area networks to support many spread-out devices.



Pros of Tree Topology

Combining elements of the star and bus topologies allows for the easy addition of nodes and network expansion. Troubleshooting errors on the network is also a straightforward process, as each of the branches can be individually assessed for performance issues.

Cons of Tree Topology

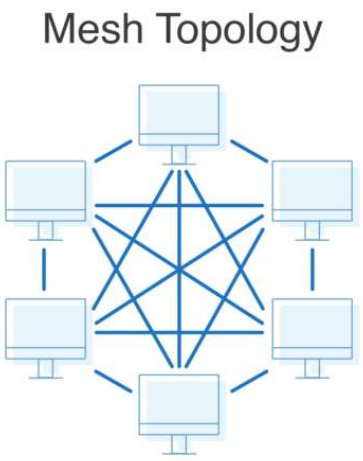
As with the star topology, the entire network depends on the health of the root node in a tree topology structure. Should the central hub fail, the various node branches will become disconnected, though connectivity within—but not between—branch systems will remain.

Because of the hierarchical complexity and linear structure of the network layout, adding more nodes to a tree topology can quickly make proper management an unwieldy, not to mention costly, experience. Tree topologies are expensive because of the sheer amount of cabling required to connect each device to the next within the hierarchical layout.

What Is Mesh Topology?

A mesh topology is an intricate and elaborate structure of point-to-point connections where the nodes are interconnected. Mesh networks can be full or

partial mesh. Partial mesh topologies are mostly interconnected, with a few nodes with only two or three connections, while full-mesh topologies are—surprise!—fully interconnected.



The web-like structure of mesh topologies offers two different methods of data transmission: routing and flooding. When data is routed, the nodes use logic to determine the shortest distance from the source to destination, and when data is flooded, the information is sent to all nodes within the network without the need for routing logic.

Advantages of Mesh Topology

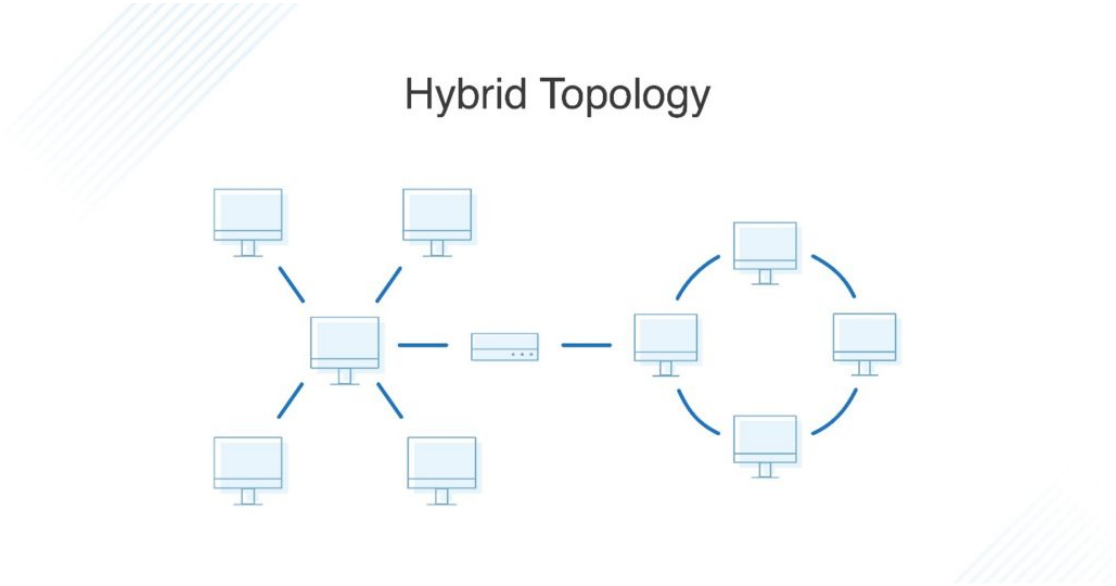
Mesh topologies are reliable and stable, and the complex degree of interconnectivity between nodes makes the network resistant to failure. For instance, no single device going down can bring the network offline.

Disadvantages of Mesh Topology

Mesh topologies are incredibly labor-intensive. Each interconnection between nodes requires a cable and configuration once deployed, so it can also be time-consuming to set up. As with other topology structures, the cost of cabling adds up fast, and to say mesh networks require a lot of cabling is an understatement.

What Is Hybrid Topology?

Hybrid topologies combine two or more different topology structures—the tree topology is a good example, integrating the bus and star layouts. Hybrid structures are most commonly found in larger companies where individual departments have personalized network topologies adapted to suit their needs and network usage.



Advantages of Hybrid Topology

The main advantage of hybrid structures is the degree of flexibility they provide, as there are few limitations on the network structure itself that a hybrid setup can’t accommodate.

Disadvantages of Hybrid Topology

However, each type of network topology comes with its own disadvantages, and as a network grows in complexity, so too does the experience and know-how required on the part of the admins to keep everything functioning optimally. There’s also the monetary cost to consider when creating a hybrid network topology.

Which Topology Is Best for Your Network?

No network topology is perfect, or even inherently better than the others, so determining the right structure for your business will depend on the needs and size of your network. Here are the key elements to consider:

- Length of cable needed
- Cable type
- Cost
- Scalability

Cable Length

Generally, the more cable involved in network topology, the more work it'll require to set up. The bus and star topologies are on the simpler side of things, both being fairly lightweight, while mesh networks are much more cable- and labor-intensive.

Cable Type

The second point to consider is the type of cable you'll install. Coaxial and twisted-pair cables both use insulated copper or copper-based wiring, while fiber-optic cables are made from thin and pliable plastic or glass tubes. Twisted-pair cables are cost-effective but have less bandwidth than coaxial cables. Fiber-optic cables are high performing and can transmit data far faster than twisted-pair or coaxial cables, but they also tend to be far more expensive to install, because they require additional components like optical receivers. So, as with your choice of network topology, the wiring you select depends on the needs of your network, including which applications you'll be running, the transmission distance, and desired performance.

Cost

As I've mentioned, the installation cost is important to account for, as the more complex network topologies will require more time and funding to set up. This can be compounded if you're combining different elements, such as connecting a more complex network structure via more expensive cables (though using fiber-optic cables in a mesh network is overdoing it, if you ask me, because of how interconnected the topology is). Determining the right topology for your needs, then, is a matter of striking the right balance between installation and operating costs and the level of performance you require from the network.

Scalability

The last element to consider is scalability. If you anticipate your company and network expanding—or if you'd like it to be able to—it'll save you time and hassle down the line to use an easily modifiable network topology. Star topologies are so common because they allow you to add, remove, and alter nodes with minimal disruption to the rest of the network. Ring networks, on the other hand, have to be taken entirely offline for any changes to be made to any of the nodes.

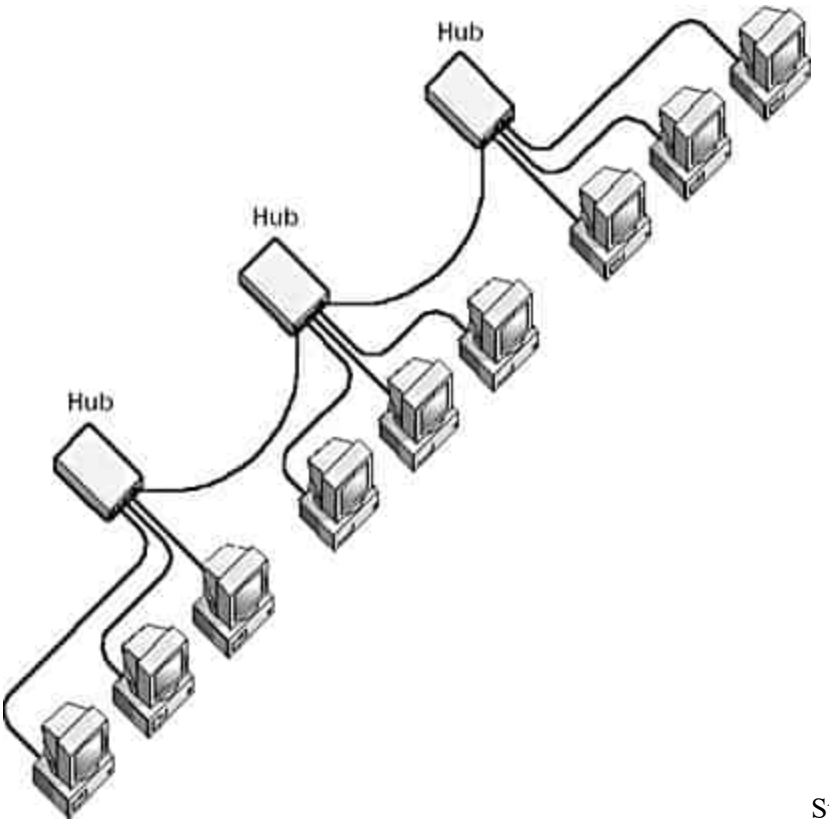
How to Map Network Topology

When you're starting to design a network, topology diagrams come in handy. They allow you to see how the information will move across the network, which, in turn, allows you to predict potential choke points. Visual representation makes it easier to create a streamlined and efficient network design, while also acting as a good reference point if you find yourself needing to troubleshoot errors.

A topology diagram is also essential for having a comprehensive understanding of your network's functionality. In addition to assisting with the troubleshooting process, the bird's-eye view provided by a topology diagram can help you visually identify the pieces of the infrastructure your network is lacking, or which nodes need monitoring, upgrading, or replacing.

What is Star Bus Topology?

Star Bus is a networking topology in which hubs for workgroups or departmental local area networks (LANs) are connected by using a network bus to form a single network. Star bus topology is a combination of star topology superimposed on a backbone bus topology.



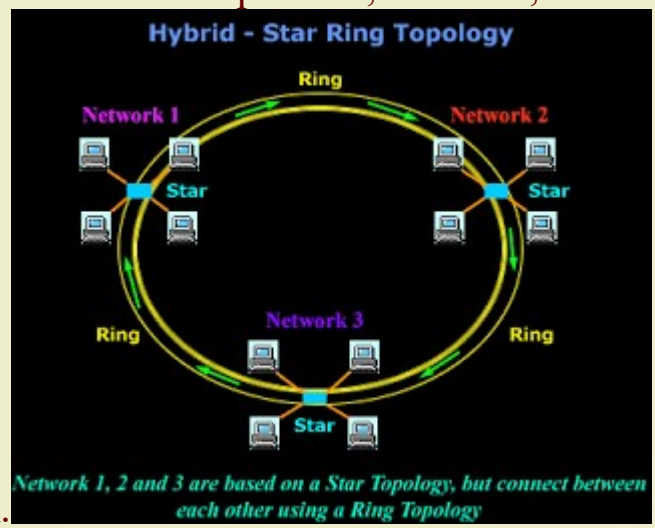
Star Bus Topology

You can connect hubs by using one of the following:

- Regular 10Base2 or 10BaseT cables with uplink ports on the hubs
- Crossover cables for regular (host) ports on the hub
- Special cables for stackable hubs

Star-Ring topology

- In the Star-Ring topology, the computers are connected to a central component as in a star network. These components, however, are wired to form a ring network.



- Like the star-bus topology, if a single computer fails, it will not affect the rest of the network. By using token passing, each computer in a star-ring topology has an equal chance of communicating. This allows for greater network traffic between segments than in a star-bus topology.

Logical Topology

A logical topology is a concept in networking that defines the architecture of the communication mechanism for all nodes in a network. Using network equipment such as routers and switches, the logical topology of a network can be dynamically maintained and reconfigured.

Logical topologies contrasts with physical topologies, which refer to the physical interconnections of all devices in the network.
The logical topology defines how the data should transfer. Contrast this to the physical topology, which consists of the layout of cables, network devices and wiring.

Two of the most common logical topologies are:

- Bus topology: Ethernet uses the logical bus topology to transfer data. Under a bus topology a node broadcasts the data to the entire network. All other nodes on the network hear the data and check if the data is intended for them.
- Ring topology: In this topology, only one node can be allowed to transfer the data in a network at a given time. This mechanism is achieved by token (the node having token only can transmit the data in a network) and hence the collision can be avoided in a network.

How to select a Network Topology?

Here are some important considerations for selecting the best topology to create a network in your organization:

- Bus topology is surely least expensive to install a network.
- If you want to use a shorter cable or you planning to expand the network is future, then star topology is the best choice for you.
- Fully mesh topology is theoretically an ideal choice as every device is connected to every other device.
- If you want to use twisted pair cable for networking, then you should build star topologies.

A logical topology is a concept in networking that defines the architecture of the communication mechanism for all nodes in a network. Using network equipment such as routers and switches, the logical topology of a network can be dynamically maintained and reconfigured.

Logical topologies contrast with physical topologies, which refer to the physical interconnections of all devices in the network.
The logical topology defines how the data should transfer. Contrast this to the physical topology, which consists of the layout of cables, network devices and wiring.

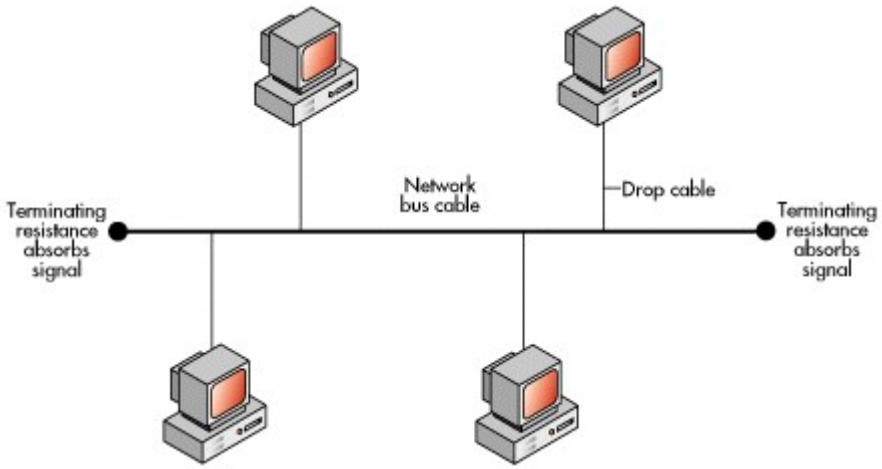
Two of the most common logical topologies are:

- Bus topology: Ethernet uses the logical bus topology to transfer data. Under a bus topology a node broadcasts the data to the entire network. All other nodes on the network hear the data and check if the data is intended for them.
- Ring topology: In this topology, only one node can be allowed to transfer the data in a network at a given time. This mechanism is achieved by token (the node having token only can transmit the data in a network) and hence the collision can be avoided in a network.

1. Bus Topology

The bus topology is the type of logical topology in which all the nodes and switches are connected to only one single cable which can be also known as backbone or bus. The nodes are connected like half-duplex mode. In the bus

topology, there is a host which is known as a station. The bus topology has multiple stations that have the capability to receive the network traffic and also have equal priority to transmit the network traffic in the network. And in the bus topology, the network is controlled by bus master which can be CSMA (carrier sense multiple access). In the bus topology, if any single segment goes down the whole network can be affected due to node failure.



Advantages of Bus Topology

1. The bus topology is easy to create and the devices can be connected to the bus easily.
2. The bus topology is very effective when the network size is small. The large network will contain a large number of nodes which can create a

problem to maintain the network and can increase the chance of network failure. So the bus topology is effective for the small size of the network.

3. The network created by the bus topology is very reliable and the network can be easily maintained.
4. The setup cost for bus topology is very less as the length of the wire is small because all nodes are connected to the bus which decreases the network cost.
5. The other network device can be easily connected to the bus like connectors and repeater. The only requirement is joining cable which will join an external device to the bus.

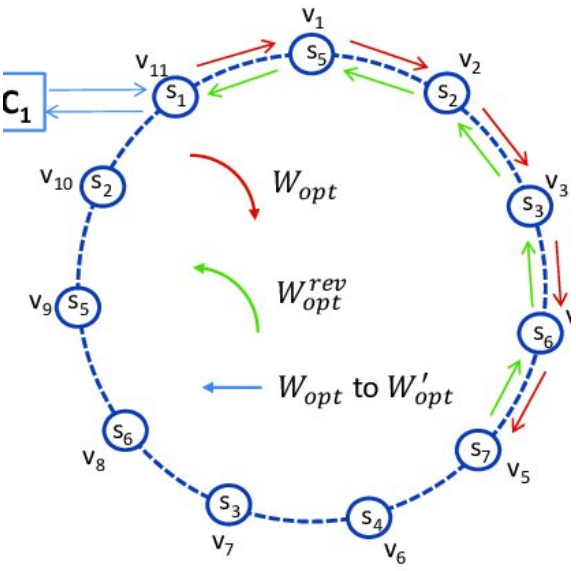
Disadvantages of Bus Topology

1. The performance results of bus topology are least if it is compared to other network topologies.
2. As all the nodes are connected to one single cable and if that single cable goes down the whole network will go down. This creates a major risk of network failure in case of bus topology.

3. The packet collisions problem is there in bus topology. Due to packet collisions, the packet loss issue occurred which creates problems in data communication in a network.

2. Ring Topology

The ring topology is another type of logical topology in which all the nodes are connected in such a manner that they form a circular path. Every node in the circular path is connected to two nodes. In this type of topology, when any source node sends any data packet it gets transferred from each node until the destination node is reached. The data packets can flow in two directions in ring topology either unidirectional or bidirectional. The ring topology is mostly used in Wide Area Network (WANs) and Local Area Network (LANs).



Advantages of Ring Topology

1. The ring topology is effective for heavy traffic load compares to bus topology. The network congestion is not there in a ring topology.
2. Every node is responsible to transmit the data packets o adjacent nodes.
3. There is no central node in the ring topology which controls the network.

Disadvantages of Network Topology

1. If any node goes down the whole network is failed in the ring topology because the connection is the break.
2. The new device cannot be added or removed from the network.

Importance of Logical Topology

The logical topology helps to create the blueprint of the network. It helps to design the network and tells the structure of a network. Using the logical topology, the network can be implemented by using the physical topology. The logical topology helps to design the initial structure of the network and if any change is where it can be done before implementing the network physically.

network protocols

Network protocols are sets of established rules that dictate how to format, transmit and receive data so computer network devices -- from servers and routers to endpoints -- can communicate regardless of the differences in their underlying infrastructures, designs or standards.

Network protocols are formal standards and policies comprised of rules, procedures and formats that define communication between two or more devices over a network.

They ensure that computer network devices can transmit and receive data using a common language regardless of their different designs, hardware or infrastructures.

Network protocols govern the end-to-end processes of timely, secure and managed data or network communication.

They can be built into hardware or software, and they’re so important that, in practice, every network use rely on network protocols for communications and connectivity.

Wireless means transmitting signals using radio waves as the medium instead of wires. Wireless technologies are used for tasks as simple as switching off the television or as complex as supplying the sales force with information from an automated enterprise application while in the field. Now cordless keyboards and mice, PDAs, pagers and digital and cellular phones have become part of our daily life.

Some of the inherent characteristics of wireless communications systems which make it attractive for users, are given below −

- **Mobility** − A wireless communications system allows users to access information beyond their desk and conduct business from anywhere without having a wire connectivity.
- **Reachability** − Wireless communication systems enable people to be stay connected and be reachable, regardless of the location they are operating from.
- **Simplicity** − Wireless communication system are easy and fast to deploy in comparison of cabled network. Initial setup cost could be a bit high but other advantages overcome that high cost.
- **Maintainability** − In a wireless system, you do not have to spend too much cost and time to maintain the network setup.

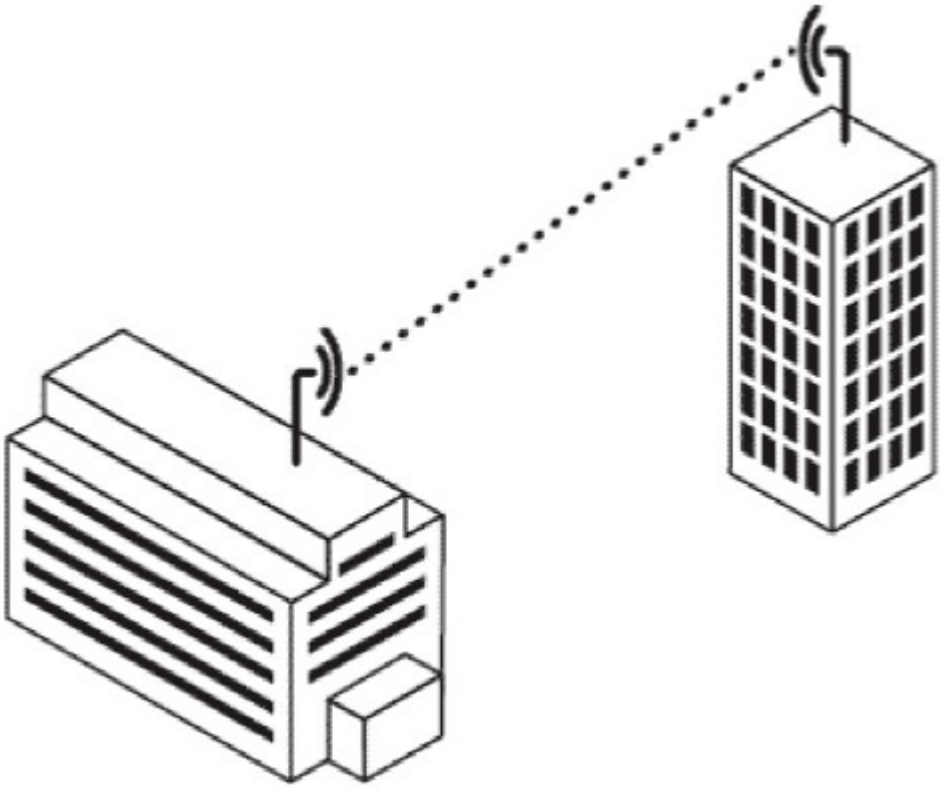
- **Roaming Services** − Using a wireless network system, you can provide service any where any time including train, buses, aeroplanes etc.
- **New Services** − Wireless communication systems provide various smart services like SMS and MMS.

Wireless Network Topologies

There are basically three ways to set up a wireless network −

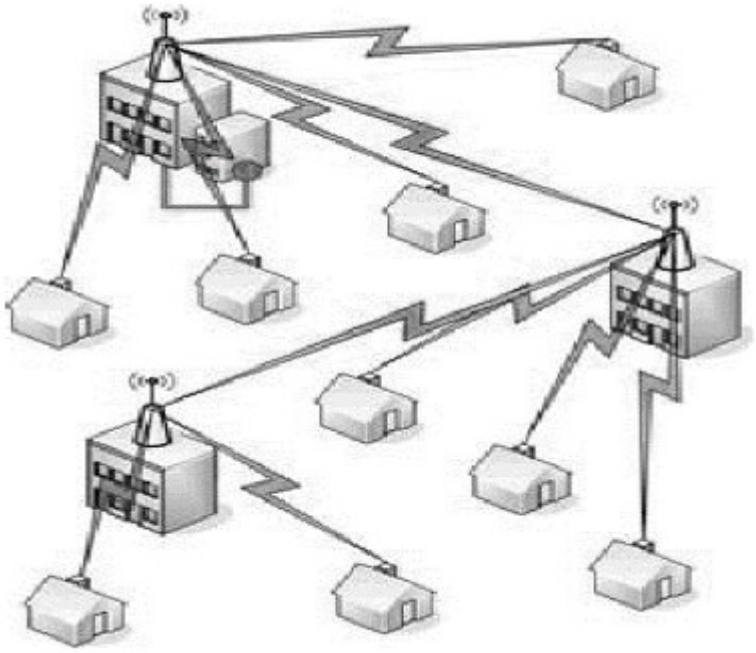
Point-to-point bridge

As you know, a bridge is used to connect two networks. A *point-to-point bridge* interconnects two buildings having different networks. For example, a wireless LAN bridge can interface with an Ethernet network directly to a particular access point (as shown in the following image).



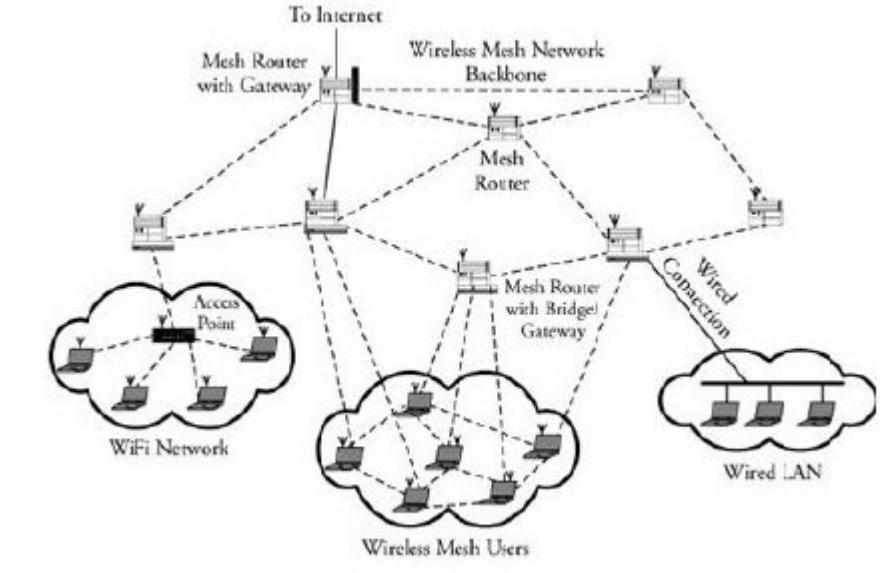
Point-to-multipoint bridge

This topology is used to connect three or more LANs that may be located on different floors in a building or across buildings(as shown in the following image).



Mesh or ad hoc network

This network is an independent local area network that is not connected to a wired infrastructure and in which all stations are connected directly to one another(as shown in the following image).



Wireless Technologies

Wireless technologies can be classified in different ways depending on their range. Each wireless technology is designed to serve a specific usage segment. The requirements for each usage segment are based on a variety of variables, including Bandwidth needs, Distance needs and Power.

Wireless Wide Area Network (WWAN)

This network enables you to access the Internet via a wireless wide area network (WWAN) access card and a PDA or laptop.

These networks provide a very fast data speed compared with the data rates of mobile telecommunications technology, and their range is also extensive. Cellular and mobile networks based on CDMA and GSM are good examples of WWAN.

Wireless Personal Area Network (WPAN)

These networks are very similar to WWAN except their range is very limited.

Wireless Local Area Network (WLAN)

This network enables you to access the Internet in localized hotspots via a wireless local area network (WLAN) access card and a PDA or laptop.

It is a type of local area network that uses high-frequency radio waves rather than wires to communicate between nodes.

These networks provide a very fast data speed compared with the data rates of mobile telecommunications technology, and their range is very limited. Wi-Fi is the most widespread and popular example of WLAN technology.

Wireless Metropolitan Area Network (WMAN)

This network enables you to access the Internet and multimedia streaming services via a wireless region area network (WRAN).

These networks provide a very fast data speed compared with the data rates of mobile telecommunication technology as well as other wireless network, and their range is also extensive.

Issues with Wireless Networks

There are following three major issues with Wireless Networks.

- **Quality of Service (QoS)** − One of the primary concerns about wireless data delivery is that, unlike the Internet through wired services, QoS is inadequate. Lost packets and atmospheric interference are recurring problems of the wireless protocols.
- **Security Risk** − This is another major issue with a data transfer over a wireless network. Basic network security mechanisms like the *service set identifier (SSID) and Wireless Equivalency Privacy (WEP);* these measures may be adequate for residences and small businesses, but they are inadequate for the entities that require stronger security.
- **Reachable Range** − Normally, wireless network offers a range of about 100 meters or less. Range is a function of antenna design and power. Now a days the range of wireless is extended to tens of miles so this should not be an issue any more.

Wireless Broadband Access (WBA)

Broadband wireless is a technology that promises high-speed connection over the air. It uses radio waves to transmit and receive data directly to and from the potential users whenever they want it. Technologies such as 3G, Wi-Fi, WiMAX and UWB work together to meet unique customer needs.

WBA is a point-to-multipoint system which is made up of base station and subscriber equipment. Instead of using the physical connection between the base station and the subscriber, the base station uses an outdoor antenna to send and receive high-speed data and voice-to-subscriber equipment.

WBA offers an effective, complementary solution to wireline broadband, which has become globally recognized by a high percentage of the population.

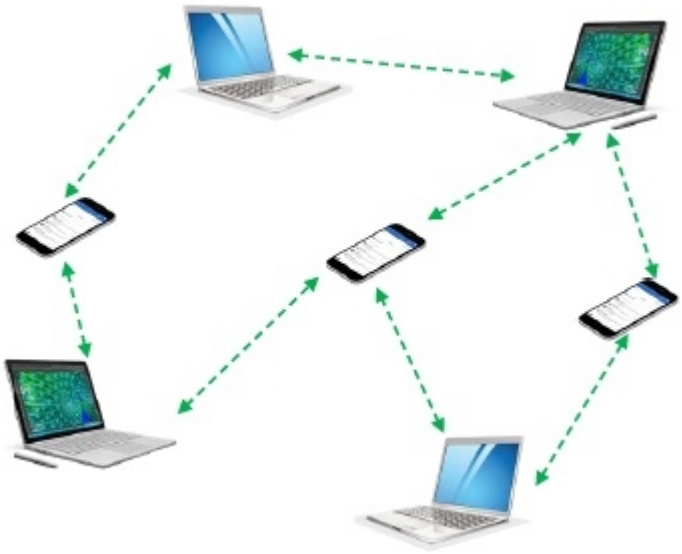
What is Wi-Fi ?

Wi-Fi stands for **Wi**reless **Fi**delity. Wi-Fi is based on the IEEE 802.11 family of standards and is primarily a local area networking (LAN) technology designed to provide in-building broadband coverage.

Ad-hoc Wireless

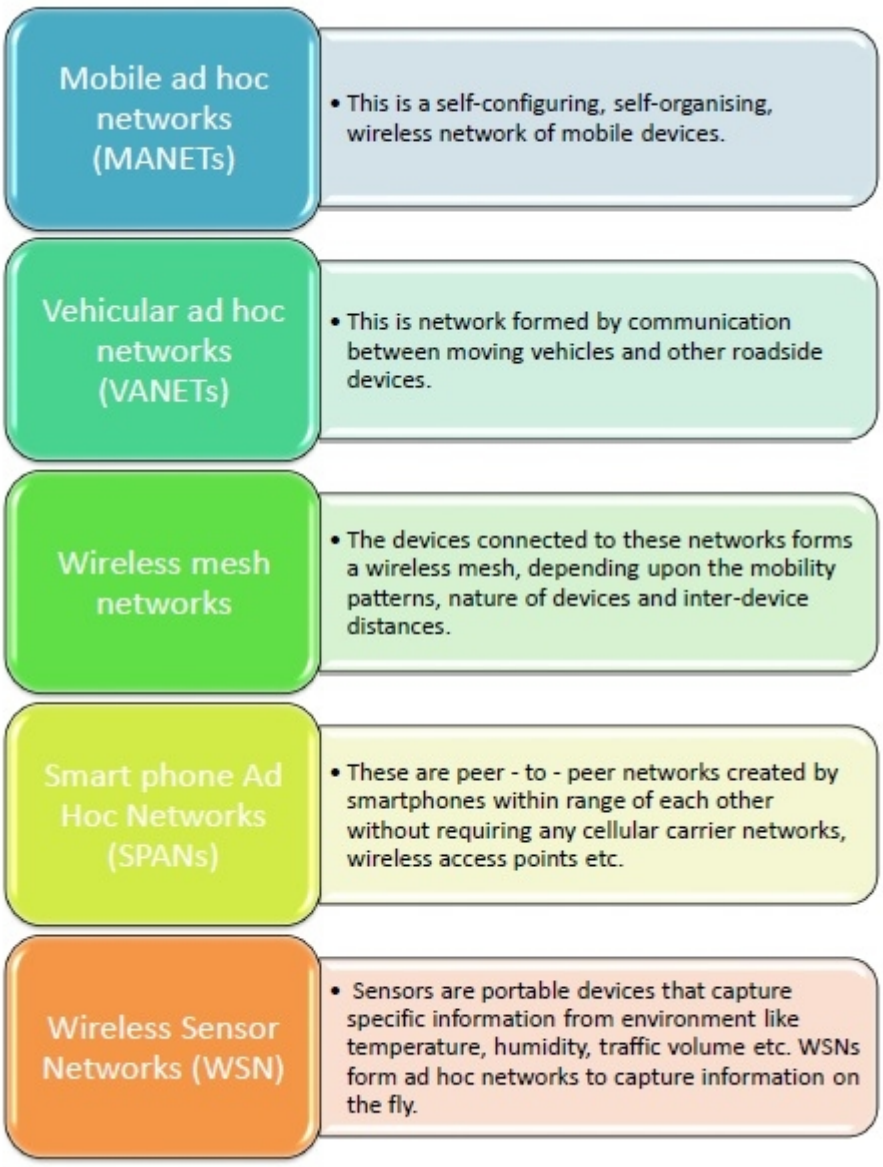
An ad hoc network is one that is spontaneously formed when devices connect and communicate with each other. The term ad hoc is a Latin word that literally means "for this," implying improvised or impromptu.

Ad hoc networks are mostly wireless local area networks (LANs). The devices communicate with each other directly instead of relying on a base station or access points as in wireless LANs for data transfer co-ordination. Each device participates in routing activity, by determining the route using the routing algorithm and forwarding data to other devices via this route.



Classifications of Ad Hoc Networks

Ad hoc networks can be classified into several types depending upon the nature of their applications. The most prominent ad hoc networks that are commonly incorporated are illustrated in the diagram below −


Mobile ad hoc networks (MANETs)
• This is a self-configuring, self-organising, wireless network of mobile devices.
Vehicular ad hoc networks (VANETs)
• This is network formed by communication between moving vehicles and other roadside devices.
Wireless mesh networks
• The devices connected to these networks forms a wireless mesh, depending upon the mobility patterns, nature of devices and inter-device distances.
Smart phone Ad Hoc Networks (SPANs)
• These are peer - to - peer networks created by smartphones within range of each other without requiring any cellular carrier networks, wireless access points etc.
Wireless Sensor Networks (WSN)
• Sensors are portable devices that capture specific information from environment like temperature, humidity, traffic volume etc. WSNs form ad hoc networks to capture information on the fly.

What does *Distributed Processing* mean?

Distributed processing is a setup in which multiple individual central processing units (CPU) work on the same programs, functions or systems to provide more capability for a computer or other device.

What is Data Communication?

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

For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).

Characteristics of Data Communications:

The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

1. Delivery:

The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

2. Accuracy:

The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

3. Timeliness:

The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.

4. Jitter:

Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 3D ms. If some of the packets arrive with 3D-ms delay and others with 4D-ms delay, an uneven quality in the video is the result.

Data Communication Network:

Data communications are the exchange of data between two devices using one

or multiple forms of transmission medium. That is, data communication is movement of data from one device or end-point to another device or end point through electrical or optical medium. Systems that facilitate this movement of data between devices or end-points are called data communication network. The devices which are in need to be a part of a data communication network made up of computer hardware and software.
Data communication networks collect data from devices such as microphone and let the data to be carried to the receiver or destination such as a micro-computer or minicomputer. However, it could be the opposite, that is data communication networks can also carry data from a micro-computer or minicomputer to a device such as printer. Data communications networks facilitate more efficient use of computers and improve the day-to-day control of a business by providing faster information flow. They also provide message transfer services to allow computer users to talk to one another via electronic mail, chat, and video streaming.

Following are the five components of a data communication network.

1. Data
2. Sender
3. Receiver
4. Transmission Medium
5. Protocol

Figure 1: Five Components of data communications system

5 Components of a Data Communication Network

Data:

Communication of data means a message or data will be transmitted from one device and will be received in the destination or target device. Thus the first component in a data communication network is data or message to that needs to be delivered and received. Data or message can be of various forms such as text, audio, video, image or combinations of these forms etc.

Sender:

A data must has to be sent to a destination from a source. This source is called the sender. The device that sends the data to the destination or target is the Sender. It can be a computer, cell phone, video camera and so on.

Receiver:

The destination of a transmitted data is the receiver which will receive the data. The device that receives the data that was sent by the Sender is the Receiver. A receiver can again be a computer, cell phone, video camera and so on.

Transmission medium:

In data communication network, the transmission medium is the physical path for the data to travel to its destination after being sent by the Sender. Receiver receives the data at one end of this path and the sender sent from another end of the path. Transmission medium could be like twisted-pair cable, coaxial cable, fiber-optic cable etc.

Protocol:

A protocol is nothing but a set of rules that applies on the full data communication procedure. This is like an agreement between the two devices to successfully communicate with each other. For example, how the data will be sent, how the data will be traveling, how to ensure that full data has received, how to handle errors in transmission etc. Both devices follow the same set of rules or protocol so that they understand each other.

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, 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.

Computer Networks: Business Applications

Following are some business applications of computer networks:

1. Resource Sharing:

The goal is to make all programs, equipments(like printers etc), and especially data, available to anyone on the network without regard to the physical location of the resource and the user.

2. Server-Client model:

One can imagine a company's information system as consisting of one or more databases and some employees who need to access it remotely. In this model, the data is stored on powerful computers called **Servers**. Often these are centrally housed and maintained by a system administrator. In contrast, the employees have simple machines, called **Clients**, on their desks, using which they access remote data.

3. Communication Medium:

A computer network can provide a powerful communication medium among employees. Virtually every company that has two or more computers now has e-mail (electronic mail), which employees generally use for a great deal of daily communication

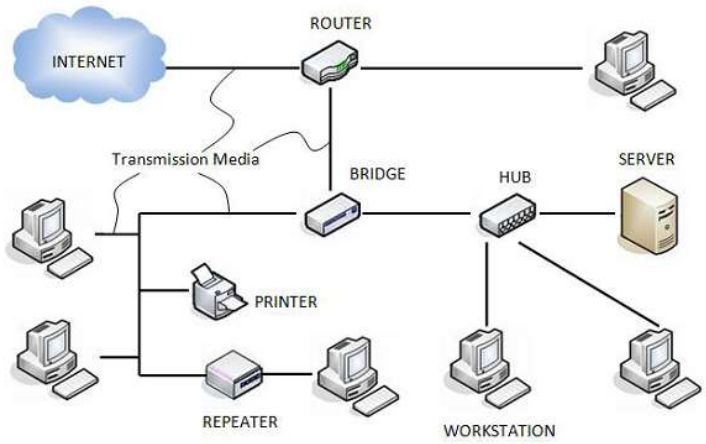
4. eCommerce:

A goal that is starting to become more important in businesses is doing business with consumers over the Internet. Airlines, bookstores and music vendors have discovered that many customers like the convenience of shopping from home. This sector is expected to grow quickly in the future.

Computer Network Components

Computer networks components comprise both physical parts as well as the software required for installing computer networks, both at organizations and at home. The hardware components are the server, client, peer, transmission medium, and connecting devices. The software components are operating system and protocols.

The following figure shows a network along with its components −



COMPUTER NETWORK COMPONENTS

Hardware Components

- **Servers** −Servers are high-configuration computers that manage the resources of the network. The network operating system is typically installed in the server and so they give user accesses to the network resources. Servers can be of various kinds: file servers, database servers, print servers etc.
- **Clients** − Clients are computers that request and receive service from the servers to access and use the network resources.
- **Peers** − Peers are computers that provide as well as receive services from other peers in a workgroup network.
- **Transmission Media** − Transmission media are the channels through which data is transferred from one device to another in a network. Transmission media may be guided media like coaxial cable, fibre optic cables etc; or maybe unguided media like microwaves, infra-red waves etc.
- **Connecting Devices** − Connecting devices act as middleware between networks or computers, by binding the network media together. Some of the common connecting devices are:

  a. Routers

  b. Bridges

c. Hubs

d. Repeaters

e. Gateways

f. Switches

Software Components

- **Networking Operating System** − Network Operating Systems is typically installed in the server and facilitate workstations in a network to share files, database, applications, printers etc.
- **Protocol Suite** − A protocol is a rule or guideline followed by each computer for data communication. Protocol suite is a set of related protocols that are laid down for computer networks. The two popular protocol suites are −
    - a. OSI Model (Open System Interconnections)
    - b. TCP / IP Model

IEEE 802.3

IEEE 802.3 is a working group and a collection of Institute of Electrical and Electronics Engineers (IEEE) standards produced by the working group defining the physical layer and data link layer's media access control (MAC) of wired Ethernet. This is generally a local area network (LAN) technology with some wide area network (WAN) applications. Physical connections are made between nodes and/or infrastructure devices (hubs, switches, routers) by various types of copper or fiber cable.

802.3 is a technology that supports the IEEE 802.1 network architecture.

802.3 also defines LAN access method using CSMA/CD.

Specification	Data Rate	Modulation Scheme	Security
802.11	1 or 2 Mbps in the 2.4 GHz band	FHSS, DSSS	WEP and WPA
802.11a	54 Mbps in the 5 GHz band	OFDM	WEP and WPA
802.11b/High Rate/Wi-Fi	11 Mbps (with a fallback to 5.5, 2, and 1 Mbps) in the 2.4 GHz band	DSSS with CCK	WEP and WPA
802.11g/Wi-Fi	54 Mbps in the 2.4 GHz band	OFDM when above 20Mbps, DSSS with CCK when below 20Mbps	WEP and WPA

Ethernet

Ethernet is the most popular physical layer LAN technology in use today. It defines the number of conductors that are required for a connection, the performance thresholds that can be expected, and provides the framework for data transmission. A standard Ethernet network can transmit data at a rate up to 10 Megabits per second (10 Mbps). Other LAN types include Token Ring, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, Fiber Distributed Data Interface (FDDI), Asynchronous Transfer Mode (ATM) and LocalTalk.

Ethernet is popular because it strikes a good balance between speed, cost and ease of installation. These benefits, combined with wide acceptance in the computer marketplace and the ability to support virtually all popular network protocols, make Ethernet an ideal networking technology for most computer users today.

The Institute for Electrical and Electronic Engineers developed an Ethernet standard known as IEEE Standard 802.3. This standard defines rules for configuring an Ethernet network and also specifies how the elements in an Ethernet network interact with one another. By adhering to the IEEE standard, network equipment and network protocols can communicate efficiently.

Fast Ethernet

The Fast Ethernet standard (IEEE 802.3u) has been established for Ethernet networks that need higher transmission speeds. This standard raises the Ethernet speed limit from 10 Mbps to 100 Mbps with only minimal changes to the existing cable structure. Fast Ethernet provides faster throughput for video, multimedia, graphics, Internet surfing and stronger error detection and correction.

There are three types of Fast Ethernet: 100BASE-TX for use with level 5 UTP cable; 100BASE-FX for use with fiber-optic cable; and 100BASE-T4 which utilizes an extra two wires for use with level 3 UTP cable. The 100BASE-TX standard has become the most popular due to its close compatibility with the 10BASE-T Ethernet standard.

Network managers who want to incorporate Fast Ethernet into an existing configuration are required to make many decisions. The number of users in each site on the network that need the higher throughput must be determined; which segments of the backbone need to be reconfigured specifically for 100BASE-T; plus what hardware is necessary in order to connect the 100BASE-T segments with existing 10BASE-T segments. Gigabit Ethernet is a future technology that promises a migration path beyond Fast Ethernet so the next generation of networks will support even higher data transfer speeds.

Gigabit Ethernet

Gigabit Ethernet was developed to meet the need for faster communication networks with applications such as multimedia and Voice over IP (VoIP). Also known as “gigabit-Ethernet-over-copper” or 1000Base-T, GigE is a version of Ethernet that runs at speeds 10 times faster than 100Base-T. It is defined in the IEEE 802.3 standard and is currently used as an enterprise backbone. Existing Ethernet LANs with 10 and 100 Mbps cards can feed into a Gigabit Ethernet backbone to interconnect high performance switches, routers and servers.

From the data link layer of the OSI model upward, the look and implementation of Gigabit Ethernet is identical to that of Ethernet. The most important differences between Gigabit Ethernet and Fast Ethernet include the additional support of full duplex operation in the MAC layer and the data rates.

10 Gigabit Ethernet

10 Gigabit Ethernet is the fastest and most recent of the Ethernet standards. IEEE 802.3ae defines a version of Ethernet with a nominal rate of 10Gbits/s that makes it 10 times faster than Gigabit Ethernet.

Unlike other Ethernet systems, 10 Gigabit Ethernet is based entirely on the use of optical fiber connections. This developing standard is moving away from a LAN design that broadcasts to all nodes, toward a system which includes some elements of wide area routing. As it is still very new, which of the standards will gain commercial acceptance has yet to be determined.

Asynchronous Transfer Mode (ATM)

ATM is a cell-based fast-packet communication technique that can support data-transfer rates from sub-T1 speeds to 10 Gbps. ATM achieves its high speeds in part by transmitting data in fixed-size cells and dispensing with error-correction protocols. It relies on the inherent integrity of digital lines to ensure data integrity.

ATM can be integrated into an existing network as needed without having to update the entire network. Its fixed-length cell-relay operation is the signaling technology of the future and offers more predictable performance than variable length frames. Networks are extremely versatile and an ATM network can connect points in a building, or across the country, and still be treated as a single network.

Power over Ethernet (PoE)

PoE is a solution in which an electrical current is run to networking hardware over the Ethernet Category 5 cable or higher. This solution does not require an extra AC power cord at the product location. This minimizes the amount of cable needed as well as eliminates the difficulties and cost of installing extra outlets.

LAN Technology Specifications

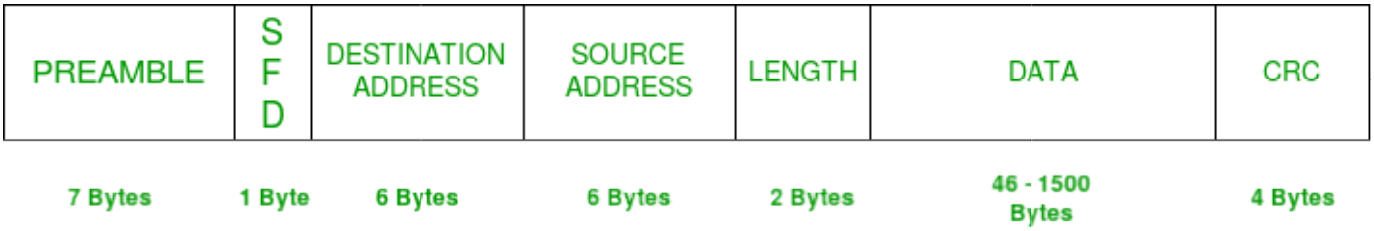
Name	IEEE Standard	Data Rate	Media Type	Maximum Distance
Ethernet	802.3	10 Mbps	10Base-T	100 meters
Fast Ethernet/ 100Base-T	802.3u	100 Mbps	100Base-TX 100Base-FX	100 meters 2000 meters
Gigabit Ethernet/ GigE	802.3z	1000 Mbps	1000Base-T 1000Base-SX 1000Base-LX	100 meters 275/550 meters 550/5000 meters
10 Gigabit Ethernet	IEEE 802.3ae	10 Gbps	10GBase-SR 10GBase-LX4 10GBase-LR/ER 10GBase-SW/LW/EW	300 meters 300m MMF/ 10km SMF 10km/40km 300m/10km/40km

Ethernet Frame Format

Prerequisite – Introduction to Ethernet
Basic frame format which is required for all MAC implementation is defined in **IEEE 802.3 standard**. Though several optional formats are being used to extend the protocol's basic capability.

Ethernet frame starts with Preamble and SFD, both works at the physical layer. Ethernet header contains both Source and Destination MAC address, after which the payload of the frame is present. The last field is CRC which is used to detect the error. Now, let's study each field of basic frame format.

Ethernet (IEEE 802.3) Frame Format –



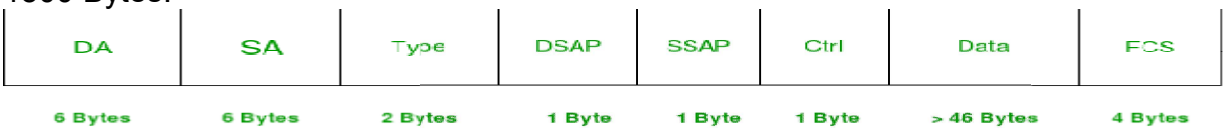
IEEE 802.3 ETHERNET Frame Format

- **PREAMBLE** – Ethernet frame starts with 7-Bytes Preamble. This is a pattern of alternative 0's and 1's which indicates starting of the frame and allows sender and receiver to establish bit synchronization. Initially, PRE (Preamble) was introduced to allow for the loss of a few bits due to signal delays. But today's high-speed Ethernet don't need Preamble to protect the frame bits.
  PRE (Preamble) indicates the receiver that frame is coming and allow the receiver to lock onto the data stream before the actual frame begins.
- **Start of frame delimiter (SFD)** – This is a 1-Byte field which is always set to 10101011. SFD indicates that upcoming bits are starting of the frame, which is the destination address. Sometimes SFD is considered the part of PRE, this is the reason Preamble is described as 8 Bytes in many places. The SFD warns station or stations that this is the last chance for synchronization.
- **Destination Address** – This is 6-Byte field which contains the MAC address of machine for which data is destined.
- **Source Address** – This is a 6-Byte field which contains the MAC address of source machine. As Source Address is always an individual address (Unicast), the least significant bit of first byte is always 0.
- **Length** – Length is a 2-Byte field, which indicates the length of entire Ethernet frame. This 16-bit field can hold the length value between 0 to 65534, but length cannot be larger than 1500 because of some own limitations of Ethernet.
- **Data** – This is the place where actual data is inserted, also known as **Payload**. Both IP header and data will be inserted here if Internet Protocol is used over Ethernet. The maximum data present may be as long as 1500 Bytes. In case data length is less than minimum length i.e. 46 bytes, then padding 0's is added to meet the minimum possible length.
- **Cyclic Redundancy Check (CRC)** – CRC is 4 Byte field. This field contains a 32-bits hash code of data, which is generated over the Destination Address, Source Address, Length, and Data field. If the checksum computed by destination is not the same as sent checksum value, data received is corrupted.

Note – Size of frame of Ethernet IEEE 802.3 varies 64 bytes to 1518 bytes including data length (46 to 1500 bytes).

Brief overview on Extended Ethernet Frame (Ethernet II Frame) :

Standard IEEE 802.3 basic frame format is discussed above in detail. Now let's see the extended Ethernet frame header, using which we can get Payload even larger than 1500 Bytes.



Proposed ETHERNET Frame Extension

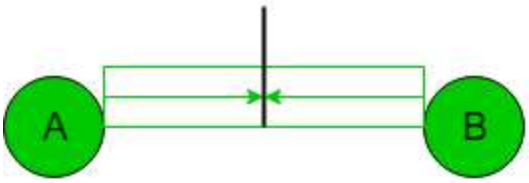
DA [Destination MAC Address] : ***6 bytes***
SA [Source MAC Address] : ***6 bytes***
Type [0x8870 (Ethertype)] : ***2 bytes***
DSAP [802.2 Destination Service Access Point] : ***1 byte***
SSAP [802.2 Source Service Access Point] : ***1 byte***
Ctrl [802.2 Control Field] : ***1 byte***
Data [Protocol Data] : > ***46 bytes***
FCS [Frame Checksum] : ***4 bytes***

Back-off Algorithm for CSMA/CD

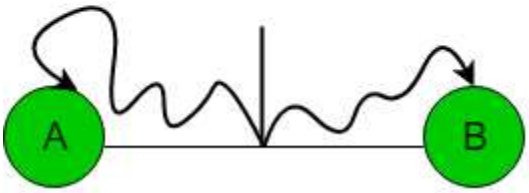
Prerequisite – Basics of CSMA/ CD, Collision Detection in CSMA/CD
Back-off algorithm is a **collision resolution** mechanism which is used in random access MAC protocols (CSMA/CD). This algorithm is generally used in Ethernet to schedule re-transmissions after collisions.
If a collision takes place between 2 stations, they may restart transmission as soon as they can after the collision. This will always lead to another collision and form an infinite loop of collisions leading to a deadlock. To prevent such scenario back-off algorithm is used.

Let us consider an scenario of 2 stations A and B transmitting some data:

At t = 0 , both A and B start transmission



Packets of both A and B collide



Both stations A and B detect collision

After a collision, time is divided into discrete slots (T_{slot}) whose length is equal to 2t, where t is the maximum propagation delay in the network.

The stations involved in the collision randomly pick an integer from the set K i.e {0, 1}. This set is called the contention window. If the sources collide again because they picked the same integer, the contention window size is doubled and it becomes {0, 1, 2, 3}. Now the sources involved in the second collision randomly pick an integer from the

set {0, 1, 2, 3} and wait that number of time slots before trying again. Before they try to transmit, they listen to the channel and transmit only if the channel is idle. This causes the source which picked the smallest integer in the contention window to succeed in transmitting its frame.

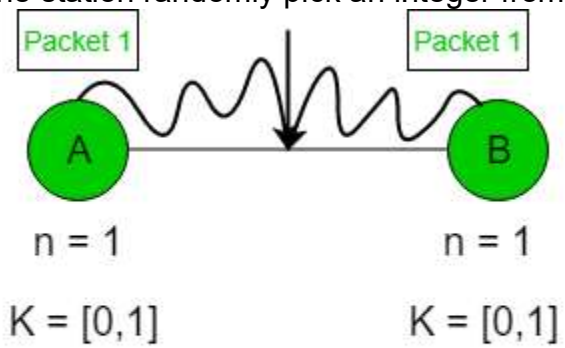
So, Back-off algorithm defines a *waiting time for the stations involved in collision*, i.e. for how much time the station should wait to re-transmit.

```
Waiting time = back-off time

Let n = collision number or re-transmission serial number.

Then,

Waiting time = K * T_slot
where K = [0, 2^n - 1 ]
```

Example –

Case-1 :

Suppose 2 stations A and B start transmitting data (Packet 1) at the same time then, collision occurs. So, the collision number n for both their data (Packet 1) = 1. Now, both the station randomly pick an integer from the set K i.e. {0, 1}.



Value of K

A	B
0	0
0	1
1	0
1	1

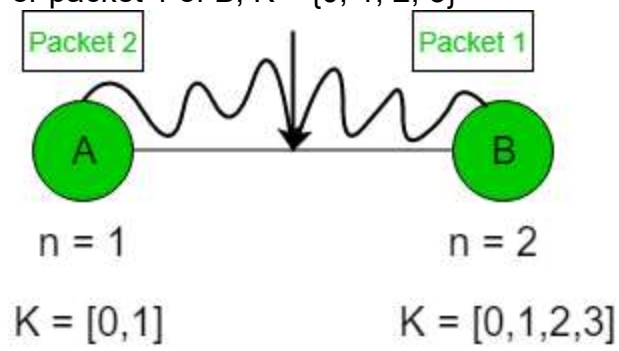
- **When both A and B choose K = 0**
  –> Waiting time for A = 0 * T_{slot} = 0
  Waiting time for B = 0 * T_{slot} = 0
  Therefore, both stations will transmit at the same time and hence collision occurs.
- **When A chooses K = 0 and B chooses K = 1**
  –> Waiting time for A = 0 * T_{slot} = 0
  Waiting time for B = 1 * T_{slot} = T_{slot}
  Therefore, A transmits the packet and B waits for time T_{slot} for transmitting and hence A wins.
- **When A chooses K = 1 and B chooses K = 0**
  –> Waiting time for A = 1 * T_{slot} = T_{slot}
  Waiting time for B = 0 * T_{slot} = 0

Therefore, B transmits the packet and A waits for time T_{slot} for transmitting and hence B wins.

- **When both A and B choose K = 1**
  –> Waiting time for A = 1 * T_{slot} = T_{slot}
  Waiting time for B = 1 * T_{slot} = T_{slot}
  Therefore, both will wait for the same time T_{slot} and then transmit. Hence, collision occurs.

```
Probability that A wins = 1/4

Probability that B wins = 1/4

Probability of collision  = 2/4
```

Case-2 :
Assume that A wins in Case 1 and transmitted its data(Packet 1). Now, as soon as B transmits its packet 1, A transmits its packet 2. Hence, collision occurs. Now collision no. n becomes 1 for packet 2 of A and becomes 2 for packet 1 of B.
For packet 2 of A, K = {0, 1}
For packet 1 of B, K = {0, 1, 2, 3}



Value of K

A	B
0	0
0	1
0	2
0	3
1	0
1	1
1	2
1	3

```
Probability that A wins = 5/8

Probability that B wins = 1/8

Probability of collision  = 2/8
```

So, probability of collision decreases as compared to Case 1.

Advantage –

- Collision probability decreases exponentially.

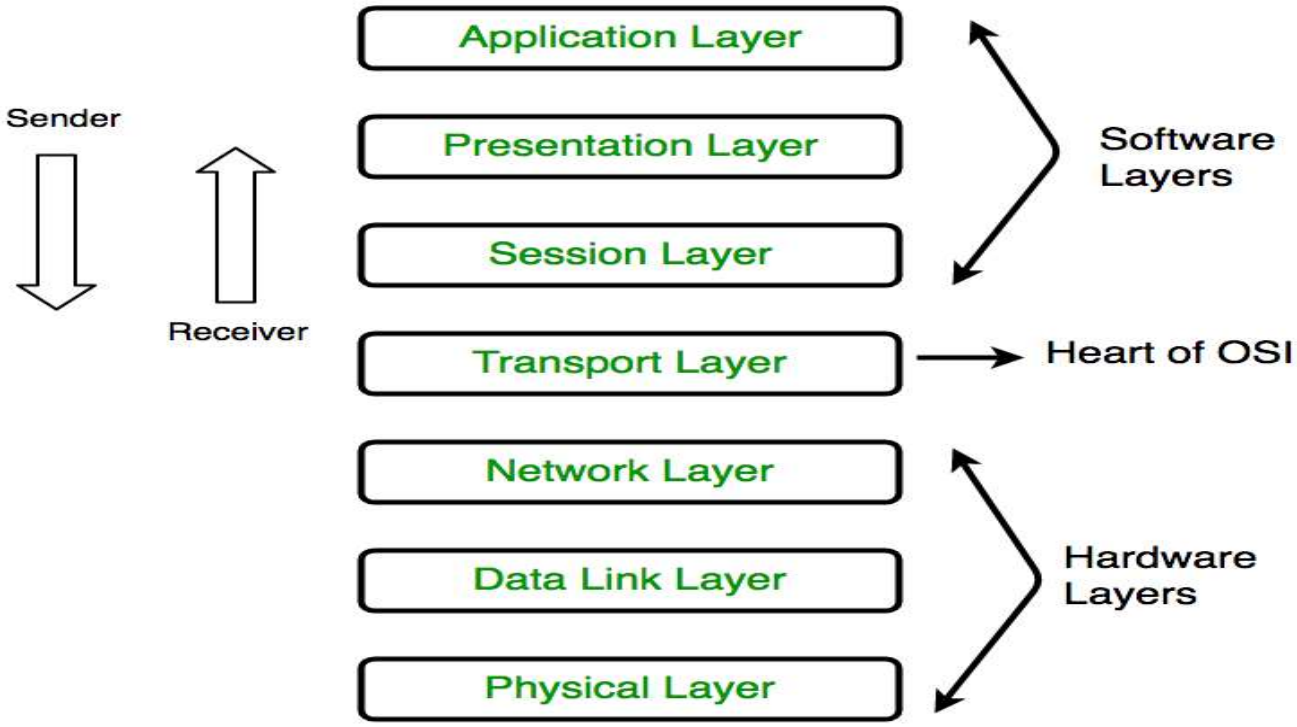
Disadvantages –

- **Capture effect:** Station who wins ones keeps on winning.
- Works only for 2 stations or hosts.

UNIT 2. The Layering Models and Data Communication

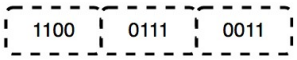
Layers of OSI Model

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) :

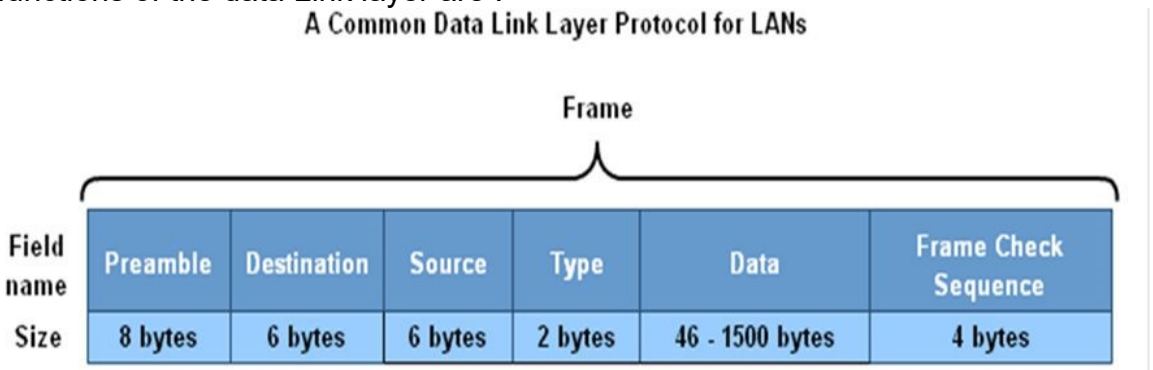
The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host 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 manage by CRC (Cyclic Redundancy Check).
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 :

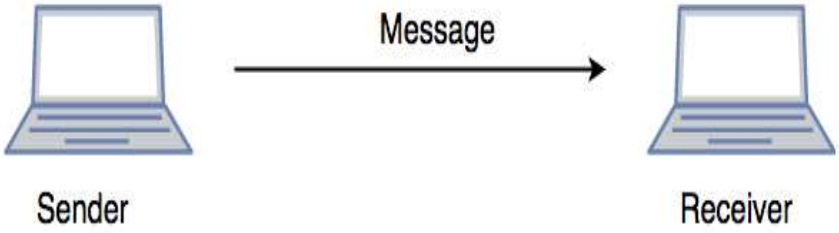
1. **Session establishment, maintenance and termination:** The layer allows the two processes to establish, use and terminate a connection.
2. **Synchronization:** This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point 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

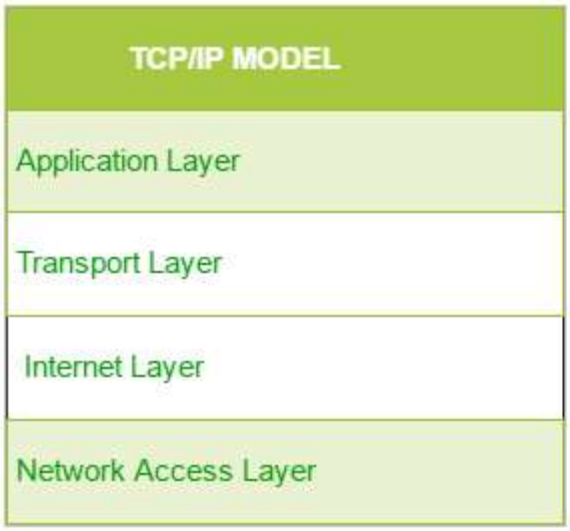
OSI model acts as a reference model and is not implemented in the Internet because of its late invention. Current model being used is the TCP/IP model

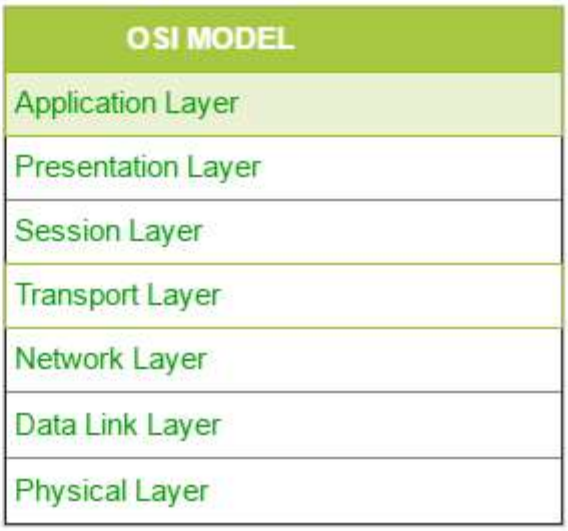
TCP/IP Model

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 :





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.

Bitrate

Bitrate, as the name implies, describes the rate at which bits are transferred from one location to another. In other words, it measures how much data is transmitted in a given amount of time. Bitrate is commonly measured in bits per second (bps), kilobits per second (Kbps), or megabits per second (Mbps). For example, a DSL connection may be able to download data at 768 kbps, while a Firewire 800 connection can transfer data up to 800 Mbps.

In networking and digital telecommunications, bit rate refers to the per-second measurement of data that passes through a communications network. In this context, bit rate is synonymous with data transfer rate (DTR).

For multimedia encoding, bit rate refers to the number of bits used per unit of playback time, such as video or audio after compression (encoding). Multimedia size and output quality often depend on the bit rate used during encoding.

Therefore, in both cases:

BR = D ÷ T

Where:

BR = Bit Rate

D = Amount of Data

T = Time (usually seconds)

Baud Rate

The **baud rate** is the **rate** at which information is transferred in a communication channel. **Baud rate** is commonly used when discussing electronics that use serial communication. In the serial port context, "9600 **baud**" means that the serial port is capable of transferring a maximum of 9600 bits per second.

Difference between Bit Rate and Baud Rate

Both Bit rate and Baud rate are generally used in data communication,

Bit rate is the transmission of number of bits per second. On the other hand, Baud rate is defined as the number of signal units per second. The formula which relates both bit rate and baud rate is given below:

Bit rate = Baud rate x the number of bit per baud.

Let's see the difference between Bit Rate and Baud Rate:

S.NO	BIT RATE	BAUD RATE
1.	Bit rate is defined as the transmission of number of bits per second.	Baud rate is defined as the number of signal units per second.
2.	Bit rate is also defined as per second travel number of bits.	Baud rate is also defined as per second number of changes in signal.
3.	Bit rate emphasized on computer efficiency.	While baud rate emphasized on data transmission.
4.	The formula of **Bit Rate** is: = baud rate x the number of bit per baud	The formula of **Baud Rate** is: = bit rate / the number of bit per baud
5.	Bit rate is not used to decide the requirement of bandwidth for transmission of signal.	While baud rate is used to decide the requirement of bandwidth for transmission of signal.

bandwidth

Network bandwidth is the capacity of a wired or wireless network communications link to transmit the maximum amount of data from one point to another over a computer network or internet connection in a given amount of time -- usually, one second. Synonymous with capacity, bandwidth describes the data transfer rate. Bandwidth is not a measure of network speed -- a common misconception.

Maximum Data Rate (channel capacity) for Noiseless and Noisy channels

Data rate governs the speed of data transmission. A very important consideration in data communication is how fast we can send data, in bits per second, over a channel. Data rate depends upon 3 factors:

- The bandwidth available

- Number of levels in digital signal
- The quality of the channel – level of noise

Two theoretical formulas were developed to calculate the data rate: one by Nyquist for a noiseless channel, another by Shannon for a noisy channel.

1. **Noiseless Channel : Nyquist Bit Rate –**
   For a noiseless channel, the Nyquist bit rate formula defines the theoretical maximum bit rate
   $\text{BitRate} = 2 * \text{Bandwidth} * \log_2(L)$
   In the above equation, bandwidth is the bandwidth of the channel, L is the number of signal levels used to represent data, and BitRate is the bit rate in bits per second. Bandwidth is a fixed quantity, so it cannot be changed. Hence, the data rate is directly proportional to the number of signal levels.
   Note –Increasing the levels of a signal may reduce the reliability of the system.
   Examples:
   Input1 : Consider a noiseless channel with a bandwidth of 3000 Hz transmitting a signal with two signal levels. What can be the maximum bit rate?
   Output1 : $\text{BitRate} = 2 * 3000 * \log_2(2) = 6000\text{bps}$
   Input2 : We need to send 265 kbps over a noiseless channel with a bandwidth of 20 kHz. How many signal levels do we need?
   Output2 : $265000 = 2 * 20000 * \log_2(L)$
   $\log_2(L) = 6.625$
   $L = 2^{6.625} = 98.7$ levels
2. **Noisy Channel : Shannon Capacity –**
   In reality, we cannot have a noiseless channel; the channel is always noisy. Shannon capacity is used, to determine the theoretical highest data rate for a noisy channel:
   $\text{Capacity} = \text{bandwidth} * \log_2(1 + \text{SNR})$
   In the above equation, bandwidth is the bandwidth of the channel, SNR is the signal-to-noise ratio, and capacity is the capacity of the channel in bits per second. Bandwidth is a fixed quantity, so it cannot be changed. Hence, the channel capacity is directly proportional to the power of the signal, as SNR = (Power of signal) / (power of noise).
   The signal-to-noise ratio (S/N) is usually expressed in decibels (dB) given by the formula:

   $10 * \log_{10}(S/N)$

   so for example a signal-to-noise ratio of 1000 is commonly expressed as:

   $10 * \log_{10}(1000) = 30$ dB.

   Examples:
   Input1 : A telephone line normally has a bandwidth of 3000 Hz (300 to 3300 Hz) assigned for data communication. The SNR is usually 3162. What will be the capacity for this channel?
   Output1 : $C = 3000 * \log_2(1 + \text{SNR}) = 3000 * 11.62 = 34860$ bps
   Input2 : The SNR is often given in decibels. Assume that SNR(dB) is 36 and the channel bandwidth is 2 MHz. Calculate the theoretical channel capacity.
   Output2 : $\text{SNR(dB)} = 10 * \log_{10}(\text{SNR})$
   $\text{SNR} = 10^{(\text{SNR(dB)}/10)}$
   $\text{SNR} = 10^{3.6} = 3981$

Hence, $C = 2 * 10^6 * \log_2(3982) = 24$ MHz

Classes of IP addresses

TCP/IP defines five classes of IP addresses: class A, B, C, D, and E. Each class has a range of valid IP addresses. The value of the first octet determines the class. IP addresses from the first three classes (A, B and C) can be used for host addresses. The other two classes are used for other purposes – class D for multicast and class E for experimental purposes.

The system of IP address classes was developed for the purpose of Internet IP addresses assignment. The classes created were based on the network size. For example, for the small number of networks with a very large number of hosts, the Class A was created. The Class C was created for numerous networks with small number of hosts.

Classes of IP addresses are:

Netwrok Classes	Address Rage of First Field	Use
class A	1-126	Scientifice techniques
class B	128-191	Special or government task
class C	192-223	General Purpose
class D	224	multicast Purpose
class E	225	Experimental Perpose

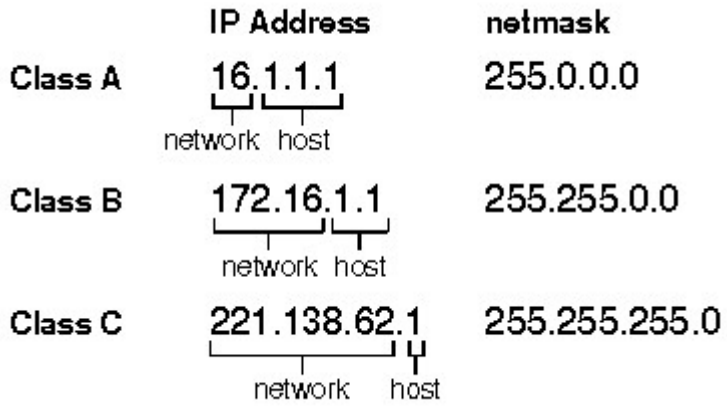
For the IP addresses from Class A, the first 8 bits (the first decimal number) represent the network part, while the remaining 24 bits represent the host part. For Class B, the first 16 bits (the first two numbers) represent the network part, while the remaining 16 bits represent the host part. For Class C, the first 24 bits represent the network part, while the remaining 8 bits represent the host part.

Subnet Mask

The subnet Mask is used to specify which part of the IP address is the network address and which part of the address is the host address.

By default, the following subnet mask are applied:

Class	Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0



Consider the following IP addresses:

10.50.120.7 – because this is a Class A address, the first number (10) represents the network part, while

the remainder of the address represents the host part (50.120.7). This means that, in order for devices to be on the same network, the first number of their IP addresses has to be the same for both devices. In this case, a device with the IP address of 10.47.8.4 is on the same network as the device with the IP address listed above. The device with the IP address 11.5.4.3 is not on the same network, because the first number of its IP address is different.
172.16.55.13 – because this is a Class B address, the first two numbers (172.16) represent the network part, while the remainder of the address represents the host part (55.13). A device with the IP address of 172.16.254.3 is on the same network, while a device with the IP address of 172.55.54.74 isn't.

Special IP address ranges that are used for special purposes are:

0.0.0.0/8 – addresses used to communicate with the local network
127.0.0.0/8 – loopback addresses
169.254.0.0/16 – link-local addresses (APIPA)

Types of IP addresses
The IP addresses are divided into three different types, based on their operational characteristics:

1. unicast IP addresses – an address of a single interface. The IP addresses of this type are used for one-to-one communication. Unicast IP addresses are used to direct packets to a specific host. Here is an example:

In the picture above you can see that the host wants to communicate with the server. It uses the (unicast) IP address of the server (192.168.0.150) to do so.

2. multicast IP addresses – used for one-to-many communication. Multicast messages are sent to IP multicast group addresses. Routers forward copies of the packet out to every interface that has hosts subscribed to that group address. Only the hosts that need to receive the message will process the packets. All other hosts on the LAN will discard them. Here is an example:

multicast ip address example

R1 has sent a multicast packet destined for 224.0.0.9. This is an RIPv2 packet, and only routers on the network should read it. R2 will receive the packet and read it. All other hosts on the LAN will discard the packet.

3. broadcast IP addresses – used to send data to all possible destinations in the broadcast domain (the one-to-everybody communication). The broadcast address for a network has all host bits on. For example, for the network 192.168.30.0 255.255.255.0 the broadcast address would be 192.168.30.255*. Also, the IP address of all 1's (255.255.255.255) can be used for local broadcast. Here's an example:

broadcast ip address example

R1 wants to communicate with all hosts on the network and has sent a broadcast packet to the broadcast IP address of 192.168.30.255. All hosts in the same broadcast domain will receive and process the packet.

Packet Switching

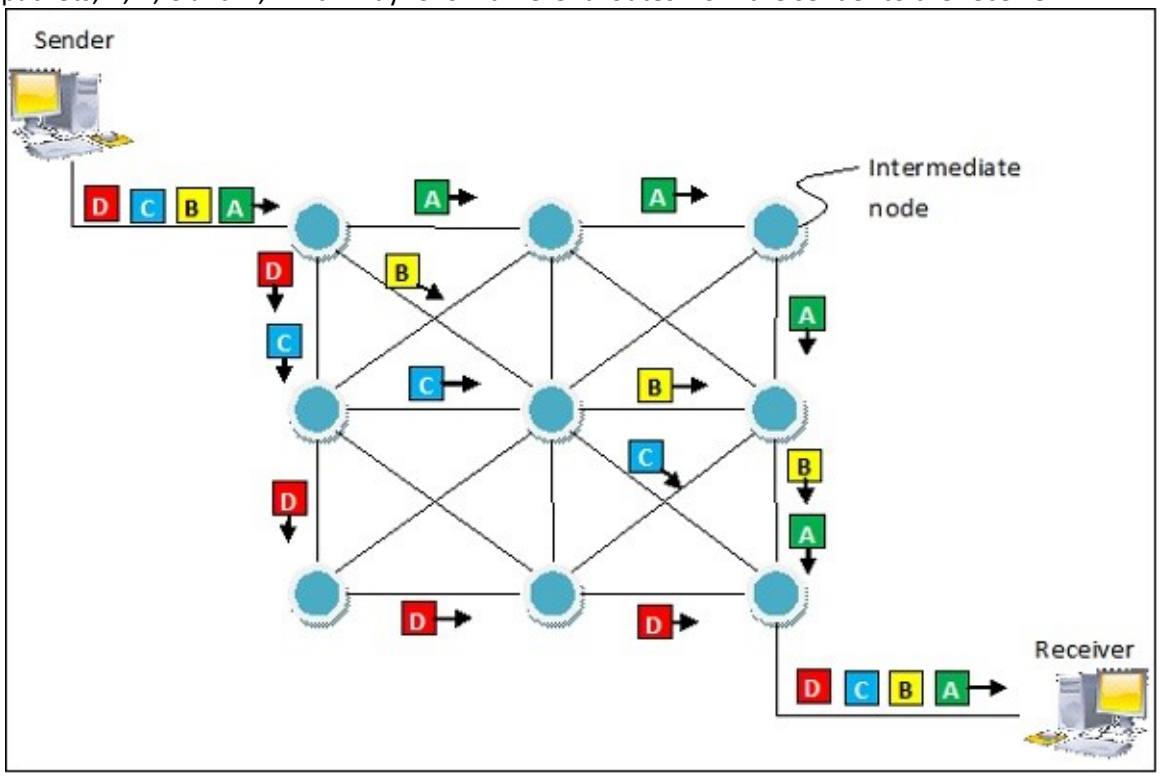
Packet switching is a connectionless network switching technique. Here, the message is divided and grouped into a number of units called packets that are individually routed from the source to the destination. There is no need to establish a dedicated circuit for communication.

Process

Each packet in a packet switching technique has two parts: a header and a payload. The header contains the addressing information of the packet and is used by the intermediate routers to direct it towards its destination. The payload carries the actual data.

A packet is transmitted as soon as it is available in a node, based upon its header information. The packets of a message are not routed via the same path. So, the packets in the message arrives in the destination out of order. It is the responsibility of the destination to reorder the packets in order to retrieve the original message.

The process is diagrammatically represented in the following figure. Here the message comprises of four packets, A, B, C and D, which may follow different routes from the sender to the receiver.



Advantages and Disadvantages of Packet Switching

Advantages

Delay in delivery of packets is less, since packets are sent as soon as they are available.

Switching devices don't require massive storage, since they don't have to store the entire messages before forwarding them to the next node.

Data delivery can continue even if some parts of the network faces link failure. Packets can be routed via

other paths.

It allows simultaneous usage of the same channel by multiple users.

It ensures better bandwidth usage as a number of packets from multiple sources can be transferred via the same link.

Disadvantages
They are unsuitable for applications that cannot afford delays in communication like high quality voice calls.

Packet switching high installation costs.

They require complex protocols for delivery.

Network problems may introduce errors in packets, delay in delivery of packets or loss of packets. If not properly handled, this may lead to loss of critical information.

Unit 3 CABLING AND CONNECTORS

OBJECTIVES

- Understand the use of wiring standards when selecting cable for different applications
- Understand the use of repeaters and media converters.

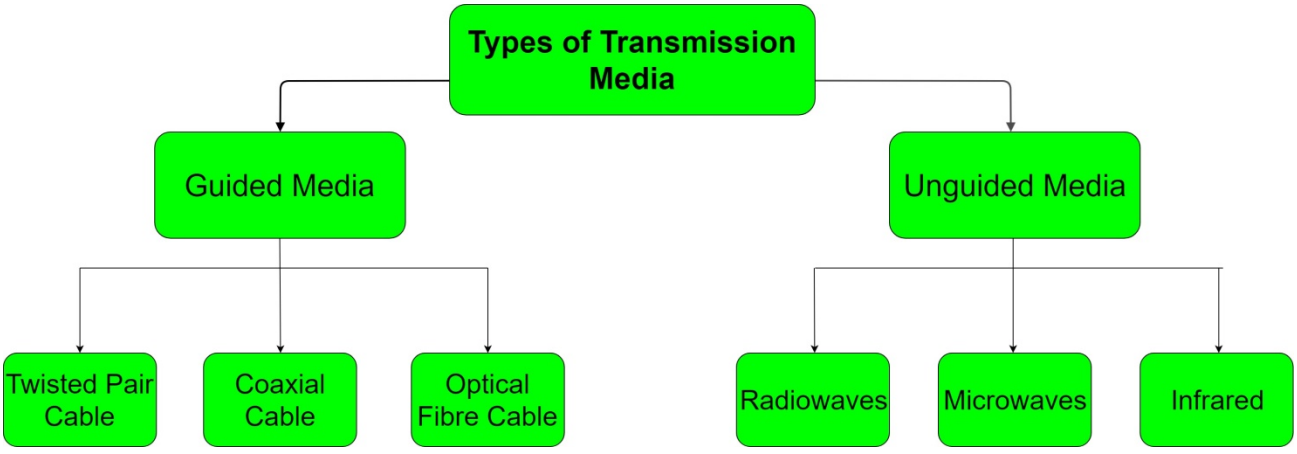
Selecting Network Cable

When selecting a suitable media for a network, the following should be considered:

1. Cost
2. Ease of installation
3. Plenum
4. Transmission speed
5. Duplex
6. Distance
7. Noise Immunity
8. Security

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
   - Comparitively faster
   - Comparitively 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. 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 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
- Light weight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials

Disadvantages:

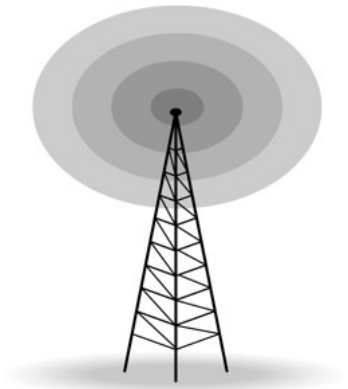
- Difficult to install and maintain
- High cost
- Fragile

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

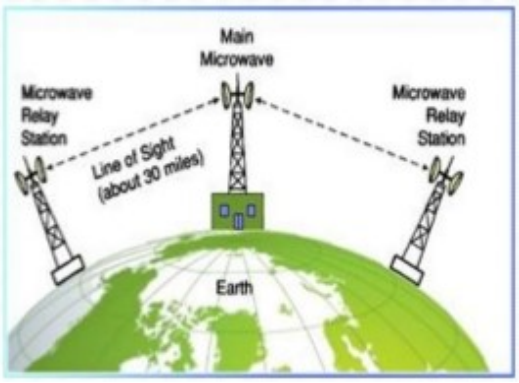
- Signal is broadcasted through air
- Less Secure
- Used for larger distances

There are 3 major types of Unguided Media:

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



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



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

Bounded or Guided Transmission Media

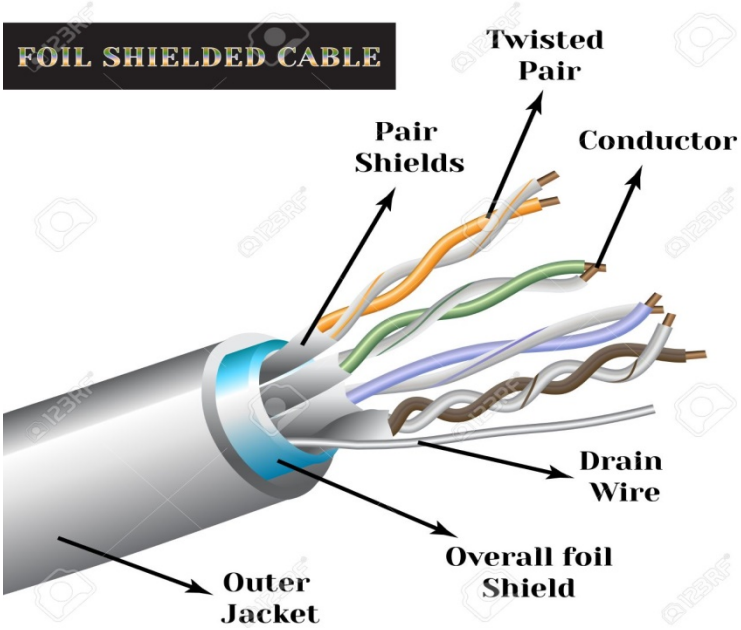
Guided media, which are those that provide a conduit from one device to another, include **Twisted-Pair Cable**, **Coaxial Cable**, and **Fibre-Optic Cable**.

A signal travelling along any of these media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. **Optical fibre** is a cable that accepts and transports signals in the form of light.

Twisted Pair Cable

This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily, and they support many different types of network. Some important points :

- Its frequency range is 0 to 3.5 kHz.
- Typical attenuation is 0.2 dB/Km @ 1kHz.
- Typical delay is 50 μs/km.
- Repeater spacing is 2km.



A twisted pair consists of two conductors(normally copper), each with its own plastic insulation, twisted together. One of these wires is used to carry signals to the receiver, and the other is used only as ground reference. The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference(noise) and crosstalk may affect both wires and create unwanted signals. If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources. This results in a difference at the receiver.

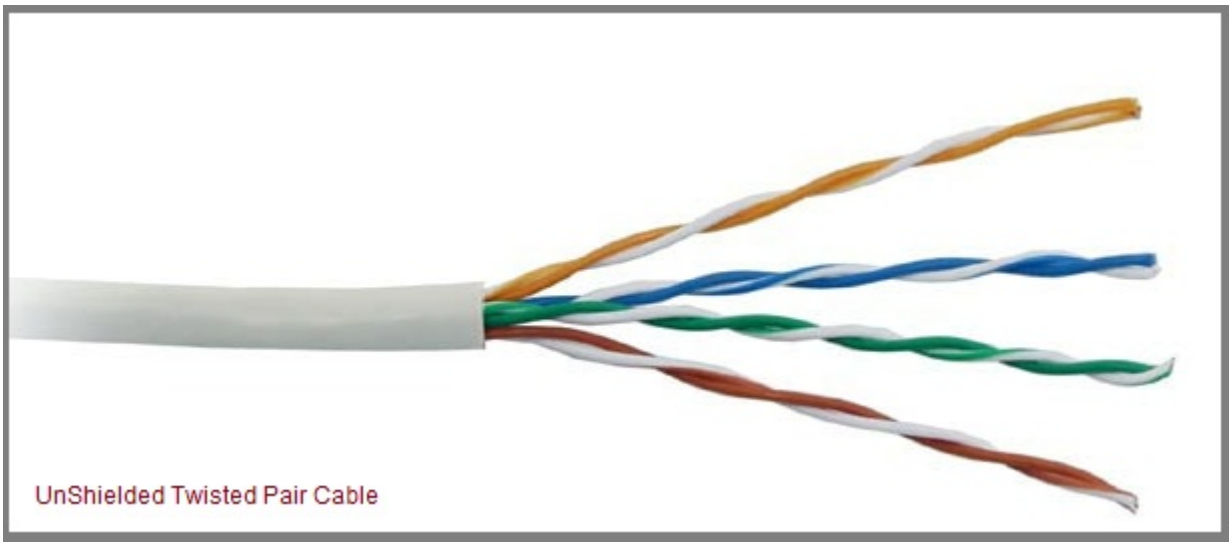
Twisted Pair is of two types:

- **Unshielded Twisted Pair (UTP)**
- **Shielded Twisted Pair (STP)**

Unshielded Twisted Pair Cable

It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own colour plastic insulator. Identification is the reason behind coloured plastic insulation.

UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use **RJ-11** connector and 4 pair cable use **RJ-45** connector.



Advantages of Unshielded Twisted Pair Cable

- Installation is easy
- Flexible
- Cheap
- It has high speed capacity,
- 100 meter limit
- Higher grades of UTP are used in LAN technologies like Ethernet.

It consists of two insulating copper wires (1mm thick). The wires are twist1ed together in a helical form to reduce electrical interference from similar pair.

Disadvantages of Unshielded Twisted Pair Cable

- Bandwidth is low when compared with Coaxial Cable
- Provides less protection from interference.

Shielded Twisted Pair Cable

This cable has a metal foil or braided-mesh covering which encases each pair of insulated conductors. Electromagnetic noise penetration is prevented by metal casing. Shielding also eliminates crosstalk (explained in KEY TERMS Chapter).

It has same attenuation as unshielded twisted pair. It is faster the unshielded and coaxial cable. It is more expensive than coaxial and unshielded twisted pair.

Advantages of Shielded Twisted Pair Cable

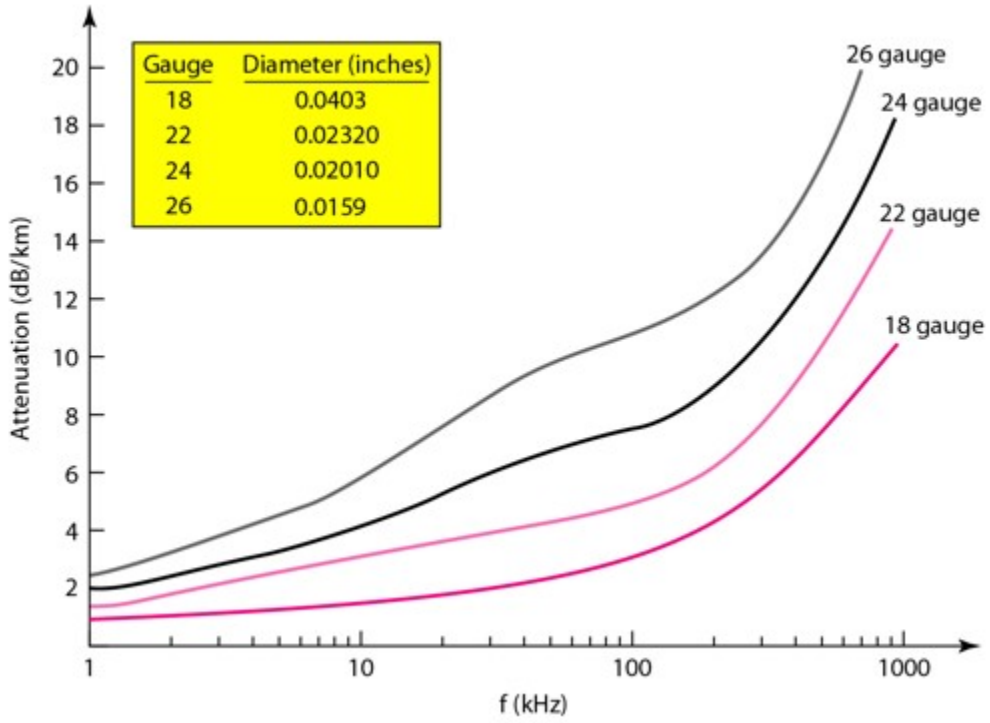
- Easy to install
- Performance is adequate
- Can be used for Analog or Digital transmission
- Increases the signalling rate
- Higher capacity than unshielded twisted pair
- Eliminates crosstalk

Disadvantages of Shielded Twisted Pair Cable

- Difficult to manufacture
- Heavy

Performance of Shielded Twisted Pair Cable

One way to measure the performance of twisted-pair cable is to compare attenuation versus frequency and distance. As shown in the below figure, a twisted-pair cable can pass a wide range of frequencies. However, with increasing frequency, the attenuation, measured in decibels per kilometre (dB/km), sharply increases with frequencies above 100kHz. Note that gauge is a measure of the thickness of the wire.



Applications of Shielded Twisted Pair Cable

- In telephone lines to provide voice and data channels. The DSL lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables.
- Local Area Network, such as 10Base-T and 100Base-T, also use twisted-pair cables.

Coaxial Cable

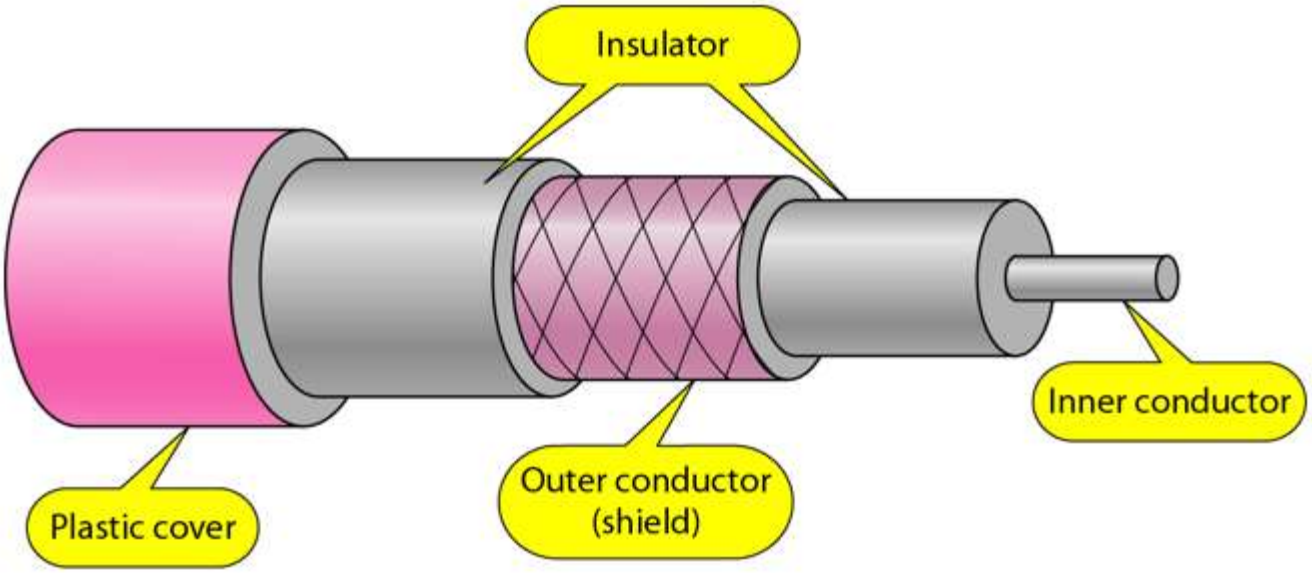
Coaxial is called by this name because it contains two conductors that are parallel to each other. Copper is used in this as centre conductor which can be a solid wire or a standard one. It is surrounded by PVC installation, a sheath which is encased in an outer conductor of metal foil, barid or both.

Outer metallic wrapping is used as a shield against noise and as the second conductor which completes the circuit. The outer conductor is also encased in an insulating sheath. The outermost part is the plastic cover which protects the whole cable.

Here the most common coaxial standards.

- 50-Ohm RG-7 or RG-11 : used with thick Ethernet.
- 50-Ohm RG-58 : used with thin Ethernet

- 75-Ohm RG-59 : used with cable television
- 93-Ohm RG-62 : used with ARCNET.



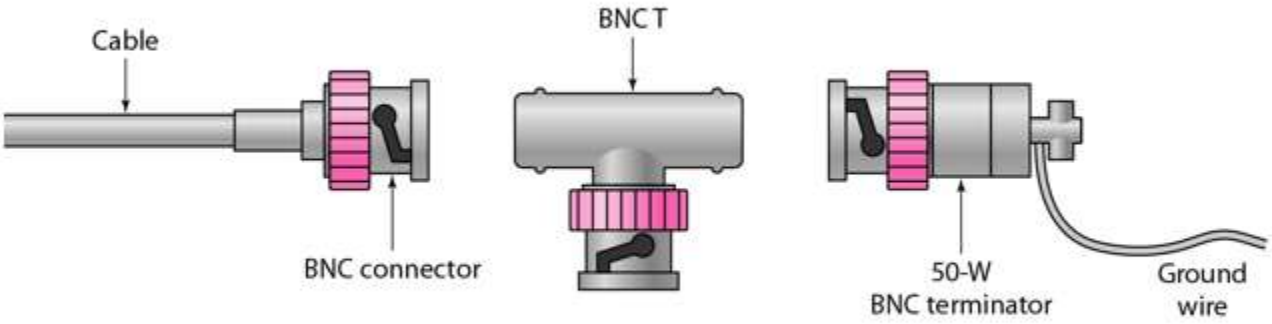
Coaxial Cable Standards

Coaxial cables are categorized by their Radio Government(RG) ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and the type of the inner insulator, the construction of the shield, and the size and type of the outer casing. Each cable defined by an RG rating is adapted for a specialized function, as shown in the table below:

Category	*Impedance*	*Use*
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet

Coaxial Cable Connectors

To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayonet Neill-Concelman (BNC) connector. The below figure shows 3 popular types of these connectors: the BNC Connector, the BNC T connector and the BNC terminator.



The BNC connector is used to connect the end of the cable to the device, such as a TV set. The BNC T connector is used in Ethernet networks to branch out to a connection to a computer or other device. The BNC terminator is used at the end of the cable to prevent the reflection of the signal.

There are two types of Coaxial cables:

1. BaseBand

This is a 50 ohm (Ω) coaxial cable which is used for digital transmission. It is mostly used for LAN's. Baseband transmits a single signal at a time with very high speed. The major drawback is that it needs amplification after every 1000 feet.

2. BroadBand

This uses analog transmission on standard cable television cabling. It transmits several simultaneous signal using different frequencies. It covers large area when compared with Baseband Coaxial Cable.

Advantages of Coaxial Cable

- Bandwidth is high
- Used in long distance telephone lines.
- Transmits digital signals at a very high rate of 10Mbps.
- Much higher noise immunity
- Data transmission without distortion.

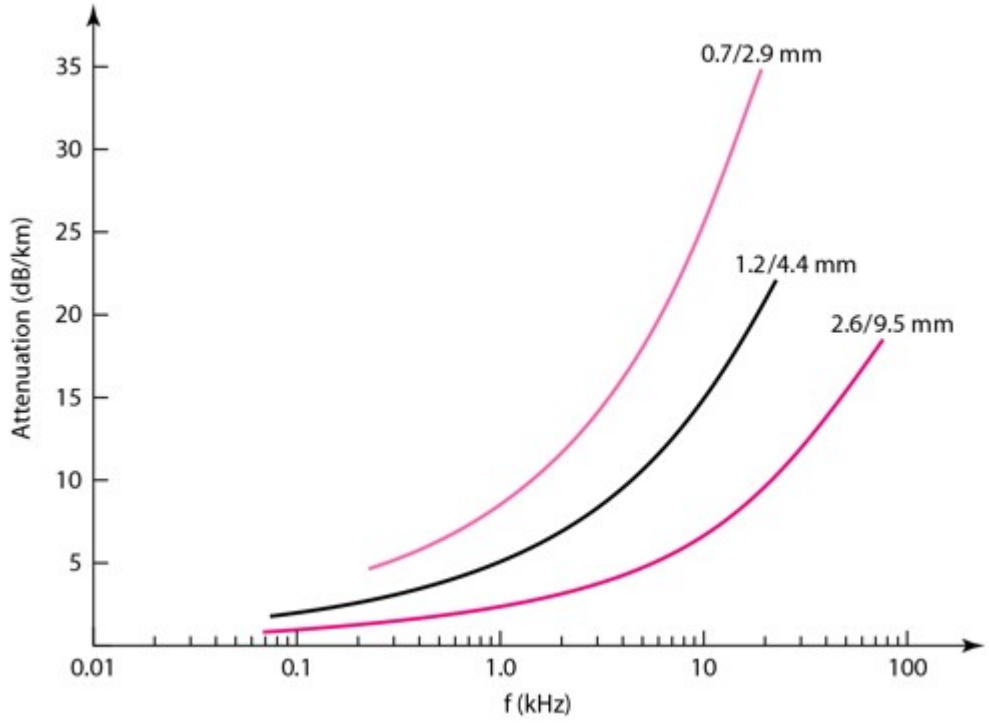
- The can span to longer distance at higher speeds as they have better shielding when compared to twisted pair cable

Disadvantages of Coaxial Cable

- Single cable failure can fail the entire network.
- Difficult to install and expensive when compared with twisted pair.
- If the shield is imperfect, it can lead to grounded loop.

Performance of Coaxial Cable

We can measure the performance of a coaxial cable in same way as that of Twisted Pair Cables. From the below figure, it can be seen that the attenuation is much higher in coaxial cable than in twisted-pair cable. In other words, although coaxial cable has a much higher bandwidth, the signal weakens rapidly and requires the frequent use of repeaters.



Applications of Coaxial Cable

- Coaxial cable was widely used in analog telephone networks, where a single coaxial network could carry 10,000 voice signals.

- Cable TV networks also use coaxial cables. In the traditional cable TV network, the entire network used coaxial cable. Cable TV uses RG-59 coaxial cable.
- In traditional Ethernet LANs. Because of it high bandwidth, and consequence high data rate, coaxial cable was chosen for digital transmission in early Ethernet LANs. The 10Base-2, or Thin Ethernet, uses RG-58 coaxial cable with BNC connectors to transmit data at 10Mbps with a range of 185 m.

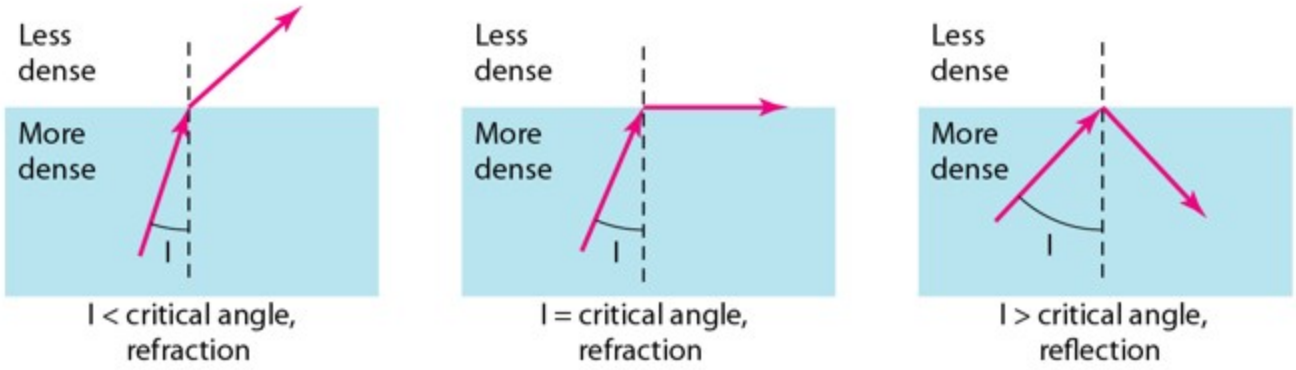
Fiber Optic Cable

A fibre-optic cable is made of glass or plastic and transmits signals in the form of light.

For better understanding we first need to explore several aspects of the **nature of light**.

Light travels in a straight line as long as it is mobbing through a single uniform substance. If ray of light travelling through one substance suddenly enters another substance (of a different density), the ray changes direction.

The below figure shows how a ray of light changes direction when going from a more dense to a less dense substance.



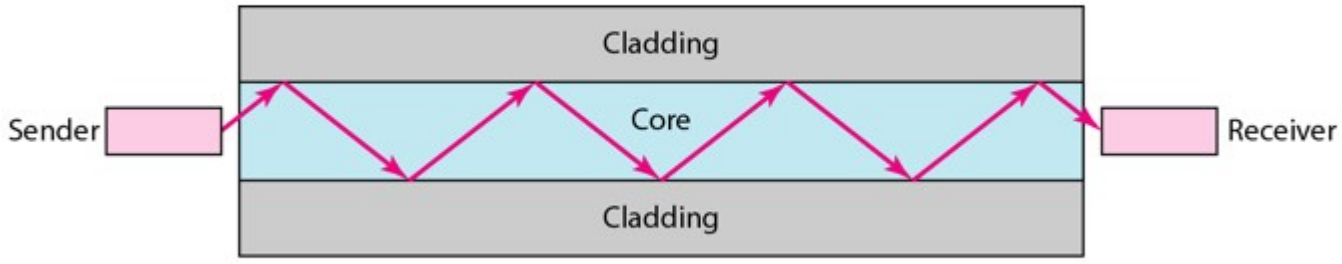
Bending of a light ray

As the figure shows:

- If the **angle of incidence I**(the angle the ray makes with the line perpendicular to the interface between the two substances) is **less** than the **critical angle**, the ray **refracts** and moves closer to the surface.

- If the angle of incidence is **greater** than the critical angle, the ray **reflects**(makes a turn) and travels again in the denser substance.
- If the angle of incidence is **equal** to the critical angle, the ray refracts and **moves parallel** to the surface as shown.

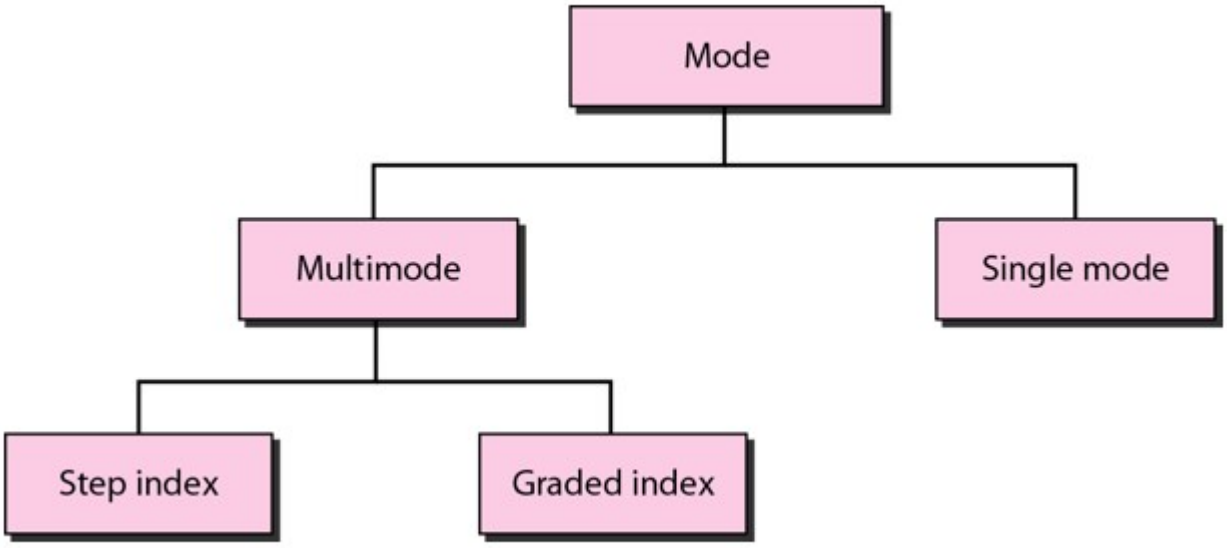
Note: *The critical angle is a property of the substance, and its value differs from one substance to another.*
Optical fibres use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.



Internal view of an Optical fibre

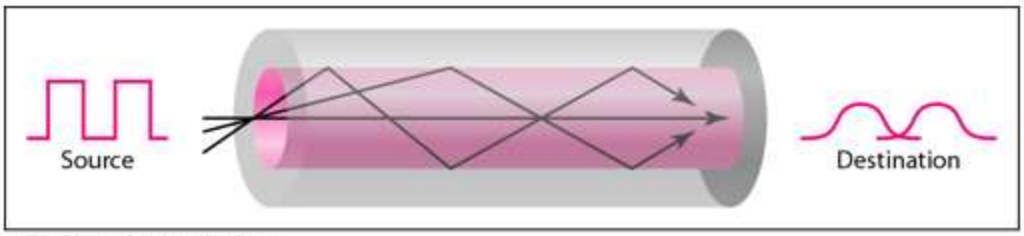
Propagation Modes of Fiber Optic Cable

Current technology supports two modes(**Multimode** and **Single mode**) for propagating light along optical channels, each requiring fibre with different physical characteristics. Multimode can be implemented in two forms: **Step-index** and **Graded-index**.

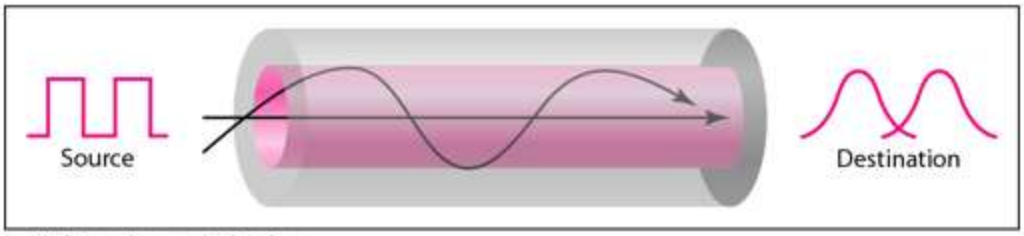


Multimode Propagation Mode

Multimode is so named because multiple beams from a light source move through the core in different paths. How these beams move within the cable depends on the structure of the core as shown in the below figure.



a. Multimode, step index



b. Multimode, graded index

c. Single mode

- In **multimode step-index fibre**, the density of the core remains constant from the centre to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding.
  The term step-index refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fibre.
- In **multimode graded-index fibre**, this distortion gets decreases through the cable. The word index here refers to the index of refraction. This index of refraction is related to the density. A graded-index fibre, therefore, is one with varying densities. Density is highest at the centre of the core and decreases gradually to its lowest at the edge.

Single Mode

Single mode uses step-index fibre and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal. The single-mode fibre itself is manufactured with a much smaller diameter than that of multimode fibre, and with substantially lower density.

The decrease in density results in a critical angle that is close enough to 90 degree to make the propagation of beams almost horizontal.

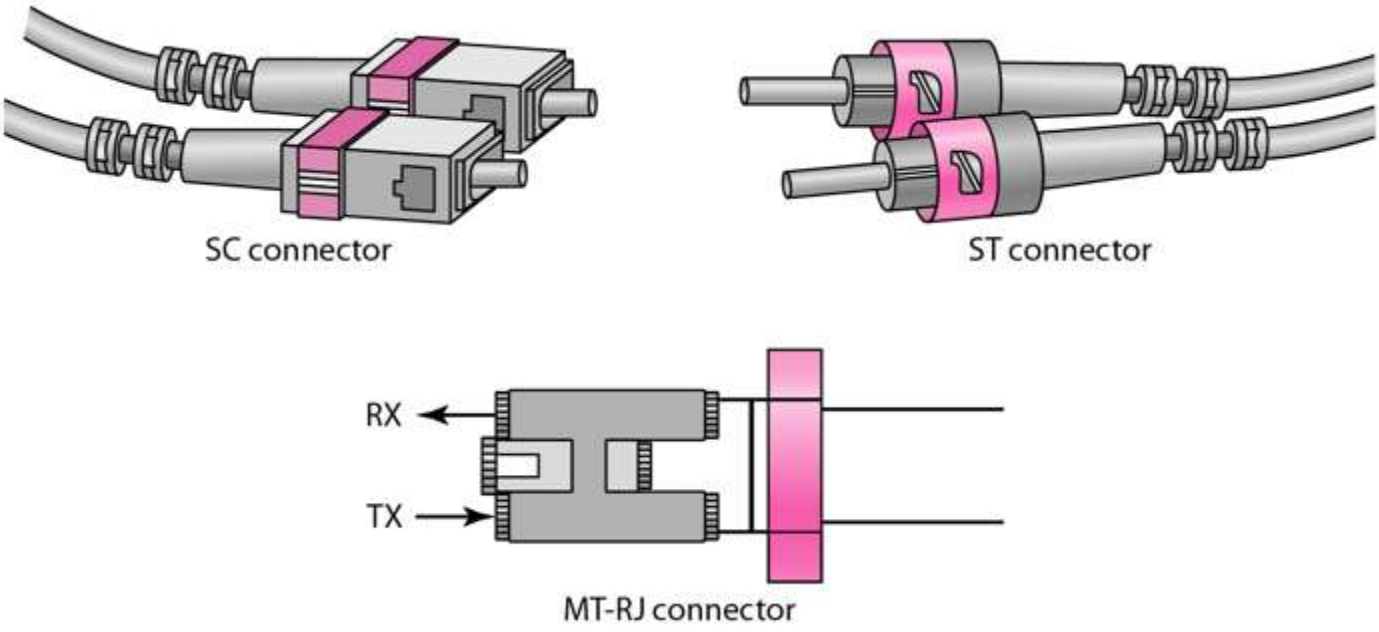
Fibre Sizes for Fiber Optic Cable

Optical fibres are defined by the ratio of the diameter or their core to the diameter of their cladding, both expressed in micrometers. The common sizes are shown in the figure below:

Type	*Core (μm)*	*Cladding (μm)*	*Mode*
50/125	50.0	125	Multimode, graded index
62.5/125	62.5	125	Multimode, graded index
100/125	100.0	125	Multimode, graded index
7/125	7.0	125	Single mode

Fibre Optic Cable Connectors

There are three types of connectors for fibre-optic cables, as shown in the figure below.



The **Subscriber Channel(SC)** connector is used for cable TV. It uses push/pull locking system. The **Straight-Tip(ST)** connector is used for connecting cable to the networking devices. MT-RJ is a connector that is the same size as RJ45.

Advantages of Fibre Optic Cable

Fibre optic has several advantages over metallic cable:

- Higher bandwidth
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials
- Light weight
- Greater immunity to tapping

Disadvantages of Fibre Optic Cable

There are some disadvantages in the use of optical fibre:

- Installation and maintenance
- Unidirectional light propagation
- High Cost

Performance of Fibre Optic Cable

Attenuation is flatter than in the case of twisted-pair cable and coaxial cable. The performance is such that we need fewer(actually one tenth as many) repeaters when we use the fibre-optic cable.

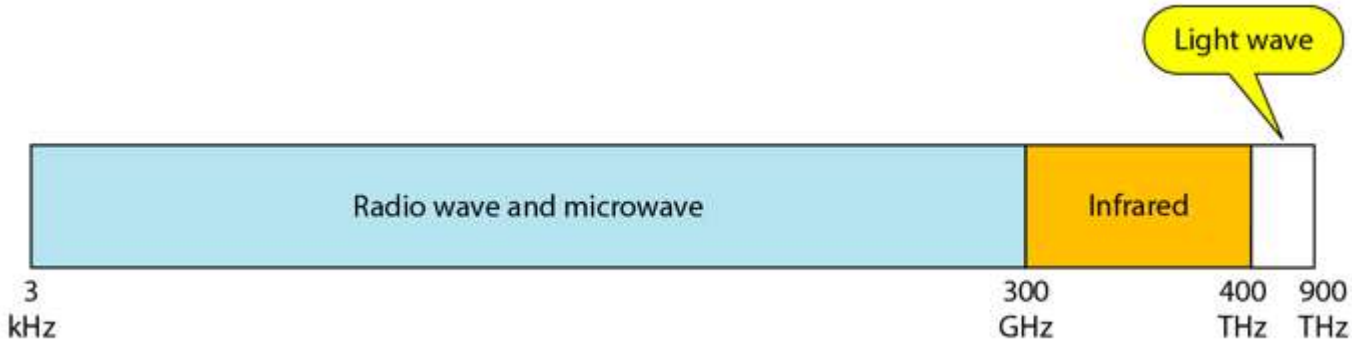
Applications of Fibre Optic Cable

- Often found in backbone networks because its wide bandwidth is cost-effective.
- Some cable TV companies use a combination of optical fibre and coaxial cable thus creating a hybrid network.
- Local-area Networks such as 100Base-FX network and 1000Base-X also use fibre-optic cable.

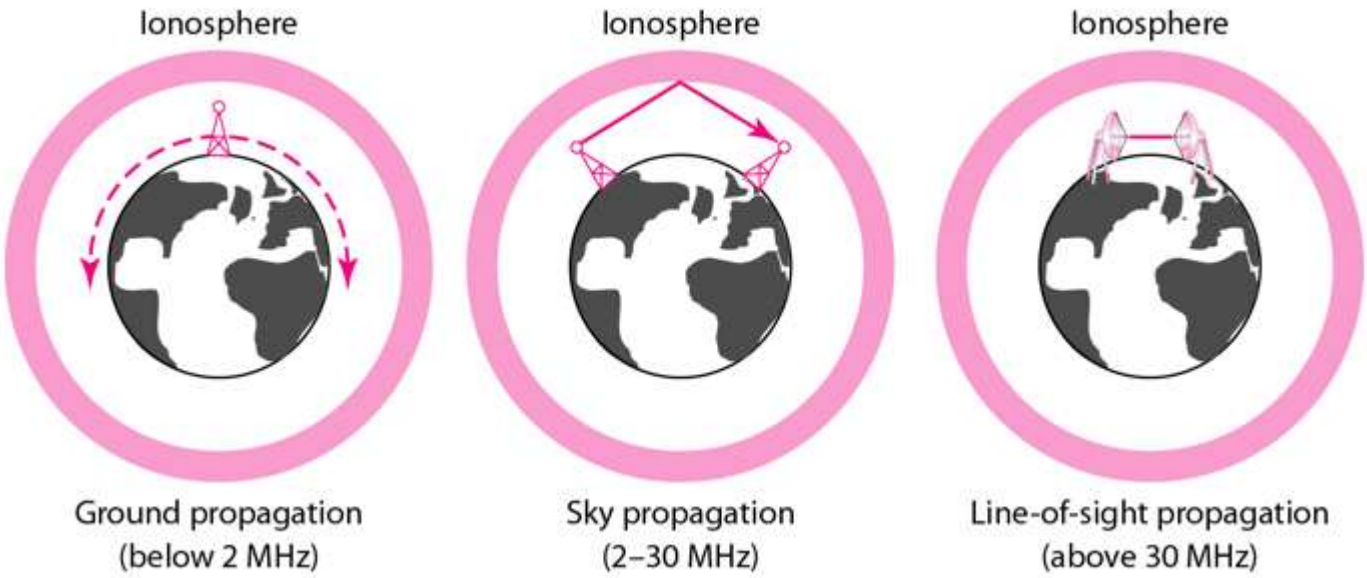
UnBounded or UnGuided Transmission Media

Unguided medium transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

The below figure shows the part of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, used for wireless communication.



Unguided signals can travel from the source to the destination in several ways: **Gound propagation**, **Sky propagation** and **Line-of-sight propagation** as shown in below figure.



Propagation Modes

- **Ground Propagation:** In this, radio waves travel through the lowest portion of the atmosphere, hugging the Earth. These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet.
- **Sky Propagation:** In this, higher-frequency radio waves radiate upward into the ionosphere where they are reflected back to Earth. This type of transmission allows for greater distances with lower output power.
- **Line-of-sight Propagation:** in this type, very high-frequency signals are transmitted in straight lines directly from antenna to antenna.

We can divide wireless transmission into three broad groups:

1. Radio waves
2. Micro waves
3. Infrared waves

Radio Waves

Electromagnetic waves ranging in frequencies between 3 KHz and 1 GHz are normally called radio waves.

Radio waves are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. A sending antenna send waves that can be received by any receiving antenna. The omnidirectional property has disadvantage, too. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signal suing the same frequency or band.

Radio waves, particularly with those of low and medium frequencies, can penetrate walls. This characteristic can be both an advantage and a disadvantage. It is an advantage because, an AM radio can receive signals inside a building. It is a disadvantage because we cannot isolate a communication to just inside or outside a building.

Omnidirectional Antenna for Radio Waves

Radio waves use omnidirectional antennas that send out signals in all directions.

Applications of Radio Waves

- The omnidirectional characteristics of radio waves make them useful for multicasting in which there is one sender but many receivers.
- AM and FM radio, television, maritime radio, cordless phones, and paging are examples of multicasting.

Micro Waves

Electromagnetic waves having frequencies between 1 and 300 GHz are called micro waves. Micro waves are unidirectional. When an antenna transmits microwaves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas.

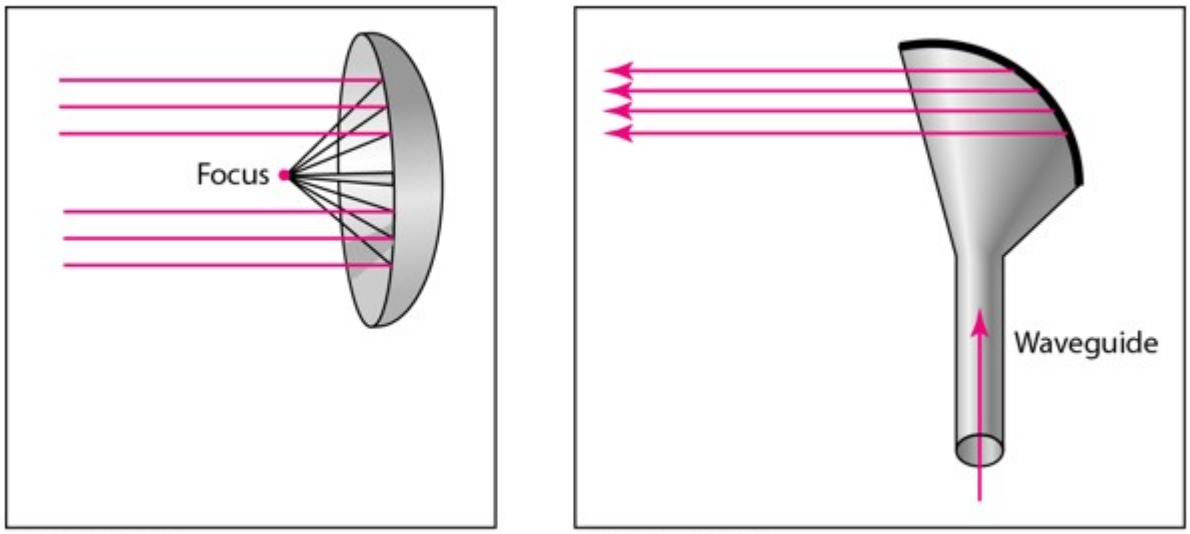
The following describes some characteristics of microwaves propagation:

- Microwave propagation is line-of-sight. Since the towers with the mounted antennas need to be in direct sight of each other, towers that are far apart need to be very tall.

- Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside the buildings.
- The microwave band is relatively wide, almost 299 GHz. Therefore, wider sub-bands can be assigned and a high date rate is possible.
- Use of certain portions of the band requires permission from authorities.

Unidirectional Antenna for Micro Waves

Microwaves need unidirectional antennas that send out signals in one direction. Two types of antennas are used for microwave communications: **Parabolic Dish** and **Horn**.



a. Dish antenna

b. Horn antenna

A parabolic antenna works as a funnel, catching a wide range of waves and directing them to a common point. In this way, more of the signal is recovered than would be possible with a single-point receiver.

A horn antenna looks like a gigantic scoop. Outgoing transmissions are broadcast up a stem and deflected outward in a series of narrow parallel beams by the curved head. Received transmissions are collected by the scooped shape of the horn, in a manner similar to the parabolic dish, and are deflected down into the stem.

Applications of Micro Waves

Microwaves, due to their unidirectional properties, are very useful when unicast(one-to-one) communication is needed between the sender and the receiver. They are used in cellular phones, satellite networks and wireless LANs.

There are 2 types of Microwave Transmission :

1. Terrestrial Microwave
2. Satellite Microwave

Advantages of Microwave Transmission

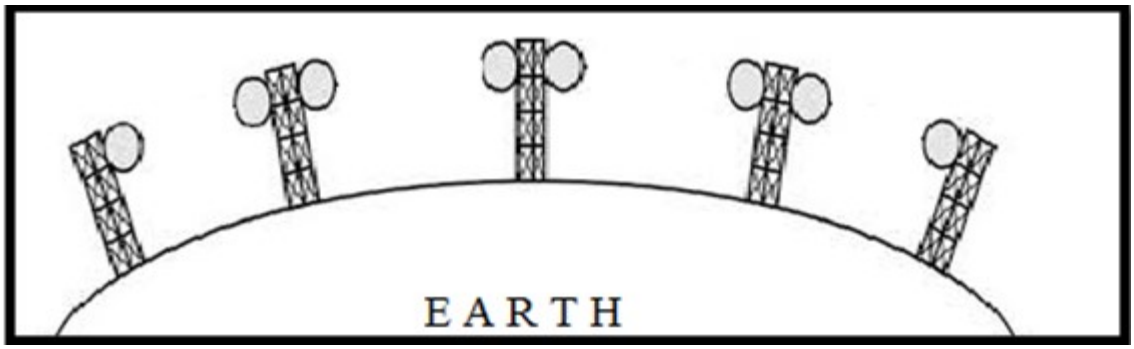
- Used for long distance telephone communication
- Carries 1000's of voice channels at the same time

Disadvantages of Microwave Transmission

- It is very costly

Terrestrial Microwave

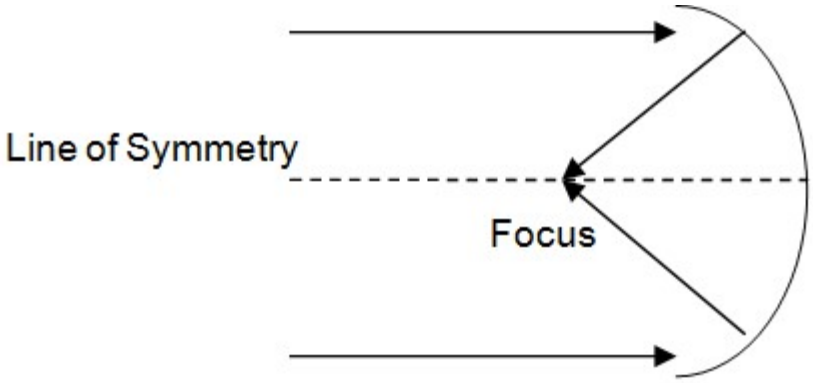
For increasing the distance served by terrestrial microwave, repeaters can be installed with each antenna .The signal received by an antenna can be converted into transmittable form and relayed to next antenna as shown in below figure. It is an example of telephone systems all over the world



There are **two types of antennas** used for terrestrial microwave communication :

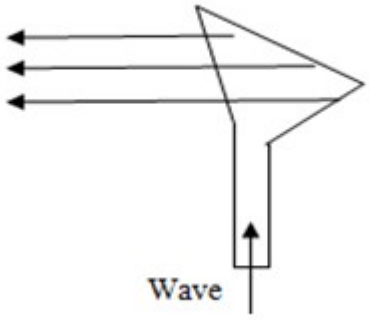
1. Parabolic Dish Antenna

In this every line parallel to the line of symmetry reflects off the curve at angles in a way that they intersect at a common point called focus. This antenna is based on geometry of parabola.



2. Horn Antenna

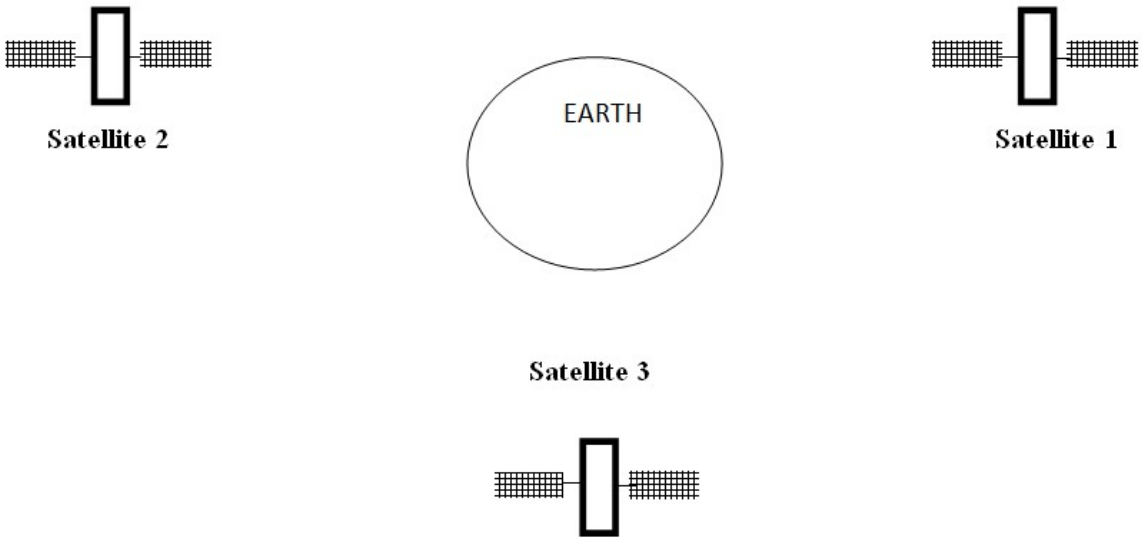
It is a like gigantic scoop. The outgoing transmissions are broadcast up a stem and deflected outward in a series of narrow parallel beams by curved head.



Satellite Microwave

This is a microwave relay station which is placed in outer space. The satellites are launched either by rockets or space shuttles carry them.

These are positioned 36000 Km above the equator with an orbit speed that exactly matches the rotation speed of the earth. As the satellite is positioned in a geo-synchronous orbit, it is stationery relative to earth and always stays over the same point on the ground. This is usually done to allow ground stations to aim antenna at a fixed point in the sky.



Features of Satellite Microwave

- Bandwidth capacity depends on the frequency used.
- Satellite microwave deployment for orbiting satellite is difficult.

Advantages of Satellite Microwave

- Transmitting station can receive back its own transmission and check whether the satellite has transmitted information correctly.
- A single microwave relay station which is visible from any point.

Disadvantages of Satellite Microwave

- Satellite manufacturing cost is very high
- Cost of launching satellite is very expensive
- Transmission highly depends on whether conditions, it can go down in bad weather

Infrared Waves

Infrared waves, with frequencies from 300 GHz to 400 THz, can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This

advantageous characteristic prevents interference between one system and another, a short-range communication system in on room cannot be affected by another system in the next room.

When we use infrared remote control, we do not interfere with the use of the remote by our neighbours. However, this same characteristic makes infrared signals useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

Applications of Infrared Waves

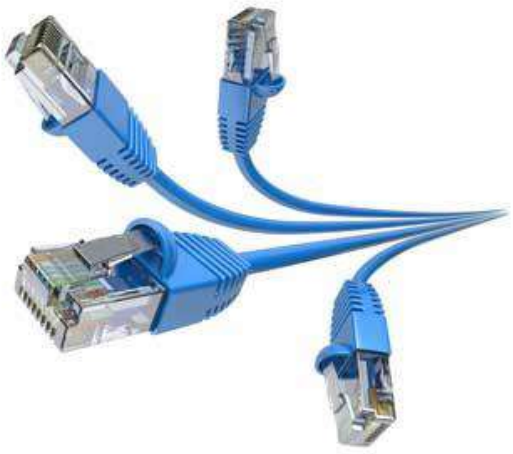
- The infrared band, almost 400 THz, has an excellent potential for data transmission. Such a wide bandwidth can be used to transmit digital data with a very high data rate.
- The Infrared Data Association(IrDA), an association for sponsoring the use of infrared waves, has established standards for using these signals for communication between devices such as keyboards, mouse, PCs and printers.
- Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

Basic Network Hardware

The basic computer hardware components that are needed to set up a network are as follows −

Network Cables

Network cables are the transmission media to transfer data from one device to another. A commonly used network cable is category 5 cable with RJ – 45 connector, as shown in the image below:



Routers

A router is a connecting device that transfers data packets between different computer networks. Typically, they are used to connect a PC or an organization's LAN to a broadband internet connection. They contain RJ-45 ports so that computers and other devices can connect with them using network cables.

Repeaters, Hubs, and Switches

Repeaters, hubs and switches connect network devices together so that they can function as a single segment.

A repeater receives a signal and regenerates it before re-transmitting so that it can travel longer distances.

A hub is a multiport repeater having several input/output ports, so that input at any port is available at every other port.

A switch receives data from a port, uses packet switching to resolve the destination device and then forwards the data to the particular destination, rather than broadcasting it as a hub.

REPEATER HUB SWITCH

Bridges

A bridge connects two separate Ethernet network segments. It forwards packets from the source network to the destined network.

Gateways

A gateway connects entirely different networks that work upon different protocols. It is the entry and the exit point of a network and controls access to other networks.

Network Interface Cards

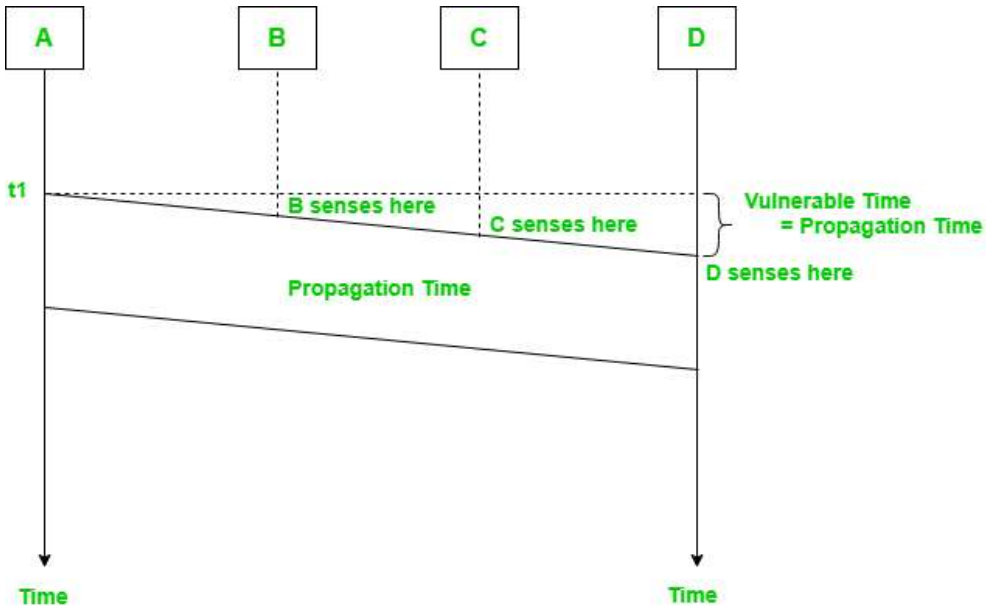
NIC is a component of the computer to connect it to a network. Network cards are of two types: Internal network cards and external network cards.

Carrier Sense Multiple Access (CSMA)

This method was developed to decrease the chances of collisions when two or more stations start sending their signals over the datalink layer. Carrier Sense multiple access requires that each station **first check the state of the medium** before sending.

Vulnerable Time –

```
Vulnerable time = Propagation time (Tp)
```



The persistence methods can be applied to help the station take action when the channel is busy/idle.

1. Carrier Sense Multiple Access with Collision Detection (CSMA/CD) –

In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If successful, the station is finished, if not, the frame is sent again.

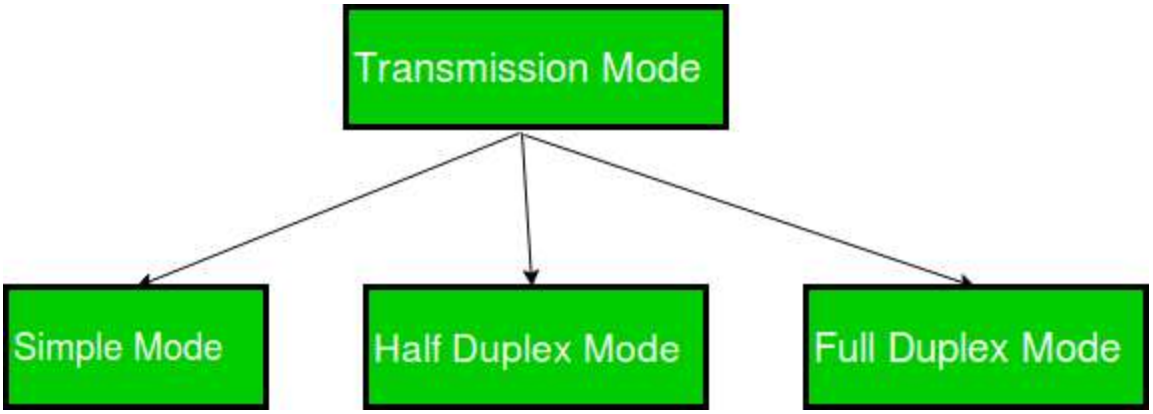
2. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) –

The basic idea behind CSMA/CA is that the station should be able to receive while transmitting to detect a collision from different stations. In wired networks, if a collision has occurred then the energy of received signal almost doubles and the station can sense the possibility of collision. In case of wireless networks, most of the energy is used for transmission and the energy of received signal increases by only 5-10% if a collision occurs. It can't be used by the station to sense collision. Therefore **CSMA/CA has been specially designed for wireless networks**.

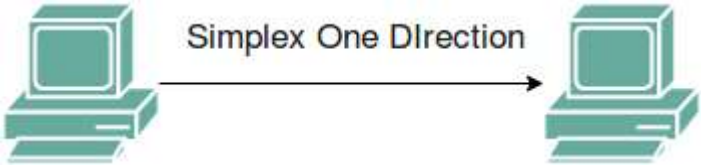
Transmission Modes in Computer Networks (Simplex, Half-Duplex and Full-Duplex)

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:-

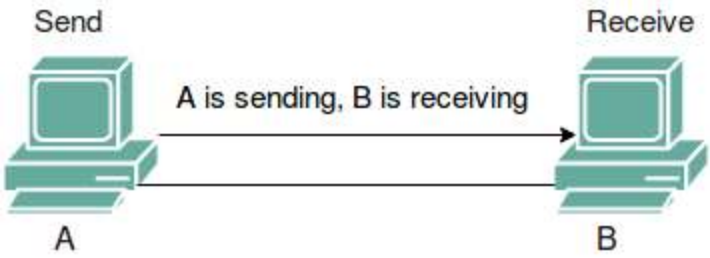
- **Simplex Mode**
- **Half-Duplex Mode**
- **Full-Duplex Mode**

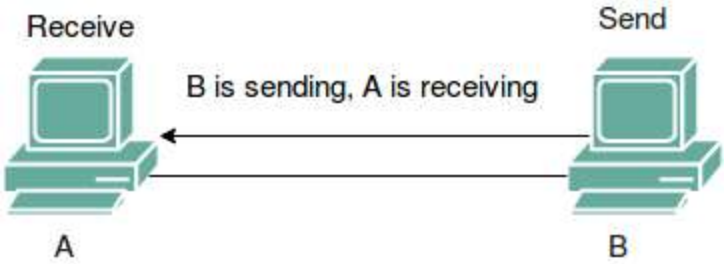


Simplex Mode
In Simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit, the other can only receive. The simplex mode can use the entire capacity of the channel to send data in one direction.
Example: Keyboard and traditional monitors. The keyboard can only introduce input, the monitor can only give the output.



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.



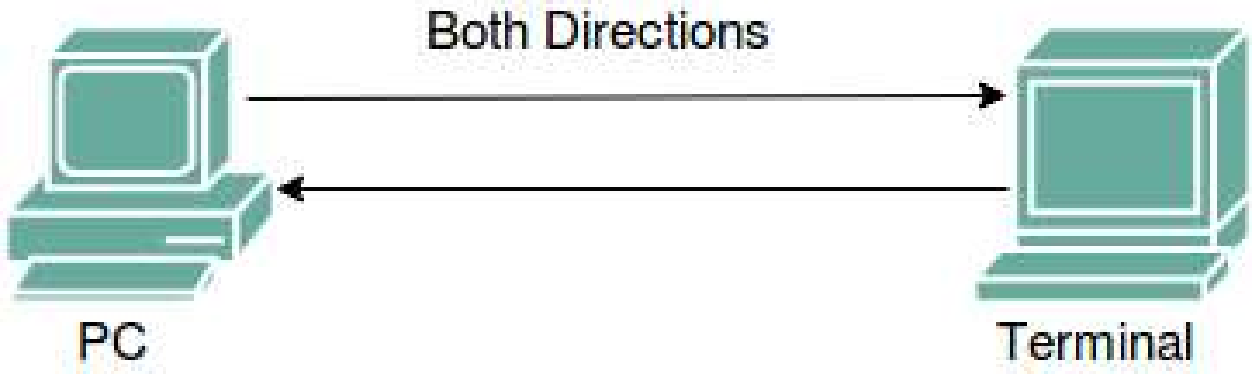


Full-Duplex Mode

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.



Application Layer:-

The application layer is present at the top of the OSI model. It is the layer through which users interact. It provides services to the user.

Application Layer protocol:-

1. TELNET:

Telnet stands for the **TEL**ecomunications **NET**work. It helps in terminal emulation. It allows Telnet client to access the resources of the Telnet server. It is used for managing the files on the internet. It is used for initial set up of devices like switches. The telnet command is a command that uses the Telnet protocol to communicate with a remote device or system. Port number of telnet is 23.

Command

```
telnet [\\RemoteServer]

\\RemoteServer   : Specifies the name of the server to which you want to connect
```

2. FTP:

FTP stands for file transfer protocol. It is the protocol that actually lets us transfer files.It can facilitate this between any two machines using it. But FTP is not just a protocol but it is also a program.FTP promotes sharing of files via remote computers with reliable and efficient data transfer. Port number for FTP is 20 for data and 21 for control.

Command

```
ftpmachinename
```

3. TFTP:

The Trivial File Transfer Protocol (TFTP) is the stripped-down, stock version of FTP, but it's the protocol of choice if you know exactly what you want and where to find it. It's a technology for transferring files between network devices and is a simplified version of FTP

Command

```
tftp [ options... ] [host [port]] [-c command]
```

4. NFS:

It stands for network file system.It allows remote hosts to mount file systems over a network and interact with those file systems as though they are mounted locally. This enables system administrators to consolidate resources onto centralized servers on the

network.

Command

```
servicenfs start
```

5. SMTP:

It stands for Simple Mail Transfer Protocol. It is a part of the TCP/IP protocol. Using a process called “store and forward,” SMTP moves your email on and across networks. It works closely with something called the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox. Port number for SMTP is 25.

Command

```
MAIL FROM:<mail@abc.com?
```

6. LPD:

It stands for Line Printer Daemon.It is designed for printer sharing.It is the part that receives and processes the request. A “daemon” is a server or agent.

Command

```
lpd [ -d ] [ -l ] [ -D DebugOutputFile]
```

7. X window:

It defines a protocol for the writing of graphical user interface–based client/server applications. The idea is to allow a program, called a client, to run on one computer. It is primarily used in networks of interconnected mainframes.

Command

```
Run xdm in runlevel 5
```

8. SNMP:

It stands for Simple Network Management Protocol. It gathers data by polling the devices on the network from a management station at fixed or random intervals, requiring them to disclose certain information. It is a way that servers can share information about their current state, and also a channel through which an administrate can modify pre-defined values. Port number of SNMP is 161(TCP) and 162(UDP).

Command

```
snmpget -mALL -v1 -cpublicsnmp_agent_Ip_address sysName.0
```

9. DNS:

It stands for Domain Name System. Every time you use a domain name, therefore, a

DNS service must translate the name into the corresponding IP address. For example, the domain name www.abc.com might translate to 198.105.232.4. Port number for DNS is 53.

Command

```
ipconfig /flushdns
```

10. DHCP:

It stands for Dynamic Host Configuration Protocol (DHCP).It gives IP addresses to hosts.There is a lot of information a DHCP server can provide to a host when the host is registering for an IP address with the DHCP server. Port number for DHCP is 67, 68.

Command

```
clearipdhcp binding {address | * }
```

IP ADDRESS AND IP SUBNET

Computers have significantly changed the way we live. A computing device when connected to other computing device(s) enables us to share data and information at lightning fast speed.

What is Network?

A Network in the world of computers is said to be a collection of interconnected hosts, via some shared media which can be wired or wireless. A computer network enables its hosts to share and exchange data and information over the media. Network can be a Local Area Network spanned across an office or Metro Area Network spanned across a city or Wide Area Network which can be spanned across cities and provinces.

A computer network can be as simple as two PCs connected together via a single copper cable or it can be grown up to the complexity where every computer in this world is connected to every other, called the Internet. A network then includes more and more components to reach its ultimate goal of data exchange. Below is a brief description of the components involved in computer network −

- **Hosts** − Hosts are said to be situated at ultimate end of the network, i.e. a host is a source of information and another host will be the destination. Information flows end to end between hosts. A host can be a user's PC, an internet Server, a database server etc.
- **Media** − If wired, then it can be copper cable, fiber optic cable, and coaxial cable. If wireless, it can be free-to-air radio frequency or some special wireless band. Wireless frequencies can be used to interconnect remote sites too.
- **Hub** − A hub is a multiport repeater and it is used to connect hosts in a LAN segment. Because of low throughputs hubs are now rarely used. Hub works on Layer-1 (Physical Layer) of OSI Model.
- **Switch** − A Switch is a multiport bridge and is used to connect hosts in a LAN segment. Switches are much faster than Hubs and operate on wire speed. Switch works on Layer-2 (Data Link Layer), but Layer-3 (Network Layer) switches are also available.
- **Router** − A router is Layer-3 (Network Layer) device which makes routing decisions for the data/information sent for some remote destination. Routers make the core of any interconnected network and the Internet.
- **Gateways** − A software or combination of software and hardware put together, works for exchanging data among networks which are using different protocols for sharing data.
- **Firewall** − Software or combination of software and hardware, used to protect users data from unintended recipients on the network/internet.

All components in a network ultimately serve the hosts.

Host Addressing

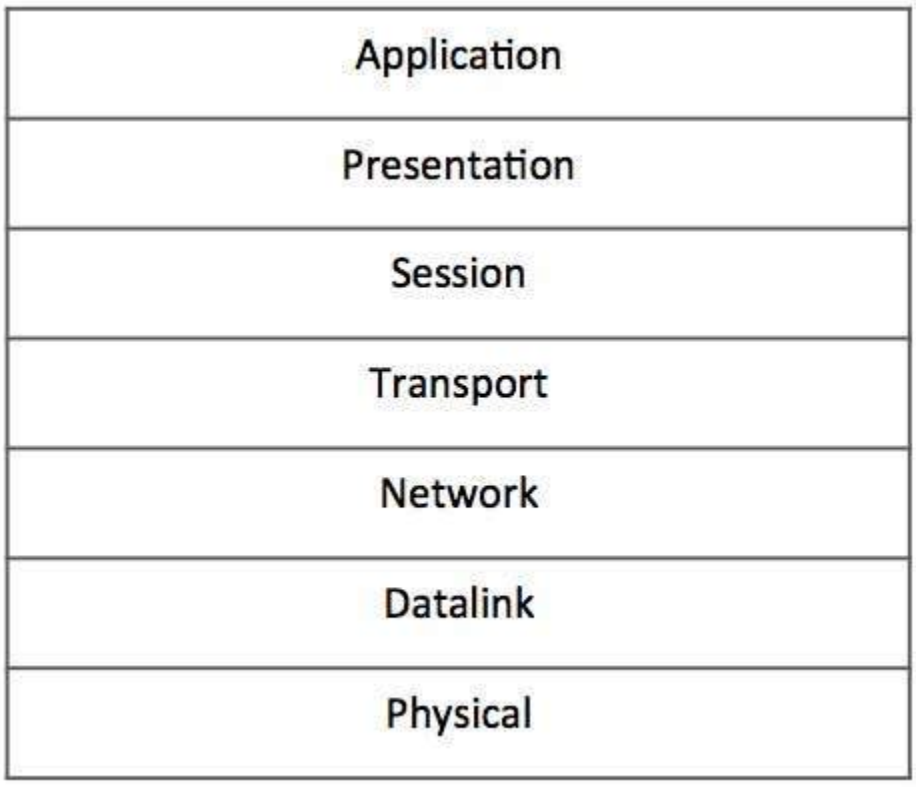
Communication between hosts can happen only if they can identify each other on the network. In a single collision domain (where every packet sent on the segment by one host is heard by every other host) hosts can communicate directly via MAC address.

MAC address is a factory coded 48-bits hardware address which can also uniquely identify a host. But if a host wants to communicate with a remote host, i.e. not in the same segment or logically not connected, then some means of addressing is required to identify the remote host uniquely. A logical address is given to all hosts connected to Internet and this logical address is called **Internet Protocol Address**.

IPv4 - OSI Model

The International Standard Organization has a well-defined model for Communication Systems known as Open System Interconnection, or the OSI Model. This layered model is a conceptualized view of how one system should communicate with the other, using various protocols defined in each layer. Further, each layer is designated to a well-defined part of communication system. For example, the Physical layer defines all the components of physical nature, i.e. wires, frequencies, pulse codes, voltage transmission etc. of a communication system.

The OSI Model has the following seven layers −



- **Application Layer (Layer-7)** − This is where the user application sits that needs to transfer data between or among hosts. For example − HTTP, file transfer application (FTP) and electronic mail etc.
- **Presentation Layer (Layer-6)** − This layer helps to understand data representation in one form on a host to other host in their native representation. Data from the sender is converted to on-the-wire data (general standard format) and at the receiver's end it is converted to the native representation of the receiver.
- **Session Layer (Layer-5)** − This layer provides session management capabilities between hosts. For example, if some host needs a password verification for access and if credentials are provided then for that session password verification does not happen again. This layer can assist in synchronization, dialog control and critical operation management (e.g., an online bank transaction).
- **Transport Layer (Layer-4)** − This layer provides end to end data delivery among hosts. This layer takes data from the above layer and breaks it into smaller units called Segments and then gives it to the Network layer for transmission.
- **Network Layer (Layer-3)** − This layer helps to uniquely identify hosts beyond the subnets and defines the path which the packets will follow or be routed to reach the destination.
- **Data Link Layer (Layer-2)** − This layer takes the raw transmission data (signal, pulses etc.) from the Physical Layer and makes Data Frames, and sends that to the upper layer and vice versa. This layer also checks any transmission errors and sorts it out accordingly.
- **Physical Layer (Layer-1)** − This layer deals with hardware technology and actual communication mechanism such as signaling, voltage, cable type and length, etc.

Network Layer

The network layer is responsible for carrying data from one host to another. It provides means to allocate logical addresses to hosts, and identify them uniquely using the same. Network layer takes data units from Transport Layer and cuts them in to smaller unit called Data Packet.

Network layer defines the data path, the packets should follow to reach the destination. Routers work on this layer and provides mechanism to route data to its destination.

IPv4 - TCP/IP Model

A majority of the internet uses a protocol suite called the Internet Protocol Suite also known as the TCP/IP protocol suite. This suite is a combination of protocols which encompasses a number of different protocols for different purpose and need. Because

the two major protocols in this suites are TCP (Transmission Control Protocol) and IP (Internet Protocol), this is commonly termed as TCP/IP Protocol suite. This protocol suite has its own reference model which it follows over the internet. In contrast with the OSI model, this model of protocols contains less layers.

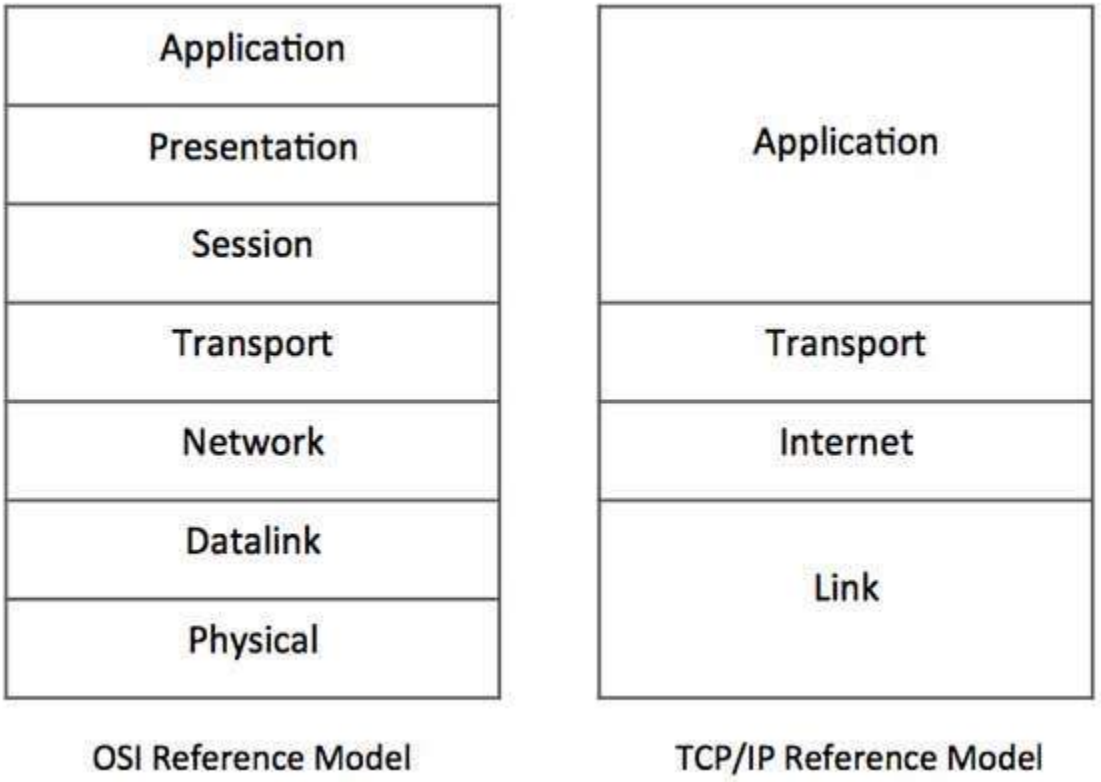


Figure − Comparative depiction of OSI and TCP/IP Reference Models

This model is indifferent to the actual hardware implementation, i.e. the physical layer of OSI Model. This is why this model can be implemented on almost all underlying technologies. Transport and Internet layers correspond to the same peer layers. All three top layers of OSI Model are compressed together in single Application layer of TCP/IP Model.

Internet Protocol Version 4 (IPv4)

Internet Protocol is one of the major protocols in the TCP/IP protocols suite. This protocol works at the network layer of the OSI model and at the Internet layer of the TCP/IP model. Thus this protocol has the responsibility of identifying hosts based upon their logical addresses and to route data among them over the underlying network.

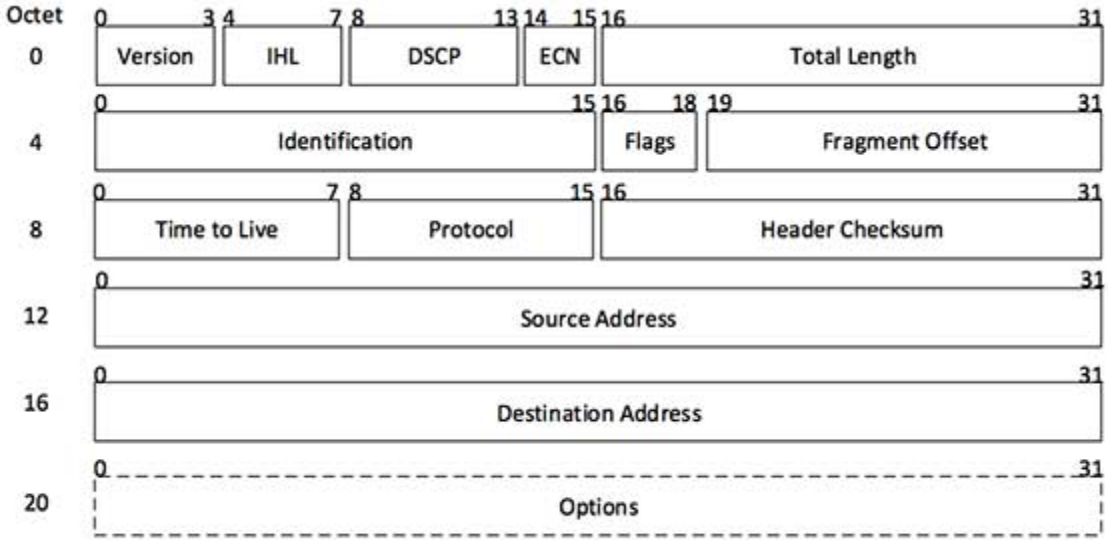
IP provides a mechanism to uniquely identify hosts by an IP addressing scheme. IP uses best effort delivery, i.e. it does not guarantee that packets would be delivered to the destined host, but it will do its best to reach the destination. Internet Protocol version 4 uses 32-bit logical address.

IPv4 - Packet Structure

Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets. IP packet encapsulates data unit received from above layer and add to its own header information.

(IP Encapsulation)

The encapsulated data is referred to as IP Payload. IP header contains all the necessary information to deliver the packet at the other end.



[Image: IP Header]

IP header includes many relevant information including Version Number, which, in this context, is 4. Other details are as follows −

- **Version** − Version no. of Internet Protocol used (e.g. IPv4).
- **IHL** − Internet Header Length; Length of entire IP header.
- **DSCP** − Differentiated Services Code Point; this is Type of Service.
- **ECN** − Explicit Congestion Notification; It carries information about the congestion seen in the route.
- **Total Length** − Length of entire IP Packet (including IP header and IP Payload).

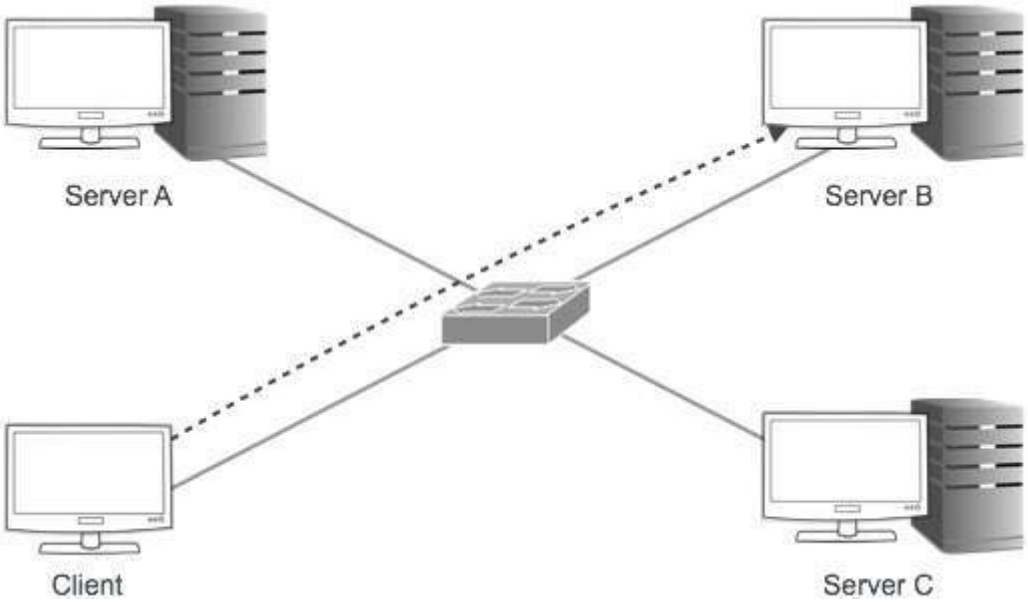
- **Identification** − If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet they belong to.
- **Flags** − As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'.
- **Fragment Offset** − This offset tells the exact position of the fragment in the original IP Packet.
- **Time to Live** − To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
- **Protocol** − Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.
- **Header Checksum** − This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
- **Source Address** − 32-bit address of the Sender (or source) of the packet.
- **Destination Address** − 32-bit address of the Receiver (or destination) of the packet.
- **Options** − This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

IPv4 - Addressing

IPv4 supports three different types of addressing modes. −

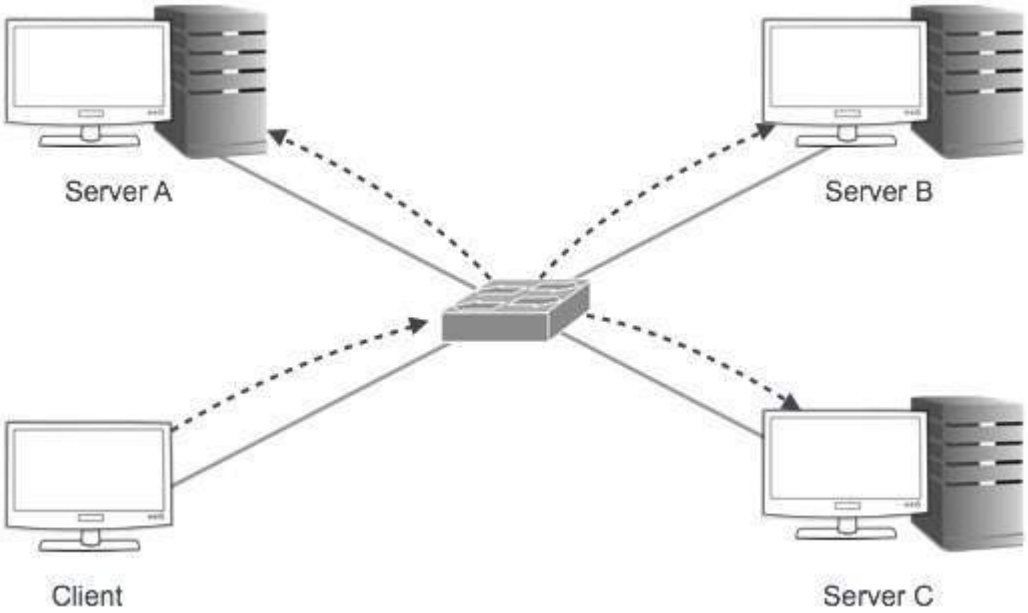
Unicast Addressing Mode

In this mode, data is sent only to one destined host. The Destination Address field contains 32- bit IP address of the destination host. Here the client sends data to the targeted server −



Broadcast Addressing Mode

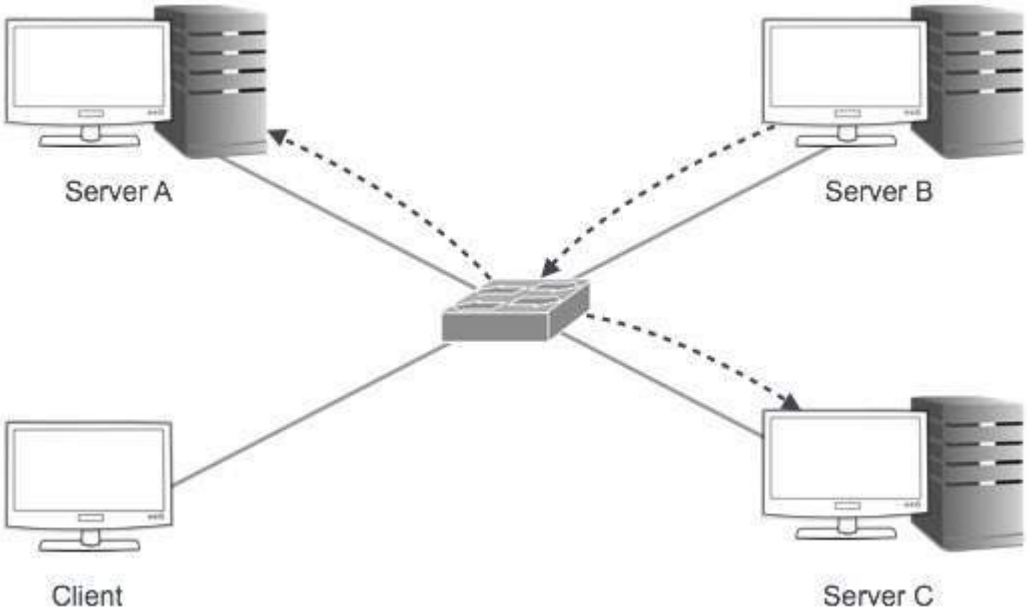
In this mode, the packet is addressed to all the hosts in a network segment. The Destination Address field contains a special broadcast address, i.e. **255.255.255.255**. When a host sees this packet on the network, it is bound to process it. Here the client sends a packet, which is entertained by all the Servers −



Multicast Addressing Mode

This mode is a mix of the previous two modes, i.e. the packet sent is neither destined to a single host nor all the hosts on the segment. In this packet, the Destination

Address contains a special address which starts with 224.x.x.x and can be entertained by more than one host.



Here a server sends packets which are entertained by more than one servers. Every network has one IP address reserved for the Network Number which represents the network and one IP address reserved for the Broadcast Address, which represents all the hosts in that network.

Hierarchical Addressing Scheme

IPv4 uses hierarchical addressing scheme. An IP address, which is 32-bits in length, is divided into two or three parts as depicted −

A single IP address can contain information about the network and its sub-network and ultimately the host. This scheme enables the IP Address to be hierarchical where a network can have many sub-networks which in turn can have many hosts.

Subnet Mask

The 32-bit IP address contains information about the host and its network. It is very necessary to distinguish both. For this, routers use Subnet Mask, which is as long as the size of the network address in the IP address. Subnet Mask is also 32 bits long. If the IP address in binary is ANDed with its Subnet Mask, the result yields the Network address. For example, say the IP Address is 192.168.1.152 and the Subnet Mask is 255.255.255.0 then −

IP	192.168.1.152	11000000	10101000	00000001	10011000	ANDed
Mask	255.255.255.0	11111111	11111111	11111111	00000000	
Network	192.168.1.0	11000000	10101000	00000001	00000000	Result

This way the Subnet Mask helps extract the Network ID and the Host from an IP Address. It can be identified now that 192.168.1.0 is the Network number and 192.168.1.152 is the host on that network.

Binary Representation

The positional value method is the simplest form of converting binary from decimal value. IP address is 32 bit value which is divided into 4 octets. A binary octet contains 8 bits and the value of each bit can be determined by the position of bit value '1' in the octet.

MSB	8^{th}	7^{th}	6^{th}	5^{th}	4^{th}	3^{rd}	2^{nd}	1^{st}	LSB
	1	1	1	1	1	1	1	1	
Positional Value	128	64	32	16	8	4	2	1	

Positional value of bits is determined by 2 raised to power (position – 1), that is the value of a bit 1 at position 6 is 2^(6-1) that is 2^5 that is 32. The total value of the octet is determined by adding up the positional value of bits. The value of 11000000 is 128+64 = 192. Some examples are shown in the table below −

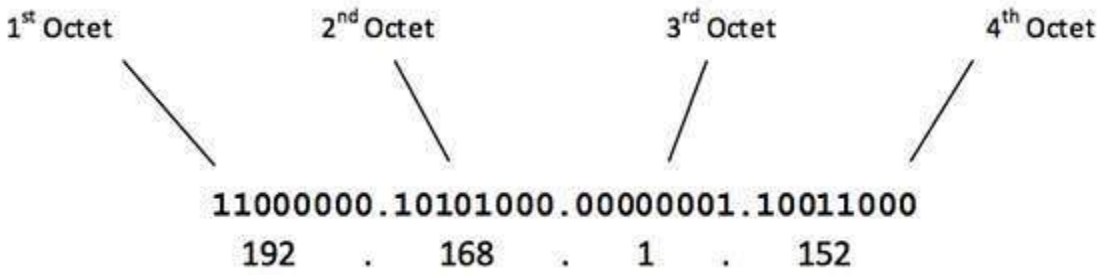
128	64	32	16	8	4	2	1	Value
0	0	0	0	0	0	0	1	1
0	0	0	0	0	0	1	0	2
0	0	0	0	0	0	1	1	3
0	0	0	0	0	1	0	0	4
0	0	0	0	0	1	0	1	5
0	0	0	0	0	1	1	0	6
0	0	0	0	0	1	1	1	7
0	0	0	0	1	0	0	0	8
0	0	0	0	1	0	0	1	9
0	0	0	0	1	0	1	0	10
0	0	0	1	0	0	0	0	16
0	0	1	0	0	0	0	0	32
0	1	0	0	0	0	0	0	64
0	1	1	0	0	1	0	0	100
0	1	1	1	1	1	1	1	127
1	0	0	0	0	0	0	0	128
1	0	1	0	1	0	0	0	168
1	1	0	0	0	0	0	0	192
1	1	1	1	1	1	1	1	255

IPv4 - Address Classes

Internet Protocol hierarchy contains several classes of IP Addresses to be used efficiently in various situations as per the requirement of hosts per network. Broadly, the IPv4 Addressing system is divided into five classes of IP Addresses. All the five classes are identified by the first octet of IP Address.

Internet Corporation for Assigned Names and Numbers is responsible for assigning IP addresses.

The first octet referred here is the left most of all. The octets numbered as follows depicting dotted decimal notation of IP Address −



The number of networks and the number of hosts per class can be derived by this formula −

Number of networks	= 2^network_bits
Number of Hosts/Network	= 2^host_bits – 2

When calculating hosts' IP addresses, 2 IP addresses are decreased because they cannot be assigned to hosts, i.e. the first IP of a network is network number and the last IP is reserved for Broadcast IP.

Class A Address

The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e.

```
00000001 – 01111111
       1 – 127
```

Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.

The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (2^7-2) and 16777214 hosts (2^{24}-2).

Class A IP address format is thus: **0NNNNNNN**.HHHHHHHH.HHHHHHHH.HHHHHHHH

Class B Address

An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.

```
10000000 – 10111111
     128 – 191
```

Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.

Class B has 16384 (2^{14}) Network addresses and 65534 (2^{16}-2) Host addresses.

Class B IP address format is: **10NNNNNN.NNNNNNNN**.HHHHHHHH.HHHHHHHH

Class C Address

The first octet of Class C IP address has its first 3 bits set to 110, that is −

11000000 – **110**11111
192 – 223

Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x.

Class C gives 2097152 (2^{21}) Network addresses and 254 (2^{8}-2) Host addresses.

Class C IP address format is: **110NNNNN.NNNNNNNN.NNNNNNNN**.HHHHHHHH

Class D Address

Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of −

11100000 – **1110**1111
224 – 239

Class D has IP address range from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

Class E Address

This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

IPv4 - Subnetting

Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of Networks and prefixed number of Hosts per network. Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more Networks per IP Class.

CIDR or **Classless Inter Domain Routing** provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class A IP address can be used to have smaller sub-

networks which provides better network management capabilities.

Class A Subnets

In Class A, only the first octet is used as Network identifier and rest of three octets are used to be assigned to Hosts (i.e. 16777214 Hosts per Network). To make more subnet in Class A, bits from Host part are borrowed and the subnet mask is changed accordingly.

For example, if one MSB (Most Significant Bit) is borrowed from host bits of second octet and added to Network address, it creates two Subnets (2^1=2) with (2^{23}-2) 8388606 Hosts per Subnet.

The Subnet mask is changed accordingly to reflect subnetting. Given below is a list of all possible combination of Class A subnets −

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
8	255.0.0.0	0	1	16777214
9	255.128.0.0	1	2	8388606
10	255.192.0.0	2	4	4194302
11	255.224.0.0	3	8	2097150
12	255.240.0.0	4	16	1048574
13	255.248.0.0	5	32	524286
14	255.252.0.0	6	64	262142
15	255.254.0.0	7	128	131070
16	255.255.0.0	8	256	65534
17	255.255.128.0	9	512	32766
18	255.255.192.0	10	1024	16382
19	255.255.224.0	11	2048	8190
20	255.255.240.0	12	4096	4094
21	255.255.248.0	13	8192	2046
22	255.255.252.0	14	16384	1022
23	255.255.254.0	15	32768	510
24	255.255.255.0	16	65536	254
25	255.255.255.128	17	131072	126
26	255.255.255.192	18	262144	62
27	255.255.255.224	19	524288	30
28	255.255.255.240	20	1048576	14
29	255.255.255.248	21	2097152	6
30	255.255.255.252	22	4194304	2

In case of subnetting too, the very first and last IP address of every subnet is used for Subnet Number and Subnet Broadcast IP address respectively. Because these two IP addresses cannot be assigned to hosts, sub-netting cannot be implemented by using more than 30 bits as Network Bits, which provides less than two hosts per subnet.

Class B Subnets

By default, using Classful Networking, 14 bits are used as Network bits providing (2^{14}) 16384 Networks and (2^{16}-2) 65534 Hosts. Class B IP Addresses can be subnetted the same way as Class A addresses, by borrowing bits from Host bits. Below is given all possible combination of Class B subnetting −

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
16	255.255.0.0	0	0	65534
17	255.255.128.0	1	2	32766
18	255.255.192.0	2	4	16382
19	255.255.224.0	3	8	8190
20	255.255.240.0	4	16	4094
21	255.255.248.0	5	32	2046
22	255.255.252.0	6	64	1022
23	255.255.254.0	7	128	510
24	255.255.255.0	8	256	254
25	255.255.255.128	9	512	126
26	255.255.255.192	10	1024	62
27	255.255.255.224	11	2048	30
28	255.255.255.240	12	4096	14
29	255.255.255.248	13	8192	6
30	255.255.255.252	14	16384	2

Class C Subnets

Class C IP addresses are normally assigned to a very small size network because it can only have 254 hosts in a network. Given below is a list of all possible combination of subnetted Class B IP address −

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
24	255.255.255.0	0	1	254
25	255.255.255.128	1	2	126
26	255.255.255.192	2	4	62
27	255.255.255.224	3	8	30
28	255.255.255.240	4	16	14
29	255.255.255.248	5	32	6
30	255.255.255.252	6	64	2

IPv4 - VLSM

Internet Service Providers may face a situation where they need to allocate IP subnets of different sizes as per the requirement of customer. One customer may ask Class C subnet of 3 IP addresses and another may ask for 10 IPs. For an ISP, it is not feasible to divide the IP addresses into fixed size subnets, rather he may want to subnet the subnets in such a way which results in minimum wastage of IP addresses.

For example, an administrator have 192.168.1.0/24 network. The suffix /24 (pronounced as "slash 24") tells the number of bits used for network address. In this example, the administrator has three different departments with different number of hosts. Sales department has 100 computers, Purchase department has 50 computers, Accounts has 25 computers and Management has 5 computers. In CIDR, the subnets are of fixed size. Using the same methodology the administrator cannot fulfill all the requirements of the network.

The following procedure shows how VLSM can be used in order to allocate department-wise IP addresses as mentioned in the example.

Step - 1

Make a list of Subnets possible.

Subnet Mask	Slash Notation	Hosts/Subnet
255.255.255.0	/24	254
255.255.255.128	/25	126
255.255.255.192	/26	62
255.255.255.224	/27	30
255.255.255.240	/28	14
255.255.255.248	/29	6
255.255.255.252	/30	2

Step - 2

Sort the requirements of IPs in descending order (Highest to Lowest).

- Sales 100
- Purchase 50
- Accounts 25
- Management 5

Step - 3

Allocate the highest range of IPs to the highest requirement, so let's assign 192.168.1.0 /25 (255.255.255.128) to the Sales department. This IP subnet with Network number 192.168.1.0 has 126 valid Host IP addresses which satisfy the requirement of the Sales department. The subnet mask used for this subnet has 10000000 as the last octet.

Step - 4

Allocate the next highest range, so let's assign 192.168.1.128 /26 (255.255.255.192) to the Purchase department. This IP subnet with Network number 192.168.1.128 has 62 valid Host IP Addresses which can be easily assigned to all the PCs of the Purchase department. The subnet mask used has 11000000 in the last octet.

Step - 5

Allocate the next highest range, i.e. Accounts. The requirement of 25 IPs can be fulfilled with 192.168.1.192 /27 (255.255.255.224) IP subnet, which contains 30 valid host IPs. The network number of Accounts department will be 192.168.1.192. The last octet of subnet mask is 11100000.

Step - 6

Allocate the next highest range to Management. The Management department contains only 5 computers. The subnet 192.168.1.224 /29 with the Mask 255.255.255.248 has exactly 6 valid host IP addresses. So this can be assigned to Management. The last octet of the subnet mask will contain 11111000.

By using VLSM, the administrator can subnet the IP subnet in such a way that least number of IP addresses are wasted. Even after assigning IPs to every department, the administrator, in this example, is still left with plenty of IP addresses which was not possible if he has used CIDR.

IPv4 - Reserved Addresses

There are a few reserved IPv4 address spaces which cannot be used on the internet. These addresses serve special purpose and cannot be routed outside the Local Area Network.

Private IP Addresses

Every class of IP, (A, B & C) has some addresses reserved as Private IP addresses. These IPs can be used within a network, campus, company and are private to it. These addresses cannot be routed on the Internet, so packets containing these private addresses are dropped by the Routers.

Class A IP Range	Subnet Mask
10.0.0.0 – 10.255.255.255	255.0.0.0
172.16.0.0 – 172.31.255.255	255.240.0.0
192.168.0.0 – 192.168.255.255	255.255.0.0

In order to communicate with the outside world, these IP addresses must have to be translated to some public IP addresses using NAT process, or Web Proxy server can be used.

The sole purpose to create a separate range of private addresses is to control assignment of already-limited IPv4 address pool. By using a private address range within LAN, the requirement of IPv4 addresses has globally decreased significantly. It has also helped delaying the IPv4 address exhaustion.

IP class, while using private address range, can be chosen as per the size and requirement of the organization. Larger organizations may choose class A private IP address range where smaller organizations may opt for class C. These IP addresses can be further sub-netted and assigned to departments within an organization.

Loopback IP Addresses

The IP address range 127.0.0.0 – 127.255.255.255 is reserved for loopback, i.e. a Host's self-address, also known as localhost address. This loopback IP address is managed entirely by and within the operating system. Loopback addresses, enable the Server and Client processes on a single system to communicate with each other. When a process creates a packet with destination address as loopback address, the operating system loops it back to itself without having any interference of NIC.

Data sent on loopback is forwarded by the operating system to a virtual network interface within operating system. This address is mostly used for testing purposes like client-server architecture on a single machine. Other than that, if a host machine can successfully ping 127.0.0.1 or any IP from loopback range, implies that the TCP/IP software stack on the machine is successfully loaded and working.

Link-local Addresses

In case a host is not able to acquire an IP address from the DHCP server and it has not been assigned any IP address manually, the host can assign itself an IP address from a range of reserved Link-local addresses. Link local address ranges from 169.254.0.0 -- 169.254.255.255.

Assume a network segment where all systems are configured to acquire IP addresses from a DHCP server connected to the same network segment. If the DHCP server is not available, no host on the segment will be able to communicate to any other. Windows (98 or later), and Mac OS (8.0 or later) supports this functionality of self-configuration of Link-local IP address. In absence of DHCP server, every host machine randomly chooses an IP address from the above mentioned range and then checks to ascertain by means of ARP, if some other host also has not configured itself with the same IP address. Once all hosts are using link local addresses of same range, they can communicate with each other.

These IP addresses cannot help system to communicate when they do not belong to the same physical or logical segment. These IPs are also not routable.

IPv4 - Example

This chapter describes how actual communication happens on the Network using Internet Protocol version 4.

Packet Flow in Network

All the hosts in IPv4 environment are assigned unique logical IP addresses. When a host wants to send some data to another host on the network, it needs the physical (MAC) address of the destination host. To get the MAC address, the host an broadcasts ARP message and asks to give the MAC address whoever is the owner of destination IP address. All the hosts on that segment receive the ARP packet, but only the host having its IP matching with the one in the ARP message, replies with its MAC address. Once the sender receives the MAC address of the receiving station, data is sent on the physical media.

In case the IP does not belong to the local subnet, the data is sent to the destination by means of Gateway of the subnet. To understand the packet flow, we must first understand the following components −

- **MAC Address** − Media Access Control Address is 48-bit factory hard coded physical address of network device which can uniquely be identified. This address is assigned by device manufacturers.
- **Address Resolution Protocol** − Address Resolution Protocol is used to acquire the MAC address of a host whose IP address is known. ARP is a Broadcast packet which is received by all the host in the network segment. But only the host whose IP is mentioned in ARP responds to it providing its MAC address.
- **Proxy Server** − To access the Internet, networks use a Proxy Server which has a public IP assigned. All the PCs request the Proxy Server for a Server on the Internet. The Proxy Server on behalf of the PCS sends the request to the server and when it receives a response from the Server, the Proxy Server forwards it to the client PC. This is a way to control Internet access in computer networks and it helps to implement web based policies.
- **Dynamic Host Control Protocol** − DHCP is a service by which a host is assigned IP address from a pre-defined address pool. DHCP server also provides necessary information such as Gateway IP, DNS Server Address, lease assigned with the IP, etc. By using DHCP services, a network administrator can manage assignment of IP addresses at ease.
- **Domain Name System** − It is very likely that a user does not know the IP address of a remote Server he wants to connect to. But he knows the name assigned to it, for example, tutorialpoints.com. When the user types the name of a remote server he wants to connect to, the localhost behind the screens sends a DNS query. Domain Name System is a method to acquire the IP address of the host whose Domain Name is known.

- **Network Address Translation** − Almost all PCs in a computer network are assigned private IP addresses which are not routable on the Internet. As soon as a router receives an IP packet with a private IP address, it drops it. In order to access servers on public private address, computer networks use an address translation service, which translates between public and private addresses, called Network Address Translation. When a PC sends an IP packet out of a private network, NAT changes the private IP address with public IP address and vice versa.

We can now describe the packet flow. Assume that a user wants to access www.TutorialsPoint.com from her personal computer. She has internet connection from her ISP. The following steps will be taken by the system to help her reach the destination website.

Step 1 – Acquiring an IP Address (DHCP)

When the user's PC boots up, it searches for a DHCP server to acquire an IP address. For the same, the PC sends a DHCPDISCOVER broadcast which is received by one or more DHCP servers on the subnet and they all respond with DHCPOFFER which includes all the necessary details such as IP, subnet, Gateway, DNS, etc. The PC sends DHCPREQUEST packet in order to request the offered IP address. Finally, the DHCP sends DHCPACK packet to tell the PC that it can keep the IP for some given amount of time that is known as IP lease.

Alternatively, a PC can be assigned an IP address manually without taking any help from DHCP server. When a PC is well configured with IP address details, it can communicate other computers all over the IP enabled network.

Step 2 – DNS Query

When a user opens a web browser and types www.tutorialpoints.com which is a domain name and a PC does not understand how to communicate with the server using domain names, then the PC sends a DNS query out on the network in order to obtain the IP address pertaining to the domain name. The pre-configured DNS server responds to the query with IP address of the domain name specified.

Step 3 – ARP Request

The PC finds that the destination IP address does not belong to his own IP address range and it has to forward the request to the Gateway. The Gateway in this scenario can be a router or a Proxy Server. Though the Gateway's IP address is known to the client machine but computers do not exchange data on IP addresses, rather they need the machine's hardware address which is Layer-2 factory coded MAC address. To obtain the MAC address of the Gateway, the client PC broadcasts an ARP request saying "Who owns this IP address?" The Gateway in response to the ARP query sends its MAC address. Upon receiving the MAC address, the PC sends the packets to the

Gateway.

An IP packet has both source and destination addresses and it connects the host with a remote host logically, whereas MAC addresses help systems on a single network segment to transfer actual data. It is important that source and destination MAC addresses change as they travel across the Internet (segment by segment) but source and destination IP addresses never change.

IPv4 - Summary

The Internet Protocol version 4 was designed to be allocated to approx. imately 4.3 billion addresses. At the beginning of Internet this was considered a much wider address space for which there was nothing to worry about.

The sudden growth in internet users and its wide spread use has exponentially increased the number of devices which needs real and unique IP to be able to communicate. Gradually, an IPS is required by almost every digital equipment which were made to ease human life, such as Mobile Phones, Cars and other electronic devices. The number of devices (other than computers/routers) expanded the demand for extra IP addresses, which were not considered earlier.

Allocation of IPv4 is globally managed by Internet Assigned Numbers Authority (IANA) under coordination with the Internet Corporation for Assigned Names and Numbers (ICANN). IANA works closely with Regional Internet Registries, which in turns are responsible for efficiently distributing IP addresses in their territories. There are five such RIRS. According to IANA reports, all the IPv4 address blocks have been allocated. To cope up with the situation, the following practices were being done −

- **Private IPs −** Few blocks of IPs were declared for private use within a LAN so that the requirement for public IP addresses can be reduced.
- **NAT −** Network address translation is a mechanism by which multiple PCs/hosts with private IP addresses are enabled to access using one or few public IP addresses.
- Unused Public IPs were reclaimed by RIRs.

Internet Protocol v6 (IPv6)

IETF (Internet Engineering Task Force) has redesigned IP addresses to mitigate the drawbacks of IPv4. The new IP address is version 6 which is 128-bit address, by which every single inch of the earth can be given millions of IP addresses.

Today majority of devices running on Internet are using IPv4 and it is not possible to shift them to IPv6 in the coming days. There are mechanisms provided by IPv6, by which IPv4 and IPv6 can co-exist unless the Internet entirely shifts to IPv6 −

- Dual IP Stack
- Tunneling (6to4 and 4to6)

- NAT Protocol Translation

IP Addressing / IP Subneting

IPV 4	IPV 6
• 32 bit • Unicast (One to One) • Multicast (One to Many) • Broadcast (One to All)	• 128 bit • Unicast • Multicast • Anycast (One to Closest)

32 bit (8 . 8 . 8 . 8)

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

IP Addressing introduced by IANA (Internet Assigned Number Authority)
IPV4 introducing 1980. It has many network to support different system. So, still we are not needed IPV6 network. 32 bit supports 4,294,967,296 Addresses.

Network Port / Subnet Mask

Class	Range	Masking $2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$	Total
Class A	1-127	0 0 0 0 0 0 0 0	0
Class B	128-191	1 0 0 0 0 0 0 0	128
Class C	192-223	1 1 0 0 0 0 0 0	128 + 64 = 192
Class D	224 – 239	1 1 1 0 0 0 0 0	128 + 64 + 32 = 224
Class E	240 – 225	1 1 1 1 0 0 0 0	128 + 64 + 32 + 16 =240

Network Port

Class	Port		Addresses
Class A	N .H .H . H	/8 (8*1)	255 .0 .0 . 0
Class B	N .N .H . H	/16 (8*2)	255 .255 .0 . 0
Class C	N .N . N. H	/24 (8*3)	255 .255 .255 . 0
Class D	Multicast		
Class E	Research / Development		

Introduction of MAC Address in Computer Network

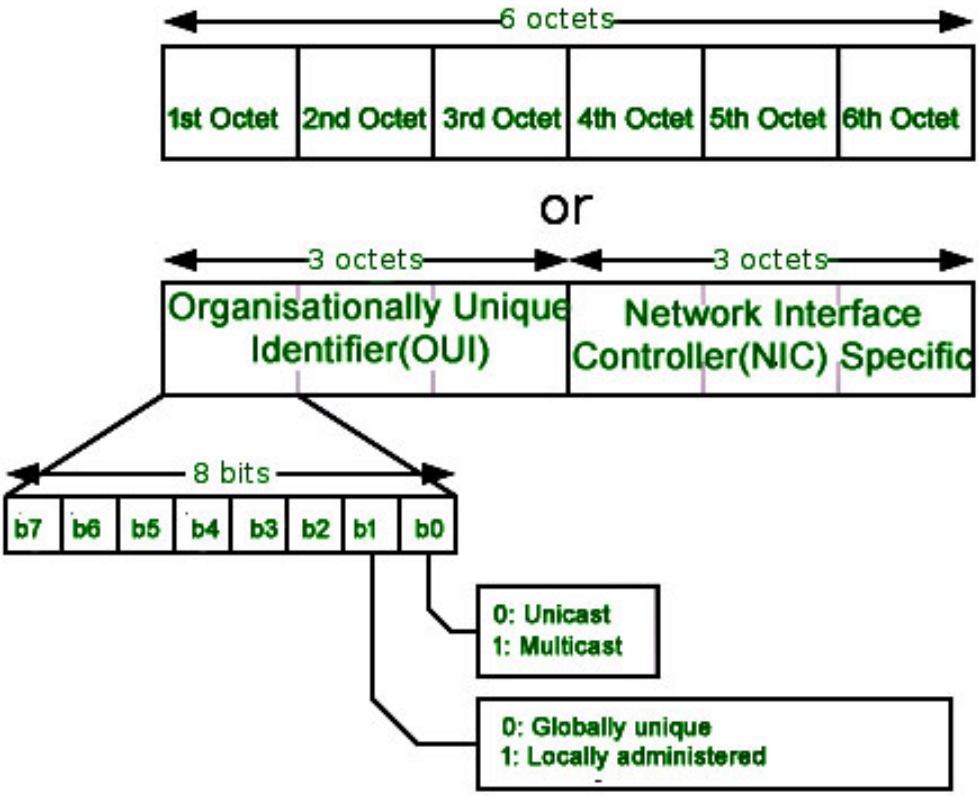
In order to communicate or transfer the data from one computer to another computer we need some address. In Computer Network various types of address are introduced; each works at different layer. Media Access Control Address is a physical address which works at Data Link Layer.

Media Access Control (MAC) Address –

MAC Addresses are unique **48-bits** hardware number of a computer, which is embedded into network card (known as **Network Interface Card**) during the time of manufacturing. MAC Address is also known as **Physical Address** of a network device. In IEEE 802 standard, Data Link Layer is divided into two sublayers –

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

MAC address is used by Media Access Control (MAC) sublayer of Data-Link Layer. MAC Address is word wide unique, since millions of network devices exists and we need to uniquely identify each.

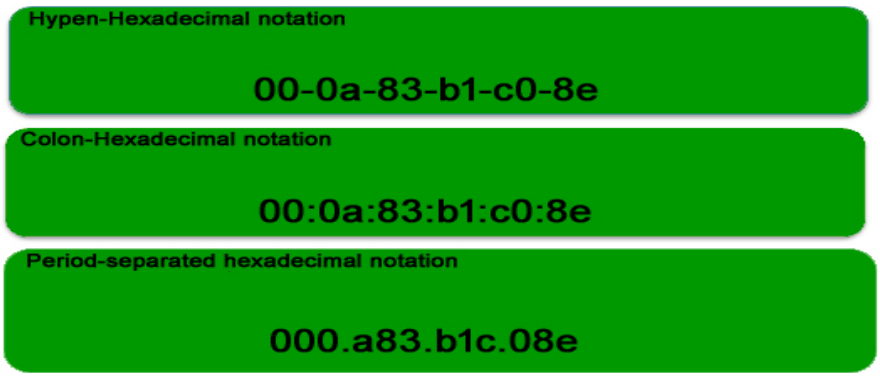


Format of MAC Address –

MAC Address is a 12-digit hexadecimal number (6-Byte binary number), which is mostly represented by Colon-Hexadecimal notation. First 6-digits (say 00:40:96) of MAC Address identifies the manufacturer, called as OUI (**Organizational Unique Identifier**). IEEE Registration Authority Committee assign these MAC prefixes to its registered vendors.
Here are some OUI of well knownmanufacturers :

```
CC:46:D6 - Cisco

3C:5A:B4 - Google, Inc.

3C:D9:2B - Hewlett Packard

00:9A:CD - HUAWEI TECHNOLOGIES CO.,LTD
```

The rightmost six digits represents **Network Interface Controller**, which is assigned by manufacturer.
As discussed above, MAC address is represented by Colon-Hexadecimal notation. But this is just a conversion, not mandatory. MAC address can be represented using any of the following formats –



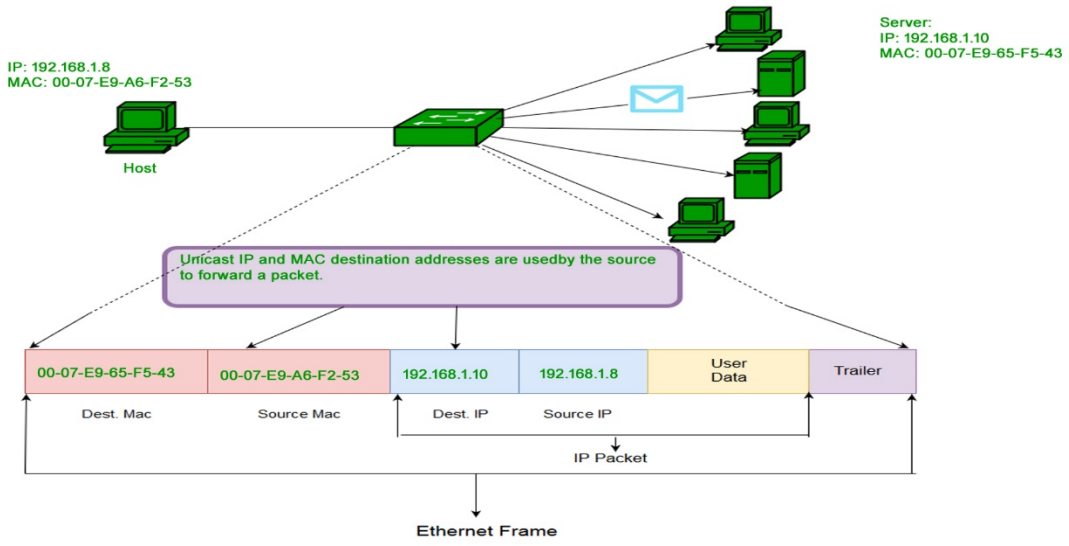
How to find MAC address –

```
Command for UNIX/Linux -  ifconfig -a
ip link list
ip address show

Command forWindows OS -  ipconfig /all

MacOS -                   TCP/IP Control Panel
```

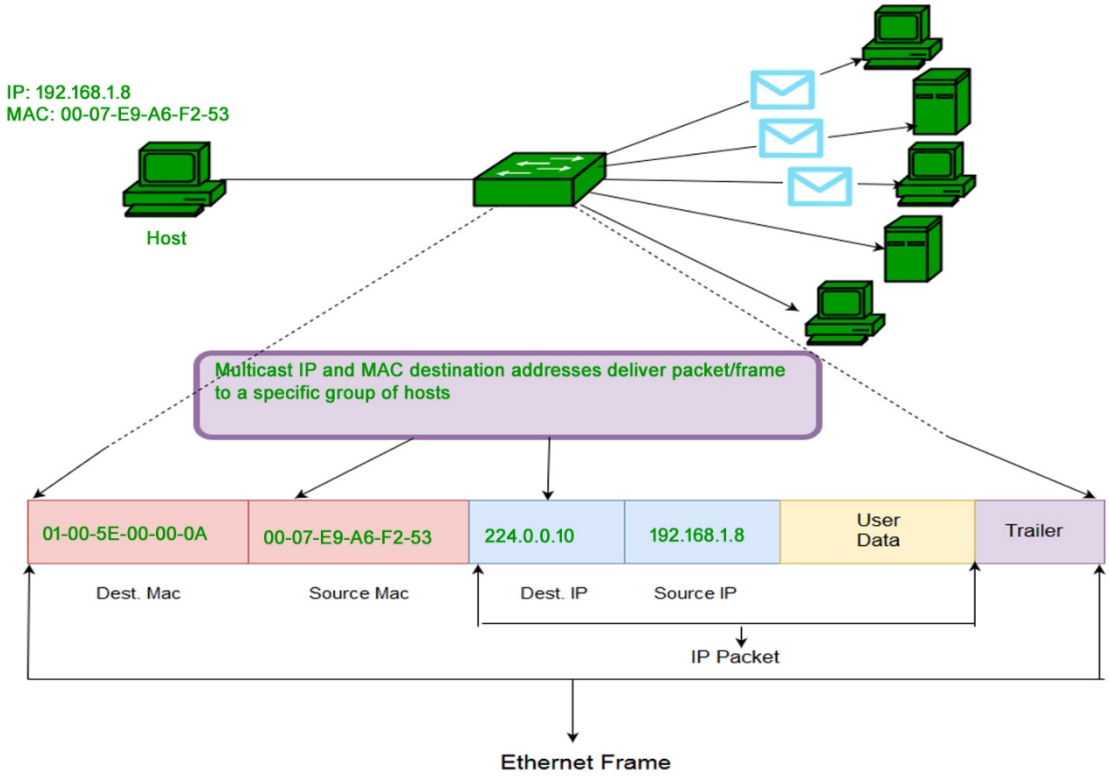
Note – LAN technologies like Token Ring, Ethernet use MAC Address as their Physical address but there are some networks (AppleTalk) which does not use MAC address.

Types of MAC Address –

1. **Unicast –** A Unicast addressed frame is only sent out to the interface leading to specific NIC. If the LSB (least significant bit) of first octet of an address is set to zero, the frame is meant to reach only one receiving NIC. MAC Address of source machine is always Unicast.

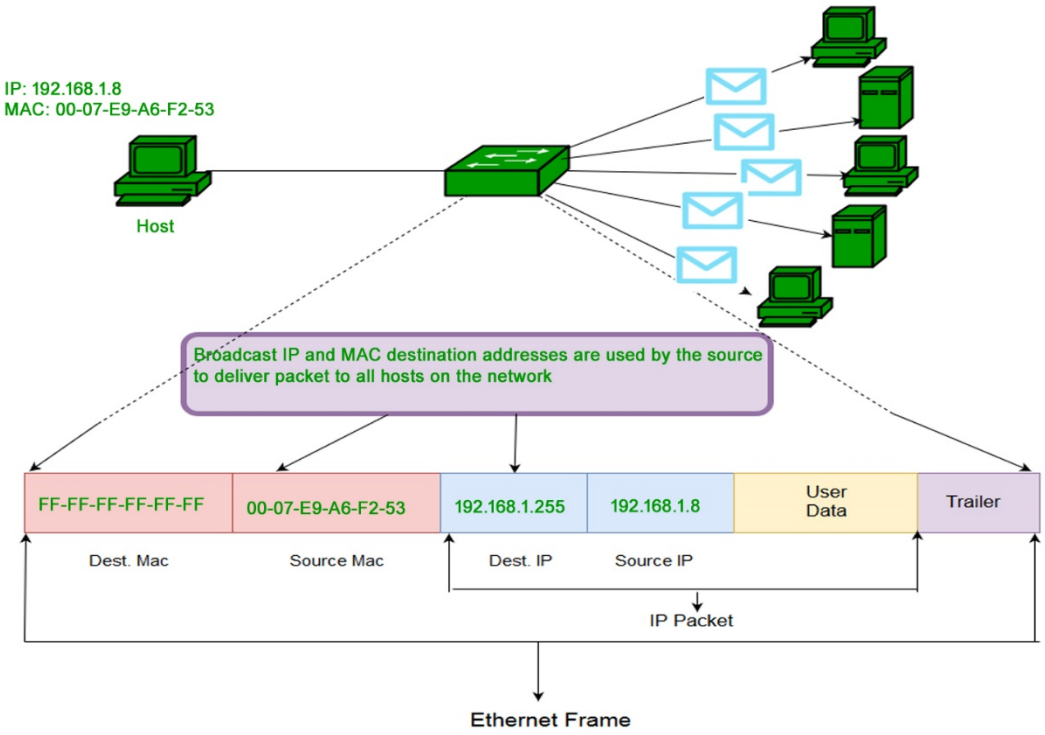


2. **Multicast –** Multicast address allow the source to send a frame to group of devices. In Layer-2 (Ethernet) Multicast address, LSB (least significant bit) of first octet of an address is set to one. IEEE has allocated the address block 01-80-C2-xx-xx-xx (01-80-C2-00-00-00 to 01-80-C2-FF-FF-FF) for group addresses for use by standard protocols.



3. **Broadcast –** Similar to Network Layer, Broadcast is also possible on underlying layer(Data Link Layer). Ethernet frames with ones in all bits of the destination address (FF-FF-FF-FF-FF-FF) are referred as broadcast address. Frames which

are destined with MAC address FF-FF-FF-FF-FF-FF will reach to every computer belong to that LAN segment.



PROTOCOL

A protocol is a standard set of rules that allow electronic devices to communicate with each other. These rules include what type of data may be transmitted, what commands are used to send and receive data, and how data transfers are confirmed.

IP (INTERNET PROTOCOL)

The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.

When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

SLIP (SERIAL / SINGLE LINE INTERNET PROTOCOL)

Serial Line Internet Protocol (SLIP) is a simple protocol that works with TCP/IP for communication over serial ports and routers. They provide communications between machines that were previously configured for direct communication with each other.

For example, a client may be connected to the Internet service provider (ISP) with a slower SLIP line. When a service is required, the client places a request to the ISP. The ISP responds to the request and passes it over to the Internet via high speed multiplexed lines. The ISP then sends the results back to the client via the SLIP lines.

Advantages of SLIP

- It has a very small overhead. So, it is suitable for usage in microcontrollers.
- It reuses the existing dial-up connections and telephone lines.
- It supports the most widely used protocol, Internet Protocol (IP). So, there is ease of deployment.

PPP (POINT TO POINT PROTOCOL)

Point - to - Point Protocol (PPP) is a communication protocol of the data link layer that is used to transmit multiprotocol data between two directly connected (point-to-point) computers. It is a byte - oriented protocol that is widely used in broadband communications having heavy loads and high speeds. Since it is a data link layer protocol, data is transmitted in frames. It is also known as RFC 1661.

Services Provided by PPP

The main services provided by Point - to - Point Protocol are −

- Defining the frame format of the data to be transmitted.
- Defining the procedure of establishing link between two points and exchange of data.
- Stating the method of encapsulation of network layer data in the frame.
- Stating authentication rules of the communicating devices.
- Providing address for network communication.
- Providing connections over multiple links.
- Supporting a variety of network layer protocols by providing a range of services.

Components of PPP

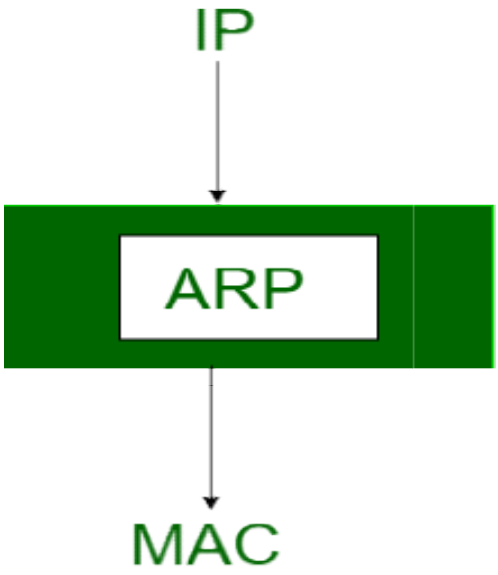
Point - to - Point Protocol is a layered protocol having three components −

- **Encapsulation Component** − It encapsulates the datagram so that it can be transmitted over the specified physical layer.
- **Link Control Protocol (LCP)** − It is responsible for establishing, configuring, testing, maintaining and terminating links for transmission. It also imparts negotiation for set up of options and use of features by the two endpoints of the links.
- **Authentication Protocols (AP)** − These protocols authenticate endpoints for use of services. The two authentication protocols of PPP are −
    - Password Authentication Protocol (PAP)
    - Challenge Handshake Authentication Protocol (CHAP)
- **Network Control Protocols (NCPs)** − These protocols are used for negotiating the parameters and facilities for the network layer. For every higher-layer protocol supported by PPP, one NCP is there. Some of the NCPs of PPP are −
    - Internet Protocol Control Protocol (IPCP)
    - OSI Network Layer Control Protocol (OSINLCP)
    - Internetwork Packet Exchange Control Protocol (IPXCP)
    - DECnet Phase IV Control Protocol (DNCP)
    - NetBIOS Frames Control Protocol (NBFCP)

- IPv6 Control Protocol (IPV6CP)

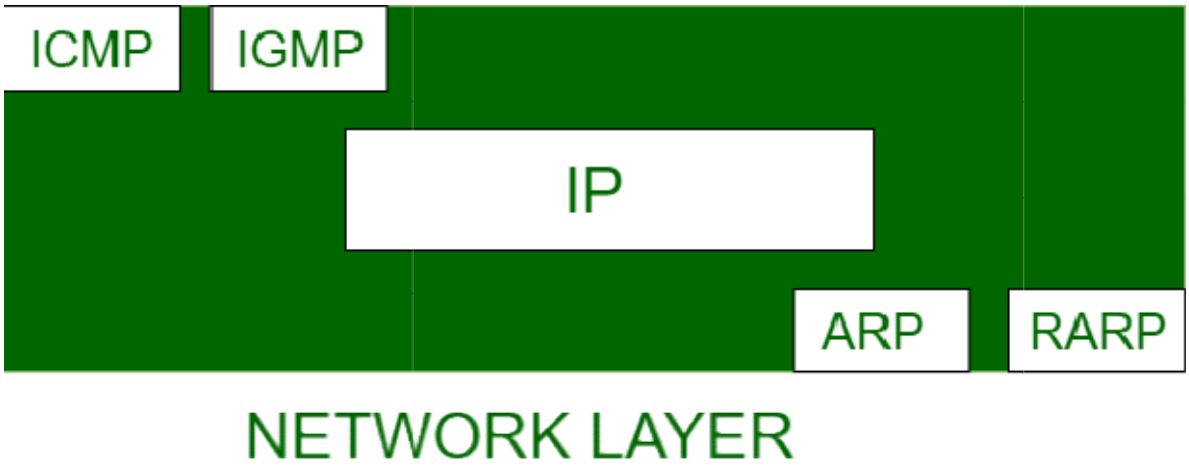
ARP (ADRESS RESOLUTION PROTOCOL)

Most of the computer programs/applications use **logical address (IP address)** to send/receive messages, however the actual communication happens over the **physical address (MAC address)** i.e from layer 2 of OSI model. So our mission is to get the destination MAC address which helps in communicating with other devices. This is where ARP comes into the picture, its functionality is to translate IP address to physical address.



The acronym ARP stands for **Address Resolution Protocol** which is one of the most important protocols of the Network layer in the OSI model.

Note: ARP finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address.



Imagine a device wants to communicate with the other over the internet. What ARP does? Is it broadcast a packet to all the devices of the source network?

The devices of the network peel the header of the data link layer from the **protocol data unit (PDU)** called frame and transfers the packet to the network layer (layer 3 of OSI) where the network ID of the packet is validated with the destination IP's network ID of the packet and if

it's equal then it responds to the source with the MAC address of the destination, else the packet reaches the gateway of the network and broadcasts packet to the devices it is connected with and validates their network ID
The above process continues till the second last network device in the path to reach the destination where it gets validated and ARP, in turn, responds with the destination MAC address.

The important terms associated with ARP are:

1. **ARP Cache:** After resolving MAC address, the ARP sends it to the source where it stores in a table for future reference. The subsequent communications can use the MAC address from the table
2. **ARP Cache Timeout:** It indicates the time for which the MAC address in the ARP cache can reside
3. **ARP request:** This is nothing but broadcasting a packet over the network to validate whether we came across destination MAC address or not.
    1. The physical address of the sender.
    2. The IP address of the sender.
    3. The physical address of the receiver is FF:FF:FF:FF:FF:FF or 1's.
    4. The IP address of the receiver
4. **ARP response/reply:** It is the MAC address response that the source receives from the destination which aids in further communication of the data.

- **CASE-1:** The sender is a host and wants to send a packet to another host on the same network.
    - Use ARP to find another host's physical address
- **CASE-2:** The sender is a host and wants to send a packet to another host on another network.
    - Sender looks at its routing table.
    - Find the IP address of the next hop (router) for this destination.
    - Use ARP to find the router's physical address
- **CASE-3:** the sender is a router and received a datagram destined for a host on another network.
    - Router check its routing table.
    - Find the IP address of the next router.
    - Use ARP to find the next router's physical address.
- **CASE-4:** The sender is a router that has received a datagram destined for a host in the same network.
    - Use ARP to find this host's physical address.

RARP (REVERSE ADDRESS RESOLUTION PROTOCOL)

Reverse ARP is a networking protocol used by a client machine in a local area network to request its Internet Protocol address (IPv4) from the gateway-router's ARP table. The network administrator creates a table in gateway-router, which is used to map the MAC address to corresponding IP address.

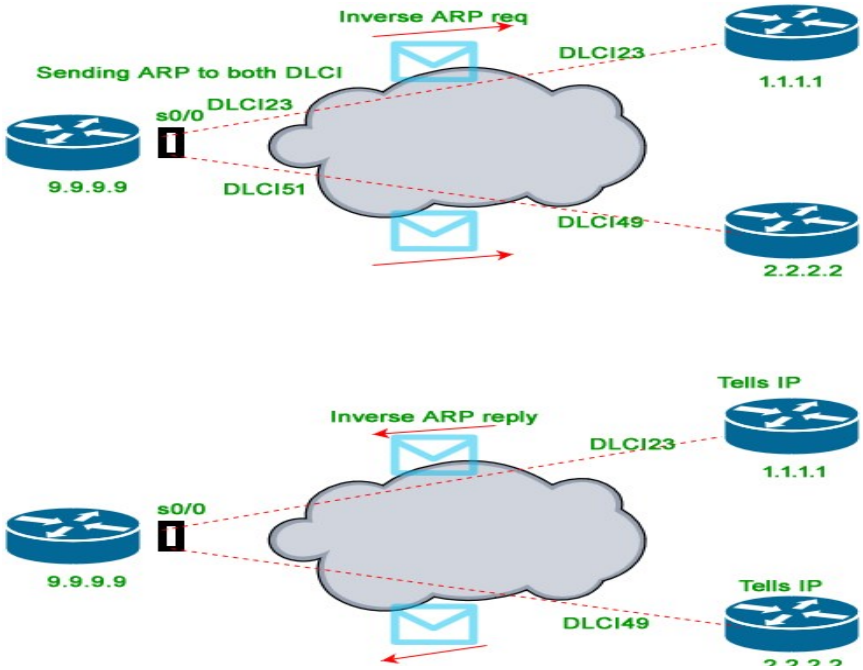
When a new machine is setup or any machine which don't have memory to store IP address, needs an IP address for its own use. So the machine sends a RARP broadcast packet which contains its own MAC address in both sender and receiver hardware address field.

A special host configured inside the local area network, called as RARP-server is responsible to reply for these kind of broadcast packets. Now the RARP server attempt to find out the entry in IP to MAC address mapping table. If any entry matches in table, RARP server send the response packet to the requesting device along with IP address.

- LAN technologies like Ethernet, Ethernet II, Token Ring and Fiber Distributed Data Interface (FDDI) support the Address Resolution Protocol.
- RARP is not being used in today's networks. Because we have much great featured protocols like BOOTP (Bootstrap Protocol) and DHCP(Dynamic Host Configuration Protocol).

3. Inverse Address Resolution Protocol (InARP) –

Instead of using Layer-3 address (IP address) to find MAC address, Inverse ARP uses MAC address to find IP address. As the name suggests, InARP is just inverse of ARP. Reverse ARP has been replaced by BOOTP and later DHCP but Inverse ARP is solely used for device configuration. Inverse ARP is enabled by default in ATM(Asynchronous Transfer Mode) networks. InARP is used to find Layer-3 address from Layer-2 address (DLCI in frame relay). Inverse ARP dynamically maps local DLCIs to remote IP addresses when you configure Frame Relay. When using inverse ARP, we know the DLCI of remote router but don't know its IP address. InARP sends a request to obtain that IP address and map it to the Layer-2 frame-relay DLCI.



TCP (TRANSMISSION CONTROL PROTOCOL)

The transmission Control Protocol (TCP) is one of the most important protocols of Internet Protocols suite. It is most widely used protocol for data transmission in communication network such as internet.

Features

- TCP is reliable protocol. That is, the receiver always sends either positive or negative acknowledgement about the data packet to the sender, so that the sender always has bright clue about whether the data packet is reached the destination or it needs to resend it.
- TCP ensures that the data reaches intended destination in the same order it was sent.
- TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data.
- TCP provides error-checking and recovery mechanism.
- TCP provides end-to-end communication.
- TCP provides flow control and quality of service.
- TCP operates in Client/Server point-to-point mode.
- TCP provides full duplex server, i.e. it can perform roles of both receiver and sender.

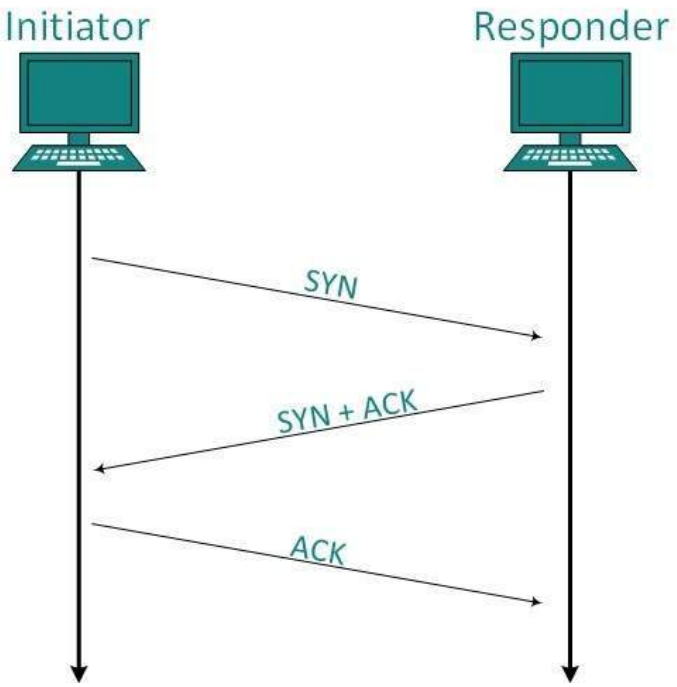
Addressing

TCP communication between two remote hosts is done by means of port numbers (TSAPs). Ports numbers can range from 0 – 65535 which are divided as:

- System Ports (0 – 1023)
- User Ports (1024 – 49151)
- Private/Dynamic Ports (49152 – 65535)

Connection Management

TCP communication works in Server/Client model. The client initiates the connection and the server either accepts or rejects it. Three-way handshaking is used for connection management.



Establishment

Client initiates the connection and sends the segment with a Sequence number. Server acknowledges it back with its own Sequence number and ACK of client's segment which is one more than client's Sequence number. Client after receiving ACK of its segment sends an acknowledgement of Server's response.

Release

Either of server and client can send TCP segment with FIN flag set to 1. When the receiving end responds it back by ACKnowledging FIN, that direction of TCP communication is closed and connection is released.

Bandwidth Management

TCP uses the concept of window size to accommodate the need of Bandwidth management. Window size tells the sender at the remote end, the number of data byte segments the receiver at this end can receive. TCP uses slow start phase by using window size 1 and increases the window size exponentially after each successful communication.

For example, the client uses windows size 2 and sends 2 bytes of data. When the acknowledgement of this segment received the windows size is doubled to 4 and next sent the segment sent will be 4 data bytes long. When the acknowledgement of 4-byte data segment is received, the client sets windows size to 8 and so on.

If an acknowledgement is missed, i.e. data lost in transit network or it received NACK, then the window size is reduced to half and slow start phase starts again.

Multiplexing

The technique to combine two or more data streams in one session is called Multiplexing. When a TCP client initializes a connection with Server, it always refers to a well-defined port number which indicates the application process. The client itself uses a randomly generated port number from private port number pools.

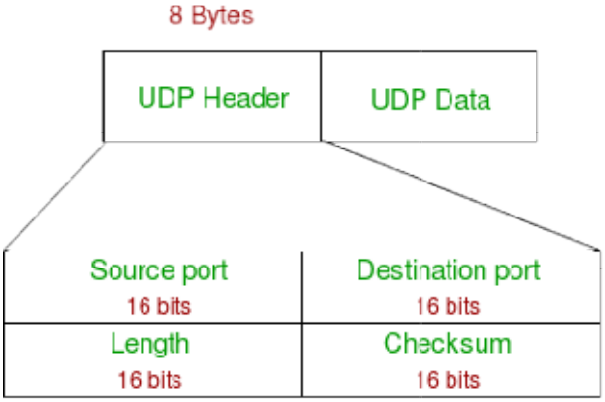
Using TCP Multiplexing, a client can communicate with a number of different application process in a single session. For example, a client requests a web page which in turn contains different types of data (HTTP, SMTP, FTP etc.) the TCP session timeout is increased and the session is kept open for longer time so that the three-way handshake overhead can be avoided.

This enables the client system to receive multiple connection over single virtual connection. These virtual connections are not good for Servers if the timeout is too long.

UDP (USER DATAGRAM PROTOCOL)

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

UDP Header –
UDP header is **8-bytes** fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. First 8 Bytes contains all necessary header information and remaining part consist of data. UDP port number fields are each 16 bits long, therefore range for port numbers defined from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or process.



1. **Source Port :** Source Port is 2 Byte long field used to identify port number of source.
2. **Destination Port :** It is 2 Byte long field, used to identify the port of destined packet.

3. **Length :** Length is the length of UDP including header and the data. It is 16-bits field.
4. **Checksum :** Checksum is 2 Bytes long field. It is the 16-bit one's complement of the one's complement sum of the UDP header, pseudo header of information from the IP header and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

HTTP (HYPER-TEXT TRANSFER PROTOCOL)

The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. This is the foundation for data communication for the World Wide Web (i.e. internet) since 1990. HTTP is a generic and stateless protocol which can be used for other purposes as well using extensions of its request methods, error codes, and headers.

Basically, HTTP is a TCP/IP based communication protocol, that is used to deliver data (HTML files, image files, query results, etc.) on the World Wide Web. The default port is TCP 80, but other ports can be used as well. It provides a standardized way for computers to communicate with each other. HTTP specification specifies how clients' request data will be constructed and sent to the server, and how the servers respond to these requests.

Basic Features

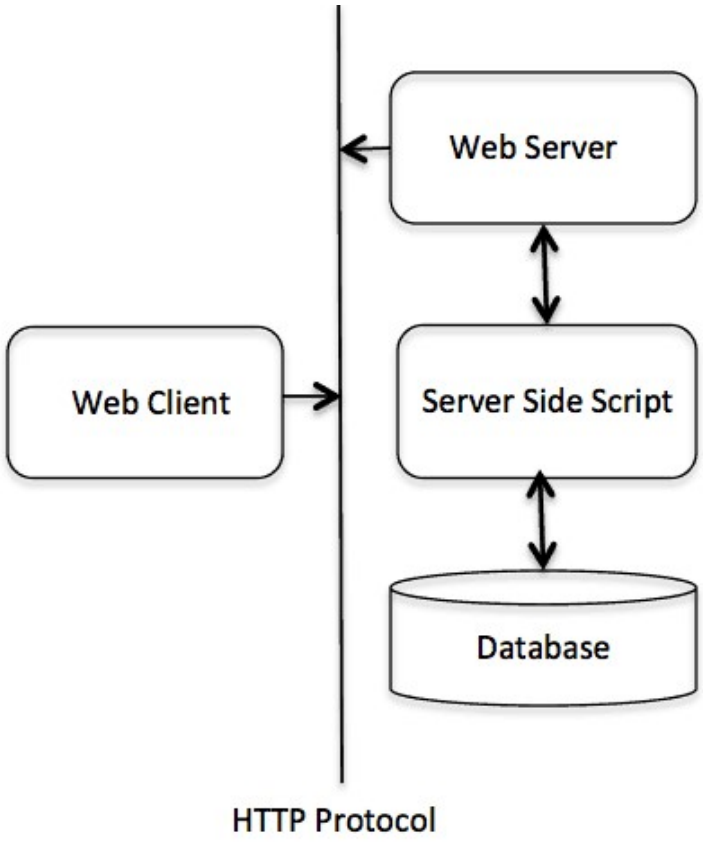
There are three basic features that make HTTP a simple but powerful protocol:

- **HTTP is connectionless:** The HTTP client, i.e., a browser initiates an HTTP request and after a request is made, the client waits for the response. The server processes the request and sends a response back after which client disconnect the connection. So client and server knows about each other during current request and response only. Further requests are made on new connection like client and server are new to each other.
- **HTTP is media independent:** It means, any type of data can be sent by HTTP as long as both the client and the server know how to handle the data content. It is required for the client as well as the server to specify the content type using appropriate MIME-type.
- **HTTP is stateless:** As mentioned above, HTTP is connectionless and it is a direct result of HTTP being a stateless protocol. The server and client are aware of each other only during a current request. Afterwards, both of them forget about each other. Due to this nature of the protocol, neither the client nor the browser can retain information between different requests across the web pages.

HTTP/1.0 uses a new connection for each request/response exchange, where as HTTP/1.1 connection may be used for one or more request/response exchanges.

Basic Architecture

The following diagram shows a very basic architecture of a web application and depicts where HTTP sits:



The HTTP protocol is a request/response protocol based on the client/server based architecture where web browsers, robots and search engines, etc. act like HTTP clients, and the Web server acts as a server.

Client

The HTTP client sends a request to the server in the form of a request method, URI, and protocol version, followed by a MIME-like message containing request modifiers, client information, and possible body content over a TCP/IP connection.

Server

The HTTP server responds with a status line, including the message's protocol version and a success or error code, followed by a MIME-like message containing server information, entity meta information, and possible entity-body content.

S-HTTP PROTOCOL (SERVER HTTP)

Secure Hypertext Transfer Protocol (SHTTP)

SHTTP extends the HTTP internet protocol with public key encryption, authentication, and digital signature over the internet. Secure HTTP supports multiple security mechanism, providing security to the end-users. SHTTP works by negotiating encryption scheme types used between the client and the server.

DNS (DOMAIN NAME SYSTEM)

DNS is a host name to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.

Requirement

Every host is identified by the IP address but remembering numbers is very difficult for the people and also the IP addresses are not static therefore a mapping is required to change the domain name to IP address. So DNS is used to convert the domain name of the websites to their numerical IP address.

Domain:

There are various kinds of DOMAIN :

1. Generic domain : .com(commercial) .edu(educational) .mil(military) .org(non profit organization) .net(similar to commercial) all these are generic domain.

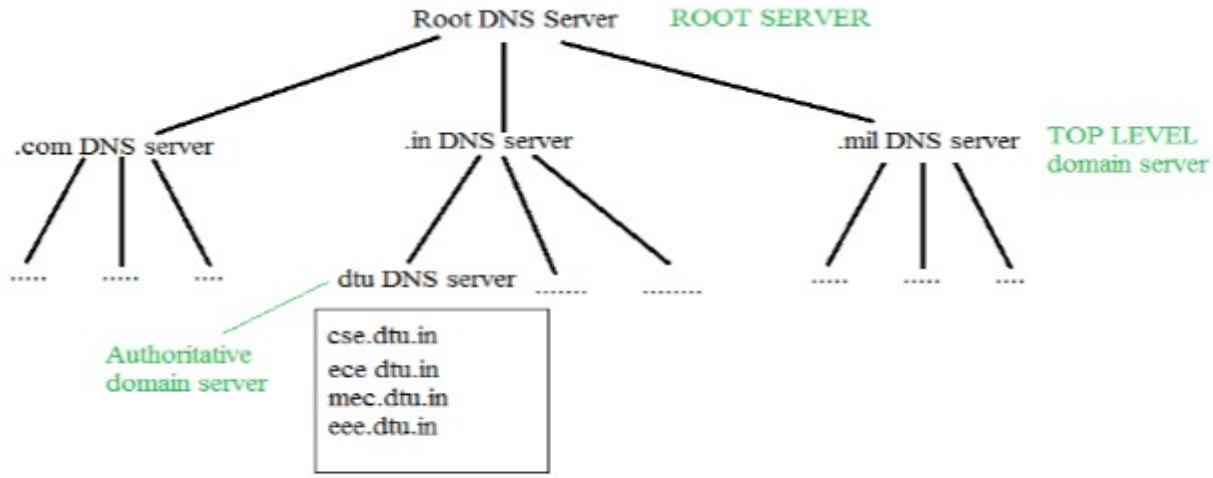
LEVEL	DESCRIPTION
.aero	Airlines & Aerospace
.biz	Business Firm
.com	Commercial Organization
.coop	Co-operative business organization
.edu	Educational Institute
.gov	Government Institute
.info	Information Service provider
.int	International Organization
.mil	Military Group
.name	Personal Name
.net	Network Support
.org	Non-profitable Organization

2. Country domain

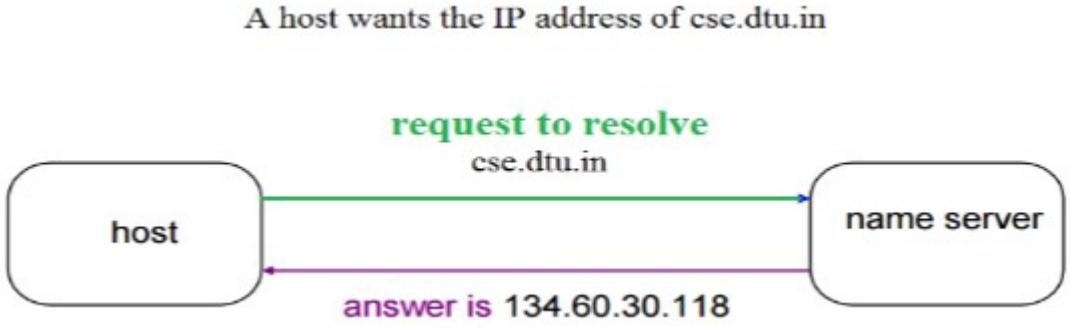
LEVEL	DESCRIPTION
.in	India
.fr	France
.us	United State
.aus	Australia
.sg	Singapore
.pk	Pakistan

3. Inverse domain if we want to know what is the domain name of the website. Ip to domain name mapping.

Organization of Domain



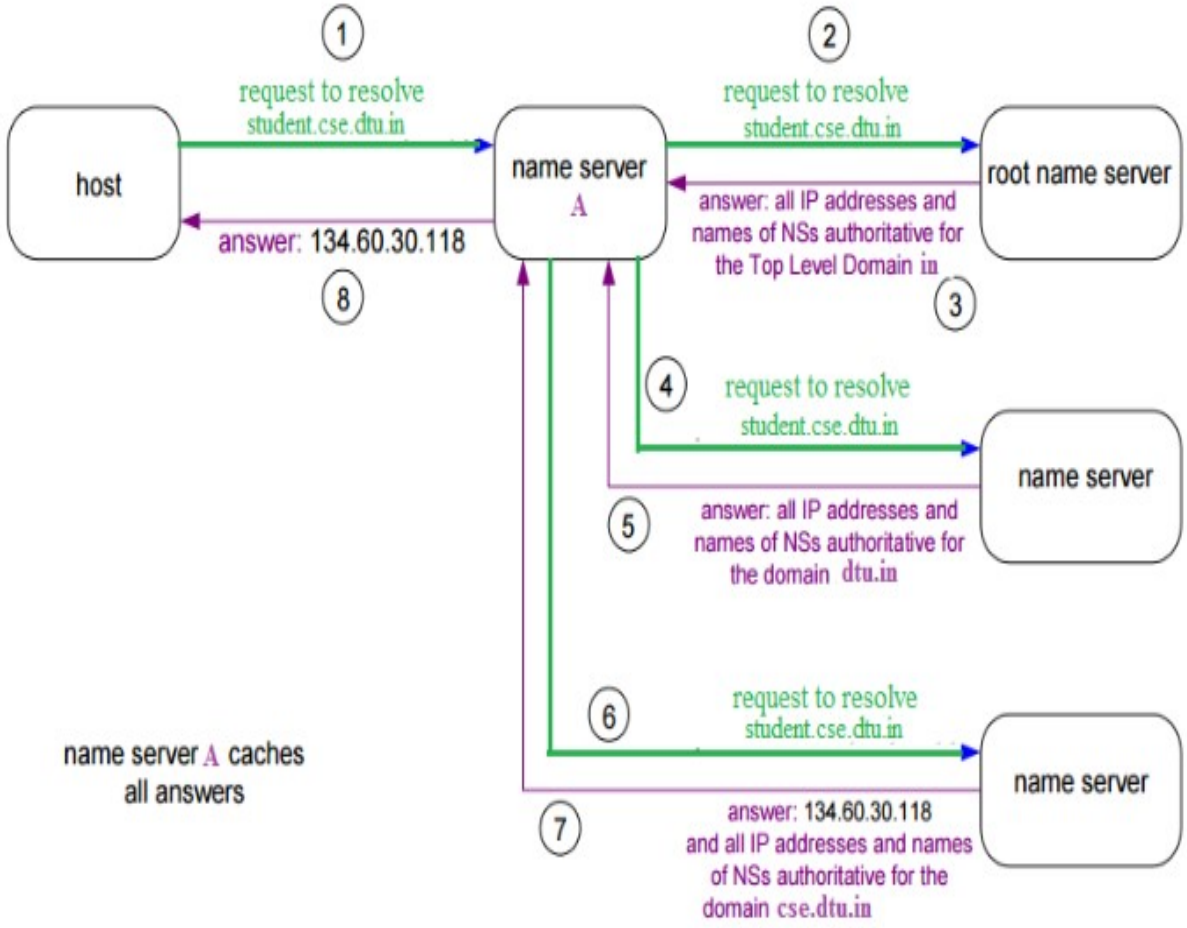
It is Very difficult to find out the ip address associated to a website because there are millions of websites and with all those websites we should be able to generate the ip address immediately, there should not be a lot of delay for that to happen organization of database is very important.
DNS record – Domain name, ip address what is the validity?? what is the time to live ?? and all the information related to that domain name. These records are stored in tree like structure.
Namespace – Set of possible names, flat or hierarchical . Naming system maintains a collection of bindings of names to values – given a name, a resolution mechanism returns the corresponding value –
Name server – It is an implementation of the resolution mechanism.. DNS (Domain Name System) = Name service in Internet – Zone is an administrative unit, domain is a subtree.
Name to Address Resolution



The host request the DNS name server to resolve the domain name. And the name server returns the IP address corresponding to that domain name to the host so that the host can future connect to that IP address.

Hierarchy of Name Servers

Root name servers – It is contacted by name servers that can not resolve the name. It contacts authoritative name server if name mapping is not known. It then gets the mapping and return the IP address to the host.
Top level server – It is responsible for com, org, eduetc and all top level country domains like uk, fr, ca, in etc. They have info about authoritative domain servers and know names and IP addresses of each authoritative name server for the second level domains.
Authoritative name servers This is organization's DNS server, providing authoritative hostName to IP mapping for organization servers. It can be maintained by organization or service provider. In order to reach cse.dtu.in we have to ask the root DNS server, then it will point out to the top level domain server and then to authoritative domain name server which actually contains the IP address. So the authoritative domain server will return the associative ip address.
Domain Name Server



The client machine sends a request to the local name server, which, if root does not find the address in its database, sends a request to the root name server, which in turn, will route the query to an intermediate or authoritative name server. The root name server can also contain

some hostname to IP address mappings. The intermediate name server always knows who the authoritative name server is. So finally the IP address is returned to the local name server which in turn returns the IP address to the host.

POP (POST OFFICE PROTOCOL)

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

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

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

POP uses the TCP/IP protocol stack for network connection and works with Simple Mail Transfer Protocol (SMTP) for end-to-end email communication, where POP pulls messages and SMTP pushes them to the

server. As of 2012, Post Office Protocol is in its third version known as POP 3 and is commonly used in most email client/server communication architecture.

IMAP (INTERNET MESSAGE ACCESS PROTOCOL)

IMAP stands for **Internet Message Access Protocol.** It was first proposed in 1986. There exist five versions of IMAP as follows:

1. Original IMAP
2. IMAP2
3. IMAP3
4. IMAP2bis
5. IMAP4

Key Points:

- IMAP allows the client program to manipulate the e-mail message on the server without downloading them on the local computer.
- The e-mail is hold and maintained by the remote server.
- It enables us to take any action such as downloading, delete the mail without reading the mail.It enables us to create, manipulate and delete remote message folders called mail boxes.
- IMAP enables the users to search the e-mails.
- It allows concurrent access to multiple mailboxes on multiple mail servers.

SMTP (SIMPLE MAIL TRANSFER PROTOCOL)

SMTP stands for **Simple Mail Transfer Protocol**. It was first proposed in 1982. It is a standard protocol used for sending e-mail efficiently and reliably over the internet.

Key Points:

- SMTP is application level protocol.
- SMTP is connection oriented protocol.
- SMTP is text based protocol.
- It handles exchange of messages between e-mail servers over TCP/IP network.
- Apart from transferring e-mail, SMPT also provides notification regarding incoming mail.
- When you send e-mail, your e-mail client sends it to your e-mail server which further contacts the recipient mail server using SMTP client.
- These SMTP commands specify the sender's and receiver's e-mail address, along with the message to be send.
- The exchange of commands between servers is carried out without intervention of any user.
- In case, message cannot be delivered, an error report is sent to the sender which makes SMTP a reliable protocol.

MIME (MULTIPURPOSE INTERNET MAIL EXTENSION)

MIME (Multipurpose Internet Mail Extension) media types were originally devised so that e-mails could include information other than plain text. MIME media types indicate the following things −

- How different parts of a message, such as text and attachments, are combined into the message.
- The way in which each part of the message is specified.
- The way different items are encoded for transmission so that even software that was designed to work only with ASCII text can process the message.

Now MIME types are not just for use with e-mail; they have been adopted by Web servers as a way to tell Web browsers what type of material was being sent to them so that they can cope with that kind of messages correctly.

MIME content types consist of two parts −

- A main type
- A sub-type

The main type is separated from the subtype by a forward slash character. For example, text/html for HTML.

This chapter is organized for the main types −

- text
- image
- multipart
- audio
- video
- message
- model
- application

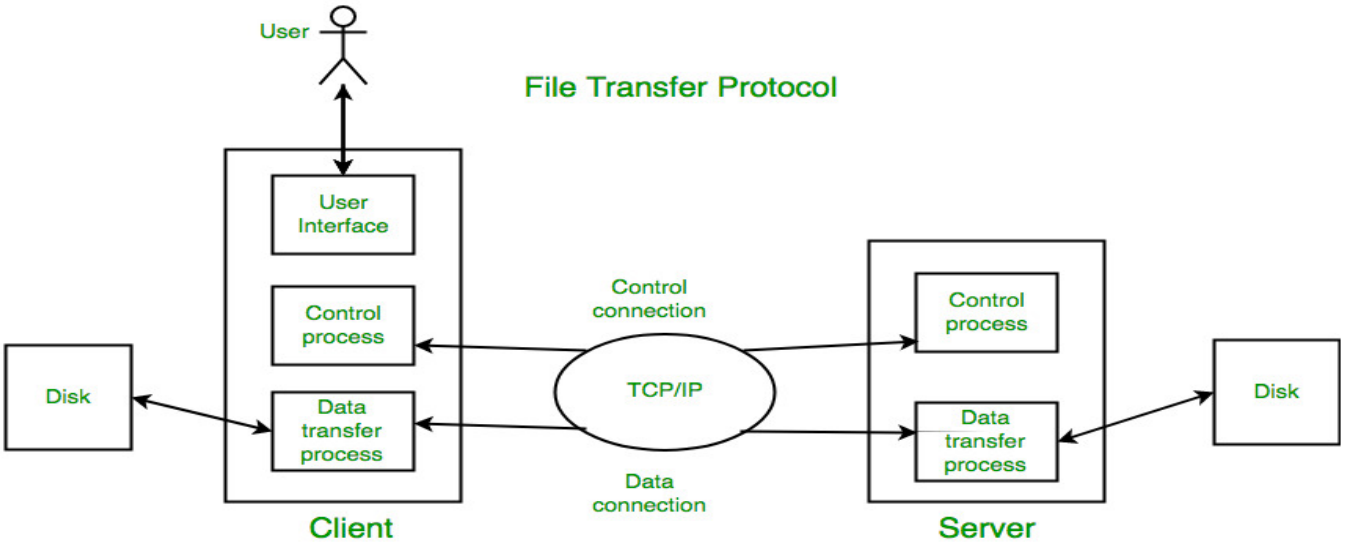
For example, the text main type contains types of plain text files, such as −

- text/plain for plain text files
- text/html for HTML files
- text/rtf for text files using rich text formatting

MIME types are officially supposed to be assigned and listed by the Internet Assigned Numbers Authority (IANA).

FTP (FILE TRANSFER PROTOCOL)

File Transfer Protocol(FTP) is an application layer protocol which moves files between local and remote file systems. It runs on the top of TCP, like HTTP. To transfer a file, 2 TCP connections are used by FTP in parallel: control connection and data connection.



What is control connection?

For sending control information like user identification, password, commands to change the remote directory, commands to retrieve and store files, etc., FTP makes use of control connection. The control connection is initiated on port number 21.

What is data connection?

For sending the actual file, FTP makes use of data connection. A data connection is initiated on port number 20.

FTP sends the control information out-of-band as it uses a separate control connection. Some protocols send their request and response header lines and the data in the same TCP connection. For this reason, they are said to send their control information in-band. HTTP and SMTP are such examples.

FTP Session:

When a FTP session is started between a client and a server, the client initiates a control TCP connection with the server side. The client sends control information over this. When the server receives this, it initiates a data connection to the client side. Only one file can be sent over one data connection. But the control connection remains active throughout the user session. As we know HTTP is stateless i.e. it does not have to keep track of any user state. But FTP needs to maintain a state about its user throughout the session.

Data Structures: FTP allows three types of data structures:

1. **File Structure –** In file-structure there is no internal structure and the file is considered to be a continuous sequence of data bytes.
2. **Record Structure –** In record-structure the file is made up of sequential records.
3. **Page Structure –** In page-structure the file is made up of independent indexed pages.

TELNET

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

ICMP (INTERNET CONTROL MESSAGE PROTOCOL)

Since IP does not have an inbuilt mechanism for sending error and control messages. It depends on Internet Control Message Protocol(ICMP) to provide an error control. It is used for reporting errors and management queries. It is a supporting protocol and used by networks devices like routers for sending the error messages and operations information.

e.g. the requested service is not available or that a host or router could not be reached.

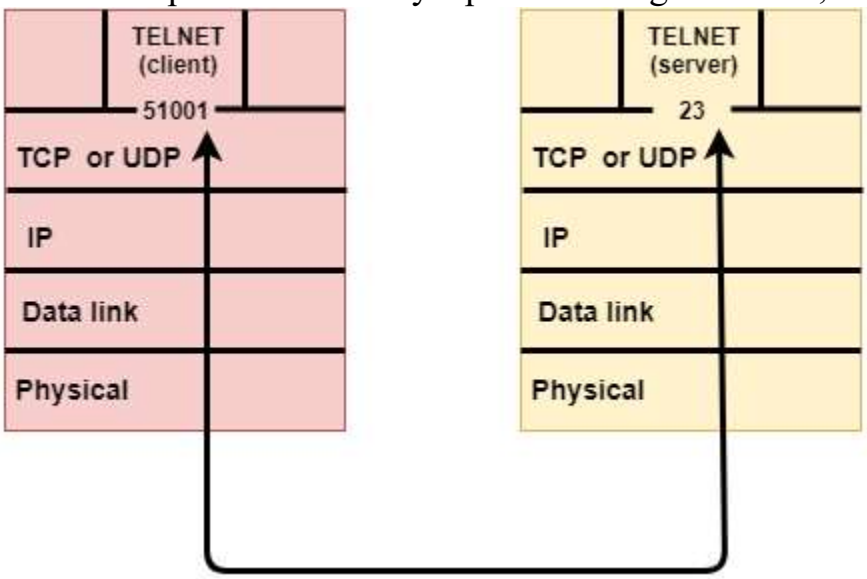
IGMP (INTERNET GROUP MANAGEMENT PROTOCOL)

IGMP is acronym for **Internet Group Management Protocol**. IGMP is a communication protocol used by hosts and adjacent routers for multicasting communication with IP networks and uses the resources efficiently to transmit the message/data packets. Multicast communication can have single or multiple senders and receivers and thus, IGMP can be used in streaming videos, gaming or web conferencing tools. This protocol is used on IPv4 networks and for using this on IPv6, multicasting is managed by Multicast Listener Discovery (MLD). Like other network protocols, IGMP is used on network layer. MLDv1 is almost same in functioning as

IGMPv2 and MLDv2 is almost similar to IGMPv3.

Transport Layer protocols

- The transport layer is represented by two protocols: TCP and UDP.
- The IP protocol in the network layer delivers a datagram from a source host to the destination host.
- Nowadays, the operating system supports multiuser and multiprocessing environments, an executing program is called a process. When a host sends a message to other host means that source process is sending a process to a destination process. The transport layer protocols define some connections to individual ports known as protocol ports.
- An IP protocol is a host-to-host protocol used to deliver a packet from source host to the destination host while transport layer protocols are port-to-port protocols that work on the top of the IP protocols to deliver the packet from the originating port to the IP services, and from IP services to the destination port.
- Each port is defined by a positive integer address, and it is of 16 bits.



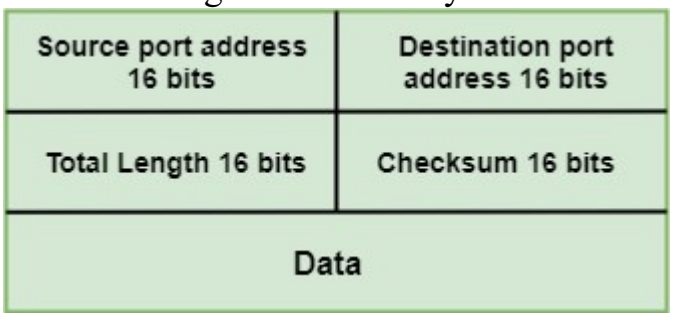
UDP

- UDP stands for **User Datagram Protocol**.
- UDP is a simple protocol and it provides non sequenced transport functionality.
- UDP is a connectionless protocol.
- This type of protocol is used when reliability and security are less important than speed and size.

- UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.
- The packet produced by the UDP protocol is known as a user datagram.

User Datagram Format

The user datagram has a 16-byte header which is shown below:



Where,

- **Source port address:** It defines the address of the application process that has delivered a message. The source port address is of 16 bits address.
- **Destination port address:** It defines the address of the application process that will receive the message. The destination port address is of a 16-bit address.
- **Total length:** It defines the total length of the user datagram in bytes. It is a 16-bit field.
- **Checksum:** The checksum is a 16-bit field which is used in error detection.

Disadvantages of UDP protocol

- UDP provides basic functions needed for the end-to-end delivery of a transmission.
- It does not provide any sequencing or reordering functions and does not specify the damaged packet when reporting an error.
- UDP can discover that an error has occurred, but it does not specify which packet has been lost as it does not contain an ID or sequencing number of a particular data segment.

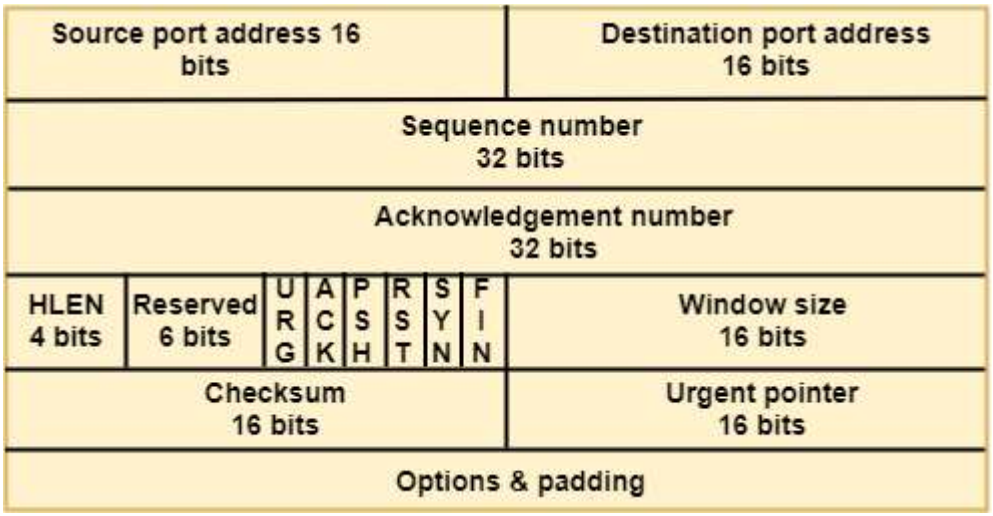
TCP

- TCP stands for Transmission Control Protocol.
- It provides full transport layer services to applications.
- It is a connection-oriented protocol means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.

Features of TCP protocol

- **Stream data transfer:** TCP protocol transfers the data in the form of contiguous stream of bytes. TCP group the bytes in the form of TCP segments and then passed it to the IP layer for transmission to the destination. TCP itself segments the data and forward to the IP.
- **Reliability:** TCP assigns a sequence number to each byte transmitted and expects a positive acknowledgement from the receiving TCP. If ACK is not received within a timeout interval, then the data is retransmitted to the destination.
  The receiving TCP uses the sequence number to reassemble the segments if they arrive out of order or to eliminate the duplicate segments.
- **Flow Control:** When receiving TCP sends an acknowledgement back to the sender indicating the number the bytes it can receive without overflowing its internal buffer. The number of bytes is sent in ACK in the form of the highest sequence number that it can receive without any problem. This mechanism is also referred to as a window mechanism.
- **Multiplexing:** Multiplexing is a process of accepting the data from different applications and forwarding to the different applications on different computers. At the receiving end, the data is forwarded to the correct application. This process is known as demultiplexing. TCP transmits the packet to the correct application by using the logical channels known as ports.
- **Logical Connections:** The combination of sockets, sequence numbers, and window sizes, is called a logical connection. Each connection is identified by the pair of sockets used by sending and receiving processes.
- **Full Duplex:** TCP provides Full Duplex service, i.e., the data flow in both the directions at the same time. To achieve Full Duplex service, each TCP should have sending and receiving buffers so that the segments can flow in both the directions. TCP is a connection-oriented protocol. Suppose the process A wants to send and receive the data from process B. The following steps occur:
  - Establish a connection between two TCPs.
  - Data is exchanged in both the directions.
  - The Connection is terminated.

TCP Segment Format



Where,

- **Source port address:** It is used to define the address of the application program in a source computer. It is a 16-bit field.
- **Destination port address:** It is used to define the address of the application program in a destination computer. It is a 16-bit field.
- **Sequence number:** A stream of data is divided into two or more TCP segments. The 32-bit sequence number field represents the position of the data in an original data stream.
- **Acknowledgement number:** A 32-field acknowledgement number acknowledge the data from other communicating devices. If ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive.
- **Header Length (HLEN):** It specifies the size of the TCP header in 32-bit words. The minimum size of the header is 5 words, and the maximum size of the header is 15 words. Therefore, the maximum size of the TCP header is 60 bytes, and the minimum size of the TCP header is 20 bytes.
- **Reserved:** It is a six-bit field which is reserved for future use.
- **Control bits:** Each bit of a control field functions individually and independently. A control bit defines the use of a segment or serves as a validity check for other fields.

There are total six types of flags in control field:

- **URG:** The URG field indicates that the data in a segment is urgent.
- **ACK:** When ACK field is set, then it validates the acknowledgement number.
- **PSH:** The PSH field is used to inform the sender that higher throughput is needed so if possible, data must be pushed with higher throughput.
- **RST:** The reset bit is used to reset the TCP connection when there is any confusion occurs in the sequence numbers.

- **SYN:** The SYN field is used to synchronize the sequence numbers in three types of segments: connection request, connection confirmation (with the ACK bit set), and confirmation acknowledgement.
- **FIN:** The FIN field is used to inform the receiving TCP module that the sender has finished sending data. It is used in connection termination in three types of segments: termination request, termination confirmation, and acknowledgement of termination confirmation.
    - **Window Size:** The window is a 16-bit field that defines the size of the window.
    - **Checksum:** The checksum is a 16-bit field used in error detection.
    - **Urgent pointer:** If URG flag is set to 1, then this 16-bit field is an offset from the sequence number indicating that it is a last urgent data byte.
    - **Options and padding:** It defines the optional fields that convey the additional information to the receiver.

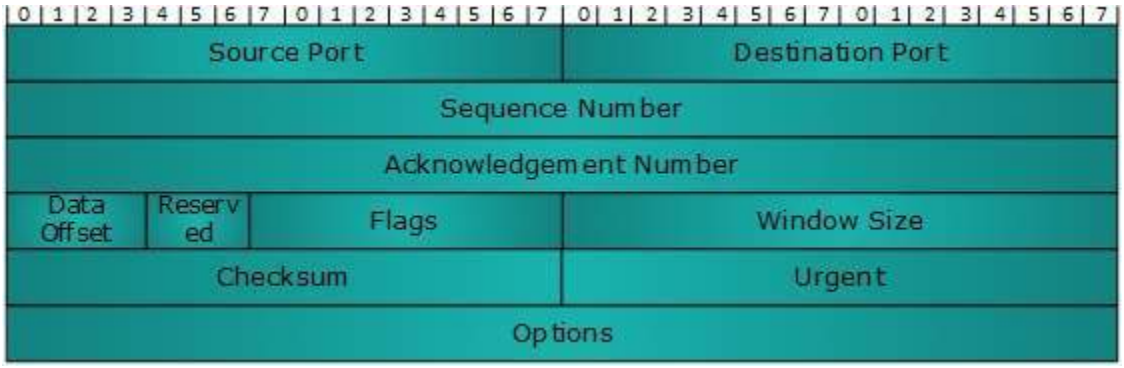
Differences b/w TCP & UDP

Basis for Comparison	TCP	UDP
Definition	TCP establishes a virtual circuit before transmitting the data.	UDP transmits the data directly to the destination computer without verifying whether the receiver is ready to receive or not.
Connection Type	It is a Connection-Oriented protocol	It is a Connectionless protocol
Speed	Slow	high
Reliability	It is a reliable protocol.	It is an unreliable protocol.
Header size	20 bytes	8 bytes
acknowledgement	It waits for the acknowledgement of data and has the ability to resend the lost	It neither takes the acknowledgement, nor does it retransmit the damaged frame.

	packets.	

Header

The length of TCP header is minimum 20 bytes long and maximum 60 bytes.



- **Source Port (16-bits)** - It identifies source port of the application process on the sending device.
- **Destination Port (16-bits)** - It identifies destination port of the application process on the receiving device.
- **Sequence Number (32-bits)** - Sequence number of data bytes of a segment in a session.
- **Acknowledgement Number (32-bits)** - When ACK flag is set, this number contains the next sequence number of the data byte expected and works as acknowledgement of the previous data received.
- **Data Offset (4-bits)** - This field implies both, the size of TCP header (32-bit words) and the offset of data in current packet in the whole TCP segment.
- **Reserved (3-bits)** - Reserved for future use and all are set zero by default.
- **Flags (1-bit each)**
    - **NS** - Nonce Sum bit is used by Explicit Congestion Notification signaling process.
    - **CWR** - When a host receives packet with ECE bit set, it sets Congestion Windows Reduced to acknowledge that ECE received.
    - **ECE** -It has two meanings:
        - If SYN bit is clear to 0, then ECE means that the IP packet has its CE (congestion experience) bit set.
        - If SYN bit is set to 1, ECE means that the device is ECT capable.
    - **URG** - It indicates that Urgent Pointer field has significant data and should be processed.
    - **ACK** - It indicates that Acknowledgement field has significance. If ACK is cleared to 0, it indicates that packet does not contain any acknowledgement.

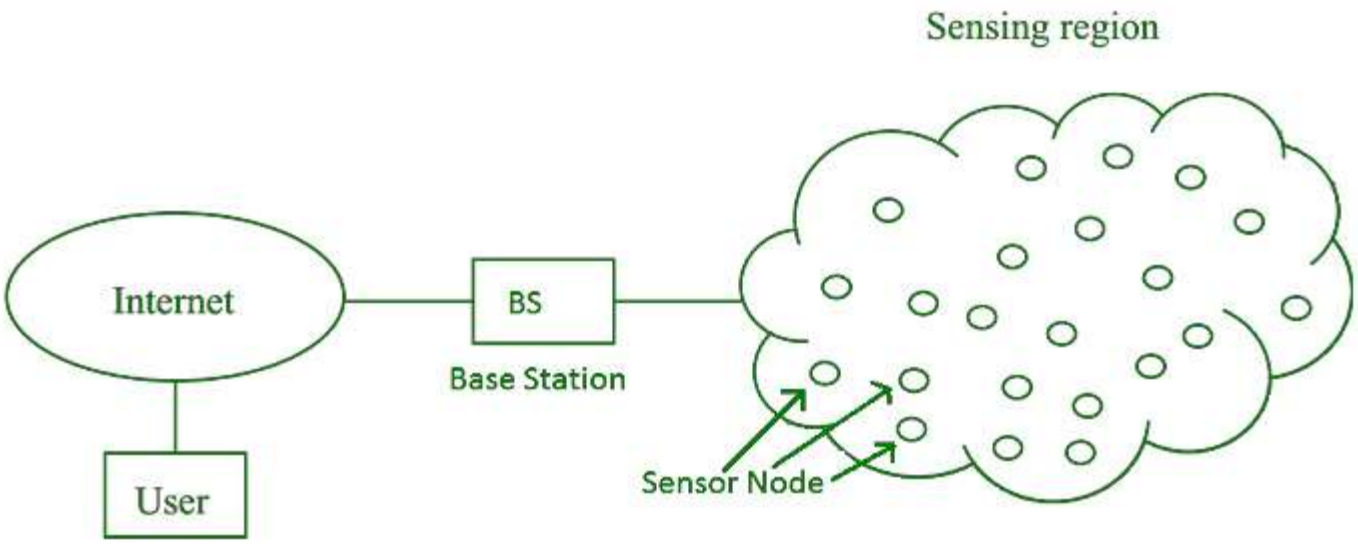
- **PSH** - When set, it is a request to the receiving station to PUSH data (as soon as it comes) to the receiving application without buffering it.
- **RST** - Reset flag has the following features:
  - It is used to refuse an incoming connection.
  - It is used to reject a segment.
  - It is used to restart a connection.
- **SYN** - This flag is used to set up a connection between hosts.
- **FIN** - This flag is used to release a connection and no more data is exchanged thereafter. Because packets with SYN and FIN flags have sequence numbers, they are processed in correct order.

- **Windows Size** - This field is used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment, i.e. how much data is the receiver expecting.
- **Checksum** - This field contains the checksum of Header, Data and Pseudo Headers.
- **Urgent Pointer** - It points to the urgent data byte if URG flag is set to 1.
- **Options** - It facilitates additional options which are not covered by the regular header. Option field is always described in 32-bit words. If this field contains data less than 32-bit, padding is used to cover the remaining bits to reach 32-bit boundary.

Wireless Sensor Network (WSN)

Wireless Sensor Network (WSN) is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical or environmental conditions.
Sensor nodes are used in WSN with the onboard processor that manages and monitors the environment in a particular area. They are connected to the Base Station which acts as a processing unit in the WSN System.

Base Station in a WSN System is connected through the Internet to share data.



WSN can be used for processing, analysis, storage, and mining of the data.

Applications of WSN:

1. Internet of Things (IOT)
2. Surveillance and Monitoring for security, threat detection
3. Environmental temperature, humidity, and air pressure
4. Noise Level of the surrounding
5. Medical applications like patient monitoring
6. Agriculture
7. Landslide Detection

Challenges of WSN:

1. Quality of Service
2. Security Issue
3. Energy Efficiency
4. Network Throughput
5. Performance
6. Ability to cope with node failure
7. Cross layer optimization
8. Scalability to large scale of deployment

Components of WSN:

1. **Sensors:**
   Sensors in WSN are used to capture the environmental variables and which is used for data acquisition. Sensor signals are converted into electrical signals.
2. **Radio Nodes:**
   It is used to receive the data produced by the Sensors and sends it to the WLAN access point. It consists of a microcontroller, transceiver, external memory, and power source.
3. **WLAN Access Point:**
   It receives the data which is sent by the Radio nodes wirelessly, generally through the internet.
4. **Evaluation Software:**
   The data received by the WLAN AcessPoing is processed by a software called as Evaluation Software for presenting the report to the users for further processing of the data which can be used for processing, analysis, storage, and mining of the data.

Wireless Adhoc Network :

A wireless ad-hoc network is a wireless network deployed without any framework or infrastructure. This incorporates wireless mesh networks, mobile ad-hoc networks, and vehicular ad-hoc networks. It's history could be traced back to the Defense Advanced Research Project Agency (DARPA) and Packet Radio Networks (PRNET) which evolved into the Survival Adaptive Radio Networks (SARNET) program. Wireless ad-hoc networks, in particular mobile ad-hoc networks (MANET), are growing very fast as they make communication simpler and progressively accessible. In any case, their conventions or protocols will in general be hard to structure due to topology dependent behavior of wireless communication, and their distributed and adaptive operations to topology dynamism. They are allowed to move self-assertively at any time. So, the network topology of MANET may change randomly and rapidly at unpredictable times. This makes routing difficult because the topology is continually changing and nodes cannot be expected to have steady data storage.

Applications:

1. Data Mining
2. Military battlefield
3. Commercial Sector
4. Personal area network or Bluetooth

Differences between Wireless Adhoc Network and Wireless Sensor Network :

WIRELESS ADHOC NETWORK	WIRELESS SENSOR NETWORK
The medium used in wireless adhoc networks is radio waves.	The medium used in wireless sensor networks are radio waves, infrared, optical media.
Application independent network is used.	Application dependent network is used.

WIRELESS ADHOC NETWORK	WIRELESS SENSOR NETWORK
Hop-to-Hop routing takes place.	Query based (data centric routing) or location based routing takes place.
It is heterogeneous in type.	It is homogeneous in type.
The traffic pattern is point-to-point.	The traffic pattern is any-to-any, many-to-one, many-to-few, one-to-many.
Wireless router is used as an inter-connecting device.	Application level gateway is used as an inter-connecting device.
The data rate is high.	The data rate is low.
Supports common services.	Supports specific applications.
Traffic triggering depends on application needs.	Triggered by sensing events.
IP address is used for addressing.	Local unique MAC address or spatial IP is used for addressing.

Unit 5. Network Security: Introductory Concepts and Terminologies

Network Security

In today's generation, communication and sharing information are the key to success. Here, the network means the interconnection of two or more computers. This networking is very beneficial in many fields like exchanging information, sharing resources such as printers and scanners, sharing software, etc. Security means protection, safety, measures taken to be safe from harm caused by others. Network security is similar. Network security means some measures taken to protect computer networking from unauthorized access and risks.

Some protection methods are used to reduce security issues.

1. **Authentication :**
   Authentication is the process of recognizing or identifying a user's identity whether it is true, real, or not. It's simply a verification of claim whether you are who you say you are or not. There are many authentication methods available nowadays like password authentication that includes using a password, physical authentication that includes the scannable card or smart card or digital certificate, biometric authentication that includes signatures and fingerprints, or visual identification, and many more.
2. **Authorization :**
   Authorization means to ensure whether you have permission to access on network or not. It's simply a verification of permission either user has access or not. Some authorization methods are ACLs (Access Control Lists), Secure objects and methods, Access control for URL's, etc.
3. **Biometric System :**
   A Biometric system is one of the most secure systems as it provides high security to the computer network. This system verifies the user's identity based on some important characteristics that are physiological and behavioral features. Physiological features include

face, eyes, fingerprints, hand. Behavioral features include voice, signature, etc.

4. **Firewall :**
   A firewall is a method of network security that prevents the computer network from users that are not authorized to have access to a network. Firewalls can either be hardware or software or both. It acts as a barrier between unauthorized Internet users and private computer networks connected to the Internet. It blocks the message, viruses, hackers if they do not have authorized access and do not meet the security criteria as per requirement. Any message entering or leaving private computer networks connected to the Internet especially Intranet pass through the firewall. Firewall than checks each message and block if found unauthorized. There are several types of firewall techniques:
   - Packet Filter
   - Application-level gateway
   - Circuit-level gateway
   - Stateful inspection firewall
   - Next-Generation Firewall (NGFW)
   - Proxy server

Network security is the security provided to a network from unauthorized access and risks. It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats.

Computer networks that are involved in regular transactions and communication within the government, individuals, or business require security. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Types of Network Security Devices

Active Devices

These security devices block the surplus traffic. Firewalls, antivirus scanning devices, and content filtering devices are the examples of such devices.

Passive Devices

These devices identify and report on unwanted traffic, for example, intrusion detection appliances.

Preventative Devices

These devices scan the networks and identify potential security problems. For example, penetration testing devices and vulnerability assessment appliances.

Unified Threat Management (UTM)

These devices serve as all-in-one security devices. Examples include firewalls, content filtering, web caching, etc.

Firewalls

A firewall is a network security system that manages and regulates the network traffic based on some protocols. A firewall establishes a barrier between a trusted internal network and the internet.

Firewalls exist both as software that run on a hardware and as hardware appliances. Firewalls that are hardware-based also provide other functions like acting as a DHCP server for that network.

Most personal computers use software-based firewalls to secure data from threats from the internet. Many routers that pass data between networks contain firewall components and conversely, many firewalls can perform basic routing functions.

Firewalls are commonly used in private networks or *intranets* to prevent unauthorized access from the internet. Every message entering or leaving the intranet goes through the firewall to be examined for

security measures.

An ideal firewall configuration consists of both hardware and software based devices. A firewall also helps in providing remote access to a private network through secure authentication certificates and logins.

Hardware and Software Firewalls

Hardware firewalls are standalone products. These are also found in broadband routers. Most hardware firewalls provide a minimum of four network ports to connect other computers. For larger networks − e.g., for business purpose − business networking firewall solutions are available.

Software firewalls are installed on your computers. A software firewall protects your computer from internet threats.

Antivirus

An antivirus is a tool that is used to detect and remove malicious software. It was originally designed to detect and remove viruses from computers.

Modern antivirus software provide protection not only from virus, but also from worms, Trojan-horses, adwares, spywares, keyloggers, etc. Some products also provide protection from malicious URLs, spam, phishing attacks, botnets, DDoS attacks, etc.

Content Filtering

Content filtering devices screen unpleasant and offensive emails or webpages. These are used as a part of firewalls in corporations as well as in personal computers. These devices generate the message "Access Denied" when someone tries to access any unauthorized web page or email.

Content is usually screened for pornographic content and also for violence- or hate-oriented content. Organizations also exclude shopping

and job related contents.

Content filtering can be divided into the following categories −

- Web filtering
- Screening of Web sites or pages
- E-mail filtering
- Screening of e-mail for spam
- Other objectionable content

Intrusion Detection Systems

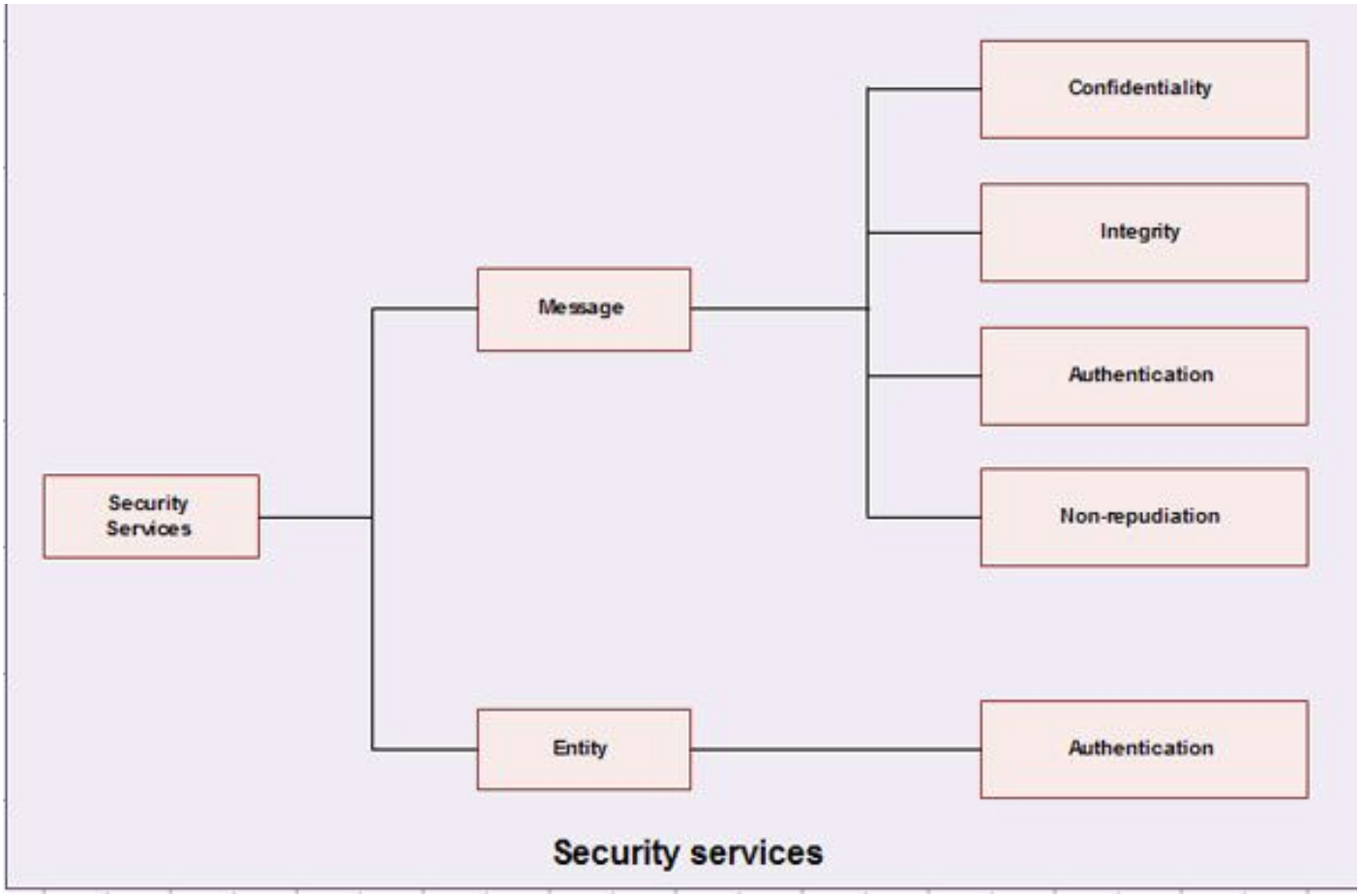
Intrusion Detection Systems, also known as Intrusion Detection and Prevention Systems, are the appliances that monitor malicious activities in a network, log information about such activities, take steps to stop them, and finally report them.

Intrusion detection systems help in sending an alarm against any malicious activity in the network, drop the packets, and reset the connection to save the IP address from any blockage. Intrusion detection systems can also perform the following actions −

- Correct Cyclic Redundancy Check (CRC) errors
- Prevent TCP sequencing issues
- Clean up unwanted transport and network layer options

Network Security Services– What is Network Security Services?

Network security can provide the following services related to a message and entity.



1. Message confidentiality

• It means that the content of a message when transmitted across a network must remain confidential, *i.e.* only the intended receiver and no one else should be able to read the message.

• The users; therefore, want to encrypt the message they send so that an eavesdropper on the network will not be able to read the contents of the message.

2. Message Integrity

• It means the data must reach the destination without any adulteration *i.e.* exactly as it was sent.

• There must be no changes during transmission, neither accidentally nor maliciously.

• Integrity of a message is ensured by attaching a checksum to the message.

• The algorithm for generating the checksum ensures that an intruder cannot alter the checksum or the message.

3. Message Authentication

• **In** message authentication the receiver needs to be .sure of the sender's identity *i.e.* the receiver has to make sure that the actual sender is the same as claimed to be.

• There are different methods to check the genuineness of the sender:

1. The two parties share a common secret code word. A party is required to show the secret code word to the other for authentication.

2. Authentication can be done by sending digital signature.

3. A trusted third party verifies the authenticity. One such way is to use digital certificates issued by a recognized certification authority.

4. Message non-reproduction

• Non-repudiation means that a sender must not be able to deny sending a message that it actually sent.

• The burden of proof falls on the receiver.

• Non-reproduction is not only in respect of the ownership of the message; the receiver must prove that the contents of the message are also the same as the sender sent.

• Non-repudiation is achieved by authentication and integrity mechanisms.

5. Entity Authentication

• In entity authentication (or user identification) the entity or user is verified prior to access to the system resources.

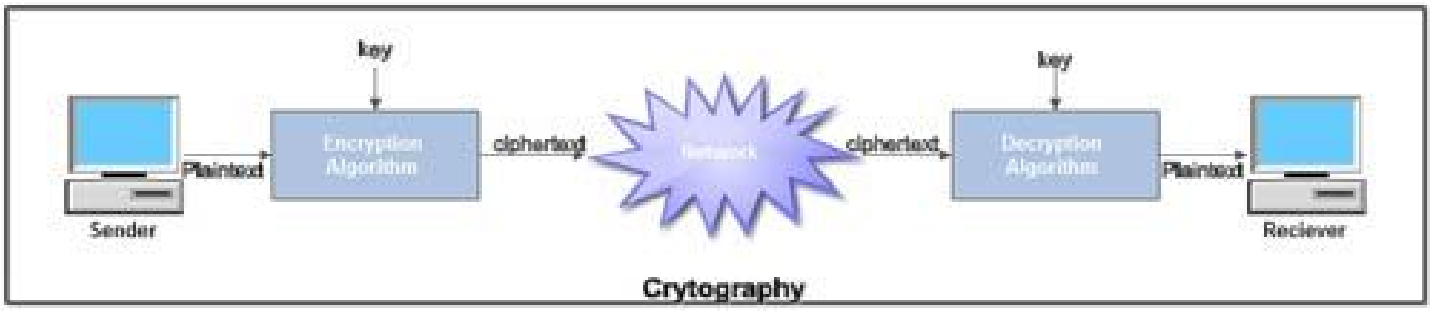
Cryptography – What is Cryptography?

• Cryptography is a technique to provide message confidentiality.

• The term **cryptography** is a Greek word which means “secret writing”.

• It is an art and science of transforming messages so as to make them secure and immune to attacks.

• Cryptography involves the process of encryption and decryption. This process is depicted.



• The terminology used in cryptography is given below:

1. **Plaintext.** The original message or data that is fed into the algorithm as input is called plaintext.

2. **Encryption algorithm**. The encryption algorithm is the algorithm that performs various substitutions and transformations on the plaintext. Encryption is the process of changing plaintext into cipher text.

3. **Ciphertext.** Ciphertext is the encrypted form the message. It is the scrambled message produced as output. It depends upon the plaintext and the key.

4. **Decryption algorithm.** The process of changing Ciphertext into plain text is known as decryption. Decryption algorithm is essentially the encryption algorithm run in reverse. It takes the Ciphertext and the key and produces the original plaintext.

5. **Key**. It also acts as input to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key. Thus a key is a number or a set of number that the algorithm uses to perform encryption and decryption.

• There are two different approaches to attack an encryption scheme:

1. Cryptanalysis

2. Brute-force attack

Cryptanalysis

• The process of attempting to discover the plaintext or key IS known as cryptanalysis.

• The strategy used by cryptanalyst depends on the nature of the encryption scheme and the information available to the cryptanalyst.

• Cryptanalyst can do any or all of six different things:

1. Attempt to break a single message.

2. Attempt to recognize patterns in encrypted messages, to be able to break subsequent ones by applying a straight forward decryption algorithm.

3. Attempt to infer some meaning without even breaking the encryption, such as noticing an unusual-frequency of communication or determining something by whether the communication was short or long.

4. Attempt to deduce the key, in order to break subsequent messages easily.

5. Attempt to find weaknesses in the implementation or environment of use encryption.

6. Attempt to find general weaknesses in an encryption algorithm without necessarily having intercepted any messages.

Brute-force attack

• This method tries every possible key on a piece of Ciphertext until an intelligible translation into plaintext is obtained.

• On an average, half of all possible keys must be tried to achieve the success.

Symmetric vs. Asymmetric Encryption – What are differences?

Information security has grown to be a colossal factor, especially with modern communication networks, leaving loopholes that could be leveraged to devastating effects. This article presents a discussion on two popular encryption schemes that can be used to tighten communication security in Symmetric and Asymmetric Encryption. In principle, the best way to commence this discussion is to start from the basics first. Thus, we look at the definitions of algorithms and key cryptographic concepts and then dive into the core part of the discussion where we present a comparison of the two techniques.

Algorithms

An algorithm is basically a procedure or a formula for solving a data snooping problem. An encryption algorithm is a set of mathematical procedure for performing encryption on data. Through the use of such an algorithm, information is made in the cipher text and requires the use of a key to transforming the data into its original form. This brings us to the concept of cryptography that has long been used in information security in communication systems.

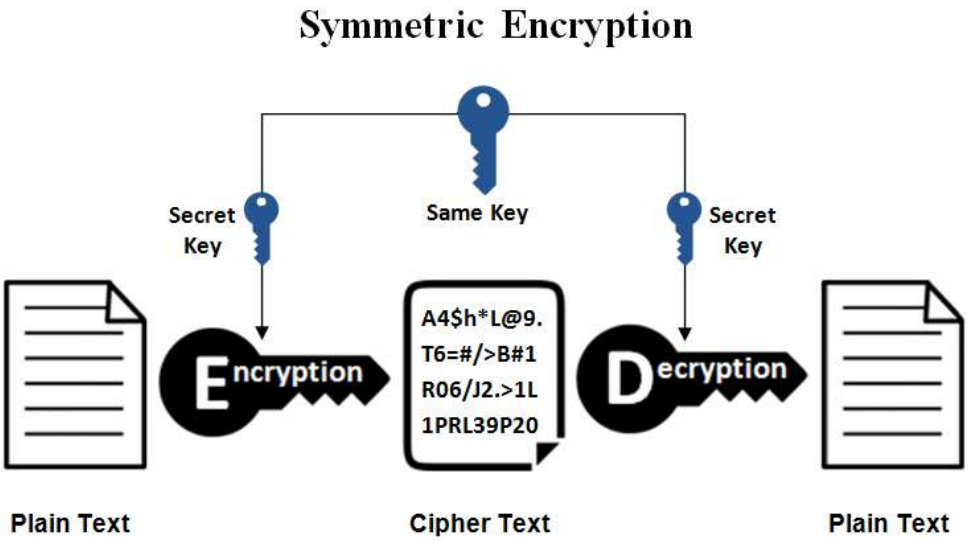
Cryptography

Cryptography is a method of using advanced mathematical principles in storing and transmitting data in a particular form so that only those whom it is intended can read and process it. Encryption is a key concept in cryptography – It is a process whereby a message is encoded in a format that cannot be read or understood by an eavesdropper. The technique is old and was first used by Caesar to encrypt his messages using Caesar cipher. A plain text from a user can be encrypted to a ciphertext, then send through a communication channel and no eavesdropper can interfere with the plain text. When it reaches the receiver end, the ciphertext is decrypted to the original plain text.

Cryptography Terms

- **Encryption**: It is the process of locking up information using cryptography. Information that has been locked this way is encrypted.
- **Decryption**: The process of unlocking the encrypted information using cryptographic techniques.
- **Key**: A secret like a password used to encrypt and decrypt information. There are a few different types of keys used in cryptography.
- **Steganography**: It is actually the science of hiding information from people who would snoop on you. The difference between steganography and encryption is that the would-be snoopers may not be able to tell there's any hidden information in the first place.

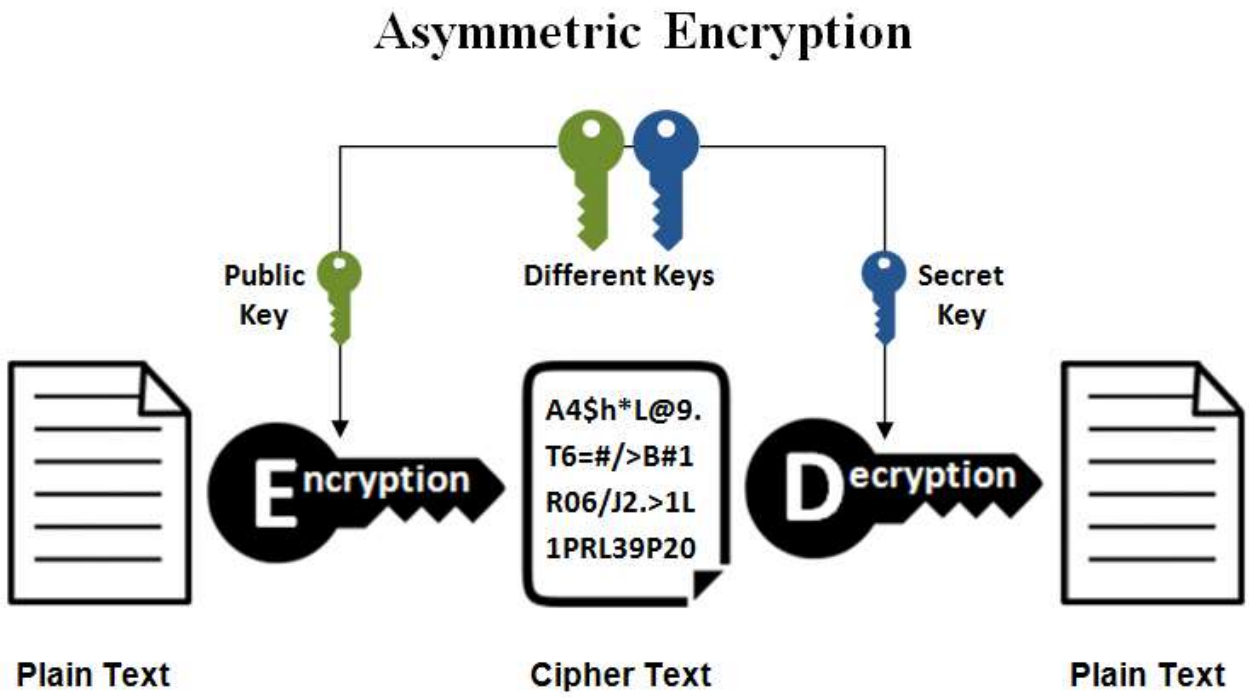
Symmetrical Encryption



This is the simplest kind of encryption that involves only one secret key to cipher and decipher information. Symmetrical encryption is an old and best-known technique. It uses a secret key that can either be a number, a word or a string of random letters. It is a blended with the plain text of a message to change the content in a particular way. The sender and the recipient should know the secret key that is used to encrypt and decrypt all the messages. Blowfish, AES, RC4, DES, RC5, and RC6 are examples of symmetric encryption. The most widely used symmetric algorithm is AES-128, AES-192, and AES-256.

The main disadvantage of the symmetric key encryption is that all parties involved have to exchange the key used to encrypt the data before they can decrypt it.

Asymmetrical Encryption



Asymmetrical encryption is also known as public key cryptography, which is a relatively new method, compared to symmetric encryption. Asymmetric encryption uses two keys to encrypt a plain text. Secret keys are exchanged over the Internet or a large network. It ensures that malicious persons do not misuse the keys. It is important to note that anyone with a secret key can decrypt the message and this is why asymmetrical encryption uses two related keys to boosting security. A public key is made freely available to anyone who might want to send you a message. The second private key is kept a secret so that you can only know.
A message that is encrypted using a public key can only be decrypted using a private key, while also, a message encrypted using a private key can be decrypted using a public key. Security of the public key is not required because it is publicly available and can be passed over the internet. Asymmetric key has a far better power in ensuring the security of information transmitted during communication.

Asymmetric encryption is mostly used in day-to-day communication channels, especially over the Internet. Popular asymmetric key encryption algorithm includes ElGamal, RSA, DSA, Elliptic curve techniques, PKCS.

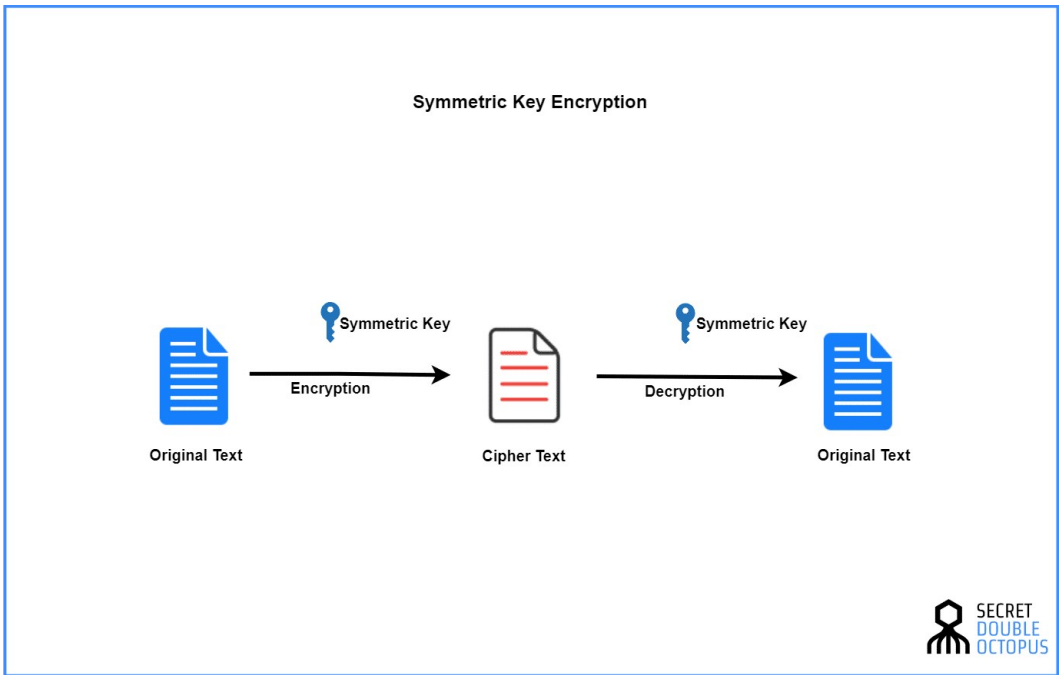
Asymmetric Encryption in Digital Certificates

To use asymmetric encryption, there must be a way of discovering public keys. One typical technique is using digital certificates in a client-server model of communication. A certificate is a package of information that identifies a user and a server. It contains information such as an organization's name, the organization that issued the certificate, the users' email address and country, and users public key.

When a server and a client require a secure encrypted communication, they send a query over the network to the other party, which sends back a copy of the certificate. The other party's public key can be extracted from the certificate. A certificate can also be used to uniquely identify the holder.

SYMMETRIC KEY ENCRYPTION	ASYMMETRIC KEY ENCRYPTION
It only requires a single key for both encryption and decryption.	It requires two key one to encrypt and the other one to decrypt.
The size of cipher text is same or smaller than the original plain text.	The size of cipher text is same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amount of data.
It only provides confidentiality.	It provides confidentiality, authenticity and non-repudiation.
Examples: 3DES, AES, DES and RC4	Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA
In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption.	In asymmetric key encryption, resource utilization is high.

SYMMETRIC KEY CRYPTOGRAPHY



Symmetric key cryptography is any cryptographic algorithm that is based on a shared key that is used to encrypt or decrypt text/cyphertext, in contract to asymmetric key cryptography, where the encryption and decryption keys are different.

Symmetric encryption is generally more efficient than asymmetric encryption and therefore preferred when large amounts of data need to be exchanged.

Establishing the shared key is difficult using only symmetric encryption algorithms, so in many cases, an asymmetric encryption is used to establish the shared key between two parties.

WHAT TYPE KEYS ARE USED IN SYMMETRIC CRYPTOGRAPHY?

Symmetric cryptography relies on one shared key that both parties know and can use to encrypt or decrypt data.

WHAT ARE THE DIFFERENCES BETWEEN ASYMMETRIC AND SYMMETRIC KEY CRYPTOGRAPHY?

Symmetric key cryptography relies on a shared key between two parties. Asymmetric key cryptography uses a public-private key pair where one key is used to encrypt and the other to decrypt.

Symmetric cryptography is more efficient and therefore more suitable for encrypting/decrypting large volumes of data. Asymmetric cryptography is not efficient and therefore used only for exchanging a shared key, after which the symmetric key is used to encrypt/decrypt data.

Asymmetric encryption is also used for creating digital signatures.

WHAT IS THE DIFFERENCE BETWEEN SYMMETRIC AND PUBLIC KEY CRYPTOGRAPHY?

Symmetric key cryptography relies on a shared key between two parties. Asymmetric key cryptography uses a public-private key pair where one key is used to encrypt and the other to decrypt.

IS AES ENCRYPTION SYMMETRIC OR ASYMMETRIC?

Yes, AES is a symmetric key cryptography.

WHICH TYPES OF ENCRYPTION DOES SYMMETRIC KEY ENCRYPTION USE?

Symmetric key encryption uses one the following encryption types:

1) **Stream ciphers:** encrypt the digits (typically bytes), or letters (in substitution ciphers) of a message one at a time

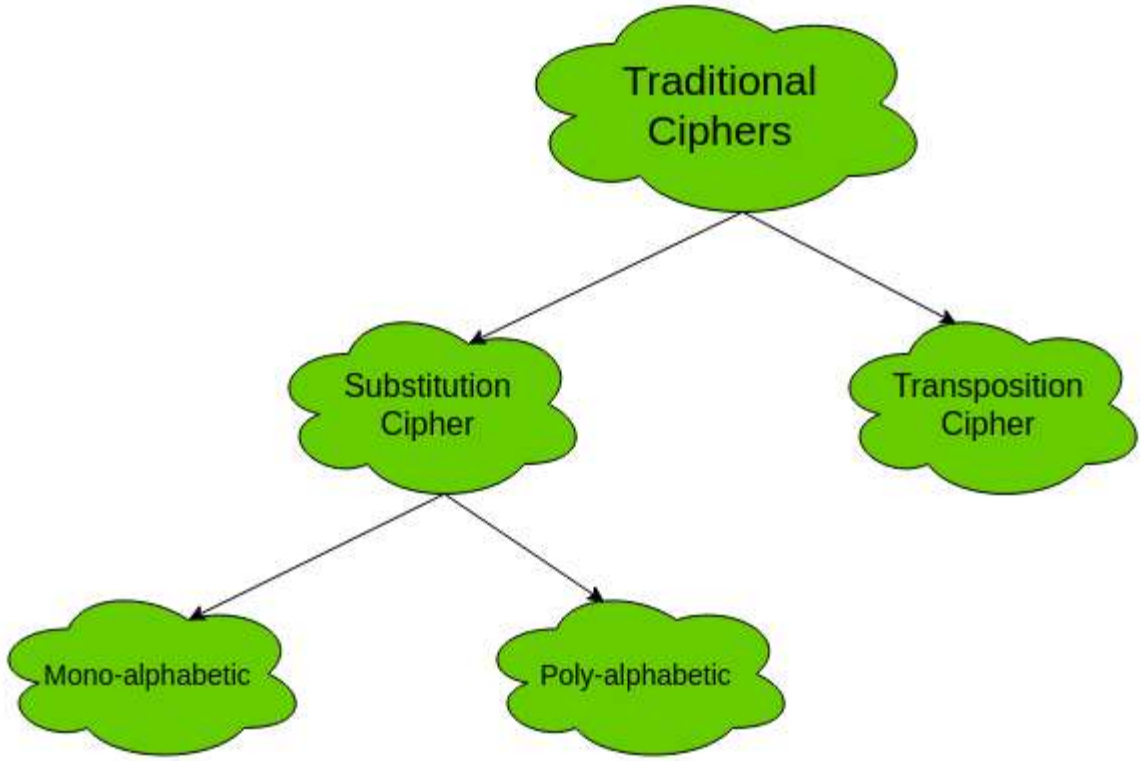
2) **Block ciphers:** encrypts a number of bits as a single unit, adding the plaintext so that it is a multiple of the block size. Blocks of 64 bits were commonly used. The Advanced Encryption Standard (AES) algorithm approved by NIST in December 2001, and the GCM block cipher mode of operation use 128-bit blocks.

WHAT ARE OTHER TERMS FOR SYMMETRIC-KEY ENCRYPTION?

secret-key, *single-key*, *shared-key*, *one-key*, and *private-key* encryption.

Traditional Symmetric Ciphers

The two types of traditional symmetric ciphers are **Substitution Cipher** and **Transposition Cipher**. The following flowchart categories the traditional ciphers:



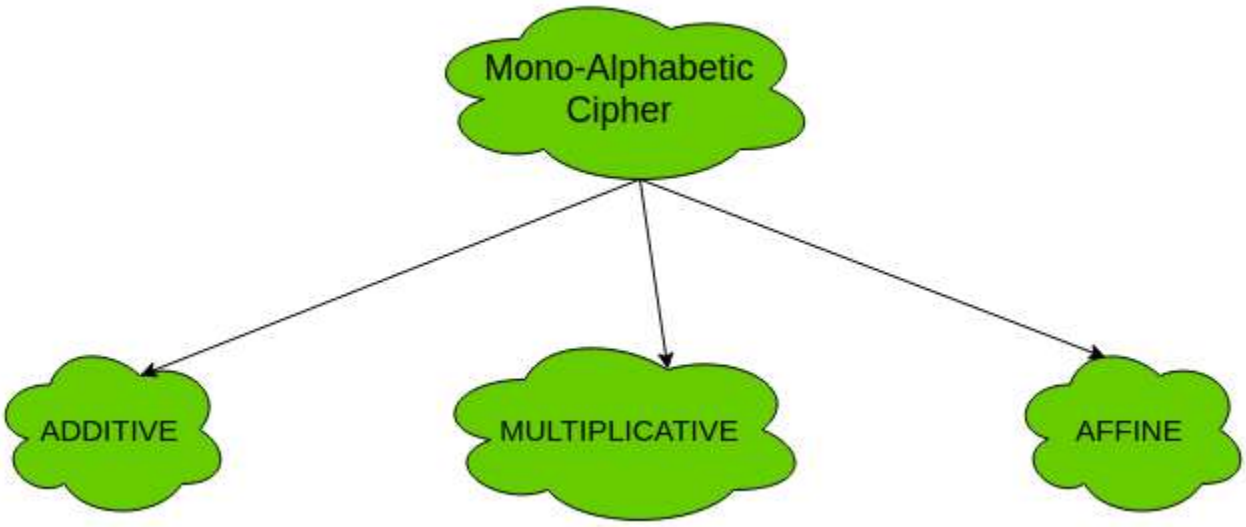
1. Substitution Cipher:
Substitution Ciphers are further divided into **Mono-alphabetic Cipher** and **Poly-alphabetic Cipher**.
First, let's study about mono-alphabetic cipher.

1. **Mono-alphabetic Cipher –**
   In mono-alphabetic ciphers, each symbol in plain-text (eg; 'o' in 'follow') is mapped to one cipher-text symbol. No matter how many times a symbol occurs in the plain-text, it will correspond to the same cipher-text symbol. For example, if the plain-text is 'follow' and the mapping is :

   - f -> g
   - o -> p
   - l -> m
   - w -> x

   The cipher-text is 'gpmmpx'.

   Types of mono-alphabetic ciphers are:



(a). Additive Cipher (Shift Cipher / Caesar Cipher) –
The simplest mono-alphabetic cipher is additive cipher. It is also referred to as 'Shift Cipher' or 'Caesar Cipher'. As the name suggests, 'addition modulus 2' operation is performed on the plain-text to obtain a cipher-text.
$C = (M + k) \bmod n$
$M = (C - k) \bmod n$

where,
C -> cipher-text
M -> message/plain-text
k -> key

The key space is 26. Thus, it is not very secure. It can be broken by brute-force attack.
For more information and implementation see Caesar Cipher
(b). Multiplicative Cipher –
The multiplicative cipher is similar to additive cipher except the fact that the key bit is multiplied to the plain-text symbol during encryption. Likewise, the cipher-text is multiplied by the multiplicative inverse of key for decryption to obtain back the plain-text.

$C = (M * k) \bmod n$
$M = (C * k^{-1}) \bmod n$
where,
k^{-1} -> multiplicative inverse of k (key)
The key space of multiplicative cipher is 12. Thus, it is also not very secure.

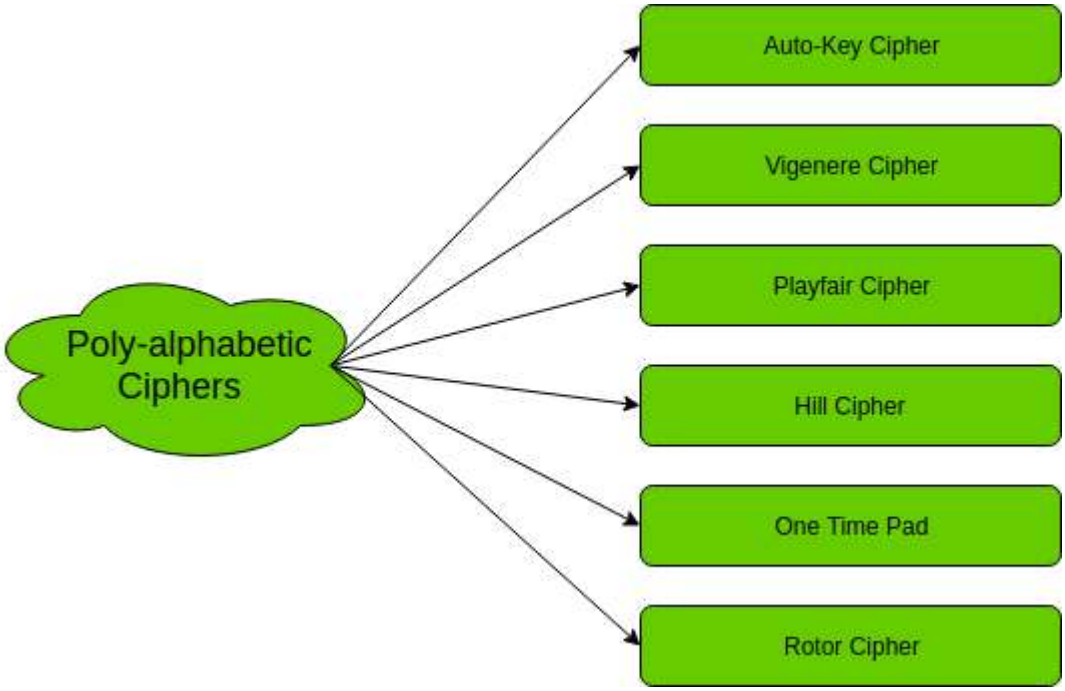
(c). Affine Cipher –
The affine cipher is a combination of additive cipher and multiplicative cipher. The key space is 26 * 12 (key space of additive * key space of multiplicative) i.e. 312. It is relatively secure than the above two as the key space is larger.
Here two keys k_1 and k_2 are used.
$C = [(M * k_1) + k_2] \bmod n$
$M = [(C - k_2) * k_1^{-1}] \bmod n$

For more information and implementation, see Affine Cipher
Now, let's study about poly-alphabetic cipher.

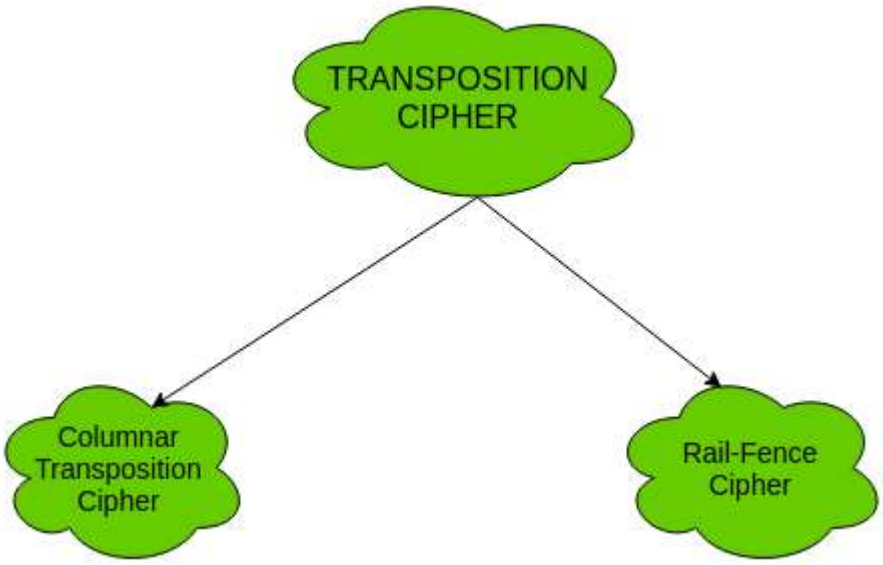
2. **Poly-alphabetic Cipher –**
In poly-alphabetic ciphers, every symbol in plain-text is mapped to a different cipher-text symbol regardless of its occurrence. Every different occurrence of a symbol has different mapping to a cipher-text. For example, in the plain-text 'follow', the mapping is :
f -> q
o -> w
l -> e
l -> r
o -> t
w -> y

Thus, the cipher text is 'qwerty'.

Types of poly-alphabetic ciphers are:



2. Transposition Cipher:
The transposition cipher does not deal with substitution of one symbol with another. It focuses on changing the position of the symbol in the plain-text. A symbol in the first position in plain-text may occur in fifth position in cipher-text.
Two of the transposition ciphers are:



1. **Columnar Transposition Cipher –**
   For information and implementation, see Columnar Transposition Cipher
2. **Rail-Fence Cipher –**
   For information and implementation, see Rail-Fence Cipher

Digital Signatures and Certificates

Encryption – Process of converting electronic data into another form, called cipher text, which cannot be easily understood by anyone except the authorized parties.This assures data security.
Decryption– Process of translating code to data.

- Message is encrypted at the sender's side using various encryption algorithms and decrypted at the receiver's end with the help of the decryption algorithms.
- When some message is to be kept secure like username, password, etc., encryption and decryption techniques are used to assure data security.

Public key– Key which is known to everyone. Ex-public key of A is 7, this information is known to everyone.
Private key– Key which is only known to the person who's private key it is.
Authentication-Authentication is any process by which a system verifies the identity of a user who wishes to access it.
Non- repudiation– Non-repudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.
Integrity– to ensure that the message was not altered during the transmission.
Message digest -The representation of text in the form of a single string of digits, created using a formula called a one way hash function. Encrypting a message digest with a private key creates a digital signature which is an electronic means of authentication..

Digital Signature
A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.

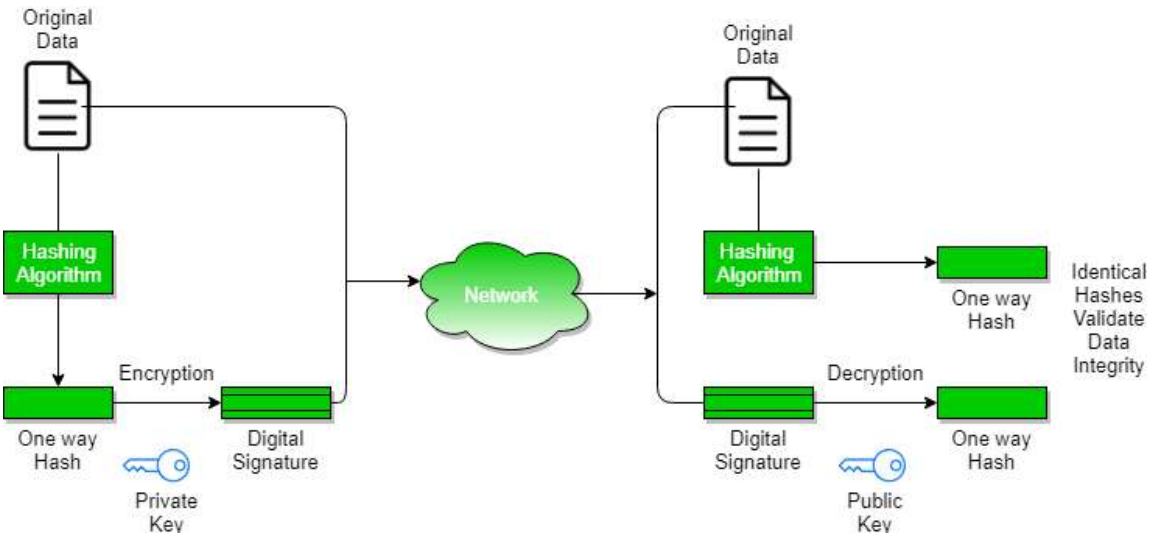
1. **Key Generation Algorithms** : Digital signature are electronic signatures, which assures that the message was sent by a particular sender. While performing digital transactions authenticity and integrity should be assured, otherwise the data can be altered or someone can also act as if he was the sender and expect a reply.
2. **Signing Algorithms**: To create a digital signature, signing algorithms like email programs create a one-way hash of the electronic data which is to be signed. The signing algorithm then encrypts the hash value using the private key (signature key). This encrypted hash along with other information like the hashing algorithm is the digital signature. This digital signature is appended with the data and sent to the verifier. The reason for encrypting the hash instead of the entire message or document is that a hash function converts any arbitrary input into a much shorter fixed length value. This saves time as now instead of signing a long message a shorter hash value has to be signed and moreover hashing is much faster than signing.
3. **Signature Verification Algorithms** : Verifier receives Digital Signature along with the data. It then uses Verification algorithm to process on the digital signature and

the public key (verification key) and generates some value. It also applies the same hash function on the received data and generates a hash value. Then the hash value and the output of the verification algorithm are compared. If they both are equal, then the digital signature is valid else it is invalid.

The steps followed in creating digital signature are :

1. Message digest is computed by applying hash function on the message and then message digest is encrypted using private key of sender to form the digital signature. (digital signature = encryption (private key of sender, message digest) and message digest = message digest algorithm(message)).
2. Digital signature is then transmitted with the message.(message + digital signature is transmitted)
3. Receiver decrypts the digital signature using the public key of sender.(This assures authenticity,as only sender has his private key so only sender can encrypt using his private key which can thus be decrypted by sender's public key).
4. The receiver now has the message digest.
5. The receiver can compute the message digest from the message (actual message is sent with the digital signature).
6. The message digest computed by receiver and the message digest (got by decryption on digital signature) need to be same for ensuring integrity.

Message digest is computed using one-way hash function, i.e. a hash function in which computation of hash value of a message is easy but computation of the message from hash value of the message is very difficult.



Digital Certificate

Digital certificate is issued by a trusted third party which proves sender's identity to the receiver and receiver's identity to the sender.

A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. Digital certificate is used to attach public key with a particular individual or an entity.

Digital certificate contains:-

1. Name of certificate holder.

2. Serial number which is used to uniquely identify a certificate, the individual or the entity identified by the certificate
3. Expiration dates.
4. Copy of certificate holder's public key.(used for decrypting messages and digital signatures)
5. Digital Signature of the certificate issuing authority.

Digital ceritifcate is also sent with the digital signature and the message.

Digital certificate vs digital signature :

Digital signature is used to verify authenticity, integrity, non-repudiation ,i.e. it is assuring that the message is sent by the known user and not modified, while digital certificate is used to verify the identity of the user, maybe sender or receiver. Thus, digital signature and certificate are different kind of things but both are used for security. Most websites use digital certificate to enhance trust of their users.

FEATURE	DIGITAL SIGNATURE	DIGITAL CERTIFICATE
Basics / Definition	Digital signature is like a fingerprint or an attachment to a digital document that ensures its authenticity and integrity.	Digital certificate is a file that ensures holder's identity and provides security.
Process / Steps	Hashed value of original message is encrypted with sender's secret key to generate the digital signature.	It is generated by CA (Certifying Authority) that involves four steps: Key Generation, Registration, Verification, Creation.
Security Services	**Authenticity** of Sender, **integrity** of the document and **non-repudiation**.	It provides security and **authenticity** of certificate holder.
Standard	It follows Digital Signature Standard (DSS).	It follows X.509 Standard Format

Public Key Infrastructure

The most distinct feature of Public Key Infrastructure (PKI) is that it uses a pair of keys to achieve the underlying security service. The key pair comprises of private key and public key.

Since the public keys are in open domain, they are likely to be abused. It is, thus, necessary to establish and maintain some kind of trusted infrastructure to manage these keys.

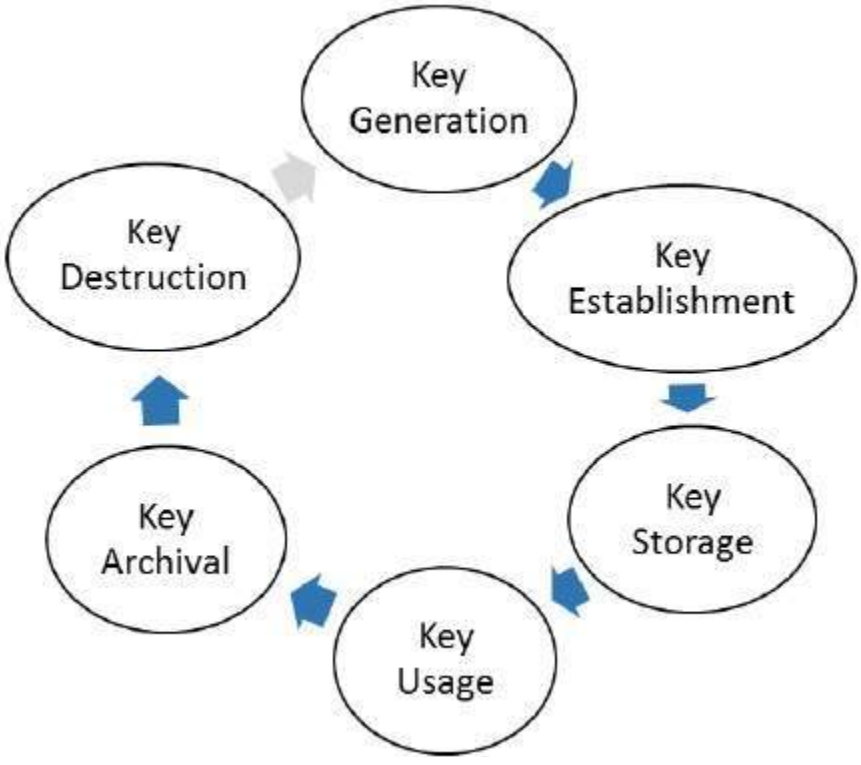
Key Management

It goes without saying that the security of any cryptosystem depends upon how securely its keys are managed. Without secure procedures for the handling of cryptographic keys, the benefits of the use of strong cryptographic schemes are potentially lost.

It is observed that cryptographic schemes are rarely compromised through weaknesses in their design. However, they are often compromised through poor key management.

There are some important aspects of key management which are as follows −

- Cryptographic keys are nothing but special pieces of data. Key management refers to the secure administration of cryptographic keys.
- Key management deals with entire key lifecycle as depicted in the following illustration −



- There are two specific requirements of key management for public key cryptography.
    - **Secrecy of private keys.** Throughout the key lifecycle, secret keys must remain secret from all parties except those who are owner and are authorized to use them.
    - **Assurance of public keys.** In public key cryptography, the public keys are in open domain and seen as public pieces of data. By default there are no assurances of whether a public key is correct, with whom it can be associated, or what it can be used for. Thus key management of public keys needs to focus much more explicitly on assurance of purpose of public keys.

The most crucial requirement of 'assurance of public key' can be achieved through the public-key infrastructure (PKI), a key management systems for supporting public-key cryptography.

Public Key Infrastructure (PKI)

PKI provides assurance of public key. It provides the identification of public keys and their distribution. An anatomy of PKI comprises of the following components.

- Public Key Certificate, commonly referred to as 'digital certificate'.
- Private Key tokens.
- Certification Authority.
- Registration Authority.
- Certificate Management System.

ENCRYPTION

Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called *cryptography*.

In computing, unencrypted data is also known as *plaintext*, and encrypted data is called *ciphertext*. The formulas used to encode and decode messages are called *encryption algorithms,* or *ciphers*.

To be effective, a cipher includes a variable as part of the algorithm. The variable, which is called a *key*, is what makes a cipher's output unique. When an encrypted message is intercepted by an unauthorized entity, the intruder has to guess which cipher the sender used to encrypt the message, as well as what keys were used as variables. The time and difficulty of guessing this information is what makes encryption such a valuable security tool.

Encryption has been a longstanding way for sensitive information to be protected. Historically, it was used by militaries and governments. In modern times, encryption is used to protect data stored on computers and storage devices, as well as data in transit over networks.

Importance of encryption

Encryption plays an important role in securing many different types of information technology (IT) assets. It provides the following:

- **Confidentiality** encodes the message's content.
- **Authentication** verifies the origin of a message.
- **Integrity** proves the contents of a message have not been changed since it was sent.

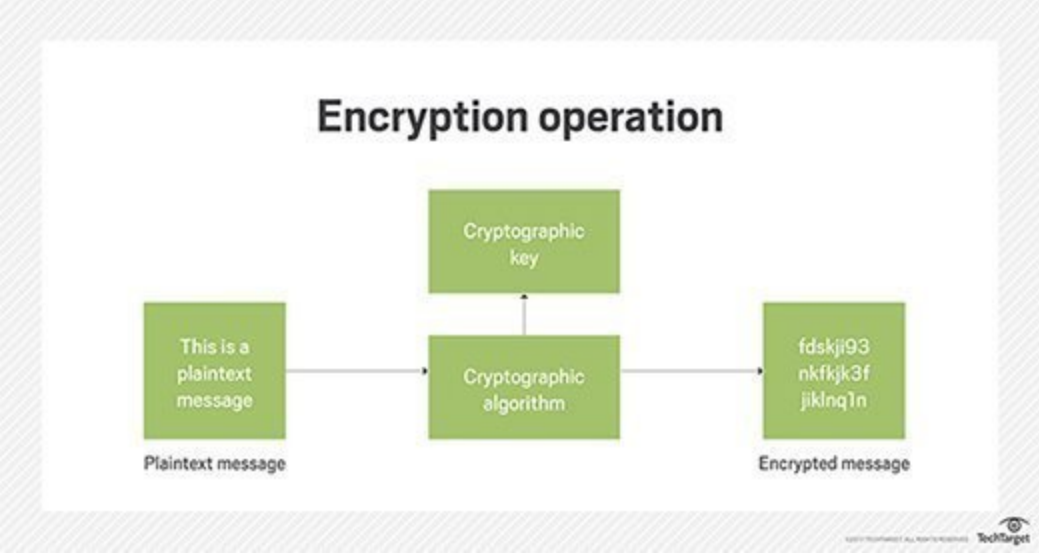
- **Nonrepudiation** prevents senders from denying they sent the encrypted message.

How is it used?

Encryption is commonly used to protect data in transit and data at rest. Every time someone uses an ATM or buys something online with a smartphone, encryption is used to protect the information being relayed. Businesses are increasingly relying on encryption to protect applications and sensitive information from reputational damage when there is a data breach.

There are three major components to any encryption system: the data, the encryption engine and the key management. In laptop encryption, all three components are running or stored in the same place: on the laptop.

In application architectures, however, the three components usually run or are stored in separate places to reduce the chance that compromise of any single component could result in compromise of the entire system.



How

Benefits of encryption

The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted over the internet or any other computer network.

In addition to security, the adoption of encryption is often driven by the need to meet compliance regulations. A number of organizations and standards bodies either recommend or require sensitive data to be encrypted in order to prevent unauthorized third parties or threat actors from accessing the data. For example, the Payment Card Industry Data Security Standard (PCI DSS) requires merchants to encrypt customers' payment card data when it is both stored at rest and transmitted across public networks.

Disadvantages of encryption

While encryption is designed to keep unauthorized entities from being able to understand the data they have acquired, in some situations, encryption can keep the data's owner from being able to access the data as well.

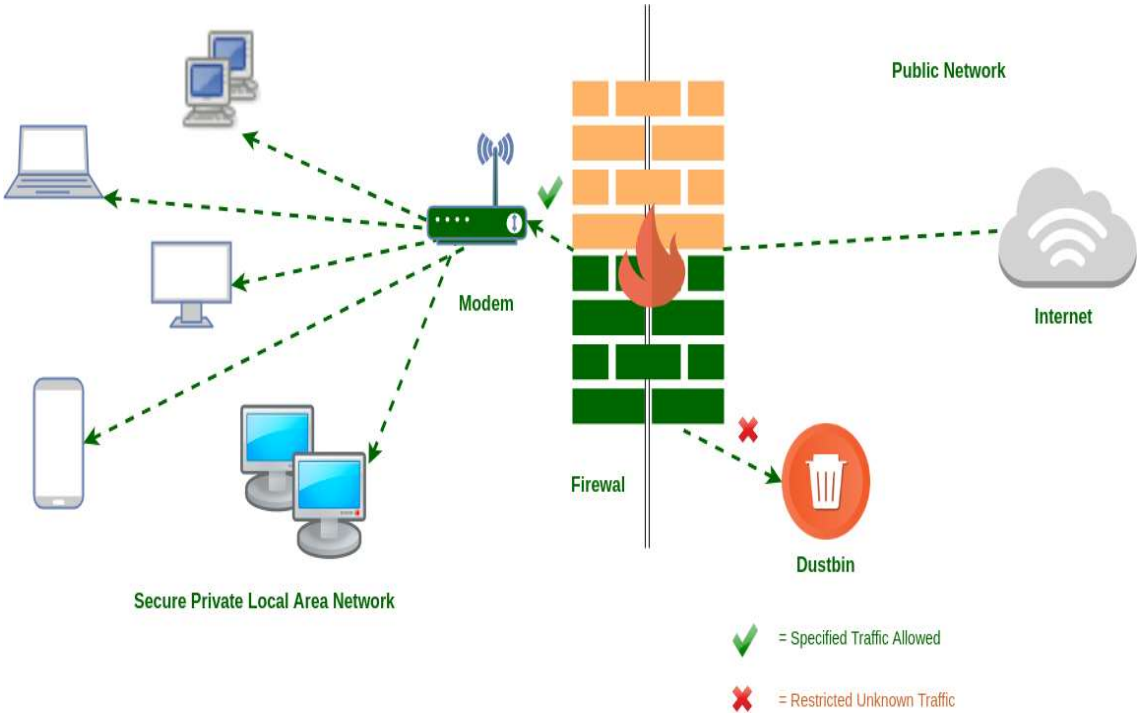
Key management is one of the biggest challenges of building an enterprise encryption strategy because the keys to decrypt the cipher text have to be living somewhere in the environment, and attackers often have a pretty good idea of where to look.

There are plenty of best practices for encryption key management. It's just that key management adds extra layers of complexity to the backup and restoration process. If a major disaster should strike, the process of retrieving the keys and adding them to a new backup server could increase the time that it takes to get started with the recovery operation.

Having a key management system in place isn't enough. Administrators must come up with a comprehensive plan for protecting the key management system. Typically, this means backing it up separately from everything else and storing those backups in a way that makes it easy to retrieve the keys in the event of a large-scale disaster.

FIREWALL

A firewall **is an essential part of your business' security system. Without it, your network is** open to threats**. A firewall keeps destructive and disruptive forces out, and controls the incoming and outgoing network traffic based on security parameters that you can control and refine.**



Firewalls majorly reduce risk for your business. A firewall could be the difference between your business succumbing to a cyber-attack, and you losing all of your data, and the attack being easily deflected and your business continuing to thrive as usual. 70% of businesses that experience a major data loss go out of business.

With a **firewall** you can completely prevent unauthorized access to your computers and network. This protects your data from being compromised. It also gives you extra protection against viruses and malware. If a firewall detects anything suspicious or malicious attempting to enter your private network from the internet, it will not allow it through.

At home, you may have a software based firewall, but your business will need a hardware based firewall to keep all unwanted traffic out of your network. You can also control what computers on your network send externally. This means that as well as blocking unwanted access, you can also control what kind of emails can be sent out from your network – which means you can prevent employees from sending business sensitive information.

Manage and control outbound traffic from your network

Your firewall can also block access within your network to specific websites. This can result in a boost to the productivity of your employees if they are spending a lot of time on distracting, non-work related websites. A firewall also prevents your employees from accessing potentially unsafe websites that could lead to your network being infected with malware.

A good firewall for businesses shouldn't result in any slow down on your computers. If you have a good IT support partner, they will configure and manage the firewall, also taking care of all the security updates.

You can also reduce the capital expenditure, and maintenance time/costs related to a firewall if you sign up to a managed firewall service. You pay a smaller, manageable monthly amount, and do not need to pay any hardware costs or worry about configuring, updating or upgrading the device.

Using a firewall can protect against:

- ***Remote Login***

  Unauthorized connections from users on the internet can allow them to remotely login and control the computer, stealing information or installing unwanted programs and spyware.

- ***Email session hijacking***

  Unauthorised access can result in hijacking of your SMTP server, which means that spam could be sent to your contacts, via your email server – making the true source of the spam difficult to trace, and damaging your reputation and relationships.

- ***Application and Operating System backdoor vulnerabilities***

  Certain programs have remote access features or bugs that allow hidden access, giving some level of control of the program.

- ***Denial of Service***

This is a disruptive attack on a server, where the server receives a request to connect. When the server attempts to respond, it can't find the system that made the request. Repeatedly hitting servers with these types of connections slows them down massively and causes them to crash.

- ***Email Bombs***

  Similar to the above, an email bomb is the same message sent to an address on a server so many times that it crashes the server.

- ***Malicious Macros***

  A macro is a script you can create that is run by an application. Hackers can create macros that tell your applications to do things that you don't want them to do, such as delete data or crash the computer.

- ***Viruses***

  Viruses are well known and well documented. They can spread very quickly through networks and emails, and often carry out unwanted activity on your computer such as monitoring your activity, slowing your computer down considerably, deleting data, locking the device completely, or crashing the computer.

What is a firewall and do you need one?

A firewall is a security device — computer hardware or software — that can help protect your network by filtering traffic and blocking outsiders from gaining unauthorized access to the private data on your computer.

Not only does a firewall block unwanted traffic, it can also help block malicious software from infecting your computer.

Firewalls can provide different levels of protection. They key is determining how much protection you need.

Firewalls are part of your network security

Firewalls represent a first line of defense in home network security.

Your home network is only as secure as its least protected device. That's where a network security system comes in.

A firewall shouldn't be your only consideration for securing your home network. It's important to make sure all of your internet-enabled devices — including mobile devices — have the latest operating system, web browsers, and security software.

Another consideration? Securing your wireless router. This might include changing the name of your router from the default ID and password it came with from the manufacturer, reviewing your security options, and setting up a guest network for visitors to your home.

What does a firewall do?

A firewall acts as a gatekeeper. It monitors attempts to gain access to your operating system and blocks unwanted traffic or unrecognized sources.

A firewall acts as a barrier or filter between your computer and another network such as the internet. You could think of a firewall as a traffic controller. It helps to protect your network and information by managing your network traffic, blocking unsolicited incoming network traffic, and validating access by assessing network traffic for anything malicious like hackers and malware.

Your operating system and your security software usually come with a pre-installed firewall. It's a good idea to make sure those features are turned on. Also, make sure your security settings are configured to run updates automatically.

How does a firewall work?

To start, a firewalled system analyzes network traffic based on rules. A firewall only welcomes those incoming connections that it has been configured to accept. It does this by allowing or blocking specific data packets — units of communication you send over digital networks — based on pre-established security rules.

A firewall works like a traffic guard at your computer's entry point, or port. Only trusted sources, or IP addresses, are allowed in. IP addresses are important because they identify a computer or source, just like your postal address identifies where you live.

Types of firewall and possible attacks

Firewall is considered as an essential element to achieve network security for the following reasons −

- Internal network and hosts are unlikely to be properly secured.
- Internet is a dangerous place with criminals, users from competing companies, disgruntled ex-employees, spies from unfriendly countries, vandals, etc.

- To prevent an attacker from launching denial of service attacks on network resource.
- To prevent illegal modification/access to internal data by an outsider attacker.

Types of Firewalls:

1. **Packet Filters –**
   It works in the **network layer** of the OSI Model. It applies a set of rules (based on the contents of IP and transport header fields) on each packet and based on the outcome, decides to either forward or discard the packet.
   For example, a rule could specify to block all incoming traffic from a certain IP address or disallow all traffic that uses UDP protocol. If there is no match with any predefined rules, it will take default action. The default action can be to 'discard all packets' or to 'accept all packets'.

   Security threats to Packet Filters:
   1. **IP address Spoofing:**
      In this kind of attack, an intruder from the outside tries to send a packet towards the internal corporate network with the source IP address set equal to one of the IP address of internal users.
      Prevention:
      Firewall can defeat this attack if it discards all the packets that arrive at the incoming side of the firewall, with source IP equal to one of the internal IPs.
   2. **Source Routing Attacks:**
      In this kind of attack, the attacker specifies the route to be taken by the packet with a hope to fool the firewall.
      Prevention:
      Firewall can defeat this attack if it discards all the packets that use the option of source routing aka path addressing.
   3. **Tiny Fragment Attacks:**
      Many times, the size of the IP packet is greater than the maximum size allowed by the underlying network such as Ethernet, Token Ring etc. In such cases, the packet needs to be fragmented, so that it can be carried further. The attacker uses this characteristic of TCP/IP protocol. In this kind of attack, the attackers intentionally create fragments of the original packet and send it to fool the firewall.
      Prevention:
      Firewall can defeat this attack if it discards all the packets which use the TCP protocol and is fragmented. *Dynamic Packet Filters* allow incoming TCP packets only if they are responses to the outgoing TCP packets.
2. **Application Gateways /Proxy Firewall –**
   It is also known as **Proxy server**. It works as follows:
   1. **Step-1:** User contacts the application gateway using a TCP/IP application such as HTTP.
   2. **Step-2:** The application gateway asks about the remote host with which the user wants to establish a connection. It also asks for the user id and password that is required to access the services of the application gateway.

3. **Step-3:** After verifying the authenticity of the user, the application gateway accesses the remote host on behalf of the user to deliver the packets.

Advantages of Using a Firewall

A Company network or a home computer will have number of advantages when using a firewall.

They are more cost effective than securing each computer in the corporate network since there are often only one or a few firewall systems to concentrate on.

There are some firewalls which are able to detect viruses, Trojans, worms and spyware etc.

There are

Disadvantages of Using a Firewall

Even if a firewall helps in keeping the network safe from intruders, but if a firewall is not used properly it would give a false impression to you that the network is safe. The main disadvantage of a firewall is that it cannot protect the network from attacks from the inside.

They often cannot protect against an insider attack.

Firewalls cannot protect a network or pc from viruses, Trojans, worms and spyware which spread through flash drives, potable hard disk and floppy etc.

They may restrict authorized users from accessing valuable services.

They do not protect against backdoor attacks.

They cannot protect the network if someone uses a broadband modem to access the internet.