Chapter 1 - Internet Basics

Computer network

Introduction to Computer Network

- Computer networks are required for sharing information when we communicate, we are sharing information. This sharing can be local or remote. Between individuals, local communication usually occurs face to face, while remote communication takes place over distance.

- The term **Data communications** means the exchange of data between two devices via some form of transmission medium such as a wire cable where as the term telecommunication, which includes telephony, telegraphy and television means communication at a distance.

- A data communications system has five components:

- **1. Message:** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

- **2. Sender:** The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

- **3. Receiver:** The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

- **4. Transmission medium:** The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

- **5. Protocol:** A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just-as a person speaking French cannot be understood by a person who speaks only Japanese.

What is a Computer Network?

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

or

- “A computer network is defined to be an interconnected collection of autonomous computers”

- Interconnected means capable of exchanging information, and autonomous means, that is independent or self governing. The connections allow users to exchange data, and pool and share resources, including Printer, Data, and Computing Power.

- In contrast to Computer Networks, where the existence of several separate machines is usually hidden from the user, distributed systems are computer networks with special software that makes the existence of several computers visible to the user.

Types of Computer Networks

- Computer Networks can be of following types:
  - Local Area Network (LAN)
  - Metropolitan Area Network (MAN)
  - Wide Area Network (WAN)
  - Personal Area Network (PAN)

Personal Area Network (PAN)

- PAN is a computer network formed around a person. It generally consists of a computer, mobile, or personal digital assistant. It is mostly personal devices network equipped within a limited area. Allows us to handle the interconnection of IT devices at the surrounding of a single user. It can be wirelessly connected to the internet called WPAN.

Advantages of PAN

- PAN networks are relatively secure and safe
- It offers only short-range solution up to ten meters

Disadvantages of PAN

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

Local Area Network (LAN)

- It is also called LAN and designed for small physical areas such as an office, gr oup of buildings or a factory.
- LAN can be a simple network like connecting two computers, to share files and network among each other while it can also be as complex as interconnecting an entire building.

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

Advantages of LAN

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

Disadvantages of LAN

- **High Setup Cost:** Although the LAN will save cost over time due to shared computer resources, but the initial setup costs of installing Local Area Networks is high.
- **Data Security Threat:** Unauthorized users can access important data of an organization if centralized data repository is not secured properly by the LAN administrator.
- **Covers Limited Area:** Local Area Network covers a small area like one office, one building or a group of nearby buildings.

Metropolitan Area Network (MAN)

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

Advantages of MAN

- Extremely efficient and provide fast communication via high-speed carriers, such as fibre optic cables.
- It provides a good back bone for large network and provides greater access to WANs.
- A MAN usually encompasses several blocks of a city or an entire city.

Disadvantages of MAN

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

Wide Area Network (WAN)

- It is also called WAN. WAN can be private or it can be public leased network. It is used for the network that covers large distance such as cover states of a country. It is not easy to design and maintain. Communication medium used are satellite, public telephone networks which are connected by routers.

Advantages of WAN

- Covers a large geographical area so long distance business can connect on the one network.
- Expensive things (such as printers or phone lines to the internet) can be shared by all the computers on the network without having to buy a different peripheral for each computer.
- Everyone on the network can use the same data. This avoids problems where some users may have older information than others.

Disadvantages of WAN

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

Types of Network Topology

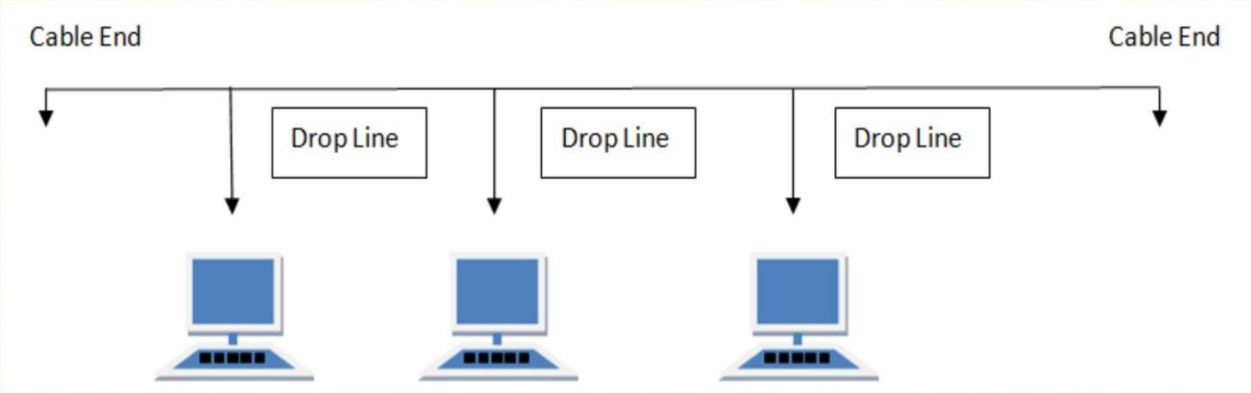
BUS Topology

- Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called Linear Bus topology.

Features of Bus Topology

- It transmits data only in one direction.

- Every device is connected to a single cable.



Advantages of Bus Topology

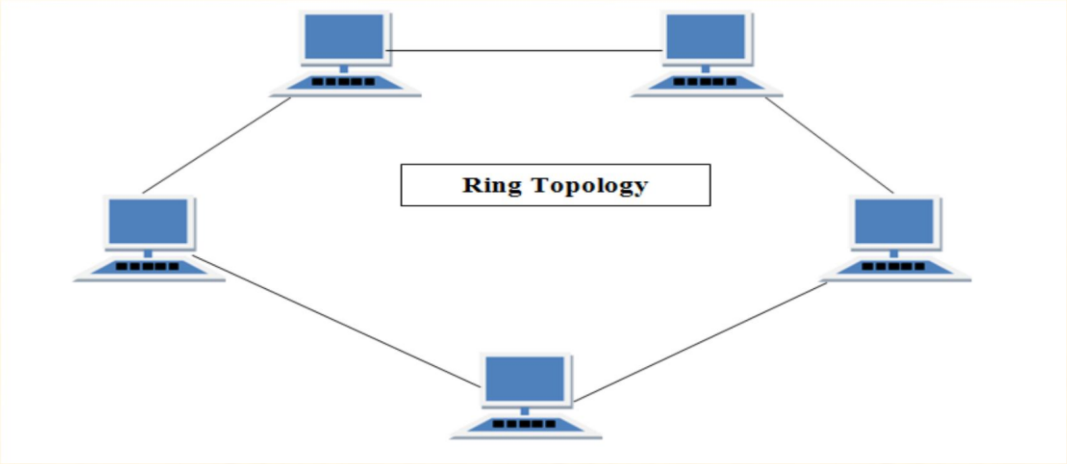
- It is cost effective.
- Cable required is least compared to other network topology.
- Used in small networks.
- It is easy to understand.
- Easy to expand joining two cables together.

Disadvantages of Bus Topology

- Cables fails then whole network fails.
- If network traffic is heavy or nodes are more the performance of the network decreases.
- Cable has a limited length.
- It is slower than the ring topology.

RING Topology

- It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbors for



each device.

Features of Ring Topology

- A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
- The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.
- In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
- Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

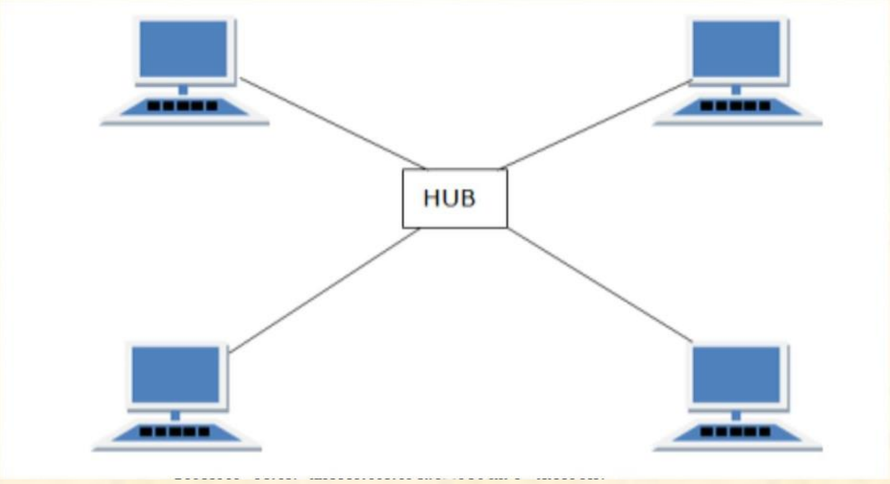
- Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
- Cheap to install and expand

Disadvantages of Ring Topology

- Troubleshooting is difficult in ring topology.
- Adding or deleting the computers disturbs the network activity.
- Failure of one computer disturbs the whole network.

STAR Topology

- In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



Features of Star Topology

- Every node has its own dedicated connection to the hub.
- Hub acts as a repeater for data flow.
- Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology

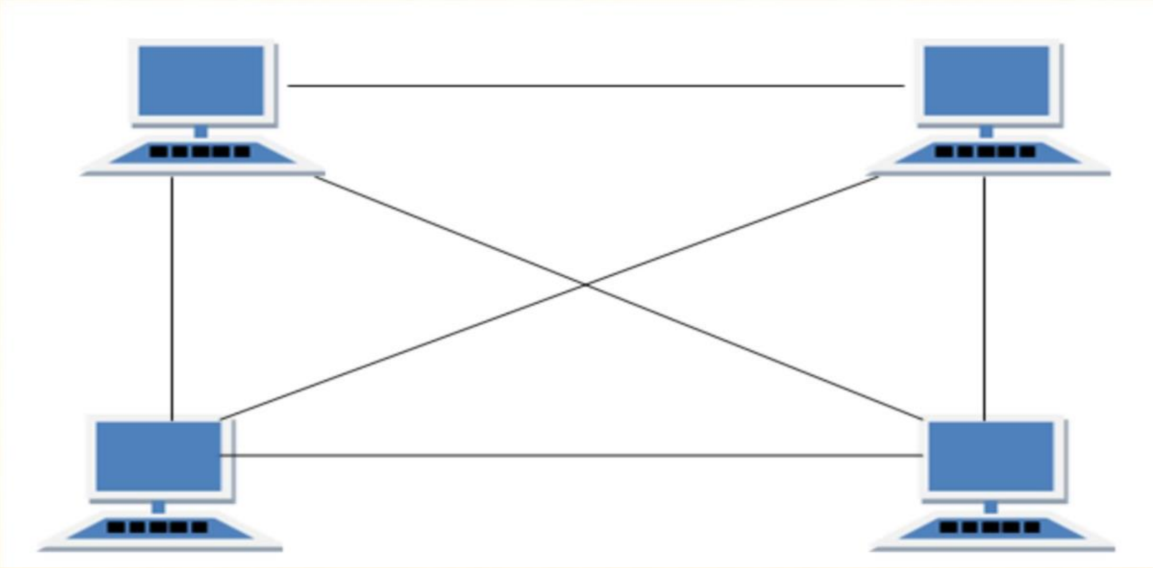
- Fast performance with few nodes and low network traffic.
- Hub can be upgraded easily.
- Easy to troubleshoot.
- Easy to setup and modify.
- Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

- Cost of installation is high.
- Expensive to use.
- If the hub fails then the whole network is stopped because all the nodes depend on the hub.
- Performance is based on the hub that is it depends on its capacity

MESH Topology

- It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices.



Types of Mesh Topology

- **1. Partial Mesh Topology:** In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
- **2. Full Mesh Topology:** Each and every nodes or devices are connected to each other.

Features of Mesh Topology

- Fully connected.
- Robust.
- Not flexible.

Advantages of Mesh Topology

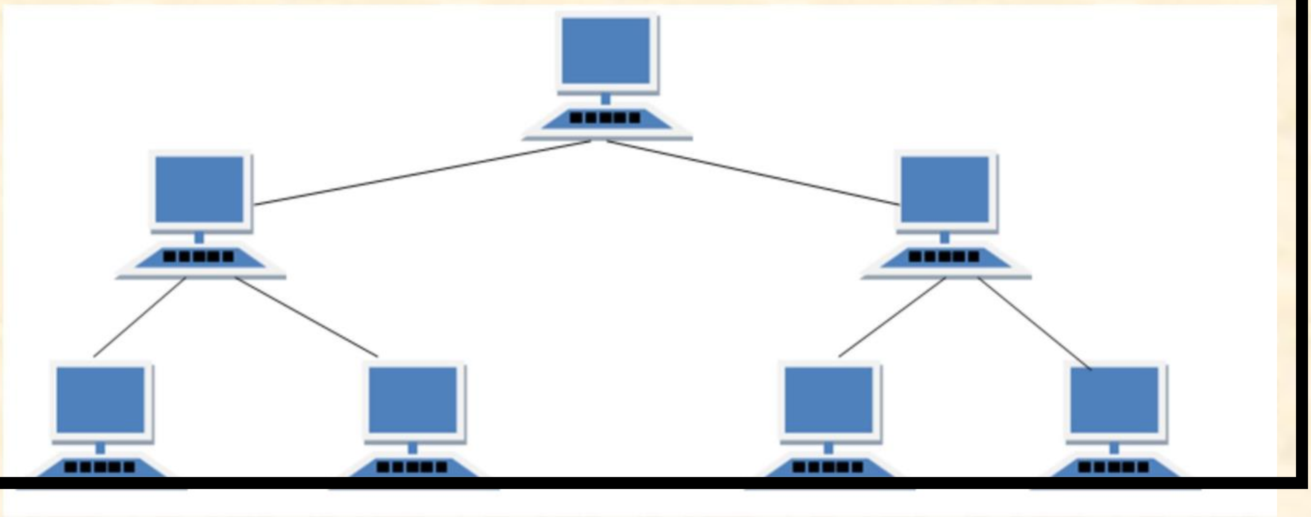
- Each connection can carry its own data load.
- It is robust.
- Fault is diagnosed easily.
- Provides security and privacy.

Disadvantages of Mesh Topology

- Installation and configuration is difficult.
- Cabling cost is more.
- Bulk wiring is required.

TREE Topology

- It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.



Features of Tree Topology

- Ideal if workstations are located in groups.
- Used in Wide Area Network.

Advantages of Tree Topology

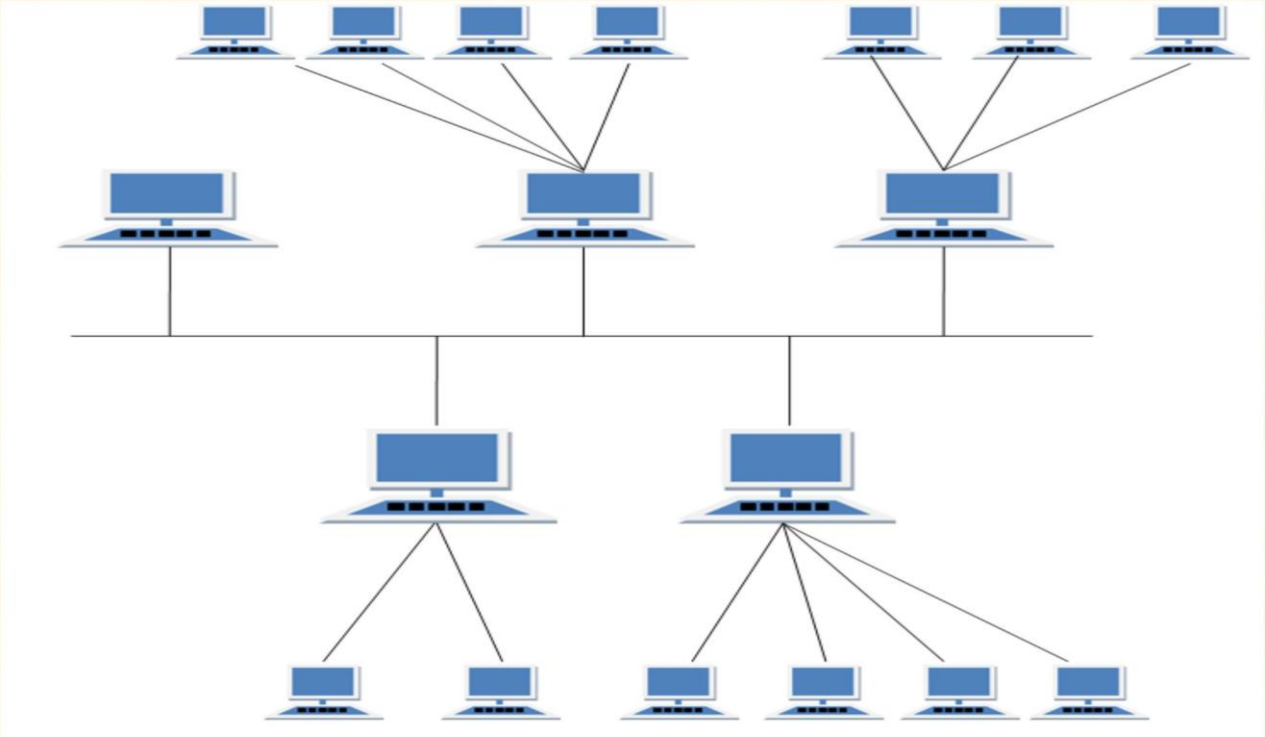
- Extension of bus and star topologies.
- Expansion of nodes is possible and easy.
- Easily managed and maintained.
- Error detection is easily done.

Disadvantages of Tree T opology

- Heavily cabled.
- Costly.
- If more nodes are added maintenance is difficult.
- Central hub fails, network fails.

HYBRID Topology

- It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).



Features of Hybrid Topology

- It is a combination of two or topologies
- Inherits the advantages and disadvantages of the topologies included

Advantages of Hybrid Topology

- Reliable as Error detecting and trouble shooting is easy.
- Effective.
- Scalable as size can be increased easily.
- Flexible.

Disadvantages of Hybrid Topology

- Complex in design.
- Costly

Concept of Internet, Intranet, Modem

Internet

What is Internet?

- The internet is a global system that uses TCP/IP protocol suite to link various types of electric devices worldwide.
- The internet is a collection of interconnected devices that are spread across the globe.
- The internet is a network of networks which consist of public, private, sales, finance, academic, business, and government networks.
- The internet is a type of network and called a network of networks.

Evolution

- The concept of Internet was originated in 1969 and has undergone several technological & Infrastructural changes as discussed below:
  - The origin of Internet devised from the concept of Advanced Research Project Agency Network (ARPANET).
  - ARPANET was developed by United States Department of Defense.
  - Basic purpose of ARPANET was to provide communication among the various bodies of government.
  - Initially, there were only four nodes, formally called Hosts.
  - In 1972, the ARPANET spread over the globe with 23 nodes located at different countries and thus became known as Internet.

- By the time, with invention of new technologies such as TCP/IP protocols, DNS, WWW, browsers, scripting languages etc., Internet provided a medium to publish and access information over the web.

Why Internet?

- The internet can be used by all, not just by scientists and engineers. As entrepreneurs, factory workers, doctors, teachers, federal employees, and citizens, people can use its technology to :
  - Create jobs, and lead towards growth.
  - Reduce health care costs while increasing the quality of services in underserved areas;
  - Deliver higher-quality, lower-cost, government services.
  - Prepare the children for the fast-paced workplace of the 21st century.
  - Build a more open and participatory democracy at all levels of government.
  - Internet enables you to know about many things just with a click, because of the internet we are able to communicate with people for away from us. It makes his feel like we are sitting next to each other.
  - It has information about everything that is known to man, and can serve various purpose bases on one's requirement.

Advantages

- The Internet is a network of computers at different locations around the world.
- Allows you to send an email message from every location
- Helps you to send or receive files between different computers
- Using the Internet, you can participate in discussion groups, such as mailing lists and newsgroups.
- It allows all small, medium, and large size businesses to sell their products with small investments.
- It makes information available worldwide
- It helps you updated with the latest news and technologies.
- It helps us meet people with the same interests as communities, forums, chats, websites, etc.

Disadvantages

- It allows everybody to speak about everything without any limitations or censorship. That could be a bad influence on impressionable minds.
- The search engines may display some fake news results.
- Internet could replace face to face collaborations and make us lose the human touch.
- Working or on the internet is surely tiring.
- The Internet makes us lazier – as for common things like search the nearest restaurant or finding the best hotel.

Applications of Internet

Now-a-days internet is being used for multiple applications. Some of them are as follows:

1. **E-mail:** E-mail is the best service offered by internet to its users. E-mail enables us to send or receive messages over internet anywhere in the world.

2. **Entertainment:** Internet is widely used for various kinds of entertainment activities like watching movies, listening music, video on demand and playing games.

3. **E-Commerce:** Many stock exchanges and banks offer almost all of their services through internet. On-line payments, accessing accounts, online shopping are very popular these days.

4. **Publicity and Advertisement:** Internet is most common medium of communication that is why internet is used by many companies for promotion and publicaity of their products.

5. **Video Conferencing:** Video conferencing uses telecommunication of audio and video to bring people of different sites together for meeting. Video conferencing may be between two individuals persons or may involve people Sitting at different sites.

6. **Product Promotion:** Internet is the cheapest means to promote own's product.

7. **Group Discussion:** A number of Newsgroups are available on the internet which allows exchanging views on topics of common interest.

8. **Software Sharing:** Many software developing organizations provides their software versions on the internet,

9. **Feedback:** Commercial organizations are using Internet together customer's satisfaction of existing products, market opportunities of new products and ideas for new produces.

10. **Online Registration:** Many universities and institutions provide training and also online enrolment forms.

11. **On-line Shopping:** On-line shopping is also becoming very popular. Many people instead of going round and wasting their precious time in shopping just, sit on the system and place the order and required stuff.

Internet Issues

Emerging technologies and especially this communications revolution we are witnessing also bring with them new issues relevant to safety, privacy, security, decency and netiquette. The issues are as follows:

1. **Safety:** Safety of information is an important issue in internet. We should be very careful to upload the information on internet.
2. **Privacy:** Don't post or write anything you wouldn't mind anyone else seeing. Remember your information is not secure nor is your e-mail necessarily private. It's supposed to be, but that isn't always the case. Also, never EVER send your credit card number via email.
3. **Security:** To enhance security, many networks have encrypted, secure transmission methods that include site certificates. Be sure you are using one of these methods if you are entering secure information, such as a credit card number at a mail-order catalog's website.
4. **Decency, Filters, Censorship:** Unfortunately this revolution in accessing information means that not all information on the Internet is suitable for everyone. While many servers maintain standards of decency and refuse to allow any indecent material on their computer network, still many others do not, or worse, some exist solely for this purpose of allowing such material. Computerized search engines that enhance our ability to find information also unfortunately make it all the more easy for children and adolescents to find information you may not want them to find.
5. **Netiquette:** All cultures and societies have standards of conduct and customs. There are many good resources for you to read online. The important thing is to take some time and read up on network etiquette so you can be a responsible, well-informed member of cyber-society.

Intranet

What is Intranet?

- An intranet is a private network which gives employees in a company the ability to organize information, manage documents, shares calendars and to-do list. It normally runs in a client/server environment in a local area network.
- In Intranet, every computer is connected via the LAN and has something known as an MAC address. It is a number that allows you to identify the place where the computer is located.

Features of Intranet

- Intranet is fast and accurate.
- Most website with large graphical images, videos, and sound, process fast on Intranet
- Your firewall protects it from external threats.
- It is easy to monitor with your organization
- Easy communication across the company from all levels
- Helps to share ideas and discussions

Elements of Corporate Intranet

- **Group collaboration:** By combining several tools on an intranet, groups can share calendars, take part in "virtual workspaces" that contain public messages and files, and log into private chat areas dedicated to specific business projects. These group collaboration features are ideal if you have employees in several branch offices that need to work together on a project.

- **Internet access:** It's not mandatory, but many companies also use their intranets to provide Web access for employees. Since the base technologies are the same, it's generally quite easy. Some all-in-one intranet servers come with built-in support for sharing a connection to an Internet service provider.
- **Security:** An intranet is generally intended for employees only - you don't want the rest of the world reading everything on it. So security is a big issue, especially if you also use you intranet to connect to the Internet. A firewall is software or hardware, or both, designed to prevent unauthorized access to your intranet by blocking outside connections.

Advantages of Intranet

- Fast, easy, low-cost to implement
- Based on open standards
- Allows connectivity with other systems
- Access to internal and external information
- Improves communication

Disadvantages of Intranet

- Threat of sharing information and the loss of control
- Unauthorized access
- Limited bandwidth for the business
- Information overload lowers productivity
- Hidden or unknown complexity and cost

Internet vs. Intranet

Apart from similarities there are some differences between the two. Following are the differences between Internet and Intranet:

Intranet	Internet
The Internet is a wide network of computers and is available to all.	Intranet is a network of computers designed for a certain group of users. Internet contains a large number of intranets. Intranet can be accessed from the Internet with specific restrictions.
Number of internet users are very high.	Number of users is limited. Internet contains various source of information. Intranet only contains group-specific information.
Anyone can access the internet	Accessible only by the organization employees or admin who have login details. It is not as safe as compared to intranet Safe and secure

	network.
It is a public network.	It is a private network.
The Internet is a wide network of computers and is available to all.	Intranet is a network of computers designed for a certain group of users. Internet contains a large number of intranets. Intranet can be accessed from the Internet with specific restrictions.

Modem

Introduction to Modem

Modem is abbreviation for Modulator – Demodulator. Modem is short for "Modulator-Demodulator." It is a hardware component that allows a computer or another device, such as a router or switch, to connect to the Internet. It converts or "modulates" an analog signal from a telephone or cable wire to digital data (1s and 0s) that a computer can recognize. Similarly, it converts digital data from a computer or other device into an analog signal that can be sent over standard telephone lines.

The first modems were "dial-up," meaning they had to dial a phone number to connect to an ISP. These modems operated over standard analog phone lines and used the same frequencies as telephone calls, which limited their maximum data transfer rate to 56 Kbps. Dial-up modems also required full use of the local telephone line, meaning voice calls would interrupt the Internet connection.

Modern modems are typically DSL or cable modems, which are considered "broadband" devices. DSL modems operate over standard telephone lines, but use a wider frequency range. This allows for higher data transfer rates than dial-up modems and enables them to not interfere with phone calls. Cable modems send and receive data over standard cable television lines, which are typically coaxial cables. Most modern cable modems support DOCSIS (Data Over Cable Service Interface Specification), which provides an efficient way of transmitting TV, cable Internet, and digital phone signals over the same cable line.

What is Modem ?

The process of modulation and demodulation, that is, the conversion of digital data to analog form and vice-versa, is carried out by a special device called modem (modulator/demodulator).

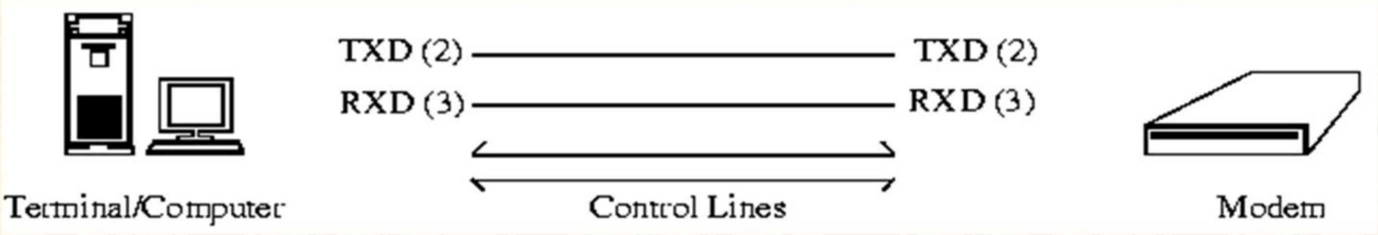
Modulation is the process of changing the form of the signal carrying the information. The demodulation process does the task of extracting information from the signals that are modulated. Analog signals can be transmitted by using devices such as a radio or a diode. Modems are classified on the basis of two criteria:

- Data sent per unit time.
- Change in the state of the signal per unit time.

Modems were first used in the 60s decade, for connecting. Computers over a network of telephone lines. The period is also known as the age of time-share computers, since the computers had to buy time in order to connect to the network by means of a modem which had a speed of 300 bits/second.

Digital Connection

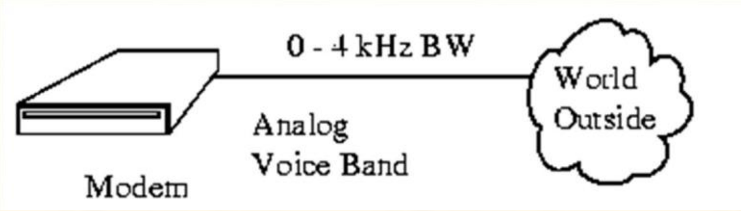
The connection between the modem and terminal/computer is a digital connection. A basic connection consists of a Transmit Data (TXD) line, a Receive Data (RXD) line and many hardware hand-shaking control lines.



The control lines determine : whose turn it is to talk (modem or terminal), if the terminal /computer is turned on, if the modem is turned on, if there is a connection to another modem, etc.

Analog Connection

The connection between the modem and outside world (phone line) is an analog connection. The Voice Channel has a bandwidth of 0-4 kHz but only 300-3400 Hz is usable for data communications. The modem converts the digital information into tones (frequencies) for transmitting through the phone lines. The tones are in the 300-3400 Hz Voice Band.



Baud

Baud is the speed at which the analog data is changing on the voice channel and bps (bits per second) is the speed that the decoded digital data is being transferred.

Features of Modem

1. **Speed :** The speed at which the modem can send data in bps (bits per second). Typically modem speeds are : 300, 600, 1200, 2400, 4800, 9600, 14.4K, 19.2K, 28.8K bps.
2. **Auto Dial /Redial :** Smart Modems can dial the phone number and auto redial if a busy signal is received.
3. **Auto Answer :** Most modems can automatically answer the phone when an incoming call comes in. They have Ring Detect capability.
4. **Self-Testing :** New modems have self-testing features. They can test the digital connection to the terminal /computer and the analog connection to a remote modem. They can also check the modem's internal electronics
5. **Voice over Data :** Voice over Data modems allow a voice conversation to take place while data is being transmitted, This requires both the source and destination modems to have this feature.
6. **Synchronous or Asynchronous Transmission :** Newer modems allow a choice of synchronous or asynchronous transmission of data. Normally, modem transmission is asynchronous. We send individual characters with just start and stop bits. Synchronous transmission or packet transmission is used in specific applications,

Functions of Modem

The essential function of a modem is to create an easily transmitted and decoded signal that allows digital data to be sent from place to place without the loss of information. The most familiar use of modems is to send information over a telephone channel, but modems can be used to relay data over any system that provides a means of transmitting analog signals, including radio and optical networks.

Data Compression

To reduce the amount of time it takes to send data and to cut down on the amount of error in the signal, modems need to employ data compression. This was especially necessary in the early days of modem technology, since data had to be sent via conventional phone lines. Not being designed for digital information, phone lines placed heavy limitations on the size and speed of signals sent over them. Data compression techniques reduce the size of the signal needed to send the required data.

Error Correction

When information is transmitted between modems, it can sometimes be damaged -- meaning that parts of the data are altered or lost. To get around this, modems use error correction. Information is grouped into batches, called frames. Each frame is tagged with a checksum, a small piece of data derived from the information in the frame. A checksum can be thought of as a kind of fingerprint, unique to the data in a particular frame. The modem that receives the information derives its own checksum from the frame it has been sent, then compares its checksum data with the checksum sent by the transmitting modem. If the checksums match, the information is undamaged. If they don't match, the data has been corrupted in transmission; the recieving modem sends it back and waits for the transmitting modem to re-send that frame.

Flow Control

Individual modems send information at different speeds. It's necessary for faster modems to slow down so that slower modems can catch up, otherwise the slower modem will receive more data than it can process. If this starts to happen, the slower modem transmits a character to the faster one. This character is a signal for the fast modem to pause in sending information until the slow modem gets caught up. When the slow modem is ready for more data, it sends a different character that signals to the fast modem that it can start transmitting again. In this way, the two modems can match their speeds.

IP Address, Internet Domains, CIDR Notation, ISP, TCP/IP

Introduction of Internet Address

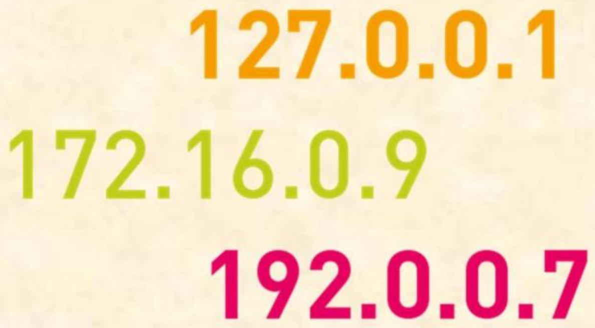
Every machine on a network has a unique identifier. Just as you would address a letter to send in the mail, computers use the unique identifier to send data to specific computers on a network. Most networks today, including all computers on the internet, use the TCP/IP protocol as the standard for how to communicate on the network. In the TCP/IP protocol, the unique identifier for a computer is called its IP address.

There are two standards for IP addresses: IP Version 4 (IPv4) and IP Version 6 (IPv6). All computers with IP addresses have an IPv4 address, and most use the new IPv6 address system as well. Here are the differences between the two address types:

IPv4 uses 32 binary bits to create a single unique address on the network. An IPv4 address is expressed by four numbers separated by dots. Each number is the decimal (base-10) representation for an eight-digit binary (base-2) number, also called an octet. For example: 216.27.61.137

IPv6 uses 128 binary bits to create a single unique address on the network. An IPv6 address is expressed by eight groups of hexadecimal (base-16) numbers separated by colons, as in 2001:cdba:0000:0000:0000:0000:3257:9652. Groups of numbers that contain all zeros are often omitted to save space, leaving a colon separator to mark the gap (as in 2001:cdba::3257:9652).

DEFINITION :



“Every machine on internet has a unique number, called an IP address. IP stands for Internet Protocol, which are the rules that computer use to communicate over the internet".

A client system communicates with an internet server. An internet server computer communicates with a client Computer. Two server computers communicate with one another. Two client computer communicating via one or more servers. The computer that originates a transaction must identify its intended destination with a unique address. Every computer on the internet has a four part number address called internet protocol address, which contains routine — information that identifies its location.

Each of the four part is a number between 0 and 255, so an IP address look like as under:

205.46.117.104

Each host on TCP/IP network is assigned or unique 32 bit logical address which represents four octets of 8 bit each separated by dots, identifies the computer system on the network. The logical address is divided into two parts:

(1) Network ID (also known as network address) identifies a network and must be assigned by the Internet Network information center. The network ID must be unique to the internetwork.

(2) Host ID (also known as host address) identifies a host (workstation server, router or other TCP/IP) on a network and is assigned by the local network administrator. The address for each host must be unique to the network ID.

Uses of IP Address in Internet

An IP address is a logical address for a network adapter. The IP address uniquely identifies computers on a TCP/IP network. An IP address can be private for use on a local area network (LAN) or public for use on the internet or other wide area network (WAN). IP addresses can be determined statically (assigned to a computer by a system administrator) or dynamically (assigned by another device on the network on demand).

Two IP addressing standards are in use today. The IPv4 standard is most familiar to people and supported everywhere on the internet, but the newer IPv6 standard is planned to replace it and starting to be deployed.

IPv4 addresses consist of four bytes (32 bits). Each byte of an IP address is known as an octet. Octets can take any value between 0 and 255. Various conventions exist for the numbering and use of IP addresses.

Classes of IP Addressing

An IP address can be private for use on LAN, or public, for use on the internet. For example, 255.128.122.25. IP addresses has different five classes:

(i) Class A: Class A is for very large organizations and networks with a large number of hosts or routers like international companies might have class A begin with Oxxx. It has number of blocks approximately 128 and block size is around 16,772,216. First octet from 1 to 126 are part of class A and other three octet are also used to identify the each host, class A is used for unicast.

(ii) Class B: Class B is used for midsize networks or organization. It begins with 10xx or 128 to 191 decimal. It has number of blocks 16,384 and block size 65,536. The block size of class B is also very large like class A. Most of addresses in class B are not used. Class B networks make up a quarter of total IP addresses.

(iii) Class C: Class C is designed for small networks or organizations with a small number of hosts and routers. It is for mid-size businesses. Its addresses begin with 110x or 192 to 223 decimal. In class C numbers of blocks are 2,097,152 and block size is 256. The block size of class C is too small for many organizations. It is used for unicost.

(iv) Class D: Class D is used for multicasting. Its addresses begin with 1110, or 224 to 239 decimal. It is used to define one group of hosts on the internet. It is different from first three classes. In class D number of blocks is one and block size D is 268,435,456.

(v) Class E: Class E is used for experiment purpose only and reserved for future use. Its addresses start wills 1111 or 240 to 254 decimal. Only a few organizations are using class E. In class E number of block is one and its block is 268,435,456. It is reserved for future.

INTERNET DOMAINS

The collection of networks making up the internet is divided into groups which are called domains. The domain name system assigns name and members to identify the computers. The names assigned by the DNS are called domain names and the numbers assigned by the DNS are called IP address. Domain names and IP addresses are assigned to all computers on the Internet. IP addresses are difficult to remember and type correctly. Therefore, people prefer to use host names. Domains divide WWW sites into categories based on the nature of their owner. DNS are divided into two parts i.e., domain and subdomains. Example of Internet domains: .com, .edu, .org, etc.

Domain Names

A name that identifies one or more IP address is called domain name. For example microsoft.com represents about a dozen IP addresses.

Domain names are used in URLs to identify particular Web pages. For example, in the URL http:// www.kiet.edu/index.html, the domain name is kiet.edu. Every domain name has a suffix that indicates which top level domain. For example:

gov – Government agencies

edu – Educational institutions

org – Organizations (nonprofit)

mil – Military

com – Commercial business

net – Network organizations

Ca – Canada

th – Thailand

in – India

Domain Name System

DNS stands for two things: Domain Name S ervice and Domain Name Servers. One acronym defines the protocol, the other defines the machines that provide the service. The job that DNS performs is very simple: it takes the IP addresses that computers connected to the Internet use to communicate with each other and it maps them to host names.

DNS translates IP addresses into hostnames and back again. The hostnames are for the benefit human end users. The IP addresses are the only essential thing, as far as the computers are concerned.

CIDR NOTATION

WHAT IS CIDR NOTATION?

Classless inter-domain routing (CIDR) is a set of Internet protocol (IP) standards that is used to create unique identifiers for networks and individual devices. The IP addresses allow particular information packets to be sent to specific computers. Shortly after the introduction of CIDR, technicians found it difficult to track and label IP addresses, so a notation system was developed to make the process more standardized. That system is known as CIDR notation. efficient and

CIDR IP addresses consist of tw o groups of numbers, which are also referred as groups of bits. The most important of these groups is the network address, and it is used to identify a network or a sub network (subnet). The lesser of the bit groups is the host identifier. The host identifier is used determine which host or device on the network should receive incoming information packets. In contrast to classful routing, which categorizes addresses into one of three blocks, CIDR allows for blocks of IP addresses to be allocated to Internet service providers. The blocks are then split up and assigned to the provider customers. Until recently, IP addresses used the IPv4 CIDR standard, but because IPv4 addresses are nearly exhausted a new standard known as IPv6 has been developed and will soon be implemented.

used for IP addresses, but early Internet developers soon discovered that it included a serious flaw in that lacked scalability. To solve this problem, the Internet Engineering Task Force created the IPv4 standard 1993. In addition, CIDR w as created as a system of routing the new IPv4 addresses. These

Development of CIDR

When the Internet domain name system (DNS) was first established, the classful routing system was standards were originally published under the names RFC 1518 and RFC 1519. In 2006, a new version of the standard was published as RFC 4632.

According to the CIDR standard, the first part of an IP address is a prefix, which identifies the network. The prefix is followed by the host identifier so that information packets can be sent to particular computers within the network. With the classful routing system, individual networks were either limited to 256 host identifiers or overburdened with 65,536 identifiers. For many network enterprises, 256 identifiers were not enough and 65,536 were too burdensome to be used efficiently. In the 1980s, as TCP/IP grew into the modern Internet, the need for a more flexible routing system was recognized. This need prompted the development of CIDR and subnets. CIDR and the process of variable-length subnet masking (VLSM) allow network administrators to divide individual networks into subnets of various sizes. In addition, addresses for related operations can be grouped together to create a simple system of categorization. Internet providers are also able to allocate a scalable number of addresses, in blocks, to organizations based on how many addresses are needed. These new routing and categorization systems solved most of the problems with IP addresses, and the only remaining problem was deciding how to identify them efficiently. Eventually, CIDR notation was established and accepted as the standard. In CIDR notation, IP addresses are written as a prefix, and a suffix is attached to indicate how many bits are in the entire address. The suffix is set apart from the prefix with a slash mark. For instance, in the CIDR notation 192.0.1.0/24, the prefix is 192.0.1.0, and the total number of bits in the address is 24.

CIDR Blocks

The ability to group blocks of addresses into a single routing network is the hallmark of CIDR, and the prefix standard used for interpreting IP addresses makes this possible. CIDR blocks share the first part of the bit sequence that comprises the binary representation of the IP address, and blocks are identified using the same decimal-dot CIDR notation system that is used for IPv4 addresses. For example, 1010116 /32 is an address prefix with 32 bits, which is the highest number of bits allowed in IPv4. Addresses with identical prefixes and the same number of bits always belong to the same block. In addition, larger blocks can be easily distinguished from smaller blocks by the length of the prefix. Short prefixes allow for more addresses while large prefixes identify small blocks. CIDR notation is also used for the newer IPv6 standard, and the syntax is the same. The only difference is that IPv6 addresses may contain up to 128 bits instead of the 32-bit maximum of IPv4. Even though IPv6 addresses may be up to 128 bits in length, it is important to note that subnets on MAC layer networks always use 64-bit host identifiers.

The assignment of CIDR blocks is handled by the Internet Assigned Numbers Authority (IANA). One of the duties of the IANA is to issue large blocks of IP addresses to regional Internet registries (RIRs). These blocks are used for large geographical areas, such as Europe, North America, Africa and Australia. It is then the duty of each RIR to create smaller, but still quite large, blocks of IP addresses to be assigned to local Internet registries (RIRS). Depending on the organization of regional and local registries, blocks may be subdivided further until they are assigned to end users. The size of blocks assigned to end users is dependent on how many individual addresses will be required by each user. Most end users receive their blocks from a single Internet service provider (ISP), but organizations that make use of multiple ISPs must obtain provider - independent blocks directly from an LIR or RIR.

Subnet Masks

Once blocks of IP addresses within a private network, which is a process known as subnetting. Computers and other connected devices within a particular subnet can be identified because they all use the same IP address prefix. The subnet identifier then becomes the most significant portion of the host identifier. Finally, the last part of the host identifier is used to distinguish individual computers on a subnet. The subnet identifiers within network are assigned according to the networks subnet mask, which is a binary pattern that is used to determine how many subnets are available in a network. In its binary form, a subnet mask begins with a series of ones and ends with a series of zeros. However, subnet masks are usually expressed using the familiar dot-decimal notation used for IP addresses and network prefixes.

In this notation, the series of ones become the number 255. For example, the most common subnet mask expressed using this notation is 2552552550 This and it is used when only one subnet is required or as the first subnet mask is known as subnet zero, of multiple subnets. A specific subnet mask is created by designating a portion of the host identifier, and larger subnets are created by moving more bits from the host identifier to the subnet mask. The final subnet of a network is designated in binary with all ones. When using the CIDR dot-decimal notation, the final 255255255255 with all ones subnet is expressed as

Before CIDR, subnet masks with all zeros 2552552550 and subnet masks 255255255255 could not be used because they could become confused with network identifiers, but CIDR-compliant equipment use the prefixes and suffixes of CIDR notation distinguish between the two.

ISP (INTERNET SERVICE PROVIDERS)

ISP is an organization or business offering public access to the Internet. It is our gateway, to the Net.

It offers access to the Internet, allowing users to travel and explore using tools like Internet explorer. These days a lots of them are available including BSNL, MTNL, etc. check with your local area ISP since this would be easier to work with. W e usually ring up ISP for any internet connection.

This is why you are charged for a single call even if you are trying to access a website which is based in USA, some ISPs like AOL or MSN are Online Service Providers. They include their own content such as bulletin boards, financial information etc, as well as offering access to public Internet sites. Other ISPS provide strictly access service users must get their content from public web sites.

Types of ISP

There are many types of Internet providers. We c an, for instance, choose one of the big commercial on-line service providers. The primary business of an ISP is looking people to the Internet by giving an Internet account to subscribers, and providing them with two different kinds of access:

1. Shell access and

2. SLIP/PPP access.

Most ISP offers both kinds of access, some offer both with a single account and others require that you choose one or the other. Once you register, your provider will give you a user name (called a user ID), a password, and a phone number to dial. To establish the Internet connection, you have your communications program dial the number. You then log in using your particular user ID and password. At present it is VSNL (Videsh Sanchar Nigam Limited) which is dominating the Internet scene in India through its GIAS (Gateway Internet Access Service). The other service providers in India are MTNL (Mahanagar Telephone Nigam Limited). Mantra -online, Airtel, Reliance Communications and Satyam-online.

TCP/IP

TCP/IP is a name given to the collection of networking protocols that have been used to construct the global Internet. it is a family of more than 100 data communications protocols used to organize computers into networks. The computers that make up the internet, talk to each other in the language of TCP/IP protocol. Any computer that can talk to each other in the language of TCP/IP protocol. Any computer that can talk the language of TCP/IP can be a direct part of the internet that is a part of the reason. Why there is such a wide variety of computers. TCP/IP specifies an addressing scheme for computers on Internet. TCP/IP sets the rules for how data should move between computers must follow in order to move different types of information from place to place.

Advantages of TCP/IP There are following advantages of TCP/IP

- It enables dissimilar systems to be connected.
- It is a protocol standard for the internet.
- It is the most widely used protocol suite by all modern operating system.
- It has many utilities available for troubleshooting.
- It is routable
- It is a scalable client/server framework. (vii) It has been modified and tested for many years and this is a proven protocol.

TCP/IP Layers

TCP/IP stands for transmission control protocol: Internet protocol TCP/IP is a to allow co-operating computers to share resources across a network TCP/IP has

i. **Application layer**
ii. **Transport layer**
iii. **Internet layer**
iv. **Network access layer** , the network access layer is split into physical and datalink components. There are above four protocol layers that data goes through before it gets sent off to another computer. If the message to be sent is long, it will be broken into smaller

(i) Application Layer: This layer is broadly equivalent to the application, presentation and session layer of OSI model. It gives an application access to the communication environment. The protocols used in application layer are: FTP, SMTP, HTTP , DNS, etc.

(ii) Transport Layer: The transport layer just above the internetwork layer is the host-to-host layer. It is responsible for end-to-end data integrity. The two most commonly protocols used at the layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). Both protocol deliver data between the application layer and the internetwork layer. The only difference between TCP and UDP is that TCP provides the guaranteed delivery of data and controls the high traffic in network because it is connection oriented protocol whereas UDP is connection less and does not guarantee the delivery of data.

(iii) Internet Layer: This layer is responsible for the routing and delivery of data across network. It allows communication across networks of the same and different types and carries out translation to deal with dissimilar data addressing scheme. The IP addresses are used by internetwork and higher layers to identify devices and to perform internetwork routing. The address Resolution Protocol (ARP) enables IP to identify the physical address that matches given IP address. The internet layer of TCP/IP support four supporting protocols.

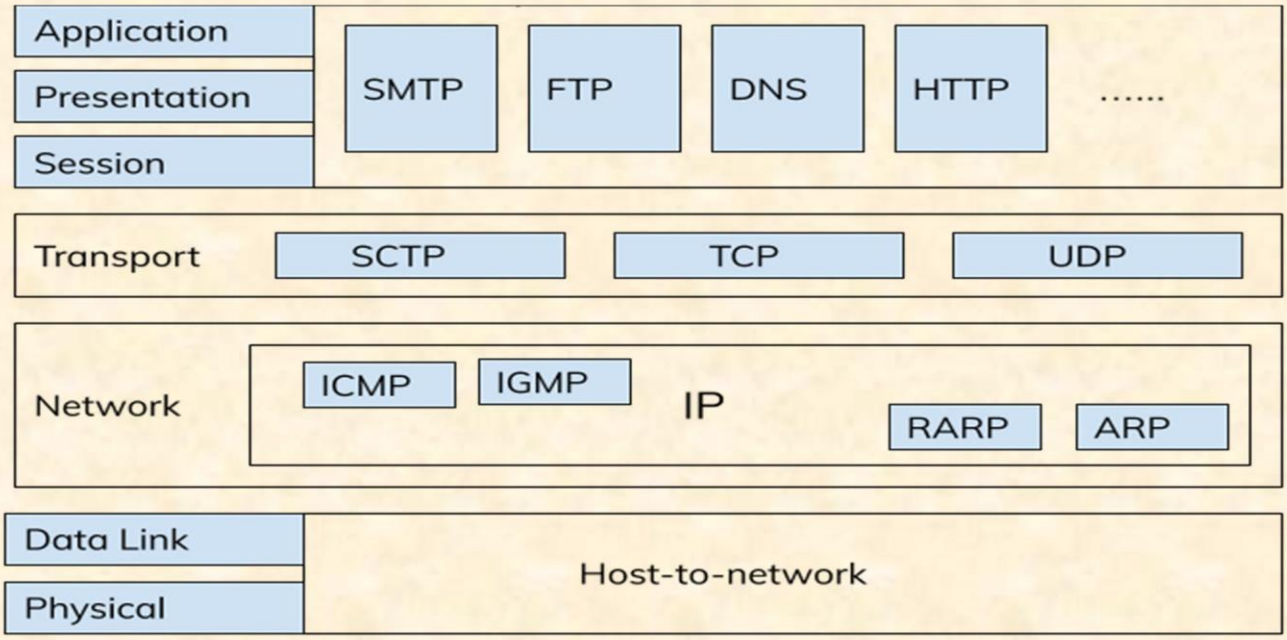
(a) ARP (b) RARP (c) ICMP (d) IGMP

The internet protocol is the transmission mechanism used by the TCP/IP protocol. It is an unreliable and connectionless protocol a best effort delivery service. IP assumes the unreliability of the underlying layers and does its best to get transmission through to its destination, but with no guarantees.

IP transports data in packets called datagrams, each of which is transported separately. Datagrams can travel along different routes and can arrive out of a sequence or be duplicated. IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination. ARP (Address Resolution Protocol) is used to associate a logical address with a physical address. RARP (Reverse Address Resolution Protocol) allows a host to discover its internet address when it knows only its physical address. It is used when a computer is connected to a network for the first time.

ICMP (Internet Control Message Protocol) is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender. IGMP (Internet Group Message Protocol) is used to facilitate the simultaneous transmission of a message to a group of recipients. with pure hardware and access methods such as

(iv) Network Access Layer: The design of TCP/IP hides the function of this layer from users. The combination of data link and physical layer deals CSMA/CD (Carrier Sense Multiple Access with Collision detection). This layer encapsulates the IP datagrams into frames that are transmitted by the network. It also maps the IP addresses to the physical addresses used by the network. The following diagram shows the layers and the protocols in each of the layers:


Application
Presentation
Session
SMTP
FTP
DNS
HTTP
......
Transport
SCTP
TCP
UDP
Network
ICMP
IGMP
IP
RARP
ARP
Data Link
Physical
Host-to-network