Chapter 1:

Computer Networking

Informatics Practices

Class XII (CBSE Board)

Revised as per CBSE Curriculum 2015

"Open Teaching-Learning Material"

Visit www.ip4you.blogspot.com for more….

Authored By:- Rajesh Kumar Mishra, PGT (Comp.Sc.)
Kendriya Vidyalaya Upper Camp, Dehradun (Uttarakhand)
e-mail : rkmalld@gmail.com

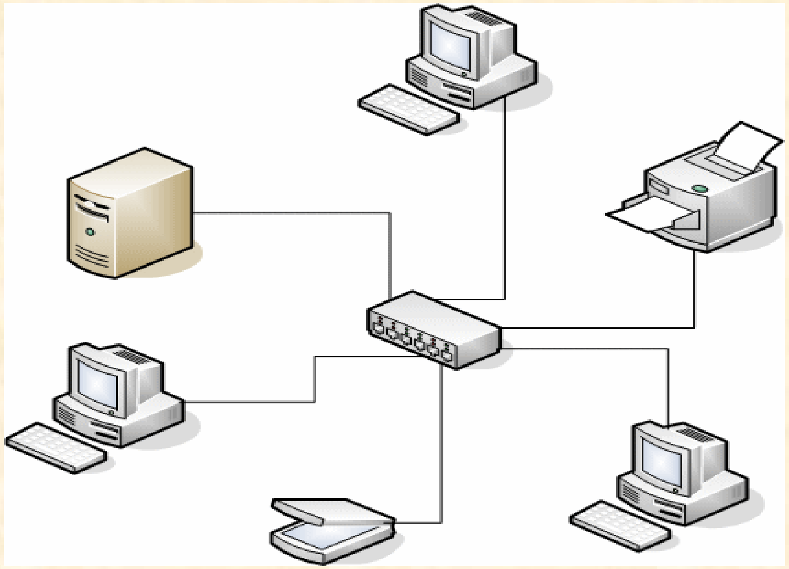
Introduction

- The advent of computer and communication technology, have affected our every walk of life. Observe the following daily-life examples-
  - Watching Cable TV
  - Withdrawing money (cash) from ATMs
  - Sending and receiving E-mails
  - Booking Railway or Air-lines Tickets.
  - Sending and receiving SMS through Mobile.
- These services are provided by the collection of interconnected communicating devices, which make Communication Network.
- The communication over network involves transfer of text/picture/audio/video data through wired or wireless transmission medium.

What is Computer Network?

- □ In simplest terms, the computer network can be defined as –

"A computer network is a collection of interconnected autonomous computers and other devices to share data and other resources."



Why we build a Network?

- □ **Sharing Resources:**

  Primary use of network is to share Program, data and Devices among users irrespective of their physical location.

  Ex. Sharing Database, Audio and video files, printers and scanners etc.

- □ **Improved Communication:**

  A computer network enables fast, reliable and secure communication between users. It saves our time and offers easy communication methods.

  Ex. Sending e-mail, SMS and MMS etc.

- □ **Reduced Communication cost:**

  Sharing resources also reduces its communication cost. Using today's public network we can send a large quantity of data at very low cost. Internet and Mobile network playing very important role in sending and receiving text, image, audio and video data at low cost.

Components of a Network

□ Sender:

A device or a computer that sends the data.

□ Receiver:

A device or a computer that receives the data.

□ Message:

Message is the information to be communicated. It may be text, images, audio or video.

□ Medium:

A transmission medium is a physical path through which the data flows from sender to receiver. A cable or wire or radio waves can be the medium.

□ Protocol:

A set of rules that governs data transmission. It represents the communication methods which to be followed by the sending and receiving devices.

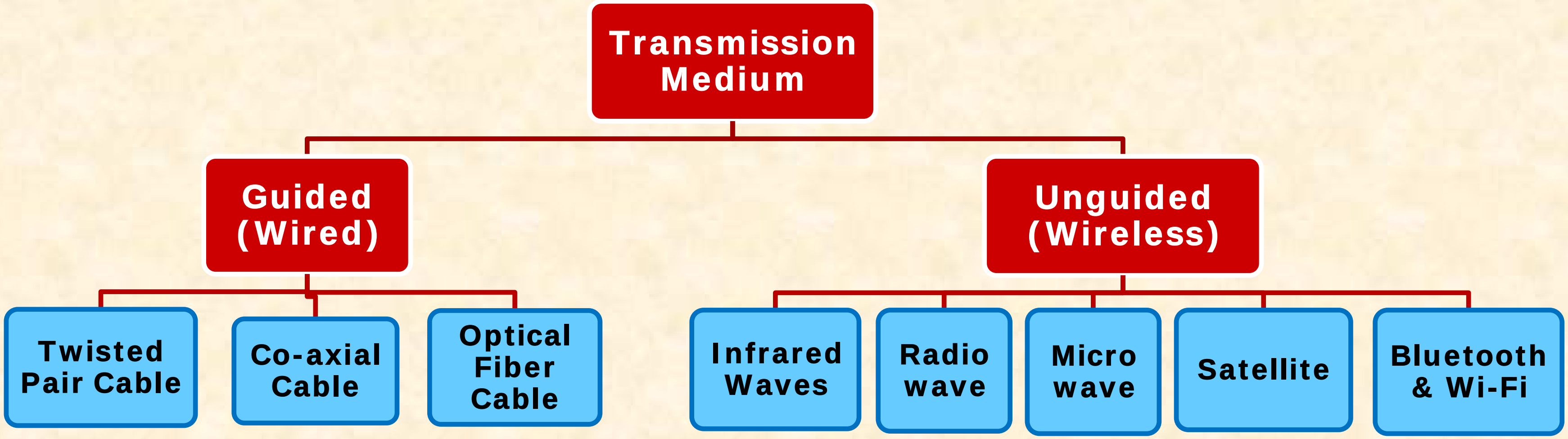
Transmission Media

What is required to connect computers ?

Transmission Media

All the computers or communicating devices in the network, must be connected to each other by a Transmission Media or channel.

- □ A Transmission medium is a medium of data transfer over a network.
- □ The selection of Media depends on the **cost**, **data transfer speed**, **bandwidth** and **distance**.
- □ Transmission media may be classified as-



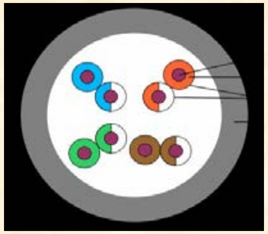
Note: Satellite, Bluetooth and Wi-Fi are Network Technologies which uses Infrared, Radio waves and Microwaves as basic carrier waves (Media) for signal transmission.

1.Twisted Pair Cables

Twisted Pair or Ethernet cable is most common type of media which consists four insulated pairs of wires twisted around each other. Twisting helps to reduce crosstalk and Electro Magnetic Interference (EMI) effects. CAT-5 and CAT-6 specifications are mostly used to setup a LAN.

It is available in Shielded Twisted Pairs (STP) or Unshielded Twisted Pair (UTP) types. In STP, pairs are covered by an extra insulation to further reduce the signal interference.

- □ Advantages:
  - It is low-cost, low-weight and flexible cables.
  - It is easy to install and maintain and requires RJ-45 Connector.
- □ Disadvantages:
  - Suitable for short distance (up to 100 mt.). For long distance Repeater is required.
  - It supports low bandwidth and offers up to 100 Mbps speed.



UTP cable

RJ-45 Connector

2.Coaxial cable

This types of cable consists a solid insulated wire surrounded by wire mesh, each separated by some kind of foil or insulator. The inner core carries the signal and mesh provides the ground. Co-axial Cable or **Coax**, is most common in Cable TV transmission.

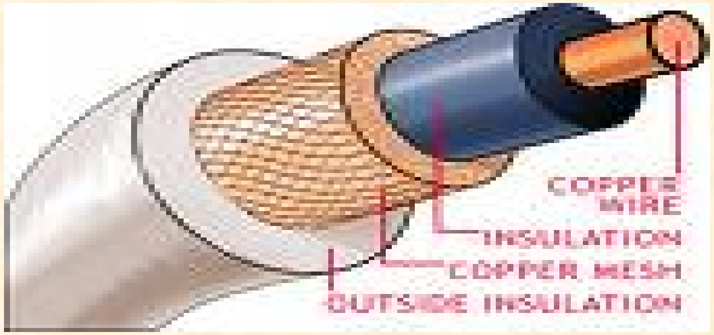
- ❖ It comes in two types- Thinnet (185 mt), Thicknet(500 mt)
- ❖ A connector known as BNC connector is used to connect network devices.

□ **Advantages:**

- ■ It offers high bandwidth and carry data for a long distance (185-500 m)
- ■ Suitable for Broadband transmission (cable TV) and can be used in shared cable network.

□ **Disadvantages:**

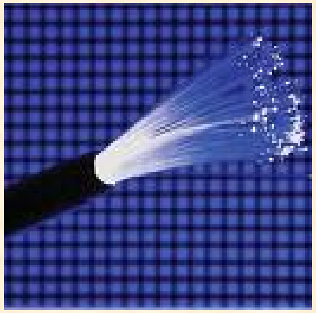
- ■ It is less flexible and expensive compared to Twisted Pair cable.
- ■ Not compatible with modern cables like UTP and STP

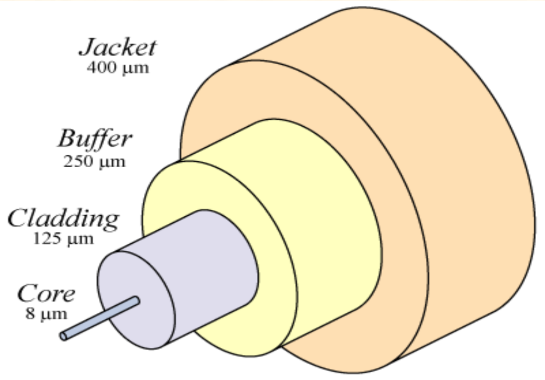


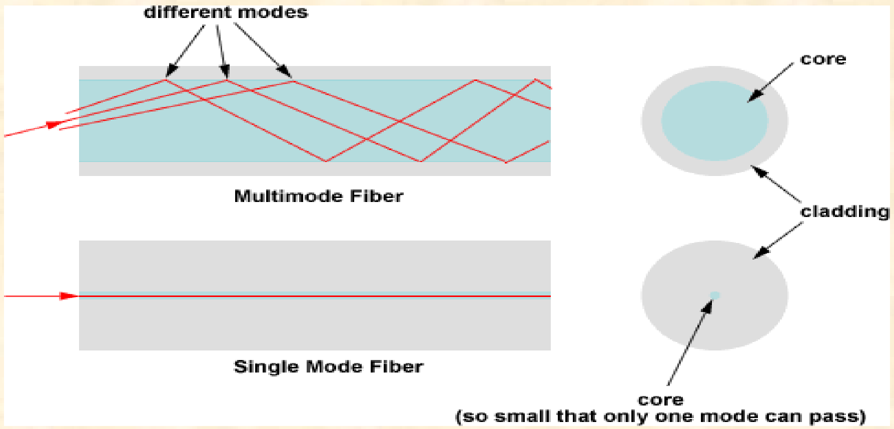
3.Fiber Optic

Optical Fiber consists of thin glass or glass like material and carry light. Signal are modulated and transmitted in the form of light pulses from source using Light Emitting Diode (LED) or LASER beam.

- **The Fiber cable consists Core (Glass or Plastic) covered by Cladding, which reflects light back to the core. A Protective cover including Buffer Jacket is used for extra protection.**
- **Two types of transmission i.e. Single mode (LESER) and Multimode (LED) is possible.**
- **Advantages:**
  - **It is free from EMI since no Electrical signal are carried.**
  - **Offers secure and high speed transmission up to a long distance.**
- **Disadvantages:**
  - **Expensive and quite fragile (breakable).**
  - **Complicated Installation procedure and difficult to join two broken fiber.**
  - **Not suitable for domestic purposes due to high maintenance cost.**







Which cable (media) is better?

- □ While setting up a Network, the selection of Transmission Media is depends on the cost, data transfer speed, bandwidth and distance.
- □ Twisted Pair Cable mostly used now days to setup Local Area Network (LAN) spread up to a building or Campus.

Factors	Twisted Pair Cable	Coaxial Cable	Optical Fiber Cable
Data Transfer Rate	10Mbps-10 Gbps	100 Mbps	> 100 Gbps
Distance (range)	100 mt.	185-500 mt.	>10 Km.
EMI susceptibility	More	Less	Nil
Cost	Least cost	More than Twisted Pair	Very expensive

Wireless Transmission Medium

- Wireless networks are being popular now days, as they uses Electromagnetic Waves for communication.
- In Wireless network, devices are connected without physical medium.
- Wireless communication uses Radio Wave, Microwave, Satellite and other short frequencies waves like infrared to transmit data.

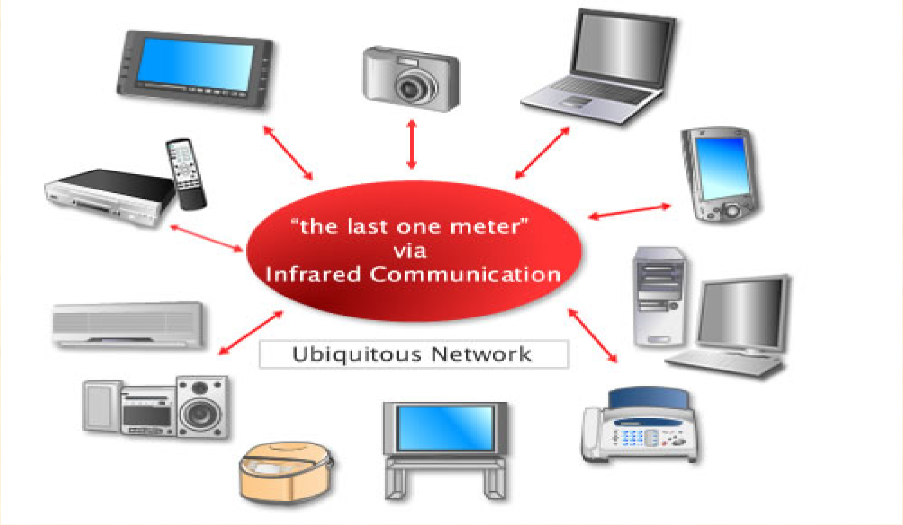
pgi0099 www.fotosearch.com

Applications of Wireless in modern lives

- Accessing the Internet using a cellular phone
- Home or business Internet connection over satellite
- Beaming data between two handheld computing devices
- Wireless keyboard and mouse for the PC

1. Infrared Waves

- □ **Infrared** Wave Network allows devices to communicate within a short-range (approx. 5 meters) using wireless signals.
- □ The infrared transmission technology used in computers is similar to that used in modern Remote Operated Electronic product like TV, Cordless phones and Toys etc.
- □ Infrared Communication is affected by various factors like angle, distance, electromagnetic noise and heat etc.
- □ The biggest drawback with Infrared communication is its short-range and angle problems which makes it unsuitable for modern day mobility needs.

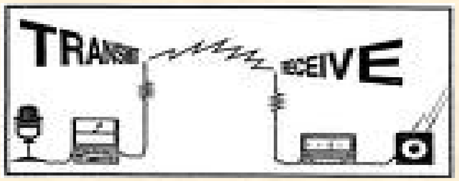


Features of Infrared Transmission

- ❖ Line of sight transmission.
- ❖ No Government License.
- ❖ Do not cross solid objects.
- ❖ Applicable for short-range.

Ex. Remote & TV, Toys etc.

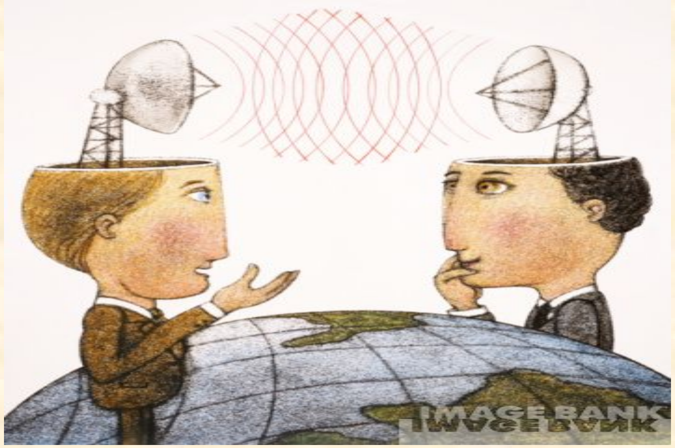
2. Radio Wave

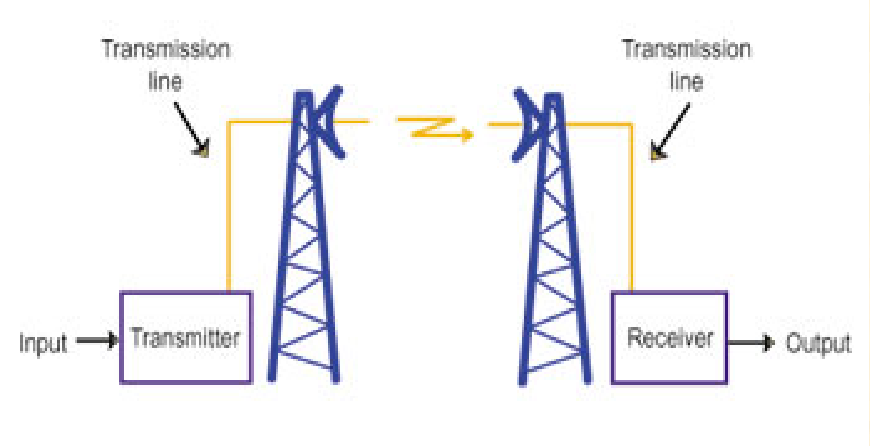


- Radio communication uses Radio frequencies like Medium Wave, Short Wave, VHF and UHF (3KHz-3 GHz).
- Signal are modulated on a high speed Radio wave carrier frequency using Amplitude Modulation (AM), Frequency Modulation(FM) or Phase Modulation(PM) etc.
- Generally, it is used to make Broadcast Network like AM/FM Radio network within a city.
- **Advantages:**
  - It covers a larger span of coverage and offers mobility.
  - Propagates in **Omni direction** (surrounding) and can penetrate solid walls/buildings easily.
- **Disadvantages:**
  - Expensive and in-secure communication.
  - It is susceptible to whether effects.

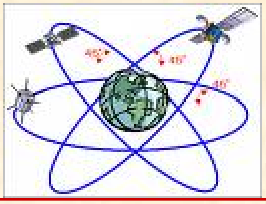
3. Microwave

- Microwaves are high energy radio waves that are used for **line of sight** communication between a pair of communication devices equipped with Parabolic antenna, aligned with each other.
- **Advantages:**
  - Suitable for high speed and long distance (upto 100 km.) communication.
  - No need for lying cable and ability to communicate over oceans.
- **Disadvantages:**
  - Implementation and maintenance cost is high.
  - Insecure communication and propagation of waves is susceptible to whether effects like Rain and thunder etc.
  - Only Line-of-sight transmission is possible.



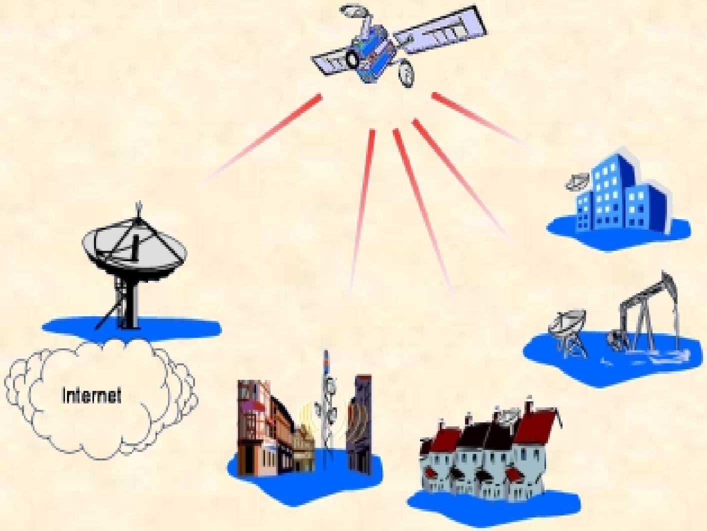


4. Satellite



- Satellite communication uses Microwave (1.5 GHz -20GHz)as media. Satellites like the Geo-stationary or Polar satellites are used to establish communication links among various earth based stations having Antenna.
- Services like DTH, VSAT, GPS and Satellite phones etc. are offered by the satellite.
- Satellite works like a Trans-Receiver Antenna in the space, which receives, regenerates and redirects signals.

- **Advantages:**
  - It covers a larger geographical area of the earth.
  - Offers secure, uninterrupted and high quality transmission.
- **Disadvantages:**
  - Very expensive and high operating cost.
  - Slower than Microwave transmission.
  - Requires legal permissions.



4. Bluetooth

- □ Bluetooth is a wireless technology for creating personal networks operating within a range of 10 meters.
- □ It uses 2.4 GHz unlicensed band.
- □ Bluetooth is used to establish a PAN across handheld devices like a cell phone and Bluetooth enabled Computer.
- □ Bluetooth is a communications protocol standard primarily designed for low power consumption, with a short range.

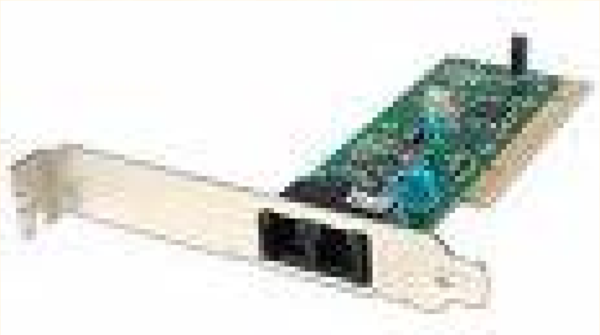
Wi-Fi (Wireless Fidelity) Communication is similar to Bluetooth in operation but covers a large range of coverage (50 -200 mts.). It offers network connectivity with mobility (Any place) within its range. Mostly it is used in home, office buildings, college or university campus, Cyber Café and Hotels to provide Internet connectivity.

Networking Devices

- Networking devices are equipments that allow receive or transmit data or signal and used to make communication channel.
- Some common Networking devices are-
  - Network Interface Card (NIC)/ LAN Card
  - Hub
  - Switch
  - Repeater
  - Router
  - Gateway
  - Modem

Network Interface Card(NIC)

- □ Any computer which has to be connected to a Network, must have an Network Interface Card (NIC) installed in it. Now days, most of the PCs and Laptops are equipped with an integrated NIC on its Motherboard.
- □ A NIC (Network Interface Card) or LAN Card enables computer to connect with a network using a Port.
- □ **WLAN** card are also being popular for connecting PCs or Laptops with Wireless Network.
- □ Each LAN card posses a unique **6 Byte** Physical address assigned by the manufacturer, called **Media Access Control (MAC) Address**. This address identifies a node uniquely over the network.



Hub

- A Hub is a connecting device which connects multiple computers together to form a Local Area Network (LAN).
- Hubs make Broadcast type Network and do not manage traffic over the network channel. Signal entering any port is broadcast out on all other ports.
- It provides various RJ-45 ports to connect Twisted Pair cable in STAR topology, making them act as a single network segment. Now days, Switch is used in place of Hubs.

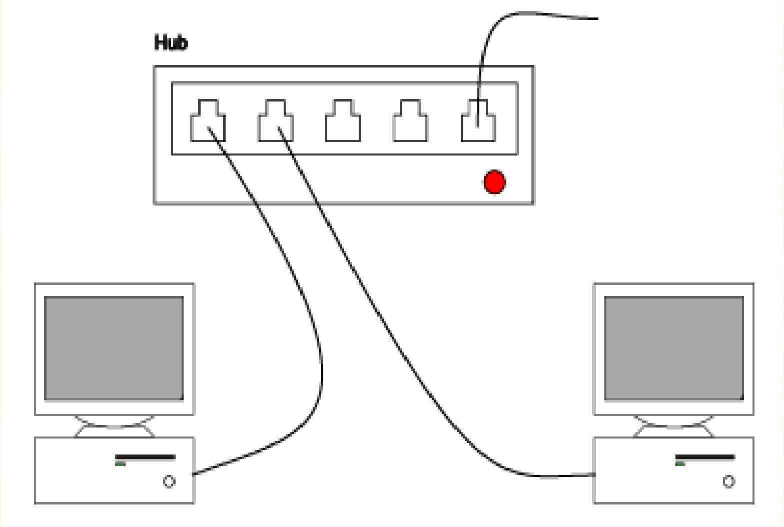
Type of Hub

- **Active Hub:**

  Amplifies the signal when required and works as a **Repeater**.

- **Passive Hub:**

  It simply passes the signal without any change.

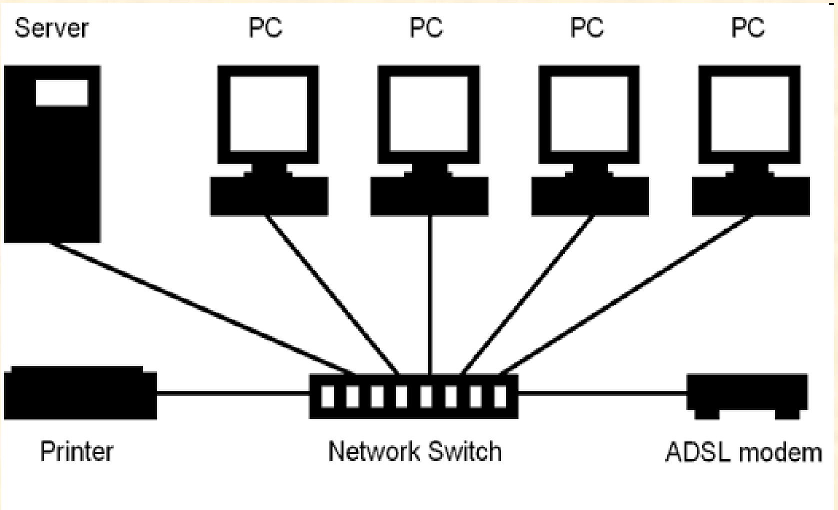


Switch

- □ Switch is a device that is used to connect several nodes to form a Network. It redirects the received signals only to the intended Node i.e. controls Network traffic.
- □ It is also used to segment a big network into different Sub-networks (Subnet) to control the network traffic and security.
- □ It can also used to combine various small network segments to form a big Network (as in Tree topology)

Hub V/s Switch

- ❖ In contrast to Hub, a Switch transmits data/signals to specified Node only, instead of broadcast the signals in a network.
- ❖ Switch is faster and efficient over Hub due to good traffic management capability.



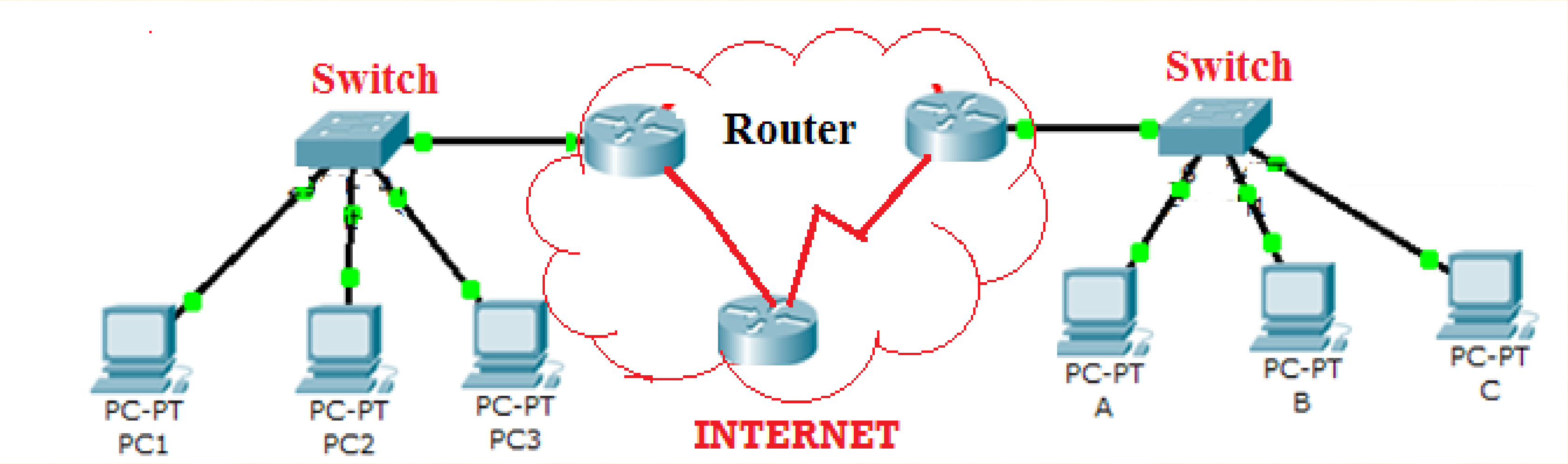
Example 1: A wired client-server network

Repeater

- □ A Repeater is a device that is used to regenerates the received signals and re-transmits to its destination.
- □ Since signal becomes weak after certain distance and can’t reach to its destination, so re-generation (amplification) of signals is required. In such case a Repeater is used.
- □ In case of Twisted pair cable, signals becomes weak after 100 meters. Repeaters are required at each 90- 100 meters to maintain signal strength.
- □ An Active Hub or Switch also works as a repeater.

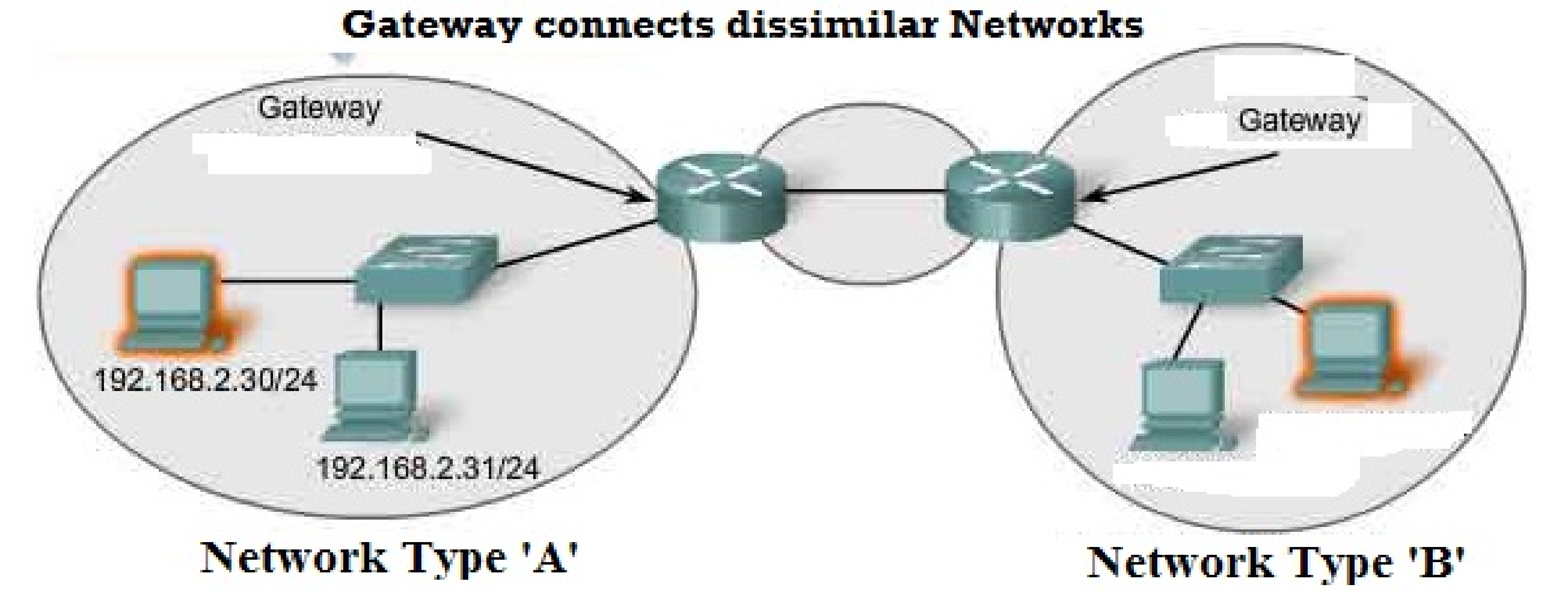
Router

- □ Router is an inter-networking device which connect multiple independent Networks to form a Wide Area Network.
- □ The basic role of Routers in a network is to determine the best possible route (shortest path) for the data packets to be transmitted. In a large network (WAN), multiple routers works to facilitate speedy delivery of data packets.
- □ Router maintains a table of addresses (called routing table) that keeps a track of paths connected to it.



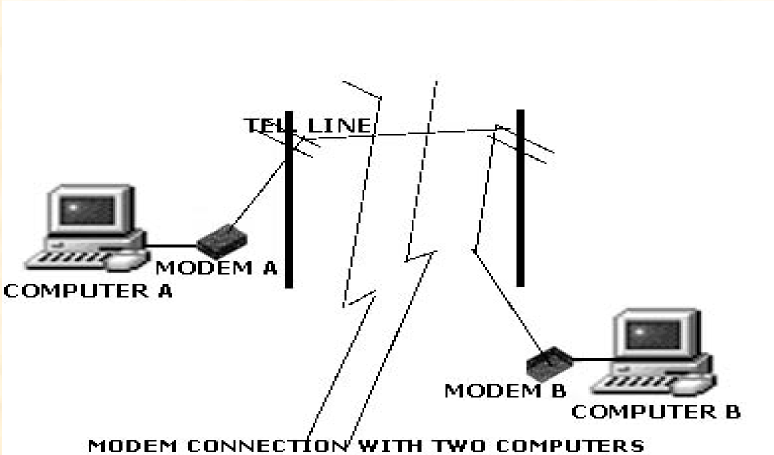
Gateway

- □ A Gateway is a device that connects dissimilar networks. It establishes connection between LAN and External Network with different structure of protocol.
- □ Gateway is also called protocol converter that convert data packets from one protocol to other and connects two dissimilar networks.
- □ A gateway can be implemented in hardware, software or both, but they are usually implemented by software installed within a router.
- □ A LAN gets connected to Internet (WAN) using a gateway.



MODEM

- A MODEM (**MO**dulator-**DEM**odulator) is a device that connect Telephone line to Computer.
- It converts Digital signal into Analog (Modulation) and Analog to Digital (Demodulation). This conversion is required because Telephone lines can’t carry digital data.
- Generally it is used to connect a PC with Telephone lines to access Internet or make voice call and FAX using PC.
- It may be Internal or External type. Now days DSL Modem is used to access Broadband Internet.



Network Topologies

How computers to be connected ?

Network Topologies

- □ In order to form a network, computers and other communicating devices (Nodes) must be interconnected in some layout.

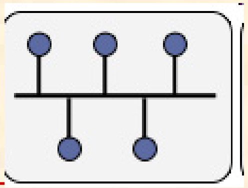
  The layout of interconnection of devices in a network is called Topology.

- □ The major types of Topologies are-

(1) Star topology	(2) Ring topology
(3) Bus topology	(4) Tree topology

- □ The selection of topology for a network depends on the following factors-
  - ■ Cost:- It includes cable/media cost and installation cost depends on the distance between nodes.
  - ■ Flexibility:- Arrangement of furniture and walls in the building may affect the selection of topology and media.
  - ■ Reliability:- Fault detection during Network failure also affects the selection of topology.

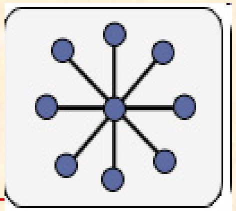
Bus Topology



In the bus topology, all devices are connected to a main cable called backbone channel. It is simple and oldest topology used in the early days of computer networking.

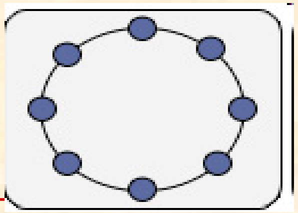
- □ Advantages:
  - Simple layout and requires less cables.
  - Easy to expand since node may be connected at any point on linear path.
- □ Disadvantages:
  - Detection of fault is quite difficult because there is no centralized control.
  - In case of main cable or terminal fault, the entire networks goes down.
  - To cover a long distance, Repeaters is needed to maintain the signal intensity. Terminator is required to terminate the signal at both end of the cable.

Star Topology



- In Star topology, each node is directly connected to a central device like Hub or Switch. It is most popular topology to form Local Area Networks (LAN).
- Advantages:
  - Easy to setup and expand.
  - Easy to locate fault in case of network failure.
  - It offers centralized control over the network.
- Disadvantages:
  - Increases cabling cost since each node is directly connected to the centre node.
  - Difficult to expand due to limited connecting points at centre node or device.
  - All nodes are dependent on central node. if the central device (Switch) goes down then entire network breaks down.

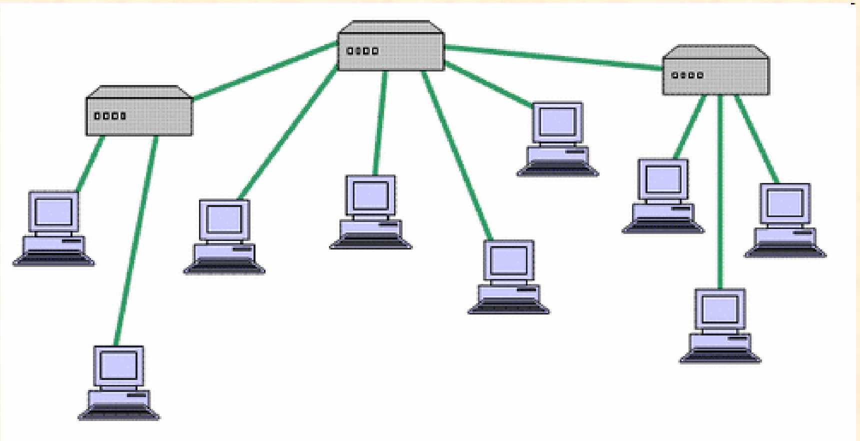
Ring Topology



- In a ring topology network, every node has exactly two neighboring nodes. All messages or data packet travel in the ring in the same direction and passes through each node. The message is taken out from the frame by the receiver and the cycle continues.
- Advantages:
  - Simple layout and requires less cables.
  - Easy to expand i.e. node may be connected at any point on circular path.
  - Optical fiber is often used for high speed transmission.
- Disadvantages:
  - Detection of fault is difficult i.e. failure of one node will affect the whole network.
  - Less reliable i.e. a failure in the cable or any node breaks the loop and entire network becomes down.

Tree Topologies

- Tree topology combines multiple star topologies together onto a bus. In its simplest form, only connecting port devices (hub or switch) are connected directly to the bus network , and works as a "root" of the network tree.
- This Bus-Star hybrid approach supports future expandability of the network much better than a bus or a Star.



Network Protocols

How Network Works ?

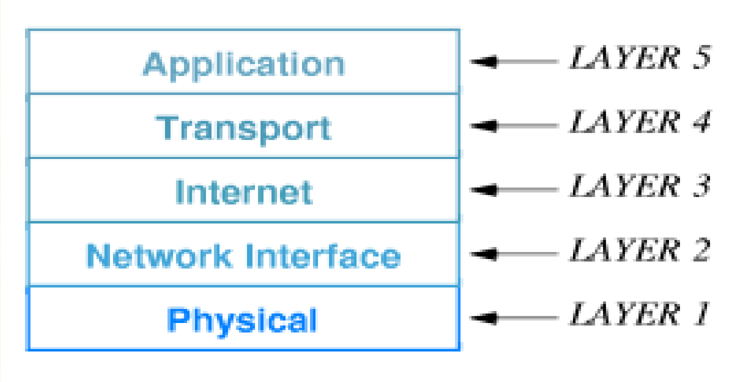
Computer or Nodes in a network will be able to communicate to each other only when they know to each other and follow some set of rules of communication. These set of rules is called Network Protocols.

“Network Protocols is a set of rules for communication which includes rules of **how** and **when** a device can **send** or **receive** the data and how it reaches its destination.”

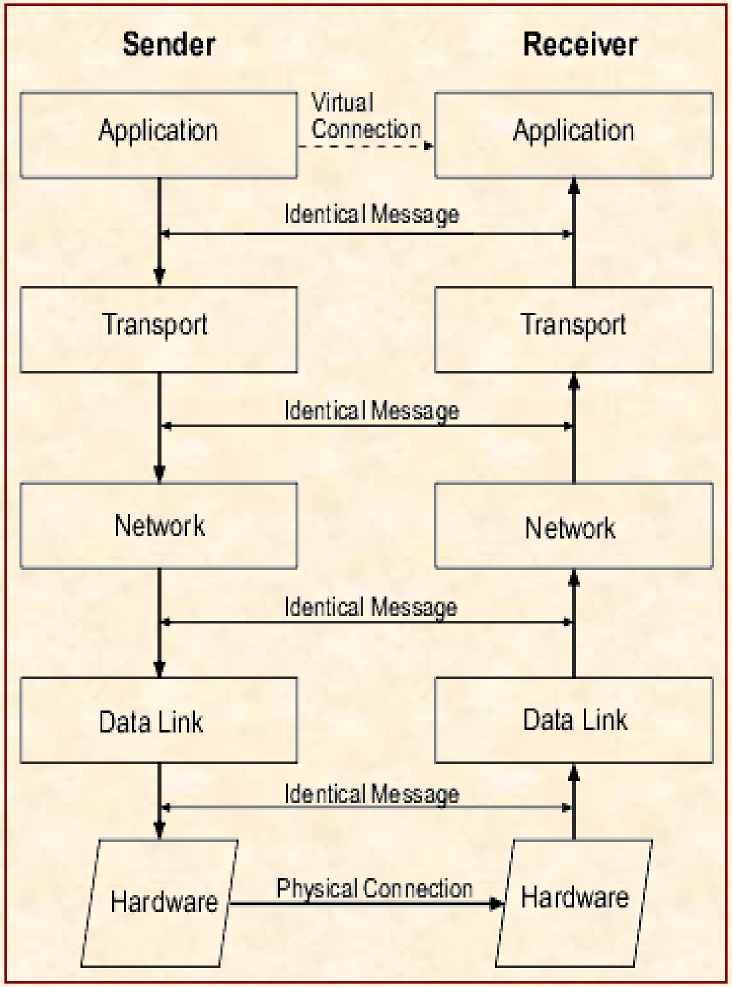
Some commonly used protocols are HTTP, TCP/IP, FTP and PPP etc. TCP/IP is a master protocol which comprises other protocols.

TCP/IP Protocol

- The **Transmission Control Protocol/ Internet Protocol Suite** (**TCP/IP**) is most commonly used protocol to setup LAN, WAN, Internet and other similar networks.
- The Internet Protocol Suite comprises 5 Layers including Physical media. Each layer is responsible for a well-defined task, and provides a well-defined service to the upper layers.



Application	LAYER 5
Transport	LAYER 4
Internet	LAYER 3
Network Interface	LAYER 2
Physical	LAYER 1



Other Protocols

- □ **Hyper Text Transfer Protocol (HTTP)**

  HTTP is used to transfer web pages and data files from one computer to another on the World Wide Web (WWW). When you visit a web site on Web Browser program like Fire Fox, your computer becomes HTTP Client which receives web pages and data from web server. This communication is governed by the HTTP Protocol.

- □ **File Transfer Protocol (FTP)**

  FTP is used to transfer files from one computer to another on the Internet. Generally, It is used by Web Developer to upload web pages on the Web Hosting servers.

- □ **Point to Point Protocol (PPP)**

  It is a protocol used to establish a direct connection between two computers using Telephone lines. Before coming to ADSL Modems, most Internet Service Providers (ISPs) use PPP to provide dial-up access for the Internet to their customers.

MAC Address

- □ A Computer or node on a network needs a Network Interface Card (NIC) or LAN card. Each LAN card has its own unique 6-Byte Physical address assigned by the manufacturer, called Media Access Control (MAC) Address for its identification purpose.
- □ MAC addresses are 48-bit (6 Byte) hexadecimal numbers like - MM:MM:MM:SS:SS:SS

  where first half (MM) shows Manufacturer ID and second half (SS) shows unique serial number of the card.
- □ In a networks, the MAC address uniquely identifies each node on network segment and allows frames to be marked for specific hosts.
- □ MAC address is a permanent physical address and does never change.
- □ Example of MAC Address – 00:A0:C9:12:C5:32

IP Address

- □ All the computers on the Network follow the some set of rules (Protocol) for communication to each other. One of the most common protocol is TCP/IP. Internet also follows this protocol.
- □ Each machine in TCP/IP network needs to have a unique 32 bit (4 Byte) address called IP address.
- □ The IP address may be static or dynamic depending on the network or service provider.
- □ In TCP/IP Network, an **IP** address of 32-bit number is known as Internet Protocol Version 4 (*IPv4)*. This version theoretically ensures 2^{32} possible addresses. IPv6 is also being used to provide more expandability.
- □ IPv4 addresses are usually represented in dot-decimal notation (four numbers, each ranging from 0 to 255, separated by dots). Example- 208.77.188.166.

Domain Name

- In general, Domain name is a group name assigned to a web server or web site.
- A Domain Name usually contains Top Level or **Primary Domain** and **Sub-Domain** name(s).

  For example- “**CBSE.NIC.IN**”

  where **.in** is Primary domain and **NIC** is sub-domain of IN.
- Top level or Primary Domain are classified into Generic Domains like .com, .org, .edu, .net, .gov and Country Domain like .in, .ca, .jp, .nz, .us etc.
- The complete unique address of the page on a website is called **URL** (Uniform Resource Locator) e.g.

  http://www.cbse.nic.in/welcome.html
- Since computers on the network are identified by its IP addresses, so it is required to convert a Domain name or URL typed in the Browser, into its corresponding IP address. This process is called Domain Name Resolution. This resolution is done by the designated servers called DNS servers, provided by the Internet Service Providers (ISP) like BSNL or MTNL etc.

Types of Network

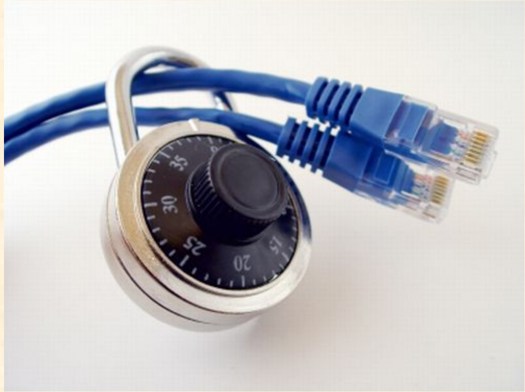
A computer network may be small or big as per number of computers and other network devices linked together. Thus, networks vary in size, complexity and geographical area spread. On the basis of geographical spread, network may be classified as-

- PAN (Personal Area Network) : The PANs are small network, used to establish communication between computer and other hand-held devices in small proximity up to 10 meters using wired USB connectivity or wireless system like Bluetooth or Infrared. PANs are used to connect computers, laptops, Mobiles and other IT-enabled devices to each others.
- LAN (Local Area Network): This system spans on a small area like a small office or home. The computer systems are linked with wire/cables or wireless (Wi-Fi) system. The key purpose of LAN is to sharing the resources. LAN users can share data, programs, printer, Disk, modem etc.
- MAN (Metropolitan Area Network): A large computer network that usually spans a city or a large campus. MAN usually interconnects a number of LANs. It also shares the computing resources among users.
- WAN (Wide Area Network): This type of network spreads over large geographical area across countries and continents. WANs are generally used to interconnect several other types of networks such as LANs, MANs etc. It facilitates fast and efficient exchange of information at high speed and low cost.

Types of Network- A comparison

Parameter	PAN	LAN	MAN	WAN
Area covered	Small Area (upto 10m radius)	A building or campus (upto 10 km)	A city (upto 100 Km radius)	Entire country, Continent or Globe
Networking Cost	Negligible	inexpensive	expensive	Very expensive
Transmission Speed	High speed	High speed	Moderate speed	Low speed
Error Rate	Lowest	Lowest	Moderate	Highest
Network Devices used	WLAN, USB Dongle	LAN/WLAN, HUB/Switch, Repeater, Modem	Router, Gateway	Router, Gateway
Technology/ Media used	Infrared, Bluetooth	Ethernet, Wi-Fi	Optical fiber, Radio wave, Microwave	Microwave, Satellite

Network Security



How to secure a Computer Network?

Network Security is a process of providing security at the boundaries of a network by keeping out unauthorized access and malwares.

Network Security Threats

Information and Network security commonly refers to various dimensions known as **CIA**.

Confidentiality: Protection against unauthorized access.

Integrity: Protected against unauthorized modification.

Authentication: Identification of authorized user.

CIA can be weakened and broken with following threats-

- **Intrusion / Access Attack**
  - □ Snooping
  - □ Eavesdropping
  - □ Spamming
  - □ Phishing
- **Denial of Service** (DoS) attack
- **Hackers & Crackers**
- Malicious Program (Virus, Worm, Trojan Horses)

Intrusion / Access Attack

In this type of threat, an unauthorized user attempts to gain access to sensitive information stored in the computer.

□ Snooping

It refers to unauthorized access of someone else data, e-mail, computer activity or data communication. It may comprises monitoring of Keystrokes pressed, Capturing of passwords and login information and interception of e-mails and other private information.

□ Eavesdropping

It the act of secretly listening/ interpreting someone else's private communication or information while data is on its way on the network.

□ Spamming

Spamming refers to the sending of bulk-mail (junk-mail) by an identified or unidentified sources.

Intrusion / Access Attack

- ## Phishing

Phishing is a process of attempting to acquire sensitive information such as User name, passwords, Credit card number, bank account details etc. using a trap-mail in which user himself discloses their private details.

- ## Denial of Service Attack:

DoS attack are those attacks that prevent the legitimate users from accessing or using the resources and information.

This types of attack may eats up all the resources of the system and computer become to a halt state.

Different types of DoS attacks are-

- **Denial of Access to Information**
- **Denial of Access to Applications.**
- **Denial of Access to Systems**
- **Denial of Access to Communication**

Hackers & crackers

- In context of computer security, a **hacker** is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers may be motivated by various reasons such as profit, protest, or challenge. They are expert computer programmers who can break security to gain the computing resources and may exploit privacy.
- A **White hat** hacker breaks security for non-malicious reasons, perhaps to test their own security system or while working for a security company which makes security software. The term "white hat” refers to an Ethical Hacker.
- A **Black hat** hacker is a hacker who "violates computer security for maliciousness or for personal gain". Black hat hackers can crack password or secure networks to destroy or theft data or make the network unusable. Black hat hackers also referred as "**crackers**“. Crackers keep the awareness of the vulnerabilities to themselves for personal gain and do not notify the general public or manufacturer for its correction.

Malicious Program threats

- □ **Virus:**

  Computer viruses are malicious and self-replicating codes/programs that cause damage to data and files on the computer system.

- □ **Worm:**

  It is also a self-replicating program which eats entire disk space or memory. It copies itself until all the disk space or memory is filled.

- □ **Trojan Horse:**

  It is a program that appears harmless (like utility program) but actually performs malicious functions such as deleting damaging files.

- □ **Spyware:**

  Spyware is a program designed to spy on your activities and report this data to people willing to pay it either legal or illegal purposes. It is get installed in your system without your consent as a file or gets downloaded from Websites on Internet.

- □ **Adware:**

  Adware are the programs that deliver unwanted ads to your computer (in Pop-up form). They consume network bandwidth. It is similar to Spyware, but it may installed with your consent.

Network Security Principles

- The entire Computer and Network security is based on some safeguards designed to protect a computer system from threats.
  - Active Protection:

    Installation of Programs and Firewall for protection against Viruses, Spyware, Adware and PC Intrusion.
  - Preventive Measures:

    You should opt some preventive measures to avoid such happenings.

Active Protection- Security tools

- □ **Authorization (User Name/Login ID)**

  User Authorization is done by a valid User Name/Login Id etc. (Some thing do you Know?) User Name is a code which authorizes user to get computer access after log-in.

- □ **Authentication (Password)**

  User is Authenticated by a valid password. Password is a secret code that is used to authenticate or confirm user's identity. Password should strong enough to avoid guessing. Generally, User name and Password in combination is used to provides better security.

- □ **Biometric Identification (Physical Authentication)**

  To provide more strong security, a system may have Biometric devices to identify a person by unique biological properties like Finger print , Retina Scan, Voice or Face Recognition etc., which can not be transferred or stolen by others. (Something do you have ?)

- □ **Anti-Virus for Malicious Program**

  These Program prevent the system from various malicious programs like Virus, Worms, Spywares and Trojan horses etc. Some commonly used Anti-virus programs are- Quick Heal, Avast, Norton AV, Mcaffee.

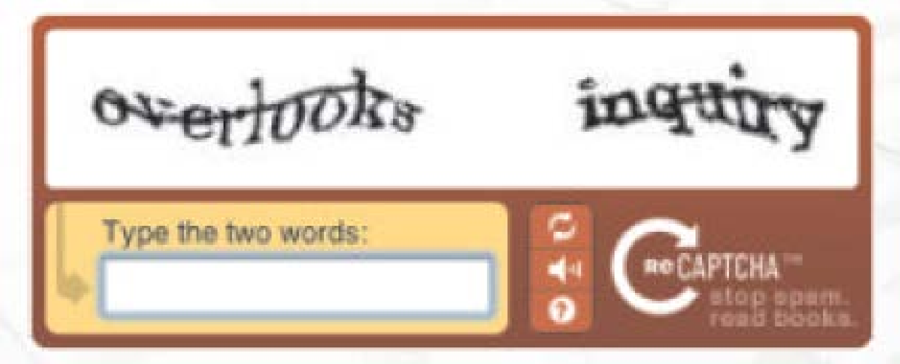
Active Protection- Security tools

□ **File Access Permissions**

Files and folders stored on the computers may have limited access permissions like Read, Modify, Create and Execute permission (rights) as per need of the other users in the network. Sometimes a file may also have password to open or modify the contents to provide additional security at file level.

□ **CAPTCHA :**

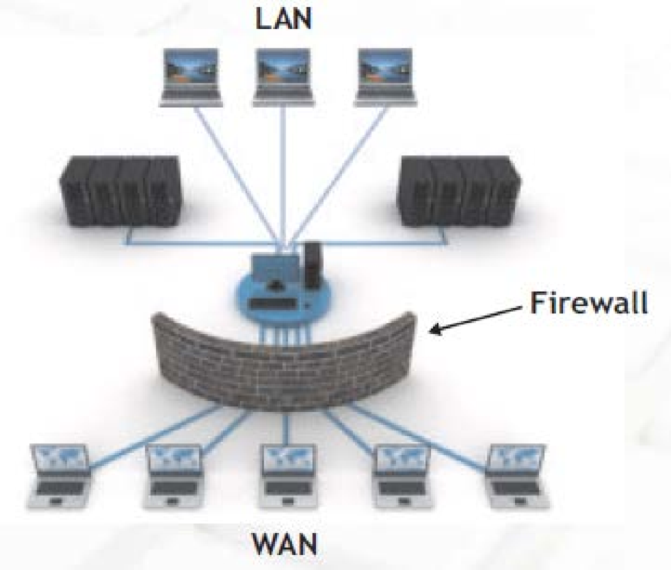
CAPTCHA(**C**ompletely **A**utomated **P**ublic **T**uring Test to tell **C**omputers and **H**uman **A**part) is a program that displays distorted text/images as a challenge, which can read by human beings only. It ensures that website/program is being accessed by human being and not by malicious computer programs (bots).



Active Protection- Security tools

- **Firewall**

  Firewall is a system (H/w or S/w) which acts like a gatekeeper to protect Computer or Network from unauthorized access. It monitors the network access as per rules defined by the Network Administrator. All requests entering or leaving the LAN passed through the Firewall, which examines each requests and blocks those that do not meet the security criteria.



- **Intrusion Detection System (IDS)**

  It is system which identifies various types if Intrusions and monitors the users activities and Network resources. It notifies to authorities in case of suspicious happenings. It is advanced system than Firewall, which provides a watch on internal and external user's suspicious activities and access for Network resources.

Active Protection- Security tools

- □ **Digital Signature :**

  Digital signature is a method for providing the authenticity of a message, document or attachment sent through e-mail. It is commonly used in Financial and Legal transactions where forgery and tempering of document is possible. It works like a valid signature of a person on a document which ensures recipient about authenticity of document.

- □ **Digital Certificate :**

  Digital Certificate (Public Key Certificate) is an electronic document which uses digital signature and requires a public key or password to open or encode a document. It verifies and ensures that document belongs to an authorized individual or organization.

- □ **Cookies :**

  A Cookie is a small text file containing information regarding a website preferences and some private data of user. It is placed in the system by web-server and used by the web browser to provide information about visitor. It can also be used for authentication and Session tracking. Some cookies may violate privacy by transferring user's private data like name and passwords etc. So, cookies should be monitored while accessing website on the Internet.

Preventive Measures

- ✓ Install an effective and reliable Anti-virus and Anti-Spyware program.
- ✓ Keep your Anti-virus program update.
- ✓ Think twice before downloading anything from the Internet. (Always Download from trusted sites)
- ✓ Be careful while opening e-mails.
- ✓ Implement proper Security policy.
- ✓ Use proper File access permissions when it is being shared among users.
- ✓ Use Filter utility to get off spam or junk-mails.
- ✓ Keep your e-mail address, passwords etc. private.
- ✓ Install Firewall to prevent unauthorized access to or from a private network.
- ✓ Disable cookies to avoid misuse of private data.
- ✓ Disconnect Internet when it is not in use.

Cyber crime & Cyber Law

- □ **Cyber crime (Computer Crime)**

  Cyber crime refers to any crime wherein the computer is either a tool or a target or both. Some forms of Cyber Crime are-

  - ❖ Creating and sending Spam mails
  - ❖ Posting offensive messages on Social Networking Portals.
  - ❖ Hacking of Computer or Cracking Security systems.
  - ❖ Unethical Financial transactions and Fraud through Internet
  - ❖ Harassment through e-mails and web messages.
  - ❖ Cyber terrorism.
  - ❖ Creation & Propagation of Virus, Worms or Trojans etc.

- □ **Cyber Law :**

  Like traditional crime such as theft, fraud, forgery, defamation and mischief, Cyber Crime are also treated as criminal activities and are subject of punishment. The Information Technology Act 2000 (IT Act) in India provides legal support to the computer users against cyber crime. The Cyber Police have right in respect of all the offences committed under IT Act. It also deals with Intellectual property rights on Internet.

Wireless / Mobile Communication

- □ **GSM :**

  Global **S**ystem for **M**obile communications (GSM) is world's most widely used cell phone technology having 80% mobile phone users. It is a standard developed by the European Telecommunications Standards Institute (ETSI) to describe protocols for second generation (2G) digital cellular networks for mobile phones.

  The GSM standard was developed as a replacement for first generation (1G) analog cellular networks, and originally described a digital, circuit-switched network for voice telephony. This was expanded to facilitate GPRS (General Packet Radio Services).

- □ **CDMA :**

  Code **D**ivision **M**ultiple **A**ccess (CDMA) is an alternative cell phone technology to GSM. CDMA uses a "broad -spectrum" electromagnetic waves for signaling with wider bandwidth. This allows multiple people on multiple cell phones to be "communicated" over the same channel to share a bandwidth of frequencies. In CDMA technology, data and voice packets are separated using codes and then transmitted using a wide frequency range. CDMA is being used for 3G high-speed Internet access on mobile.

Wireless / Mobile Communication

- □ **3 G:**

  3G is the third generation of Wireless & Mobile technologies. It comes with enhancements over previous wireless technologies, like high-speed transmission, advanced multimedia access and global roaming.

  3G is mostly used with mobile phones and handsets as a means to connect the phone to the Internet or other IP networks in order to make voice and video calls, to download and upload data and to surf the net.

- □ **4 G:**

  4G is fourth-generation of wireless service, which refers to the next wave of high-speed mobile technologies that will be used to replace current 3G networks.

  4G wireless network is next step of 3G, which is currently the most widespread, high-speed wireless service.

  At present 4G is available in limited countries and areas.

Wireless / Mobile Communication

- □ **WLL (Wireless Local Loop):**

  In traditional telephone networks, phone would be connected to the nearest exchange through a pair of copper wires. Wireless local loop (WLL) technology simply means that the subscriber is connected to the nearest telephone exchange through a radio link instead of copper wires.

  WLL is basically the use of radio wave to provide a telephone connection to the home. In general, WLL is cheaper and quicker than copper wire connectivity.

- □ **Wi-Fi (Wireless Fidelity):**

  Wi-Fi is a very common wireless technology that was developed in the 1990s. It is used to connect machines in a Local Area Network (LAN). So, Wi-Fi is like a wireless version of Ethernet.

  Wi-Fi is technically referred to as the 802.11 protocol. Over time, Wi-Fi has improved, giving rise to different variations of the protocol like **802.11a (**allows 54 Mbps speed upto 100 feet), **802.11b** (allows 11 Mbps upto 300 feet) etc.

Internet & its Applications

□ Overview of Internet :

- **Internet** is a **network of networks** that consists of millions of private, public, academic, business, and government networks, that are linked by various wired, wireless, and optical networking technologies.
- The **Internet** is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to serve several billion users worldwide.
- The modern Internet is an extension of **ARPANet** (Advanced Research Project Agency Network), created in 1969 by the American Department of Defense.
- In 1990 the British Programmer **Tim Berners-Lee** devised Hypertext and HTML to create World Wide Web (WWW).
- The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW), the communicational infrastructure to support e-mail, chat and transfer of Text, Images, Audio, Video etc.

Internet & its Applications

□ Internet Applications :

- **WWW:** Word Wide Web (WWW) or Web is a collection of Hyper-linked pages accessed through Web Browser program using Hypertext Transfer Protocol (HTTP). A web page may contains information in form of text, images, audio, video or Animation.
- **Electronic Mail :** E-Mail allows you to send text messages as well as files as an attachment. Web-based e-mail service is offered free of cost through various portals like Gmail, RediffMail or Hotmail etc.
- **Instant Messaging (Chat):** It is similar to e-mail, except that message is sent immediately to recipient. It facilitates user to type and send messages to make conversation. It is also called Live Chat.
- **SMS & MMS:** Short Message Service or SMS is small text which can be sent to any mobile phone at no cost. Generally, this service is used by individuals or any organization to send Bulk-Message to promote a product, advertisement or greeting messages. Some service providers allows Multimedia Messages (MMS) which may contains pictures or small video along with text.

Internet & its Applications

□ Internet Applications :

- **Video Conferencing :** It is an application which allow two or more people at different locations to communicate by simultaneous two-way video and audio transmissions. Videoconferencing differs from videophone calls in that it is designed to serve a conference in group of people at multiple locations rather than individuals.
- **Voicemail** : It is also known as **voice message.** It is a computer based system that allows users to exchange personal voice messages or deliver voice information relating to individuals, organizations, products and services, using an ordinary telephone. The term is also used more broadly to denote any system of conveying a stored telecommunications voice messages, including using an answering machine. Most cell phone services offer voice-mail as a basic feature.
- **Voice Over Internet Protocol (VoIP):** It is technology which allows communication between PC and Mobile or Telephone using Internet at very little cost. Internet Protocol television (IPTV) allows user to listen music or see video films on PC using Internet.