Chapter 1:

Computer Networking

Informatics Practices

Class XII

By- Rajesh Kumar Mishra

PGT (Comp.Sc.)

KV No.1, AFS, Suratgarh

e-mail : rkmalld@gmail.com

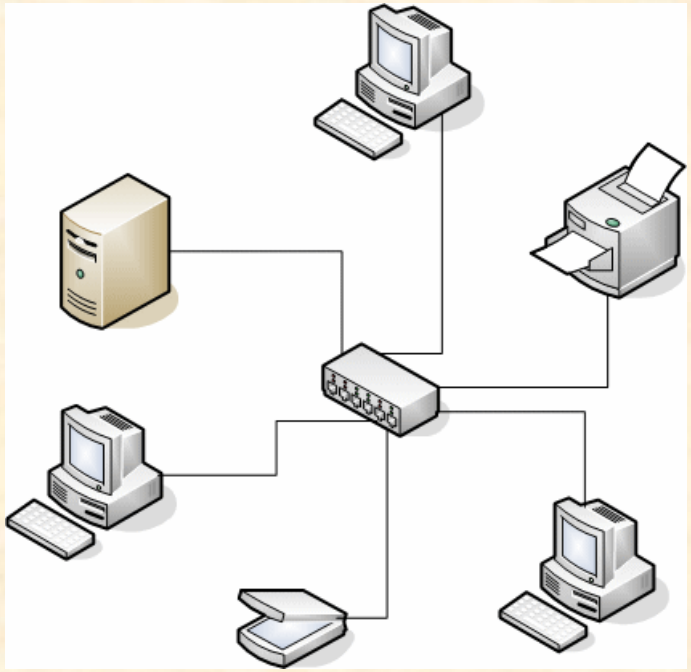
Introduction

- The advent of computer and communication technology have changed our daily life. Observe the following daily life examples-
  - Watching Cable TV
  - Cash Withdrawal from ATM
  - 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 like computers, which make Communication Network.
- The communication over network are possible through transfer of text/picture/audio/video data through wire or wireless transmission medium.

What is a Network?

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

  "A *computer network consists of two or more connected autonomous computers*."



Why we build a Network?

- Sharing Resources:

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

  Ex. Sharing database, program files, audio and video files, printer and scanners etc.

- Improved Communication:

  A computer network enables reliable, secure and faster communication between users. It saves our time and offers easy communication methods. Ex. 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 a very important role in sending and receiving text, image, audio and video data.

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: Information to be communicated. It may be text, images, sound or video.
- Medium: A transmission medium is a physical path through which the data flows from sender to receiver. A cable, fiber-optics or radio waves can be the medium.
- Protocol: A set of rules that govern data communication. It represents an agreement between the communicating devices.

Category of Network

- Peer-to-Peer (P2P): P2p networking type is most commonly used computer networks. All computers possesses same status within the network and no computer control any other computer but it self, this network does not have server to control and monitor. Security level is not towards higher side and each work station it self is responsible for security.
- Client-Server: Client-server model has one dedicated computer which is called server. Server is responsible to perform according to the request sent to it by clients. This concept is known as centralization, this enables server to keep profile of users, data, and software etc completely in tacked and organized.

Network Topologies

How computers to be connected ?

Network Topologies

- In order to form a network, computers must be interconnected in some layout.

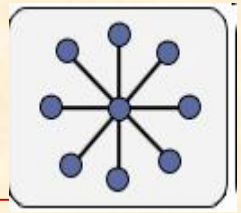
  The layout of interconnection of computers in a network is called Topology.

- The major types of Topologies are-

  (1) Star topology (2) Tree topology
  (3) Bus topology (4) Graph topology
  (5) Ring topology (6) Mesh topology

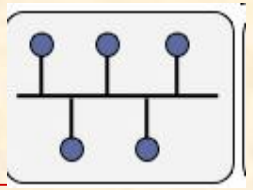
- The selection of topology for a network depends on the following factors-
  - Cost:- It includes cable/media cost and installation cost depends on the distance between nodes.
  - Flexibility:- Arrangement of furniture and walls in the building may affect the selection of topology and media.
  - Reliability:-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

Star Topology



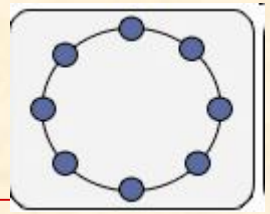
- This topology consists of a central node to which all other nodes are connected by a single path. It is most popular for LANs.
- Advantages:
  - Easy to setup and requires simple protocol.
  - Easy to locate fault in case of network failure.
  - It offers centralized control over the network.
- Disadvantages:
  - Increases cabling cost since each node is directly connected to the center 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 goes down then entire network rendered inoperable.

Bus Topology



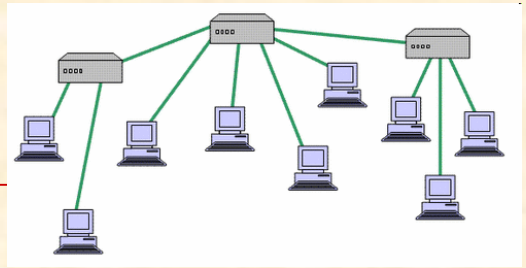
- In the bus topology, all devices are connected using a single cable. It is simple and oldest topology used in the early days of networking.
- Advantages:
  - Simple layout and requires less cables.
  - Easy to expand since node may be connected at any point on linear path.
- Disadvantages:
  - Detection of fault is quite difficult because there is no centralized control.
  - Node should be equipped with processing capability (intelligent) because it requires complicated protocols.
  - 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.

Ring Topology



- In a ring topology network, every node has exactly two neighbouring nodes. All messages travel in the ring in the same direction and passes through each node. The message is taken out from the frame 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 whole network.
  - Less reliable i.e. a failure in the cable or any node breaks the loop and entire network becomes down.

Tree Topologies

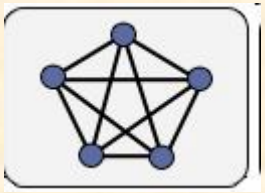


- Tree topology combines multiple star topologies together onto a bus. In its simplest form, only connecting port devices (hub or switch) connect directly to the tree bus, and works as a "root" of the network tree.
- This bus-star hybrid approach supports future expandability of the network much better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

Graph topology

- In Graph topology nodes are connected together in an arbitrary fashion. A link may or may not connect two or more nodes. Also there may be multiple link between two nodes.
- A path can be established in two-nodes via one or more links. It is extension of tree and bus network where node may interconnected to make a close loop or to provide alternative links.

MESH topology



- In Mesh topology each node is connected to more than one node to provide alternative route for data transmission. When every device connects to every other device then it is called a full mesh.
- Unlike each of the previous topologies, messages sent on a mesh network can take any of several possible paths from source to destination and offers faster and reliable network.
- It is commonly used in large internetworking environments with Star, Ring and Bus networks. It is ideal for distributed networks.

Types of Network

- A computer network may be small or big as per number of various types of computers linked together. Thus, networks vary in size, complexity and geographical area spread. On the basis of geographical spread, network may be classified as-
  - **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 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 share the resources among users.**
  - **WAN (Wide Area Network) : This type of network spreads across large geographical boundaries, 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.**
  - **PAN (Personal Area Network) : The PANs are small network, used to establish communication between computer and other 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.**

Transmission Media

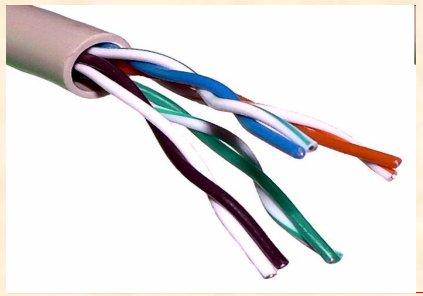
What is required to connect computers ?

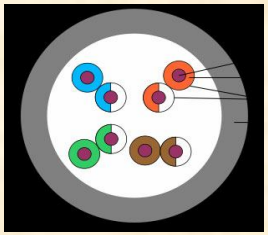
Transmission Media

- All the computers or connecting devices in the network, must be connected to each other by a Transmission Media or channel.
- The selection of Media depends on the cost, data transfer speed, bandwidth and distance.
- Transmission media may be classified as-
  - **Guided Media (Wired)**
    1. Twisted Pair Cable
    2. Coaxial Cable
    3. Optical Fiber
  - **Unguided Media (Wireless)**
    1. Microwave
    2. Radio wave
    3. Satellite
    4. Others (Blue tooth, Infrared and Laser etc.)

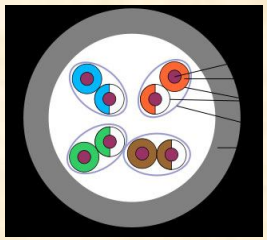
1.Twisted Pair Cables

- It is most common type of media consisting insulated pairs of wires twisted around each other. Twisting helps to reduce crosstalk and Electro Magnetic Interference.
- It comes in Shielded (STP) or Unshielded Twisted Pair (UTP) types. In UTP, pairs are covered by an extra insulation to further reduce the signal interference.
- CAT 5 and CAT 6 are commonly used in the networking.
- Advantages:
  - It is simple, flexible, low weight and inexpensive.
  - 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

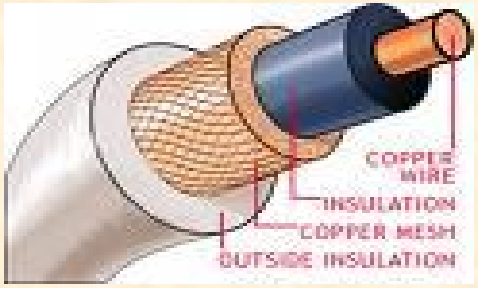


STP

RJ-45 Connector

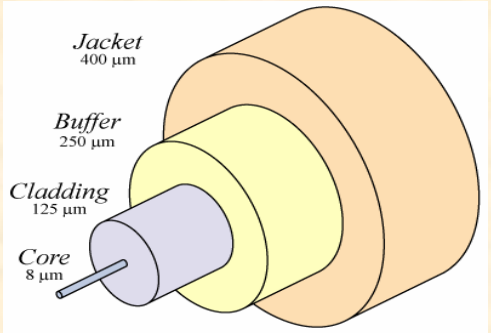
2.Coaxial cable

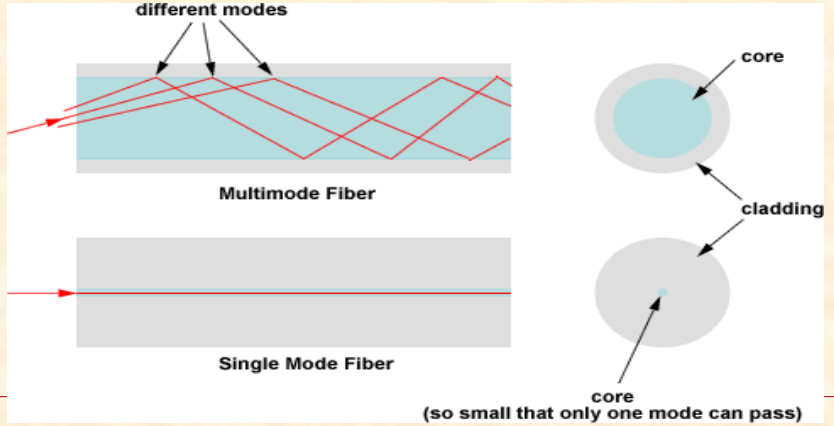
- This types of cable consists a solid insulated wire core surrounded by wire mesh or shield , each separated by some find of foil or insulator. The inner core carries the signal and mesh provides the ground. Co-axial Cable or **coax**, is most common in Cable TV transmission. Generally it is used in Bus topology network.
- It is two type- Thinnet (185 mt), Thicknet(500 mt)
- A connector known as a *vampire tap* or BNC connector to connect network devices.
- **Advantages:**
  - It offers high bandwidth and better speed than other cables.
  - Suitable for Broadband transmission (cable TV) and can be used in shared cable network.
- **Disadvantages:**
  - It is 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 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. Also 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.
  - Complicated Installation procedure and difficult to join two fiber or broken fiber.
  - Not suitable for domestic purposes due to high maintenance cost.





Wireless Transmission Medium

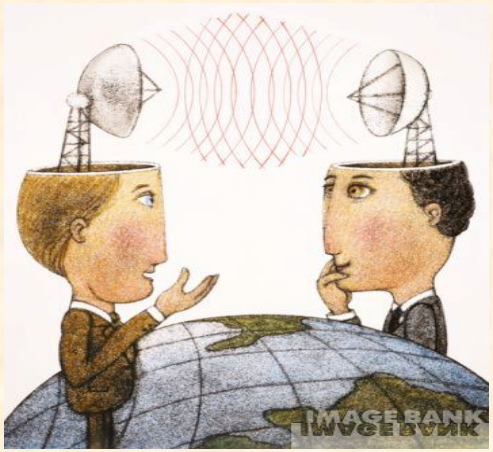
- Wireless networks are becoming increasingly popular, and they utilize a different type of technology.
- Wireless communication uses Satellite, Microwave, Radio Wave and Other short frequencies waves like infrared to transmit data.
- No physical medium is necessary for wireless signals, making them a versatile way to build a network.
- The data-transmission rates are highr than wired media.

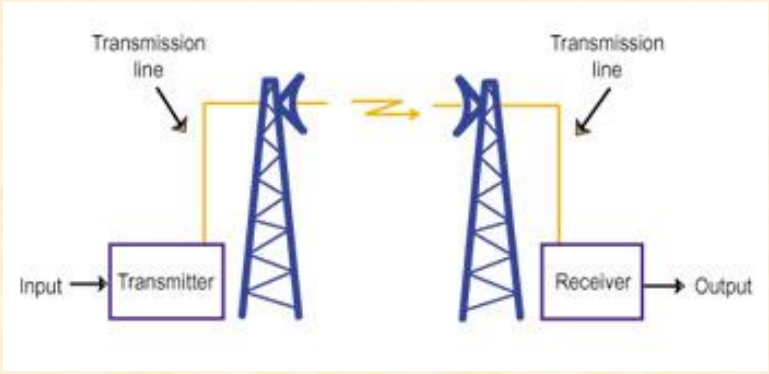
Uses of Wireless

- 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

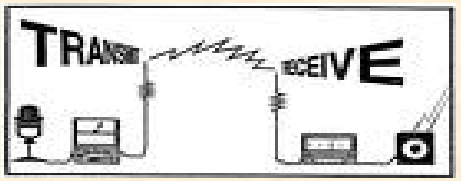
1. Microwave

- Microwaves are high energy radio waves that are used for line of sight communication between a pair of communication devices equipped with Parabolic antenna.
- Satellite communication is possible with microwaves.
- **Advantages:**
  - Suitable for high speed and long distance (upto 100 km.) communication.
  - No need for lying cable and offers 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.



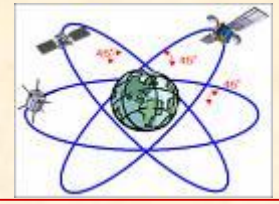


2. Radio Wave

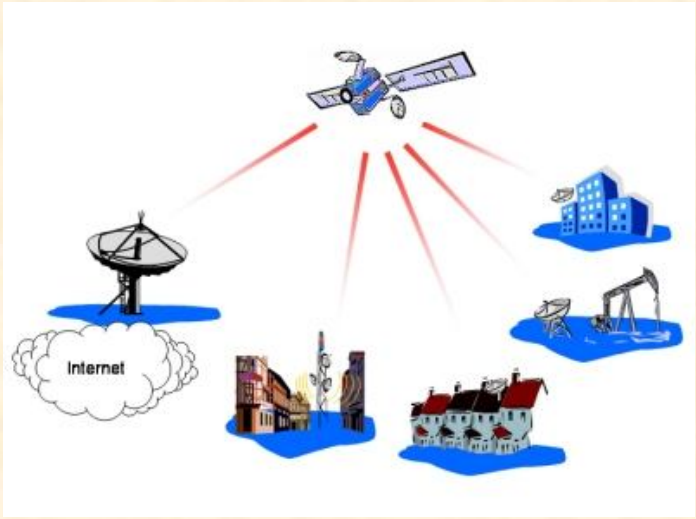


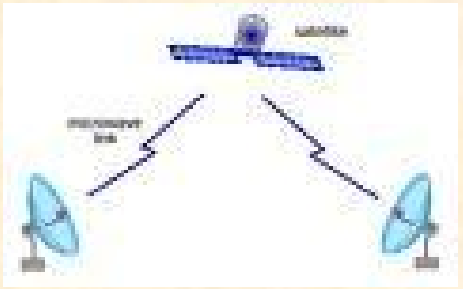
- Radio communication uses Radio frequencies like Medium Wave, Short Wave, VHF and UHF.
- Signal are modulating on a high speed Radio wave carrier frequency using Amplitude Modulation (AM), Frequency Modulation (FM) and Phase Modulation (PM).
- Generally it is used to make Broadcast Network within a range.
- **Advantages:**
  - It covers a larger span of spared and offers mobility.
- **Disadvantages:**
  - Expensive and Insecure communication.
  - It is susceptible to whether effects.

3. Satellite



- Satellite communication is done over the microwave frequency range. 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.
- **Advantages:**
  - It covers a larger geographical area of the earth.
  - Offers secure, uninterrupted and high quality transmission.
- **Disadvantages:**
  - Very expensive and operating cost.
  - Slower than Microwave transmission.





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 standard communications protocol primarily designed for low power consumption, with a short range.

5. Infrared

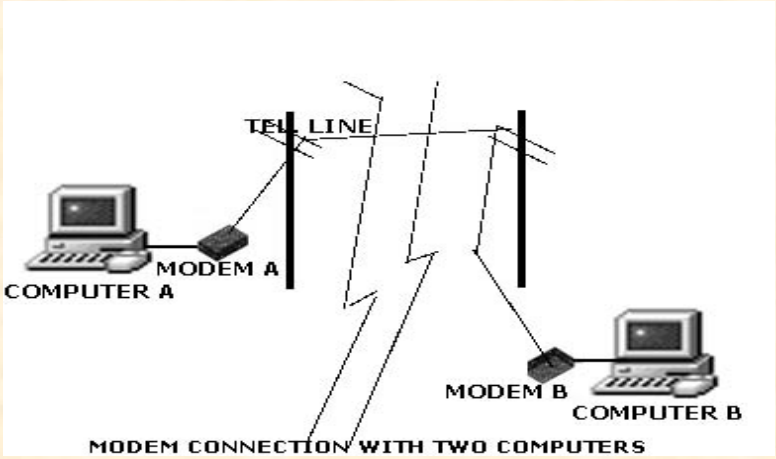
- **Infrared** technology allows computing devices to communicate via short-range wireless signals.
- The infrared transmission technology used in computers is similar to that used in electronic consumer product with remote control units.
- The range is about 5 meters.
- Infrared Communication is very agile and is affected by various factors including angle, distance, noise and heat.
- The biggest drawback in infrared communication is its range and angle problems which makes its impossible for modern day mobility needs to be fulfilled by this protocol.

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-
  - Modem
  - Hub
  - Switch
  - Router
  - Bridge
  - Gateway
  - Repeater

1. MODEM

- A MODEM (MOdulator-DEModulator) 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 Internal or External type. Now days DSL Modem is used to access Broadband Internet.



MODEM CONNECTION WITH TWO COMPUTERS

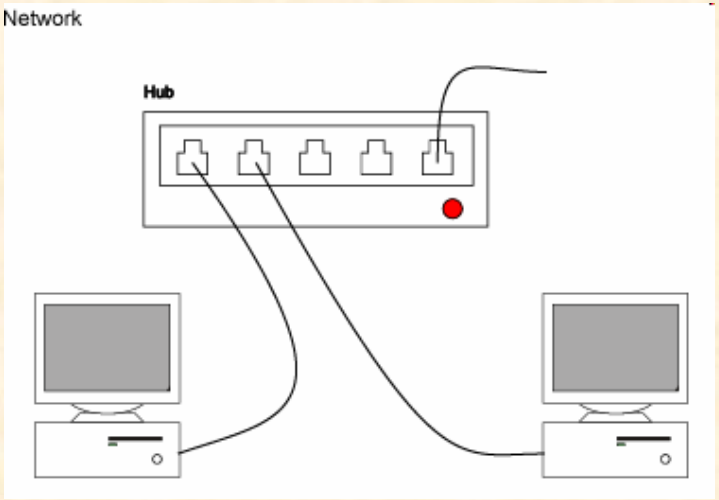
2. Hub & Repeater

- A Hub or Concentrator is a connecting device which connects multiple computers together to form a LAN.
- It provides various RJ-45 ports to connect Twisted Pair cable in STAR topology and making them act as a single network segment.
- Hubs make Broadcast type Network and do not manage traffic that comes through them. Signal entering any port is broadcast out on all other ports.

- Type of Hub
  - **Active Hub:**

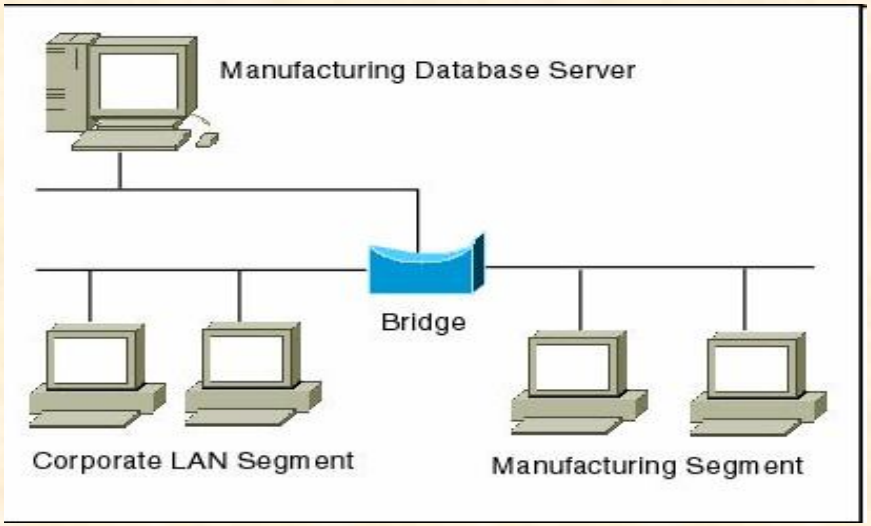
    Amplify the signal when required and works as a **Repeater**.
  - **Passive Hub:**

    It simply passes the signal without any change.



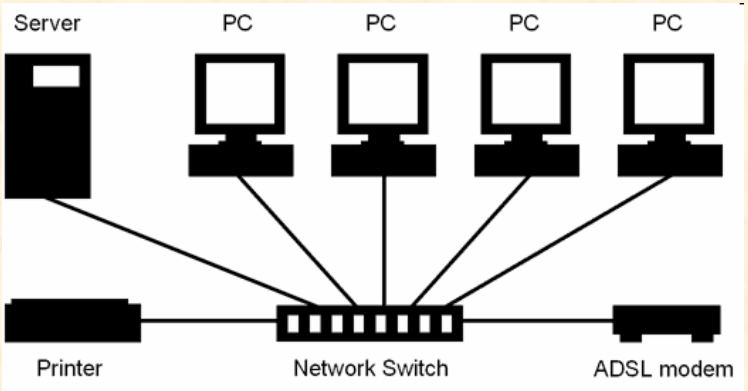
3. Bridges

- Bridges are used to connect two LAN or two segment of the same LAN or divide a large network into smaller segments. Connecting LANs must have the same Protocol.
- Unlike repeaters, bridges contain logic that allows them to keep traffic for each segment separate. This way bridges provide some security to the individual segments.
- When a data frame enters a bridge, it not only regenerates the signal but also checks its destination and forwards only to the segment to which the address belongs.



4. Switch

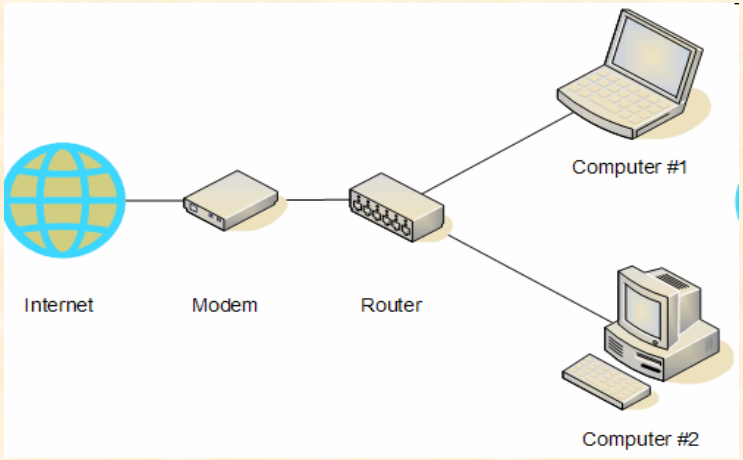
- Switch is a device that is used to segment network into different Sub-networks (Subnet) to control the network traffic. It provides bridging functionality with greater efficiency.
- It is responsible for filtering data in a specific way and for forwarding packets between LAN segments.
- A switch has a buffer that stores the packets from the sender and checks the address to find out the outgoing link. If the outgoing link is free the switch sends the packet to the particular link.
- Modern day switches are equipped with Router functionalities and offers faster throughput than Hubs.



Example 1: A wired client-server network

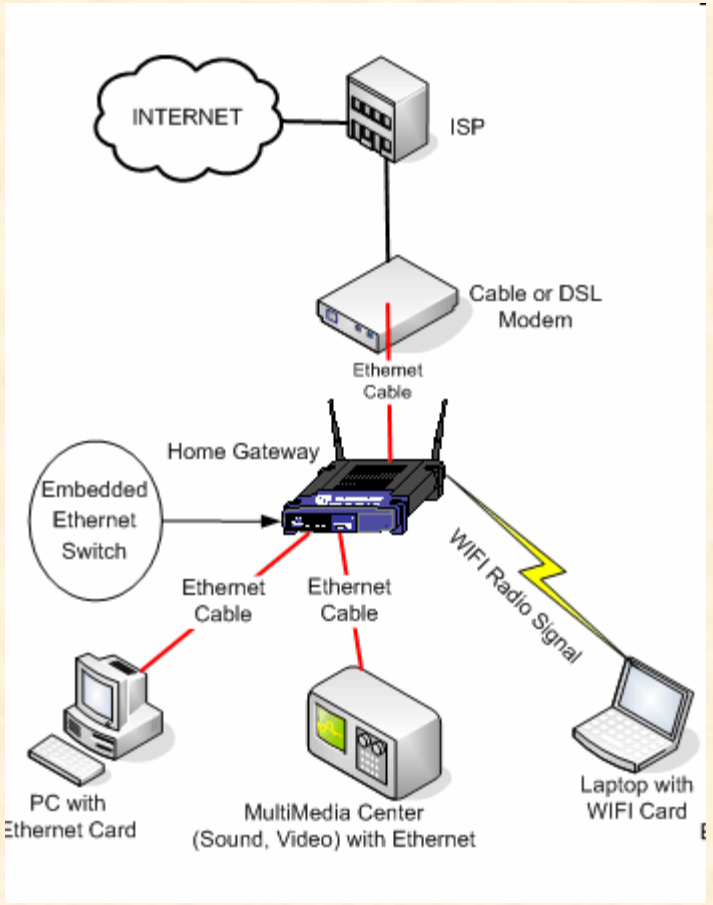
5. Router

- Router is a networking device which connect multiple Networks irrespective of their Protocols.
- Routers works at IP Address where as Bridge works at MAC address.
- Routers have the intelligence to determine the best possible route for data packets to travel. There are a number of routers present in large network to aid in speedy delivery of data packets.
- Router maintains a table of addresses (called routing table) that keeps a track of delivery paths of data packets.



6. Gateways

- A Gateway is a device that connects dissimilar networks. It establishes connection between LAN and External Network with different structure.
- A Gateway is a protocol converter that connects two dissimilar networks having different protocols i.e. It can accept a packet formatted for one protocol (e.g. AppleTalk) and convert it to a packet formatted for another protocol (e.g. TCP/IP) before forwarding it.
- 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.



Terminology of Networks

How a Network Works ?

Terms used in the Networks

- **Workstation (Node):**

  The term node reefers to a computer when it is attached to the network. It is equipped with processing capability, memory and storage and OS.

- **Server:**

  A computer that facilitates the sharing of data, software and devices like printer, scanners and modem etc. on the network is called server.

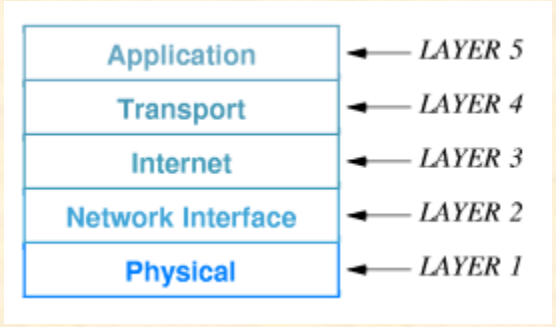
- **Network Interface Unit:**

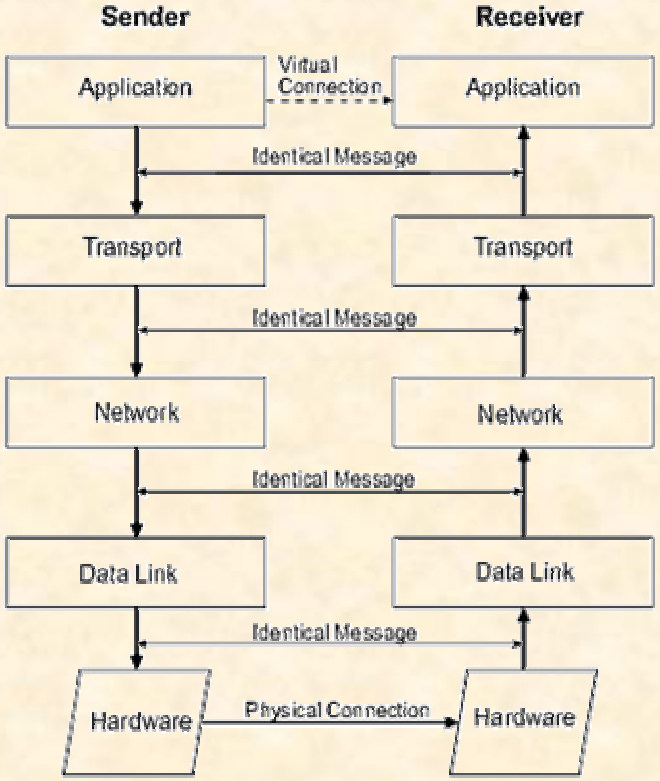
  A Network Interface Unit establishes communication between computer and rest network. Generally a node pr PC is equipped with Network Interface Card (NIC) or LAN card with connecting port, which makes connection to the network.

  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.

TCP/IP Protocol

- The **Transmission Control Protocol/ Internet Protocol Suite** (**TCP/IP**) is the set of communications protocols used for the LAN, Internet and other similar networks.
- The Internet Protocol Suite, may be viewed as a set of layers. Each layer solves a set of problems involving the transmission of data, and provides a well-defined service to the upper layer protocols based on using services from some lower layers.
- It comprises 5 Layers including Physical media. Each layer is responsible for a well defined task.





MAC Address

- Each Computer or node on a network needs a special circuit known as 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 identification purpose. A MAC address is like a phone number by which any other machine on the network can communicate.
- In a networks, the MAC address uniquely identifies each node on that segment and allows frames to be marked for specific hosts.

IP Address

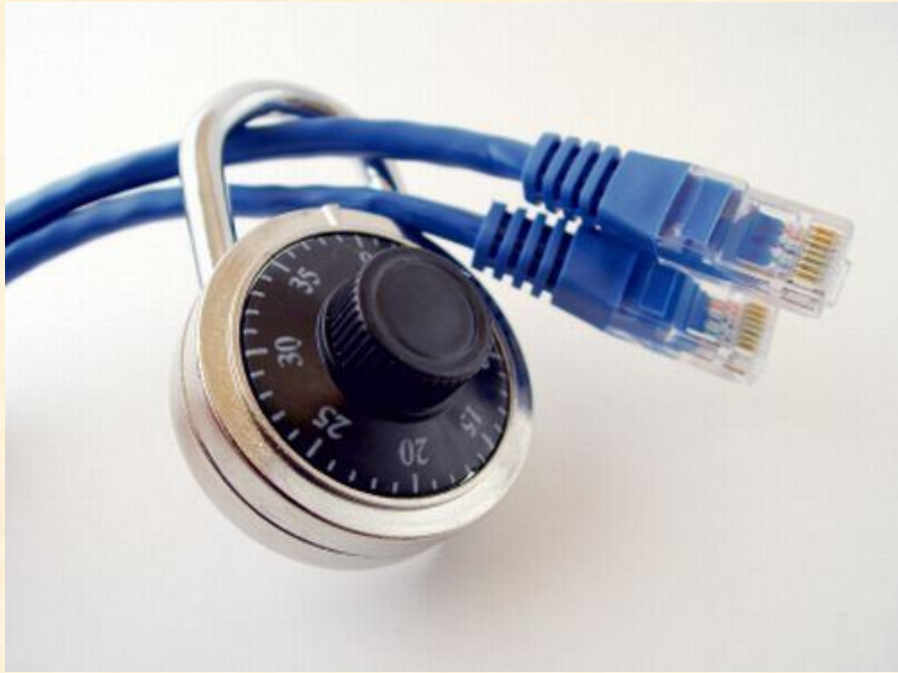
- All the computers on the Network follow the some set of rules (Protocol) for communication to each other. One of the most common protocol is TCP/IP. Internet also follows this protocol. Each machine in TCP/IP network needs to have a unique 32 bit address called IP address.
- The IP address may be static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

Domain Name

- In simple term, Domain name is a unique group name assigned to a web server or web site.
- Some common domains on the Internet are- .com, .org, .edu, .net, .gov and country domain like .in, .ca, .jp etc.
- The complete unique address of the website is called URL (Universal Resource Locator) like www.google.com
- Since computers on the network are identified by its IP addresses, so it is required to convert a Domain name into its corresponding IP address, This is called Domain Name Resolution.
- Domain Name Resolution is done by the designated servers called Domain Name Service (DNS) servers. When you type an URL on the web browser program, your request is forwarded to nearest DNS server to obtain its IP address over the Internet. A domain name is an identification label that defines a realm of administrative autonomy, authority, or control in the Internet, based on the Domain Name System (DNS)
- A hostname is a domain name that has at least one IP addresses associated.

Network Security

How you can secure your Network?



Introduction

- Network Security is a process of providing security at the boundaries of an organizational network by keeping out unauthorized access.
- Some common Network threats are-
  - Intrusion / Access Attack
    - Snooping
    - Eavesdropping
    - Spamming
    - Phishing
  - Denial of Service (DoS) attack
  - Malicious Program (Virus, Worm, Trojon Horses)

Intrusion / Access Attack

- In this type of threat, an un authorized user attempts to gain access to sensitive information.
- **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 emails and other private information.
- **Eavesdropping**

  It the act of secretly listening/ interpreting someone else's private communication or information.
- **Spamming**

  Spamming refers to the sending of bulk-mail by an identified or unidentified sources.
- **Phising**

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

Denial of Service (DoS) 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 attack are-
  - **Denial of Access to Information**
  - **Denial of Access to Applications.**
  - **Denial of Access to Systems**
  - **Denial of Access to Communication**

Malicious Program

- **Virus:**

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

- **Worm:**

  It is 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.

How to protect yourself ..

- 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

- **Authorization**

  User Authorization is done by a valid Login Id etc. (Some thing Know?)

- **Authentication**

  User is Authenticated by a valid password etc. (Something have ?)

- **Firewall**

  It is a System (H/w or S/w) to prevent authorized access to or from a private network.

- **Intrusion Detection System (IDS)**

  It is system which identifies various Intrusion and monitors the system and Network resources and activities. It notifies to authorities in case suspicious happenings.

- **Anti-Malicious Program**

  These are the program which prevent the system from various malicious programs like Virus, Worms, Spywares and Trojan horses etc.

Preventive Measures

- **Install a reliable Antivirus and Anti-Spyware program.**
- **Keep your Anti-virus program update.**
- **Think twice before downloading anything from Internet. (Down load 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.**
- **Keep your e-mail address, passwords etc. private.**
- **Install Firewall to prevent unauthorized access to or from a private network.**
- **Disconnect Internet when it is not in use.**