COMPUTER NETWORKING
CHAPTER 1

LEARNING OBJECTIVES

After learning this chapter, the students will be able to:

- Define what a Computer Network is
- List the benefits of networking
- List different wired and wireless media for communication
- Identify different network devices
- Identify different types of Network Topologies
- Identify the type of network on the basis of area covered
- Describe various terms associated with computer networks.
- List various network security concepts and security threats to computer networks
- List the preventive and corrective measures against these threats
- Understand various internet applications
- Understand wireless/mobile communication

INTRODUCTION

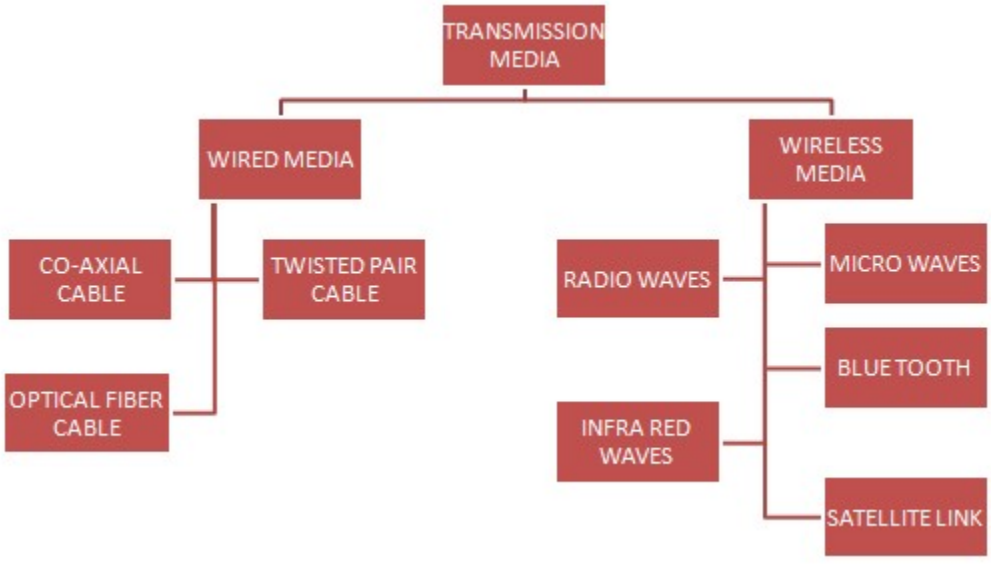
A **computer network** is a collection of interconnected computers and other devices which are able to communicate with each other and share hardware and software resources.

Advantages:

- **Resource Sharing**: Data, Hardware resources (Modem, Hard Disk, DVD Drive, Scanner etc.) and Software resources (Application Software, Anti-Virus tools etc.) can be easily shared on computer networks by connecting these devices to one computer(server).
- **Cost saving**: Sharing of resources in computer networking leads to cost saving.
- **Improved Communication**: A computer network enables fast, reliable and easy communication among its users. We can easily communicate with anyone through email, video conferencing or chatting through networking.
- **Time saving**: It takes negligible time to send and receive messages, audio, video and images on a computer network. We can easily watch live videos and can talk live to anyone sitting in some other corner of the world on the computer network. This leads to time saving.
- **Increased storage**: On a computer network, same data is replicated on multiple computers to ensure the availability of data in case of some computer getting faulty. Mostly the data is kept on servers and is shared with legitimate users. This ensures data security and reliability.

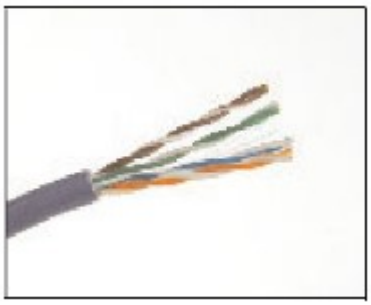
Networking Hardware

Transmission/Communication Media- A transmission medium is a medium of data transfer over a network. It can be wired or wireless.



Wired Media- It includes various types of cables which are used to transfer data over computer networks.

1.Twisted Pair Cable – This is one of the common forms of wiring in networks, especially in LANs and it consists of four pairs of two insulated wires arranged in a regular spiral pattern (double helix). These pairs are colour coded. An RJ-45 connecter is used to connect this cable to a computer.



Advantages:

(i) It is easy to install and maintain.

(ii) It is very inexpensive

(iii) It is an adequate and least expensive medium for low speed (up to 10 mbps) applications where the distance between the nodes is relatively small.

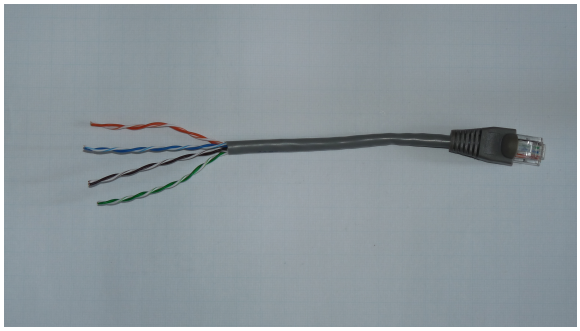
Disadvantages:

(i) It is incapable to carry a signal over long distances without the use of repeaters.

(ii) Due to low bandwidth, these are unsuitable for broadband applications.

Twisted pair cable is of two types:

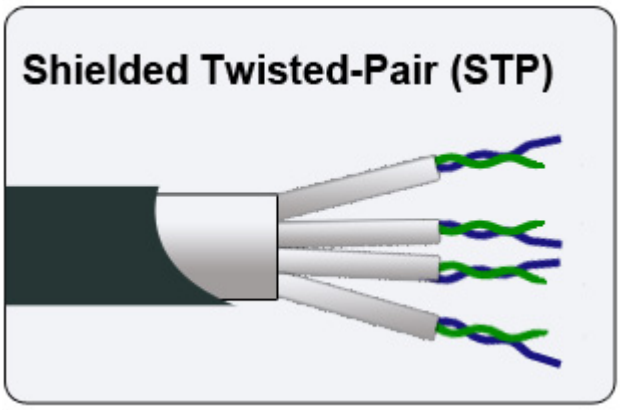
UTP (Unshielded Twisted Pair): As the name suggests in UTP cables individual pairs are not shielded. UTP has become the most closely identified cable for Ethernet, and is therefore called **Ethernet cable**. Ethernet cables are used to attach the computer to the modem to set up the internet connection at home or office.



Characteristics of UTP cable:

i. It is a low-cost cable available for setting up small networks.
ii. It is a thin (External diameter app. 0.43cm) and flexible cable and therefore it offers ease of installation.
iii. It can carry data upto a length of 100m at a stretch.

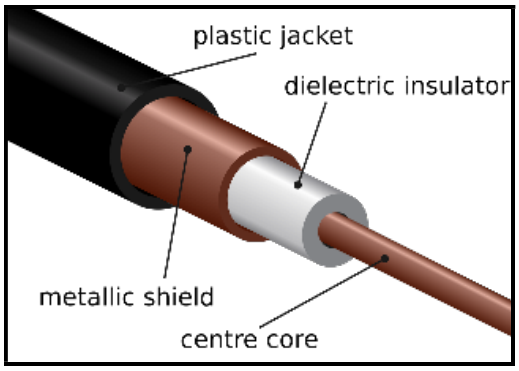
STP (Shielded Twisted pair): It is the same cable as the UTP, but with each pair shielded individually. An outer shield then covers all the pairs like in UTP. STP data connectors are used to connect STP cable to the computer. RJ-45 connectors can also be used to connect this cable to a computer.



Characteristics of STP cable:

i. As compared to UTP, STP offers better immunity against internal and external electromagnetic interferences.
ii. It is expensive than UTP cable.
iii. As compared to UTP cable, STP cable is difficult to install.

2. **Co-axial cable (or coax)-** It is the most commonly used transmission media for LANs. It is widely used for television signals and also by large corporations in building security systems. Multi-channel television signals can be transmitted around metropolitan areas at considerably less cost.



Advantages-

(i) It can carry data for a larger distance (185m - 500m) at a stretch.

(ii) Less susceptible to electromagnetic fields.

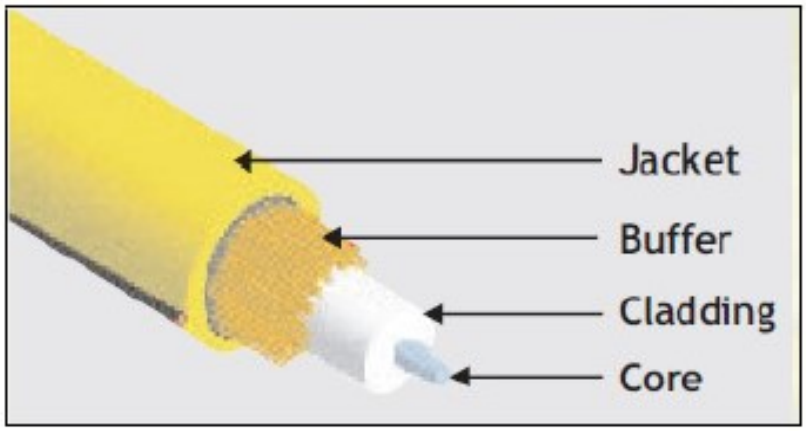
(iii) It offers high bandwidth (up to 400 mbps).

Disadvantages-

(i)Bulkier and less flexible than twisted pair.

(ii)Due to its thickness (1cm diameter) and less flexibility, it is difficult to install as compared to twisted pair cable.

3. **Optical Fiber cable –** Optical fibers offer a very high bandwidth and this makes it capable of multichannel communication.



Advantages-

(i)It can carry data for a very large distance at a stretch.

(ii)Not susceptible to electromagnetic fields

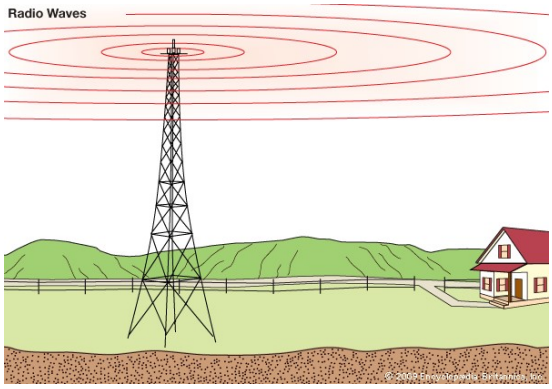
Disadvantages-

(i)Especially skilled people are required to install optical fiber cables.

(ii)Till date it is the most expensive and at the same time the most efficient cable available for computer networks.

Wireless Media

1. **Radio Waves -** They are widely used for communication, both indoors and outdoors. Cordless phones, AM and FM radio broadcast, Garage door openers etc. are examples of radio wave transmission.



ADVANTAGES

(i)It offers ease of communication over difficult terrain.

(ii)These waves are omni-directional, so the transmitting and receiving antennas need not be aligned.

DISADVANTAGES

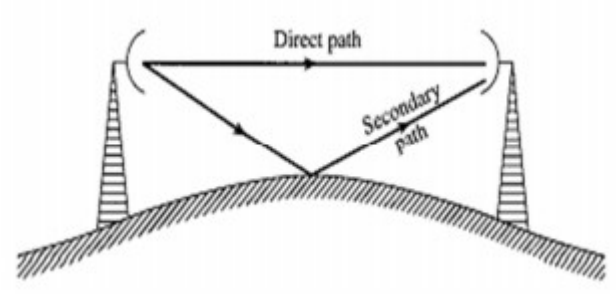
(i)The transmission can be interfered by motors or other electrical equipment

(ii)Permission from concerned authorities is required for use of radio wave transmission.

(iii)Less secure mode of transmission

(iv)Radio wave propagation is susceptible to weather effects like rains, thunder storms etc.

2. **Micro Waves:** Microwaves travel in straight lines and cannot penetrate any solid object. Therefore, for long distance microwave communication, high towers are built and microwave antennas are put on their top.



In the big cities where land is very costly and a lot of formalities have to be completed to get permission to dig land for cabling, microwave antennas can be put on top of high rise buildings and communication can be started in a short time.

ADVANTAGES

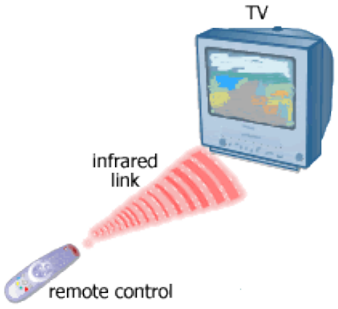
(i)Free from land acquisition rights

(ii)Offers ease of communication over difficult terrain

DISADVANTAGES

(i)The transmission is in straight lines so the transmitting and receiving antennas need to be properly aligned. (line of sight transmission)

3. **Infrared Waves:** These waves are used for short range communication (approx. 5m). Home-entertainment remote-control devices, Cordless mouse, and Intrusion detectors are some of the devices that utilize infrared communication.



ADVANTAGES

(i)It is a line of sight transmission; therefore, information passed to one device is not leaked to another device.

(ii)No government license is required for their use

DISADVANTAGES

(i)It is a line of sight transmission, therefore at a time only two devices can communicate.

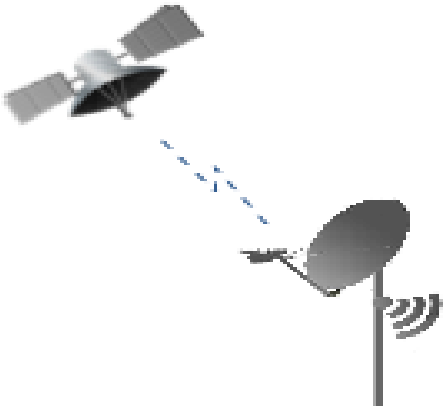
(ii)Performance drops with longer distances

4. **Bluetooth-** This technology is used for short range communication (approx. 10m). Baby monitors, door openers, and cell phones are some of the devices that utilize Bluetooth communication.

ADVANTAGES
(i)Line of sight between communicating devices is not required.
(ii)Bluetooth can connect up to eight devices simultaneously.

DISADVANTAGES
(i)Slow data transfer rate (upto 1Mbps).

5. **Satellite Link:** Satellite links are used for very long distance wireless communication which may range from intercity to intercontinental. The satellite system is very expensive but its area coverage and fringe benefits compensate for the expenses.

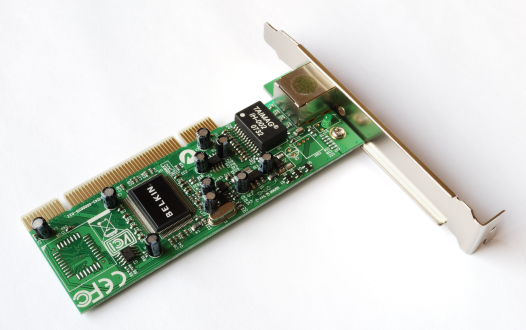


ADVANTAGES
(i)Satellites cover large area of earth
(ii)Since communication over very long distances is possible, this becomes a commercially attractive option.
DISADVANTAGES
(i)This system is expensive
(ii)Requires legal permissions

Network Devices

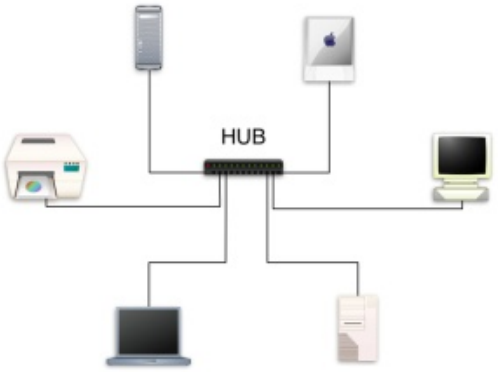
Other than the transmission media many other devices are required to form computer networks. Some of these devices are:

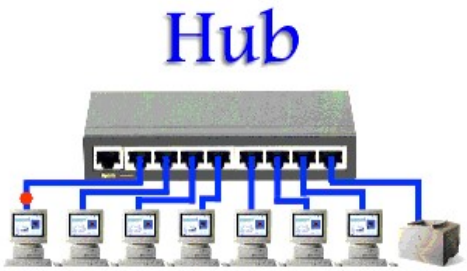
1. N**IC(Network Interface Card):**An **NIC** (Network Interface Card) is a device that enables a computer to connect to a network and communicate. Any computer which has to be a part of a computer network must have an NIC installed in it.



2. **MODEM:** A **modem** (Modulator - Demodulator) is a peripheral device that enables a computer to transmit data over, telephone or cable lines. It converts the digital data from the sender computer into analog form to be able to send it over telephone lines. At the receiving end modem converts the data from analog form to digital form and stores into receiving computer.

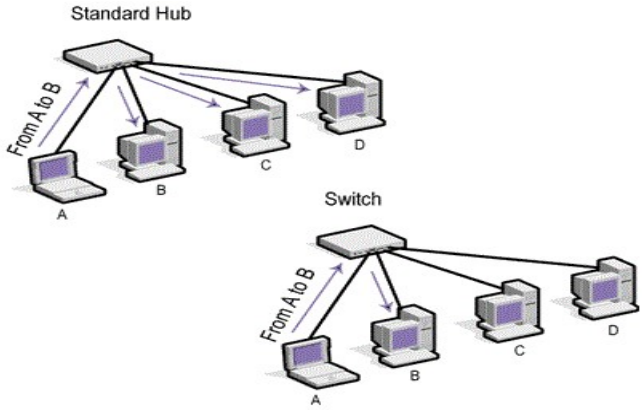
3. **HUB**: A **Hub** is an electronic device that connects several nodes to form a network and redirects the received information to all the connected nodes in broadcast mode. The computer(s) for which the information is intended receive(s) this information and accept(s) it. Other computers on the network simply reject this information.



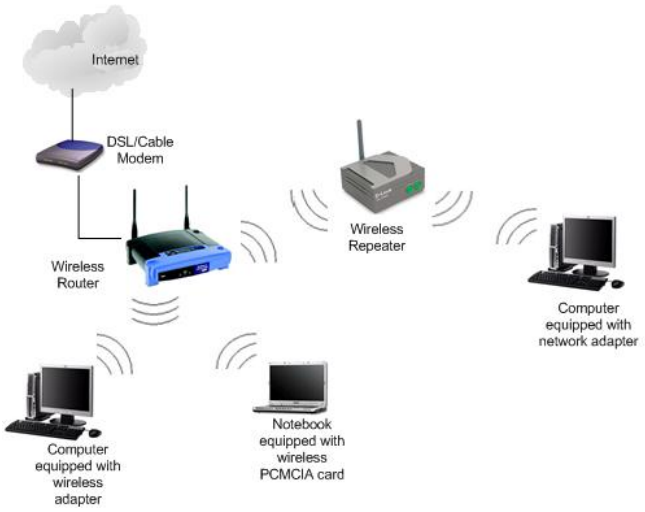


4. **SWITCH**: A **Switch** is an intelligent device that connects several nodes to form a network and redirects the received information only to the intended node(s).

The difference between the two is that Hub broadcasts the received information to all the nodes. Switch does not broadcast instead sends the information selectively only to those computers for which it is intended. This makes a switch more efficient than a hub.



5. **Repeater:** A **Repeater** is a device that is used to regenerate a signal which is on its way through a communication channel. A repeater regenerates the received signal and re-transmits it to its destination.

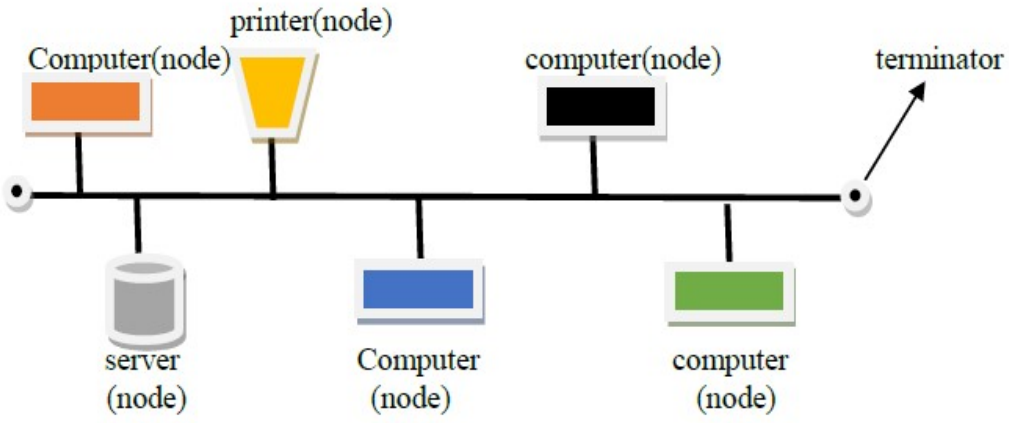


6. **Gateway:** A **Gateway** is a device, which is used to connect different types of networks.

Network Topologies

A **Topology** is an arrangement of physical connections among nodes in a network. There exist different network topologies:

1. **Bus Topology:** In bus topology, all the nodes are connected to a main cable called Backbone.

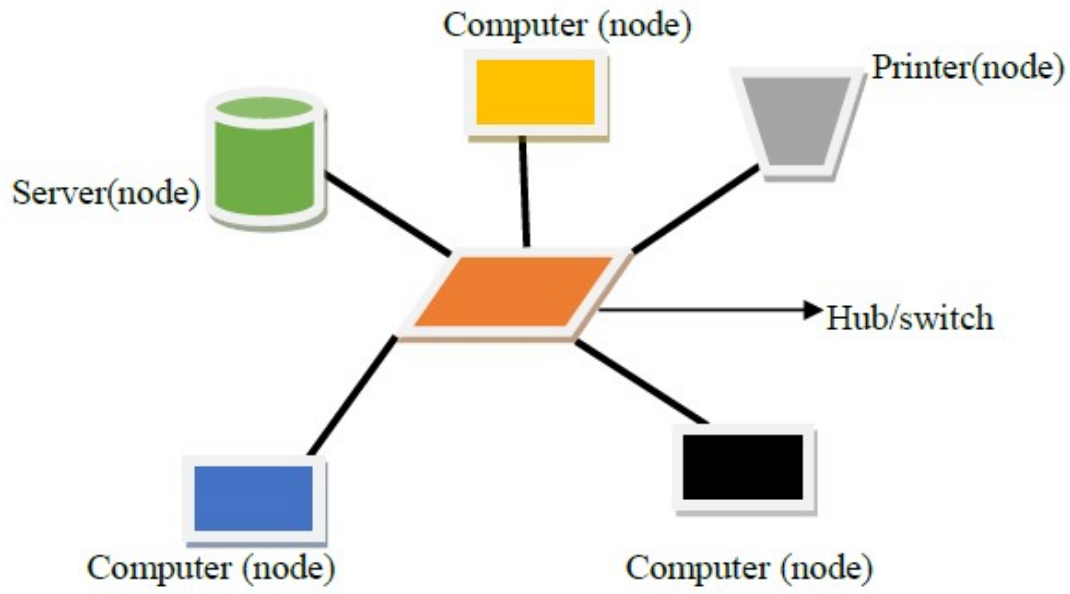


ADVANTAGES
(i)It is easy to install.
(ii)It requires less cable length and hence it is cost effective.

DISADVANTAGES
(i)In case of cable (backbone) or terminator fault, the entire network breaks down.

(ii)Fault diagnosis is difficult.
(iii)At a time only one node can transmit data.

2. **Star Topology:** In star topology, each node is directly connected to a hub/switch.



ADVANTAGES
(i)It is easy to install.
(ii)It is easy to diagnose the fault in Star topology.
(iii)It is easy to expand depending on the specifications of central hub/switch.

DISADVANTAGES
(i)Failure of hub/switch leads to failure of entire network.
(ii)It requires more cable length as compared to bus topology.

3. **Tree Topology:** Tree topology is a combination of bus and star topologies. It is used to combine multiple star topology networks.

ADVANTAGES
(i)It offers easy way of network expansion.
(ii)Even if one network (star) fails, the other networks remain connected and working.

Network Protocols

A **network protocol** is a set of rules for communication among networked devices. These Protocols are HTTP, TCP/IP, PPP.

1. **HTTP (Hyper Text Transfer Protocol):** HTTP is used to transfer all files and other data (collectively called resources) from one computer to another on the world wide web.

1. **TCP/IP (Transmission Control Protocol / Internet Protocol):** Communication between two computers on internet is done using TCP/IP protocol. TCP/IP is a two-layer protocol. When data is to be sent from one computer to another over internet, it is first broken into smaller packets which are actually sent. When these packets are received by the receiver computer, they are assembled into the original message. This job of dividing the original message into packets and re-assembling the received packets into the original message is done following TCP protocol. Internet protocol is followed to ensure that each of these packets gets to the right destination. Different packets from the same message may be routed differently, but they reach the same destination and are reassembled there.

2. **PPP (Point to Point Protocol):** It is a protocol for direct communication between two computers, typically a personal computer connected by phone line to a server. PPP is used over many types of physical networks including cellular telephone, serial cable, phone line, trunk line, specialized radio links, and fiber optic links.

3. **TEAM VIEWER:** Team Viewer is a computer software package for remote control, desktop sharing, online meetings, web conferencing and file transfer between computers. People can use Team viewer for presentations, watching videos, work on presentations, etc. Up to 25 members can be added at a time.

Types of Networks: On the basis of area covered computer networks are classified as:

1. **PAN - Personal Area Network**- A PAN is a network of communicating devices (Computer, Phone, MP3/MP4 Player, Camera etc.) in the proximity of an individual. It spans an area of around 10 m radius. A PAN can be set up using guided media (USB cable) or unguided media (Bluetooth, Infrared).

2. **LAN - Local Area Network-** A LAN is a network of computing/Communicating devices in a room, building, or campus. It can cover an area of a few meters to a few kilometers radius. Sometimes it spans a group of nearby buildings.

3. **MAN - Metropolitan Area Network**- A MAN is a network of computing/communicating devices within a city. It can cover an area of a few kilometers to a few hundred kilometers radius. A network of schools, banks or Government offices etc. within a city, are examples of MANs. A good example of a MAN is the interconnected offices of a state government.

4. **WAN -Wide Area Network**- A WAN is a network of computing/communicating devices crossing the limits of a city, country, or continent. It can cover an area of over hundreds of kilometer radius. A network of ATMs, BANKs, National Government Offices, International Organizations' Offices etc., spread over a country, continent, or covering

many continents are examples of WANs. The best-known example of a WAN is the internet.

Identification of computers and users over a network

1. **MAC (Media Access Control) address-** A machine with an NIC can be identified uniquely through its NIC's (Network Interface Card) MAC address. MAC address of an NIC is permanent and does never change. For example, in the following MAC address,

   00:A0:C9 : 14:C8:35

   The prefix 00:A0:C9 indicates ID number of the adapter manufacturer. The second half (14:C8:35) of a MAC address represents the serial number assigned to the adapter (NIC) by its manufacturer.

2. **IP Address-** Every machine in a network has another unique identifying number, called its IP Address. An IP address is a group of four bytes (or 32 bits) each of which can be a number from 0 to 255. A typical IP address looks like this:

   59.177.134.72

   On a network, IP address of a machine is used to identify it. MAC address is used only when a specific machine is to be targeted. For example, suppose we want to block a specific PC to access some network resource. If we use the PCs IP address, then the PC is not blocked permanently as its IP address may change when it connects to the network next time. Instead, we use the PCs MAC address for this purpose.

   IP Address Vs MAC Address

   (i)The IP address is assigned by the network administrator or the internet service provider while the MAC address is assigned by the manufacturer.
   (ii)If a computer is transferred from one network to another, its IP address gets changed where as the MAC address remains the same.

3. **Domain Name:** In context of internet, a **Domain Name** is a name assigned to a server through Domain Name System (DNS). Examples of some domain names are cbse.nic.in, sikkimipr.org, indianrailway.gov.in etc. Domain names are used in URLs to identify particular Web servers. For example, in the URL *http://www.cbse.nic.in/welcome.htm*, the domain name is *www.cbse.nic.in*

A domain name usually has more than one part: top level domain name or primary domain name and sub-domain name(s). Top level domains are divided into two categories: Generic Domain Names and Country-Specific Domain Names. For example:

Generic Domain Names:

- **.com** - commercial business
- **.edu** - Educational institutions
- **.gov** - Government agencies
- **.mil** - Military
- **.net** - Network organizations
- **.org** - Organizations (nonprofit)

Country Specific Domain Names:

- **.in** - India
- **.au** - Australia
- **.ca** - Canada
- **.ch** - China
- **.nz** - New Zealand
- **.pk** - Pakistan
- **.jp** - Japan
- **.us** - United States of America

Domain Name Resolution is the process of getting corresponding IP address from a domain name.

Suppose you mention a URL in the web-browser to visit a website. The browser first checks your computer to find if the IP address of the server corresponding to the Domain Name (embedded in the URL) is present. If this address is present then with the help of this address, the corresponding server is contacted and then the website opens in your browser. Otherwise the browser sends this domain name to some specific servers (called domain name servers) to find the corresponding IP address. Once the IP address is known, the server is contacted and then the website opens in your browser.

Network Security Concepts

CYBER LAW: Cyber law is an attempt to integrate the challenges presented by human activity on the internet with legal system of laws applicable to the physical world.

FIREWALL: A firewall is hardware or software based network security system. It prevents unauthorized access (hackers, viruses, worms etc.) to or from a network. Firewalls are used to prevent unauthorized internet users to access private networks connected to the internet. All data entering or leaving the Intranet pass through the firewall, which examines each packet and blocks those that do not meet the specified security criteria.

COOKIES: When the user browses a website, the web server sends a text file to the web browser. This small text file is a cookie. Generally, a cookie contains the name of the website from which it has come from and a unique ID tag. They are usually used to track the pages that you visit so that information can be customized for you for that visit.

HACKERS: A hacker accesses the computer without the intention of destroying data or maliciously harming the computer. A computer enthusiast, who uses his computer programming skills to intentionally access a computer without authorization is known as a **hacker**.

CRACKERS: A person who gains unauthorized access to a computer with the intention of causing damage is known as a cracker.

Network Security Threats

Some kinds of attacks on network security are as:

1. **Denial of Service (DoS) attack** is an attempt to make one or more network resources unavailable to their legitimate users. Examples of such attacks are:

a) Denial of Access to Information: Corrupting, Encrypting, or changing the status of information so that it is not accessible to its legitimate user.

b) Denial of Access to Application: Forced shutting of an application as soon as the user opens it.

c) **Denial of Access to Resources:** Blocking a resource, may be a printer or scanner or USB port, of a computer from proper working.

d) **Denial of Access to a Website:** Continuously sending bulk requests to a website so that it is not available to any other user.

2. **Intrusion problem** is an attempt to mischievously steal some information from someone's computer. Examples of Intrusion are:

a)Snooping refers to gaining unauthorized access to another person's or organization's data. This may be done in a number of ways:

- By getting someone's login information by casually watching what he/she is typing.
- Reading the files on someone's computer in an unauthorized manner.
- Using some software which keeps track of the activities and data being sent or received on someone's computer.

b) Eavesdropping refers to unauthorized access to another person's or organization's data while the data is on its way on the network. This may be done in a number of ways:

- By setting up parallel telephone lines.
- By installing some software (spyware) in the target computer.
- By installing some receiver which captures the data while on its way.

Protecting a network from security attacks

1. Login-Password: By assigning login names and strong passwords to the users of a system, it can be ensured that only authorized people access a computer.

2.Firewall: A firewall is a hardware device or a software that is installed to monitor the data entering the computer/Network or leaving it.

3.Anti Virus Software: Anti-virus software work against not only the virus but also against almost all kinds of malware. Therefore, by installing a full version legal (not the pirated one or freeware) anti-virus software network security can be increased.

4.File Permissions: Different rights (privileges) can be given to different users of a computer to perform one or more of these tasks. For eg. 'Read', 'Write', and 'Modify' rights can be given. By giving appropriate rights to respective users, computer security as well as network security can be increased.

INTERNET APPLICATIONS

SMS(Short Message Service): SMS is the transmission of short text messages to and from a mobile pone, fax machine and or IP address.

VOICE MAIL: It is an electronic communication system in which spoken messages are recorded or digitized and stored for later playback to the intended recipient. Voicemail systems are designed to convey a caller's recorded audio message to a recipient.

ELECTRONIC MAIL(Email): Email is sending and receiving messages by computer.

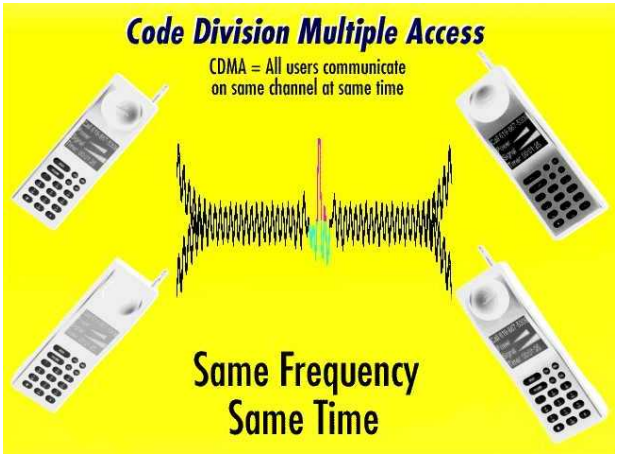
CHAT: Online textual talk in real time, is called Chatting. A chat program is software which is required for chatting over the internet. AOL Instant Messenger, Campfire, Internet Messenger, MSN Messenger are some commonly used chat programs.

VIDEO CONFRENCING: It is a two way videophone conversation among multiple participants is called video conferencing.

Wireless/mobile communication

1.GSM(Global System for Mobile communication): GSM (Global System for Mobile Communications) is a second-generation digital mobile telephone standard using a variation of Time Division Multiple Access (TDMA). It is the most widely used of the three digital wireless telephone technologies - CDMA (Code Division Multiple Access), GSM and TDMA. It provides its subscribers with roaming facility, so that they can use their mobile phone all over the world. It provides customers with better voice and low cost alternative to making calls such as short message service(SMS). The main feature of GSM is the Subscriber Identity Module(SIM) called as SIM card. It is a detachable smart card that contains subscriber's information along with phone book. It which allows eight simultaneous calls on the same radio frequency.

2. **CDMA(Code Division Multiple Access):** Code Division Multiple Access (CDMA) is a sort of multiplexing that facilitates various signals to occupy a single transmission channel. It optimizes the use of available bandwidth. It is a digital cellular technology that uses spread- spectrum techniques. CDMA does not assign a specific frequency to each user. Instead, every channel uses the full available spectrum. The user has access to the whole bandwidth for the entire duration. The basic principle is that different CDMA codes are used to distinguish among the different users.



Difference between GSM and CDMA

GSM	CDMA
It's a "time division" system.	It's a "code division" system.
Calls take turns. Your voice is transformed into digital data, which is given a channel and a time slot, so three calls on one channel look like this: 123123123123. On the other end, the receiver listens only to the assigned time slot and pieces the call back together.	Every call's data is encoded with a unique key, then the calls are all transmitted at once; if you have calls 1, 2, and 3 in a channel, the channel would just say 66666666. The receivers each have the unique key to "divide" the combined signal into its individual calls.
GSM also has the advantage of easily swappable SIM cards. GSM phones use the SIM card to store your (the subscriber's) information like your phone number and other data that proves you are in fact a subscriber to that carrier.	With CDMA phones, however, the SIM card does not store such information. Your identity is tied to the CDMA network and not the phone.
all GSM networks support making phone calls while using data. This means you can be out and about on a phone call but still use your navigation map or browse the internet.	Such capability is not supported on most CDMA networks.

4. **WLL(Wireless in Local Loop) :** WLL is a system that connects subscribers to the public switched telephone network using radio signals as a substitute for other connecting media.
5. **3G/4G:**

   1G => Voice
   2G => Voice + Data
   3G => Voice + Data + Video (Broadband)+ multimedia
   4G =>wireless, Faster than 3G, anytime/anywhere feature

   3G: The 3G technology adds multimedia facilities to 2G phones by allowing video, audio, live chat, fast downloading, video conferencing, faster web services etc. over mobile phones.

   4G: It is a wireless access technology. 4G will provide internet access, high quality streaming video and "anytime, anywhere" voice and data transmission at a much faster speed than 3G. The "anytime, anywhere" feature of 4G is also referred to as "MAGIC" (Mobile multimedia; Anytime/anywhere; Global mobility support; Integrated wireless solution; Customized personal services).