UNIT 5: COMMUNICATION AND NETWORK CONCCEPT

Network: A computer network is a set of computers connected together for the purpose of sharing resources. Each computer on the network is called a **node**.

Advantages for Networking

1. **Resource sharing** – All programs, data and peripherals are available to everyone irrespective of the location of the resource and the user.
2. **Reliability** – Backup copy of a file is kept on different machines, which is available in case of hardware crash or any other problem.
3. **Cost factor** –Cost is reduced since the resources can be shared
4. **Communication Medium** - Changes done by a user on a shared resource are conveyed to all.

Disadvantages of Networking

1. **Threat to data:** A computer network may be used by unauthorized users to steal or corrupt the data and even to deploy computer virus or worms on the network.
2. **Difficult to set up**:

Evolution of Networking:

ARPANET (Advanced Research Projects Agency NETwork): In 1969, The US govt. formed an agency named ARPANET to connect computers at various **universities and defense agencies**. The main objective of ARPANET was to develop a network that could continue to function efficiently even in the event of a nuclear attack.

Internet (INTERconnection NETwork): The Internet is a worldwide network of computer networks. It is not owned by anybody.

Interspace: is a client/server software program that allows multiple users to communicate online with real – time audio, video and text chat in dynamic 3D environments.

Switching Techniques: Switching techniques are used for transmitting data across networks. Different ways of sending data across the network are:

Circuit Switching:	**Packet Switching:**
• First the complete **end-to-end transmission path is established** between the source and the destination computers. • Then the message is transmitted through the path. • The main advantage of this technique is **guaranteed delivery** of the message. • Mostly used for **voice communication.**	• Using the **TCP protocol** a single large message is **divided into a sequence of packets** of size limits from 128 to 4096 bytes. • Each packet is independent and **has the address of sender and destination**. • The **IP** (Internet protocol) does the **routing** for the packets. It keeps track of all the different routes available to the destination. If one route is not available it finds the alternate route to the destination. • At the destination, the **TCP** protocol **re-assembles** the packets into the complete message. • If any packets are lost or damaged, a request is sent to **retransmit** the same message.

Communication terminologies:

Communication Channel (Transmission media): Is a medium through which a message is transmitted to its intended destination. Communication channel can be wired (Guided) or Wireless (Unguided).
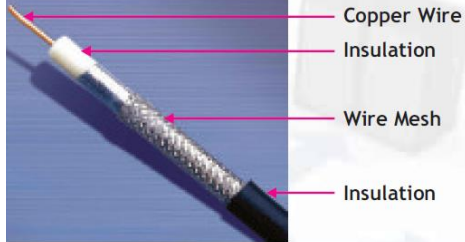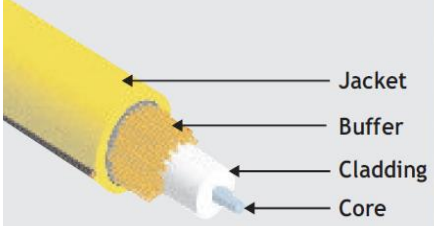
UNIT 5: COMMUNICATION AND NETWORK CONCCEPT

Bandwidth: Is a range of frequencies within a given band that is used for transmitting an analog signal. Bandwidth is expressed in **Hz, KHz, and MHz**

Data transfer rate: DTR is the amount of data in digital form that is moved from one place to another in a given time on a network. Data rates are often measured in megabits (million bits) or megabytes (million bytes) per second.

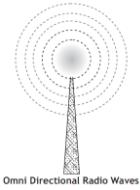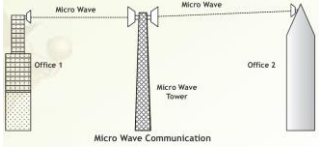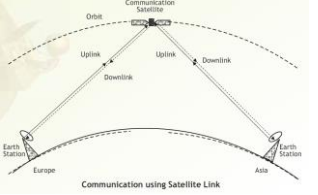|			
bps	bits per second	Bps	bytes per second
Kbps	kilobits per second	KBps	kilo bytes per second
Mbps	megabits per second	MBps	megabytes per second
Gbps	giga bits per second	GBps	giga bytes per second
Tbps	tera bits per second	TBps	tera bytes per second

Wired Media (Guided media)

Twisted pair cable	Co-axial Cables	Optical fiber
It consists of two identical 1 mm thick copper wires insulated and twisted together. The twisted pair cables are twisted in order to reduce crosstalk and electromagnetic induction	It consists of a solid wire core surrounded by one or more foil or braided wire shields, each separated from the other by some kind of plastic insulator. It is mostly used in the cable wires.	An optical fiber consists of thin glass fibers that can carry information in the form of visible light.
Very Inexpensive	**Expensive** than twisted pair cables.	**Very Expensive** as compared to other guided media.
Easy to install and maintain	**Difficult to manage and reconfigure.**	**Need special care and training while installation**
Attenuation is very high. It is incapable to carry a signal over long distances (only **100m**) without the **use of repeaters**.	**Attenuation is low.** Data transmission rate is **better than twisted pair cables.** Carries signal up to **150m to 500 m**	**Attenuation is very low**. Transmit data **over very long distance** with **high security**.
Due to **low bandwidth**, these are unsuitable for broadband applications	**Moderate bandwidth** It provides a cheap means of **transporting multi-channel** television signals around metropolitan areas.	**Very High Bandwidth is up to 10 Gbps.** Data transmission **speed is very high.**
Low noise immunity. Susceptible to electromagnetic interference	**Higher noise immunity than twisted pair. Less Susceptible to electromagnetic interference**	**Immune to noise** as light rays are unaffected by electrical noise. **Not Susceptible to electromagnetic interference.**

Ethernet cable : It is also called a Cat 5 cable, is used to connect devices together within a local area network, it consists of **4 pairs (8 wires)** of unshielded twisted pair cable and delivers data **transmission rate of 1 Gbps**. Two pairs (Green and Orange) are used for transmitting and receiving packets respectively while the other Two pairs (Blue and Brown) are used in VoIP and PoC (Push to Talk over Cellular)
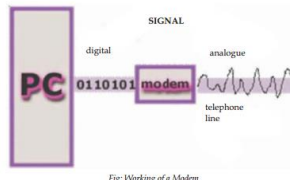
UNIT 5: COMMUNICATION AND NETWORK CONCCEPT
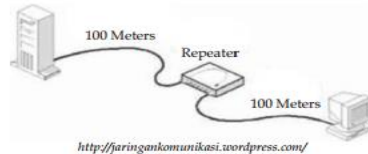
Wireless Media (Unguided media)

Infrared Wave Transmission	Radio Wave Transmission	Micro Wave Transmission	Satellite Link
	Omni Directional Radio Waves	Micro Wave Communication	Communication using Satellite Link
Short Range Communication: Infrared waves can travel from a few centimetres to several meters.(Approx. 5m)	**Long Range Communication :** Radio waves can cover distances ranging from a few meters (in walkie-talkies) up to covering an entire city	**Long Range Communication** Microwave signals travel at a higher frequency than radio waves and are used for transmitting data over several miles or kilometres.	**Very Long Range Communication :** Satellite is a relay station in orbit above the earth that receive from one end of earth (uplink) regenerates, and redirects signals to other end of earth (downlink).
Line of Sight Propagation: Infrared uses point to point communication, both transmitter and receiver should be placed in line of sight of each other and there should not be any obstacle in-between.	**Omnidirectional:** Radio waves are propagated in all directions. Therefore sending and receiving antennas do not have to be aligned. Radio waves can easily bend along mountains and reach valleys.	**Line of Sight Propagation:** Microwaves towers transmitting and receiving antennas need to be properly aligned.	**Line of Sight Propagation** Since microwave signals cannot bend around the curvature of earth. Satellite act as a relay between the transmitting earth stations covering the entire surface of earth
Cannot Penetrate Solid Objects : Infrared waves can propagate throughout a room but could not cross the walls of the room, so that the remote does not interfere with appliances in other room	**Penetrates Solid Objects:** Radio receivers can catch the signal inside buildings also. Thus it can be used for both indoor and outdoor communication	**Cannot Penetrate Solid Objects:** High towers are built and microwave antennas are put on their tops so that signal does not get blocked by building structures	**Cannot Penetrate Solid Objects**: Signals can get blocked by solid material or objects such as rocks, wood or solid building structures
Inexpensive mode of communication: Infrared communication is a common, inexpensive, and easy to use wireless communication technology.	**Inexpensive mode of communication** Radio waves are the most economical way of communicating. It is cheaper than laying cables and fibres.	**Very Expensive mode of communication:** Signals become weak after travelling as it gets absorbed by atmosphere. So repeaters are used at regular intervals (25-30 km). Towers are expensive to build.	**Very Expensive:** Placing the satellite into orbit involves very high cost. Installation is extremely complex. But, satellite communication is very economical keeping in mind the fact that the area covered quite large.
Secure : At a time only two devices can communicate therefore information passed to one device is not leaked to another device	**Insecure:** Radio wave communication is insecure communication.	**Insecure:** Microwave communication is an insecure communication. Multiple channels are available. It can carry 25000 voice channels at the same time.	**Insecure:** Signals sent to a satellite are broadcasted to all receivers, so necessary security measures have to be taken to prevent tampering of data.

Could not be used for long and difficult terrains	Communication over difficult terrains: Since no cables are to be laid down and no digging is to be done, it offers ease of communication over difficult terrains like hilly areas.	Communication over difficult terrains: Since no cables are to be laid down and no digging is to be done so it offers ease of communication over difficult terrains like hilly areas.	No restrictions of difficult terrains such as natural mountains, tall building, towers etc.
Not Susceptible To Weather Conditions	Susceptible To Weather : Radio wave propagation is susceptible to weather effects like rains, thunder storms etc.	Susceptible To Weather: Microwave propagation is susceptible to weather effects like rains, thunder storms etc.	Susceptible To Weather Transmission is affected by weather conditions like rain, thunderstorm etc.
USES: TV remotes, Cordless mouse, and Intrusion detectors, automotive garage doors, wireless speakers etc.	USES: Cordless phones, AM and FM radio broadcast, Garage door openers etc.	USES: It is used for long distance telephonic communications.	USES: Communicate anywhere in the world

Network devices:

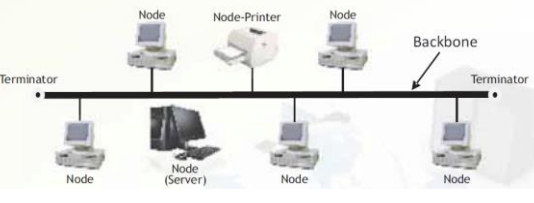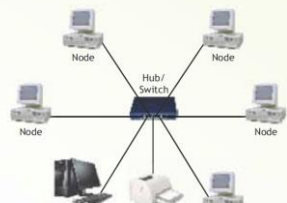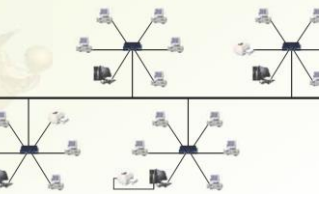|	
Modem (MOdulator DEModulator) is an electronic device which converts digital signals into analog signals for transmission over telephone lines (Modulation). At the receiving end, a modem performs the reverse function and converts analog signal into digital form (Demodulation) A modem can also amplify a signal so that it can travel a long distance without attenuation.	Fig: Working of a Modem
RJ-45 (Registered Jack – 45) is an eight wired connector that is used to connect computers on a local area network (LAN), especially Ethernet.	
Ethernet card is a kind of network adapter and is also known as Network Interface Card (NIC). These adapters support the Ethernet standard for high-speed network connections via cables. An Ethernet Card contains connections for either coaxial or twisted pair cables or fiber optic cable	
Switch/Hub is an electronic device that connects several nodes to form a network and redirects the received information to the destination. It has ports into which the cables from individual computers' NICs are inserted. **Switch** is an **intelligent hub** redirects the received information **only to the intended node**(s). **Hub broadcasts** the information all the connected nodes	Hub/Switch
Repeater When the data is transmitted over a network for long distances, the data signal gets weak due to attenuation. A repeater **regenerates** the received signal and **re-transmits** it to its destination.	Fig: A Repeater

Router is a network device used to establish connection between two **similar networks.** They can connect networks with **different architectures** such as Token Ring and Ethernet. But, routers **cannot transform information from one data format to another** such as TCP/IP to IPX/SPX.
Gateway is a device, which is used to **connect dissimilar networks** and perform the necessary translation so that the connected networks can communicate properly. A gateway can **translate information between different network data formats and network architectures.** It can translate TCP/IP to AppleTalk so computers supporting TCP/IP can communicate with Apple brand computers.
Wi-Fi cards are small and portable cards that allow your computer to **connect to the internet through a wireless network.** Wi-Fi transmission is through the **radio waves**, these signals are picked up by Wi-Fi receivers such as computers and cell phones equipped with Wi-Fi cards. The devices need to be within the range of a Wi-Fi network to receive the signals and produces a wireless internet connection. Once a connection is established between user and the network, the user is prompted with a **login screen and password for establishing is a secure connection**. Wi-Fi cards can be external or internal. If a Wi-Fi card is not installed inside your computer, you may purchase an external USB antenna attachment and connect it to your device. Many computers and mobile devices are now a days equipped with wireless networking capability and do not require a Wi-Fi card.

Network Topologies
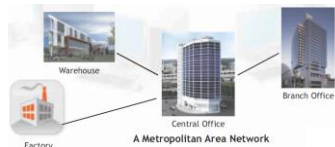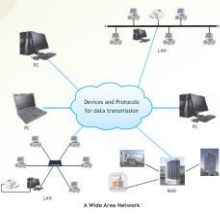
It refers to the geometrical arrangement of nodes in a (LAN). The criteria for choosing a topology: Installation cost, Reliability, Flexibility, Fault detection etc.

Bus Topology	**Star Topology**	**Tree Topology**
In bus topology **all the nodes are connected to a main cable called backbone**. If any node has to send some information to any other node, **it sends the signal to the backbone.** **The signal travels through the entire length of the backbone and is received by the node for which it is intended**. A small device called terminator is attached at each end of the backbone. **When the signal reaches the end of backbone, it is absorbed by the terminator and the backbone gets free to carry another signal.** This prevents the reflection of signal back on the cable and hence eliminates the chances of signal interference.	In star topology **each node is directly connected to a hub/switch.** If any node has to send some information to any other node, **it sends the signal to the hub/switch.** **In the case of a switch the signal is sent directly to the intended node(s).** In case of a hub this signal is broadcast to all the nodes but is accepted by the intended node(s).	Tree topology is a **combination of bus and star** topologies. It is used to combine multiple star topology networks. All the stars are connected together like a bus. This bus-star hybrid approach supports **future expandability** of the network

Characteristics of Bus topology:	Characteristics of Star topology:	Characteristics of Tree topology:
• **Linear architecture is easy to install.** Additional nodes can be easily connected to the existing bus network at any point along the length of the backbone cable	• **Easy to install and easy to expand** Additional nodes can be easily connected to the existing star network according to the specifications of central hub/switch	• It offers **easy way of network expansion** • Even if one network (star) fails, the other networks remains connected and working.
• **Requires less cable length and hence it is less costly:** All the nodes are connected through drop cables to the main backbone cable.	• **Requires more cable length hence it is more costly than Bus**: Every node is directly connected to the central hub/switch.	
• **Fault diagnosis and isolation is difficult in Bus Topology**. If a node is faulty on the bus, detection of fault may have to be performed at many points on the network.	• **Fault diagnosis and isolation is easy in Star topology.** Failure of a node involves disconnecting the node from otherwise functional network.	
• **Backbone cable or terminator fault leads to failure of entire network**: But failure of one node does not affect the network.	• **Hub or switch fault leads to failure of entire network**: But, failure of one node does not affect the network.	

Network Types:

PAN (Personal Area Network):	LAN (Local Area Network):	MAN (Metropolitan Area Network):	WAN (Wide Area Network):
Spread in the **proximity of an individual**	Spread **across a room, building, or campus**	Spread **within a city**	Spread **across a city, country, or continent**.
Cover an area of a **few meters radius.**	Cover an area of a **few meters to a few kilometres radius.**	Cover an area of a **few kilometres to a few hundred kilometres radius**	Cover an area of **over hundreds of kilometres radius.**
Set up using guided media (**USB cable**) or unguided media (**Bluetooth, Infrared**).	Set up using wired media (**UTP cables, Co-axial cables** etc.) or wireless media (**Infrared, radio waves**) i.e. WLAN (wireless LAN)	Set up using all types of **all guided and unguided media**	Set up using **all types of all guided and unguided media**
Owned, controlled, and managed by a **single person**	Owned, controlled, and managed by a **single person or organization.**	Owned and operated by a **government body or a large corporation**	**Not owned by anyone**, WANs is interconnected computers, LANs, MANs, and maybe other WANs.
Examples: A network of devices such as computer, Phone, MP3/MP4 Player, Camera etc. Transferring songs from one cell phone to another is a PAN of two phones. Transferring files from a PC to an MP3 player is a PAN between the two.	**Examples:** A networked office building, school or home. Sometimes one building can contain a few small LANs (Like some schools have independent LANs in each computer lab.).	**Examples:** A network of schools, or banks, or Government offices etc. within a city. A MAN is usually formed by interconnecting a number of LANs and individual computers.	**Examples:** A network of ATMs, BANKs, National Government Offices, International Organizations' Offices etc., spread over a country, continent, or covering many continents.

UNIT 5: COMMUNICATION AND NETWORK CONCCEPT

Network Protocol

A protocol is the special **set of rules** that two or more machines on a network follow **to communicate** with each other. Some of the important protocols used are as follows:

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.
- Using the **TCP protocol** a single large message is **divided into a sequence of packets** of size limits from 128 to 4096 bytes.
- Each packet is independent and **has the address of sender and destination**.
- The **IP** (Internet protocol) does the **routing** for the packets. It keeps track of all the different routes available to the destination. If one route is not available it finds the alternate route to the destination.
- At the destination, the **TCP** protocol **re-assembles** the packets into the complete message.
- If any packets are lost or damaged, a request is sent to **retransmit** the same message.

FTP (File Transfer Protocol)

The File Transfer Protocol (FTP) is a standard network protocol used for the **transfer of computer files from a server to a client** using the Client–server model on a computer network. The objectives of FTP are:
- To promote sharing of files (computer programs and/or data).
- To encourage indirect or implicit use of remote computers.
- To shield a user from variations in file storage systems among different hosts.
- To transfer data reliably, and efficiently.

PPP (Point to Point Protocol): In computer networking, Point-to-Point Protocol (PPP) is a data link protocol used to establish a **direct connection between two nodes.** The Point-to-Point Protocol (PPP) is an encapsulation protocol for transporting IP traffic across point-to-point links. PPP is used over many types of physical networks including serial cable, phone line, trunk line, cellular telephone, radio links, and fibre optic links etc.

Electronic mail protocols

Simple Mail Transfer protocol (SMTP): Simple Mail Transfer Protocol, a protocol for **sending e-mail messages between servers**. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; In addition, SMTP is generally used to send **messages from a mail client to a mail server**. The messages can then be retrieved with an e-mail client using either POP or IMAP. This is why you need to specify both the POP or IMAP server and the SMTP server when you configure your e-mail application.

ESMTP (Extended Simple Mail Transfer Protocol) specifies extensions to the original SMTP protocol for sending e-mail that supports graphics, audio and video files, and text in various national languages.

MIME (Multi-Purpose Internet Mail Extensions) is an extension of the original Internet e-mail protocol that lets people use the protocol to exchange different kinds of data files on the Internet: audio, video, images, application programs, and other kinds, as well as the ASCII text handled in the original protocol, the Simple Mail Transport Protocol (SMTP).

Post Office Protocol Version 3 (POP3): POP3 is a client/server protocol **used for opening the remote e-mail boxes, the POP3 mail server receives e-mails, filters and holds them into the appropriate user folders.** When a user connects to the mail server to retrieve his mail, the messages are downloaded from mail server to the user's hard disk.

Remote Access Protocol (Telnet) : This protocol helps a user **(Telnet Client) to log in at a remote computer (Telnet Server)** and function as if he/she were connected directly to that computer. Telnet is the main internet protocol for creating a connection with a remote machine. It allows you to connect to remote computers (called remote hosts) over a TCP/IP network (such as the Internet). Once your telnet client establishes a connection to the remote host, your client becomes a virtual terminal, allowing you to communicate with the remote host from your computer with whatever privileges you may have been granted to the specific application and data on that host computer.

Wireless/Mobile Communication protocol

GSM: (Global System for Mobile communication): is a digital mobile telephony system that is widely used in Europe and other parts of the world. GSM) is a second generation **(2G)** standard for mobile networks. The GSM standard has given birth to wireless services like General Packet Radio Service (GPRS) and Enhanced Data Rates for GSM Evolution (EDGE). GSM uses a variation of time division multiple access (TDMA) and is the most widely used telephony technology.

TDMA (Time division Multiple Access): It allows several users to **share the same frequency channel by dividing the signal into different time slots**. The users transmit in rapid succession, one after the other, each using its own time slot. For example, the radio frequency say 890 MHz is shared by different users in time. This means if user A, B, C and D all talk at the same time. You assign the 890 MHz frequency to A for some time and allow him to talk, then you assign 890 band to B for some time to speak, then to C , and finally to D, before coming back to A. So the process continues in a round robin fashion, as long as A, B, C, and D want to talk. This way many users talk at same time on the same frequency.

CDMA (Code Division Multiple Access): Code Division Multiple Access (CDMA) is a multiple access technology whereby a number of users share the same frequency channel at the same time. Every channel uses the full available spectrum. Individual conversations are encoded with a pseudo-random digital sequence. Every communicator will be allocated the entire spectrum all the time. **Each user's signal is spread over the entire bandwidth by a unique spreading code.** At the receiver end, that same unique code is used to receive the signal. CDMA consistently provides **better capacity for voice and data communications**; it is the common platform on which **3G** technologies are built.

GPRS (General Packet Radio Service): is a packet oriented mobile data service on the 2G and 3G GSM communications. GPRS usage is typically charged based on volume of data transferred.

WLL (Wireless Local Loop): Wireless local loop (WLL), is the use of a **wireless communications link for delivering telephone service (POTS) or Internet access (broadband)** to telecommunications customers. This system is based on radio networks which provide services like telephone in remote areas. Different types of wireless local loop include Broadband Wireless Access, Radio in the Loop, Fixed Radio Access and Fixed Wireless Access. Microwave frequencies are used to provide wireless broadband connection. The local loop can be referred as "last mile" of the telecom network which resides between Central office (CO) and user's location.

Generations of Mobile technology:
➢ **1G technology** was used in the first mobile phones. 1G used **analog radio signals**. 1G was introduced in 1980s
➢ **2G technology** was introduced in 1992. 2G technology used a **digital format and introduced text messaging**. 2G also introduced data services for mobiles, starting with **SMS**.
➢ **3G technology** has introduced more efficient ways of carrying data, making it possible to have faster web-services, **live chat, fast downloading, video conferencing** etc. over mobile phones. Today we are living in the world of 3G.
➢ **4G technology** unlike previous generations of mobile technology, 4G mobile technology will be used for internet access on computers also, and it will be **totally wireless**. 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).

Mobile processors: mobile processor is found in mobile computers and cellphones.

➢ A CPU chip is designed which is typically housed in a **smaller chip package**.

➢ In order to run cooler, it uses **lower voltages than its desktop counterpart** and has more "**sleep mode**" capability.

➢ A mobile processor can be **throttled down to different power levels** or sections of the chip can be turned off entirely when not in use.

➢ Further, the **clock frequency may be stepped down** under low processor loads. This stepping down conserves power and prolongs battery life.

➢ Initially mobile processor was Single core, and then came Dual core; we now have **Quad core, Hexa core and even Octa core.**

➢ Most processors are **64 bit now** as against 32 bit when it started initially.

➢ The processing speed has reached up to **3.0 -3.5 GHz.**

➢ The ability to include **GPU** (Graphic Processing Unit) inside mobile processors has enabled devices to churn out the best graphics picture, 3D capability, Virtual Reality capability and 4k recording.

➢ Some latest mobile processors are: **Qualcomm Snapdragon, Texas Instruments OMAP, Nvidia Tegra 2, Samsung Hummingbird**

Chat Protocol and VOIP

Chatting

A real time **informal communication over the Internet is 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. In order to chat, the user should have an account on a chatting program. A phone call is a voice based chat while online chat is **textual conversation**.

VOIP: Voice over Internet Protocol (Voice over IP, VoIP and IP telephony) is a group of **technologies for the delivery of voice communications and multimedia sessions over Internet**. The terms Internet telephony, broadband telephony, and broadband phone service specifically refer to the provisioning of communications services (voice, fax, SMS, voice-messaging) over the public Internet, rather than via the public switched telephone network (PSTN). This method of making phone calls is much cheaper than convectional way because the service of Telecommunication Company is not used.

Wi-Fi Wireless Fidelity is a brand, originally licensed by the Wi-Fi Alliance to describe the underlying technology of wireless local area networks (WLAN) that **uses radio waves to provide wireless high-speed Internet** and network connections. A person with a Wi-Fi device can connect to the internet or Local area network using an access point, provided that the device should be in the range of that Wireless access point. Wi-Fi networks have no physical wired connection between sender and receiver and transmit by using radio frequency (RF) technology. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space. A computer utilizes a wireless adapter to translate data transmitted by radio waves.

WiMAX (Worldwide Interoperability for Microwave Access) is a wireless industry coalition dedicated to the **advancement of broadband wireless access** (BWA) networks. WiMAX is one of the hottest broadband wireless technologies around today. WiMAX systems are expected to deliver broadband access services to residential and enterprise customers in an **economical** way.

Network Security Concepts: Network security deals with policies adopted by network administrator to protect the network from unauthorized access and misuse of network resources. It also ensures that the authorized users have adequate access to all the network resources.

UNIT 5: COMMUNICATION AND NETWORK CONCCEPT

Virus	Worm	Trojan
A virus is a **self-replicating** malicious piece of code that **attaches itself to other host programs** and gain control over the system without the owner's knowledge.	A worm is a **self-replicating** piece of code that uses security holes in a computer networks to copy itself to the new machine and then starts replicating from there as well. It **does not need to attach itself to a host program.**	A Trojan horse is a **non-self-replicating** a program that contains hidden malicious functions.
It **requires human interaction** to propagate The virus gets executed each time the host program is executed.	It **does not require human interaction**; a worm works by itself as an independent object and copies itself hundreds or thousands of time.	**It tricks users into installing them disguised as useful program.** Once installed on a system, they reveal their true nature and cause damage
They could produce **annoying effects like changing desktop, adding silly icons etc.**	They could **consume the entire memory or bandwidth and clog the network traffic.**	They could **steal confidential information and can open a backdoor.** Trojan horses contact a central server and report back information such as passwords, user IDs, and captured keystrokes.
They can spread **through external media such as CDs, browsing infected internet sites and from email attachments.**	Spreads itself to other computer networks **through mail or address book.**	Spread **through internet browsing.**

Types of Viruses
- ❖ **File Virus:** These viruses infect and replicate when it **gets attached to executable program files** with extensions .COM, .EXE .SYS, .DLL, .OCX, .CPL, and .SCR.
- ❖ **Boot sector virus:** These viruses **infect the boot sector of hard drives**. The master boot record is part of the boot sector that contains an executable that knows where the files to start the operating system are located on the hard drive. Boot sector viruses attach themselves to the master boot record and are executed every time the computer boots up.
- ❖ **Macro virus:** Viruses that infect document files are called macro viruses. They only **infect documents that support macros**. Microsoft Office, WordPerfect Office, StarOffice, and AutoCAD are common applications that support macros in their documents. When the virus attaches itself to the document, it must make sure that the macro will be run so its code can be executed. Viruses ensure this occurs by attaching themselves to common subroutines that are run every time a document is opened or closed.

Spam: **Repetition of worthless text in the form of messages or mails** is known as Spam. Most spam is commercial advertising. In addition to wasting people's time, spam also eats up a lot of network bandwidth.

Cookies: When the user browses a website, the web server sends a **small text file** to the web browser known as a cookie. Generally a cookie contains the name of the website from which it has come from and a unique ID tag. Some cookies are **stored on your hard drive** until you delete them or they reach their expiry date. These may be **used to remember your preferences when you use the website.** While, some cookies last only until the browser is closed are not stored on your hard drive. They are usually **used to track the pages that you visit so that information can be customized for you** for that visit.

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

UNIT 5: COMMUNICATION AND NETWORK CONCCEPT

Https: Hyper Text Transfer Protocol Secure (HTTPS) is the **secure version of HTTP**, the protocol over which data is sent between your browser and the website that you are connected to. The 'S' at the end of HTTPS stands for 'Secure'. It means all communications between your browser and the website are **encrypted.**

India IT Act: The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It is the **primary law in India dealing with cybercrime and electronic commerce**. The laws apply to the whole of India. Persons of other nationalities can also be indicted under the law, if the crime involves a computer or network located in India. The Act provides legal framework for electronic governance by giving recognition to electronic records and digital signatures. The above Act was further amended in the form of IT Amendment Act, 2008 [ITAA-2008]. Some of the offenses and penalties are listed below:

Section	Offence	Penalty
65	Tampering with computer source documents	Imprisonment up to three years, or/and with fine up to ₹200,000
66	Hacking with computer system	Imprisonment up to three years, or/and with fine up to ₹500,000
66F	Acts of cyber terrorism	Imprisonment up to life.
67	Publishing information which is obscene in electronic form.	Imprisonment up to five years, or/and with fine up to ₹1,000,000
70	Securing access or attempting to secure access to a protected system	Imprisonment up to ten years, or/and with fine.

Cyber Law: Cyber law or Internet law is a term that encapsulates the **legal issues related to use of the Internet**. It is less a distinct field of law than intellectual property or contract law, as it is a domain covering many areas of law and regulation. Some leading topics include internet access and usage, privacy, freedom of expression, and jurisdiction.

Cyber Crime: In Simple way we can say that cyber-crime is **unlawful acts wherein the computer is either a tool or a target or both.** Cyber-crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code.
We can categorize Cyber-crimes in two ways

1. The Computer as a Target:-**using a computer to attack other computers**. E.g. Unauthorized access and Hacking, Trojan/Virus/Worm attacks, Email spoofing, Email Spamming, Email bombing, DoS- Denial of Service attacks etc.
2. The Computer as a weapon:-**using a computer to commit real world crimes**. E.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography, Cyber Stacking etc.

Intellectual property rights (IPR) Issues: Intellectual property rights are the rights given to an individual over the invention of their own. They usually give the creator an exclusive right over the use of his/her creation for a certain period of time.
There are only three ways to protect intellectual property

1. **Patents:** A Patent is a term used for a specific product designed by an individual. The designer is given exclusive rights over the patent for a limited period of time. With help of the patent right, the owner can stop others from making, using or selling the product design. The owner can take a legal action if someone uses the patent without his/ her permission
2. **Trademarks:** Trademark can be defined as a name or a different sign or a device identifying a product or a service provided by a person or a company. A Trademark is also known as brand name. It should be officially registered and legally restricted to use of the specific person or the company.
3. **Copyrights:** Copyright is the term used for a written document. A legal action can be taken, if copyrights are violated.

Hacking: Hacking is **unauthorized intrusion** into a computer or a network. The person engaged in hacking activities is generally referred to as a hacker. This hacker may alter system or security features to accomplish a goal that differs from the original purpose.

A hacker (white hat) accesses the computer **without the intention of destroying data** or maliciously harming the computer. White hat is known as ethical hacker	• **A cracker (black hat)** gain unauthorized access to a computer **with the intention to cause damage**. Black hat is a hacker who violates computer security for maliciousness or for personal gain

Introduction to Web Services

WWW (World Wide Web): WWW is a network of web servers. It can be defined as a hypertext information retrieval system on the Internet. It is the universe of the information available on the internet. All the web pages on WWW use HTTP for making hypertext jumps.

HTML (Hypertext Markup Language)	**XML (eXtensible Markup Language)**
➢ HTML is a markup language to create and design web content.	➢ XML is a markup language that is self-descriptive.
➢ It is used to **display the data in formatted manner**.	➢ It is used to **carry, store or exchange data**.
➢ It has a variety of **predefined tags** and attributes for defining the layout and structure of the web document.	➢ It does not have predefined tags. It is possible to define new tags in XML. It allows the programmer to use **customized tags**.
➢ HTML is **not case sensitive**	➢ XML is **case sensitive**.
➢ A HTML document has the extension **.htm or .html.**	➢ A HTML document has the extension **.xml**
➢ HTML documents have a **head and body**. <html> <head>……………… </head> <body>……………… </body> </html>	➢ XML documents form a **tree structure**. <root> <child> <subchild>..... </subchild> </child> </root>

HTTP is the protocol that is used for **transferring hypertext** (text, graphic, image, sound, video etc.) between two computers and is particularly used on the World Wide Web. It is a TCP/IP based communication protocol and provides a standard for Web browsers and servers to communicate. HTTP is based on **Client/Server** principle. Communication between the host and the client occurs through a **request/response pair**. A connection is established between two computers - out of which one is client (generally the browser) that initiates the request and the other is the server that responds to the request. Also HTTP identifies the resource that the client has requested for and informs the server about the action to be taken. When the user clicks on the hypertext link, the client program on their computer uses HTTP to contact the server, identify the resource and ask the server to respond with an action. The server accepts the request and then uses HTTP to respond to perform the action.

Domain Names: Every computer on the network has a unique numeric address assigned to it which is a combination of four numbers from 0-255 separated by a dot. For example, 59.177.134.72 since it is practically impossible for a person to remember the IP addresses. A system has been developed which assigns domain **names to web servers** and maintains a database of these names and corresponding IP addresses on **DNS** (*Domain Name Service*) **server.**
Examples of some domain names are **cbse.nic.in**, **indianrailway.gov.in** etc. A domain name usually has more than one part for example, in the domain name **www.cbse.nic.in**
- ➢ **in** is the **primary domain name**
- ➢ **nic** is the **sub-domain of in**
- ➢ **cbse** is the **sub-domain of nic**
- ➢ www indicates the server is on world wide web

➤

Top level domains are further divided into two categories:	
Generic Domain Names:	**Country Specific Domain Names:**
·com - commercial business	.in - India
·edu - Educational institutions	·au - Australia
·gov - Government agencies	·ca - Canada
·mil - Military	.ch - China
·net - Network organizations	.nz - New Zealand
·org - Organizations (non-profit	.pk - Pakistan
	.jp - Japan
	.us - United States of America

URL (Uniform resource locator): A URL is a formatted **text string used to identify a network resource on the Internet**. Network resources can be plain Web pages, text documents, graphics, downloadable files, services or programs. Every network resource on the web has a unique URL in the following format:

Protocol: // domain name /path / file name

The URL text string consists of three parts:

- ❖ **Network Protocol:** The network protocol identifies the protocol to be used to access the network resource. These strings are short names followed by the three characters ': //'. Some examples of protocols include http, gopher, ftp and mailto.
- ❖ **Domain name:** It identifies the host/server that holds the resource. For example: www. School.com is a **domain name.**
- ❖ **Resource Location:** It consists of the path or directory and the file name of resource. For example in the URL : **http://www.school.com/syllabus/preprimary/nursery.htm** the file *nursery.htm* is stored in the sub directory *preprimary*, of the directory *syllabus* on the server *www.school.com*

Website: Related **webpages from a single web domain** is termed as a website. A website has multiple webpages providing information about a particular entity.

Web browser: Web browser is **software program to navigate the web pages on the internet**. A bowser interprets the coding language of the web page and displays it in graphic form. Internet works on client -server model. A web browser is a client which requests the information from the web server. The web server sends the information back to the client. Some of the web browsers are: **Netscape Navigator, Internet Explorer, Mozilla Firefox** etc.

Web Server: A Web server is a computer or a group of computers that stores web pages on the internet. It works on client/server model. It delivers the requested web page to web browser. Web servers use special programs such as **Apache or IIS** to deliver web pages over the http protocol.
Each server has a unique IP address and domain name. In order to access a webpage, the user writes the URL of the site on the address bar of the browser. The machine on which the browser is running sends a request to the IP address of the machine running the web server for that page. Once the web server receives that request, it sends the page content back to the IP address of the computer asking for it. The web browser then translates that content into all of the text, pictures, links, videos, etc. A single web server may support multiple websites or a single website may be hosted on several linked servers.

Web hosting: Web hosting is the **process of uploading/saving the web content on a web server** to make it available on WWW. In case an individual or a company wants to make its website available on the internet, it should be hosted on a web server.

Web page: Web page is an electronic **document designed using HTML**. It displays information in textual or graphical form. It may also contain downloadable data files, audio files or video files. Traversal from one webpage to another web page is possible through hyperlinks**. A web page can be classified into two types:

UNIT 5: COMMUNICATION AND NETWORK CONCCEPT

Static web page: A web page which displays same kind of information whenever a user visits it is known as a static web page. A static web page generally has **.htm or .html** as extension	**Dynamic web page**: An interactive web page is a dynamic webpage. A dynamic web page uses scripting languages to display changing content on the web page. Such a page generally has **.php, .asp** or **.jsp** as extension.

Scripting language: It is a programming language which can be embedded or integrated with other languages. Some of the most widely used scripting languages are JavaScript, VBScript, PHP, Perl, Python, Ruby, and ASP. They have been used extensively to create dynamic web pages.

Dynamic web pages support two types of scripting:

Client-Side Scripting: On some web pages the **contents change in response to an action done by the user**, for example a click from the mouse or a key press from a keyboard action. Such pages use client-side scripting. In this technology, the content is generated on the user's local computer. **VB Script** and **Java Script** are examples of client-side scripting languages.	**Server-Side Scripting:** Some web pages use **applications running on the server to generate the web content**. Such pages use server-side scripting language. Web page display the current time and date, forums, submission forms, shopping carts etc., use server-side scripting. **ASPS, JSP, PHP** are examples of server-side scripting languages.

Web 2.0: Web 2.0 refers to **new generation of dynamic and interactive websites**. Web 2.0 websites uses a new programming language called **AJAX (Asynchronous JavaScript and XML)**. AJAX helps a dynamic website connect to the web server and download small amount of data based on the interaction with the user. In this technology only the part of the website which is updated is reloaded. The entire page does not get reloaded each time. This helps in making the website interactive.

Applications supported by web 2.0 are as followings:
- ❖ blogging
- ❖ social bookmarking
- ❖ RSS (Really Simple Syndication)
- ❖ wikis and other collaborative applications
- ❖ interactive encyclopedias and dictionaries
- ❖ Advanced Gaming

E-commerce payment transactions: E-Commerce or Electronics Commerce sites use electronic payment where electronic payment refers to **paperless monetary transactions**. Electronic payment has revolutionized the business processing by reducing paper work, transaction costs, labour cost. Being user friendly and less time consuming than manual processing it helps business organization to expand its market.

Online Banking: Online banking, also known as **internet banking, e-banking or virtual banking**, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of **financial transactions through the financial institution's website**

Mobile Banking: Mobile banking refers to the **use of a smartphone or other cellular device to perform online banking** tasks while away from your home computer, such as monitoring account balances, transferring funds between accounts, bill payment and locating an ATM.

Payment Apps and Services: Most mobile payment apps offer users reasonable, **pay-as-you-go** plans. This requires users to pay a flat percentage of the total expenditure as a processing fee. Many of these apps also allow the user to keep track of their payment and even print receipts of their transactions. Some mobile payment apps are **Google Wallet, PayPal, Paytm, Freecharge, Bhim** and **UPI (Unified Payment Interface)** apps etc.