University of Jammu
Course: Bachelor of Computer Applications (CBCS)
Course No: UBCATC-101

Unit-5
Introduction to Computer Networks and Data Communication

Dr. Parveen Singh
Associate Professor

Syllabus

- Introduction to Computer Network
- Centralized vs Distributed Processing System
- Network Operating Systems and their features
- Data Communication
- Components of Data Communication
- Network Protocols
- Transmission modes
- Types of network
- Network Topologies
- Internet and Intranet
- IP Address, DNS
- Web page, Website,Browsers
- URLs, email
- Applications of Internet

Contents:

Outline of lecture-1

1. Introduction to Computer Network

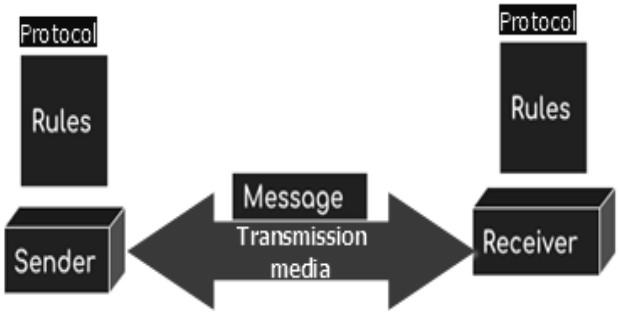
1. What is a computer network?

A computer network is a group of devices that use a set of common communication protocols and are connected with each other through a transmission medium which allows devices to exchange data .To understand the definition we need to understand the three keywords here the devices, transmission media and the protocols.

The **devices** used in the network can be computers, printers, scanners, fax machines, switches, routers or any other devices capable of exchanging information over the network. These devices are often referred to as **nodes** in the network. Two such devices can be said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other.

The networked computing devices exchange data with each other using a data link called **transmission medium**. The transmission medium can be defined as a pathway that can transmit information from a sender to a receiver. The transmission media can be Guided/Wired Transmission Medium or Unguided/Wireless Transmission Medium.

All communications between devices require that the devices agree on the format of the data. A **communication protocol** is a system of rules that allow two or more entities of a communications system to transmit information via any kind of variation of a physical quantity. The protocol defines the rules, syntax, semantics and synchronization of communication and possible error recovery methods.Popular protocols include: File Transfer Protocol (FTP), TCP/IP, User Datagram Protocol .(UDP), Hypertext Transfer Protocol.The best-known computer network is the Internet. Figure shows information exchange between two nodes in a network.



2. Uses of networking

Networks are ubiquitous nowadays - from social networks to transport, study and business networks.Computer networks have become invaluable to organizations as well as individuals. Some of its main uses are as follows :

- Information and Resource Sharing

Computer networks allow organizations having units which are placed apart from each other, to share information in a very effective manner. Programs and software in any computer can be accessed by other computers linked to the network. It also allows sharing of hardware equipment, like printers and scanners among varied users.

- Retrieving Remote Information

The information is stored in remote databases to which the user gains access through information systems like the World Wide Web

- Interpersonal Communication

A computer network facilitates interpersonal communications allowing users to communicate efficiently and easily via various means: email, instant messaging, chat rooms, telephone, video telephone calls, and video conferencing that has completely revolutionized the teaching learning process.

- E-Commerce

Computer networks have paved the way for a variety of business and commercial transactions online, popularly called e-commerce. Users and organizations can pool funds, buy or sell items, pay bills, manage bank accounts, pay taxes, transfer funds and handle investments electronically.

- Highly Reliable Systems

Computer networks allow systems to be distributed in nature, by the virtue of which data is stored in multiple sources. This makes the system highly reliable. If a failure occurs in one source, then the system will still continue to function and data will still be available from the other sources.

- Cost–Effective Systems

Computer networks have reduced the cost of establishment of computer systems in organizations. Previously, it was imperative for organizations to

set up expensive mainframes for computation and storage. With the advent of networks, it is sufficient to set up interconnected personal computers (PCs) for the same purpose. Users may access and use resources provided by devices on the network, such as printing a document on a shared network printer also reduces the overall setup cost.

- VoIP

VoIP or Voice over Internet protocol has revolutionized telecommunication systems. Through this, telephone calls are made digitally using Internet Protocols instead of the regular analog phone lines.

3. Types of Transmission Media

Computer networks differ in transmission medium used to carry their signals.The transmission medium can be defined as a pathway that can transmit information from a sender to a receiver. Transmission media are also called communication channels.

Transmission media are of two types −

- Guided Transmission Medium
- Unguided Transmission Medium

Guided Transmission Medium

Guided transmission media are also called bounded media or wired media. They comprise cables or wires through which data is transmitted. They are called guided since they provide a physical conduit from the sender device to the receiver device. The signals traveling through these media are bounded by the physical limits of the medium.

The most popular guided media are −

- Twisted pair cable
- Coaxial cable
- Fiber optics

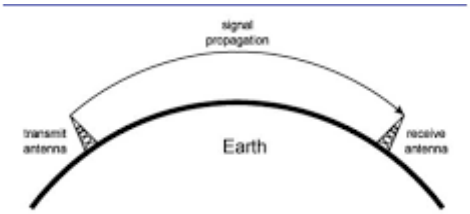
Unguided Transmission Medium

Unguided transmission media are also called wireless media. They transport data in the form of electromagnetic waves that do not require any cables for transmission. These media are bounded by geographical boundaries. This type of communication is commonly referred to as wireless communications.

Unguided signals can travel in three ways −

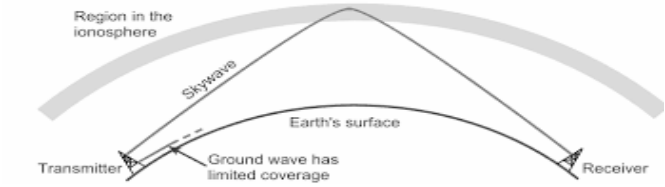
- Ground propagation:

  In this, radio waves travel through the lowest portion of the atmosphere, hugging the Earth. These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet.



- Sky propagation:

  In this, higher-frequency radio waves radiate upward into the ionosphere where they are reflected back to Earth. This type of transmission allows for greater distances with lower output power.



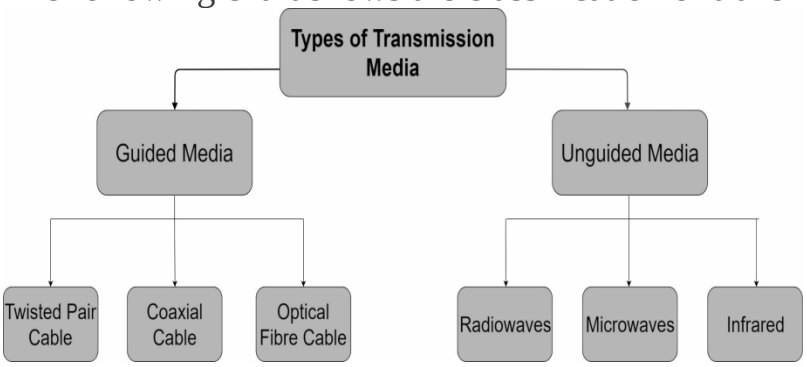
- Line – of – sight propagation:

  In this type, very high-frequency signals are transmitted in straight lines directly from antenna to antenna.

The commonly used unguided transmissions are −

- Radio transmission
- Microwave transmission
- Infrared transmission

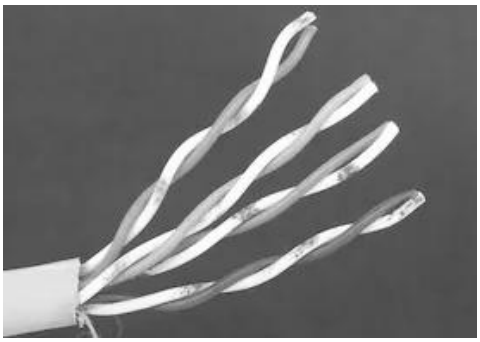
The following chart shows the classification of transmission medium:



1. Twisted Pair Cable

It consists of two separately insulated conductor wires twisted around each other to reduce interference by adjacent wires. They are the most widely used transmission media. Twisted Pair is of two types:

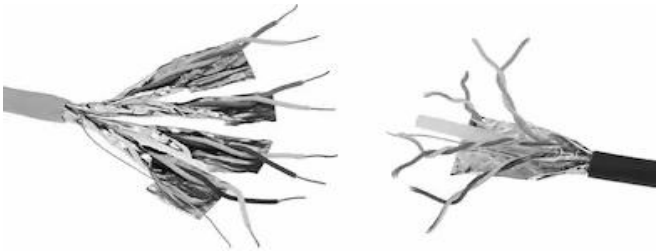
1. Unshielded Twisted Pair (UTP):
   This type of cable has the ability to block interference and other than plastic insulation nothing else shields it from outside interference . It is used for telephonic applications.



Advantages:

- Least expensive
- Easy to install
- High speed capacity
- Susceptible to external interference
- Lower capacity and performance in comparison to STP
- Short distance transmission due to attenuation

2. Shielded Twisted Pair (STP):
   This type of cable consists of a special jacket to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.

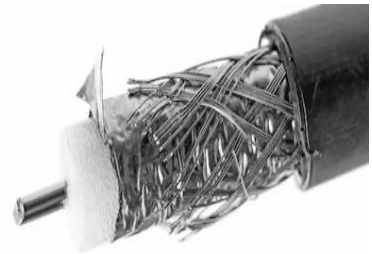


Advantages:

- Better performance at a higher data rate in comparison to UTP
- Eliminates crosstalk
- Comparatively faster
- Comparatively difficult to install and manufacture
- More expensive
- Bulky

2. **Coaxial Cable**

Coaxial Cables are a group of wrapped and insulated wires capable of transmitting data at higher rates. They consist of a central copper wire surrounded by a PVC insulation over which there is a sleeve of copper mesh.The copper mesh sleeve is shielded again by PVC material.Signal is transmitted by inner copper wire and is shielded by outer mesh. Coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.



Advantages:

- High Bandwidth
- Better noise Immunity
- Easy to install and expand
- Inexpensive
- Long distance transmission

Disadvantages:

- Single cable failure can disrupt the entire network

3. **Optical Fibre Cable**

Optical fibers are long, thin strands of very pure glass about the diameter of a human hair. The optical fiber consists of three concentric elements, the core, the cladding and the outer coating, often called the buffer. The core is usually made of glass or plastic. The core is the light-carrying portion of the fiber. The cladding surrounds the core. The cladding is made of a material with a slightly lower index of refraction than the core. This difference in the indices causes total internal reflection to occur at the core-cladding boundary along the length of the fiber. Light is transmitted down the fiber and does not escape through the sides of the fiber.

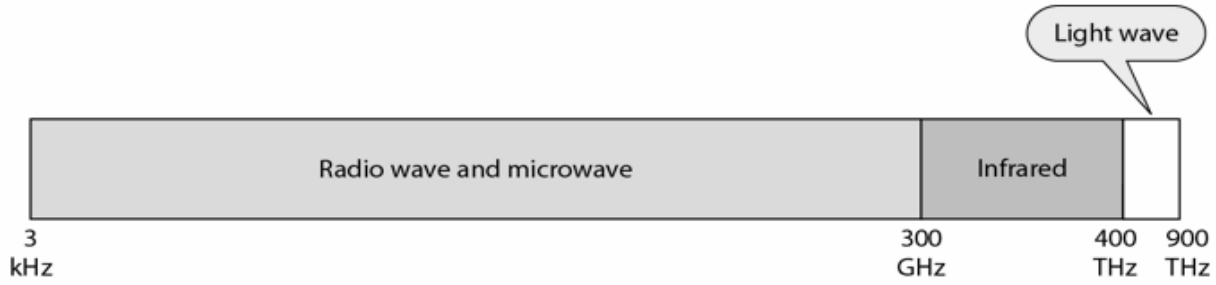
the outer layer, which serves as a "shock absorber" to protect the core and cladding from damage. The coating usually comprises one or more coats of a plastic material to protect the fiber from the physical environment. Sometimes metallic sheaths are added to the coating for further physical protection.
The cable can be unidirectional or bidirectional.
Advantages:

- Increased capacity and bandwidth
- Light weight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials
- Analog and digital transmissions
- Security from tampering

Disadvantages:

- Difficult to install and maintain
- High cost
- Fragile

2. **Unguided Media:**
The below figure shows the part of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, used for wireless communication.



1. Radio Waves

Electromagnetic waves ranging in frequencies between 3 KHz and 1 GHz are normally called radio waves.Radio waves are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. A sending antenna sends waves that can be received by any receiving antenna. The omnidirectional property has disadvantages, too. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.

Radio waves, particularly with those of low and medium frequencies, can penetrate walls. This characteristic can be both an advantage and a disadvantage. It is an advantage because an AM radio can receive signals inside a building. It is a disadvantage because we cannot isolate a communication to just inside or outside a building

Applications of Radio Waves

- The omnidirectional characteristics of radio waves make them useful for multicasting in which there is one sender but many receivers.
- AM and FM radio, maritime radio, cordless phones, and paging are the examples

2. Microwaves

Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves. Microwaves are unidirectional. When an antenna transmits microwaves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas.For increasing the distance served by terrestrial microwave, repeaters can be installed with each antenna .The signal received by an antenna can be converted into transmittable form and relayed to next antenna

The following describes some characteristics of microwaves propagation:

- Microwave propagation is line-of-sight. Since the towers with the mounted antennas need to be in direct sight of each other, towers that are far apart need to be very tall.
- Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside the buildings.
- The microwave band is relatively wide, almost 299 GHz. Therefore, wider sub-bands can be assigned and a high data rate is possible.
- Use of certain portions of the band requires permission from authorities
- They are used in cellular phones, satellite networks and wireless LANs.

Disadvantages of Microwave Transmission

- It is very costly

3. Satellite Microwave

This is a microwave relay station which is placed in outer space. The satellites are launched either by rockets or space shuttles. These are positioned 36000 Km above the equator with an orbit speed that exactly matches the rotation speed of the earth. As the satellite is positioned in a geo-synchronous orbit, it is stationary relative to earth and always stays over the same point on the ground. This is usually done to allow ground stations to aim antennas at a fixed point in the sky.

Features of Satellite Microwave

- Bandwidth capacity depends on the frequency used.
- Satellite microwave deployment for orbiting satellites is difficult.

Advantages of Satellite Microwave

- Transmitting station can receive back its own transmission and check whether the satellite has transmitted information correctly.
- A single microwave relay station which is visible from any point.

Disadvantages of Satellite Microwave

- Satellite manufacturing cost is very high
- Cost of launching satellite is very expensive
- Transmission highly depends on whether conditions, it can go down in bad weather

4. Infrared Waves

Infrared waves, with frequencies from 300 GHz to 400 THz, can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one system and another, a short-range communication system in one room cannot be affected by another system in the next room.

When we use infrared remote control, we do not interfere with the use of the remote by our neighbours. However, this same characteristic makes infrared signals useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

Applications of Infrared Waves

- The infrared band, almost 400 THz, has an excellent potential for data transmission. Such a wide bandwidth can be used to transmit digital data with a very high data rate.

4. MCQs based on the lecture

1. A _____ is the physical path over which a message travels.

a) Path
b) Medium
c) Protocol

d) Route

2. A _____ set of rules that governs data communication.

a) Protocols
b) Standards
c) RFCs
d) Servers

3. In computer network nodes are _____

a) the computer that originates the data
b) the computer that routes the data
c) the computer that terminates the data
d) all of the mentioned

4. _____ cable consists of an inner copper core and a second conducting outer sheath.

A) Twisted-pair
B) Shielded twisted-pair
C) Coaxial
D) Fiber-optic

5. _____ are used for cellular phone, satellite, and wireless LAN communications.
   A) Radio waves
   B) Infrared waves
   C) Microwaves
   D) none of the above
6. The inner core of an optical fiber is _____ in composition.
   A) copper
   B) glass or plastic
   C) bimetallic
   D) liquid

5. References:

1. https://en.wikiversity.org/wiki/Introduction_to_Computers/ available under the Creative Commons Attribution-ShareAlike License

2. https://courses.lumenlearning.com/computerapps/chapter/reading-the-internet/
   License: *CC BY-SA: Attribution-ShareAlike*
3. https://psu.pb.unizin.org/ist110/chapter/2-2-computer-networks/
   licensed under a Creative Commons Attribution-ShareAlike 4.0
4. https://commotionwireless.net/docs/cck/networking/learn-networking-basics/
   licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
5. **P. K. Sinha** & Priti Sinha , "**Computer Fundamentals**", BPB Publications, Chapter 17
6. All images used in the document are royalty free downloaded from https://stock.adobe.com/in/ or self made.

Outline of lecture-2

1. Network Criteria

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

Performance

Performance can be measured in many ways, including transit time and response time.

Transit time is the amount of time required for a message to travel from one device to another.

Response time is the elapsed time between an inquiry and a response.

Performance is often evaluated by following networking metrics: throughput and delay.

Bandwidth:commonly measured in bits/second is the maximum data transmission rate possible on a network. For optimal network operations, we want to get as close to our maximum bandwidth as possible without reaching critical levels. This indicates that the network is sending as much data as it can within a period of time.

Throughput measures the network's actual data transmission rate, which can vary wildly through different areas of the network. While a network's bandwidth measures the theoretical limit of data transfer, throughput tells you how much data is actually being sent. Specifically, throughput measures the percentage of data packets that are successfully being sent; a low throughput means there are a lot of failed or dropped packets that need to be sent again.

Network delay. It specifies the latency for a bit of data to travel across the network from one communication endpoint to another.We often need more throughput and less delay. However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

Reliability

In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

Security

Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

2. Types of Connection

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. There are two possible types of connections: point-to-point and multipoint.

Point-to-Point

A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. When we change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

Multipoint

A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link. In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the

link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.

3. Network Topologies

The term topology refers to the way in which a network is laid out physically.The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are four basic topologies possible: mesh, star, bus, and ring. The choice of topology for a network depends on factors such as :desired performance, desired reliability, size of the system, cost, availability of communication lines etc.

Mesh

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. The control is distributed with each node deciding its communication priorities.

Advantages:

- The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
- A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
- There is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it.
- A point-to-point link makes fault identification and fault isolation easy.

Disadvantages:

- The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required. If there are n nodes in the network, n(n-1)/2 links are required.
- Every device must be connected to every other device, installation and reconnection are difficult.

- The bulk of the wiring can be greater than the available space can accommodate.
- The hardware required to connect each link (I/O ports and cable) is very expensive.

  An example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

Star Topology

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub or host node. The devices are not directly linked to one another.A star topology does not allow direct traffic between devices. If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.

Advantages:

- A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure.
- Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.
- If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation.
- As long as the hub is working, it can be used to monitor link problems and bypass defective links.

Disadvantages:

- One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead. Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus). High-speed LANs often use a star topology with a central hub.

Bus Topology

A bus topology is a multipoint topology in which one long cable acts as a backbone to link all the devices in a network .That is all nodes are attached to the

same communication line. When a node wants to send a message to another node, it appends the destination address to the message and checks whether the line is free. As soon as the line is free, it broadcasts the message on the line. The message is picked up by the addressee node that sends an acknowledgement to the source node and frees the line. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

Advantages:

- Ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies.
- Failure of a node does not affect the communication among other nodes.

Disadvantages:

- Difficult reconnection and fault isolation.
- A fault or break in the bus cable stops all transmission, even between devices on the same side of the line. Ethernet LANs can use a bus topology, but they are less popular now.

Ring Topology

In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along .

Advantages:

- A ring is relatively easy to install and reconfigure. To add or delete a device requires changing only two connections.
- In addition, fault isolation is simplified.

Disadvantages:

- Generally in a ring, a signal is circulating at all times. The communication delay is proportional to the number of nodes in the network.

- In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

Ring topology was prevalent when IBM introduced its local-area network Token Ring. Today, the need for higher-speed LANs has made this topology less popular.

Hybrid Topology

A network can be a hybrid that is a combination of two or more different network topologies. Exact configuration depends on the needs and structure of organization. For example, we can have a main star topology with each branch connecting several stations in a bus topology.

A hybrid topology: a star backbone with three bus networks

4. MCQs based on the lecture

1. Physical or logical arrangement of network is _____

a) Topology
b) Routing
c) Networking
d) Control

2. Which network topology requires a central controller or hub?

a) Star
b) Mesh
c) Ring
d) Bus

3. _____ topology requires a multipoint connection.

a) Star
b) Mesh
c) Ring
d) Bus

4.Which network topology is a combination of two or more topologies?

a)Hybrid
b)Ring
c)Mesh

d)Bus

5. **References:**

1. **P. K. Sinha** & Priti Sinha , "**Computer Fundamentals**", BPB Publications, Chapter 17.
2. Behrouz A. **Forouzan**," **Data Communication and Networking"** (2003)., Edition, 4th. ISBN, 978-0073376226.
3. All images used in the document are self made using google drawing.

Outline of lecture-3

1. Data Communication:

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware and software. The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

I. Delivery. The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

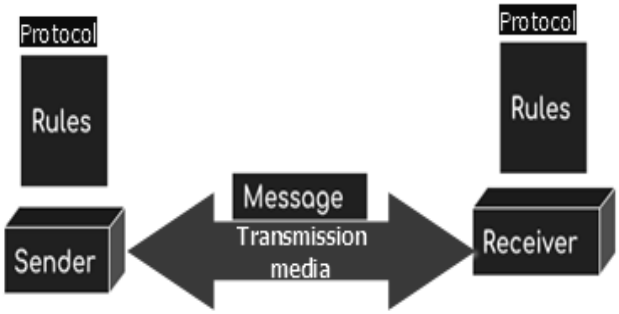
2. Accuracy. The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

3. Timeliness. The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.

4. Jitter. Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 30 ms. If some of the packets arrive with 30ms delay and others with 40ms delay, an uneven quality in the video is the result.

Components of Data Communication:

A data communications system has five components. Figure shows the five components of data communication



1. Message. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
2. Sender. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. Receiver. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
4. Transmission medium. The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
5. Protocol. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

2. DATA TRANSMISSION MODES

There are three ways, or modes, of transmitting data from one point to another. These are simplex, half-duplex, and full-duplex.

Simplex

In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive. Keyboards and traditional monitors are examples of simplex devices. The key-board can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

Half-Duplex

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa.The half-duplex mode is like a one-lane road with traffic allowed in both direc- tions. When cars are traveling in one direction, cars going the other way must wait. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) radios are both half-duplex systems. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.

Full-Duplex

In full-duplex mode, both stations can transmit and receive simultaneously.The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time. In full-duplex mode,signals going in one direction share the capacity of the link: with signals going in the other direction.

This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions. One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.

3. CENTRALIZED VS DISTRIBUTED COMPUTING SYSTEMS

Centralized computing is computing done at a central location called server or host, using terminals that are attached to a central computer over the network. The computer itself may control all the peripherals directly (if they are physically connected to the central computer), or they may be attached via a terminal. In the centralized data networks all the data is maintained in central server and to access the information one must request the server, the main computer of the system. The terminals may be text terminals or thin clients, for example.It offers greater security over decentralized systems because all of the processing is controlled in a central location. In addition, if one terminal breaks down, the user can simply go to another terminal and log in again, and all of their files will still be accessible.

Advantages of Centralized System –

- Easy to physically secure. It is easy to secure and service the server and client nodes by virtue of their location
- Smooth and elegant personal experience – A client has a dedicated system which he uses(for example, a personal computer) and the company has a similar system which can be modified to suit custom needs
- Dedicated resources (memory, CPU cores, etc)
- More cost efficient for small systems upto a certain limit – As the central systems take less funds to set up, they have an edge when small systems have to be built
- Quick updates are possible – Only one machine to update.
- Easy detachment of a node from the system. Just remove the connection of the client node from the server and node detached.

This type of arrangement does have some disadvantages.

Disadvantages of Centralized System –

- Highly dependent on the network connectivity – System can fail if the nodes lose connectivity as there is only one central node.
- No graceful degradation of system – abrupt failure of the entire system
- Less possibility of data backup. If the server node fails and there is no backup, you lose the data straight away
- Difficult server maintenance – There is only one server node and due to availability reasons, it is inefficient and unprofessional to take the server down for maintenance. So, updates have to be done on-the-fly(hot updates) which is difficult and the system could break.

Another disadvantage is that central computing relies heavily on the quality of administration and resources provided to its users. Should the central computer be

inadequately supported by any means (e.g. size of home directories, problems regarding administration), then the usage will suffer greatly. The reverse situation, however, (i.e., a system supported better than your needs) is one of the key advantages to centralized computing.

Distributed Computing system:

A distributed computing system is a collection of computers which may be geographically far apart are connected by a communication network, and in which messages, processing tasks, programs, data, and other resources are transmitted between cooperating computer systems. Such an arrangement enables the sharing of many hardware and software resources as well as information among several users who may be sitting far away from each other. It also increases the usability of computers by bringing them closer to the end users and by integrating them into daily business activities at the locations at which these activities take place. The individual computers of a distributed computing system are often referred to as nodes. It is obvious that distributed computing systems are much more complex and difficult to build than traditional centralized systems.

The major advantages that have led to the emergence and popularity of distributed computing systems are as follows

1. Inherently distributed applications. Several applications are inherently distributed in nature and require a distributed computing system for their realization. A few examples of inherently distributed applications are electronic mail facility, a computerized worldwide airline reservation system, a computerized banking system in which a customer can deposit/withdraw money from his or her account from any branch of the bank, and a factory automation system controlling robots and machines all along an assembly line.

2. Information sharing among distributed users. In a distributed computing system, information generated by one of the users can be easily and efficiently shared by the users working at other nodes of the system. For example, a project can be performed by two or more users who are geographically far off from each other but whose computers are a part of the same distributed computing system. In this case, although the users are geographically separated from each other, they can work in cooperation, for example, by transferring the files of the project, logging on to each other's remote computers to run programs, and exchanging messages by electronic mail to coordinate the work.

3. Resource sharing. Information is not the only thing that can be shared in a distributed computing system. Sharing of software resources such as software libraries and databases as well as hardware resources such as printers, hard disks,

and plotters can also be done in a very effective way among all the computers and the users of a single distributed computing system.

4. Better price-performance ratio. Distributed computing systems potentially have a much better price-performance ratio than a single large centralized system because they facilitate resource sharing among multiple computers. For example, a single unit of expensive peripheral devices such as color laser printers, high-speed storage devices, and plotters can be shared among all the computers of the same distributed computing system. If these computers are not linked together with a communication network, each computer must have its own peripherals, resulting in higher cost.

5. Shorter response times and higher throughput. Multiple processors of a distributed computing system can be utilized properly for providing shorter response times and higher throughput than a single-processor centralized system.

6. Higher reliability. Reliability refers to the degree of tolerance against errors and component failures in a system. A reliable system prevents loss of information even in the event of component failures. The multiplicity of storage devices and processors in a distributed computing system allows the maintenance "of multiple copies of critical information within the system and the execution of important computations redundantly to protect them against catastrophic failures. With this approach, if one of the processors fails, the computation can be successfully completed at the other processor, and if one of the storage devices fails, the information can still be used from the other storage device. Furthermore, the geographical distribution of the processors and other resources in a distributed computing system limits the scope of failures caused by natural disasters.

7. Extensibility and incremental growth. Another major advantage of distributed computing systems is that they are capable of incremental growth. That is, it is possible to gradually extend the power and functionality of a distributed computing system by simply adding additional resources (both hardware and software) to the system as and when the need arises. For example, additional processors can be easily added to the system to handle the increased workload of an organization that might have resulted from its expansion.

8. Better flexibility in meeting users' needs. Different types of computers are usually more suitable for performing different types of computations. For example, computers with ordinary power are suitable for ordinary data processing jobs, whereas high-performance computers are more suitable for complex mathematical computations. In a centralized system, the users have to perform all types of computations on the only available computer. However, a distributed computing system may have a pool of different types of computers, in which case

the most appropriate one can be selected for processing a user's job depending on the nature of the job.

4. NETWORK OPERATING SYSTEMS

A network operating system is an operating system designed for the sole purpose of supporting workstations, database sharing, application sharing and file and printer access sharing among multiple computers in a network. Basically, a network operating system controls other software and computer hardware to run applications, share resources, protect data and establish communication. Individual computers run client operating systems, while network systems create the software infrastructure for wireless, local and wide area networks to function.

Certain standalone operating systems, such as Microsoft Windows NT and Digital's OpenVMS, come with multipurpose capabilities and can also act as network operating systems. Some of the most well-known network operating systems include Microsoft Windows Server 2003, Microsoft Windows Server 2008, Linux and Mac OS X.

Common tasks associated with network operating systems include:

- User administration
- System maintenance activities like backup
- Tasks associated with file management
- Security monitoring on all resources in the network
- Setting priority to print jobs in the network

FEATURES OF NOS

1. Basic Operating Features

Network operating systems support the basic underlying operating features of networks. Basic operating system features support like protocol support, processor support, hardware detection and multiprocessing support for applications.These include support for processors and the various protocols that allow computers to share data. Many network operating systems can detect hardware within the system to allow for asset discovery within the network. Also, network operating systems support the processing of other software applications that run on both individual computers and within the network.

2. Security Features

Network operating systems support a number of security features that control access to the network.Security features like authentication, restrictions, authorizations and access control. These include authorization and permission for access to the network, with specific control of features such as user management, log-on controls and passwords. Systems also provide access control for features such as remote access and network monitoring.

3. Networking

A network operating system is the platform on which computer networking takes place. Basic features allow for file, print and Internet connections. Data backup and replication functions are controlled through the network operating system. The management of connective systems for local and wide area networks (LANs and WANs), such as routing, switches and other ports are configured and managed through network operating system features.

4. Administrative Interface

One of the features of a network operating system is that it has an administrative interface that allows a network administrator to monitor and maintain the system. This interface will have a menu that allows the administrator to perform functions such as formatting hard drives and setting up security protocols for both the system and individual users. He can also and configure security and data backup requirements for individual computers or the network as a whole.

TYPES OF NOS:

1. **Peer-to-peer** network operating systems allow users to share resources and files located on their computers and to access shared resources found on other computers. In a peer-to-peer network, all computers are considered equal; they all have the same privileges to use the resources available on the network. Peer-to-peer networks are designed primarily for small to medium local area networks. Windows for Workgroups is an example of the program that can function as peer-to-peer network operating systems.

Advantages of Peer-to-Peer(P2P) Operating System are as follows:

• Less requirement of hardware is there.

• No server needs to be established.

• Its setup process is natural.

Disadvantages of Peer-to-Peer(P2P) Operating System are as follows:

• It has no central location for storage, i.e. different systems have different storage capacity.

• It has less security as compared to the client-server model.

2. **Client/server** network operating systems allow the network to centralise functions and applications in one or more dedicated file servers. The file servers become the heart of the system, providing access to resources and providing security. The workstations (clients) have access to the resources available on the file servers. The network operating system allows multiple users to share the same resources irrespective of physical location simultaneously. Novell Netware and Windows 2000 Server are examples of client/ server network operating systems.

Each computer in the workgroup runs an autonomous operating system; yet cooperates to allow a variety of facilities including sharing of files, sharing of hardware resources and execution of remote machines etc.

Some resources, of which dedicated hardware devices such as printers, tape drives are connected to and managed by a particular machine and are made available to other machines in the network via a service. A typical example of such a system is a set of workstations connected through a local area network (LAN). Every workstation has its operating system every user has its workstation in exclusive use and cooperates to allow a variety of facilities including sharing of files, sharing of hardware resources and execution of remote machines etc. A user can execute a login command to connect to another station and also can access a set of shared files maintained by a workstation named/file server.

Advantages of Client Server Operating System are as follows:

• In this, security to the machines is provided through the server.

• Here, hardware can be easily connected to the system.

• Also, new technology is easily integrated into the system.

• The central server is more stable in a client-server model.

• Hardware and the operating system can be specialised.

• In this model, different machines can remotely access the server from different locations.

Disadvantages Client Server Operating System are as follows:

• It seems to be costly as buying and running a server is cost effective.

• Also, here we always have to depend on the central location for any type of operation like for storage, for accessing data etc..

• It requires regular maintenance.

• Daily updation is required as per requirement.

5. MCQs

Q1:Operating Systems that provide all necessary features to communicate over the network to access and share resources is known as:

a)disk operating system

b)network operating system

c)disk operating system

d)MAC operating system

Q2: 1. A term that defines the direction of flow of information between devices.
a)interconnectivity
b)intraconnectivity
c)transmissionmode
d) transmission

Q3: Transmission mode controls the direction of signal flow.
a)True
b) False

Q4: Which of the following isn't a type of transmission mode?
a)physical
b)simplex
c)fullduplex
d) half duplex

Q5: A transmission mode that can transmit data in both the directions but transmits in only one direction at a time.
a)simplex
b)halfduplex
c)fullduplex
d) semi-duplex

6. References:

4. **P. K. Sinha** & Priti Sinha , "**Computer Fundamentals**", BPB Publications, Chapter 17.
5. Behrouz A. **Forouzan**," **Data Communication and Networking"** (2003)., Edition, 4th. ISBN, 978-0073376226.
6. All images used in the document are self made using google drawing.

Outline Lecture 4

1COMMUNICATION PROTOCOLS

2 ELECTRONIC MAIL

3 MCQs

4 REFERENCES

1. COMMUNICATION PROTOCOLS

A protocol is a set of formal operating rules, procedures, or conventions that govern a given process. A communication or network protocol, therefore, describes the rules that govern the transmission of data over communication networks. These rules provide a method for orderly and efficient exchange of data between the sender and the receiver and for the proper interpretation of controls and data transmitted as raw bits and bytes. These rules are embedded in the data communication software.

Roles of a Communication Protocol

In any computer network, a communication protocol normally performs the following functions for the efficient and error-free transmission of data. It has a separate set of rules (implemented in software) for performing each of these functions.

1. Data sequencing. It refers to breaking a long message into smaller packets of fixed size. Data sequencing rules define the method of numbering (or sequencing) packets to detect loss or duplication of packets, and to correctly identify packets that belong to the same message.

2. Data routing. Routing algorithms are designed to find the most efficient paths between a source and a destination. They can handle varying degrees of traffic on the present network configuration with optimal time utilization.

3. Data formatting. Data formatting rules define which group of bits or characters within a packet constitutes data, control, addressing, or other information.

4. Flow control. A communication protocol also prevents a fast sender from overwhelming a slow receiver. It ensures resource sharing and protection against traffic congestion by regulating the flow of data on the communication lines.

5. Error control. These rules are designed to detect errors in messages and to ensure transmission of correct messages. The most common method for correcting errors is to retransmit the erroneous message block. This method requires coordination between the sender and the receiver nodes so that the block having error is discarded by the receiver node and is retransmitted by the sender node.

6. Precedence and order of transmission. These rules condition all nodes about when to transmit their data and when to receive data from other nodes. It is ensured

that all nodes get a chance to use the communication lines and other resources of the network depending upon the priorities assigned to them.

7. Connection establishment and termination. These rules define how connections are established, maintained and terminated when two nodes of a network want to communicate with each other.

8. Data security. Providing data security and privacy is also built into most communication software packages. It prevents access of data by unauthorized users.

9. Log information. Several data communication software are also designed to develop log information, which consists of all jobs and data communications tasks that have taken place. Such information is normally used for charging the various users of the network based on their usage of the network resources.

There are several types of network protocols.

1. THE INTERNET PROTOCOL SUITE

The Internet protocol suite is the conceptual model and set of communications protocols used in the Internet and similar computer networks. It is commonly known as TCP/IP because the foundational protocols in the suite are the Transmission Control Protocol (TCP) and the Internet Protocol (IP). Its implementation is a protocol stack.

The Internet protocol suite provides end-to-end data communication specifying how data should be packetized, addressed, transmitted, routed, and received. This functionality is organized into four abstraction layers, which classify all related protocols according to the scope of networking involved. From lowest to highest, the layers are the link layer, containing communication methods for data that remains within a single network segment ; the internet layer, providing internetworking between independent networks; the transport layer, handling host-to-host communication; and the application layer, providing process-to-process data exchange for applications.

2. Transmission Control Protocol (TCP)

The Transmission Control Protocol is the core protocol of the internet protocol suite. It originated in the network implementation in which it complemented the Internet Protocol. Therefore the entire suite is commonly referred to as TCP/IP. TCP provides reliable delivery of a stream of octets over an IP network. Ordering and error-checking are main characteristics of the TCP. All major Internet applications such as World Wide Web, email and file transfer rely on TCP.

3. Internet Protocol(IP)

The Internet Protocol is the principal protocol in the Internet protocol suite for relaying data across networks. Its routing function essentially establishes the internet. Historically it was the connectionless datagram service in the original Transmission Control Program; the other being the connection oriented protocol(TCP). Therefore, the Internet protocol suite is referred to as TCP/IP.

4. Hypertext Transfer Protocol (HTTP)

The HTTP is the foundation of data communication for the World Wide Web. The hypertext is structured text that uses hyperlinks between nodes containing texts. The HTTP is the application protocol for distributed and collaborative hypermedia information system.HTTP functions as a request–response protocol in the client–server computing model. A web browser, for example, may be the client and an application running on a computer hosting a website may be the server. The client submits an HTTP request message to the server. The server, which provides resources such as HTML files and other content, or performs other functions on behalf of the client, returns a response message to the client. The response contains completion status information about the request and may also contain requested content in its message body.

5. File Transfer Protocol (FTP)

The FTP is the most common protocol used in the file transferring in the Internet and within private networks.A file may contain any type of digital information - text document, image, artwork, movie, sound, software, etc. Hence, anything that can be stored on a computer can be moved with FTP service.The default port of FTP is 20/21.By using the FTP service, a file transfer takes place in the following manner:

1. A user executes the ftp command on his/her local computer, specifying the address of the remote computer as a parameter.

2. An FTP process running on the user's computer (called FTP client process) establishes a connection with an FTP process running on the remote computer (called FTP server process).

3. The user is then prompted for login name and password to ensure that the user is allowed to access the remote computer.

4. After successful login, the desired file(s) are downloaded or uploaded by using get (for downloading) and put (for uploading) commands. The user can also list directories or move between directories of the remote computer before deciding the file(s) to be transferred.

6. Secured Shell (SSH)

SSH is the primary method used to manage the network devices securely at the command level. It usually used as the alternative of the Telnet which does not support secure connections. The default port of SSH is 22.

7. Telnet

Telnet is the primary method used to manage network devices at the command level. The telnet service allows an Internet user to log in to another computer somewhere on the Internet. That is, a user can execute the telnet command on his/her local computer to start a login session on a remote computer. This action is also called "remote login."

To start a remote login session, the user types the command telnet and the address of the remote computer on the terminal of his/her local computer. The user then receives a prompt asking to enter a login name (user ID) and a password to ensure that the user has the access rights for accessing the remote computer. If the user specifies a correct login name and password, he/she gets logged in to the remote computer. Once the login session is established with the remote computer, telnet enters the input mode and anything typed on the terminal of the local computer by the user is sent to the remote computer for processing.

Unlike SSH, Telnet does not provide a secure connection, but it provides a basic unsecured connection.The default port of Telnet is 23.

8. Simple Mail Transfer Protocol (SMTP)

SMTP is used for two primary functions. It is used to transfer email from source to destination between mail servers and it is used to transfer email from end users to a mail system.The default port of SMTP is 25 and secured (SMTPS) is 465 (Not standard).

9. Domain Name System (DNS)

Domain name system is used to convert the domain name to IP address. There are root servers, TLDs and authoritative servers in the DNS hierarchy.The default port of DNS is 53.

10. Post Office Protocol version 3 (POP 3)

The Post Office Protocol version 3 is one of the two main protocols used to retrieve mail from the internet. It is very simple as it allows the client to retrieve complete content from the server mail box and deletes contents from the server.The default port of POP3 is 110 and secured is 995.

11.Internet Message Access Protocol (IMAP)

IMAP version 3 is another main protocol that used to retrieve mail from a server. IMAP does not delete the content from the mail box of the server.The default port of IMAP is 143 and secured is 993.

12.Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol is used to manage networks. It has abilities to monitor, configure and control network devices. SNMP traps can also be configured on network devices to notify a central server when specific action are occurring.The default port of SNMP is 161/162.

13. Hypertext Transfer Protocol over SSL/TLS (HTTPS)

HTTPS is used with HTTP to provide same services, but with a secured connection which is provided by SSL or TLS.The default port of HTTPS is 443.

2. ELECTRONIC MAIL

The electronic mail service (known as e-mail in short) allows an Internet user to send a mail (message) to another Internet user in any part of the world in a near-real-time manner. The message may not reach its destination immediately, but may take anywhere from few seconds to several minutes, because it must be passed from one network to another until it reaches its destination.

E-mail service has many similarities with the postal mail service that all of us are familiar with. All Internet users have an e-mail address, just like all of us have a

postal address. Each Internet user has a logical mail box just like each one of us has a mail box in our house. When sending a mail to another user, the sender

specifies the e-mail address of the receiver just as we write the postal address of the receiver in the postal mail system. The e-mail service delivers an already sent mail into the receiver's mail box. The receiver extracts the mail from the mail box and reads it at his/her own convenient time just like in a postal mail system. After reading the message, the receiver can save it, delete it, pass it on to someone else, or respond by sending another message back. Email operates across computer networks, primarily the Internet. Today's email systems are based on a store-and-forward model. Email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need to connect, typically to a mail server or a webmail interface to send or receive messages or download it. Originally an ASCII text-only communications medium, Internet email was extended by Multipurpose Internet Mail Extensions (MIME) to carry text in other character sets and multimedia content attachments.

Messages in e-mail service can contain not only text documents but also image, audio and video data. The only restriction is that the data to be sent must be digitized, that is, converted to a computer-readable format.

Let’s take a look at how email is sent from a strictly technical standpoint.

- Once an email is composed and the send button is clicked, the message is sent to the Mail Transfer Agent (MTA). This communication is done via the Simple Mail Transfer Protocol (SMTP).
- The SMTP queries the Domain Name System (DNS) to find the address of the recipient. This is done with the help of a Mail eXchanger (MX) record. The MX record is a resource record which specifies the mail server of a domain name. Once located, the SMTP server will send the message to that server.
- The next step involves transferring the message between mail servers. The SMTP has done its job of routing the message to the destination server. The message is now in the recipient’s mail server (MTA). The receiving server will store the message and make it available to the recipient who can access it via web, POP, or IMAP protocols.

Types

Web-based email

Many email providers have a web-based email client (e.g. AOL Mail, Gmail, Outlook.com and Yahoo! Mail). This allows users to log into the email account by using any compatible web browser to send and receive their email. Mail is typically not downloaded to the web client, so can't be read without a current Internet connection.

POP3 email servers

The Post Office Protocol 3 (POP3) is a mail access protocol used by a client application to read messages from the mail server. Received messages are often deleted from the server. POP supports simple download-and-delete requirements. POP3 allows you to download email messages on your local computer and read them even when you are offline.

IMAP email servers

The Internet Message Access Protocol (IMAP) provides features to manage a mailbox from multiple devices. Small portable devices like smartphones are increasingly used to check email while traveling and to make brief replies, larger devices with better keyboard access being used to reply at greater length. IMAP shows the headers of messages, the sender and the subject and the device needs to request to download specific messages. Usually, the mail is left in folders in the mail server.

MAPI email servers

Messaging Application Programming Interface (MAPI) is used by Microsoft Outlook to communicate to Microsoft Exchange Server - and to a range of other email server products such as Axigen Mail Server, Kerio Connect, , HP OpenMail, IBM Lotus Notes, where vendors have added MAPI support to allow their products to be accessed directly via Outlook

3. MCQs

Q1: Protocol is a set of
a) Formats
b) Procedures
c) Formats & Procedures
d) None of the mentioned

Q2: The key element of a protocol is
a)Syntax
b)Semantics
c)timing
d)All the above

Q3: The term HTTP stands for?

a. Hyper terminal tracing program
b. Hypertext tracing protocol
c. Hypertext transfer protocol
d. Hypertext transfer program

4. References:

- **P. K. Sinha** & Priti Sinha , "**Computer Fundamentals**", BPB Publications, Chapter 17.
- Behrouz A. **Forouzan**," **Data Communication and Networking"** (2003)., Edition, 4th. ISBN, 978-0073376226.
- https://en.wikipedia.org/wiki/Email available under the Creative Commons Attribution-ShareAlike License

- All images used in the document are royalty free downloaded from https://stock.adobe.com/in/ or self made.

Outline Lecture 5

1. TYPES OF NETWORK
2. INTRANET
3. MCQS
4. REFERENCES

1. NETWORK TYPES:

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications. A computer network can be categorized by their size. A computer network is mainly of four types:

- LAN(Local Area Network)
- PAN(Personal Area Network)
- MAN(Metropolitan Area Network)
- WAN(Wide Area Network)

LAN(Local Area Network)

Local area networks are a group of computers connected with each other in small places such as school, hospital, apartment etc through a communication medium such as twisted pair, coaxial cable, etc. It is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.LAN is secure because there is no outside connection with the local area network thus the data which is shared is safe on the local area network and can't be accessed outside. LAN due to their small size are considerably faster, their speed can range anywhere from 100 to 100Mbps. We can use different types of topologies through LAN, these are Star, Ring, Bus, Tree etc.LAN can be a simple network like connecting two computers, to share files and network among each other while it can also be as complex as interconnecting an entire building.

PAN(Personal Area Network)

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters. It is used for connecting computer devices, laptop, mobile phones, media player and play stations that are used to develop the personal area network. There are two types of Personal Area Network:
- Wired Personal Area Network
- Wireless Personal Area Network

Wireless Personal Area Network: Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.

Wired Personal Area Network: Wired Personal Area Network is created by using the USB.

- MAN(Metropolitan Area Network)

A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LANs to form a larger network.The size of the Metropolitan area network is larger than LANs and smaller than WANs(wide area networks), a MANs covers the larger area of a city or town.Government agencies use MAN to connect to the citizens and private industries.In MAN, various LANs are connected to each other through a telephone exchange line.

It has a higher range than Local Area Network(LAN).

Uses Of Metropolitan Area Network:

- MAN is used in communication between the banks in a city.

- It can be used in an Airline Reservation.
- It can be used in a college within a city.
- It can also be used for communication in the military.

WAN(Wide Area Network)

A Wide Area Network is a network that extends over a large geographical area such as states or countries through a telephone line, fibre optic cable or satellite links.Wide area network provides long distance transmission of data. The size of the WAN is larger than LAN and MAN. A WAN can cover a country, continent or even a whole world. Internet connection is an example of WAN. Other examples of WAN are mobile broadband connections such as 3G, 4G etcA Wide Area Network is quite bigger network than the LAN.A Wide Area Network is widely used in the field of Business, government, and education.

Examples of Wide Area Network:

- Mobile Broadband: A 4G network is widely used across a region or country.

Advantages Of Wide Area Network:

Following are the advantages of the Wide Area Network:

- Geographical area: A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. The internet provides a leased line through which we can connect with another branch.

Disadvantages of Wide Area Network:

The following are the disadvantages of the Wide Area Network:

- Security issue: A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
- Needs Firewall & antivirus software: The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
- High Setup cost: An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
- Troubleshooting problems: It covers a large area so fixing the problem is difficult.

.

2. INTRANET:

An intranet is a private network based on the internet protocol such as Transmission Control protocol and internet protocol. An intranet belongs to an organization which is only accessible by the organization's employee or members. The main aim of the intranet is to share the information and resources among the organization employees. An intranet provides the facility to work in groups and for teleconferences.

Intranet advantages:

- Communication: It provides a cheap and easy communication. An employee of the organization can communicate with another employee through email, chat.
- Time-saving: Information on the intranet is shared in real time, so it is time-saving.
- Collaboration: Collaboration is one of the most important advantage of the intranet. The information is distributed among the employees of the organization and can only be accessed by the authorized user.
- Platform independency: It is a neutral architecture as the computer can be connected to another device with different architecture.
- Cost effective: People can see the data and documents by using the browser and distributes the duplicate copies over the intranet.

3. MCQs

Q1:The term WAN stands for?

a. Wide Area Net
b. Wide Access Network
c. Wide Area Network
d. Wide Access Net

Q2: The term LAN stands for?

a. Local Area Net
b. Local Aera Network
c. Local Array Network
d. Local Array Net

Q3: A LAN (Local Area Network) can cover a distance of ___ KM.

A) 2
B) 8
C) 16
D) 32

References

- https://computersciencewiki.org/index.php/Types_of_networks -Content is available under Creative Commons Attribution-NonCommercial-ShareAlike https://www.youtube.com/watch?v=Y8NClf4475Y - Creative Commons Attribution license (reuse allowed) leads to a reduction in the cost.
  - **P. K. Sinha** & Priti Sinha , "**Computer Fundamentals**", BPB Publications, Chapter 17.
  - Behrouz A. **Forouzan**," **Data Communication and Networking"** (2003)., Edition, 4th. ISBN, 978-0073376226.

OUTLINE LECTURE 6

1. INTERNET
2. IP ADDRESS
3. APPLICATION OF INTERNET
4. MCQS
5. REFERENCES

1. INTERNET

The Internet is the global system of interconnected computer networks that uses the Internet protocol suite (TCP/IP) to communicate between networks and devices. It is a network of networks that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries a vast range of information resources and services, such as the inter-linked hypertext documents and applications of the World Wide Web (WWW), electronic mail, telephony, and file sharing. The Internet has no single centralized governance in either technological implementation or policies for access and usage; each constituent network sets its own policies. The two principal name spaces in the Internet, the Internet Protocol address (IP address) space and the Domain Name System (DNS), are directed by a maintainer organization, the Internet Corporation for Assigned Names and Numbers (ICANN). The technical underpinning and standardization of the core protocols is an activity of the Internet Engineering Task Force (IETF), a non-profit organization of loosely affiliated international participants that anyone may associate with by contributing

technical expertise. A special computer DNS (Domain Name Server) is used to provide a name to the IP Address so that the user can locate a computer by a name. For example, a DNS server will resolve a name https://www.example.com to a particular IP address to uniquely identify the computer on which this website is hosted.

Internet protocol

The most prominent component of the Internet model is the Internet Protocol (IP). IP enables internetworking and, in essence, establishes the Internet itself. Two versions of the Internet Protocol exist, IPV4 and IPV6.

2. IP Addresses

For locating individual computers on the network, the Internet provides IP addresses. IP addresses are used by the Internet infrastructure to direct internet packets to their destinations. They consist of fixed-length numbers, which are found within the packet. IP addresses are generally assigned to equipment either automatically via DHCP, or are configured.

However the network also supports other addressing systems. Users generally enter domain names (e.g. "en.wikipedia.org") instead of IP addresses because they are easier to remember, they are converted by the Domain Name System (DNS) into IP addresses which are more efficient for routing purposes.

IPv4

Internet Protocol version 4 (IPv4) defines an IP address as a 32-bit number. Internet Protocol Version 4 is the initial version used on the first generation of the Internet and is still in dominant use. An IP address is generally shown as 4 octets of numbers from 0-255 represented in decimal form instead of binary form. For example, the address 168.212.226.204 represents the 32-bit binary number 10101000.11010100.11100010.11001100.

The binary number is important because that will determine which class of network the IP address belongs to. IPv4 addresses are composed of two parts. The first numbers in the address specify the network, while the latter numbers specify the specific host. A subnet mask specifies which part of an address is the network part, and which part addresses the specific host. It was designed to address up to ≈4.3 billion (109) hosts. However, the explosive growth of the Internet has led to

IPv4 address exhaustion, which entered its final stage in 2011, when the global IPv4 address allocation pool was exhausted.

IPv6

Because of the growth of the Internet and the depletion of available IPv4 addresses, a new version of IP IPv6, was developed in the mid-1990s, which provides vastly larger addressing capabilities and more efficient routing of Internet traffic. IPv6 uses 128 bits for the IP address and was standardized in 1998. IPv6 deployment has been ongoing since the mid-2000s. IPv6 is currently in growing deployment around the world, since Internet address registries (RIRs) began to urge all resource managers to plan rapid adoption and conversion.

3. Subnetwork

A subnetwork or subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting. Computers that belong to a subnet are addressed with an identical most-significant bit-group in their IP addresses. This results in the logical division of an IP address into two fields, the network number or routing prefix and the rest field or host identifier. The rest field is an identifier for a specific host or network interface.The routing prefix may be expressed in Classless Inter-Domain Routing (CIDR) notation written as the first address of a network, followed by a slash character (/), and ending with the bit-length of the prefix. For example, 198.51.100.0/24 is the prefix of the Internet Protocol version 4 network starting at the given address, having 24 bits allocated for the network prefix, and the remaining 8 bits reserved for host addressing. Addresses in the range 198.51.100.0 to 198.51.100.255 belong to this network. For IPv4, a network may also be characterized by its subnet mask or netmask, which is the bitmask that when applied by a bitwise AND operation to any IP address in the network, yields the routing prefix. Subnet masks are also expressed in dot-decimal notation like an address. For example, 255.255.255.0 is the subnet mask for the prefix 198.51.100.0/24.

4. APPLICATIONS OF INTERNET

The Internet carries many applications and services, most prominently the World Wide Web, including social media, electronic mail, mobile applications,

multiplayer online games, Internet telephony, file sharing, and streaming media services.

World Wide Web

The World Wide Web is a global collection of documents, images, multimedia, applications, and other resources, logically interrelated by hyperlinks and referenced with Uniform Resource Identifiers (URIs), which provide a global system of named references. URIs symbolically identifies services, web servers, databases, and the documents and resources that they can provide. Hypertext Transfer Protocol (HTTP) is the main access protocol of the World Wide Web. Web services also use HTTP for communication between software systems for information transfer, sharing and exchanging business data and logistic and is one of many languages or protocols that can be used for communication on the Internet

Communication

Email is an important communications service available via the Internet. Internet telephony is a common communications service realized with the Internet. VoIP systems now dominate many markets, and are as easy to use and as convenient as a traditional telephone.

Data transfer

File sharing is an example of transferring large amounts of data across the Internet. A computer file can be emailed to customers, colleagues and friends as an attachment. It can be uploaded to a website or File Transfer Protocol (FTP) server for easy download by others. It can be put into a "shared location" or onto a file server for instant use by colleagues. Streaming media is the real-time delivery of digital media for the immediate consumption or enjoyment by end users.

Usage

The Internet allows greater flexibility in working hours and location, especially with the spread of unmetered high-speed connections. Educational material at all levels from pre-school to post-doctoral is available from websites. The Internet in general and the World Wide Web in particular are important enablers of both formal and informal education. The Internet allows universities, in particular, researchers from the social and behavioral sciences, to conduct research remotely

via virtual laboratories, with profound changes in reach and generalizability of findings as well as in communication between scientists and in the publication of results. The low cost and nearly instantaneous sharing of ideas, knowledge, and skills have made collaborative work dramatically easier, with the help of collaborative software.

Social networking and entertainment

Many people use the World Wide Web to access news, weather and sports reports, to plan and book vacations and to pursue their personal interests. People use chat, messaging and email to make and stay in touch with friends worldwide, sometimes in the same way as some previously had pen pals. Social networking websites such as Facebook, Twitter, and Myspace have created new ways to socialize and interact. Users of these sites are able to add a wide variety of information to pages, to pursue common interests, and to connect with others.

Electronic business

Electronic business (e-business) encompasses business processes spanning the entire value chain: purchasing, supply chain management, marketing, sales, customer service, and business relationship. E-commerce seeks to add revenue streams using the Internet to build and enhance relationships with clients and partners.

4. MCQs

Q1: A collection of hyperlinked documents on the internet forms the ?

a. World Wide Web (WWW)
b. E-mail system
c. Mailing list
d. Hypertext markup language

Q2:The location of a resource on the internet is given by its?

a. Protocol
b. URL
c. E-mail address
d. ICQ

Q3: The term HTTP stands for?

a. Hyper terminal tracing program
b. Hypertext tracing protocol
c. Hypertext transfer protocol
d. Hypertext transfer program

Q4: The term FTP stands for?

a. File transfer program
b. File transmission protocol
c. File transfer protocol
d. File transfer protection

Q5: The maximum length (in bytes) of an IPv4 datagram is?

a. 32
b. 1024
c. 65535
d. 512

REFERENCES:

• P. K. Sinha & Priti Sinha , “Computer Fundamentals”, BPB Publications, Chapter 17.
• Behrouz A. Forouzan,” Data Communication and Networking” (2003)., Edition, 4th. ISBN, 978-0073376226.
• https://en.wikipedia.org/wiki/Internet available under the Creative Commons Attribution-ShareAlike License

OUTLINE LECTURE 7

1DNS

The Domain Name System (DNS) is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. By providing a worldwide, distributed directory service, the Domain Name System has been an essential component of the functionality of the Internet since 1985.

The Domain Name System delegates the responsibility of assigning domain names and mapping those names to Internet resources by designating authoritative name servers for each domain. A DNS name server is a server that stores the DNS records for a domain; a DNS name server responds with answers to queries against its database.

- DNS resolver - The recursor can be thought of as a librarian who is asked to go find a particular book somewhere in a library. The DNS recursor is a server designed to receive queries from client machines through applications such as web browsers. Typically the recursor is then responsible for making additional requests in order to satisfy the client's DNS query.
- Root nameserver - The root server is the first step in translating (resolving) human readable host names into IP addresses. It can be thought of like an index in a library that points to different racks of books - typically it serves as a reference to other more specific locations.
- TLD nameserver - The top level domain server (TLD) can be thought of as a specific rack of books in a library. This nameserver is the next step in the search for a specific IP address, and it hosts the last portion of a hostname (In example.com, the TLD server is "com").
- Authoritative nameserver - This final nameserver can be thought of as a dictionary on a rack of books, in which a specific name can be translated into its definition. The authoritative nameserver is the last stop in the nameserver query. If the authoritative name server has access to the requested record, it will return the IP address for the requested hostname back to the DNS Recursor (the librarian) that made the initial request.

The 8 steps in a DNS lookup:

1. A user types ‘example.com’ into a web browser and the query travels into the Internet and is received by a DNS recursive resolver.
2. The resolver then queries a DNS root nameserver (.).
3. The root server then responds to the resolver with the address of a Top Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, our request is pointed toward the .com TLD.
4. The resolver then makes a request to the .com TLD.
5. The TLD server then responds with the IP address of the domain’s nameserver, example.com.
6. Lastly, the recursive resolver sends a query to the domain’s nameserver.
7. The IP address for example.com is then returned to the resolver from the nameserver.
8. The DNS resolver then responds to the web browser with the IP address of the domain requested initially.

2. URL

A URL (Uniform Resource Locator) is a unique identifier used to locate a resource on the internet. It is also referred to as a web address. URLs consist of multiple parts -- including a protocol and domain name -- that tell a web browser how and where to retrieve a resource.End users use URLs by typing them directly into the address bar of a browser or by clicking a hyperlink found on a webpage, bookmark list, in an email or from another application.

How is a URL structured?

The URL contains the name of the protocol needed to access a resource, as well as a resource name. The first part of a URL identifies what protocol to use as the primary access medium. The second part identifies the IP address or domain name -- and possibly subdomain -- where the resource is located.

URL protocols include HTTP (Hypertext Transfer Protocol) and HTTPS (HTTP Secure) for web resources, mail to for email addresses, FTP for files on a File Transfer Protocol (FTP) server, and telnet for a session to access remote computers. Most URL protocols are followed by a colon and two forward slashes; “mail to” is followed only by a colon.

Optionally, after the domain, a URL can also specify:

- a path to a specific page or file within a domain;
- a network port to use to make the connection;

- a specific reference point within a file, such as a named anchor in an HTML file; and
- a query or search parameters used -- commonly found in URLs for search results.

Example:

Using the URL https://whatis.techtarget.com/search/query?q=URL as an example, components of a URL can include:

•. In this example, the protocol is https.

- Host name or domain name. For this example, whatis.techtarget.com.
- Port name. Usually not visible in URLs, but necessary. Always following a colon, port 80 is the default port for web servers, but there are other options. For example, :port80.
- Path. For this example, search/query.
- Query. Found in the URL of dynamic pages. The query consists of a question mark, followed by parameters. For this example, ?.
- Parameters. Pieces of information in a query string of a URL. Multiple parameters can be separated by ampersands (&). For this example, q=URL.
- Fragment. This is an internal page reference, which refers to a section within the webpage. It appears at the end of a URL and begins with a hashtag (#). Although not in the example above, an example could be #history in the URL https://en.wikipedia.org/wiki/Internet#History.

3. WEBSITE:

A website is a collection of web pages and related content that is identified by a common domain name and published on at least one web server. Notable examples are wikipedia.org, google.com, and amazon.com.All publicly accessible websites collectively constitute the World Wide Web. There are also private websites that can only be accessed on a private network, such as a company's internal website for its employees.Websites are typically dedicated to a particular topic or purpose, such as news, education, commerce, entertainment, or social networking. Hyperlinking between web pages guides the navigation of the site, which often starts with a home page.Users can access websites on a range of devices, including desktops, laptops, tablets, and smartphones. The software application used on these devices is called a web browser.

Static website

A static website is one that has web pages stored on the server in the format that is sent to a client web browser. It is primarily coded in Hypertext Markup Language

(HTML); Cascading Style Sheets (CSS) are used to control appearance beyond basic HTML. Images are commonly used to effect the desired appearance and as part of the main content. Audio or video might also be considered "static" content if it plays automatically or is generally non-interactive. This type of website usually displays the same information to all visitors. Although the website owner may make updates periodically, it is a manual process to edit the text, photos, and other content and may require basic website design skills and software. Static websites may still use server side includes (SSI) as an editing convenience, such as sharing a common menu bar across many pages.

Dynamic website

A dynamic website is one that changes or customizes itself frequently and automatically. Server-side dynamic pages are generated "on the fly" by computer code that produces the HTML. There are a wide range of software systems, such as CGI, Java Servlets and Java Server Pages (JSP), Active Server Pages and ColdFusion (CFML) that are available to generate dynamic web systems and dynamic sites. Various web application frameworks and web template systems are available for general-use programming languages like Perl, PHP, Python and Ruby to make it faster and easier to create complex dynamic websites.

For example, when the front page of a news site is requested, the code running on the webserver might combine stored HTML fragments with news stories retrieved from a database or another website via RSS to produce a page that includes the latest information. Dynamic sites can be interactive by using HTML forms, storing and reading back browser cookies, or by creating a series of pages that reflect the previous history of clicks. Dynamic HTML uses JavaScript code to instruct the web browser how to interactively modify the page contents.

4 WEB PAGES:

Hypertext documents on the Internet are known as Web Pages. Web Pages are created by using a special language called HyperText Markup Language. A web page (or webpage) is a specific collection of information provided by a website and displayed to a user in a web browser. The core element of a web page is one or more text files written in the Hypertext Markup Language. Many web pages also make use of JavaScript code for dynamic behavior and Cascading Style Sheets (CSS) code for presentation semantics.Images, videos, and other multimedia files are also often embedded in web pages.A website typically consists of many web pages linked together in a coherent fashion. Each web page is identified by a

distinct Uniform Resource Locator (URL). When the user inputs a URL into their browser, that page's elements are downloaded from web servers. The browser then transforms all of the elements into an interactive visual representation on the user's device. From the perspective of server-side website deployment, there are two types of web pages: static and dynamic. Static pages are retrieved from the web server's file system without any modification, while dynamic pages must be created by the web server on the fly, typically drawing from a database to fill out a web template, before being sent to the user's browser. The WWW uses the client-server model and an Internet Protocol called HyperText Transport Protocol (HTTP in short) for interaction between the computers on the Internet. Any computer on the Internet that uses the HTTP protocol is called a Web Server and any computer that can access that server is called a Web Client.

4.BROWSERS

To be used as a web client, a computer needs to be loaded with a special software tool that is known as WWW browser (or browser in short). When a user requests a web page from a particular website, the web browser retrieves the necessary content from a web server and then displays the page on the user's device. This process begins when the user inputs a Uniform Resource Locator (URL), such as https://en.wikipedia.org/, into the browser. Virtually all URLs on the Web start with either http: or https: which means the browser will retrieve them with the Hypertext Transfer Protocol (HTTP). In the case of https:, the communication between the browser and the web server is encrypted for the purposes of security and privacy. Once a web page has been retrieved, the browser's rendering engine displays it on the user's device. This includes image and video formats supported by the browser. The most used browser is Google Chrome, with a 64% global market share on all devices, followed by Safari with 18%. Other notable browsers include Firefox and Microsoft Edge.

Features

The most popular browsers have a number of features in common. They allow users to set bookmarks and browse in a private mode. They also can be customized with extensions, and some of them provide a sync service.

Most browsers have these user interface features:

- Allow the user to open multiple pages at the same time, either in different browser windows or in different tabs of the same window.

- Back and forward buttons to go back to the previous page visited or forward to the next one.
- A refresh or reload button to reload the current page.
- A stop button to cancel loading the page
- A home button to return to the user's home page.
- An address bar to input the URL of a page and display it.
- A search bar to input terms into a search engine.

5.MCQs

A DNS client is called _____

a) DNS updater

b) DNS resolver

c) DNS handler

d) none of the mentioned

DNS database contains _____

a) name server records

b) hostname-to-address records

c) hostname aliases

d) all of the mentioned

Which of the following is used to read a HTML page and render it?

a) Web browser

b) Web server

c) Web matrix

d) Web network

Which of the following is the first web browser?

a) Nexus

b) Netscape Navigator

c) Internet Explorer

d) Mosaic

A piece of icon or image on a web page associated with another webpage is called _____

a) url

b) hyperlink

c) plugin

d) extension

References:

- P. K. Sinha & Priti Sinha , “Computer Fundamentals”, BPB Publications, Chapter 17.
- Behrouz A. Forouzan,” Data Communication and Networking” (2003)., Edition, 4th. ISBN, 978-0073376226.
- https://en.wikipedia.org/wiki/Web_Browser available under the Creative Commons Attribution-ShareAlike License

- All images used in the document are royalty free downloaded from https://stock.adobe.com/in/ or self made.