2022

Introduction to Computer Networks

Dr. Babasaheb Ambedkar Open University

Expert Committee

Prof. (Dr.) Nilesh K. Modi Professor and Director, School of Computer Science, Dr. Babasaheb Ambedkar Open University, Ahmedabad	(Chairman)
Prof. (Dr.) Ajay Parikh Professor and Head, Department of Computer Science Gujarat Vidyapith, Ahmedabad	(Member)
Prof. (Dr.) Satyen Parikh Dean, School of Computer Science and Application Ganpat University, Kherva, Mahesana	(Member)
M. T. Savaliya Associate Professor and Head Computer Engineering Department Vishwakarma Engineering College, Ahmedabad	(Member)
Mr. Nilesh Bokhani Assistant Professor, School of Computer Science, Dr. Babasaheb Ambedkar Open University, Ahmedabad	(Member)
Dr. Himanshu Patel Assistant Professor, School of Computer Science, Dr. Babasaheb Ambedkar Open University, Ahmedabad	(Member Secretary)

Course Writer

Mr. Nilesh N. Bokhani	Assistant Professor, School of Computer Science, Dr. Babasaheb Ambedkar Open University, Ahmedabad
Dr. Mahesh D. Mulani	Assistant Professor, Department of Computer Science, KSKV Kachchh University
Mr. Madhavendra V. Kacha	Assistant Professor, Department of Computer Science, KSKV Kachchh University

Content Editor

Mr. Nilesh N. Bokhani	Assistant Professor, School of Computer Science, Dr. Babasaheb Ambedkar Open University, Ahmedabad

Content Reviewer

Prof. (Dr.) Nilesh K. Modi	Professor and Director, School of Computer Science, Dr. Babasaheb Ambedkar Open University, Ahmedabad

ISBN -

Printed and published by: Dr. Babasaheb Ambedkar Open University, Ahmedabad While all efforts have been made by editors to check accuracy of the content, the representation of facts, principles, descriptions and methods are that of the respective module writers. Views expressed in the publication are that of the authors, and do not necessarily reflect the views of Dr. Babasaheb Ambedkar Open University. All products and services mentioned are owned by their respective copyrights holders, and mere presentation in the publication does not mean endorsement by Dr. Babasaheb Ambedkar Open University. Every effort has been made to acknowledge and attribute all sources of information used in preparation of this learning material. Readers are requested to kindly notify missing attribution, if any.

Dr. Babasaheb Ambedkar Open University

BCAR-301

Introduction to Computer Network

Block-1: Introduction of Computer Network

Block-2: Networking Standards

Block-3: Transmission Media and TCP/IP

Block-4: Connectivity Devices, Network Topologies and Architecture

BLOCK – 1

Introduction of Computer Network

Unit 1: Introduction to Networking

1

Unit Structure

1.1 LEARNING OBJECTIVES

After studying this unit student should be able to:

- Clear understanding about invention of Computer Network
- Basic concept of Data and Information
- Importance of Computer Network through in current scenario
- Difference between components of Computer Network
- Understand the use of Computer Network according to Area
- Understand basic concept of various Computing Models

1.2 INTRODUCTION TO NETWORKING

ARPANET (Advanced Research Project Agency Network) is considered as one of the first computer networks. ARPANET has started implementation in 1969 in which first two nodes were connected to use packet switching Networking. Before ARPANET, if we see our old model where only a single computer was available to satisfy all the necessary computational requirements. But the situation is now replaced by large number of separate but interconnected computers are used as computer networks for the same purpose. Computer Networking supports the way we communicate. If we take the example of traditional land-line phone for communication then we used to send our voice data, but now the communication pattern has entirely changed. In networking, we are sending and receiving data between nodes over a shared medium in information system. Here, we can say computer is a node because computer can send data as well as receive the data. Node can be defined as a computer, printer or any other device capable of sending/receiving data generated by other nodes in the network. Through Computer Networking, Devices can be connected with each other on a Local Area Network (LAN) or to a larger network which can be Internet or a private Wide Area Network. It will be helpful to share resources worldwide.

If we think about any mobile messaging application, we have been provided different features like send text, images, animations, videos, audios and also voice calls and video calls which are real time communications. This is all possible because of

Computer networks. Computer network also supports the way we work as we can we can work from home by accessing the files and software which are available at remote site.

Data Communication

Let's understand the basic terms Data and Information before going on Data Communication as it will help us to understand the topic very well. **Data** is raw material or raw facts that are collected while **Information** refers to processed data based on which one can take the decision. Let's take one example to understand the concept of Data and Information. Data of all the students is available in the result but whether you have cracked the exam or not is based on the marks you got in the exam which is considered as information.

Data communication is the process where one device is sending the information to another device in computer network. To complete the process of Data communication, a system is available made up of software and hardware where sending and receiving of information through devices considered as hardware part and some protocols should be followed them for sending the information like what information should be sent, how and when. Delivery, Accuracy, Timeliness and Jitter (variation in the packet arrival time) are the characteristics of Data Communication.

1.3 USE OF COMPUTER NETWORK

Looking at current scenario of organization, Computer networks are very important or we can say invaluable for organizations as well as individuals. Let's discuss some of the most important uses of Computer Network.

Business Applications

Here we discuss about the issue of **Resource sharing** so the organization's main goal is to make data available to every employees of the organization without regard to the physical location of resource or the user. A Second goal is related with people rather than information. So each employee is using **E-Mail** (Electronic mail) for professional

communication. **Desktop sharing** is a common name for technologies and products that allow remote access and remote collaboration through graphical terminal emulator on a person's computer desktop. The third goal for most of organizations is to do business electronically with customers. This is satisfied by new model called E-Commerce. Actually E-Commerce is nothing but buying and selling things on internet. Now-a-days, most of the companies are interested in E-Commerce for the growth of their sales globally.

Home Applications:

Today all the home users are having internet connectivity to buy products and services on E-Commerce. Some of the E-Commerce forms are B2C(Business-to-Consumer), B2B(Business-t Most newspapers are available online. Client-server model provides information but Peer-to-Peer communications is getting popular. BitTorrent is an example of Peer-to-Peer systems, where it doesn't provide central database of content. Instead of this, each user maintains his own database locally and provides a list of other nearby people who are member of the system. There are many social applications are available in the market like Facebook for person to person communications and accessing information.

Mobile Users:

Mobile users use laptops and handheld devices etc connected through internet to work from any place. Wireless hotspot 802.11 standard is used as wireless network for mobile computers. Fixed wireless and Mobile wireless networks are also available in market. Through wireless applications available in mobile phone, we can have various services like text messaging, GPS (Global positioning system), M-Commerce etc. Wearable computers are also popular in the market.

Social Issues

Through social network, anyone can share his/her reviews but the problem arises when the topic is related to religion, political or sex. As the content is publicly available, there will be chances of discussions as well as arguments and legal actions in worst situation.

There are other issues concerned with it like advertisements based on your email content and activities on internet and anonymous messages to increase privacy through computer networks. Here we have to understand other terms like Botnets, Phishing and CAPTCHAs etc which are related with Social issues through computer network. Botnets are used to steal data through unauthorized access. After sending spam mails, hacker can access device for malicious activities. Ransomware is an example of phishing where attacker will have sensitive information through fraudulent message.

1.4 BENEFITS OF COMPUTER NETWORKING

Computer network facilitates distributed processing of information which results in better performance with high speed of processing. It also provides central storage of Data, Faster problem solving, reliability, flexibility and security through authorization.

Following are some of the benefits of Computer Networking:

File Sharing: It means the practice of distributing or providing access to digital media, such as computer programs, multimedia, documents or electronic books.

Hardware Sharing: In a networked environment, each computer on a network may access and use hardware resources on the network, such as printing a document on a shared network printer.

Application Sharing: Application sharing is an element of remote access, falling under the collaborative software umbrella that enables two or more users to access a shared application or document from their respective computers simultaneously in real time.

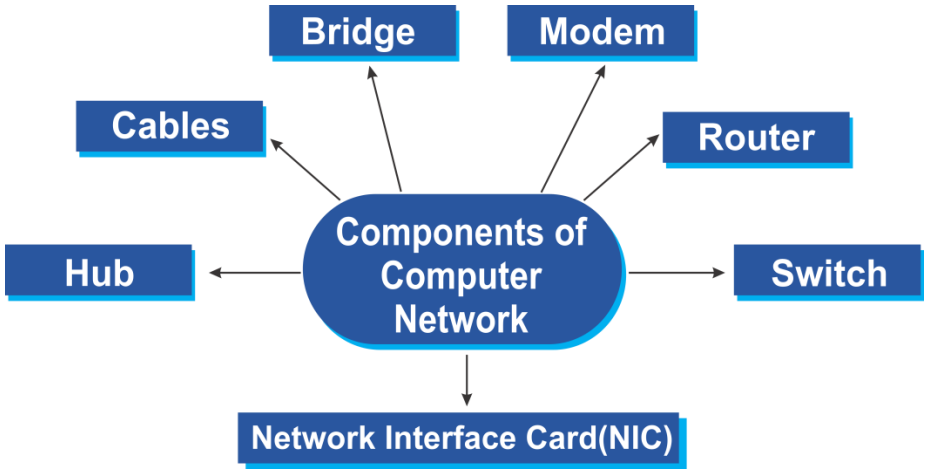
User Communication: ability for Users/computers to communicate with one another and, maybe more importantly, to facilitate communication between individuals and groups, has been an important factor in the growth of computing over the past several decades.

Network Gaming: It refers to games played on a local network of computers, either via direct cable connection to a switch/hub, or a wireless router.

1.5 COMPONENTS OF NETWORKING

Computer network consists of components such as data, software, hardware, Operating system etc.

The hardware components are mentioned below.



Hub:

Hub works in half duplex mode. It sends Data in form of bits. Broadcasting is the main purpose of Hub so it is used as Broadcast device. In our further study, we will understand the concept of OSI (Open system interconnection) model which will have physical layer for Hub. Hub is used to connect devices to the same network. MAC address stands for Media Access Control address which is a unique value associated with a network adapter. It is also knows as hardware addresses or physical addresses which is used to identify an adapter on a LAN uniquely. Hub is not going to store any MAC Address of a node in the network.

Passive Hub, Active Hub, and Intelligent Hub are the types of Hub. In the simplest words, Hub is used to provide pathway for the electrical signals so signals can travel along. This kind of device is known as Passive Hub. But now-a-days, Active Hub is very popular because it provides a path for the data signals as well as regenerates the signal before it forwards it to connected devices. Intelligent Hub is having more features than

Active Hub as it performs functionalities like network management, bridging, routing, and switching. So the performance of Network can be improved through problem diagnosis and rectifying feature for network.

Switch:

Switch works in full duplex mode. It sends Data in form of frames. Switch is used as Multicast device. Actually network switch is a telecommunication device which receives a message from any device connected to it and then transmits the message only to the device for which the message was meant. This is why Switch is considered as more intelligent than Hub. Switches are totally ON or OFF as they are paired Gadgets because Switch is used to intrude on the progression of electrons in circuit. As we discussed before for OSI Model, Switch works in Data link/ Network layer. Switch is used to connect devices to the network. An IP (Internet protocol) address is a numerical label of computer which is connected to computer network for communication through Internet protocol. Switch stores MAC address and IP address of nodes in the network. Many organizations are using switch to increase data transfer capacity without burdening individual host PCs. Workstations and switches are integrated easily and bandwidth can be increased. Though switch data will be received by destination only so there will be fewer frame collision. Let's discuss some the problems which occur through switch in organization. As the organization grow, network should be managed accordingly so switches are more costly in contrast with network spans. Sometimes the problem occurs because of broadcast traffic in switch.

Router:

To connect LAN and WAN, Router is used in computer network. Router works in full duplex mode. It sends Data in forms of Packets. Router is used as Routing device as it provides traffic direction on the internet. Actually router looks at packet headers to determine which port it needs to forward a packet through, and also will translate packets between different protocols if needed. A router can also define subnets and will filter traffic as needed. Routers usually include Dynamic Host Configuration Protocol (DHCP) for port forwarding capabilities. In OSI Model, Router works in Network

layer. Router is used to connect two networks. Router also does the same as it stores MAC address and IP address of nodes in the network. The most important feature of router is dynamic directing strategy where the best possible path can be decided across the internetwork. Here configuration is possible, so the manual policies can be available based on routing decision as per the requirement of network manager. The bandwidth for user data will be less due to dynamic router communication and router has less speed compared to repeaters and bridge.

Bridge:

Actually bridging is different from routing as bridge device creates a single and aggregate network with the help of multiple communication networks which are having same protocol. In short, A bridge is the network device which can provide connectivity between two LANs (Local area network) or two segments of the same Local area network. The functionality of Bridge is similar like Hub related to broadcast the data to each node. To prevent the data traffic, The MAC (Media Access Control) address can be helpful. Extension of Network and Increased Bandwidth are the main advantages of Bridge. There are some disadvantages of Bridge like cost compared to Hub is more and Potential network performance is poor because of the process to view MAC address of frame on the network. Apart from this, Broadcast Traffic has not individual filtering option.

Modem:

Modem stands for Modulator-Demodulator. The first Modem was Dialup as it was necessary to dial a telephone number to connect to an ISP but now-a-days DSL (Digital Subscriber Line) or Cable Modems are used. Modem is a kind of Hardware Device which is used for to send and receive information between computers. The information will be converted from Analog to Digital and Digital to Analog as per the medium like computer and telephone. In simple words, Modem converts or "modulates" an analog signal from a telephone or cable wire to digital data (1s and 0s) that a computer can recognize. The Modem can be categorized according to its features like Direction capacity, Connection to the line and Transmission Mode. Modem is used to connect

LAN with Internet but the speed depends on cost. If we compare it with Hub, Modem provides slow speed so it's nothing but an interface between LAN and Internet. There is no traffic maintenance related feature so the user can spend more money to achieve speed but it shouldn't be expectable.

Cables:

Various kinds of Wires are used for Computer network. Each computer or Central Device is connected through wires. So cable is the medium between network devices for data communication. Actually several types of cables are available but network will utilize only one type of cable. Wireless network or mixture of wire and wireless connection are possible.

In wired computer network, different types of cables are being used to carry the signal from one point to another. The form of signal depends upon the type of wire is used.

- Coaxial cable – Coaxial is type of electrical cable. It has mainly three layers. The inner most layers is copper wire. Copper wire is surrounded by insulator as the middle layer. The outer layer is made up of conducting shield. It is primarily used in cable TV companies to connect customer TV set with single receiver.

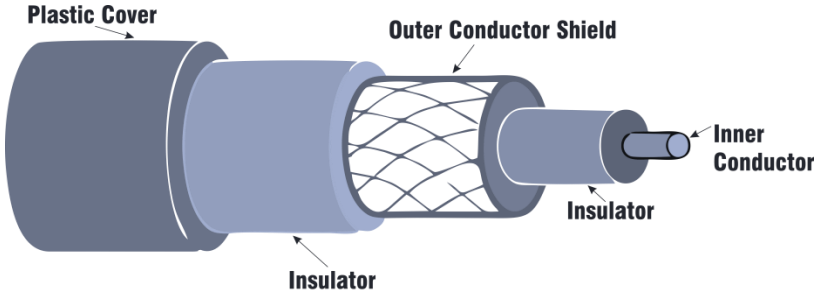


Figure - Coaxial Cable

- Twisted pair- A twisted-pair cable is a cable made by twisting two separate insulated wires. There are such four pairs in cable which is used in network set up. There are two types of twisted pair cables. A STP (Shielded Twisted Pair) cable has a fine wire mesh surrounding

the wires to protect the transmission and a UTP (Unshielded Twisted Pair) cable does not.

- Fibre optics - A fiber optic cable is made up of glass fibers surrounded by plastic coating. Data are transmitted in form of pulses of light. The fibers are protected from heat, cold or any other external interference by coating. The speed of data transmission in fiber optics cables is very high compared to coaxial cable and twisted pair cable. On the side, the initial set up cost and maintenance is also high.

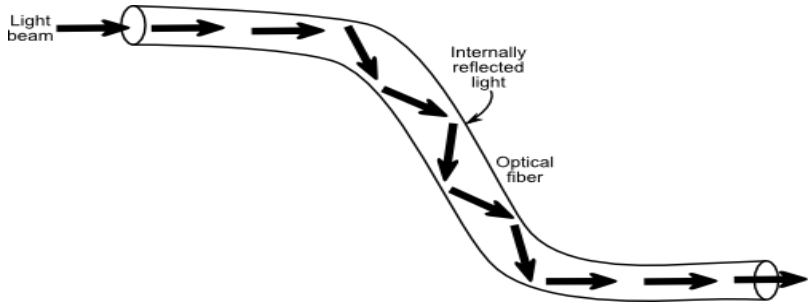


Fig – Fiber optics cable

Image source - http://www.robotoid.com/appnotes/images/fiber-optic-tir.png

Network Interface Card (NIC) – As name implies, it is a device which makes interface between computer and rest of the network. A network cable is inserted into the NIC. NIC prepares the frame as per the format, sends and receives the data. It controls the flow between sender and receiver such that no data loss occurs.

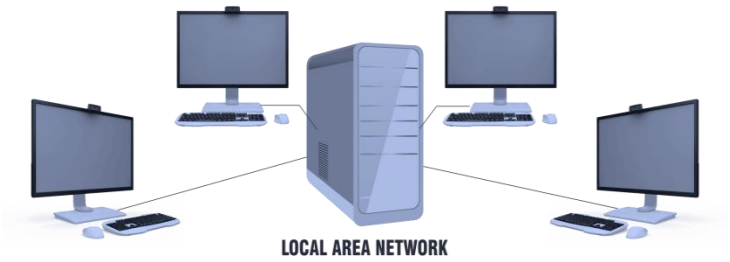
1.6 TYPES OF COMPUTER NETWORK

There are different criteria to categorize computer network like geographical area, type of delivery, mode of communication. Here, we have categorized the network with Geographical Area.

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

Local Area Network (LAN)

A LAN is a network which is used for small physical area such as College, Hospital and School. It allows single pair of devices to communicate with each other. Usually LANs are having private ownership. Design of LAN is very easy so the problem can be resolved quickly. Sending and receiving of information as well as resource sharing becomes easy through it. LAN is having highest transmission speed of 10,100 and 1000 MBPS compared to MAN and WAN. As the wireless technology is expanded, there are many devices available which can be connected to LAN. Thus, we can say nearly everything imaginable can be Connected. There will be different types of Topologies available like star, tree, bus and ring which can be used with it.



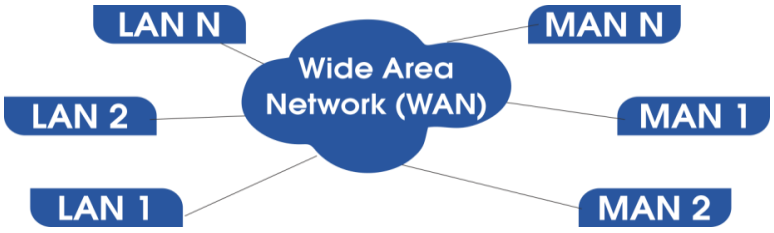
Metropolitan Area Network (MAN)

A WAN is a network which spans a small town or city. It allows multiple computers to communicate simultaneously. We can say MAN is between LAN and WAN technology but it uses the same technology which is available in LAN so there is moderate propagation delay in MAN and the speed of transmission is average up to 100 MBPS. We can work on competitive price with MAN network. MAN has less fault tolerance.

Wide Area Network (WAN)

A WAN is a network which covers Country or Continent. So it allows a huge group of computers to be connected with each other for communication at the same time. In

simple words, LAN is not possible to connect computers which are located at widely separated locations so WAN is used when the network spans over a large distance. Here the communication is possible through the medium like leased telephone lines and satellite links so it has low data transfer rates between 10 to 20 MBPS. WAN technology is very expensive in the market. The main advantage of LAN is large amount of data transfer but WAN has less fault tolerance.



1.7 DIFFERENT COMPUTING MODELS OF NETWORK

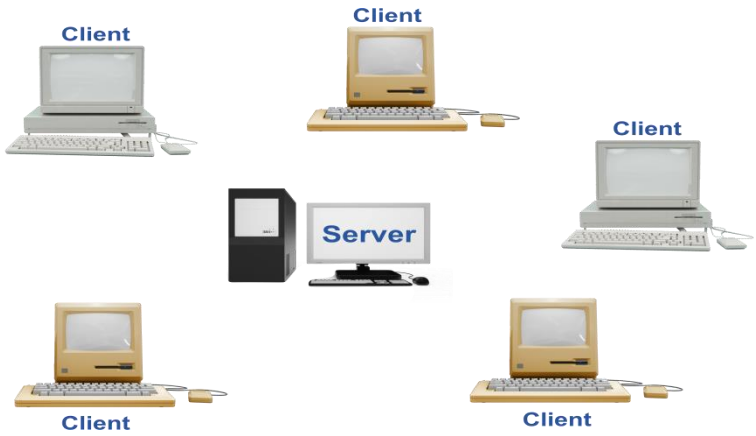
The entire process of communication between two entities seems straightforward. It looks like a single step process. But it takes several steps one after another. Also these steps are carried out in sequence.

For example, the task of sending an email from source to the destination can be divided into several sub tasks. Each sub tasks would be performed by a specific program of software. Again, each sub task provides service to another sub task and also takes service from another sub task. If all sub tasks are arranged in some hierarchy, then lowest sub tasks transforms the binary data to digital signal. The process is reversed at the receiving side. It converts the digital signal to the binary to takes the sub tasks from bottom to the top.

Communication is done between two or more computers though different computing model where information will be sent from source to destination like E-mail service. There are different computing models of Network is available like Client-Server Network, Peer-to-Peer Network, Centralized Computer Network and Distributed Computer Network which will be discussed in detail.

Client-Server Network

Client-Server Network is a model where a central controller called a server exists. It's a computer which provides services to other computers and it also controls the network resources and other computers are requesting for the services. These resources can be files, directories, applications and shared devices which are centrally managed and also hosted so it can be accessed by client. This way, there are some computers which act as servers and other act as clients. The main advantage of Client-Server Network is security with better performance. As the data will have centrally back up facility, it's very reliable. Client-Server Network should have professional administration with expensive dedicated software. So it's more hardware and software intensive. Local Area Networks are based on this network.



Peer-to-Peer Network

As its not possible to set up 1000-node CDN (Content distribution network) by every organization, so we have the solution which is called Peer-to-Peer (P2P) network which is simple to use and it can distribute large amount of content. In this network, all the computers are having equal status. As there is not centralized management strategy, it's possible to provide data to any computer. In office, Peer-to-Peer (P2P) network can be used as there are small numbers of computers at the same location. In 1999, Napster application was used by 50 million users for sharing copyright content without copyright owners and today BitTorrent is very popular among users but it should be considered with legal use. In simple words, many home computers are going to pool their resource in P2P network to form a Content distribution system so basically it's a

network for file sharing. Each computer is called Peer as sometimes it can be requesting for resource as client as sometimes the same computer will be responding as Server to another computer. Each user will have broadband connectivity at 1 MBPS and each user can upload as well as download at the same time in P2P network. The basic requirement of P2P network is just a Network Interface Card (NIC) and Operating system which supports Networking.

Centralized Computer Network

In Centralized computer Network, one or more client computers are connected directly with server and request and response is done between client and server. In simple words, though centrally available main location resources can be managed by administrators. There will be one secure and dedicated server room in central location to manage resources easily. In this Network, workload should be managed and if the central node is having problem or failure it causes entire system to fail. Components of Centralized Computer Network are Node like computer or mobile, Server and Communication link like Cables, Wi-Fi etc. One limitation should be discussed over here of this network; the performance will not be increased at reaching one point even after increasing hardware and software capabilities of the server node. Network can't scale up vertically after a certain limit and less chances for the backup in this Network. In the situation of high traffic like shopping sale, it may suffer from a Denial-of-Service attack.

Distributed Computer Network

In Distributed Computer Network, Many computers are managing programming related code and data. Distributed network is a type of computer network which are connected through different networks. So it can be managed jointly or separately and distributes processing also. Here, IT infrastructure of organization is divided in number of networks and processors. Distributed computer is responsible for data routing, network bandwidth and access control with other basic responsibilities related to networking. Each computer will have its own private memory or distributed memory and through message information will be sent from one computer to another. In Distributed Computer Network, network topology, network latency and number of computer is not available in advance and system may change while execution of distrusted program.

Characteristics of Distributed computer network are as below:

- Heterogeneous
- Shared resources
- The network management through multiple points
- Easy to scale
- Not so easy administration

1.8 LET US SUM UP

In networking, we are sending and receiving data between nodes over a shared medium in information system so we can consider the computer network as the interconnection between devices. Data communication is the process where one device is sending the information to another device in computer network. We can use computer network for business applications, Home applications, and Mobile users. There are several networking devices such as hub, switch, cable, router, bridge, model etc.

1.9 CHECK YOUR PROGRESS

Attempt following True/False Statement:

1) Data is raw material and Information is processed data. T

2) A Computer Network permits sharing of information but not resources. F

3) Router is used to connect two different LAN segments. F

4) Hub works in Half-duplex mode. T

5) UTP (Unshielded twisted pair) is the cheapest cabling choice. T

6) A Server can run on a workstation computer. T

7) In a peer-to-peer network, any client computer can also be a server. T

8) There is moderate propagation delay in WAN. F

9) In Distributed Computer Network, Many computers are managing programming related code and data. T

10) BitTorrent is the example of Peer-to-Peer Network. T

Answer the following MCQs:

1) ARPANET stands for

a) American Research Project Agency Network

b) Advanced Research Project Area Network

c) American Research Programs and Network

d) Advanced Research Project Agency Network

2) The abbreviation of E-Mail is

a) Easy message b) Early message

c) Electronic Mail d) All of these

3) Which of the following is/are benefits of Networking?

a) File sharing b) Application sharing

c) Network Gaming d) All of these

4) Which transmission media has the highest transmission speed in a network?

a) Coaxial cable b) Twisted pair wire

c) Optical fiber d) Electrical cable

5) Select the cable that transports signals in the form of light:

a) Twisted-pair Cable b) Fiber optic Cable

c) Coaxial Cable d) Shielded twisted pair cable

6) Which of the following performs modulation and demodulation?

a) Fiber optics b) Switch

c) Modulator d) Model

6) A simple WIFI modem forms a __ wireless network.

a) LAN b) MAN

c) WAN d) None

7) Identify the characteristics of Distributed Computer Network.

a) Heterogeneous b) Shared Resources

c) Easy to scale d) All of these

8) MAN is used in

a) College, School and Hospital b) Small towns, City

c) Country/Continent d) None of these

9) Ownership of MAN can be

a) Public b) Private

c) Public or Private d) can’t say

10) Fiber optic, radio wave and satellite are available as Transmission media type in

a) LAN b) MAN

c) WAN d) None of these

1.10 FURTHER READING

- Recommended Text

1) Forouzan (2013). Data Communication and Networking, McGraw Hill
2) Andrew S. Tanenbaum and David J. Wetherall (2011). Computer Networks

1.11 ASSIGNMENT

1) Discuss various components of Computer Networking.
2) Differentiate LAN, MAN and WAN.
3) Define Peer-to-Peer Network and Distributed Computer Network

Unit 2: Intranets and Internets Network Services

2

Unit Structure

2.1 LEARNING OBJECTIVES

After studying this unit student should be able to:

- Understand the concept of Intranets and Internets
- Know about FTP and File Services
- Understand printing and applications services
- Explain the concept of Telnet services

2.2 INTRANETS AND INTERNETS NETWORK SERVICES

A client is requesting to server for services and Server gives response to the Client based on its request. This is called Client-Server Communication where the process is done for exchange of information. There are some predefined rules which should be followed by client and server regarding format, size etc regarding information. The service of server might include data or resource sharing. In simple words we can say that it's possible that many clients are connected with single server and many servers are providing their services to single client. Let's discuss about some of the servers like Database server, Mail server, Web server and Game server.

Database server

As per the client-server model, Database server provides services to other computers or clients through its application. Database server functionality is provided by DBMS which is known as Database Management System. Here database access is totally dependent on the client-server model. Database server is crucial component which provides business-critical information requested by the client systems. In simple words, to store and manage databases stored on the server we use database server. These databases are accessible after authentication only. Regular back up is necessary here as the data is available in central location. Hardware and Software are used to run database so there will be back-end application which is used to represent a set of memory structure and there are some processing running in background to access database files. If we

think about Hardware side then there will be server system to store and retrieve data from database.

Mail server

Mail server is also known as email server. It is used to send and receive email over a network, usually over the internet. A mail server will deliver email to another mail server which is received from client computers. Dedicated hardware is used by Internet service providers (ISP) for sending mails. ISPs are responsible for mail server address and other information etc. As the post office works on mails like storing and sorting before doing further process for its destination regarding delivery, the same concept is applicable on Mail server. On the request of someone's email by user, the contact will be established with mail server which will send its data to client's computer. A computer can perform as mail server with specialized software which will manage data like creating email accounts for any domains which are hosted on the server. There are some protocols available for mail servers to send and receive email like Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP) and Post Office Protocol version 3 (POP3) which will be covered in our further study. Some of known mail servers are Microsoft exchange server, Exim, Ipswitch IMail server and IceWarp Mail server etc. Massaging system can be developed by integration of mail server with other programs. Microsoft outlook can be considered as program which is used to forward the message to other mail server when the email is sent. Then it will be delivered from one mail server to another or it will be in the holding area of the same area as it can be forwarded after some point of time. To find another mail server to send the email, a mail server is taking the help of domain name as the address. Actually we can categorize mail servers into incoming mail server and outgoing mail server. In incoming mail server, the mail will be stored and then it will be sent to inbox of user like POP3 and IMAP. But outgoing mail server doesn't work like incoming mail server. In outgoing mail server, user's machine communicates with SMTP to handle the process of email delivery.

Web server

A computer to store web content is known as web server like Apache HTTP server. In most of web server machine, you will find Apache HTTP Server so we can say it is the popular among all the web servers. Apache Software Foundation has developed Apache HTTP server as kept it as open source as user can access and change it's code according to requirement. It's running on almost all the Operating systems like windows, MacOS and Linux. In web server, a program will be managing the incoming network requests of user and giving response with files for creating web pages through HTTP (Hypertext transfer protocol). In simple words, a user will be provided specific website through a web server. To store website, there can be one or more web server but it doesn't affect the web site which is available on your monitor. Hardware and software both can be used to perform the functionality of web server but usually software is used for it. As it's not possible to avail web server for each user, web server is having feature to handle multiple users at a time. A web server must be connected to the internet 24x7 as it won't be able to receive the request from the client without internet and can't process them.

Game server

Now-a-days, gaming profession is going high in the market. Many game developers are providing multiplayer facility to play the game simultaneously by many users at a time. Game server is required at this point to satisfy this requirement of Gamers. These types of servers are hosted locally as well as remotely. If servers are hosted locally then access is limited to intranet but if servers should be accessed worldwide then it's mandatory to host them remotely. There are various types of Game server available like dedicated server, listen server, peer-to-peer server and listen-peer server. In dedicated server, there's no direct input and output but each player should used client program to connect with server. In Listen-server, game player is having the same process as the server. In Peer-to-Peer, server is not available but each client received data from other client and processing the result. Listen-peer is used for large number of clients where it can be considered as the alternative of dedicated server.

2.3 FILE SERVICES

File server

In computer network, there are many client computers connected to a computer which serves as file server for storing and fetching various types of files over the network. A file server can have large disk drive with specialized software and also microcomputer in some of the LANs. Only authorized clients or devices can access the data stored in file server as the data is managed centrally in file server. So we can consider central storage, remote access and configuration as the advantages of file server. There are also disadvantages of file server like inherent maintenance for managing a server, limited scalability depending on the server specification and bottlenecking when overcome with requests. In the age of cloud computing, we have popular cloud file servers available like MS Azure, DropBox and MS OneDrive etc. Dedicated and Non-dedicated are two types of file server. Dedicated file server can be used for file server, along with their workstation which is used for reading and writing files as well as database. Non-dedicated servers are made to perform as file server as well as database server.

Some of the advantages of file server are:

- Reduce maintenance cost of software
- Without affecting whole system, file server can be implemented
- Data migration is possible from old database to new one
- Recompilation is not necessary when file is modified used by application program.

Some of the Disadvantages of file server are:

- File server takes some time for response on external call to server.
- Program made for file server tend to be large

2.4 FILE TRANSFER SERVICES

In computer network, when a file is moved from one computer to another is called File transfer. This process can be done locally as well as remotely. File upload and download both can be considered as file transfer. Other than network and Internet, we are performing file transfer while we copy our file to a new folder, USB Pen Drive and CD etc. There are popular protocols available for file transfer like FTP (File Transfer Protocol) and HTTP (Hypertext Transfer Protocol). One can choose HTTP protocol to move file from remote computer, but File Transfer Protocol (FTP) is the best protocol for copying files from one computer to another over the internet. We can categorize file transfer in pull-based and push-based. In Pull-based technique, the receiver initiates the file transfer request while the sender initiates the file transfer request in Push-based technique.

The network supports users to locate the specific files on the internet. FTP resolves several issues related with transferring files between two different. Such as,

- Two computers may have different encoding scheme to represent the data.
- Two computers may have different directory structures.
- Two computers may follow different file name conventions.

The framework of FTP composed of two major modules, the client and the server.

Client Module

The client module has three components.

- The user interface
- The client control process
- The client data transfer process

Server Module

The server module has three components.

- The server control process

- The server data transfer process

The client control process is connected with server control process. Similarly, the client data transfer process is connected with server data transfer process.

2.5 PRINTING SERVICES

Print server

Print server is also known as printer server is device or program which is used to connect printers with computers over the network. Print server is used to manage all the functionalities related to printing like accepting request from specific computer and provide response to it. Actually the job of print server is to send the request of print to the right computer. Provide client access, Administration of printing jobs and feedbacks to user with notification are the main functions of print server. Sometimes user can also give command of printing through Direct IP which is considered as alternative of print server. There will be single dedicated computer serving as print server in large organization and a small network device performs the same function in small organization. The main advantage in small organization is related to memory where a small network device frees up valuable disk space as limited numbers of computers are available.

2.6 APPLICATION SERVICES

Application server

Application server is used to run applications for client computers on network. Application server is intermediate between database information and end user or client program. It helps to deliver various applications to other devices. Web based applications as well as enterprise based applications are being managed through application server. So these servers are designed to install, operate and host applications. Basically, application server is used in web application having 3-tier architecture where it helps clients for processing the request by connecting to the

database for information retrieval to the web server. Oracle WebLogic Server is one of the popular application servers.

Some of the advantages of Application server are:

- Security: Firewall provides security in application server.
- Performance: Due to limited network traffic, performance can be increased.
- Data integrity: As single server is responsible for managing updates and upgrades for business logic with central database.
- Configuration: No need to configure each system as all the systems are managed centrally.

2.7 TELNET SERVICES

A Telnet is short form of Teletype Network. There are some client server programs like FTP (File transfer protocol) and SMTP (Simple mail transfer protocol), these are used by user to run application programs remote site and result should be displayed on the local site. Here specific program for each demand is not possible so as a solution we have Telnet. Through Telnet, user can log on to the remote computer and can access any application program. In simple words, Telnet will be helpful to display local terminal at the remote side and it can be considered as general purpose client/server application program. Virtual terminal service can be provided by TELNET through single TCP/IP (Transmission Control Protocol/Internet Protocol) Connection.

Some of the advantages of Telnet:

- Information send and receive
- Admin work related to network
- User authentication

Some of the disadvantages of Telnet:

- No encryption for authentication like user name and password
- It supports only CUI(Character user interface), no GUI tools will work in Telnet
- Inefficient protocol

2.8 CHECK YOUR PROGRESS

- Fill in the blanks:
  - _____is a protocol that allows to send / upload email message from local computer to an email server.
  - HTTP stands for _____.
  - POP3 is for _____ service.
  - TELNET service is used for _____ login.
- Match the following.

A	B
Email server	Remote login
Web server	POP3
TELNET server	Storing files on remote system
FTP	HTTP

- Multiple Choice Questions:

1. In File Transfer Protocol (FTP), while control connection is open, data connection can be opened and closed

   A. One time
   B. Several Times
   C. Not even Once
   D. None of the given

2. File Transfer Protocol (FTP), uses same operation used by

   A. ICMP
   B. STMP
   C. TCP
   D. FSK

3. File Transfer Protocol (FTP), uses well-known port 21 is used for control connection and port 20 for the

   A. Data Rate
   B. Data Connection
   C. Data Protocol
   D. Data Congestion

4. In File Transfer Protocol (FTP), a user needs an account (user name) and a password on the

   A. Same Server
   B. Remote Server
   C. Central Server
   D. Data Host

5. Well-known port used for FTP's control connection is

   A. Port 6
   B. Port 8
   C. Port 20
   D. Port 21

6. FTP is built on architecture

   A. client-server
   B. P2P
   C. IRC
   D. IM

7. In a computer, ISP stands for

   A. international service provider
   B. internet service provider

C. interlinked services provision
D. intranet's service party

8. Specialized server found on internet is

A. e-mail server
B. file (htp) server
C. web server
D. all of these

9. Protocol in URL "http://www.Microsoft.com" is

A. www
B. http
C. Microsoft
D. .com

10. Software which is used to access internet is called

A. browser
B. packaged
C. spreadsheet
D. HTTP

11. MIME stands for

A. Multipurpose Internet Mail Extensions
B. Multipurpose Internet Mail Email
C. Multipurpose International Mail Entity
D. Multipurpose International Mail End

12. Mail access starts with client when user needs to download e-mail from the

A. Mail Box

B. Mail Server
C. Mail Host
D. Internet

13. When sender and receiver of an e-mail are on same system, we need only two

A. IP
B. Domain
C. Servers
D. User Agents

14. Most famous HTTP response error "Not Found", code is

A. 400
B. 404
C. 405
D. 408

15. TELNET is a general-purpose

A. Client/server application program
B. Database-server application program
C. Client-End application program
D. Server-End application program

2.9 FURTHER READING

1) An Introduction to FRP
   https://www.2brightsparks.com/resources/articles/an-introduction-to-ftp.pdf
2) File Transfer Protocol
   http://www.indigoo.com/dox/itdp/07_FTP-TFTP/FTP.pdf
3) Dedicated Server Gaming Solution
   https://cloud.google.com/files/DedicatedGameServerSolution.pdf

4) Email Client Configuration Guide
https://beaconnet.com/wp-content/uploads/2012/02/email_client_config.pdf

2.10 ASSIGNMENT

- Why TELNET server does compromise the security?
- How file server does provide more availability?
- Describe the database server importance in the application server.
- How the utilization of print resources can be optimized using print server?
- Explain the module of FTP.

2.11 ACTIVITIES

- Configure FTP server for Windows Operating System.
- Install and Configure Database server. (Oracle 10g or MS SQL Server)
- Share a printer in the LAN.

Unit 3: Fundamentals of Communication Theory

3

Unit Structure

3.1 LEARNING OBJECTIVES

After studying this unit you should be able to understand following:

- Fundamentals of Communication Theory
- Analog and Digital signals
- Comparison between Analog and Digital signals
- Periodic and Non-Periodic signals
- Comparison between Periodic and Non-Periodic signals
- Transmission impairments

3.2 FUNDAMENTALS OF COMMUNICATION THEORY

After studying this unit you should be able to understand following:

Friends, in earlier units we have seen the fundamental of networking and its components. We have also seen the types of networking and their communication details. We have also seen physical components being used in communication among the networks.

Now, the question arise is how the communication is done internally. What is theory behind the communication being taken place in network? In simpler terms communication means there is a sender, receiver and medium of communication. In networking communication information can flow in terms of text, audio, video etc... As far as computer networking is concern information is transmitted electronically and such electronic communication is performed via electronic signals.

So the information which sender sends to receiver is in the form of signal rather we can say analog signal and this analog signal should be converted into binary format to make it suitable for computer readable form. We can say this computer readable form as binary signal or digital signal. Again, at reviving side this digital signal need to be converted in analog form to make it human understandable form.

So, in this particular unit we are going to discuss the following topics in brief:

- Signal and types of signal
    - Analog and digital signal
    - Periodic and aperiodic signal
- Transmission impairment
    - Distortion
    - Attenuation
    - Noise
        - Types of Noise

3.3 ANALOG AND DIGITAL SIGNALS

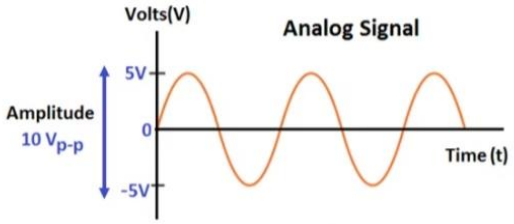
In simple term, we can say that signal is transmission of electronic current that carries data from one device to another on computer network. There are mainly two types of signals:

- Analog Signal
- Digital Signal

Lets us discuss them in detail.

Analog and digital Signal

Analog signal is a form of electrical energy (voltage, current or electromagnetic power) for which there is a linear relationship between electrical quantity and the value that the signal represents. The signal whose amplitude takes any value in a continuous range is called analog signal. Analog Signals are continuous in nature which varies with respect to time. Following figure shows a typical diagram of analog signal.



Analog signal can be periodic or non-periodic. We will discuss these types later in this unit. Voltage, current, frequency, pressure, sound, light, temperature are the physical variables that are measured with respect to their changes with respect to time to obtain information. As shown in the figure, when voltage versus time graph is plotted we see curve with continuous values like sine waves.

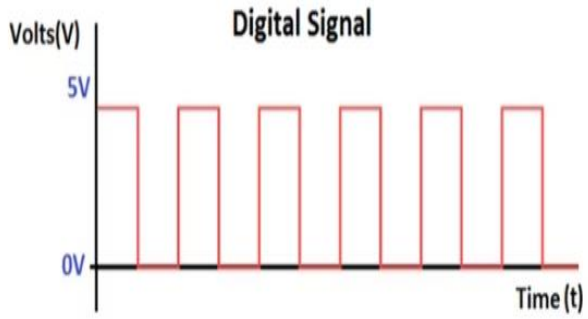
Analog to digital converter converts analog signal to digital signal by a process called sampling and quantization. Sound waves are converted to sequence of samples by the process Sampling.

Following are the examples of analog signals:

- Old transmitters
- Transducers convey data in analog mode
- Audio signals transmitted through wires
- Radio signals
- Analog watches etc.

Now let's discuss digital signal.

The signal, whose amplitude takes only limited values is called digital signal. Digital signal are discrete in nature and they contain only distinct values. Digital signals carry binary data i.e. 0 or 1 in form of bits. It can only contain one value at a period of time. Digital signals are represented as square waves or clock signals. The minimum value is 0 volts whereas maximum value is 5 volts. Digital signals are less subjected to noise compared to analog signal. Transmission of digital data in analog channel is done by process called Modulation. Following figure shows the typical diagram of digital signal.



There are many types of digital modulation. Mainly they are Amplitude Shift Key (ASK), Frequency Shift Key (FSK) and Phase Shift Key (PSK). Generally, amplitude modulation is widely used in digital communication.

Amplitude modulation is a process in which digital data is converted to analog signals using single frequency carrier signal. Similarly frequency shift keying uses a constant amplitude carrier signal and two frequencies to differentiate between 1 and 0.

Following are the examples of digital signals:

- Smart transmitters
- Digital watches
- Digital video signals
- CD's, DVD's, etc

3.4 COMPARISION: ANALOG AND DIGITAL SIGNALS

Analog Signals	Digital Signals
Analog signals may be affected during Data transmission.	Digital signals are not affected during Data transmission.
Analog signals use more power.	Digital signals use less power.
Analog signal is usually in the form of sine wave.	A digital signal is usually in the form of square wave.
Applications of Analog Signals are Audio and Video Transmission.	Applications of Digital Signals are Computing and Digital Electronics.
Analog Signals can be represented through continuous range of values.	Digital Signals can be represented through Discontinuous values.
Easily affected by the noise.	These are stable and less prone to noise.
Components like resistors, Capacitors and Inductors are used in Analog Circuits.	Components like transistors, logic gates are used in Digital Signals.
Human Voice, Temperature and Pressure are examples of Analog Signals	Optical Drives, Motor Start, Trip and Computers are examples of Digital

	Signals
Troubleshooting of analog signals is difficult.	Troubleshooting of digital signals are easy.
In Implementation point of view, Analog Hardware is not flexible.	While Digital Hardware is flexible in implementation.
Analog Signals are stored in the form of Wave signal.	While Digital Signals are stored in the form of binary bit.

3.5 PERIODIC AND NON-PERIODIC SIGNAL

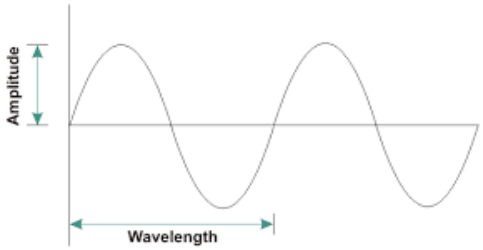
Based on the patterns of the signal they are classified in to two more types, one is periodic signal and another is non-periodic signal. A signal is periodic if it has a definite pattern and repeats itself at a regular interval of time. A signal is non-periodic if it does not have definite pattern and does not have regular interval. There are two types of periodic signal. One is simple periodic signal and other is non-periodic signal. If signal satisfy the following functional equation then we can say that signal is simple periodic.

$f(x + T) = f(x)$, Where T represents the time period.

The smallest value of T justifies the definition of periodic signal, such time period is known as fundamental time period. The reciprocal of the time period is known as frequency of the signal. We can measure frequency in Hz, KHz, MHz, GHz and THz.

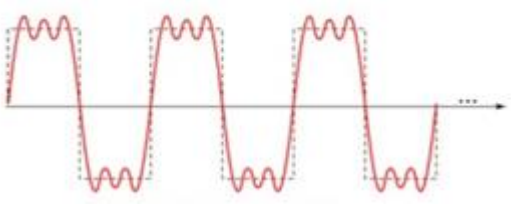
$$f = \frac{1}{T}$$

Simple periodic signals like sine wave and cosine wave cannot be decayed into simpler signals. Following figure shows a simple periodic wave.

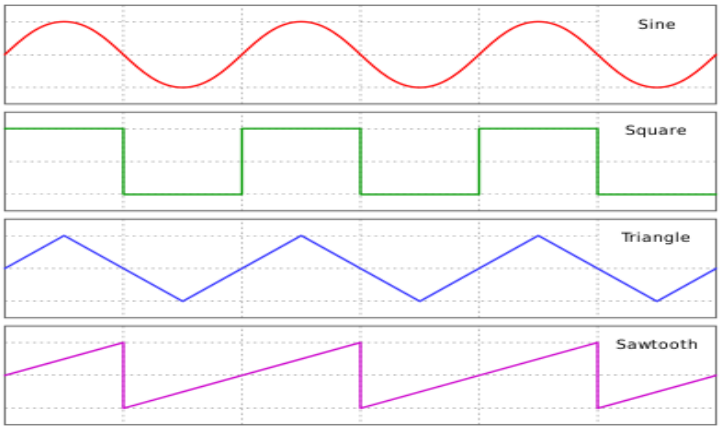


(Image Source :https://www.ecstuff4u.com/2018/07/periodic-and-non-periodic-signals.html)

A composite periodic signal is made of multiple sine waves. The following figure represents typical composite periodic signal.



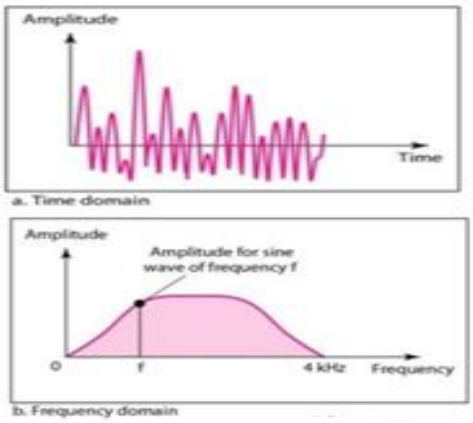
Examples of periodic waveforms are sinusoidal wave, square wave, triangular wave etc. Following figure shows all such waves:



(Image Source:
https://en.wikibooks.org/wiki/Signals_and_Systems/Periodic_Signals)

Now let's discuss non-periodic signals

We can consider signal as non-periodic signal, if it is not repeating its pattern over a period or interval of time. Following figure shows non-periodic signal.



A non-periodic signal is decomposed into time and frequency as shown in the above figure. There are many area where non-periodic signals can be used. For example,

- Signal created by microphone or telephone when one or two words are pronounced.
- Signal propagated by AM radio station or FM radio station.
- Speech waveform and random signals arising from unpredictable disturbance of all kind

3.6 COMPARISONS: PERIODIC AND NON-PERIODIC SIGNAL

Periodic Signals	Non-Periodic Signals
At specific Interval of Time, Signals are repeating itself. These signals are considered as Periodic Signals.	At specific Interval of Time, Signals are not repeating itself. These signals are considered as Aperiodic Signals or Non-Periodic Signals.
In Periodic Signals, Pattern plays very important role as Pattern will be repeated by Periodic signals over a period of time.	In Non-Periodic Signals, No Patter will be repeated over a period of time.
Periodic signals are considered as deterministic signals.	Non-Periodic signals are considered as random signals.
To represent Periodic Signals, Mathematical	Mathematical equation cannot be used

Equation is used.	to represent Non-Periodic Signals.
We can determine the value of Periodic Signal at any point of time.	In Non-Periodic Signals, Value cannot be determined with certainty at any point of time.
Examples of Periodic signals are sin cosine square and sawtooth wave (non-sinusoidal waveform).	Examples of Non-Periodic signals are all kind of noise signals and sound signals generated by radio.

Both the Analog and Digital can be periodic or aperiodic. but in data communication periodic analog signals and aperiodic digital signals are used.

3.7 SIGNAL TRANSMISSION IMPAIRMENTS

In simple term, we can say that signal is transmission of electronic current that carries

There are some situations where signal transmission get disturbed and some time get destroyed. There may be a situation where there are problems in signal delivery during transmission. So in this section we are going to discuss about the factors that can affect the signal transmission, we call it transmission impairment.

The signals which are transmitting through transmission media, this signals are not proper. The defection is the origin of signal impairment. In the signal impairment, the signal at the starting point of the medium is not the same as the signal at the ending point of the medium. Means the signal which is sent and the signal received is not same.

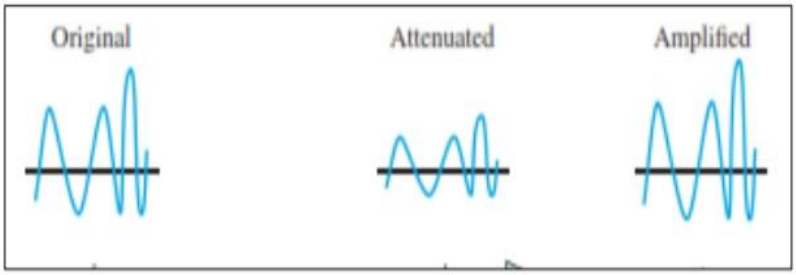
There are mainly three types of impairment are as follows:

1. Attenuation,
2. Distortion
3. Noise

Attenuation

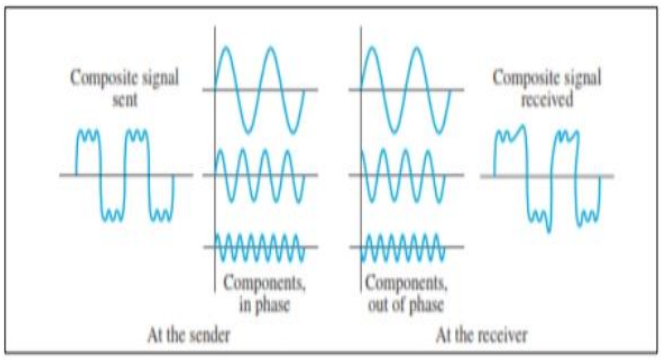
Attenuation is a loss of energy. When a signal, simple or composite, transmits through a medium, it loses some of its energy in overcoming the resistance of the medium. That is why a wire carrying electric signals gets warm, if not hot, after a while. Some of the

electrical energy in the signal is converted to heat. To compensate for this loss, amplifiers are used to amplify the signal. Following Figure shows the effect of attenuation and amplification.



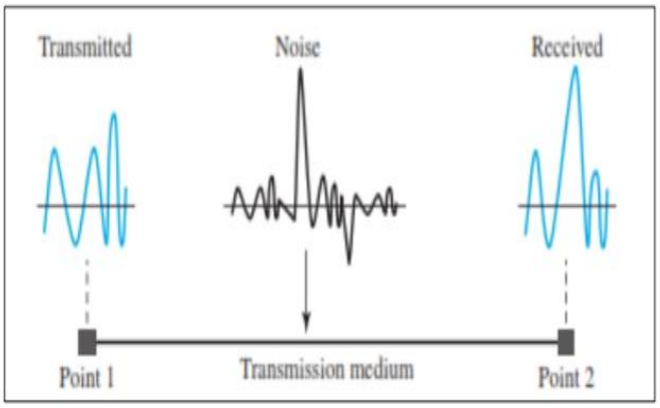
Distortion:

In distortion, the signal changes its form or shape. Distortion can occur in a composite signal made of different frequencies. Each signal component has its own propagation speed through a medium and, therefore, its own delay in arriving at the final destination. Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration. In other words, signal components at the receiver have phases different from what they had at the sender. The shape of the composite signal is therefore not the same. Following figure shows the effect of distortion on a composite signal.



Noise

Noise is another cause of impairment. There are different types of notice like thermal noise, induced noise, crosstalk, and impulse noise, may corrupt the signal. Following figure shows the typical diagram of noise.



There are many types of noise:

- **Thermal noise:**
  - It is the random motion of electrons in a wire, which creates an extra signal not originally sent by the transmitter.
- **Induced noise:**
  - It comes from sources such as motors and appliances. These devices act as a sending antenna, and the transmission medium acts as the receiving antenna
- **Crosstalk:**
  - It is the effect of one wire on the other. One wire acts as a sending antenna and the other as the receiving antenna.
- **Impulse noise:**
  - It is a spike (a signal with high energy in a very short time) that comes from power lines, lightning, and so on.

3.8 LET US SUM UP

In this unit, we have seen the fundamentals of communication theory of computer network. For better communication between the computers types of signal and its transmission is most important. There are two types of signals we have discussed, one in analog signal and another is digital. The continuous form of signal is known as analog whereas discrete form is known as digital. Digital signals are transmitted in the form of

bits that is 0's and 1's. Signals can be periodic and non-periodic as well. The signal which repeats a particular pattern in equal interval of time is known as periodic signal and others are non-periodic one. During the signal transmission there are disturbance, we call it impairment. Attenuation, distortion and noise are the impairments that caused the signal disturbance during transmission. For effective utilization of network we need effectively deal with these impairments.

3.9 CHECK YOUR PROGRESS

In this unit, we have seen the fundamentals of communication theory of computer

Do as Directed.

1. Define Signal.
2. Hertz is the unit of frequency. (True/False)
3. The reciprocal of time period is known as _____.
4. The continuous form of signal is known as _____ signal.
5. The discrete form of signal is known as _____ signal.
6. Crosstalk is type of noise in signal transmission. (True/False)
7. Expand: ASK, PSK
8. Define amplitude.
9. Define frequency.
10. A radio signal is the example of _____ signal.
11. Give any two example of digital signal.
12. Define communication.
13. A spike that comes from power line is known as _____ noise.
14. A signal that changes its shape is known as _____.
15. Which one of the following is not transmission impairment?
    a. Noise b. Distortion c. Attenuation d. None
16. _____ is the loss of energy.
    a. Noise b. Distortion c. Attenuation d. None
17. During transmission effect of one wire on other wire is known as _____.
    a. Noise b. Thermal noise c. Attenuation d. Crosstalk
18. Which one of the following is/are unit(s) of frequency?

a. Hz b. KHz c. GHz d. All

19. Telegraph signals are examples of

a. Digital signals b. Analog signals c. Impulse signals d. Pulse train

20.

21. Which one of the following is/are example(s) of periodic waves?

a. Sine wave b. Square Wave c. Triangular Wave d. All

22. Signal produced by microphone is _____ type of signal.

23. _____ is used to amplify the signal to avoid distortion.

3.10 FURTHER READING

In this unit, we have seen the fundamentals of communication theory of computer

1. “Computer networking”, A Top-down approach by Kurose and Ross, Seventh Edition.
2. The all new switch book, the complete guide to LAN switching technology by Rich Selfert and Jim Edwards.
3. e-resource: https://www.ibm.com/in-en/cloud/learn/networking-a-complete-guide

3.11 ASSIGNMENT

In this unit, we have seen the fundamentals of communication theory of computer

1 Define and differentiate periodic signal and non-periodic signal.
2 State the example of periodic signal.
3 Define noise and discuss its types.
4 Compare and contrast analog and digital signal.
5 State the examples of analog and digital signal.

3.10 ACTIVITY

Demonstration activity of distortion in the signal:

Plug in the old microphone, cut a plastic wire little bit and check for electronic disturbance if any.

BLOCK – 2

Networking Standards

Unit 1: Introduction to Standards

1

Unit Structure

2.1 LEARNIG OBJECTIVES

After studying this unit you should be able to understand following:

- Internet standards and its details.
- Application of internet standards.
- What is the process of methods to develop internet standards?
- How the communication process takes place through OSI

2.2 INTERNET STANDARDS

In previous block, we have seen fundamental of networking and its components. We have also seen types of network, internet, intranet and extranet. We have also discussed communication theory of the computer network. Now it is a time that we discuss the hierarchy of network communication and set of standards as well as protocol one need to follow for network and Internet.

So, in this particular unit we will focus on network or rather Internet standards that needs to be follow for establishing communication all across network. So let's start!

To operate, maintain and balance the usage of Internet and Internet community across World Wide Web (WWW), there arises a need of internet standards. There should be a body to maintain the community across the web for uniform usage of internet and its communications. For this purpose, Internet Society (ISOC) supports, promotes and supervise the formation of internet standards. It is also responsible for the policy creation and implementation of Internet standards and builds communities that make internet work.

Further section discusses a process of formation of Internet Society and also focuses on its various activities.

Formation of Different Network and Internet Standards Bodies

In the beginning of internet era, there were no authorised body or committees that can define roles and responsibility of the users of the internet. So, there arise needs of a

regulatory body which can manage and regulate standards of internet. So people started thinking to create a global body to facilitate the development of internet standards and protocols.

ARPANET (Advanced Research Project Agency Network) founded by the Department of Defence (DoD) of U.S in 1960 to set up a standards for computer communications. Several networking standards were developed in 1966 for computer communication. Many of the networking protocols we are following now days are also supported by ARPANET. One of the prominent protocols, namely TCP/IP (Transmission Control Protocol/Internet Protocol) was developed in 1977 to enable communications between the two different networks.

The next standard formation body is I**nternet Architecture Board (IAB)**. The main objective of this body to is to provide long range technical direction for the development of internet. There were approximately thirteen members in IAB, where each member was assigned a task, which they used to report to DoD. IAB strives to promote the technical evolution of an open and free internet without any special controls.

Following are the responsibilities of IAB:

- To provide architectural view of internet standards and procedures.
- To liaising with other organization on behalf of Internet Engineering Task Force (IETF)
- To manage and administer the appeal of process of internet standards.
- To select the chair of Internet Research Task Force (IRTF) and IETF.
- To give advice and guidance to the Internet Society.

In 1989, IAB is divided into two different task forces namely Internet Research Task Force (IRTF) and Internet Engineering Task Force (IETF). The responsibility of IRTF is to focuses on long term research issues related to the internet. The details will be discusses in the further sections. The Internet Society comes out as an organization. This organization has capability of creating standards for the internet. The members of IAB were appointed by trustees of internet society. This is how the Internet Society

(ISOC) was formed which thoroughly test and approved the proposed internet standards.

It is the responsibility of IETF to create and publish internet standards. Now, let's see the procedure for getting internet standards.

Procedure:

- **Proposed Standard:** This is the first step taken by IETF to define a proposed standard as well reviewed specification.
- **Internet Draft:** It is intermediary step after proposing standard and before internet standards.
- **Request for Comment (RFC):**

i. A Draft can be published by internet authority as a Request for Comment (RFC) and if it gets recommendation from the same.
ii. Each RFC can be edited and every RFC have a number also.
iii. RFC is categorized according to its requirement level and go through maturity levels before gaining the status of standard.

There are six maturity levels of RFC:

1. **Experimental**: This is a maturity level when RFC is applicable for experimental situation only.
2. **Informational**: If information regarding internet is there in RFC then such maturity level is classified as informational level.
3. **Proposed Standard**: If the work of RFC is in the interest of internet community then it is considered as proposed standards.
4. **Draft Standard**: If proposed standards seem promising for the further development then such RFC is classified as draft standards.
5. **Internet Standard:** When draft standards are successfully validated then it is considered as internet standard.

6. **Historic**: Such RFCs, falls in the category which can never achieve a goal of maturity level.

2.3 STANDARD ORGANIZATIONS

There are many organizations for establishment of the standards of internet. Following are the main organizations for developing a standard for internet:

- The Internet Society (ISOC)
- The Internet Architecture Board (IAB)
- The Internet Engineering Task Force (IETF)
- The Internet Research Task Force (IRTF).
- Internet Corporation for Assigned Names and Numbers (ICANN)

ISOC and IAB are already discussed above, so let's discuss it in brief.

Internet Society (ISOC)

ISOC is an international organization and it works on proposed specification of standards before final registration process. ISOC is not responsible for testing of this proposed standards, rather is assign such jobs to IETF and IRTF. The major objective of ISOC is to address the issues related to internet and its future. ISOC also promotes the research and scholarly activities also through IRTF.

IAB (Internet Architecture Board)

The role of IAB is to issue technical advice to the ISOC to ensure continuous growth of the internet. The evolution of internet is continuously monitored by IAB. IETF and IRTF are the two main task forces are supervised by IAB. IAB have the authority also to manage and suggest changes in RFCs.

Internet Research Task Force (IRTF)

- IRTF promotes research of importance to the evolution of the internet protocols, architecture, application and technology.

- IRTF research groups' focuses on longer term research issues and its member have long term membership to promote research collaboration within and outside the organizations.
- It is managed by IRTF chair in association with Internet Research Steering Group (IRSG).

Internet Engineering Task Force (IETF)

- IETF is an international community of network designers, operators and vendors.
- The mission of IETF is to make internet work better by providing relevant high quality technical documents to internet fertility so people can manage and use the internet in a proper way.
- It is responsible for publishing and accessing RFCs, managing intellectual property rights and approves the standard process.

Internet Corporation for Assigned Names and Numbers (ICANN)

- It is a non-profit organization responsible for maintain the several databases namespaces related to Internet.
- The duty of this body is to perform actual maintenance work and frame the standard related to names and numbers assigned to IP addresses.
- The other responsibility of ICANN is for IP address space allocation, protocol identifier assignment, generic and country code top level domain name system, etc.
- It is also responsible for setting up rules for financial transactions, Internet content control, data protection etc..

2.4 OSI RULES

History

International Organization for Standardization (ISO), the International Telegraph and Consultative Committee for International Telephony and Telegraphy (CCITT – *Now ITU-T*) are three main bodies to regulate the networking standards.

There are large numbers of users who use internet and are located across the world. Each user may find connection to the internet from all over world. That's why we need some common platform for the rules and regulation over internet. Each user can communicate with other over these rules and regulations. Systems must be developed which are harmonious to communicate with each other. A standard developed by the Internet Organization of Standardization (ISO). This standard knows as a model for Open System Interconnection (OSI) which is also well-known as OSI model.

Initially, they worked independently but after that they have merged their developed documents and formed well defined standards for network and internet as well. The merged document is known as Open System Interconnection (OSI) or basic reference model. It has two main parts: the seven layers and set of protocols.

The basic idea of seven layers of OSI model was proposed by Charles Bachman. The design of OSI model led to development of many networks such as: APRANET, National Physical Laboratory (NPLNET), European Informatics *Network* (EIN) etc. OSI model is layered architecture where each layers acts as neighbor and interconnected with their functionality. Each layer interacts directly with layer above and layer beneath.

The main aim of OSI model is to provide direction to manufactures, developers and the entire stake holder in order that program and device can operate together. OSI reference model gave complete guidance for having complete communication network. This thing generates importance of this model.

Features of OSI reference model

- It allows users to understand network communication.
- It provide means to devices about when to transmit data and when not.
- It facilitates arrangement and connection of physical transmission media.
- It is easy to correct and track the faults and/or errors in networking using OSI.
- It promotes the design of networking products that corresponds with each other over network.
- Troubleshooting is easier by separating layers.
- It can be used to compare basic functional relationship on different networks.

The principles of OSI reference model

- A well defined set of functions should be performed by each layer.
- Layer boundaries should be established to minimize the information flow across all the layers.
- There should be a separate layer for the relevant set of functions.
- Each layer function must be defined in such a way that it gets aligned with international protocols.
- Each layer communicates with its neighbor layers using interface only.
- The number of layers should be large enough so distinct functions need not be thrown together in the same layer and should not be small enough that network architecture does not become unwieldy.

2.5 COMMUNICATION PROCESS

This particular topic is related with how each layer communicates with its neighbouring layer.

There are seven layers of OSI model and following process describe how the communication process is taken place between the layers starting from topmost layers to the bottom layer.

- The topmost layer in OSI is application layer and the message which is going to transmit is prepared by this layer. This message is known as Protocol Data Unit (PDU) and application layer's message is known as Application Protocol Data Packet (APDU)
- The next layer is presentation layer and the APDU message is shared to this layer by application layer. APDU is processed by presentation layer and when process completed this message is named Presentation Protocol Data Unit (PPDU)
- The next layer session layer and the PPDU message is passed to the session layer.
- This PPDU is addressed as Session Protocol Data Unit (SPDU). The main job of this layer is to establish and control the dialog between the computers.

- Afterwards, SPDU is shared to transport layer, it process the SPDU and now it is termed as Transport Protocol Data Unit (TPDU). The main function of transport layer is to spilt the message from session layer to smaller unit and to pass these pieces (segment) to the next layer that is network layer.
- Network layer divides this segment in Packet. The basic function of this layer is to enable different network to be interconnected. This layer delivers packets from source to destination across multiple networks.
- These packets are divided into frames at the data link layer. This layer performs framing of packets, error detection and correction, acknowledgement and flow control.
- The final layer is physical layer which creates raw binary streams from frames and connect this stream to the physical components.

2.6 LET US SUM UP

This unit had discussed the introduction to internet standards and ISOC. History and emergence of ARPANET were also discussed. ISOC is an organization which consists of the organization like IAB, IETF, IRTF, ICANN and many more. Each this body is responsible per particular task. Then formation of ISOC is discussed and there were five maturity levels that one needs to deal with to formulate any standard. The five levels are proposed standard, draft standard, internet standard, experimental and informational. The International Organization for Standardization (ISO), the International Telegraph and Telephone Consultative Committee (CCITT) developed a standard for methods of networking. Finally, OSI reference model rules and communication process was discussed.

2.7 CHECK YOUR PROGRESS

1. Multiple Choice Questions

1. Largest professional engineering society in the world is

   A. American National Standards Institute (ANSI)

B. International Organization for Standardization (ISO)

C. Association of Computer Manufactures (ACM)

D. Institute of Electrical and Electronics Engineers (IEEE)

2. Organization that is developing cooperation in realms of scientific, technological and economic activity is.

A. Association of Computer Manufactures (ACM)

B. Institute of Electrical and Electronics Engineers (IEEE)

C. International Organization for Standardization (ISO)

D. American National Standards Institute (ANSI)

3. The protocol data unit (PDU) for the application layer in the Internet stack is

A. Data

B. Segment

C. Message

D. Frame

4. Write the full form of SMTP:

A. Synchronous Mail Transfer Protocol

B. Synchronous Mail Transfer Process

C. Synchronous Mail Transfer Process

D. Simple Mail Transfer Protocol

5. Total maturity levels for ISOC is _____

A. Three

B. Five

C. Seven

D. Eight

6. Which standard goes to internet standard after modification?

A. Proposed standard

B. Draft standard

C. Informational Standard

D. Experimental Standard

7. _____ Standard have never passed the maturity level.

A. Draft

B. Historic

C. Experimental

D. None of these

8. Which standard does define experimental situation?

A. Experimental standard

B. Proposed standard

C. Draft standard

D. None of these

9. An RFC is labeled _____ is not required to have minimum conformance.

A. Required

B. Recommended

C. Elective

D. Limited use

10. An organization which works on long-term research projects is _____.

A. IAB

B. IRTF

C. IETF

D. ARPANET

11. The organization which is responsible for the overall planning and designing of the Internet is _____.

A. ISOC

B. ARPANET

C. IETF

D. IAB

12. The topmost layer of OSI reference model is _____ layer.

A. application

B. presentation

C. data link

D. Physical

13. The _____ layer deals with representation of bits on the media.

A. application

B. data link

C. physical

D. presentation

14. Error correction and detection is performed by _____ layer of OSI.

A. Data link

B. Application

C. Transport

D. Physical

15. The network layer deals with _____ format.

A. packet

B. segment

C. frame

D. bit

2. True/False:

1. OSI reference model is invented by Alan Turing.
2. There are seven layers in OSI model.
3. IAB stands for Internal Architectural Board
4. The lowest layer of OSI model is application layer.
5. Data link layer is responsible to decide flow control of packets.
6. Authentication is performed by session layer.
7. The main function of transport layer is to accept data from session layer and pass it to network layer.

2.8 FURTHER READING

- Brief history of Internet https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf
- Andrew S. Tanenbaum, “Computer Networks”, Prentice Hall PTR
- Data and Computer Communication, William Stalling, Pearson Education, Delhi.

2.9 ASSIGNMENT

1) Describe the formation of ISOC.
2) Define and differentiate the roles and responsibility of IETF and IRTF.
3) Define and differentiate (i) Internet (ii) draft (iii) proposed standard.
4) Write brief note on IAB.
5) What is RFC? Explain in brief.
6) Discuss various maturity levels in detail.
7) Discuss the basic purpose of OSI reference model.
8) Discuss the features of OSI in detail.

Unit 2: OSI Reference Model

2

Unit Structure

2.1 LEARNIG OBJECTIVES

After studying this unit you should be able to know about:

- OSI Reference Model and its relevance in computer networks
- Brief understanding of all OSI Layers

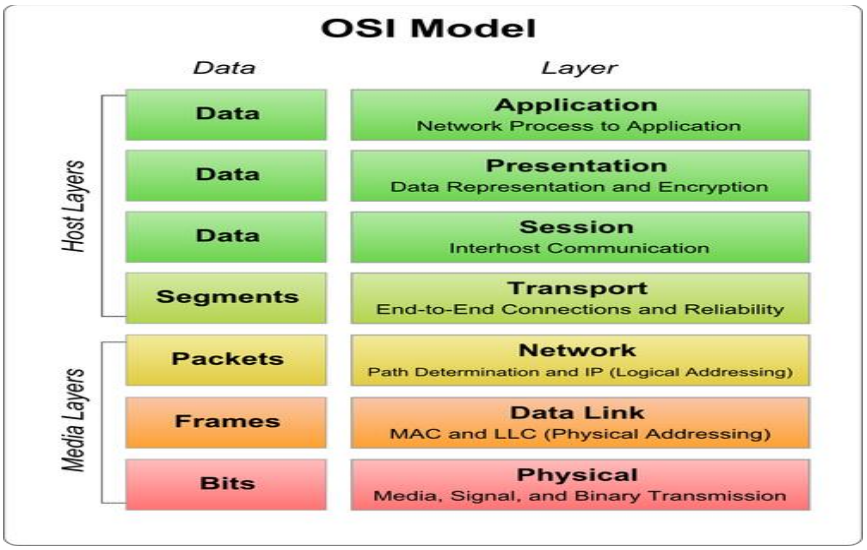
2.2 INTRODUCTION OF OSI REFERENCE MODEL

OSI stands for Open Systems Interconnection and it is developed by International standard organization (ISO) in 1984. There are seven layers according to the OSI model. It is basic framework which describes the functioning of networking systems and their intercommunications. It is a kind of universal set of rules as well as requirement which describes interoperability between different devices, hardware, software etc.

The seven OSI layers have several grouped different communication protocols that have similar functions. Functions like communication, management, security etc.

The OSI model is designed in such a way that each layer can perform its functions independently. Each layer is dependent upon the layers below it to function. Following image shows the layers of OSI model.

There are two parts of OSI layers: Upper and Lower. Upper layer mainly deals with application and end user related issues while lower layers deals with data transportation related issues. Let's see the each layer in detail.



[Image Source: https://www.tech-faq.com/wp-content/uploads/2009/01/osimodel.png]

2.3 APPLICATION LAYER

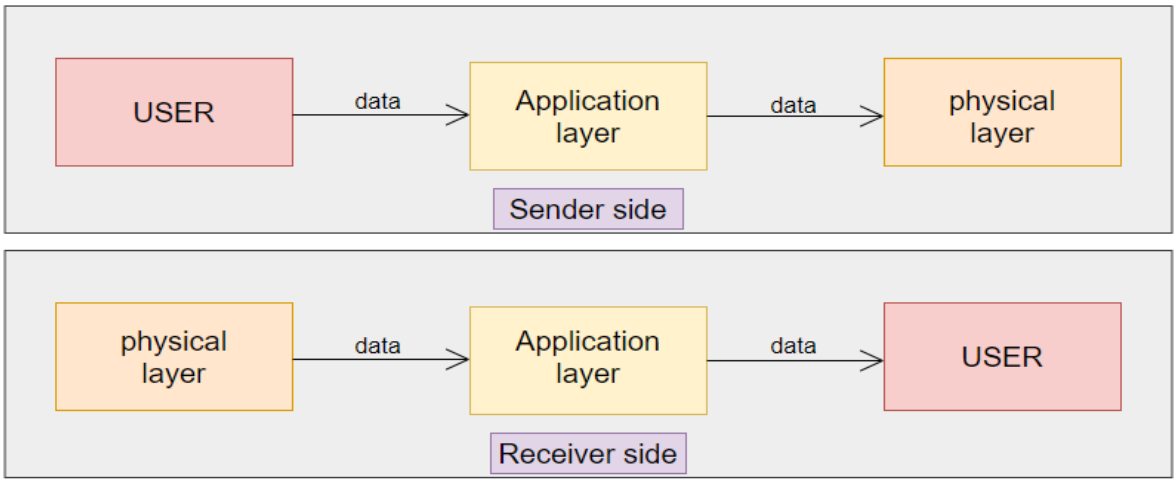


Figure: Application layer

An interface provided for the end – user operating device which is connected to the network by the application layer. Issues like network transparency, resource allocation etc. are handled by this layer. An application performs functions of application layer but application is not an application layer. The end-user able to use the network services which are provided by the application layer.

The Functions which are provided by application layer are listed below:

- **File transfer, access and management (FTAM):**
    - An application layer provides facility to the user for access the files, fetch the files and manage files which are stored in remote computer.
- **Mail services:**
    - An application layer allow user to forwarding emails or e-messages. An application layer provides storage to end-users.
- **Directory services:**
    - The distributed database sources are provided via

application. This functionality also uses to provide that global information about various objects.

There are various protocols which are included in this layer. Some of them are listed here.

- Teletype Network (TELNET)
- File Transfer Protocol (FTP)
- Simple Mail Transfer Protocol (SMTP)
- Domain Name System (DNS)
- Hyper Text Transfer Protocol (HTTP)

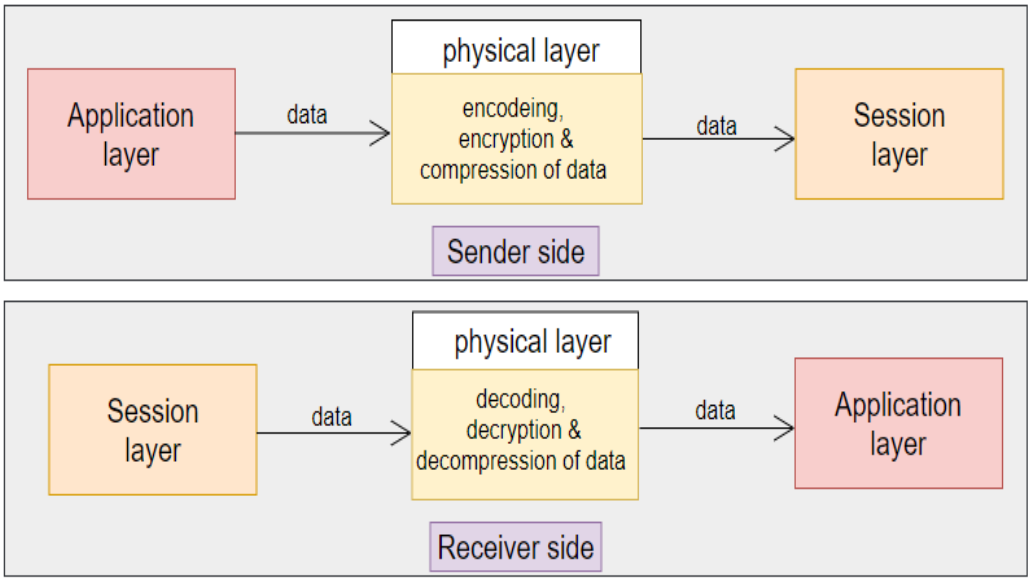
Let's discuss in detail.

- **TELNET (Teletype Network):**
  - Telnet provides facility to remote computer in such manner that connected local computer can managed by remote computer using terminal shown on remote computer.
- **HTTP (Hyper Text Transfer Protocol):**
  - For accessing the data on the World Wide Web (WWW) we can use HTTP protocol. The HTTP protocol used to transfer various forms of data like plain text, hypertext, audio, video etc.
- **FTP (File Transfer Protocol):**
  - FTP is standard internet protocol. This protocol is provided by TCP/IP. The main task of this protocol is to transfer files from one host to another one. We can use FTP protocol for downloading the files to computer from other servers.
- **DNS (Domain Name System):**
  - DNS provides a directory service. This directory store the host name on the network and numerical address of host, DNS also map this information. DNS protocol is very important and required for the network functions. For

example, the Web site had IP address of 132.137.156.85, we can reach to this site by specify the name of site www.abc.com.There is no need of IP address for visit the site.

- **SMTP (Simple Mail Transfer Protocol):**
    - SMTP protocol allows software/application to transmit an electronic mail through the internet using set of communication guidelines. This protocol use e-mail addresses for sending messages to other user's computer. These messages include text, audio, video or graphic.

2.4 PRESENTATION LAYER



Presentation model translate or interpret the message comes from application layer to network format vice versa. It is a bridge between application layer and the network. For example conversions of text file to ASCII code file. It works on Main three tasks: Translation, Encryption/decryption and last one is Compression.

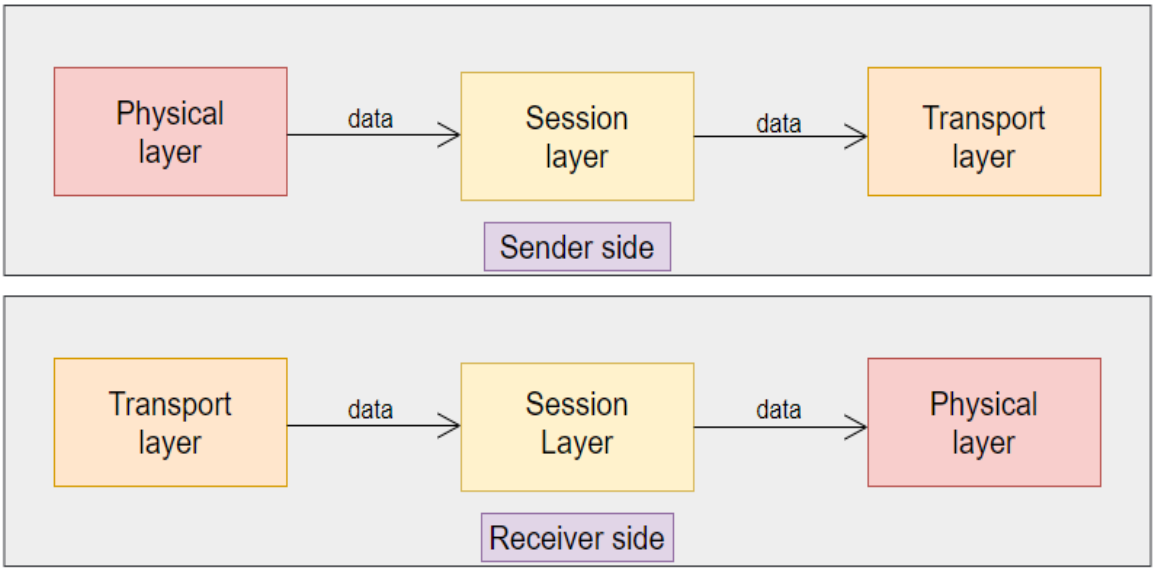
There are three functions of physical layer:

- **Translation:**

- The task of translation is to convert the end user's message into binary format at sender side and at receiver side convert this binary message in to original message which sender sent. End user's message is in many form link characters, numbers, images, audio, video etc. The translation of data is based on computer and requirement of network. The conversion of sender-dependent format to common/binary format is known as encoding. The conversion of common/binary format to receiver-dependent format is known as decoding.

- **Encryption:**
  - The task of encryption is to secure the data before sent to the destination. Security is important thing because data is sent over unsecured channels. So the data is transformed in such format that unauthorized person could not understand the data. This transformed data known as encrypted data. When the encrypted data reach to the destination, receiver performs operations to decrypt the encrypted data to achieve original data. In short, Encryption means to transform the data for securing it and decryption means to retrieve original data which is encrypted through sender.
- **Compression:**
  - Before transmission of message/data the sender reduce the size of message. This is called as compression. When receiver receives the compressed message some operations are performed by receiver to decompress the compressed message to retrieve the original message. Compression of data is very important in multimedia like text, audio, video.

2.5 SESSION LAYER



Connections between two computers were controlled by this session. Local and remote application's connection is established, managed and terminated by this layer. First it receives message from physical layer and transfer this message to transport layer.

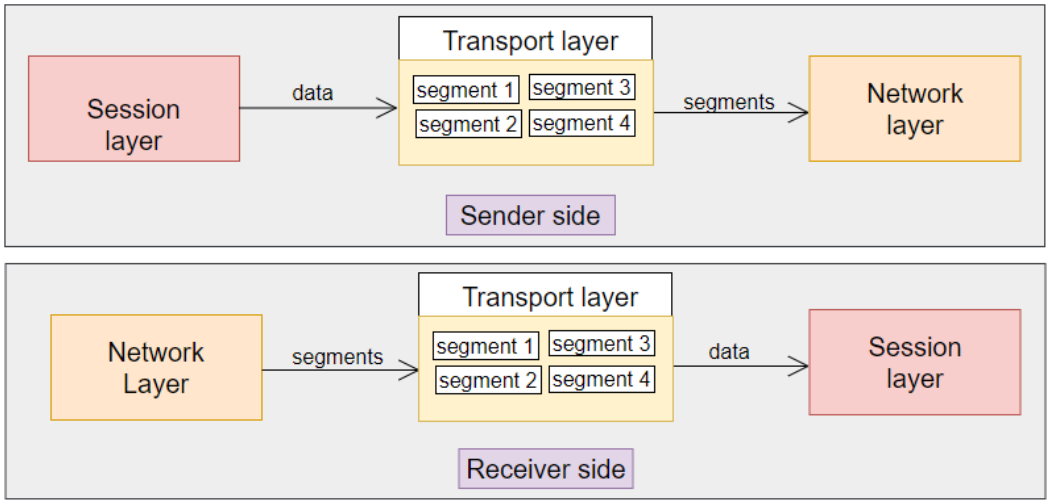
The functions of the application layer are listed below:

- **Dialog control**:
  - Session layer supports two transmission mode half-duplex and full duplex. If two processes are communicating using any one mode from these two modes then the session layer allow them to communicate.
- **Synchronization:**

It is used to establishing procedures for check-pointing, suspending, restarting and terminating a session. This layer is answerable for closing a session, check- pointing and recovery. In the middle of the transmission of data, if some error occurs then the transmission, then the transmission occur again from the checkpoint.

For example there are total 500MB data are transmitted. It puts check points at every 50MB. Then it ensures the successful transmission of every 50MB and acknowledged about it. If system has some issue like crash and reported at 300MB data transferred, then sender does not have to retransmit all 300MB. But it will resume the transmission after the last checkpoint.

2.6 TRANSPORT LAYER



Messages/services are received form session layer and this messages/services shares to the network layer by transport layer. It is responsible for delivering entire message from source device to destination device.

There are two protocols used by this layer which are listed here in brief:

- **Transmission Control Protocol (TCP):**
  - This is a standard protocol that provides facility to the systems to communicate over the internet. A connection between hosts are established and maintained by this protocol. The data is divided into smaller units / chunks, these units known as segments. This rebuilding process of data to segment is provided by TCP protocol. This protocol use different routers for transmitting each segment through the internet and the receiver is receiving these segments

which is not in same order as same they are transmitted. After receiving all segment at receiver side, the TCP protocol perform task of rearrangement of the segment in the same order as they are transmitted.

- **User Datagram Protocol (UDP**):
  - UDP is used for transmission of the data. The transmitted data is not acknowledged, and that's why this protocol is not reliable. When sender sends data into smaller segments, the sender is not waiting for any acknowledgement that transmitted segments are properly received by receiver successfully. And the receiver is not sending any acknowledgment that packets / segments are received successfully.

The functions of the transport layer are listed below:

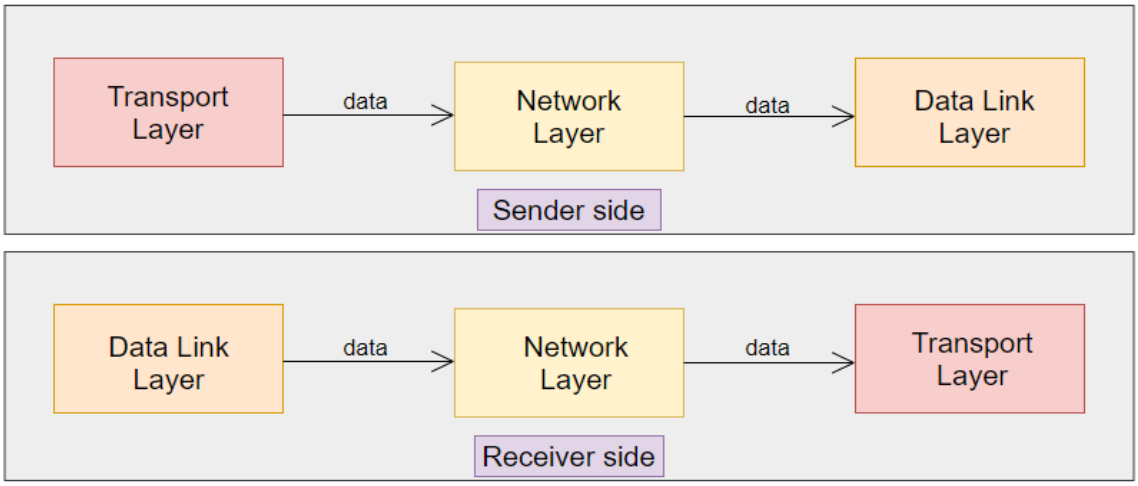
- Port address is added by transport layer to the header of the data packets. From specific process of one computer to a specific process of another computer, message is delivered.
- The message is sent into smaller segment. Segment is nothing but smaller units of received data from upper layer. Each segment contains sequence number with the destination port number. This sequence number ensures that the segments arrive correctly at receiver side. After collection all segments at receiver side, this layer reassembles them.
- For both connection-oriented and connection less services, it provides an error free point-to-point channel.

Error identification is done in this layer. It also provides error correction techniques for removing errors. These errors can be of damaged packets, lost packets or duplication of packets.

2.7 NETWORK LAYER

- This layer control delivery of data packets from the source to across provided by this layer.
- Issues like transmission delays, transmission time, avoidance of jitters etc. are tackled by the network layer.

multiple nodes. The operations of subnet are controlled by this layer.

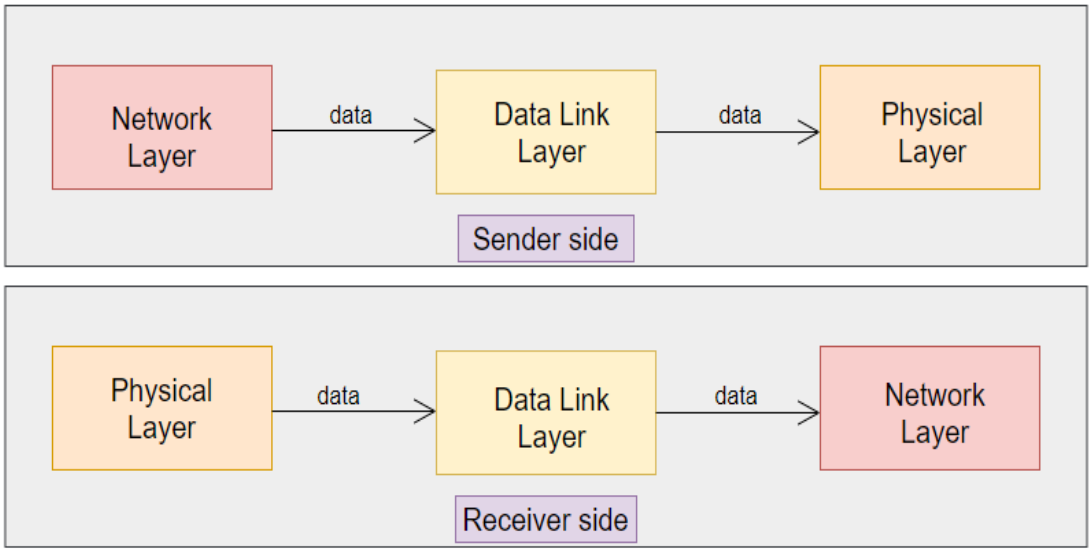


The functions of the network layer are listed below:

- This layer takes responsibility for routing packets from the sender to receiver. Routes are rarely changed and they are based on static tables. Based on the condition of the network they can be updated automatically. When the data packets are routed to remote locations, we need a logical addressing schema to differentiate between the source system and the destination system. This schema

2.8 DATALINK LAYER

Node to node data transformation is provided by data link layer. It create link between two nodes which are directly connected. It finds and rectifies errors that may occur in the physical layer.



The functions of the Data link layer are listed below:

- **Framing:**

Frame is nothing but streams of bits. These bits are retrieved from one of its neighbor layer the network layer into data packs which are manageable. These streams of bits are created by Data link Layer.

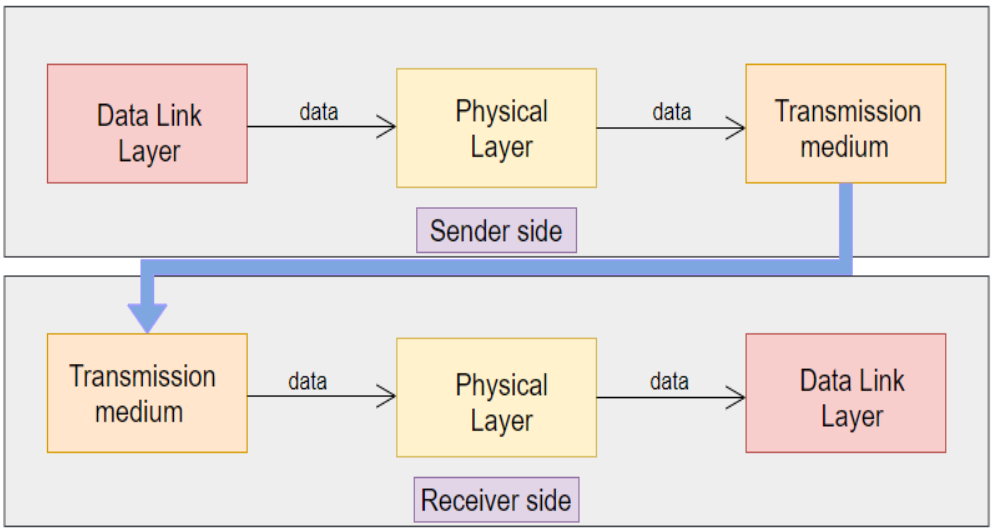
HEADER	PACKET	TRAILER

- **Physical Addressing:**
  - A header is added to the frame by the data link layer. If the frame is transmitted over different systems of the network, the header stores the physical address of sender as well as receiver's address.
- **Flow control:**
  - Flow control provides extra bits. This extra bit is

known as buffer. Task of buffer is to avoid a fast transmitter from running a slow receiver. Mainly, buffer is used for avoiding issue of traffic jam at receiver side.

- **Error control:**
  - At the end of frame we are using mechanism of adding trailer at the end of frame for reduce the duplication of frame. The task of adding trailer is done by Error control.
- **Access control:**
  - When two or more devices are use same link for connection, this protocol decides a fix time for every device for control over the link.

2.9 PHYSICAL LAYER



The responsibility of this layer is to send bits form one system to other system of the network. The main task of this layer is of setting up physical connection to the network, relaying signals and receiving signals.

The functions of the Data link layer are listed below:

- **Representation of Bits**:

- Data contains streams of bits. For transmission, it is essential task to encode bits into signals for the transmission. Type of encoding is defined by this layer. For example how 0's and 1's are changed to signals

- **Data Rate:**
  - How much bits are transferred per second is defined by this layer as rate of transmission.
- **Synchronization:**
  - Coordination of sender and receiver is done by this layer. At bit level, the sender and receiver coordinate with each other.
- **Interface:**
  - The transmission interface which is also known as communication interface between devices and transmission medium are defined at this layer.
- **Line Configuration:**
  - This layer connects devices with the medium like node-to-node configuration and multimode configuration. There are different mediums for connections of devices like point-to-point configuration or multipoint configuration.
- **Topologies:**
  - Topology is Physical or logical arrangement of network. Devices have to connect using topologies for transmission of the Data.
  - There are many types of topologies like Mesh, Star, Ring and Bus. In next, block detail study of topologies will be covered.
- **Transmission Modes:**
  - The task of transmission mode is to direct the transmission between two devices.
  - There are basically three transmission modes: Simplex,

Half Duplex, and Full Duplex.

- A device can only send data but cannot receive the data is known as simplex transmission.
    - For example sending command to computer via keyboard.
- A device that can send and receive the data but not both operations at the same time is known as half duplex.
    - For example: walkie-talkie.
- A device can send the data as well as receive the data at same time is known as full duplex transmission.
    - For example: Telephonic conversation where we can talk and listen at the same time.

- One can also deal with baseband and broadband transmission in this layer.

So, this was all about OSI reference models and its detail. In next unit IEEE standards will be covered.

2.10 SUMMARY

In this chapter we learnt about OSI reference model and its layers. We learned about different functions of OSI layers. There are seven layers in OSI reference model. Each layer has its own several functions. Each layer is dependent on its neighboring layer.

2.11 FURTHER READING

1. Computer network by Tanenbaum
2. OSI model:
   https://en.wikipedia.org/wiki/OSI_model

3. Network topologies:
   https://www.tutorialspoint.com/data_communication_computer_network/computer_network_topologies.htm -:~:text=A%20Network%20Topology%20is%20the,different%20in%20a%20same%20network.
4. Transmission modes:
   https://www.javatpoint.com/computer-network-transmission-modes

2.12 CHECK YOUR PROGRESS

1. Match the pairs:

A	B
Source to source delivery	Network layer
Point to point delivery	Transport layer
Process to process delivery	Data link layer

2. Match the pairs:

A	B
Network layer	Segments
Data link layer	Frames
Session layer	Packets
Transport layer	Sessions

3. Multiple choice questions:

1) Full form of OSI is _____
   a) open system interconnection
   b) operate system interface
   c) optional services implementation
   d) open service Intranet
2) There are _____ numbers of layers in ISO OSI reference model

a) 4 b) 5 c) 6 d) 7

3) _____ address is used to identify a process on a host by the transport layer?
   a) Physical address
   b) Logical address
   c) Port address
   d) Specific address
4) The services to user is provided by _____
   a) application layer
   b) session layer
   c) presentation layer
   d) physical layer

5) Which layer decides the Transmission data rate?
   a) Network layer
   b) Physical layer
   c) Data link layer
   d) Transport layer
6) The physical layer deliver data by _____
   a) bit-by-bit delivery
   b) application to application delivery
   c) process to process delivery
   d) port to port delivery
7) The data link layer takes the packets from _____ and encapsulates them into frames for transmission.
   a) Transport layer
   b) physical layer
   c) Network layer
   d) application layer
8) Which of the following tasks is not done by data link layer?

a) Framing

b) Error control

c) Flow control

d) **C**hannel coding

9) Which of the following tasks is not done by data link layer?

a) Framing

b) error control

c) flow control

d) channel coding

10) Automatic repeat request error management mechanism is provided by _____

a) logical link control sub layer

b) media access control sub layer

c) network interface control sub layer

d) application access control sub layer

11) Which type of data is concerned by the network layer?

a) Bits

b) Frames

c) Packets

d) Bytes

12) Which one of the following is not a function of network layer?

a) Routing

b) Inter-networking

c) Congestion control

d) Error control

13) Transport layer aggregates data from different applications into a single stream before passing it to _____

a) Network layer

b) Data link layer

c) Application layer

d) Physical layer

14) Transport layer protocols deals with _____

a) application to application communication

b) process to process communication

c) node to node communication

d) man to man communication

15)_____ is a Physical or logical arrangement of network

a) Topology

b) Routing

c) Networking

d) Control

16)Using _____ we can communicate with whole world.

a) LAN

b) WAN

c) MAN

d) PAN

17)A building or campus use _____network for Data communication system internally.a) LAN

b) WAN

c) MAN

d) PAN

18)The full form of WAN is _____

a) World area network

b) Wide area network

c) Web area network

d) Web access network

19) _____ give permission to LAN users for sharing computer programs and data.

a) Communication server

b) Print server

c) File server

d) Network

20)OSI reference model is developed by _____

A) ANSI - American National Standards Institute

B) ISO - International Standards Organization

C) IEEE - Institute of Electrical and Electronics Engineers

D) ACM - Association for Computing Machinery

2.12 ASSIGNMENT

1. Draw diagram of OSI Reference model. Write down in brief about OSI model.
2. Write down functions of network layer.
3. Write down functions of physical layer.
4. Write down functions of data link layer.
5. What are the functionalities of transport layer?

Unit 3: IEEE 802 Family Standard

3

Unit Structure

3.1 LEARNIG OBJECTIVES

After studying this unit student should have:

- Introduction of IEEE 802 standard
- Understanding of IEEE 802.2 standards
- Understanding of IEEE 802.3 standards
- Understanding of IEEE 802.11 standards
- Understanding of IEEE 802.15 standards

3.2 INTRODUCTION TO IEEE 802 STANDARDS

Before we start with IEEE 802 standards, let's understand what IEEE stands for? IEEE stands for Institute of electrical and electronic engineering. IEEE is non profitable organization, who sets standards for electrical and electronic equipment. Standard is nothing but level of quality to be provided.

The physical and the data link layer specifications for technologies like Ethernet to wireless are covered by IEEE 802 standard. There are 22 subparts of IEEE 802. IEEE 802 standard is mainly used by Local Area Network (LAN), Personal Area network (PAN), and Metropolitan Area network (MAN).

Now we will see some popular networking technologies from IEEE 802, which are used for computer networking: IEEE 802.2, IEEE 802.3, IEEE 802.5, IEEE 802.11, IEEE 802.15, and IEEE 802.16.

3.3 IEEE 802.2 (LOGICAL LINK CONTROL SUBLAYER)

The data link layer of The OSI (Open System Interconnection) model is subdivided into two sub layers. The first one is Logical Link control (LLC) and the second one is Media Access control (MAC). Originally LLC sublayer was invented by IEEE with collaboration of American National Standards Institute (ANSI). After that LLC sublayer was also adopted by International Organization for Standardization (ISO) in 1998. LLC is also known as

ISO/IEC 8802-2 standard.

Medium access control (MAC) is the upper layer of LLC. This MAC sublayer creates message and then passes the message to LLC sublayer. LLC sublayer adds some control information on the message. Now this resulting packet from the processing of message by LLC sublayer is known as protocol data unit (PDU) and the additional information is known as LLC Header. This LLC Header is comprised of three segments: control field, SSAP (source service access point) and DSAP (Destination service access point).

The protocol data unit (PDU) structure for data communication systems is defined using bit-oriented procedures. There are two types of operation for data communication between service access points. In one type of operation, PDUs are exchanged between LLCs. There is no need of creation of a data link connection. Whereas in the second type of operation, a data link connection is established between two LLCs prior to any exchange of information-bearing PDUs.

Operation Mode:

IEEE 802.2 provides total three operation modes. From these three operation modes two operation modes are for connectionless operation modes and one operation mode is for connection oriented operation mode.

- **Type – 1:** It is a connectionless mode without acknowledgement for datagram services. There are three different ways for sending frames which are supported by this type. These ways are as following:
    - Point to point (single destination/ unicast transfer)
    - Multicast (multiple destination of same network)
    - To all systems of the network (Broadcast)

When we want to share same information to all system of the network and at the same time we want to reduce network traffic, we can use multicast and broadcast way of sending frames.

- **Type – 2:** It is a connection oriented operation mode. Sequence of numbering indicates that the received frames are in order of they were sent. So in this type we can track loss of frames during transmission of message.
- **Type – 3:** we can use this type for connectionless acknowledged service. It only supports single destination.

Each network node is assigned an LLC Class in accordance to which service type network node is supporting. Following table depicts the same.

LLC class	Supported Service Type		
	Type – 1	Type – 2	Type – 3
1	YES		
2	YES	YES	
2	YES		YES
4	YES	YES	YES

LLC Header:

Ideal Format for IEEE 802.2 LLC PDU			
802.2 LLC header			Information
DSAP address	SSAP address	Control	
8 bits	8 bits	8 or 16 bits	Multiple of 8 bits

Above table shows the format of any IEEE 802.2 LLC PDU.

Two eight-bit address fields are included in the 802.2 header. These fields are known as service access points (SAP) in the OSI terminology. SAP is divided into two parts:

1. SSAP (Source Service Access Point):
- ✓ SSAP stores logical address with 8 bit length.
- ✓ The network layer entity creates the message. The logical address of this entity is represented by the SSAP.

2. DSAP (Destination Service Access Point):
- ✓ For receiving message we need to store a logical address of the network layer entity.
- ✓ This logical address is 8 bit long which is represented by the DASP

Many protocols use the Sub-network Access Protocol (SNAP) extension which gives permission using Ether Type values to specify the protocol being transported atop IEEE 802.2. The SNAP extension is added to the 802.2 LLC PDU headers.

Sub Network Access Protocol (SNAP) Extension					
802.2 LLC header			SNAP extension		Upper layer data
DSAP address	SSAP address	Control	OUI	Protocol ID	
8 bits	8 bits	8 or 16 bits	24 bits	16 bits	Multiple of 8 bits

Control Field:

Control field is to follow the destination and source SAP fields. IEEE 802.2 was derived from HDLC (High-Level Data Link Control). There are three types of PDUs, which are as following:

1. U-format PDUs:

- ✓ Here U represents Unnumbered.
- ✓ U-format is used for connectionless applications. The length of U-format PDU's control field is 8 bit.

2. I-format PDUs:

- ✓ Here I represent Information Transfer.
- ✓ U-format is used for connection oriented applications.
- ✓ The length of U-format sequence numbering is 16 bit.

3. S-format PDUs:

- ✓ Here S represents supervisory. U-format is used at LLC layer for supervisory function. The length of U-format PDU's control field is 16 bit.

3.4 IEEE 802.3 (Medium Access Control Sub layer)

IEEE 802.3 is a working group. Medium Access Control Sublayer (MAC) defines the physical layer and data link layer's media access control of wired Ethernet. Medium Access Control Sublayer is a LAN technology with some WAN applications. Various types of copper or fiber cables are used to create physical connection between nodes and/or infrastructure devices like hubs, switches and routers. IEEE 802.3 is a technology that supports the IEEE 802.1 network architecture. IEEE 802.3 defines LAN access methods using CSMA/CD.

CSMA/CD is an abbreviation for Carrier Sense Multiple Access/Collision Detection. This protocol use carrier transmission which one is operated in

Medium Access Layer. This protocol checks whether channel is busy or not and also delays transmissions if the channel is not free. Collision detection is also done by this protocol by sensing transmissions. Various functions of MAC sublayer are as described in following text:

- MAC sublayer provides an abstraction of the physical layer to the sublayer of Data Link layer the LLC and upper layers of the OSI network.
- Responsibility for summarizing frames is on MAC sub layer. The need of summarize the frames to make them acceptable for transmission via physical layer.
- MAC sublayer works on sorting out the addressing of source station and the sorting of the destination station/stations also.
- When there is a requirement to share more than one data frame at a time, MAC sublayer performs multiple access resolution. MAC sublayer controls the channel access methods for transmission of messages.
- In case of collision MAC sublayer also executes collision resolution and takes action on retransmission of messages.
- MAC sublayer generates the frame check sequences and in this way the protection against transmission errors are done.

AC Addressing:

MAC address stands for media access control address. MAC address is nothing but unique identifier allocated to a network interface controller (NIC) of device. This MAC address is used as network address. This network address is for data transmission within a network segments like, Wi-Fi, Bluetooth and Ethernet.

At the time of manufacturing, this MAC address is assigned to a network adapter. MAC address consists of six groups of two hexadecimal digits. These six groups are separated by no separators or colons or hyphens. MAC address is of 6 bytes, which means 48 bits long. For example, MAC address is 00:A0:74:5B:E0:62.

3.5 IEEE 802.11 (Wireless Local Area Network)

IEEE 802.11 standard is also known as Wi-Fi. This Wi-Fi / WLAN use high –frequency radio waves instead of cable for connecting the devices in LAN. Users can do transmission within the coverage of area of network, which are connected to WLAN.

There are many standards of IEEE 802.11 WLANs. From all the standards some of very important standards are described in text below:

802.11:

It is the first and original version of Wi-Fi.

The data transfer rate is 1 Mbps or 2 Mbps in the 2.4 GHz band in this version.

802.11a:

This is modified version of 802.11. The data transfer rate is 54 Mbps in the 5 GHz band in this version. This version also provides facility of error correction code.

802.11b:

This standard uses same technique as 802.11. But the data transfer rate of this standard is higher than 802.11 standards in the same 2.4 GHz band. The data transfer rate is 11 Mbps in 2.4 GHz band in this standard or version.

802.11g:

It also uses same 2.4 GHz band but data transfer rate is of 22Mbps. It is fully backward compatible with 802.11a and 802.11b.

802.11n:

It uses both the 2.4 GHz and the 5 GHz bands. The data transfer rate is in range from 54 Mbps to 600 Mbps in this version. 802.11p: This version of Wi-Fi uses 5.9 GHz band and data transfer rate is 27 Mbps.

All the Wi-Fi standards are summarized as follows:

Wi-Fi Standards	Description
802.11	First and Original standard. Used the 2.4GHz frequency band and a maximum bandwidth of 2 Mbps.
802.11a	Under ideal conditions, it has achieved speed up to 54 Mbps.
802.11b	Much cheaper to develop because it uses the 2.4GHz band. Achieves speed up to 11 Mbps.
802.11c	Associated with bridging 802.11 wireless client device.
802.11d	Allows clients to automatically configure themselves to the specifications of its operating country.
802.11e	Offers quality of service features to improve delay-sensitive applications like data, voice, and video.
802.11f	Provides communication between standard 802.11 access points on the distribution system.
802.11g	Combined the best of 802.11a/b to achieve speed up to 54 Mbps on the 2.4GHz band.
802.11h	Originally designed for European regulations to resolve interference issues with satellite and radars using the 5GHz band.
802.11i	Addressed vulnerabilities in WEP (Wired Equivalent Privacy) security and improved wireless encryption by replacing short authentication and privacy with detailed

	security for 802.11a/b/g networks.
802.11j	Designed for Japan, it provides specifications for the use of the 4.9GHz and 5 GHz bands for outdoor, indoor, and mobile applications.
802.11k	Improves traffic distribution within a WLAN.
802.11m	Maintenance of the 802.11 series and related documentation.
802.11n	Uses the 2.4GHz and 5GHz bands and improves speed up to 600 Mbps.
802.11p	Adds wireless access in vehicular environments (WAVE).

3.6 IEEE 802.15 (Wireless Personal Area Network)

IEEE 802.15 group is set up to reflect on wireless networks with a range of 10 meters or WPANs. The aim is to provide connections between different portable single user or multiple users. This network can connect laptop, mobile phone, PDAs etc. Following table briefly describes IEEE 802.15 standards with its description.

IEEE 802.15 Standards with their description	
Standard	Description
IEEE 802.15.1	It is based on Bluetooth Technology. Used for Wireless Medium Access Control (MAC) specifications for Wireless Personal Area Networks (WPAN)
IEEE 802.15.2	It supports interoperability between WPANs and WLANs.
IEEE 802.15.3	It supports high data rates greater than 20 Mbps.
IEEE 802.15.4	It defines the operations on a low rate

	WPANs.
IEEE 802.15.5	It is used for Mesh Topology Capability in Wireless Personal Area Networks (WPANs)
IEEE 802.15.6	It standardizes Wireless Body Area Networks (WBAN).
IEEE 802.15.7	Use in Visible Light Communication and Short-Range Optical Wireless Communications
IEEE 802.15.8	Handles Peer Aware Communications (PAC). PAC includes discovery of peer information without any association.
IEEE 802.15.9	It provides key management support to IEEE 802.15.4 and IEEE 802.15.7.
IEEE 802.15.10	It supports dynamically routing of packets in dynamically changing IEEE 802.15.4 with minimum impact on route management.

Above is only brief information, there are lot of versions and up gradation of each and every standard. But, currently it is not in our scope of our study, so we will learn in the forthcoming semesters.

3.7 SUMMARY

We learnt about IEEE, The IEEE 802 standard and different sub standards of it. The physical and the data link layer specifications for technologies like Ethernet to wireless are covered by IEEE 802 standard. Different standards like IEEE 802.2, IEEE 802.3, IEEE802.11 and IEEE 802.15 have their own specifications. IEEE 802.2 offers three operation units. From these three operation unit, two are of connectionless and one is of connection-oriented units. IEEE 802.3 works with medium access control (MAC) of the physical layer and the data link layer. IEEE 802.11 works on wireless local area networks (Wi-Fi / WLAN). There are several extensions of IEEE 802.11 standards, some of them are

IEEE 802.11a, IEEE 802.11b, IEEE 802.11d, IEEE 802.11e and IEEE 802.11g. After that we have also seen that IEEE 802.15 works on Bluetooth, Wireless Personal Area Network (WPAN), etc.

will learn in the forthcoming semesters.

3.8 FURTHER READING

1. Computer networks by Tanenbaum, 5th edition.
2. Bluetooth standards and ZigBee : (https://www.cse.wustl.edu/~jain/cse574-06/ftp/wpans/index.html - :~:text=1%20(Bluetooth)-,802.15.,to%20other%20IEEE%20networking%20stacks.)

3.9 CHECK YOUR PROGRESS

1. Fill in the blanks.

a. Bluetooth is _____ technology that connected devices in small area.

b. The size of the DSAP address in LLC PDU header is_____bits.

c. The size of the SSAP address in LLC PDU header is _____bits.

d. The RF band for802.11g is_____GHz.

e. The MAC address is_____byte long.

f. 802.15 is for_Area Network.

g. 802.2 is for__Area Network.

h. 802.11 is for_Area Network.

i. MAC stands for _____

j. PDU stands for _____

k. LLC stands for _____

2. Multiple choice questions

1. The wireless LAN specification is defined by IEEE, called, _____ which covers the data link and physical layer.

A. IEEE 802.2

B. IEEE 802.11

C. IEEE 802.3

D. IEEE 802.5

2. Bluetooth is a _____ technology that connected devices in a small area.

A. VLAN

B. Wireless LAN

C. Wired LSN

D. None of the above

3. Token Ring is a data link technology for?

A. WAN

B. MAN

C. LAN

D. Both A and B

4. _____ is the most widely used local area network protocol.

A. Token Ring

B. Token Bus

C. Ethernet

D. None of the above

5. Protocol Data Unit is similar to _____

A. LLC

B. HDLC

C. MAC

D. DSAP

6. IEEE standard was adopted by the

A. ISO

B. ANSI

C. OSI

D.IEEE

7. IEEE 802.11 have three categories of

A. Frames

B. Fields

C. Signals

D. Sequences

3. Match the pairs.

A	B
802.3	Wireless Personal Area Network
802.11	Logical Link Control Sub layer
802.15	Wireless Local Area Network
802.2	Medium Access Control Sub layer

3.10 ASSIGNMENT

1. Write note on IEEE 802.2 LLC Header in detail.
2. Write note on IEEE 802.2.
3. Write note on IEEE 802.3
4. Write note on IEEE 802.11
5. Write note on IEEE 802.15
6. Write in brief: LAN, WAN, PAN

BLOCK – 3

Transmission Media and TCP/IP

Unit 1: Transmission Media 1

Unit Structure

1.1 LEARNIG OBJECTIVES

After studying this unit student should be able to understand following:

- Transmission media and its types.
- Factors and causes of transmission media.
- Electromagnetic interference and its detail.
- Concepts of broadband, baseband and their differences.
- Classification of transmission media.

1.2 INTRODUCTION

Friends, in previous block we have gain the knowledge of networking standards, organization and rules regarding communication process. We have also discussed OSI reference model and protocol suits of IEEE family.

Now, it's a time to proceed further that what particular media are needed for communication, what are the factors that affects network communication and so and so forth.

So, in this particular unit we are going to discuss the basics of transmission media, basic terminology regarding media and factors responsible for transmission impairment too.

So, let's start.

As we know, transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted via this channel through electromagnetic signals. At this stage, we need to focus on two things one is format of the data and forms of the data. The format of the data is of different types and form can be wired or wireless. Following points will make you more clear regarding transmission media:

- It is a path between transmitters and receiver.
- Its main functionality is to carry the information in the form of bits using LAN (Local Area Network).
- In a copper-based network, the bits will in the form of electrical signals.

- In a fibre based network, the bits will be in the form of light pulses.

Now, if we talk about OSI, then transmission media supports the Layer 1 i.e physical lay er and hence it is considered to be a component of first layer.

Another thing is that the electrical signals can be sent through the copper wire, fibre optics, atmosphere, water, and vacuum. So, we need to discuss the factors affecting these types of physical channel. Properties of such different kinds of physical channels determine the performance of the network. Performance factors like throughput, latency and error rate will be discussed in later units.

In network transmission the most important characteristics is quality of data transmission and quality depends on characteristics of medium and signal both.

So, let's see the types of transmission media. There are two types:

- Wired (Guided) media
    - In this media, medium characteristics are most important.
    - Coaxial cable, twisted pair, fibre optics are the example of such media which we will discuss it further sections.
- Wireless (Unguided) media
    - In this media signal characteristics are most important.

Moreover, different transmission media have various properties such as bandwidth, delay, cost and ease of installation and maintenance. It has lot of other factors that affects impairment of transmission. So, let's hope that you all are clear regarding basics of transmission media and now in further section we will discuss factors responsible for designing transmission media and transmission impairment.

1.3 CHARACTERISTICS OF TRANSMISSION MEDIA

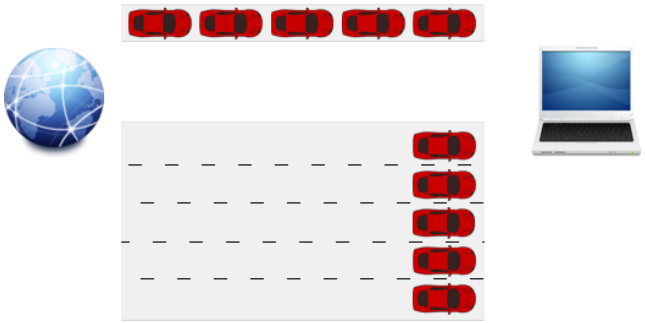
Every transmission media has their specific quality to deal with data transmission and its services. Which media to use and where to use and when to use is depend on the characteristics of particular media.

Following are the characteristics of transmission media

- Cost
    - There are two types of cost involved:

        - Installation Cost
            - This cost deals with installation of supportive devices which are used in the transmission process.
        - Maintenance cost
            - After installation we need to maintain the transmission. For example user wants change the bandwidth or wants to increase or decrease a length a cable etc.....
            - So this cost deals with such factors of maintenance activities.
- Installation Requirements
    - In wired (Guided) transmission, installation requirement is very complex.
    - In wireless (unguided) transmission, installation requirement is less complex.
- Bandwidth
    - The maximum amount of data transmitted over a network in a given amount of time is known as bandwidth.
    - It is also considered as data transfer capacity of particular device also.
    - A medium with high limit has a high data transfer capacity, while a medium that has constrained limit has a low transmission capacity.
    - Data transmission rates are expressed as far as the bits transmitted per second.
    - An Ethernet LAN theoretically can transfer 10 Mbps million bits (megabits for every second)
    - For Example:
        - Consider data transfer capacity like a road. All autos (information) travel at a similar speed, so to get more information from the web to your PC quicker, the roads should be wider.

- As it were, state 1 Mbps is the comparable to a one path road. What's more, suppose that you were expect to download a picture, which is 5 Mb in size. So on the off chance that you had a bandwidth of 1 Mbps (1 lane road) it would take you approximately 5 seconds to download the picture.
- Presently suppose that you have a 5 Mbps connection, or a 5 lane roads. How quick will you get your picture? Answer is one second.



(Image Source: https://images.squarespace cdn.com/content/v1/59053091d482e95dce661d89/1499509725149-1VDQEYW21JAR0MTOUVG8/bandwidth.png?format=750w)

- Transmission capacity can be communicated in any unit like bytes, kilobytes, megabytes, gigabits, and so on.

- Band Usage
  - We need to set the limit of the transmission and for that there are two famous terminologies are there:
    - Baseband
    - Broadband
  - Baseband is the most well-known method. Most LANs work in baseband mode, for instance, baseband signalling can be adapted with both analog and discrete signals.

- We are experiencing examples of broadband transmissions in our day to day life.
    - For example, the television cable coming in our home from a radio wire or a cable supplier is a broadband medium. Numerous TV signals can share the data transfer capacity of the link in signal of the fact that each signal is modulated utilizing an independently appointed frequency. We can utilize the TV tuner to pick the channel you need to watch by choosing its frequency.
    - Baseband defines the whole limit of the medium to one correspondence channel. Broadband allows at least two correspondence channels to share the transfer speed of the communications medium.

- Attenuation
    - A loss of signal strength in network cable or connections is known as attenuation.
    - It is a proportion of how much communicating signals weakens when it passes through a medium.
    - Attenuation is measured in unit called decibels (dB) or voltage.
    - Attenuation can occur due to variety of factors. For example, when our wireless device, say mobile is connected to router, a signal may weaken due to many reasons.
    - In wired medium, more effective cable strength is decided the greater signal strength. There is a device called amplifier and repeater that are used to increase the signal strength. The signal speed can weaken if we add more such components.
- Electromagnetic Interference
    - It is the disruption of operation an electronic device.
    - It includes outside electromagnetic noise that distorts the signal in a medium. For example, internal circuits of our personal computer can generate EMI.

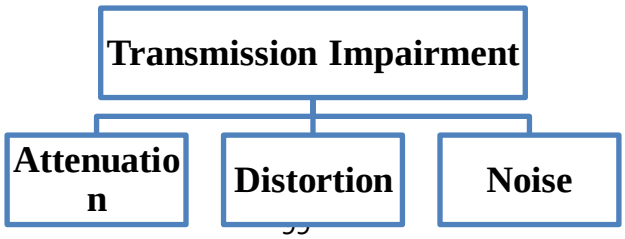
- EMI is the electrical noise induced in cabling by the presence of nearby electrical equipment such as motors, air conditioners, fluorescent lights, and power lines etc.

- One can avoid EMI by using following guidelines:
  - ✓ Avoiding bunching of unshielded cabling
  - ✓ Keeping all cabling away from power cords and transformers
  - ✓ Using shielded twisted-pair (STP) cabling instead of unshielded twisted-pair (UTP) cabling
  - ✓ Enclosing cabling in external mesh or wire shielding
  - ✓ Properly grounding electrical equipment and external shielding
  - ✓ Taking care not to excessively untwist the terminating ends of twisted-pair cabling
- Crosstalk is one common example of EMI. Crosstalk occurs when signal transmitted in one copper twisted pair radiated and cause interference the communication and degrade the performance of the transmission

So, above are all the characteristics which are required for smooth transmission media communication. In next section, we are going to talk about disturbance that can happen in transmission.

1.4 CAUSES OF TRANSMISSION IMPAIRMENT

When we talk about transmission impairment, it is nothing but the parameters of disturbance that can disrupt the transmission. There are three main impairments as shown below:



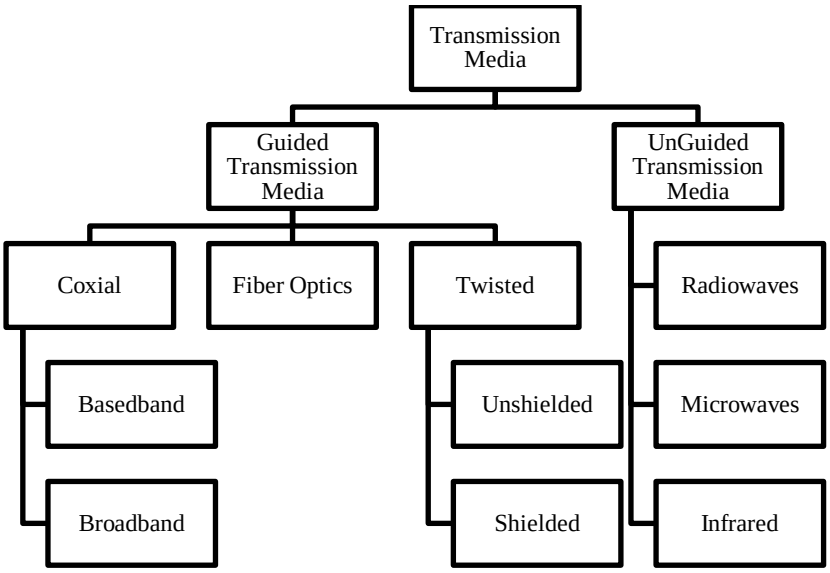
- **Attenuation:** As we have seen it earlier also attenuation means the loss of energy, for Example, the strength of the signal reduces with increasing the distance which causes the loss of energy.
- **Distortion:** When there is a change in the shape of the signal, Distortion occurs. This type of distortion is examined on basis of different signals having different frequencies. Each frequency component has its own propagation speed, so they reach at a different time which leads to the delay distortion.
- **Noise:** When data is travelled over a transmission medium, some unwanted signal is added to it which creates the noise.

Hence, for smooth transmission we should minimize the above impairment as much as possible.

Now, at the end of unit we need to discuss the types of transmission media and its detail. In later units we will cover it in more detail.

1.5 CLASSIFICATION OF TRANSMISSION MEDIA

Following figure depicts the overall classification of transmission media.



Mainly, there are two types of transmission media:

- **Guided:**
  - It is also known as wired media.

- Transmission limit depends fundamentally on the types of medium and its length.
- Coaxial cables, twisted pair, Fibre Optics are the well-known examples of it.
- In such media, transmission of data will be faster than wireless media but when we think of larger range, transmission is little complex in guided medium.

- **Unguided:**
  - Unguided media is also known as wireless media.
  - In such media signal attributes are more significant.
  - In this media, transmission of data is slower comparative to guided media but for larger range unguided media is much preferable.
  - They are in the form of infrared, radio waves and microwave forms.

Now, let's have some more discussion on differences between Guided and Unguided Media.

The key difference between both media is that guided media uses a physical path or conductor to transmit the signals or in simple language we can say it uses wired path where the unguided media broadcast the signal through the air or we can say that it is wireless.

Guided media has physical path so it may provide direction to the signal whereas, the unguided media does not direct the signal because it is wireless.

Guided media is used to establish point to point communication whereas unguided media is used to establish communication using broadcasting in all direction.

Moreover, there are two types of twisted pair one is unshielded twisted pair (UTP) and another is shielded twisted pair (STP). We will cover it in detail in the next sections.

Coaxial cable is used in two types of communications: (1) baseband (2) broadband. In earlier section itself we have discussed the basics now let's summaries the differences between these two:

- Baseband works on digital signaling where as broadband works on analog signaling.

- Baseband transmission is bidirectional where broadband transmit data in one direction.
- Baseband are basically used to transmit data on a short distance while broadband singles can travel on long distance.
- Baseband transmission is cheaper to design compared to broadband.

1.6 LET US SUM UP

Transmission media are situated at the physical layer. We can send Signals in form of electromagnetic energy. There are two types of transmission media are being classified as: Guided and Unguided. Bandwidth refers to the data carrying capacity of a channel or medium. Higher bandwidth communication channels support higher data rates. Broadband and baseband are the terminology used to data communication over network. In baseband LAN, the data rates lies in the range of 1 KHz to 20 MHz over a distance in the range of 1 Km. Attenuation refers to loss of energy as signal propagates outwards. The amount of energy lost depends on frequency. Radiations and physical characteristics of media contribute to attenuation. Crosstalk refers to the picking up of electromagnetic signals from other adjacent wires by electromagnetic induction.

1.7 CHECK YOUR PROGRESS

1. Transmission Media supports which level of OSI Model?
2. OSI stands For _____.
3. LAN Stands for _____.
4. What is transmission media? How many types of it?
5. 5MBps = _____ Kbps.
6. What is Bandwidth?
7. Give one example of broadband signal.
8. _____ refers to the loss of signal in communication process.

9. Give minimum four real-time examples of Electromagnetic interference (EMI).
10. Hertz (Hz) is the unit of _____.

1.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

A.1. Physical Layer

A.2. Open System Interconnection

A.3. Local Area Networks

A.4. Transmission media is a physical path between sender and receiver that can be classified in two types:

Guided: Transmission limit depends fundamentally on the medium, its length etc. Coaxial cable, twisted pair, Fibre Optics is the examples of it.

Unguided (Often known as wireless): Transmitting electromagnetic waves yet do not control them.

A.5. 5MBps = 5*8 Mbps=40 Mbps =40*1024 Kbps = 40,960 Kbps

A.6. Satellite, Wi-Fi, Digital Subscriber line (DSL)

A.7.A baseband signal or low pass signal is a signal that can include frequencies that are very near zero, by comparison with its highest frequency.

A.8. Attenuation

A.9. Self-Study

A.10. Frequency

1.9 FURTHER READING

- ForouzanBehrouzA," Data Communications and Networking", McGrawHill,New York.
- TANENBAUM | WETHERALL, " Computer Networks ",Pearson

1.10 ASSIGNMENT

- Explain the characteristics of different transmission media in detail.

- Differentiate Guided transmission media and Unguided transmission media.
- Define and differentiate baseband and broadband communication with example.

1.11 ACTIVITIES

- Make a chart of different guided and unguided transmission media on the basis of its characteristics.
- Create a sheet which shows the comparison between bit, byte, KB, MB, TB

Unit 2: Cable Media 2

Unit Structure

2.1 LEARNIG OBJECTIVES

In this unit student will able to:

- Understand what guided media is.
- Understand about different kinds of wired transmission media with their advantages and disadvantages

2.2 INTRODUCTION

Friends, in Unit 1 we have seen the basics of transmission and its characteristics. We have also discussion the types of transmission media in brief and now it's a time that we understand each and every media in detail.

So, in this particular unit we are going to discuss the guided media which is also termed as cable media or wired media. So let's

As we know, the purpose of the physical layer is to send and receive bits/bytes from one machine to another. Each kind of Transmission media has its own properties in terms of bandwidth, delay, cost, and ease of installation and maintenance. Basically Transmission media can be classified in two parts:

1. Guided Transmission Media (Cable Transmission)
2. Unguided Transmission Media (Wireless Transmission)

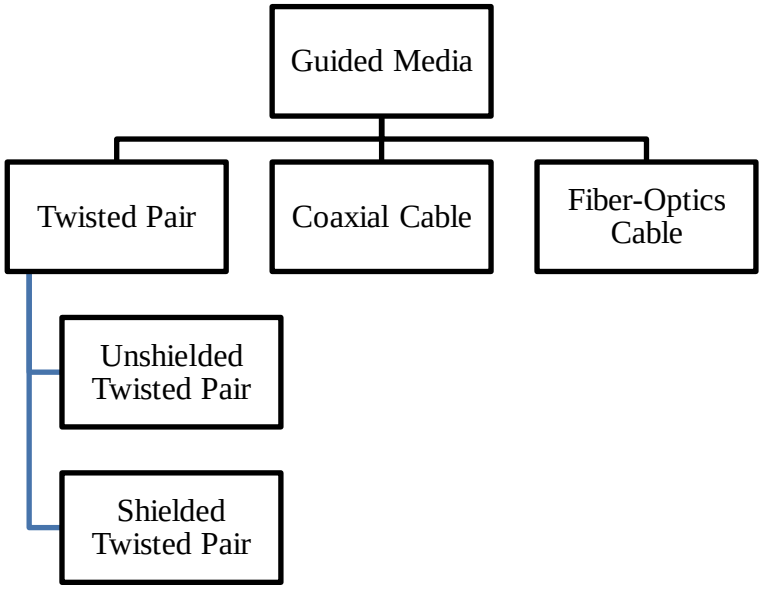
So, in this Unit we are going to study about Cable Transmission which means a Transmission media that transmits data on physical path. It is also known as wired transmission media. Guided media focuses on point to point or multipoint communication where medium, length of cable are important factors.

2.3 CLASSIFICATION OF GUIDED MEDIA

As shown in the below figure Guided media is divided into three basic types of cable which are:

1. Twisted Pair

2. Coaxial Cable
3. Fibre-Optics Cable



Further sections describe the types of each media in detail. So, Let's cover each media in detail.

2.4 TWISTED PAIR CABLE

Twisted pair is one of the most common and oldest transmission media. Twisted pair is made up of pair of cables which are twisted with each other and is considered as a physical media.

Here in this kind of cable both cable are two conductors (typically copper), each with its own plastic protection, wound together. Two insulated copper wires, typically about 1 mm thick are contained by twisted pair.

Twisting is done because two parallel wires constitute a fine antenna. It is a light weight cable, installation of which is easy.

For twisted pair the frequency ranges from 0 to 3.5 KHz.

Twisted pairs can be used for transmitting either analog or digital information. The bandwidth depends on the thickness of the wire and the distance travelled, but several megabits/sec can be achieved for a few kilometres in many cases. Due to their adequate performance and low cost, twisted pairs are widely used and are likely to remain so for years to come.

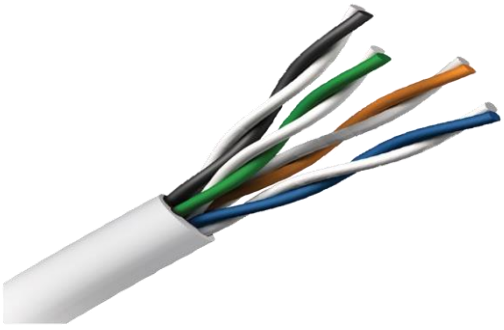
Here Copper wires are known as bare wire which will be twisted and come with insulation. This twisted pair will also have cover which is known as Jacket. The types of twisted pair cables are:

- Unshielded Twisted Pair (UTP)
- Shielded Twisted Pair (STP)

Let's have small introduction about both Unshielded and Shielded cable.

2.4.1 Unshielded Twisted Pair (UTP)

- UTP consists of two insulated copper wires twisted around one another.
- It is the most common type of telecommunication; while STP cable consists of two conductors usually copper, each with its own colour plastic insulator. Coloured plastic insulation is used for identification purpose.
- UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use RJ-11 connector and 4 pair cable use RJ-45 connector.
- Following figure shows the UTP:



(Image Source: https://www.pngegg.com/1abdbfc1-dd25-46ca-b124-5468798c0b43)

There are various categories of UTPs available for difference purposes, following table depicts the categories of UTPs:

Sr. No	Category	Description
1	**Category 1**	Category 1 is used for telephone lines that have low-speed data.
2	Category 2	It can support up to 4Mbps.
3	Category 3	It can support upto 16Mbps.
4	Category 4	It can support up to 20Mbps. Therefore, it can be used for long-distance communication.
5	Category 5	It can support up to 200Mbps.

So, this was the basics of UTP and we can use it according to our requirements. There are lot of advantages of UTP and many disadvantages also. Let's brief look into that.

Advantages of Unshielded Twisted Pair Cable:

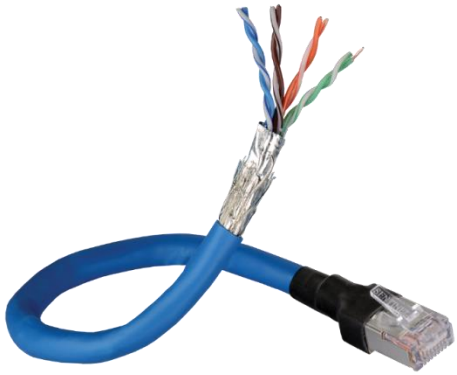
- ✓ When we talk about UTP cables, its installation is easy comparative to others.
- ✓ They are least expensive.
- ✓ It has high speed capacity.

Disadvantages of Unshielded Twisted Pair Cable:

- ✓ They are only used for shorter distances because of attenuation.
- ✓ It has Lower capacity and performance in comparison to STP.
- ✓ When compared with Coaxial cable, UTP cable is low in terms of Bandwidth.
- ✓ It provides less protection from interference.

2.4.2 Shielded Twisted Pair (STP)

In Shielded Twisted Pair (STP) type of cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference. Electromagnetic noise penetration is prevented by metal casing. Metal packaging improves the nature of link by keeping the infiltration of commotion or crosstalk. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.



(image source: https://www.pngwing.com/a73a692b-73e1-43ff-8d10-d03e2a45f4af)

Advantages of Shielded Twisted Pair:

- ✓ Installation of STP cables is easy.
- ✓ It can be used for both analog and digital transmission.
- ✓ It has high signalling rate.
- ✓ The capacity of STP is higher than UTP.
- ✓ Crosstalk is eliminated in STP.

Disadvantages of Shielded Twisted Pair Cable:

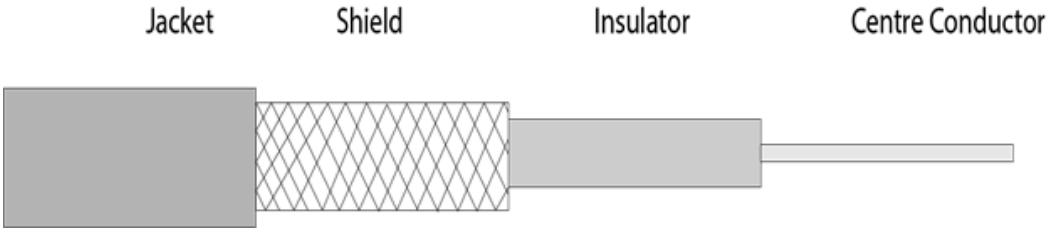
- ✓ Manufacturing Shielded Twisted Pair cables is difficult.
- ✓ STP cables are more expensive as compared to UTP and coaxial cable.

Application of Sheilded Transmission Media:

- ✓ STP are used in telephone lines to provide voice and data channels. The DSL lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of UTP cables.
- ✓ 10Base-T and 100Base-T are Local Area Networks, which use twisted-pair cables.

2.5 COAXIAL CABLE

The most commonly and widely used transmission media is coaxial cable, for example, TV wire. The name of the cable is coaxial as it contains two conductors parallel to each other.It has a higher frequency as compared to Twisted pair cable. Following figure shows the ideal coaxial cable.



(Image Source: https://static.javatpoint.com/tutorial/computernetwork/images/coaxial-cable.png)

Let's have look on coaxial cables structure. It cantains a copper cable as inner conductor, insulation on that copper cable, on insulation it will contain copper shield and on that shield one cover will be there which is known as jacket.

Copper is used to make inner conductor of the coaxial cable, and copper mesh is used to make the outer conductor. Non-conductive cover that separates the inner conductor from the outer conductor is used to make middle core of coaxial cable.

It has better shielding and greater bandwidth than unshielded twisted pairs, so it can span longer distances athigher speeds.

Two kinds of coaxial cable are widely used.

- 50-ohm cable:
    - It is commonly used when it is intended for digital transmission from thestart.
- 75-ohm cable: It is commonly used for analog transmission and cable television.

This distinction is based on historical, rather than technical factors. Starting in the mid1990s, cable TV operators began to provide Internet access over cable, which has made 75-ohm cable more important for data communication.

Let’s have look on where we can utilize Coaxial cables.

- They can be utilized over longer distance and support a bigger number of stations on a common line than twisted pair cable.
- They are utilized both for baseband and broadband communications.
- In baseband LAN, the information rates lies in the scope of 1 KHz to 20 MHz over a distance in the scope of 1 Km. For broadband this cables offer data rate of 300 to 400 MHz.

So, that was all about basics of coaxial cables. Now lets see the classification of coaxial cable according to goverment standards and ratings.

2.5.1. Standards

- Government (RG) ratings are used to classify Coaxial links.
- Every RG number includes an interesting arrangement of physical details, including the wire measure ofthe inner conductor,the thickness and the development of the shield, type of the inner insulator, and the size and sort of the external packaging.
- Each cable characterized by a RG rating is assigned a specific capacity.
- Following table describe each category, resitance and its uses.

Category	Resistance (ohm)	Use
RG-59	75	Cable Television
RG-58	50	Thin Ethernet
RG-11	50	Thick Ethernet

Now, let’s see the applications of coaxial cable.

2.5.2. Applications

Coaxial cable is a flexible transmission medium, utilized in a wide assortment of uses. The most vital of these are

- ✓ Television distribution
- ✓ Long-distance telephone transmission
- ✓ Short-run computer system links
- ✓ Local area networks

Coaxial link was broadly utilized in analog telephone systems where a solitary coaxial system could convey 10,000 voice signals. Later it was utilized in digital telephone systems where a solitary coaxial link could convey advanced information up to 600 Mbps.

Cable TV networks also utilize coaxial cables. In the conventional satellite TV organize, the whole system utilized coaxial cables.

Finally, at the end let's discuss advantages and disadvantages:

2.5.3. Advantages & Disadvantages

Advantages:

- The data can be transmitted at high speed.
- Greater channel capacity than twisted pair.
- Greater bandwidth compared to twisted pair.

Disadvantages:

- Installation is difficult
- Installation cost
- Great noise

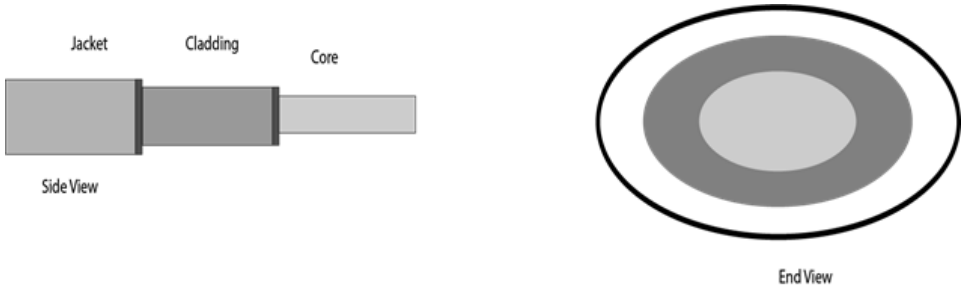
2.6 FIBRE OPTIC CABLE

Glass or plastic materials are used to make fibre-optic cables and it transmits signals in the form of light. They are also known as optical fibre cable.

It holds the optical fibres coated in plastic which are used to send the data by pulses of light. To protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring, plastic coating is used. Many elements are there in fibre optic cable, like core, cladding , jacket etc. Let's discuss it in detail.

2.6.1. Basic elements of Fibre optic cable:

Following figure shows the elements in fibre optic cable and its end view:



(Image source: https://static.javatpoint.com/tutorial/computer-network/images/fibre-optic-cable.png)

There are three basic elements of fibre optic cable:

- **Core:**
  - Narrow strand of glass or plastic known as a core of optical fibre.
  - It is a light transmission area of the fibre.
  - The more the space of the core, the lighter will be transmission.
- **Cladding:**
  - Cladding is the concentric layer of glass.
  - The main functionality of the cladding is to provide the lower refractive index at the core interface as to create the reflection within the core so that the light waves are transferred through the fibre.
- **Jacket:**
  - Jacket is the protective coating consisting of plastic.
  - The main idea of using a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

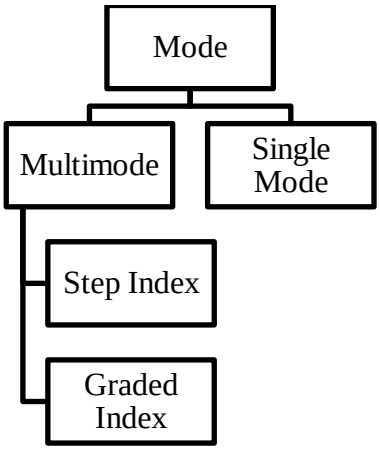
2.6.2. Advantages of fibre optic cable:

- **Greater Bandwidth:**
  - The fibre optic cable gives more bandwidth as compared copper. Therefore, the fibre optic transfers more data as compared to copper cable.
- **Faster speed:**
  - Fibre optic cable transfers the data in the form of light.
  - This makes it easier to carry the signals at a higher speed.
- **Longer distances:**
  - The fibre optic cable carries the data at a longer distance in comparison to copper cable.
- **Better reliability:**
  - The fibre optic cable is more dependable than the copper cable as it is safe from any temperature changes while it can cause obstruct in the connectivity of copper cable.

Other than above information, fiber optic cables can provide many forms of communication.

Let's briefly look into that.

2.6.3. Types of communication using fibre-optics



Basically fibre optics has two kinds of mode of communications which are based on Propagation. So let's understands propagation first.

Propagation is the manner in which radio signals travel from a transmitting media to a receiving media.

Fibre optics technology supports two modes

- Multimode Communication
  - It has large diameter core that allows multiple modes of light for propagation.
  - Due to this more light reflection will be created and so light passes through the core will increase.
  - So using this more data can be passed through fibre optic cable.
  - There are two types:
    - Step index multimode communication
    - Graded index multimode communication
- In multimode step-index fibre, the density of the core remains constant from the centre to the edges.
- The term step-index refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fibre.
- In multimode graded-index fibre, this distortion gets decreases through the cable. A graded-index fibre, therefore, is one with varying densities.
- Single mode :
  - It is a common type of fibre cable that is used to transmit over longer distance.
  - It is a single glass fibre, which is used to pass single ray of light.

2.6.4. Applications of Fibre Optic Cable

- Fibre optic cables are most useful in long-distance broadcast communications, as it has many advantages such as: small diameter, lighter weight, low attenuation, invulnerability to electromagnetic resistance and many more.

- Fibre-optic cable is often found in backbone networks because its wide bandwidth is effective in terms of cost.
- Some cable TV companies use a combination of optical fibre and coaxial cable which creating a hybrid network. Optical fibre provides the backbone structure while coaxial cable provides the connection to the user premises.
- Local-area networks such as 100Base-FX network (Fast Ethernet) and 1000Base-X also uses fibre-optic cable.

2.6.6. Advantages & Disadvantages

Now, let's conclude the fibre optic with its advantages and disadvantages.

Advantages:

- Higher Bandwidth
- Less Signal Attenuation
- Light weight
- Resistance to corrosive materials
- Immune to electromagnetic interference

Disadvantages

- Require expertise in installation & maintenance.
- Unidirectional in signal propagation.
- Cost

This was all about cable media being used for transmission of data in computer networks. Last topic compares and summarises all the media in tabular form.

2.7 COMPARISIONS

Sr. No.	Type	Sub Type	Segment Length	Bandwidth	Installation	Cost	Interference
1	Twisted Pair Cable	UTP	100meters	100Mbps	Easy	Cheapest	High
2		STP	100meters	500Mbps	Moderate	Moderate	Moderate
3	Coaxial Cable	Thick net	500meters	10Mbps	Hard	Moderate	Low
4		Thin net	185meters	10Mbps	Easy	Cheap	Moderate
5	Fibre Optics Cable	Multi node	2Kms	100Mbps	Very Hard	Expensive	None
6		Single node	100Kms	2Gbps	Very Hard	Expensive	None

2.8 LET US SUM UP

In category of guided media the communication device is used to communicate to each other directly with cables. Some kinds of guided media are coaxial cable, twisted pair wire and fibre optic cable. Twisted Pair Cable is the most widely recognized utilized correspondence media and utilized in LAN for exchange of information between different PCs. Coaxial Cables are called coax and convey signals with high frequencies. They are produced using a solitary copper wire. Fibre Optic Cable utilizes light to exchange information. The information is exchanged at an exceptionally rapid of billions bits/second. All the media has their own advantages and disadvantages based on their applications.

Now, it’s time to check your progress!

2.9 CHECK YOUR PROGRESS

1. How many types of Guided Media are there?
2. UTP stands for _____.
3. Fiber Optics Transmits data in form of ____.
4. STP stands for ___.
5. Bandwidth of coaxial cable is ____.

2.10 CHEK YOUR PROGRESS (ANSWERS)

A.1. There is three types of guided media.

Twisted Pair Cable – It is the most widely recognized utilized correspondence media and utilized in LAN for exchange of information between different PCs.

Coaxial Cable – They are otherwise called coax and convey signals with high frequencies. They are produced using a solitary copper wire.

Fibre Optic Cable – They utilize light to exchange information. The information is exchanged at an exceptionally rapid of billions bits/second.

A.2. Unshielded Twisted Pair.

A.3. Light

A.4. shielded Twisted Pair.

A.5. 10 MBPs.

2.11 FURTHER READING

- TANENBAUM | WETHERALL, " Computer Networks ",Pearson
- Gary A. Donahue, Network Warrior, 2nd Edition

2.12 ASSIGNMENT

1. Why are the wires twisted in twisted-pair copper wire?
2. What are some major limitations of twisted-pair wire?
3. What is the difference between unshielded twisted pair and shielded twisted pair?
4. Describe the components of optical fibre cable.
5. Discuss the advantage and disadvantages of optical fibre.
6. Compare and contrast all the media in brief.

2.13 ACTIVITIES

Prepare a chart on the basis of characteristics of each guided media.

Unit 3: Wireless Media 3

Unit Structure

3.1 LEARNING OBJECTIVES

After studying this unit student should be able to:

- Describe wireless communication methods.
- Describe the applications of wireless media.
- Describe the advantages and disadvantages of wireless communications.

3.2 INTRODUCTION

In previous unit, we have seen guided (cable) media and its types. There many advantages and disadvantages of guided media. Now it is a time that we explore unguided media, we call it wireless media. In Further section we will discuss wireless media in detail.

In wireless transmission media there is no physical association between source and goal, instead they utilize wireless median for the same. In such media, electromagnetic vitality is most important. In this transmission, it transmits the electromagnetic waves without utilizing any physical medium. Therefore it is also known as remote transmission.

Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them. For example, mobile and or any device which supports this media.

To understand wireless transmission in a better way we need to learn how the signal propagates and the propagation modes that available for transmission.

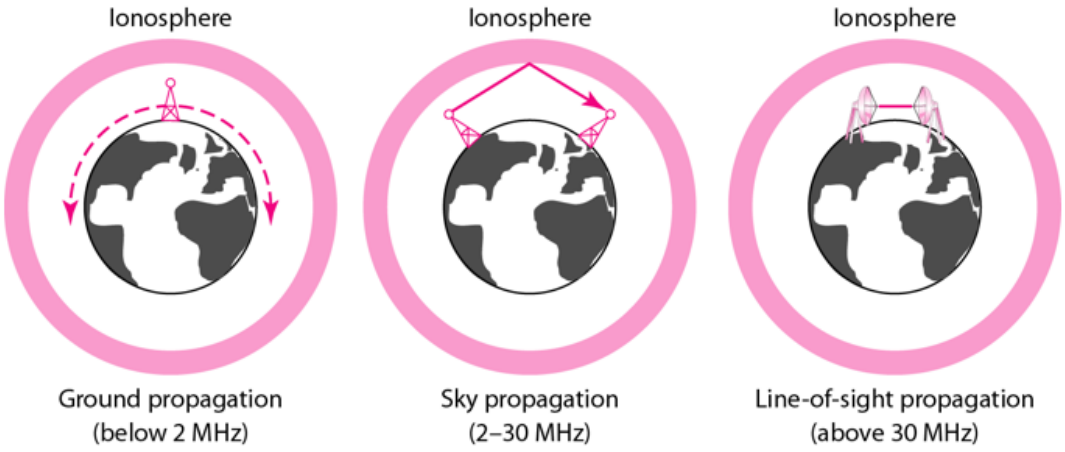
So, let’s discuss propagation modes in detail.

3.3 PROPOGATION MODES OF WIRELESS TRANSMISSION

Wireless signals can travel from the source to the goal via many ways and they are as follows:

- Ground propagation
- Sky propagation
- Line-of-sight propagation

Following figure shows the propagation modes of wireless media.



(Image Source: https://static.studytonight.com/computer-networks/images/unbounded-transmission-media-2.png)

Now, let's look all the three modes in detail.

Ground Propagation:

- In this, radio waves travel through the most reduced parcel of the climate, embracing the Soil.
- 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 emanate 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:

- Very high-frequency signals are transmitted in form of straight lines directly from antenna to antenna in such propagation.

In short, wireless signal propagates through ground, sky or line of sight having different – different frequencies. We will learn about this in more detail in forthcoming semesters.

As we know there are many disadvantages of wired media and as demand of wireless communication increasing, it is a right time to discuss the need of wireless networks.
Next we'll discuss the reasons for wireless networks.

3.4 REASON OF WIRELESS NETWORK

Friends, as we all know world is leading towards wireless networks and most of the smart devices needs to be controlled using wireless media, it is necessary to discuss that what are reasons that we need wireless network.
So, following are the points that we need to look into:

- **Increased Mobility:**
  - Wireless networks allow mobile users to access real-time information so they can roam around their own space without getting disconnected from the network.
  - So, without worrying about wired network, user can mobilised himself free all over the network.
- **Installation Speed and Simplicity:**
  - Installing a wireless network system reduces cableling.
  - It can also be installed quickly and easily compared to a traditional network.
  - Even troubleshooting is somewhat easy in such transmission than wired network.
- **Wider reach:**
  - Such network can be extended to places in our organization whenever we want with very less technical and human effort.
  - So in wireless media one can have larger audience and hence wider reach.
- **More Flexibility:**
  - Such networks are flexible enough to change and upgrade with new configurations.

    - Just by upgrading wireless configuration one can switch to the newer version easily. That's it!
- **Reduced cost of ownership:**
    - Initially, it seems that cost of installing wireless systems is high, but after some time the general cost of ownership will be low compared to traditional networks.
- **Increased Scalability:**
    - Wireless systems can be easily scaled to the new application with different organization's need.
    - Changes and up-gradation are simple and straight-forward in wireless systems.

So, above are the reasons for using wireless network. Now it is a time to look into various wireless media. Let's begin with basic types!

3.5 TYPES OF WIRELESS TRANSMISSION

Wireless transmission can be divided into three types as follows:

- **Radio waves:**
    - Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- **Micro waves:**
    - Microwave transmission is a technology that transmits the focused beam of a radio signal.
- **Infrared waves:**
    - It is a technology used for communication over shorter ranges.

So let's discuss each of these media one by one.

3.6 RADIO WAVES

Radio waves are the electromagnetic waves that are transmitted in all the bearings of free space. Radio waves are omni directional, i.e., the signals are propagated in all the directions. We can extend frequencies of radio waves from 3 KHz to 1 kHz.

In radio waves the sending and accepting antenna is not adjusted, i.e., the wave sent by the sending antenna can be received by any accepting antenna. FM radio is the best example of radio waves.

Radio waves transmit data in form of low and medium frequencies. It can penetrate into walls also. This characteristic can be both an advantage and disadvantage as well. An AM radio can receive signals inside a building that can be advantage and we cannot isolate a communication to just inside or outside a building is a disadvantage.

Radio waves are frequency dependent. At low frequencies, they pass through obstacles but the power falls off sharply with distance from the source. At high frequencies, radio waves tend to travel in straight lines and bounce off obstacles. High-frequency radio waves are also absorbed by rain and other obstacles to a larger extent than low-frequency ones. Radio waves are subject to interference from motors and other electrical equipment at both low and high frequencies.

Applications of Radio Waves:

- The Omni-directional characteristics of radio waves make them valuable for multicasting in which there's one sender but many receivers.
- AM and FM radio, TV, oceanic radio, cordless phones, and paging are multicasting devices.

Advantages of Radio transmission:

- Radio transmission is primarily utilized for wide region systems and mobile cellular phones.
- Radio waves cover a wide range and they can enter into the walls.
- Radio transmission gives a better transmission rate.

3.7 MICRO WAVES

Electromagnetic waves having frequencies between 300MHz and 300 GHz are called smaller scale or microwaves. The wavelength of microwave is ranging from 1mm to 1 meter. They are unidirectional in nature. The unidirectional property has an obvious advantage. A match of antennas can be adjusted without interfering with another pair of adjusted antennas. When an antenna transmits microwaves they can be nearly centred. This implies that the sending and accepting radio wires need to be adjusted.

Microwave antennas concentrate the waves making a bar of it. Different antennas can be adjusted to reach more distant. Microwaves have higher frequencies and don't enter divider like obstacles. Microwave transmission depends exceedingly upon the climate conditions and the frequency it is utilize.

Microwaves are of two types:

- Terrestrial microwave
- Satellite microwave communication

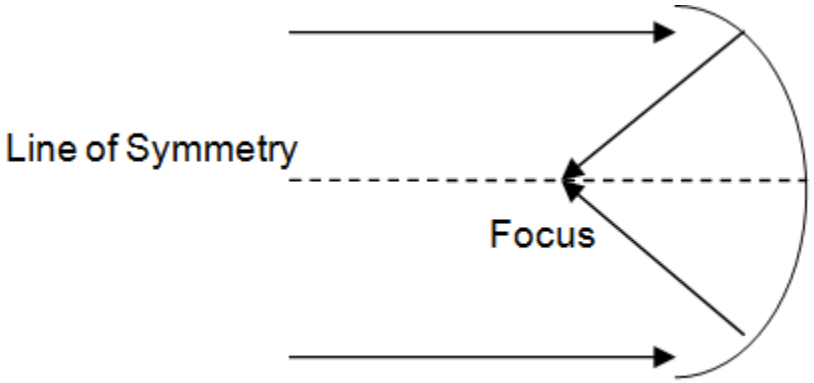
3.7.1 Terrestrial Microwave Transmission

A which transmits the centred beam of a radio signal from one ground-based microwave transmission antenna to another is known as terrestrial microwave transmission. In this transmission, directional parabolic antenna is used receive and transmit signal in lower gigahertz range. Such signals are highly focused.

There are two types of antennas used for terrestrial microwave communication:

- **Parabolic Dish Antenna**

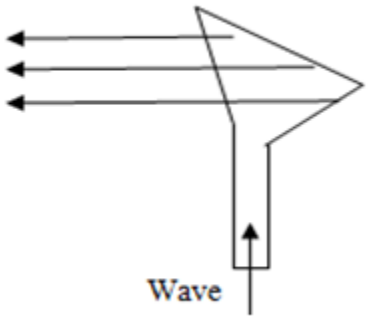
  In this type of antenna every line parallel to the line of symmetry reflects off the curve at angles in a way that they intersect at a common point called focus. This antenna is based on geometry of parabola.



(Image source:https://static.studytonight.com/computer-networks/images/Figure20.png)

- **Horn Antenna**

  It is a like a gigantic scoop. The outgoing transmissions are broadcast up a stem and deflected outward in a series of narrow parallel beams by curved head.



(Image Source:https://static.studytonight.com/computer-networks/images/Figure21.png)

Above are the basic phenomena of terrestrial microwave transmission. Let's see some of the characteristics of the same.

Characteristics of Terrestrial Microwave:

- **Frequency range:**
  - The frequency range is from 4-6 GHz to 21-23 GHz.
- **Bandwidth:**

- It supports the bandwidth from 1 to 10 Mbps.

- **Short distance:**
  - It is inexpensive for short distance.
- **Long distance:**
  - It is expensive as it requires a higher tower for a longer distance.

Advantages of Terrestrial Microwave:

- It is cheaper than using cables.
- It is free from land acquisition as it does not require any land for the installation of cables.
- It provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task.
- Communication over oceans can be achieved using such transmission.

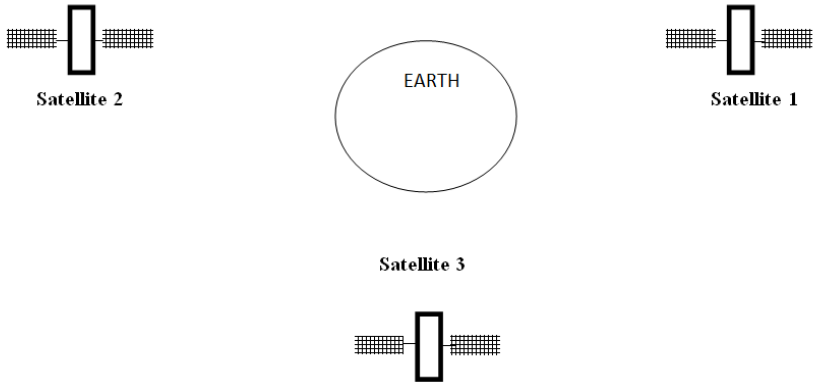
Disadvantages of Terrestrial Microwave transmission:

- Eavesdropping:
  - It is kind of activity in which secret listening makes uncertain communication. Any malicious client can passively listens to the network communications to gain access of private information.
- Out of stage signal:
  - A signal can be moved out of phase by utilizing microwave transmission.
- Susceptible to climate condition:
  - A microwave transmission is helpless to climate condition. It implies that any natural condition such as rain, wind can disturb the signal.
- Bandwidth constrained:
  - Assignment of bandwidth is restricted within the case of microwave transmission.

3.7.2 Satellite Microwave Communication

A satellite is a physical object that revolves around the earth at a known height. Satellite communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems. We can communicate with any point on the globe by using satellite communication.

It 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 stationery relative to earth and always stays over the same point on the ground. This is usually done to allow ground stations to aim antenna at a fixed point in the sky.



(Image Source:https://static.studytonight.com/computer-networks/images/Figure22.png)

The satellite acknowledges the signal that's transmitted from the earth station, and it increases the signal. The increased signal is retransmitted to another earth station.

Advantages of Satellite Microwave Communication:

- The coverage area of a satellite transmission is more than the terrestrial transmission.
- The transmission cost of the satellite is independent of the distance from the centre of the coverage area.
- It is used in mobile and wireless communication applications.
- It is easy to install.
- It is used in a wide variety of applications such as weather forecasting, radio/TV signal broadcasting, mobile communication, etc.

Disadvantages of Satellite Microwave Communication:

- Satellite designing and development requires more time and higher cost.
- The satellite needs to be monitored and controlled on regular periods so that it remains in orbit.
- The life of the satellite is about 12-15 years. Due to this reason, another launch of the satellite has to be planned before it becomes non-functional.

So, above was the brief discussion about microwave transmission. Let's see the basics of infrared waves now.

3.8 INFRARED WAVES

An infrared transmission is a wireless technology utilized for communication over short ranges. The frequency of the infrared is within the range from 300 GHz to 400 THz. It is utilized for shorter range communication such as information exchange between two cell phones, TV remote operation, information exchange between a computer and cell phone resides within the same closed area. These waves cannot penetrate into the walls. These waves are longer than visible light and shorter than radio waves.

3.8.1. Applications of Infrared Waves

- As these waves have higher frequency up to 400 THz, so it can be used to transmit data with a very high data rate.
- These signals can be used for short range communication in a closed area.
- It is also used in thermal imaging cameras which detect people in dark.

So, we have completed the types of waves which support the different categories of wireless communication. Earlier we have seen the IEEE standard thatsupports wireless communication. So, now it's time that we briefly discuss how wireless communication is performed on LANs.

3.9 WIRELESS COMMUNICATION WITH LANs

Wireless LAN (WLAN) is a wireless computer network that links two or more devices using wireless transmission to form LAN. It is used within a limited area such as home, campus or office building, etc. WLANs allow users to move around in a confined area while they are still connected to the network. In some instance wireless LAN technology is used to save costs and avoid laying cable.

As we have seen earlier units also, wireless LANs is based on IEEE 802.11 standards. There WLANs are also known as Wi-Fi. Wireless router is used to provide the connectivity to the devices.

There are two ways of WLAN set up:

- Infrastructure mode:
  - A home or office network set up is an example of such mode. In this end points are connected and communicated with each through a common base station, which provides internet access. Router can act as base station.
- Ad hoc mode:
  - A WLAN which we can set up without using base station is called ad hoc mode. It is easy to set up and can provide basic peer-to-peer communication.

3.9.1 Advantages of WLANs

- Device Flexibility:
  - WLAN supports use of wide range of devices like mobile, computers, laptops, tablet etc.
- Planning:
  - Only wireless ad-hoc networks allow for communication without any previous planning and any wired network needs wiring plans.
- Design:

- Wireless systems permit for the plan of independent, small devices which can for case be put into a pocket.

- Scalability:
  - WLANs are scalable. Adding users is as simple as given new login credentials only.
- Extended Reach:
  - WLAN can be extended to perform computing anywhere.

3.10 LET US SUM UP

Wireless communication includes the transmission of data over a separation without the assistance of wires, links or some other types of electrical conductors. Wireless communication is an expansive term that joins all systems and types of associating and conveying between at least two devices utilizing a remote signal through wireless communication advances and devices.

We have seen many types of transmission waves such as infrared, microwave, and radio. Each transmission has its own advantages and disadvantages. At last we have seen WLAN which is supported by IEEE 802.11 standards. There are many advantages of WLANs also such as flexibility, scalability etc.

3.11 FURTHER READING

- TANENBAUM | WETHERALL, " Computer Networks ",Pearson
- T. Imielinski and B. R. Badrinath, Wireless Mobile Computing: Solutions and Challenges in Data Management, Communications of the ACM, 1994.
- J. B. Andersen, T. S. Rappaport, S. Yoshida, Propagation Measurements and Models for Wireless Communications Channels, IEEE Communications Magazine, (January 1995), pp. 42-49

3.12 ASSIGNMENT

1. Why are the types of wireless media?
2. Define and differentiate infrared, radio wave and microwave transmission.
3. What is Terrestrial Microwave?
4. Describe WLAN.
5. Discuss the advantages of WLANs.

Unit 4: TCP/IP 4

Unit Structure

4.1 LEARNING OBJECTIVES

After studying this unit student should be able to:

- Explain TCP/IP protocols, ports, sockets, and data encapsulation
- Describe the process of packet fragmentation and reassembly
- Explain the key features and functions of TCP and UDP

4.2 INTRODUCTION TO TCP/IP

Till now, we have seen the basics of transmission, types of transmission and its pros and cons. Now it is a time that we learn about set of rules or protocol that are vital for communication over computer network. TCP/IP is one such protocol suite or we can say a model which is used for setting communication standards. So, in this unit we will learn about TCP/IP in detail. So, let's start.

TCP stands for Transmission Control Protocol and IP stands for Internet Protocol. It is a suite of protocols utilized for the communication of devices over a network. The network can be of any type such as Internet intranet, extranet or any personal network.

We are well aware about OSI layer. The TCP/IP suite is also a model which was created earlier to the OSI model. The TCP/IP model comprises of five layers: the application layer, transport layer, network layer, data link layer and physical layer.

The first four layers provide physical standards, network interface, internetworking and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.

TCP/IP is a hierarchical protocol made up of interactive modules and each of them gives particular functionality. The objective is to gather an interconnection of systems and perform common correspondence over heterogeneous physical frameworks. To perform a communication each host or a computer is allocated a location and that location has specific address we call it an IP address. We can say that an IP address is a unique address that identifies a device over internet or a network. IP is set of rules

which govern the format of data sent via network. Hence, IP address is a numeric label which is managed by Internet Protocol for communication. So, it is necessary for us to know the structure of IP address.

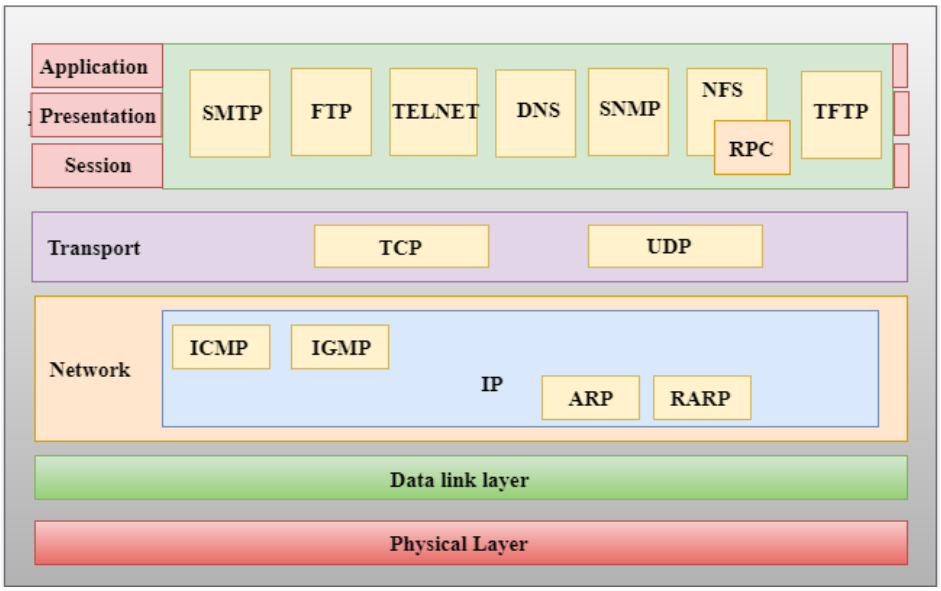
IP address comprises of two sections: (i) Network Number (ii) Host Number

The network number of an IP address identifies the system within the web and is assigned by an expert lead and is new throughout the web. The host number belongs to the system control association distinguished by the network number.

In forthcoming sections we will have more discussion on IP address but before that we need to understand the layers of TCP/IP protocol suit and how the communication is establish between the layers.

4.3 TCP/IP LAYERS

The following figure shows different layers of TCP/IP model. Mainly, we are going to focus on network layer, internet layer, transport layer and application layer.



4.3.1. Network Layer

The network layer is the lowest layer of the TCP/IP model. It is a combination of the physical layer and the data link layer defined in the OSI reference model. It defines how data should be physically sent over the network.

This layer is mainly responsible for the transmission of data between two devices in the same network. The functions performed by this layer are to encapsulate IP data in frames transmitted by the network and map IP addresses to physical addresses.

The protocols used by this layer are Ethernet, token ring, FDDI, X.25, frame relay. We will learn about these protocols in more details in forthcoming semesters.

4.3.2 Internet Layer

The Internet layer is the second layer of the TCP/IP model. The main responsibility of the Internet layer is to send packets from any network and they reach their destination no matter what path they take. Here are the protocols used in this layer:

- IP Protocol
- ARP Protocol
- ICMP Protocol

Let's discuss all the protocols in brief.

IP protocol is used in this layer and it is the most important part of the whole TCP/IP suite.

Following are the responsibilities of IP protocol:

- IP Addressing:
    - This protocol implements logical host addresses known as IP addresses. IP addresses are used by the Internet and higher layers to identify devices and provide routing of internet connections.
- Host-to-host communication:
    - It defines the path through which the data will be transmitted.
- Data Encapsulation and Formatting:
    - The IP protocol accepts transport layer protocol data. The IP protocol ensures that data is sent and received securely; it encapsulates the data in a message known as an IP datagram.

- Fragmentation and Reassembly:
    - The limit imposed on the size of the IP scheme by the data link layer protocol is called the maximum transport unit (MTU). If the size of the IP datagram is larger than the MTU, the IP protocol divides the datagram into smaller units so that they can travel across the local network.
    - Fragmentation can be done by the sender or the intermediate router. On the receiver side, all the fragments are assembled to form an original message.
- Routing:
    - When IP datagram is sent over the same local area network as LAN, MAN, WAN, it is called drop delivery. When the source and destination are on the remote network, the IP datagram is sent indirectly. This can be done by routing the IP data scheme through different devices such as routers.

Next is ARP Protocol. ARP stands for Address Resolution Protocol. It is a network layer protocol used to find physical addresses from IP Address. There are two terms which are mainly related to the ARP protocol:

- ARP request:
    - When the sender wants to know the physical address of the device it broadcasts an ARP request on the network.
- ARP reply:
    - Any device connected to the network will accept the ARP request and process the request, but only the receiver recognizes the IP address and returns its actual address as an ARP response. The receiver adds the physical address to both its cache and in the datagram's header

Next is IMCP Protocol where ICMP stands for Internet Control Message Protocol. It is a mechanism used by servers or routers to send notifications of datagram to the sender.

A datagram travels from router to router until it reaches its destination. If a router is unable to forward data due to some abnormal conditions such as broken link, device fire

or network congestion, ICMP is used to notify the sender that the data packet cannot be delivered.

An ICMP protocol mainly uses two terms:

- ICMP Check:
    - ICMP check is used to check if the destination is reachable or not.
    - ICMP response: The ICMP response is used to check if the target device is responding.

The main responsibility of the ICMP protocol is to report problems, not to fix them. The responsibility for the repair rests with the sender.

ICMP can only send messages to the source but not to intermediate routers because the IP datagram carries the addresses of the source and destination and not the router to which it was transmitted.

4.3.3. Transport Layer

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

The two protocols used in the transport layer are User Datagram protocol and Transmission control protocol.

- **User Datagram Protocol (UDP)**
    - It provides end-to-end transport and connectionless services.
    - This protocol detects errors but does not specify errors. So it is unreliable in nature.
    - UDP includes the following fields:
        - Source port address:
            - The source port address is the address of the application program that generated the message.
            - Destination port address: The destination port address is the address of the application program that receives the message.
            - Total Length: Specifies the total number of bytes of the user scheme in bytes.

- Checksum: A checksum is a 16-it field used to detect errors.

- **Transmission Control Protocol (TCP)**

  It provides complete transport layer services for applications. It creates a virtual circuit between the sender and the receiver and it operates for the duration of the transmission.

  It is a reliable protocol because it detects errors and retransmits corrupted frames. Hence, it ensures that all the segments must be received and acknowledged before a transmission is considered complete and a virtual circuit is discarded.

  At the end of sending, TCP divides the entire message into smaller units called segments, and each segment contains the sequence number needed to reorganize the frames to form the original message.

  At the end of the reception, TCP collected all the segments and rearranged them according to the order number.

So, this was all about TCP/IP and next layer is application layer.

4.3.4 Application Layer

The application layer is the top layer of the TCP/IP model. It is responsible for managing high-level protocols issues. This layer allows the user to interact with the application.

When an application layer protocol wants to communicate with another application layer, it passes its data to the transport layer.

There is an ambiguity in the application layer. Not all applications can be placed inside the application layer except those that interact with the communication system. For example, a text editor cannot be considered in the application layer while a web browser uses the HTTP protocol to interact with the network where the HTTP protocol is the application layer protocol.

Following are the main protocols and important terminology used in the application layer:

- HTTP:

    - HTTP stands for Hypertext Transfer Protocol. This protocol allows us to access data on the World Wide Web. It transmits data as plain text, audio, video. It is called Hypertext Transfer Protocol because it is effectively used in hypertext environments where there are rapid transitions from one document to another.
- SNMP:
    - SNMP stands for Simple Network Management Protocol. It is a framework used to manage devices on the Internet using the TCP/IP protocol suite.
- SMTP:
    - SMTP stands for Simple Mail Transfer Protocol. The TCP/IP protocol that supports email is known as the Simple Mail Transfer Protocol.
    - This protocol is used to send data to another email address.
- DNS:
    - DNS stands for Domain Name System. The IP address is used to uniquely identify the server's connection to the Internet. However, people prefer to use names instead of addresses. Therefore, the system that associates names with addresses is called a domain name system.
- TELNET:
    - This is an abbreviation for Terminal Network.
    - It establishes a connection between the local computer and the remote computer in such a way that the local terminal appears to be a terminal of the remote system.
- FTP:
    - FTP stands for File Transfer Protocol.
    - FTP is a standard Internet protocol used to transfer files from one computer to another.

So, till now we have seen all the layers of TCP/IP model. We have also discussed important protocols used in each and every layer. Till now we have seen the how the

communication is established between the layers, so now we need to identify the process and for that we need to give a unique numeric value to every process. We need to connect this process with IP address also. To achieve these both students requires knowledge of ports and sockets. So, let's discuss!

4.4 PORT AND SOCKETS

Port and sockets are the concepts which are supposed to determine which processes near to a given host are actually talking to which processes, on which remote server, using the protocol if any. As IP address identifies the computer, the network port identifies the application or process running on the computer. A socket is a combination of IP address and port which is used to establish connection between two computers. Let's discuss ports and sockets in detail.

4.4.1. Ports

Each process needs to communicate with another process that is distinguished from the TCP/IP protocol suite by at least one port. A port is a 16-bit number used by the host protocol to recognize the higher-level protocol or application or a process to which it should forward messages.

There are mainly two types of ports:

- Well-known:
    - These are allocated to server services by the Internet Assigned Numbers Authority (IANA). For example, Web server used port number 80 and SMTP services uses port number 25.
    - Generally, the known numbers are often odd, as early systems using the port concept required an even/odd port pair for duplex operation. Most servers only require one port. Special cases are the BOOTP server, which uses two: 67 and 68.
- Ephemeral:

- Some clients don't care about known port numbers since they started communicating with the server and the port numbers they use application is contained in UDP / Graph TCP data is sent to the server.
- Each client procedure is assigned a port number, depending on the server it is running on. The temporary port number has a value greater than 1023, usually between 102 and 65535.
- Since two unique applications are attempting to use the same port numbers on a single host, avoid dealing those applications to request a port accessible from TCP/IP. This port number is being named gradually; it may change with each transition from one application to another.

4.4.2. Sockets

As we know socket is a combination IP address and port, so each end connection will have socket. The socket interface is one of the few application programming interfaces for communication protocols.

For example, in your computer you have two browsers open where in one is looking at Google search and another is looking at facebook website. So the connection for Google is the IP address of client PC and port assigned for Google and for Google server there will be combination of IP with port 80 for the destination socket. In a similar fashion, socket is assigned for facebook server. Here, client port is dynamically assigned and it can be reused once the session is closed for the particular website.

In the TCP/IP suite (version), the following can be a valid association:

Two processes are communicating through TCP sockets. The socket model provides a process with a duplex byte stream connection to another process. The application doesn't have to worry about managing this stream; these facilities are provided by TCP.

So, this was the discussion about ports and sockets and at the end of unit we need to know the structure of IP address and its types.

4.5 STRUCTURE AND TYPES OF IP ADDRESS

The IP address is represented by an unsigned 32-bit binary value. It is usually expressed as a decimal point. For example, 91.67.15.28 is a valid IP address. The digital form is used by IP software.

IP addressing standards are described in RFC 1166. To identify a host on the Internet, each host is assigned an IP address. When a server is connected to more than one network, it is called multi-network and has an IP address for each network interface.

The IP address consists of a pair of numbers:

IP address =<network number><host number>

IP addresses are 32-bit numbers strings to in a spotted decimal structure For example; 128.2.7.9 is an IP address with 128.2 being the network number and 7.9 being the host number. Next, we disclose the guidelines used to isolate an IP address into its system and host parts.

The binary configuration of the IP address 128.2.7.9 is:

10000000 00000010 00000111 00001001

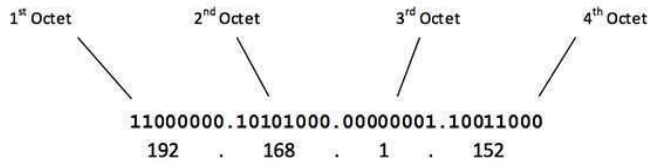
We can see that above is combination of 4 octets of binary digits.

IP addresses are divided into different – different classes depending upon the uses and applications. Let's discuss it.

4.6 CLASS BASED IP ADDRESSES

The first bits of an IP address specify how the rest of the address is separated into its network and host parts. The terms network address and netID are sometimes used interchangeably with network numbers, but the official term, used in RFC 1166, is network number. In addition, the terms host address and hostID are sometimes used instead of host number. Internet Corporation for Assigned Names and Numbers (ICANN) is a responsible body for assigning IP addresses.

Look at the following IP address, here 1st octet the left most of all.



For assigning IP address and to divide it into classes we need to decide number of network and number of host per class. For that following formula is used.

Number of Network = $2^{Network\ Bits}$

Number of Host per Network = $2^{Host\ Bits}$ - 2

When calculating host IP address, two IP address are decreased because they cannot be assigned to host. The first IP of a network is network number and last IP is specifically reserved for broadcast IP.

IP addresses are divided into five classes depending upon the requirement.

- Class A:
  - The first bit of first octet is always set to zero, so range is 1 – 127.
  - i.e

    00000001 - 01111111
  - In this class it uses range from 1 to 126 and 127 is reserved for loopback address.
- Class B:
  - The first two bits of first octet are set to 10, so range is 128 – 191.
  - i.e

    10000000 - 10111111
  - So, Class B IP address ranges from 128 – 191.
- Class C:
  - The first octet of class C IP address has its first three bits set to 110, so range is 192 – 223.
  - i.e

    11000000 - 11011111
- Class D:

- The first octet of class D IP address has its first four bits set to 1110, so range is 224 – 239.
- i.e

  11100000 - 11101111
- This class is reserved for multicasting.

- Class E:
  - This class is reserved for experimental and R&D purposes.
  - IP address of this class is ranging from 240 to 254

So, above is the basic discussion of IP address classes and there are many concepts like subnet mask and subletting that we will learn in next semesters.

4.6.1 Special use IP addresses

There are some IP addresses which are assigned for some specific uses. Following table describes the IP address and its specific uses.

IP Address Block	Specific use
0.0.0.0/8	Current network
14.0.0.0/8	Public Data Network
24.0.0.0/8	Cable Television Network
128.0.0.0/16	Reserved but subject to allocation
169.254.0.0/16	Link local
191.255.0.0/16	Reserved but subject to allocation
198.18.0.0/15	Network interconnect device benchmark testing
223.255.255.0/24	Reserved but subject to allocation
224.0.0.0/4	Multicast and for future use

4.7 LET US SUM UP

TCP/IP stands for “Transmission Control Protocol / Internet Protocol”. It is basically a network protocol that defines the details of how data is sent and received through network adapters, hubs, switches, routers and other network communications hardware. It was developed by the US department of defence for the purpose of connecting government computer systems to each other through a global, fault tolerant, network. It is a protocol suite which describes the four layers of OSI model. We have many protocols which are being used in each and every layer. Concept of ports and socket is also discussed. At the end we have discussed about structure of IP address. There are five classes of IP addresses and each has their specific use.

4.8 FURTHER READING

- James F. Kurose, Keith W. Ross, “Computer Networking – A Top-Down Approach Featuring the Internet”, Fifth Edition, Pearson Education, 2009.
- Nader. F. Mir, “Computer and Communication Networks”, Pearson Prentice Hall Publishers, 2010.
- Ying-Dar Lin, Ren-Hung Hwang, Fred Baker, “Computer Networks: An Open Source Approach”, McGraw Hill Publisher, 2011.

4.9 ASSIGNMENT

1. Explain the different layers of TCP/IP.
2. Differentiate OSI & TCP/IP layers.
3. Discuss various classes of IP address.
4. Describe port and socket in brief.

BLOCK – 4

Connectivity Devices, Network Topologies and Architectures

Unit 1: Connectivity Devices

1

Unit Structure

1.1 LEARNING OBJECTIVES

After studying this unit student should be able to:

- Understand basic concept of connectivity devices used in network.
- Analyzing the role of routing and switching in communication network.
- Understand process of modulation and demodulation.

1.2 INTRODUCTION

Till now we have seen, fundamental of networking to network architecture and models and protocols being used in computer network. At last, in this particular block we are going to discuss hardware components used in network and many network architecture related topics. In this unit, we are going to discuss all about connectivity devices.

Let's start with network devices!

Hardware devices which are used to establish connection with devices like computers, printers and other electronic devices to a network are called network devices. These devices are used to transfer data in a fast, secure and correct way over same or different networks. These devices may be inter-network or intra-network. Some devices are installed on the devices, for example NIC card or RJ45 connector. Some devices are part of network like modem, router, switch, etc.

Let us explore some of these devices.

1.3 MODEM

MODEM stands for Modulator and Demodulator. It is a device which allows a computer to transmit data over telephone or cable lines. The data stored on the computer is in form of digital data however a telephone line or cable wire can send and receive only analog data.

The main function of the modem is to convert digital signal into analog and vice versa. It is a combination of two devices − modulator and demodulator. The modulator converts digital data into analog data when the data is being sent by the computer. The

demodulator converts analog data signals into digital data when it is being received by the computer.

A MODEM sends or receives data in bits per second (bps). One can establish a smooth connection between digital devices and analog devices using MODEM. It has an important role as a translator between the devices and rapidly transmits the information. In short, we can say that it encodes the signal and decodes it at the other end and vice versa.

Now, let's discuss its types in brief.

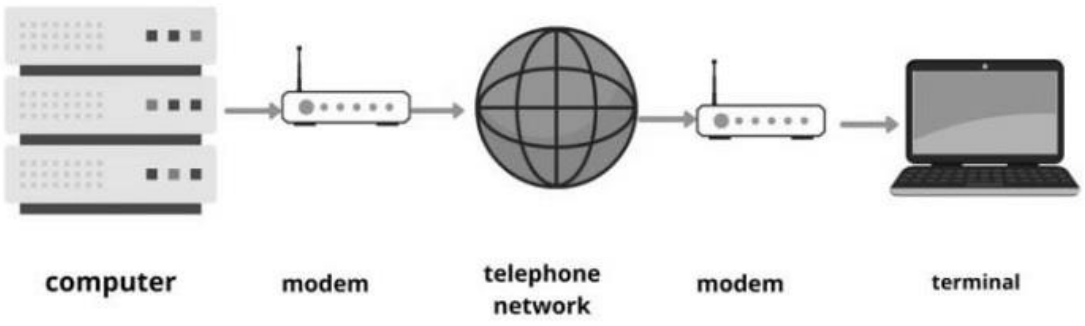
Types of Modems

The different types of modems used to access the internet are as follows:

- Telephone Modem
- Digital Subscriber Line
- Cable Modem
- Satellite Modem

1.3.1 Telephone Modem:

Computers are connected using telephone lines to get access the network. When we are comparing to other modems, it is comparatively cheaper because it does not take any installation cost. A monthly fee for a telephone modem is quite low.

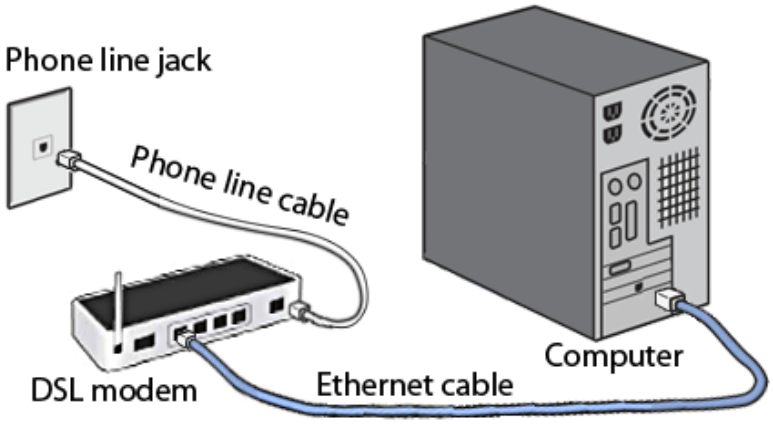


(Image Source: https://bit.ly/3sOf8oK)

1.3.2 Digital Subscriber Line:

Digital Subscriber Line (DSL) provides high speed internet connection using telephone lines. DSL is expensive in comparison with telephone modem. The DSL is also connected with phone lines just like telephone modem, but the difference is in DSL

voice communication and internet service is used simultaneously where in telephone modem this service is not provided.



(Image Source: https://bit.ly/3vMMkig)

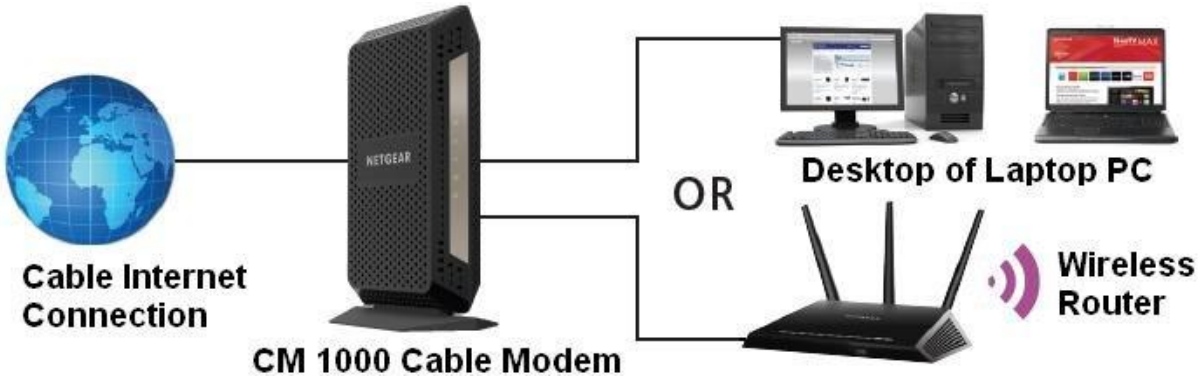
Types of DSL

- **SDSL:**
  - Symmetric DSL provides equal bandwidth for both uploading and downloading and is mostly preferred by small organizations.
- **ADSL:**
  - It is Asymmetric DSL.
  - Most users download more data then they upload, for this they use ADL.
  - In this, downstream speed is much more than upstream. Uploading capacity may not work as good as downloading capacity. Users who do not upload that much in comparison to downloading can use ASDL.
  - It may offer as high as 20 Mbps speed for downloading while for uploading 1.5 Mbps.
- **HDSL:**
  - It is high bit-rate Digital Subscriber Line.
  - It is a wideband digital transmission which is used within a corporate site and between the telephone company and its customers.
  - It is a symmetrical line which offers equal bandwidth in both directions.

- **RADSL:**
    - It is Rate-Adaptive DSL.
    - In this, the modem is capable of adjusting bandwidth and operating speed to maximize the data transfer.
    - It supports both symmetrical and asymmetrical applications with variable speeds.
- **VDSL:**
    - It is very high data rate DSL.
    - It is a developing DSL technology that offers more reliable internet experience than basic broadband.
    - It offers much higher data transfer rate over short distances, e.g. 50 to 55 Mbps over lines up to 300 meters in length.

1.3.4 Cable modem

It is a device that provides high-speed data access using a cable TV (CATV) network. Most cable modems are currently external devices which are used to connect to the PC with the help of a standard 10 BASE-T Ethernet card and twisted-pair wiring.



(Image Source: https://encryptedtbn0.gstatic.com/images?q=tbn:ANd9GcTN9x6oKB1ybJG_uC59EVW1h4RqZu9gnoq4ig&usqp=CAU)

1.3.5 Satellite modem:

The device that provides internet connection using satellite dishes are known as Satellite Modem. It sends the input bits to output radio signals and then executes input radio signal to output bit. Cost of this device is higher compared to all other modems but provides better reliability to the internet network.

(Image Source: https://www.idirect.net/wp-content/uploads/2020/02/MDM2510_white.png)

This was all about Modems and its types. Let's further discuss other devices.

1.4 NETWORK INTERFACE CARD (NIC)

A NIC is a hardware component without it; computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also known as network interface controller, network adapter or LAN adapter.

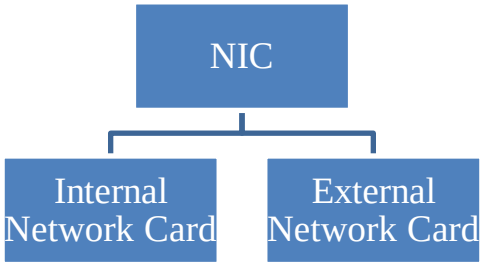
It allows both wired as well as wireless communications. It also allows communications between computers connected via LAN as well as communications over large-scale network.

NIC is considered as both a physical layer and a data link layer device. It means that it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.

Let's discuss its types now.

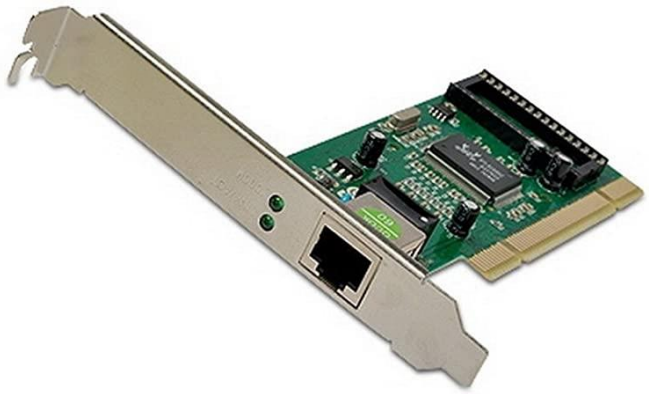
1.4.1 Types of NIC Cards

NIC cards are of two types –



Internal Network Cards

It is inserted in motherboard, so it is known as internal network card. Motherboard has a specific slot for the card where it can be inserted. It requires network cables to provide network access. It can be classified in two types. The first type of these uses Peripheral Component Interconnect (PCI) connection, whereas the second type uses Industry Standard Architecture (ISA). Following figure depicts the same.



(Image Source:https://m.media-amazon.com/images/I/51tGjrWgylL._AC_SY450_.jpg)

External Network Cards

External network cards can be used on the devices like desktops and laptops that do not have an internal NIC. There are two types of external network cards:

- Wireless:
  - Wireless network card needs to be inserted into the motherboard where no network cable is required to connect to the network.
- USB based:
  - They are useful while travelling or accessing a wireless signal.

(Image Source:https://www.elprocus.com/wp-content/uploads/wireless-network-interface-card.jpg)

1.5 REPEATER

Repeaters are network devices that amplify or regenerate an incoming signal before retransmitting it. Repeaters were introduced in wired data communication networks due to the limitation of a signal in propagating over a longer distance and now are a common installation in wireless networks for expansion. Following figure depicts a repeater device.

(Image Source: https://389880-1226307-raikfcquaxqncofqfm.stackpathdns.com/wp-content/uploads/2020/03/Repeater.jpg)

When an electrical signal is transmitted through a channel, it gets attenuated depending upon the nature of the channel. This is a limitation because of the limited length of the LAN and coverage area of cellular networks. This problem is alleviated by installing repeaters at certain intervals.

Repeaters amplify the attenuated signal and then retransmit it. Digital repeaters can even reconstruct signals distorted by transmission loss.

Now, let's discuss the types.

Repeaters are classified into two categories on basis of the types of signals which they regenerate.

- **Analog Repeaters**:
  - It can only amplify the analog signal.
- **Digital Repeaters:**
  - It can reconstruct a distorted signal.

Repeaters can also be categorized into two types on the basis of the types of networks that they connect:

- **Wired Repeaters:**
  - They are used in wired LANs.
- **Wireless Repeaters:**
  - They are used in wireless LANs and cellular networks.

Moreover, they are also classified according to the domain of LANs they connect.

- **Local Repeaters:**
  - They connect LAN segments separated by small distance.
- **Remote Repeaters:**
  - They connect LANs that are far from each other.

1.6 HUB

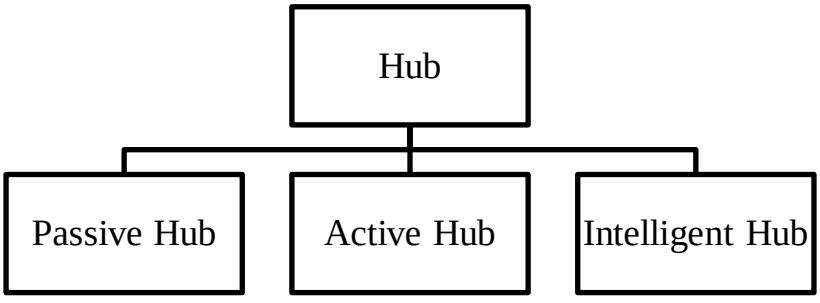
Hub is a hardware device that divides the network connection among multiple devices. Networking devices operating at a physical layer of the OSI model that are used to connect multiple devices in a network are known as hub. They are generally used to connect computers in a LAN.

A hub contains many ports. A computer which intends to be connected to the network is plugged in to one of these ports. When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination device or not.

(Image Source: https://thecybersecuritymancom.files.wordpress.com/2018/01/hub4.png)

1.6.1 Types of Hubs

Initially, hubs were passive devices. However, with development of advanced technology, active hubs and intelligent hubs came into use.



- **Passive Hubs:**
    - Passive hubs connect nodes in a star configuration by collecting wiring from nodes.

- They broadcast signals onto the network without amplifying or regenerating them.
- As they cannot extend the distance between nodes, they limit the size of the LAN.

- **Active Hubs:**
  - Active hubs amplify and regenerate the incoming electrical signals before broadcasting them.
  - They have their own power supply and serve as a repeater and connecting centre as well.
  - Due to their regenerating capabilities, they can extend the maximum distance between nodes, thus increasing the size of LAN.
- **Intelligent Hubs**:
  - Intelligent hubs are active hubs that provide additional network management facilities.
  - They can perform a variety of functions of more intelligent network devices like network management, switching, providing flexible data rates etc.

One more important device is switch, let's discuss it.

1.7 SWITCH

It is a hardware device that connects multiple devices on a computer network. It contains more advanced features than hub. It contains the updated table that decides where the data is transmitted or not. It delivers the message to the correct destination based on the physical address present in the incoming message.

A switch does not broadcast the message to the entire network like the hub. It determines the device to whom the message is to be transmitted. Therefore, we can say that switch provides a direct connection between the source and destination. It increases the speed of the network.

A switch has many ports to which computers are plugged in. When a data frame arrives at any port of a network switch it examines the destination address, performs necessary checks and sends the frame to the corresponding device. It supports unicast, multicast as well as broadcast communications. Following figure shows an ideal network switch.

(Image Source: https://infinity-cable-products.com/blogs/hardware/what-is-a-network-switch)

1.6.1 Types of Switch

It can be classified into four types

- Unmanaged Switch
- Managed Switch
- LAN Switch
- PoE Switch

Unmanaged Switch:

- These are inexpensive switches.
- These are commonly used in home networks and small businesses.
- They can be set up by simply plugging in to the network, after which they instantly start operating.
- When more devices need to be added more switches are simply added by this plug and play method.
- They are referred to as unmanaged since they do not require to be configured or monitored.

Managed Switch:

- These are costly switches that are used in organisations with large and complex networks.
- They can be customized to enhance the functionalities of a standard switch.
- The augmented features may be QoS (Quality of Service) like higher security levels, better precision control and complete network management.
- Despite their cost, they are preferred in growing organizations due to their scalability and flexibility.
- Simple Network Management Protocol (SNMP) is used for configuring managed switches.

LAN Switch:

- These switches connect devices in the internal LAN of an organization.
- They are also referred as Ethernet switches or data switches.
- These switches are particularly helpful in reducing network congestion or bottlenecks.
- They allocate bandwidth in a manner so that there is no overlapping of data packets in a network.

PoE Switch:

- Powers over Ethernet (PoE) switches are used in PoE Gogabit Ethernets.
- PoE technology combines data and power transmission over the same cable so that devices connected to it can receive both electricity as well as data over the same line.
- PoE switches offer greater flexibility and simplifies the cabling connections

1.6.2 Features of Switches

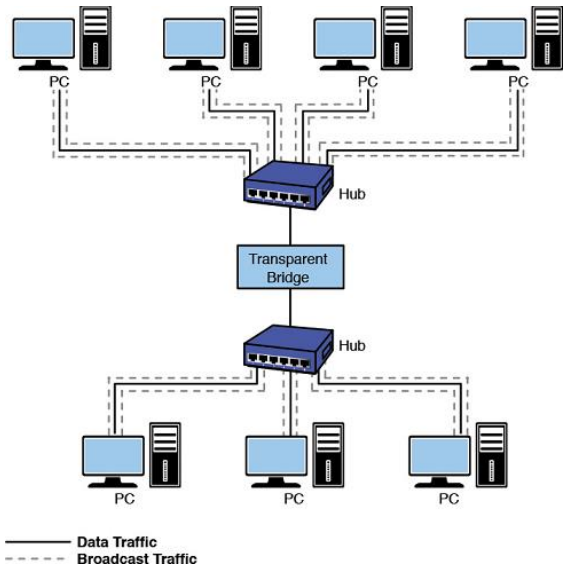
The following are features of Switches:

- ✓ It is an intelligent network device that works as a multiport network bridge.
- ✓ It uses MAC addresses to send data packets to selected destination ports.
- ✓ It uses packet switching technique to transmit data packets from the source to the destination device.
- ✓ It is supports unicast, multicast and broadcast communications.
- ✓ Transmission mode is full duplex and hence collisions do not occur.

- ✓ These are active devices, equipped with network software and network management capabilities.
- ✓ It also performs some error checking before forwarding data to the destined port.

1.8 BRIDGE

Bridge can divides traffic on a local area network by separating the LAN into several different segments. A bridge is a repeater; with add on the functionality of filtering content by reading the MAC addresses of source node and destination node. Bridge operates within the layers of the network and also controls the data that crosses the boundaries from one local area network to the other. Following figure shows the working of bridge.



(Image Source: https://www.pearsonitcertification.com/articles/article.aspx?p=2474237&seqNum=2)

1.7.1 Uses of Bridges

The main uses of bridges are:

- Bridges are used to divide large busy networks into multiple smaller and interconnected networks to improve performance.
- Bridges also can increase the physical size of a network.
- Bridges are also used to connect a LAN segment through a synchronous modem relation to another LAN segment at a remote area

1.7.2 Types of Bridges

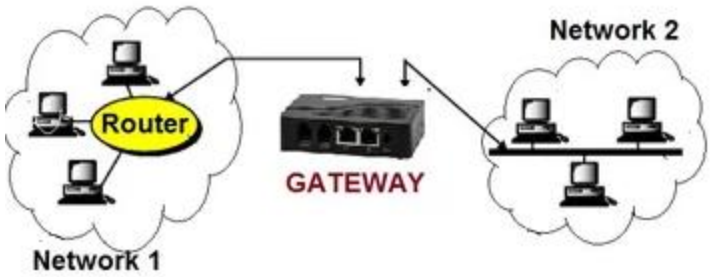
There are generally two types of bridges which are as follows:

- **Transparent Bridges:**
  - It is also called learning bridges.
  - It constructs its table of terminal addresses on its own as it implements connecting two LANs.
  - It facilitates the source location to create its table.
  - It is a self-updating device.
  - It is a plug and play device.
- **Source Routing Bridge:**
  - In this type, the source computer provides destination address along with the packet.
  - It is widely used on Token Ring networks.
  - This type of bridge is used to prevent looping problem.

1.9 GATEWAY

A gateway is a connecting device that can relate to multiple networks. They perform at the application layer of the OSI model. They manage messages, locations, and protocol conversion to deliver a packet to its terminal between two connections.

The major difference between gateways and routers is that routers operate at the OSI model's network layer whereas gateways operate from the lowest to the topmost layer. Following figure shows a simple working of a gateway.



(Image Source: http://digitalthinkerhelp.com/what-is-gateway-in-networking-types-examples-functions-uses-working/)

Gateways and routers are used correspondently. It can change data packets from one protocol structure to another before forwarding them to connect two different networks. Hence it incorporates a protocol conversion function at the application layer.

Characteristics of Gateways

- It can support complete protocol transformation from one proprietary computer network technology to other technology.
- It means transformation of Ethernet to Token Ring or FDDI or some different model or protocol instead of encapsulation.
- It needs higher layers of the OSI model, possibly, the application layer. IBM SNA, DEC net, Internet TCP/IP and other protocols can be transformed from connection to connection.
- Gateways work casually due to protocol conversion. Therefore, they can generate bottlenecks of the blockage during the time of peak operation.

Advantages of Gateways

- It can connect the devices of two several networks having a different design.
- It is an intelligent tool with filtering capabilities.
- It has control over both collisions and the advertisement area.
- It needs a full-duplex mode of connection.
- It can make data translation and protocol conversion of the data packet according to the destination network's requires.
- It is used to encapsulate and encapsulate the data packets.
- It has enhanced security over any other network relating device

1.10 LET US SUM UP

In this unit, we have sees various networking devices which are essential for communication among devices on a computer network. Modem, NIC, Switch, Hub, Router, Gateway etc are the various devices used for internetworking. Modem is modulator-demodulator and it is a device that enables a computer to transmit and receive data over a telephonic line or cable or satellite connections.

The NIC used connect the computer to the external network. A Hub connects all the nodes of a network using UTP or STP cables. In a Hub, the signals received on one port are transmitted to all other ports and vice versa. A Switch, on the other hand does not distribute signals without verifying whether it really needs to propagate to a given port or ports. Bridge is used to filter the content over a network. Gateway is used to connect several networks with different designs. Each and every devices has their own advantages, disadvantages, features and application.

1.11 FURTHER READING

- ForouzanBehrouzA ,"Data Communications and Networking" ,McGrawHill,New York.
- Andrew S. Tanenbaum, "Computer Networks", Prentice Hall PTRComer, Douglas E., and Ralph E. Droms. Computer networks and internets. Prentice-Hall, Inc.,
- Data and Computer Communication, William Stalling, Pearson Education, 2ndEdition, Delhi.

1.12 ASSIGNMENT

1) What are the primary conditions that affect routing?

2) Define and differentiate hub and switch.

3) Discuss the functions of gateways in brief.

4) Write brief note on MODEM.

5) Define and differentiate repeater and gateway.

Unit 2: Network Architecture

2

Unit Structure

2.1 LEARNING OBJECTIVES

After studying this unit student should be able to:

- Understand peer to peer Computer Network Architecture
- Understand Client - Server Architecture
- Differences and applications of peer to peer and Client Server Architecture.

2.2 INTRODUCTION

In earlier unit, we have seen all about connective devices. In this particular unit we are going to discuss the architecture of network communication.

Computer network architecture is a design in which all the computers are well-organized in a network. The architecture defines and describes how computers should communicate with each other to obtain maximum benefits from a computer network. Architecture is responsible for various benefits such as better response time, security, scalability, data transfer rate, connectivity and many more.

Mainly, there are two types of computer network architectures available:

- Peer to Peer Network
- Client-server Network

Let’s discuss it one by one.

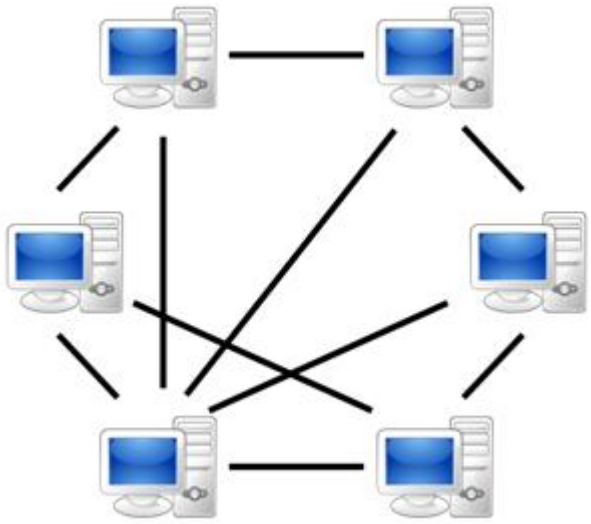
2.3 PEER TO PEER NETWORK

It is an architecture in which all the computers are linked with each other with equal privilege and responsibilities for data processing. It is feasible to use for small environment up to 10 computers.

It has no dedicated server, only direct communication can be done and hence it is known as peer-to-peer (P2P) network architecture. For sharing the available resources, special permissions are assigned to each computer but there can be a problem if the computer with the resource is down.

P2P architecture consists of a decentralized network of peers or nodes that act as both clients and servers as well. This network share workload between peers and all peers share resources within the network without a centralized server.

P2P architecture is completely decentralized. However, in application, sometimes there is a central tracking server situated on top of the Peer to Peer network to help nodes or peers find each other and manage the network. Following figure shows the basic P2P network.



(Image Source:https://upload.wikimedia.org/wikipedia/commons/thumb/3/3f/P2P-network.svg/1200px-P2P-network.svg.png)

2.3.1. Application of Peer to Peer Architecture

P2P architecture works efficient and effective when there are lots of active peers in a network and hence new peers who are joining the network can easily find other peers to establish connection. If a large number of peers drop out of the network, there are still enough remaining peers to pick up. If there are only a few peers, at that time less resources will be available. Let's take an example, in a P2P file-sharing application lots of peers are sharing the file so can be downloaded in a faster way.

It works best if the workload is divided into small chunks means divide into smaller parts that can be reassembled later. A large number of peers can work together on one task and each peer has less work to do. In the case of P2P file-sharing, a file can be broken

down so that a peer can download many chunks at a time of the file from different peers we can get that in fastest way.

Following are the uses of P2P architecture:

- File sharing
- Instant messaging
- Voice Communication
- Collaboration
- High Performance Computing

There are many applications where P2P architecture is used, so let's seethem in detail.

2.3.2. Examples of Peer to Peer Architecture

Napster:

- Napster was introduced by American college student Shawn Fanning, in 1999.
- It used for file sharing service over the internet and music could be store on your PCs.
    - It was shut down in 2001.

Bit Torrent:

- Bit Torrent is used to distribute data and all files on the internet into decentralized manner to improve speed of data transmission.
- Its main objective is to transfer files like as video files and audio files to host computers.

Skype:

- It is a peer to peer VoIP (Voice over Internet Protocol) client that is designed for audio – video interface and communication.
- With the help of it, all users can make voice call and sent text messages to another user but they must be Skype user.

Bitcoin:

- It also uses the P2P payment network and in which cryptographic protocols are used for operating which helps to users for sending and receiving bitcoins.

Gnutella:

- It is a P2P network that is used for file sharing.
- It allows users to send and obtain all data on the internet.

Kazaa:

- It was P2P file sharing application that was enabled with FastTrack protocol licensed by Joltid LTD, and it was operated by Sharman Networks.
- Its main goal was to transfer different kinds of over the internet.

Limewire:

- It is used for P2P file sharing in freely for different types of operating systems like as Windows, OS X, Linux and Solaris.
- LimeWire implemented gnutella network along with BitTorrent protocol.

2.3.3. Advantages of Peer-To-Peer Network:

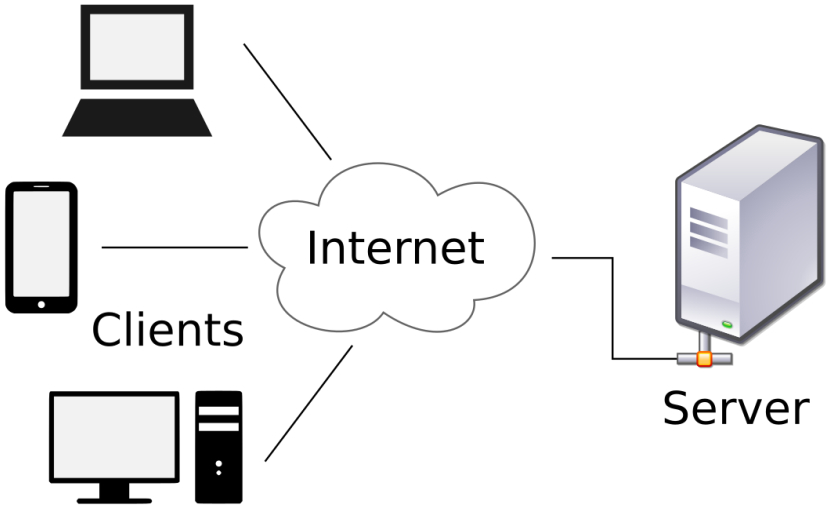
- Cost will be less as it does not contain any dedicated server.
- If one computer stops working but other computers will not stop working.
- It is easy to set up and maintain.

2.3.4. Disadvantages of Peer-To-Peer Network:

- As it does not contain the centralized system. So that, it cannot back up the data as the data will be divided and located on different locations.
- It has a security issue as the device is managed itself.

2.4 CLIENT AND SERVER ARCHITECTURE

It is a model in which computers such as servers provide the network services to the other computers such as clients to perform a user based tasks. Following figure shows the architecture.



(ImageSource:https://upload.wikimedia.org/wikipedia/commons/thumb/c/c9/Client-server-model.svg/1200px-Client-server-model.svg.png)

An application program is known as a client program, running on the local machine that requests for a service from an application program known as a server program, running on the remote machine.

A client program runs only when it requests for a service from the server while the server program runs all time as it does not know when its service is required.

A server provides a service for many clients not just for a single client. Therefore, we can say that client-server follows the many-to-one relationship. Many clients can use the service of one server.

Services are required frequently and many users have a specific client-server application program. For example, the client-server application program allows the user to access the files, send e-mail, and many more. If the services are more customized,

then we should have one generic application program that allows the user to access the services available on the remote computer.

2.4.1. Client-Server Architecture Components

There are three interconnected components are used in this architecture:

- Workstations
- Servers
- Networking Devices

Workstations:

- Workstation is the system of users that are sometimes also named as “client’s computer”.
- These workstations use various kinds of operating systems.
- Most of the times MS Windows are used on the workstations.
- The operating system used on the client’s workstation is much cheaper than that of servers.

Server:

- An ultra-performer device that retains a fast processing speed, extra storage space and more memory to deal with multiple requests approaching at a time from various location.
- It performs numerous kinds of functions, such as mail servers, database servers, file servers, and domain controllers etc.

Networking Devices:

- Workstations and servers are interconnected with each other by means of a specific medium. This medium is a network device.
- Each device used in the client-server architecture has its own operations and properties.
- For making a connection to a server with various workstation hubs are used.

- For transferring data from a device to another device, repeaters are used.
- For isolated network segmentation bridges are used.
- And there are many other which we have already seen in previous unit.

2.4.2. Types of Client-Server Architecture

The functionality of client-server architecture is in various tiers. Below are the types of architecture..

1. One Tier Architecture
2. Two Tier Architecture
3. Three Tier Architecture
4. N Tier Architecture

1. One Tier Architecture:

This architecture contains all loads on a single device. The setting involves configuration setting, data and marketing logic. This is one of the reliable sources because of its services. Handling of such architecture is difficult. Below are the few layers that hold one tier architecture.

- Presentation layer
- Business layer
- Data access layer

All the layers work integrated with the help of a unique software package. In this architecture the data is stored on local devices.

2. Two Tier Architecture:

This architecture facility has the best environment. As it helps in saving the user interface (UI) on the system of the user (client) and the related data based are stored on the server device. Database logic and business logic both needs to be maintained where these logics are to be stored either on the user's end and the server's end. When these logics are stored on the client's end, the architecture is called "fat client thin

server" however, if these logics are handled at server device then we call it as "thin client fat server".

Command fired by client gives quick response and the fastest rate is achieved as client-server devices are directly in relation. Ticket reservation agencies mostly employ this architecture.

This approach has many benefits:

- ✓ It has good performance.
- ✓ Application designing of this architecture is easy.
- ✓ Users will get satisfactory results in a response of this architecture and homogeneous environment.

The limitation of this framework includes:

- ✓ Less secure.
- ✓ Growing users can affect the performance of architecture.
- ✓ Least portability.

3. Three Tier Architecture:

A middleware is there between the client and the server machines in this architecture. If a user needs particular information from the server, the user will send the request that will first be received by the middle layer, which will then be dispatched to the server for further actions. In the same pattern, the response will be reached to the user side. That first is received at the middle layer and then the middle layer will dispatch the received data from the server to the user's end. Middleware has a provision to control and store the data logic and business logic. Middleware in the 3-tier architecture helps to optimize the flexibility and performance of the architecture. The framework is categorized into three main layers

- Presentation layer (Users' Tier)
- Application layer (Business Tier)
- Database Tier (Data Tier)

Different layers can control all the tiers. As the presentation layer is controlled at the user device. The business tier or middleware handles the application layer and the server machine tackles the database tier.

This architecture has also a few benefits:

- ✓ Better security of data
- ✓ Invisible database structure
- ✓ Outperformed data integrity.

The single limitation of this approach is the complexity of communication due to the presence of the middleware system.

4. N Tier Architecture:

The technique is similar to three tiers. This is also known as “Multi-tier architecture”. This architecture has a provision for locating each function as an isolated layer which includes presentation, application processing and management of data functionalities.

2.4.3. Client-Server Architecture Examples:

- **Web Servers:**
  - A strong computational device which can manage many websites is like a web server.
  - Installing numerous kinds of web server applications on this computer like Apache or Microsoft IIS, offers links to the various web pages hosted on the online, and such servers are connected to the Internet by higher-speed connections that offer ultra-speed data transfer speeds.
- **E-Mail Servers:**
  - These servers are a valuable asset for companies, agencies and individuals as well.
  - That enables the transferring of messages among various users.
  - Specific applications perform functions on the mailing servers that permit the administrators to establish and control email accounts for the specific domain that the server hosts. Various protocols include SMTP, IMAP, POP3 for email communication.

    - Service Mail Transfer Protocol (SMTP) is a general approach used for firing the messages as well as to controlling the outgoing emails.
    - The Internet Message Access Protocol (IMAP) and Post Office Protocol V3 (POP3) is used for reception and controlling the incoming emails.
- **File Servers:**
    - These servers are exclusively allocated structures which facilitate all data to be accessed by clients.
    - It serves as a consolidated place for storing data and many terminal systems may manage it.
- **Domain Name Server (DNS):**
    - The DNS is a term of the Internet.
    - Most of the internet users are getting benefit from this application daily but not each user is familiar with this.
    - DNS is a kind of digital directory that holds the names of and matches those names with numbers. Here we consider the IP as numbers. IP's are used as addresses for communication of devices connected with the Internet. Devices connected to the Internet that includes a Smartphone, laptops, personal computers, and tablets have a unique IP address. Therefore, it is the decentralized system used for matching the website names (URL) and numerical address (IP) on the web of a specific website for which the client is requesting.

2.4.4. Client-Server Architecture Advantages:

The benefits related to client-server architecture are discussed below.

- There is a centralized network that has full leverage to control the processes as well as activities in client-server architecture.
- The central area of the architecture is used for the data storage.
- The devices which can be controlled centrally used in architecture.
- Network protection, data backup and all other elements are tackled centrally.

- Users have the authority to access all the files at any time available on the central storage.
- It also improves the speed of the sharing resources.
- Security is better in Client/Server network where a single server administers the shared resources.
- There exists no restriction regarding geography to access the information. One can access any information from any place.

2.4.6. Client-Server Architecture Disadvantages:

The limitations related to client-server architecture are discussed below.

- Client/Server network is costly as it requires the server with huge amount of memory.
- A server has a Network Operating System to give the resources to the clients, but the expense of such OS is very high.
- It requires a network admin to manage all the resources.

2.5. LET US SUM UP

A Computer Architecture is a design in which all computers in a computer network are organized. Architecture defines how the computers should get connected to get the maximum advantages of a computer network such as better response time, security, scalability etc. The two most popular computer architectures we have discussed are Peer to Peer and Client-Server architecture.

In peer to peer architecture all the computers in a computer network are connected with every computer in the network. In Client Server architecture a central computer acts as a hub and serves all the requests from client computers. At last, we have also discussed the advantages, disadvantages and applications of both the architectures.

2.6. FURTHER READING

- Andrew S. Tanenbaum,"Computer Networks"
- Larry L. Peterson, Bruce S. Davie, "computer networks a systems approach 6th edition"

2.7. ASSIGNEMENT

1. Differentiate between peer to peer and client-server architecture.
2. Define and differentiate client-side and server-side architecture.
3. Discuss in brief: SMTP,POP3,IMAP
4. Write brief note on: DNS

Unit 3: Network Topologies

3

Unit Structure

3.1 LEARNING OBJECTIVES

After studying this unit student should be able to:

- Specify what is meant by network topology
- Classify different Network topologies
- Categorize various Network topologies
- Explain the characteristics of the following topologies:
    - Bus
    - Ring
    - Star
    - Mesh

3.2 INTRODUCTION TO NETWORK TOPOLOGIES

Network topology is defining the different ways for share data from one system to another into the network. It is an agreement of the network. This agreement is diagrammatic explanation with all connection of nodes with is connecting lines of all topologies. Mechanism of each and every topology is different from other one and has its own advantages and disadvantages. The selection of the network topology is dependent upon type and number of equipment being used, rate of data transfer required, planned applications, response time, and cost.

There are two types of topology:

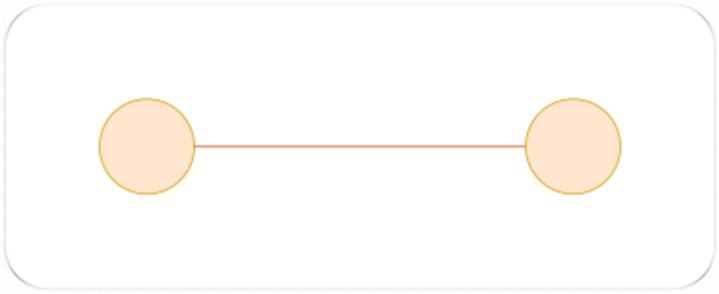
- Physical topology
    - Physical topology describes where the network's different components like its devices and cables are placed and installed.
- Logical topology
    - Logical topology indicates network's information (data) flow and transmission, apart from physical design.

Transmission rates, physical interconnections, distances among nodes and or signal types may different among two networks, yet their topologies may be interchangeable. For communications to happen, two devices must be connected in some way to the same link at the same time. There are two basic types of connections:

- Point-to-point
- Multipoint.

Point-to-Point:

In point to point network one system is only connected to another one system means there is one-to-one communication between these two systems using single cable. This system is may be compute, switch, router server etc.

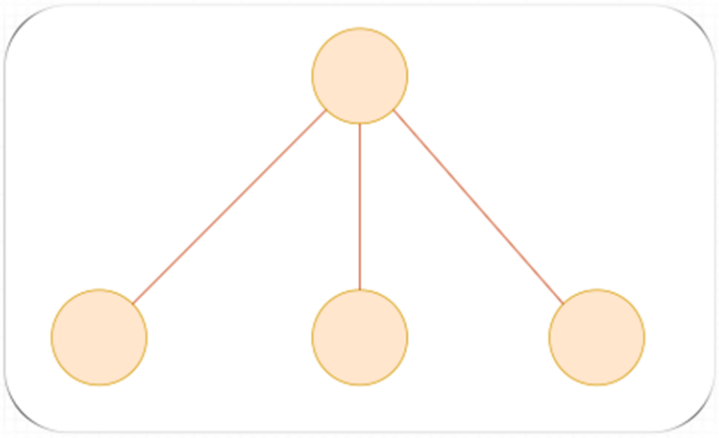


Point to point connection

If the network is ended up of point-to-point connections, then the packet will have to travel from end to end many in-between devices. The link among the multiple intermediate devices may be of dissimilar length. So, in point-to-point network ruling the smallest distance to get to the receiver is most important.

Multipoint Connection:

There are more than two specific devices share a single link. The capacity of the channel is shared in a multipoint connection environment. For share the data, each devices need to identify itself and the device to which it want to share the information. The process of validating sender and receiver is known as addressing.



Multipoint connection

In the figure above, you can see that the five workstations share the common link between the main frame and the workstations. The multipoint networks are also described Broadcast network. In a broadcast network, the packet transmitted by the sender is received and processed by each device on the link. But, by the address field in the packet, the receiver determines whether the packet belongs to it or not, if not, it discards the packet. If packet goes to the receiver then keeps the packet and react to the sender therefore.

Now let see the differences between Point-to-Point and Multipoint Connection:

No.	Point-to-Point Connection	Multipoint Connection
1.	There is a single dedicated link only among two devices	There is a single link is shared by more than two devices
2.	The whole channel capacity is reserved only for the two devices in the connection.	The channel capacity is shared provisionally by the devices in connection
3.	A single transmitter and a single receiver	A single transmitter, and there can be several receivers.

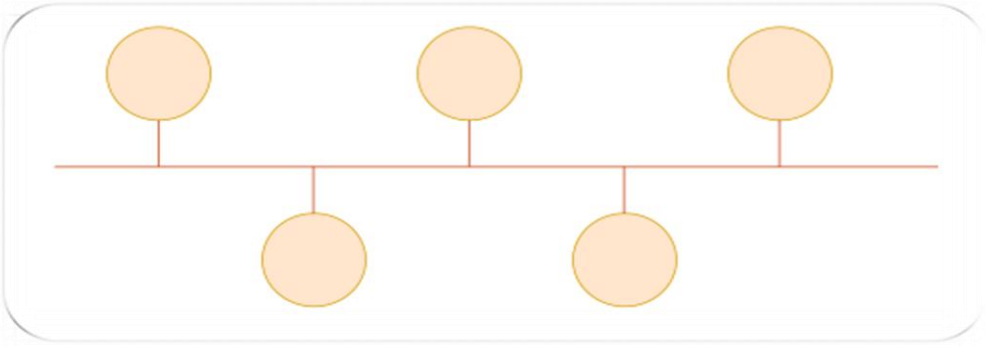
Both topologies are interchangeable or different from each other in same network. There are mainly four basic topologies which are: Bus, Star, Ring, and Mesh. Let discuss it one by one.

3.3 BUS TOPOLOGY

In bus topology the all work stations are connected via a single cable. This single cable is known as backbone cable for the network. Each node communicates to the network via direct connection to the main cable or by drop the cable. If any node wants to transmit a message over the network, this node put a message over the network. This

message was received by all stations which are connected to the network. There is no need to address the destination node.

This topology is mainly used in IEEE 802.3 (Ethernet) and IEEE 802.4 standard networks. The configuration of this topology is simple as compare with other topologies. This backbone cable is also known as “single lane”. Through this cable, broadcasting of message to all the stations is performed. Carried Sense Multiple Access (CSMA) is the most popular and common access method of bus topologies. Following figure shows the structure of bus topology.



CSMA:

- It is a media access control.
- Data flow is controlled by this protocol.
- Controlling of data flow helps to maintain the data integrity.
- For example, the packets do not get lost.
- There are two different ways of handling the problems, these problems like when two nodes send the messages at the same time. When two nodes send the messages synchronously, there are two different ways of handling problems.

CSMA CD:

- CSMA CD **(Collision detection)** is an access method.
- This method is used for detection of collision.

- If any the collision is detected while transmission of data, the sender will stop the transmission of the data.

CSMA CA:

- **CSMA CA (Collision Avoidance)** is also an access method.
- In this method first the checking of transmission media is done to reduce the collision.
- If the transmission media is busy then the sender waits for media when media is not busy sender will send the data.
- This technique is use to reduce risk of collision effectively.

Now, Lets discuss advantages of Bus Topology:

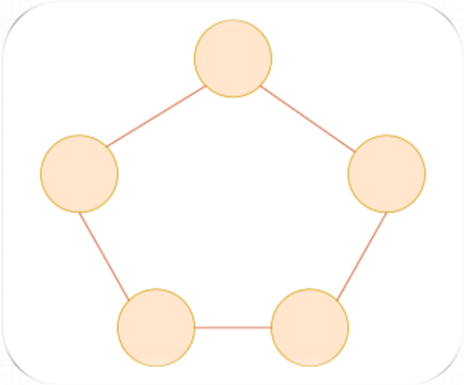
- **Low-cost cable:**
    - Each and every node is connected via each other using cable directly; there is no need of hub that is why the initial cost of installation is low of this topology.
- **Moderate data speeds:**
    - This technology use Coaxial or twisted pair cable.
    - The data rate supported by these cables is up to 10 Mbps.
- **Familiar technology:**
    - Bus topology uses simple techniques for troubleshooting and the installation process is easy.
    - Hardware component are available easily also. So this is familiar technology.
- **Limited failure:**
    - Each node is connected to the backbone cable directly. So if there is an issue with one node then this node will not affect any other node's working.

Disadvantages of Bus topology:

- **Extensive cabling:**
    - Connection between one node with other nodes of the network is simple but these need lots of cables for connection.
- **Difficult troubleshooting:**
    - It requires specialized test equipment to determine the cable faults.
    - If any fault occurs in the cable, then it would disrupt the communication for all the nodes. It is used specified test equipment to find out cable faults.
- **Signal interference:**
    - If two nodes want to transmit messages at a same time then the signals of both nodes cannot reach at the destination because they are crashed with one another.
- **Reconfiguration difficult:**
    - If any new device added in the network. This device makes the network slow.
- **Attenuation:**
    - Attenuation is a loss of signal. This cause issues in communication. Reconstruction of the signal done by repeaters.

3.4 RING TOPOLOGY

In the ring topology, each node is connected to its two neighbour nodes means if the message is received from previous node then it will retransmit to the next node. The form of data in ring topology is unidirectional means data flows in one way.
If the flow of data is in a single loop and it flows constantly then this loop is known as endless loop. The flow of data is in clockwise direction. There is no terminated end because each node is connected to next one and having to end point. Following figure depicts the ring topology.



For example, if there are four nodes in the network the data flow is in this direction node 1 → node 2 → node 3 → node 4 →node 1. **Token passing** is the most common access method of the ring topology. In token passing each node pass the message to another one as token. Token is a frame that passes on the network. Let's see the working of token passing.

Working of Token passing:

- A token move around the network and it is passed from computer to computer until it When the token reach at the destination system, destination system send acknowledgement otherwise token pass around the whole network and transmit this token to one system to other system.
- The data also store the address of the destination. The sender is able to make change in the token.
- The data is passed from one device to another device until the destination address matches. When token reaches the destination, the receiver device sends acknowledgment to sender.
- Here, a token is used as a carrier.

Advantages of Ring topology:

- **Network Management:**
    - If there is any fault in the device then this device can be taken out from the network without carrying the network down.

- **Product availability:**
    - There are different types of hardware and software tools are available for the network operation and for monitoring the network.
- **Cost:**
    - This topology uses twisted pair cables for communication.
    - These cables are inexpensive and easily available and this will reduce the cost of installation.
- **Reliable:**
    - There is no single host computer on which whole network is dependent.
    - All computers are work independently and that is use to make network reliable.

Disadvantages of Ring topology:

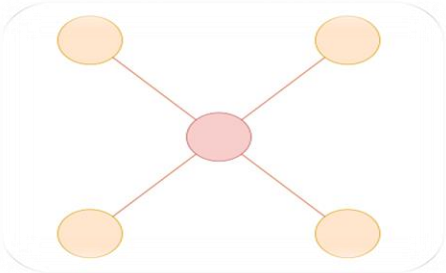
- **Difficult troubleshooting:**
    - If any issue occurs in the cable, then it would disrupt the communication of all the nodes.
    - If there is any issue in the cable, there is particularized test equipment for finding it.
    - The faulty cable makes disturbance to all nodes which are communicating through the network.
- **Failure:**
    - If there is any issue in one station. This one station becomes reason of failure of the overall network.
- **Reconfiguration difficult:**
    - If any new device added in the network. This device makes the network slow because if new device is added it also affects the number of transmission. It will make the number of transmission larger.

- Adding new devices to the network would slow down the network because the numbers of nodes are increase means the number of transmission become larger.

- **Delay:**
  - If new device is added in the network that will increase the communication delay.
  - Means the communication delay directly corresponds on the number of nodes.

3.5 STAR TOPOLOGY

Following figure shows the architecture of start topology.



In this topology, each and every node is connected to other one using central hub or switch or server. The nodes which are attached to the server are known as clients. For connection from client to server use coaxial cable or RJ-45 cables. Mostly Server is used as connection device in logical star topology and Hubs or witches are used as connection device in physical start topology.

Advantages of Star topology:

- **Efficient troubleshooting:**
  - Troubleshooting is efficient with compare to bus topology.
  - **In this topology all nodes are connected through one system, this system is called as central system. So the network administrator has to go to the single node for resolve the issue whereas in bus topology network administrator has to pass**

through number of stations and after that he/she is able to reach the station and resolve the issues.

- **Network control:**
  - Complex network control features can be easily implemented in the star topology.
  - Any changes made in the star topology are automatically accommodated.
- **Limited failure:**
  - As each station is connected to the central system via its own cable, if any failure occurs in one cable, it will not affect the entire network system.
- **Familiar technology:**
  - Star topology is a familiar technology as its tools are cost-effective.
- **Easily expandable:**
  - Installation of new station is very easy; we just have to add this new station on the central system's open ports.
- **Cost effective:**
  - Star topology networks are cost-effective as it uses inexpensive coaxial cable.
- **High data speeds:**
  - It supports a bandwidth of approx 100Mbps. the most popular Star topology networks is Ethernet 100BaseT.

Disadvantages of Star topology

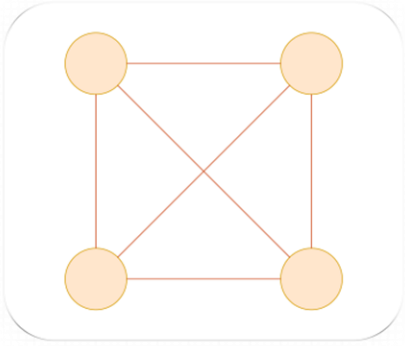
- **A Central point of failure:**
  - If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.
- **Cable:**
  - Sometimes cable routing becomes difficult when a significant amount of routing is required.

3.6 MESH TOPOLOGY

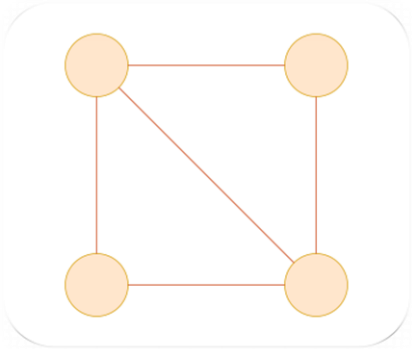
In the mesh topology, each node is interconnected to each other node using different redundant connections. There are numbers of path from one system to another system of the network. This topology is not using any switch, hub or servers as a central point of communication. This topology is used where communication failures are a critical concern like WAN implementations. Mesh topology is mainly used for wireless network. The best example of this topology is Internet.

Mesh topology is divided into two categories:

- **Full Mesh Topology:** If each node is directly connected to every other node of the network, then this is known as fully mesh topology. Following figure depicts the same.



- **Partial Mesh Topology:** In a partial mesh topology, not all but certain computers are connected to those computers with which they communicate frequently. Following figure depicts the same.



Advantages of Mesh topology:

- **Reliable:**
  - The mesh topology networks are very reliable as if any link has failure issue; it will not affect the communication between connected computers.
- **Fast Communication:**
  - Communication is very fast between the nodes.
- **Easier Reconfiguration:**
  - Adding new devices would not disturb the communication between other devices because each node is not dependent in a view of connections to other nodes.

Disadvantages of Mesh topology:

- **Cost:**
  - A mesh topology contains lots of connected devices like a router and more transmission media with compare to other topologies. This will increase the cost of network and make this topology expensive.
- **Management:**
  - The management and maintenance is too difficult because it is complex and large network. If the network is not monitored properly, the fault of the connection is not easy to connect.
- **Efficiency:**
  - In this topology, unnecessary connections are high that decreases the efficiency of the network.

So, this was all about the topologies used in computer network. Let summarise whatever we have learn in this unit.

3.7 LET US SUM UP

- Computer networks are used to transfer data between the communicating systems. Computer networks need to be intended using suitable topology and network technologies in order to be fast, reliable and easy expandable.
- Computer networking method is called topology. The term topology in the context of networks defines a way in which the hosts are interconnected in a network.
- Topology is explained as the layout of lines and switching elements and defines the data transmission pathways, which can be used among any pair of hosts.
- There are physical and logical topologies. The physical topology describes the ways of physical connections between network hosts, while a logical topology describes the data flow between network hosts.
- Bus topology is a network type in which each and every computer is connected through network device using single cable.
- Bus topology transmits data only in one direction. Every device in bus topology is connected to single cable.
- In Bus topology, if a cable fails then whole network fails.
- In ring topology, every host machine connects to precisely two other machines, creating a circular network arrangement. Ring topology is easy to install and expand.
- In ring topology, if failure of one computer or device disturbs the whole network.
- In the star topology, each station is directly connected to a general central node. Star topology provides fast performance with few nodes and low network traffic. This topology is the easiest to preserve, amongst the other topologies.
- In Mesh topology, each and every network equipment is connected to other network devices. Mesh topology is very costly because of the more numbers of cables needed and it is very complex and that why it is not easy to manage.
- The main benefit of mesh topology is numbers of paths to the destination computer. If there is failure in one link, there is alternative path to reach the destination.

3.8 CHECK YOUR PROGRESS

1) Number of links to connect n nodes in a mesh topology is = _____.
2) In BUS topology, at each end of the bus is a _____, which absorbs any signal, removing it from the bus.
3) _____ and _____ will force a maximum length of shared medium which can be used in BUS topology.
4) In Ring Topology, the links are _____; that is, data are transmitted in _____ direction only and all are oriented in the same way
5) _____ Topology can be considered as an extension to BUS topology.
6) Coaxial cable is suitable for use in _____ topology.

3.9 FURTHER READING

- Andrew S. Tanenbaum, “Computer Networks”, Prentice Hall PTR, Edition - 5
- Data and Computer Communication, William Stalling, Pearson Education, Delhi.

3.10 ASSIGNMENTS

1) List down advantages and disadvantages of bus topology, star topology, mesh topology, ring topology.
2) Explain mesh topology and star topology with suitable example.
3) Write note on ring topology and also explain working of token passing.

Unit 4: Switching and Routing in Network

4

Unit Structure

4.1 LEARNING OBJECTIVES

After studying this unit student should be able to:

- Specify what is meant by switching network
- Classify different switching network
- Categorize various switching network
- Compare circuit switching with packet switching

4.2 INTRODUCTION

Messages are sent through the network of transmission media, when a user accesses the internet or another computer network outside their immediate location. This process of transmitting the information from one computer network to another is known as switching. For switching purpose, switches are used in a computer network. A switch is a small hardware device which is used to join multiple computers together with one LAN.

Network switches operate at Data Link Layer of the OSI model. Switching is transparent to the user. It does not require any configuration in the home network. Based on MAC addresses, packets are forwarded using switches.

A Switch is used to transfer the data only to the device that has been addressed. Switch verifies the destination address to send the packet appropriately. It works in full duplex mode. In further section, we will discuss why switching is required and different types of switching methods.

4.3 REASONS FOR SWITCHING

Network administrator need switching due to following two main reasons:

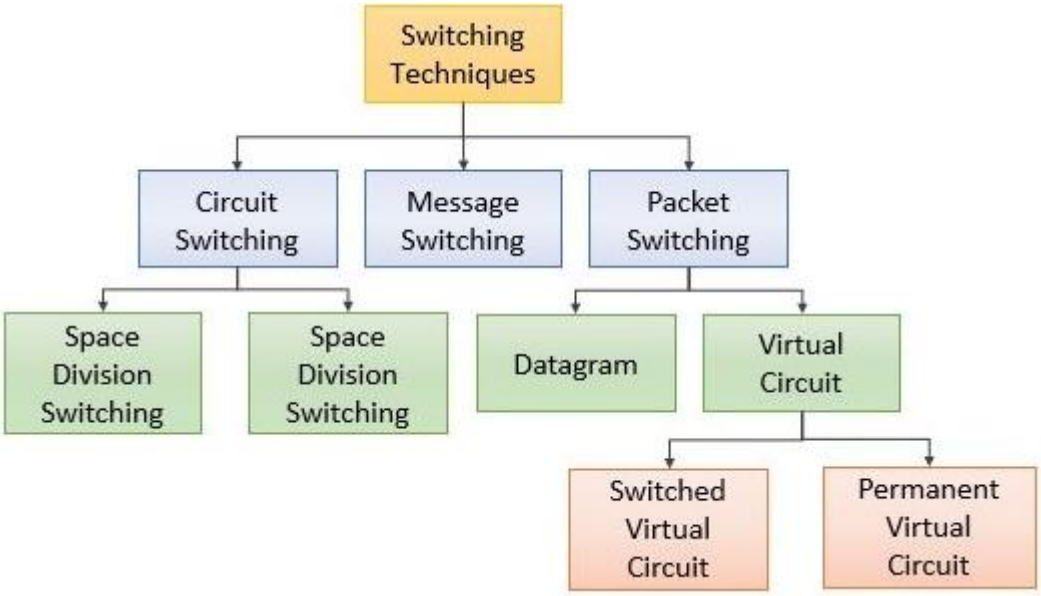
- Bandwidth:
    - Bandwidth is defined as the maximum transfer rate of a cable. It is a much critical and costly resource.
    - So that, switching techniques are used for the effective utilization of the bandwidth.

- Collision:
    - It is the effect which occurs when one or more devices transfer the message over the same physical media, and they collide with each other.
    - To solve this problem of collision of packets, switching technology is implemented.

Now let's discuss techniques for switching in detail.

4.4 SWITCHING TECHNIQUES

In large networks, there can be multiple ways from sender to receiver to communicate. The switching technique will be used to decide the best route for data transmission. For making one-to-one communication, switching technique can be used. Following figure shows the different types of switching techniques.



(Image source:https://binaryterms.com/wp-content/uploads/2021/05/Switching Techniques.jpg

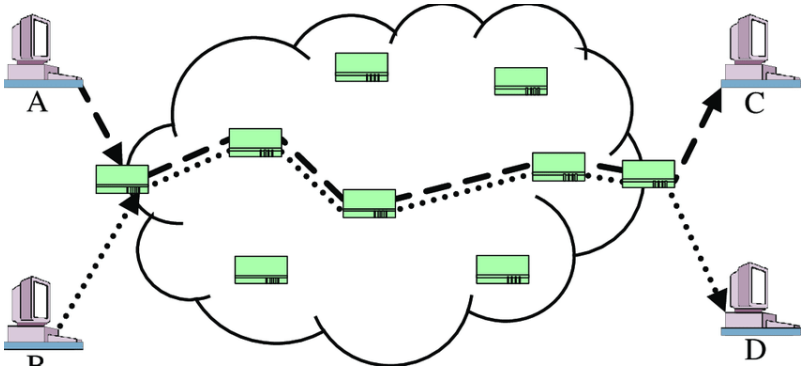
4.5 CIRCUIT SWITCHING

Circuit switching provides a dedicated path between sender and receiver. In this technique, the path exists until the connection is terminated. It operates in a similar way

as the telephone works. A complete one to one path must exist before the communication takes place.

To ensure the availability of the dedicated path the receiver sends back the acknowledgment, after getting the request signal from user for sending the data, voice, and video.

It is used in public telephone network and also used for voice transmission. Fixed data can be transferred at a time in circuit switching technology. Following figure shows the working of circuit switching.



(Image Source: https://www.researchgate.net/profile/Michele-Weigle/publication/34985230/figure/fig1/AS:669546071470086@1536643631853/Circuit-Switching-Example.png)

In circuit switching communication is taken place via three phases:

- **Circuit establishment**:
  - Establish the connection of end-to-end before the communication happened between two stations.
- **Data transfer:**
  - Data is transferred from source to destination. The data may be analog or digital, depending on the nature of the communication network.
- **Circuit Disconnect:**
  - At the end of the data transfer the circuit is disconnected.

- Resources which are allocated during the transmission are de-allocated.

There are two technologies which are used by Circuit Switching are:

- Space Division Switching
- Time Division Switching

4.5.1 Space Division Switching

In space division switching, the paths in a circuit are separated from each other geographically. In spite of initially being designed for analog networks, it is being used for both analog and digital switching. A Cross point switch is mostly considered as a space division switch as because it moves a bit stream from one circuit or bus to another circuit or bus.

In this, a single transmission path is accomplished in a switch by using a physically separate set of cross points. Crossbar switch can be used to achieve Space Division. A crossbar switch is a metallic cross point or semiconductor gate that can be enabled or disabled by a control unit.

Space Division Switches can be divided in two ways:

- Crossbar Switch
- Multistage Switch

- **Crossbar Switch:**
  - It is a switch that has N output lines and N input lines. The crossbar switch has N^2 intersection points known as cross points.

- **Multistage Switch:**
  - It is made up by dividing the crossbar switch into the smaller units and then connecting them. It reduces the number of cross points. If one path fails, then alternative path will be used.

4.5.2. Time-Division Switching

Time-Division Switching is also known as TSI (Time-Slot Interchanger). This switching involves the sharing of cross points for time periods.

Now, let’s discuss its advantages and disadvantages.

4.5.3. Advantages and Disadvantages

Advantages:

- It has fixed bandwidth.
- The devoted path/circuit recognized among sender and receiver provides a guaranteed data rate.
- Once the circuit is recognized, data is transmitted with no delay as there is no waiting time at each switch.
- The technique is appropriate for long continuous transmission as a dedicated continuous transmission path is recognized,

Disadvantages:

- Once the dedicated path is recognized, the only delay occurs is in the speed of data transmission.
- It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.
- It is more expensive than other switching methods as a dedicated path is required for each connection.
- Once the path is established and no data is transferred, the capacity of the path is wasted. Hence, it is inefficient in such cases.

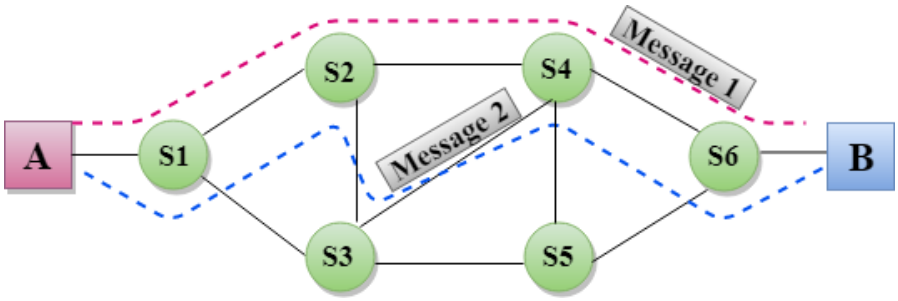
4.6 MESSAGE SWITCHING

Message Switching is a switching technique in which a message is transferred as a complete unit and passed through intermediate nodes which will be stored and forwarded. Here we have no establishment of a dedicated path between the sender and receiver.

The destination address will be there in the message. Message Switching provides a dynamic routing as the message is routed or passed through the intermediate nodes based on the information which is available in the message.

Message switches are programmed in particular manner so that they can provide the most efficient routes. Each and every node stores the entire message and then forwards it to the next. This is known as store and forward network. Message switching

treats each message as an independent entity. Following figure shows the working of message switching.



(Image Source:https://static.javatpoint.com/tutorial/computer-network/images/switching-techniques-message-switching.png)

Characteristics of message switching networks:

- **Store and forward:**
  - The middle nodes have the responsibility of transmitting the message to the next node. So, each node must have storage capacity. If the next hop and the link connecting it are both accessible, or else it will be stored for an indefinite period, at that time only message will be delivered.
  - It forwards a message only if sufficient resources are available as well as the next hop is accepting data. Hence, this is called the store-and forward property.
- **Message delivery:**
  - This involves packaging the whole information in a single message and transferring it from the source to the destination node.
  - Every message must have a header that contains the message routing information, with the source and destination.

Now, let's discuss advantages and disadvantages of message switching.

Advantages:

- Data channels are shared between devices to improve bandwidth.
- Messages can be stored at message switches, when network congestion becomes a trouble.

- It helps in reducing traffic congestion.
- The message may be provisionally stored in the route and then forwarded when required.
- It is accommodating in setting the message priorities due to store and forward method.
- It can used to manage network traffic.

Disadvantages:

- As message length has no limit, each switching node must have fix storage to buffer message.
- Storing and forwarding the massage capability introduces delay which makes message switching inappropriate.
- It requires adequate storage at every switch to accommodate the whole message during the transmission.
- It is enormously slow due to store and forward method.
- Also, the message has to wait until adequate resources become accessible to transfer it to the next switch.
- The Long delay may happen due to the storing and forwarding facility provided by this.

4.7 PACKET SWITCHING

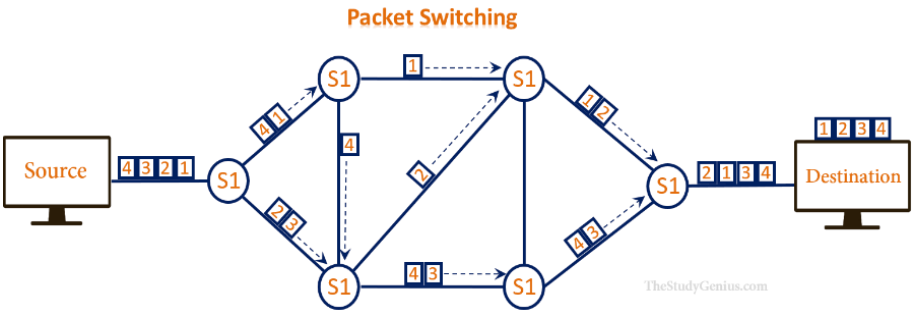
It is a technique in which the message is sent in one go, but it is divided into smaller pieces and they are sent individually.

The message divided into smaller pieces known as packets and packets are given a unique number to identify their sequence at the receiving side. Every packet contains some information like source address, destination address and sequence number in its headers.

Packets will travel throughout the network and taking the shortest path as much possible as. All the packets are reassembled at the receiving side in particular order. If

any packet is missing or corrupted, then the acknowledgement will be sent to resend the message.

If the correct order of the packets is reached, then the acknowledgment message will be sent. Following figure shows the same.



(Image Source: https://www.thestudygenius.com/wp-content/uploads/2020/08/Packet-Switching-1.png)

4.7.1. Approaches of Packet Switching:

There are two approaches:

- Datagram Packet switching
- Virtual Circuit Switching

Datagram Packet switching:

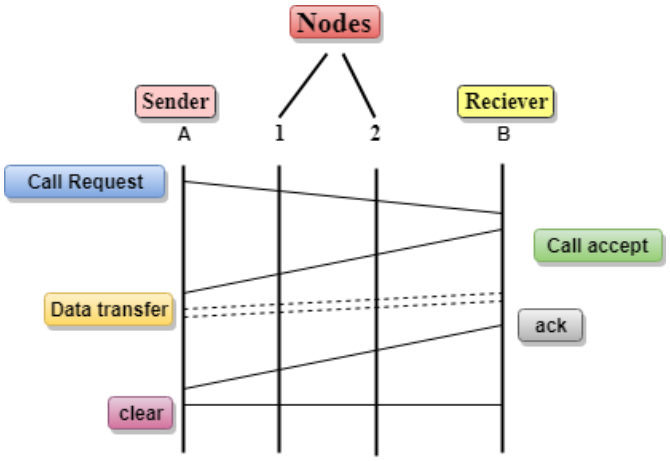
- It is a technology in which a packet is known as a datagram, which will be considered as an independent entity.
- Each packet contains the information about the destination and switch uses this information to forward the packet at the correct destination. The packets are reassembled at the receiving end in order.
- The path is not fixed un this technique. Intermediate nodes take the routing decisions to forward. It is also known as connectionless switching.

Virtual Circuit Switching:

- It is known as connection-oriented switching.
- In this, a pre-planned route is established before the messages are transmitted.

- Call request and call accept packets are used to establish the connection between both sides.
- The path is fixed for the duration of a logical connection.

Following figure shows the concept of virtual circuit switching through a diagram:



(Image Source: https://bit.ly/3w68Fb5)

- In the above diagram, A and B are the sender and receiver respectively. 1 and 2 are the nodes.
- Call request and call accept packets are used to establish a connection between the sender and receiver.
- When a route is established, data will be transferred.
- After transmission of data, an acknowledgment signal is sent by the receiver that the message has been received.
- If the user wants to terminate the connection, a clear signal is sent for the termination.

Now, let's discuss differences between both the approaches.

Datagram approach	**Virtual Circuit approach**
Node takes routing decisions to forward the packets.	Node does not take any routing decision.
Congestion cannot occur as all the packets travel in different	Congestion can occur when the node is busy, and it does not allow

directions.	other packets to pass through.
It is more flexible as all the packets are treated as an independent entity.	It is not very flexible.

4.7.2. Advantages and Disadvantages of Packet Switching

Advantages:

- Delay in delivery of packets is fewer, seeing as packets are sent as soon as they are accessible.
- Switching devices don't need large storage, since they don't have to store the whole messages before forwarding them to the next node.
- Data delivery can continue even if some parts of the network face link failure. Packets can be routed via other paths.
- It allows instantaneous usage of the similar channel by multiple users.
- It makes sure enhanced bandwidth usage as a number of packets from multiple sources can be transferred via the similar link.

Disadvantages:

- They are inappropriate for applications that cannot afford delays in communication.
- It has high installation costs.
- It requires complex protocols for delivery.
- Switching nodes for packet switching need huge amount of memory to handle great quantities of packets.
- If the network is overloaded or corrupted, then it requires retransmission of lost packets.
- It can also lead to the loss of critical information if errors are not recovered properly.

This was all about switching and its various techniques. Not at last, we need to learn the basic concept of routing. So let's discuss the same in brief.

4.8 INTRODUCTION TO ROUTING

Routing is a process of selecting path along which the data can be transferred from source to the destination. It is performed by a special device known as a router.

A Router works at the network layer in the OSI model and internet layer in TCP/IP model. A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.

Various routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.

The routing protocols use the metric to determine the best path for the packet delivery. The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path, etc. used by the routing algorithm to determine the optimal path to the destination.

The routing algorithm initializes and maintains the routing table for the process of path determination. Now, let's discuss types of routing in brief.

4.9 TYRES OF ROUTING

Routing can be classified into three categories:

- Static Routing
- Default Routing
- Dynamic Routing

Static Routing:

- Static Routing is also known as non adaptive routing.
- It is a technique in which the administrator manually adds the routes in a routing table.

- A Router can send the packets for the destination along the route defined by the administrator.
- In this technique, routing decisions are not made based on the condition or topology of the networks

Following are the advantages of Static Routing:

- **No Overhead:**
  - It has no overhead on the CPU usage of the router. So, the cheaper router can be used to obtain static routing.
- **Bandwidth:**
  - It has not bandwidth usage between the routers.
- **Security:**
  - It provides security as the system administrator is allowed only to have control over the routing to a particular network.

Following are the disadvantages of Static Routing:

- For a large network, it is a very difficult task to add each route manually to the routing table.
- The system administrator should have a good knowledge of a topology to add each route manually.

Default Routing:

- Default Routing is a technique in which a router is configured to send all the packets to the same hop device, and it doesn't matter whether it belongs to a particular network or not.
- A Packet is transmitted to the device for which it is configured in default routing.
- Default Routing is used when networks deal with the single exit point.
- It is also useful when the bulk of transmission networks have to transmit the data to the same device.

- When a specific route is mentioned in the routing table, the router will choose the specific route rather than the default route. The default route is chosen only when a specific route is not mentioned in the routing table.

Dynamic Routing:

- It is also known as Adaptive Routing.
- It is a technique in which a router adds a new route in the routing table for each packet in response to the changes in the condition or topology of the network.
- Dynamic protocols are used to discover the new routes to reach the destination.
- In this routing, RIP (Routing Information Protocol) and OSPF (Open Shortest Path First) are the protocols used to discover the new routes. If any route goes down, then the automatic adjustment will be made to reach the destination.

Advantages of Dynamic Routing:

- It is easier to configure.
- It is more effective in selecting the best route in response to the changes in the condition or topology.

Disadvantages of Dynamic Routing:

- It is more expensive in terms of CPU and bandwidth usage.
- It is less secure as compared to default and static routing.

4.10 LET US SUM UP

In this unit, we have seen the procedure of moving the data packets towards their destination by forwarding them from one port to the other. It is called as switching. We have discussed switching techniques such as Circuit Switching, Message Switching, and Packet Switching.

Circuit switching technique operates on three phases like establishment of a circuit, transferring the data, disconnecting the circuit. It has its own advantages and disadvantages. Message switching requires enough storage at every switch to accommodate the entire message during the transmission. Packet Switching technique cannot be implemented in applications in which require low delay and high-quality services. At last, we have seen routing and its types.

4.11 FURTHER READING

- Andrew S. Tanenbaum, “Computer Networks”, Prentice Hall
- PTRComer, Douglas E., and Ralph E. Droms. Computer networks and internets. Prentice-Hall, Inc.,
- Data and Computer Communication, William Stalling, Pearson Education, 2nd Edition, Delhi.

4.12 ASSIGNMENT

1. Describe the need of switching and define a switch.
2. Compare and contrast a circuit-switched network and a packet-switched network.
3. What are the three basic steps involved in data communication through circuit switching?
4. Mention the key advantages and disadvantages of circuit switching technique.