MADHYA PRADESH BHOJ(OPEN) UNIVERSITY BHOPAL

Computer Networks

POST GRADUATION DIPLOMA IN CYBER SECURITY

Madhya Pradesh Bho□
Open University

PGDCS-102

Fundamentals of Computer Networking

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 OBJECTIVE

After studying this unit student should be able to:

- Understand basic concept of data communication and networking
- Identify the components of data communication
- Explain fundamental of networking models
- Categorize different types of network
- Explain basic functions of networking devices

1.2 INTRODUCTION TO NETWORKING

Business decisions have to be made quickly in this time of online commercial activities. Computers have resulted extreme improvement for business, industry, science and technology.

Likewise, data communication and networking also made same effect. Advance technology research progressed remarkable which can do job for us very quickly.

Computer Network is required to send the data from one place to another.Two remote machine can communication with each other through a process called networking. The communication means exchange of data with the help of set of protocols and networking devices.

Computer network mainly consist of two parts. One is the software and other is the hardware. The software is a stack of computer network protocols. The hardware part is collection of devices such as cable, switch, hub, router etc.In simple terms, protocols are a set of rules. Those rules are to be followed by each entity of computer network.

Any Computer Networking communication need a sender, a receiver and a communication medium to transfer signal or Data from sender to the receiver. One needs sender, receiver, communication channel, protocols and operating system to establish a computer networking.

What is Data Communication?

When two people talks with each other, they are said to be communicating with each other. They exchange their ideas, thoughts, opinions, feelings with the help of words of some natural language.

Similarly, when two computers exchange the information using some set of rules and networking devices, the process is said to be data communication. The information is presented in the form of data.

The data may take various forms such as text, audio, video, images etc.

To have successful data communication, it must satisfy several characteristics.

1) Correctness of data communication

First, the data must be received correctly by the remote receiver. Putting in simple words, the data which sender has transmitted, receiver must receive the same data bit by bit. There must not be a single bit in error.

For example, we assume that sender have sent the binary stream 110101. Then receiver must receive exactly110101.

2) Timeliness

Data must be received timely. The data are not useful if it arrives out of time. It means that sender and receiver must be synchronized with the order of transmission and receiving. The sender might have sent the whole message in the several units. The receiver must receive the whole message in the same sequence of units.

For example, sender is sending the video message to the receiver. The whole video message is transmitted in small parts. Then receiver can understand the message if all parts of the video message arrives at receiver in the sequence. This is applicable for audio form of the message too.

3) Correct destination

The data must be received by the machine to which data actually has been transmitted. It must not reach to any other destination.

1.3 COMPONENTS OF NETWORKING

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

The hardware components are mentioned below.

Hub - Hub is a central device to which all machines are connected. Whenever a sender machine transmits the message, it is sent through the hub. The hub is kind of broadcasting device. So it will receive the request and transmit it to the entire network. The intended receiver will accept the message and all other computers will ignore the message. It is used for N-to-N communication. Here, N indicates all computers of the network.

Switch - Switch is networking device as one of computer network components. It looks like hub but it does not work similar to the hub.It has got built-in memory and intelligence. It sends the data to the specific receiver. It uses physical device addresses in each incoming messages so that it can deliver the message to the right destination or port. It is used for point-to-point (P-to-P) communication. Here, P indicates identificationof a specific computer.Both switch and hub have common features: Multiple RJ-45 ports, power supply and connection lights.

Router –Routers are mainly used to send the message from source machine to the destination machine. There is a large number of routers are connected among themselves. Hence, there may be several alternative paths from source router to the destination router. Router finds the best possible path between them using routing algorithms and routing table information. Router tables are used to stores information of other neighbour routers in the network. Router also can be used to connect LANs, MANs or WANs.

Repeater – It strengthen the weak signal. If distance between two directly connected computers is long, then the signal which passes through may get weaker and weaker. So the receiver may not get the correct data as it was transmitted. In this case, a repeater is placed between these two computers. When signal becomes weak, repeater makes it strong such that it reaches to the destination without any difficulty.

Cables – Computer network can be established thorough wires. The wire connects a computer to another computer or to the central device. There might be wireless network or mixture of wire and wireless connection.

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.

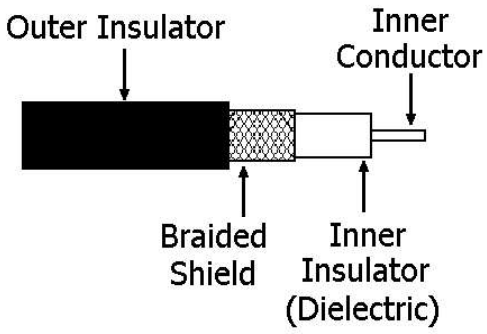


Fig – Coaxial Cable

- **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.

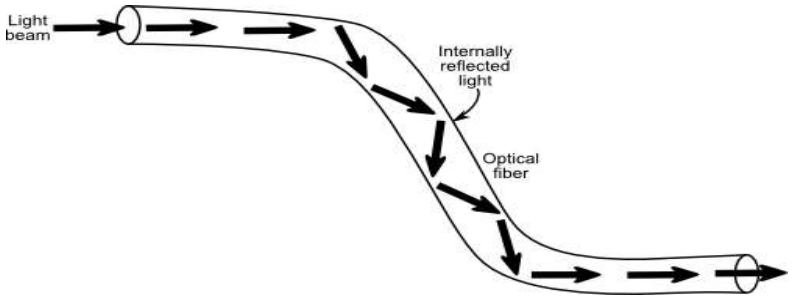


Fig – Fiber optics cable

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

Network Interface Card –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.

Servers - Servers are computers that hold shared files, programs, and the network operating system. Servers provide access to network resources to all the users of the network. There are many different kinds of servers, and one server can provide several functions. For example, there are file servers, print servers, mail servers, communication servers, database servers, fax servers and web servers, to name a few.

Network Interface Card - Each computer in a network has a special expansion card called a network interface card (NIC). The NIC prepares (formats) and sends data, receives data, and controls data flow between the computer and the network. On the transmit side, the NIC passes frames of data on to the physical layer, which transmits the data to the physical link. On the receiver's side, the NIC processes bits received from the physical layer and processes the message based on its contents.

1.4 LOCAL AND WIDE AREA NETWORK

The network can be categorized with respect to several criteria. Some of them are geographical boundary in which the networkexpanded, type of delivery, mode of communication. We categorize the network based on the size first.

LOCAL AREA NETWORK

It connects the networking devices in single office, building or campus. It mainly spans based on the need of organizations.

Generally, a network which is formed within fewkilometers peripheral can be said as Local Area Network.For instance, in an academic institute, an interconnection among the computers can be considered as Local Area Network. Similarly, several computer laboratories are connected to form the Local Area Network only.

LAN has been designed to share various hardware and/or software resources. Resources may contain printer, scanner etc. Software resources might be data, tools, programs etc.The speed in LAN was 4 to 16 mbps earlier. Now-a-days the speed can be achieved upto 100 to 1000 Mbps.

The computers and other devise in LAN might be interconnected via a central device such as switch or hub. Wireless LAN are also have been getting popularity as it needs no cabling or minimum cabling.

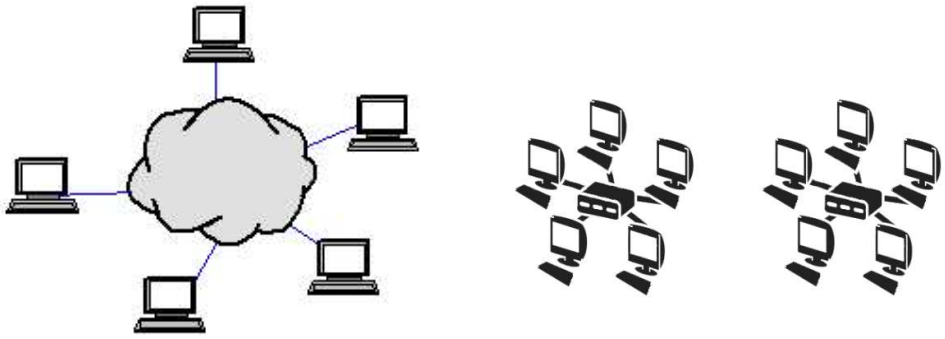


Fig – Local Area Network

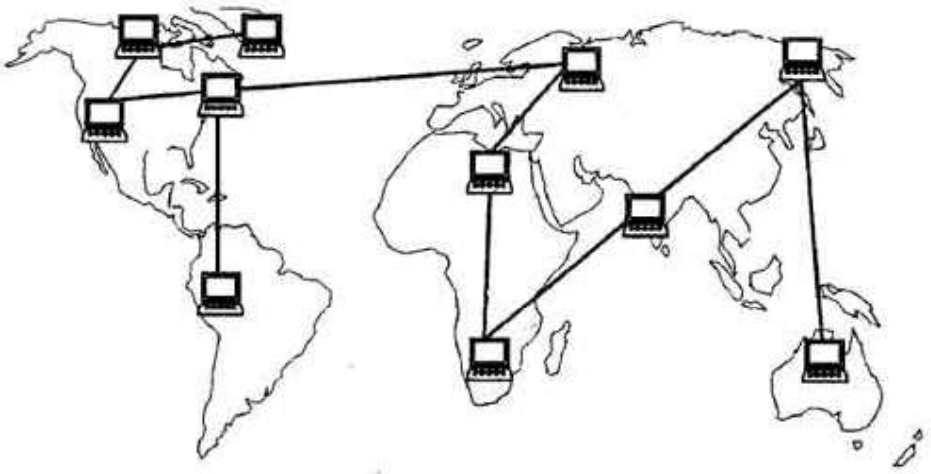
WIDE AREA NETWORK

Wide Area Network (WAN) had been designed to transmit the data for the long distance.

WAN may covers the large geographical area such as a country, a continent or across the world. The internet of the whole world can be considered as a WAN.

A WAN of one country or a continent is connected to the WAN of another country or continent, it forms WAN. Therefore, the Internet is connection of all Wide Area Network of all countries of the world.

WAN can be wired, wireless or mixture of both.



Wide area network

METROPOLITAN AREA NETWORK

Metropolitan Area Network (MAN) is the larger than LAN and smaller than WAN in size. Mainly, it expands within the boundary of a city or town.

The customer can be provided high speed connectivity using MAN. For example, A TV cable operator offers the service at high speed. Similarly, a telephone company provides the networks of DSL line across the city.

1.5 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.

Client-Server Network

A computer network in which one centralized, powerful computer is called the server. There are several less powerful computers are connected with server called clients. The server owns numerous resources such as printers, scanners, files, video etc. The server's primary purpose it to provide services to the clients connected with it. Whenever a client demands for the specific resources, the server locates that resource and provides to the client.

There are two settings in the client-server network. First, all clients have the same set of access of privileges. In this case, all clients can use the same set of resources. In the second case, two different clients have different resources to access.

The main benefit of the client-server network setup is that all resources are to be placed on one place. The network administrator can control all the resources from the server only. It becomes easy to control and maintain the whole network. Moreover, software and hardware resources are shared. So it results in cost-effective environment. On the other side, all clients depends upon the server. Therefore, if server fails, then the whole network goes down.

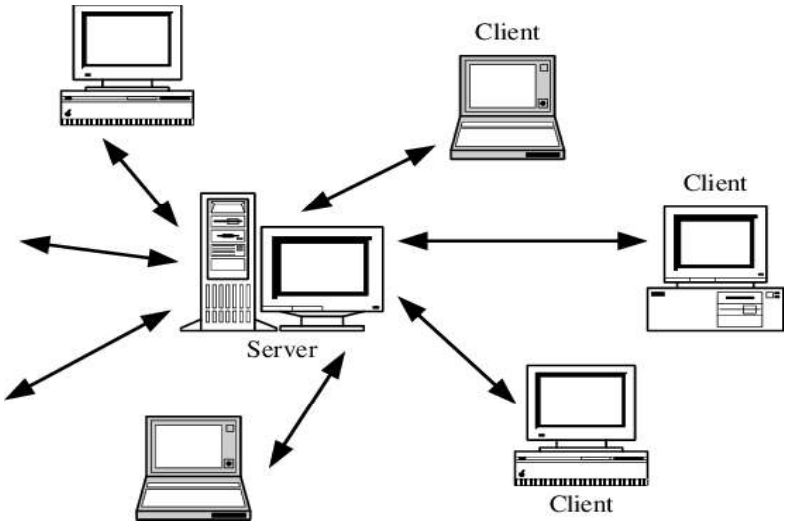


Fig – Client-Server Network

Peer-to-Peer Network

A peer-to-peer (P2P) network is a network in which all connected computers are neither servers nor client. A P2P network can be an ad hoc network – a couple of computers are connected through media to share the resources. It is set-up for

temporary. In contrast, a P2P network may own permanent infrastructure. For example, 10 to 12 computers are interconnected in a small office to share the printer. In simple words, it does not require any configuration such as access privileges.

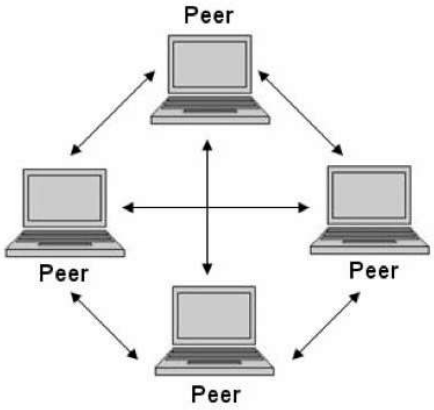


Fig – Peer-to-Peer Network

Centralized Computer Network

Another logical classification of computer networks is Centralized and Distributed Computer Network Model.

All resources are placed on one machine only. Moreover, all computing process are done on a dedicated computer only. For example, if there are three documents to be shared among N computers, then all the documents would be stored on a specific computer. A node or a computer needs any resources or set of resources, it demands that from centralized machine.

Characteristics of Centralized computer network

- Homogeneous – all computers have same type of configuration, such as Operating System, processing power,RAM
- Single point of failure – if central computer fails, then resources can't be accessed at all
- The network is controlled from a single point
- Difficult to scale – e.g more computers are to be added in the existing network
- Easy administration

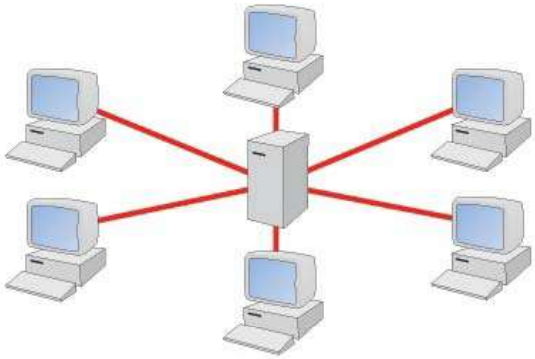


Fig – Centralized Computer Network

Distributed Computer Network

In Distributed network model, the network resources are placed on more than one computers. The processing also is done on different computers. The computers are located on different geographical locations. The resources are distributed among them. The resources might have been distributed on all computers or group of computers.

Characteristics of Distributed computer network

- Heterogeneous – computers may have different type of configuration, such as Operating System, processing power, RAM
- Shared resources – Resources are shared and replicated, so in case of failure the same can be fetched from other computer(s)
- The network is controlled from multiple points
- Easy to scale
- Not so easy administration

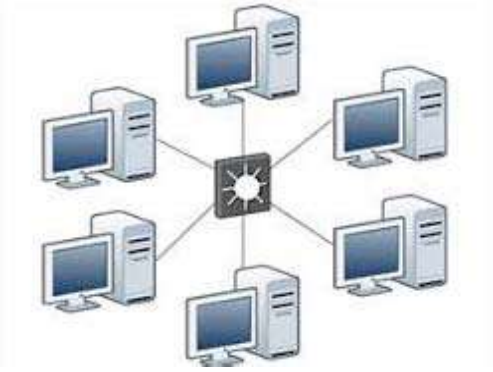


Fig – Distributed Computer Network

Collaborative Computer Network

Collaborative computer network model is a diverse group of networking devices intended to support work between individuals. Collaborative model uses the applications such as chat programs, instant messaging, and video conferencing. These applications empower users to access each other and information whenever it is required.

1.6 LET US SUM UP

A computer network is the interconnection of devices those send and receive information among them. There are several networking devices such as hub, switch, cable, router, repeater etc. There are several computer network models, such as client-server verses peer-to-peer, distributed computer network verses centralized computer network or collaborative network. Moreover, computer network can be classified as Local Area Network, Metropolitan Area Network or Wide Area Network. The classification is based on the geographical expansion of the computer network.

1.7 CHECK YOUR PROGRESS

1) True-False

1. All machines have different access privileges in peer-to-peer network.
2. Computer network is a set of protocols.
3. Hub is a broadcasting device.
4. Switch is used for point-to-point communication.
5. The function of repeater and switch is the same in computer network.
6. The router is for forwarding the packet from source to destination.
7. A computer network of government office is a category of WAN.
8. A network of landline telephone is the category of MAN.

2) Match the following.

A	B
Local Area Network	All resources are placed on server machine
Wide Area Network	Building or office network
Peer-to-Peer Network	Network expanded across city
Client Server Network	Resources are placed on more than one computers
Distributed Network	Network of whole country
MetropolitanArea Network	All computers have equal priority

3) Fill in the blanks

1. Hub is a _____ device. (broadcasting, point-to-point)
2. Switch is a _____ device. (broadcasting, point-to-point)
3. Repeater _____ regenerate the digital signal.

4) Multiple choice

- Combination of two or more networks are called

  A. Internetwork
  B. WAN
  C. MAN
  D. LAN

- A communication path way that transfers data from one point to another is called

  A. Link
  B. Node
  C. Medium
  D. Topology

- Network providing a high speed connectivity is

  A. MAN
  B. LAN
  C. WAN

D. Internetwork

- Nodes are another name of

  A. Devices
  B. Links
  C. Medium
  D. Modes

- Cable TV and DSL are examples of

  A. Interconnection of network
  B. LAN
  C. MAN
  D. WAN

- Network that is usually owned privately and links devices in single office is called

  A. MAN
  B. LAN
  C. WAN
  D. Internetwork

- In 10Base2, cable is

  A. Thick
  B. Thin
  C. Twisted Pair
  D. None of the above

- NIC stand for

  A. Network Interface Card
  B. National Internet code
  C. Network Isolated card
  D. Network international code

5) Why computer network is highly needed for business activities?
6) What kind of applications needs to have distributed computer network?
7) How does client-server computer network differ from peer-to-peer computer network?

1.8 FURTHER READING

- Recommended Text

1) Forouzan (2013). Data Communication and Networking – 5E, McGraw Hill

2) Andrew S. Tanenbaum and David J. Wetherall (2011). Computer Networks - 5th Edition

1.9 ASSIGNMENTS

1) Differentiate LAN, MAN and WAN.
2) Compare centralized and distributed computer network model.
3) Discuss the characteristics of peer-to-peer network model.

1.10 ACTIVITIES

Activities are required to:

- Set-up a peer-to-peer network of 5 computers as a part of laboratory work.
- Design diagram of the computer network of your department/institute.

Unit 2: Intranets and Internets Network Services

2

Unit Structure

2.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Explain what is internet and intranet services
- Describe what is file services and FTP
- Explain database server
- Explain email server
- Explain how printing service would be useful concerning resource sharing
- Explain how remote login can be done using TELNET server

2.2INTRANETS AND INTERNETS NETWORK SERVICES

Computer network may provide services within the local network and over the internet. A server is a program or devices which provides services to the entity called client. This type of computer network architecture is known as client-server architecture. The service might include data or resource sharing. Many clients may access single servers, and single client may avail service from many services. A client runs on single machine. A server may distributed services over many devices. Example of servers may include database servers, mail servers, print servers, file servers, web servers, application servers, and game servers.

Client-server works on request-response concept. A client makes request to the server for the specific service. The intended server performs some actions and then sends the response back to the client. Normally, response composed of service which client demanded for. But sometime server replies the negative response if it is not capable to provide the service at that moment.

Database server

- Database server is the computer used to run the back-end system of a database application using client/server architecture. The back-end, sometimes called a database server, performs tasks such as data analysis, storage, data manipulation, archiving, and other non-user specific tasks.

- The database server also provides concurrent access control, integrity constraint management, locking mechanisms, transaction management, backup and recovery.

- User can deal with database through various mode of access. For example, one may interact with database through website. A user also can use some client program to access the database.

- The database server is replicated for the backup and recovery purpose. The primary database server is used to store and retrieve the data. The primary server synchronizes with the secondary server at regular interval.

Mail servers

- A mail server is the computerized version of conventional mailing system. When a person sends an email, it reaches to the receiver through the mail server.
- The sending of an email is quite complex process. The user does not get feel of this because the email is transferred from sender to the receiver in the blink of an eye.
- There are three types of email server protocols.
    1. When one sends an e-mail, the client email program will connect to a server called an SMTP server. SMTP is an acronym for Simple Mail Transfer Protocol and it is a protocol that is used when e-mails are delivered from clients to servers and from servers to other servers.
    2. A POP3 server uses a protocol named POP3 for its communication. That is the reason why it is called a POP3 server and POP3 is an acronym for Post Office Protocol version 3.
    3. IMAP4 is a further development of the POP3 protocol and is used to read e-mail from mail servers. IMAP4 is not used as much as POP3, but many modern mail but many modern mail servers have support for IMAP4.

Game server

- The gaming is one of the most demanding service for the game lovers. A video game is a computer program created for entertainment, based on the interaction between one or more persons and an electronic device that executes the video game, this electronic device can be a computer, an arcade system, a game console, handheld device or mobile phone.
- In many cases, video games recreate virtual environments and circumstances in which the player can control one or more characters.
- The games are played either offline or online.
- There are a numerous online games which attracts users. The online game comprises of a game client and a game server. Moreover, games are also classified by single player or multiplayer game.
- A game client is a software program that connects to a game server. The server provides the connection and sends packets of information to the client.
- A game server is a local or remote server used by game clients to play multiplayer games
- Many clients can connect to the server at the same time, and will maintain an overview of the game world.

2.3FILE SERVICES

A file server is a computer attached to the computer network that have shared storage. The shared storage stores computer files such as text, audio, video, images etc. The shared storage can accessed by authorized workstation which is connected in that network.

Characteristics of file servers

- ✓ File server does not perform in computation. It does not execute any program on the client request.
- ✓ It mainly allows clients to access the files and retrieve the files.

- ✓ File servers are configured normally for local area network. However, there are file server available for the wide area network or Internet.
- ✓ File server may be one of two types, dedicated and non-dedicated.
- ✓ A dedicated file server is designed only for accessing files for reading and writing.
- ✓ Internet file servers are accessed by File Transfer Protocol (FTP) or Hyper Text Transfer Protocol (HTTP).
- ✓ The file servers on LAN are accessed by SMB/CIFS or NFS protocol.

The design of file server

- ✓ The file server can be designed concerning several points such as speed of access of the files, storage spaced needed, security, cost, recoverability.
- ✓ Moreover, file server design is subject to change when modern technology replaces the old technology.
- ✓ Robust protocols and methods are to be implemented to provide throughput and response time.
- ✓ Design of file server may also focuses on load balancing aspects. It comes into play when server gets hit from large number of clients.
- ✓ Storage is the primary component of the file servers. The disk array environment must be supported.
- ✓ The disk array increases the level of availability. In addition, the design should include advance functions such as RAID and storage visualization.
- ✓ File server must impose the security aspects over the accessible storage. In simple words, it must allow only authentic workstation to access the files.
- ✓ The security for the file server can be implemented by active directory.

2.4FILE TRANSFER PROTOCOL

This is a process of moving a file from remote computer to local computer. 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. The network supports users to locate the specific files on the internet. FTP

resolves several issues related with transferring files between two different computers. 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 have 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.

2.5PRINTING SERVICES

Print server enables network administrator to manage the printing queue in the shared network environment. Basically, print server is an application or computer that manages the print requests coming from various computers of the LAN.

Instead of setting up printer for each individual computer, it would be cost effective to have a single shared printer among multiple computers. The shared printer saves

initial cost and maintenance cost. In the small scale offices, a central hub performs the task of print server.

How does print server work?

- ✓ It accepts the print requests from the computers of that network.
- ✓ It sends the print request to the appropriate printer.
- ✓ It handles the queue of the printing requests.
- ✓ It examines the queue, reorder the queue and delete the print job sometime.
- ✓ It also set some policies, such as restricting the number of colour prints during the definite time span, departmental/individual authentication or watermarking printing documents.
- ✓ It has to perform page counting sometimes.

- A print server would be either a networked computer with one or more shared printer connected with it. This networked computer is not dedicated for the print server only.

- On the other end, a dedicated print server device is designated for print server relevant jobs only. A printer may have a built-in print server.

- A print server might have been integrated with wireless router or firewall too. Print servers may support a variety of industry-standard or proprietary printing protocols including Internet Printing Protocol

2.6 APPLICATION SERVICES

An application server is a software application in computer that provides business logic for an application program. An application server comprises of three components: A graphical user interface, a business logic and a database server. It also may be viewed as three tier architecture.

1. Front end – front end contains graphical user interface. It runs on the client machine.

2. Back end – Database server runs as a back end.
3. Business logic is part of middle layer.

Web server is also known as application server. The web server develops the dynamic web pages, which is interactive environment basically. Moreover, application server also offers service as load balancing, clustering, cloud storage and service on demand.

Application server based on technology

- Java application servers – java platform, Enterprise edition defines core set of Java APIs and java application servers.
- Microsoft Application server - .Net framework technology defines the Microsoft application server.
- PHP application server – It runs PHP applications.
- Mobile application server – It supports mobile application development and deployment of mobile applications.

2.7 TELNET SERVICE

Telnet allows to connect to the remote host over a TCP/IP network. The telnet client make connection with telnet server. After establishing the connection successfully, the client becomes the virtual terminal. It allows to interact with remote host from the client machine virtual terminal only. Many operating systems such as Windows, Unix, Linux, MacOS etc. facilitates command-line telnet clients.

Telnet does not encrypt the data including password which are sent over the connection. Therefore, there is a serious issue of eavesdropping. The person, who have access to the central device such as hub, can intercept the data easily. In addition, intruder can also steal the data through some packet analyser tool. Most implementations of Telnet have no authentication that would ensure communication is carried out between the two desired hosts and not intercepted in the middle.

2.8LET US SUM UP

Internet and intranet offers services for the ease of communication. It includes file server, File Transfer Protocol (FTP). Email server, print server, database server, web server, game server etc. Database server is the computer used to run the back-end system of a database application using client/server architecture. An email server is the computerized version of conventional mailing system. When a person sends an email, it reaches to the receiver through the mail server. The email server uses protocol such as SMTP, POP3, and IMAP. Game lovers uses the game server for online gaming, which runs for multiuser environment. The file server is for storing the files in shared and distributed environment. File Transfer Protocol (FTP) is the best protocol for copying files from one computer to another over the internet. Print server enables network administrator to manage the printing queue in the shared network environment. Basically, print server is an application or computer that manages the print requests coming from various computers of the LAN. An application server is a software application in computer that provides business logic for an application program. An application server comprises of three components: A graphical user interface, a business logic and a database server. It also may be viewed as three tier architecture. Telnet allows to connect to the remote host over a TCP/IP network. The telnet client make connection with telnet server.

2.9CHECK YOUR PROGRESS

- Fill in the blanks:

  - File Transfer Protocol works on well-known port _____.
  - 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

2.10 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

2.11ASSIGNMENTS

- 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.

2.12ACTIVITIES

- 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: Fundamental of Communication Theory

3

Unit Structure

3.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Explain how communication takes place in the form of signal
- Differentiate between analog signal and digital signal
- Discriminate between periodic and aperiodic signal
- Explain features of the signal
- Explain the cause of transmission impairment
- Define different types of noise in the signal

3.2 FUNDAMENTAL OF COMMUNICATION THEORY

The information may be presented in any of the forms, such as text, image, audio or video. The sender or receiver may need any of the form or combination of them. No matter which form is used, the transmission of the information in the media will be in the form of signals only. Therefore, the data or information first needs to be converted into signal. Then signal will be sent in the transmission cable. At the sender side, the information is first converted in the binary format using some encoding technique such as Manchester encoding. Consequently, binary data stream is converted to signal. On the receiving side, it converts the signal to the binary format. And finally, binary format will be converted to actual form of the information.

For example, the sender A wish to transmit a photograph to the receiver B. The image of photograph is represented by pixel. Each pixel is represented by 8 bits. Likewise, all pixels of whole photograph is then transformed to the binary. This binary stream is represented in signals form. These signals travel in the transmission media from one end to another end. The receiver B would follow the process in reverse order that of sender has followed, i.e. from signals to the binary and from binary to the photograph.

3.3 ANALOG AND DIGITAL SIGNAL

The information can be represented by either analog signal or digital signal. Analog signal is a continuous signal. For example, human voice can be considered as analog signal. An analog signal is represented by sin waves. An analog signal is described by amplitude, frequency, phase or period. It does not has any fixed range. Amplitude illustrates the maximum peak of signal. Frequency is about the rate at which signal is changing. Phase indicates the position of the wave with respect to time zero. Analog signal can be classified into simple and composite signal. Analog signals are more probable for distortion or noise. Analog signals are best for audio data transmission. Analog signal processing can be done in real time and consumes less bandwidth.

Digital signal carries information in discrete value form, unlike continuous form in analog signal. A digital signal is denoted by square waves. Digital signal represents information in bits. The data in CD/DVD are stored in form of binary, i.e. 0 and 1. Digital signals can be characterized by bit rate or bit interval. Bit rate is about number of bits can be sent within a unit of time. Digital signals are less probable for getting affected by noise.

3.4 PERIODIC VERSUS APERIODIC SIGNAL

Another category of signal is periodic and aperiodic. Analog signal and digital signal can be either periodic or aperiodic signal too.

A signal is said to be periodic signal if it completes a pattern within a unit of time, known as period. It repeats that pattern over consequent identical periods. A simple periodic analog signal such as sine wave or cosine wave cannot be decomposed into simpler signals. A composite periodic analog signal is composed of multiple sine waves. The figure depicts typical composite periodic signal. The units

such as seconds(s), milliseconds (ms), microseconds (μs) or nanoseconds (ns) are considered as a unit of time.

A signal is considered as aperiodic or non-periodic when it does not repeat its pattern or cycle over a regular interval of time. A signal produced in telephone when a word is pronounced is a good example of aperiodic signal. The signals broadcasted by AM radio station or FM radio station also are examples of periodic signals.

Peak Amplitude

Basically, each signal (any combination of periodic/aperiodic or digital/analog) carries some energy. The energy indicates the strength of the signal. Peak Amplitude of a signal is the maximum hike of the wave from the symmetry line.

Peak-to-Peak Amplitude is the distance from a negative peak to a positive peak. In the case of the sine wave, the peak-to-peak value is exactly twice the peak value because the waveform is symmetrical. The electrical signal's peak amplitude is denoted in volts.

Bit rate

In data communication, bit rate is referred as number of bits can be transmitted per unit of time. The unit of time is second generally. Bit rate ranges from bps for smaller values to kbps, Mbps or Gbps for larger value. The bps is non-standard abbreviation for bit rate. The standard symbol is bis/s, so 1 kbps is used for 1000 bits are transmitted per second from source to destination. In most of data communication environment, bit rate is replaced by Byte rate, which is Byte per second (Bps).
Bit rate is represented in baud rate sometimes. Baud rate is number of symbols per second. A symbol is denoted by some number of bits. So, if a symbol requires more than one bits, then bit rate would be greater than baud rate.
Baud rate (symbol rate) = bits per second / number of bits per baud (symbol)

Frequency

We learned that period is number of time units, a signal needs to complete 1 cycle. Frequency is number of periods in 1 second. So, one can say that frequency and period are inverse of each other. Say, T denotes period and f denotes frequency.
f = 1/T and T = 1/f

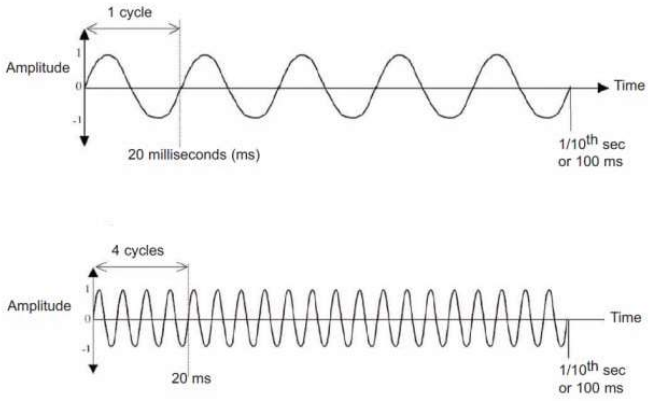


Fig – frequency
https://www.hsa.org.uk/images/publications/onlineguideelectricalwaterbathpoultry/frequency-626x391.png

Frequency can be considered as the measurement of the rate of change of energy from the highest to the lowest voltage level. If the changes takes place over the short time, then it is high frequency. On the other side, if changes of energy level takes long time, it is said to low frequency. For example, in the figure shown above, first part shows the low frequency. To reach from the lowest to the highest level of amplitude, it takes more distance on X axis. While in another part, it takes short time comparatively. In simple words, the former completes 5 cycles and later part completes 20 cycles.

Bit Interval

Data can be represent by a digital signal. For Example a 1 can be encoded as a positive voltage and a 0 can be encoded as a zero voltage . The bit interval is

the time required to send one single bit. This means that the bit rate is number of bits sent in one second, usually expressed in bits per second (bps).

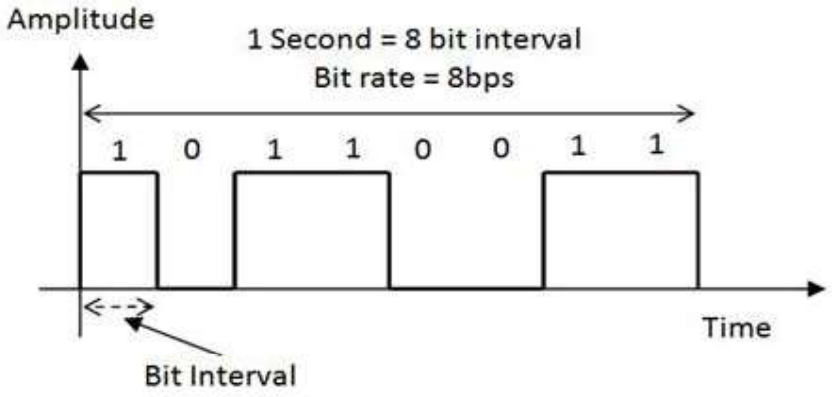


Fig – Bit interval

3.5 TRANSMISSION IMPAIRMENT

Analog signals travel through the transmission media from one end to another. Transmission media usually inclines to weaken the quality of analog signal. Therefore, the receiver does not receive same signals what sender have transmitted. This deficiency origins signal impairment.

There are mainly three causes of analog signals impairment.

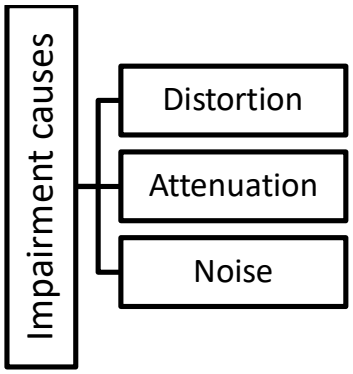


Fig – Impairment causes

Distortion

As per the electronics characteristics of a signal, any change in a signal that modifies the basic association between various frequency components. It can be considered generally a quality degradation of the signal. Distortion may occur in composite signal generally.

Each signal component has its own propagation speed in the transmission medium. Therefore, it may take its own time to reach at receiver. It results in delay sometimes. The delay may vary from the duration of a cycle so the phase also varies.

Attenuation

We learned that signal is in the form of energy. As signal travels the distance through the transmission media, it gets weaker and weaker. This weakness is caused by resistance of the transmission medium itself. This phenomena is called attenuation of signals.

Ideally, the receiver must receive the signal in original condition what sender has transmitted. Amplifier is used to strengthen the signal. It makes the signal in original shape. The analog signals are amplified by amplifier, while digital signals can be amplified using device named 'Repeater'.

Decibel

- Decibel is the unit of measurement for the strength of the signal.
- It is denoted by dB.
- It measures the relative strength of two signals or one signal at two different points.

  The value of dB can be computed using the formula $dB = 10 \log_{10} P_2 / P_1$, where P_1 and P_2 are power of a signal at point 1 and 2 respectively.

- As power is proportional to the square of voltage, the above formula can be written as dB = 20 $\log_{10} V_2/V_1$

Noise – The haphazard or undesirable signal that mixes up with the original signal is called noise. There are four types of noise as depicted in the figure.

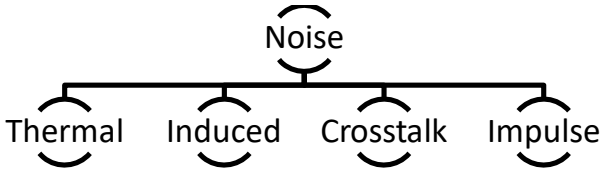


Fig – Types of noise

- Thermal – Thermal noise is generated by random movement of electrons in cable. This random movement produces extra signal which is not part of the original signal.

- Induced – The noise created by sources like motors, cables etc. The induced noise also degrades the useful signal and leads to the error. Induced noise may be electromagnetic or electrostatic noise. In computer network, twisted pair cables are used to reduce induced noise. In twisted wires, the noise voltages that are induced in the signal wires usually cancel out with each other.

- Crosstalk – A wire in network influence another wire, then crosstalk noise is produced. This state is like pair or transmitter and receiver. One wire plays a role of sender and another as a receiver. Crosstalk can cause noise, or prevent cables from transmitting data.

- Impulse Noise – Impulse noise is irregular pulses or noise spikes in short time. The energy carriers or sources such as power lines, lightening and high temperature may cause the sudden energy spike in the regular pulses.

3.6 LET US SUM UP

The signal can be either analog or digital signal. In data communication, the digital signals are used. The binary data fits to the digital signal better. On the other side, analog signal can be either periodic or aperiodic. The signal takes several characteristics such as frequency, amplitude, Bit rate and Bit interval etc. The transmission might get some hindrance. It may be distortion, attenuation, noise. Moreover, noise itself can be categorized into four types, thermal, induced, crosstalk, and impulse.

3.7 CHECK YOUR PROGRESS

1. True-False

- A periodic signal completes a pattern within a measurable time frame.
- A nonperiodic signal does not show any specific repeating pattern.
- The Change over a long time span is a high frequency signal.
- A digital signal have infinite number of values in the range.
- The transmission time is a time for a bit required to travel from source to the destination.
- SNR is the abbreviation for Signal to noise ration.

2. Fill in the blanks

- Bit Rate is measured in _____.
- _____ is the loss of signal strength.
- A completer full pattern is called _____.
- Frequency is represented in _____.

3. Multiple choice

1) Completion of one full pattern is called a

A. period
B. Cycle
C. Frame
D. Segment

2) Bit Rate is number of bits sent in

A. 1sec
B. 2sec
C. 10sec
D. 100sec

3) Term that refers to infinite no of values in range is

A. Peak
B. Analog Signal
C. Digital Signal
D. None of the above

4) Period is inverse of

A. Frequency
B. Phase
C. Amplitude
D. Signals

5) Propagation time is equals to

A. Distance/Propagation speed
B. Propagation speed/Bandwidth
C. Message size/ Bandwidth
D. Bandwidth/Queuing time

6) If signal does not change at all, its frequency is

A. Zero
B. Maximum

C. Infinite
D. None of Above

7) Change over a long span of time means

A. High Frequency
B. Low Frequency
C. High Phase
D. Low phase

8) Analog data refers to information that is

A. Discrete state
B. Continuous state
C. Randomly arranged
D. None of Above

9) Bit rate is measured in

A. Bits per Hertz
B. Bits Per Second
C. Nano seconds
D. Pixels per second

10) Digital data refers to information that is

A. Continuous
B. Discrete
C. Bits
D. Bytes

11) Digital signals are represented in

A. Sine Waves
B. Levels
C. Stages
D. None of the above

12) Term that refers to loss of strength of a signal is called

A. attenuation
B. distortion
C. Noise
D. Impairments

13) Transmission impairment that refers to a signal with high energy in a very short time is

A. Thermal Noise
B. Induced Noise
C. Cross talk
D. Impulse Noise

14) Time required for a bit to travel from source to destination is

A. Latency
B. Propagation Time
C. Delay
D. Transmission time

15) A transmission media can have signal impairment because of

A. Noise
B. Attenuation
C. distortion
D. All of the above

16) Bandwidth of a composite signal is difference between highest and

A. zero frequency
B. lowest frequencies
C. two Parallel frequencies
D. None of Above

17) Frequency is expressed in

A. Second
B. Nanosecond
C. Hertz
D. Megahertz

18) In induced noise, impairment is created by sources like

A. Motor & appliances
B. Power lines
C. the sending and receiving antenna
D. Motion of electrons in wire

19) SNR stands for

A. Shannon Noise ratio
B. Shannon Noise Relation
C. Signal Noise ratio
D. Signal Noise Relation

3.8 FURTHER READING

1) Transmission Impairments and Channel Capacity https://nptel.ac.in/courses/106105080/pdf/M2L3.pdf
2) Noise in Analog Communication Systems https://www.gatestudy.com/wp-content/uploads/2015/06/Noise-In-Communication-Systems.pdf

3.9 ASSIGNMENTS

- What would be the maximum Bit Rate for a noiseless channel with a bandwidth of 3000 Hz transmitting a signal with two signal level?
- Imagine a signal travels through a transmission medium and its power is reduced to half. This means that P2 = P1/2. Calculate the attenuation in decibel.

3.10 ACTIVITIES

- What are the units of frequency and periods?
- What does the amplitude of signal measure?
- What does the frequency of signal measure?
- What is bit interval?
- What is bit rate?
- Name three types of transmission impairment.
- Name four types of noise?

Unit 4: Throughput 4

Unit Structure

4.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Define and explain throughput
- Explain propagation speed
- Explain bandwidth
- Explain waveforms
- Define jitter
- Describe network performance metrics

4.2THROUGHPUT

In the context of computer network, the throughput is the rate of successful message transmission over the communication media.Network throughput is measured in bits per second (bps). It can also be computed in terms successful transmission of data packets per second.Putting in simple words, two systems communicates by exchanging information in the form of data packets. Throughput specifies the level of successful packet sending from one system to another system.

There are several factors which may affects the network throughput. These includes computation power of networking devices such as switch, hub, routers or cables. Network congestion may result in packet loss. Consequently it decreases the throughput of the network.

Sometimes computer network users may not distinguish between terms bandwidth and throughput. However, there are two major differences. The bandwidth refers to the maximum capacity of transmission channel to carry the data from source to the destination. Bandwidth points to ideal capacity of the channel. On the other side, throughput is about the actual number of packets that get sent.

For example, the speed of a network is 100 Mbps. This is the ideal scenario for the exchange of information. After the loss of packets, erroneous packets and other issues, the actual transmission speed is much less than the 100 Mbps. This actual speed is throughput.

Unit of throughput measurement

Network throughput is commonly measured with the following units.

Notation	Term	Speed
Gbps	gigabits per second	billion bits per second
Mbps	megabits per second	million bits per second
Kbps	kilobits per second	thousand bits per second

Table – Throughput measurement

Upload versus Download

An upload is about data that goes out of your computer or machinewhile download gets the data from the server or remote machine. The upload and download throughput may be different.

Latency

Latency is also another relevant but different feature that of throughput. Latency is the time taken to start arriving of the response.

Low throughput causes

- Network load – a very busy network has lower throughput because of more amount of data are to be transmitted over the network. Generally, during working day and office time throughput is found less compared to weekly off days.
- Error in the messages – When packets or messages over the network encounters high errors, then it causes low throughput. As the erroneous message is to be discarded by the receiver, it asks for the retransmission of the same message. If the frequency of error is high, definitely it results low efficiency of the network.
- Quality of service – QoS affects the throughput by putting the priority for the some specific type of the message. For example, video data packets are given higher priority over the textual information packets. Then it will result the delay of the textual data packets.

- Bandwidth – sometimes bandwidth of underlying network gets restricted by the provider of internet.
- Network infrastructure – The throughput gets affected by the limitations of the network infrastructure.
- Network congestion due to heavy network usage.
- Too many users are accessing the same server.

Jitter

- The message may contains several packets normally.
- The sender transmit all packets sequentially at regular time interval.
- But certain factor (improper queuing, network congestion etc.) causes different delay for the receiver.
- Some of them arrive in the order, while some of them may arrive after unexpected delay. This situation is said to be jitter in terms of network performance.
- We consider the scenario of playing video online as an example. Ideally, video should keep on playing without buffering. Because the video packets must arrive with the uniform delay between them. Due to poor network, packets do not reach to the receiver in the order. This situation will lead to the poor quality of video playing.

4.3 PROPAGATION SPEED

In computer network, propagation speed is time requires a signal to reach from source to the destination. Propagation delay can be measured with respect to the distance and propagation speed.

Propagation delay = Distance / Propagation speed

In a communications system, propagation delay refers to the time interval between the departure of a message from the source and the arrival of the message at the destination. This can range from a few nanoseconds or microseconds in local area networks (LANs). Additional propagation delays can occur as a result of the time

required for packets to make their way through land-based cables and nodes of the Internet.

Propagation time = Distance / (Propagation Speed)

Transmission time

The transmission time is the time gap between first bit and last bit of the message. The message is comprises of many bits. The first bit leave the sender machine earlier and last bit leaves sometimes later. The transmission time relies on the size of the message and bandwidth of the channel.

4.4 WAVEFORMS

A graphical representation of a signal as a plot of amplitude versus time, i.e., the shape of a wave. It indicates variation of alternating current (AC) with times. The most popular waveform is sine wave.

Square wave, triangular wave are also known forms of waveforms.

Deviation of voltage or current over the time is represented as an electrical waveform. Let X-axis represents the time and Y-axis shows the voltage of current over the time, the resulting graph would be illustrating waveforms. There are mainly two types of waveforms.

- **Uni-directional Waveforms –** These electrical waveforms always forms either in positive direction or in negative direction. They never cross the zero axis point. Square-wave is the example of the uni-directional waveforms.
- **Bidirectional waveforms** – This type of waveform cross the zero axis alternatively from positive direction to negative direction. It is also known as alternate waveforms.

The waveforms comprise the following three common features:

- Period: – This is the length of time in seconds that the waveform takes to repeat itself from start to finish.
- Time period. Frequency: – This is the number of times the waveform repeats itself within a one second
- Amplitude: – This is the magnitude or intensity of the signal waveform measured in volts or amps.

4.5 BANDWIDTH

Bandwidth defines the maximum data transfer rate of a network or Internet connection. It measures how much data can be sent over a specific connection in a given amount of time. There are many ways to transmit the data across the network. Also, there can be several alternative ways to send the message over the communication media. It is very much essential to measure the performance of the network. The performance of the specific network relies on numerous aspects such as bandwidth, throughput, propagation speed, transmission time etc.

Bandwidth is one of the major features to measure the performance of the network. Bandwidth is considered as number of bits per seconds that can be sent in the channel. For example, a network can send 5000 bits per second at max. Therefore, the bandwidth of that network is said to be 5 kbps.

Bandwidth generally is considered equal from both the communicating sides. In simple terms, data capacity for upload and download is the same. This type of bandwidth setup is said to be symmetrical. On the other end, asymmetrical bandwidth have more download speed than upload speed.

Bandwidth can be explained with analogy of water can flow through a pipeline. The water can be thought of data while pipe is considered the bandwidth of a channel. The amount of water which can flow through pipe depends on the diameters of the pipe. The bigger the pipe diameter, the more the amount of water can flow through it. Computer network user asks for the greater capacity of the channel. They get ready to pay more for the more capacity.

The network performance does not depend only on the maximum bandwidth available at that specific part of the network. It also takes the factors such as packet loss, latency, and jitter into consideration.

How to compute the bandwidth

The calculation of bandwidth depends on the type of network, type of link etc. The fiber optic cable can transmit more number of bits per second compared to the twisted pair cable or coaxial cable. Therefore, the network with fiber optic setup may have more bandwidth. Time-division multiplexing can transmit more data through connection to increase the bandwidth. The effective bandwidth is measured by averaging the time of multiple experiments of sending the same file between the predefined source and destination. This process is known as bandwidth test.

The bandwidth requirement for any commercial sector or industry depends on several points. These includes what types of applications organization need to run, how many such applications are needed, the number of active network users at any given point of time etc.

Allocation of bandwidth

Bandwidth can be allocated dynamically. The acquiring of bandwidth relies on the type of utilization of the network. The dynamic bandwidth allocation is also said to be ‘bandwidth on demand. The dedicated communication link provides bandwidth with the specific capacity all the time. The dedicated bandwidth is sold at price per month or year. Sometimes, the network link is under used and bandwidth is not utilized up to the capacity.

The dynamic bandwidth allocation overcomes the dedicated allocation of bandwidth in advance. The user can demand the more bandwidth for the specific event on the specific day. The user pay only for additional bandwidth used. If a user needed more than the absolute maximum bandwidth available on that link, another physical connection would be required.Intermittently, a service provider will permit consumers to burst above their subscribed bandwidth cap without charging additional usage fees.

How the bandwidth differs from the throughput

The bandwidth is relevant with the throughput but not the synonym of it. It is very important to understand the precise distinction between throughput and bandwidth as we already defined **bandwidth** as the maximum number of bits that can flow through a network connection in a given period of time. The fundamental unit of network bandwidth is bits per second (bps). In computer network, **throughput** is defined as the number of bits that actually passes through a network connection in a given period of time. Throughput is always less than or equal to bandwidth but can never beat bandwidth.

4.6LET US SUM UP

In this chapter, we learned a few points relevant with transmission of the message over the communication network. The throughput is the rate of successful message transmission over the communication media. There are several factors causing the low throughput. These includes network load, error, Quality of Service, Bandwidth, network infrastructure, network congestion etc. We also came across the propagation delay. Propagation delay can be measured with respect to the distance and propagation speed. A graphical representation of a signal as a plot of amplitude versus time, i.e., the shape of a wave. It indicates variation of alternating current (AC) with times. The most popular waveform is sine wave. There are two types of waveforms, unidirectional and bidirectional. At the end, Bandwidth defines the maximum data transfer rate of a network or Internet connection.

4.7CHECK YOUR PROGRESS

1. True-False

    1) Bidirectional waveforms never cross the zero axis when it is formed.
    2) High network load causes the better throughput.
    3) Good quality of service is desirable feature for better throughput.
    4) Network congestion may decrease the throughput of the network.

5) Propagation delay does not depend on the distance between the sender and the receiver.
6) Jitter causes uneven delay between the packets for the receiver.

2. Fill in the blanks

1) Unidirectional waveform always forms in _____direction.
2) _____ is the length of time in seconds that a waveform takes to repeat itself from start to finish.
3) _____ is the magnitude of the signal waveform measured in volts or amps.
4) Square wave is the example of _____ waveform.
5) The maximum data transfer rate of a network is _____ of that network.
6) A graphical representation of a signal as a plot of amplitude versus time is called _____.
7) 'Bandwidth on demand' can be achieved by _____ bandwidth allocation.
8) _____ is defined as the number of bits that actually passes through a network connection in a given period of time.
9) _____ is the time taken to start arriving the response.

3. Multiple choice

1) Techniques for efficient utilization of bandwidth includes

A. Multiplexing
B. medium linking
C. Sampling
D. Both A &C

2) Coaxial cable has a bandwidth that ranges from

A. 5- 750MHz
B. 10-300 MHz
C. 5-550 MHz
D. 10-3000MHz

3) Propagation speed of electromagnetic signals depends on the

A. medium
B. Period
C. Phase
D. delay

4) Range of frequencies a channel can pass is called bandwidth in

A. Bits per second
B. Hertz
C. Kilogram
D. Nanosecond

5) When there is heavy traffic on network, queuing time is

A. Remains same
B. increases
C. decreases
D. None of the above

6) Time required for a bit to travel from source to destination is

A. Latency
B. Propagation Time
C. Delay
D. Transmission time

7) Uneven delay between the packets is said to be

A. Jitter
B. Propagation Time
C. Delay
D. Transmission time

4.8 FURTHER READING

1. Data communication and computer network tutorial https://www.tutorialspoint.com/data_communication_computer_network/data_communication_computer_network_tutorial.pdf
2. Bandwidth Measurements in Wired and Wireless Networks http://www.es.mdh.se/pdf_publications/706.pdf

4.9ASSIGNMENTS

- Differentiate bandwidth and throughput.
- Enlist and explain types of waveforms.
- Which are the reasons for low throughput?
- What is propagation delay?
- What advantages does fiber optics have over other media?
- Explain jitter with example

4.10ACTIVITIES

Solve the following:

- A network with bandwidth of 10 Mbps can pass only an average of 12,000 frames per minute with each frame carrying an average of 10,000 bits. What is the throughput of this network?
- What is the propagation time if the distance between the two points is 2, km? Assume the propagation speed to be 0.4 * 10^8m/s in cable.
- What are propagation time and the transmission time for a 2 MB (Megabyte) message in the bandwidth of the network is 1 Gbps? Assume that the distance

between the transmitter and receiver is 4,000 km and the light travels at the speed of 2.4 X 10^8 m/s.

- What are the propagation time and the transmission time for a 1 KB (kilobyte) message if the bandwidth of the network is 512 Kbps? Assume that the distance between the transmitter and receiver is 2,000 km and the light travels at the speed of 2.4 X 10^8 m/s.

Block-2

Networking Standards

Unit 1: Introduction to Standards

1

Unit Structure

1.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Understand what is internet standards
- Explain why internet standards are useful
- Describe the process of methods to become internet standards
- Explain how the communication process takes place through OSI

1.2 INTERNET STANDARDS

Internet standard is a normative description of technology relevant to the internet. The Internet Engineering Task Force (IETF) is the organization which publishes internet standards. An internet standard is characterized by its usefulness. The internet standards have to pass a level called 'Request for Comment' (RFC) before getting recognized as an internet standard. Following are the characteristics of the internet standard.

- An Internet standards is a comprehensively tested specification that is useful to those who work with the Internet.
- It might have multiple implementations, at the same time they may be independent and interoperable.
- It is used almost over all parts of the Internet.
- It gains remarkable public support.
- It must be followed in the Internet regulation.

Procedure for getting Internet standard

- **Internet draft** – An internet draft is a working document, which indicates the specification in progress. It has validity of six months.
- **Request for Comment** – The Internet draft is assessed by Internet authority. If the Internet draft gets recommendation from the same, they it can be published as a Request for Comment (RFC). Each RFC is edited, given a

number and made accessible to all interested parties. RFCs go through maturity levels and are categorized according to their requirement level.

Maturity levels – RFCs may fall in one of six standards. They are proposed standard, draft standard, Internet standard, historic standard, experimental, informational.

- Proposed standard – A proposed standard is well-understood and stable specification. It must have achieved sufficient interest by the Internet community. The specification might get implemented by multiple party.
- Draft standard – having two successful independent and interoperable implementations, a proposed standard is raised to a draft standard.
- Internet standard – Draft standard goes to Internet standard after modification. The modification might have caused due to some specific problem.
- Historic standard – They might be one of the two reason for a specification having historic standard. First, it has never passed the necessary maturity level to become an Internet standard. Second, it might be significant from historic perspective.
- Experimental standard – An RFC which defines the experimental situation is called experimental standard. It does not affect the operation of Internet.
- Informational standard – Informational standard is written by non-Internet organization. It comprises of general, historical or tutorial information.

Requirement levels – RFCs are classified into five requirement levels: required, recommended, elective, limited use, and not recommended.

- **Required –** An RFC is categorized required if it must be implemented by all Internet systems to achieve the minimum conformance.
- **Recommended –** An RFC is labelled recommended is not required to have minimum conformance. It must be useful. For example, FTP and TELNET are recommended protocols.
- **Elective –** An RFC labelled elective is neither required nor recommended. However, a system can use it for its own benefit.
- **Limited use –** An RFC labelled limited use should be used only in limited situations. Most of the experimental RFCs fall under this class.

- **Not Recommended –** An RFC labelled not recommended is inappropriate for general use. Normally a historic RFC may fall under this category.

1.3 STANDARD ORGANIZATIONS

The governance and administration of the Internet is administered by several organizations composed mostly of volunteers from the global Internet community. These organizations consist of the Internet Society (ISOC), the Internet Architecture Board, the Internet Engineering Task Force, and the Internet Research Task Force. The administrative organizational structure of the Internet is shown in Figure below.

ISOC

The internet Society was founded in 1992 by a number of people involved with the Internet Engineering Task Force (IETF). ISOC provides support Internet standard process. ISOC coordinates with other Internet organization such as IAB, IETF, IRTF and IANA. One of the fundamental objectives of ISOC is to encourage research and other Internet relevant activities.

IAB

The internet Architecture Board is responsible for the overall planning and designing of the Internet. It plays the role of technical advisor for the ISOC. It sets the internet standards, publishes the RFC documents, and resolves technical challenges. IAB also synchronize other bodies such as Internet Engineering Task Force (IETF) and the Internet Research Task Force (IRTF).

IETF

IETF is principally concerned with addressing short- or medium-term Internet engineering matters. It identifies the operational problems and offers solutions for these problems. Moreover, it develops and review specifications targeted for Internet standards. Basically, IETF is a forum of working group. The working groups forms the areas. Each area focuses on the specific tasks.

IRTF

IRTF works on long-term research projects. An example of its work is the e-mail privacy issue. Both task forces also have steering committees that prioritize and coordinate their respective activities. IETF's steering committee is called the Internet Engineering.

1.4 OSI RULES

History

The International Organization for Standardization (ISO) and the International Telegraph and Telephone Consultative Committee (CCITT) developed a standard for methods of networking. They did not carried out work jointly, but on parallel track separately. Then they have merged their documents and produced a standard called The Basic Reference Model for Open Systems Interconnection. The standard is known as OSI reference model. The proposed standard had two major parts, the seven layers and set of protocols.

Charles Bachman given the concept of seven layers. The various networks have contributed directly or indirectly in the design the OSI reference model. These networks includes the ARPANET, NPLNET, EIN, and CYCLADES. The OSI model later updated into layered architecture. Each layer interact directly with layer above and layer beneath. Service of layers defines abstractly the functionalities of the layer.

There are mammoth numbers of users who use Internet and are located across the globe. One may find access to the Internet from each corner of the world. So there must be some common platform for the rules and regulation. All users would agree to communicate over those rules and regulations. Systems must be developed which are harmonious to communicate with each other. The ISO has developed a standard. ISO stands for International organization of Standardization. This is called a model for Open System Interconnection (OSI) and is commonly known as OSI model.

The chief objective of the OSI reference model is to give direction to manufacturers and developers so that devices and program can interoperate. The reference model such as OSI is very important because it may give thoroughly guidelines for having a

complete communication network. When a system is very complex in the nature, it would be easy to understand by dividing into pieces.

Features of OSI reference model

- ✓ The complex communication system can be understood with ease using OSI reference model.
- ✓ It clears the picture about how hardware/devices and protocols/software works together.
- ✓ The newly added technology, software, protocols, hardware can be developed and integrated.
- ✓ The faults, errors, damage, disconnection etc. can be tracked and corrected easily.
- ✓ Two or more networks and relevant technologies can be compared having OSI as a benchmark.

The principles of OSI reference model

- ✓ Each layer must perform a specific set of functions.
- ✓ There should be a separate layer for the relevant set of functions.
- ✓ The functions of layer must be defined such a way that it get aligned with international standard protocols.
- ✓ There must be an interface to communicate with the neighbor layers.

1.5 COMMUNICATION PROCESS

Communication in the OSI reference model

- ✓ The topmost layer prepares the message which is to be transmitted. The message is said to be Protocol Data Unit (PDU). The application layer PDU is known as APDU.
- ✓ The PDU is handed over to the presentation layer. Now it becomes Presentation PDU.

- ✓ It is passes to session layer. On the session layer is becomes Session PDU and consequently it becomes Transport PDU. It also known as segment.
- ✓ At the network layer, TPDU is divided into packets.
- ✓ The datalink layer divides the packet into the frame.
- ✓ The physical layers convert the frame into raw binary stream.

Layer	**Name of Unit exchanged**
Application	APDU – Application Protocol Data Unit
Presentation	PPDU - Presentation Protocol Data Unit
Session	SPDU - Session Protocol Data Unit
Transport	TPDU - Transport Protocol Data Unit (segment)
Network	Packet
Datalink	Frame
Physical	Bit

Table – Layer and data unit for that layer

1.6 LET US SUM UP

This chapter Introduced about Internet standard. The Internet standard is normative description of technology relevant to the internet. The Internet Engineering Task Force (IETF) is the organization which publishes the internet standards. There are five maturity levels: proposed standard, draft standard, Internet standard, historic standard, experimental, informational. The requirement levels for RFC are required, recommended, elective, limited use, and not recommended. Those standard are defined by the standard organizations. The standard organizations are ISOC, IAB, IETF and IRTF. Each of Internet standards is responsible for some specific set of duties. The International Organization for Standardization (ISO) and the International Telegraph and Telephone Consultative Committee (CCITT) developed a standard for

methods of networking. The OSI model got modified and shaped into layered architecture. We have come across features of the OSI reference model. We have also learned how communication process take place in OSI model.

1.7 CHECK YOUR PROGRESS

1. Multiple choice

   1) Largest professional engineering society in world is

   A. American National Standards Institute
   B. Electronic Industries Association
   C. Institute of Electrical and Electronics Engineers
   D. International Organization for Standardization

   2) Working document with no official status and a 6-month lifetime is called

   A. Internet draft
   B. Internet standard
   C. Internet Protocol
   D. Regulatory Agencies

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

   A. Institute of Electrical and Electronics Engineers
   B. International Organization for Standardization
   C. American National Standards Institute
   D. Electronic Industries Association

   4) The protocol data unit(PDU) for the application layer in the Internet stack is
   (A) Segment
   (B) Datagram

(C) Message

(D) Frame

5) Which of the following transport layer protocol is used to support electronic mail?

(A) SMTP

(B) IP

(C) TCP

(D) UDP

6) What does indicate that specification is in progress?

(A) Internet draft

(B) Request for Comment

(C) none of the above

7) How many total maturity levels?

A. Four

B. Five

C. Six

D. Seven

8) The stable specification is required by _____?

A. Proposed standard

B. Draft standard

C. Internet standard

D. Informational standard

9) Which standard goes to internet standard after modification?

A. Proposed standard

B. Draft standard

C. Internet standard

D. Informational standard

10) Which standard must have two successful implementation?

A. Proposed standard

B. Draft standard

C. Internet standard

D. Informational standard

11)_____ standard have never passed the maturity level.

A. Proposed standard
B. Historic standard
C. Internet standard
D. Informational standard

12)_____ is written by non-Internet organization.

A. Proposed standard
B. Historic standard
C. Informal standard
D. Informational standard

13)Which standard does define experimental situation?

A. Experimental standard
B. Historic standard
C. Informal standard
D. Informational standard

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

A. Required
B. Recommended
C. Elective
D. Limited use

15)An RFC labeled _____ is neither required nor recommended.

A. Required
B. Recommended
C. Elective
D. Limited use

16)An RFC labeled _____is inappropriate for general use.

A. Required
B. Recommended
C. Not recommended
D. Limited use

17)_____ works on long-term research projects.

A. ISOC
B. IRTF
C. IETF
D. IAB

18)The _____ is responsible for the overall planning and designing of the Internet.

A. ISOC
B. IRTF
C. IETF
D. IAB

19)The physical layer deals with _____ format.

A. packet
B. segment
C. frame
D. bit

20)The transport layer deals with _____ format.

A. packet
B. segment
C. frame
D. bit

21)The data link layer deals with _____ format.

A. packet
B. segment
C. frame
D. bit

22)The network layer deals with _____ format.

A. packet
B. segment
C. frame
D. bit

23)Data unit exchanged at the application layer is _____.

A. PPDU

B. SPDU
C. APDU
D. TPDU

24) Data unit exchanged at the presentation layer is _____.
A. PPDU
B. SPDU
C. APDU
D. TPDU

25) Data unit exchanged at the session layer is _____.
A. PPDU
B. SPDU
C. APDU
D. TPDU

26) Data unit exchanged at the transport layer is _____.
A. PPDU
B. SPDU
C. APDU
D. TPDU

1.8 FURTHER READING

- Brief history of Internet https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf
- IETF Structure and Internet Standards Process https://www.ietf.org/proceedings/93/slides/slides-93-edu-newcomers-5.pdf
- IRTF Overview https://datatracker.ietf.org/meeting/99/materials/slides-99-edu-sessd-irtf-overview-01.pdf
- IAB NEW STANDARD AD UNIT PORTFOLIO https://www.iab.com/wp-content/uploads/2017/08/IABNewAdPortfolio_FINAL_2017.pdf

1.9 ASSIGNMENTS

- Explain the difference between a required RFC and recommended RFC.
- Differentiate between internet and Internet.
- Explain the difference between IETF and IRTF.
- Differentiate between an Internet draft and proposed standard.
- Write short note on Internet Standard Organizations
- How Internet standards are useful?
- Explain the communication process of OSI reference model.
- Describe the various data units generated at various layers of OSI model.
- What is the process for getting Internet standard?
- Explain various maturity levels.
- Enlist requirement levels. Differentiate between recommended and not recommended requirement levels.

1.10 ACTIVITIES

- Export packet analyser tool (wire shark) for observing the data unit at the various layers of the protocol stack.

Unit 2: The OSI Reference Model

2

Unit Structure

2.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Explain what is reference model
- Understand OSI Reference model
- Explain how layers interacts with each other
- Describe what is protocol stack
- Explain how the layers of OSI maps with layers of TCP/IP

2.2 THE OSI REFERENCE MODEL

The International Organization for Standardization (ISO) is an international body to decide international standards of any product or service. The majority of countries across the world are associated with ISO.

The Open System Interconnection (OSI) model is recognized by ISO as a reference model which covers all aspects of network communications. The OSI reference model was first introduced in 1970s.

The OSI reference model is layered architecture. In other words, seven layers are arranged one above another. There are some words needs to be unpacked for better understanding of the OSI reference model. Such as ‘Open System’, ‘Reference model’, ‘Layers’.

The phrase ‘Open system’ conveys that it is a set of protocols that enables two different computers to exchange the information irrespective of their underlying architecture. In simple terms, underlying architectures does mean that operating system being used in that two computers, type of processor, temporary memory, permanent storage, etc. Open system does not demand to change or upgrade the hardware of software for the participating computers in the communication.

The ‘Reference model’ is a benchmark that help set-up a flexible, robust and working network. The OSI is a reference model because it guide network designers what are the main services are to be provided. It also directs one to design various protocols required for giving the services.

The layers indicates the specific part of whole model. There are total seven distinct layers. Each of them defines the specific set of tasks to be provided. The layers are interactive and dependent. That means, each layers is related with the layer above it and the layer beneath it. Furthermore, each layer plays a precise role for transmitting information across the network.

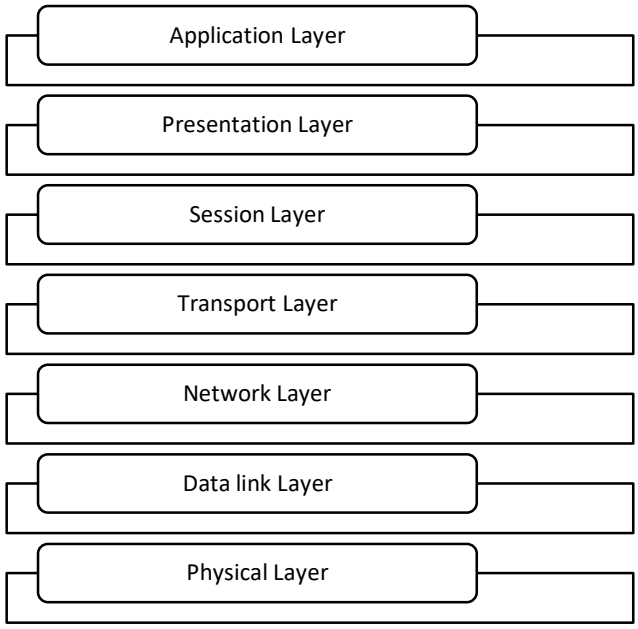


Fig- The OSI reference model

2.3 HOW PEER OSI LAYER COMMUNICATES

We consider the OSI reference model layer architecture works at both the side, sender side and receiver side. Each OSI layer have got a set of duties to perform. The Sender start processing from the application layer to the physical layer. The receiver start processing in the reverse order, from the physical layer to the application layer.

At the sender side, the layer takes the service from above layer and provides the service from the bottom layer. For example, application layer perform some functions and prepares an intermediate format of the message. Application layer handover the message to the layer below, the presentation layer. The presentation layer performs specific duties and gives the prepared message to the session layers.

Likewise, at the receiver side, the layer provides the service to the layer above it. So the physical layer accept the message, do some functions and then handover the intermediate format of the message to the data link layer for further processing. The data link layers follows the same procedure. It process the message and gives to the layer above, the network layer. The entire procedure goes in a very systematic way. The interface allows the layer to communicate with the layer above and below.

2.4 HOW POSTAL COMMUNICATION WORKS – AN EXAMPLE

For better understanding, we may consider the working mechanism of postal communication. The postal service transport postcards, letters, parcels physically from one location to another location.

Right from a person writes a letter to the receiver reads that letter, the process can be described in sequence of steps.

Steps at the sender side

- A sender writes a letter.
- Put the address of the recipient on the envelope.
- Insert the letter in to the envelope.
- The letter is submitted to the post-box.
- Postman comes and collect letter from post-box.
- It submit all letters to the post office.
- Post office bifurcate the letters city wise.
- Send all letters to the respective city by physical transport mode. (e.g. vehicle)

Steps at the receiver side.

- Post-office collects the letters from vehicle.
- Post-office bifurcates the letters area wise.
- Letters are handed over to the post-man of that specific area.
- Post-man submit the letter to the post-box of the recipient.
- Receiver collects the envelope from the post-box.

- Open the envelope and take the letter out.
- Receiver reads the letter.

The above mentioned process can be understood by dividing all steps into layers.

Sender performs writing, addressing and enveloping of letters. So it can be considered as higher layer or sender layer.

Once all sub tasks of sender are completed, post-man takes the charge and performs collection of letters and submission of letters. Therefore, this can be considered as middle layer or post-man layer.

After that, post-office performs the rest of the job. It classifies the letters city wise and send them through some carrier. This layer can be considered as lower layer.

Similarly at receiver side, sub tasks can be organised in the same manner.

2.5 TCP/IP PROTOCOL STACK

Open System Interconnection (OSI) is the reference model. It defines an ideal scenario under which a computer network can be designed successfully. On the other end, Transmission Control Protocol/Internet Protocol (TCP/IP) is the network model which is being used in the current internet architecture. The TCP/IP follows the guidelines defined by TCP/IP for the network models. It explains the exchange between end computers.

The TCP/IP protocol stack is basically comprises four layers.

Application Layer
Transport Layer
Internet Layer
Host-to-Network Layer

Fig – TCP/IP Protocol stack layer

Overview of TCP/IP protocol stack

The TCP/IP protocol stack was developed with concerns to support the flexible architecture. That is, more number of machines can be added to the network with ease. The network is to make robust and source and destination machine must be functioning. The main focus was to build the network such that one application on one computer is able to exchange the information on another application running on different computer.

Functions of TCP/IP protocol stack layers

OSI reference model layers have got very specific set of functions. Likewise, TCP/IP protocol stack also has got four layers. Furthermore, each layer has to perform predefined functions.

Application	TELNET FTP SMTP DNS
Transport	TCP UDP
Internet	IP
Host-to-Network	ARPANET SATNET LAN

Fig – Protocols in the TCP/IP

Layer1: Host-to-network Layer

- ✓ It is the lowest layer of the TCP/IP protocol stack.
- ✓ This layer provides the ability to connect the host. The messages or packets are sent over this established network.
- ✓ It differs from machine to machine and network to network.

Layer2: Internet Layer

- ✓ This layer helps routing the packets from the source to the destination.
- ✓ It is used for assuring the delivery of packets to the end machine.

- ✓ It also controls the congestion in the various part of the network.
- ✓ It holds the whole network architecture together.
- ✓ It is used for forwarding the packets independently.
- ✓ The packets may not arrive in the order at the receiver.
- ✓ Internet Protocol (IP) is used in this layer.
- ✓ The packet switching network is selected based on the connectionless internetwork layer.

Layer3: Transport Layer

- ✓ The transport layer take decision for parallel path or single path.
- ✓ The multiplexing is done at this layer.
- ✓ It does segmentation and reassembly.
- ✓ The transport layer adds the header information to the data.

Layer4: Application Layer

- ✓ The application layer identifies a group of applications. Some of them are SMTP, FTP, TELNET, DNS etc.
- ✓ SMTP – It stands for Simple Mail Transfer Protocol. It sends the electronic mail from source to the destination.
- ✓ FTP (File Transfer Protocol) – It enables computers in the network to transfer the file from the server to the client. The FTP is simple, reliable and very efficient protocol.
- ✓ DNS (Domain Name System) – It transforms IP address into names. The process of DNS locates the service requested by the client.
- ✓ It specifies two end-to-end protocols, TCP and UDP.
    - o TCP (Transmission Control Protocol) – It is connection oriented protocol.
    - o It is reliable and transmit the packets from the source to the destination without error.
    - o UDP (User Datagram Protocol) – It is unreliable and connection-less protocol.
    - o It does not provides sequencing and flow control.

Advantages of TCP/IP

- ✓ It is scalable.
- ✓ It offers client-server architecture.

- ✓ It supports numerous routing protocols.

Disadvantages of TCP/IP

- ✓ It has not clear separation of services, protocols and interface.
- ✓ The transport layer does not guarantee for the delivery of the packets.

2.6 LET US SUM UP

We have come across the concepts of OSI reference model and how the layers interacts with each other. The Open System Interconnection (OSI) model is recognized by ISO as a reference model which covers all aspects of network communications. The 'Reference model' is a benchmark that help set-up a flexible, robust and working network. We understood that how layers of the OSI reference model interacts with the layer above and below to provide successful communication between sender and receiver. The layer architecture better explained with the help of the traditional communication system, postal communication system. Then after, TCP/IP protocol stack has been introduced. Transmission Control Protocol/Internet Protocol (TCP/IP) is the network model which is being used in the current internet architecture. The TCP/IP follows the guidelines defined by TCP/IP for the network models. It explains the exchange between end computers.

2.7 CHECK YOUR PROGRESS

1. Matching

A	B
Reliable packet delivery	MAC address
Unreliable packet delivery	IP address
Logical address	TCP

Physical address	UDP
Application layer	Transport layer
Process-to-process delivery	FTP

2. Fill in the blanks

    1) The OSI reference Model is comprises of _____ layers.
    2) The TCP/IP protocol stack is contains _____ layers.
    3) The host-to-network in TCP/IP protocol stack can be mapped with _____ layer and _____ layer of the OSI reference model.
    4) The application layer of TCP/IP protocol stack performs functions of _____, _____ and _____ layers of the OSI reference model.
    5) The _____ protocol provides the reliable packet delivery.
    6) The _____ protocol does not guarantee for successful packet delivery.

3. Multiple choice

    1) Transmission Control Protocol/Internet Networking Protocol have

    A. Four Layers
    B. Five Layers
    C. Six Layers
    D. Seven Layers

    2) Parameter that is normally achieved through a trailer added to end of frame is

    A. Access Control
    B. Flow Control
    C. Error Control
    D. Physical addressing.

3) Packets of data that is transported by IP is called

A. datagrams
B. Frames
C. Segments
D. Encapsulate message

4) Application layer provides basis for

A. Email services
B. Frame Division
C. File Making
D. None of the above

5) Trailer is added only at

A. Physical Layer
B. Data Link Layer
C. transport Layer
D. Network LAYER

6) Segmentation and reassembly is responsibility of

A. 7th Layer
B. 6th Layer
C. 5th Layer
D. 4th layer

7) Port address is also known as

A. Service point address
B. Receiver point address
C. Sender point address
D. Both B & C

8) Logical Addresses are

A. 16bit long
B. 32bit long
C. 64bit long
D. 128bit long

9) Both TCP and SCTP protocols are

A. Connection less
B. connection oriented
C. start but no ending
D. None of Above

10) TCP is related to

A. ARPANET
B. ISO-OSI
C. DECNET
D. None of Above

11) Length of Port addresses in TCP/IP are

A. 4bit long
B. 16bit long
C. 32bit long
D. None of Above

12) TCP/IP layer is equivalent to combined Session, Presentation and

A. Network layer
B. Application layer
C. Transport layer
D. both a and c

13) How many levels of addressing in TCP/IP protocol provides

A. One
B. Two
C. Three
D. four

14) ICMP Stands for

A. Internet Connect Message Protocol
B. Internet Control Message Protocol
C. International Connect Message Protocol
D. International Control Message Protocol

15) Transmission Control Protocol/Internet Networking Protocol have

A. Four Layers
B. Five Layers
C. Six Layers
D. Seven Layers

16) Packets of data that is transported by IP is called

A. datagrams
B. Frames
C. Segments
D. Encapsulate message

17) Transmission Control Protocol divides a stream of data into smaller units that are called

A. Frames
B. Datagrams
C. Segments
D. Information

18) Term that refers to associate a logical address with a physical address is

A. RARP
B. IGMP
C. ARP
D. ICMP

19) Which protocol ensures reliable delivery

A. TCP
B. UDP
C. Both of above
D. None of above

20) TCP is a ……. protocol.

A. stream-oriented
B. message-oriented
C. block-oriented
D. packet-oriented

21) TCP/IP suite was created by

A. IEEE
B. Department of defence
C. Open source
D. None of above

22) Which of the following is not the layer of TCP/IP protocol.

A. Physical layer
B. link layer
C. network layer
D. transport layer.

23)Which layer of TCP/IP stack is equivalent to transport layer of OSI

A. Application layer
B. Host to Host layer
C. Internet
D. Network access

24)Which layer will be used while transmitting data using FTP or Telnet

A. Presentation
B. Application
C. Session
D. Transport

25) Which company developed TCP/IP protocol for networking

A. IBM
B. DEC
C. DARPA
D. Xerox

26)Which protocol finds the MAC address from IP address

A. SMTP
B. ICMP
C. ARP
D. RARP

27)Which protocol uses both TCP and UDP

A. FTP
B. SMTP
C. Telnet
D. DNS

28) Telnet

A. allows user to connect client machine
B. transferring files
C. sharing files
D. none of above

29) Which protocol uses window flow system

A. UDP
B. TCP
C. FTP
D. None of above

30) Which protocol deals with resolving domain names

A. X-Window
B. SMTP
C. DNS
D. FTP

31) ICMP works on which layer

A. Physical Layer
B. Datalink Layer
C. Network layer
D. Transport Layer

32) The ……. of TCP/IP protocol is responsible for figuring out how to get data to its destination.

A. application layer
B. link layer
C. network layer
D. transport layer.

33) TCP is a(n) …….. transport protocol.

A. protocol delivery
B. reliable
C. best-effort delivery
D. effortless delivery

34) …… is the protocol that hides the underlying physical network by creating a virtual network view.

A. Internet Protocol(IP)
B. Internet Control Message Protocol(ICMP)
C. Address Resolution Protocol(ARP)
D. Bootstrap Protocol(BOOTP)

35) To use the services of UDP, we need …… socket addresses.

A. four
B. two
C. three
D. four

36) Which of the following is not the name of Regional Internet Registries(RIR) to administer the network number portion of IP address.

A. American Registry for Internet Numbers(ARIN)
B. Reseaux IP Europeans(RIPE)
C. Europeans Registry for Internet Numbers(ERIN)
D. Asia Pacific Network Information Center(APNIC)

37) UDP packets are called …….

A. user datagrams
B. segments
C. frames
D. packets

38)…… addresses use 21 bits for the and 8 bits for the portion of the IP address for TCP/IP network.

A. Class A
B. Class B
C. Class C
D. Class D

39) UDP packets have fixed-size header of ……. bytes.

A. 16
B. B. 8
C. 32
D. 64

40)……. messages are never sent in response to datagrams with a broadcast or a multicast destination address.

A. ICMP
B. ARP
C. IP
D. BOOTP

41) TCP assigns a sequence number to each segment that is being sent. The sequence number for each segment is number of the ……. byte carried in that segment.

A. first
B. last
C. middle
D. zero

42) Which protocol deals with emails

A. FTP
B. SMTP

C. LPD
D. X window

43)……. is responsible for converting the higher level protocol address (IP addresses) to physical network addresses.

A. Internet Protocol(IP)
B. Internet Control Message Protocol(ICMP)
C. Address Resolution Protocol(ARP)
D. Bootstrap Protocol(BOOTP)

44)UDP and TCP are both …… layer protocols.

A. data link
B. network
C. transport
D. interface

45)…….. is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from upper layer.

A. TCP
B. UDP
C. IP
D. ARP

46)Which of the following functions does UDP perform?

A. Process-to-process communication
B. Host-to-host communication
C. End-to-end reliable data delivery
D. Interface-to-interface communication.

47) A port address in TCP/IP is ……bits long.

A. 32
B. 48
C. 16
D. 64

48)When the IP layer of a receiving host receives a datagram…

A. delivery is complete
B. a transport layer protocol takes over
C. a header is added
D. a session layer protocol takes over

49)TCP/IP is a ……. hierarchical protocol suite developed before the OSI model.

A. seven-layer
B. five-layer
C. six-layer
D. four-layer

2.12 FURTHER READING

1. Introduction to TCP/IP
   https://www.jameco.com/Jameco/Products/ProdDS/320733%20(TCP%20IP)%20Intro.pdf
2. Introduction to TCP/IP
   https://www.cse.wustl.edu/~jain/tutorials/ftp/t_2tcp.pdf
3. TCP/IP Tutorial and Technical Overview
   https://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf
4. The TCP/IP Protocol Suite
   http://www.fujitsu.com/downloads/TEL/fnc/pdfservices/TCPIPTutorial.pdf

5. OSI Model
   http://www.srmuniv.ac.in/sites/default/files/files/OSI%20Reference%20model.pdf
6. OSI Reference Model
   https://www.routeralley.com/guides/osi.pdf

2.13 ASSIGNMENTS

- Explain how the headers are added layer by layer at the sender side?
- Differentiate TCP and UDP.
- List application layer protocols in the TCP/IP.

2.14 ACTIVITIES

- Configure active directory in windows server machine.
- Setup a client server network with domain login.
- Configure DHCP server.
- Configure FTP server for LAN.

Unit 3: Conceptualizing the Layers of OSI Model

3

Unit Structure

3.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Explain functions of layers of OSI reference model
- Explain how OSI layer provides/avails the service to/from other layers
- Describe network topology and comparison among topology.
- Differentiate among the mode of transmission

3.2 CONCEPTUALIZING THE LAYERS OF THE OSI MODEL

The OSI model was conceptualized to standardize the characteristics of communication of computer without concerning the underlying technology. In simple words, it allows diverse communicating systems to exchange information. OSI (Open systems interconnect) is a reference model that describes data communication over a network. It was formed based on a proposal from International Organization for Standardization (ISO). Its authorized title is ISO OSI Reference Model because it narrates systems that are available for communication with other devices. It defines the standards for several important features of communication. For example, it inform the computers when to transmit the data for successful communication, and also when not to transmit the data. It also ensures the correctness of whatever the message received. Moreover, it guarantees about the recipient of the message to whom sender intends to send. It also make arrangement of connection of the physical medium such as cables and central devices.

3.3 THE PHYSICAL LAYER

Physical layer provides the physical medium which carries the data in the form of signal from the sender machine to the receiver computer. It includes cables (twisted pair, fibre optics or coaxial), sockets, signal generators as physical medium. There

may be wireless medium of transmission. The physical layer defines the mechanical, electrical, timing and functional characteristics of physical link between end computers. The functions of physical layers are as follows:

- This layer receiver the data from the data link layer at the sender computer. Then it converts the data stream from binary format to the signal format.
- It carries signal from source to the destination.
- It defines how to convert 0 and 1 into electrical signal or light signal.
- It defines the data rate according to the Ethernet standards. For example, Ethernet 802.3 carries the data on the speed of 10 Mbps. Fast Ethernet works at 100 Mbps. Gigabit Ethernet works at 1000 Mbps.
- It establish the synchronization between sender and receiver. For example, sender and receiver computer might be working at different frequencies. Then clocks of these computes must be synchronized.
- It determines the mode of transmission, which is direction (unidirectional or bidirectional) of signal transmission. There are three mode of transmission.
- It defines the physical topology layout.

3.3.1 Modes of transmission

- ✓ Simplex – signal can be transmitted in one direction only. There is a fix transmitter and receiver. For example, the remote control sends signal to tune television set. Therefore, this kind of communication is said to be simplex mode of transmission. In simplex mode of transmission, transmitter and receiver cannot be interchanged.
- ✓ Half duplex – In this transmission mode, signal can be sent in both direction, But not at the same time. The walkie-talkie is the example of half duplex. Two person may communicate through walkie-talkie device. But once the first person finish its transmission, it indicates the other person by transmitting a code word ‘over’. After that, second person start speaking.
- ✓ Full duplex - Full-duplex data transmission means that data can be sent in both directions on a signal carrier at the same time. For example, on a local area network with a technology that has full-duplex transmission, one workstation can be sending data on the line while another workstation is

receiving data. Full-duplex transmission necessarily implies a bidirectional line (one that can move data in both directions).

3.3.2 Physical topology layout

The computer network topology defines the physical layout of network. It explains how computers are interconnected among themselves physically. Each computer in the network is connected to every other computer in the network through some specific topology. The connection may be direct or indirect. Also it might be either wired or wireless.

- Bus topology – Every computers and devices are connected through a common cable in local area network. The cable has exactly two end points. There are several features of the bus topology as follows:
  - ✓ The data are transmitted in one direction only.
  - ✓ The bus topology requires minimum cabling compared to other topology.
  - ✓ The cost to bus topology set-up is less.
  - ✓ The set-up of the bus topology is easy to understand.
  - ✓ If cable get damaged, then network breaks.
- Star topology – Star topology connects every computers in a network through a central device. Also, they are connected via a dedicated cable to the central device. Generally, hub or switch works as a central device. There are some features of the star topology as follows:
  - ✓ Start topology is easy to expand.
  - ✓ If a cable breaks, then only that specific computer is disconnected.
  - ✓ Start topology is easy to establish.
  - ✓ The start topology installation cost is high.
  - ✓ If the hub fails, then the whole network stops working. Because each computers are connected among themselves through hub only.
  - ✓ Performance of depends on the capacity of the hub.
  - ✓ Stat topology is expensive compared to the bus topology.
- Ring Topology – Each computer is connected to exactly two neighbours. It forms a ring shape of the physical connection of all computers in the network. The features of the ring topology are as under:

- ✓ If sender is allowed to transmit the data in one direction only (clockwise or anti-clock wise), then it is called unidirectional.
- ✓ Ring topology follows token passing technique. That is, the node having token is allowed to transmit the data
- ✓ If transmission is allowed in both direction, then it is called bidirectional.
- ✓ Easy to expand comparatively.
- ✓ If any computer fails in the network, then it damages the whole network.

- Mesh topology – Each network computer is connected to every other computer in the same network. There is a dedicated cable for connection. In other words, a computer does not share the cable. There are some features of mesh topology as follows:
  - ✓ The mesh topology offers most reliable communication. Because there would be several alternative paths from one computer to other.
  - ✓ Mesh topology is very robust.
  - ✓ It provides better security and privacy.
  - ✓ It requires more cabling.
  - ✓ The cost of mesh topology is more compared other topology.
  - ✓ The installation and configuration is difficult.
- Tree topology – Tree topology connects computers in hierarchy. The interconnection of computers forms a tree shape structure. The root computer connects two other computers with it. It must have at least three level of hierarchy.
  - ✓ The expansion of the tree topology is easy.
  - ✓ It is easy to manage and maintain the tree topology.
  - ✓ The cabling cost is high.
- Hybrid topology – When two or different types of topologies are connected among each other, the resultant topology is said to be the hybrid topology. For example if in an office in one department mesh topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology mesh topology and star topology). The main characteristics of the hybrid topology are as mentioned below.

- ✓ As it is mixture of more than one topologies, it is also derives the advantages and disadvantages of those.
- ✓ The hybrid topology can be scaled easily.
- ✓ It is more flexible and effective.
- ✓ The design of the hybrid topology is more complex.

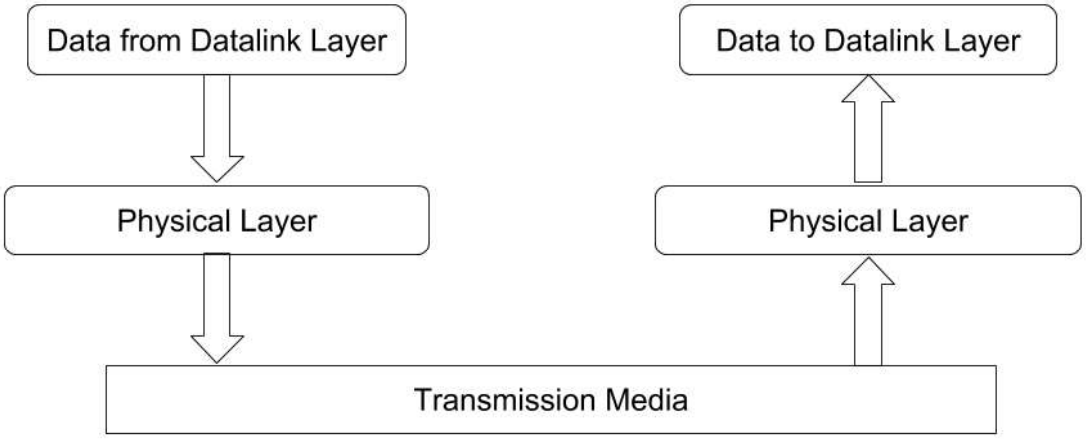


Fig – Physical Layer

3.4 THE DATA LINK LAYER

The Data Link Layer is second layer of OSI Layered Model. Data link layer accomplishes the tasks of the computers which are directly connected. There might be point-to-point connection or broadcast connection. Data link layer makes the most reliable node to node delivery of data. It receive packets from the network layer. It formulates the frames from the packets and transfers to the physical layer. The data link layer has two sub-layers.

1. Logical Link Control (LLC) – it provides the flow control, error control and framing functionalities.
2. Medium Access Control (MAC) – it deals with controlling the shared medium when multiple users access the channels.

The functions of the Data link layer are as follows:

- Framing: - As mentioned, the data link layers receives the packets from the network layer. Now packet size might be longer than the manageable data units in the local network. Therefore, data link layers forms a number of frames from the received packets. A frame can be of fixed size or variable size.
- Flow control:-The sender machine and the receiver machine may have different configuration. They may have distinct transmission speed or buffer capacity.
  - ✓ The flow control mechanism of the data link layers confirms that sender and receiver works on the same speed.
  - ✓ It provides surety that all data which have been sent by the transmitter mast be received by the receiver.
  - ✓ There are a set of protocols for achieving flow control. For instance, Stop-N-Wait, Selective Repeat, Go-back-N etc.
- Error Control: - This is a very important functionality provided by the data link layer.
  - ✓ Error control mechanism enables receiver to check that received data is correct or not.
  - ✓ In other words, the receiver accepts only correct data.
  - ✓ There might be possible that bits gets inverted during the transmission. That is, 0 is flipped to 1 and 1 is flipped to 0. When receiver receives the message with corrupted bits, it detects that this is not the correct data.
  - ✓ Once error is detected, receiver asks sender to retransmit the same data. Or receiver itself corrects the error and accept the data.
  - ✓ To achieve error control mechanism, the sender adds some redundant bits in the original message.
- Access control: - The access control is done by the Medium Access Control sub-layer.
  - ✓ There are multiple number of computers shares the common channel for the communication. Only one computer may transmit the data at

given time. If more than one computer attempts to transmit, collision occurs. Collision results in unsuccessful transmission.

- ✓ The MAC mechanism provides ways to administrate the communication over a shared channel from multiple user. It ensure that no collision occurs. And if collision occurs, then all affected machines comes to know.

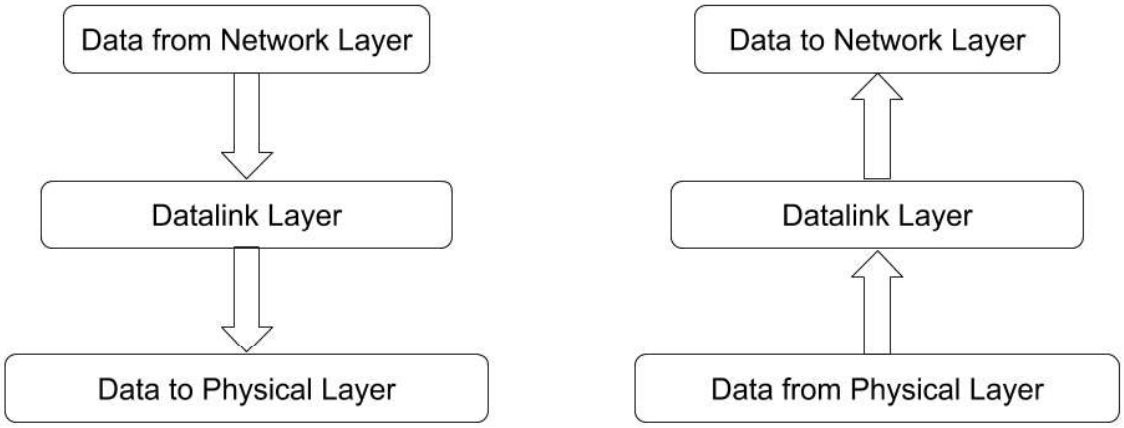


Fig – Datalink Layer

3.5 THE NETWORK LAYER

Network layer provides host-to-host transmission. Network layer is responsible for forwarding the packet from source to the destination. There may be several intermediate hosts between source and destination. The network layers performs the functions as follows:

- Packetizing: - Network layer accept the segment from the transport layer. It divides the segment into small size packets at sender side. At the receiver side, it bunches packets to prepare a segment.
- Routing: - It routes the packet from the source to the destination. It forward the packet to the next router. The packet is forwarded from router to router and reaches to the destination.
- Routing is performed according to the routing protocols. The router also considers the information exists in the routing table. The routing table entries guides the routing process to find and reach to the destination.

- IP addressing: - It assign the logical addressing to the packet. The logical address is also known as IP address. The IP address of a machine is unique in the internet.

In addition to the major functionalities of the network layer, it can provide several other features as well. Such as,

Quality of service management

- Congestion control – Congestion control in the network layer is the primary requirement. Congestion in the network is a state in which too many datagrams are present at a particular location of the network.
- Congestion occurs if the computers in the network too many packets which exceeds the capacity of the router.
- To get rid of this situation, some router starts dropping the packets. This may lead to the worst situation of the network. Because due to error control mechanism, the sender retransmit for the lost or unacknowledged packets.
- There are some congestion control mechanism, which helps router come out of congestion or prevent the congestion at all. For example, a leaky bucket method prevents the network from running into congestion.

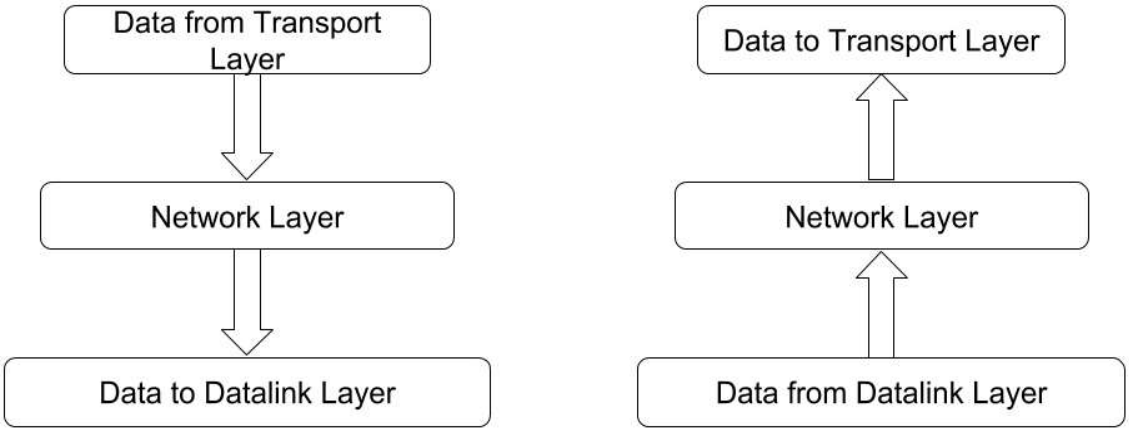


Fig – Network Layer

3.6 THE TRANSPORT LAYER

The transport layer receives the service from session layer and provides the service to the network layer in OSI reference model stack. Basically it receives the message from session layer and divides into segments. It guarantees about correct delivery of all segments. The major duties of the transport layer are as follows:

- It provides process-to-process delivery between source and destination. The transport layer uses a port to identify the process of application. The process-to-process delivery is important because multiple applications might be exchanging the data between source and destination.
- It does segmentation and reassembly. The session layer hands over the complete session of the data to the transport layer. The transport layer splits the session of data into smaller segments.
- The segmentation of the session data is taken place at the sender. The assembly of the segments is performed at the receiver to form the session.
- It also provides error control for the data in the segment.
- It can provide connection less and connection oriented service.

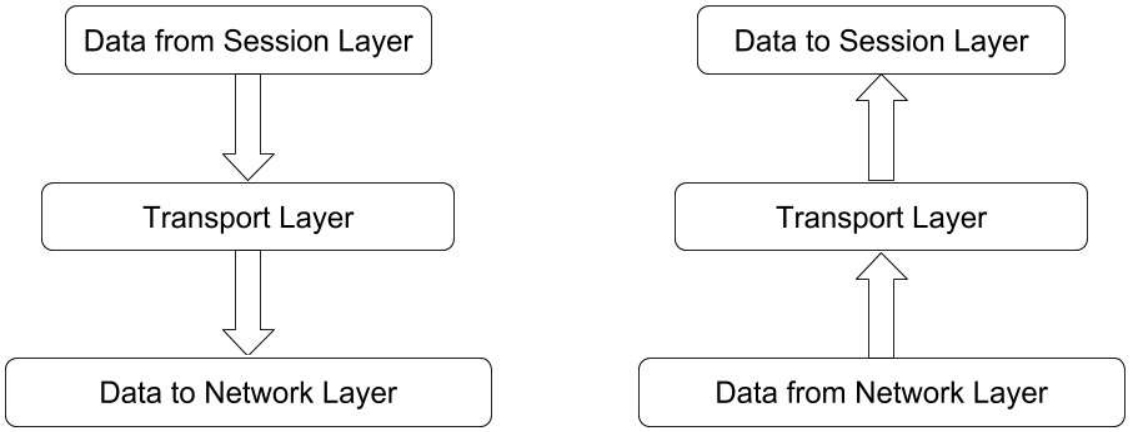


Fig – Transport Layer

3.7 THE SESSION LAYER

The session layer enables computers in the network to set the active communication sessions between them. It establishes the session first and synchronize the communication between two end systems. It receives the message from the presentation layer and gives to the transport layer. The functions of the session layer are:

- It allows computers to start the communication either in full-duplex mode or half-duplex mode.
- It allows the system to put check points at regular interval. In other words, it marks the successful transmission after a fix unit of data sending successfully. For example, there are total 1000 Mb data are to be transmitted. It puts check points at every 100 Mb. Then it ensures the successful transmission of every 100 Mb data and acknowledged.
- The checkpoint mechanism is very beneficial when at the time of system crash. If system crash is reported at 130 Mb data transmission, then sender does not retransmit all 130 Mb data. But it resume the transmission after the last check point. That is, it transmit recent 30 Mb data.

The Session Layer allows users on different machines to establish active communication sessions between them.

Its main aim is to establish, maintain and synchronize the interaction between communicating systems. Session layer manages and synchronize the conversation between two different applications. In Session layer, streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

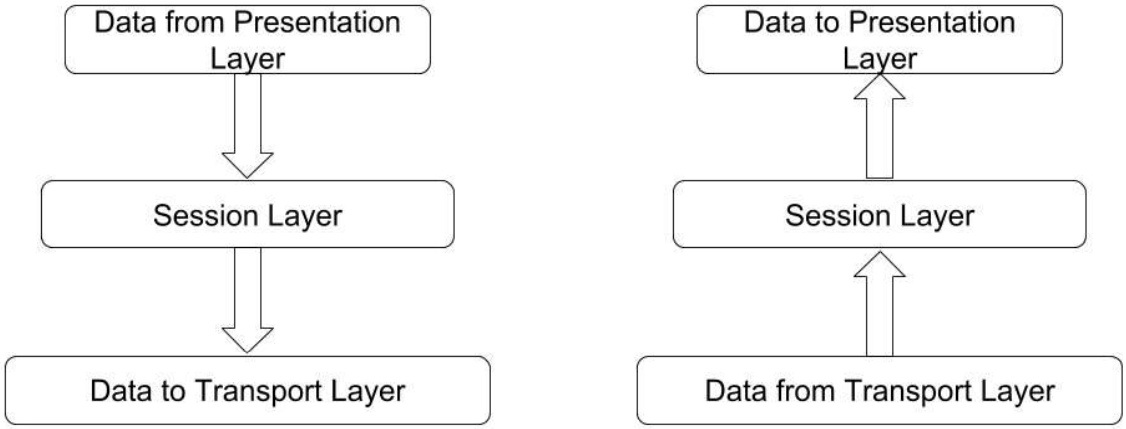


Fig – Session Layer

3.8 THE PRESENTATION LAYER

The presentation layers enables two computers to communicate, even though they are using different data representation. Presentation layer mainly does three tasks.

- Translation – The end user prepare the message in the form of characters, numbers, images, audio, video etc. The presentation layer is responsible to convert the message into binary format. It translate the data based on the computer and network requirement.
- Encryption – The data is sent at far distance geographically over unsecured channel. The cable cannot be protected between the source and the destination. Therefore, data is to be transformed in such a form, which cannot be understood by some unauthorized person. An encryption technique provides this strength. It encrypt the data the sender side, and decrypts the data at the receiver side. Decryption does exactly reverse process that of encryption. It retransform the encrypted message to the original form.
- The encryption of the message is carried out at the sender, and decryption at the receiver.
- Compression – The compression is very important feature of the presentation layer. Compression is about reducing the size of the message before transmission. The sender fist reduce the size up to some possible extent and then it transmit to the receiver.

- The percentage of compression of original message depends on the technique of the compression applied on it.
- The receiver receives the compressed message and then decompress to get the original message.

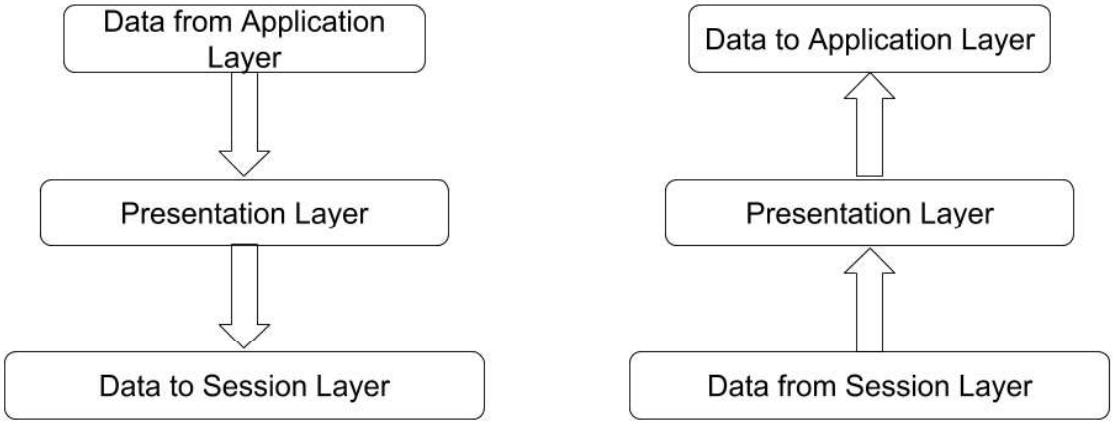


Fig – Presentation Layer

3.9 THE APPLICATION LAYER

The application layer is the top most layer of the OSI reference model. It provides user interface (graphical or command line) to the communication parties basically. The application layer offers variety of protocols through the user interface. It defines message format, syntax and semantics. The protocols includes Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Simple Mail Transfer Protocol (SMTP), Teletype Network (TELNET), Domain Name System (DNS) etc.

- Application layer provides the email services.
- It provides access to World Wide Web.
- It allows to use file transfer service.
- User can log in from remote place using application layer.

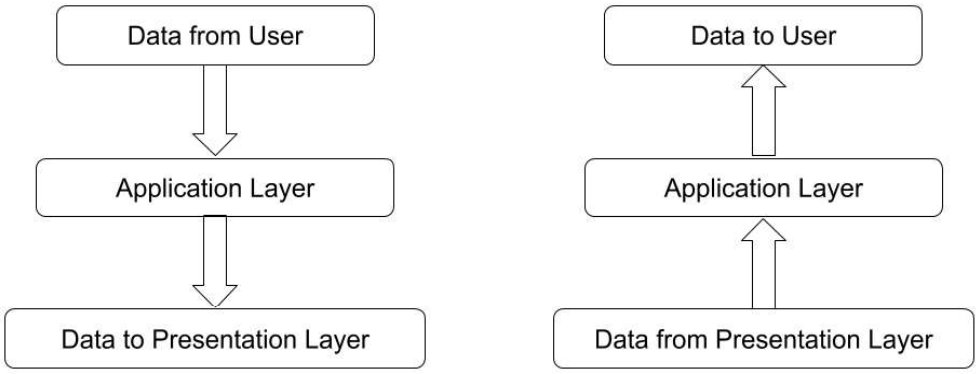


Figure – Application Layer

3.10 LET US SUM UP

- In this chapter, the conceptualization of the OSI reference model has been described.
- We learned the functions OSI reference model layers.
- We also gone through the basic three types of transmission mode.
- We understood various network topologies.
- We learned about the interaction between the layers of the OSI model.

3.11 CHECK YOUR PROGRESS

1. True-False

    1) Physical layer is responsible for framing of the packets.
    2) Presentation layer compress the original message before passing to the session layer.
    3) Network layer is responsible for IP addressing.
    4) Data link layer provides error control and flow control.
    5) Graphical user interface is a part of presentation layer.
    6) Assemble of packets is performed by receiver transport layer.

2. Matching

A	B
Node-to-node delivery	Network layer
Host-to-host delivery	Transport layer
Process-to-process delivery	Data link layer

A	B
Segments	Network layer
Fames	Transport layer
Packets	Data link layer
sessions	Session layer

3. Multiple choice

1) Which topology covers security, robust and eliminating traffic factor?

A. Mesh
B. Ring
C. Star
D. Bus

2) Multipoint topology is

A. Bus
B. Star
C. Mesh
D. Ring

3) What is/are the major role/s of Data Link Layer (DLL) in an OSI model?

A. Detection & Correction of transmission errors
B. Provision of data flow control to prevent DTE from overburdening

C. Identification of various devices on the network
D. Generation of a frame for easy data transfer

4) Which OSI layer allows the transmission and reception of data segments to a session layer in addition to the provision of flow control, sequence numbering and messageacknowledgment?

a. Network Layer
b. Session Layer
c. Transport Layer
d. Application Layer

5) Which is the only layer of OSI layer that prevents itself from adding its own header to the data during the data transmission process?

a. Application layer
b. Network layer
c. Physical layer
d. None of the above

6) Which among the following represents the objectives/requirements of Data Link Layer?

a. Frame Synchronization
b. Error & Flow Control
c. Both a & b
d. None of the above

7) Which layer deals with TCP and UDP

A. Transport Layer

B. Physical Layer

C. Network Layer

D. None of above

8) Which type of RJ45 UTP calbe is used between switches

A. straight-through cable

B. Crossover cable

C. Both can be used

D. None can be used

9) Which layer deals with Network topology

A. Physical Layer

B. Datalink Layer

C. Network Layer

D. Session Layer

10) Segments are made on which layer

A. Session Layer

B. Transport Layer

C. Application Layer

D. Network Layer

11) Physical layer is responsible for

A. Node to node communication
B. Peer to peer communication
C. Hop to hop communication

D. both a and c

12)OSI model deals with physical, data link, network, transport, session and

A. Presentation layer
B. Application layer
C. both a and b
D. None of Above

13)Logical Addresses are

A. 16bit long
B. 32bit long
C. 64bit long
D. 128bit long

14) Error Control and Flow Control are responsibilities of

A. data link and network Layers
B. data link and Physical Layer
C. Application and Presentation Layer
D. data link and Transport Layer

15) In transport layer, message is divided into transmittable

A. packets
B. bits
C. Segments
D. frames

16) Layer that are used to deal with mechanical and electrical specifications are

A. Physical Layer
B. Data Link Layer
C. Network Layer
D. Transport Layer

17) Process on each machine that communicate at a given layer is called

A. peer-to-peer
B. Physical transmission
C. Node to Node
D. Hop to hop

18) Layer that is responsible for transferring Frames is

A. Application layer
B. Presentation layer
C. Data link layer
D. Session layer

19) Framing, Error Control, Flow control, Access control are responsibilities of

A. 1st layer
B. 2nd layer
C. 3rd layer
D. 4th layer

20) Session layer is responsible for

A. Error Control and Flow Control
B. Framing and Access Control
C. dialog control and synchronization
D. Segmentation and reassembly

21) Route determination can be identified by

A. Transport layer
B. Application layer
C. Network layer
D. Presentation layer

4. Why framing is required?

5. Why flow control is needed?
6. What is process to process delivery? How does differ from host-to-host and node-to-node delivery?

3.12 FURTHER READING

Recommended Text

1. Forouzan (2013). Data Communication and Networking – 5E, McGraw Hill
2. Andrew S. Tanenbaum and David J. Wetherall (2011). Computer Networks - 5th Edition

3.13 ASSIGNMENTS

- Enlist the functions of layers of OSI reference model.
- Describe the functions of transport layer.
- What is the difference between physical address and logical address?
- What is segmentation and reassembly? Which OSI layer is responsible for it?
- What is the difference between error correction and error detection?

3.14 ACTIVITIES

- Download Cisco packet tracer tool and install in a system.
- Setup start topology in cisco packet tracer.
- Check network commands such ping, tracert using Cisco packet tracer tool.
- Assign IP address to the system connected in the network.

Unit 4: IEEE Standards

4

Unit Structure

4.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Explain what is IEEE standards and why they are needed to define
- Describe IEEE 802.2 standards and its variations
- Describe IEEE 802.3 standards and its variations
- Describe IEEE 802.11 standards and its variations
- Describe IEEE 802.15 standards and its variations

4.2802 STANDARDS

The IEEE 802 Standard contains the networking standards that cover the physical layer specifications of technologies from Ethernet to wireless. IEEE 802 is subdivided into 22 parts that cover the physical and data-link aspects of networking.

The Institute of Electrical and Electronics Engineers is a standards setting organization. Each of their standards is numbered and a subset of the number is the actual standard. The 802 family of standards is ones developed for computer networking. we will look at several networking technologies: 802.2, 802.3 ethernet, 802.5, 802.11 Wi-Fi, 802.15 Bluetooth/ZibBee and 802.16

4.3IEEE 802.2 (LOGICAL LINK CONTROL SUBLAYER)

The logical link control is the sub layer of data link layer. The IEEE 802.2 is the part of family of local area network. It basically deals with the physical layer and datalink layer of the OSI reference model. It describes the functions, features, protocol, and services of the logical link control (LLC) sublayer. It is also known as ISO/IEC 8802-2 standard. The original standard settled by the IEEE in collaboration with the American National Standards Institute (ANSI) was adopted by the International Organization for Standardization (ISO) in 1998, but it still remains an integral part of the family of IEEE 802 standards for local and metropolitan networks.

The Medium Access Control (MAC) is the upper layer of LLC. The MAC sublayer creates the message and passes to the LLC. The LLC sublayer adds some control

information to this message. The resulting packet is denoted as protocol data unit (PDU). The additional information is said to be LLC header. The LLC header comprised on three segments: of DSAP (Destination Service Access Point), SSAP (Source Service Access Point) and the Control field.

The protocol data unit (PDU) structure for data communication systems is defined using bit-oriented procedures, as are two types of operation for data communication between service access points. In one type of operation, PDUs are exchanged between LLCs without the need for the establishment of a data link connection. In the other, a data link connection is established between two LLCs prior to any exchange of information-bearing PDUs.

Lets look at the LLC PDU header.

LLC PDU header

802.2 LLC header			Information
DSAP address	SSAP address	Control	
8 bits	8 bits	8 or 16 bits	Multiple of 8 bits

DSAP address and SSAP address is the length of 8 bits. They do allow to multiplex various upper layer protocol above the LLC. However, many protocols use the Subnetwork Access Protocol (SNAP) extension which permits using EtherType values to specify the protocol being transported atop IEEE 802.2. The SNAP extension is added to the 802.2 LLC PDU header.

Subnetwork 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

The 802.2 header includes two eight-bit address fields, called service access points (SAP) or collectively LSAP in the OSI terminology:

- SSAP (Source SAP) is an 8-bit long field that represents the logical address of the network layer entity that has created the message.
- DSAP (Destination SAP) is an 8-bit long field that represents the logical addresses of the network layer entity intended to receive the message.

IEEE 802.2 offers two connectionless and one connection-oriented operational units.

- Type 1 – This is unacknowledged mode for datagram service. It allows sending of frames with three options.
  - Unicast transmission (point-to-point or single destination)
  - Multicast transmission (multiple destinations)
  - Broadcast transmission (to all machines of the network)
- Type 2 – This is for connection-oriented operation mode. The frame orders are guaranteed by the sequence number. The loss of the frame is tracked.
- Type 3 – This is for acknowledged connectionless service. It supports unicast communication.

Each network node is assigned an **LLC Class** according to which service types it supports.

LLC class	Supported service type		
	1	2	3
I	X		
II	X	X	
III	X		X
IV	X	X	X

Control Field

The control field is the third field after destination SAP and source SAP. IEEE 802.2 was conceptually derived from HDLC. Therefore, it has three types of PDUs.

- **U-format** (Unnumbered) PDUs with an 8-bit control field. This is for connectionless service.
- **I-format** (Information) PDUs, with a 16-bit control and sequence numbering field, which are intended to be used in connection-oriented applications;
- **S-format** (Supervisory) PDUs, with a 16-bit control field, which are intended to be used for supervisory functions at the LLC (Logical Link Control) layer.

4.4IEEE 802.3 (MEDIUM ACCESS CONTROL SUBLAYER)

IEEE 802.3 standard defines physical layer and datalink layer's medium access control sublayer. 802.3 is a technology that supports the 802.1 architecture. 802.3 also defines LAN access using the technique Carrier Sense Multiple Access/Collision Detection (CSMA/CD).

Each Ethernet standard possess a basic frame format. So, all implementation of MAC sublayer does have a specific frame format.

PREAMBLE	SFD	DESTINATION ADDRESS	SOURCE ADDRESS	LENGTH	DATA	CRC
7 byte	1 byte	6 byte	6 byte	2 byte	46-1500 byte	4 byte

802.3 ETHERNET FRAME FORMAT

- PREAMBLE – This field indicates starts of the Ethernet frame. It composed of 7 bytes. The pattern is alternative 0's and 1's. PREAMBLE helps sender and receiver establish the synchronization. It specifies the receiver that frame is to arrive and allow receiver to get ready to receive actual data stream.
- Start of frame delimiter (SFD) – The length of SFD is 1 byte and pattern is set to 10101011 always. Sometimes SFD is appended with PREAMBLE. So it becomes 8 byte long.

- Destination Address – It is the physical address of the destination machine. The MAC deals with 6-byte long physical address.
- Source Address - It is the physical address of the destination machine. It is also 6-byte long.
- Length – It specifies length of the entire frame. It is 2-byte long. The 16-bit can map the decimal value from 0 to 65534. But the maximum data present may be 1500 bytes at max.
- Cyclic Redundancy Check (CRC) – CRC for error detection at the receiver point. It is 32-bits long hash value, which is generated at both sides. If the sender and receiver check sum does not match, the error is detected.

Extended Ethernet Frame (Ethernet II Frame)

Standard IEEE 802.3 basic frame format is discussed above in detail. Now let's see the extended Ethernet frame header, using which we can get Payload even larger than 1500 Bytes.

DA	SA	Type	DSAP	SSAP	Ctrl	Data	FCS
6 Byte	6 Byte	2 Byte	1 Byte	1 Byte	1 Byte	> 46 Byte	4 Byte

DA - Destination MAC Address
SA - Source MAC Address
Type - Ethertype
DSAP - 802.2 Destination Service Access Point
SSAP - 802.2 Source Service Access Point
Ctrl - 802.2 Control Field
Data - Protocol Data
FCS - Frame Checksum

Various extensions of the IEEE 802.3 standard are mentioned in the table below.

STANDARD SUPPLEMENT	YEAR	DESCRIPTION
802.3a	1985	10Base-2 (thin Ethernet)
802.3c	1986	10 Mb/s repeater specifications (clause 9)
802.3d	1987	FOIRL (fiber link)
802.3i	1990	10Base-T (twisted pair)
802.3j	1993	10Base-F (fiber optic)
802.3u	1995	100Base-T (Fast Ethernet and auto-negotiation)
802.3x	1997	Full duplex
802.3z	1998	1000Base-X (Gigabit Ethernet)
802.3ab	1999	1000Base-T (Gigabit Ethernet over twisted pair)
802.3ac	1998	VLAN tag (frame size extension to 1522 bytes)
802.3ad	2000	Parallel links (link aggregation)
802.3ae	2002	10-Gigabit Ethernet
802.3as	2005	Frame expansion
802.3at	2005	Power over Ethernet Plus

4.5IEEE 802.11 (WIRELESS LOCAL AREA NETWORK)

IEEE working group developed 802.11 for wireless local area networks. It encompasses several specifications and newly are added at times. Likewise 802.2 MAC sublayer, the 802.11 also uses CSMA/CD. The phase-shift keying was used originally in 802.11. Nonetheless, other code keying was also added such as complementary code keying (CSK).

802.11a

- ✓ 802.11a uses the Orthogonal Frequency Division Multiplexing (OFDM).
- ✓ The maximum data rate for 802.11a is 54 Mbit/s, but the achievable throughput is around 20 Mbit/s.
- ✓ It defines a Wi-Fi format for providing wireless connectivity in the 5 GHz ISM band.

- ✓ 802.11a has 12 non-overlapping channels, 8 dedicated to indoor and 4 to point to point.

802.11b

- ✓ It is broadly accepted and adopted for the Wi-Fi LAN.
- ✓ It may transmit the data at raw data rates up to 11 Mbps. However, it does not operate at full data rate.
- ✓ It uses the complementary Code Keying (CCK).
- ✓ When a node wants to transmit, it listen the channel and transmit.
- ✓ It listen the channel for a back off random amount of time. If it does not receive, then it retransmit the data.
- ✓ The machine examines the quality of signal. It the quality of the signal falls then it slows down the data rate.
- ✓ Under this condition, the system first curtails the speed at 5.5 Mbps, 2 Mbps and then 1 Mbps.

SUMMARY OF 802.11B WI-FI STANDARD SPECIFICATION

PARAMETER	VALUE
Date of standard approval	July 1999
Maximum data rate (Mbps)	11
Typical data rate (Mbps)	5
Typical range indoors (Meters)	~30
Modulation	CCK (DSSS)
RF Band (GHz)	2.4
Channel width (MHz)	20

802.11d

- ✓ It is similar to 802.11b in most of the factors.
- ✓ In some countries, 802.11b is not allowed to operate, such countries opt for 802.11d.

- ✓ The key characteristics of 802.11d is that it can be customized to fulfil the requirements of rules and regulations.
- ✓ This feature eliminates the need of manufacturing dozens of different hardware solutions.

802.11e

- ✓ 802.11e is proposed enhancement over 802.11a and 802.11b.
- ✓ It provides good Quality of Service. It gives prioritization of data, video and voice transmission.
- ✓ 802.11e enhanced 802.11 with Time Division Multiple Access (TDMA).
- ✓ In 2005, it became widely used for business and consumer products.

802.11g

- ✓ It can support high data speed as it uses frequency band 2.4 GHz.
- ✓ The lower cost of chips using 2.4GHz joined with the higher speed. It caused to become the 802.11g dominant Wi-Fi technology.
- ✓ 802.11g provides number of improvements over 802.11a and 802.11b. The main specifications are mentioned in the table.

FEATURE	802.11G
Date of standard approval	June 2003
Maximum data rate (Mbps)	54
Modulation	CCK, DSSS, or OFDM
RF Band (GHz)	2.4
Channel width (MHz)	20

4.6 802.15 WIRELESS PERSONAL AREA NETWORK

- ✓ IEEE 802.15 defines Wireless Personal Area Network (WPAN). The IEEE 802.15 has also got several alternations.

802.15.1

- ✓ The IEEE 802.15.1 was the first version. It was adapted from the Bluetoothspecification and is fully compatible with Bluetooth 1.1.
- ✓ 802.15 is a communications specification that was approved in early 2002 by the Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) for wireless personal area networks (WPANs).
- ✓ Bluetooth is a renowned and extensively used description that describes parameters for wireless communications among portable digital devices.
- ✓ The notebook computers, peripherals, cellular telephones are the examples of personal area network.
- ✓ The specification also permits for connection to the Internet.
- ✓ There are two categories of IEEE 802.15 named TG3 and TG4.
- ✓ The version TG4 supports low data speeds from 20 Kbps to 250 Kbps.
- ✓ The version TG3 supports high data speeds from 11 Mbps to 55 Mbps.
- ✓ It allows to inter connect up to 254 devices.
- ✓ There are some smart features it supports such as dynamic addressing, full handshaking, security provision and power management.
- ✓ There are total 16 channels in the 2.4 GHz band, 10 channels in 915 MHz band, one channel in 868 MHz band.

802.15.2

- ✓ It supports the coexistence of a wireless personal area network with other wireless personal area network.
- ✓ Such scenario arises due to two PANs operating in unlicensed frequency.
- ✓ The IEEE 802.15.2-2003 standard was published in 2003.

802.15.3

- ✓ IEEE 802.15.3-2003 is a MAC and PHY standard for high-rate (11 to 55 Mbit/s) WPANs.

802.15.3a

- ✓ IEEE 802.15.3 was an attempt to provide high data speeds.
- ✓ It is designed for the applications which use the imaging and multimedia.

802.15.3b

- ✓ It enhanced the IEEE 802.15.3a for improving implementation and interoperability of MAC.
- ✓ It is backward compatible and also added more clarifications. Such as,
    - o Acknowledgement policy and polling
    - o Multicast address assignment
    - o Multiple contention period in super frame

4.7 LET US SUM UP

We learned several important IEEE standards for the Local Area Network. The IEEE 802 Standard contains the networking standards that cover the physical layer specifications of technologies from Ethernet to wireless. The protocol data unit (PDU) structure for data communication systems is defined using bit-oriented procedures, as are two types of operation for data communication between service access points. IEEE 802.2 offers two connectionless and one connection-oriented operational units. IEEE 802.3 standard defines physical layer and datalink layer's medium access control sublayer. IEEE working group developed 802.11 for wireless local area networks. 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. 802.11a uses the Orthogonal Frequency Division Multiplexing (OFDM). 802.11b is broadly accepted and adopted for the Wi-Fi LAN. It is similar to 802.11b in most of the factors. 802.11e is proposed enhancement over 802.11a and 802.11b. 802.11g can support high data speed as it uses frequency band 2.4 GHz. Each Ethernet standard have their own frame or packet format. Moreover, the source address, destination address and some control fields are the part of frame format. The IEEE standards are sometimes customized for specific region or territory.

4.8 CHECK YOUR PROGRESS

1. Fill in the blanks.

1) The size of the DSAP address in LLC PDU header is _____ bits.
2) The size of the SSAP address in LLC PDU header is _____ bits.
3) The RF band for 802.11g is _____ GHz.
4) Maximum Data rate for 802.11g is _____ Mbps.
5) The modulation technique for 802.11b is _____.
6) SFD stands for _____.
7) The preamble of the Ethernet frame is _____ byte long.
8) The MAC address is _____ byte long.
9) Cyclic Redundancy Check is for _____ mechanism.
10) 802.11e uses _____ Division Multiple Access.
11) 802.15 is for _____ Area Network.
12) 802.2 is for _____Area Network.

2. Multiple choice Questions.

1) Protocol Data Unit (PDU) is similar to

A. LLC
B. HDLC
C. MAC
D. DSAP

2) Computer Society of IEEE started a project named project 802 in

A. 1970
B. 1975
C. 1980
D. 1985

3) Term that is used to set standards to enable intercommunication among equipment from a variety of manufacturers is called

A. Project 802
B. Project 8802
C. Project 2088
D. Project 208

4) IEEE Standard was adopted by the

A. ISO
B. ANSI
C. OSI
D. None of the above

5) In IEEE Project 802, Logic Link Control (LLC) is used to control and handle the

A. errors
B. flow
C. frames
D. all of the above

6) IEEE 802.11 have three categories of

A. frames
B. fields
C. signals
D. sequences

7) DCF stands for

A. Direct Control Function
B. Distributed Control Function
C. Direct Cooperate Function
D. Distributed Coordination Function

8) Bluetooth is _____ technology that connected devices in small area.

A. VLAN
B. Wireless LAN
C. Wired LAN
D. None of the above

9) 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

10) Token ring is a data link technology for?

A. Wide Area Network
B. Metropolitan Area Network
C. Local Area Network
D. Both A and B above

3. Match the following.

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

4.9 FURTHER READING

- IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture
  http://www.ieee802.org/secmail/pdfocSP2xXA6d.pdf

- Part 2: Logical Link Control
  https://signallake.com/publications/1998802.2LogicalLinkControl.pdf

- IEEE CSMS/CD based LANs
  https://nptel.ac.in/courses/106105080/pdf/M5L3.pdf

- LLC-802.2 Based Congestion Management
  http://www.ieee802.org/3/cm_study/email/pdf00000.pdf

- http://protocols.netlab.uky.edu/~calvert/classes/571/lectureslides/802overview.pdf
  Overview of IEEE 802 Standards

4.10 ASSIGNMENTS

- Show the format for 802.2 LLC PDU header. Explain the importance of each field.
- Compare different 802.11 wireless network standards.
- Explain three type of PDUs for 802.2 control fields.
- Write short note on PAN.
- Compare Wireless LAN with Wireless PAN with respect to IEEE 802 standards.

4.11 ACTIVITIES

- Analyze the packet header of 802.2 using network simulator tool.

Block-3

Transmission Media and TCP/IP

Unit 1: Transmission Media 1

Unit Structure

1.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Distinguish the characteristics of wired transmission.
- Understand the Bandwidth usage and attenuation in wired transmission.
- Understand about Electromagnetic Interference.

1.2 INTRODUCTION

In Computer Networks, Transmission media is a physical path between sender and receiver, that can be classified in two types as shown in Figure-1:

- **Guided: Transmission** limit depends fundamentally on the medium, its length etc. Coaxial cables, twisted pair, Fiber Optics are the examples of it.
- **Unguided** (**Often known as wireless**)**:** Transmitting electromagnetic waves yet do not control them.

In guided media, medium qualities is progressively essential, while in unguided media, signal attributes is increasingly vital.In this unit we will examine the attributes of different transmission media, both guided and unguided.

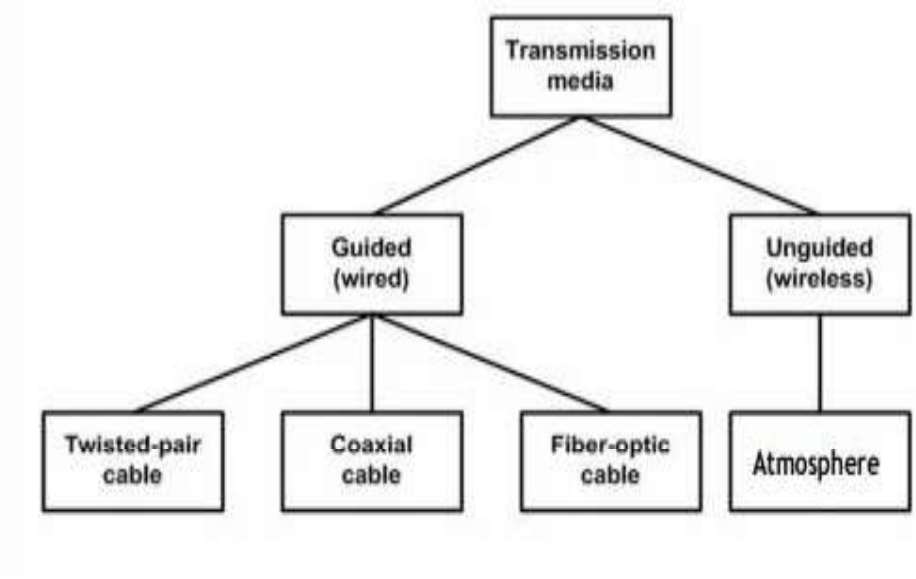


Figure-1:Classification of the transmission media

1.3 CHARACTERISTICS OF MEDIA

Each kind of transmission media has exceptional qualities that make it reasonable for a particular sort of services. We should be familiar with these characteristics:

- Cost
- Installation Requirements
- Bandwidth
- Band Usage (Baseband or Broadband)
- Attenuation
- Electromagnetic Interference

1.3.1 Cost

There are two types of costs that are important for transmission media :

1. The cost of installing media
2. Maintenance cost

The cost of installing media includes the other supportive devices which can be used in future. There is generally a requirement for tradeoffs between cost, data transfer capacity(Bandwidth), and distance ,i.e. if distance of media increase then cost increases and bandwidth decreases.

1.3.2 Installation Requirements

As we have discussed about guided and unguided transmission types; instalment requirements generally very complex in guided transmission where less complex in unguided one.

1.3.3 Bandwidth

In networking, the term bandwidth alludes to the proportion of the limit of a medium to transmit information. A medium that has a high limit, for instance, has a high data

transfer capacity (bandwidth), while a medium that has constrained limit has a low transmission capacity (bandwidth).

Data transmission rates as often as possible are expressed as far as the bits that can be transmitted every second. An Ethernet LAN theoretically can transmit 10 million bits for every second and has a transmission capacity of 10 megabits for every second (Mbps).

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 1 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 1 second.Refer Fig.-2.

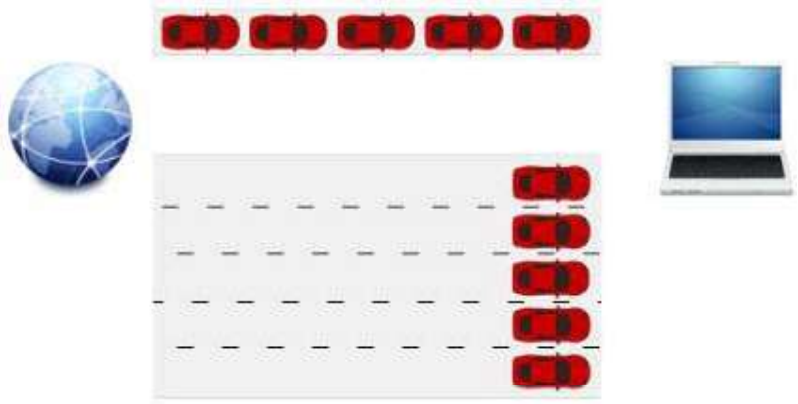


Figure-2: Bandwidth explanation with roads example

The data transmission that a link(Cable’s length) can accommodate is resolved to some degree by the link's length. A short link by and large can oblige more

prominent data transfer capacity than a long link, which is one reason every link configuration indicate most extreme lengths for link runs. Past those limits, the most noteworthy recurrence signs can break down, and blunders start to happen in information signals.

Understand that transmission capacity can be communicated in any unit (bytes, kilobytes, megabytes, gigabits, and so on.). Your ISP may utilize one term, a testing administration another, and a video spilling administration one more. You'll have to see how these terms are altogether related and how to change over between them on the off chance that you need to abstain from paying for an excess of network access or, possibly more awful, requesting unreasonably little for what you need to do with it.

For instance, 15 MBps isn't equivalent to 15 Mbps (note the lowercase b). The principal peruses as 15 mega BYTES while the second is 15 mega BITS. These two qualities are diverse by a factor of 8 since there are 8 bits in a byte.

1.3.4 Band Usage (Baseband or Broadband)

The two different ways to allot the limit of transmission media are with baseband and broadband transmissions. Baseband dedicates the whole limit of the medium to one correspondence channel. Broadband empowers at least two correspondence channels to share the transfer speed of the communications medium.

Baseband is the most well-known method of networkingactivity. Most LANs work in baseband mode, for instance, baseband signalling can be adapted with both analog and discrete signals.

Despite the fact that you probably won't understand it, you have a lot of experiments with broadband transmissions. Consider, for instance, that the television cable coming into your 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. You can utilize the TV tuner to pick the channel you need to watch by choosing its frequency. This strategy of isolating transfer speed into recurrence groups is called

Frequency Division Multiplexing (FDM) and works just with analog signals. Another system, called Time Division Multiplexing (TDM), supports discrete signals.

1.3.5Attenuation

Attenuation is a proportion of how much a signals weakens as it goes through a medium. The degree of attenuation is typically expressed in units called decibels (dBs).

If P_t is the signal power at the transmitting end (source) of a communications circuit and P_r is the signal power at the receiving end (destination), then $P_t > P_r$. The power attenuation A_p in decibels is given by the formula:

$$\boldsymbol{A_p = 10 \log_{10}(P_t/P_r)}$$

Attenuation can also be represented in terms of voltage. If A_v is the voltage attenuation in decibels, V_t is the source signal voltage, and V_r is the destination signal voltage, then:

$$\boldsymbol{A_v = 10 \log_{10}(V_t/V_r)}$$

Attenuation is a contributing element to why cables structures must determine restrains in the lengths of cables runs. At the point when signal quality falls beneath specific restricts, the electronic equipments that gets the signals can encounter trouble segregating the original signal from the noise present in every single electronic transmission.

1.3.6 Electromagnetic Interference

Electromagnetic interference (EMI) consists of outside electromagnetic noise that distorts the signal in a medium. For instance, you frequently hear EMI as commotion brought about by engines or lightning. Some system media are more helpless to EMI than others.

Crosstalk is an uncommon sort of obstruction brought about by nearby wires. Crosstalk is an especially critical issue with PC systems since huge quantities of

cables regularly are found near one another with insignificant regard for definite position.

1.4 LET US SUM UP

Transmission media are located below the physical layer. Signals are transmitted in form of electromagnetic energy. There are two types of transmission media are being classified as : 1)Guided & 2) Unguided. Bandwidth refers to the data carrying capacity of a channel or medium. Higher bandwidth communication channels support higher data rates. 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.

1.5 CHECK YOUR PROGRESS

1. What is transmission media? How many types of it?
2. 5MBps = _____ Kbps.
3. Find out the attenuation power(loss) when the signal power at transmitter is 80 db and at the receiver side it reduces to 25 db.
4. Give minimum 4 real time examples of Electromagnetic interference (EMI).

1.6 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

A.1 Transmission media is a physical path between sender and receiver that can be classified in two types as shown in Figure-1:

- **Guided :** Transmission limit depends fundamentally on the medium, its length etc. Coaxial cable, Twisted pair, Fiber Optics are the examples of it.
- **Unguided** (**Often known as wireless**)**:** Transmitting electromagnetic waves yet do not control them.

A.2 5MBps = 5*8 Mbps=40 Mbps =40*1024 Kbps ≈ 40000 Kbps

A.3 Attenuation Power=10log(80/25)=5.0515 db

A.4 Self Study

1.7 FURTHER READING

1. ForouzanBehrouzA ," Data Communications and Networking" , McGraw-Hill,New York.

1.8 ASSIGNMENTS

- Explain the characteristics of transmission media in detail.
- Differentiate Guided transmission media and Unguided transmission media.

1.9 ACTIVITIES

- Make a chart of different guided and unguided transmission media on the basis of its characteristics.

Unit 2: Cable Media 2

Unit Structure

2.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Understand the properties and uses of coaxial cable.
- Understand the the properties and uses of twisted pair cable.
- Understand the properties and uses of fiber optic cable.

2.2 INTRODUCTION

As we know, the task of physical layer is to transmit and receive bits/bytes from source to receiver. We discussed the types of transmission media is last unit which are:

1) Guided transmission media and

2) Unguided transmission media.

Guided media focuses on point to point or multipoint communication where medium, length of cable are important factors. On the other hand unguided media focuses on electromagnetic signal for communication where noise is an important factor.

In this unit we are going to focus on different guided media which are coaxial cable , twisted pair &fiber optic cable.

2.3 COAXIAL CABLE

Coaxial cable (Sometimes referred as coax) , comprises of two conductors, to allow it to work over a more wider range of frequencies.It comprises ofa hollow outer cylindrical conductor that encompasses a single inner wire conductor (Figure-1).The inward transmitter is held set up by eitherregularly spaced insulating rings or a solid dielectric material.The external conductor is secured with a coat or shield.A solitary coaxial cable has a diameter across of from 1 to 2.5 cm.Coaxial cable can be utilized over longer distance and support a bigger number of stations on a common line than twisted pair cable. Coaxial cables 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.

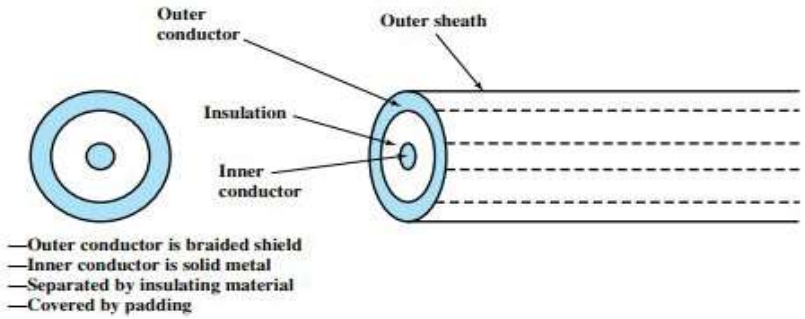


Figure-1 Coaxial Cable

2.3.1 Standards

Coaxial links are classified bytheir radio government (RG) ratings.Every RG number means an interesting arrangement of physical details, including the wire measure ofthe inner conductor,the thickness and type of the inner insulator,the development of the shield, and the size and sort of the external packaging.Each cable characterized by a RG rating is adjusted for a specific capacity.

Category	Impedance	Use
RG-59	75Ω	Cable Television
RG-58	50Ω	Thin Ethernet
RG-11	50Ω	Thick Ethernet

Table:-1 Categories of coaxial cables

2.3.2 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 analogtelephone systems where a solitary coaxial system could convey 10,000 voice signals. Later it was utilized in digitaltelephone systems where a solitary coaxial link could convey advanced information up to 600 Mbps. In any case, coaxial link in phone systems has generally been supplanted today with fiber optic link.

Cable TV networks also utilize coaxial cables.In the conventional satellite TV organize, the whole system utilized coaxial cables.Later, however, cable TV providers replaced most of the media with fiber-optic cable; crossover systems utilize coaxial link just at the system boundaries,close to the customer premises. Digital TV utilizes RG-59 coaxial link.

2.3.3 Advantages & Disadvantages

Advantages:

- Greater channel capacity than twisted pair.
- Greater bandwidth compared to twisted pair.
- Lower error rate (Appox. 10^{-9} bps)

Disadvantages:

- Installation is difficult
- Installation cost
- Great noise

2.4TWISTED PAIR CABLE

A twisted pair comprises of two conductors (typically copper), each with its own plastic protection, wound together, as appeared in Figure-2.

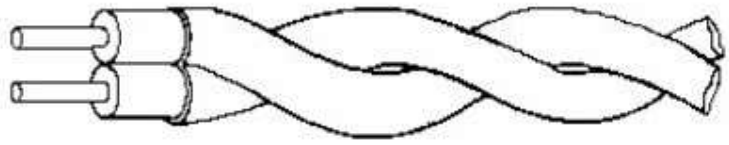


Figure-2 Twisted pair cable

One of the wires is utilized to convey signals to the receiver, and the other is utilized just as a ground reference. The receiver uses the contrast(difference) between the two.thesignal sent by the sender on one of the wires, obstruction (noise) and crosstalk may influence the two wires and make undesirable signals.

If the two wires are parallel, the impact of these undesirable signals isn't the equivalent in the two wires since they are at various areas in respect to the noise or crosstalk sources (e.g., one is nearer and the other is more remote). This outcomes in a distinction at the receiver. By twisting pair, equalization is kept up.The information rate that can be bolstered over a twisted pair is inversely relative to the square of the line length. Most extreme transmission distance of 1 Km can be accomplished for information rates up to 1 Mb/s. For analog voice signals, amplifiers are required about each 6 Km and for digitalsignals, repeaters are required for around 2 Km.

2.4.1 Unshielded Versus Shielded Twisted-Pair Cable

The most widely recognized twisted pair cable utilized in correspondences is referred to as Unshielded Twisted Pair (UTP). IBM has additionally created a form of twisted pair cable for its utilization called Shielded Twisted Pair (STP). STP cable has a metal shield or plaited – work covering that encases each pair of protected conductors. Albeit metal packaging improves the nature of link by keeping the infiltration of commotion or crosstalk, it is bulkier and progressively costly. Figure-3 demonstrates the distinction among UTP and STP.

EIA-568-A perceives three classes of UTP cabling:

- **Category 3:** UTP cables and related associating equipment whose transmission attributes are indicated up to 16 MHz.
- **Category 4:** UTP cables and related associating equipment whose transmission attributes are indicated up to 20MHz.
- **Category 5:** UTP cables and related associating equipment whose transmission attributes are indicated up to 100MHz.

Of these, it is Category 3 and Category 5 link that have gotten the most consideration for LAN applications. A key contrast between Category 3 and Category 5 cable is the quantity of twist in the cable per unit distance. Class 5 is considerably more firmly twisted, with a run of the mill twist length of 0.6 to 0.85 cm, contrasted with 7.5 to 10 cm for Category 3.

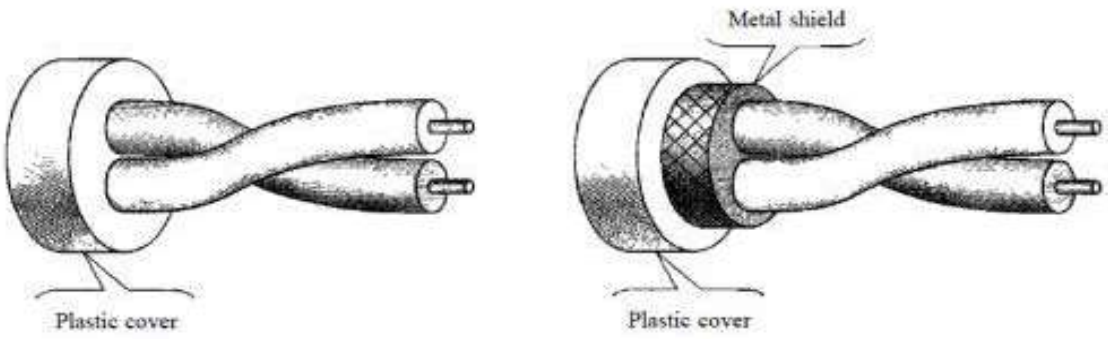


Figure-3 UTP and STP cables respectively

2.4.2 Applications

Twisted-pair cables are used in telephone lines to provide voice and data channels. The local loop-the line that connects subscribers to the central telephone office---commonly consists of unshielded twisted-pair cables. The DSL lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables.Local-area networks, such as 10Base-T and 100Base-T, also use twisted-pair cables.

2.4.3Advantages & Disadvantages

Advantages:

- Simple
- Easy to install and maintain
- Inexpensive
- can be easily connected
- In turn are less likely to cause interference themselves.
- Physically flexible

Disadvantages:

- It is not feasible for broadband applications only because of its low data rates capabilities.
- It supports data rates upto 1Mbps without conditioning and 10Mbps with conditioning.
- STP is more difficult to connect to a terminating block.

2.5 FIBER OPTICS CABLE

A fiber-optic link is made of glass or plastic and transmits signals as light. Optical fiber use reflection to control light through a channel. A glass or plastic center is encompassed by a cladding of less thick glass or plastic. The distinction in thickness of the two materials must be with the end goal that a light emission traveling through the center is reflected off the cladding as opposed to being refracted into it.For example, a beat of light methods "1", absence of pulses implies "0". It has a barrel shaped and comprises of three concentric areas: the core, the cladding and the jacket as shown in figure-4.

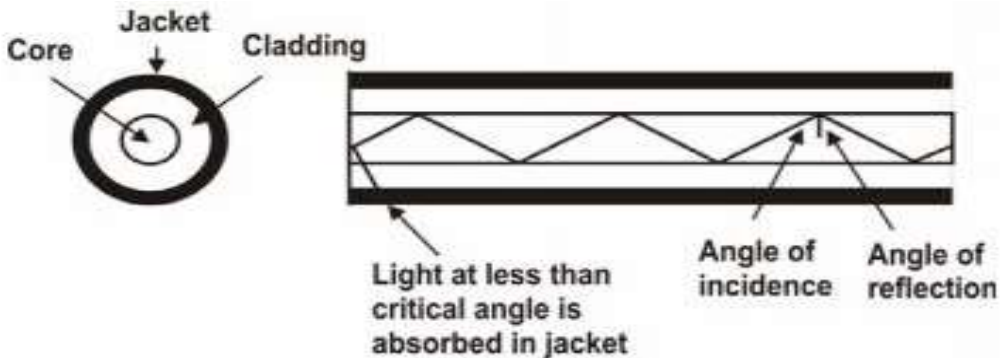


Figure-4 Optical Fiber

The core is the deepest area and comprises of at least one extremely slight strands, or filaments, made of glass or plastic; the core has a diameter in the scope of 8 to 50µm. Each fiber is encompassed by its very own **cladding**, a glass or plastic covering that has optical properties not quite the same as those of the core and a measurement of 125µm. The interface between the core and cladding goes about as a reflector to limit light that would somehow or another break the core. The furthest layer, encompassing one or a heap of cladded filaments, is the **Jacket**. The jacket is

composed of plastic and other material layered to protect against moisture, abrasion, crushing, and other environmental dangers.

2.5.1 Types of communication using fiber optics

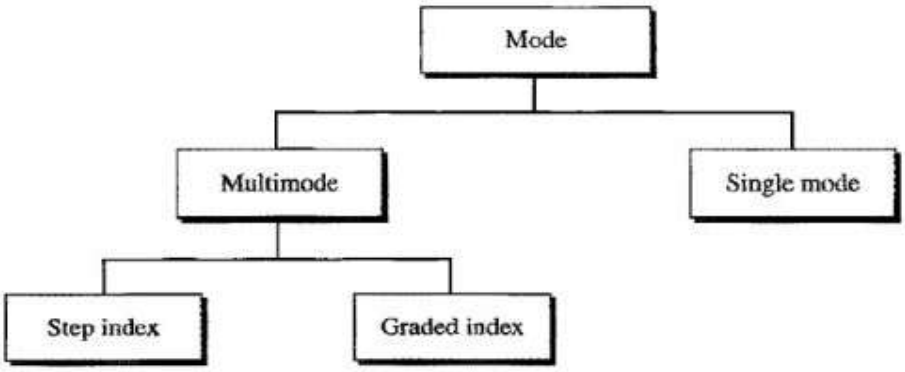


Figure-5 Propagation mode

Optical Fiber works in three unique kinds of modes. Optical fibers are accessible in two types; Multi-Mode Fiber (MMF) and Single-Mode Fiber (SMF). For multi-mode fiber the core and cladding diameter across lies in the range 50-200μm and 125-400μm, individually.While in single-mode fiber, the core and cladding diameter across lie in the range 8-12μm and 125μm, individually. Single-mode fibers are otherwise called Mono-Mode Fiber. Additionally, both single-mode and multi modefibers can have two types; step index and graded index. In the previous case the refractive index of the core is uniform all through and at the core cladding limit there is an unexpected change in refractive index. In the later case, the refractiveindex of the core shifts radially from the middle to the corecladding limit straight way. Figure -5 shows different types of communication for fiber optics cable.

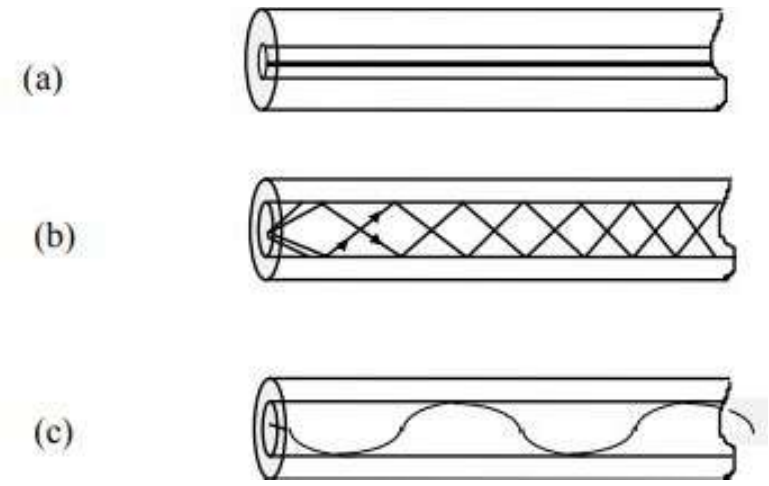


Figure – 6 Schematics of three optical fiber types, (a) Single-mode step-index, (b) Multi-mode step-index, and (c) Multi-mode graded-index

In a multi-mode fiber, the nature of signal encoded light crumbles more quickly than single-mode fiber, because of deteriorate of many light beams. As an outcome, singlemode fiber permits longer distances without repeater. For multi-mode fiber, the normal most extreme length of the cable without a repeater is 2km, while for single-mode fiber it is 20km.

2.5.2 Transmission Characteristics

Optical fiber goes about as a dielectric waveguide that works at optical frequencies (1014 to 1015 Hz). Three frequencies groups based on 850,1300 and 1500 nanometers are utilized for best outcomes. At the point when light is connected toward one side of the optical fiber core, it achieves the opposite end by methods for complete interior reflection in view of the decision of refractive index of core and cladding material.The light source can be either light emitting diode (LED) or injection laser diode (ILD). These semiconductor devices emanate a light emission when a voltage is connected over the devices. At receiver end, a photodiode can be utilized to recognize the signal encoded light. Either PIN indicator or APD (Avalanche photodiode) detector can be utilized as the light detector.

2.5.3Applications

Due to more prominent data transmission (2Gbps), smalldiameter, lighter weight, low attenuation, invulnerability to electromagnetic impedance and longer repeater spacing, optical fiber cables are finding broad use in long-distance broadcast communications.

Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective. Today, with wavelength-division multiplexing (WDM), we can transfer data at a rate of 1600 Gbps.

Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid network. Optical fiber 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 use fiber-optic cable.

2.5.4 Advantages & 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

2.6 Comparisons

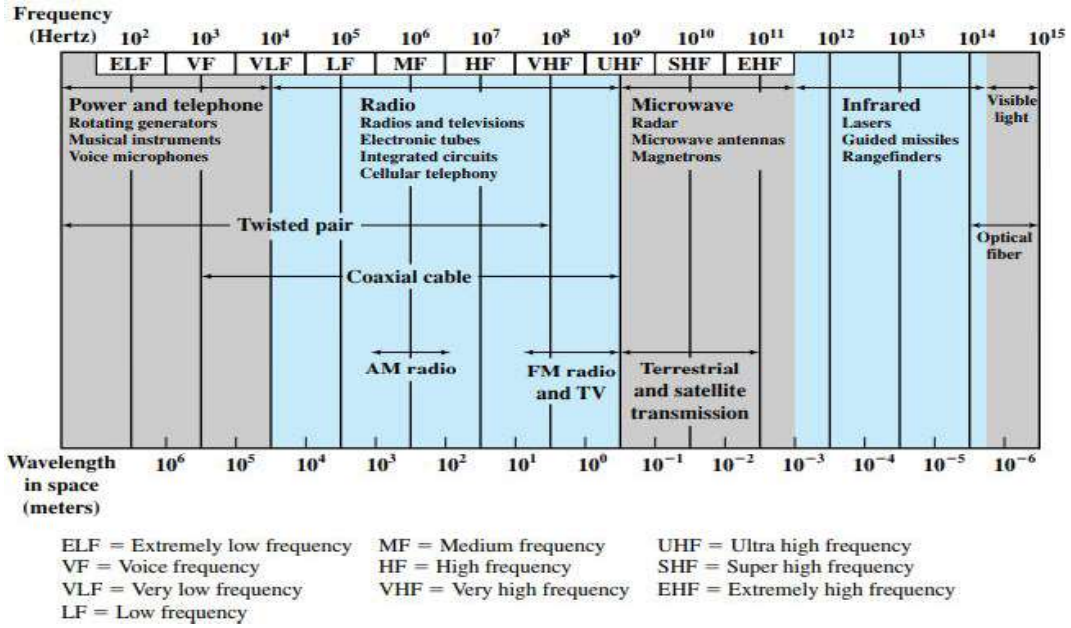


Figure 7 represent the electromagnetic spectrum and indicates the frequencies at which various guided media operates on.

Type	Sub Type	Segment Length	Bandwidth	Installation	Cost	Interference
Twisted Pair Cable	UTP	100 meters	100Mbps	Easy	Cheapest	High
	STP	100 meters	500Mbps	Moderate	Moderate	Moderate
Coaxial Cable	Thicknet	500 meters	10Mbps	Hard	Moderate	Low
	Thinnet	185 meters	10Mbps	Easy	Cheap	Moderate
Fiber Optics Cable	Multinode	2Kms	100Mbps	Very Hard	Expensive	None
	Singlenode	100Kms	2Gbps	Very Hard	Expensive	None

Table:-2 Comparison of various guided media

All the comparison shows on table-2 suggest about various characteristics about types of guided media.

2.7 LET US SUM UP

In category of guided media the communication device is used to communicate to each other directly with cables. The data signals are restricted to a cabling platform and thus they are also known as bounded media. Generally the guided media is called LAN. Some kinds of guided media are coaxial cable, twisted pair wire and fiber optic cable.

1. **Twisted Pair Cable –** It is the most widely recognized utilized correspondence media and utilized in LAN for exchange of information between different PCs.
2. **Coaxial Cable** – They are otherwise called coax and conveys signals with high frequencies. They are produced using a solitary copper wire.
3. **Fiber Optic Cable** – They utilize light to exchange information. The information is exchanged at an exceptionally rapid of billions bits/second.

2.8 FURTHER READING

Detailed descriptions of the transmission characteristics of the transmission media discussed in this chapter can be found in [FREE98]. [REEV95] provides an excellent treatment of twisted pair and optical fiber. [BORE97] is a thorough treatment of optical fiber transmission components. Another good paper on the subject is [WILL97]. [FREE02] is a detailed technical reference on optical fiber. [STAL00] discusses the characteristics of transmission media for LANs in greater detail.

For a more thorough treatment on wireless transmission and propagation, see [STAL05] and [RAPP02]. [FREE97] is an excellent detailed technical reference on wireless topics.

- BORE97 Borella, M., et al. “Optical Components for WDM Lightwave Networks.” Proceedings of the IEEE, August 1997.
- FREE97 Freeman, R. Radio System Design for Telecommunications. New York:Wiley, 1997.
- FREE98 Freeman, R.Telecommunication Transmission Handbook. New York:Wiley, 1998.

- FREE02 Freeman, R.Fiber-Optic Systems for Telecommunications. New York:Wiley, 2002. RAPP02 Rappaport, T. Wireless Communications. Upper Saddle River, NJ: Prentice Hall, 2002.
- REEV95 Reeve, W. Subscriber Loop Signaling and Transmission Handbook. Piscataway, NJ: IEEE Press, 1995.
- STAL00 Stallings,W. Local and Metropolitan Area Networks, Sixth Edition. Upper Saddle River, NJ: Prentice Hall, 2000.
- STAL05 Stallings, W. Wireless Communications and Networks, Second Edition. Upper Saddle River, NJ: Prentice Hall, 2005.
- WILL97 Willner, A. “Mining the Optical Bandwidth for a Terabit per Second.” IEEE Spectrum, April 1997.

2.9 ASSIGNMENTS

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 fiber cable.

2.10 ACTIVITIES

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

Unit 3: Wireless Media 3

Unit Structure

3.1 LEARNING OBJECTIVE

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

Wireless is a method of communication that uses electromagnetic wavesrather than wire conductors to transmit data between devices.Wirelessnetworks are phone or PC organizes that utilization radio frequenciesand infrared waves as their carrier.The mediums utilized in wireless interchanges are air, vacuum andeven water. Air is the most usually utilized medium.Signals are ordinarily communicated through air and are accessible toanyone who has a device ready for accepting them.

Wireless transmission can be sorted into three general gatherings:

- **Radio waves**
- **Microwaves**
- **Infrared**

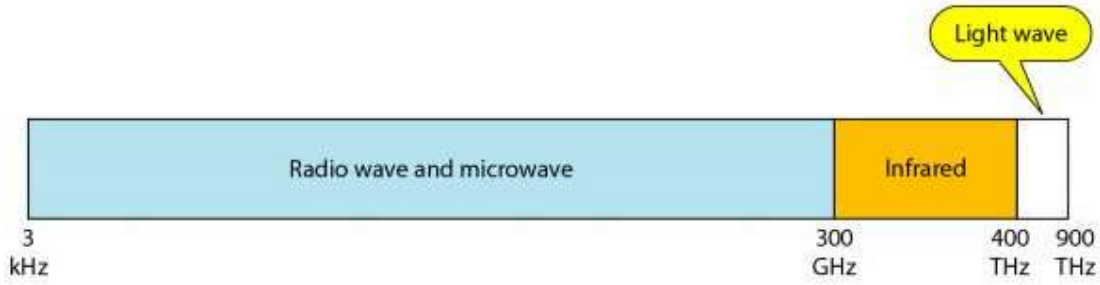


Figure 1: Electromagnetic spectrum for wireless communication

Figure 1 shows the part of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, used for wireless communication.

3.3 REASON FOR WIRELESS NETWORKS

Wireless networks offer the following **six** advantages when compared to traditional wired networks:

1. **Increased Mobility:** Wireless networks enable portable clients to get to ongoing data so they can wander around organization's space without getting disengaged from the system. This builds cooperation and efficiency vast that is beyond the realm of imagination with customary systems.

2. **Installation Speed and Simplicity:**Introducing a wireless networks framework lessens cables, which are awkward to setup and can force a danger, should workers stumble on them. It can likewise be introduced rapidly and effectively, when contrasted with a traditional system.

3. **Wider Reach of the Network:** The wireless system can be reached out to places in your association that are not open for wires and cables.

4. **More Flexibility:** Should your system change later on, you can without much of a stretch update the wireless system to meet new setups.

5. **Reduced Cost of Ownership over Time:** Wireless systems administration may convey a marginally higher beginning speculation, yet the general costs after some time are lower. It likewise may have a more extended lifecycle than a traditional system.

6. **Increased Scalability:** Wireless frameworks can be explicitly configured to address the issues of explicit applications. These can be effectively changed and scaled relying upon your association's needs.

3.4WIRELESS COMMUNICATION WITH LANS

Many people use WLANs(Wireless LANs) on a regular basis today. PC sales continue to trend toward more laptop sales versus desktop computers, in part to

support a more mobile workforce. PC users need to connect to whatever network they are near, whether at work, at home, in a hotel, or at a coffee shop or bookstore. The migration toward a work model in which you find working moments wherever you are, with a need to be connected to the Internet at any time, continues to push the growth of wireless LANs.

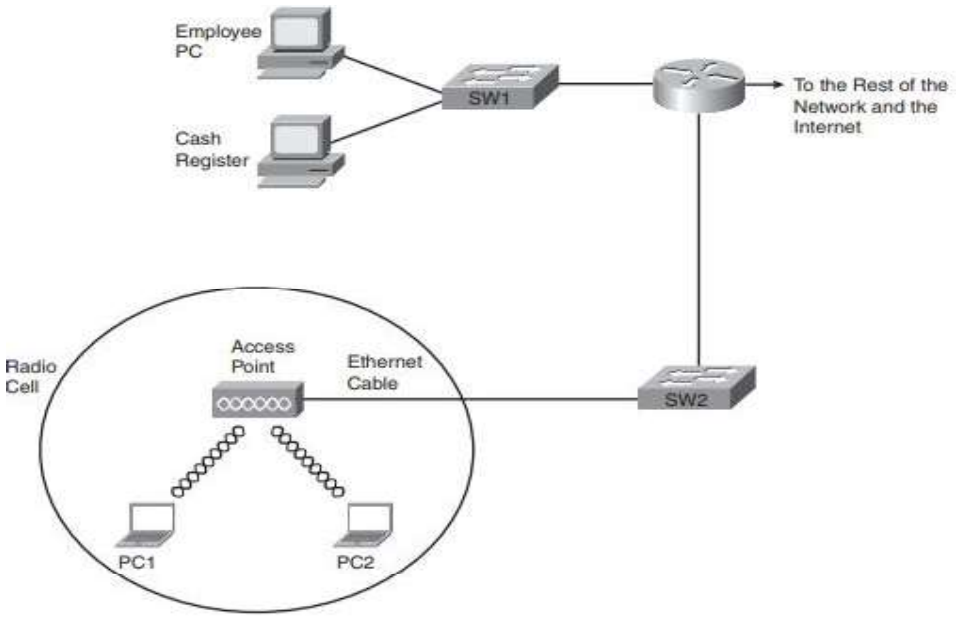


Figure 2:Sample WLAN at a Bookstore

For example, Figure 11-1 shows the design of a LAN at a retail bookstore. The bookstore provides free Internet access via WLANs while also supporting the bookstore's devices via a wired LAN. The wireless-capable customer laptops communicate with a WLAN device called an access point (AP). The AP uses wireless communications to send and receive frames with the WLAN clients (the laptops). The AP also connects to the same Ethernet LAN as the bookstore's own devices, allowing both customers and employees to communicate with other sites.

3.4.1 WLAN standards

WLAN devices work with the IEEE 802.11 standard. This is a gathering of gauges that expand on the prior IEEE models for LANs. The best known about these is IEEE 802.3 for Ethernet. Among the different IEEE 802.11 models, some determine wireless transmissions in different recurrence groups and at various rates:

- **IEEE 802.11n** with up to 300 Mbps data rate in the 5 GHz or 2.4 GHz frequency bands, featuring new mechanisms such as MIMO, 40-MHz channels, packet aggregation, and block acknowledgement.
- **IEEE 802.11a**with up to 54 Mbps data rate in the 5 GHz frequency band, up to 108 Mbps with Turbo Mode (extension to the standard).
- **IEEE 802.11g**with up to 54 Mbps data rate in the 2.4 GHz frequency band, up to 108 Mbps with Turbo Mode (extension to the standard).
- **IEEE 802.11b** (also referred to as 802.11 High Rate or Wi-Fi) — an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1-Mbps) in the 2.4 GHz band.

3.5 COMPARISONOFDIFFERENTWIRELESSMEDIA

3.5.1 Radio Wave

Radio frequency systems must use spread spectrum technology in the United States. This spread spectrum technology currently comes in two types: direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS). There is a lot of overhead involved with spread spectrum and so most of the DSSS and FHSS systems have historically had lower data rates than IR or MW.

Direct Sequence Spread Spectrum (DSSS)

Direct Sequence Spread Spectrum (DSSS) speaks to each piece in the edge by numerous bits in the transmitted casing. DSSS speaks to every datum 0 and 1 by the image – 1 and +1 and afterward increases every image by a twofold example of +1's and – 1's to acquire digital signal that fluctuates all the more quickly involving bigger band. The IEEE 802.11 utilizations a basic 11-chip Barker grouping B11 [-1, +1, - 1, - 1, +1, - 1, - 1, - 1, +1, +1, +1] with QPSK or BPSK balance. The DSSS transmission framework takes 1 Mbps information, changes over it into 11 Mbps signal utilizing differential parallel stage move keying (DBPSK) regulation.

Frequency Hopping Spread Spectrum (FHSS)

The idea behind spread spectrum is to spread the signal over a wider frequency band, so as to make jamming and interception more difficult and to minimize the

effect of interference from other devices In FH it is done by transmitting the signal over a random sequence of frequencies; that is, first transmitting at one frequency, then second, then a third and so on. The irregular grouping of frequencies is produced with the assistance of a pseudorandom number generator. As both the collector and sender utilize a similar calculation to create arbitrary grouping, both the devices bounce frequencies in a synchronous way and edges transmitted by the sender are gotten accurately by the beneficiary. This is to some degree like sending distinctive pieces of one melody more than a few FM channels. Spies hear just confused blips and any endeavor to stick the signal brings about harming a couple of bits as it were.

3.5.2 Microwave

Microwave (MW) systems operate at less than 500 milliwatts of power in compliance with FCC regulations. MW systems are by far the fewest on the market. They use narrow-band transmission with single frequency modulation and are set up mostly in the 5.8GHz band. The big advantage to MW systems is higher throughput achieved because they do not have the overhead involved with spread spectrum systems. Radio LAN is an example of systems with microwave technology.

3.5.2 Infrared

Infrared systems (IR systems) are simple in design and therefore inexpensive. They use the same signal frequencies used on fiber optic links. IR systems detect only the amplitude of the signal and so interference is greatly reduced. These systems are not bandwidth limited and thus can achieve transmission speeds greater than the other systems. Infrared transmission operates in the light spectrum and does not require a license from the FCC to operate. There are two conventional ways to set up an IR LAN. Logical Link Layer (LLC) 802.2 Data Link Layer Medium Access Control 802.11b (MAC) The infrared transmissions can be aimed. This gives a good range of a couple of kilometer and can be used outdoors. It also offers the highest bandwidth and throughput.

The other way is to transmit Omni-directionally and bounce the signals off of everything in every direction. This reduces coverage to 30 - 60 feet, but it is area

coverage. IR technology was initially very popular because it delivered high data rates and relatively cheap price.

The downsides to IR frameworks are that the transmission range is imparted to the sun and different things, for example, bright lights. In the event that there is sufficient impedance from different sources it can render the LAN pointless. IR frameworks require an unhindered Line of Sight (LOS). IR signals can't infiltrate misty items. This implies dividers, dividers, draperies, or even fog can deter the signal. InfraLAN is a case of remote LANs utilizing infrared technology

3.6 Time Division Multiplexing(TDM)

In Time-division multiplexing all signals operate with same frequency at different times. This is a base band transmission system, where an electronic commutator sequentially samples all data source and combines them to form a composite base band signal, which travels through the media and is being demultiplexed into appropriate independent message signals by the corresponding commutator at the receiving end. The incoming data from each source are briefly buffered. Each buffer is typically one bit or one character in length. The buffers are scanned sequentially to form a composite data stream. The scan operation is sufficiently rapid so that each buffer is emptied before more data can arrive. Composite data rate must be at least equal to the sum of the individual data rates. The composite signal can be transmitted directly or through a modem. The multiplexing operation is shown in Figure 3.

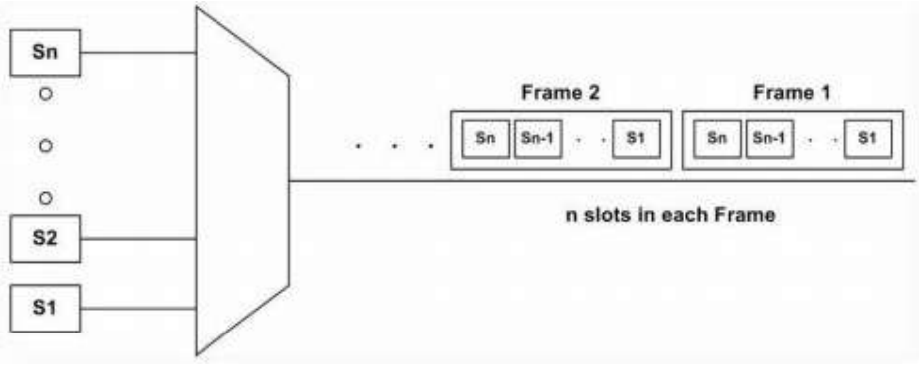


Figure 3:Time division multiplexing operation

As shown in the Figure the composite signal has some dead space between the successive sampled pulses, which is essential to prevent interchannel cross talks.

Along with the sampled pulses, one synchronizing pulse is sent in each cycle. These data pulses along with the control information form a frame. Each of these frames contain a cycle of time slots and in each frame, one or more slots are dedicated to each data source. The maximum bandwidth (data rate) of a TDM system should be at least equal to the same data rate of the sources.

Synchronous TDM is called synchronous essentially on the grounds that each schedule opening is preassigned to a fixed source. The schedule openings are transmitted independent of whether the sources have any information to send or not. Thus, for straightforwardness of execution, channel limit is squandered. Albeit fixed task is utilized TDM, devices can deal with wellsprings of various information rates. This is finished by relegating less spaces per cycle to the slower input devices than the quicker devices.

3.7 TIME DIVISION MULTIPLE ACCESS(TDMA)

Every user is assigned one or a set of well-defined time-slots within a 'Time Frame'. A transmitting user sends its own data only in the designated time-slot(s), and waits for the remaining time-frame duration till it gets another time-slot in the next time frame. Precise time synchronization among all users is an important and necessary feature of TDMA multiple access strategy. Usually, a central unit controls the synchronization and the assignment of time-slots.(**Refer Figure 4**)

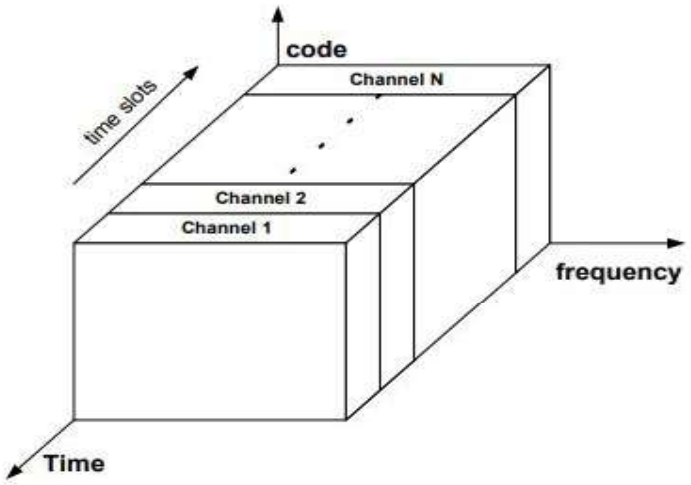


Figure 4: Time Divisional Multiple Access

3.8 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.

Wireless LANs come in many types: infrared, microwave, and radio. Radio is further broken down into direct sequence and frequency hopping spread spectrum. The MAC layer protocol used by wireless LANs as standardized in 802.11 is CSMA/CA.

TDMA requires a centralized control node, whose primary function is to transmit a periodic reference burst that defines a frame and forces a measure of synchronization of all the users.

3.9 FURTHER READING

- 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.
- D. D. Falconer, F. Adachi, B. Gudmundson, **Time Division Multiple Access Methods for Wireless Personal Communications**, IEEE Communications Magazine, (January 1995), pp. 50-57.

3.10 ASSIGNMENT

1. Why are the types of wireless media?
2. What are some major limitations of TDMA?
3. What is the difference between Infrared, Radio wave & Microwave?
4. Describe the operations of TDM.

3.11 ACTIVITIES

- Prepare a chart on the basis of characteristics of TDMA ,FDMA& CDMA.

Unit 4: TCP/IP 4

Unit Structure

4.1 LEARNING OBJECTIVE

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 TCP/IP AND INTERNETWORKING

The TCP/IP protocol suite is so named for two of its most important protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP).The principle structure objective of TCP/IP was to assemble an interconnection of networks, referred to as an internetwork, or web, that gave general correspondence benefits over heterogeneous physical systems.

The main advantage of such an internetwork is the empowering of correspondence between hosts on various systems, maybe isolated by a substantial topographical zone. The words internetwork and internet are just a compression of the expression interconnected system. In any case, when composed with a capital "I", the Internet alludes to the overall arrangement of interconnected systems. Accordingly, the Internet is a web, yet the turn around does not have any significant bearing. The Internet is once in a while called the associated Internet.Figure 1 shows two examples of internets. Each consists of two or more physical networks.

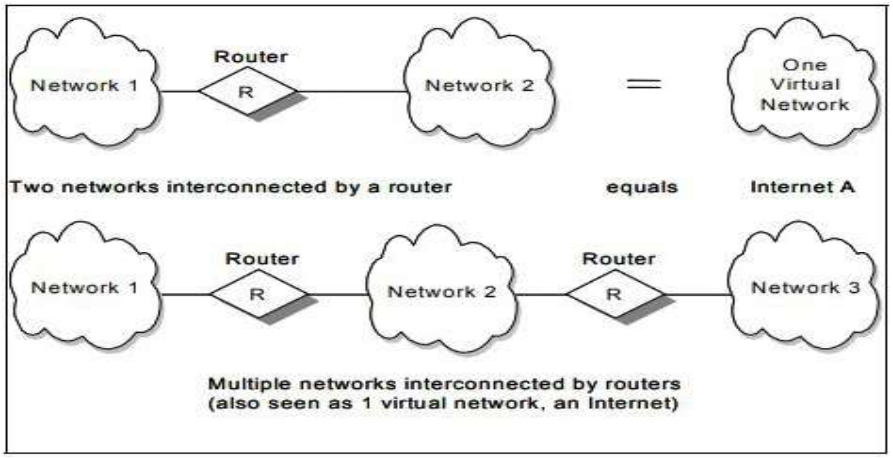


Figure 1:Internet

Another significant part of TCP/IP internetworking is the production of an institutionalized reflection of the correspondence systems given by each sort of system. Each physical system has its own innovation subordinate correspondence interface, as a programming interface that gives fundamental correspondence capacities (natives). TCP/IP gives correspondence benefits that keep running between the programming interface of a physical system and client applications.

To have the capacity to recognize a host inside the internetwork, each host is allocated a location, called the IP address. At the point when a host has different system connectors (interfaces, for example, with a switch, every interface has a remarkable IP address. The IP address comprises of two sections:

IP address = <network number><host number>

The system number piece of the IP address recognizes the system inside the web and is allotted by a focal expert and is novel all through the web. The specialist for allocating the host number piece of the IP address dwells with the association that controls the system distinguished by the system number.

4.3TCP/IP PROTOCOLS

Like most systems administration programming, TCP/IP is displayed in layers. This layered portrayal prompts the term protocol stack, which alludes to the heap of layers in the protocol suite. It very well may be utilized for situating (yet not for practically contrasting) the TCP/IP protocol suite against others, for example, Systems Network Architecture (SNA) and the Open System Interconnection (OSI) model. By isolating the correspondence programming into layers, the protocol stack considers division of work, simplicity of usage and code testing, and the capacity to create elective layer executions.Figure 2 shows how the TCP/IP protocols are modeled in four layers.

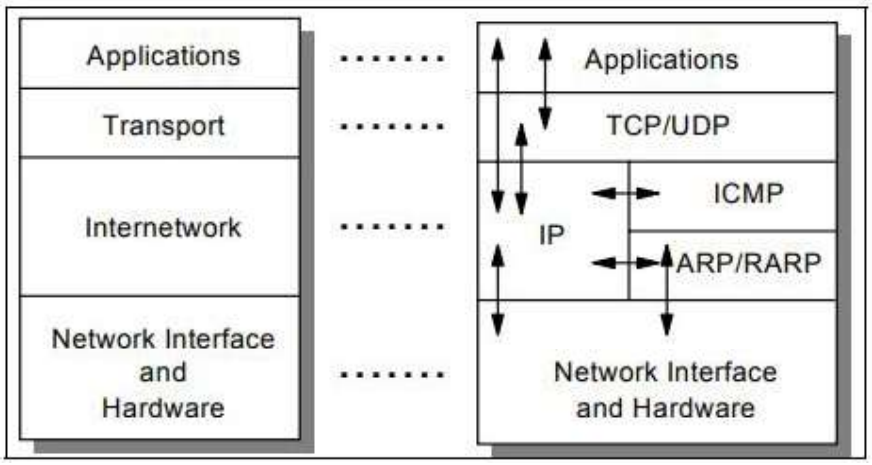


Figure 2: TCP/IP Protocol Stack

1. **Application layer** :The application layer is provided by the program that uses TCP/IP for communication. An application is a client process collaborating with another process more often than not on an alternate host (there is additionally an advantage to application correspondence inside a solitary host).The interface between the application and transport layers is characterized by port numbers and sockets.

2. **Transport layer**:The transport layer provides the start to finish information exchange by conveying information from an application to its remote peer. Different applications can be bolstered all the while. The most-utilized transport layer protocol is the Transmission Control Protocol (TCP), which gives connection-oriented reliable data delivery, duplicate data suppression, congestion control, and flow control.Another transport layer protocol is the User Datagram Protocol(UDP) . It provides connectionless, unreliable,best-effort service. As a result, applications using UDP as the transport protocol have to provide their own end-to-end integrity, flow control, and congestion control, if desired. Usually, UDP is used by applications that need a fast transport mechanism and can tolerate the loss of some data.

3. **Internetwork layer** :The internetwork layer, likewise called the internet layer or the network layer, gives the "virtual system" picture of a web (this layer shields the more elevated amounts from the physical system design beneath it). InternetProtocol (IP) is the most significant protocol in this layer. It is a

connectionless protocol that does not expect dependability from lower layers. IP does not give reliability, flow control, or error recovery. These functions must be provided at a higher level.

4. **Network interface layer :**The network interface layer, also called the link layer or the data link layer, is the interface to the actual network hardware. Interface may or may not provide reliable delivery, and may be packet or stream oriented. In fact, TCP/IP does not specify any protocol here, but can use almost any network interface available, which illustrates the flexibility of the IP layer. Examples are IEEE 802.2, X.25 (which is reliable in itself), ATM, FDDI, and even SNA.

4.4PORTS AND SOCKETS

This area presents the ideas of the port and socket, which are expected to figure out which nearby process at a given host really speaks with which process, at which remote host, utilizing which protocol. Following points needs to be remembered:

- An application process is assigned a process identifier number (process ID), which is likely to be different each time that process is started.
- Process IDs differ between operating system platforms, thus they are not uniform.

The idea of ports and attachments gives an approach to consistently and exceptionally recognize associations and the projects and hosts that are occupied with them, independent of explicit process IDs.

4.4.1 Ports

Each process that needs to speak with another process distinguishes itself to the TCP/IP protocol suite by at least one ports. A port is a 16-bit number utilized by the host-to-have protocol to recognize to which more elevated amount protocol or application program (process) it must convey approaching messages.

There are two sorts of ports:

- **Well-known**: Well-known ports have a place with standard servers, for instance, Telnet utilizes port 23. Surely understood port numbers run somewhere in the range of 1 and 1023 (preceding 1992, the range somewhere in the range of 256 and 1023 was utilized for UNIX-explicit servers). Surely Well-known numbers are regularly odd, on the grounds that early frameworks utilizing the port idea required an odd/even pair of ports for duplex activities. Most servers require just a solitary port. Special cases are the BOOTP server, which utilizes two: 67 and 68 .
- **Ephemeral: Some** clients needn't bother with well-known port numbers since they start communication with servers, and the port number they are utilizing is contained in the UDP/TCP datagrams sent to the server. Every client procedure is allotted a port number, for whatever length of time that it needs, by the host on which it is running. Ephemeral port numbers have values greater than 1023, normally in the range of 1024 to 65535.

Because of two unique applications attempting to utilize a similar port numbers on one host, is kept away from by composing those applications to demand an accessible port from TCP/IP. Since this port number is progressively appointed, it can vary starting with one conjuring of an application then onto the next.

4.4.2 Sockets

Socket interface is one of a few application programming interfaces to the communication protocols.
Consider the following terminologies:

- A socket is a special type of file handle, which is utilized by a process to demand arrange administrations from the operating system.
- A socket address is the triple: For example, in the TCP/IP (version 4) suite:<tcp, 192.168.54.34, 8080>
- A conversation is the communication interface between two procedures.
- An association is the 5-tuple that completely specifies the two processes that comprise a connection:<protocol, local-address, local-port, foreign-address,

foreign-port>In the TCP/IP (version 4) suite, the following could be a valid association:<tcp, 192.168.14.234, 1500, 192.168.44, 22>.

Two processes communicate through TCP sockets. The socket model provides a process with a full-duplex byte stream connection to another process. The application need not concern itself with the management of this stream; these facilities are provided by TCP.

4.5THE IP ADDRESS STRUCTURE

IP addresses are represented by a 32-bit unsigned binary value. It is usually expressed in a dotted decimal format. For example, 91.67.15.28 is a valid IP address. The numeric 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 address, the IP address, or in some cases, the Internet address. When the host is attached to more than one network, it is called multihomed and has one 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 (as the decimal portrayal of four 8-bit esteems linked with specks). For instance, 128.2.7.9 is an IP address with 128.2 being the system 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 paired configuration of the IP address 128.2.7.9 is:

10000000 00000010 00000111 00001001

IP addresses are utilized by the IP protocol to particularly distinguish a host on the Internet (or all the more for the most part, any web). Carefully, an IP address recognizes an interface that is fit for sending and getting IP datagrams. One framework can have numerous such interfaces. In any case, the two hosts and switches must have no less than one IP address, so this disentangled definition is adequate. IP datagrams (the essential information bundles traded between hosts)

are transmitted by a physical system joined to the host. Every IP datagram contains a source IP address and a destination IP address.

4.5.1 Class-based IP addresses

The first bits of the IP address specify how the rest of the address should be separated into its network and host part. The terms network address and netID are sometimes used instead of network number, but the formal term, used in RFC 1166, is network number. Similarly, the terms host address and hostID are sometimes used instead of host number.

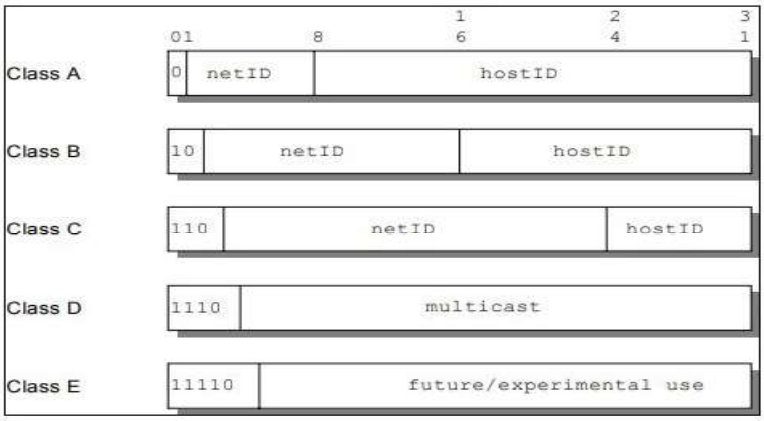


Figure 3: CLASSES OF IP ADDRESS

Where:

Class A addresses: These addresses use 7 bits for the and 24 bits for the portion of the IP address. This allows for 2^7-2 (126) networks each with 2^{24}-2 (16777214) hosts—a total of more than 2 billion addresses.

Class B addresses: These addresses use 14 bits for the and 16 bits for the portion of the IP address. This allows for 2^{14}-2 (16382) networks each with 2^{16}-2 (65534) hosts—a total of more than 1 billion addresses.

Class C addresses: These addresses use 21 bits for the and 8 bits for the portion of the IP address. That allows for 2^{21}-2 (2097150) networks each with 2^8-2 (254) hosts—a total of more than half a billion addresses.

Class D addresses: These addresses are reserved for multicasting (a sort of broadcasting, but in a limited area, and only to hosts using the same Class D address).

Class E addresses: These addresses are reserved for future or experimental use.

Class A location is appropriate for systems with an amazingly huge number of hosts. Class C addresses are appropriate for systems with few hosts. This implies medium-sized systems (those with in excess of 254 hosts or where there is a desire for in excess of 254 hosts) must utilize Class B addresses. In any case, the quantity of little to medium-sized systems has been becoming all around quickly. It was expected that if this development had been permitted to proceed with unabated, the majority of the accessible Class B arrange addresses would have been utilized by the mid-1990s.

Special use IP addresses: RFC 3330 discusses special use IP addresses. We provide a brief description of these IP addresses in Figure 4.

Address block	Present use
0.0.0.0/8	"This" network
14.0.0.0/8	Public-data networks
24.0.0.0/8	Cable television networks
39.0.0.0/8	Reserved but subject to allocation
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
192.0.0.0/24	Reserved but subject to allocation
192.0.2.0/24	Test-Net 192.88.99.0/24 6to4 relay anycast
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
240.0.0.0/4	Reserved for future use

Figure 4 : Special Use IP addresses

4.6 IP DATAGRAM

The unit of transfer in an IP network is called an IP datagram. It consists of an IP header and data relevant to higher-level protocols.

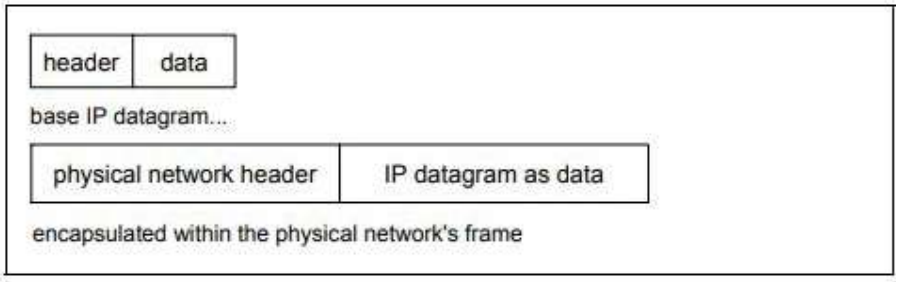


Figure 5: IP Datagram Format

IP can give fragmentation and reassembly of datagrams. The most extreme length of an IP datagram is 65,535 octets. All IP has must help 576 octets datagrams without fracture.

Pieces of a datagram each have a header. The header is replicated from the first datagram. A part is treated as an ordinary IP datagrams while being transported to their goal. Be that as it may, in the event that one of the parts gets lost, the total datagram is viewed as lost. Since IP does not give any affirmation components, the rest of the sections are disposed of by the goal have.

IP datagram header format

The IP datagram header has a minimum length of 20 octets, as illustrated in Figure 6.

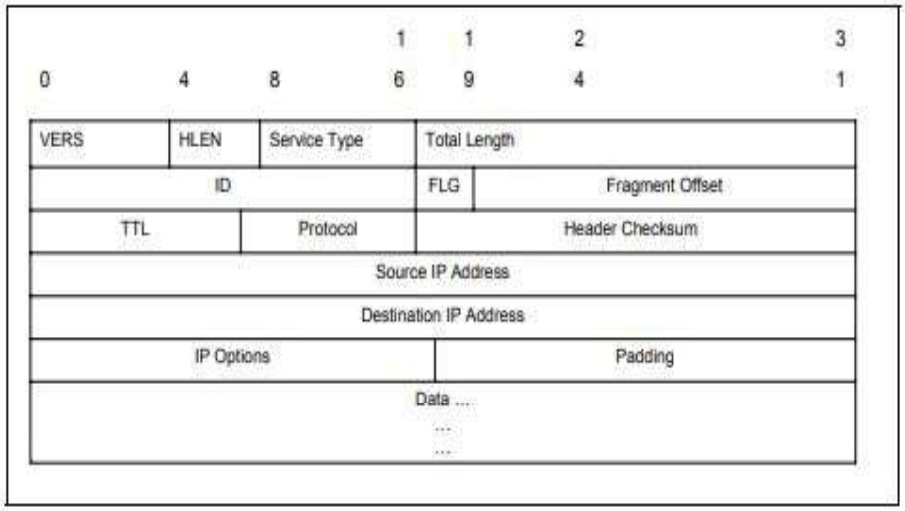


Figure 6: IP Datagram Header Format

Where:

VERS: The field contains the IP protocol version. The current version is 4. Version 5 is an experimental version. Version 6 is the version for IPv6 (see 9.2, “The IPv6 header format” on page 330).

HLEN: The length of the IP header counted in 32-bit quantities. This does not include the data field.

Service Type: The service type is an indication of the quality of service requested for this IP datagram.

Where:

– Precedence: This field specifies the nature and priority of the datagram:

• 000: Routine

• 001: Priority

• 010: Immediate

• 011: Flash

• 100: Flash override

• 101: Critical

• 110: Internetwork control

• 111: Network control

– TOS: Specifies the type of service value:

• 1000: Minimize delay

• 0100: Maximize throughput

• 0010: Maximize reliability

• 0001: Minimize monetary cost

• 0000: Normal service

Total Length: The total length of the datagram, header and data.

Identification: A unique number assigned by the sender to aid in reassembling a fragmented datagram. Each fragment of a datagram has the same identification number.

Flags:

Where:

– 0: Reserved, must be zero.

– DF (Do not Fragment): 0 means allow fragmentation; 1 means do not allow fragmentation.

– MF (More Fragments): 0 means that this is the last fragment of the datagram; 1 means that additional fragments will follow.

Fragment Offset: This is used to aid the reassembly of the full datagram. The value in this field contains the number of 64-bit segments (header bytes are not counted)

contained in earlier fragments. If this is the first (or only) fragment, this field contains a value of zero.

Time to Live: This field specifies the time (in seconds) the datagram is allowed to travel. Theoretically, each router processing this datagram is supposed to subtract its processing time from this field. In practice, a router processes the datagram in less than 1 second. Therefore, the router subtracts one from the value in this field. The TTL becomes a hop-count metric rather than a time metric.

Protocol Number: This field indicates the higher-level protocol to which IP should deliver the data in this datagram.

Header Checksum: This field is a checksum for the information contained in the header. If the header checksum does not match the contents, the datagram is discarded.

Source IP Address: The 32-bit IP address of the host sending this datagram.

Destination IP Addresss: The 32-bit IP address of the destination host for this datagram.

Options: An IP implementation is not required to be capable of generating options in a datagram. However, all IP implementations are required to be able to process datagrams containing options. The Options field is variable in length (there can be zero or more options). There are two option formats.

Padding: If an option is used, the datagram is padded with all-zero octets up to the next 32-bit boundary.

Data: The data contained in the datagram. It is passed to the higher-level protocol specified in the protocol field.

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 defense for the purpose of connecting government computer systems to each other through a global, fault tolerant, network. The defense department network was opened up to research institutions and eventually the general public to create what is now the Internet. The

TCP/IP protocol was also placed in the public domain so that any software company could develop networking software based on the protocol.

4.8 FURTHER READING

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

4.9 ASSIGNMENTS

1.Explain the different layers of TCP/IP.

2. Differenciate OSI & TCP/IP layers

3. Describe IP header format in details.

4.10 ACTIVITIES

- Prepare a chart for comaprision of UDP and TCP on the basis of their communication purpose.

Block-4

Connectivity Devices, Network Topologies and Architecture

Unit 1: Connectivity Devices

1

Unit Structure

1.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Understand basic concept of connectivity devices used in network
- Identify the network architecture
- Apply the network topology
- Analyzing the role of routing and switching in communication network

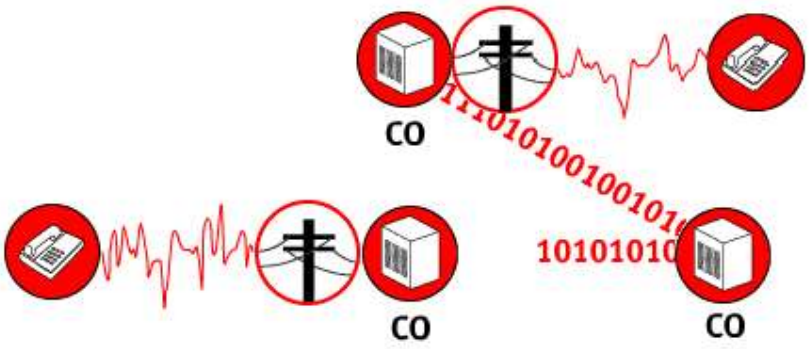
1.2 INTRODUCTION

Networking devices, also referred as network hardware, network equipment, are physical devices which are requisite for communication and interaction among devices on a computer network. Explicitly, they mediate data in computer network. Connectivity devices are units that intervene data in a communication network and are also called network component. Components which are the end receiver or produce data are referred as a hosts or data terminal component / equipment.

1.3 MODEM

Modem is short form of ***mo****dulator-****dem****odulator.* A modem is a device or a program that enables a computer to transmit and receive data over a telephonic line or cable or satellite connections. Basically modem is an electronic device used to right to use the Internet that modulates carrier waves to determine information to transmit and also demodulates incoming carrier waves to interpret the information they carry. In a simple terminology, modem is the device that unites a computer to the Internet. For appetizers, modulation is a procedure of adding significant information to a carrier wave so that it can be transmitted over far distance. When an electrical signal containing some meaningful information required being transmitted over far distance, it's added to carrier wave. This procedure of growing the original signal on a carrier wave is referred as a modulation. In old days, landline phones were the primary component to communicate over far distance; modem came in pretty useful to gain Internet connectivity using telephone lines. In fact, without modem, it would have been not possible for most users to connect to Internet. Most telephone lines were designed to carry analog signals. The Public Switched

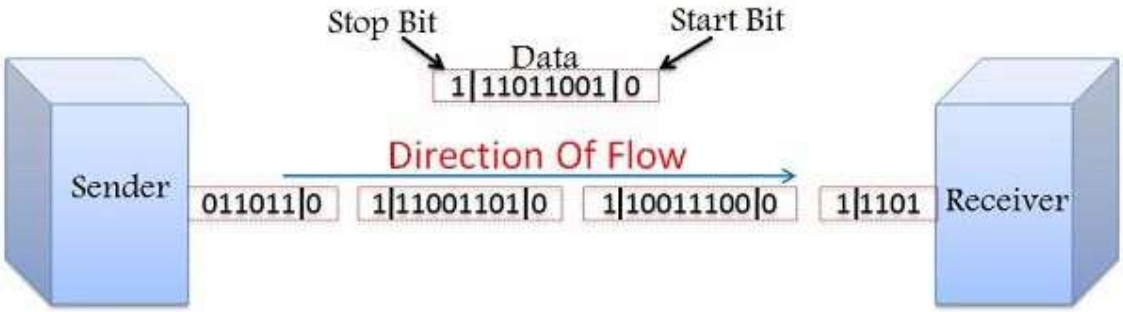
Telephone Network (PSTN) picks up these analog signals and basically converts them into digital signal to transfer them from one Central Office (CO) to another. On the other hand, these digital signals are converted back into an analog signal.



The modulator part of the modem converts digital signals to analog signals and the demodulator part converts analog signals to digital signals.

1.4 ASYNCHRONOUS TRANSMISSION

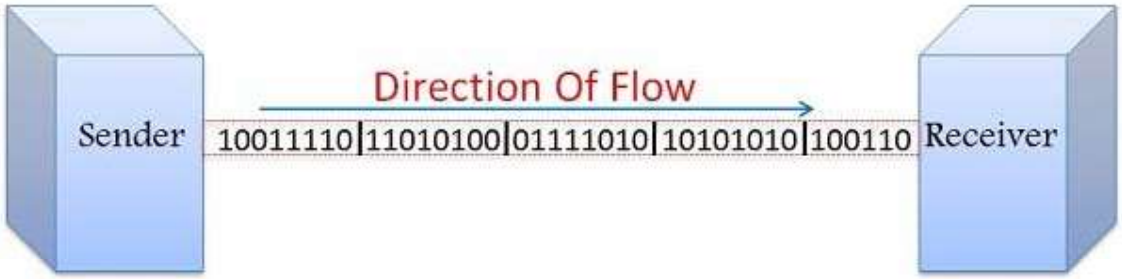
Asynchronous transmission is named suggest the timing of a signal is unimportant. Transmission is the act of transferring somewhat from one site to another. A correspondence can be given to you, received in the email, read to you or received by via email. These are all nothing but different approaches of transmitting the letter. Likewise, in communication network, data transmission is the transferring of data from one system part to another. In asynchronous transmission, the data or signals being transmitted and received are not done in synchronization. In asynchronous transmission, data flows in a half duplex mode, one byte or a character at a time. It transfer the data in continues stream of bytes. Without synchronization, the receiver cannot use timing to predict when the next set will arrive. To aware the receiver to the arrival of a new set, therefore, an extra bit is added to the beginning of each byte. This bit, usually a zero, is called the start bit. To let the receiver know about that the byte is finished, one or more additional bits are appended to the end of the byte. These bits, usually ones, are called stop bits.



It is simple, fast economical and does not require a full duplex communication. Emails, letters, televisions, radios, and forums are some of the examples of Asynchronous Transmission.

1.5 SYNCHRONOUS TRANSMISSION

The word synchronous is used to illustrate a continuous and consistent timed transfer of data blocks. Each byte, however, is introduced onto the transmission link without a gap between it and the next one. It is depend to the receiver to differentiate the bit stream into bytes for decoding purposes.



In synchronous transmission, data flows in a full-duplex manner in the structure of blocks or frames. Synchronous transmission is capable, consistent and is used for transferring a large quantity of data. Synchronous transmission provides real-time communication between connected devices. Examples of the synchronous transmission are video conferencing, telephonic conversion, chat rooms.

1.6 NETWORK ADAPTER CARD

A network adapter card is hardware part, basically a circuit board or chip. It is installed on a computer so that it can connect to a network. These days, almost all new computers motherboards have in-built network adapter card or network interface card (NIC). Every network interface card has a 48-bit globally unique identifier called as Media Access Control Address (MAC) burned into its ROM chip. This MAC address is used to convey Ethernet packets to a computer.

A network adapter card works by taking the data given to it by the Central Processing Unit (CPU) and sending it to a destination. It translates the data into a type that can be transferred via cables and then translates the data it receives back into data usable by the computer. Network interface cards obtain this data from buses on the computer's motherboard; usually send information on the road to the peripheral slots. The information is transformed from a corresponding structure to a linear structure by the network card, so it can willingly transmit beside cables. Formerly the network card receives the destination device address, the data is sent. Information sent reverse is then transformed back into corresponding structure and redistributed along the computer motherboard's buses, so the CPU can progression the received data.

A network adapter card allows you to connect to a computer network. A computer network is a compilation of two or more computers with communication among them in the course of a medium. The communication medium can be through infrared, optical fibers, radio waves, etc.. By connecting to a network we can able to share or access the resources in network, also we can able to access the Internet.

1.7 REPEATER, HUB, BRIDGE, ROUTER, GATEWAY

Repeater, Hub, Bridge, Router and Gateway all are they consider as hardware which can be used in computer networking for resource sharing and accessing the Internet.

Repeater:A repeater operates at the physical layer. Basic function of the repeater is to regenerate the signal over the same network before the signal becomes too weak or corrupted. A repeater has the simple job of receiving big signal generating by NICs and other devices strengthening the signal and then sending them along repeating them to other parts of the network. Ttypically, repeaters are used to connect two physically close buildings together (when they are too far apart to just extend the segment). They can be used to join flooring of a building that would normally exceed the maximum allowable section length. Analog repeaters frequently can only amplify signals. Digital repeaters can as well rebuild signals to close to their new quality. In a data communication network, a repeater can transmit messages between sub-networks that use diverse protocols. Hubs can work as repeaters by relaying messages to all connected computers. A repeater cannot accomplish the *intelligent* routing performed by bridges and routers, because it only repeats the signals without considerate the packets, with their sources and destinations.

Hub:A hub is basically multiport repeater. Hub is used to connect multiple computers or other network device together. Hub broadcasts all network data across each connection. It has a number of Ethernet ports that are used to join two or more network equipment together. Each device or computer connected to the hub can commune with any other equipment connected to one of the hub's Ethernet ports.

Types of Hub

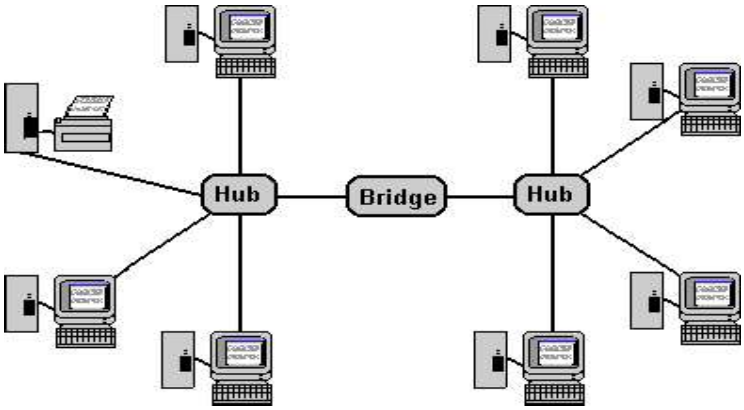
- **Active Hub:-**These are the hubs which have their have possession of power supply and can boost, clean and communicate the signal along the communication network. It serves both as a repeater as well as wiring center. These are used to expand maximum distance between nodes.
- **Passive Hub:-**These are the hubs which gather wiring from nodes and power supply from active hub. These hubs communicate signals onto the communication network without cleaning and boosting them and can't be used to extend distance between nodes.

Bridge: Bridge can divides traffic on a local area network by separating the LAN into several different segments. A bridge is operates at data link layer. A bridge is a repeater; with functionality of clean 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.

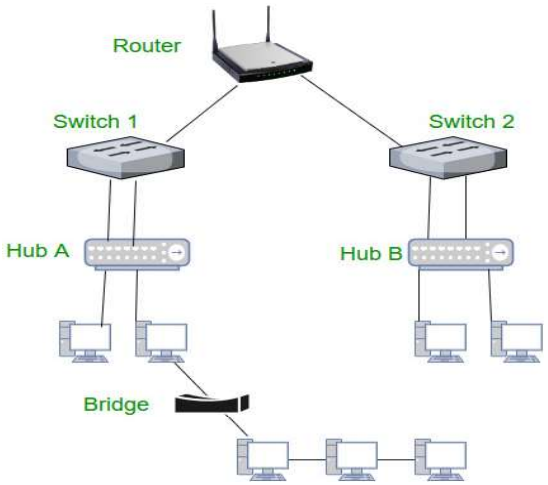
Types of Bridges

- **Transparent Bridges: -** These are the bridge in which the stations are totallyuninformedofthebridge's subsistence i.e. whether or not a bridge is addedordeletedfromthenetwork;re-configurationof
  the stations is pointless. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
- **Source Routing Bridges:-**In these bridges, routing procedure is performed by source station and the frame specifies which route to go after. The hot can

discover frame by sending a special frame called discovery frame, which spreads through the entire network using all possible paths to destination.

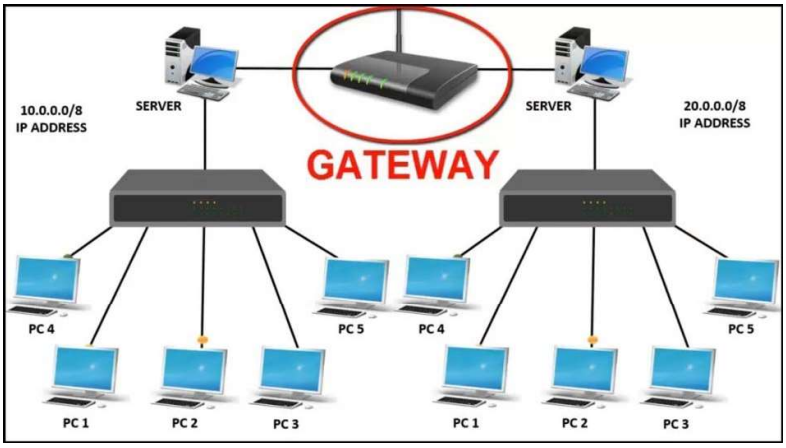


Router: The Internet is formed by networks all through the world interconnecting and passing on data to each other. Router makes the Internet work by forwarding data using a unified addressing system. Router operates at the network layer. Basic function of the router is to connect two or more networks. Router contains a processor (CPU), several kinds of digital memory, and input-output interfaces. The router is usually located within the layers of a network that determine the path for the transfer of data with the router acting as a processing unit for information packets. The router uses a specific protocol or set of rules to determine which information packets are to be routed to certain interfaces within the network. Different types of routers perform different functions depending upon the requirements of the network system.



Routers usually attach LANs and WANs together and have a energetically updating routing table based on which they make decisions on routing the data packets. Router separate broadcast domains of hosts connected all the way through it.

Gateway: A gateway acts as the meeting point or go between point between 2 different networks, using different protocols. e.g. Network A uses one protocol, Network B uses another. A computer from A needs to commune with a machine from B but due to the distinction in protocols, it does not know how to communicate. It can accept or add B's protocol but this is a tasking process and is not really competent. Instead, a gateway will decode the request from the computer in A's network, into B's language and then translate the reply from B's language into A's. So, the two machines can commune without any change in protocol. They serve up as the point of entry to a network and operate at a variety of network layers. Gateway servers are hardware equipments and gateway nodes are related with routers and switches.

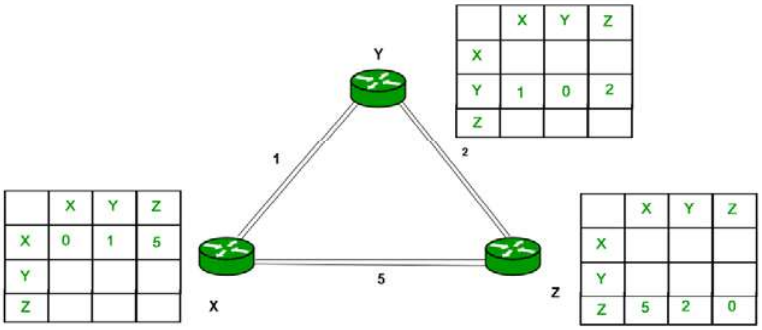


Gateways are also referred protocol converters and can function at any network layer. Gateways are normally more complex than switch or router.

Brouter – It is also known as bridging router is a device which combines features of both bridge and router. It can work moreover at data link layer or at network layer. Functioning as router, it is competent of routing packets athwart networks and working as bridge, it is capable of filtering LAN traffic.

The network layer monitors the handling of the packets by the underlying physical networks. The delivery of a packet to its final destination is consummate by using two diverse methods of delivery, direct and indirect. Routing is the process of finding a path from a source to destination in the network. When the packet travel in the network it may encountered intermediate node, that time it's required to choose path over which to send packets. The routing algorithm is the part of the network layer responsible for deciding which output interface an incoming packet should be transmitted. Means what should be the next intermediate node for the packet. To perform this task routing protocols to be used to achieve the destination. Routing algorithm use metrics to estimate what path will be the best for a packet to travel. A metric is a standard of measurement; such as reliability, path bandwidth, delay, current load on that path etc; that is used by routing algorithms to determine the best optimal path to a destination. For these purpose all different routing algorithm will initialise and maintain the routing table. Routing table contains the route information; route information varies depending on the routing algorithm used. Routing algorithm will fill routing table with a variety of information. Every routing algorithm main goal is to find the optimal path from source to destination based on the information available on the routing table. When the packet received by router, it's main task is to forward the packet to next node which always to be optimal.

Example – Consider three-routers X, Y and Z as given away in figure. Each router has their routing table. Every routing table will enclose distance to the destination nodes.

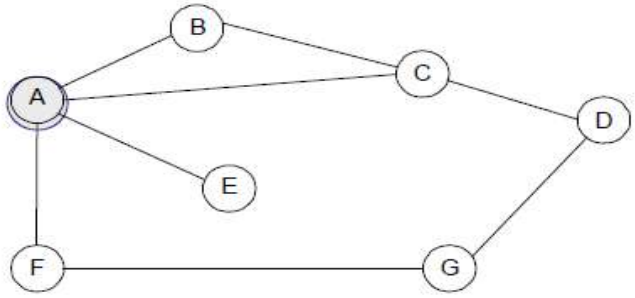


Routing Task:

- Forwarding
    - Move packet from input link to the suitable output link
    - Purely local computation
    - Must go be very fast (implement for everypacket)

Example: The routing table at A, lists –at a minimum–the next hops for the different destinations.

Destination	Next Hop
B	B
C	C
D	C
E	E
F	F
G	F



1.8 ROUTING ALGORITHM

1.8.1 Distance Vector Routing

In distance vector routing, the least-cost route between any two nodes is the routewith minimum distance. In this protocol, as the name involves, each node preserves avector (table) of minimum distances to each node. The table at each node also directs the packets to the preferred node by showing the next stop in the route (next-hop routing). A distance vector routing protocol needs that a router inform its neighbors of topology changes intermittently and,in some cases, when a change is detected in the topology of a network.

Method

The methods used to compute the best path for a network are dissimilar between different routing protocols, but the essential features of distance vector algorithms are the same crossways all DV based protocols. Distance Vector means that Routers are publicized as vector of distance and Direction. Direction is simply next

hopaddress and outlet interface and Distance means such as hop count.Routers using distance vector protocol do not have knowledge of the entire path to a destination. Instead DV usestwo methods:

1. Direction in which or interface to which a packet should be forwarded.
2. Distance from its destination.

As the name proposes the DV protocol is based on manipulative the direction and distance to any link in a network.The cost of reaching a destination is calculated using a variety of route metrics. RIP uses the hop count of the destinationwhereas IGRP takes into explanation other information such as node delay and accessible bandwidth.Updates are executed periodically in a distance-vector protocol.All or part of a router's routing table is sent toall its neighbors that are configured to use the same distance-vector routing protocol. RIP supports cross-platformdistance vector routing whereas IGRP is a Cisco Systems proprietary distance vector routing protocol. Once a routerhas this information it can amend its own routing table to reflect the changes and then inform its neighbors ofthe changes. This process has been illustrated as routing by rumor because routers are relying on the informationthey receive from other routers and cannot determine if the information is actually applicable and accurate. There are several features which can be used to help with instability and inaccurate routing information.

Vector of distances to each probable destination at each router

- How to find distances?
    - Distance to local network is 0
    - Look in neighbours' distance vectors, and add link cost to reach the neighbour
    - Find minimum distance to destination

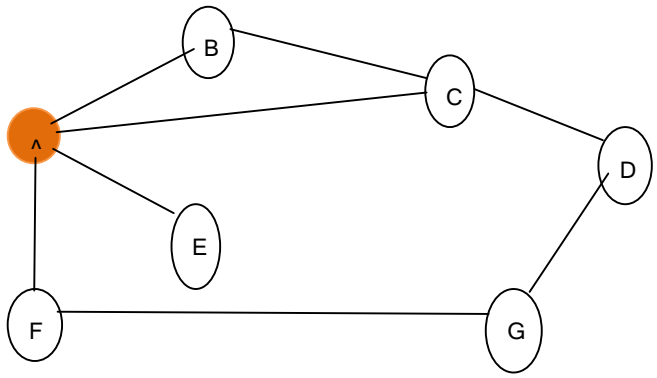
Distance Vector Routing Algorithm Summary:

- Every router preserves a vector of costs to all destinations as well as routing table
    - Initialize neighbours with known cost, others with infinity
- Periodically send copy of distance vector to neighbours

- On reception of a vector, if neighbours' path to a destination plus neighbour cost is better, then switch to better path
  - bring up to date cost in vector and next hop in routing table
- Assuming no changes, will converge to shortest paths
  - But what happens if there are changes?

Example: Initial Table at A

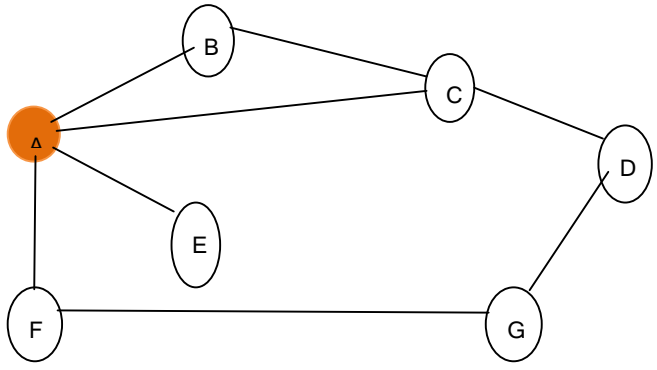
Dest	Cost	Next
B	1	B
C	1	C
D	∞	-
E	1	E
F	1	F
G	∞	-



Final Table at A

- Reached in a single iteration … single example

Dest	Cost	Next
B	1	B
C	1	C
D	2	C
E	1	E
F	1	F
G	2	F

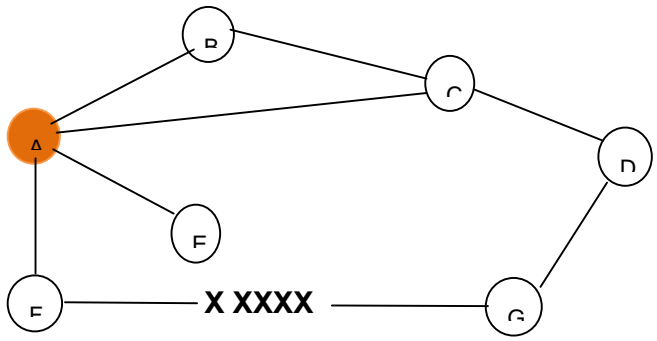


What if there are changes?

One situation: assume link between F and G fails

1. F notices breakdown, sets its cost to G to infinity and informs A
2. A sets its cost to G to infinity too, since it learned it from F
3. A find out route from C with cost 2 and accepts it

Dest	Cost	Next
B	1	B
C	1	C
D	2	C
E	1	E
F	1	F
G	3	C



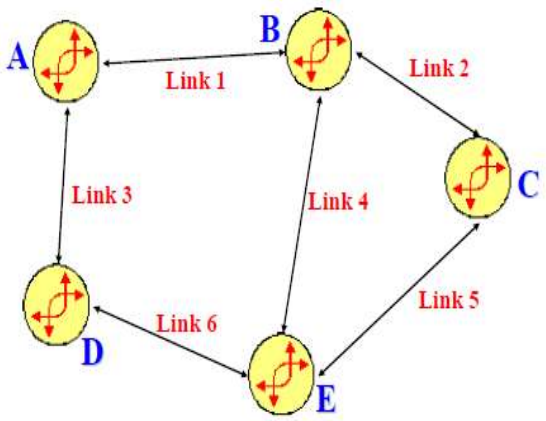
1.8.2 Link State Routing

- Principle of link state routing
  - each router remains a topology database of whole network
  - link state inform flooded or multicast to all network
  - routers compute their routing tables based on topology frequently employsDijkstra's shortest path algorithm

In Link State Routing, each router spreads information about its links to its neighbours. This information is flooded to every router in the domain of routing so that every router has knowledge of the entire network topology. Using Dijkstra's algorithm, the shortest path to each prefix in the network is calculated. Link State Routing algorithm works in mainly two phases: 1) topology dissemination (flooding) and 2) shortest path calculation.

Flooding: Each router maintains link state database and periodically sends link state packets (LSPs) to neighbour. LSP contains [router, neighbour, costs] information. Each router forwards LSPs not already in its database on all ports except where it received. Each LSP travels over the same link at most once in each direction. Flooding is fast and can be made reliable with acknowledgement.

Example: To illustrate the concept of a link state protocol and itsmode of operation, we shall consider a simple 5 nodeand 6 link network with unit link costs:



The idea following Link State Routing is to have all the nodes maintain a complete copy of thenetwork map and perform acalculation of the best routes based on this local copy of the map.The database opposite represents the network shown on the figure.

From	To	Link	Distance	Number
A	B	1	1	2
A	D	3	1	1
B	A	1	1	2
B	C	2	1	2
B	E	4	1	1
C	B	2	1	2
C	E	5	1	1
D	A	3	1	1
D	E	6	1	1
E	B	4	1	1
E	C	5	1	1
E	D	6	1	2

Comparison with Distance-Vector:

- Link-state uses a distributed database model
- Distance-vector uses a distributed processing model
- Link-state pros:
    - further functionality due to allocation of original data, no dependency on intermediate routers

    - Easier to troubleshoot
    - Fast convergence: when the network changes, new routes are calculated rapidly
    - Less bandwidth consuming
- Distance-vector pros:
    - Less complex – easier to implement and administrate
    - Needs less memory

Dijkstra's shortest path:

From the link-state database, compute a shortest path deliverytree using a *permanent* set S and a *tentative* set Q:

1) Define the root of the tree: the router
2) Allocate a cost of 0 to this node and make it the first eternal node.
3) Examine each neighbour node of the last permanent node.
4) Allocate a cumulative cost to each node and make it uncertain.
5) Among the list of tentative nodes:
    - Find the node with the smallest increasing cost and make it stable.
    - If a node can be arrived at from more than one direction, select the direction with the smallest increasing cost.
6) Repeat steps 3 to 5 until each node is stable.

1.9 LET US SUM UP

- Networking devices, also referred as network hardware, network equipment, are physical devices which are essential for communication among devices on a computer network.
- Modem is short form of ***mo****dulator-****dem****odulator.*
- A modem is a device or a program that enables a computer to transmit and receive data over a telephonic line or cable or satellite connections.
- Asynchronous transmission is named suggest the timing of a signal is unimportant. Transmission is the action of transferring something from one position to another.

- The expression synchronous is used to illustrate a continuous and consistent timed transfer of data blocks.
- A repeater operates at the physical layer. Basic function of the repeater is to regenerate the signal over the same network before the signal becomes too weak or corrupted.
- A hub is basically multiport repeater. Hub is used to connect multiple computers or other network device together. Hub broadcasts all network data across each connection.
- Bridge can divides traffic on a local area network by separating the LAN into several different segments. A bridge is operates at data link layer.
- The Internet is formed by networks all through the world interconnecting and passing on data to each other. Router makes the Internet work by forwarding data using a unified addressing system. Router operates at the network layer. Basic function of the router is to connect two or more networks.
- A gateway proceeds as the meeting point or go between points between two different networks, using dissimilar protocols.
- Brouter is also known as bridging router is a device which combines features of both bridge and router. Brouter can work whichever at data link layer or at network layer.
- A routing algorithm is that division of the networklayer dependable for deciding which output line anincoming packet should be transmitted on.
- A distance-vector routing protocol necessitates that a router notify its neighbours of topology changes cyclically and,in some cases, when alter is detected in the topology of a network.
- In distance vector, router recognizes only cost to every destination
    - hides information, causing problems
- In link state, router knows entire network topology, andcomputes shortest path by itself
    - independent computation of routes
    - potentially less robust

1.10 CHECK YOUR PROGRESS

1) Following statements are True or False

(i) Dijkstra algorithm divides the node into two sets i.e., tentative and permanent.

T ☐ F ☐

(ii) Flooding generates lots of redundant packets.

T ☐ F ☐

(iii) Flooding discovers only the optimal routes

T ☐ F ☐

2) What is Dijkstra algorithm.

3) What is LSP?

1.11 FURTHER READING

- ForouzanBehrouzA ,"Data Communications and Networking" ,McGraw-Hill,New York.
- Andrew S. Tanenbaum, "Computer Networks", Prentice Hall PTR
- Comer, Douglas E., and Ralph E. Droms. *Computer networks and internets*. Prentice-Hall, Inc.,
- Data and Computer Communication, William Stalling, Pearson Education, 2nd Edition, Delhi.

1.12 ASSIGNMENTS

1) What are the primary conditions that affect routing?
2) What is flooding? Why flooding technique is not commonly used for routing?
3) Differentiate between Link State and Distance Vector routing algorithms.
4) Differentiate between hub and switch.

Unit2: Network Architecture 2

Unit Structure

2.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

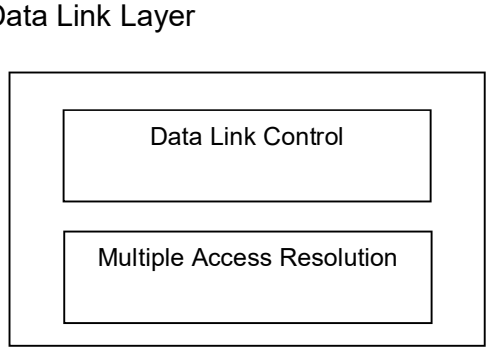
- Understand basic concept of access method used in network
- Identify the network architecture
- Apply the access method in the network
- Analysing the role of access method in communication network

2.2 INTRODUCTION TO ACCESS METHOD

Data Link layer is responsible for the creation and interpretation of different frame types based on the actual physical network being used. For instance, Ethernet and Token-ring networks support different and numerous frame types, and the Data link layer must understand the difference between them. The Data Link layer is also responsible for interpreting what it receives from the physical layer using error detection and error correction algorithms to determine when information need to be re-send. Data Link layer are normally spilt between the following sub layers.

1) Media Access Control (MAC)
2) Logical Link Control (LLC)

The two main function of the Data Link layer are data link control and media access control. The data link control function deals with the design and dealings for communication among two adjacent nodes: node to node communication. The media access control deals with how to share the link. The data link control function provides framing, flow and error control that gives smooth and reliable transmission of frames among nodes.



IEEE has made this division for LANs. The upper sublayer that is accountable for flow and error control is described the logical link control (LLC) layer. The lower sublayer that is mainly accountable for multiple access resolution is described the media access control (MAC) layer.

When stations or nodes are connected and use a common link, called a broadcast or multipoint link. For that we require multiple-access protocol to manage access the link.

Framing: The Data Link layer needs to pack bits into frames, so that every frame is distinct from another. Framing in the data link layer separates a message from one source to a destination, or from other messages to other destination, by adding a sender address and a destination address. The destination address defines where the packet is to be delivered. Frames can be variable size or fixed size.

Channel Access Method: When several nodes or stations are connected to a single channel, there must be some rules to govern these nodes or stations as they access, transmit, and release the channel. There are mainly three basic channel access methods:

1) Contention
2) Polling
3) Token Passing

Access methods employ a sure amount of the channel's bandwidth for access control. The usable portion of the channel's bandwidth is limited by the access method being used. Different access methods have different overhead effects on network traffic.

2.3 CONTENTION

In contention method or random-access method, no station is superior to another station and none is assigned the control over another. No station authorizes, or does not authorize, another station to send. To avoid contention, with other transmissions on the medium or channel, the MAC unit first observes the carrier sense signal and, if necessary, defers to any passing frame. After a short additional delay (known as the **inter-frame gap**) to allow the passing frame to be received and processed by the addressed station(s), transmission of the frame is initiated. As the bitstream is

transmitted, the transmitter simultaneously monitors the received signal to detect whether a collision has occurred. Assuming a collision has not been detected, the complete frame is transmitted and, after the FCS field has been sent, the MAC unit awaits the arrival of a new frame, either from the cable or from the link control layer within the station. If a collision is detected, the transmitter immediately turns on the collision detect signal and enforces the collision by transmitting the jam sequence to ensure that the collision is detected by all other stations involved in the collision. After the jam sequence has been sent, the MAC unit terminates the transmission of the frame and schedules are transmission attempt after a short randomly computed interval. Figure summarizes the frame reception sequence.

Advantages of Contention:

- Contention is a very simple access method that has low administrative overhead necessities. No network traffic is essential to direct the access method.
- Actual user data throughput is rather high at low traffic levels in contrast to the total amount of utilized network band width.

Disadvantages of Contention:

- At high traffic levels, data collisions and the resulting retransmission reduce performance dramatically. It is in theory possible that collisions can be so recurrent at higher traffic levels that no station has a apparent chance to transmit.
- Channel access is *probabilistic* rather than *deterministic*. Since of retransmissions and the time it takes to sense collisions, automatic equipment that cannot tolerate delays cannot use this kind of access. Contention presents no means of set up the frequency of a station's chance to transmit.

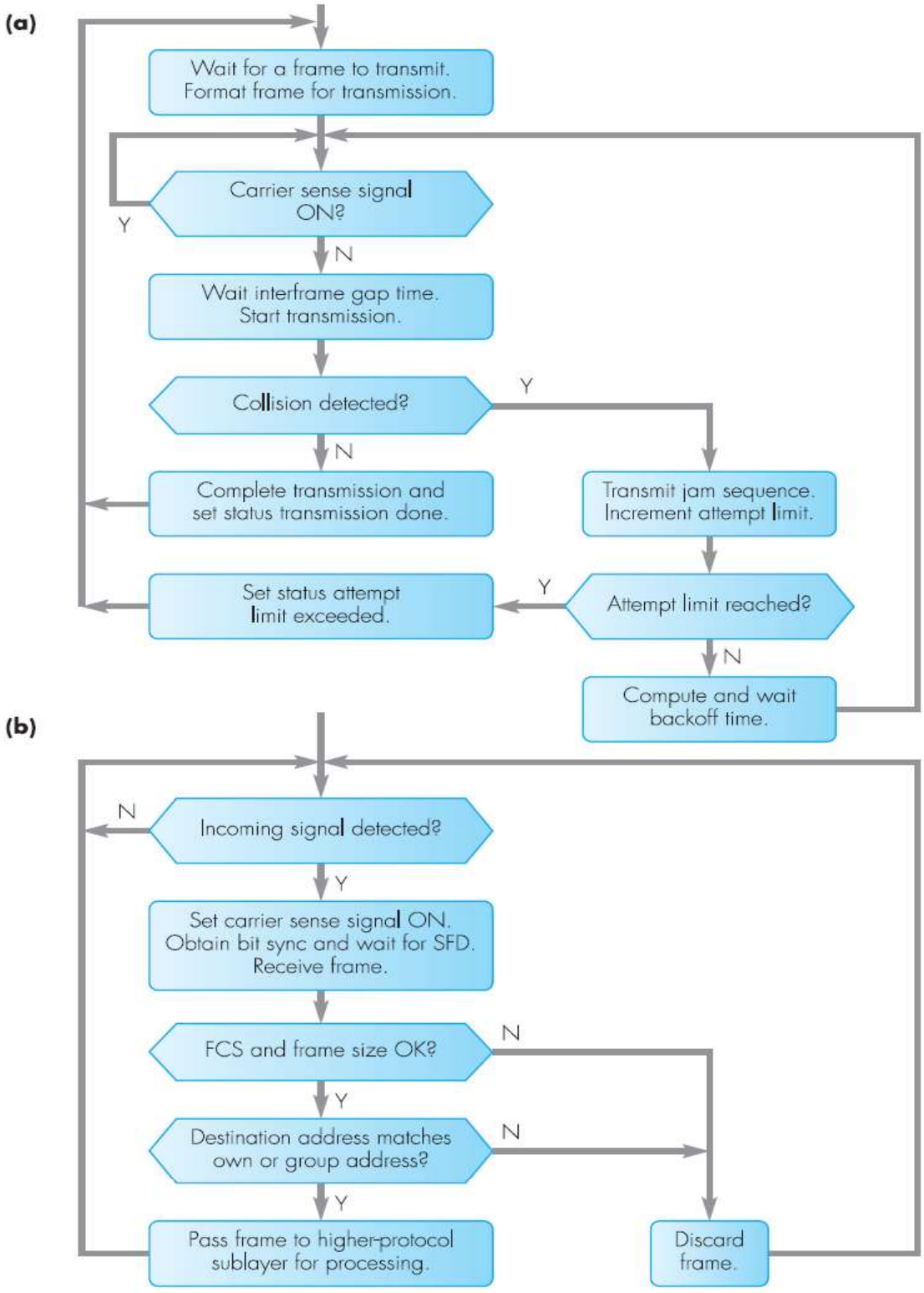


Figure: (a) transmit (b) receive

2.4 POLLING

Polling bear a resemblance to a well-ordered gathering in which the chairman must distinguish an attendee before that person is permitted to speak. The chairman's accountability is to maintain organize in the meeting and make sure that each person who wants to speak has a chance to do so. It's also called master-slave method. The master device describes out the slave device's address, the slave reacts. Polling is an access method that assigns one device (described a "controller", "primary", or "master") as a channel access administrator. This device (Master) queries every one of the other devices ("secondaries") in some determined order to see whether they have information to transmit. If so, they transmit (usually through the master). All data interactions must be made through the primary device when the ultimate destination is a secondary device. The master device controls the link; the secondary devices follow its instructions. It is up to the master device to determine which device is allowed to use the channel at a given time. The master device therefore is always the initiator of a session. The message sent by the controller encloses the address of the node being selected for surrendering access. Even though all nodes receive the message but the addressed one reacts to it and sends data, if any. If there is no data, typically a poll reject(NAK) message is sent reverse. Problems include high overhead of the polling messages and high dependence on the reliability of the controller.

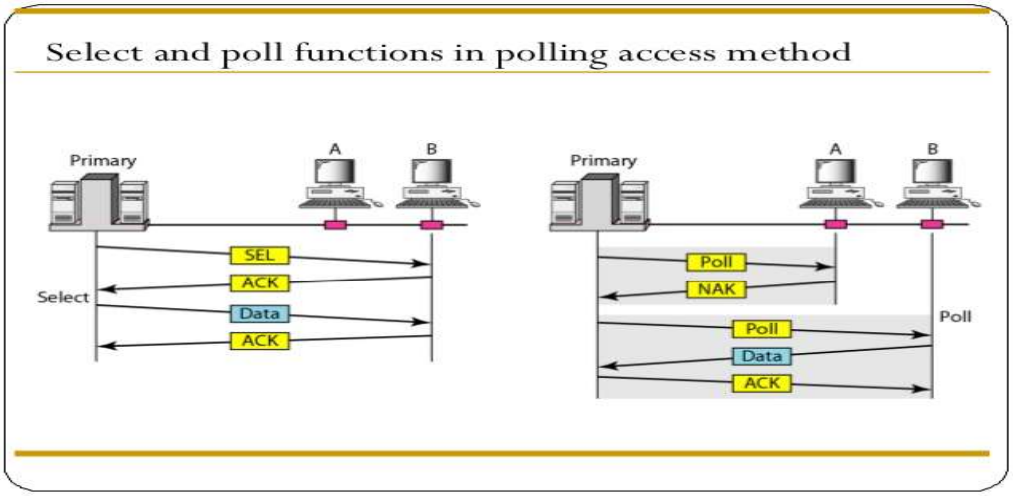


Figure: Polling access method

Advantages of Polling:

- Many individuality of polling can be resolute centrally, including the polling order and node priorities.
- Polling makes certain that channel access is expected and fixed. Since the time delays among the primary and secondary devices can be considered, this access method is called deterministic. Deterministic access methods are appropriate for calculating some automated equipment because every piece of equipment is guaranteed access to the network at predetermined intervals.
- Polled channels cannot be over saturatedwith traffic. As demand increases, traffic raises up to a greatest level. The polling mechanism ensures that maximum traffic level cannot be exceeded. Nor can surplus traffic decrease the performance of the network.

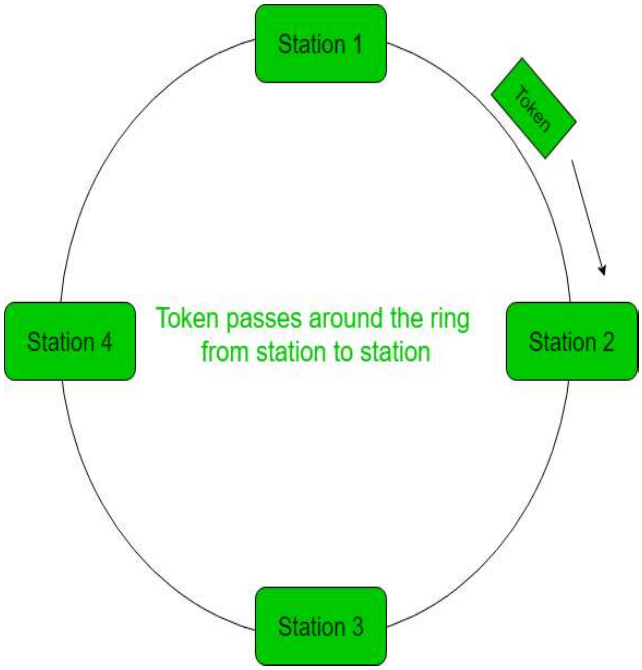
Disadvantages of Polling:

- Several applications cannot purpose with the time delays required for polling other devices.
- The process of polling involves large numbers of messages that take up available band width. Traffic is required to poll every node, even nodes that are inactive.
- Some polled networks use half-duplex transmission lines. These resources that the primary and secondary devices must revolve around the line, requiring some bandwidth.
- Polling requires a complicated central control mechanism that requires extensive configuration

2.5 TOKEN PASSING

In the token passing method, the nodes or stations in a network are organized in a logical ring. In the token passing only one station can talk at a time. The station waits for a free token in order to use the communication channel to talk. The token circulate among the stations until one of them wants to use the available channel or link. The station then takes the token and uses the channel. One the station or node uses the channel, the sending device sets the token busy bit, adds an information

field, add the message it would like to send and adds a trailer packet. The header packet contains the address of the station for which the message was anticipated. The entire message is then send out on the communication link. Every station examines the header and checks the address to see if it is being talked to. If not, it ignores the message. The anticipated station copies the message and sets bits in the trailer field to indicate that the message was received, and then sends the message back out on the communication link. The original station receives the message back and checks that the message was received. It then frees the token and sends it out for other station to use. There exist problems similar to repetition of token or token is lost or insertion of new station, removal of a station, which need be attempt for correct and reliable operation of this method.



Advantages of Token Passing:

- Token passing offers the maximum data throughput probable under high traffic conditions.
- One transmission can happen at a time, and collisions cannotoccur (non-contention). Therefore, token passing practice less recital degradation at higher traffic levels than contention.
- Token passing is deterministic. Each station is sure an opportunity to transmit each time the token travels approximately the ring.

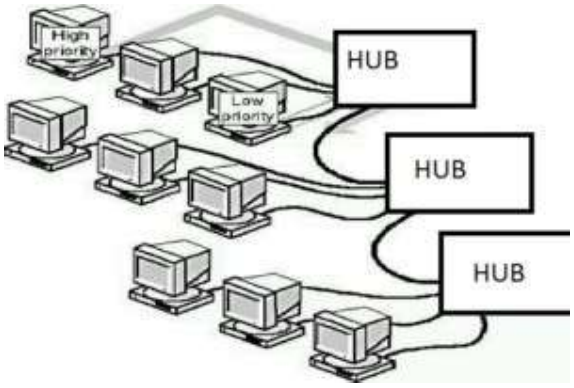
- Some token passing systems facilitate you to set priorities for devices that need prohibited access to the token.
- As the traffic enlarges, data throughput also enlarges to a certain level, and then steady.

Disadvantages of Token Passing:

- Token passing involves complex protocols for managing the network and improving from errors. The traffic associated with these protocols has higher band width overhead then is required for CSMA.
- All devices require complicated software that needs to be modified whenever a station is added or removed.
- Some systems necessitate an additional innermost controller that adds to the overhead and reduces throughput. Cabling and network hardware can be more expensive for token passing networks than for CSMA networks.

2.6 DEMAND PRIORITY

Demand priority is the media access protocol definite in the IEEE 802.12 draft standard. Various methods are used to ensure equality of access for all nodes and to guarantee access time for individual nodes. Round-robin selection methods are used to give each node an equal opportunity to transmit data. Two priority levels are provided. A network using the demand priority method has groups of nodes connected to a series of interconnected hubs. Nodes communicate only with their hubs; the computers do not access the network directly. Each hub is responsible for monitoring the nodes attached to it, listening for requests to transmit. Nodes can receive and transmit at the same time, due to the cabling method used. Administrators can designate that certain types of data will be given higher priority than other types. Because demand priority is a contention method, two nodes can request to transmit simultaneously, but the hub will allow the one with the highest priority data to transmit first.



Advantages of demand priority:

- More efficient; each hub interacts only with the computers connected directly to it.
- Flexible; Computers can transmit and receive simultaneously.
- Selective; Transmissions are not broadcast to the whole network, so there is less congestion of network bandwidth.

Disadvantages of demand priority:

- Relatively costly; Implementation requires expensive equipment.
- Limited; Few experienced support persons available due to limited usage of demand priority networking

2.7 LET US SUM UP

- With contention schemes, network devices may transmit when they want.
- No referee authorization when a device may or may not use the channel.
- This scheme is simple to design.
- The method provides identical access rights to all stations.
- Stations basically transmit when they are ready, with no considering what other stations are doing.
- Regrettably, the "transmit whenever ready" policy has one important shortcoming.
- Stations can transmit at the same time.
- Polling centralizes channel access control.

- Maximum and minimum access times and data rates on the channel are expected and set.
- Priorities can be allocated to ensure faster access from some secondary.
- Polling is deterministic and is measured appropriate for channels controlling some kinds of automated equipment.
- In token-passing scheme, a small frame is agreed in an orderly way from one device to another.
- A token is an extraordinary authorizing message that temporarily gives control of the channel to the device holding the token.
- Passing the token about distributes access control amongst the channel's devices.

2.8 CHECK YOUR PROGRESS

Answer in brief.

1. What are the disadvantages of contention?

……

……

2. Explain the term “arbitration?

……

……

3. Which method of media access provides a centralize administration?

……

……

4. What are the standards for IEEE 802.4 protocol?

……

……

2.9 FURTHER READING

- ForouzanBehrouzA ,”Data Communications and Networking” ,McGraw-Hill,New York.
- Andrew S. Tanenbaum, “Computer Networks”, Prentice Hall PTR

- Comer, Douglas E., and Ralph E. Droms. *Computer networks and internets*. Prentice-Hall, Inc.,
- Data and Computer Communication, William Stalling, Pearson Education, 2nd Edition, Delhi.

2.10 ASSIGNMENTS

1) Explain the protocols in Data link layer.
2) Explain the concept of Token ring
3) Define flow control?
4) In what situations contention based MAC protocols are suitable?

Unit 3: Network Topologies 3

Unit Structure

3.1 LEARNING OBJECTIVE

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

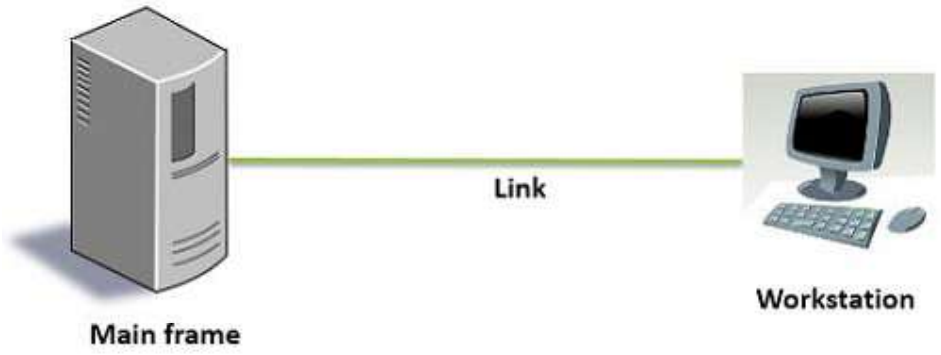
3.2 INTRODUCTION TO NETWORK TOPOLOGY

Basically network topology refers to the way in which the nodes/computers connected into the network. Network topology is typically a schematic explanation of the agreement of a network, together with its nodes and connecting lines. Each and every network topology is appropriate to specific tasks 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 ways of essential network geometry: the physical topology and the logical topology. Physical topology describes where the network's different components like its devices and cables are placed and installed, while logical topology explains network's information (data) flow and transmission, apart from physical design. Distances among nodes, physical interconnections, transmission rates, and / or signal types may vary among two networks, yet their topologies may be identical. For communications to happen, two devices must be connected in some way to the same link at the same time. There are two probable types of connections: point-to-point and multipoint.

Point-to-Point:

Point-to-point networks contains precisely two hosts such as computer, switches, routers, or servers connected back to back using a single part of cable. Frequently,

the receiving end of one host is connected to sending end of the other and vice versa.

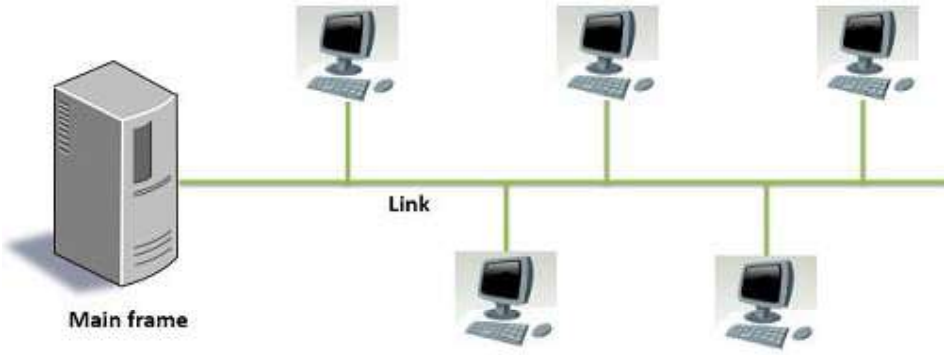


Point-to-point Connection

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:

In a multipoint connection, more than two specific devices share a single link. In a multipoint connection environment, the capacity of the channel is shared, either spatially or temporally. For sharing a general *channel*, each device needs ameans to identify itself and the device to which it wantsto send information. The process used to recognizesenders and receivers is called *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.

Key Differences between Point-to-Point and Multipoint Connection:

1. While there is a single dedicated link only among two devices, it is a point-to-point connection whereas, if a single link is shared by more than two devices then it is said to be a multipoint connection.
2. During multipoint connection, the channel capacity is shared provisionally by the devices in connection. In a point-to-point connection, the whole channel capacity is reserved only for the two devices in the connection.
3. During point-to-point connection, simply is a single transmitter and a single receiver. On the other hand, in multipoint connection, single transmitter, and there can be several receivers.

Both logical and physical topologies could be identical or dissimilar in a same network.There are four fundamental topologies likely: Bus, Star, Ring, and Mesh.

3.3 BUS TOPOLOGY

In Bus Topology, all stations connect through proper hardware interfacing known as a *tap*, straight to a linear transmission medium, or bus as shown in Figure. It is one of the easy forms of networking where a breakdown of a device does not influence the other devices. But breakdown of the shared communication line can make all other devices stop functioning. One long communication cable acts as a backbone to link all the devices in a network. While one host sends an electrical signal on the bus, the signal is received by all hosts close to the bus. A downside of bus-based networks is that if the bus is actually cut, then the network is tearing into two inaccessible networks. For this basis, bus-based networks are sometimes measured to be hard to operate and preserve, particularly when the cable is long and there are

many places where it can shatter. Bus-based topology was used in early Ethernet networks.

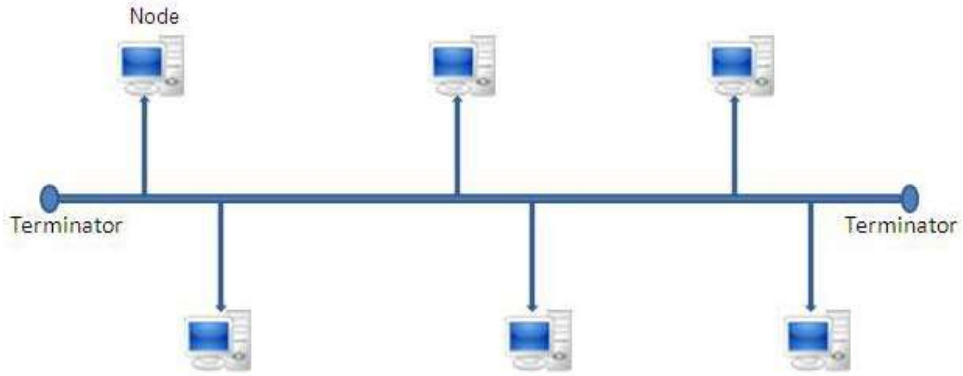


Figure: Bus Topology

At every end of the bus here is a *terminator*, which takes up any signal, stopping reflection of signal from the endpoints. If the terminator is not present, the endpoint takes step like emulate and reflects the signal back causing interference and other problems.Bus topology contains the key characteristics like flexible, moderate reliability, expandable and moderate performance. A shared communication link is used between different stations; hence it is very much cost effective. Anyone can easily add any new node or delete any node without affecting other nodes; this makes Bus topology easily expandable. As the distance during which signal traverses increases, the attenuation increases. If the sender sends data with a little strength signal, the utmost station will not be able to receive the signal appropriately. While on the other hand if the transmitter sends the signal with a superior strength then the utmost station will get the signal properly but the station near to it may face over-drive. Therefore, delay and signal unbalancing will might a maximum length of shared medium, which can be used in bus topology.

3.4 RING TOPOLOGY

During the ring topology, the network consists of a set of repeaters joined by point-to-point links in a closed round as shown in Figure. Like the bus organization, each host has a single physical interface connecting it to the ring. Whichever signal sent

by a host on the ring will be received by all hosts connected to the ring. When one host attempts to commune or send message to a host which is not nearby to it, the data travels through all intermediate hosts. To connect one more host in the existing structure, the administrator may need only one more extra cable. Each device in the ring topology incorporates a repeater. When a device receives a signal intended for another device its regenerates the bits using the repeater and passes them along. A ring topology, relatively easy to reconfigure and install. To add or remove a device requires changing only two connections. Basically in a ring topology, a signal is circulating at all times. One device does not receive a signal within specified time, it can issue an alarm.

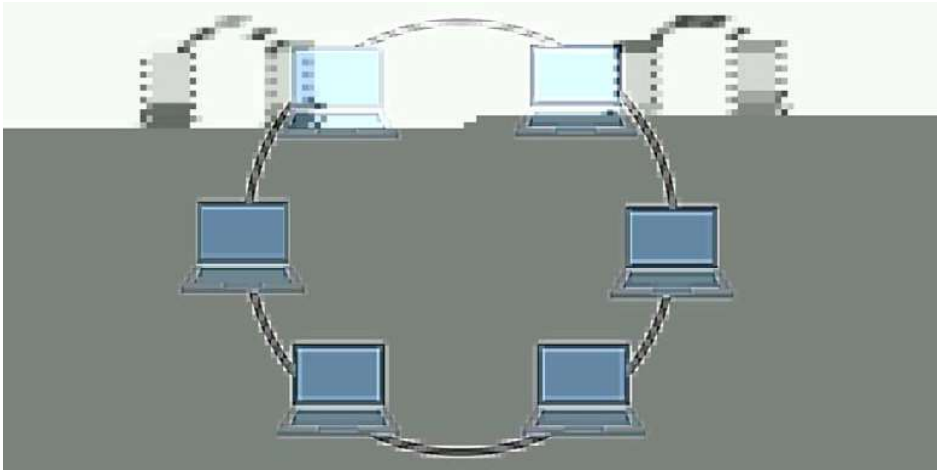


Figure: Ring Topology

The links are unidirectional, that is data are transmitted in one direction only and all are leaning in the similar way. Thus, data travel around the ring in one direction either clockwise or counterclockwise. This topology is not very trustworthy, because when a link fails the whole ring connection is broken. But consistency can be improved by using *wiring concentrator*, which helps in bypassing a defective node and rather is similar to star topology.

3.5 STAR TOPOLOGY

Star topology, every device has a committed point-to-point link only to central controller, typically called a hub. In such topologies, hosts have a lone

physicalinterface and there is one physical link among each host and the center of the star. The breakdownof the central node implies the stoppage of the network. However, if one physical link fails (e.g. because the cablehas been cut), then only and only one node is disconnected from the network.

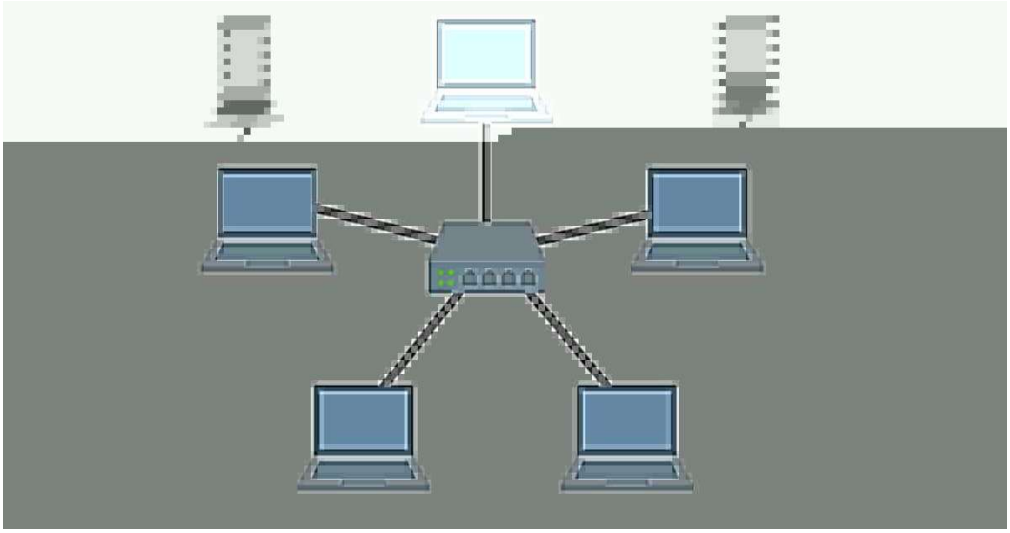


Figure: Star Topology

In do, star-shaped networks are easier to work and preserve than bus-shaped networks. Many network administrators also are glad about the fact thatthey can manage the network from a central point. Star topology contains key features like, high speed, very flexible, provide high reliability, and also provide the high maintainability. Exceptionally High speeds of data transfer can be achieved by using star topology, mainly when the star coupler is used in the switch mode. This topology is the easiest to preserve, between the other topologies. In a star topology, the failure of a single device or cable does not bring down the entire network which is most important advantage of the star topology compare to other network topology. Also, the centralized networking device can reduce cost in the extended run by making network management much easier but in the opposite site of these, if the failure of the central device (hub) causes the whole network failure. This topology is very supple and is the most favored topology.

3.6 MESH TOPOLOGY

When all the hosts on the network are connected with each other in separate communication lines, the network topology is called the *Mesh topology* as shown inFigure.

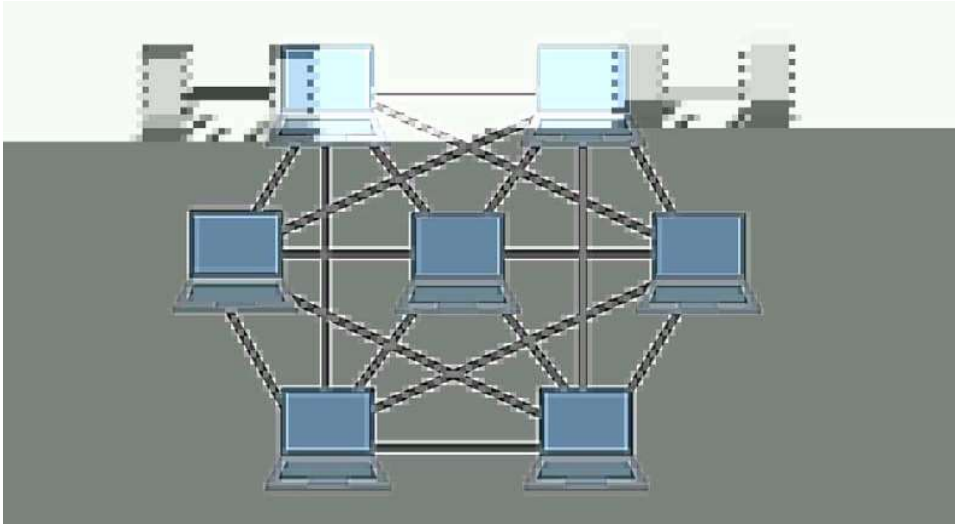


Figure: Mesh Topology

The key characteristics of the mesh technologies are: Fully connected, Robust – Highly reliable, not flexible, poor expandability. This topology has hosts in point-to-point connection with each other host or may also have hosts which are in point-to-point connection with little hosts only. Hosts in Mesh topology also work as communicate for other hosts which do not have through point-to-point links. Hosts in Mesh topology also work as relay for other hosts which do not have direct point-to-point links. In practice, usually only partialmesh network topology is applied,where not all but a few particularly relevant to the network hosts are connectedby separate lines. Mesh topology provides advantage like to ensure a reliable and fast data transfer, upon failure of one communication line the data can be transmitted through other communication lines. But on other side, mesh topology also gives the disadvantage like, it is not cost-effective, because it requires a large amount of connections on each host and also applied only to small networks.

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 computer and network device is associated to 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 network equipments are connected to other network devices. Mesh topology is expensive because of the additional cables needed and it is very composite and not easy to manage.
- The main benefit of mesh topology is many paths to the destination computer. If one link is fail, we have another 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.

Solutions:

1. n(n-1)/2
2. terminator
3. Delay, signal unbalancing
4. unidirectional, one
5. Tree
6. BUS

3.9 FURTHER READING

- ForouzanBehrouzA ,"Data Communications and Networking" ,McGraw-Hill,New York.
- Andrew S. Tanenbaum, "Computer Networks", Prentice Hall PTR
- Comer, Douglas E., and Ralph E. Droms. *Computer networks and internets*. Prentice-Hall, Inc.,
- Data and Computer Communication, William Stalling, Pearson Education, 2nd Edition, Delhi.

3.10 ASSIGNMENTS

1) List out the advantages and drawbacks of bus topology.
2) List out the advantages and drawbacks of ring topology.
3) Why star topology is commonly preferred?

Unit 4: Switching & Routing In Networks

4

Unit Structure

4.1 LEARNING OBJECTIVE

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

As discussed in the previous chapter about the point-to-point connection between each pair of device (mesh technology) or between a central device and every other device (a star topology). These methods used to connect the set of devices. Using this method we are able to connect the multiple devices in the network and so that the communication among them possible but these methods, however impractical and inefficient when applied to very large networks.

The length and number of the links require too much infrastructure to be cost-efficient. In this kind of situation, the most of the links would be the idle most of the time. A fruitful solution for that is switching. Switching is a method by which data or information sent from source towards destination which is not directly connected. Networks have interconnecting devices, which receives data from directly connected sources, stores data, also analyze it and then forwards to the next interconnecting device closest to the destination.

Switching can be categorized in three categories: 1) Message Switching 2) Packet Switching and 3) Circuit Switching.

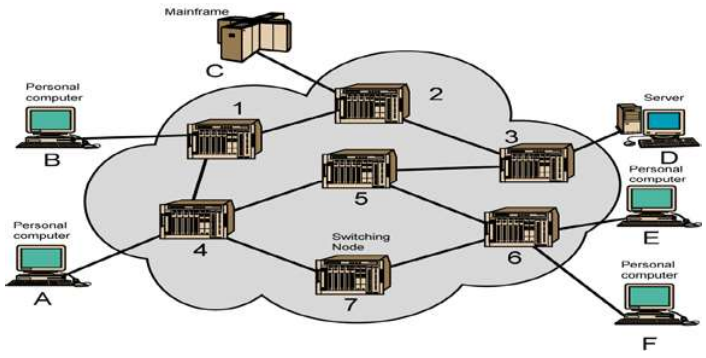


Figure: Simple Switching Network

Key features of a switched network are given under:

- There exist several paths among a source-destination pair for better network reliability.
- The switching nodes are not concerned with the stuffing of data.
- Their reason is to offer a switching capability that will move data from node to node until they reach the destination.
- Uses FDM or TDM for node-to-node communication
- Network topology is not regular.

Routing and switching can be two terms that are hard to distinguish. First of all switching and routing is not the similar thing. Switching engages moving packets among devices on the same network. Conversely, routing involves moving packets between different networks. Switches work at layer 2 of the OSI Model. A switch, also referred to as a multi-port bridge, is able to determine where a packet should be sent by examining the MAC address inside the data link header of the packet. A switch preserves a database of MAC addresses and what port they are linked to. Routers, on the other hand, work at layer 3 of the OSI Model.

A router is able to establish where to send a packet with the Network ID within the Network layer header. It then uses the routing table to decide the route to the destination host. A Router maintains a table described Routing Table and uses the routing table to establish the route to the destination network.

4.3 MESSAGE SWITCHING

Message switching was a technique developed as an alternate to circuit switching, before packet switching was introduced. Message switching is a network switching technique in which data is routed in its entirety from the source node to the destination node, one hope at a time. In message switching, if a station desires to send a message to a further station, it first adds the destination address to the message. Message switching does not set up a devoted path among the two communicating devices *i.e.* no straight link is established among sender and receiver.

Each message is treated as an independent unit. In message switching, each complete message is then transmitted from device to device through the internetwork *i.e.* message is broadcast from the source node to intermediate node. The center node stores the entire message provisionally, examines it for errors and transmits the message to the next node based on an accessible free channel and its routing information. Because of this reason message switched networks are called store and forward network as shown in figure. Message switching extravagances each message as an autonomous entity.

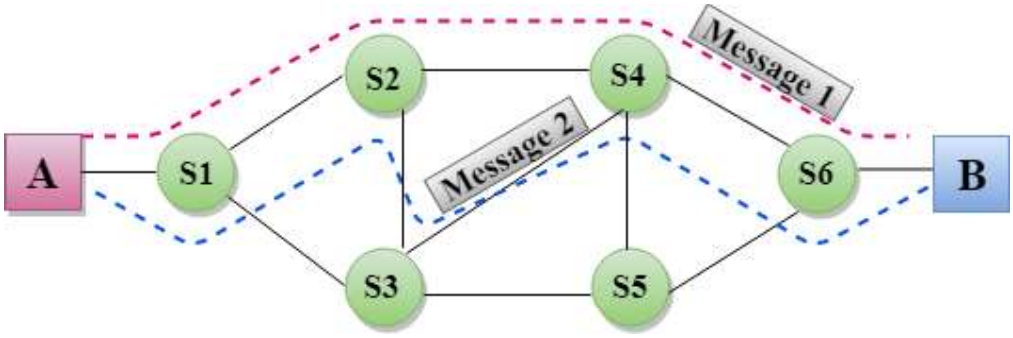


Figure: Message Switching

Message switched data networks are therefore called hop-by-hop systems.

They provide 2 distinct and important characteristics:

1. **Store and forward –** The middle nodes have the responsibility of transferring the whole message to the next node. Hence, each node must have storage capacity. A message will only be delivered if the next hop and the link connecting it are both accessible, or else it'll be stored for an indefinite period. A store-and-forward switch forwards a message only if sufficient resources are available and the next hop is accepting data. This is called the store-and-forward property.
2. **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.

Advantages of Message Switching

The advantages to message switching are:

- Data channels are shared between communication devices, improving the use of bandwidth.
- Messages can be stored provisionally at message switches, when network congestion becomes a trouble.
- It is helpful 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.
- Priorities may be used to manage network traffic.
- Broadcast addressing uses bandwidth more competently since messages are delivered to multiple destinations.

Disadvantages of Message Switching

The various disadvantages of message switching are:

- As message length is limitless, each switching node must have adequate storage to buffer message.
- Storing & forwarding capability introduces delay thus making message switching inappropriate for real time applications like voice and video.
- 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 can occur due to the storing and forwarding facility provided by the message switching technique.

4.4 PACKET SWITCHING

The packet switching is a switching technique in which the message is sent in one goes, but it is divided into smaller pieces, and they are sent individually. Through this technology, packets are sent as soon as they are accessible. There is no need to set up a devoted path in advance. It is up to routers to use store-and-forward transmission to send every packet on its mode to the destination on its own. In computer network, we need to send data from one system to another. If the data is going to pass through packet switched network, it needs to be divided into packets of fixed or variable size. The size of the packet is determined by the network and the protocol used in the network. There is no resource allocation is made for packet in packet switching network. Its means that there is no bandwidth is reserved for the communication links, and also there is no scheduled processing time for each packet. In packet switching, the resources are allocated based on the demand. The resource allocation is also done on the basis of first come first served basis only. In this type of network, each packet is treated independently of all others. Packet in this approach is referred to as datagram.

Every packet contains some information in its headers such as source address, destination address and sequence number. One path is selected between source and destination. When the sender has data to send, it exchanges them into packets and forwards them to subsequently computer or router. The router stores this packet until the output line is available. Then, this packet is transferred to next computer or router (called as hop). This way, it moves to the destination hop by hop. All the packets belonging to a transmission may or may not take the identical path / route. The route of a packet is determined by network layer protocols.

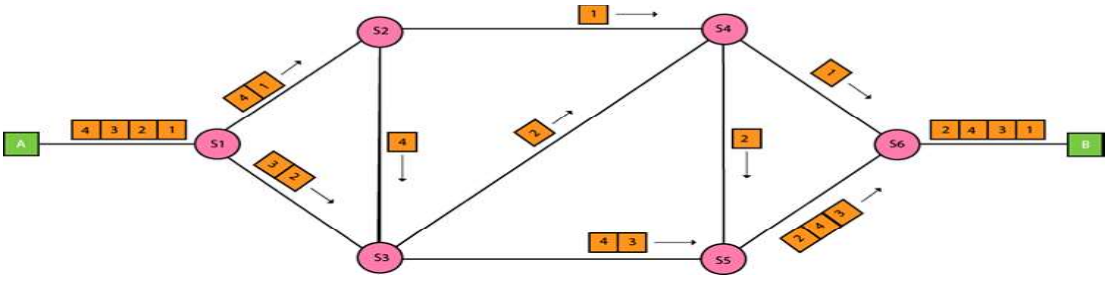


Figure: Packet Switching

Advantages of Packet Switching

- Delay in delivery of packets is fewer, seeing as packets are sent as soon as they are accessible.
- Switching devices don't need huge 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 of Packet Switching

- They are inappropriate for applications that cannot afford delays in communication like high quality voice calls.
- Packet switching high installation costs.
- They require complex protocols for delivery.
- Switching nodes for packet switching need huge amount of RAM 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.

4.5 PACKET ROUTING

Routing is a procedure which is performs by layer 3 (or network layer) devices in order to deliver the packet by deciding an optimal path from one network to another. The routing algorithms used for routing the packets. The routing algorithm is nothing but a software accountable 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 dimension such as hop count, delay, bandwidth, current load on the path, etc. used by the routing

algorithm to decide the optimal path to the destination. The routing algorithm initializes and preserves the routing table for the method of path determination. Mainly three types of routing:

1) Static Routing
2) Default Routing
3) Dynamic Routing

Static Routing:

- Static Routing is also known as Non-adaptive Routing.
- It is a method in which the administrator manually adds the paths / routes in a routing table.
- A Router can send the packets for the destination next to the route definite by the administrator.
- In this method, routing decisions are not made based on the circumstance or topology of the networks

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 arrangement with the single exit end.
- It is also useful when the mass of transmission networks have to transmit the data to the similar device.
- When a definite route is mentioned in the routing table, the router will select the explicit route rather than the default route. The default route is select only when a specific route is not declared in the routing table.

Dynamic Routing

- It is also known as Adaptive Routing.
- It is a method in which a router adds a latest route in the routing table for each packet in response to the changes in the situation or topology of the network.

- Dynamic protocols are used to find out the new routes to make the destination.
- In Dynamic Routing, RIP and OSPF are the protocols used to discover the new routes.
- If any route goes fail, then the automatic modification will be made to reach the destination.

4.6 CIRCUIT SWITCHING

Communication via circuit switching means that there is a devoted communication path / route among the two stations. The path is a associated through a succession of links among network nodes. In a circuit switching network, this consists of a set of switches connected by physical links. A dedicated path is available between two stations from one or more links. But, each connection uses only one dedicated channel on each link. Each communication link is divided into *n* channels by using TDM or FDM. Circuit switching is commonly used technique in telephony, where the caller sends a special message with the address of the caller (i.e. by dialing a number) to state its destination. Circuit switching takes place at the physical layer. Compared to the packet switching, in circuit switching the resources are to allocate during the communication.

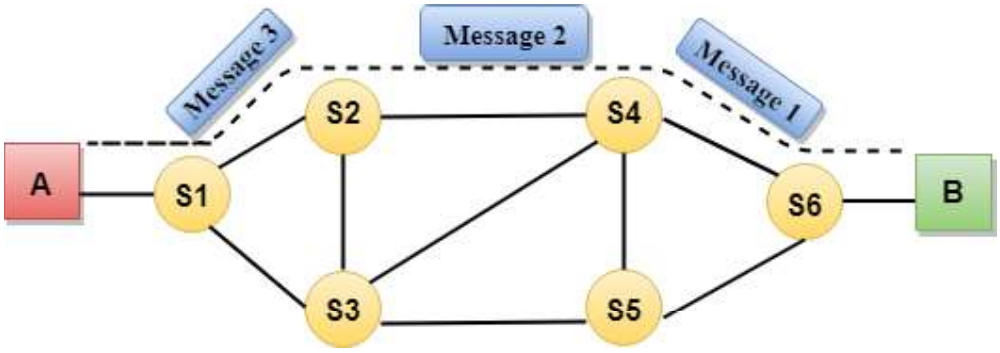


Figure: Circuit Switching

Data transferred between the two stations are not to be divided in packets. The data are a continuous flow sent by the source station and received by the destination station. There is no addressing involved during data transfer. The

switches route the data based on their occupied time slot (TDM) or band (FDM). Circuit switching mainly involves three distinct phases.

4) Circuit establishment: establish the connection of end-to-end before the communication happened between two stations.
5) Data transfer: data is transfer from source to destination. The data may be analog or digital, depending on the nature of the communication network. Connection is full-duplex type.
6) Circuit disconnect: at the end of the data transfer the circuit is disconnected. Resources which are allocated during the transmission are de-allocated.

Advantages of Circuit Switching

- 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 any delay as there is no waiting time at each switch.
- Since a devoted continuous transmission path is recognized, the technique is appropriate for long continuous transmission.

Disadvantages of Circuit Switching

- Once the dedicated path is recognized, the only delay occurs 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 devoted path is required for each connection.
- Dedicated channels require more bandwidth.
- It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.

- In this case, the connection is devoted consequently no other data can be transferred even if the channel is available for free.

Circuit Switching VS Packet Switching

In circuit switching there are 3 phases i) Connection Establishment. ii) Data Transfer. iii) Connection Released.	In Packet switching directly data transfer takes place .
In circuit switching, each data unit know the entire path address which is provided by the source	In Packet switching, each data unit just know the final destination address intermediate path is decided by the routers.
In Circuit switching, data is processed at source system only	In Packet switching, data is processed at all intermediate node including source system.
Delay between data units in circuit switching is uniform.	Delay between data units in packet switching is not uniform.
Resource reservation is the feature of circuit switching because path is fixed for data transmission.	There is no resource reservation because bandwidth is shared among users.
Circuit switching is more reliable.	Packet switching is less reliable.
Wastage of resources are more in Circuit Switching	Less wastage of resources as compared to Circuit Switching
It is not a store and forward technique.	It is a store and forward technique.
Transmission of the data is done by the source	Transmission of the data is done not only by the source, but also by the intermediate routers
Congestion can occur during connection establishment time	Congestion can occur during data transfer phase

4.7 LET US SUM UP

- The procedure of moving the data packets towards their destination by forwarding them from one port to the other port is called as **switching**.
- Various switching techniques are-
  1. Circuit Switching
  2. Message Switching
  3. Packet Switching
- Circuit switching technique operates in the following three phases-
  - Establishing a circuit
  - Transferring the data
  - Disconnecting the circuit
- Total time taken to convey a message in circuit switched network = Connection set up time + Transmission delay + Propagation delay + Tear down time
- Circuit switching has well defined and dedicated path exists for the data to travel.
- Circuit switching has no waiting time at any switch and the data is transmitted without any delay.
- In Circuit switching, no re ordering is required.
- In Circuit switching, the channel is blocked for two ends only.
- In Circuit switching, the time required for establishing the circuit between the two ends is too long.
- In Circuit switching, dedicated channels require more bandwidth.
- In message switching,
  - There exists no dedicated path to transfer data.
  - The whole message is treated as a single data unit.
  - The message is then forwarded from hop to hop.
  - Store and forward is an important characteristic of message switching.
- Message switching requires enough storage at every switch to accommodate the entire message during the transmission.
- In packet switching,
  - The whole message to be sent is divided into numerous smaller size packets.

- This procedure of dividing a single message into smaller size packets is called as packetization.
- These smaller packets are sent after the other.

- Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.

4.8 CHECK YOUR PROGRESS

1) A local telephone network is an example of a _____ network
2) In _____ resources are allocated on demand.
3) Most packet switches use the principle
4) The resources needed for communication between end systems are reserved for the duration of session between end systems in _____

Solution:

1) Packet switched
2) packet switching
3) Store and forward
4) Circuit switching

4.9 FURTHER READING

- ForouzanBehrouzA ,"Data Communications and Networking" ,McGraw-Hill,New York.
- Andrew S. Tanenbaum, "Computer Networks", Prentice Hall PTR
- Comer, Douglas E., and Ralph E. Droms. *Computer networks and internets*. Prentice-Hall, Inc.,
- Data and Computer Communication, William Stalling, Pearson Education, 2nd Edition, Delhi.

4.10 ASSIGNMENTS

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.

યુનિવર્સિટી ગીત

સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ

શિક્ષણ, સંસ્કૃતિ, સદ્‌ભાવ, દિવ્યબોધનું ધામ
ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી નામ;
સૌને સૌની પાંખ મળે, ને સૌને સૌનું આભ,
દશે દિશામાં સ્મિત વહે હો દશે દિશે શુભ-લાભ.

અભણ રહી અજ્ઞાનના શાને, અંધકારને પીવો ?
કહે બુદ્ધ આંબેડકર કહે, તું થા તારો દીવો;
શારદીય અજવાળા પહોંચ્યાં ગુર્જર ગામે ગામ
ધ્રુવ તારકની જેમ ઝળહળે એકલવ્યની શાન.

સરસ્વતીના મયૂર તમારે ફળિયે આવી ગહેકે
અંધકારને હડસેલીને ઉજાસના ફૂલ મહેંકે;
બંધન નહીં કો સ્થાન સમયના જવું ન ઘરથી દૂર
ઘર આવી મા હરે શારદા દૈન્ય તિમિરના પૂર.

સંસ્કારોની સુગંધ મહેંકે, મન મંદિરને ધામે
સુખની ટપાલ પહોંચે સૌને પોતાને સરનામે;
સમાજ કેરે દરિયે હાંકી શિક્ષણ કેરું વહાણ,
આવો કરીયે આપણ સૌ
ભવ્ય રાષ્ટ્ર નિર્માણ...
દિવ્ય રાષ્ટ્ર નિર્માણ...
ભવ્ય રાષ્ટ્ર નિર્માણ

DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY
(Established by Government of Gujarat)
'Jyotirmay' Parisar,
Sarkhej-Gandhinagar Highway, Chharodi, Ahmedabad-382 481
Website : www.baou.edu.in

978-81-945801-9-5