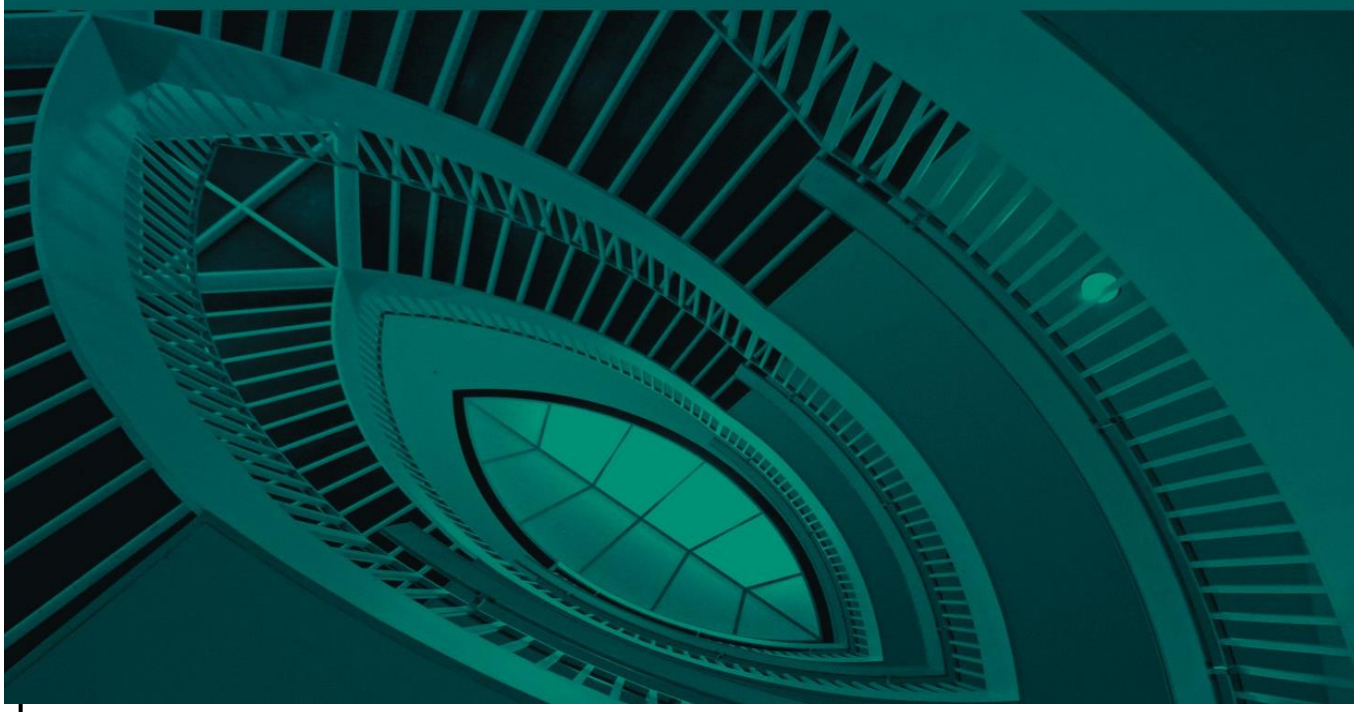
Karnataka State Open University
Mukthagangotri, Mysore-570006

M.Sc. CYBER SECURITY

Second Semester

Computer Networks



COMPUTER NETWORKS

COURSE BLOCK –1

Preface

With clear, straightforward text and engaging examples, this book brings an active style of learning to the study of computer networking. It can be used as a primary textbook to accompany lecture material or as a companion text to provide hands-on assignments. It is also an ideal guide to self-study for the computing professional. In fact, this book can help any interested readers look under the hood of the network they use every day and become a more informed network consumer.

The book consists of a set of exercises, each of which involves analyzing traces of actual network activity. Important concepts are presented in the context of actual traces of real-world scenarios. Readers learn the details of networking protocols in the best ways possible—by seeing them in action!

Well-chosen examples make it clear how the details of networking protocols are relevant to everyday life. For example, security issues are highlighted throughout the book. Readers will see what is sent over the network when they browse the web or shop online. They will see what a home wireless network looks like to someone driving by if WEP is not enabled. These and many more concrete illustrations help readers understand how to secure their networks against attack.

Anywhere people are learning about computer networking, this book will help them learn by doing rather than simply hearing information. The material contained in this book has been used Master's level courses

UNIT–I: INTRODUCTION TO COMPUTER NETWORKS

Structure

1.0 OBJECTIVES

After going through this lesson you will be able to

- Discuss basics of computer networks
- Describe components of computer networks
- Elucidate direction of data flow
- Discuss networks
- Explain network criteria

1.1 INTRODUCTION

A computer network is a collection of two or more computer systems that are linked together. A network connection can be established using either cable or wireless media. Hardware and software are used to connect computers and tools in any network.

A computer network consists of various kinds of nodes. Servers, networking hardware, personal computers, and other specialized or general-purpose hosts can all be nodes in a computer network. Hostnames and network addresses are used to identify them.

1.2 BASICS OFCOMPUTERNETWORKS

The term 'Network' means a group, chain or a collection of something that come together for the purpose of communication. In computer's reference – the same definition holds value but there is a slight change which is –A network is a group of related computers that exchange resources, files and possess some kind of communications within themselves.

The communication word in this reference means 'DATA'. Since these activities are going in between the computers they are called as Computer Networks.

Definition: A computer network is a group of devices connected with each other through a transmission medium such as wires, cables etc. These devices can be computers, printers, scanners, Fax machines etc. The purpose of having computer network is to send and receive data stored in other devices over the network. These devices are often referred as nodes.

ADVANTAGES

Many organizations. already have a substantial number of computers,often located far apart. For example, a company with many offices may have acomputerateachlocationtokeeptrackofcustomerorders,monitorsales,anddo the local payroll. Previously, each of these computers may have worked inisolation from others but at some point, management decided to connect themtogetherinformationaboutentirecompany.Ingeneral,wecanrefertoitas.

ResourceSharing:

Theaimistomakeallprograms,dataandperipheralsavailabletoanyoneonthenetworkirrespectiveof thephysicallocationoftheresourcesand theuser.

Reliability: Afilecanhavecopiesontwoorthreedifferentmachines,so if one of them is unavailable (hardware crash), the other copies could beused. For military, banking, air reservation and many other applications it is ofgreat importance.

Cost Factor: Personal computers have better price/performance

ratiothanmicrocomputers.Soitisbetter tohavePC's,oneperuser,withdatastoredon onesharedfileservermachine.

CommunicationMedium:Usinganetwork,itispossibleformanagers,workingfarapart,toprepare financialreportofthecompany.Thechangesatoneendcanbeimmediatelynoticedatanotherandhenc eitspeedsup co-operationamong them.

ELEMENTARYTERMINOLOGYOFNETWORKS

Itissometimetolearnaboutthecomponents/termsmostlyusedinnetworking.Whenever wetalk aboutanetwork itincludes thehardwareandthe software that make up the network. Now let us have a look at some typicalhardwarecomponentsofnetwork.

Nodes(Workstations)

Thetermnodesrefertothecomputersthatareattachedtoanetworkandareseekingtosharetheresource softhenetwork.Ofcourse,iftherewerenonodes(alsocalledworkstations),therewouldbenonetwork atall.

A computer becomes a workstation of a network as soon as it is attachedtoanetwork.

Server

Def: A computer that facilitates "the sharing of data" software" and hardware - resources(e.g."printer's"modemsetc,)onthenetwork"istermedasaSERVER.

On small networks, sometimes, all the shareable stuff (like files, data,software etc.) is stored on the server. A network can have more than one serveralso. Each server has a unique name on the network and all users of networkidentifytheserverbyitsuniquename.Serverscanbeoftwotypes:non-dedicatedanddedicatedservers.

Non-dedicatedServers: Onsmallnetworks,aworkstationthatcandoubleupasaserver,isknownasnon -dedicatedserversinceitisnot completely dedicated to the cause of serving. Such servers can facilitate theresource-sharing among workstations on a proportionately smaller scale. Sinceone computer works as a workstation as well as a server, it is. slower andrequires. more memory. The (small) networks using such a server are known aspeer-to-peernetworks.

DedicatedServers: Onbiggernetworkinstallations,thereisacomputerreservedforserver'sjoba nditsonlyjobistohelpworkstationsaccessdata,softwareandhardwareresources.Itdoesnotdoubl

e-
upasaworkstationandsuchaserverisknownasdedicatedserver.Thenetworksusingsuchaservera reknownasmaster-slavenetworks.

On a network, there may be several servers that allow workstations toshare specific resources. For example, there may be a server exc1usivelyforservingfiles-relatedrequestslikestoringfiles,decidingabouttheiraccessprivilegesandregulatingtheamounto fspaceallowedforeachuser.Thisserverisknownasfileserver.Similarly,theremaybeprinterserve randmodem server. The printer server takes care of the printing requirements of anumberofworkstationsandthemodemserverhelpsagroupofnetworkusersuseamodemtotrans mitlongdistancemessages.

NetworkInterfaceUnit(NIU)

Def: A NETWORK INTERFACE UNIT is an interpreter that helps to establishcommunicationbetweentheserverandworkstations.

Astandalonecomputer(acomputerthatisnotattachedtoanetwork)livesinitsownworldandcarrie soutitstaskswithitsowninbuiltresources.Butassoonasitbecomesaworkstation,itneedsaninterf acetohelpestablisha connection with the network because without this, the workstations will not beable tosharenetwork resources.

The network-interface-unit is a device that is attached to each of theworkstations and the server, and helps the workstation toestablish the all-importantconnectionwiththenetwork.Eachnetwork-interface-unitthatisattached to a workstation has a unique number identifying it which is known asthenodeaddress.TheNIUisalsocalledTerminalAccessPoint(TAP).Differentmanufacturersha vedifferentnamesfortheinterface.

Computernetworkscanbeusedfornumerousservices,bothforcompanies and for individuals. For companies, networks of personal computersusing shared servers often provide access to corporate information. Typically,theyfollowtheclient-servermodel,withclientworkstationsonemployeedesktopsaccessingpowerfulserversinthemac hineroom.Forindividuals,networks offer access to a variety of information and entertainment resources.IndividualsoftenaccesstheInternetbycallingupanISPusingamodem,although increasingly many people have a fixed connection at home. An up-and-coming area is wireless networking with new application such as mobile e-mailaccessandm-commerce.

Applications&UsesofNetworks

In the short time they have been around, data communication networkshave become an indispensable partof business, industry, and entertainment.Someofthenetworkapplicationsindifferentfieldsarethefollowing:

Marketing and sales. Computer networks are used extensively in bothmarketing and sales organizations. Marketing professionals use them to collect,exchange,andanalyzedatarelatingtocustomerneedsandproduct development cycles. Sales applications include teleshopping, which uses order-entry computers or telephones connected to an order-processing network, andon-linereservationservicesforhotels,airlines,andsoon.

Financial services. Today's financial services are totally dependent oncomputernetworks.Applicationsincludecredithistorysearches,foreignexchange and investment services, and electronic funds transfer (EFT), whichallows a user, to transfer money without going into a bank (an automated tellermachine is a kind of electronic funds transfer; automatic paycheck deposit isanother).

Manufacturing. Computer networks are used today in, many aspects ofmanufacturing,includingthemanufacturingprocessitself.Twoapplicationsthat usenetworks to provideessentialservicesare computer-assisted design(CAD)andcomputer-assistedmanufacturing(CAM),bothofwhichallowmultipleusers toworkon aprojectsimultaneously.

Electronicmessaging:Probablythemostwidelyusednetworkapplicationiselectronicmail(e-mail).

Directoryservices: Directoryservicesallowlistsoffilestobestoredinacentrallocationtospeedworldwidesearchoperations.

Informationservices: Networkinformationservicesincludebulletinboardsanddatabanks.AWorldWideWebsiteofferingthetechnicalspecificationsforanewproductisaninformationservice.

Electronic data interchange (EDI): EDI allows business information(including documents such as purchase orders and invoices) to be transferredwithoutusing paper.

Teleconferencing: Teleconferencing allows conferences to occurwithouttheparticipantsbeinginthesameplace.Applicationsincludesimpletextconferencing(whereparticipantscommunicatethroughtheirkeyboardsand computer monitors). voice conferencing (where participants at a number oflocations communicate simultaneously over the phone) and video conferencing(whereparticipantscanseeaswellastalktooneanother).

Cellulartelephone: Inthepasttwopartieswishingtousetheservicesof the telephone company had to be linked by a fixed physical connection.Today'scellularnetworksmakeitpossibletomaintainwirelessphoneconnectionseven whiletravelingoverlargedistances.

Cable television: Future services provided by cable television networksmay include video on request, as well as the same information, financial, andcommunications services currently provided by the telephone companies andcomputernetworks.

History(Development)ofComputerNetworks

Eachofthepastthreecenturieshasbeendominatedbyasingletechnology.The18thcenturywastheer aofthegreatmechanicalsystemsaccompanying the Industrial Revolution. The 19th century was the age' of thesteam engine. During the 20th century, the key technology was informationgathering, processing, and distribution. Among other developments, we saw theinstallationofworldwidetelephonenetworks,theinventionofradioandtelevision,thebirthandu nprecedentedgrowthofthecomputerindustry,andthelaunching ofcommunication satellites.

Asaresultofrapidtechnologicalprogress,theseareasarerapidlyconverging and the differences between collecting, transporting, storing, andprocessinginformationarequicklydisappearing.Organizationswithhundreds of offices spread over a wide geographical area routinely expect to be able toexamine the current status of even their most remote output at the push of abutton. As our ability together, process and distribute information grows, thedemandforevermoresophisticatedinformationprocessinggrowsevenfaster.

Althoughthecomputerindustryisstillyoungcomparedtootherindustries(e.g.,automobilesandairt ransportation),computershavemadespectacularprogressinashorttime.Duringthefirsttwodecade softheirexistence,computersystemswerehighlycentralized,usuallywithinasinglelarge room. Not infrequently, this room had glass walls, through which visitorscould gawk at the great electronic wonder inside. A medium-sized company oruniversity might have had one or two computers, while. large institutions had atmostafewdozens.Theideathatwithintwentyyearsequallypowerfulcomputerssmallerthanpost agestampswouldbemassproducedbythemillionswaspurescience fiction.

Themergingofcomputersandcommunicationshashadaprofoundinfluenceonthewaycomputersyst emsareorganized.Theconceptofthe"computer center" as a room with a large computer to which users bring

theirworkforprocessingisnowtotallyobsolete.Theoldmodelofasinglecomputerservingalloftheorganization'scomputationalneedshasbeenreplacedbyone.inwhichalarge,numberofseparatebutinterconnectedcomputers do the job. These systems are called computer networks. The designandorganizationofthesenetworksarethesubjectsofthisbook.

Throughoutthebookwewillusetheterm"computernetwork"tomeana collection of autonomous computers interconnected by a single technology.Twocomputersaresaidtobeinterconnectediftheyareabletoexchange

information.Theconnectionneednotbeviaacopperwire;fiberoptics,microwaves, infrared, and communication satellites can also be used. Networkscome in many sizes, shapes and forms, as we will see later. Although it maysoundstrangetosomepeople,neithertheInternetnortheWorldWideWebisa computer network. By the end of this book, it should be clear why. The quickanswer is- the Internet is not a single network butanetwork ofnetworks andtheWebisadistributedsystem thatrunsontopoftheInternet.

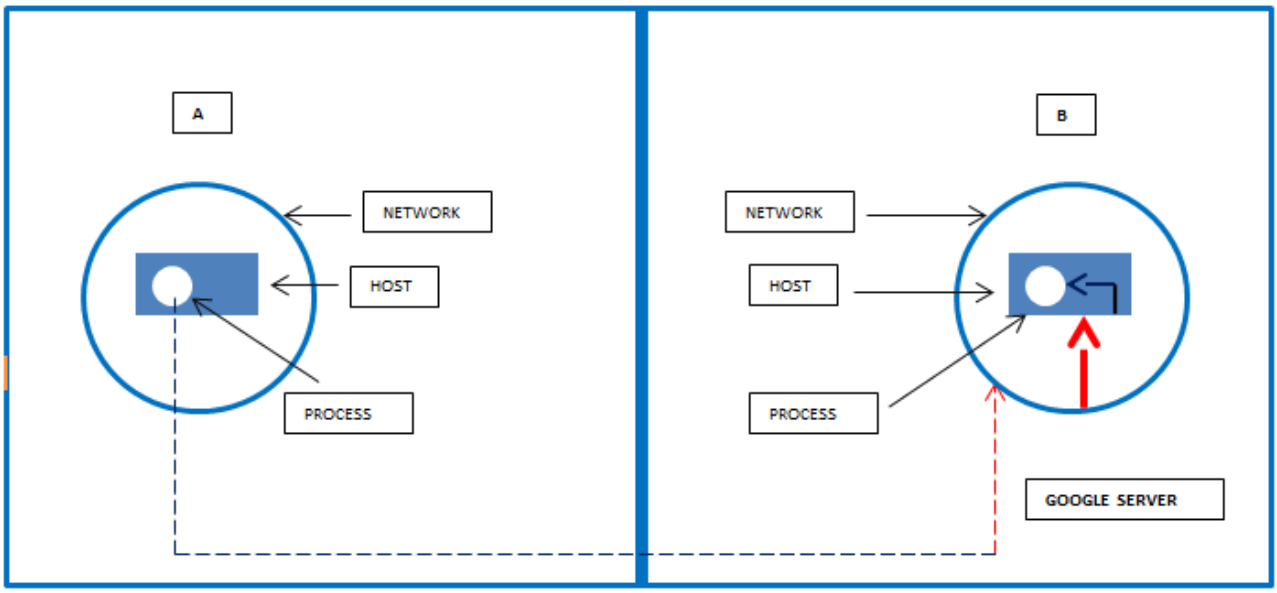
There is considerable confusion in the literature, between a computernetwork and a distributed system. The key distinction is that in a distributedsystem, a collection of independent computers appears to its users as a singlecoherent system. Usually,it has a single model or paradigm thatitpresentstotheusers.Oftenalayerofsoftwareontopoftheoperatingsystem,calledmiddleware, isresponsibleforimplementingthismodel.Awell-knownexample of a distributed system is the World Wide Web, in which everythinglookslikeadocument(Web page).

In a computer network, this coherence, model, and software are absent.Users are exposed to the actual machines, without any attempt by the system tomakethemachineslookandactinacoherentway.Ifthemachineshavedifferent hardware and different operating systems, that is fully visible to theusers.Ifauserwantstorunaprogramonaremotemachine,hethastologontothatmachineandrunit there.

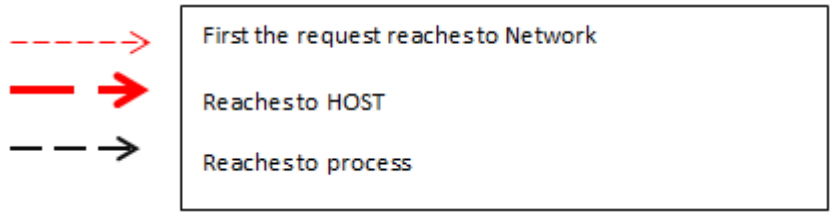
In effect, a distributed system is a software system built on top of anetwork. The software gives it a high degree of cohesiveness and transparency.Thus, the distinction between a network and a distributed system lies with thesoftware(especiallytheoperatingsystem),ratherthanwiththehardware.

Data Communication**:** When we communicate, we are sharing information. This sharing canbe local or remote. Between individuals, local communication usually occurs face to face, whileremotecommunication takesplaceoverdistance.

Let's see an example of a Computer Network for overall understanding, this explanation will make readers understand how things work



Within a network, there is a host (many hosts can be there) and within a host, there is a process (many processes can be there).



So the process is Mr. Ron wants to open www.google.com (domain name) on his web browser. He has to connect to the Google server to get the web page on his system. See the dotted lines that emerge from A and reaches to B (image description is available).

Now with using only the domain name, we have to identify the network, the host and the process which is the entire thing we will see happening.

The domain name (i.e. www.google.com) must be converted to IP address so that it can be understood by the receiving host and networks.

So, IP address has 2 parts

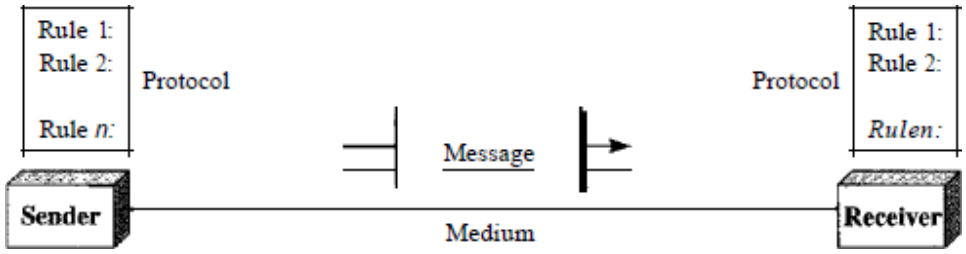
1. HOST ID
2. NETWORK ID.

So using the network ID we can reach the target network and using the Host ID we can reach the Target host. After this, we need Port Number to reach the process. This is how the connection works for web services.

1.3 COMPONENTS OF COMPUTER NETWORK

Components: There are five basic components of a computer network

Adatacommunicationssystemhasfivecomponents.



1. Message.Themessageistheinformation(data)tobecommunicated.Popularformsofinformation include text,numbers,pictures,audio,andvideo.
2. Sender.Thesenderisthedevicethatsendsthedatamessage.Itcanbeacomputer,workstation, telephone handset,videocamera,andso on.
3. Receiver.Thereceiveristhedevicethatreceivesthemessage.Itcanbeacomputer,workstation,telephonehandset,television,andsoon.

4. Transmission medium. The transmission medium is the physical path by which a messagetravels from sender to receiver. Some examples of transmission media include twisted-pair wire,coaxialcable,fiber-opticcable,andradiowaves

5. Protocol.Aprotocolisasetofrulesthatgoverndatacommunications.Itrepresentsanagreement between thecommunicatingdevices.Withoutaprotocol,twodevicesmaybeconnected but not communicating, just as a person speaking French cannot be understood by apersonwho speaks onlyJapanese.

DataRepresentation:

Informationtodaycomesindifferentformssuchastext,numbers,images,audio,andvideo.

Text: In data communications, text is represented as a bit pattern, a sequence of bits (Os or Is).Different sets of bit patterns have been designed to represent text symbols. Each set is called acode,and theprocessofrepresenting symbolsiscalled coding.Today,theprevalentcodingsystem is called Unicode, which uses 32 bits to represent a symbol or character used in anylanguageintheworld.TheAmericanStandardCodeforInformationInterchange(ASCII),developed some decades ago in the United States, now constitutes the first 127 characters inUnicodeandis alsoreferred toasBasicLatin.

Numbers: Numbersarealsorepresentedbybitpatterns.However,acodesuchasASCIIisnotusedto representnumbers;thenumberisdirectlyconvertedtoabinarynumbertosimplifymathematicaloperations.AppendixBdiscussesseveraldifferentnumberingsystems.

Images: Imagesarealsorepresentedbybitpatterns.Initssimplestform,animageiscomposedofa matrixof pixels (picture elements), where each pixel is a small dot. The size of thepixeldepends on the *resolution.* For example, an image can be divided into1000 pixels or 10,000pixels. In the second case, there isa better representation of the image (betterresolution),butmore memory is needed to store the image. After an image is divided into pixels, each pixel isassigned a bit pattern. The size and the value of the pattern depend on the image. For an imagemade of only blackand- white dots (e.g., a chessboard), a I-bit pattern is enough to represent apixel. If an image is notmade of pure white and pure black pixels,you can increase thesize ofthe bit pattern to include gray scale. For example, to show

four levels of gray scale, you can use2-bitpatterns.Ablackpixelcanberepresentedby00,adarkgraypixelby01,alightgraypixelby10,anda whitepixelby11.Thereareseveralmethodstorepresentcolorimages.OnemethodiscalledRGB,soc alledbecauseeachcolorismadeofacombinationofthreeprimarycolors:*red,* green, and blue. The intensity of each color is measured, and a bit pattern is assigned to it.Another method is called YCM, in which a color is made of a combination of three other primarycolors:yellow,cyan,andmagenta.

Audio: Audio refers tothe recording or broadcasting of soundor music. Audio is by naturedifferent from text, numbers, or images.It is continuous, not discrete. Even when we use amicrophone to change voice or music to an electric signal, we create a continuous signal. InChapters4and5,welearnhowtochangesoundormusictoa digitalorananalog signal.

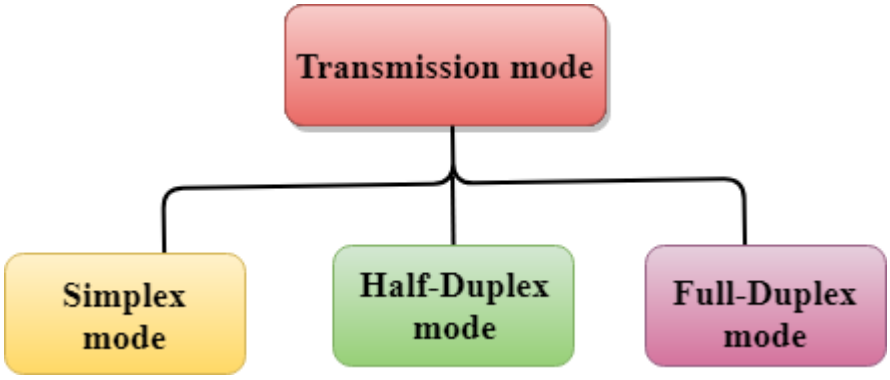
Video: Video refers to the recording or broadcasting of a picture or movie. Video can either beproducedas a continuous entity (e.g., by a TVcamera), or it can be a combination ofimages,each a discrete entity, arranged to convey the idea of motion. Again we can change video to adigitaloran analogsignal.

1.4 DIRECTION OF DATAFLOW

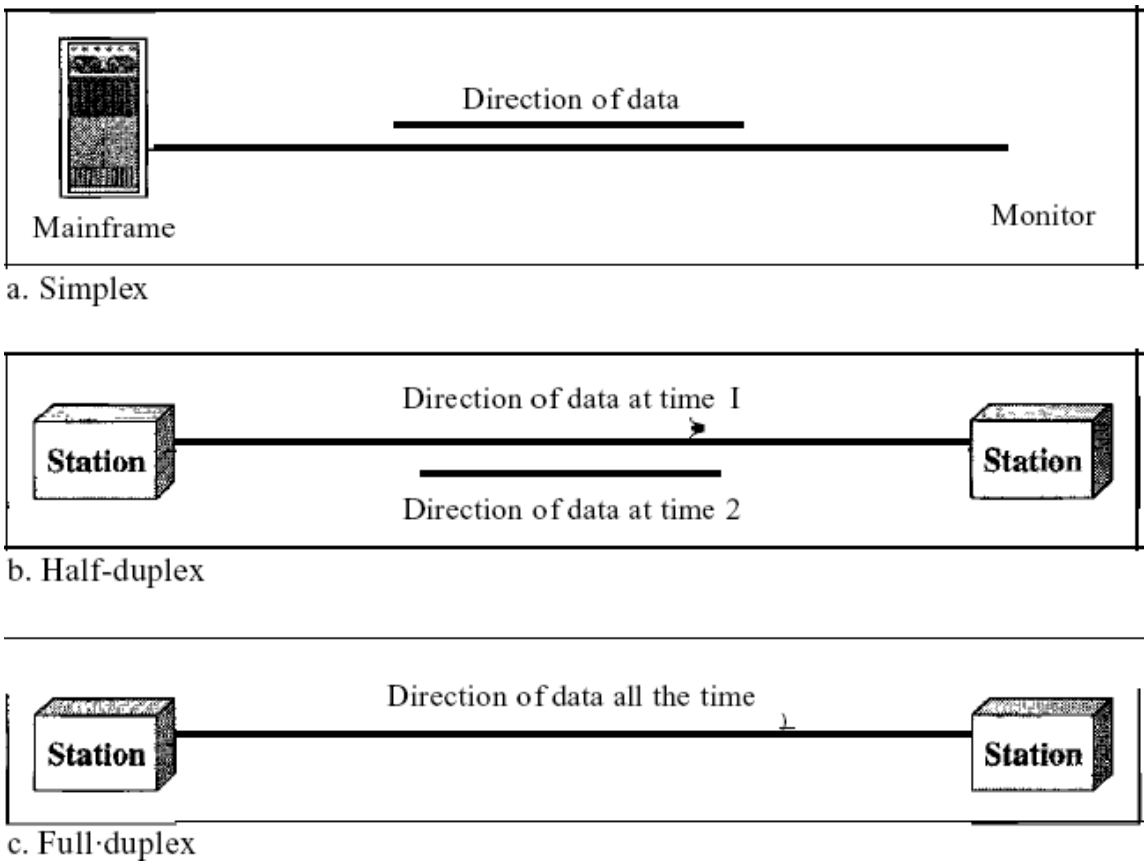
- The way in which data is transmitted from one device to another device is known as **transmission mode**.
- The transmission mode is also known as the communication mode.
- Each communication channel has a direction associated with it, and transmission media provide the direction. Therefore, the transmission mode is also known as a directional mode.
- The transmission mode is defined in the physical layer.

The Transmission mode is divided into three categories:

- Simplex mode
- Half-duplex mode
- Full-duplex mode



Communicationbetweentwodevicescanbesimplex,half-duplex,orfull-duplexasshownin figure:



Simplex:

Insimplexmode, the communicationis unidirectional, as on a one-way street.Only oneof the two devices on a link can transmit; the othercan only receive (see Figurea).

Keyboardsand traditionalmonitorsareexamplesof simplexdevices.The keyboardcan only introduceinput; the monitor can only accept output. The simplex mode can use the entire capacity of thechannel tosend data in onedirection.

Half-Duplex:

In half-duplex mode, each station can both transmit and receive, but not at the same time.When one device is sending, the other can only receive, and vice versa The half-duplex mode islikeaone-laneroadwithtrafficallowedin bothdirections.

When cars are traveling in one direction, cars going the other way must wait. In a half-duplextransmission, the entire capacity of a channel is taken over by whichever of the two devices istransmittingatthetime.Walkie-talkiesandCB(citizensband)radiosarebothhalf-duplexsystems.

Thehalf-duplexmodeisusedincaseswherethereisnoneedforcommunicationinbothdirectionsatthesametime;theentirecapacityofthechannelcanbeutilizedforeachdirection.

Full-Duplex:

In full-duplex both stations can transmit and receive simultaneously (see Figure c). Thefull-duplex mode is like a tW<D-way streetwith trafficflowing in bothdirectionsat the sametime.Infull-duplex mode, si~nalsgoing in one direction share thecapacity of the link:withsignals going in the other din~c~on. This sharing can occur in two ways: Either the link mustcontain two physically separate t:nmsmissiIDn paths, one for sending and the other for receiving;or the capacity of the ch:arilliel is divided between signals traveling in both directions. Onecommon example of full-duplex communication is the telephone network. When two people arecommunicating by a telephone line,bothcan talk andlistenat the same time. The full-duplexmode is used when communication in both directions is required all the time. The capacity of thechannel,however,mustbedividedbetweenthe two directions.

1.5 NETWORKS

A network is a set of devices (often referred to as *nodes)* connected by communication links. Anode can be a computer, printer, or any other device capable of sending and/or receiving datagenerated byothernodeson the network.

DistributedProcessing

Most networks use distributed processing, in which a task is divided among multiple computers.Insteadofonesinglelargemachinebeingresponsibleforallaspectsofaprocess,separatecomputers(usuallya personalcomputerorworkstation)handle asubset.

1.6 NETWORKCRITERIA

A networkmustbe ableto meetacertain number of criteria. Themostimportantofthese areperformance,reliability,andsecurity.

Performance:

Performancecanbemeasuredinmanyways,includingtransittimeandresponsetime. Transit time is the amount of time requiredfor a message to travelfrom one device toanother.Responsetimeistheelapsedtimebetweenaninquiryandaresponse.Theperformance ofanetworkdependsonanumberoffactors,includingthenumberofusers,thetypeoftransmissionmedium,thecapabilitiesoftheconnectedhardware,andtheefficiencyofthesoftware.

Performance is often evaluated by two networking metrics: throughput and delay. Weoften needmore throughputand lessdelay.However, these two criteria are oftencontradictory.If we try to send more data to the network, we may increase throughput but we increase the delaybecauseoftrafficcongestion in the network.

Reliability:

In addition to accuracy of delivery, network reliability is measured by the frequency offailure, the time it takes a link torecover from a failure, and the network'srobustness inacatastrophe.

Security:

Network security issues include protecting data from unauthorized access, protecting datafrom damage and development, and implementing policies and procedures for recovery frombreachesand datalosses.

1.7 SUMMARY

In this unit we have discussed about basics of computer networks. We also explainedcomponents of computer networks and direction of data flow. At the end of this unit reader are able to figure out the concept of networks and network criteria.

1.8 KEYWORDS

Computer networks, Simplex, Half-duplex, Full-duplex, Sender, Receiver, NIU, Server.

1.9 QUESTIONS

1. Define computer networks. Write the advantages of computer networks.
2. Briefly explain direction of data flow.
3. Explain components of computer network.
4. Write a short note on network criteria.
5. Discuss advantages of computer networks.

1.10 REFERENCES

- WilliamStallings,DataandComputerCommunication,PrenticeHallofIndia
- BehrouzA.Forouzan,DataCommunicationandNetworking,McGraw-Hill
- Andrew STanenbaum,ComputerNetworks, PrenticeHall.

UNIT 2: TYPES OF NETWORKS AND REFERENCE MODELS

Structure:

2.0 OBJECTIVES

After going through this lesson you will be able to

- Elucidate Physical structures
- Discuss Categories of network
- Describe Protocols and standards
- Elucidate Reference models such as OSI Reference Model and TCP/IP Reference Model. Also discuss comparative study.

2.1 INTRODUCTION

In this unit we will learn about the different types of networks, their applications and networking models. We will also examine reference models, its various layers and functions of each layer.The networking model describes the architecture, components, and design used to establish communication between the source and destination systems. Aliases for network models include protocol stacks, protocol suites, network stacks, and network protocols. There are 2 predominant models available. Let us take a look at them

1. Open Systems Interconnection (OSI) Model
2. Transmission Control Protocol/Internet Protocol (TCP/IP) Model

2.2 PHYSICALSTRUCTURES

TypeofConnection

A network is two or more devices connected through links. A link is a communicationspathwaythattransfersdatafromonedevicetoanother.Forvisualizationpurposes,itissimplesttoimagineany linkasalinedrawn between twopoints.Forcommunicationtooccur,twodevices must be connected in some way to the same link at the same time. There are two possibletypesofconnections:point-to-point andmultipoint.

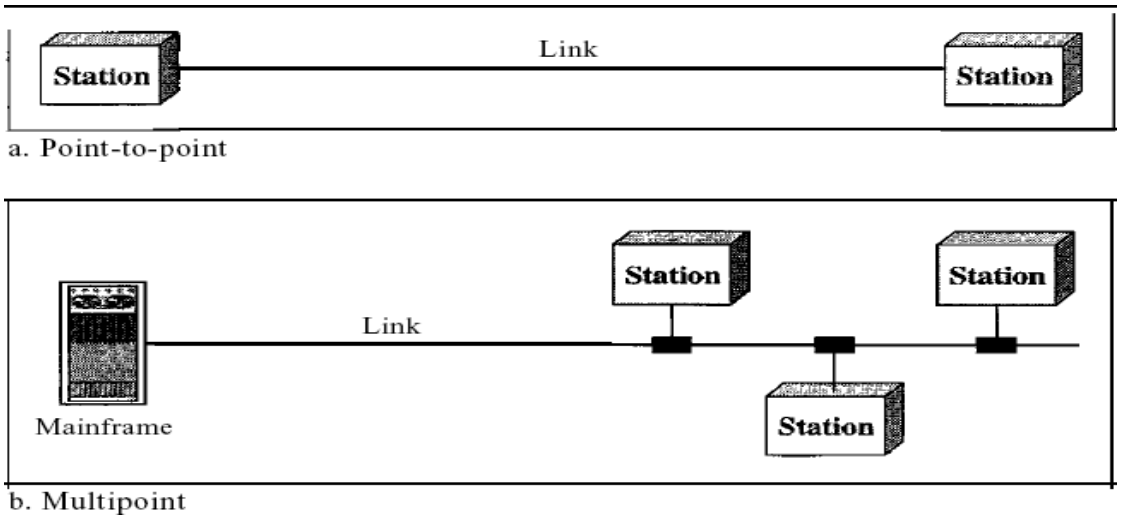
Point-to-Point

A point-to-point connection provides a dedicated link between two devices. The entirecapacity of the link is reserved for transmission between those two devices. Most point-to-pointconnectionsuseanactuallengthofwireorcabletoconnectthetwoends,butotheroptions,suchasmicrowaveorsatellitelinks,arealsopossible.Whenyouchangetelevisionchannelsbyinfrared remote control,you are establishing apoint-to-point connection between the remotecontroland thetelevision'scontrolsystem.

Multipoint

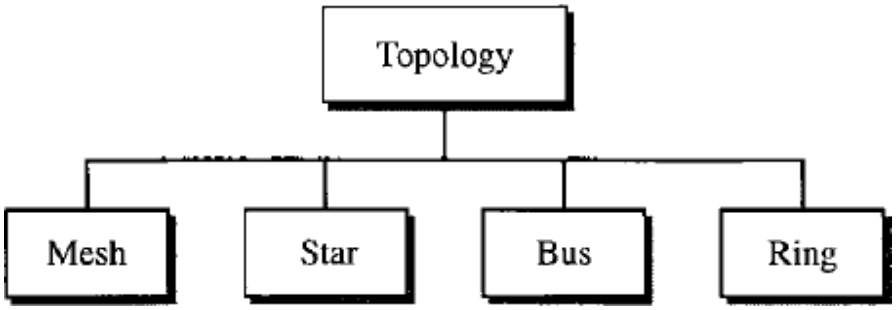
A multipoint (also called multidrop) connection is one in which more than two specificdevices share a single link. In a multipoint environment, the capacity of the channel is shared,either spatiallyor temporally. If several devices can use the link

simultaneously, it is a *spatiallyshared*connection.Ifusersmusttaketurns,itisa*timeshared*connection.



PhysicalTopology

The term *physical topology* refers to the way inwhich a network is laid out physically. One ormore devices connect to a link; two or more links form a topology. The topology of a network isthegeometricrepresentationoftherelationshipofallthelinks andlinking devices(usuallycallednodes)tooneanother.Therearefourbasictopologiespossible:mesh,star, bus,andring

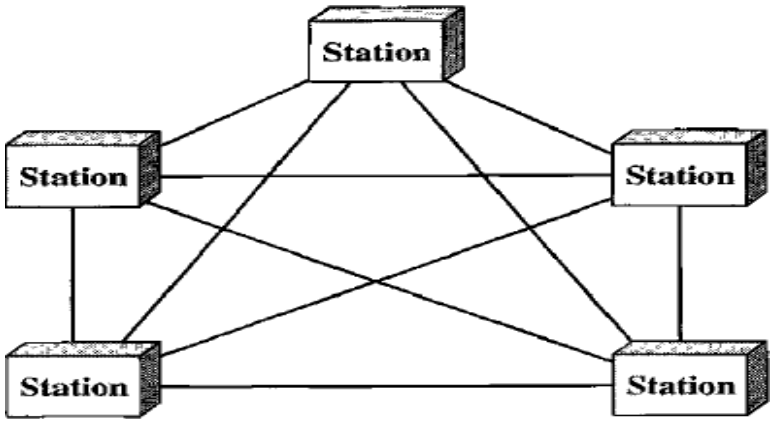


Mesh: Inameshtopology,every device hasadedicatedpoint-to-pointlink toevery otherdevice. The term *dedicated* means that the link carries traffic only between the two devices

itconnects.Tofindthenumberofphysicallinksinafullyconnectedmeshnetworkwith*n*nodes,wefirstconsiderthateachnodemustbeconnectedtoeveryothernode.Node1mustbeconnected to *n* - I nodes, node 2 must be connected to *n* – 1 node, and finally node *n* must beconnected to *n* - 1 nodes. We need *n(n* - 1) physical links. However, if each physical link allowscommunication in bothdirections(duplexmode),wecan divide the number of linksby 2.Inotherwords,wecansaythatinameshtopology,weneed*n* *(n*-1) /2duplex-modelinks.

Toaccommodatethatmanylinks,everydeviceonthenetworkmusthave*n*–1input/output

(VO) portstobeconnectedtotheother*n*- 1stations.



Advantages:

1. The use of dedicatedlinksguarantees thateachconnection can carry itsown data load,thuseliminatingthetrafficproblemsthatcanoccurwhenlinksmustbesharedbymultipledevices.
2. Amesh topology isrobust.If one link becomesunusable, it doesnotincapacitate theentire system. Third, there is the advantage of privacy or security. When every messagetravels along a dedicated line, only the intended recipient sees it. Physical boundariesprevent other users from gaining access to messages. Finally, point-to-point links makefault identificationand fault isolation easy. Traffic can be routed to avoid links withsuspected problems. This facility enables the network manager to discover the preciselocation ofthe fault andaidsinfindingitscauseandsolution.

Disadvantages:

1. Disadvantageofamesharerelatedtotheamountofcablingbecauseeverydevicemustbe

connectedtoeveryotherdevice,installationandreconnectionaredifficult.

2. Second, the sheer bulk of the wiring can be greater than the available space (in walls,ceilings, or floors) can accommodate. Finally, the hardware required to connect each link(I/Oportsandcable)canbe prohibitivelyexpensive.

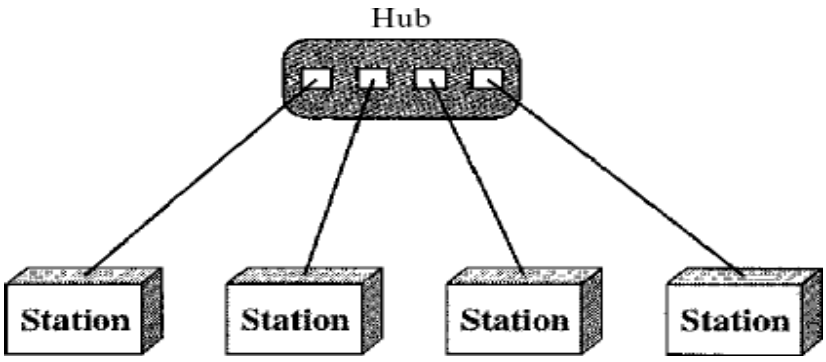
For these reasons a mesh topology is usually implemented in a limited fashion, for example, as abackbone connecting the main computers of ahybridnetwork that caninclude several othertopologies.

StarTopology:

Inastar topology,eachdevice hasadedicatedpoint-to-point link only toacentralcontroller, usually called a hub. The devices are not directly linked to one another. Unlike a meshtopology, a star topology does not allow direct traffic between devices. The controller acts as anexchange: If one device wants to send data toanother, it sends the data to the controller, whichthenrelaysthe datatotheotherconnected device.

A star topology is less expensive than a mesh topology. In a star, each device needs only one linkand one I/O port to connect it to any number ofothers. Thisfactor alsomakes it easy to installand reconfigure. Far less cabling needs to be housed, and additions, moves, and deletions involveonlyoneconnection:betweenthatdeviceandthehub.

Other advantages include robustness. If one link fails, only that link is affected. All other linksremainactive.Thisfactoralsolendsitselftoeasyfaultidentificationandfaultisolation.Aslo ngasthehubisworking,itcanbeusedtomonitorlinkproblemsandbypassdefectivelinks.

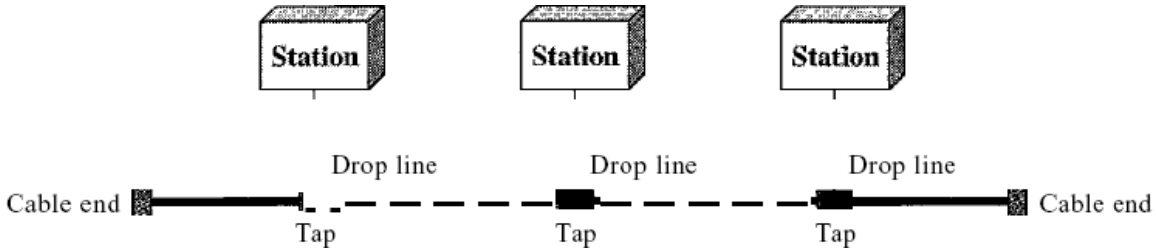


One big disadvantage of a star topology is the dependency of the whole topology on one

singlepoint, the hub. If the hub goes down, the whole system is dead. Although a star requires far lesscablethanamesh,eachnodemustbelinkedtoacentralhub.Forthisreason,oftenmorecabling isrequiredinastarthaninsome othertopologies(such asringorbus).

BusTopology:

The preceding examples all describe point-to-point connections. A **bus topology,** on theotherhand,ismultipoint.Onelongcableactsasa**backbone**tolinkallthedevicesinanetwork



Nodes are connected to the bus cable by drop lines and taps. A drop line is a connectionrunning between the device and the main cable. A tap is a connector that either splices into themain cable or punctures the sheathing of a cable to create a contact with the metallic core. As asignal travels along the backbone, some of its energy is transformed into heat. Therefore, itbecomes weaker and weaker as it travels farther and farther. For this reason there is a limit on thenumberoftapsabuscansupportandonthe distance betweenthose taps.

Advantages of a bus topology include ease of installation. Backbone cable can be laid along themost efficient path, then connected to the nodes by drop lines of variouslengths.In this way, abus uses less cabling than mesh or star topologies. In a star, for example, four network devices inthe same room require four lengths of cable reaching all the way to the hub. In a bus, thisredundancy is eliminated.Only the backbonecablestretches through theentire facility.Eachdrop line hastoreachonlyasfarasthenearestpointonthebackbone.

Disadvantages include difficult reconnection and fault isolation. A bus is usually designed to beoptimallyefficientatinstallation.Itcanthereforebedifficulttoaddnewdevices.Signalreflecti on at the taps can cause degradation in quality. This degradation can be controlled

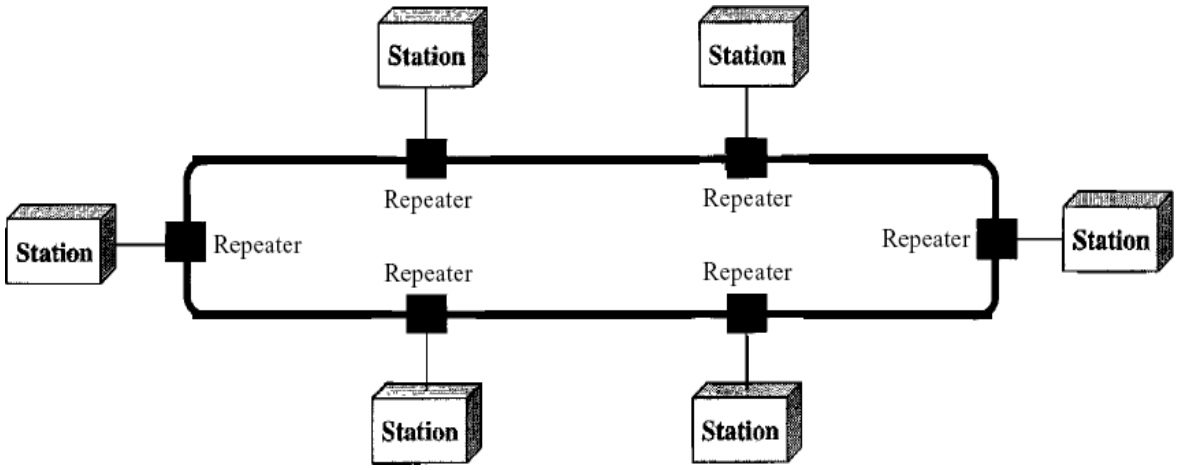
bylimiting the number and spacing of devices connected to a given length of cable. Adding newdevicesmaythereforerequiremodificationorreplacementofthe backbone.

In addition, a fault or break in the bus cable stops all transmission, even between devices on thesame side of the problem. The damaged area reflects signals back in the direction of origin,creatingnoisein bothdirections.

Bus topology was the one of the first topologies used in the design of early local area networks.EthernetLANscan use abus topology,buttheyarelesspopular.

RingTopology

Inaringtopology,eachdevicehasadedicatedpoint-to-pointconnectionwithonlythetwodevicesoneithersideofit.Asignalispassedalongtheringinonedirection,fromdevice todevice,untilitreachesitsdestination.Eachdeviceintheringincorporatesarepeater.Whenadevicereceivesasignalintendedforanotherdevice,itsrepeaterregeneratesthebitsandpassesthem along



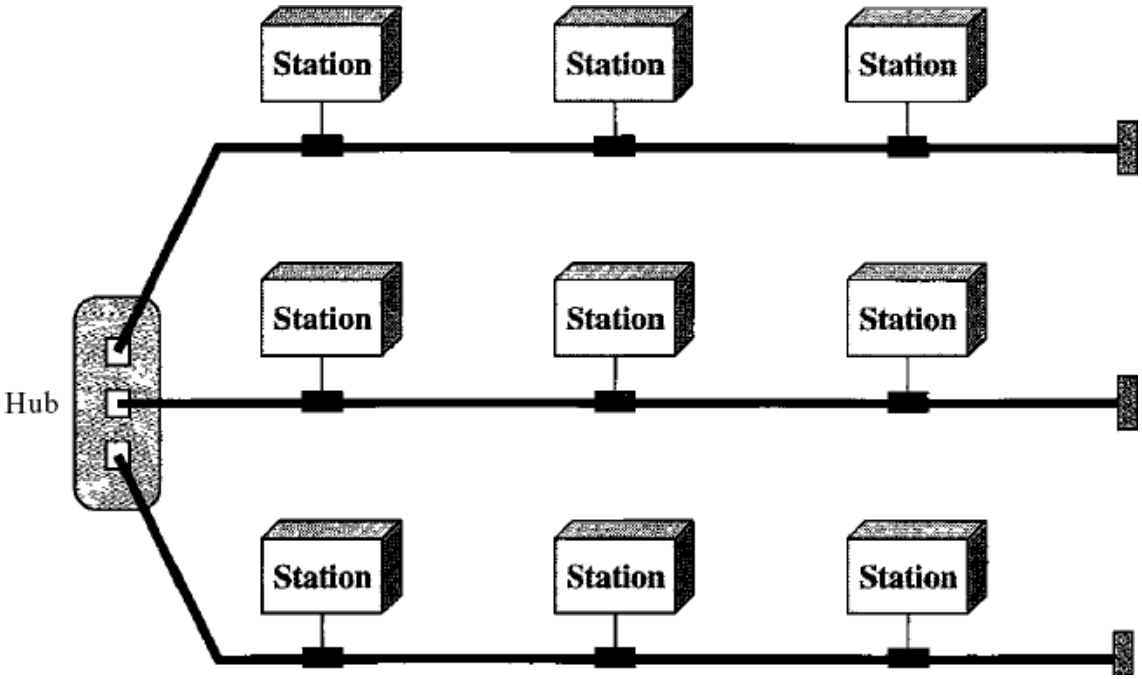
A ring is relatively easy to install and reconfigure. Each device is linked to only its immediateneighbors (either physically or logically). To add or delete a device requires changing only twoconnections. The only constraints are media and traffic considerations (maximum ring length andnumber of devices).

In addition, fault isolation is simplified. Generally in a ring, a signal iscirculating at all times. If one device doesnotreceive a signalwithin a specified period, it canissue analarm.Thealarm alertsthenetwork operatortotheproblemanditslocation.

However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring(suchasadisabledstation)candisabletheentirenetwork.Thisweaknesscanbesolvedby usinga dual ring or a switch capable of closing off the break. Ring topology was prevalent when IBMintroduced its local-area network Token Ring.

Today, the need for higher-speed LANs has madethistopologylesspopular.HybridTopology

Anetworkcanbehybrid.Forexample,wecanhavea main star topology with each branch connecting several stations in a bus topology as shown inFigure



2.3: CATEGORIES OF NETWORKS

LocalAreaNetworks:

Localareanetworks,generallycalledLANs,areprivately-ownednetworkswithinasinglebuilding or campus of up to a few kilometers in size. They are widely used to connect personalcomputers and workstations in company officesand factories toshare resources(e.g.,

printers)andexchangeinformation.LANsaredistinguishedfromotherkindsofnetworksbythre echaracteristics:

(1) Theirsize,

(2) Theirtransmissiontechnology,and

(3) Theirtopology.

LANs are restricted in size, which means that the worst-case transmission time is bounded andknown inadvance.Knowing this boundmakesit possible to use certainkinds ofdesigns thatwouldnototherwisebepossible.Italsosimplifiesnetworkmanagement.LANsmay useatransmission technology consisting of a cable to which all the machines are attached, like thetelephone company party lines once used in rural areas. TraditionalLANs run at speeds of 10Mbps to 100 Mbps, have low delay (microseconds or nanoseconds), and make very few errors.Newer LANs operate at up to 10 Gbps Various topologies are possible for broadcast LANs.Figure1 shows two of them. In a bus (i.e., a linear cable) network, at any instant at most onemachine is the master and is allowed to transmit. All other machines are required to refrain fromsending. Anarbitrationmechanism is needed to resolve conflictswhentwo or more machineswant to transmit simultaneously. The arbitration mechanism may be centralized or distributed.IEEE802.3,popularlycalledEthernet,forexample,isabus-basedbroadcastnetworkwithdecentralized control, usually operating at 10 Mbps to 10 Gbps. Computers on an Ethernet cantransmitwheneverthey wantto;iftwoormorepacketscollide,eachcomputerjustwaitsarandom time and tries again later.

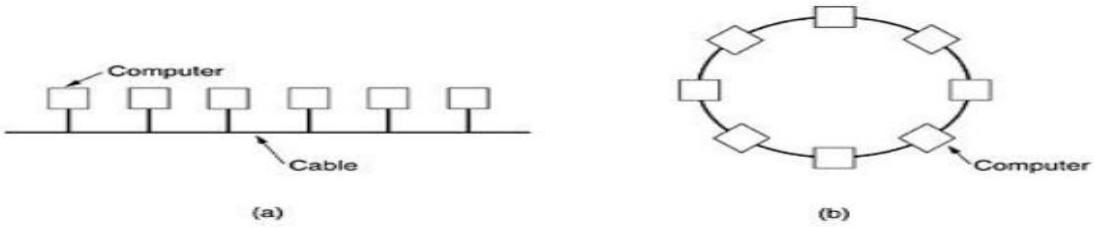


Fig.1:Twobroadcastnetworks.(a)Bus.(b)Ring.

A second type of broadcastsystem isthe ring.Ina ring, each bitpropagates around onits own,not waiting for the rest of the packet to which it belongs. Typically, each bit

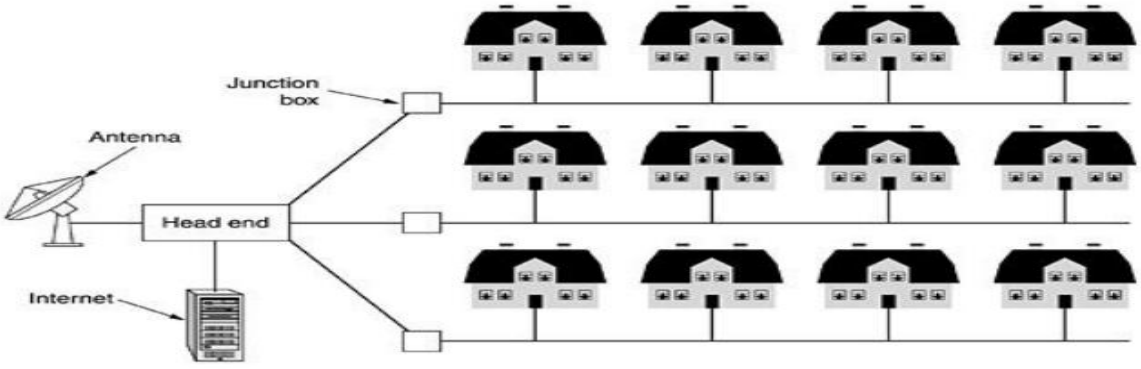
circumnavigates theentire ring in the time it takes to transmit a few bits, often before thecomplete packet has evenbeentransmitted.Aswithallotherbroadcastsystems,someruleisneededforarbitratingsimultaneousaccessestothering.Variousmethods,suchashavingthemachinestaketurns,areinuse. IEEE802.5(theIBMtokenring),isaring-basedLANoperatingat4and16Mbps.FDDIisanotherexampleofaringnetwork.

MetropolitanAreaNetwork(MAN):

MetropolitanAreaNetwork:

A metropolitan area network, or MAN, covers a city. The best-known example of a MAN is thecable television network available in many cities. This system grewfrom earliercommunityantennasystemsusedinareaswithpoorover-the-airtelevisionreception.Intheseearlysystems,a large antenna was placed on top of a nearby hill and signal was then piped to the subscribers'houses.Atfirst,thesewere locally-designed,adhoc systems.Then companies beganjumpinginto the business, getting contracts from city governments to wire up an entire city. The next stepwastelevisionprogrammingandevenentirechannelsdesignedforcableonly.Oftenthesechannelswerehighlyspecialized,suchasallnews,allsports,allcooking,allgardening,andsoon.

But from their inception until the late 1990s, they were intended for television reception only.To a first approximation, a MAN might look something like the systemshown inFig. Inthisfigure both television signals and Internet are fed into the centralized head end for subsequentdistribution to people's homes. Cable television is not the only MAN. Recent



developments inhigh-speed wireless Internet access resulted in another MAN,which has been standardized asIEEE802.16.

Fig.2:MetropolitanareanetworkbasedoncableTV.

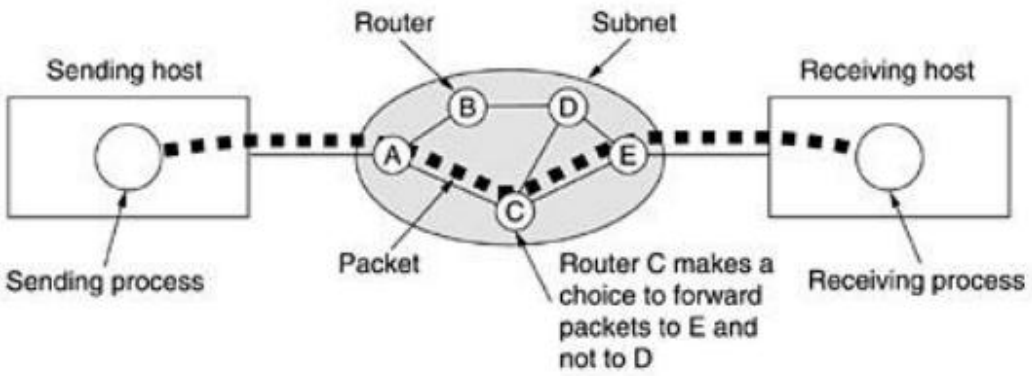
A MAN is implemented by a standard called DQDB (Distributed Queue Dual

Bus) orIEEE 802.16. DQDB has two unidirectional buses (or cables) to which all the computers areattached.

Wide Area Network (WAN).

WideAreaNetwork: A wide area network, or WAN, spans a large geographical area, often a country or continent. Itcontains a collection of machines intended for running user (i.e., application) programs. Thesemachines are called as hosts. The hosts are connected by a communication subnet, or just subnetfor short. The hosts are owned by the customers (e.g., people's personal computers), whereas thecommunicationsubnetistypically ownedandoperatedbyatelephonecompany orInternetservice provider.Thejobofthesubnetistocarry messagesfromhosttohost,justasthetelephonesystemcarrieswordsfromspeakertolistener. Separationofthepurecommunicationaspectsofthenetwork(thesubnet)fromtheapplicationas pects(thehosts),greatlysimplifiesthecompletenetworkdesign.Inmostwideareanetworks,the subnetconsistsoftwodistinctcomponents:transmissionlinesandswitchingelements.Transmi ssionlinesmovebitsbetweenmachines.Theycanbemadeofcopperwire,opticalfiber,orevenra diolinks.InmostWANs,thenetworkcontainsnumeroustransmissionlines,eachoneconnectin gapairofrouters.Iftworoutersthatdonotshareatransmissionlinewishtocommunicate,theymu stdothisindirectly,viaotherrouters.Whenapacketissentfromoneroutertoanotherviaoneormo reintermediaterouters,thepacketisreceivedateachintermediaterouterinitsentirety,storedther euntiltherequiredoutputlineisfree,andthenforwarded.Asubnetorganizedaccordingtothispri ncipleiscalledastore-and-forwardorpacket-switchedsubnet.Nearlyallwideareanetworks(exceptthoseusingsatellites)havestore-and-forwardsubnets.Whenthepacketsare smallandallthesamesize,theyare oftencalledcells. Theprincipleofapacket-switchedWANissoimportant.Generally,whenaprocessonsomehost has a message to be sent to a process on some other host, the sending host first cuts themessage intopackets,eachone bearing itsnumberinthe sequence.These packetsaretheninjectedintothenetworkoneatatimeinquicksuccession.Thepacketsaretranspo rtedindividually over thenetwork and deposited atthe receiving host,wherethey arereassembledinto the original message and delivered to thereceiving process.A stream of packetsresultingfrom someinitialmessageis illustrated inFig.

In thisfigure, all the packets followthe routeACE,rather thanABDE orACDE.Insomenetworks all packets from a given message must follow the same route; in others each packed isroutedseparately.Ofcourse,ifACEisthebestroute,allpacketsmaybesentalongit,evenifeach



packetis individuallyrouted.

Fig.3.1:Astreamofpacketsfromsendertoreceiver.

Not all WANs are packet switched. A second possibility for a WAN is a satellite system. Eachrouter has an antenna through which it can send and receive. All routers can hear the output fromthesatellite,andinsomecasesthey canalsohear theupwardtransmissionsoftheirfellowrouters to the satellite as well. Sometimes the routers are connected to a substantial point-to-pointsubnet,with only someofthemhaving asatelliteantenna.Satellitenetworksare inherentlybroadcastandaremostusefulwhenthebroadcastpropertyis important.

THEINTERNET

The Internet has revolutionized many aspects of our daily lives. It has affected the way we dobusiness as well as the way we spend our leisure time. Count the ways you've used the Internetrecently. Perhapsyou've sent electronic mail (e-mail) to a business associate, paid a utility bill,read a newspaper froma distant city, or lookedup a localmovie schedule-all by using theInternet. Or maybe you researched a medical topic, booked a hotel reservation, chatted with afellow Trekkie, or comparison-shoppedfor acar. TheInternet is acommunication system thathasbroughtawealthofinformationtoourfingertipsandorganizeditforouruse.

ABriefHistory

A network is a group of connected communicating devices such as computers and printers. Aninternet (note the lowercase letter i) is two or more networks that can communicatewith eachother. The most notable internet is called the Internet (uppercase letter I), a collaboration of morethan hundreds of thousands of interconnected networks. Private individuals as well as variousorganizationssuchasgovernmentagencies,schools,researchfacilities,corporations,andlibrariesinmore than 100 countriesusetheInternet.Millions of people are users.Yet thisextraordinarycommunicationsystemonlycame intobeingin1969.

Inthemid-1960s,mainframecomputersinresearchorganizationswerestandalonedevices.Computers from different manufacturers were unable to communicatewith one another. TheAdvancedResearchProjectsAgency(ARPA)intheDepartmentofDefense(DoD)wasinterested in finding a way to connect computers so that the researchers they funded could sharetheirfindings,therebyreducing costsandeliminatingduplicationofeffort.

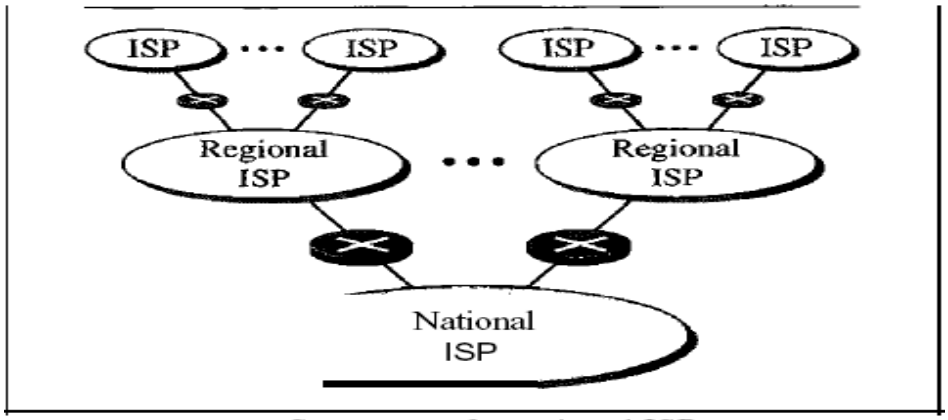
In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideasfor ARPANET, a small network of connected computers. The idea was that each host computer(notnecessarily fromthesamemanufacturer)wouldbeattachedtoaspecializedcomputer,called an *inteiface message processor*(IMP). The IMPs, in tum, would be connected to oneanother. EachIMP had to be able to communicatewith other IMPs aswell as with its ownattached host.By 1969,ARPANET was areality. Four nodes, at the University of California atLos Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford ResearchInstitute (SRI), and the University of Utah, were connected via the IMPs to form a network.Softwarecalledthe*NetworkControlProtocol*(NCP)providedcommunicationbetweenthehosts.

In1972,Vint Cerf andBobKahn, bothofwhomwere part of the core ARPANETgroup,collaborated on what they called the *Internetting Projec1*. Cerf and Kahn's landmark 1973 paperoutlined the protocols to achieve end-to-end delivery of packets. This paper on TransmissionControlProtocol(TCP)includedconceptssuchasencapsulation,thedatagram,andthefunctionsof a gateway. Shortly thereafter, authorities made a decision to split TCP into two protocols:TransmissionControlProtocol(TCP)andInternetworkingProtocol(lP).IPwouldha

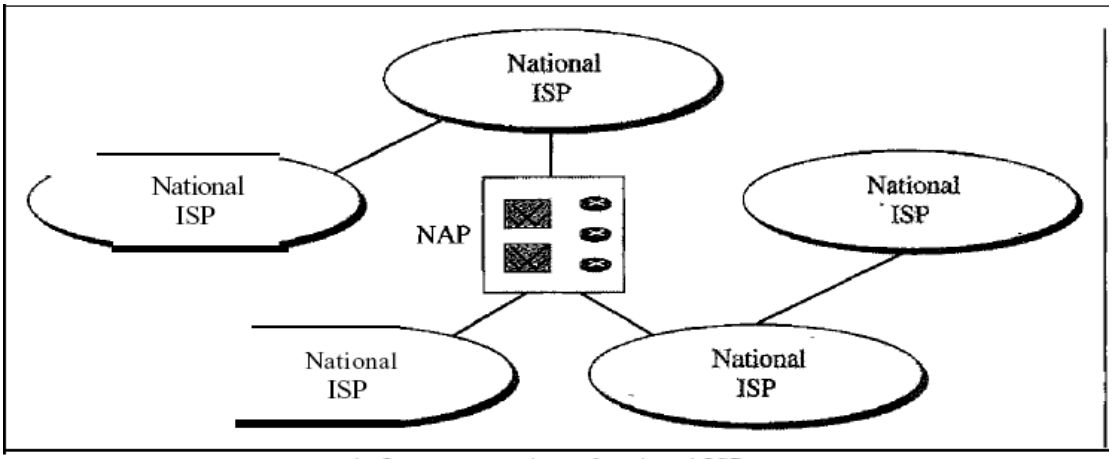
ndledatagramroutingwhileTCPwouldberesponsibleforhigher-levelfunctionssuchas segmentation,reassembly,anderrordetection.Theinternetworkingprotocolbecameknownas TCPIIP.

TheInternetToday

TheInternethascomealongway sincethe1960s.TheInternettodayisnotasimplehierarchicalstructure.Itismadeupofmanywid e-andlocal-areanetworksjoinedbyconnectingdevicesandswitchingstations.Itisdifficulttogiveanaccurat erepresentationoftheInternetbecauseitiscontinuallychanging-newnetworksarebeingadded,existingnetworksareaddingaddresses,andnetworksofdefunctc ompaniesarebeingremoved.Todaymostendusers whowantInternetconnectionusetheservice sofInternetserviceproviders(lSPs).Thereareinternationalserviceproviders,nationalservicep roviders,regionalserviceproviders,andlocalserviceproviders.TheInternettodayisrunby privatecompanies,notthegovernment.Figureshowsaconceptual(notgeographic)viewoftheI nternet.



a. Structure of a national ISP



b. Interconnection of national ISPs

InternationalInternetServiceProviders:

At the top of the hierarchy are the international service providers that connect nationstogether.

NationalInternetServiceProviders:

The national Internet service providers are backbone networks created and maintained byspecialized companies. There are many national ISPs operating in North America; some of themostwellknownareSprintLink,PSINet,UUNetTechnology,AGIS,andinternetMel.Topro vide connectivity between the end users, these backbone networks are connected by complexswitching stations (normally run by a third party) called network access points (NAPs). Somenational ISP networks are alsoconnected to one another by private switching stations called*peeringpoints.* These normallyoperateata highdatarate(upto600Mbps).

RegionalInternetServiceProviders:

RegionalinternetserviceprovidersorregionalISPsaresmallerISPsthatareconnectedto oneormorenationalISPs.Theyareatthethirdlevelofthehierarchywithasmallerdatarate.*Local Internet ServiceProviders:*

LocalInternetserviceprovidersprovidedirectservicetotheendusers.ThelocalISPscan beconnectedtoregionalISPsordirectlytonationalISPs.Mostendusersareconnectedtothe local ISPs. Note that in this sense, a local ISP can be a company that just provides Internetservices, a corporation with a network that supplies services to its own employees, or a nonprofitorganization, such asacollege orauniversity, that runsits ownnetwork. Eachof these localISPscanbeconnectedtoaregionalornationalserviceprovider.

2.4 PROTOCOLS AND STANDARDS

Protocols:

In computer networks, communication occurs between entities in different systems. Anentity is anything capable of sending or receiving information. However, two entities cannotsimply send bit streams to each other and expect to be understood. For communication to occur,theentitiesmustagreeonaprotocol.Aprotocolisasetofrulesthatgoverndatacommunicat

ions.A protocol defineswhat iscommunicated, how it iscommunicated, andwhenitiscommunicated.Thekeyelementsofaprotocolaresyntax,semantics,andtiming.

o Syntax.Theterm*syntax*referstothestructureorformatofthedata,meaningtheorderin which they are presented.For example, a simple protocol might expectthefirst 8 bitsof datato be the address of the sender, the second 8 bits to be the address of the receiver, and the rest ofthestreamtobethemessageitself.

o Semantics. The word *semantics* refers to the meaning of each section of bits. How is aparticularpatterntobeinterpreted,andwhatactionistobetakenbasedonthatinterpretation?For example,doesanaddressidentify theroutetobetakenorthefinaldestinationofthemessage?

o Timing. The term *timing* refers to two characteristics:when data should be sentandhow fast they can be sent. For example, if a sender produces data at 100Mbpsbut the receivercanprocessdataatonly1Mbps,thetransmissionwilloverloadthereceiverandsomedat awillbelost.

Standards

Standards are essential in creating and maintaining an open and competitive market forequipment manufacturers and inguaranteeing national and international interoperability of dataandtelecommunicationstechnologyandprocesses.Standardsprovideguidelinestomanuf acturers, vendors, government agencies, and other service providers to ensure the kind ofinterconnectivitynecessaryintoday'smarketplaceandininternationalcommunications. Datacommunicationstandardsfallintotwocategories:*defacto*(meaning"by fact"or"byconvention")and*de jure*(meaning"bylaw"or"byregulation").

o De facto. Standards that have not been approved by an organized body but have beenadopted as standards through widespread use are de facto standards. De facto standards are oftenestablished originally by manufacturers who seek to define the functionality of a new product ortechnology.

o De jure. Those standards that have been legislated by an officially recognized body aredejurestandards.

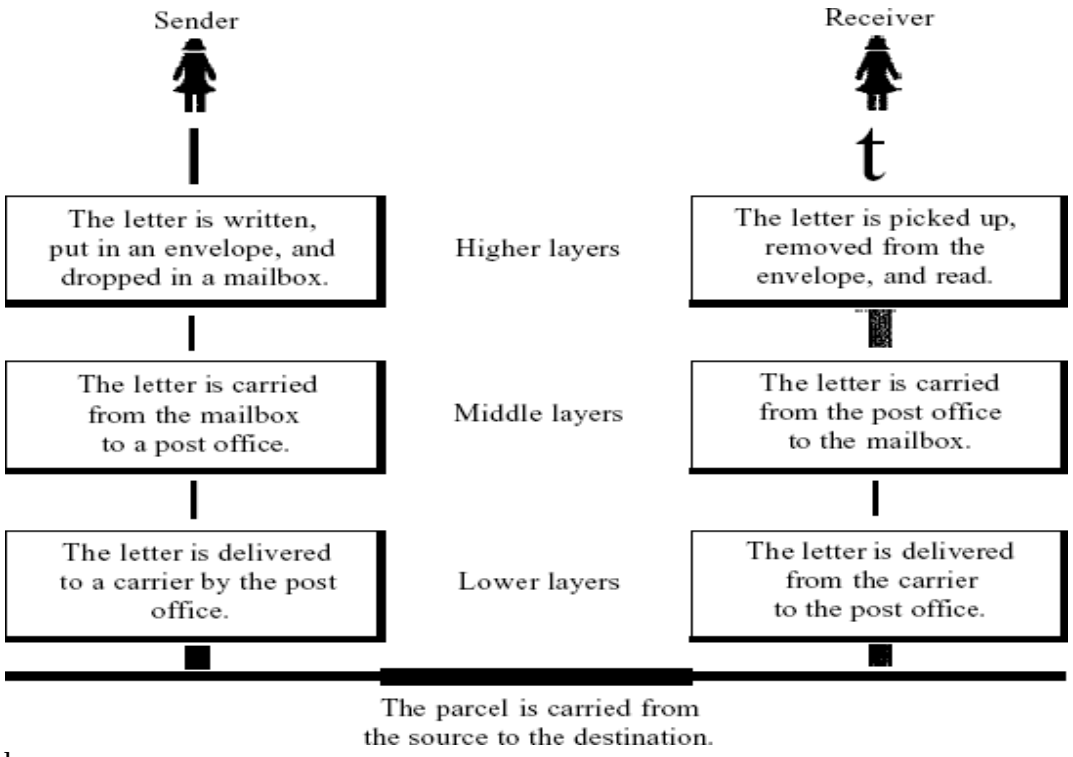
LAYEREDTASKS

We use the concept of layers in our daily life. As an example, let us consider two friendswho

communicate through postal maiL The process of sending a letter to a friend would becomplex if there were no services available from the post office. Below Figure shows the steps inthistask

Sender,Receiver,andCarrier

InFigurewehaveasender,areceiver,andacarrierthattransportstheletter.Thereisahierarchyoft



asks.

AttheSenderSite

Letusfirstdescribe,inorder,theactivitiesthattakeplaceatthesendersite.

o Higherlayer.Thesenderwritestheletter,insertstheletterinanenvelope,writesthesenderandreceiveraddresses, anddropstheletterina mailbox.

o Middlelayer.Theletterispickedupbyalettercarrieranddeliveredtothepostoffice.

o Lower layer.Theletterissortedatthepostoffice;acarriertransportstheletter.

0n the Way: The letter is then on its way to the recipient. On the way to the recipient's local postoffice, the letter may actually go through a central office. In addition, it may be transported bytruck,train,airplane,boat,oracombinationofthese.

AttheReceiverSite

- Lowerlayer.Thecarriertransportsthelettertothepostoffice.
- Middlelayer.Theletterissortedanddeliveredtotherecipient'smailbox.
- Higherlayer.Thereceiverpicksuptheletter,openstheenvelope,andreadsit.

2.5 REFERENCE MODELS

TheOSIReferenceModel:

The OSI model (minus the physical medium) is shown in Fig. This model is based on a proposaldeveloped by the International Standards Organization (ISO) as a first step toward internationalstandardization of the protocols used in the various layers (Day and Zimmermann, 1983). It wasrevised in 1995(Day, 1995). The model is called the ISO-OSI (Open Systems Interconnection)Reference Model because it deals with connecting opensystems—that is,systems that are openforcommunicationwithothersystems.

The OSImodel hassevenlayers. The principlesthat were applied toarrive atthesevenlayerscan bebrieflysummarizedasfollows:

1. Alayershouldbecreatedwhereadifferentabstractionisneeded.
2. Eachlayershouldperformawell-definedfunction.
3. The function of eachlayer should be chosenwithan eye towarddefining internationallystandardized protocols.
4. Thelayerboundariesshouldbechosentominimizetheinformationflowacrosstheinterfaces.
5. The number of layers should be largeenough that distinct functions need not bethrowntogetherinthe samelayeroutofnecessity andsmallenoughthatthearchitecture doesnotbecomeunwieldy.

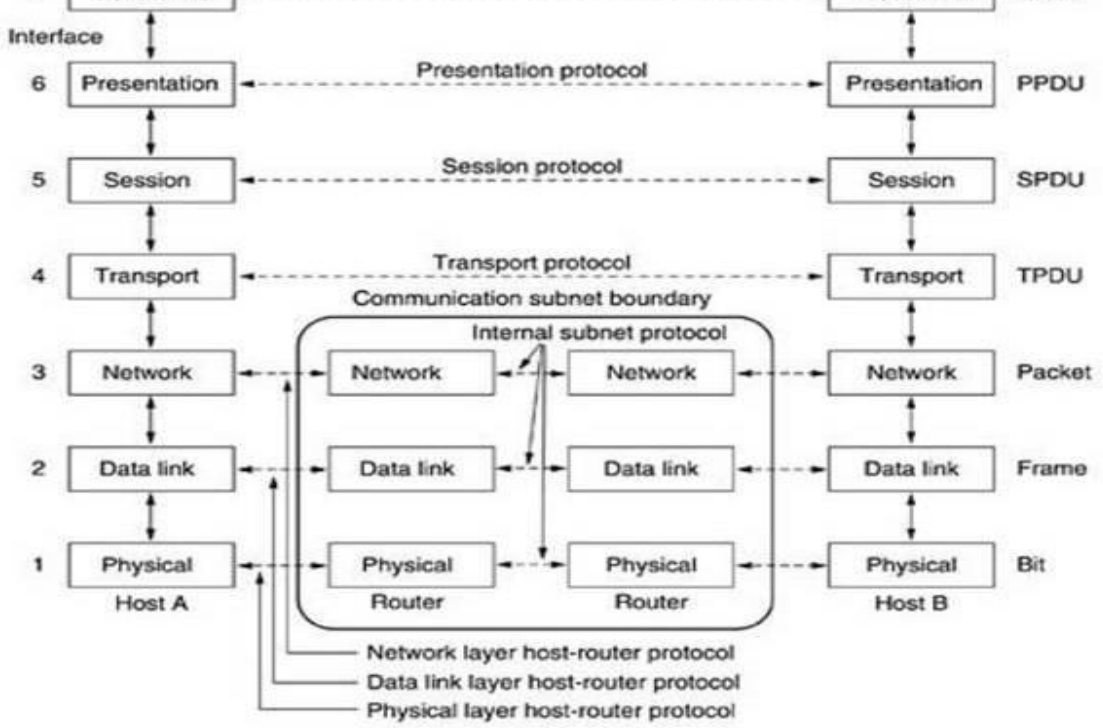


Fig.4:TheOSIreferencemodel

ThePhysicalLayer:

The physical layer is concerned with transmitting raw bits over a communication channel. Thedesign issues have to do with making sure that when one side sends a 1 bit, it is received by theothersideas a1 bit,notas a0 bit.

TheDataLinkLayer:

The main task of the data link layer is to transform a raw transmission facility into a line thatappears free of undetected transmission errors to the network layer. It accomplishes this task byhaving the sender break up the input data into data frames (typically a few hundred or a fewthousand bytes) and transmits the frames sequentially. If the service isreliable, the receiverconfirmscorrectreceiptof eachframe bysending backanacknowledgementframe.

Another issue that arises in the data link layer (and most of the higher layers as well)is how tokeepafasttransmitterfromdrowningaslowreceiverindata.Sometrafficregulationmechanismisoftenneededtoletthetransmitterknowhowmuchbufferspacethereceiverhasatthemoment. Frequently,thisflowregulationandtheerrorhandlingare integrated.

TheNetworkLayer:

The network layer controls the operation of the subnet. A key design issue is determining howpackets are routed from source to destination. Routes can be based on static tables that are

"wiredinto"thenetworkandrarelychanged.Theycanalsobedeterminedatthestartofeachconversation,for example, a terminal session (e.g., a login to a remotemachine).Finally, theycan be highly dynamic,being determined anewfor each packet, toreflect the current networkload.

If too many packets are present in the subnet at the same time, they will get in one another's way,forming bottlenecks. The control of such congestion also belongs to the network layer. Moregenerally, the quality of service provided (delay, transit time, jitter, etc.) is also a network layerissue.

When a packet has to travel from one network to another to get to its destination, many problemscan arise. The addressing used by the second network may be different from the first one. Thesecondonemay notacceptthepacketatallbecauseitistoolarge.Theprotocolsmaydiffer,andso on.It is up to the network layer to overcome all these problemsto allow heterogeneousnetworks to be interconnected.In broadcast networks, theroutingproblem issimple, so thenetworklayerisoften thinoreven nonexistent.

TheTransportLayer:

Thebasicfunctionofthetransportlayeristoacceptdatafromabove,splititupintosmallerunits ifneed be,passthese to the network layer,and ensure that the pieces allarrive correctly atthe other end. Furthermore, all this must be done efficiently and in a way that isolates the upperlayersfromtheinevitablechangesinthehardwaretechnology.Thetransportlayeralsodetermineswhat type ofservice to provide tothe session layer, and, ultimately,to the users ofthenetwork.Themostpopulartypeoftransportconnectionisanerror-freepoint-to-pointchannel that delivers messages or bytes in the order in which they were sent. However, otherpossible kinds of transport service are the transporting of isolated messages, with no guaranteeabout the orderofdelivery, andthebroadcasting of messagestomultiple destinations. The typeofservice isdeterminedwhen theconnection isestablished.

The transport layer is a true end-to-end layer, all the way from the source to the destination. Inotherwords,a programon the source machine carries on a conversation withasimilarprogramonthedestinationmachine,usingthemessageheadersandcontrolmessages.Inthelowerlayers, the protocols are between each machine and its immediate neighbours,and not between theultimatesource

anddestinationmachines,whichmaybeseparatedby manyrouters.

TheSessionLayer:

Thesessionlayerallowsusersondifferentmachinestoestablishsessionsbetweenthem.Sessions offer various services, including dialog control (keeping track of whose turn it is totransmit), token management (preventing two parties from attempting the same criticaloperationatthe sametime),andsynchronization(checkpointing long transmissionstoallowthem tocontinuefrom wheretheywereafteracrash).

ThePresentationLayer:

The presentation layer is concerned with the syntax and semantics of the information transmitted.Inorder to make itpossible for computers withdifferent data representations tocommunicate,the data structures to be exchanged can be defined in an abstract way, along with a standardencoding to be used "on the wire." The presentation layer manages these abstract data structuresandallowshigher-leveldatastructures(e.g.,bankingrecords),tobedefinedandexchanged.

TheApplicationLayer:

The application layer contains a variety of protocols that are commonly needed by users. Onewidely-used application protocolisHTTP (HypertextTransfer Protocol),which isthe basis
fortheWorldWideWeb.WhenabrowserwantsaWebpage,itsendsthenameofthepageitwantsto the server using HTTP. The server then sends the page back. Other application protocols areusedforfiletransfer,electronicmail,and networknews.

2.6 TheTCP/IPReferenceModel:

TheTCP/IPreferencemodelwasdevelopedpriortoOSImodel.Themajordesigngoalsofthismodel were,

1. Toconnectmultiplenetworkstogethersothatthey appearasasinglenetwork.

2. Tosurviveafterpartialsubnethardwarefailures.

3. Toprovideaflexiblearchitecture.

UnlikeOSIreferencemodel,TCP/IPreferencemodelhasonly4layers.Theyare,

1. Host-to-NetworkLayer

2. InternetLayer

3. TransportLayer

4. Application

LayerApplicat

ionLayerTrans

portLayerInter

netLayer

Host-to-NetworkLayer

Host-to-NetworkLayer:

The TCP/IP reference model does not really say muchabout what happens here,except to pointout that the host has to connect to the network using some protocol so it can send IP packets to it.Thisprotocolisnotdefinedandvariesfromhosttohostandnetworktonetwork.

InternetLayer:

Thislayer,called the internetlayer, is the linchpin thatholds the whole architecturetogether. Itsjob is to permit hosts to inject packets into any network and have they travel independently to thedestination (potentially ona differentnetwork). They may evenarrive ina differentorder thantheyweresent,inwhichcaseitisthejobofhigherlayerstorearrangethem,ifin-orderdeliveryis desired. Note that "internet" is used here in a generic sense, even though this layer is present intheInternet.

The internetlayer defines anofficial packet formatand protocol calledIP(InternetProtocol).The job of the internetlayer is to deliverIP packets where they are supposed to go.Packetroutingisclearlythemajorissuehere,asisavoidingcongestion.Forthesereasons,itisreasonable tosay that the TCP/IP internetlayeris similar infunctionality totheOSI networklayer.Fig.shows thiscorrespondence.

TheTransportLayer:

The layer above the internetlayer in the TCP/IPmodelis nowusually called thetransport layer.Itisdesignedtoallowpeerentitiesonthesourceanddestinationhoststocarryonaconversation, just as in the OSI transport layer. Two end-to-end transport protocols have beendefinedhere.Thefirstone,TCP(TransmissionControlProtocol),isareliableconnection-oriented protocolthatallows a byte stream originating on one machine to be

deliveredwithouterror on any other machine in the internet. It fragments the incoming byte stream into discretemessages and passes each one on to the internet layer. At the destination, the receiving TCPprocessreassemblesthereceivedmessagesintotheoutputstream.TCPalsohandlesflowcontrol tomakesureafastsendercannotswampaslowreceiverwithmoremessagesthanitcanhandle.

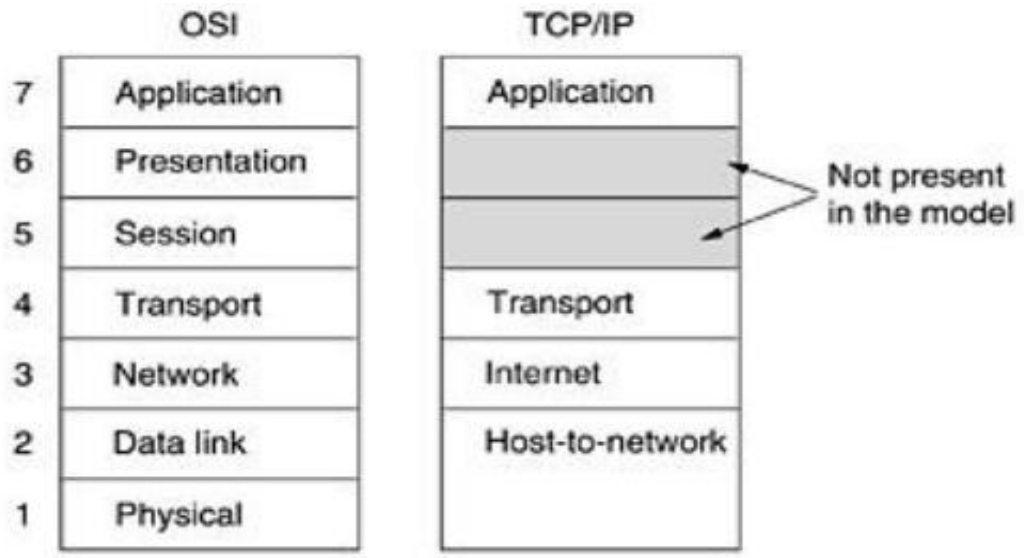


Fig.1:TheTCP/IPreferencemodel.

Thesecondprotocolinthislayer,UDP(UserDatagramProtocol),isanunreliable,connectionless protocol for applications that do not want TCP's sequencing or flow control andwish to provide their own. It is also widely used for one-shot, client-server-type request-replyqueriesand applications in which prompt delivery is more important than accurate delivery, suchas transmitting speech or video. The relation of IP, TCP, and UDP is shown in Fig.2. Since themodelwasdeveloped,IPhasbeenimplementedonmanyothernetworks.

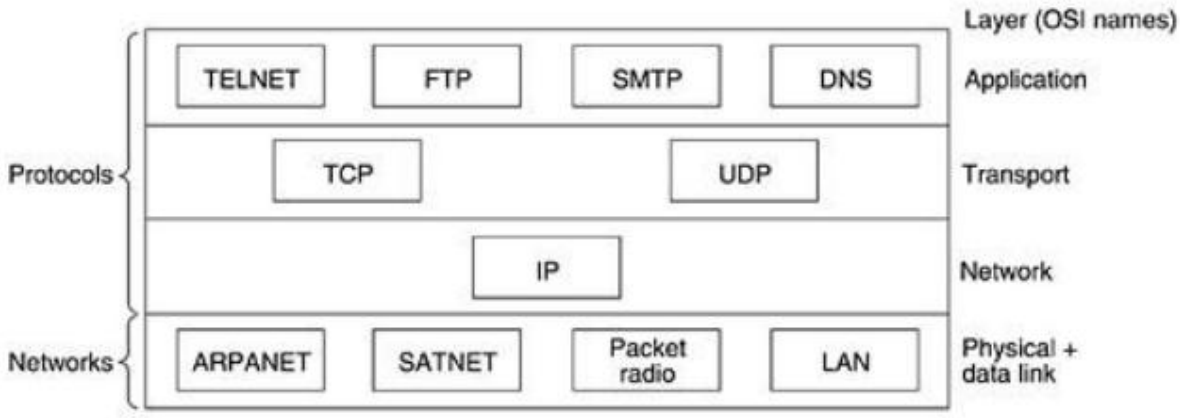


Fig.2:ProtocolsandnetworksintheTCP/IPmodelinitially.

TheApplicationLayer:

The TCP/IP modeldoes nothave session or presentation layers.On top of the transportlayer isthe application layer. It contains all the higher-level protocols. The early ones included virtualterminal (TELNET), file transfer (FTP), and electronic mail (SMTP), as shown in Fig.6.2. Thevirtual terminal protocol allows a user on one machine to log onto a distant machine and workthere. The file transfer protocol provides a way to move data efficiently from one machine toanother. Electronic mail was originally just a kind of file transfer, but later a specialized protocol(SMTP) was developed for it. Many other protocols have been added to these over the years: theDomain Name System (DNS) for mapping host names onto their network addresses, NNTP, theprotocolformovingUSENETnewsarticlesaround,andHTTP,theprotocolforfetchingpage son theWorldWideWeb,andmanyothers.

ComparisonoftheOSIandTCP/IPReferenceModels:

The OSI and TCP/IP reference models have much in common. Both are based on theconcept ofa stack of independent protocols.Also, the functionality ofthe layers isroughlysimilar. For example, in both models the layers up through and including the transport layer arethere to provide an end-to-end, network-independent transport service to processes wishing tocommunicate. These layers form the transport provider. Again in both models, the layers abovetransportareapplication-orientedusersofthetransportservice.Despitethesefundamentalsimilarities, the two models also have many differences Three concepts are central to the OSImodel:

1. Services.

2. Interfaces.

3. Protocols.

Probably the biggest contribution of the OSI model is to make the distinction between these threeconceptsexplicit.Eachlayerperformssomeservicesforthelayeraboveit.Theservicedefinition tells what the layer does, not how entities above it access it or how the layer works. Itdefinesthelayer'ssemantics.

A layer's interface tells the processes above it how to access it.It specifies what theparametersareandwhatresultstoexpect.It, too, saysnothingabouthowthelayerworksinside.

Finally, the peer protocols used in a layer are the layer's own business. It can use any protocols itwants to, as long as itgets the job done (i.e., provides the offered services). It canalso changethematwillwithoutaffectingsoftware in higherlayers.

The TCP/IP model did not originally clearly distinguish between service, interface, and protocol,although people have tried to retrofit it after the fact to make it more OSI-like. For example, theonlyrealservicesofferedbytheinternetlayerareSENDIPPACKETandRECEIVEIPPACKET.

As a consequence, the protocols intheOSI model are better hidden thanin theTCP/IP modelandcanbereplacedrelativelyeasilyasthetechnologychanges.Beingabletomakesuchchanges is one of the main purposes of having layered protocols in the first place. The OSIreference model was devised before the corresponding protocols were invented. This orderingmeans that the model was not biased toward one particular set ofprotocols, a fact that made itquite general. The downside of this ordering is that the designers did not have much experiencewiththesubjectanddidnothaveagoodideaofwhichfunctionalitytoputinwhichlayer.

Another difference isintheareaof connectionlessversus connection-oriented communication.TheOSImodelsupportsbothconnectionlessandconnection-orientedcommunicationinthenetworklayer,butonlyconnection-orientedcommunicationinthetransportlayer,whereitcounts (because the transportservice isvisible to the users). TheTCP/IP model has only onemode in the network layer (connectionless) but supports both modes in the transport layer, givingtheusersachoice.Thischoiceisespeciallyimportantforsimplerequest-responseprotocols.

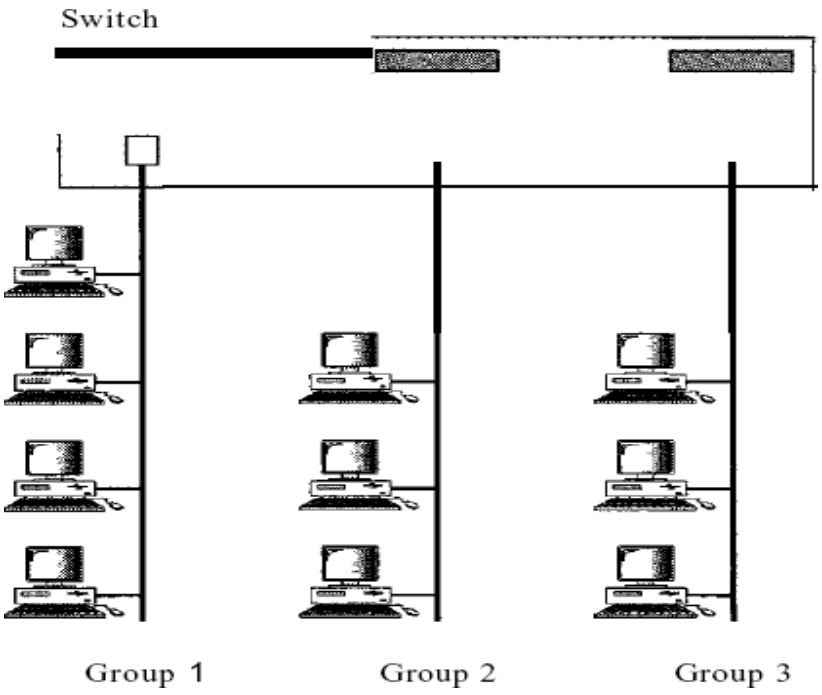


Figure6*AswitchconnectingthreeLANs*

2.6 SUMMARY

At the end of this unit we have learnt about physical structure which includes topologies of networks; we dealt with the concept of categories of networks (LAN, MAN,WAN). In the later stage we focused protocols and standards. In the last section of this unit we have discussed reference models which includes OSI reference model and TCP/IP reference model.

2.7 KEYWORDS

Mesh topology, Star topology, Bus topology, Ring topology, LAN, WAN, MAN, Internet.

2.8 QUESTIONS

1. Briefly explain physical structure.
2. Discuss protocols and standards.
3. With neat diagram explain OSI reference model.
4. Differentiate OSI and TCP/IP reference model.

5. Describe categories of network.

2.9 REFERENCES

- WilliamStallings,DataandComputerCommunication,PrenticeHallofIndia
- BehrouzA.Forouzan,DataCommunicationandNetworking,McGraw-Hill
- AndrewS.Tanenbaum,ComputerNetworks, PrenticeHall.

UNIT 3: PHYSICAL LAYER

Structure:

3.0 OBJECTIVES

After going through this lesson you will be able to

- Describe Overview of data
- Discuss data and signals.
- Elucidate digital transmission
- Explain analog transmission

3.1 INTRODUCTION

Physical Layer is the bottom-most layer in the **Open System Interconnection (OSI) Model** which is a physical and electrical representation of the system. It consists of various network components such as power plugs, connectors, receivers, cable types, etc. Physical Layer sends data bits from one device(s) (like a computer) to another device(s). Physical Layer defines the types of encoding (that is how the 0's and 1's is encoded in a signal). Physical Layer is responsible for the communication of the unstructured raw data streams over a physical medium.

PHYSICAL LAYER

Physical layer in the OSI model plays the role of interacting with actual hardware and signaling mechanism. Physical layer is the only layer of OSI network model which actually

deals with the physical connectivity of two different stations. This layer defines the hardware equipment, cabling, wiring, frequencies, pulses used to represent binary signals etc.

Physical layer provides its services to Data-link layer. Data-link layer hands over frames to physical layer. Physical layer converts them to electrical pulses, which represent binary data.The binary data is then sent over the wired or wireless media.

Signals

When data is sent over physical medium, it needs to be first converted into electromagnetic signals. Data itself can be analog such as human voice, or digital such as file on the disk.Bothanalog and digital data can be represented in digital or analog signals.

- **Digital Signals**
  Digital signals are discrete in nature and represent sequence of voltage pulses. Digital signals are used within the circuitry of a computer system.
- **Analog Signals**
  Analog signals are in continuous wave form in nature and represented by continuous electromagnetic waves.

Transmission Impairment

When signals travel through the medium they tend to deteriorate. This may have many reasons as given:

- **Attenuation**
  For the receiver to interpret the data accurately, the signal must be sufficiently strong.When the signal passes through the medium, it tends to get weaker.As it covers distance, it loses strength.
- **Dispersion**
  As signal travels through the media, it tends to spread and overlaps. The amount of dispersion depends upon the frequency used.
- **Delay distortion**
  Signals are sent over media with pre-defined speed and frequency. If the signal speed and frequency do not match, there are possibilities that signal reaches destination in arbitrary fashion. In digital media, this is very critical that some bits reach earlier than the previously sent ones.

- **Noise**

  Random disturbance or fluctuation in analog or digital signal is said to be Noise in signal, which may distort the actual information being carried. Noise can be characterized in one of the following class:

  - **Thermal Noise**

    Heat agitates the electronic conductors of a medium which may introduce noise in the media. Up to a certain level, thermal noise is unavoidable.

  - **Intermodulation**

    When multiple frequencies share a medium, their interference can cause noise in the medium. Intermodulation noise occurs if two different frequencies are sharing a medium and one of them has excessive strength or the component itself is not functioning properly, then the resultant frequency may not be delivered as expected.

  - **Crosstalk**

    This sort of noise happens when a foreign signal enters into the media. This is because signal in one medium affects the signal of second medium.

  - **Impulse**

    This noise is introduced because of irregular disturbances such as lightening, electricity, short-circuit, or faulty components. Digital data is mostly affected by this sort of noise.

Transmission Media

The media over which the information between two computer systems is sent, called transmission media. Transmission media comes in two forms.

- **Guided Media**

  All communication wires/cables are guided media, such as UTP, coaxial cables, and fiber Optics. In this media, the sender and receiver are directly connected and the information is send (guided) through it.

- **Unguided Media**

  Wireless or open air space is said to be unguided media, because there is no connectivity between the sender and receiver. Information is spread over the air, and anyone including the actual recipient may collect the information.

Channel Capacity

The speed of transmission of information is said to be the channel capacity. We count it as data rate in digital world. It depends on numerous factors such as:

- **Bandwidth:** The physical limitation of underlying media.
- **Error-rate:** Incorrect reception of information because of noise.
- **Encoding:** The number of levels used for signaling.

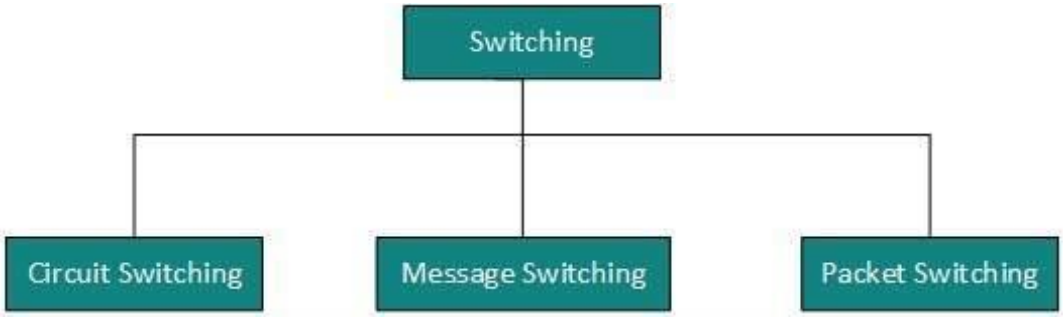
Multiplexing

Multiplexing is a technique to mix and send multiple data streams over a single medium. This technique requires system hardware called multiplexer (MUX) for multiplexing the streams and sending them on a medium, and de-multiplexer (DMUX) which takes information from the medium and distributes to different destinations.

Switching

Switching is a mechanism by which data/information sent from source towards destination which are not directly connected. Networks have interconnecting devices, which receives data from directly connected sources, stores data, analyze it and then forwards to the next interconnecting device closest to the destination.

Switching can be categorized as:



Data or information can be stored in two ways, analog and digital. For a computer to use the data, it must be in discrete digital form.Similar to data, signals can also be in analog and digital form. To transmit data digitally, it needs to be first converted to digital form.

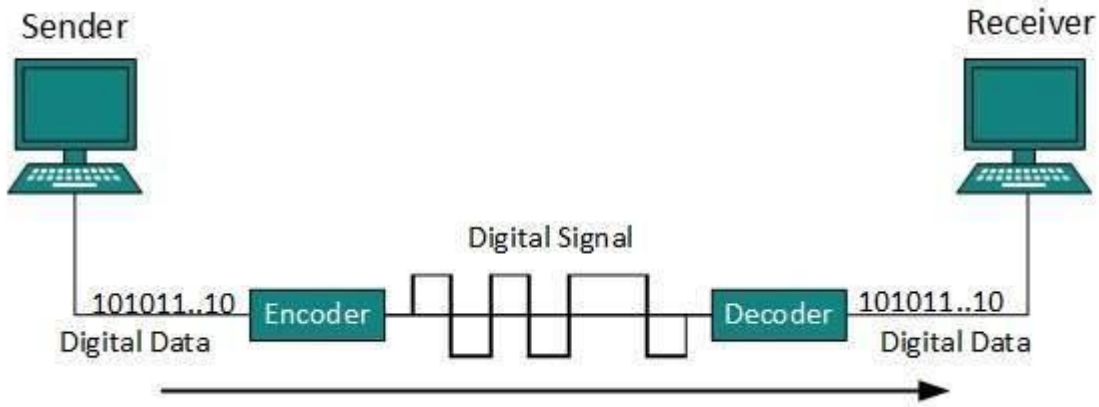
3.4 DIGITAL TRANSMISSION

Digital-to-Digital Conversion

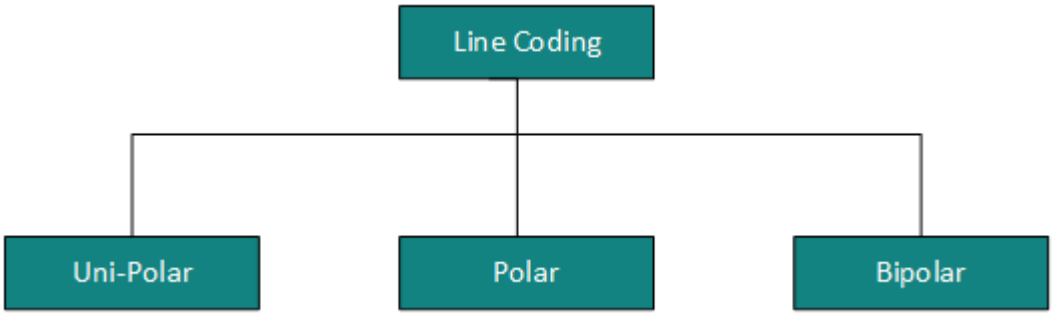
This section explains how to convert digital data into digital signals. It can be done in two ways, line coding and block coding. For all communications, line coding is necessary whereas block coding is optional.

Line Coding

The process for converting digital data into digital signal is said to be Line Coding. Digital data is found in binary format.It is represented (stored) internally as series of 1s and 0s.

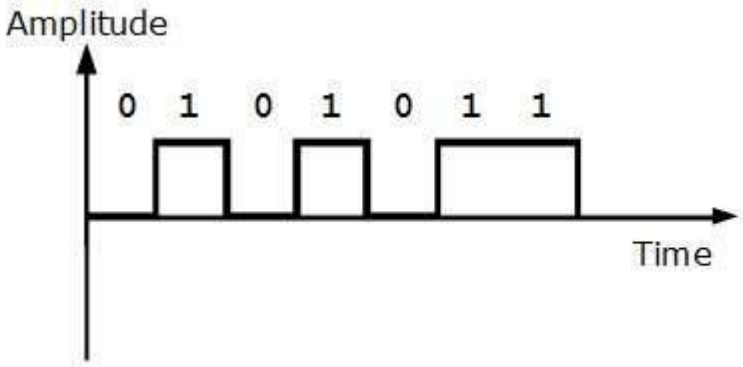


Digital signal is denoted by discreet signal, which represents digital data.There are three types of line coding schemes available:



Uni-polar Encoding

Unipolar encoding schemes use single voltage level to represent data. In this case, to represent binary 1, high voltage is transmitted and to represent 0, no voltage is transmitted. It is also called Unipolar-Non-return-to-zero, because there is no rest condition i.e. it either represents 1 or 0.



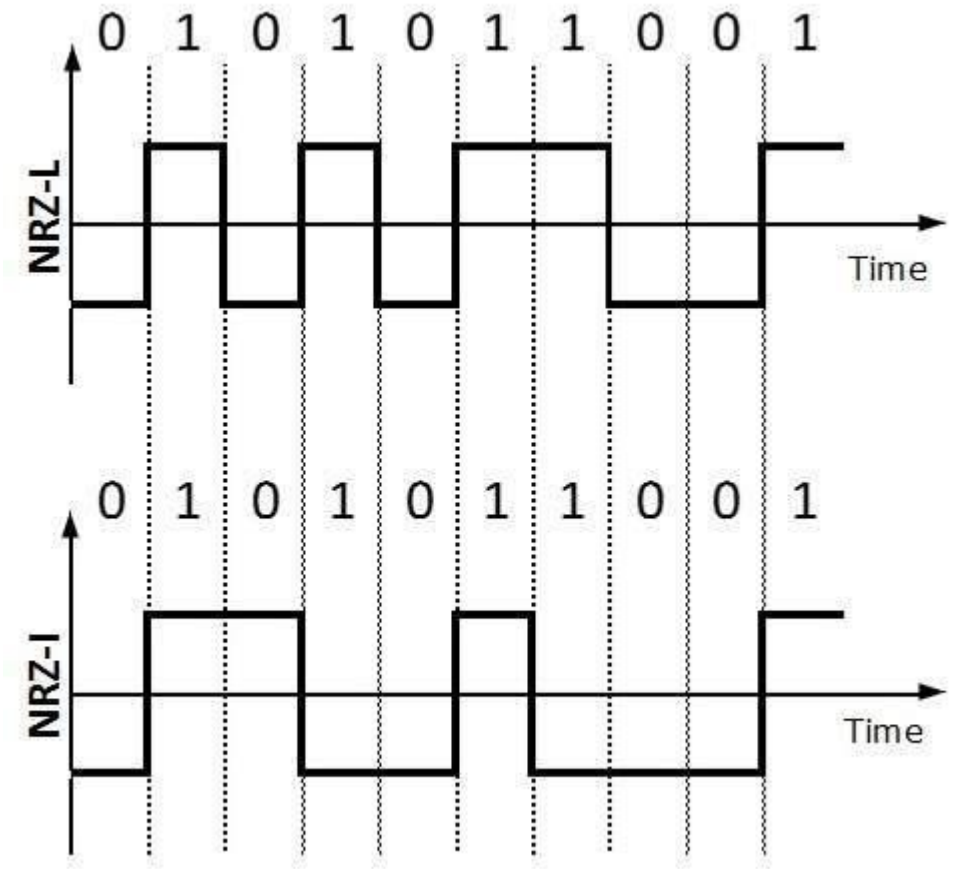
Polar Encoding

Polar encoding scheme uses multiple voltage levels to represent binary values. Polar encodings is available in four types:

- Polar Non-Return to Zero (Polar NRZ)

  It uses two different voltage levels to represent binary values. Generally, positive voltage represents 1 and negative value represents 0. It is also NRZ because there is no rest condition.

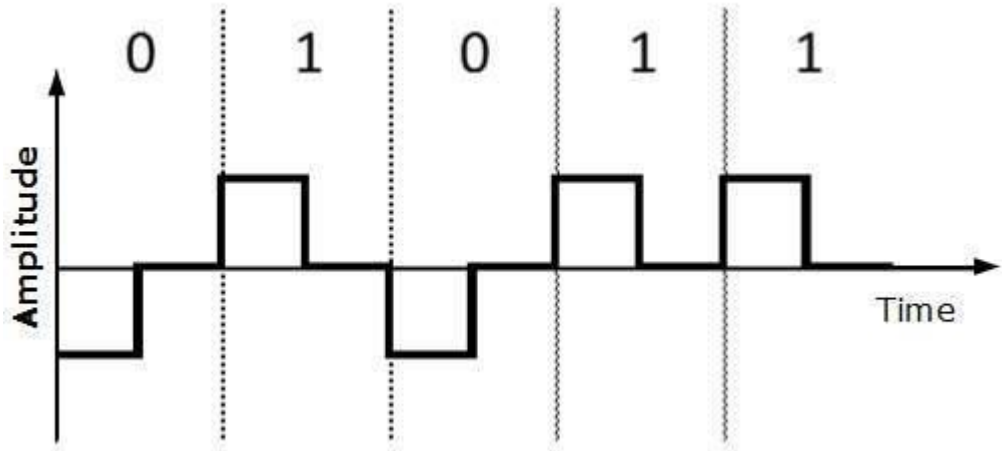
  NRZ scheme has two variants: NRZ-L and NRZ-I.



NRZ-L changes voltage level at when a different bit is encountered whereas NRZ-I changes voltage when a 1 is encountered.

- Return to Zero (RZ)

  Problem with NRZ is that the receiver cannot conclude when a bit ended and when the next bit is started, in case when sender and receiver's clock are not synchronized.



RZ uses three voltage levels, positive voltage to represent 1, negative voltage to represent 0 and zero voltage for none. Signals change during bits not between bits.

- Manchester

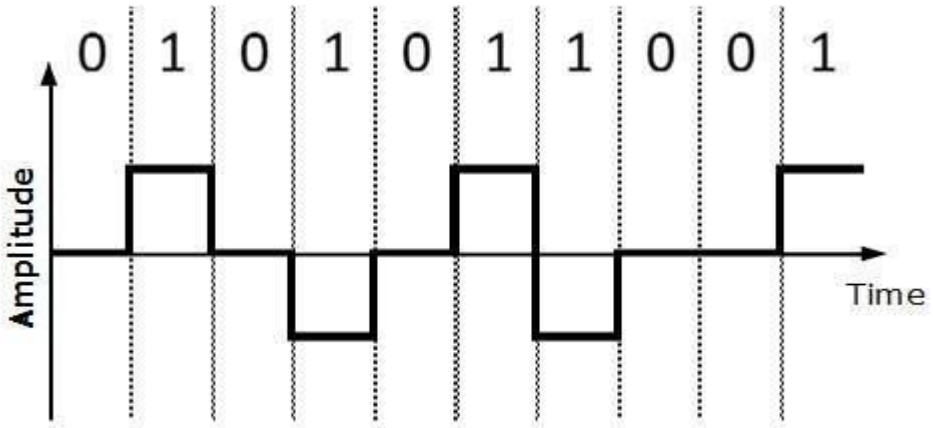
  This encoding scheme is a combination of RZ and NRZ-L. Bit time is divided into two halves. It transits in the middle of the bit and changes phase when a different bit is encountered.

- Differential Manchester

  This encoding scheme is a combination of RZ and NRZ-I. It also transit at the middle of the bit but changes phase only when 1 is encountered.

Bipolar Encoding

Bipolar encoding uses three voltage levels, positive, negative and zero. Zero voltage represents binary 0 and bit 1 is represented by altering positive and negative voltages.



Block Coding

To ensure accuracy of the received data frame redundant bits are used. For example, in even-parity, one parity bit is added to make the count of 1s in the frame even. This way the original number of bits is increased. It is called Block Coding.

Block coding is represented by slash notation, mB/nB.Means, m-bit block is substituted with n-bit block where n > m. Block coding involves three steps:

- Division,
- Substitution
- Combination.

After block coding is done, it is line coded for transmission.

Analog-to-Digital Conversion

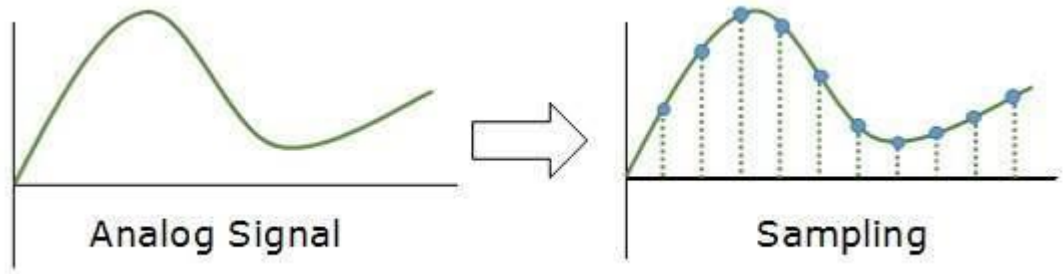
Microphones create analog voice and camera creates analog videos, which are treated is analog data. To transmit this analog data over digital signals, we need analog to digital conversion.

Analog data is a continuous stream of data in the wave form whereas digital data is discrete. To convert analog wave into digital data, we use Pulse Code Modulation (PCM).

PCM is one of the most commonly used method to convert analog data into digital form. It involves three steps:

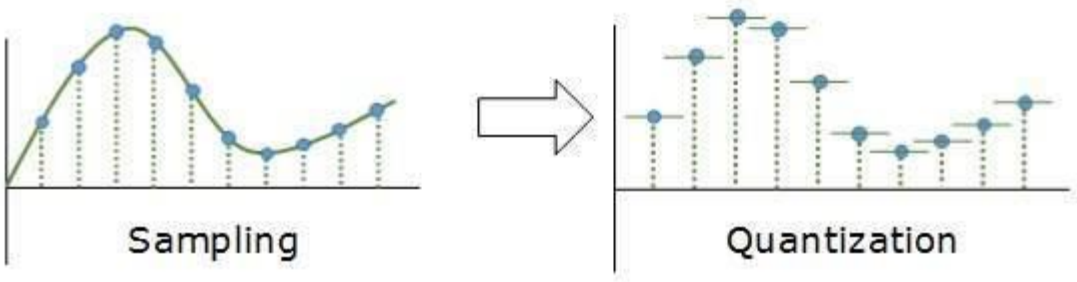
- Sampling
- Quantization
- Encoding.

Sampling



The analog signal is sampled every T interval. Most important factor in sampling is the rate at which analog signal is sampled. According to Nyquist Theorem, the sampling rate must be at least two times of the highest frequency of the signal.

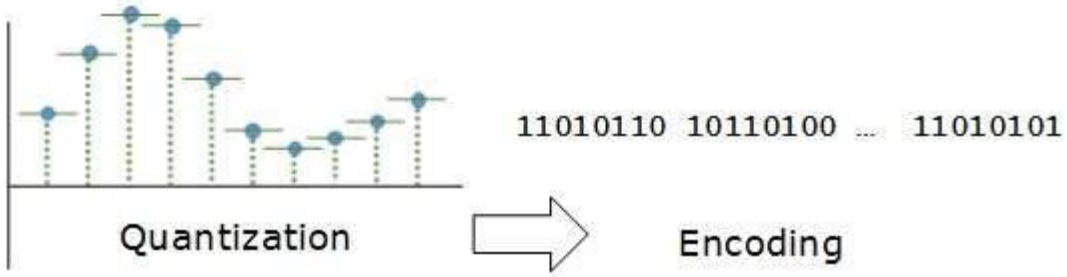
Quantization



Sampling yields discrete form of continuous analog signal. Every discrete pattern shows the amplitude of the analog signal at that instance. The quantization is done between the

maximum amplitude value and the minimum amplitude value. Quantization is approximation of the instantaneous analog value.

Encoding

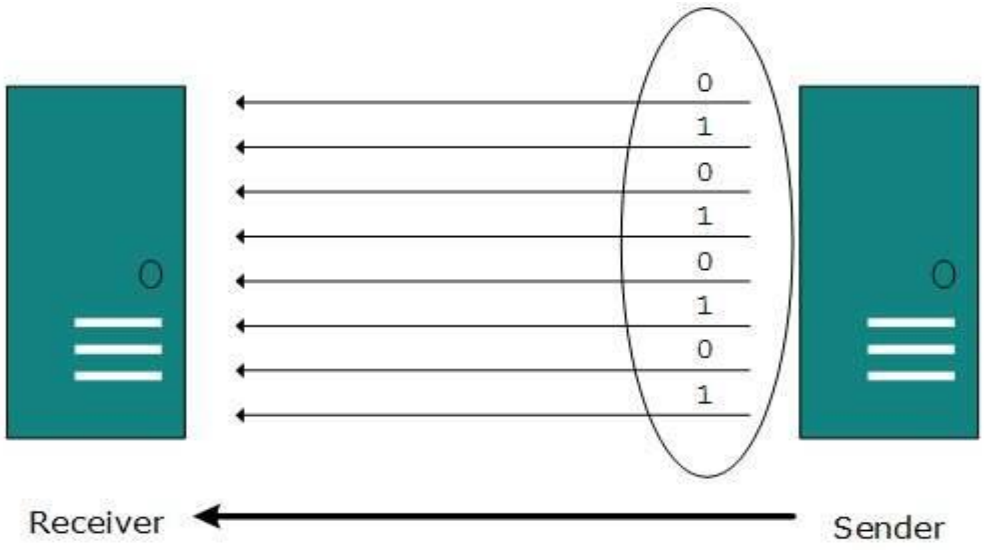


In encoding, each approximated value is then converted into binary format.

Transmission Modes

The transmission mode decides how data is transmitted between two computers.The binary data in the form of 1s and 0s can be sent in two different modes: Parallel and Serial.

Parallel Transmission

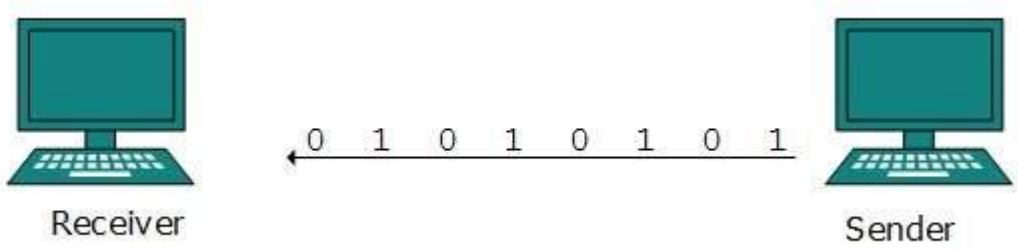


The binary bits are organized in-to groups of fixed length. Both sender and receiver are connected in parallel with the equal number of data lines. Both computers distinguish between high order and low order data lines. The sender sends all the bits at once on all lines.Because the data lines are equal to the number of bits in a group or data frame, a complete group of bits (data frame) is sent in one go. Advantage of Parallel transmission is

high speed and disadvantage is the cost of wires, as it is equal to the number of bits sent in parallel.

Serial Transmission

In serial transmission, bits are sent one after another in a queue manner. Serial transmission requires only one communication channel.



Serial transmission can be either asynchronous or synchronous.

Asynchronous Serial Transmission

It is named so because there'is no importance of timing. Data-bits have specific pattern and they help receiver recognize the start and end data bits.For example, a 0 is prefixed on every data byte and one or more 1s are added at the end.

Two continuous data-frames (bytes) may have a gap between them.

Synchronous Serial Transmission

Timing in synchronous transmission has importance as there is no mechanism followed to recognize start and end data bits.There is no pattern or prefix/suffix method. Data bits are sent in burst mode without maintaining gap between bytes (8-bits). Single burst of data bits may contain a number of bytes. Therefore, timing becomes very important.

It is up to the receiver to recognize and separate bits into bytes.The advantage of synchronous transmission is high speed, and it has no overhead of extra header and footer bits as in asynchronous transmission.

3.5 ANALOG TRANSMISSION

To send the digital data over an analog media, it needs to be converted into analog signal.There can be two cases according to data formatting.

Bandpass: The filters are used to filter and pass frequencies of interest. A bandpass is a band of frequencies which can pass the filter.

Low-pass: Low-pass is a filter that passes low frequencies signals.

When digital data is converted into a bandpassanalog signal, it is called digital-to-analog conversion. When low-pass analog signal is converted into bandpassanalog signal, it is called analog-to-analog conversion.

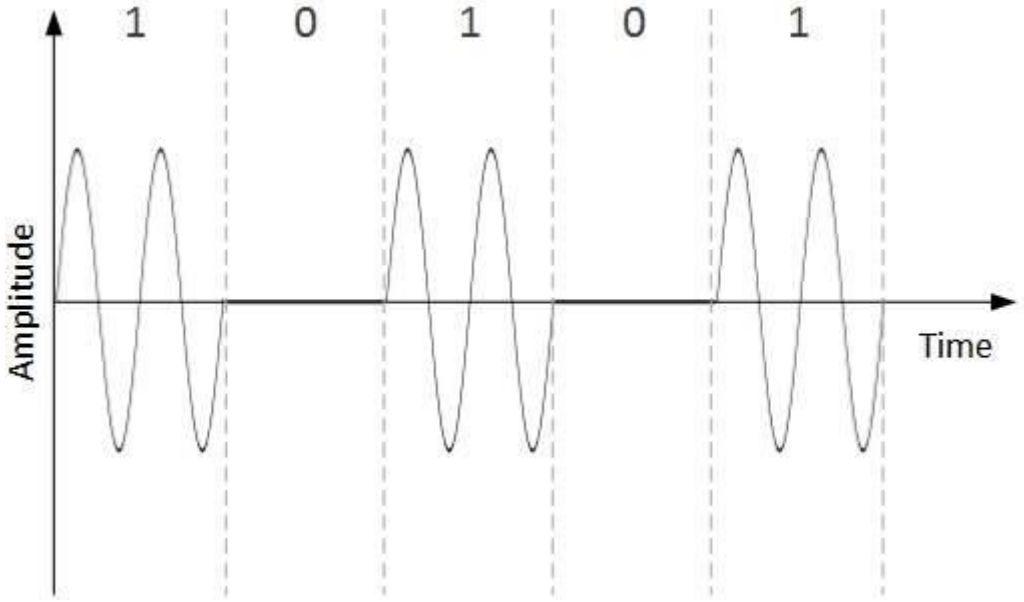
Digital-to-Analog Conversion

When data from one computer is sent to another via some analog carrier, it is first converted into analog signals. Analog signals are modified to reflect digital data.

An analog signal is characterized by its amplitude, frequency, and phase. There are three kinds of digital-to-analog conversions:

- **Amplitude Shift Keying**

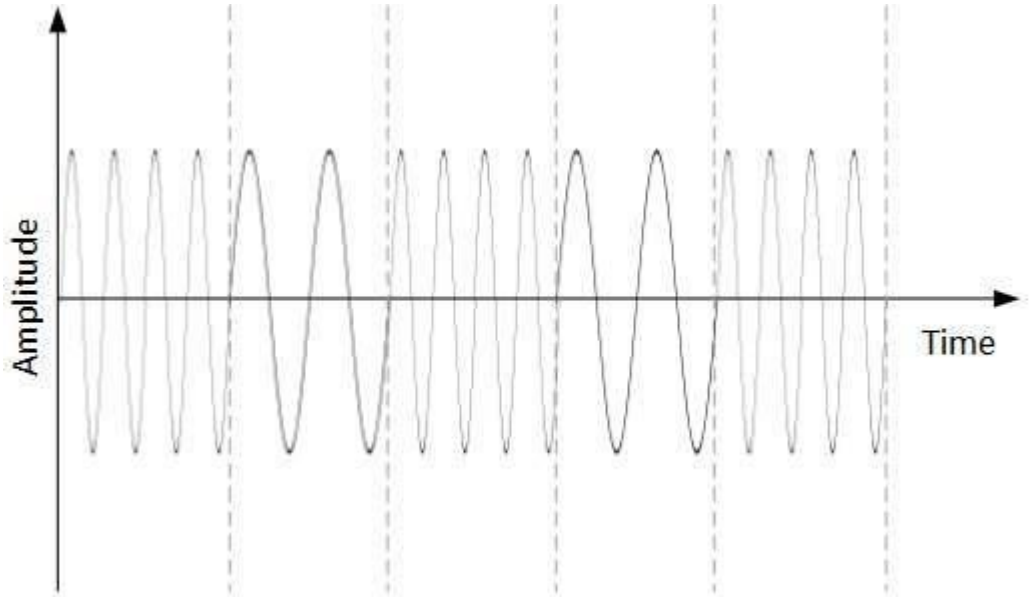
  In this conversion technique, the amplitude of analog carrier signal is modified to reflect binary data.



  When binary data represents digit 1, the amplitude is held; otherwise it is set to 0. Both frequency and phase remain same as in the original carrier signal.

- **Frequency Shift Keying**

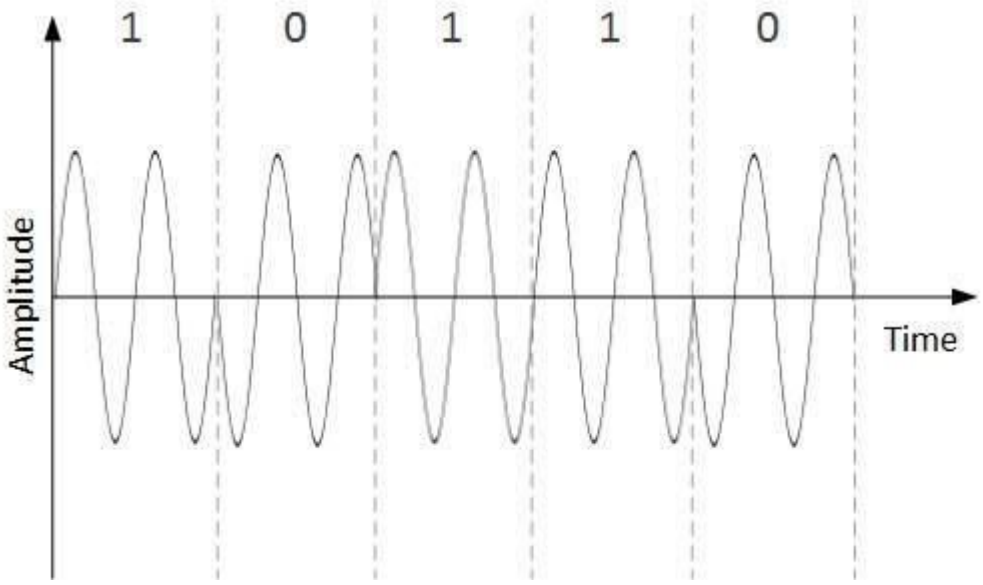
  In this conversion technique, the frequency of the analog carrier signal is modified to reflect binary data.



This technique uses two frequencies, f1 and f2. One of them, for example f1, is chosen to represent binary digit 1 and the other one is used to represent binary digit 0. Both amplitude and phase of the carrier wave are kept intact.

- **Phase Shift Keying**

  In this conversion scheme, the phase of the original carrier signal is altered to reflect the binary data.



When a new binary symbol is encountered, the phase of the signal is altered. Amplitude and frequency of the original carrier signal is kept intact.

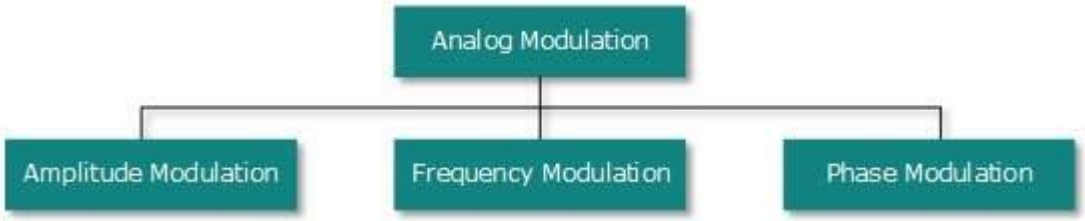
- **Quadrature Phase Shift Keying**

  QPSK alters the phase to reflect two binary digits at once. This is done in two different phases. The main stream of binary data is divided equally into two sub-

streams. The serial data is converted in to parallel in both sub-streams and then each stream is converted to digital signal using NRZ technique. Later, both the digital signals are merged together.

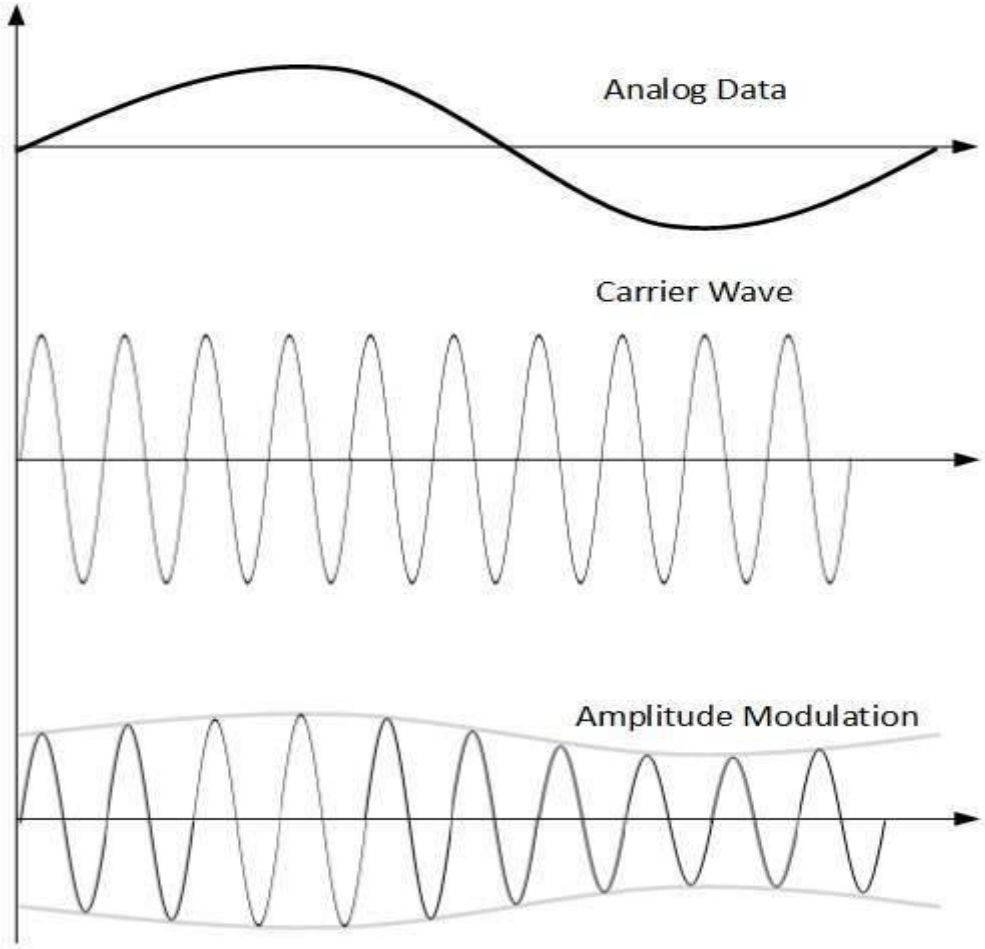
Analog-to-Analog Conversion

Analog signals are modified to represent analog data. This conversion is also known as Analog Modulation. Analog modulation is required when bandpass is used. Analog to analog conversion can be done in three ways:



- **Amplitude Modulation**

  In this modulation, the amplitude of the carrier signal is modified to reflect the analog data.

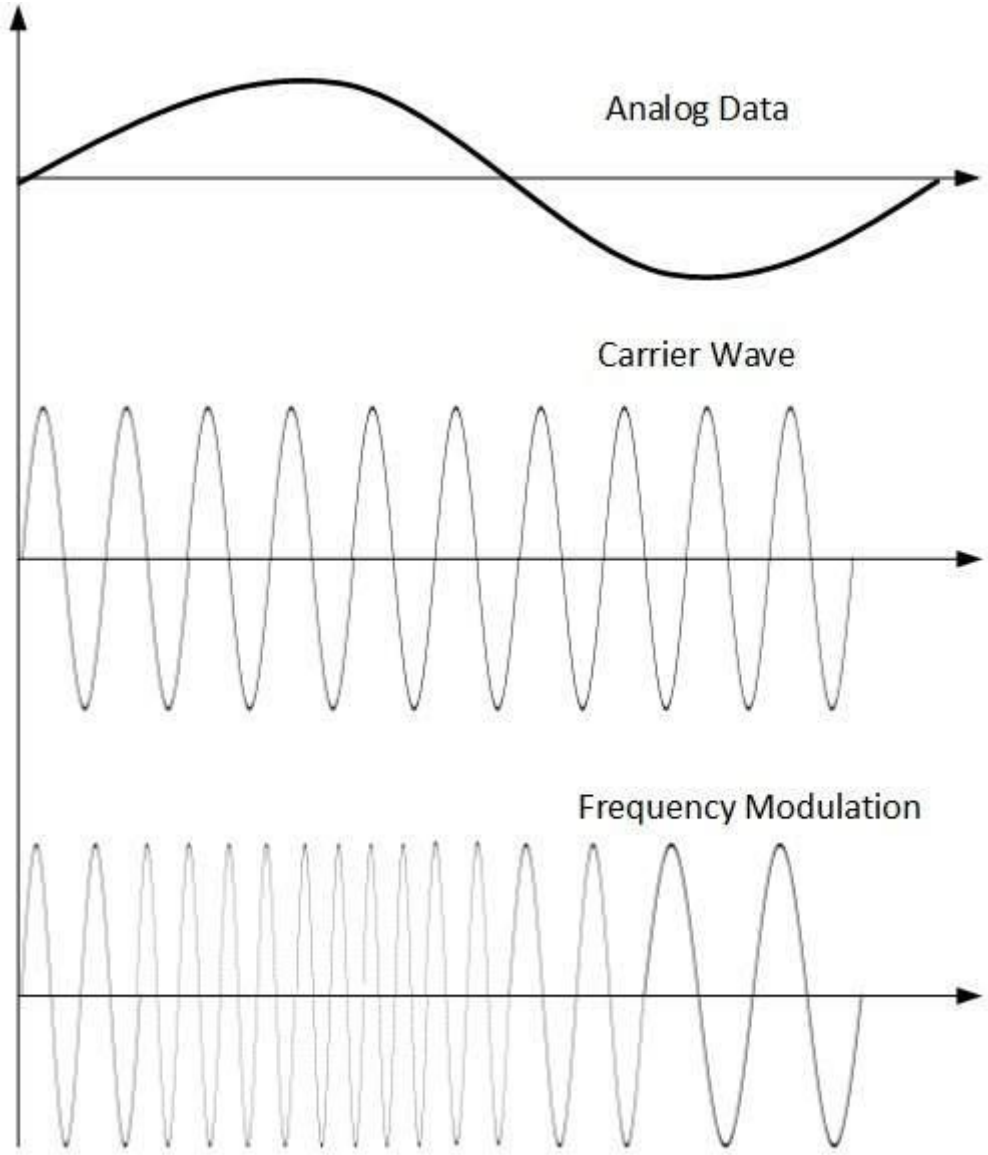


Amplitude modulation is implemented by means of a multiplier. The amplitude of modulating signal (analog data) is multiplied by the amplitude of carrier frequency, which then reflects analog data.

The frequency and phase of carrier signal remain unchanged.

- **Frequency Modulation**

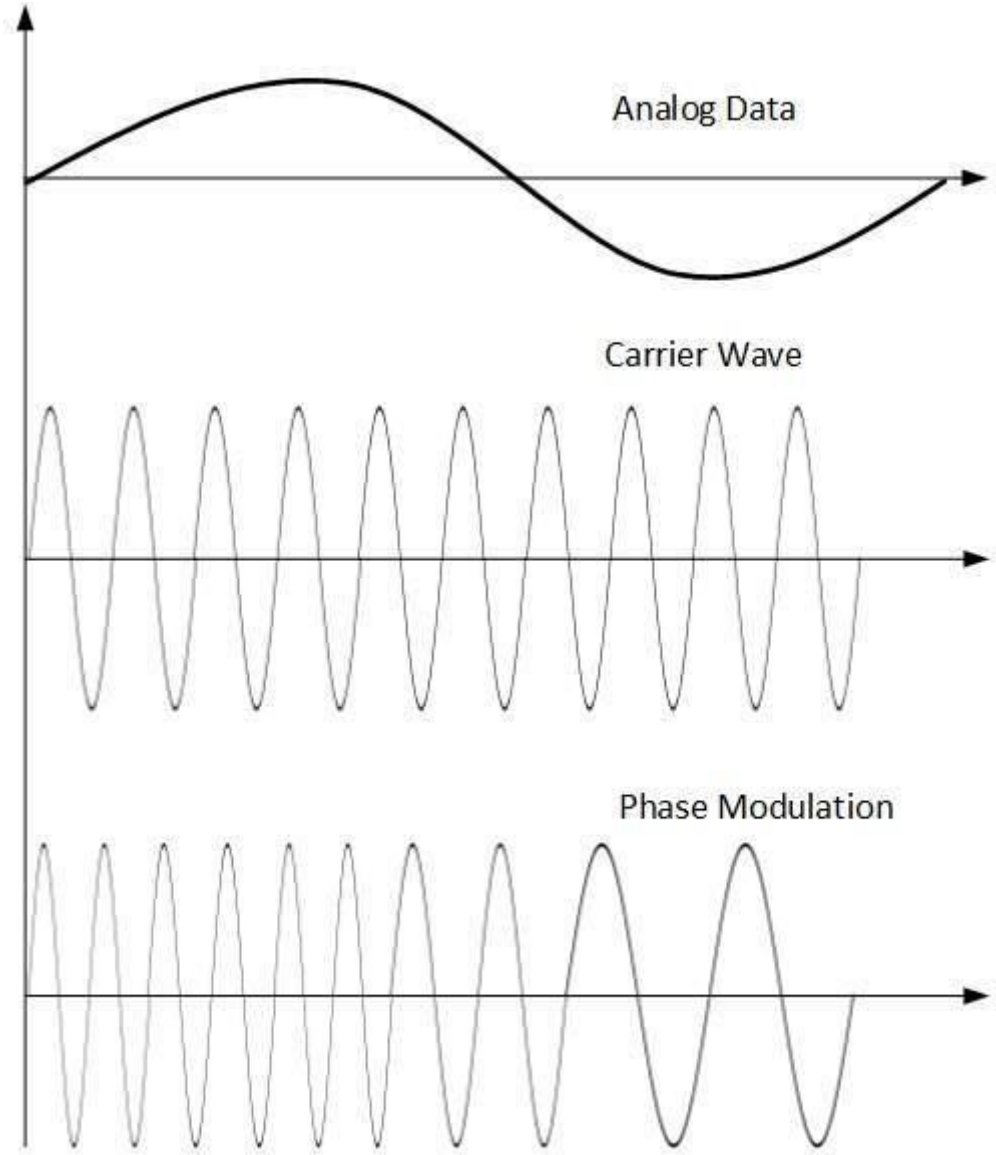
  In this modulation technique, the frequency of the carrier signal is modified to reflect the change in the voltage levels of the modulating signal (analog data).



The amplitude and phase of the carrier signal are not altered.

- **Phase Modulation**

  In the modulation technique, the phase of carrier signal is modulated in order to reflect the change in voltage (amplitude) of analog data signal.



Phase modulation is practically similar to Frequency Modulation, but in Phase modulation frequency of the carrier signal is not increased. Frequency of carrier is signal is changed (made dense and sparse) to reflect voltage change in the amplitude of modulating signal.

3.6 SUMMARY

In this unit we have discussed in detail about physical layer and also covered data and signals. We also explained about digital transmission. At the end of this unit also covered in detail analog transmission.

3.7 KEYWORDS

Analog signal, Digital signal, Noise, Switching, Multiplexing, Sampling, Quantization and Encoding.

3.8 QUESTIONS

1.Define analog and digital signal.

2. Describe line coding.

3. Elucidate amplitude shift keying.

4. Briefly explain analog to digital conversion.

3.9 REFERENCES

- WilliamStallings,DataandComputerCommunication,PrenticeHallofIndia
- BehrouzA.Forouzan,DataCommunicationandNetworking,McGraw-Hill
- AndrewS.Tanenbaum,ComputerNetworks, PrenticeHall.

UNIT 4: DATA LINK LAYER

Structure

4.0 OBJECTIVES

At the end of this unit, you should be able to

- Discuss data link layer
- Describe error detection and correction
- Explain multiple access protocols
- Elucidate virtual circuit switching
- Discuss frame relay and ATM

4.1 INTRODUCTION

The Data-link layer is the second layer from the bottom in the OSI (Open System Interconnection) network architecture model. It is responsible for the node-to-node delivery of data. Its major role is to ensure error-free transmission of information. DLL is also responsible to encode, decode and organize the outgoing and incoming data. This is considered the most complex layer of the OSI model as it hides all the underlying complexities of the hardware from the other above layers.

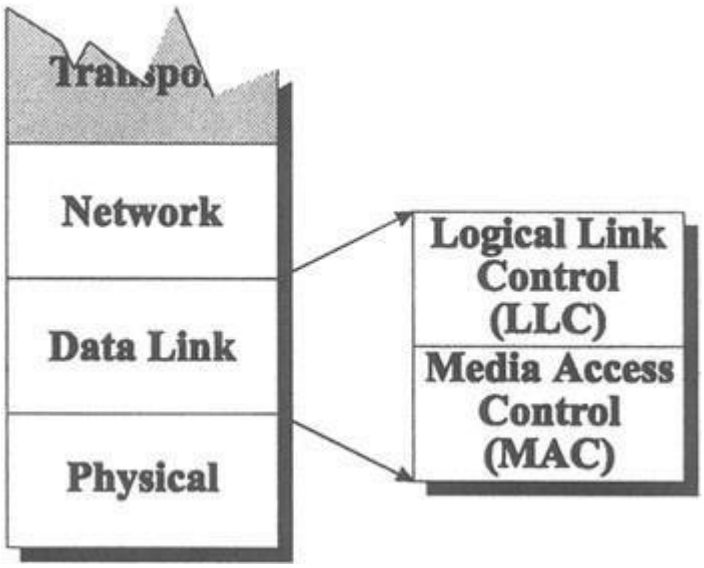
4.2 DATA LINK LAYER

FunctionsofDataLinkLayer:

Thedatalinklayertransformsthephysicallayer,arawtransmissionfacility,toalinkresponsibleforn

ode-to-node (hop-to-hop) communication. Specific responsibilities of the data link layer include framing,addressing, flow control, error control, and media access control. The data link layer divides the streamofbitsreceivedfromthenetworklayerintomanageabledataunitscalledframes.Thedatalinklayeraddsaheadertotheframetodefinetheaddressesofthesenderandreceiveroftheframe.Iftherateatwhichthe data are absorbed by the receiver is less than the rate at which data are produced in the sender, thedatalinklayerimposesaflowcontrolmechanismtoavoidoverwhelmingthereceiver.Thedatalinklayeralso adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged,duplicate, or lost frames. When two or more devices are connected to the same link, data link layerprotocolsarenecessarytodeterminewhichdevice hascontroloverthe linkat any given time.

OverviewofLogicalLinkControl(LLC)andMediaAccessControl(MAC):



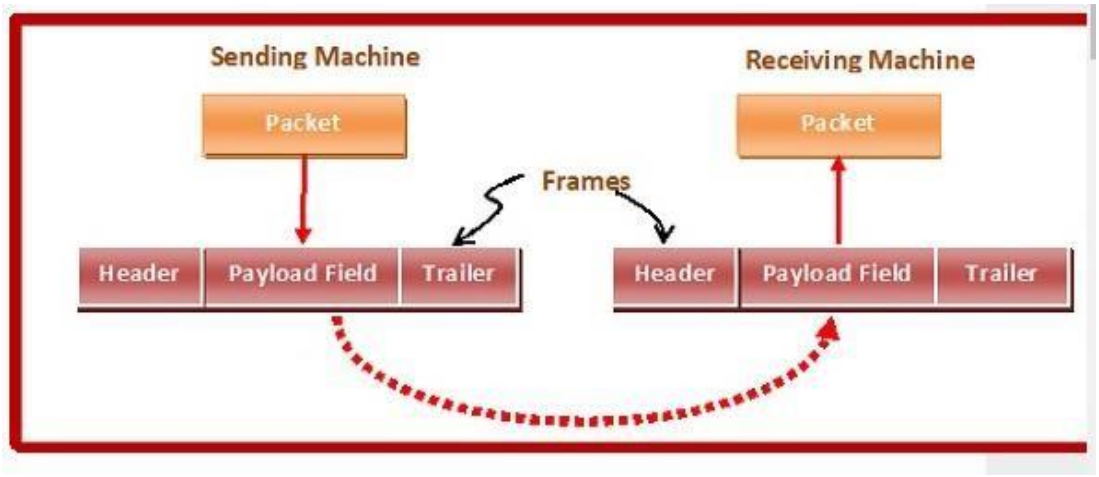
Thedatalinklayerisdividedinto two sublayers:

- The LLC sublayer acts as an interface between the media access control (MAC) sublayer and thenetwork layer. Logical Link Control (LLC) sublayer provides the logic for the data link. The LLCsublayer provides multiplexing mechanisms that make it possible for several network protocolsto coexist within a multipoint network and to be transported over the same network medium.Thus, it controls the synchronization, flow control, and error checking functions of the data linklayer.
- Media Access Control (MAC) sublayer provides control for accessing the transmission medium. Itis responsible for moving data packets from one network

interface to another, across a sharedtransmissionmedium.PhysicaladdressingishandledattheMACsublayer.Whensendingdatatoanother device on the network, the MAC sublayer encapsulates higher-level frames into framesappropriateforthetransmissionmedium,addsaframechecksequencetoidentifytransmissionerrors,andthenforwardsthedatatothephysicallayer.Additionally,theMACisalsoresponsibleforcompensatingfor collisionsbyinitiatingretransmissionifajamsignalisdetected.

Framing:

In the physical layer, data transmission involves synchronized transmission of bits from the source to thedestination. The data link layer packs these bits into frames. Data-link layer takes the packets from theNetwork Layer and encapsulates them into frames. If the frame size becomes too large, then the packetmay be divided into small sized frames. Smaller sized frames make flow control and error control moreefficient. Then, it sends each frame bit-by-bit on the hardware. At receiver's end, data link layer picks upsignalsfromhardwareandassembles themintoframes.



Partsofa Frame

Aframe hasthe followingparts−

Frame Header− Itcontains the sourceandthedestinationaddressesofthe frame.

Payloadfield−Itcontainsthe messagetobedelivered.

Trailer − It contains the error detection and error correction bits.Flag− Itmarks thebeginningandendofthe frame.

TypesofFraming

Framingcanbeoftwotypes,fixedsizedframingandvariablesizedframing.

Fixed-sizedFraming

Here thesizeoftheframeisfixedandsotheframelengthactsasdelimiterofthe frame.Consequently,itdoes not requireadditional boundary bitstoidentifythestart andendoftheframe.

Example −ATMcells.

Variable–SizedFraming

Here, the size of each frame to be transmitted may be different. So additional mechanisms are kept tomarktheendofoneframeandthebeginningofthe next frame.

Itis used inlocalarea networks.

FlowControlMechanisms:

Flow control coordinates the amount of data that can be sent before receiving an acknowledgment andis one of the most important duties of the data link layer. In most protocols, flow control is a set ofproceduresthattellsthesenderhowmuchdataitcantransmitbeforeitmustwaitforanacknowledgmentfromthereceiver.Theflowofdatamustnotbeallowedtooverwhelmthereceiver.Anyreceiving device has a limited speed at which it can process incoming data and a limited amount ofmemory in which to store incoming data. The receiving device must be able to inform the sending devicebefore those limits are reached and to request that the transmitting device

send fewer frames or stoptemporarily. Incoming data must be checked and processed before they can be used. The rate of suchprocessingisoftenslowerthantherateoftransmission.Forthisreason,eachreceivingdeviceha sablockofmemory,calledabuffer,reservedforstoringincomingdatauntiltheyareprocessed.Iftheb ufferbeginsto fill up, the receiver must be able to tell the sender to halt transmission until it is once again able toreceive.

When a data frame is sent from one host to another over a single medium, it is required that the senderand receiver should work at the same speed. That is, sender sends at a speed on which the receiver canprocess and accept the data. If sender is sending too fast, the receiver may be overloaded and data maybe lost.

Twotypesofmechanismscanbe deployedtocontrolthe flow:

- AsimplestopandwaitProtocol

Sliding Window Protocol

4.3 ERRORDETECTIONANDCORRECTIONTECHNIQUES:

Networks must be able to transfer data from one device to another with acceptable accuracy. For mostapplications, a system must guarantee that the data received are identical to the data transmitted.

Anytimedataaretransmittedfromonenodetothenext,theycanbecomecorruptedinpassage.Manyf actorscan alter one or more bits of a message. Some applications require a mechanism for detecting andcorrectingerrors.

Someapplicationscantolerateasmalllevelof error.Forexample,randomerrorsinaudioorvideotrans missionsmaybetolerable,but whenwe transfertext,we expect averyhighlevelofaccuracy.

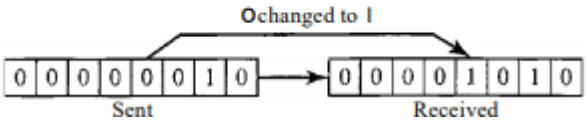
TypesofErrors:

Whenever bits flow from one point to another, they are subject to unpredictable changes because ofinterference. This interference can change the shape of the signal. In a single-bit error, a 0 is changed toa 1or a1toa 0.Ina bursterror,multiplebits arechanged.

Single-BitError:

The term single-bit error means that only 1 bit of a given data unit (such as a byte, character, or packet)is changed from1to0or from0to1.

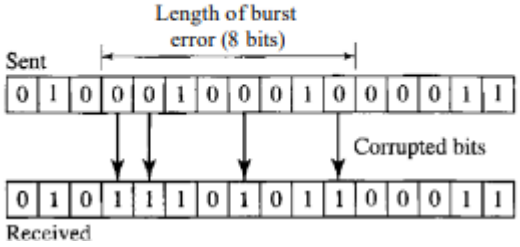
Single-bit error



BurstError:

Thetermburst errormeansthat2ormorebitsin thedata unit have changed from1 to0or from0to1.

Burst error oflength 8



A burst error is more likely to occur than a single-bit error. The duration of noise is normally longer thanthe duration of 1 bit, which means that when noise affects data, it affects a set of bits. The number ofbits affecteddepends onthe data rate anddurationofnoise.

Redundancy

Thecentralconceptindetectingorcorrectingerrorsisredundancy.Tobeabletodetectorcorrecterrors,we need to send some extra bits with our data. These redundant bits are added by the sender andremovedbythe receiver.Their presence allowsthe receiver to detectorcorrectcorruptedbits.

DetectionVersusCorrection

Thecorrectionoferrorsismoredifficultthanthedetection.Inerrordetection,wearelookingonlytoseeif any error has occurred. The answer is a simple yes or no. We are not even interested in the number oferrors.Asingle-biterroristhesameforusasabursterror.Inerrorcorrection,weneedtoknowtheexactnumber of bits

that are corrupted and more importantly, their location in the message. The number ofthe errors and the size of the message are important factors. If we need to correct one single error in an8-bit data unit, we need to consider eight possible error locations; if we need to correct two errors in adataunit ofthesamesize,we need toconsider28possibilities.

ForwardErrorCorrectionVersusRetransmission

There are two main methods of error correction. Forward error correction is the process in which thereceiver tries to guess the message by using redundant bits. This is possible if the number of errors issmall.Correctionbyretransmissionisatechniqueinwhichthereceiverdetectstheoccurrenceofan errorandasksthesendertoresendthemessage.Resendingisrepeateduntilamessagearrivesthatther eceiverbelieves iserror-free.

ErrorDetectingCodes

Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoidthis, we use error-detecting codes which are additional data added to a given digital message to help usdetectif anyerror hasoccurred duringtransmissionofthemessage.

Some populartechniquesforerror detectionare:

- Parity
- Checksum
- Cyclicredundancycheck

Paritycheck

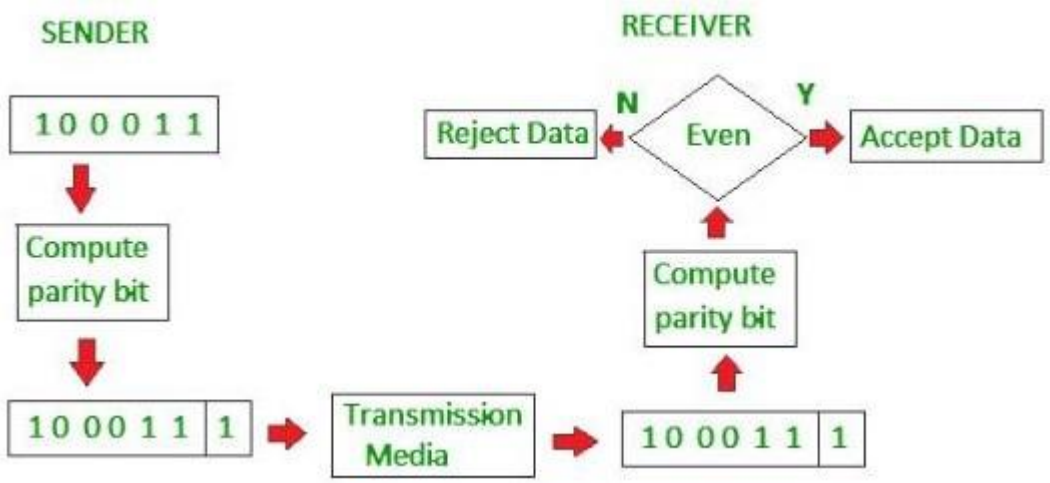
The most common and least expensive mechanism for error- detection is the parity check. The paritycheck is done by adding an extra bit, called parity bit to the data to make a number of 1s either even incaseofevenparityoroddincaseofoddparity.Whilecreatingaframe,thesender countsthenumberof1sin itandadds theparitybit in the followingway:

- Incaseofevenparity:Ifanumberof1siseventhenparitybitvalueis0.Ifthenumberof1sisod d,then paritybitvalueis1.
- Incaseofoddparity:Ifanumberof1sisoddthenparitybitvalueis0.Ifanumberof1siseven,t

hen paritybitvalueis1.

On receiving a frame, the receiver counts the number of 1s in it. In case of even parity check, if the countof1siseven,theframeisaccepted,otherwise,itisrejected.Asimilarruleisadoptedforoddparit ycheck.

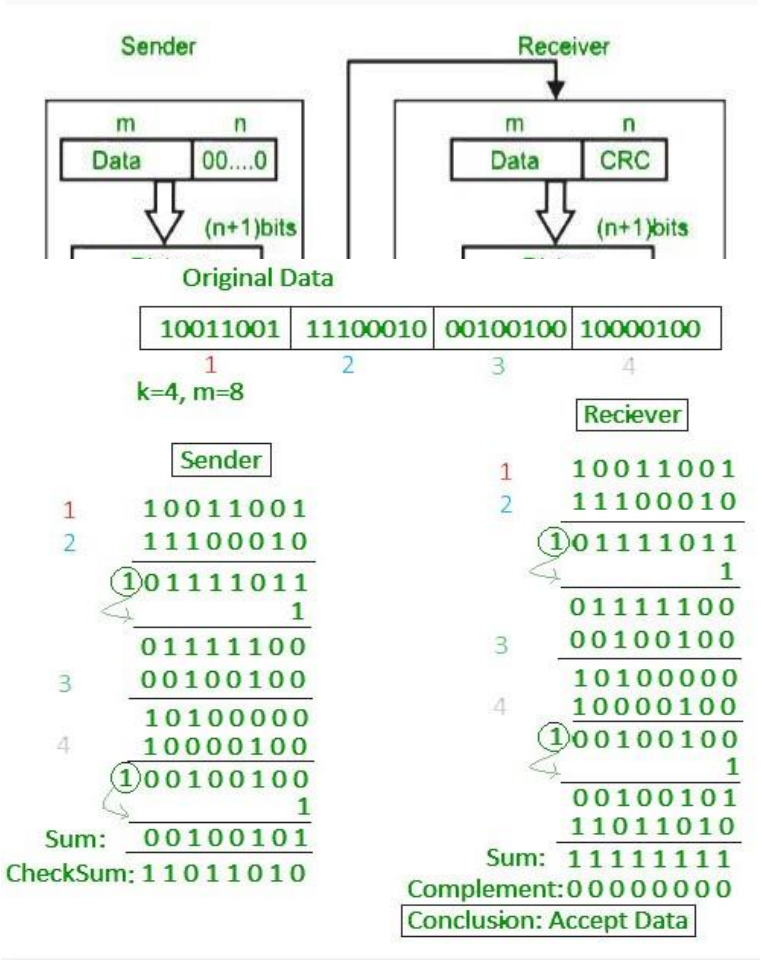
Theparitycheck issuitableforsinglebiterrordetectiononly.



Checksum

Inthiserrordetectionscheme,the following procedure isapplied:

- Dataisdividedinto fixedsizedframesorsegments. (ksegmentseachofm bits)
- Thesenderaddsthesegmentsusing1'scomplementarithmetictogetthesum.Itthen complementsthesumtoget thechecksumandsendsit alongwiththedataframes.
- Thereceiveraddstheincomingsegmentsalongwiththechecksumusing1'scomplement arithmeticto getthesum andthencomplementsit.

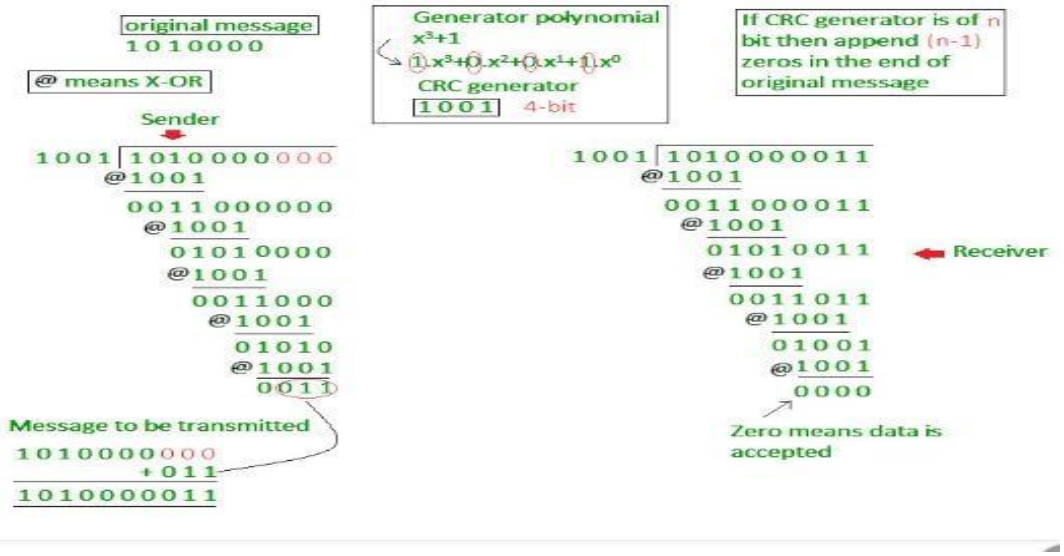


- Iftheresultiszero,thereceivedframes areaccepted;otherwise,theyare discarded.

CyclicRedundancyCheck:

Acyclicredundancycheck(CRC)isanerror-detectingcodecommonlyusedindigitalnetworksandstoragedevices to detect accidental changes to raw data. Unlike checksum scheme, which is based on addition,CRCisbasedonbinarydivision.InCRC,asequenceofredundantbits,calledcyclicredundancycheckbits,areappendedtotheendofdataunitsothattheresultingdataunitbecomesexactlydivisiblebyasecond,predeterminedbinarynumber.Atthedestination,theincomingdataunitisdividedbythesamenumber.If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted. Aremainderindicatesthatthedataunit has beendamaged intransit andtherefore must berejected.Atthesenderside,thedataunittobetransmittedISdividedbyapredetermineddivisor(binarynumber)in order to obtain the remainder. This remainder is called CRC. The CRC has one bit less than the divisor.It means that if CRC is of n bits, divisor is of n+ 1 bit. The sender appends this CRC to the end of data unitsuch that the resulting data unit becomes exactly divisible by predetermined divisor i.e. remainderbecomes zero. At the destination, the incoming data unit i.e. data + CRC is divided by the same number(predetermined binary divisor). If the remainder after division is zero then there is no error in the dataunit &

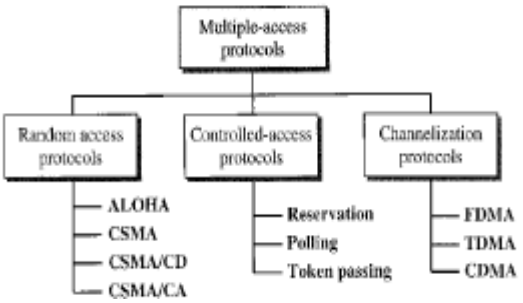
receiver accepts it. If remainder after division is not zero, it indicates that the data unit has beendamagedintransitandthereforeitisrejected.Thistechniqueismorepowerfulthantheparityche ckandchecksum error detection.



4.5 MULTIPLEACCESSPROTOCOLS(CHANNELALLOCATIONTECHNIQUES)

When nodes or stations are connected and use a common link, called a multipoint or broadcast link, weneedamultipleaccessprotocoltocoordinateaccesstothelink.Manyformalprotocolshavebeend

Taxonomy of multiple-access protocols discussed in this chapter



evisedto handleaccess toasharedlink. Wecategorizethemintothree groups.

Randomaccess:

In random access or contention methods, no station is superior to another station and none is

assignedthecontroloveranother.Nostationpermitsordoesnotpermitanotherstationtosend.Ateachinstance,astationthathastosendusesaproceduredefinedbytheprotocoltomakeadecisiononwhetherornottosend.Thisdecisiondependsonthestateofthemedium(idleorbusy).Inotherwords,eachstationcantransmitwhen it desiresontestingofthe stateofthemedium.

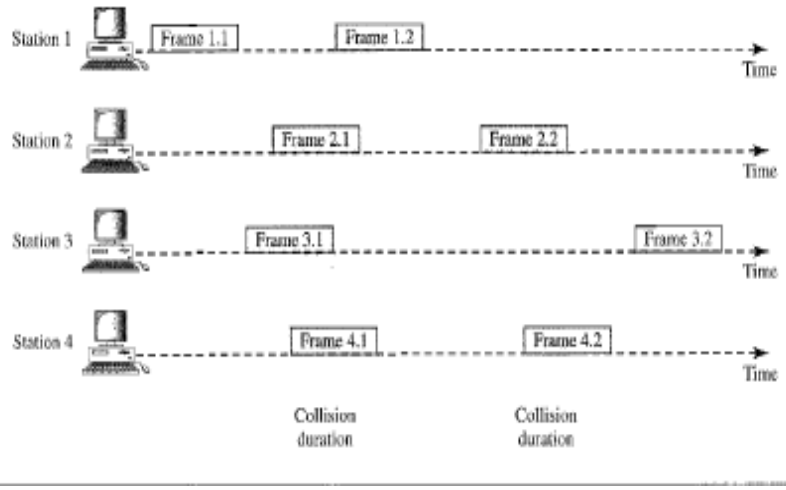
ALOHA:

ALOHA is the earliest random-access method developed for wireless LAN but can be used on any sharedmedium.Inthis,multiplestationscantransmitdataatthesametimeandcanhenceleadtocollision.Thedatafromthe twostationscollide.

PureALOHA:

Theideabehindthisprotocolisthateachstationsendsaframewheneverithasaframetosend.However,since there is only one channel to share, there is possibility of collision between frames from differentstations. Even if one bit of a frame coexists on the channel with one bit from

Figure 12.3 *Frames in a pure ALOHA network*



another frame, there is acollisionandbothwill bedestroyed.

The pure ALOHA protocol relies on acknowledgements from the receiver. When a station sends a frame,it expects the receiver to send an acknowledgement. If the acknowledgement does not arrive after thetime out period, the station assumes that the frame (or the acknowledgement) has been destroyed andresendstheframe.Acollisioninvolvestwoormorestations.Ifallthesestationstrytoresendtheirf

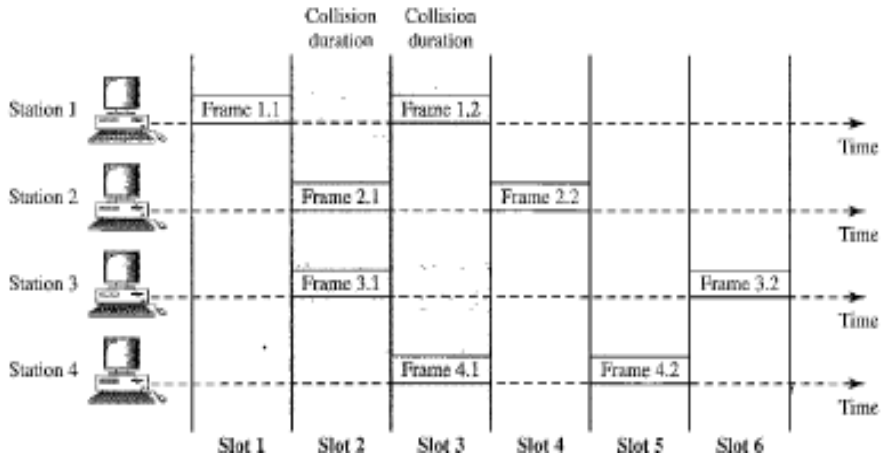
ramesafterthetimeoutperiodpasses,eachstationwaitsarandomamountoftimebeforeresendingits frame.Therandomnesswillhelpavoidmorecollisions,calledback-offtime.Sincedifferentstationsmaywaitfordifferent amount oftime,theprobability offurthercollisiondecreases.

SlottedALOHA:

In pure ALOHA, there is no rule that defines when the station can send. A station may send soon afteranotherstationhasstartedorsoonbeforeanotherstationhasfinished.So,stillthe collisionmayoccur.

Slotted ALOHA is similar to pure ALOHA, except that we divide time into slots and sending of data isallowed only at the beginning of these slots. If a station misses out the allowed time, it must wait for thenextslot.This reducestheprobabilityof collision.

Figure 12.6 *Frames in a slotted ALOHA network*



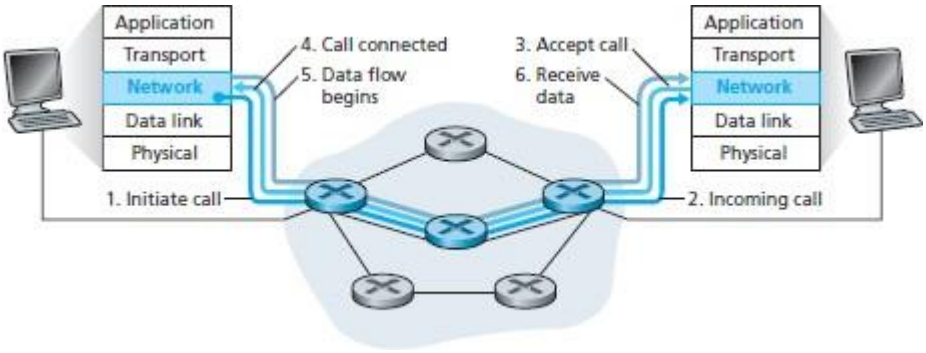
Allowing a station to send only at the beginning of the time slot means that the station sending in theprevious slot has finished sending its frame already. However, there is still possibility of collision if twostationstry tosendat thebeginningof thesame timeslot.

4.6 VIRTUALCIRCUITSWITCHING

Virtual circuit switching is a packet switching methodology whereby a path is established between thesource and the final destination through which all the packets will be routed during a call. This path iscalled a virtual circuit because to the user, the connection appears to be a dedicated physical

circuit.However,othercommunicationsmayalsobesharingthepartsofthesamepath.So,virtualci rcuitpacketswitchingis connectionoriented.

Before the data transfer begins, the source and destination identify a suitable path for the virtual circuit.All intermediate nodes between the two points put an entry of the routing in their routing table for thecall. Additional parameters, such as the maximum packet size, are also exchanged between the sourceandthe destinationduringcallsetup.Thevirtual circuitisclearedafterthedatatransfer is completed.



Advantagesofvirtualcircuit switchingare:

- Packetsare deliveredinorder, sincetheyall takethesameroute;
- The overhead in the packets is smaller, since there is no need for each packet to contain the fulladdress;
- Theconnectionismorereliable,networkresourcesareallocatedatcallsetupsothatevendur ingtimes of congestion, provided that a call has been setup, the subsequent packets should getthrough;
- Billingiseasier,sincebillingrecordsneedonlybe generatedper callandnot perpacket.

4.7 FRAMERELAY

Frame Relay is a virtual-circuit wide-area network that was designed in response to demands for a newtypeofWAN. FrameRelay is a wideareanetworkwiththe followingfeatures:

1. Frame Relayoperatesatahigher speed(1.544Mbps andrecently44.376Mbps).

2. Frame Relay operates in just the physical and data link layers. This means it can easily

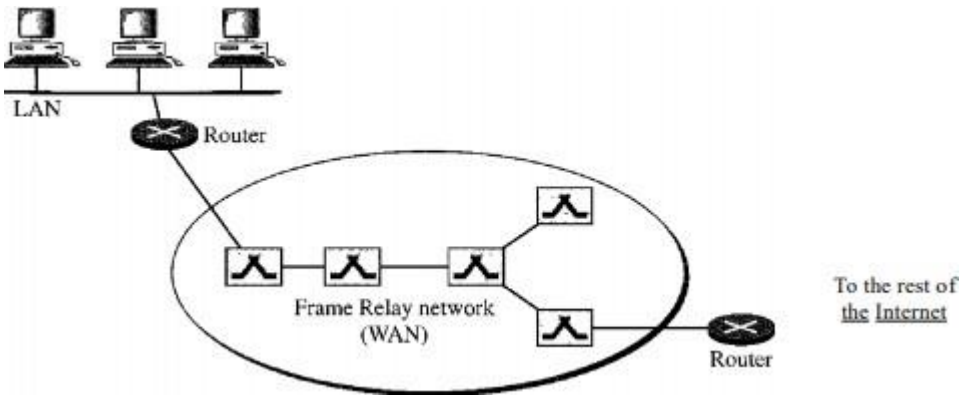
be used as abackbone network to provide services to protocols that already have a network layer protocol, such asthe Internet.

3. FrameRelayallowsburstydata.

4. Frame Relay allows a frame size of 9000 bytes, which can accommodate all local area network framesizes.

5. FrameRelayislessexpensive thanothertraditionalWANs.

6. Frame Relay has error detection at the data link layer only. There is no flow control or error control.There is not even a retransmission policy if a frame is damaged; it is silently dropped. Frame Relay wasdesigned in this way to provide fast transmission capability for more reliable media and for thoseprotocolsthathaveflowanderrorcontrolat thehigher layers.



Framerelayisavirtualcircuitpacketswitchingtechnologythatfragmentedintotransmissionunits calledframesandsentinhigh-speedburststhroughadigitalnetwork.Establishesanexclusiveconnectionduringthe transmission period called virtual connection. Frame relay puts data in a variable-size unit called aframe and leaves any necessary error correction (retransmission of data) up to the endpoints, whichspeeds up overall data transmission. Configuring user equipment in a Frame Relay network is extremelysimple. The connection-oriented service provided by Frame Relay has properties like non-duplication offrames,preservationoftheframetransferorderandsmallprobabilityofframeloss.ThefeaturesprovidedbyFrameRelaymakeitoneofthebestchoicesforinterconnectinglocalareanetworksusing awideareanetwork. However, the drawback in this method is that it becomes prohibitively expensive with growthof thenetwork.

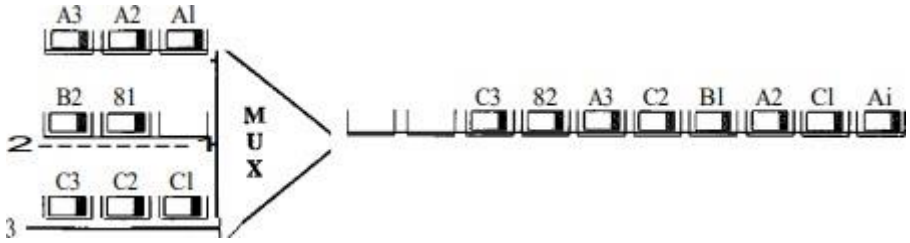
Thereare certain benefitswhichare associatedwithFrameRelay.

- Ithelpsinreducingthecostofinternetworking,asthereisconsiderablereductioninthenumberof circuitsrequiredandtheassociated bandwidths.
- Ithelpsinincreasingthe performance dueto reducednetworkcomplexity.
- Itincreases theinteroperabilitywiththehelpofinternationalstandards.
- FrameRelayisprotocolindependentandcaneasilybeusedtocombinetrafficfromothernetworkingprotocols.

In business scenarios, where there is a slow connection or continuous traffic flow due to applications likemultimedia,FrameRelay isnot arecommended choice.

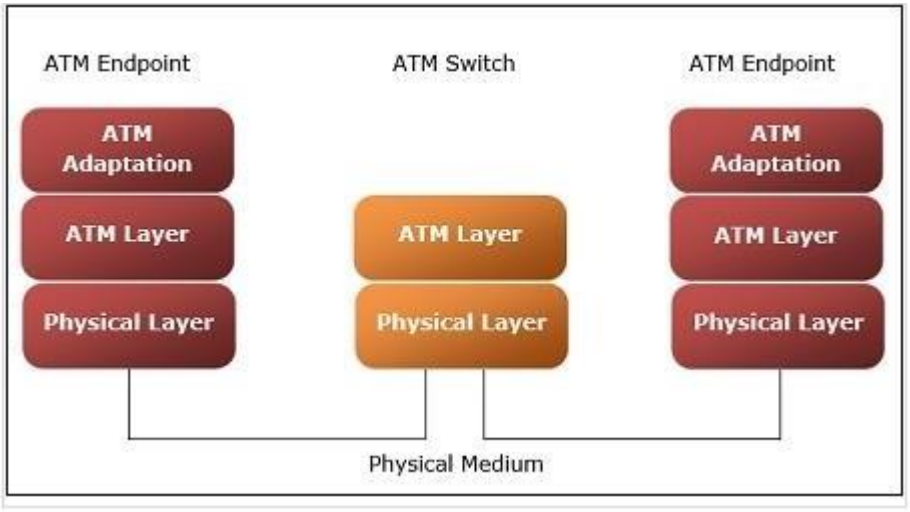
4.8 ATM

Asynchronous transfer mode (ATM) is a switching technique used by telecommunication networks thatuses asynchronoustime-divisionmultiplexingto encode dataintosmall,fixed-sizedcells.



ATMnetworksareconnection-orientednetworksthatsupportsvoice,videoanddatacommunications.Itencodes data into small fixed - size cells so that they are suitable for TDM and transmits them over aphysicalmedium.

Thesizeof anATMcellis 53bytes: 5-byteheaderand48-byte payload.



PhysicalLayer−Thislayercorrespondstophysicallayerof OSImodel.Atthislayer,thecellsareconverted intobitstreamsandtransmittedoverthephysicalmedium.

ATMLayer−Thislayeriscomparabletodatalinklayerof OSImodel.Itacceptsthe48-bytesegmentsfromthe upper layer, adds a 5-byte header to each segment and converts into 53-byte cells. This layer isresponsiblefor routingofeachcell,trafficmanagement, multiplexingandswitching.

ATM Adaptation Layer −This layer corresponds to network layer of OSI model. It provides facilities to theexisting packet switched networks to connect to ATM network and use its services. It accepts the dataandconvertsthemintofixed sized segments.

BenefitsofATMNetworksare

- Itprovidesthedynamicbandwidththatisparticularlysuitedforburstytraffic.
- Sincealldataareencodedintoidenticalcells,datatransmissionissimple,uniformandpredictable.
- Uniformpacketsizeensuresthatmixedtrafficishandledefficiently.
- Smallsizedheaderreducespacketoverload,thusensuringeffectivebandwidthusage.
- ATM networksarescalablebothinsize andspeed.

4.9 SUMMARY

In this unit, we were able to see about the concept of data link layer. We were also able to clearly discuss on the importance error correction and detection. And also know n about the concepts of data link control and multiple access. At the end of this unit discussed about virtual circuit networks such as frame relay and ATM.

4.10 KEYWORDS

LLC, Framing, Burst error, CRC, ALOHA, Frame relay and ATM

4.11 QUESTIONS

1. Describe cyclic redundancy check.
2. Explain briefly ALOHA.
3. Write a short note on ATM
4. Discuss frame relay.
5. Explain virtual-circuit switching

4.12 REFERENCES

1. Carl Hamacher, ZvonkoVranesic, SafwatZaky: **Computer Organization**, 5th Edition, TMH 2002
2. William Stallings: **Computer Organization and Architecture,** 7th Edition, PHI 2006
3. Vincenet P. Heuring and Harry F. Jordan: **Computer Systems Design and Architecture,** 2nd Edition, Pearson Education, 2004