MAR GREGORIOS COLLEGE OF ARTS & SCIENCE

Block No.8, College Road, Mogappair West, Chennai – 37

Affiliated to the University of Madras
Approved by the Government of Tamil Nadu
An ISO 9001:2015 Certified Institution

DEPARTMENT OF ELECTRONICS & COMMUNICATION SCIENCE

SUBJECT NAME: COMPUTER NETWORKS

SUBJET CODE: TAG6C

SEMESTER: VI

PREPARED BY: PROF.V.SAVITHRI / PROF.S.SHANTHA

COMPUTER NETWORKS (SYLLABUS)

UNIT I

INTRODUCTION TO COMPUTER NETWORKS – Uses of network – Network structure – The OSI referencemodel concepts – Layers of the OSI model.

UNIT II

THE PHYSICAL LAYER – Different types of transmission medium - CODEC – Switching techniques – Channelallocation methods – ALOHA protocol-LAN protocol (any one protocol) – IEEE standards 802.3, 802.4 and 802.5.

UNIT III

THE DATA LINK LAYER – design issues – Concept of framing – Different methods – Error detection andcorrection: Single error correction and cyclic redundancy check.

UNIT IV

THE NETWORK LAYER – design issues – Internal organization of network layer – Congestion controlalgorithm, Leaky bucket algorithm and token bucket algorithm – Dijikstra routing algorithm.

UNIT V

Repeaters, bridges, routers and gateways – Brief introduction to the transport layer, session layer, presentation layer and application layer-Basic concepts of Internet – WWW.

UNIT –I

INTRODUCTION

When we communicate, we are sharing information. This sharing can be local orremote.

- Between individuals, local communication usually occurs face to face, while remotecommunication takes place over distance. The telecommunication which includes,telephony, telegraphy and television, means communication at a distance (tele isGreekwordforfardistance).
- The word **data** refers to facts, concepts and instructions presented in the variety offorsuchasnumbers,text,bitsandbytes.
- Incomputer, data ar erepresented by binary information units produced andconsumedintheformof0sand1s.
- **Data communication** refers to the exchange of data between a two devices such assourceandreceiver,viasomeformoftransmissiondevices.
- The device that transmits the data is known as **source** and the device that receivesthetransmitteddataisknownas**receiver**.

CharacteristicsofDataCommunication

The effectiveness of data communication system depends on the three *fundamentalcharacteristics*:

Delivery: The system must deliver data to the correct destination.Datamustbereceivedbytheintendeddevice oruser.

Accuracy : Thesystemmustdeliverdataaccurately.

Timeliness : The system must deliver data in timely manner in the sameorderastheyareproduced.

AdvantagesofaComputerNetwork

Helpsustoconnectwithmultiplecomputerstogethertosendandreceiveinformationwhen accessingthenetwork.

Helpsustoshareprinters,scanners,andemail.

Helpsustoshareinformationatveryfastspeed

Electroniccommunicationismoreefficientandlessexpensivethanwithoutthenetwork.

DisadvantagesofusingComputerNetworks

Investmentforhardwareandsoftwarecanbecostlyforinitialset-up

Ifwedon'ttakepropersecurityprecautionslikefileencryption,firewallsthenourdatawillbeatrisk.

Somecomponentsofthenetworkdesignmaynotlastformanyyears,anditwillbecome uselessormalfunctionandneedtobereplaced.

Requirestimeforconstantadministration

Frequentserverfailureandissuesofregularcablefaults

Uses of Computer Network

BusinessApplications

to distribute information throughout the company (**resource sharing).**sharingphysicalresourcessuchasprinters,andtapebackupsystems,issharinginformation

client-servermodel.Itiswidelyusedandformsthebasisofmuchnetwork usage.

communication mediumamong employees.**email**(**electronic mail**),whichemployeesgenerallyuseforagreatdealofdailycommunication.

Telephonecallsbetweenemployeesmaybecarriedbythecomputernetwork insteadofbythephonecompany.ThistechnologyiscalledIP**telephony**or **VoiceoverIP**(**VoIP**)whenInternettechnologyisused.

Desktopsharingletsremoteworkersseeandinteractwithagraphicalcomputerscreen

doingbusinesselectronically,especiallywithcustomersandsuppliers.This newmodeliscalled**e-commerce**(**electroniccommerce**)and ithasgrownrapidlyinrecentyears.

2 HomeApplications

peer-to-peer communication

person-to-personcommunication

electronic commerce

entertainment.(gameplaying,)

3 MobileUsers

Textmessagingortexting

Smartphones,

GPS(GlobalPositioningSystem)

m-commerce

NFC(NearFieldCommunication)

4 SocialIssues

Withthegoodcomesthebad,asthisnew-foundfreedombringswithitmanyunsolvedsocial,political,andethicalissues.

Social networks,message boards,contentsharingsites,anda host ofotherapplicationsallowpeopletosharetheirviewswith like-mindedindividuals. As long as the subjects are restricted to technical topics or hobbieslikegardening,nottoomanyproblemswillarise.

Thetroublecomeswithtopicsthatpeopleactuallycareabout,likepolitics,religion, or sex. Views that are publicly posted may be deeply offensive to somepeople. Worse yet, they may not be politically correct. Furthermore, opinionsneednotbelimitedtotext;high-resolutioncolorphotographsandvideoclipsare easily shared over computer networks. Some people take a live-and-let-liveview, but others feel that posting certain material (e.g., verbal attacks onparticular countries or religions, pornography, etc.) is simply unacceptable andthat such content must be censored. Different countries have different andconflictinglawsinthisarea.Thus,thedebaterages.

Computer networks make it very easy to communicate. They also make iteasy for the people who run the network to snoop on the traffic. This sets upconflicts over issues such as **employee rights versus employer rights**.Many people read and write email at work. Many employers have claimed theright to read and possibly censor employee messages, including messages sentfromahomecomputeroutsideworkinghours.Notallemployeesagreewiththis,especiallythelatterpart.

Anotherconflictiscenteredaroundgovernmentversuscitizen’srights.

A new twist with mobile devices is location privacy. As part of the process ofproviding service to your mobile device the network operators learn where youare at different times of day. This allows them to track your movements. Theymayknowwhichnightclubyoufrequentandwhichmedicalcenteryouvisit

Features of Computer network

A list of Computer network features is given below.

- Communication speed
- File sharing
- Back up and Roll back is easy
- Software and Hardware sharing
- Security
- Scalability
- Reliability

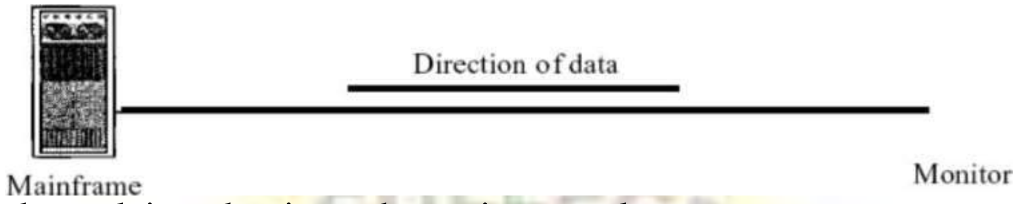
DataFlow

Communicationbetween twodevices canbe simplex,half-duplex, or full-duplex.

Simplex:

Insimplexmode,thecommunicationisunidirectional,asonaone-waystreet.Onlyoneof

the twodeviceson a linkcantransmit; theother canonly receive.The simplexmodecanusetheentirecapacityofthechanneltosenddatainonedirection.
Example:Keyboardsandtraditionalmonitors



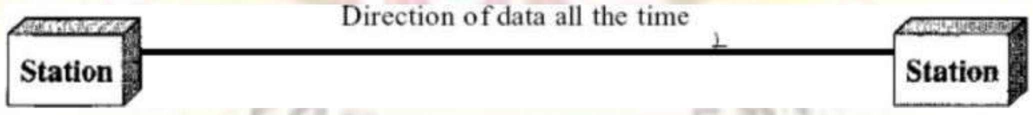
Thekeyboardcanonlyintroduceinput;themonitorcanonlyacceptoutput.

Half-Duplex:

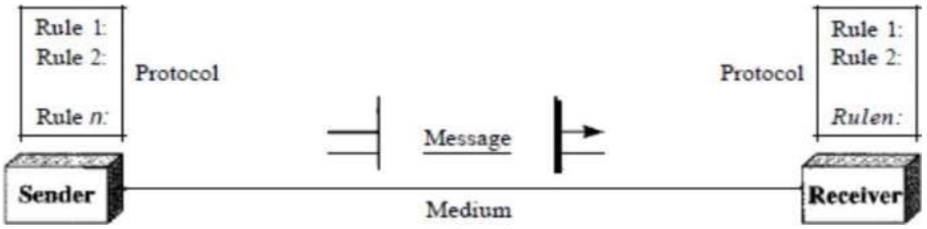
Inhalf-duplexmode,eachstationcanbothtransmitandreceive,butnotatthesametime.
Whenonedeviceissending,theothercanonlyreceive,andviceversa.
Thehalf-duplexmodeislikeaone-laneroadwithtrafficallowedinbothdirections.Inahalf-duplextransmission,theentirecapacityofachannelistakenoverbywhicheverofthetwodevicesistransmittingatthetime.
Ex.:Walkie-talkiesandCB(citizensband)radiosarebothhalf-duplexsystems.

Full-Duplex:

Infull-duplexbothstationscantransmitandreceivesimultaneously.Thefull-duplexmode is like a two-way street with traffic flowing in both directions at the same time.Infull-duplexmode,signalsgoinginonedirectionsharethecapacityofthelink:withsignalsgoingin theotherdirection.
Example:Thetelephonenetwork.Whentwopeoplearecommunicatingbyatelephoneline,bothcantalkandlistenatthesametime.



Componentsofdatacommunicationsystem



ACommunication system hasfollowing components:

1. **Message**:Itistheinformationordatatobecommunicated.Itcanconsistoftext,numbers,pictures,soundorvideooranycombinationofthese.
2. **Sender** **:**Thesenderisthedevicethatsendsthedatamessage.Itcanbeacomputer,workstation,telephonehandset,video,camera&soon.
3. **Receiver:**Thereceiveristhedevicethatreceivesthemessage.Itcanbecomputer,workstation,telephoneandsoon.
4. **Medium:**Thetransmissionmediumisthephysicalpathbywhichamessagetravelsfromsendertoreceiver.
5. **Protocol** **:**Acomputernetworkisagroupoftwoormoreinterconnectedcomputersystems.Youcanestablishanetworkconnectionusingeithercableorwirelessmedia.

NetworkCriteria

Anetworkmustbeabletomeetacertainnumberofcriteria.Themostimportantofthesearerperformance,reliability,andsecurity.

Performance

Performancecanbemeasuredinmanyways,includingtransittimeandresponsetime.*Transit time*istheamountoftimerequiredforamessagetotravelfromonedevicetoanother.*Responsetime*istheelapsedtimebetweenaninquiryandaresponse. The performance of a network depends on a number of factors, including thenumberofusers,thetypeoftransmissionmedium,thecapabilitiesoftheconnectedhardware,andtheefficiencyofthesoftware.

Reliability

Inadditiontoaccuracyofdelivery,networkreliabilityismeasuredbythefrequencyoffailure, the time it takes a link to recover from a failure, and the network's robustnessinacatastrophe.

Security

Networksecurityissuesincludeprotectingdatafromunauthorizedaccess,protectingdatafromdamageanddevelopment,andimplementingpoliciesandproceduresforrecoveryfrombreaches anddatalosses.

Internetworks

When two or more networks are connected, they become and internetwork. Individual networks are jointed into internetworks by the use of internetworking devices. These devices include sr outersand gateways.

The terminternet (lowercasei)isused tomeaninterconnection of networks and thetermInternet(Uppercasei)isaspecificworldwidenetwork.

Protocols

Incomputernetworks,communicationoccursbetweenentitiesindifferentsystems.Anentityisanythingcapableofsendingorreceivinginformation. Forcommunicationtooccur,theentitiesmustagreeonaprotocol.

Aprotocolisasetofrulesthatgoverndatacommunications.Aprotocoldefineswhatis communicated, how it is communicated, and whenit is communicated. The keyelementsofaprotocolaresyntax,semantics,andtiming.

o **Syntax :** The term *syntax* refers to the structure or format of the data, meaning theorder in which they are presented. For example, a simple protocol might expect thefirst8bitsofdatatobetheaddressofthesender,thesecond8bitstobetheaddressofthereceiver,andtherestofthestreamtobethemessageitself.

o **Semantics**:Theword*semantics* referstothemeaningofeachsectionofbits.

o **Timing** : The term *timing* refers to two characteristics: when data should be sent andhow fast they can be sent. For example, if a sender produces data at 100 Mbps but thereceiver can process data at only 1 Mbps, the transmission will overload the receiverandsomedatawillbelost.

Standards

Standards are essential in creating and maintaining an open and competitive marketforequipmentmanufacturersandinguaranteeingnationalandinternationalinteroperability of data and telecommunications technology and processes. Standardsprovide guidelines to manufacturers, vendors, government agencies, and other serviceproviders to ensure the kind of interconnectivity necessary in today's marketplace andininternationalcommunications.

Datacommunicationstandardsfallintotwocategories:*defacto*(meaning"byfact"or"byconvention")and*dejure*(meaning"bylaw"or"byregulation").

o De facto : Standards that have not been approved by an organized body but havebeen adopted as standards through widespread use are de facto standards. De factostandards are often established originally by manufacturers who seek to define thefunctionalityofanewproductortechnology.

o**Dejure:**Thosestandardsthathavebeenlegislatedbyanofficiallyrecognizedbodyaredejurest ndards.

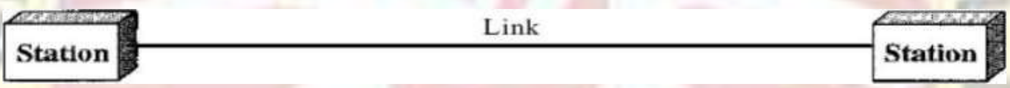
LineConfigurationorTypeofConnection

Lineconfigurationdefinestheattachmentofcommunicationdevicestoalink.

Alinkisthephysicalcommunicationpathwaythattransfersdatafromonedevicetoanother.Therear etwopossiblelineconfiguration.

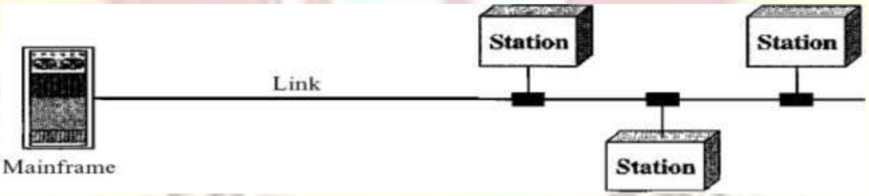
1. **Point-to-Point**

Point-to-pointlineconfigurationprovidesadedicatedlinkbetweentwodevices.Theentirecapacityofthe channelisreservedfortransmissionbetweenthosetwodevices.



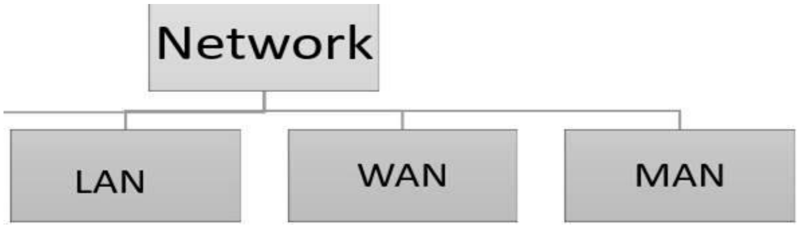
2. **Multipoint**

A Multipoint lineconfiguration isone inwhichmore thattwospecific devicesshare asinglelink.Here,thecapacityofthechannelisshared,eitherspatiallyortemporarily.Ifsever al**devicescanusethelinksimultaneously,itisaspatiallysharedlineconfiguration.Ifuse rsmusttaketurns,itisatime-sharedlineconfiguration.**



TypesofNetwork

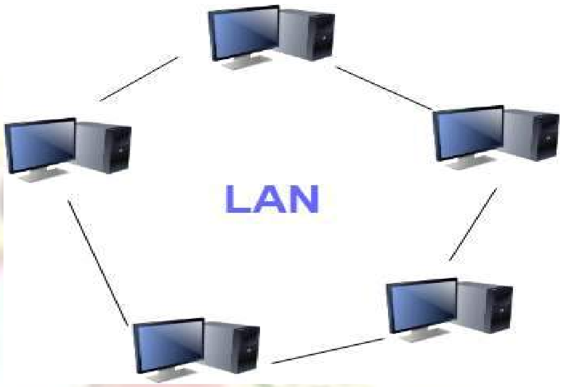
Therearevarioustypesofcomputernetworksavailable.Wecancategorize]



themaccordingtotheirsizeaswellastheirpurpose.Thesizeof a network should beexpressed by the geographic area and number of computers, which are a part of theirnetworks.Itincludesdeviceshousedinasingleroom to millions of devices spreadacrosstheworld.Someofthemostpopularnetworktypesare:

LAN (Local Area Network) :

A LAN is a group of computer and peripheral devices which are connected in a limited area such as school, laboratory, home, and office building. It is a widely useful network for sharing resources like files, printers, games, and other application. It is a network which consists of less than 5000 interconnected devices across several buildings.



Characteristics of LAN

- It is a private network, so an outside regulatory body never controls it.
- LAN operates at a relatively higher speed compared to other WAN systems.
- There are various kinds of media access control methods like token ringand ethernet.

Advantages of LAN

- We can use the same software over the network instead of purchasing thelicensed software for each client in the network.
- Data of all network users can be stored on a single hard disk of the servercomputer.
- We can easily transfer data and messages over networked computers.
- LAN offers the facility to share a single internet connection among all theLAN users.

Disadvantages of LAN

- LAN will indeed save cost because of shared computer resources, but theinitial cost of installing Local Area Networks is quite high.
- The LAN admin can check personal data files of every LAN user, so it doesnot offer good privacy.
- Unauthorized users can access critical data of an organization in case LANadmin is not able to secure centralized data repository.
- Local Area Network requires a constant LAN administration as there areissues related to software setup and hardware failures

Characteristics of WAN:

- The software files will be shared among all the users; therefore, all canaccess to the latest files.
- Any organization can form its global integrated network using WAN.

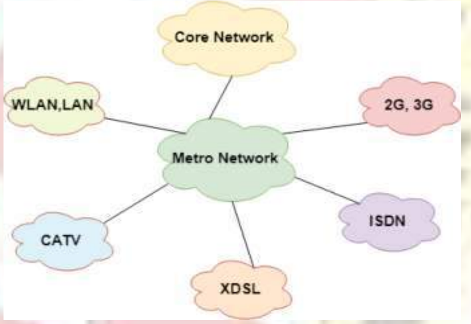
Advantages of WAN

- WAN helps you to cover a larger geographical area. Therefore businessoffices situated at longer distances can easily communicate.
- Contains devices like mobile phones, laptop, tablet, computers, gamingconsoles, etc.
- WLAN connections work using radio transmitters and receivers built intoclient devices.

Disadvantage of WAN

- The initial setup cost of investment is very high.
- It is difficult to maintain the WAN network. You need skilled techniciansand network administrators.
- There are more errors and issues because of the wide coverage and the useof different technologies.
- It requires more time to resolve issues because of the involvement ofmultiple wired and wireless technologies.
- Offers lower security compared to other types of networks.

MAN (Metropolitan Area Network) MAN is consisting of a computernetwork across an entire city, collegecampus, or a small region. This typeof network is large than a LAN,which is mostly limited to a singlebuilding or site. Depending upon thetype of configuration, this type of network allows you to cover an areafrom several miles to tens of miles.



Characteristics of MAN

- It mostly covers towns and cities in a maximum 50 km range
- Mostly used medium is optical fibers, cables
- Data rates adequate for distributed computing applications.

Disadvantages of MAN

- We need more cable to establish MAN connection from one place to another.
- In MAN network it is tough to make the system secure from hackers

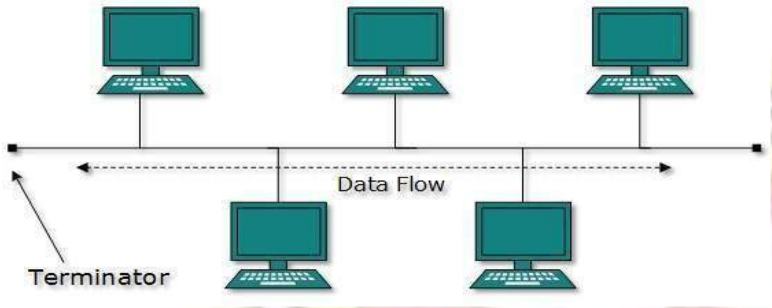
Advantages of MAN

- It offers fast communication using high-speed carriers, like fiber optic cables.
- It provides excellent support for an extensive size network and greater accessto WANs.
- The dual bus in MAN network provides support to transmit data in bothdirections concurrently.
- A MAN network mostly includes some areas of a city or an entire city.

Topology

A Network Topology is the arrangement with which computer systems or network devices are connected to each other. Topologies may define both physical and logical aspect of the network. Both logical and physical topologies could be same or different in a same network.

Bus Topology



- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
- The configuration of a bus topology is quite simpler as compared to other topologies.
- The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.
- The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).

CSMA: It is a media access control used to control the data flow so that data integrity is maintained, i.e., the packets do not get lost. There are two alternative ways of handling the problems that occur when two nodes send the messages simultaneo

Advantages of Bus topology:

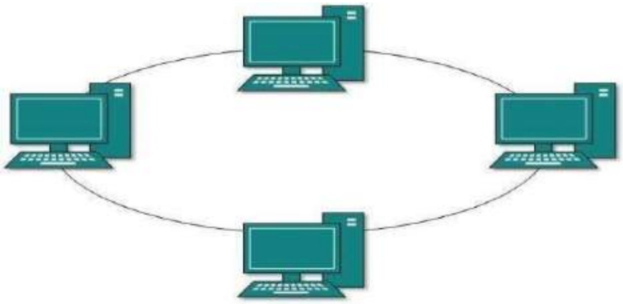
- **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
- **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.

- **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
- **Limited failure:** A failure in one node will not have any effect on other nodes.

Disadvantages of Bus topology:

- **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.
- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal..

Ring Topology



- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.
- The most common access method of the ring topology is **token passing**.
    - **Token passing:** It is a network access method in which token is passed from one node to another node.
    - **Token:** It is a frame that circulates around the network.

Working of Token passing

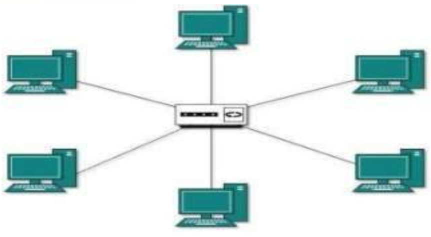
- A token moves around the network, and it is passed from computer to computer until it reaches the destination.
- The sender modifies the token by putting the address along with the data.
- The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.
- In a ring topology, a token is used as a carrier.

Advantages of Ring topology:

- **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- **Product availability:** Many hardware and software tools for network operation and monitoring are available.
- **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
- **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

Disadvantages of Ring topology:

- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Failure:** The breakdown in one station leads to the failure of the overall network.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.



Star Topology

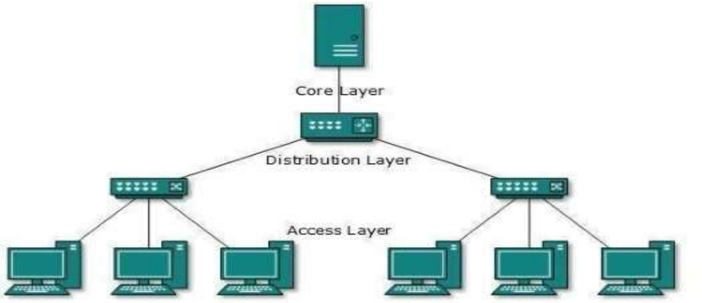
- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
- Coaxial cable or RJ-45 cables are used to connect the computers.
- Hubs or Switches are mainly used as connection devices in a **physical star topology**.
- Star topology is the most popular topology in network implementation.

Advantages of Star topology

- **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator has to go to the single station to troubleshoot the problem.
- **Network control:** Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
- **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
- **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
- **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
- **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
- **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

Disadvantages of Star topology

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



Tree topology

- Tree topology combines the characteristics of bus topology and star topology.
- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
- The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
- There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

Advantages of Tree topology

- **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
- **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
- **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.
- **Error detection:** Error detection and error correction are very easy in a tree topology.
- **Limited failure:** The breakdown in one station does not affect the entire network.
- **Point-to-point wiring:** It has point-to-point wiring for individual segments.

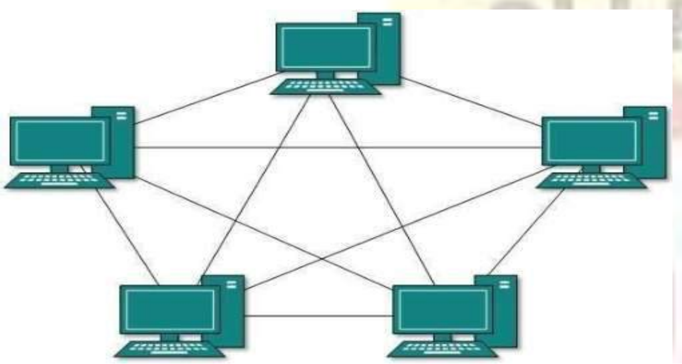
Disadvantages of Tree topology

- **Difficult troubleshooting:** If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
- **High cost:** Devices required for broadband transmission are very costly.

- **Failure:** A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.
- **Reconfiguration difficult:** If new devices are added, then it becomes difficult to reconfig

Mesh topology

- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.

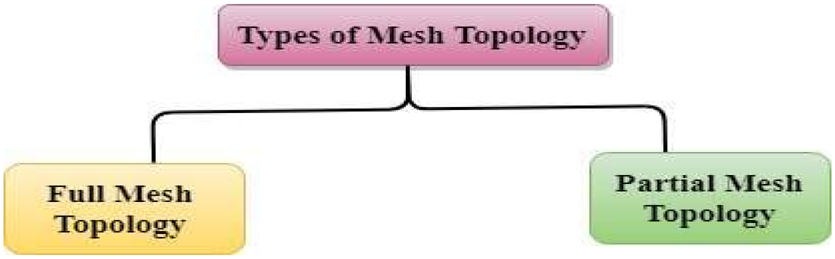


- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.
- Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
- Mesh topology is mainly used for wireless networks.
- Mesh topology can be formed by using the formula: **Number of cables = (n*(n-1))/2;**

Where n is the number of nodes that represents the network.

Mesh topology is divided into two categories:

- Fully connected mesh topology
- Partially connected mesh topology



- **Full Mesh Topology:** In a full mesh topology, each computer is connected to all the computers available in the network.
- **Partial Mesh Topology:** In a partial mesh topology, not all but certain computers are connected to those computers with which they communicate frequently.

Advantages of Mesh topology:

Reliable: The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.

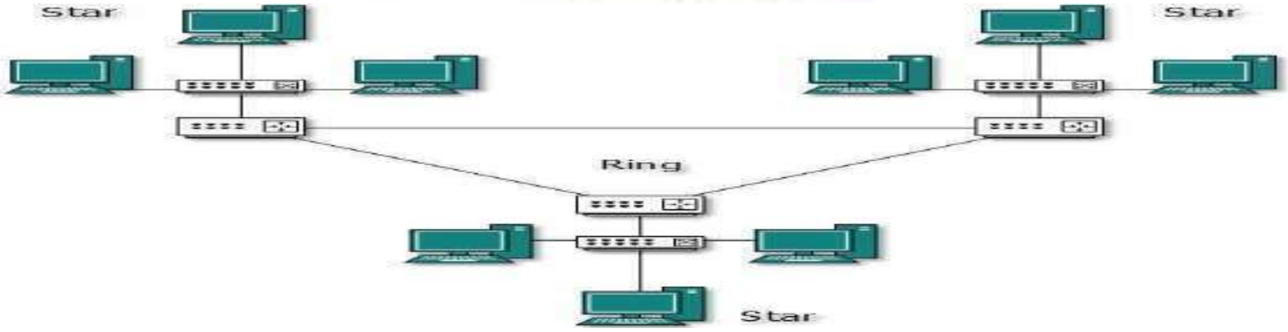
Fast Communication: Communication is very fast between the nodes.

Easier Reconfiguration: Adding new devices would not disrupt the communication between other devices.

Disadvantages of Mesh topology

- **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
- **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication link failure goes undetected.
- **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.

Hybrid Topology



- The combination of various different topologies is known as **Hybrid topology**.
- A Hybrid topology is a connection between different links and nodes to transfer the data.
- When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.

Advantages of Hybrid Topology

- **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
- **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
- **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
- **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

Disadvantages of Hybrid topology

- **Complex design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
- **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
- **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

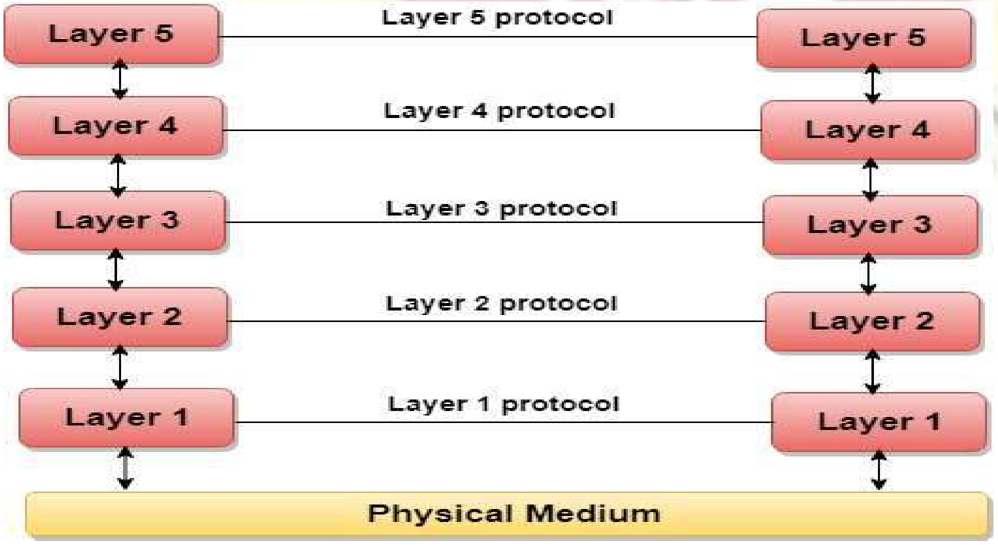
Computer Network Models

A communication subsystem is a complex piece of Hardware and software. Early attempts for implementing the software for such subsystems were based on a single, complex, unstructured program with many interacting components. The resultant software was very difficult to test and modify. To overcome such problem, the ISO has developed a layered approach. In a layered approach, networking concept is divided into several layers, and each layer is assigned a particular task. Therefore, we can say that networking tasks depend upon the layers.

Layered Architecture

- The main aim of the layered architecture is to divide the design into small pieces.
- Each lower layer adds its services to the higher layer to provide a full set of services to manage communications and run the applications.
- It provides modularity and clear interfaces, i.e., provides interaction between subsystems.
- It ensures the independence between layers by providing the services from lower to higher layer without defining how the services are implemented. Therefore, any modification in a layer will not affect the other layers.
- The number of layers, functions, contents of each layer will vary from network to network. However, the purpose of each layer is to provide the service from lower to a higher layer and hiding the details from the layers of how the services are implemented.
- The basic elements of layered architecture are services, protocols, and interfaces.
  - **Service:** It is a set of actions that a layer provides to the higher layer.
  - **Protocol:** It defines a set of rules that a layer uses to exchange the information with peer entity. These rules mainly concern about both the contents and order of the messages used.
  - **Interface:** It is a way through which the message is transferred from one layer to another layer.
- In a layer n architecture, layer n on one machine will have a communication with the layer n on another machine and the rules used in a conversation are known as a layer-n protocol.

Let's take an example of the five-layered architecture.



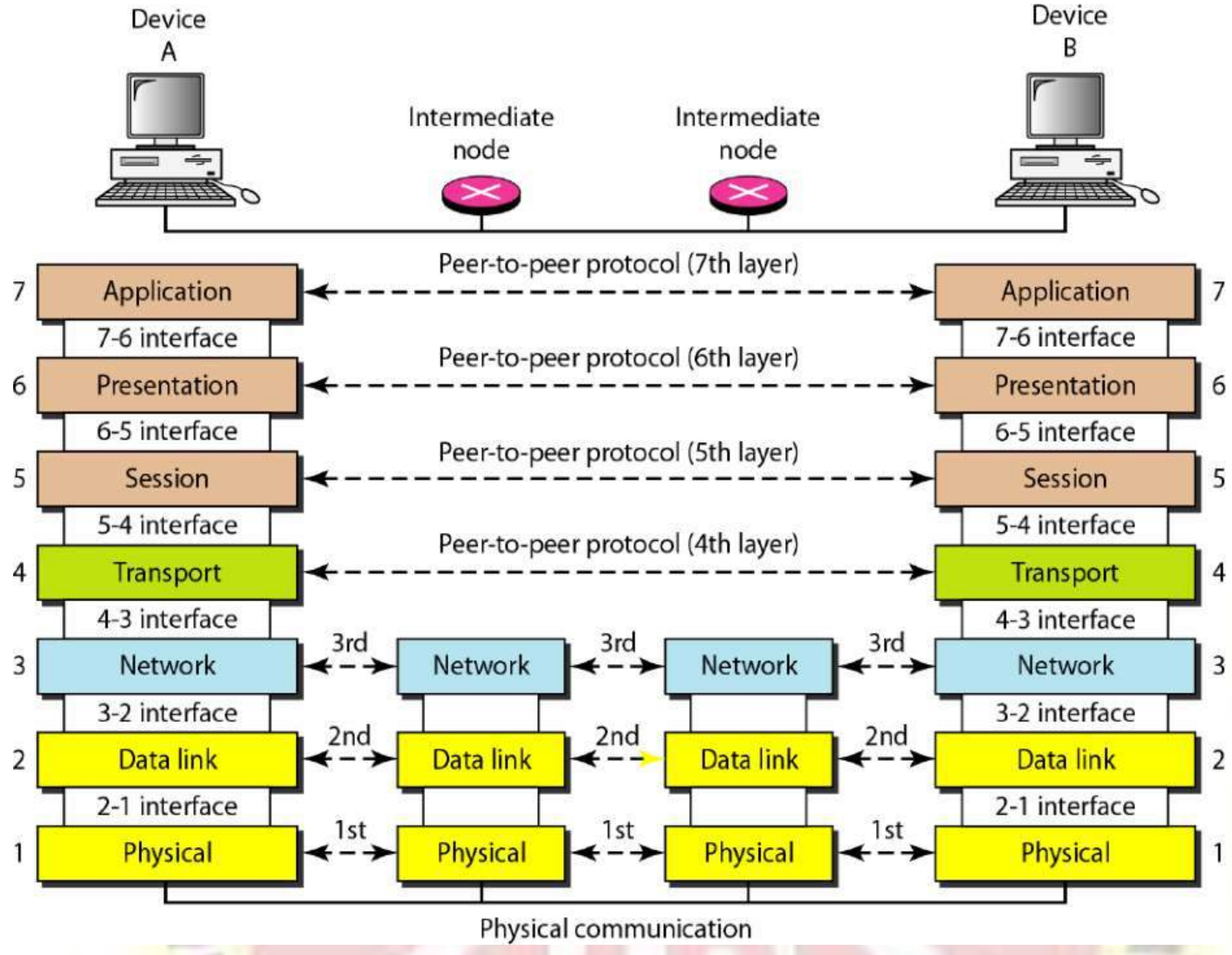
- In case of layered architecture, no data is transferred from layer n of one machine to layer n of another machine. Instead, each layer passes the data to the layer immediately just below it, until the lowest layer is reached.
- Below layer 1 is the physical medium through which the actual communication takes place.
- In a layered architecture, unmanageable tasks are divided into several small and manageable tasks.
- The data is passed from the upper layer to lower layer through an interface. A Layered architecture provides a clean-cut interface so that minimum information is shared among different layers. It also ensures that the implementation of one layer can be easily replaced by another implementation.
- A set of layers and protocols is known as network architecture.

Why do we require Layered architecture?

- **Divide-and-conquer approach:** Divide-and-conquer approach makes a design process in such a way that the unmanageable tasks are divided into small and manageable tasks. In short, we can say that this approach reduces the complexity of the design.
- **Modularity:** Layered architecture is more modular. Modularity provides the independence of layers, which is easier to understand and implement.
- **Easy to modify:** It ensures the independence of layers so that implementation in one layer can be changed without affecting other layers.
- **Easy to test:** Each layer of the layered architecture can be analyzed and tested individually

TheOSIReferenceModel

The OSI model is shown in Fig. This model is based on a proposal developed bytheInternationalStandardsOrganization(ISO).ThemodeliscalledtheISO-OSI(OpenSystemsInterconnection) ReferenceModelbecauseitdealswith connectingopen systems—that is, systems that are open for communicationwithothersystems.TheOSI



ThePhysicalLayer:

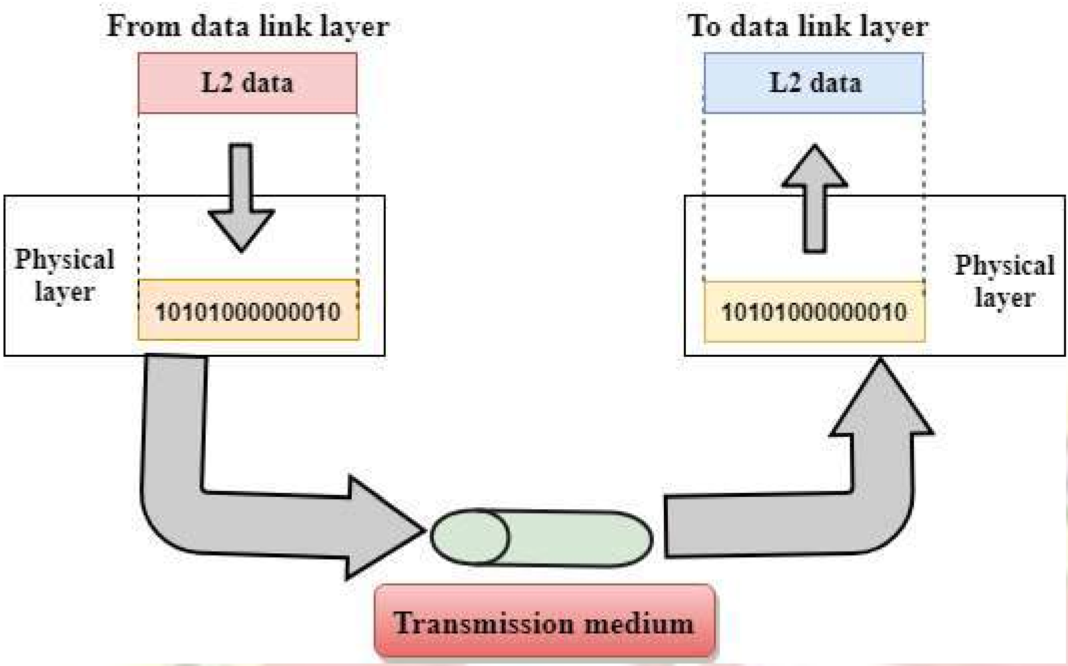
The physical layer is concerned with mechanical and electrical specifications oftheinterfaceandtransmissionmedium.Italsodefinestheproceduresandfunctionsth atphysicaldevicesandinterfaceshavetoperformfortransmissiontooccur.

Thephysicallayerisconcernedwiththefollowing:

Physicalcharacteristics

- Representationofbits
- Datarate
- Synchronizationofbits
- Lineconfiguration
- Physicaltopology
- TransmissionMode

Physical layer



- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

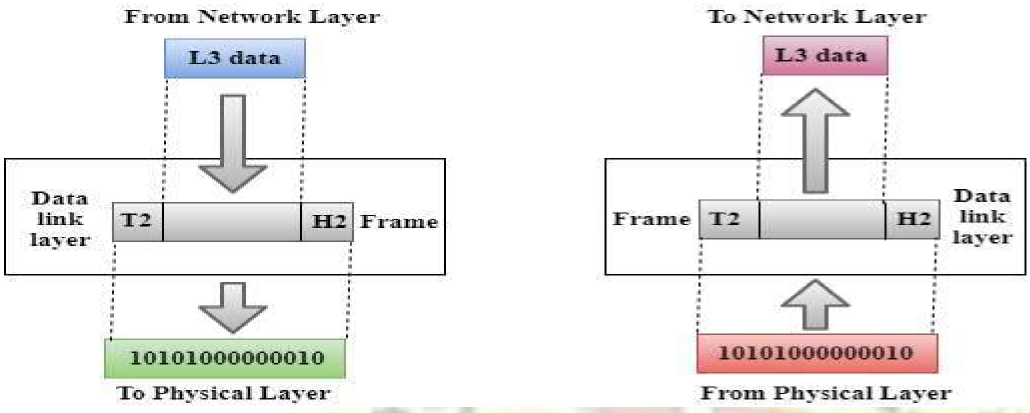
Functions of a Physical layer:

- **Line Configuration:** It defines the way how two or more devices can be connected physically.
- **Data Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- **Topology:** It defines the way how network devices are arranged.
- **Signals:** It determines the type of the signal used for transmitting the information.

Data-Link Layer

- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.

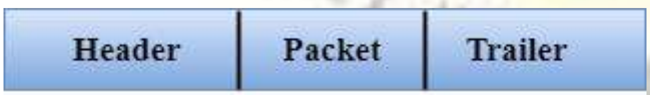
- It contains two sub-layers:



  - **Logical Link Control Layer**
    - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
    - It identifies the address of the network layer protocol from the header.
    - It also provides flow control.
  - **Media Access Control Layer**
    - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
    - It is used for transferring the packets over the network.

Functions of the Data-link layer

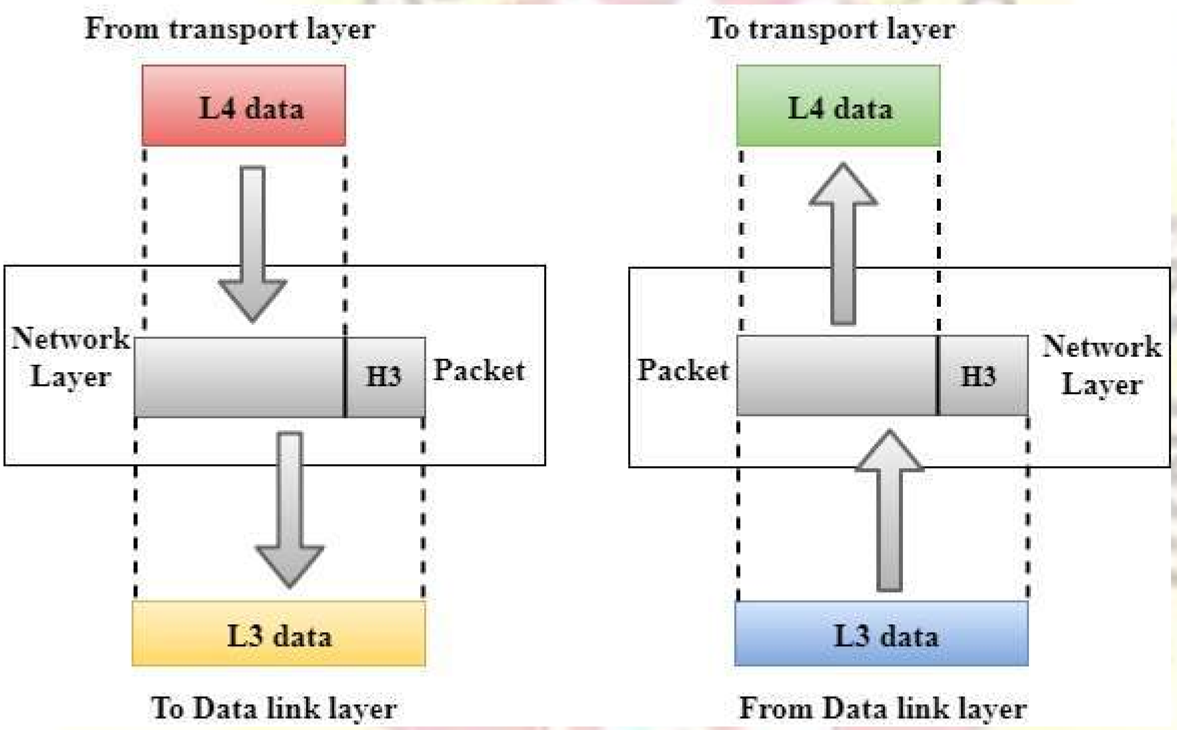
- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.



- **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.

- **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

Network Layer

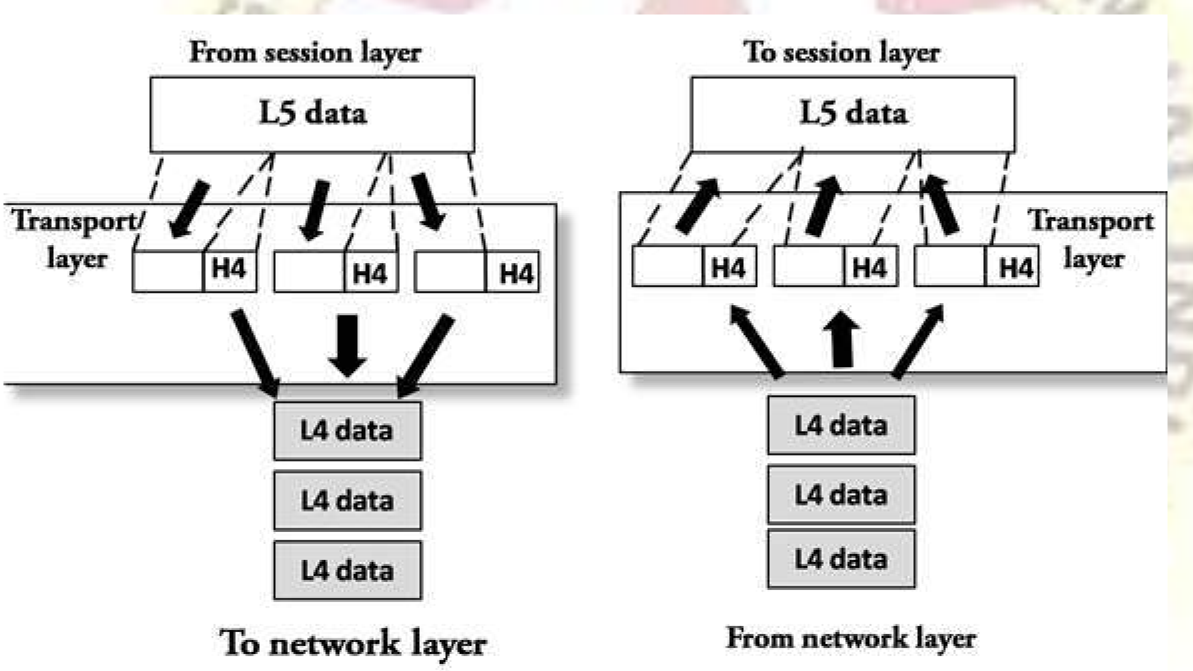


- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

- **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- **Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
- **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

Transport Layer



- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

- **Transmission Control Protocol**
  - It is a standard protocol that allows the systems to communicate over the internet.
  - It establishes and maintains a connection between hosts.
  - When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.
- **User Datagram Protocol**
  - User Datagram Protocol is a transport layer protocol.
  - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

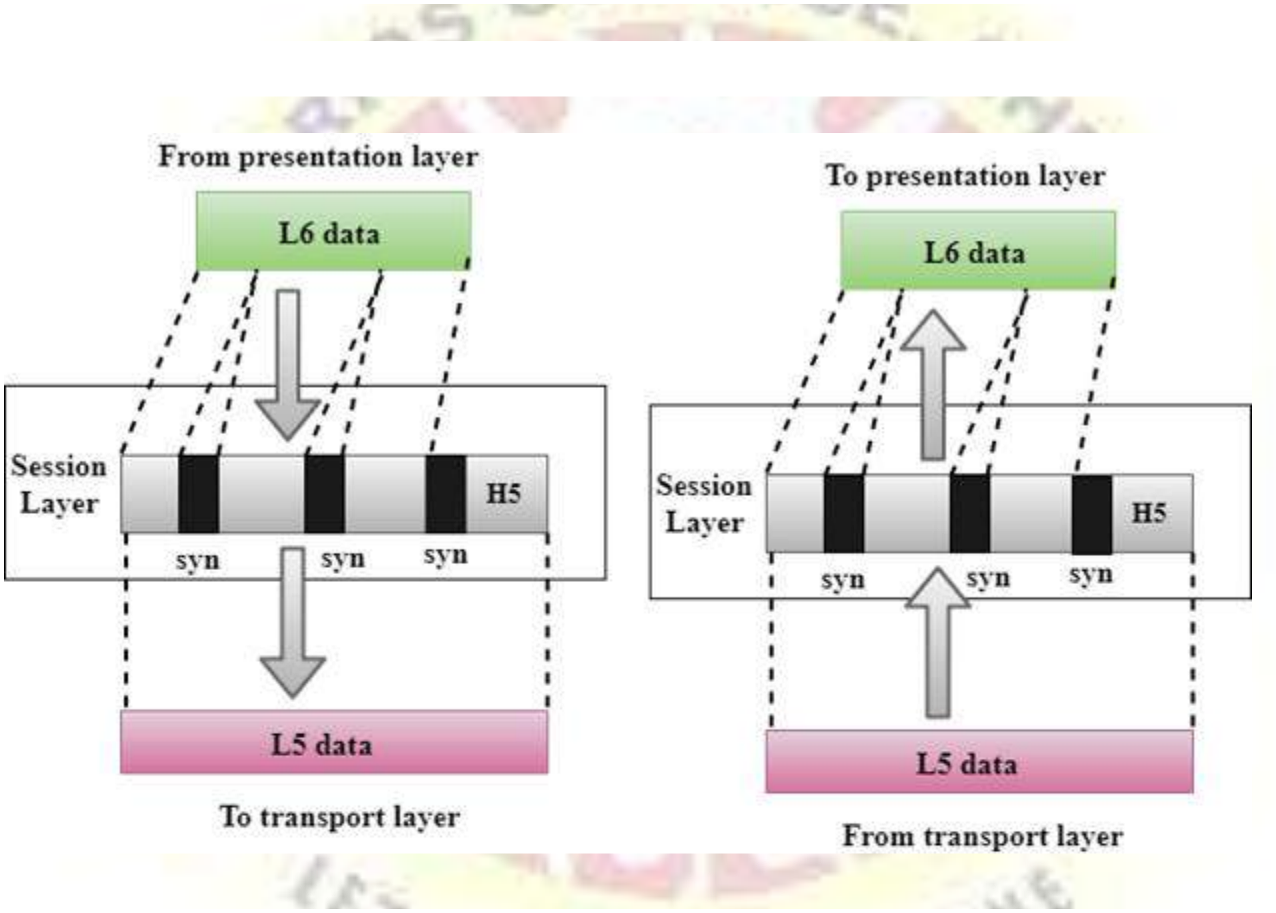
Functions of Transport Layer:

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.

- **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

Session Layer

- It is a layer 5 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

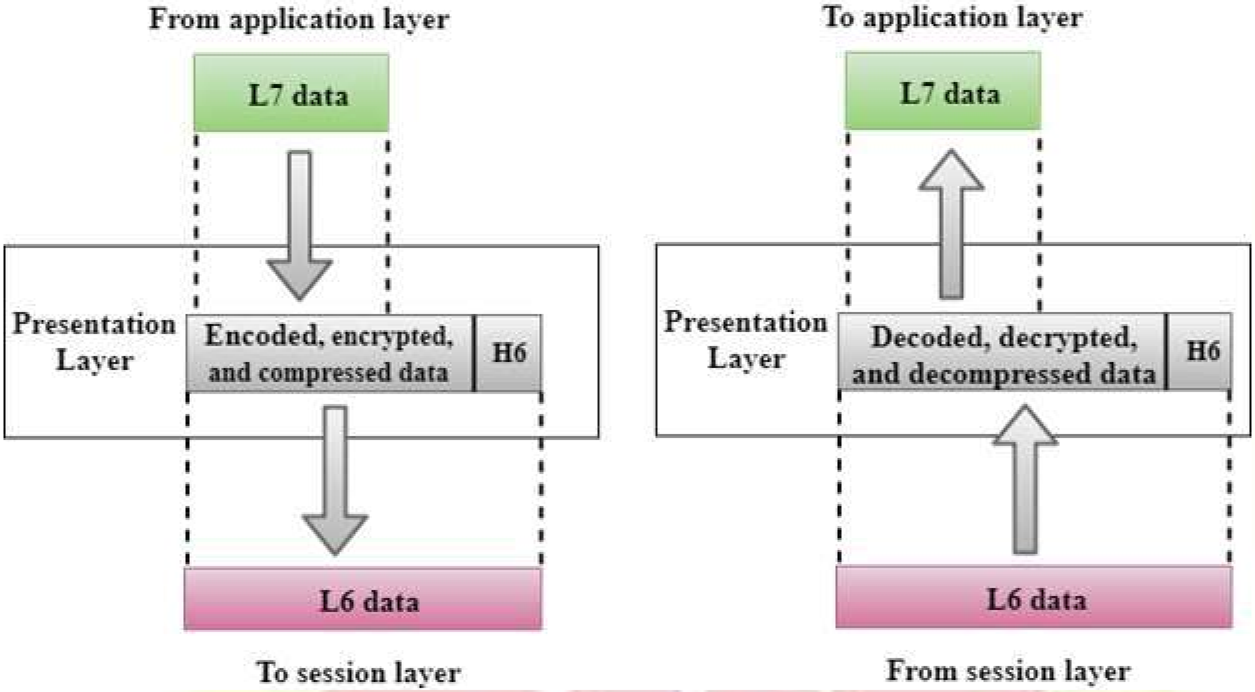


Functions of Session layer:

- **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
- **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

Presentation Layer

- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation layer is also known as the syntax layer.



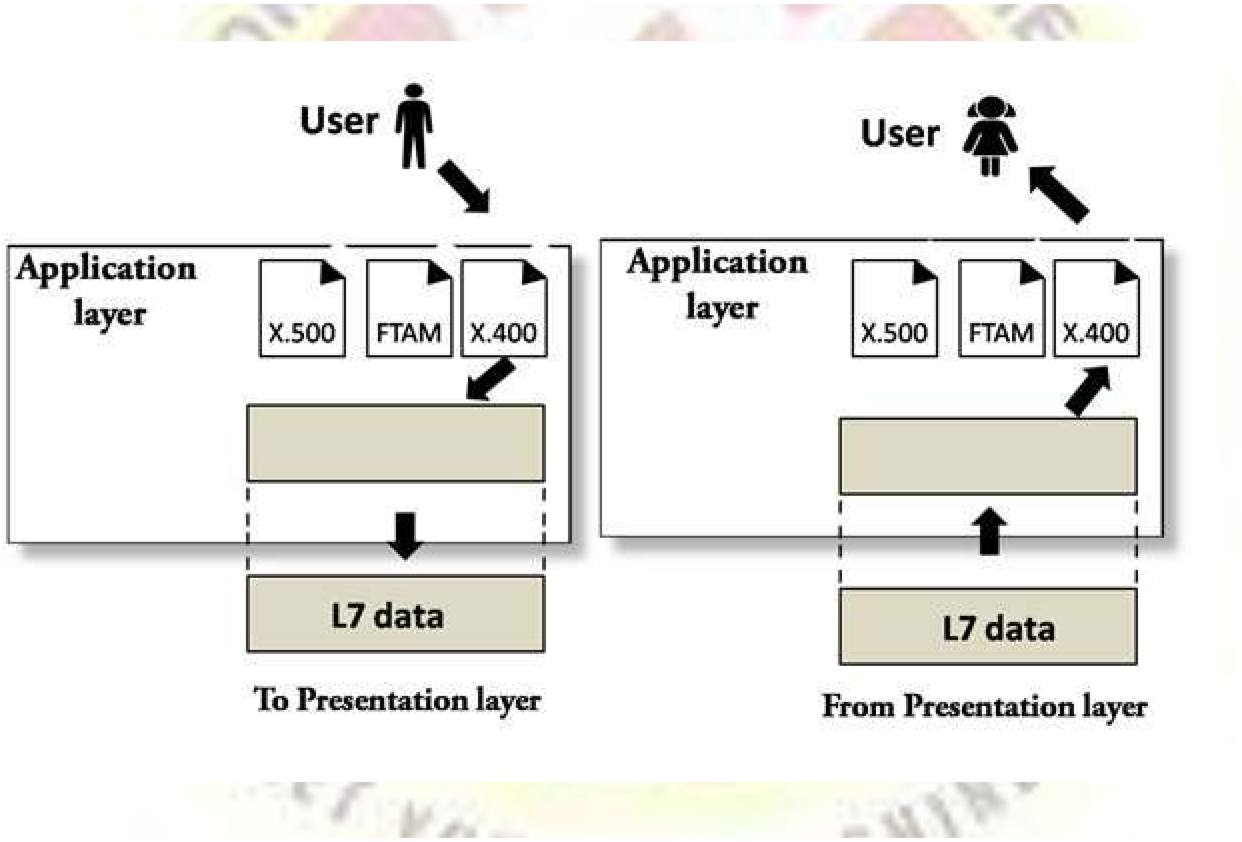
Functions of Presentation layer:

- **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.
- **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.

- **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

Application Layer

- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application layer is not an application, but it performs the application layer functions.
- This layer provides the network services to the end-users.



Functions of Application layer:

- **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services:** An application layer provides the facility for email forwarding and storage.
- Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

UNIT -II

THE PHYSICAL LAYER –

Different types of transmission medium

MetallicCableTransmissionmedium

It is the physical path between transmitter and receiver in a data transmission system. It is included in the physical layer of the OSI protocol hierarchy. The transmission medium is usually free space, metallic cable, or fiber-optic cable. The information is usually a signal that is the result of a conversion of data from another form. Transmission media can be generally categorized as either unguided or guided.

Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.

The main functionality of the transmission media is to carry the information in the form of bits through **LAN**(Local Area Network).

It is a physical path between transmitter and receiver in data communication.

In a copper-based network, the bits in the form of electrical signals.

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

In **OSI**(Open System Interconnection) phase, transmission media supports the Layer 1. Therefore, it is considered to be as a Layer 1 component.

The electrical signals can be sent through the copper wire, fibre optics, atmosphere, water, and vacuum.

The characteristics and quality of data transmission are determined by the characteristics of medium and signal.

Transmission media is of two types are wired media and wireless media. In wired media, medium characteristics are more important whereas, in wireless media, signal characteristics are more important.

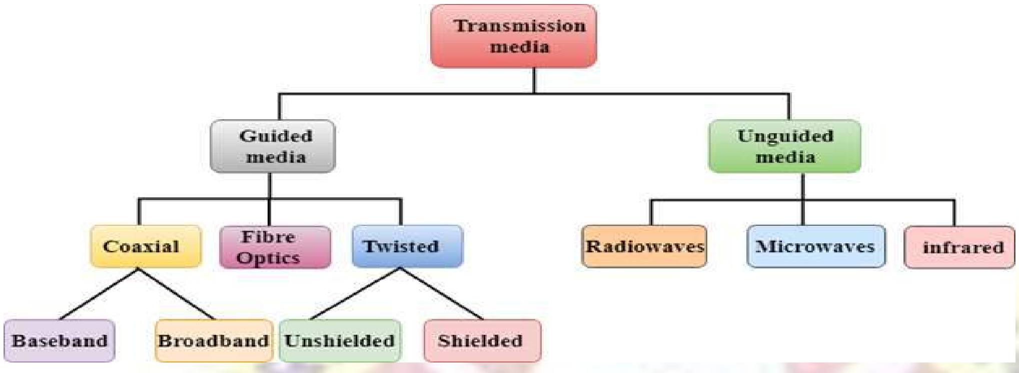
Different transmission media have different properties such as bandwidth, delay, cost and ease of installation and maintenance.

The transmission media is available in the lowest layer of the OSI reference model, i.e., **Physical layer**.

TypesofTransmissionMedia

Indatacommunicationterminology,atransmissionmediumisaphysicalpathbetween the transmitter and the receiver i.e it is the channel through which data issent from one place to another. Transmission Media is broadly classified into thefollowingtypes.

1. GuidedMedia
    (i) TwistedPairCable (ii)CoaxialCable (iii)OpticalFibreCable
2. UnguidedMedia
    (i) Radio Waves (ii)Microwaves (iii)Infrared



1. GuidedMedia:

ItisalsoreferredtoasWiredorBoundedtransmissionmedia.Signalsbeingtransmittedare directed and confinedin a narrow pathway by using physicallinks.

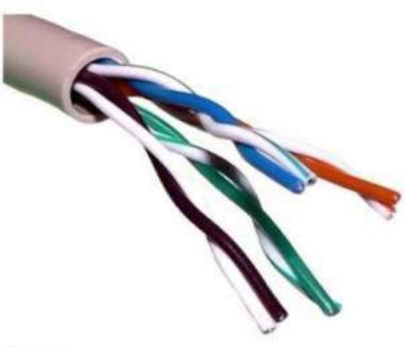
Features:

- HighSpeed
- Secure
- Usedforcomparativelyshorterdistances

Thereare3majortypesofGuidedMedia:

(i) TwistedPairCable

A twisted pair cable is made of two plasticinsulated copper wires twisted together toformasinglemedia.Outof these twowires,onlyonecarriesactualsignaland another is used for ground reference. Thetwistsbetweenwiresarehelpful inreducingnoiseandcrosstalk.



Therearetwotypesoftwistedpaircables:

UnshieldedTwistedPair(UTP)Cable

ShieldedTwistedPair(STP)Cable

Unshielded Twisted Pair (UTP)

This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.

Advantages:

Leastexpensive

Easytoinstall

Highspeedcapacity

Disadvantages:

Susceptibletoexternalinterference

LowercapacityandperformanceincomparisontoSTP

Shortdistancetransmissionduetoattenuation

ShieldedTwistedPair(STP)

Thistypeofcableconsistsofaspecialjackettoblockexternalinterference.Itisusedinfast-data-rateEthernetandinvoiceanddatachannelsoftelephonelines.

Advantages

BetterperformanceatahigherdatarateincomparisontoUTP

Eliminatescrosstalk

Comparatively faster

Disadvantages

Comparativelydifficulttoinstallandmanufacture

Moreexpensive

Bulky

(ii) CoaxialCable

Coaxial cable has two wires of copper.Thecorewireliesinthecenteranditis made of solid conductor. The core isenclosed in an insulating sheath. Thesecond wire is wrapped around overthesheathandthattoointurnencasedbyinsulatorsheath.

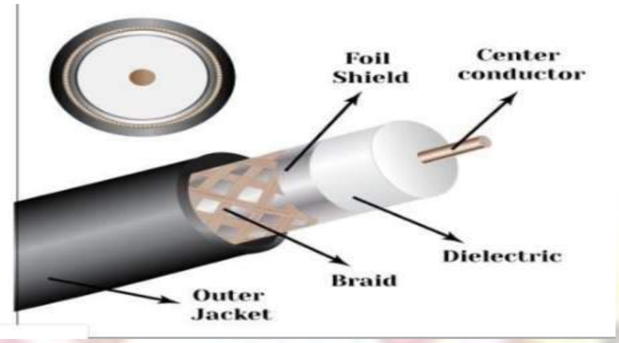
Stiffcopperwireascoreand

Insulating material surrounding thecore

Closely woven braided meshof conductingmaterial surroundingtheinsulator

Protective plasticsheath encasingthewire

These are widely used for cableTV connectionsand LANs.Itprovidehighbandwidthratesofupto450mbps.Therearethreecategoriesofcoax cables namely, RG-59 (Cable TV),RG-58(ThinEthernet),andRG-11(Thick Ethernet). RG stands for RadioGovernment



Advantages

- HighBandwidth
- BetternoiseImmunity
- Easytoinstallandexpand
- Inexpensive

Disadvantages

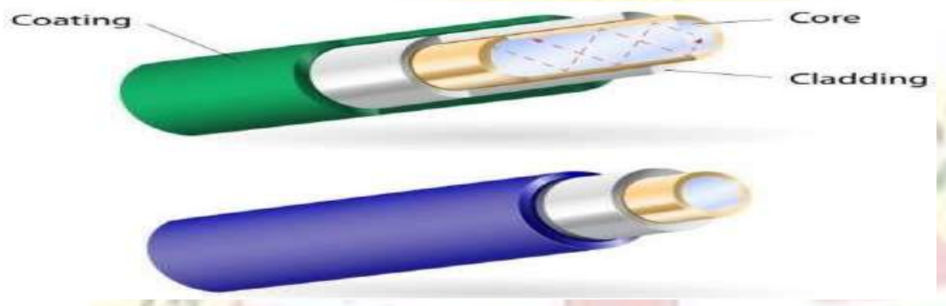
- Singlecable failure can disrupt the entire network
- **OpticalFibreCable**

Itusestheconceptofreflectionoflightthroughacoremadeupofglassorplastic.Thecoreissurroundedbyplasticcoveringcalledthe*cladding*.

Thin glassorplasticthreadsusedtotransmitdatausing light waves arecalled optical fibre. Light Emitting Diodes (LEDs) or Laser Diodes (LDs) emit lightwavesatthe source,whichisreadby a detector at the other end. Optical fibrecable hasabundleofsuchthreadsorfibresbundledtogetherinaprotectivecovering. Each fibre is made up of these three layers, starting with the innermostlayer−

- Coremadeofhighqualitysilicaglassorplastic
- Claddingmadeofhighqualitysilicaglassorplastic,withalowerrefractiveindex thanthecore
- Protectiveoutercoveringcalledbuffer

Optical fibre is rapidly replacing copperwiresintelephonelines,internetcommunicationandevencableTVconnectionsbecausetransmitteddatacan travel very long distances withoutweakening. Singlenode fibreopticcablecanhavemaximumsegmentlengthof2kmsandbandwidthofupto 100Mbps.Multi-nodefibreopticcable canhavemaximumsegmentlengthof100kmsandbandwidthupto2Gbps.



Advantages

- Increasedcapacityandbandwidth
- Lightweight
- Lesssignalattenuation
- Immunitytoelectromagneticinterference
- Resistancetocorrosivematerials

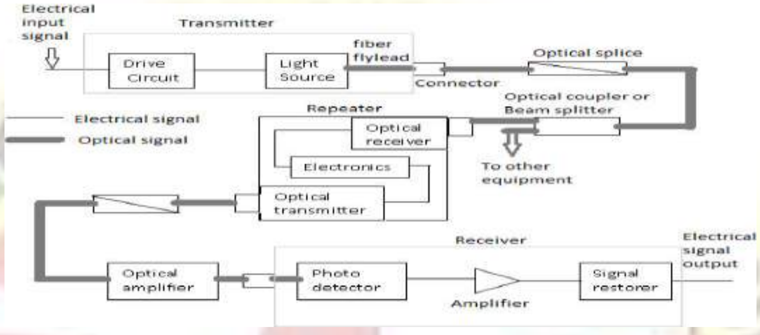
Disadvantages

- Difficulttoinstallandmaintain
- Highcost
- Fragile
- unidirectional,ie,willneedanotherfibre,ifweneedbidirectionalcommunication

Electromagnetic spectrum

The entire distribution ofelectromagnetic radiation according to frequencyorwavelength.Althoughallelectromagneticwavestravelatthespeedoflightinavacuum,theydosoatawiderangeoffrequencies,wavelengths,andphotonenergies.Theelectromagneticspectrumcomprisesthe span of all electromagnetic radiationandconsistsofmanysubranges,commonlyreferredto as portions, such as visiblelightorultravioletradiation.Theentireelectromagneticspectrum,from the lowest to the highest frequency(longest to shortest wavelength), includes all radio waves (e.g.,commercial radio and television, microwaves, radar), infrared radiation,visiblelight,ultravioletradiation,X-rays,andgammarays.Nearlyallfrequenciesandwavelengthsofelectromagneticradiationcanbeusedforspectroscopy.

BlockdiagramofOpticalFibreCommunicationSystem



Theopticalfiberconsistsofthreemainelements:

1. Transmitter:Anelectricsignalisappliedtotheopticaltransmitter.Theopticaltransmitterconsistsofdrivercircuit,lightsourceandfiberflylead.
   - Drivercircuitdrivesthelightsource.
   - Lightsourceconvertselectricalsignaltoopticalsignal.
   - Fiberflyleadisusedtoconnectopticalsignaltoopticalfiber.
2. Transmissionchannel:Itconsistsofacablethatprovidesmechanicalandenvironmentalprotectiontotheopticalfiberscontainedinside.Eachopticalfiberactsasanindividualchannel.
   - Opticalspliceisusedtopermanentlyjointwoindividualopticalfibers.
   - Opticalconnectorisfortemporarynon-fixedjointsbetweentwoindividualopticalfibers.
   - Opticalcouplerorsplitterprovidessignaltootherdevices.
   - Repeaterconvertstheopticalsignalintoelectricalsignalusingopticalreceiverandpassesittoelectroniccircuitwhereitisreshapedandamplifiedasitgetsattenuatedanddistortedwithincreasingdistancebecauseofscattering,absorptionanddispersioninwaveguides,andthissignalisthenagainconvertedintoopticalsignalbytheopticaltransmitter.
3. Receiver:Opticalsignalisappliedtotheopticalreceiver.Itconsistsofphotodetector, amplifierandsignalrestorer.
   - Photodetectorconvertstheopticalsignaltoelectricalsignal.

  - Signalrestorersandamplifiersareusedtoimprovesignaltonoiseratioofthesignalastherearechancesofnoisetobeintroducedinthesignalduetotheuseofphoto detectors.

- Forshortdistancecommunicationonlymainelementsarerequired.
  Source-LED Fiber-Multimodestepindexfiber Detector-PINdetector
- For long distance communication along with the main elements there is needforcouplers,beamsplitters,repeaters,opticalamplifiers.
  Source-LASERdiode Fiber-singlemodefiberDetector-Avalanchephotodiode(APD)

WirelessCommunicationsSystems(UnguidedMedia)

- ItisalsoreferredtoasWireless or Unbounded transmission media. Anunguidedtransmissiontransmitstheelectromagneticwaveswithoutusinganyphysicalmedium.Thereforeitisalsoknownas**wirelesstransmission**.
- Inunguidedmedia,airisthemediathroughwhichtheelectromagneticenergycanfloweasily.

Unguidedtransmissionisbroadlyclassifiedinto**three**categories:

1. Radiowaves

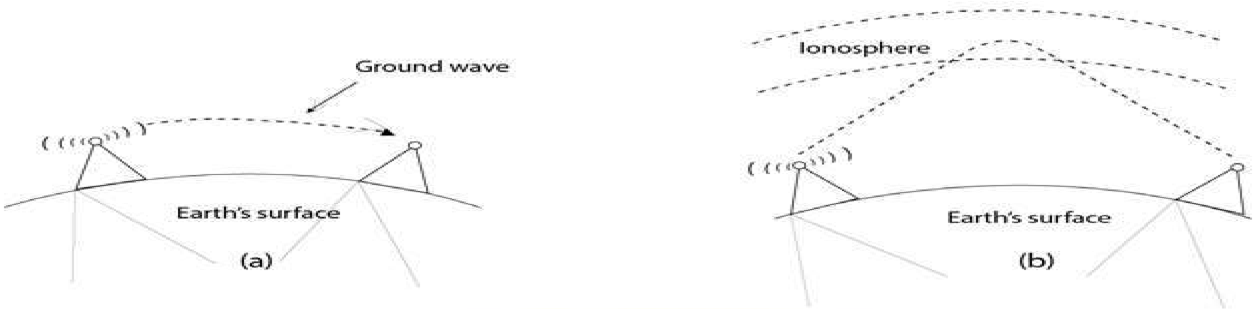
- Radiowavesaretheelectromagneticwavesthataretransmittedinallthedirectionsoffreespace.
- Radiowavesareomnidirectional,i.e.,thesignalsarepropagatedinallthedirections.
- Therangeinfrequenciesofradiowavesisfrom3Khzto1khz.
- Inthecaseofradiowaves,thesendingandreceivingantennaarenotaligned,i.e.,thewavesentbythesendingantennacanbereceivedbyanyreceivingantenna.
- Anexampleoftheradiowaveis**FMradio**.**A**

pplicationsOfRadiowaves:

- ARadiowaveisusefulformulticastingwhenthereisonesenderandmanyreceivers.
- AnFMradio,television,cordlessphonesareexamplesofaradiowave.

AdvantagesOfRadiotransmission:

- Radiotransmissionismainlyusedforwideareanetworksandmobilecellularphones.
- Radiowavescoveralargearea,andtheycanpenetratethewalls.
- Radio transmissionprovidesa highertransmissionrate.



2. Microwaves

Microwavesareoftwotypes:

- Terrestrialmicrowave
- Satellitemicrowavecommunication.

(i) TerrestrialMicrowaveTransmission

- TerrestrialMicrowavetransmissionisatechnologythattransmitsthefocusedbeamofaradiosignalfromoneground-basedmicrowavetransmissionantennatoanother.
- Microwavesaretheelectromagneticwaveshavingthefrequencyintherangefrom1GHzto1000GHz.
- Microwaves are unidirectional as the sending and receiving antenna is to bealigned,i.e.,thewavessentbythesendingantennaarenarrowlyfocussed.
- Inthiscase,antennasaremountedonthetowerstosendabeamtoanotherantennawhichiskmaway.
- Itworksonthelineofsighttransmission,i.e.,theantennasmountedonthetowersarethedirectsightofeachother.

CharacteristicsofMicrowave:

- **Frequencyrange:**Thefrequencyrangeofterrestrialmicrowaveisfrom4-6GHzto21-23GHz.
- **Bandwidth:**Itsupportsthebandwidthfrom1to10Mbps.
- **Shortdistance:**Itisinexpensiveforshortdistance.
- **Long distance:**Itisexpensiveasitrequiresahighertowerforalongerdistance.
- **Attenuation:**Attenuationmeanslossofsignal.Itisaffectedbyenvironmentalconditionsandantennasize.

AdvantagesOfMicrowave:

- Microwavetransmissionischeaperthanusingcables.
- Itisfreefromlandacquisitionasitdoesnotrequireanylandfortheinstallationofcables.
- Microwavetransmissionprovidesaneasycommunicationinterrainsastheinstallationofcableinterrainisquiteadifficulttask.
- Communication over oceans can be achieved by using microwave transmission.

DisadvantagesofMicrowavetransmission:

- **Eavesdropping:**Aneavesdroppingcreatesinsecurecommunication.Anymalicioususercancatchthesignalintheairbyusingitsownantenna.
- **Outofphasesignal:**A signal canbe moved out ofphase by usingmicrowavetransmission.
- **Susceptibletoweathercondition:**Amicrowavetransmissionissusceptibletoweathercondition.Thismeansthatanyenvironmentalchangesuchasrain,windcandistortthesignal.
- **Bandwidthlimited:**Allocationofbandwidthislimitedinthecaseofmicrowavetransmission.

(ii) Satellite Microwave Communication

- Asatelliteisaphysicalobjectthatrevolvesaroundtheearthataknownheight.
- Satellitecommunicationismorereliablenowadaysasitoffersmoreflexibilitythancableandfibreopticsystems.
- We can communicate withany point ontheglobe by using satellitecommunication.
- Thesatelliteacceptsthesignalthatistransmittedfromtheearthstation,anditamplifiesthesignal.Theamplifiedsignalisretransmittedtoanotherearthstation.

AdvantagesOfSatelliteMicrowaveCommunication:

- Thecoverageareaofasatellitemicrowaveismorethantheterrestrialmicrowave.
- Thetransmissioncostofthesatelliteisindependentofthedistancefromthecentreofthecoveragearea.
- Satellitecommunication isused inmobileand wirelesscommunicationapplications.
- Itiseasytoinstall.
- ItisusedinawidevarietyofapplicationssuchasweatherforecastingradioTVsignalbroadcasting,mobilecommunication,etc.

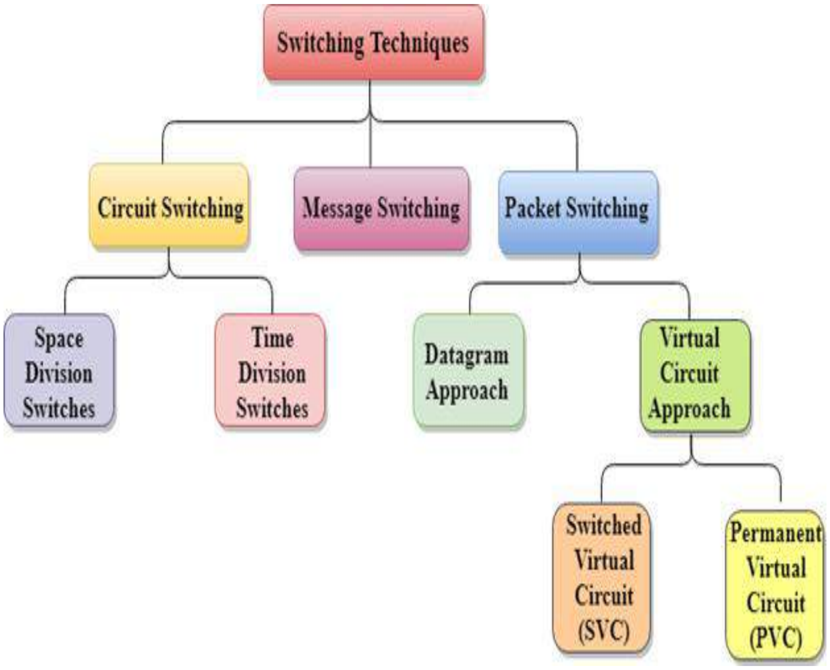
DisadvantagesOfSatelliteMicrowaveCommunication:

- Satellitedesigninganddevelopmentrequiresmoretimeandhighercost.
- TheSatelliteneedstobemonitoredandcontrolledonregularperiodssothatitremainsinorbit.
- Thelifeofthesatelliteisabout12-15years.Duetothisreason,anotherlaunchofthesatellitehastobeplannedbeforeitbecomesnon-functional.

SWITCHING TECHNIQUES

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission. Switching technique is used to connect the systems for making one-to-one communication.

Classification Of Switching Techniques

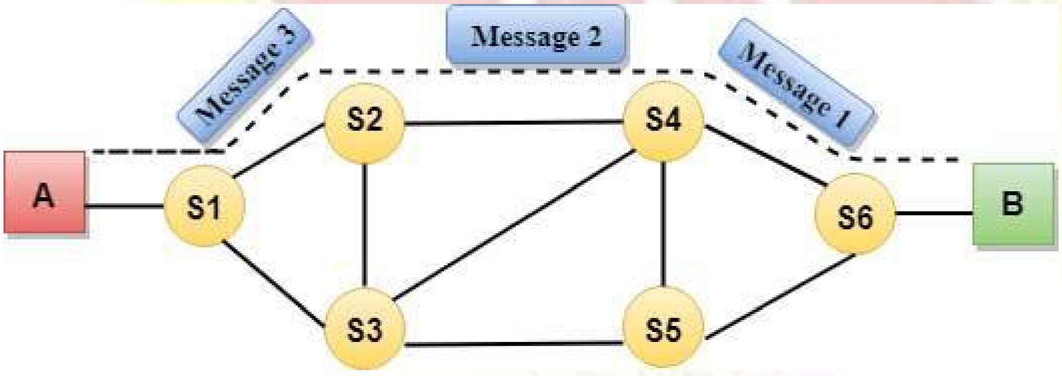


Circuit Switching

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.

Communication through circuit switching has 3 phases:

- Circuit establishment
- Data transfer
- Circuit Disconnect



Circuit Switching can use either of the two technologies:

Space Division Switches:

- Space Division Switching is a circuit switching technology in which a single transmission path is accomplished in a switch by using a physically separate set of crosspoints.

- Space Division Switching can be achieved by using crossbar switch. A crossbar switch is a metallic crosspoint or semiconductor gate that can be enabled or disabled by a control unit.
- The Crossbar switch is made by using the semiconductor. For example, Xilinx crossbar switch using FPGAs.
- Space Division Switching has high speed, high capacity, and nonblocking switches.

Space Division Switches can be categorized in two ways:

- **Crossbar Switch**
- **Multistage Switch**

Crossbar Switch

The Crossbar switch is a switch that has n input lines and n output lines. The crossbar switch has n^2 intersection points known as **crosspoints.**

Disadvantage of Crossbar switch:

The number of crosspoints increases as the number of stations is increased. Therefore, it becomes very expensive for a large switch. The solution to this is to use a multistage switch.

Multistage Switch

- Multistage Switch is made by splitting the crossbar switch into the smaller units and then interconnecting them.
- It reduces the number of crosspoints.
- If one path fails, then there will be an availability of another path.

Advantages Of Circuit Switching:

- In the case of Circuit Switching technique, the communication channel is dedicated.
- It has fixed bandwidth.

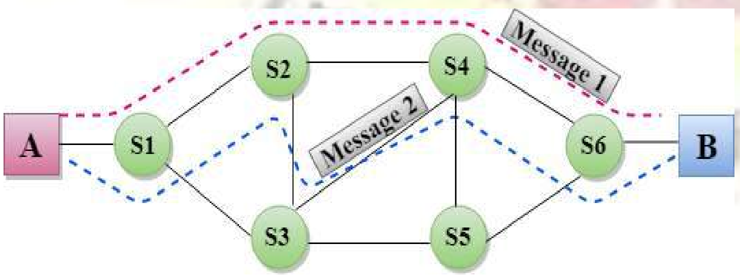
Disadvantages Of Circuit Switching:

- Once the dedicated path is established, the only delay occurs in the speed of data transmission.

- It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.
- It is more expensive than other switching techniques as a dedicated path is required for each connection.
- It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.
- In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.



Advantages Of Message Switching

- Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.

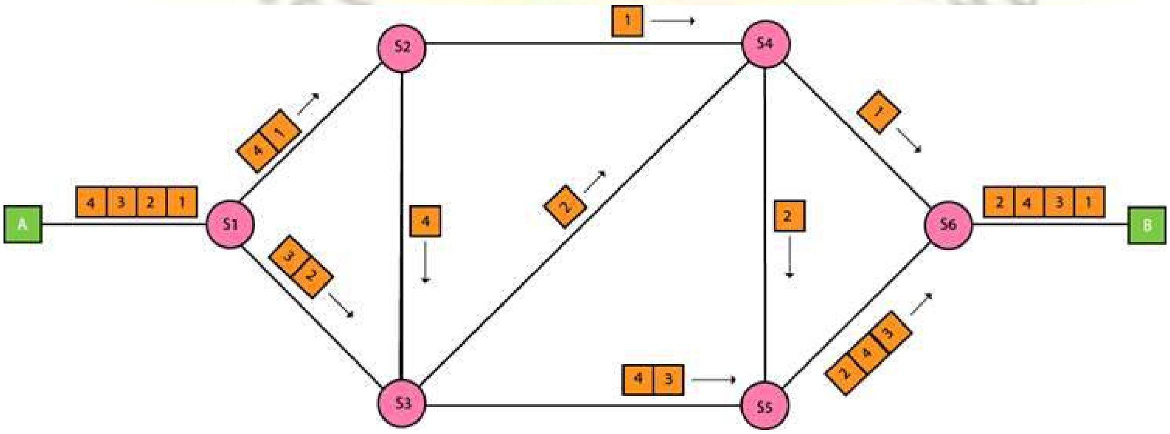
- Traffic congestion can be reduced because the message is temporarily stored in the nodes.
- Message priority can be used to manage the network.
- The size of the message which is sent over the network can be varied. Therefore, it supports the data of unlimited size.

Disadvantages Of Message Switching

- The message switches must be equipped with sufficient storage to enable them to store the messages until the message is forwarded.
- The Long delay can occur due to the storing and forwarding facility provided by the message switching technique.

Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.



Approaches Of Packet Switching:

There are two approaches to Packet Switching:

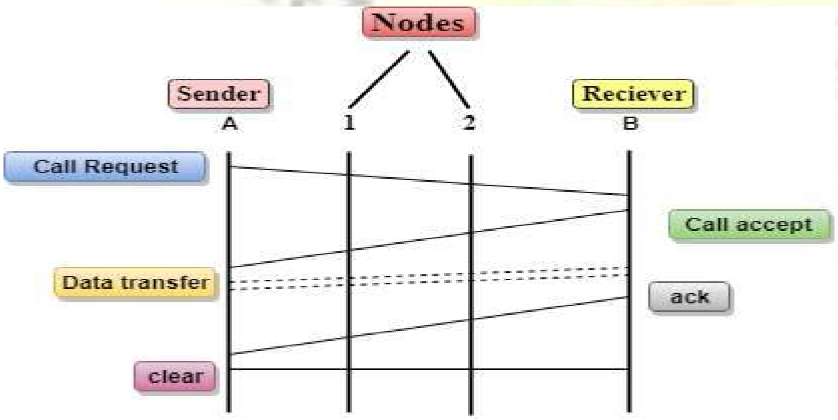
Datagram Packet switching:

- It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
- The packets are reassembled at the receiving end in correct order.
- In Datagram Packet Switching technique, the path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.
- Datagram Packet Switching is also known as connectionless switching.

Virtual Circuit Switching

- Virtual Circuit Switching is also known as connection-oriented switching.
- In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this case, the path is fixed for the duration of a logical connection.

Let's understand the concept of virtual circuit switching through a diagram:



- n the above diagram, A and B are the sender and receiver respectively. 1 and 2 are the nodes.

- Call request and call accept packets are used to establish a connection between the sender and receiver.
- When a route is established, data will be transferred.
- After transmission of data, an acknowledgment signal is sent by the receiver that the message has been received.
- If the user wants to terminate the connection, a clear signal is sent for the termination.

Differences b/w Datagram approach and Virtual Circuit approach

Datagram approach	Virtual Circuit approach
Node takes routing decisions to forward the packets.	Node does not take any routing decision.
Congestion cannot occur as all the packets travel in different directions.	Congestion can occur when the node is busy, and it does not allow other packets to pass through.
It is more flexible as all the packets are treated as an independent entity.	It is not very flexible.

Advantages Of Packet Switching:

- **Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.
- **Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- **Efficient:** Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

Disadvantages Of Packet Switching:

- Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.
- The protocols used in a packet switching technique are very complex and requires high implementation cost.

- If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered.

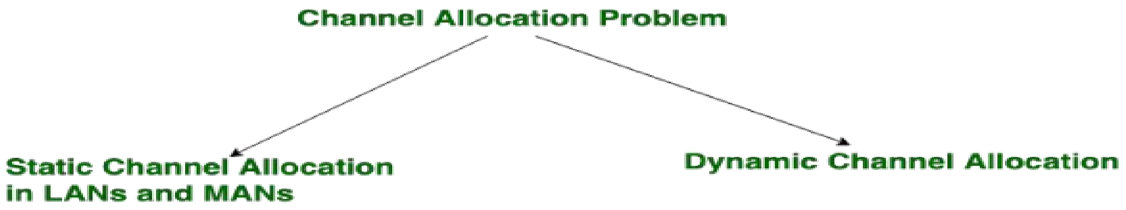
Channel allocation

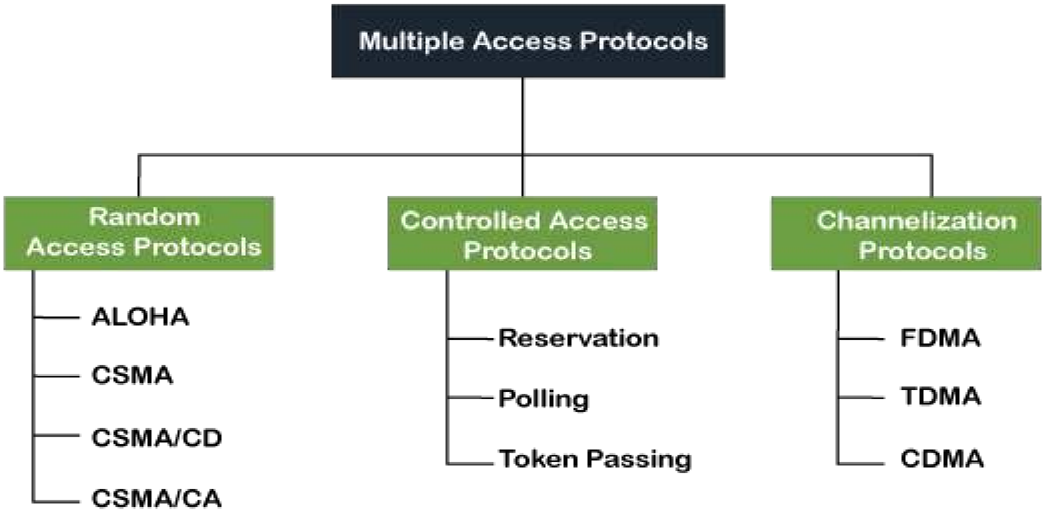
Multiple access protocol

When a sender and receiver have a dedicated link to transmit data packets, the data link control is enough to handle the channel. Suppose there is no dedicated path to communicate or transfer the data between two devices. In that case, multiple stations access the channel and simultaneously transmits the data over the channel. It may create collision and cross talk. Hence, the multiple access protocol is required to reduce the collision and avoid crosstalk between the channels

Channel allocation is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks. There are user's quantity may vary every time the process takes place. If there are N number of users and channel is divided into N equal-sized sub channels, Each user is assigned one portion. If the number of users are small and don't vary at times, than Frequency Division Multiplexing can be used as it is a simple and efficient channel bandwidth allocating technique.

Channel allocation problem can be solved by two schemes: Static Channel Allocation in LANs and MANs, and Dynamic Channel Allocation.


Channel Allocation Problem
Static Channel Allocation in LANs and MANs
Dynamic Channel Allocation



Random Access Protocol

In this protocol, all the station has the equal priority to send the data over a channel. In random access protocol, one or more stations cannot depend on another station nor any station control another station. Depending on the channel's state (idle or busy), each station transmits the data frame. However, if more than one station sends the data over a channel, there may be a collision or data conflict. Due to the collision, the data frame packets may be lost or changed. And hence, it does not receive by the receiver end.

Following are the different methods of random-access protocols for broadcasting frames on the channel.

- Aloha
- CSMA
- CSMA/CD
- CSMA/CA

ALOHA Random Access Protocol

It is designed for wireless LAN (Local Area Network) but can also be used in a shared medium to transmit data. Using this method, any station can transmit data across a network simultaneously when a data frameset is available for transmission.

Aloha Rules

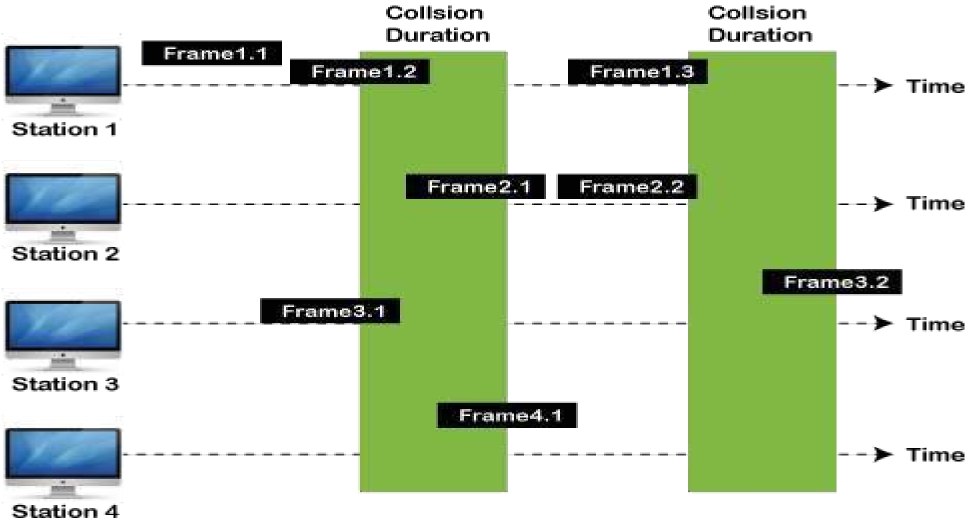
1. Any station can transmit data to a channel at any time.
2. It does not require any carrier sensing.
3. Collision and data frames may be lost during the transmission of data through multiple stations.
4. Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
5. It requires retransmission of data after some random amount of time.

Types of ALOHA
Pure ALOHA
Slotted ALOHA

Pure Aloha

Whenever data is available for sending over a channel at stations, we use Pure Aloha. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost. When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment. If it does not acknowledge the receiver end within the specified time, the station waits for a random amount of time, called the backoff time (Tb). And the station may assume the frame has been lost or destroyed. Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.

1. The total vulnerable time of pure Aloha is 2 * Tfr.
2. Maximum throughput occurs when G = 1/ 2 that is 18.4%.
3. Successful transmission of data frame is S = G * e ^ - 2 G.



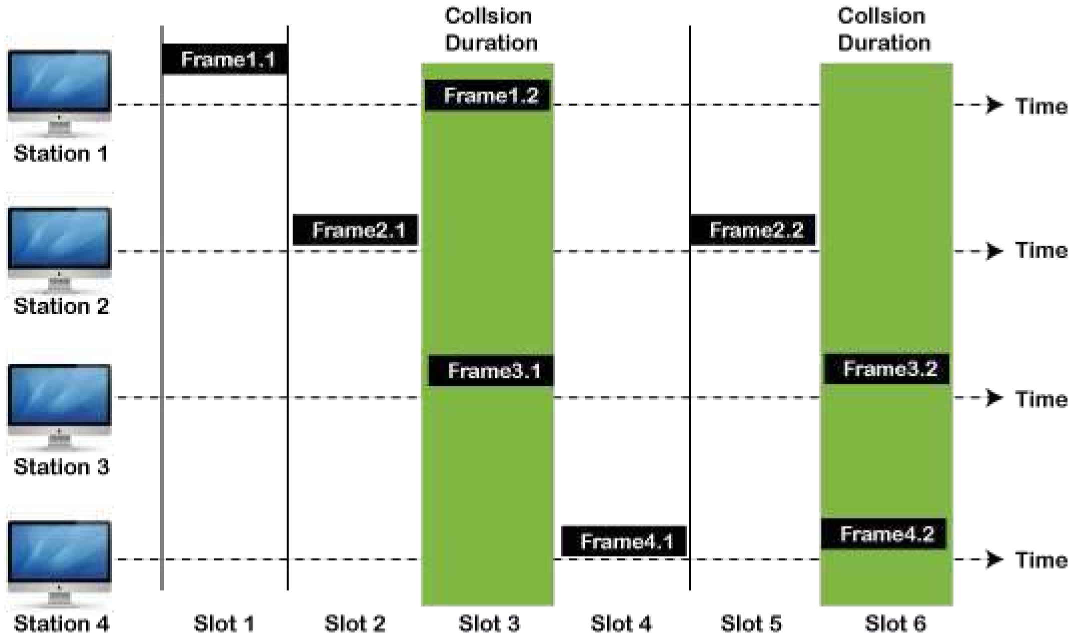
Frames in Pure ALOHA

As we can see in the figure above, there are four stations for accessing a shared channel and transmitting data frames. Some frames collide because most stations send their frames at the same time. Only two frames, frame 1.1 and frame 2.2, are successfully transmitted to the receiver end. At the same time, other frames are lost or destroyed. Whenever two frames fall on a shared channel simultaneously, collisions can occur, and both will suffer damage. If the new frame's first bit enters the channel before finishing the last bit of the second frame. Both frames are completely finished, and both stations must retransmit the data frame.

Slotted Aloha

The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting. In slotted Aloha, the shared channel is divided into a fixed time interval called **slots**. So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot. And if the stations are unable to send data to the beginning of the slot, the station will have to wait until the beginning of the slot for the next time. However, the possibility of a collision remains when trying to send a frame at the beginning of two or more station time slot.

1. Maximum throughput occurs in the slotted Aloha when G = 1 that is 37%.
2. The probability of successfully transmitting the data frame in the slotted Aloha is S = G * e ^ - 2 G.
3. The total vulnerable time required in slotted Aloha is Tfr.



Frames in Slotted ALOHA

CSMA (Carrier Sense Multiple Access)

It is a **carrier sense multiple access** based on media access protocol to sense the traffic on a channel (idle or busy) before transmitting the data. It means that if the channel is idle, the station can send data to the channel. Otherwise, it must wait until the channel becomes idle. Hence, it reduces the chances of a collision on a transmission medium.

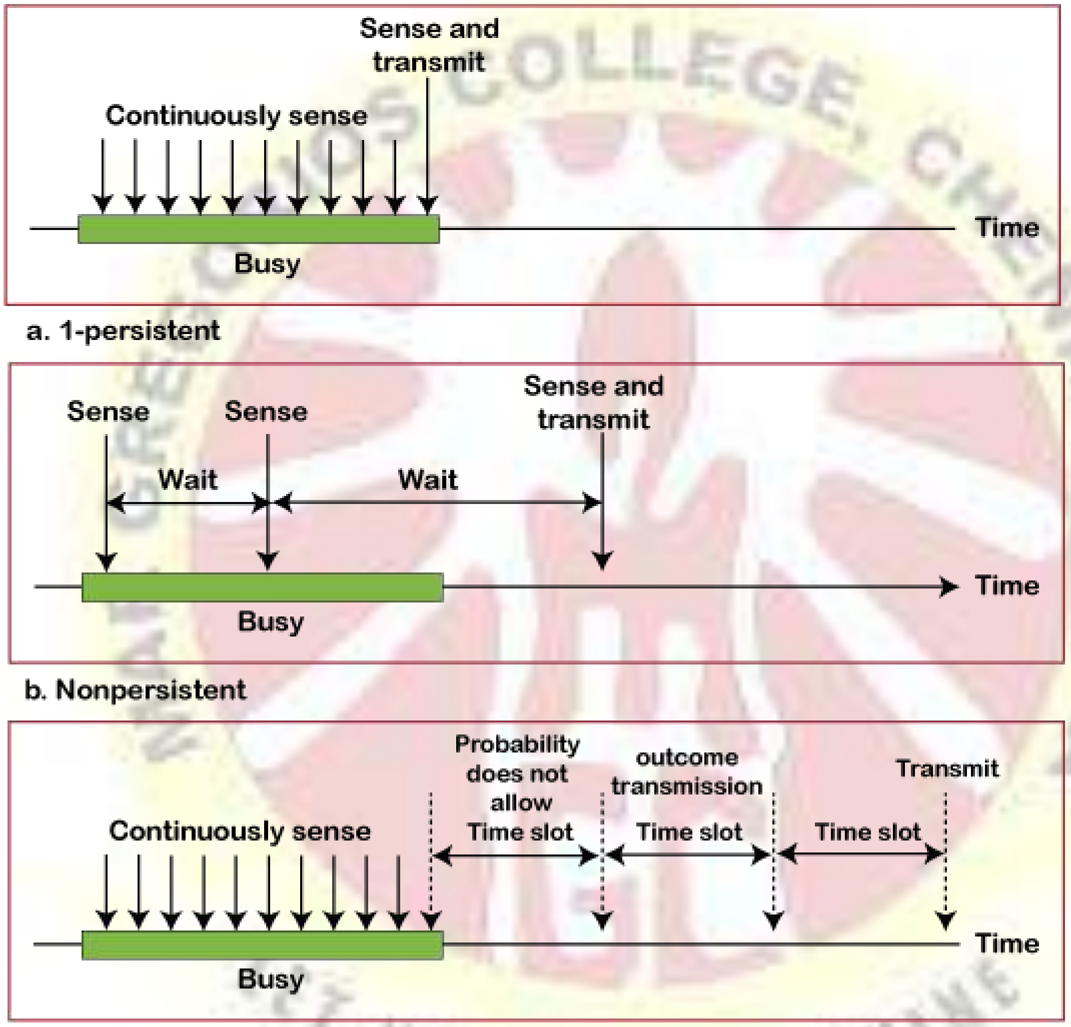
CSMA Access Modes

1-Persistent: In the 1-Persistent mode of CSMA that defines each node, first sense the shared channel and if the channel is idle, it immediately sends the data. Else it must wait and keep track of the status of the channel to be idle and broadcast the frame unconditionally as soon as the channel is idle.

Non-Persistent: It is the access mode of CSMA that defines before transmitting the data, each node must sense the channel, and if the channel is inactive, it immediately sends the data. Otherwise, the station must wait for a random time (not continuously), and when the channel is found to be idle, it transmits the frames.

P-Persistent: It is the combination of 1-Persistent and Non-persistent modes. The P-Persistent mode defines that each node senses the channel, and if the channel is inactive, it sends a frame with a **P** probability. If the data is not transmitted, it waits for a (**q = 1-p probability**) random time and resumes the frame with the next time slot.

O- Persistent: It is an O-persistent method that defines the superiority of the station before the transmission of the frame on the shared channel. If it is found that the channel is inactive, each station waits for its turn to retransmit the data.



a. 1-persistent

b. Nonpersistent

c. p-persistent

CSMA/ CD

It is a **carrier sense multiple access/ collision detection** network protocol to transmit data frames. The CSMA/CD protocol works with a medium access control layer. Therefore, it first senses the shared channel before broadcasting the frames, and if the channel is idle, it transmits a frame to check whether the transmission was successful. If the frame is successfully received, the station sends another frame. If any collision is detected in the CSMA/CD, the station sends a jam/ stop signal to the shared channel to terminate data transmission. After that, it waits for a random time before sending a frame to a channel.

CSMA/ CA

It is a **carrier sense multiple access/collision avoidance** network protocol for carrier transmission of data frames. It is a protocol that works with a medium access control layer. When a data frame is sent to a channel, it receives an acknowledgment to check whether the channel is clear. If the station receives only a single (own) acknowledgments, that means the data frame has been successfully transmitted to the receiver. But if it gets two signals (its own and one more in which the collision of frames), a collision of the frame occurs in the shared channel. Detects the collision of the frame when a sender receives an acknowledgment signal.

Following are the methods used in the CSMA/ CA to avoid the collision:

Interframe space: In this method, the station waits for the channel to become idle, and if it gets the channel is idle, it does not immediately send the data. Instead of this, it waits for some time, and this time period is called the **Interframe** space or IFS. However, the IFS time is often used to define the priority of the station.

Contention window: In the Contention window, the total time is divided into different slots. When the station/ sender is ready to transmit the data frame, it chooses a random slot number of slots as **wait time**. If the channel is still busy, it does not restart the entire process, except that it restarts the timer only to send data packets when the channel is inactive.

Acknowledgment: In the acknowledgment method, the sender station sends the data frame to the shared channel if the acknowledgment is not received ahead of time.

B. Controlled Access Protocol

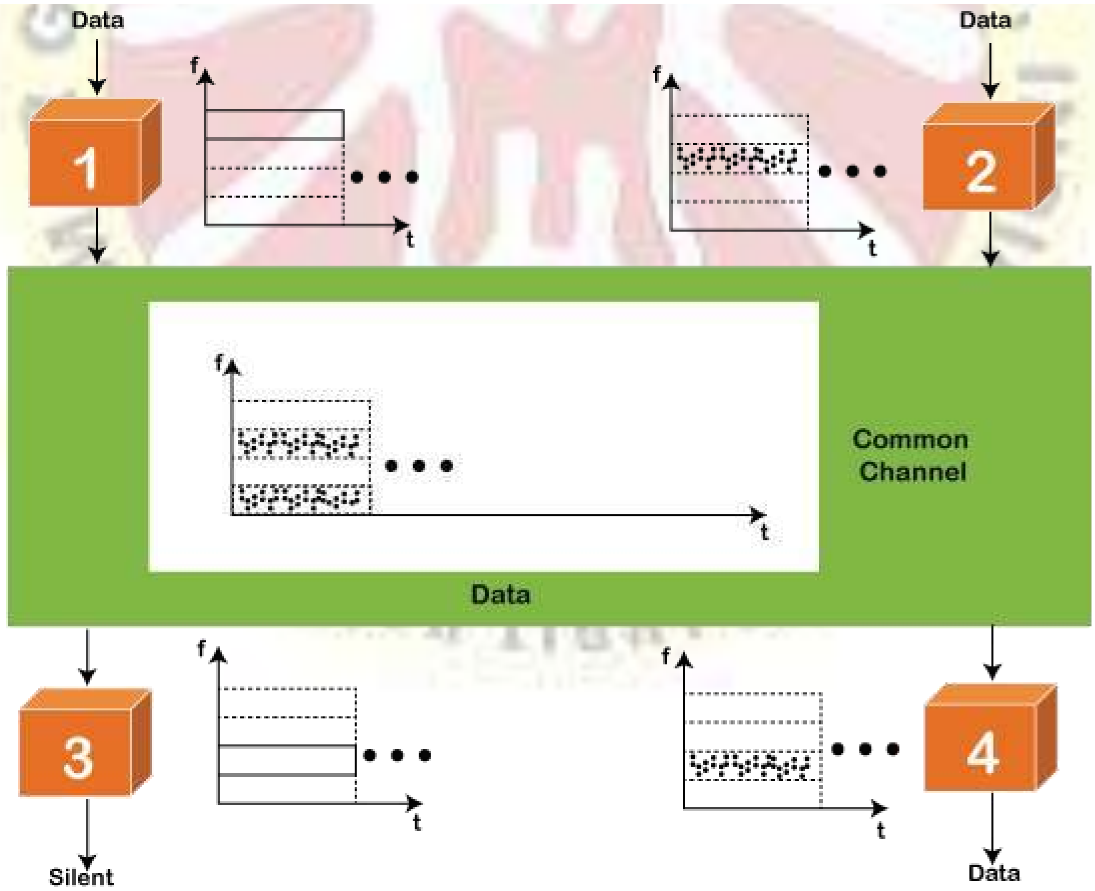
It is a method of reducing data frame collision on a shared channel. In the controlled access method, each station interacts and decides to send a data frame by a particular station approved by all other stations. It means that a single station cannot send the data frames unless all other stations are not approved. It has three types of controlled access: **Reservation, Polling**, and **Token Passing**.

C. Channelization Protocols

It is a channelization protocol that allows the total usable bandwidth in a shared channel to be shared across multiple stations based on their time, distance and codes. It can access all the stations at the same time to send the data frames to the channel.

Following are the various methods to access the channel based on their time, distance and codes:

1. FDMA (Frequency Division Multiple Access)
2. TDMA (Time Division Multiple Access)
3. CDMA (Code Division Multiple Access)
4. **FDMA**
5. It is a frequency division multiple access (**FDMA**) method used to divide the available bandwidth into equal bands so that multiple users can send data through a different frequency to the subchannel. Each station is reserved with a particular band to prevent the crosstalk between the channels and interferences of stations.



6.
7. **TDMA**

8. Time Division Multiple Access (**TDMA**) is a channel access method. It allows the same frequency bandwidth to be shared across multiple stations. And to avoid collisions in the shared channel, it divides the channel into different frequency slots that allocate stations to transmit the data frames. The same **frequency** bandwidth into the shared channel by dividing the signal into various time slots to transmit it. However, TDMA has an overhead of synchronization that specifies each station's time slot by adding synchronization bits to each slot.
9. **CDMA**
10. The code division multiple access (CDMA) is a channel access method. In CDMA, all stations can simultaneously send the data over the same channel. It means that it allows each station to transmit the data frames with full frequency on the shared channel at all times. It does not require the division of bandwidth on a shared channel based on time slots. If multiple stations send data to a channel simultaneously, their data frames are separated by a unique code sequence. Each station has a different unique code for transmitting the data over a shared channel. For example, there are multiple users in a room that are continuously speaking. Data is received by the users if only two-person interact with each other using the same language. Similarly, in the network, if different stations communicate with each other simultaneously with different code language.

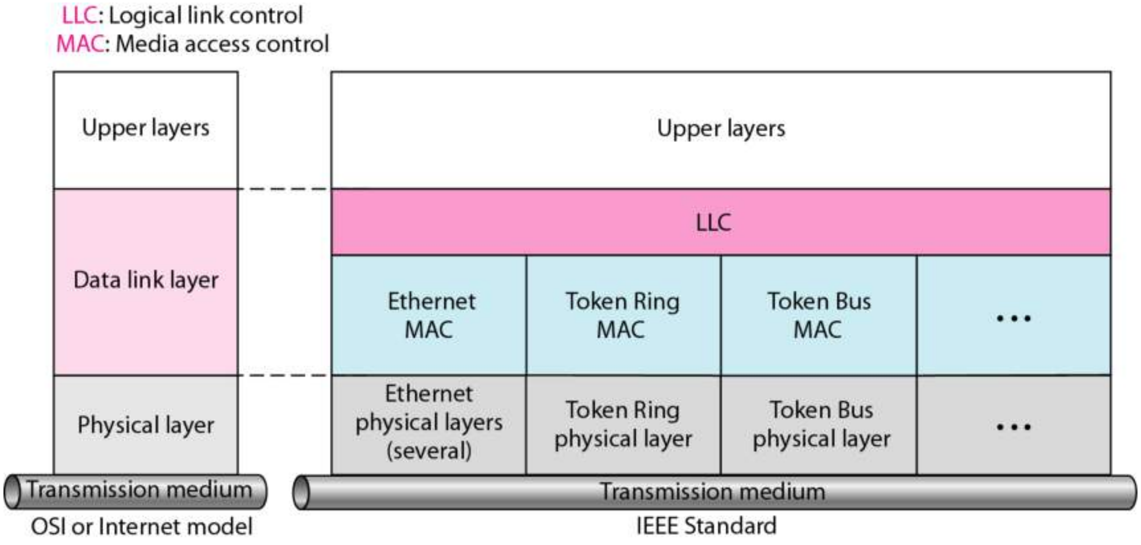
IEEE SAYANDARDS

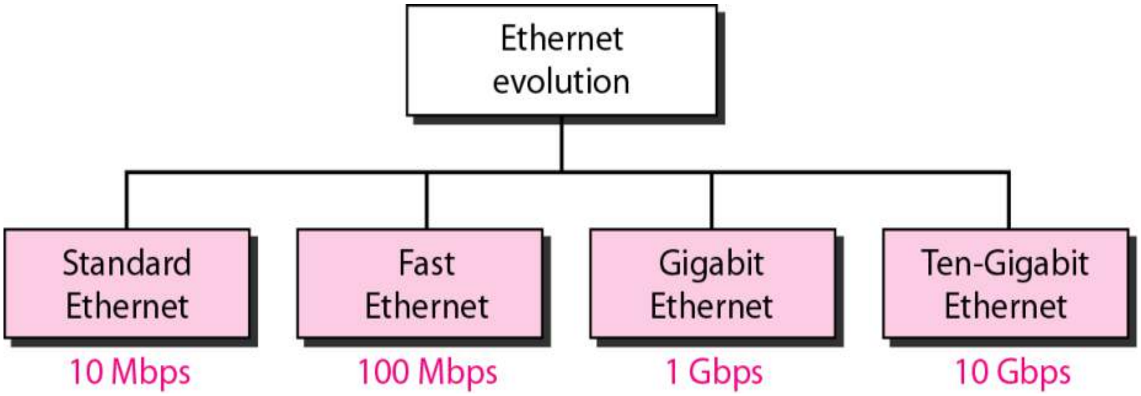
In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers. Project 802 is a way of specifying functions of the physical layer and the data link layer of major LAN protocols.

Ethernet is a set of technologies and protocols that are used primarily in LANs. It was first standardized in 1980s by IEEE 802.3 standard. IEEE 802.3 defines the physical layer and the medium access control (MAC) sub-layer of the data link layer for wired Ethernet networks. Ethernet is classified into two categories: classic Ethernet and switched Ethernet.

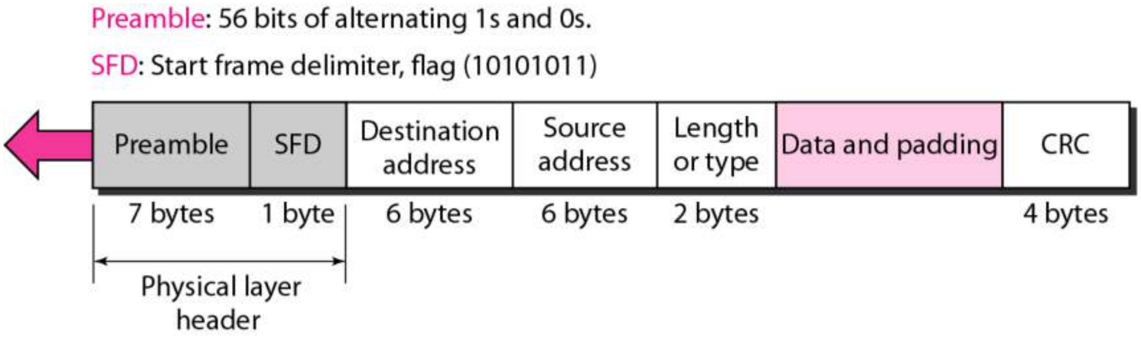
Classic Ethernet is the original form of Ethernet that provides data rates between 3 to 10 Mbps. The varieties are commonly referred as 10BASE-X. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and X is the type of medium used. Most varieties of classic Ethernet have become obsolete in present communication scenario.

A switched Ethernet uses switches to connect to the stations in the LAN. It replaces the repeaters used in classic Ethernet and allows full bandwidth utilization.





802.3 MAC frame



Frame Format of Classic Ethernet and IEEE 802.3

The main fields of a frame of classic Ethernet are -

- **Preamble**: It is the starting field that provides alert and timing pulse for transmission. In case of classic Ethernet it is an 8 byte field and in case of IEEE 802.3 it is of 7 bytes.
- **Start of Frame Delimiter**: It is a 1 byte field in a IEEE 802.3 frame that contains an alternating pattern of ones and zeros ending with two ones.
- **Destination Address**: It is a 6 byte field containing physical address of destination stations.
- **Source Address**: It is a 6 byte field containing the physical address of the sending station.
- **Length**: It a 7 bytes field that stores the number of bytes in the data field.
- **Data**: This is a variable sized field carries the data from the upper layers. The maximum size of data field is 1500 bytes.
- **Padding**: This is added to the data to bring its length to the minimum requirement of 46 bytes.
- **CRC**: CRC stands for cyclic redundancy check. It contains the error detection information

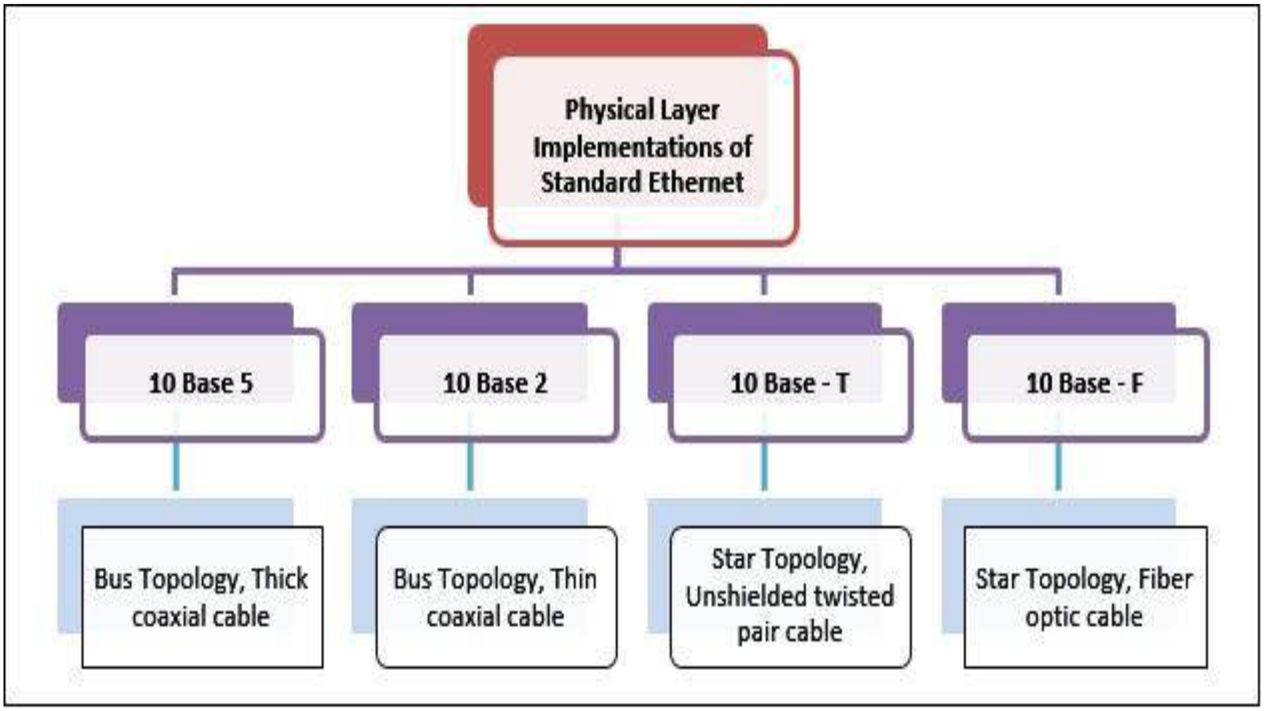
Cassic Ethernet is the original form of Ethernet that provides data rates between 3 to 10 Mbps. The varieties are commonly referred as 10BASE-X. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and X is the type of medium used. Most varieties of classic Ethernet have become obsolete in present communication scenario.

Varieties of Classic Ethernet

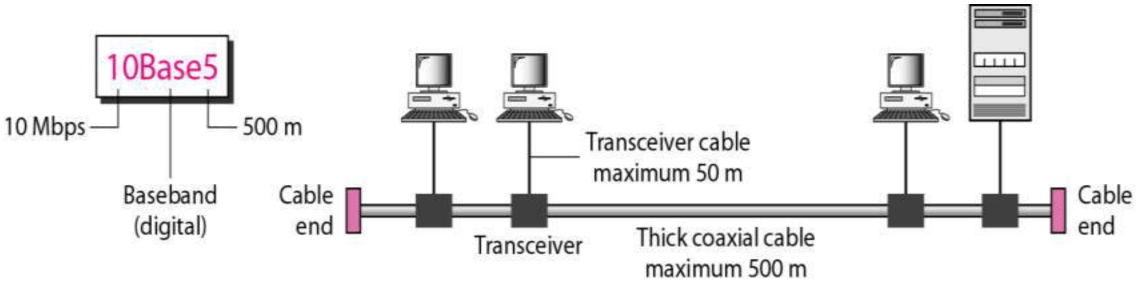
The common varieties of classic Ethernet are -

- **Thick coax (10BASE-5)**: This was the original version that used a single coaxial cable into which a connection can be tapped by drilling into the cable to the core. The 5 refers to the maximum segment length of 500m.
- **Thin coax (10BASE-2)**: This is a thinner variety where segments of coaxial cables are connected by BNC connectors. The 2 refers to the maximum segment length of about 200m (185m to be precise).
- **Twisted pair (10BASE-T)**: This uses unshielded twisted pair copper wires as physical layer medium.

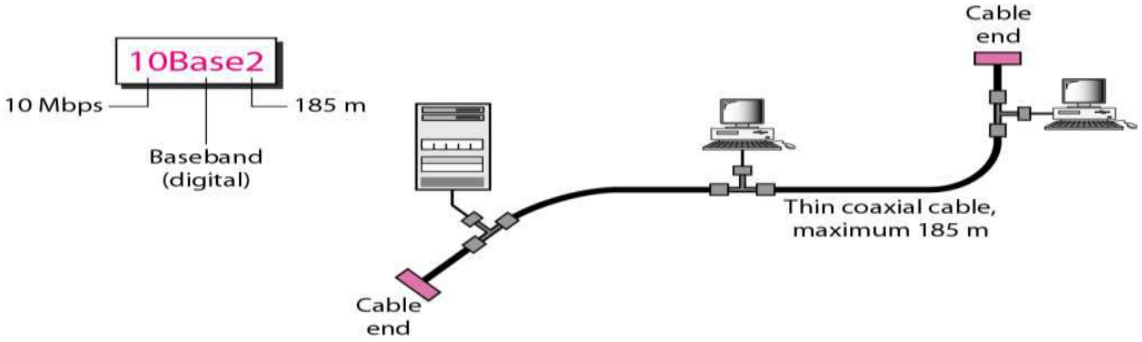
- Ethernet over Fiber (10BASE-F): This uses fiber optic cables as medium of transmission.


Physical Layer Implementations of Standard Ethernet
10 Base 5
10 Base 2
10 Base - T
10 Base - F
Bus Topology, Thick coaxial cable
Bus Topology, Thin coaxial cable
Star Topology, Unshielded twisted pair cable
Star Topology, Fiber optic cable

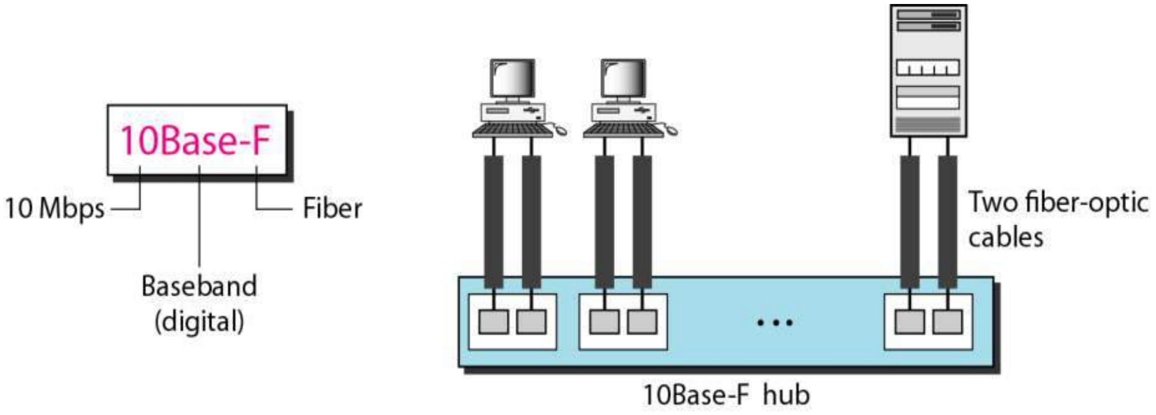
10Base5 implementation



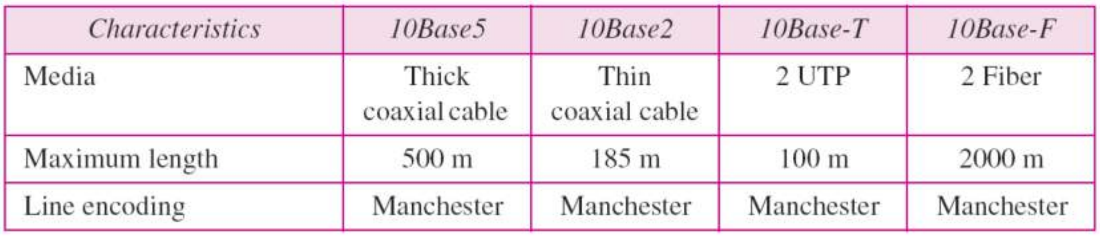
10Base2 implementation



10Base-F implementation



Summary of Standard Ethernet implementations



Characteristics	*10Base5*	*10Base2*	*10Base-T*	*10Base-F*
Media	Thick coaxial cable	Thin coaxial cable	2 UTP	2 Fiber
Maximum length	500 m	185 m	100 m	2000 m
Line encoding	Manchester	Manchester	Manchester	Manchester

Thick Ethernet

Thick Ethernet was the first commercially available form of cabling supported by Ethernet. It is technically known as 10-BASE-5. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and 5 refers to the maximum segment length of 500 metres (1,600 ft). This type of cabling allows 100 stations to be connected to it by vampire taps.

Thin Ethernet

Thin Ethernet, popularly known as cheapernet or thinnet, is among the family of Ethernet standards that uses thinner coaxial cable as a transmission media. It is technically known as 10-BASE-2.

Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and 2 refers to the maximum segment length of about 200 metres (precisely 185 metres). This type of cabling allows a maximum of 30 stations to be connected to it by BNC connectors with 50 centimetres minimum gap between subsequent stations.

Differences between Thick Ethernet and Thin Ethernet

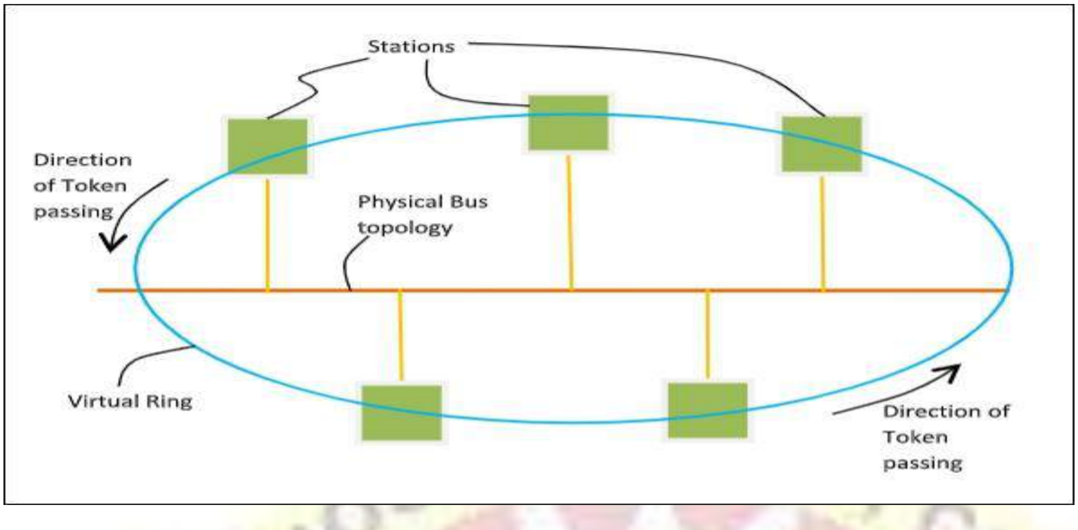
Thick Ethernet	Thin Ethernet
It is technically known as 10-BASE-5.	It is technically known as 10-BASE-5.
The maximum segment length is 500 metres.	The maximum segment length is nearly 200 metres (185 m to be exact).
It uses the thick coaxial cable RG-8/U.	It uses the thinner coaxial cable RG-58/AU.
Connectors used are vampire taps.	Connectors used are BNC connectors.
It allows a maximum of 100 stations to be connected.	It allows a maximum of 30 stations to be connected.

Token Bus (IEEE 802.4) Network

Token Bus (IEEE 802.4) is a standard for implementing token ring over the virtual ring in LANs. The physical media has a bus or a tree topology and uses coaxial cables. A virtual ring is created with the nodes/stations and the token is passed from one node to the next in a sequence along this virtual ring. Each node knows the address of its preceding station and its succeeding station. A station can only transmit data when it has the token. The working principle of the token bus is similar to Token Ring.

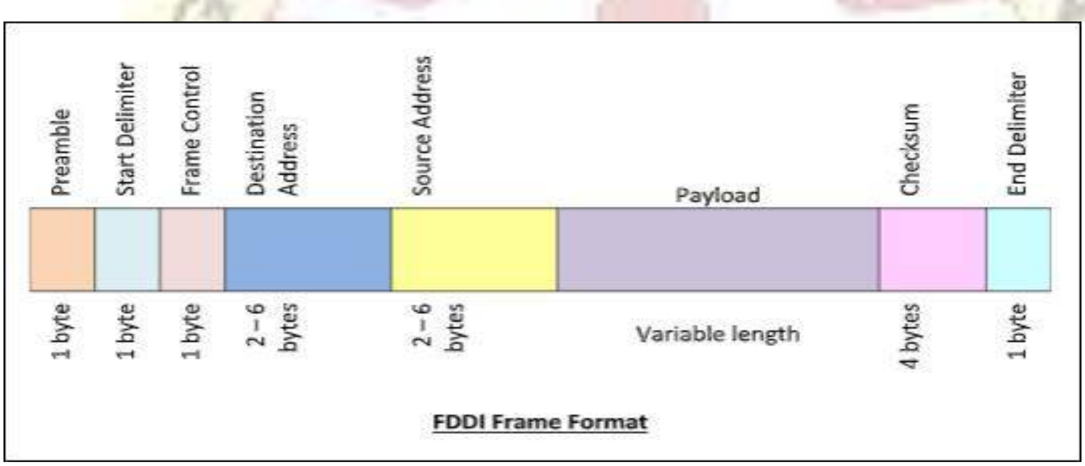
Token Passing Mechanism in Token Bus

A token is a small message that circulates among the stations of a computer network providing permission to the stations for transmission. If a station has data to transmit when it receives a token, it sends the data and then passes the token to the next station; otherwise, it simply passes the token to the next station. This is depicted in the following diagram −



Frame Format of Token Bus

The frame format is given by the following diagram −



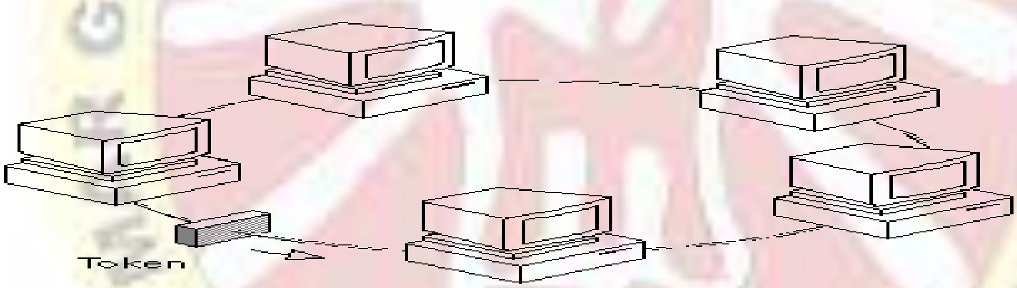
FDDI Frame Format

The fields of a token bus frame are −

- **Preamble:** 1 byte for synchronization.
- **Start Delimiter:** 1 byte that marks the beginning of the frame.
- **Frame Control:** 1 byte that specifies whether this is a data frame or control frame.
- **Destination Address:** 2-6 bytes that specifies address of destination station.
- **Source Address:** 2-6 bytes that specifies address of source station.
- **Payload:** A variable length field that carries the data from the network layer.
- **Checksum:** 4 bytes frame check sequence for error detection.
- **End Delimiter:** 1 byte that marks the end of the frame.

IEEE 802.5: Token Ring Network

- Token Ring is formed by the nodes connected in ring format as shown in the diagram below. The principle used in the token ring network is that a token is circulating in the ring and whichever node grabs that token will have right to transmit the data.
- Whenever a station wants to transmit a frame it inverts a single bit of the 3-byte token which instantaneously changes it into a normal data packet. Because there is only one token, there can atmost be one transmission at a time.
- Since the token rotates in the ring it is guarenteed that every node gets the token with in some specified time. So there is an upper bound on the time of waiting to grab the token so that starvation is avoided.
- There is also an upper limit of 250 on the number of nodes in the network.
- To distinguish the normal data packets from token (control packet) a special sequence is assigned to the token packet. When any node gets the token it first sends the data it wants to send, then recirculates the token.



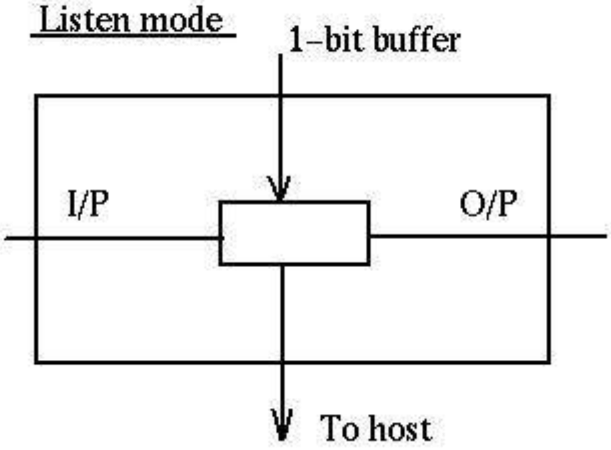
If a node transmits the token and nobody wants to send the data the token comes back to the sender. If the first bit of the token reaches the sender before the transmission of the last bit, then error situation araises. So to avoid this we should have:

propogation delay + transmission of n-bits (1-bit delay in each node) > transmission of the token time

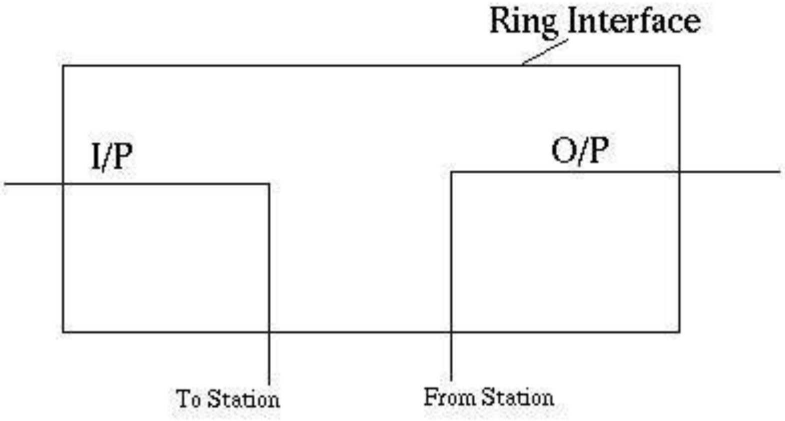
A station may hold the token for the token-holding time. which is 10 ms unless the installation sets a different value. If there is enough time left after the first frame has been transmitted to send more frames, then these frames may be sent as well. After all pending frames have been transmitted or the transmission frame would exceed the token-holding time, the station regenerates the 3-byte token frame and puts it back on the ring.

Modes of Operation

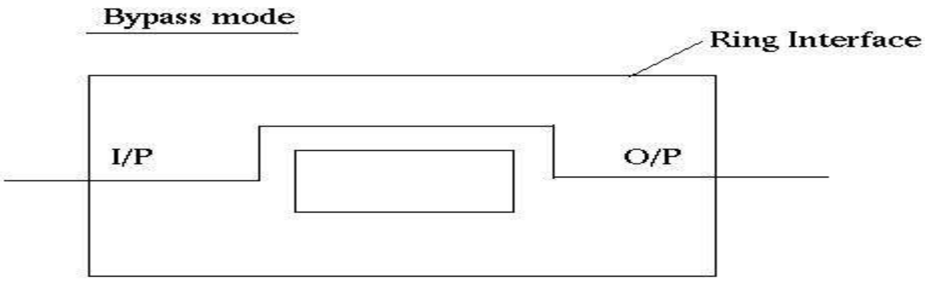
Listen Mode: In this mode the node listens to the data and transmits the data to the next node. In this mode there is a one-bit delay associated with the transmission.



Transmit Mode: In this mode the node just discards the any data and puts the data onto the network.



By-pass Mode: In this mode reached when the node is down. Any data is just bypassed. There is no one-bit delay in this mode.



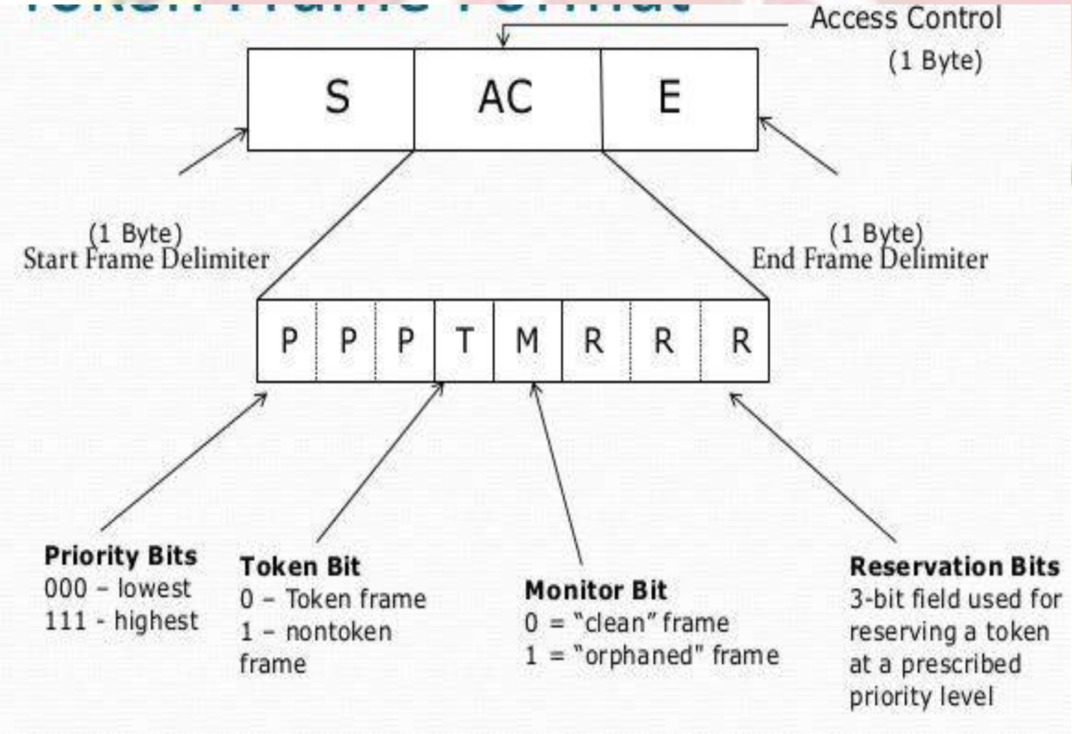
Who should remove the packet from the ring ?

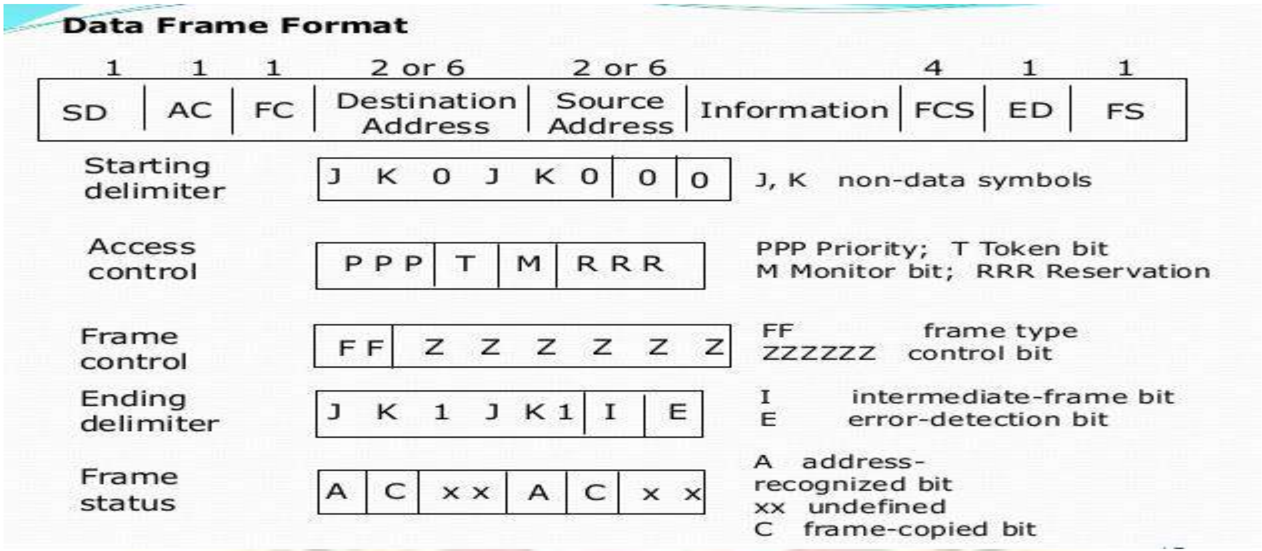
There are 3 possibilities-

1. **The source itself removes the packet after one full round in the ring**.
2. **The destination removes it after accepting it**: This has two potential problems. Firstly, the solution won't work for broadcast or multicast, and secondly, there would be no way to acknowledge the sender about the receipt of the packet.
3. **Have a specialized node only to discard packets**: This is a bad solution as the specialized node would know that the packet has been received by the destination only when it receives the packet the second time and by that time the packet may have actually made about one and half (or almost two in the worst case) rounds in the ring.

Thus the first solution is adopted with the source itself removing the packet from the ring after a full one round. With this scheme, broadcasting and multicasting can be handled as well as the destination can acknowledge the source about the receipt of the packet (or can tell the source about some error).

Token Format





Data Frame Format

SD	AC	FC	Destination Address	Source Address	Information	FCS	ED	FS
1	1	1	2 or 6	2 or 6		4	1	1

Starting delimiter	J K 0 J K 0 | 0 | 0	J, K non-data symbols
Access control	P P P | T | M | R R R	PPP Priority; T Token bit M Monitor bit; RRR Reservation
Frame control	F F | Z Z Z Z Z Z	FF frame type ZZZZZZ control bit
Ending delimiter	J K 1 J K 1 | I | E	I intermediate-frame bit E error-detection bit
Frame status	A | C | x x | A | C | x x	A address-recognized bit xx undefined C frame-copied bit

Tokens are 3 bytes in length and consist of a start delimiter, an access control byte, and an end delimiter.

The *start delimiter* serves to alert each station to the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.

The *access control byte* contains the priority and reservation fields, as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).

Finally, the *end delimiter* signals the end of the token or data/command frame. It also contains bits to indicate a damaged frame and a frame that is the last in a logical sequence.

Data/Command Frames

Data/command frames vary in size, depending on the size of the information field. Data frames carry information for upper-layer protocols; command frames contain control information and have no data for upper-layer protocols.

In data/command frames, a *frame control* byte follows the access control byte. The frame control byte indicates whether the frame contains data or control information. In control frames, this byte specifies the type of control information.

Following the frame control byte are the two *address* fields, which identify the destination and source stations..

The *data* field follows the address fields. The length of this field is limited by the ring token holding time, which defines the maximum time a station may hold the token.

Following the data field is the *frame check sequence* (FCS) field. This field is filled by the source station with a calculated value dependent on the frame contents. The destination station recalculates the value to determine whether the frame may have been damaged in transit. If so, the frame is discarded.

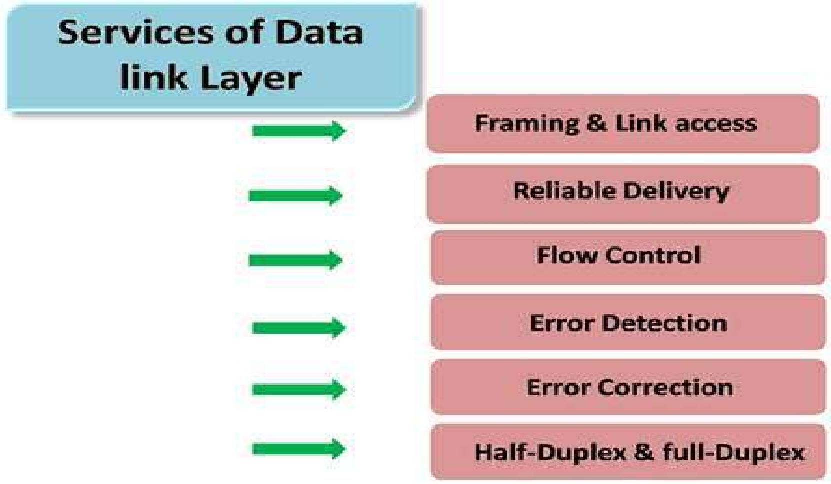
As with the token, the *end delimiter* completes the data/command frame.

UNIT-III

Data Link Layer

- In the OSI model, the data link layer is a 4th layer from the top and 2nd layer from the bottom.
- The communication channel that connects the adjacent nodes is known as links, and in order to move the datagram from source to the destination, the datagram must be moved across an individual link.
- The main responsibility of the Data Link Layer is to transfer the datagram across an individual link.
- The Data link layer protocol defines the format of the packet exchanged across the nodes as well as the actions such as Error detection, retransmission, flow control, and random access.
- The Data Link Layer protocols are Ethernet, token ring, FDDI and PPP.
- An important characteristic of a Data Link Layer is that datagram can be handled by different link layer protocols on different links in a path.

Following services are provided by the Data Link Layer:



Framing & Link access: Frames are the streams of bits received from the network layerintomanageabledataunits.ThisdivisionofstreamofbitsisdonebyDataLinkLayer.

Reliable delivery: Data Link Layer provides a reliable delivery service, i.e., transmits the network layer datagram without any error. A data link layer mainly provides the reliable delivery service over the links as they have higher error rates and they can be corrected locally, link at which an error occurs rather than forcing to retransmit the data.

Flow control: A receiving node can receive the frames at a faster rate than it can process the frame. Without flow control, the receiver's buffer can overflow, and frames can get lost. To overcome this problem, the data link layer uses the flow control to prevent the sending node on one side of the link from overwhelming the receiving node on another side of the link.

Error detection: Errors can be introduced by signal attenuation and noise. Data Link Layer protocol provides a mechanism to detect one or more errors. This is achieved by adding error detection bits in the frame and then receiving node can perform an error check.

Error correction: Error correction is similar to the Error detection, except that receiving node not only detect the errors but also determine where the errors have occurred in the frame.

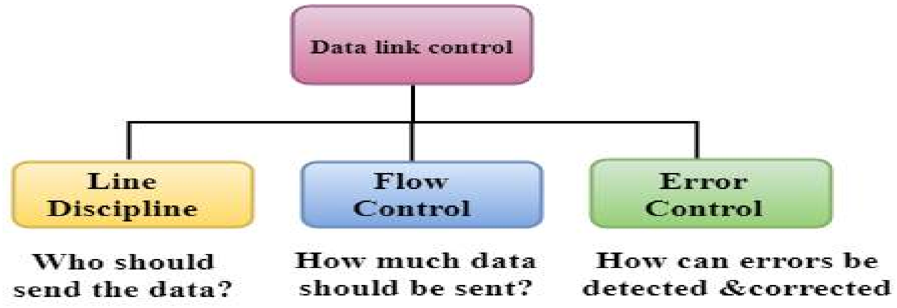
Half-Duplex & Full-Duplex: In a Full-Duplex mode, both the nodes can transmit the data at the same time. In a Half-Duplex mode, only one node can transmit the data at the same time.

Data Link Controls

Data Link Control is the service provided by the Data Link Layer to provide reliable data transfer over the physical medium.

The Data link layer provides three functions:

- Line discipline
- Flow Control
- Error Control


Data link control
Line Discipline
Flow Control
Error Control
Who should send the data?
How much data should be sent?
How can errors be detected &corrected

Line Discipline

- Line Discipline is a functionality of the Data link layer that provides the coordination among the link systems. It determines which device can send, and when it can send the data.

Line Discipline can be achieved in two ways:

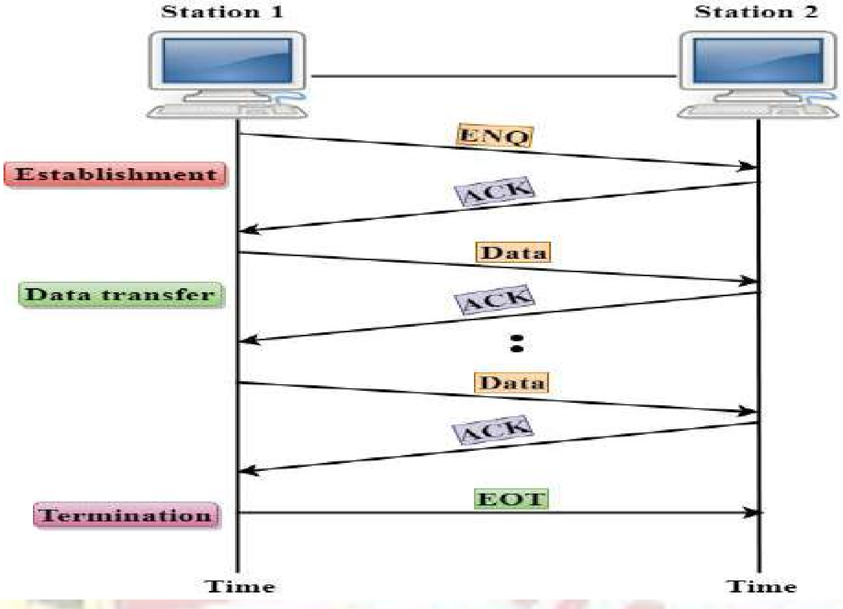
- ENQ/ACK
- Poll/select

END/ACK

- END/ACK stands for Enquiry/Acknowledgement is used when there is no wrong receiver available on the link and having a dedicated path between the two devices so that the device capable of receiving the transmission is the intended one.
- END/ACK coordinates which device will start the transmission and whether the recipient is ready or not.
- The transmitter transmits the frame called an Enquiry (ENQ) asking whether the receiver is available to receive the data or not.
- The receiver responses either with the positive acknowledgement(ACK) or with the negative acknowledgement(NACK) where positive acknowledgement means that the receiver is ready to receive the transmission and negative acknowledgement means that the receiver is unable to accept the transmission.

Following are the responses of the receiver:

- If the response to the ENQ is positive, the sender will transmit its data, and once all of its data has been transmitted, the device finishes its transmission with an EOT (END-of-Transmission) frame.

- If the response to the ENQ is negative, then the sender disconnects and restarts the transmission at another time.
- If the response is neither negative nor positive, the sender assumes that the ENQ frame was lost during the transmission and makes three attempts to establish a link before giving up.
- 

Poll/Select

The Poll/Select method of line discipline works with those topologies where one device is designated as a primary station, and other devices are secondary stations.

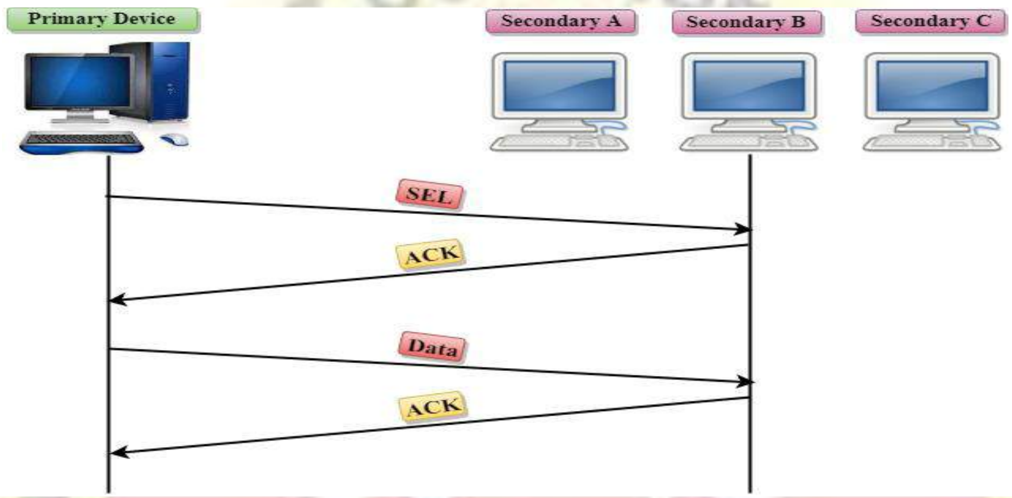
Working of Poll/Select

- In this, the primary device and multiple secondary devices consist of a single transmission line, and all the exchanges are made through the primary device even though the destination is a secondary device.
- The primary device has control over the communication link, and the secondary device follows the instructions of the primary device.
- The primary device determines which device is allowed to use the communication channel. Therefore, we can say that it is an initiator of the session.
- If the primary device wants to receive the data from the secondary device, it asks the secondary device that they anything to send, this process is known as polling.
- If the primary device wants to send some data to the secondary device, then it tells the target secondary to get ready to receive the data, this process is known as selecting.

Select

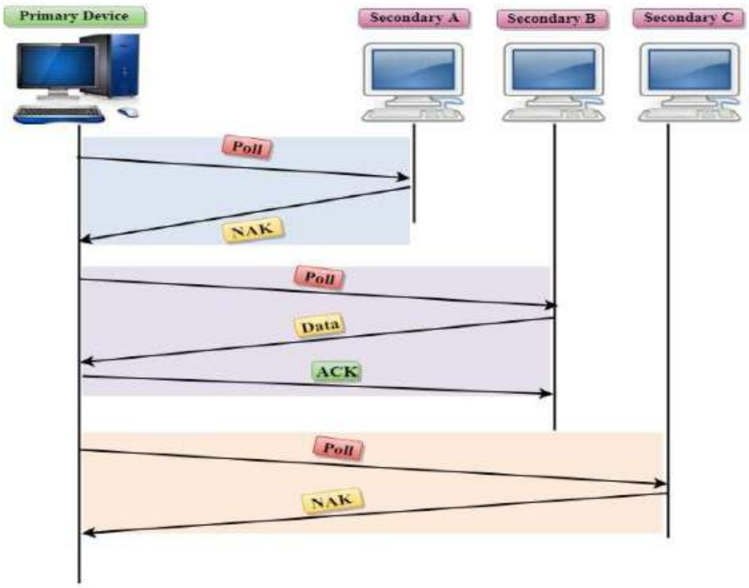
- The select mode is used when the primary device has something to send.

- When the primary device wants to send some data, then it alerts the secondary device for the upcoming transmission by transmitting a Select (SEL) frame, one field of the frame includes the address of the intended secondary device.
- When the secondary device receives the SEL frame, it sends an acknowledgement that indicates the secondary ready status.
- If the secondary device is ready to accept the data, then the primary device sends two or more data frames to the intended secondary device. Once the data has been transmitted, the secondary sends an acknowledgement specifies that the data has been received.



Poll

- The Poll mode is used when the primary device wants to receive some data from the secondary device.
- When a primary device wants to receive the data, then it asks each device whether it has anything to send.
- Firstly, the primary asks (poll) the first secondary device, if it responds with the NACK (Negative Acknowledgement) means that it has nothing to send. Now, it approaches the second secondary device, it responds with the ACK means that it has the data to send. The secondary device can send more than one frame one after another or sometimes it may be required to send ACK before sending each one, depending on the type of the protocol being used.



Flow Control

- It is a set of procedures that tells the sender how much data it can transmit before the data overwhelms the receiver.
- The receiving device has limited speed and limited memory to store the data. Therefore, the receiving device must be able to inform the sending device to stop the transmission temporarily before the limits are reached.
- It requires a buffer, a block of memory for storing the information until they are processed.

Two methods to control the flow of data:

- Stop-and-wait
- Sliding window

Stop-and-wait

- In the Stop-and-wait method, the sender waits for an acknowledgement after every frame it sends.
- When acknowledgement is received, then only next frame is sent. The process of alternately sending and waiting of a frame continues until the sender transmits the EOT (End of transmission) frame.

Advantage of Stop-and-wait

- The Stop-and-wait method is simple as each frame is checked and acknowledged before the next frame is sent.

Disadvantage of Stop-and-wait

- Stop-and-wait technique is inefficient to use as each frame must travel across all the way to the receiver, and an acknowledgement travels all the way before the next frame is sent.

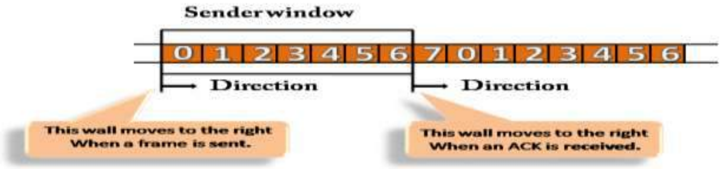
Sliding Window

- The Sliding Window is a method of flow control in which a sender can transmit the several frames before getting an acknowledgement.
- In Sliding Window Control, multiple frames can be sent one after the another due to which capacity of the communication channel can be utilized efficiently.
- A single ACK acknowledge multiple frames.
- Sliding Window refers to imaginary boxes at both the sender and receiver end.
- The window can hold the frames at either end, and it provides the upper limit on the number of frames that can be transmitted before the acknowledgement.
- Frames can be acknowledged even when the window is not completely filled.
- The window has a specific size in which they are numbered as modulo-n means that they are numbered from 0 to n-1. For example, if n = 8, the frames are numbered from 0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,0,1........
- The size of the window is represented as n-1. Therefore, maximum n-1 frames can be sent before acknowledgement.
- When the receiver sends the ACK, it includes the number of the next frame that it wants to receive. For example, to acknowledge the string of frames ending with frame number 4, the receiver will send the ACK containing the number 5. When the sender sees the ACK with the number 5, it got to know that the frames from 0 through 4 have been received.

Sender Window

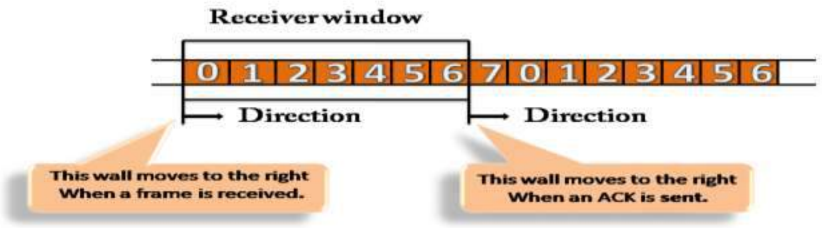
- At the beginning of a transmission, the sender window contains n-1 frames, and when they are sent out, the left boundary moves inward shrinking the size of the window. For example, if the size of the window is w if three frames are sent out, then the number of frames left out in the sender window is w-3.
- Once the ACK has arrived, then the sender window expands to the number which will be equal to the number of frames acknowledged by ACK.
- For example, the size of the window is 7, and if frames 0 through 4 have been sent out and no acknowledgement has arrived, then the sender window contains only two frames, i.e., 5 and 6. Now, if ACK has arrived with a number 4 which means that 0 through 3

frames have arrived undamaged and the sender window is expanded to include the next four frames. Therefore, the sender window contains six frames (5,6,7,0,1,2).


Sender window
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6
Direction
Direction
This wall moves to the right When a frame is sent.
This wall moves to the right When an ACK is received.

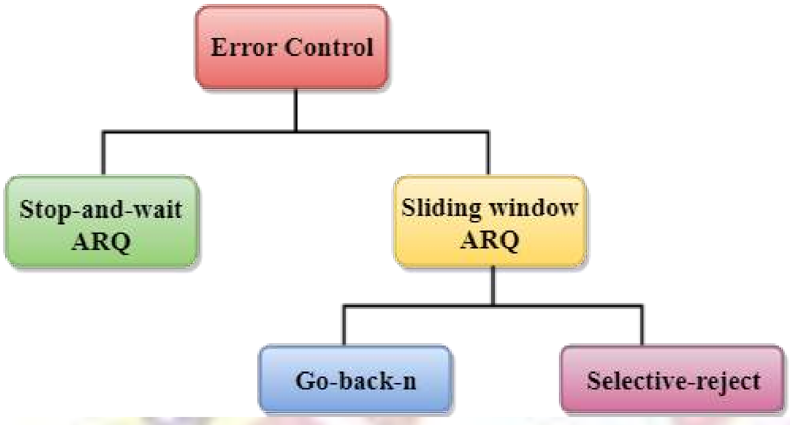
Receiver Window

- At the beginning of transmission, the receiver window does not contain n frames, but it contains n-1 spaces for frames.
- When the new frame arrives, the size of the window shrinks.
- The receiver window does not represent the number of frames received, but it represents the number of frames that can be received before an ACK is sent. For example, the size of the window is w, if three frames are received then the number of spaces available in the window is (w-3).
- Once the acknowledgement is sent, the receiver window expands by the number equal to the number of frames acknowledged.
- Suppose the size of the window is 7 means that the receiver window contains seven spaces for seven frames. If the one frame is received, then the receiver window shrinks and moving the boundary from 0 to 1. In this way, window shrinks one by one, so window now contains the six spaces. If frames from 0 through 4 have sent, then the window contains two spaces before an acknowledgement is sent.


Receiver window
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6
Direction
Direction
This wall moves to the right When a frame is received.
This wall moves to the right When an ACK is sent.

Error Control

Error Control is a technique of error detection and retransmission.



Stop-and-wait ARQ

Stop-and-wait ARQ is a technique used to retransmit the data in case of damaged or lost frames.

This technique works on the principle that the sender will not transmit the next frame until it receives the acknowledgement of the last transmitted frame.

Four features are required for the retransmission:

- The sending device keeps a copy of the last transmitted frame until the acknowledgement is received. Keeping the copy allows the sender to retransmit the data if the frame is not received correctly.
- Both the data frames and the ACK frames are numbered alternately 0 and 1 so that they can be identified individually. Suppose data 1 frame acknowledges the data 0 frame means that the data 0 frame has been arrived correctly and expects to receive data 1 frame.
- If an error occurs in the last transmitted frame, then the receiver sends the NAK frame which is not numbered. On receiving the NAK frame, sender retransmits the data.
- It works with the timer. If the acknowledgement is not received within the allotted time, then the sender assumes that the frame is lost during the transmission, so it will retransmit the frame.

Two possibilities of the retransmission:

- **Damaged Frame:** When the receiver receives a damaged frame, i.e., the frame contains an error, then it returns the NAK frame. For example, when the data 0 frame is sent, and then the receiver sends the ACK 1 frame means that the data 0 has arrived correctly, and transmits the data 1 frame. The sender transmits the next frame: data 1. It reaches undamaged, and the receiver returns ACK 0. The sender transmits the next frame: data 0. The receiver reports an error and returns the NAK frame. The sender retransmits the data 0 frame.

- **Lost Frame:** Sender is equipped with the timer and starts when the frame is transmitted. Sometimes the frame has not arrived at the receiving end so that it can be acknowledged neither positively nor negatively. The sender waits for acknowledgement until the timer goes off. If the timer goes off, it retransmits the last transmitted frame.

Sliding Window ARQ

SlidingWindow ARQ is a technique used for continuous transmission error control.

Three Features used for retransmission:

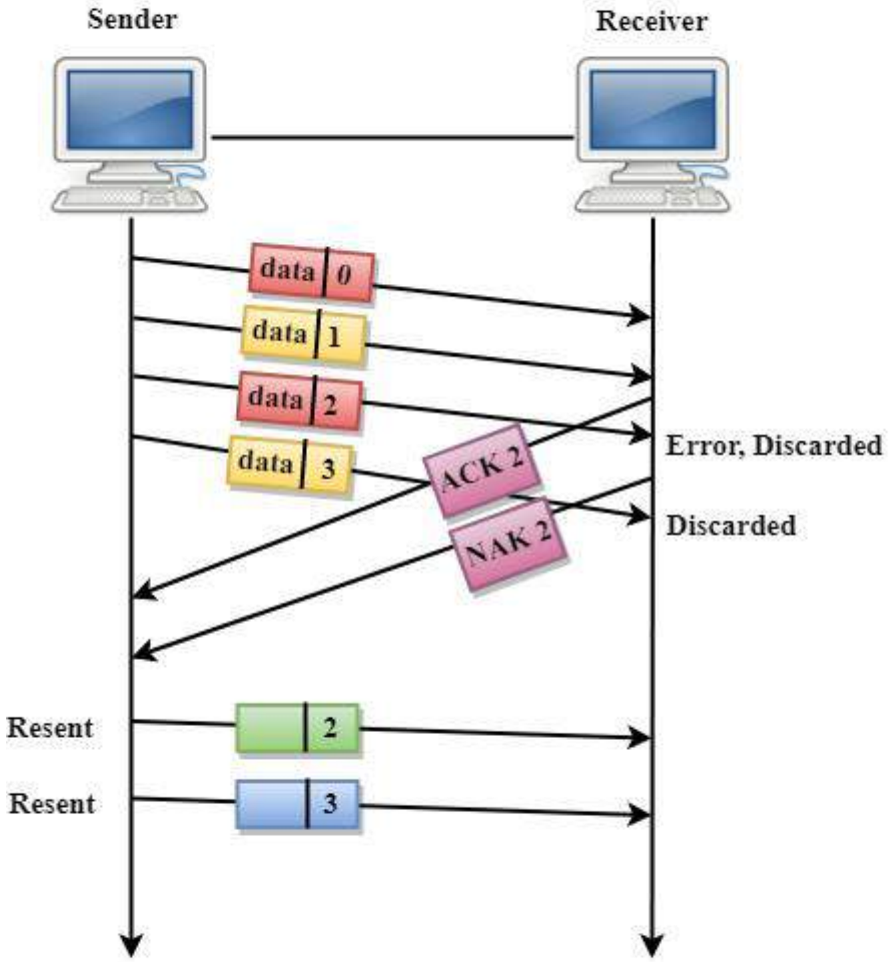
- In this case, the sender keeps the copies of all the transmitted frames until they have been acknowledged. Suppose the frames from 0 through 4 have been transmitted, and the last acknowledgement was for frame 2, the sender has to keep the copies of frames 3 and 4 until they receive correctly.
- The receiver can send either NAK or ACK depending on the conditions. The NAK frame tells the sender that the data have been received damaged. Since the sliding window is a continuous transmission mechanism, both ACK and NAK must be numbered for the identification of a frame. The ACK frame consists of a number that represents the next frame which the receiver expects to receive. The NAK frame consists of a number that represents the damaged frame.
- The sliding window ARQ is equipped with the timer to handle the lost acknowledgements. Suppose then n-1 frames have been sent before receiving any acknowledgement. The sender waits for the acknowledgement, so it starts the timer and waits before sending any more. If the allotted time runs out, the sender retransmits one or all the frames depending upon the protocol used.

Two protocols used in sliding window ARQ:

- **Go-Back-n ARQ:** In Go-Back-N ARQ protocol, if one frame is lost or damaged, then it retransmits all the frames after which it does not receive the positive ACK.

Three possibilities can occur for retransmission:

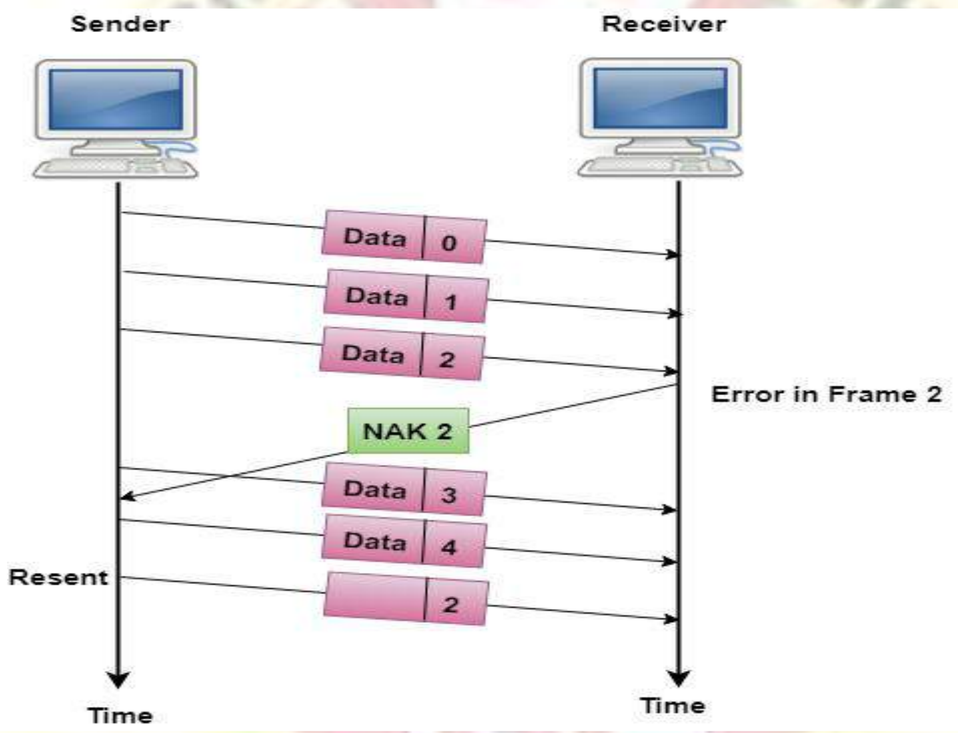
- **Damaged Frame:** When the frame is damaged, then the receiver sends a NAK frame. In the below figure, three frames have been transmitted before an error discovered in the third frame. In this case, ACK 2 has been returned telling that the frames 0,1 have been received successfully without any error. The receiver discovers the error in data 2 frame, so it returns the NAK 2 frame. The frame 3 is also discarded as it is transmitted after the damaged frame. Therefore, the sender retransmits the frames 2,3.



- **Lost Data Frame:** In Sliding window protocols, data frames are sent sequentially. If any of the frames is lost, then the next frame arrive at the receiver is out of sequence. The receiver checks the sequence number of each of the frame, discovers the frame that has been skipped, and returns the NAK for the missing frame. The sending device retransmits the frame indicated by NAK as well as the frames transmitted after the lost frame.
- **Lost Acknowledgement:** The sender can send as many frames as the windows allow before waiting for any acknowledgement. Once the limit of the window is reached, the sender has no more frames to send; it must wait for the acknowledgement. If the acknowledgement is lost, then the sender could wait forever. To avoid such situation, the sender is equipped with the timer that starts counting whenever the window capacity is reached. If the acknowledgement has not been received within the time limit, then the sender retransmits the frame since the last ACK.

Selective-Reject ARQ

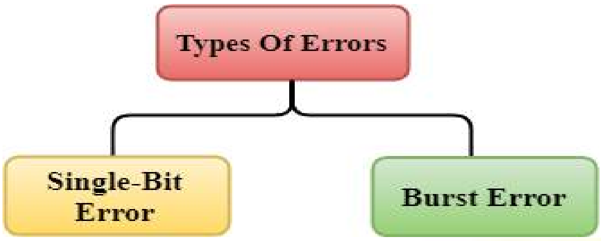
- Selective-Reject ARQ technique is more efficient than Go-Back-n ARQ.
- In this technique, only those frames are retransmitted for which negative acknowledgement (NAK) has been received.
- The receiver storage buffer keeps all the damaged frames on hold until the frame in error is correctly received.
- The receiver must have an appropriate logic for reinserting the frames in a correct order.
- The sender must consist of a searching mechanism that selects only the requested frame for retransmission.



Error Detection

When data is transmitted from one device to another device, the system does not guarantee whether the data received by the device is identical to the data transmitted by another device. An Error is a situation when the message received at the receiver end is not identical to the message transmitted.

Types Of Errors

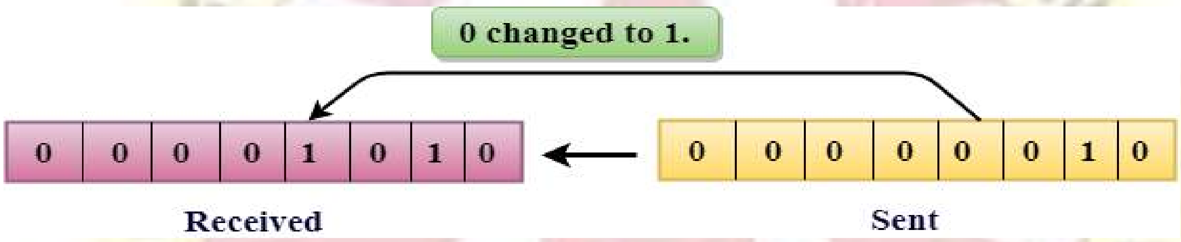


Errors can be classified into two categories:

- Single-Bit Error
- Burst Error

Single-Bit Error:

The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.

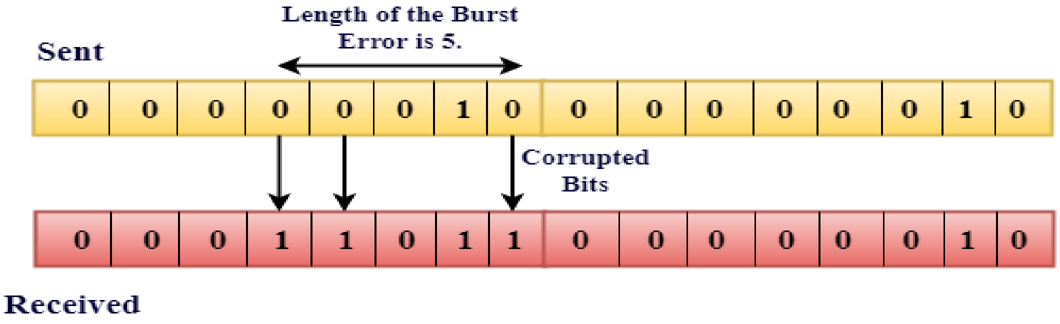


Single-Bit Error does not appear more likely in Serial Data Transmission. Single-Bit Error mainly occurs in Parallel Data Transmission.

Burst Error:

The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.

The Burst Error is determined from the first corrupted bit to the last corrupted bit.



The duration of noise in Burst Error is more than the duration of noise in Single-Bit.

Burst Errors are most likely to occurr in Serial Data Transmission.

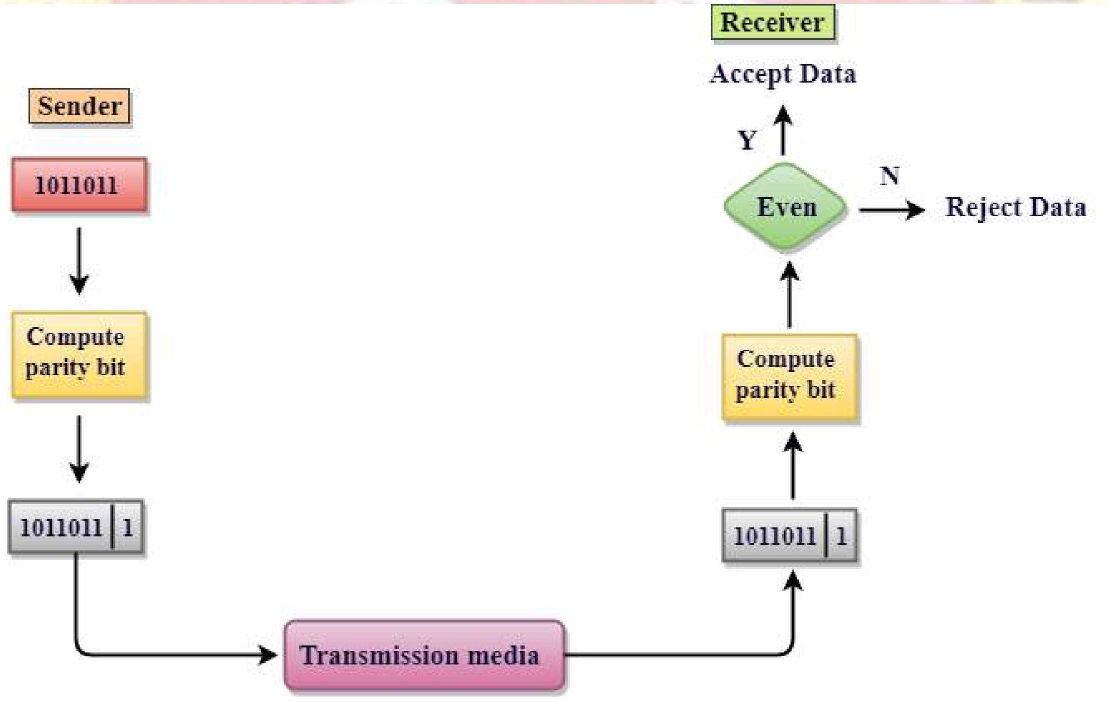
The number of affected bits depends on the duration of the noise and data rate.

The most popular Error Detecting Techniques are:

- Single parity check
- Two-dimensional parity check
- Checksum
- Cyclic redundancy check

Single Parity Check

- Single Parity checking is the simple mechanism and inexpensive to detect the errors.
- In this technique, a redundant bit is also known as a parity bit which is appended at the end of the data unit so that the number of 1s becomes even. Therefore, the total number of transmitted bits would be 9 bits.
- If the number of 1s bits is odd, then parity bit 1 is appended and if the number of 1s bits is even, then parity bit 0 is appended at the end of the data unit.
- At the receiving end, the parity bit is calculated from the received data bits and compared with the received parity bit.
- This technique generates the total number of 1s even, so it is known as even-parity checking.

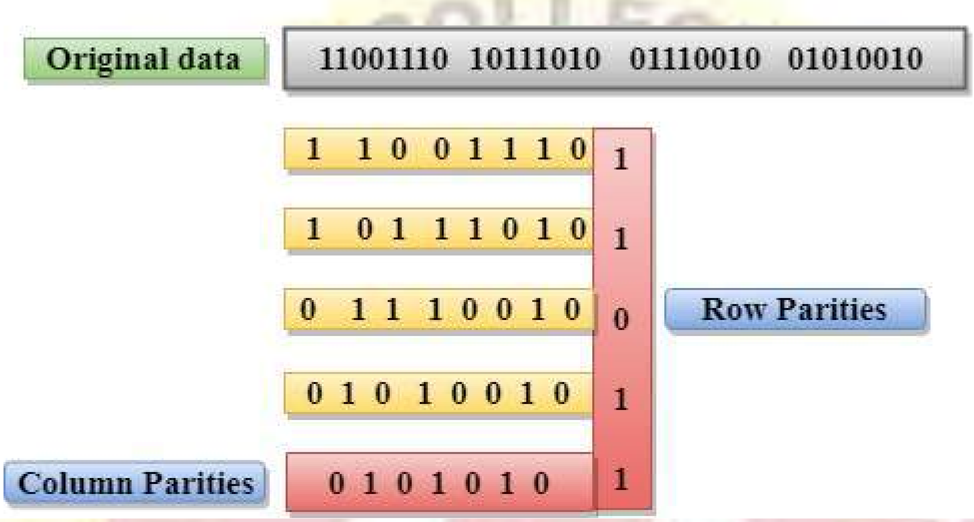


Drawbacks Of Single Parity Checking

- It can only detect single-bit errors which are very rare.
- If two bits are interchanged, then it cannot detect the errors.

Two-Dimensional Parity Check

- Performance can be improved by using **Two-Dimensional Parity Check** which organizes the data in the form of a table.
- Parity check bits are computed for each row, which is equivalent to the single-parity check.
- In Two-Dimensional Parity check, a block of bits is divided into rows, and the redundant row of bits is added to the whole block.
- At the receiving end, the parity bits are compared with the parity bits computed from the received data.



Drawbacks Of 2D Parity Check

- If two bits in one data unit are corrupted and two bits exactly the same position in another data unit are also corrupted, then 2D Parity checker will not be able to detect the error.
- This technique cannot be used to detect the 4-bit errors or more in some cases.

Checksum Generator

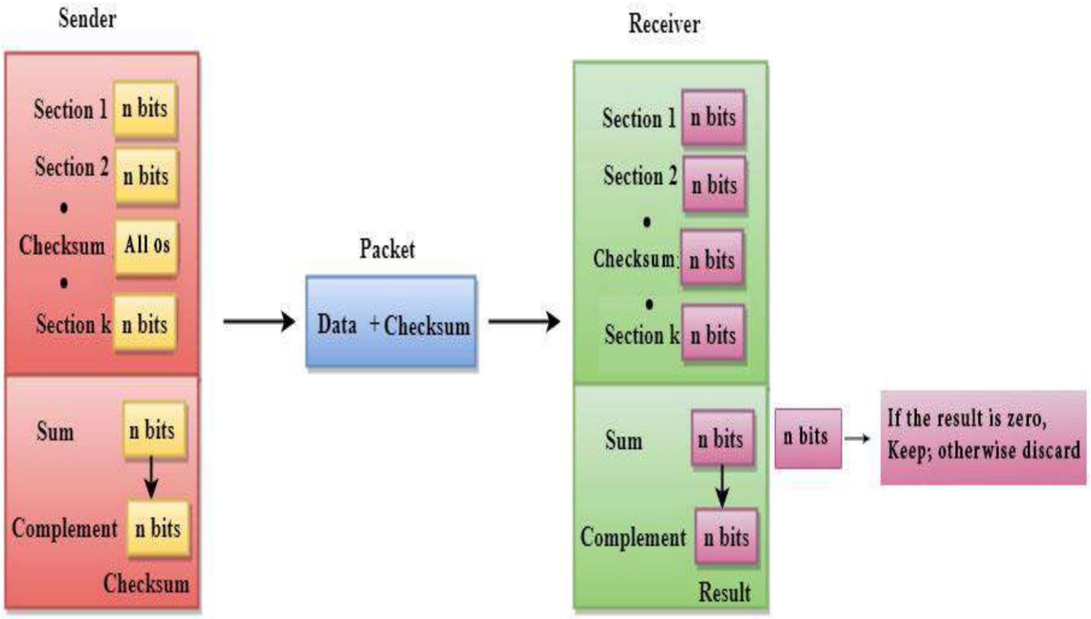
A Checksum is generated at the sending side. Checksum generator subdivides the data into equal segments of n bits each, and all these segments are added together by using one's complement arithmetic. The sum is complemented and appended to the original data, known as checksum field. The extended data is transmitted across the network.

The Sender follows the given steps:

1. The block unit is divided into k sections, and each of n bits.
2. All the k sections are added together by using one's complement to get the sum.
3. The sum is complemented and it becomes the checksum field.
4. The original data and checksum field are sent across the network.

Checksum Checker

A Checksum is verified at the receiving side. The receiver subdivides the incoming data into equal segments of n bits each, and all these segments are added together, and then this sum is complemented. If the complement of the sum is zero, then the data is accepted otherwise data is rejected.



The Receiver follows the given steps:

1. The block unit is divided into k sections and each of n bits.
2. All the k sections are added together by using one's complement algorithm to get the sum.
3. The sum is complemented.
4. If the result of the sum is zero, then the data is accepted otherwise the data is discarded.

Cyclic Redundancy Check (CRC)

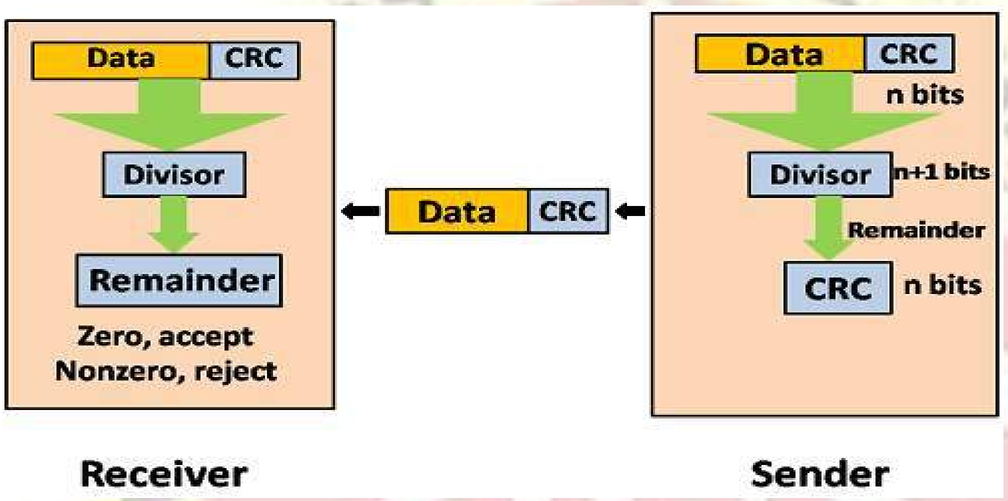
Following are the steps used in CRC for error detection:

- In CRC technique, a string of n 0s is appended to the data unit, and this n number is less than the number of bits in a predetermined number, known as division which is n+1 bits.
- Secondly, the newly extended data is divided by a divisor using a process is known as binary division. The remainder generated from this division is known as CRC remainder.

- Thirdly, the CRC remainder replaces the appended 0s at the end of the original data. This newly generated unit is sent to the receiver.
- The receiver receives the data followed by the CRC remainder. The receiver will treat this whole unit as a single unit, and it is divided by the same divisor that was used to find the CRC remainder.

If the resultant of this division is zero which means that it has no error, and the data is accepted.

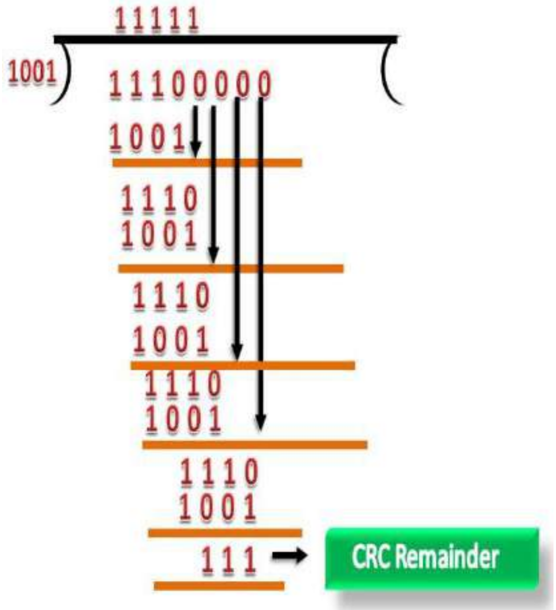
If the resultant of this division is not zero which means that the data consists of an error. Therefore, the data is discarded.



Suppose the original data is 11100 and divisor is 1001.

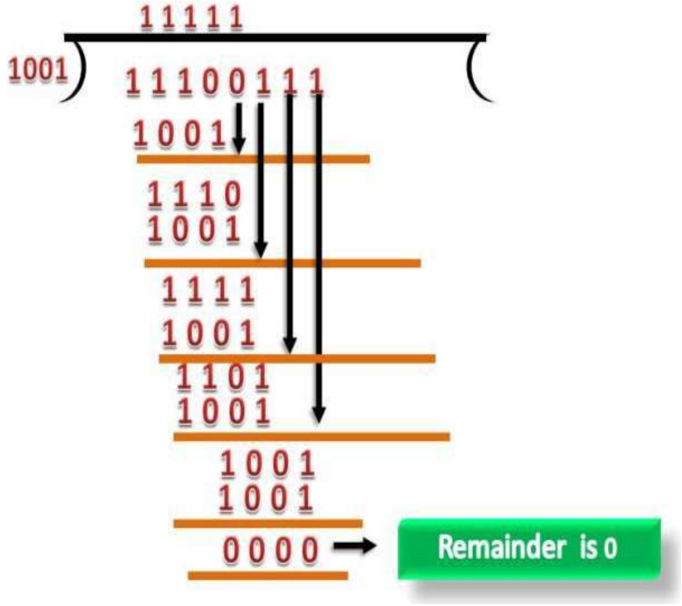
CRC Generator

- A CRC generator uses a modulo-2 division. Firstly, three zeroes are appended at the end of the data as the length of the divisor is 4 and we know that the length of the string 0s to be appended is always one less than the length of the divisor.
- Now, the string becomes 11100000, and the resultant string is divided by the divisor 1001.
- The remainder generated from the binary division is known as CRC remainder. The generated value of the CRC remainder is 111.
- CRC remainder replaces the appended string of 0s at the end of the data unit, and the final string would be 11100111 which is sent across the network.



CRC Checker

- The functionality of the CRC checker is similar to the CRC generator.
- When the string 11100111 is received at the receiving end, then CRC checker performs the modulo-2 division.
- A string is divided by the same divisor, i.e., 1001.
- In this case, CRC checker generates the remainder of zero. Therefore, the data is accepted.



Network Layer

- The Network Layer is the third layer of the OSI model.
- It handles the service requests from the transport layer and further forwards the service request to the data link layer.
- The network layer translates the logical addresses into physical addresses
- It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
- The main role of the network layer is to move the packets from sending host to the receiving host.

The main functions performed by the network layer are:

- **Routing:** When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.
- **Logical Addressing:** The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.
- **Internetworking:** This is the main role of the network layer that it provides the logical connection between different types of networks.
- **Fragmentation:** The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.

Services Provided by the Network Layer

- **Guaranteed delivery:** This layer provides the service which guarantees that the packet will arrive at its destination.
- **Guaranteed delivery with bounded delay:** This service guarantees that the packet will be delivered within a specified host-to-host delay bound.
- **In-Order packets:** This service ensures that the packet arrives at the destination in the order in which they are sent.
- **Guaranteed max jitter:** This service ensures that the amount of time taken between two successive transmissions at the sender is equal to the time between their receipt at the destination.

- **Security services:** The network layer provides security by using a session key between the source and destination host. The network layer in the source host encrypts the payloads of datagrams being sent to the destination host. The network layer in the destination host would then decrypt the payload. In such a way, the network layer maintains the data integrity and source authentication services.

Network Addressing

- Network Addressing is one of the major responsibilities of the network layer.
- The boundary between the router and link is known as an interface, and the router can have multiple interfaces, one for each of its links. Each interface is capable of sending and receiving the IP packets, so IP requires each interface to have an address.
- Each IP address is 32 bits long, and they are represented in the form of "dot-decimal notation" where each byte is written in the decimal form, and they are separated by the period. An IP address would look like 193.32.216.9 where 193 represents the decimal notation of first 8 bits of an address, 32 represents the decimal notation of second 8 bits of an address.

Routing

- A Router is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router.
- A Router works at the network layer in the OSI model and internet layer in TCP/IP model
- The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.
- The routing protocols use the metric to determine the best path for the packet delivery. The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path, etc. used by the routing algorithm to determine the optimal path to the destination.
- The routing algorithm initializes and maintains the routing table for the process of path determination.

Routing Metrics and Costs

Routing metrics and costs are used for determining the best route to the destination. The factors used by the protocols to determine the shortest path, these factors are known as a metric.

- **Hop count:** Hop count is defined as a metric that specifies the number of passes through internetworking devices such as a router, a packet must travel in a route to move from source to the destination. If the routing protocol considers the hop as a primary metric value, then the path with the least hop count will be considered as the best path to move from source to the destination.

- **Delay:** It is a time taken by the router to process, queue and transmit a datagram to an interface. The protocols use this metric to determine the delay values for all the links along the path end-to-end. The path having the lowest delay value will be considered as the best path.
- **Bandwidth:** The capacity of the link is known as a bandwidth of the link. The bandwidth is measured in terms of bits per second. The link that has a higher transfer rate like gigabit is preferred over the link that has the lower capacity like 56 kb. The protocol will determine the bandwidth capacity for all the links along the path, and the overall higher bandwidth will be considered as the best route.
- **Load:** Load refers to the degree to which the network resource such as a router or network link is busy. A Load can be calculated in a variety of ways such as CPU utilization, packets processed per second. If the traffic increases, then the load value will also be increased. The load value changes with respect to the change in the traffic.
- **Reliability:** Reliability is a metric factor may be composed of a fixed value. It depends on the network links, and its value is measured dynamically. Some networks go down more often than others. After network failure, some network links repaired more easily than other network links. Any reliability factor can be considered for the assignment of reliability ratings, which are generally numeric values assigned by the system administrator.

Types of Routing

Static Routing(Non adaptive)

- Static Routing is also known as Nonadaptive Routing.
- It is a technique in which the administrator manually adds the routes in a routing table.
- A Router can send the packets for the destination along the route defined by the administrator.
- In this technique, routing decisions are not made based on the condition or topology of the networks

Advantages of Static Routing

Following are the advantages of Static Routing:

- **No Overhead:** It has ho overhead on the CPU usage of the router. Therefore, the cheaper router can be used to obtain static routing.

- **Bandwidth:** It has not bandwidth usage between the routers.
- **Security:** It provides security as the system administrator is allowed only to have control over the routing to a particular network.

Disadvantages of Static Routing:

Following are the disadvantages of Static Routing:

- For a large network, it becomes a very difficult task to add each route manually to the routing table.
- The system administrator should have a good knowledge of a topology as he has to add each route manually.

Dynamic Routing (Adaptive)

- It is also known as Adaptive Routing.
- It is a technique in which a router adds a new route in the routing table for each packet in response to the changes in the condition or topology of the network.
- Dynamic protocols are used to discover the new routes to reach the destination.
- If any route goes down, then the automatic adjustment will be made to reach the destination.

Advantages of Dynamic Routing:

- It is easier to configure.
- It is more effective in selecting the best route in response to the changes in the condition or topology.

Disadvantages of Dynamic Routing:

- It is more expensive in terms of CPU and bandwidth usage.
- It is less secure as compared to default and static routing.

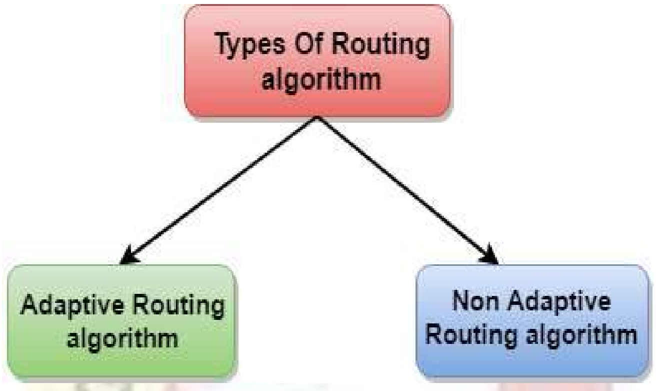
Routing algorithm

- In order to transfer the packets from source to the destination, the network layer must determine the best route through which packets can be transmitted.
- Whether the network layer provides datagram service or virtual circuit service, the main job of the network layer is to provide the best route. The routing protocol provides this job.
- The routing protocol is a routing algorithm that provides the best path from the source to the destination. The best path is the path that has the "least-cost path" from source to the destination.
- Routing is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm.

Classification of a Routing algorithm

The Routing algorithm is divided into two categories:

- Adaptive Routing algorithm
- Non-adaptive Routing algorithm

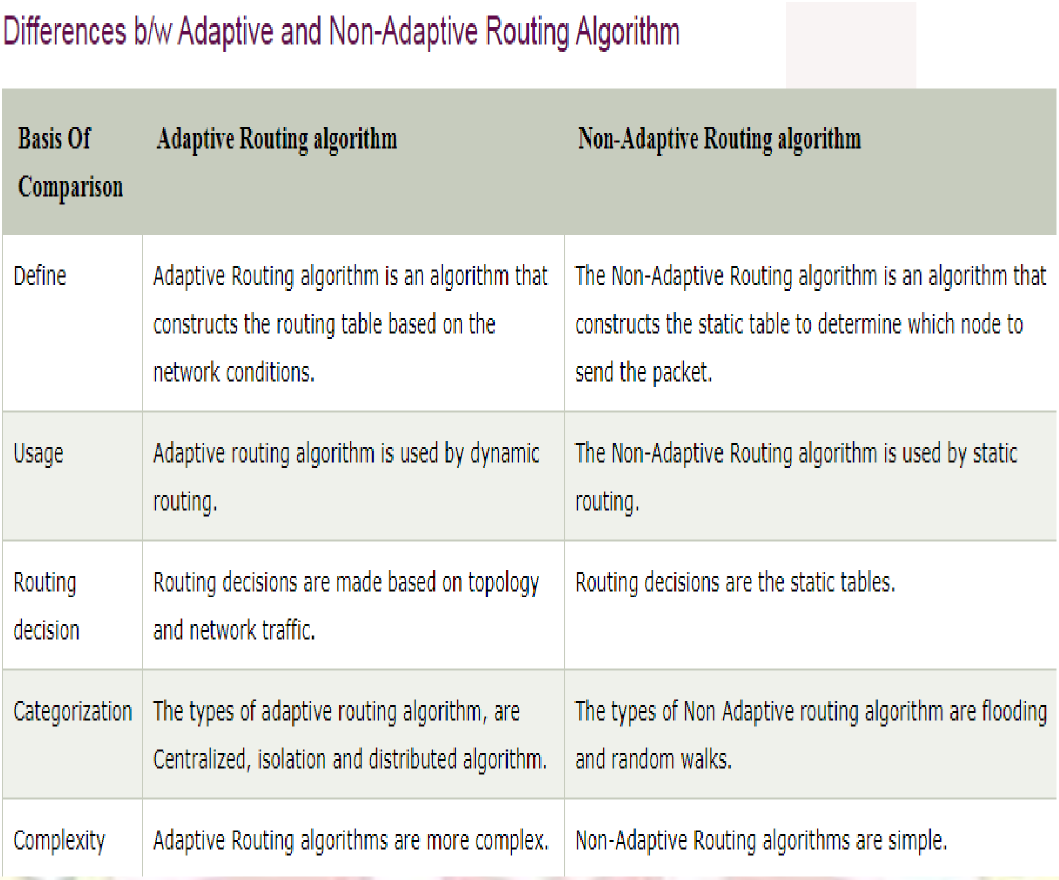

Types Of Routing algorithm
Adaptive Routing algorithm
Non Adaptive Routing algorithm

Adaptive Routing algorithm

- An adaptive routing algorithm is also known as dynamic routing algorithm.
- This algorithm makes the routing decisions based on the topology and network traffic.
- The main parameters related to this algorithm are hop count, distance and estimated transit time.

Non-Adaptive Routing algorithm

- Non Adaptive routing algorithm is also known as a static routing algorithm.
- When booting up the network, the routing information stores to the routers.
- Non Adaptive routing algorithms do not take the routing decision based on the network topology or network traffic.



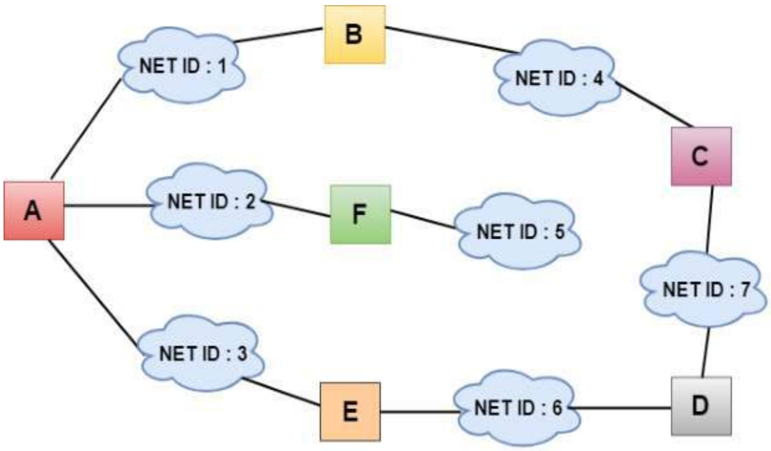
Differences b/w Adaptive and Non-Adaptive Routing Algorithm

Basis Of Comparison	Adaptive Routing algorithm	Non-Adaptive Routing algorithm
Define	Adaptive Routing algorithm is an algorithm that constructs the routing table based on the network conditions.	The Non-Adaptive Routing algorithm is an algorithm that constructs the static table to determine which node to send the packet.
Usage	Adaptive routing algorithm is used by dynamic routing.	The Non-Adaptive Routing algorithm is used by static routing.
Routing decision	Routing decisions are made based on topology and network traffic.	Routing decisions are the static tables.
Categorization	The types of adaptive routing algorithm, are Centralized, isolation and distributed algorithm.	The types of Non Adaptive routing algorithm are flooding and random walks.
Complexity	Adaptive Routing algorithms are more complex.	Non-Adaptive Routing algorithms are simple.

Distance Vector Routing Algorithm

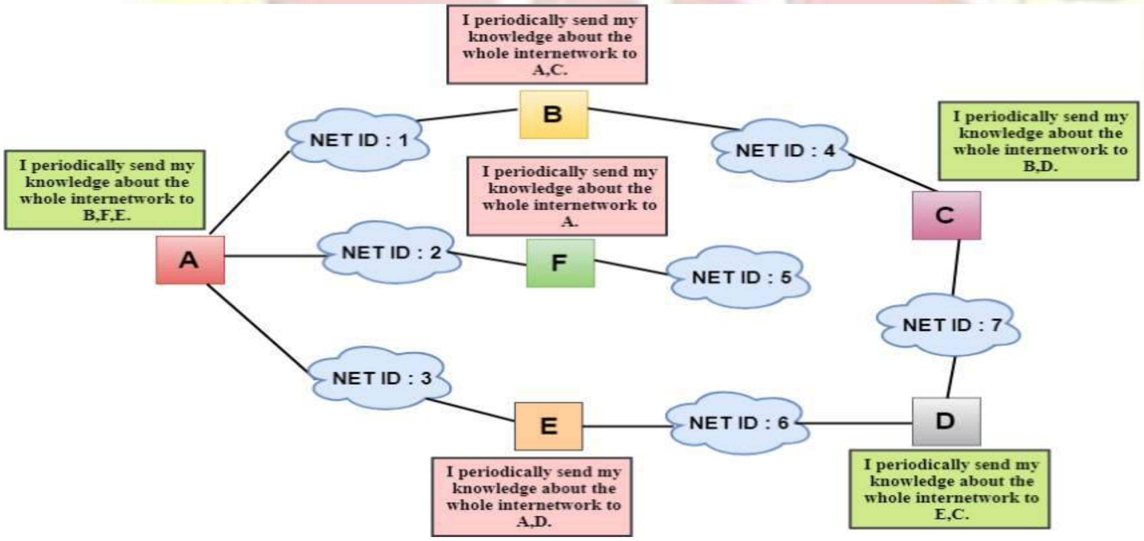
Three Keys to understand the working of Distance Vector Routing Algorithm:

- **Knowledge about the whole network:** Each router shares its knowledge through the entire network. The Router sends its collected knowledge about the network to its neighbors.
- **Routing only to neighbors:** The router sends its knowledge about the network to only those routers which have direct links. The router sends whatever it has about the network through the ports. The information is received by the router and uses the information to update its own routing table.
- **Information sharing at regular intervals:** Within 30 seconds, the router sends the information to the neighboring routers.



- In Distance vector each cloud represents the network, and the number inside the cloud represents the network ID.
- All the LANs are connected by routers, and they are represented in boxes labeled as A, B, C, D, E, F.
- Distance vector routing algorithm simplifies the routing process by assuming the cost of every link is one unit. Therefore, the efficiency of transmission can be measured by the number of links to reach the destination.
- In Distance vector routing, the cost is based on hop count.

The router sends the knowledge to the immediate neighbors. The neighbors add this knowledge to their own knowledge and sends the updated table to their own neighbors. In this way, routers get its own information plus the new information about the neighbors.


I periodically send my knowledge about the whole internetwork to A,C.
B
NET ID : 1
NET ID : 4
I periodically send my knowledge about the whole internetwork to B,D.
I periodically send my knowledge about the whole internetwork to B,F,E.
I periodically send my knowledge about the whole internetwork to A.
C
A
NET ID : 2
F
NET ID : 5
NET ID : 7
NET ID : 3
E
NET ID : 6
D
I periodically send my knowledge about the whole internetwork to A,D.
I periodically send my knowledge about the whole internetwork to E,C.

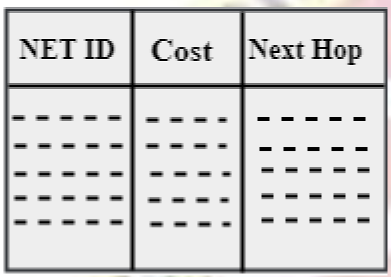
Routing Table

Two process occurs:

- Creating the Table
- Updating the Table

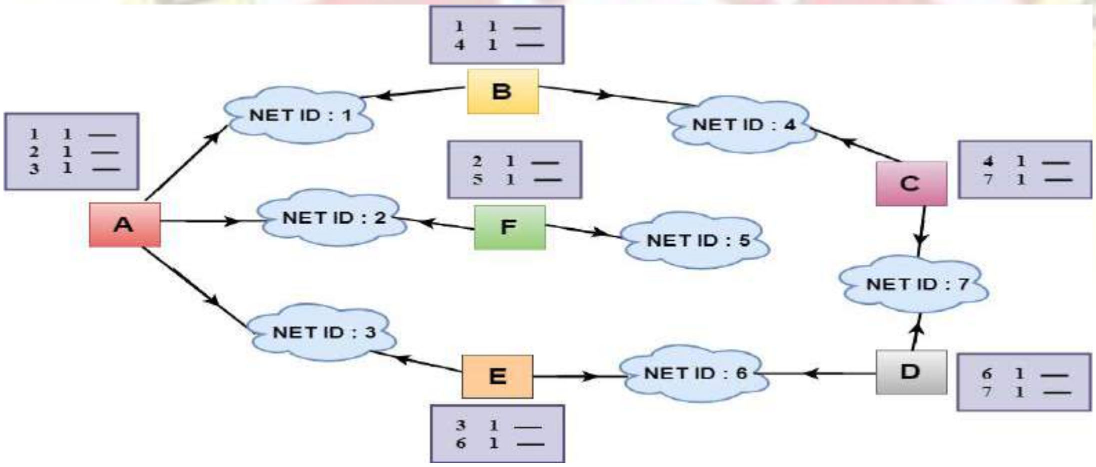
Creating the Table

Initially, the routing table is created for each router that contains atleast three types of information such as Network ID, the cost and the next hop.



NET ID	Cost	Next Hop
- - - - -	- - - -	- - - - -
- - - - -	- - - -	- - - - -
- - - - -	- - - -	- - - - -
- - - - -	- - - -	- - - - -
- - - - -	- - - -	- - - - -

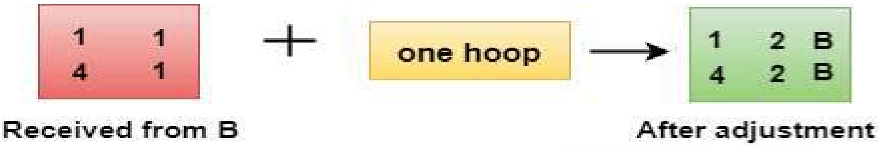
- **NET ID:** The Network ID defines the final destination of the packet.
- **Cost:** The cost is the number of hops that packet must take to get there.
- **Next hop:** It is the router to which the packet must be delivered.



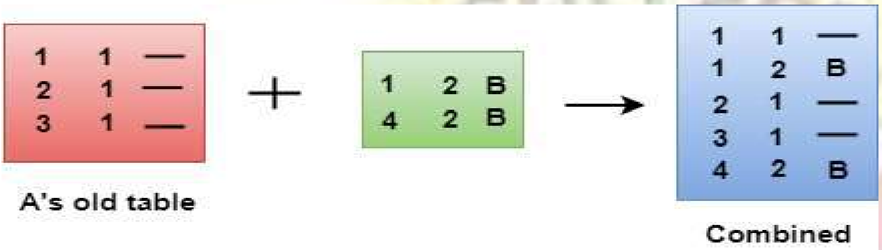
Updating the Table

- When A receives a routing table from B, then it uses its information to update the table.
- The routing table of B shows how the packets can move to the networks 1 and 4.

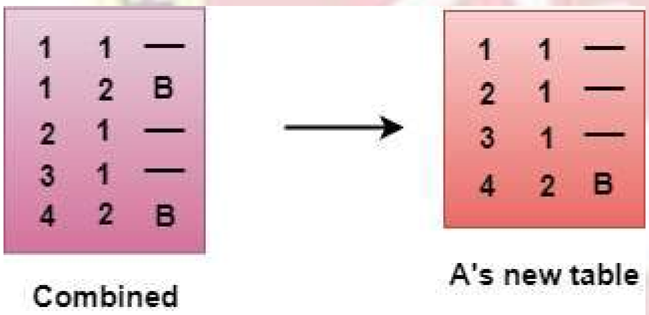
- The B is a neighbor to the A router, the packets from A to B can reach in one hop. So, 1 is added to all the costs given in the B's table and the sum will be the cost to reach a particular network.



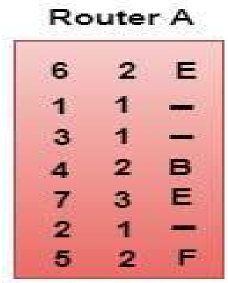
- After adjustment, A then combines this table with its own table to create a combined table.



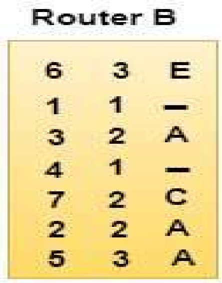
- The combined table may contain some duplicate data. In the above figure, the combined table of router A contains the duplicate data, so it keeps only those data which has the lowest cost. For example, A can send the data to network 1 in two ways. The first, which uses no next router, so it costs one hop. The second requires two hops (A to B, then B to Network 1). The first option has the lowest cost, therefore it is kept and the second one is dropped.



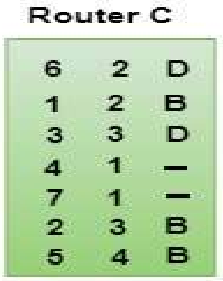
- The process of creating the routing table continues for all routers. Every router receives the information from the neighbors, and update the routing table.


Router A

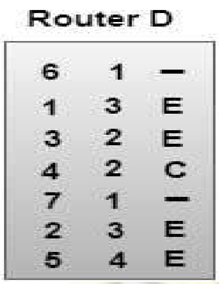
6	2	E
1	1	—
3	1	—
4	2	B
7	3	E
2	1	—
5	2	F


Router B

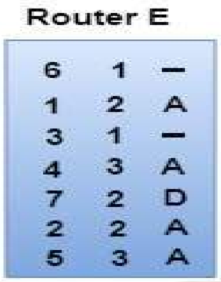
6	3	E
1	1	—
3	2	A
4	1	—
7	2	C
2	2	A
5	3	A


Router C

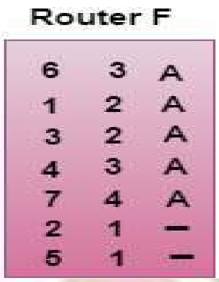
6	2	D
1	2	B
3	3	D
4	1	—
7	1	—
2	3	B
5	4	B


Router D

6	1	—
1	3	E
3	2	E
4	2	C
7	1	—
2	3	E
5	4	E


Router E

6	1	—
1	2	A
3	1	—
4	3	A
7	2	D
2	2	A
5	3	A


Router F

6	3	A
1	2	A
3	2	A
4	3	A
7	4	A
2	1	—
5	1	—

Link State Routing

Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router in the internetwork.

- The Link state routing algorithm is also known as Dijkstra's algorithm which is used to find the shortest path from one node to every other node in the network.
- The Dijkstra's algorithm is an iterative, and it has the property that after kth iteration of the algorithm, the least cost paths are well known for k destination nodes.

The three keys to understand the Link State Routing algorithm:

- **Knowledge about the neighborhood:** Instead of sending its routing table, a router sends the information about its neighborhood only. A router broadcast its identities and cost of the directly attached links to other routers.
- **Flooding:** Each router sends the information to every other router on the internetwork except its neighbors. This process is known as Flooding. Every router that receives the packet sends the copies to all its neighbors. Finally, each and every router receives a copy of the same information.
- **Information sharing:** A router sends the information to every other router only when the change occurs in the information.

Leaky Bucket Algorithm

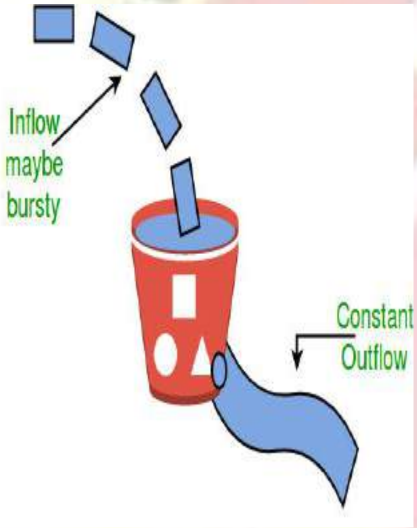
Consider a Bucket with a small hole at the bottom, whatever may be the rate of water pouring into the bucket; the rate at which water comes out from that small hole is constant. Once the bucket is full, any additional water entering it spills over the sides and is lost. The same idea of leaky bucket can be applied to packets. Each network interface contains a leaky bucket.

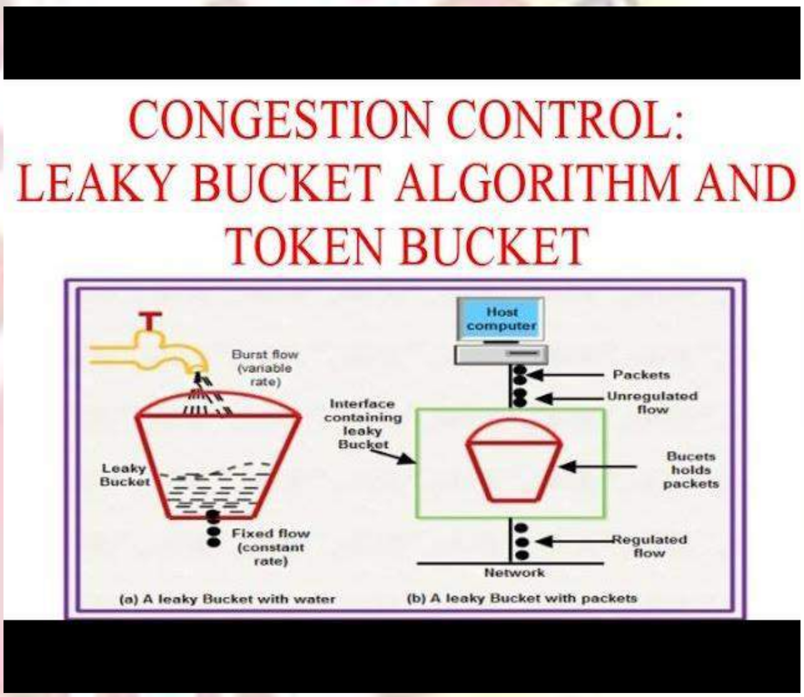
- When the host has to send a packet, the packet is thrown into the bucket.

• The bucket leaks at a constant rate, meaning the network interface transmits packets at aconstant rate.

• Bursty traffic is converted to a uniform traffic by the leaky bucket.

• In practice the bucket is a finite queue that outputs at a finite rate.




CONGESTION CONTROL: LEAKY BUCKET ALGORITHM AND TOKEN BUCKET

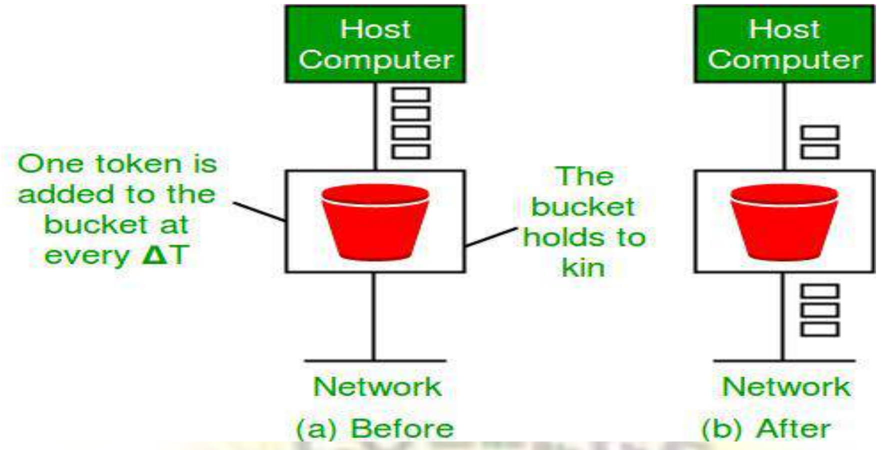
Burst flow (variable rate)
Leaky Bucket
Fixed flow (constant rate)
Interface containing leaky Bucket
Host computer
Packets
Unregulated flow
Bucets holds packets
Regulated flow
Network
(a) A leaky Bucket with water
(b) A leaky Bucket with packets

Implementation of this algorithm is easy and consists of a finite queue. Whenever a packet arrives, if there is room in the queue it is queued up and if there is no room then the packet is discarded.

Token Bucket Algorithm

For many applications it is better to allow the output to speed up somewhat when a larger burst arrives than to loose the data. Token Bucket algorithm provides such a solution. In this algorithm leaky bucket holds token, generated at regular intervals.

- In regular intervals tokens are thrown into the bucket. ƒ
- The bucket has a maximum capacity. ƒ
- If there is a ready packet, a token is removed from the bucket, and the packet is send. ƒ
- If there is no token in the bucket, the packet cannot be send.



The bucket holds two tokens, and three packets are waiting to be sent out of the interface, two packets have been sent out by consuming two tokens, and 1 packet is still left.

The token bucket algorithm is less restrictive than the leaky bucket algorithm that it allows bursty traffic. However, the limit of burst is restricted by the number of tokens available in the bucket at a particular instant of time.

The implementation of basic token bucket algorithm is simple; a variable is used just to count the tokens. This counter is incremented every t seconds and is decremented whenever a packet is sent. Whenever this counter reaches zero, no further packet is sent.

UNIT V

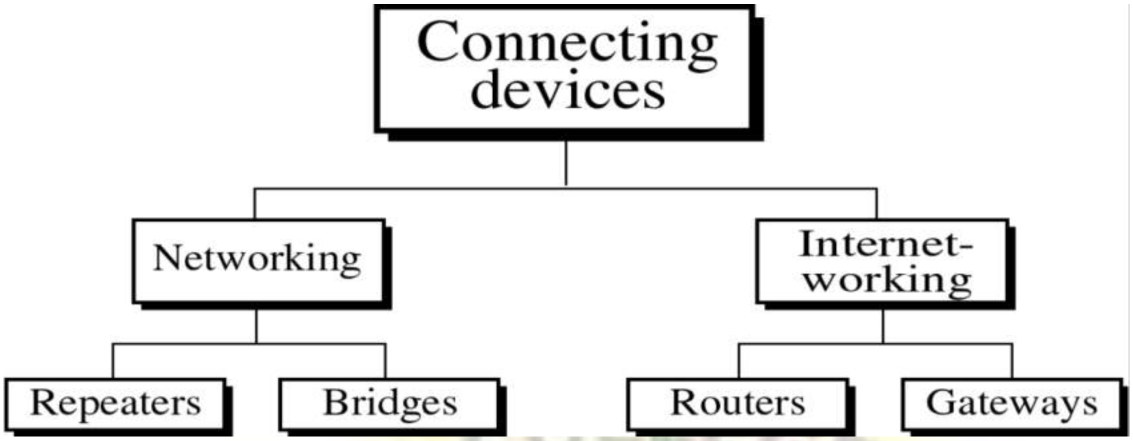
Internetworking Devices.

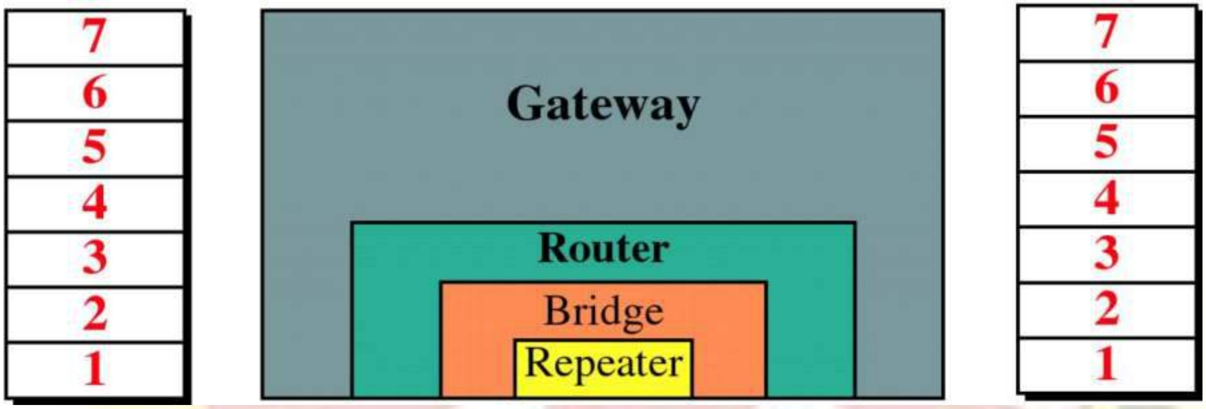
Devices that connect networks are called Inter networking devices.

Internetworking devices are divided into categories based on the *OSI* layer at which they operate

Internetworking devices are divided into categories based on the *OSI* layer at which they operate.

- Repeaters operate at the physical layer.
- Bridges operate at the Data Link layer.
- Routers operate at the Network layer.
- Gateways operate at any layer higher than the Network layer





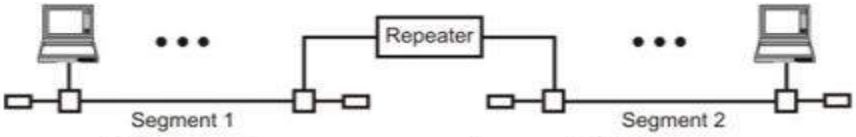
Devices

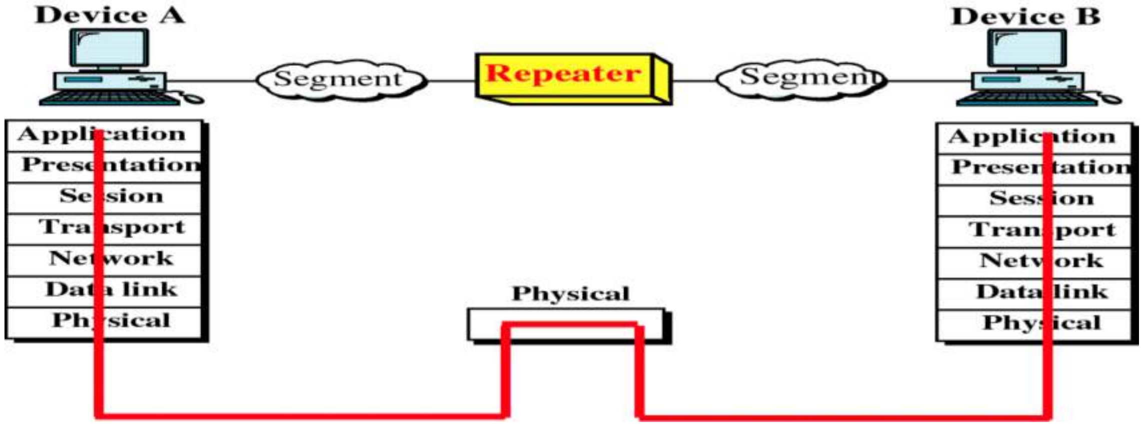
. Repeaters

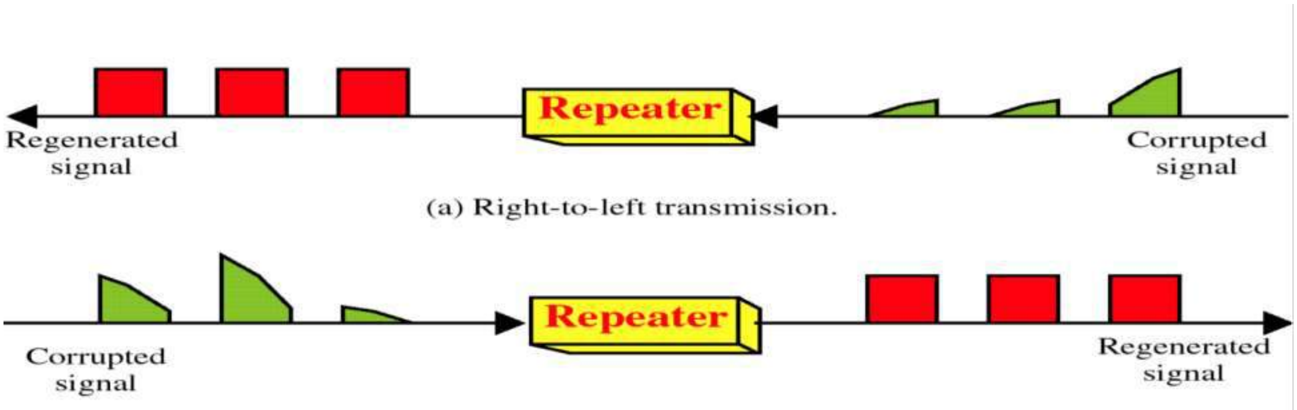
Repeaters are used to extend the length of the Network. Repeaters were created to regenerate and amplify weak signals, thus extending the length of the network. The basic function of a repeater is to retime, reshape, and reamplify the data signal to its original level.

Important features of a repeater are as follows:

- A repeater connects different segments of a LAN
- A repeater forwards every frame it receives
- A repeater is a regenerator, not an amplifier
- Repeaters operate at the physical layer of the OSI model.





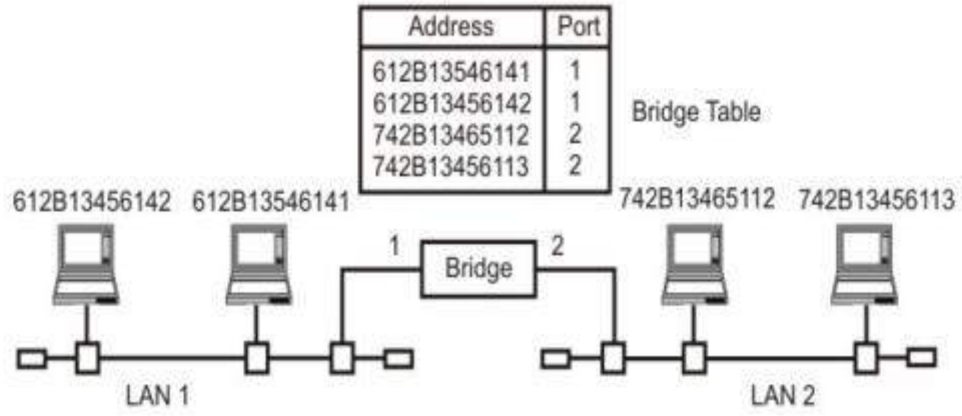


(a) Right-to-left transmission.

(b) Left-to-right transmission.

III. BRIDGES

- The device that can be used to interconnect two separate LANs is known as a bridge. It is commonly used to connect two similar or dissimilar LANs
- The bridge operates in layer 2, that is data-link layer and that is why it is called level-2 relay with reference to the OSI model. It links similar or dissimilar LANs, designed to store and forward frames, it is protocol independent and transparent to the end stations. A bridge must contain addressing and routing capability.



Address	Port
612B13546141	1
612B13456142	1
742B13465112	2
742B13456113	2

Key features of a bridge are mentioned below:

a. A bridge operates both in physical and data-link layer

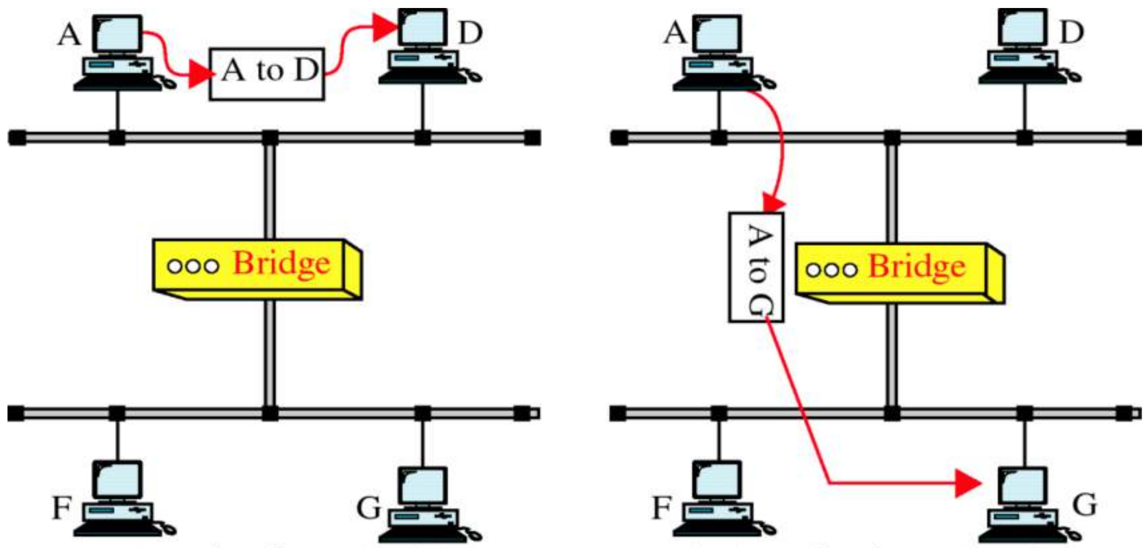
b. A bridge uses a table for filtering/routing

c. A bridge does not change the physical (MAC) addresses in a frame.

- Types of bridges:

a. Transparent Bridges

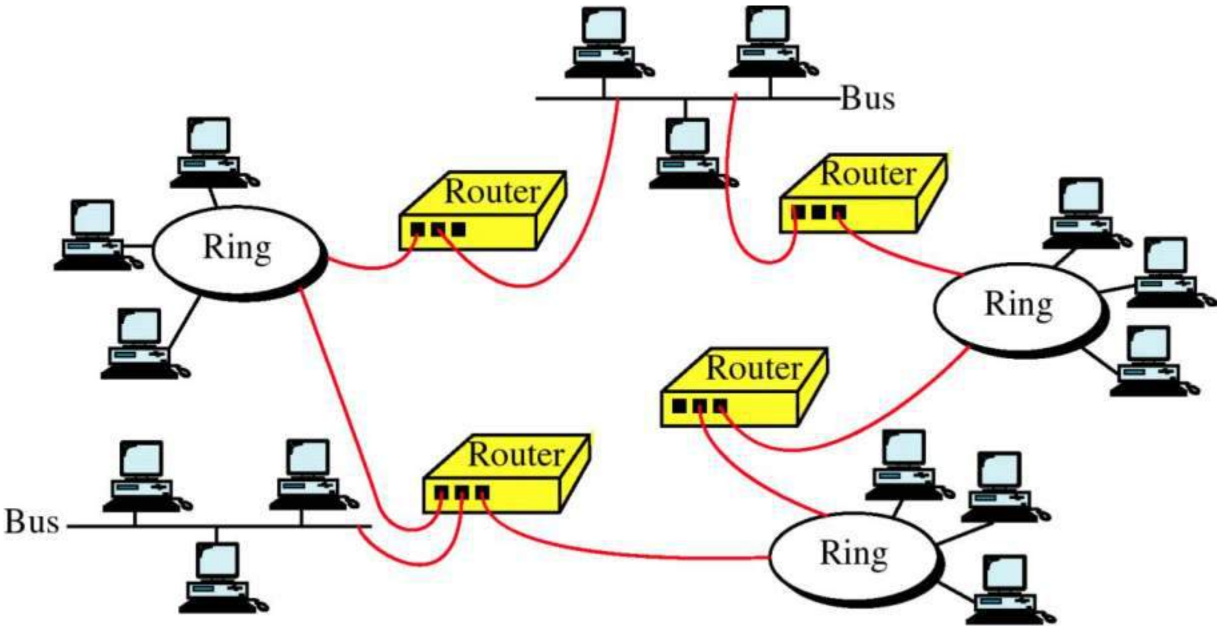
b. Source routing bridges



a. A packet from A to D

b. A packet from A to G

V. ROUTER

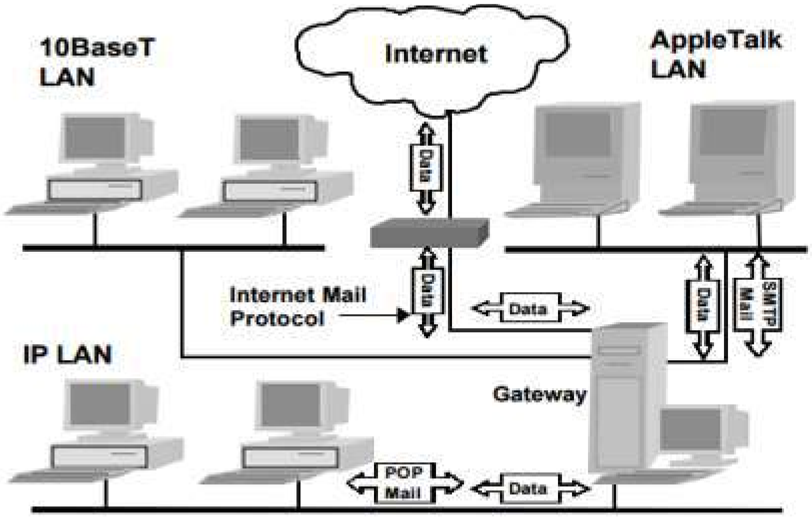


- Routers link two or more different networks together, such as an Internet Protocol network. These networks can consist of various types of LAN segments, for example, Ethernet, token ring, or Fiber Distributed Data Interface (FDDI).
- A router receives packets and selects the optimum path to forward the packet across the network.
- Routers build a table of all the device addresses (routing table) across the networks.
- Using this table, the router forwards a transmission from the sending station to the receiving station across the best path. Routers operate at the network level of the OSI model.

VI. GATEWAYS

- Gateways are multi-purpose connection devices. They are able to convert the format of data in one computing environment to a format that is usable in another computer environment (for example, AppleTalk and DEC net).
- The term gateway is sometimes used when referring to a router.
- For example, gateways translate different electronic mail protocols and convey email across the Internet.

Gateways Translate Different Network Protocols



Gateways can operate at all layers of the OSI model since them:

Gateways can operate at all layers of the OSI model since them:

- Can provide a physical link between networks.
- Create junctions between dissimilar networks.
- Translate different network protocols and/ or applications (for example, electronic mail between the Internet and a commercial online service with its own mail protocol).

TRANSPORT LAYER

- The transport layer is a 4th layer from the top.
- The main role of the transport layer is to provide the communication services directly to the application processes running on different hosts.
- The transport layer provides a logical communication between application processes running on different hosts. Although the application processes on different hosts are not physically connected, application processes use the logical communication provided by the transport layer to send the messages to each other.
- The transport layer protocols are implemented in the end systems but not in the network routers.
- A computer network provides more than one protocol to the network applications. For example, TCP and UDP are two transport layer protocols that provide a different set of services to the network layer.

- All transport layer protocols provide multiplexing/demultiplexing service. It also provides other services such as reliable data transfer, bandwidth guarantees, and delay guarantees.
- Each of the applications in the application layer has the ability to send a message by using TCP or UDP. The application communicates by using either of these two protocols. Both TCP and UDP will then communicate with the internet protocol in the internet layer. The applications can read and write to the transport layer. Therefore, we can say that communication is a two-way process.

Services provided by the Transport Layer

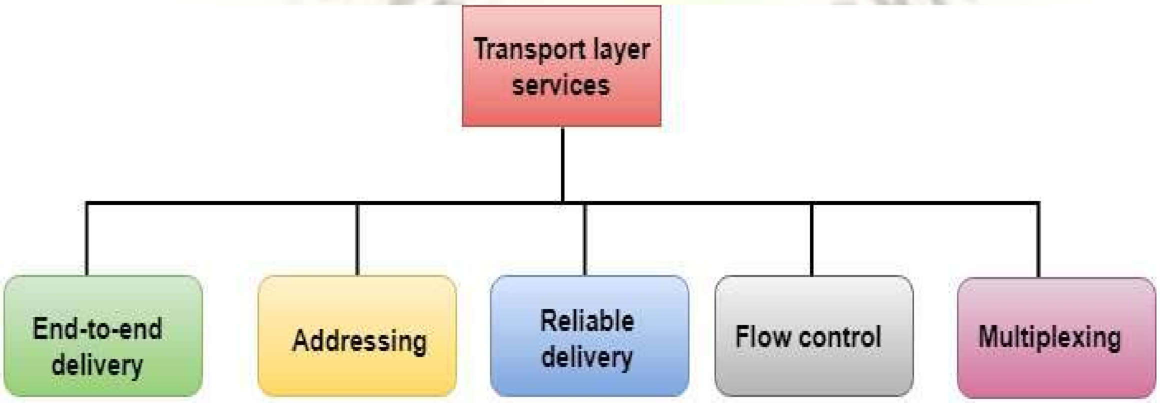
The services provided by the transport layer are similar to those of the data link layer. The data link layer provides the services within a single network while the transport layer provides the services across an internetwork made up of many networks. The data link layer controls the physical layer while the transport layer controls all the lower layers.

The services provided by the transport layer protocols can be divided into five categories:

- End-to-end delivery
- Addressing
- Reliable delivery
- Flow control
- Multiplexing

End-to-end delivery:

The transport layer transmits the entire message to the destination. Therefore, it ensures the end-to-end delivery of an entire message from a source to the destination.



Reliable delivery:

The transport layer provides reliability services by retransmitting the lost and damaged packets.

The reliable delivery has four aspects:

- Error control
- Sequence control
- Loss control
- Duplication control

Error Control

- The primary role of reliability is **Error Control**. In reality, no transmission will be 100 percent error-free delivery. Therefore, transport layer protocols are designed to provide error-free transmission.
- The data link layer also provides the error handling mechanism, but it ensures only node-to-node error-free delivery. However, node-to-node reliability does not ensure the end-to-end reliability.
- The data link layer checks for the error between each network. If an error is introduced inside one of the routers, then this error will not be caught by the data link layer. It only detects those errors that have been introduced between the beginning and end of the link. Therefore, the transport layer performs the checking for the errors end-to-end to ensure that the packet has arrived correctly.

Sequence Control

- The second aspect of the reliability is sequence control which is implemented at the transport layer.
- On the sending end, the transport layer is responsible for ensuring that the packets received from the upper layers can be used by the lower layers. On the receiving end, it ensures that the various segments of a transmission can be correctly reassembled.

Loss Control

Loss Control is a third aspect of reliability. The transport layer ensures that all the fragments of a transmission arrive at the destination, not some of them. On the sending end, all the fragments of transmission are given sequence numbers by a transport layer. These sequence numbers allow the receiver?s transport layer to identify the missing segment.

Duplication Control

Duplication Control is the fourth aspect of reliability. The transport layer guarantees that no duplicate data arrive at the destination. Sequence numbers are used to identify the lost packets; similarly, it allows the receiver to identify and discard duplicate segments.

Flow Control

Flow control is used to prevent the sender from overwhelming the receiver. If the receiver is overloaded with too much data, then the receiver discards the packets and asking for the retransmission of packets. This increases network congestion and thus, reducing the system performance. The transport layer is responsible for flow control. It uses the sliding window protocol that makes the data transmission more efficient as well as it controls the flow of data so that the receiver does not become overwhelmed. Sliding window protocol is byte oriented rather than frame oriented.

Multiplexing

The transport layer uses the multiplexing to improve transmission efficiency.

Multiplexing can occur in two ways:

- **Upward multiplexing:** Upward multiplexing means multiple transport layer connections use the same network connection. To make more cost-effective, the transport layer sends several transmissions bound for the same destination along the same path; this is achieved through upward multiplexing.
- **Downward multiplexing:** Downward multiplexing means one transport layer connection uses the multiple network connections. Downward multiplexing allows the transport layer to split a connection among several paths to improve the throughput. This type of multiplexing is used when networks have a low or slow capacity.

Addressing

- According to the layered model, the transport layer interacts with the functions of the session layer. Many protocols combine session, presentation, and application layer protocols into a single layer known as the application layer. In these cases, delivery to the session layer means the delivery to the application layer. Data generated by an application on one machine must be transmitted to the correct application on another machine. In this case, addressing is provided by the transport layer.

- The transport layer provides the user address which is specified as a station or port. The port variable represents a particular TS user of a specified station known as a Transport Service access point (TSAP). Each station has only one transport entity.
- The transport layer protocols need to know which upper-layer protocols are communicating.

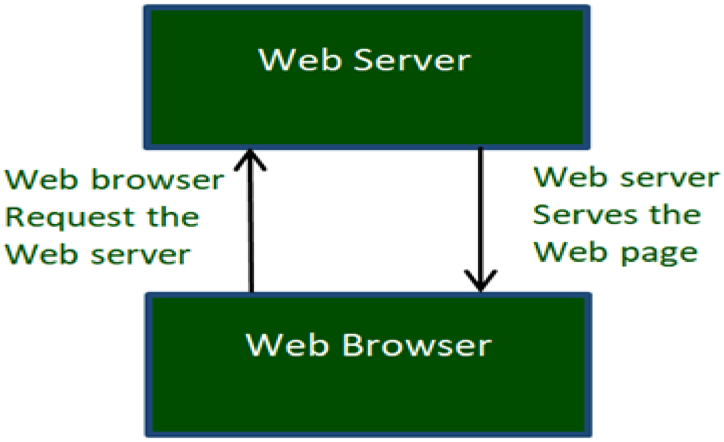
World Wide Web

World Wide Web, which is also known as a Web, is a collection of websites or web pages stored in web servers and connected to local computers through the internet. These websites contain text pages, digital images, audios, videos, etc. Users can access the content of these sites from any part of the world over the internet using their devices such as computers, laptops, cell phones, etc. The WWW, along with internet, enables the retrieval and display of text and media to your device.

A web page is given an online address called a Uniform Resource Locator (URL). A particular collection of web pages that belong to a specific URL is called a website, e.g., *www.facebook.com*, *www.google.com*, etc. So, the World Wide Web is like a huge electronic book whose pages are stored on multiple servers across the world.

Small websites store all of their WebPages on a single server, but big websites or organizations place their WebPages on different servers in different countries so that when users of a country search their site they could get the information quickly from the nearest server.

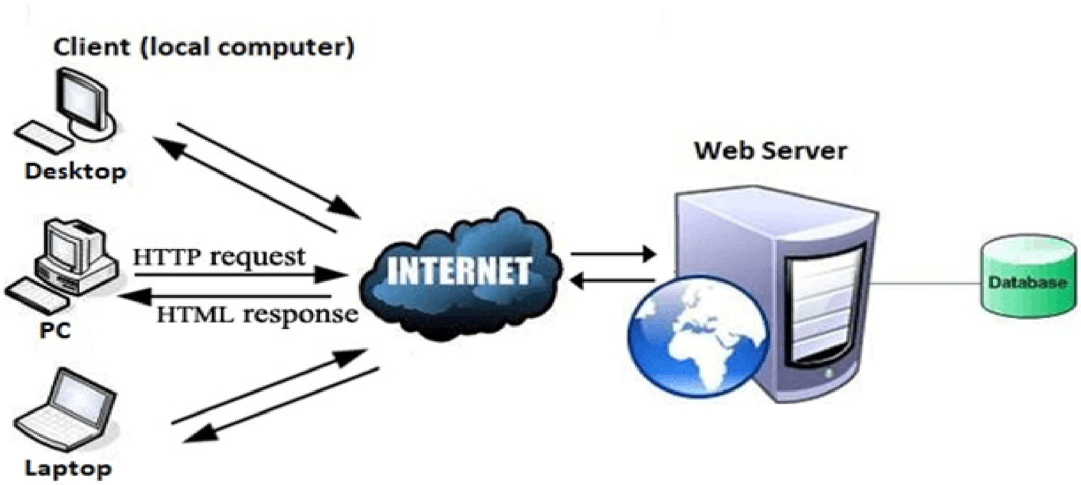
So, the web provides a communication platform for users to retrieve and exchange information over the internet. Unlike a book, where we move from one page to another in a sequence, on World Wide Web we follow a web of hypertext links to visit a web page and from that web page to move to other web pages. You need a browser, which is installed on your computer, to access the Web.


Web Server
Web browser Request the Web server
Web server Serves the Web page
Web Browser

The Web works as per the internet's basic client-server format as shown in the following image. The servers store and transfer web pages or information to user's computers on the network when requested by the users. A web server is a software program which serves the web pages requested by web users using a browser. The computer of a user who requests documents from a server is known as a client. Browser, which is installed on the user' computer, allows users to view the retrieved documents.

All the websites are stored in web servers. Just as someone lives on rent in a house, a website occupies a space in a server and remains stored in it. The server hosts the website whenever a user requests its WebPages, and the website owner has to pay the hosting price for the same.

The moment you open the browser and type a URL in the address bar or search something on Google, the WWW starts working. There are three main technologies involved in transferring information (web pages) from servers to clients (computers of users). These technologies include Hypertext Markup Language (HTML), Hypertext Transfer Protocol (HTTP) and Web browsers.



All the websites are stored in web servers. Just as someone lives on rent in a house, a website occupies a space in a server and remains stored in it. The server hosts the website whenever a user requests its WebPages, and the website owner has to pay the hosting price for the same.

The moment you open the browser and type a URL in the address bar or search something on Google, the WWW starts working. There are three main technologies involved in transferring information (web pages) from servers to clients (computers of users). These technologies include Hypertext Markup Language (HTML), Hypertext Transfer Protocol (HTTP) and Web browsers.

Internet

Internet is a global network that connects billions of computers across the world with each other and to the World Wide Web. It uses standard internet protocol suite (TCP/IP) to connect billions of computer users worldwide. It is set up by using cables such as optical fibers and other wireless and networking technologies. At present, internet is the fastest mean of sending or exchanging information and data between computers across the world.

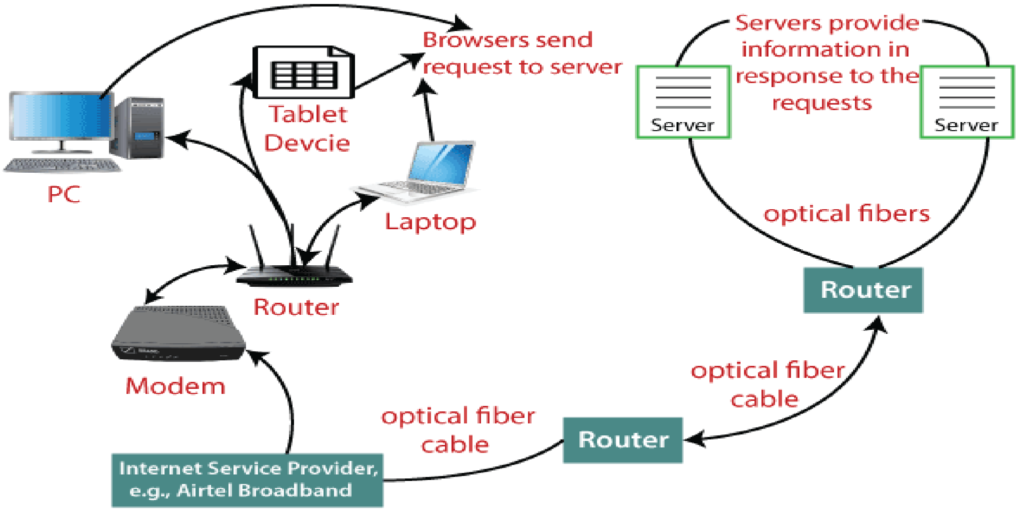
Internet is different from the World Wide Web as the World Wide Web is a network of computers and servers created by connecting them through the internet. So, the internet is the backbone of the web as it provides the technical infrastructure to establish the WWW and acts as a medium to transmit information from one computer to another computer.

The internet is not owned by a single person or organization entirely.

The internet works with the help of clients and servers. A device such as a laptop, which is connected to the internet is called a client, not a server as it is not directly connected to the internet. However, it is indirectly connected to the internet through an Internet Service Provider (ISP) and is identified by an IP address, which is a string of numbers. Just like you have an address for your home that uniquely identifies your home, an IP address acts as the shipping address of your device. The IP address is provided by your ISP, and you can see what IP address your ISP has given to your system.

A server is a large computer that stores websites. It also has an IP address. A place where a large number of servers are stored is called a data center. The server accepts requests send by the client through a browser over a network (internet) and responds accordingly.

To access the internet we need a domain name, which represents an IP address number, i.e., each IP address has been assigned a domain name. For example, youtube.com, facebook.com, paypal.com are used to represent the IP addresses. Domain names are created as it is difficult for a person to remember a long string of numbers. However, internet does not understand the domain name, it understands the IP address, so when you enter the domain name in the browser search bar, the internet has to get the IP addresses of this domain name from a huge phone book, which is known as DNS (Domain Name


Browsers send request to server
Servers provide information in response to the requests
Server
Server
Tablet Devcie
PC
Laptop
optical fibers
Router
Router
Modem
optical fiber cable
optical fiber cable
Router
Internet Service Provider, e.g., Airtel Broadband

Advantages of the Internet:

- **Instant Messaging:** You can send messages or communicate to anyone using internet, such as email, voice chat, video conferencing, etc.
- **Get directions:** Using GPS technology, you can get directions to almost every place in a city, country, etc. You can find restaurants, malls, or any other service near your location.
- **Online Shopping:** It allows you to shop online such as you can be clothes, shoes, book movie tickets, railway tickets, flight tickets, and more.
- **Pay Bills:** You can pay your bills online, such as electricity bills, gas bills, college fees, etc.

- **Online Banking:** It allows you to use internet banking in which you can check your balance, receive or transfer money, get a statement, request cheque-book, etc.
- **Online Selling:** You can sell your products or services online. It helps you reach more customers and thus increases your sales and profit.
- **Work from Home:** In case you need to work from home, you can do it using a system with internet access. Today, many companies allow their employees to work from home.
- **Entertainment:** You can listen to online music, watch videos or movies, play online games.
- **Cloud computing:** It enables you to connect your computers and internet-enabled devices to cloud services such as cloud storage, cloud computing, etc.
- **Career building:** You can search for jobs online on different job portals and send you CV through email if required.

*****