COMPUTER NETWORKS & INTERNET PROTOCOLS NOTES

Prepared By
P. Leelavathi
Assistant Professor
CSE-DS

UNIT-I
INTRODUCTION TO COMPUTER NETWORKS

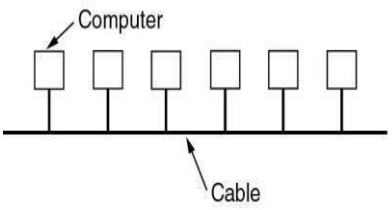
Computer Networks:

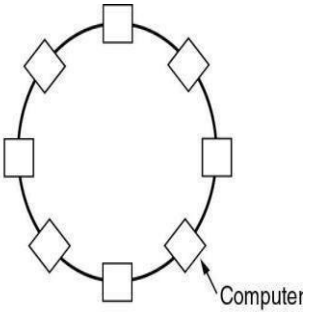
- ✓ A network consists of two or more computers that are linked in order to share resources exchange files, or allow electronic communications.
- ✓ The computers on a network may be linked through cables,telephone lines,radio waves, satellites, or infrared light beams.
- ✓ In network design two dimensions standout as important: **transmission technology and scale.**
- ✓ There are two types of transmission technology that are in widespread use: **broadcast links and point-to-point links.**
    - **Point-to-point links**:
        - It connects individual pairs of machines. To go from the source to the destination on a network made up of point-to-point links, short messages, called packets in certain contexts, may have to first visit one or more intermediate machines. Point-to-point transmission with exactly one sender and exactly one receiver is sometimes called **unicasting.**
    - **Broadcast network**:
        - The communication channel is shared by all the machines on the network; packets sent by any machine are received by all the others.An address field within each packet specifies the intended recipient. Upon receiving a packet, a machine checks the address field. If the packet is intended for the receiving machine, that machine processesthe packet; if the packet is intended for some other machine, it is just ignored.
        - Broadcast systems usually also allow the possibility of addressing a packet to all destinations by using a special code in the address field. When a packet with this code is transmitted, it is received and processed by every machine on the network. This mode of operation is called **broadcasting.** Some broadcast systems also supporttransmission to a subset of the machines, which known as**multicasting.**
- ✓ Analternativecriterionforclassifyingnetworksisby**scale.**

Interprocessordistance	Processorslocatedinsame	Example
1m	Squaremeter	Personalarea network
10m	Room	
100 m	Building	Localareanetwork
1 km	Campus	
10km	City	Metropolitanarea network
100 km	Country	
1000 km	Continent	Wideareanetwork
10,000 km	Planet	Theinternet

Network Hardware

- ✓ DifferentTypesofNetworks
  - Dependinguponthegeographicalareacoveredby anetwork,it isclassifiedas:
    - PersonalAreaNetwork(PAN)
    - LocalAreaNetwork(LAN)
    - MetropolitanArea Network(MAN)
    - WideAreaNetwork(WAN)
    - Internetworks
  - **PersonalAreaNetwork (PAN)**
    - A personal area network (PAN) is a computer network used for communication among computer devices, including telephones and personal digital assistants, in proximity to an individual's body.
    - The devices may or may not belong to the person in question. Thereach of a PAN is typically a few meters.
  - **LocalAreaNetwork (LAN)**
    - ALANisanetworkthatisusedforcommunicatingamongcomputer devices, usually within an office building or home.
    - LAN'senablethesharingofresourcessuchasfilesorhardware devices that may be needed by multiple users.
    - Itislimitedinsize,typicallyspanningafewhundredmeters,andno more than a mile.
    - Itisfast, withspeeds from10Mbps to 10 Gbps.
    - Requireslittlewiring,typicallyasinglecableconnectingtoeach device.
    - LAN'scanbeeitherwiredorwireless.Twistedpair,coaxorfiberoptic cable can be used in wired LAN's.
    - EveryLANusesaprotocol–asetofrulesthatgovernshowpackets are configured and transmitted.
    - IthaslowercostcomparedtoMAN'sorWAN's
    - NodesinaLANarelinkedtogetherwithacertaintopology.These topologies include: Bus, Ring, Star.
    - Requireslittlewiring,typicallyasinglecableconnectingtoeach device.
    - Typesof LANs:The threemost common typesofLANare:
      - CablebasedLAN
      - PrivateBranchExchange(PBX)
      - Hierarchicalnetworks



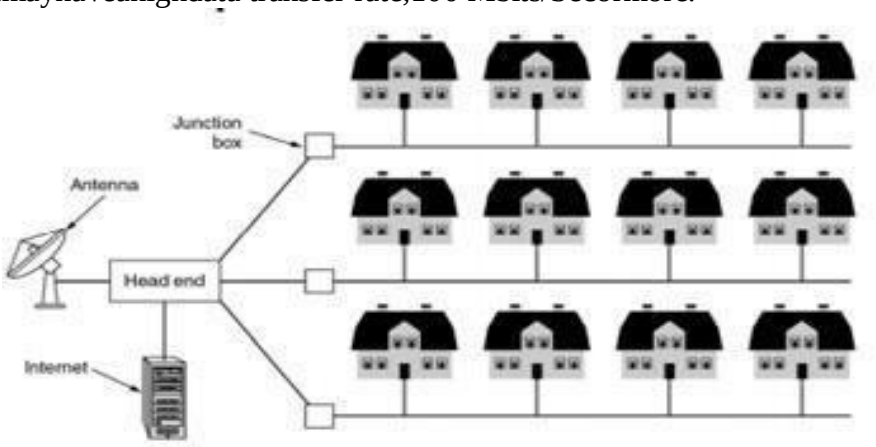


    - AdvantagesofLAN

- Speed
- Security
- ResourceSharing

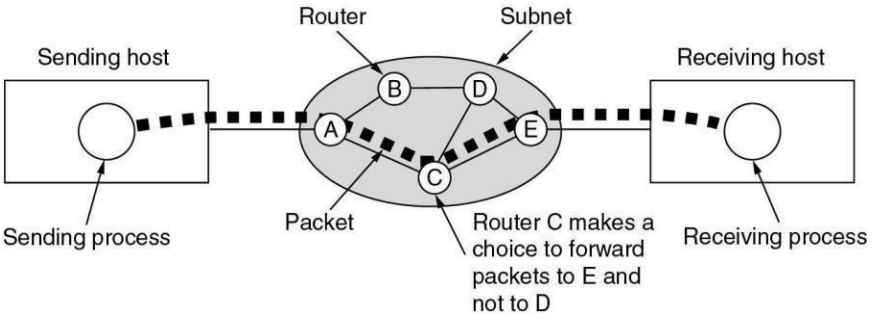
- DisadvantagesofLAN
  - ExpensiveTo Install
  - RequiresAdministrativeTime
  - FileServerMayFail
  - CablesMayBreak

- **MetropolitanAreaNetwork(MAN)**
  - The area that is covered by this network is larger than that in LAN but smaller than that in WAN, i.e it covers the entire city.
  - Itusessimilartechnologyas LAN.
  - It can be a single network such as cable TV network, or a measure of connecting a number of LAN's o a large network so that resources can be shared LAN to LAN as well as device to device.
  - Itmayhaveahighdata transfer rate,100 Mbits/Secormore.



  - Advantages:
    - Fast&efficientindatatransmission.
    - Possibilitytoconnectcomputersinonecity.
  - Disadvantages:
    - Rarelyused.
    - Difficultyin maintainingMANduetoits largesize.

- **WideAreaNetwork(WAN)**
  - When network spans over a large distance or when the computers to be connected to each other are at widely separated locations a local area network cannot be used.
  - The communication between different users of WAN is established using leased telephone lines, satellite links and similar channels.
  - Itis cheaperand moreefficient tousethephonenetworkforthe link.
  - Most WAN networks are used to transfer large blocks of data between its users.

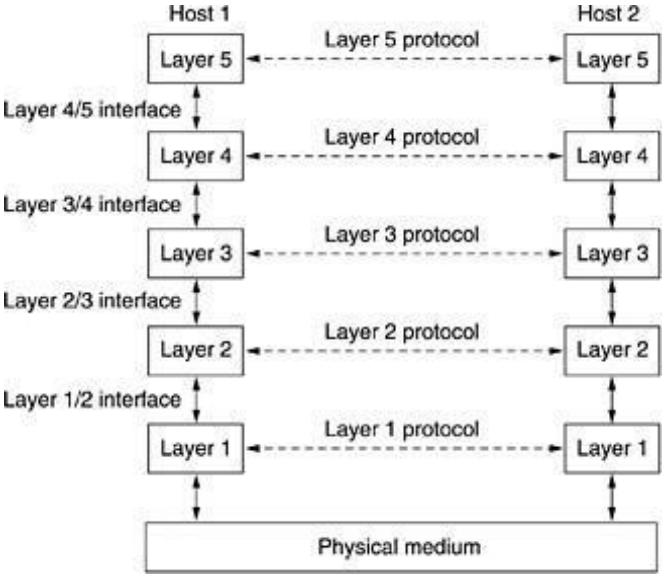


- Advantages:
  - ThespeedsofWANcanbeveryslowandthiscanbeamajor source of frustration.
  - ThecostofsettingupWANespeciallyinremoteareascan be extremely high.
  - Possibilitytoconnectthousandsofcomputers.
  - PossibilitytoconnectdifferentLANsownedbydifferent organizations.
- Disadvantages:
  - Requiresexpensivehardware& software.
  - Hardto operate
  - Requiresspecialkindof programs.

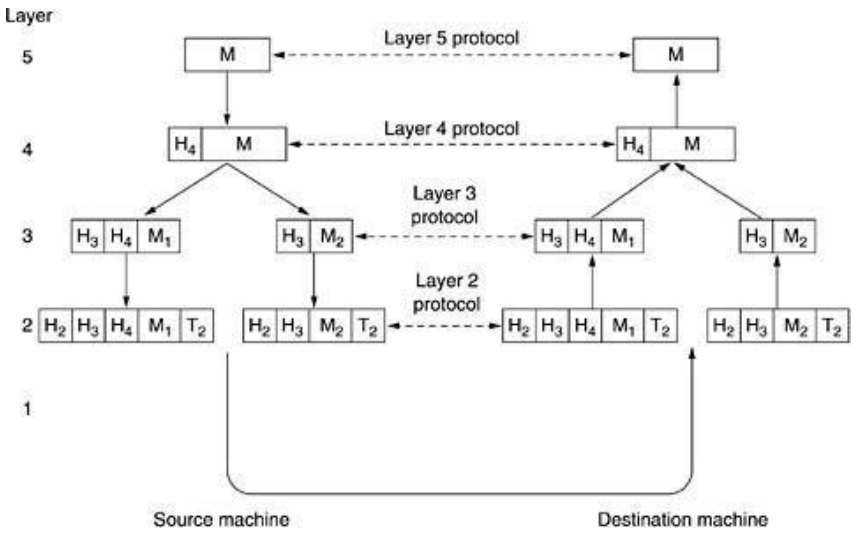
- **Internetworks**
  - Many networks exist in the world, often with different hardware and software. People connected to one network often want to communicate with people attached to a different one. The fulfillment of this desire requires that different, and frequently incompatible networks, be connected, sometimes by means of machines called gateways to make the connection and provide the necessary translation, both in terms of hardware and software.
  - A collection of interconnected networks is called an internetwork or internet. These terms will be used in a generic sense, in contrast to the worldwide Internet, which we will always capitalize.
  - An internetwork is formed when distinct networks are interconnected. In our view, connecting a LAN and a WAN or connecting two LAN s forms an internetwork, but there is little agreement in the industry over terminology in this area.
  - One rule of thumb is that if different organizations paid to construct different parts of the network and each maintains its part, we have an internetwork rather than a single network. Also, if the underlying technology is different in different parts (e.g., broadcast versus point-to-point), we probably have two networks.

Network Software

- ✓ Protocol Hierarchies
  - To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it.
  - The purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services are actually implemented.
  - A protocol is an agreement between the communicating parties on how communication is to proceed.



  - Interface:Betweeneachpairofadjacentlayersisaninterface.
  - Networkarchitecture:Asetoflayersandprotocolsiscalledanetwork architecture.
  - Protocolstack:Alistofprotocolsusedbyacertainsystem,oneprotocolper layer, is called a protocol stack.
  - Anexamplenetworkprotocolstack



- Messageisgeneratedby theapplicationofthesourcemachine.
- Messagewill besent fromthesourceto thedestination.
- Message "M" is transferred from layer 5 to layer 4, with a header containing control information, such as sequence numbers, which helps layer 4 maintain the message order.
- Layer 3 break the message from layer 4 into two pieces to fit the transmission restrictions, while adding another header to tell layer 2 where the dest. is.
- Layer 2 adds the messages from layer 3 with another header, telling the actual (physical) address of the dest, and a trailer, which is the checksum of the message for correction assertion.
- At thereceiving machine themessagemoves upward,fromlayerto layer, with headers being stripped off as it progresses. Message is sent to the dest. machine.
- Design IssuesfortheLayers
  - Everylayerneedsamechanismforidentifyingsendersandreceivers.
  - The protocol must also determine how many logical channels the connection corresponds to and what their priorities are. (simplex or duplex? single or multiple channel?)
  - Error control is an important issue because physical communication circuits are not perfect.
  - Message ordering is important 'cause Not all communication channels preserve the order of messages sent on them.
  - An issue that occurs at every level is how to keep a fast sender from swamping a slow receiver with data.
  - Inability of all processes to accept arbitrarily long messages. (fragmentation and reassembling the messages)
- Connection-OrientedandConnectionlessServices
  - Connection-Oriented Service: the service user first establishes a connection,usestheconnection,andthenreleasestheconnection.(e.g., the telephone, tube)
  - Connectionless Service: Each message carries the full destination address, and each one is routed through the system independent of all the others. (e.g., the postal system) Usually, connectionless service cannot guarantee the order of messages.
  - In order to enhance the reliability of transmission of connection-oriented service, acknowledge each received message is helpful. For example, the files transfer.
  - However, some applications prefer fast speed than the reliability. For example, the digitized voice traffic, video conference.
- ServicePrimitives

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

OSI Reference model

- ✓ This model is developed by the International Standards Organization (ISO) as the first step toward international standardization of the protocols used in the various layers. The model is called the ISO-OSI (Open System Interconnection) Reference Model because it deals with connecting open systems- that is, systems that are open for communication with other systems.
- ✓ TheOSImodelhas seven layers. In layerstheprincipal ideasareasfollows.
    1. Alayershouldbecreated whereadifferentlevelof abstractionisneeded.
    2. Eachlayershouldperformawelldefinedfunction.
    3. The function of each layer should be defined international standardized protocols.
    4. The layer boundaries should be chosen to minimize the information flowacross the interfaces.
    5. The number of layers should be large enough that distinct functions need notbe thrown together in the same layer out of necessity, and small enough thatthe architecture does not become unwieldy.

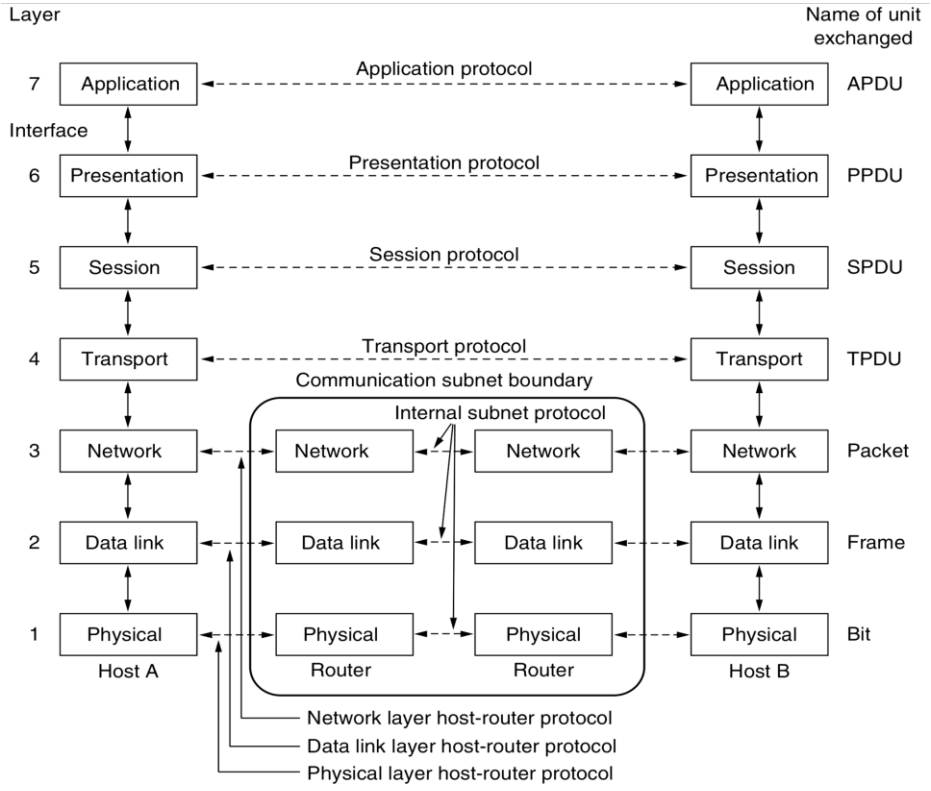
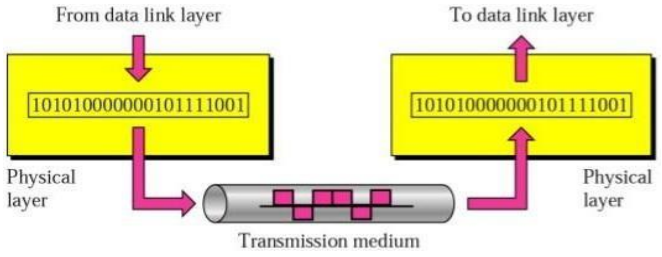


Figure:TheOSIreferencemodel

- ✓ **ThePhysicalLayer**
    - o ThePhysicallayerisconcernedwithtransmittingrawbitsovera communication channel.
    - o The design issues here largely deal with mechanical, electrical, and procedural interfaces, and the physical transmission medium, which lies below the physical layer.
    - o Physical Layer receives data from the upper layer called the data link layer. It convertsthereceiveddataintobitstream.Thedataisthentransmittedthrough

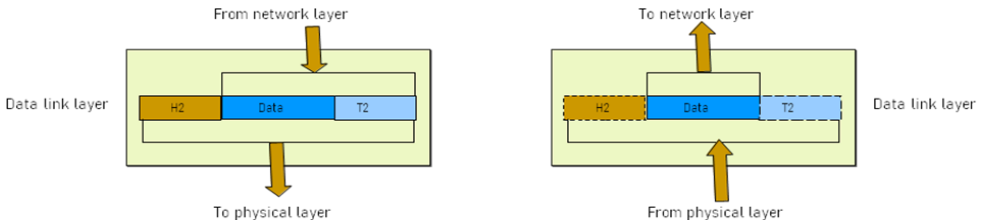
the medium to the receiver. At the receiving end, Physical Layer receives the data in bit format. It forwards the data to the Data Link Layer. Thisfunctioning of the physical layer is shown in Figure.



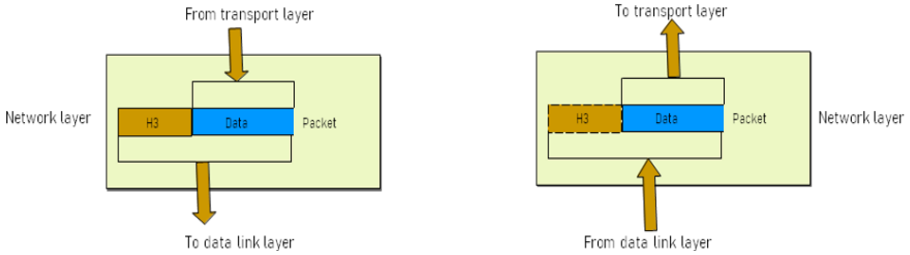
- ResponsibilitiesofthePhysicalLayerare:
  - Characteristics of media:- Defines the characteristics of the interface which is used for connecting the devices. It also defines the type of the transmission media such as copper wires or fiber optic cables.
  - Encoding:- Defines the encoding type. Encoding means changing bit stream (0s and 3s) into signal. Before transmission, Physical Layer encodes the signal into electrical or optical form depending upon the media.
  - Transmission Rate:- Defines the transmission rate of bits.Thisprovides number of bits transmitted per second. It defines how longwill the duration of a bit be.
  - Transmission mode:- Defines the transmission mode between two devices. Transmission mode specifies the direction of signal flow. The different types of transmission modes are:
    - Simplex
    - Half-Duplex
    - Full-Duplex

✓ **DataLink Layer**

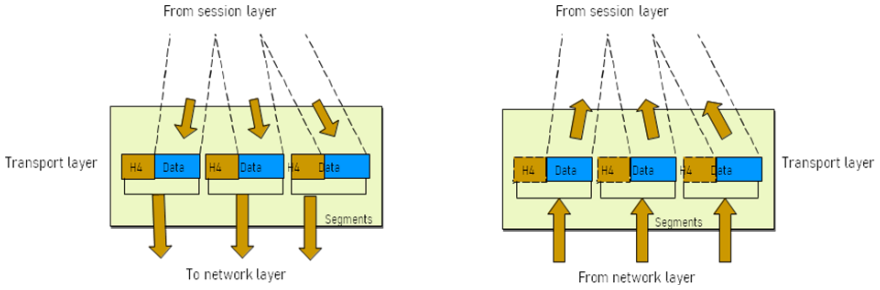
- Responsiblefordelivery ofdatabetweentwosystemsonthesamenetwork
- Mainfunctionsofthislayerare:
  - Framing–dividesthestreamofbitsreceivedfromnetworklayerinto manageable data units called frames.
  - PhysicalAddressing–Addaheadertotheframetodefinethephysical address of the source and the destination machines.
  - Flowcontrol–controlrateatwhichdataistransmittedsoasnotto flood the receiver
  - ErrorControl–Addsmechanismstodetectandretransmitdamagedor lost frames. This is achieved by adding a trailer to the end of a frame



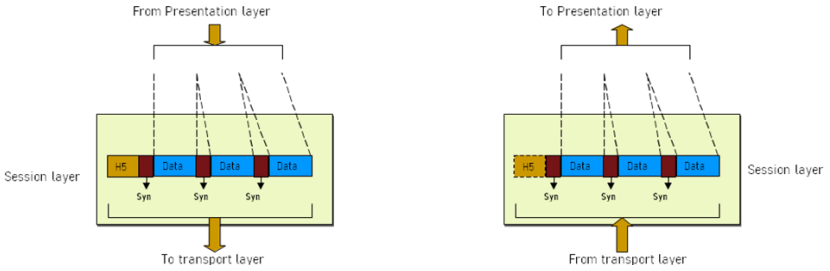
- ✓ **NetworkLayer**
  - The networklayerisresponsible forthedeliveryofindividualpackets from the source host to the destinationhost.
  - Mainfunctionsofthislayerare:
    - Responsiblefordeliveryofpackets acrossmultiplenetworks
    - Routing–Providemechanismstotransmitdataoverindependent networks that are linked together.
    - Networklayerisresponsibleonlyfordeliveryofindividualpackets and it does not recognize any relationship between those packets.



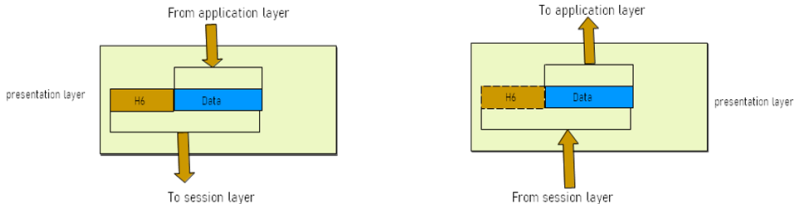
- ✓ **TransportLayer**
  - The transport layer is responsible for the delivery of a message from one process to another
  - Mainfunctionsofthislayerare:
    - Responsibleforsource-todestinationdeliveryoftheentiremessage
    - Segmentation and reassembly – divide message into smaller segments, number them and transmit. Reassemble these messages at the receiving end.
    - Error control – makes sure that the entire message arrives withouterrors – else retransmit.



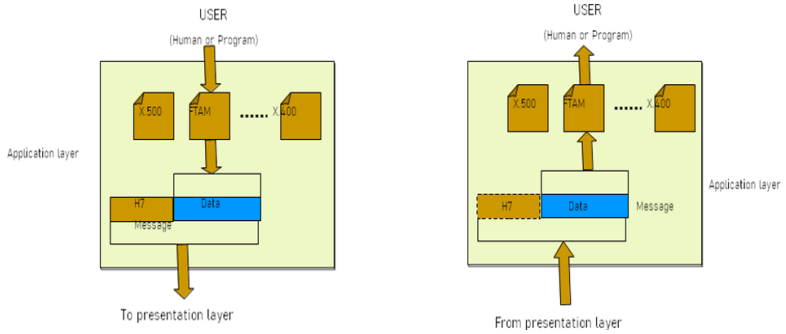
- ✓ **Session Layer**
  - Thesessionlayerisresponsible fordialogcontroland synchronization.
  - Session layer provides mechanism for controlling the dialogue between thetwo end systems. It defines how to start, control and end conversations (called sessions) between applications.
  - This layer requests for a logical connection to be established on an end- user's request.
  - Anynecessarylog-onorpasswordvalidationisalso handledbythislayer.
  - Sessionlayerisalsoresponsibleforterminatingthe connection.
  - Mainfunctionsofthislayerare:
    - Dialogcontrol–allowstwosystemstoenterintoadialog,keepatrack of whose turn it is to transmit.
    - Synchronization–addscheckpoints(synchronizationpoints).



- ✓ **PresentationLayer**
  - The presentation layer is responsible for translation, compression and encryption
  - Responsibilitiesofthislayer are:
    - Translation
      - Different computers use different encoding systems (bit order translation)
      - Convertdataintoa commonformatbefore transmitting.
      - Syntax represents info such as character codes - how many bits to represent data – 8 or 7 bits.
    - Compression – reduce number of bits to be transmitted into stream of data.
    - Encryption and Decryption – transform data into an unintelligible format at the sending end for data security and Decryption at the receiving end.

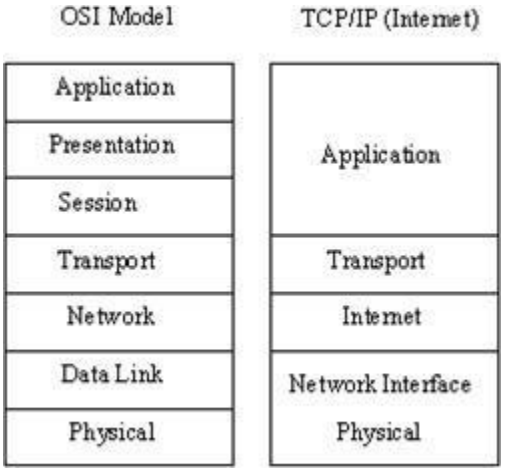


- ✓ **Application Layer**
  - Theapplicationlayerisresponsibleforprovidingservicestotheuser
  - Responsibilitiesofthislayer are:
    - Networkvirtualterminal(Software)
    - Filetransfer,accessandmanagement
    - Mailservices
    - Directoryservices (access to distributed databasesources for global information about various objects andservices).



TCP/IP Reference model

- ✓ It was first described by Cerf and Kahn (1974), and later refined and defined as a standard in the Internet community (Braden, 1989).
- ✓ A majority of the internet uses a protocol suite called the Internet Protocol Suite also known as the TCP/IP protocol suite.
- ✓ This suite is a combination of protocols which encompasses a number of different protocols for different purpose and need. Because the two major protocols in these suites are TCP (Transmission Control Protocol) and IP (Internet Protocol), this is commonly termed as TCP/IP Protocol suite.
- ✓ Thisprotocolsuite hasits ownreferencemodelwhich itfollows overthe internet.
- ✓ Incontrast withthe OSImodel, this modelof protocolscontains lesslayers.



- ✓ **Layer1:Host-to-networkLayer(Link Layer)**
  - Lowestlayeroftheall.
  - Protocolisused toconnect tothe host,sothat thepackets canbesentoverit.
  - Variesfromhost tohostand networkto network.
- ✓ **Layer2:Internet layer**
  - Selectionofapacketswitchingnetworkwhichisbasedonaconnectionless internetwork layer is called a internet layer.
  - Ithelpsthepacketto travelindependentlytothedestination.
  - Orderinwhich packetsarereceived isdifferent fromtheway theyaresent.
  - The internet layer defines an official packet format and protocol called IP (Internet Protocol), plus a companion protocol called ICMP (Internet Control Message Protocol) that helps it function.
  - IP(InternetProtocol)isusedinthislayer.
  - Thevariousfunctionsperformedbythe InternetLayerare:
    - DeliveringIPpackets
    - Performingrouting
    - Avoiding congestion
- ✓ **Layer3:Transport Layer**
  - Itdecidesif datatransmission shouldbeon parallelpath orsinglepath.
  - Functionssuchasmultiplexing,segmentingorsplittingonthedataisdoneby transport layer.
  - Theapplicationscan readand writeto thetransportlayer.
  - Transportlayeraddsheaderinformationtothedata.

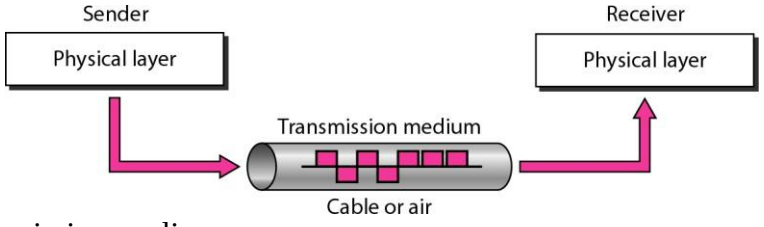
- Transportlayerbreaksthemessage(data)intosmallunitssothattheyare handled more efficiently by the network layer.
- Transportlayer alsoarrangethe packetsto besent, insequence.
- Itdefinestwoend-to-end protocols:TCP and UDP
  - TCP(Transmission Control Protocol): It is a reliable connection-oriented protocol which handles byte-stream from sourceto destination without error and flow control.
  - UDP(User-Datagram Protocol): It is an unreliable connection-less protocol that do not want TCPs, sequencing and flow control. Eg: One-shot request-reply kind of service.

✓ **Layer4:ApplicationLayer**

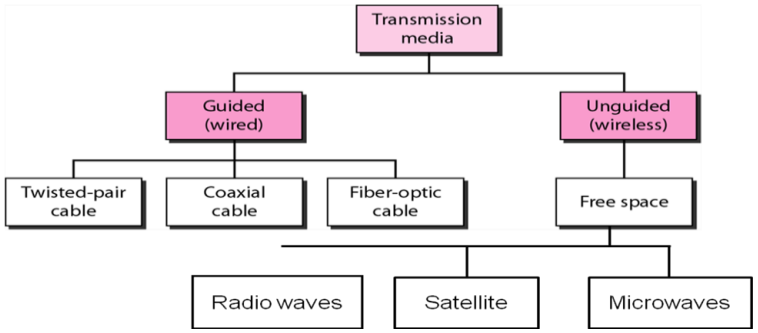
- TheTCP/IPspecificationsdescribedalotofapplicationsthatwereat the top of the protocol stack.
- TELNETisatwo-waycommunicationprotocolwhichallowsconnectingtoa remote machine and run applications on it.
- FTP(File Transfer Protocol) is a protocol, that allows File transfer amongst computerusersconnectedoveranetwork.Itisreliable,simpleandefficient.
- SMTP(Simple Mail Transport Protocol) is a protocol, which is used to transportelectronicmailbetween asourceanddestination,directedviaaroute.
- DNS(DomainNameServer)resolvesan IPaddressintoatextualaddressfor Hosts connected over a network.
- Itallowspeer entitiestocarryconversation.

Transmission Media

✓ The purposeofthephysicallayeristotransportbitsfromonemachinetoanother through transmission medium.
✓ Transmissionmediaarelocated belowthephysical layer.
✓ Computersusesignalstorepresentdata.
✓ Signalsaretransmittedintheformofelectromagneticenergy.
✓ Variousphysicalmediacanbeusedfor theactual transmission.



✓ Classesoftransmission media



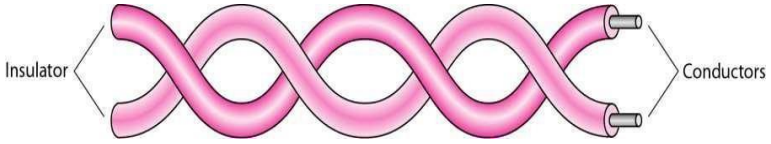
✓ Design Factors

- Bandwidth
  - Higherbandwidthgiveshigherdatarate
- Transmissionimpairments
  - Attenuation
- Interference
- Numberofreceivers
  - Inguided media
  - Morereceivers(multi-point)introducemoreattenuation(needmore amplifies or repeaters)

GuidedTransmissionmedia

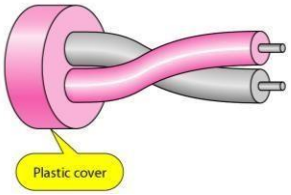
- ✓ Guidedmedia,whicharethosethatprovideachennelfromonedevicetoanother, include twisted-pair cable, coaxial cable, and fiber-optic cable.

- ✓ **Twisted-Pair Cable**



- Atransmissionmediumconsistingofpairsoftwistedcopperwiresarrangedin a regular spiral pattern.
- Tominimizetheelectromagneticinterferencebetweenadjacentpairs.
- Onewireusetocarry signals to thereceiver
- Secondwireusedas aground reference
- Fortwisting,afterreceivingthesignalremainssame.
- Thereforenumber oftwists perunit length,determines thequality ofcable.
- Lowfrequencytransmissionmedium
- Wecantransmit1Mbpsovershortdistances(lessthan 100m).
- Theyaremainlyusedtotransmitanalogsignals,buttheycanbeusedfor digital signals.
- <u>Applications</u>
  - Mostcommon medium
  - Telephonenetwork
  - Betweenhouse andlocal exchange(subscriber loop)
  - Withinbuildings
  - Toprivatebranch exchange (PBX)
  - Forlocal areanetworks(LAN)
  - 10Mbps or 100Mbps
- <u>Advantages</u>
  - Inexpensiveandreadilyavailable
  - Flexibleandlightweight
  - Easytoworkwithandinstall
- <u>Disadvantages:</u>
  - Lowdatarate(Relatively lowbandwidth(3000Hz))
  - Shortrange(lessthan100m).
  - Attenuation problem
  - Foranalog,repeatersneededevery5-6km
  - Fordigital,repeatersneededevery2-3km

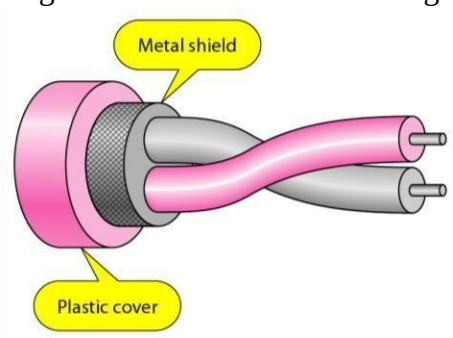
- Therearetwotypeof Twistedcable
  - UnshieldedTwistedPair(UTP)
    - Ordinarytelephonewire
    - Cheapest
    - Easiesttoinstall
    - SuffersfromexternalEMinterference



    - Categoriesofunshieldedtwisted-paircables

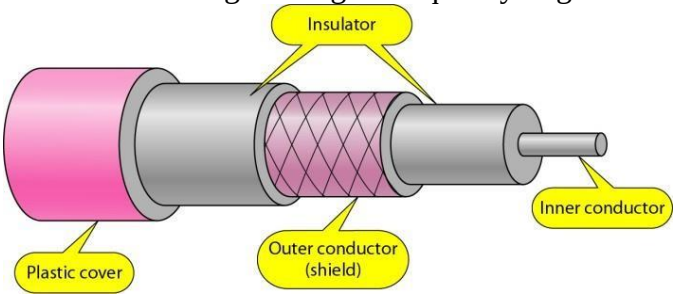
Category	*Specification*	*Data Rate (Mbps)*	*Use*
1	Unshielded twisted-pair used in telephone	< 0.1	Telephone
2	Unshielded twisted-pair originally used in T-lines	2	T-1 lines
3	Improved CAT 2 used in LANs	10	LANs
4	Improved CAT 3 used in Token Ring networks	20	LANs
5	Cable wire is normally 24 AWG with a jacket and outside sheath	100	LANs
5E	An extension to category 5 that includes extra features to minimize the crosstalk and electromagnetic interference	125	LANs
6	A new category with matched components coming from the same manufacturer. The cable must be tested at a 200-Mbps data rate.	200	LANs
7	Sometimes called SSTP (shielded screen twisted-pair). Each pair is individually wrapped in a helical metallic foil followed by a metallic foil shield in addition to the outside sheath. The shield decreases the effect of crosstalk and increases the data rate.	600	LANs

  - ShieldedTwistedPair (STP)
    - Metalbraidorsheathingthatreduces interference
    - Moreexpensive
    - Hardertohandle(thick,heavy)
    - Highertransmissionrates overlonger distances.



✓ **Coaxial cable**

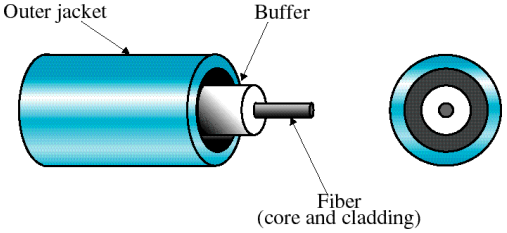
- Co-axialcable carriessignalofhigherfrequencyrangesthantwistedpaircable



- Innerconductorisasolidwire
- Outerconductorservesas ashieldagainstnoise andasecondconductor.
- Twokinds ofcoaxial cablearewidelyused.
  - Onekind,50-ohmcable,iscommonlyusedwhenitisintendedfor digital transmission from the start.
  - Theotherkind,75-ohmcable,iscommonlyusedforanalog transmission and cable television.
- TransmissionCharacteristics
  - Analog
    - Amplifierseveryfewkm
    - Closerif higherfrequency
    - Up to 500MHz
  - Digital
    - Repeaterevery1km
    - Closerforhigherdatarates
- Applications
  - Mostversatilemedium
  - Televisiondistribution
    - ArieltoTV
    - CableTV
  - Longdistancetelephonetransmission
    - Cancarry10,000 voicecallssimultaneously
    - Beingreplacedbyfiberoptic
  - Shortdistancecomputer systemslinks
  - Localareanetworks
- Advantages
  - Easytowire
  - Easytoexpand
  - ModeratelevelofElectroMagneticInterference
- Disadvantages
  - Singlecablefailurecantakedownanentirenetwork
  - Costofinstallationofacoaxialcableishighduetoitsthicknessand stiffness
  - Costof maintenanceis alsohigh

✓ **Fiber-OpticCable**

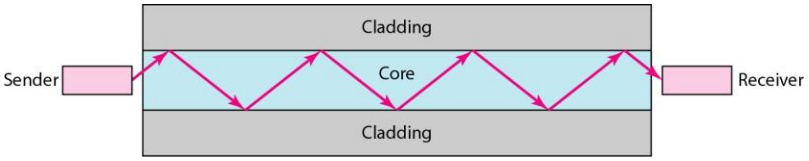
- Afiberopticcableismadeofglassorplasticand transmitssignalsintheform of light.



- **Natureoflight:**
  - Lighttravelsinastraightline

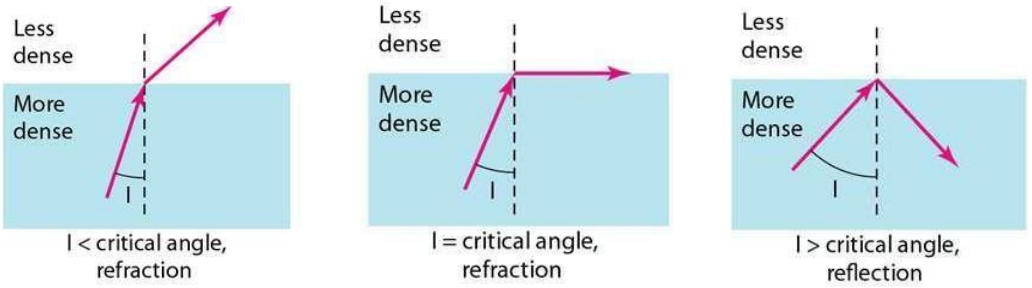
- Iflightgoesfromonesubstancetoanotherthentherayoflight changes Direction
- Rayoflightchangesdirectionwhengoesfrommoredensetoaless dence substance

- StructureofFiberopticcable:



- Requirealightsourcewithinjectionlaserdiode(ILD)or light emitting diodes (LED)
- Opticalfiberconsistsofaglasscore,surroundedbyaglasscladding with slightly lower refractive index.

- TransmissionCharacteristics
  - Actas waveguide for 1014 to 1015 Hz
    - Portionsofinfraredandvisiblespectrum
  - Light Emitting Diode(LED)
    - Cheaper
    - Wideroperatingtemprange
    - Last longer
  - InjectionLaserDiode(ILD)
    - Moreefficient
    - Greaterdatarate
- Bendingof lightray



- Theabovefigureshowshowarayoflightchangesdirectionwhen going from a more dense to a less dense substance.
- AngleofIncidence(I):theangletheraymakeswiththeline perpendicular to the interface between the two substances
- CriticalAngle:theangleofincidencewhichprovidesanangleof refraction of 90-degrees.

- Advantages
  - Greatercapacity
    - Example:Dataratesat100 Gbps
  - Smallersize& lightweight
  - Lowerattenuation
  - Electromagneticisolation

        - Moreresistanceto corrosivematerials
        - Greaterrepeaterspacingfacility
            - Example:After every10sofkmatleast
    - Disadvantages
        - Installationandmaintenanceneed expertise
        - OnlyUnidirectionallightpropagation
        - Muchmoreexpensive
        - Application
    - AreasofApplication
        - Telecommunications
        - LocalAreaNetworks
        - CableTV
        - CCTV
        - MedicalEducation

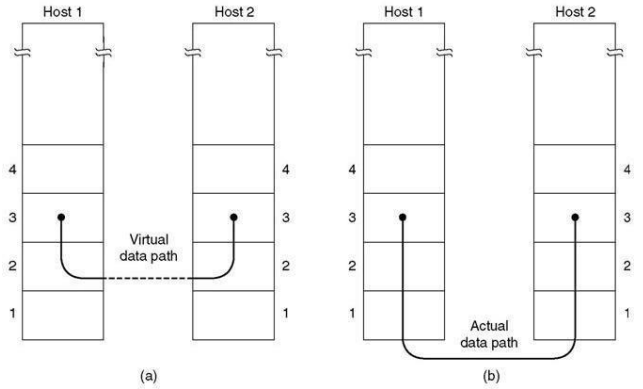
Reference Book: Computer Networks, Andrew Tanenbaum, 6th Edition.

UNIT-II
THE DATA LINK LAYER

Design Issues in Data Link Layer

- ✓ Thedatalinklayerusestheservicesofthephysicallayertosend andreceivebitsover communication channels. It has a number of functions, including:
  - Providingawell-definedserviceinterfacetothe networklayer.
  - Dealingwithtransmissionerrors.
  - Regulatingtheflowofdatasothatslowreceiversarenotswampedbyfast senders.
- ✓ Themainjobofthedatalinklayeristomakethecommunicationonthephysicallink reliable & efficient.
- ✓ Issues,
  - ServicesProvidedtotheNetworkLayer
  - Framing
  - FlowControl
  - ErrorControl
  - Synchronization

- ✓ **Services Provided to the Network Layer**
  - Thefunction ofthe data linklayer is toprovideservices tothenetworklayer.
  - The principal service is transferring data from the network layer on the source machine to the network layer on the destination machine. On the source machineis an entity, callit aprocess, inthenetworklayerthat hands somebits to the data link layer for transmission to the destination.
  - The job of the data link layer is to transmit the bits to the destination machine so theycan behanded overto thenetworklayerthere, as shownin Fig.(a). The actual transmission follows the path of Fig. (b).



- The data link layer can be designed to offer various services. The actual services that are offered vary from protocol to protocol. Three reasonable possibilities that we will consider in turn are:
    1. Unacknowledged connectionless service:
        - Unacknowledged connectionless service consists of having the source machine send independent frames to the destination machine without having the destination machine acknowledge them.
        - Ethernet is a good example of a data link layer that providesthis class of service.
    2. Acknowledged connection less service:
        - The next step up in terms of reliability is acknowledged connectionless service. When this service is offered, there are still no logical connections used, but each frame sent is individually acknowledged. In this way, the sender knows whether a frame has arrived correctly or been lost. If it has not arrived within a specified time interval, it can be sent again. This service is useful over unreliable channels, such as wireless systems.
        - 802.11(WiFi) isa good exampleof thisclass ofservice.
    3. Acknowledged connection-oriented service:
        - The most sophisticated service the data link layer canprovideto the network layer is connection-oriented service. With this service, the source and destination machines establish a connection before any data are transferred. Each frame sentover the connection is numbered, and the data link layer guarantees that each frame sent is indeed received.

✓ **Framing**

- Data-link layer takes packets from Network Layer and encapsulates them into Frames.Then,itsendseachframebit-by-bitonthehardware.Atreceiver'end, data link layer picks up signals from hardware and assembles them intoframes.
- The usual approach is for the data link layer to break up the bit stream into discrete frames, compute a short token called a checksum for each frame, and include the checksum in the frame when it is transmitted. When a framearrives at the destination, the checksum is recomputed. If the newly computed

checksum is different from the one contained in the frame, the data link layer knows that an error has occurred and takes steps to deal with it.

- Breaking up the bit stream into frames is more difficult than it at first appears. A good design must make it easy for a receiver to find the start of new frames while using little of the channel bandwidth. We will look at four methods:
    1. Bytecount:
        - This method uses a field in the header to specify the number of bytes in the frame.
    2. Flagbyteswithbytestuffing:
        - This method gets around the problem of resynchronization after an error by having each frame start and end with special bytes. Often the **same** byte, called a flag byte, is used as both the starting and ending delimiter. Two consecutive flag bytes indicate the end of one frame and the start of the next.
        - This method insert a special escape byte (ESC) just before each ‘‘accidental’’ flag byte in the data. Thus, a framing flag bytecan be distinguished from one in the data by the absence or presence of an escape byte before it. The data link layer on the receiving end removes the escape bytes before giving the datato the network layer. This technique is called byte stuffing.
    3. Flagbitswith bitstuffing:
        - In this method each frame begins and ends with a special bit pattern, 01111110 or 0x7E in hexadecimal. This pattern is aflag byte. Whenever the sender’s data link layer encounters five consecutive 1s in the data, it automatically stuffsa 0 bit into the outgoing bit stream.
    4. Physicallayercodingviolations:
        - The final framing method is physical layer coding violationsand is applicable to networks in which the encoding on the physical medium contains some redundancy. In such cases normally, a 1 bit is a high-low pair and a 0 bit is a low-highpair. The combinations of low-low and high-high which are not used for data may be used for marking frame boundaries.

✓ **FlowControl**

- Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machines to exchange data on same speed.

✓ **ErrorControl**

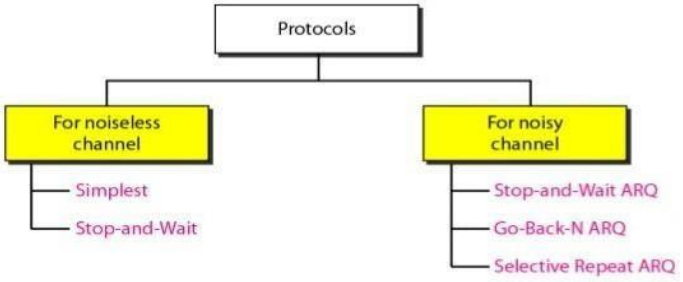
- Sometimessignalsmayhaveencounteredproblem intransitionandthebitsare flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.

✓ **Synchronization**

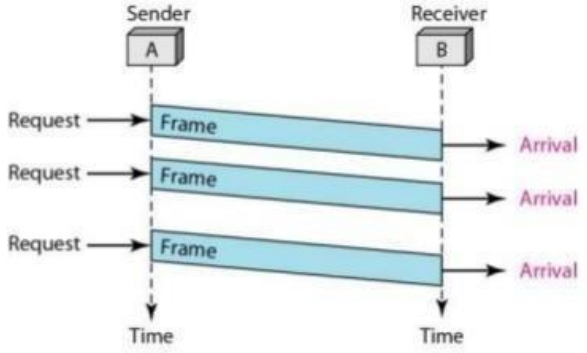
- When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.

Elementary Data Link Protocols

- ✓ Theprotocolsarenormallyimplementedinsoftwarebyusingoneofthecommon programming languages.
  - AnUnrestrictedSimplexProtocol
  - ASimplexStop-and-Wait Protocol
  - ASimplexProtocol foraNoisyChannel



- ✓ **AnUnrestrictedSimplex Protocol**
  - In order to appreciate the step by step development of efficient and complex protocols we will begin with a simple but unrealistic protocol. Inthisprotocol: Data are transmitted in one direction only
  - Thetransmitting (Tx)andreceiving (Rx)hosts arealwaysready
  - Processingtimecanbeignored
  - Infinitebufferspaceis available
  - Noerrorsoccur;i.e.nodamaged framesandnolostframes(perfectchannel)



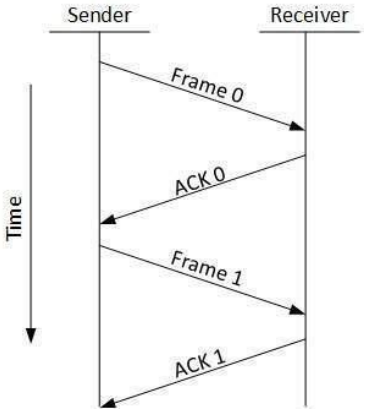
  - The protocol consists of two procedures, a sender and receiver as depicted below:

```
/*protocol 1 */

Sender()
{
    forever
    {
        from_host(buffer);
        S.info = buffer;
        sendf(S);
    }
}
```

```
Receiver()
{
        forever
        {
                wait(event);
                getf(R);
                to_host(R.info);
        }
}
```

Simple Stop&Wait Protocol

- ✓ Thisflowcontrolmechanismforcesthesenderaftertransmittingadataframetostop and wait until the acknowledgement of the data-frame sent is received.



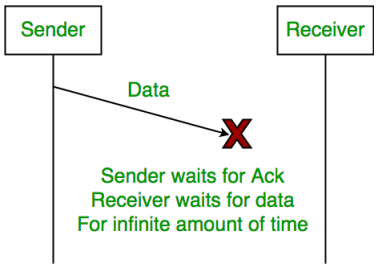
- ✓ Inthismethodofflowcontrol,thesendersendsasingleframetoreceiver&waitsfor an acknowledgment.
- ✓ Thenextframeissentbysenderonlywhen acknowledgmentofpreviousframeis received.
- ✓ Thisprocessofsendingaframe&waitingforanacknowledgmentcontinuesaslong as the sender has data to send.
- ✓ Toendupthetransmissionsendertransmitsendoftransmission(EOT) frame.
- ✓ Advantage:
  - Itis accuracy.
  - Thereis nochanceofframe beinglost.
- ✓ Disadvantage:
  - Itis inefficient.
  - Itmakesthetransmissionprocessslow
  - lotoftimeiswastedwaitingforACKsthatleadstoincreaseintotal transmission

- ✓ AlgorithmforStop-and- Wait Protocol

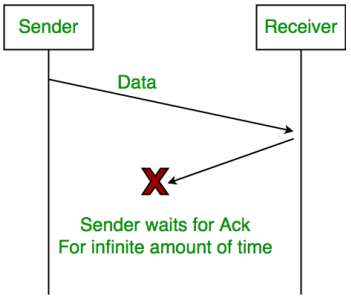
```
typedefenum{framearrival}eventtype; #include
"protocol.h"
void sender(void)
{
frame s;              /* buffer for an outbound frame */
packet buffer;        /* buffer for an outbound packet */
event type event;     /*framearrivalistheonlypossibility*/
```

```
while(true){
from network layer(&buffer);        /* go get something to send */
s.info = buffer;                    /*copyitintosfortransmission*/
tophysical layer(&s);               /*bye-byelittleframe*/
waitforevent(&event);               /*donotproceed untilgiventhego
                                    ahead*/

}
}

void receiver(void)
{
framer,s;                           /*buffersforframes*/
event type event;                   /*framearrivalistheonlypossibility*/
while (true) {
wait for event(&event);             /*onlypossibilityisframearrival*/
from physical layer(&r);            /* go get the inbound frame */
to network layer(&r.info);          /*passthedatatothenetworklayer*/ to
physical layer(&s);                 /* send a dummy frame to awaken
                                    sender*/

}
}
```

- ✓ ProblemsinSimpleStopandWaitProtocol
  1. LostData:



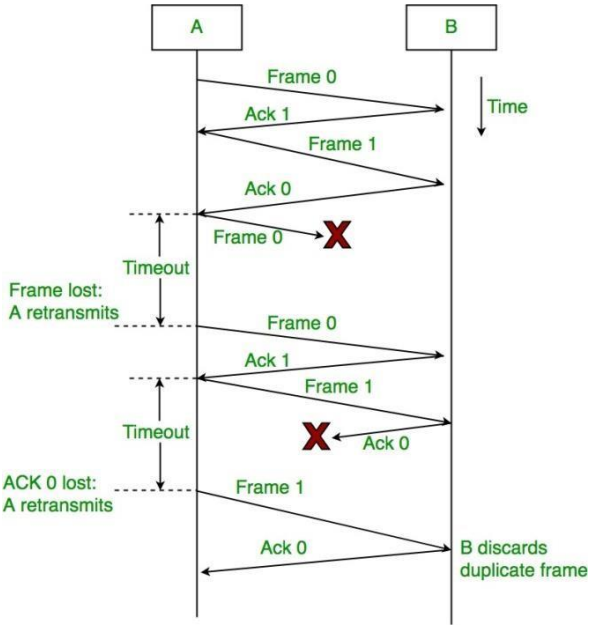
  2. LostAcknowledgement:



  3. DelayedAcknowledgement/Data:
     - Aftertimeout on sender side, a long delayed acknowledgement might be wrongly considered as acknowledgement of some other recent packet.

Stop&WaitProtocolwithARQ

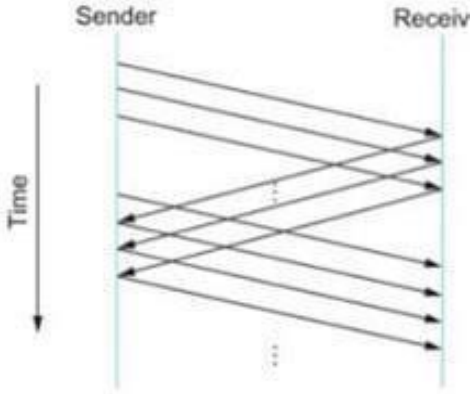
- ✓ Automatic Repeat reQuest (ARQ), an error control method, is incorporated with stop and wait flow control protocol
  - If error is detected by receiver, it discards the frame and send a negative ACK (NAK), causing sender to re-send the frame
  - In case a frame never got to receiver, sender has a timer: each time a frame is sent, timer is set
    - If no ACK or NAK is received during timeout period, it re-sends the frame
  - Timer introduces a problem: Suppose timeout and sender retransmits a frame but receiver actually received the previous transmission → receiver has duplicated copies
  - To avoid receiving and accepting two copies of same frame, frames and ACKs are alternatively labeled 0 or 1
    - ACK0:frame1isreceived, waitingfornext(frame0)
    - ACK1:frame0isreceived, waitingfornext(frame1)



  - SenderAsendsadata frameorpacketwith sequencenumber0.
  - Receiver B, after receiving data frame, sends and acknowledgement with sequence number 1 (sequence number of next expected data frame or packet)
  - There is only one bit sequence number that implies that both sender and receiver have buffer for one frame or packet only.
  - **CharacteristicsofStopandWait ARQ:**
    - Ituseslink betweensenderand receiveras halfduplex link
    - Throughput=1Datapacket/frameperRTT
    - If Bandwidth*Delay product is very high, then stop and wait protocolis not so useful. The sender has to keep waiting for acknowledgements before sending the processed next packet.
    - Itisan specialcategory ofSWPwhereitswindowsizeis1
    - Irrespective of number of packets sender is having stop and wait protocol requires only 2 sequence numbers 0 and 1.

Sliding Window Protocol

- ✓ In Stop and Wait protocol, only 1 packet is transmitted onto the link and then sender waits for acknowledgement from the receiver. The problem in this setup is that efficiency is very less
- ✓ Slidingwindowalgorithms areamethodof flowcontrolfornetworkdatatransfers.
- ✓ DataLinkLayeruses aslidingwindowalgorithm, whichallowsasendertohavemore than one unacknowledged packet "in flight" at a time, which improves network throughput.
- ✓ Itisbasedonconceptofpipelining.
- ✓ **Concepts ofthe SlidingWindow**
  - Both the sender and receiver maintain a finite size buffer to hold outgoing and incoming packets from the other side.
  - Every packet sent by the sender, must be acknowledged by the receiver. The sender maintains a timer for every packet sent, and any packetunacknowledged in a certain time, is resent.
  - The sender may send a whole window of packets before receiving an acknowledgement for the first packet in the window. This results in higher transfer rates, as the sender may send multiple packets without waiting foreach packet's acknowledgement.
  - The Receiver advertises a window size that tells the sender how much data it can receive, in order for the sender not to fill up the receiver's buffers.
  - Efficiencycanalsobeimprovedby makinguseof thefull-duplexline.

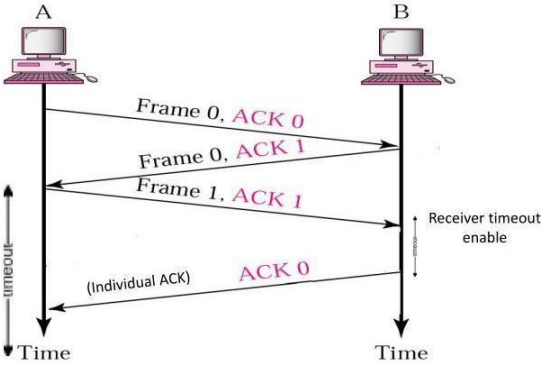


- ✓ **SenderSide**
  - Tokeeptrackoftheframes,senderstationsendssequentiallynumbered frames.
  - Sincethesequencenumbertobeusedoccupiesafieldin theframe,itshould be limited size.
  - Iftheheaderoftheframeallowsnbits,thesequencenumbersrangefrom0to $2^n - 1$.
  - Sendermaintainsalistofsequencenumbersthatitisallowedtosend(sender window).
  - Thesizeof thesenderswindow is atmost $2^n - 1$.
    - Eg:-if frameallows 3 bits, then thesizeof thewindow is 2^3-1=7
  - Thesenderis providedwith abufferequalto the window size.
- ✓ **ReceiverSide**
  - Receiveralwaysmaintainswindowsizeas1.
  - ThereceiveracknowledgesaframebysendinganACKframethatincludes the sequence number of the next frame expected.

- This also explicitly announces that it is prepared to receive the next N frames, beginning with the number specified.
- Thisschemecanbeusedtoacknowledge multiple frames.
- It could receive frames 2,3,4 but withhold ACK until frame 4 has arrived. By returning an ACK with sequence number 5, it acknowledges frames 2, 3, 4 at one time.

✓ **Piggybacking**

- When a data frame arrives, instead of immediately sending a separate control frame, the receiver restrains itself and waits until the network layer passes it to the next packet.
- The acknowledgement is attached to the outgoing data frame (using the ack field in the frame header).
- Theacknowledgement gets a freeride on thenextoutgoing dataframe.
- Thetechniqueoftemporarilydelayingoutgoingacknowledgementssothey can be hooked onto the next out going data frame is piggybacking.
- Betteruseof bandwidth.Ackisonly afewbits.
- Ifno dataframe goingout aftertimeout,just sendack frameon itsown.



✓ **Merits**

- Multiplepacketscanbetransmitwithoutwaitingforacknowledgements.(not like stop & wait)
- Piggibacking(using full-duplexlines)

✓ **Demerits**

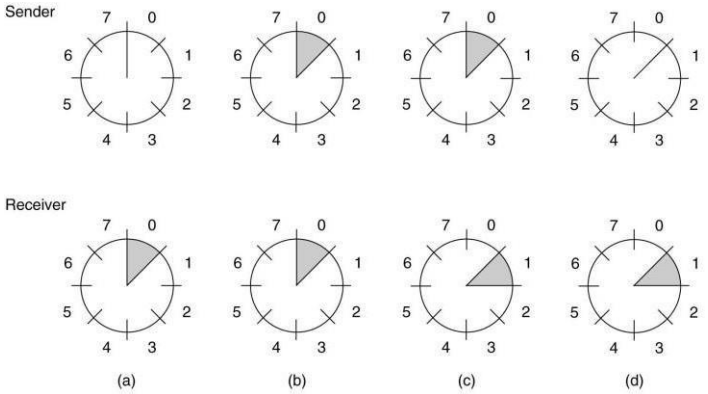
- Nolimit ofthesizeor sequencenumbersthat canberequiredin thisprotocol.
- Thebandwidth maybewasted insomespecialsituations.

✓ **TheslidingwindowARQtechniquehastwocategories,namely,**

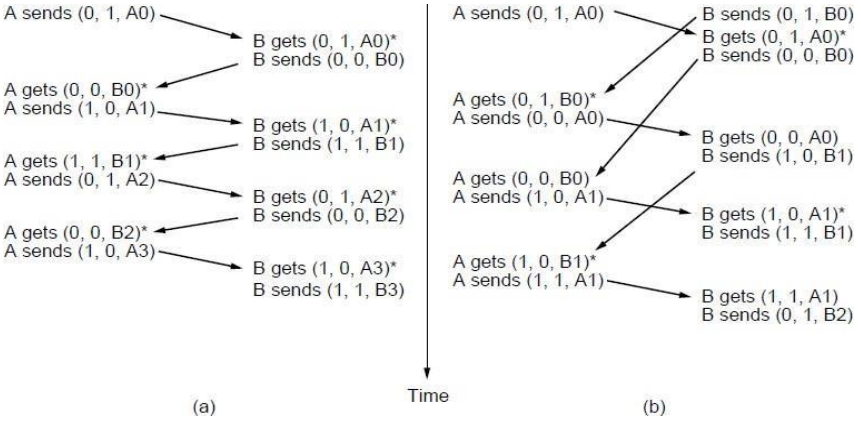
1. **Onebit SlidingWindow**
2. **Go-Back–N**
3. **SelectiveRepeat**

✓ **<u>Onebit SlidingWindow</u>**

- HerewindowsizeK=1 atthe sendersside.
- Thenthesizeofthesenderswindowis, 2^k – 1
  K=1
  2^1-1=2-1=1
- Thisis sameas thestop and waits protocol.



- In abovefigureshowsaslidingwindowofsize1,witha3-bitsequence number-
  - (a)Initially.
  - (b)Afterthefirstframe hasbeensent.
  - (c)Afterthefirstframehasbeen received.
  - (d)Afterthefirstacknowledgement hasbeenreceived.

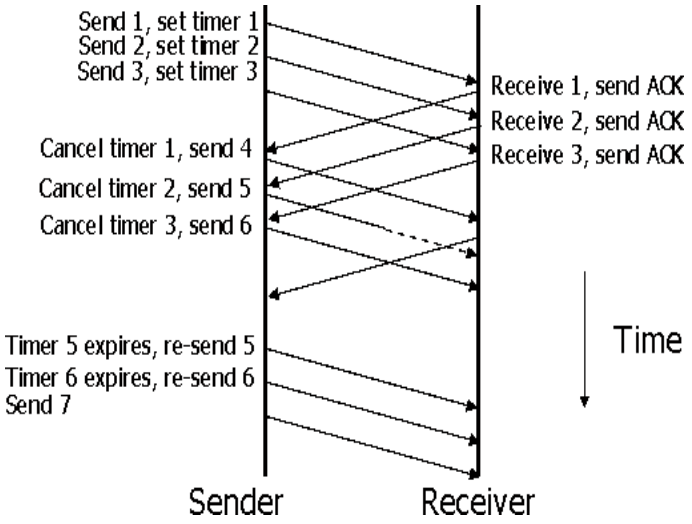


*Thenotationis (seq,ack,packet number).

- In above figurePart (a): IfB waits for A's first framebefore sending one ofits own. Each frame arrival brings a new packet for the network layer; there areno duplicates.
- In above figure Part (b): If A and B simultaneously initiate communication, theirfirst framescross,and thedatalink layersgets into asituation. Halfofthe frames contain duplicates, even though there are no transmission errors.

✓ Go-Back–N

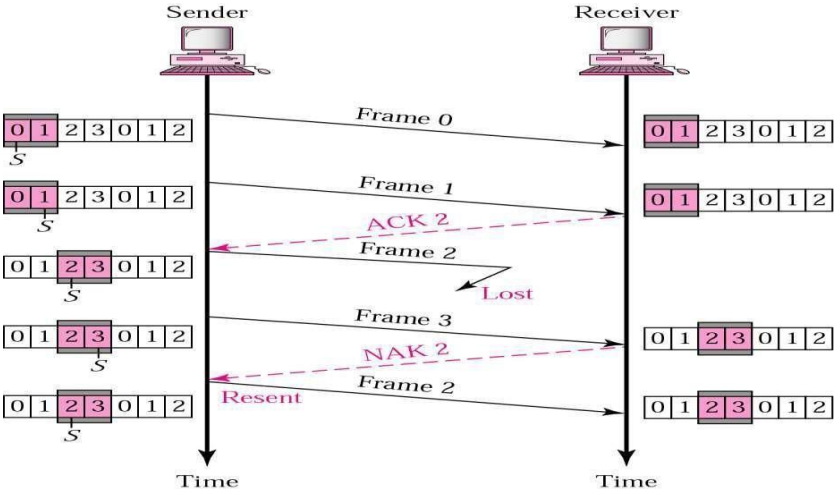
- In Go-Back-NARQmethod,bothsenderandreceivermaintaina window.
- In this protocol we can send several frames before receivingacknowledgments; we keep a copy of these frames until the acknowledgments arrive.
- This procedure requires additional features to be added to Stop-and-WaitARQ.



- Inabove, example
  - It can be seen in figure that error occurs in Frame 5.Hence the receiver sends negative acknowledgment of Frame 5 to the sender.
  - In such a case, the sender needs to retransmit Frame 5 and all the succeeding frames (Frame 6 and Frame 7)
- The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.
- When the sender sends all the frames in window, it checks up to whatsequence number it has received positive acknowledgement. If all frames are positively acknowledged, the sender sends next set of frames. If sender finds that it hasreceived NACK or has not received any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.

✓ **Selective-Reject ARQ**

- In selective-reject ARQ error control, the only frames retransmitted are those receive a NAK or which time out.
- Go-Back-N ARQ simplifies the process at the receiver site. Receiver only keeps track of only one variable, and there is no need to buffer out-of-order frames, they are simply discarded.
- However, Go-Back-N ARQ protocol is inefficient for noisy link. It bandwidth inefficient and slows down the transmission.
- In Selective Repeat ARQ, only the damaged frame is resent. More bandwidth efficient but more complex processing at receiver.
- It defines a negative ACK(NAK)to reportthesequence number of adamaged frame before the timer expires.



- Frames 0 and 1 are accepted when received because they are in the range specified by the receiver window. Same for frame 3.
- Receiver sends a NAK2 to show that frame 2 has not been received and then sender resends only frame 2 and it is accepted as it is in the range of the window.
- Size of thesenderandreceiverwindowsmustbeatmostone-halfof 2m.Ifm =2, window size should be 2^m /2 = 2. Fig compares a window size of 2 with a window size of 3. Window size is 3 and all ACKs are lost, sender sends duplicate of frame 0, window of the receiver expect to receive frame 0 (part of the window), so accepts frame 0, as the 1st frame of the next cycle – an **error.**
- Efficiency of Selective Repeat Protocol (SRP) is same as GO-Back-N's efficiency :
  - Efficiency=N/(1+2a)
  - Wherea=Propagationdelay /Transmissiondelay
  - Buffers=N+N
  - Sequencenumber =N(sender side) +N(ReceiverSide).

Medium Access Control Sublayer:

Channel allocation problem:

- ✓ To allocate a single broadcast channel among competing users. The channel might bea portion of the wireless spectrum in a geographic region, or a single wire or optical fiber to which multiple nodes are connected.
- ✓ There are two types of channel allocation: **Static Channel Allocation and Dynamic Channel Allocation.**
  - **StaticChannel Allocation**:
    - If there are N users, the bandwidth is divided into N equal sized portions, with each user being assigned one portion. Since each userhasaprivate frequencyband,thereisnownointerference amongusers.
    - When there is only a small and constant number of a user, each of which has a steady stream or a heavy load of traffic, this division is a simple and efficient allocation mechanism.
    - A wireless example is FM radio stations. Each station gets a portion of the FM band and uses it most of the time to broadcast its signal. When the number of senders is large and varying or the traffic is suddenly changing (burst of data), FDM presents some problems.
    - If the spectrum is cut up into N regions and fewer than N users are currently interested in communicating, a large piece of valuable spectrum will be wasted. And if more than N users want to communicate, some of them will be denied permission for lack of bandwidth, even if some of the users who have been assigned a frequency band hardly ever transmit or receive anything.
    - Astaticallocationisapoorfittomostcomputersystems,inwhichdata traffic is extremely burst, often with peak traffic to mean traffic ratios of 1000:1. Consequently, most of the channels will be idle most of the time.
    - The poor performance of static FDM can easily be seen with a simple queuingtheory calculation.Letusstartby finding themeantimedelay, T, to send a frame onto a channel of capacity C bps.
    - Weassumethattheframesarriverandomlywithanaveragearrivalrate of λ frames/sec, and that the frames vary in length with an average length of 1/μ bits. With these parameters, the service rate of thechannel is μC frames/sec.
    - Astandardqueueingtheoryresultis $T = 1/(\mu C - \lambda)$
    - Now let us divide the single channel into N independent subchannels, each with capacity C /N bps. The mean input rate on each of the subchannels will now be λ/N. Recomputing T, we get

      $TN = 1/(\mu(C/N) - (\lambda/N)) = N/(\mu C - \lambda) = NT$

- Eg: if C is 100 Mbps, the mean frame length, 1/μ, is 10,000 bits, andthe frame arrival rate, λ, is 5000 frames/sec, then
- T=1/(μC −λ)èT =200 μsec.
- Now if 100-Mbps network with 10 networks of 10 Mbps each and staticallyallocateeachusertooneofthem,themeandelaywouldjump from 200 μsec to 2 msec.
- The mean delay for the divided channel is N times worse than that of without dividing. (TN = NT)
- ThissameresultsaysthatabanklobbyfullATMmachinesisbetteroff having a single queue feeding all the machines than a separate queue in front of each machine

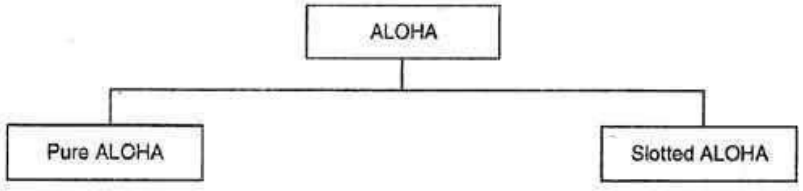
- **AssumptionsforDynamicChannelAllocation:**
  - Underlying all the work done in this area are the following five key assumptions:
  - Independent
    - The model consists of N independent stations each with a program or user that generates frames for transmission. Once a frame has been generated, the station is blocked and does nothing until the frame has been successfully transmitted.
  - TrafficSingleChannel
    - A single channel is available for all communication. Allstations can transmit on it and all can receive from it.
  - ObservableCollisions
    - All stations can detect that a collision has occurred. A collided frame must be transmitted again later.
  - Continuousor SlottedTime
    - Time may be assumed continuous; frame transmission canbegin at any instant. Alternatively, time may be slotted or divided into discrete intervals (called slots). Frame transmissions must then begin at the start of a slot.
  - CarrierSenseorNoCarrierSense
    - With the carrier sense assumption, stations can tell if the channel is in use before trying to use it. Station will transmit only when channel is free.

Multiple access protocols

✓ ALOHA

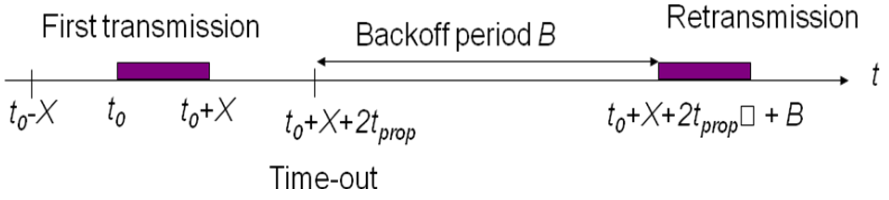
- It was developed at the University of Hawaii in the early 1970s to connect computers situated on different Hawaiian islands. The computers of the ALOHA network transmit on the same radio channel whenever they have a packet to transmit. From time-to-time packet transmission will collide, but these can be treated as transmission errors, and recovery can take place by retransmission. When traffic is very light, the probability of collision is very small, and so retransmissions need to be carried out infrequently.
- ALOHA scheme requires stations to use a random retransmission time. ALOHA is the father of multiple access protocols.

- Abramson's work, called the ALOHA system, used ground based radio broadcasting. The basic idea is applicable to any system in which uncoordinated users are competing for the use of a single shared channel.
- Two versions of ALOHA: pure and slotted. They differ with respect towhethertimeiscontinuous,asinthepureversion, ordividedintodiscreteslots into which all frames must fit.(slotted aloha)

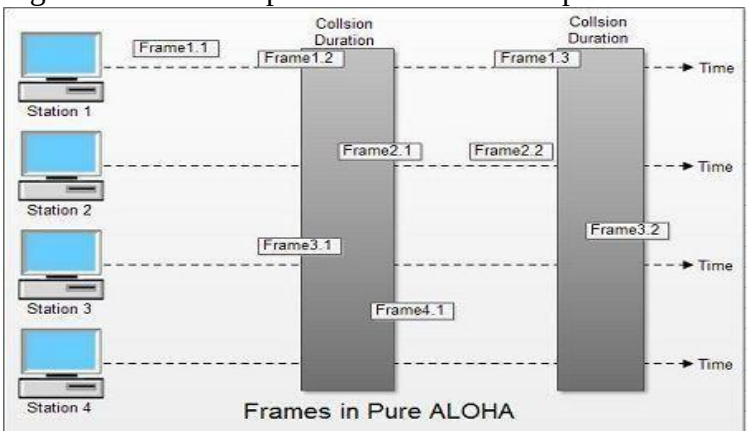


Types of ALOHA

- **PureALOHA(unslottedALOHA):**
  - In pure ALOHA, the stations transmit frames whenever they have data to send.
  - In pure ALOHA, wheneverany station transmits aframe,it expects the acknowledgement from the receiver.
  - If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed.
  - If the frame is destroyed because of collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise same frames will collide again and again.
  - Systems in which multiple users sharea common channel in a way that can lead to conflicts are known as contention systems
  - Therefore pure ALOHA dictates that when time-out period passes,each station must wait for a random amount of time before resendingits frame. This randomness will help avoid more collisions.

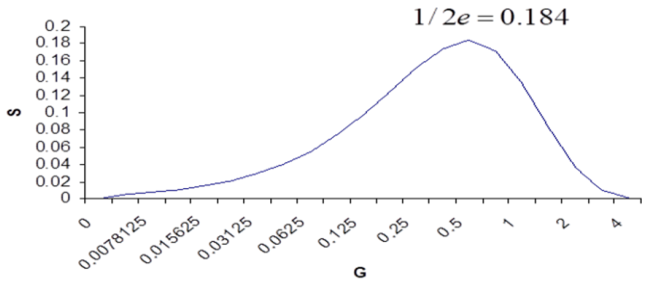


  - Figureshowsanexample offramecollisionsinpureALOHA.



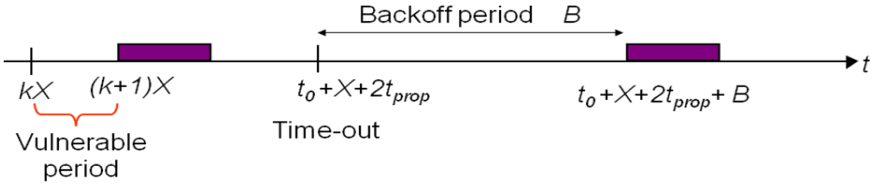
Frames in Pure ALOHA

- In figtherearefourstationsthat.contendedwith oneanotherforaccess to shared channel. All these stations are transmitting frames. Some of these frames collide because multiple frames are in contention for the shared channel. Only two frames, frame 1.1 and frame 2.2 survive. All other frames are destroyed.
- Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be damaged. If first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted.
- Performancegraph:



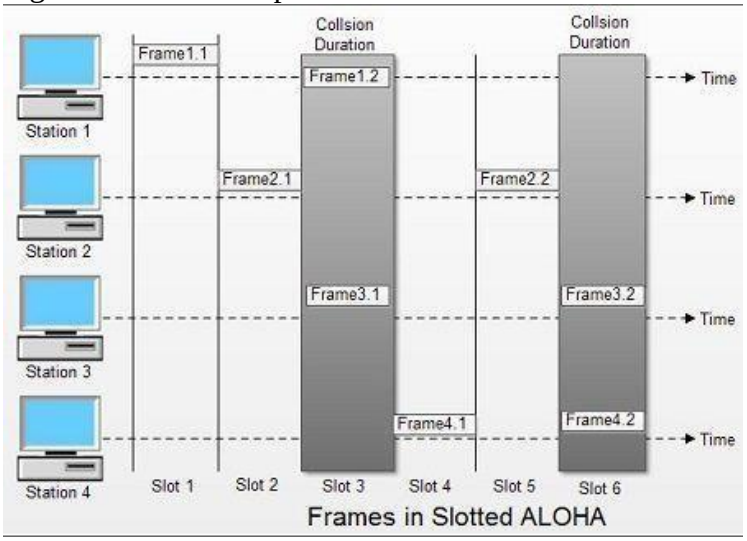
Throughput S versus load G for pure ALOHA

- **SlottedALOHA**
  - SlottedALOHAwasinventedtoimprovetheefficiencyofpure ALOHA as chances of collision in pureALOHA areveryhigh.
  - InslottedALOHA,thetimeofthesharedchannelisdividedinto discrete intervals called slots.
  - Thestationscansendaframeonlyatthebeginningoftheslotandonly one frame is sent in each slot.

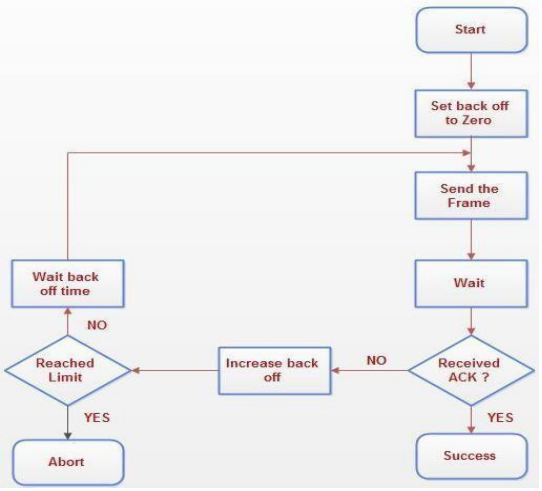


Only packets that arrive during prior X seconds collide.

- Figureshows anexampleofframecollisionsinslottedALOHA.



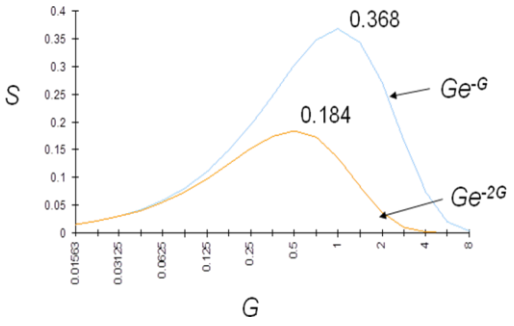
- In slotted ALOHA, if any station is notable to place the frame onto the channel at the beginning of the slot i.e. it misses the time slot then the station has to wait until the beginning of the next time slot.
- In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot as shown in fig.
- Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half.
- Flowchartfor ALOHA:



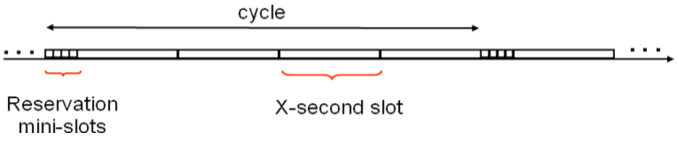
- ThroughputofSlottedALOHA

$S = GP[\text{nocollision}] = GP[\text{noarrivalsinXseconds}]$

$= G \cdot \frac{(G)^0 e^{-G}}{0!} = G \cdot e^{-G}$

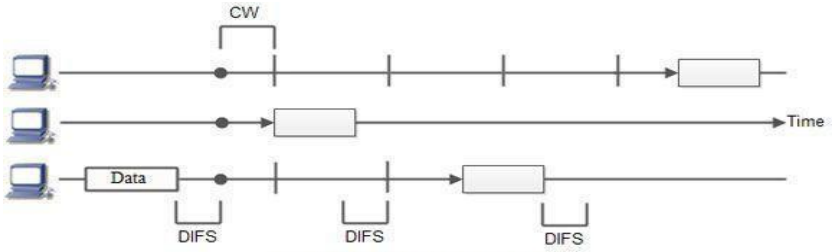


- **ApplicationofSlottedALOHA**



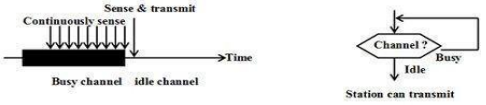
- Reservationprotocolallowsalargenumberofstationswithinfrequent traffic to reserve slots to transmit their packets in future cycles
- Eachcyclehasmini-slotsallocatedformakingreservations
- StationsuseslottedALOHAduring mini-slotsto requestslots

- ✓ **CarrierSensingMultipleAccess(CSMA)Protocols**
  - CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network.
  - MA (Multiple Access) indicates that many devices can connect to and sharethe same network. All devices have equal access to use the network when it is clear.
  - Astationsensesthechannelbeforeitstarts transmission
    - Ifbusy,eitherwait orschedulebackoff(differentoptions)
    - Ifidle,start transmission
    - A station that wants to communicate "listen" first on the media communication and awaits a "silence" of a preset time (called the Distributed Inter Frame Space or DIFS). After this compulsory period, the station starts a countdown for a random period considered. The maximum duration of this countdown is called the collision window (Window Collision, CW). If no equipment speaks before the end of the countdown, the station simply delivers its package. However, if it is overtaken by another station, it stops immediately its countdown and waits for the next silence.

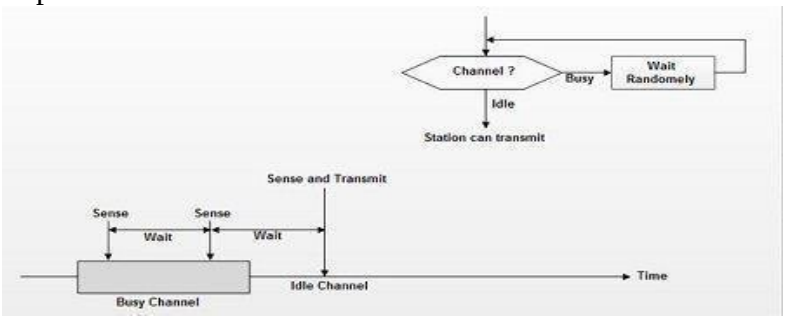


Sharing time with CSMA method.

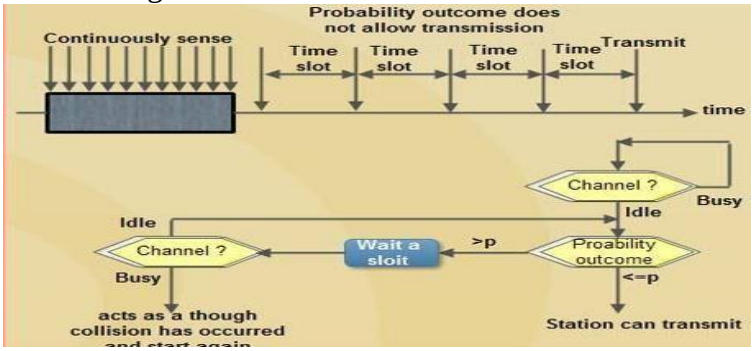
  - CSMAprotocolwasdevelopedtoovercometheproblemfoundin ALOHA i.e. to minimize the chances of collision, so as to improve the performance.
  - CSMA protocol is based on the principle of 'carrier sense'. The station senses the carrier or channel before transmitting a frame. It means the station checks the state of channel, whether it is idle or busy. The chances of collision still exist because of propagation delay. The frame transmitted by one station takes some time to reach other stations. In the meantime, other stations may sensethe channel to be idle and transmit their frames. This results in the collision.
  - **TherearеThreeDifferentTypeofCSMA Protocols**
    - **1-persistentCSMA**
      - In this method, station that wants to transmit data continuously senses the channel to check whether the channel is idle orbusy.
      - Ifthechannelis busy,thestationwaits untilitbecomesidle.
      - When the station detects an idle-channel, it immediately transmits the frame with probability 1. Hence it is called I-persistent CSMA.
      - This method has the highest chance of collision because two or more stations may find channel to be idle at the same time and transmit their frames. When the collision occurs, the stations wait a random amount of time and start all over again.



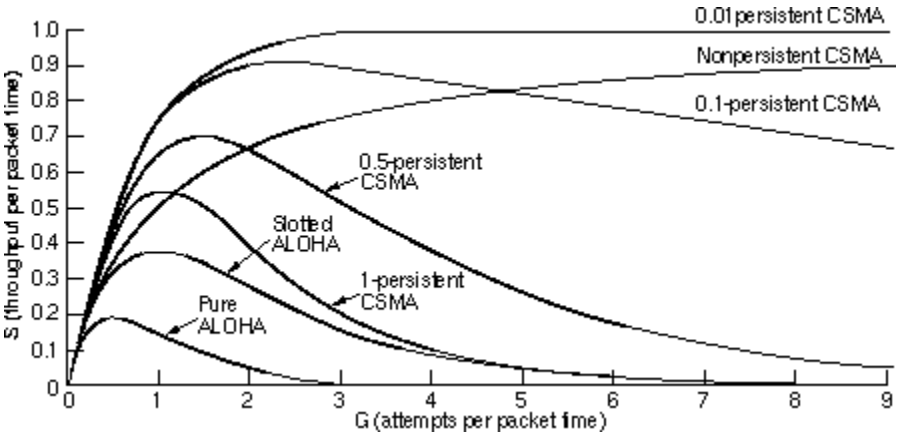
- **Non-persistentCSMA**
  - Inthisscheme,ifastationwantstotransmitaframeanditfinds that thechannel is busy (someotherstation is transmitting)then it will wait for fixed interval of time.
  - After this time, it again checks the status of the channel and if the channel is free it will transmit.
  - Astationthat hasaframetosend sensesthechannel.
  - Ifthechannel isidle, itsendsimmediately.
  - If the channel is busy, it waits a random amount of time and then senses the channel again.
  - Innon-persistentCSMAthestationdoesnotcontinuouslysense the channel for the purpose of capturing it when it detects the end of previous transmission.



- **p-persistentCSMA**
  - This method is used when channel has time slots such that the time slot duration is equal to or greater than the maximum propagation delay time.
  - Whenever a station becomes ready to send, it senses the channel.
  - Ifchannel isbusy, station waitsuntil nextslot.
  - Ifchannelisidle, ittransmitswith aprobabilityp.
  - With the probability q=l-p, the station then waits for the beginning of the next time slot.
  - If the next slot is also idle, it either transmits or waits againwith probabilities p and q.
  - This process is repeated till eitherframehas been transmitted or another station has begun transmitting.
  - In caseofthetransmission by anotherstation, the station acts as thoughacollisionhasoccurredanditwaitsarandomamount of time and starts again.

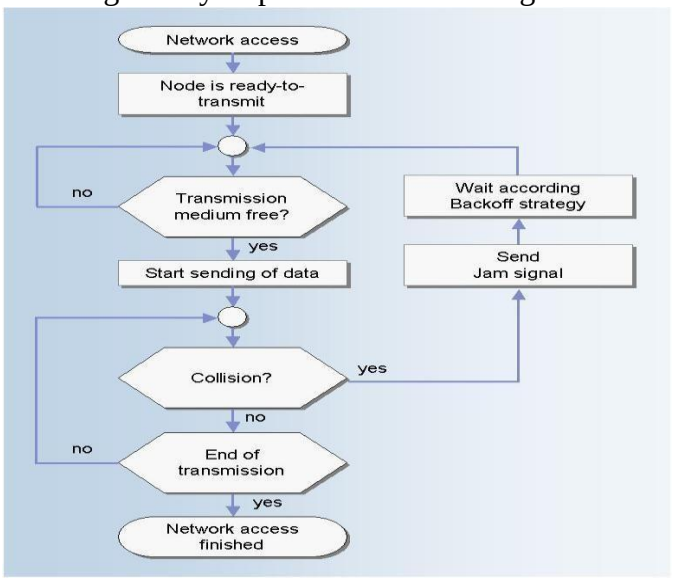


- Comparison of the channel utilization versus load for various random access protocols.



✓ **CarrierSensingMultipleAccesswithcollisiondetectionProtocolsCSMA/CD**

- CSMA/CD (carrier sense multiple access with collision detection) media access protocol is used.
  - Dataistransmittedintheformofpackets.
  - Sensechannelpriorto actualpacket transmission.
  - Transmit packet only if channel is sensed idle; else, defer the transmission until channel becomes idle.
  - After packet transmission is started, the node monitors its own transmission to see if the packet has experienced a collision.
  - Thejam signal is a signal that carries a 32-bit binary pattern sent by a data station to inform the other stations that they must not transmit.
  - If the packet is observed to be undergoing a collision, the transmission is aborted and the packet is retransmitted after a random interval oftime using Binary Exponential Backoff algorithm.



Ethernet

- ✓ Ethernet(pronounced "eethernet") isacomputer networktechnology whichisusedin different area networks like LAN, MAN, WAN.
- ✓ Ethernetconnectingcomputerstogetherwithcablesothecomputerscan share information.
- ✓ Within each main branch of the network, "Ethernet" can connect up to 1,024 personal computers and workstations.
- ✓ Ethernet provides services on the Physical (Layers 1) and Data Link Layer (Layers 2) of OSI reference model.
- ✓ The Data Link Layer is further divided into two sub layers that are Logical Link Control (LLC) and Media Access Control (MAC),these sub layers can be used to establish the transmission paths and format data before transmitting on the same network segment.
- ✓ **History of Ethernet**
    - Ethernet was developed at Xerox PARC between 1973 and 1974. It was inspired by ALOHAnet, which Robert Metcalfe had studied as part of his PhD dissertation. The idea was first documented in a memo that Metcalfe wrote on May 22, 1973, where he named it after theluminiferous aether once postulated to exist as an omnipresent, completely-passive medium for the propagation of electromagnetic waves. In 1975, Xerox filed a patent application listing Metcalfe, David Boggs,Chuck Thacker, and Butler Lampson as inventors. In 1976, after the system was deployed at PARC, Metcalfe and Boggs publishedaseminalpaper.Thatsameyear,RonCrane,BobGarner,andRoyOgus facilitated the upgrade from theoriginal2.94 Mbit/sprotocoltothe 10 Mbit/s protocol which was released to the market in 1980.
    - Metcalfe left Xerox in June 1979 to form 3Com. He convinced DigitalEquipment Corporation (DEC), Intel, and Xerox to work together to promote Ethernet as a standard. The so-called "DIX" standard, for"Digital/Intel/Xerox", specified 10 Mbit/s Ethernet, with 48-bit destination and source addresses and a global 16-bit Ethertype-type field. It was published on September 30, 1980 as "The Ethernet, A Local Area Network. Data LinkLayer and Physical Layer Specifications". Version 2 was published in November, 1982 and defines whathasbecomeknownas EthernetII. Formal standardization efforts proceeded at the same time and resulted in the publication of IEEE 802.3 on June 23, 1983.

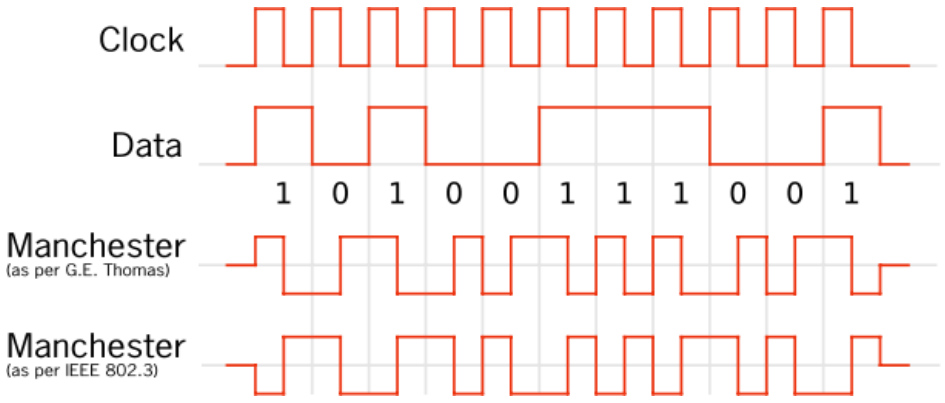
Ethernet cabling

Name	IEEE Standard	DataRate	MediaType	MaximumDistance
Ethernet	802.3	10 Mbps	10Base-T	100 meters
FastEthernet/ 100Base-T	802.3u	100 Mbps	100Base-TX 100Base-FX	100 meters 2000 meters
Gigabit	802.3z	1000	1000Base-T	100 meters

Ethernet/ GigE		Mbps	1000Base-SX 1000Base-LX	275/550 meters 550/5000meters
10Gigabit Ethernet	IEEE 802.3ae	10 Gbps	10GBase-SR 10GBase-LX4 10GBase-LR/ER 10GBase-SW/LW/EW	300 meters 300mMMF/10km SMF 10km/40km 300m/10km/40km

Manchester encoding

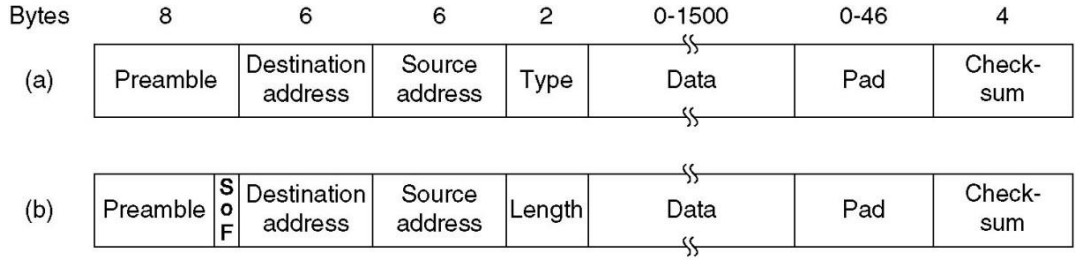
- ✓ Manchester code (also known as phase encoding, or PE) is a line code in which the encoding of each data bit is either low then high, or high then low, for equal time. Itis a self-clocking signal with no DC component.
- ✓ Manchester code was used in early Ethernet physical layer standards and is still usedin consumer IR protocols, RFID and near-field communication.
- ✓ Manchester coding is a special case of binary phase-shift keying (BPSK), where the data controls the phase of a square wave carrier whose frequency is the data rate. Manchester code ensures frequent line voltage transitions, directly proportional to the clock rate; this helps clock recovery.



- ✓ Manchester code always has a transition at the middle of each bit period and may (depending on the information to be transmitted) have a transition at the start of the periodalso.Thedirectionofthemid-bittransitionindicatesthedata.Transitionsat the period boundaries do not carry information. They exist only to place the signal in the correct state to allow the mid-bit transition.

The Ethernet MAC sublayer protocol

- ✓ In Standard Ethernet, the MAC sublayer governs the operation of the access method.It also frames data received from the upper layer and passes them to the physicallayer.



Figure(a)DIXFrame Format(b) IEEE82.3Frame Format

- ✓ PREAMBLE
  - o Itcontains7bytesofalternating0'sand1'sthatalertsthereceivingsystemto the coming frame and enables it to synchronize its input timing
  - o Itprovidesonlyanalertandthepatternallowsthestationstomisssomebytes at the beginning of the frame.
  - o Itisactuallyadded atthephysicallayer.

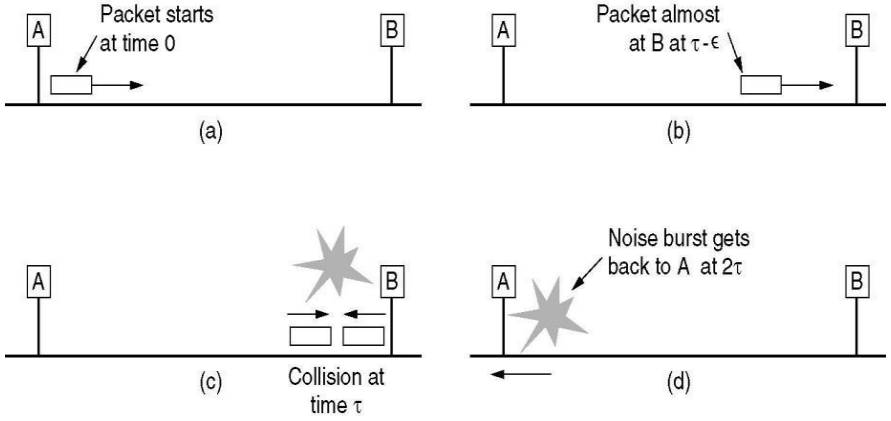
- ✓ STARTFRAMEDELIMITER(SFD)
  - o Signalsthebeginning ofthe frame
  - o Warnsthestations thatthis is thelast chanceforsynchronization
  - o Thelast2bitsare11andalertsthereceiverthatthenextfieldisthe destination address
- ✓ DESTINATIONADDRESS(DA)
  - o SizeoftheDestinationaddress is6bytes
  - o Containsthephysicaladdressofthe destinationstationtoreceivethepacket
- ✓ SOURCEADDRESS(SA)
  - o Sizeof theSourceaddressis 6bytes
  - o Containsphysicaladdress ofthesenderof thepacket.
  - o ADDRESSING
    - o EachstationonanEthernetnetworkhasitsown*networkinterfacecard* (NIC)
    - o Itprovidesthestationwitha6-bytephysicaladdress,normallywriteina hexadecimal notation, with a colon between the bytes, for eg.

      06: 01 : 02: 2C: 4B :7C
- ✓ LENGTH
  - o Usedas alengthfield todefinethenumberofbytes inthedatafield
- ✓ DATA
  - o Carriesthedataencapsulatedfromtheupperlayerprotocols
  - o Minimum 46bytes
  - o Maximum1500bytes
- ✓ CheckSum (CRC)
  - o Thisfieldcontainserror detectioninformation
- ✓ TYPE
  - o Unicast:one–to-one
  - o Multicast:one-to–many

- Broadcast:recipientsare all thestationsontheLAN
- Iftheleastsignificantbit ofthe1stbyteinadestinationaddressis0,the address is unicast; otherwise it is a multicast

✓ FRAME LENGTH
- Minimumlengthofdatafrom upper layer is46bytes
- Ifthe datais less than46bytes, padding isadded to makeup theDifference
- Maximumlengthof data fromupperlayeris1500 bytes
- MemorywasveryexpensivewhenEthernetwasdesigned,maximumlength restriction helped to reduce the size of the buffer
- Maximumlengthrestrictionpreventsonestationfrommonopolizingthe shared medium , blocking other stations that have data to send

✓ Collision Detection



- Collisiondetectioncantakeaslongas 2t.
- The reason for having a minimum length frame is to prevent a station from completing the transmission of a short frame before the first bit has even reached the far end of the cable, where it may collide with another frame.
- This problem is illustrated in Fig. At time 0, station A, at one end of the network, sends off a frame. Let us call the propagation time for this frame to reachtheotherend τ.Justbeforethe framegetstotheotherend(i.e.,attimeτ-ε), the most distant station, B, starts transmitting. When B detects that it is receiving more power than it is putting out, it knows that a collision has occurred, so it aborts its transmission and generates a 48-bit noise burst towarn all other stations. In other words, it jams the ether to make sure thesender does not miss the collision. At about time 2τ, the sender sees the noise burst and aborts itstransmission, too. Itthen waits a random time before trying again.

Thebinaryexponentialbackoffalgorithm

✓ After a collision the time is divided in discrete slots (equal to worst round trip propagation, which is 512 bits time or 51.2 us)

✓ Afterthefirstcollision,each stationwaits0or1 slottimebeforetriesagain
- Iftwostation collideandtheypick samenumber, they willcollideagain

✓ Afterasecondcollision,eachstationwaits0,1,2or3atrandomandwaitsthat number of slot times.

✓ Afterathirdcollisionwillhappen,thenextnumbertopickisbetween0 and23 -1and that number of slots is skipped.

✓ After10collisionshave beenreached,the numberintervalisfrozenat0– 1023.

- ✓ After 16 collisions, the station gives upto sent the frame and reports the failure.Further recovery it is up to the higher.

Switched ethernet

- ✓ Multiple network devices in a LAN require network equipments such as a network switch or hub. When using a network switch, a regular network cable is used insteadof a crossover cable. The crossover cable consists of a transmission pair at one endand a receiving pair at the other end.
- ✓ The main function of a network switch is to forward data from one device to another device on the same network. Thus a network switch performs this task efficiently as the data is transferred from one device to another without affecting other devices on the same network.

- ✓ The network switch normally supports different data transfer rates. The most common datatransferratesinclude10 Mbps – 100 Mbps forfast Ethernet, and 1000 Mbps – 10 Gbps for the latest Ethernet.
- ✓ Switch Ethernet uses star topology, which is organized around a switch. The switch in a network uses a filtering and switching mechanism similar to the one used by the gateways, in which these techniques have been in use for a long time.
- ✓ ThistypeofEthernetmakes useofstartopology.

Fast Ethernet

- ✓ ThistypeofEthernetcantransferdataatarateof100Mbps.FastEthernetmakesuse of twisted pair cable or fiber optic cable for communication.
- ✓ Fast Ethernet is one of the versions of the Ethernet standard that enables the transmissionofdataover100megabitspersecondonlocalareanetworks(LAN).
- ✓ Itwaslaunchedin 1995andwas thefastestnetwork connectionofitstime.
- ✓ FastEthernetisalsoknownas100BaseXor100MbpsEthernet,andisdefinedby the IEEE 802.3u protocol.
- ✓ Itwasinitiallydesignedforcopper-basedtwistedpaircablenetworksandincludedthe 100 Base-TX, 100 Base-T4 and 100 Base-T2 standards.
- ✓ Thelength ofthe cable incopper-based fastEthernet was restrictedto 100meters.
- ✓ Thefiber-basedfastEthernetstandards100Base-FX,100BaseSX,100BaseBXand 100 Base LX10 use one or more strands and modes of fiber optics to transmit data.
- ✓ Therangeoffast Ethernet forfiber mode canbefrom 400yards to upto 25miles.

Reference Book: Computer Networks, Andrew Tanenbaum, 6th Edition.

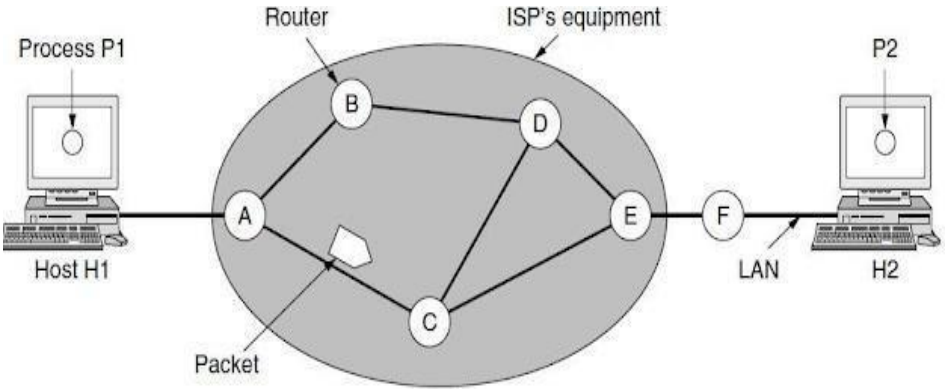
UNIT-III
THE NETWORK LAYER

Functions of Network Layer

- ✓ Routing– find apath from onehost to anotherhost.
- ✓ Congestioncontrol–mechanismsto preventhostsfromfloodingthe network.
- ✓ QualityofService(QoS) -transmission rates, errorrates,andothercharacteristics can be measured, improved, and, to some extent, guaranteed in advance.
- ✓ Internetworkingprovides translationbetweensubnetusingdifferentprotocols.

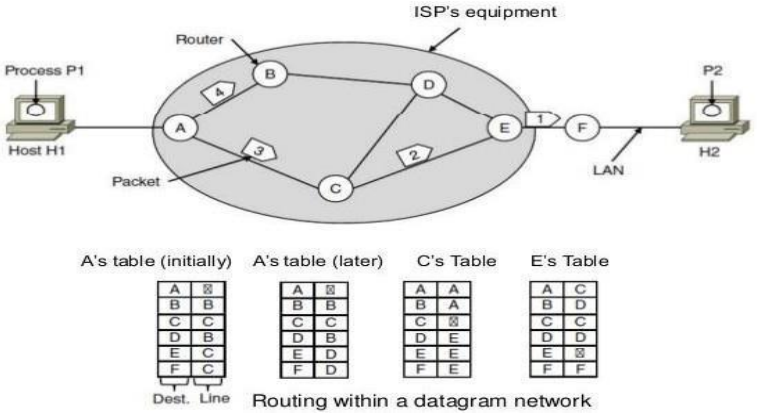
Network layer design issues

- ✓ Store-and-ForwardPacketSwitching
- ✓ ServicesProvidedtothe TransportLayer
- ✓ ImplementationofConnectionlessService
- ✓ ImplementationofConnection-OrientedService
  - **Store-and-Forward Packet Switching**

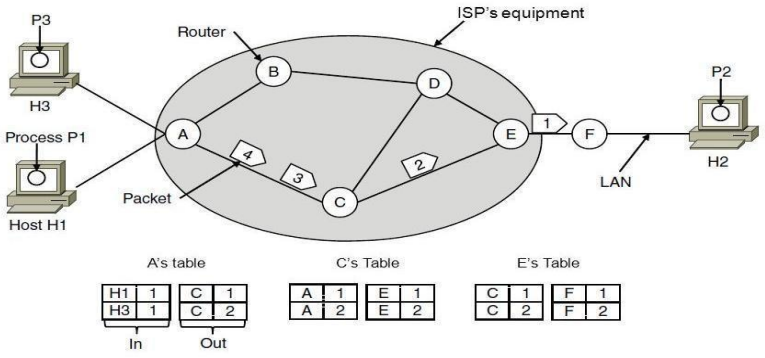


- The major components of the network are the carrier's equipment (routers connected by transmission lines), shown inside theshaded oval, and the
- Customers'equipment,shownoutsidetheoval.
- Host H1 is directly connected to one of the carrier's routers, A, by a leased line. In contrast, H2 is on a LAN with a router, F, owned and operated by the customer. This router also has a leased line to the carrier's equipment.
- We have shown F as being outside the oval because it does not belong to the carrier, but in terms of construction, software, and protocols, it is probably no different from the carrier's routers.
- This equipment is used as follows. A host with a packet to send transmits it tothenearest router,eitheron its ownLANoroverapoint- to-point link to the carrier. The packet is stored there until it has fully arrived so the checksum can be verified.
- Then it is forwarded tothe next router along the path until it reachesthe destination host, where it is delivered. This mechanism is store- and-forward packet switching.

- **Services Provided to the Transport Layer**
  - The network layer provides services to the transport layer at the network layer/transport layer interface. An important question is what kind of services the network layer provides to the transport layer.
  - The network layer services have been designed with the followinggoals in mind.
    - 1.Theservicesshouldbeindependent oftherouter technology.
    - 2. The transport layer should be shielded fromthe number,type, and topology of the routers present.
    - 3. Network addresses available to transport layer should use be uniform, even across LANs and WANs.
- **Implementation of Connection less Service**
  - Noadvancesetupisneeded.
  - Thepacketsarefrequentlycalleddatagrams.
  - Thesubnetiscalled adatagramnetwork.
  - Theroutingalgorithmisthealgorithmthatmanagesthetablesand makes the routing decision.



- **Implementation of Connection-Oriented Service**
  - A path from the source router to the destination router must be established before any data packets can be sent.
  - TheconnectioniscalledaVC(virtualcircuit).
  - Thenetworkiscalledavirtual-circuit network.
  - To distinguish packets from different hosts, replacing connection identifiers in outgoing packets is called label switching.



Routing within a virtual-circuit network

- ✓ **Comparison of Virtual-Circuit and Datagram Network**

Issue	Datagram subnet	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

Routing Algorithms

- ✓ Routing is the process of moving packets from the source to a destination ininternetworking.
- ✓ Routingprotocols usearoutingalgorithm whichisamathematical formula toforward the packet to its destination.
- ✓ The main function of the network layer is routing packets from the source machine to the destination machine.
- ✓ Inmost networks,packetswill requiremultiplehopstomakethe journey.
- ✓ More than one route is possible in every network; however the shortest route shouldbe selected.
- ✓ The shortest route means, a route which passes through the least number of nodes toreach the destination.
- ✓ The routing algorithm is designed to find the shortest route and it is part of networksoftware.
- ✓ Routing Table: To route IP packets, a host or a router has a routing table with entries for each destination or a combination of destinations.
    - Astaticroutingtablecontainsinformation,whichisenteredmanually.The administrator enters the route for each destination into the table.
    - Dynamic routing table is updated periodicallyby using dynamic protocols like RIP, OSPF or BGP.
- ✓ **The routing algorithm can be classified into two types:**
    - **Static(non-adaptive)routingalgorithms**
        - In this type, the network topology determines the final path. All the possible paths which are already calculated are loaded into the routing table.
        - Staticroutingis suitableforsmall networks.
        - The disadvantage of static routing is, inability to respond quickly in case of network failure.
    - **Dynamic(Adaptive)routingalgorithms**
        - The dynamic routing algorithms can change their routing decision on the basis of some changes made in the topology.

- Each router can check the network status by communicating with theneighbours. So, the changes in the topologyare reflected to all routers.
- Finally,theroutercancalculatethesuitablepathtothefinal destination.
- Thedisadvantageofthistypeiscomplexityin therouter.

✓ **Intra-domainRoutingandInter-domainRouting**

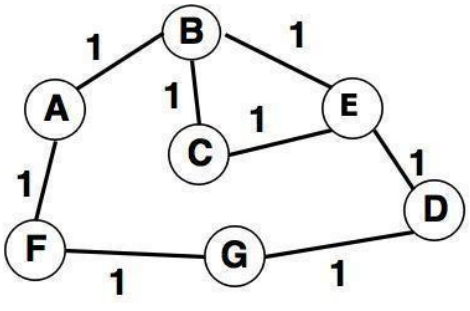
- An autonomous system is a group of the networks and the routers, which are operated by the network administrator. Internet can be dividedinto autonomous systems.
- Routinginsideanautonomous systemisreferred toasintra-domainrouting.
  - Protocols for Intra-domain routing are called as interior gateway protocols.
  - Distance vector and link state routing are the examples of Intra-domain routing.
    - Example:RIPandOSPF
- Routing between two or more autonomous systems can be referred to as inter-domain routing.
  - ProtocolforInter-domainroutingarealsocalledas exteriorgateway protocols.
  - Pathvectorisanexampleofaninter-domainrouting.
    - Example: BGP

Distance VectorRouting

✓ Distancevector routingis the dynamic routing algorithm and also known as**Bellman-Ford** routing algorithm and **Ford- Fulkerson** algorithm.
✓ Itwasdesignedforsmallnetworktopologies.
✓ In this algorithm, node router constructs a table containing the distance (total cost of path) to all other nodes and distributes that vector to its immediate neighbors.
✓ For distance vector routing, it is assumed that each node knows the cost of the link to each of its directly connected neighbors.
✓ Alink,whichis'down'isassignedasaninfinitecost.
✓ Everynodesendsamessageto itsdirectlyconnectedneighbors

- **Forexample:**AsendsitsinformationtoBand F.

✓ After communicating to each directlyconnected node the shortest path can be easyto compute (as shown in above table).



Distance Vector Routing

Information at Node	Cost to Reach Node						
	A	B	C	D	E	F	G
A	0	1	2	3	2	1	2
B	1	0	1	2	1	2	3
C	2	1	0	2	1	3	3
D	3	2	2	0	1	2	2
E	2	1	1	1	0	3	2
F	1	2	3	2	3	0	1
G	2	3	3	1	2	1	0

Routing Information Protocol(RIP)

- ✓ RIP is a dynamic,distance vector routing protocol based around the Berkely BSD application *routed* andwasdevelopedforsmaller IP based networks.RIP uses UDP port 520 for route updates. RIP calculates the best routebased on hopcount.Likeall distancevectorroutingprotocols,RIPtakessometime to converge. While RIP requires less CPU power and RAM than some other routing protocols, RIP does have some limitations:
  - o Metric:Hop Count
    - SinceRIP calculates the best routeto a destination based solelyon how many hops it is to the destination network, RIP tends to be inefficientinnetwork usingmorethanoneLANprotocol,suchasFastEthernet and serial or Token Ring. This is because RIP prefers paths with the shortest hop count. The path with the shortest hop count might be over the slowest link in the network.
  - o HopCountLimit
    - RIP cannot handle more than 15 hops. Anything more than 15 hops away is considered unreachable by RIP. This fact is used by RIP to prevent routing loops.
  - o ClassfulRouting Only
    - RIP is a classfulrouting protocol. RIP cannot handle classless routing. RIP v1 advertises all networks it knows as classfulnetworks, so it is impossible to subnet a network properly via VLSM if you are running RIP v1, which
- ✓ However,itmustbepointedoutthatRIPistheonly routing protocolthat all routing devices and software support, so in a mixed equipment environment, RIP may be your only option for dynamic routing.

- ✓ RIPMESSAGES
  - o RIPupdatesareplacedasUDPpayloadinsidean IPdatagram.Belowisthe base format of a RIP message.

command	version	zeroes
AddressFamily ID		zeroes
IPAddress		
zeroes		
zeroes		
Metric		
Payload		

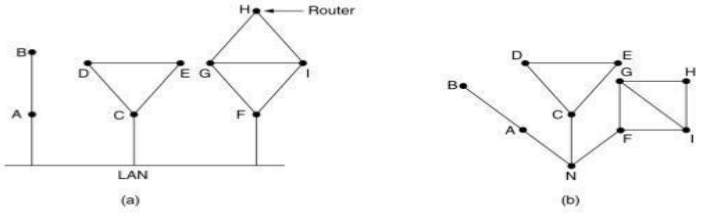
  - o COMMANDtypes(fieldvalue)
    - REQUEST (1)- Request either a partial or full table update from another RIP router.
    - RESPONSE(2)-Aresponse toa request.Allrouteupdatesusethis command in the command field.
    - TRACEON(3)/ TRACEOFF(4)-Obsoleteand ignored.
    - RESERVED (5) - Sun Microsystems uses this field for it's own purposes.
  - o VERSIONfield -Describes whichversionoftheRIPprotocol itis (1or2).
  - o ADDRESS FAMILY ID - Identifies which addressing protocol is being used

(CLNS, IPX, IP etc.)

- METRIC-Metricmeasureshow'good'arouteis.RIPusesthenumberof hops as the metric. The route with the fewest number of hops is preferred.

Link State Protocol

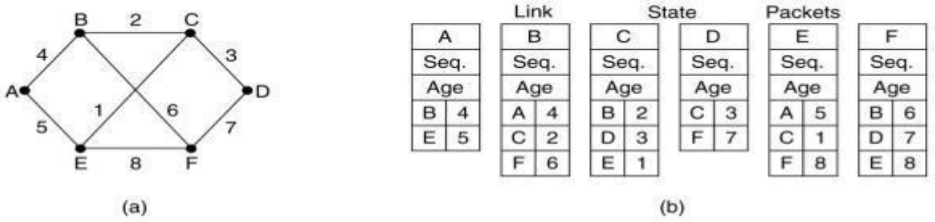
- ✓ Link stateroutingis thesecond familyofroutingprotocols.
- ✓ Link-state routing uses link-state routers to exchange messages that allow each router to learn the entire network topology.
- ✓ Based onthislearnedtopology, each routeristhen abletocomputeitsroutingtableby using a shortest path computation.
- ✓ Theideabehind link stateroutingis fairlysimple and can be stated as five parts. Each router must do the following things to make it work:
  - ✓ 1.Discoveritsneighbors andlearntheirnetwork addresses.
  - ✓ 2.Set thedistanceorcostmetrictoeachofits neighbors.
  - ✓ 3.Constructapackettellingall ithasjustlearned.
  - ✓ 4.Sendthispackettoandreceivepackets fromallother routers.
  - ✓ 5.Compute the shortestpathto everyother router.
- ✓ Dijkstra's algorithm can be run at each router to find the shortest path to every other router.
- ✓ **Learningabout theNeighbors**
  - Each Link State enabled router periodically sends a HELLO message on each of its links.
  - Neighbor routers respond to these HELLO messages identifying themselves. Within the replies, network addresses of the routers are attached and are used by the HELLO initiator to build up its neighbor table.



(a) Nine routers and a LAN. (b) A graph model of (a).

- ✓ **Setting Link Costs**
  - The link state routing algorithm requires each link to have a distance or costmetric for finding shortest paths.
  - Thecosttoreachneighborscanbesetautomatically,orconfiguredbythe network operator.
  - A common choice is to make the cost inversely proportional to the bandwidth of the link.
    - For example, 1-Gbps Ethernet may have a cost of 1 and 100-Mbps Ethernet a cost of 10. This makes higher-capacity paths better choices.
    - The most direct way to determine this delay is to send over the line a special ECHO packet that the other side is required to send back immediately.
    - By measuring the round-trip time and dividing it by two, the sending router can get a reasonable estimate of the delay.
- ✓ **BuildingLinkStatePackets**
  - Oncetheinformationneededfortheexchangehasbeencollected,thenextstep is for each router to build a packet containing all the data.
  - Thepacketstartswiththeidentityofthe sender,followed bya sequence number and age and a list of neighbors.

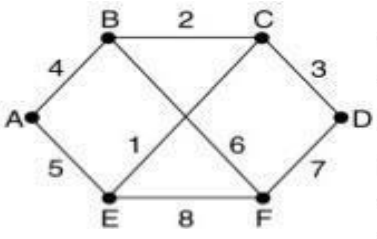
- The cost to each neighbor is also given. An example network is presented inFig. (a) with costs shown as labels on the lines.
- Thecorrespondinglinkstatepacketsforall sixroutersareshowninFig.(b).



(a) A subnet. (b) The link state packets for this subnet.

✓ **Distributing the Link State Packets**

- The trickiest part of the algorithm is distributing the link state packets. All of the routers must get all of the link state packets quickly and reliably.
- Forfloodingpackets,hereusedbasicdistribution algorithm.
  - The fundamental idea is to use flooding to distribute the link state packets to all routers.
  - To keep the flood in check, each packet contains a sequence number that is incremented for each new packet sent. Routers keep track of all the (source router, sequence) pairs they see.
  - When a new link state packet comes in, it is checked against the list of packets already seen.
    - If it is new, it is forwarded on all lines except the one it arrived on.
    - Ifitisaduplicate,itis discarded.
    - If a packet with a sequence number lower than the highest one seen so far ever arrives, it is rejected as being obsolete as the router has more recent data.



Source	Seq.	Age	Send flags A	Send flags C	Send flags F	ACK flags A	ACK flags C	ACK flags F	Data
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	

✓ **ComputingtheNew Routes**

- Once a router has accumulated a full set of link state packets, it can construct the entire network graph because every link is represented.
- Everylink is, in fact, represented twice, once for each direction. The different directions may even have different costs.
- The shortest-path computations maythen find different paths from router A to B than from router B to A.
- Now Dijkstra's algorithm can be run locally to construct the shortest paths to all possible destinations.
- Theresultsofthisalgorithmtellthe routerwhichlinktousetoreacheach destination.

Open Shortest Path First(OSPF)

✓ The Internet is made up of a large number of autonomous systems. Each AS is

operated by a different organization and can use its own routing algorithm inside.

- For example, the internal networks of companies X, Y, and Z are usually seen as three ASes if all three are on the Internet.

✓ All three may use different routing algorithms internally. Nevertheless, having standards, even for internal routing, simplifies the implementation at the boundaries between ASes and allows reuse of code.

✓ A routing algorithm within an AS is called an interior gateway protocol; an algorithm for routing between ASes is called an exterior gateway protocol.

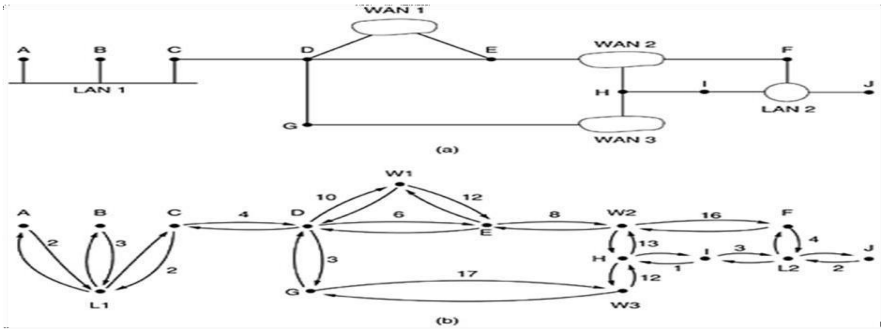
✓ The original Internet interior gateway protocol was a distance vector protocol (RIP)based on the Bellman-Ford algorithm inherited from the ARPANET.

✓ In1988,theInternetEngineeringTaskForcebeganworkonasuccessor.That successor, called OSPF (Open Shortest Path First), became a standard in 1990.

✓ OSPFsupportsthreekinds ofconnections and networks:

- 1.Point-to-pointlinesbetweenexactlytworouters.
- 2.Multiaccessnetworkswithbroadcasting(e.g.,mostLANs).

✓ 3.Multiaccessnetworkswithoutbroadcasting(e.g.,mostpacket-switchedWANs).

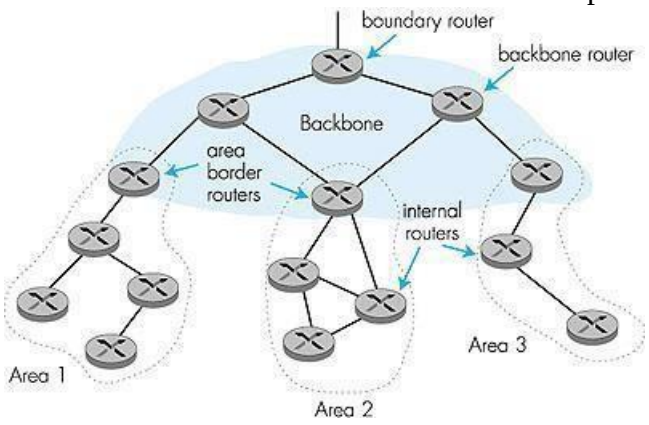


(a) An autonomous system. (b) A graph representation of (a).

✓ Many of the ASes in theInternet arethemselves largeandnontrivialto manage.

✓ OSPF allows them to be divided into numbered areas, where an area is a network or a set of contiguous networks.

✓ EveryAS has a backbone area, called area 0. All areas are connected to the backbone, possiblybytunnels, so it is possible to go from any area in the AS to anyother area in the AS via the backbone. A tunnel is represented in the graph as an arc and has a cost. Each router that is connected to two or more areas is part of the backbone.



✓ ThefivetypesofOSPF messages:

Messagetype	**Description**
Hello	Used to discover who the neighbors are
Link state update	Providesthesender'scoststoitsneighbors
Link state ack	Acknowledges link state update

Database description	Announceswhichupdatesthesenderhas
Link state request	Requests information from the partner

- Hello
  - Hello messages are used as a form of greeting, to allow a router to discover other adjacent routers on its local links and networks.
  - The messages establish relationships between neighboring devices and communicate key parameters about how OSPF is to be used in the autonomous system or area.
  - During normal operation, routers send hello messages totheir neighbors at regular intervals (the hello interval); if a router stops receiving hello messages from a neighbor, after a set period (the dead interval) the router will assume the neighbor has gone down.
- DatabaseDescription (DBD)
  - Database description messages contain descriptions of the topology of the autonomous system or area. They convey the contents of the link-state database (LSDB) for the area from one router to another. Communicating a large LSDB may require several messages to be sent by having the sending device designated as a master deviceand sending messages in sequence, with the slave (recipient of the LSDB information) responding with acknowledgements.
- LinkStateRequest (LSR)
  - Link state request messages are used by one router to request updated information about a portion of the LSDB from another router. The message specifies the link(s) for which the requesting device wants more current information.
- LinkStateUpdate(LSU)
  - *Link state update* messages contain updated information about the state of certain links on the LSDB. They are sent in response to a Link State Request message, and also broadcast or multicast by routers on a regular basis. Their contents are used to update the information in the LSDBs of routers that receive them.
- LinkStateAcknowledgment (LSAck)
  - *Link state acknowledgement* messages provide reliability to the link-state exchange process, by explicitly acknowledging receipt of a Link State Update message.

Destination Sequenced Distance Vectorrouting (DSDV)

- ✓ Destination Sequenced Distance Vector (DSDV) routing is a table driven or proactive and hop-by-hop distance vector routing protocol based on the concept of the classical distributed Bellman-Ford Algorithm, in which each mobile node maintains a routing table that contains the number of hops to reach the destination node in the shortest path, all available destinations in the network and the sequence number fixed by the destination node to prevent looping problem.
- ✓ To maintain the regularity of routing tables in a dynamically varying topology, each and every neighbor node exchanges its routing tables periodically at regular time intervals.
- ✓ A node also broadcasts its routing table to neighbors if any change occurs in the routing table due to changes in the local topology.
- ✓ Updating of the routing table is both time-driven and event-driven and is done by two

methods:

- Incremental updates: An incremental update takes a single Network Data Packet Unit (NDPU) which is used when a node does not detect considerable changes in topology.
- Full dump updates: A full dump update may take multiple NDPUs. It is done either when an incremental update wants more than a single network data packet unit or when the topology changes significantly.

✓ If thereis aspacein theincremental updatepacket, thenthoseentries maybeincluded whose sequence number has changed when routing table information is modified. When two routes to a destination are received from two different neighbors, the one with greatest number is selected. If equal the smaller hop count is selected.

✓ DSDVprotocolguarantees loopfreepathsand counttoinfinityproblemis reduced.

✓ DSDVprotocolhasfourdifferentphases,whicharedescribedas follows :

- **Route advertisements:**
  - Each node has to maintain a routing table in which all the accessible destinations within the network and the number of hops to every destination are saved.
  - Each entry in the table has a sequence number fixed by the destination node. This number enables the mobile node to distinguish stale routes from new ones, and also keep away from the formation of routing loops.
  - These routing tables are transmitting to its immediate neighbors periodically at regular intervals time.

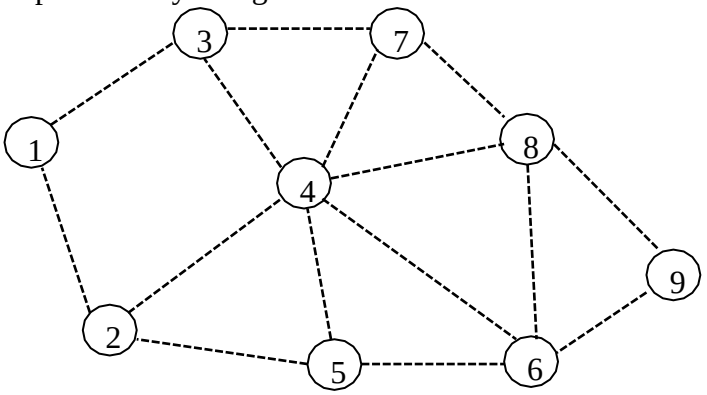


Figure1. Routeestablishments inDSDV.

- **Routingtableentryconstruction:**
  - The packet broadcast by each node has the new sequence number and the information in the packet for each new route are the destination address, the number of hops to reach the destination and the sequence number of the information received about that destination and stamped through the destination.

Table1Routingtableatnode1

Destination	Next hop	Number ofhops	Sequence number
1	1	0	20
2	2	1	16
3	3	1	78
4	3	2	48
5	2	2	52

6	2	3	18
7	3	2	78
8	2	3	58
9	2	4	24

- **Responsetochangesintopology:**
  - Each and every immediate neighbor node in the network can exchange its routing tables periodically at regular time intervals to maintain the consistency of routing tables in a dynamically changing topology. A node updates its routing table and broadcasts immediately when significant new information is available.

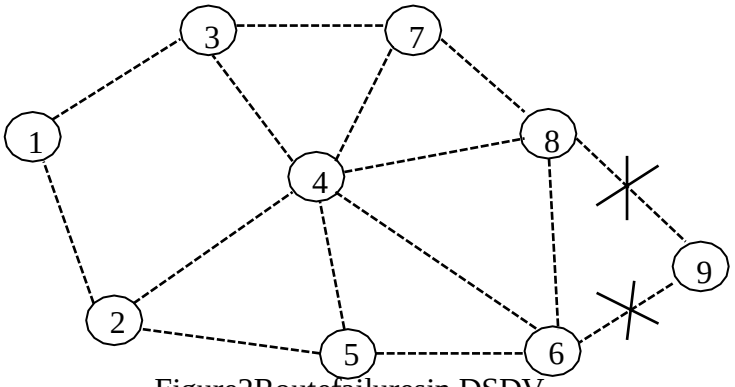


Figure2Routefailuresin DSDV

Table2Routingtable atnode1(Link failure)

Destination	Next hop	Numberof hops	Sequence number
1	1	0	20
2	2	1	16
3	3	1	78
4	3	2	48
5	2	2	52
6	2	3	18
7	3	2	78
8	2	3	58
9	2	∞	24

- **Routeselection:**
  - If thesourcenode getsnew routinginformationthrough anincremental packet, it compares with available routing information from previous routing packets.

Table3 Routingtableatnode 1(update discardbased onsequencenumber)

Destination	Next hop	Number ofhops	Sequence number
1	1	0	20
2	2	1	16
3	3	1	78
4	3	2	48
5	2	2	52
6	2	3	18
7	3	2	78
8	2	3	58

Newpacket

Destination 5

Nexthop 2

Numberof hops 2

Sequencenumber:51

Table4Routingtableat node1 (updatediscardbased onthe numberofhops)

Destination	Next hop	Number ofhops	Sequence number
1	1	0	20
2	2	1	16
3	3	1	78
4	3	2	48
5	2	2	52
6	2	3	18
7	3	2	78
8	2	3	58
9	2	4	24

Newpacket

Destination 5

Nexthop 2

Numberof hops 3

Sequencenumber:52

- The route uses the recent sequence number information. Routes with existing sequence numbers are removed. A route with a sequence number equal to an existing route is elected if it is more cost effective. Then an existing route may be removed or stored as a less preferable route.
- Table 3 indicates the routing table at node 1 forupdate discard based on sequence number. Table 4 indicates the routing table at node 1 for update discard based on the number of hops. Table 5 indicates the updated routing table at node 1.

Table5Updated routingtableatnode1

Destination	Next hop	Numberof hops	Sequence number
1	1	0	20
2	2	1	16
3	3	1	78
4	3	2	48
5	2	2	~~52~~54
6	2	3	18
7	3	2	78
8	2	3	58
9	2	4	24

Dynamic Source routing Protocol

- ✓ Dynamic Source Routing (DSR) protocol is a simple and efficient routing protocol. It is also known as on-demand protocol because the packets are forwarded only when thereisdemandbythenodes. Itdoesnotneedanynetworkinfrastructureasitisbased on demand.
- ✓ The protocol consists of route discovery and route maintenance. They are used together to discover and maintain routers.
- ✓ DSR avoids flooding and it does not need the up-to-date routing information. Hence the operation of DSR has been evaluated on a variety of patterns and communication patterns in an ad hoc network.
- ✓ DSR divides the task of routing into two distinct problems. They are route discovery and route maintenance.In route discovery, A node only tries to discover a route to a destination if it has to send something to this destination and there is currently no known route.
- ✓ In route maintenance, if a node is continuously sending packets via a route, it has to make sure that the route is held upright. As soon as a node detects problems with the current route, it has to find an alternative.
- ✓ The above two mechanisms are based on demand. When compared to other protocols, DSR is independent of periodic update of routing table. It does not use any periodic routing advertisement, link status sensing, neighbor detection packets.

- ✓ DSR allows unidirectional links and asymmetric routes. A node can send the packets to other nodes while the opponent is free i.e. idle. It increases the overall performance and network connectivity.
- ✓ DSRalsoactsasaninterfacebetweendifferent typesofwirelessnetworks.
    - **DSR route discovery:**

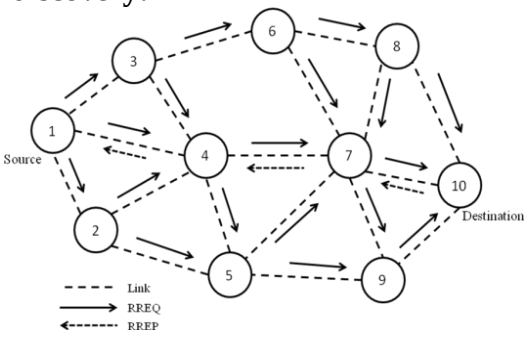


Figure1 Anexample forDSRroute discovery

- Routediscoveryis themechanismbywhich anodewishingtosenda packetto a destination node obtains a source route.
- A route is discovered only when a node sendsa packet to the other node.Route discovery takes place while a node that wants to send a packet first establishes a route by sending ROUTE REQUEST message to all the other nodes available in the network.
- If the request has reached the target node, the ROUTE REPLY message is beingtransferred to the initiator node. Otherwise, if the target node has already received this ROUTE REQUEST message, thenit drops the request, or elsethenodes append theirownaddress to alist oftraversed hops in thepacket and broadcast this updated route request.
- The address of the intermediate node is maintained in the ROUTE REQUEST message for future use.
- The copy of the original packet is saved in the local buffer called send buffer by the sending nodes.
- To reduce the overhead, once a node discovers a route, it can send various packets to the same target node.
- Additionalroutediscoveryfeatures:
    - Cachingoverhead,
    - Replyingtorouterequests usingcachedroutes,
    - Preventingroutereplystorms,
    - Routerequesthoplimits.
- **DSRroute maintainance:**

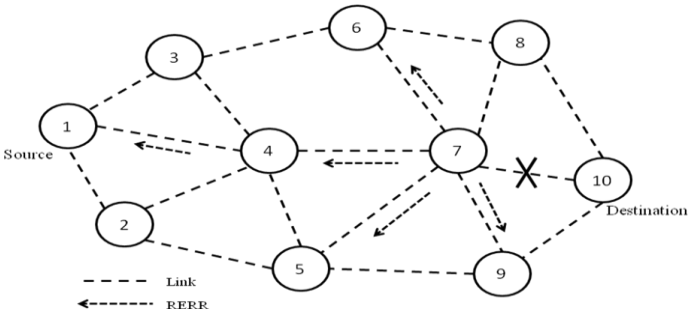
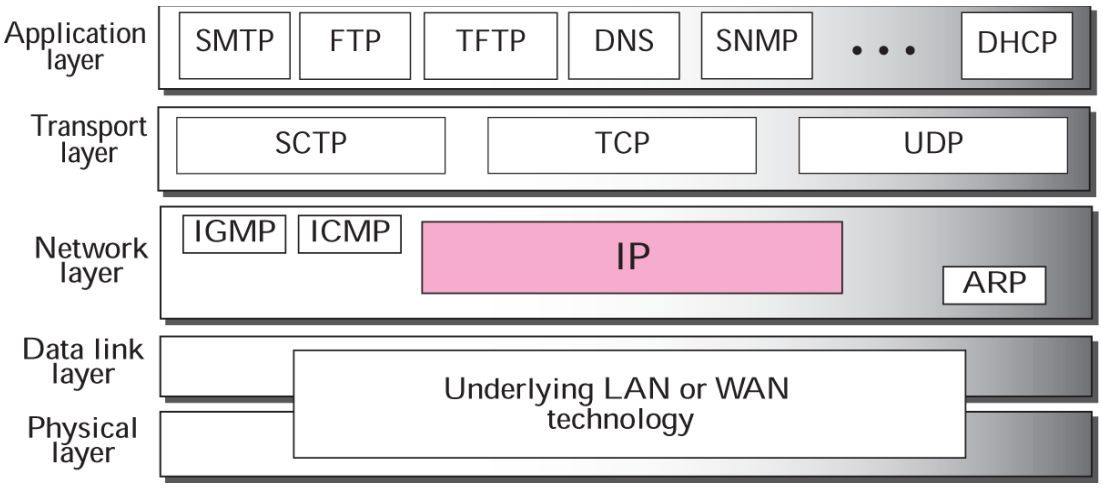


Figure2 AnexampleforDSRroute maintenance

- Afterthe discoveryofaroute, thereshould bemaintenanceofaroute.
- Routemaintenanceinvolvesthemaintenanceofarouteaslongasthenode sends packets along this route.
- Whenanodehasdiscovered aroute,apassiveacknowledgement isbeingsent.
- A ROUTE ERROR message is sent to the sender when the packet is retransmitted maximum number of times and no acknowledgement is being received.
- Figure 2 shows the link failure between node 7 and node 10. Hence the need for route maintenance.

Internet protocol version4(IPv4)

- ✓ The Internet Protocol (IP) is the transmission mechanism used by the TCP/IP protocols at the network layer.
- ✓ Figureshowsthepositionof IPin thesuite.

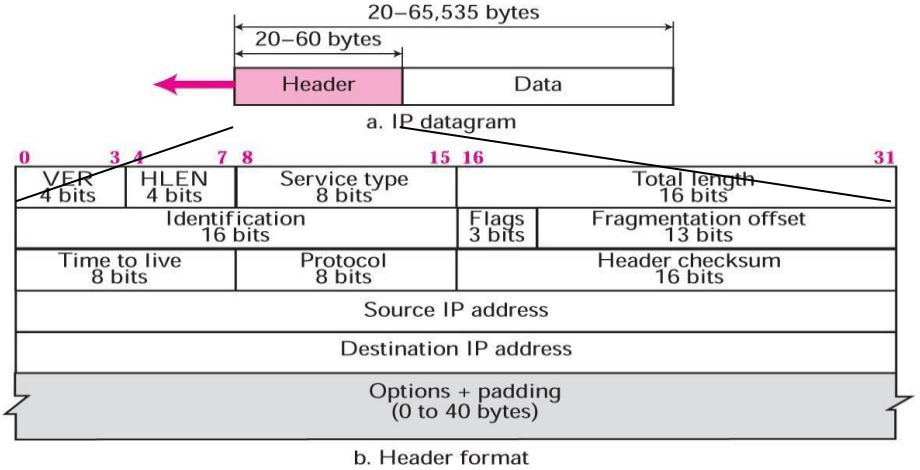


- ✓ IPisanunreliableand connectionlessdatagram protocol.
- ✓ It is a best-effort delivery service. The term best-effort means that IP packets can be corrupted, lost, arrive out of order, or delayed and may create congestion for the network.
- ✓ Ifreliabilityisimportant,IPmust bepairedwithareliableprotocolsuch asTCP.
- ✓ IP is also a connectionless protocol for a packet switching network that uses the datagram approach.

Datagrams

- ✓ Packetsinthenetwork(internet)layerarecalleddatagrams.
- ✓ Adatagram isavariable-lengthpacketconsistingoftwoparts:
  - Header-Itis20to60bytesinlengthandcontainsinformationessentialto routing and delivery.
  - Data–Payloaddata.

- ✓ FigureshowstheIPdatagram format.



- ✓ **Version(VER):**
  - This4-bitfielddefinestheversionoftheIPprotocol.Currentlytheversionis 4.This field tells theIPsoftware running in the processing machine that thedatagram has the format of version 4.

- ✓ **Headerlength(HLEN):**
  - This 4-bit field defines thetotal length ofthedatagram headerin 4-byte words. This field is needed because the length of the header is variable (between 20 and 60 bytes).
    - Whentherearenooptions,theheaderlength is20 bytes.
    - Whentheoptionfield isat itsmaximumsize60 bytes.
- ✓ **Servicetype:**
  - In the original design of IP header, this field was referred to as type of service (TOS)
  - TOS component is used to determine the type of service that must be provided by the Internet layer depending on the type of application for which the data transfer needs to be done.
  - Ithas8bitsfield.
    - The first three bits filed are known as precedence bits (ignored as today).
    - Thenext4bitsrepresenttypeof service
      - TOSare:
        - 0000 -Normal
        - 0001 -Minimizing Cost
        - 0010 -Maximizereliability.
        - 0100 -Maximizethroughput
        - 1000 -Minimize delay.
    - Lastbit isunused.
- ✓ **Totallength:**
  - This is a 16-bit field that defines the total length(header plus data) of the IPdatagram in bytes.
  - To find the length of the data coming from the upper layer, subtract the header length from the total length.

    Length ofdata=totallength-headerlength
  - The header length can be found bymultiplying the value in the HLEN field by four.

- ✓ **Identification:**
  - This 16-bit field identifies a datagram originating from the source host. The combination of the identification and source IP address must uniquelydefine a datagram as it leaves the source host.
  - Allfragments ofadatagramcontain thesameidentificationvalue.
  - This allowsthedestination host to determine which fragment belongs to which datagram.
- ✓ **Flags:**
  - Thisisathree-bit field.

    - Thefirstbit isreserved(notused).
    - Thesecondbit(D)is calledthe**donotfragmentbit.**
      - Ifitsvalueis1,themachinemust notfragmentthedatagram
      - Ifitsvalueis0,thedatagramcanbefragmentedif necessary.
    - Thethirdbit (M)iscalledthe**morefragment bit.**
      - If its value is 1, it means the datagram is not the last fragment; there are more fragments after this one.
      - If its valueis 0, itmeans this is thelastoronlyfragment.

- ✓ **Fragmentationoffset:**
  - This13-bitfieldshowstherelativepositionofthisfragmentwithrespecttothe whole datagram.
  - Itistheoffsetofthedata in theoriginaldatagrammeasuredinunits of8bytes.
- ✓ **Timeto live:**
  - Adatagram hasalimitedlifetimeinitstravelthroughaninternet.
  - This field was originallydesigned to hold atimestamp, which was decremented by each visited router.
  - Thedatagramwasdiscardedwhenthevaluebecamezero.
- ✓ **Protocol:**
  - This8-bitfielddefinesthehigher-levelprotocolthatusestheservicesofthe IP layer.
  - An IP datagram can encapsulate data from several higher level protocols such as TCP, UDP, ICMP, and IGMP.
  - ThisfieldspecifiesthefinaldestinationprotocoltowhichtheIPdatagram should be delivered.
  - Someofthevalueofthisfieldfordifferenthigher-level protocols

Value	*Protocol*	*Value*	*Protocol*
1	ICMP	17	UDP
2	IGMP	89	OSPF
6	TCP		

- ✓ **Checksum:**
  - Toprovidebasicprotectionagainstcorruptionintransmission.
  - Example – CRC

- ✓ **Sourceaddress:**
  - This 32-bit field defines the IP address of the source. This field must remain unchanged during the time the IP datagram travels from the source host to the destination host.
- ✓ **Destinationaddress:**
  - This 32-bit field defines the IP address of the destination. This field must remainunchangedduringthetimetheIPdatagramtravelsfromthesourcehost to the destination host.
- ✓ **Options:**
  - One or more several types of options may be included after thestandardheader in certain IP datagrams.
- ✓ **Padding:**
  - Thevariablepart comprises theoptions, which can be amaximum of40 bytes. Options, as the name implies, are not required for a datagram. They can be used for network testing and debugging.
- ✓ **Data:**
  - Thedatato betransmittedinthedatagram.

Internet protocol version6(IPv6)

IPv6- Introduction

- ✓ Severalreasons fortheneedofanewprotocol,InternetProtocol version6(IPv6).
  - Themainreasonwastheaddressdepletion.
  - Other reasons are related to the slowness of the process due to some unnecessaryprocessing, the need for new options, support for multimedia, and the desperate need for security.

ComparisonbetweenIPv4andIPv6Headers

IPv4	IPv6
Source and destination address are 32bits or 4Bytes Example: 192.168.0.1	Sourceanddestinationaddressare128bits or 16Bytes Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
Headercontainschecksum	Headerdoesnot containschecksum
Headercontainsoptions	All optional data in moved to IPv6 extension headers
Broadcastaddressesareusedtosend packets to all nodes on a subnet.	NoBroadcastaddresses,Insteadlinklocal scope all nodes multicast address is used.
ManualorDHCPbasedIPconfiguration.	Nodesarecapableofauto configuration.
Fragmentation is done by sending host and also router which slows down the process.	Fragmentation is done onlybythe sender of the packet.
IPSecheadersupportisoptional	IPSecheadersupportisrequired.
No identification of packet flow in IP header.	Flow label field is used to identify the packet flow and prioritized delivery

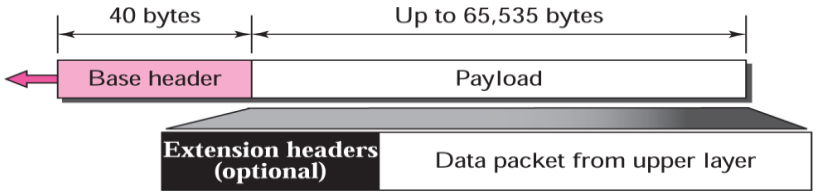
Advantages of IPv6

- ✓ **Larger address space:** An IPv6 address is 128 bits long. Compared with the 32-bit address of IPv4, this is a huge (296 times) increase in the address space.
- ✓ **Better header format:** IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the upper-layer data. This simplifies and speeds up the routing process because most ofthe options do not need to be checked by routers.
- ✓ **Newoptions:**IPv6hasnewoptionstoallowforadditional functionalities.
- ✓ **Allowance for extension:** IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.
- ✓ **Support for resource allocation:** In IPv6, the type-of-service field hasbeenremoved, but two new fields, traffic class and flow label have been added to enablethe source to request special handling of the packet. This mechanism can be used to support traffic such as real-time audio and video.
- ✓ **Support for more security:** The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

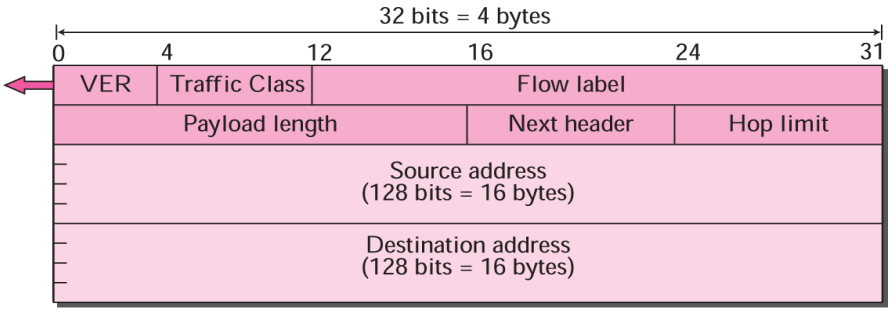
IPv6 Header

- ✓ TheIPv6packetisshowninbelow.Eachpacketiscomposedofamandatorybase header followed by the payload.
- ✓ Thepayload consistsoftwo parts:
  - optionalextensionheadersand
  - datafromanupper layer.
- ✓ The base header occupies 40 bytes, whereas the extension headers and data from the upper layer contain up to 65,535 bytes of information.

- ✓ IPv6datagram



- ✓ Formatofthebase header



  - Thesefieldsareasfollows:
    - **Version:** This 4-bit field defines the version number of the IP. For IPv6,the value is 6.

- **Traffic Class:** This 8-bit field is used to distinguish different payloadswith different delivery requirements. It replaces the service class field in IPv4.
- **Flow label:** The **flow label** is a 20-bit field that is designed to provide special handling for a particular flow of data.
- **Payload length:** The 2-byte payload length field defines the length of the IP datagram excluding the base header.
- **Next header:** The **next header** is an 8-bit field defining the header that follows the base header in the datagram. The next header is either one of the optional extension headers used by IP or the header of an encapsulated packet such as UDP or TCP.

Code	*Next Header*	*Code*	*Next Header*
0	Hop-by-hop option	44	Fragmentation
2	ICMP	50	Encrypted security payload
6	TCP	51	Authentication
17	UDP	59	Null (No next header)
43	Source routing	60	Destination option

- **Hop limit:** This 8-bit **hop limit** field serves the same purpose as the TTL field in IPv4.
- **Source address:** The source address field is a 16-byte (128-bit) Internet address that identifies the original source of the datagram.
- **Destination address:** The destination address field is a 16-byte (128-bit) Internetaddressthatusuallyidentifiesthefinaldestinationofthedatagram. However, if source routing is used, this field contains the address of the next router.

✓ **FlowLabel:**

- In version 6, the flow label has been directly added to the format of the IPv6 datagram to allow us to use IPv6 as as connection-oriented protocol.
- To a router, a flow is a sequence of packets that share the same characteristics, such as traveling the same path, using the same resources, having the same kind of security, and so on. A router that supports the handling of flow labels has a flow label table.
- The table has an entry for each active flow label; each entry defines the services required by the corresponding flow label. When therouter receives a packet, it consults its flow. It then provides the packet with the services mentioned in the entry.

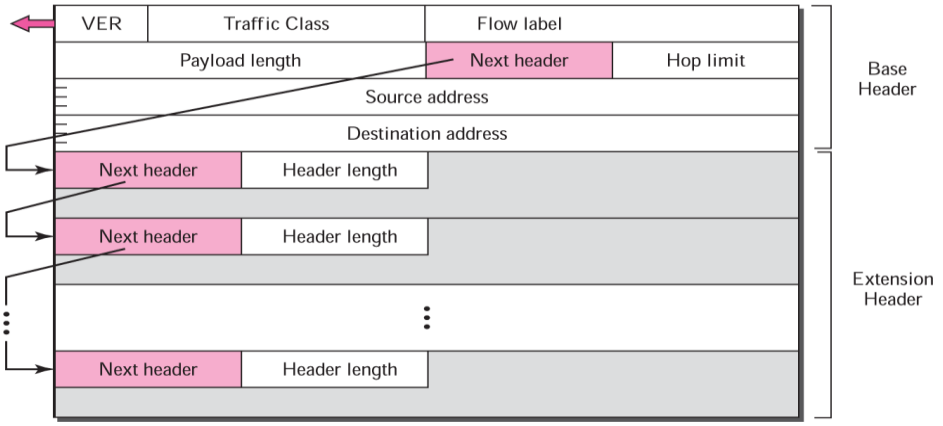
- In its simplest form, a flow label can be used to speed up the processing of a packet bya router. When a router receives a packet, instead of consulting the routing table and going through a routing algorithm to define the address of the next hop, it can easily look in a flow label table for the next hop label table to find the corresponding entry for the flow label value defined in the packet. It then provides the packet with the services mentioned in the entry.
- In its more sophisticated form, a flow label can be used to support the transmission of real-time audio and video. Real-time audio or video,

particularly in digital form, requires resources such as high bandwidth, large buffers, long processing time, and so on.

- The use of real-time data and the reservation of these resources require other protocols such as Real-Time Protocol (RTP) and Resource Reservation Protocol (RSVP) in addition to IPv6.
- Toallowtheeffectiveuseofflowlabels,threeruleshavebeendefined:
  1. The flow label is assigned to a packet by the source host. The label is a random number between 1 and 2^{24}– 1. A source must not reuse a flow label for a new flow while the existing flow is still alive.
  2. If a host does not support the flow label, it sets this field to zero. If a router does not support the flow label, it simply ignores it.
  3. All packets belonging to the same flow have the same source, same destination, same priority, and same options.

IPv6 extension headers

- ✓ Thelengthofthebaseheaderis fixedat40bytes. However,togivemorefunctionality to the IP datagram, the base header can be followed by up to six extension headers. Manyof these headers are options in IPv4. Figure shows the extension header format.



- ✓ Six types of extension headers have been defined. These are **hop-by-hop option, source routing, fragmentation, authentication, encrypted security payload, and destination option.**

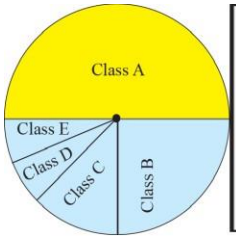
IP ADDRESS

- ✓ An IPv4addressis32bitslong.
- ✓ TheIPv4addressesareuniqueanduniversal.
- ✓ AddressSpace:Theaddressspaceof IPv4is 232or4,294,967,296.
- ✓ Notation:
  - Binary notation (base 2) – In binary notation, an IPv4 address is displayed as 32 bits. To make the address more readable, one or more spaces is usually inserted between each octet (8 bits). Each octet is often referred to as a byte.
    - 01110101 10010101 00011101 11101010
  - Dotted-decimal notation (base 256)- IPv4 address is usually written in decimal form with a decimal point (dot) separating the bytes.
    - 192.168.10.1

- Hexadecimalnotation(base16)-Eachhexadecimaldigitisequivalenttofourbits. This means that a 32-bit address has 8 hexadecimal digits.
  - 0X810B0BEF

CLASSFUL ADDRESSES

- ✓ IP addresses, when started a few decadesago, used the concept of classes. Thisarchitecture is called Classful addressing.
- ✓ Inthemid-1990s,anewarchitecture,calledclasslessaddressing,wasintroducedthat supersedes the original architecture.
- ✓ Classes:
  - In Classful addressing, the IP address space is divided into five classes: A, B, C,D, and E. Each class occupies some part of the whole address space.



Class A: $2^{31} = 2{,}147{,}483{,}648$ addresses, 50%
Class B: $2^{30} = 1{,}073{,}741{,}824$ addresses, 25%
Class C: $2^{29} = 536{,}870{,}912$ addresses, 12.5%
Class D: $2^{28} = 268{,}435{,}456$ addresses, 6.25%
Class E: $2^{28} = 268{,}435{,}456$ addresses, 6.25%

- ✓ Findingtheclassofaddress
  - Find the class of an address when the address is given either in binary or dotted-decimal notation.
  - Inthebinary notation,thefirstfewbitscanimmediately tellustheclassofthe address.
  - In the dotted-decimal notation, the value of the first byte can give the class of anaddress.

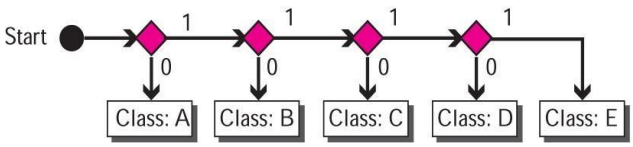
	Octet 1	Octet 2	Octet 3	Octet 4
Class A	0.....			
Class B	10.....			
Class C	110.....			
Class D	1110....			
Class E	1111....			

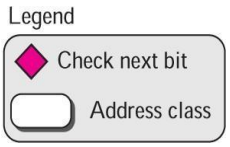
Binary notation

	Byte 1	Byte 2	Byte 3	Byte 4
Class A	0–127			
Class B	128–191			
Class C	192–223			
Class D	224–299			
Class E	240–255			

Dotted-decimal notation

- ✓ Findingtheclassofanaddressusingcontinuous checking





Example

1. Findtheclass of each address:

a) 00000001 0000101100001011 11101111
b) 11000001 10000011 00011011 11111111
c) 10100111 11011011100010110110111 1
d) 11110011 10011011 11111011 00001111

Solution:

a) Thefirstbit is0. Thisisa class A address.
b) Thefirst2 bitsare1;thethirdbitis 0.Thisis aclassC address.

c) **Thefirstbitis1;thesecondbit is0.Thisis aclassB address.**
d) **Thefirst4 bits are1s. Thisis aclass E address.**

2. Findtheclassof eachaddress:

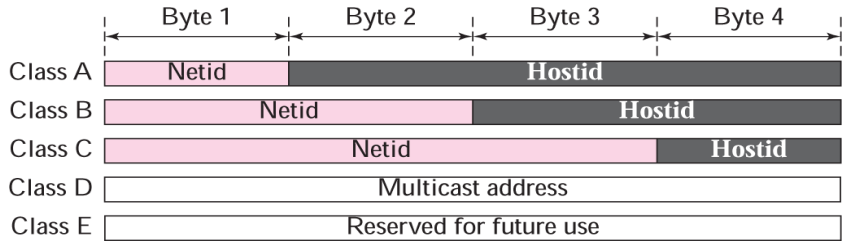
e) **227.12.14.87**
f) **193.14.56.22**
g) **14.23.120.8**
h) **252.5.15.111**

Solution:

e) **Thefirstbyteis 227(between224 and239);theclassisD.**
f) **Thefirstbyteis 193(between192and 223);theclassisC.**
g) **Thefirstbyteis14(between0 and127);theclass is A.**
h) **Thefirstbyteis252(between 240and255);theclass is E.**

✓ NetidandHostid

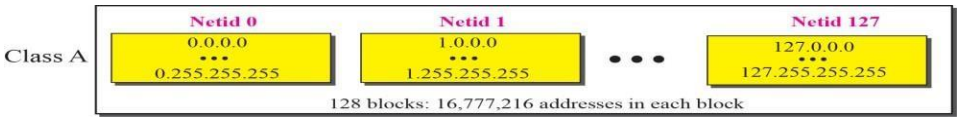
- In classful addressing, an IP address in classes A, B, and C is divided into netid and hostid. These parts are of varying lengths, depending on the class of the address. Figure shows the netid and hostid bytes.
- Classes Dand Earenotdividedinto netidand hostid.



- In classA,1bytedefinesthenetidand3bytesdefinethe hostid.
- InclassB,2bytesdefinethenetidand2bytesdefinethe hostid.
- InclassC,3bytesdefinethenetidand1bytedefinesthe hostid.

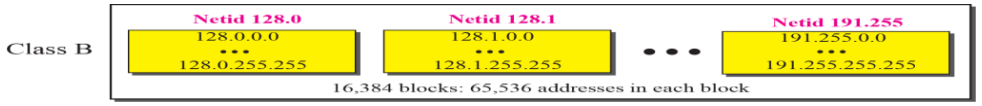
✓ Classes and Blocks

- Each class is divided into afixed numberofblocks with each block having afixed size.
- **Class A:**
  - Only 1 byte in class A defines the netid and theleftmost bit should be 0,the next 7 bits can be changed to find the number of blocks in this class.
  - Therefore, class A is divided into 2^7 = 128 blocks that can be assigned to 128 organizations.
  - Eachblockinthis classcontains16,777,216addresses.
  - Manyaddresses arewasted in this class.

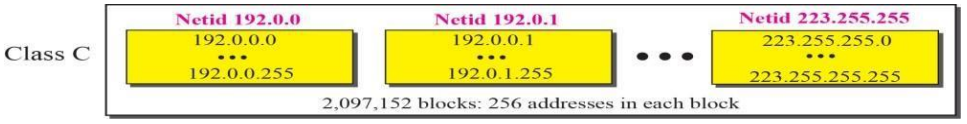


- **Class B:**
  - Two bytesinclassB definesthe netidand theleftmostbitshould be 10, the next 14 bits can be changed to find the number of blocks in this class.

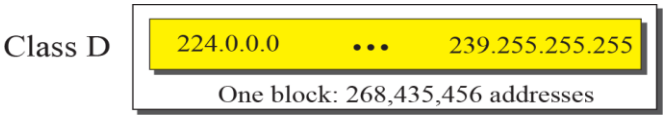
- Therefore, class B is divided into 2^14 = 16,384 blocks that can be assigned to 16,384 organizations.
- Eachblockinthisclasscontains65,536addresses.
- Manyaddresses arewasted in this class



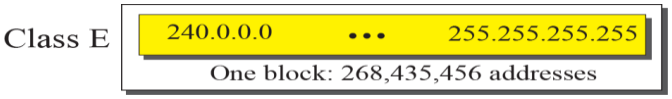
- **Class C**
  - Three bytes in class C defines the netid and the leftmost bit should be 110, the next 21 bits can be changed to find the number of blocks in this class.
  - Therefore,classBisdividedinto2^21=2,097,152blocksthatcanbe assigned to 2,097,152 organizations.
  - Eachblockinthisclasscontains256addresses.



- **Class D**
  - Oneblockofclass D addresses.
  - Itisdesignedformulticasting.
  - Each address in this class is used to define one group of hosts on the Internet.
  - When a group is assigned an address in this class, every host that is a member of this group will have a multicast address in addition to itsnormal (unicast) address.



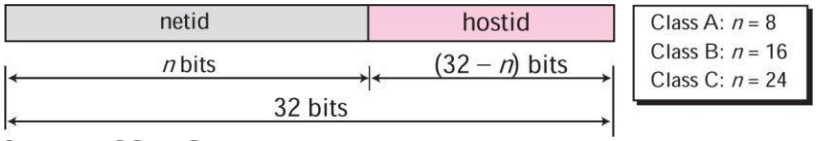
- **Class E**
  - Oneblockofclass E addresses.
  - Itwasdesignedforuseasreservedaddresses,



✓ Two-Level Addressing

- ThewholepurposeofIPv4addressingistodefineadestinationforanInternet packet.
- When classful addressing was designed, it was assumed that the whole Internet is divided into many networks and each network connects many hosts.
- Anetworkwasnormallycreated byanorganizationthatwantedtobeconnectedto the Internet.
- The Internet authorities allocated a block of addresses to the organization (in class A, B, or C).
- Eachaddress inclassfuladdressingcontainstwoparts: netidandhostid.

- Thenetiddefinesthe network;
- Thehostiddefines aparticularhostconnectedtothat network.

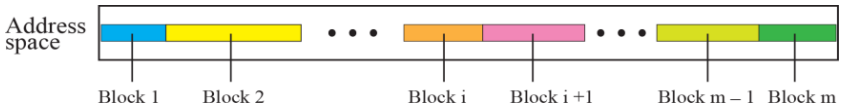


CLASSLESS ADDRESSING

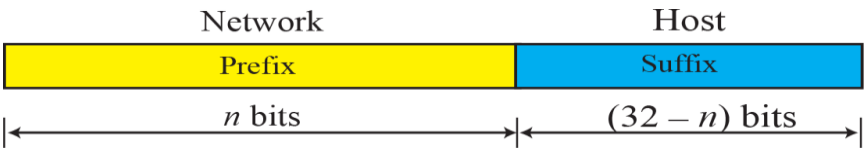
✓ Subnetting and supernetting in classful addressing did not really solve the address depletion problem. With thegrowth ofthe Internet, it was clear that alargeraddress space was needed as a long-term solution. Although the long-range solution has already been devised and is called IPv6, a short-term solution was also devised to use the same address space but to change the distribution of addresses to provide a fair share to each organization. The short-term solution still uses IPv4 addresses, but it is called classless addressing.

✓ Variable-LengthBlocks
- Inclasslessaddressing,thewholeaddressspaceisdividedintovariablelength blocks.

✓ NumberofAddresses inaBlock
- Thereisonlyoneconditiononthenumberofaddressesinablock;itmust bea power of 2 (2, 4, 8, . . .).
  - Ahousehold maybegivenablock of2 addresses.
  - Asmall businessmaybe given 16 addresses.
  - Alargeorganizationmaybegiven 1024addresses.

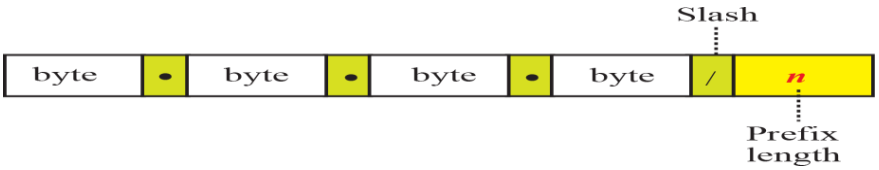


✓ Two-LevelAddressing
- Inclassfuladdressing,two-leveladdressingwasprovidedbydividinganaddress into *netid and hostid.*
  - Thenetiddefinedthenetwork
  - Thehostid definedthehost in the network.
- Inclasslessaddressing,theblockisactuallydividedintotwoparts,theprefixand the suffix.
  - Theprefixplaysthesameroleasthenetid
  - Thesuffixplaysthesameroleasthe hostid.
- Alladdressesintheblockhavethesameprefix;eachaddresshasadifferent suffix.



- Theprefixlengthinclasslessaddressingcanbe1to 32.

- ✓ **Slashnotation**
  - Inclasslessaddressing,weneedtoincludetheprefixlengthtoeachaddressifwe need to find the block of the address.
  - Inthiscase,theprefixlength,n,isadded totheaddressseparatedbyaslash.The notation is informally referred to as slash notation.
  - Theslashnotationisformallyreferredtoasclasslessinterdomainroutingor CIDR notation.



- ✓ **Example**

1.Asmallorganizationisgivenablockwiththebeginningaddressandtheprefix length 205.16.37.24/29 (in slash notation). What is the range of the block?

Solution

Thebeginningaddressis205.16.37.24.Tofindthelastaddresswekeepthefirst29 bits and change the last 3 bits to 1s.

Beginning:11001111000100000010010100011000

Ending :11001111000100000010010100011111

There areonly8addresses in this block.

IPv6 addressing format

- ✓ An IPv6 address is made of 128 bits divided into eight 16-bits blocks. Each block isthen converted into 4-digit Hexadecimal numbers separated by colon symbols.
- ✓ For example, given below is a 128 bit IPv6 address represented in binary format and divided into eight 16-bits blocks:

0010000000000001000000000000000011001000111000110111111110000100000000011000110000000000000000000000000000000001111111011111011

- ✓ EachblockisthenconvertedintoHexadecimal andseparatedby‘:’symbol:

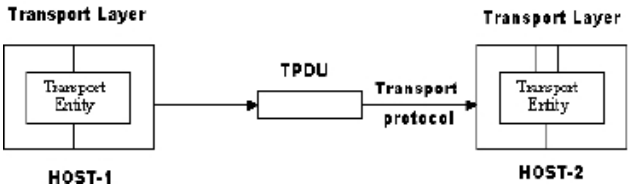
2001:0000:3238:DFE1:0063:0000:0000:FEFB

- ✓ Even after converting into Hexadecimal format, IPv6 address remains long. IPv6 provides some rules to shorten the address. The rules are as follows:
  - Rule.1:Discardleading Zero(es):
    - In Block 6, 0036, the leading two 0s can be omitted, such as (6th block):
    - 2001:0000:3238:DFE1:1263:36:0000:FEFB
  - Rule.2: If two of more blocks contain consecutive zeroes, omit them all and replace with double colon sign ::, such as (6th and 7th block):
    - 2001:0000:3238:DFE1:1263::FEFB
  - Consecutive blocks of zeroes can be replaced only once by :: so if there arestill blocks of zeroes in the address, they can be shrunk down to a single zero, such as (2nd block):
    - 2001:0:3238:DFE1:1263::FEFB

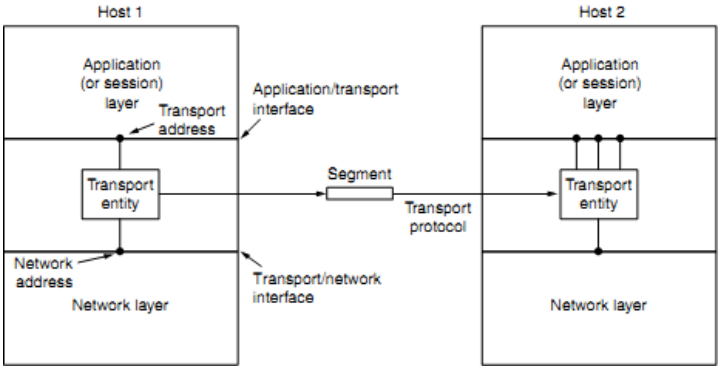
UNIT-IV
THE TRANSPORT LAYER

Overview of Transport layer

- ✓ The network layer provides end-to-end packet delivery using data-grams or virtual circuits. The transport layer builds on the network layer to provide data transport from a process on a source machine to a process on a destination machine with a desired level of reliability that is independent of the physical networks currently in use. It provides the abstractions that applications need to use the network.
- ✓ Transport Entity: The hardware and/or software which make use of services provided bythe network layer, (within the transport layer) is called transport entity.
- ✓ TransportServiceProvider: Layers1to4arecalledTransportService Provider.
- ✓ TransportServiceUser:Theupperlayersi.e.,layers5to7arecalledTransport Service User.
- ✓ Transport Service Primitives: Which allow transport users (application programs) to access the transport service?
- ✓ TPDU(TransportProtocol Data Unit):
  - Transmissions ofmessage between 2 transport entities arecarried out by TPDU.
  - The transport entity carries out the transport service primitives byblocking the caller and sending a packet the service.
  - Encapsulated in the payload of this packet is a transport layer message for the server's transport entity.
  - The task of the transport layer is to provide reliable, cost-effective data transport from the source machine to the destination machine, independent of physical network or networks currently in use.



- ✓ **Services Provided to the Upper Layers**
  - The ultimate goal of the transport layer is to provide efficient, reliable, and cost-effective data transmission service to its users, normally processes in the application layer. To achieve this, the transport layer makes use of the services provided by the network layer.
  - The software and/or hardware within the transport layer that does the work is called the transport entity.
  - The transport entity can be located in the operating system kernel, in a library package bound into network applications, in a separate user process, oreven on the network interface card.



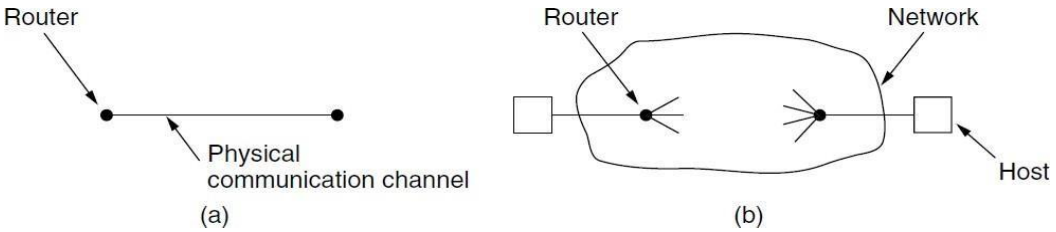
- ✓ Therearetwotypesofnetworkservice
  - Connection-oriented
  - Connectionless
- ✓ Similarly, there are also two types of transport service. The connection-oriented transportserviceissimilartotheconnection-orientednetworkserviceinmanyways.
- ✓ Inbothcases,connectionshavethreephases:
  - Establishment
  - Datatransfer
  - Release.
- ✓ Addressing and flow control are also similar in both layers. Furthermore, the connectionless transport service is also very similar to the connectionless network service.
- ✓ The bottom four layers can be seen as the transport service provider,whereas the upper layer(s) are the transport service user.

- ✓ **Transport Service Primitives**
  - To allow users to access the transport service, the transport layer must provide some operations to application programs, that is, a transport service interface. Each transport service has its own interface.
  - The transport service is similar to the network service, but there are also some important differences.
  - The main difference is that the network service is intended to modeltheservice offered by real networks. Real networks can lose packets, so the network service is generally unreliable.
  - The(connection-oriented)transportservice,incontrast, isreliable

Primitive	Packet sent	Meaning
LISTEN	(none)	Block until some process tries to connect
CONNECT	CONNECTION REQ.	Actively attempt to establish a connection
SEND	DATA	Send information
RECEIVE	(none)	Block until a DATA packet arrives
DISCONNECT	DISCONNECTION REQ.	This side wants to release the connection

Elements of transport protocols

- ✓ Thetransportserviceisimplementedby atransportprotocolusedbetweenthetwo transport entities.
- ✓ Thetransportprotocolsresemblethedatalink protocols.
- ✓ Bothhavetodeal witherrorcontrol, sequencing,andflow control.
- ✓ Thedifferencetransport protocol and data link protocol depends uponthe environment in which they are operated.
- ✓ These differences are due to major dissimilarities between the environments in which the two protocols operate, as shown in Fig.

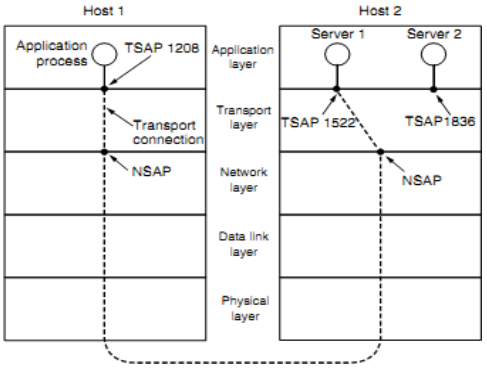


(a)Environment ofthedata link layer (b)Environmentof thetransport layer

- ✓ **DifferentiatebetweenDatalinkLayerandTransportLayerprotocols**

	DataLink Layer	TransportLayer
Communication	directlyviaphysical channel	overtheentirenetwork
Addressing	noneedtospecifyaddress.Just select outgoing line	explicit addressing of destinationisrequired
Connection establishment	overawireis simple	morecomplicated
Delay	frameeitherarrivesorlost,not stored and delayed	packetsmightbestoredfor secondsanddeliveredlater
Bufferingand flow control	simpler	morecomplicated;largeand dynamic number of simultaneous connections

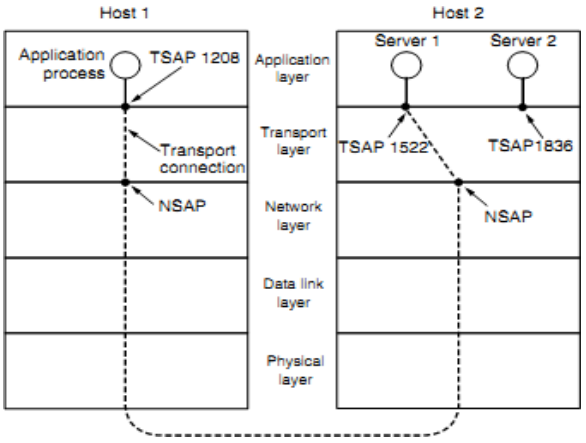
- ✓ The transport service is implemented by a transport protocol between the 2 transport entities.



- ✓ **The elements of transport protocols are:**
  - Addressing
  - ConnectionEstablishment
  - ConnectionRelease
  - FlowControlandBuffering
  - Multiplexing

- ✓ **Addressing**
  - When an application (e.g., a user) process wishes to set up a connection to a remote application process, it must specify which one to connect to.
  - The method normally used is to define transport addresses to which processes can listen for connection requests. In the Internet, these endpoints are called ports.
  - Therearetwotypesofaccess points:
    - TSAP (Transport Service Access Point) to mean a specific endpoint in the transport layer.
    - The analogous endpoints in the network layer (i.e., network layer addresses) are not surprisingly called NSAPs (Network Service Access Points). IP addresses are examples of NSAPs.

- ✓ Example
  - Application processes, both clients and servers, can attach themselves toa localTSAPtoestablishaconnectionto aremoteTSAP.These connectionsrun through NSAPs on each host. The purpose of having TSAPs is that in some networks, each computer has a single NSAP, so some way is needed to distinguish multiple transport endpoints that share that NSAP.

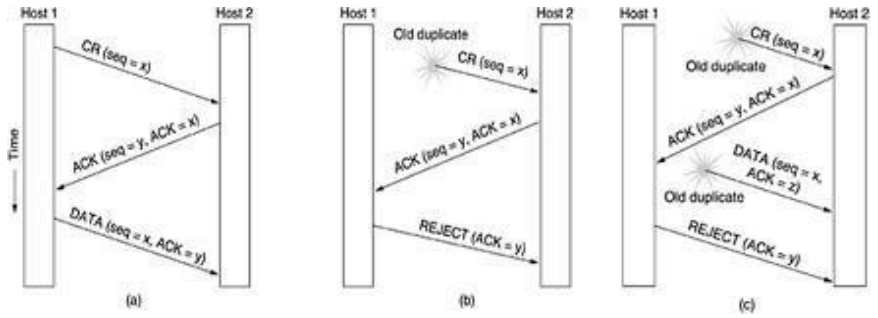


- ✓ Apossiblescenariofora transportconnectionis as follows:
  1. A mail server process attaches itself to TSAP 1522 on host 2 to wait for an incoming call. How a process attaches itself to a TSAP is outside the networking model and depends entirely on the local operating system. A call such as our LISTEN might be used, for example.
  2. An application process on host 1 wants to send an email message, so it attaches itself to TSAP 1208 and issues a CONNECT request. The request specifies TSAP 1208 on host 1 as the source and TSAP 1522 on host 2 as the destination. This action ultimately results in a transport connection being established between the application process and the server.

3. Theapplication processsendsoverthemail message.
4. Themailserverrespondsto saythat itwilldeliver themessage.
5. Thetransportconnectionisreleased.

✓ **Connection Establishment**

- With packet lifetimes bounded, it is possible to devise a fool proof way to establish connections safely. Packet lifetime can be bounded to a known maximum using one of the following techniques:
  - Restrictedsubnetdesign
  - Puttingahop counterineach packet
  - Timestampingineach packet
- Usinga3-wayhandshake,aconnectioncanbeestablished.Thisestablishment protocol doesn't require both sides to begin sending with the same sequence number.
  - The first technique includes any method that prevents packets from looping, combined with some way of bounding delay including congestion over the longest possible path. It is difficult, given that internets may range from a single city to international in scope.
  - Thesecondmethodconsistsofhavingthehopcountinitializedtosome appropriate value and decremented each time the packet is forwarded. The network protocol simply discards any packet whose hop counter becomes zero.
  - The third method requires each packet to bear the time it was created, with the routers agreeing to discard anypacket older than some agreed-upon time.

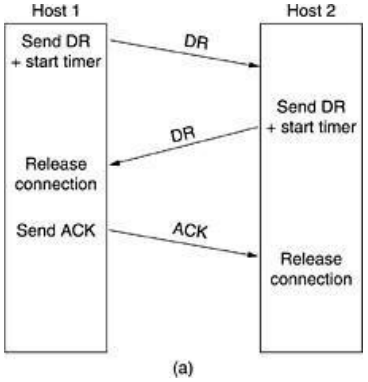


- The above Figure shows the three protocol scenarios for establishing a connection using a three-way handshake. CR denotes CONNEC TION REQUEST (a) Normal operation (b) Old duplicate CONNECTION REQUEST appearing out of nowhere (c) Duplicate CONNECTION REQUEST and duplicate ACK
- Infig(a)Tomlinson (1975)introducedthethree-wayhandshake.
  - This establishment protocol involves one peerchecking with the other that the connection request is indeed current. Host 1 chooses a sequence number, x , and sends a CONNECTION REQUEST segment containing it to host 2. Host 2replies with an ACK segment acknowledging x and announcing its own initial sequence number, y.
  - Finally, host 1 acknowledges host 2's choice of an initial sequence number in the first data segment that it sends.

- In fig (b) the first segment is a delayed duplicate CONNECTION REQUEST from an old connection.
  - Thissegmentarrivesathost2withouthost1'sknowledge.Host 2 reacts to this segment by sending host1an ACK segment, in effect asking forverification that host 1 was indeed tryingto set up a new connection.
  - When host 1 rejects host 2's attempt to establish a connection, host 2 realizes that it was tricked by a delayed duplicate and abandons the connection. In this way, a delayed duplicate does no damage.
  - The worst case is when both a delayed CONNECTION REQUEST and an ACK are floating around in the subnet.
- In fig (c) previous example, host 2 gets a delayed CONNECTION REQUEST and replies to it.
  - At this point, it is crucial to realize that host 2 has proposed using y as the initial sequence number for host 2 to host 1 traffic, knowing full well that no segments containing sequence number y or acknowledgements to y are still in existence.
  - Whentheseconddelayedsegmentarrivesathost2,thefactthat z has been acknowledged ratherthan ytells host 2 that this, too, is an old duplicate.
  - The important thing to realize here is that there is no combination of old segments that can cause the protocol to fail and have a connection set up byaccident when no one wants it.

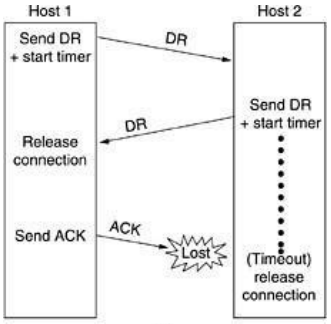
✓ **Connection Release**

- A connection is released using either asymmetric orsymmetric variant. But, the improved protocol for releasing a connection is a 3-way handshake protocol.
- Therearetwo stylesofterminatingaconnection:
  - Asymmetricrelease
    - Asymmetric release is the way the telephone system works: when one party hangs up, the connection is broken.
  - Symmetricrelease
    - Symmetric release treats the connection as two separate unidirectional connections and requires each one to be released separately.
- ConnectionReleasescenariousingthree handshake



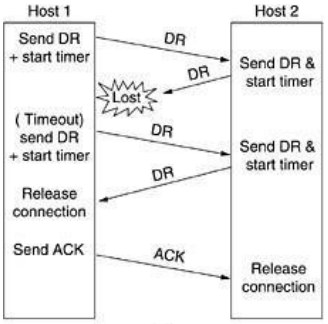
(a)

- OneoftheuserssendsaDISCONNECTIONREQUESTTPDUin order to initiate connection release.
- When it arrives, the recipient sends back a DR-TPDU, too, and starts a timer.
- When this DR arrives, the original sender sends back an ACK-TPDU and releases the connection.
- Finally,whentheACK-TPDUarrives,thereceiveralsoreleasesthe connection.



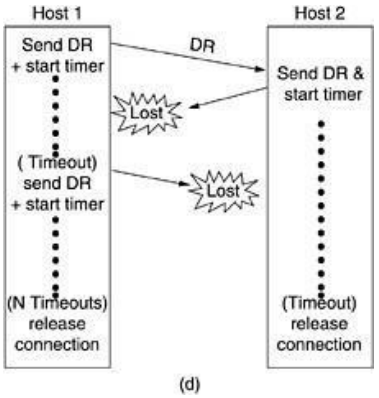
(b)

- Initialprocessis doneinthe samewayasin fig-(a).
- IfthefinalACK-TPDUislost,thesituationissavedbythetimer. When the timer is expired, the connection is released.



(c)

- If the second DR is lost, the user initiating the disconnection will not receive the expected response, and will timeout and starts all overagain.

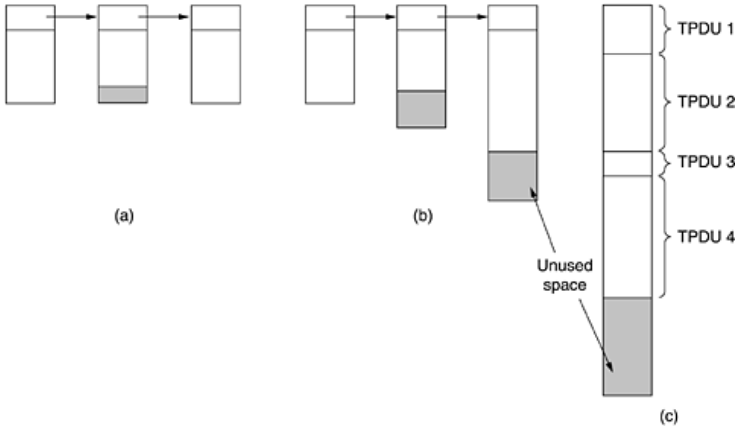


(d)

- Same as in fig(c) except that all repeated attempts to retransmit the DR is assumed to be failed due to lost TPDUs. After 'N' entries, the sender just gives up and releases the connection.

✓ **Flow Control and Buffering**

- Flow control is donebyhaving aslidingwindow on each connection to keep a fast transmitter from over running a slow receiver.
- Bufferingmust bedonebythe sender,ifthe networkserviceis unreliable.
- The sender buffers all the TPDUs sent to the receiver. The buffer size variesfor different TPDUs.
- Theyare:



- a)ChainedFixed-sizeBuffers
  - If most TPDUs are nearly the same size, the buffers are organized as a pool of identical size buffers, withone TPDUper buffer.

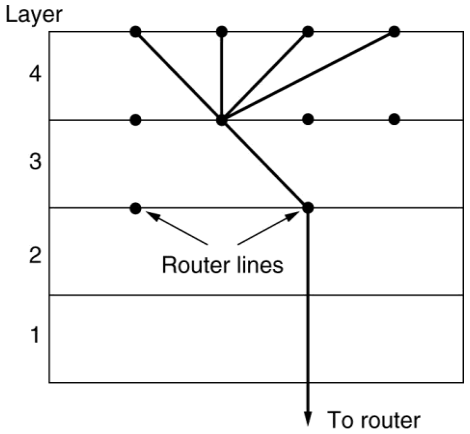
- b)ChainedVariable-size Buffers
  - This is an approach to the buffer-size problem. i.e., if there is wide variation in TPDU size, from a few characters typed at a terminal to thousands of characters from file transfers, some problems may occur:
  - If the buffer size is chosen equal to the largest possible TPDU, space will be wasted whenever a short TPDU arrives.
  - If the buffer size is chosen less than the maximum TPDU size, multiple buffers will be needed for long TPDUs.
  - Toovercome theseproblems, weemployvariable-sizebuffers.

- c)OnelargeCircularBufferperConnection
  - A single large circular buffer per connection is dedicated when all connections are heavily loaded.
    - 1. Source Buffering is used for low band width burstytraffic
    - 2.DestinationBufferingisusedforhighbandwidth smooth traffic.
    - 3. Dynamic Buffering is used if the traffic pattern changes randomly.

✓ **Multiplexing**

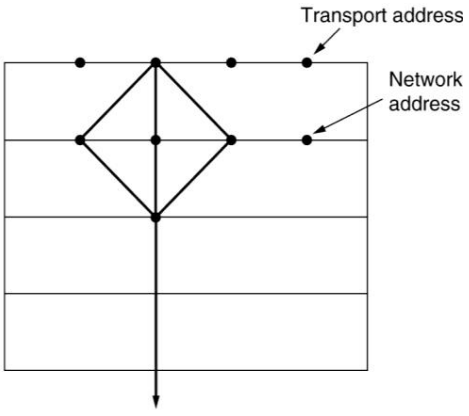
- In networks that use virtual circuits within the subnet, each open connection consumes some table space in the routers for the entire duration of the connection.

- If buffers are dedicated to the virtual circuit in each router as well, a user who left a terminal logged into a remote machine, there is need for multiplexing.
- Thereare2kinds ofmultiplexing:
  - (a)Upwardmultiplexing
    - In the below figure, all the 4 distinct transport connections use the same network connection to the remote host. When connect time forms the major component of the carrier's bill, it is up to the transport layer to group port connections according to their destination and maps each group onto the minimum number of port connections.



(a)

  - (b)Downwardmultiplexing
    - If too many transport connections are mapped onto the one network connection, the performance will be poor.
    - If too few transport connections are mapped onto one network connection, the service will be expensive.
    - The possible solution is to have the transport layeropen multiple connections and distribute the traffic among them on round-robin basis, as indicated in the below figure:
    - With 'k' network connections open, the effective bandwidth is increased by a factor of 'k'.

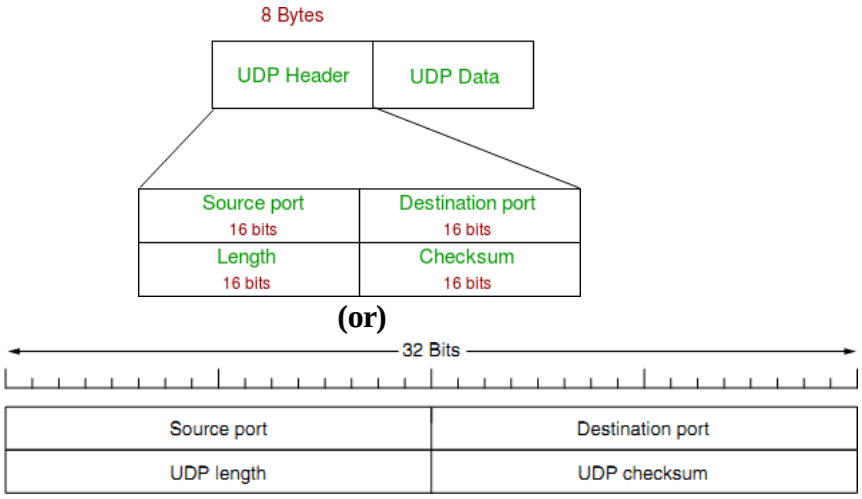


(b)

The internet transport protocols:UDP

- ✓ UserDatagramProtocol(UDP)isaTransport Layerprotocol.
- ✓ UDPisapartofInternetProtocolsuite,referred asUDP/IP suite.
- ✓ It is unreliable and connectionless protocol. So, there is no need toestablish connection prior to data transfer.
- ✓ The Internet protocol suite supports a connectionless transport protocol called UDP (User Datagram Protocol). UDP provides a way for applications to send encapsulated IP datagrams without having to establish a connection.
- ✓ UDP transmits segments consisting of an 8-byte header followed bythe pay-load. The two ports serve to identify the end-points within the source and destination machines.
- ✓ When a UDP packet arrives, its payload is handed to the process attached to the destination port. This attachment occurs when the BIND primitive. Without the port fields, the transport layer would not know whatto do with each incoming packet.With them, it delivers the embedded segment to the correct application.

- ✓ **UDP Header:**
  - ✓ UDP header is 8-bytesfixed and simple header,while for TCP it may vary from 20 bytes to 60 bytes.
  - ✓ First8Bytescontainsallnecessaryheaderinformationandremainingpartconsists of data.
  - ✓ UDPportnumber fieldsare each16bitslong,therefore range for portnumbers defined from 0 to 65535; port number 0 is reserved.
  - ✓ Portnumbershelptodistinguishdifferentuserrequests or process.



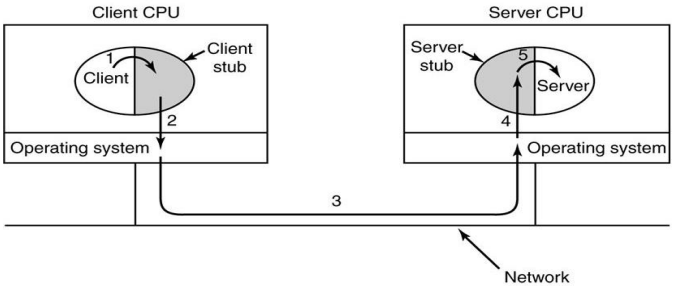
- **Source Port:** Source Port is 2 Byte long field used to identify port number of source.
- **Destination Port:** It is 2 Byte long field, used to identify the port of destined packet.
- **Length:** Length is the length of UDP including header and the data. It is 16-bits field.
- **Checksum:** Checksum is 2 Bytes long field. It is the 16-bit one's complement of the one's complement sum of the UDP header, pseudo headerof information from the IP header and thedata,padded with zerooctets at theend (if necessary) to make a multiple of two octets.

✓ **Applications of UDP:**

- Used for simple request response communication when size of data is less and hence there is lesser concern about flow and error control.
- ItissuitableprotocolformulticastingasUDPsupportspacketswitching.
- UDP is used for some routing update protocols like RIP (Routing Information Protocol).
- Normallyused for real time applications which can not tolerate uneven delays between sections of a received message
  - FollowingimplementationsusesUDPasatransportlayer protocol:
  - NTP(NetworkTimeProtocol)
  - DNS(DomainName Service)
  - BOOTP,DHCP.
  - NNP(NetworkNews Protocol)
  - Quoteof the dayprotocol
  - TFTP,RTSP,RIP,OSPF.
- Application layercandosomeofthetasksthrough UDP-
  - TraceRoute
  - RecordRoute
  - Time stamp

✓ Remote Procedure Call(RPC)

- In a certain sense, sending a message to a remote host and getting a reply back is like making a function call in a programming language. This is to arrange request-reply interactions on networks to be cast in the form of procedurecalls.
- For example, just imagine a procedure named get IP address (host name) that works by sending a UDP packet to a DNS server and waiting the reply, timing out and trying again if one is not forthcoming quickly enough. In this way, all the details of networking can be hidden from the programmer.
- RPC isusedto call remoteprograms usingtheprocedural call. When aprocess on machine 1 calls a procedure on machine 2, the calling process on 1 is suspended and execution of the called procedure takes place on 2.
- Information can be transported from the caller to the callee in the parameters and can come back in the procedure result. No message passing is visible tothe application programmer. This technique is known as RPC (Remote Procedure Call) and has become the basis for many networking applications.
- Traditionally, the calling procedure is known as the client and the called procedure is known as the server.
- In the simplest form, to call a remote procedure, the client program must be bound with a small library procedure, called the client stub that represents the server procedure in the client's address space. Similarly, the server is bound with a procedure called the server stub.
- These procedures hide the fact that the procedure call from the client to the server is not local.



- Step1: is theclient callingtheclient stub. This call is alocal procedure call, with the parameters pushed onto the stack in the normal way.
- Step 2: is the client stub packing the parameters into a message and making a system call to send the message. Packing the parameters is called marshaling.
- Step 3: is the operating system sending the message from the client machine to the server machine.
- Step 4: is the operating system passing the incoming packet to the server stub.
- Step 5: is the server stub calling the server procedure with the unmarshaled parameters. The reply traces the same path in the other direction.

The internet transport protocols:TCP

- ✓ It was specifically designed to provide a reliable end-to end byte stream over an unreliable network. It was designed to adapt dynamically to properties of the inter network and to be robust in the face of many kinds of failures.
- ✓ Each machine supporting TCP has a TCP transport entity, which accepts user data streams from local processes, breaks them up into pieces not exceeding 64kbytes and sends each piece as a separate IP datagram. When these datagrams arrive atamachine, they are given to TCP entity, which reconstructs the original byte streams. It is up to TCP totimeoutandretransmits them as needed, also to reassembledatagrams into messages in proper sequence.
- ✓ Thedifferent issuestobeconsideredare:
  1. TCP ServiceModel
  2. TCPProtocol
  3. TCPSegmentHeader
  4. TheConnectionManagement
  5. TCP Transmission Policy
  6. TCPCongestionControl
  7. TCPTimerManagement

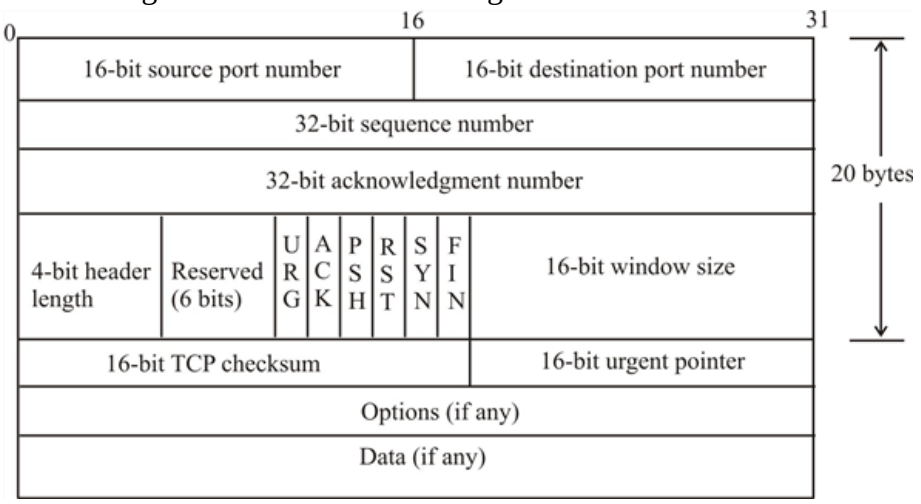
- ✓ **The TCP Protocol**
  - A key feature of TCP, and one which dominates the protocol design, is that every byte on a TCP connection has its own 32-bit sequence number.
  - When the Internet began, the lines between routers weremostly56-kbps leased lines, so a host blasting away at full speed took over 1 week to cycle through the sequence numbers.
  - Thebasic protocol usedbyTCPentities istheslidingwindow protocol.
  - Whenasendertransmits asegment,it alsostartsatimer.
  - WhenthesegmentarrivesatthedestinationthereceivingTCPentitysends

back a segment (with data if any exist, otherwise without data) bearing an acknowledgement number equal to the next sequence number it expects to receive.

- If the sender's timer goes off before the acknowledgement is received, the sender transmits the segment again.

✓ **TCP Segment Header**

- Every segment begins with a fixed-format, 20-byte header. The fixed headermaybe followed byheaderoptions. Afterthe options, if any, up to 65,535-20
  - 20 = 65,495 data bytes may follow, where the first 20 refer to the IP header and the second to the TCP header.
- Segments without any data are legal and are commonlyused for acknowledgements and control messages.



- **SourcePort:**Identifiesthesendingport
- **DestinationPort:**Identifiesthereceivingport.
- **Sequence number:**
  - If the SYN flag is set (1), then this is the initial sequence number. The sequence number of the actual first data byte and the acknowledged number in the corresponding ACK are then this sequence number+1.
  - If the SYN flag is clear (0), and then this is the accumulated sequence number of the first data byte of this segment for the current session.

- **AcknowledgementNumber:** If the ACKflagis set thenthevalueofthis field is the next sequence number that the sender of the ACK is expecting. This acknowledges receipt of all prior bytes (if any). The first ACKsent by eachend acknowledges the other end's initial sequence number itself, but no data.
- **TCPheaderlength:** SpecifiesthesizeoftheTCP headerin 32-bit words. The minimum size header is 5 words and the maximum is 15 words thus giving the minimum size of 20 bytes and maximum of 60 bytes, allowing for up to 40 bytes of options in the header. This field gets its name from the fact that it is also the offset from the start of the TCP segment to the actual data.
- **Reserved (3bits):**Forfutureuse andshouldbesetto zero.
- **Control Flags:**
  - URG: It is set to 1 if URGENT pointer is in use, which indicates start of urgent data.
  - ACK:Itissetto1toindicatethattheacknowledgementnumberis valid.
  - PSH:Indicatespushed data
  - RST: It is used to reset a connection that has become confused due to reject an invalid segment or refuse an attempt to open a connection.
  - FIN:Usedtoreleasea connection.
  - SYN:Usedtoestablish connections.
- **Window size (16 bits):** The size of the receive window, which specifies the number of window size units (by default, bytes) (beyond thesegment identified by the sequence number in the acknowledgment field) thatthe senderofthissegmentiscurrentlywillingtoreceive(seeFlowcontrol and Window Scaling).
- **Checksum (16 bits):** The 16-bit checksum field is used for error-checking of the header, the Payload and a Pseudo-Header. The Pseudo-Header consists of theSource IPAddress, theDestination IPAddress,theprotocolnumberforthe TCP-Protocol (0x0006) and the length of the TCP-Headers including Payload (in Bytes).
- **Urgent pointer (16 bits):** if the URG flag is set, then this 16-bit field is an offset from the sequence number indicating the last urgent data byte.
- **Options (Variable 0–320 bits, divisible by 32):** The length of this field is determined by the data offset field.
- **Padding:** The TCP header padding is used to ensure that the TCP header ends and data begins, on a 32 bit boundary. The padding is composed of zeros.

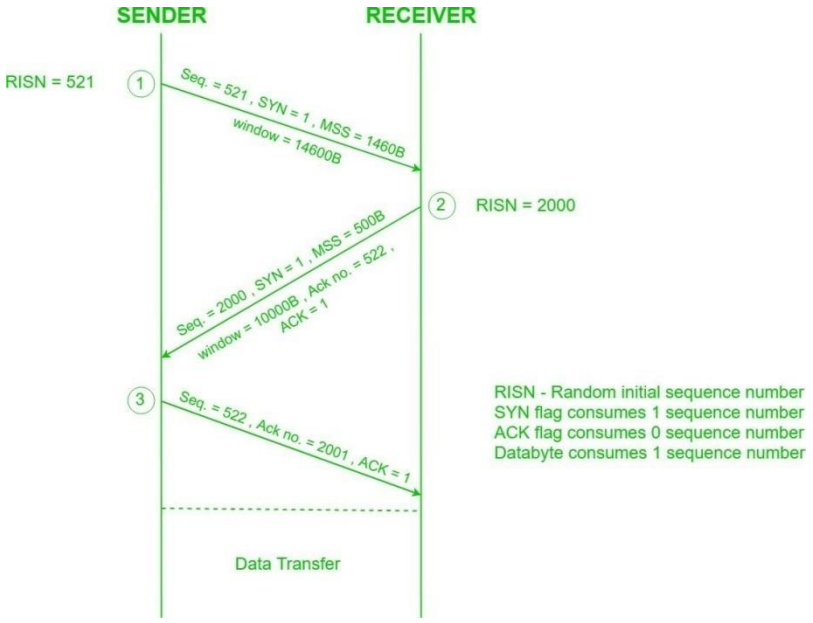
✓ **TCP Connection Establishment**

- TCP is a connection oriented protocol and every connection oriented protocol needs to establish connection in order to reserve resources at both the communicating ends.

1. Sender starts the process with following:
   - **Sequence number (Seq=521):** contains the random initial sequence number which generated at sender side.
   - **Syn flag (Syn=1):** request receiver to synchronize its sequence number with the above provided sequence number.
   - **Maximum segment size (MSS=1460 B):** sender tells its maximum segment size, so that receiver sends datagram which won't require any fragmentation. MSS field is present inside **Option** field in TCP header.

- **Window size(window=14600B):**sendertellsabouthis buffer capacity in which he has to store messages from receiver.

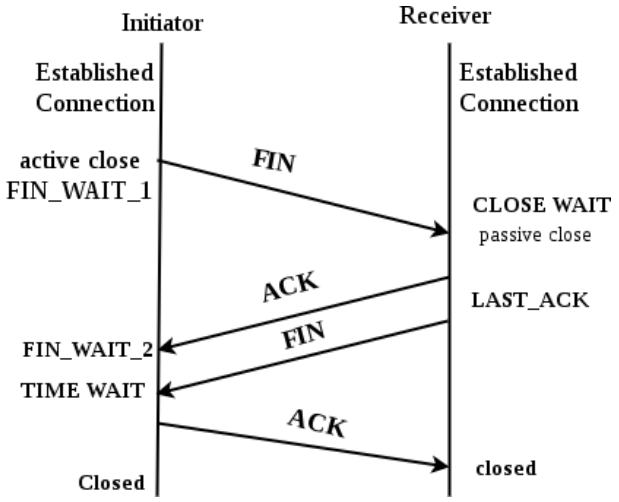
2. TCP isa full duplex protocol so both sender and receiver require a window for receiving messages from one another.
   - **Sequence number (Seq=2000):** contains the random initial sequence number which generated at receiver side.
   - **Syn flag (Syn=1):** request sender to synchronize its sequence number with the above provided sequence number.
   - **Maximumsegmentsize(MSS=500B):**sendertellsitsmaximum



segment size, so that receiver sends datagram which won't require any fragmentation. MSS field is present inside **Option** field in TCP header. Since MSSreceiver < MSSsender, both parties agree forminimumMSS i.e., 500 B to avoid fragmentation of packets at both ends.

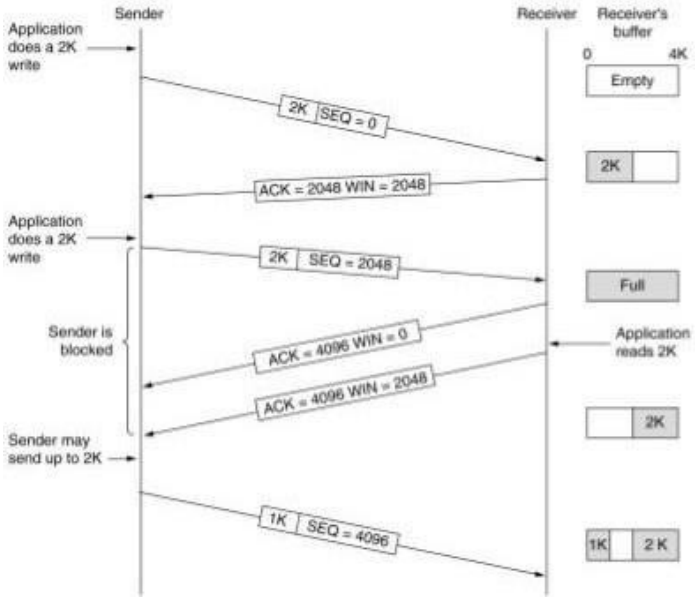
   - **Window size (window=10000 B):** receiver tells about his buffer capacity in which he has to store messages from sender.
   - **Acknowledgement Number (Ack no.=522):** Since sequence number 521 is received by receiver so, it makes a request of next sequence number with Ack no.=522 which is the next packet expected byreceiver since Syn flag consumes 1 sequence no.
   - **ACKflag (ACk=1):** tells that acknowledgement numberfield contains the next sequence expected by receiver.
3. Sender makes the final reply for connection establishment in followingway:
   - **Sequence number(Seq=522):** sincesequencenumber=521in1st step and SYN flag consumes one sequence number hence, next sequence number will be 522.
   - **Acknowledgement Number (Ack no.=2001):** since sender is acknowledgingSYN=1packetfromthereceiverwithsequencenumber 2000 so, the next sequence number expected is 2001.
   - **ACK flag (ACK=1):** tells that acknowledgement numberfield contains the next sequence expected by sender.

- ✓ **TCP Connection Release**
  - In TCP 3-way Handshake Process we studied that how connection establish betweenclientandserverinTransmissionControlProtocol(TCP)using **SYN** bit segments. TCP closes connection between Client and Server. Here wewill also need to sendbit segments to serverwhich **FIN**bit is set to 1.



  - How mechanism works inTCP:
    - **Step 1 (FIN From Client):** Suppose that the client application decides it wants to closetheconnection. (Notethat theservercould also choose to close the connection). This causes the client send a TCP segment with the **FIN** bit set to **1** to server and to enter the **FIN_WAIT_1** state. While in the **FIN_WAIT_1** state, the client waits for a TCP segment from the server with an acknowledgment (ACK).
    - **Step 2 (ACK From Server):** When Server received FIN bit segment from Sender (Client), Server Immediately send acknowledgement (ACK) segment to the Sender (Client).
    - **Step 3 (Client waiting):** While in the **FIN_WAIT_1** state, the client waits for a TCP segment from the server with an acknowledgment. Whenitreceivesthissegment,thecliententers the **FIN_WAIT_2** state. While in the **FIN_WAIT_2** state, the client waits for another segment from the server with the FIN bit set to 1.
    - **Step 4 (FIN from Server):** Server sends FIN bit segment to the Sender(Client) after some time when Server send the ACK segment (because of some closing process in the Server).
    - **Step 5 (ACK from Client):** When Client receive FIN bit segmentfrom the Server, the client acknowledges the server's segment and enters the **TIME_WAIT** state. The **TIME_WAIT** state lets the client resend the final acknowledgment in case the **ACK** is lost. The time spent by client in the **TIME_WAIT** state is depend on their implementation, but their typical values are 30 seconds, 1 minute, and
      2 minutes. After the wait, the connection formally closes and all resources on the client side (including port numbers andbuffer data) are released.

- ✓ **TCP Transmission Policy**
  - WindowmanagementinTCP



    - Intheabove example,thereceiverhas4096-byte buffer.
    - If the sender transmits a 2048-byte segment that is correctly received, the receiver will acknowledge the segment.
    - Now the receiver will advertise a window of 2048 as it has only 2048of buffer space, now.
    - Now the sender transmits another 2048 bytes which are acknowledged, but the advertised window is'0'.
    - Thesendermust stop untiltheapplicationprocessonthereceivinghost has removed some data from the buffer, at which time TCP can advertise a layer window.

- ✓ **SillyWindow Syndrome**
  - ThisisoneoftheproblemsthatruintheTCP performance,whichoccurs when data are passed to the sending TCP entity in large blocks, but an interactive application on the receiving side reads 1 byte at a time.

- ✓ **TCPTimer Management**
  - TCPuses 3 kinds oftimers:
    - Retransmissiontimer
    - Persistencetimer
    - Keep-Alivetimer.

  - **Retransmission timer:**
    - When a segment is sent, a timer is started. If the segment is acknowledged before the timer expires, the timer is stopped. If on the other hand, the timer goes off before the acknowledgement comes in, the segment is retransmitted and the timer is started again.
    - The algorithm that constantly adjusts the time-out interval, based on continuous measurements of n/w performance was proposed by JACOBSON and works as follows:

- For each connection, TCP maintains a variable RTT, that is the best current estimate of the round trip time to the destination.
- When a segment is sent, a timer is started, both to see how long the acknowledgement takes and to trigger a retransmission if it takes too long.
- If the acknowledgement gets back before the timerexpires,TCP measures how long the measurements took say M. It then updates RTT according to the formula:

  $$RTT=\alpha RTT+(1-\alpha)\ M$$

  - where α = a smoothing factor that determines how much weight is given to the old value. Typically, $\alpha = 7/8$
- Retransmissiontimeoutiscalculatedas

  $$D =\alpha D+ (1-\alpha)|RTT-M|$$

  - where D = another smoothed variable, Mean RTT = expected acknowledgement value
  - M=observedacknowledgement value
- Timeout=RTT+(4*D)

- **Persistence timer:**
  - Itisdesignedtoprevent thefollowingdeadlock:
    - The receiver sends an acknowledgement with a window size of '0' telling the sender to wait later, the receiver updates the window, but the packet with the update is lost now both the sender and receiver are waiting for each other to do something
    - When the persistence timer goes off, the sender transmits a probe to the receiver the response to the probe givesthe window size. If it is still zero, the persistence timer is set again and the cycle repeats. If it is non zero, data can now be sent.

- **Keep-Alivetimer:**
  - When a connection has been idle for along time, this timer may go off to cause one side to check if other side is still there.If it fails to respond, the connection is terminated.

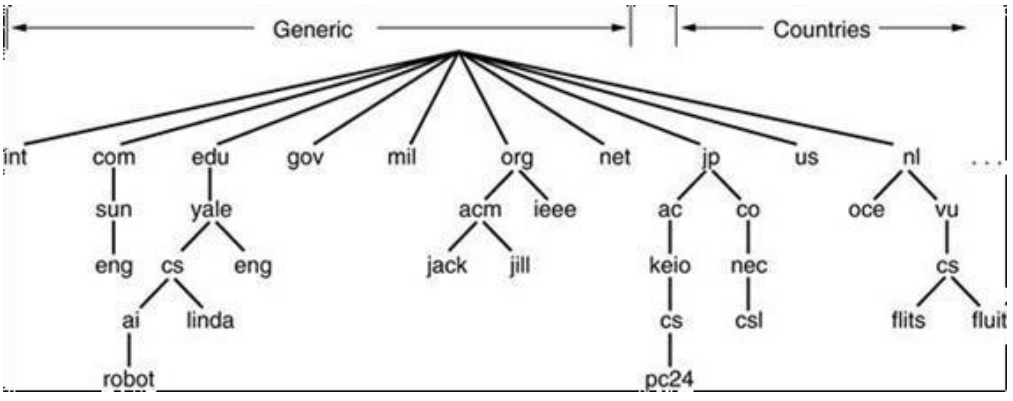
Reference Book: Computer Networks, Andrew Tanenbaum, 6th Edition.

UNIT-V
THE APPLICATION LAYER

DOMAIN NAME SYSTEM (DNS)

- ✓ This is primarily used for mapping host and e-mail destinations to IP addresses but can also be used other purposes. DNS is defined in RFCs 1034 and 1035.
- ✓ **DNS Working**
  - To map a name onto an IP address, an application program calls a library procedure called Resolver, passing it the name as a parameter.
  - The resolver sends a UDP packet to a local DNS server, which then looks up the name and returns the IP address to the resolver, which then returns it to the caller.
  - Armed with the IP address, the program can then establish a TCP connection with the destination, or send it UDP packets.

- ✓ **DNS Name Space**
  - The Internet is divided into several hundred top level domains, where each domain covers many hosts. Each domain is partitioned into sub domains, and these are further partitioned as so on. All these domains can be represented bya tree, in which the leaves represent domains that have no sub domains. A leaf domain may contain a single host, or it may represent a company and contains thousands of hosts. Each domain is named by the path upward from it to the root. The components are separated by periods (pronounced "dot")
  - Example:Microsoft.Development=dev.microsoft.com.
  - Thetop domain comesin two flavours
    - **Generic:** com (commercial), edu (educational instructions), mil (the U.S armed forces, government), int (certain international organizations), net (network providers), org(non profit organizations).
    - **Country:** include one entry for every country. Domain names can be either absolute (ends with a period e.g. dev.microsoft.com) or relative (doesn't end with a period). Domain names are case sensitive and the component names can be up to 63 characters long and full path names must not exceed 255 characters.



✓ **Resource Records**

- Every domain can have a sent of resource records associated with it. For a single host, the most common resource record is just its IP address. When a resolver gives a domain name to DNS, it gets both the resource records associated with that name i.e., the real function of DNS is to map domain names into resource records.
- Aresourcerecordisa5-tupleandits formatisas follows:

Domain_Name	Time to live	Type	Class	Value

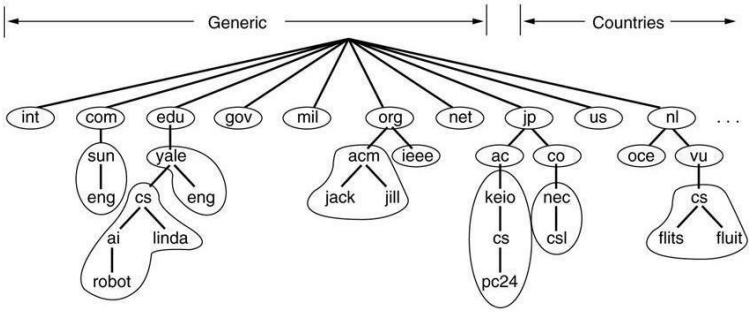
  - **Domain_name:**Tellsthedomaintowhichthisrecord applies.
  - **Time-to-live:**Givesanidentificationofhowstabletherecordis (High Stable =86400 i.e. no. ofseconds /day) (High Volatile =1 min)
  - **Type:**Tellswhatkindofrecordthis is

Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept e-mail
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

  - **Class:** It is IN for the internet information and codes for non internetinformation
  - **Value:**This field can beanumberadomain nameoran ASCIIstring

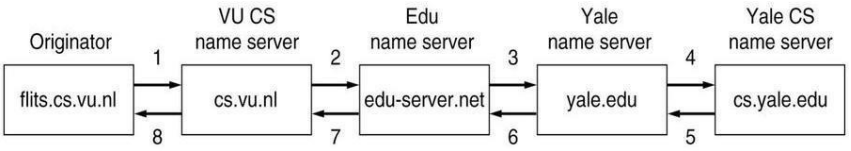
✓ **Name Servers**

- It contains the entire database and responds to all queries about it. DNS name space is divided up into non-overlapping zones, in which each zone contains some part of the tree and also contains name servers holding the authoritative information about that zone.
- Partofthe DNS namespaceshowingthe divisioninto zones:



- When a resolver has a query abouta domain name, it passes the query to one of the local name servers:
  - 1. If the domain being sought falls under the jurisdiction of name server,itreturnstheauthoritativeresourcerecords(thatcomesfromthe authority that manages the record, and is always correct).
  - 2. If the domain is remote and no information about the requested domain is available locally the name server sends a query message to the top level name server for the domain requested.

- Example: A resolver of flits.cs.vle.nl wants to know the IP address of the host Linda.cs.yale.edu

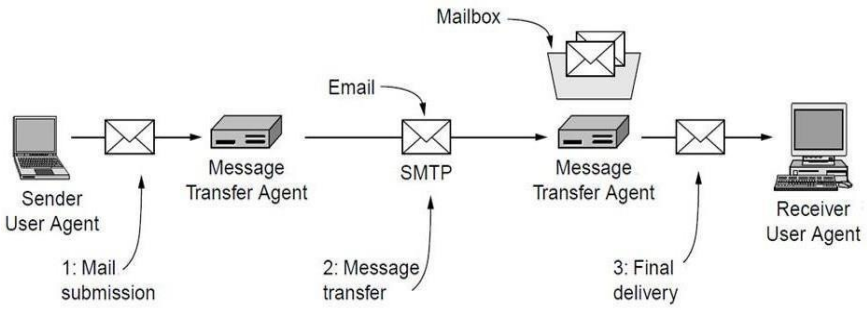


  - Step 1: Resolver sends a query containing domain name sought the type and the class to local name server, cs.vu.nl.
  - Step 2: Suppose local name server knows nothing about it, it asks few others nearby name servers. If none of them know, it sends a UDP packet to the server for edu-server.net.
  - Step 3: This server knows nothing about Linda.cs.yale.edu or cs.yale.edu and so it forwards the request to the name server for yale.edu.
  - Step 4: This oneforwards the request to cs.yale.edu which must have authoritative resource records.
  - Step 5 to 8: The resource record requested works itsway back in steps 5-8 This query method is known as Recursive Query
- 3. When a query cannot be satisfied locally, the query fails butthe name of the next server along the line to try is returned.

Electronic mail (SMTP,POP3,IMAP,MIME)

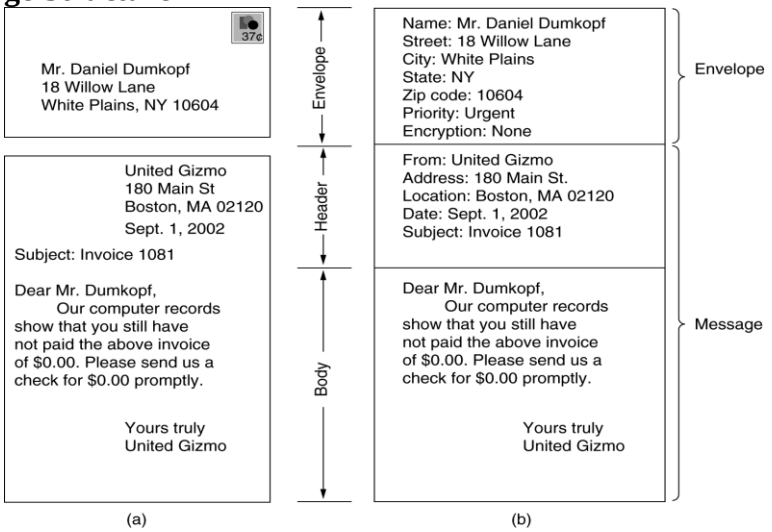
- ✓ Emailisa service whichallowsustosendthemessage inelectronicmode overthe internet.
- ✓ Itoffersanefficient,inexpensiveandrealtimemeanofdistributinginformation among people.
- ✓ Emailisastore-and-forwardmethodofsending,storing,andretrievingelectronic messages.
- ✓ Emailmessagesarestoredindatabasesonmail servers.
- ✓ Emailclients communicatewithmailserverstosendandreceive email.
- ✓ Mailserverscommunicatewithothermailserverstotransportmessagesfromone domain to another.
- ✓ Emailclients do notcommunicate directlywhen sending email.
- ✓ Emailrelies onthreeseparateprotocolsforoperation:
  - SMTP(sending)
  - POP(retrieving)
  - IMAP(retrieving)

- ✓ **Architecture and Services**



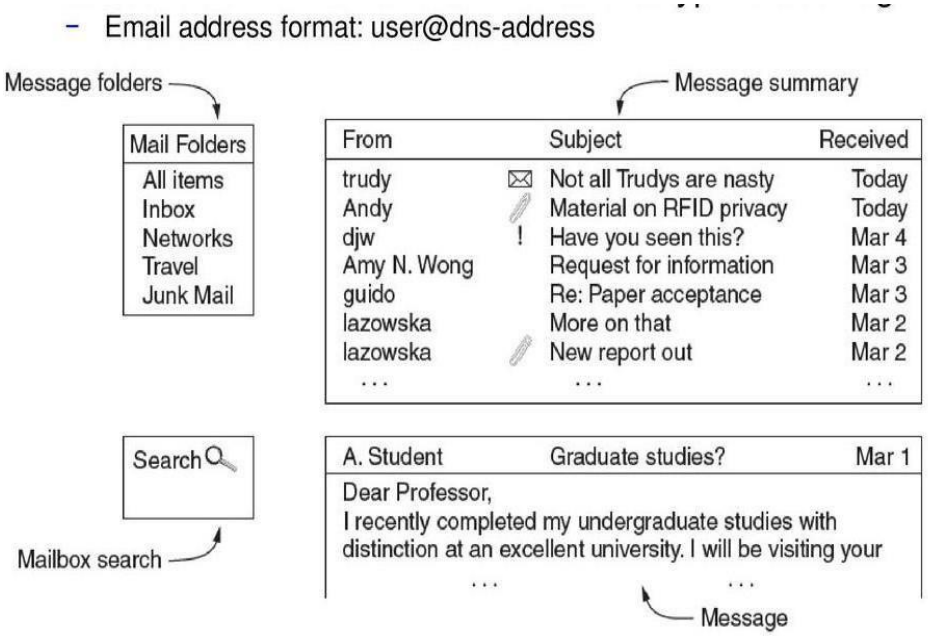
- ✓ **E-mail systems consist of two subsystems.They are:**
  - (1).UserAgents: which allowpeopletoreadandsende-mail
    - A program that accepts a variety of commands for composing, receiving, and replying to messages, as well as for manipulating mailboxes
      - Sending E-Mail: To send an e-mail message, a user must providethemessage,the destinationaddress,and possiblysome other parameters. The message can be produced with a free-standing text editor, a word processing program, or possibly with a specialized text editor built into the user agent. The destination address must be in a format that the user agent can deal with. Many user agents expect addresses of the form user@dns-address.
      - Reading E-Mail: When a user agent is started up, it looks at the user's mailbox for incoming e-mail before displaying anything on thescreen. Then it mayannounce thenumberofmessages in themailbox ordisplaya one-linesummaryofeachoneandwait for a command.
  - (2). Message Transfer Agents: which move messages from source to destination
- ✓ **Basic email functions**
  - **Composition**: The process of creating messages and answers. Any text editor is used for bodyof the message. While the system itself can provide assistance with addressing and numerous header fields attached to each message.
  - **Reporting**: It has to do with telling the originator what happened to the message that is, whether it was delivered, rejected (or) lost.
  - **Transfer**:Itreferstomovingmessagesfromoriginatortotherecipient.
  - **Displaying**: Incoming messages are to be displayed so that people can read their email.
  - **Disposition**: It concerns what the recipient dose with the message after receiving it. Possibilities include throwing it away before reading (or) after reading, saving it and so on.

- ✓ **Email Message Structure**



Envelopes and messages.(a)Paper mail(b)Electronic mail

✓ **Typical elements of the user agent interface.**



✓ **Message Formats**

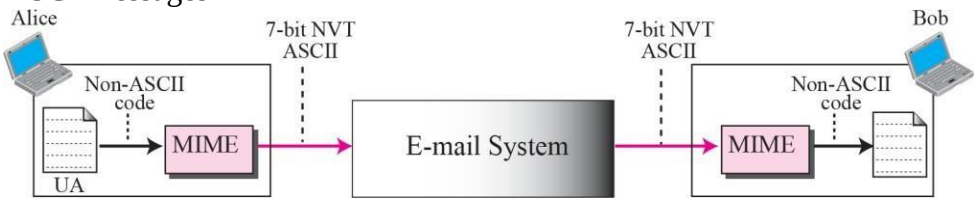
- RFC822headerfieldsrelatedtomessagetransport.

Header	Meaning
To:	E-mail address(es) of primary recipient(s)
Cc:	E-mail address(es) of secondary recipient(s)
Bcc:	E-mail address(es) for blind carbon copies
From:	Person or people who created the message
Sender:	E-mail address of the actual sender
Received:	Line added by each transfer agent along the route
Return-Path:	Can be used to identify a path back to the sender

- SomefieldsusedintheRFC 822message header.

Header	Meaning
Date:	The date and time the message was sent
Reply-To:	E-mail address to which replies should be sent
Message-Id:	Unique number for referencing this message later
In-Reply-To:	Message-Id of the message to which this is a reply
References:	Other relevant Message-Ids
Keywords:	User-chosen keywords
Subject:	Short summary of the message for the one-line display

- ✓ **MIME–Multipurpose Internet Mail Extensions**
  - SomeproblemswhenusingASCIIformattedmessages:
    - Languageswithaccents(French,German).
    - Languagesinnon-Latinalphabets(Hebrew, Russian).
    - Languageswithoutalphabets(Chinese,Japanese).
    - Messagesnotcontainingtextat all(audio orimages).
  - MIMEaddsstructuretothemessagebodyanddefinesencodingrulesfornon-ASCIImessages



  - RFC822headersaddedbyMIME

Header	Meaning
MIME-Version:	Identifies the MIME version
Content-Description:	Human-readable string telling what is in the message
Content-Id:	Unique identifier
Content-Transfer-Encoding:	How the body is wrapped for transmission
Content-Type:	Type and format of the content

  - The MIME types and subtypes definedinRFC2045.

Type	Subtype	Description
Text	Plain	Unformatted text
	Enriched	Text including simple formatting commands
Image	Gif	Still picture in GIF format
	Jpeg	Still picture in JPEG format
Audio	Basic	Audible sound
Video	Mpeg	Movie in MPEG format
Application	Octet-stream	An uninterpreted byte sequence
	Postscript	A printable document in PostScript
Message	Rfc822	A MIME RFC 822 message
	Partial	Message has been split for transmission
	External-body	Message itself must be fetched over the net
Multipart	Mixed	Independent parts in the specified order
	Alternative	Same message in different formats
	Parallel	Parts must be viewed simultaneously
	Digest	Each part is a complete RFC 822 message

  - Example: multipart/mixed

```
From: Nathaniel Borenstein <nsb@bellcore.com>
To:  Ned Freed <ned@innosoft.com>
Subject: Sample message
MIME-Version: 1.0
Content-type: multipart/mixed; boundary="simple
boundary"

This is the preamble.  It is to be ignored, though it
is a handy place for mail composers to include an
explanatory note to non-MIME compliant readers.
--simple boundary

This is implicitly typed plain ASCII text.
It does NOT end with a linebreak.
--simple boundary
Content-type: text/plain; charset=us-ascii

This is explicitly typed plain ASCII text.
It DOES end with a linebreak.

--simple boundary--
This is the epilogue.  It is also to be ignored.
```

- Example:multipart/alternative

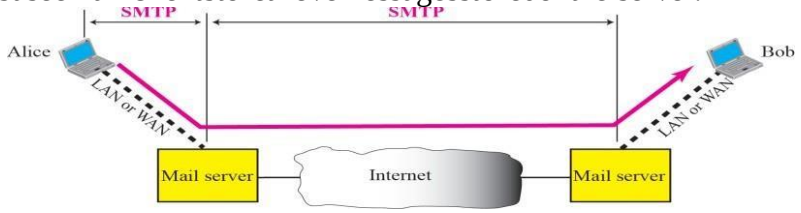
```
From:  Nathaniel Borenstein <nsb@bellcore.com>
To: Ned Freed <ned@innosoft.com>
Subject: Formatted text mail
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary=boundary42


--boundary42
Content-Type: text/plain; charset=us-ascii

...plain text version of message goes here....

--boundary42
Content-Type: text/richtext

.... richtext version of same message goes here ...
--boundary42
Content-Type: text/x-whatever

.... fanciest formatted version of same  message  goes  here
...
--boundary42--
```

- Example:multipart/digest

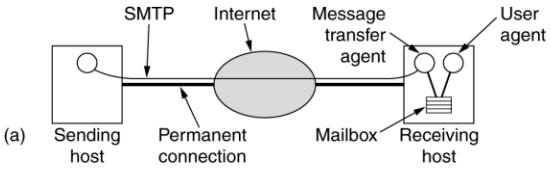
```
From: Moderator-Address
MIME-Version: 1.0
Subject:  Internet Digest, volume 42
Content-Type: multipart/digest;
     boundary="---- next message ----"


------ next message ----

From: someone-else
Subject: my opinion

...body goes here ...

------ next message ----

From: someone-else-again
Subject: my different opinion

... another body goes here...

------ next message ------
```

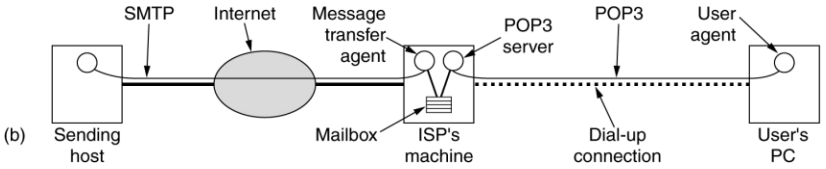
✓ **Simple Message Transfer Protocol(SMTP)**

- SMTPmessageformatsrequireamessageheader and body.
- Thebodycancontain anyamount oftext.
- Theheadermusthaveaproperlyformattedrecipientemailaddressanda sender address.
- AnSMTPclientsendsanemailbyconnectingtoa SMTPserveronport 25.
- Theserverreceivesthemessageandstoresitmessageinalocalmailboxor relays the message to another mail server.
- Usersuseemail clientstoretrievemessagesstoredonthe server.



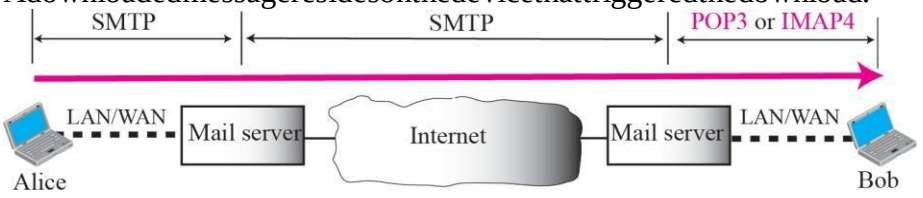
- Final Delivery
  - With the advent of people who access the Internet by calling their ISPover a modem, it breaks down.
  - One solution is to have amessage transfer agent onan ISP machine accept e-mail for its customers and store it in their mailboxes on an ISP machine. Since this agent can be on-line all the time, e-mail can be sent to it 24 hours a day.



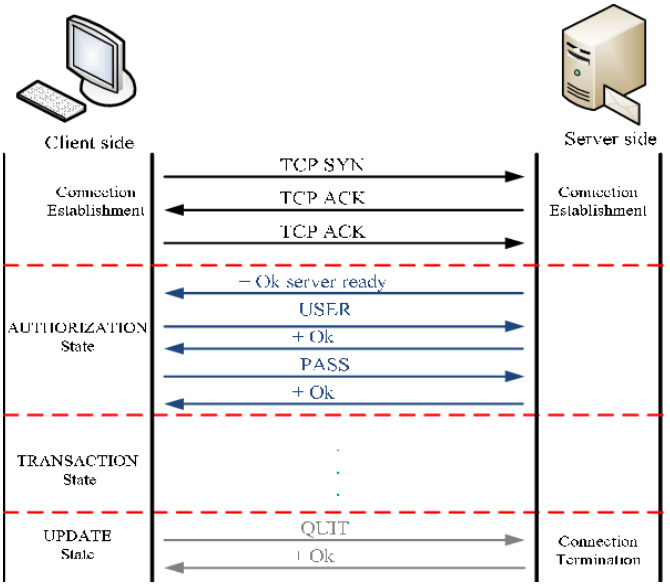


(a) Sending and reading mail when the receiver has a permanent Internet connection and the user agent runs on the same machine as the message transfer agent.
(b) Readinge-mailwhenthereceiverhasadial-upconnectiontoanISP.

- ✓ **POP3**
  - Messagesaredownloadedfromtheservertotheclient.
  - Theserverlistenson port110 TCP forclient requests.
  - Emailclients directtheirPOP requeststomailserversonportTCP110.
  - The POP client and server exchange commands and responses until the connection is closed or aborted.
  - POP allows for email messages to be downloaded to the client's device (computer or phone) and removed from the server.
  - Thereisnocentralizedlocationwhereemailmessagesarekept.
  - Adownloadedmessageresidesonthedevicethattriggeredthedownload.



  - POP3–Client/ServerProcedure:



- ✓ **IMAP-(Internet MessageAccessProtocol)**
  - IMAPisanotherprotocolusedtoretrieveemailmessages.
  - Allowsformessagesto bedisplayedtotheuserratherthandownloaded.
  - Theoriginal messagesreside on theserver until manuallydeleted bytheuser.
  - Usersview copiesofthemessages intheiremail client software.
  - Userscancreate afolderhierarchyontheservertoorganizeandstoremail.
  - That filestructureisdisplayed ontheemail client.
  - Whena user decides to delete a message, the server synchronizes that action and deletes the message from the server.
  - POP3 is not convenient when users frequently use different machines to read email from servers, as emails have to be downloaded to different computers more or less random
  - IMAPcanresolvethisissuesasemailswill bealwayson theservers

- ✓ **Acomparison of POP3 and IMAP.**

Feature	POP3	IMAP
Where is protocol defined?	RFC 1939	RFC 2060
Which TCP port is used?	110	143
Where is e-mail stored?	User's PC	Server
Where is e-mail read?	Off-line	On-line
Connect time required?	Little	Much
Use of server resources?	Minimal	Extensive
Multiple mailboxes?	No	Yes
Who backs up mailboxes?	User	ISP
Good for mobile users?	No	Yes
User control over downloading?	Little	Great
Partial message downloads?	No	Yes
Are disk quotas a problem?	No	Could be in time
Simple to implement?	Yes	No
Widespread support?	Yes	Growing

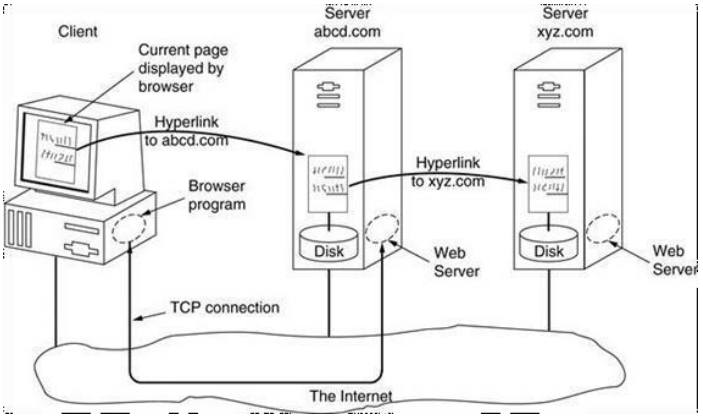
WWW-World Wide Web

- ✓ The World Wide Web is an architectural framework for accessing linked documents spread out over millions of machines all over the Internet. The initial proposal for a web of linked documents came from CERN physicist Tim Berners-Lee in 1989.

- ✓ **Architectural Over view**
  - Fromtheusers'point of view, theWeb consists ofavast, worldwide collection of documents or Web pages. Each page may contain links to other pages anywhere in the world. Users can follow a link by clicking on it, which then takes them to the page pointed to. This process can be repeated indefinitely.
  - Pages are viewed with a program called a browser, of which Internet Explorer and Netscape Navigator are two popular ones. The browser fetches the page requested, interprets the text and formatting commands on it, and displays the page, properly formatted, on the screen.

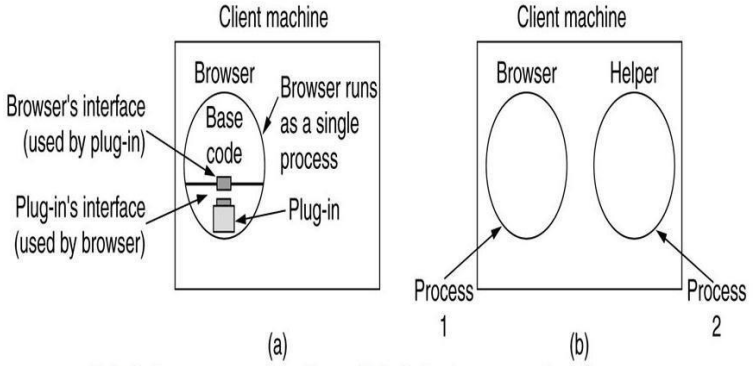
- Strings of text that are links to other pages, called hyperlinks, are often highlighted, by underlining, displaying them in a special color, or both.

✓ **Parts of the Web Model**



- HerethebrowserisdisplayingaWebpageontheclient machine.
- When the user clicks on a line of text that is linked to a page on the abcd.com server, the browser follows the hyperlink by sending a message to the abcd.com server asking it for the page.
- When the page arrives, it is displayed. If this page contains a hyperlink to a page on the xyz.com server that is clicked on, thebrowser then sends a request to that machine for the page.

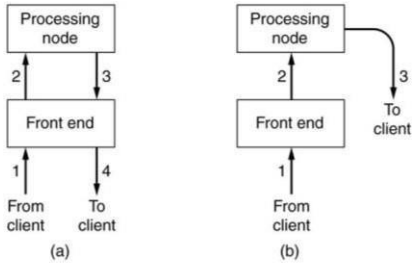
- **Client Side**
  - When an item is selected, the browser follows the hyperlinkandfetches the page selected. Therefore, the embedded hyperlink needs a wayto name any other page on the Web. Pages are named using URLs (Uniform Resource Locators).
  - Thesteps thatoccurat theclient sideare:
    - ThebrowserdeterminestheURL
    - ThebrowserasksDNSfortheIPaddress
    - DNSreplieswiththeIPaddress
    - ThebrowsermakesaTCPconnectiontoport80ontheIP address
    - Itsendsarequestaskingforfile
    - Thesiteserversendsthe file
    - TheTCPconnectionis released.
    - Thebrowserfetchesanddisplaysallthetextandimagesinthefile.
    - Web pages are written in standard HTML language to make it understandable by all browsers.
  - There are two possibilities: plug-ins and helper applications. A plug-in is a code module that the browser fetches from a special directory on the disk and installs as an extension to itself.
  - The other way to extend a browser is to use a helper application. Thisis a complete program, running as a separate process.



(a) A browser plug-in. (b) A helper application.

- **Server Side**
  - Thesteps to befollowedbytheserver sideare:
    - Accept aTCP connectionfromaclient(abrowser).
    - Getthename ofthefilerequested.
    - Getthefile(from disk).
    - Returnthefiletotheclient.
    - ReleasetheTCP connection.

- **Processing of Request**



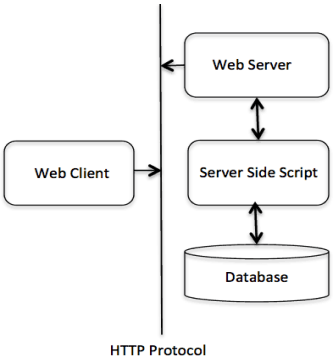
(a) Normal request-reply message sequence.
(b) Sequence when TCP handoff is used.

  - Theprocessingofrequest onthe web is as follows:
    - Resolvethe nameoftheWeb pagerequested.
    - Authenticatethe client.
    - Performaccesscontrolontheclient.
    - Performaccess controlontheWebpage.
    - Checkthe cache.
    - Fetchtherequestedpage from disk.
    - Determinethe MIMEtypetoincludeintheresponse.
    - Takecareofmiscellaneous oddsand ends.
    - Return the replyto the client.
    - Makean entryin theserverlog.

HTTP

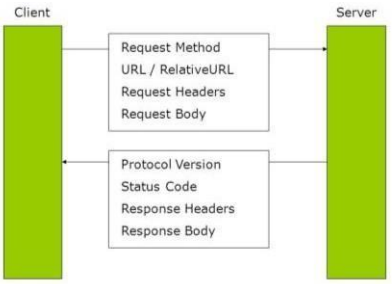
- ✓ **HTTP** (Hyper Text Transfer Protocol) is the most popular protocol used for web browsing. It is basically a computer networking application layer protocol provided to the applications for accessing data on the world wide web (www).

- ✓ **Basic Architecture**
  - The following diagram shows a very basic architecture of a web application and depicts where HTTP sites:



  - The HTTP protocol is a request/response protocol based on the client/server basedarchitecturewherewebbrowsers,robotsandsearchengines, etc.actlike HTTP clients and the Web server acts as a server.
    - **Client:** The HTTP client sends a request to the server in the form of a request method, URI, and protocol version, followed by a MIME-like message containing request modifiers, client information, and possible body content over a TCP/IP connection.
    - **Server:** The HTTP server responds with a status line, including the message's protocol version and a success or error code, followed by a MIME-like message containing server information, entity meta information, and possible entity-body content.

- ✓ **HTTP Basic Operation**



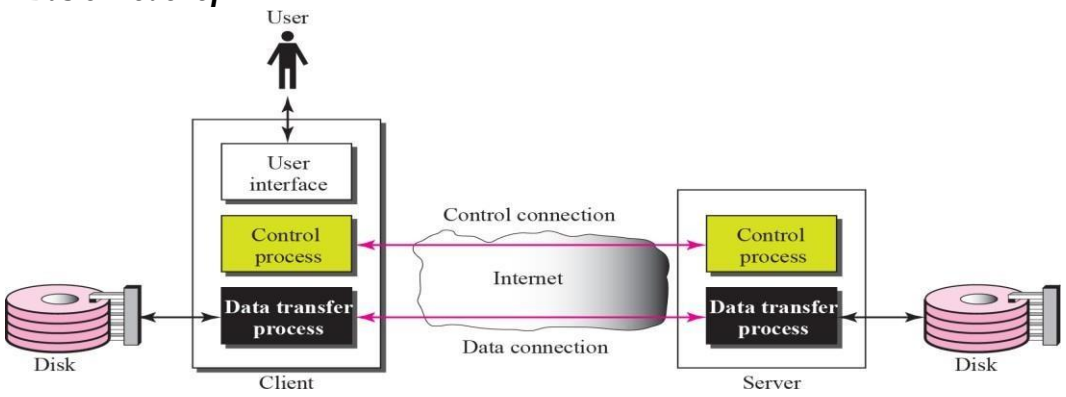
  - HTTP is a standard textbased, application layer protocol, used by all browsers to access millions and millions of web pages, stored across the entire globe.
  - It is similar to FTP in some aspects as it uses TCP as the underlying transport layer protocol to transfer files and supports methods like get and put for data transfer. However, HTTP uses just a single TCP connection compared to two TCP connections used by FTP (one control and one data).HTTP isalso similar to SMTP in the structure of protocol messages.
  - HTTP is a reliable protocol, making sure that all data transferred through it reaches the peer machine without any loss. Due to this reliability requirement, HTTP uses TCP as the transport layer protocol.

- It isa simple **Client-ServerREQUEST-REPLYprotocol**, where clients send HTTP requests and servers respond with HTTP replies.
- HTTP is a **stateless protocol** as each HTTP Requests and Replies are treated independently by the client and server. So server does not maintainany specific state about each HTTP transaction.
- HTTP supports multiple basic operations in the form of different HTTP methods:
  - GET Method: It is used to retrieve information from the given server using a given URI. Requests using GET should only retrieve data and should have no other effect on the data.
  - POST Method: It is used to send data to the server, for example, customer information, file upload, etc. using HTML forms.
  - HEAD: Same as GET, but transfers the status line and header section only.
  - PUT: Replaces all current representations of the target resource withthe uploaded content.
  - DELETE: Removes all current representations of the target resource given by a URI.
  - CONNECT: Establishes a tunnel to the server identified by a given URI.
  - OPTIONS: Describes the communication options for the target resource.
  - TRACE:Performsamessageloop-backtestalongthepathtothetarget resource.

FTP

- ✓ FileTransferProtocol (FTP)isthestandardmechanismprovidedbyTCP/IPfor copying a file from one host to another.
- ✓ Although transferring files from one system to another seems simple and straightforward, some problems must be dealt with first.
- ✓ Forexample,
  - Two systems mayusedifferent file name conventions. Two systems mayhave different ways to represent text and data.
  - Twosystems mayhavedifferent directorystructures.
  - All of these problems have been solved by FTP in a very simple and elegantapproach.
- ✓ FTP differs from other client-server applications in that it establishes two connections between the hosts.
  - Oneconnection is usedfordata transfer
  - Theotherforcontrolinformation (commandsandresponses).
- ✓ Separationofcommandsanddatatransfermakes FTP moreefficient.
  - Thecontrol connectionuses verysimplerules ofcommunication.
  - The data connection, on the other hand, needs more complex rules due to the variety of data types transferred.
- ✓ FTPusestwowell-knownTCPports:
  - Port21isusedforthecontrolconnection,and
  - Port 20 is usedforthedata connection.

✓ ***Basic model of FTP***

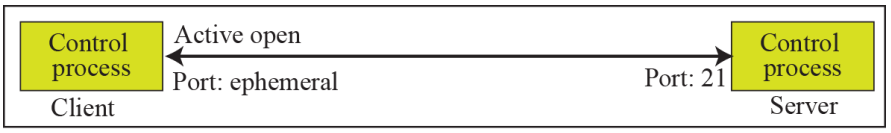


- Theclienthasthree components:
  - Userinterface, client control process, and the client data transfer process.
- Theserverhastwo components:
  - Servercontrolprocessandtheserverdatatransfer process.
- Thecontrolconnectionismadebetweenthecontrol processes.
- Thedataconnection ismadebetween thedatatransfer processes.
  - Thecontrol connection remains connected duringtheentireinteractive FTP session.
  - Thedataconnectionisopenedandthenclosedforeachfile transferred.

✓ ***Control Connection***

- The control connection is created in the same way as other application programs. There are two steps:
  - 1.Theserverissuesapassiveopenonthewell-knownport21and waits for a client.
  - 2.Theclientusesanephemeralportandissues anactiveopen.
- Theconnectionremainsopenduringtheentireprocess.

a. First, passive open by server



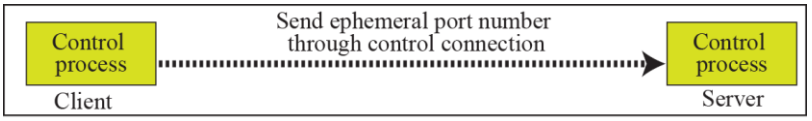
b. Later, active open by client

✓ ***Data Connection***

- 1. The client, not the server, issues a passive open using an ephemeral port. This must be done by the client because it is the client that issues the commands for transferring files.

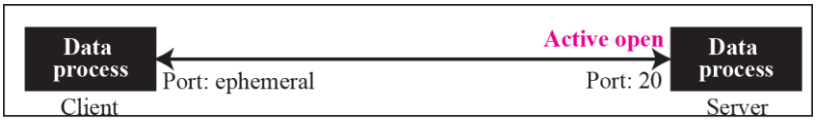
a. First, passive open by client

- 2.Theclientsends this portnumbertotheserverusingthe PORT command.



b. Second, sending of ephemeral port

- 3.Theserverreceivestheportnumberandissuesanactiveopenusingthe wellknown port 20 and the received ephemeral port number.



c. Third, active open by server

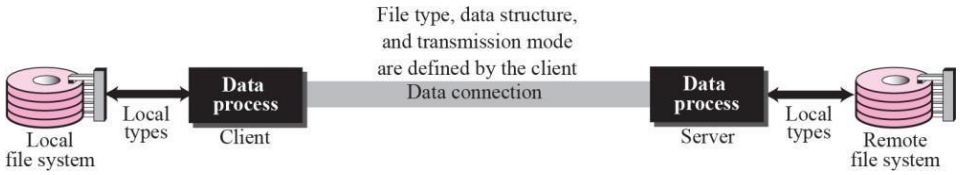
✓ ***Communication:***

- TheFTPclient andserver,whichrunondifferent computers,must communicate with each other.
- These two computers may use different operating systems, different character sets, different file structures, and different file formats.
- FTP must makethisheterogeneitycompatible.
- FTP has two different approaches, one for the control connection and one for the data connection.

- ***Communication over Control Connection***

  - FTP uses the same approach as TELNET or SMTP to communicate across the control connection.
  - ItusestheNVTASCIIcharacterset.
  - Communication is achieved through commands and responses. This simple method is adequate for the control connection because we send one command (or response) at a time. Each command or response is only one short line so we need not worry about file format or file structure. Each line is terminated with a two-character (carriage return and line feed) end-of-line token.

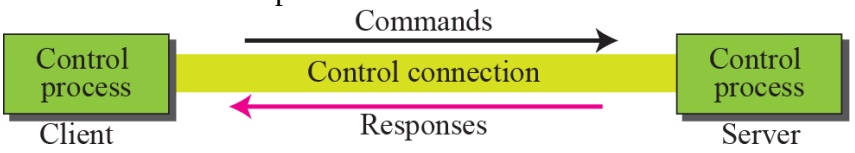
- ***Communication over Data Connection***



  - The purpose andimplementation of the data connection are differentfrom that of the control connection.
  - Itusedtotransferfilesthroughthedata connection.
  - Theclient must definethetype of fileto be transferred, the structureof the data, and the transmission mode.
  - Before sending thefile throughthe dataconnection,firstprepare for transmission through the control connection.

- The heterogeneity problem is resolved by defining three attributes ofcommunication: file type, data structure, and transmission mode.
- FileType:
  - ASCIIfile,EBCDICfileand Imagefile
- DataStructure:
  - Filestructure(default),RecordstructureandPage structure.
- Transmission Mode:
  - Streammode,Blockmodeandcompressedmode.

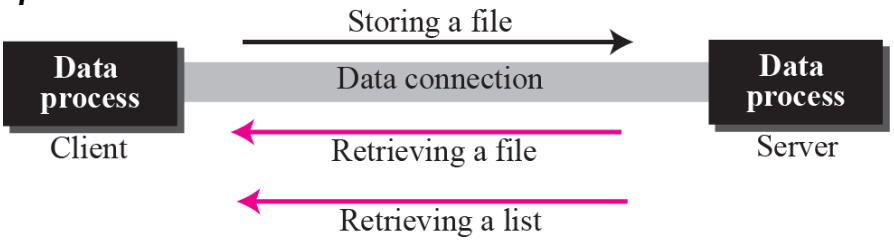
- ***Command processing***
  - FTP uses the control connection to establish a communication between the client control process and the server control process.
  - During this communication, the commands are sent from the client to the server and the responses are sent from the server to the client



✓ ***Commands:***

- Commands,whicharesentfromtheFTPclient controlprocess, are intheform of ASCII uppercase, which may or may not be followed by an argument.
- Divide the commands into six groups: access commands, file management commands, data formatting commands, port defining commands, file transferring commands, and miscellaneous commands.

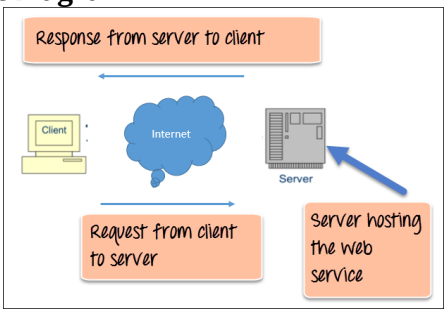
✓ ***File transfer:***



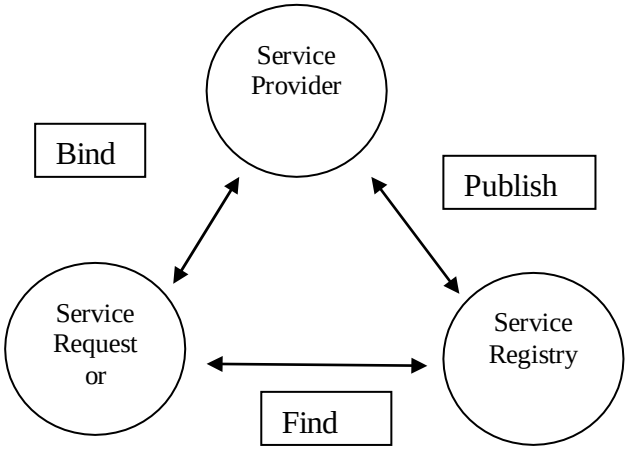
- File transfer occurs over the data connection under the control of the commands sent over the control connection. However, we should remember that file transfer in FTP means one of three things:
  - A file is to be copied from the server to the client (download). This is called retrieving a file. It is done under the supervision of the RETR command.
  - A file is to be copied from the client to the server (upload). This is called storing a file. It is done under the supervision of the STOR command.
  - A list of directory or file names is to be sent from the server to the client. This is done under the supervision of the LIST command. Note that FTP treats a list of directory or file names as a file. It is sent over the data connection.

Web Services

- ✓ Webserviceisastandardizedmediumtopropagatecommunicationbetweentheclient and server applications on the World Wide Web.
- ✓ Awebserviceisasoftwaremodulewhichisdesignedtoperformacertainsetof tasks.
  - Theweb services can besearched foroverthenetworkand can also be invoked accordingly.
  - When invoked the web service would be able toprovide functionality to theclient which invokes that web service.
- ✓ **WebServiceArchitectureDiagram**



  - The above diagram shows a very simplistic view of how a web service would actually work. The client would invoke a series of web service calls via requests to a server which would host the actual web service.
  - These requests are made through what is known as remote procedure calls. Remote Procedure Calls (RPC) are calls made to methods which are hosted by the relevant web service.



  - Every framework needs some sort of architecture to make sure the entire framework works as desired. Similarly, in web services, there isanarchitecture which consists of three distinct roles as given below
    - **Provider** - The provider creates the web service and makes it available to client application who wants to use it.
    - **Requestor** - A requestor is nothingbut the clientapplication that needs to contact a web service. The client application can be a .Net, Java, or any other language based application which looks for some sort of functionality via a web service.
    - **Broker** - The broker is nothing but the application which provides access totheUDDI(UniversalDescription,Discoveryandintegration). The UDDI, as discussed in the earlier topic enables the client application to locate the web service.

- **Publish** - A provider informs the broker (service registry) about the existence of the web service by using the broker's publish interface to make the service accessible to clients
- **Find** - The requestor consults the broker to locate a published web service
- **Bind** - With the information it gained from the broker(service registry) about the web service, the requestor is able to bind, or invoke, the web service.

✓ **Type of Web Service**

- Therearemainlytwo types of web services.
  - SOAPwebservices.
  - RESTfulwebservices.

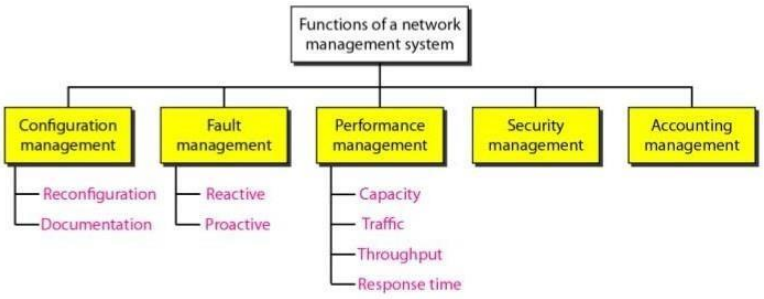
- **SOAP(SimpleObject AccessProtocol)**
  - SOAP is known as a transport-independent messaging protocol. SOAP is based on transferring XML data as SOAP Messages. Each message has something which is known as an XML document.
  - Onlythe structure of the XMLdocument follows a specific pattern, but not the content. The best part of Web services and SOAP is that its all sent via HTTP, which is the standard web protocol.
- **WSDL(Webservicesdescriptionlanguage)**
  - **A web service cannot be used if it cannot be found**. The client invoking the web service should know where the web service actually resides.
- **UniversalDescription,Discovery,andIntegration(UDDI)**
  - UDDIis a standard for describing, publishing, and discovering the web services that are provided bya particular service provider. It provides a specification which helps in hosting the information on web services.

✓ **Web Services Advantages**

- ExposingBusinessFunctionalityonthenetwork
- Interoperabilityamongstapplications
- AStandardized Protocolwhicheverybodyunderstands
- Reductionin costofcommunication

SNMP

- ✓ **Functions of a network management system**



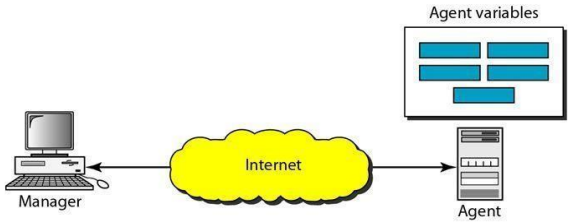
- **Configuration Management**
  - A large network is usually made up of hundreds of entities that are physicallyorlogicallyconnectedto one another. These entitieshave an initial configuration when the network is set up, but can change withtime.
  - Desktop computers may be replaced by others; application software may be updated to a newer version; and users may move from one group to another.
  - The configuration management system must know, at any time, thestatus of each entity and its relation to other entities.
  - Configuration management can be divided into two subsystems: reconfiguration and documentation.
- **Fault Management**
  - Complexnetworkstodayaremadeupofhundreds andsometimesthousands of components.
  - Properoperationofthenetworkdependsontheproperoperationof each component individually and in relation to each other.
  - Fault management is the area of network management that handles this issue.
  - Aneffectivefaultmanagementsystemhastwosubsystems:reactivefault management and proactive fault management.
- **Performance Management**
  - Performance management, which is closely related to fault management, tries to monitor and control the network to ensure that itis running as efficiently as possible.
  - Performance management tries to quantify performance by using somemeasurable quantity such as capacity, traffic, throughput, or responsetime.
- **Security Management**
  - Security management is responsible for controlling access to thenetwork based on the predefined policy.
- **Accounting Management**
  - Accounting management is the control of users' access to networkresources through charges. Under accounting management, individualusers, departments, divisions, or even projects are charged for theservices they receive from the network. Charging does not necessarily mean cash transfer; it may mean debiting the departments or divisions for budgeting purposes.

- Today,organizationsuseanaccountingmanagementsystemforthe following reasons:
  - Itpreventsusersfrommonopolizinglimitednetworkresources.
  - Itprevents usersfromusingthesystem inefficiently.
  - Network managers can do short- and long-term planning based on the demand for network use.

✓ SNMP–Simple Network Management Protocol

- The Simple Network Management Protocol (SNMP) is a framework for managing devices in an internet using the TCPIIP protocol suite. It provides a set of fundamental operations for monitoring and maintaining an internet.

- **SNMP concept**



- SNMP is an application-levelprotocol inwhicha fewmanagerstationscontrola set of agents. The protocol is designed at the application level so that it can monitor devices made by different manufacturers and installed on different physical networks.
- In other words, SNMP frees management tasks from both the physical characteristics of the managed devices and the underlying networking technology. It can be used in a heterogeneous internet made of different LANs and WANs connected by routers made by different manufacturers.

- **Components of SNMP**
  - There are four main components in anSNMP-managednetwork:
    - **SNMP agent:** This program runs on the hardware or servicebeingmonitored,collectingdataaboutvariousmetricslike bandwidth use or disk space. When queried by the SNMP manager, the agent sends this information back to the management system. An agent may also proactively notify theNMS if an error occurs. Most devices come with an SNMPagent preinstalled; it typically just needs to be turned on andconfigured.
    - **SNMP-managed devices and resources:** These are the nodeson which an agent runs.
    - **SNMP manager (aka NMS):** This software platform functionsas a centralized console to which agents feed information.It will actively request agents send updates via SNMP at regular intervals.Whatanetworkmanagercandowiththatinformation depends heavily on how feature-rich the NMS is. There are several free SNMP managers available, but they are typically limited in their capabilities or the number of nodes they can support. At the other end of the spectrum, enterprise-grade

platforms offer advanced features for more complex networks, with some products supporting up to tens of thousandsofnodes.

- **Management information base (MIB):** This database is a textfile (.mib) that itemizes and describes all objects used by aparticular device that can be queried or controlled using SNMP. This database must be loaded into the NMS so that it can identify and monitor the status of these properties. Each MIBitem is assigned an object identifier (OID).

- **SNMP Message Types**
  - There are different types of SNMP messages that can be used to set up network monitoring via SNMP:
    - **GetRequest** –Thisisthemost commonSNMPmessagethatanSNMP manager sends out to request data. The targeted devicereturns the requested value with a Response message.
    - **GetNextRequest** – The SNMP manager can send this message type to discover what information is available from the device. By starting at OID 0, the manager can continue to senda request for the next available data until there is no more "next" data. This way, users can discover all of the available data on a certain device even though they might not have had any prior knowledge of the responding system or device.
    - **GetBulkRequest** – Added in SNMP Version 2, this is a newer, optimized version of GetNextRequest. The solicited Response will contain as much data as allowed bytherequest. Essentially, this is a way to do several GetNextRequestsat once, which enables users to create a list of all available data and parameters.
    - **SetRequest** – This is a manager-initiated command to set or change the value of a parameter via SNMP on the agent device or system. This message type can be used to manage or update configuration settings or other parameters. But be careful! An incorrect SetRequest may seriously damage systems and network setups.
    - **Response** – The Response is the message that a device agent sends upon a Request from the manager. When sent in response to a GetRequest type, the packet contains the requested data or values. In the case of a SetRequest, the packetresponds withthe newly set value as a confirmation that the SetRequest has been completed successfully.
    - **Trap(v2)** – A trap is sent ("pushed out") by the SNMP agent without having been requested by the manager.Rather, trapsare sent upon determined conditions, such as in the event of an error, or upon crossing a preset threshold. If users want to benefit from traps for monitoring, which is an excellent idea in terms of proactive monitoring, they might have to configure traps first with the help of the SNMP manager.

- **InformRequest** – This messagetype was added inSNMPv2to give the manager the possibility to confirm that it received an agent's trap message. Some agents are configured to continueto send a trap until an inform message is received.
- **Report** – SNMP v3 is needed to use Report messages. They allow an SNMP manager to determine what kind of problem was detected bythe remote SNMP agent. Based on the detected error, the SNMP engine may try to send a corrected SNMP message. If that is not possible, it may pass an indication of the error to the application on whose behalf the failed SNMP request was issued. [RFC3412]

Reference Book: Computer Networks, Andrew Tanenbaum, 6th Edition.