MODULE1SECTIO

N:A,B,C,D

Topic	Portion
Introduction Chapter 1	Data Communications: Components, Representations, Data Flow,Networks: Physical Structures, Network Types: LAN, WAN, Switching,Internet
Network ModelsChapter 2	ProtocolLayering:Scenarios,Principles,LogicalConnections.
	TCP/IPProtocolSuite:LayeredArchitecture,LayersinTCP/IPsuite, Descriptionoflayers
	EncapsulationandDecapsulation,Addressing,Multiplexingand Demultiplexing,TheOSIModel: OSIVersusTCP/IP
Data-Link LayerChapter 11	Introduction:NodesandLinks,Services,Categories'oflink,Sublayers, LinkLayeraddressing:Typesofaddresses,ARP.
	DataLinkControl(DLC)services:Framing, Flowand ErrorControl,
	DataLinkLayerProtocols: SimpleProtocol,Stopand Waitprotocol, Piggybacking

TEXTBOOK:DataCommunicationsand Networking,B Forouzan**,**5thEd,McGrawHillEducation, 2016,ISBN:1-25-906475-3

MODULE1

Datacommunications

Whenwecommunicate,wearesharinginformation.Thissharingcanbelocalorremote.Between individuals,

local communication usually occurs face to face, while remote communication takes place overdistance.

Theterm**telecommunication**,whichincludestelephony,telegraphy, andtelevision,meanscommunication at a distance (tele is Greek for “far”). The word data refers to informationpresented in whateverform isagreeduponbythe partiescreatingandusingthedata.

Datacommunicationsaretheexchangeofdatabetweentwodevicesviasomeformoftransmissionmediumsuchasawirecable.Fordatacommunicationstooccur,thecommunicating devices must be part of a communication system made up of a combination ofhardware(physicalequipment)andsoftware(programs).Theeffectivenessofadatacommunicationssystemdependsonfourfundamentalcharacteristics:delivery,accuracy,timeliness, andjitter.

1. **Delivery**-The system must deliver data to the correct destination. Data must be received bytheintendeddeviceoruserand only bythatdeviceoruser.

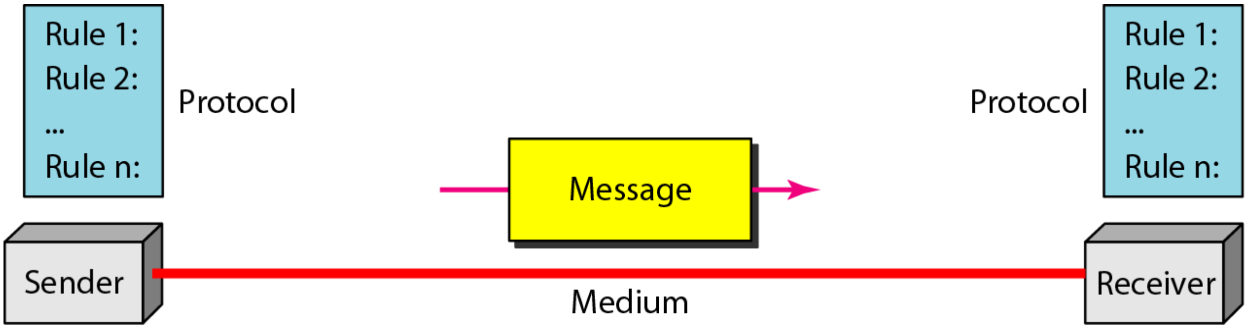
2. **Accuracy**- The system must deliver the data accurately. Data that have been altered intransmission andleftuncorrectedareunusable.

3. **Timeliness**. The system must deliver data in a timely manner. Data delivered late are useless.In the case of video and audio, timely delivery means delivering data as they are produced, inthe same order that they are produced, and without significant delay. This kind of delivery iscalledreal-timetransmission.

4. **Jitter**. Jitter refers to the variation in the packet arrival time. It is the uneven delay in thedelivery of audio or video packets. For example, let us assume that video packets are sent every30 ms. If some of the packets arrive with 30-ms delay and others with 40-ms delay, an unevenqualityinthevideoistheresult.

Components

Adatacommunicationssystemhasfivecomponents



1. **Message-.** The message is the information (data) to be communicated. Popular forms ofinformation includetext,numbers,pictures,audio,andvideo.

2. **Sender**-. The sender is the device that sends the data message. It can be a computer,workstation,telephonehandset,videocamera,andsoon.

3. **Receiver**-.Thereceiveristhedevicethatreceivesthemessage.Itcanbeacomputer,workstation ,telephonehandset,television,andsoon

4. **Transmission medium-.** The transmission medium is the physical path by which a messagetravels fromsender toreceiver. Someexamples oftransmissionmedia includetwisted-pairwire, coaxial cable,fiber-optic cable, andradiowaves.

5. **Protocol-**. A protocol is a set of rules that govern data communications. It represents anagreementbetweenthecommunicatingdevices.Withoutaprotocol,twodevicesmaybeconnected but not communicating, just as a person speaking French cannot be understood by apersonwhospeaks onlyJapanese.

DataRepresentation

Informationtodaycomesindifferentformssuchastext,numbers,images, audio, andvideo.

Text -In data communications, text is represented as a bit pattern, a sequence of bits (0s or 1s).Different sets of bit patterns have been designed to represent text symbols. Each set is called acode, and the process of representing symbols is called coding. Today, the prevalent codingsystem is called **Unicode**, which uses 32 bits to represent a symbol or character used in anylanguageintheworld.TheAmericanStandardCodeforInformationInterchange(ASCII),developed some decades ago in the United States, now constitutes the first 127 characters inUnicode andis alsoreferredtoasBasic Latin.

Numbers- are also represented by bit patterns. However, a code such as ASCII is not used torepresentnumbers;thenumberisdirectlyconvertedtoabinarynumbertosimplifymathematical operations. Appendix B discusses several different numbering systems. Images**Images**- are also represented by bit patterns. In its simplest form, an image is composed of amatrixofpixels(pictureelements),whereeachpixelisasmalldot.Thesizeofthepixeldependsonthere solution.

For example, animage canbe dividedinto 1000 pixels or 10,000 pixels. Inthe secondcase,thereisabetterrepresentationoftheimage(betterresolution),butmorememoryisneede dto store the image. After an image is divided into pixels, each pixel is assigned a bit pattern. Thesize and the value of the pattern depend on the image. For an image made of only black and-white dots (e.g., a chessboard), a 1-bit pattern is enough to represent a pixel. If an image is notmade of pure white and pure black pixels, we can increase the size of the bit pattern to includegray scale. For example, to show four levels of gray scale, we can use 2-bit patterns. A blackpixel can be represented by 00, a dark gray pixel by 01, a light gray pixel by 10, and a white pixelby11.Thereareseveralmethodstorepresentcolorimages.OnemethodiscalledRGB,socalled because each color is made of a combination of three primary colors: red, green, andblue. The intensity of each color is measured, and a bit pattern is assigned toit. Another methodis called YCM, in which a color is made of a combination of three other primary colors: yellow,cyan, andmagenta.

Audio- Audio refers to the recording or broadcasting of sound or music. Audio is by naturedifferent from text, numbers, or images. It is continuous, not discrete. Even when we use amicrophonetochange voice ormusicto anelectricsignal,we createa continuoussignal.

Video- Video refers to the recording or broadcasting of a picture or movie. Video can either beproduced as a continuous entity (e.g., by a TV camera), or it can be a combination of images,eachadiscreteentity,arrangedtoconveytheideaofmotion.

DataFlow

Communication between two devices can be simplex, half-duplex, or full-duplex as shown inFigure

simplexmode-thecommunicationisunidirectional,asonaone-waystreet.Onlyoneofthetwo devicesonalinkcantransmit;theother canonlyreceive(seeFigurea).

example-Keyboardsandtraditionalmonitorsareexamplesofsimplexdevices.Thekeyboardcanonlyin troduceinput;themonitor canonly acceptoutput.

simplexmode canuse theentirecapacityofthechanneltosenddata inonedirection

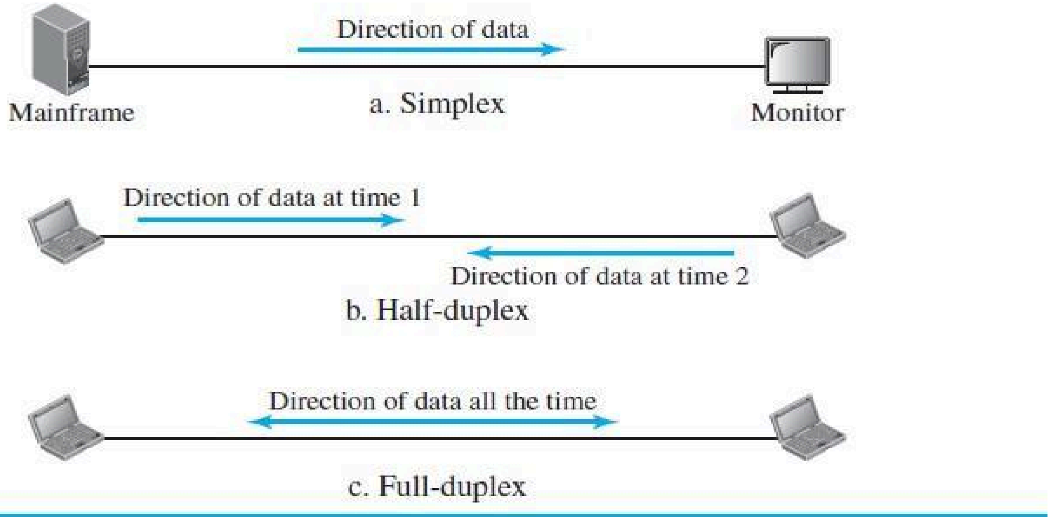

Direction of data
Mainframe
a. Simplex
Monitor
Direction of data at time 1
Direction of data at time 2
b. Half-duplex
Direction of data all the time
c. Full-duplex

fig:dataflow

Half-Duplex- In half-duplex mode, each station can both transmit and receive, but not at thesame time. When one device is sending, the other can only receive, and vice versa (see Figureb). The half-duplex mode is like a one-lane road with traffic allowed in both directions. Whencarsaretravelinginonedirection,carsgoingtheotherway mustwait.

example-Walkie-talkiesand CB(citizensband)radiosarebothhalf-duplexsystems.

The half-duplex mode is used in cases where there is no need for communication in bothdirectionsatthesametime;theentirecapacityofthechannelcanbeutilizedforeachdirection.

Full-Duplex- In full-duplex mode (also called duplex), both stations can transmit and receivesimultaneously (see Figure c). The full-duplex mode is like a two-way street with traffic flowingin both directions at the same time. In full-duplex mode, signals going in one direction share thecapacityofthelinkwithsignals goingintheotherdirection.

Thissharingcanoccurintwoways:Eitherthelinkmustcontaintwophysicallyseparatetransmissionpaths,oneforsendingandtheotherforreceiving;orthecapacityofthechannelisdividedbetweensignalstraveling inbothdirections.

NETWORKS

A network is the interconnection of a set of devices capable of communication. a device can bea host (or an end system as it is sometimes called) such as a large computer, desktop, laptop,workstation,cellularphone,orsecurity system.

A device can also be a connecting device such as a router, which connects the network to othernetworks,aswitch,whichconnectsdevicestogether,amodem(modulator-demodulator),whichchangestheformofdata,andsoon.

These devices in a network are connected using wired or wireless transmission media such ascable or air. When we connect two computers at home using a plug-and-play router, we havecreatedanetwork,althoughverysmall.

NetworkCriteria

A network must be able to meet a certain number of criteria. The most important of these areperformance,reliability,andsecurity.

Performance- Performance can be measured in many ways, including transit time and responsetime. Transit time is the amount of time required for a message to travel from one device toanother.Responsetimeistheelapsedtime between aninquiryand aresponse.

The performance of a network depends on a number of factors, including the number of users,thetypeoftransmissionmedium,thecapabilitiesoftheconnectedhardware,andtheefficiencyofthesoftware

Performanceisoftenevaluatedbytwonetworkingmetrics:throughputanddelay.

Reliability- network reliability is measured by thefrequency of failure, thetimeittakes a linkto recoverfromafailure,andthenetwork's robustnessinacatastrophe.

Security-security issues include protecting data from unauthorizedaccess, protecting datafrom damage and development, and implementing policies and procedures for recovery frombreachesanddatalosses.

PhysicalStructures

Networkattributes-TypeofConnectionandphysicaltopology

TypeofConnection

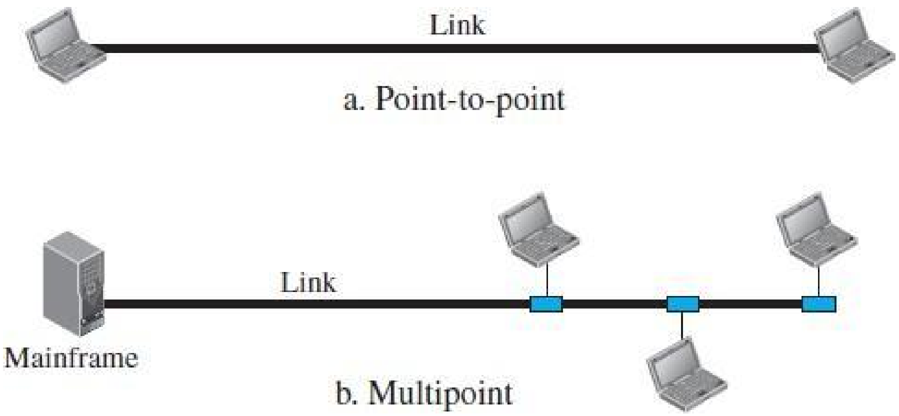
A network is two or more devices connected through links. A link is a communications pathwaythattransfersdatafromonedevicetoanother.

Therearetwopossible typesofconnections:

Point-to-Point-Apoint-to-pointconnectionprovidesadedicatedlinkbetweentwodevices.Theentire capacityofthelinkisreservedfortransmissionbetweenthosetwodevices.Most point-to-point connections use an actual length of wire or cable to connect the two ends, butother options, suchasmicrowave or satellite links, are also possible(see Figure a).

example-When we change television channels by infrared remote control, we are establishing apoint-to-point connectionbetweentheremotecontrol andthetelevision'scontrolsystem.

Multipoint A multipoint (also called multidrop) connection is one in which more than twospecificdevices shareasinglelink(seeFigureb).



a. Point-to-point

b. Multipoint

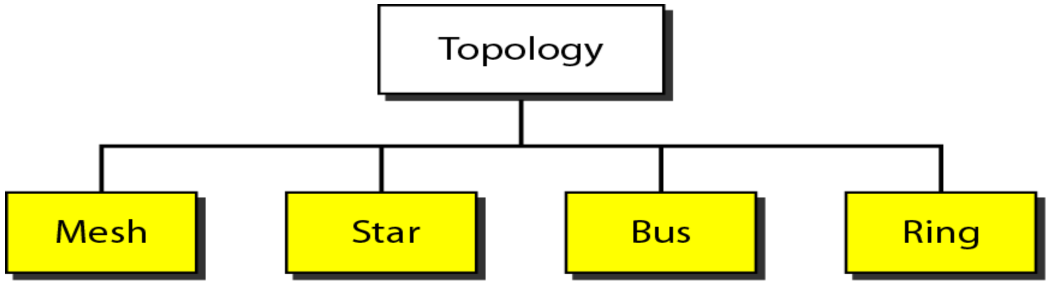
fig:Typeofconnection

amultipointenvironment,thecapacityofthechannelisshared,eitherspatiallyortemporally.If several devices can use the link simultaneously, it is a spatially shared connection. If usersmusttaketurns,itis atimesharedconnection.

PhysicalTopology

The term physical topology refers to the way in which a network is laid out physically. Two ormore devices connect to a link; two or more links form a topology. The topology of a network isthe geometric representation of the relationship of all the links and linking devices (usuallycalled nodes)tooneanother.

Thereare fourbasictopologiespossible: mesh,star,bus,andring.



Mesh Topology- In a mesh topology, every device has a dedicated point-to-point link to everyother device. The term dedicated means that the link carries traffic only between the twodevicesitconnects.

We need n (n – 1) physical links in a fully connected mesh network with n nodes.if eachphysical link allows communication in both directions (duplex mode),we need n (n – 1) / 2duplex-mode links.

To accommodate that many links, every device on the network must have n – 1 input/output(I/O)ports (seeFigure)tobeconnectedtotheothern–1stations.

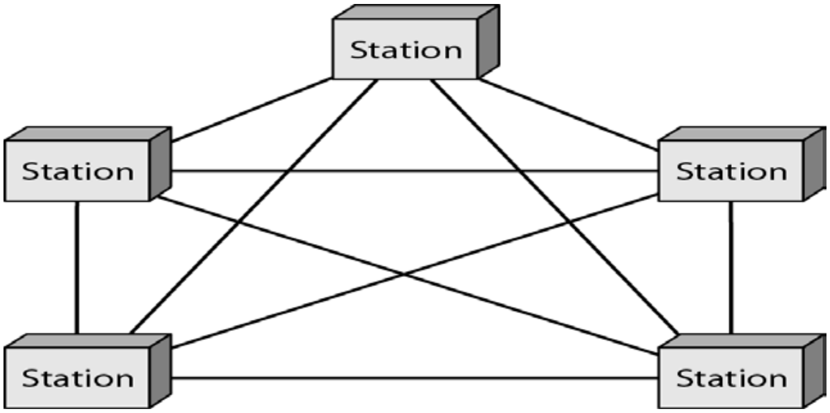
Advantages-

1. Use of dedicated links guarantees that each connection can carry its own data load, thuseliminatingthe trafficproblemsthat can occurwhenlinksmustbe sharedbymultipledevices.

2. A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entiresystem.

3. Privacy or security. When every message travels along a dedicated line, only the intendedrecipient seesit.Physicalboundariespreventother usersfrom gainingaccesstomessages.

4. Point-to-point links make fault identification and fault isolation easy. Traffic can be routed toavoid links with suspected problems. This facility enables the network manager to discover theprecise locationofthefaultandaidsinfinding itscauseandsolution.



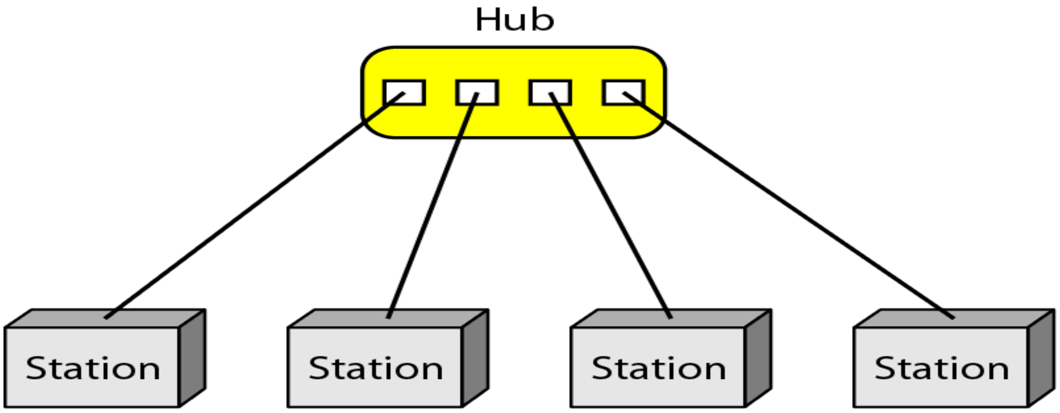
Afullyconnectedmeshtopology(fivedevices)

example- of a mesh topology is the connection of telephone regional offices in which eachregionalofficeneeds tobe connectedtoevery otherregionaloffice.

Star Topology

In a star topology, each device has a dedicated point-to-point link only to a central controller,usuallycalledahub.

The devices are not directly linked to one another.A star topology does not allow direct trafficbetween devices. The controller acts as an exchange: If one device wants to send data toanother, it sends the data to the controller, which then relays the data to the other connecteddevice



A star topology connecting four

stationsAdvantages

1. Astartopologyislessexpensivethan amesh topology.

2. Each device needs only one link and one I/O port to connect . This factormakes it easy toinstallandreconfigure.Farlesscablingneedstobehoused,andadditions,moves,anddeletionsinvolveonlyoneconnection:between thatdeviceandthehub.

3. robust. If one link fails, only that link is affected. All other links remain active. This factor alsolends itself to easy fault identification and fault isolation. As long as the hub is working, it can beusedtomonitorlinkproblems andbypassdefectivelinks.

Disadvantage

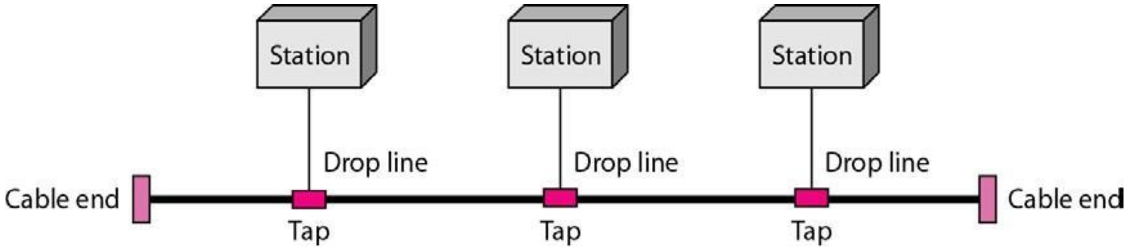
1. The dependency of the whole topology on one single point, the hub. If the hub goes down,thewholesystemisdead.

2. morecablingisrequired ina starthan insomeother topologies(suchasringorbus).

The star topology is used in local-area networks (LANs), High-speed LANs often use a startopologywithacentralhub.

BusTopology

Abustopology,ismultipoint.One longcableactsasabackbone to linkallthe devicesinanetwork



Nodesareconnectedtothebuscablebydroplinesandtaps.Adroplineisaconnectionrunningbetweenthedeviceandthemain cable.

A tap is a connector thateither splices into the main cable or punctures the sheathing of acable tocreateacontactwiththemetallic core.

As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, itbecomes weaker and weaker as it travels farther and farther. For this reason there is a limit onthenumberoftapsabuscansupportandonthedistancebetweenthosetaps.

Advantages

1. Easyto install.

2. bususeslesscablingthanmeshorstartopologies.Onlythebackbonecablestretchesthrough the entire facility. Each drop line has to reach only as far as the nearest point on thebackbone.

Disadvantages

1. Difficultreconnectionandfaultisolation.

2. Difficultto addnewdevices.

3. Signalreflectionatthetapscancausedegradationinquality.Thisdegradationcanbecontrolled by limiting the number and spacing of devices connectedto the given length of thecable

4. Addingnewdevicesrequiremodificationorreplacementofthe backbone.

5. a fault or break in the bus cable stops all transmission. The damaged area reflects signalsbackinthedirectionoforigin, creatingnoiseinbothdirections.

Bus topology was the one of the first topologies used in the design of early local area networks.TraditionalEthernetLANscanuse abustopology,buttheyare less popular now.

RingTopology

In a ring topology, each device has a dedicated point-to-point connection with only the twodevices on either side of it. A signal is passed along the ring in one direction, from device todevice, untilitreaches its destination.

Each device in the ring incorporates a repeater. When a device receives a signal intended foranotherdevice,its repeaterregeneratesthebitsandpassesthemalong

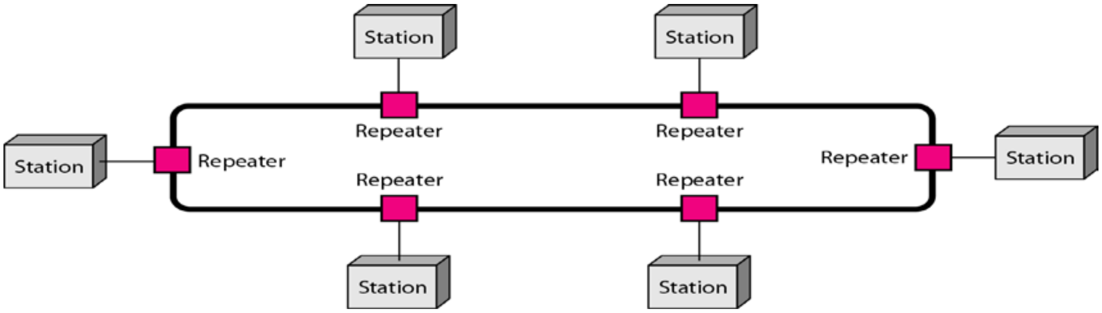


fig:Aringtopologyconnectingsixstations

Advantages

1. A ring is relatively easy to install and reconfigure. Each device is linked to only its immediateneighbors (either physically or logically). To add or delete a device requires changing only twoconnections.

2. Fault isolation issimplified.

Generally, in a ring a signal is circulating at all times. If one device does not receive a signalwithin a specified period, it can issue an alarm. The alarm alerts the network operator to theproblem andits location.

Disadvantage

In a simple ring, a break in the ring (such as a disabled station) can disable the entire network.Thisweaknesscan be solved byusingadualringor aswitchcapableofclosingoffthebreak.

Ring topology was prevalent when IBM introduced its local-area network, Token Ring. Today,theneedforhigher-speedLANshasmadethistopology lesspopular.

NETWORKTYPES

Differenttypesofnetworks

LocalAreaNetwork(LAN)-

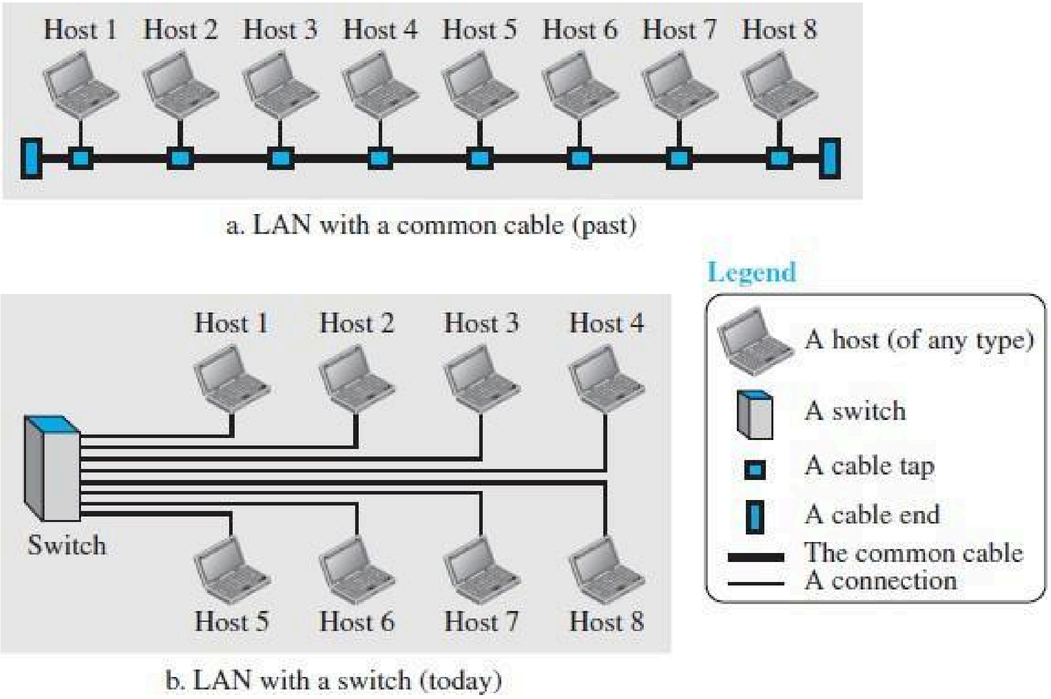


fig:AnisolatedLANinthepastandtoday

Alocalareanetwork (LAN) is usually privately ownedandconnects somehosts inasingleoffice,building,orcampus.Dependingontheneedsofanorganization,

A LAN can be as simple as two PCs and a printer in someone’s home office, or it can extendthroughoutacompanyand includeaudioand videodevices.

Each host in a LAN has an identifier, an address, that uniquely defines the host in the LAN. Apacket sent by a host to another host carries both the source host’s and the destination host’saddresses.

In the past, all hosts in a network were connected through a common cable, which meant that apacket sent from one host to another was received by all hosts. The intended recipient kept thepacket;theothersdroppedthepacket.

Today, most LANs use a smart **connecting switch**, which is able to recognize the destinationaddress of the packet and guide the packet to its destination without sending it to all otherhosts.TheswitchalleviatesthetrafficintheLANandallowsmorethanonepairtocommunicate with each other at the same time if there is no common source and destinationamongthem.

WideAreaNetwork

A wide area network (WAN) is also an interconnection of devices capable of communication.However, it. We see two distinct examples of WANs today: point-to-point WANs and switchedWANs.

Point-to-PointWAN

Apoint-to-pointWANisanetworkthatconnectstwocommunicatingdevicesthroughatransmissionmedia(cableorair).

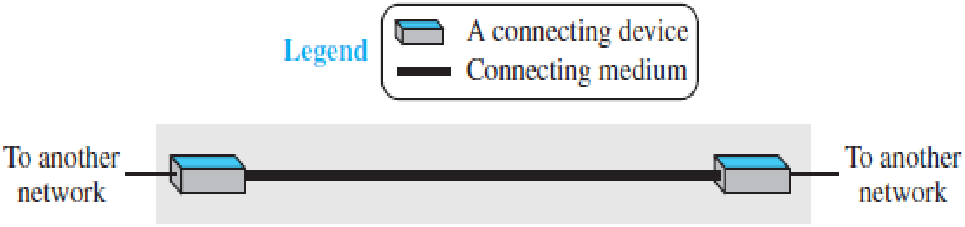


fig:Point-to-PointWAN

SwitchedWAN

A switched WAN is a network with more than two ends. A switched WAN,is used in thebackbone of global communication today. We can say that a switched WAN is a combination ofseveral point-to-pointWANs thatareconnectedbyswitches..

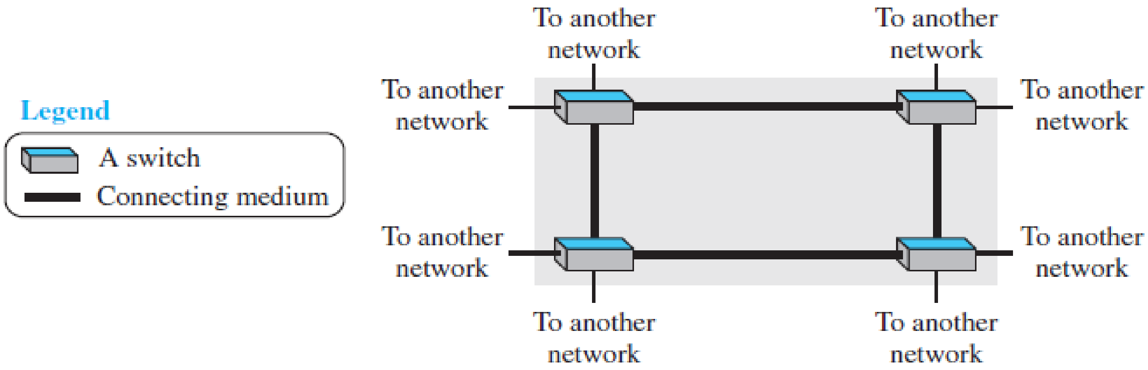


fig: A switched

WANLAN VS WAN

1. ALANisnormallylimitedinsize,spanningan office,abuilding,oracampus. 2. ALAN interconnectshosts 3. ALANisnormallyprivatelyownedbytheorganizationthatuses it	1. AWANhasawidergeographicalspan,spanninga town, a state, a country, or eventheworld 2. WAN interconnects connecting devices suchasswitches,routers,ormodems 3. aWANisnormallycreatedandrunbycommunication companies and leased by anorganizationthatuses it.

Internetwork

Today, it is very rare to see a LAN or a WAN in isolation; they are connected to one another.Whentwo or morenetworksare connected,theymake aninternetwork,or internet.

example-Assume that an organization has two offices, one on the east coast and the other onthe west coast. Each office has a LAN that allows all employees in the office to communicatewith each other. To make the communication between employees at different offices possible,the management leases a point-to-point dedicated WAN from a service provider, such as atelephone company, and connects the two LANs. Now the company has an internetwork, or aprivateinternet(withlowercase i).Communicationbetweenofficesisnowpossible.

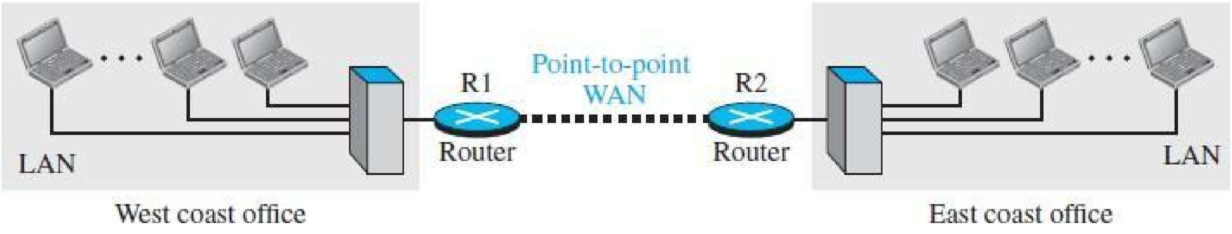


fig:AnnetworkmadeoftwoLANandpoint-to-pointdedicatedWAN

When a host in the west coast office sends a message to another host in the same office, therouter blocks the message, but the switch directs the message to the destination. On the otherhand, when a host on the west coast sends a message to a host on the east coast, router R1routes the packet to router R2, and the packet reaches the destination. Figure shows anotherinternet with several LANs and WANs connected. One of the WANs is a switched WAN with fourswitches.

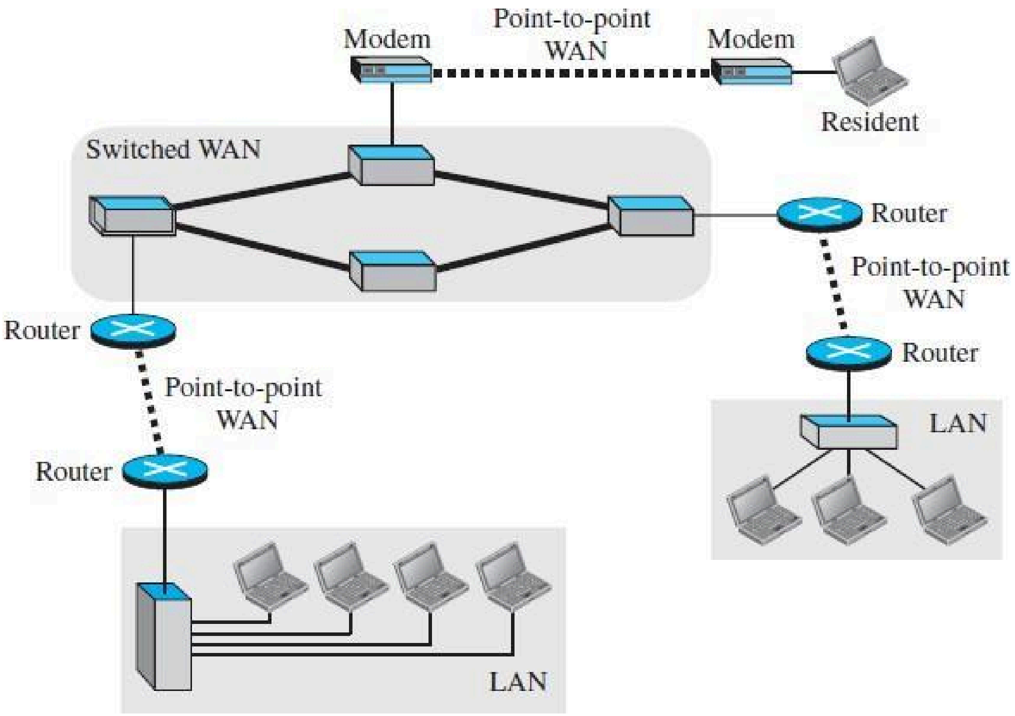


fig:A heterogeneousnetworkmadeoffourWANs andthreeLANs

Switching

An internet is a switched network in which a switch connects at least two links together. Aswitch needs to forward data from a network to another network when required. The two mostcommontypesofswitchednetworksarecircuit-switchedandpacket-switchednetworks.

Circuit-SwitchedNetwork

Inacircuit-switchednetwork,adedicatedconnection,calledacircuit,isalwaysavailablebetweenthetwoendsystems;theswitchcanonlymakeitactiveorinactive(continuouscommunicationbetweentwo telephone).FIGshowsaverysimpleswitchednetworkthatconnectsfourtelephonestoeachend.Wehaveusedtelephonesetsinsteadofcomputersasanend systembecausecircuitswitchingwasverycommon intelephonenetworksinthepast,

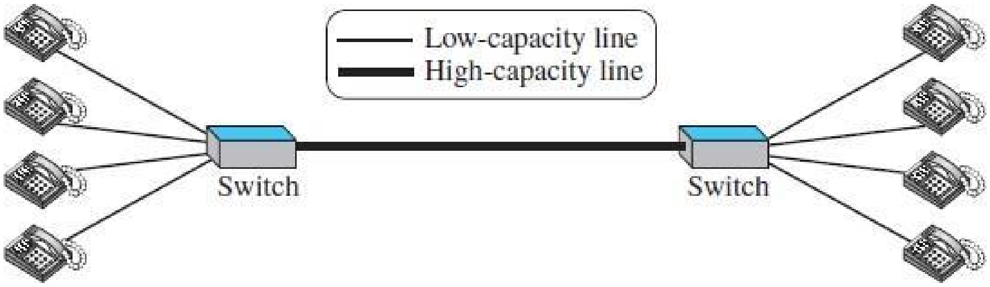


fig:Circuit-SwitchedNetwork

The thick line connecting two switches is a high-capacity communication line that can handlefour voice communications at the same time; the capacity can be shared between all pairs oftelephonesets.Theswitchesusedinthisexamplehaveforwardingtasksbutnostoringcapability.

Letuslookattwo cases.

In the first case,alltelephonesetsare busy;fourpeopleatonesite aretalkingwith fourpeople attheothersite;thecapacityof thethicklineisfullyused.

In the second case, only one telephone set at one side is connected to a telephone set at theother side; only one-fourth of the capacity of the thick line is used. This means that a circuit-switched network is efficient only when it is working at its full capacity; most of the time, it isinefficientbecauseitisworking atpartialcapacity.

The reason to make the capacity of the thick line four times the capacity of each voice line isthat we do not want communication to fail when all telephone sets at one side want to beconnected withalltelephonesetsattheotherside

Packet-SwitchedNetwork

In a computer network, the communication between the two computersis done in blocks ofdatacalledpackets

Thisallowsswitchestofunctionforbothstoringandforwardingbecauseapacketisanindependententit ythatcanbestoredandsentlater.Figshowsasmallpacket-switchednetworkthatconnectsfour computersatonesite tofourcomputersatthe othersite.

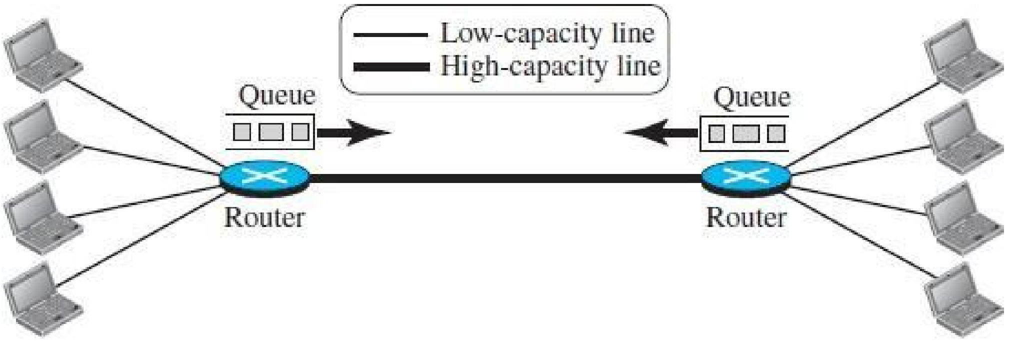


fig:**Packet-SwitchedNetwork**

Arouterina packet-switchednetworkhasaqueue thatcanstoreandforward thepacket.

Example- Now assume that the capacity of the thick line is only twice the capacity of the dataline connectingthecomputerstotherouters.

If only two computers (one at each site) need to communicate with each other, there is nowaiting for the packets. However, if packets arrive at one router when the thick line is alreadyworking at its full capacity, the packets should be stored and forwarded in the order theyarrived. The two simple examples show that a packet-switched network is more efficient than acircuitswitchednetwork, butthepacketsmay encounter somedelays.

TheInternet

An internet (note the lowercase i) is two or more networks that can communicate with eachother. The most notable internet is called the Internet (uppercase I), and is composed ofthousandsofinterconnectednetworks.

Figure 1.15 shows a conceptual (not geographical) view of the Internet. The figure shows theInternet as several backbones, provider networks, and customer networks. At the top level, thebackbonesarelargenetworksownedbysomecommunicationcompaniessuchasSprint,Verizon (MCI), AT&T, and NTT. The backbone networks are connected through some complexswitching systems, called peering points. At the second level, there are smaller networks, calledprovider networks, that use the services of the backbones for a fee. The provider networks areconnectedtobackbonesand sometimestootherprovidernetworks.

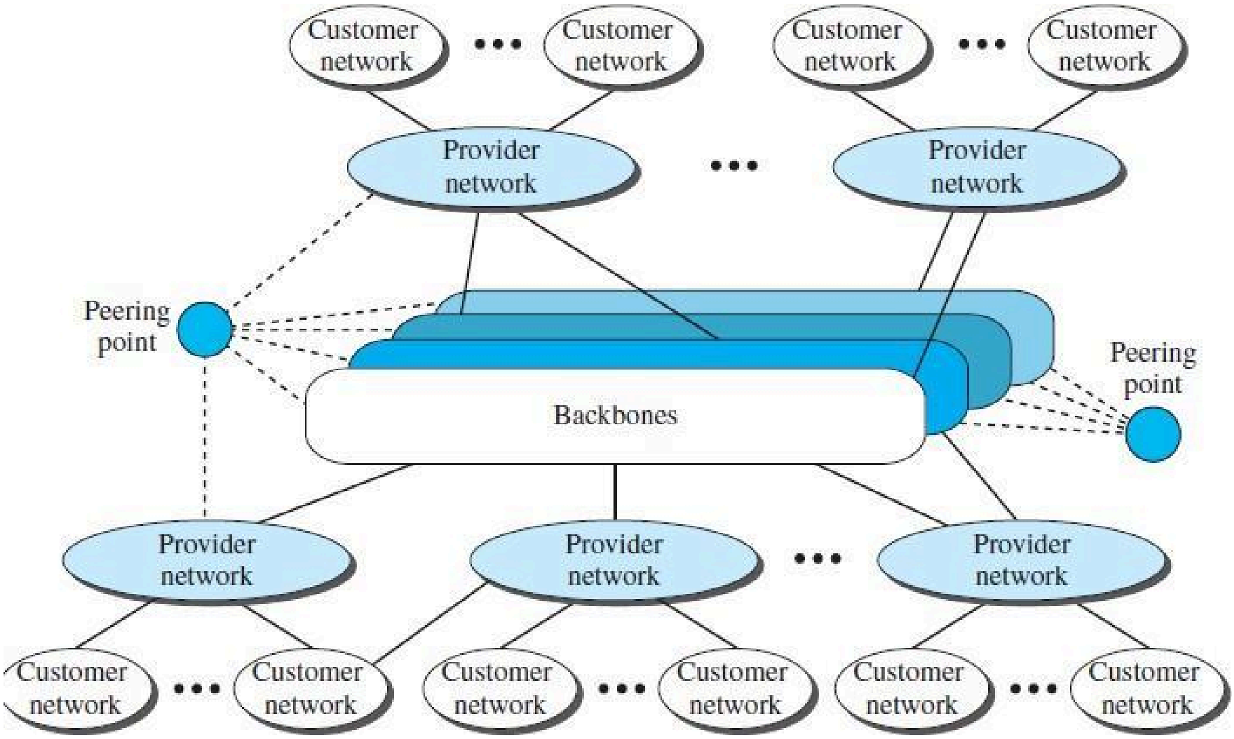


fig:Theinternettoday

The customer networks are networks at the edge of the Internet that actually use the servicesprovided by the Internet. They pay fees to provider networks for receiving services. Backbonesand provider networks are also called Internet Service Providers (ISPs). The backbones are oftenreferred to as international ISPs; the provider networks are often referred to as national orregionalISP

NetworkModels

ProtocolLayering

Protocol defines the rules that both the sender and receiver and all intermediate devices needtofollowtobeabletocommunicateeffectively.

Whencommunicationissimple,wemayneedonlyonesimpleprotocol;whenthecommunication is complex, we may need to divide the task between different layers, in whichcase weneedaprotocolateachlayer,orprotocollayering.

Letusdeveloptwosimplescenariostobetterunderstandtheneedforprotocollayering.

Scenarios

FirstScenario

In the first scenario, communication is so simple that it can occur in only one layer. AssumeMaria and Ann are neighbors with a lot of common ideas. Communication between Maria andAnntakesplace inone layer,facetoface,inthesame language,asshowninFigure

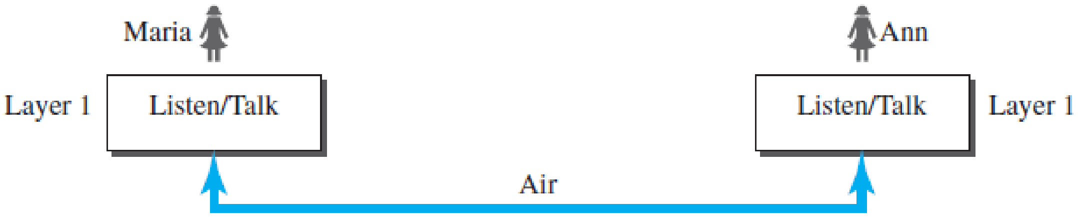


fig:singlelayerprotocol

SecondScenario

In the second scenario, we assume that Ann is offered a higher-level position in her company,but needs to move to another branch located in a city very far from Maria. The two friends stillwant to continue their communication and exchange ideas because they have come up with aninnovative project to start a new business when they both retire. They decide to continue theirconversation using regular mail through the post office. However, they do not want their ideastoberevealedbyotherpeopleifthelettersareintercepted.Theyagreeonanencryption/decryption technique. The sender of the letter encrypts it to make it unreadable byan intruder;thereceiveroftheletterdecrypts itto gettheoriginalletter.

Nowwecansaythatthecommunicationbetween MariaandAnntakesplaceinthreelayers,as shown in Figure . We assume that Ann and Maria each have three machines (or robots) thatcanperformthetaskateachlayer.

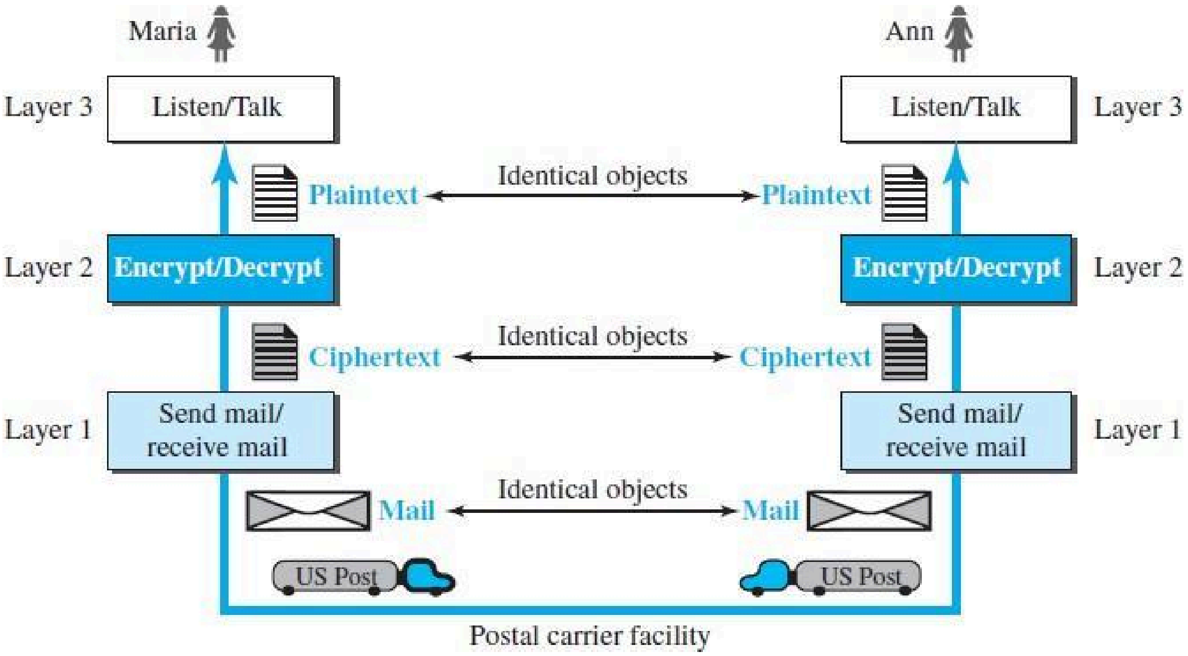


fig:Athreelayer protocol

Assume that Maria sends the first letter to Ann. Maria talks to the machine at the third layer asthough the machine is Ann and is listening to her. The third layer machine listens to what Mariasaysandcreatestheplaintext(a letterinEnglish),whichispassedtothe secondlayermachine.

The second layer machine takes the plaintext, encrypts it, and creates the ciphertext, which ispassedtothefirstlayermachine.Thefirstlayermachine,presumablyarobot,takestheciphertext,puts itin anenvelope, addsthesender and receiveraddresses,andmailsit

At Ann's side, the first layer machine picks up the letter from Ann's mail box, recognizing theletterfromMariabythesenderaddress.Themachinetakesouttheciphertextfromtheenvelope and delivers it to the second layer machine. The second layer machine decrypts themessage, creates the plaintext, and passes the plaintext to the third-layer machine. The thirdlayer machinetakes theplaintextandreadsitasthoughMariais speaking.

Needforprotocollayering

1) Protocollayeringenablesustodivideacomplextaskintoseveralsmallerand simplertasks.

Forexample,fromfig,wecouldhaveusedonlyonemachinetodothejobofallthreemachines.However,iftheencryption/decryptiondonebythemachineisnotenoughtoprotect their secrecy, they would have to change the whole machine. In the present situation,they need to change only the second layer machine; the other two can remain the same. This isreferredtoasmodularity. Modularityinthiscasemeansindependentlayers.

2) A layer (module) can be defined as a black box with inputs and outputs, without concernabout how inputs are changed to outputs. If two machines provide the same outputs whengiventhesameinputs,they canreplaceeachother.

Forexample,AnnandMariacanbuythesecondlayermachinefromtwodifferentmanufacturers.Aslongasthetwomachinescreatethesameciphertextfromthesameplaintextandviceversa,theydothejob.

advantages

1) Protocol layering allows to separate the services from the implementation. Lower layergivetheservices totheupperlayer;wedon’tcareabouthowthelayerisimplemented.

Forexample, Maria may decide notto buy the machine (robot) for the firstlayer; she candothe job herself. As long as Maria can do the tasks provided by the first layer, in both directions,thecommunicationsystemworks.

2) Protocol layering in the Internet, is that communication does not always use only two endsystems; there are intermediate systems that need only some layers, but not all layers. If we didnot use protocol layering, we would have to make each intermediate system as complex as theendsystems,whichmakesthewholesystemmoreexpensive.

Principlesof ProtocolLayering

First Principle The first principle dictates that if we want bidirectional communication, we needtomakeeachlayer sothatitisabletoperform**two oppositetasks**,one in eachdirection.

For example, the third layer task is to listen (in one direction) and talk (in the other direction).The second layer needs to be able to encrypt and decrypt. The first layer needs to send andreceive mail.

SecondPrincipleThesecondprinciplethatweneedtofollowinprotocollayeringisthatthe **twoobjects**under eachlayer atbothsitesshouldbe**identical**.

Forexample,theobjectunderlayer3atbothsitesshouldbeaplaintextletter.Theobjectunder layer 2 at both sites should be a cipher text letter. The object under layer 1 at both sitesshouldbeapieceofmail.

LogicalConnections

After following the above two principles, we can think about logical connection between eachlayer as shown in Figure . This means that we have layer-to-layer communication. Maria andAnncanthink thatthere is a logical (imaginary) connection at each layer through which theycan send the object created from that layer. We will see that the concept of logical connectionwill help us better understand the task of layering we encounter in data communication andnetworking.

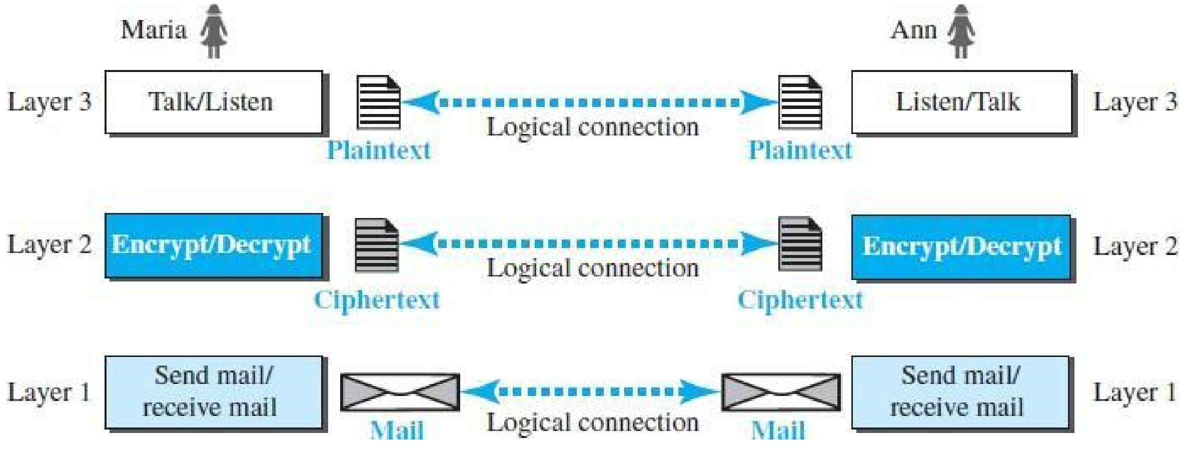


fig:Logicalconnectionbetweenpeerlayer

TCP/IPPROTOCOLSUITE

TCP/IP is a protocol suite (a set of protocols organized in different layers) used in the Internettoday. It is a hierarchical protocol made up of interactive modules, each of which provides aspecific functionality. The term hierarchical means that each upper level protocol is supportedbytheservicesprovidedbyoneormorelowerlevelprotocols.TheoriginalTCP/IPprotocolsuite was defined as four software layers built upon the hardware. Today, however, TCP/IP isthoughtofasafive-layermodel. Figureshowsbothconfigurations.

LayeredArchitecture

To show how the layers in the TCP/IP protocol suite are involved in communication betweentwohosts,weassumethatwewanttousethesuiteinasmallinternetmadeupofthreeLANs (links),eachwithalink-layerswitch.Wealsoassumethatthelinksareconnectedbyonerouter, asshowninFigure

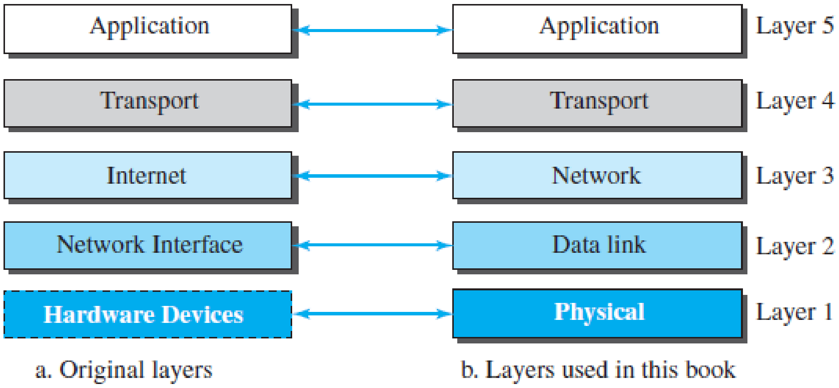


fig:layers inTCP/IPprotocolsuite

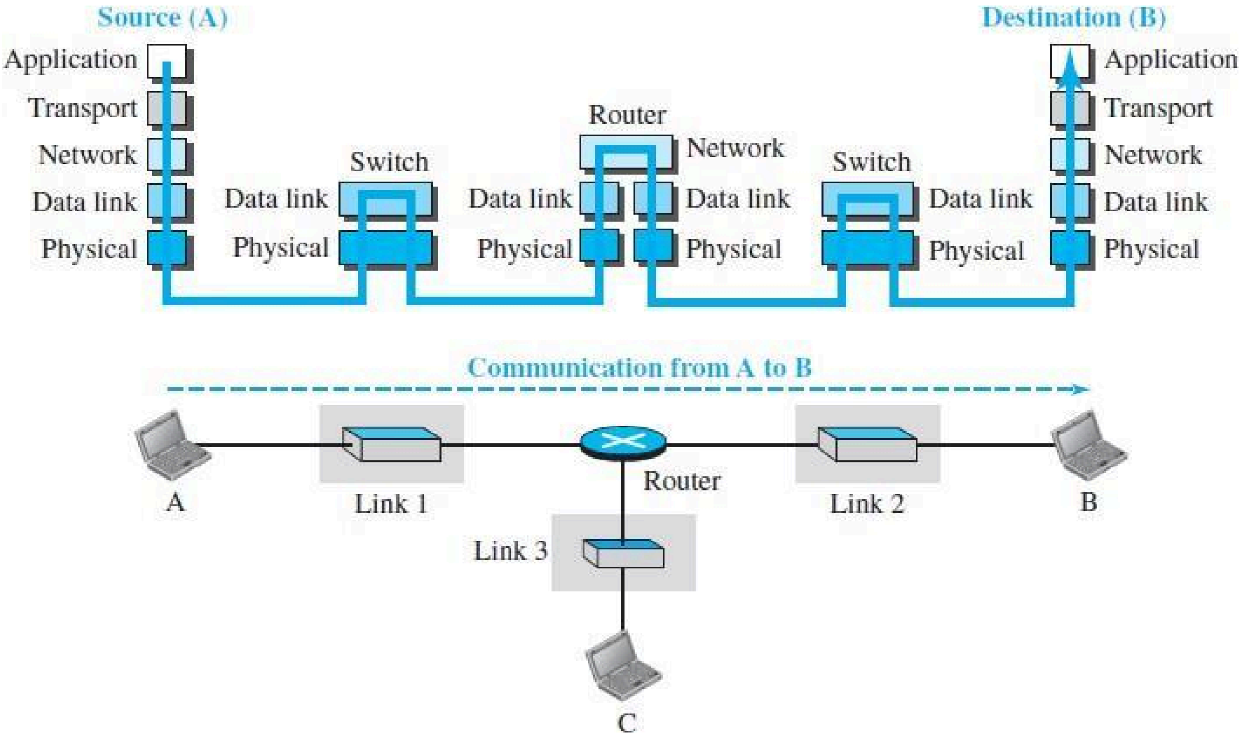


fig:Communicationthroughaninternet

AssumethatcomputerAcommunicateswithcomputerB.Asthefigureshows,fivecommunicating devices in this communication: source host (computer A), the link-layer switchin link1,therouter,thelink-layer switchinlink2,andthedestinationhost(computerB).

The source host needs to create a message in the application layer and send it down the layersso that it is physically sent to the destination host. The destination host needs to receive thecommunicationatthephysicallayerandthendeliveritthroughtheotherlayerstotheapplicationlayer

The router is involved in only three layers; there is no transport or application layer in a router.Although a **router is always involved in one network layer**, it is involved in n combinations oflink and physical layers in which n is the number of links the router is connected to. The reasonisthateachlinkmayuseits owndata-linkorphysicalprotocol.

Forexample,intheabovefigure,therouterisinvolvedinthreelinks,butthemessagesentfrom source A to destination B is involved in **two links**. Each link may be using **different link-layer and physical-layer protocols**; the router needs to receive a packet from link 1 based ononepairofprotocolsanddeliverittolink2basedonanotherpairofprotocols.

A link-layer switch in a link, however, is involved only in two layers, data-link and physical.Although each switch in the above figure has two different connections, the connections are inthe **same link,** which uses **only one set of protocols**. This means that, unlike a router, a link-layer switchisinvolvedonly inonedata-linkandonephysical layer.

Layersin theTCP/IPProtocolSuite

To better understand the duties of each layer, we need to think about the logical connectionsbetweenlayers.

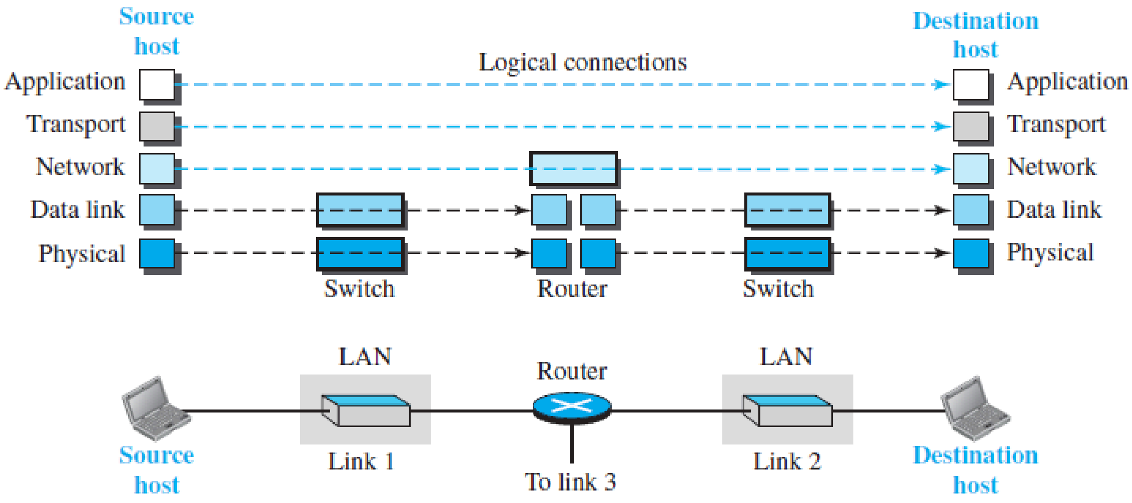


fig:Figureshowslogicalconnectionsinoursimpleinternet.

Using logical connections makes it easierto think about the duty of each layer. As the figureshows, the duty of the application, transport, and network layers is **end-to-end**. However, thedutyofthedata-linkandphysicallayersis**hop-to-hop**,inwhichahopisahostor router.

In other words, the domain of duty of the top three layers is the **internet**, and the domain ofdutyofthetwolowerlayers is the**link**.

Another way of thinking of the logical connections is to think about the data unit created fromeach layer. In the top three layers, the data unit (packets) should not be changed by any routeror link-layer switch. In the bottom two layers, the packet created by the host is changed only bytherouters,notby thelink-layerswitches.

Fig shows the second principle discussed previously for protocol layering. We show the identicalobjectsbeloweachlayerrelatedtoeachdevice.

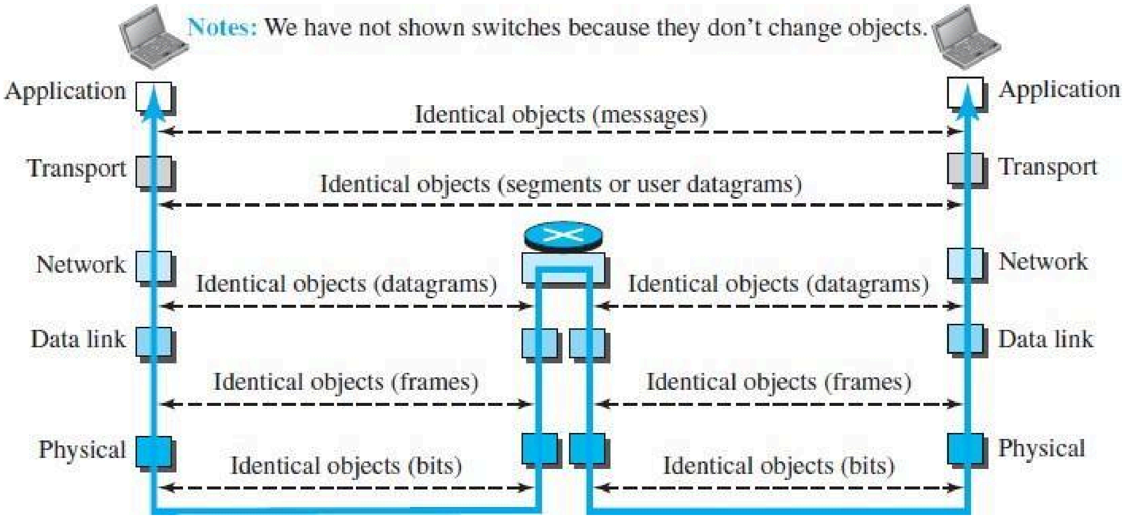

Notes: We have not shown switches because they don't change objects.
Application
Transport
Network
Data link
Physical
Identical objects (messages)
Identical objects (segments or user datagrams)
Identical objects (datagrams)
Identical objects (datagrams)
Identical objects (frames)
Identical objects (frames)
Identical objects (bits)
Identical objects (bits)
Application
Transport
Network
Data link
Physical

fig:identicalobjectsin theTCP/IPprotocolsuite

Note that, although the logical connection at the network layer is between the two hosts, wecan only say that identical objects exist between two hops in this case because a router mayfragment the packet at the network layer and send more packets than received .Note that thelinkbetweentwohopsdoes notchangetheobject.

DescriptionofEachLayer

PhysicalLayer

Physical layer is responsible for **carrying individual bits** in a frame across the link. Although thephysical layer is the lowest level in the TCP/IP protocol suite, the communication between twodevices at the physical layer is still a logical communication because there is another, hiddenlayer, thetransmissionmedia,underthephysicallayer.

Two devices are connected by a transmission medium (cable or air). Transmission medium doesnot carry bits, **it carries electrical or optical signals**. So the bits received in a frame from thedata-link layer are transformed and sent through the transmission media, but we can think thatthe logical unit between two physical layers in two devices is a bit. There are several protocolsthattransformabittoasignal.

The physical layer of TCP/IP describes hardware standards such as IEEE 802.3, the specificationforEthernetnetworkmedia, and RS-232, thespecificationfor standardpinconnectors.

Thefollowingarethemainresponsibilitiesofthephysicallayer

DefinitionofHardwareSpecifications,EncodingandSignaling,DataTransmissionandReception,TopologyandPhysicalNetwork Design

Data-linkLayer

Internet is made up of several links (LANs and WANs) connected by routers. The data-link layerisresponsiblefortakingthedatagramandmovingitacrossthelink.(nodetonodecommunication)

The link can be a wired LAN with a link-layer switch, a wireless LAN, a wired WAN, or a wirelessWAN.Wecanalsohavedifferentprotocolsusedwithanylinktype.

In each case, the data-link layer is responsible for moving the packet through the link. TCP/IPdoes not define any specific protocol for the data-link layer. It supports all the standard andproprietary protocols. The data-link layer takes a datagram andencapsulates itin a packetcalleda**frame**.

Each link-layer protocolprovide a different service like framing, Flow control, Error controland congestioncontrol.

NetworkLayer

The network layer is responsible for creating a connection between the source computer andthe destination computer. The communication at the network layer is **host-to-host**. However,sincetherecanbeseveralroutersfromthesourcetothedestination,theroutersinthepathare responsibleforchoosing the**bestroute**foreachpacket.

The network layer is responsible packetizing and routingand forwarding the packet throughpossibleroutes.others servicesareerrorandflowcontrol,congestioncontrol.

ThenetworklayerintheInternetincludesthemainprotocol,InternetProtocol(IP),thatdefines the format of the packet, **called a datagram** at the network layer. IP also defines theformatandthestructureofaddressesusedinthis layer.

IP is also responsible for routing a packet from its source to its destination, which is achieved byeach routerforwarding thedatagramtothenextrouterin its path.

IPisaconnectionlessprotocolthatprovidesnoflowcontrol,noerrorcontrol,andnocongestioncontrol services.Thismeansthatifanyoftheseservicesisrequiredforanapplication,theapplication should relyonlyonthetransport-layerprotocol.

Thenetworklayeralsoincludesunicast(one-to-one)andmulticast(one-to-many)routingprotocols. A routing protocol does not take part in routing (it is the responsibility of IP), but itcreatesforwardingtablesforrouterstohelpthemintheroutingprocess.Thenetworklayeralso hassomeauxiliaryprotocolsthathelpIPinitsdeliveryandroutingtasks.

The Internet Control Message Protocol (ICMP) helps IP to report some problems when routing apacket. The Internet Group Management Protocol (IGMP) is another protocol that helps IP inmultitasking. The Dynamic Host Configuration Protocol (DHCP) helps IP to get the network-layeraddress for a host. The Address Resolution Protocol (ARP) is a protocol that helps IP to find thelink-layer addressofahostorarouter when itsnetwork-layer addressisgiven.

TransportLayer

The logical connection at the transport layer is also end-to-end. The transport layer at thesource host gets the message from the application layer, encapsulates it in a transport layerpacket (called a segment or a user datagram in different protocols) and sends it, through thelogical (imaginary) connection,tothetransportlayeratthedestinationhost.

The transport layer is responsible for giving services to the application layer: to get a messagefrom an application program running on the source host and deliver it to the correspondingapplicationprogram onthedestinationhost.(**process toprocess coommunication**)

There are more than one protocol in the transport layer, which means that each applicationprogram can use the protocol that best matches its requirement. There are a few transport-layer protocolsintheInternet, eachdesignedforsomespecifictask.

The main protocol, **Transmission Control Protocol (TCP**), is a connection-oriented protocol thatfirst establishes a logical connection between transport layers at two hosts before transferringdata. It creates a logical pipe between two TCPs for transferring a stream of bytes. TCP providesflow control (matching the sending data rate of the source host with the receiving data rate ofthe destination host to prevent overwhelming the destination), error control (to guarantee thatthe segments arrive at the destination without error and resending the corrupted ones), andcongestion control to reducethelossofsegments dueto congestion inthe network.

User Datagram Protocol (UDP), is a connectionless protocol that transmits user datagramswithout first creating a logical connection. In UDP, each user datagram is an independent entitywithout being related to the previous or the next one (the meaning of the term connectionless).UDP isasimple protocolthatdoesnotprovideflow, error,or congestioncontrol.

Itssimplicity,whichmeanssmalloverhead,isattractivetoanapplicationprogramthatneedsto send short messages and cannot afford the retransmission of the packets involved in TCP,when apacketis corruptedorlost.

A new protocol, Stream Control Transmission Protocol (SCTP) is designed to respond to newapplicationsthatareemerging inthemultimedia.

ApplicationLayer

As Figureshows, the logical connection between the two application layers is end to-end. Thetwo application layers exchange messages between each other as though there were a bridgebetweenthetwo layers.However, communicationisdone throughallthelayers.

Communication at the application layer is between two processes (two programs running atthis layer). To communicate, a process sends a request to the other process and receives aresponse.Process-to-processcommunicationisthe dutyofthe applicationlayer.

Theapplicationlayer intheInternetincludesmanypredefinedprotocols.

1) TheHypertextTransferProtocol(HTTP)isavehicleforaccessingtheWorldWideWeb(WWW).

2) TheSimpleMailTransferProtocol(SMTP)isthemainprotocolusedinelectronicmail(e-mail)ser vice.

3) TheFile TransferProtocol(FTP)isusedfortransferringfilesfromonehosttoanother.

4)TheTerminalNetwork(TELNET)andSecureShell(SSH)areusedforaccessingasite remotely.

5) TheSimpleNetworkManagementProtocol(SNMP)isusedbyanadministratortomanagetheInternetatglobalandlocallevels.

6) The Domain Name System (DNS) is used by other protocols to find the network-layer addressofacomputer.

7) TheInternet GroupManagementProtocol(IGMP)isusedtocollectmembershipinagroup.

EncapsulationandDecapsulation

OneoftheimportantconceptsinprotocollayeringintheInternetisencapsulation/decapsulation.Figureshows this conceptforthesmallinternet

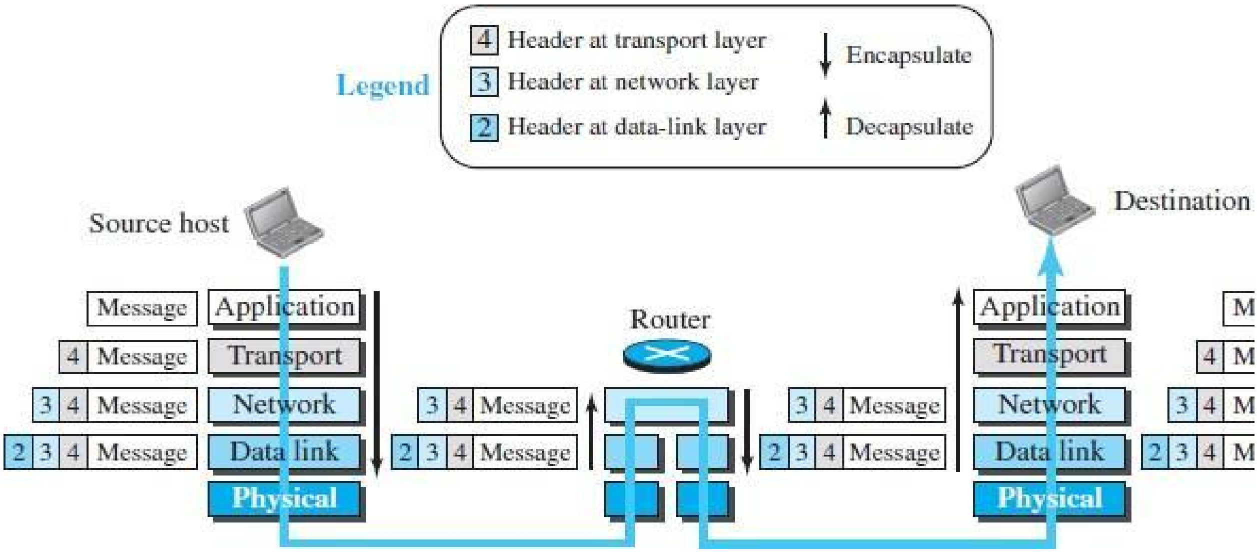


***fig:*encapsulation/decapsulation**

Wehavenotshownthelayersforthelink-layerswitchesbecausenoencapsulation/decapsulationoccursinthisdevice.Figureshowtheencapsulationinthesourcehost,decapsulationinthedestinationhost, and encapsulation anddecapsulation inthe router.

EncapsulationattheSourceHost

Atthesource,we haveonlyencapsulation.

1. At the application layer, the data to be exchanged is referred to as a message. A messagenormally does not contain any header or trailer, but if it does, we refer to the whole as themessage.Themessageispassedtothetransportlayer.

2. The transport layer takes the message as the payload, the load that the transport layershould take care of. It adds the transport layer header to the payload, which contains theidentifiers of the source and destination application programs that want to communicate plussome more information that is needed for the end-to end delivery of the message, such asinformation needed for flow, error control, or congestion control. The result is the transport-layerpacket,whichiscalledthesegment(inTCP)andtheuserdatagram(inUDP).Thetransportlayerthenpasses thepackettothenetworklayer.

3. The network layer takes the transport-layer packet as data or payload and adds its ownheader to the payload. The header contains the addresses of the source and destination hostsand some more information used for error checking of the header, fragmentation information,and so on. The result is the network-layer packet, called a datagram. The network layer thenpassesthepackettothedata-linklayer.

4. The data-link layer takes the network-layer packet as data or payload and adds its ownheader, which contains the link-layer addresses of the host or the next hop (the router). Theresult is the link-layer packet, which is called a frame. The frame is passed to the physical layerfortransmission.

DecapsulationandEncapsulationattheRouter

Attherouter,wehavebothdecapsulationandencapsulationbecausetherouterisconnectedtotwoormorelinks.

1. After the set of bits are delivered to the data-link layer, this layer decapsulates the datagramfromtheframeandpasses ittothenetworklayer.

2. The network layer only inspects the source anddestinationaddresses inthe datagramheader and consults its forwarding table to find the next hop to which the datagram is to bedelivered. The contents of the datagram should not be changed by the network layer in therouter unless there is a need to fragment the datagram if it is too big to be passed through thenextlink. Thedatagramis thenpassedtothedata-linklayerofthenextlink.

3. The data-link layer of the next link encapsulates the datagram in a frame and passes it to thephysical layerfortransmission.

DecapsulationattheDestinationHost

At the destination host, each layer only decapsulates the packet received, removes the payload,anddeliversthepayloadtothenext-higherlayerprotocoluntilthemessagereachestheapplicationlayer.Itisnecessarytosaythatdecapsulation inthehost involveserrorchecking

Addressing

we have logical communication between pairs of layers in this model. Any communication thatinvolves two parties needs two addresses: source address and destination address. Although itlooks as if we need five pairs of addresses, one pair per layer, we normally have only fourbecause **the physical layer does not need addresses**; the unit of data exchange at the physicallayer is abit,whichdefinitely cannothaveanaddress.

Figure 2.9 shows the addressing at each layer. At the application layer, we normally use namesto define the site that provides services, such as someorg.com, or the e-mail address, such assomebody@coldmail.com.

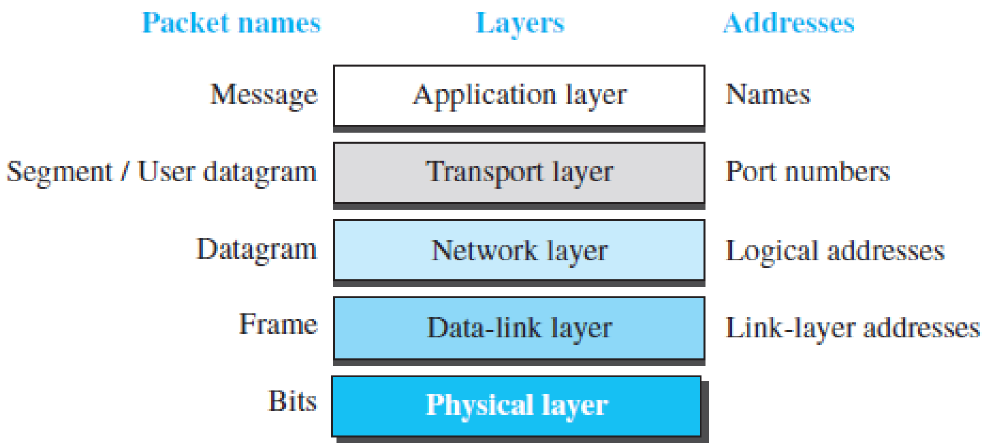


fig:AddressingintheTCP/IPProtocolsuite

At the transport layer, addresses are called port numbers, and these define the application-layer programs at the source and destination. Port numbers are local addresses that distinguishbetweenseveral programs runningatthesametime.

Atthenetwork-layer,theaddressesareglobal,withthewholeInternetasthescope.Anetwork-layeraddressuniquely definestheconnectionofadevicetotheInternet.

The link-layer addresses, sometimes called MAC addresses, are locally defined addresses, eachofwhichdefinesaspecific hostorrouterin anetwork(LANorWAN).

MultiplexingandDemultiplexing

TCP/IP protocol suite uses several protocols at some layers, we have multiplexing at the sourceanddemultiplexingatthedestination.

Multiplexingmeans that a protocol at a layer can encapsulate a packet from several next-higher layer protocols (one at a time); demultiplexing means that a protocol can decapsulateand deliver a packet to several next-higher layer protocols (one at a time). Figureshows theconceptofmultiplexinganddemultiplexingatthethreeupperlayers.

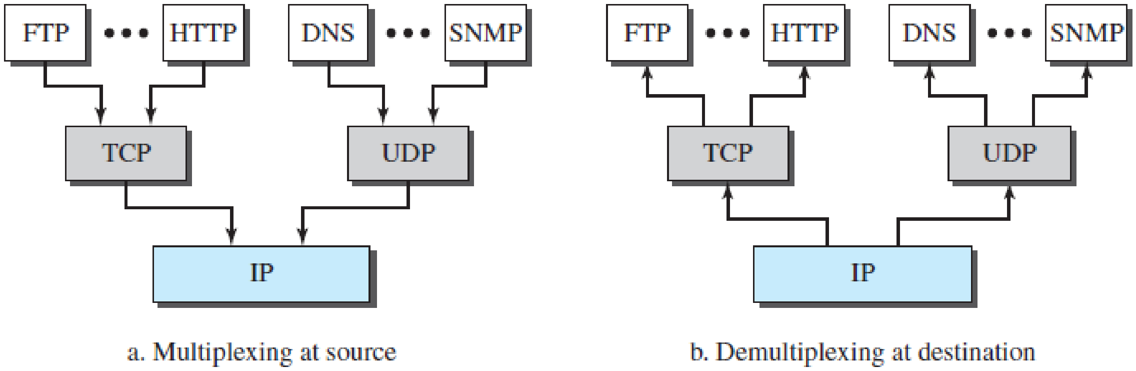


fig:multiplexinganddemultiplexing

Tobeabletomultiplexanddemultiplex,aprotocolneedstohaveafieldinitsheadertoidentifytowhichprotocoltheencapsulatedpackets belong.

At the transport layer, either UDP or TCP can accept a message from several application-layerprotocols.

At the network layer, IP can accept a segment from TCP or a user datagram from UDP. IP canalso acceptapacketfrom otherprotocolssuchas ICMP, IGMP,and soon.

At the data-link layer, a frame may carry the payload coming from IP or other protocols such asARP.

THEOSIMODEL

AnISOstandardthatcoversallaspectsofnetworkcommunicationsistheOpenSystemsInterconnection(OSI)model.Itwasfirst introduced inthelate 1970s.Anopen system isa setof protocols that allows any two different systems to communicate regardless of their underlyingarchitecture.

The purpose of the OSI model is to show how to facilitate communication between differentsystems without requiring changes to the logic of the underlying hardware and software.
The**OSImodelisnotaprotocol**;itisamodelforunderstandinganddesigninganetworkarchitecture that is flexible, robust, and interoperable. The OSI model was intended to be thebasisforthecreationoftheprotocolsintheOSIstack.TheOSImodelisalayeredframeworkfor the design of network systems that allows communication between all types of computersystems.

It consists of seven separate but related layers, each of which defines a part of the process ofmovinginformationacross anetwork

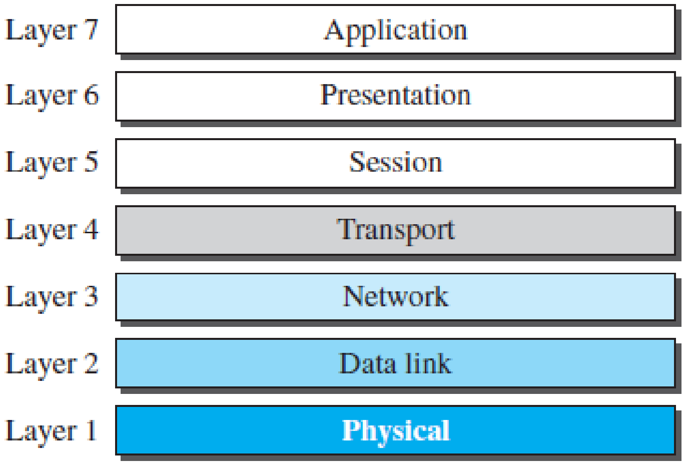


fig:OSImodelOSIv

ersusTCP/IP

When we compare the two models, we find that two layers, session and presentation, aremissing from the TCP/IP protocol suite. These two layers were not added to the TCP/IP protocolsuiteafterthepublicationoftheOSImodel.Theapplicationlayerinthesuiteisusuallyconsideredtobethe combinationofthreelayersintheOSImodel, asshowninFigure.

Two reasons were mentioned for this decision. First, TCP/IP has more than one transport-layerprotocol. Some of the functionalities of the session layer are available in some of the transport-layer protocols.

Second, the application layer is not only one piece ofsoftware. Many applications can bedevelopedatthislayer.Ifsomeofthefunctionalitiesmentionedinthesessionandpresentationlayers areneededforaparticularapplication,theycanbeincludedinthedevelopmentofthatpieceofsoftware
.

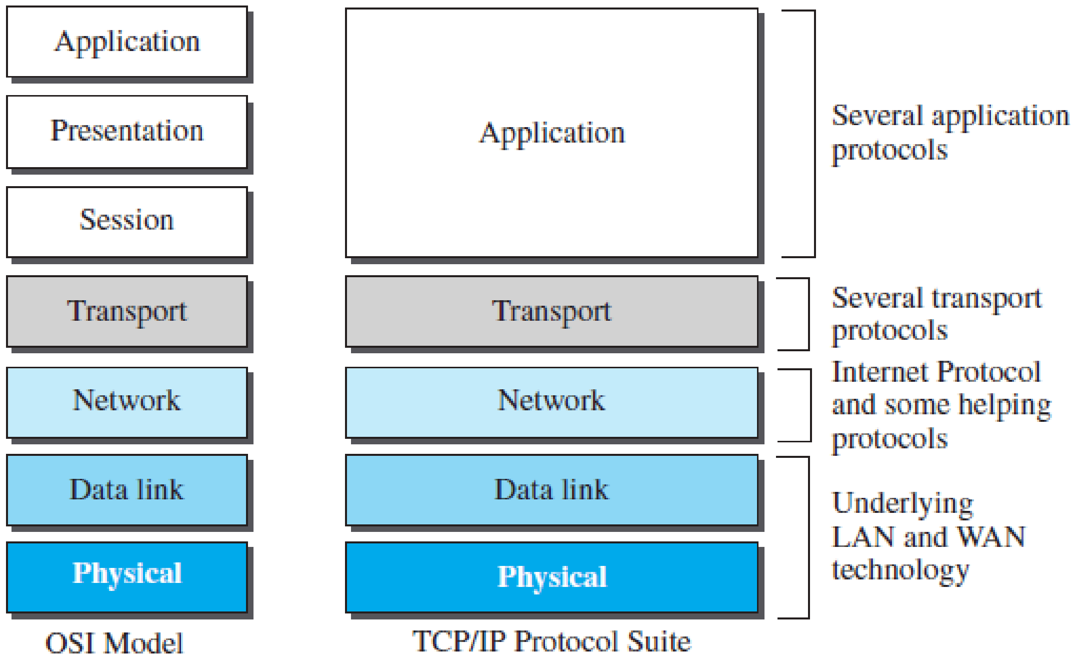


fig:TCP/IPandOSI model