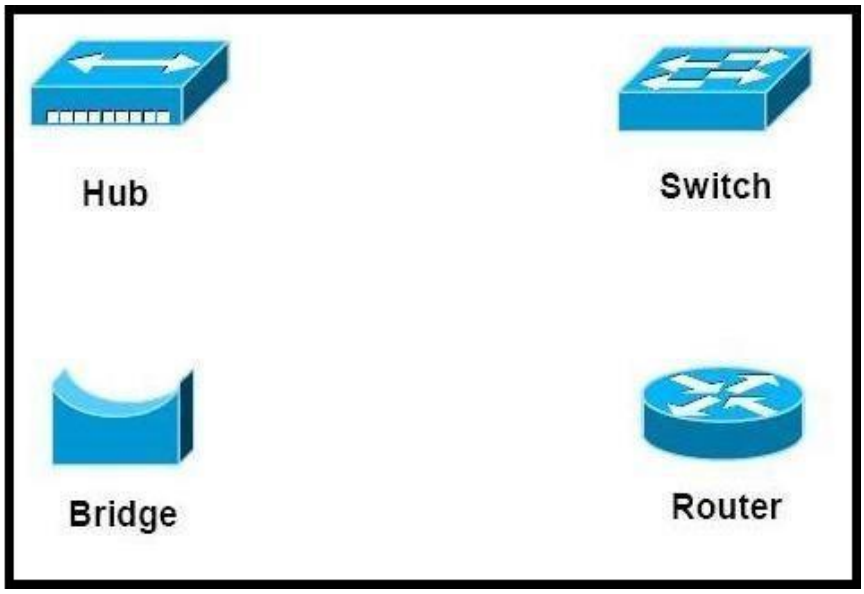
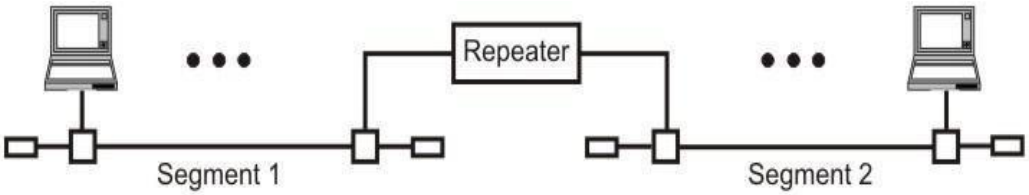
NetworkDevices(Hub,Repeater,Bridge,Switch, Router and Gateways)



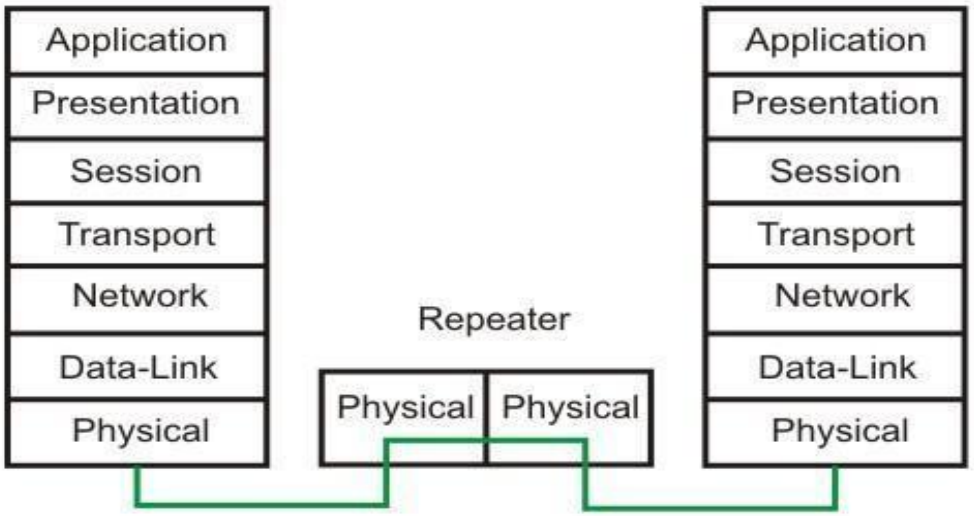
1. Repeater– A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do no amplify the signal. When the signal becomes weak, theycopythe signal bit by bit and regenerate it at the original strength. It is a 2 port device.

AsingleEthernet segment canhavea maximumlengthof500 meterswitha maximumof 100 stations (in a cheapernet segment it is 185m). To extend the length of the network, a *repeater* may be used as shown in Fig. 6.1.1. Functionally, a repeater can be consideredas two transceivers joined together and connected to two different segments of coaxial cable. The repeater passes the digital signal bit-by-bit in both directions between the two segments. As the signal passes through a repeater, it is amplified and regenerated at the other end. The repeater does not isolate one segment fromthe other, ifthere is a collision ononesegment, it isregeneratedontheother segment. Therefore,thetwo segments form a single LAN and it is transparent to rest ofthe system. Ethernet allows five segments to be used in cascade to have a maximum network span of 2.5 km. With reference of theISO model, a repeater is considered as a *level-1 relay* as depicted in Fig. 6.1.2. It simply repeats, retimes and amplifies the bits it receives. The repeater is merely used to extend the span of a single LAN. Important features of a repeater are as follows:

- ArepeaterconnectsdifferentsegmentsofaLAN
- Arepeaterforwardseveryframeitreceives
- Arepeaterisaregenerator,notanamplifier
- Itcanbeusedto createasingleextended LAN



FigureRepeaterconnectingtwo LANsegments

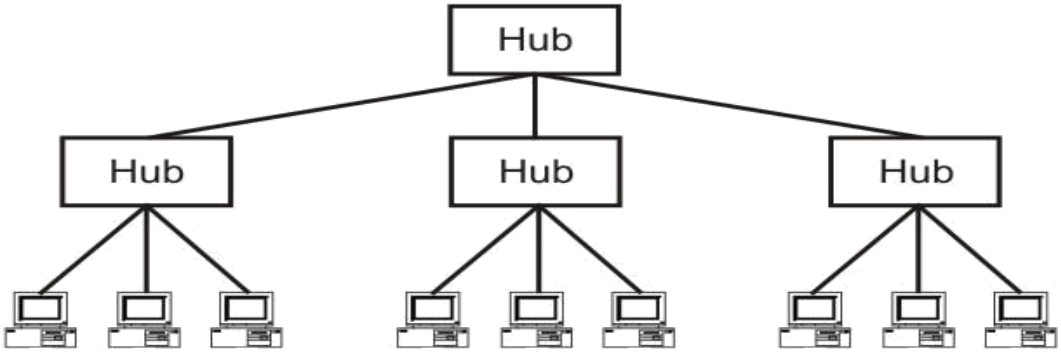


FigureOperationofa repeaterasa level-1relay

2. Hub –A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices.In other words, collision domain of all hosts connected through Hub remains one.Also, they do not have intelligence tofind out best path for data packets which leads to inefficiencies and wastage.

Hub is a generic term, but commonly refers to a multiport repeater. It can be used to create multiple levels of hierarchyofstations. The stations connect to the hubwithRJ-45 connectorhavingmaximumsegmentlengthis100meters.Thistypeofinterconnectedset

of stations is easy to maintain and diagnose. Figure shows how several hubs can be connected in a hierarchical manner to realize a single LAN of bigger size with a large number of nodes.



FigureHub as a multi-port repeater can be connected in a hierarchical manner to form a single LAN with many nodes

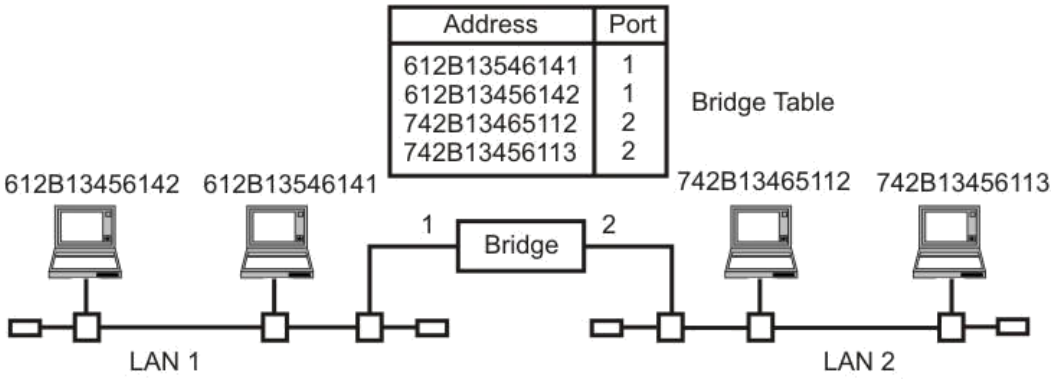
3. Bridge– A bridge operates at data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

The device that can be used to interconnect two separate LANs is known as a*bridge*. Itis commonlyused to connect two similar or dissimilar LANs as shown in Fig. 6.1.4. The bridge operates in layer 2, that is data-link layer and that is why it is called *level-2 relay* with reference to the OSI model. It links similar or dissimilar LANs, designed to storeand forward frames, it is protocol independent and transparent to the end stations. The flow of information through a bridge is shown in Fig. 6.1.5. Use of bridges offer anumber ofadvantages, such as higher reliability, performance, security, convenience and larger geographic coverage. But, it is desirable that the quality of service (QOS) offered by a bridge should match that of a single LAN. The parameters that define the QOS include *availability, frame mishaps, transit delay, frame lifetime, undetected bit errors, frame size* and *priority*. Key features of a bridge are mentioned below:

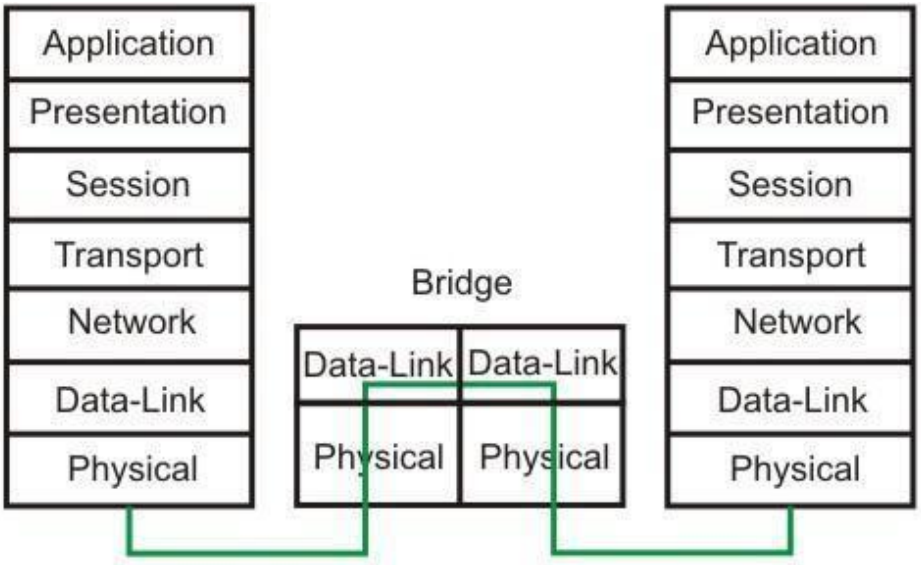
- Abridge operatesbothinphysicalanddata-linklayer
- Abridgeusesatablefor filtering/routing
- Abridgedoesnot changethephysical(MAC) addressesinaframe
- Typesofbridges:
    - ○TransparentBridges○
      Sourceroutingbridges

A bridge must contain addressing and routing capability. Two routing algorithms have been proposed for a bridged LAN environment. The first, produced as an extension of IEEE802.1andapplicabletoallIEEE802LANs,isknownas*transparentbridge*.And

the other, developed for the IEEE 802.5 token rings, is based on *source routingapproach*. It applies to many types of LAN including token ring, token bus and CSMA/CD bus.



FigureAbridgeconnectingtwoseparateLANs



FigureInformationflowthrougha bridge

4. Switch– A switch is a multi port bridge with a buffer and a design that can boost its efficiency(large number ofports imply less traffic) and performance. Switch is data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors andforward good packets selectivelyto correct port only.In other words, switch divides collision domain of hosts, butbroadcast domainremains same.

A switch is essentially a fast bridge having additional sophistication that allows faster processing of frames. Some of important functionalities are:

- Portsareprovidedwithbuffer
- Switchmaintainsadirectory:#address-port#
- Eachframeisforwardedafterexaminingthe#addressandforwardedtothe proper port#
- Threepossibleforwardingapproaches:Cut-through,Collision-freeandFully-buffered as briefly explained below.

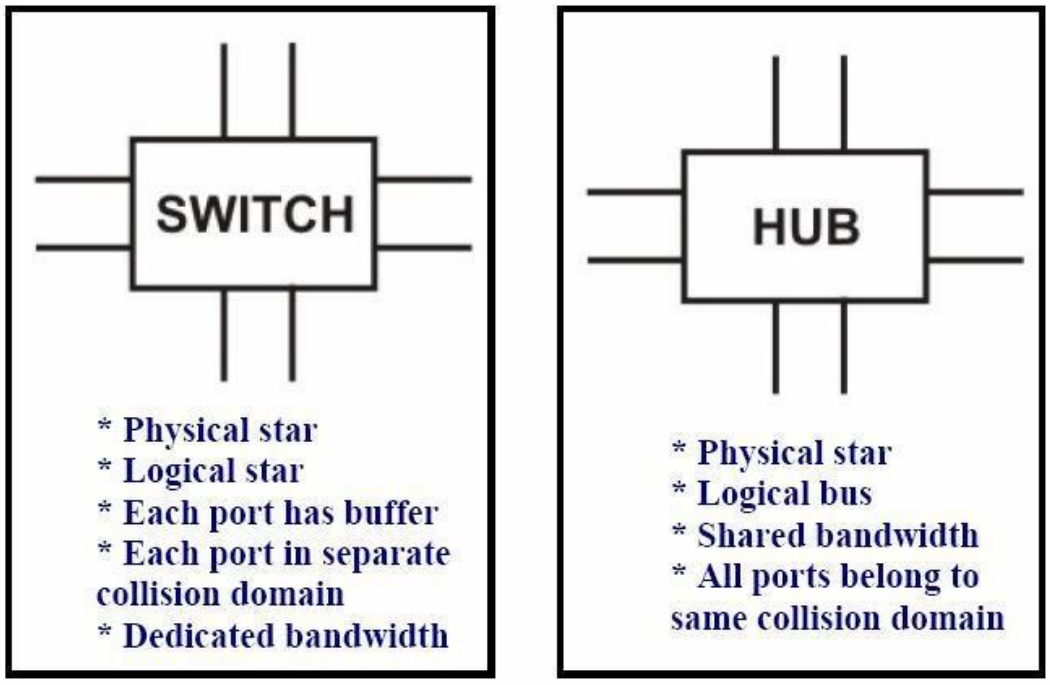
Cut-through: A switch forwards a frame immediately after receiving the destination address. As a consequence, the switch forwards the frame without collision and error detection.

Collision-free:Inthis case, theswitchforwardsthe frameafter receiving64 bytes, which allows detection of collision. However, error detection is not possible because switch is yet to receive the entire frame.

Fully buffered: Inthis case, the switch forwards the frame onlyafter receiving the entire frame. So, the switch can detect both collision and error free frames are forwarded.

Comparisonbetweenaswitchanda hub

Although a hub and a switch apparently look similar, they have significant differences.As shown in Fig. , both can be used to realize physical star topology, the hubs works like a logical bus, because the same signal is repeated on all the ports. On the other hand, a switch functions like a logical star with the possibility of the communication of separate signals between any pair ofport lines. As a consequence, all the ports ofa hub belong to the same collision domain, and in case of a switch each port operates on separatecollision domain. Moreover, in case of a hub, the bandwidth is shared by all the stations connected to all the ports. Onthe other hand, in case ofa switch, each port has dedicated bandwidth. Therefore, switches can be used to increase the bandwidth of a hub-based network by replacing the hubs by switches.



FigureDifferencebetweenaswitchandabridge

5. Routers– A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

Arouter is used to route data packets between two networks. It readsthe information in each packet to tell where it is going. If it is destined for an immediate network it has access to, it will strip the outer packet (IP packet for example), readdress the packet to the proper ethernet address, and transmit it on that network. If it is destined for another network and must be sent to another router, it will re-package the outer packet to be received bythe next router and send it to the next router. Routing occurs at the network layer of the OSI model. They can connect networks with different architectures such as Token Ring and Ethernet. Although they can transform information at the data link level, routers cannot transform information from one data format such as TCP/IP to another such as IPX/SPX. Routers do not send broadcast packets or corrupted packets.If the routing table does not indicate the proper address of a packet, the packet is discarded. There are two types of routers:

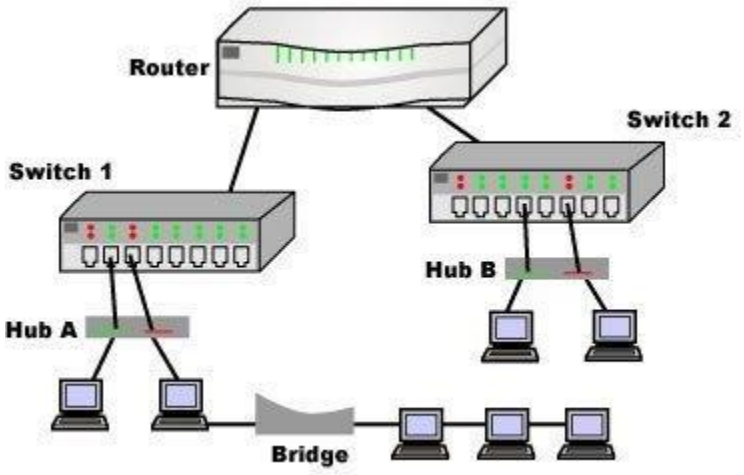
1. Static routers - Are configured manuallyand route data packets based on information in a router table.
2. Dynamic routers - Use dynamic routing algorithms. There are two types of algorithms:

- Distance vector - Based on hop count, and periodicallybroadcasts the routing table to other routers which takes more network bandwidth especially with more routers. RIP uses distance vectoring. Does not work on WANs as well as it does on LANs.
- Link state - Routing tables are broadcast at startup and then only when they change. The open shortest path first (OSPF) protocol uses the link state routing method to configure routes or distance vector algorithm (DVA).

Commonroutingprotocolsinclude:

- IS-IS-Intermediatesystemtointermediatesystemwhichisarouting protocol for the OSI suite of protocols.
- IPX-InternetPacketExchange.UsedonNetwaresystems.
- NLSP - Netware Link Services protocol - Uses OSPF algorithm and isreplacing IPX to provide internet capability.
- RIP-Routinginformationprotocolusesadistancevectoralgorithm.

There is a device called a brouter which will function similar to a bridge for network transport protocols that are not routable, and will function as a router for routable protocols. It functions at the network and data link layers of the OSI network model.



A router is considered as a layer-3 relay that operates in the network layer, that is it acts on network layer frames**.** It can be used to link two dissimilar LANs**.** A router isolates LANs in to subnets to manage and control network traffic. However, unlike bridges it is nottransparenttoendstations.AschematicdiagramoftherouterisshownonFig.
6.1.13. A router has four basic components: Input ports, output ports, the routing processor and the switching fabric. The functions of the four components are briefly mentioned below.

- *Input port* performs physical and data-link layer functions of the router. As shown in Fig. 6.1.14 (a), the ports are also provided with buffer to hold the packet before forwarding to the switching fabric.
- *Output ports*, as shown in Fig., perform the same functions as the input ports, but in the reverse order.
- The *routing processor* performs the function of the network layer. The process involves table lookup.
- The *switching fabric*, shown in Fig.moves the packet from the input queue to the output queue by using specialized mechanisms. The switching fabric is realized with the help of multistage interconnection networks.

- CommunicationofaframethrougharouterisshowninFig.6.1.16.

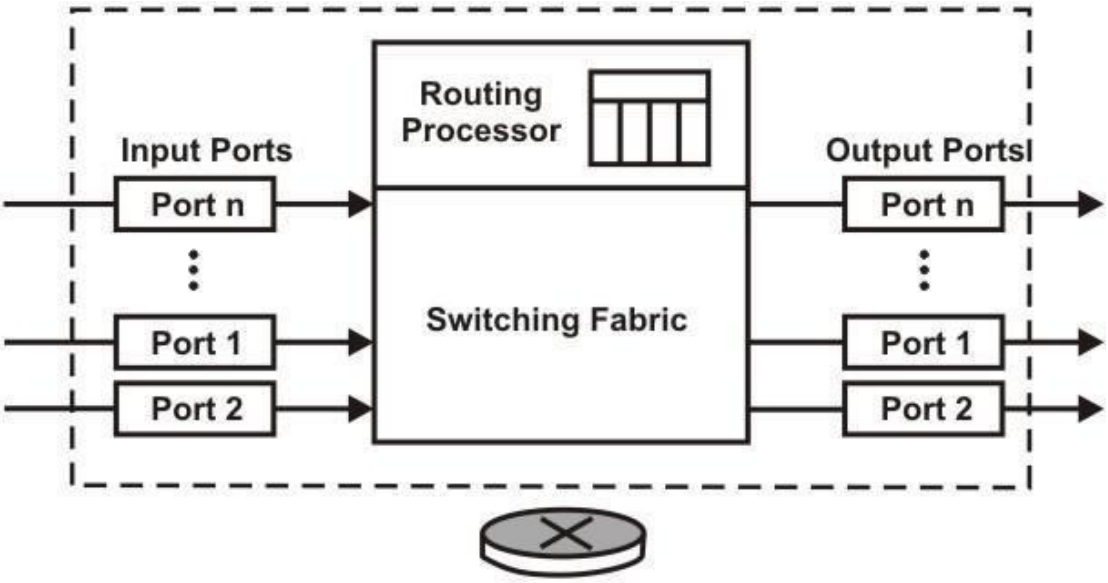
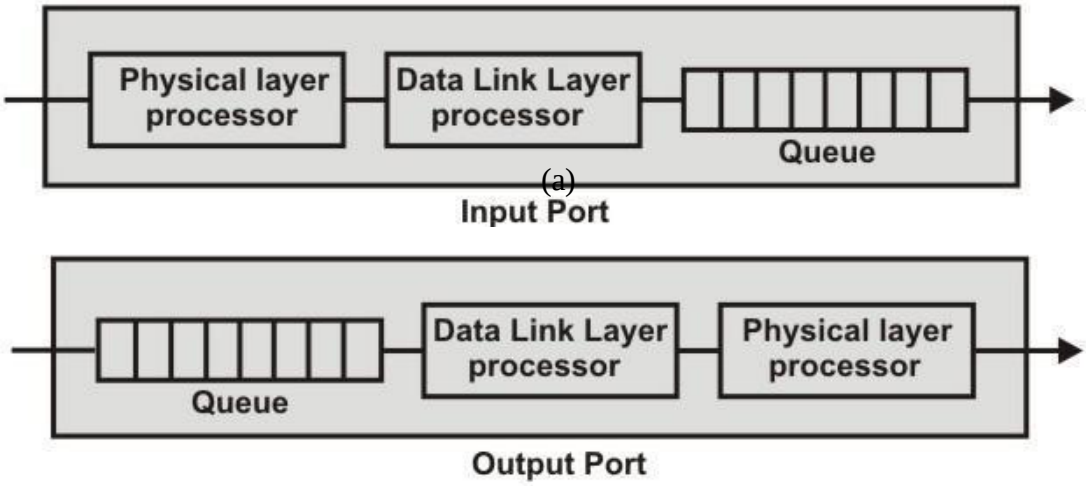
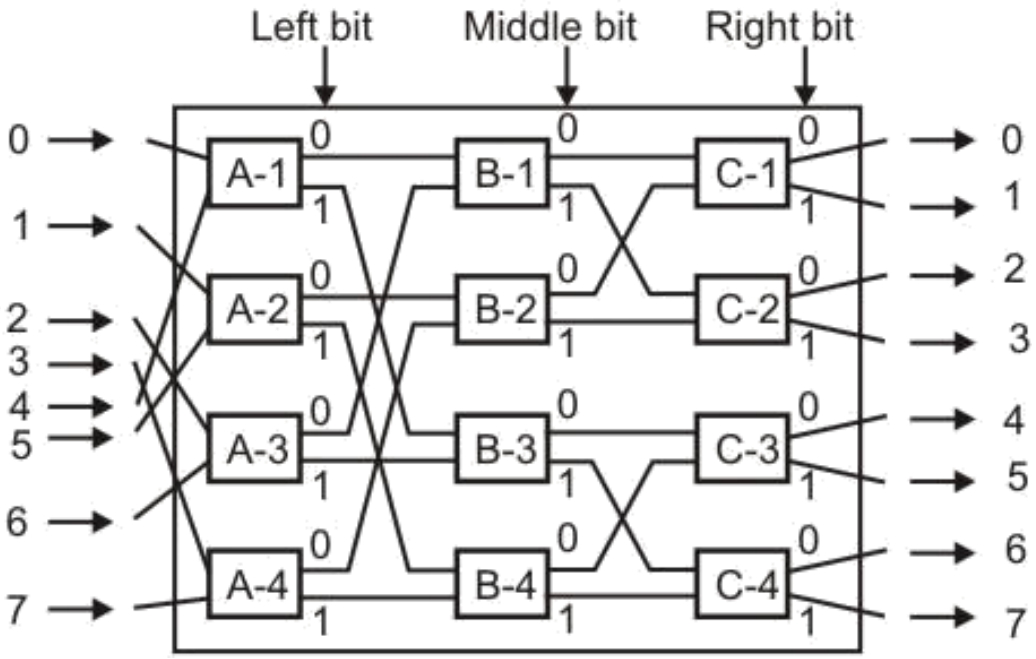


Figure Schematic diagramofarouter

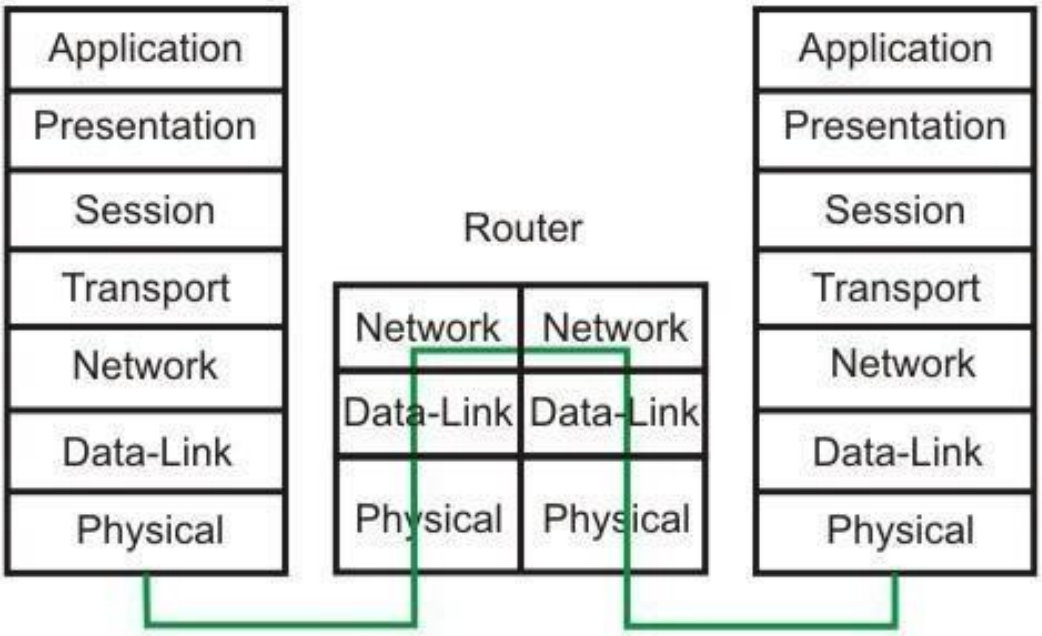


(a)

Figure6.1.14Schematic diagramofa router



FigureSwitchingfabricofa router



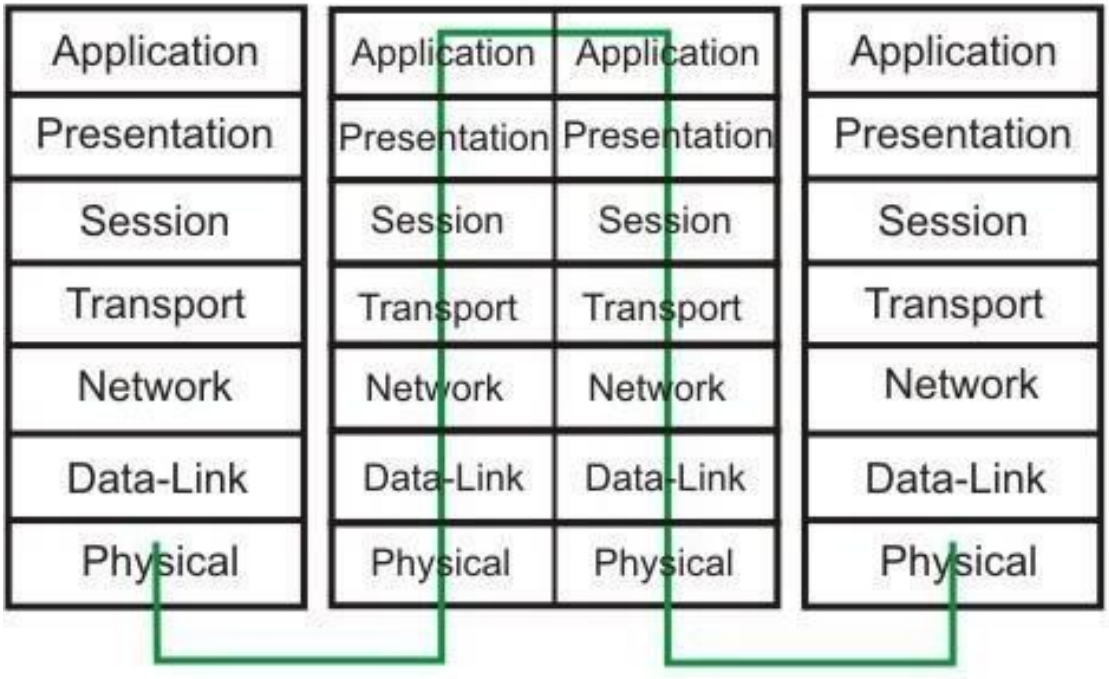
FigureCommunicationthrougha router

6. Gateway–Agateway,asthenamesuggests,isapassagetoconnecttwo networkstogetherthatmayworkupondifferentnetworkingmodels.They

basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

A gateway can translate information between different network data formats or network architectures. It can translate TCP/IP to AppleTalk so computers supporting TCP/IP can communicate with Apple brand computers. Most gateways operate at the application layer, but can operate at the network or session layer of the OSI model. Gateways will start at the lower level and strip informationuntil it gets totherequiredlevel andrepackagetheinformationand work its way back toward the hardware layer of the OSI model. To confuse issues, when talking about a router that is used to interface to another network, the word gateway is often used. This does not mean the routing machine is a gateway as defined here, although it could be.

Agatewayworksabovethenetworklayer,suchasapplicationlayerasshowninFig.
6.1.17. As a consequence, it is knownas a Layer-7 relay. The application level gateways can look into the content application layer packets such as email before forwarding it to the other side. This property has made it suitable for use in Firewalls discussed in thenext module.



FigureCommunicationthrougha gateway

TCP/IPprotocolsuite

This section presents an in-depth introduction to the protocols that are included in TCP/IP. Although the information is conceptual, you should learn thenames of the protocols.

TCP/IP"is the acronymthat is commonlyusedforthe set of network protocols that compose the Internet Protocol suite. Many texts use the term "Internet" to describe both the protocol suite and the global wide area network.

- DescribehowtheTCP/IPprotocolsuitemapstotheDepartmentofDefenseAdvanced Research Projects Agency (DARPA) and Open System Interconnection (OSI) models.
- ListthemainprotocolsintheNetworkInterface,Internet,Transport,andApplication layers of the DARPA model.
- DescribethepurposeofthecoreprotocolsoftheIPv4Internetlayer.
- DescribethepurposeofthecoreprotocolsoftheIPv6Internetlayer.
- DescribethepurposeandcharacteristicsoftheTCP and UserDatagramProtocol(UDP) protocols.
- ExplainhowIPusestheinformationinIPpacketstodeliverdatatothecorrectapplication on a destination node.
- Describethepurposeandcharacteristicsof theWindowsSocketsandNetworkBasic Input/Output System (NetBIOS) APIs.
- Describethepurposeandcharacteristicsofthehostnameand NetBIOSnamingschemes used by TCP/IP components in Microsoft Windows Server™ 2003 and Windows XP operating systems.

ProtocolLayersandtheOpenSystemsInterconnection Model

Most network protocol suites are structured as a series of layers, sometimes collectively referred to as a protocol stack. Each layer is designed for a specific purpose.

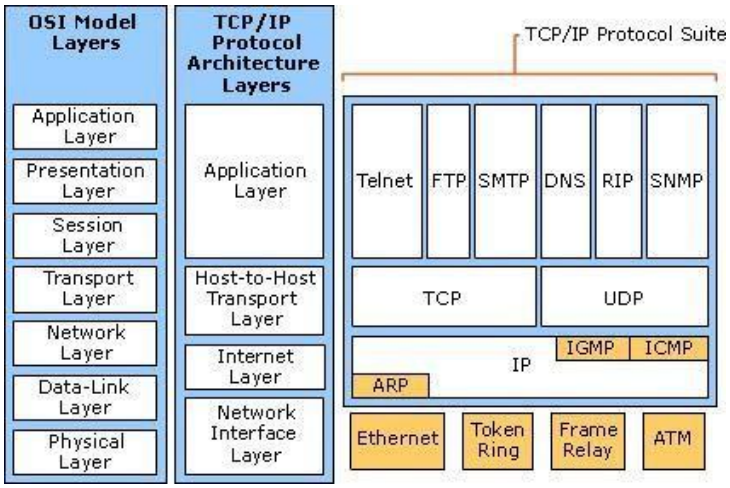
Each layer exists on both the sending and receiving systems. A specific layer on one system sends or receives exactly the same object that another system's peer process sends or receives.

ArchitectureModel

The OSI model describes idealized network communications with a family of protocols. TCP/IP does not directly correspond to this model. TCP/IP either combinesseveralOSIlayersintoasinglelayer,ordoesnotusecertainlayersat all.

TCP/IPModelLayers

The TCP/IP model uses four layers that logically span the equivalent of the top six layers of the OSI reference model; this is shown (The physical layer is not covered by the TCP/IP model becausethedatalinklayeris considered the point atwhich the interface occurs between the TCP/IP stack and the underlying networking hardware.) The following



aretheTCP/IPmodellayers,startingfromthebottom.

TCP/IPprotocolsuitemapstoafour-layerconceptualmodelknown astheDARPAmodel,which was named after the U.S. government agency that initially developed TCP/IP. The four layers of the DARPA model are: Application, Transport, Internet,and Network Interface. Each layer in the DARPA model corresponds to one or more layers of the seven-layer OSI model. Figure2-1showsthearchitectureoftheTCP/IPprotocolsuite.

TheTCP/IPprotocolsuitehastwosetsofprotocolsattheInternetlayer:

- IPv4,alsoknown asIP,istheInternet layerincommonusetodayonprivateintranetsand the Internet.
- IPv6isthenewInternetlayerthatwilleventuallyreplacetheexistingIPv4Internetlayer.

NetworkInterfaceLayer

The Network Interface layer(alsocalledtheNetworkAccess layer)sendsTCP/IPpacketsonthe networkmediumandreceives TCP/IPpacketsoffthenetworkmedium.TCP/IPwasdesigned to be independentof the network access method,frame format, and medium.Therefore,you can useTCP/IPtocommunicate acrossdifferingnetworktypesthatuseLANtechnologies—such as

Ethernet and 802.11 wireless LAN—and WAN technologies—such as Frame Relay and AsynchronousTransferMode(ATM).Bybeing independentofanyspecificnetworktechnology, TCP/IP can be adapted to new technologies.
The Network Interface layer of the DARPA model encompasses the Data Link andPhysical layers oftheOSImodel.TheInternetlayeroftheDARPAmodeldoesnottakeadvantageofsequencing and acknowledgmentservices that mightbepresent inthe Data Linklayer oftheOSImodel.The Internet layer assumes an unreliable Network Interface layer and that reliable communications through session establishment and the sequencing and acknowledgment of packets is the responsibility of either the Transport layer or the Application layer.

InternetLayer

TheInternetlayerresponsibilitiesincludeaddressing,packaging,androutingfunctions.The Internet layer is analogous to the Network layer of the OSI model.
ThecoreprotocolsfortheIPv4Internetlayerconsistofthe following:

- TheAddressResolutionProtocol(ARP)resolvestheInternetlayer address to aNetwork Interface layer address such as a hardware address.
- TheInternetProtocol(IP)is aroutableprotocolthataddresses,routes,fragments, and reassembles packets.
- TheInternetControlMessageProtocol(ICMP)reportserrorsandotherinformationto help you diagnose unsuccessful packet delivery.
- The Internet Group Management Protocol (IGMP) manages IP multicast groups.For moreinformation aboutthecoreprotocolsfortheIPv4Internetlayer,see"IPv4Internet Layer" later in this chapter.

ThecoreprotocolsfortheIPv6Internetlayerconsistofthe following:

- IPv6isaroutableprotocolthataddressesandroutespackets.
- TheInternetControlMessageProtocolfor IPv6(ICMPv6)reportserrorsandother information to help you diagnose unsuccessful packet delivery.
- TheNeighborDiscovery(ND)protocolmanagestheinteractionsbetweenneighboring IPv6 nodes.
- The Multicast Listener Discovery (MLD) protocol manages IPv6 multicast groups.

For moreinformation aboutthecoreprotocolsfortheIPv6Internetlayer,see"IPv6Internet Layer" later in this chapter.

TransportLayer

The Transport layer (also known as the Host-to-Host Transport layer) provides the Application layer with session and datagramcommunication services. The Transportlayer encompasses the responsibilitiesof theOSITransportlayer.ThecoreprotocolsoftheTransportlayer areTCPand UDP.
TCPprovidesaone-to-one,connection-oriented,reliablecommunicationsservice.TCPestablishes connections, sequences and acknowledges packets sent, and recovers packets lost during transmission.
In contrast to TCP, UDP provides a one-to-one or one-to-many, connectionless, unreliable communicationsservice.UDPisused whentheamountofdatatobetransferredissmall(such as the data that would fit into a single packet), when an application developer does not want the overhead associated with TCP connections, or when the applications or upper-layer protocols provide reliable delivery.
TCPandUDPoperateoverbothIPv4andIPv6Internetlayers.
Note The Internet Protocol (TCP/IP) component of Windows contains separate versions of the TCPandUDPprotocolsthantheMicrosoftTCP/IPVersion6componentdoes.The versions in the Microsoft TCP/IP Version 6 component are functionally equivalent to those provided with the MicrosoftWindows NT®4.0 operating systems and contain all the mostrecentsecurity updates.
TheexistenceofseparateprotocolcomponentswiththeirownversionsofTCP andUDP isknown

as adualstack architecture.The idealarchitecture isknown as aduallPlayer,inwhichthesame versionsof TCP and UDP operateover both IPv4 and IPv6 (asFigure2-1 shows).WindowsVista has a dual IP layer architecture for the TCP/IP protocol components.

ApplicationLayer

TheApplicationlayer allows applicationsto accesstheservicesoftheotherlayers,anditdefines the protocols that applications use to exchange data. The Application layer contains many protocols, and more are always being developed.
ThemostwidelyknownApplicationlayerprotocolshelpusersexchangeinformation:

- TheHypertextTransferProtocol(HTTP)transfers files thatmakeuppageson theWorld Wide Web.
- TheFileTransferProtocol(FTP) transfersindividualfiles,typicallyfor aninteractiveuser session.
- The Simple Mail Transfer Protocol (SMTP) transfers mail messages and attachments.

Additionally,thefollowingApplicationlayerprotocolshelpyouuseandmanageTCP/IPnetworks:

- The Domain Name System (DNS) protocol resolves a host name, such as www.microsoft.com,toanIPaddressandcopiesnameinformationbetweenDNSservers.
- TheRoutingInformationProtocol(RIP)isaprotocolthatroutersuseto exchangerouting information on an IP network.
- The Simple Network Management Protocol (SNMP) collects and exchanges network managementinformationbetweenanetworkmanagementconsoleandnetworkdevices such as routers, bridges, and servers.

Windows Sockets and NetBIOS are examples of Application layer interfaces for TCP/IP applications.For moreinformation,see"ApplicationProgrammingInterfaces"laterinthischapter. Top of page

Physicalnetwork layer

The physical network layer specifies the characteristics of the hardware to be used for the network.

For example, physical network layer specifies the physical characteristics of the communications media.

The physical layer of TCP/IP describes hardware standards such as IEEE 802.3,the specification for Ethernet network media, and RS-232, the specification for standard pin connectors.

Data-LinkLayer

The data-linklayeridentifiesthe networkprotocoltype of the packet, in thisinstance TCP/IP.

Thedata-linklayeralsoprovideserrorcontroland“framing.”

Examplesof data-linklayerprotocolsareEthernetIEEE802.2framingandPoint-to- Point Protocol (PPP) framing.

NetworkLayer

The Internet layer, also known as the network layer or IP layer, accepts and delivers packets for the network.

ThislayerincludesthepowerfulInternetProtocol(IP),theAddressResolution Protocol(ARP),andtheInternetControlMessageProtocol(ICMP).

IP Protocol

- TheIPprotocolanditsassociatedroutingprotocolsarepossiblythemost significant of the entire TCP/IP suite. IP is responsible for the following:

IP addressing

The IP addressing conventions are part of the IP protocol. Designing an IPv4Addressing Scheme introduces IPv4 addressing and IPv6 Addressing Overview introduces IPv6 addressing.

Host-to-hostcommunications – IPdeterminesthepathapacketmusttake,basedon the receivingsystem'sIPaddress.

ARPProtocol

The Address Resolution Protocol (ARP) conceptually exists between the data-link and Internet layers.

- ARPassistsIPindirectingdatagram’stotheappropriatereceivingsystem by mapping Ethernet addresses (48 bits long) to known IP addresses (32 bits long).

ICMPProtocol

TheInternetControlMessageProtocol(ICMP)detectsandreportsnetwork error conditions. ICMP reports on the following:

Droppedpackets –Packetsthatarrivetoofasttobeprocessed

Connectivity failure – A destination system cannot be reached

TransportLayer

The TCP/IP transport layer ensures that packets arrive in sequence and without error, by swapping acknowledgments of data reception, and retransmitting lost packets.

This type of communication is known as end-to-end. Transport layer protocols at this level are Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP). TCP and SCTP provide reliable, end-to-end service.

UDPprovidesunreliabledatagramservice.

TCP Protocol

TCP enables applications to communicate with each other as though they were connected by a physical circuit.

TCPsendsdatainaformthatappearstobetransmittedinacharacter-by-character

fashion,ratherthanasdiscretepackets.Thistransmission consistsof the following:

SCTPProtocol

SCTP is a reliable, connection-oriented transport layer protocol that provides the same services to applications that are available from TCP.

Moreover, SCTP can support connections between systems that have more than one address, or multihued.

The SCTP connection between sending and receiving system is called an association.

ApplicationLayer

The application layer defines standard Internet services and network applications that anyone can use.

These services work with the transport layer to send and receive data.

Manyapplication layer protocols exist.

Thefollowinglistshowsexamplesofapplicationlayerprotocols:

1.StandardTCP/IPservicessuchastheftp,tftp,andtelnet commands

- **Node-to-node delivery**: At the data-link level, delivery of frames take place between two nodes connected by a point-to-point link or a LAN, by using the data-link layers address, say MAC address.
- **Host-to-host delivery**: At the network level, deliveryofdatagramscantakeplace between two hosts by using IP address.

From user's point of view, the TCP/IP-based internet can be considered as a set of application programs that use the internet to carry out useful communication tasks. Most popular internet applications include Electronic mail, File transfer, and Remote login. IP allows transfer ofIP datagrams among a number of stations or hosts, wherethe datagram is routed through the internet based on the IP address ofthe destination. But, in this case, several application programs (processes) simultaneously running on a source host has to communicate with the corresponding processes running on a remote destination host through the internet. This requires an additional mechanism called *process-to-process delivery*, which is implemented with the help ofa transport -level protocol. The transport level protocol will require an additional address, known as *port number*, to select a particular process among multiple processes running on the destination host. So, there isa requirement of the following third type of delivery system.

- **Process-to-process delivery**: At the transport level, communication can take place between processes or application programs by using port addresses

Basic communication mechanism is shown in Fig. 6.3.1. The additional mechanism needed to facilitate multiple application programs in different stations to communicate with each other simultaneously can be provided by a transport level protocol such asUDP or TCP, which are discussed in this lesson.

.6.3.2.

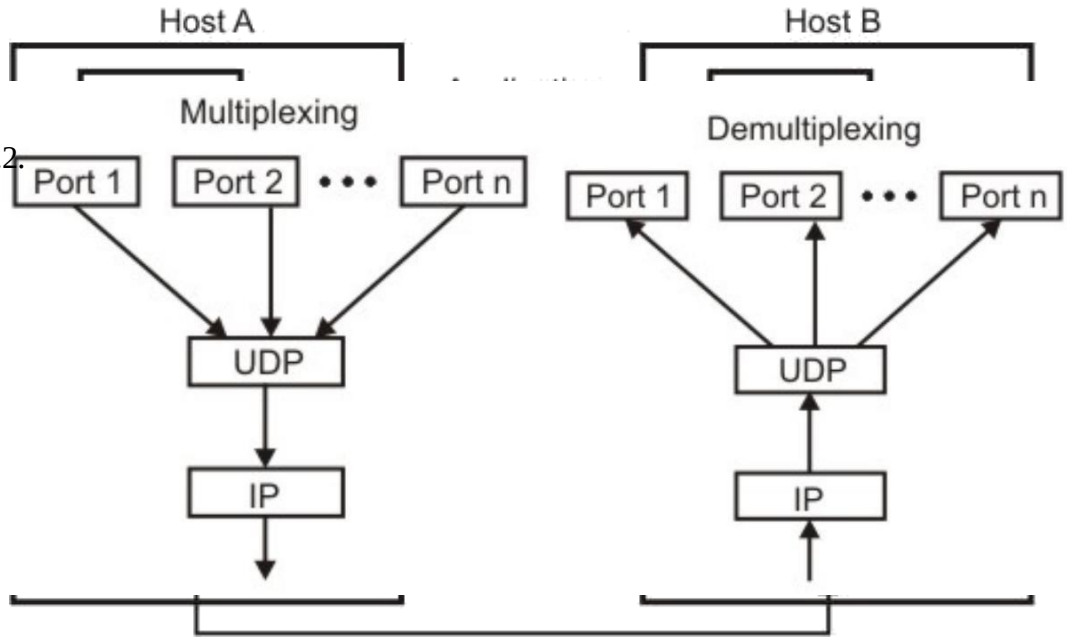


Figure6.3.1Communicationmechanismthroughtheinternet

UserDatagramprotocol(UDP)

UDP is responsible for differentiating among multiple source and destination processes withinone host.Multiplexinganddemultiplexing operationsareperformedusingtheport mechanism as depicted in Fig

Figure6.3.2Multiplexinganddemultiplexing mechanismofUDP

UDPDatagram

TheUDPdatagramformat isshowninFig. 6.3.3.Abriefdescriptionofdifferent fieldsof the datagram are given below:

- Sourceport(16bits):Itdefinestheportnumberoftheapplicationprograminthehost of the sender
- Destinationport(16bits):It definestheport numberoftheapplicationprograminthe host of the receiver
- Length:Itprovidesacount ofoctetsintheUDPdatagram,minimum length=8
- Checksum:Itisoptional,0incaseitisnotinuse

CharacteristicsoftheUDP

KeycharacteristicsofUDP aregiven below:

- UDPprovidesanunreliableconnectionlessdeliveryserviceusingIPto transport messages between two processes
- UDPmessagescanbelost,duplicated, delayedandcanbedeliveredoutoforder
- UDPisathinprotocol,whichdoesnotadd significantlytothe functionalityofIP
- Itcannotprovidereliablestreamtransportservice

The above limitations can be overcome by using connection-oriented transport layer protocol known as *Transmission Control Protocol* (TCP), which is presented in the following section.

TransmissionControlProtocol(TCP)

TCP provides a connection-oriented, full -duplex, reliable, streamed delivery service using IP to transport messages between two processes.

Reliabilityisensuredby:

- Connection-orientedservice
- Flowcontrolusingsliding windowprotocol
- Errordetectionusing checksum
- Error controlusinggo-back-NARQtechnique
- Congestionavoidancealgorithms;multiplicativedecreaseandslow-start

TCPDatagram

TheTCPdatagramformat isshowninFig.6.3.4.Abriefexplanationofthe functionsof different fields are given below:

- Sourceport(16bits):Itdefinestheportnumberoftheapplicationprograminthehost of the sender
- Destinationport(16bits):It definestheport numberoftheapplicationprograminthe host of the receiver
- Sequencenumber(32bits):Itconveysthereceivinghost whichoctetinthissequence comprises the first byte in the segment
- Acknowledgement number(32bits):Thisspecifiesthesequencenumberofthenext octet that receiver expects to receive
- HLEN(4bits):Thisfield specifiesthenumberof32-bit wordspresent intheTCP header
- Controlflagbits(6bits):URG:Urgentpointer
- ACK:Indicateswhetheracknowledgefield is valid
- PSH:Pushthedatawithout buffering
- RST:Resenttheconnection
- SYN:Synchronizesequence numbersduringconnectionestablishment
- FIN:Terminatetheconnection
- Window(16bits):Specifiesthesizeofwindow
- Checksum(16bits):Checksumusedforerrordetection.
- Userpointer (16bits):UsedonlywhenURGflagis valid
- Options:Optional40bytesofinformation

The well-known ports used by TCP are given in Table 6.3.2 and the three types of addresses used inTCP/IP are shown in Fig. 6.3.5. TCP establishes a virtualpath between the source and destination processes before any data communication by using two procedures, *connection establishment* to start reliably and *connection termination* to terminate gracefully, as discussed in the following subsection.

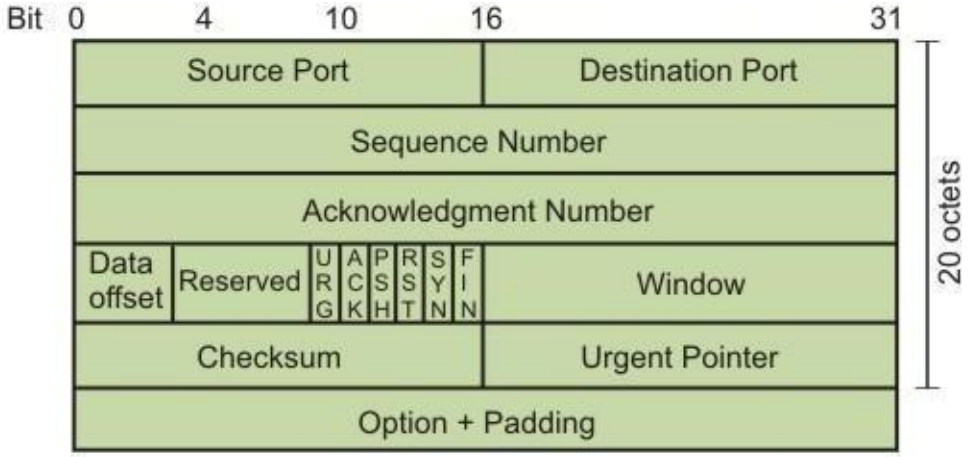


Figure6.3.4TheTCPdatagramformat

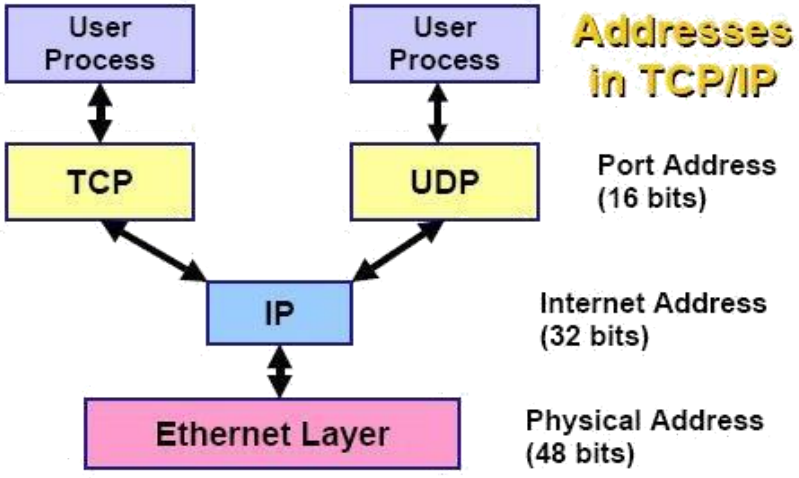


Figure6.3.5ThreetypesofaddressesusedinTCP/IP

Table6.3.2Well-knownportsusedbyTCP

Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
20	FTP, Data	File Transfer Protocol (data connections)
21	FTP, Control	File Transfer Protocol (control connection)
23	TELNET	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	BOOTP Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure Call

ElectronicMail

Simple Mail Transfer Protocol (**SMTP**) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

SMTPisaconnection-oriented,text-basedprotocolinwhicha mailsendercommunicates with a mail receiver by issuing command strings and supplying necessary data over a reliable ordered data stream channel, typically a Transmission Control Protocol (TCP) connection. An SMTP session consists of commands originated by an SMTP client (the initiating agent, sender, or transmitter) and corresponding responses from the SMTP server (the listening agent, or receiver) so that the session is opened, and session parameters are exchanged. A session may include zero or more SMTP transactions. An SMTPtransactionconsistsofthree command/replysequences(see example below.) They are:

1. MAILcommand,toestablishthereturnaddress,a.k.a.Return-Path,5321.From,mfrom, or

envelopesender.Thisistheaddressforbouncemessages.

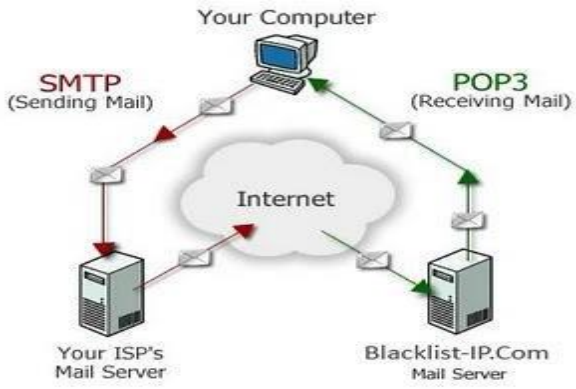
2. RCPT command, to establisha recipient ofthis message. This command canbe issued multiple

times,oneforeachrecipient.Theseaddressesarealsopartofthe envelope.

3. DATA to send the message text. This is the content of the message, as opposed to its envelope.

Itconsistsofamessageheader and amessagebodyseparatedbyanemptyline.DATAis

actuallya groupofcommands, and the server replies twice: once tothe DATA command proper, to acknowledge that it is ready to receive the text, and the second time after the end-of-data sequence, to either accept or reject the entire message.



Electronic mail is among the most widely available application services. Each user, who intends to participate in email communication, is assigned a mailbox, where out-going and incoming messages are buffered, allowing the transfer to take place inthebackground. The message contains a header that specifies the sender, recipients, and subject, followed by a body that contains message. The TCP/IP protocol that supports electronic mail on the internet is called *Simple Mail Transfer Protocol* (SMTP), which supports the following:

- Sendingamessagetooneormorerecipients
- Sendingmessagesthatincludetext,voice,video,or graphics

A software package, known as *User Agent*, is used to compose, read, reply or forward emails and handle mailboxes. The email address consists of two parts divided by a @ character. The first part is the local name that identifies mailbox and the second part is a domain name.

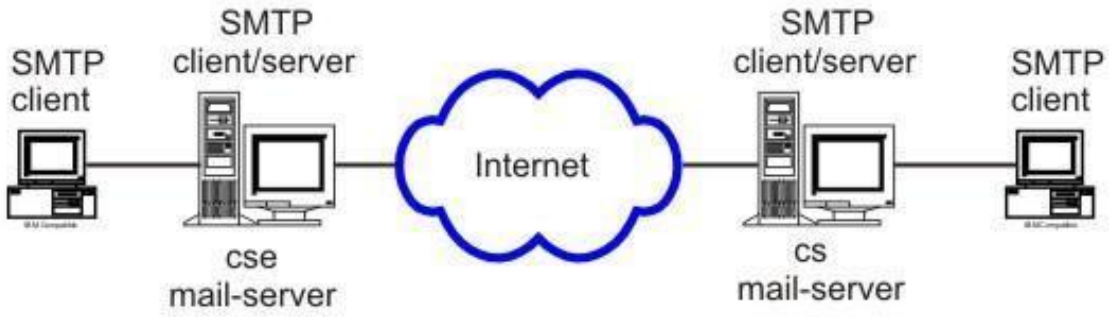


Figure6.3.14SimpleMailTransferProtocol(SMTP)

Telnet

Telnet is a simple remote terminal protocol that provides a remote log-on capability, which enables a user to log on to a remote computer and behaves as if it is directly connected to it. The following three basic services are offered by TELNET:

- Itdefinesanetworkvirtualterminalthatprovidesastandardinterfaceto remote systems
  - It includes a mechanism that allows the client and server to negotiate options from a standard set
  - Ittreatsbothends symmetrically

FileTransferProtocol(FTP)

File Transfer Protocol (FTP) is a TCP/IP client -server application for transfer files between two remote machines through internet. A TCP connection is set up before file transfer and it persists throughout the session. It is possible to send more than one file before disconnecting the link. Acontrolconnection is established first witha remote host before any file can be transferred. Two connections required are shown in Fig. 6.3.15. Users view FTP as an interactive system

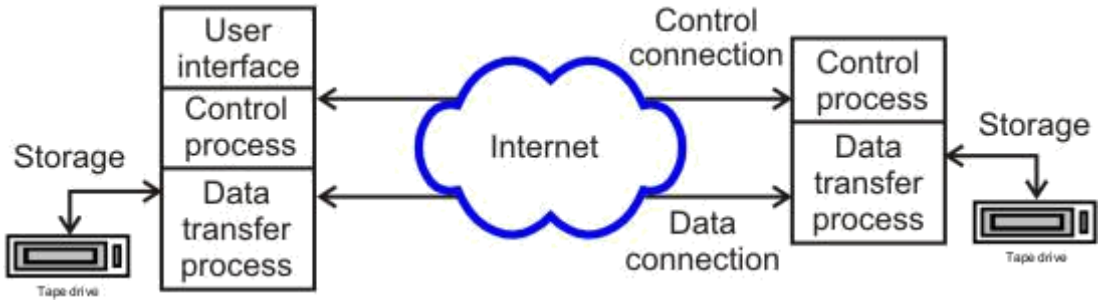


Figure6.3.15FileTransferProtocol(FTP)

SimpleNetworkManagementProtocol(SNMP)

Network managers use network management software that help them to locate, diagnose and rectify problems. Simple Network Management Protocol(SMTP) provides a systematic way for managing network resources. It uses transport layer protocol for communication. It allows them to monitor switches, routers and hosts. There are four components of the protocol:

- Managementofsystems
- Managementofnodes;hosts,routers,switches
- Management of Information Base; specifies data items a host or a router must keep and the operations allowed on each (eight categories)
- Management of Protocol; specifies communication between network management client program a manager invokes and a network management server running on a host orrouter

HTTP(HyperTextTransferProtocol)

TheWEB

Internet (or The Web) is a massive distributed client/server information system as depicted in the following diagram.

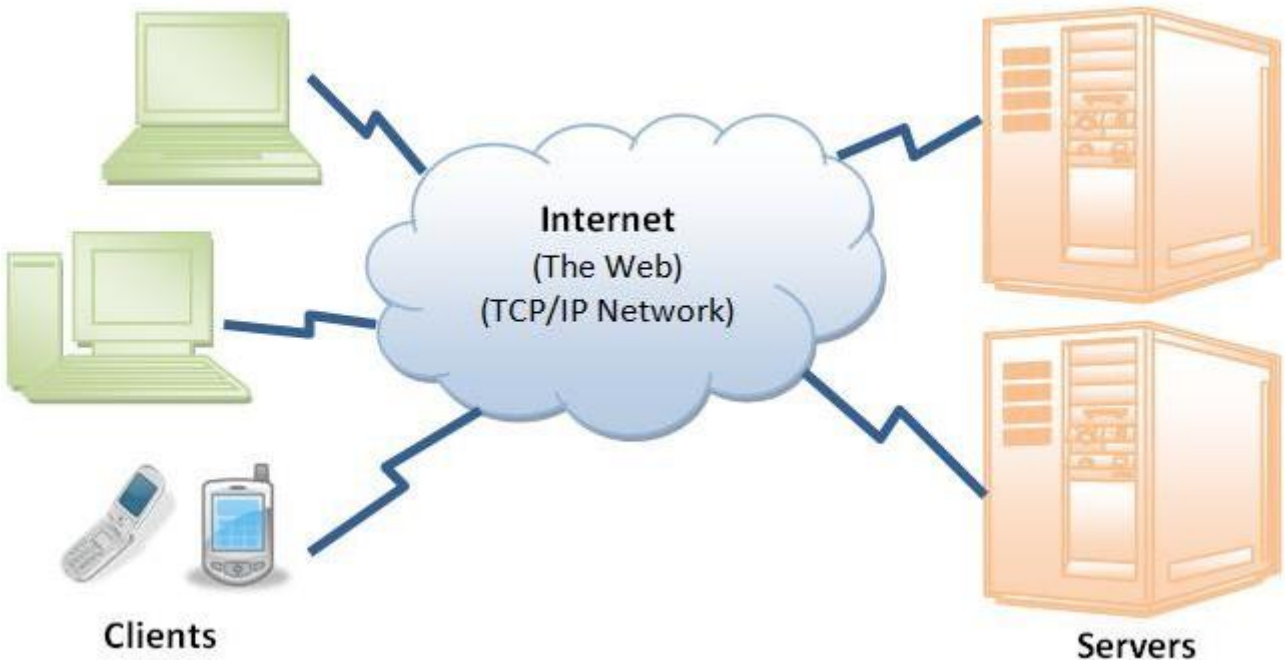
Many applications are running concurrently over the Web, such as web browsing/surfing, e-mail, file transfer, audio & video streaming, and so on.In order for proper communication to take place between the client and the server, these applications must agree on a specific application-level protocol such as HTTP, FTP, SMTP, POP, and etc.

HyperTextTransferProtocol(HTTP)

HTTP (Hypertext Transfer Protocol) is perhaps the most popular application protocol used in the Internet (or The WEB).

TheWEB

Internet (or The Web) is a massive distributed client/server information system as depicted in the following diagram.



Many applications are running concurrently over the Web, such as web browsing/surfing, e-mail, file transfer, audio & video streaming, and so on.In order for proper communication to take place between the client and the server, these applications must agree on a specific application-level protocol such as HTTP, FTP, SMTP, POP, and etc.

HyperTextTransferProtocol(HTTP)

Hypertext Transfer Protocol (HTTP) is communications protocol of the TCP/IP Suit. It is used for retrieving inter-linked text documents (hypertext). HTTP led to the establishment of the World Wide Web.

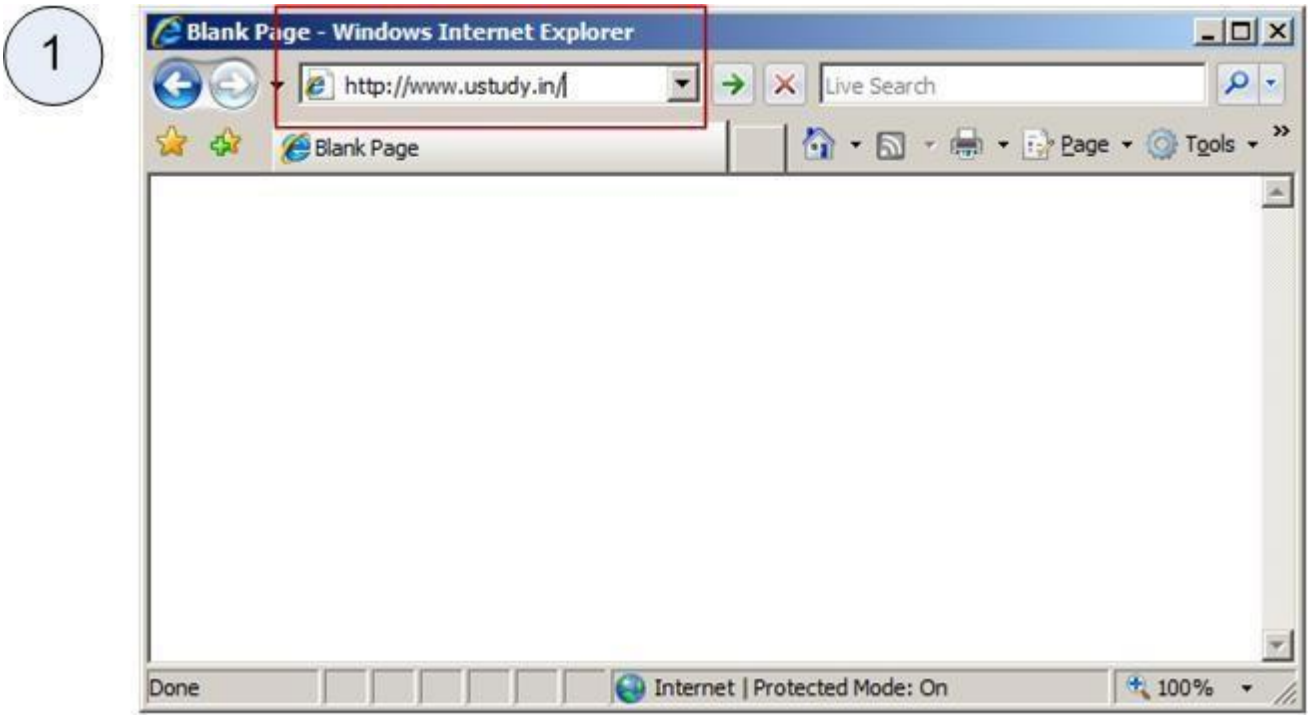
HTTP's development was coordinated by the World Wide Web Consortium and the Internet Engineering Task Force(IETF), resulting in the publicationofaseriesofRequest for Comments (RFCs), most notably RFC 2616 (June 1999), which defines HTTP/1.1, the version of HTTP in common use.

HTTP isa request/response standard betweena client and a server. The end-user client making a HTTPrequest—using a web browser typically—is referred to asthe **useragent**. The responding server—which serves resources such as HTML files and images—is called the **origin server**.

Typically, an HTTP client initiates a request. It establishes a Transmission Control Protocol (TCP) connectionto aparticular port onahost (port 80 bydefault). AnHTTP server listening on that port waits for the client to send a request message. Upon receiving the request, the server sends back the requested resource. Resources to be accessed by HTTP are identified using UniformResourceIdentifiers(URIs) (or,morespecifically, UniformResourceLocators(URLs)) using the http: or https: URI schemes.

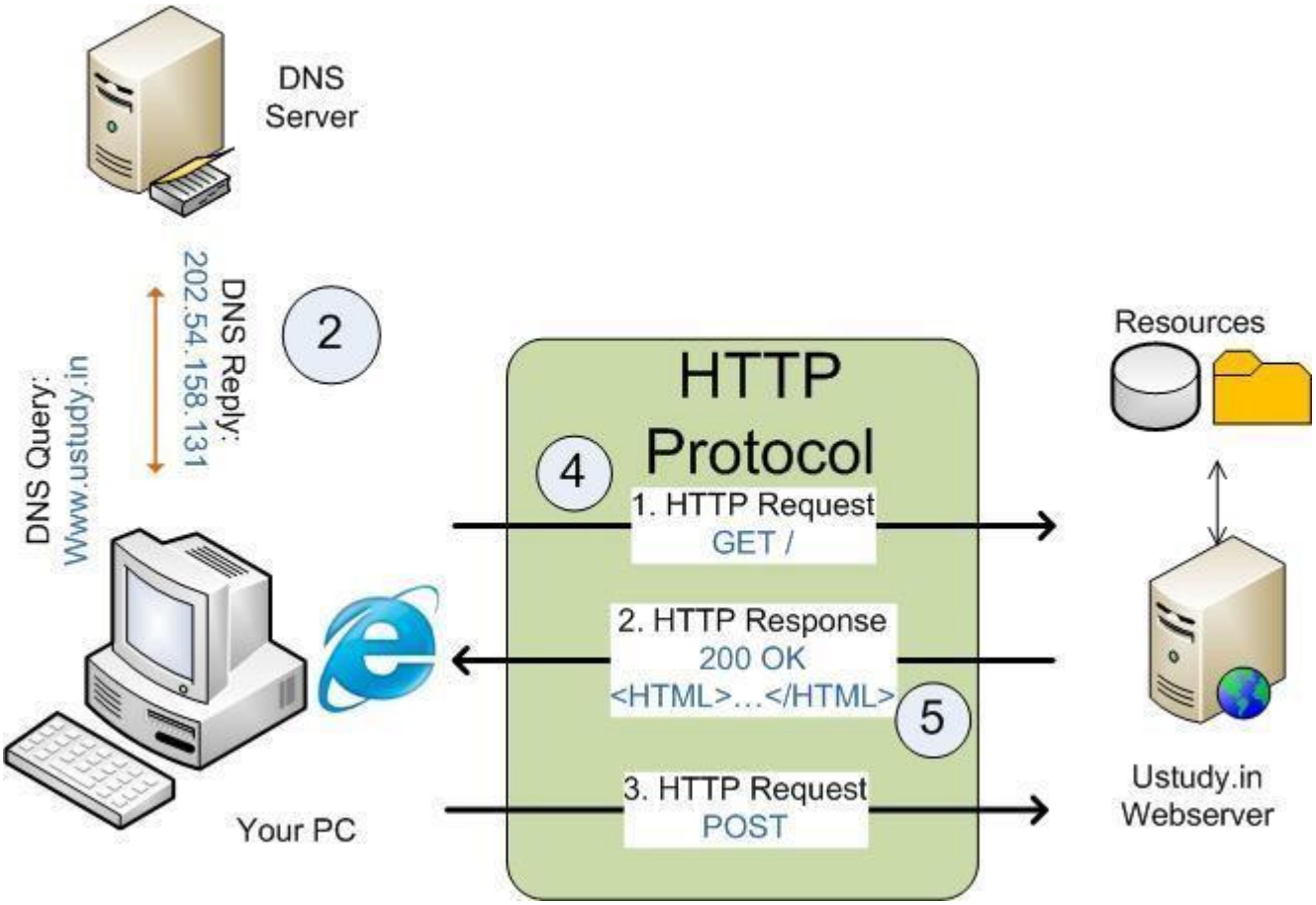
HereishowHTTP works:

1. Youtypeawebsite'sURL,forexample, www.ustudy.ininyourfavoritebrowser(IE,Firefox,Opera, Safari)



2. Your web browser looks up the IP address ofwww.ustudy.inusing DNS services - it is resolved as 202.54.158.131.

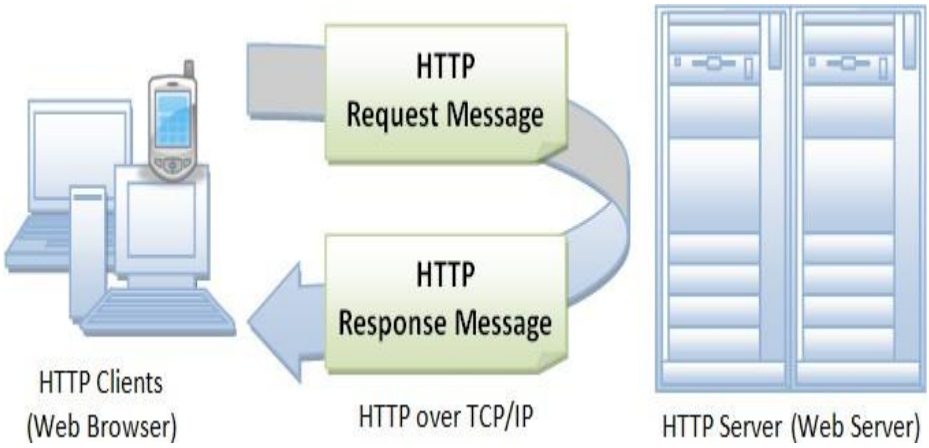
3. Yourwebbrowserthenestablishes aTCPconnectiontotheIPaddress 202.54.158.131onport 80. The web browser's packets are transported to the Ustudy.in server over the internet using IP. The server for UStudy.in successfully receives the packet and acknowledges a connection. On seeing it is for port 80, delivers it to the web server software (apache, IIS etc.).



HTTP(Hypertext TransferProtocol) is perhapsthe most popularapplicationprotocolused inthe Internet (or The WEB).

HTTP is an*asymmetric request-response client-server*protocol as illustrated.An HTTP client sends a request message to anHTTP server.The server, in turn, returns a response message.In otherwords,HTTPisa*pullprotocol*,theclient*pulls*informationfromtheserver(insteadof

server*pushes* information down to the client).



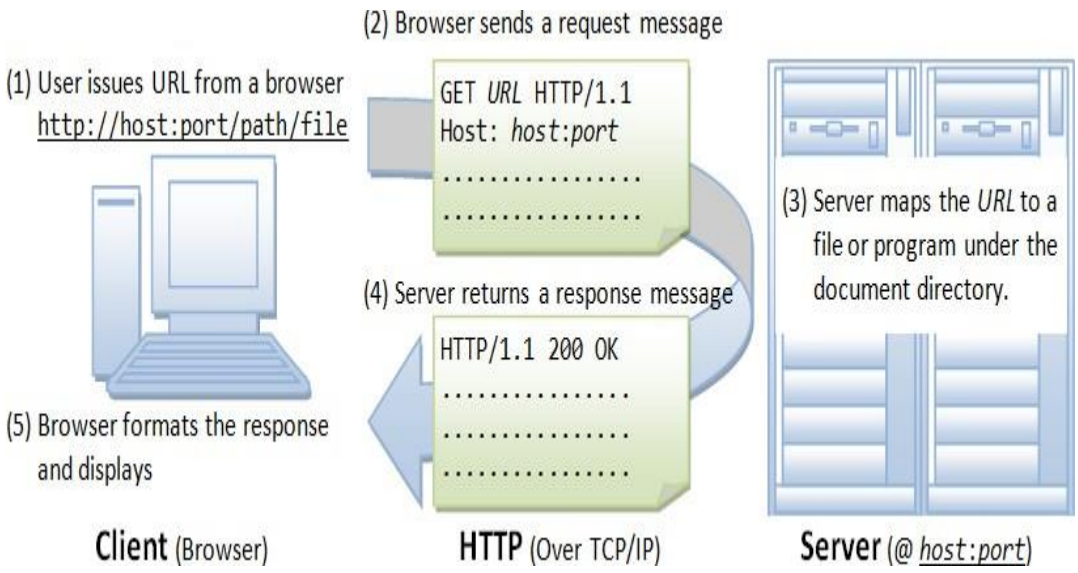
HTTP is a stateless protocol. In other words, the current request does not know what has been done in the previous requests.

HTTP permits negotiating of data type and representation, so as to allow systems to be built independently of the data being transferred.

Quoting from the RFC2616: "The Hypertext Transfer Protocol (HTTP) is an application-level protocolfor distributed, collaborative, hypermedia information systems. It is a generic, stateless, protocol which can be used for many tasks beyond its use for hypertext, such as name serversand distributed object management systems, through extension of its request methods, errorcodes and headers."

Browser

WheneveryouissueaURLfromyourbrowsertogetawebresourceusingHTTP, e.g. http://www.nowhere123.com/index.html,thebrowserturnstheURLintoa *request message*and sends it to the HTTP server. The HTTP server interprets the request message, and returns you an appropriate response message, which is either the resource you requested or an error message. This process is illustrated below:



UniformResourceLocator(URL)

A URL (Uniform Resource Locator) is used to uniquely identify a resource over the web. URL has the following syntax:

```
protocol://hostname:port/path-and-file-name
```

Thereare4parts ina URL:

1. *Protocol*:Theapplication-levelprotocolusedbytheclientandserver,e.g.,HTTP,FTP,and telnet.
2. *Hostname*:TheDNSdomainname(e.g., `www.nowhere123.com`)orIPaddress(e.g., 192.128.1.2) of the server.
3. *Port*:TheTCPportnumberthattheserverislisteningforincomingrequestsfromtheclients.
4. *Path-and-file-name*:Thenameandlocationoftherequestedresource,undertheserver document base directory.

- HTTP is an *asymmetric request-response client-server* protocol as illustrated.An HTTP client sends a requestmessage to an HTTP server.The server, in turn, returns a responsemessage.In otherwords,HTTPisa*pullprotocol*,theclient *pulls*informationfromtheserver (insteadof

  server*pushes*informationdowntotheclient).
- HTTP is a stateless protocol. In other words, the current request does not know what has been done in the previous requests.
- HTTP permits negotiating of data type and representation, so as to allow systems to be built independently of the data being transferred.
- Quoting from the RFC2616: "The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. It is a generic, stateless, protocolwhichcanbeusedformanytasksbeyond itsuseforhypertext,suchasnameservers

and distributed object management systems, through extension of its request methods, errorcodes and headers."

WorldWideWeb (WWW)

- The **World Wide Web** (WWW) is a repository of information linked together from points all overtheworld.TheWWWhasauniquecombination offlexibility,portability,anduser-friendly features that distinguish it from other services provided by the Internet.

- Eachsiteholdsone ormoredocuments,referredtoas *Webpages.*EachWebpagecancontain alinktootherpagesinthesamesiteor atothersites.Thepagescanberetrievedandviewedby using browsers.

  Client(Browser)

  AvarietyofvendorsoffercommercialbrowsersthatinterpretanddisplayaWebdocument,and all use nearly the same architecture. Each browser usually consists of three parts: a controller, client protocol, and interpreters. The controller receives input from the keyboard or the mouse and uses the client programs to access the document. After the document has been accessed, the controller uses one of the interpreters to display the document on the screen. The client protocol can be one of the protocols described previously such as FTP or HTTP (described later in the chapter). The interpreter can be HTML, Java, or JavaScript, depending on the type of document.

  Server

The Web page is stored at the server. Each time a clientrequestarrives,the corresponding documentis sent to the client. To improve efficiency, servers normally store requested files in a cache in memory; memoryisfastertoaccessthan disk.Aservercanalsobecomemoreefficientthroughmultithreadingor multiprocessing.Inthiscase,aservercananswermorethanonerequestata time.

ReviewQuestions

Q1.Whatistherelationship betweenTCP/IPandInternet?

Ans: Internet is a network ofdifferent types of network. TCP/IP is a set of rules and procedures that governtheexchangeofmessages betweenhostslinkedtodifferent networks.TCP/IPcreates an environment as if all hosts are connected to a single logical network.

Q2.DistinguishbetweenTCPandUDP?

Ans: Both TCP and UDP belong to transport layer. The UDP is simpler with much less overhead. UDP provides unreliable connectionless service. On the other hand, TCP provides connection oriented reliable service with the help of suitable flow control and error control protocols. As a consequence, TCP has much more overhead.

Q3.WhatisthemainfunctionofUDP protocol?

Ans:UDPprotocolprovidesuserprogramstheabilityto communicateusingunreliable connectionless packet delivery service with minimum overhead.

Q4.Whypseudo-headerisaddedinaUDPdatagram?

Ans: As the UDP datagram does not contain source and destination address information, a pseudo-header is added with these information to verify that the UDP datagram has reached its correct destination.

Q5.WhatprotocolisusedbyTCPforflowcontrol?

Ans.TCPusesslidingwindowprotocolforflowcontrol.

Q6.WhatARQprotocolisusedinTCP?

Ans. Go-back-NARQ.

Q7.Whatispiggybacking?

Ans. Instead ofsending a separate packet for positive/negative acknowledgement, piggybacking technique utilizes the full-duplex communication environment of TCP. The positive/negative acknowledgement information is added to a normalpacket sent bythe receiving side. It helps to save precious network bandwidth.

Q8.HowTCPestablishesandterminates connection?

Ans. TCP establishes connection using a three-way handshaking protocol and connection is terminated by a 2-way/4-way handshaking protocol.

Q9. WhataretheadvantagesofDNS?

Ans: KeyadvantageofDNS istheuseofahierarchical naming systemand theuseofdistributed database to store the huge amount of address information in many servers. The host that needs mapping of name to address can contact the closest server holding the required information.

Q10.Whatkindofparadigmis usedbytheapplicationlayer protocols?**Ans.**
Client-Serverparadigmisused byalltheapplicationlayerprotocols.

Q1.Whydoyouneedinternetworking?

Ans: As stations connected to different LANs and WANs want to communicate with eachother, it is necessary to provide this facility. Internetworking creates a single virtual network overwhich all stations in different network can communicate seamlessly and transparently.

Q2.Whyarepeater iscalledlevel-1relay?

Ans: Arepeater operates inthe physical layer. Data received onone ofitsportsisrelayed onthe remainingportbit-by-bit withoutlooking intothecontents.That iswhyrepeateriscalleda level- 1 relay.

Q3.Whatisbridge?Howitoperatesintheinternetworking scenario?

Ans: A bridge operates in the Data link layer. It looks into various fields of a frame to take various actions. For example, it looks at the destination address field so that it can forward the frame to a port where destination stations is connected. It also looks at the FCS field to check error in the received frame, it any. A bridge helps to create a network having different collision domains.

Q4.Whyspanning treetopologyisnecessaryforrouting using a bridge?

Ans: If there exit more than one path between two LANs through different bridges, there is a possibility of continuous looping of a frame between the LANs. To avoid the loop problem, spanning tree topology is used. It is essentially an overlay oftree topologyon the physical graph topology, providing only one path between any two LANs.

Q5.Whatisdiscoveryframe?

Ans: In the source routing protocol, a host can discover a route by sending a *discovery frame***,** which spreads through the entire network using all possible paths to the destination. Each frame gradually gathers addresses as it goes. The destination responds to each frame and the sourcehost chooses an appropriate route from these responses.

Q6.Whatlimitationoftransparentbridgeprotocolisovercomebythesourceroutingprotocol?

Ans: Transparent bridge protocol uses spanning tree algorithm, where a unique path is used for communication between two stations. As a consequence, it does not make use of other paths leading to lesser utilization of network resources. This problem is overcome in source routing algorithm.

Q7.Whatlimitations ofabridgeareovercomebyarouter? **Ans:**A router overcomes the following limitations of a bridge:

- Linking oftwodissimilarnetworks
- Routingdataselectivelyand efficiently
- Enforcementofsecurity
- Vulnerabilityto broadcaststorm