B.E.

Fifth Semester Examination, Dec.-2006

Computer Networks (IT-305-E)

Note: Attempt any ***five*** questions. Each question carries equal marks.

Q. 1. (a) What do you mean by Network topologies? Compare some popular one in term of performance.

Ans. Network Topology : Network topology is the shape or physical connectivity of the network. A network configuration is also called network topology.

Bus Topology : In a Bus (i.e. a linear cable) network, at any instant at most one machine is the master & is allowed to transmit. All other machines are required to regain from sending. An arbitration mechanism is needed to residue conflicts when two or more machines want to transmit simultaneously. The arbitration mechanism may be centralized or distributed. IEEE 802.3, popularly called Ethernet, eg., is a bus based broadcast network with decentralized control, usually operating at 10 Mbps to 10 Gbps.

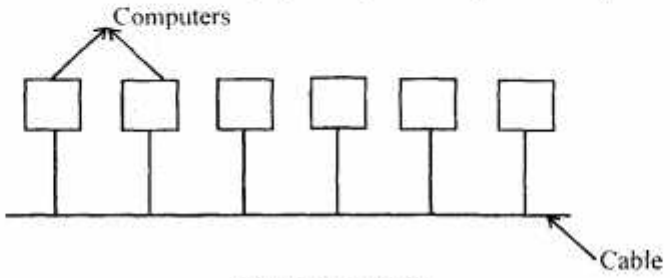


Fig. Bus Topology

Ring Topology : In a ring, each bit propagates around on its own, not waiting for the rest of the packet to which it belongs. Typically, each bit circumnavigates the entire ring in the time it takes to transmit a few bits, often before the complete packet has even been transmitted. As with all other broadcast systems, some rule is needed for arbitrating simultaneous accesses to the ring. Various methods, such as having the machines take turns, are in use. IEEE 802.5 is a ring based LAN operating at 4 & 16 Mbps. FDDI is another example of a ring network.

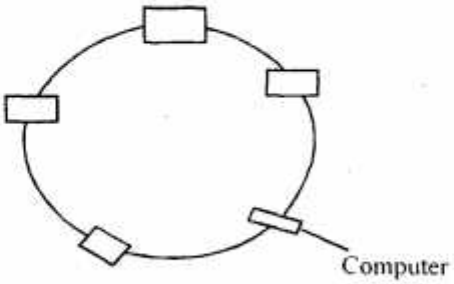


Fig. Ring Topology

Q. 1. (b) What do you understand by networking of computer? Explain MAN with example.

Ans. Computer network means a collection of autonomous computers interconnected by a single technology. Two computers are said to be interconnected if they are able to exchange information. The connection

need not be via a copper wire; fibre optics, infrared, & communication satellites can also be used. Networks came in many sizes, shapes & forms.

MAN : Metropolitan Area Network, or MAN, covers a city. The best known example of a MAN is the Cable Television network available in many cities. This system grew from earlier community antenna systems used in areas with poor over-the-air television reception. To a first approximation, a MAN might look something like the system shown in fig. below :

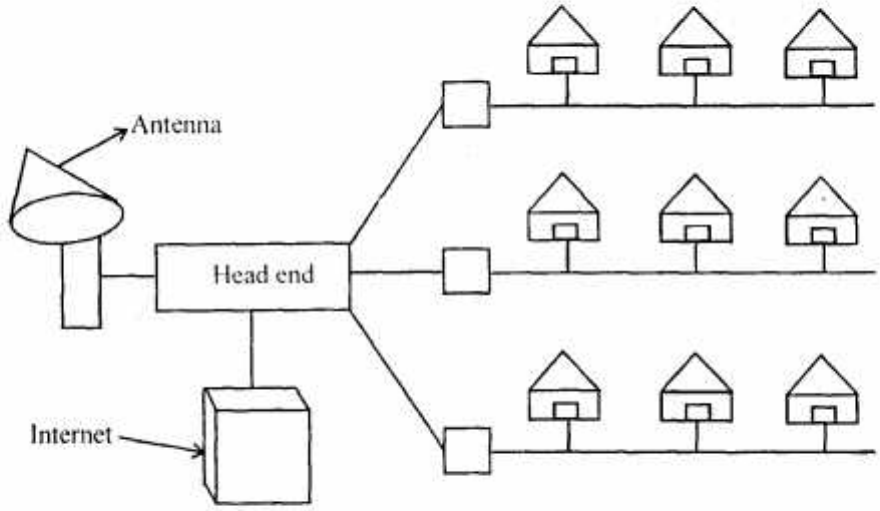


Fig. A Metropolitan Area N/W based on Cable TV

Q. 2. (a) What is TCP/IP model? Explain function of each layer.

Ans. TCP/IP Model : TCP/IP was developed prior to the OSI model. Therefore, layers in the TCP/IP protocol stack do not match exactly with those in the OSI model. The TCP/IP model is made up of five layers :

1. Physical layer
2. Data link layer
3. Network layer (IP)
4. Transport layer (TCP)
5. Application layer.

The first four layers provide physical standards, network interface, internet working & transport functions that correspond to the first four layers of the OSI model. The three top layers of the OSI model, however, are represented in the TCP/IP by a single layer called application layer. The fig. illustrates how TCP/IP protocol stack fits itself in the OSI reference model.

Physical & Data Link Layer : At this level, TCP/IP does not define any specific protocol. It supports all of the standard & proprietary protocols.

Network Layer : The Internet Protocol (IP) is used at this layer to provide the rating functions across multiple networks. IP is the transmission mechanism used by the TCP/IP protocols. IP in turns, contains four supporting protocols, ARP, RARP, ICMP & IGMP.

Transport Layer : At this layer, TCP/IP suite defines two protocols–UDP (User Datagram Protocol) & TCP (Transmission Control Protocol).

Application Layer : Finally, application layer contains the logic needed to support the various user applications.

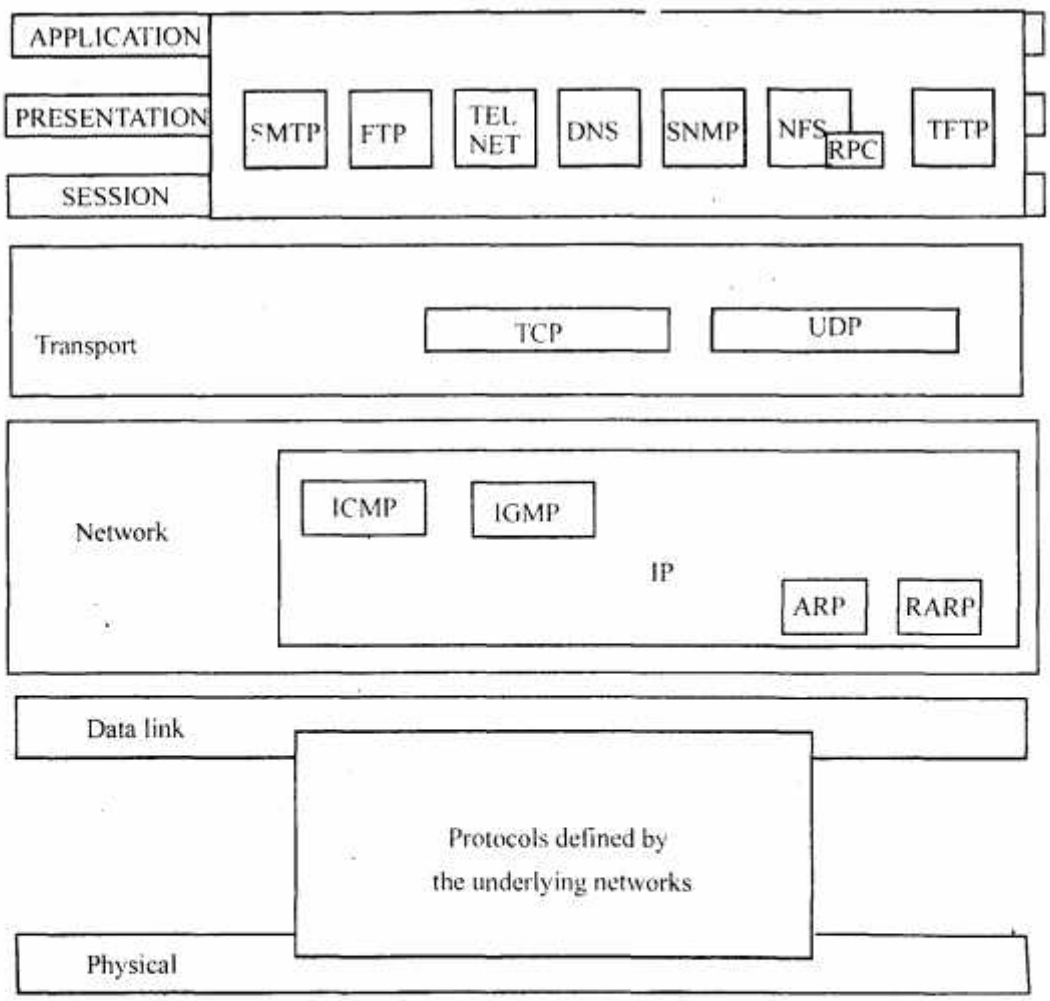


Fig. TCP/IP Protocols

Q. 2. (b) How IP addressing is carried out?

Ans. IP Addressing : Every host & router on the Internet has an IP address, which encodes its network number & host number. The combination is unique : no two machines have the same IP Address. All IP addresses are 32 bits long & are used in the source address & Destination address fields of IP packets. The formats used for IP address are shown in fig. Those machines connected to multiple networks have a different IP address on each network.

The class A, B, C & D formats allow for up to 126 networks with 16 million hosts each, 16,382 networks with up to 64k hosts, 2 million networks, with upto 254 hosts each, & multicast, in which a datagram is directed to multiple hosts. Addresses beginning with 11110 are reserved for future use. The lowest IP address is 0.0.0.0 & the highest is 255.255.255.255. The IP address 0.0.0.0 is used by hosts when they are being booted but is not used afterward.

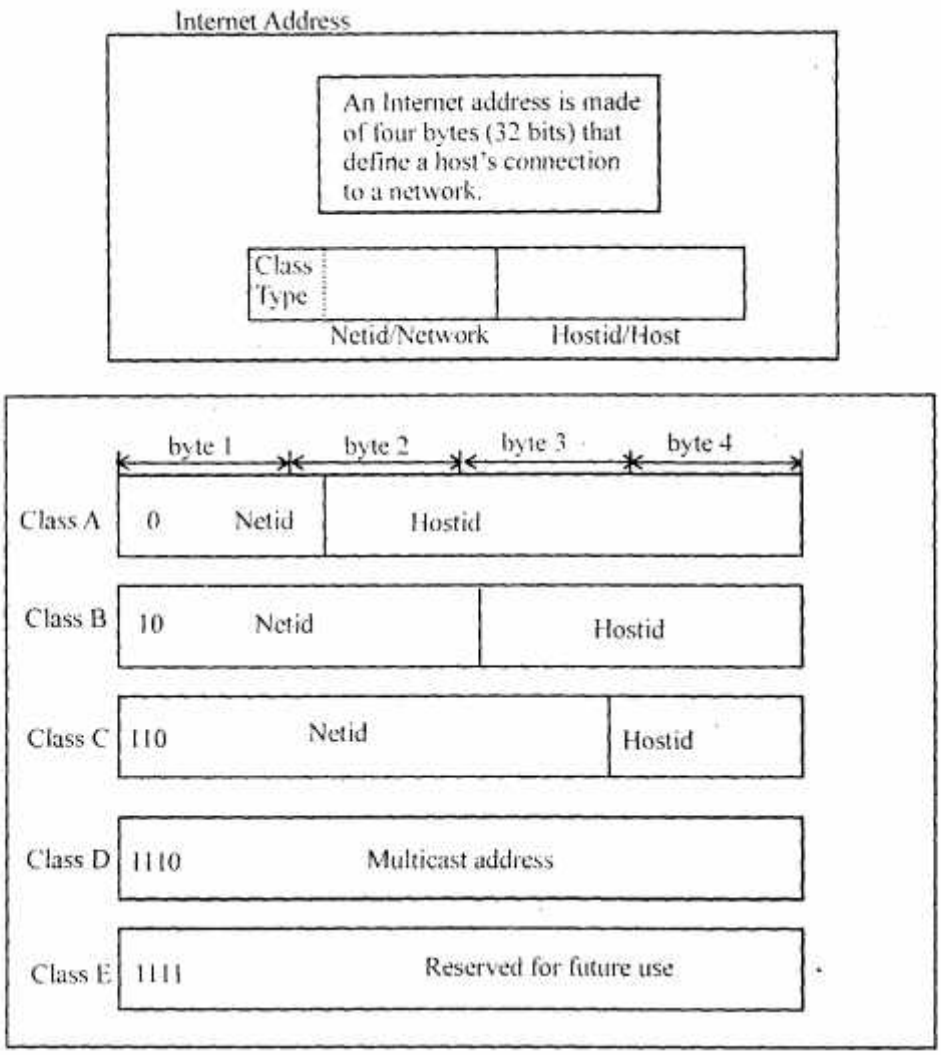


Fig. Internet Classes

Q. 2. (c) Compare TCP/IP with OSI model.

Ans. A Comparison of the OSI & TCP Reference Models : The OSI & TCP/IP reference models have much in common. Both are based on the concept of a stack independent protocols. Also, the functionality of the layers is roughly similar. The two models also have many differences. OSI model is to make the distinction between these three concepts (services, Interfaces, Protocols) explicit.

The TCP/IP model did not originally clearly distinguish between service, interface, & protocol, although people have tried to retrafit it after the fact to make it more OSI-Like.

The protocols in the OSI model are better hidden than in the TCP/IP model & can be replaced relatively easily as the technology changes. With the TCP/IP the reverse was true; the protocols came first, & the model was really just a description of existing protocols.

Q. 3. (a) Compare Bridges, Routers and Gateways.

Ans. Bridges : Bridges operate at data link layer of OSI model, giving it access to the physical addresses of all stations connected to it. When a frame enters a bridge, the bridge not only regenerates the signal but checks the address of the destination & forwards new copy only to the segment to which address belongs. As a packets arrives to the bridge, it reads the address in the frame & compose the address with table of all stations on both segments when it finds a match, it discovers the segment for forwarding the frame.

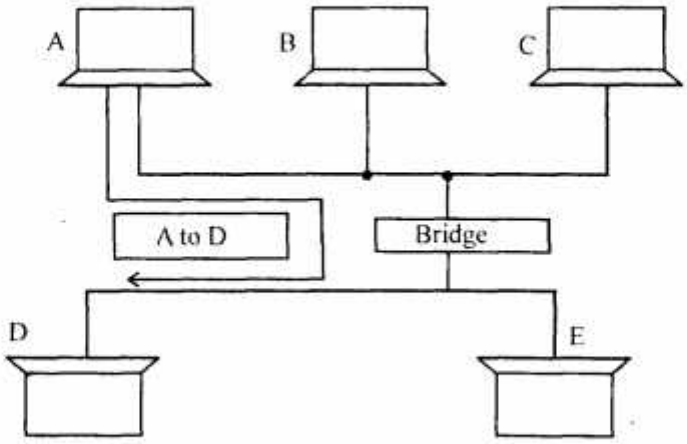


Fig. Bridge (Racket from A to D)

Routers : Routers access the network layer addresses & determine which of several possible paths between those addresses is the best for a particular transmission. Routers are found in network layer. They just take incoming packets from one line & forward them on another line, but lines may belong to different networks & use different protocols. A packet sent from a station or one network to a station on a neighbouring network gees first to the Jointing held router, which switches it over to the destination network.

Gateways : Gateways operate at transport layer. It is basically a protocol converter. A gateway can accept a packet formatted for one protocol (eg. Apple talk) & convert it to a packet formulated for another protocol (eg. TCP/IP) before forwarding it.

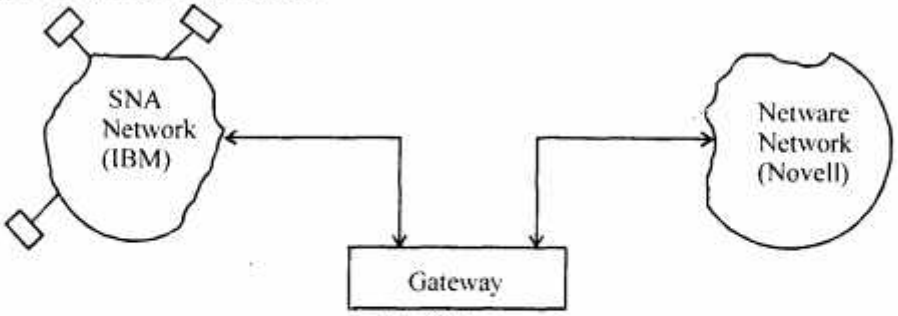


Fig. Gateway

Q. 3. (b) How CSMA/CD improves the performance of CSMA?

Ans. CSMA/CD Improves the Performance of CSMA : Whenever multiple users have unregulated access to a single line, there is a danger of signals overlapping and destroying each other. Such overlaps, which turn the signals into unusable noise are called collisions. The access mechanism used in an Ethernet is called carrier sense multiple access with collision detection (CSMA/CD, standardized in IEEE 802.3).

CSMA/CD is the result of an evolution from multiple access (MA) to carrier sense multiple access (CSMA) and finally to carrier sense multiple access with collision detection (CSMA/CD). In a CSMA system,

any workstation wishing to transmit must first listen for existing traffic on the line. A device listens by checking for a voltage.

If no voltage is detected, the line is considered idle and the transmission is initiated. CSMA cuts down on the number of collisions but does not eliminate them. Collisions can still occur. If another station has transmitted too recently for its signal to have reached the listening station, the listener assumes the line is idle and introduces its own signal onto the line. The final step is the addition of collision detection (CD). In CSMA/CD the station wishing to transmit first listens to make certain the link is free, then transmits its data, then listens again. During the data transmission, the station checks the line for the extremely high voltages that indicate a collision. If a collision is detected, the station quits the current transmission and waits a predetermined amount of time for the line to clear, then sends its data again.

Q. 3. (c) What are components of LAN?

Ans. Components of LAN : LAN is a made up of hardware as well as software components.

1. Hardware Components of LAN : Hardware components of LAN are :

(i) Transmission Channel : Transmission channel for LAN are :

(a) Twisted pair cable (b) Coaxial cable

(c) Fibre-optic cable (d) Radio waves

(ii) Servers

(a) File server (b) Printer server

(c) Modem server

(iii) Work stations.

(iv) Network Interface Units (NIU)

(v) Hub

(a) Active hub (b) Passive hub

(vi) Shared resources

(vii) Modem.

2. Software Components of LAN : The software includes the drivers for all peripherals and LAN operating system that manages the network. The LAN operating system is the software that facilitates file and print serving, as well as ordinary communications between workstations, such as electronic mail. Some popular LAN operating system are :

(i) Novel network (ii) PC network

(iii) Ethernet (iv) Arc Net

(v) Token ring etc.

Q. 4. (a) What are congestion control protocols?

Ans. Congestion occurs when the no. of packets in the subnet is more than the no. of buffers. There are congestion control protocols for solving the congestion problem. There are various strategies for congestion control :

1. Traffic Shaping : If host transmits at a uniform rate, congestion is less. Another method to manage congestion is to force the packets to be transmitted at more predictable rate. This approach to congestion management is called traffic shaping.

2. Leaky Bucket Algorithm : Each host is connected to network by an interface containing a Leaky Bucket, a finite internal queue. If a packet arrives at the queue when it is full, packet is discarded. This arrangement can be built into the hardware interface or simulated by host operating system. This algorithm is called leaky bucket algorithm.

3. Token Bucket Algorithm : Sometimes it is better to allow the output to speed up when large burst arrives, so a more flexible algorithm is required, one that never loses data. One such algorithm is token bucket algorithm.

Q. 4. (b) What is a Frame relay?

Ans. Frame Relay : It is a service for possible who want an absolute base bones connection oriented way to move bits from A to B at reasonable speed & low cost. Its existence is due to changes in technology over the past two decades. Frame relay can best be thought of as a virtual leased line. The difference between an actual leased line & a virtual leased line is that with an actual one, the user can send traffic all day long at the maximum speed. With a virtual one, data bursts may be sent at full speed, but the long term average usage must be below a predetermined level. In return, the carrier charges much less for a virtual line than a physical one.

In addition to competing with leased lines, frame relay also competes with X 2S permanent virtual circuits, except that it operates at higher speeds, usually 1.5 Mbps, & provides fewer features.

Q. 4. (c) What do you mean by wireless networks? Explain.

Ans. Wireless Network : Connecting computers in a network without wire is wireless network. Since having a wired connection is impossible in care & airplanes, there is a lot of interest in wireless network. Wireless networks have many uses. A common one is the portable office. People on the road often want to use their portable electronic equipment to send & receive telephone calls, faxes & electronic mail, read remote files, login on remote machines & so on, & do this from anywhere on land, sea or air. Wireless networks are of great value to fleets of trucks, taxis buses & repair persons for keeping in contact with home. Although wireless LANs are easy to install, they also have some disadvantages. Typically they have a capacity of 1-2 Mbps, which is much slower than wired LANs. The error rates are often much higher , too, & the transmissions from different computers can interfere with one another.

Q. 5. (a) What are popular remote monitoring techniques?

Ans. When a user wants to access an application program or utility located on a remote machine, he or she performs remote login. Here the TELNET client and server programs come into use. The user sends the keystrokes to the terminal driver where the local operating system accepts the characters but does not interpret them. The characters are sent to the TELNET client, which transforms the characters to a universal character set called network virtual terminal characters and delivers them to the local TCP/IP stack.

Network Virtual Terminal (NVT) : The mechanism to access a remote computer is complex. This is because every computer and its operating system accepts a special combination of characters as tokens. For example, the end-of-file token in a computer running the DOS operating system is ctrl+z, while the UNIX operating system recognizes ctrl+d.

We are dealing with heterogeneous systems. If we want to access any remote computer in the world. We first must know to what type of computer we will be connected, and we also must install the specific terminal emulator used by that computer. TELNET solves this problem by defining a Universal interface called the network virtual terminal (NVT) character set. Via this interface, the client TELNET translates characters that come from the local terminal into NVT form and delivers them to the network. The server TELNET, on the other hand, translates data and commands from NVT form into the form acceptable by the remote computer.

Q. 5. (b) What are Firewalls? How these are helpful?

Ans. Firewalls : A firewall is a security mechanism used by organizations to protect their LANs from the Internet. A firewall keeps private resources confidential & minimizes security risks. The firewall has two components : two routers that do packet filtering & an application gateway. Simpler configurations also exist, but the advantage of this design is that every packet must transit two filters & an application gateway to go in or out. No other route exists. Each packet filter is a standard router equipped with some functionality. The extra functionality allows every incoming or outgoing packet to be inspected. Packets meeting some criterion are

forward normally. Those that fail the test are dropped. Thus overall we can say like; a company can have many LANs connected in arbitrary ways, but all traffic to or from the company is forced through an electronic drawbridge (firewall).

Q. 5. (c) How performance of a network is managed?

Ans. Performance issues are very important in computer networks. When thousands of computers are connected together complex interactions, with unforeseen consequences are common. Frequently this complexity leads to poor performance & no one knows why. There are various issues related to network performance. Five aspects of network performance are :

1. Performance problems
2. Measuring network performance
3. System design for better performance.
4. Fast TPDU processing.
5. Protocols for future high performance networks.

Network performance is typically dominated by protocol & TPDU processing overhead, & this situation gets worse at higher speeds. Protocols should be designed to minimize the no. of TPDUs, context switches, & times each TPDU is copied. For gigabit networks, simple protocols using rate, rather than credit, flow control are called for.

Q. 6. (a) What is difference between scope of SMTP, POP, HTTP and FTP?

Ans. SMTP : One of the most popular network services is electronic mail (e-mail). The TCP/IP protocol that supports electronic mail on the Internet is called Simple Mail Transfer Protocol (SMTP). It is a system for sending messages to other computer users based on e-mail addresses

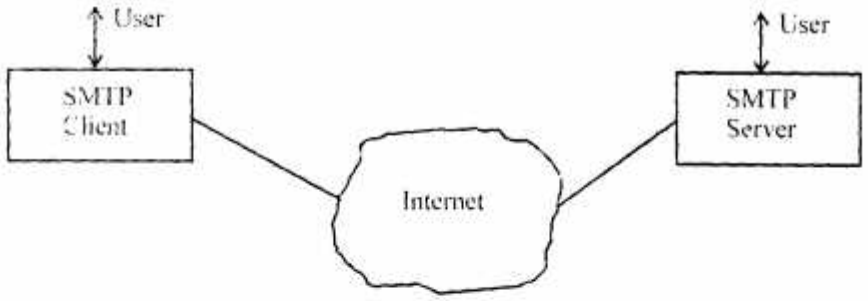
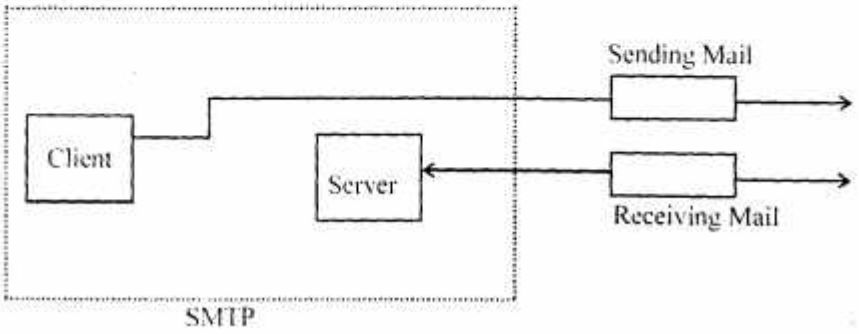
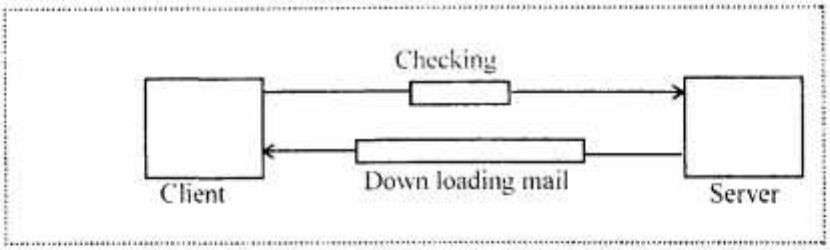


Fig. SMTP concept

POP (Post Office Protocol) :



http://studentsuvidha.in/ and http://studentsuvidha.in/forum



POP3

SMTP expects the destination host, the mail server receiving the mail, to be on aline all the time, otherwise, a TCP connection cannot be established. For this reason, it is not practical to establish in SMTP session with a desktop computer because desktop computers are usually powered down at the end of the day. In many organizations, mail is received by an SMTP server that is always on line. This SMTP server provides a mail drop service.

The server receives the mail on behalf of every host in the organization. Workstations interact with the SMTP host to receive messages by using a client server protocol such as Post Office Protocol (POP) version 3 (POP 3).

Although POP3 is used to download messages from the server, the SMTP client is still needed on the desktop to forward messages from the workstation user to its SMTP mail server.

HTTP : The standard web transfer protocol is HTTP (Hyper Text Transfer Protocol). The HTTP protocol consist of two fairly distinct items; the set of requests from browsers to servers & the set of responses going back the other way.

FTP : The FTP protocol is used to access files by FTP, the Internet's file transfer protocol. FTP has been around more than two decades and is well entrenched. Numerous FTP servers all over the world allow people anywhere on the Internet to log in and download whatever files have been placed on the FTP server. The web does not change this, it just makes obtaining files by FTP easier, as FTP has a somewhat arcane interface. In due course, FTP will probably vanish, as there is no particular advantage for a site to run an FTP server instead of an HTTP server, which can do everything that the FTP server can do, and more.

Q. 6. (b) What are internet control protocols?

Ans. The IP module is central to the success of internet technology. The Internet Protocol or IP builds a single logical network from multiple physical networks. Thus, Internet Protocol (IP) is the most important protocol. The higher layers see only a one virtual or logical network & they need not be aware of where exactly the physical network resides, its architecture & so on. As far as the higher layers are concerned, each host on the Internet is a system with a unique IP address. This interconnection of physical networks into a single virtual or logical network is the source of the name : internet. A set of interconnected physical networks, that limit the range of an IP packet is called an Internet. Apart from providing a virtual network service to the upper layers, it is the IP layer which transports the datagram packet from source to destination system across several physical networks. It is the lowest level protocol which provides the host-to-host datagram delivery mechanism. The layers below this only deliver the datagram within a single physical network.

It is an unreliable & connectionless datagram protocol—a best effort delivery service. The term best effort means that IP provides no error checking or tracking. IP assumes the unreliability of the underlying layers & does its best to get a transmission through to its destination, but with no guarantees. IP assumes that upper layer protocols will take care of the reliability issues if they need. The important concepts of the Internet Protocols are such as addressing, routing & IP datagrams.

Q. 7. (a) What is an Ethernet? How you define a fast ethernet? Where it is required?

Ans. IEEE 802.3 supports a LAN standard originally developed by a xerox & later extended by a joint venture between digital equipment corporation, Intel & Xerox. This was called Ethernet.

The IEEE 802.3 standard is for a 1-Persistent CSMA/CD LAN. Or, CSMA/CD is fast Ethernet. To review the idea, when a station wants to transmit, it listens to the cable. If the cable is busy, the station waits until it goes idle; otherwise it transmits immediately. If two or more stations simultaneously begin transmitting on an idle cable, they will collide. All colliding stations then terminate their transmission, wait a random time, & repeat the whole process all over again.

Q. 7. (b) Explain features of a network OS (Operating System).

Ans. A network operating system, or NOS, is software that manages the sharing of files over a network. A network operating system is, therefore, usually responsible for the following :

1. Maintaining user accounts & passwords to provide some level of security for the network.
2. File management on the server.
3. Scheduling of programs & services to be run at regular internals.
4. Printing.
5. File locking & synchronization.
6. Accounting

NOS may be an add-on to a single user operating system or it may be integrated into a complete operating system product.

Q. 8. Write short notes on :

(a) IPV 6 and IPV 4 (b) ATM (c) UDP

Ans. (a) IPV 6 and IPV 4 : IPV 6 & IPV4 (Internal Protocol Version 6 & Internet Protocol Version 4), respectively are the versions of IP routing protocol. IPV 6 has layer addresses than IPV4. They are 16 bytes long, which solves the problem that IPV6 was set out to solve; provide an effectively unlimited supply of internet addresses. The second improvement of IPV6 is the simplification of the header. It contains only 7 fields (versus 13 in IPV 4). This change allows routers to process packets faster & thus improve throughout. The third major improvement was better support for options. The change was essential with the new header because fields that previously were required are now optional. A fourth area in which IPV6 represents a big advance is in security.

(b) ATM : Asynchronous Transfer Mode (ATM) is the cell relay protocol designed by ATM forum & adopted by ITU-T. The Combination of ATM & B-ISDN will allow high speed Interconnection of all the world's networks. ATM represents cell switching technology that can operate at speeds ranging from T11.s44 Mbps to gigabit speeds of SONET. The ATM components are :

1. ATM n/w interface cards.
2. ATM Law switches
3. ATM Routers
4. ATM WAN switches
5. ATM services processor.

Thus ATM is a network of end point & switches.

(c) UDP : UDP is User Datagram Protocol. UDP is a connectionless, unreliable transport protocol. It does not add anything to the services of IP except for providing process-to-process communication. Also it performs very limited error checking. Because of its simplicity, it is more efficient. Establishing a connection with the destination process is fast, & if reliability is not an important criteria, then the transfer of data is faster for bulk transfer. This is because reliability requires implementing the acknowledgements, resending the lost or corrupted datagrams & many more overheads. This definitely decreases rate at which datagrams can be sent. UDP is the desired protocol for various applications at transport layer.