Solved Paper 2013-14
Computer Network
B.Tech (IT) VI semester

Q.1.

a. Discuss the TCP/IP protocol suite on the basis of protocol layering principle.

Application Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Physical Layer : The physical layer is responsible for transmitting individual bits from one node to the next.

Data Link Layer : The data link layer is responsible for transmitting frames from one node to the next.

Network Layer: The network layer is responsible for the delivery of packets from the original source to the final destination.

Transport Layer : The transport layer is responsible for delivery of a message from one process to another.

Application Layer : The application layer is responsible for providing services to the user.

b. Define topology and explain the advantage and disadvantage of Bus, Star and Ring topologies.

A Topology of the network defines the manner in which the network devices are arranged and connected to each other in a network. It defines the shape of communication network. There are five common types of network Topologies.

Advantages of Bus Topology

- Most bus networks have the advantage of being passive i.e all the active components are in the stations or nodes, and a failure affects only that one node.
- It does not require all the computers to be up and running in order for network to function.

Disadvantages of Bus Topology

- Because single cable is dedicated to all the computers the performance can suffer at time because of heavy traffic.
- There is a distance limitation in bus topology. After certain length of cable the performance of the Bus network degrades

Advantages Of star topology

- This topology has the advantage of minimum data traffic along the cables (node to server only)., thus providing optimum performance.
- The main advantage of star LAN are that the access to the network i.e decision on when a station can or cannot transmit, is under central control.

Disadvantages of Star Topology

- Because single central machine must coordinate all communications, this topology requires an extremely powerful server. Hence Star Topology is expensive.

- Speed is generally limited and central switch is an obvious potential source of catastrophic failure i.e if centralised server fails, whole topology fails.

Advantages of ring topology

- Performance is good because each portion of cabling system is handling the data flow between two nodes (machines) only.
- They do not have distance limitations as in Bus topology (difference between Bus and ring topology).
- They can take advantages of fiber optic cables to speed up the performance, because only two machines are involved in packet exchange at a time.

Disadvantages of Ring Topology

- Since all the nodes or computers are involved in data transfer, the failure of single node can bring whole network to the halt.
- The ring control mechanism required to determine as to who should start up the ring, to determine that the packets are not corrupt, and to prevent the same packet to go around the ring because of network fault. Some Ring LANs need to deploy special computer to monitor this issue.

c. Explain briefly the bus backbone and star backbone.

Bus Backbone: In a bus backbone, the topology of the backbone is a bus. The backbone itself can use one of the protocols that support a bus topology such as lOBase5 or lOBase2. Bus backbones are normally used as a distribution backbone to connect different buildings in an organization. Each building can comprise either a single LAN or another backbone (normally a star backbone). A good example of a bus backbone is one that connects single- or multiple-floor buildings on a campus. Each single-floor building usually has a single LAN. Each multiple-floor building has a backbone (usually a star) that connects each LAN on a floor. A bus backbone can interconnect these LANs and backbones

Star Backbone: In a star backbone, sometimes called a collapsed or switched backbone, the topology of the backbone is a star. In this configuration, the backbone is just one switch (that is why it is called, erroneously, a collapsed backbone) that connects the LANs. Star backbones are mostly used as a distribution backbone inside a building. In a multifloor building, we usually find one LAN that serves each particular floor. A star backbone connects these LANs. The backbone network, which is just a switch, can be installed in the basement or the first floor, and separate cables can run from the switch to each LAN. If the individual LANs have a physical star topology, either the hubs (or switches) can be installed in a closet on the corresponding floor, or all can be installed close to the switch. We often find a rack or chassis in the basement where the backbone switch and all hubs or switches are installed.

d. Explain the user access in ISDN.

ISDN stands for Integrated Services Digital Network. It is a design for a completely digital telephone/telecommunications network. It is designed to carry voice, data, images, video, everything you could ever need. It is also designed to provide a single interface (in terms of both hardware and communication protocols) for hooking up your phone, your fax machine, your computer, your videophone, your video-on-demand system (someday), and your microwave.

- Two types of user access are defined
  - Basic Access - Consists of two 64Kbps user channels (B channel) and one 16Kbps signally channel (D channel) providing service at 144 Kbps.

- Primary access - Consists of thirty 64Kbps user channels (B channels) and a 64 Kbps signally channel (D channel) providing service at 2.048Mbps (One 64 Kbps channel is used for Framing and Synchronization).

- **Explain the user access in ISDN.**

e. Compare the twisted pair, coaxial cable and fiber optic cable.

- **COAXIAL CABLE**

  - advantages

  sufficient frequency range to support multiple channel, which allows for much greater throughput.

- lower error rates. because the inner conductor is in a Faraday shield, noise immunity is improved, and coax has a lower error rates and therefore slightly better performance than twisted pair.
- greater spacing between amplifiers coax's cable shielding reduces noise and crosstalk, which means amplifiers can be spaced farther apart than with twisted pair.

  - disadvantages

    - more expensive to install compare to twisted pair cable.
    - the thicker the cable, the more difficult to work with.

FIBER OPTIC CABLE

- advantages

- system performance
- greatly increased bandwidth and capacity
- lower signal attenuation (loss)
- immunity to electrical noise
- immune to noise (electromagnetic interference and radio frequency interference)
- less restrictive in harsh environments
- overall system economy

- disadvantages

fiber optic component are expensive

- fiber optic transmitters and receivers are still relatively expensive compared to electrical interfaces
- the lack of standardization in the industry has also limited the acceptance of fiber optics.

TWISTED PAIR CABLE

- advantages

using telephone wires are their relative low cost and their availability

- handled a data flow of up to approximately one megabit per second (Mbps) over several hundred feet
- small local area network with a limited number of users, twisted pair is an ideal choice because it is both inexpensive and easy to install.

- disadvantages

susceptibility to signal distortion errors and the relatively low transmission rates they provide over long distances.

f. Explain the various types of Switching Methods with suitable example.

Circuit Switching

When two nodes communicates with each other over a dedicated communication path, it is called circuit switching. There's a need of pre-specified route from which data will travel

and no other data will permitted. In simple words, in circuit switching, to transfer data circuit must established so that the data transfer can take place.

Circuits can be permanent or temporary. Applications which use circuit switching may have to go through three phases:

- Establish a circuit
- Transfer of data
- Disconnect the circuit

Circuit switching was designed for voice applications. Telephone is the best suitable example of circuit switching. Before a user can make a call, a virtual path between caller and callee is established over the network.

Message Switching

This technique was somewhere in middle of circuit switching and packet switching. In message switching, the whole message is treated as a data unit and is switching / transferred in its entirety.

A switch working on message switching, first receives the whole message and buffers it until there are resources available to transfer it to the next hop. If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits.

This technique was considered substitute to circuit switching. As in circuit switching the whole path is blocked for two entities only. Message switching is replaced by packet switching. Message switching has some drawbacks:

- Every switch in transit path needs enough storage to accommodate entire message.
- Because of store-and-forward technique and waits included until resources available, message switching is very slow.
- Message switching was not a solution for streaming media and real-time applications.

Packet Switching

Shortcomings of message switching gave birth to an idea of packet switching. The entire message is broken down into smaller chunks called packets. The switching information is added in the header of each packet and transmitted independently.

It is easier for intermediate networking devices to store smaller size packets and they do not take much resources either on carrier path or in the switches' internal memory.

Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier. The internet uses packet switching technique. Packet switching enables the user to differentiate data streams based on priorities. Packets are stored and forward according to their priority to provide Quality of Service.

Q 2.

a. State drawbacks of stop and wait protocols.

Major Drawback of Stop-and-Wait Flow Control:

- Only one frame can be in transmission at a time
- This leads to inefficiency if propagation delay is much longer than the transmission delay

b. What is Piggybacking?

Piggybacking is a bi-directional data transmission technique in the network layer (OSI model). It makes the most of the sent data frames from receiver to emitter, adding the confirmation that the data frame sent by the sender was received successfully (ACK acknowledge). This practically means, that instead of sending an acknowledgement in an individual frame it is piggy-backed on the data frame.

c. Which are the requirements of CRC?

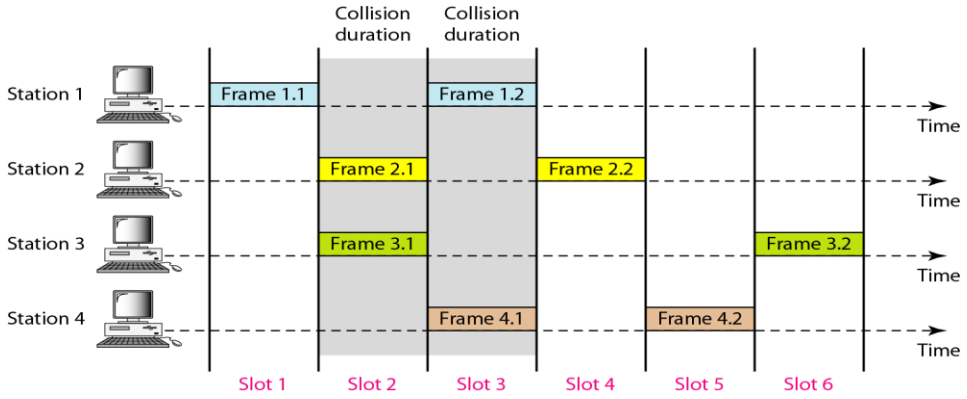
Cyclic redundancy checking is a method of checking for errors in data that has been transmitted on a communications link. A sending device applies a 16- or 32-bit polynomial to a block of data that is to be transmitted and appends the resulting cyclic redundancy code (CRC) to the block. The receiving end applies the same polynomial to the data and compares its result with the result appended by the sender. If they agree, the data has been received successfully. If not, the sender can be notified to resend the block of data.

d. How can you compare pure ALOHA and Slotted Aloha?

Pure ALOHA has a vulnerable time of 2 x *Tfr* . This is so because there is no rule that defines when the station can send. A station may send soon after another station has started or soon before another station has finished. Slotted ALOHA was invented to improve the efficiency of pure ALOHA.

In slotted ALOHA we divide the time into slots of Tfr s and force the station to send only at the beginning of the time slot.

Frames in a slotted ALOHA network



Because a station is allowed to send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot. This means that the station which started at the beginning of this slot has already finished sending its frame. Of course, there is still the possibility of collision if two stations try to send at the beginning of the same time slot. However, the vulnerable time is now reduced to one-half, equal to *Tfr* Figure shows the situation. Figure shows that the vulnerable time for slotted ALOHA is one-half that of pure ALOHA.

SlottedALOHA vulnerable time = Tfr

Throughput It can be proved that the average number of successful transmissions for slotted ALOHA is S = G x *e-G*. The maximum throughput Smax is 0.368, when G = 1. In other words, if a frame is generated during one frame transmission time, then 36.8 percent of these frames reach their destination successfully. This result can be expected because the vulnerable time is equal to the frame transmission time. Therefore, if a station generates only one frame in this vulnerable time (and no other station generates a frame during this time), the frame will reach its destination successfully.

e. Explain about CSMA/CD and CSMA/CA and its uses.

CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network. Devices attached to the network cable listen (carrier sense) before transmitting. If the channel is in use, devices wait before transmitting. MA (multiple access) indicates that many devices can connect to and share the same network. All devices have equal

access to use the network when it is clear. Even though devices attempt to sense whether the network is in use, there is a good chance that two stations will attempt to access it at the same time. On large networks, the transmission time between one end of the cable and another is enough that one station may access the cable even though another has already just accessed it. There are two methods for avoiding these so-called collisions, listed here:

CSMA/CD (carrier sense multiple access/collision detection) CD (collision detection) defines what happens when two devices sense a clear channel, then attempt to transmit at the same time. A collision occurs, and both devices stop transmission, wait for a random amount of time, then retransmit. This is the technique used to access the 802.3 Ethernet network channel. This method handles collisions as they occur, but if the bus is constantly busy, collisions can occur so often that performance drops drastically. It is estimated that network traffic must be less than 40 percent of the bus capacity for the network to operate efficiently. If distances are long, time lags occur that may result in inappropriate carrier sensing, and hence collisions.

CSMA/CA (carrier sense multiple access/collision avoidance) In CA (collision avoidance), collisions are avoided because each node signals its intent to transmit before actually doing so. This method is not popular because it requires excessive overhead that reduces performance.

f. Differentiate between 802.3 and 802.4 and 802.5 IEEE Standards.

802.3 Ethernet

Now that we have an overview of the OSI model, we can continue on these topics. I hope you have a clearer picture of the network model and where things fit on it. 802.3 is the standard which Ethernet operates by. It is the standard for CSMA/CD (Carrier Sense Multiple Access with Collision Detection). This standard encompasses both the MAC and Physical Layer standards. CSMA/CD is what Ethernet uses to control access to the network medium (network cable). If there is no data, any node may attempt to transmit, if the nodes detect a collision, both stop transmitting and wait a random amount of time before retransmitting the data. The original 802.3 standard is 10 Mbps (Megabits per second). 802.3u defined the 100 Mbps (Fast Ethernet) standard, 802.3z/802.3ab defined 1000 Mbps Gigabit Ethernet, and 802.3ae define 10 Gigabit Ethernet. Commonly, Ethernet networks transmit data in packets, or small bits of information. A packet can be a minimum size of 72 bytes or a maximum of 1518 bytes. The most common topology for Ethernet is the star topology.

802.5 Token Ring

When discussing the ring topology, Token Ring was developed primarily by IBM. Token ring is designed to use the ring topology and utilizes a token to control the transmission of data on the network. The token is a special frame which is designed to travel from node to node around the ring. When it does not have any data attached to it, a node on the network can modify the frame, attach its data and transmit. Each node on the network checks the token as it passes to see if the data is intended for that node, if it is; it accepts the data and transmits a new token. If it is not intended for that node, it retransmits the token on to the next node. The token ring network is designed in such a way that each node on the network is guaranteed access to the token at some point. This equalizes the data transfer on the network. This is different from an Ethernet network where each workstation has equal access to grab the available bandwidth, with the possible of a node using more bandwidth than other nodes. Originally, token ring operated at a speed of about 4 Mbps and 16 Mbps. 802.5t allows for 100 Mbps speeds and 802.5v provides for 1 Gbps over fibber. Token ring can be run over a

star topology as well as the ring topology. There are three major cable types for token ring: Unshielded twisted pair (UTP), Shielded twisted pair (STP), and fibber. Token ring utilizes a Multi-station Access Unit (MAU) as a central wiring hub. This is also sometimes called a MSAU when referring to token ring networks.

Q 3.

a. What is meant by fragmentation? Is fragmentation needed in concentrated virtual circuit internets, or in any datagram system?

Networks differ in various ways, so when multiple networks are interconnected problems can occur. Sometimes the problems can be finessed by tunneling a packet through a hostile network, but if the source and destination networks are different, this approach fails. When different networks have different maximum packet sizes, fragmentation may be called for.

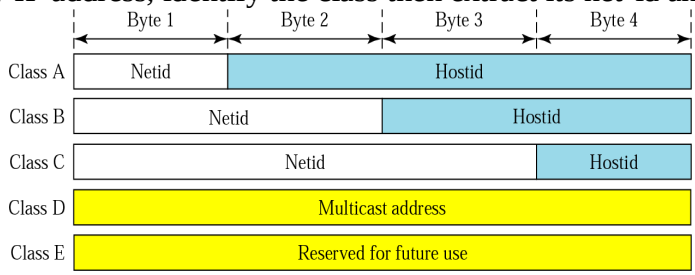
Definition of: IP fragmentation: Breaking an IP datagram (packet) into pieces in order to be sent across a transmission link with a frame size smaller than the datagram. Performed in a router, the header of the original IP packet is replicated with minor changes to each of the fragments. If one of the fragments is dropped, the original datagram must be fragmented again and retransmitted.

Fragmentation is when a datagram has to be broken up into smaller datagrams to fit the frame size of a certain network. Different networks have different MTUs (maximum transfer unit), when a datagram enters a network with a smaller MTU the gateway/router needs to fragment this packet into smaller packets that fit the new MTU.

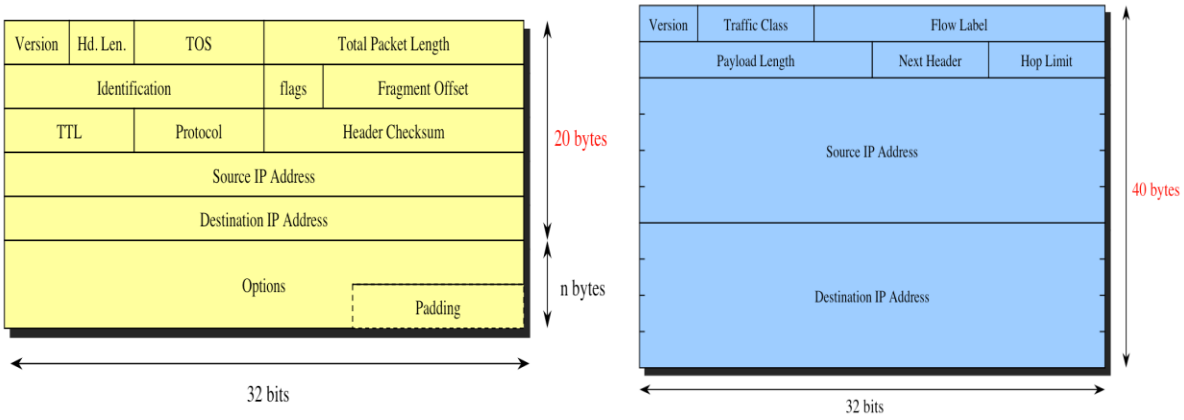
Fragmentation is needed in both. Even in a concatenated virtual-circuit network, some networks along the path might accept 1024 – byte packets, and others might only accept 48-byte packets. Fragmentation is still needed.

b. Give an IP address, how will you extract its net-id and host-id and compare IPv4 and IPv6 with frame format.

For any IP address, identify the class then extract its net-id and host-id.



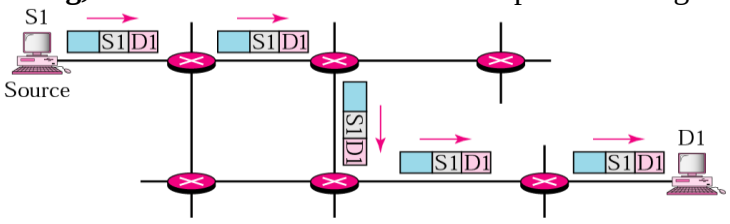
IPv4 Header **IPv6 Header**



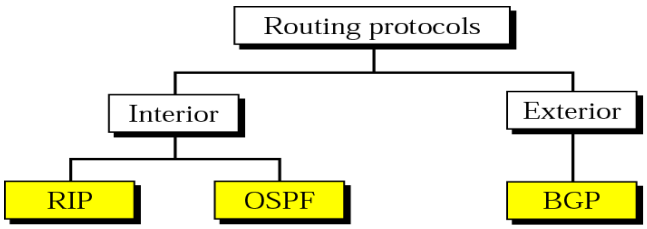
Comparison
1. The header length field is eliminated in IPv6 because the length of the header is fixed in this version.
2. The service type field is eliminated in IPv6. The priority and flow label fields together take over the function of the service type field.
3. The total length field is eliminated in IPv6 and replaced by the payload length field.
4. The identification, flag, and offset fields are eliminated from the base header in IPv6. They are included in the fragmentation extension header.
5. The TTL field is called hop limit in IPv6.
6. The protocol field is replaced by the next header field.
7. The header checksum is eliminated because the checksum is provided by upper-layer protocols; it is therefore not needed at this level.
8. The option fields in IPv4 are implemented as extension headers in IPv6.

c. (i) What is meant by unicast and multicast routing with suitable diagrams?

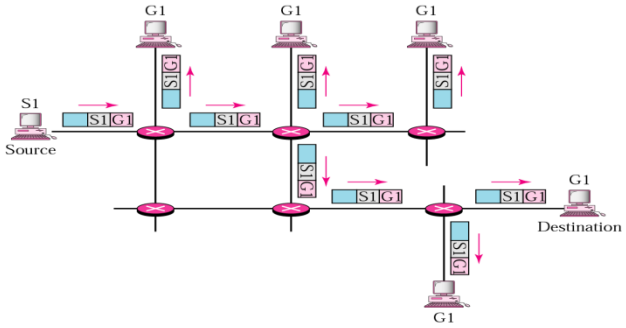
In unicast routing, the router forwards the received packet through only one of its ports



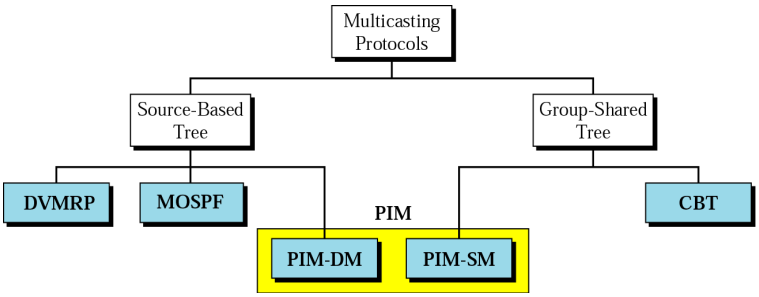
Unicast Routing Protocols:



In multicast routing, the router may forward the received packet through several of its ports.

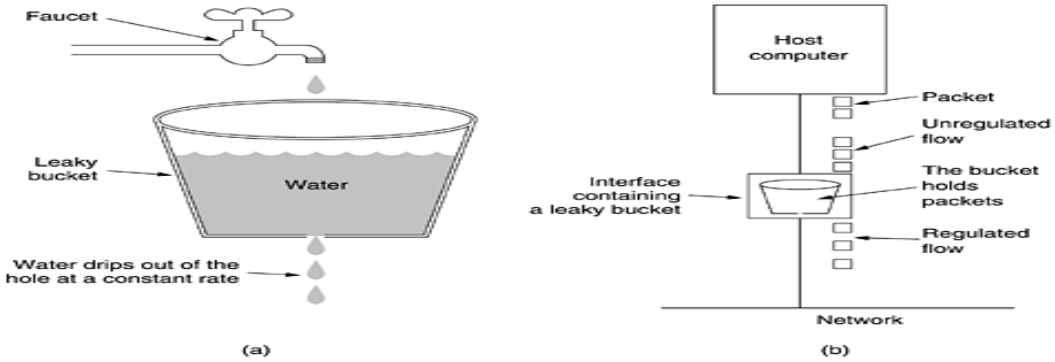


Multicast Routing Protocols:



(ii) Write a short note on Leaky bucket algorithm.

Leaky Bucket Algorithm



Conceptually, each host is connected to the network by an interface containing a leaky bucket, that is, a finite internal queue. If a packet arrives at the queue when it is full, the packet is discarded. In other words, if one or more processes within the host try to send a packet when the maximum number is already queued, the new packet is unceremoniously discarded. This arrangement can be built into the hardware interface or simulated by the host operating system. It was first proposed by Turner (1986) and is called the leaky bucket algorithm. In fact, it is nothing other than a single-server queueing system with constant service time.

The host is allowed to put one packet per clock tick onto the network. Again, this can be enforced by the interface card or by the operating system. This mechanism turns an uneven flow of packets from the user processes inside the host into an even flow of packets onto the network, smoothing out bursts and greatly reducing the chances of congestion.

When the packets are all the same size (e.g., ATM cells), this algorithm can be used as described. However, when variable-sized packets are being used, it is often better to allow a fixed number of bytes per tick, rather than just one packet. Thus, if the rule is 1024 bytes per tick, a single 1024-byte packet can be admitted on a tick, two 512-byte packets, four 256-byte packets, and so on. If the residual byte count is too low, the next packet must wait until the next tick.

Implementing the original leaky bucket algorithm is easy. The leaky bucket consists of a finite queue. When a packet arrives, if there is room on the queue it is appended to the queue; otherwise, it is discarded. At every clock tick, one packet is transmitted (unless the queue is empty).

The byte-counting leaky bucket is implemented almost the same way. At each tick, a counter is initialized to n. If the first packet on the queue has fewer bytes than the current value of the counter, it is transmitted, and the counter is decremented by that number of bytes.

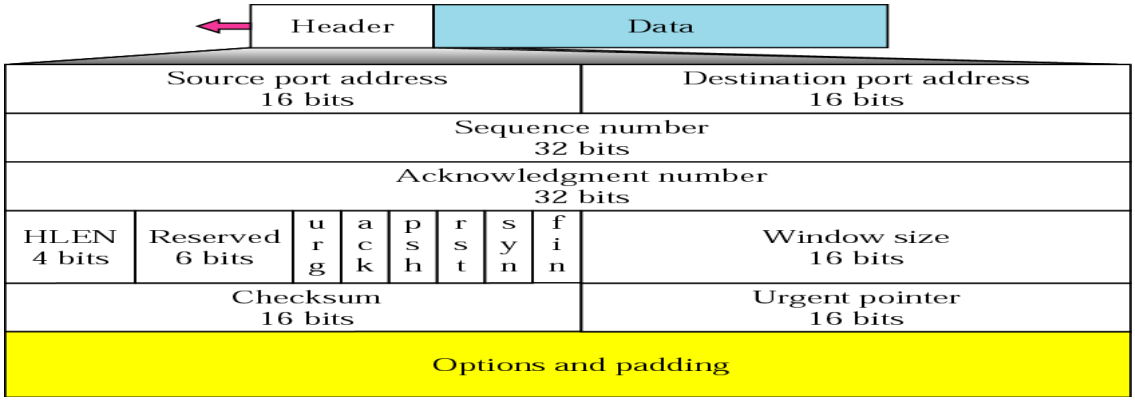
Additional packets may also be sent, as long as the counter is high enough. When the counter drops below the length of the next packet on the queue, transmission stops until the next tick, at which time the residual byte count is reset and the flow can continue.

Q 4.

a. Explain about the TCP header and working of TCP protocol and difference between TCP and UDP with frame format.

TCP is a connection-oriented protocol; it creates a virtual connection between two TCPs to send data. In addition, TCP uses flow and error control mechanisms at the transport level.

TCP segment format



Source Port. 16 bits.

Destination Port. 16 bits.

Sequence Number. 32 bits. The sequence number of the first data byte in this segment. If the SYN bit is set, the sequence number is the initial sequence number and the first data byte is initial sequence number + 1.

Acknowledgment Number. 32 bits. If the ACK bit is set, this field contains the value of the next sequence number the sender of the segment is expecting to receive. Once a connection is established this is always sent.

Data Offset. 4 bits. The number of 32-bit words in the TCP header. This indicates where the data begins. The length of the TCP header is always a multiple of 32 bits.

reserved. 3 bits. Must be cleared to zero.

Difference between TCP and UDP

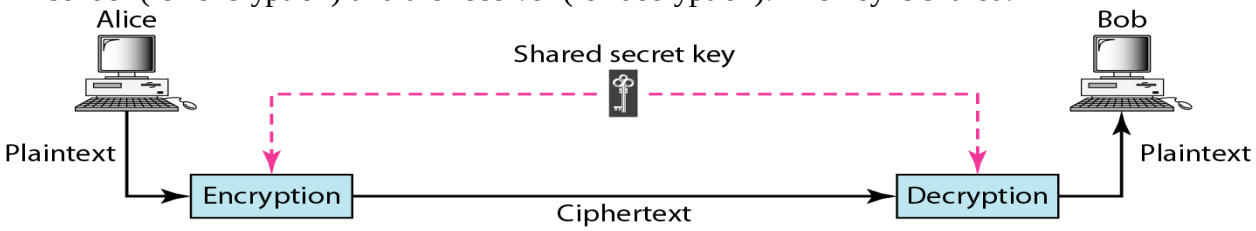
TCP	UDP
Reliability: TCP is connection-oriented protocol. When a file or message send it will get delivered unless connections fails. If connection lost, the server will request the lost part. There is no corruption while transferring a message.	*Reliability*: UDP is connectionless protocol. When you a send a data or message, you don't know if it'll get there, it could get lost on the way. There may be corruption while transferring a message.
Ordered: If you send two messages along a connection, one after the other, you know the first message will get there first. You don't have to worry about data arriving in the wrong order.	*Ordered*: If you send two messages out, you don't know what order they'll arrive in i.e. **no ordered**

Heavyweight: - when the low level parts of the TCP "stream" arrive in the wrong order, resend requests have to be sent, and all the out of sequence parts have to be put back together, so requires a bit of work to piece together.	*Lightweight*: No ordering of messages, no tracking connections, etc. It's just fire and forget! This means it's a lot quicker, and the network card / OS have to do very little work to translate the data back from the packets.
Streaming: Data is read as a "stream," with nothing distinguishing where one packet ends and another begins. There may be multiple packets per read call.	*Datagrams*: Packets are sent individually and are guaranteed to be whole if they arrive. One packet per one read call.
Examples: World Wide Web (Apache TCP port 80), e-mail (SMTP TCP port 25 Postfix MTA), File Transfer Protocol (FTP port 21) and Secure Shell (OpenSSH port 22) etc.	*Examples*: Domain Name System (DNS UDP port 53), streaming media applications such as IPTV or movies, Voice over IP (VoIP), Trivial File Transfer Protocol (TFTP) and online multiplayer games etc

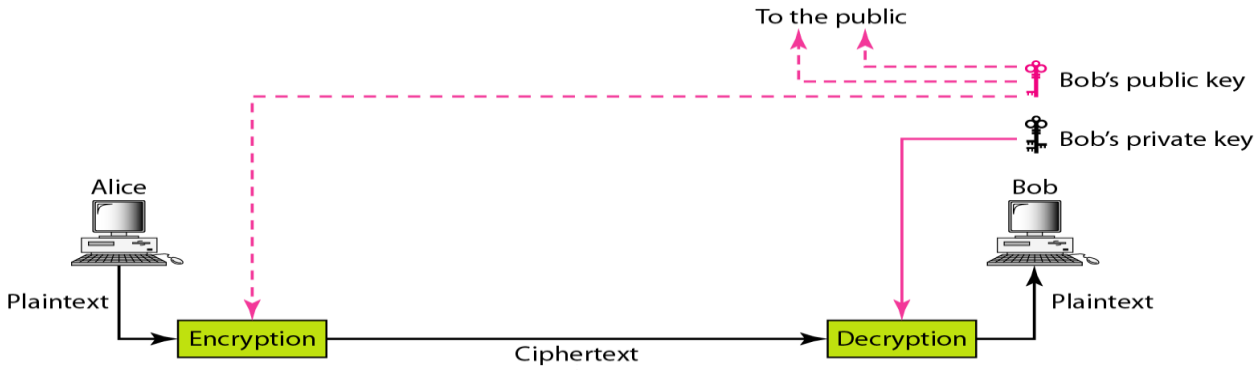
b. Define cryptography with the help of block diagram of Symmetric and Asymmetric key cryptography.

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. The term is most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear text) into cipher text (a process called encryption), then back again (known as decryption).

Symmetric-key cryptography: In symmetric-key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared.



Asymmetric-key cryptography: In Asymmetric-key cryptography, the public key is used by the sender (for encryption) and the private key is used by receiver (for decryption).



c. Write short notes on:

i. Digital audio

Digital audio is technology that can be used to record, store, generate, manipulate, and reproduce sound using audio signals encoded in digital form. Following significant advances in digital audio technology during the 1970s, it rapidly replacedanalog audio technology in most areas of sound production, sound engineering and telecommunications. A microphone converts sound to an analog electrical signal, then an analog-to-digital converter (ADC)—typically using pulse-code modulation—converts the analog signal into a digital signal. A digital-to-analog converter performs the reverse process, converting a digital signal back into an analog signal, which analog circuits amplify and send to a loudspeaker. Digital audio systems may include compression, storage, processing and transmission components. Conversion to a digital format allows convenient manipulation, storage, transmission and retrieval of an audio signal.

Digital audio is useful in the recording, manipulation, mass-production, and distribution of sound. Modern online music distribution depends on digital recording and data compression. The availability of music as data files, rather than as physical objects, has significantly reduced the costs of distribution. An analog audio system captures sounds, and converts their physical waveforms into electrical representations of those waveforms by use of a transducer, such as amicrophone. The sounds are then stored, as on tape, or transmitted. The process is reversed for playback: the audio signal is amplified and then converted back into physical waveforms via a loudspeaker. Analog audio retains its fundamental wave-like characteristics throughout its storage, transformation, duplication, and amplification. Analog audio signals are susceptible to noise and distortion, due to the innate characteristics of electronic circuits and associated devices. Disturbances in a digital system do not result in error unless the disturbance is so large as to result in a symbol being misinterpreted as another symbol or disturb the sequence of symbols. It is therefore generally possible to have an entirely error-free digital audio system in which no noise or distortion is introduced between conversion to digital format, and conversion back to analog. A digital audio signal may be encoded for correction of any errors that might occur in the storage or transmission of the signal, but this is not strictly part of the digital audio process. This technique, known as "channel coding", is essential for broadcast or recorded digital systems to maintain bit accuracy. The discrete time and level of the binary signal allow a decoder

to recreate the analog signal upon replay. Eight to Fourteen Bit Modulation is a channel code used in the audio Compact Disc (CD).

ii. Audio compression

Audio data compression, as distinguished from dynamic range compression, has the potential to reduce the transmission bandwidth and storage requirements of audio data.Audio compression algorithms are implemented in software as audio codecs. Lossy audio compression algorithms provide higher compression at the cost of fidelity and are used in numerous audio applications. These algorithms almost all rely on psychoacoustics to eliminate less audible or meaningful sounds, thereby reducing the space required to store or transmit them.

In both lossy and lossless compression, information redundancy is reduced, using methods such as coding, pattern recognition, and linear prediction to reduce the amount of information used to represent the uncompressed data.

The acceptable trade-off between loss of audio quality and transmission or storage size depends upon the application. For example, one 640MB compact disc (CD) holds approximately one hour of uncompressed high fidelity music, less than 2 hours of music compressed losslessly, or 7 hours of music compressed in the MP3 format at a mediumbit rate. A digital sound recorder can typically store around 200 hours of clearly intelligible speech in 640MB.

Lossless audio compression produces a representation of digital data that decompress to an exact digital duplicate of the original audio stream, unlike playback from lossy compression techniques such as Vorbis and MP3. Compression ratios are around 50–60% of original size,[19] which is similar to those for generic lossless data compression. Lossless compression is unable to attain high compression ratios due to the complexity of waveforms and the rapid changes in sound forms. Codecs like FLAC, Shorten and TTAuse linear prediction to estimate the spectrum of the signal. Many of these algorithms use convolution with the filter [-1 1] to slightly whiten or flatten the spectrum, thereby allowing traditional lossless compression to work more efficiently. The process is reversed upon decompression.

When audio files are to be processed, either by further compression or for editing, it is desirable to work from an unchanged original (uncompressed or losslessly compressed). Processing of a lossily compressed file for some purpose usually produces a final result inferior to the creation of the same compressed file from an uncompressed original. In addition to sound editing or mixing, lossless audio compression is often used for archival storage, or as master copies.

iii. Streaming audio

Streaming media is multimedia that is constantly received by and presented to an end-user while being delivered by a provider. The verb "to stream" refers to the process of delivering media in this manner; the term refers to the delivery method of the medium rather than the medium itself. A client media player can begin playing the data (such as a movie) before the entire file has been transmitted. Distinguishing delivery method from the media distributed

applies specifically to telecommunications networks, as most of the delivery systems are either inherently streaming (e.g., radio, television) or inherently non streaming (e.g., books, video cassettes, audio CDs). For example, in the 1930s, elevator music was among the earliest popularly available streaming media; nowadays Internet television is a common form of streamed media. The term "streaming media" can apply to media other than video and audio such as live closed captioning, ticker tape, and real-time text, which are all considered "streaming text". The term "streaming" was first used in the early 1990s as a better description for video on demand on IP networks; at the time such video was usually referred to as "store and forward video", which was misleading nomenclature.

Live streaming, which refers to content delivered live over the Internet, requires a form of source media (e.g. a video camera, an audio interface, screen capture software), an encoder to digitize the content, a media publisher, and a content delivery network to distribute and deliver the content.

5.

a. Explain in brief :

i. POP3

Post Office Protocol 3 (POP3) servers hold incoming e-mail messages until you check your e-mail, at which point they're transferred to your computer. POP3 is the most common account type for personal e-mail. Messages are typically deleted from the server when you check your e-mail.

ii. IMAP

Internet Message Access Protocol (IMAP) servers let you work with e-mail messages without downloading them to your computer first. You can preview, delete, and organize messages directly on the e-mail server, and copies are stored on the server until you choose to delete them. IMAP is commonly used for business e-mail accounts.

iii. SMTP

Simple Mail Transfer Protocol (SMTP) servers handle the sending of your e-mail messages to the Internet. The SMTP server handles outgoing e-mail, and is used in conjunction with a POP3 or IMAP incoming e-mail server.

b. Write short notes on :

i. FTP

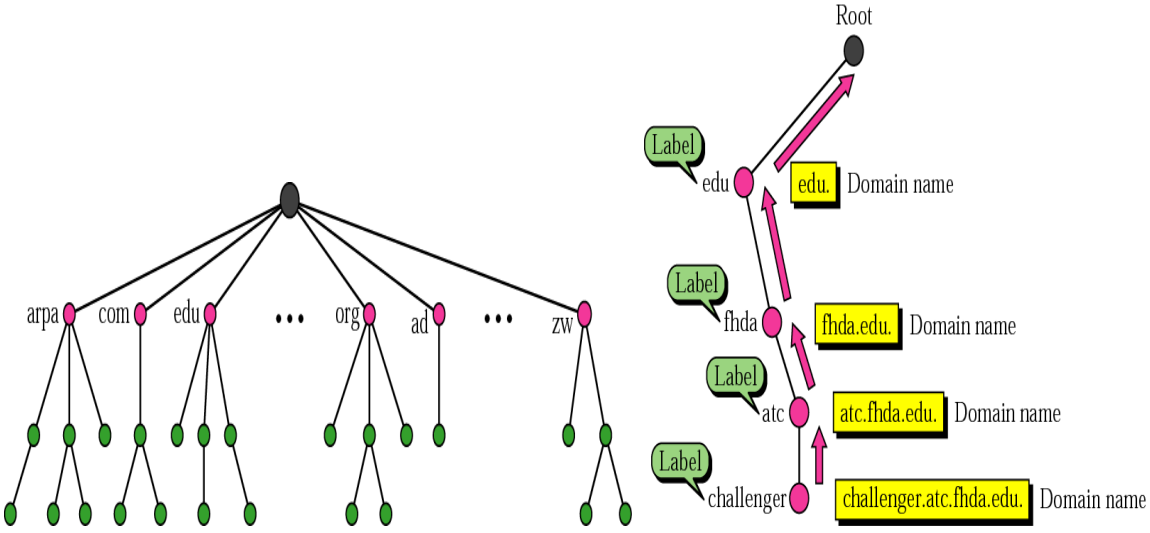
File Transfer Protocol (FTP) is the standard mechanism provided by *TCP/IP* for copying a file from one host to another. Although transferring files from one system to another seems simple and straightforward, some problems must be dealt with first. For example, two systems may use different file name conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. All these problems have been solved by FTP in a very simple and elegant approach. FTP differs from other client/server applications in that it establishes two connections between the hosts. One connection is used for data transfer, the other for control information (commands and responses). Separation of commands and data transfer makes FTP more efficient. The control connection uses very simple rules of communication. Wc need to transfer only a line of command or a line of response at a time. The data connection, on the other hand, needs more complex rules due to the variety of data types

transferred. However, the difference in complexity is at the FTP level, not TCP.For TCP, both connections are treated the same.

ii. DNS

The **Domain Name System** (**DNS**) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates domain names, which can be easily memorized by humans, to the numerical IP addresses needed for the purpose of computer services and devices worldwide. The Domain Name System is an essential component of the functionality of most Internet services because it is the Internet's primary directory service.

The Domain Name System distributes the responsibility of assigning domain names and mapping those names to IP addresses by designating authoritative name servers for each domain. Authoritative name servers are assigned to be responsible for their supported domains, and may delegate authority over sub-domains to other name servers. This mechanism provides distributed and fault tolerant service and was designed to avoid the need for a single central database.



iii. MIME

Electronic mail has a simple structure. Its simplicity, however, comes at a price. It can send messages only in NVT 7-bit ASCII format. In other words, it has some limitations. For example, it cannot be used for languages that are not supported by 7-bit ASCII characters (such as French, German, Hebrew, Russian, Chinese, and Japanese). Also, it cannot be used to send binary files or video or audio data. Multipurpose Internet Mail Extensions (MIME) is a supplementary protocol that allows non-ASCII data to be sent through e-mail. MIME transforms non-ASCII data at the sender site to NVT ASCII data and delivers them to the client MTA to be sent through the Internet. The message at the receiving side is transformed back to the original data. We can think of MIME as a set of software functions that transforms non-ASCII data (stream of bits) to ASCII data and vice versa.

MIME defines five headers that can be added to the original e-mail header section to define the transformation parameters:

1. MIME-Version
2. Content-Type
3. Content-Transfer-Encoding
4. Content-Id
5. Content-Description

iv. TFTP

Trivial File Transfer Protocol (**TFTP**) is a simple, lock-step, file transfer protocol which allows a client to get from or put a file onto a remote host. One of its primary uses is in the early stages of nodes booting from a Local Area Network. TFTP has been used for this application because it is very simple to implement.

Why TFTP?

In the old days, TFTP was typically used for downloading boot code to diskless workstations. TFTP was simple enough to fit into EEPROMs of diskless workstations (only a few KBytes of code). Today, TFTP is most often used for downloading new code to Internet appliances (Internet Access Devices, routers, switches, VOIP gateways etc.).

TFTP versus FTP

FTP and TFTP both are protocols for transferring files between a client and a server. However, TFTP and FTP are 2 totally different protocols and do not have anything in common.

Value	FTP	TFTP
Authentication	Authentication based on login with username and password.	TFTP does not provide authentication (login).
Connection	FTP uses TCP (reliable transmission). Errors are handled by the underlying TCP layer.	TFTP uses UDP and thus no connections. Errors in the transmission (lost packets, checksum errors) must be handled by the TFTP server.
Protocol algorithm	Transmission of data and control information is handled by the underlying TCP layer. TCP guarantees maximum throughput (flow control, congestion control) and error control.	TFTP uses a simple lock-step protocol (each data packet needs to be acknowledged). Thus the throughput is limited.
Footprint	FTP is more complex than TFTP, thus requires a larger memory footprint. Often FTP is not suited for small device bootloaders which must fit into constrained EEPROM storage.	TFTP is very simple. Because it uses the equally simple UDP transport protocol, TFTP clients or servers have a very small footprint and are thus suited for use in bootloaders.

Control and data channel	FTP separates user data and control information by using 2 separate TCP connections.	TFTP uses only "1 channel", i.e. control packets (commands) flow in one direction while data packets carrying user data flow in the reverse direction over the same UDP sockets.

c. Explain about e-mail architecture and services.

Electronic mail (e mail) is one of the use of the World Wide Web, according to most businesses, improves productivity. Traditional methods of sending mail within an office environment are inefficient, as it normally requires an individual requesting a secretary to type the letter. This must then be proof-read and sent through the internal mail system, which is relatively slow and can be open to security breaches.

A faster method, and more secure method of sending information is to use electronic mail where by a computer user can exchange messages with other computer users (or groups of users) via a communications network. Electronic mail is one of the most popular uses of the Internet. For example, a memo with 100 words will be sent in a fraction of a second. Other types of data can also be sent with mail message such as images, sound, and so on.

The main standards that relate to the protocols of email transmission and reception are:

Simple Mail Transfer Protocol (SMTP) - which is used with the TCP/IP protocol suite? It has traditionally been limited to the text based electronic messages.

Multipurpose Internet Mail Extension (MIME) - Which allows the transmission and reception of mail that contains various types of data, such as speech, images, and motion video? It is a newer standard than STMP and uses much of its basic protocol.

S/MIME (Secure MIME). RSA Data security created S/MIME which supports encrypted e-mail transfer and digitally signed electronic mail.

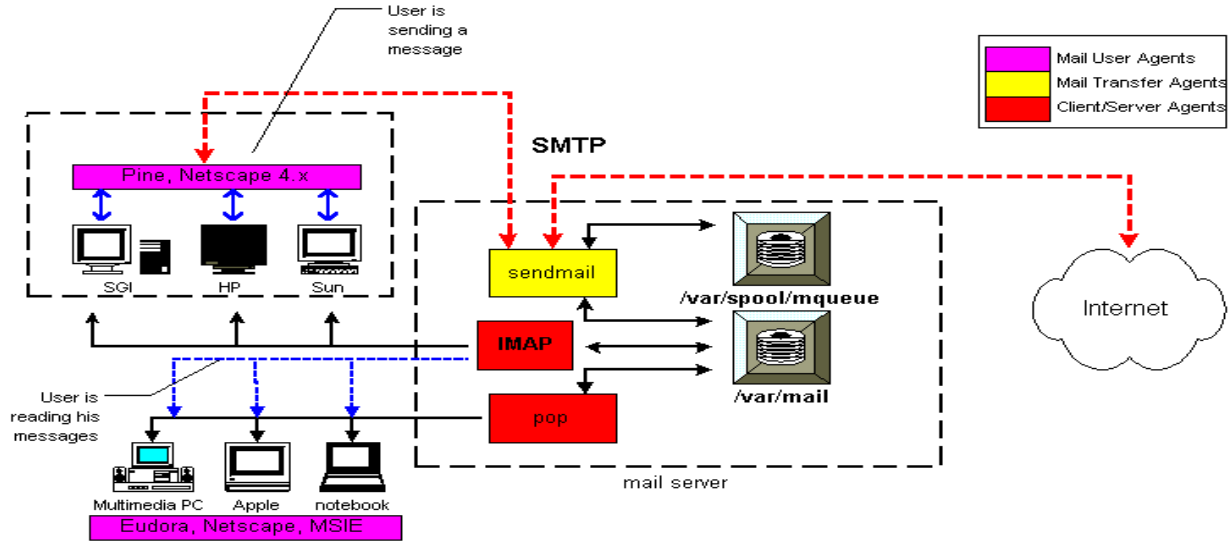
A typical email-architecture contains four elements:

1. **P**ost offices- where outgoing messages are temporally buffered (stored) before transmission and where incoming messages are stored. The post office runs the server software capable of routing messages (a message transfer agent) and maintaining the post office database.
2. **M**essage transfer agents- for forwarding messages between post offices and to the destination clients. The software can either reside on the local post office or on a physically separate server.
3. **G**ateways-which provide parts of the message transfer agent functionally. They translate between different e-mail systems, different e-mail addressing schemes and messaging protocols.
4. **E**-mail clients- normally the computer which connects to the post office. It contains three parts:

E-mail Application Program Interface (API), such as MAPI, VIM, MHS and CMC.

. Messaging protocol. The main messaging protocols are SMTP or X.400.STMP is defined in RFC 822 and RFC 821, Where as x.400 is an OSI-defined e-mail message delivery standard.

. Network transport protocol, such as Ethrnet, FDDI, and so on.



Client/server Email Architecture

Typically, e-mail systems support five basic functions. Let us take a look at them.

Composition refers to the process of creating messages and answers. Although any text editor can be used for the body of the message, the system itself can provide assistance with addressing and the numerous header fields attached to each message. For example, when answering a message, the e-mail system can extract the originator's address from the incoming e-mail and automatically insert it into the proper place in the reply.

Transfer refers to moving messages from the originator to the recipient. In large part, this requires establishing a connection to the destination or some intermediate machine, outputting the message, and releasing the connection. The e-mail system should do this automatically, without bothering the user.

Reporting has to do with telling the originator what happened to the message. Was it delivered? Was it rejected? Was it lost? Numerous applications exist in which confirmation of delivery is important and may even have legal significance ("Well, Your Honor, my e-mail system is not very reliable, so I guess the electronic subpoena just got lost somewhere").

Displaying incoming messages is needed so people can read their e-mail. Sometimes conversion is required or a special viewer must be invoked, for example, if the message is a PostScript file or digitized voice. Simple conversions and formatting are sometimes attempted as well.

Disposition is the final step and concerns what the recipient does with the message after receiving it. Possibilities include throwing it away before reading, throwing it away after reading, saving it, and so on. It should also be possible to retrieve and reread saved messages, forward them, or process them in other ways..