Q.1 a. Briefly explain the main differences between OSI and TCP/IP reference models.

Answer:
Three concepts are central to OSI model: services, interfaces and protocols. OSI model makes the clear distinction between these three concepts. The TCP/IP model did not originally clearly distinguish between services, interface and protocols. For example the only real services offered by the Internet layer are SEND IP packet and RECEIVE IP packet.

The OSI reference model was devised before the protocols were invented. This ordering means that model was not biased towards one particular set of protocols, which made it quite general. With TCP/IP reverse is true. The protocol came first, and the model was really just a description of the existing protocols. So problem was model did not fit for any other protocol stack.

Another difference is in the area of connectionless versus connection-oriented communication. The OSI model supports both connectionless and connection-oriented communication in the network layer, but only connection oriented in the transport layer. The TCP/IP model has only connection less in network layer but supports both the mode in transport layer.

b. Differentiate between trivial FTP and FTP application layer protocols.

Answer:
The Trivial File Transfer Protocol (TFTP) allows a local host to obtain files from a remote host but does not provide reliability or security. It uses the fundamental packet delivery services offered by UDP.

The File Transfer Protocol (FTP) is the standard mechanism provided by TCP / IP for copying a file from one host to another. It uses the services offer by TCP and so is reliable and secure. It establishes two connections (virtual circuits) between the hosts, one for data transfer and another for control information.

c. What is Pulse-Amplitude Modulation? What is their disadvantage?

Answer:
One analog-to-digital conversion method is called pulse amplitude modulation (PAM). This technique takes an analog signal, samples it, and generates a series of pulses based on the results of the sampling. The term sampling means measuring the amplitude of the signal at equal intervals.
In PAM, the original signal is sampled at equal intervals. PAM uses a technique called sample and hold. At a given moment, the signal level is read, and then held briefly. The sampled value occurs only instantaneously in the actual waveform, but is generalized over a still short but measurable period in the PAM result.
PAM is not useful to data communication because even though it translates the original waveform to a series of pulses, these pulses are still of any amplitude. To make them digital, we must modify them by using pulse code modulation.

d. Describe briefly Piggybacking.

Answer:
A technique called **piggybacking** is used to improve the efficiency of the bidirectional protocols. When a frame is carrying data from A to B, it can also carry control information about arrived (or lost) frames from B; when a frame is carrying data from B to A, it can also carry control information about the arrived (or lost) frames from A.
Each node now has two windows: one send window and one receive window. Both also need to use a timer. Both are involved in three types of events: request, arrival, and time-out. However, the arrival event here is complicated; when a frame arrives, the site needs to handle control information as well as the frame itself. Both of these concerns must be taken care of in one event, the arrival event. The request event uses only the send window at each site; the arrival event needs to use both windows.
An important point about piggybacking is that both sites must use the same algorithm. This algorithm is complicated because it needs to combine two arrival events into one.

e. Describe Routing Information Protocol (RIP).

Answer:
The **Routing Information Protocol (RIP)** is an intradomain routing protocol used inside an autonomous system. It is a very simple protocol based on distance vector routing. RIP implements distance vector routing directly with some considerations:
1. In an autonomous system, we are dealing with routers and networks (links). The routers have routing tables; networks do not.
2. The destination in a routing table is a network, which means the first column defines a network address.
3. The metric used by RIP is very simple; the distance is defined as the number of links (networks) to reach the destination. For this reason, the metric in RIP is called a hop count.
4. Infinity is defined as 16, which means that any route in an autonomous system using RIP cannot have more than 15 hops.
5. The next-node column defines the address of the router to which the packet is to be sent to reach its destination.

f. List the services provided by Point-to-Point protocol.

Answer:
Point-to-Point Protocol *provides several services:*
1. PPP defines the format of the frame to be exchanged between devices.
2. PPP defines how two devices can negotiate the establishment of the link and the exchange of data.
3. PPP defines how network layer data are encapsulated in the data link frame.
4. PPP defines how two devices can authenticate each other.
5. PPP provides multiple network layer services supporting a variety of network layer protocols.
6. PPP provides connections over multiple links.
7. PPP provides network address configuration. This is particularly useful when a home user needs a temporary network address to connect to the Internet.

g. Why is packet switching important? Give at least two reasons.

Answer:

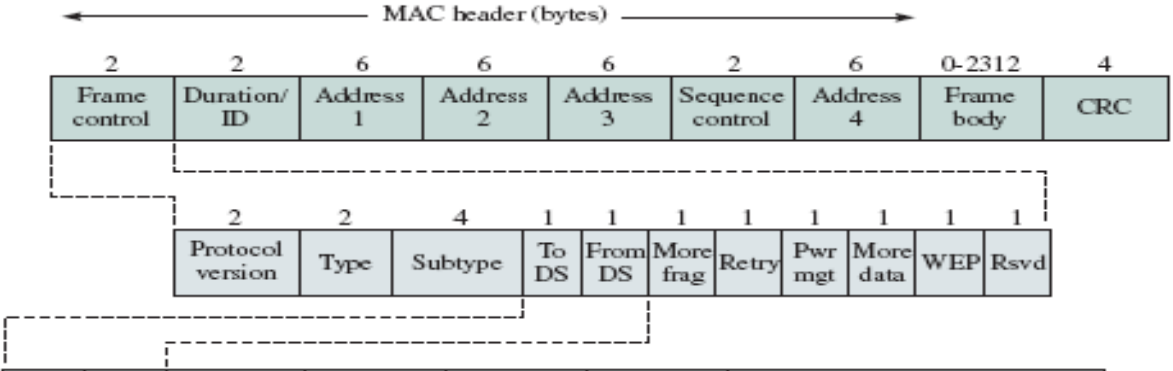
Packet switching is important because of the following two reasons:

- A sender and the receiver need to coordinate transmission to ensure that data arrives correctly. Dividing the data into small blocks helps a sender and receiver determines which block arrive intact and which do not.
- Second, because communication circuits and the associated modem hardware are expansive, multiple computers often share underlying connections and hardware. To ensure that all computers receive fair, prompt access to a shared communication facility, a network system allows one computer to deny access to others. Using small packets helps ensure fairness.

Q.2 a. With the help of a figure, explain the frame structure of IEEE 802.11

Answer:

IEEE 802.11 supports three types of frames: management frames, control frames and data frames. The management frames are used for station association and disassociation with the access point (AP), timing and synchronization, and authentication and deauthentication. Control frames are used for handshaking and for positive acknowledges during the data exchange. Data frames are used for transmission of data. The MAC header provides information on frame control duration, addressing, and sequence control. Following figure shows the format of the MAC frame consists of a MAC header, a frame body and a CRC checksum.



To DS	From DS	Address 1	Address 2	Address 3	Address 4	Meaning
0	0	Destination address	Source address	BSS ID	N/A	Data frame from station to station within a BSS
0	1	Destination address	BSS ID	Source address	N/A	Data frame exiting the DS
1	0	BSS ID	Source address	Destination address	N/A	Data frame destined for the DS
1	1	Receiver address	Transmitter address	Destination address	Source address	WDS frame being distributed from AP to AP

DS = distribution system AP = access point

The frame control field in the MAC header is 16 bits long, and it specifies the following items:

- The 802.11 protocol version.
- The type of frame, that is, management (00), control (01), or data (10).
- The subtype within a frame type, for example, type = "management", subtype = "association request" or type = "control" , subtype = "ACK".
- The To DS field is set to 1 in Data type frames destined for the DS, including Data type frames from a station associated with the AP that have broadcast or multicast addresses.
- The From DS field is set to 1 in Data type frames exiting the distribution system.
- The More fragments field is set to 1 in frames that have another fragment of the current MSDU to follow.
- The Retry field is set to 1 in Data or Management type frames that are retransmissions of an earlier frame; this helps the receiver deal with duplicate frames.
- The Power Management bit is set to indicate the power management mode of a station.
- The More Data field is set to 1 to indicate to a station power save mode that more MSDUs are buffered for it at the AP.
- The Wired Equivalent Privacy (WEP) field is set to 1 if the frame body field contains information that has been processed by the cryptographic algorithm.

The Duration/ID filed in the MAC header is 16 bits long and is used in two ways. It usually contains a duration value (net allocation vector) that is used in the MAC protocol. The only exception is in Control type frames of the subtype PS-Poll, where this field carries the ID of the station that transmitted the frame.

The use of the four Address fields is specified by the To DS and From DS fields in the Frame Control field as shown in figure. Addresses are 48-bit long IEEE 802 MAC addresses and can be individual or group (multicast/broadcast). The Address1 field contains the destination address. The BSS identifier (BSS ID) is a 48-bit field of the same format as IEEE 802 MAC addresses, uniquely identifies a BSS, and is given by the MAC address of the station in the AP of the BSS. The destination address is an IEEE MAC individual or group address that specifies the MAC entity that is the final recipient of the MSDU that is contained in the Frame Body field. The source address is a MAC individual address that identifies the MAC entity from which the MSDU originated. The receiver address is a MAC address that identifies the intended immediate recipient station for the MAC PDU (MPDU) in the Frame Body field. The transmitter address is a MAC individual address that identifies the station that transmitted the MPDU contained in the frame body field.

The Sequence Control field is 16 bits long, and it provides 4 bits to indicate the number of the each fragment of an MSDU and 12 bits of the sequence numbering for a sequence number space of 4096. The Frame Body field contains information of the type and subtype specified in the Frame Control field. For Data type frames, the Frame Body field contains an MSDU or a fragment of an MSDU. Finally, the CRC field contains the 32-bit cyclic redundancy check calculated over the MAC header and Frame Body field.

b. Differentiate between FDM and TDM multiplexing techniques.

Answer:
FDM and TDM multiplexing technique.
Frequency-division multiplexing (FDM) is an analog technique that can be applied when the bandwidth of a link (in hertz) is greater than the combined bandwidths of the signals to be transmitted. In FDM, signals generated by each sending device modulate different carrier frequencies. These modulated signals are then combined into a single composite signal that can be transported by the link. Carrier frequencies are separated by sufficient bandwidth to accommodate the modulated signal. These bandwidth ranges are the channels through which the various signals travel. Channels must be separated by strips of unused bandwidth to prevent signals from overlapping. Also, carrier frequencies must not interfere with the original data frequencies. Failure to adhere to either condition can result in the unsuccessful recovery of the original signals.

Time-division multiplexing (TDM) is a digital process that allows several connections to share the high bandwidth of a link. Instead of sharing a portion of the bandwidth as in FDM, time is shared. Each connection occupies a portion of time in the link. In TDM, the data rate of the link that carries data from n connections must be n times the data rate of a connection to guarantee the flow of data. Therefore, the duration of a unit in a connection is n times the duration of a time slot in a frame.

c. What do you mean by a stateless protocol? Comment on the following statement: "HTTP is a stateless protocol".

Answer: Refer Page No. 82 of text book.

Q.3 a. Distinguish between Multicasting and Multiple unicasting. Also, give reason why we have a separate mechanism for multicasting, when it can be emulated with unicasting?

Answer:
Multicasting starts with one single packet from the source that is duplicated by the routers. The destination address in each packet is the same for all duplicates. Only one single copy of the packet travels between any two routers.

In **multiple unicasting**, several packets start from the source. If there are five destinations, for example, the source sends five packets, each with a different unicast destination address. There may be multiple copies travelling between two routers. For when a person sends an e-mail message to a group of people, this is multiple unicasting. The e-mail software creates replicas of the message, each with a different destination address and sends them one by one. This is not multicasting, it is multiple unicasting.

We have a separate mechanism for multicasting, when it can be emulated with unicasting because of following two reasons:

- Multicasting is more efficient than multiple unicasting. Multicasting requires less bandwidth than does multiple unicasting. In multiple unicasting, some of the link must handle several copies.
- In multiple unicasting, the packets are created by the source with a relative delay between packets. If there are 1000 destinations, the delay between the first and the last packet may be unacceptable. In multicasting, there is no delay because one packet is created by the source.

b. A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces
(i) 1000 frames per second
(ii) 500 frames per second
(iii) 250 frames per second
In which case percentage wise maximum throughput would be achieved?

Answer:
The frame transmission time is 200/200 kbps or 1 mbps.

(i) If the system creates 1000 frames per second, this is 1 frame per millisecond. The load is 1.
In this case $S = G \times e^{-2G}$ or S = 0.135 (13.5 percent). This means that the throughput is 1000 x 0.135 = 135 frames. Only 135 frames out of 1000 will probably survive.

(ii) If the system creates 500 frames per second, this is 1/2 frame per millisecond. The load is 1/2.
In this case $S = G \times e^{-2G}$ or S = 0.184 (18.4 percent). This means that the throughput is 500 x 0.184 = 92 and that only 92 frames out of 500 will probably survive.
This is the maximum throughput case, percentagewise.

(iii) If the system creates 250 frames per second, this is 1/4 frame per millisecond. The load is 1/4.
In this case $S = G \times e^{-2G}$ or S = 0.152 (15.2 percent). This means that the throughput is 250 x 0.152 = 38 frames. Only 38 frames out of 250 will probably survive.

Q.4 a. What are the various goals of a routing algorithm?

Answer:
A routing algorithm should seek one or more of more of the following goals:

- *Rapid and accurate delivery of packets*: A routing algorithm must operate correctly, i.e. it must be able to find a path to the correct destination if it exists. In addition, the algorithm should not take an unreasonably long time to find the path to the destination.
- *Adaptability to changes in network topology resulting from node or link failures*: In an operational network equipment and transmission lines are subject to failures. A routing algorithm must be able to adapt and reconfigure the path automatically when equipment fails.

- *Adaptability to varying source-destination traffic loads*: Traffic loads are quantities that are changing dynamically. In a period of 24 hours, traffic loads may go through cycles of heavy and light periods. An adaptive routing algorithm would be able to adjust the paths based on the current traffic loads.
- *Ability to route packets away from temporarily congested links*: A routing algorithm should avoid heavily congested links. Often it is desirable to balance the load on each link / path.
- *Ability to determine the connectivity of the network*: To find optimal paths, the routing system needs to know the connectivity or reachability information.
- *Ability to avoid routing loops*: Inconsistent information in distributed computation may lead to routing tables that create routing loops. The routing system should avoid persistent routing loops even in presence of distributed routing systems.
- *Low overhead*: A routing system typically obtains the connectivity information by exchanging control messages with other routing systems. These messages represent an overload on bandwidth usage that should be minimized.

b. Discuss the different fields related to fragmentation and reassembly of an IPv4 datagram.

Answer:

The fields that are related to fragmentation and reassembly of an IPv4 datagram are the identification, flags and fragmentation offset fields.

- **Identification :** This 16-bit field identifies a datagram originating from the source host. The combination of the identification and source IPv4 address must uniquely define a datagram as it leaves the source host. To guarantee uniqueness, the IPv4 protocol uses a counter to label the datagrams. This counter is initialized to a positive number. When the IPv4 protocol sends a datagram, it copies the current value of the counter to the identification field and increments the counter by 1. As long as the counter is kept in main memory, uniqueness is guaranteed. When a datagram is fragmented, the value in the identification field is copied to all fragments.
- **Flags :** This is a 3-bit field. The first bit is reserved. The second bit is called the do not fragment bit. If its value is 1, the machine must not fragment the datagram. If it cannot pass the datagram through any available physical network, it discards the datagram and sends an ICMP error message to the source host. If its value is 0, the datagram can be fragmented if necessary. The third bit is called the more fragment bit. If its value is 1, it means the datagram is not the last fragment; there are more fragments after this one. If its value is 0, its means this is the last or only fragment.
- **Fragmentation offset :** this 13-bit field shows the relative position of this fragment with respect to the whole datagram. It is the offset of the data in the original datagram measured in units of 8 bytes.

c. Suppose a router receives an IP packet containing 600 data bytes and has to forward the packet to a network with maximum transmission unit of 200 bytes. Assume that the IP header is 20 bytes long. Show the fragments that the router creates and specify the relevant values in each fragment header (i.e., total length, fragment offset and more bit).

Answer:
Given:

IP packet = 600 data bytes
MTU = 200 bytes
IP header = 20 header bytes
Maximum possible data length per fragment = MTU – IP header = 200 – 20 = 180 bytes.
The data length of each fragment must be a multiple of eight bytes; therefore the maximum number of data bytes that can be carried per fragment is 22*8=176.
The data packet must be divided into 4 frames, as shown by the following calculations:

176 + 176 + 176 + 72 = 600

The sequence of frames and packet headers is shown below:

	Total Length	Id	Mf	Fragment offset
Original Packet	620	x	0	0
Fragment 1	196	x	1	0
Fragment 1	196	x	1	22
Fragment 1	196	x	1	44
Fragment 1	196	x	0	66

Q.5 a. Differentiate between Connectionless and Connection-Oriented services.

Answer:
The network service can be connectionless or connection-oriented. A connectionless service is simple, with only two basic interactions between the transport layer (user of the service) and the network layer (provider of the service): a request to the network layer that it sends a packet and an indication from the network layer that a packet has arrived. The user can request transmission of a packet at any time, and does not need to inform the network that the user intends to transmit information ahead of time. A connectionless service puts total responsibility for error control, sequencing, and flow control on the end-system transport layer.

The network service can be connection-oriented. In this case, the transport layer cannot request transmission of information until a connection between the end systems has been set up. The essential points here are that the network layer must be informed about the new flow that is about to be sent to the network and that the network layer maintains state information about the floe it is handling. During connection setup, parameters related to usage and quality of service may be

negotiated and network resources may be allocated to ensure that the user flow can be handled as required. A connection-release procedure may also be required to terminate the connection. It is clear that providing connection-oriented service entails greater complexity than connectionless service in the network layer.

b. Explain the following CSMA schemes:
(i) Non-persistent
(ii) 1-persistent
(iii) p-persistent

Answer:
Non-Persistent CSMA attempts to reduce the incidence of collisions. Station with a frame to transmit sense the channel. If the channel is busy, the stations immediately run the backoff algorithm and reschedule a future resensing time. If the channel is idle, the stations transmit. By immediately rescheduling a resensing time and persisting, the incidence of collision is reduced relative to 1-Persistent CSMA. This immediate rescheduling also results in longer delays than are found in 1-Persistent CSMA.

In **1-Persistent CSMA,** the stations with a frame to transmit sense the channel. If the channel is busy, they sense the channel continuously, waiting until the channel become idle. As soon as the channel is sensed idle, they transmit the frames. Consequently if more than one channel is waiting, a collision will occur. In addition, stations that have a frame arrive within *time* Δt of the end of the preceding transmission will also transmit and possibly be involved in collision. Stations that are involved in a collision perform the backoff algorithm to schedule a future time for resensing the channel. In a sense, in 1-Persistent CSMA stations act in a 'greedy' fashion, attempting to access the medium as soon as possible. As a result, 1-Persistent CSMA has a relatively high collision rate.

The class of **p-Persistent CSMA** schemes combines elements of the above two schemes. Stations with a frame to transmit sense the channel, and if the channel is busy, they persist with sensing until the channel becomes idle. If the channel is idle, the following occurs: with probability p, the station transmits its frame; with probability (1 - p) the station decides to wait an additional propagation delay before again sensing the channel. This behavior is intended to spread out the transmission attempts by the stations that have been waiting for a transmission to be completed and hence to increase the likelihood that a waiting station successfully seizes the medium.

c. What are the different threats that can arise in a network?

Answer: Following are the several threats that can arise in a network setting:
1. Information transmitted over the network is not secure and can be observed and recorded by eavesdroppers. This information can be replayed in attempts to access the server.
2. Imposters can attempt to gain unauthorized access to a server, for example, a bank account or a database or personal records.
3. An attacker can also flood a server with request, overloading the server resources and resulting in a *denial of service* to legitimate clients.

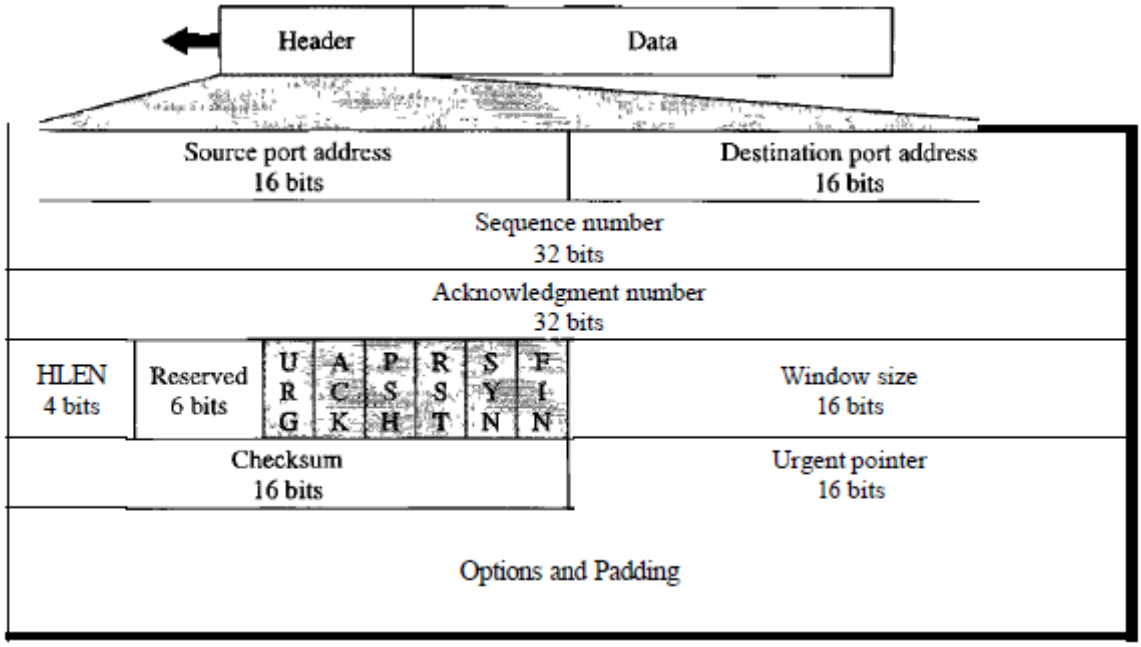
4. An imposter can impersonate a legitimate server and gain sensitive information from a client, foe example, a bank account and associated user password.
5. An imposter manages to place itself as the man in middle, convincing the server that it is the legitimate client that it is the legitimate server.

Q.6 a. Define TCP and discuss the different fields of TCP packet format with the help of a diagram.

Answer:

TCP (i.e. Transmission Control Protocol) is a process-to-process protocol. It is a connection-oriented, reliable transport protocol; it creates a virtual connection between two TCPs to send data. TCP uses flow and error control mechanisms at transport level. It adds connection-oriented and reliability features to the services of IP.

The format of TCP segment is shown in the figure below:



The segment consists of a 20- to 60-byte header, followed by data from the application program. The header is 20 bytes if there are no options and up to 60 bytes if it contains options. The meaning and purpose of the header fields are discussed below:

- **Source port address**. This is a 16-bit field that defines the port number of the application program in the host that is sending the segment. This serves the same purpose as the source port address in the UDP header.
- **Destination port address**. This is a 16-bit field that defines the port number of the application program in the host that is receiving the segment. This serves the same purpose as the destination port address in the UDP header.

- **Sequence number**. This 32-bit field defines the number assigned to the first byte of data contained in this segment. As we said before, TCP is a stream transport protocol. To ensure connectivity, each byte to be transmitted is numbered. The sequence number tells the destination which byte in this sequence comprises the first byte in the segment. During connection establishment, each party uses a random number generator to create an initial sequence number (ISN), which is usually different in each direction.
- **Acknowledgment number**. This 32-bit field defines the byte number that the receiver of the segment is expecting to receive from the other party. If the receiver of the segment has successfully received byte number *x* from the other party, it defines *x* + 1 as the acknowledgment number. Acknowledgment and data can be piggybacked together.
- **Header length**. This 4-bit field indicates the number of 4-byte words in the TCP header. The length of the header can be between 20 and 60 bytes. Therefore, the value of this field can be between 5 (5 x 4 =20) and 15 (15 x 4 =60).
- **Reserved**. This is a 6-bit field reserved for future use.
- **D Control**. This field defines 6 different control bits or flags. One or more of these bits can be set at a time. These bits enable flow control, connection establishment and termination, connection abortion, and the mode of data transfer in TCP. A brief description of each bit is shown in the table below.

Description of flags in control field	
Flag	**Description**
URG	The value of the urgent pointer field is valid
ACK	The value of the acknowledgment field is valid
PSH	Push the data
RST	Reset the connection
SYN	Synchronize sequence numbers during connection
FIN	Terminate the connection

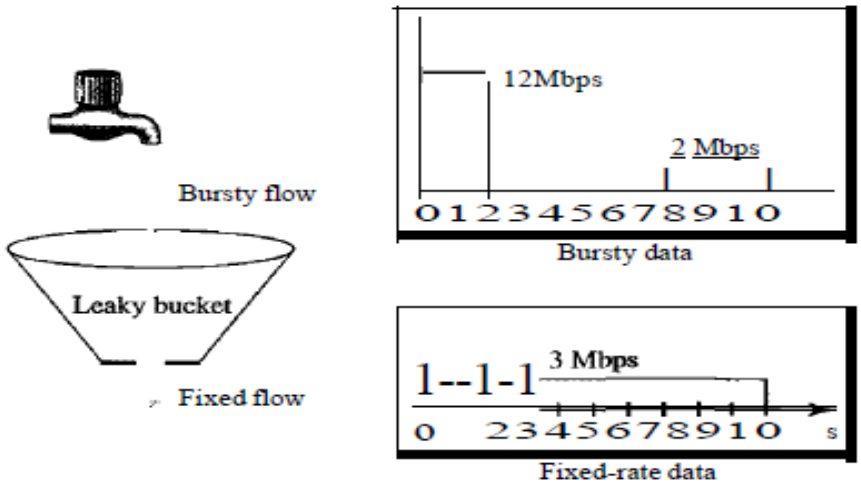
- **Window size**. This field defines the size of the window, in bytes, that the other party must maintain. Note that the length of this field is 16 bits, which means that the maximum size of the window is 65,535 bytes. This value is normally referred to as the receiving window (rwnd) and is determined by the receiver. The sender must obey the dictation of the receiver in this case.
- **Checksum**. This 16-bit field contains the checksum. The calculation of the checksum for TCP follows the same procedure as the one described for UDP. However, the inclusion of the checksum in the UDP datagram is optional, whereas the inclusion of the checksum for TCP is mandatory. The same pseudoheader, serving the same purpose, is added to the segment. For the TCP pseudoheader, the value for the protocol field is 6.
- **Urgent pointer**. This l6-bit field, which is valid only if the urgent flag is set, is used when the segment contains urgent data. It defines the number that must be added to the sequence number to obtain the number of the last urgent byte in the data section of the segment.
- **Options**. There can be up to 40 bytes of optional information in the TCP header.

b. What is traffic shaping? Briefly explain two techniques of traffic shaping.

Answer:
Traffic shaping is a mechanism to control the amount and the rate of the traffic sent to the network. **Two techniques can shape traffic: leaky bucket and token bucket.**

Leaky Bucket: ***A leaky bucket algorithm shapes bursty traffic into fixed-rate traffic by averaging the data rate. It may drop the packets if the bucket is full.***

If a bucket has a small hole at the bottom, the water leaks from the bucket at a constant rate as long as there is water in the bucket. The rate at which the water leaks does not depend on the rate at which the water is input to the bucket unless the bucket is empty. The input rate can vary, but the output rate remains constant. Similarly, in networking, a technique called leaky bucket can smooth out bursty traffic. Bursty chunks are stored in the bucket and sent out at an average rate. The following figure shows a leaky bucket and its effects.

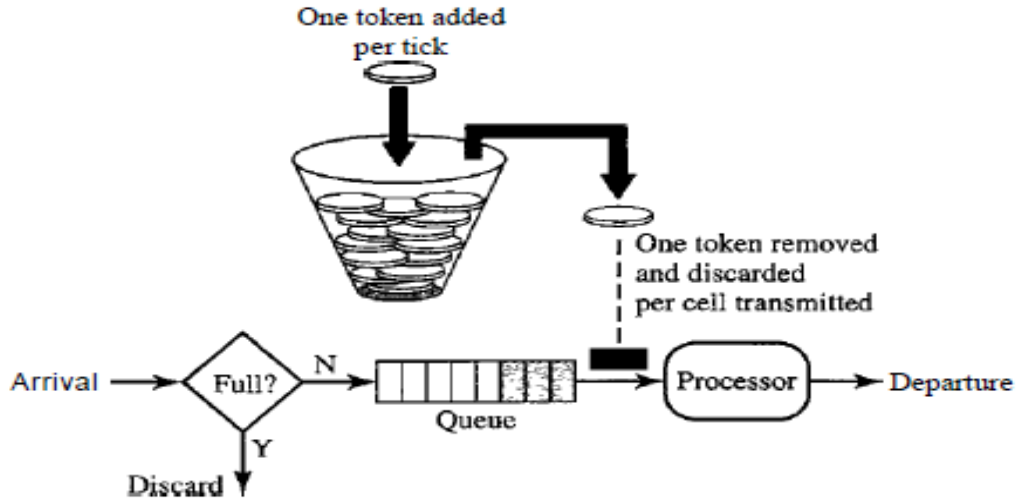


In the figure, we assume that the network has committed a bandwidth of 3 Mbps for a host. The use of the leaky bucket shapes the input traffic to make it conform to this commitment. In Figure the host sends a burst of data at a rate of 12 Mbps for 2 s, for a total of 24 Mbits of data. The host is silent for 5 s and then sends data at a rate of 2 Mbps for 3 s, for a total of 6 Mbits of data. In all, the host has sent 30 Mbits of data in l0s. The leaky bucket smooths the traffic by sending out data at a rate of 3 Mbps during the same 10 s. Without the leaky bucket, the beginning burst may have hurt the network by consuming more bandwidth than is set aside for this host. We can also see that the leaky bucket may prevent congestion.

Token Bucket: ***The token bucket allows bursty traffic at a regulated maximum rate.***

The leaky bucket is very restrictive. It does not credit an idle host. For example, if a host is not sending for a while, its bucket becomes empty. Now if the host has bursty data, the leaky bucket allows only an average rate. The time when the host was idle is not taken into account. On the other hand, the token bucket algorithm allows idle hosts to accumulate credit for the future in the form of tokens. For each tick of the clock, the system sends *n* tokens to the bucket. The system removes one token for every cell (or byte) of data sent. For example, if *n* is 100 and the host is

idle for 100 ticks, the bucket collects 10,000 tokens. Now the host can consume all these tokens in one tick with 10,000 cells, or the host takes 1000 ticks with 10 cells per tick. In other words, the host can send bursty data as long as the bucket is not empty. Following figure shows the idea. The token bucket can easily be implemented with a counter. The token is initialized to zero. Each time a token is added, the counter is incremented by 1. Each time a unit of data is sent, the counter is decremented by 1. When the counter is zero, the host cannot send data.



Q.7 a. Explain Simple Network Management Protocol in detail.

Answer:

The Simple Network Management Protocol (SNMP) is an application-layer protocol that facilitates the exchange of management information between network devices. It is part of the TCP/IP protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems and plan for network growth.

There are two versions of SNMP, v1 and v2. Both versions have a number of features in common, but SNMP v2 offers enhancements, such as additional protocol operations. SNMP version 1 is described in RFC 1157 and functions within the specifications of the Structure of Management Information (SMI). SNMP v1 operates over protocols such as the User Datagram Protocol (UDP), IP, OSI Connectionless Network Service (CLNS), Apple-Talk Datagram-Delivery Protocol (DDP), and Novell Internet Packet Exchange (IPX). SNMP v1 is widely used and is the *de facto* network management protocol in the Internet community.

SNMP is a simple request–response protocol. The network management system issues a request, and managed devices return responses. This behaviour is implemented using one of four protocol operations: Get, GetNext, Set and Trap. The Get operation is used by the network management system (NMS) to retrieve the value of one or more object instances from an agent. If the agent responding to the Get operation cannot provide values for all the object instances in a list, it provides no values. The GetNext operation is used by the NMS to retrieve the value of the next object instance in a table or list within an agent. The Set operation is used by the NMS to set the values of object instances within an agent. The Trap operation is used by agents to

asynchronously inform the NMS of a significant event. SNMP version 2 is an evolution of the SNMP v1. It was originally published as a set of proposed Internet Standards in 1993. SNMP v2 functions within the specifications of the Structure of Management Information (SMI) which defines the rules for describing management information, using Abstract Syntax Notation One (ASN.1). The Get, GetNext and Set operation used in SNMP v1 are exactly the same as those used in SNMP v2. However, SNMP v2 adds and enhances some protocol operations. SNMP v2 also defines two new protocol operations: GetBulk and Inform. The GetBulk operation is used by the NMS to efficiently retrieve large blocks of data, such as multiple rows in a table. GetBulk fills a response message with as much of the requested data as will fit. The Inform operation allows one NMS to send trap information to another NMS and receive a response.

SNMP lacks any authentication capabilities, which results in vulnerability to a variety of security threats. These include masquerading, modification of information, message sequence and timing modifications and disclosure.

b. What is RSA Public-key Cryptosystem? Explain RSA encryption algorithm with the help of an example.

Answer:
In 1976, Diffie and Hellman introduced the idea of the exponential key exchange. In 1977 Rivest, Schamir and Adleman invented the RSA algorithm for encryption and digital signatures which was the first public-key cryptosystem. Soon after the publication of the RSA algorithm, Merkle and Hellman devised a public-key cryptosystem for encryption based on the knapsack algorithm. The RSA cryptosystem resembles the D–H key exchange system in using exponentiation in modula arithmetic for its encryption and decryption, except that RSA operates its arithmetic over the composite numbers. Even though the cryptanalysis was researched for many years for RSA's security, it is still popular and reliable. The security of RSA depends on the problem of factoring large numbers. It is proved that 110-digit numbers are being factored with the power of current factoring technology. To keep RSA's level of security, more than 150-digit values for n will be required. The speed of RSA does not beats DES, because DES is about 100 times faster than RSA in software.

RSA Encryption Algorithm
Given the public key e and the modulus n, the private key d for decryption has to be found by factoring n. Choose two large prime numbers, p and q, and compute the modulus n which is the product of two primes:
$n = pq$

Choose the encryption key e such that e and $\varphi(n)$ are coprime, i.e. gcd $(e, \varphi(n)) = 1$, in which $\varphi(n) = (p-1)(q-1)$ is called Euler's totient function. Using euclidean algorithm, the private key d for decryption can be computed by taking the multiplicative inverse of e such that
$d \equiv e^{-1} \pmod{\varphi(n)}$

or $ed \equiv 1 \pmod{\varphi(n)}$

The decryption key d and the modulus n are also relatively prime. The numbers e and n are called the public keys, while the number d is called the private key.

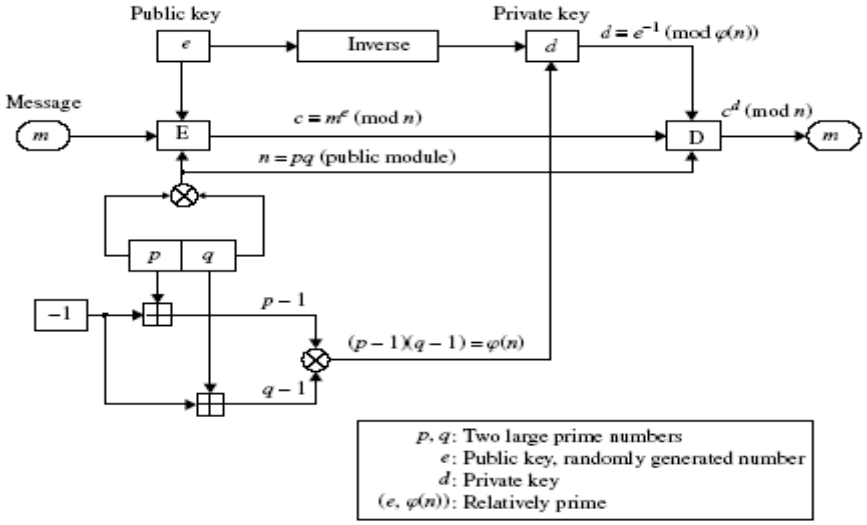
To encrypt a message m, the ciphertext c corresponding to the message block can be found using the following encryption formula:
$c \equiv m^e \pmod{n}$

To decrypt the ciphertext c, c is raised to the power d in order to recover the message m as follows:
$m \equiv c^d \pmod{n}$
It is proved that
$c^d \equiv (m^e)^d \equiv m^{ed} \equiv m \pmod{n}$

due to the fact that $ed \equiv 1 \pmod{\varphi(n)}$.
Because Euler's formula is $m^{\varphi(n)} \equiv 1 \pmod{n}$, the message m is relatively prime to n such that gcd $(m, n) = 1$. Since $m^{\lambda\varphi(n)} \equiv 1 \pmod{n}$ for some integer λ, it can be written $m^{\lambda\varphi(n)+1} \equiv m \pmod{n}$, because $m^{\lambda\varphi(n)+1} \equiv mm^{\lambda\varphi(n)} \equiv m \pmod{n}$. Thus, the message m can be restored.

Figure and Table below illustrate the RSA algorithm for encryption and decryption. Using Table, the following examples are demonstrated.

Example If $p = 17$ and $q = 31$ are chosen, then
$n = pq = 17 \times 31 = 527$
$\varphi(n) = (p - 1)(q - 1) = 16 \times 30 = 480$
If $e = 7$ is chosen, then compute:
$d \equiv e{-}1 \pmod{\varphi(n)} \equiv 7{-}1 \pmod{480} \equiv 343$
This decryption key d is calculated using the extended euclidean algorithm.
$ed \equiv 7 \times 343 \pmod{480} \equiv 2401 \pmod{480} \equiv 1$



RSA encryption algorithm

Public key e:

n (product of two primes p and q (secret integers))
e (encryption key, relatively prime to $\phi(n) = (p-1)(q-1)$)

Private key d:

d (decryption key, $d = e^{-1} \pmod{\phi(n)}$)
$ed \equiv 1 \pmod{\phi(n)}$

Encryption:

$c \equiv m^e \pmod{n}$, where m is a plaintext.

Decryption:

$m \equiv c^d \pmod{n}$, where c is a ciphertext.

Text Book

Leon Garcia and Indra Widjaja, Communication Networks: Fundamental Concepts and key Architecture, 2nd ed., Tata McGraw-Hill, 2004.