Solutions
2018-19
COMPUTER NETWORK

SECTION A

1. Attempt *all* questions in brief. 2 x 7 = 14

a. What are header and trailers and how do they get added and removed?

The control data added to the beginning of a data is called headers. The control data added to the end of a data is called trailers. At the sending machine, when the message passes through the layers each layer adds the headers or trailers. At the receiving machine, each layer removes the data meant for it and passes the rest to the next layer.

b. A large FDDI ring has 100 stations & a token rotation time of 40msec. The token holding time is 10msec. What is the maximum achievable efficiency of the ring?

– Assumption: Every station has unlimited data to send
– Assumption: Data is send during the whole token holding time
– One token circulation takes 100 *10 ms + 40ms = 1040 ms
Efficiency = time used for data transmission / total time
Efficiency = 1000 ms / 1040 ms
Efficiency =0.96

c. What is the difference between network layer delivery and the transport layer delivery?

The transport layer is responsible for process-to-process delivery of the entire message, whereas the network layer oversees host-to-host delivery of individual packets.

d. If a class B network on the Internet has a subnet mask of 255.255.248.0, what is the maximum number of hosts per subnet?

2^{11} = 2046

e. What is count-to-infinity problem?

1. One of the important issue in Distance Vector Routing is County of Infinity Problem.
2. Counting to infinity is just another name for a routing loop.
3. In distance vector routing, routing loops usually occur when an interface goes down.
4. It can also occur when two routers send updates to each other at the same time.

f. What is the difference between a user agent (UA) and a mail transfer agent (MTA)?

The UA prepares the message, creates the envelope, and puts the message in the envelope. The MTA transfers the mail across the Internet.

g. What is time-to-live or packet lifetime

Time to live (TTL) is a mechanism used to limit the lifespan of data on a network. Data is discarded if the prescribed TTL elapses. The idea behind having a TTL is to prevent any data packet from circulating indefinitely.

SECTION B

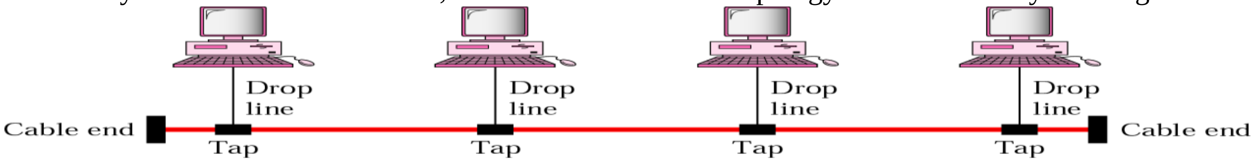
2. Attempt any *three* of the following: 7 x 3 = 21

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

Network topology is the interconnected pattern of network elements. A network topology may be physical, mapping hardware configuration, or logical, mapping the path that the data must take in order to travel around the network.

Bus Topology :

Commonly referred to as a linear bus, all the devices on a bus topology are connected by one single cable.



Advantages:

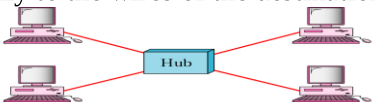
- Easy to use & inexpensive simple network
- Easy to extend thus allowing long distance traveling of signal
- Requires less cable length than a star topology

Disadvantages:

- Becomes slow by heavy network traffic with a lot of computer
- Difficult to troubleshoot & difficult to identify the problem if the entire network shut down
- Terminator is required at both ends of the backbone cable
- Not meant to be used as a stand alone solution in a large buildin

2. Star Topology

The star topology is the most commonly used architecture in Ethernet LANs. When installed, the star topology resembles spokes in a bicycle wheel. Larger networks use the extended star topology. When used with network devices that filter frames or packets, like bridges, switches, and routers, this topology significantly reduces the traffic on the wires by sending packets only to the wires of the destination host.



Advantages:

- Easy to modify and add new computer to a star network without disturbing the rest of the network
- Ease of diagnosis of network faults through the central computer
- Single computer failure do not necessarily bring down the whole star network
- Use of several cable types in the same network

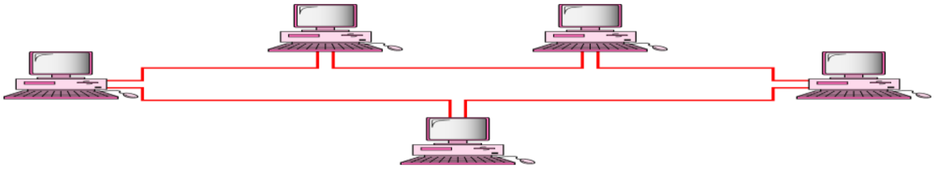
Disadvantages:

- Requires more cable length than a linear topology.
- If the hub or concentrator fails, nodes attached are disabled.
- More expensive than linear bus topologies because of the cost of the concentrators

3. Ring Topology :

A frame travels around the ring, stopping at each node. If a node wants to transmit data, it adds the data as well as the destination address to the frame. The frame then continues around the ring until it finds the destination node, which takes the data out of the frame.

- Single ring – All the devices on the network share a single cable
- Dual ring – The dual ring topology allows data to be sent in both directions although only one ring is used at a time.



Advantages:

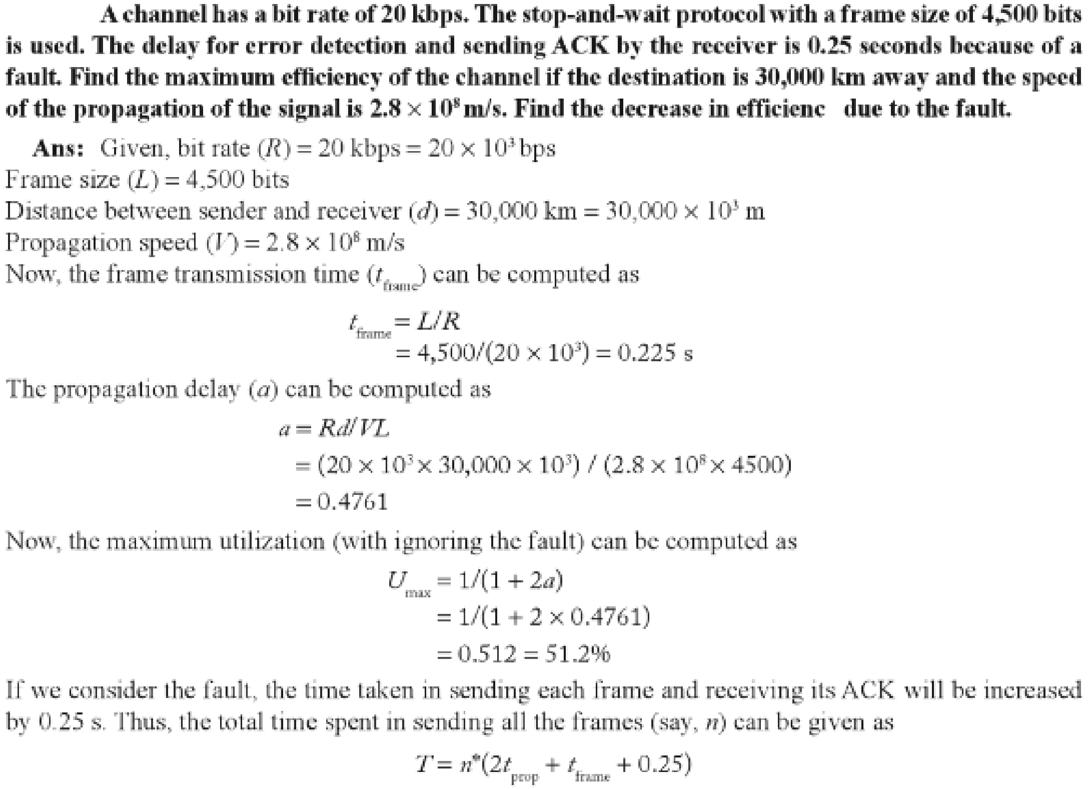
- Every computer is given equal access to the token; no one computer can monopolize the network
- Fair sharing of the network allows the network to degrade gracefully as more users are added

Disadvantages:

- Failure to one network can affect the whole network
- Difficult to troubleshoot a ring network
- Adding or removing computer disrupts the network

Ring network layout ring network is a topology of computer network where each node is connected to two other nodes, so as to create a ring. Ring networks tend to be inefficient when compared to Star networks because data must travel through less number of points before reaching its destination. For example , if a given ring network has eight computers on it, to get from computer one to computer four, data must be travel from computer one, through computers two and three, and to it's destination at computer four. It could also go from computer one through eight, seven, six, and five until reaching four, but this method is slower because it travels through more computers. Ring network also carry the disadvantage that if one of the nodes in the network breaks then the entire network will break down with it as it requires a full circle in order to function.

b. A channel has a bit rate of 20 kbps. The stop and wait protocol with frame size 4500 bits is used. The delay for error detection and sending ACK by the receiver is 0.25 seconds because of a fault. Find the maximum efficiency of the channel if the destination is 30000km away and the speed of the propagation of the signal is 2.8X10^8 m/s. Find the decrease in efficiency due to the fault.



A channel has a bit rate of 20 kbps. The stop-and-wait protocol with a frame size of 4,500 bits is used. The delay for error detection and sending ACK by the receiver is 0.25 seconds because of a fault. Find the maximum efficiency of the channel if the destination is 30,000 km away and the speed of the propagation of the signal is 2.8 × 10^8 m/s. Find the decrease in efficienc due to the fault.

Ans: Given, bit rate (R) = 20 kbps = 20×10^3 bps

Frame size (L) = 4,500 bits

Distance between sender and receiver (d) = 30,000 km = $30{,}000 \times 10^3$ m

Propagation speed (V) = 2.8×10^8 m/s

Now, the frame transmission time (t_{frame}) can be computed as

$$t_{\text{frame}} = L/R$$
$$= 4{,}500/(20 \times 10^3) = 0.225 \text{ s}$$

The propagation delay (a) can be computed as

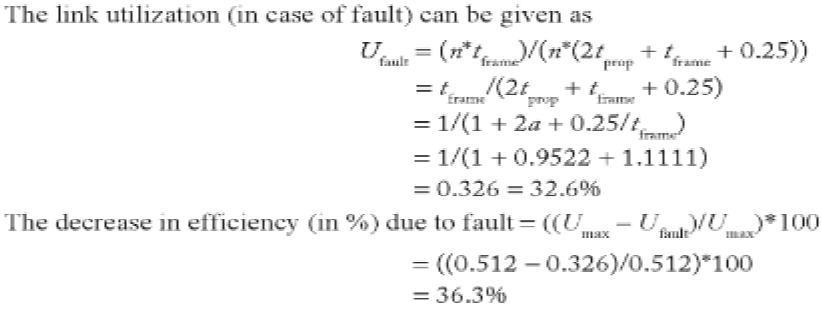
$$a = Rd/VL$$
$$= (20 \times 10^3 \times 30{,}000 \times 10^3) / (2.8 \times 10^8 \times 4500)$$
$$= 0.4761$$

Now, the maximum utilization (with ignoring the fault) can be computed as

$$U_{\max} = 1/(1 + 2a)$$
$$= 1/(1 + 2 \times 0.4761)$$
$$= 0.512 = 51.2\%$$

If we consider the fault, the time taken in sending each frame and receiving its ACK will be increased by 0.25 s. Thus, the total time spent in sending all the frames (say, n) can be given as

$$T = n^*(2t_{\text{prop}} + t_{\text{frame}} + 0.25)$$



The link utilization (in case of fault) can be given as

$$\begin{aligned} U_{\text{fault}} &= (n^*t_{\text{frame}})/(n^*(2t_{\text{prop}} + t_{\text{frame}} + 0.25)) \\ &= t_{\text{frame}}/(2t_{\text{prop}} + t_{\text{frame}} + 0.25) \\ &= 1/(1 + 2a + 0.25/t_{\text{frame}}) \\ &= 1/(1 + 0.9522 + 1.1111) \\ &= 0.326 = 32.6\% \end{aligned}$$

The decrease in efficiency (in %) due to fault $= ((U_{\text{max}} - U_{\text{fault}})/U_{\text{max}})^*100$

$$\begin{aligned} &= ((0.512 - 0.326)/0.512)^*100 \\ &= 36.3\% \end{aligned}$$

c. What is unicast routing? Discuss unicast routing protocols.

Unicast means the transmission from a single sender to a single receiver. It is a point to point communication between sender and receiver. There are various unicast protocols such as TCP, HTTP, etc.

- TCP is the most commonly used unicast protocol. It is a connection oriented protocol that relay on acknowledgement from the receiver side.
- HTTP stands for Hyper Text Transfer Protocol. It is an object oriented protocol for communication.

There are three major protocols for unicast routing:

1. Distance Vector Routing
2. Link State Routing
3. Path-Vector Routing

Interior and Exterior Routing

Routing inside an autonomous system is called interior routing. In interior routing, the IP datagram travels from a router to another router of the same network. Routing between autonomous systems is called exterior routing. In exterior routing, an IP datagram travels from a router of one network to the router of another network. Each autonomous system can choose the routing protocol it implements for interior routing. Popular protocols for interior routing are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF). An internet uses only one exterior routing protocol. A popular exterior routing protocol is Border Gateway Protocol (BGP).

The RIP treats all networks as equals. The cost of passing through all routers is one hop count. The OSPF allows the administrator to assign a cost depending on the service required (such as throughput or minimum delay). The BGP assigns metrics based on criterion.

Routing Information Protocol Updating Algorithm

```
Receive: a response RIP message
1. Add one hop to the hop count for each advertised destination.
2. Repeat the following steps for each advertised destination:
    1. If (destination not in the routing table)
        1. Add the advertised information to the table.
    2. Else If (next-hop field is the same)
        1. Replace entry in the table with the advertised one.
    2. Else If (advertised hop count smaller than one in the table)
        1. Replace entry in the routing table.
3. Return.
```

Open Shortest Path First (OSPF)

Autonomous System Boundary Routers are responsible for delivering information about other autonomous systems into the current system. Within the autonomous system, the OSPF divides the hosts into areas. Each area has a area border router which summarizes information in the area and distributes it to other areas. All areas are connected to a special area called a backbone and areas can be connected to other areas. The backbone has the AS boundary router. If the direct connection between an area and the backbone the administrator must create a virtual link which may pass though several other areas.

OSPF Connections

- The point-to-point link connects two routers without any other host or router in between.
- The transient link is a network with several routers. Data can come in and out of the network through all the routers. All LANs and some WANs are of this type. To avoid a mesh topology, a router called a designated router is positioned at the center such that every other router has only one neighbor which is the designated router. The designated router is not an additional router. One of the existing routers is “designated” with the task.
- The stub link is a special case of the transient link where the number of routers equals one. All data going in and out of the network pass through this router.
- The virtual link is created when the direct link between two routers has been broken. Because it is not anymore possible for the data to go from router A to router B directly then the data would need to pass fro from router A to router C to router E then finally to router B for example.

Link State Advertisement

Link state advertisements serve to inform the network about the information of an entity’s neighbors. The type of LSA depends on the different entities that broadcast them.

1. Router LSA - the router announces its presence and lists the links to other routers or networks in the same area, together with the metrics to them. Type 1 LSAs are flooded across their own area only.
2. Network LSA - the designated router on a broadcast segment (e.g. Ethernet) lists which routers are joined together by the segment. Type 2 LSAs are flooded across their own area only.
3. Summary LSA to Network - an Area Border Router (ABR) takes information it has learned on one of its attached areas and it can summarize it (but not by default) before sending it out on other areas it is connected to. This summarization helps provide scalability by removing detailed topology information for other areas, because their routing information is summarized into just an address prefix and metric.
4. ASBR-Summary LSA - this is needed because Type 5 External LSAs are flooded to all areas and the detailed next-hop information may not be available in those other areas. This is solved by an Area Border Router flooding the information for the router (i.e. the Autonomous System Boundary Router) where the type 5 originated.
5. External LSA - these LSAs contain information imported into OSPF from other routing processes. They are flooded to all areas (except stub areas).

The Dijkstra algorithm

The Dijkstra (silent j) algorithm is an algorithm which determines the best (shortest) route from a single node to all other nodes. Each route is one source to one destination. The source of the route is only one node but the destination changes though there is only one destination for every shortest route. Thus this is very useful for unicast routing wherein the source node (which is permanent) should know the shortest path to a single destination node (which changes).

Dijkstra algorithm is as follows

1. Start with the local node (router): the root of the tree.
2. Assign a cost of 0 to this node and make it the first permanent node.
3. Examine each neighbor node of the node that was the last permanent node.
4. Assign a cumulative cost to each node and make it tentative.
5. Among the list of tentative nodes

1. Find the node with the smallest cumulative cost and make it permanent.
2. If a node can be reached from more than one direction

1. Select the direction with the shortest cumulative cost.

6. Repeat steps 3 to 5 until every node becomes permanent.

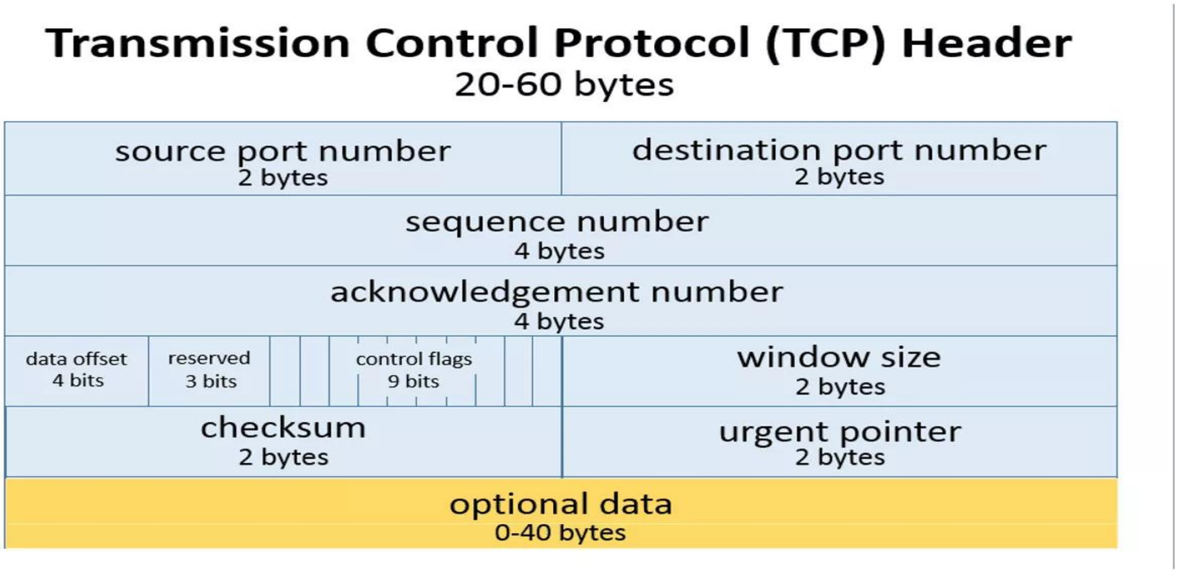
d. Explain about the TCP header and working of TCP protocol anddifferentiate between TCP and UDP with frame format.

TCP vs. UDP Headers

Both TCP and UDP use headers as part of packaging the message data for transfer over network connections. Because TCP is the more robust of the two protocols, its header is larger at 20 bytes with an option for additional data, while UDP headers are limited to 8 bytes in size.

TCP Header Format

Each TCP header has 10 required fields totaling 20 bytes (160 bits) in size. It can optionally include an additional data field up to 40 bytes in size.



TCP headers appear in the following sequence, beginning with the source and destination communication endpoints:

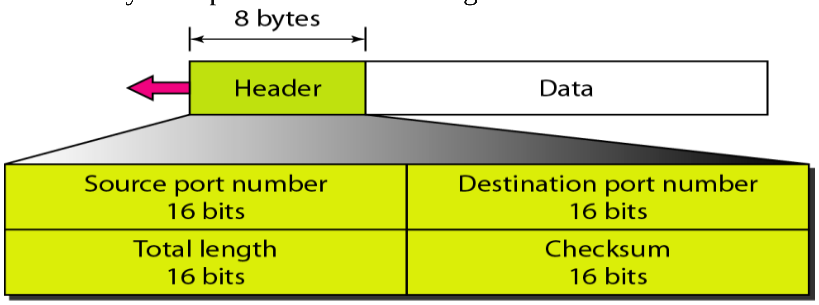
- **Source TCP port number** (2 bytes or 16 bits): The source TCP port number represents the sending device.
- **Destination TCP port number** (2 bytes or 16 bits): The destination TCP port number is the communication endpoint for the receiving device.
- **Sequence number** (4 bytes or 32 bits): Message senders use sequence numbers to mark the ordering of a group of messages.
- **Acknowledgment number** (4 bytes or 32 bits): Both senders and receivers use the acknowledgment numbers field to communicate the sequence numbers of messages that are either recently received or expected to be sent.
- **TCP data offset** (4 bits): The data offset field stores the total size of a TCP header in multiples of four bytes. A header not using the optional TCP field has a data offset of 5 (representing 20 bytes), while a header using the maximum-sized optional field has a data offset of 15 (representing 60 bytes).
- **Reserved data** (3 bits): Reserved data in TCP headers always has a value of zero. This field serves the purpose of aligning the total header size as a multiple of four bytes, which is important for the efficiency of computer data processing.
- **Control flags** (up to 9 bits): TCP uses a set of six standard and three extended control flags — each an individual bit representing On or Off — to manage data flow in specific situations.

- **Window size** (2 bytes or 16 bits): TCP senders use a number called window size to regulate how much data they send to a receiver before requiring an acknowledgment in return. If the window size is too small, network data transfer is unnecessarily slow. If the window size is too large, the network link may become saturated, or the receiver may not be able to process incoming data quickly enough, resulting in slow performance. Windowing algorithms built into the protocol dynamically calculate size values and use this field of TCP headers to coordinate changes between senders and receivers.
- **TCP checksum** (2 bytes or 16 bits): The checksum value inside a TCP header is generated by the protocol sender as a mathematical technique to help the receiver detect messages that are corrupted or tampered with.
- **Urgent pointer** (2 bytes or 16 bits): The urgent pointer field is often set to zero and ignored, but in conjunction with one of the control flags, it can be used as a data offset to mark a subset of a message as requiring priority processing.
- **TCP optional data** (0 to 40 bytes): Usages of optional TCP data include support for special acknowledgment and window scaling algorithms.

UDP Header Format

Because UDP is significantly more limited in capability than TCP, its headers are much smaller. A UDP header contains 8 bytes, divided into the following four required fields:

- **Source UDP port number** (2 bytes): The source UDP port number represents the sending device.
- **Destination UDP port number** (2 bytes): The destination UDP port number is the communication endpoint for the receiving device.
- **Length of data** (2 bytes): The length field in UDP represents the total size of each datagram, including both header and data. This field ranges in value from a minimum of 8 bytes — the required header size — to sizes above 65,000 bytes.
- **UDP checksum** (2 bytes): Similar to TCP, a UDP checksum allows receivers to cross-check incoming data for any corrupted bits of the message.



e. (i) How is TFTP different from FTP?
(ii)What three functions can SNMP perform to manage network devices?

(i) How is TFTP different from FTP?

FTP and TFTP both are the application layer protocols. Both are used to transfer a file from client to server or from the server to the client . But FTP is more complex than TFTP. There are many differences between FTP and TFTP, but the major difference between FTP and TFTP is that FTP establishes two connection for transferring a file between client and server that are TCP’s port 20 for data connection and TCP’s port 21 for the control connection.

S.NO	FTP	TFTP
1.	FTP stands for File Transfer Protocol.	TFTP stands for Trivial File Transfer Protocol.
2.	The software of FTP is larger than TFTP.	While software of TFTP is smaller than FTP.
3.	FTP works on two ports: 20 and 21.	While TFTP works on 69 Port number.
4.	FTP services are provided by TCP.	While TFTP services are provided by UDP.
5.	The complexity of FTP is higher than TFTP.	While the complexity of TFTP is less than FTP complexity.
6.	There are many commands or messages in FTP.	There are only 5 messages in TFTP.
7.	FTP need authentication for communication.	While TFTP does not need authentication for communication.

(ii) What three functions can SNMP perform to manage network devices?

SNMP is an application layer protocol which uses UDP port number 161/162.SNMP is used to monitor the network, detect network faults and sometimes even used to configure remote devices

.

SNMP components –

There are 3 components of SNMP:

1. **SNMP Manager –**
   It is a centralised system used to monitor network.It is also known as Network Management Station (NMS)
2. **SNMP agent –**
   It is a software management software module installed on a managed device. Managed devices can be network devices like PC, router, switches, servers etc.
3. **Management Information Base –**
   MIB consists of information of resources that are to be managed. These information is organised hierarchically. It consists of objects instances which are essentially variables.

SNMP agents.

An agent is a program that can gather information about a piece of hardware, organize it into predefined entries, and respond to queries using the SNMP protocol.

The component of this model that queries agents for information is called an SNMP **manager**. These machines generally have data about all of the SNMP-enabled devices in their network and can issue requests to gather information and set certain properties.

SNMP Managers

An SNMP manager is a computer that is configured to poll SNMP agent for information. The management component, when only discussing its core functionality, is actually a lot less complex than the client configuration, because the management component simply requests data.

The manager can be any machine that can send query requests to SNMP agents with the correct credentials. Sometimes, this is implemented as part of a monitoring suite, while other times this is an administrator using some simple utilities to craft a quick request.

Almost all of the commands defined in the SNMP protocol (we will go over these in detail later) are designed to be *sent* by a manager component. These include GetRequest, GetNextRequest, GetBulkRequest, SetRequest, InformRequest, and Response. In addition to these, a manager is also designed to *respond to* Trap, and Response messages.

SNMP Agents

SNMP agents do the bulk of the work. They are responsible for gathering information about the local system and storing them in a format that can be queried.updating a database called the "management information base", or **MIB**.

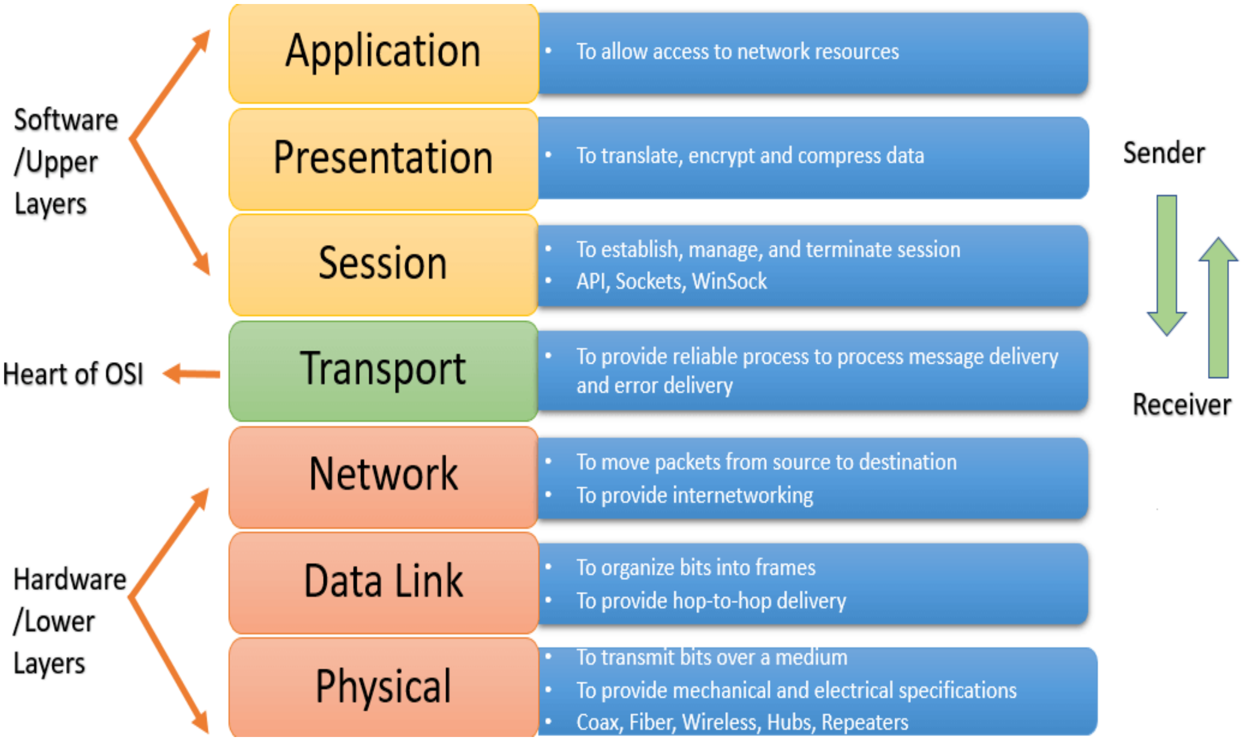
The MIB is a hierarchical, pre-defined structure that stores information that can be queried or set. This is available to well-formed SNMP requests originating from a host that has authenticated with the correct credentials (an SNMP manager).

The agent computer configures which managers should have access to its information. It can also act as an intermediary to report information on devices it can connect to that are not configured for SNMP traffic. This provides a lot of flexibility in getting your components online and SNMP accessible.

SECTION C

3. What is OSI Model? Explain the functions; protocols and services of each layer?

The OSI Model is a logical and conceptual model that defines network communication used by systems open to interconnection and communication with other systems. The Open System Interconnection (OSI Model) also defines a logical network and effectively describes computer packet transfer by using various layers of protocols.


Software
/Upper
Layers
Heart of OSI
Hardware
/Lower
Layers
Application
Presentation
Session
Transport
Network
Data Link
Physical
To allow access to network resources
To translate, encrypt and compress data
To establish, manage, and terminate session
API, Sockets, WinSock
To provide reliable process to process message delivery and error delivery
To move packets from source to destination
To provide internetworking
To organize bits into frames
To provide hop-to-hop delivery
To transmit bits over a medium
To provide mechanical and electrical specifications
Coax, Fiber, Wireless, Hubs, Repeaters
Sender
Receiver

1. Physical Layer (Layer 1) :

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.** It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

The functions of the physical layer are :

1. **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
2. **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
3. **Physical topologies:** Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topolgy.
4. **Transmission mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

2. Data Link Layer (DLL) (Layer 2) :

The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.

Data Link Layer is divided into two sub layers :

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

The packet received from Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver’s MAC address in the header.

The Receiver’s MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking “Who has that IP address?” and the destination host will reply with its MAC address.

The functions of the data Link layer are :

1. **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
2. **Physical addressing:** After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
3. **Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
4. **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus , flow control coordinates that amount of data that can be sent before receiving acknowledgement.
5. **Access control:** When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

3. Network Layer (Layer 3) :

Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver’s IP address are placed in the header by the network layer.

The functions of the Network layer are :

1. **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.

2. **Logical Addressing:** In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

4. Transport Layer (Layer 4) :

Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

The functions of the transport layer are :

1. **Segmentation and Reassembly:** This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the segment produced has a header associated with it. The transport layer at the destination station reassembles the message.
2. **Service Point Addressing:** In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.

The services provided by the transport layer :

1. **Connection Oriented Service:** It is a three-phase process which include
   – Connection Establishment
   – Data Transfer
   – Termination / disconnection
   In this type of transmission, the receiving device sends an acknowledgement, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.
2. **Connection less service:** It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

5. Session Layer (Layer 5) :

This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.

The functions of the session layer are :

1. **Session establishment, maintenance and termination:** The layer allows the two processes to establish, use and terminate a connection.
2. **Synchronization :** This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
3. **Dialog Controller :** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

6. Presentation Layer (Layer 6) :

Presentation layer is also called the **Translation layer**.The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.
The functions of the presentation layer are :

1. **Translation :** For example, ASCII to EBCDIC.
2. **Encryption/ Decryption :** Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
3. **Compression:** Reduces the number of bits that need to be transmitted on the network.

7. Application Layer (Layer 7) :

At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

The functions of the Application layer are :

1. Network Virtual Terminal
2. FTAM-File transfer access and management
3. Mail Services
4. Directory Services

OSI model acts as a reference model and is not implemented in the Internet because of its late invention. Current model being used is the TCP/IP model.

4. (a) A slotted ALOHA network transmits 400-bit frames on a shared channel of 400 kbps. What is the throughput if the system (all stations together) produces

(i) 1000 frames per second

The frame transmission time is 200/200 kbps or 1 ms.
If the system creates 1000 frames per second, this is 1
frame per millisecond. The load is 1. In this case
$S = G\times e-2\ G$ or $S = 0.135$ (13.5 percent).
This means that the throughput is 1000 × 0.135 = 135 frames. Only
135 frames out of 1000 will probably survive.

(ii) 500 frames per second

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 × 0.184 = 92 and that
only 92 frames out of 500 will probably survive.

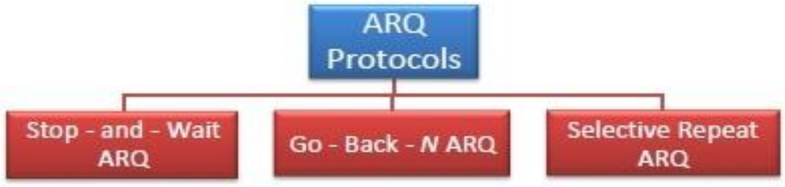
(iii) 250 frames per second

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 × 0.152 = 38. Only 38
frames out of 250 will probably survive.

4.(b) Explain ARQ Error Control technique, in brief.

Automatic Repeat ReQuest (ARQ) is a group of error – control protocols for transmission of data over noisy or unreliable communication network. These protocols reside in the Data Link Layer and in the Transport Layer of the OSI (Open Systems Interconnection) reference model. They are named so because they provide for automatic retransmission of frames that are corrupted or lost during transmission. ARQ is also called Positive Acknowledgement with Retransmission (PAR).

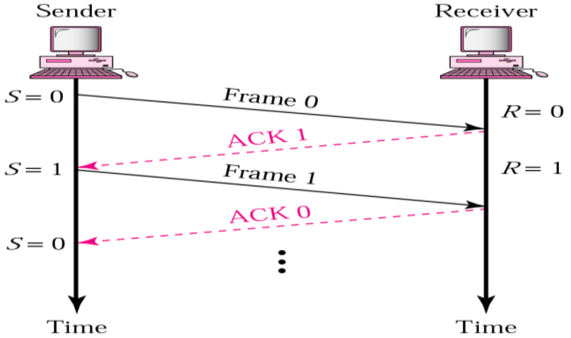
Types of ARQ Protocols



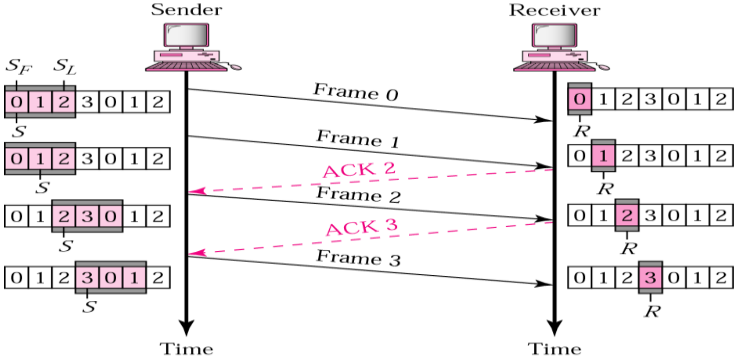
- **Stop – and – Wait ARQ** − Stop – and – wait ARQ provides unidirectional data transmission with flow control and error control mechanisms, appropriate for noisy channels. The sender keeps a copy of the sent frame. It then waits for a finite time to receive a positive acknowledgement from receiver. If the timer expires, the frame is retransmitted. If a positive acknowledgement is received then the next frame is sent.

The following transition may occur in Stop-and-Wait ARQ:

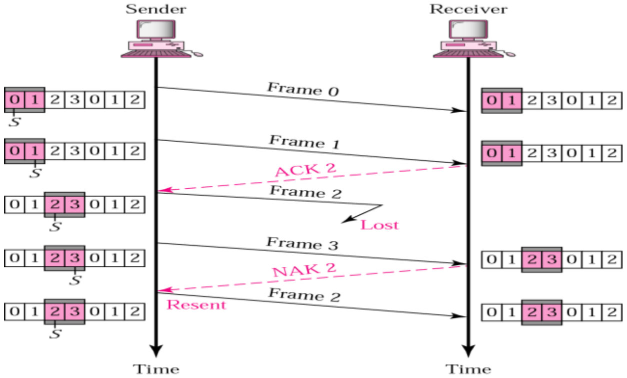
- The sender maintains a timeout counter. When a frame is sent, the sender starts the timeout counter.
- If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
- If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.



- **Go – Back – N ARQ** − Go – Back – N ARQ provides for sending multiple frames before receiving the acknowledgement for the first frame. It uses the concept of sliding window, and so is also called sliding window protocol. The frames are sequentially numbered and a finite number of frames are sent. If the acknowledgement of a frame is not received within the time period, all frames starting from that frame are retransmitted.
- Stop and wait ARQ mechanism does not utilize the resources at their best.
- When the acknowledgement is received, the sender sits idle and does nothing. In Go-Back-N ARQ method, both sender and receiver maintain a window.
- The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones.
- The receiving-window enables the receiver to receive multiple frames and acknowledge them.
- The receiver keeps track of incoming frame's sequence number.
- When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement.
- If all frames are positively acknowledged, the sender sends next set of frames. If sender finds that it has received NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.



- **Selective Repeat ARQ** − This protocol also provides for sending multiple frames before receiving the acknowledgement for the first frame. However, here only the erroneous or lost frames are retransmitted, while the good frames are received and buffered.
- In Go-back-N ARQ, it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes.
- This enforces the sender to retransmit all the frames which are not acknowledged.
- In Selective-Repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged.
- The sender in this case, sends only packet for which NACK is received.



5.(a) Write advantages of Next-generation IPV6 over IPV4

With IPv6, everything from appliances to automobiles can be interconnected. But an increased number of IT addresses isn't the only advantage of IPv6 over IPv4. In honor of World IPv6 Day, here are six more good reasons to make sure your hardware, software, and services support IPv6.

1. **More Efficient Routing**IPv6 reduces the size of routing tables and makes routing more efficient and hierarchical. IPv6 allows ISPs to aggregate the prefixes of their customers' networks into a single prefix and announce this one prefix to the IPv6 Internet. In addition, in IPv6 networks, fragmentation is handled by the source device, rather than the router, using a protocol for discovery of the path's maximum transmission unit (MTU).
2. **More Efficient Packet Processing**IPv6's simplified packet header makes packet processing more efficient. Compared with IPv4, IPv6 contains no IP-level checksum, so the checksum does not need to be recalculated at every router hop. Getting rid of the IP-level checksum was possible because most link-layer technologies already contain checksum and error-control capabilities. In addition, most transport layers, which handle end-to-end connectivity, have a checksum that enables error detection.
3. **Directed Data Flows**IPv6 supports multicast rather than broadcast. Multicast allows bandwidth-intensive packet flows (like multimedia streams) to be sent to multiple destinations simultaneously, saving network bandwidth. Disinterested hosts no longer must process broadcast packets. In addition, the IPv6 header has a new field, named Flow Label, that can identify packets belonging to the same flow.
4. **Simplified Network Configuration**Address auto-configuration (address assignment) is built in to IPv6. A router will send the prefix of the local link in its router advertisements. A host can generate its own IP address by appending its link-layer (MAC) address, converted into Extended Universal Identifier (EUI) 64-bit format, to the 64 bits of the local link prefix.
5. **Support For New Services**By eliminating Network Address Translation (NAT), true end-to-end connectivity at the IP layer is restored, enabling new and valuable services. Peer-to-peer networks are easier to create and maintain, and services such as VoIP and Quality of Service (QoS) become more robust.

6. **Security**
   IPSec, which provides confidentiality, authentication and data integrity, is baked into in IPv6. Because of their potential to carry malware, IPv4 ICMP packets are often blocked by corporate firewalls, but ICMPv6, the implementation of the Internet Control Message Protocol for IPv6, may be permitted because IPSec can be applied to the ICMPv6 packets.

5.(b) The IP network 200.198.160.0 is using subnet mask 255.255.255.224. Design the subnets.

Mask 255.255.255.224 means 2^3 =8 subnets and 2^5 =32 host per subnet are there.

Subnet 1:	200.198.160.0	to	200.198.160.31
Subnet 2:	200.198.160.32	to	200.198.160.63
Subnet 3:	200.198.160.64	to	200.198.160.95
Subnet 4:	200.198.160.96	to	200.198.160.127
Subnet 5:	200.198.160.128	to	200.198.160.159
Subnet 6:	200.198.160.160	to	200.198.160.191
Subnet 7:	200.198.160.192	to	200.198.160.223
Subnet 8:	200.198.160.224	to	200.198.160.255

6.(a) The following is the dump of a TCP header in hexa decimal format: 05320017 00000001 00000000 500207FF 00000000

(i) What is the sequence number?
Sequence number:- 000000001 -> 1

(ii) What is the destination port number?
Destination port number:- (2 byte) -> 0017

(iii) What is the acknowledgment number?
Acknowledgement number:- 00000000 -> 0

(iv) What is the window size?
Window size -> 07FF

6.(b) What do you understand by Quality of service, parameters? List various Qualities of service parameters.

The notion of quality of service, or QoS, concerns certain characteristics of a network connection under the sole of the network service provider liability.

A QoS value applies to the whole of a network connection. It must be identical at both ends of the connection, even if it is supported by several interconnected subnetworks each offering different services.

QoS is described by parameters. Defining a QoS parameter indicates how to measure or determine its value, mentioning if necessary the events specified by the network service primitives.

Two types of QoS parameters have been defined:

• Those whose values are transmitted peer users via the Network service during the establishment phase of the network connection. During this transmission, a tripartite negotiation can take place between users and the network service provider to define a value for the QoS parameters.

• Those whose values are transmitted or negotiated between users and network service provider. For these QoS parameters, it is possible to obtain, by local means, information on the value to the supplier and values to each user of the network service.

The main QoS parameters are:

• **Time of establishment of the network connection**. Is the time that elapses between a network connection request and confirmation of the connection? This QoS parameter indicates the maximum time acceptable to the user.

• **Probability of failure of the establishment of the network connection**. This probability is established from the applications which have not been met in the normal time limit for establishing the connection.

• **Flow data transfer**. The flow rate defines the number of bytes transported over a network connection in a reasonably long time (a few minutes, a few hours or days). The difficulty in determining the speed of a connection network comes from the asynchronous transport packets. To obtain a value acceptable, observe the network on a sequence of several packages and consider number of bytes of data transported taking into account the elapsed time since the application or the data transfer indication.

• **Transit time when transferring data**. The transit time corresponds to elapsed time between a data transfer request and indicating transfer of data. This transit time is difficult to calculate because of the geographical distribution ends. The satisfaction of a quality service on the transit time may moreover contradict flow control.

• **Residual error rate**. Is calculated from the number of packets that arrive erroneous, lost or duplicated on the total number of transmitted packets. It is a rate Error packet. Also denotes the probability that a packet does not arrive correctly to the receiver.

• **Transfer Probability incident**. Is obtained by the ratio of the number of incidents listed on the total number of transfer taken. To have a correct estimate of this probability, just consider the number of network disconnection relative to the number of transfer taken.

• **Probability of failure of the network connection**. Is calculated from the number of release and resetting of a network connection based on the number of transfer made.

• **Release time the network connection**. This is the maximum acceptable delay between a disconnection request and the actual release.

• Probability of failure upon release of the network connection. The number Liberation of failure required by the total number requested release.

The following three additional parameters used to characterize the quality of Service:

• **Protection of the network connection**. Determines the probability that the network connection be in working order throughout the period when it is opened by the user. There is ways to protect a connection by duplicating or having a Backup connection ready to be opened in case of failure. The value for a telephone network is 99.999%, the so-called five nines, equivalent to a few minutes of downtime per year. The protection is much lower for an IP network, with a value of the order of 99.9%, three or nine. This value arises besides problem for IP telephony, which requires stronger protection telephone connections.

• **Priority of the network connection**. Determines priority of access to a connection network, the holding priority of a network connection and priority of data connection.

• **Maximum acceptable cost**. Determines if the network connection is tolerable or not. The definition of the cost is quite complex since it depends on the use of resources for the establishment, maintenance and release of the connection network.

Flow Characteristics

Traditionally, four types of characteristics are attributed to a flow: reliability, delay, jitter and bandwidth.

Reliability

- Reliability is an important characteristic of flow.
- Lack of reliability means losing a packet or acknowledgement which then requires retransmission.
- However, the sensitivity of application programs to reliability is not the same. For example, it is more important that electronic mail, file transfer, and internet access have reliable transmissions than audio conferencing or telephony.

Delay

- Source to destination delay is another flow characteristic.
- Applications can tolerate delay in different degrees.
- In this case, telephony, audio conferencing, video conferencing and remote log in need minimum delay while delay in file transfer or e-mail is less important.

Jitter

- Jitter is defined as the variation in delay for packets belonging to the same flow.
- High Jitter means the difference between delays is large and low jitter means the variation is small.
- For example, if four packets depart at times 0, 1,2,3 and arrive at 20, 21,22, 23, all have same delay, 20 units of time. On the other hand, if the above four packets arrive at 21,23,21, and 28 they will have different delays of21, 22, 19 and 24.

Bandwidth

- Different applications need different bandwidths.
- In video conferencing we need to send million of bits per second to refresh a colour screen while the total number of bits in an email may not reach even a million.

7(a)(i). How is the BOOTP different from DHCP?

BOOTP, Bootstrap protocol, is used to configure host and get address of host along with bootstrap info. DHCP, Dynamic Host Configuration Protocol Server is an extended version of BOOTP and is used to configure hosts mechanically.

Following are the important differences between BOOTP and DHCP.

Sr. No.	Key	BOOTP	DHCP
1	Definition	BOOTP stands for Bootstrap protocol.	DHCP stands for Dynamic Host Configuration Protocol.
2	Temporary IP Address	BOOTP has no support for temporary IP Addressing.	DHCP Server support for temporary IP Addressing but for limited period of time.
3	Client Support	BOOTP does not support DHCP Clients.	DHCP server supports BOOTP Clients.
4	Configuration Type	In BOOTP, configuration has to be done manually.	In DHCP, configuration is automatic.
5	Mobile Machine Support	Mobile machine are not supported.	Mobile machines are supported
6	Error Probability	Configuration being manual often leads to errors.	Automatic configuration prevents any error to occur.

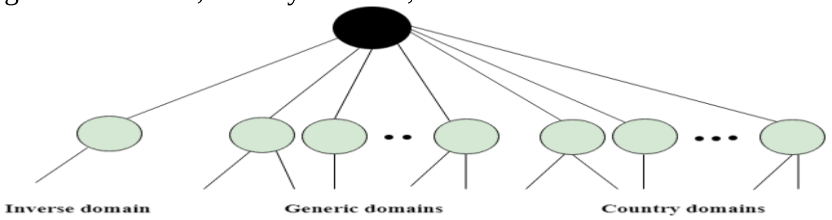
7(a)(ii). What is the purpose of the Domain Name System? Discuss the three main divisions of the domain name space

An application layer protocol defines how the application processes running on different systems, pass the messages to each other.

- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.

- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
- For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than IP address.

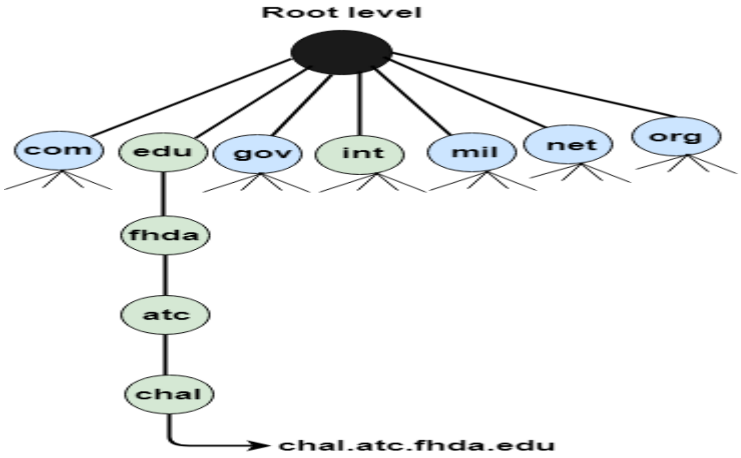
DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.



Generic Domains

- It defines the registered hosts according to their generic behavior.
- Each node in a tree defines the domain name, which is an index to the DNS database.
- It uses three-character labels, and these labels describe the organization type.

Label	Description
aero	Airlines and aerospace companies
biz	Businesses or firms
com	Commercial Organizations
coop	Cooperative business Organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International Organizations
mil	Military groups
museum	Museum & other nonprofit organizations
name	Personal names
net	Network Support centers
org	Nonprofit Organizations
pro	Professional individual Organizations



Country Domain

The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States) in place of three character organizational abbreviations.

Inverse Domain

The inverse domain is used for mapping an address to a name. When the server has received a request from the client, and the server contains the files of only authorized clients. To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name.

Working of DNS

- DNS is a client/server network communication protocol. DNS clients send requests to the. server while DNS servers send responses to the client.
- Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups.
- DNS implements a distributed database to store the name of all the hosts available on the internet.
- If a client like a web browser sends a request containing a hostname, then a piece of software such as **DNS resolver** sends a request to the DNS server to obtain the IP address of a hostname. If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

7(b).Write short notes on any two:

(i) SMTP

Simple Mail Transfer Protocol (SMTP)

Email is emerging as one of the most valuable services on the internet today. Most of the internet systems use SMTP as a method to transfer mail from one user to another. SMTP is a push protocol and is used to send the mail whereas POP (post office protocol) or IMAP (internet message access protocol) are used to retrieve those mails at the receiver's side.

SMTP Fundamentals: SMTP is an application layer protocol. The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is always on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection on that port (25). After successfully establishing the TCP connection the client process sends the mail instantly.

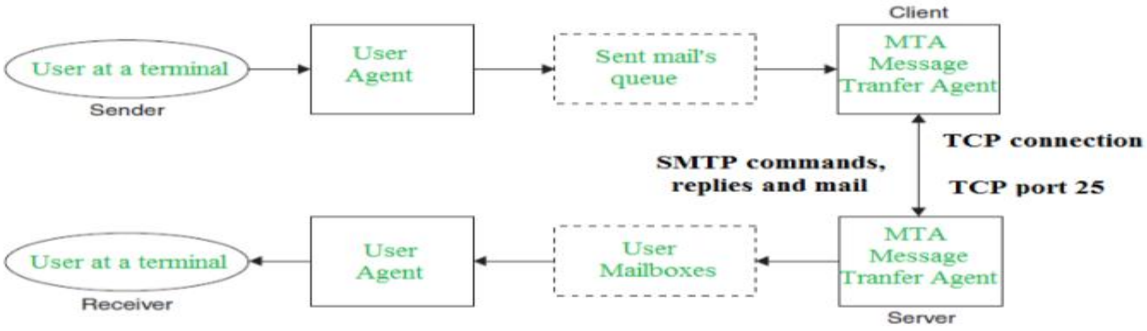
The SMTP model is of two type :

1. End-to- end method
2. Store-and- forward method

The end to end model is used to communicate between different organizations whereas the store and forward method are used within an organization. A SMTP client who wants to send the mail will contact the destination's host SMTP directly in order to send the mail to the destination. The SMTP server will keep the mail to itself until it is successfully copied to the receiver's SMTP. The client SMTP is the one which initiates the session let us call it as the client- SMTP and the server SMTP is the one which responds to the session request and let us call it as receiver-SMTP. The client- SMTP will start the session and the receiver-SMTP will respond to the request.

Model of SMTP system

In the SMTP model user deals with the user agent (UA) for example Microsoft Outlook, Netscape, Mozilla, etc. In order to exchange the mail using TCP, MTA is used. The users sending the mail do not have to deal with the MTA it is the responsibility of the system admin to set up the local MTA. The MTA maintains a small queue of mails so that it can schedule repeat delivery of mail in case the receiver is not available. The MTA delivers the mail to the mailboxes and the information can later be downloaded by the user agents.



Both the SMTP-client and MSTP-server should have 2 components:

1. User agent (UA)
2. Local MTA

Communication between sender and the receiver : The senders, user agent prepare the message and send it to the MTA. The MTA functioning is to transfer the mail across the network to the receivers MTA. To send mail, a system must have the client MTA, and to receive mail, a system must have a server MTA.

SENDING EMAIL: Mail is sent by a series of request and response messages between the client and a server. The message which is sent across consists of a header and the body. A null line is used to terminate the mail header. Everything which is after the null line is considered as the body of the message which is a sequence of ASCII characters. The message body contains the actual information read by the receipt.

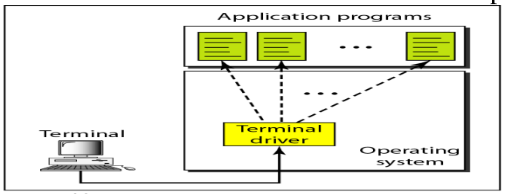
RECEIVING EMAIL: The user agent at the server side checks the mailboxes at a particular time of intervals. If any information is received it informs the user about the mail. When the user tries to read the mail it displays a list of mails with a short description of each mail in the mailbox. By selecting any of the mail user can view its contents on the terminal.

Some SMTP Commands:

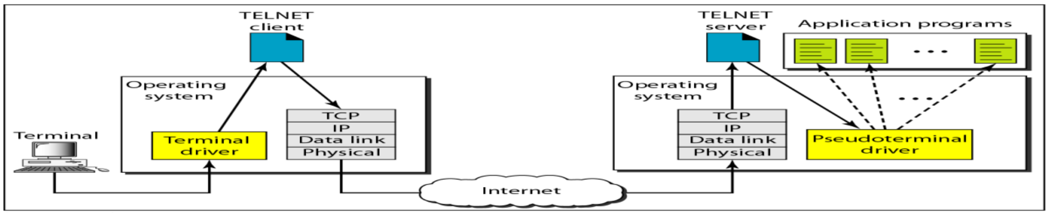
- HELO – Identifies the client to the server, fully qualified domain name, only sent once per session
- MAIL – Initiate a message transfer, fully qualified domain of originator
- RCPT – Follows MAIL, identifies an addressee, typically the fully qualified name of the addressee and for multiple addressees use one RCPT for each addressee
- DATA – send data line by line

(ii) TELNET

TELNET is a general-purpose client-server program that lets a user access any application program on a remote computer; in other words, it allows the user to log onto a remote computer. After logging on, a user can use the services available on the remote computer and transfer the results back to the local computer. TELNET is an abbreviation for terminal network. TELNET enables the establishment of a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system. Local Login When a user logs onto a local time-sharing system, it is called local login. As a user types at a terminal or at a workstation running a terminal emulator, the keystrokes are accepted by the terminal driver. The terminal driver passes the characters to the operating system. The operating system, in turn, interprets the combination of characters and invokes the desired application program or utility



a. Local log-in



b. Remote log-in

The mechanism, however, is not as simple as it seems because the operating system may assign special meanings to special characters. For example, in UNIX some combinations of characters have special meanings, such as the combination of the control character with the character z means suspend; the combination of the control character with the character c means abort; and so on. Whereas these special situations do not create any problem in local login because the terminal emulator and the terminal driver know the exact meaning of each character or combination of characters, they may create problems in remote login. Which process should interpret special characters? The client or the server? We will clarify this situation later in this section. Remote Login 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.

(iii) HTTP

The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. This is the foundation for data communication for the World Wide Web (i.e. internet) since 1990. HTTP is a generic and stateless protocol which can be used for other purposes as well using extensions of its request methods, error codes, and headers.

Basically, HTTP is a TCP/IP based communication protocol, that is used to deliver data (HTML files, image files, query results, etc.) on the World Wide Web. The default port is TCP 80, but other ports can be used as well. It provides a standardized way for computers to communicate with each other. HTTP specification specifies how clients' request data will be constructed and sent to the server, and how the servers respond to these requests.

Basic Features

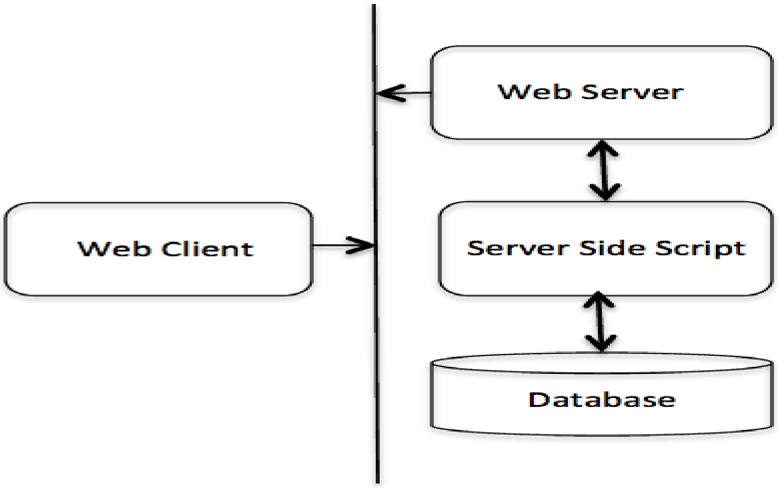
There are three basic features that make HTTP a simple but powerful protocol:

- **HTTP is connectionless:** The HTTP client, i.e., a browser initiates an HTTP request and after a request is made, the client waits for the response. The server processes the request and sends a response back after which client disconnect the connection. So client and server knows about each other during current request and response only. Further requests are made on new connection like client and server are new to each other.
- **HTTP is media independent:** It means, any type of data can be sent by HTTP as long as both the client and the server know how to handle the data content. It is required for the client as well as the server to specify the content type using appropriate MIME-type.
- **HTTP is stateless:** As mentioned above, HTTP is connectionless and it is a direct result of HTTP being a stateless protocol. The server and client are aware of each other only during a current request. Afterwards, both of them forget about each other. Due to this nature of the protocol, neither the client nor the browser can retain information between different requests across the web pages.

HTTP/1.0 uses a new connection for each request/response exchange, where as HTTP/1.1 connection may be used for one or more request/response exchanges.

Basic Architecture

The following diagram shows a very basic architecture of a web application and depicts where HTTP sits:



HTTP Protocol

The HTTP protocol is a request/response protocol based on the client/server based architecture where web browsers, robots and search engines, etc. act like HTTP clients, and the Web server acts as a server.

Client

The HTTP client sends a request to the server in the form of a request method, URI, and protocol version, followed by a MIME-like message containing request modifiers, client information, and possible body content over a TCP/IP connection.

Server

The HTTP server responds with a status line, including the message's protocol version and a success or error code, followed by a MIME-like message containing server information, entity meta information, and possible entity-body content.