Solution of University QP 2017-18

Q1.i.

Sol. We can use Shannon’s theorem to determine the maximum achievable data rate

$$DataRate=Blog_2(1+SNR)$$

Thus, Bandwidth (in Hz) = 3 * 103= 3000 Hz. And we need to convert SNR to power ratio,

$$20dB=10log_{10}(S/N)$$

$$SN=10^2=100$$

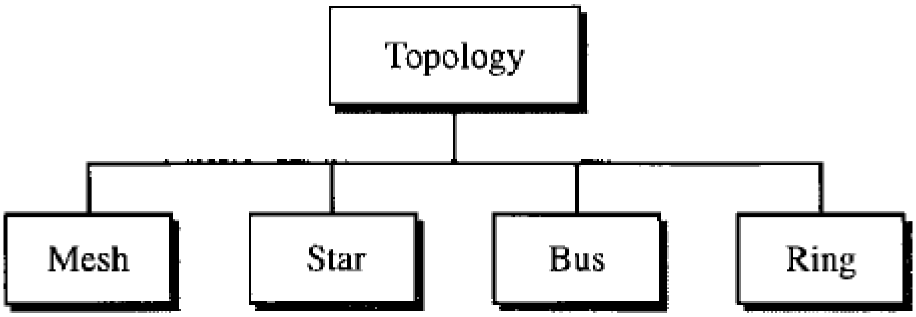
DataRate=3000 log_2(1+100)= 3000 (6.658) = 19974.63 bits/sec or 19.975 kbps.

Nyquist max rate = 2∗Blog_2L= 2∗3000 $log_2$2= 6 kbps.

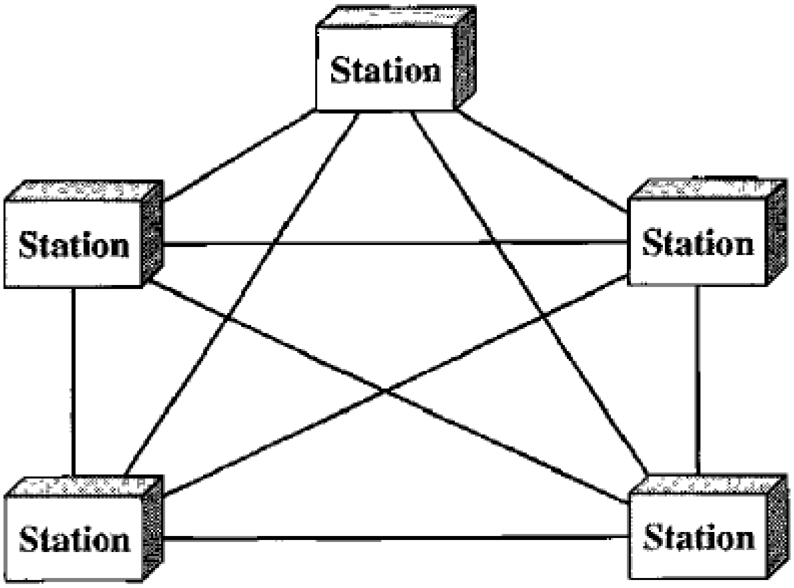
Therefore, the maximum achievable data rate is 6 kbps.

Q2. A. Explain network topological design with necessary diagram and brief the advantages and disadvantages of various topologies.

Ans. 2.a. The term physical topology refers to the way in which a network is laid out physically. One or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are four basic topologies possible: mesh, star, bus, and ring



a. **Mesh:** In a mesh topology, every device has a dedicated point-to-point link to every other device. The term *dedicated* means that the link carries traffic only between the two devices it connects.
Note: In other words, we can say that in a mesh topology, we need n(n -1) /2 duplex-mode links.



Advantages:

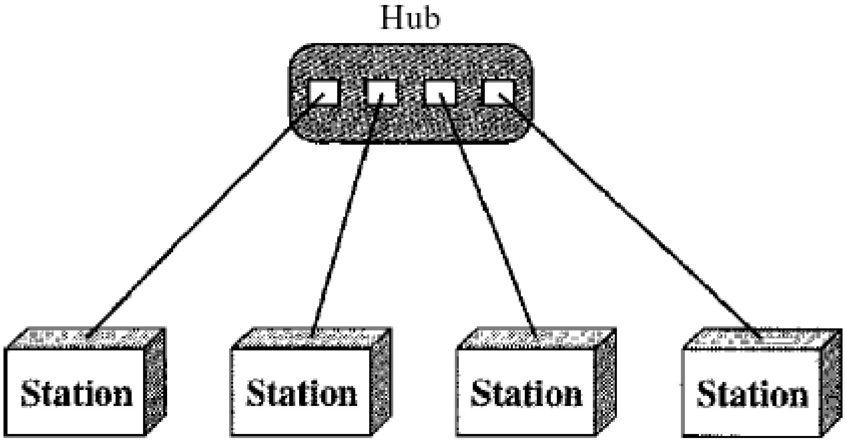
- The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
- A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
- There is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it.
- Finally, point-to-point links make fault identification and fault isolation easy.

Disadvantages:

- Disadvantage of a mesh are related to the amount of cabling because every device must be connected to every other device, installation and reconnection are difficult.
- Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
- Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

b. Star Topology:

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a meshtopology, a star topology does not allow direct traffic between devices. The controller acts as anexchange: If one device wants to send data to another, it sends the data to the controller, whichthen relays the data to the other connected device.



Advantages:

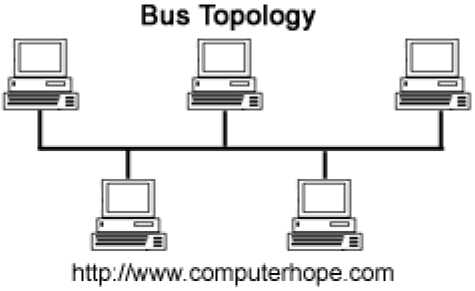
- Fast performance with few nodes and low network traffic.
- Hub can be upgraded easily.
- Easy to troubleshoot.
- Easy to setup and modify.
- Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages:

- Cost of installation is high.
- Expensive to use.
- If the hub fails then the whole network is stopped because all the nodes depend on the hub.
- Performance is based on the hub that is it depends on its capacity

c. Bus Topology:

Alternatively referred to as a ***line topology***, a bus topology is a network setup in which each computer and network device are connected to a single cable or backbone.



Advantages:

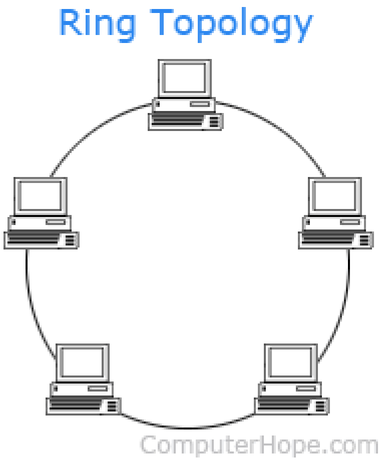
- It works well when you have a small network.
- It's the easiest network topology for connecting computers or peripherals in a linear fashion.
- It requires less cable length than a star topology.

Disadvantages:

- It can be difficult to identify the problems if the whole network goes down.
- It can be hard to troubleshoot individual device issues.
- Bus topology is not great for large networks.
- Terminators are required for both ends of the main cable.
- Additional devices slow the network down.
- If a main cable is damaged, the network fails or splits into two.

d. Ring Topology:

In a ring topology, each device has a dedicated point-to-point connection withonly the two devices on either side of it. A signal is passed along the ring in one direction, fromdevice to device, until it reaches its destination. Each device in the ring incorporates a repeater.When a device receives a signal intended for another device, its repeater regenerates the bits andpasses them along.



Advantages:

- All data flows in one direction, reducing the chance of packet collisions.
- A network server is not needed to control network connectivity between each workstation.
- Data can transfer between workstations at high speeds.
- Additional workstations can be added without impacting performance of the network.

Disadvantages:

- All data being transferred over the network must pass through each workstation on the network, which can make it slower than a star topology.
- The entire network will be impacted if one workstation shuts down.
- The hardware needed to connect each workstation to the network is more expensive than Ethernet cards and hubs/switches.

Q2.B. Discuss the issues in the data link layer and about its protocol on the basis of layering principle.

Ans 2.B. Data Link Layer is second layer of OSI Layered Model. This layer is one of the most complicated layers and has complex functionalities and liabilities. Data link layer hides the details of underlying hardware and represents itself to upper layer as the medium to communicate.

Data link layer works between two hosts which are directly connected in some sense. This direct connection could be point to point or broadcast. Systems on broadcast network are said to be on same link. The work of data link layer tends to get more complex when it is dealing with multiple hosts on single collision domain.

Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware. At the receiving end, Data link layer picks up data from hardware which are in the form of electrical signals, assembles them in a recognizable frame format, and hands over to upper layer.

Data link layer has two sub-layers:

Logical Link Control: It deals with protocols, flow-control, and error control

Media Access Control: It deals with actual control of media

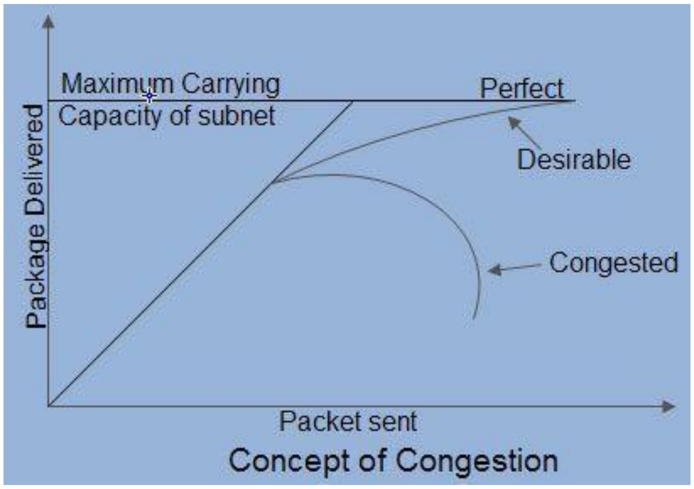
Functionality of Data-link Layer

Data link layer does many tasks on behalf of upper layer. These are:

- **a. Framing:** Data-link layer takes packets from Network Layer and encapsulates them into Frames. Then, it sends each frame bit-by-bit on the hardware. At receiver' end, data link layer picks up signals from hardware and assembles them into frames.
- **b. Addressing:** Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.
- **c. Synchronization:** When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.
- **d. Error Control:** Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.
- **e. Flow Control:** Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machine to exchange data on same speed.
- **f. Multi-Access:** When host on the shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple Systems.

Q2. C. What is congestion? Briefly describe the techniques that prevent congestion.

Ans.2.c. Congestion is a situation in Communication Networks in which too many packets are present in a part of the subnet, performance degrades. Congestion in a network may occur when the load on the network (i.e. the number of packets sent to the network) is greater than the capacity of the network (i.e. the number of packets a network can handle.). Network congestion occurs in case of traffic overloading.



Congestion control algorithms

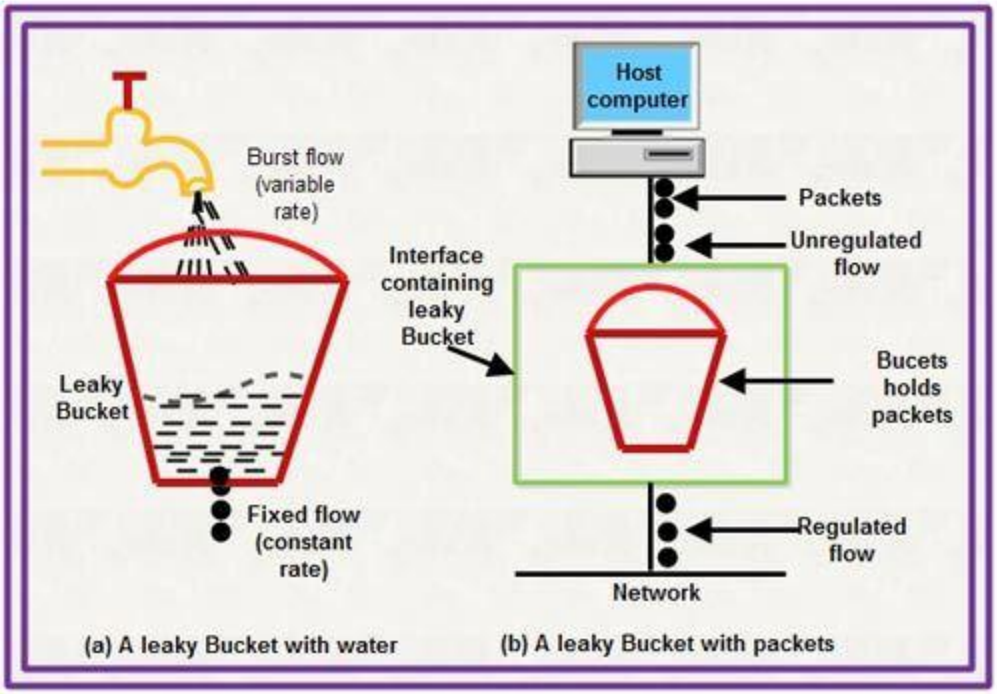
Leaky Bucket Algorithm

• It is a traffic shaping mechanism that controls the amount and the rate of the traffic sent to the network.

• A leaky bucket algorithm shapes bursty traffic into fixed rate traffic by averaging the data rate.

• Imagine a bucket with a small hole at the bottom.

• The rate at which the water is poured into the bucket is not fixed and can vary but it leaks from the bucket at a constant rate. Thus (as long as water is present in bucket), the rate at which the water leaks does not depend on the rate at which the water is input to the bucket.


Burst flow (variable rate)
Leaky Bucket
Fixed flow (constant rate)
Host computer
Packets
Unregulated flow
Interface containing leaky Bucket
Bucets holds packets
Regulated flow
Network
(a) A leaky Bucket with water
(b) A leaky Bucket with packets

• Also, when the bucket is full, any additional water that enters into the bucket spills over the sides and is lost.

• The same concept can be applied to packets in the network. Consider that data is coming from the source at variable speeds. Suppose that a source sends data at 12 Mbps for 4 seconds. Then there is no data for 3 seconds. The source again transmits data at a rate of 10 Mbps for 2 seconds. Thus, in a time span of 9 seconds, 68 Mb data has been transmitted.

If a leaky bucket algorithm is used, the data flow will be 8 Mbps for 9 seconds. Thus constant flow is maintained.

Token bucket Algorithm

• The leaky bucket algorithm allows only an average (constant) rate of data flow. Its major problem is that it cannot deal with bursty data.

• A leaky bucket algorithm does not consider the idle time of the host. For example, if the host was idle for 10 seconds and now it is willing to sent data at a very high speed for another 10 seconds, the total data transmission will be divided into 20 seconds and average data rate will be maintained. The host is having no advantage of sitting idle for 10 seconds.

• To overcome this problem, a token bucket algorithm is used. A token bucket algorithm allows bursty data transfers.

• A token bucket algorithm is a modification of leaky bucket in which leaky bucket contains tokens.

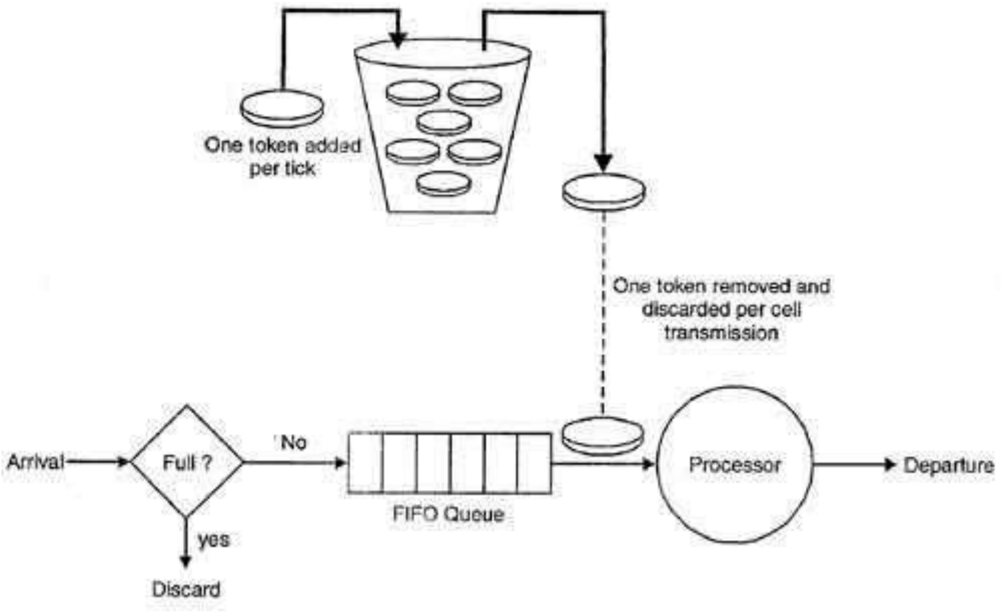
• In this algorithm, a token(s) are generated at every clock tick. For a packet to be transmitted, system must remove token(s) from the bucket.

• Thus, a token bucket algorithm allows idle hosts to accumulate credit for the future in form of tokens.

• For example, if a system generates 100 tokens in one clock tick and the host is idle for 100 ticks. The bucket will contain 10,000 tokens.

Now, if the host wants to send bursty data, it can consume all 10,000 tokens at once for sending 10,000 cells or bytes.

Thus a host can send bursty data as long as bucket is not empty.



Token bucket algorithm

Q.2.d. Enumerate on TCP header and working of TCP and differentiate TCP and UDP with frame format.

Ans .2.d. TCP (Transmission Control Protocol) is a standard that defines how to establish and maintain a network conversation via which application programs can exchange data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other.

TCP is a connection-oriented protocol, which means a connection is established and maintained until the application programs at each end have finished exchanging messages.

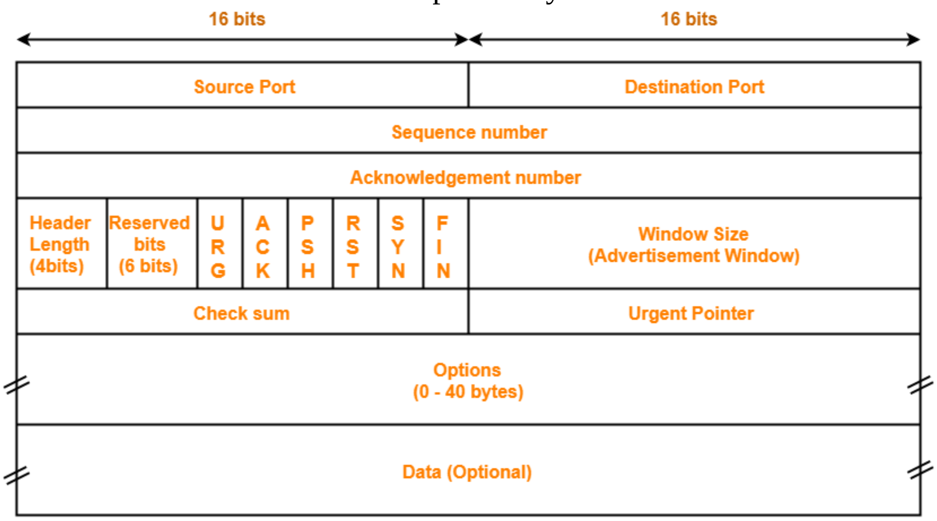
a. The application while sending the message to TCP, it arranges the message as a block of data.

b. The TCP divides this block into a number of smaller pieces for manageability. It then adds control information to each piece called TCP header. Now this piece of message along with TCP header forms a Segment.

c. Next, each segment is handed over to IP. The IP now adds extra control information to each segment called IP header to form an IP Datagram.
d. Each IP diagram is then presented to network access layer which then appends another header to form a Packet or a Frame.
e. The frame is then transmitted across the sub network to reach the Rooter.
f. The Rooter removes the frame header and checks the IP header to determine the destination address.
g. The IP module present in the router forwards the diagram to the specified network
h. Upon receiving the data gram, the receiver would remove one header and passes the remainder on to the next higher layer until the original user data is delivered to the application.

TCP Header Format

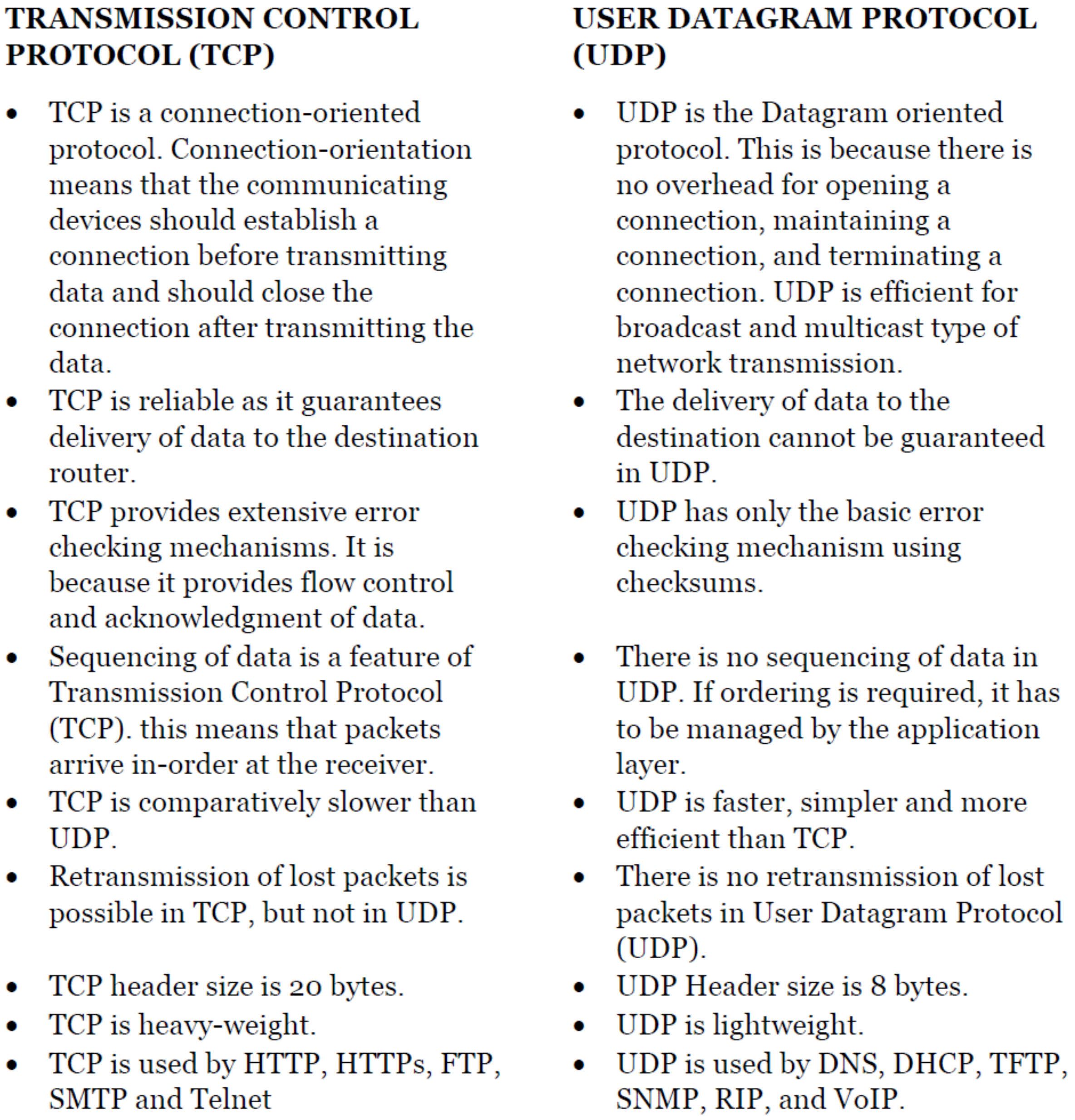
Each TCP header has ten required fields totaling 20 bytes (160 bits) in size. They can also optionally include an additional data section up to 40 bytes in size.



TCP Header

TCP headers appear in the following sequence:

1. Source TCP port number (2 bytes)
2. Destination TCP port number (2 bytes)
3. Sequence number (4 bytes)
4. Acknowledgment number (4 bytes)
5. TCP data offset (4 bits)
6. Reserved data (3 bits)
7. Control flags (up to 9 bits)
8. Window size (2 bytes)
9. TCP checksum (2 bytes)
10. Urgent pointer (2 bytes)
11. TCP optional data (0-40 bytes)



TRANSMISSION CONTROL PROTOCOL (TCP)	USER DATAGRAM PROTOCOL (UDP)
• TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	• UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission.
• TCP is reliable as it guarantees delivery of data to the destination router.	• The delivery of data to the destination cannot be guaranteed in UDP.
• TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data.	• UDP has only the basic error checking mechanism using checksums.
• Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in-order at the receiver.	• There is no sequencing of data in UDP. If ordering is required, it has to be managed by the application layer.
• TCP is comparatively slower than UDP.	• UDP is faster, simpler and more efficient than TCP.
• Retransmission of lost packets is possible in TCP, but not in UDP.	• There is no retransmission of lost packets in User Datagram Protocol (UDP).
• TCP header size is 20 bytes.	• UDP Header size is 8 bytes.
• TCP is heavy-weight.	• UDP is lightweight.
• TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet	• UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.

Q. 2. E. Elaborate about TELNET and its working procedure.

Ans. 2 e. Telnet is a tool that can be used to open a command line on a remote computer, typically a server.

Telnet is a system for opening a text-based connection between two computers. The term is sometimes said to be a shortened form of "terminal network."
Telnet is usually implemented purely in software, and you can find Telnet software (sometimes referred to as terminal emulator software) for all modern operating systems.

How Telnet Works?

To use Telnet, you need to know the address of the whose resources you want to use. Your client contacts the host using its Internet address. When you contact the host, the distant computer and your computer negotiate how they will communicate with each other. They decide which terminal emulation will be used.

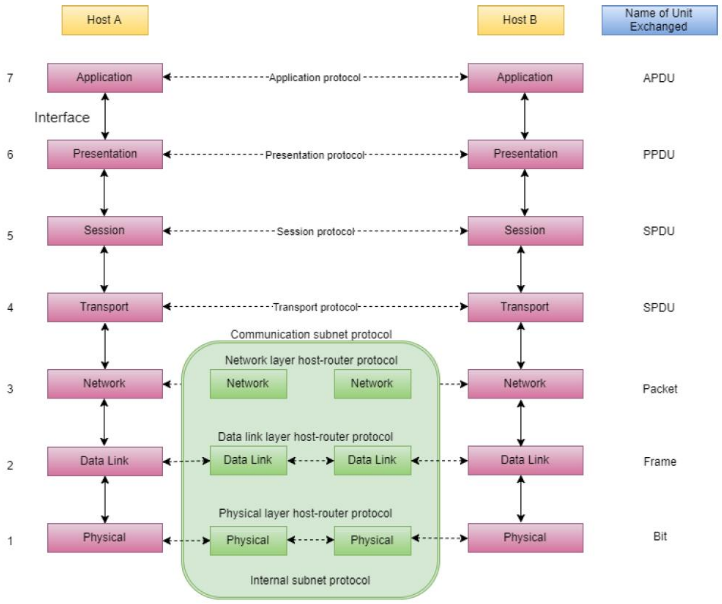
Telnet emulation determines how your keyboard will transmit information to the distant computer and how information will be displayed on your screen. For example, it determines how a back-space key will work. VT-100 (VT stands for virtual terminal) is the most common type of terminal emulation.

The Telnet protocol assumes that each end of the connecting – the client and the server – is a network Virtual Terminal (NVT). Each NVT has a virtual "printer" and "virtual" keyboard." The keyboard sends data from one NVT to the other. When you type text on your keyboard, you are using the NVT keyboard.

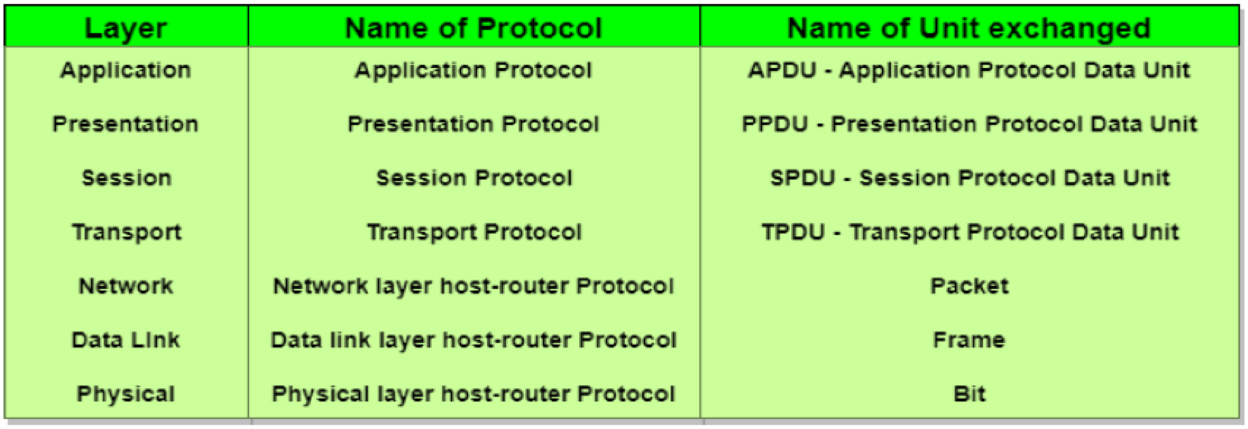
Because packets must go through many Internet router in each direction between your computer and the host, there may be a delay between the time you send a command and the time you see the results on your own computer screen.

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

Ans.3.a. OSI model is a layered framework for the design of network systems that allows communications between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.



✓ **Protocols used and the data unit exchanged by each layer of the OSI Model.**



Layer	Name of Protocol	Name of Unit exchanged
Application	Application Protocol	APDU - Application Protocol Data Unit
Presentation	Presentation Protocol	PPDU - Presentation Protocol Data Unit
Session	Session Protocol	SPDU - Session Protocol Data Unit
Transport	Transport Protocol	TPDU - Transport Protocol Data Unit
Network	Network layer host-router Protocol	Packet
Data Link	Data link layer host-router Protocol	Frame
Physical	Physical layer host-router Protocol	Bit

✓ Functions of Different Layers

Following are the functions performed by each layer of the OSI model.

OSI Model Layer 1: The Physical Layer

1. Physical Layer is the lowest layer of the OSI Model.

2. It activates, maintains and deactivates the physical connection.

3. It is responsible for transmission and reception of the unstructured raw data over network.

4. Voltages and data rates needed for transmission is defined in the physical layer.

5. It converts the digital/analog bits into electrical signal or optical signals.

6. Data encoding is also done in this layer.

OSI Model Layer 2: Data Link Layer

1. Data link layer synchronizes the information which is to be transmitted over the physical layer.

2. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.

3. Transmitting and receiving data frames sequentially is managed by this layer.

4. This layer sends and expects acknowledgements for frames received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.

5. This layer establishes a logical layer between two nodes and also manages the Frame traffic control over the network. It signals the transmitting node to stop, when the frame buffers are full.

OSI Model Layer 3: The Network Layer

1. Network Layer routes the signal through different channels from one node to other.

2. It acts as a network controller. It manages the Subnet traffic.

3. It decides by which route data should take.

4. It divides the outgoing messages into packets and assembles the incoming packets into messages for higher levels.

OSI Model Layer 4: Transport Layer

1. Transport Layer decides if data transmission should be on parallel path or single path.

2. Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer.

3. It receives messages from the Session layer above it, convert the message into smaller units and passes it on to the Network layer.

4. Transport layer can be very complex, depending upon the network requirements.

5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

OSI Model Layer 5: The Session Layer

1. Session Layer manages and synchronize the conversation between two different applications.

2. Transfer of data from source to destination session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

OSI Model Layer 6: The Presentation Layer

1. Presentation Layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data.

2. While receiving the data, presentation layer transforms the data to be ready for the application layer.

3. Languages(syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.

4. It performs Data compression, Data encryption, Data conversion etc.

OSI Model Layer 7: Application Layer

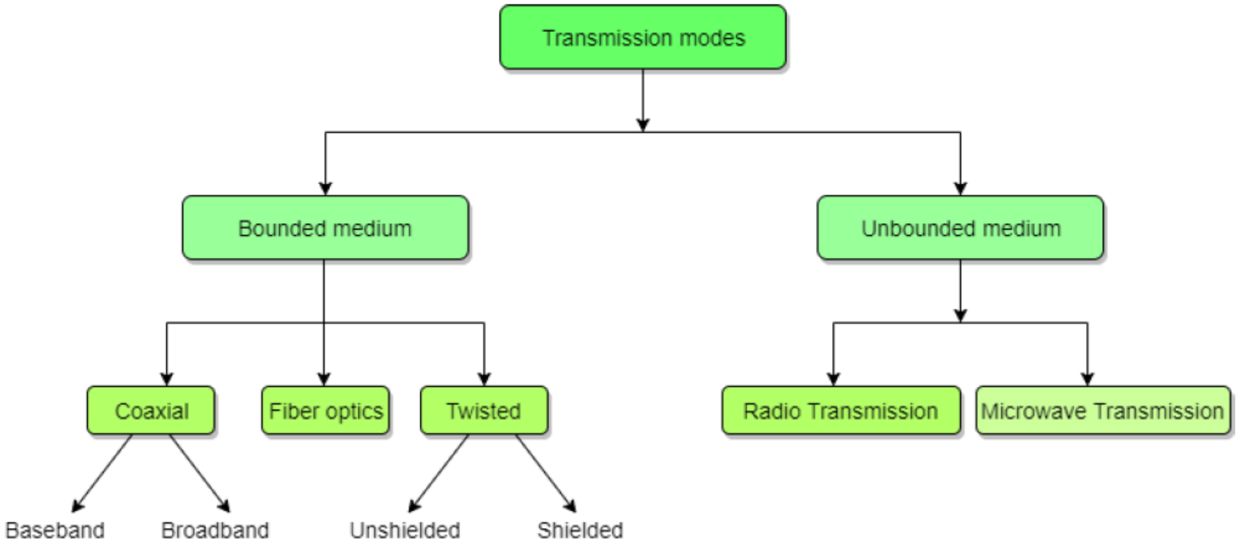
1. Application Layer is the topmost layer.

2. Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc are services provided by application layer.

3. This layer mainly holds application programs to act upon the received and to be sent data.

Q.3.b. Discuss the different physical layer transmission media.

Ans.3.b. Transmission medium is the means through which we send our data from one place to another. The first layer (physical layer) of Communication Networks OSI Seven-layer model is dedicated to the transmission media.



1. Guided Media:

It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

Features:

- High Speed
- Secure
- Used for comparatively shorter distances

There are 3 major types of Guided Media:

(i) Twisted Pair Cable –

It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:

1. **Unshielded Twisted Pair (UTP):**

   This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.

   Advantages:

   - Least expensive
   - Easy to install
   - High speed capacity

   Disadvantages:

   - Susceptible to external interference
   - Lower capacity and performance in comparison to STP
   - Short distance transmission due to attenuation

2. **Shielded Twisted Pair (STP):**

   This type of cable consists of a special jacket to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.

   Advantages:

- Better performance at a higher data rate in comparison to UTP
- Eliminates crosstalk
- Comparitively faster

Disadvantages:

- Comparitively difficult to install and manufacture
- More expensive
- Bulky

(ii) Coaxial Cable –

It has an outer plastic covering containing 2 parallel conductors each having a separate insulated protection cover. Coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.

Advantages:

- High Bandwidth
- Better noise Immunity
- Easy to install and expand
- Inexpensive

Disadvantages:

- Single cable failure can disrupt the entire network

(iii) Optical Fibre Cable –

It uses the concept of reflection of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for transmission of large volumes of data.

Advantages:

- Increased capacity and bandwidth
- Light weight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials

Disadvantages:

- Difficult to install and maintain
- High cost
- Fragile
- unidirectional, ie, will need another fibre, if we need bidirectional communication

2. Unguided Media:

It is also referred to as Wireless or Unbounded transmission media.No physical medium is required for the transmission of electromagnetic signals.

Features:

- Signal is broadcasted through air
- Less Secure
- Used for larger distances

There are 3 major types of Unguided Media:

(i) Radiowaves –
These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radiowaves for transmission.
Further Categorized as (i) Terrestrial and (ii) Satellite.

(ii) Microwaves –
It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

(iii) Infrared –
Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

Q4. A Discuss different carrier sense protocols. How are they different than collisions protocols?

Ans. Carrier Sense Multiple Access (CSMA) is a network protocol that listens to or senses network signals on the carrier/medium before transmitting any data. CSMA is implemented in Ethernet networks with more than one computer or network device attached to it. CSMA is part of the Media Access Control (MAC) protocol.

1. Carrier Sense Multiple Access with Collision Detection (CSMA/CD) –

In this method, a station monitors the medium after it sends a frame to see if the transmission was successful.If succcessful, the station is finished, if not, the frame is sent again.

Throughput and Efficiency – The throughput of CSMA/CD is much greater than pure or slotted ALOHA.

- For 1-persistent method throughput is 50% when G=1.
- For non-persistent method throughput can go upto 90%.

2. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) –

The basic idea behind CSMA/CA is that the station should be able to receive while transmitting to detect a collision from different stations. In wired networks, if a collision has occurred then the energy of received signal almost doubles and the station can sense the possibility of collision. In case of wireless networks, most of the energy is used for transmission and the energy of received signal increases by only 5-10% if collision occurs. It can't be used by station to sense collision. Therefore **CSMA/CA has been specially designed for wireless networks**.

Q.4.b. Write short notes on following:

1. Stop and Wait ARQ: Stop-and-wait ARQ, also referred to as alternating bit protocol, is a method in telecommunications to send information between two connected devices. It ensures

that information is not lost due to dropped packets and that packets are received in the correct order. It is the simplest automatic repeat- request (ARQ) mechanism. A stop-and-wait ARQ sender sends one frame at a time; it is a special case of the general sliding window protocol with transmit and receive window sizes equal to one and greater than one respectively. After sending each frame, the sender doesn't send any further frames until it receives an acknowledgement (ACK) signal. After receiving a valid frame, the receiver sends an ACK. If the ACK does not reach the sender before a certain time, known as the timeout, the sender sends the same frame again. The timeout countdown is reset after each frame transmission. The above behavior is a basic example of Stop-and-Wait. However, real-life implementations vary to address certain issues of design.

Typically, the transmitter adds a redundancy check number to the end of each frame. The receiver uses the redundancy check number to check for possible damage. If the receiver sees that the frame is good, it sends an ACK. If the receiver sees that the frame is damaged, the receiver discards it and does not send an ACK—pretending that the frame was completely lost, not merely damaged.

One problem is when the ACK sent by the receiver is damaged or lost. In this case, the sender doesn't receive the ACK, times out, and sends the frame again. Now the receiver has two copies of the same frame, and doesn't know if the second one is a duplicate frame or the next frame of the sequence carrying identical DATA

Another problem is when the transmission medium has such a long latency that the sender's timeout runs out before the frame reaches the receiver. In this case the sender resends the same packet. Eventually the receiver gets two copies of the same frame and sends an ACK for each one. The sender, waiting for a single ACK, receives two ACKs, which may cause problems if it assumes that the second ACK is for the next frame in the sequence.

2. Sliding Window Protocol:

Sliding window protocols are data link layer protocols for reliable and sequential delivery of data frames. The sliding window is also used in Transmission Control Protocol.

In this protocol, multiple frames can be sent by a sender at a time before receiving an acknowledgment from the receiver. The term sliding window refers to the imaginary boxes to hold frames. Sliding window method is also known as windowing.

Working Principle

In these protocols, the sender has a buffer called the sending window and the receiver has buffer called the receiving window.

The size of the sending window determines the sequence number of the outbound frames. If the sequence number of the frames is an n-bit field, then the range of sequence numbers that can be assigned is 0 to 2^n-1. Consequently, the size of the sending window is 2^n-1. Thus in order to accommodate a sending window size of 2^n-1, a n-bit sequence number is chosen.

The sequence numbers are numbered as modulo-n. For example, if the sending window size is 4, then the sequence numbers will be 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, and so on. The number of bits in the sequence number is 2 to generate the binary sequence 00, 01, 10, 11.

The size of the receiving window is the maximum number of frames that the receiver can accept at a time. It determines the maximum number of frames that the sender can send before receiving acknowledgment.

3 Go Back N ARQ:

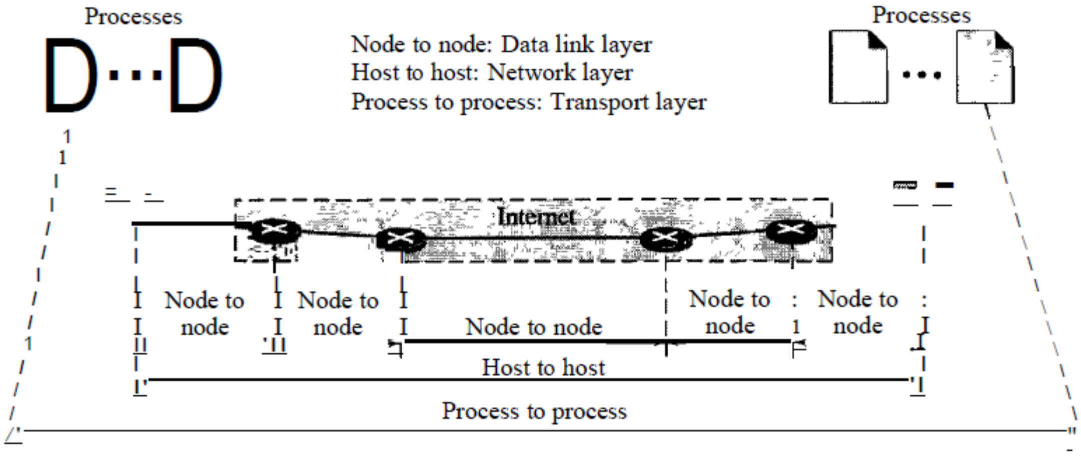
Go-Back-N ARQ is a specific instance of the automatic repeat request (ARQ) protocol, in which the sending process continues to send several frames specified by a *window size* even without receiving an acknowledgement (ACK) packet from the receiver. It is a special case of the general sliding window protocol with the transmit window size of N and receive window size of 1. It can transmit N frames to the peer before requiring an ACK.

The receiver process keeps track of the sequence number of the next frame it expects to receive and sends that number with every ACK it sends. The receiver will discard any frame that does not have the exact sequence number it expects (either a duplicate frame it already acknowledged, or an out-of-order frame it expects to receive later) and will resend an ACK for the last correct in-order frame. Once the sender has sent all of the frames in its *window*, it will detect that all of the frames since the first lost frame are *outstanding*, and will go back to the sequence number of the last ACK it received from the receiver process and fill its window starting with that frame and continue the process over again.

Go-Back-N ARQ is a more efficient use of a connection than Stop-and-wait ARQ, since unlike waiting for an acknowledgement for each packet, the connection is still being utilized as packets are being sent. In other words, during the time that would otherwise be spent waiting, more packets are being sent. However, this method also results in sending frames multiple times – if any frame was lost or damaged, or the ACK acknowledging them was lost or damaged, then that frame and all following frames in the window (even if they were received without error) will be re-sent. To avoid this, Selective Repeat ARQ can be used.

Q6.a. Enumerate how the transport layer unsure that the complete message arrives at the destination and in the proper order.

Ans 6.a. The transport layer is responsible for process-to-process delivery-the delivery of a packet, part of a message, from one process to another. Two processes communicate in a client/server relationship,



Client/Server Paradigm

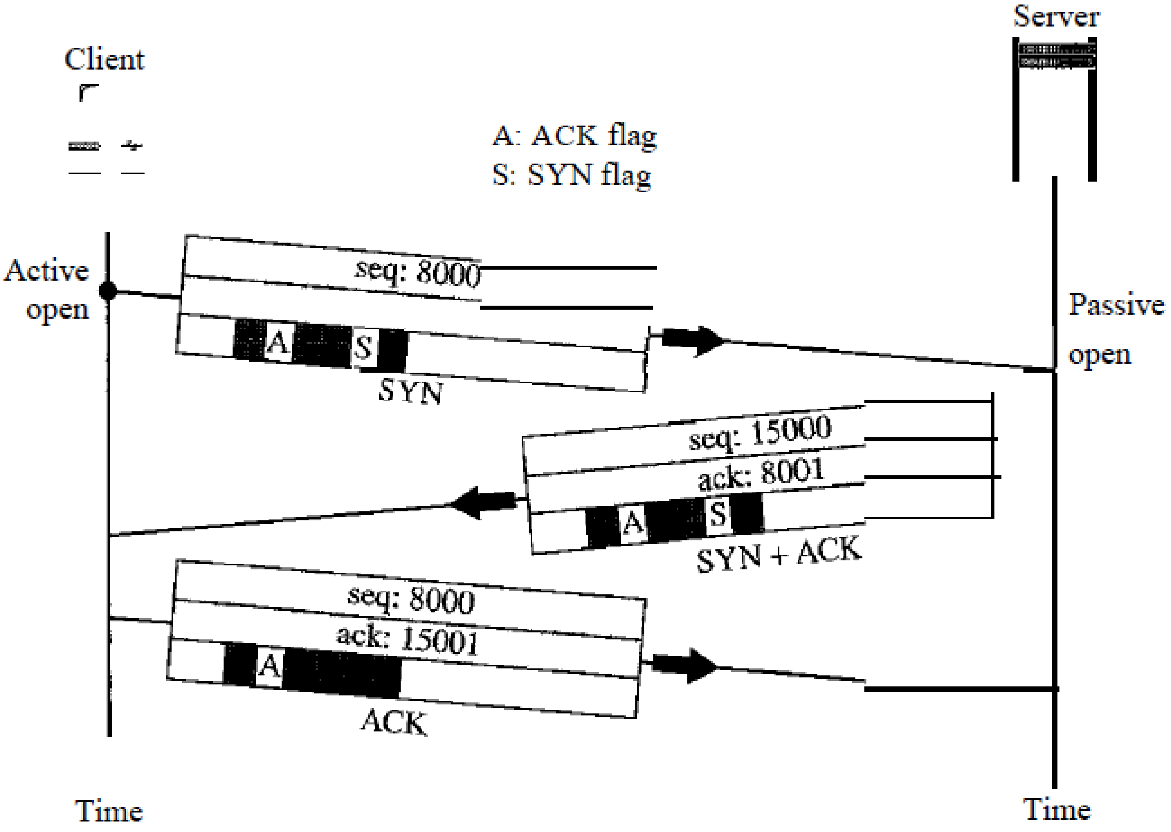
Although there are several ways to achieve process-to-process communication, the most common one is through the client/server paradigm. A process on the local host, called a client, needs services from a process usually on the remote host, called a server. Both processes (client and server) have the same name. For example, to get the day and time from a remote machine, we need a Daytime client process running on the local host and a Daytime server process running on a remote machine. Operating systems today support both multiuser and multiprogramming environments. A remote computer can run several server programs at the same time, just as local computers can run one or more client programs at the same time.

The transport layer service can be reliable or unreliable. If the application layer program needs reliability, we use a reliable transport layer protocol by implementing flow and error control at the transport layer. This means a slower and more complex service. On the other hand, if the application program does not need reliability because it uses its own flow and error control mechanism or it needs fast service or the nature of the service does not demand flow and error control (real-time applications), then an unreliable protocol can be used.
In the Internet, there are three common different transport layer protocols, as we have already mentioned. UDP is connectionless and unreliable; TCP and SCTP are connection oriented and reliable. These three can respond to the demands of the application layer programs.

b. Explain the three way handshaking protocol to establish the transport level connection.

Ans b. Three-Way Handshaking The connection establishment in TCP is called three way handshaking. In our example, an application program, called the client, wants to make a connection with another application program, called the server, using TCP as the transport layer protocol.
The process starts with the server. The server program tells its TCP that it is ready to accept a connection. This is called a request for a *passive open.* Although the server TCP is ready to accept any connection from any machine in the world, it cannot make the connection itself. The client program issues a request for an *active open.* A client that wishes to connect to an open

server tells its TCP that it needs to be connected to that particular server. TCP can now start the three-way handshaking process as shown in Figure



The three steps in this phase are as follows.

1. The client sends the first segment, a SYN segment, in which only the SYN flag is set. This segment is for synchronization of sequence numbers. It consumes one sequence number. When the data transfer starts, the sequence number is incremented by 1. We can say that the SYN segment carries no real data, but we can think of it as containing 1 imaginary byte.
2. The server sends the second segment, a SYN +ACK segment, with 2 flag bits set: SYN and ACK. This segment has a dual purpose. It is a SYN segment for communication in the other direction and serves as the acknowledgment for the SYN segment. It consumes one sequence number.
3. The client sends the third segment. This is just an ACK segment. It acknowledges the receipt of the second segment with the ACK flag and acknowledgment number field. Note that the sequence number in this segment is the same as the one in the SYN segment; the ACK segment does not consume any sequence numbers.

7. Attempt any *one* part of the following: 10 x 1 = 10

(a) Write short notes on any two of the following:

i. DNS in the internet

ii. Voice Over IP
iii. File Transfer Protocol

Anw 7.a.i. DNS: DNS is a host name to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.

Requirement

Every host is identified by the IP address but remembering numbers is very difficult for the people and also the IP addresses are not static therefore a mapping is required to change the domain name to IP address. So DNS is used to convert the domain name of the websites to their numerical IP address.

Domain:

There are various kinds of DOMAIN:

1. Generic domain: .com (commercial), .edu (educational), .mil (military), .org (non- profit organization) .net(similar to commercial) all these are generic domain.
2. Country domain .in (india), .us .uk
3. Inverse domain if we want to know what is the domain name of the website. Ip to domain name mapping.

ii. Voice Over IP: Voice over Internet Protocol (VoIP), is a technology that allowing you to make voice calls over a broadband Internet connection instead of a analog (regular) phone line. Some VoIP services allow you to call people using the same service, but others may allow you to call anyone. They can have a telephone number – including local, long distance, mobile, and international numbers or not. Some VoIP services only work over your computer or a special VoIP phone while other services allow you to use a traditional phone connected to a VoIP adapter.

Advantages of VoIP –

- Some VoIP services offer features and services that are not available with a traditional phone, or are available but only for an additional fee.
- Paying for both a broadband connection and a traditional telephone line can be avoided.
- Smoother connection than an analog signal can be provided.

Disadvantages of VoIP –

- Some VoIP services don’t work during power outages and the service provider may not offer backup power.
- Not all VoIP services connect directly to emergency services through emergency service numbers.
- VoIP providers may or may not offer directory assistance.

iii. File Transfer Protocol is a standard network protocol used to exchange and manipulate files over a TCP/IP-based network, such as the Internet. FTP is built on client-server architecture and utilizes separate control and data connections between the client and server applications. FTP is used with user-based password authentication or with anonymous user access. Applications were originally interactive command-line tools with standardized command syntax, but graphical user interfaces have been developed for all desktop operating systems in use today. The Trivial File Transfer Protocol (TFTP) is a similar, but simplified, not interoperable, and unauthenticated version of FTP.

Numerous FTP servers all over the world allow users anywhere on the Internet to log in and down-load files placed on them. The main competitor for FTP is HTTP (Hyper Text Transfer Protocol) and the day is not very far when sites would run HTTP servers instead of the FTP servers. It is so because HTTP servers can do whatever FTP server can do and do it more efficiently.

b. If an organization has 1000 of devices then to check all devices, one by one everyday, are working properly or not is a hectic task. To ease these up, Simple Network Management Protocol (SNMP) is used.

Simple Network Management Protocol (SNMP) –
SNMP is an application layer protocol which uses UDP port number 161/162.SNMP is used to monitor network, detect network faults and sometimes even used to configure remote devices.

SNMP components –

There are 3 components of SNMP:

SNMP Manager –
It is a centralized system used to monitor network.It is also known as Network Management Station (NMS)
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.
Management Information Base –
MIB consists of information of resources that are to be managed. These information is organized hierarchically. It consists of objects instances which are essentially variables.

SNMP messages –
Different variables are:

GetRequest –
SNMP manager sends this message to request data from SNMP agent. It is simply used to retrieve data from SNMP agent. In response to this, SNMP agent responds with requested value through response message.
GetNextRequest –
This message can be sent to discover what data is available on a SNMP agent. The SNMP manager can request for data continously until no more data is left. In this way, SNMP manager can take knowledge of all the available data on SNMP agent.
GetBulkRequest –
This message is used to retrieve large data at once by the SNMP manager from SNMP agent. It is introduced in SNMPv2c.

SetRequest –
It is used by SNMP manager to set the value of an object instance on the SNMP agent.
Response –
It is a message send from agent upon a request from manager. When sent in response to Get messages, it will contain the data requested. When sent in response to Set message, it will contain the newly set value as confirmation that the value has been set.
Trap –
These are the message send by the agent without being requested by the manager. It is sent when a fault has occurred.
InformRequest –
It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to set trap continuously until it receives an Inform message. It is same as trap but adds an acknowledgement that traps doesn't provide.

SNMP versions –
There are 3 versions of SNMP:

1. **SNMPv1 –**
   It uses community strings for authentication and use UDP only.
2. **SNMPv2c –**
   It uses community strings for authentication. It uses UDP but can be configured to use TCP.
3. **SNMPv3 –**
   It uses Hash based MAC with MD5 or SHA for authentication and DES-56 for privacy.This version uses TCP. Therefore, conclusion is the higher the version of SNMP, more secure it will be.