CN MODULE-4

P.Rajeshwari | K.Lalitha

PART-B

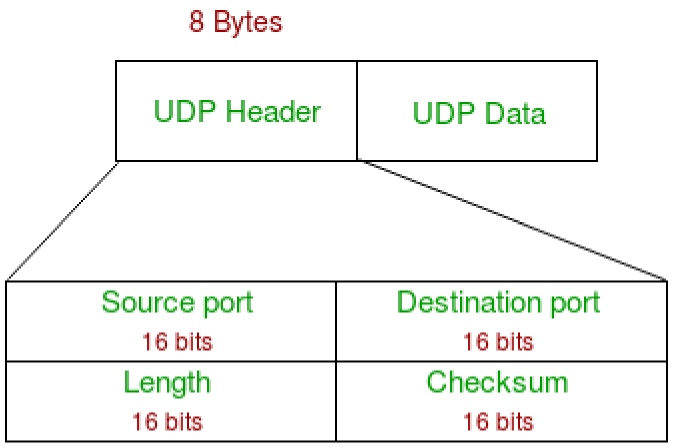
1.)Explain the real transport protocol of UDP and how will you calculate checksum in UDP.?

A.)**User Datagram Protocol (UDP)** is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as UDP/IP suite. Unlike TCP, it is an **unreliable and connectionless protocol.** So, there is no need to establish a connection prior to data transfer.

Though Transmission Control Protocol (TCP) is the dominant transport layer protocol used with most of the Internet services, it provides assured delivery, reliability, and much more but all these services cost us additional overhead and latency.

UDP Header –

UDP header is an **8-bytes** fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. The first 8 Bytes contain all necessary header information and the remaining part consists of data. UDP port number fields are each 16 bits long, therefore the range for port numbers is defined from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or processes.



HOW WILL YOU CALCULATE CHECKSUM IN UDP:

https://www.ques10.com/p/10930/how-is-checksum-computed-in-udp-1/

2.)Show neatly the TCP segment format and describe each of it.?

A.)https://www.tutorialspoint.com/what-is-the-tcp-segment-header

REFER THIS LINK

3.)List out the network performance characteristics.?

A.)Performance of a network pertains to the measure of service quality of a network as perceived by the user. There are different ways to measure the performance of a network, depending upon the nature and design of the network. The characteristics that measure the performance of a network are :

- Bandwidth
- Throughput
- Latency (Delay)

- Bandwidth – Delay Product
- Jitter

BANDWIDTH

One of the most essential conditions of a website's performance is the amount of bandwidth allocated to the network. Bandwidth determines how rapidly the web server is able to upload the requested information. While there are different factors to consider with respect to a site's performance, bandwidth is every now and again the restricting element.

Bandwidth is characterised as the measure of data or information that can be transmitted in a fixed measure of time. The term can be used in two different contexts with two distinctive estimating values.

THROUGHPUT

Throughput is the number of messages successfully transmitted per unit time. It is controlled by available bandwidth, the available signal-to-noise ratio and hardware limitations. The maximum throughput of a network may be consequently higher than the actual throughput achieved in everyday consumption. The terms 'throughput' and 'bandwidth' are often thought of as the same, yet they are different. Bandwidth is the potential measurement of a link, whereas throughput is an actual measurement of how fast we can send data.

LATENCY

In a network, during the process of data communication, latency(also known as delay) is defined as the total time taken for a complete message to arrive at the destination, starting with the time when the first bit of the message is sent out from the source and ending with the time when the last bit of the message is delivered at the destination. The network connections where small delays occur are called “Low-Latency-Networks” and the network connections which suffer from long delays are known as “High-Latency-Networks”.

BANDWIDTH – DELAY PRODUCT

Bandwidth and delay are two performance measurements of a link. However, what is significant in data communications is the product of the two, the bandwidth-delay product.

JITTER

Jitter is another performance issue related to delay. In technical terms, jitter is a “packet delay variance”. It can simply mean that jitter is considered as a problem when different packets of data face different delays in a network and the data at the receiver application is time-sensitive, i.e. audio or video data. Jitter is measured in milliseconds(ms). It is defined as an interference in the normal order of sending data packets. For example: if the delay for the first packet is 10 ms, for the second is 35 ms, and for the third is 50 ms, then the real-time destination application that uses the packets experiences jitter.

4.)Illustrate the adaptive retransmission policy in detail.?

A.)**Doubt**

5.)Show the TCP connection establishment and termination using timeline diagram. ?

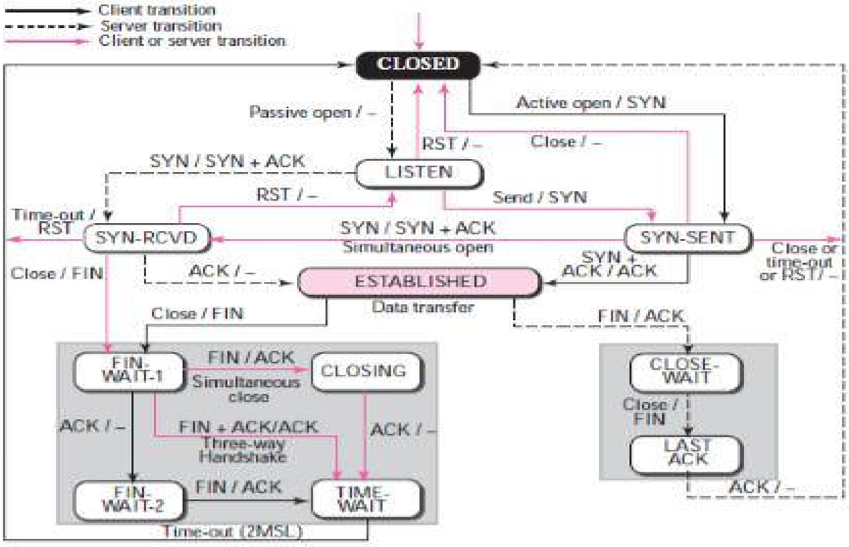
A.)https://www.vskills.in/certification/tutorial/tcp-connection-establish-and-terminate/

6.)Explain the three way handshake protocol to establish the transport level connection.?

A.)https://www.geeksforgeeks.org/tcp-3-way-handshake-process/

7.)Design TCP state transition diagrams and describe each of them.

A.)To keep track of all the different events happening during connection establishment, connection termination, and data transfer, TCP is specified as the finite state machine shown in Figure.

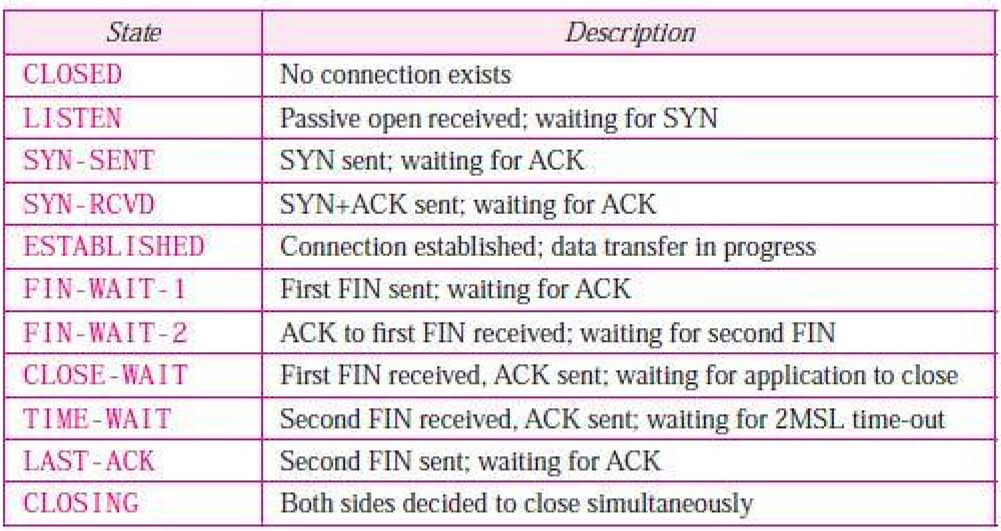


The figure shows the two FSMs used by the TCP client and server combined in one diagram. The ovals represent the states. The transition from one state to another is shown using directed lines.

The dotted black lines in the figure represent the transition that a server normally goes through; the solid black lines show the transitions that a client normally goes through.

The state marked as ESTABLISHED in the FSM is in fact two different sets of states that the client and server undergo to transfer data.

The states for TCP are as follows:



State	*Description*
CLOSED	No connection exists
LISTEN	Passive open received; waiting for SYN
SYN-SENT	SYN sent; waiting for ACK
SYN-RCVD	SYN+ACK sent; waiting for ACK
ESTABLISHED	Connection established; data transfer in progress
FIN-WAIT-1	First FIN sent; waiting for ACK
FIN-WAIT-2	ACK to first FIN received; waiting for second FIN
CLOSE-WAIT	First FIN received, ACK sent; waiting for application to close
TIME-WAIT	Second FIN received, ACK sent; waiting for 2MSL time-out
LAST-ACK	Second FIN sent; waiting for ACK
CLOSING	Both sides decided to close simultaneously

8)Explain a detailed note on connection establishment.

To make the transport services reliable, TCP hosts must establish a connection-oriented session with one another. Connection establishment is performed by using the three-way handshake mechanism. A three-way handshake synchronises both ends of a network by enabling both sides to agree upon original sequence numbers.

This mechanism also provides that both sides are ready to transmit data and learn that the other side is available to communicate. This is essential so that packets are not shared or retransmitted during session establishment or after session termination. Each host randomly selects a sequence number used to track bytes within the stream it is sending and receiving.

9)Discuss about the TCP sliding window algorithm for flow control.

A.)The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol)In this technique, each frame is sent from the sequence number. The sequence numbers are used to find the missing data in the receiver end. The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.

Types of Sliding Window Protocol

Sliding window protocol has two types:

1. Go-Back-N ARQ
2. Selective Repeat ARQ

Go-Back-N ARQ

Go-Back-N ARQ protocol is also known as Go-Back-N Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. In this, if any frame is corrupted or lost, all subsequent frames have to be sent again.

Selective Repeat ARQ

Selective Repeat ARQ is also known as the Selective Repeat Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. The Go-back-N ARQ protocol works well if it has fewer errors. But if there is a lot of error in the frame, lots of bandwidth loss in sending the frames again. So, we use the Selective Repeat ARQ protocol. In this protocol, the size of the sender window is always equal to the size of the receiver window. The size of the sliding window is always greater than 1.

10)Summarise all congestion control algorithms and describe how it works.

Congestion causes choking of the communication medium. When too many packets are displayed in a method of the subnet, the subnet's performance degrades. Hence, a network's communication channel is called congested if packets are traversing the path and experience delays mainly over the path's propagation delay.

Leaky Bucket

The leaky bucket algorithm discovers its use in the context of network traffic shaping or rate-limiting. The algorithm allows controlling the rate at which a record is injected into a network and managing burstiness in the data rate.

In this algorithm, a bucket with a volume of, say, b bytes and a hole in the Notes bottom is considered. If the bucket is null, it means b bytes are available as storage. A packet with a size smaller than b bytes arrives at the bucket and will forward it. If the packet's size increases by more than b bytes, it will either be discarded or queued. It is also considered that the bucket leaks through the hole in its bottom at a constant rate of r bytes per second.

The outflow is considered constant when there is any packet in the bucket and zero when it is empty. This defines that if data flows into the bucket faster than data flows out through the hole, the bucket overflows.

Token Bucket Algorithm

It is a control algorithm that indicates when traffic should be sent. This order comes based on the display of tokens in the bucket. The bucket contains tokens. Each of the tokens defines a packet of predetermined size. Tokens in the bucket are deleted for the ability to share a packet.

11)Illustrate leaky bucket and token bucket algorithm.

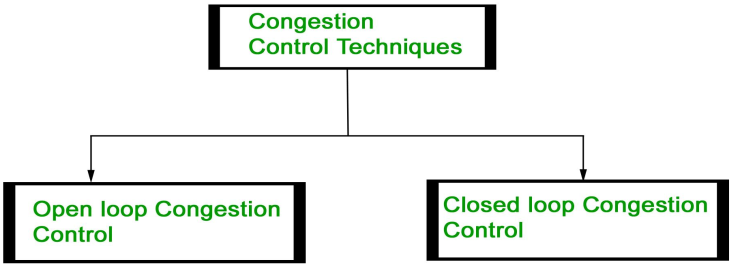
A.) refer part-b Q 10

12)Compare & Contrast UDP & TCP with suitable example.

A.)https://www.geeksforgeeks.org/differences-between-tcp-and-udp/

13)Explain congestion avoidance techniques in detail.

A.)Congestion control refers to the techniques used to control or prevent congestion. Congestion control techniques can be broadly classified into two categories:


Congestion Control Techniques
Open loop Congestion Control
Closed loop Congestion Control

Open Loop Congestion Control

Open loop congestion control policies are applied to prevent congestion before it happens. The congestion control is handled either by the source or the destination.

Policies adopted by open loop congestion control –

1.)Retransmission Policy

2.)Window policy

3.)Acknowledgment policy

4.)Discarding policy

5.)Admission policy

Closed Loop Congestion Control

Closed loop congestion control techniques are used to treat or alleviate congestion after it happens. Several techniques are used by different protocols; some of them are:

1.)Backpressure

2.) Choke Packet Technique

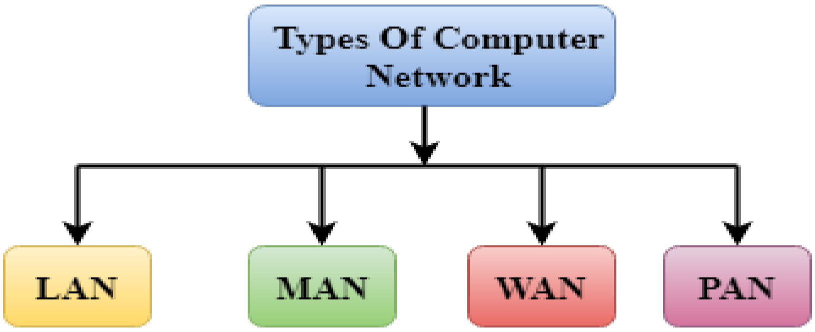
3.) Implicit Signalling

4.) Explicit Signalling

14)List major types of networks and give a brief note on each of them.

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

A computer network can be categorised by their size. A computer network is mainly of four types:



- LAN(Local Area Network)
- PAN(Personal Area Network)
- MAN(Metropolitan Area Network)
- WAN(Wide Area Network)

LAN(Local Area Network)

- Local Area Network is a group of computers connected to each other in a small area such as a building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.

PAN(Personal Area Network)

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 metres.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.

MAN(Metropolitan Area Network)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.

WAN(Wide Area Network)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite a bigger network than the LAN.

15)Illustrate data units at different layers of the TCP / IP protocol suite.

The data unit created at the application layer is called a message At the transport layer the data unit created is called either a segment or an user datagram At the network layer the data unit created is called the datagram At the data link layer the datagram is encapsulated in to a frame and finally transmitted as signals along the transmission media.

Different layers of the TCP / IP protocol suite are:

1.physical layer – stream of bits

2.data link layer - frame

3.network layer - datagram

4.transport layer - segment

5.application layer. –message

16)Discuss in detail about the connection establishment and release in TCP.

A.)To make the transport services reliable, TCP hosts must establish a connection-oriented session with one another. Connection establishment is performed by using the three-way handshake mechanism. A three-way handshake synchronises both ends of a network by enabling both sides to agree upon original sequence numbers.This mechanism also provides that both sides are ready to transmit data and learn that the other side is available to communicate. This is essential so that packets are not shared or retransmitted during session establishment or after session termination. Each host randomly selects a sequence number used to track bytes within the stream it is sending and receiving.

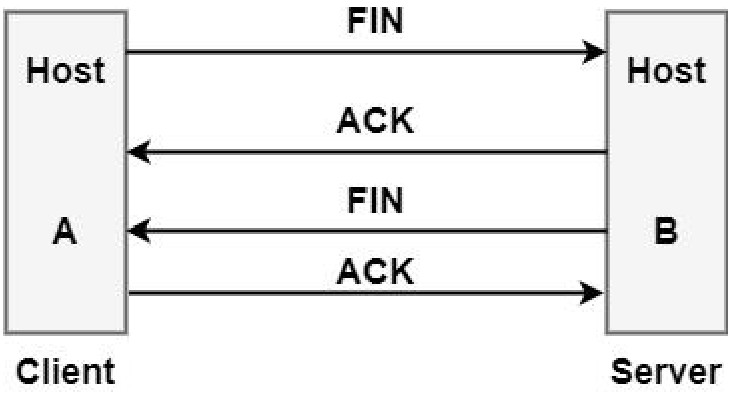
Connection Termination Protocol (Connection Release)

While it creates three segments to establish a connection, it takes four segments to terminate a connection. During a TCP connection is full-duplex (that is, data flows in each direction independently of the other direction), each direction should be shut down alone.

The termination procedure for each host is shown in the figure. The rule is that either end can share a FIN when it has finished sending data.

When a TCP receives a FIN, it should notify the application that the other end has terminated that data flow direction. The sending of a FIN is usually the result of the application issuing a close.

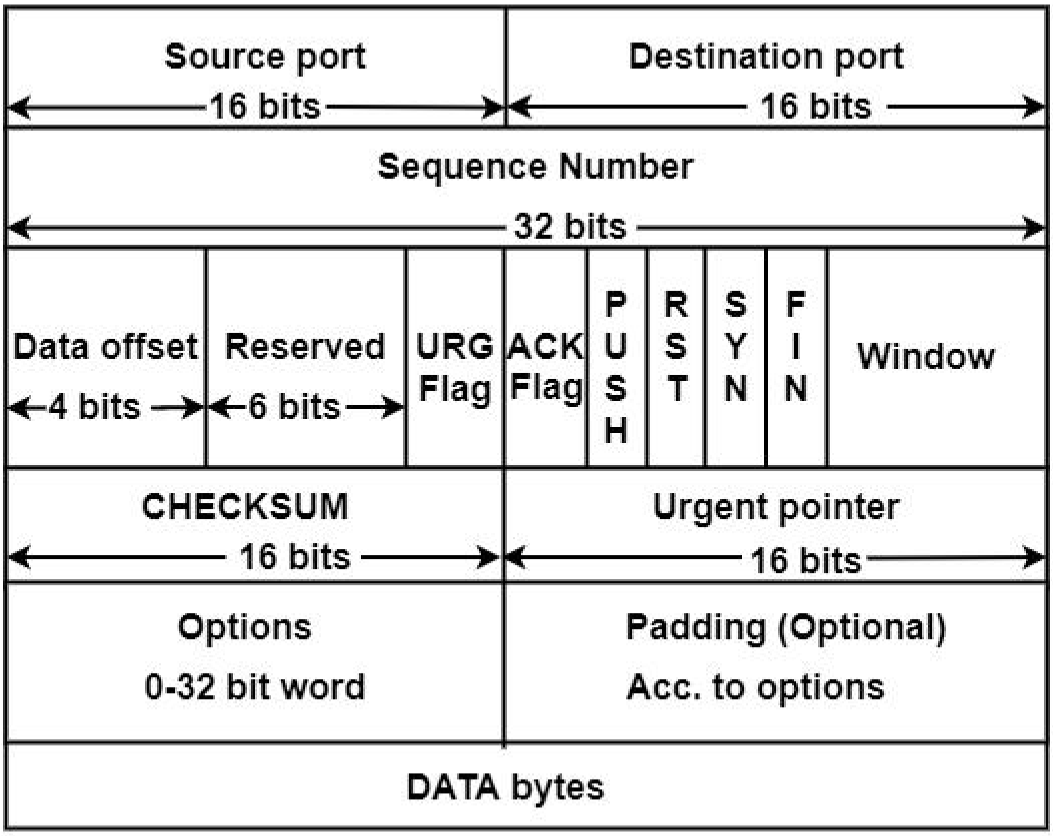
The receipt of a FIN only means that there will be no more data flowing in that direction. A TCP can send data after receiving a FIN. The end that first issues the close (example, send the first FIN) executes the active close. The other end (that receives this FIN) manages the passive close.



TCP Termination

17)Draw and explain each field in the TCP Segment header.

Every TCP segment consists of a 20 byte fixed format header. Header options may follow the fixed header. With a header so that it can tag up to 65535 data bytes.



TCP Segment Header

Source Port: It is a 16-bit source port number used by the receiver to reply.

Destination Port:It is a 16-bit destination port number.

Sequence Number: The sequence number of the first data byte in this segment. During the SYN Control bit is set, and the sequence number is n, and the first data byte is n + 1.
Acknowledgement Number: If the ACK control bit is set, this field contains the next number that the receiver expects to receive.
Data Offset: The several 32-bit words in the TCP header shows from where the user data begins.
Reserved (6 bit): It is reserved for future use.
URG: It indicates an urgent pointer field that data type is urgent or not.
ACK: It indicates that the acknowledgement field in a segment is significant, as discussed early.
PUSH: The PUSH flag is set or reset according to a data type that is sent immediately or not.

RST: It Resets the connection.
SYN: It synchronises the sequence number.
FIN: This indicates no more data from the sender.
Window: It is used in Acknowledgement segment. It specifies the number of data bytes, beginning with the one indicated in the acknowledgement number field that the receiver is ready to accept.
Checksum: It is used for error detection.
Padding: Options in each may vary in size, and it may be necessary to "pad" the TCP header with zeros so that the segment ends on a 32-bit word boundary as per the standard.
Data: Although in some cases like acknowledgement segments with no data in the reverse direction, the variable-length field carries the application data from sender to receiver. This field, connected with the TCP header fields, constitute a TCP segment.

18)Explain leaky bucket and token bucket algorithms.

refer part-b Q 10

19)Explain in detail about transport layer protocols

A.) The transport layer is represented by two protocols: TCP and UDP.The IP protocol in the network layer delivers a datagram from a source host to the destination host.

UDP

- UDP stands for **User Datagram Protocol**.
- UDP is a simple protocol and it provides nonsequenced transport functionality.
- UDP is a connectionless protocol.
- This type of protocol is used when reliability and security are less important than speed and size.

- UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.
- The packet produced by the UDP protocol is known as a user datagram.

TCP

- TCP stands for Transmission Control Protocol.
- It provides full transport layer services to applications.
- It is a connection-oriented protocol that means the connection established between both ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.

20)Explain the services provided by the transport layer?

A.)The services provided by the transport layer are similar to those of the data link layer. The data link layer provides the services within a single network while the transport layer provides the services across an internetwork made up of many networks. The data link layer controls the physical layer while the transport layer controls all the lower layers.

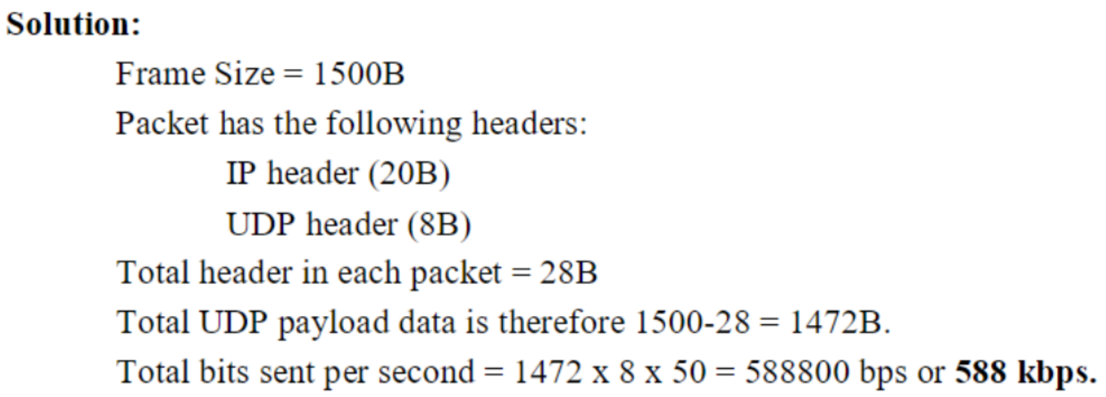
The services provided by the transport layer protocols can be divided into five categories:

- **End-to-end delivery**
- **Addressing**
- **Reliable delivery**
- **Flow control**
- **Multiplexing**

PART-A

1.)Assume An end system sends 50 packets for second using UDP over a full duplex mode 100 Mbps Ethernet LAN Connection. Each packet consists of 1500 Bytes of the Ethernet frame payload data. What is the throughput when measured at UDP protocol?

A.)



Solution:

Frame Size = 1500B

Packet has the following headers:

IP header (20B)

UDP header (8B)

Total header in each packet = 28B

Total UDP payload data is therefore 1500-28 = 1472B.

Total bits sent per second = 1472 x 8 x 50 = 588800 bps or **588 kbps.**

2.)Assume each packet has typical TCP and IP headers each 20bytes long. If we have three computers, A, B and C. The link between A and B has an MTU of 3000 bytes, while the link between B and C has an MTU of 1000 bytes. Consider the case where a packet needs to be sent from A to C that has a size of 3000 bytes (including headers). How many fragments will we have from B to C, and how much data will be in each fragment (i.e. excluding headers). (all connections are assumed to be Ethernet)

A.)

3.)Design a TCP connection is using a window size of 12000 bytes and the previous acknowledgement remembrance number was 22001.It receives a segment with

acknowledgment number 24001 and window size advertisement of 12000. Design a diagram to show the situation of the window before and after.

A.)

4.)Organise a client that uses UDP to send data to a server. The data are 15 bytes. Calculate the efficiency of this transmission at the UDP level (ratio of useful bytes to total bytes).

A.) Data are 15 bytes, length of UDP header is 8 bytes, so the ratio is

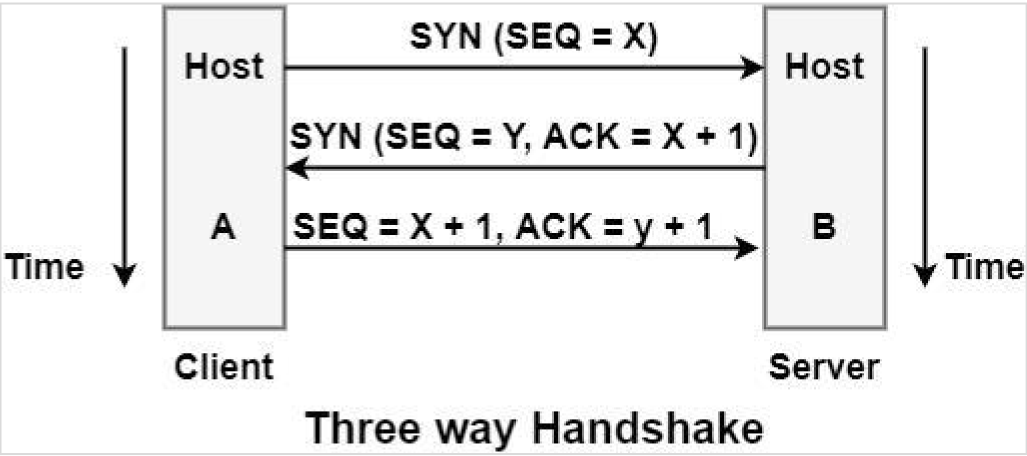
15/ 15+8 = 15/23.

5.)Discuss in detail about the connection establishment and release in TCP.

A.) To make the transport services reliable, TCP hosts must establish a connection-oriented session with one another. Connection establishment is performed by using the three-way handshake mechanism. A three-way handshake synchronises both ends of a network by enabling both sides to agree upon original sequence numbers.

This mechanism also provides that both sides are ready to transmit data and learn that the other side is available to communicate. This is essential so that packets are not shared or retransmitted during session establishment or after session termination. Each host randomly selects a sequence number used to track bytes within the stream it is sending and receiving.

The three-way handshake proceeds in the manner shown in the figure below –



The requesting end (Host A) sends an SYN segment determining the server's port number that the client needs to connect to and its initial sequence number (x).

The server (Host B) acknowledges its own SYN segment, including the servers initial sequence number (y). The server also responds to the client SYN by accepting the sender's SYN plus one (X + 1).

An SYN consumes one sequence number. The client should acknowledge this SYN from the server by accepting the server's SEQ plus one (SEQ = x + 1, ACK = y + 1). This is how a TCP connection is settled.

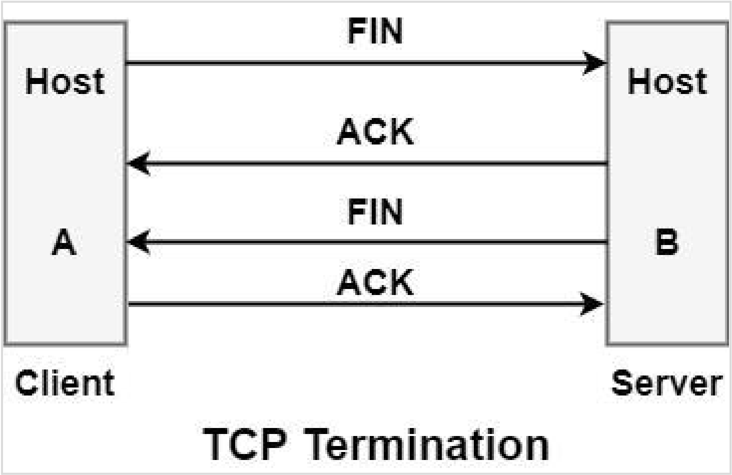
Connection Termination Protocol (Connection Release)

While it creates three segments to establish a connection, it takes four segments to terminate a connection. While a TCP connection is full-duplex (that is, data flows in each direction independently of the other direction), each direction should be shut down alone.

The termination procedure for each host is shown in the figure. The rule is that either end can share a FIN when it has finished sending data.

When a TCP receives a FIN, it should notify the application that the other end has terminated that data flow direction. The sending of a FIN is usually the result of the application issuing a close.

The receipt of a FIN only means that there will be no more data flowing in that direction. A TCP can send data after receiving a FIN. The end that first issues the close (example, send the first FIN) executes the active close. The other end (that receives this FIN) manages the passive close.



6.)Describe in detail about TCP segment header and connection Establishment

A,)refer part -B 17

7.)a) Explain the Services of Transport layer. b) Explain leaky bucket and token bucket algorithms

A.)

a.)https://www.tutorialspoint.com/what-are-the-services-provided-by-the-transport-layer

b.)refer part-b q-9

8.)Draw and explain each field in the TCP Segment header.

A.)refer part-b 17