UNIT - IV

TRANSPORT LAYER

M. KUMAR
ASST. PROFESSOR
DEPT OF ECE

INTRODUCTION

DEFINITION: Define Transport layer? (or) what is meant by Transport layer?

A Transport layer protocol provides for logical communication b/w application processes running on different hosts. (local host to other remote host)

Logical Communication, communicating application processes not physically connected to each other from the applications "viewpoint".

All Transport layer protocols provide an application Multiplexing / demultiplexing Service.

To perform "peer-to-peer" communication, with remote transport entity.

TRANSPORT LAYER FUNCTIONS: What are the functions of transport layer? (or) List the Advantages of transport layer

1. It breaks messages into packets.
2. It performs error recovery, not adequately error free
3. Flow control if not done adequately at N/w layer.
4. Responsible for setting up and releasing connections across the N/w.

Data link layer → Responsible for delivery of frames b/w two neighbouring nodes over a link (node to node delivery)

N/w layer: host-to-host delivery, delivery of datagrams b/w two hosts.

Transport layer: process-to-process delivery, delivery of packet, part of a message one process to another.

DIAGRAM OF DATA DELIVERY:

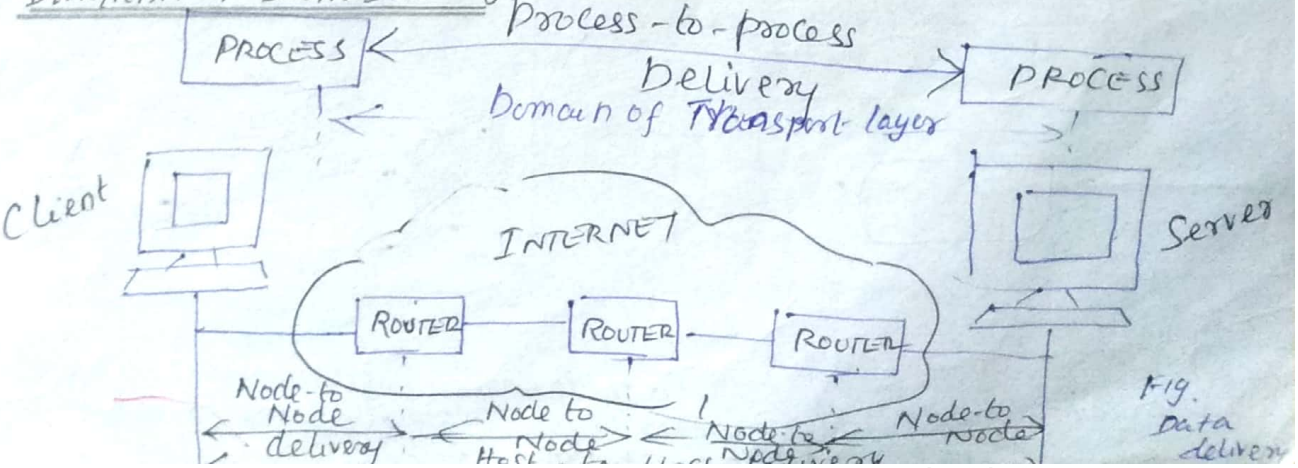


Fig. Data delivery

Client Server paradigm is used for process-to-process Communication.

A process on local machine (host) → client needs services from a process usually on the remote host called server.

Parameters used for Communication,

1. Local Host
2. Local process
3. Remote host
4. Remote process.

Define Transport layer protocol? (or) Explain briefly about transport layer protocols?

TRASPORT LAYER PROTOCOLS:

DEFINITION: TCP/IP protocol uses a transport layer protocol either a modification or a combination of some of these protocols.

1. SIMPLE PROTOCOL:

1st protocol is a simple connectionless protocol with neither flow nor error control.

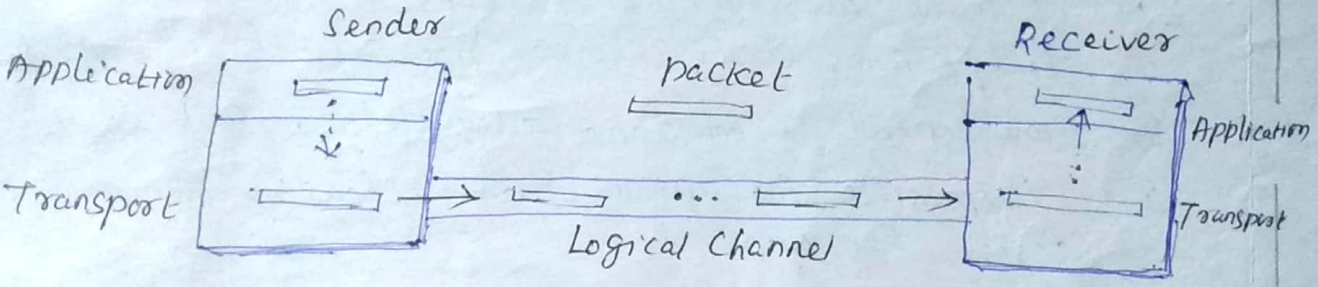


Fig: Simple protocol

Transport layer at sender gets a message from its application layer, packet out of it, and sends the packet.

Transport layer of the sender & receiver provide transmission services for their application layer.

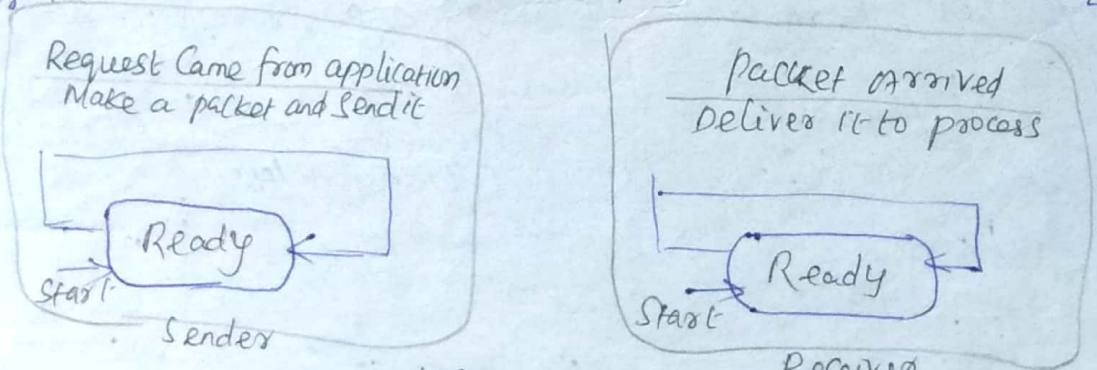


Fig. FSMs for the Simple protocol

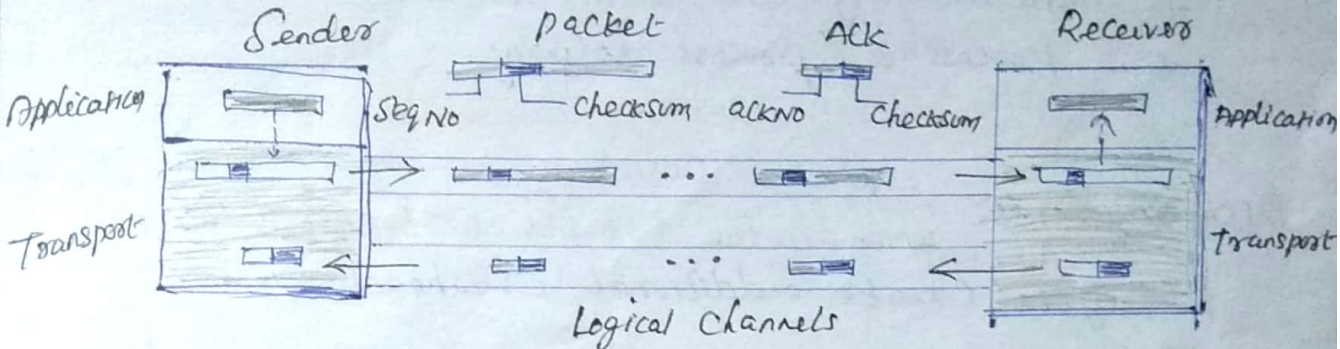
FSM [Finite State Machine]: Each transport layer (Sender or Receiver) is a machine with a finite number of states. The machine always in one of states until an FSM event occurs

SELECTIVE-REPEAT PROTOCOL: Explain briefly about Selective-Repeat protocol. Explain, with neat diagram of Selective-Repeat protocol.

DEFINITION:

It implies to resends only selective packets, those that are actually lost is called the Selective-Repeat (SR) protocol.

DIAGRAM OF SELECTIVE-REPEAT PROTOCOL:



Sent, but not acknowledged

Acknowledged out of order

packet received out of order.

EXPLANATION:

Windows: The Selective-Repeat protocol uses two windows.

1) Send window 2) Receive window

The maximum size of the send window is much smaller, it is 2^{m-1}.

for ex. if $m=4$, sequence numbers from 0 to 15. maximum size of the window '8'. [15 in the Go-Back-N-protocol].

The Receive window in Selective-Repeat is totally different from one in Go-Back-N.

The size of the receive window is same as the size of the send window (Maximum 2^{m-1}).

The Selective-Repeat protocol allows as many packets as size of the receive window to arrive out of order kept until there is a set of consecutive packets to be delivered to the application layer.

To reliable protocol the receiver never delivers packets out of order to the application layer.

In the Selective-Repeat protocol, an acknowledgment number defines the sequence number of error-free packet received.

what are the Advantages of traspoot layer protocol?

ADVANTAGES: List out the (or) merits of transport layer?

1. Reliability
2. Flow Control
3. Congestion avoidance
4. Data integrity and Error Correction
5. Process-to-process delivery.

List the DisAdvantages of Transport layer protocol?

DISADVANTAGES: what are the Demerits (or) of Transport layer?

1. Layers Create additional Overhead
2. Bad interactions between Layers can be hard to solve.

Write any two Applications of transport layer protocol?

Application: what are the uses (or) of transport layer protocol?

1. User Datagram protocol
2. Transmission Control protocol
3. Datagram Congestion Control protocol.
4. Stream Control Transport-protocol.

Explain the concepts of Stop and wait protocol

STOP-AND-WAIT PROTOCOL:

Define (or) stop-and-wait protocol.

DEFINITION: Protocol is a connection-oriented protocol called the Stop-and-wait protocol, which uses both flow and error control.

Both sender and Receiver use a sliding window of size 1

Sender sends one packet at time and waits for an acknowledgment before sending next one.

To detect corrupted packets, need to add a checksum to each data packet

When a packet arrives at receiver site, it is checked. If its checksum is incorrect, the packet is corrupted and silently discarded.

DIAGRAM:

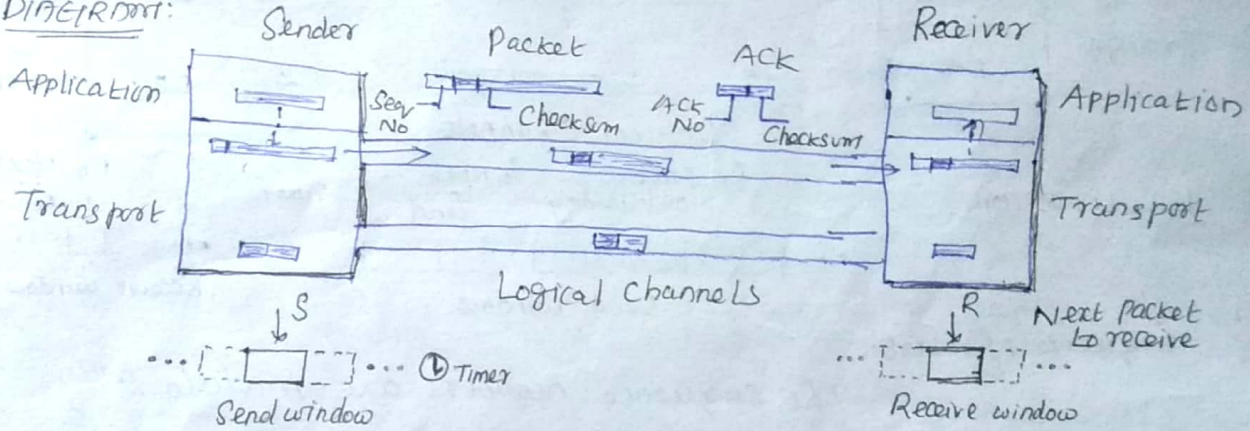


Fig: Stop-and-wait protocol

EXPLANATION:

Silence of the Rx^r is a signal for sender a packet was either corrupted (or) Lost.

Every time sender sends a packet, it starts a timer. If an acknowledgment arrives before the timer expires, the timer is stopped and sender sends the next packet.

If the timer expires, the sender resends the previous packet, assuming the packet was either lost (or) corrupted.

only one packet and one acknowledgment in the channels at any time.

"In stop-and-wait protocol, the acknowledgment number always, in modulo-2 arithmetic, the sequence number of the next packet expected.

Pipelining: Networking and other areas, a task is often begun before the previous task ended, known as pipelining.

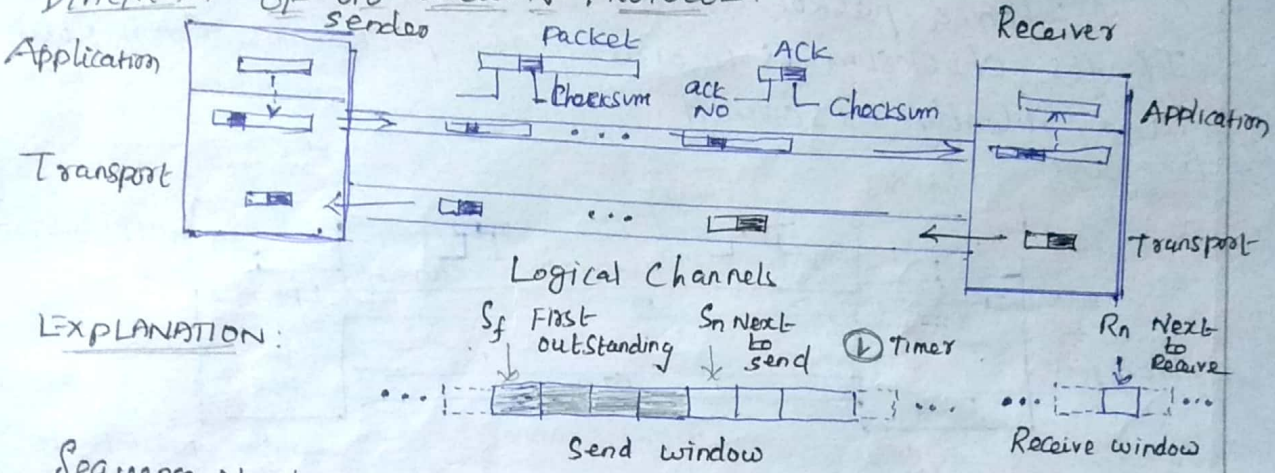
Go-Back-N Protocol (GBN): Explain the operation of Go-Back N-protocol?

AIM: To improve the efficiency of transmission (to fill pipe), multiple packets must be transition while the sender is waiting for acknowledgment.

DEFINITION: Go-back-N is send several packets before Rx'g acknowledgments, but receiver can only buffer one packet. Keep a copy of the sent packets until the acknowledgments arrive.

* Several data packets and acknowledgments in the Channel at same time

DIAGRAM OF GO-BACK-N PROTOCOL:



EXPLANATION:

Sequence Numbers:

The sequence numbers are modulo 2^m, where, m → size of the sequence number field in bits.

Acknowledgment Numbers:

An acknowledgment number in this protocol is cumulative and defines the sequence number of next packet expected to arrive.

Send window:

The Send window is an abstract Concept defining an imaginary box of Maximum size $= 2^m - 1$ with three variables, S_f, S_n and S_{size}.

Send window can slide one (or) more slots when an error-free ACK with ackNo greater than (or) equal to S_f and less than S_n (Modular Arithmetic) arrives.

Receive window: Is an abstract Concept defining an imaginary box of size 1 with a single variable R_n.

The window slides when a correct packet has arrived. Sliding occurs one slot at a time.

Client/server paradigm: Write short notes on Client/server paradigm.

At transport layer, need a transport layer address is called a port Number. To choose among multiple processes running on the destination host.

Port Numbers are 16-bit integers between 0 and 65,535. The client program defines itself with a port number, chosen randomly by transport layer s/w running on the client host. is known "ephemeral port number"

The internet has decided to use universal port numbers for servers, called "well-known port numbers".

The destination IP address defines host among the different hosts in the world. After the host has been selected, the port number defines one of processes on this particular host. What are the Ranges of IANA?

IANA Ranges: [Internet Assigned Number Authority]

3 Ranges:

1. Well-known ports: port ranging from 0 to 1023 are assigned and controlled by IANA.
2. Registered ports: ports ranging from 1024 to 49,151 are not assigned (or) controlled by IANA. only be registered with IANA to prevent duplication.
3. Dynamic ports: ports ranging from 49,152 to 65,535 are neither controlled nor registered. used by any process. These are "ephemeral ports."

The combination of an IP address and a port number is called a "socket address", Server processes uniquely

Define Multiplexing? (or) what is meant by multiplexing

MULTIPLEXING: Many-to-one relationship and requires MUX. Protocol accepts messages from different processes, differentiated by assigned port numbers.

After Adding the header, the transport layer passes the packet to the N/w Layer.

DEMULTIPLEXING: what do you meant by Demultiplexing?

one-to-many and requires DEMUX. Transport layer receives datagrams from N/w layer. After Error checking and dropping of the header, Transport layer delivers each message to appropriate process based on the port number

what is Difference b/w connectionless and connection oriented service.

CONNECTIONLESS Vs CONNECTION-ORIENTED SERVICE:

A Transport layer protocol can either be connectionless (or) connection oriented.

Connectionless service: The packets are sent from one party to another with no need for connection establishment (or) Connection release.

The packets are not numbered, may be delayed (or) lost (or) may arrive out of sequence.

No acknowledgment either.

UDP is connectionless.

Connection-oriented Service:

a connection is 1st established b/w the sender and Rx^r.

Data are transferred. At the end, the connection is released. TCP and SCTP are connection-oriented protocol.

Explain briefly about UDP: (or) Discuss about User Datagram Protocol)

UDP [USER DATAGRAM PROTOCOL]

DIAGRAM OF UDP, TCP and SCTP:

Bootstrap Protocol

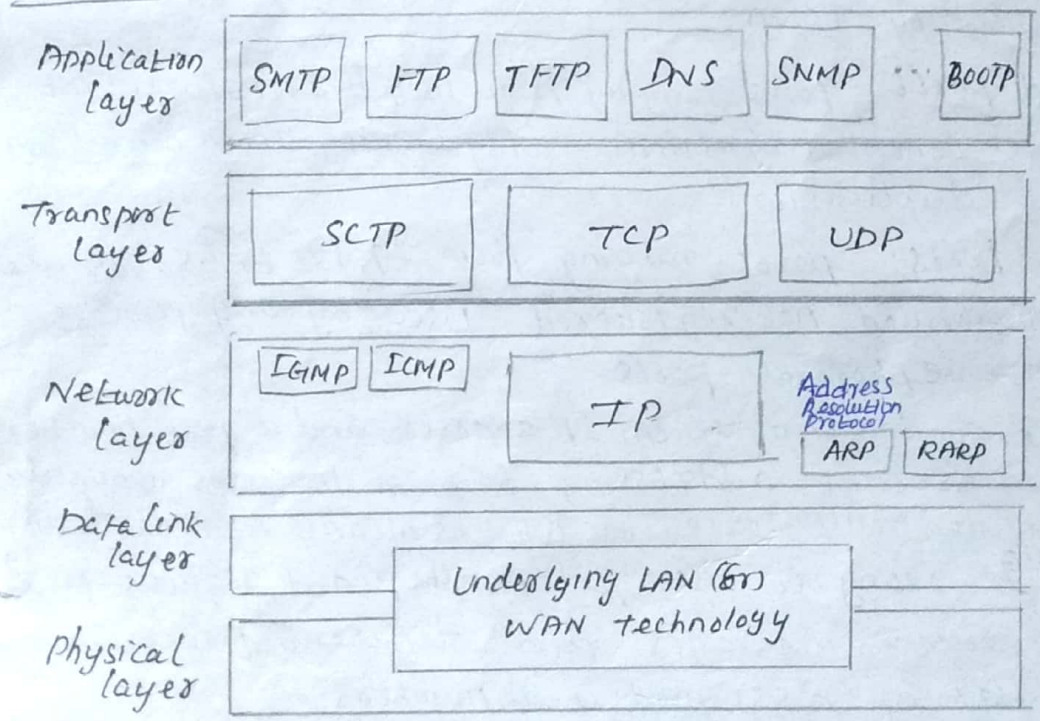


Fig: position of UDP, TCP and SCTP in TCP/IP suite.

DEFINITION:

UDP is called a connectionless, unreliable transport protocol. It does not add anything to the services of IP except to provide process-to-process communication instead of host-to-host communication, It performs limited Error checking.

UDP is very simple protocol using a minimum of overhead. If process wants to send a small message and does not care much about reliability, use UDP.

Sending a small message by using UDP takes much less interaction b/w the Sender and Receiver than using TCP (or) SCTP.

USER DATAGRAM: Define user Datagram. (or) what is meant by user datagram.

DEF: UDP packets, called User datagrams, a fixed-size header of 8 bytes

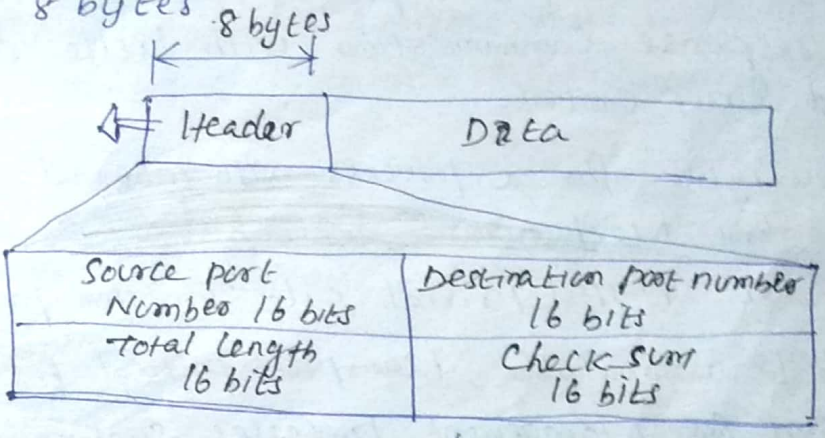


Fig. User datagram Format

Source port Number: port number used by process running on source host. 16 bits long. Ranges from 0 to 65,535.

If source host is the server [server sending a response] the port number is a well-known port number.

Destination port number: by process running on destination host. 16 bits long.

destination host is server (client sending a request) the port number is a well-known port number

If destination host is client, the port number, is an ephemeral port number.

Length: 16-bit field defines total length of user datagram, header plus data. Total length of 0 to 65,535 bytes

A datagram is Encapsulated in an Ip datagram.

UDP length = IP Length − Ip header's Length.

CHECKSUM: Used to detect errors over the entire User datagram (header plus data).

UDP operation: List out the operation of UDP? (or) what are the operation of UDP.

1. Connectionless services
2. Flow and Error Control
3. Encapsulation and Decapsulation

To send a message from one process to another, The UDP protocol encapsulates and decapsulates messages in an IP datagram.

USE OF UDP: what are the uses of UDP: (or) List out the applications of UDP.

1. UDP suitable for a process that requires simple request-response communication with little concern for flow and Error control.
2. Suitable for a process with internal flow and Error control Mechanisms.

   Ex: TFTP (Trivial File Transfer protocol)
3. It is a suitable transport protocol for multicasting
4. Used for Management processes such as SNMP. [Simple N/w Management protocol]
5. UDP is used for some route updating protocols such as RIP [Routing Information protocol]

Define TCP?

TCP [TRANSMISSION CONTROL PROTOCOL]

DEFINITION: TCP connection oriented protocol, it creates a virtual connection between two TCPs to send data.

TCP uses flow and Error control mechanisms at Transport level.

TCP is called a Reliable transport protocol.

TCP SERVICES: what are the services of TCP?

1. Process-to-process Communication: Well-known port numbers used by TCP.
2. Stream Delivery Service → To deliver data as a stream of bytes.
3. Sending and Receiving buffers:
4. Segments.
5. Full-Duplex Communication
6. Reliable Service.

List the features of TCP? (or) What are the benefits of TCP?

TCP FEATURES:

1. Numbering System → TCP S/w track of segments being Tx^d (or) Rx^d, no field for segment number value in segment header.

Two fields called Sequence number and Acknowledgment number. Fields refer to byte number & not segment number.

" The bytes of data being transferred in each connection are numbered by TCP. The numbering starts with a randomly generated number."

" The value of the sequence number field of a segment defines the number of first data byte contained in segment."

" The value of the acknowledgment field in a segment defines the number of the next byte a party expects to receive. The acknowledgment number is cumulative.

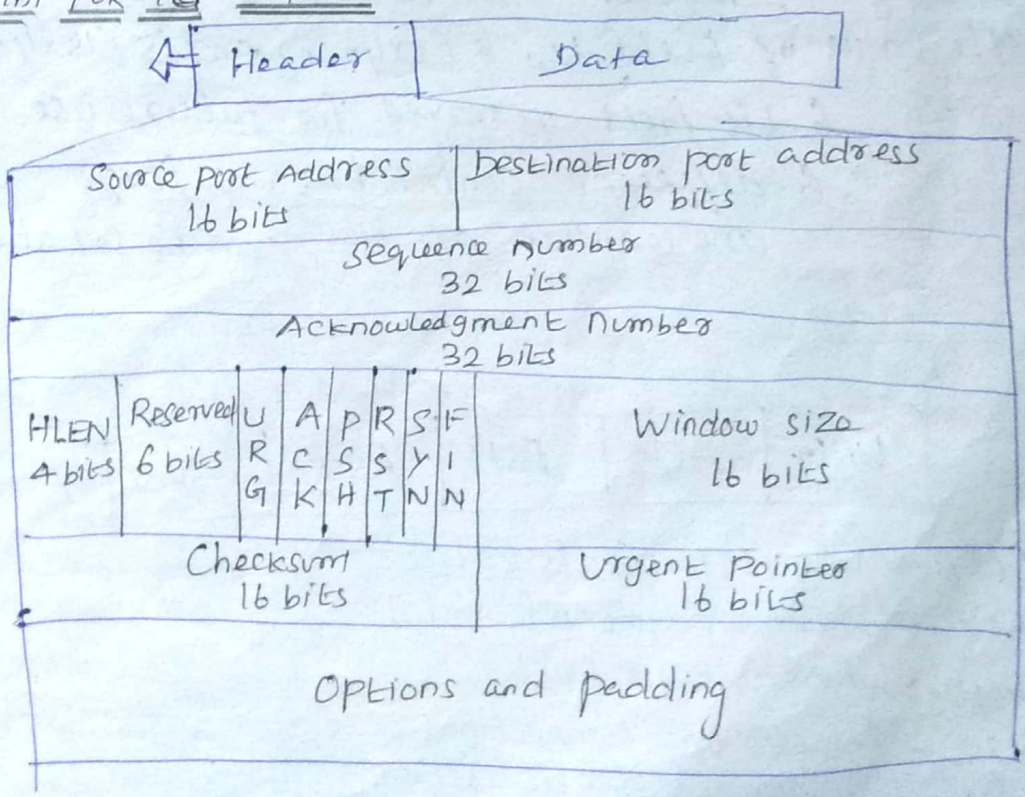
2. Flow Control
3. Error control
4. Congestion Control

Explain the operation of TCP segment format.

TCP Segment format: Draw and Explain about TCP segment format.

DEFINITION: A packet in TCP is called a segment.

FORMAT FOR TCP SEGMENT:



The segment consists of a 20 to 60 byte header by data from the application program.

Source port address: 16 bit field defines the port number of application program in host is sending the segment.

Destination port address: 16-bit field is the port number of application program in host is Receiving the Segment.

Sequence Number: 32-bit field the number assigned to first byte of data contained in this segment.

TCP is a stream transport protocol.

To ensure connectivity, each byte to be Tx^d is numbered.

During connection Establishment, each party uses a random number generator to Initial Sequence Number (ISN), usually different in each direction.

Acknowledgment number: 32-bit field defines byte number that receiver of segment is expecting to receive from the other party.

Header length: 4-bit field indicates the number of 4 byte words in the TCP header.

Length of header b/w 20 and 60 bytes.

The value of field b/w 5 (5x4=20) and 15 (15x4=60).

Reserved: 6-bit field reserved for future use.

Control: 6 different control bits (or flags).

one (or) more of bits can be set at a time.

CONTROL FIELD:

URG	ACK	PSH	RST	SYN	FIN

URG → Urgent pointer is valid.
ACK → Acknowledgment is valid.
PSH → Request for push.
RST → Reset the Connection
SYN → Synchronize sequence numbers
FIN → Terminate the Connection

TCP SERVICES:

What are the services avilable in TCP?
List out (or) the TCP services?

(i) TCP and UDP use same Network layer (IP), TCP provides a connection-oriented, reliable, byte Stream Service.

(ii) TCP does not support multicasting and broadcasting.

(iii) The unit of information passed by TCP to IP is called a segment.

(iv) When TCP sends a segment it maintains a timer, waiting for other end to acknowledge reception of segment.

(v) When TCP receives data from the other end of the connection, it sends an acknowledgment. TCP maintains a checksum on its header and data.

(vi) IP datagrams can get duplicated, a receiving TCP must discard duplicate data.

(vii) TCP provides flow control.

(viii) TCP connection is a byte Stream, not a message Stream.

(ix). TCP does not interpret the contents of the bytes to all.

Discuss the operation of TCP connection. (or) Briefly about approaches used for TCP connection Establishment)

TCP CONNECTION ESTABLISHMENT.

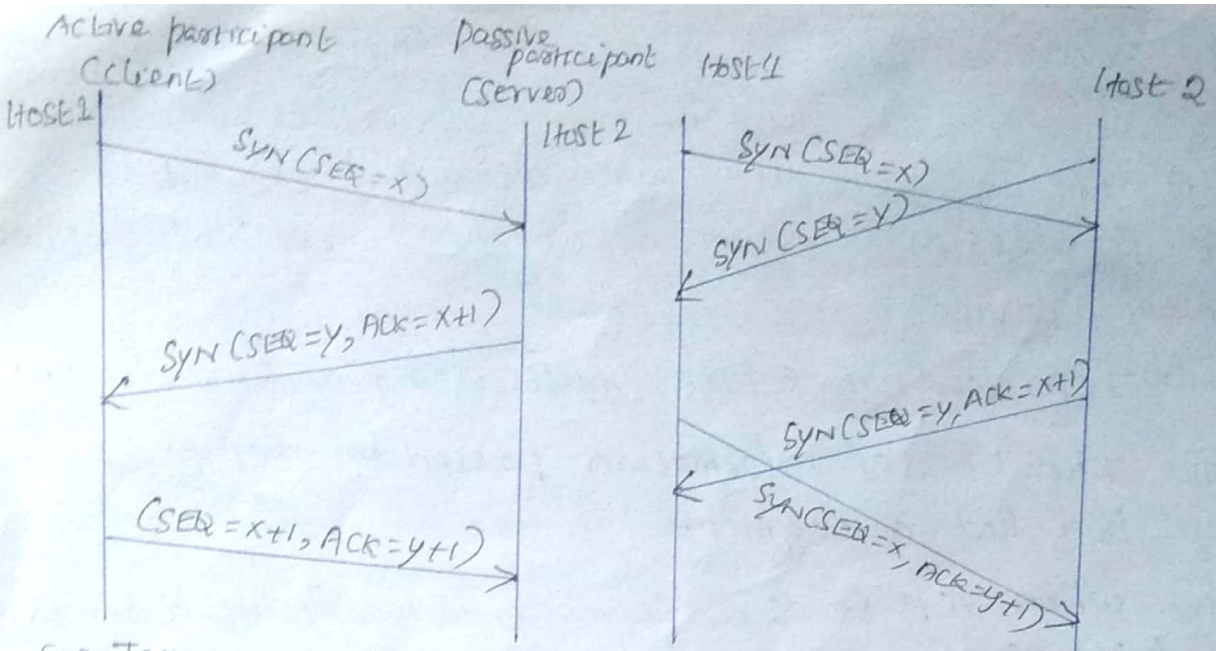
AIM:

To Establish the Connection, one side (server) passively waits for an incoming connection by executing the LISTEN and ACCEPT primitives, either Specifying a Specific Source.

CONCEPT OF TCP CONNECTION ESTABLISHMENT:

A connection is established using a three-way handshake.

The Transmitter sends Connection Request (Seq=x) to start a Connection with Transmitter message id x.



(a) TCP connection establishment in the normal case

(b) Call collision

EXPLANATION:

The receiver replies Connection Accepted (seq=y, ACK = x+1), to acknowledge 'x' and establish for its messages the identity 'y'.

Finally the Transmitter confirms the Connection with Connection Accepted (Seq = x+1, ACK = y+1) to Confirm its own identifier 'x' and accept the receivers identifier 'y'.

If the Received wanted to reject 'x', it would send Reject (ACK = x).

If the transmitter wanted to reject 'y' it would send Reject (ACK = y)

Part of the handshake the transmitter and Receiver Specify MSS (Maximum Segment Size) that is maximum size of segment can accept. A typical value is 1460.

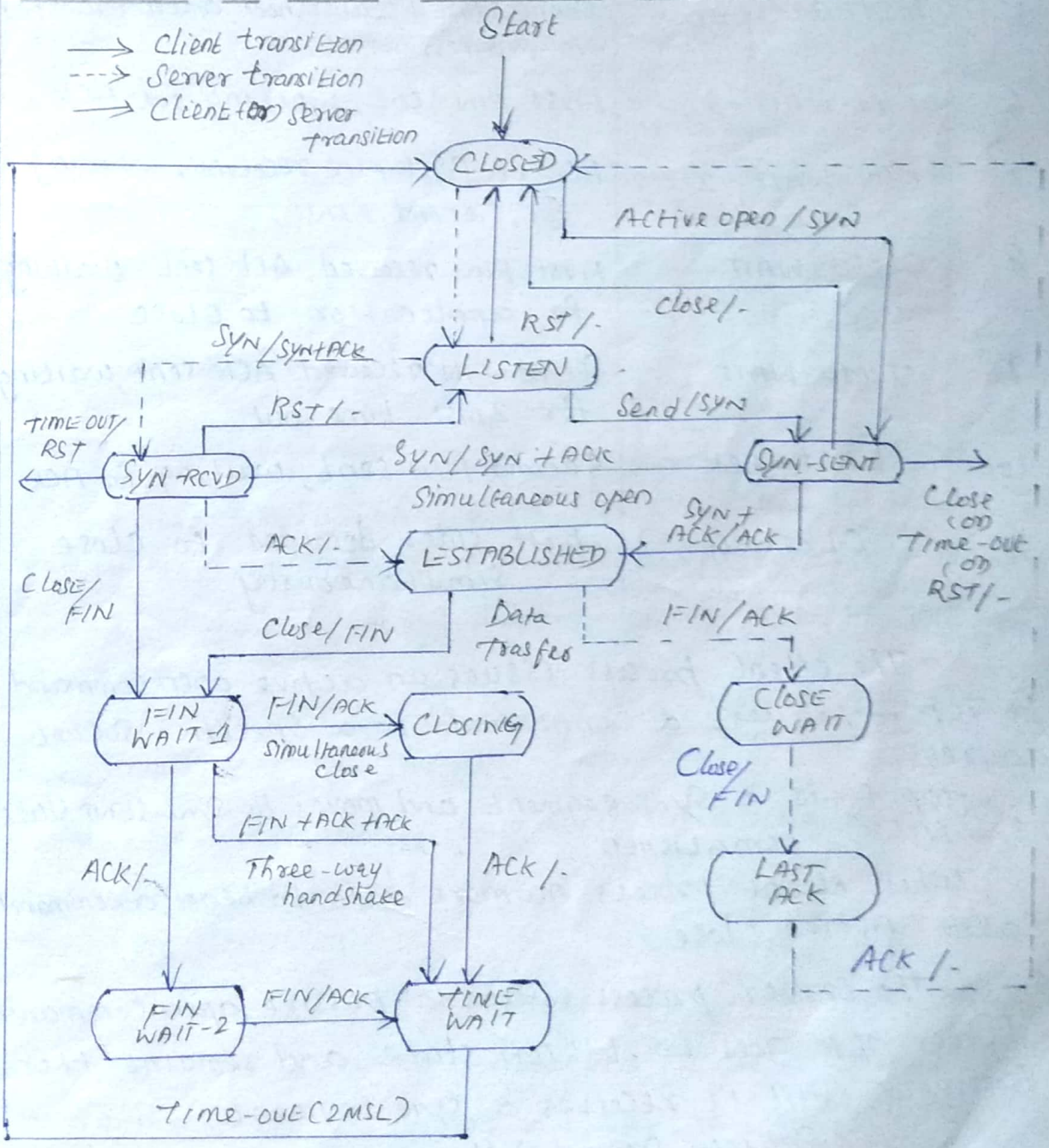
TCP connections are full duplex. The steps required establishing and release connections can be represented in finite State Machine [FSM].

STATE TRANSITION DIAGRAM:

AIM:

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 (FSM).

DIAGRAM OF STATE TRANSITION DIAGRAM:



EXPLANATION:

The State Marked ESTABLISHED in the FSM is in fact two different set of states that the client and server undergo to transfer data"

TABLE STATES FOR TCP:

S.NO	STATE	DESCRIPTION
1.	CLOSED	NO connection Exists
2.	LISTEN	passive open received, waiting for SYN
3.	SYN-SENT	SYN Sent, waiting for ACK
4.	SYN-RCVD	SYN + ACK Sent, waiting for ACK
5.	ESTABLISHED	Connection Established, data transfer in progress
6.	FIN-WAIT-1	First FIN Sent, waiting for ACK
7.	FIN-WAIT-2	ACK to first FIN received, waiting for second FIN
8.	CLOSE-WAIT	First FIN received, ACK sent, waiting for application to close
9.	TIME-WAIT	Second FIN received, ACK sent, waiting for 2MSL time-out
10.	LAST-ACK	Second FIN Sent, waiting for ACK
11.	CLOSING	Both sides decided to close simultaneously

* The client process issues an active open command to TCP to request a connection to a specific socket address.

* TCP sends a SYN segment and moves to SYN-SENT state.

SYN+ACK = ESTABLISHED,

* When client process no more data to send, a command called ACTIVE close.

* The server process issues a passive open command. Server TCP goes to LISTEN state and remains there passively until it receives a SYN segment.

SYN+ACK SEGMENT → SYN-RCVD → ESTABLISHED STATE

* It sends ACK segment and goes to "CLOSE-WAIT" state.

After receiving the passive close command, server sends a "FIN" segment to client and goes to "LAST-ACK" state, waiting for final ACK. When ACK segment received from client, the server goes to "CLOSE" state.

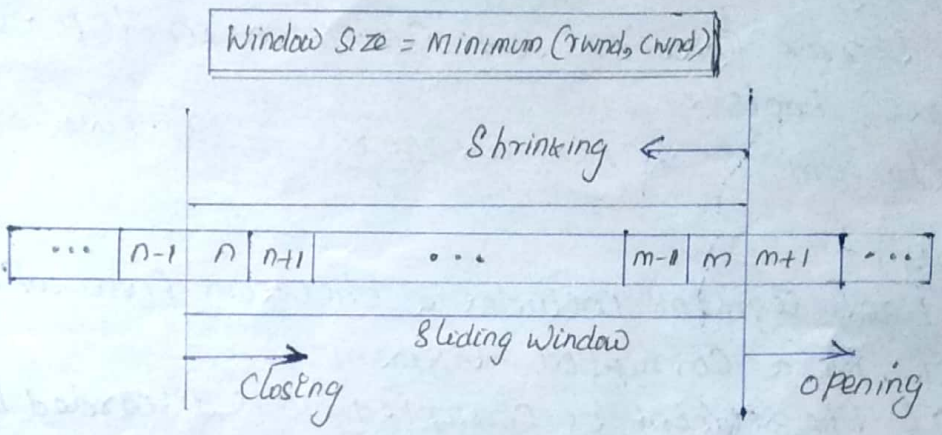
FLOW CONTROL:

DEFINITION

A Sliding window is used to make transmission more efficient as well as to control the flow of data so that the destination does not become overwhelmed with data.

TCP sliding windows are byte-oriented.

DIAGRAM OF SLIDING WINDOW:



EXPLANATION:

* The size of the window is the lesser of rwnd and cwnd that is (Received window) (or) and Congestion window
* The source does not have to send a full window's worth of data.
* The window can be opened (or) closed by the receiver, but should not be shrunk.
* The destination can send an acknowledgment at any time as long as it does not result in a shrinking window.
* The Receiver can temporarily shut down the window, the sender however, can always send a segment of 1 byte after the window is shut down.

ERROR CONTROL:

DEFINITION/DESCRIPTION:

TCP provides reliability using error control. Error Control includes mechanisms for detecting corrupted segments, lost segments, out-of order segments and duplicated segments.

Error Control also a mechanism for correcting errors after they are detected.

Error Detection and Correction in TCP is achieved by three tools.

1. Checksum 2. Acknowledgment 3. Time-out

CHECKSUM:

Each segment includes a checksum field which is used to check for a corrupted segment.

If the segment is corrupted, it is discarded by destination TCP and is considered as lost.

TCP uses a 16-bit checksum is mandatory in every segment.

ACKNOWLEDGMENT:

TCP uses Acknowledgment to confirm the receipt of data segments.

Ack segments do not consume sequence numbers and are not acknowledged.

RE-TRANSMISSION:

A Re-transmission occurs if the retransmission timer expires (or) three duplicate Ack segments have arrived.

No retransmission timer is set for an Ack segment.

RE-TRANSMISSION AFTER RTO (Re-Transmission time-out):

No time-out timer is set for segment carries only an acknowledgment, there is no segment is resent.

The value of RTO is dynamic in TCP and updated based on Round-Trip-Time (RTT). of segments.

RE-TRANSMISSION AFTER THREE DUPLICATE ACK SEGMENTS:

One segment is lost and R_x Receives many out-of-order segments cannot be saved (limited buffer size),

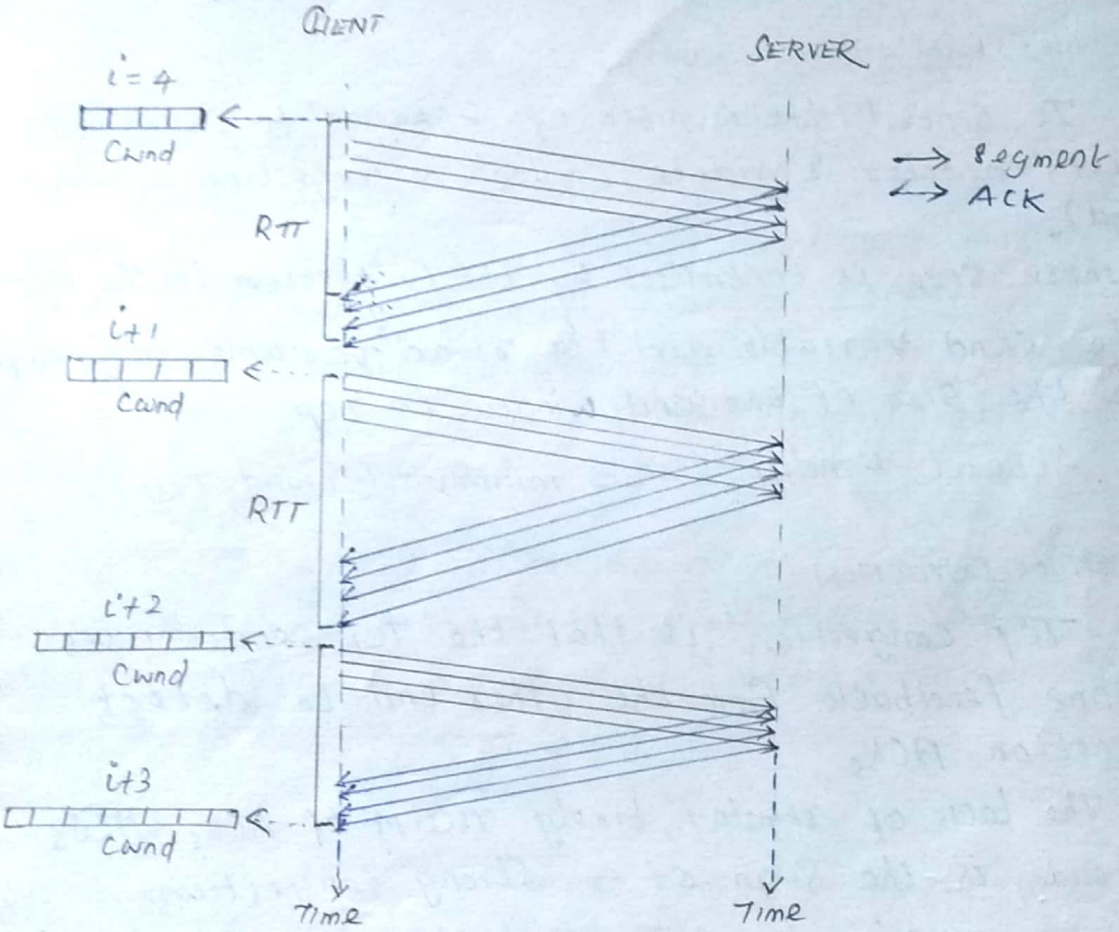
To follow the three duplicate-Ack rule and retransmit the missing segment immediately. It referred to "fast Retransmission.

CONGESTION AVOIDANCE:

DEFINITION / DESCRIPTION:

In the Congestion-Avoidance Algorithm, the size of the Congestion window increases additively until Congestion is detected.

DIAGRAM / CONCEPT OF CONGESTION AVOIDANCE:



EXPLANATION: The sender starts with cwnd=4. After four ACKs arrive, the acknowledged segments are purged from window, there is now one extra empty segment slot in window.

The size of the Congestion window is increased by 1. The size of window is now 5. After sending five segments and receiving five acknowledgments for them,

The size of the Congestion window now becomes 6

If an ACK arrives, cwnd = cwnd + (1/cwnd) → portion of 1 MSS (Max. segment size)

Start → cwnd = i

After 1 RTT → cwnd = i+1

After 2 RTT → cwnd = i+2

After 3 RTT → cwnd = i+3

RTT → Round-Trip-Time

TCP CONGESTION CONTROL:

DEFINITION:

Congestion Control is a process of Maintaining the number of packets in a network below a certain level at which performance falls off.

TCP uses different policies to handle the congestion in the Network.

CONGESTION WINDOW:

To control the number of segments to transmit, TCP uses another variable called a Congestion Window, (cwnd),

whose size is controlled by the Congestion in the N/w.

The cwnd variable and the rwnd variable together define the size of the send window in TCP.

Actual window size = minimum (rwnd, cwnd)

CONGESTION DETECTION:

TCP congestion is that the TCP sender uses only one feedback from the other end to detect congestion ACKs.

The lack of regular, timely receipt of ACKs, this time-out, is the sign of a strong congestion.

The receiving of three duplicate ACKs is the sign of a weak Congestion in the N/w.

CONGESTION POLICIES:

TCP's general policy for handling Congestion is based on three algorithms.

1) Slow Start 2) Congestion Avoidance 3) fast recovery

1) SLOW START:

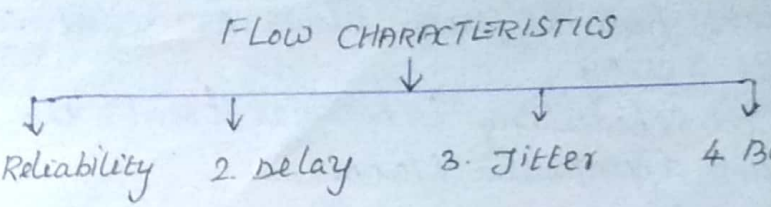
In the slow-start algorithm, the size of the congestion window increases exponentially until it reaches a threshold.

QUALITY OF SERVICE (QoS)

DEFINITION:

QoS is an internetworking is define Quality of Service as something a flow seeks to attain

FLOW CHARACTERISTICS:



EXPLANATION:

(1) RELIABILITY:

Reliability is a characteristic that a flow needs. Lack of reliability means losing a packet (or) acknowledgment, which entails retransmission

Eg. Electronic Mail, File transfer, telephony (or) audio conferencing

2) DELAY:

Source-to-destination delay is another flow characteristic. It can tolerate delay in different degrees.

Eg. Telephony, Audio Conferencing, Video Conferencing and remote log-in need minimum delay.

3) JITTER:

Jitter is the variation in delay for packets belonging to the same flow.

Jitter is defined as the variation in the packet delay. High Jitter means the difference b/w delays is large. Low Jitter means the variation is small.

Eg. Multimedia Communication deals with Jitter

4) BANDWIDTH:

Different applications need different bandwidths. In video Conferencing need to send millions of bits per second to refresh a color screen while the total number of bits in an e-mail may not reach even a million.

Based on flow characteristics, Categorization is not formal (or) universal.

TECHNIQUES TO IMPROVE QoS:

AIM/DESCRIPTION:

To improve the Quality of Service based on four methods are, Scheduling, Traffic Shaping, Admission Control and Resource Reservation.

SCHEDULING:

Packets from different flows arrive at a switch (or) router for processing

A good scheduling techniques treats the different flows in a fair and appropriate Manner.

Several Scheduling techniques are FIFO queuing, priority Queuing and weighted fair queuing.

FIFO QUEUING:

In First-in, First-out (FIFO) queuing packets wait in a buffer (queue) until the node (router (or) switch) is ready to process them.

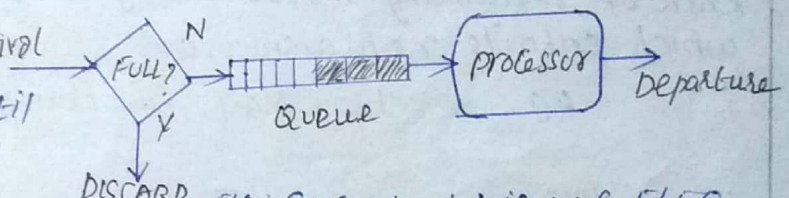


Fig: Conceptual view of FIFO Queue

If avg arrival rate is higher than Average processing rate

PRIORITY QUEUING:

Packets are first assigned to a priority class. Each priority class has its own queue.

Continuous flow in high-priority queue, packets in lower-priority queues will never chance to processed. Called as STARVATION.

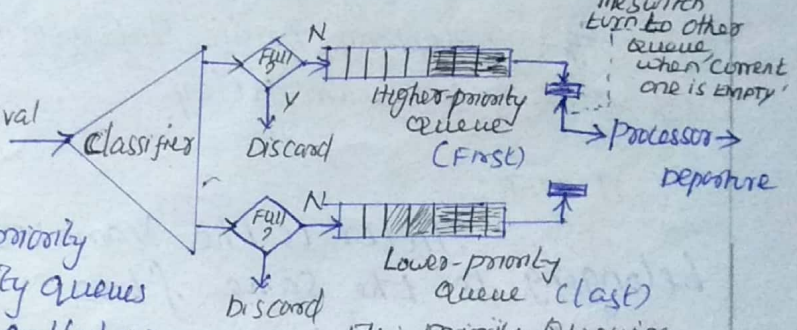


Fig: Priority Queuing

WEIGHTED FAIR QUEUING:

The packets are still assigned to different classes and admitted to different Queues.

However, are weighted based on the priority of the Queues, higher priority means a heigher weight.

The turning switch selects 3 packets from first Queue, then 2 packets from the second Queue, then 1 packet from the third Queue.

The cycle Repeats the process.

ADVANTAGES OF TCP:

1. Connection Oriented
2. Stream data transfer
3. Reliable
4. Point-to-point (or end-to-end delivery
5. Error and flow control
6. Full Duplex

DISADVANTAGES:

1. TCP need the overhead required to detect reliablity.
2. To maintain the unexpected of data flow
3. Complexity to use for a Network.

APPLICATION REQUIREMENTS:

1. End-to-End Connection between hosts.
2. process-to-process delivery.
3. Multiplexing and Demultiplexing.
4. Congestion Control.
5. Data integrity and Error Correction
6. Flow Control.

CONGESTION AVOIDANCE:

DEC BIT [DIGITAL EQUIPMENT CORPORATION BIT]

DEFINITION:

It is a technique implemented in routers to avoid congestion. Its utility to predict possible congestion and prevent it. protocol works with TCP

CONCEPT:

The router calculates the area under the curve and divides value by time interval to compute average queue length.

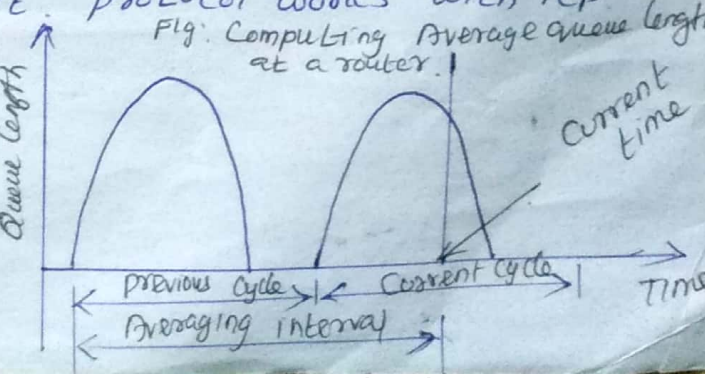


Fig: Computing Average queue length at a router.

ADVANTAGES:

1. Dynamically manages the window to avoid Congestion.

2. Try to balance bandwidth with respect to the delay.

RED / RANDOM EARLY DETECTION [FOR Congestion Avoidance)

DEFINITION:

RED is also known as Random Early discard (or) Random early drop is a queueing discipline for a network scheduler suited for Congestion Avoidance.

FLOW DIAGRAM / ALGORITHM: