Unit-5 Transport Layer

- Ankit Pargeni DATE

* Introduction

The transport layer is the layer in OSI Responsible for end-to-end connection over a network. It is responsible for the management of error correction, providing quality and reliability to the end user. This layer enable the host to send & receive error corrected data, packets or messages over a network.

Responsibilities: (services)

- Process-to-process delivery
- End-to-End connection between hosts
- Multiplexing & de-multiplexing.
- Data Integrity & Error correction
- Flow control

* Functions

i) Service point addressing → It includes service point address which makes sure that the message is delivered to the correct process.

ii) Segmentation & reassembly → It accepts the message from session layer & breaks into smaller units. The transport layer at the destination reassembles the message.

iii) Flow control : Flow control is performed end to end

iv) Error control : Error control is performed end to end in this layer to ensure that the complete message arrives at the receiving end without any error. Error correction is done through retransmission

* Services

i) Process to process delivery → While Data link requires MAC address of source-destination hosts to correctly deliver a frame, Network layer requires IP address for appropriate routing of packets, Transport layer requires a port number to correctly deliver the segments of data to the correct process amongst multiple processes running on a particular host.

ii) End-to-End connection between hosts → It mainly uses TCP and UDP for creating end-to-end connection between hosts. TCP ensures reliable delivery of messages & UDP ensures best-effort delivery.

iii) Multiplexing & De-Multiplexing
Multiplexing allows simultaneous use of different applications over networks which are running on a host. Demultiplexing is done at the receivers side to obtain the data coming from various sources

DATE

* Transport protocols.

The transport protocols provide services to their upper layers at well-defined interface points, which are also reffered as ports. The Ip address & the port are an important combination to setup a transport connection. TCP & UDP are the main transport layer protocols that provide different set of services to the network layer.

The comparision of TCP & UDP *:

Transmission Control protocol (TCP)	User Datagram protocol (UDP)
1. TCP is a connection-oriented protocol.	1. UDP is a datagram oriented protocol.
2. TCP is reliable as it guarantees the delivery of data to the destination router.	2. Delivery of data to the destination cannot be guaranteed in UDP
3. TCP provides extensive error checking mechanisms. as it provides flow control & acknowledgment of data.	3. UDP has only the basic error checking mechanisms using checksums
4. TCP doesn't support broad casting.	4. Supports broadcasting
5. TCP is comparitively slower.	5. UP is faster, simpler & more efficient than TCP.
6. TCP is used by HTTP, HTTPS, FTP, SMTP & Telnet.	6. UDP used by DNS, DHCP, SNMP, & VOIP.

IMP Q. Difference between connection less & Connection oriented.

DATE

* Connection less and Connection Oriented Network Service

Both connection-less and connection oriented service are used for the connection establishment between two or more than two devices. These type of services are offered by the network layer.

Connection less service :

→ Connection less system is related to postal system
→ It does not include any connection establishment and termination.
→ This service does not give the guarantee of reliability.
→ Here, packets do not follow the same path to reach the destination. so they are not received in order they sent.
→ It transfers data without any authentication.
→ No handshaking is used as there is no any virtual connection between sender & the receiver.
→ User Datagram protocol (UDP), Internet Protocol (IP) and Internet Protocol (IP) are some examples.
→ Requires low bandwidth to transfer the data packets.

Connection Oriented Service.

→ This Service is based on the telephone system.
→ It creates end to end connection between the senders to the receiver before transmitting data packets over network and there is connection termination after data is transferred.
→ The data packets follow the same path to reach the dest. So--
→ Handshaking method is used to establish the connection.
→ Requires more bandwidth to transfer data packet so it is preferred by long & steady communication
→ TCP is an example of connection oriented. service.

PAGE

DATE

* Congestion Control

Congestion is a situation in which too many sources over a network attempt to send data and the router buffers start overloading due to which loss of packets occur. In this case, the transport layer uses different mechanisms & techniques to control the congestion & keep the load below the capacity :-

There are mainly two categories of congestion control

1) Open Loop Congestion control policy.

In open loop congestion control, policies are applied to prevent congestion before it happens. Here, Congestion control is managed by either the source or the destination. Some policies are

- Retransmission policy :- If the sender feels that a sent packet is lost or corrupted, the packet need to be retransmitted. It may increase congestion in network. However, a good retransmission policy can prevent congestion.
- Window policy :- The type of window at the sender may also affect congestion. The selective repeat window is better than Go back - N window for congestion control.

DATE

- Acknowledgement-Policy : The acknowledgement policy imposed by the receiver may also affect congestion. If receiver doesn't acknowledge every packet it receives, it may slow down the sender & help prevent congestion.

- Discarding-policy:- A good discarding policy by the routers may prevent congestion & at the same time may not harm the integrity of transmission

- Admission policy:- It also can prevent congestion in virtual-circuit networks. A router can deny establishing a virtual-circuit connection if there is congestion in network or if there is possibility of future congestion.

2.) Closed-loop Congestion Control

In closed-loop congestion control, policies are applied to prevent congestion after it happens. Following are the policies used to prevent congestion in closed loop

- Backpressure : It is a mechanism in which a congested node stops receiving data from the immediate upstream node or nodes. This technique can be only applied to virtual circuit networks.

DATE

- Choke packet: It is sent by a node to the source to inform its congestion. In backpressure, the warning is from one node to it's upstream node but in choke packet method, the warning is from the router, which has encountered congestion
- Implicit Signaling: Here, ~~there~~ is no communication between the congested node(s) & the source. The source guesses that there is a congestion somewhere in the network from other symptoms
- Explicit signaling: Here, the signal is included in the packets that carry data
- Backward signaling: A bit can be set in a packet moving in the direction opposite to the congestion. This bit can warn the source that there is congestion
- Forward signaling: A bit can be set in a packet moving in the direction to the congestion. This bit can warn the destination that there is congestion

classmate

PAGE

DATE

* TCP Congestion Control

TCP uses a network congestion-avoidance algorithm that includes various aspects of an additive increase/multiplicative decrease (AIMD) scheme. It's general policy for handling congestion consists of following.

i) Slow start phase:

It helps to avoid sending more data than the network is capable of forwarding. Initially sender sets congestion window size = Maximum Segment size (MSS). After receiving each acknowledgement, sender increases the congestion window size by 1 MSS. Here, the size of congestion increases exponentially

Congestion window Size = Congestion window size + Maximum Segment size

Initially cwnd = 1

After, 1 RTT, cwnd = $2^1 = 2$

2 RTT, cwnd = $2^2 = 4$

3 RTT, cwnd = $2^3 = 8$

cwnd = congestion window

RTT = Round trip time

ii) Congestion avoidance phase:

It is also called additive increment. The phase starts after the threshold value also denoted as ssthresh. The size of congestion window increases additive.

Initially cwnd = P

After 1 RTT, cwnd = P+1

After 2 RTT, cwnd = P+2

After 3 RTT, cwnd = P+3

iii) Congestion detection.

It is also called multiplicative decrement. If Congestion occurs, the ~~cwnd is~~ congestion window size is decreased. The only way a sender can guess that congestion has occurred is the need to retransmit a segment. Retransmission can occur in one of two cases:- when the RTO timer times out or when three duplicate ACKs are received

* Traffic Shaping algorithms

Traffic Shaping is a bandwidth management technique used on computer networks which delays some or all datagrams to make them compatible with a desired traffic profile. It is used to optimize or guarantee performance, improve latency.

It is basically a mechanism to control the amount & the rate of traffic sent to the network. There are two types:

1) Leaky Bucket

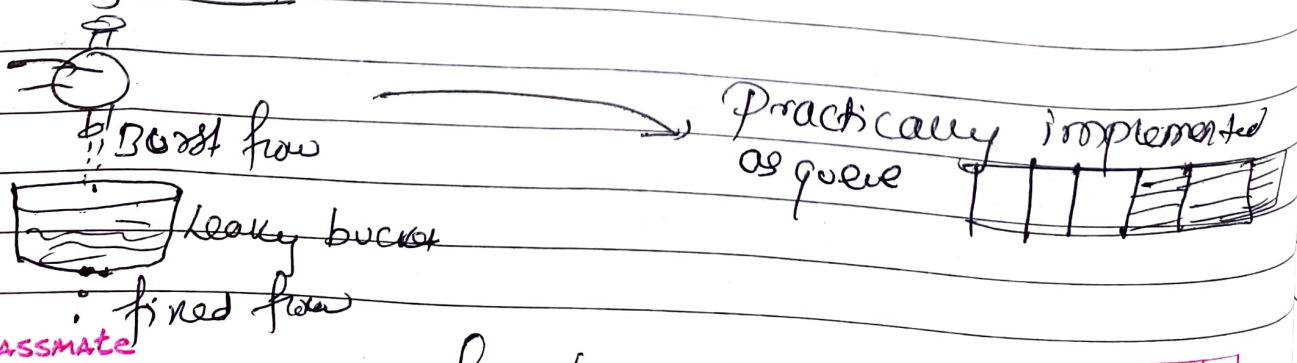

fig: Leaky bucket can visit

DATE

This algorithm is used to control rate in a network. It is implemented as a single server queue with constant server time. If bucket overflows then packets are discarded. Here, input rate can vary but output rate remains constant. It saves busty traffic into fixed rate traffic by averaging the data rate.

Algorithm

1. Initialize the counter to n at every tick of clock.
2. If n > size of packet in front of queue, send the packet into the network and decrement counter by size of packet.
   Repeat the step until n < size of packet.
3. Reset the counter & go to step-1.

2. Token Bucket

This algorithm compared to leacky bucket allows the output rate to vary depending on the size of burst. Here, the bucket holds token to transmit a packet, the host must capture & destroy one token. Token are generated by a clock at the rate of one token every second.

Algorithm:

1. A token is added at every Δ time.
2. Bucket can hold b-token. If a token arrives when bucket is full, it is discarded.
3. When a packet of m bytes arrived, m tokens are removed from the bucket & packet is sent to the network.
4. If less than n tokens are available, no tokens are removed from the buckets & packet is said to be non conformant.

PAGE

classmate

DATE

Formula:

i) Burst length = $\frac{\text{Capacity of bucket (KB)}}{(\text{output rate (mbps)} - \text{arrival rate (mbps)}) * 1000}$ = ---msec

ii) For another 500 KB (capacity of bucket considers 500 KB), the time taken will be

$\frac{\text{Capacity of bucket}}{\text{Arrival rate} * 1000}$ = x msec.

∴ output time = Burst length + x = y msec.

Leaky buckets	Token bucket
i) Token independent	i) Token dependent
ii) If bucket is full, packet is discarded.	ii) If bucket is full, token are discarded, but not packet
iii) Bucket leaks at constant rate	iii) Bucket has maximum capacity
iv) Queue outputs at finite rate.	iv) If there is no token in bucket, packet can't be sent
v) It doesn't save token.	v) It saves token to send large bursts
vi) It Sends packet at constant rate.	vi) Allows large bursts to be sent faster rate after that constant rate.
vii) Packets are transmitted continuously	vii) Packets can only be transmitted when there are enough token.

CLASSMATE

PAGE

DATE

* Techniques to improve QoS

Quality of Service (QoS) refers to traffic control mechanisms that ensures the performance of critical applications with limited network capacity. It helps organizations to adjust their overall network traffic by prioritizing special high-performance applications.

Some techniques to improve QoS are:

1) Scheduling → A good scheduling technique treats the different flows of packets in a fair and appropriate manner. Different scheduling techniques are FIFO queuing, priority queuing, weighted (Round Robin) fair queuing are used to improve QoS.

2) Traffic Shaping → Discussed before.

3) Resource reservation → A flow of data needs resources such as a buffer, bandwidth, CPU time, and so on. The QoS is improved if all these resources are reserved in a proper manner beforehand. Integrated services depend heavily on resource reservation to improve QoS.

4) Admission Control : It refers to the mechanism used by a router, or a switch, to accept or reject a flow based on predefined parameters called flow specifications. Before a router accepts a flow for processing, it checks the flow specifications to see if its capacity & its previous commitments to other flows can handle the new flow.

DATE

* Queuing Techniques for scheduling

Some queuing techniques for scheduling are:

i) FIFO Queuing :) Here, all the packets wait in a queue until the node is ready to process them. The packet which came first will be processed first. If the average arrival rate is higher than the average processing rate, the queue will fillup & new packets will be discarded.

ii) Priority Queuing:- Here, packets are first assigned to a priority class. Each priority class has its own queue. The packets in the highest priority queue are processed followed by the packets with the lower priority.

iii) Weighted fair Queuing → It is a better scheduling technique in which the packets are assigned to different classes & admitted to different queues. The queues are weighted based on the priority of queues; higher priority means a higher weight. It processes packets in each queue in a round-robin fashion.

classmate

PAGE

DATE

* Introduction to Ports and Sockets

Port	Sockets
i) Port is a number used by a particular software. The same port may be used in different computers/servers running same software	i) Socket is a combination of port and IP-address to identify particular software & particular computer/server
ii) It is a logical data connection that can be used to exchange data without the use of a temporary file or storage.	ii) It is an endpoint of a bidirectional communication that occurs in a computer network that is based on the internet protocol.
iii) It helps to identify a specific application or a process.	iii) It works as the interface to send & receive data through a specific port.
iv) Port operates at the transport layer of OSI.	iv) Sockets are a means of plugging the application layer.
v) A port functions like a telephone number, identifying the machine & giving the socket an area to connect	v) While the socket functions like a cord that ties the computers together.
vi) Port ranges from 0 to 65535, port no. 0 is reserved & unused.	vi) Ex. of socket: 192.168.10 : 8080

classmate

PAGE

DATE

✗ Socket programming

It is a way of connecting two nodes on a network to communicate with each other. One socket (node) listens on a particular port at an IP, while other socket reaches out to the other to form a connection. Server forms the listener socket while client reaches out to the server.

Socket connections normally run between two different computers on a LAN or across the internet, but they can also be used for inter-process communication on a single computer.

Questions asked from this chapter

DATE

Q. What is open loop congestion control? Compare it wit closed loop congestion protocol. (2078 - 5 marks)

Q Short note: Connection-oriented service. (2076 - 2.5 marks)

Q What is congestion control? Why do we need it? (2071 - 5 marks) (2072 - 5 marks)

Q. Differentiate between UDP & TCP. (2075)

Q. Differentiate between Leaky & Token buckets (Imp)

Q. Differentiate between Port & socket (Imp)

Q Difference between connection oriented & connection less service. (Imp)