Indian Institute of Technology Patna
Date: 30 Sep 2023
MIDSEM: CS358 Computer Networks

DURATION: 2 HOURS Full Marks ?

Instruction: No doubts would be entertained. Write suitable assumptions, if necessary on last page beside the question. Students are allowed to use scientific calculators. Calculations are in terms of 10^x. Like 1Gbps = 10^9, 1Mbps = 10^6, 1Kbps = 10^3 and so on. Each question from Q1 should start on a fresh page. So if the Q1 takes 1/2 page to finish, begin Q2 from the next page.

Q(1) a) What is the difference between Flow Control & Congestion Control **[Marks 5]**
Flow control: control packet tranmissions at the host in order to make sure that the buff er at the receiver does not overflow (drop packet). Congestion control: control of packet tranmissions in order to make sure that the buff ers at the routers in the network do not overflow (get congested)

b) Consider sending a packet from a sending host to a receiving host over a fixed route. List the delay components in the end-to-end delay computation. Which of these delays are constant and which are variable? Briefly describe the delays in 1-2 lines each. Also show a pictorial representation of the delay using a small network example.
Answer: The delay components are processing delays, transmission de- lays, propagation delays, and queuing delays. All of them are fixed for a fixed-size packet except queuing delay. **[Marks 5]**

Q(2) Stop-and-Wait ARQ. Think about a scenario where sender A and receiver B engage in stop-and-wait ARQ communication. Let's say A uses the initial sequence number (ISN) 300; in other words, let's say ISN=300. Let's assume that A sends B 100 bytes in the first packet that the two of them exchange. **[Marks 10]**
(a) What is the SN number that A puts into the packet header (such as for example a TCP packet header)?
Ans: 300
(b) If B receives the first 100 bytes packet from A without an error, what is the ACK number that B uses in the packet that is sends to A in response to the packet it received?
Ans: 400 or 401
(c) If B detects an error in the first 100 bytes packet that it receives from A, what is the ACK number that B uses in the packet that is sends to A in response to the packet it received?
Ans: 300
(d) Which flag is set by B while sending the previous packet?
Ans: ACK

Q(3) Consider a TCP connection between two applications running on two end-hosts A and B. **[Marks 20]**
(a) For hosts A and B, show a diagram of the three-way TCP handshake. Assume A initiates the process.
Ans: Diagram

(b) Indicate which flags are set for each packet represented in the diagram in (a), as well as which (important) information is contained in the TCP packet header. Enter the response as text.
Ans: SYN: A's port, B's port, A's initial sequence number ISNA, SYN fl ag SYN ACK: A's port, B's port, A's initial sequence number ack ISNA+1, B's initial se- quency number ISNB, SYN fl ag, ACK flag ACK: A's port, B's port, B's initial sequency number ack ISNB+1, ACK flag

(c) Give a brief explanation of the three-way handshake's packets' functions.
Ans: SYN: A tells B that it wants to open a new TCP connection and indicates initial se- quence number at A for the connection. SYN ACK: B acknowledges the connection set up request and the initial sequence number at A for the connection, and indicates the initial sequence number at B for the connection. ACK: A acknowledges the initial sequence number at B for the connection.

(d) Justify why a two-way handshake wont suffice for a TCP connection
Ans: The short answer is because a two way handshake would only allow one party to establish an ISN, and the other party to acknowledge it. Which means only one party can send data. But TCP is a bi-directional communication protocol, which means either end ought to be able to send data reliably. Both parties need to establish an ISN, and both parties need to acknowledge the other's ISN.

Q(4) A 10,000 bit message traveling through two routers R1 and R2 from source node A to destination node B. The path's three links all have a 30 ms delay. R1 and R2 transmit data at a rate of 1000 bits per second, while Node A transmits data at 100 bits per second. For simplicity's sake, we assume that this is a store-and-forward system, that there is no queueing delay, and that all header overheads are irrelevant. **[Marks 10]**

(a) Find the end-to-end latency of the message when it is sent as a whole.

Ans:Propagation delay per link: 0.03 sec transmission delay at A: 100 sec transmission delay at router R1and R2: 10 sec total delay over 3 links: 100.03 sec + 2x10.03 sec = 120.09 sec

(b) Find the message's end-to-end delay after it has been divided into 10 packets, each 1000 bits in size, and then transmitted to the destination..

Note that message transmission delay at A is larger than at R1 and R2. As a re- sult, there are 'gaps' between the packet transmissions at R1 Propagation delay per link: 0.03 sec message transmission delay at A: 100 sec packet transmission delay at router R1and R2: 1 sec total delay over 3 links: 100.03 sec + 1.03 sec + 1.03 sec = 102.09 sec

Q(5) Using a dependable stop-and-wait protocol, an application must send 100KB of data. The protocol divides the data into chunks with a 1KB application data payload. Each segment fits within a single IP packet. There is no packetization or queuing delay, and the RTT is 50 ms. The protocol has no retransmission cap and a set retransmission timeout of 200ms. How long, in seconds, will the transfer take if the network doesn't duplicate, drop, or corrupt any packets? Since there is no additional latency from connection setup and only data transactions are occurring, you can assume the connection is already established when you begin your test. Your response needs to be precise to two decimal places. **[Marks 5]**

Answer: Total number of frames needed = 100KB / 1KB = 100. Since this is stop-and-wait, the time needed = 100 * 50 = 5000 ms = 5s.

Q(6) You type the following URL into your web browser: http://iitp.ac.in/dept/cse.html Assuming that

- your DNS resolver is 8.8.8.8.
- neither your host nor your DNS resolver have any cached DNS entries,
- DNS never needs to fail over to TCP, and
- the HTML response returns 200 OK with a web page,
- the HTML request and response each fit in a single segment, and
- the web page requires loading no additional resources,

Write down the series of packet exchanges that will occur for your host to receive the web page. Include packets sent by your DNS server as well as control packets for TCP connection setup and teardown. You need not include any ARP packets, and you do not need to write down message/packets formats. Simple descriptions such as 'X sends a UDP segment to the HTML server on the HTTP port' are suficient. In the case of the HTTP request, clearly state the path of the file requested in the GET. **[Marks 10]**

Answer: • Client sends a DNS A request for iitp.ac.in to 8.8.8.8, using UDP port 53. • Resolver on 8.8.8.8 iterates from root server (for in) to TLD server (for ac) to ac's server (for iitpatna), finally getting the address and sending it back to the client, using UDP port 57. • Client sends TCP SYN packet to port 80, dest IP address returned by resolver • Server sends SYN-ACK, client completes three way handshake with ACK, sends GET re- quest as TCP data. The GET request is for /dept/cse.html. • Server sends back web page. If the client requests a persistent connection, the server keeps the socket open until the timeout. Otherwise, the server closes its sending end of the connection, sending a FIN packet.

Q(7) (a) List three services provided by TCP that are not provided by UDP. **[Marks 3]**

Answer: Reliability, In-order delivery, Congestion control and others (NOT port numbering, since UDP provides that as well) (1 POINT EACH UP TO 3 CORRECT RESPONSES)

(b) Give two examples of similarities between TCP and UDP. **[Marks 2]**

Answer- both are transport-layer protocols - both use 16-bit port numbers in headers for TL multiplexing - both use 16-bit Internet checksum in headers for error detection - both allow variable size segments (up to 64 KB)

(c) For each of the following applications, indicate whether you believe TCP or UDP would be more appropriate, and briefly explain why.Any assumptions you are making for each application should be stated. **[Marks 5]**

• Streaming video client/server.
• Multiplayer online first-person shooting game.
• IRC (chat) client/server.
• Internet telephony voice channel.
• A protocol designed to synchronize the clocks of computers over a network, what protocol should be used for packets exchanged to identify time differences?.

Answer: • Streaming video client/server Answer: UDP – reliability is not needed, but a guaranteed transfer rate is. UDP will give a higher-quality transmission if there are limited net- work resources..
• Multiplayer online first-person shooting game Answer: Probably UDP – reliability is needed here, but so is low latency. A case could be made for both, but many games use UDP in order to achieve the low latency..
• IRC (chat) client/server Answer: Definitely TCP – reliability, in-order delivery are needed, and band- width/latency guarantees are not..
• Internet telephony voice channel Answer: UDP – Same as answer to streaming video: reliability is not needed, but a guaranteed transfer rate is. UDP will give a higher-quality transmission if there are limited network resources..
• A protocol designed to synchronize the clocks of computers over a network, what protocol should be used for packets exchanged to identify time differences? Answer: Most likely UDP: designed particularly to resist the effects of vari- able latency. (NTP uses UDP.) TCP will incur additional overhead and becomes harder to synchronize the clock.

Q(8) Using the following criteria, compare and contrast Go-Back-N and Selective Repeat. **[Marks 6*2+1*3=15]**

(1) Comment on the interpretation of the Acknowledges being different?
(2) Comment on the interpretation of timeout being different?
(3) How is the number of timers required at the sending node being different?
(4) Comment on the memory requirement at the receiving node being different?
(5) Comment on the actual amount of packets in-flight being different?
(6) Comment on the amount of packet retransmission being different?
(7) Let's say we are aware that the majority of packet losses on the Internet are caused by congestion, and that during periods of congestion, successive packets frequently end up being completely lost as a result of buffer overflow at the intermediate routers. Which is more effective for the Internet, G-Back-N or Selective Repeat? Then why?

Answer:-Sample Solution: (1) GBN: accumulative ack, acking for all packets with lower sequence number SR: individual ack, acking for a specific packet each (2) GBN: a timeout means a whole window of packets are lost. Retransmit from the beginning of the window SR: a timeout means a specific packet is lost. Retransmit only the packet (3) GBN: 1 per window SR: 1 per packet in window (4) GBN: no need SR: the window size to be safe. Not-in-sequence packets need to buffered until the gaps are filled to ensure ordering to the application layer (5) GBN: the whole window SR: could be only a part of the window. The window base does not advance unless the lowest in-sequence unacked packet is acked (6) GBN: each timeout triggers retransmission from the beginning of the window. Some of the packets might actually have arrived but will be retransmitted anyway SR: retransmission will only happen to packets that are truly lost. (7) Your choice. Whatever reason justifies your choice. (For example: I choose GBN. GBN is better in terms of criteria compared in (3)(4)(5) and worse in (6). However if the network tends to drop packets consecutively, then GBN will not retransmit redundant packets too much, which means the problem in (6) is less critical and yet has the advantages in (3)(4)(5). Therefore, GBN is more suitable for the Internet.)

Q(9) Define each phrase and spell out the main distinction(s) between the two for each of the technical term pairings below. Be succinct and clear. If you're unsure about your definition, feel free to add a pertinent example. **[Marks 3*3+1=10]**

(a) 'circuit-switched' and 'packet-switched'.
Circuit-switched: traditional telephone network design; end-to-end call setup; single path for duration of call; switches maintain important state about calls; dumb devices at network edge; all the smarts are in the network core. Packet-switched: data network design for Internet; data is split into packets, which are independently addressed and routed through the network; simple core; routers maintain minimal state about active calls; smarts are at network edge.
(b) 'client-server' and 'peer-to-peer'.
Client-server: traditional paradigm for network applications; server is special and well-resourced; clients are simple and numerous; client requests service from the server. Example: World Wide Web Peer-to-peer: alternative paradigm for network applications; all nodes are equal; each node can function both as a client (requesting service or resources) and as a server (providing service or resources). Example: BitTorrent.
(c) 'positive ACK' and 'negative ACK'.
Positive ACK: a control packet that conveys "good news" about the successful delivery of data; used in the PNA protocol for RDT. Negative ACK: a control packet that conveys "bad news" about the unsuccessful delivery of data; used in the PNA protocol for RDT to indicate corrupted data. Key difference: ACK triggers new data, while NAK triggers retransmission.
(d) What is the 4 tuple identifier for a TCP connection?

Q(10) The following is a dump of a UDP header in hexadecimal form: 08 12 00 1F 00 1C E2 17. What is the

(A) Source port number

(B) Destination port number

(C) Total length of the UDP

(D) Length of tha data

(E) Considering that an IP frame can have a maximum total length of 65 535 bytes, what is the maximum length of the data in a UDP frame?

Provide your answers in decimal format. **[Marks 2*5=10]**

Solution: The UDP header has four parts, each of two bytes. That means we get the following interpretation of the header. (a)Source port number = 0812 Hex = 2066 (b)Destination port number = 001F-Hex = 31 (c)Total length = 001C16 = 28 bytes (d)Since the header is 8 bytes the data length is 28 - 8 = 20 bytes. (e)The IP header is minimum 20 bytes, which gives the maximum payload 65515 bytes. To fit a UDP frame in this with header of 8 bytes we get data 65515-8 = 65507 bytes.

Q(11) DNS uses two methods for resolving host names to IP address. What are those? Resolve the URL cse.iitp.ac.in using both the methods and show a diagram for both the methods indicating relevant numbers on the edge. **[Marks 10]**
Ans: Two diagrams with numbers

Q(12) **Ans** 1) A set of rules that governs internet is called protocol. TRUE
2) A document that uses HTTP is called a web page. TRUE
3) A computer is identified by 64 bit IP address. FALSE
4) Every object on the Internet has a unique URL. TRUE
5) TCP is a connection oriented protocol. TRUE
6) UDP is a connection oriented protocol. FALSE
7) UDP is a connectionless protocol. TRUE
8) PING checks if a computer is connected to a network or not. TRUE
9) IMAP, SMTP, POP3 are all email protocols. TRUE
10) HTTP is a secure protocol. FALSE