Solutions to the Questions- Week 2

Q1) Why is SMTP not used for transferring e-mail messages from the recipient's mail server to the recipient's personal computer?

Answer: SMTP is a push protocol; the task of transferring e-mail messages from the recipient's mail server to the recipient's personal computer is a pull operation.

Q2) Why do you think DNS uses UDP, instead of TCP, for its query and response messages?

Answer: TCP involves a connection establishment phase while UDP does not. Using TCP for DNS may end up involving several TCP connections to be established since several name servers may have to be contacted to translate a name into an IP address. This imposes a high overhead in delay that is acceptable for larger transfers but not acceptable for very short messages such as DNS queries and responses. In addition, UDP affords a smaller packet size and also imposes a smaller load on name servers due to its simplicity in comparison to TCP.

Q3) Suppose you are sending an email from your Hotmail account to your friend, who reads his/her e-mail from his/her mail server using IMAP. Briefly describe how your email travels from your host to your friend's host. Also, what are the application-layer protocols involved?

Answer: Message is sent from your host to your mail server over HTTP. Your mail server then sends the message to your friend's mail server over SMTP. Your friend then transfers the message from his/her mail server to his/her host over IMAP.

Q4) How can iterated DNS queries improve the overall performance?

Answer: Iterated request can improve overall performance by offloading the processing of requests from root and TLD servers to local servers. In recursive queries, root servers can be tied up ensuring the completion of numerous requests, which can result in a substantial decrease in performance. Iterated requests move that burden to local servers, and distributed the load more evenly throughout the Internet. With less work at the root servers, they can perform much faster.

Q5) Suppose within your Web browser you click on a link to obtain a web page. The IP address for the associated URL is not cached in your local host, so a DNS look-up is necessary to obtain the IP address. Suppose that *n* DNS servers are visited before your host receives the IP address from DNS; the successive visits incur an RTT of RTT_1, ..., RTT_n. Further suppose that the web page associated with the link contains exactly one object, consisting of a small amount of HTML text. Let RTT_0 denote the RTT between the local host and the server containing the object. Assuming zero transmission time of the object, how much time elapses from when the client clicks on the link until the client receives the *object*?

Answer: The total amount of time to get the IP address is $RTT_1 + RTT_2 + ... + RTT_n$.

Once the IP address is known, RTT_O elapses to set up the TCP connection and another RTT_O elapses to request and receive the small object. The total response time is

$2RTT_0 + RTT_1 + RTT_2 + ... + RTT_n$.

Q6) Which protocol – Go-Back-N or Selective-Repeat - makes more efficient use of network bandwidth? Why?

Answer: Selective repeat makes more efficient use of network bandwidth since it only retransmits those messages lost at the receiver (or prematurely timed out). In Go-Back- N, the sender retransmits the first lost (or prematurely timed out) message as well as all following messages (without regard to whether or not they have been received).

Q7) Consider a reliable data transfer protocol that uses only negative acknowledgements. Suppose the sender sends data only infrequently. Would a NAK-only protocol be preferable to a protocol that uses ACKs? Why? Now suppose the sender has a lot of data to send and the end-to-end connection experiences few losses. In this second case, would a NAK-only protocol be preferable to a protocol that uses ACKs? Why?

Answer: In a NAK only protocol, the loss of packet x is only detected by the receiver when packet x+1 is received. That is, the receiver receives x-1 and then x+1, only when x+1 is received does the receiver realizes that x was missed. If there is a long delay between the transmission of x and the transmission of x+1, then it will be a long time until x can be recovered, under a NAK only protocol.

On the other hand, if data is being sent often, then recovery under a NAK-only scheme could happen quickly. Moreover, if errors are infrequent, then NAKs are only occasionally sent (when needed), and ACK are never sent – a significant reduction in feedback in the NAK-only case over the ACK-only case.

Q8) If the RTT from London to Cape Sydney is 120ms and all links in the network have a 155 Mbits/second data-rate, how much data can fit in the "pipe"? Hint: Bandwidth Delay Product. Express your answer in bytes.

Answer: Bandwidth Delay product BDP = 155 Mbits/sec * 120 ms = 18.6 x 10^6 bits = 2,325,000 bytes will fit in the pipe.

Q9) Is it possible for an application to enjoy reliable data transfer even when the application runs over UDP? If so, how?

Answer: Only if the application itself implements reliability measures, such as ACK, retransmission, timer, etc.

Q10) Consider a TCP connection between Host A and Host B. Suppose that the TCP segments travelling from Host A to Host B have source port number x and destination port number y. What are the source and destination port numbers for the segments travelling from Host B to Host A?

Answer: The port numbers are swapped. They would become source port: y and destination port: x for segments travelling from Host B to Host A.

Q11) Suppose that the UDP receiver computes the Internet checksum for the received UDP segment and finds that it matches the value carried in the checksum field. Can the receiver be absolutely sure that no bit errors have occurred? Explain. Would things be different with TCP?

Answer: No, the receiver cannot be absolutely certain that no bit errors have occurred. This is because of the manner in which the checksum for the packet is calculated. If the corresponding bits (that would be added together) of two 16-bit words in the packet were 0 and 1 then even if these get flipped to 1 and 0 respectively, the sum still remains the same. Hence, the 1s complement of the sum the receiver calculates will also be the same. This means the checksum will verify even if there was transmission error. Since TCP uses the same 16 bit Internet checksum mechanism, the above would hold true with TCP as well.

Q12) In protocol rdt3.0, the ACK packets flowing from the receiver to the sender do not have sequence numbers (although they do have an ACK field that contains the sequence numbers of the packet they are acknowledging). Why is that the ACK packets do not require sequence numbers?

Answer: To best answer this question, consider why we needed sequence numbers in the first place. We saw that the sender needs sequence numbers so that the receiver can tell if a data packet is a duplicate of an already received data packet. In the case of ACKs, the sender does not need this info (i.e., a sequence number on an ACK) to detect a duplicate ACK. A duplicate ACK is obvious to the rdt3.0 sender, since when it has received the original ACK it transitioned to the next state. The duplicate ACK is not the ACK that the sender needs and hence is ignored by the rdt3.0 sender.