CS425: Computer Networks
Mid Semester Exam
September 23, 2017

Duration: 2 hours Max: 50 marks

Please note the following:

- Any act of academic dishonesty may lead to award of an 'F' grade.
- You should not be carrying your mobile phone, not even in switched off mode.
- It is a closed-book exam. You cannot refer to your notes or any other material.
- Please try to answer questions in sequence. That will help me in grading.
- You must use a blue/black pen to answer questions. In particular, answers written with a pencil will not be graded.
- I don' expect you to exactly remember the names of the fields in a protocol header, or the overall structure. So referring to functionality of those fields is just fine.

1. In the following questions, give a brief answer. **8 marks**

   (a) I want to indulge in a DOS (Denial-of-service) attack on a victim machine using DNS service. Would arrange to send a large number of DNS requests with a from address of the victim node. and the victim node will be overwhelmed with DNS responses. My intention is to ensure that the requests sent are as few as possible, but the number of bytes that the victim receives is as large as possible. What kind of DNS requests I could use.

   (b) Assume all nodes have a unique global IP addresses. Can I have a node in the CSE department, which is named `www.ibm.com`. If no, what would stop this from happening. If yes, how would it be known to the rest of the world. (Hint: DNS)

   (c) I want to use DNS for load balancing, say on lots of servers, all serving the site, `www.facebook.com`. What role could TTL (Time to Live) field play in this.

   (d) When I ask for the IP address ('A' type record) for `cs425.cse.iitk.ac.in`, I might get a response even though there may not be any 'A' type record in the DNS database for this domain name. How am I getting the IP address.

2. Consider the RTT Measurement option in TCP. In each of the following cases what would be the timestamps returned in each ACK. Assume that the sender has used timestamp t1 for packet 1, and so on. Assume delayed acks are implemented. **8 marks**

   (a) Packets are received in the order: 1, 2, 3, 4

   (b) Packets are received in the order: 1, 2, 4, 3

   (c) Packets are received in the order: 1, 2, 4, 5

(d) Packets are received in the order: 1, 1, 2, 3

10 marks

3. More questions on Transport Layer.

   (a) How does a TCP entity knows whether the other side understands a new TCP option or not.

   (b) Give an example of what could go wrong if TCP were to use 2-way handshake instead of 3-way handshake.

   (c) How does a UDP recipient distinguish between the checksum being 0 and checksum not computed by sender at all.

   (d) What would be wrong with using a nanosecond clock graunlarity in the RTT Measurement option in TCP.

   (e) Why do we use TLV (Type-Lenght-Value) format for options. Why not just TV.

11 marks

4. Network Layer.

   (a) In the class, we had given an extreme example of how a routing protocol could compute unstable routes. How could we ensure stability of routing tables in Internet.

   (b) Why can't we run the standard Dijkstra or Bellman Ford algorithm to find routes across Internet. (Hint: AS) **2 marks**

   (c) Dijkstra algorithm requires broadcast of link states to all routers. How do we ensure that the broadcast does not result in infinite load on the network.

   (d) If all routers have a default entry in their routing table, then what kind of packets could face problem even if routes are correct and stable.

8 marks

5. Applications.

   (a) We visit a website, and we find that the interface or look and feel is different on the laptop and is different on the mobile phone, even though we typed the same URL in both cases. How does it happen. (Explain purely in terms of HTTP and not complicated scripts, etc.)

   (b) If we visit a web page which has 20 embedded objects, and if we were to monitor the number of TCP connections to fetch all these objects, they are not 20 (or 21, if you include the first access). What is happening.

   (c) How does an ESMTP node knows what are the SMTP extensions understood by the other side.

   (d) I am trying to access a webpage, which was cached the last time I accessed it. Some times, I see the same old page (and if I were to monitor the network, there will not be a fresh download), and some other times, I see that a new page has come. In both instances we are going to the same page, and in both instances, we did have the page in our cache. Is this a random activity of the browser.

6. How can cookies be used to monitor what all sites you are visiting on the Internet. **5 marks**

CS425: Computer Networks
End Semester Exam
November 23, 2017

Duration: 3 hours

Max: 80 marks

NAME: [redacted]

ROLL NO: [redacted]

Please note the following:

- Please do write your name and roll number on the question paper in the space above.
- This paper consists of four sheets.
- You should not be carrying your mobile phone.
- Any act of academic dishonesty, if caught, will be taken seriously, as per the course policy.
- It is a closed-book exam. You cannot refer to your notes or any other material.
- Please answer all questions in the serial order. Will make it easy for me to grade.
- The total questions are worth more than 80 marks. You may choose to attempt questions worth more than 80 marks. If you get more than 80 marks, they will be reduced to 80.

1. Explain the following types of Routing. 1 marks each

(a) Multipath Routing
(b) **Loose** Source Routing
(c) Type-of-Service Routing
(d) Inter-domain Routing
(e) Hot-potato or Deflection Routing

2. Consider a TCP connection which implements Slow Start, Congestion Avoidance, and Delayed Ack. A data packet takes one millisecond to transmit. One way delay in reaching the destination is 50 ms (not counting the transmission time at source). Transmission of ACK

takes negligible time, but takes 50 ms delay to reach back the source. The timer for waiting for the second data packet before sending an in-sequence ACK is 2 ms.

Show when each data packet will be transmitted, assuming that the first one begins transmission at t = 0 ms. Show all data packets till there are four data packets in transit. **4 marks**

Hint: More than 4 packets will be transmitted.

3. What all processing happens to a message in PGP. Preferably use a figure. **4 marks**

4. When I type in a URL in the browser, and start wireshark at the same time. What all packets am I likely to see. Assume that the webpage is very small, and will fit into one response HTTP packet. **4 marks**

5. In the following questions, the answer may need some explanation. **3 marks each**

   (a) Earlier Ethernet (10Base5) used an encoding scheme called "Differential Manchester" which ensured that there was a transition in every bit. Design an encoding scheme which will ensure that there is at least one transition in every 4 bits.

   (b) Consider a 1 Gbps network connecting two nodes with a round-trip time of 100 milliseconds. Assume 20 percent of the network capacity is used by various headers, gaps between successive packets and other overheads.

   What is the maximum rate at which data can be transmitted from one node to the other assuming no Window Scale option and a WS option with a large value. Assume there is no packet loss.

   (c) In Public-key cryptography, if host A is sending a message to host B, how should the message be encrypted so that it provides integrity, privacy, authentication and non-repudiation.

   (d) What is the difference between a multi-port repeater (or a hub) and a switch.
   Difference between a switch and a router.
   Difference between an amplifier and a repeater.

   (e) Explain ASK, FSK, and PSK.

   (f) What are the following timers used for in DHCP.

      i. Lease renewal
      ii. Lease rebinding
      iii. Lease expiry

   (g) We can't keep adding repeaters to extend Ethernet, there is a limit of 4 repeaters between any two nodes. Why such a limit.

   But we can extend the Ethernet if we connect two segments with a switch. Why is the above limit not applicable to a switch.

   We can't have the entire Internet based on connecting networks by switches (at least not with today's technology). What could be a limiting factor (or what do routers do that switches do not).

   (h) In Random Early Drop variant where there is no drop but just warning to the source about a possible congestion building up, how/when are the two unused bits in IP header of ToS field used.

6. In the following questions, the answer is at most a few lines. **2 marks each**

(a) The minimum Ethernet packet size (assume 10Base5) is 64 bytes. If a transmitter is noticing collision for the 4th time, what is the maximum backoff (in time) it will face for the next attempted transmission of the same packet.

(b) Why is error checking done at multiple layers.

(c) If a TCP source receives Selective ACK for a packet, it cannot delete that packet from its buffers, and must wait for the good old cumulative ACK. What purpose does SACK option serve?

(d) Why can we use NRZ encoding to store bits on a disk, but not to code bits on a wire to send to another node.

(e) In TCP, we monitor the round-trip time of only one packet at a time. (Assuming that we are not using RTTM Option.) Suppose the packet which was being monitored got lost and had to be retransmitted. When it is finally acknowledged, will we consider RTT as the time from 1st transmission or the 2nd transmission. Why?

(f) Is a `bind()` call necessary for server software. Why?
How about client software.

(g) What does Cyclic Redundancy Checksum (CRC) cover in a TCP packet.

(h) Assume an MTU of 600 bytes for an outgoing link at a router. There is an incoming IP packet of 1200 bytes (including IP header of 20 bytes). What will be the sizes of various fragments of this packet.

(i) What is the total number of valid IP addresses that can be assigned to nodes in the Internet. Assume that all networks can have as many nodes as the number of addresses in that network. Assume there are no private addresses.

(j) A router acting as a firewall is called a filtering router as it filters (allows or drops) incoming/outgoing packets based on some information in the packet. Name five fields that a filtering router can look at for firewall purposes.

(k) How can ARP be used to detect if there is another machine on my subnet that is using the IP address assigned to my machine.

(l) How does Token Bus handle a single node going down and breaking the virtual ring.

(m) Explain the process of removing an orphaned packet in Token Ring. (That is, the source goes down after transmission of packet.)

(n) What all system calls are called by a server of a connection-oriented application. Please use only Socket programming system calls in C.

7. In the following questions, the answer is very short. **1 mark each**

(a) Ethernet has a 8-byte preamble, whose purpose is to ensure that the receiver hardware is ready and its clock is synchronized to the sender's clock. If the receiver's hardware will take some time to get ready during which an unknown number of bits have been received (and lost), how will it know when the 8-byte preamble is over.

(b) A 160-bit address in IPv6 would have enabled it to have the same addressing size as ATM and OSI's Network layer protocols, making it easier to inter-operate. Why did we not accept that size.

(c) In 1970s, General Motors was interested in developing a protocol stack for factory automation in which all machines on the assembly line would be connected by a LAN. The research led to MAP (Manufacturing Automation Protocol). For its MAC layer,

GM chose Token Bus, instead of Ethernet, which was the dominant standrd of the time.

Can you guess why Token Bus was chosen ove Ethernet?

(d) In WiFi MAC, we used CSMA/CA (RTS/CTS messages with the time of transmission mentioned). Under what condition would the CA part be reduntant. (CD part may still remain a problem.)

(e) In TCP, a source can retransmit a packet even before the retrasmission time expires. Under what condition?

(f) In order to avoid reflection attack, we want to ensure that a random number used in one direction can not be used in another direction. Give one way to do so.

(g) The network utility, *ping*, operates as follows: You send a packet and the destination replies. From the replies, you can know which packets were received and which were not and you can also estimate the round trip times of packets which were replied to.

What type of message is used in this utility.

(h) To be able to detect collision in a CSMA/CD network, a minimum packet size is specified. When we moved from a 10Mbps Ethernet to a 100Mbps Ethernet, the minimum packet size should have become 10 times, keeping all other parameters constant. But it didn't happen this way. The minimum packet size remained the same. What changed?

(i) There is a folklore regarding "Net 10." The erstwhile ARPAnet was assigned IP addresses of the type, **10.0.x.y**. As ARPAnet stopped functioning, the IP address range became available for Private IP addresses. What class of network was ARPAnet.

(j) There is a transient routing loop (which can happen because the routing table updates are not synchronized and information that each router has is different). A packet is going around in this loop. For how long will the packet keep moving in this loop.

(k) What is the drawback of TCP when it comes to supporting a transaction oriented application.

(l) In a sliding window protocol, a receiver is allowed to store at most two out-of-sequence packets. That is, if the receiver is expecting a packet with sequence number x, the receiver can buffer packets numbered $x+1$ and $x+2$. If the sequence number is 4 bits, what is the maximum send-window size.

(m) Two nodes are communicating using TCP. The receiver crashes and reboots within a few seconds. The sender does not get ACKs and has retransmitted packets while the receiver was rebooting. How will the source eventually realize that it has only a half-open connection.

(n) I want to know the IP addresses of all the routers that the packet will pass through. Record Route Option was defined just for this purpose. But it does not work. What is the limitation.

(o) What functionality (other than error checking) is implemented at multiple layers of network protocols.

(p) What is coding violation.

(q) Why can we not have a protocol purely based on negative ACKs. Why do we must have some form of positive ACKS in a protocol for reliability.

(r) When a router sends an ICMP error message to a source, how does the source know which connection did the dropped packet belong to.

(s) Why is it that a fragmented IP packet is not re-assembled by the next router.