CS144 Practice Midterm
Fall 2010

*Note: This practice midterm only covers a **subset** of the topics you are required to know.*

Question 1:

Suppose you are writing a file copy program in TCP. You send a TCP packet with the length of the file, then send packets with 1459 bytes of the file at a time. After you see an end of file, the receiver sends you a checksum to verify the file.

You then switch to sending packets with 1460 bytes of the file at a time instead and notice a huge performance improvement. You are sending the data over an Ethernet connection, which can accept 1500 byte payloads. What may be happening?

Question 2:

Route flapping has the potential to adversely affect which of the following TCP algorithms? Circle all that apply, if any.

a) RTT estimation
b) Flow control
c) Fast retransmit/recovery
d) Path MTU discovery

Question 3:

Alyssa P. Hacker issues a traceroute from her machine to another machine, bmistree.stanford.edu, and gets the following output:

bmistree@bcoli:~$ traceroute bmistree.stanford.edu

traceroute to bmistree.stanford.edu (128.12.180.59), 30 hops max, 60 byte packets
1 yoza-vlan376.Stanford.EDU (171.67.76.2) 0.387 ms 0.515 ms 0.591 ms
2 bbra-rtr.Stanford.EDU (172.20.4.1) 0.601 ms 0.704 ms 0.754 ms
3 coza-rtr-22.SUNet (172.20.2.17) 0.557 ms 0.660 ms 0.680 ms
4 172.20.10.35 (172.20.10.35) 0.939 ms 0.527 ms 0.981 ms
5 bmistree.Stanford.EDU (128.12.180.59) 1.791 ms ***1.456 ms*** 1.778 ms

Intrigued, Ben Bitdiddle asks Alyssa what the highlighted number means. Alyssa responds, "It means that it took a packet .728 ms to get to bmistree.stanford.edu and .728 ms bmistree.stanford.edu's packet to come back to my machine.

Ignoring the time it took for bmistree.stanford.edu to internally process the traceroute packet and generate a response, is there anything wrong with Alyssa's statement?

Question 4:

The OSI model conceptually separates networking into 7 different layers: the physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer.

Give an example from a protocol that we have discussed that violates the strict separation of layers.

Question 5:

Roughly speaking, the end-to-end principle states that protocol operations should occur as much at the edges of the network as possible. Give an example from a protocol we discussed that violates the end-to-end principle.

Question 6:

Which of these organizations currently set policy for Internet related matters in the United States:

a) FCC
b) FTC
c) FDIC
d) NSF

Question 7:

TCP guarantees fairness between:

a) Flows
b) Applications
c) End hosts.
d) Autonomous systems

Question 8:

We have seen that TCP has a number of features that UDP does not. For each of the following problems that can occur in IP networks, explain how TCP supports reliable delivery.

1. Dropped packets
2. Duplicated packets
3. Reordered packets

Question 9:

Curious to learn about the Internet's internals, Ida Investigator writes a simple program to send large UDP datagrams from office in Gates to her home machine. She runs a simple listening server on her home machine and opens Wireshark to observe the traffic. She notices something strange: when she sends a UDP datagram with a payload of size 4432 bytes, it arrives as three IP fragments at her home machine. Each delivered IP fragment is exactly 1500 bytes, including headers.

Part a:
Why does Ida's datagram get split up?

Part b:
If Ida were to repeat her experiment between a different pair of computers, would she necessarily get the same fragmentation? If so, explain what is special about the value 1500. If not, describe a way to programmatically determine the IP fragment size.

Part c:
Suppose the route between Ida's office and home is congested and one of the three fragments gets dropped somewhere in the network. Ida's home computer receives the other two fragments. Will her large UDP datagram be delivered to the listening server? Why or why not? Assume no fragments are duplicated.

Part d:
The UDP header is 8 bytes. From this data, calculate the IP header size.

Question 10:

Recall that the *active closer* enters the TIME_WAIT state for a period of time before a TCP connection is considered closed. Describe the significance of the TIME_WAIT state and give an example of what go wrong if both sides entered the CLOSED state immediately after ACKing each other's FIN.

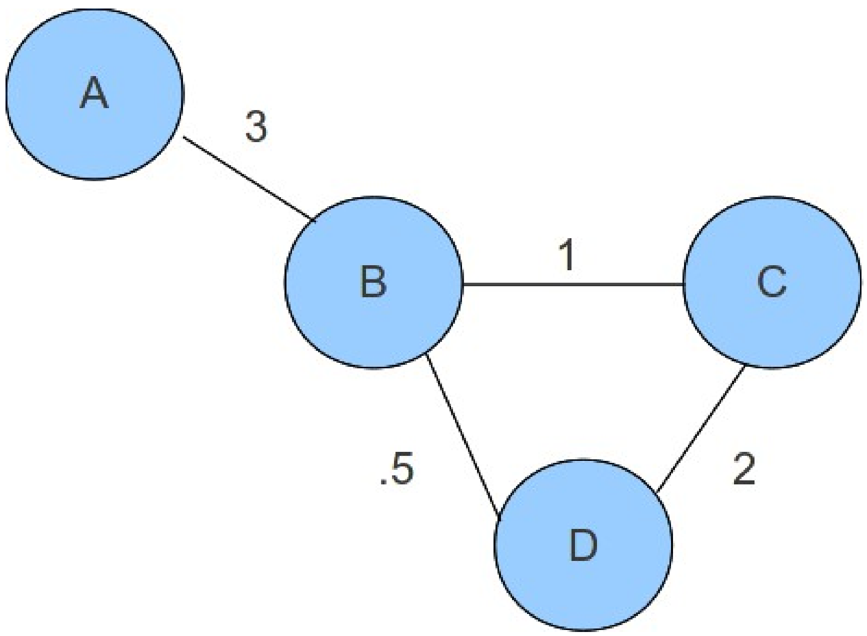
Question 11:

Host A is connected to host B with a 100 Mbps link that has a 100 ms one-way latency. How much data can A send to B before B's first acknowledgement reaches A?

Question 12:

What problem did CIDR seek to solve?

Question 13:



What routes do A, B, and C advertise for

Part a:
Split horizon;

Part b:
Split horizon + poison reverse?

Question 14:

Without window scaling, TCP allows window sizes to grow up to 65,535 bytes long.
Part a:
What is the motivation for such large window sizes? When would they be useful?

Part b:
If a receiver receives a packet with a higher sequence number than the one expected, but still within a window size away, what happens to that packet?

Part c:
Can you think of a potential security issue that might arise from having very large window sizes? (Hint I: What if an adversary can create a packet to any destination that appears from any destination? Hint II: Think RST packets.)

Question 15:

In TCP's congestion control mechanism, what is the purpose of 1) slow start and 2) congestion avoidance?