UNIVERSITÉ YORK UNIVERSITY

Department of Computer Science and Engineering

CSE 3214: Computer Network Protocols and Applications

Final Examination

Instructor: N. Vlajic
Date: April 15, 2011

Instructions:

- Examination time: 180 min.
- Print your name and CS student number in the space provided below.
- This examination is closed book and closed notes. Use of calculators is allowed.
- There are 9 questions. The points for each question are given in square brackets, next to the question title. The overall maximum score is 100.
- Answer each question in the space provided. If you need to continue an answer onto the back of a page, clearly indicate that and label the continuation with the question number.

FIRST NAME: ______________________________

LAST NAME: ______________________________

STUDENT #: ______________________________

Question	Points
1	/ 10
2	/ 10
3	/ 12
4	/ 10
5	/ 16
6	/ 12
7	/ 9
8	/ 14
9	/ 7
Total	/ 100

1. Multiple Choice, True/False [10 points]

1.1) Multiple choice questions – each question is worth [1 point].

a) What is the limited broadcast address corresponding to the node with the following IP address: 131.15.46.59?

(a) 131.15.46.255

(b) 131.15.255.255

(c) 255.255.255.255

(d) None of the above.

b) In hexadecimal colon notation, a 128-bit long IPv6 address is divided into _____________ sections, each comprising _____________ hexadecimal digits

(a) 4 : 2

(b) 8 : 4

(c) 16 : 2

(d) none of the above

c) An ARP reply is normally _____________ .

(a) broadcast

(b) multicast

(c) unicast

(d) none of the above

d) When the hop-count field in an IP packet reaches zero and the destination has not been reached, an ICMP _____________ error message is sent back to the sending machine.

(a) destination-unreachable

(b) time-exceeded

(c) parameter-problem

(d) none of the above

e) Which statement(s) is true regarding the advantages of static over dynamic routing?

(a) reduces the probability of packet drop due to router (i.e. route) failures

(b) easier to implement and maintain in large, complex networks

(c) increased security

(d) none of the above

f) A port address in UDP is ____________ bits long.

(a) 8

(b) 16

(c) 32

(d) none of the above

g) The ports ranging from 1,024 to 49,151 are called ____________ .

(a) well-known

(b) dynamic

(c) registered

(d) none of the above

h) In TCP, Clark's solution can solve the silly window syndrome created by the ____________ .

(a) sender

(b) receiver

(c) both sender and receiver

(d) none of the above

i) The ____________ utility allows you to query the DNS database from any computer on the network and find the host name of a device by specifying its IP address, or vice versa?

(a) ipconfig

(b) tracert

(c) nslookup

(d) netstat

j) A user needs to send the server some information. The request line method is ____________ .

(a) GET

(b) HEAD

(c) SEND

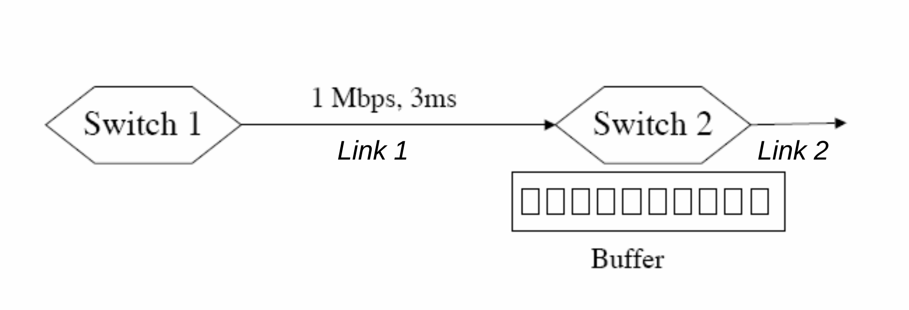
(d) POST

2. Packet Switching [10 points]

Consider two serially connected packet switches as shown in the figure below. The link connecting the two switches (*Link 1*) is full-duplex, with datarate of 1 Mbps and propagation delay of 3 ms (in each direction). The packets sent through the network are 1000 bits long. The input buffer/queue of Switch 2 can store at most 100 packets.

To control congestion and avoid packet loss, the switches employ the so-called ‘back pressure’ mechanism. According to this mechanism, whenever Switch 2 detects congestion on its outgoing link (i.e., no more packets can be sent over *Link 2*), Switch 2 sends a signal back to Switch 1 instructing Switch 1 to halt further packet transmission over *Link 1*.

In this question, you are asked to determine how big Switch 2 should let its buffer grow (in case of congestion on *Link 2*), before sending a back pressure signal to Switch 1. Your answer should be in the units of ‘packets’.



Additional assumptions:

- There is an unlimited number of packets at Switch 1; therefore, when active, Switch 1 sends packet continuously, back-to-back.
- Once detected, the congestion on *Link 2* could be alleviated at any point in time. Hence, the back pressure signal should not be sent too early (unless there is a real risk of Switch 2 running out of buffer space), nor too late (no packet should ever be lost/dropped).

SOLUTION:

Let us first assume that Switch 2 waits for its buffer to get 100% full before sending the back pressure signal to Switch 1. In this case, all those packets already in transit as well those generated by Switch 1 within the time it takes for the back pressure signal to arrive to Switch 1, will be lost.

The actual number of such (lost) packet would be:

$$\text{packets in transit} + \text{packets generated} = 2 * \frac{t_{\text{propagation}}}{t_{\text{transmission}}} = 2 * \frac{t_{\text{propagation}}[\text{sec}]}{\frac{\text{P [bits[}}{\text{R [bps]}}} = 2 * \frac{3 \cdot 10^{-3}\ [\text{sec}]}{\frac{1000\ [\text{bits}]}{1 \cdot 10^{6}\ [\text{bps}]}} = 6\ [\text{packets}]$$

Thus, to prevent packet loss, yet allow its buffer to grow to maximally allowable size, Switch 2 needs to send the back pressure signal at the time when it has just enough space to absorb the packets that will be in transit or generated during the time the back pressure signal is propagating back to Switch 1.

Accordingly, Switch 2 should let is buffer grow to the size of 94.

3. NAT and IPv6 [12 points]

3.1) [3 points] Assume an IP packet carrying an HTTP request is going from a local (i.e. home) area network onto the wider Internet through a NAT router. Name all header fields that the NAT router needs to change in the given packet? Explain your answer.

(Hint: encapsulation as well as the syntax/semantics of all involved protocols must be taken into consideration.)

SOLUTION:

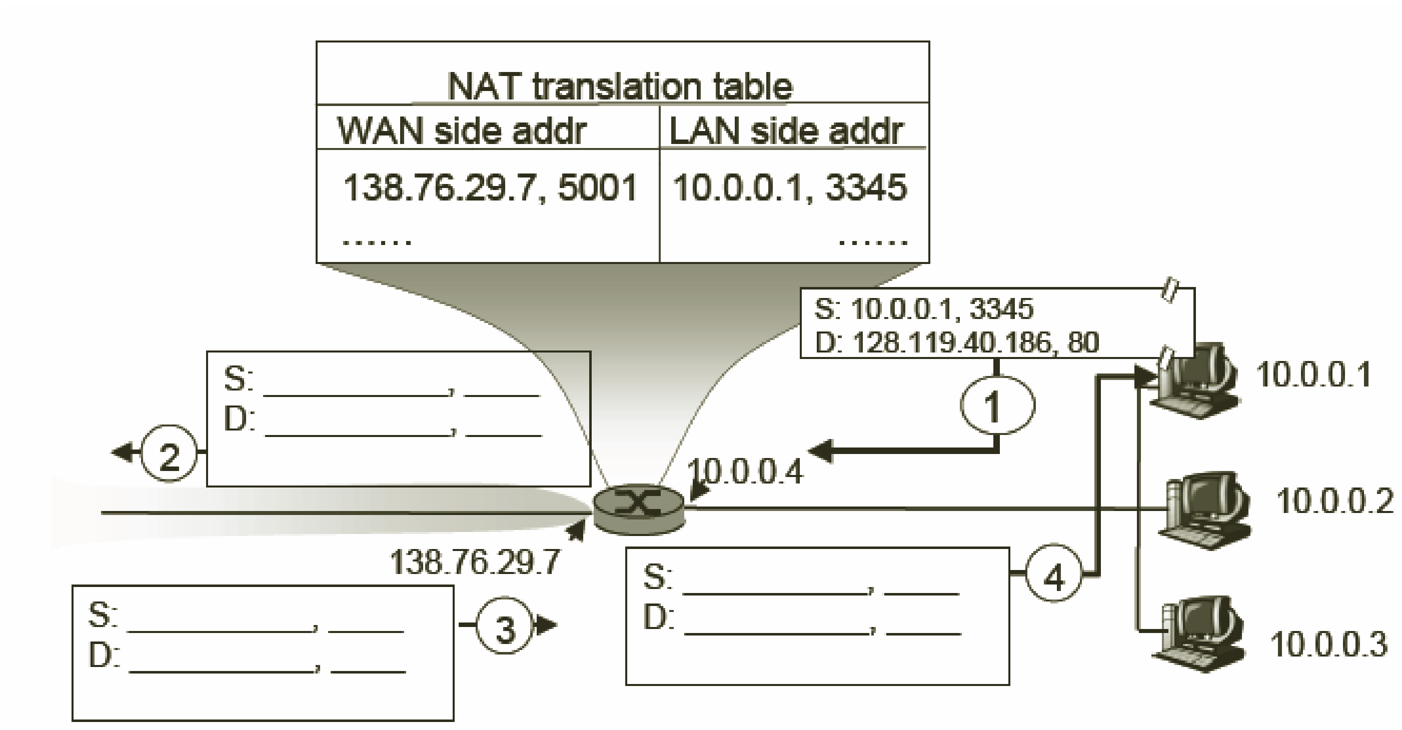
It is very much clear from 3.1) that one IP and TCP header field need to be changed:

1) the source IP address,
2) TCP source port number.

The change in the value of these two parameters implies that the following two fields also need to be changed:

3) IP checksum
4) TCP checksum

3.2) [3 points] The diagram below shows a packet traveling through a NAT router. Packet 1 is sent from the internal host (S) to the NAT router, packet 2 is sent from the NAT router to the external web server (D), packet 3 is received from the web server by the NAT router, and packet 4 is sent by the NAT router to the original host.
Fill in the missing source and destination IP addresses and port numbers in packets 2-4.



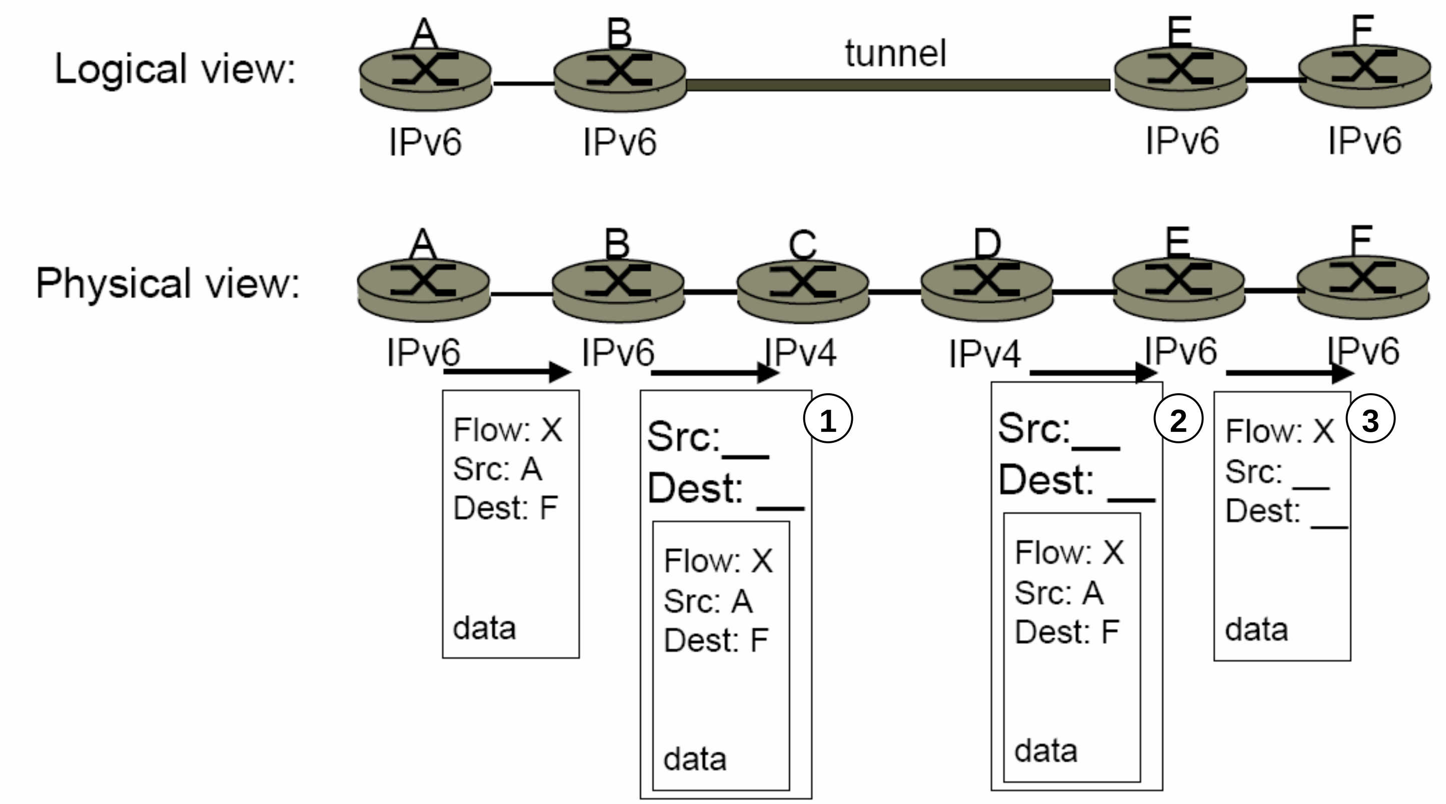
NAT translation table

WAN side addr	LAN side addr
138.76.29.7, 5001	10.0.0.1, 3345
……	……

SOLUTION:

P2:	S=138.76.29.7, 5001	D=128.110.40.186, 80
P3:	S=128.110.40.186, 80	D=138.76.29.7, 5001
P4:	S=128.110.40.186, 80	D=10.0.0.1, 3345

3.3) [3 points] The diagram below shows an IPv6 packet tunnelled over IPv4. Fill in the missing source and destination addresses at places/packets marked 1, 2, and 3.



SOLUTION:

1:	S=B	D=E
2:	S=B	D=E
3:	S=A	D=F

3.4) [3 points] Name two modifications of IPv6, from the IPv4, that allow a router to process a packet quicker.

SOLUTION:

1: fixed header length / better header format
2: no packet fragmentation at routers
3: no checksum

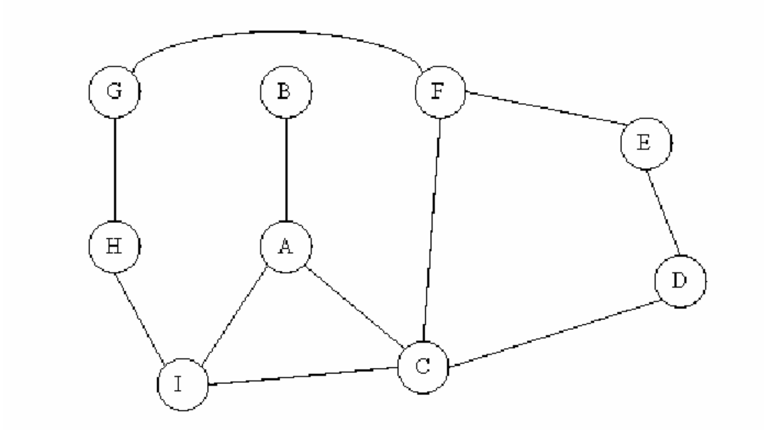
4. Routing [10 points]

4.1) [3 points] What are the differences between routing and forwarding? Briefly explain each of them.

SOLUTION:

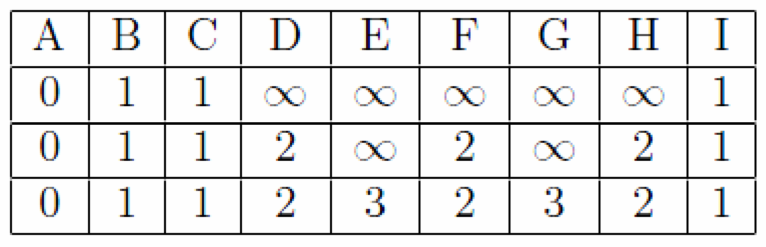
forwarding: move packets from router’s input to appropriate router output.
routing: determine route taken by packets from source to destination.

4.3) [7 points] Consider the network configuration shown in figure below. Assume that each link has the same cost.



a) Run Bellman-Ford algorithm on this network to compute the routing table for node A. Show A's distance to all other nodes at each step.

SOLUTION:



A	B	C	D	E	F	G	H	I
0	1	1	∞	∞	∞	∞	∞	1
0	1	1	2	∞	2	∞	2	1
0	1	1	2	3	2	3	2	1

b) Suppose the link A-B goes down. As a result, A advertises a distance of infinity to B. Describe in detail a scenario where C takes a long time to learn that B is unreachable

SOLUTION:

A advertizes a distance of infinity to B, but, C and I advertize a distance of 2 to B. Depending on the ordering (i.e. timing) of these messages, this might happen: I upon knowing that B can be reached from C with distance 2, concludes that it can reach B with a distance of 3 (via C) and advertises this to A. A concludes that it can reach B with a distance of 4 (via I), and advertises this to C. C concludes that it can reach B with a distance of 5 (via A). This continues forever if the distances are unbounded. This is called the count-to-infinity problem.

5. TCP Potpourri [16 points]

5.1) [5 points] Suppose you want to send a file of size 255,000 over a 2 Mbps link using TCP. The maximum segment size (MSS), which represents the size of TCP payload, is 1,000 bytes. Two-way propagation delay between the source and the destination is 10 [msec] . TCP Threshold = 130 packets.

How long will it take to transmit the given file, from the start to the end of TCP transmission?

SOLUTION:

1st RTT – connection established
2nd RTT – window: 1 MSS => transmitted bytes: 1,000
3rd RTT – window: 2 MSS => transmitted bytes: 1,000 + 2,000 = 3,000
4th RTT – window: 4 MSS => transmitted bytes: 3,000 + 4,000 = 7,000
5th RTT – window: 8 MSS => transmitted bytes: 7,000 + 8,000 = 15,000
6th RTT – window: 16 MSS => transmitted bytes: 15,000 + 15,000 = 31,000
7th RTT – window: 32 MSS => transmitted bytes: 31,000 + 32,000 = 63,000
8th RTT – window: 64 MSS => transmitted bytes: 63,000 + 64,000 = 127,000
9th RTT – window: 128 MSS => transmitted bytes: 127,000 + 128,000 = 255,000

Delay: 9*2-way propagation + (1+2+4+8+16+32+64+128)*packet-transmissions =
= 9*0.01 [sec] + 255*1,020***8** [bits] /2,000,000 [bit/sec] =
= 0.09 + 0.10404 [sec] = 1.13 [sec]

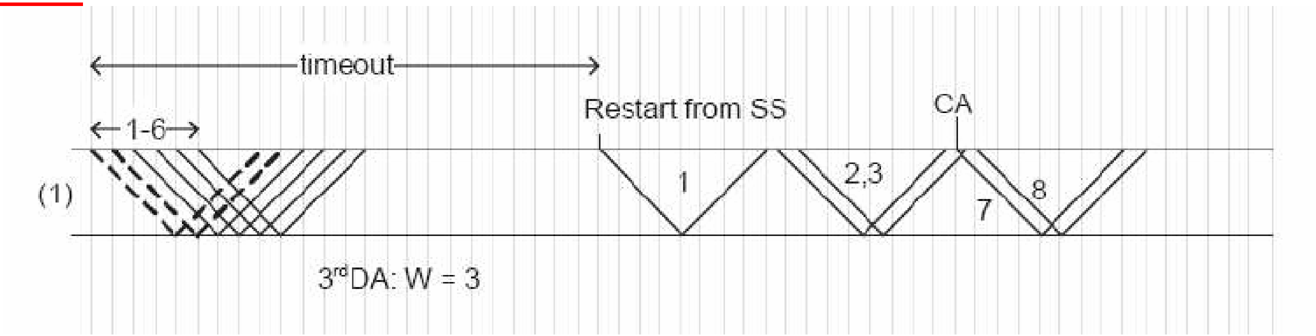
We could possibly add another 1.5 RTT for the (2-way) closing of the connection.

5.2) [6 points] Consider a TCP connection that, at time 0, is in the congestion avoidance phase with a window size equal to 6 MSS, and then sends packets {1, 2, 3, .., 6}. (The connection has sent packet before that were properly acknowledged. The packet transmission time of a single packet is $P_{transmission}$=1 sec, while RTT = 8 sec and timeout = 24 sec.) The sender does <u>not</u> implement fast retransmit and fast recovery, and after every timeout it restarts in slow start.

Now, assume packets 1 and 2 are lost. Draw a timing diagram that shows the transmission of the first 8 packets by completing the figure below. Indicate the significant events, such as start of slow start (SS), or of congestion avoidance (CA), and the relevant congestion window sizes.

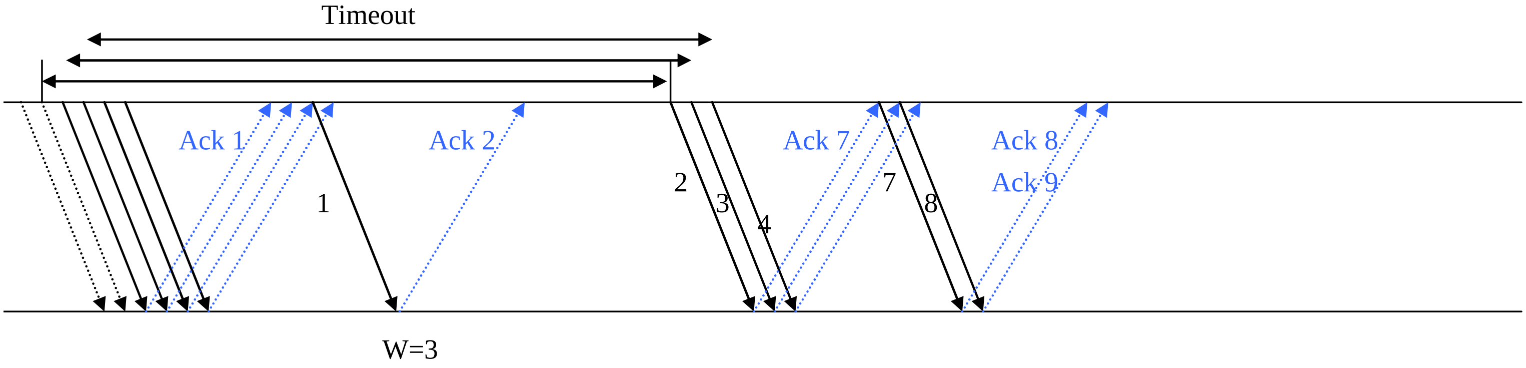
Also, calculate how long, overall, it takes to transmit those 8 packets.

SOLUTION:



5.3) [5 points] Repeat the previous problem assuming that the host now uses fast retransmit and fast recovery.

SOLUTION:



6. Socket Programming [12 points]

6.1 [2 points]

Consider the following Java application:

```
socket = new DatagramSocket(12345);
while (true) {socket.receive(packet);}
```

What happens if somebody decides to run two instances of this application on one machine and 4 UDP segments arrive at port 12345?

a) both instances of the application receive all 4 segments

b) one instance receives all 4 segments

c) some segments are received by one instance, other segments are received by the other instance

d) one instance receives segments 1 and 3, the other receives segments 2 and 4

6.2 [2 points]

Given the following lines from a Java program segment:

```
byte[] dataOut = new byte [512];
String userInput = inFromUser.readLine();
dataOut = userInput.getBytes();
```

Which of the following lines of code could be used to create a new UDP datagram packet to send the data that was provided by the user to a host identified by the InetAddress object IPAddress?

a) DatagramPacket packetToSend = new DatagramPacket(dataOut, dataOut.length, IPAddress)

b) UDPPacket = new UDPDatagram (userInput, userInput.length, IPaddress, 9876)

c) DatagramPacket packet = new DatagramPacket(dataOut, dataOut.length, IPAddress, 9876)

d) Socket datagramSocket = new dataGramPacket(dataOut, IPAddress)

6.3 [2 points]

Consider a server socket object

```
socket = ServerSocket(12345);
```

What does the invocation of `socket.accept()` return?

a) 'true' if there is a new TCP segment in the socket's buffer, false otherwise

b) a new TCP segment from the socket's buffer (blocks if no segments are available)

c) 'true' if a new TCP connection request has arrived, false otherwise

d) a socket associated with a new TCP connection (blocks if no connections are available)

6.4 [2 points]

Assume the following two lines of code are to be executed on the machine blue.cse.yorku.ca:

```
Socket myFirstSocket = new Socket("blue.cse.yorku.ca", 5555);
Socket mySecondSocket = new Socket(5555);
```

Are the two lines/commands in conflict? Explain briefly!

SOLUTION:

Yes. They both attempt to connect to (i.e. open) port 5555 on the same, local host - blue.cse.yorku.ca

6.5 [4 points]

Suppose application A is using a UDP socket, i.e. DatagramSocket(), to transfer data to application B on a remote host. Suppose application A calls send() method on the given socket 10 times.

a) Can the underlying network stack transmit more than 10 data packets?

b) Can the underlying network stack transmit fewer than 10 data packets?

Explain briefly!

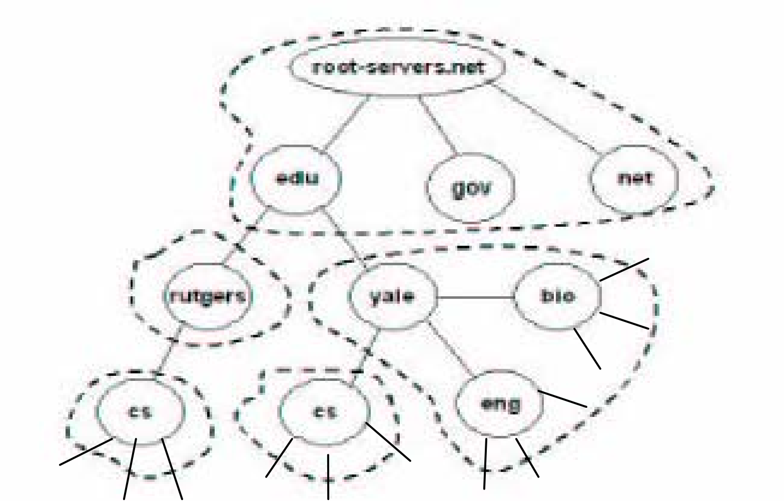
SOLUTION:

a) Yes. UDP packets larger than the network MTU will experience IP fragmentation.

b) No. Unlike TCP, UDP does not provide a mechanism for 'packing' smaller chunks of application data into a single UDP packet. Hence, each send() method will generate a separate UDP -> IP packet.

7. DNS [9 points]

Consider the DNS topology in the figure below, in which different DNS zones are indicated with a dashed line. There is only one DNS server per each zone, and it happens to have the same name as the highest node in that zone: yale.edu, cs.yale.edu, ruthgers.edu, cs.rutgers.edu, and root-servers.net. The only servers supporting recursive querying are cs.yale.edu and cs.rutgers.edu.



For each of the queries below, list in order all the DNS servers contacted by the resolver (located in the OS of the machine running the query). Assume there is no caching performed at any level of the hierarchy.

6.1 [3 points] A machine called *lab1.bio.yale.edu* exists in the biology department at Yale, and a user on *eden.rutgers.edu* launches this query: "**nslookup lab1.bio.yale.edu**".

SOLUTION:

rutgers.edu
root-server.net
yale.edu

6.2 [3 points] At the prompt of *paul.cs.rutgers.edu* somebody launches this query: "**nslookup lab1.bio.yale.edu**".

SOLUTION:

cs.rutgers.edu

6.3 [3 points] On *lab1.bio.yale.edu* somebody queries: "**nslookup paul.cs.rutgers.edu**".

SOLUTION:

yale.edu
root-server.net
rutgers.edu
cs.rutgers.edu

8. HTTP [14 points]

8.1) [6 points] Suppose that a browser on host A wants to retrieve an HTML document (D), and an embedded image (I), from a host B. Assume that A does not initially now the IP address of B, but A's local name server S does know B's IP address. Also, assume that the browser on A uses HTTP/1.0 (the non-persistent version).

Show the chronological sequence of transport layer segments (TCP or UDP) sent and the respective application layer data type (DNS or HTTP) by filling in the following table. Also, for each TCP packet state when any of the SYN, FIN and/or ACK bits in the TCP header are set to 1.

SOLUTION:

Source	Destination	Transport Layer Protocol	Application Layer Protocol
A	S	UDP	DNS
S	A	UDP	DNS
A	B	TCP SYN=1	
B	A	TCP SYN=ACK=1	
A	B	TCP ACK=1	HTTP
B	A	TCP	HTTP
A	B	TCP FIN=1	
B	A	TCP FIN=ACK=1	
A	B	TCP ACK=1	
A	B	TCP SYN=1	
B	A	TCP SYN=ACK=1	
A	B	TCP ACK=1	HTTP
B	A	TCP	HTTP
A	B	TCP FIN=1	
B	A	TCP FIN=ACK=1	
A	B	TCP ACK=1	

8.2) **[8 points]** An institution has a T1 access line (1.544 Mbps) which services web requests from about 150 users in the network. The institution is considering putting up a proxy server which can act as a cache for all these users. (I.e., whenever a user makes a web request, the request is first sent to the proxy server to see if it can service the request from its cache. Otherwise, the proxy forwards the requests to the origin server.)

a) [2 points] The users make on the average 1 request per second, with an average size of a request object being 10 kbits. What percentage of the bandwidth is consumed by the web traffic when there is no proxy server, and all requests are serviced by the origin server?

SOLUTION:

Bandwidth consumed = 150 × 1/sec × 10 Kbits = 1.5Mbits/sec.
Therefore percentage consumption = 100 × (1.5 / 1.544) % = 97.15%

b) [3 points] After installing the proxy server, it was found that the hit rate to the cache is 40%. What percentage of the institutional bandwidth is now consumed by the Web traffic?

SOLUTION:

Bandwidth consumed = 60 x (150 × 1/sec × 10Kbits) / 1.544 Mbits/sec = 58.29 %

c) [3 points] If the round trip time (RTT) from a user node to the proxy server is 50 msec, and the RTT from the proxy server into the Internet is 2 sec, then what is the average delay experienced by web requests in scenario b).

SOLUTION:

60% of requests take 2.05 seconds, and 40% of requests take 0.05 seconds.
Therefore, average time taken = (0.6 × 2.05) + (0.4 × 0.05) = 1.25 seconds

9. Security [7 points]

8.1) [4 points] Consider one security system using a Key Distribution Center (KDC) server, and another security system using Certification Authority (CA) server.
a) Suppose the KDC goes down. What is the impact on the ability of parties in the respective system to communicate?
b) Now suppose that the CA goes down. What is the impact of this failure instead?

Briefly justify your answer, by clearly stating which of the two events would have more serious consequences.

SOLUTION:

In the case of a KDC going down, no new session keys can be generated. People with existing tickets and keys can use them until they expire, but nothing new can be created, causing a serious impact on the ability to communicate. If a CA goes down, the only thing affected is the ability to generate new certificates. Otherwise, communication can proceed as normal using existing issued certificates. As a result, a CA going down has a relatively minor impact on the ability to communicate - there is only an issue if you need a new certificate issued by the CA.

8.2) [3 points] We have discussed the concept of Reflector DDoS in class. Do you think it would be possible to conduct such an attack using DNS protocol? Briefly justify your answer.

SOLUTION:

Yes, it is possible. Such attacks are known as DNS amplification attacks. In these attacks the attackers identify several third-party DNS servers that will respond to any DNS query, and send many spoofed DNS queries to those DNS servers. In particular, each DNS query is sent in a UDP packet, with the source address forged to be the IP address of the targeted victim. Also, each query is deliberately complex, so that it will trigger a response that is much larger than the query itself, amplifying the effect of the attack.