CS3 Networks, Prac 1

SOLUTIONS

(all from Kurose/Ross textbook, except Q2)

Q0.

Review questions *(some answers might be wrongly numbered; there will be answers for questions that should be ignored because outside the area covered)*

1. There is no difference. Throughout this text, the words "host" and "end system" are used interchangeably. End systems include PCs, workstations, Web servers, mail servers, Internet-connected PDAs, WebTVs, etc.

2. Suppose Alice, an ambassador of country A wants to invite Bob, an ambassador of country B, over for dinner. Alice doesn't simply just call Bob on the phone and say, "come to our dinner table now". Instead, she calls Bob and suggests a date and time. Bob may respond by saying he's not available that particular date, but he is available another date. Alice and Bob continue to send "messages" back and forth until they agree on a date and time. Bob then shows up at the embassy on the agreed date, hopefully not more than 15 minutes before or after the agreed time. Diplomatic protocols also allow for either Alice or Bob to politely cancel the engagement if they have reasonable excuses.

3. A networking program usually has two programs, each running on a different host, communicating with each other. The program that initiates the communication is the client. Typically, the client program requests and receives services from the server program.

4. 1. Dial-up modem over telephone line: residential; 2. DSL over telephone line: residential or small office; 3. Cable to HFC: residential; 4. 100 Mbps switched Etherent: company; 5. Wireless LAN: mobile; 6. Cellular mobile access (for example, WAP): mobile

5. You can use here your answer to Q1.

6. (You can ignore for the moment.)

7. Ethernet most commonly runs over twisted-pair copper wire and "thin" coaxial cable. It also can run over fibers optic links and thick coaxial cable.

8. You can use here your answer to Q1.

9. Ethernet LANs have transmission rates of 10 Mbps, 100 Mbps, 1 Gbps and 10 Gbps. For an X Mbps Ethernet (where X = 10, 100, 1,000 or 10,000), a user can continuously transmit at the rate X Mbps if that user is the only person sending data. If there are more than one active user, then each user cannot continuously transmit at X Mbps.

10. There are two most popular wireless Internet access technologies today:
    a) Wireless LAN
    In a wireless LAN, wireless users transmit/receive packets to/from a base station (wireless access point) within a radius of few tens of meters. The base station is typically connected to the wired Internet and thus serves to connect wireless users to the wired network.

    b) Wide-area wireless access network
    In these systems, packets are transmitted over the same wireless infrastructure used for cellular telephony, with the base station thus being managed by a telecommunications provider. This provides wireless access to users within a radius of tens of kilometers of the base station.

11. A circuit-switched network can guarantee a certain amount of end-to-end bandwidth for the duration of a call. Most packet-switched networks today (including the Internet) cannot make any end-to-end guarantees for bandwidth.

12. At time t_0 the sending host begins to transmit. At time $t_1 = L/R_1$, the sending host completes transmission and the entire packet is received at the router (no propagation delay). Because the router has the entire packet at time *t1*, it can begin to transmit the packet to the receiving host at time t_1. At time $t_2 = t_1 + L/R_2$, the router completes transmission and the entire packet is received at the receiving host (again, no propagation delay). Thus, the end-to-end delay is $L/R_1 + L/R_2$.

13. See textbook.

14. Ignore.

15. A tier-1 ISP connects to all other tier-1 ISPs; a tier-2 ISP connects to only a few of the tier-1 ISPs. Also, a tier-2 ISP is a customer of one or more tier-1.

16. The delay components are processing delays, transmission delays, propagation delays, and queuing delays. All of these delays are fixed, except for the queuing delays, which are variable.

17. Java Applet

18. 10msec; d/s; no; no

19. a) 250 kbps
    b) 64 seconds
    c) 200kbps; 80 seconds

20. Java Applet

21. End system A breaks the large file into chunks. To each chunk, it adds header generating multiple packets from the file. The header in each packet includes the address of the destination: end system B. The packet switch uses the destination address to determine the outgoing link. Asking which road to take is analogous to a packet asking which outgoing link it should be forwarded on, given the packet's address.

22. Five generic tasks are error control, flow control, segmentation and reassembly, multiplexing, and connection setup. Yes, these tasks can be duplicated at different layers. For example, error control is often provided at more than one layer.

23. The five layers in the Internet protocol stack are – from top to bottom – the application layer, the transport layer, the network layer, the link layer, and the physical layer. The principal responsibilities are outlined in Section 1.5.1.

24. Routers process layers 1 through 3. (This is a little bit of a white lie, as modern routers sometimes act as firewalls or caching components, and process layer four as well.) Link layer switches process layers 1 through 2. Hosts process all five layers.

25. Application-layer message: data which an application wants to send and passed onto the transport layer; transport-layer segment: generated by the transport layer and encapsulates application-layer message with transport layer header; network-layer datagram: encapsulates transport-layer segment with a network-layer header; link-layer frame: encapsulates network-layer datagram with a link-layer header.

26. a) Virus
    Requires some form of human interaction to spread. Classic example: E-mail viruses.

    b)Worms

No user replication needed. Worm in infected host scans IP addresses and port numbers, looking for vulnerable processes to infect.

c) Trojan horse
Hidden, devious part of some otherwise useful software.

27. Trudy can pretend to be Bob to Alice (and vice-versa) and partially or completely modify the message(s) being sent from Bob to Alice. For example, she can easily change the phrase "Alice, I owe you $1000" to "Alice, I owe you $10,000". Furthermore, Trudy can even drop the packets that are being sent by Bob to Alice (and vise-versa), even if the packets from Bob to Alice are encrypted.

28. *(not required)* Creation of a botnet requires an attacker to find vulnerability in some application or system (e.g. exploiting the buffer overflow vulnerability that might exist in an application). After finding the vulnerability, the attacker needs to scan for hosts that are vulnerable. The target is basically to compromise a series of systems by exploiting that particular vulnerability. Any system that is part of the botnet can automatically scan its environment and propagate by exploiting the vulnerability. An important property of such botnets is that the originator of the botnet can remotely control and issue commands to all the nodes in the botnet. Hence, it becomes possible for the attacker to issue a command to all the nodes, that target a single node (for example, all nodes in the botnet might be commanded by the attacker to send a TCP SYN message to the target, which might result in a TCP SYN flood attack at the target).

Q1.

The answers to this question are very variable. Make sure that your answer makes sense checking out answers from other people. Somebody had problems in finding out the speed of their connections: use ***speedtest.net*** *by Ookla for example. (As an aside, read how it works.)*

Q2. (Protocol design)

Problem P4 of your textbook.

There is no single right answer to this question. Many protocols would do the trick. Here's a simple answer:

Messages from ATM machine to Server

```
Msg name              purpose
--------              -------
HELO <userid>         Let server know that there is a card in the ATM
                      machine
                      ATM card transmits user ID to Server
PASSWD <passwd>       User enters PIN, which is sent to server
BALANCE               User requests balance
WITHDRAWL <amount>    User asks to withdraw money
BYE                   user all done
```

Messages from Server to ATM machine (display)

```
Msg name              purpose
--------              -------
PASSWD                Ask user for PIN (password)
OK                    last requested operation (PASSWD, WITHDRAWL) OK
```

```
ERR                 last requested operation (PASSWD, WITHDRAWL) in
                    ERROR
AMOUNT <amt>        sent in response to BALANCE request
BYE                 user done, display welcome screen at ATM
```

Correct operation:

```
client                          server

HELO (userid)    --------------> (check if validuserid)
                 <-----------------  PASSWD
PASSWD <passwd> --------------> (check  password)
                 <-------------  OK (password is OK)
BALANCE----------------------->
                 <-------------  AMOUNT <amt>
WITHDRAWL <amt> --------------> check if enough $ to cover
                 withdrawl
                 <-----------------  OK
ATM dispenses $
BYE--------------------------->
                 <-----------------  BYE
```

In situation when there's not enough money:

```
HELO (userid)    --------------> (check if validuserid)
                 <-----------------  PASSWD
PASSWD <passwd> --------------> (check  password)
                 <-------------  OK (password is OK)
BALANCE----------------------->
                 <-------------  AMOUNT <amt>
WITHDRAWL <amt> --------------> check if enough $ to cover  withdrawl
                 <-------------  ERR (not enough funds)
error msg displayed
no $ given out
BYE--------------------------->
                 <-----------------  BYE
```

Q3. (End-to-end delay)

Problems P12 of your textbook.

The first end system requires L/R_1 to transmit the packet onto the first link; the packet propagates over the first link in d_1/s_1; the packet switch adds a processing delay of d_{proc}; after receiving the entire packet, the packet switch requires L/R_2 to transmit the packet onto the second link; the packet propagates over the second link in d_2/s_2. Adding these five delays gives

$$d_{end\text{-}end} = L/R_1 + L/R_2 + d_1/s_1 + d_2/s_2 + d_{proc}$$

To answer the second question, we simply plug the values into the equation to get 8 + 8 + 16 + 4 + 1 = 37 msec.

Q4. (Route tracing)

Problem P16 of your textbook.

Results might vary, but calculations and observations straightforward, apart maybe from identifying ISPs. Nowadays, the identification can be done rather easily using a search engine and asking the query 'who is' followed by the IP address of the router whose ownership you want to identify. For example, asking 'who is 105.186.107.193' will return something like 'AS37457 Telkom SA Ltd.', indicating that the router belongs to Telkom SA.

Importantly, make sure you understand fully what traceroute returns, even if for the moment it is unclear how it works (it is actually simple, as we will see later in the course.)

Q5. (Segmentation)

Problem P24 of your textbook.

Problem 24

a) & c) Time to send message from source host to first packet switch = $\frac{8\times10^6}{2\times10^6}$ sec = 4sec .

With store-and-forward switching, the total time to move message from source host to destination host = 4sec× 3 *hops* = 12 sec

Time to send 1st packet from source host to first packet switch = . $\frac{2\times10^3}{2\times10^6}$ sec = 1 *m* sec .

Time at which 1st packet is received at the destination host = . 1 *m* sec× 3 *hops* = 3 *m* sec. After this, every 1msec one packet will be received; thus time at which last (4000th) packet is received = 3 *m* sec+ 3999 *1*m* sec = 4.002 sec . It can be seen that delay in using message segmentation is significantly less (almost 1/3rd).

d) Drawbacks:

i. Packets have to be put in sequence at the destination.
ii. Message segmentation results in many smaller packets. Since header size is usually the same for all packets regardless of their size, with message segmentation the total amount of header bytes is more.

Q6.

Do the Wireshark lab 1, from the textbook companion website

(See WIRESHARK LAB#1 SOLUTION in the same folder)