Dept. Computer Science **Computer Networks**
Vrije Universiteit **22.08.2008**

Always explain your answers concisely

1a The OSI reference model has seven layers. Name them in order and briefly explain the main purpose of each of them. *5pt*

See the book

1b NAT firewalls violate the strict separation of layers of the OSI model. How? *5pt*

They rewrite IP addresses using transport-layer addresses that are found in the packet headers.

1c There are many advantages to strict layering. However, what is the main disadvantage? Be sure to explain your answer. *5 pt*

The main disadvantage is potential loss of performance. Because higher layers are essentially deprived from any formation on how the lower layers implement their protocols, they cannot fine-tune their implementations to the behavior at, say, the data-link layer. A good example where this can be seen is the implementation of TCP on a hybrid wired/wireless network. If the TCP layer would know be able to make use of the transmission characteristics of the datalink layer, it can follow a different strategy for retransmissions and congestion control in the case of wired or wireless networks.

2a Explain the difference between Frequency Division Multiplexing and Time Division Multiplexing. Which technique is used in ADSL? *5pt*

See book for FDM/TDM. ADSL obviously uses FDM.

2b Explain when we need modulation techniques. *5pt*

Whenever a cable cannot support digital signal transmission, we will have to resort to modulation techniques to encode binary data as analog signals (i.e., as waves). This lack of support generally happens with poor media, such as long copper wires, in which case a digital signal will arrive completely corrupted, beyond the point of being able to be detected by the receiver.

2c When sending a series of bits over a wire, the clocks of the sender and receiver need to be synchronized. Why? *5pt*

If the clocks are not synchronized, the receiver will not be able to sense the wire at the correct moment to detect the proper value of the signal. In turn, this will lead to missing bits and thus poor transmission quality.

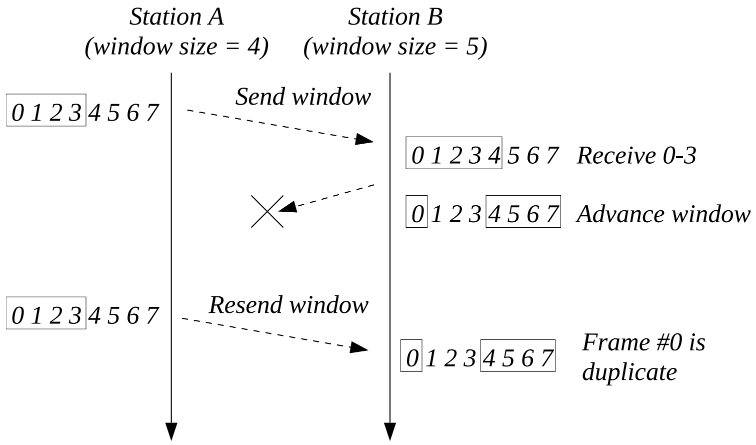
3a Wireless transmission can benefit from error correction coding, but at the cost of bandwidth. Explain. *5pt*

Error correcting codes require that frames are extended with a relatively large number of bits. As a consequence, we are sacrificing bandwidth by making frames longer, but will be able to correct more frames, making the transmission moer relaible.

3b Explain how fragmentation of frames in IEEE 802.11 can help to improve reliability of transmissions. *5pt*

The idea is simple: because the chance of successfully transmitting a frame depends on the length of a frame, we put ourselves in a situation that not an entire frame, but only a few smaller fragements need to be retransmitted in the case of an error.

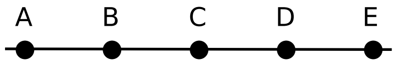
3c In order to support sliding windows of size N, we need to make use of sequence numbers in the range $[0...2N-1]$. Show by example what can go wrong if we use a smaller range for sequence numbers. *5pt*



4a IPv6 is gradually replacing IPv4 in the Internet. Briefly discuss its benefits compared to the IPv4 protocol. *5pt*

See the book

4b Considering the network depicted below, illustrate how the routing tables of the nodes change in response to host A's failure if the distance-vector routing protocol is used. What is the name of this phenomenon? *5pt*



The phenomenon is known as count-to-infinity *problem. All nodes will keep on incrementing their routes for ever (unless an upper bound has been specified) without detecting that no actual route to A exists.*

4c BGP adopts a *path-vector* routing protocol which solves the issue discussed in the previous question. How does BGP solve that issue? *5pt*

The count-to-infinity problem arises because every node does not realize that the routes advertised by their neighbors are of no interest since they pass through it. The path-vector routing protocol solves this by advertising the entire route (instead of just the number of hops). This way, nodes can easily exclude routes passing through them.

5a Assume a company has two production sites located in New York and Los Angeles, respectively. These sites are connected through a dedicated 1 Gbps fiber connection and communicate using TCP with a congestion window of 64 KB. In order to improve efficiency, two different options are available: either replace the line with a 2 Gbps fiber or add another 1 Gbps line in parallel. Ignoring installation costs, which solution would improve the throughput? And the latency? *5pt*

The bottleneck for the throughput is the small TCP congestion window used which combined with the high latency yields a poor utilization of the channel bandwidth. A 2Gbps line does not reduce the latency and, hence, has no noticeable impact on the throughput. Conversely, adding a second line enables sending data in parallel, thus effectively doubling the throughput. As for latency, instead, neither solution is useful because the latency of a fiber channel depends on the distance, so the only solution to improve it would be to move the two sites closer.

5b To ensure reliable transfer, two different strategies are commonly used: *go-back-n* and *selective repeat*. Briefly describe each of them and highlight their pros and cons. *5pt*

See the book

5c UDP provides a connectionless service, just as IP. Why could not applications use IP directly? Why is UDP needed? *5pt*

UDP is a transport protocol and enable addressing different applications running on the same hosts, using UDP ports. Conversely, IP addresses identify only hosts.

5d The *two army* theorem formally demonstrates that no solution can be devised to release a connection such that the two parties will always agree. Yet, the TCP connection-release protocol is widely used. How did it solve the two army problem? Which particular case is not tolerated? *5pt*

To circumvent the two-army problem, timeouts are used. If any of the message sent during the disconnection process is never acknowledged, after few retransmissions the connection is closed unilaterally. This approach works well in most cases but it fails if the first disconnection request message and all its subsequent retransmissions are lost. This would result in a half-open connection because the other party is unaware that a disconnection is taking place.

6a The receipt of undesired mail (spam) is one of the most annoying flaws experienced nowadays. Traditional solutions consisted into allowing incoming mail only from known senders (*white-list*). This approach, however, proved to be unsatisfactory due to a weakness of the SMTP protocol. Which? Why may a widespread use of PGP solve this? *5pt*

SMTP does not check the authenticity of the `From:` *field, thus letting malicious spammers be able to forge email with fake address in order to bypass the white list filter. PGP enables a user to check the authentication of the message, thus making this type of attack more complex.*

6b Usually the DNS protocol is used to obtain the IP address of a host given its symbolic name (e.g., `google.nl`). However, it also possible to query DNS servers to obtain the symbolic name associate with a given host, as shown below. Explain how this information is obtained. *5pt*

```
seuss> host 209.85.135.103
seuss> 103.135.85.209.in-addr.arpa domain name pointer mu-in-f103.google.com
```

IP addresses are stored in the special `in-addr.arpa` *domain. See the book for more details.*

Grading: *The final grade is calculated by accumulating the scores per question (maximum: 90 points), and adding 10 bonus points. The maximum total is therefore 100 points.*