Dept. Computer Science	**Computer Networks**
Vrije Universiteit	**26.06.2008**

Always explain your answers concisely

1a Explain the benefits of the layered architecture of network protocols ?*See the book* *5pt*

1b Name at least one case discussed in class in which the layer separation has been violated. Discuss the reasons behind this choice and the possible consequence in the near future *5pt*

NAT violates the most fundamental rule of protocol layering: layer k may not make any assumptions about what layer k + 1 has put into the payload field. This implies that if a new transport protocol was to be deployed, the NAT would be unable to handle it.

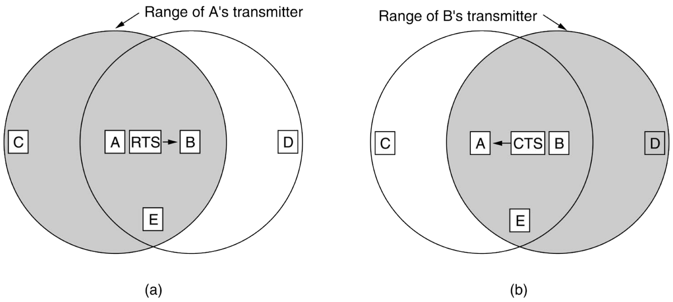
1c Briefly characterize the main difference between packet-switched networks and circuit-switched networks, highlights pros and cons of each solution *5 pt*

See the book.

1d Based on the answer to the above question motivate why telephone networks and the Internet are designed differently *5 pt*

Phone companies were mainly interested in offering high QoS to their customer and charging them for the time they spent on-line. This was much easier to achieve with a circuit-switched model. On the other hand, Internet designers were mainly concerned about the reliability of the Internet and so they aimed at ensuring that communication was still possible even in presence of massive failures (e.g., a rocket attack). Therefore, the redundant paths of a packet-switched network offered more guarantees.

2a Referring to the figure below, explain the basics of the MACA protocol and show how it can effectively solve the hidden station and exposed station problem (give also a concise description of the two phenomena). *5pt*



C is within range of A but not within range of B. Therefore, it hears the RTS from A but not the CTS from B. As long as it does not interfere with the CTS, it is free to transmit while the data frame is being sent. This solves the exposed station problem. In contrast, D is within range of B but not of A. It does not hear the RTS but does hear the CTS. Hearing the CTS tips it off that it is close to a station that is about to receive a frame, so it defers sending anything until that frame is expected to be finished. This solves the hidden station problem

2b IEEE 802.11 exploits a variant of the MACA protocol, called MACAW. Describe the main difference and discuss why MACAW suffers from the exposed station problem *5pt*

MACAW introduces data link layer acknowledgments to enable retransmission of lost frames. Therefore, since A has to listen for the ack from B, C cannot speak until the ack is received, thus leaving the exposed station problem unsolved.

2c Bridges and switches are part of the infrastructure of modern LANs. They operate at data link layer and are therefore unable to handle network addresses. Explain how they can still properly deliver messages to the intended nodes. *5pt*

They use data link layer addresses, i.e., MAC addresses. The conversion from IP addresses to MAC addresses is made by the LAN router, using the ARP protocol.

3a Explain why different protocols are used for inter-AS and intra-AS routing *5pt*

The need for different protocols comes from the fact that within an AS only efficiency (i.e., shortest paths) matters while in routing between different ASes policies and business deals are often the critical factor.

3b Suppose a router has built up the routing table shown below. The router can deliver packets over interfaces 0 and 1 or it can forward packets to routers R2, R3, or R4. Describe what the router does with a packet addressed to each of the following destinations:

1. 128.96.171.92
2. 128.96.167.151
3. 128.96.163.151
4. 128.96.169.192
5. 128.96.165.121

SubnetNumber	Subnet Mask	NextHop
128.96.170.0	255.255.254.0	Interface 0
128.96.168.0	255.255.254.0	Interface 1
128.96.166.0	255.255.254.0	R2
128.96.164.0	255.255.252.0	R3
0.0.0.0	0.0.0.0.0	R4

5pt

1. *→ Interface 0*
2. *→ R2*
3. *→ R4*
4. *→ Interface 1*
5. *→ R3*

3c Briefly describe how MobileIP and DHCP provide two different solutions for nomadic user and motivate why DHCP enjoyed larger diffusion than MobileIP *5pt*

MobileIP enable the user to maintain the same IP address while moving to different locations by tunnelling messages through her home agent. DHCP, instead, is a protocol to dynamically assign an IP address when a host is connected to the network. Actually, it turns out that DHCP is more than enough in most cases as very few mobile users need a stable IP addresses. What they often need is just a connection to the Internet.

4a Assuming a typical client-server interaction (e.g., fetching a page from a web-server), consisting of a client request and reply, explain how many packets respectively are sent if TCP or UDP are used. *5pt*

If TCP is used, ten messages are exchanged: three for establish a connection (SYN, SYN-ACK, and ACK). Four to transfer and acknowledge data and finally three to release the connection (FIN, FIN-ACK, and ACK). With UDP, only two messages are needed.

4b Beside reducing the number of packets sent, is there any other reason why sometimes UDP is preferred? *5pt*

If real-time is needed, there is no need to recover lost messages so the TCP overhead is useless and a lightweight protocol like UDP is preferable. In other cases, instead, the application may want to employ different flow control mechanism and hence TCP is not an option. Finally, UDP is used to implement multicast and broadcast services as these are not supported by TCP.

4c When downloading large files from a host, some applications open more than one TCP connection to the host. Why ? [*Hint: compare what would happen if you had a congestion window of 10 Mb and a packet gets lost every minute against the case in which you have ten TCP connection with 1 Mb congestion window each and, again, only a single packet is lost per minute (regardless the connection it belongs to)]* *5pt*

If we use a single connection with a congestion window of 10 Mb, as soon as a packet gets lost, the TCP congestion control mechanism will reset the window to the MTU size. Instead, if we have ten connections, each with a congestion window of 1 Mb, a packet loss will impact only one of them so the overall congestion window will be (9 Mb + MTU size).

4d Assume that two host A and B are connected though a 10 Gbps fiber connection with a one-way speed-of-light-delay of 50ms. If TCP is used, with a window size of 64KB, what is the actual throughput? *5pt*

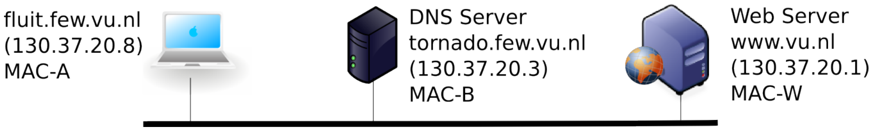
Before the sender can transmit a second bunch of messages, it must wait 100 ms for the first acknowledgment to get through. This means that the actual data rate is:

$$\textit{Data rate} = \frac{W}{\textit{RTT}} = \frac{64 \cdot 1024 \cdot 8}{0.1} \approx 5.2Mbps$$

5a Provide a short description of the mechanism adopted by BitTorrent to incentive users to share their upload bandwidth and explain why it prevents selfish behaviors. *5pt*

BitTorrent leverages off a strategy called Tit-for-tat. This scheme requires that every user exhibit a cooperative approach: a user optimistically start uploading bandwidth to another user but it will stop as soon as the other party does not reciprocate. This way, in order to obtain high download speed, users are obliged to provide high upload rate as well.

5b Consider the network depicted below in which host are identified by their symbolic name, IP address and MAC address. Suppose that a user connected to `fluits` wants to access the homepace located at `http://www.vu.nl`. Fill the table with all the messages exchanged on the network, indicating for each of them the protocol used and the addresses used in the Ethernet, IP and TCP header. *X* means that a given address cannot be known, while *n/a* indicates that the specific protocol is not used ((e.g., TCP for an ARP packet). For simplicity, assume that the ARP table is empty and no DNS or HTTP cache is used.



5pt

MAC Src	*MAC Dest.*	*IP Src*	*IP Dest.*	*TCP/UDP Src*	*TCP/UDP Dest.*	*Protocol*	*Request / Reply*
MAC-A	*Broadcast*	*n/a*	*n.a*	*n/a*	*n.a*	*ARP*	*Request*
MAC-B	*MAC-A*	*n/a*	*n.a*	*n/a*	*n.a*	*ARP*	*Reply*
MAC-A	*MAC-B*	*130.37.20.8*	*130.37.20.3*	*X*	*53*	*DNS (UDP)*	*Request*
MAC-B	*MAC-A*	*130.37.20.3*	*130.37.20.8*	*53*	*X*	*DNS (UDP)*	*Reply*
MAC-A	*Broadcast*	*n/a*	*n.a*	*n/a*	*n.a*	*ARP*	*Request*
MAC-W	*MAC-A*	*n/a*	*n.a*	*n/a*	*n.a*	*ARP*	*Reply*
MAC-A	*MAC-W*	*130.37.20.8*	*130.37.20.1*	*X*	*80*	*HTTP*	*Request*
MAC-A	*MAC-W*	*130.37.20.1*	*130.37.20.8*	*80*	*X*	*HTTP*	*Reply*

6a Many firewalls preclude any incoming connections while opening TCP connections to outside host is allowed. Nevertheless, clients behind the firewall are still able to receive replies from outside servers (e.g., html pages). How is that possible? *5pt*

TCP connections are full-duplex. Hence, once a connection has been established, communication can occur in both directions.

6b In the SSL protocol, the public key is used only at the begininning to exchange a session key. Why is the latter needed ? Would it be possible to use the public key encryption throughout all the session? *5pt*

In theory yes but asymmetric encryption is much more expensive than symmetric one. Therefore, it is more efficient to use asymmetric encryption only to exchange the session key and then rely on symmetric key to encrypt the rest.

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.*