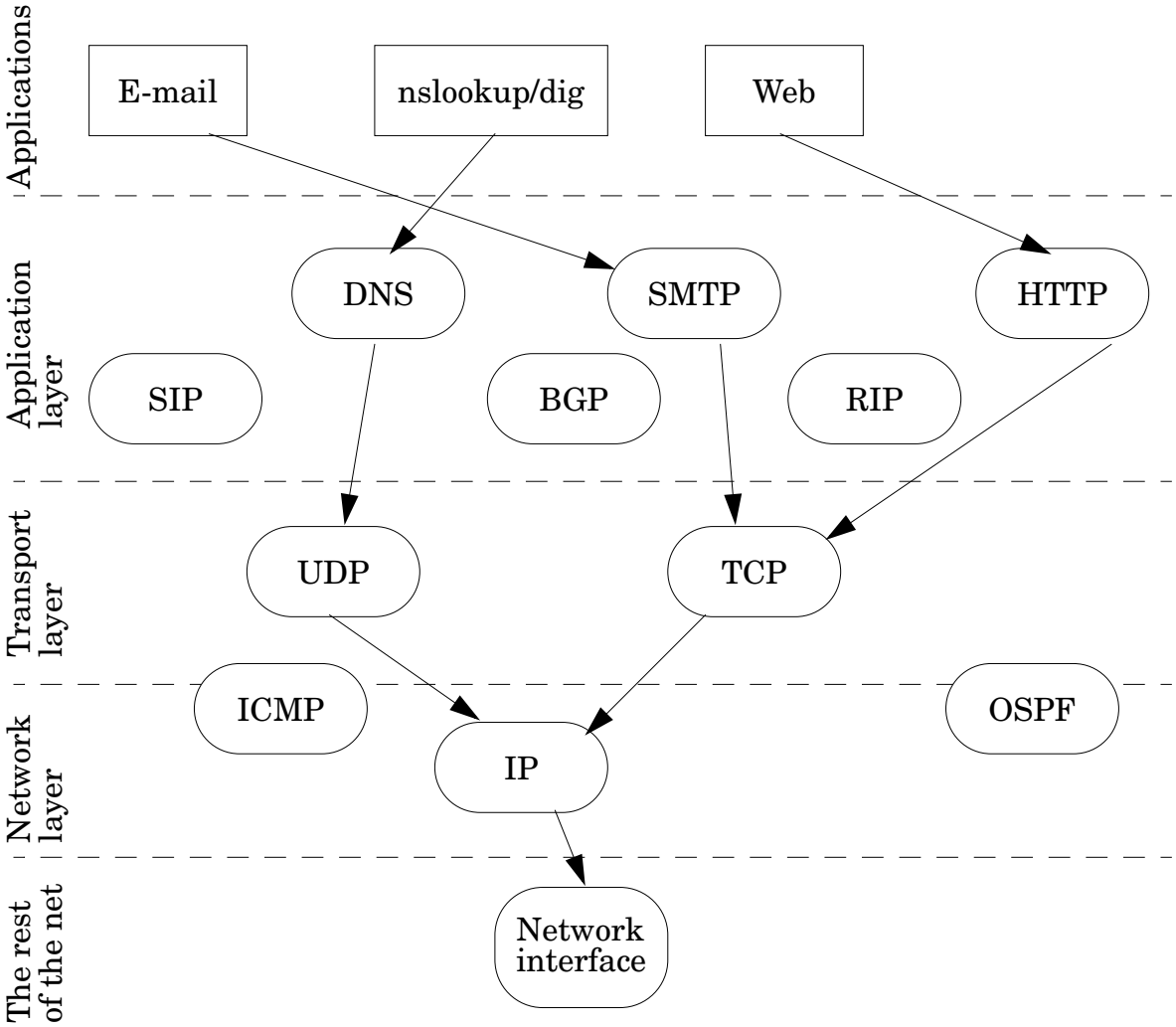
TDTS06 Computer networks, August 23, 2008

Sketched answers to the written examination, provided by Juha Takkinen, IDA, juhta@ida.liu.se. (“Sketched” means that you, in addition to the below answers, need to show your calculations, assumptions and justifications.)

Question 1.

a)



Describe one of the protocols not in use in the figure: For example, SIP (Session Initiation Protocol) is a protocl for managing connections for multimedia. More specifically, SIP provides mechanisms for establishing calls over an IP network and negotiating encodings and other protocols to be used for the call; it can determine the current IP address of the recipient; and it can add new media streams during calls, change the encoding, invite new participants, transfer calls, and hold calls.

b)

The event/action pair in the second leg of the three-way handshake is the SYN+ACK sent by the server to the client, which is interpreted as the ACK for client’s initial SYN packet and the server’s own SYN request to the client. The second leg also contains the

sequence number that the server wants to use for the upcoming data channel communication.

Question 2.

a)

- call setup time: the CS network requires time to set up the circuit, before data can be transferred, while the PS network can start sending data immediately.
- potentially wasted bw: the CS network can waste bandwidth when a connection has been established and the user is not using the connection, because the bw used by the connection will not be made available to other users until the connection is closed. In PS networks bw is allocated on demand, as long as the aggregated bw is not larger than the link's capacity.
- handling of node failures: in a CS network the connection has to be re-established if a node breaks down, while in a PS network the connection will be re-routed on-the-fly to another path past the node that failed.
- packets arrive in order: in a CS network packets arrive in order because of the network design, while in a PS network the packets can arrive out-of-order because the packets have been routed different paths and delayed along the way.

b)

The size of the ring is determined by the size of the packet in microsecs when put into the ring.

The packet is 250 B = 2000 bits, which corresponds to 2000 / 100 Mbps = 20 microsecs of delay if the packet should fit into the ring.

The propagation delay of the ring determines how far the bits will travel in the ring, which should be equal to the circumference of the ring determined by the size of the packet, that is, x meters / (2×10^8 m/s) = 20 microsecs, where x is the circumference in meters. This gives us x = 4000 meters. This is without the nodes.

The number of nodes that physically can fit the ring is 4000 meters / 100 meters = 40 nodes. However, each node introduces 10 bits of delay = 10 bits / 100 Mbps = 0.1 microsecs.

For the 2000-bit packet of 20 microsecs in delay to fit exactly into the ring of 40 nodes, each introducing a delay of 0.1 microsecs, the ring has to be 40 x 0.1 microsecs = 4 microsecs "shorter" in circumference. 4 microsecs in meters is 4 x the propagation delay of the ring (2×10^8 m/s) = 800 meters.

Answer: the circumference of the ring is 4000 – 800 = 3200 meters.

c)

The two types of delay in a router are processing delay and queueing delay. See textbook for explanations.

Question 3.

a)

In a push protocol the sender sends data without a previous request from the receiver, while in a pull protocol the receiver first sends a request for data, which is then sent by the sender

HTTP is mainly a pull protocol because its main function is to request web pages from a server via the GET method. However, in HTTP/1.1 it is also possible to push data by using PUT and POST.

SMTP is a push protocol because an e-mail message is delivered to the receiver's SMTP server, from where she then can download it to her e-mail client via other protocols (that are pull-based).

b)

i) False
ii) True
iii) False
iv) True

Question 4.

a)

MSS = 1500 bytes, ssthresh = 32 KB = 32,768 bytes

Round no.	Congestion window (bytes)	Phase
1	1500	Slow start
2	3000	Slow start
3	6000	Slow start
4	12,000	Slow start
5	24,000	Slow start
6	48,000	Congestion avoidance (AIMD)
7	49,500	Congestion avoidance
…	…	…

The slowstart phase goes on for 5 rounds until the threshold is reached, after which the congestion-avoidance phase begins.

b)

The TCP retransmission timer is updated approximately each round, based on the ACK received for an original transmission of a segment. The value is set to the EstimatedRTT + 4 x DevRTT, where both the EstimatedRTT and DevRTT are EWMAs of collected sample values.

c)

For example, UDP data packets do not have sequence numbers, so duplicates and lost packets cannot be detected. UDP is also lacking the ACK bit, so data cannot be acknowledged as having been received by a receiver.

Question 5.

a)

i) Packet fragmentation is done by either the sender or an intermediate router (in IPv4) when the MTU of the next hop (network) is too small for the whole packet. Every fragment becomes a new IP packet and is sent separately, indistinguishable from an ordinary IP packet. The fragments are reassembled at the receiver before delivered to the upper layer.

ii) Address aggregation is the technique based on netmasks that enables a router to represent a range of network addresses with only one entry in the forwarding table. Longest-prefix matching is then used to distinguish between several hits in the table on a certain destination IP address.

iii) IPv6 is the next-generation IP protocol, developed as a solution to the limited address space of IPv4. In addition to an extended address space (128 bits are used instead of 32 bits), IPv6 has a header that is faster to process by routers, because it is fixed in size, among other things.

b)

The statement is False because although a router retransmits IP packets, it does not use or need DNS to find the destination address because IP packets already have the IP address. Furthermore, DNS, which is used to find mappings between hostnames and IP addresses, is also an application layer protocol ans as such it is not visible to routers, which work in the network layer and below.

Question 6.

a)

Station A will select a K randomly from {0, 1, 2, 3 4, 5, 6, 7} and multiply it with 512 bit times of the network bandwidth to set the value of the backoff timer. Station B will select K from {0, 1} x 512 bit times.

b)

Step	Description
4	Every host and router receives the frame. All machines except the one targeted drop the frame. The target recognizes its IP address.
2	IP asks ARP to create an ARP request message, containing the sender MAC address, the sender IP address, and the target IP address, with the target MAC address filled with zeros.

Step	Description
7	The IP datagram with data for the target is now encapsulated in a frame and is unicast to the destination.
5	The target replies with an ARP reply message containing its MAC address, which is unicast.
3	The message is passed to the link layer and put into a frame with the MAC address of the sender as the source address and the LAN broadcast address as the destination address.
6	The sender receives the reply message. It knows the MAC address of the target.
1	The sender knows the IP address of the target.

c)

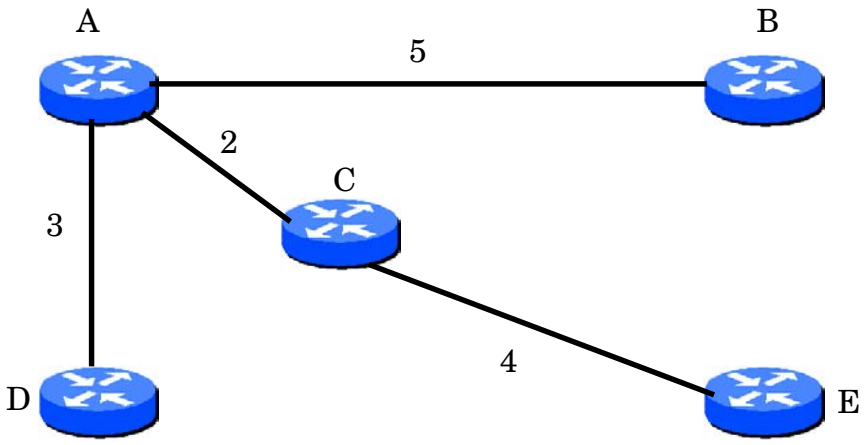
The BSS consists of at least a station and an access point, plus the MAC protocol. It can also consist of the ad-hoc mode, that is, two stations and the MAC protocol.

Question 7.

a)

The links B–C and B–E will not be used.

S	**N'**	**D(b), p(b)**	**D(c), p(c)**	**D(d), p(d)**	**D(e), p(e)**
0	a	5, b	2, c	3, d	-
1	ac	5, x	done	3, d	4, c
2	acd	5, x		done	4, c
3	acde	5, x			done
4	acdeb	done			



b)

LS avoids loops in the routing information thanks to the centralized Dijkstra's algorithm, while DV can cause loops because of its distributed nature.

The amount of control information sent in the network when a new link is discovered is larger in LS than in DV because the new information must be flooded to all nodes by the new node's neighbours. In DV, information is exchanged only between neighbours.

c)

All routers will use BGP because they all must know either what other networks are reachable (boundary router) or where the closest boundary router is (all other routers in the current network), so that hot-potatoe routing can be employed on packets that do not belong in the current network.

Question 8.

a)

Term	Explanation
playback attack	The method of retransmitting an old message, typically with a forged source address, to fool a receiver.
chosen-plaintext attack	The technique of using some knowledge about the contents of the message being sent to crack the ciphertext, for example, language statistics or certain text patterns ("alice" and "bob" for example)
known-plaintext attack	The technique of making a sender to transmit a known plaintext so that the ciphertext can be cracked.
packet sniffing	The technique of eavesdropping on a communication channel and reading its raw contents (as done with wireshark).
ip spoofing	The technique of forging the source address of one's IP packets so that it looks like the packets are coming from someone else.

b)

In the upper left corner, a hash is created of the e-mail message. The hash is a checksum of the message, ensuring that the content has not been altered after being sent.

The hash is then encrypted with the secret key of Alice and attached to the message itself. The encryption of the hash with the private key creates an authentication code that shows that the message was created by Alice.

c)

AES, Advanced encryption standard, is a symmetric key algorithm, typically used for encrypting large portions of text, because symmetric encryption is tenfold faster than asymmetric encryption.