LiTH, Tekniska högskolan vid Linköpings universitet
IDA, Institutionen för datavetenskap
Juha Takkinen
2008-10-22

Written examination in TDTS06 and TDTS41 Computer Networks 2008-10-22 at 8–12

Hall

KÅRA.

Helping materials

A basic calculator with memory erased and an English dictionary (not electronical) are allowed.

Results

The results are published at latest twelve working days after the exam.

Points

Maximum is 40 points (44 if you passed the optional assignment). For grade 3, 20 points are needed. For grades 4 and 5, 28 points and 36 points, respectively, are needed. ECTS grades are given separately.

Teachers on duty

Juha Takkinen, 0731-50 03 93, will visit the hall around 9 and at 11 o'clock.

Instructions

You can use either English or Swedish. Read each question carefully and make sure you have answered everything in the question. Motivate your answers, if not told otherwise. You should convince the examiner that you understand what you are writing about. Be thorough and to the point with your answers but avoid "shotgun" answers that try to answer everything except the problem; this will not score any points. If something is unclear or seems contradictionary, ask the teacher-on-duty and write down your assumptions that make the problem reasonable, if applicable. The use of figures is encouraged, except where other instructions apply. Answers that are not legible will not be graded.

Put only one problem on each sheet of paper, except subproblems a, b, etc., which can be on the same sheet. Use only one side of each paper. Keep *the same order* of each alternative and table entry when you copy answers from the examination paper to your answer sheet. Put your name and SSN on every paper handed in. *Also, read the instructions on the exam wrapper, front and back.*

"On the Internet, nobody knows you're a dog." —New Yorker, July 5, 1993, p. 61

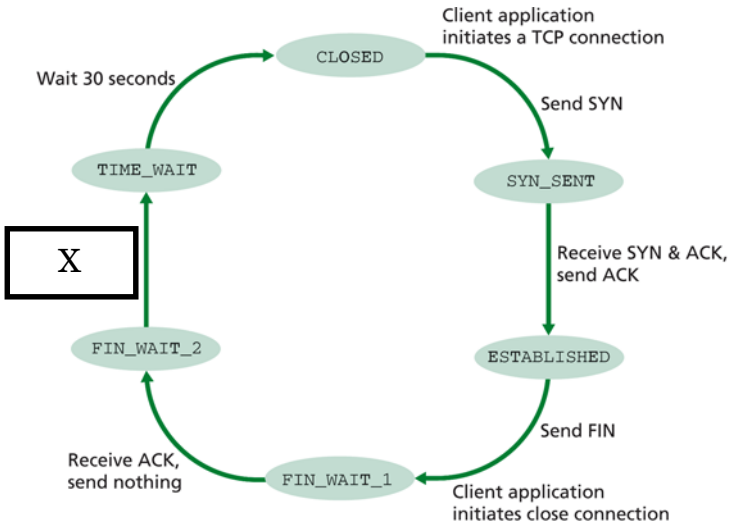
Good luck!

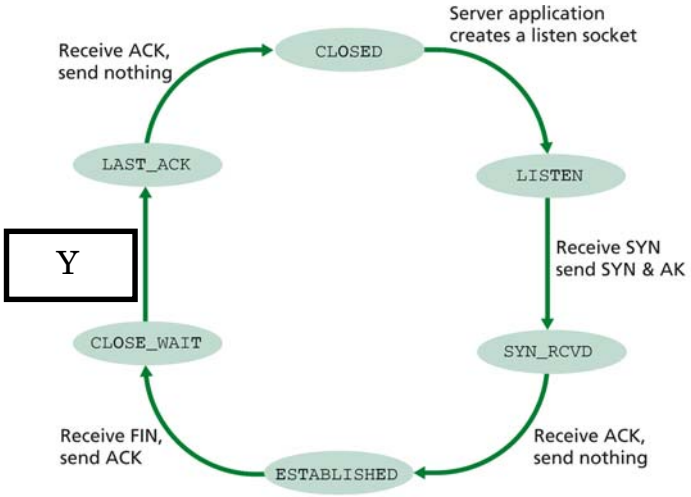
1. Protocols

a. For the following services, select a layer 1–5 (as counted from the bottom of the network architecture used in the course) and describe an implementation of each service. You can use either x-kernel terminology or specific Internet terminology. See the two example explanations for the amount of detail you should use. (3 p.)

Term	Layer	Explanation
Error detection	2	Implemented by CRC, Cyclic Redundancy Code, in IEEE 802.3, a powerful error detection scheme based on polynomial division.
Error detection	4	Implemented by the inCkSum function in x-kernel, based on adding 16-bit chunks together using one's complement.
Addressing		
Demultiplexing		
Flow control		

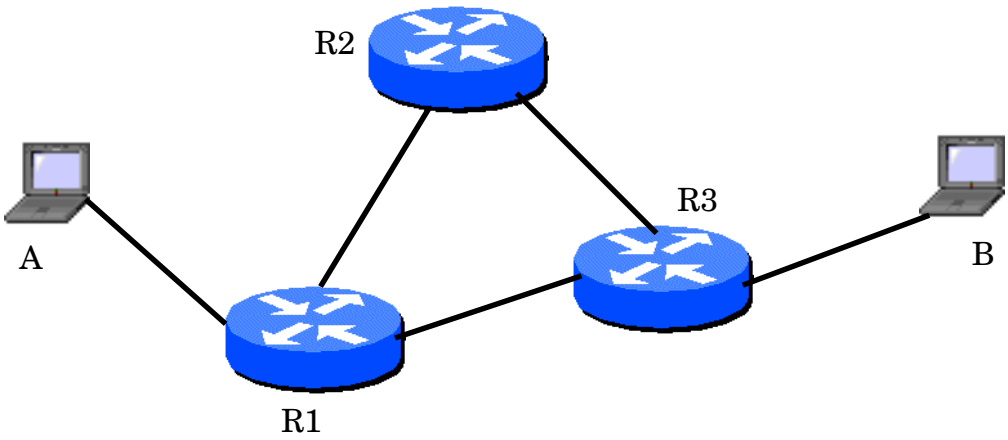
b. Explain what event-action pairs that are missing in X and Y in the two figures below (also, see top of next page). (2 p.)





2. Networking basics

a. Presuppose a network as shown in the figure below and with the four different delay characteristics for each link as listed in the table that follows. With regard to d_{trans}, L stands for "large packet of 1 KB in size" and S means "small packet of 100 B in size".



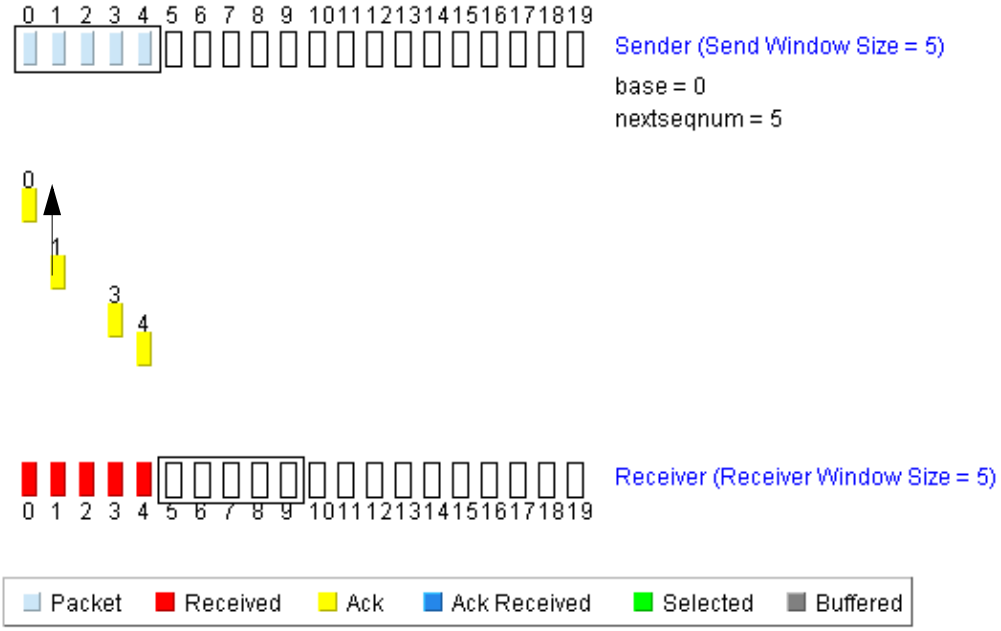
Link vs. Delay type	Link A–R1	Link R1–R2	Link R1-R3	Link R2–R3	Link R3–B
d_{proc}	50 µs	20 µs	20 µs	30 µs	20 µs
d_{queue}	0 µs	10 µs	10 µs	20 µs	5 µs
$d_{trans(L)}$	800 µs	5.5 ms	5.5 ms	5.5 ms	5.5 ms
$d_{trans(S)}$	100 µs	660 µs	660 µs	660 µs	660 µs
d_{prop}	4 µs	18 µs	40 µs	12 µs	6 µs

i. What is the minimal end-to-end delay for a small packet from A to B? (1 p.)

ii. What is the total nodal delay for two large packets at A? (1 p.)

iii. How many small packets can R3 send towards B per second? (1 p.)

d. Assume that the selective-repeat sliding window protocol is used in the below figure. The sender (at the top) has sent one window of packets, numbered 0–4, which have been received correctly at the receiver (at the bottom). The receiver has just transmitted the ACKs shown in the figure and moved the window to positions 5–9. Describe what happens next and when will the Send window have advanced to positions 5–9? (2 p.)



3. Applications

a. Explain what DNS is, with a maximum of two sentences, as if you wanted to impress a friend with your new knowledge acquired in the course. (1 p.)

b. In the four items below, tick off True, False, or none of the two. Do not justify your answer. *Copy your answer to your answering sheet*. (2 p.)

	True	False	
i.	❑	❑	HTTP is mainly a push-based protocol, because web pages are published on a web server (“pushed” to the readers).
ii.	❑	❑	TCP is used by both SMTP and FTP to create a secure communication channel, where messages cannot be altered by other network users.
iii.	❑	❑	The MX record in the DNS shows information about a mail server’s hostname and IP address.
iv.	❑	❑	IMAP is a pull-based protocol, used for stateful downloading of e-mail from a mail server.

(+0.5 p. for each correct, –0.5 p. for each wrong, 0 p. for no answer, and min. 0 p.)

c. Consider the following string of ASCII characters captured using wireshark when the web browser sent an HTTP GET message. The characters <cr> and <lf> are carriage-return and line-feed characters.

```
GET /cs453/index.html HTTP/1.1<cr><lf>Host: gai
a.cs.umass.edu<cr><lf>User-Agent: Mozilla/5.0 (
Windows;U; Windows NT 5.1; en-US; rv:1.7.2) Gec
ko/20040804 Netscape/7.2 (ax) <cr><lf>Accept:ex
t/xml,application/xml,application/xhtml+xml,text
/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
<cr><lf>Accept-Language: en-us,en;q=0.5<cr><lf>Accept-
Encoding: zip,deflate<cr><lf>Accept-Charset: ISO
-8859-1,utf-8;q=0.7,*;q=0.7<cr><lf>Keep-Alive: 300<cr>
<lf>Connection:keep-alive<cr><lf><cr><lf>
```

i. What is the URL of the document being requested by the browser? (1 p.)

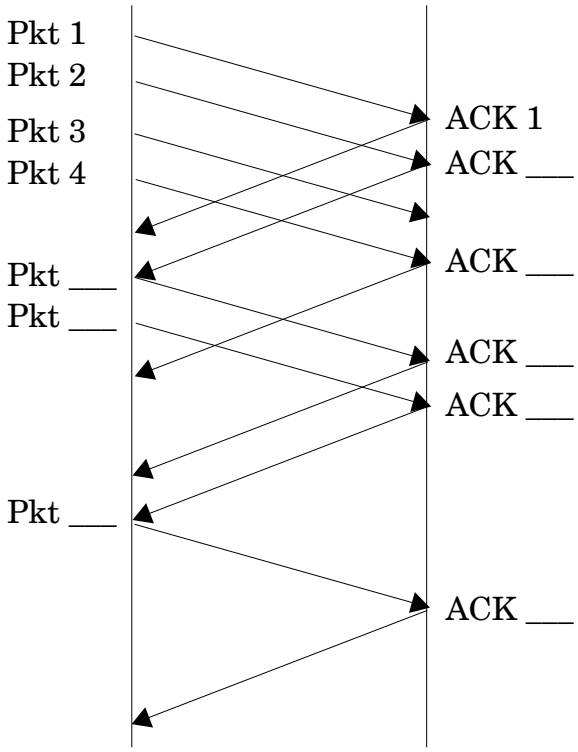
ii. Does the browser request a non-persistent or persistent connection? (1 p.)

4. TCP

a. Consider the TCP scenario below.

i. Fill in the correct sequence numbers on the packets and ACKs in the figure. (1 p.)

ii. Explain the concepts of Duplicate ACK, Delayed ACK and Cumulative ACK. Which ones occur in the figure below? (2 p.)



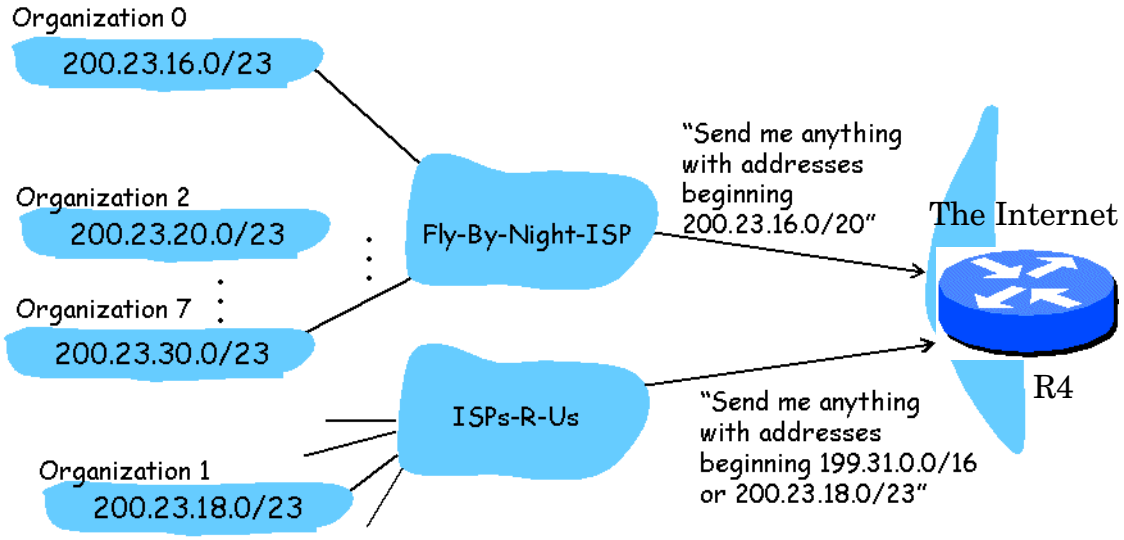
b. Explain the role of the Triple duplicate ACK in the context of TCP's congestion control mechanism. Sketch out a scenario. (2 p.)

5. IP

a. The CIDRized address of Organization 1 in the figure below is 200.23.18.0/23.

i. Organization 1 has decided to divide its internal network into four subnets with a number of hosts in each subnet. Suggest a subnet mask for Organization 1's routers. Explain your answer. (1 p.)

ii. A packet with IP address 200.23.20.129 arrives at router R4 in the figure. Explain how the packet is delivered to the appropriate host in Organization 1, using the subnet division in i) above. Sketch out your interpretation of Organization 1's internal network. (2 p.)



b. Discuss if the following statement is true or false: "ARP is used to translate an IP address into hostnames, as opposed to DNS[1], which translates from hostnames to IP addresses." (2 p.)

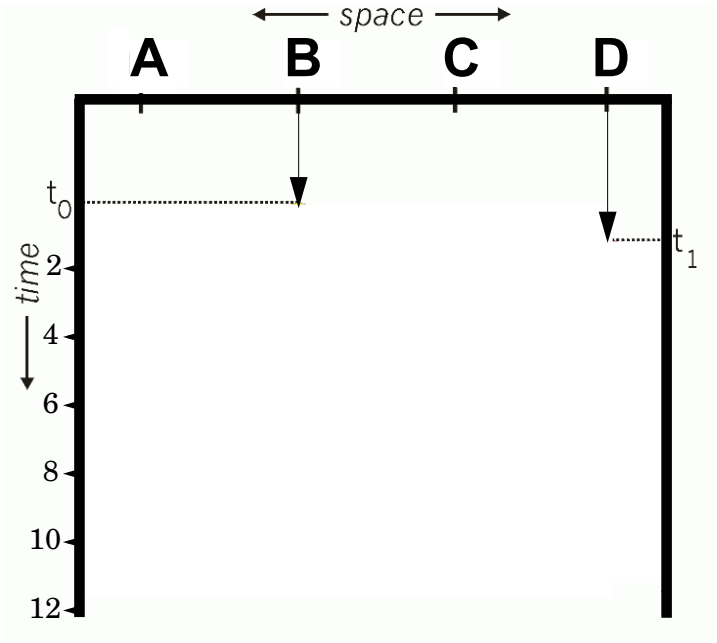
6. LANs

a. Assume a CSMA/CD network with four stations A–D as shown in the time–space diagram below (see top of next page).

i. What constitutes the collision domain in the diagram and why? (1 p.)

ii. Show what happens, by filling in the diagram, when station B begins to transmit at time t_0 and station D at time t_1. The length of each station's frame is 6 time units. The propagation delay is *not* zero. (2 p.)

1. Which you already described in 3a.

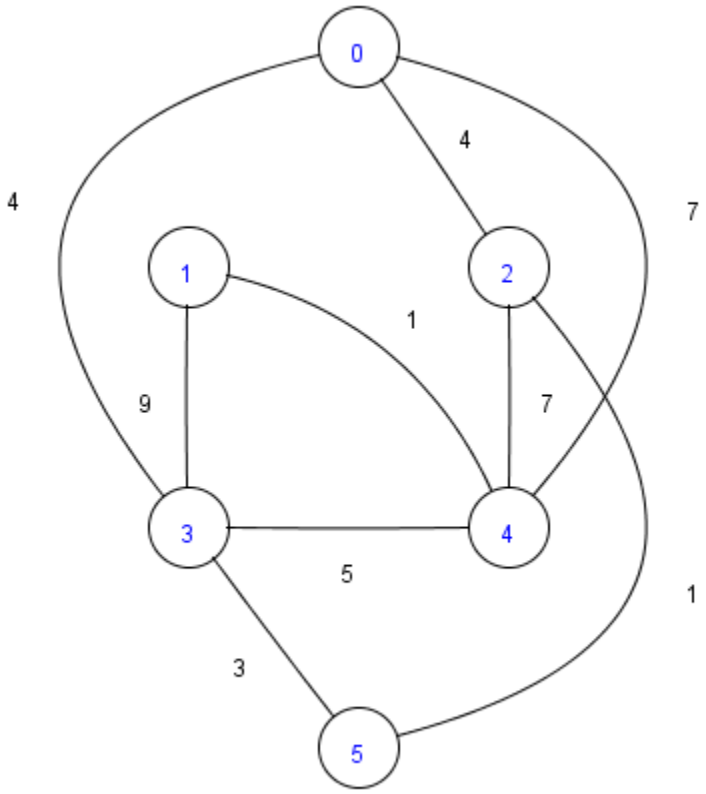


iii. Suppose that the two stations in ii) above detect a collision, and that it is the first time for both of them. Describe how A and D go about to retransmit their respective frames. (1 p.)

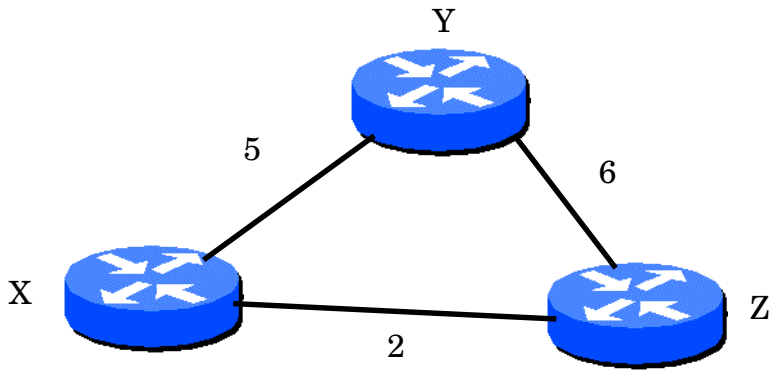
b. Explain the concept of a hidden terminal and why it is a problem for efficient communication in a wireless network. (1 p.)

7. Routing

a. Calculate the spanning tree for the network below, starting from node 3 and using Dijkstra's algorithm. Show your calculations. Explain your notation if not using the textbook's notation. Which links will not be part of the spanning tree? (2 p.)



b. Consider the three-node network below. Assume the distance vector tables have been initialized and updates are sent synchronously, that is, all nodes receive simultaneously distance vectors from their neighbours. Compute the final distance vector tables when the path costs have stabilized themselves, using the distance-vector algorithm. (2 p.)



c. Explain what an autonomous system (AS) is, with regard to routing, and how it is related to BGP. (1 p.)

8. Network security

a. SSL, Secure Sockets Layer, is used to implement security at the transport layer. SSL does its own handshake directly after TCP's three-way handshake, as shown in the list below. The purpose of the SSL handshake is to authenticate the server, agree on crypto algorithms to use, and to establish the keys:

- Client sends list of algorithms it supports, along with client nonce
- Server chooses algorithms from list; sends back its choice, plus its certificate and a server nonce
- Client verifies the certificate, extracts the server's public key from the certificate, generates a pre-master secret, encrypts it with the server's public key, and sends all to the server
- Client and server independently compute encryption and MAC keys from the pre-master secret and nonces
- Client sends a MAC of all the handshake messages
- Server sends a MAC of all the handshake messages.

i. What is the purpose of the nonce used in steps 1 and 2? (1 p.)

ii. Explain how the client can verify the certificate in step 3. (1 p.)

iii. Explain what a MAC is, as used in the two last steps above. (1 p.)

iv. If SSL provides security at the transport layer, why is it that security mechanisms are still needed at layers above and below SSL? (2 p.)

9. Optional assignment result

The number of points that you received in the optional assignment is: _____