# Computer Communication
# EDA344, EDA343, DIT 420

*Time and Place*: Wednesday 18 March, 2015, 14.00-18.00 M

*Course Responsible*: Marina Papatriantafilou (Tel: 772 5413 -in case of need 0768-563132)

*Allowed material*:

- English-X (X can be French, German, Swedish, etc) dictionary
- *No other books, no notes, no calculators, no electronic devices.*

*Grading - updated thresholds*:

CTH students registered for the EDA344 or EDA343 course, 7.5 hp: 3: 28-38 p, 4: 39-49 p, 5: 50-60 p

GU (DIT 420): Godkänd 28-43, Väl godkänd 44-60 p

*Instructions*

- **Write clearly your course-code (EDA344/EDA343/DIT420)**
- **Start answering each assignment on a new page; use only one side of each sheet of paper; please sort the sheets according to the question-ordering and number them.**
- Write in a **clear manner** and **motivate** (explain, justify) your answers. If it is not clear what is written for some answer, it will be considered wrong. If some answer is not explained/justified, it will get **significantly** lower marking.
- If you make any **assumptions** in answering any item, do not forget to clearly state what you assume.
- A good rule-of-thumb for the extend of detail to provide, is to include enough information/explanation so that a person, whose knowledge on computer communication is at the level of our introductory lecture, can understand.
- Please answer in English, if possible. If you have large difficulty with that (with all or some of the questions) and you think that your grade might be affected, feel-free to write in Swedish.
- Results, inspection of exam: Monday April 20, 12.00-13.00, room 6128 (EDIT building, west wing)

**Good Luck !!! Lycka till !!!!**

1. General questions and applications (12 p)

   (a) (2p) Give one example of a stateful protocol and one of a stateless protocol. Explain why they are characterized as stateful and stateless respectively.

   (b) (2p) Explain the role of playout delay in taking care of jitter in streaming traffic.

   (c) (4p) A popular social network site can become overwhelmed if it has only one server handling all its requests. How is this tackled in practice? Explain carefully.

   (d) (4p) Suppose Alice, with a web-based email account (such as hotmail or gmail) sends a message to Bob, who accesses his mail from a server using POP3. Describe how the email-message gets from Alice's host to Bob's host. In your description, make sure to mention the application-layer protocols that are used.

```
Answer directions:
- TCP maintains state for RDT; http no state, lightweight protocol, relies on TCP for eg RDT.
- lecture on multimedia networking
- Bandwidth is usually the bottleneck. It replicates to proxy servers, or CDNs. DSN is needed t
- The message is first sent from Alices host to her mail server over HTTP;
DNS used first to translate te URL to IP address.
Alices mail server then sends the message to Bobs mail server over SMTP.
Bob then transfers the message from his mail server to his host over POP3.
```

2. Transport layer, reliable data transfer and congestion control(12p)

   (a) (2p) Is it possible to have reliable data transfer over UDP? How or why not?

   (b) (2p) In reliable data transfer, show why we need sequence numbers when the sender may retransmit due to timeouts.

   (c) (4p) (i) Why does TCP do fast retransmit upon a 3rd acknowledgment and not a 2nd? (ii) Why might TCP reduce its sending rate upon a 3rd acknowledgment and how does this happen?

   (d) (4p) Consider a pipelined protocol for reliable data transfer between two hosts (for simplicity we assume that they are directly connected with each other). Show how to compute the sending window size in order to have channel utilization greater than 90%, supposing that the packet size is 1200 bytes, that transmission rate is $10^9$ bits/sec and the one-way propagation delay is 15 sec. make sure to also use a space-time diagram in your answer.

```
Answers/directions
- Application can provide that
- Duplicate ack can be due to datagram routing and out-of order
arrival of consecutive segments.;
3 acks indicate loss, hence  TCP retransmits;
TCP assumes that the loss is due to congestion in the network;
hence also reduces rate i.e. the sender's congestion window shrinks.
-similar ex. done in exercise session
```

3. Data Link Layer and Wireless (12p)

   (a) (3p) Explain the differences between link layer switches and network-layer routers.

   (b) (4p) Describe the principles of the Carrier Sense Multiple Access method for medium access in shared medium networks. Give two examples of such protocols, one for wired communication and one for wireless and explain how and why they differ.

(c) (5p) Assume an Ethernet network with the following configuration:

| Host | IP address | MAC address |
|---|---|---|
| A | 192.168.0.1 | 49-BD-D2-C7-56-2A |
| B | 192.168.0.2 | 5C-66-AB-90-75-B1 |
| C | 192.168.0.3 | 1A-23-F9-CD-06-9B |

Suppose A wants to communicate with B. What is the purpose of the Address Resolution Protocol (ARP)? Describe how the protocol works (by giving an example of a run by host A).

```
HINTS
- in book, chapter link layer
- carrier sense multiple accessCSMA in book, link layer;
CSMA CA (collision avoidance) for wireless (hidden station problem)
and CD (collision-detection; Ethernet, collision at receiver is collision at sender,
hence detectable).
- To identify (lookup) the MAC address of an IP address (1p).
A sends a link-layer broadcast message to FF-FF-FF-FF-FF-FF (with source MAC 49-BD-D2-C7-56-2A)
to request the MAC address of 192.168.0.2 .
Only B, who has the IP address, answers to the request by sending
a response with source MAC address, 5C-66-AB-90-75-B1
and destination MAC address of A, 49-BD-D2-C7-56-2A (2p).
```

4. Network core and routing (12 p)

(a) (6p (2+4 resp.)) Consider an ISP that has an address block 200.23.16.0/20 and 4 customers A, B, C, and D that each needs a maximum of 510 host addresses. Furthermore, suppose that the ISP has a router with two links, 0 and 1, where customer A and B are located on link 0, and customer C and D on link 1. (i) Propose a possible allocation of address space by the ISP for these customers on the form xxx.xxx.xxx.xxx/yy. (ii) Provide a forwarding table that uses the longest prefix matching and forwards packets to the correct customers. Explain your answer and calculations carefully.

(b) (4p) What is an Autonomous System (AS)? Mention two commonly used intra-AS routing protocols in Internet and the routing methods they use.

(c) (2p) What is the purpose of ICMP?

**Answers/directions:**

A: 200.23.16.0/23, B: 200.23.18.0/23, C: 200.23.20.0/23, D: 200.23.22.0/23. (2p)
Forwarding Table:

| Address | Link |
|---|---|
| 11001000 00010111 000100 | 0 |
| 11001000 00010111 000101 | 1 |

(4p) - An AS is a group of routers that are typically under the same administrative control *which runs the same routing algorithm* (2p). RIP (Distance-Vector protocol) and OSPF (Link-State protocol)

- Internet Control Message Protocol (ICMP): used by hosts & routers to communicate network-level information, e.g., error reporting: unreachable host, network, port, protocol.

5. Security-related topics (12 p)

(a) (4p) Symmetric and asymmetric encryption systems are two different categories of encryption systems. Explain (with a figure) the principles of *asymmetric* encryption. Why are both encryption systems needed.

(b) (3p) Suppose A is connecting to an FTP server B, where password authentication is required, over a communication network and that C is positioned in the network so that it can capture all packets from A to B (and from B to A). Give an attack that C can perform. Describe the principle for preventing this attack.

(c) (5p) What security services are provided by IPSec? Mention a problem that IPSec is commonly used for to solve and briefly how it solves the problem. What is the main difference between IPSec and SSL?

```
- Figure 8.6 (or slide 8-19) (3p).
Symmetric encryption is much faster
 than asymmetric encryption, however asymmetric encryption
solves the key distribution problem of symmetric encryption (1p).
- C can capture the authentication being performed and
 perform a replay attack and authenticate as A (1p).
A nonce should be added to the authentication procedure,
where B sends a nonce (random number) that A has to include in its response (2p).
- data integrity, confidentiality, authentication, and
replay attack prevention (2p).
Implement Virtual Private Networks (VPN), to connect several offices together in a network.
IPSec is implemented at the border GWs of the offices and traffic between
the networks are encapsulated and forwarded over Internet in IPSec datagrams (2p).
SSL is implemented at the application layer (and secures the communication
of an application), IPSec is implemented at the network layer (and secures TCP/UDP, ICMP) (1p).
```