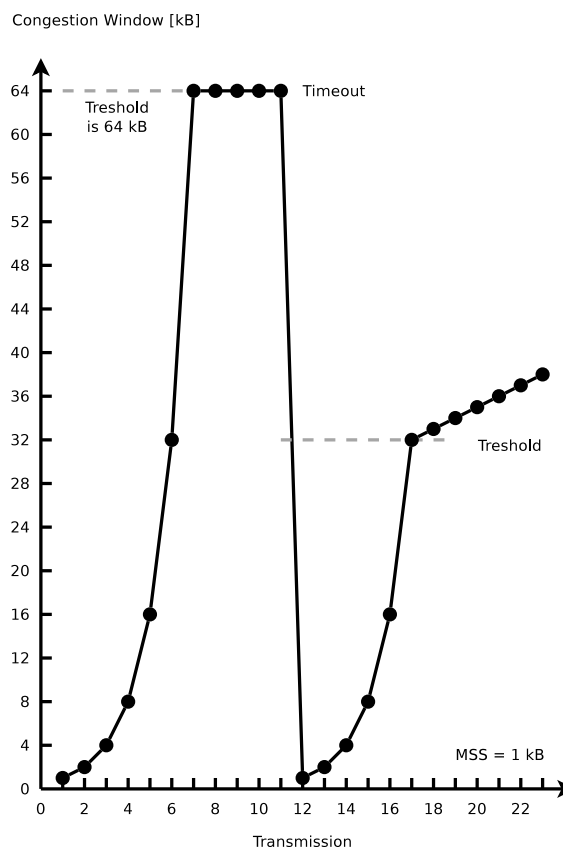# Exercise Sheet 8

Exercise 1   (TCP Congestion Control)

1. Describe what the slow-start phase is.

2. Describe what the congestion avoidance phase is.

3. Mark in the figure both the slow-start phase and the congestion avoidance phase.

4. Describe what fast retransmit is.

5. Describe what fast recovery is.

6. The concept of TCP congestion control is called **AIMD** (= Additive Increase / Multiplicative Decrease). **Describe the reason** for the aggressive reduction and conservative increase of the congestion window.

7. Describe the functioning of a Denial-of-Service attack via **SYN flood**.

Exercise 2   (Transmission Control Protocol)

1. Consider the effect of using slow start on a line with a RTT of 10 ms. The maximum segment size is 2 kB and the receive window has a size of 24 kB. How long does it take before the first full window can be sent if no congestion occurs?

2. Given a maximum segment size of 1 kB: Assume that the congestion window is set to 18 kB just before a timeout occurs. How big will the window be after four consecutive successful transmissions if fast recovery is **not** used?

3. A TCP machine is sending full windows of 65,535 bytes over a 1 Gb/s channel. The channel provides a one-way delay of 10 ms. What is the maximum throughput that can be achieved? What does this mean for the efficiency of the channel usage?

4. What is the impact of the bandwidth-delay product on flow control?

Sources: Andrew Tanenbaum, Computer Networks, Fourth Edition. Pearson (2003), and Prof. Dr. Jochen Schiller, FU Berlin (2015)

Exercise 3   (Domain Name System)

1. DNS uses UDP instead of TCP. In case of packet loss on the network layer, there is no automatic recovery. Does this cause a problem, and if so, how is it solved?

2. In addition to being subject to loss, UDP packets have a maximum length, potentially as low as 576 bytes. What happens when a DNS name to be looked up exceeds this length? Can it be sent in two packets?

3. The TTL of resource record may cause a delay of various hours or even days until the change of an IP address for a given name is updated for every host. Hence, would it be a good idea to use only very small values for the TTL? Explain why or why not.

4. Which of the following specifies a valid domain name:

   ☐ mail.frankfurt-university.de.

   ☐ www.frankfurt/university.de.

   ☐ sea-01.cit.frankfurt-university.de.

   ☐ university.berlin.

   ☐ www1.frankfurt-university.de.

☐ 1www.frankfurt-university.de.

☐ www.frankfurt.-university.de.

☐ myhost.local.domain.

Exercise 4   (Networking Applications)

1. Describe which protocols are involved when you boot up your computer, open a web browser, go to the `https://webmail.frankfurt-university.de`, login, and send an email to `oliver.hahm@fb2.fra-uas.de`.

2. Explain the purpose for each of the protocols from the previous question.

3. Which of these protocols act on the application layer?

4. The DNS *A record* for `teaching.dahahm.de` resolves to `176.9.70.110`. An alternative way to enter the URL into the browser's address field is: `https://176.9.70.110/index.html` How does the browser know whether the given name is a DNS name or an IP address?

5. When you try to access my personal web page via `https://176.9.70.110/index.html` you will get an HTTP status code `404`. When you access it via `https://teaching.dahahm.de/index.html` you will get HTTP status HTTP status code `200`. Explain the meaning of both status codes. Can you imagine why the result is different?

6. For the exchange of emails more than one protocol is used. Name at least two of them and explain the provided service for each of them.

Exercise 5   (Do some research)

1. The FTP protocol specification requires two ports. Why?

2. Explain the term *Open Relay*.

3. Basically all relevant protocols on the layers above 2 and below 7 have been specified by the IETF. Name two protocols on the Application Layer which has also been specified by the IETF and two protocols which have **not**.

4. Name two popular software projects that implement the HTTP protocol.