Exercise Sheet 6

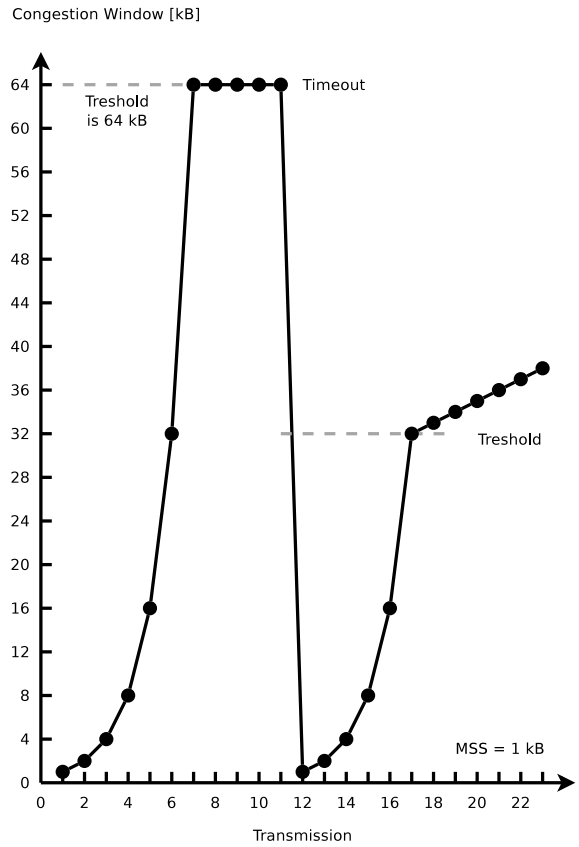
Exercise 1 (Applications and Transport Layer Protocols)

1. Select the most appropriate transport layer protocol for each of the following applications or application scenarios and explain your choice.
   a) File transfer (exchange file between two hosts over the network)
   b) Video conferencing
   c) Instant messaging
   d) Retrieving sensor information (e.g., temperature) from a sensor network
   e) Accessing a complex web page
   f) Accessing a simple web page
   g) Clock synchronization
   h) Video streaming
2. Many IoT applications rather use UDP as a transport layer protocol. Why?
3. CoAP is an application layer protocol designed to be used on top of UDP. However, it specifies certain features one would rather expect from a transport layer protocol. Explain the reason why no new transport layer protocol was specified instead.
4. CoAP offers four different message types. Name them and describe what their meaning.

Exercise 2 (TCP and UDP)

1. Explain the **differences** between TCP and UDP.
2. Describe **two examples**, where using the Transport Layer protocol TCP makes sense.
3. Describe **two examples**, where using the Transport Layer protocol UDP makes sense.
4. Describe what a socket is.

5. Describe what the Seq number in an TCP segment specifies.
6. Describe what the ACK number in an TCP segment specifies
7. Describe the **silly window syndrome** and its effect.
8. Describe the functioning of **silly window syndrome avoidance**.
9. Which two possible **reasons** for the occurrence of congestion in computer networks exist?
10. Why does the sender maintain **two windows** when using TCP and not just a single one?
11. Describe what the slow-start phase is.
12. Describe what the congestion avoidance phase is.
13. Mark in the figure both the slow-start phase and the congestion avoidance phase.



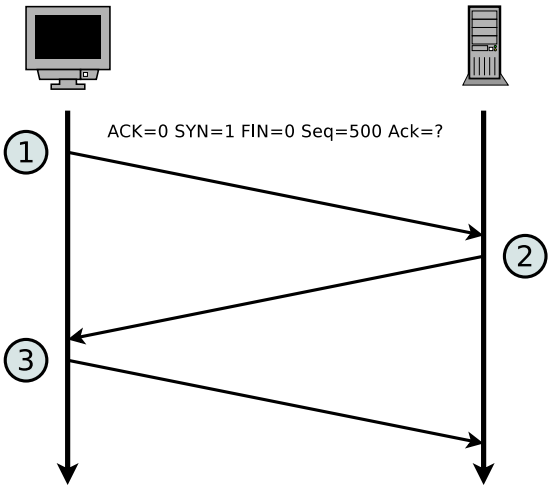
14. Describe what fast retransmit is.
15. Describe what fast recovery is.

16. 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.

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

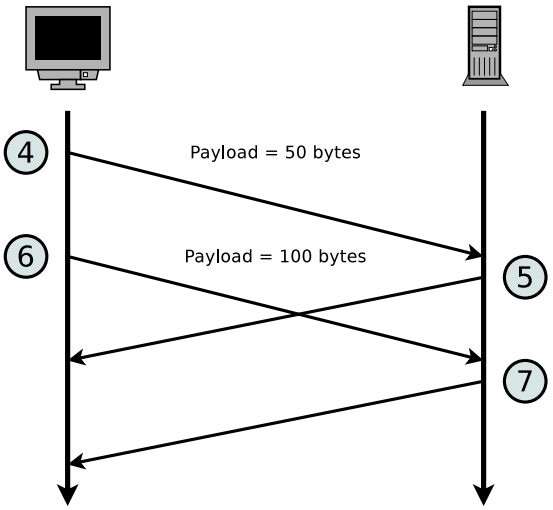
Exercise 3 (TCP Connections)

1. The diagram shows the establishment of a TCP connection. Complete the information in the table for TCP messages 2 and 3 according to TCP messages 1.



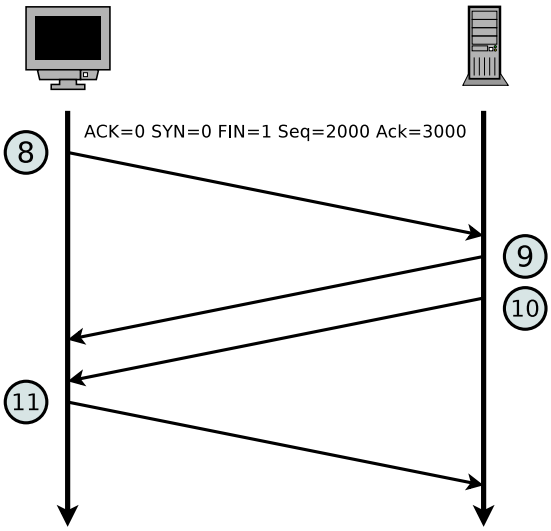
Message	ACK	SYN	FIN	Payload length	Seq number	ACK number
1	0	1	0	0	500	
2					1000	
3						

2. The diagram shows an excerpt of the transmission phase of a TCP connection. Complete the table.



Message	ACK	SYN	FIN	Payload length	Seq number	ACK number
4	0			50	501	1001
5	1			0		
6	0			100		
7	1			0		

3. The diagram shows the termination of a TCP connection. Complete the table.



Message	ACK	SYN	FIN	Payload length	Seq number	ACK number
8	0	0	1	0	2000	3000
9				0		
10				0		
11				0		

Exercise 4 (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?

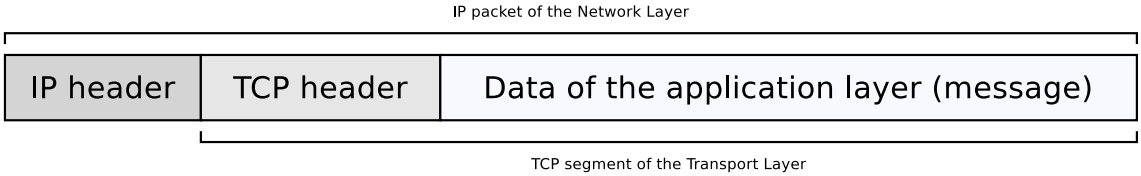
3. A TCP machine is sending full windows of 65,535 bytes over a 1 Gb/s channel. The channel provides a one-way delay of 10 ms. What is the maximum throughput that can be achieved? What does this mean for the efficiency of the channel usage?

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 5 (Header and Payload)

An application generates 40 bytes payload which is first packed into a single TCP segment, and then packed into a single IP packet. What is the percentage of header data in the IP packet and what is the percentage of application generated payload?



Exercise 6 (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 7 (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 8 (Do some research)

1. The checksum in UDP is optional, i.e., it can be used to protect the integrity of the entire datagram or not. Is there also a way to *partially* protect the payload against transmission errors?
2. The original congestion control algorithm in TCP was called Tahoe. Many other algorithms were introduced over the last decades. Name two of them that can be used without any knowledge about the TCP implementation on the receiver side and two that requires information about the receiver's TCP implementation.
3. The FTP protocol specification requires two ports. Why?
4. Explain the term *Open Relay*.