Solution of Exercise Sheet 5

Exercise 1   (Transport Protocols)

1. Explain the **differences** between TCP and UDP.

    - *UDP*

        - *Connectionless Transport Layer protocol. Transmissions take place without previous connection establishment.*

        - *More simple protocol in contrast to the connection-oriented TCP. Only responsible for addressing of the segments. Does not secure the data transmission.*

        - *The receiver does not acknowledge transmissions at the sender. Segments can get lost during transmission.*

    - *TCP*

        - *Connection-oriented Transport Layer protocol.*

        - *Makes connections via IP reliable in a way that is desired or simply necessary for many applications.*

        - *Guarantees that segments reach their destination completely and in the correct order. Lost or unacknowledged TCP segments are requested by the receiver at the sender.*

2. Describe **two examples**, where using the Transport Layer protocol TCP makes sense.

    TCP is used for Email transmission, file transmission and web page transmission because no part of the information is allowed to get lost.

3. Describe **two examples**, where using the Transport Layer protocol UDP makes sense.

    If UDP is used for video tra<nsmission or video telephony, the only consequence of losing a segment is losing an image.

4. Describe what a socket is.

    Sockets are the platform-independent, standardized interface between the implementation of the network protocols in the operating system and the applications.

    A socket consists of a port number and an IP address.

5. Describe what the Seq number in a TCP segment specifies.

   The sequence number of a segment is the position of the segment's first byte in the data stream.

6. Describe what the Ack number in a TCP segment specifies

   The sequence number of the next expected segment.

7. Describe the silly window syndrome and its effect.

   The Silly window syndrome is a problem where a large number of packets is sent, which increases the protocol overhead.

   Scenario: A receiver is overloaded and its receive buffer is completely filled. Once the application has read a few bytes (e.g. 1 byte) from the receive buffer, the receiver sends a segment with the free storage capacity of the receive buffer. For this reason, the sender transmits a segment which contains just 1 byte payload.

   Overhead: At least 40 bytes for the TCP/IP headers, 40 bytes for the acknowledgement and 40 bytes for the segment with notifies about the current free storage capacity in the receive window.

8. Describe the functioning of silly window syndrome avoidance.

   The receiver does not notify the sender about free storage capacity in the receive window before 25% of the reception buffer is free or a segment size of size MSS can be received.

9. Name the two possible reasons for the occurrence of congestion in computer networks.

   Receiver capacity. The receiver can not process the received data fast enough and therefore its receive buffer becomes full.

   Network capacity. Congestion of the network occurs.

10. Explain why the sender does maintain two windows when using TCP and not just a single one.

    The Advertised Receive Window avoids congestion of the receiver.

    The Congestion Window avoids congestion of the network.
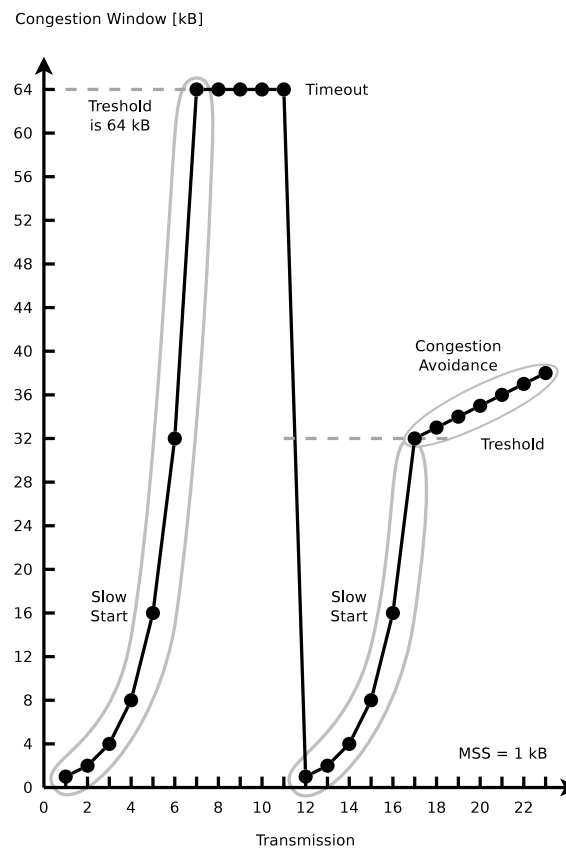
11. Describe what the slow-start phase is.

    The exponential growth phase.

12. Describe what the congestion avoidance phase is.

    The linear growth phase.

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

14. Describe what fast retransmit is.

    After three duplicate ACKs arrived, the lost segment is sent again.

15. Describe what fast recovery is.

    The slow-start phase after three duplicate ACKs arrived is avoided. If three duplicate ACKs arrive, the congestion window is set directly on the threshold value.

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.

    The consequences of a congestion window which is too large in size are worse than for a window which is too small.

    If the window is too small in size, available bandwidth remains unused. If the window is too large in size, segments will get lost and must be transmitted again. This increases the congestion of the network even more!

    The congestion state must be left as fast as possible. Therefore, the size of the congestion window is reduced significantly.

17. Describe how a Denial-of-Service attack via SYN flood works.

    A client sends many connection requests (SYN), but does not respond to the acknowledgments (SYN ACK) of the server via ACK. The server waits some time for the acknowledgment of the clients because the delay of the confirmation could be caused by a network issue. During this period, the address of the client and the status of incomplete connection are stored in the memory of the network stack.

    By flooding the server with connection requests, the table which stores the TCP connections in the network stack is completely filled. This causes the server to become unable to establish new connections. The memory consumption at the server may become so large that the main memory gets completely filled and the server crashes.
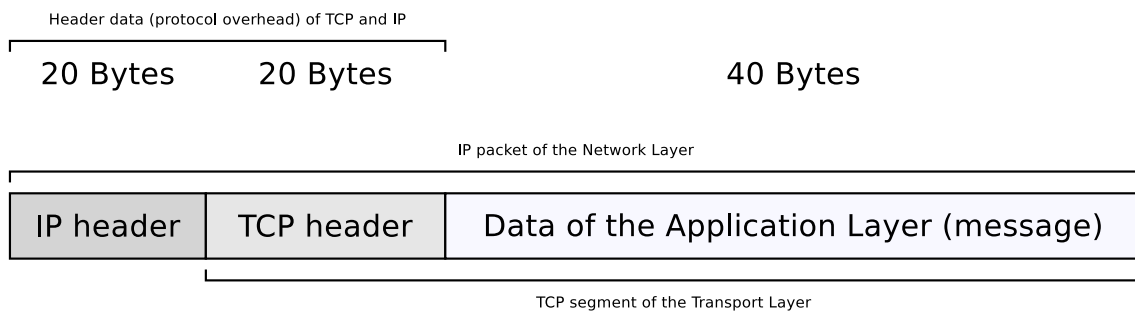
Exercise 2   (Header and Payload)

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?

TCP header = usually 20 bytes
IP header = usually 20 bytes
$\implies$ *the IP packet contains usually 40 bytes (= 50%) header data.*

Header data (protocol overhead) of TCP and IP

20 Bytes	20 Bytes	40 Bytes

IP packet of the Network Layer

| IP header	TCP header	Data of the Application Layer (message)

TCP segment of the Transport Layer

Exercise 3 (Transmission Control Protocol)

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

ACK=0 SYN=1 FIN=0 Seq=500 Ack=?
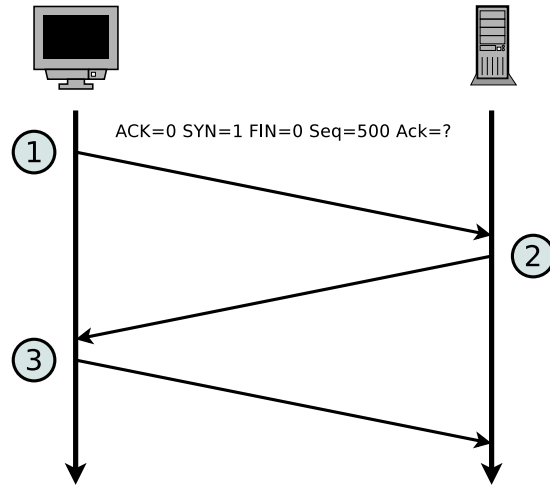
Message	ACK	SYN	FIN	Payload length	Seq number	Ack number
1	0	1	0	0	500	0
2	1	1	0	0	1000	501
3	1	0	0	0	501	1001

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

Payload = 50 bytes

Payload = 100 bytes
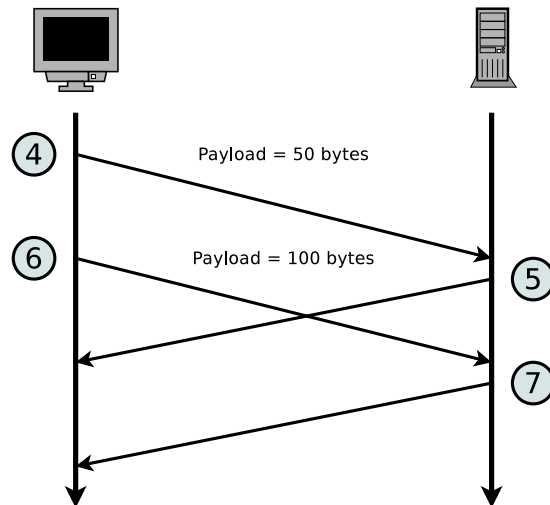
Message	ACK	SYN	FIN	Payload length	Seq number	Ack number
4	0	0	0	50	501	1001
5	1	0	0	0	1001	551
6	0	0	0	100	551	1001
7	1	0	0	0	1001	651

ACK=0 SYN=0 FIN=1 Seq=2000 Ack=3000

3. The diagram shows the termination of a TCP connection. Complete the table.
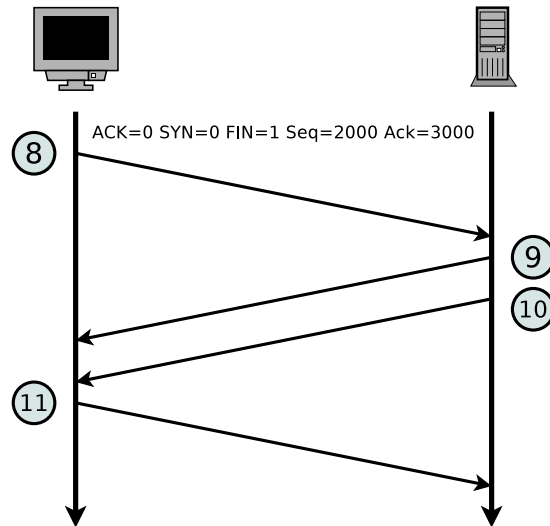
Message	ACK	SYN	FIN	Payload length	Seq number	Ack number
8	0	0	1	0	2000	3000
9	1	0	0	0	3000	2001
10	0	0	1	0	3000	2001
11	1	0	0	0	2001	3001

Exercise 4　(Devices in Computer Networks)

1. Name the network devices that were discussed in this module in this semester.

   Modem, Repeater, Hub (Multiport Repeater), Bridge, Layer-2-Switch, Router, Layer-3-Switch, Gateway

2. Assign the devices to the layers of the hybrid reference model.

   Physical Layer: Modem, Repeater, Hub (Multiport Repeater)
   Data Link Layer: Bridge, Layer-2-Switch
   Network Layer: Router, Layer-3-Switch, Gateway

Exercise 5　(Devices in Computer Networks)

What network device(s) is (are) used to. . .

1. connect networks with different logical address ranges?

   Router or Layer-3-Switch

2. transmit signals over long distances by modulating them to a carrier frequency in the ultra low frequency band?

Modem

3. connect physical networks?

   Bridge or Switch

4. extend the range of LANs?

   Repeater or Hub (Multiport Repeater)

5. connect wireless network devices in the infrastructure mode?

   Access Point

6. enable communication between networks, which use different protocols?

   Gateway

Exercise 6   (Reference Models)

For the network devices, protocols, transmission units, line codes and addressing schemes in the table, mark the corresponding layer of the **hybrid reference model**.

1 stands for the bottom layer and 5 for the top layer in the hybrid reference model. If more than just a single layer are a correct answer, it is sufficient to select at least one correct layer.

	Hybrid reference model layer				
	1	2	3	4	5
4B5B	X				
Address Resolution Protocol (ARP)		X			
Alternate Mark Inversion (AMI)	X				
Autonomous Systems			X		
Border Gateway Protocol (BGP)			X	X	
Bridge	X	X			
Congestion control				X	
CSMA/CA		X			
CSMA/CD		X			
Cyclic Redundancy Check (CRC)		X			
Distance vector routing protocols			X		
Dynamic Host Configuration Protocol (DHCP)					X
Ethernet	X	X			
File Transfer Protocol (FTP)					X
Flow control				X	
Gateway	X	X	X	X	X
Hub	X				
Hypertext Transfer Protocol (HTTP)					X
ICMP			X		
Internet Protocol (IP)			X		
Link state routing protocols			X		
Logical addresses			X		
Manchester-Code	X				
Media access control		X			
Modem	X	X			
Multilevel Transmission Encoding - 3 Levels	X				
Multiport Bridge	X	X			
Non-Return to Zero	X				
Open Shortest Path First (OSPF)			X		
Physical addresses		X			
Port numbers				X	

	Hybrid reference model layer				
	1	2	3	4	5
Reliable end-to-end data connection				X	
Repeater	X				
Router	X	X	X		
Routing Information Protocol (RIP)			X	X	
Security		X	X	X	X
Spanning Tree Protocol (STP)		X			
Switch	X	X	X		
Telnet					X
Transmission Control Protocol (TCP)				X	
User Datagram Protocol (UDP)				X	
Wireless LAN	X	X			

A couple of words regarding the Border Gateway Protocol (BGP): It is an inter-AS routing protocol. Therefore it is correct to assign BGP to the Network Layer. But because BGP messages are exchanged via the connection-oriented Transport Layer protocol TCP, it is also not wrong to assign BGP to the Transport Layer.

A couple of words regarding RIP: The existence of a routing protocol like RIP is essential for the functioning of the Routers in the Network Layer. Therefore it is correct to assign RIP to the Network Layer, equal to the routing protocol OSPF. But because RIP messages are exchanged via the connectionless Transport Layer protocol UDP, it is also not wrong to assign RIP to the Transport Layer.

A couple of words regarding Security: Security protocols or protocol extensions are used on almost all layers. Some Application Layer protocols (e.g. HTTPS) use encryption. On Transport Layer exist e.g. Transport Layer Security (TLS) and Secure Sockets Layer (SSL). On Network Layer exist e.g. IPsec and Layer-3 VPN. On Data Link Layer exist e.g. WEP, WPA and WPA2 of WLAN and Layer-2 VPN.

Exercise 7   (Protocols in Computer Networks)

Name the protocol that is used to. . .

1. provide congestion control and flow control.

   TCP

2. resolve logical addresses into physical addresses.

   ARP

3. avoid collisions inside physical networks.

   CSMA/CA

4. provide routing within autonomous systems via the Bellman-Ford algorithm.

   RIP

5. remote control computers in an encrypted way.

   SSH

6. provide routing within autonomous systems via the Dijkstra algorithm.

   OSPF

7. assign the network configuration to network devices.

   DHCP

8. remote control computers in a unencrypted way.

   Telnet

9. realize connectionless inter-process communication.

   UDP

10. resolve domain names into logical addresses.

    DNS

11. detect collisions inside physical networks.

    CSMA/CD

12. download and upload files in an unencrypted way.

    FTP

13. exchange (deliver) emails.

    SMTP or POP3

14. exchange diagnostic and control messages.

    ICMP

15. reduce the logical topology of a computer network to a loop-free tree.

    Spanning Tree Protocol (STP)

Exercise 8   (Network Address Translation – NAT)

Fill the missing IP addresses and port numbers into the figure that describes a NAT scenario where device X sends a request for a web page to a web server process that runs on the server and can be accessed via port number 80.

NAT Translation Table	
LAN	WAN
10.0.0.2:59272	84.169.219.45:37450

Device X
10.0.0.2

Device Y
10.0.0.3

Device Z
10.0.0.4

Server
151.101.112.250

Default
Gateway

Router
NAT Device

10.0.0.1

Public
IP address

84.169.219.45

```
                     Source                    Destination
(Message 1) 10.0.0.2:59272        --> 151.101.112.250:80
(Message 2) 84.169.219.45:37450 --> 151.101.112.250:80
(Message 3) 151.101.112.250:80  --> 84.169.219.45:37450
(Message 4) 151.101.112.250:80  --> 10.0.0.2:59272
```