# Telematics

Winter Semester 2008/09



| | |
|---|---|
| Number: | 6. Assignment |
| Issued: | 29.01.09 |
| Tutorial: | 05.02.09 & 06.02.09 |
| Lecturer: | Prof. Dr. Güneş, Dipl.-Inf. Blywis |
| Contact: | {guenes, blywis}@inf.fu-berlin.de |

**General information about the exercises**
Accompanying the lecture, we will give out some assignments. You shall do the exercises on your own but you do not have to submit your solutions. The solutions will be presented in the tutorial sessions. We expect each student to have solved the exercises and might ask anyone to present these.

## Exercise 1, Purpose of the Transport Layer:

What services does a transport layer protocol provide?

## Exercise 2, The History of TCP:

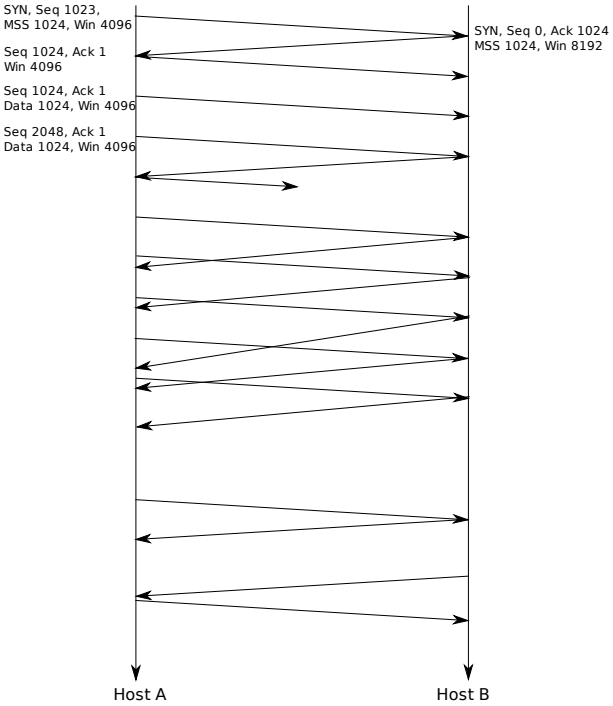
The original Transmission Control Protocol has gotten many extensions over time. Research at which time the following extensions got added, name the corresponding RFCs (if any), and briefly explain the extension:

- Fast Retransmit
- Fast Recovery
- Congestion Control
- Flow Control
- Karn's Algorithm
- Some modification to adapt TCP to networks with high bandwidth-delay product

Start with the original TCP and its features. Under which names are these TCP variants known?

## Exercise 3, TCP Connection:

Consider the following time-sequence diagram of a TCP connection. The arrows represent the transmission of a segment; the labels show some of the TCP header fields.

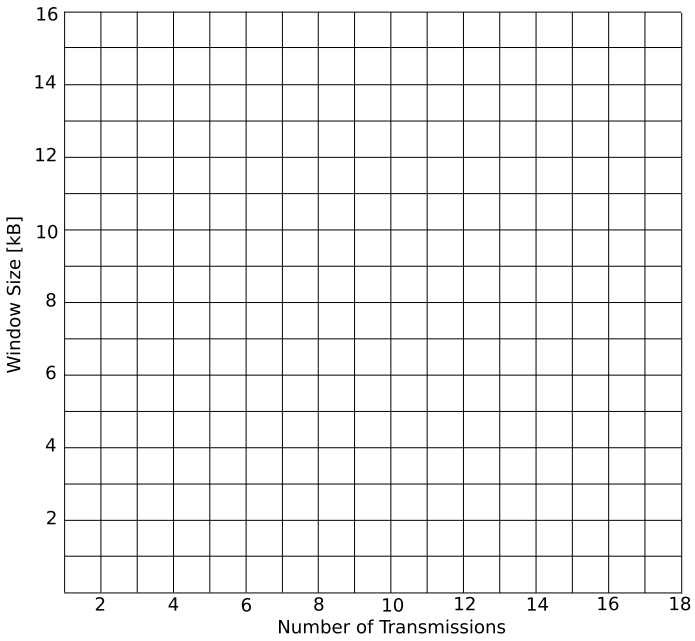



1. Discuss the exchange of the the first three segments. Explain the meaning of the shown header fields.

2. Host A wants to transmit 7 segments with a payload size of 1024 Byte to host B. The connection will be closed afterwards. The first two segments with data are already annotated in the time-sequence diagram. Continue to label the segments with the values of the headers header fields. As can be seen, one of the segments is lost in the network. Assume that host A supports fast retransmit and no timeouts occur.

## Exercise 4, TCP Slowstart and Congestion Avoidance:

Consider a TCP implementation that uses an initial slow start threshold of 8 kB. The maximum segment size shall be set to 1 kB and the receiver's window is 16 kB. Due to congestion timeouts occur after the 8th, the 11th, and the 17th transmission. The term "transmission" has to be understood as a transmission of the maximum number of segments that are allowed to be sent in the current round. The number is limited by the size of the congestion or receiver window.
Sketch the size of the congestion window and the slow start threshold into the following diagram. Assume that no fast retransmit and fast recovery is supported.




## Exercise 5, TCP Limitations:

TCP is a reliable transport protocol but reliability can decrease throughput and increase delay.

1. The maximum payload size of a TCP segment is limited to 65495 Byte. Why was this size chosen?
2. Consider a communication channel with a data rate of 1 GBit/s and a delay of 10 ms. What is the maximum throughput a TCP connection can achieve using this channel? How efficient is the TCP connection?

## Exercise 6, Application layer protocols:

What do many application layer protocols have in common? Hint: Capture some HTTP streams with Wireshark.

## Exercise 7, Universal Resource Locator:

An URL can be divided in multiple parts. Give an example and assign these to the layers in the ISO/OSI reference model.

## Exercise 8, DNS, SMTP, POP3:

Alice and Bob want to communicate via email.

| | Bob | Alice |
|---|---|---|
| IP address: | 192.45.56.127 | 208.115.92.45 |
| Name server: | 192.47.56.2 | 208.115.92.2 |
| SMTP server: | `mail.server.org` | `mail.server.org` |
| Email Address: | `bob@realword.org` | `alice@wonderland.org` |

1. Let's consider Bob likes to send an email. In order to establish a connection with the SMTP server, the server's name has to be resolved into an IP address by using the DNS service. Explain which messages are exchanged when using recursive name resolution. Assume that only the name server responsible for the domain `server.org` is aware of the requested IP address.

2. Now it is Alice's turn to reply to Bob. Explain which messages are exchanged when using iterative name resolution. Assume that only the name server responsible for the domain `server.org` is aware of the requested IP address.

## Exercise 9, Firewalls:

What are firewalls and on which layer(-s) of the ISO/OSI reference model do they operate?

## Exercise 10, Secure Network Topology:

Develop a concept to connect a LAN to the Internet. To provide public services you have the IP address interval 137.226.12.32 - 137.226.12.39. The internal network uses the address interval 192.168.0.0 - 192.168.255.255.
The following services are provided by individual hosts in the LAN. It is noted from where theses hosts shall be accessible.

- WWW server (access from anywhere)
- SMTP server (access from anywhere)
- SMTP and POP3 server (access from LAN only)
- DNS server (access from LAN only)
- DNS server (access from anywhere)
- DHCP server (access from LAN only)
- Printer with network connection (access from LAN only)
- Management server with administration tools (access from LAN only)
- Several workstations (access from LAN only)
- Two firewalls: one simple stateless packet filter and a stateful firewall with integrated NAT box.

The network (and its topology) shall be set up as follows:

- The WWW server, SMTP server, and one of the DNS servers shall be accessibly from the Internet. Those servers run SSH daemons which are accepting connections on port 22 and shall be accessible only from the management server.
- The second DNS server shall be accessible only from the internal network. The workstations are configured to use this DNS server. The DNS server resolves names recursively by passing on requests to the public accessible DNS.
- The server with the SMTP and POP3 services allows the workstation users to send and receive emails. Thus, the SMTP server has to connect to the public accessible SMTP server for sending emails, and analogously the public SMTP server has to connect to the internal SMTP server for delivering emails.
- The workstation user are only allowed to connect to the WWW server.

Solve the task with the following steps:

1. Develop a network topology which considers all requirements. Assign an IP address to each host.
2. Define rule sets for both firewalls as follows:
   - The rules are evaluated one after another accordings to their order in the configuration file. The first matching rule is applied by performing the assigned action; all following rules are ignored.
   - A rule consists of two parts: a condition for the rule to be applied and an action. Use the following notation as rule format:

     <Protocol, Src IP, Src Port, Dest. IP, Dest. Port, [State,] Action>

     The (non obvious) entries have the following meaning:
     - State: Used only in the stateful firewall. Defines the state of a TCP connection. The value ESTAB represents an established TCP connection (packets with a set ACK flag). SYN matches to segments with set SYN flag.
     - Action: May have the values ALLOW and DENY.

     A "*" matches any value. Example: <TCP,123.45.0.0/16,*,198.182.196.56,80,SYN,ALLOW> TCP packets from a host within the network 123.45.0.0/16 and are addressed to host 198.182.196.56 with port 80 are allowed to pass the firewall.