TECHNISCHE
UNIVERSITÄT
DARMSTADT

Technical University Darmstadt

– Department of Computer Science –

Application-Layer Protocols on the Internet

A Summary of the Course Contents

Author:

Jonas Weßner

Teaching professor	:	Prof. Björn Scheuermann
Semester	:	Winter semester 2022/2023

CONTENTS

LIST OF ABBREVIATIONS

MAC Medium Acess Control

IP Internet Protocol

HTTP Hypertext Transfer Protocol

SSH Secure Socket Shell

DNS Domain Name System

DHCP Dynamic Host Configuration Protocol

NTP Network Time Protocol

NAT Network Adress Translation

RTT Round Trip Time

POP3 Post Office Protocol version 3

IMAP Internet Message Acess Protocol

SMTP Simple Mail Transfer Prtocol

SSL Secure Sockets Layer

TLS Transport Layer Security

PPP Point to Point Protocol

UDP User Datagram Protocol

TCP Transmission Control Protocol

2 BASIC TERMS AND DEFINITIONS

In this chapter, basic terms will defined and explained.

1. **TCP/IP Conceptional Layers:**
   a) *Application:* Standardizes communication interfaces built on Transport Layer protocols for specific classes of applications.
   Protocols: Hypertext Transfer Protocol (HTTP), Secure Socket Shell (SSH), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Network Time Protocol (NTP), Post Office Protocol version 3 (POP_3), Internet Message Acess Protocol (IMAP), Simple Mail Transfer Prtocol (SMTP), Secure Sockets Layer (SSL)/Transport Layer Security (TLS) (...)
   b) *Transport:* Provide process-to-process communication for application using ports. Features which might be given depending on the protocol are connection-oriented communication, reliability, error correction, flow-control and multiplexing (e.g. multicast / broadcast).
   Protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP) (...)
   c) *Internet:* Routing and transmission from source to destination.
   Protocols: Internet Protocol (IP) (v4, v6) (...)
   d) *Network Interface:* Transmission of data between two computers in the same network via physical connection.
   Protocols: Medium Acess Control (MAC), Tunnels, Point to Point Protocol (PPP) (...)

2. **Datagram:** A datagram is a basic transfer unit in a packet-switched network. Datagrams consist of a header and payload. They contain address information and can be send in connectionsless communication.

3. **User Datagram Protocol (UDP):** UDP provides a simple connectionless communication model. It provides checksums for verification of data integrity and port numbers for addressing specific services on the target machine. It does not have handshaking dialogues and requires no previous packets to be send prior to communication. Messages are mapped directly to packets and are not split up into peaces. UDP does not provide a guarantee of delivery, order of packets, or duplicate protection. It therefore exposes the application layer to any unreliability of the network for the sake of less communication overhead. It is suitable for applications which do not require reliability but do require speed e.g. in video streaming or for applications which handle resubmission, ordering and duplicate checking themselves.

4. **Transmission Control Protocol (TCP):** TCP follows a connection-oriented communication model providing reliability, ordering and error checking and flow-control (not allowing one side to send too fast). Messages are handled as a stream of bytes which is split into packets of undefined size for transmission.
   a) *Connection establishment and termination:* The connection is established using a three-way handshake consisting of the packets SYN $\rightarrow$, SYN-ACK $\leftarrow$ and ACK $\rightarrow$. The connection termination is done with a four-way handshake consisting of the packets FIN $\rightarrow$, ACK $\leftarrow$, FIN $\leftarrow$ and ACK $\rightarrow$. It is possible to shorten this by sending a FIN-ACK as a reply to the FIN
   b) *Reliability:* TCP uses a sequence number to identify each byte of data, as shown in figure 1. The sequence number of the first byte is randomly chosen by the sender of the first packet in order to defend against TCP sequence prediction attacks. Each TCP-packet contains a sequence number and – if it is an ACK packet – an acknowledgement number. The sequence number of the packet is the sequence number of the first byte send in this message or the sequence number of the last byte send in previous messages in case the payload (data) of the packet has size zero (as for ACK packets). The acknowledgement number is the incremented sequence number of the last byte received. TCP uses cumulative ACKs, which means that an acknowledgement number of n acknowledges all bytes with sequence number $< n$.
   c) *Resubmission:*
   d)

   .
5. **Autonomous System:**
6. **Round Trip Time (RTT):** Is the transmission time for a packet from point A to point B plus the transmission time of the ACK-packet from point B back to point A. It can be determined using the ping command.
7. **Network Adress Translation (NAT):**
8. **Subnetting:**

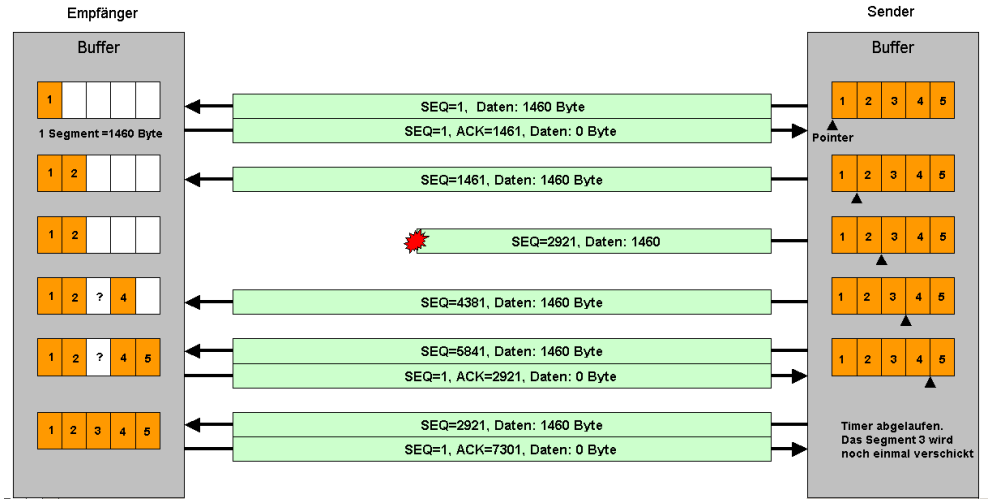

Figure 1: TCP data Transmission with sequence numbers