

Rechnernetze Laborbericht

Labor 3: Socket-Schnittstelle

TIB3 SS 2016

Kazim Kaya
Murat Durgun

Inhalt

1. TCP-Sockets	2
1.1 Nicht nebenläufiger Server und 1 Client	2
1.1.1 Ein Server und ein Client	2
1.1.2 Ein Server und zwei Clients	3
1.1.3 Ein Server und ein Client, vorzeitige Beendigung des Clients	5
1.2 Client-Server-Kommunikation über Tunnel	6
1.3 Zustand half closed untersuchen	7
1.4 Client mit bind	8
1.5 Nebenläufiger Server, zwei Clients.....	9
1.6 UDP-Sockets	10
1.6.1 Requester und Responder im gleichem Sub	10
1.6.2 Requester und Responder in unterschiedlichen Sub mit einem Router dazwischen	10

1. TCP-Sockets

Benutzung der Socket-Schnittstelle mit Verwendung der Transportprotokolle TCP und UDP, Beeinflussung von sockets mit „setsockopt()“, Beobachtung der Arbeitsweise des ONC-RPC sowie Analyse von Datenkommunikation über Tunnel.

1.1 Nicht nebenläufiger Server und 1 Client

Wichtige Funktionen vom **Server**

Zeile: Funktion	Beschreibung
95: socket()	TCP socket
113: bind()	Registrierung
127: listen()	Buffer
150: accept()	Verbindungsaufbau
219: read() (allgemein=recv())	Lese Buffer
270: write() (allgemein=send())	Schreibe an Client
116: close(ss)	Schließt den Socket

Wichtige Funktionen des **Clients**

Zeile: Funktion	Beschreibung
112: socket()	TCP socket
149: bind()	Registrierung
155: close(cs)	Schließt Socket
244: write()	Schreibe an Server
262: read()	Lese Buffer

1.1.1 Ein Server und ein Client

Versuchsziel: Übersetzen und ausführen der vorgegebenen Programme auf zwei verschiedene Rechnern. Dokumentation des Datentransfers im Netzwerk über Wireshark. Herausfinden woran man erkennt, dass es kein nebenläufiger Server ist.

Versuchsdurchführung: Man kann in der Konsolenausgabe sehr schön sehen, dass der Server sich nur mit einem Client verbindet und auch nur mit einem Client unterhält.

Verbindungsaufbau: Client Port (134.108.8.36-54604) Server Port (134.108.8.37)									
21	8.855027	134.108.8.36	134.108.8.37	TCP	74	54604 > 9006 [SYN] Seq=0 win=2920 Len=0 MSS=1460 SACK_PERM=1 TSval=2290216 TSecr=0 WS=1			
22	8.855067	134.108.8.37	134.108.8.36	TCP	74	9006 > 54604 [SYN, ACK] Seq=0 Ack=1 win=2896 Len=0 MSS=1460 SACK_PERM=1 TSval=2962289 TSecr=2290216 WS=1			
23	8.855301	134.108.8.36	134.108.8.37	TCP	66	54604 > 9006 [ACK] Seq=1 Ack=1 win=2920 Len=0 TSval=2290217 TSecr=2962289			
Datenübertragung mit Verbindungsabbau:									
1120	516.699369	134.108.8.36	134.108.8.37	TCP	66	54604 > 9006 [ACK] Seq=60001 Ack=13033 win=2920 Len=0 TSval=2798061 TSecr=3470133			
1121	516.699420	134.108.8.37	134.108.8.36	TCP	1034	9006 > 54604 [PSH, ACK] Seq=13033 Ack=60001 win=2896 Len=968 TSval=3470133 TSecr=2798061			
1122	516.739061	134.108.8.36	134.108.8.37	TCP	66	54604 > 9006 [ACK] Seq=60001 Ack=14001 win=2920 Len=0 TSval=2798101 TSecr=3470133			
1129	520.120153	134.108.8.36	134.108.8.37	TCP	69	54604 > 9006 [PSH, ACK] Seq=60001 Ack=14001 win=2920 Len=3 TSval=2801482 TSecr=3470133			
1130	520.120175	134.108.8.36	134.108.8.37	TCP	66	54604 > 9006 [FIN, ACK] Seq=60004 Ack=14001 win=2920 Len=0 TSval=2801482 TSecr=3470133			
1131	520.120202	134.108.8.37	134.108.8.36	TCP	66	9006 > 54604 [ACK] Seq=14001 Ack=60004 win=2896 Len=0 TSval=3473554 TSecr=2801482			
1132	520.159604	134.108.8.37	134.108.8.36	TCP	66	9006 > 54604 [ACK] Seq=14001 Ack=60005 win=2896 Len=0 TSval=3473594 TSecr=2801482			
1135	521.120323	134.108.8.37	134.108.8.36	TCP	66	9006 > 54604 [FIN, ACK] Seq=14001 Ack=60005 win=2896 Len=0 TSval=3474554 TSecr=2801482			
1136	521.120553	134.108.8.36	134.108.8.37	TCP	66	54604 > 9006 [ACK] Seq=60005 Ack=14002 win=2920 Len=0 TSval=2802482 TSecr=3474554			

Server stdout:

```
[kakait01@itpc3106 tcp_v11]$ ./server_s.out 9006
SERVER: Nicht nebenlaefiger Server, Version: 1.2 ; Autor: H.Ws
SERVER: server_port = 9006
SERVER: socket 4 : Window-Size = 3000
SERVER: socket 4 : MAXSEG = 1448
SERVER: Socket 4 : Mit Client 134.108.8.36 auf Port 54601 Verbindung aufgenommen
SERVER: Socket 4 : Insgesamt 12 Sekunden auf Client gewartet
SERVER: socket 4 : Jetzt vom Client lesen ? (j/n) j
SERVER: socket 4 : Nachricht von Client:
AabcdefghijklmnopqrstuvwxyzBabcdefghijklmnopqrstuvwxyz ...
SERVER: socket 4 : Anzahl gelesener Zeichen in read = 55024
SERVER: socket 4 : Nachricht von Client:
yzKabcdefghijklmnopqrstuvwxyzLabcdxyzabcdefghijklmnopqrstuvwxyz ...
SERVER: socket 4 : Anzahl gelesener Zeichen in read = 2896
.
.
.
SERVER: socket 4 : Nachricht von Client:
efghijklmnopqrstuvwxyz0abcdefghijklmnopqrstuvwxyzP ...
SERVER: socket 4 : Anzahl gelesener Zeichen in read = 2080
SERVER: socket 4 : Jetzt zum Client schreiben ? (j/n) j
SERVER: socket 4 : Anzahl geschriebener Zeichen in write = 14000
SERVER: Socket 4 : Verbindung zum Client beendet. Return-code close() = 0
```

1.1.2 Ein Server und zwei Clients

Versuchsziel: Bei einem nicht neben läufigen Server eine Verbindung mit zwei Clients aufzubauen

Versuchsdurchführung: Client A wird gestartet und sendet direkt Daten zum Server. Anschließend in einem weiteren Fenster, einen weiteren Client B starten und Daten zum Server schicken. Danach wird die Übertragung von A fortgesetzt und nach der Terminierung von A wird B fortgesetzt und beendet.

Woran ist eindeutig erkennbar, dass der Server sequentiell arbeitet?

Auch hier kann man wieder schön in dem Konsolentext erkennen, dass der Server alles nacheinander abarbeitet. Erst Client A, dann Client B.

Wo blockiert der Server?

Wird durch die Funktion listen() blockiert, da nur eine Verbindung zugelassen ist.

Server stdout:

```
SERVER: Nicht nebenlaefiger Server, Version: 1.2 ; Autor: H.Ws
SERVER: server_port = 9006
SERVER: socket 3 : Window-Size = 4096
SERVER: socket 3 : MAXSEG = 536
SERVER: socket 4 : Window-Size = 3000
SERVER: socket 4 : MAXSEG = 1448
SERVER: socket 4 : Mit Client 134.108.8.36 auf Port 54626 Verbindung aufgenommen
SERVER: socket 4 : Insgesamt 279 Sekunden auf Client gewartet
SERVER: socket 4 : Jetzt vom Client lesen ? (j/n) j
SERVER: socket 4 : Nachricht von Client:
AabcdefghijklmnopqrstuvwxyzBabcdefghijklmnopqrstuvwxyz ...
SERVER: socket 4 : Anzahl gelesener Zeichen in read = 55024
SERVER: socket 4 : Nachricht von Client:
yzKabcdefghijklmnopqrstuvwxyzLabcdxyzabcdefghijklmnopqrstuvwxyz ...
SERVER: socket 4 : Anzahl gelesener Zeichen in read = 2896
```

```

SERVER: socket 4 : Nachricht von Client:
efghijklmnopqrstuvwxyz0abcdefghijklmnopqrstuvwxyzP ...
SERVER: socket 4 : Anzahl gelesener Zeichen in read = 2080
SERVER: socket 4 : Jetzt zum Client schreiben ? (j/n) j
SERVER: socket 4 : Anzahl geschriebener Zeichen in write = 14000
SERVER: socket 4 : Verbindung zum Client beendet. Return-code close() = 0
SERVER: socket 4 : Window-Size = 3000
SERVER: socket 4 : MAXSEG = 1448
SERVER: socket 4 : Mit Client 134.108.8.36 auf Port 54627 Verbindung aufgenommen
SERVER: socket 4 : Insgesamt 338 Sekunden auf Client gewartet
SERVER: socket 4 : Jetzt vom Client lesen ? (j/n) j
SERVER: socket 4 : Nachricht von Client:
AabcdefghijklmnopqrstuvwxyzBabcdefghijklmnopqrstuvwxyz ...
SERVER: socket 4 : Anzahl gelesener Zeichen in read = 55024
SERVER: socket 4 : Nachricht von Client:
yzKabcdefghijklmnopqrstuvwxyzLabcd efghijklmnopqrst ...
SERVER: socket 4 : Anzahl gelesener Zeichen in read = 2896
SERVER: socket 4 : Nachricht von Client:
efghijklmnopqrstuvwxyz0abcdefghijklmnopqrstuvwxyzP ...
SERVER: socket 4 : Anzahl gelesener Zeichen in read = 2080
SERVER: socket 4 : Jetzt zum Client schreiben ? (j/n) j
SERVER: socket 4 : Anzahl geschriebener Zeichen in write = 14000
SERVER: socket 4 : Verbindung zum Client beendet. Return-code close() = 0

```

Beschreibung des Wireshark trace

- 1) Hier könne wir den Three-Way-Handshake zum Verbindungsaufbau des ersten Clients sehen.

No.	Time	Source	Destination	Protocol	Length	Info
134	66.064372	134.108.8.36	134.108.8.37	TCP	74	54626 > 9006 [SYN] Seq=0 win=2920 Len=0 MSS=1460 SACK_PERM=1 TSval=4642103 TSecr=0 WS=1
135	66.064613	134.108.8.37	134.108.8.36	TCP	74	9006 > 54626 [SYN, ACK] Seq=0 Ack=1 win=2896 Len=0 MSS=1460 SACK_PERM=1 TSval=5314177 TSecr=4642103 WS=1
136	66.064651	134.108.8.36	134.108.8.37	TCP	66	54626 > 9006 [ACK] Seq=1 Ack=1 win=2920 Len=0 TSval=4642104 TSecr=5314177

- 2) Dynamische Buffer Erweiterung Client 1

No.	Time	Source	Destination	Protocol	Length	Info
170	76.132920	134.108.8.36	134.108.8.37	TCP	1514	54626 > 9006 [ACK] Seq=1 Ack=1 win=2920 Len=1448 TSval=4652173 TSecr=5314177
171	76.132943	134.108.8.36	134.108.8.37	TCP	1514	[TCP window Full] 54626 > 9006 [PSH, ACK] Seq=1449 Ack=1 win=2920 Len=1448 TSval=4652173 TSecr=5314177
172	76.133212	134.108.8.37	134.108.8.36	TCP	66	9006 > 54626 [ACK] Seq=1 Ack=1449 win=2896 Len=0 TSval=5324245 TSecr=4652173
173	76.133242	134.108.8.36	134.108.8.37	TCP	1514	[TCP window Full] 54626 > 9006 [ACK] Seq=2897 Ack=1 win=2920 Len=1448 TSval=4652173 TSecr=5324245
174	76.133471	134.108.8.37	134.108.8.36	TCP	66	9006 > 54626 [ACK] Seq=1 Ack=4345 win=2896 Len=0 TSval=5324245 TSecr=4652173
175	76.133497	134.108.8.36	134.108.8.37	TCP	1514	54626 > 9006 [PSH, ACK] Seq=4345 Ack=1 win=2920 Len=1448 TSval=4652173 TSecr=5324245
176	76.133505	134.108.8.36	134.108.8.37	TCP	1514	[TCP window Full] 54626 > 9006 [ACK] Seq=5529 Ack=1 win=2920 Len=1448 TSval=4652173 TSecr=5324245
177	76.133720	134.108.8.37	134.108.8.36	TCP	66	9006 > 54626 [ACK] Seq=1 Ack=7241 win=2896 Len=0 TSval=5324246 TSecr=4652173
178	76.133745	134.108.8.36	134.108.8.37	TCP	1514	54626 > 9006 [PSH, ACK] Seq=7241 Ack=1 win=2920 Len=1448 TSval=4652173 TSecr=5324246
179	76.133753	134.108.8.36	134.108.8.37	TCP	1514	[TCP window Full] 54626 > 9006 [ACK] Seq=8689 Ack=1 win=2920 Len=1448 TSval=4652173 TSecr=5324246
180	76.133975	134.108.8.37	134.108.8.36	TCP	66	9006 > 54626 [ACK] Seq=1 Ack=10137 win=2896 Len=0 TSval=5324246 TSecr=4652173
181	76.134000	134.108.8.36	134.108.8.37	TCP	1514	54626 > 9006 [PSH, ACK] Seq=10137 Ack=1 win=2920 Len=1448 TSval=4652174 TSecr=5324246
182	76.134009	134.108.8.36	134.108.8.37	TCP	1514	[TCP window Full] 54626 > 9006 [PSH, ACK] Seq=11385 Ack=1 win=2920 Len=1448 TSval=4652174 TSecr=5324246
183	76.134230	134.108.8.37	134.108.8.36	TCP	66	9006 > 54626 [ACK] Seq=1 Ack=13033 win=2896 Len=0 TSval=5324246 TSecr=4652174
184	76.134255	134.108.8.36	134.108.8.37	TCP	1514	54626 > 9006 [ACK] Seq=13033 Ack=1 win=2920 Len=1448 TSval=4652174 TSecr=5324246
185	76.134263	134.108.8.36	134.108.8.37	TCP	1514	[TCP window Full] 54626 > 9006 [PSH, ACK] Seq=14481 Ack=1 win=2920 Len=1448 TSval=4652174 TSecr=5324246
186	76.134437	134.108.8.37	134.108.8.36	TCP	66	9006 > 54626 [ACK] Seq=1 Ack=15929 win=2896 Len=0 TSval=5324246 TSecr=4652174

- 3) Buffer ist voll

No.	Time	Source	Destination	Protocol	Length	Info
224	76.137449	134.108.8.36	134.108.8.37	TCP	1514	[TCP window Full] 54626 > 9006 [PSH, ACK] Seq=52129 Ack=1 win=2920 Len=1448 TSval=4652177 TSecr=5324249
225	76.177561	134.108.8.37	134.108.8.36	TCP	66	9006 > 54626 [ACK] Seq=1 Ack=53577 win=1448 Len=0 TSval=5324290 TSecr=4652177
226	76.177603	134.108.8.36	134.108.8.37	TCP	1514	[TCP window Full] 54626 > 9006 [ACK] Seq=53577 Ack=1 win=2920 Len=1448 TSval=4652217 TSecr=5324290
227	76.217555	134.108.8.37	134.108.8.36	TCP	66	[TCP ZeroWindow] 9006 > 54626 [ACK] Seq=1 Ack=55025 win=0 Len=0 TSval=5324330 TSecr=4652217
228	76.426832	134.108.8.36	134.108.8.37	TCP	66	[TCP Keep-Alive] 54626 > 9006 [ACK] Seq=55024 Ack=1 win=2920 Len=0 TSval=4652467 TSecr=5324330
229	76.427054	134.108.8.37	134.108.8.36	TCP	66	[TCP ZeroWindow] 9006 > 54626 [ACK] Seq=1 Ack=55025 win=0 Len=0 TSval=5324339 TSecr=4652217
230	76.845841	134.108.8.36	134.108.8.37	TCP	66	[TCP Keep-Alive] 54626 > 9006 [ACK] Seq=55024 Ack=1 win=2920 Len=0 TSval=4652887 TSecr=5324339
231	76.847104	134.108.8.37	134.108.8.36	TCP	66	[TCP ZeroWindow] 9006 > 54626 [ACK] Seq=1 Ack=55025 win=0 Len=0 TSval=5324959 TSecr=4652217
232	77.098624	134.108.8.36	134.108.8.37	TCP	66	[TCP Keep-Alive] 54626 > 9006 [ACK] Seq=55024 Ack=1 win=2920 Len=0 TSval=4653727 TSecr=5324959
233	77.097069	134.108.8.37	134.108.8.36	TCP	66	[TCP ZeroWindow] 9006 > 54626 [ACK] Seq=1 Ack=55025 win=0 Len=0 TSval=5325799 TSecr=4652217
237	79.396840	134.108.8.36	134.108.8.37	TCP	66	[TCP Keep-Alive] 54626 > 9006 [ACK] Seq=55024 Ack=1 win=2920 Len=0 TSval=4655407 TSecr=5325799
238	79.367088	134.108.8.37	134.108.8.36	TCP	66	[TCP ZeroWindow] 9006 > 54626 [ACK] Seq=1 Ack=55025 win=0 Len=0 TSval=5327479 TSecr=4652217
241	82.726848	134.108.8.36	134.108.8.37	TCP	66	[TCP Keep-Alive] 54626 > 9006 [ACK] Seq=55024 Ack=1 win=2920 Len=0 TSval=4658767 TSecr=5327479
242	82.727120	134.108.8.37	134.108.8.36	TCP	66	[TCP ZeroWindow] 9006 > 54626 [ACK] Seq=1 Ack=55025 win=0 Len=0 TSval=5330839 TSecr=4652217

- 4) Verbindungsaufbau des 2. Clients

No.	Time	Source	Destination	Protocol	Length	Info
248	86.679035	134.108.8.36	134.108.8.37	TCP	74	54627 > 9006 [SYN] Seq=0 win=2920 Len=0 MSS=1460 SACK_PERM=1 TSval=4662718 TSecr=0 WS=1
249	86.679260	134.108.8.37	134.108.8.36	TCP	74	9006 > 54627 [SYN, ACK] Seq=0 Ack=1 win=2896 Len=0 MSS=1460 SACK_PERM=1 TSval=5334791 TSecr=4662718 WS=1
250	86.679296	134.108.8.36	134.108.8.37	TCP	66	54627 > 9006 [ACK] Seq=1 Ack=1 win=2920 Len=0 TSval=4662719 TSecr=5334791

5) Dynamische Buffer Erweiterung Client 2

No.	Time	Source	Destination	Protocol	Length	Info
274	102.126266	134.108.8.36	134.108.8.37	TCP	1514	54627 > 9006 [ACK] Seq=13033 Ack=1 win=2920 Len=1448 TSval=4678166 TSecr=5350238
275	102.126274	134.108.8.36	134.108.8.37	TCP	1514	[TCP window Full] 54627 > 9006 [PSH, ACK] Seq=14481 Ack=1 win=2920 Len=1448 TSval=4678166 TSecr=5350238
276	102.126467	134.108.8.37	134.108.8.36	TCP	66	9006 > 54627 [ACK] Seq=1 Ack=15929 win=2896 Len=0 TSval=5350238 TSecr=4678166
277	102.126492	134.108.8.36	134.108.8.37	TCP	1514	54627 > 9006 [ACK] Seq=15929 Ack=1 win=2920 Len=1448 TSval=4678166 TSecr=5350238
278	102.126500	134.108.8.36	134.108.8.37	TCP	1514	[TCP window Full] 54627 > 9006 [PSH, ACK] Seq=17377 Ack=1 win=2920 Len=1448 TSval=4678166 TSecr=5350238
279	102.126714	134.108.8.37	134.108.8.36	TCP	66	9006 > 54627 [ACK] Seq=1 Ack=18825 win=2896 Len=0 TSval=5350239 TSecr=4678166
280	102.126728	134.108.8.36	134.108.8.37	TCP	1514	54627 > 9006 [ACK] Seq=18825 Ack=1 win=2920 Len=1448 TSval=4678166 TSecr=5350239
281	102.126735	134.108.8.36	134.108.8.37	TCP	1514	[TCP window Full] 54627 > 9006 [PSH, ACK] Seq=20273 Ack=1 win=2920 Len=1448 TSval=4678166 TSecr=5350239
282	102.126949	134.108.8.37	134.108.8.36	TCP	66	9006 > 54627 [ACK] Seq=1 Ack=21721 win=2896 Len=0 TSval=5350239 TSecr=4678166
283	102.126963	134.108.8.36	134.108.8.37	TCP	1514	54627 > 9006 [ACK] Seq=21721 Ack=1 win=2920 Len=1448 TSval=4678167 TSecr=5350239
284	102.126969	134.108.8.36	134.108.8.37	TCP	1514	[TCP window Full] 54627 > 9006 [PSH, ACK] Seq=23169 Ack=1 win=2920 Len=1448 TSval=4678167 TSecr=5350239
285	102.127177	134.108.8.37	134.108.8.36	TCP	66	9006 > 54627 [ACK] Seq=1 Ack=24617 win=2896 Len=0 TSval=5350239 TSecr=4678167
286	102.127191	134.108.8.36	134.108.8.37	TCP	1514	54627 > 9006 [ACK] Seq=24617 Ack=1 win=2920 Len=1448 TSval=4678167 TSecr=5350239
287	102.127196	134.108.8.36	134.108.8.37	TCP	1514	[TCP window Full] 54627 > 9006 [PSH, ACK] Seq=26065 Ack=1 win=2920 Len=1448 TSval=4678167 TSecr=5350239
288	102.127395	134.108.8.37	134.108.8.36	TCP	66	9006 > 54627 [ACK] Seq=1 Ack=27513 win=2896 Len=0 TSval=5350239 TSecr=4678167

6) Buffer wieder voll

No.	Time	Source	Destination	Protocol	Length	Info
314	102.129437	134.108.8.36	134.108.8.37	TCP	1514	[TCP window Full] 54627 > 9006 [PSH, ACK] Seq=52129 Ack=1 win=2920 Len=1448 TSval=4678169 TSecr=5350241
315	102.129558	134.108.8.37	134.108.8.36	TCP	66	9006 > 54627 [ACK] Seq=1 Ack=53577 win=2896 Len=0 TSval=5350282 TSecr=4678169
316	102.129605	134.108.8.36	134.108.8.37	TCP	1514	[TCP window Full] 54627 > 9006 [ACK] Seq=53577 Ack=1 win=2920 Len=1448 TSval=4678209 TSecr=5350282
318	102.129554	134.108.8.37	134.108.8.36	TCP	66	[TCP ZeroWindow] 9006 > 54627 [ACK] Seq=1 Ack=55025 win=0 Len=0 TSval=5350322 TSecr=4678209
319	102.418851	134.108.8.36	134.108.8.37	TCP	66	[TCP keep-alive] 54627 > 9006 [ACK] Seq=55024 Ack=1 win=2920 Len=0 TSval=4678459 TSecr=5350322
320	102.419089	134.108.8.37	134.108.8.36	TCP	66	[TCP ZeroWindow] 9006 > 54627 [ACK] Seq=1 Ack=55025 win=0 Len=0 TSval=5350331 TSecr=4678209
321	102.838836	134.108.8.36	134.108.8.37	TCP	66	[TCP keep-alive] 54627 > 9006 [ACK] Seq=55024 Ack=1 win=2920 Len=0 TSval=4678879 TSecr=5350331
322	102.839059	134.108.8.37	134.108.8.36	TCP	66	[TCP ZeroWindow] 9006 > 54627 [ACK] Seq=1 Ack=55025 win=0 Len=0 TSval=5350391 TSecr=4678209
323	102.866821	134.108.8.36	134.108.8.37	TCP	66	[TCP keep-alive] 54626 > 9006 [ACK] Seq=55024 Ack=1 win=2920 Len=0 TSval=4678927 TSecr=5357359
324	102.867048	134.108.8.37	134.108.8.36	TCP	66	[TCP ZeroWindow] 9006 > 54626 [ACK] Seq=1 Ack=55025 win=0 Len=0 TSval=5350399 TSecr=4683217
325	103.678819	134.108.8.36	134.108.8.37	TCP	66	[TCP keep-alive] 54627 > 9006 [ACK] Seq=55024 Ack=1 win=2920 Len=0 TSval=4679719 TSecr=5350391
326	103.679049	134.108.8.37	134.108.8.36	TCP	66	[TCP ZeroWindow] 9006 > 54627 [ACK] Seq=1 Ack=55025 win=0 Len=0 TSval=5351791 TSecr=4678209
328	103.358868	134.108.8.36	134.108.8.37	TCP	66	[TCP keep-alive] 54627 > 9006 [ACK] Seq=55024 Ack=1 win=2920 Len=0 TSval=4681399 TSecr=5351791
287	102.127196	134.108.8.36	134.108.8.37	TCP	1514	[TCP window Full] 54627 > 9006 [PSH, ACK] Seq=26065 Ack=1 win=2920 Len=1448 TSval=4678167 TSecr=5350239

7) Daten vom 1. Client empfangen und Verbindung beenden

No.	Time	Source	Destination	Protocol	Length	Info
441	124.269372	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54626 [PSH, ACK] Seq=4345 Ack=60001 win=2896 Len=1448 TSval=5372381 TSecr=4700308
442	124.269390	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54626 [ACK] Seq=5793 Ack=60001 win=2896 Len=1448 TSval=5372381 TSecr=4700308
443	124.269415	134.108.8.36	134.108.8.37	TCP	66	54626 > 9006 [ACK] Seq=60001 Ack=7241 win=2920 Len=0 TSval=4700309 TSecr=5372381
444	124.269627	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54626 [PSH, ACK] Seq=7241 Ack=60001 win=2896 Len=1448 TSval=5372382 TSecr=4700309
445	124.269635	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54626 [ACK] Seq=8689 Ack=60001 win=2896 Len=1448 TSval=5372382 TSecr=4700309
446	124.269653	134.108.8.36	134.108.8.37	TCP	66	54626 > 9006 [ACK] Seq=60001 Ack=10137 win=2920 Len=0 TSval=4700309 TSecr=5372382
447	124.269699	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54626 [PSH, ACK] Seq=10137 Ack=60001 win=2896 Len=1448 TSval=5372382 TSecr=4700309
448	124.269926	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54626 [PSH, ACK] Seq=11585 Ack=60001 win=2896 Len=1448 TSval=5372382 TSecr=4700309
449	124.269938	134.108.8.36	134.108.8.37	TCP	66	54626 > 9006 [ACK] Seq=60001 Ack=13033 win=2920 Len=0 TSval=4700309 TSecr=5372382
450	124.270151	134.108.8.37	134.108.8.36	TCP	1034	9006 > 54626 [PSH, ACK] Seq=13033 Ack=60001 win=2896 Len=968 TSval=5372382 TSecr=4700309
451	124.270181	134.108.8.36	134.108.8.37	TCP	66	54626 > 9006 [ACK] Seq=60001 Ack=14001 win=2920 Len=0 TSval=4700310 TSecr=5372382
452	124.270202	134.108.8.36	134.108.8.37	TCP	69	54626 > 9006 [PSH, ACK] Seq=60001 Ack=14001 win=2920 Len=3 TSval=4700310 TSecr=5372382
453	124.270215	134.108.8.36	134.108.8.37	TCP	66	54626 > 9006 [FIN, ACK] Seq=60004 Ack=14001 win=2920 Len=0 TSval=4700310 TSecr=5372382
454	124.270390	134.108.8.37	134.108.8.36	TCP	66	9006 > 54626 [ACK] Seq=14001 Ack=60004 win=2896 Len=0 TSval=5372382 TSecr=4700310
455	124.309562	134.108.8.37	134.108.8.36	TCP	66	9006 > 54626 [ACK] Seq=14001 Ack=60005 win=2896 Len=0 TSval=5372422 TSecr=4700310
459	125.270557	134.108.8.37	134.108.8.36	TCP	66	9006 > 54626 [FIN, ACK] Seq=14001 Ack=60005 win=2896 Len=0 TSval=5373382 TSecr=4700310
460	125.270593	134.108.8.36	134.108.8.37	TCP	66	54626 > 9006 [ACK] Seq=60005 Ack=14002 win=2920 Len=0 TSval=4701310 TSecr=5373382

8) Daten vom 2. Client empfangen und Verbindung beenden

No.	Time	Source	Destination	Protocol	Length	Info
622	157.773617	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54627 [PSH, ACK] Seq=7241 Ack=60001 win=2896 Len=1448 TSval=5405886 TSecr=4733813
623	157.773636	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54627 [ACK] Seq=8689 Ack=60001 win=2896 Len=1448 TSval=5405886 TSecr=4733813
624	157.773647	134.108.8.36	134.108.8.37	TCP	66	54627 > 9006 [ACK] Seq=60001 Ack=10137 win=2920 Len=0 TSval=5405886 TSecr=5405886
625	157.773914	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54627 [PSH, ACK] Seq=10137 Ack=60001 win=2896 Len=1448 TSval=5405886 TSecr=4733813
626	157.773934	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54627 [PSH, ACK] Seq=11585 Ack=60001 win=2896 Len=1448 TSval=5405886 TSecr=4733813
627	157.773945	134.108.8.36	134.108.8.37	TCP	66	54627 > 9006 [ACK] Seq=60001 Ack=13033 win=2920 Len=0 TSval=5473814 TSecr=5405886
628	157.774220	134.108.8.37	134.108.8.36	TCP	1034	9006 > 54627 [PSH, ACK] Seq=13033 Ack=60001 win=2896 Len=968 TSval=5405886 TSecr=4733814
629	157.813822	134.108.8.36	134.108.8.37	TCP	66	54627 > 9006 [ACK] Seq=60001 Ack=14001 win=2920 Len=0 TSval=5473854 TSecr=5405886
646	163.309947	134.108.8.36	134.108.8.37	TCP	69	54627 > 9006 [PSH, ACK] Seq=60001 Ack=14001 win=2920 Len=3 TSval=4739350 TSecr=5405886
647	163.309967	134.108.8.36	134.108.8.37	TCP	66	54627 > 9006 [FIN, ACK] Seq=60004 Ack=14001 win=2920 Len=0 TSval=4739350 TSecr=5405886
648	163.310208	134.108.8.37	134.108.8.36	TCP	66	9006 > 54627 [ACK] Seq=14001 Ack=60004 win=2896 Len=0 TSval=5411422 TSecr=4739350
649	163.349558	134.108.8.37	134.108.8.36	TCP	66	9006 > 54627 [ACK] Seq=14001 Ack=60005 win=2896 Len=0 TSval=5411462 TSecr=4739350
652	164.310345	134.108.8.37	134.108.8.36	TCP	66	9006 > 54627 [FIN, ACK] Seq=14001 Ack=60005 win=2896 Len=0 TSval=5412422 TSecr=4739350
653	164.310376	134.108.8.36	134.108.8.37	TCP	66	54627 > 9006 [ACK] Seq=60005 Ack=14002 win=2920 Len=0 TSval=4740350 TSecr=5412422

1.1.3 Ein Server und ein Client, vorzeitige Beendigung des Clients

Versuchsziel: Ein Server (nicht neben läufig) und ein Client, jedoch wird die Verbindung frühzeitig von der Clientseite beendet.

Versuchsdurchführung: Der Server und der Client werden gestartet. Im Server beantworten wir zunächst die Frage nach Lesen mit „n“ und die anschließende Frage nach Schreiben mit „j“. Im Client beantworten wir nun die Frage nach Schreiben mit „n“ und die anschließende Frage nach Lesen ebenfalls mit „n“.

Warum wird kein PDU mit FIN gesendet?

Der Server schickt zwar Daten, welche auch im Buffer landen aber der Client lehnt jede reinkommende Nachricht vom Server ab. Wie man auch am Schluss sieht wird sogar die Bestätigung des RST Signals abgelehnt.

Wozu dient die RST-PDU?

Damit der Server mitgeteilt bekommt das der Client nichts annehmen will.

Was passiert mit den Daten des Servers?

Die befinden sich im Buffer werden aber nicht ausgelesen.

No.	Time	Source	Destination	Protocol	Length	Info
23	28.087199	134.108.8.36	134.108.8.37	TCP	74	54638 > 9006 [SYN] Seq=0 win=2920 Len=0 MSS=1460 SACK_PERM=1 TSval=6155704 TSecr=0 WS=1
24	28.087251	134.108.8.37	134.108.8.36	TCP	74	9006 > 54638 [SYN, ACK] Seq=0 Ack=1 win=2896 Len=0 MSS=1460 SACK_PERM=1 TSval=6827776 TSecr=6155704 WS=1
25	28.087471	134.108.8.36	134.108.8.37	TCP	66	54638 > 9006 [ACK] Seq=1 Ack=1 win=2920 Len=0 TSval=6155704 TSecr=6827776
100	80.491931	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54638 [ACK] Seq=1 Ack=1 win=2896 Len=1448 TSval=6880181 TSecr=6155704
101	80.491948	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54638 [PSH, ACK] Seq=1449 Ack=1 win=2896 Len=1448 TSval=6880181 TSecr=6155704
102	80.492183	134.108.8.36	134.108.8.37	TCP	66	54638 > 9006 [ACK] Seq=1 Ack=1449 win=2920 Len=0 TSval=6208109 TSecr=6880181
103	80.492213	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54638 [ACK] Seq=2897 Ack=1 win=2896 Len=1448 TSval=6880181 TSecr=6208109
104	80.492422	134.108.8.36	134.108.8.37	TCP	66	54638 > 9006 [ACK] Seq=1 Ack=4345 win=2920 Len=0 TSval=6208109 TSecr=6880181
105	80.492454	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54638 [PSH, ACK] Seq=4345 Ack=1 win=2896 Len=1448 TSval=6880181 TSecr=6208109
106	80.492462	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54638 [ACK] Seq=5793 Ack=1 win=2896 Len=1448 TSval=6880181 TSecr=6208109
107	80.492666	134.108.8.36	134.108.8.37	TCP	66	54638 > 9006 [ACK] Seq=1 Ack=7241 win=2920 Len=0 TSval=6208109 TSecr=6880181
108	80.492704	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54638 [PSH, ACK] Seq=7241 Ack=1 win=2896 Len=1448 TSval=6880182 TSecr=6208109
109	80.492714	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54638 [ACK] Seq=8689 Ack=1 win=2896 Len=1448 TSval=6880182 TSecr=6208109
110	80.492915	134.108.8.36	134.108.8.37	TCP	66	54638 > 9006 [ACK] Seq=1 Ack=10137 win=2920 Len=0 TSval=6208110 TSecr=6880182
111	80.492946	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54638 [PSH, ACK] Seq=10137 Ack=1 win=2896 Len=1448 TSval=6880182 TSecr=6208110
112	80.492955	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54638 [PSH, ACK] Seq=11585 Ack=1 win=2896 Len=1448 TSval=6880182 TSecr=6208110
113	80.493159	134.108.8.36	134.108.8.37	TCP	66	54638 > 9006 [ACK] Seq=1 Ack=13033 win=2920 Len=0 TSval=6208110 TSecr=6880182
114	80.493189	134.108.8.37	134.108.8.36	TCP	1034	9006 > 54638 [PSH, ACK] Seq=13033 Ack=1 win=2896 Len=968 TSval=6880182 TSecr=6208110
115	80.532878	134.108.8.36	134.108.8.37	TCP	66	54638 > 9006 [ACK] Seq=1 Ack=14001 win=2920 Len=0 TSval=6208150 TSecr=6880182
333	169.612984	134.108.8.36	134.108.8.37	TCP	69	54638 > 9006 [PSH, ACK] Seq=1 Ack=14001 win=2920 Len=3 TSval=6297230 TSecr=6880182
334	169.613004	134.108.8.36	134.108.8.37	TCP	66	54638 > 9006 [RST, ACK] Seq=4 Ack=14001 win=2920 Len=0 TSval=6297230 TSecr=6880182
335	169.613028	134.108.8.37	134.108.8.36	TCP	66	9006 > 54638 [ACK] Seq=14001 Ack=4 win=2896 Len=0 TSval=6969302 TSecr=6297230
336	169.613293	134.108.8.36	134.108.8.37	TCP	60	54638 > 9006 [RST] Seq=4 win=0 Len=0

Server stdout:

```
[kakait01@itpc3106 tcp_v11]$ ./server_s.out 9006
SERVER: Nicht nebenlaeufiger Server, Version: 1.2 ; Autor: H.Ws
SERVER: server_port = 9006
SERVER: socket 3 : Window-Size = 4096
SERVER: socket 3 : MAXSEG = 536
SERVER: socket 4 : Window-Size = 3000
SERVER: socket 4 : MAXSEG = 1448
SERVER: socket 4 : Mit Client 134.108.8.36 auf Port 54638 Verbindung aufgenommen
SERVER: socket 4 : Insgesamt 21 Sekunden auf Client gewartet
SERVER: socket 4 : Jetzt vom Client lesen ? (j/n) n
SERVER: socket 4 : Jetzt zum Client schreiben ? (j/n) j
SERVER: socket 4 : Anzahl geschriebener Zeichen in write = 14000
SERVER: socket 4 : Verbindung zum Client beendet. Return-code close() = 0
```

1.2 Client-Server-Kommunikation über Tunnel

Versuchsziel: Verbindung mit einem Rechner in einem anderen Subnetz. Da die **mss** nicht ausreicht (zu klein) muss diese angepasst werden.

Versuchsdurchführung: Ein Rechner aus dem Rechenzentrum verbindet sich auf den Rechner außerhalb des Subnetzes und startet dort den Server. Der Rechner innerhalb des Subnetzes ist unser Client. Dann werden die vorgegebenen Programme ausgeführt.

Wie wurde die MSS berechnet?

Headergröße besteht aus 20 Byte IP, 20 Byte TCP und 24 Byte Tunneling)
somit bleiben: von 1500 Bytes - 20 Bytes - 20 Bytes - 24 Bytes = 1436 Bytes für die **mss** (maximum segment size).

Was sagt die ICMP Nachricht vom Router?

Wie auf dem Bild vom Wireshark zu sehen bei Frame No. 8 schickt der Router eine ICMP Nachricht mit der Info, dass eine Fragmentierung notwendig ist.

Warum soll fragmentiert werden?

Das Datenpaket muss fragmentiert werden, da Ethernet maximal 1500 Bytes pro Paket versendet.

Wie sieht TCP Segmentierung aus? Ist diese Segmentierung sinnvoll?

Die TCP Segmentierung fragmentiert das Datenpaket in zwei Datenpakete, einmal mit 1424 Bytes und einmal mit 24 Bytes Daten, dies führt zu unnötigem Datenverkehr. Dies könnte man durch verringern der **mss** um 24 Bytes auf dem Clientserver.

Mit Zwangsfragmentierung

No.	Time	Source	Destination	Protocol	Length	Info
6	4.950733	134.108.8.36	134.108.190.10	TCP	1514	9005 > sdr [ACK] Seq=1 Ack=1 win=2920 Len=1448 Tsva1=494248 TSecr=3623469218
7	4.950755	134.108.8.36	134.108.190.10	TCP	1514	9005 > sdr [PSH, ACK] Seq=1449 Ack=1 win=2920 Len=1448 Tsva1=494248 TSecr=3623469218
8	4.951461	134.108.11.254	134.108.8.36	ICMP	70	Destination unreachable (Fragmentation needed)
9	4.951497	134.108.8.36	134.108.190.10	TCP	1490	[TCP out-of-order] 9005 > sdr [ACK] Seq=1 Ack=1 win=2920 Len=1424 Tsva1=494249 TSecr=3623469218
10	4.951507	134.108.8.36	134.108.190.10	TCP	90	[TCP out-of-order] 9005 > sdr [ACK] Seq=1425 Ack=1 win=2920 Len=24 Tsva1=494249 TSecr=3623469218
11	4.951513	134.108.8.36	134.108.190.10	TCP	1490	[TCP out-of-order] 9005 > sdr [ACK] Seq=1449 Ack=1 win=2920 Len=1424 Tsva1=494249 TSecr=3623469218
12	4.951513	134.108.8.36	134.108.190.10	TCP	90	[TCP out-of-order] 9005 > sdr [PSH, ACK] Seq=2873 Ack=1 win=2920 Len=24 Tsva1=494249 TSecr=3623469218
13	4.952199	134.108.190.10	134.108.8.36	TCP	66	sdr > 9005 [ACK] Seq=1 Ack=1425 win=2896 Len=0 Tsva1=3623493010 TSecr=494249
14	4.952229	134.108.8.36	134.108.190.10	TCP	1490	9005 > sdr [ACK] Seq=2897 Ack=1 win=2920 Len=1424 Tsva1=494249 TSecr=3623493010
15	4.952261	134.108.190.10	134.108.8.36	TCP	66	sdr > 9005 [ACK] Seq=1 Ack=2873 win=2896 Len=0 Tsva1=3623493010 TSecr=494249
16	4.952270	134.108.8.36	134.108.190.10	TCP	90	9005 > sdr [ACK] Seq=4321 Ack=1 win=2920 Len=24 Tsva1=494249 TSecr=3623493010
17	4.952275	134.108.8.36	134.108.190.10	TCP	1490	9005 > sdr [ACK] Seq=4345 Ack=1 win=2920 Len=1424 Tsva1=494249 TSecr=3623493010
18	4.952891	134.108.190.10	134.108.8.36	TCP	66	sdr > 9005 [ACK] Seq=1 Ack=4321 win=2896 Len=0 Tsva1=3623493011 TSecr=494249
19	4.952924	134.108.8.36	134.108.190.10	TCP	90	9005 > sdr [PSH, ACK] Seq=5769 Ack=1 win=2920 Len=24 Tsva1=494250 TSecr=3623493011
20	4.952934	134.108.8.36	134.108.190.10	TCP	1490	9005 > sdr [ACK] Seq=5793 Ack=1 win=2920 Len=1424 Tsva1=494250 TSecr=3623493011
21	4.953010	134.108.190.10	134.108.8.36	TCP	66	sdr > 9005 [ACK] Seq=1 Ack=5769 win=2896 Len=0 Tsva1=3623493011 TSecr=494249
113	80.493159	134.108.8.36	134.108.8.37	TCP	66	54638 > 9006 [ACK] Seq=1 Ack=13033 win=2920 Len=0 Tsva1=6208110 TSecr=6880182
114	80.493189	134.108.8.37	134.108.8.36	TCP	1034	9006 > 54638 [PSH, ACK] Seq=13033 Ack=1 win=2896 Len=968 Tsva1=6880182 TSecr=6208110
115	80.532878	134.108.8.36	134.108.8.37	TCP	66	54638 > 9006 [ACK] Seq=1 Ack=14001 win=2920 Len=0 Tsva1=6208150 TSecr=6880182

Ohne Zwangsfragmentierung

No.	Time	Source	Destination	Protocol	Length	Info
334	162.246585	134.108.8.37	134.108.190.10	TCP	74	44287 > 9005 [SYN] Seq=0 win=2872 Len=0 MSS=1436 SACK_PERM=1 Tsva1=10283103 TSecr=0 WS=1
335	162.247079	134.108.190.10	134.108.8.37	TCP	74	9005 > 44287 [SYN, ACK] Seq=0 Ack=1 win=2896 Len=0 MSS=1460 SACK_PERM=1 Tsva1=3538582296
336	162.247117	134.108.8.37	134.108.190.10	TCP	66	44287 > 9005 [ACK] Seq=1 Ack=1 win=2872 Len=0 Tsva1=10283104 TSecr=3538582296
342	166.131734	134.108.8.37	134.108.190.10	TCP	1490	44287 > 9005 [ACK] Seq=1 Ack=1 win=2872 Len=1424 Tsva1=10286989 TSecr=3538582296
343	166.131782	134.108.8.37	134.108.190.10	TCP	1490	44287 > 9005 [PSH, ACK] Seq=1425 Ack=1 win=2872 Len=1424 Tsva1=10286989 TSecr=3538582296
344	166.132446	134.108.190.10	134.108.8.37	TCP	66	9005 > 44287 [ACK] Seq=1 Ack=1425 win=2896 Len=0 Tsva1=3538586182 TSecr=10286989
345	166.132474	134.108.8.37	134.108.190.10	TCP	1490	44287 > 9005 [ACK] Seq=2849 Ack=1 win=2872 Len=1424 Tsva1=10286989 TSecr=3538586182
346	166.133161	134.108.190.10	134.108.8.37	TCP	66	9005 > 44287 [ACK] Seq=1 Ack=4273 win=2896 Len=0 Tsva1=3538586182 TSecr=10286989
347	166.133191	134.108.8.37	134.108.190.10	TCP	1490	44287 > 9005 [PSH, ACK] Seq=4273 Ack=1 win=2872 Len=1424 Tsva1=10286990 TSecr=3538586182
348	166.133200	134.108.8.37	134.108.190.10	TCP	1490	44287 > 9005 [ACK] Seq=5697 Ack=1 win=2872 Len=1424 Tsva1=10286990 TSecr=3538586182
349	166.133975	134.108.190.10	134.108.8.37	TCP	66	9005 > 44287 [ACK] Seq=1 Ack=7121 win=2896 Len=0 Tsva1=3538586183 TSecr=10286990
350	166.134000	134.108.8.37	134.108.190.10	TCP	1490	44287 > 9005 [PSH, ACK] Seq=7121 Ack=1 win=2872 Len=1424 Tsva1=10286991 TSecr=3538586183
351	166.134009	134.108.8.37	134.108.190.10	TCP	1490	44287 > 9005 [ACK] Seq=8545 Ack=1 win=2872 Len=1424 Tsva1=10286991 TSecr=3538586183
352	166.134807	134.108.190.10	134.108.8.37	TCP	66	9005 > 44287 [ACK] Seq=1 Ack=9969 win=2896 Len=0 Tsva1=3538586184 TSecr=10286991

1.3 Zustand half closed untersuchen

```
[kakait01@itpc3106 tcp_v11]$ ./client_s.out 134.108.8.36 9005
```

CLIENT: Version: 1.2 ; Autor : H.Ws

CLIENT: server_port = 9005

CLIENT: socket = 3 : MAXSEG = 536

CLIENT: socket = 3 : Window-Size = 4096

CLIENT: Verbindung mit Server 134.108.8.36 auf Port 9005 aufgenommen

CLIENT: socket = 3 ; Nach setsockopt : TTL = 32

CLIENT: 0 Sek.: Vor write(s_buf,60000), vor read!

CLIENT: Socket zum Schreiben schliessen ? (j/n) j

CLIENT: Jetzt zum Server schreiben ? (j/n) n

CLIENT: Jetzt vom Server lesen ? (j/n) j

CLIENT: Nachricht vom Server : Ihre IP-Adresse lautet '134.108.8.37' Ihre Port- CLIENT:

Anzahl gelesener Zeichen in read = 14000

Hier kann man sehen, dass bei No. 74 der Client die Verbindung halbseits beendet, indem er ein FIN,ACK an den Server schickt. Somit kann der Client nur noch Daten empfangen, also keine mehr senden. Im folgenden schickt der Server an den Client noch Daten und anschließend beendet der Server seinerseits die Verbindung.

No.	Time	Source	Destination	Protocol	Length	Info
6	2.308061	134.108.8.37	134.108.8.36	TCP	74	58366 > 9005 [SYN] Seq=0 win=2872 Len=0 MSS=1436 SACK_PERM=1 Tsva1=11494572 TSecr=0 WS=1
7	2.308116	134.108.8.36	134.108.8.37	TCP	74	9005 > 58366 [SYN, ACK] Seq=0 Ack=1 win=2896 Len=0 MSS=1460 SACK_PERM=1 Tsva1=10822500 TSecr=11494572 WS=1
8	2.308351	134.108.8.37	134.108.8.36	TCP	66	58366 > 9005 [ACK] Seq=1 Ack=1 win=2872 Len=0 Tsva1=11494573 TSecr=10822500
74	5.561933	134.108.8.37	134.108.8.36	TCP	66	58366 > 9005 [FIN, ACK] Seq=1 Ack=1 win=2872 Len=0 Tsva1=11497827 TSecr=10822500
75	5.562036	134.108.8.36	134.108.8.37	TCP	66	9005 > 58366 [ACK] Seq=1 Ack=2 win=2896 Len=0 Tsva1=10825754 TSecr=11497827
80	10.399650	134.108.8.36	134.108.8.37	TCP	1490	9005 > 58366 [ACK] Seq=1 Ack=2 win=2896 Len=1424 Tsva1=10830592 TSecr=11497827
84	10.399666	134.108.8.36	134.108.8.37	TCP	1490	9005 > 58366 [PSH, ACK] Seq=1425 Ack=2 win=2896 Len=1424 Tsva1=10830592 TSecr=11497827
85	10.399929	134.108.8.37	134.108.8.36	TCP	66	58366 > 9005 [ACK] Seq=2 Ack=1425 win=2872 Len=0 Tsva1=11502665 TSecr=10830592
86	10.399957	134.108.8.36	134.108.8.37	TCP	1490	9005 > 58366 [ACK] Seq=2849 Ack=2 win=2896 Len=1424 Tsva1=10830592 TSecr=11502665
87	10.400271	134.108.8.37	134.108.8.36	TCP	66	58366 > 9005 [ACK] Seq=2 Ack=4273 win=2872 Len=0 Tsva1=11502665 TSecr=10830592
88	10.400295	134.108.8.36	134.108.8.37	TCP	1490	9005 > 58366 [PSH, ACK] Seq=4273 Ack=2 win=2896 Len=1424 Tsva1=10830593 TSecr=11502665
89	10.400303	134.108.8.36	134.108.8.37	TCP	1490	9005 > 58366 [ACK] Seq=5697 Ack=2 win=2896 Len=1424 Tsva1=10830593 TSecr=11502665
90	10.400352	134.108.8.37	134.108.8.36	TCP	66	58366 > 9005 [ACK] Seq=1 Ack=7121 win=2872 Len=0 Tsva1=11502665 TSecr=10830593
91	10.400375	134.108.8.36	134.108.8.37	TCP	1490	9005 > 58366 [PSH, ACK] Seq=7121 Ack=2 win=2896 Len=1424 Tsva1=10830593 TSecr=11502665
92	10.400583	134.108.8.36	134.108.8.37	TCP	1490	9005 > 58366 [ACK] Seq=8545 Ack=2 win=2896 Len=1424 Tsva1=10830593 TSecr=11502665
93	10.400839	134.108.8.37	134.108.8.36	TCP	66	58366 > 9005 [ACK] Seq=2 Ack=9969 win=2872 Len=0 Tsva1=11502665 TSecr=10830593
94	10.400863	134.108.8.36	134.108.8.37	TCP	1490	9005 > 58366 [PSH, ACK] Seq=9969 Ack=2 win=2896 Len=1424 Tsva1=10830593 TSecr=11502665
95	10.400870	134.108.8.36	134.108.8.37	TCP	1490	9005 > 58366 [PSH, ACK] Seq=11393 Ack=2 win=2896 Len=1424 Tsva1=10830593 TSecr=11502665
96	10.401130	134.108.8.37	134.108.8.36	TCP	66	58366 > 9005 [ACK] Seq=2 Ack=12817 win=2872 Len=0 Tsva1=11502666 TSecr=10830593
97	10.401154	134.108.8.36	134.108.8.37	TCP	1250	9005 > 58366 [PSH, ACK] Seq=12817 Ack=2 win=2896 Len=1184 Tsva1=10830593 TSecr=11502666
98	10.440886	134.108.8.37	134.108.8.36	TCP	66	58366 > 9005 [ACK] Seq=2 Ack=14001 win=2872 Len=0 Tsva1=11502706 TSecr=10830593
101	11.400130	134.108.8.36	134.108.8.37	TCP	66	9005 > 58366 [FIN, ACK] Seq=14001 Ack=2 win=2896 Len=0 Tsva1=10831592 TSecr=11502706
102	11.400381	134.108.8.37	134.108.8.36	TCP	66	58366 > 9005 [ACK] Seq=2 Ack=14002 win=2872 Len=0 Tsva1=11503665 TSecr=10831592

1.4 Client mit bind

Ohne Fehlerbehandlung

No.	Time	Source	Destination	Protocol	Length	Info
252	111.242455	134.108.8.36	134.108.8.37	TCP	74	9006 > 9006 [SYN] Seq=0 win=2920 Len=0 MSS=1460 SACK_PERM=1 TSval=12359627 TSecr=0 WS=1
253	111.242705	134.108.8.37	134.108.8.36	TCP	74	9006 > 9006 [ACK] Seq=0 Ack=1 win=2896 Len=0 MSS=1460 SACK_PERM=1 TSval=13031700 TSecr=12359627 WS=1
254	111.242741	134.108.8.36	134.108.8.37	TCP	66	dynamid > 9006 [ACK] Seq=1 Ack=1 win=2920 Len=0 TSval=12359627 TSecr=13031700
264	113.474529	134.108.8.36	134.108.8.37	TCP	74	54676 > 9006 [SYN] Seq=0 win=2920 Len=0 MSS=1460 SACK_PERM=1 TSval=12361858 TSecr=0 WS=1
265	113.474789	134.108.8.37	134.108.8.36	TCP	74	9006 > 54676 [SYN, ACK] Seq=0 Ack=1 win=2896 Len=0 MSS=1460 SACK_PERM=1 TSval=13033932 TSecr=12361858 WS=1
266	113.474824	134.108.8.36	134.108.8.37	TCP	66	54676 > 9006 [ACK] Seq=1 Ack=1 win=2920 Len=0 TSval=12361859 TSecr=13033932
279	124.616369	134.108.8.36	134.108.8.37	TCP	69	54676 > 9006 [PSH, ACK] Seq=1 Ack=1 win=2920 Len=3 TSval=12373001 TSecr=13033932
280	124.616396	134.108.8.36	134.108.8.37	TCP	66	54676 > 9006 [FIN, ACK] Seq=4 Ack=1 win=2920 Len=0 TSval=12373001 TSecr=13033932
281	124.616622	134.108.8.37	134.108.8.36	TCP	66	9006 > 54676 [ACK] Seq=1 Ack=4 win=2896 Len=0 TSval=13045074 TSecr=12373001
282	124.656630	134.108.8.37	134.108.8.36	TCP	66	9006 > 54676 [ACK] Seq=1 Ack=5 win=2896 Len=0 TSval=13045114 TSecr=12373001
285	127.392446	134.108.8.36	134.108.8.37	TCP	69	dynamid > 9006 [PSH, ACK] Seq=1 Ack=1 win=2920 Len=3 TSval=12375777 TSecr=13031700
286	127.392470	134.108.8.36	134.108.8.37	TCP	66	dynamid > 9006 [FIN, ACK] Seq=4 Ack=1 win=2920 Len=0 TSval=12375777 TSecr=13031700
287	127.392692	134.108.8.37	134.108.8.36	TCP	66	9006 > dynamid [ACK] Seq=1 Ack=4 win=2896 Len=0 TSval=13047850 TSecr=12375777
288	127.432623	134.108.8.37	134.108.8.36	TCP	66	9006 > dynamid [ACK] Seq=1 Ack=5 win=2896 Len=0 TSval=13047890 TSecr=12375777
303	134.873783	134.108.8.37	134.108.8.36	TCP	66	9006 > dynamid [FIN, ACK] Seq=1 Ack=5 win=2896 Len=0 TSval=13055331 TSecr=12375777
304	134.873809	134.108.8.36	134.108.8.37	TCP	66	dynamid > 9006 [ACK] Seq=5 Ack=2 win=2920 Len=0 TSval=12383258 TSecr=13055331
333	140.905776	134.108.8.37	134.108.8.36	TCP	66	9006 > 54676 [FIN, ACK] Seq=1 Ack=5 win=2896 Len=0 TSval=13061363 TSecr=12373001
334	140.905800	134.108.8.36	134.108.8.37	TCP	66	54676 > 9006 [ACK] Seq=5 Ack=2 win=2920 Len=0 TSval=12389290 TSecr=13061363

Hier wird gezeigt, wie mit bind eine Port-Nummer, über die man senden/empfangen kann, an den Socket gebunden. Das bind liefert einen Rückgabewert bei erfolgreichen binden eine 0, ansonsten einen negativen Wert (-1).

Mit Fehlerbehandlung

No.	Time	Source	Destination	Protocol	Length	Info
8	0.740282	134.108.8.36	134.108.8.37	TCP	74	9005 > 9006 [SYN] Seq=0 win=2920 Len=0 MSS=1460 SACK_PERM=1 TSval=14122773 TSecr=0 WS=1
9	0.740553	134.108.8.37	134.108.8.36	TCP	74	9006 > 9005 [SYN, ACK] Seq=0 Ack=1 win=2896 Len=0 MSS=1460 SACK_PERM=1 TSval=14794847 TSecr=14122773 WS=1
10	0.740583	134.108.8.36	134.108.8.37	TCP	66	9005 > 9006 [ACK] Seq=1 Ack=1 win=2920 Len=0 TSval=14122774 TSecr=14794847

-----Ohne Fehlerbehebung-----

(Port wird beim ersten client erfolgreich gesetzt
und beim zweiten wird ein dynamischer port genommen -> durch bind)

```
[kakait01@itpc3105 tcp_v11]$ ./client_s.out 134.108.8.37 9006
```

CLIENT: Version: 1.2 ; Autor: H.Ws

CLIENT: server_port = 9006

CLIENT: addr = 0.0.0.0 ; Port = 9005

CLIENT: socket = 3 : Window-Size = 4096

CLIENT: Verbindung mit Server 134.108.8.37 auf Port 9006 aufgenommen

CLIENT: socket = 3 ;Nach setsockopt: TTL = 32

CLIENT: 0 Sek.: Vor write(s_buf,60000), vor read!

CLIENT: Jetzt zum Server schreiben? (j/n)

```
[kakait01@itpc3105 tcp_v11]$ ./client_s.out 134.108.8.37 9006
```

CLIENT: Version: 1.2 ; Autor: H.Ws

CLIENT: server_port = 9006

CLIENT: addr = 0.0.0.0 ; Port = 9005

CLIENT: socket = 3 : Window-Size = 4096

CLIENT: Verbindung mit Server 134.108.8.37 auf Port 9006 aufgenommen

CLIENT: socket = 3 ;Nach setsockopt: TTL = 32

CLIENT: 0 Sek.: Vor write(s_buf,60000), vor read!

CLIENT: Jetzt zum Server schreiben? (j/n)

-----Mit Fehlerbehebung-----

(erste client bekommt die port nummer der zweite bekommt

einen negativen return wert und die verbindung

kommt nicht zustande da das programm abbricht)

```
[kakait01@itpc3105 tcp_v11]$ ./client_s.out 134.108.8.37 9006
```

CLIENT: Version: 1.2 ; Autor: H.Ws

CLIENT: server_port = 9006

CLIENT: addr = 0.0.0.0 ; Port = 9005

CLIENT: socket = 3 : Window-Size = 4096

CLIENT: Verbindung mit Server 134.108.8.37 auf Port 9006 aufgenommen

CLIENT: socket = 3 ;Nach setsockopt: TTL = 32

CLIENT: 0 Sek.: Vor write(s_buf,60000), vor read!

CLIENT: Jetzt zum Server schreiben? (j/n)

```
[kakait01@itpc3105 tcp_v11]$ ./client_s.out 134.108.8.37 9006
```

CLIENT: Version: 1.2 ; Autor: H.Ws

CLIENT: server_port = 9006

CLIENT: addr = 0.0.0.0 ; Port = 9005

CLIENT: Fehler bei (bind), Return-Code = -1

CLIENT: Fehler bei bind, fester Port belegt : Address already in use

```
[kakait01@itpc3105 tcp_v11]$
```


1.5 Nebenläufiger Server, zwei Clients

Der Nebenläufiger Server kann mehrerer Clients zugleich bedienen. Dies kann man im Wireshark trace sehen wie Client B und Client A zugleich bedient werden.

```
[kakait01@itpc3106 tcp_v11]$ ./server_n.out 9006
SERVER_N: PID = 8309 : Nebenlaeufiger Server, Version: 1.2 ; Autor: H.Ws
SERVER_N 18:20:08.7 > PID = 8309 : server_port = 9006
SERVER_N 18:20:36.4 > PID = 8309 ; Parent-Socket = 3 : Mit Client 134.108.8.36 auf Port 54695
Verbindung aufgenommen
SERVER_N 18:20:36.4 > PID = 8313 : Local socket in child = 4
SERVER_N 18:20:39.7 > PID = 8309 ; Parent-Socket = 3 : Mit Client 134.108.8.36 auf Port 54696
Verbindung aufgenommen
SERVER_N 18:20:39.7 > PID = 8314 : Local socket in child = 4
SERVER_N 18:20:49.2 > PID = 8314 : clientport 54696 : Nachricht von Client:
AabcbdefghijklmnopqrstuvwxyzBabcbdefghijkl ...
SERVER_N 18:20:49.2 > PID = 8314 : clientport 54696 : Anzahl gelesener Zeichen in read = 3000
SERVER_N 18:20:54.1 > PID = 8314 : clientport 54696 : Anzahl geschriebener Zeichen in write = 2000
SERVER_N 18:20:52.2 > PID = 8313 : clientport 54695 : Nachricht von Client:
AabcbdefghijklmnopqrstuvwxyzBabcbdefghijkl ...
SERVER_N 18:20:52.2 > PID = 8313 : clientport 54695 : Anzahl gelesener Zeichen in read = 3000
SERVER_N 18:20:52.2 > PID = 8313 : clientport 54695 : Anzahl geschriebener Zeichen in write = 2000
SERVER_N 18:20:53.1 > PID = 8313 : clientport 54695 : Nachricht von Client:
AabcbdefghijklmnopqrstuvwxyzBabcbdefghijkl ...
SERVER_N 18:20:53.1 > PID = 8313 : clientport 54695 : Anzahl gelesener Zeichen in read = 3000
SERVER_N 18:20:53.1 > PID = 8313 : clientport 54695 : Anzahl geschriebener Zeichen in write = 2000
SERVER_N 18:20:55.7 > PID = 8314 : clientport 54696 : Nachricht von Client:
AabcbdefghijklmnopqrstuvwxyzBabcbdefghijkl ...
SERVER_N 18:20:55.7 > PID = 8314 : clientport 54696 : Anzahl gelesener Zeichen in read = 3000
SERVER_N 18:20:55.7 > PID = 8314 : clientport 54696 : Anzahl geschriebener Zeichen in write = 2000
SERVER_N 18:20:56.7 > PID = 8314 : Verbindung mit Client 134.108.8.36 auf Port 54696 beendet
```

No.	Time	Source	Destination	Protocol	Length	Info
17	15.412222	134.108.8.36	134.108.8.37	TCP	74	54695 > 9006 [SYN] Seq=0 win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=14920586 TSecr=0 ws=128
18	15.412482	134.108.8.36	134.108.8.36	TCP	74	9006 > 54695 [SYN, ACK] Seq=0 Ack=1 win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=15592659 TSecr=0
19	15.412519	134.108.8.36	134.108.8.37	TCP	66	54695 > 9006 [ACK] Seq=1 Ack=1 win=14720 Len=0 TSval=14920586 TSecr=15592659
23	18.651129	134.108.8.36	134.108.8.37	TCP	74	54696 > 9006 [SYN] Seq=0 win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=14923824 TSecr=0 ws=128
24	18.651385	134.108.8.37	134.108.8.36	TCP	74	9006 > 54696 [SYN, ACK] Seq=0 Ack=1 win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=15595898 TSecr=0
25	18.651421	134.108.8.36	134.108.8.37	TCP	66	54696 > 9006 [ACK] Seq=1 Ack=1 win=14720 Len=0 TSval=14923825 TSecr=15595898
39	28.145103	134.108.8.36	134.108.8.37	TCP	2962	54696 > 9006 [ACK] Seq=1 Ack=1 win=14720 Len=2896 TSval=14933319 TSecr=15595898
40	28.145120	134.108.8.36	134.108.8.37	TCP	170	54696 > 9006 [PSH, ACK] Seq=2897 Ack=1 win=14720 Len=104 TSval=14933319 TSecr=15595898
41	28.145472	134.108.8.37	134.108.8.36	TCP	66	9006 > 54696 [ACK] Seq=1 Ack=1449 win=17408 Len=0 TSval=15605392 TSecr=14933319
42	28.145492	134.108.8.37	134.108.8.36	TCP	66	9006 > 54696 [ACK] Seq=1 Ack=2897 win=20352 Len=0 TSval=15605392 TSecr=14933319
43	28.145496	134.108.8.37	134.108.8.36	TCP	66	9006 > 54696 [ACK] Seq=1 Ack=3001 win=20352 Len=0 TSval=15605392 TSecr=14933319
44	28.145594	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54696 [ACK] Seq=1 Ack=3001 win=20352 Len=1448 TSval=15605392 TSecr=14933319
45	28.145611	134.108.8.37	134.108.8.36	TCP	618	9006 > 54696 [PSH, ACK] Seq=1449 Ack=3001 win=20352 Len=552 TSval=15608400 TSecr=14933319
46	28.145650	134.108.8.36	134.108.8.37	TCP	66	54696 > 9006 [ACK] Seq=3001 Ack=1449 win=17536 Len=0 TSval=14933319 TSecr=15605392
47	28.145661	134.108.8.36	134.108.8.37	TCP	66	54696 > 9006 [ACK] Seq=3001 Ack=2001 win=20480 Len=0 TSval=14933319 TSecr=15605392
50	31.153107	134.108.8.36	134.108.8.37	TCP	2962	54695 > 9006 [ACK] Seq=1 Ack=1 win=14720 Len=2896 TSval=14936327 TSecr=15592659
51	31.153124	134.108.8.36	134.108.8.37	TCP	170	54695 > 9006 [PSH, ACK] Seq=2897 Ack=1 win=14720 Len=104 TSval=14936327 TSecr=15592659
52	31.153454	134.108.8.37	134.108.8.36	TCP	66	9006 > 54695 [ACK] Seq=1 Ack=1449 win=17408 Len=0 TSval=15608400 TSecr=14936327
53	31.153478	134.108.8.37	134.108.8.36	TCP	66	9006 > 54695 [ACK] Seq=1 Ack=2897 win=20352 Len=0 TSval=15608400 TSecr=14936327
54	31.153482	134.108.8.37	134.108.8.36	TCP	66	9006 > 54695 [ACK] Seq=1 Ack=3001 win=20352 Len=0 TSval=15608400 TSecr=14936327
55	31.153627	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54695 [ACK] Seq=1 Ack=3001 win=20352 Len=1448 TSval=15608400 TSecr=14936327
56	31.153645	134.108.8.37	134.108.8.36	TCP	618	9006 > 54695 [PSH, ACK] Seq=1449 Ack=3001 win=20352 Len=552 TSval=15608400 TSecr=14936327
57	31.153684	134.108.8.36	134.108.8.37	TCP	66	54695 > 9006 [ACK] Seq=3001 Ack=1449 win=17536 Len=0 TSval=14936327 TSecr=15608400
58	31.153695	134.108.8.36	134.108.8.37	TCP	66	54695 > 9006 [ACK] Seq=3001 Ack=2001 win=20480 Len=0 TSval=14936327 TSecr=15608400
59	32.065080	134.108.8.36	134.108.8.37	TCP	2962	54695 > 9006 [ACK] Seq=3001 Ack=2001 win=20480 Len=2896 TSval=14937239 TSecr=15608400
60	32.065101	134.108.8.36	134.108.8.37	TCP	170	54695 > 9006 [PSH, ACK] Seq=5897 Ack=2001 win=20480 Len=104 TSval=14937239 TSecr=15608400
61	32.065445	134.108.8.37	134.108.8.36	TCP	66	9006 > 54695 [ACK] Seq=2001 Ack=5897 win=26112 Len=0 TSval=15609312 TSecr=14937239
62	32.065578	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54695 [ACK] Seq=2001 Ack=6001 win=26112 Len=1448 TSval=15609312 TSecr=14937239
63	32.065595	134.108.8.37	134.108.8.36	TCP	618	9006 > 54695 [PSH, ACK] Seq=3449 Ack=6001 win=26112 Len=552 TSval=15609312 TSecr=14937239
64	32.065634	134.108.8.36	134.108.8.37	TCP	66	54695 > 9006 [ACK] Seq=6001 Ack=3449 win=23296 Len=0 TSval=14937239 TSecr=15609312
65	32.065650	134.108.8.36	134.108.8.37	TCP	66	54695 > 9006 [ACK] Seq=6001 Ack=4001 win=26240 Len=0 TSval=14937239 TSecr=15609312
66	32.065678	134.108.8.36	134.108.8.37	TCP	69	54695 > 9006 [PSH, ACK] Seq=6001 Ack=4001 win=26240 Len=3 TSval=14937239 TSecr=15609312
67	32.065694	134.108.8.36	134.108.8.37	TCP	66	54695 > 9006 [FIN, ACK] Seq=6004 Ack=4001 win=26240 Len=0 TSval=14937239 TSecr=15609312
69	32.105102	134.108.8.37	134.108.8.36	TCP	66	9006 > 54695 [ACK] Seq=4001 Ack=6005 win=26112 Len=0 TSval=15609352 TSecr=14937239
70	33.066030	134.108.8.37	134.108.8.36	TCP	66	9006 > 54695 [FIN, ACK] Seq=4001 Ack=6005 win=26112 Len=0 TSval=15610312 TSecr=14937239
71	33.066056	134.108.8.36	134.108.8.37	TCP	66	54695 > 9006 [ACK] Seq=6005 Ack=4002 win=26240 Len=0 TSval=14938240 TSecr=15610312
73	34.666075	134.108.8.36	134.108.8.37	TCP	2962	54696 > 9006 [ACK] Seq=3001 Ack=2001 win=20480 Len=2896 TSval=14939840 TSecr=15605392
74	34.666095	134.108.8.36	134.108.8.37	TCP	170	54696 > 9006 [PSH, ACK] Seq=5897 Ack=2001 win=20480 Len=104 TSval=14939840 TSecr=15605392
75	34.666387	134.108.8.37	134.108.8.36	TCP	66	9006 > 54696 [ACK] Seq=2001 Ack=5897 win=26112 Len=0 TSval=15611913 TSecr=14939840
76	34.666532	134.108.8.37	134.108.8.36	TCP	1514	9006 > 54696 [ACK] Seq=2001 Ack=6001 win=26112 Len=1448 TSval=15611913 TSecr=14939840
77	34.666549	134.108.8.37	134.108.8.36	TCP	618	9006 > 54696 [PSH, ACK] Seq=3449 Ack=6001 win=26112 Len=552 TSval=15611913 TSecr=14939840
78	34.666591	134.108.8.36	134.108.8.37	TCP	66	54696 > 9006 [ACK] Seq=6001 Ack=3449 win=23296 Len=0 TSval=14939840 TSecr=15611913
79	34.666602	134.108.8.36	134.108.8.37	TCP	66	54696 > 9006 [ACK] Seq=6001 Ack=4001 win=26240 Len=0 TSval=14939840 TSecr=15611913
80	34.666631	134.108.8.36	134.108.8.37	TCP	69	54696 > 9006 [PSH, ACK] Seq=6001 Ack=4001 win=26240 Len=3 TSval=14939840 TSecr=15611913
81	34.666651	134.108.8.36	134.108.8.37	TCP	66	54696 > 9006 [FIN, ACK] Seq=6004 Ack=4001 win=26240 Len=0 TSval=14939840 TSecr=15611913
82	34.706091	134.108.8.37	134.108.8.36	TCP	66	9006 > 54696 [ACK] Seq=4001 Ack=6005 win=26112 Len=0 TSval=15611953 TSecr=14939840
84	35.667015	134.108.8.37	134.108.8.36	TCP	66	9006 > 54696 [FIN, ACK] Seq=4001 Ack=6005 win=26112 Len=0 TSval=15612913 TSecr=14939840
85	35.667043	134.108.8.36	134.108.8.37	TCP	66	54696 > 9006 [ACK] Seq=6005 Ack=4002 win=26240 Len=0 TSval=14940841 TSecr=15612913

1.6 UDP-Sockets

1.6.1 Requester und Responder im gleichem Sub

Erklären Sie den Ablauf bei UDP:

Bei UDP müssen die Ports mitgesendet werden, da UDP ein verbindungsloses Protokoll ist (kein SYN,ACK/FIN,ACK) wie bei TCP.

Was ist anders zu TCP?

Bei UDP wird eine Checksummenprüfung gemacht, ob das Paket beim Empfänger angekommen ist, wird nicht überprüft. Im folgenden sieht man den Datenaustausch über UDP, wobei im ersten Paket die Portnummern übertragen werden und anschließend die Daten.

No.	Time	Source	Destination	Protocol	Length	Info
412	217.943374	134.108.8.37	134.108.8.36	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=16b4) [Reassembled in #414]
413	217.943386	134.108.8.37	134.108.8.36	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=16b4) [Reassembled in #414]
414	217.943388	134.108.8.37	134.108.8.36	UDP	82	Source port: 9006 Destination port: 9005
415	217.943407	134.108.8.37	134.108.8.36	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=16b5) [Reassembled in #417]
416	217.943410	134.108.8.37	134.108.8.36	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=16b5) [Reassembled in #417]
417	217.943412	134.108.8.37	134.108.8.36	UDP	82	Source port: 9006 Destination port: 9005
423	226.131220	134.108.8.36	134.108.8.37	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=6c0d) [Reassembled in #425]
424	226.131233	134.108.8.36	134.108.8.37	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=6c0d) [Reassembled in #425]
425	226.131237	134.108.8.36	134.108.8.37	UDP	82	Source port: 9005 Destination port: 9006
431	231.727309	134.108.8.37	134.108.8.36	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=16b6) [Reassembled in #433]
432	231.727317	134.108.8.37	134.108.8.36	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=16b6) [Reassembled in #433]
433	231.727319	134.108.8.37	134.108.8.36	UDP	82	Source port: 9006 Destination port: 9005
434	231.727344	134.108.8.37	134.108.8.36	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=16b7) [Reassembled in #436]
435	231.727348	134.108.8.37	134.108.8.36	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=16b7) [Reassembled in #436]
436	231.727361	134.108.8.37	134.108.8.36	UDP	82	Source port: 9006 Destination port: 9005
466	238.387147	134.108.8.36	134.108.8.37	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=6c0e) [Reassembled in #468]
467	238.387160	134.108.8.36	134.108.8.37	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=6c0e) [Reassembled in #468]
468	238.387163	134.108.8.36	134.108.8.37	UDP	82	Source port: 9005 Destination port: 9006

1.6.2 Requester und Responder in unterschiedlichen Sub mit einem Router dazwischen

Hier ist das gleiche zu beobachten. Als erstes werden die Portnummern übertragen und anschließend die Daten in diesem Fall fragmentiert.

No.	Time	Source	Destination	Protocol	Length	Info
252	131.474084	134.108.8.37	134.108.190.10	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=0527) [Reassembled in #254]
253	131.474095	134.108.8.37	134.108.190.10	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=0527) [Reassembled in #254]
254	131.474096	134.108.8.37	134.108.190.10	UDP	82	Source port: 9006 Destination port: 9010
255	131.474116	134.108.8.37	134.108.190.10	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=0528) [Reassembled in #257]
256	131.474118	134.108.8.37	134.108.190.10	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=0528) [Reassembled in #257]
257	131.474120	134.108.8.37	134.108.190.10	UDP	82	Source port: 9006 Destination port: 9010
265	137.439183	134.108.190.10	134.108.8.37	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=7b74) [Reassembled in #267]
266	137.439328	134.108.190.10	134.108.8.37	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=7b74) [Reassembled in #267]
267	137.439337	134.108.190.10	134.108.8.37	UDP	82	Source port: 9010 Destination port: 9006

Time to live = 1

Wenn TTL auf 1 gesetzt wird, so werden die Daten beim Router verworfen und der Router sendet ein **Time to live exceeded** zurück.

No.	Time	Source	Destination	Protocol	Length	Info
72	35.899398	134.108.8.37	134.108.190.10	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=0529) [Reassembled in #74]
73	35.899409	134.108.8.37	134.108.190.10	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=0529) [Reassembled in #74]
74	35.899411	134.108.8.37	134.108.190.10	UDP	82	Source port: 9006 Destination port: 9010
75	35.899431	134.108.8.37	134.108.190.10	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=052a) [Reassembled in #77]
76	35.899433	134.108.8.37	134.108.190.10	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=052a) [Reassembled in #77]
77	35.899435	134.108.8.37	134.108.190.10	UDP	82	Source port: 9006 Destination port: 9010
78	35.900569	134.108.11.254	134.108.8.37	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
79	35.900655	134.108.11.254	134.108.8.37	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)