Technische Universität München
Informatik VIII
Netzarchitekturen und Netzdienste
Prof. Dr.-Ing. Georg Carle

*Marc-Oliver Pahl, Gerhard Münz*

# Übungen zur Vorlesung Rechnernetze und Verteilte Systeme

## Übungsblatt 9, SS 2009

Abgabe: 24. Juni 2009 (in der Vorlesung)

### Aufgabe 20 - Programmieraufgabe: TCP-Kommunikation (12 Punkte)

In dieser Aufgabe sollen Sie einen TCP-Client programmieren. Dazu steht Ihnen bereits ein Grundgerüst in Java zur Verfügung. Sie finden es auf der Übungswebsite.

Als Gegenstelle Ihres Programms haben wir einen TCP-Server aufgesetzt. Den Sourcecode des Servers finden Sie ebenfalls auf der Website.

Der Server ist erreichbar unter der Adresse ilab.net.in.tum.de:2342.

Sie können sich per „telnet ilab.net.in.tum.de 2342“ mit dem Rechner verbinden und das Protokoll ausprobieren. Ein Protokollbeispielablauf ist nachfolgend abgedruckt:

```
GrnvsTcpServer: Verbindung 9 von IP /131.159.14.62:56745
--> HELLO
Welcome!
Please answer the following challenge by summing up the numbers:
5428
1145
2363
--> 8936
Please send your Teamletter...
--> B
Please send your Name formatted as [Surname] [Prename]...
--> Pahl Marc-Oliver
Submitted data:
B,Pahl Marc-Oliver,/131.159.14.62:56745,Fri Jun 20 00:19:17 GMT+01:00 2008
Your data was saved.
Thank you!
Bye...
```

Die Eingaben des Client sind jeweils durch einen Pfeil gekennzeichnet.

Ziel der Aufgabe ist es, dass Ihr Client Ihre Gruppe und Ihren Namen an unseren Server überträgt. Da dies prinzipiell auch per Telnet möglich ist, haben wir eine kleine Challenge eingebaut, die darin besteht, die drei zufällig vom Server gewählten Zahlen zu addieren und das Ergebnis innerhalb von maximal 5 Sekunden zurückzusenden. Ihr Programm sollte dies in weniger als einer Sekunde durchführen können. Als menschliche Gegenstelle werden Sie es allerdings nicht schaffen, die Antwort in weniger als 5 Sekunden zur Verfügung zu stellen.

War Ihre Eingabe zu langsam, so weist Sie der Server darauf hin:

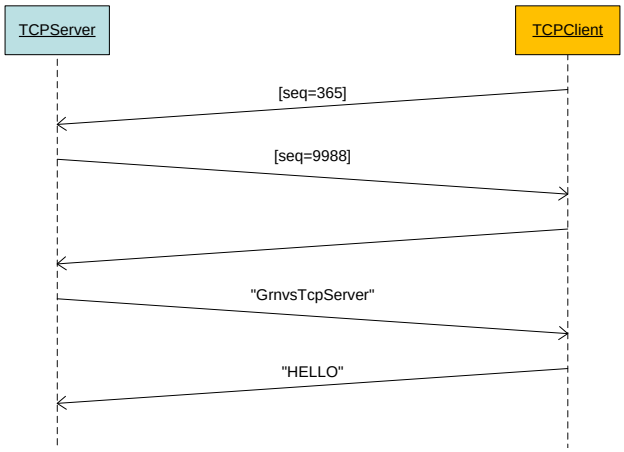
```
Your data was *NOT SAVED* since you answered too slowly...
(You took 38 seconds, maximum allowed time is 5 seconds.)
Pease try again!
```

Der Server ist so programmiert, dass er bei falschen Eingaben die Verbindung beendet. Sie können dieses Verhalten vorab in einer Telnet-Sitzung ausprobieren.

Die Liste der bisher erfolgreichen Übermittlungen finden Sie auf der passwortgeschützten Website „https://ilab.net.in.tum.de/extern/grnvs“. Sie können sich dort mit folgenden Daten einloggen:

```
username: grnvs
passwort: ss09
```

In folgendem Sequenzdiagramm sehen Sie beispielhaft den Beginn einer TCP-Sitzung zwischen Ihrem Client und dem Server:




a) Vervollständigen Sie im Sequenzdiagramm für alle angegebenen TCP-Pakete die Flags, Sequenznummern (seq) sowie die bestätigten Sequenznummern (ACK).

b) Programmieren Sie basierend auf dem Grundgerüst einen Client in Java, der es Ihnen ermöglicht, die gewünschten Daten innerhalb der 5 Sekunden an unseren Server zu übertragen.

c) Übermitteln Sie Ihre Daten (Gruppennummer und Namen) in dem vom Server gewünschten Format (siehe Servertexte in obigem Kommunikationsprotokoll). Bitte übermitteln Sie für jeden Teamteilnehmer einzeln die Daten.
Auf der oben angegebenen Website können Sie überprüfen, ob Ihre Abgabe erfolgreich war.

d) Drucken Sie Ihren Client aus und geben Sie ihn mit Ihren Lösungen ab.

## Aufgabe 21 - Paketanalyse mit TCPdump (12 Punkte)

TCPdump ist ein Linuxprogramm zum Mitschneiden von Netzwerkverkehr[1].

Nachfolgend sehen Sie eine Ausgabe von TCPdump (Parameter „-e“):

```
14:13:52.912726 00:16:6f:81:65:ab > 00:0e:0c:80:61:4d, ethertype IPv4 (0x0800), length 74:
                131.159.14.176.49374 > 209.85.135.147.80: S 2072795046:2072795046(0) win 5840
                <mss 1460,sackOK,timestamp 5102381 0,nop,wscale 6>

14:13:52.929226 00:0e:0c:80:61:4d > 00:16:6f:81:65:ab, ethertype IPv4 (0x0800), length 74:
                209.85.135.147.80 > 131.159.14.176.49374: S 4069019396:4069019396(0) ack 2072795047 win 5672
                <mss 1430,sackOK,timestamp 1849744697 0,nop,wscale 6>

14:13:52.929274 00:16:6f:81:65:ab > 00:0e:0c:80:61:4d, ethertype IPv4 (0x0800), length 66:
                131.159.14.176.49374 > 209.85.135.147.80: . ack 1 win 92
                <nop,nop,timestamp 5102385 1849744697>

14:13:52.929475 00:16:6f:81:65:ab > 00:0e:0c:80:61:4d, ethertype IPv4 (0x0800), length 709:
                131.159.14.176.49374 > 209.85.135.147.80: P 1:644(643) ack 1 win 92
                <nop,nop,timestamp 5102385 1849744697>
```

Der Aufbau einer Zeile ist:

```
19:27:01.454488 00:00:0c:04:b2:33 > 00:03:e3:d9:26:c0, ethertype IPv4 (0x0800), length 1687:
[1]             [2]                 [3]                          [4]            [5]
                138.97.18.88.63259 > 64.154.80.51.80: P    0:   1633(1633) ack  1634 win 33580
                [6]          [7]     [8]          [9] [10] [11] [12] [13]  [14]

[1] TimeStamp           [8]  Destination IP
[2] SourceMac           [9]  Destination Port
[3] DestinationMac      [10] TCP Flags
[4] Network Protocol    [11] TCP Sequence Number
[5] IP Packet Length    [12] TCP Last Sequence Number
[6] Source IP           [13] TCP Length
[7] Source Port         [14] ACK flag
```

Hinweis: Wie Sie an den Sequenznummern sehen können, gibt TCPdump nicht die absoluten sondern die relativen Sequenznummern nach dem SYN-Paket aus. In Zeile 3 wird also die absolute Sequenznummer ACK 4069019397 versendet.

a) Welche Rechner kommunizieren miteinander auf welchen Ports? Wie sind die DNS-Namen der Rechner?

b) Welchen TCP-Mechanismus zeigt der Mitschnitt? Um welche Verbindungsphase handelt es sich dabei?

c) Welcher Bestätigungsmodus kommt bei der Kommunikation zum Einsatz? Welche Vorteile bietet dies?

d) Ordnen Sie die in der TCPdump-Ausgabe angezeigten Adressen einer geeigneten Schicht im OSI-Modell zu.

In der Vorlesung haben Sie so genannte „well-known“ Ports kennen gelernt.

e) Um welchen Service beim Zielrechner handelt es sich vermutlich? Welchen Dateninhalt wird daher das vierte Paket transportieren?

f) Was bewirkt das gesetzte Flag? Wieso ist es zweckmäßig, es in diesem Zusammenhang zu setzen?

[1] http://www.tcpdump.org; mit Wireshark existiert eine grafische Benutzeroberfläche. Falls Sie im nächsten Semester an unserem Praktikum teilnehmen, lernen Sie derartige Tools kennen.

Angenommen, der Mitschnitt wurde im lokalen Netz des Rechners 131.159.14.176 angefertigt und der Rechner 209.85.135.147 ist nicht direkt erreichbar.

g) Zu welchen an der Kommunikation beteiligten Knoten gehören die beiden angegebenen MAC-Adressen? Wieso stellt dies kein Problem dar?

h) Welches Schicht-2-Protokoll kommt im mitgeschnittenen Verbindungsabschnitt auf dem Medium zum Einsatz? Begründen Sie Ihre Vermutung!

i) Wer sind die Hersteller der Netzwerkgeräte?