

Rechnernetze: Übungen zur Transportschicht

Inhalt

5.1	Übungsaufgabe: TCP- und UDP-Ports in Wireshark.....	2
5.2	Übungsaufgabe: Länge von TCP- und UDP-Segmenten.....	2
5.3	Übungsaufgabe: netstat.....	2
5.4	Übungsaufgabe: tcpdump.....	2
5.5	Übungsaufgabe: Schiebefenster.....	3
5.6	Übungsaufgabe: TCP Flusskontrolle in Wireshark	3
5.7	Übungsaufgabe: TCP-Flags und –Sequenznummern.....	4
5.8	Übungsaufgabe: TCP Window Size und Größe der Sequenznummern	4
5.9	Übungsaufgabe: TCP-Flusskontrolle	5
5.10	Übungsaufgabe: TCP-Flusskontrolle 2	5
5.11	Übungsaufgabe: TCP-Zustandsdiagramm.....	6
5.12	Übungsaufgabe: TCP-Retransmission-Timer	7
5.13	Übungsaufgabe: TCP-Überlastungsüberwachung in Wireshark.....	8
5.14	Übungsaufgabe: TCP Slow Start.....	8
5.15	Übungsaufgabe: NAT.....	8

5.1 Übungsaufgabe: TCP- und UDP-Ports in Wireshark

Erzeugen Sie TCP- und UDP-Traffic mit möglichst vielen unterschiedlichen Anwendungsprotokollen und zeichnen Sie den Traffic mit Wireshark auf.

Mindestens enthalten sollten sein TCP Ports 21, 22, 23, 80, 443 und UDP Port 53.

- Finden Sie den Destination-Port der Segmente. Welche Protokolle der Anwendungsschicht verbergen sich dahinter?
- Wie lang sind die kürzesten bzw. längsten Segmente?
- Erstellen Sie eine Statistik aller verwendeten Anwendungsprotokolle und der damit ausgetauschten Datenmengen.
- Sowohl UDP als auch TCP verwenden Port-Nummern, um das Ziel bei der Zustellung einer Nachricht anzugeben. Geben Sie Gründe an, warum die beiden Protokolle Port-Nummer anstelle der Prozesskennung der Anwendungsschicht verwenden.

5.2 Übungsaufgabe: Länge von TCP- und UDP-Segmenten

- Die maximale Länge der Nutzdaten eines TCP-Segments, das über IPv4 versendet wird, ist 65.495 Byte. Warum?
- Was ist die maximale Länge der Nutzerdaten eines UDP-Segments, das über IPv4 versendet wird.

Hinweis: Gehen Sie von der klassischen Version von TCP und UDP ohne optionale Erweiterungen aus.

5.3 Übungsaufgabe: netstat

Stellen Sie geeignete TCP-Verbindungen her, führen Sie dann das Kommando `netstat` aus und interpretieren Sie den Output.

- Erklären Sie die Ausgabe.
- Was bewirken die Optionen `-a`, `-e`, `-n`, `-s` und `-o`?

Hinweis: Die Optionen beziehen sich auf Windows-Systeme.

5.4 Übungsaufgabe: tcpdump

Tcpdump ist wie Wireshark in der Lage, den Netzwerkverkehr zu belauschen, zu speichern und zu analysieren.

- Installieren Sie `tcpdump` und zeichnen Sie eine vollständige TCP-Verbindung auf.
- In welchem Datei-Format ist die Speicherung möglich?
- Wie groß ist die resultierende Datei?

5.5 Übungsaufgabe: Schiebefenster

In einem speziellen Schiebefenster-Protokoll (kein TCP) gelten folgende Festlegungen:

- Der Sender sendet 1 Rahmen/Sekunde aus, wenn dies durch das Sendefenster möglich ist.
 - Die Übertragungszeit für Rahmen und ACKs beträgt jeweils 2 Sekunden.
 - Die Verarbeitungszeit eines Rahmens beim Empfänger und eines ACKs beim Sender beträgt eine Sekunde.
 - Es werden kumulative ACKs mit der empfangenen Rahmennummer versendet.
 - Der Timeout für den Retransmission-Timer sei 7 Sekunden.
 - Die Fenstergrößen von Sender und Empfänger sind 4.
- a) Geben Sie ein Diagramm mit Zeitstrahl für die Übertragung der Rahmen 1, 2, ..., 8 und der zugehörigen ACKs zwischen Sender und Empfänger an unter der Voraussetzung, dass jede Übertragung erfolgreich war.
- b) Geben Sie ein Diagramm mit Zeitstrahl für die Übertragung der Rahmen 1, 2, ..., 8 und der zugehörigen ACKs an, unter der Voraussetzung, dass jede Übertragung außer der ersten von Rahmen 2 erfolgreich war.

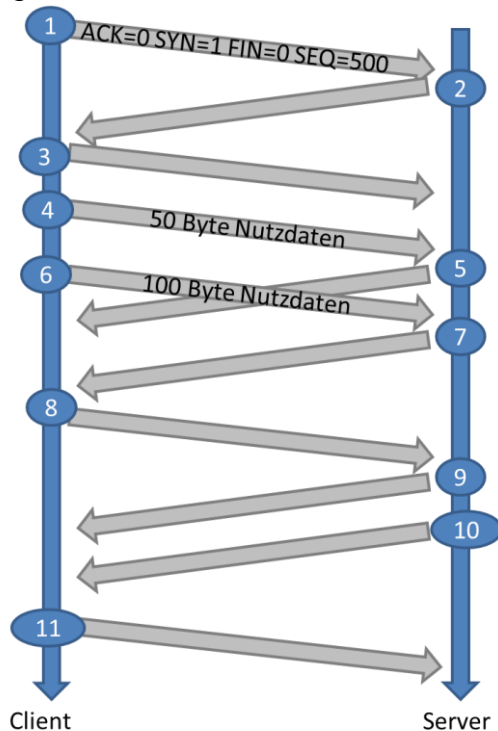
5.6 Übungsaufgabe: TCP Flusskontrolle in Wireshark

Erzeugen Sie TCP-Traffic und schneiden Sie diesen mittels Wireshark mit.

- a) Zeigen Sie die TCP-Segmente, die für den Verbindungsaufbau zuständig sind. Welche Flags sind im TCP-Header jeweils gesetzt?
- b) Verfolgen Sie die Verbindung weiter und beobachten Sie die Entwicklung der Sequenznummern.
- c) Zeigen Sie die TCP-Segmente, die für den Verbindungsabbau zuständig sind. Welche Flags sind im TCP-Header jeweils gesetzt?
- d) Wie groß ist die verwendete Fenstergröße der Segmente?
- e) Wo finden Sie Informationen zur Maximum Segment Size und zum Window Scale Factor?

5.7 Übungsaufgabe: TCP-Flags und –Sequenznummern

Die Abbildung zeigt die ausgetauschten Segmente einer TCP-Verbindung. Ergänzen Sie in der Tabelle die fehlenden Angaben. Es gehen keine Bytes verloren.



Segment	ACK	SYN	FIN	Länge Nutzdaten	SEQ-Nummer	ACK-Nummer
1	0	1	0	0	500	
2				0	1000	
3				0		
4	1			50		
5	1			0		
6	1			100		
7	1			0		
8	0	0	1	0		
9				0		
10	0	0	1	0		
11				0		

5.8 Übungsaufgabe: TCP Window Size und Größe der Sequenznummern

- Nach wie vielen Sekunden läuft bei einer 100 Mbit/s bzw. 1 Gbit/s-Verbindung die TCP-Sequenznummer über? Vergleichen Sie diese Zeit mit der „Maximum Segment Lifetime“ aus RFC 793 von TCP. Was bedeutet das für TCP schlimmstenfalls? Welche Lösung gibt es für dieses Problem?
- Angenommen ein 1, 10, bzw. 100 Mbit/s Übertragungskanal wird vom Sender bei einer Verzögerung von 100ms stets gefüllt gehalten.
 - Was ist die maximale in der Übertragung befindliche Datenmenge (= Verzögerungs-Bandbreite-Produkt)?
 - Wie hängt das mit der Window Size bei TCP zusammen?
 - Welche Lösung gibt es für das resultierende Problem?

5.9 Übungsaufgabe: TCP-Flusskontrolle

Es gelte $\text{MaxSendBuffer} = 1000$, $\text{MaxRcvBuffer} = 200$. Vervollständigen Sie die folgende Tabelle.

Hinweise: Der Sendepuffer sei ständig durch die sendende Anwendung gefüllt. Es gehen keine Pakete verloren, und es findet keine Router-Überlastung statt. Es wird ausschließlich Flusskontrolle und keine Überlastungsüberwachung durchgeführt. Im Falle von $\text{AdWin}=0$ kann der Sender Probe-Segmente verwenden.

	Sender				Empfänger			
	Last Byte ACKed	EffWin	First Byte Sent	Last Byte Sent	Last Byte Read	Last Byte Rcvd	Next Byte Expected (=ACK)	AdWin
1			1	50	0	50	51	150
2	50	150	51		10		201	
3					20		211	
4					30	220	216	
5					40		226	
6					50		241	
7					50		251	
8					50		251	
9					60		252	
10					70		261	

Quelle: Roth

5.10 Übungsaufgabe: TCP-Flusskontrolle 2

Nehmen Sie an, alle Bytes bis zur Sequenznummer 2000 einschließlich seien quittiert und es seien Bytes bis zur Sequenznummer 2400 einschließlich bereits gesendet worden. Ferner sei es dem Sender möglich, weitere 600 Bytes zu senden. Wir haben damit folgende Intervalle vorliegen:

- Intervall der gesendeten, aber noch nicht quittierten Bytes: [2001, 2400]
- Intervall der Bytes, die gesendet werden können: [2401, 3000]

Nehmen Sie an, es treffen für die betrachtete Verbindung folgende TCP-Segmente ein:

- TCP-Segment mit ACK-Nr. 2100 und Fenstergröße 901
- TCP-Segment mit ACK-Nr. 2201 und Fenstergröße 800
- TCP-Segment mit ACK-Nr. 2201 und Fenstergröße 980
- TCP-Segment mit ACK-Nr. 2401 und Fenstergröße 1000

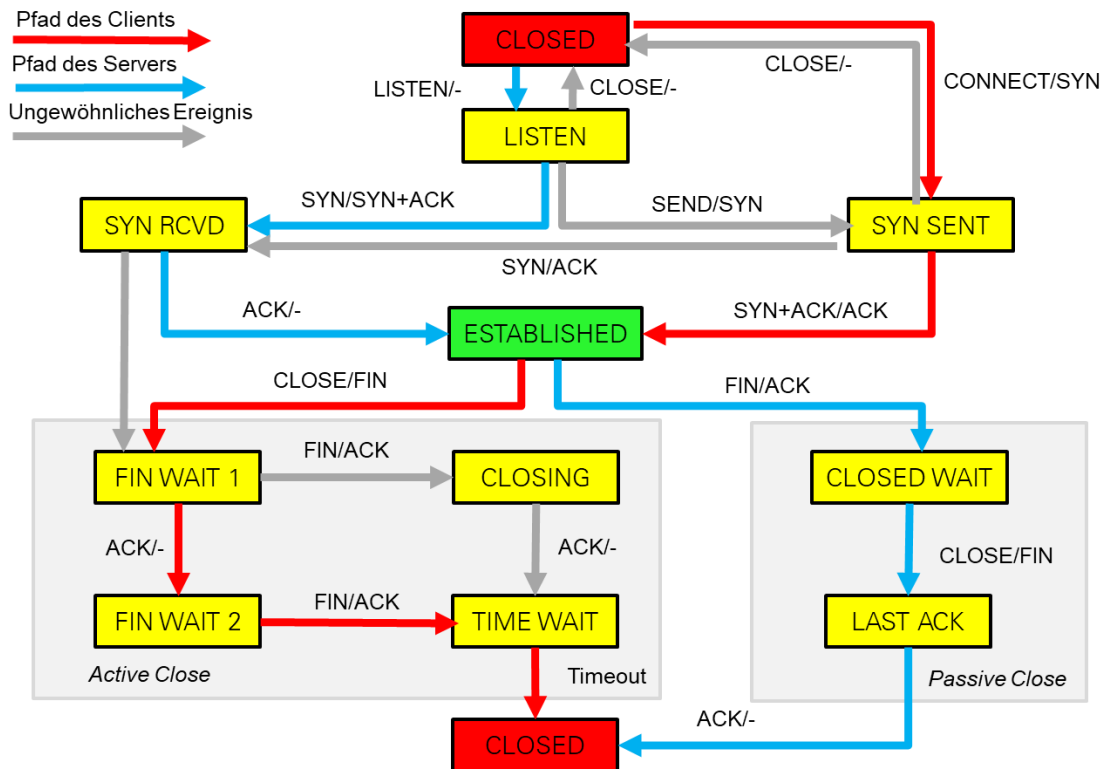
Geben Sie an, wie sich die beiden oben angegebenen Intervalle nach jedem Ereignis verändern.

5.11 Übungsaufgabe: TCP-Zustandsdiagramm

Gegeben sei das TCP-Zustandsdiagramm.

- Wie kommt der Client in den Zustand SYN RCVD bzw. SYN EMPFANGEN?
- Unter welchen Umständen kommt es zu einem Durchlaufen der Zustände ESTABLISHED, FIN WAIT 1, CLOSING und TIME WAIT?

Geben Sie jeweils Zeitachsen inklusive der Zustände für die beiden Kommunikationspartner und die Ereignisse an, die zu den Zustandsübergängen führen.



5.12 Übungsaufgabe: TCP-Retransmission-Timer

Gegeben sei die zeitliche Abfolge von gemessenen Round-Trip-Zeiten „SampleRTT“ in der folgenden Tabelle.

- a) Berechnen Sie die jeweiligen Timeouts nach der im Originalalgorithmus (RfC 793) mit $\alpha = 0.75$.

$$\text{EstimatedRTT} = \alpha * \text{EstimatedRTT} + (1-\alpha) * \text{SampleRTT}$$

$$\text{TimeOut} = 2 * \text{EstimatedRTT}$$

- b) Berechnen Sie die jeweiligen Timeouts nach der Formel von Jacobsen mit $\alpha = 0.75$, $\mu = 1$ und $\phi = 4$.

$$\text{EstimatedRTT} = \alpha * \text{EstimatedRTT} + (1-\alpha) * \text{SampleRTT}$$

$$\text{Abweichung} = \alpha * \text{Abweichung} + (1-\alpha) * |\text{SampleRTT} - \text{EstimatedRTT}|$$

$$\text{TimeOut} = \mu * \text{EstimatedRTT} + \phi * \text{Abweichung}$$

- c) Stellen Sie die Werte SampleRTT, EstimatedRTT und die beiden berechneten Timeouts graphisch dar und interpretieren Sie die Kurvenverläufe. Setzen Sie die Zeit in die X-Achse und die anderen Werte auf die Y-Achse.

Zeit	SampleRTT	EstimatedRTT	Timeout1 (Original)	Abweichung	Timeout2 (Jacobsen)
		200	400	10	240
1	200				
2	190				
3	180				
4	210				
5	200				
6	190				
7	210				
8	190				
9	210				
10	100				
11	90				
12	80				
13	90				
14	110				
15	100				
16	100				
17	90				
18	110				
19	100				
20	90				

Quelle: Roth

5.13 Übungsaufgabe: TCP-Überlastungsüberwachung in Wireshark

Generieren Sie TCP-Traffic in Wireshark zum Beispiel durch Download einer großen Datei. Alternativ analysieren Sie den zur Verfügung gestellten Mitschnitt. Bearbeiten Sie dann die folgenden Punkte:

- a) Zeigen Sie Segmente mit der SACK-Option.
- b) Zeigen Sie Duplicate ACKs.
- c) Zeigen Sie Segmente, die das ECE oder CWR-Flag nutzen. Für was werden diese Flags benötigt?
- d) Erstellen Sie mittels Wireshark den „Round-Trip Time Graph“ und interpretieren Sie dessen Verlauf.

5.14 Übungsaufgabe: TCP Slow Start

Analysieren Sie den zur Verfügung gestellte Wireshark Mitschnitt bzgl. des TCP Slow Starts. Hinweis: Verwenden Sie dazu den Time-Sequence Graph.

5.15 Übungsaufgabe: NAT

Ein Unternehmen verwendet intern das private IP-Netz 10.0.0.0/8. Ein NAT-Gateway erlaubt den internen Clients den Zugriff auf externe Netze und verwendet dazu die externen IP-Adressen 1.2.3.4 und 1.2.3.5. Zudem gibt es im internen Netz einen Web-Server mit der IP-Adresse 10.0.0.1, der von extern unter der Adresse 1.2.3.6 erreichbar ist. Im externen Netzwerk gibt es einen DNS-Server mit der IP-Adresse 1.2.3.7 und einen Client mit der IP-Adresse 1.2.3.8.

- a) Skizzieren Sie das Netzwerk-Szenario.
- b) Wie viele interne Clients können in diesem Szenario maximal gleichzeitig im Internet surfen?
- c) Geben Sie an, welche Einträge das NAT-Gateway verwalten muss, wenn
 - der interne Client den externen DNS-Server aufruft.
 - der externe Client den internen Web-Server aufruft.

Hinweise:

- Machen Sie geeignete Annahmen über die verwendeten Ports.
- Das NAT-Gateway verwendet Port- und IP-Adress-Umsetzung.