



4. Blatt: Network Protocols and Architectures, WS 11/12

Aufgabe 1: (30 Punkte) *Analyse von TCP-Verkehr*

Diese Übungsaufgabe soll als Einführung in Techniken der Verkehrsanalyse am Beispiel realer TCP-Verbindungen dienen. Lade hierzu eine Version von Wireshark für dein Betriebssystem von <http://www.wireshark.org/> herunter und mache dich mit dem Werkzeug vertraut. Beschäftige dich insbesondere mit Anzeigefiltern (Display Filter) und deren Konfiguration.

Nun zum eigentlichen Experiment: Starte in Wireshark die Aufzeichnung des Verkehrs und öffne anschließend eine Webseite in deinem Browser. Nachdem die Webseite aufgerufen wurde, beende die Aufzeichnung wieder. Da in der Aufzeichnung vermutlich auch Pakete enthalten sind, die gar nicht zur angeforderten HTTP-Verbindung gehören, sollen diese nun mit einem Anzeigefilter ausgeblendet werden. Am einfachsten ist dies, wenn man nach der IP-Adresse des Webservers und dem HTTP-Protokoll filtert.

Analysiere die erhaltenen Daten und markiere Pakete, die zu den folgenden Abschnitten gehören, in einem Screenshot: i) TCP-Verbindungsaufbau, ii) Übertragung der HTTP-Anfrage, iii) HTTP-Antwort und iv) Verbindungsabbau. Füge diesen Screenshot in deine Lösung ein und gib ebenfalls den Hostnamen des verwendeten Webservers sowie dessen IP-Adresse und den benutzten Anzeigefilter an.

Aufgabe 2: (10 · 4 = 40 Punkte) *Größe des TCP-Staufens*

Angenommen, als Protokoll wird TCP Reno verwendet und weist das in Abbildung 1 gezeigte Verhalten. Beantworte die folgenden Fragen. Füge jeder deiner Antworten eine kurze Erklärung hinzu, die deine Antwort begründet. Die Beantwortung mit nur einer Zahl ist hierbei nicht ausreichend. Die Herleitung der angegebenen Werte sollte aus der Antwort ersichtlich werden. **Threshold** ist die Grenze, nach der TCP von Slow-Start in Stauvermeidung („congestion avoidance“) übergeht.

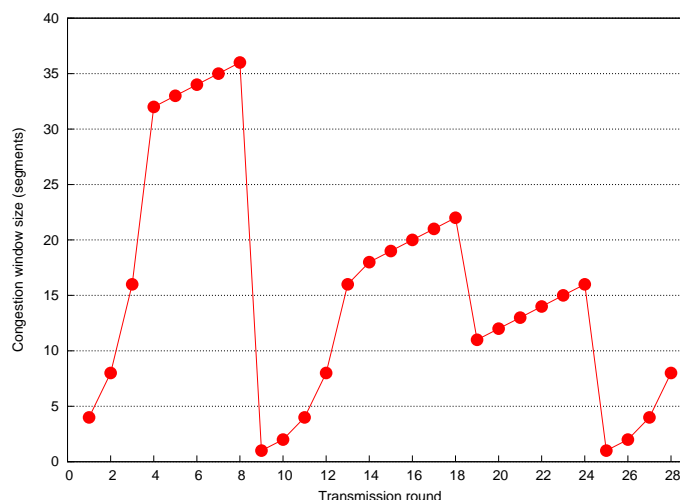
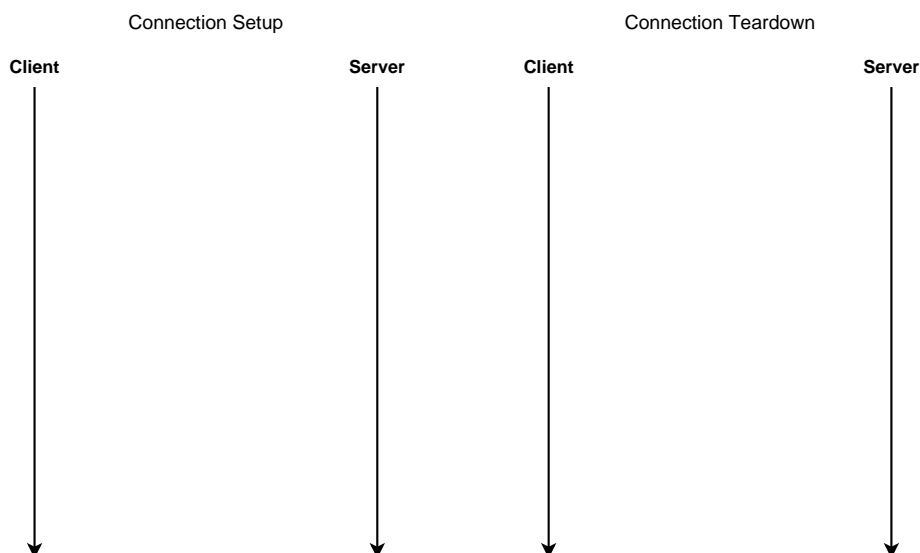


Abbildung 1: TCP-Staufenstergröße im Verlauf der Zeit.

- Wie lautet die initiale Fenstergröße?
- Bestimme die Zeitintervalle, in denen TCP im Slow-Start-Modus arbeitet.
- Bestimme die Zeitintervalle, in denen TCP im Stauverhinderungsmodus („congestion avoidance“) arbeitet.
- Wird der Segmentverlust nach der 8. Übertragungsrunde durch drei doppelte Bestätigungen („duplicate acknowledgements“) oder durch Zeitüberschreitung („timeout“) festgestellt?
- Wird der Segmentverlust nach der 18. Übertragungsrunde durch drei doppelte Bestätigungen („duplicate acknowledgements“) oder durch den Ablauf eines Timers („timeout“) festgestellt?
- Auf welchen Wert wurde **Threshold** zu Beginn der Verbindung gesetzt?
- Welchen Wert hat **Threshold** in der 10. Übertragungsrunde?
- Welchen Wert hat **Threshold** in der 20. Übertragungsrunde?
- In welcher Übertragungsrunde wird das 100. Segment gesendet?
- Angenommen, ein Paketverlust wird nach der 28. Runde durch drei doppelte Bestätigungen („duplicate Acknowledgements“) festgestellt. Wie ändern sich die Größe des Staufensters („congestion window“) und der Wert von **Threshold**?

Aufgabe 3: (15 + 15 = 30 Punkte) *TCP-Verbindungsauf- und -abbau*

TCP gilt als Paradebeispiel für verbindungsorientierte Dienste. Im Folgenden wird das Verbindungsmanagement daher etwas genauer untersucht.



- Trage den Ablauf eines erfolgreichen Verbindungsaufbaus in ein Diagramm (siehe links oben) ein. Beschrifte die Pfeile mit den dabei relevanten Teilen der TCP-Segmentstruktur (Flags, Sequenznummer, Bestätigungsnummer). Die initialen (zufällig bestimmten) Sequenznummern von Client und Server sind 2500 (Client) und 10030 (Server).
- Trage den erfolgreichen Verbindungsabbau in ein weiteres Diagramm (siehe rechts oben) ein. Beschrifte wiederum die Pfeile mit den dabei relevanten Teilen der TCP-Segmentstruktur (Flags, Sequenznummer, Bestätigungsnummer). Gehe davon aus, dass seit dem Aufbau aus (a) folgende Daten übertragen worden sind: 500 Bytes vom Client zum Server und 10000 Bytes vom Server zum Client. Berücksichtige diese Werte zur Bestimmung der Sequenz- und Bestätigungsnummern.

Abgabe bis Donnerstag, den 24. November 2011 nur bis 13:55 h s. t.

- **Als PDF-Dateien (keine MS-Office- oder OpenOffice-Dateien):** Mittels ISIS hochladen (<https://www.isis.tu-berlin.de/course/view.php?id=5258>)
- **In Papierform:** Postfach im Telefunkenhochhaus (Erdgeschoss, hinter dem Pfortner rechts)
- Gib auf deiner Lösung deinen Namen, deine Matrikelnummer **und** den Namen deines Tutors an.