Karlsruher Institut für Technologie

Institut für Telematik
Karlsruher Institut für Technologie (KIT)
Prof. Dr. M. Zitterbart
T. Gerhard, M. Sc.
M. Flittner, M. Sc.
M. Jung, M. Sc.
S. Friebe, M. Sc.

Einführung in Rechnernetze
Sommersemester 2017

4. Übungsblatt

Aufgabe 1: TCP-Analyse mit Wireshark

Wireshark (`https://www.wireshark.org/`) ist ein mächtiges Werkzeug zur Analyse von Datenströmen in Netzwerken. Es bietet vielfältige Möglichkeiten, um ein- und ausgehende Pakete mitzuschneiden, zu filtern und auszuwerten. In dieser Aufgabe sollen Sie Wireshark dazu nutzen, das Kommunikationsverhalten Ihres Chat-Clients aus den vorherigen Übungsblättern näher zu untersuchen. Sollten Sie diese Aufgabe nicht gelöst haben, können Sie ersatzweise auch mit einem Webbrowser auf den Chat-Server zugreifen: `http://i72tmdjango.tm.kit.edu:8000/chat`

(a) Starten Sie Wireshark und machen Sie sich mit der Oberfläche vertraut. Zu Beginn ist eine (oder mehrere) Netzwerkschnittstelle auszuwählen, deren ein- und ausgehende Pakete von Wireshark aufgezeichnet werden sollen. Wenn Ihr Computer mehr als eine Netzwerkschnittstelle hat (etwa Ethernet+WLAN, oder auch VPNs), sollten Sie eine verwenden die zur Zeit genutzt wird. Starten Sie die Aufzeichnung und beobachten Sie Ihren Netzwerkverkehr. Welche Protokolle erkennt Wireshark? Können Sie Datenströme den gerade ausgeführten Anwendungen zuordnen?

(b) Starten Sie nun zunächst eine neue Aufzeichnung und dann Ihren Chat-Client. Nachdem die Ausführung des Clients abgeschlossen ist, können Sie die Aufzeichnung anhalten. Wireshark interpretiert die aufgezeichneten Dateneinheiten und stellt die in Protokollfeldern und aus dem Kontext abgeleitete Informationen dar. Können Sie die Anfragen Ihres Chat-Clients in der Aufzeichnung ausfindig machen? Wodurch können Sie den Datenstrom Ihres Clients von anderen unterscheiden?

(c) Die von Wireshark ausgewerteten Informationen können auch genutzt werden, um die Ansicht auf erwünschte Datenströme zu beschränken. Dazu können oberhalb der Paketliste Anzeigefilter konfiguriert werden, etwa `ip.addr == 141.3.10.5`. Versuchen Sie alle Datenströme welche nicht zu ihrem Chat-Client gehören herauszufiltern.

(d) Analysieren Sie ausgetauschten TCP-Segmente:

- Wo findet der Verbindungsaufbau und -abbau statt? Welche Informationen werden ausgetauscht?
- Wie erfolgt die Übertragung der HTTP-Requests? Können Sie Datensegmente und Quittungen zuordnen?
- Wo gibt es Unterschiede gegenüber den in der Vorlesung besprochenen Abläufen und Mechanismen?

Aufgabe 2: TCP-Mechanismen und Verbindungsverwaltung

(a) Ein TCP-Segment wird mit `seq=17,ack=92` empfangen. Es sind keine weiteren Flags gesetzt. Verändert sich das Flusskontrollfenster?

(b) Wie groß muss Ihr Flusskontrollfenster sein, damit Sie ein Netz mit der Datenrate 1000 MBit/s voll auslasten können? Die insgesamt zurückgelegte Strecke zwischen Sender und Empfänger betrage 800 km. Die Ausbreitungsgeschwindigkeit sei 200.000 km/s, Verzögerungen durch Zwischensysteme werden vernachlässigt.

(c) Warum sieht TCP ein Fluss- und ein Staukontrollfenster vor? Genügt nicht eines von beiden oder könnte man beide Fenster nicht zusammen fassen?

(d) Befindet sich im TCP-Kopf ein Flag zum Anzeigen von Fragmentierung?

(e) Warum etabliert TCP eine Verbindung? Könnte die Funktionalität von TCP auch ohne Verbindungskontext realisiert werden?

(f) Welche Informationen müssen Endsysteme zum Zustand einer TCP-Verbindung speichern? Wozu dienen diese?

(g) Wieso ist bei TCP ein 3-Wege-Handshake erforderlich? Könnte der Verbindungskontext nicht einfach implizit mit Beginn der Datenübertragung durch den Sender etabliert werden?

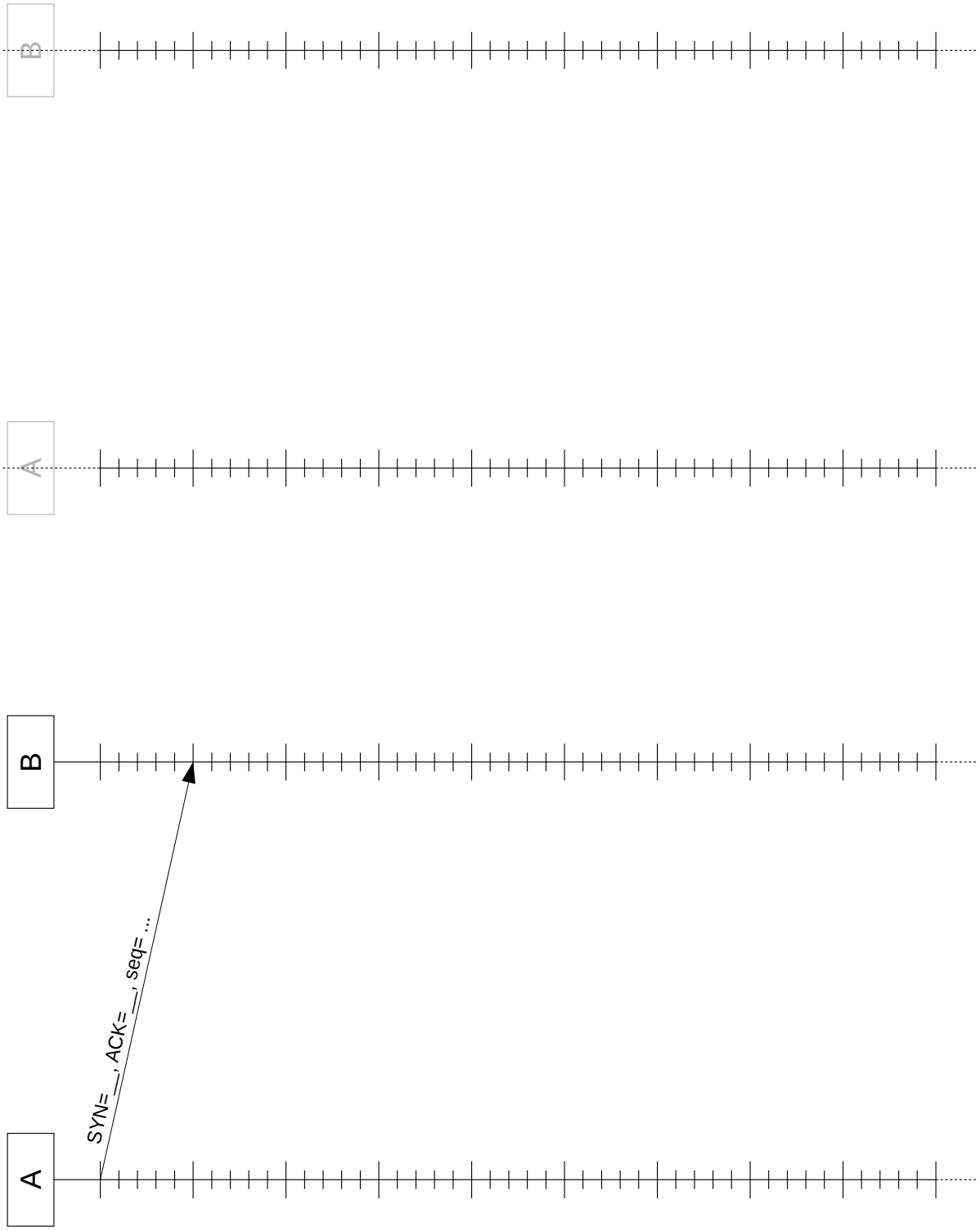
Aufgabe 3: TCP-Arbeitsweise und Flusskontrolle

Host A will über eine TCP-Verbindung 700 Byte an Host B übertragen. Host B antwortet im Anschluss mit 350 Byte. Host A arbeitet mit einem Empfangsfenster von 200 Byte, Host B mit 300 Byte. Die MSS betrage 100 Byte. Ein Segment kommt eine Zeiteinheit nach dem es abgesendet wurde beim Empfänger an. Innerhalb einer Zeiteinheit können bis zu fünf Segmente versendet werden. Der Timer für Quittungen laufe nach je drei Zeiteinheiten ab. Berücksichtigen Sie, dass TCP Go-Back-N nutzt. Es kommt keine Staukontrolle zum Einsatz.

(a) Zeichnen Sie den Verbindungsaufbau in das nachfolgende Weg-Zeit-Diagramm ein. Welche Informationen werden übertragen? Hinweis: Host A wählt als initiale Sequenznummer 2020, Host B 4221.

(b) Bei der folgenden Übertragung gehe das fünfte Segment von Host A verloren. Vervollständigen sie das Weg-Zeit-Diagramm mit dem kompletten Ablauf der Übertragung. Geben Sie für jedes Segment an: Sequenznummer, Quittung und, sofern zutreffend, die Nutzdaten (etwa: Byte 51-100).

(c) Host A initiiert einen Verbindungsabbau. Ergänzen Sie den Ablauf im Weg-Zeit-Diagramm.



Aufgabe 4: TCP-Staukontrolle

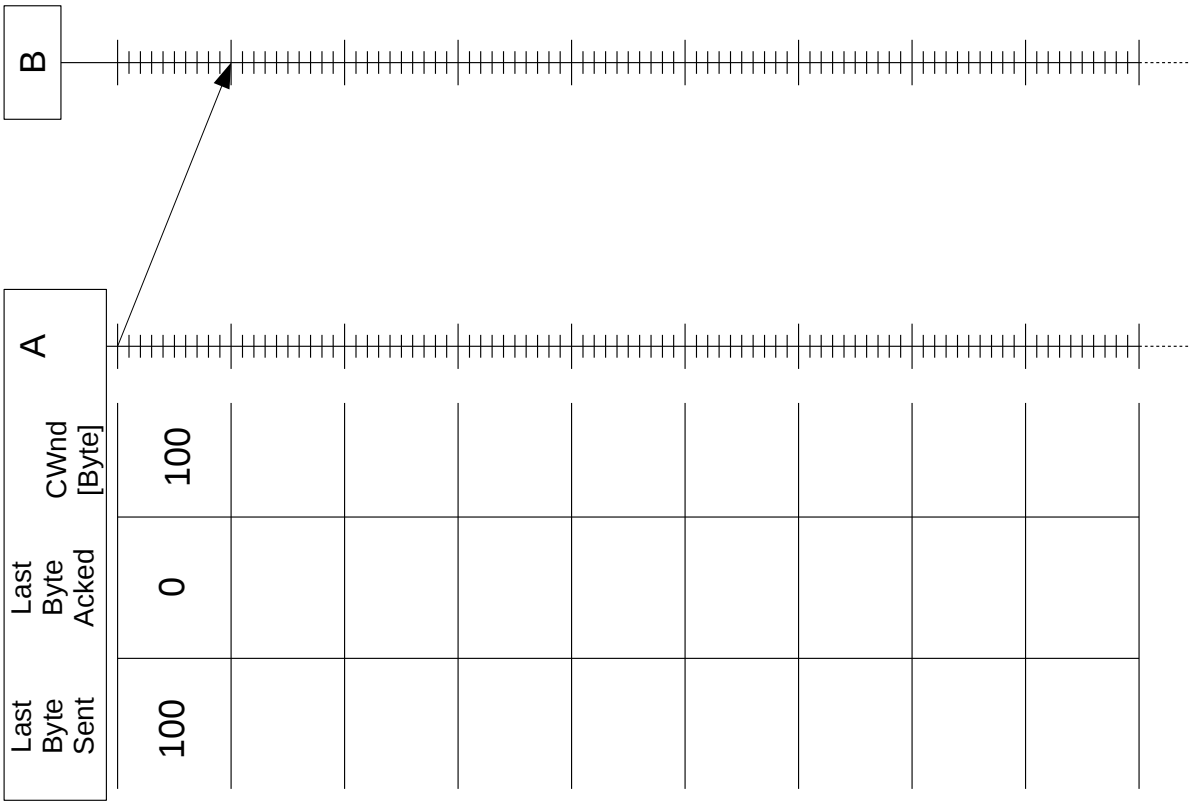
Host A will über eine TCP-Verbindung 3500 Byte an Host B übertragen. Hierbei kommt das Staukontrollverfahren aus der Vorlesung, aber keine Flusskontrolle, zum Einsatz. Die MSS betrage 100 Byte. Ein Segment kommt eine Zeiteinheit nach dem es abgesendet wurde beim Empfänger an. Innerhalb einer Zeiteinheit können bis zu zehn Segmente versendet werden. Werden acht oder mehr Segmente innerhalb einer Zeiteinheit versendet, kommt es zu einer Stausituation. Nehmen Sie vereinfachend an, dass dann alle in dieser Zeiteinheit gesendeten Segmente den Empfänger nicht erreichen. Der Timer für Quittungen laufe nach je drei Zeiteinheiten ab.

Der Verlauf der Übertragung soll im nachfolgenden Weg-Zeit-Diagramm dargestellt werden. Setzen Sie dieses bis zum Abschluss der Übertragung fort. Bearbeiten Sie außerdem die nachfolgenden Teilaufgaben:

(a) Markieren Sie, an welcher Stelle eine Stausituation erkannt wird.

(b) Zeichnen Sie ein, wo sich die Staukontrolle in der Slow-Start und Congestion-Avoidance-Phase befindet.

(c) Tragen Sie in jedem Zeitschritt die jeweils zuletzt gültigen Werte ein für: Größe des Staukontrollfensters (CWnd), jeweils größte gesendete Sequenznummer (LastByteSent) und größte quittierte Sequenznummer (LastByteAcked).



B

A
Last Byte Sent
Last Byte Acked
CWnd [Byte]

B

A
Last Byte Sent
Last Byte Acked
CWnd [Byte]

Aufgabe 5: Vermittlungsformen und -prinzipien

(a) Worin unterscheidet sich die Datagrammvermittlung von virtuellen Verbindungen?

(b) Sind bei virtuellen Verbindungen die Kennungen im ganzen Netz global?

(c) Wie funktioniert die Datagrammvermittlung?

(d) Welche Ebenen werden in der Vermittlungsschicht unterschieden? Was sind ihre Aufgaben?

Aufgabe 6: IP

(a) Welche Informationen stehen im Kopf eines IP-Datagramms?

(b) Die im Internet eingesetzten Protokolle TCP und IP bieten beide die Möglichkeit zum Aufteilen von Paketen (Segmentierung und Fragmentierung). Welche Möglichkeit wäre hierbei zu bevorzugen? Erläutern Sie entsprechende Vor- und Nachteile.

Aufgabe 7: IP-Adresskonfiguration und Subnetze

Das 1993 in RFC 1519 spezifizierten *Classless Inter-Domain Routing* (CIDR) definiert eine flexible Aufteilung von IP-Adressen in Netzwerk-Teil und lokalen Teil. Die Subnetzmaske, welche in ihrer Darstellung als folge von Bits festlegt, welche Bit der IP-Adresse das Netzwerk und welche Bit den Endsystem-Teil repräsentieren, kann mit CIDR eine beliebige Länge haben. Zudem wurde eine neue Notation eingeführt, bei der die Anzahl gesetzten Bits („1“) der Subnetzmaske als »/Anzahl« hinter die IP-Adresse geschrieben wird.

Beispiel: 13.12.11.10/28 entspricht der IP-Adresse 13.12.11.10 mit Subnetzmaske 11111111. 11111111.11111111.11110000 (28 Einsen, Binärschreibweise) bzw. 255.255.255.240 (Dezimalschreibweise). In diesem Fall bestimmen daher die ersten 28 Bit der binären IP-Adresse den Netzwerk-Teil, während die letzten 4 Bit den Endsystem-Teil repräsentieren. Aufgrund des 4 Bit langen Endsystem-Teils können daher mit dieser Subnetzmaske maximal 2^4 und damit 16 Adressen im zugehörigen Netzwerk verwendet werden.

(a) Gegeben sei der IP-Adressbereich 141.22.67.0/24. Liegt die Adresse 141.22.70.198 im zugehörigen Netzwerk oder nicht?

(b) Gegeben sei der IP-Adressbereich 141.22.67.0/20. Liegt die Adresse 141.22.70.198 im zugehörigen Netzwerk oder nicht?

(c) Gegeben sei der IP-Adressbereich 141.22.67.0/22. Welche IP-Adressen bilden den Anfang und das Ende dieses Adressbereichs?

(d) Ihnen sei von Ihrem Netzbetreiber der IP-Adressbereich 141.22.67.0/26 zur freien Verfügung zugeteilt worden. Sie möchten diese Adressen getrennt auf drei Netzwerk-Standorte verteilen. Am ersten Standort sind 10 Endsysteme anzubinden, am zweiten 13 und am dritten 21. Mit welchen Adressen und Subnetzmasken konfigurieren Sie die einzelnen Standorte?