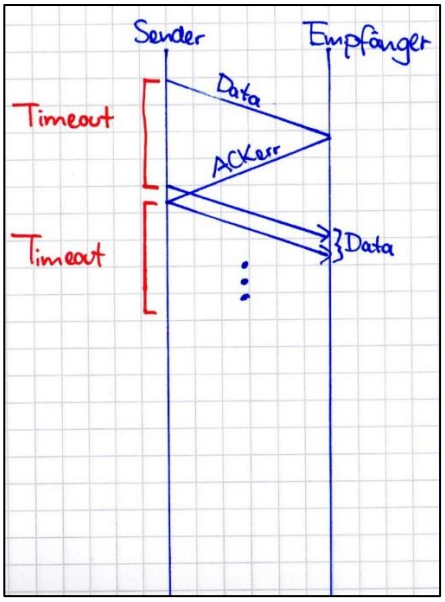
Übung 10: Zuverlässige Datenübertragung

Aufgabe 1: Timeout vs. Retransmission



Sie setzen das fiktive TCP-Protokoll der ***Version 2.0*** aus der Vorlesung ein. Durch einen unglücklichen Zufall haben ***ALLE*** ACK-Bestätigungen des Empfängers an den Sender *Bitfehler*. Empfängt der Sender korrupte ACKs hat er 2 Möglichkeiten:

i. Starte ***immer sofort*** eine *Retransmission*.
ii. Warte mit der *Retransmission* bis zum *Timeout*.

Bewerten Sie den Ansatz (i) für den Fall, dass durch eine aktuelle Überlastung des Netzes die **Round Trip Time vorübergehend größer ist als der Timeout-Wert** zur Erkennung von Paketverlusten.

Vervollständigen Sie dazu das in *Abbildung 1* vorgegebene Sequenzdiagramm um eine weitere Iteration und überlegen Sie sich, was ungünstig ist. Nehmen Sie an, dass keine Paketverluste auftreten.

Aufgabe 2: Go-Back-N (GBN) und Selective Repeat (SR)[1]

Es gilt das ***fiktive*** Protokoll Version 3 der Vorlesung, siehe Folie 17ff. Eine nette Animation zu den beiden Implementierungsvarianten gibt es hier: http://www.ccs-labs.org/teaching/rn/animations/gbn_sr/

a) Nehmen Sie an, dass zwei Hosts *A* und *B* ein GBN-Verfahren verwenden. Die Sendefenster beträgt $N = 3$, die Anzahl der verfügbaren Sequenznummern sei ausreichend[2]. *A* sendet 6 Nutzdatennachrichten zu *B*. Alle ausgetauschten Nachrichten werden korrekt empfangen mit Ausnahme des 1. Acknowledgements von *B* zu *A* und des 5. Datensegments von *A* zu *B*. Zeichnen Sie ein Diagramm ähnlich wie auf Folie 20.

b) Es gilt das Szenario von a), es wird nun aber das SR-Verfahren eingesetzt. Zeichen Sie nun ein Diagramm ähnlich wie auf Folie 22 und versuchen Sie die Unterschiede zu verstehen.

c) Sie wissen Folgendes:
- Bei einem *Go-Back-N* Protokoll beträgt die Größe des Sendefensters 4.
- Die Sequenznummern laufen von 0 bis 1024.
- Gemäß der Reihenfolge erwartet der Empfänger als nächstes das Paket mit der Sequenznummer 500.
- Der Übertragungskanal ändert die Reihenfolge der Pakete nicht.

Welche Sequenznummern könnte das ***Sendefenster*** des Senders theoretisch enthalten?

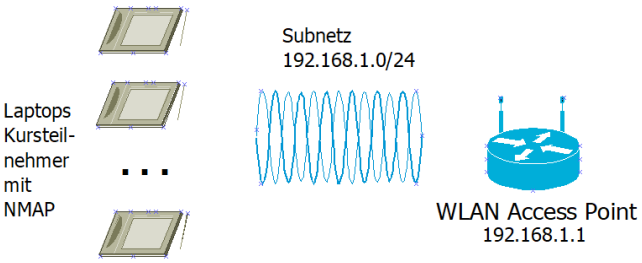
d) Pipelining: Sender *A* an der Ostküste der USA sendet Nutzdaten zum Empfänger *B* an der Westküste. Wie groß müsste das Sendefenster von *A* sein, damit der Sender zu mindestens 98% der Zeit senden kann? Es gelten die folgenden Annahmen:
- Jedes Paket ist *L*=1500 Byte groß.
- Propagation Delay: $d_{prop} = 15\ ms$
- (Konstante) Datenrate: *R*=1 Gbit/s
- ACK-Pakete seien vernachlässigbar klein, der Empfänger kann ein ACK zurücksenden unmittelbar nachdem das letzte Bit des Datenpakets angekommen ist.

---

[1] Es werden fiktive Lehrprotokolle betrachtet, nicht TCP. Sequenznummern beziehen sich auf Pakete.
[2] Annahme: Der Datenkanal ändert nicht die Reihenfolge der Pakete.

Aufgabe 3: Scanning mit `nmap`

a) Verbinden Sie sich mit dem WLAN „`rechnernetze`“ das im Übungsraum zur Verfügung steht. Das Passwort ist ebenfalls „`rechnernetze`“.
Der WLAN Router vergibt per DHCP IP Adressen aus dem Bereich von 192.168.1.100 bis 192.168.1.199.



b) Falls nicht bereits vorhanden: Installieren Sie `nmap` auf Ihrem PC und starten Sie das Programm ggfs. mit Administratorrechten! Link: https://nmap.org/download.html

c) Hosterkennung[3]: `nmap -SP <CIDR-Präfix>`
- Finden Sie heraus, welche Hosts /IPs im Subnetz 192.168.1.0/24 aktiv sind?
- Erklären Sie mit einer Wireshark-Aufzeichnung was im Hintergrund passiert!

d) Port Scanning[4]: `nmap -sS <target-ip>`
- Legen Sie sich auf eine „Opfer“ IP-Adresse fest.
- Finden Sie nun heraus, welche Ports auf diesem Host offen sind!
- Schneiden Sie wieder parallel in Wireshark mit, erklären Sie was passiert.

e) Nachdem Sie aktive Hosts und Port kennengelernt haben, können Sie mit nmap versuchen, noch mehr herauszufinden. Wer möchte kann folgende Kommandos testen. Es wird empfohlen, den jeweiligen Scan mit der Option –p nur auf einen erkannten offenen Port anzuwenden.
Möglichkeiten:
- Erkennen des Betriebssystems: `nmap –p <active port> -O <target-ip>`
- Erkennung der Anwendung hinter Port: `nmap –sV <active port> -O <target-ip>`

Vorsicht: Exzessives Scanning z.B. im Studentenwohnheim wird meistens erkannt, Ihr Zugang könnte gesperrt werden.

[3] https://nmap.org/man/de/man-host-discovery.html
[4] https://nmap.org/man/de/man-port-scanning-techniques.html