



Übung 10: Go-Back-N, Selective Repeat, nmap

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

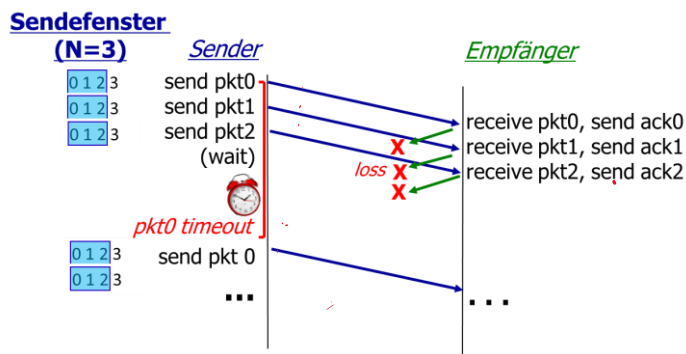
Es gilt das **fiktive** Protokoll Version 3.0 der Vorlesung. Beachten Sie hierzu auch die Animation:
http://www.ccs-labs.org/teaching/rn/animations/gbn_sr/

- Nehmen Sie an, dass zwei Hosts *A* und *B* ein GBN-Verfahren² verwenden. Die Sendefenster beträgt $N = 3$. *A* sendet 6 Nutzdatennachrichten zu *B*. Alle ausgetauschten Nachrichten werden korrekt empfangen, nur das 1. Acknowledgement von *B* zu *A* und des 5. Datensegments von *A* zu *B* gehen verloren. Zeichnen Sie ein Diagramm ähnlich wie in der Vorlesung.
- Es gilt weiterhin das Szenario von a). Nun wird aber das SR-Verfahren eingesetzt. Zeichnen Sie erneut ein Diagramm und erläutern Sie die Unterschiede zu a).
- Go-Back-N: Welche Sequenznummern könnte das **Sendefenster** theoretisch enthalten?
 - Die Größe des Sendefensters ist $N = 4$.
 - Die Sequenznummern laufen von 0 bis 1024.
 - Der Empfänger benötigt als **nächstes** das Paket mit der Sequenznummer 500.
 - Der Übertragungskanal ändert die Reihenfolge der Pakete nicht.

Aufgabe 2: Maximale Größe des Sende- und Empfangsfensters

Nehmen Sie an, dass für die Sequenznummern $m = 2$ Bits zur Verfügung stehen. Es gibt 2^m mögliche Sequenznummern, diese liegen im Bereich $[0, 2^m - 1]$. Im konkreten Beispiel lauten die Sequenznummern $\{0, 1, 2, 3\}$. Im Folgenden überlegen wir, wie groß das Sendefenster N beim *Go-Back-N* und *Selective-Repeat* Verfahren sein darf.

Hilfreich das folgende Beispiel einer Paketübertragung, bei dem jeweils alle Acknowledgements verloren gehen. Das Sendefenster in der Zeichnung hat die Größe $N=3$, Fall von **Aufgabe c**).



- Was ist m beim realen TCP? Was ist hier die maximale und minimale Sequenznummer?
- Go-Back-N: Die Größe des Sendefensters sei $N = 2^m = 4$. Warum funktioniert das nicht? Erklären Sie anhand des Beispiels! *Tipp*: Was erwartet der Empfänger?
- Go-Back-N: Die Größe des Sendefensters sei $N = 2^m - 1 = 3$. Funktioniert das? Erklären Sie am Beispiel!
- Selective Repeat: Die Größe des Sendefensters N ist stets gleich der Größe des Empfängerfensters. Was passiert, falls $N = 2^m - 1 = 3$? Erklären Sie am Beispiel!
- Selective Repeat: Wie groß darf das Sende- und Empfängerfensters maximal sein?

¹ Es werden fiktive Lehrprotokolle betrachtet, nicht TCP. Sequenznummern beziehen sich auf Pakete.

² Annahmen: Der Datenkanal ändert nicht die Reihenfolge der Pakete. Die Anzahl der verfügbaren Sequenznummern sei ausreichend.

Aufgabe 3: Scanning mit nmap

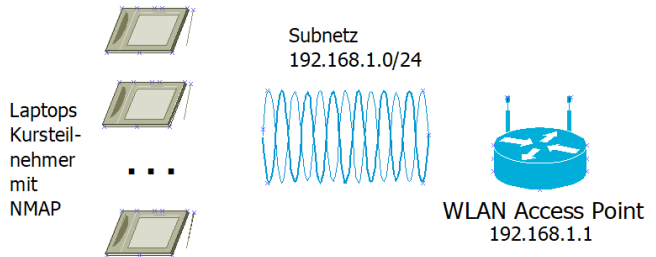
Vorsicht: Exzessives Scanning im öffentlichen LAN, z.B. Studentenwohnheim, kann zur Sperrung Ihres Zugangs führen. Nehmen Sie nur ein WLAN/LAN, das Sie selbst administrieren!

- a) Verbinden Sie sich mit Ihrem Heim-WLAN oder LAN!
- 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) Hosterkennung³: nmap -sn <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 Scanning⁴: 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.

- Erkennen des Betriebssystems: nmap -p <active port> -O <target-ip>
- Erkennung der Anwendung hinter Port: nmap -sV <active port> -O <target-ip>

³ <https://nmap.org/man/de/man-host-discovery.html>

⁴ <https://nmap.org/man/de/man-port-scanning-techniques.html>