המרכז לחינוך סייבר
CYBER EDUCATION CENTER

רשתות מחשבים

פרק 6ד' – שכבת התעבורה, פרוטוקול TCP

ברק גונן
מבוסס על ספר הלימוד "רשתות מחשבים" מאת
עומר רוזנבוים

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

מטרות הפרק

- בפרק זה נעמיק בפרוטוקול TCP
- נבין מהו sequence number של TCP
- נבין מהו מנגנון ה-ACK של TCP
- נבין את תהליך הקמת קשר TCP שבין שרת ולקוח
- נחקור קובץ הסנפה של מתקפת SYN FLOOD

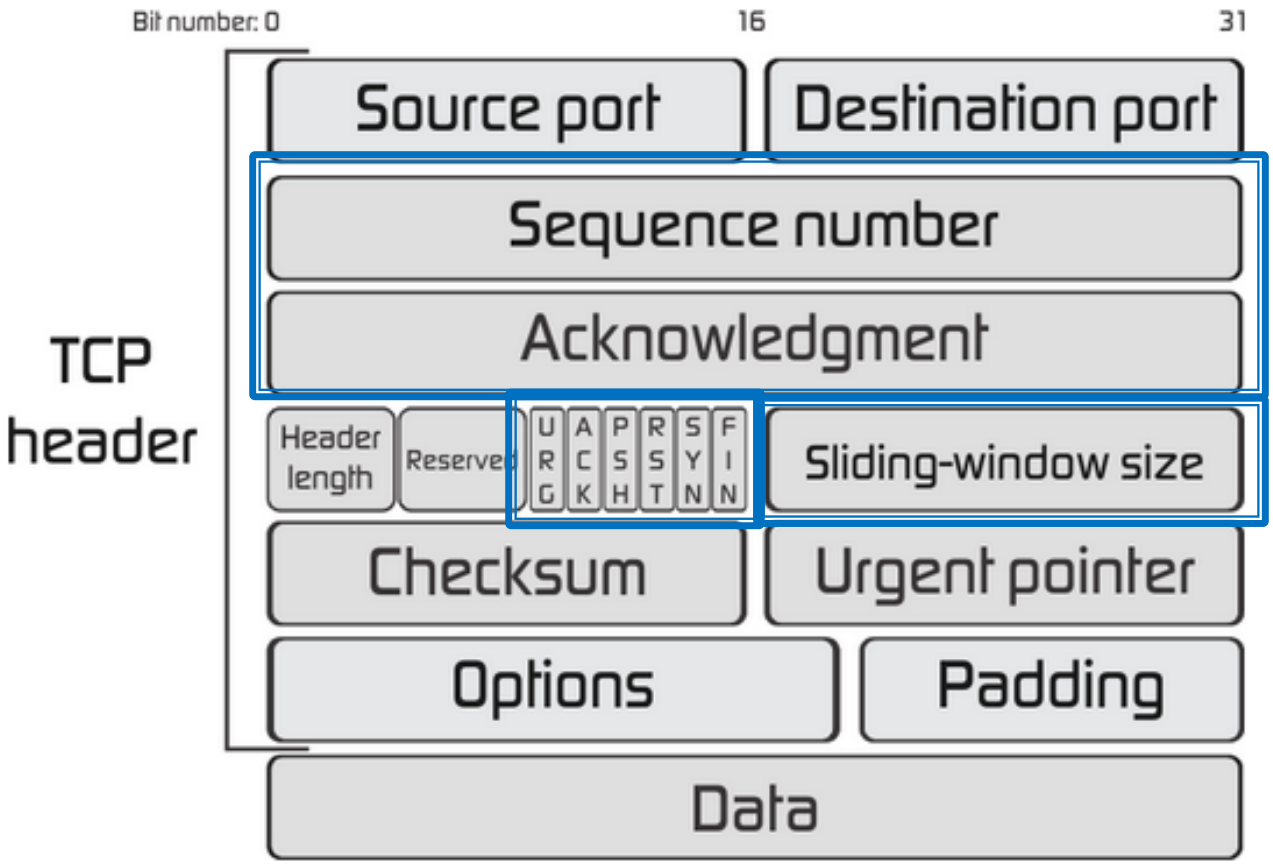
המרכז לחינוך סייבר
CYBER EDUCATION CENTER

חזרה קצרה

- למדנו ששכבת התעבורה יכולה (אופציונלית) לספק שירות אמין
  - שירות לא אמין- UDP
  - שירות אמין- TCP
- מהו שירות אמין?
  - כל הפקטות הגיעו
  - הסדר לא התבלבל
  - אין שגיאות במידע

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

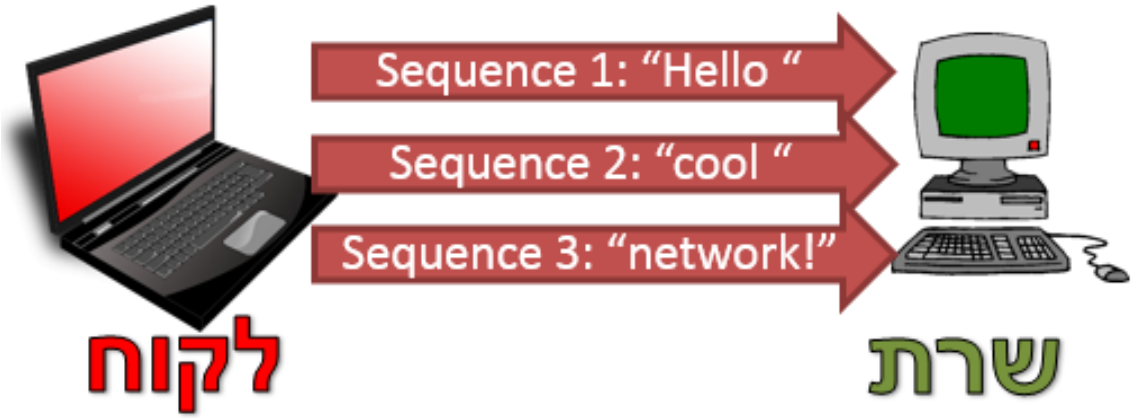
TCP Header



המרכז לחינוך סייבר
CYBER EDUCATION CENTER

Sequence Numbers

- נפרק את המשפט 'Hello cool network!' למקטעים, שנקראים Segments*
- כל סגמנט ישודר עם sequence number



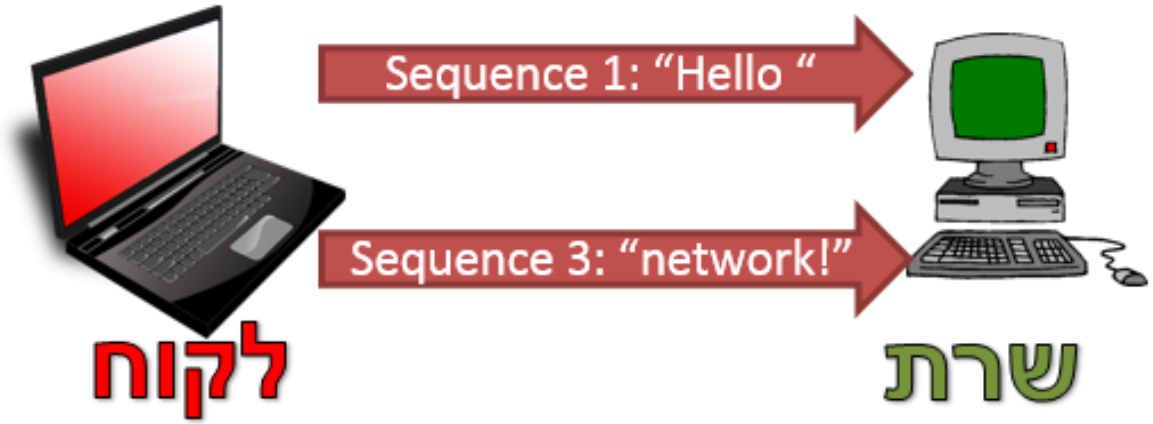
- חישבו: בשביל מה זה טוב?

* סגמנט- גוש מידע של שכבת התעבורה. עקב מודל השכבות, כל סגמנט נעטף בפקטה של שכבת הרשת, לכן נהוג לקרוא לסגמנט שעובר ברשת "פקטה".

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

המשך -Sequence Numbers

- כעת, אם נופל סגמנט בדרך, או אם הסדר מתבלבל, לצד השני יש דרך לדעת זאת



המרכז לחינוך סייבר
CYBER EDUCATION CENTER

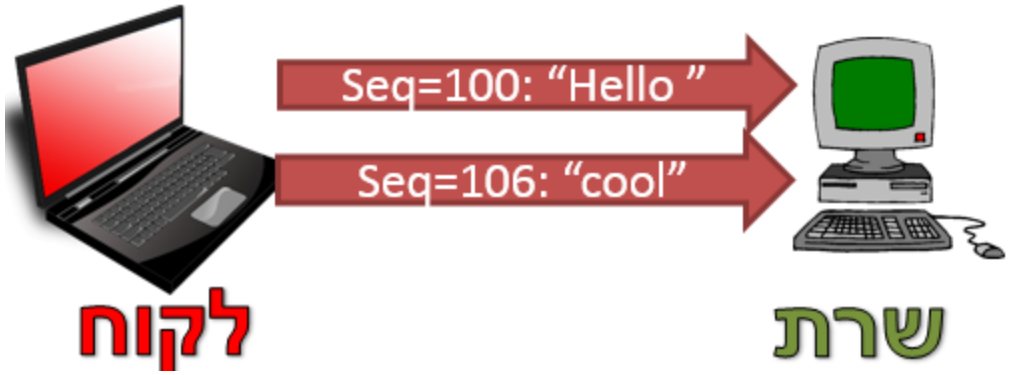
ACK

- ACK- קיצור של Acknowledgement, אישור
- לא מספיק שהצד המקבל יידע שמשהו חסר, הצד השולח צריך לדעת זאת, ואם אין ACK- לשלוח שוב

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

TCP Sequential Numbers

- נעבור מתיאוריה כללית למימוש ב-TCP
- כל בית של מידע מקבל מספר
- שדה Seq מקבל את הערך של הבית הראשון



שימו לב- יש סימן רווח אחרי Hello

- מה יהיה ה-Seq בסגמנט הבא?
  - 110 (106+4)

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

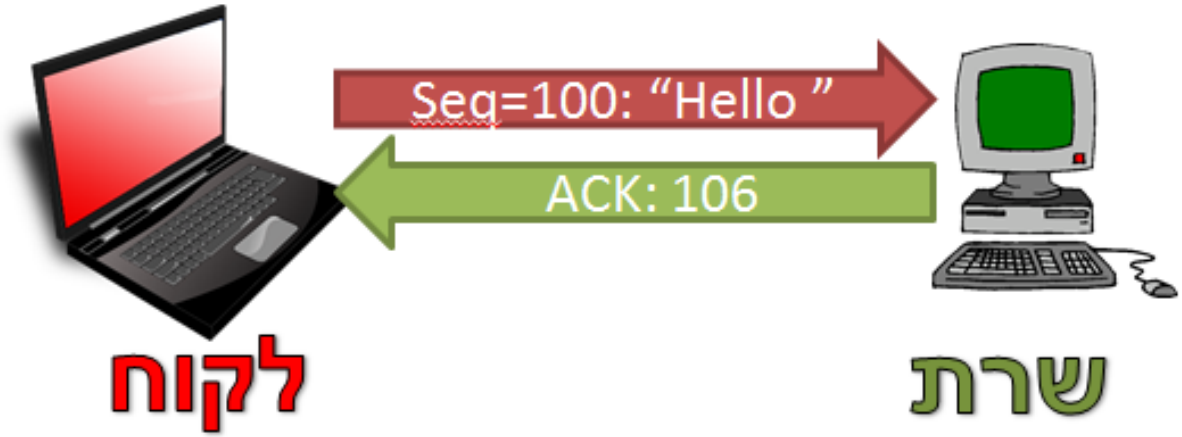
TCP Sequence Numbers

- בצעו את תרגיל 6.14 מודרך, צפיה ב-TCP Seq

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

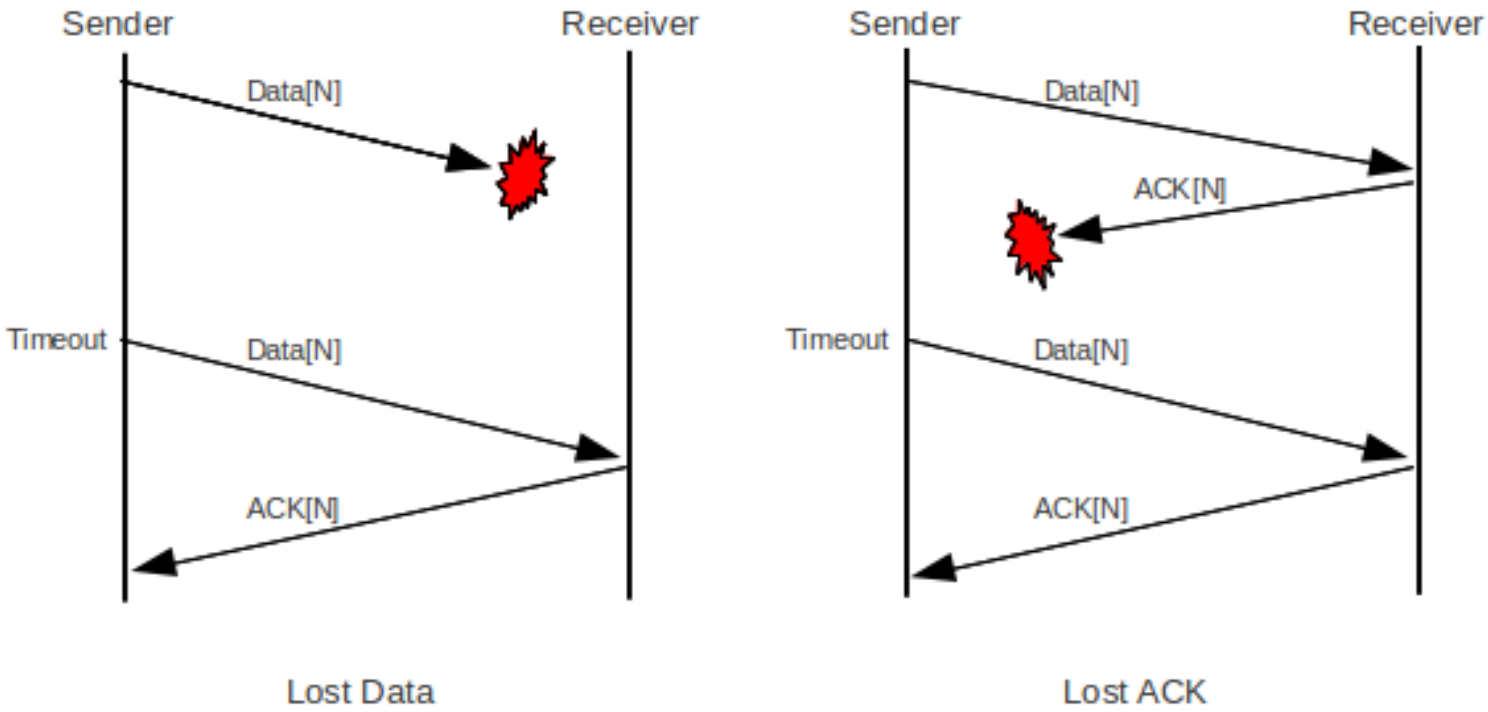
TCP ACK

- כמו שה-Seq מתייחס לבתים, גם ה-ACK
  - לדוגמה: ACK 106 = "קיבלתי עד בית 105, כולל. הבית הבא שאני מצפה לקבל הוא 106"



באילו מקרים יבוצע Retransmit?

- חישבו על תרחישים בהם יבוצע retransmit



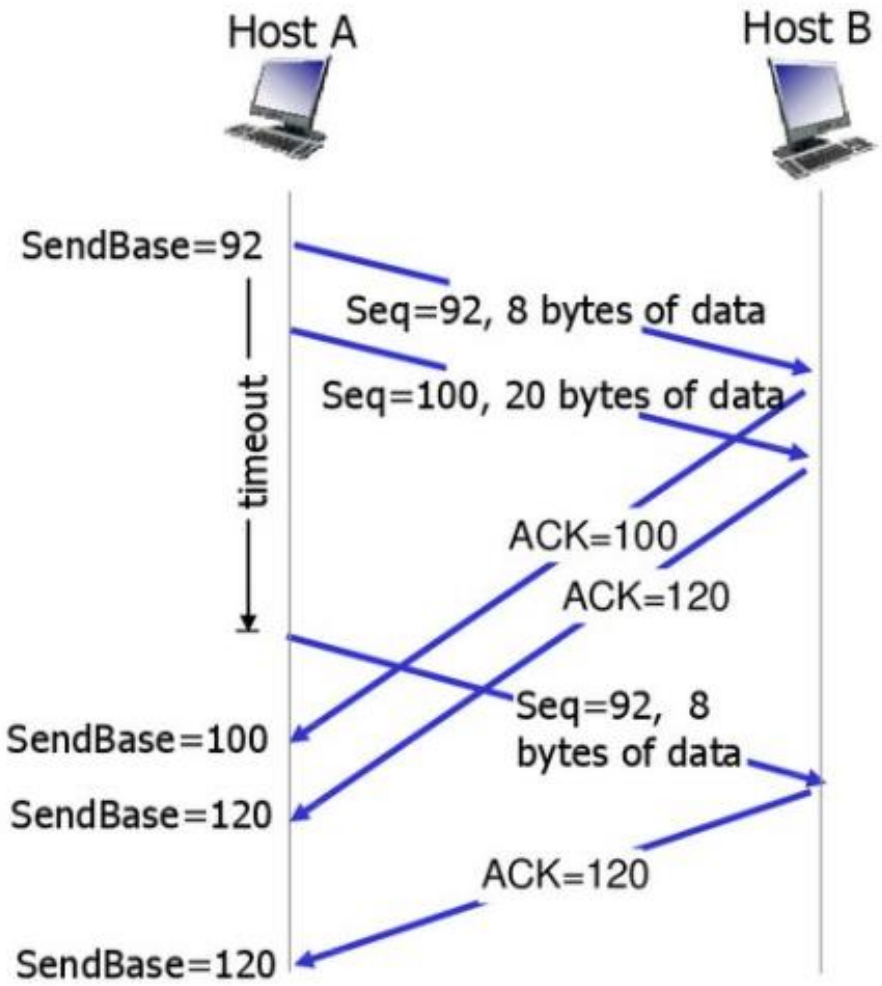
המרכז לחינוך סייבר
CYBER EDUCATION CENTER

TCP ACK

- בצעו את תרגיל 6.15 מודרך, צפיה ב-TCP ACK

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

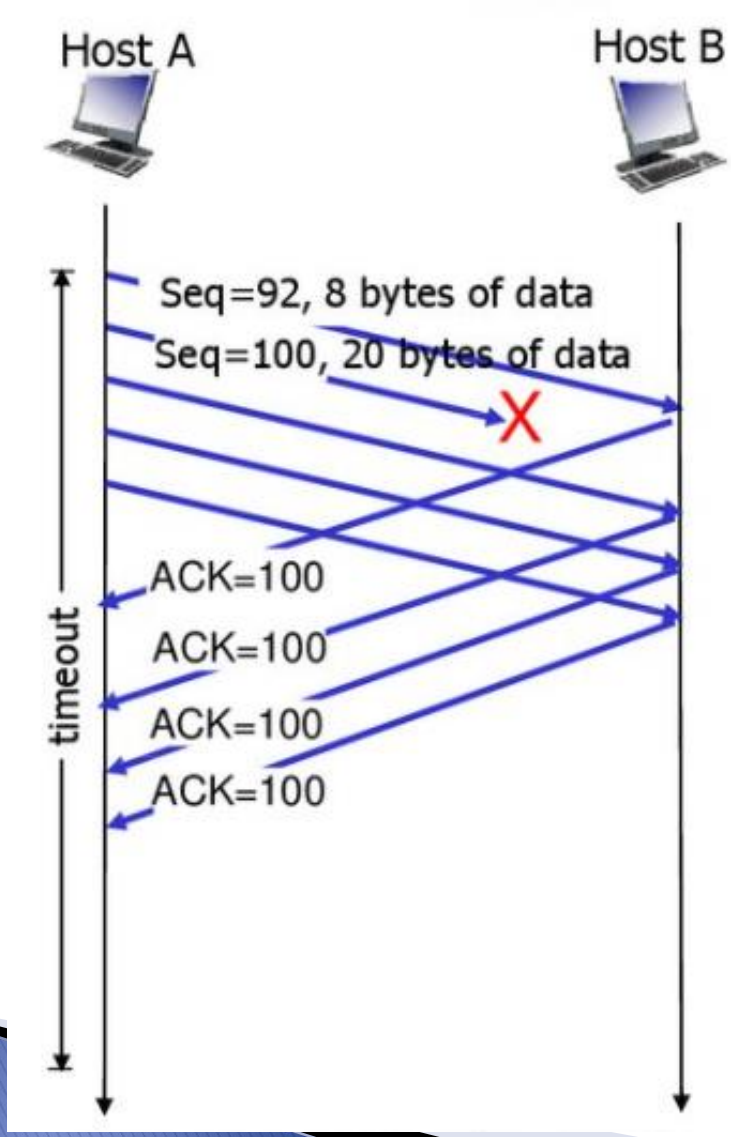
Premature Timeout



- כיצד ניתן לקבוע את ה-timeout בצורה מושכלת?

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

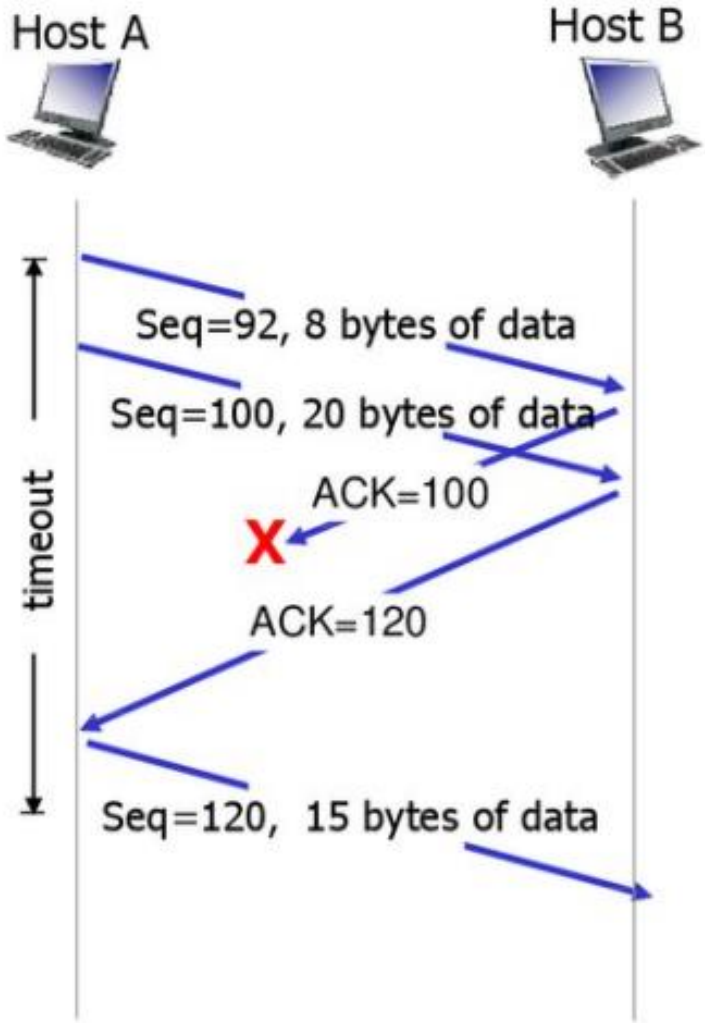
Fast retransmit



- מה הייתם עושים במקום A?

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

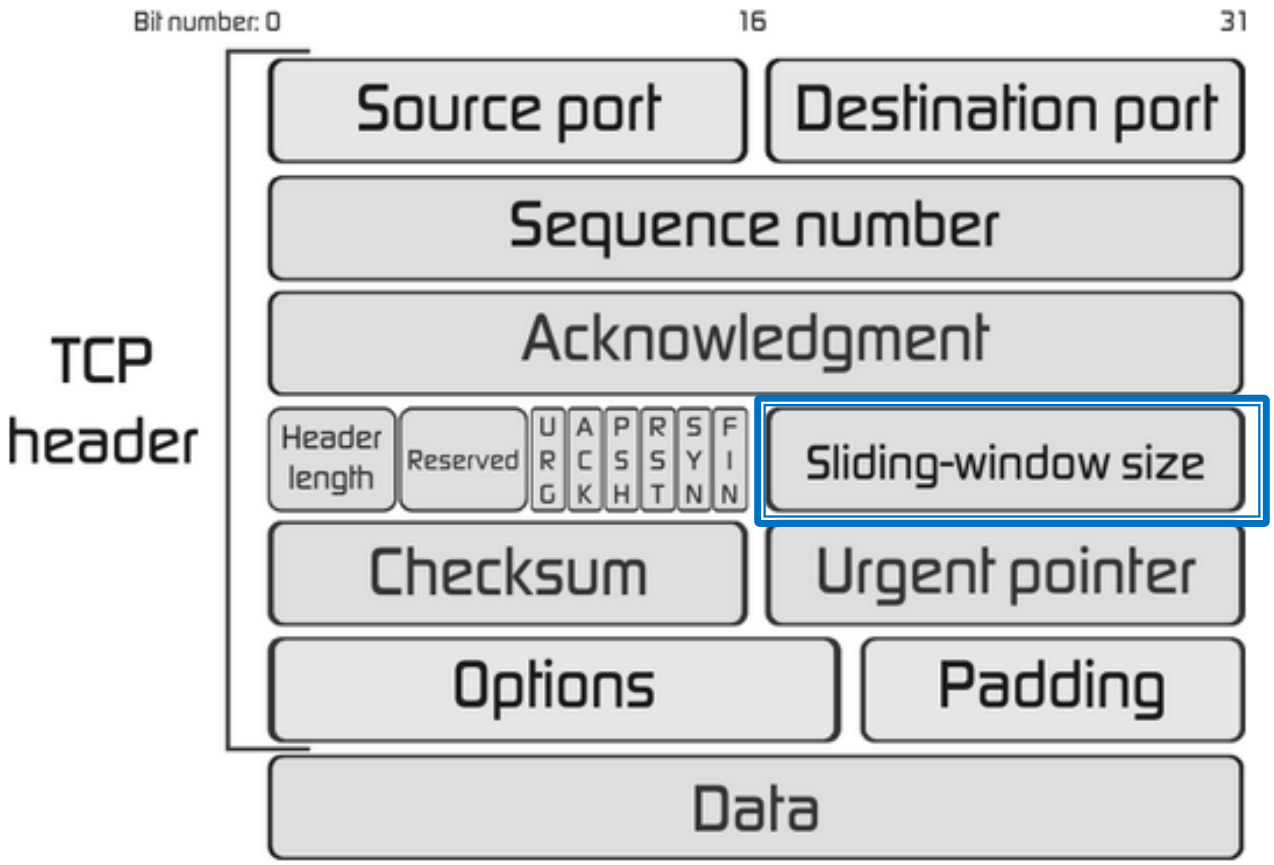
Cumulative ACK



- מדוע A לא שלח שוב את החבילה בעלת seq=100?

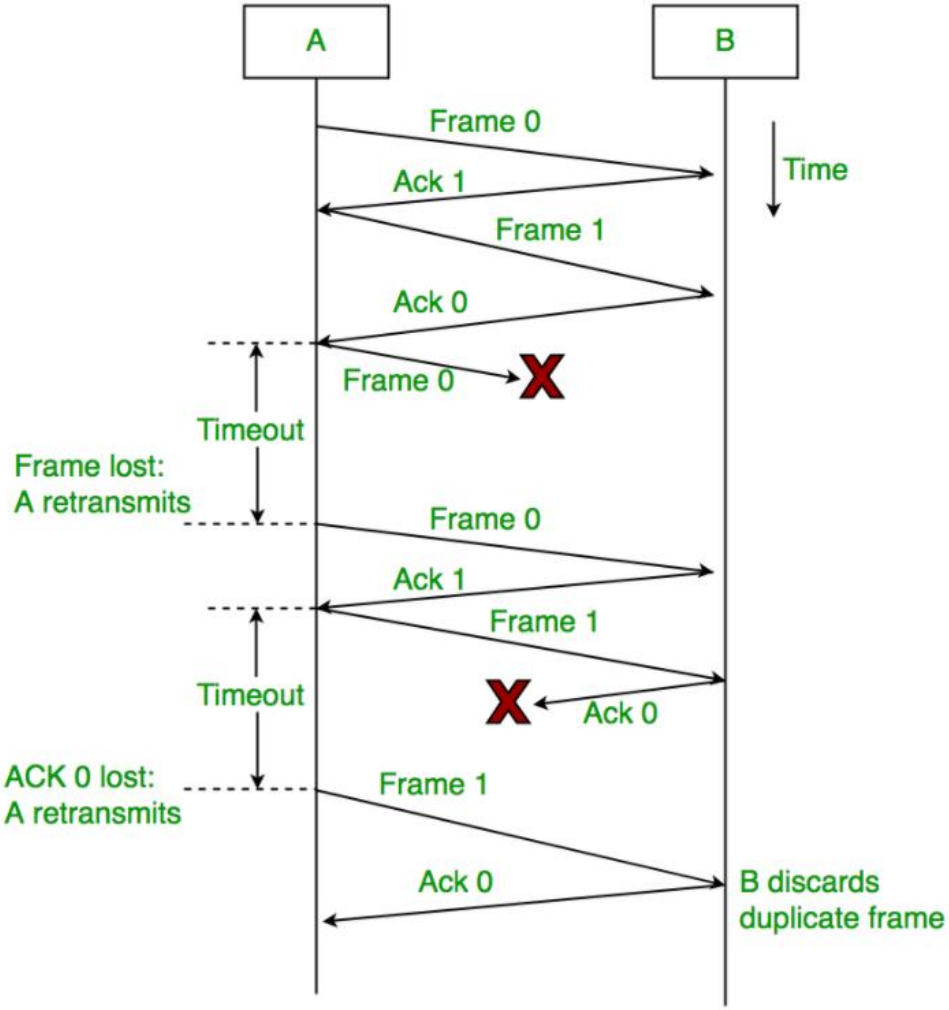
המרכז לחינוך סייבר
CYBER EDUCATION CENTER

TCP Header



המרכז לחינוך סייבר
CYBER EDUCATION CENTER

Stop and Wait



- מה החיסרון של אלגוריתם זה?

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

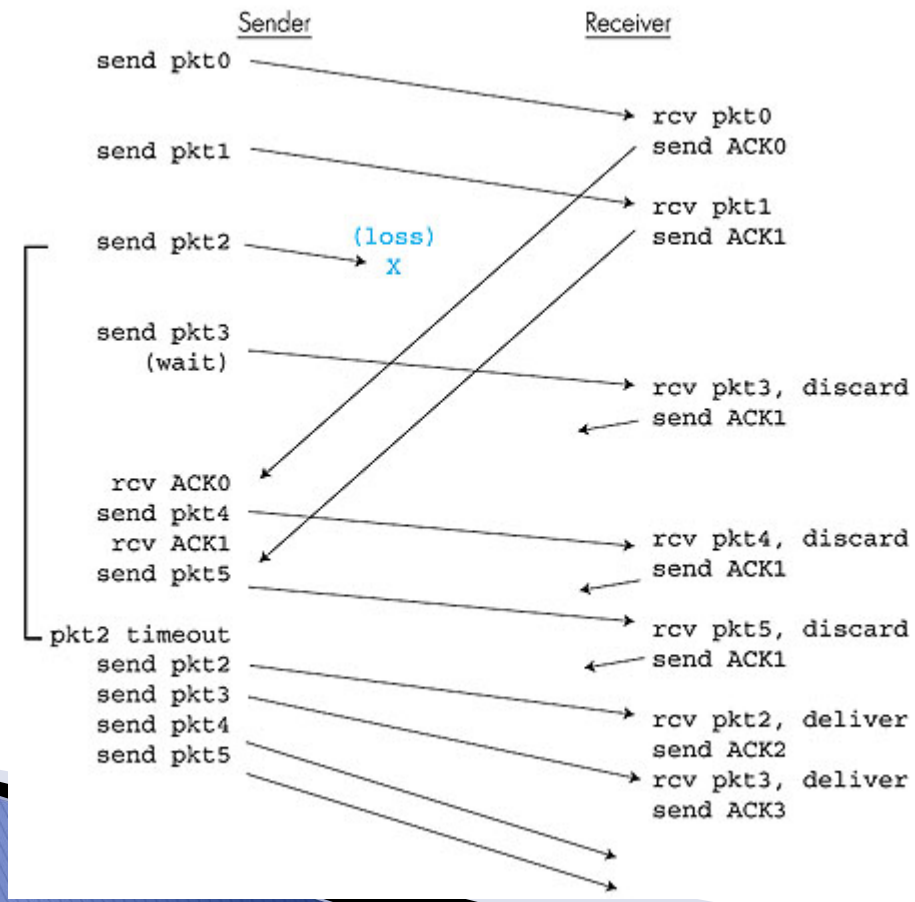
Stop and Wait

- שאלה:
  - ערוץ יכול להעביר 1Gb מידע לשניה. למידע לוקח 25msec להגיע מהשולח ליעד. השולח משתמש בפקטות בגודל 1024 בתים. מה קצב העברת המידע?
- תשובה:
  - השולח יצטרך לחכות לפחות 50msec עד שיגיע ACK על פקטה (זמן הגעת הפקטה + חזרת ה-ACK). לכן יישלחו 20 פקטות בשניה- 20KB בלבד על ערוץ של 1Gb.

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

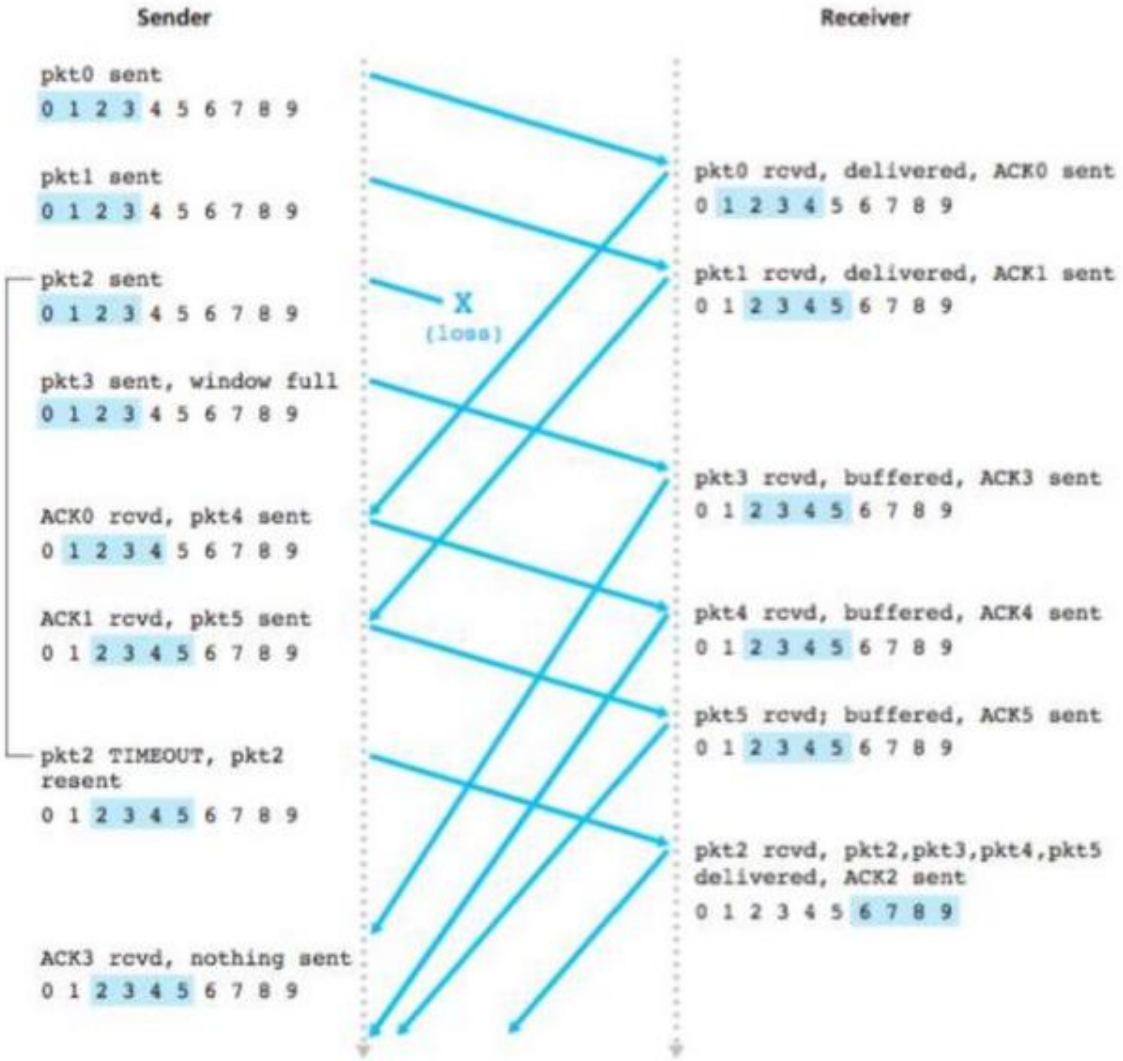
Go-Back-N

- השולח לא מחכה ל-ACK, ממשיך לשלוח פקטות ואוסף ACKים בדיעבד (צפו: Go-Back-N)



המרכז לחינוך סייבר
CYBER EDUCATION CENTER

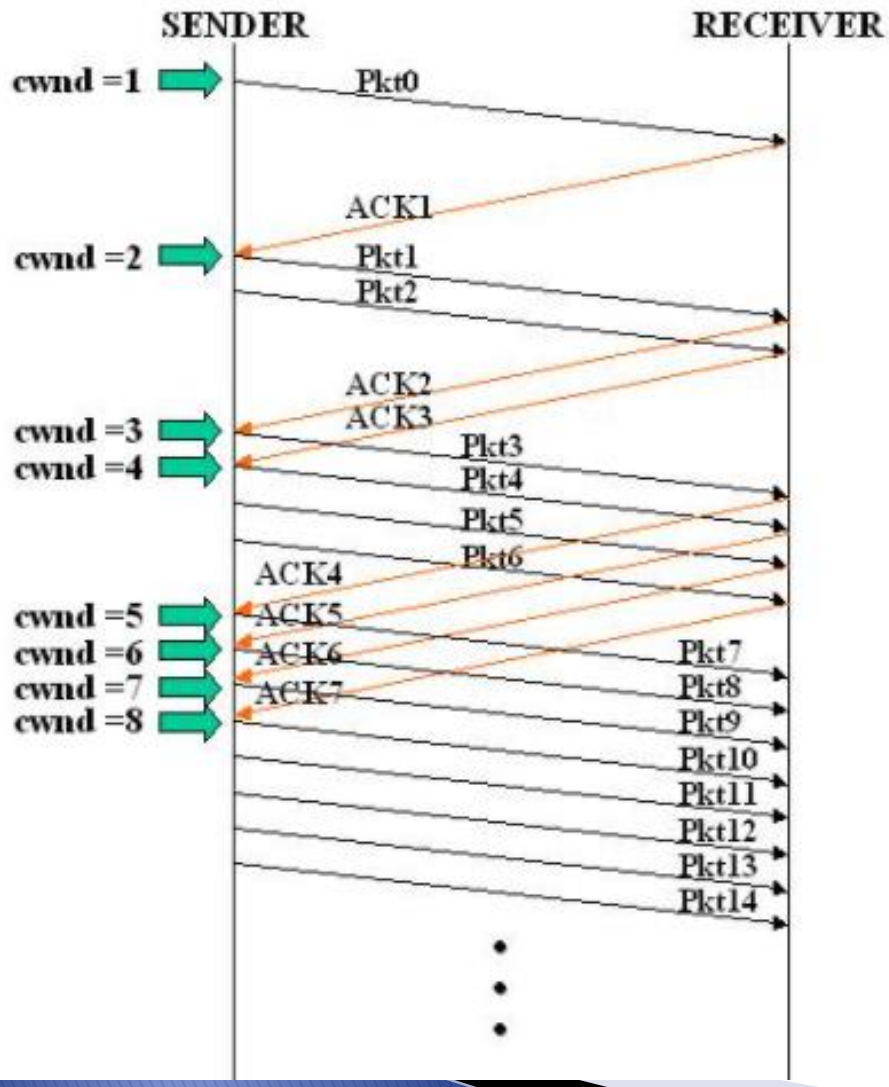
Selective Repeat



- האין Selective Repeat עדיפה תמיד על Commulative ACK?
- אנחנו "מפסידים" את ה-cumulative ack

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

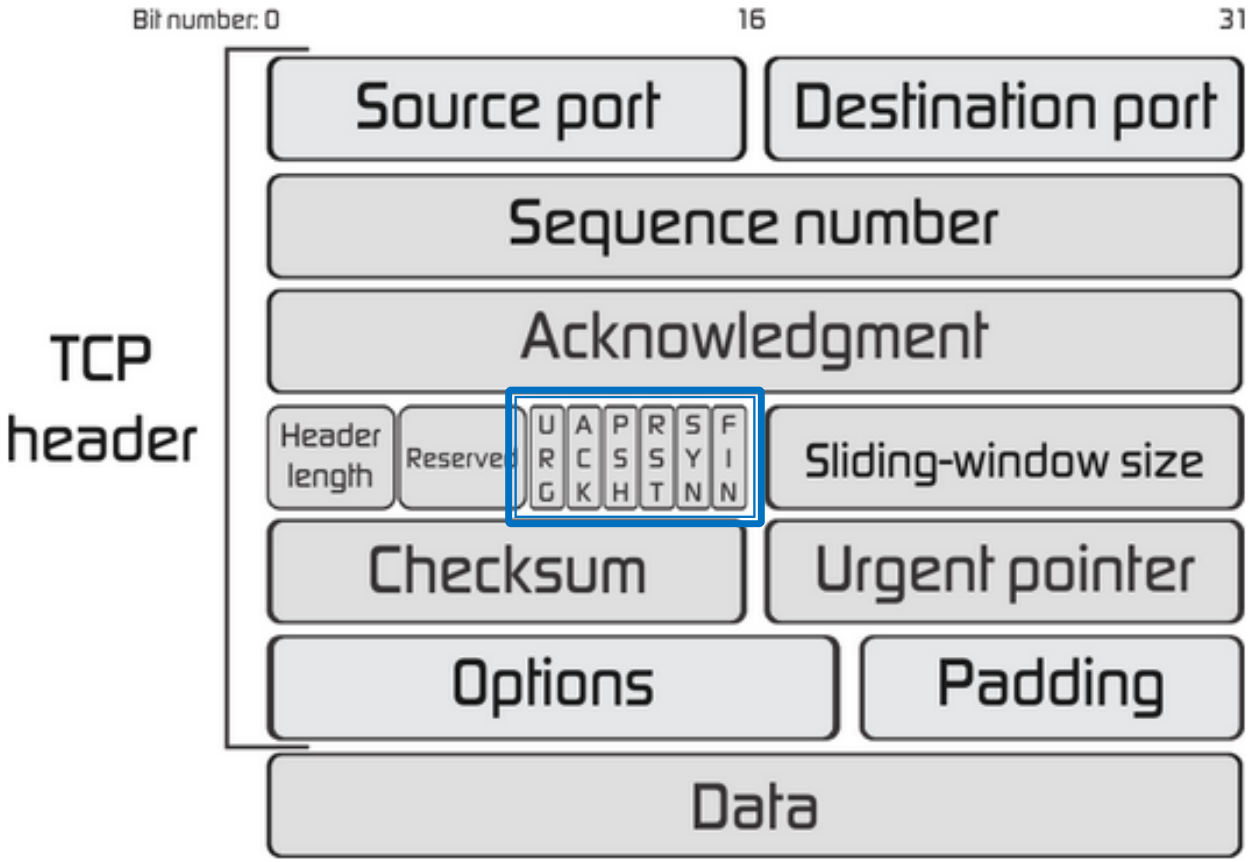
Congestion Control – Slow Start



- חפשו את cwnd ב-Wireshark

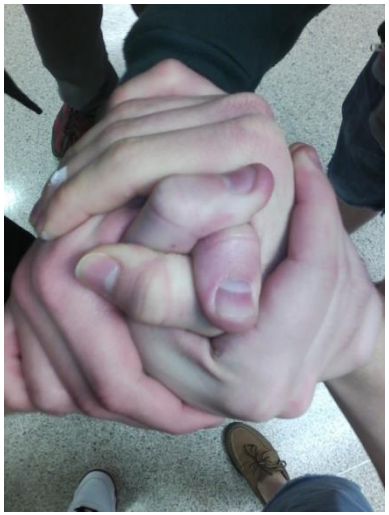
המרכז לחינוך סייבר
CYBER EDUCATION CENTER

TCP Header

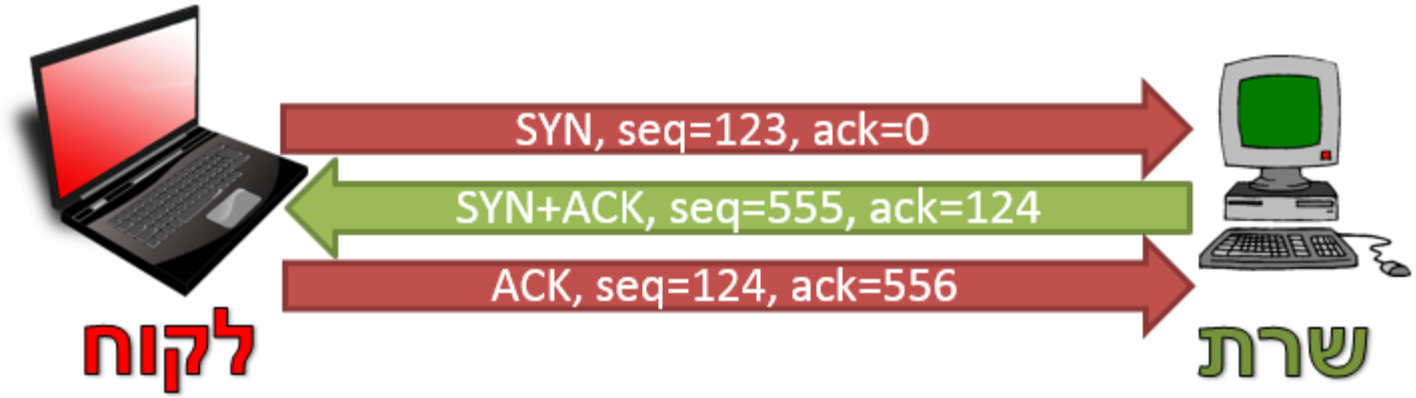


המרכז לחינוך סייבר
CYBER EDUCATION CENTER

TCP: Three Way Handshake



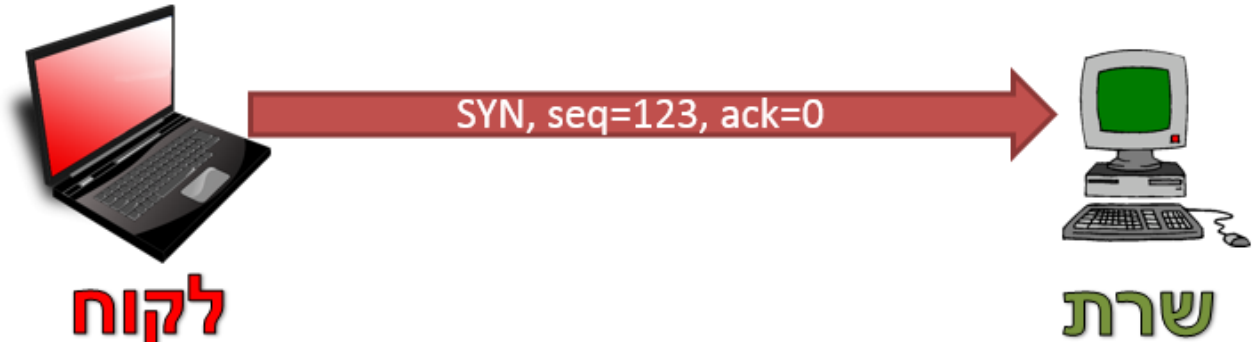
- מנגנוני ה-Sequential Number וה-ACK מחייב תהליך של הקמת קישור
  - שני הצדדים מודיעים שמוכנים לקלוט ולשדר
  - אם אחד הצדדים אינו מוכן, מנגנון ה-ACKים אינו יכול לעבוד
- התהליך נקרא Three Way Handshake ומורכב מ-3 פקטות- פירוט בהמשך:



המרכז לחינוך סייבר
CYBER EDUCATION CENTER

פקטה א'- SYN

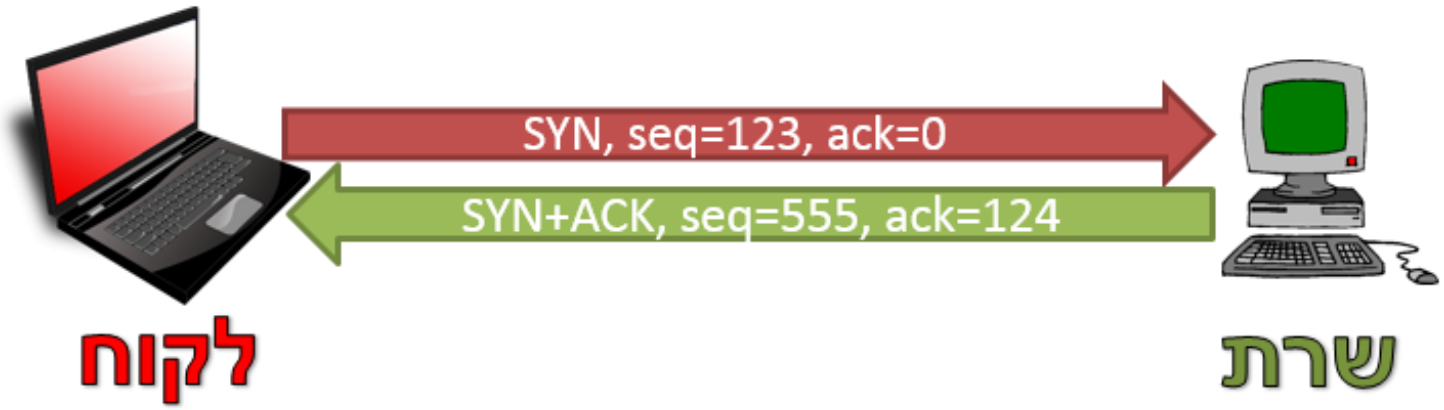
- משמעות: "אני רוצה להקים קישור"
- דגל ה-SYN דולק
- פקטת SYN לא נושאת מידע, אך סופרים אותה באורך 1
- בחירת Seq התחלתי אקראי
  - חישבו: מדוע לא להתחיל מ- Seq = 0?
  - תשובה: נניח שקישור מתנתק ונוצר חדש, חבילה מהקישור הקודם עלולה להגיע באיחור, עם Seq של הקישור הישן
- ערך ה-ACK תמיד יהיה 0



המרכז לחינוך סייבר
CYBER EDUCATION CENTER

פקטה ב'- SYN ACK

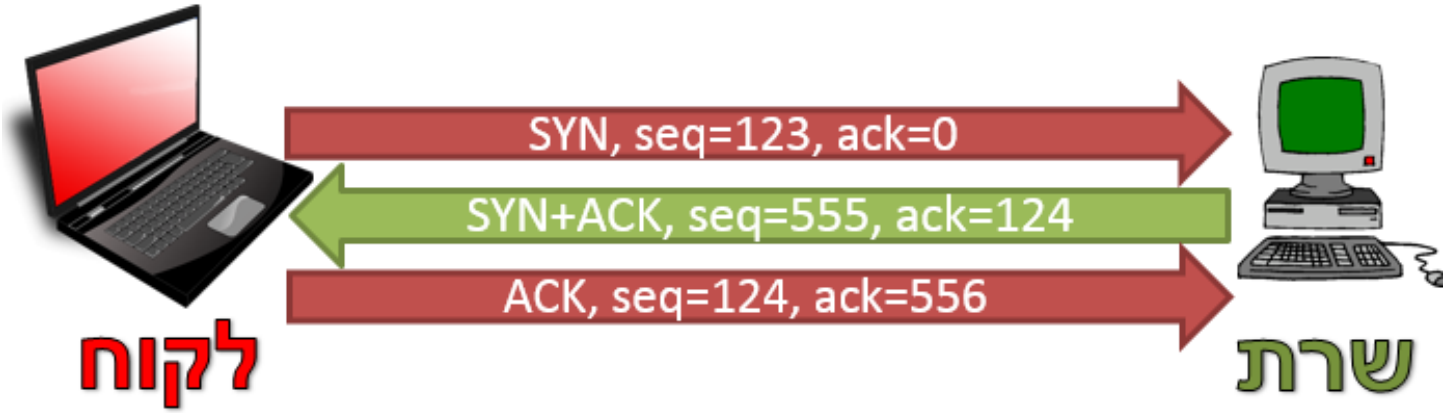
- משמעות: "אני מסכים להרים את הקישור"
- פקטה באורך בית אחד, דגלי ה-SYN וה-ACK דולקים
- בחירת Seq אקראי (לא קשור ל-Seq של פקטת ה-SYN)
- ערך ה-ACK שווה ל-Seq של פקטת ה-SYN + 1
  - היזכרו- 1 הוא אורך פקטת ה-SYN



המרכז לחינוך סייבר
CYBER EDUCATION CENTER

פקטה ג' - ACK

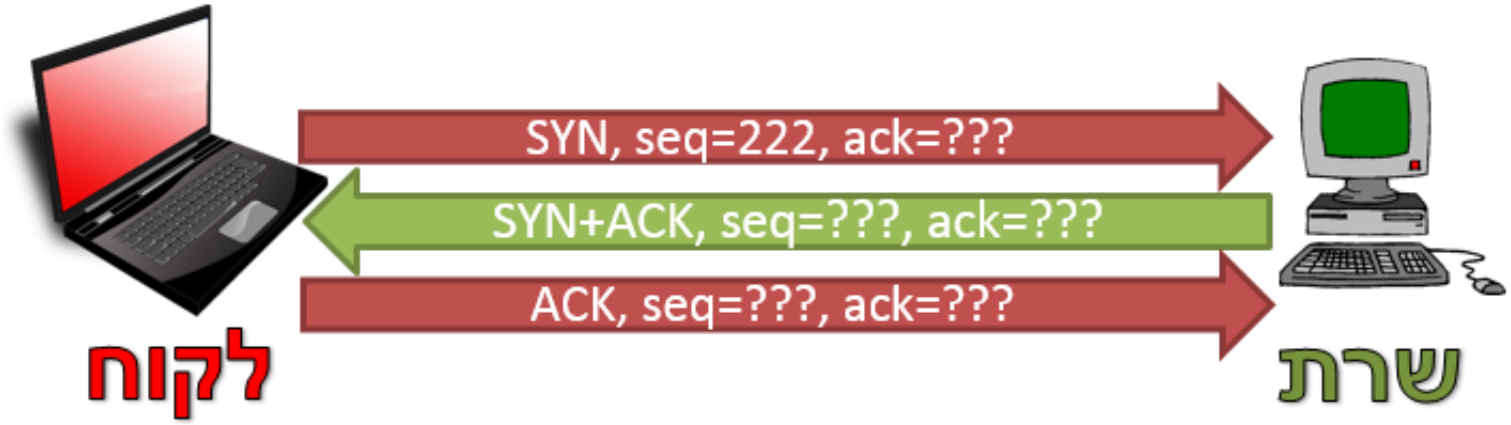
- משמעות: "קיבלתי את ה-SYN ACK ואנחנו מסונכרנים. אפשר להתחיל בתקשורת"
- דגל ה-ACK דולק (דגל ה-SYN כבוי)
- ערך ה-Seq הוא מספר הבית האחרון שנשלח
- ערך ה-ACK הוא ה-Seq של פקטת ה-SYN ACK ועוד 1



המרכז לחינוך סייבר
CYBER EDUCATION CENTER

סיכום – חישובי Seq, ACK

- חשבו את ערכי ה-Seq וה-ACK של תהליך הקמת הקשר הבא
  - הכניסו ערך אקראי במקום הנכון



המרכז לחינוך סייבר
CYBER EDUCATION CENTER

צפיה ב- Three Way Handshake

- בצעו את תרגיל מודרך 6.16, השוו את הערכים למה שציפיתם לקבל

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

Keep Alive

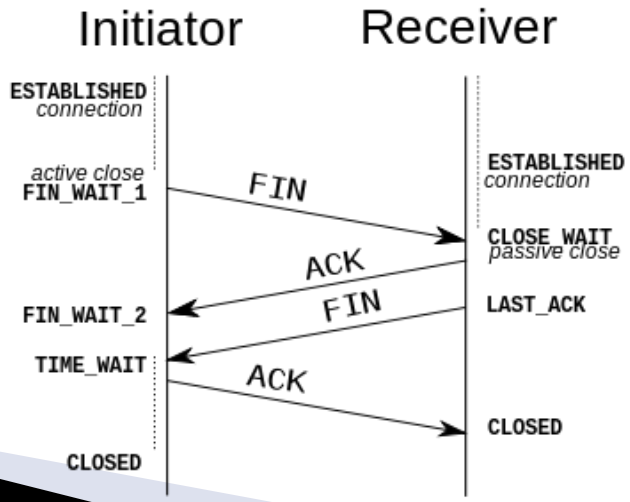
- חפשו Keep Alive ב-Wireshark. כיצד ניתן לזהות אותם? איך הצד המקבל יודע שהם Keep Alive?

No.	Time	Source	Destination	Protoc	Lengtl	Info
72398	305.601872	192.168.1.104	104.244.42.66	TCP	54	51044 → 443 [ACK] Seq=1825 Ack=895 Win=509 Len=0
72399	305.661710	104.244.42.66	192.168.1.104	TLSv1.2	175	Application Data
72400	305.711120	192.168.1.104	104.244.42.66	TCP	54	51044 → 443 [ACK] Seq=1825 Ack=1016 Win=509 Len=0
74353	350.675104	192.168.1.104	104.244.42.66	TCP	55	[TCP Keep-Alive] 51044 → 443 [ACK] Seq=1824 Ack=1016 Win=509 Len=1
74355	350.818828	104.244.42.66	192.168.1.104	TCP	66	[TCP Keep-Alive ACK] 443 → 51044 [ACK] Seq=1016 Ack=1825 Win=1701 Len=0 SLE=1824 S
74573	365.673006	192.168.1.104	104.244.42.66	TLSv1.2	153	Application Data
74574	365.673277	192.168.1.104	104.244.42.66	TLSv1.2	100	Application Data
74575	365.673386	192.168.1.104	104.244.42.66	TLSv1.2	213	Application Data
74577	365.738375	104.244.42.66	192.168.1.104	TCP	60	443 → 51044 [ACK] Seq=1016 Ack=1924 Win=1701 Len=0
74578	365.738376	104.244.42.66	192.168.1.104	TCP	60	443 → 51044 [ACK] Seq=1016 Ack=1970 Win=1701 Len=0
74579	365.768743	104.244.42.66	192.168.1.104	TCP	60	443 → 51044 [ACK] Seq=1016 Ack=2129 Win=1701 Len=0
74580	365.769660	104.244.42.66	192.168.1.104	TLSv1.2	100	Application Data
74582	365.811074	192.168.1.104	104.244.42.66	TCP	54	51044 → 443 [ACK] Seq=2129 Ack=1062 Win=509 Len=0
74584	365.872608	104.244.42.66	192.168.1.104	TLSv1.2	179	Application Data
74585	365.922480	192.168.1.104	104.244.42.66	TCP	54	51044 → 443 [ACK] Seq=2129 Ack=1187 Win=508 Len=0
75257	410.884981	192.168.1.104	104.244.42.66	TCP	55	[TCP Keep-Alive] 51044 → 443 [ACK] Seq=2128 Ack=1187 Win=508 Len=1
75262	410.985100	104.244.42.66	192.168.1.104	TCP	66	[TCP Keep-Alive ACK] 443 → 51044 [ACK] Seq=1187 Ack=2129 Win=1701 Len=0 SLE=2128 S

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

סגירת קישור TCP

- סגירת קישור TCP מתבצעת לפי הסדר הבא:
  - 1. צד א' (שמבקש לסגור) שולח פקטה עם דגל FIN
  - 2. צד ב' עונה בפקטה עם דגל ACK
  - 3. צד ב' שולח פקטה עם דגל FIN
  - 4. צד א' מאשר על ידי ACK



אם שלבים 3-4 לא מתבצעים הקישור נותר פתוח לשליחת מידע רק מצד אחד- Half Close ☺

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

Three Way Handshake מימוש

- בצעו את תרגיל 6.18 מודרך

Info	Length	Protocol	Destination	Source	Time	
Seq=0 Win=8192 Len=0 [SYN] 80 → 55555	54	TCP	142.250.186.132	192.168.1.221	2.189167	489
Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 [SYN, ACK] 55555 → 80	60	TCP	192.168.1.221	142.250.186.132	2.258783	503
Seq=1 Ack=1 Win=8192 Len=0 [ACK] 80 → 55555	54	TCP	142.250.186.132	192.168.1.221	2.313947	511

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

תרגיל: SYN-Flood

- כל בקשת SYN גורמת לשרת להקצות משאבים לסוקט חדש
- תוקף יכול לנצל זאת לטובת DoS
- הרעיון: "הצפה" בפקטות TCP Syn, בלי לשלוח TCP Ack

- https:/data.cyber.org.il/networks/SYN-Flood.pdf

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

סיכום- TCP

- מהם Sequence Numbers וכיצד הם נקבעים?
- למה משמשות פקטות ACK?
- תארו את שלבי ה-Three Way Handshake
- בכמה מעלה פקטת SYN את ה-Seq?
- בכמה מעלה פקטת ACK את ה-Seq?
- במהלך שיחה, צד א' שלח seq=1200, ack=580, data='Jon Snow'. מה ערך ה-ack שהצד השני אמור להחזיר לו?