# תרגיל בית 3

1. הנח שמבנה נתונים של TCP תופס KB32 בזיכרון של המחשב לכל חיבור, אורך הודעת SYN אחת של חיבור TCP היא 15 בתים וסה"כ יש במחשב GB2 זיכרון, מה צריך להיות קצב השידור המינימלי של תוקף על מנת שיצליח למלא את כל הזיכרון של המחשב המותקף תוך 30 שניות ?
2. קראי את הכתבה הזו.
א. צייני שני שימושים, מסחרי ופוליטי, שנעשו לכאורה ב-TCP Rst.
ב. כיצד הצליחו הבודקים של IEE לזהות, שחברת Comcast "שתלה" חבילות מזויפות בתעבורה שבין שני המשתמשים?
עבור הסעיפים הבאים, קראו כאן. ניתן לגלול ישירות לכותרת: What Is So Bad About Comcast's Actions?.
ג. כיצד מה שביצעה Comcast פוגע ב-end-to-end principle, ומה הבעיה בכך?
ד. איזו בעיה עלולה להיווצר מבחינת התחרותיות ההוגנת והנחיות הממונה על ההגבלים העסקיים?
ה. תני דוגמא לצעד דומה שבזק יכולה לנקוט כדי לפגוע באופן לא-הוגן במתחרות שלה.
* למותר לציין, שהשאלה לא מעלה טענה כלשהי על צעד שבזק נקטה בפועל ☺.

3. נתונים: SSThresh=N MSS, כאשר N הוא חזקה של 2.
נסמן ב-$\tau$ את הזמן מרגע המשלוח של החבילה הראשונה בחלון עד לקבלת החיוויים על כל החבילות בחלון. כדי לפשט, נניח ש-$\tau$ הוא קבוע, ולא תלוי במספר החבילות בחלון. כדי לפשט, נתעלם גם מזמני ההקמה והסגירה של הקשר.

א. כמה מידע נשלח בקשר TCP מתחילתו ועד להגעה ל-SSThresh (כולל הפעם שבה גודל החלון הוא SSThresh)?
ב. בקשר מסויים יש צורך בשליחת N-1 סגמנטים בלבד מ-A ל-B. כמה $\tau$ יקח לשלוח את המידע?
ג. בקשר מסויים, מצליחים לשלוח מידע עד לנקודה שבה גודל החלון הוא 2N, בלי לאבד אף חבילה ואף Ack. כמה סגמנטים נשלחו סה"כ (כולל המשלוח של 2N סגמנטים בחלון יחיד)? כמה $\tau$ יקח לשלוח את המידע?
ד. מוצע להגדיל את החלון ההתחלתי מ-MSS יחיד ל-N/4 MSS. פי כמה קטן הזמן הנדרש לשליחת המידע בקשר של סעיף ב'? פי כמה קטן הזמן הנדרש לשליחת המידע בקשר של סעיף ג'?
ה. לאור תשובתך לסעיף הקודם – עבור איזה סוג של קשרים ויישומים כדאי במיוחד "להסתכן" ולהשתמש בחלון בגודל התחלתי > 1? עבור איזה סוג של קשרים אין הרבה תועלת בנטילת סיכון כזה?

4. לקוח מתחבר לשרת בפרוטוקול telnet, וכתוצאה מכך, בכל פעם שהוא מקליד תו אחד במקלדת, TCP שולח מהלקוח אל השרת סגמנט ובו בית מידע יחיד (התו שהוקלד), ומקבל בתגובה סגמנט, וגם בו תו מידע יחיד.
נתון שלשני הסגמנטים הנ"ל יש את גודל הרישא המקסימלי של TCP. כמו כן, נניח שגודל הרישא של שכבת הרשת שלהם הוא 20 בתים; ושגודל הרישא של שכבת הקו שלהם הוא 20 בתים.
א. מהי התקורה של התחיליות – כלומר, היחס בין הגודל הכולל של החבילה, כולל כל התחיליות, לבין גודל המידע?
ב. הסבר, כיצד שימוש באלגוריתמים של נייגל ושל קלארק יכול להקטין את התקורה שחישבנו בסעיף א'.
ג. מהי הבעיה שנוצרת בשימוש באלגוריתמים הנ"ל במקרה של יישום אינטראקטיבי בין שתי תחנות עם RTT מאוד גדול?

5. הקלד את שורת הכתובת:
https://www.youtube.com/watch?v=IU54pW8KiIY
ויירט באמצעות Wireshark את חבילות ה-TCP שנשלחו לשם כך, כפי שלמדנו במעבדה הקודמת.
הדבק צילום מסך של Wireshark.
הערה: אף שה-# Initial Seq מוגרל, כפי שנלמד בהרצאה, Wireshark מציג את הערך ההתחלתי שהוגרל כ"אפס", כדי להקל על ספירת הבתים שעברו מאז תחילת הקשר.
א. תאר בקצרה את "לחיצת הידיים המשולשת" שהתבצעה ביצירת הקשר של TCP.

ב. האם המחשב שלך תומך ב-Sack? האם השרת שניגשת אליו תומך ב-Sack?
ג. האם המחשב שלך הציע להשתמש ב-Window Scale? מהו גודל חלון הקבלה המקסימלי האפשרי במחשב שלך? מהו גודל חלון הקבלה המקסימלי אצל השרת, שבו מאוחסנת הכתבה?
ד. התחל ליירט חבילות תוך כדי הרצה של ה"סרטון" ב-youtube. ואז עצור את הסרטון (Pause). התבונן בחבילות ב-Wireshark, ועצור את היירוט לאחר שזיהית, שהדפדפן שלך סגר את קשר ה-TCP עם Youtube. הדבק צילום מסך של הסגירה. תאר בקצרה את תהליך הסגירה: מי יזם את הסגירה, האם הצד השני השאיר את הקשר "חצי פתוח" או סגר גם הוא, איזה דגל הודלק כדי להודיע על בקשת הסגירה וכו'.
הערה: כרגיל בשאלות WIRESHARK, התשובה עלולה להשתנות ממחשב למחשב, או אף מדפדפן לדפדפן.

6. בכדי להעביר מידע רגיש ברשת נהוג להצפין אותו. האם לדעתכם ניתן להצפין את ה header בחבילות המועברות ברשת? נמקו.

7. קרא את תחילת המאמר על DCTCP, עד סוף החלק 2.1.
א. ציין שלושה יישומים שבהם תומכי מרכזי נתונים מודרניים, ואת דרישות התעבורה של כל אחד מהיישומים האלה מבחינת השהיה ותפוקה.
ב. ציין 3 הבדלים בין רשתות במרכזי נתונים לבין רשתות לטווחים גדולים (Wide Area Networks).
ג. תאר בקצרה כיצד מטפל מרכז נתונים בשאילתה למנוע חיפוש כגון Google או Bing. מה קורה כאשר אחד השרתים לא עונה בזמן על השאילתה? מדוע לא ניתן לעכב מעט את התשובה לשאילתה?
ד. באיזו שיטה השתמשה Facebook כדי להתגבר על הקושי הרב לעמוד ב"דדליינים" קפדניים בקשרי TCP?
הערה:
SLA = Service Level Agreement הוא הסכם איכות שירות, המגדיר מחוייבות להשהיה ולתפוקה ברשת. הסכם כזה נחתם בין ISPs (למשל, בזק, AT&T) לבין חברות וארגונים (למשל, אב"ג, בנק לאומי, וגם – מה שרלבנטי למאמר – חברות ששוכרות את השימוש במרכז המידע).
Incast היא "פקק התנועה" שנוצר כאשר הרבה מאוד תעבורה מופנית באופן פתאומי ליעד אחד – למשל צובר (aggregator) שמאחה את תוצאות החיפוש בשרתים אחרים לכדי תשובה אחת ללקוח.

**שאלה 8**
1. קרא על חוק אמדל, והסבר אותו בקצרה **במילים שלך, ובעברית.**

משתמש מוריד קובץ משרת Web מרוחק. הקובץ נכנס בחבילה אחת גדולה.
בין המשתמש לבין השרת יש נתב יחיד.
למשתמש יש כבר קשר TCP פתוח עם השרת.
**נתוני הבסיס הם:**

- גודל הקובץ:99kb
- גודל הרישא (header) של כל חבילה:1kb .
- בחבילה שאין בה נתונים (קובץ) יש רק רישא. בחבילה שנושאת את הקובץ, יש הקובץ + רישא.
- זמן העיבוד בנתב:1ms
- זמן עיבוד הבקשות בשרת:1ms
- זמני ההמתנה בתורים זניחים.
- המרחק מהלקוח לשרת: 10,000 ק"מ.
- רוחבי הפס: מהלקוח לנתב – 1Gbps. מהנתב לשרת – 1Mbps.

נציין ב-$D$ את ההמתנה הכוללת מהרגע שבו הלקוח מתחיל לשלוח בקשת HTTP, ועד שהחבילה עם הקובץ מגיעה אליו במלואה.
בחישובים ניתן להזניח כל גורם שתורם פחות מ-1.5% לתוצאה הסופית.
כדי להקל, נניח גם ש:k=10^3, M=10^6, G=10^9 .

2.
א. חשבי את $D$.

ב. הנתב משמש מעתה גם כשרת עזר (*proxy web server*), שמשתמש ב-*Conditional Get*. נתון כי הקובץ המעודכן ביותר כבר נמצא בשרת העזר (אך עליו לבדוק זאת, כמובן). מצא את *D* כעת.
ג. מהו החיסכון היחסי בהשהיה שנגרם בזכות השימוש ב-*cond. Get*?

בכל אחד מהסעיפים הבאים נשנה רק פרמטר אחד. יתר הפרמטרים הם כמו בנתוני הבסיס שלמעלה.

3. גודל הקובץ הוא כעת 199kb. חזור על 1.

4. גודל הקובץ הוחזר להיות 99kb, אך גודל הרישא עלה ל-10kb.

5. זמן העיבוד בנתב עלה ל-100 ms .

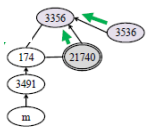
6. המרחק מהלקוח לשרת עלה ל-20,000 ק"מ.

7. רוחב הפס מהנתב לשרת שודרג ל-10 Mbps.

## תרגיל בית 4

1. קרא את הכתבה הזו, שדנו בה גם בתרגיל הבית הקודם.
א. בכוכבית (*) בתחתית הכתבה מצוין תרחיש, שבו עשויות להיווצר בקשר בין שני משתמשים, A ו-B, חבילות, שלא נשלחו במקור ע"י A אבל הגיעו ל-B עם הכתובת של A ככתובת השולח. מהו התרחיש הזה?
ב. הסבירי בקצרה כיצד ISP שהיא גם ספקית טלפוניה קווית או טלויזיה בכבלים יכולה לנצל לרעה את השדות DSCP ו-ECN ב-IP Header, כדי לפגוע במתחרים שלה.

2. קראו על פגמי האבטחה באינטרנט עד סוף פרק 3, וכן את פרק 6.1.1; וצפו במצגת הזו עד דקה 18:00. ענו בקצרה.
א. כיצד פעלו המתקפות מסוג prefix hijack, שאירעו בשנים האחרונות? כיצד ניצלו התוקפים את הכלל Longest Prefix Match?
ב. כיצד origin authentication מונע מתקפות מסוג prefix hijack?
ג. איזו מתקפה origin authentication לא יכול למנוע? תאר בקצרה את המתקפה.
ד. כיצד BGPSEC מונע את המתקפה שתיארת בסעיף הקודם?
ה. כיצד ASes מחליטות על מסלול הניתוב המועדף ב-BGP רגיל? ציין את סדר העדיפויות המדוייק.
ו. כיצד ASes מחליטות על מסלול הניתוב המועדף ב-BGPSEC במקרה הנפוץ ביותר ("מקרה 3" במאמר)?

| | |
|---|---|
|  | ז. ברשת שבשרטוט משמאל, איזה מסלולים תפרסם AS 174 לכל אחד מהשכנים שלה?<br>שים לב לכך שקישורים ללא חץ מסמנים קשר בין רשתות עמיתות, כלומר, רשתות שאין ביניהן קשר של ספק – לקוח; וקישורים עם חץ מסמנים קשר בין ספק ללקוח. כמו כן, שים לב הן לאופן הבחירה של מסלולים (ראה הסעיף הקודם), והן לאופן הבחירה של איזה מסלולים לפרסם. |

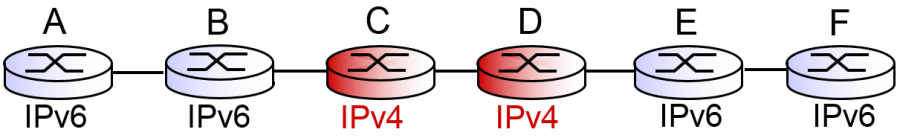
ח. ציין שני חסרונות של פרישה חלקית של BGPSEC באינטרנט, כאשר חלק / כל ה-ASes משתמשות במודל האבטחה 2 או 3 המתואר במאמר.
ט. נניח כי אב"ג **לא** משתמשת ב-BGPSEC; ואילו הספק של אב"ג החליט לשפר את אבטחת הרשת שלו, ולשם כך התחיל להשתמש ב-BGPSEC. שרטט ותאר בקצרה תרחיש שבו, דווקא בעקבות העובדה שהספק התחיל להשתמש ב-BGPSEC, אב"ג חשופה לאיום חדש, שלא היתה חשופה לו קודם.

3. קראי את המאמר על הרשת הפנימית של גוגל בכתובת:
http://cseweb.ucsd.edu/~vahdat/papers/b4-sigcomm13.pdf

הערה: הכוונה ב- over-provisioning היא ליתרות של הרשת – למשל, אם משתמשים בכבל של 30 Gbps לצורך העברת תעבורה שברוב הזמן היא רק 10 Gbps, יש over-provisioning של פי 3.
א. מדוע לרוב משתמשים ב-WAN ב-over-provisioning גבוה?
ב. מהו החיסרון של שימוש ב-over-provisioning גבוה?
ג. ציין 4 מאפיינים יחודיים לרשת הפנימית של גוגל, יחסית ל-WAN אחרות.
ד. ציין שני יתרונות של Software Defined Networks.

**.4**

א. נתב מטפל בחבילות שממתינות לצאת מפורט מוצא מסויים בשיטת Round Robin בין כל הזרמים (flows), שחבילה שלהם צריכה לצאת מהמוצא הנ"ל. ציין והסבר בקצרה שני חסרונות של שיטה זו.
ב. ציין והסבר בקצרה שיטה מעשית שנלמדה בהרצאה, ופותרת את החסרונות של Round Robin.
ג. ברשת שבשרטוט, כיצד ניתן לשלוח חבילת IPv6 מ-A אל F, אף שהנתבים C,D בדרך לא תומכים ב-IPv6?




**<u>שאלה 5</u>**

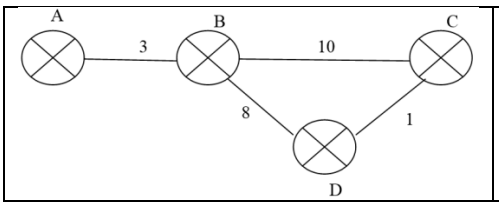
נסתכל על טופלוגיית רשת כללית כלשהיא (כלומר, אי אפשר להניח דבר על מבנה הרשת). בהינתן גרסא סינכרונית של אלגוריתם distance-vector (DV) כך שבכל איטרציה כל ראוטר (node) ברשת מקבל את ה DV של כל השכנים שלו ושולח את ה DV שלו אל כל השכנים שלו.
בהנחה שכל ראוטר מתחיל את ריצת האלגוריתם כשהוא יודע אך ורק את המרחקים לראוטרים השכנים שלו, מה מספר האיטרציות המירבי שייקח לאלגוריתם להתכנס? הסבר בקצרה את תשובתך.

**<u>שאלה 6</u>**

אחת הבעיות העכשוויות הקשות ברשתות תקשורת היא קיומם של "חורים שחורים" ברשת – קרי, מקומות, שבהם חבילות "הולכות לאיבוד". זאת, כתוצאה מכשלים בחומרה או מקינפוג שגוי של נתבים. הבעיה היא, שכאשר חבילה לא מגיעה ליעדה, קשה לנו מאוד לדעת איזה נתב בדרך הפיל את החבילה. כמו כן, התנהגות הנתב הפגום היא לאו דווקא זהה לכל החבילות, כלומר: נתב פגום עלול לזרוק את כל החבילות של חלק מהזרימות העוברות דרכו, אך להעביר באופן תקין זרימות אחרות.
נניח לצורך השאלה, שכל הנתבים התקינים מטפלים כראוי בחבילות ICMP, ולא זורקים אותן; וכן שהכשלים האפשריים הם בנתבים בלבד, ולא בקישורים ביניהם.
(5) א. חושדים שאחד הנתבים במסלול מ-S ל-T זורק את כל החבילות שמנותבות במסלול זה. הצע דרך, המבוססת על traceroute, לקבלת הערכה של מקומו של הנתב הפגום.
(8) ב. הצע והסבר בקצרה דרך שלא תשתמש בפונקציה הקיימת traceroute, אבל תשתמש בשיטה דומה לקבלת הערכה על מקומו של הנתב הפגום, תוך חיסכון מירבי במספר החבילות שנשלחות.
(3) ג. מדוע בשיטות שבסעיף א' וב' ניתן לקבל רק הערכה על מקומו של הנתב הפגום, אך לא את כתובתו המדויקת?

**<u>שאלה 7</u>**

מלאי את הטבלה שלמטה עבור הרצה של אלג' מסוג Link State ברשת שבתמונה עם צומת A כמקור.



| N’ | A | B | C | D |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |