

פתרון שאלות נבחרות במבחן
בקורס תקשורת דיגיטלית בעידן המודרני (67594) – מועד א'

המרצה: דני ביקסון

תאריך הבחינה: 10.2.05

משך הבחינה: שעתיים

חומר עזר מותר בשימוש: אין

הוראות: יש לענות על **שלוש שאלות** מתוך ארבע. במקרה שעניתם על יותר משלוש שאלות שלוש השאלות הראשונות יבדקו. משקל כל שאלה 33 נקודות.

הערה כללית: ישנה אמרת ידועה האומרת "כל המוסיף גורע". תלמידים אשר ענו תשובה נכונה, אולם הוסיפו לה הסברים לא נכונים ולא קשורים, גרמו לי לחשוב שאינם מבינים את החומר ולכן איבדו חלק מהנקודות. למשל, מי שבסעיף 1' הסביר בנוסף ל- TCP flow control גם על ATM, frame relay, quality of service וכו' וכו' גורם לי לחשוב שיש לו זכרון צילומי והוא מצטט את המחברת בלי להבין מה קשור ומה לא קשור. גם מי שעה מאוד בקצרה ולעניין קיבל את מלוא הנקודות. דוגמא נוספת: בשאלה 4' מישהו ענה שבשיעור חזרה למדנו על DNS ולכן אם היה DNS בשאלה אז היינו עושים כך וכך...

1. א. (5 נק') הסבר מהו ההבדל בין Flow Control ל- Congestion Control.
פתרון: flow control מונע משולח מהיר להציף מקבל איטי מתבצע end-to-end ברמת ה- congestion control, transport מונע הווצרות עומס (congestion) לכל אורך הרשת ויכול להתבצע בשכבות ה- transport וה- network.
פרס התשובה המקורית: למנוע מ-A להאביס את B יותר ממה שיכול לאכול. (קיבל את הניקוד).

ב. (15 נק') בחר את אחד המנגנונים TCP Flow Control או TCP Congestion Control ותאר בפירוט כיצד הם מיושמים. (כולל שדות ב- TCP Header ואילו חישובים מתבצעים על ידי הצדדים המתקשרים).
פתרון: הרוב ענו נכון. מי שלא ציין את השימוש בשדות ack, seq num, receiver win size, num ב- TCP header איבד מספר נקודות. ראה פתרון בפרקים 3.5.6, 3.7 ברוס.
פרס התשובה המקורית: א. שימוש ב- RM cells ב- TCP, EFCI, EBCI, bit DE ועוד.
 ב. שימוש ב- ACK, SYN ו- timers כדי להגביל את קצב השידור.

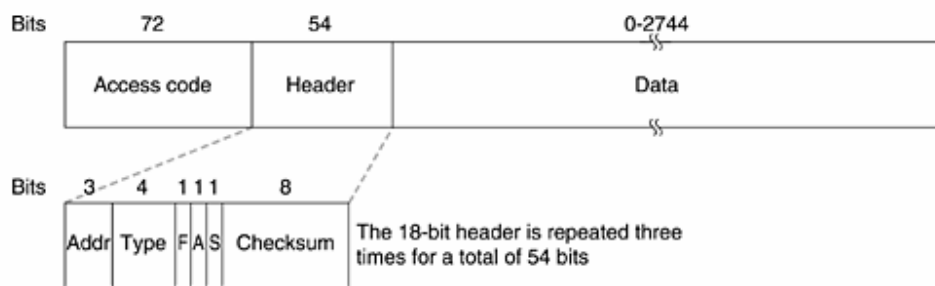
ג. (7 נק') מהם החסרונות של הגבלת קצב השידור (Additive increase multiplicative) decrease) כאשר ישנו איבוד הודעות (אך אין עומס).
פתרון: מכיוון שלא ניתן להבחין בין הודעה שלא הגיעה עקב עומס לבין הודעה שלא הגיעה עקב איבוד הודעות בקו רועש, בשני המקרים יופעל TCP slow start. במקרה של עומס, זהו פתרון טוב כאשר כל התחנות העדות לעמוס מייד מפחיתות את קצב השידור בצורה דרסטית ובכך גורמות ל- TCP להיות fair. אולם, במקרה של איבוד הודעה, אין טעם להוריד את קצב השידור בצורה כה דרסטית כי בכך אנו מפחיתים מאוד את נצילות הקו, באופן אופטימלי עדיף היה דווקא להעלות את קצב השידור המקרה של איבוד הודעות (כאשר אין עומס) כדי להתמודד עם הצורך בשידורים חוזרים.

טעויות נפוצות: אין איבוד הודעות בקוי האינטרנט הקיימים. (לא נכון). במיוחד שישנם קוים לווייניים ו-wireless.

ד. (6 נק') הצע דרך לפתור את הבעיה בסעיף ג'.
פתרון: פתרון מקובל הינו בשיטת Reno כאשר מפחיתים את גודל חלון העומס להיות $w=w/2$. במקום $w=1$. כל הפתרונות שהיצעו לצמצם את ההגבלה על השידור בשיטה כלשהיא התקבלו. כל הפתרונות המחייבים תמיכה לאורך הרשת קיבלו ניקוד חלקי בלבד.
פרס התשובה המקורית: נוסף לשדות ה-RM ב-TCP header אינדיקציות על עומס.

2. נתון מבנה של Header של חבילה בפרוטוקול Bluetooth.

Figure 4-38. A typical Bluetooth data frame.



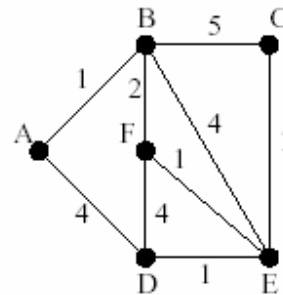
- א. (5 נק') הסבר לאיזה צרכים תוכנן הפרוטוקול.
פתרון: הפרוטוקול תוכנן לצורך תקשורת wireless זולה לטווחים של עד עשרה מטר. במקור ע"י חברת Ericsson עבור תקשורת אלחוטית של PDAs עם מחשב.
פרס התשובה המקורית: א. פרוטוקול להנחיית טורפדו.
 ב. פרוטוקול שנועד להשגת קבצי שידור הרבה יותר מהירים ונועד לכסות על הטעויות בבניית פרוטוקול IP.
 ג. (3 נק') מדוע ישנם רק שלושה ביטים בשדה הכתובת?
פתרון: מכיוון שישנו master ועד שבעה slaves שיכולים להיות פעילים בשידור, לכן מספיקות שמונה כתובות.
פרס התשובה המקורית: כי יש עד שמונה כתובות רשת.
 ד. (5 נק') למה משמש ביט ה-Flow? מה המקבילה שלו ב-TCP ומה ההבדל?
פתרון: ביט זה מציין כי ה-slave buffer הינו מלא ולכן על ה-master להפחית את קצב השידור. הדבר דומה ל-TCP flow control רק ההבדל שפה יש שימוש בביט אחד בלבד ואילו ב-TCP flow control ישנו גודל חלון המקבל המועבר בכל TCP header.
פרס התשובה המקורית: מנגנון עבור IP fragmentation.
 ד. (5 נק') מדוע אין sequence numbers כמו ב-TCP עבור כל חבילה ועבור ה-ACK?
פתרון: מכיוון שזהו פרוטוקול מסוג 1-bit-stop-&-wait, אסור להמשיך בשידור לפני שמתקבל ACK על החבילה האחרונה, ולכן מספיק ביט אחד.
 ה. (4 נק') הסבר מדוע משדרים את ה-Header שלוש פעמים בזה אחר זה בכל חבילה.
פתרון: מכיוון שזוהי תקשורת אלחוטית החשופה להפרעות משדרים שלוש פעמים את ה-header ומקבלים את דעת הרוב.
 ו. (4 נק') מהו שדה ה-checksum ולאיזה צורך הוא משמש?
פתרון: זהו שדה המשמש לבדיקת שגיאות. השולח מחשב את ה-checksum ומצרפו לחבילה, המקבל חוזר על החישוב ומשווה את התוצאה.
 ז. (7 נק') ציין מהם ההבדלים העיקריים בין פרוטוקול Bluetooth ל-Ethernet.

פתרון: wireless לעומת wired. מדיה לא אמינה לעומת מדיה אמינה. טווח שידור עשרה מטר לעומת טווח של מאות מטר. שמונה תחנות מקסימום לעומת מאות תחנות. כתובת לוגית לעומת כתובות MAC פיזיות. שידור בעזרת time slots לעומת שידור בשיטת CSMA/CD. מחייב שעון אצל ה-master כאשר אין צורך בשעון ב- ethernet. קצבי שידור נמוכים יחסית לעומת קבצי שידור עד Gigabytes. פרוטוקול משתמש ב- ACK לעומת פרוטוקול הבונה על זיהוי התנגשות לבדיקה האם חבילה הגיעה (ללא ACK). מאפיינים של שכבת ה- transport שהינם flow control ו- ACK לעומת מאפיינים של שכבת ה- data link.

פרס התשובה המקורית: ישן מול חדש, יקר מול זול.

3. א. (5 נק') הסבר מהו ההבדל בין אלגוריתמי ניתוב Link state ל- Distance vector. **פתרון:** שימוש במידע גלובלי ב- LS שכולל את כל ה- links לעומת שימוש במידע חלקי ב- DV שכולל רק את הצלעות לשכנים. ב- LS בד"כ כולם מספרים לכולם על כל הצלעות בעזרת flooding לעומת תקשורת רק בין שכנים ב- DV. ב- LS כל קודקוד מכיר את כל הגרף ומריץ עליו מקומית את אלג' הניתוב בשעה שב- DV האלגוריתם מתבצע בצורה מבוזרת בין שכנים המעבירים רק מרחקים אל היעדים השונים. ב- LS לאחר הרצת הניתוב כל קודקוד יודע את כל המסלולים המלאים לכל הקודקודים האחרים ואילו ב- DV כל קודקוד יודע רק את שכן היציאה ואת אורך המסלול והניתוב נעשה בצורת next hop routing. ב- DV משתמשים בד"כ ב- dijkstra (OSPF) ואילו ב- DV (Bellman Ford) RIP. ב- LS במקרה של שינוי בצלע יהיה עלינו להפיץ את המידע לכולם ואילו ב- DV שינוי בצלע יגרור עדכונים רק של המסלולים הרלוונטיים.

ב. (20 נק') נתונה הרשת הבאה:



הרץ את אלגוריתם Dijkstra למציאת מסלולי ניתוב הקצרים ביותר, כאשר מתחילים מקודקוד A. יש לפרט את תוצאות החישוב.

פתרון: הרוב ענו נכון. ראה רוס 4.2.1 לדוגמא.

ג. (3 נק') מדוע אי אפשר להשתמש באלגוריתם Dijkstra לניתוב גלובלי באינטרנט?

פתרון: כמות המחשבים באינטרנט כיום הינו מאות מליונים ולכן לא ניתן לשמור ולעבד מידע זה בצורה יעילה בקודקוד אחד, זמן הריצה לא יהיה ישים, עדכונים של צלעות יגרור תעבורה אקספוננציאלית לכולם. בנוסף הרשת הינה דינמית, אין ישות מרכזית היודעת את מבנה הרשת השלם. עומס על מסלולים הינו דינמי ומשתנה כל הזמן. בנוסף ישנם שיקולי ניתוב נוספים כגון מעברים בין מדינות וארגונים, שיקולים כלכליים ואחרים שלא באים לידי ביטוי באלגוריתם.

ד. (5 נק') הצע פיתרון לבעיה זו.

פתרון: כל פיתרון שכלל חלוקה היררכי לקבוצות ניתוב, כאשר בצורה הפנימית יכול להתבצע ניתוב אחד ובין הקבוצות יכול להתבצע ניתוב אחר התקבל. רבים טעו וכתבו כי ניתן להשתמש בפרוטוקול DV (ללא חלוקה היררכית) ובכך יפתרו הבעיות. אולם פתרון זה הינו שגוי מכיוון

שלא ניתן לשלוח הודעות ניתוב כאשר ישנם מאות מליוני יעדים לניתוב. בנוסף צריך פתרון שניתן יהי לקבוע בו מסלולי ניתוב סטטיים למשל משיקולים כלכליים ארגוניים או בין מדינותיים.

4. א. (3 נק') הסבר למה מיועד ping utility , באיזה פרוטוקול הוא משתמש ובאיזה רמה במודל השכבות.

פתרון: זהו utility עבור debugging המאפשר לזהות האם מחשב או router הינו חי ומחובר לרשת וכן למדוד את זמן התגובה שלו. הוא פועל בפרוטוקול ICMP ברמת ה-network. **פרס התשובה המקורית:** משתמש בפרוטוקול UDP, TCP, IGMP, בשכבות ה-transport link—למציאת מסלולים.

ב. (3 נק') הסבר מהו default gateway ב-LAN.

פתרון: זוהי כתובת IP של הנתב אשר אחראי לנתב חבילות מה-LAN החוצה ולהיפך. במידה והתחנות ב-LAN אינן מודעות ליציאה מהרשת לא יוכלו לתקשר החוצה. פונקציונאליות זו ברמת ה-network.

ג. (3 נק') מהו ההבדל בין Network mask ל-subnet mask.

פתרון: network prefix הינו החלק בביטים משמאל של כתובת ה-IP אשר מחלק בין כתובת הרשת לכתובת ה-host. הניתוב באינטרנט מתבצע לפי כתובת הרשת הפיזית. כאשר אנו מבצעים bitwise and לכתובת עם network mask כדי לגלות מהי כתובת הרשת. Subnet mask הינו חלוקה אופציונלית של חלק ה-host לרשתות משנה לוגיות, הדבר משמש פנימית ארגונים אשר רוצים ליצור מספר תתי רשתות לצרכים פנימיים. שיטה זאת נקראת subnetting. RFC 950.

פרס התשובה המקורית: ה-subnetting דרושים ל-router למציאת הניתוב ואילו ה-network mask בשימוש ע"י תחנות הקצה בלבד.

ד. (24 נק') נתונות שתי רשתות LAN Ethernet: LAN A בה נמצא מחשב A, LAN B בו נמצא מחשב B. שתי הרשתות מחוברות ביניהם ב-router שהינו ה-gateway של שתיהן. המשתמש במחשב A מבצע ping IP(B). תאר את כל השלבים בביצוע ה-ping request וקבלת ה-ping reply.

נא להשתמש בסימונים: IP(A), IP(B), IP(GW1), IP(GW2), MAC(A), MAC(B), MAC(GW1), MAC(GW2)

יש להניח כי כל הטבלאות המתעדכנות אוטומטית ריקות, וטבלאות הניתוב של ה-router תקינות.

פתרון: הרוב ענו נכון. שגיאות נפוצות: ראשית A בודק בעזרת net mask של IP(B) האם B נמצא באותה הרשת. ל-A אין טבלת ניתוב משום שיש לו רק interface יחיד לרשת.

פרס התשובה המקורית: א. הניתוב ב-router מתבצע ע"י ה-ARP TABLES ברמת ה-MAC, ואילו בתחנות הקצה ע"י ה-routing tables.

ב. מכיוון ש-GW אינו יודע היכן MAC(B) הוא זורק את ה-Ping חזרה על A כדי לרמוז לו ש-B לא נמצא ב-LAN.

בהצלחה!