בס"ד

פרויקט גמר קורס תקשורת ומחשוב

חלק ג' :

1. בהינתן מחשב חדש המתחבר לרשת נתאר את כל ההודעות העוברות החל מהחיבור הראשוני ל switch ועד שההודעה מתקבלת בצד השני של הצ'אט (מחשב היעד):

שלב ראשון: המחשב החדש יוצא חיבור ל switch ושולח בקשה ל switch עם כתובת IP של הצא'ט.

כתובת IP מקור:	כתובת IP של המחשב החדש
כתובת IP יעד:	כתובת IP של מחשב היעד
כתובת PORT מקור:	כתובת IP של PORT של המחשב החדש
כתובת PORT יעד:	כתובת הPORT של ה switch
כתובת MAC מקור:	כתובת MAC של המחשב החדש
כתובת MAC יעד:	כתובת MAC של מחשב היעד
פרוטוקול תעבורה:	אין – אנו בשכבה הפיזית

שלב שני: כעת ה switch ייקח את כתובת ה IP של מחשב היעד יבצע בדיקה אם כתובת היעד נמצאת תחת הרשת שלו, הוא יבחין כי אינה נמצאת ולכן יעביר את הפאקטה ל Router .

כתובת IP מקור:	כתובת IP של המחשב ה switch
כתובת IP יעד:	כתובת IP של מחשב ה Router
כתובת PORT מקור:	כתובת IP של PORT של ה switch
כתובת PORT יעד:	כתובת הPORT של הRouter
כתובת MAC מקור:	כתובת MAC של המחשב החדש
כתובת MAC יעד:	כתובת MAC של מחשב היעד
פרוטוקול תעבורה:	אין – אנו בשכבה הפיזית

שלב שלישי: בשלב זה פאקטה נמצאת אצל ה Router של המקור, לכן הוא יחפש לאן להעביר אותה על פי כתובת הרשת של הכתובת המבוקשת, לאחר מציאת הכתובת הוא יבדוק דרך איזה מסלול ניתוב כדאי לו להעביר את הפאקטה אל ה Router של הצאט.

כתובת IP מקור:	כתובת IP של הRouter - מקור
כתובת IP יעד:	כתובת IP של הRouter - צאט
כתובת PORT מקור:	כתובת IP של PORT של הRoute- מקור
כתובת PORT יעד:	כתובת הPORT של הRouter- צאט
כתובת MAC מקור:	כתובת MAC של המחשב החדש
כתובת MAC יעד:	כתובת MAC של מחשב היעד
פרוטוקול תעבורה:	TCP

שלב רביעי: כעת הפאקטה נמצאת אצל הRouter של הצאט ממנה היא תועבר לכתובת היעד. הRouter של הצאט יחפש את כתובת הרשת של היעד ויעביר אותה אל ה switch המתאים לה שתחתיו נמצאת כתובת היעד המבוקשת.

כתובת IP מקור:	כתובת IP של הRouter - צאט
כתובת IP יעד:	כתובת IP של ה switch - יעד
כתובת PORT מקור:	כתובת IP של PORT של הRoute- צאט
כתובת PORT יעד:	כתובת הPORT של הswitch - יעד
כתובת MAC מקור:	כתובת MAC של המחשב החדש
כתובת MAC יעד:	כתובת MAC של מחשב היעד
פרוטוקול תעבורה:	אין – אנו בשכבה הפיזית

שלב חמישי: הפאקטה נמצאת אצל ה switch של היעד אליו נרצה להעביר את ההודעה, ה switch ימצא את כתובת הMAC של היעד המבוקש וכך ההודעה תועבר למחשב היעד.

כתובת IP מקור:	כתובת IP של הswitch - יעד
כתובת IP יעד:	כתובת IP של היעד
כתובת PORT מקור:	כתובת IP של PORT של הswitch - יעד
כתובת PORT יעד:	כתובת הPORT של היעד
כתובת MAC מקור:	כתובת MAC של המחשב החדש
כתובת MAC יעד:	כתובת MAC של מחשב היעד
פרוטוקול תעבורה:	אין – אנו בשכבה הפיזית

כאשר הפאקטה הועברה לכתובת הIP של היעד, המחשב יפתח את המידע שיש בפאקטה וכך תתקבל ההודעה בצד השני של הצ'אט.

2. **<u>CRC -</u>** יתירות מחזורית "Cyclic redundancy check" הוא מנגנון Checksum המשמש לאיתור שגיאות בהעברת נתונים.
לפני העברת המידע, מחושב ה־ CRC ומתווסף למידע המועבר. לאחר העברת המידע, הצד המקבל מאשר באמצעות ה־ CRC שהמידע הועבר ללא שינויים.
השימוש ב־ CRC נפוץ בעיקר בשל קלות המימוש שלו בחומרה בינארית, קלות החישוב המתמטית שלו, ובמיוחד היעילות שלו בגילוי שגיאות נפוצות הנובעות כתוצאה מערוצי תקשורת רועשים.
בפרוטוקול, Ethernet אורך ה Checksum- הוא 32 ביטים, גם שדה זה לא נראה ב- Wireshark שכן הווידוא שלו מתרחש אצל כרטיס הרשת עוד לפני ש " Wireshark- רואה " את המסגרת.

3. <u>ההבדל בין http 1.0 ,http 1.1, http 2.0, QUIC :</u>
פרוטוקול תקשורת HTTP נועד להעברת דפי HTML ואובייקטים המכילים תמונות, קובצי קול, סרטוני פלאש וכו' ברשת האינטרנט וברשתות אינטראנט מיועד לאפשר לאפליקציות לגשת ולעשות שימוש במשאבי רשת באינטרנט.
ה HTTP משתמש בפרוטוקול **TCP** - שמבצע את פעולת החיבור מהלקוח לשרת (תהליך "לחיצת הידיים") ויוצר את הסוקטים בפורט 80.
(לפרוטוקול http ישנם שלוש גרסאות 1.0 , 1.1 , 2.0 (– החדשה ביותר) וכולן משתמשות בפרוטוקול TCP).
לעומת זאת, QUIC מבצע את אותן המשימות רק בדרך קצת שונה, ומהירה יותר.
QUIC הוא הפרוטוקול חדש של גוגל המשתמש בפרוטוקול **UDP** שעובד מהר יותר מ TCP אך לא כולל את היכולת לאחזר פאקטות מידע שהלכו לאיבוד בדרך, אך Quic ידאג לאחזור הזה, ויעשה זאת מהר יותר מ TCP.
כמו כן, Quic מהיר יותר מ-TCP גם ביצירת קשרים מוצפנים.

4. מדוע צריך מספרי PORT :
כדי לענות על שאלה זאת נסביר מה זה בעצם PORT-
במחשב פועלים בד"כ מספר סוגי יישומים בו-זמנית (בעזרת מערכת הפעלה), כדי שהמחשב יידע לסווג את הנתונים המתקבלים ליישומים השונים הפועלים בו-זמנית, לא מספיק רק כתובת IP אלא גם איזשהו כתובת פנימית - Port (פורט פנימי) שממפה אותי לשירות שאליו אני רוצה לגשת.
ישנם כל מיני סוגי פורטים לדוגמא: פורט 80 - כדי לגשת לHTTP מסוים, פורט 25 – מייל.
הלקוח יוצר את הקשר עם הסרבר לכן הלקוח צריך לדעת לאיזה פורט לגשת בסרבר אבל כשהוא כבר מגיע לסרבר, הסרבר כבר יודע מאיזה פורט הלקוח ניגש בצד שלו ואז הוא השולח לו את הנתונים שהלקוח דורש בהתאם לדרישות.
השימוש הנפוץ בPORT הוא בפרוטוקולים בשכבת התעבורה (המשמשת לתקשורת בין מחשבים) TCP ו- UDP .

השימוש במספרי PORT נועד כדי ששני צדדי התקשורת ישתמשו באותו פרוטוקול תעבורה.
לדוגמא : על מנת שהדפדפן יפנה לאתר אינטרנט ב HTTP - הדפדפן צריך לפנות לפורט פתוח על השרת שיקבל את הפניות אליו ויטפל בהן, והפורט הזה הוא הפורט המוכר לתעבורת HTTP - פורט 80 המשתמש בפרוטוקול TCP.

5. **SUBNET -**
הגדרה: כתובת רשת אשר מחלקת את כתובת ה IP לשתי רשתות או יותר.
מחשבים השייכים לאותה subnet (רשת משנה) הינם בעלי קבוצת סיביות זהה בכתובת הIP שלהם. ה subnet מחלק את כתובת הIP לשני שדות: 1. מספר הרשת המקומית \ כתובת הניתוב, 2. מספר מזהה ייחודי למחשב. בכל subnet תמיד יהיו שתי כתובות IP שמורות, הראשונה עבור שם הרשת והאחרונה עבור הברודקאסט.
צורך: ה subnet זו תת רשת שלא עוברת דרך ראוטר, כלומר עבור תקשורת בין שני מחשבים באותה רשת אין צורך לעבור דרך ראוטר והם יתקשרו תחת אותו subnet – תת רשת. כמו כן ה subnet נועד למיפוי המחשבים שנמצאים תחת אותה רשת וכאשר מחשב רוצה לתקשר עם מחשב אחר והם אינם תחת אותה רשת מקומית, נוכל למצוא את המחשב הספציפי שאנו מחפשים ע"י כתובת הIP שלו כך שהמיקום האחרון בכתובת ייחודי לכל מחשב עבור מחשבים תחת אותה רשת מקומית.

Subnet Mask – הוא מושג תחת SUBNET, שתפקידו לתת את הכתובת של הרשת בה נמצא המחשב . Subnet Mask הינו אובייקט בעל 4 אוקטטות (אוקטטה - תבנית בעלת 8 ביטים, מיוצגת עשרונית ע"י מספרים מ-0 עד 255), אשר מקביל לכתובת IP ומציין למחשב היכן נגמר ה Network ID (המספרים שמציינים את הרשת הכללית) והיכן מתחיל ה Host ID (המספרים ב IP שמציינים את המחשבים ברשת).

<u>דוגמא:</u> עבור חברה המורכבת מכמה מחלקות ניתן לייצר כתובת IP ספציפית לכל מחלקה.
לכל מחלקה יש צורך ברשת נפרדת על מנת לאפשר תקשורת, לכן 6 האוקטטות הראשונות בכתובת הIP יהיו זהות לכל המחלקות, האוקטטה השביעית תסמן את מספר המחלקה והאוקטטה האחרונה תייצג את המחשב הספציפי (או המדפסת).

6. למה צריך כתובת MAC ולמה לא מספיק לעבוד רק עם כתובת IP:
כתובת IP: היא מספר המשמש לזיהוי נקודות קצה כמו מחשב, מדפסת או ברשתות תקשורת שבהן משתמשים בפרוטוקול התקשורת IP כמו רשת האינטרנט. כתובת הIP היא חלק משכבת הרשת שכבת הקו של מודל ה OSI.

כתובת MAC: היא מזהה ייחודי המוטבע על כל רכיב תקשורת לתקשורת נתונים בעת הייצור. כתובת ה MAC מוטבעת בדרך כלל בכרטיס הרשת של המחשב או במודם .
הכתובת מחולקת לשני חלקים: הראשון הוא מספר הסידורי של היצרן והשני הוא הספר הסידורי של הרכיב (הייחודי לכל רכיב). כתובות MAC נחשבות כחלק משכבת הקו של מודל הOSI או השכבה הפיזית של מודל הTCP/IP.

הצורך בכתובת MAC בנוסף לכתובת IP הוא משום שאת כתובת IP ניתן לשנות או שתחת אותה כתובת IP יהיו 2 מחשבים (או יותר) לכן, כדי לדעת מהי כתובת היעד המדויקת של מחשב ספציפי נשלח גם כתובת MAC שיציין לנו את הרכיב הספציפי אליו אנו מיעדים את ההודעה \ תקשורת.

7. ההבדל בין Router vs Switch Nat :

Router - נתב הוא רכיב **תקשורת מחשבים** שנועד לקביעת נתיב הנתונים ולהעברת נתונים מרשת אחת לרשת אחרת ברשת ה WAN. לדוגמה, מרשת האינטרנט ,לרשת הפרטית של המשתמש הביתי.
Switch - הוא רכיב **ברשת מחשבים** המחבר בין צמתים שונים באותה הרשת, בין אם הם מכשירי קצה (כגון מחשבים) ובין אם הם מרכיבי רשת בסיסיים (כגון רכזות), ה Switch מרכז את כל כתובות הקצה תחת אותה רשת LAN .
טבלת Nat - כאשר ה Router צריך לנתב את המידע למחשב או להתקן הפנימי הוא משתמש בטבלת NAT הממירה את הכתובת הפנימית ל IP חיצוני , כתובת היעד ופורט היעד תמיד נשמרים גם שהמידע יעבור דרך Routers אחרים הנמצאים ברשת האינטרנט.
Switch Nat – הוא Switch הפועל כמו Router באותה רשת WAN ותפקידו למצא ולהתאים כתובת NAT אחידה לכל הרכיבים ברשת כך שתמיר את כתובת הIP הפנימי של הרשת לכתובת IP חיצונית.

ההבדל הראשון בין Router vs Switch Nat הוא שהנתב עובד בשכבת הרשת ואחראי למצוא את הנתיב הקצר ביותר לחבילה ואילו Switch מחבר התקנים שונים ברשת. הנתב מחבר מכשירים על פני מספר רשתות.
לפיכך ההבדל העיקרי בניהם הוא שה Router מתרגם כמה כתובת IP של רשת התקשורת הפנימית לכתובות NAT ואילו ה Switch מתרגם כתובת IP אחת בהתאם לצורך בכך, אם אין צורך בתרגום כתובת הIP לכתובת גלובלית הSwitch ישאיר את הכתובת IP כפי שהיא.

8. שיטות להתגבר על מחסור ב IPV4 :

1. הפתרון השכיח ביותר להתמודדות עם מחסור כתובות היא טכנולוגית ה NAT - טכנולוגיית ה NAT מתמקמת בין הרשת הפנימית של ארגון והחיבור שלו לאינטרנט, ומקצה ברשת הפנים ארגונית לכל מחשב כתובת IP פנימית שאינה ייחודית, אולם כאשר המחשב יוצא לאינטרנט הוא מקבל כתובת IP חיצונית מתוך המאגר שהוקצה לארגון. בתהליך אופטימיזציה זה, ארגון יכול לאפשר גישה של כמות גדולה של ציוד קצה לאינטרנט, תוך שימוש במאגר מוגבל של כתובות IPv4. באופן זה נחסכות כתובות IP שמקושרות אל עולם האינטרנט. טכנולוגית ה NAT -משמשת גם כ"גישור" בין פרוטוקול IPv4 לבין IPv6 (נסביר בהמשך).

פתרונות זמניים: (2,3,4)

2. רשת פרטית - מאפשרת שימוש בחיבורים רבים בתוך הרשת, ללא כתובת, אך כל יציאה לאינטרנט מחייבת לעשות שימוש בכתובת השער. שיטה זו נפוצה בחיבורים ביתיים.
3. שרת מארח וירטואלי - מאפשר לעשות שימוש בכתובת השרת המארח.

4. המשמש תקשורת פרוטוקול DHCP (Dynamic Host Configuration Protocol) - פרוטוקול תקשורת המשמש להקצאה של כתובות IP ייחודיות למחשבים ברשת מקומית LAN.
5. הפתרון הטוב ביותר ולטווח ארוך הוא- יצירת גרסה חדשה לפרוטוקול שכבת הרשת והיא IPv6 .
ההבדל המהותי בין IPv4 וIPv6 נובע מהגדלת מרחב הכתובות המקשרות בין אמצעי המחשוב השונים על גבי רשת העברת נתונים.
בעוד ש **IPv4** - מכיל 32 סיביות**, IPv6** - מכיל 2^128 סיביות שהן כמות הכתובות האפשריות ב IPV6, ז"א שהכתובת תהיה מורכבת ממספר בן 39 ספרות והוא : 19340,282,366,920,938,000,000,000,000,000,000,000,000.
לכן נהוג לומר כי בפרוטוקול IPv6 ניתן להצמיד כתובות IP לכל גרגיר חול ביקום. משום כך יישום IPv6 מאפשר הקצאה מחודשת של כתובות למשך העתיד הרחוק ומבטל את הצורך בפתרונות זמניים שהומצאו על מנת להתמודד עם מחסור הכתובות בIPv4 (כגון DHCP, NAT וכו').

9. נתונה הרשת הבאה:
* AS2 , AS3 מריצים OSPF
* AS1 , AS4 מריצים RIP
* בין ה ASS רץ BGP
* אין חיבור פיזי בין AS2 , AS4

e . בעזרת פרוטוקול BGP לומד הנתב c3 על תת רשת x .

f . בעזרת פרוטוקול OSPF לומד הנתב a3 על תת רשת x .

g . בעזרת פרוטוקול BGP לומד הנתב c1 על תת רשת x .

h . בעזרת פרוטוקול BGP לומד הנתב c2 על תת רשת x .