

פרויקט סיום תקשורת ומחשוב - חלק ג'

1. בהינתן מחשב חדש המתחבר לרשת אנא תארו את כל ההודעות שעוברות החל מהחיבור הראשוני ל switch ועד שההודעה מתקבלת בצד השני של הצאט. אנא פרטו לפי הפורמט הבא:
 - a. סוג הודעה, פירוט הודעה והשדות הבאים
 - i. כתובת IP מקור/יעד, כתובת פורט מקור/יעד, כתובת MAC מקור/יעד, פרוטוקול שכבת התעבורה.

לאחר חיבור ראשוני ל-Switch כתובת ה-MAC של המחשב שלנו תרשם בטבלת הנתונים של ה-Switch. בפעם הראשונה בה המחשב שלנו ישלח מסגרת כלשהי למשל חבילת DHCP Discover, ה-Switch יקרא את כתובת המקור של המסגרת אותה שלחנו וישייך אותה לפורט הפיזי אליו מחובר המחשב. כעת נרצה למצוא את כתובת ה-MAC של הנתב, וזאת מפני שהנתב מהווה לתחנת המעבר הקרובה ביותר בדרך אל היעד. נציין כי נשיג את הכתובת הפיזית הרצויה, באמצעות פרוטוקול ARP, פרוטוקול זה שייך לשכבת הקו, מאחר ומדובר בחיבור פיזי. כעת נוכל לבקש מהנתב לייצר לנו כתובת IP למחשב, מה שישמש אותנו בבקשות אל מעבר לנתב שלנו. אנו נשיג את את ה-IP שלנו באמצעות DHCP, פרוטוקול זה שייך לשכבת הקו והוא פועל על גבי פורטים 67, 68. לאחר שהשגנו את כתובת ה-IP עבור המחשב שלנו, אנו נשלח בקשה להתחברות לסרבר (נשתמש בהנחה שאנו יודעים מהי כתובת הסרבר מראש ע"פ הוראות הפרוייקט). אנו נשלח את הבקשה לשלוח הודעה לסרבר באמצעות TCP, ששייך לשכבת התעבורה, נציין כי כתובת הפורט של המחשב שלנו יהיה מספר רנדומלי בטווח : 49251 ובין 65535. לאחר מכן הסרבר יחזיר תשובה באותו הפורט באמצעות TCP.

2. הסבירו מה זה CRC

בדיקת יתירות מחזורית או "CRC" היא קטע קוד בו נשתמש על מנת לאתר שגיאות בהעברת נתונים, נשים לב שהקוד מבוסס על מנגנון ה-Checksum.

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.

3. מה ההבדל בין http 1.0, http 1.1, http 2.0, QUIC

תחילת נגדיר מה הם כל אחד מהפרוטוקולים המצוינים לעיל :

- **פרוטוקול QUIC** : הינו פרוטוקול ניסיוני שפותח ע"י גוגל. הפרוטוקול מתעסק בשכבת התעבורה ומטרו הכללית הינה הורדת העומס (LATENCY) בהשוואה ל-TCP. באופן כללי פרוטוקול QUIC מאפשר יצירה של חיבורים בצורה כזאת שתחסוך לנו בתעבורה עצמה, כלומר פחות הלוך ושוב בין המכונות הרלוונטיות מה שיחסוך לנו בזמן כללי לביצוע המשימה. בנוסף פרוטוקול QUIC נועד להביא את כל המשאבים שנדרשו על מנת לטעון דף אינטרנט תוך שימוש בחיבור יחיד.

- **פרוטוקול HTTP** : הוא פרוטוקול תקשורת שנועד להעברה של דפי HTML והאובייקטים שהם מכילים ברשת האינטרנט. התקשורת באמצעות HTTP מתחילה ביצירת השיחה בין השרת למשתמש באמצעות פרוטוקול TCP.

שלוש השיטות העיקריות להעברת מידע הינן : GET, POST, HEAD
בנוסף, פרוטוקול HTTP הוא פרוטוקול חסר מצבים ועל מנת ליצור תקשורת בין משתמש לשרת המבוססת על היסטוריית הבקשות-תשובות נעשה שימוש ב-COOKIES.

● פרוטוקול HTTP 1.0 :

גרסה זו של הפרוטוקול משתמשת בחיבור יחיד עבור מס' בקשות.
עד גרסה 1.0 הלקוח המשתמש בפרוטוקול נאלץ לפתוח ולסגור את החיבור מחדש בכל בקשה דבר היוצר עומס מיותר, מתוך הבעיה שצוינה לעיל נוצרה גרסה 1.0 ובעקבותיה נוצרו בעיות חדשות המתקשרות בחיבור לשרתי proxy.

● פרוטוקול HTTP 1.1 :

גרסה זו של הפרוטוקול גם היא משתמשת בחיבור יחיד עבור מס' בקשות כך שיהיה ניתן להשתמש בשרתי proxy.
גרסה זו באה לשפר את הבעיות שהוצגו לעיל בעקבות גרסה 1.0, ומכאן שופר המנגנון כך שיהיה ניתן להשתמש בשרתי proxy. המנגנון נוצר כך שיתאים גם למנגנון הקודם וגם לשרתים ישנים יותר.

● פרוטוקול HTTP 2.0 :

גרסה זו משתמשת בכל העקרונות עבודה של גרסה 1.1 ובאה להוסיף בצורה כזו שאפליקציות חדשות משתמשות בפרוטוקול מקבלות גישה לפיצ'רים מתקדמים יותר של העברת הנתונים (כלומר הנתונים יכולים לעבור מהר יותר) וזאת בעוד אפליקציות ישנות שהיו תלויות בפרוטוקול הישן יותר עדיין מקבלות את אותה התמיכה.

ההבדלים המרכזיים בין הפרוטוקולים :

ב-HTTP 1.0 פותחים וסוגרים את הקשר עבור כל בקשה וקבלה. ואם כי עבור HTTP 1.1 אנו נמשיך לבקש או לקבל כלומר נבקש מס' כלשהו של אובייקטים ונקבל אותם אחד אחרי השני.
עבור HTTP 2.0 ההבדלים המהותיים בין שאר הגרסאות באים לידי ביטוי בפאן החדשני יותר, כלומר אפליקציות חדשות יותר יקבלו גישה להעברות נתונים מהירות יותר בעוד שאפליקציות שתומכות בגרסה הישנה יותר ימשיכו לקבל את אותה התמיכה שקיבלו.
עבור HTTP 3.0 המשתמש בQUIC עבור שכבת התעבורה לטפל ברצף הנתונים בעוד ש-HTTP 2.0 משתמש בפרוטוקול TCP בשכבת ה-HTTP על מנת לבצע את אותה המשימה.
לפרוטוקול HTTP 3.0 יש מנגנון לחיצת יד המבטיח התקשרות הרבה יותר מהיר מ-HTTP 2.0 (פה נעשה שימוש ב-TCP ו-TLS).

4. למה צריך מספרי port?

ראשית, מספרי PORT היא דרך לאפיין תהליך ספציפי עבורו האינטרנט או הודעת רשת מקודמת בהגעה לסרבר.

במילים אחרות, מס' הפורט מקטלגים לנו את ההודעות שנקבל כל הודעה למקומה בעת ההגעה לסרבר.

- פורטים מוכרים הם פורטים המשמשים פרוטוקולים מוגדרים כסטנדרט. הצורך בפורטים מוכרים קיים כדי לקבוע סטנדרטים בהתחברות לשרתים המספקים שירותים מסוימים.

אז למה בעצם צריך אותם ?

הפורטים עושים לנו סדר בכל הבלאגן שנוצר בעקבות הבקשות המרובות שסרבר מקבל.

במקום שנשים את כל הבקשות באותו הפורט, אנו נוכל לייצר פורטים משלנו או לחלופין להשתמש בפורטים מוכרים על מנת למיין ולקטלג את הבקשות שנקבל בזמן אמת, ובכך לחסוך זמן בעת המהנה על אותן הבקשות שמיינו.

לדוגמא : נניח ויש לנו 2 מצלמות בבית ואנו נרצה לגשת לשתייהן, במידה והן נמצאות על אותו הפורט בניסיון לגישה אליהן אנו נקבל גישה רק לאחת מהן, ולכן אם נשים כל מצלמה בפורט משלה אנו נוכל לקבל גישה ישירה לשתי המצלמות במקביל ולקבל את המידע מהן יחד.

5. מה זה subnet ולמה צריך את זה?

סאב-נט או סאב-נטוורק היא חלק מחלקה גדולה יותר של אינטרנט או רשת.

הסאב-נט מהווה חלוקה למחיצות לוגיות עבור IP network, כלומר עבור חלקת אינטרנט גדולה נוכל לחלק למחיצות כאשר לכל מחיצה תפקיד שונה.

לכל מחשב שמחובר לאינטרנט יש לפחות כתובת IP אחת בעלת משתנה ייחודי וכל מחשב שמחובר לרשת האינטרנט זהה יקבל את אותו המשתנה לכתובת ה-IP שלו, בזכות זה שני המחשבים יוכלו לתקשר אחד עם השני בצורה יעילה ומהירה יותר

השימושים של סאב-נט :

- ייעוד מחדש של כתובות IP.
- שחרור תעבורה ברשת.
- שיפור של אבטחת האינטרנט.

6. למה צריך כתובות mac למה לא מספיק לעבוד עם כתובות ip?

תחילה כתובת MAC הינה כתובת פיזית ייחודית לכל מחשב, כתובת זו אינה ניתנת לשינוי ומהווה הכתובת העיקרית של המחשב בעת שימוש ברשת המקומית אליה מחובר.

כתובת IP לעומת זאת הינה כתובת לוגית, כלומר היא איננה ברמת החומרה והיא ניתנת לשינוי בהתאם לצרכים של המשתמש.

שימוש בכתובת זו נעשית בעיקר בעת התחברות לרשתות אחרות שהן לא הרשת המקומית של המחשב.

אנו לא נוכל להתחבר לשום רשת מחוץ לרשת המקומית שלנו אילולא היינו משתמשים בכתובת IP, השימוש בכתובת ה-MAC לא מקנה לנו את האופציה להתחבר לרשתות חיצוניות ואילו כתובת ה-IP כן.

7. מה ההבדל בין Router Switch Nat?



Router: רכיב תקשורת מחשבים, שנועד לקביעת נתיבן והפצתן של חבילות נתונים ברשתות תקשורת הנתונים.

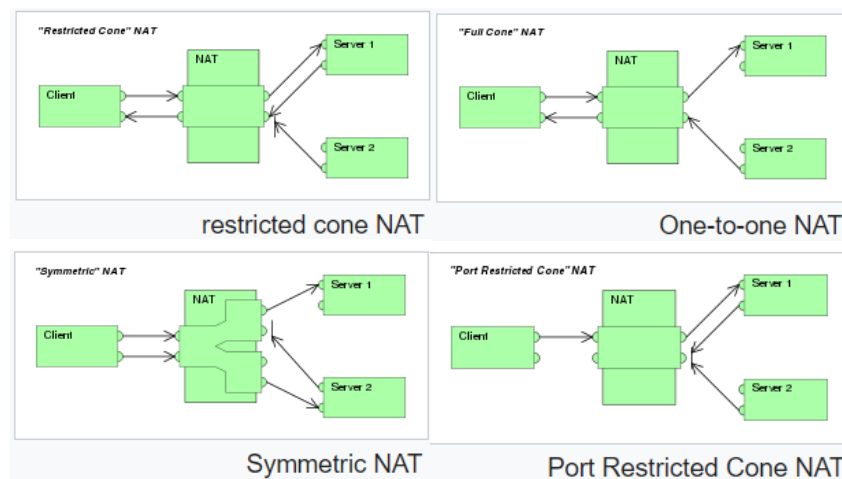


Switch: רכיב ברשת מחשבים המחובר בין צמתים שונים ברשת, בין מכשירי קצה ובין מכשירי מרכזי רשת. מספר הכניסות יכול לנוע בין כניסות בודדות ועד למאות כניסות במקרים של רשתות תקשורת גדולות.

NAT: Network Address Translation היא טכניקת ניתוב ברשת מחשבים, בה נכתבות מחדש כתובות ה-IP של הפאקטות שעוברות ב-Router, כלומר כתובת ה-IP שתצא משימוש תחזור אל מאגר הכתובות ותינתן למחשב אחר במידת הצורך.

הטכניקה מאוד יעילה ונמצאת בשימוש נרחב ולרוב משומשת כפונקציה בסיסית.

• סוגים של NAT :



Router עושה שימוש ב-NAT בעוד Switch עובד רק ברשת המקומית ולכן אין לו כל שימוש ב-NAT

טבלת השוואה עבור שאלה 7:

Router	Switch
פועל בשכבה ה-3 (Network).	פועל בשכבה ה-2 (Data Link).
מציע שירותי NAT, NetFlow, QoS.	אינו מציע שירותי כאלה.
שומר כתובות IP בטבלת הניתוב ושומר על כתובת משלו.	שומר כתובות MAC בטבלת החיפוש ושומר על כתובת משלו, ובכך בעצם "לומד" את כתובת ה-MAC.
מגבלת המהירות היא 1-10 Mbps עבור חיבור אלחוטי וכ-100 Mbps עבור חיבור קווי.	המהירות היא 10\100 Mbps.
עוזר למשתמש לקחת את הנתיב הטוב ביותר.	עלול לנתב בדרך מסובכת.
בכמה סוגים של סביבות רשת (MAN/WAN) הראוטר עובד מהר יותר.	בסביבת רשת מקומית (LAN) הסוויץ' עובד מהר יותר.
לכל PORT יש כתובת שידור.	יש רק כתובת שידור אחת למעט VLAN.
עיקר הפעולות נעשות על כתובות IP.	עובד רק עם כתובות MAC תוך כדי עבודה בתוך רשת אחת.
עובד גם על חיבור קווי וגם על חיבור אלחוטי	מוגבל אך ורק לחיבור קווי.
מספק אמצעי אבטחה להגנה על הרשת מפני איומים.	מספק רק PORT אבטחה אחד.

8. שיטות להתגבר על המחסור בIPv4 ולפרט?

ראשית, כיום קיים מחסור בכתובות IPv4, וזאת מאחר ואף אחד לא ציפה בשנות ה-80 שהאינטרנט יגדל לגדלים שלו כיום, מחסור בכתובות כללו יוצר בעייתיות ישנן 2 שיטות עיקריות להתגבר על המחסור :

• מעבר לכתובות IPv6 :

כתובות ה-IPv6 נוצרו על מנת לתת מענה למחסור בכתובות IPv4. IPv6 הינו הדור הבא של הפרוטוקולים, משתמש בכתובות של 128 bits מה שאומר שישנן 2^{128} כתובות כאלה. IPv6 מציע מס' הרבה יותר גדול של כתובות מס' ובנוסף מוסיף עוד פיצ'רים של אבטחה. שימוש בכתובות IPv6 החל באמצע שנות ה-2000 ועדיין נמצא בשלבים מוקדמים יחסית של פיתוח. המון ספקי אינטרנט וחברות של ציוד תקשורת גדולות הסכימו לתת תמיכה תמידית בכתובות IPv6 ביוני 2012, ומאז החל להיעשות שימוש נרחב בכתובות IPv6. המצב כיום הוא ששימוש בכתובות IPv6 מקנה פתרון בטווח הרחוק למחסור בכתובות IPv4 ישנן בעיות הכרוכות במעבר לשימוש בלעדי בכתובות IPv6 כגון :

- השקעה כספית עצומה
- חוסר תאימות עם כתובות IPv4

ומכאן שאמנם לטווח הרחוק שימוש בכתובות IPv6 מקנה פתרון ישיר לבעיה, אך הדבר לא יקרה בקרוב.

• השכרת כתובות IPv4 :

מאחר והיום עדיין קיימת דרישה רצינית למשאבים של IPv4, מכירה והשכרה של הכתובות היא המענה הזמין למחסור בכתובות IPv4. חברות שמציעות סחר בכתובות IPv4 ושירותי השכרה של הכתובות הלא משומשות ומתמחרים אותם לחברות שונות. בעלי IP יכולים להשתמש באפשרות הזאת כרווח צדדי. מסחר בכתובות IP שימושי לשני הצדדים מכיוון שממחזר כתובות IPv4 קיימות ונותן מענה לאלו שרוצים לתמחר את הכתובות שניתנו להם. המסחר בכתובות IPv4 יכול לפתור את המחסור בכתובות IPv4 באופן זמני, מה שמאפשר לשמור זמני של כתובות וגם ייתן את הזמן הדרוש על מנת לעבור לכתובות IPv6 מה שיפתור את הבעיה לטווח הרחוק.

9. נתונה הרשת הבאה.

a. AS2, AS3 מריצים OSPF

b. AS1, AS4 מריצים RIP

c. בין ה-Ass רץ BGP

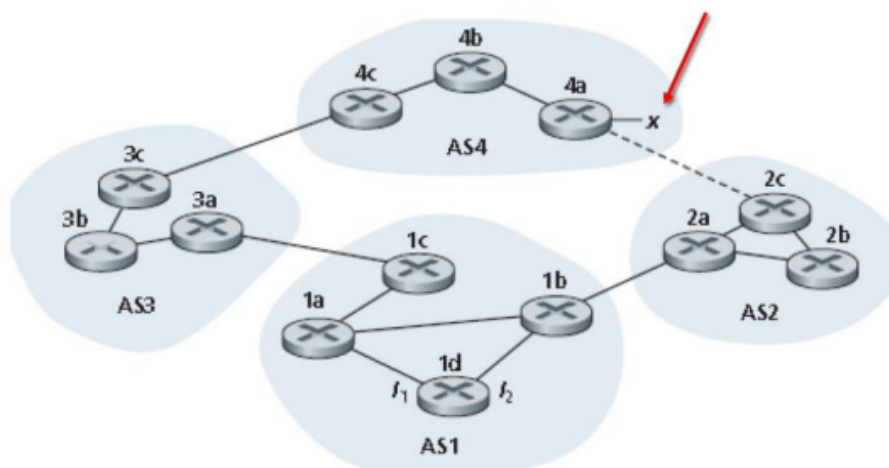
d. אין חיבור פיזי בין AS2, AS4

e. בעזרת איזה פרוטוקול לומד הנתב 3c על תת רשת x

f. בעזרת איזה פרוטוקול לומד הנתב 3a על תת רשת x

g. בעזרת איזה פרוטוקול לומד הנתב 1c על תת רשת x

h. בעזרת איזה פרוטוקול לומד הנתב 2c על תת רשת x



OSPF - open shortest path first

נתב המנתב חבילות בהתבסס על OSPF מנהל רישום של כל הנתבים שהוא "מכיר", והנתיבים אליהם. כאשר מגיעה אליו חבילה הוא מעביר אותה אל נתב היעד דרך הנתיב בו עלות התעבורה היא הזולה ביותר.

RIP - router information protocol

נתב המשתמש ב-RIP מנהל רישום של כל הנתבים אותם הוא "מכיר", הרשתות המחוברות אליהן, וכמות הצעדים בכל נתיב לכל יעד

BGP - border gateway protocol

נתב שפועל באמצעות BGP מנהל טבלה של הרשתות המחוברות אליו, והקשרים ביניהן לבין רשתות אחרות, ומבצע החלטות ניתוב על בסיס הקשרים בין הרשתות ומדיניות המוכתבת בצורה ידנית על ידי מנהל הרשת.

To start things off - the subnet "x" transmits it's existence to every router in AS4, we then transmits information from 'x' to 4b and 4c using the 4a router.

e) We learn about the existence of the subnet 'x' via eBGP using 4c -> 3c routers.

f) 3c transmits the information to 3b which transmits to 3a, it all happens using iBGP..

g) 3a transmits the existence of the subnet 'x' via eBGP using 3a -> 1c routers.

h) 1c transmits about the existence of the subnet 'x' via iBGP to the other routers that are in the cluster.

now since the router 1b knows, it transmits to the router 2a via eBGP.

then 2a transmits to the other routers in the cluster using iBGP.