שיעור 10 – שכבת הקו

**תרגיל: חדל קשקשת ברשת!**

בתרגיל זה נתבונן במספר הסנפות שבוצעו ברשת פנימית של ארגון, ממספר מחשבים שונים. נצטרך להבין מתוך ההסנפות איך הרשת בנויה, תוך התמקדות בפרוטוקוליםEthernet ו-ARP. בתרגיל מומלץ לעבוד עם פילטרים ב-Wireshark כדי להקל על החיפוש של המידע בתוך ההסנפה. בהצלחה!

1. **חלק 1 – הסנפה ממחשב A**
   * 1. נסו להסיק מתוך ההסנפה מיהו המחשב שממנו בוצעה ההסנפה – מה כתובת ה-IP וכתובת ה-MAC שלו?

|  |
| --- |
| ניתן לראות מספר כתובות IP בהסנפה שמבצעות שיחות, אבל יש רק שתי כתובת שמופיעות כמעט בכל השיחות, והן 192.168.0.5 ו- 192.168.0.51  כדי להבין מי מהן היא באמת מחשב A יש צורך להשתמש בפילטר שיציג לנו רק פאקטות שמכילות את פרוטוקול ARP.  אחרי שנכתוב פילטר זה - נישאר עם 6 פאקטות. מתוכן 5 שאילתות ותשובה אחת.  אנו רואים כי 192.168.0.4 שואל מי יודע מה כתובת ה-MAC של 192.168.0.1 ושל 192.168.0.51 ואנחנו לא רואים את התשובה לשאילתות האלה.  אנו רואים כי גם 192.168.0.5 שואל מי יודע מה כתובת ה-MAC של 192.168.0.51 ואנחנו **כן** רואים את התשובה לשאילה זו.  מכיוון שהכתובת 192.168.0.51 מופיע גם עבור השאילתה של 192.168.0.5 וגם עבור השאילתה של 192.168.0.4 אבל יש רק תשובה עבור השאלה של 192.168.0.5 נסיק כי מחשב**A הוא המחשב בכתובת ה-IP 192.168.0.5**  כתובת ה-MAC שמופיעה כ-Src בחבילות היוצאות היא **00:02:b3:00:02:b3.**  כמו כן, אחדד כי אנו רואים גם בקשות ARP של כתובות שלא ניתן לזהות שיחות שלהן, ואת הבקשות הללו אנחנו יכולים לראות בגלל שהן משלחות ב-Broadcast... |
| תשובה |

* + 1. עם איזה מחשב מתקשר בעיקר מחשב A? באיזה פרוטוקול?  
       מאיזה IP ו-MAC מגיעות החבילות?

|  |
| --- |
| המחשב מנהל שיחת HTTP עם שרת ווב שנמצא איתו בסאבנט (192.168.0.51).  ה-MAC מהן הן מגיעות הוא :0c00:00: 00:00:0c. |
| תשובה |

* + 1. האם המחשב איתו מדבר מחשב A ב-HTTP נמצא באותו סאבנט איתו? כיצד הבנתם זאת?

|  |
| --- |
| אפשר להבין זאת כי מחשב A מבצע שאילתת ARP ומבקש את כתובת ה-MAC של 192.168.0.51. מכיוון שאנו מבקשים כתובת MAC רק של מחשבים שמחוברים אלינו ישירות, הרי שהם באותו סאבנט. |
| תשובה |

* + 1. מהי כתובת ה-Dst MAC בשאילתות ה-ARP בהסנפה? מדוע מחשב A מקבל את השאילתות אם הן לא מיועדות לכתובת MAC שלו?

|  |
| --- |
| בקשות ה-ARP בהסנפה נשלחות לכתובת MAC – FF:FF:FF:FF:FF:FF.  לשליחה זו אנו קוראים Broadcast והיא מיועדת לכל המחשבים בסאבנט, ואנחנו הרי איתו בסאבנט! את התשובות לעומת זאת אנחנו לא רואים, כי הן נשלחות באופן ישיר בין שני המחשבים.  ניתן להסיק מההסנפה שהמחשב גם כן גולש ל-192.168.0.51. |
| תשובה |

1. **חלק 2 – הסנפה ממחשב B**
2. מאיזה מחשב בוצעה ההסנפה? מה כתובת ה-IP וה-MAC שלו?

|  |
| --- |
| כמו מקודם, יש רק מחשב אחד שנמצא בכל השיחות שבהסנפה הזו – 192.168.0.4  כתובת ה-MAC שלו היא 00:00:63:00:00:63 |
| תשובה |

1. האם מחשב B נמצא באותו סאבנט יחד עם מחשב A? בהנחה שכל תתי הרשתות ברשת הן בגודל של 255 מחשבים כל אחת, מהו ה- Subnet Mask של הרשת? (כתבו בשתי הדרכים שלמדנו).

|  |
| --- |
| כן, שניהם באותה רשת. אפשר לקבל הוכחה לכך ע"י זה שמחשב B מקבל שאלות ARP ממחשב A (מזהים זאת ע"י Tell 192.168.0.5), ושאילתות ARP מוחלפות רק על ידי מחשבים באותו סאבנט.  ה-Mask הוא 255.255.255.0 או 192.168.0.0/24 |
| תשובה |

1. האם מחשב B מדבר עם מחשבים הנמצאים מחוץ לסאבנט שלו? אילו מחשבים?

|  |
| --- |
| כן, עם המחשבים בכתובת 192.168.2.97 ובכתובת 192.168.2.8 אפשר לדעת זאת מכיוון שלא מתבצעת שאילתת ARP של מחשב B כדי לגלות את ה-MAC של 192.168.2.97 או 192.168.2.8. |
| תשובה |

1. מהן כתובות ה-Src MAC המופיעות בחבילות שמגיעות משני המחשבים הנמצאים מחוץ לסאבנט?

|  |
| --- |
| שתיהן מגיעות עם כתובת Src MAC זהה = 00:05:5d:00:05:5d |
| תשובה |

1. כיצד תוכל להסביר שחבילות משני המחשבים הללו מגיעות עם כתובת MAC זהה?

|  |
| --- |
| מכיוון שבשני המקרים מחשב B מדבר עם מחשב מחוץ לסאבנט שלו, הרי שהתקשורת הזאת צריכה לעבור דרך ראוטר כלשהו המקשר בין תתי הרשתות.  לכן כתובת ה-MAC שאנחנו רואים היא לא של המחשבים איתם הוא מדבר על של המחשב שהעביר לנו את החבילות, הלא הוא הראוטר שלנו. |
| תשובה |

1. מהי כתובת ה-MAC של ה-Default Gateway (הראוטר) של מחשב B? כיצד גילית זאת?

|  |
| --- |
| למעשה התשובה כאן היא זהה לסעיפים הקודמים.  דרך נוספת לגלות את ה-Defatult Gateway היא בעזרת התעבורה שיוצאת מ-B: נבחר חבילה היוצאת מ-B אל מחוץ לסאבנט ונראה למי הוא מייעד את החבילות ברמת ה-MAC. למעשה זהו ה-Next Hop של החבילות שיוצאות מ-B ל-192.168.2.97 למשל.  כתובת ה-MAC היא 00:05:5d:00:05:5d, בדיוק זו שראינו בסעיפים ד-ה. |
| תשובה |

1. מהי כתובת ה-IP של ה-Default Gateway (הראוטר) של מחשב B? כיצד גילית זאת? צרף צילום מסך של החבילה שעזרה לך להבין זאת (רמז: ARP הוא חבר)

|  |
| --- |
| כדי לתקשר עם ה-Gateway חייב מחשב B לגלות את ה-MAC שלו, ואכן אנחנו רואים שהוא מבצע שאילתת ARP ל-IP 192.168.0.1 ומקבל את ה-MAC שכתבנו בסעיף הקודם. |
| תשובה |

1. **חלק 3 – הסנפה ממחשב C**
2. מאיזה מחשב בוצעה ההסנפה? מה כתובת ה-IP וה-MAC שלו?

|  |
| --- |
| 192.168.2.8, 00:0c:6e:00:0c:6e |
| תשובה |

1. האם המחשב נמצא באותו סאבנט כמו מחשבים A ו-B? הסבירו את תשובתכם.

|  |
| --- |
| לא. כבר ראינו שהסאבנט השני הוא 192.168.0.0/24 וכתובת ה-IP של מחשב C לא תואמת. |
| תשובה |

1. עם אילו מחשבים בסאבנט השני מתקשר מחשב C?

|  |
| --- |
| עם מחשב A ועם שרת הווב בכתובת 192.168.0.51. |
| תשובה |

1. לאיזו כתובת MAC מייעד מחשב C את החבילות שמיועדות לסאבנט השני?

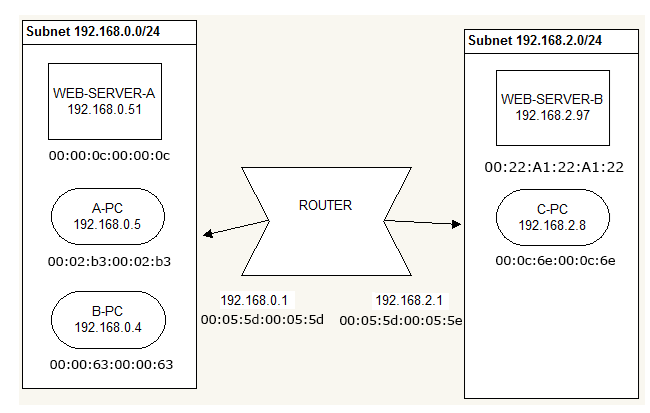
|  |
| --- |
| ל-MAC של הראוטר אותו כבר היכרנו מקודם - 00:05:5d:00:05:5e. |
| תשובה |

1. האם תוכלו להסיק מההסנפה הנוכחית מהו ה-IP של הראוטר (ה-Default Gateway של C)?

|  |
| --- |
| ניתן לראות את כתובת ה-IP מכך שהראוטר שולח בקשת ARP שניתן לראות בהסנפה, בה הוא גם מפרט את כתובת ה-IP שלו. הכתובת היא 192.168.2.1. |
| תשובה |

1. מדוע כתובת ה-IP וה-MAC של הראוטר הן שונות מאלו שגילינו בחלק 2?

|  |
| --- |
| ניתן לראות את כתובת ה-IP מכך שהראוטר שולח בקשת ARP שניתן לראות בהסנפה, בה הוא גם מפרט את כתובת ה-IP שלו. הכתובת היא 192.168.2.1.  ובכן, אנחנו מסניפים כעת מהסאבנט השני ולכן אנחנו רואים את הראוטר מתת רשת שונה, ולכן רואים כרטיס רשת שונה ולכן כתובת MAC שונה!  ובכן, אנחנו מסניפים כעת מהסאבנט השני ולכן אנחנו רואים את הראוטר מתת רשת שונה. לראוטר יש רגל בכל תת רשת וגם כתובת IP שונה בכל תת רשת (לראוטר יש 2 ממשקים רשת = כרטיסי רשת, או יותר). |
| תשובה |

1. **חלק 4 – תמונת הרשת כולה**
2. נסו ליצור שרטוט של הרשת כולה כפי שהצלחתם להבין מההסנפות.   
   מומלץ להשתמש בתוכנת PowerPoint ובקובץ template.pptx המצורף או במצגת של שיעור 8 בה יש שרטוטי רשת רבים.
3. **ליד כל מחשב כתבו את הכתובת (או הכתובות) IP ו-MAC שלו.** ליד כל תת-רשת כתבו את כתובת הסאבנט.
4. שימו לב שבשרטוט שלכם מופיעות כל הישויות אשר ראיתם בהסנפות.
5. צרפו צילום של השרטוט כאן.

|  |
| --- |
| ראינו בהסנפות השונות שהרשת מחולקת לשני סאבנטים – 192.168.0.0/24 וגם 192.168.2.0/24, ובכל תת רשת ישנו שרת HTTP ושני מחשבים. כתובות ה-IP הקיימות ברשת (כולל הכתובות של הראוטר):  192.168.0.1  192.168.0.4  192.168.0.4  192.168.0.51  192.168.2.1  192.168.2.8  192.168.2.97 |
| תשובה |

1. **בונוס**
2. אילו אתרים נמצאים בשני שרתי הווב שבתרגיל? לאילו עמודים גלשו המחשבים שניגשו אליהם? צרפו צילום מסך של עמוד אינטרנט שאחד השרתים העביר לגולשים.  
   רמז: קראו על אופציה של Export HTTP Objects ב-Wireshark.

|  |
| --- |
| גלישות לערכים בוויקיפדיה.  אפשר להוציא את המידע דרך Follow TCP Stream ואפשר גם דרך File->Export Objects->HTTP שמאפשר ממש לשמור קבצים שווירשארק מצא הסנפה. |
| תשובה |