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?

|  |
| --- |
| Mac: 00:00:0c:00:00:0c  Ip: 192.168.0.51 |
| תשובה |

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

|  |
| --- |
| עם מחשב ששמו intel\_00:02:b3, הוא מדבר איתו ב2 פרוטוקולים httpו,tcp ip שלו הוא:192.168.0.5 וmac שלו הוא: 00:02:b3:00:02:b3 |
| תשובה |

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

|  |
| --- |
| כן, כי הם נמצאים באותו סבנט מאסק. |
| תשובה |

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

|  |
| --- |
| הכתובת mac שלו היא: FF:FF:FF:FF:FF:FF ואנו מקבלים את התשובה כי זו כתובת MAC של BROADCAST וכאשר כתובת היא כתובת זו אז היא שולחת את תשובה לכול המחשבים הנמצאים ברשת. |
| תשובה |

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

|  |
| --- |
| היא בוצאה ממחשב ששמו BarcoControl\_00:00:63, וכתובת ip וmac שלו היא 192.168.0.4 ו00:00:63:00:00:63. |
| 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, שני מחשבים נמצאים באותו מחשב בגלל שהוא שולח בקשת ping למחשב שני שנמצא באותו רשת איתו, בנוסף בתוך הפקטה אפשר לראות את הsubnet mask שלו והסבנט מסק היא 255.255.255.0 ואפשר לראות בכך ששניהם נמצאים באותו תת רשת. |
| תשובה |

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

|  |
| --- |
| כן, הוא מדבר עם מחשב שip שלו הוא 192.168.2.8 ומחשב 192.168.2.97. |
| תשובה |

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

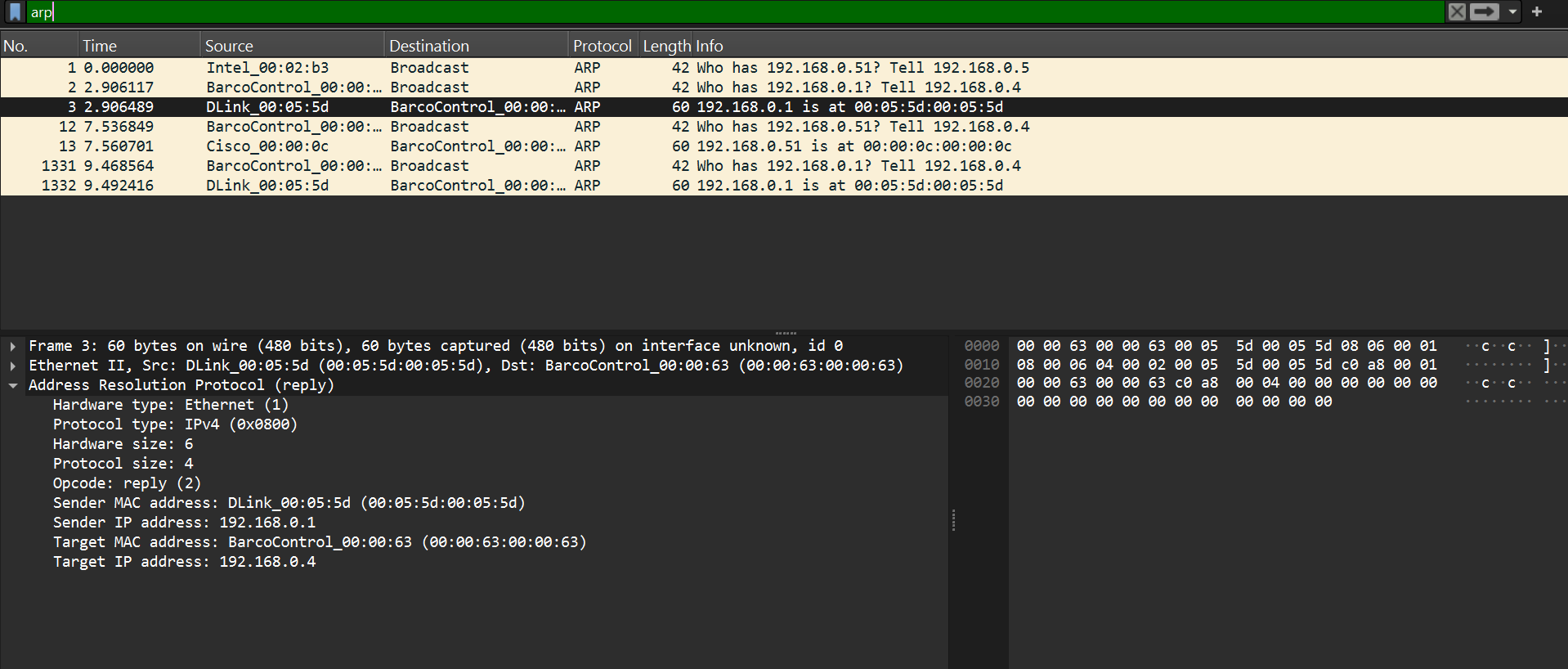
|  |
| --- |
| 00:05:d5:00:05:d5 |
| תשובה |

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

|  |
| --- |
| הם מגיעים מאותו כתובת MAC בגלל שהם נמצאים באותו תת רשת. |
| תשובה |

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

|  |
| --- |
| הכתובת מאק של דיפולט של מחשב ב זה 00:05:5d:00:05:5d, אפשר לראות זות בפקאתות TCP כי בהם איפי היעד הוא נמצאה בסבנט אחר ובגלל שזה סבנט אחר זה מאביר את התשובה לדיפולט גטאבי. |
| 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)

|  |
| --- |
| הכתובת הגאתאוי היא 192.168.0.1. |
| תשובה |

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

|  |
| --- |
| ממחשב ששמו ASUSTekCOMPU\_00:0c:6e, הכתובות שלו הם: 192.168.2.8 ו00:0c:6e:00:0c:6e. |
| תשובה |

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

|  |
| --- |
| לא, כי בשדה השלישי המספר שלו היא לא 0 אך 2. |
| תשובה |

1. עם אילו מחשבים בסאבנט השני מתקשר מחשב C?

|  |
| --- |
| 192.168.0.5 ו 192.168.0.51 |
| תשובה |

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

|  |
| --- |
| 00:05:5d:00:05:5e |
| תשובה |

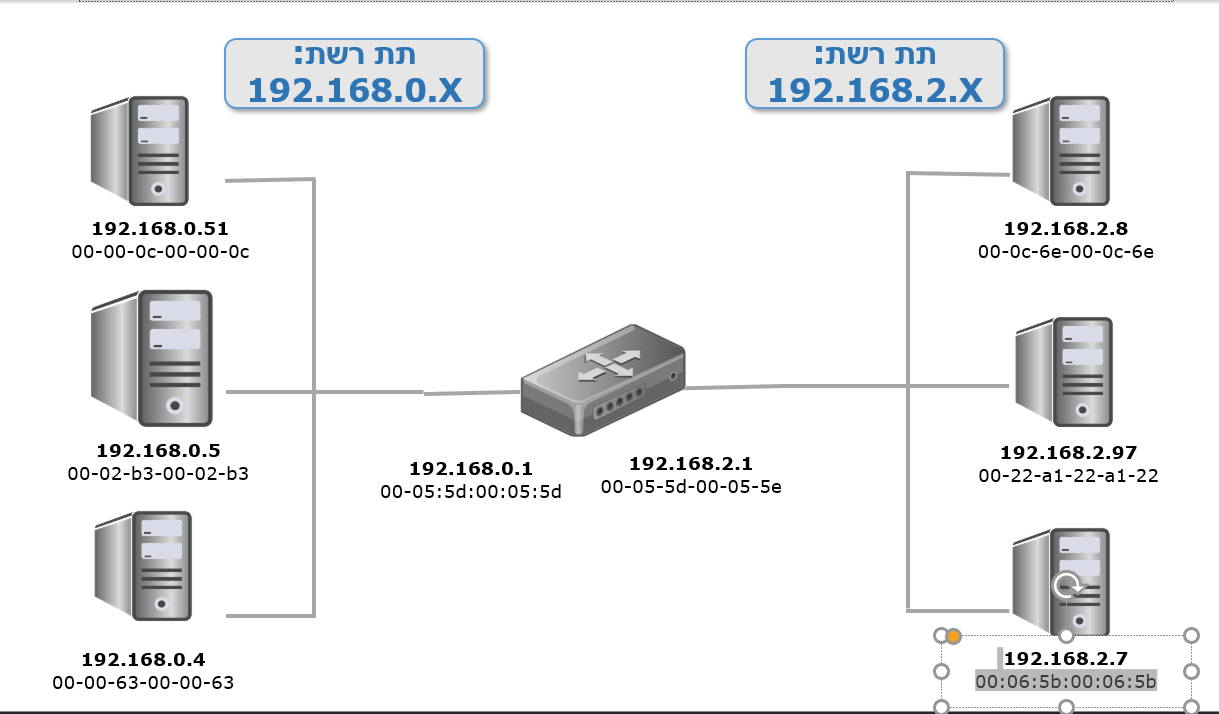
1. האם תוכלו להסיק מההסנפה הנוכחית מהו ה-IP של הראוטר (ה-Default Gateway של C)?

כן, האיפי שלו זה 192.168.2.8.

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

|  |
| --- |
| הן שונות בגלל שהתחברנו לאינטרפיסים שונים של אותו ראוטר. |
| תשובה |

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



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.

|  |
| --- |
|  |
| תשובה |