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?

|  |
| --- |
| 192.168.0.5 , 00:02:b3:00:02:b3 |
| תשובה |

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

|  |
| --- |
| 192.168.0.51 , 00:00:0c:00:00:0c, TCP |
| תשובה |

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

|  |
| --- |
| כן, כי יש לשניהם את הקידומת של רשת פרטית (192.168), וחוץ מזה שואלים ארפ לדברים בסאבנט. |
| תשובה |

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

|  |
| --- |
| ff:ff:ff:ff:ff:ff, כי את הכתובת המאק הזאת כל מחשב מקבל גם אם היא לא לו. בשביל מקרים כאלו... |
| תשובה |

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

|  |
| --- |
| 192.168.0.4 , 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, A וB נמצאות באותו סאבנט, אפילו רואים את הבקשה של A מהשאלה הקודמת.  255.255.255.\* (הכוכבית בסוף לא הצלחתי להפוך נורמלי...), 192.168.0.0/24 |
| תשובה |

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

|  |
| --- |
| כן, 192.168.2.8 ו- 192.168.2.97 מאוחר יותר |
| תשובה |

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

|  |
| --- |
| 00:05:5d:00:05:5d, ו- 00:05:5d:00:05:5d שוב... |
| תשובה |

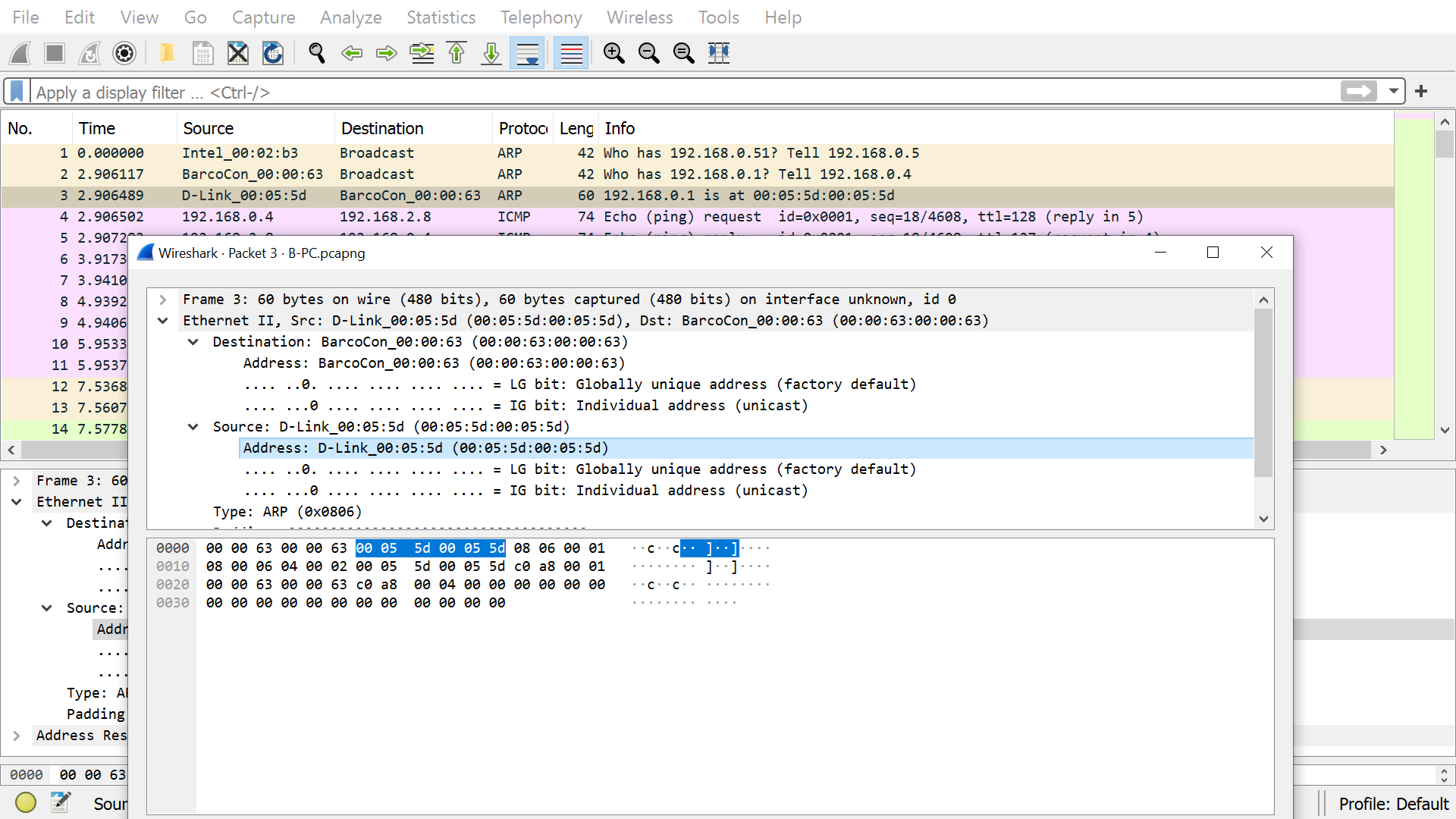
1. כיצד תוכל להסביר שחבילות משני המחשבים הללו מגיעות עם כתובת MAC זהה?

|  |
| --- |
| כי שתיהן עוברות דרך הראוטר שלנו שהכתובת מאק שלו היא זו. |
| תשובה |

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

|  |
| --- |
| 00:05:5d:00:05:5d בגלל ההסבר הקודם, וגם כי זה היה כתוב בהתחלה בארפ |
| 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)



|  |
| --- |
| 192.168.0.1, אחרי שהבנו ש00:05:5d:00:05:5d זה הראוטר, הסתכלתי בהודעה שנותנת לנו את 00:05:5d:00:05:5d וההודעה מצמידה את המאק לIP, כתוב [IP] is at [MAC] |
| 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, הוא נמצא ברשת שכנה (למעלה ואז שוב סאבנט אחר), בעיקר כי יש לו 2 במקום 0 במקום השלישי. |
| תשובה |

1. עם אילו מחשבים בסאבנט השני מתקשר מחשב C?

|  |
| --- |
| 192.168.0.5, 192.168.0.51 |
| תשובה |

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

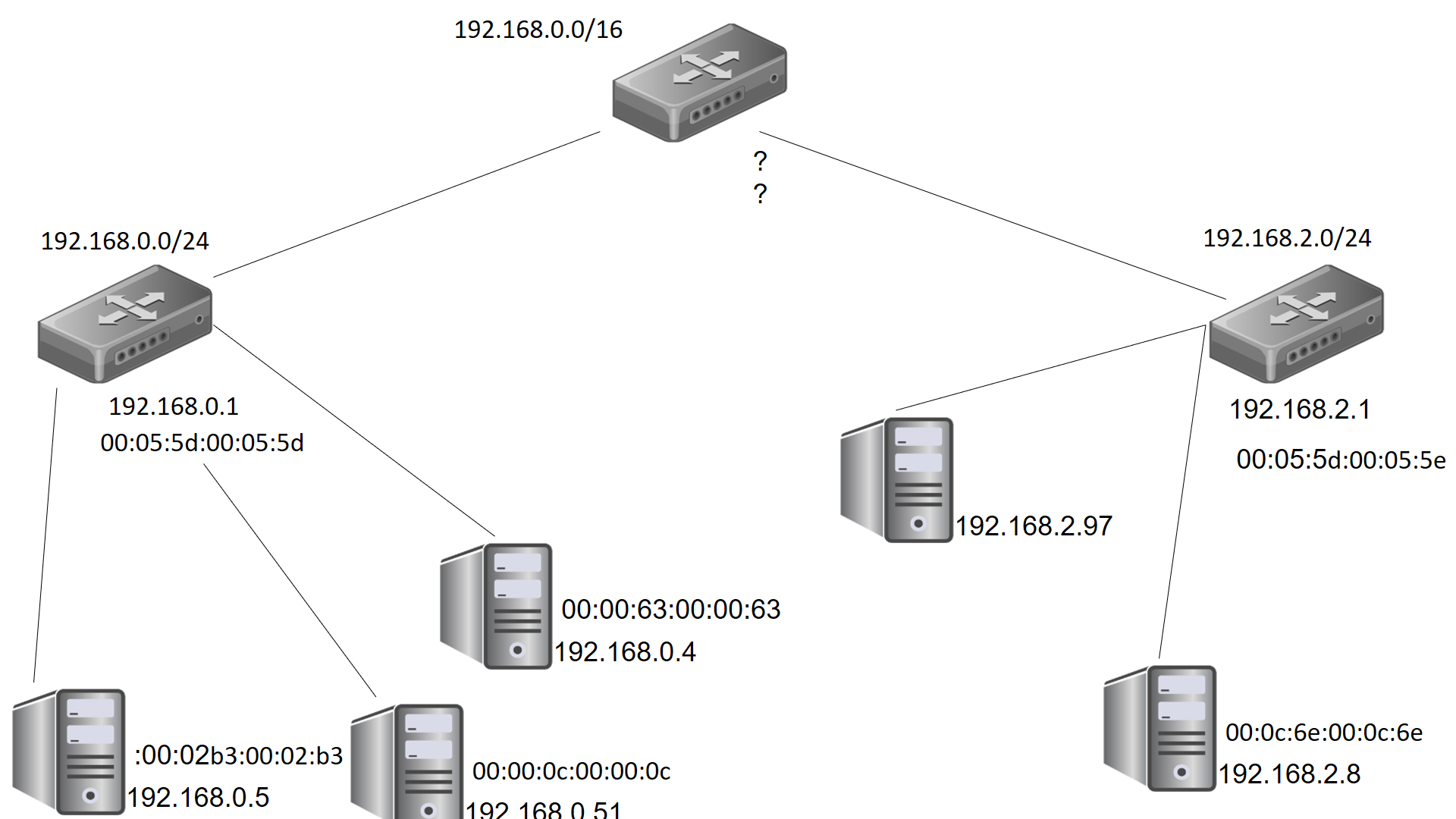
|  |
| --- |
| 00:05:5d:00:05:5e, כנראה כי זה הראוטר |
| תשובה |

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

|  |
| --- |
| 192.168.2.1, כי חוץ מהמבנה הרגיל של הראוטרים שנמצאים ב1 בסאבנט- יש בקשת ארפ ע"י האייפי הזה אלינו וישר אחרי זה מתחילות להגיע אלינו חבילות ממחוץ לסאבנט, יש אחרי מקרה שאנחנו מבקשים את 192.168.2.1 ואחרי שיש לנו אנחנו שולחים חבילות למחוץ לסאבנט |
| תשובה |

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

|  |
| --- |
| כנראה כי זה לא אותו ראוטר, יש ראוטר לסאבנט A, B ויש לC, ששני הראוטרים האלה נמצאים מתחת לאותו הראוטר |
| 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.
4. 
5. **בונוס**
6. 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.

|  |
| --- |
| דברים שקשורים לאחד באפריל, בעיקר RFC's כנראה של ויקיפדיה |
| תשובה |

