Безжични технологии за пренос на данни

Упражнение № 11

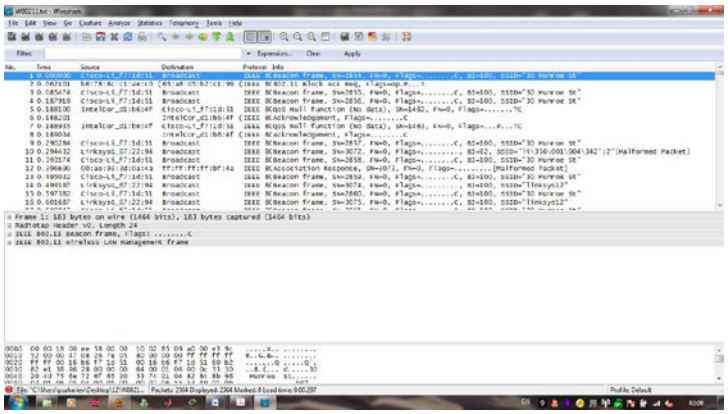
Използване на Wireshark за проследяване на трафика в безжична мрежа.

Цел на упражнението: това упражнение има за цел да предостави възможност за анализиране на реален трафик, предаван в безжична локална мрежа. Студентите ще използват софтуерния продукт Wireshark, който се използва за прихващане и анализиране на данните, предавани в мрежите.

Софтуерното приложение Wireshark е използвано на компютър в мрежа, състояща се от комбинирана точка за достъп/маршрутизатор Linksys 802.11g, два персонални компютъра и един безжичен приемник на персонален компютър свързан към точката за достъп/маршрутизатора. Достъпни са и други точки за достъп в съседство с наблюдаваната. В този проследяващ файл, ще са видими кадри уловени използвайки Канал 6. Тъй като безжичния приемник и точката за достъп, които ни интересуват не са единствените устройства използващи канал 6, ще са видими и много кадри, които не ни интересуват в това упражнение, като кадри-маяци предадени от другите точки за достъп, които също работят на канал 6. От този файл са известни следните характеристики на безжичния потребител:

- Безжичния потребител е свързан с точката за достъп **30 Munroe St**, когато проследяването е започнало.
- Във времевия момент $t = 24.82$, потребителя прави HTTP заявка към http://gaia.cs.umass.edu/wireshark-labs/alice.txt. IP адреса на gaia.cs.umass.edu е 128.119.245.12.
- При $t = 32.82$, потребителя прави HTTP заявка към http://www.cs.umass.edu, чийто IP адрес е 128.119.240.19.
- При $t = 49.58$, потребителя прекратява връзката с точката за достъп **30 Munroe St** и се опитва да се свърже към точката за достъп **lynksys_ses_24086**. Това не е отворена точка за достъп и потребителя не успява да се свърже с нея.
- В $t = 63.0$ потребителя прекратява опитите да се свърже с точката за достъп **lynksys_ses_24086** и се свързва отново с точката за достъп **30 Munroe St**.

Щом заредите файла с данните за проследяване на трафика в Wireshark, използвайки падащото меню File, избирайки Open и след това файла W80211.txt, резултата трябва да изглежда точно като на Фигура 1.



Фиг. 1. Файла с данните за проследяване на трафика в Wireshark.

Кадри маяци.

Припомнете си, че кадри маяци се използват от 802.11 точките за достъп, за да съобщят за своето съществуване в мрежата. За да отговорите на някои от въпросите по-долу, ще трябва да разгледате IEEE 802.11 кадрите и подполетата им в средния прозорец на Wireshark.

1. Какви са SSID-тата на двете точки за достъп, които са генерирали повечето от кадрите маяци?

2. Какви са времевите интервали между предаването на кадрите маяци на точката за достъп **lynksys_ses_24086**? А от точката за достъп **30 Munroe St**? (Съвет: този времеви интервал се съдържа в самия кадър маяк).

3. Какъв (в шестнадесетична бройна система) е MAC адреса на източника, съдържащ се в кадъра маяк от **30 Munroe St**?

4. Какъв (в шестнадесетична бройна система) е MAC адреса на приемника, съдържащ се в кадъра маяк от **30 Munroe St**?

5. Какъв (в шестнадесетична бройна система) е MAC адреса на ID-то на BSS на кадъра маяк от **30 Munroe St**?

6. Кадрите маяци от точката за достъп **30 Munroe St** съдържат информацията, че устройството може да поддържа четири скорости на обмен на информация и осем допълнителни разширени поддържани скорости. Какви са тези скорости?

Прехвърляне на информация.

Тъй като проследяването на трафика започва след като потребителя вече се е свързал с точката за достъп, проследете информацията за предадените данни преди да се разгледа и процеса по осъществяване и разпадане на връзката. Припомнете си, че при $t = 24.82$, потребителя прави **HTTP заявка** към

http://gaia.cs.umass.edu/wireshark-labs/alice.txt. IP адреса на **gaia.cs.umass.edu** е **128.119.245.12**. След това в $t = 32.82$ потребителя прави **HTTP заявка** към **http://www.cs.umass.edu**.

7. Открийте 802.11 кадъра съдържащ **SYN TCP** сегмента за тази първа TCP сесия (посредством която се изтегля alice.txt). В кой момент от време се изпраща **TCP SYN**. Каква информация съдържат трите полета за **MAC** адреси в 802.11 кадъра? Кой MAC адрес в този кадър се използва от безжичния потребител (запишете шестнадесетичния MAC адреса на потребителя), точката за достъп и първия маршрутизатор във връзката (next hop)? Какъв е **IP адреса** на безжичния потребител изпращащ този **TCP** сегмент? Какъв е **IP адреса** на приемника? IP адреса на приемника отговаря ли на този на безжичния потребител, точката за достъп, първия маршрутизатор във връзката или на което и да е друго устройство свързано в мрежата? **Аргументирайте се!**

8. Открийте 802.11 кадъра съдържащ сегмента **SYNACK** за тази TCP сесия. Кога се получава **TCP SYNACK**? Какви са трите полета за MAC адреси в 802.11 кадъра съдържащ **SYNACK** сегмента? Кой MAC адрес в този кадър отговаря на адреса ма потребителя, точката за достъп и първия маршрутизатор по продължение на връзката?

Свързване/разпадане на връзката с безжичния маршрутизатор.

Припомнете си, че всеки потребител трябва първо да свърже с дадена точка за достъп преди да може да изпраща информация. Асоцииране при устройствата поддържащи стандарта 802.11 се изпълнява чрез използването на кадъра **ASSOCIATE REQUEST** (изпратен от потребителя към точка за достъп) и кадъра **ASSOCIATE RESPONSE** (изпратен от точката за достъп към потребителя в отговор на приетия **ASSOCIATE REQUEST**)

9. Изследвайте файла за проследяване на трафика и търсете **AUTHENICATION** кадри изпратени от потребителя към точката за достъп и обратно. Кога се приема първия **AUTHENICATION** кадър изпратен от безжичния потребител към точката за достъп **lynksys_ses_24086 AP** (която има MAC адрес Cisco_Li_f5:ba:bb)? Търсете след $t = 49$?

10. Потребителя изисква ли идентификация посредством ключ или не?

11. Намирате ли отговор на **AUTHENTICATION** заявката от точката за достъп **lynksys_ses_24086**?

12. Разгледайте данните, когато потребителя се откаже (след $t = 63.0$) да се свързва с точката за достъп **lynksys_ses_24086** и започне процеса по асоциация с точката за достъп **30 Munroe St**. Разгледайте **AUTHENTICATION** кадрите изпратени от потребителя към точката за достъп и обратно. Кога се изпращат тези кадри от

потребителя към точката за достъп и кога потребителя получава **AUTHENTICATION** отговор?

13. Продължете с наблюдението на процеса по асоциация между безжичния клиент и точката за достъп **30 Munroe St**, който се осъществява след **t=63.0**. За да се асоциира клиента с точката за достъп се използват **ASSOCIATE** и **ASSOCIATE RESPONSE** кадри. В кой времеви момент се изпраща **ASSOCIATE REQUEST** кадър от потребителя към точката за достъп **30 Munroe St.**? Кога се изпраща и съответния **ASSOCIATE REPLY** кадър? (Можете да използвате филтриране на изразите, използвайки "**wlan.fc.subtype<2** и **wlan.fc.type==0** и **wlan.addr==IntelCor_d1:b6:4f**" за да визуализирате само **ASSOCIATE REQUEST** и **ASSOCIATE REPLY** кадрите).

14. Какви скорости за предаване на данни ще поддържа потребителската станция? А какви точката за достъп? За да отговорите на този въпрос ще трябва да погледнете в полето **parameters** на кадъра за управление на 802.11 безжичните локални мрежи (**802.11 wireless LAN management frame**).

Други видове кадри.

Файла с данните от проследяването на трафика съдържа множество **PROBE REQUEST** и **PROBE RESPONSE** кадри.

15. Вземете предвид първия **PROBE REQUEST** кадър и непосредственият му **PROBE RESPONSE PAIR** кадър, който възниква след **t=2.0** секунди време. Кога се изпращат тези кадри и какви са **MAC адресите** на предавателя, приемника и BSS ID за тези кадри? Какво е предназначението на тези кадри (за домашно ☺)?