Lucrarea de laborator nr.10.
Protocolul wireless 802.11

În acest laborator vom studia protocolul wireless 802.11. Deoarece acest laborator este mai dificil, este bine să studiaţi "*A Technical Tutorial on the 802.11Protocol*" de Pablo Brenner (Breezecom Communications), http://www.sss-mag.com/pdf/802_11tut.pdf , şi "*Understanding 802.11 Frame Types*" de Jim Geier, http://www.wi-fiplanet.com/tutorials/article.php/1447501. De asemenea, este util să consultaţi şi standardul însuşi, "*ANSI/IEEE Std 802.11, 1999 Edition (R2003)*".

Un LAN 802.11 se bazează pe o arhitectură celulară în care fiecare celulă numită BSS (Basic Service Set) este controlată de o staţie de bază numită AP (Access Point). Mai multe celule se pot interconecta prin intermediul unui sistem de distribuţie DS (Distribution System) bazat pe Ethernet, care poate fi el însuşi wireless. Întregul sistem este văzut ca o reţea independentă numită ESS (Extended Service Set).

Ca şi alte protocoale 802.x, protocolul 802.11 acoperă nivelul fizic şi MAC, folosind tehnologiile de acces:

- FHSS (Frequency Hopping Spread Spectrum), în banda 2,4GHz
- DSSS (Direct Sequence Spread Spectrum), în banda 2,4GHz
- Infraroşu

<table>
<tr><td colspan="3">802.2</td><td rowspan="2">Data Link Layer</td></tr>
<tr><td colspan="3">802.11MAC</td></tr>
<tr><td>FHSS</td><td>DSSS</td><td>IR</td><td>PHY Layer</td></tr>
</table>

Protocolul 802.11 beneficiază şi de alte funcţii de nivel superior cum ar fi Fragmentarea, Retransmisia şi Confirmarea.

Metoda de acces de bază definită de nivelul MAC, este CSMA/CA (Carrier Sense Multiple Access width Collision Avoidance).

În toate laboratoarele Wireshark de până acum, am capturat cadre de la o conexiune Ethernet "cu fir". Aici vom captura cadre "de prin aer". Din păcate, majoritatea driverelor dispozitivelor pentru NIC-uri 802.11 (în special pentru Windows) nu oferă posibilitatea de a captura/copia cadrele 802.11 recepţionate în Wireshark. În consecinţă, în acest laborator, veţi folosi un trace propriu. Dacă puteţi captura cadre 802.11, puteţi folosi trace-urile voastre. Sau dacă vreţi să aprofundaţi captura de cadre, vă puteţi cumpăra un mic dispozitiv USB, AirPcap, http://www.cacetech.com , care capturează cadre 802.11 şi oferă suport integrat pentru Wireshark.

1. Modul de lucru

Folosiţi fişierul *Wireshark_802_11.pcap* de pe CD. Acest trace a fost colectat folosind AirPcap şi Wireshark, pe un computer dintr-o reţea, care are un access point/router combinat Linksys 802.11g, cu două PC-uri şi un host wireless ataşat la access point/router. Autorul trace-ului a avut şansa de a beneficia şi de alte access point-uri din casele învecinate. În acest trace, vom vedea cadre capturate pe canalul 6. Deoarece host-ul şi AP-ul care ne interesează nu sunt singurele dispozitive care folosesc canalul 6, vom vedea multe cadre care nu ne interesează în acest laborator, cum ar fi "beacon frames" care sunt anunţate de un AP învecinat care funcţionează şi el pe canalul 6.

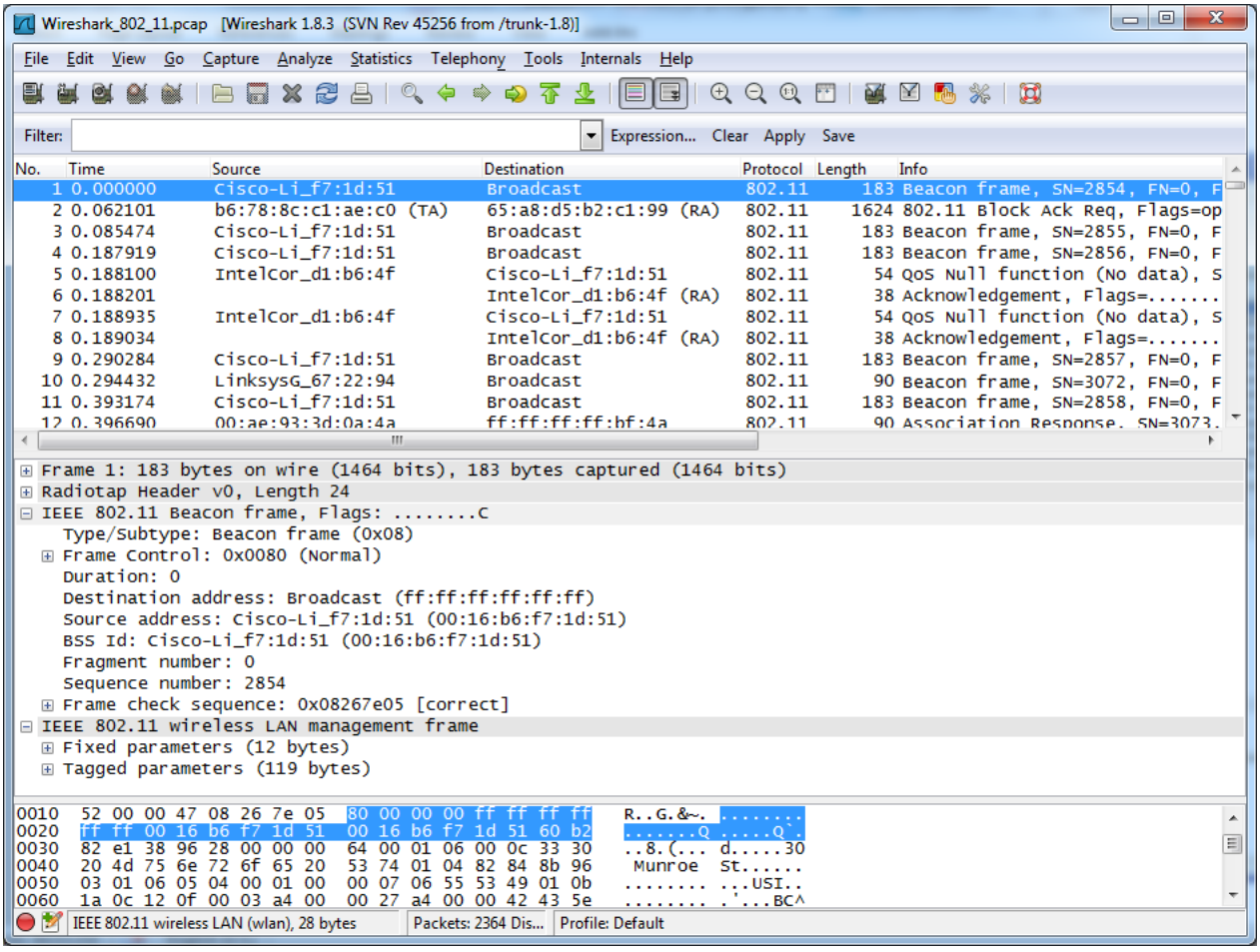

Figura 26 - Cadre "beacon frames" de la un AP învecinat

Activităţile host-ului wireless din acest trace sunt:

- Host-ul este deja asociat cu AP-ul *30 Munroe St* când începe trace-ul.

- La *t=24.82*, host-ul face o cerere. Adresa IP pentru pagina accesată este 128.119.245.12
- La *t=32.82*, host-ul face o cerere HTTP la o altă pagină, a cărei adresă IP este 128.119.240.19.
- La *t=49.58*, host-ul se deconectează de la AP-ul *30 Munroe St* şi încearcă să se conecteze la *Linksys_ses_24086*. Acesta nu este un AP deschis, şi astfel host-ul nu poate să se conecteze la acest AP.

- La *t=63.0*, host-ul renunţă la a încerca să se mai asocieze cu *Linksys_ses_24086 AP*, şi se asociază din nou cu AP-ul *30 Munroe St.*

După ce aţi descărcat trace-ul, îl puteţi încărca în Wireshark.

2. Cadre “beacon” (jalon)

După cum se ştie, cadrele jalon sunt folosite de un AP 802.11, pentru a-şi anunţa existenţa. Pentru a răspunde la întrebările de mai jos, studiaţi detaliile cadrului “IEEE 802.11” şi subcâmpurile ferestrei Wireshark.

1. Care sunt SSID-urile celor două AP-uri care livrează cele mai multe dintre cadrele jalon din acest trace?
2. Care sunt intervalurile de timp dintre transmisia cadrelor jalon ale AP-ului *Linksys_ses_24086*? Dar pentru AP-ul *30 Munroe St.*? (indiciu: acest interval este conţinut chiar în cadrul jalon)
3. Care (în notaţia hexa) este adresa MAC sursă a cadrului jalon din *30 Munroe St.*? Reţineţi că sursa, destinaţia şi BSS-ul sunt 3 adrese folosite într-un cadru 802.11.
4. Care (în notaţia hexa) este adresa MAC destinaţie a cadrului jalon din *30 Munroe St.*?
5. Care (în notaţia hexa) este ID-ul MAC BSS a cadrului jalon din *30 Munroe St.*?
6. Cadrele jalon din AP-ul *30 Munroe St* anunţă faptul că AP-ul poate suporta 4 “data rates” şi 8 “extended support rates” adiţionale. Ce sunt aceste “rates” ?

3. Transferul de date

Deoarece trace-ul începe cu host-ul care este deja asociat cu AP-ul, să ne uităm întâi la transferul de date peste o asociere 802.11, înainte să ne uităm la asocierea/dezasocierea AP. Ştim că în acest trace, la *t=24.82*, host-ul face o cerere HTTP către o pagină web aflată la adresa IP 128.119.245.12. Apoi, la *t=32.82*, host-ul face o cerere HTTP către o altă pagină, la adresa 128.119.240.19.

7. Găsiţi cadrul 802.11 care conţine segmentul SYN TCP pentru această primă sesiune TCP (care descarcă alice.txt). Care sunt trei câmpuri de adrese MAC din cadrul 802.11? Care adresă MAC din acest cadru corespunde host-ului wireless (daţi reprezentarea hexa a adresei MAC pentru host)? Dar AP-ului? Dar primului router (first-hop router)? Care este adresa IP a host-ului wireless care trimite acest segment TCP? Care este adresa IP destinaţie? Această adresă IP destinaţie corespunde host-ului, AP-ului, primului router, sau unui altui dispozitiv ataşat la rețea? Justificaţi răspunsul.
8. Găsiți cadrul 802.11 care conţine segmentul SYN ACK pentru această sesiune TCP. Care sunt trei câmpuri de adrese MAC din cadrul 802.11? Care adresă MAC din acest cadru corespunde host-ului? Dar AP-ului? Dar primului router? Adresa MAC a transmiţătorului din cadru corespunde adresei IP a dispozitivului care a trimis segmentul TCP încapsulat în această datagramă?

3. Asociere/Dezasociere

Reţineţi că un host trebuie întâi să se *asocieze* cu un AP înainte de a trimite date. Asocierea în 802.11 se face folosind cadrul ASSOCIATE REQUEST (trimis de la host la AP, cu tipul cadrului 0 şi subtipul 0) şi cadrul ASSOCIATE RESPONSE (trimis de AP către un host cu tipul cadrului 0 şi subtipul 1, ca răspuns unui ASSOCIATE REQUEST primit).

9. Care două acţiuni sunt făcute (de exemplu cadre trimise) de către host în trace-ul imediat după *t=49*, pentru a termina asocierea cu AP-ul *30 Munroe St* care a fost iniţial activ atunci când a început captura trace-ului? (indiciu: una este o acţiune de layer IP, iar alta este de layer 802.11). Privind specificaţiile 802.11, există vreun alt cadru pe care v-aţi fi aşteptat să-l vedeți, dar care nu se vede aici?
10. Priviţi trace-ul şi căutaţi cadrele AUTHENTICATION trimise de la host către AP şi viceversa. Câte mesaje AUTHENTICATION sunt trimise de la host-ul wireless către AP-ul *Linksys_ses_24086* (care are adresa MAC Cisco_Li_f5:ba:bb) care începe în jurul lui *t=49*?

11. Host-ul doreşte ca autentificarea să folosească o cheie, sau să fie deschis?
12. Se vede o replică AUTHENTICATION de la AP-ul *Linksys_ses_24086* în trace?
13. Acum să studiem ce se întâmplă dacă host-ul renunţă la a mai încerca să se asocieze cu AP-ul *Linksys_ses_24086* şi acum încearcă să se asocieze cu AP-ul *30 Munroe St*. Căutaţi cadrele AUTHENTICATION trimise de la host către ţi viceversa. La care momente de timp apare un cadru AUTHENTICATION de la host către AP-ul *30 Munroe St*, şi când apare un răspuns AUTHENTICATION trimis de la acel AP către host? (puteţi folosi expresiile de filtrare "wlan.fc.subtype == 11 si wlan.fc.type == 0 şi wlan.addr == IntelCor_d1:b6:4f" pentru a afişa doar cadrele AUTHENTICATION)
14. Un cadru ASSOCIATE REQUEST şi un cadru ASSOCIATE RESPONSE corespunzător de la AP la host sunt folosite pentru ca hostul să se asocieze cu un AP. La care moment de timp apare un ASSOCIATE REQUEST de la host la AP-ul *30 Munroe St*? Când este trimis cadrul ASSOCIATE REPLY corespunzător? (puteţi folosi expresiile de filtrare wlan.fc.subtype<2 si wlan.fc.type == 0 si wlan.addr == IntelCor_d1:b6:4f pentru a afişa doar cadrele ASSOCIATE REQUEST şi ASSOCIATE RESPONSE)
15. Ce rate de transmisie doreşte host-ul să folosească? Dar AP-ul? Pentru a răspunde la aceste întrebări, trebuie să căutaţi în câmpurile de parametri ai cadrului de management 802.11 wireless LAN.

4. Alte tipuri de cadre

Trace-ul nostru conţine un număr de cadre PROBE REQUEST şi PROBE RESPONSE.

16. Care sunt adresele de BSS ID MAC ale transmiţătorului şi receptorului din aceste cadre? Care este scopul acestor două tipuri de cadre? (este bine să consultaţi aici referinţele online citate în acest laborator).

Cuprins