UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE ENGENHARIA ELÉTRICA

WIRESHARK LAB – REDES SEM FIO

[Universidade Federal de Uberlândia – UFU; Faculdade de Engenharia Elétrica – FEELT; WIRESHARK LAB – REDES SEM FIO referente à disciplina de Redes de Comunicações II, ministrada pelo Prof. Dr. Éderson Rosa da Silva]

LUCAS ALBINO MARTINS 12011ECP022
ALAN NICOLAS DE OLIVEIRA E SILVA 12011ECP025

Uberlândia – MG
2021

Wireshark Lab: 802.11 v6.0

1. Getting Started

Download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the file Wireshark_802_11.pcap. This trace was collected using AirPcap and Wireshark running on a computer in the home network of one of the authors, consisting of a Linksys 802.11g combined access point/router, with two wired PCs and one wireless host PC attached to the access point/router. The author is fortunate to have other access points in neighboring houses available as well. In this trace file, we'll see frames captured on channel 6. Since the host and AP that we are interested in are not the only devices using channel 6, we'll see a lot of frames that we're not interested in for this lab, such as beacon frames advertised by a neighbor's AP also operating on channel 6. The wireless host activities taken in the trace file are:

- **The host is already associated with the *30 Munroe St* AP when the trace begins. At *t = 24.82*, the host makes an HTTP request to http://gaia.cs.umass.edu/wiresharklabs/alice.txt.**
  The IP address of gaia.cs.umass.edu is 128.119.245.12.

- **At *t=32.82, t*he host makes an HTTP request to http://www.cs.umass.edu, whose IP address is 128.119.240.19.**

- **At *t = 49.58,* the host disconnects from the *30 Munroe St* AP and attempts to connect to the *linksys_ses_24086*. This is not an open access point, and so the host is eventually unable to connect to this AP.**

- **At *t=63.0* the host gives up trying to associate with the *linksys_ses_24086 AP,* and associates again with the *30 Munroe St* access point.**

Once you have downloaded the trace, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the Wireshark_802_11.pcap trace file. The resulting display should look just like Figure 1.

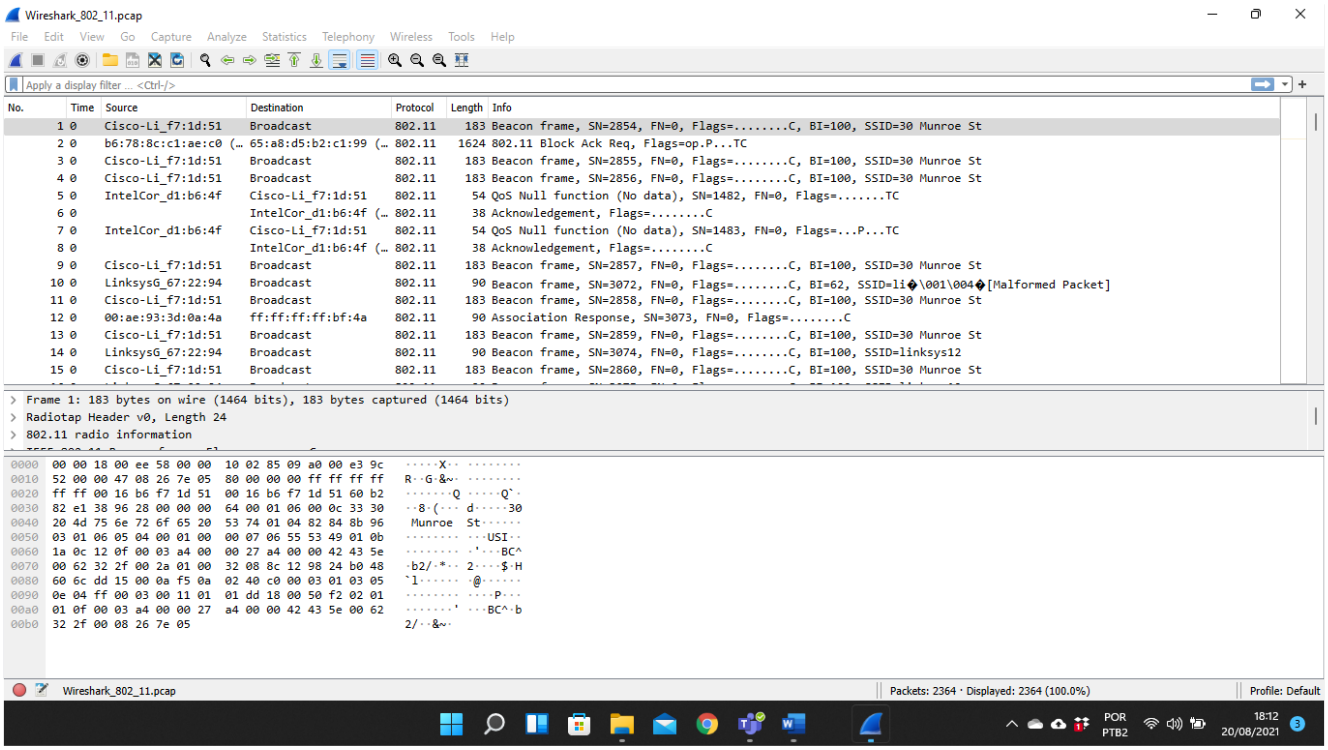

Figura 1: Janela do Wireshark, após abrir o arquivo Wireshark_802_11.pcap

2. Beacon Frames

Recall that beacon frames are used by an 802.11 AP to advertise its existence. To answer some of the questions below, you'll want to look at the details of the "IEEE 802.11" frame and subfields in the middle Wireshark window. Whenever possible, when answering a question below, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout to explain your answer. To print a packet, use *File->Print*, choose *Selected packet only*, choose *Packet summary line,* and select the minimum amount of packet detail that you need to answer the question.

1. **What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?**

   Os dois pontos de acesso estão emitindo a maioria dos quadros de beacon e tem um SSID de “30 Munroe St” e outro “linksys12 referente ao linksys_ses_24086”.

2. **What are the intervals of time between the transmissions of the beacon frames the linksys_ses_24086 access point? From the 30 Munroe St. access point? (Hint: this interval of time is contained in the beacon frame itself).**

   O intervalo dos beacons para ambos os pontos de acesso é relatado no intervalo de beacon do 802.11 Wireless Gerenciador Lan de redes sem fio com frames de 0,1024 segundos, ou seja pouco mais de 100 milissegundos. Observando que os beacon frames do 30 Munroe St AP aparecem com essa regularidade, mas os beacons frames do Linksys_SES_24086 AP não.

3. **What (in hexadecimal notation) is the source MAC address on the beacon frame from 30 Munroe St? Recall from Figure 6.13 in the text that the source, destination, and BSS are three addresses used in an 802.11 frame. For a detailed discussion of the 802.11 frame structure, see section 7 in the IEEE 802.11 standards document (cited above).**

   O endereço MAC de origem é 00:16:b6:f7:1d:51.

4. **What (in hexadecimal notation) is the destination MAC address on the beacon frame from 30 Munroe St??**

   O destino é ff:ff:ff:ff:ff:ff, ou seja, o endereço de transmissão Ethernet.

5. **What (in hexadecimal notation) is the MAC BSS IS on the beacon frame from 30 Munroe St?**

   O MAC BSS IS é 00:16:b6:f7:1d:51, podendo deixar como observação que esse e o mesmo do endereço de origem, já que este é um frame de beacon.

6. **The beacon frames from the 30 Munroe St access point advertise that the access point can support four data rates and eight additional "extended supported rates." What are these rates?**

   Os quatro são 1.0, 2.0, 5.5 e 11.0 Mbps e os oito adicionais são 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0 e 54.0 Mpbs.

3. Data Transfer

Since the trace starts with the host already associated with the AP, let first look at data transfer over an 802.11 association before looking at AP association/disassociation. Recall that in this trace, at *t = 24.82*, the host makes an HTTP request to http://gaia.cs.umass.edu/wireshark-labs/alice.txt. The IP address of gaia.cs.umass.edu is 128.119.245.12. Then, at *t=32.82,* the host makes an HTTP request to http://www.cs.umass.edu.

7. **Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)? To the access point? To the first-hop router? What is the IP address of the wireless host sending this TCP segment? What is the destination IP address? Does this destination IP address correspond to the host, access point, first-hop router, or some other network-attached device?**

O TCP SYN é enviado em t = 24,811093 segundos para a rota. O endereço MAC do host que envia o TCP SYN é 00:13:02:d1:b6:4f. O endereço MAC para o destino, que é o roteador de primeiro salto para o qual o host está conectado é 00:16:b6:f4:eb:a8. O endreço MAC para o BSS é 00:16:b6:f7:1d:51. O endereço IP do host que envia o TCP SYN é 192.168.1.109. Observe que este é um endereço NAT. O endereço de destino é 128.199.245.12. Isso corresponde ao servidor gaia.cs.umass.edu. É importante entender que o MAC de destino do endereço do frame que contém o SYN, é diferente do endereço IP de destino do pacote IP contido neste frame.

8. **Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the host? To the access point? To the first-hop router? Does the sender MAC address in the frame correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram? (Hint: review Figure 5.19 in the text if you are unsure of how to answer this question, or the corresponding part of the previous question. It's particularly important that you understand this).**

O TCP SYNACK é recebido em t = 24,827751 segundos na rota. O MAC address do remetente do 802.11 fram contendo o segmento TCP SYNACK é 00:16:b6:f4:eb:a8, que é o primeiro roteador de salto ao qual o host está conectado. O MAC address do desitno, que é o próprio host é 91:2ª:b0:49:b6:4f, como curiosamente o endereço e diferente do MAC addres do host usado para enviar os frams do TCP SYN. A interface sem fio do host está comportando como se tivesse duas interfaces de endereços. O MAC address do BSS é 00:16:b6:f7:1d:51. O endereço IP do servidor que está enviando o TCP SYNACK é 128.199.245.12 (gaia.cs.umass.edu) e o endereço de destino é 192.168.1.109 (rede wireless do PC).

3. Association/Disassociation

Recall from Section 6.3.1 in the text that a host must first *associate* with an access point before sending data. Association in 802.11 is performed using the ASSOCIATE REQUEST frame (sent from host to AP, with a frame type 0 and subtype 0, see Figure 6.13 in the text) and the ASSOCIATE RESPONSE frame (sent by the AP to a host with a frame type 0 and subtype of 1, in response to a received ASSOCIATE REQUEST). For a detailed explanation of each field in the 802.11 frame, see page 34 (Section 7) of the 802.11 spec at http://gaia.cs.umass.edu/wireshark-labs/802.11-1999.pdf.

9. **What two actions are taken (i.e., frames are sent) by the host in the trace just after t=49, to end the association with the 30 Munroe St AP that was initially in place when trace collection began? (Hint: one is an IP-layer action, and one is an 802.11-layer action). Looking at the 802.11 specification, is there another frame that you might have expected to see, but don't see here?**

   Em t = 49,583615 a liberação do DHCP é enviada pelo host para o servidor DHCP, cujo endereço IP é 192.168.1.1 na rede de onde o host está saindo. Em t = 49,6096617, o host envia um quadro de DESAUTHENTICATION (Frametype = 00 [Management], subframe type 12 [DESAUTHENTICATION]). Logo seria de esperar um pedido de DESAUTHENTICATION ter sido enviado.

10. **Examine the trace file and look for AUTHENICATION frames sent from the host to an AP and vice versa. How many AUTHENTICATION messages are sent from the wireless host to the linksys_ses_24086 AP (which has a MAC address of Cisco_Li_f5:ba:bb) starting at around t=49?**

    A primeira AUTHENICATION do host para o AP é de t = 49.638857.

11. **Does the host want the authentication to require a key or be open?**

O host está solicitando que a associação seja aberta (Authentication Algorithm: Open System).

12. **Do you see a reply AUTHENTICATION from the linksys_ses_24086 AP in the trace?**

Não foi encontrado resposta do AP. Provavelmente porque o AP está configurado para exigir uma chave ao se associar a esse AP, então é provável que o AP ignora solicitações de acesso aberto.

13. **Now let's consider what happens as the host gives up trying to associate with the linksys_ses_24086 AP and now tries to associate with the 30 Munroe St AP. Look for AUTHENICATION frames sent from the host to and AP and vice versa. At what times are there an AUTHENTICATION frame from the host to the 30 Munroe St. AP, and when is there a reply AUTHENTICATION sent from that AP to the host in reply? (Note that you can use the filter expression "wlan.fc.subtype == 11and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" to display only the AUTHENTICATION frames in this trace for this wireless host.).**

Em t = 63.168087 há um frame de AUTHENTICATION enviado de 00:13:02:d1:b6:4f (Host wireless) para o 00:16:b7:f7:1d:51 (BSS). E,t = 63,169071, há um AUTHENTICATION enviado na direção reversa do BSS para o host wireless.

14. **An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to associated with an AP. At what time is there an ASSOCIATE REQUEST from host to the 30 Munroe St AP? When is the corresponding ASSOCIATE REPLY sent? (Note that you can use the filter expression "wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" to display only the ASSOCIATE REQUEST and ASSOCIATE RESPONSE frames for this trace.)**

    Em t = 63169910, há um ASSOCIATE REQUEST frame enviado de 00:13:02:d1:b6:4f (host wireless para o 00:16:b7:f7:1d:51 (BSS). Em t = 63,192101 há uma ASSOCIATE RESPONSE frame enviado na direção reversa do BSS para o host wireless.

15. **What transmission rates is the host willing to use? The AP? To answer this question, you will need to look into the parameters fields of the 802.11 wireless LAN management frame.**

    No frame ASSOCIATION REQUEST as rates suportadas são 1, 2, 5, 5, 11, 6, 9, 12, 18, 24, 32, 48 e 54 Mbps. As mesmas rates também no frame ASSOCIATION RESPONSE.

4. Other Frame types

Our trace contains a number of PROBE REQUEST and PROBE RESPONSE frames.

16. **What are the sender, receiver and BSS ID MAC addresses in these frames? What is the purpose of these two types of frames? (To answer this last question, you'll need to dig into the online references cited earlier in this lab).**

    Em t = 2,297613 há um PROBE REQUEST enviado pela origem 00:12:f0:1f:57:13 com destino ff:ff:ff:ff:ff:ff, e o BSSID para ff:ff:ff:ff:ff:ff. Em t = 2,300697 há uma PROBE RESPONSE enviada pela origem

00:16:b6:f7:1d:51, com destino e a BSSID para 00:!6:b6:f7:1d:51. Um PROBE REQUEST é usado por um host na varredura ativa para encontrar um ponto de acesso. A PROBE RESPONSE é enviada pelo de acesso ao host que está enviando a solicitação.

Referência Bibliográfica

KUROSE, James F. **Redes de computadores e a Internet**: uma abordagem top-down. São Paulo: Pearson Education do Brasil, 2013. xxii, 634 p., il. Inclui bibliografia e índice. ISBN 9788581436777 .