INSTITUTO FEDERAL DE EDUCAÇÃO CIÊNCIA E TECNOLOGIA
DO RIO GRANDE DO NORTE

REDES SEM-FIO

ATIVIDADE DO WIRESHARK

CARLOS HENRIQUE PIRES DOS SANTOS

PARNAMIRIM - RN
2016

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

   SSID's : 30 Munroe St, 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).**

   Beacon Interval: 0.102400 [Seconds]

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).**

   MAC: 00:16:b6:f7:1d:51

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

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

   Cisco-Li_f7:1d:51 00:16:b6:f7:1d:51

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?**

   Suported Rates: 1, 2, 5.5 e 11 Mbps
   Extended Supported Rates: 6,9,12,18,24,36,48,54 Mbps

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? ©2013 Pearson Education, Inc. Upper Saddle River, NJ. All Rights Reserved. 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? Explain.**

   Destino: (00:16:b6:f4:eb:a8) IP: 128.119.245.12

Origem: (00:13:02:d1:b6:4f) IP: 192.168.1.109
Enviando pacote para: (00:16:b6:f7:1d:51) Wireless host (first-hot router)

Um computador quer solicitar uma requisição de um outro computador que também está associado a mesma rede sem fio, assim, o primeiro salto será ao dispositivo sem fio que se encarregará de enviar a solicitação ao destino.

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).**

   Semelhante a questão anterior, computador enviando ack para finalizar a conexão e confirmar o recebimento do pacote.
   Destino: 91:2a:b0:49:b6:4f
   Origem: 00:16:b6:f7:1d:51
   Primeiro Salto: 91:2a:b0:49:b6:4f

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?**

   Primeiro o hospedeiro se desassocia da rede, depois envia uma solicitação de requisição para a nova rede que irá se conectar.

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 Upper Saddle River, NJ. All Rights Reserved. Cisco_Li_f5:ba:bb) starting at around t=49?**

    Foi enviado 2 mensagens na tentativa de se autenticar a rede linksys.

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

    Há a autenticação, contudo, não há nenhuma senha, logo, a rede está aberta.

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

    Não foi encontrado nenhuma resposta do AP ao hospedeiro autenticado, porque a rede está aberta,

portanto não há uma preocupação em confirmar autenticação ou com quem se conecta a ela.

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 == 11 and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" to display only the AUTHENTICATION frames in this trace for this wireless host.).**

    Há uma requisição a rede 30 Munroe no time = 63.168087, e a resposta confirmando a autenticação no time = 63.169071.

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.) .**

    Há uma requisição de autenticação a rede 30 Munroe no time=63.169910, em seguida é enviado uma resposta ao hospedeiro confirmando a autenticação no time=63.192101.

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.**

    As transmissões que podem ser utilizadas são 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48 e 54 Mbps.

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).**

    O hospedeiro enviado os quadros inicialmente para endereço de broadcast para que possa ser encontrado algum AP e em seguida se autenticar.