HO CHI MINH CITY UNIVERSITY OF TECHNOLOGY
FACULTY OF COMPUTER SCIENCE AND ENGINEERING

COMPUTER NETWORK

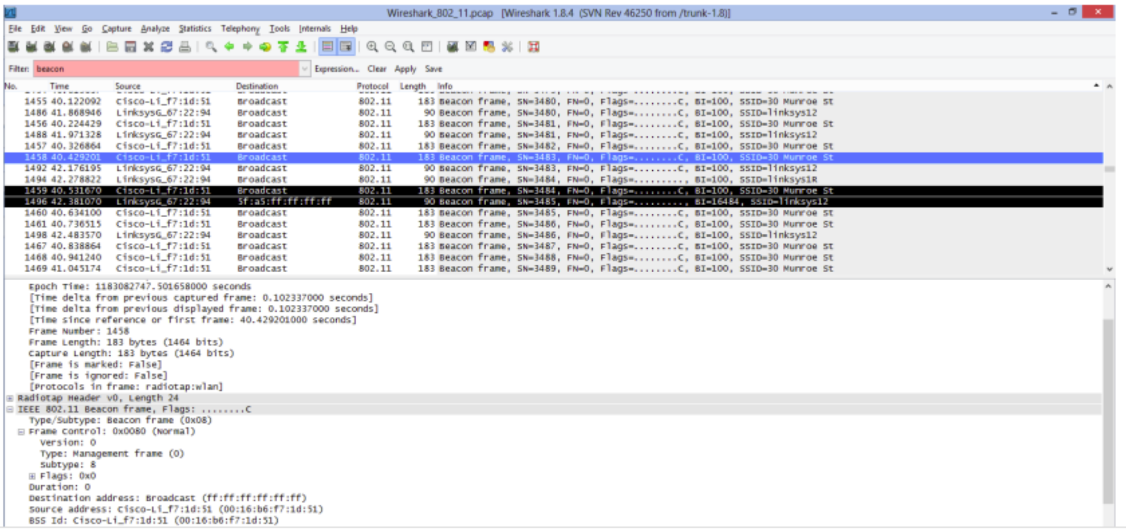
Wireshark Lab 10

Lecturer: Nguyen Le Duy Lai
Author: Vuong Le Huy

June, 2020

Contents

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


Wireshark_802_11.pcap [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: beacon
Expression... Clear Apply Save

```
No.   Time       Source               Destination          Protocol Length Info
 1455 40.122092  Cisco-Li_f7:1d:51    Broadcast            802.11   183 Beacon frame, SN=3480, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
 1486 41.868946  LinksysG_67:22:94    Broadcast            802.11    90 Beacon frame, SN=3480, FN=0, Flags=........C, BI=100, SSID=linksys12
 1456 40.224429  Cisco-Li_f7:1d:51    Broadcast            802.11   183 Beacon frame, SN=3481, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
 1488 41.971328  LinksysG_67:22:94    Broadcast            802.11    90 Beacon frame, SN=3481, FN=0, Flags=........C, BI=100, SSID=linksys12
 1457 40.326864  Cisco-Li_f7:1d:51    Broadcast            802.11   183 Beacon frame, SN=3482, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
 1458 40.429201  Cisco-Li_f7:1d:51    Broadcast            802.11   183 Beacon frame, SN=3483, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
 1492 42.176195  LinksysG_67:22:94    Broadcast            802.11    90 Beacon frame, SN=3483, FN=0, Flags=........C, BI=100, SSID=linksys12
 1494 42.278822  LinksysG_67:22:94    Broadcast            802.11    90 Beacon frame, SN=3484, FN=0, Flags=........., BI=100, SSID=linksys1R
 1459 40.531670  Cisco-Li_f7:1d:51    Broadcast            802.11   183 Beacon frame, SN=3484, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
 1496 42.381070  LinksysG_67:22:94    5f:a5:ff:ff:ff:ff    802.11    90 Beacon frame, SN=3485, FN=0, Flags=........., BI=16484, SSID=linksys12
 1460 40.634100  Cisco-Li_f7:1d:51    Broadcast            802.11   183 Beacon frame, SN=3485, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
 1461 40.736515  Cisco-Li_f7:1d:51    Broadcast            802.11   183 Beacon frame, SN=3486, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
 1498 42.483570  LinksysG_67:22:94    Broadcast            802.11    90 Beacon frame, SN=3486, FN=0, Flags=........C, BI=100, SSID=linksys12
 1467 40.838864  Cisco-Li_f7:1d:51    Broadcast            802.11   183 Beacon frame, SN=3487, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
 1468 40.941240  Cisco-Li_f7:1d:51    Broadcast            802.11   183 Beacon frame, SN=3488, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
 1469 41.045174  Cisco-Li_f7:1d:51    Broadcast            802.11   183 Beacon frame, SN=3489, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
```

```
  Epoch Time: 1183082747.501658000 seconds
  [Time delta from previous captured frame: 0.102337000 seconds]
  [Time delta from previous displayed frame: 0.102337000 seconds]
  [Time since reference or first frame: 40.429201000 seconds]
  Frame Number: 1458
  Frame Length: 183 bytes (1464 bits)
  Capture Length: 183 bytes (1464 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: radiotap:wlan]
⊞ Radiotap Header v0, Length 24
⊟ IEEE 802.11 Beacon frame, Flags: ........C
  Type/Subtype: Beacon frame (0x08)
 ⊟ Frame Control: 0x0080 (Normal)
    Version: 0
    Type: Management frame (0)
    Subtype: 8
  ⊞ Flags: 0x0
  Duration: 0
  Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
  Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
  BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
```

An SSID is a one or two word identifiers of the access point. In this case, Cisco-Li's SSID is 30 Munroe St, and LinksysG_67:22:94's SSID is linksys12.

2 What are the intervals of time between the transmissions of the beacon frames the linksys_ses_24086access point? From the30 Munroe St. access point?

The beacon interval for both access points in reported in the Beacon Interval of the 802.11 wireless LAN Management frame as .1024 seconds (i.e., just over 100 milliseconds). Note that the 30 Munroe St AP beacon frames show up in the trace at this regularity,but the beacons from the linsys_SES_24086 AP do not.

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).3.

The source MAC address on the 30 Munroe St, beacon frame is 00:16:b6:f7:1d:51

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

The destination MAC address on the 30 Munroe St, beacon frame is ff:ff:ff:ff:ff:ff, i.e., the Ethernet broadcast address.

5 What (in hexadecimal notation) is the MAC BSS ISon the beacon framefrom 30 Munroe St?

The MAC BSS ID address on the 30 Munroe St, beacon frame is 00:16:b6:f7:1d:51. Note thatthis is the same as for the source address (since this is a beacon frame)

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

The support rates are 1.0, 2.0, 5.5, 11.0 Mbps. The extended rates are 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0 and 54.0 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? 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

The TCP SYN is sent at t = 24.811093 seconds into the trace. The MAC address for the host sending the TCP SYN is 00:13:02:d1:b6:4f. The MAC address for the destination, which the first hop router to which the host is connected, is 00:16:b6:f4:eb:a8. The MAC address for the BSS is 00:16:b6:f7:1d:51. The IP address of the host sending the TCP SYN is 192.168.1.109. Note that this is a NATed address. The destination address is 128.199.245.12. This corresponds to the server gaia.cs.umass.edu. It is important to understand that the destination MAC address of the frame containing the SYN, is different from the destination IP address of the IP packet contained within this frame. Make sure you understand this distinction! (If you're a bit hazy on this, re-read pages 468 and 469 in the 4th edition of the text).

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 sentthe 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).

The TCP SYNACK is received at t = 24.827751 seconds into the trace. The MAC address for the sender of the 802.11 frame containing the TCP SYNACK segment is00:16:b6:f4:eb:a8, which is the 1st hop router to which the host is attached . The MAC address for the destination, which the host itself, is 91:2a:b0:49:b6:4f. (Curiously, this is different from the MAC address of the host used in the frame that sends the TCP SYN. The host wireless interface is behaving as if it has two interface addresses -interesting!). The MAC address for the BSS is 00:16:b6:f7:1d:51. The IP address of the server sending the TCP SYNACK is 128.199.245.12 (gaia.cs.umass.edu) The destination address is 192.168.1.109 (our wireless PC).

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?

At t = 49.583615 a DHCP release is sent by the host to the DHCP server (whose IP address is 192.168.1.1) in the network that the host is leaving. At t = 49.609617, the host sends a DEAUTHENTICATION frame (Frametype = 00 [Management], subframe type = 12[Deauthentication]). One might have expected to see a DISASSOCIATION request to have been sent.

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 aroundt=49?

The first AUTHENTICATION from the host to the AP is at t = 49.638857

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

The host is requesting that the association be open (by specifying Authentication Algorithm: Open System).

12 Do you see a reply AUTHENTICATION from the linksys$_ses_24086APi$

I can't find any reply from the AP. This is probably because the AP is configured to require a key when associating with that AP, so the AP is likely ignoring (i.e., not responding to) requests for open access.

13 Now let's consider what happens as the host gives up trying to associate with the linksys_ses_24086 APand 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$_d1 : b6 : 4f"todisplayonlytheAUTHENTICATIONframesinthistraceforthisw$

At t = 63.168087 there is a AUTHENTICATION frame sent from 00:13:02:d1:b6:4f (the wireless host) to 00:16:b7:f7:1d:51 (the BSS). At t = 63.169071 there is an AUTHENTICATION from sent in the reverse direction from the BSS to the wireless host.

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 the30 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.)

At t = 63.169910 there is a ASSOCIATE REQUEST frame sent from 00:13:02:d1:b6:4f (the wireless host) to 00:16:b7:f7:1d:51 (the BSS). At t = 63.192101 there is an ASSOCIATE RESPONSE from sent in the reverse direction from the BSS to the wireless host.

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.

In the ASSOCIATION REQUEST frame the supported rates are advertised as 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48, and 54 Mbps. The same rates are advertised in the ASSOCIATION RESPONSE.

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).

At t = 2.297613 there is a PROBE REQUEST sent with source 00:12:f0:1f:57:13, destination: ff:ff:ff:ff:ff:ff, and a BSSID of ff:ff:ff:ff:ff:ff. At t = 2.300697 there is a PROBE RESPONSE sent with source: 00:16:b6:f7:1d:51, destination and a BSSID of 00:16:b6:f7:1d:51. A PROBE REQUEST is used by a host in active scanning to find an Access Point (see Figure 6.9 on page 531 in the text). A PROBE RESPONSE is sent by the access point to the host sending the request.