# EE673 Assignment 4

Adit Jain, 200038

November $26^{th}$, 2023

## 1 Solution 1

1. The two access points that are issuing most of the beacon frames have an SSID of ”30 Munroe St” and ”linsys_SES_24086”.

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

4. 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. The MAC BSS ID address on the 30 Munroe St, beacon frame is *00:16:b6:f7:1d:51*. This is the same as for the source address.

6. The support rates are 1, 2, 5.5 and 11 Mbps. The extended rates are 6, 9, 12, 18, 24, 36, 48 and 54 Mbps.

7. The TCP SYN is sent at $t = 24.811903s$ 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*. This is a NATed address. The destination address is *128.199.245.12*. This corresponds to the server gaia.cs.umass.edu.

8. The TCP SYNACK is received at $t = 24.827751s$ into the trace. The MAC address for the sender of the 802.11 frame containing the TCP SYNACK segment is *00:16: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*. 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* (the wireless PC).

9. At $t = 49.583615s$, 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 $t = 49.609617s$, 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. The first AUTHENTICATION from the host to the AP is at $t = 49.638857s$.

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

12. 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. At $t = 63.168087s$ 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 $t = 63.169071s$ there is an AUTHENTICATION from sent in the reverse direction from the BSS to the wireless host.

14. At $t = 63.169910s$ 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 $t = 63.192101s$ there is an ASSOCIATE RESPONSE from sent in the reverse direction from the BSS to the wireless host.

15. 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. At $t = 2.297613s$ 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 $t = 2.300697s$ 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. A PROBE RESPONSE is sent by the access point to the host sending the request.

# 2 Solution 2

1. The ethernet address of my computer is 00:09:5b:61:8e:6d

2. The destination address *00:0c:41:45:90:a8* is not the ethernet address of gaia.cs.umass.edu. It is the address of the router, which is the link used to get off the subnet.

3. The hex value for the Frame type field is *0x0800.* This corresponds to the IP protocol. The frame type field indicates that the nest layer abpve IP - the layer to which the payload of this Ethernet frame will be passed - is IP.

4. The ASCII ”G” appears 53 bytes from the start of the Ethernet frame. There are 14 B Ethernet frame, and then 20 bytes of IP header followed by 20 bytes of YCP header before the HTTP data is encountered.

5. The source address 00:0c:41:45:90:a8 is neither the Ethernet address of gaia.cs.umass.edu nor the address of the computer. It is the address of the router, which is the link used to get onto the subnet.

6. Yes, the destination address *00:09:5b:61:8e:6d* is the address of the computer.

7. The hex value for the Frame type field is *0x0800*. This value corresponds to the IP protocol.

8. The ASCII "O" appears 53 bytes from the start of the Ethernet frame. Again, there are 14 bytes of Ethernet frame, and then 20 bytes of IP header followed by 20 bytes of TCP header before the HTTP data is encountered.

9. The Internet Address column contains the IP address, the physical address column contains the MAC address, and the type indicates the protocol type.

10. The hex value for the source address is *00:d0:59:a9:3d:68.* The hex value for the destination address is *ff:ff:ff:ff:ff:ff*, the broadcast address.

11. The hex value for the Ethernet Frame type is *0x0806*, for ARP.

12. (a) The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.
    (b) The hex value for opcode field within t he ARP-payload of the request is *0x0001*, for request.
    (c) Yes, the ARP message containing the IP address *192.168.1.105* for the sender.
    (d) The field "Target MAC address" is set to *00:00:00:00:00:00* to question the machine whose corresponding IP address (*192.168.1.1*) is being queried.

13. - The ARP code field begins 20 bytes from the very beginning of the Ethernet frame.
    - The hex value for opcode field within the ARP-payload of the request is *0x0002*, for reply.
    - The answer to the earlier ARP request appears in the "Sender MAC address" field, which contains the Ethernet address *00:06:25:da:af:73* for the sender with IP address *192.168.1.1*

14. The hex value for the source address is *00:06:25:da:af:73* and for the destination is *00:d0:59:a9:3d:68.*

15. There is no reply in this trace, because we are not at the machine that sent the request. The ARP request is broadcast, but the ARP reply is sent back directly to the sender's Ethernet address.