

# EE673 Assignment 4

Adit Jain, 200038

November 26<sup>th</sup>, 2023

## 1 Solution 1 - WiFi Lab

1. The SSIDs issuing the most Beacon frames are:
  - *30 Munroe St*
  - *linksys12*
2. Their respective frequencies are:
  - *2437 MHz*
  - *2437 MHz*
3. Interval: *0.1024 seconds*
4. Source MAC address: *00:16:b6:f7:1d:51*
5. Destination MAC address: *ff:ff:ff:ff:ff:ff*
6. MAC BSS ID: *00:16:b6:f7:1d:51*
7.
  - Support Rates: 1, 2, 5.5 and 11 *Mbps*
  - Extended Rates: 6, 9, 12, 18, 24, 36, 48 and 54 *Mbps*
8.
  - MAC address of the host sending TCP SYN: *00:13:02:d1:b6:4f*
  - MAC address of the destination (also the first hop router): *00:16:b6:f4:eb:a8*
  - MAC of BSS ID: *00:16:b6:f7:1d:51*
  - IP of host sending TCP SYN: *192.168.1.109*
  - IP of destination: *128.119.245.12*
9. The destination IP corresponds to the destined *web-server*
10.
  - Sender MAC address (also the first hop router): *00:16:b6:f4:eb:a8*
  - MAC address of the destination (the host itself): *91:2a:b0:49:b6:4f*
  - MAC address of BSS: *00:16:b6:f7:1d:51*
  - IP address of server: *128.199.245.12*
  - Destination IP address: *192.168.1.109*

11. A DHCP release is sent by the host to the DHCP server (192.168.1.1). The host also sends a DEAUTHENTICATION frame.
  - Frame type = 00 (Management)
  - Subframe type = 12 (Deauthentication)
12. Authentication type requested: *Open System*
13. Authentication SYQ: *0x0001*
14. Yes, the status code is: *Successful (0x0000)*
15. SEQ: *0x0002*
16.
  - AP supported rates: 1, 2, 5.5 and 11 *Mbps*
  - Host: 1, 2, 5.5, 6, 8, 9, 11, 12 *Mbps*
17. Yes, it has the status code: *Successful (0x0000)*
18. Yes, both of them have an extended support rate of 54 *Mbps*

## 2 Solution 2 - ARP Lab

1. Ethernet address of the PC: *c4:41:1e:75:b1:52*
2. Destination address (corresponding to the TP Link router, the first hop router): *00:0c:41:45:90:a8*
3. Corresponding to the IP protocol, the hex value of frame type is *IP (0x0800)*
4. The ASCII "G" appears 52 **bytes** from the start of the Ethernet frame
  - Ethernet frame: 14 *bytes*
  - IP header: 20 *bytes*
  - TCP header: 20 *bytes* (before HTTP data is encountered)
5. Ethernet source address: *00:1e:c1:7e:d9:01*. It is the address of the router, the link used to get onto my computer. It is not that of my PC or the destination
6. Destination address (my computer's): *c4:41:1e:75:b1:52*
7. Hex value (corresponding to IP protocol): *0x0800*
8. The ASCII "O" appears 52 bytes before the start of the Ethernet frame.
  - Ethernet frame: 14 *bytes*
  - IP header: 20 *bytes*
  - TCP header: 20 *bytes* before HTTP data is encountered
9. The data that is the part of the complete HTTP 200 OK response is carried by 4 ethernet frames

10. ARP cache for just one interface:  
*\_gateway (172.20.0.1) at 00:50:e8:04:50:d3 [ether] on wlp0s20f3*
11. Each ARP query contains 3 items:
  - Internet address: IP address
  - Physical address: MAC address
  - Type: Protocol type
12. MAC address of the source: *c4:41:1e:75:b1:52*
13. MAC address of destination (broadcast type message): *ff:ff:ff:ff:ff:ff*
14. Hex value (corresponding to ARP upper layer protocol): *0x0806*
15. ARP opcode starts from 20 *bytes* from the very beginning of the ethernet frame
16. Hex value of opcode field (corresponding to the request): *0x0001 = 1*
17. Yes, sender's IP address: *128.119.247.66*
18.
  - Target MAC address: *00:00:00:00:00:00*
  - Broadcast queries machine with IP address: *128.119.247.1*
19. Opcode for ARP reply is: *0x0002 = 2*
20.
  - Sender IP address: *128.119.247.1*
  - Sender MAC address: *c4:41:1e:75:b1:52*
21. There are multiple ARP request messages but only a single ARP reply message in the trace in response to the ARP queries because the ARP request is broadcast, but the ARP reply is not broadcast. The reply will be sent to the computer who initiated the request directly.