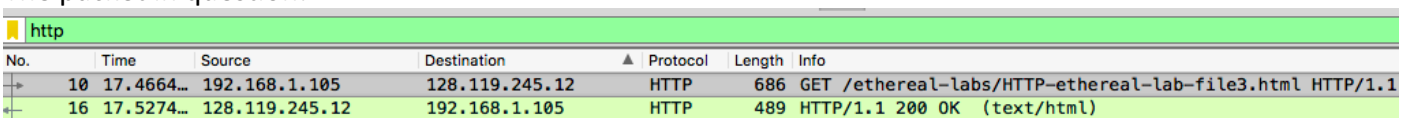
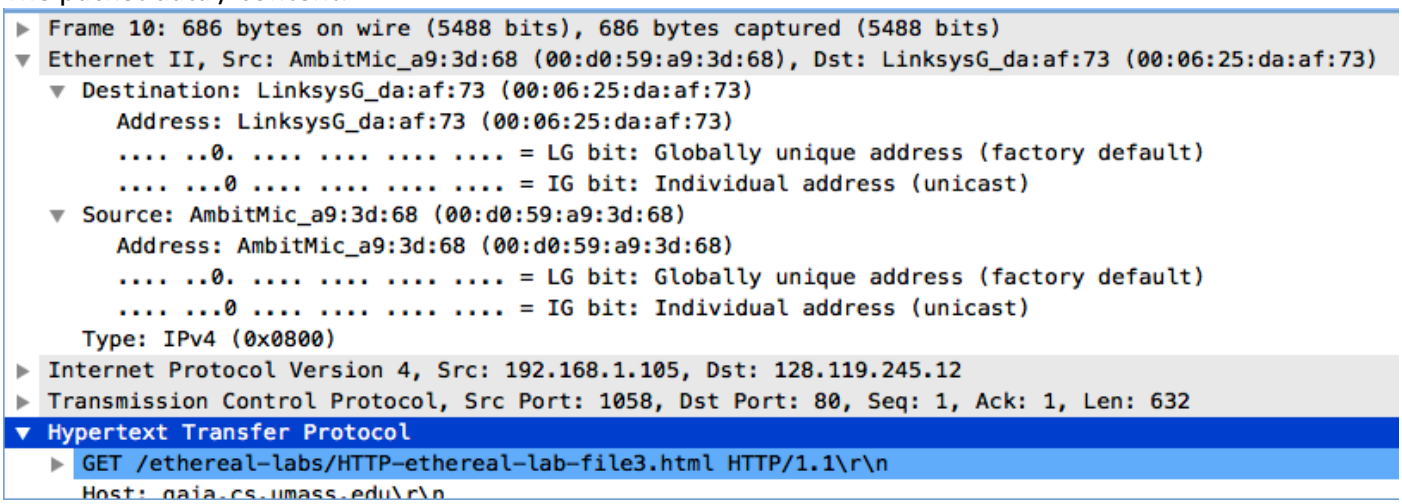
Brian Lam
z5035087

Exercise 1: Using Wireshark to understand Ethernet

The packet in question:



The packet data / content:



Question 1: What is the 48-bit Ethernet address of the source host of this packet?

- 00:d0:59:a9:3d:68

Question 2: What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? If not, then which device has this address?

- 00:06:25:da:af:73
- No, it is most likely the Ethernet address of a link called LinksysG, a router.

Question 3: Give the hexadecimal value for the two-byte Frame type field.

- 0x0800

Question 4: **How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame? Note that when you examine the Data portion of this frame, it actually consists of both the Ethernet frame headers as well as the payload (i.e. bottom window in Wireshark shows the entire 686 byte frame that is captured). Of the bytes preceding the G, the first few bytes are the Ethernet frame header. Does this include the preamble bytes, or are those bytes omitted from the capture? Given this, how many bytes of frame header are present? What are the remainder of the bytes before the G?**

- It follows position 0x36 = 54 bytes from the very start of the Ethernet frame until the ASCII "G" appears.
- The Ethernet frame header omits the preamble bytes from capture.
- 14 bytes are present in the Ethernet frame header
- The remaining bytes are the IP and TCP layer headers, with a total of 20+20 bytes.

Now looking at the HTTP response packet:

```
▼ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  ▼ Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▼ Source: LinksysG_da:af:73 (00:06:25:da:af:73)
      Address: LinksysG_da:af:73 (00:06:25:da:af:73)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

Question 5: What is the value of the Ethernet source address? Is this the address of the host that sent the GET HTTP request, or of gaia.cs.umass.edu? If not then which device has this address?

- Ethernet source address = 00:06:25:da:af:73
- No it is not the same address as the host that sent the GET HTTP request or address of gaia.cs.umass.edu.
- The device that has the address is LinksysG.

Question 6. What is the destination address in the Ethernet frame? Is this the Ethernet address of the source host that sent the earlier GET HTTP request?

- Destination address of the Ethernet frame is 00:d0:59:a9:3d:68
- Yes it is the same Ethernet address of the source host in the HTTP GET request.

Question 7. How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" (i.e., the HTTP response code) appear in the Ethernet frame?

- Preceding ASCII "O" is position 13 = 13 bytes from the start of the Ethernet frame

Exercise 2: Using Wireshark to understand ARP

Now looking at the first two frames in the trace:

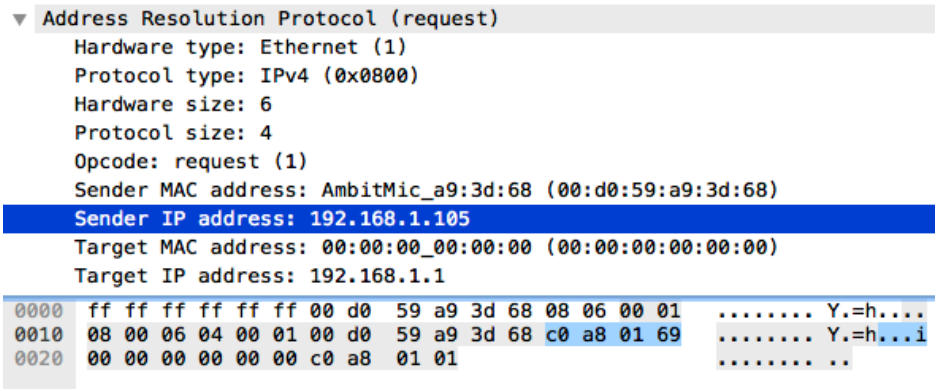
```
▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▼ Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▼ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  ▼ Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
▶ Address Resolution Protocol (request)
```

Question 1. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message? Is there something special about the destination address?

- Hex source = 00:d0:59:a9:3d:68
- Hex dest = ff:ff:ff:ff
- The dest address is a broadcast address sent to all hosts on the network.

Question 2. Give the hexadecimal value for the two-byte Ethernet Frame type field.

- Hex value = 0x0806



Question 3: How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?

- Opcode field begins after position 0x0e from the frame = 14 bytes

Question 4. What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

- Value is 0x001 = 1

Question 5. Does the ARP message contain the IP address of the sender?

- Yes, it contains the IP address of 192.168.1.105

Question 6. Where in the ARP request does the "question" appear? By "question", I mean the IP address for which the mapping is being requested.

- It appears in the Target IP field, with an address of 192.168.1.1

Question 7. How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?

- Same question as before? It appears after pos 0x0e = 14 bytes from the beginning of the Ethernet frame

Question 8. What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

- Opcode value = 0x0002 = 2 in the response frame.

Question 9. Where in the ARP message does the "answer" to the earlier ARP request appear – the Ethernet address of the machine whose corresponding IP address is being queried?

- The "answer" to the "question" earlier appears in the Sender MAC address.

Question 10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

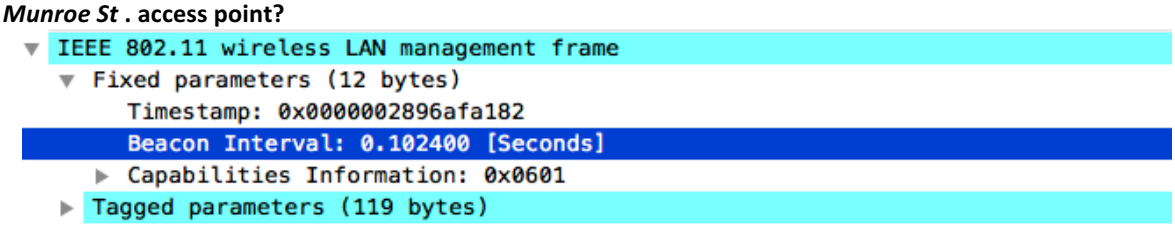
- Hex source = 00:06:25:da:af:73
- Hex dest = 00:d0:59:a9:3d:68

Exercise 3: Using Wireshark to understand 802.11

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

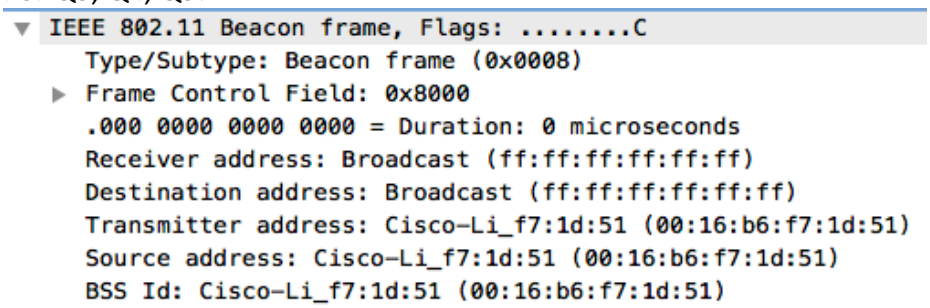
- It seems like **30 Munroe St** access point is issuing the most beacon frames in this trace.
- Other than that, there are some beacon frames issued by a **linksys12** access point.

Question 2. What are the intervals of time between the transmission of the beacon frames the *linksys* access point? From the *30 Munroe St* . access point?



- As shown above, **beacon interval = 0.1024 seconds** between transmission of beacon frames for seemingly all the frames in the trace.

For Q3, Q4, Q5:



Question 3. What (in hexadecimal notation) is the source MAC address on the beacon frame from *30 Munroe St*?

- MAC source = 00:16:b6:f7:1d:51

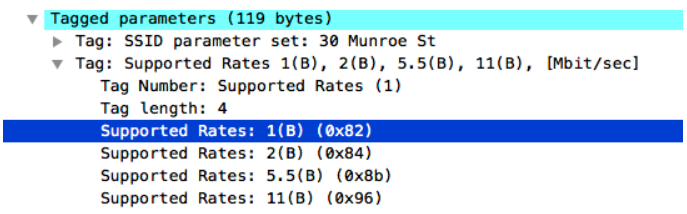
Question 4. What (in hexadecimal notation) is the destination MAC address on the beacon frame from *30 Munroe St* ?

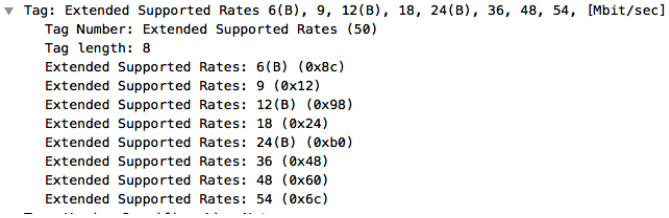
- MAC dest = ff:ff:ff:ff

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

- MAC BSS id = 00:16:b6:f7:1d:51

Question 6. The beacon frame 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?

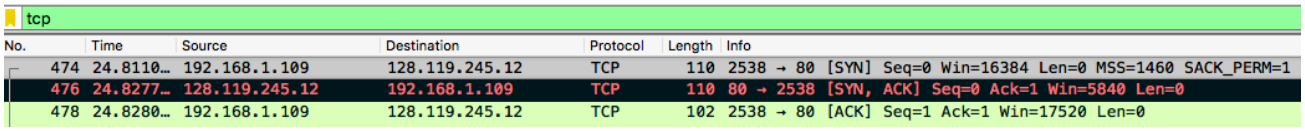




- The four supported data rates: 1, 2, 5.5, 11 Mbits/s
- The eight extended supported rates are: 6, 9, 12, 18, 24, 36, 48, 54 Mbits/s

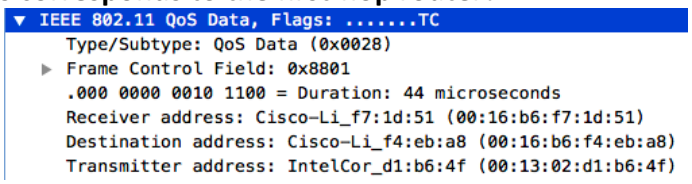
Question 7. At what time is the TCP SYN sent?

- The handshake:



- The TCP SYN segment was sent at 24.811093 seconds

Question 8. What are the three MAC address fields in the 802.11 frame that encapsulates the TCP SYN segment? Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)? Which address corresponds to the access point? Which address corresponds to the first-hop router?

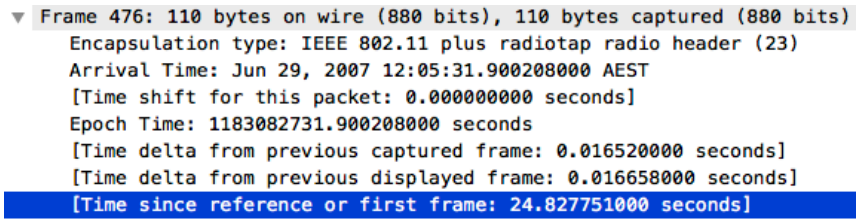


- The Receiver, Destination and Transmitter addresses
- The host = Transmitter Address = **00:13:02:d1:b6:4f**
- The AP = Receiver Address = **00:16:b6:f7:1d:51**
- The first-hop router = Destination Address = **00:16:b6:f4:eb:a8**

Question 9. What is the IP address of the wireless host sending this TCP segment? What is the destination IP address? Does the destination IP address correspond to the host, access point, first-hop router, or some other network-attached device? Explain.

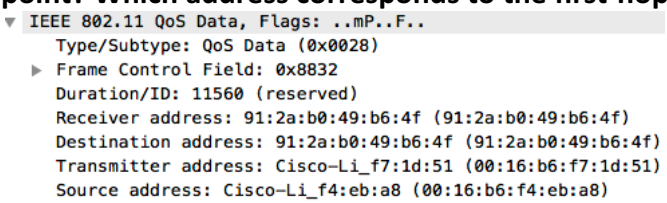
- Host IP = 192.168.1.198
- Dest IP = 128.119.245.12

Question 10. At what time is the TCP SYNACK received?



- The TCP SYNACK segment was received at **24.827751 seconds** since the first frame

Question 11. What are the three MAC address fields in the 802.11 frame that encapsulates the SYNACK? Which MAC address in this frame corresponds to the wireless host? Which address corresponds to the access point? Which address corresponds to the first-hop router?



- Receiver, Transmitter, Source fields as in the TCP SYN segment
- Wireless Host = Receiver address = 91:2a:b0:49:b6:f4
- AP = Transmitter address = 00:16:b6:f7:1d:51
- First-Hop = Source address = 00:16:b6:f4:eb:a8

Question 12. 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?

- No it does not correspond