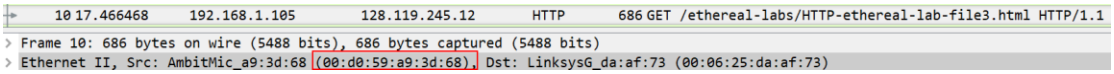
Exercise 1:

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

Answer:

The 48-bit Ethernet address of the source host of this packet**: 00:d0:59:a9:3d:68**

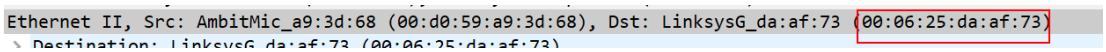


Question 2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? If not, then which device has this address? (Note: this is an important question, and one that students sometimes get wrong. You may want to refer back to relevant parts of the text and lecture notes and make sure you understand the answer here.)

Answer:

The 48-bit destination address in the Ethernet frame: **00:06:25:da:af:73**

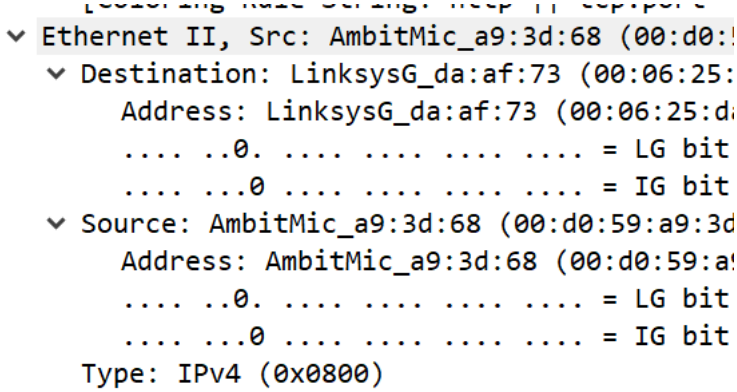
This is **not** the Ethernet address of gaia,cs,umass.edu. This is the **first hop router**.



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

Answer:

The hexadecimal value for the two-byte Frame type field is **0x0800.**



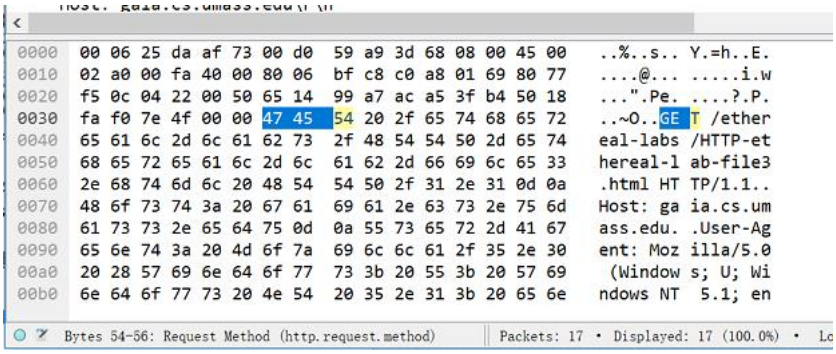
Question 4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame? Note that when you examine the Data portion of this frame, it actually consists of both the Ethernet frame headers as well as the payload (i.e. bottom window in Wireshark shows 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?

Answer:

54 bytes.

It **does not** include the preamble bytes, which are not captured by Wireshark.

First 14 bytes show the Ethernet frame header. Next 20 bytes is IP header and 20 bytes following is TCP headers.



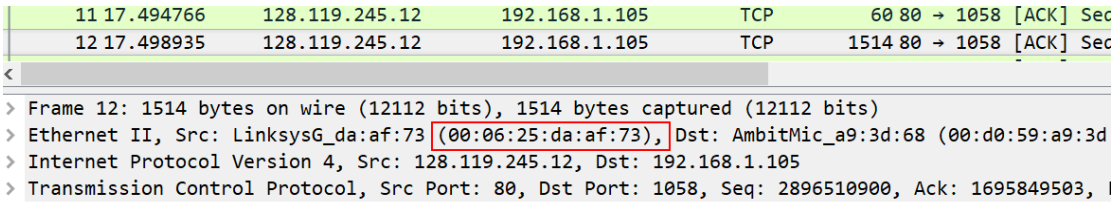
Question 5. What is the value of the Ethernet source address? Is this the address of the host that sent the GET HTTP request, or of gaia.cs.umass.edu? If not then which device has this address?

Answer:

The source Ethernet address for this frame is **00:06:25:da:af:73**.

This is neither the Ethernet address of gaia.cs.umass.edu nor the source host.

This is **the first hop router** from the source host.

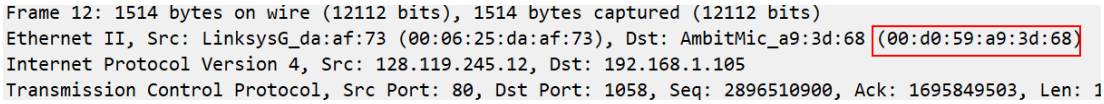


Question 6. What is the destination address in the Ethernet frame? Is this the Ethernet address of the source host that sent the earlier GET HTTP request?

Answer:

The destination address of the frame is **00:d0:59:a9:3d:68.**

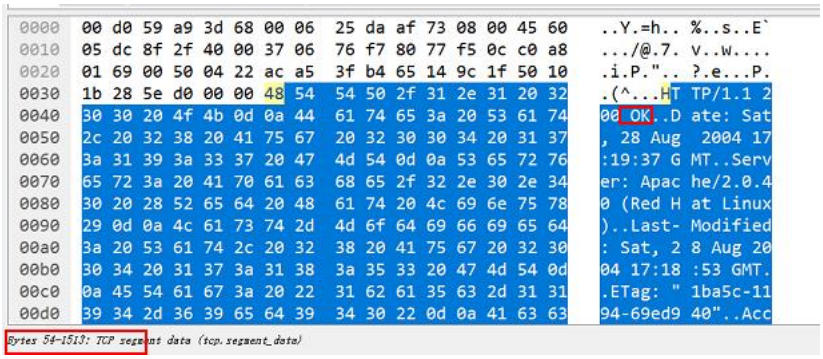
This is the Ethernet address of the source host that sent the earlier GET HTTP request.



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?

Answer:

67 bytes



Exercise 2:

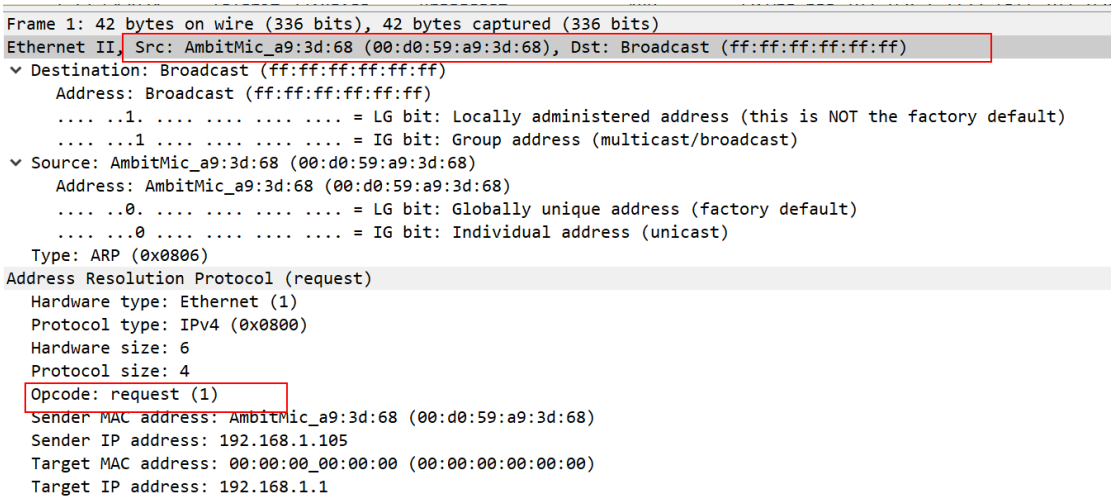
Question1. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message? Is there something special about the destination address?

Answer:

Source address: **00:d0:59:a9:3d:68**

Destination address: **ff:ff:ff:ff:ff:ff**

Because this is the broadcast, it is ff:ff:ff:ff:ff:ff. When the target node address is specified as FFFFFFFFFFFF, the packet is intended to be received by all hosts in the network.



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

Answer:

0x0806, ARP

```
Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0
  Destination: Broadcast (ff:ff:ff:ff:ff:
      Address: Broadcast (ff:ff:ff:ff:ff:ff
      .... ..1. .... .... .... .... = LG bi
      .... ...1 .... .... .... .... = IG bi
  Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3
      Address: AmbitMic_a9:3d:68 (00:d0:59:
      .... ..0. .... .... .... .... = LG bi
      .... ...0 .... .... .... .... = IG bi
  Type: ARP (0x0806)
```

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

Answer:

20 bytes

```
000  ff ff ff ff ff ff 00 d0  59 a9 3d 68 08 06 00 01   ........ Y.=
010  08 00 06 04 00 01 00 d0  59 a9 3d 68 c0 a8 01 69   ........ Y.=
020  00 00 00 00 00 00 c0 a8  01 01                     ........ ..

Bytes 20-21: Opcode (arp.opcode)
```

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?

Answer:

The value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made is **1.**

```
Protocol size: 4
Opcode: request (1)
Sender MAC address: Ambi
```

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

Answer:

Yes, it contains the IP address of the sender.

```
Protocol size: 4
Opcode: request (1)
Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
Sender IP address: 192.168.1.105
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.1.1
```

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.

Answer:

In target MAC address,

```
Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
Sender IP address: 192.168.1.105
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.1.1
```

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

Answer:

20 bytes

```
Protocol size: 4
Opcode: reply (2)
Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
00  00 d0 59 a9 3d 68 00 06  25 da af 73 08 06 00 01    ..Y.=h.. %..s...
10  08 00 06 04 00 02 00 06  25 da af 73 c0 a8 01 01    ........ %..s...
20  00 d0 59 a9 3d 68 c0 a8  01 69 00 00 00 00 00 00    ..Y.=h.. .i......
Opcode (arp.opcode), 2 bytes
```

```
Opcode: reply (2)
Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
00  00 d0 59 a9 3d 68 00 06  25 da af 73 08 06 00 01    ..Y.=h.. %..s....
10  08 00 06 04 00 02 00 06  25 da af 73 c0 a8 01 01    ........ %..s....
20  00 d0 59 a9 3d 68 c0 a8  01 69 00 00 00 00 00 00    ..Y.=h.. .i......
Bytes 20-21: Opcode (arp.opcode)
```

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?

Answer:

The value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made is **2.**

```
Opcode: reply (2)
Sender MAC address: LinksysG_d
Sender IP address: 192.168.1.1
```

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?

Answer:

Sender MAC Address

```
Opcode: reply (2)
Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
Sender IP address: 192.168.1.1
Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
Target IP address: 192.168.1.105
```

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

Answer:

Source Address: **00:06:25:da:af:73**

Destination Address: **00:d0:59:a9:3d:68**

```
> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
    Sender IP address: 192.168.1.1
    Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Target IP address: 192.168.1.105
```

Exercise 3

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

Answer:

SSID of Cisco-Li_f7:1d:51： **30 Munroe St,**

SSID of LinksysG_67:22:94: **linksys12.**

32	1.314223	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2868, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
33	1.416593	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2869, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
34	1.420565	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3083, FN=0, Flags=....., BI=20580, SSID=linksys12

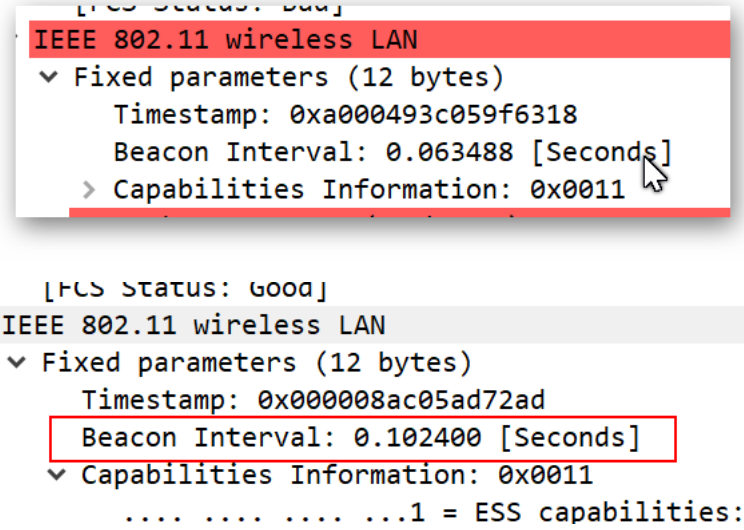
Question 2. What are the intervals of time between the transmission of the beacon frames the linksys access point? From the 30 Munroe St . access point? (Hint: this interval of time is contained in the beacon frame itself).

Answer:

linksys：

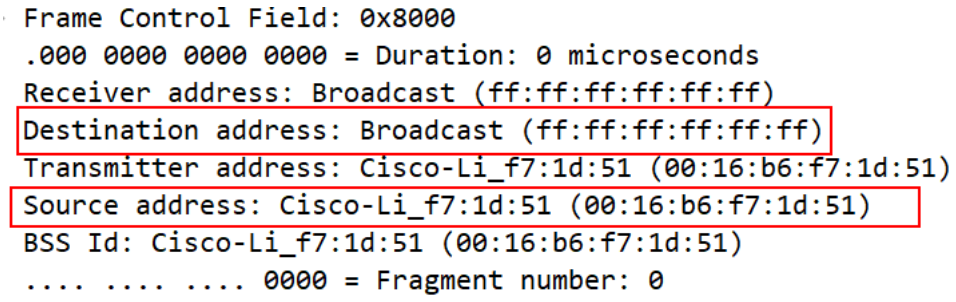
Most are 0.1024 seconds，one is 0.063488 seconds.

30 Munroe St:
0.1024 seconds



Question 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 80.11 standards document (cited above).

Answer:
The source MAC address on the beacon frame from 30 Munroe St is **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 ?

Answer:
The destination MAC address on the beacon frame from 30 Munroe St is **ff:ff:ff:ff:ff:ff.**

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

Answer:

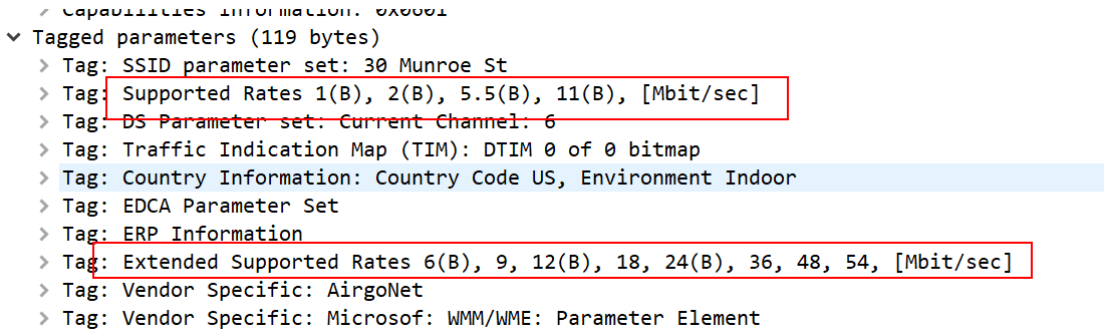
The MAC BSS id on the beacon frame from 30 Munroe St is **Cisco-Li-f7:1d:51 (00:16:b6:f7:1d:51)**

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?

Answer:

Data rates: 1(B), 2(B), 5.5(B), 11(B) [Mbit/sec]

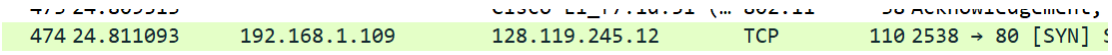
Extended supported rates: 6(B), 9, 12(B), 18, 24(B), 36, 48 and 54 [Mbit/sec]



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

Answer:

At time, t=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?

Answer:

Three MAC address fields: 00:16:b6:f7:1d:51 ,00:16:b6:f4:eb:a8, 00:13:02:d1:b6:4f.

wireless host: 00:13:02:d1:b6:4f.

access point: 00:16:b6:f7:1d:51

first-hop router: 00:16:b6:f4:eb:a8

```
Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
```

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. (Hint: review Figure 5.19 in the text if you are unsure how to answer this and later questions)

Answer:

The IP address of the wireless host sending the TCP SYN **:192.168.1.109.**

The destination address: **128.199.245.12.** It corresponds to the **server(gaia.cs.umass.edu)**

```
Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12
```

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

Answer:

At time, t=24.827751 seconds.

476	24.827751	128.119.245.12	192.168.1.109	TCP	110 80 → 2538 [SYN, ACK] S

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 (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?

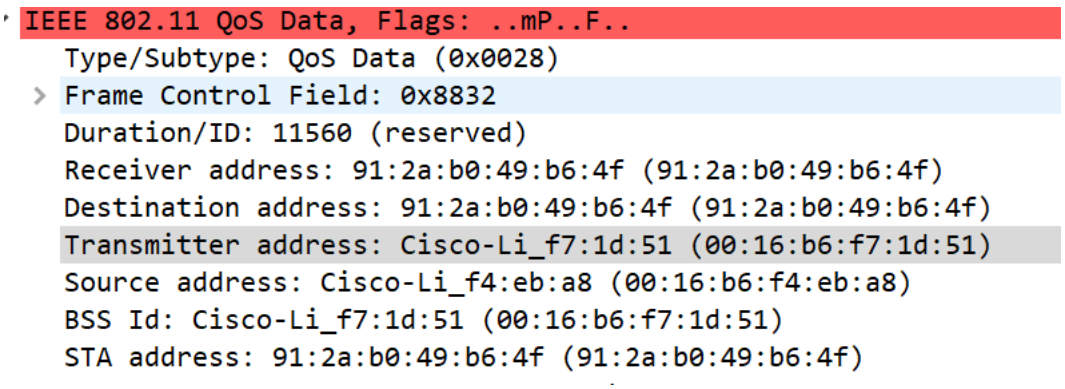
Answer:

Three MAC address fields: 91:2a:b0:49:b6:4f, 00:16:b6:f7:1d:51, 00:16:b6:f4:eb:a8

wireless host: 00:16:b6:f4:eb:a8

access point: 00:16:b6:f7:1d:51

first-hop router: 91:2a:b0:49:b6:4f



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?

Answer:

Yes, the source address is server(gaia.cs.umass.edu). The destination address is our wireless PC.