

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**

```
10.17.466468 192.168.1.105 128.119.245.12 HTTP 686 GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)
> Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
```

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**.

```
Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
  Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
```

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**.

```
10.17.466468 192.168.1.105 128.119.245.12 HTTP 686 GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
v Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
  Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
    Address: LinksysG_da:af:73 (00:06:25:da:af:73)
      .... ..0. .... = LG bit
      .... ..0 .... = IG bit
  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
      .... ..0 .... = IG bit
  Type: IPv4 (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.

Offset	Hex	ASCII
0000	00 06 25 da af 73 00 d0 59 a9 3d 68 08 00 45 00	..%..S.. Y.=h..E.
0010	02 a0 00 fa 40 00 80 06 bf c8 c0 a8 01 69 80 77@... ..i.W
0020	f5 0c 04 22 00 50 65 14 99 a7 ac a5 3f b4 50 18	...".Pe.?.P.
0030	fa f0 7e 4f 00 00 47 45 54 20 2f 65 74 68 65 72	..~O..GET /ether
0040	65 61 6c 2d 6c 61 62 73 2f 48 54 54 50 2d 65 74	eal-labs /HTTP-et
0050	68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 33	hereal-l ab-file3
0060	2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a	.html HT TP/1.1..
0070	48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d	Host: ga ia.cs.um
0080	61 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67	ass.edu. .User-Ag
0090	65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30	ent: Moz illa/5.0
00a0	20 28 57 69 6e 64 6f 77 73 3b 20 55 3b 20 57 69	(Window s; U; Wi
00b0	6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b 20 65 6e	ndows NT 5.1; en

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.

Source IP	Destination IP	Protocol	Source Port	Destination Port	Sequence	Length
11 17.494766	128.119.245.12	TCP	60 80	1058	[ACK]	Sec
12 17.498935	128.119.245.12	TCP	1514 80	1058	[ACK]	Sec

> Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 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)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.105
> Transmission Control Protocol, Src Port: 80, Dst Port: 1058, Seq: 2896510900, Ack: 1695849503, Len: 1

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.

Source IP	Destination IP	Protocol	Source Port	Destination Port	Sequence	Length
11 17.494766	128.119.245.12	TCP	60 80	1058	[ACK]	Sec
12 17.498935	128.119.245.12	TCP	1514 80	1058	[ACK]	Sec

> Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 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)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.105
> Transmission Control Protocol, Src Port: 80, Dst Port: 1058, Seq: 2896510900, Ack: 1695849503, Len: 1

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

0000	00 d0 59 a9 3d 68 00 06	25 da af 73 08 00 45 60	..Y.=h.. %..s..E`
0010	05 dc 8f 2f 40 00 37 06	76 f7 80 77 f5 0c c0 a8	.../@.7. v..w....
0020	01 69 00 50 04 22 ac a5	3f b4 65 14 9c 1f 50 10	.i.P.".. ?e...P.
0030	1b 28 5e d0 00 00 48 54	54 50 2f 31 2e 31 20 32	..(^...HT TP/1.1 2
0040	30 30 20 4f 4b 0d 0a 44	61 74 65 3a 20 53 61 74	00 OK..D ate: Sat
0050	2c 20 32 38 20 41 75 67	20 32 30 30 34 20 31 37	, 28 Aug 2004 17
0060	3a 31 39 3a 33 37 20 47	4d 54 0d 0a 53 65 72 76	:19:37 G MT..Serv
0070	65 72 3a 20 41 70 61 63	68 65 2f 32 2e 30 2e 34	er: Apache/2.0.4
0080	30 20 28 52 65 64 20 48	61 74 20 4c 69 6e 75 78	0 (Red H at Linux
0090	29 0d 0a 4c 61 73 74 2d	4d 6f 64 69 66 69 65 64)..Last- Modified
00a0	3a 20 53 61 74 2c 20 32	38 20 41 75 67 20 32 30	: Sat, 2 8 Aug 20
00b0	30 34 20 31 37 3a 31 38	3a 35 33 20 47 4d 54 0d	04 17:18 :53 GMT.
00c0	0a 45 54 61 67 3a 20 22	31 62 61 35 63 2d 31 31	.ETag: " 1ba5c-11
00d0	39 34 2d 36 39 65 64 39	34 30 22 0d 0a 41 63 63	94-69ed9 40"..Acc

Bytes 54-1513: TCP segment data (tcp.segment_data)

Exercise 2:

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?

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 FFFFFFFF, the packet is intended to be received by all hosts in the network.

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)	
Hardware type: Ethernet (1)	
Protocol type: IPv4 (0x0800)	
Hardware size: 6	
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 2. Give the hexadecimal value for the two-byte Ethernet Frame type field.

Answer:

0x0806, ARP

- ▼ Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
 - ▼ Destination: Broadcast (ff: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:a9:3d:68)
 - Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
 -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

```

0000  ff ff ff ff ff ff 00 d0 59 a9 3d 68 08 06 00 01  .... Y.=
0100  08 00 06 04 00 01 00 d0 59 a9 3d 68 c0 a8 01 69  .... Y.=
0200  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: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

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: LinksvsG 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: LinksvsG 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) on 0
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  > 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.

31.1.413347	LinksysG_67:22:94	Broadcast	802.11	90 Beacon frame, SN=3081, FN=0, Flags=.....C, BI=100, SSID=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=.....C, BI=20580, SSID=linksys12
35.1.510000	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=2870, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

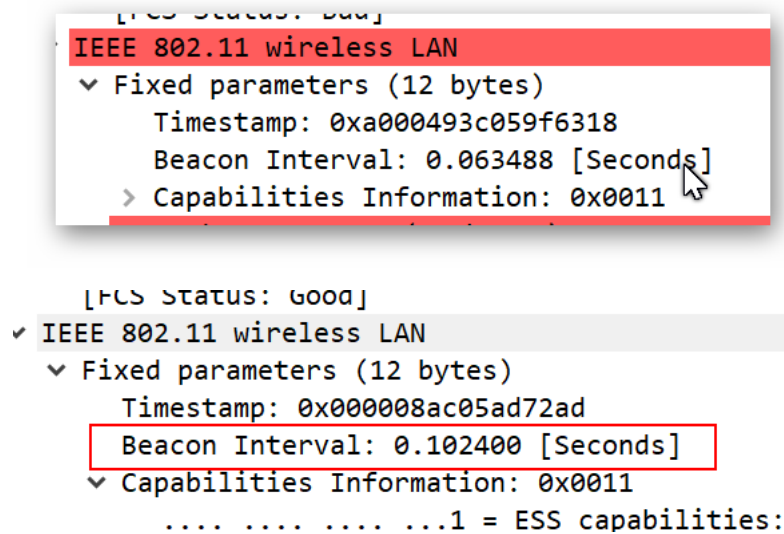
Question 2. What are the intervals of time between the transmission of the beacon frames the linksys access point? From the 30 Munroe St . access point? (Hint: this interval of time is contained in the beacon frame itself).

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**

Frame Control Field: 0x8000
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
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)
.... 0000 = Fragment number: 0

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]

```
Capabilities Information: 0x0001
Tagged parameters (119 bytes)
  Tag: SSID parameter set: 30 Munroe St
  Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
  Tag: DS Parameter Set: Current Channel: 6
  Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
  Tag: Country Information: Country Code US, Environment Indoor
  Tag: EDCA Parameter Set
  Tag: ERP Information
  Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
  Tag: Vendor Specific: AirgoNet
  Tag: Vendor Specific: Microsoft: WMM/WME: Parameter Element
```

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

Answer:

At time, t=24.811093 seconds.

Time	Source IP	Destination IP	Protocol	Source Port	Destination Port
474 24.811093	192.168.1.109	128.119.245.12	TCP	110 2538	80 [SYN]

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	11080 → 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

IEEE 802.11 QoS Data, Flags: ..mP..F..

Type/Subtype: QoS Data (0x0028)

> Frame Control Field: 0x8832

Duration/ID: 11560 (reserved)

Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)

Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)

Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)

Source address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)

BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)

STA address: 91:2a:b0:49:b6:4f (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.

Type: IPv4 (0x0000)

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

0100 = Version: 4