

Exercise 1

Question 1

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

The source host 48-bit Ethernet address is 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.)

The destination 48-bit address is 00:06:25:da:af:73.

This is not the Ethernet address of gaia.cs.umass.edu. Since when the client exchange information with server, it should transfer through several router. Although the source and destination IP address are stable, the Ethernet should follow the next transmission machine's MAC address. So this address is the first router connected to the client.

Question 3

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

The hexadecimal value 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?

The “G” appear after 54 bytes in the Ethernet. It does not include the preamble bytes. The first 14 bytes Ethernet source and destination address with type. The next 20 bytes is IP header and followed by 20 bytes 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?

The source Ethernet address is 00:06:25:da:af:73. This is neither Ethernet address of the gaia.cs.umass.edu nor the source host. It is the router link with client.

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?

The destination Ethernet address is 00:d0:59:a9:3d:68. It is Ethernet address of the source host that send 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?

There are 54 bytes appears before “O”.

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?

The source address 00:d0:59:a9:3d:68.

The destination address ff:ff:ff:ff:ff:ff. It is just combine by “f”.

Question 2

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

Type :0x0806.

Question 3

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

There are 20 bytes before 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?

The opcode is request(1).

Question 5

Does the ARP message contain the IP address of the sender?

Yes, the sender IP address is 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.

Shows on the target MAC address which is 00:00:00:00:00:00.

Question 7

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

There 20 bytes before 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?

Opcode value: reply(2).

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?

It send the MAC address back to reply the request.

Question 10

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

The source MAC address 00:06:25:da:af:73.

The destination MAC address 00:d0:59:a9:3d:68.

Exercise 3

Question 1.

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

Two access points SSIDs are “30 Munroe St” and “linsys_SES_24086”.

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).

It should be 1024s.

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).

The source MAC address of the “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 ?

The destination MAC address 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 ?

The MAC BSS ID address is 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 support rates are 1.0, 2.0, 5.5, 11.0 Mbps.

The extended rates are 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0 and 54.0 Mbps.

Question 7.

At what time is the TCP SYN sent?

At time 24.811093 TCP SYN sent.

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 MAC address for the host sending the TCP SYN is 00:13:02:d1:b6:4f.

The MAC address for the destination, which corresponds to the first-hop router, is 00:16:b6:f4:eb:a8.

The MAC address for the BSS is 00:16:b6:f7:1d:51.

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)

The IP address of the host sending the TCP SYN is 192.168.1.109.

The destination address is 128.199.245.12. This corresponds to the server gaia.cs.umass.edu. The IP is different with the Ethernet address, it just point to the

final destination.

Question 10.

At what time is the TCP SYNACK received?

At time 24.827751.

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?

The MAC address for the sender is 00:16:b6:f4:eb:a8, which corresponds to the first-hop route.

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.

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 doesn't.