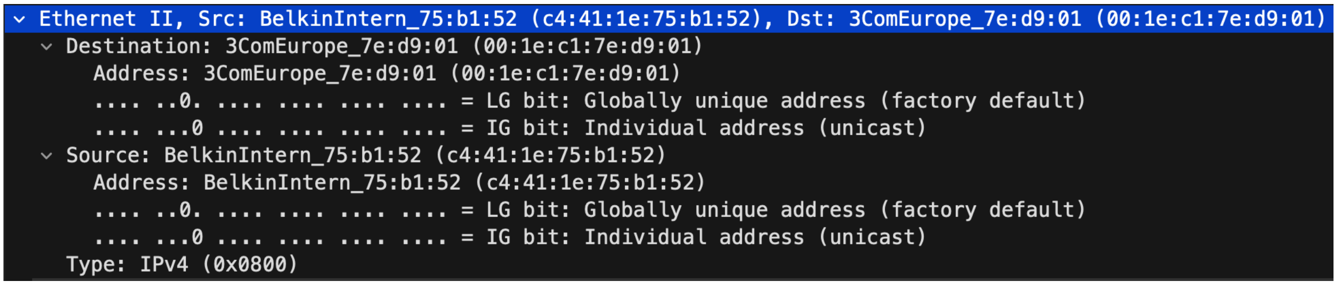
Student Information

Full Name : Mehmet Rüçhan Yavuzdemir
Id Number: 2522159

1 Ethernet



```
⌄ Ethernet II, Src: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52), Dst: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01)
  ⌄ Destination: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01)
      Address: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ⌄ Source: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
      Address: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

Figure 1: Answer 1-2-3

Answer 1

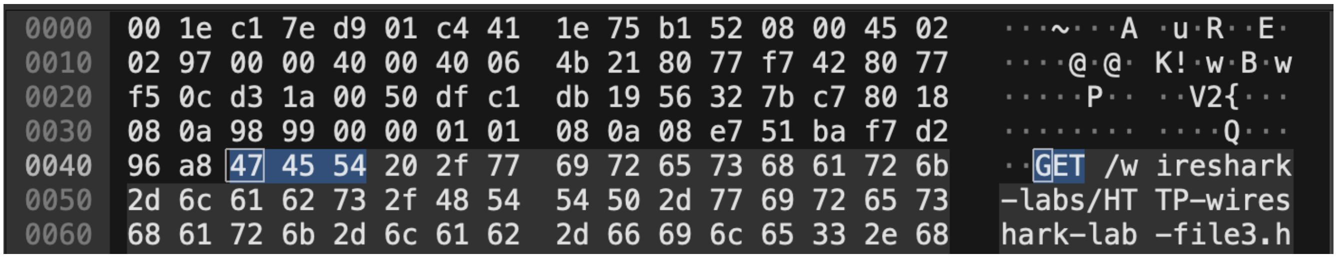
48-bit Ethernet source address is `c4:41:1e:75:b1:52`.

Answer 2

48-bit Ethernet destination address is `00:1e:c1:7e:d9:01`. However, this address is not the server's Ethernet address, it is the Ethernet address of the router `3ComEurope`, responsible for forwarding the sent packet to its final destination.

Answer 3

The `Type` field of the frame carrying the HTTP GET request is `0x0800` in hexadecimal notation, which corresponds to the upper layer `IPv4`.

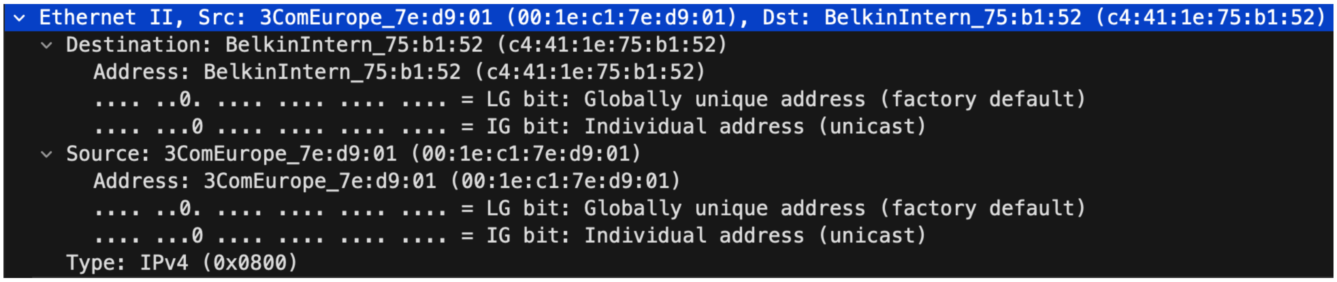


```
0000  00 1e c1 7e d9 01 c4 41  1e 75 b1 52 08 00 45 02   ···~···A ·u·R··E·
0010  02 97 00 00 40 00 40 06  4b 21 80 77 f7 42 80 77   ····@·@· K!·w·B·w
0020  f5 0c d3 1a 00 50 df c1  db 19 56 32 7b c7 80 18   ·····P·· ··V2{···
0030  08 0a 98 99 00 00 01 01  08 0a 08 e7 51 ba f7 d2   ········ ····Q···
0040  96 a8 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   ··GET /w ireshark
0050  2d 6c 61 62 73 2f 48 54  54 50 2d 77 69 72 65 73   -labs/HT TP-wires
0060  68 61 72 6b 2d 6c 61 62  2d 66 69 6c 65 33 2e 68   hark-lab -file3.h
```

Figure 2: Answer 4

Answer 4

There are no preamble bits in the .pcap file, the Ethernet frame directly starts with the Ethernet destination address. There are 14 bytes reserved for the Ethernet header, 20 bytes for the IP header, and 32 bytes for the TCP header. Hence, there is a total of `14 + 20 + 32 = 66` bytes until the 'G' letter of the HTTP 'GET'.



```
⌄ Ethernet II, Src: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01), Dst: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
  ⌄ Destination: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
      Address: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ⌄ Source: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01)
      Address: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

Figure 3: Answer 5-6-7

Answer 5

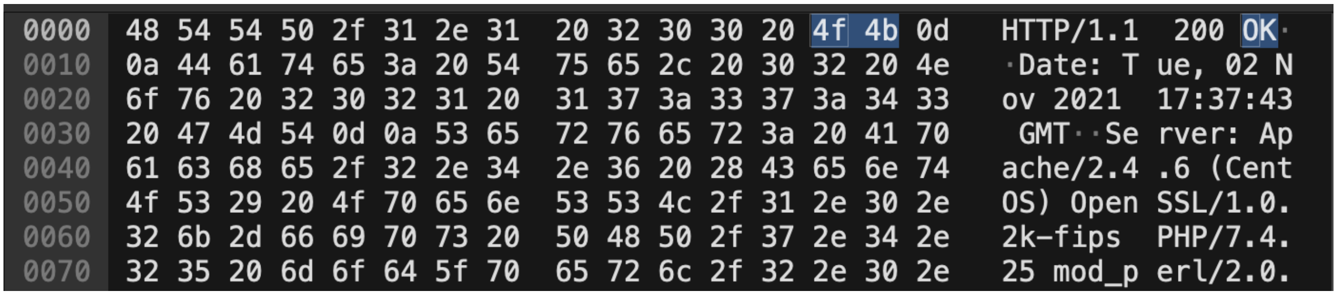
48-bit Ethernet source address is `00:1e:c1:7e:d9:01`. However, this address is not the server's Ethernet address, it is the Ethernet address of the router `3ComEurope`, responsible for forwarding the sent packet to the possibly other routers.

Answer 6

48-bit Ethernet destination address is `c4:41:1e:75:b1:52`. Yes, it is the Ethernet address of the sender.

Answer 7

The `Type` field of the frame carrying the HTTP GET request is `0x0800` in hexadecimal notation, which corresponds to the upper layer `IPv4`.

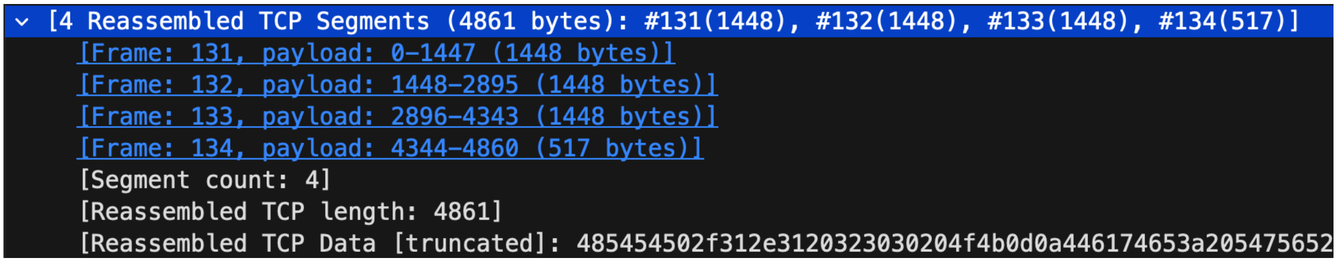


```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
0010  0a 44 61 74 65 3a 20 54  75 65 2c 20 30 32 20 4e   ·Date: T ue, 02 N
0020  6f 76 20 32 30 32 31 20  31 37 3a 33 37 3a 34 33   ov 2021  17:37:43
0030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0040  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0050  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
0060  32 6b 2d 66 69 70 73 20  50 48 50 2f 37 2e 34 2e   2k-fips  PHP/7.4.
0070  32 35 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   25 mod_p erl/2.0.
```

Figure 4: Answer 8

Answer 8

The header bits are exactly as is in Figure 4. The frame containing the Ethernet, IP, and TCP header information does not contain an HTTP OK message, it is segmented. Still, since we assume a frame starting with an Ethernet frame begins with the Ethernet frame's destination address, that's fine. `’HTTP/1.1 200 ’` takes `13 bytes`, as shown in the figure. Hence, there is a total of `14 + 20 + 32 = 66` bytes until `’HTTP/1.1 200 ’`, and there are `66 + 13 = 79 bytes` until the 'O' letter of the `HTTP/1.1 200 ’O’`.



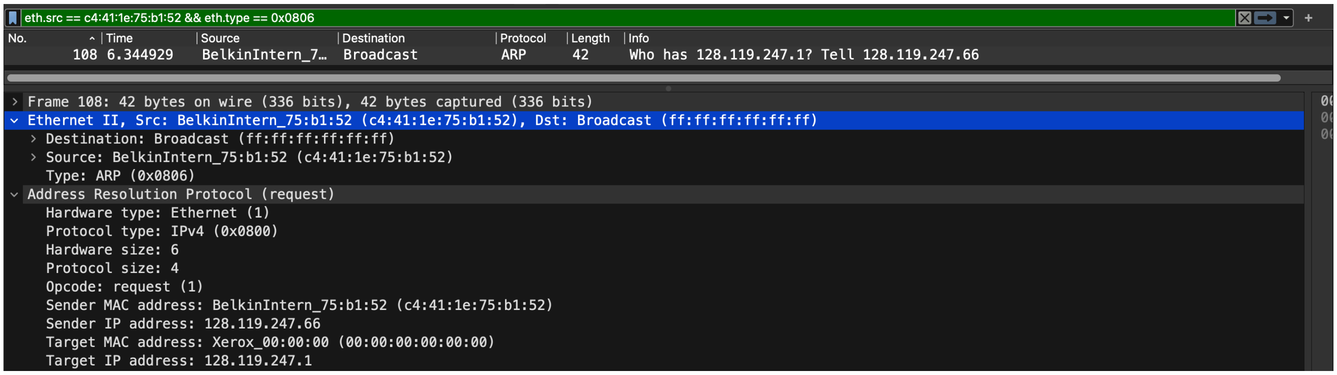
```
⌄ [4 Reassembled TCP Segments (4861 bytes): #131(1448), #132(1448), #133(1448), #134(517)]
      [Frame: 131, payload: 0-1447 (1448 bytes)]
      [Frame: 132, payload: 1448-2895 (1448 bytes)]
      [Frame: 133, payload: 2896-4343 (1448 bytes)]
      [Frame: 134, payload: 4344-4860 (517 bytes)]
      [Segment count: 4]
      [Reassembled TCP length: 4861]
      [Reassembled TCP Data [truncated]: 485454502f312e3120323030204f4b0d0a446174653a205475652
```

Figure 5: Answer 9

Answer 9

As shown in the figure above, 4 Ethernet frames carry the complete data of the HTTP OK 200 response message.

2 The Address Resolution Protocol



```
eth.src == c4:41:1e:75:b1:52 && eth.type == 0x0806
No.          Time       Source            Destination        Protocol  Length  Info
       108  6.344929   BelkinIntern_7…   Broadcast          ARP       42      Who has 128.119.247.1? Tell 128.119.247.66

> Frame 108: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
⌄ Ethernet II, Src: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
    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: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
    Sender IP address: 128.119.247.66
    Target MAC address: Xerox_00:00:00 (00:00:00:00:00:00)
    Target IP address: 128.119.247.1
```

Figure 6: Answer 10-11-12

Answer 10

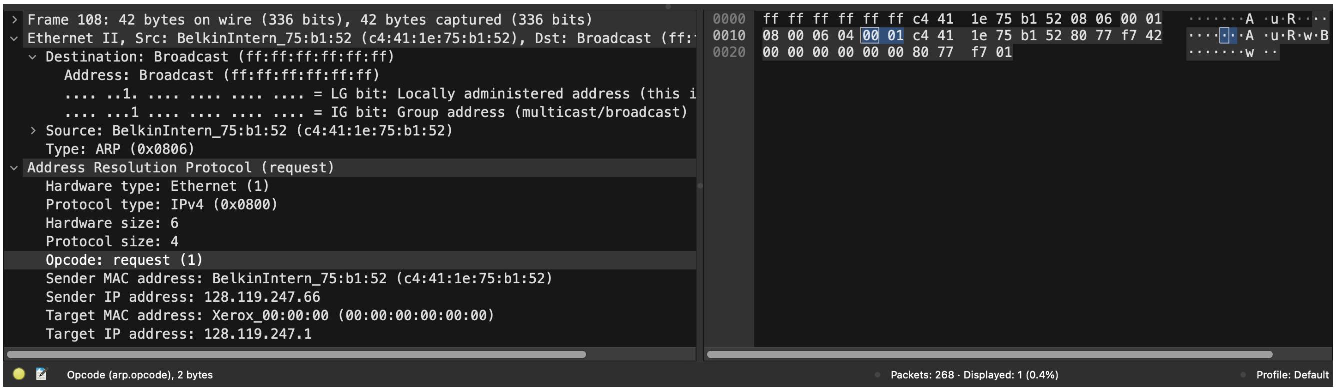
The hexadecimal value of the source address in the Ethernet frame containing the `ARP` request message is `c4:41:1e:75:b1:52`.

Answer 11

The hexadecimal value of the destination address in the Ethernet frame containing the `ARP` request message is `ff:ff:ff:ff:ff:ff`, which is the broadcast `MAC` address. Hence, there is no specific device to be sent, all the machines on the Local Area Network (LAN) receive this request message.

Answer 12

The `Type` field of the frame carrying the ARP messages is `0x0806` in hexadecimal notation, which corresponds to the upper layer `ARP`.



```
> Frame 108: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
v Ethernet II, Src: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52), Dst: Broadcast (ff:
  v Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this i
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  > Source: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
    Type: ARP (0x0806)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
    Sender IP address: 128.119.247.66
    Target MAC address: Xerox_00:00:00 (00:00:00:00:00:00)
    Target IP address: 128.119.247.1
```

```
0000  ff ff ff ff ff ff c4 41  1e 75 b1 52 08 06 00 01   ·······A ·u·R····
0010  08 00 06 04 00 01 c4 41  1e 75 b1 52 80 77 f7 42   ·······A ·u·R·w·B
0020  00 00 00 00 00 00 80 77  f7 01                     ·······w ··
```

```
Opcode (arp.opcode), 2 bytes          Packets: 268 · Displayed: 1 (0.4%)          Profile: Default
```

Figure 7: Answer 13-14-15

Answer 13

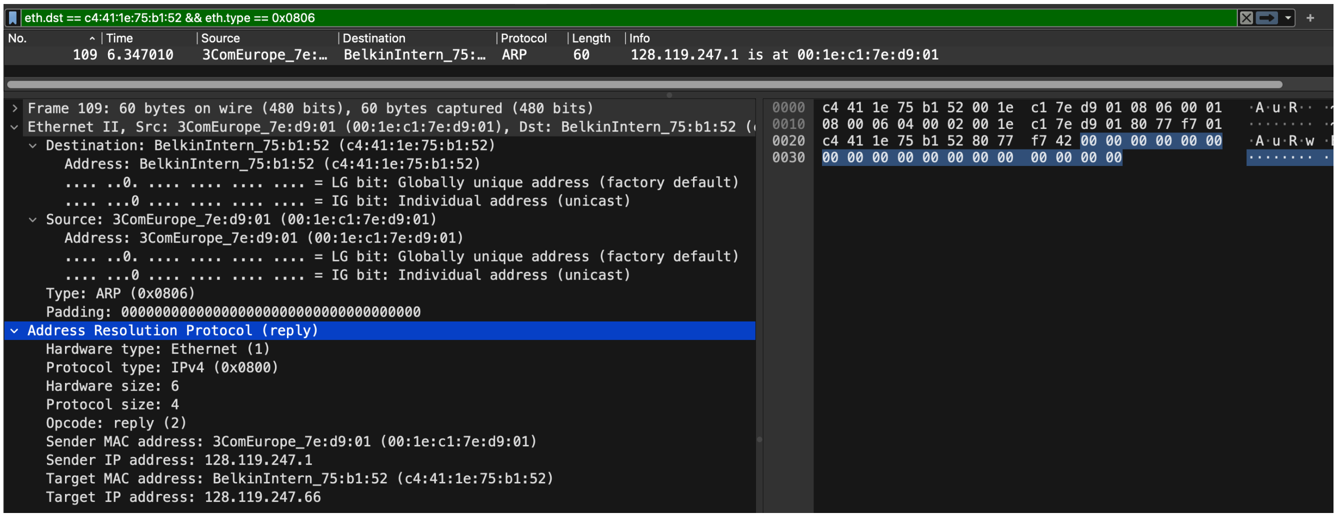
The Ethernet header is 14 bytes, ARP hardware, and protocol type is 2 bytes each, and hardware and protocol size is 1 byte each. Hence, there is `14 + 2 + 2 + 1 + 1 = 20 bytes` from the very beginning of the Ethernet frame until `ARP opcode` field begins.

Answer 14

Yes, it does. The `IP` address of the sender is `128.119.247.66`.

Answer 15

Since the `ARP` request message is broadcasted, the target `IP` address, which is the `IP` address of the gateway router within the same subnet is `128.119.247.1`.



```
eth.dst == c4:41:1e:75:b1:52 && eth.type == 0x0806
No.     Time       Source            Destination        Protocol Length Info
    109 6.347010   3ComEurope_7e:…   BelkinIntern_75:…  ARP      60     128.119.247.1 is at 00:1e:c1:7e:d9:01
```

```
> Frame 109: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
v Ethernet II, Src: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01), Dst: BelkinIntern_75:b1:52 (
  v Destination: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
      Address: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01)
      Address: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
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: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01)
    Sender IP address: 128.119.247.1
    Target MAC address: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
    Target IP address: 128.119.247.66
```

```
0000  c4 41 1e 75 b1 52 00 1e  c1 7e d9 01 08 06 00 01   ·A·u·R·· ·
0010  08 00 06 04 00 02 00 1e  c1 7e d9 01 80 77 f7 01   ········ ·
0020  c4 41 1e 75 b1 52 80 77  f7 42 00 00 00 00 00 00   ·A·u·R·w ·
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ·
```

Figure 8: Answer 16-17-18

Answer 16

The value of the `opcode` field in the `ARP` reply message is `2`.

Answer 17

By looking at the `ARP` response message in Figure 8 above, the Ethernet address of the `IP` address specified in the ARP request message is the Ethernet source address, which is `00:1e:c1:7e:d9:01`.

Answer 18

The `ARP` request is broadcast, however, the ARP response message is specifically sent to the sender's Ethernet address. Hence, we cannot see other response messages being sent to the other devices.