

Assignment 11: Ethernet and Arp

210010020

1. What is the 48-bit Ethernet address of your computer?

A] c4:41:1e:75:b1:52

2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? What device has this as its Ethernet address?

A] 00:1e:c1:7e:d9:01. This is address of next hop router, to which the device is connected.

> Frame 126: 677 bytes on wire (5416 bits), 677 bytes captured (5416 bits) on interface en0, id 0	0000 00 1e c1 7e d9 01 c4 41 1e 75 b1 52
▼ Ethernet II, Src: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52), Dst: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01)	0010 02 97 00 00 40 00 40 05 4b 21 15
▼ Destination: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01)	0020 f5 0c d3 1a 00 50 df c1 db 19 55
Address: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01)	0030 08 0a 98 99 00 00 01 01 08 0a 0f
.....0..... = IG bit: Globally unique address (factory default)	0040 96 a8 47 45 54 20 2f 77 69 72 65
.....0..... = IG bit: Individual address (unicast)	0050 2d 6c 61 62 73 2f 48 54 54 50 2d
▼ Source: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)	0060 68 61 72 6b 2d 6c 61 62 2d 66 69
Address: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)	0070 74 6d 6c 20 48 54 54 50 2f 31 2e
.....0..... = IG bit: Globally unique address (factory default)	0080 73 74 3a 20 67 61 69 61 2e 63 73
.....0..... = IG bit: Individual address (unicast)	0090 73 2e 65 64 75 0d 0a 55 73 65 73
Type: IPv4 (0x0800)	00a0 74 3a 20 4d 6f 7a 69 6c 6c 61 72
> Internet Protocol Version 4, Src: 128.119.247.66, Dst: 128.119.245.12	00b0 4d 61 63 69 6e 74 6f 73 68 3b 72
> Transmission Control Protocol, Src Port: 54042, Dst Port: 80, Seq: 1, Ack: 1, Len: 611	00c0 20 4d 61 63 20 4f 53 20 58 20 20
> Hypertext Transfer Protocol	00d0 20 72 76 3a 39 33 2e 30 29 20 2f
	00e0 32 30 31 30 30 31 30 31 20 46 6f
	00f0 2f 39 33 2e 30 0d 0a 41 63 63 6f
	0100 65 78 74 2f 68 74 6d 6c 2c 61 72

3. What is the hexadecimal value for the two-byte Frame type field in the Ethernet frame carrying the HTTP GET request? What upper layer protocol does this correspond to?

A] Type 0x800, Upper layer protocol: IPv4

4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear?

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
0070	74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f	tml HTTP /1.1·Ho
0080	73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73	st: gaia .cs.umas

Initializing from 0 'G' appears in address 66 bytes.

5. What is the value of the Ethernet source address? Is this the address of your computer, or gaia.cs.umass.edu? What device has this as its Ethernet address?

A] 00:1e:c1:7e:d9:01. No not of computer / gaia.cs.umass.edu but of router.

6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

A] c4:41:1e:75:b1:52 . Yes of computer capturing the wireshark trace.

7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

A] 0x800. Upper layer Protocol: IPv4

```
> Frame 134: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface en9, id 0
▼ 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)
```

8. How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” appear?
After how many bytes in the HTTP does the “O” in “OK” appear?

A] 13 bytes initializing from 0 from start of the HTTP.

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: Tue, 02 Nov 2021 17:37:43
0020	6f 76 20 32 30 32 31 20 31 37 3a 33 37 3a 34 33	GMT. Server: Apache/2.4.6 (Cent
0030	20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70	OS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/ v5.16.3
0040	61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 6e 74	Last Modified:
0050	4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e	
0060	32 6b 2d 66 69 70 73 20 50 48 50 2f 37 2e 34 2e	
0070	32 35 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e	
0080	31 31 20 50 65 72 6c 2f 76 35 2e 31 36 2e 33 0d	
0090	0a 44 61 74 65 3a 20 54 75 65 2c 20 30 32 20 4e	

After 79 bytes , O appears in the Ethernet frame.

c4 41 1e 75 b1 52 00 1e c1 7e d9 01 08 00 45 02	.A.u.R. .~. .E.
05 dc ed 6c 40 00 3f 06 5b 6f 80 77 f5 0c 80 77	. .l@.? [o.w.w
f7 42 00 50 d3 1a 56 32 7b c7 df c1 dd 7c 80 10	.B.P.V2 { . . .
00 ec e4 36 00 00 01 01 08 0a f7 d2 96 ad 08 e7	. .6.
51 ba 48 54 50 2f 31 2e 31 20 32 30 30 20 4f	Q HTTP/1 .1 200 O
4b 0d 0a 44 61 74 65 3a 20 54 75 65 2c 20 30 32	K .Date: Tue, 02

9. How many Ethernet frames (each containing an IP datagram, each containing a TCP segment) carry data that is part of the complete HTTP “OK 200 ...” reply message?

A] 4 Ethernet frames as seen in the reassembled TCP segment.

Part-2: The Address Resolution Protocol:

A1]

```
PS D:\SEM VI\Computer Networks\Labs\Lab11> arp -a

Interface: 192.168.56.1 --- 0xf
    Internet Address      Physical Address      Type
    192.168.56.255        ff-ff-ff-ff-ff-ff    static
    224.0.0.22            01-00-5e-00-00-16    static
    224.0.0.251           01-00-5e-00-00-fb    static
    224.0.0.252           01-00-5e-00-00-fc    static
    239.255.255.250       01-00-5e-7f-ff-fa    static

Interface: 10.200.253.103 --- 0x15
    Internet Address      Physical Address      Type
    10.200.240.2          44-b6-be-0a-9a-f3    dynamic
    10.200.246.26         38-d5-7a-32-87-2d    dynamic
    10.200.247.17         00-41-0e-a8-6b-d5    dynamic
    10.200.248.144        74-4c-a1-7b-cf-b5    dynamic
    10.200.252.46         2a-5a-cc-bd-d7-4f    dynamic
    10.200.255.255        ff-ff-ff-ff-ff-ff    static
    224.0.0.22            01-00-5e-00-00-16    static
    224.0.0.251           01-00-5e-00-00-fb    static
    224.0.0.252           01-00-5e-00-00-fc    static
    239.255.255.250       01-00-5e-7f-ff-fa    static
    255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

16 entries stored in the arp cache.

A2] Each entry consists of IP to physical address mapping along with the Type.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\hirsh> netsh interface ip delete arpccache
Ok.

PS C:\Users\hirsh> |
```

A3] Source address: c4:41:1e:75b:b1:52. This corresponds to address of my system. This is address of client.

A4] The hexadecimal value of the destination address in an Ethernet frame containing the first ARP request is typically ff:ff:ff:ff:ff:ff. This address is known as the broadcast address, which means that the ARP request is sent to all devices on the local network segment.

A5] Hexadecimal value is 0x0806 and upper layer protocol is ARP.

```

.....0..... = IG bit: Individual address (unicast)
Type: ARP (0x0806)
▼ Trailer: 0000000000000000000000000000000020202020
  > [Expert Info (Note/Protocol): Didn't find padding of zeros, and an undecoded trailer exists. There may be padding of no
> Address Resolution Protocol (request)

```

A6] Begins after 20byte from beginning of ethernet frame.

A7] The value of the opcode field within the ARP request message sent by computer is 1.

110	2021-11-02 23:07:43.073475	3ComEurope_7e:d9:01	Broadcast	ARP	60 Who has 128.119.247.41? Tell 128.119.247.1	
117	2021-11-02 23:07:43.073475	3ComEurope_7e:d9:01	Broadcast	ARP	60 Who has 128.119.247.111? Tell 128.119.247.1	
118	2021-11-02 23:07:43.089761	3ComEurope_7e:d9:01	Broadcast	ARP	60 Who has 128.119.247.49? Tell 128.119.247.1	
119	2021-11-02 23:07:43.089762	3ComEurope_7e:d9:01	Broadcast	ARP	60 Who has 128.119.247.19? Tell 128.119.247.1	

> Frame 108: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface en0, id 0 > Ethernet II, Src: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52), Dst: Broadcast (ff:ff:ff:ff:ff:ff) > Address Resolution Protocol (request)		0000 ff ff ff ff ff ff c4 41 1e 75 b1 52 00 06 00 01A-u-R-.. 0010 00 00 06 04 00 00 c4 41 1e 75 b1 52 80 77 f7 42 ...-A-u-R-u-B 0020 00 00 00 00 00 80 77 f7 01M..
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: 00:00:00:00:00:00 (00:00:00:00:00:00) Target IP address: 128.119.247.1		

A8] Yes . contains sender IP address = 128.119.247.1

A9] Sender IP address as above.

A10] Opcode field reply =2

```

  ▾ 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

```

A11] Ethernet address corresponding to the IP address that was specified in the ARP request message sent by computer is 00:1e:c1:7e:d9:01

Screenshot as above.

A12] We cannot find reply messages in the trace since they were broadcasted . However, the reply will only be sent to the device that requested it. As a result, this trace does not include all of the answers.