

CS 315: Computer Networks Lab
Spring 2024-25, IIT Dharwad
Assignment-11
Wireshark Lab: Ethernet and ARP
April 2, 2025
Chidurala Tejaswini
(220010012 / CS22BT012)

Part 0: Paste a screenshot of your system IP address, using ipconfig (on Windows) or ifconfig (on Mac and Linux), and fill out [this Google form](#) to submit the details of your system. The same system must be used to attempt all exercises of this lab.

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ ifconfig
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.240.118.97 netmask 255.255.248.0 broadcast 10.240.119.255
    inet6 fe80::1d6b:1bfb:2bd6:ef0d prefixlen 64 scopeid 0x20<link>
    ether e0:73:e7:0a:99:9a txqueuelen 1000 (Ethernet)
    RX packets 391173 bytes 254098205 (254.0 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 113219 bytes 14485817 (14.4 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 memory 0x80900000-80920000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 9065 bytes 931682 (931.6 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 9065 bytes 931682 (931.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Part-1: Capturing and analyzing Ethernet frames

Let's begin by capturing a set of Ethernet frames to study. To do this, of course, you'll need access to a wired Ethernet connection for your system.

Do the following:

1. First, make sure your browser's cache of previously downloaded documents is empty.
2. Start up Wireshark and enter the following URL into your browser:
`http://httpforever.com/`
3. Stop Wireshark packet capture.

Answer the following questions based on the Ethernet frame carrying the first HTTP GET request to the requested webpage:

No.	Time	Source	Destination	Protocol	Length	User Datagram Protocol	Info
33	4.734843937	10.240.118.97	146.190.62.39	HTTP	409		GET / HTTP/1.1
48	5.009220718	146.190.62.39	10.240.118.97	HTTP	2806		HTTP/1.1 200 OK (text/html)
71	5.046093569	10.240.118.97	146.190.62.39	HTTP	364		GET /js/init.min.js HTTP/1.1
86	5.314737212	146.190.62.39	10.240.118.97	HTTP	1896		HTTP/1.1 200 OK (application/javascript)
171	8.172274345	10.240.118.97	146.190.62.39	HTTP	382		GET /css/stvle.min.css HTTP/1.1

Frame 33: 409 bytes on wire (3272 bits), 409 bytes captured (3272 bits) on interface eno1, id 0
 Ethernet II, Src: e0:73:e7:0a:99:9a (e0:73:e7:0a:99:9a), Dst: Cisco_13:e0:82 (bc:d2:95:13:e0:82)
 Destination: Cisco_13:e0:82 (bc:d2:95:13:e0:82)
 Source: e0:73:e7:0a:99:9a (e0:73:e7:0a:99:9a)
 Type: IPv4 (0x0800)

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

The 48-bit Ethernet address of my computer is source MAC address in the Ethernet Frame i.e **e0:73:e7:0a:99:9a**

2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of `httpforever.com`? What device has this as its Ethernet address?

- The destination MAC address is: **bc:d2:95:13:e0:82**
- This is **not** the Ethernet address of `httpforever.com` because MAC addresses are only relevant within the local network (LAN).
- This MAC address likely belongs to the **default gateway (router)**, which forwards packets to external networks.

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

- The hexadecimal value for the two-byte Frame Type field is: **0x0800**
- This corresponds to network layer protocol **IPv4 (Internet Protocol version 4)**.

4. What is the total size (in bytes) of the Ethernet frame encapsulating the HTTP GET request in Wireshark?

The total size of the Ethernet frame encapsulating the HTTP GET request is **409 bytes**(since the frame size is **409 bytes** in wireshark).

5. Is the Ethernet frame carrying the first HTTP GET request transmitted as a unicast, multicast, or broadcast frame? How can this be determined from the destination MAC address?

- Unicast.** The destination MAC address is **bc:d2:95:13:e0:82**, which is a specific, unique hardware address. This means the frame is being sent directly to a single device (likely a router or gateway).
- Broadcast addresses have all bits set to 1 (**FF:FF:FF:FF:FF:FF**), and multicast addresses typically start with **01:00:5E** for IPv4. Since the destination address doesn't match either of these formats, it confirms that the frame is **unicast**.

Answer the following questions based on the Ethernet frame carrying the first HTTP response from the requested webpage:

No.	Time	Source	Destination	Protocol	Length	User Datagram Protocol	Info
33	4.734643937	10.240.118.97	146.190.62.39	HTTP	409		GET / HTTP/1.1
48	5.098220718	146.190.62.39	10.240.118.97	HTTP	2806		HTTP/1.1 200 OK (text/html)
71	5.046093569	10.240.118.97	146.190.62.39	HTTP	364		GET /js/init.min.js HTTP/1.1
86	5.314737212	146.190.62.39	10.240.118.97	HTTP	1896		HTTP/1.1 200 OK (application/javascript)
171	8.172274345	10.240.118.97	146.190.62.39	HTTP	382		GET /css/style.min.css HTTP/1.1

Frame 48: 2806 bytes on wire (22448 bits), 2806 bytes captured (22448 bits) on interface eno1, id 0
 Ethernet II, Src: Cisco_13:e0:82 (bc:d2:95:13:e0:82), Dst: e0:73:e7:0a:99:9a (e0:73:e7:0a:99:9a)
 Destination: e0:73:e7:0a:99:9a (e0:73:e7:0a:99:9a)
 Source: Cisco_13:e0:82 (bc:d2:95:13:e0:82)
 Type: IPv4 (0x0800)

6. What is the value of the Ethernet source address? Is this the address of your computer, or httpforever.com? What device has this as its Ethernet address?

- The **source MAC address** is `bc:d2:95:13:e0:82`, as seen in the **Ethernet II** section of the frame.
- This is **not** the MAC address of httpforever.com because MAC addresses are only relevant within a local network.
- Instead, this MAC address belongs to the **default gateway (router)** that forwards packets between your computer and external servers like httpforever.com.

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

- The **destination MAC address** is `e0:73:e7:0a:99:9a`.
- Yes, this is the **MAC address of your computer** because it matches the previously identified address of our computer (previously identified in the GET request frame).

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?

The Ethernet frame consists of:

- **Ethernet header:** 14 bytes
- **IPv4 header:** 20 bytes
- **TCP header:** 32 bytes
- **HTTP response headers:** A typical HTTP response starts with a status line like this: **HTTP/1.1 200 OK**. Each character in the response is 1 byte in size. The breakdown is:

Part	Content	Byte Count
HTTP version	“HTTP/1.1”	9

Status Code	"200"	4
Status Message	"OK"	2

- The **ASCII "O" in "OK"** appears **after 13 bytes(9+4=13)** in the HTTP message from the start of the HTTP response.
- The ASCII "O" in "OK" appears **after 79 bytes(14+20+32+13=79)** from the start of the Ethernet frame.

Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK

0040	d9 9f 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f	..HTTP/1 .1 200 O
0050	4b 0d 0a 53 65 72 76 65 72 3a 20 6e 67 69 6e 78	K..Serve r: nginx
0060	2f 31 2e 31 38 2e 30 20 28 55 62 75 6e 74 75 29	/1.18.0 (Ubuntu)
0070	0d 0a 44 61 74 65 3a 20 57 65 64 2c 20 30 32 20	..Date: Wed, 02
0080	41 70 72 20 32 30 32 35 20 30 33 3a 31 32 3a 32	Apr 2025 03:12:2
0090	37 20 47 4d 54 0d 0a 43 6f 6e 74 65 6e 74 2d 54	7 GMT..C ontent-T
00a0	79 70 65 3a 20 74 65 78 74 2f 68 74 6d 6c 0d 0a	ype: tex t/html..
00b0	4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 3a 20 57	Last-Mod ified: W
00c0	65 64 2c 20 32 32 20 4d 61 72 20 32 30 32 33 20	ed, 22 M ar 2023
00d0	31 34 3a 35 34 3a 34 38 20 47 4d 54 0d 0a 54 72	14:54:48 GMT..Tr
00e0	61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a	ansfer-E ncoding:
00f0	20 63 68 75 6e 6b 65 64 0d 0a 43 6f 6e 6e 65 63	chunked ..Connec
0100	74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65	tion: ke ep-alive
0110	0d 0a 45 54 61 67 3a 20 57 2f 22 36 34 31 62 31	..ETag: W/"641b1
0120	36 62 38 2d 31 34 30 34 22 0d 0a 52 65 66 65 72	6b8-1404 " ..Refer
0130	72 65 72 2d 50 6f 6c 69 63 79 3a 20 73 74 72 69	rer-Poli cy: stri
0140	63 74 2d 6f 72 69 67 69 6e 2d 77 68 65 6e 2d 63	ct-origi n-when-c
0150	72 6f 73 73 2d 6f 72 69 67 69 6e 0d 0a 58 2d 43	ross-ori gin..X-C
0160	6f 6e 74 65 6e 74 2d 54 79 70 65 2d 4f 70 74 69	ontent-T ype-Opti
0170	6f 6e 73 3a 20 6e 6f 73 6e 69 66 66 0d 0a 46 65	ons: nos niff..Fe
0180	61 74 75 72 65 2d 50 6f 6c 69 63 79 3a 20 61 63	ature-Po licy: ac

Frame (2806 bytes)
De-chunked entity body (1910 bytes)
Uncompressed entity body (5124 bytes)

Text item (text), 17 bytes

Part-2: The Address Resolution Protocol

In this section, we'll observe the ARP protocol in action.

Recall that the ARP protocol typically maintains a cache of IP-to-Ethernet address translation pairs on your computer. The *arp* command (in both DOS, MacOS and Linux) is used to view and manipulate the contents of this cache. Since the *arp* command and the ARP protocol have the

same name, it's understandably easy to confuse them. But keep in mind that they are different - the `arp` command is used to view and manipulate the ARP cache contents, while the ARP protocol defines the format and meaning of the messages sent and received, and defines the actions taken on ARP message transmission and receipt.

```
sysad@sysad-OptiPlex-7080: ~  
sysad@sysad-OptiPlex-7080:~$ arp -a  
gateway (10.250.65.250) at 02:04:96:9a:82:e8 [ether] on eno2  
? (10.42.0.35) at <incomplete> on wlo1  
? (10.250.65.243) at 30:b6:2d:a7:1c:ff [ether] on eno2  
? (10.250.65.254) at 00:04:96:9e:8b:e5 [ether] on eno2  
? (10.250.65.253) at 00:04:96:9e:47:a3 [ether] on eno2  
? (10.42.0.220) at f0:9e:4a:e5:09:ca [ether] on wlo1  
? (10.250.65.251) at 00:04:96:9e:78:77 [ether] on eno2  
sysad@sysad-OptiPlex-7080:~$
```

Note: To delete the ARP cache on a Linux machine use the following command:

Observing ARP in action

No.	Time	Source	Destination	Protocol	Length	User Datagram Protocol	Info
4	302.486575	LexmarkP_83:76:2c	Broadcast	RARP	60		who is 00:04:00:83:76:2c? Tell 00:04:00:83:76:2c
13	113831509.141076	c2:3d:19:6c:00:01	c2:3c:19:6c:00:01	ARP	60		who has 10.0.0.2? Tell 10.0.0.1
14	113831509.141076	c2:3d:19:6c:00:01	c2:3c:19:6c:00:01	ARP	60		who has 10.0.0.2? Tell 10.0.0.1
15	113831509.157076	c2:3c:19:6c:00:01	c2:3d:19:6c:00:01	ARP	60		10.0.0.2 is at c2:3c:19:6c:00:01
16	113831509.157076	c2:3d:19:6c:00:01	Broadcast	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)

Frame 13: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface -, id 43
 Ethernet II, Src: c2:3d:19:6c:00:01 (c2:3d:19:6c:00:01), Dst: c2:3c:19:6c:00:01 (c2:3c:19:6c:00:01)
 Address Resolution Protocol (request)
 Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: request (1)
 Sender MAC address: c2:3d:19:6c:00:01 (c2:3d:19:6c:00:01)
 Sender IP address: 10.0.0.1
 Target MAC address: c2:3c:19:6c:00:01 (c2:3c:19:6c:00:01)
 Target IP address: 10.0.0.2

1. State the sender's MAC address.

- The sender's MAC address in the ARP request (Frame 13) is **c2:3d:19:6c:00:01**.
- This MAC address belongs to the system with IP **10.0.0.1**.

2. Which target is the sender trying to connect to? Mention its IP and MAC addresses.

- **Target IP Address:** **10.0.0.2**
- **Target MAC Address:** **c2:3c:19:6c:00:01**
- **Explanation:** The sender at **10.0.0.1** is looking for the MAC address associated with **10.0.0.2**. Once the target responds, its MAC address is identified as **c2:3c:19:6c:00:01** (seen in Frame 15).

3. At what point does broadcasting occur in the ARP trace? Explain the reason for broadcasting.

arp							
No.	Time	Source	Destination	Protocol	Length	User Datagram Protocol	Info
4	382.486575	LexmarkP_83:76:2c	Broadcast	RARP	68		Who is 00:04:00:83:76:2c? Tell 00:04:00:83:76:2c
13	113831509.141876	c2:3d:19:6c:00:01	c2:3c:19:6c:00:01	ARP	68		Who has 10.0.0.2? Tell 10.0.0.1
14	113831509.141876	c2:3d:19:6c:00:01	c2:3c:19:6c:00:01	ARP	68		Who has 10.0.0.2? Tell 10.0.0.1
15	113831509.157076	c2:3c:19:6c:00:01	c2:3d:19:6c:00:01	ARP	68		10.0.0.2 is at c2:3c:19:6c:00:01
16	113831509.157076	c2:3d:19:6c:00:01	Broadcast	ARP	68		Gratuitous ARP for 10.0.0.1 (Reply)

Frame 13: 68 bytes on wire (480 bits), 68 bytes captured (480 bits) on interface -, id 43
Ethernet II, Src: c2:3d:19:6c:00:01 (c2:3d:19:6c:00:01), Dst: c2:3c:19:6c:00:01 (c2:3c:19:6c:00:01)
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: c2:3d:19:6c:00:01 (c2:3d:19:6c:00:01)
Sender IP address: 10.0.0.1
Target MAC address: c2:3c:19:6c:00:01 (c2:3c:19:6c:00:01)
Target IP address: 10.0.0.2

arp && eth.dst==ff:ff:ff:ff:ff:ff						
Time	No.	Source	Destination	Protocol	Length	Info
113831509.157076	16	c2:3d:19:6c:00:01	Broadcast	ARP	60	Gratuitous ARP for 10.0.0.1 (Reply)
113831509.157076	18	c2:3d:19:6c:00:01	Broadcast	ARP	60	Gratuitous ARP for 10.0.0.1 (Reply)
113831512.729076	39	c2:3c:19:6c:00:01	Broadcast	ARP	60	Gratuitous ARP for 10.0.0.2 (Reply)
113831512.729076	41	c2:3c:19:6c:00:01	Broadcast	ARP	60	Gratuitous ARP for 10.0.0.2 (Reply)
113831625.112076	536	c2:3d:19:6c:00:01	Broadcast	ARP	60	Gratuitous ARP for 10.0.0.1 (Reply)
113831625.112076	538	c2:3d:19:6c:00:01	Broadcast	ARP	60	Gratuitous ARP for 10.0.0.1 (Reply)
113831628.544076	547	c2:3c:19:6c:00:01	Broadcast	ARP	60	Gratuitous ARP for 10.0.0.2 (Reply)
113831628.544076	549	c2:3c:19:6c:00:01	Broadcast	ARP	60	Gratuitous ARP for 10.0.0.2 (Reply)
113831684.128076	783	c2:3d:19:6c:00:01	Broadcast	ARP	60	Gratuitous ARP for 10.0.0.1 (Reply)
113831684.128076	784	c2:3d:19:6c:00:01	Broadcast	ARP	60	Gratuitous ARP for 10.0.0.1 (Reply)
113831684.143076	785	c2:3d:19:6c:00:01	Broadcast	ARP	60	Gratuitous ARP for 10.0.0.1 (Reply)
113831684.143076	786	c2:3d:19:6c:00:01	Broadcast	ARP	60	Gratuitous ARP for 10.0.0.1 (Reply)
113831684.237076	793	c2:3d:19:6c:00:01	Broadcast	ARP	60	Who has 10.0.0.2? Tell 10.0.0.1
113831684.237076	794	c2:3d:19:6c:00:01	Broadcast	ARP	60	Who has 10.0.0.2? Tell 10.0.0.1
113831684.252076	796	c2:3d:19:6c:00:01	Broadcast	ARP	60	Who has 10.0.0.2? Tell 10.0.0.1
113831684.252076	798	c2:3d:19:6c:00:01	Broadcast	ARP	60	Who has 10.0.0.2? Tell 10.0.0.1
188826405.324635	1597	Sercomm_76:5b:78	Broadcast	ARP	60	Who has 192.168.2.102? Tell 192.168.2.1
247148819.462012	4613	Cisco_a1:2b:99	Broadcast	ARP	64	Gratuitous ARP for 192.168.121.253 (Reply)
247148821.180036	4633	Cisco_a1:2b:99	Broadcast	ARP	64	Who has 192.168.7.87? Tell 192.168.121.253
247148828.240124	4694	Cisco_a1:2b:99	Broadcast	ARP	64	Gratuitous ARP for 192.168.121.253 (Reply)
247148829.457063	4708	Cisco_a1:2b:99	Broadcast	ARP	64	Gratuitous ARP for 192.168.121.253 (Reply)

arp							
No.	Time	Source	Destination	Protocol	Length	User Datagram Protocol	Info
15	113831509.157076	c2:3d:19:6c:00:01	c2:3d:19:6c:00:01	ARP	60		10.0.0.2 is at c2:3d:19:6c:00:01
16	113831509.157076	c2:3d:19:6c:00:01	Broadcast	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)
17	113831509.157076	c2:3d:19:6c:00:01	c2:3d:19:6c:00:01	ARP	60		10.0.0.2 is at c2:3d:19:6c:00:01
18	113831509.157076	c2:3d:19:6c:00:01	Broadcast	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)
37	113831512.713076	c2:3d:19:6c:00:01	c2:3d:19:6c:00:01	ARP	60		Who has 10.0.0.1? Tell 10.0.0.2

> Frame 16: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface -, id 43
 > Ethernet II, Src: c2:3d:19:6c:00:01 (c2:3d:19:6c:00:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 > Address Resolution Protocol (reply/gratuitous ARP)
 Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: reply (2)
 [Is gratuitous: True]
 Sender MAC address: c2:3d:19:6c:00:01 (c2:3d:19:6c:00:01)
 Sender IP address: 10.0.0.1
 Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
 Target IP address: 10.0.0.1

arp && eth.dst==ff:ff:ff:ff:ff:ff							
Time	No.	Source	Destination	Protocol	Length	Info	
113831684.237076	793	c2:3d:19:6c:00:01	Broadcast	ARP	60	Who has 10.0.0.2? Tell 10.0.0.1	
113831684.237076	794	c2:3d:19:6c:00:01	Broadcast	ARP	60	Who has 10.0.0.2? Tell 10.0.0.1	
113831684.252076	796	c2:3d:19:6c:00:01	Broadcast	ARP	60	Who has 10.0.0.2? Tell 10.0.0.1	
113831684.252076	798	c2:3d:19:6c:00:01	Broadcast	ARP	60	Who has 10.0.0.2? Tell 10.0.0.1	
188826405.324635	1597	Sercomm_76:5b:78	Broadcast	ARP	60	Who has 192.168.2.102? Tell 192.168.2.1	

> Frame 793: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface -, id 43
 > IEEE 802.3 Ethernet
 > Logical-Link Control
 > Address Resolution Protocol (request)
 Hardware type: IEEE 802 (6)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: request (1)
 Sender MAC address: c2:3d:19:6c:00:01 (c2:3d:19:6c:00:01)
 Sender IP address: 10.0.0.1
 Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
 Target IP address: 10.0.0.2

0000 ff ff ff ff ff ff c2 3d 19 6c 00 01 00 24
 0010 03 00 00 00 08 06 00 06 08 00 06 04 00 01
 0020 19 6c 00 01 0a 00 00 01 00 00 00 00 00 00
 0030 00 02 00 00 00 00 00 00 00 00 00 00 00 00

Broadcasting in the ARP trace occurs mainly in the following two scenarios:

1. ARP Requests

- When it occurs:**
 When a device wants to find the MAC address corresponding to a specific IP address (e.g., "Who has 10.0.0.2? Tell 10.0.0.1").
- Example Frames:** Frame 13, 14, and 793 in the trace.
- Mechanism:**
 The sender (e.g., 10.0.0.1) doesn't know the MAC address of the target IP (10.0.0.2), so it sends an ARP request to the broadcast MAC address: **ff:ff:ff:ff:ff:ff**.
- Reason for Broadcasting:**
 Since the sender doesn't know which device on the network owns the target IP, it broadcasts the request so **all devices on the local network** receive the message and the correct device can respond.

2. Gratuitous ARP

- When it occurs:**
 When a device sends an unsolicited ARP reply to announce its own IP-MAC mapping (e.g., "10.0.0.1 is at c2:3d:19:6c:00:01").

- **Mechanism:**

The device sends a broadcast packet with the destination MAC as **ff:ff:ff:ff:ff:ff** even though no ARP request was made.

- **Reason for Broadcasting:**

Gratuitous ARP is used to:

- Announce or update its IP-MAC mapping across the network
- Detect IP address conflicts
- Inform switches of the device's presence for proper packet forwarding
- Update other devices' ARP caches

Broadcasting in ARP occurs in:

- **ARP Requests:** When the sender doesn't know the MAC address of the target IP.
- **Gratuitous ARP:** When the sender announces its own IP-MAC mapping.

These broadcasts ensure that **all relevant devices on the local network** receive the necessary information to either respond or update their ARP tables.

4. List out all field values in the ARP request from the sender to the target.

No.	Time	Source	Destination	Protocol	Length	User Datagram Protocol	Info
4	382.486575	LexmarkP_83:76:2c	Broadcast	RARP	60		who is 00:04:00:83:76:2c? Tell 00:04:00:83:76:2c
13	113831509.141076	c2:3d:19:6c:00:01	c2:3c:19:6c:00:01	ARP	60		who has 10.0.0.2? Tell 10.0.0.1
14	113831509.141076	c2:3d:19:6c:00:01	c2:3c:19:6c:00:01	ARP	60		who has 10.0.0.2? Tell 10.0.0.1
15	113831509.157076	c2:3c:19:6c:00:01	c2:3d:19:6c:00:01	ARP	60		10.0.0.2 is at c2:3c:19:6c:00:01
16	113831509.157076	c2:3d:19:6c:00:01	Broadcast	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)

Frame 13: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface -, id 43
 Ethernet II, Src: c2:3d:19:6c:00:01 (c2:3d:19:6c:00:01), Dst: c2:3c:19:6c:00:01 (c2:3c:19:6c:00:01)
 Address Resolution Protocol (request)
 Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: request (1)
 Sender MAC address: c2:3d:19:6c:00:01 (c2:3d:19:6c:00:01)
 Sender IP address: 10.0.0.1
 Target MAC address: c2:3c:19:6c:00:01 (c2:3c:19:6c:00:01)
 Target IP address: 10.0.0.2

From **Frame 13 (ARP Request):**

- **Hardware type:** Ethernet (1)
- **Protocol type:** IPv4 (0x0800)
- **Hardware size:** 6
- **Protocol size:** 4
- **Opcode:** Request (1)
- **Sender MAC address:** c2:3d:19:6c:00:01
- **Sender IP address:** 10.0.0.1
- **Target MAC address:** c2:3c:19:6c:00:01
- **Target IP address:** 10.0.0.2

5. List out all field values in the ARP reply from the target to the sender.

arp							
No.	Source	Destination	Time	Protocol	Length	User Datagram Protocol	Info
4	LexmarkP_83:76:2c	Broadcast	392.486575	RARP	60		who is 00:04:00:83:76:2c? Tell 00:04:00:83:76:2c
13	c2:3d:19:6c:00:01	c2:3c:19:6c:00:01	113831509.141076	ARP	60		who has 10.0.0.2? Tell 10.0.0.1
14	c2:3d:19:6c:00:01	c2:3c:19:6c:00:01	113831509.141076	ARP	60		who has 10.0.0.2? Tell 10.0.0.1
15	c2:3c:19:6c:00:01	c2:3d:19:6c:00:01	113831509.157076	ARP	60		10.0.0.2 is at c2:3c:19:6c:00:01
16	c2:3d:19:6c:00:01	Broadcast	113831509.157076	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)
17	c2:3c:19:6c:00:01	c2:3d:19:6c:00:01	113831509.157076	ARP	60		10.0.0.2 is at c2:3c:19:6c:00:01
18	c2:3d:19:6c:00:01	Broadcast	113831509.157076	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)

Frame 15: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface -, id 43
 Ethernet II, Src: c2:3c:19:6c:00:01 (c2:3c:19:6c:00:01), Dst: c2:3d:19:6c:00:01 (c2:3d:19:6c:00:01)
 Address Resolution Protocol (reply)
 Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: reply (2)
 Sender MAC address: c2:3c:19:6c:00:01 (c2:3c:19:6c:00:01)
 Sender IP address: 10.0.0.2
 Target MAC address: c2:3d:19:6c:00:01 (c2:3d:19:6c:00:01)
 Target IP address: 10.0.0.1

From **Frame 15 (ARP Reply)**:

- **Hardware type:** Ethernet (1)
- **Protocol type:** IPv4 (0x0800)
- **Hardware size:** 6
- **Protocol size:** 4
- **Opcode:** Reply (2)
- **Sender MAC address:** c2:3c:19:6c:00:01
- **Sender IP address:** 10.0.0.2
- **Target MAC address:** c2:3d:19:6c:00:01
- **Target IP address:** 10.0.0.1

6. What are the differences between the ARP request and ARP reply field values?

- ARP request: The sender asks for a MAC address.
- ARP reply: The target provides its MAC address.

Field	ARP request	ARP reply
Opcode	Request(1)	Reply(1)
Sender MAC address	MAC of the requesting host: c2:3d:19:6c:00:01	MAC of the target host: c2:3c:19:6c:00:01
Sender IP address	IP of the requesting host: 10.0.0.1	IP of the target host: 10.0.0.2
Target MAC address	MAC of the target host(since MAC Address of the target is known before already as ARP cache is not cleared ,Otherwise need to be broadcasted). c2:3c:19:6c:00:01	MAC Address of the sender(request): c2:3d:19:6c:00:01
Target IP address	IP of the target host: 10.0.0.2	IP Address of the sender(request): 10.0.0.1

7. Explain the presence of a Gratuitous ARP packet in the trace. What is its purpose?

arp							
No.	Source	Destination	Time	Protocol	Length	User Datagram Protocol	Info
15	c2:3d:19:6c:00:01	c2:3d:19:6c:00:01	113831509.157076	ARP	60		10.0.0.2 is at c2:3d:19:6c:00:01
16	c2:3d:19:6c:00:01	Broadcast	113831509.157076	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)
17	c2:3d:19:6c:00:01	c2:3d:19:6c:00:01	113831509.157076	ARP	60		10.0.0.2 is at c2:3d:19:6c:00:01
18	c2:3d:19:6c:00:01	Broadcast	113831509.157076	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)

Frame 16: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface -, id 43
Ethernet II, Src: c2:3d:19:6c:00:01 (c2:3d:19:6c:00:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (reply/gratuitous ARP)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
[Is gratuitous: True]
Sender MAC address: c2:3d:19:6c:00:01 (c2:3d:19:6c:00:01)
Sender IP address: 10.0.0.1
Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
Target IP address: 10.0.0.1

- The **Gratuitous ARP (GARP)** is seen in **Frame 16 ("Gratuitous ARP for 10.0.0.1 (Reply)")**. They are broadcasted and typically contain the sender's own IP as both sender and target.
- **Purpose:**
 - To **announce or update** a device's IP-to-MAC mapping to the entire network.
 - It helps to detect **IP conflicts**, ensuring no two devices use the same IP.
 - It allows devices like switches to update their ARP caches.

8. What is the significance of the IP and MAC addresses in the Gratuitous ARP packet?

- **Sender IP and Target IP** are the **same (10.0.0.1)**, meaning the sender is announcing its own address.
- **Sender MAC address** is **c2:3d:19:6c:00:01**, and the **Target MAC address** is **ff:ff:ff:ff:ff:ff** (broadcast), meaning it informs all devices about its presence.

Significance:

- It tells all network devices that **10.0.0.1** is at **c2:3d:19:6c:00:01**.
- Ensures that **no other device** on the network is using **10.0.0.1**.

9. How many Gratuitous ARP packets are present in the trace corresponding to the sender's IP Address? Provide the packet number(s).

arp.opcode == 2 && arp.src.proto_ipv4 == 10.0.0.1 && arp.src.proto_ipv4 == arp.dst.proto_ipv4							
No.	Source	Destination	Time	Protocol	Length	User Datagram Protocol	Info
16	c2:3d:19:6c:00:01	Broadcast	113831509.157076	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)
18	c2:3d:19:6c:00:01	Broadcast	113831509.157076	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)
536	c2:3d:19:6c:00:01	Broadcast	113831625.112076	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)
538	c2:3d:19:6c:00:01	Broadcast	113831625.112076	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)
783	c2:3d:19:6c:00:01	Broadcast	113831684.128076	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)
784	c2:3d:19:6c:00:01	Broadcast	113831684.128076	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)
785	c2:3d:19:6c:00:01	Broadcast	113831684.143076	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)
786	c2:3d:19:6c:00:01	Broadcast	113831684.143076	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)

Filter type :

arp.opcode == 2 && arp.src.proto_ipv4 == 10.0.0.1 && arp.src.proto_ipv4 == arp.dst.proto_ipv4

There are **8 Gratuitous ARP packets** for **10.0.0.1**:

- **Frame 16:** "Gratuitous ARP for 10.0.0.1 (Reply)"
- **Frame 18:** "Gratuitous ARP for 10.0.0.1 (Reply)"
- **Frame 536:** "Gratuitous ARP for 10.0.0.1 (Reply)"
- **Frame 538:** "Gratuitous ARP for 10.0.0.1 (Reply)"
- **Frame 783:** "Gratuitous ARP for 10.0.0.1 (Reply)"
- **Frame 784:** "Gratuitous ARP for 10.0.0.1 (Reply)"
- **Frame 785:** "Gratuitous ARP for 10.0.0.1 (Reply)"
- **Frame 786:** "Gratuitous ARP for 10.0.0.1 (Reply)"

10. What is the sender and target MAC address in the Gratuitous ARP packet?

```
> Frame 16: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface -, id 43
> Ethernet II, Src: c2:3d:19:6c:00:01 (c2:3d:19:6c:00:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (reply/gratuitous ARP)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  [Is gratuitous: True]
  Sender MAC address: c2:3d:19:6c:00:01 (c2:3d:19:6c:00:01)
  Sender IP address: 10.0.0.1
  Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
  Target IP address: 10.0.0.1
```

In the Gratuitous ARP packet (Frame 16):

- **Sender MAC address:** **c2:3d:19:6c:00:01**
- **Target MAC address:** **ff:ff:ff:ff:ff:ff** (Broadcast)

Submission Details

- Write your answers in a single doc/tex file, and submit its PDF named after your IIT Dharwad roll number, which contains all answers (with screenshots, if necessary).