

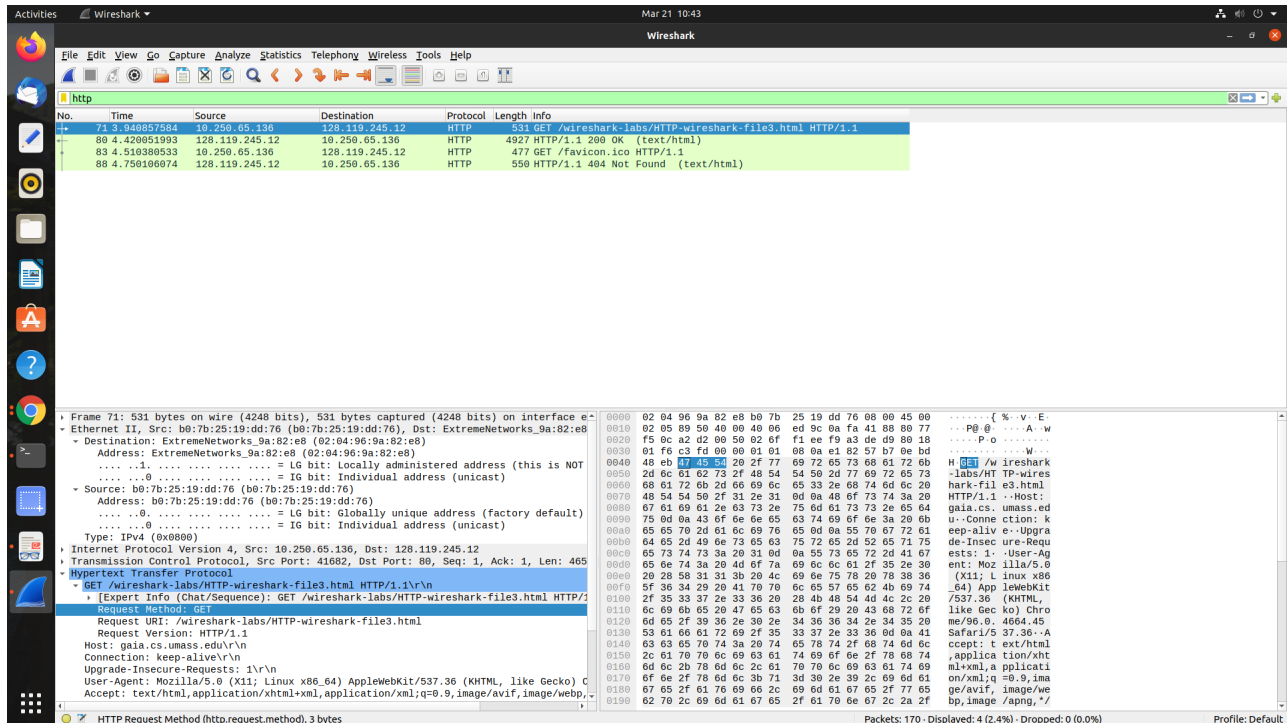
CS315 : Computer Networks Lab

Assignment 11

Sourabh Bhosale (200010004)

March 21, 2023

1 Part-1: Capturing and analyzing Ethernet frames



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

Ethernet address of my computer: bo:7b:25:19:dd:76

2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address?

Destination address: 02:04:96:9a:82:e8

No, this address is not the Ethernet address of gaia.cs.umass.edu. It is address of my ExtremeNetworks Link router.

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?

Hexadecimal value for frame type field is Type: IPv4 (0x0800). This corresponds to IP protocol.

4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame? Do not count any preamble bits in your count, i.e., assume that the Ethernet frame begins with the Ethernet frame's destination address.

66 bits into the frame.

The screenshot shows a Wireshark capture of an HTTP GET request. The packet list at the top shows a GET request for /wireshark-labs/HTTP-wireshark-file3.html. The packet details pane shows the destination MAC address b0:7b:25:19:dd:76 and the source MAC address 02:04:96:9a:82:e8. The packet bytes pane shows the ASCII string 'GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1' starting at offset 66.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|----------------|----------------|----------|--------|--|
| 71 | 3.940857584 | 10.250.65.136 | 128.119.245.12 | HTTP | 531 | GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1 |
| 80 | 4.420851993 | 128.119.245.12 | 10.250.65.136 | HTTP | 492 | HTTP/1.1 200 OK (text/html) |
| 83 | 4.516390533 | 10.250.65.136 | 128.119.245.12 | HTTP | 477 | GET /favicon.ico HTTP/1.1 |
| 88 | 4.750160074 | 128.119.245.12 | 10.250.65.136 | HTTP | 550 | HTTP/1.1 404 Not Found (text/html) |

Destination: b0:7b:25:19:dd:76 (b0:7b:25:19:dd:76)
Address: b0:7b:25:19:dd:76 (b0:7b:25:19:dd:76)
.....0..... = LG bit: Globally unique address (factory default)
.....0..... = IG bit: Individual address (unicast)
Source: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8)
Address: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8)
.....1..... = LG bit: Locally administered address (this is NOT the factory default)
.....0..... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.250.65.136
Transmission Control Protocol, Src Port: 80, Dst Port: 41682, Seq: 1, Ack: 466, Len: 4861
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
Date: Tue, 21 Mar 2023 04:53:33 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\nLast-Modified: Mon, 20 Mar 2023 05:59:02 GMT\r\nETag: "1194-5f74e9faf3137"\r\nAccept-Ranges: bytes\r\nContent-Length: 4500\r\nKeep-Alive: timeout=5, max=100\r\nHTTP Response Reason Phrase (http.response.reason), 2 bytes

0000 b0 7b 25 19 dd 76 02 04 96 9a 82 e8 08 00 45 00 [%-v.....E
0010 13 31 96 33 40 00 3f 06 d0 8d 80 77 f5 0c 0a fa .1.30.?.....w
0020 41 88 00 50 a2 d2 f9 a3 de 09 02 0f f3 bf 80 18 A.P.....o
0030 00 7a d5 29 00 00 01 01 08 0a 0e bd 49 1b e1 82 z.).....I
0040 57 b7 48 54 54 50 2f 31 2e 31 20 32 30 30 2f W HTTP/1.1 200
0050 0d 0a 44 61 74 05 3a 20 54 75 05 2c 20 32 31 .-Date: Tue, 21
0060 20 4d 61 72 20 32 30 32 33 20 30 34 3a 35 33 3a Mar 2023 04:53:
0070 33 33 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 33 GMT- Server:
0080 41 70 61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 Apache/2.4.6 (Ce
0090 6e 74 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e ntOS) Op enSSL/1.
00a0 30 2e 32 6b 2d 66 69 70 73 20 58 48 50 2f 37 2e 0.2k-fip s PHP/7.
00b0 34 2e 33 33 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 4.33 mod_perl/2.
00c0 30 2e 31 31 20 50 65 65 72 6c 2f 76 35 2e 31 36 2e 0.11 Per l/v5.16.
00d0 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 3--Last- Modified
00e0 3a 20 4d 6f 6e 2c 20 32 30 20 4d 61 72 20 32 30 : Mon, 2 0 Mar 20
00f0 32 33 20 30 35 3a 35 39 3a 30 32 20 47 4d 54 0d 23 05:59 :02 GMT-
0100 0a 45 54 61 67 3a 20 22 31 31 39 34 2d 35 06 37 -ETag: " 1194-5f7
0110 34 65 39 66 61 66 33 31 33 37 22 0d 0a 41 63 63 4e9faf31 37"-Acc
0120 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 ept-Rang es: byte
0130 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 s--Conte nt-Lengt
0140 68 3a 20 34 35 30 30 0d 0a 4b 65 65 70 2d 41 6c h: 4500-Keep-Al
0150 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20 lve: tim eout=5,
0160 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 74 max=100-Connect
0170 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 9d ion: Kee p-Alive-
0180 0a 43 6f 6e 74 65 6e 74 2d 54 78 70 65 3a 20 74 -Content -Type: t
0190 6e 78 74 2f 68 74 64 6a 2b 2a 63 68 61 72 72 6e ept/html -charac

Packets: 170 · Displayed: 4 (2.4%) · Dropped: 0 (0.0%) Profile: Default

5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?

Source address: 02:04:96:9a:82:e8

No, this is not the address of my computer or of gaia.cs.umass.edu. This is the address of my router.

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

Destination address: 08:00:2b:25:19:dd:76

This is the address of my computer.

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

Hexadecimal value for frame type field is Type: IPv4 (0x0800). This corresponds to IP protocol.

8. 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? Do not count any preamble bits in your count, i.e., assume that the Ethernet frame begins with the Ethernet frame's destination address.

79 bytes into the frame.

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?

Only 1 Ethernet frame carries data that is part of complete HTTP "OK 200 ..." reply message.

| | | |
|---|--|--|
| <p>Frame 80: 4927 bytes on wire (39416 bits), 4927 bytes captured (39416 bits) on interface eno2, id 0</p> <p>Ethernet II, Src: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8), Dst: b0:7b:25:19:dd:76 (b0:7b:25:19:dd:76)</p> <p>Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.250.65.136</p> <p>Hypertext Transfer Protocol, Src Port: 80, Dst Port: 41662, Seq: 1, Ack: 466, Len: 4961</p> <p>HTTP/1.1 200 OK\r\n</p> <p>Date: Tue, 21 Mar 2023 04:53:33 GMT\r\n</p> <p>Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n</p> <p>Last-Modified: Mon, 20 Mar 2023 05:59:02 GMT\r\n</p> <p>Etag: "1194-5f74e9faf3137"\r\n</p> <p>Accept-Ranges: bytes\r\n</p> <p>Content-Length: 4500\r\n</p> <p>Keep-Alive: timeout=5, max=100\r\n</p> <p>Connection: Keep-Alive\r\n</p> <p>Content-Type: text/html; charset=UTF-8\r\n</p> <p>\r\n</p> <p>[HTTP response 1/2]</p> <p>[Time since request: 0.479194409 seconds]</p> <p>[Request in frame: 71]</p> <p>[Next request in frame: 83]</p> <p>[Next response in frame: 88]</p> <p>[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]</p> <p>File Data: 4500 bytes</p> <p>Line-based text data: text/html (98 lines)</p> | | <p>0020 41 88 00 50 a2 d2 f9 a3 de d9 02 6f f3 bf 80 1e A .P.....p....</p> <p>0030 80 7a 05 29 80 00 01 01 06 0a 0e bd 49 1b e1 02 .Z).....I...</p> <p>0040 52 03 48 54 5a 59 2f 31 2e 31 29 32 30 38 29 4f .HTTP/1.1 200 O</p> <p>0050 4b 60 0a 44 61 74 65 3a 20 54 75 65 2c 28 32 31 K Date: Tue, 21</p> <p>0060 20 40 61 72 20 32 30 32 33 20 30 34 3a 35 33 3a Mar 2023 04:53:</p> <p>0070 33 33 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 33 GMT Server:</p> <p>0080 41 70 61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 Apache/2.4.6 (Ce</p> <p>0090 6e 74 4f 53 29 20 4f 70 65 6e 53 43 ac 2f 31 2e ntOS) Op enSSL/1.</p> <p>00a0 30 2e 32 6b 2d 66 69 70 73 29 50 48 50 2f 37 2e 0.2k-fips PHP/7.</p> <p>00b0 34 2e 33 33 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 4.33 mod_perl/2.</p> <p>00c0 30 2e 31 31 20 50 65 72 6c 2f 76 35 2e 31 30 2e 0.11 Perl/v5.16.</p> <p>00d0 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 3-Last-Modified</p> <p>00e0 3a 20 4d 6f 6e 2c 20 32 30 20 4d 61 72 20 32 30 : Mon, 20 Mar 20</p> <p>00f0 32 33 20 30 35 3a 35 39 3a 30 32 20 47 4d 54 0d 22 05:59:02 GMT</p> <p>0100 0a 45 54 61 67 3a 20 22 31 31 39 34 2d 35 66 37 Etag: "1194-5f7</p> <p>0110 34 05 39 66 61 66 33 31 33 37 22 0d 0a 41 63 63 4e9faf3137" Acc</p> <p>0120 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 ept-Ranges: byte</p> <p>0130 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 s Content-Lengt</p> <p>0140 68 3a 20 34 35 30 30 0d 0a 4b 65 65 70 2d 41 6c h: 4500 -Keep-AL</p> <p>0150 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20 ive: timout=5,</p> <p>0160 6d 61 70 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 74 max=100 Connect</p> <p>0170 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d ion: Keep-Alive:</p> <p>0180 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 Content-Type: t</p> <p>0190 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 ext/html; charse</p> <p>01a0 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d 6c t=UTF-8 ...html</p> <p>01b0 3e 3c 68 65 61 64 3e 20 0a 3c 74 69 74 6c 65 3c >=<html> <title></p> |
|---|--|--|

2 Part-2: The Address Resolution Protocol

```

user@sysad-OptiPlex-7050-1:~$ arp -a
? (10.250.65.251) at 00:04:96:9e:78:77 [ether] on eno2
? (10.250.65.252) at 00:04:96:cc:fd:68 [ether] on eno2
? (10.250.65.253) at 00:04:96:9e:47:a3 [ether] on eno2
_gateway (10.250.65.250) at 02:04:96:9a:82:e8 [ether] on eno2
? (10.250.65.243) at 30:b6:2d:a7:1c:ff [ether] on eno2
user@sysad-OptiPlex-7050-1:~$

```

1. How many entries are stored in your ARP cache?

5 entries.

2. What is contained in each displayed entry of the ARP cache?

The ARP cache contains entries that map IP addresses to MAC addresses.

3. What is the hexadecimal value of the source address in the Ethernet frame containing the ARP request message sent out by your computer?

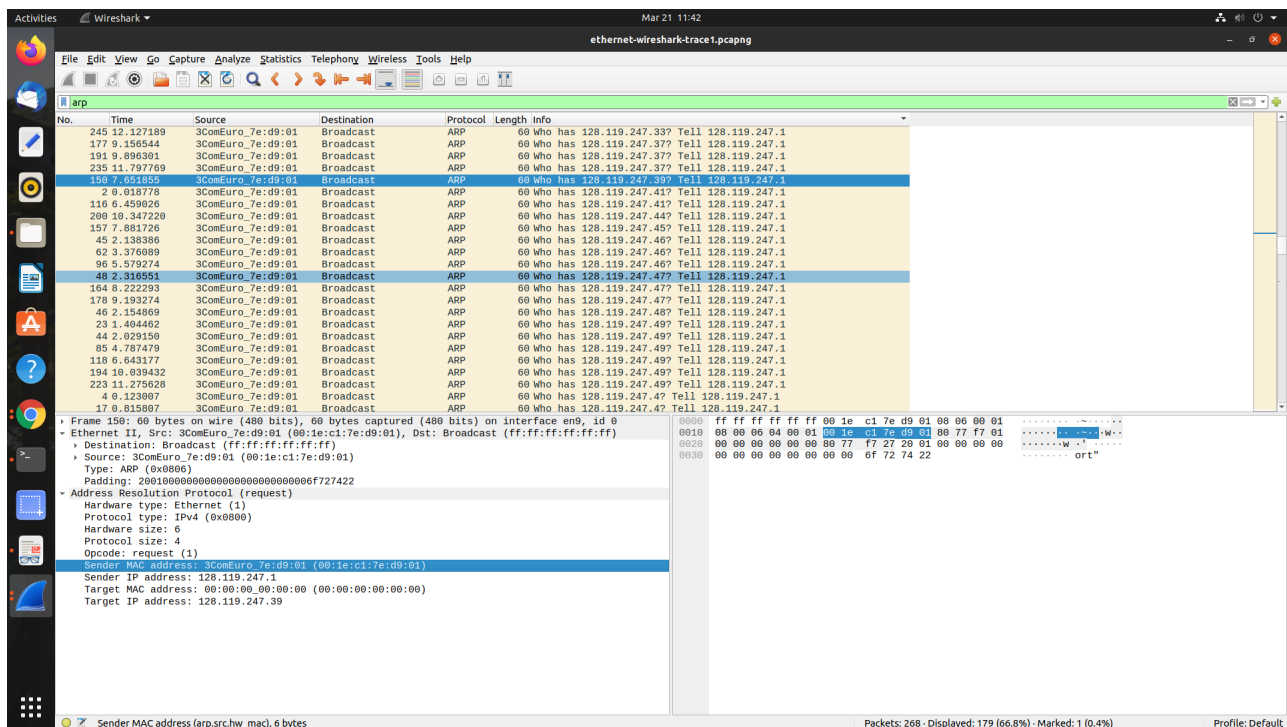
Source address: 00:1e:c1:7e:d9:01

4. What is the hexadecimal value of the destination addresses in the Ethernet frame containing the ARP request message sent out by your computer? And what device(if any) corresponds to that address (e.g., client, server, router, switch or otherwise...)?

Destination address: Broadcast (ff:ff:ff:ff:ff:ff). This is a broadcast address, which corresponds to all devices on the network.

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

Type: ARP (0x0806). This corresponds to ARP protocol.



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

ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.

7. What is the value of the opcode field within the ARP request message sent by your computer?

Opcode: 0x0001

8. Does the ARP request message contain the IP address of the sender? If the answer is yes, what is that value?

Yes, Sender IP address: 128.119.247.1

9. What is the IP address of the device whose corresponding Ethernet address is being requested in the ARP request message sent by your computer?

Target IP address: 128.119.247.39

10. What is the value of the opcode field within the ARP reply message received by your computer?

Opcode: 0x0002 (request (2))

11. What is the Ethernet address corresponding to the IP address that was specified in the ARP request message sent by your computer?

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

12. We've looked at the ARP request message sent by your computer running Wireshark, and the ARP reply message sent in response. But there are other devices in this network that are also sending ARP request messages that you can find in the trace. Why are there no ARP replies in your trace that are sent in response to these other ARP request messages?

There is no reply in this trace, because we are not at the machine that sent the request. The ARP request is broadcast, but the ARP reply is sent back directly to the sender's Ethernet address.