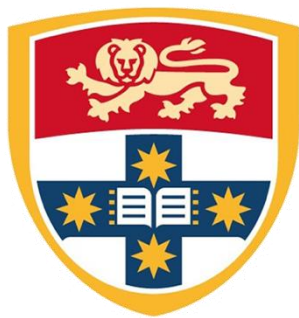


University of Sydney

ELEC3506 Data Communications and Internet – Lab Report 1

Student: Mengzhen Chen
SID:480462613



THE UNIVERSITY OF
SYDNEY

Table of Contents

| | | |
|-----|---|---|
| 1 | Introduction..... | 0 |
| 2 | Phase I: Wireshark | 2 |
| 3 | Phase II: Ethernet and Address Resolution Protocol..... | 3 |
| 3.1 | Capture and analyzing Ethernet frames | 3 |
| 3.2 | Address Resolution Protocol..... | 4 |

1 Introduction

This report is aimed to demonstrating the basic operations of Wireshark. It then took a closer look upon ethernet frames and hopefully reveal how HTTP and ARP protocol works.

2 Phase I: Wireshark

Step1:

1. TCP
2. HTTP
3. ARP

| | | | | | | |
|------|-----------|-------------------|----------------|------|-----|---|
| 1691 | 11.918437 | 192.168.1.110 | 128.119.245.12 | HTTP | 467 | GET /favicon.ico HTTP/1.1 |
| 1692 | 11.932397 | 192.168.1.110 | 204.79.197.200 | TCP | 66 | 51454 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 1693 | 11.947677 | Tp-LinkT_a3:b3:27 | Broadcast | ARP | 42 | Who has 192.168.1.100? Tell 192.168.1.1 |

Figure 1. protocols examples

Step2:

09:35:37.624921 – 09:35:37.343532 ≈ 0.2814 seconds

| | | | | | | |
|------|-----------------|----------------|----------------|------|-----|---|
| 1613 | 09:35:37.343532 | 192.168.1.110 | 128.119.245.12 | HTTP | 535 | GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 |
| 1682 | 09:35:37.624921 | 128.119.245.12 | 192.168.1.110 | HTTP | 492 | HTTP/1.1 200 OK (text/html) |

Figure 2. GET-OK pair

Step3:

IP address for gaia.cs.umass.edu is 128.119.245.12

IP address for my laptop is 192.168.1.110

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|-----------------|---------------|----------------|----------|--------|---|
| 1613 | 09:35:37.343532 | 192.168.1.110 | 128.119.245.12 | HTTP | 535 | GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 |
| Frame 1613: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{C4B97F8B-4A14-4252-BB93-497BF370C1B6}, id 0 | | | | | | |
| Interface id: 0 (\Device\NPF_{C4B97F8B-4A14-4252-BB93-497BF370C1B6}) | | | | | | |
| Encapsulation type: Ethernet (1) | | | | | | |
| Arrival Time: Oct 11, 2020 09:35:37.343532000 AUS Eastern Daylight Time | | | | | | |
| [Time shift for this packet: 0.000000000 seconds] | | | | | | |
| Epoch Time: 1602369337.343532000 seconds | | | | | | |
| [Time delta from previous captured frame: 0.000370000 seconds] | | | | | | |
| [Time delta from previous displayed frame: 0.000000000 seconds] | | | | | | |
| [Time since reference or first frame: 11.566389000 seconds] | | | | | | |
| Frame Number: 1613 | | | | | | |
| Frame Length: 535 bytes (4280 bits) | | | | | | |
| Capture Length: 535 bytes (4280 bits) | | | | | | |
| [Frame is marked: False] | | | | | | |
| [Frame is ignored: False] | | | | | | |
| [Protocols in frame: eth:ethertype:ip:tcp:http] | | | | | | |
| [Coloring Rule Name: HTTP] | | | | | | |
| [Coloring Rule String: http tcp.port == 80 http2] | | | | | | |
| Ethernet II, Src: Microsof_17:b3:06 (c4:9d:ed:17:b3:06), Dst: Tp-LinkT_a3:b3:27 (68:ff:7b:a3:b3:27) | | | | | | |
| Destination: Tp-LinkT_a3:b3:27 (68:ff:7b:a3:b3:27) | | | | | | |
| Source: Microsof_17:b3:06 (c4:9d:ed:17:b3:06) | | | | | | |
| Type: IPv4 (0x0800) | | | | | | |
| Internet Protocol Version 4, Src: 192.168.1.110, Dst: 128.119.245.12 | | | | | | |
| Transmission Control Protocol, Src Port: 51442, Dst Port: 80, Seq: 1, Ack: 1, Len: 481 | | | | | | |
| Hypertext Transfer Protocol | | | | | | |

Figure 3. Message for GET

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|-----------------|----------------|---------------|----------|--------|-----------------------------|
| 1682 | 09:35:37.624921 | 128.119.245.12 | 192.168.1.110 | HTTP | 492 | HTTP/1.1 200 OK (text/html) |
| Frame 1682: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{C4B97F8B-4A14-4252-BB93-497BF370C1B6}, id 0 | | | | | | |
| Interface id: 0 (\Device\NPF_{C4B97F8B-4A14-4252-BB93-497BF370C1B6}) | | | | | | |
| Encapsulation type: Ethernet (1) | | | | | | |
| Arrival Time: Oct 11, 2020 09:35:37.624921000 AUS Eastern Daylight Time | | | | | | |
| [Time shift for this packet: 0.000000000 seconds] | | | | | | |
| Epoch Time: 1602369337.624921000 seconds | | | | | | |
| [Time delta from previous captured frame: 0.010840000 seconds] | | | | | | |
| [Time delta from previous displayed frame: 0.281389000 seconds] | | | | | | |
| [Time since reference or first frame: 11.847778000 seconds] | | | | | | |
| Frame Number: 1682 | | | | | | |
| Frame Length: 492 bytes (3936 bits) | | | | | | |
| Capture Length: 492 bytes (3936 bits) | | | | | | |
| [Frame is marked: False] | | | | | | |
| [Frame is ignored: False] | | | | | | |
| [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines] | | | | | | |
| [Coloring Rule Name: HTTP] | | | | | | |
| [Coloring Rule String: http tcp.port == 80 http2] | | | | | | |
| Ethernet II, Src: Tp-LinkT_a3:b3:27 (68:ff:7b:a3:b3:27), Dst: Microsof_17:b3:06 (c4:9d:ed:17:b3:06) | | | | | | |
| Destination: Microsof_17:b3:06 (c4:9d:ed:17:b3:06) | | | | | | |
| Source: Tp-LinkT_a3:b3:27 (68:ff:7b:a3:b3:27) | | | | | | |
| Type: IPv4 (0x0800) | | | | | | |
| Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.110 | | | | | | |
| Transmission Control Protocol, Src Port: 80, Dst Port: 51442, Seq: 1, Ack: 482, Len: 438 | | | | | | |
| Hypertext Transfer Protocol | | | | | | |
| Line-based text data: text/html (3 lines) | | | | | | |

Figure 4. Message for OK

3 Phase II: Ethernet and Address Resolution Protocol

3.1 Capture and analyzing Ethernet frames

Step 4:

HTTP GET message:

- I. The MAC address of my laptop is c4:9d:ed:17:b3:06
- II. The MAC address of destination is 68:ff:7b:a3:b3:27. It is the MAC address of my router which is connected to my laptop.
- III. That "0x0800" is corresponding to the Internet Protocol.
- IV. The "G" from GET starts from the 54th (in decimal) byte.

```
· Ethernet II, Src: Microsof_17:b3:06 (c4:9d:ed:17:b3:06), Dst: Tp-LinkT_a3:b3:27 (68:ff:7b:a3:b3:27)
> Destination: Tp-LinkT_a3:b3:27 (68:ff:7b:a3:b3:27)
> Source: Microsof_17:b3:06 (c4:9d:ed:17:b3:06)
Type: IPv4 (0x0800)
```

Figure 5. Ethernet II information

```
030 01 02 37 c8 00 00 47 45 54 20 2f 77 69 72 65 73 ..7...GE /wires
040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 65 hark-lab s/HTTP-e
050 74 68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 thereal- lab-file
060 33 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 3.html H TTP/1.1
070 0a 48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 .Host: g aia.cs.u
080 6d 61 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 mass.edu .Connec
090 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 tion: ke ep-alive
0a0 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 .Upgrad e-Insecu

is 54-56: Request Method (http.request.method)
```

Figure 6.

HTTP response message:

- I. The MAC address of source is 68:ff:7b:a3:b3:27. It is the MAC address of my router which is connected to my laptop.
- II. The destination address is c4:9d:ed:17:b3:06. It is the MAC address of my laptop.
- III. That "0x0800" is corresponding to the Internet Protocol.
- IV. The "O" from the 13th (in decimal) byte.

```
· Ethernet II, Src: Tp-LinkT_a3:b3:27 (68:ff:7b:a3:b3:27), Dst: Microsof_17:b3:06 (c4:9d:ed:17:b3:06)
> Destination: Microsof_17:b3:06 (c4:9d:ed:17:b3:06)
> Source: Tp-LinkT_a3:b3:27 (68:ff:7b:a3:b3:27)
Type: IPv4 (0x0800)
```

Figure 7. Packet information

```
Date: Sun, 11 Oct 2020 12:48:35 GMT\r\n
0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 45 0d HTTP/1.1 200 OK
0010 0a 44 61 74 65 3a 20 53 75 6e 2c 20 31 31 20 4f .Date: S un, 11 O
0020 63 74 20 32 30 32 30 20 31 32 3a 34 38 3a 33 35 ct 2020 12:48:35
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 31 30 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e 10 mod_p erl/2.0.

Frame (595 bytes) Reassembled TCP (4861 bytes)
Bytes 13-14: Response Phrase (http.response.phrase)
```

Figure 8.

3.2 Address Resolution Protocol

Step 9: We have IP address, Physical address and type columns in ARP Caching table. Physical address is the MAC address. The Type stands for the protocol type which is indicated about the mapping methods.

| Interface: 192.168.1.113 --- 0x15 | | |
|-----------------------------------|-------------------|---------|
| Internet Address | Physical Address | Type |
| 192.168.1.1 | 68-ff-7b-a3-b3-27 | dynamic |
| 192.168.1.103 | 0c-b5-27-bd-a9-f5 | dynamic |
| 192.168.1.106 | 10-08-c1-4f-a9-35 | dynamic |
| 192.168.1.255 | 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 |

Figure 9. Result for arp -a

Step 10: Source address is c4:9d:ed:17:b3:06. it is the MAC address of my laptop

Destination address is ff:ff:ff:ff:ff:ff, namely, the broadcasting address

Step 11: 0x0806. It is corresponding to Address Resolution Protocol.

Step 12:

- a) The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.
- b) 0x00 01 for request.
- c) Yes, it does contain the ip address of sender.
- d) The target MAC address, namely, the 00:00:00:00:00:00 part. It is set to broadcasting MAC

address to question the machine whose corresponding IP address (in this case, 192.168.1.106) is being queried.

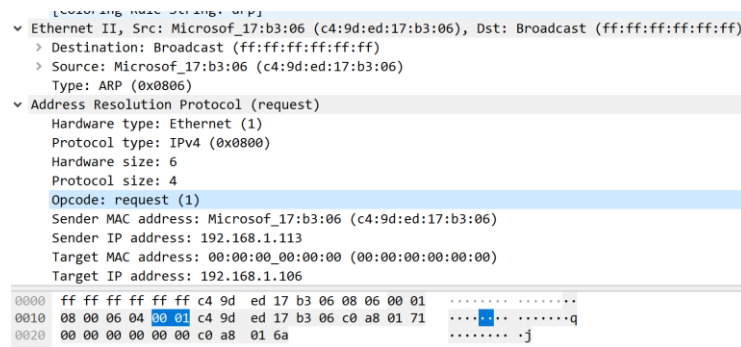


Figure 10. ARP request

Step 13:

- The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.
- 0x 00 02 for reply.
- The sender Mac address (10:08:c1:4f:fa:35). It indicates the MAC address for IP: 192.168.1.10

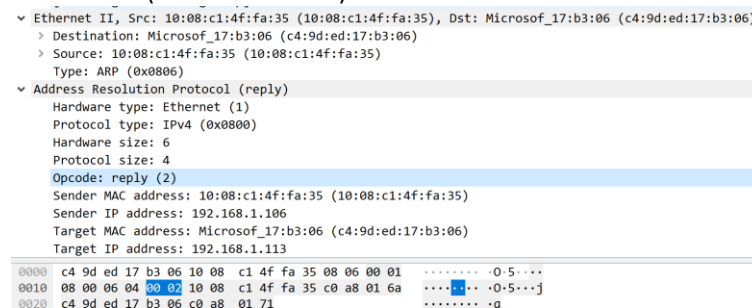


Figure 11. ARP reply

Step 14: Destination MAC address: c4:9d:ed:17:b3:06, namely, the MAC address of my laptop.
Source MAC address: 10:08:c1:4f:fa:35.

Step 15:

Although ARP request is broadcast message, but the ARP reply is not. The ARP reply only send from the sender node to the destination node, s.t. there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace.