LAB 2 – Application Layer

Name – Sati, Ankit Date – 9/30/2021

Section - 001

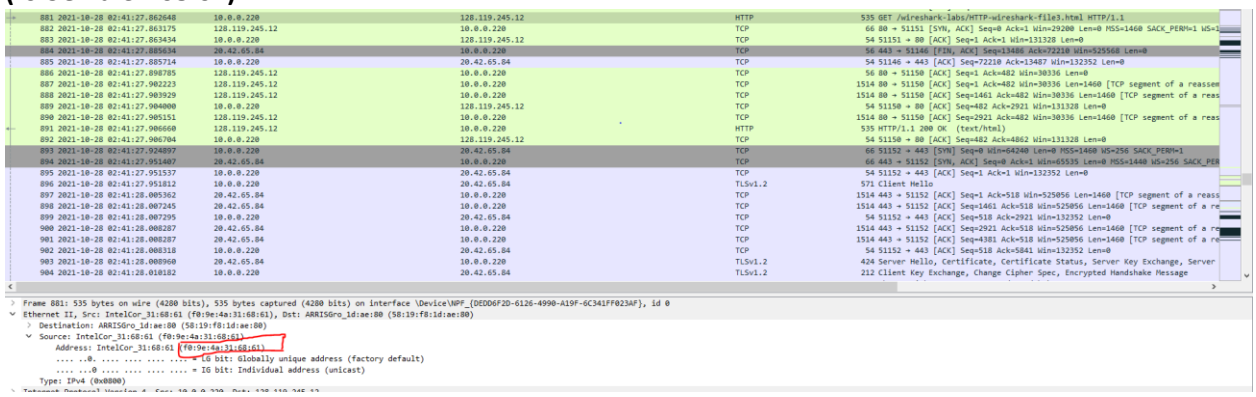
Total in points (Maximum 100 points)–

Professors Comments –

Affirmation of Independent Effort – Ankit Sati

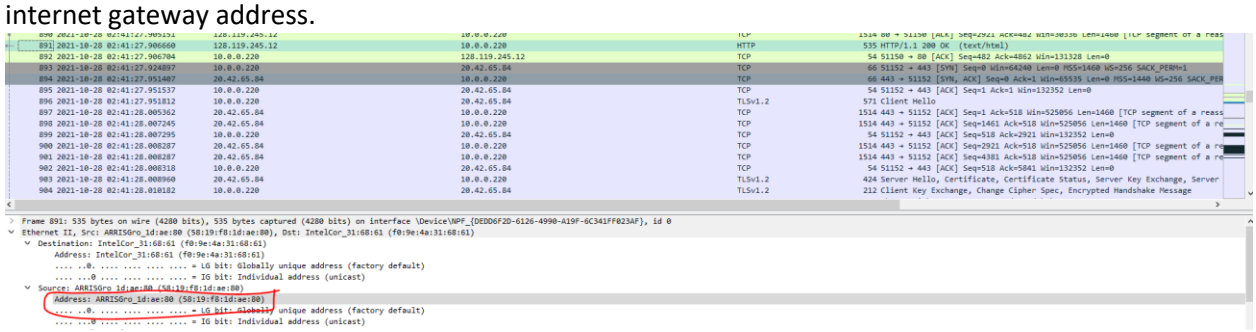
Problem 1

1. IP address(48 bit) of my computer is marked below. - Address: IntelCor_31:68:61 **(f0:9e:4a:31:68:61)**



2. IP address of destination frame. For this question we need to look at the **acknowledgement** message.
   Address: ARRISGro_1d:ae:80 **(58:19:f8:1d:ae:80)**

   This is not the Ethernet address of gaia.cs.umass.edu. It is the mac address for my **router** or internet gateway address.



3. The hexadecimal frame type field in the ethernet header of this packet is **0x0800**.
   It indicates that the upper layer protocol is **Internet Protocol version 4 (IPv4)**

   Source: ARRISGro_1d:ae:80 (58:19:f8:1d:ae:80)
   Address: ARRISGro_1d:ae:80 (58:19:f8:1d:ae:80)
   .... ..0. .... = LG bit: Globally unique address (factory default)
   ....0 .... = IG bit: Individual address (unicast)
   Type: IPv4 (0x0800)

4. This gets **55 bytes** as shown in the screenshot below.

```
> Transmission Control Protocol, Src Port: 51150, Dst Port: 80, Seq: 1, Ack: 1, Len: 481
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36 Edg/95.0.1020.30\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
```

```
0030  02 01 82 5b 00 00 47 45  54 20 2f 77 69 72 65 73
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 33 2e 68
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d
00b0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65
00c0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61
00d0  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54
00e0  20 31 30 2e 30 3b 20 57  69 6e 36 34 3b 20 78 36
00f0  34 29 20 41 70 70 6c 65  57 65 62 4b 69 74 2f 35
```

5. No, this is the address of the router to which my PC is connected to.

   Source: ARRISGro_1d:ae:80 (58:19:f8:1d:ae:80)

   Address: ARRISGro_1d:ae:80 **(58:19:f8:1d:ae:80)**

   .... ..0. .... = LG bit: Globally unique address (factory default)

   ....0 .... = IG bit: Individual address (unicast)

   First ACK message.

878	2021-10-28 02:41:27.860190	10.0.0.220	20.42.65.84	TCP	54	51146 → 443 [FIN, ACK] Seq=72209 Ack=13486 Win=132352 Len=
879	2021-10-28 02:41:27.862122	128.119.245.12	10.0.0.220	TCP	66	80 → 51150 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
880	2021-10-28 02:41:27.862235	10.0.0.220	128.119.245.12	TCP	54	51150 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
881	2021-10-28 02:41:27.862648	10.0.0.220	128.119.245.12	HTTP	535	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
882	2021-10-28 02:41:27.863175	128.119.245.12	10.0.0.220	TCP	66	80 → 51151 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
883	2021-10-28 02:41:27.863434	10.0.0.220	128.119.245.12	TCP	54	51151 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0

6. Yes, this is the Ethernet address of my PC.

   Destination: IntelCor_31:68:61 **(f0:9e:4a:31:68:61)**

   Address: IntelCor_31:68:61 (f0:9e:4a:31:68:61)

   .... ..0. .... = LG bit: Globally unique address (factory default)

   ....0 .... = IG bit: Individual address (unicast)

7. The Hex value of the first two frames is given below.

   0x00000800 - **0x0800**.

   It indicates that the upper layer protocol is **Internet Protocol version 4 (IPv4)**

8. The total distance is 13 bytes.

   Screenshot attached below for reference.

```
v Hypertext Transfer Protocol
  v 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: Thu, 28 Oct 2021 06:41:28 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Thu, 28 Oct 2021 05:59:02 GMT\r\n
```

```
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  68 75 2c 20 32 38 20 4f   ·Date: T hu, 28 O
0020  63 74 20 32 30 32 1 20  30 36 3a 34 31 3a 32 38   ct 2021  06:41:28
```

Problem 2 – Observing ARP Protocol in action

9. The 3 columns represent **the IP Address at the network layer, the MAC Address** to physically communicate with the hardware that is located at that IP address, and whether or not it is changing **dynamic or static.**
   a. **the IP Address at the network layer**
   b. **the MAC Address to physically communicate**
   c. **dynamic or static.**

```
Microsoft Windows [Version 10.0.19042.1288]
(c) Microsoft Corporation. All rights reserved.

C:\windows\system32>arp -a

Interface: 169.254.142.49 --- 0x12
  Internet Address      Physical Address      Type
  169.254.255.255       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

Interface: 10.0.0.220 --- 0x14
  Internet Address      Physical Address      Type
  10.0.0.1              58-19-f8-1d-ae-80     dynamic
  10.0.0.156            e4-f0-42-1e-b5-9b     dynamic
  10.0.0.255            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

Interface: 172.30.96.1 --- 0x37
  Internet Address      Physical Address      Type
  172.30.111.255        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
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\windows\system32>
```

ARP IN ACTION

1. The values are mentioned below.

   Destination: Broadcast (ff:ff:ff:ff:ff:ff)
   Address: Broadcast (f:ff:ff:ff:ff:ff)
   .... ..0. .... = LG bit: Globally unique address (factory default)
   ....0 .... = IG bit: Individual address (unicast)
   Source: ARRISGro_1d:ae:80 (58:19:f8:1d:ae:80)
   Address: ARRISGro_1d:ae:80 (58:19:f8:1d:ae:80)
   .... ..0. .... = LG bit: Globally unique address (factory default)
   ....0 .... = IG bit: Individual address (unicast)

2. The Hexadecimal value is **0x0806.**
   the bit flags represent a **mulitcast (broadcast) that is sent to hte subnet** and not the internet

3. The answers given below for the files.
   a. It begins from **20 bytes**. (21 if you count 0)
   b. The value of the opcode field is **001.**
   c. **Yes** it does contain the IP of the sender.
   d. This information can be seen in the **Target IP Address.**

4. **ARP reply.**
   a. This is like the one above which equal to **20 bytes**. (21 if you count 0)
   b. The value of the opcode field is **002.**
   c. This information is available in the **sender MAC address**.

5. Both the values are mentioned below.
   Values taken from part 1.

   Destination: ff:ff:ff:ff:ff:ff
   Source: 58:19:f8:1d:ae:80

6. There is no reply because, this host computer is not the router that maintains the ARP table and therefore does not give the sender an answer. Only the router running the network will respond to the ARP request.
   It is an IP address within the same subnet that the router has already mapped in its ARP table and does not need to be rediscovered and chronicled.

Extra credit

EX1.

- This not a common scenario because generally IP's are traced to a specific ethernet address. If we have entered the correct IP, It will be able to resolve and locate it in the ARP table. This can lead to two scenarios.
  Scenario 1 – It will not be able to update the value since there is a look ahead and look back counter which can trace a difference in the **Ethernet address for the same IP address.**
  Scenario 2 – In a rare case it can add one of the new values to the table but this will soon result in breaking the chain and the old ethernet address will be resolved soon. If not we will hit a roadblock as the router information is different. (**This does not happen in IPV4**)

EX2.

- From the screenshot attached below we can see the cache allocated to the MAC of the system.

Answer – How much time ?

This depends on the device that we are working on.

MAC of our system – 20 mins and then the table refreshes. (my device Windows)

This depends on many factors right down to the version of windows and caching policies.

How to check this

- We can use the below command and select the interface to check the caching policy .

```
C:\Users\ankit>netsh interface ipv4 show interfaces

Idx     Met         MTU          State                Name
---  ----------  ----------  ------------  ---------------------------
  1          75  4294967295  connected     Loopback Pseudo-Interface 1
 20          35        1500  connected     Wi-Fi
 14          25        1500  disconnected  Local Area Connection* 1
 10          65        1500  disconnected  Bluetooth Network Connection
  8          25        1500  disconnected  Local Area Connection* 2
 13           5        1500  disconnected  Ethernet 2
 18          25        1500  connected     Npcap Loopback Adapter
 55          15        1500  connected     vEthernet (WSL)

C:\Users\ankit>netsh interface ipv4 show interface 13

Interface Ethernet 2 Parameters
----------------------------------------------
IfLuid                             : ethernet_32771
IfIndex                            : 13
State                              : disconnected
Metric                             : 5
Link MTU                           : 1500 bytes
Reachable Time                     : 16500 ms
Base Reachable Time                : 30000 ms
Retransmission Interval            : 1000 ms
DAD Transmits                      : 3
Site Prefix Length                 : 64
Site Id                            : 1
Forwarding                         : disabled
Advertising                        : disabled
Neighbor Discovery                 : enabled
Neighbor Unreachability Detection  : enabled
Router Discovery                   : dhcp
Managed Address Configuration      : enabled
Other Stateful Configuration       : enabled
Weak Host Sends                    : disabled
Weak Host Receives                 : disabled
Use Automatic Metric               : disabled
Ignore Default Routes              : disabled
Advertised Router Lifetime         : 1800 seconds
Advertise Default Route            : disabled
Current Hop Limit                  : 0
Force ARPND Wake up patterns       : disabled
Directed MAC Wake up patterns      : disabled
ECN capability                     : application
RA Based DNS Config (RFC 6106)     : disabled
DHCP/Static IP coexistence         : disabled
```