

## Lab 6

Name: Mohammad Alhomidan

ID: 2510431

My IP 192.168.0.5

```
C:\windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\user>ipconfig

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Wireless Network Connection:

    Connection-specific DNS Suffix . :
    IPv6 Address. . . . . : 2600:8806:6101:e600:99f1:4a6c:6bfa:4ada
    Temporary IPv6 Address. . . . . : 2600:8806:6101:e600:8067:c4d8:5453:beef
    Link-local IPv6 Address . . . . . : fe80::99f1:4a6c:6bfa:4ada%12
    IPv4 Address. . . . . : 192.168.0.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::3e37:86ff:fede:1d73%12
                                192.168.0.1

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Tunnel adapter isatap.{05DA48C7-5141-437A-BCED-1F29AF2DE6D1}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Tunnel adapter Local Area Connection* 12:

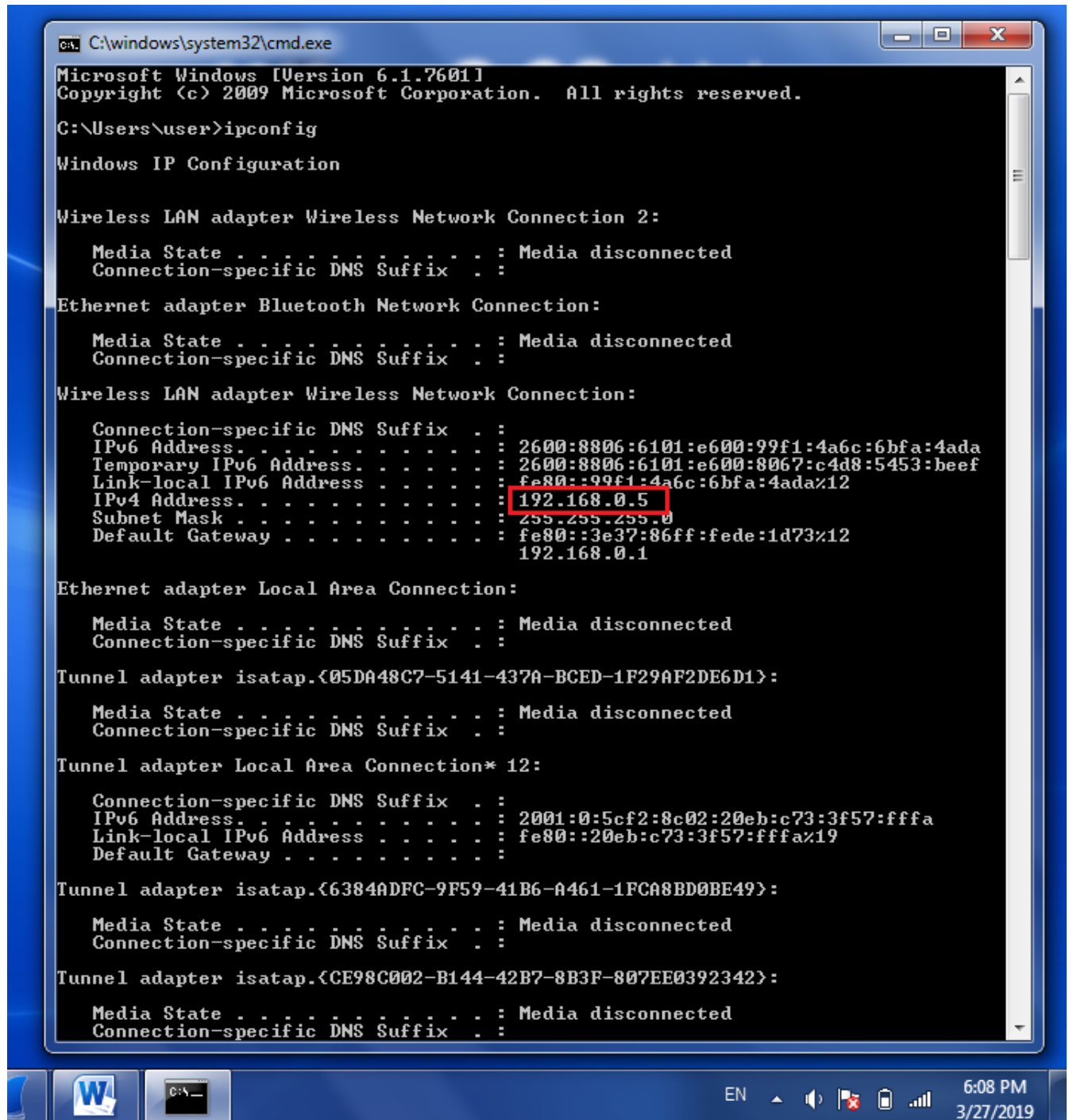
    Connection-specific DNS Suffix . :
    IPv6 Address. . . . . : 2001:0:5cf2:8c02:20eb:c73:3f57:fffa
    Link-local IPv6 Address . . . . . : fe80::20eb:c73:3f57:fffa%19
    Default Gateway . . . . . :

Tunnel adapter isatap.{6384ADFC-9F59-41B6-A461-1FCA8BD0BE49}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Tunnel adapter isatap.{CE98C002-B144-42B7-8B3F-807EE0392342}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
```



# 1. What is the MAC address from your computer?

My computer mac address 38:59:f9:26:b5:f1

The image shows a Wireshark network traffic capture window titled "\*Wireless Network Connection". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar with various icons, and a packet list pane. The packet list pane shows a list of captured packets, with packet 25 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data of the selected packet, with the MAC address 38:59:f9:26:b5:f1 highlighted in red.

No.	Time	Source	Destination	Protocol	Length	Info
25	17:51:54.857801	192.168.0.5	128.119.245.12	HTTP	514	GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP...
33	17:51:54.890561	128.119.245.12	192.168.0.5	HTTP	535	HTTP/1.1 200 OK (text/html)
38	17:51:58.062603	192.168.0.1	192.168.0.5	HTTP/X...	662	NOTIFY /upnp/eventing/rboqhlxyhl HTTP/1.1
39	17:51:58.063308	192.168.0.5	192.168.0.1	HTTP	191	HTTP/1.1 200 OK
56	17:52:01.276484	192.168.0.1	192.168.0.5	HTTP/X...	662	NOTIFY /upnp/eventing/rboqhlxyhl HTTP/1.1
57	17:52:01.277094	192.168.0.5	192.168.0.1	HTTP	191	HTTP/1.1 200 OK

Frame 25: 514 bytes on wire (4112 bits), 514 bytes captured (4112 bits) on interface 0

- Ethernet II, Src: HonHaiPr\_26:b5:f1 (38:59:f9:26:b5:f1), Dst: Netgear\_de:1d:73 (3c:37:86:de:1d:73)
  - Destination: Netgear\_de:1d:73 (3c:37:86:de:1d:73)
  - Source: HonHaiPr\_26:b5:f1 (38:59:f9:26:b5:f1)
    - Address: HonHaiPr\_26:b5:f1 (38:59:f9:26:b5:f1)
    - .... 0. .... = LG bit: Globally unique address (factory default)
    - .... 0. .... = IG bit: Individual address (unicast)
  - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.0.5, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 62455, Dst Port: 80, Seq: 1, Ack: 1, Len: 460
- Hypertext Transfer Protocol

0000 3c 37 86 de 1d 73 38 59 f9 26 b5 f1 08 00 45 00 <7...sBY .&...E.  
0010 01 f4 1d d0 40 00 80 06 a5 02 c0 a8 00 05 80 77 ...@... ..w  
0020 f5 0c f3 f7 00 50 5f df bf 99 64 fe 24 8f 50 18 ....P\_ .d\$.P.  
0030 40 29 37 d6 00 00 47 45 54 20 2f 77 69 72 65 73 @)7...GE T /wires  
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 65 hark-lab s/HTTP-e  
0050 74 68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 thereal- lab-file  
0060 33 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 3.html H TTP/1.1  
0070 0a 48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 .Host: g aia.cs.u  
0080 6d 61 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 mass.edu ..Connec  
0090 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 tion: ke ep-alive  
00a0 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 ..Upgrad e-Insecu  
00b0 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a re-Reque sts: 1..

## 2. What is the destination MAC address?

3c:37:86:de:1d:73

The image shows a Wireshark packet capture window titled '\*Wireless Network Connection'. The packet list shows several packets, with packet 25 selected. The packet details pane shows the following structure:

- Frame 25: 514 bytes on wire (4112 bits), 514 bytes captured (4112 bits) on interface 0
- Ethernet II, Src: HonHaiPr\_26:b5:f1 (38:59:f9:26:b5:f1), Dst: Netgear\_de:1d:73 (3c:37:86:de:1d:73)
  - Destination: Netgear\_de:1d:73 (3c:37:86:de:1d:73)
    - Address: Netgear\_de:1d:73 3c:37:86:de:1d:73
    - .... .. = LG bit: Globally unique address (factory default)
    - .... .. = IG bit: Individual address (unicast)
  - Source: HonHaiPr\_26:b5:f1 (38:59:f9:26:b5:f1)
  - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.0.5, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 62455, Dst Port: 80, Seq: 1, Ack: 1, Len: 460
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data of the selected packet, with the destination MAC address 3c 37 86 de 1d 73 highlighted in blue.

0000 3c 37 86 de 1d 73 38 59 f9 26 b5 f1 08 00 45 00 <7...8Y ·&...E·  
0010 01 f4 1d d0 40 00 80 06 a5 02 c0 a8 00 05 80 77 ...@... ..w  
0020 f5 0c f3 f7 00 50 5f df bf 99 64 fe 24 8f 50 18 ....P\_ ..d.\$·P·  
0030 40 29 37 d6 00 00 47 45 54 20 2f 77 69 72 65 73 @)7...GE T /wires  
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 65 hark-lab s/HTTP-e  
0050 74 68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 thereal- lab-file  
0060 33 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 3.html H TTP/1.1·  
0070 0a 48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 ·Host: g aia.cs.u  
0080 6d 61 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 mass.edu ·Connec  
0090 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 tion: ke ep-alive  
00a0 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 ·Upgrad e-Insecu  
00b0 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a re-Reque sts: 1·

The system tray at the bottom shows the date and time as 6:38 PM 3/27/2019.

3. What device has the MAC address shown in the destination?

Netgear which is my router.

The image shows a Wireshark packet capture window titled "Wireless Network Connection". The packet list pane displays several HTTP packets. Packet 25 is a GET request from 192.168.0.5 to 128.119.245.12. Packet 33 is the corresponding 200 OK response from 128.119.245.12 to 192.168.0.5. Other packets (38, 39, 56, 57) are NOTIFY and HTTP 1.1 200 OK messages between 192.168.0.1 and 192.168.0.5.

The packet details pane for packet 25 shows the Ethernet II layer with the destination MAC address highlighted in a red box: `3c:37:86:de:1d:73`. The source MAC address is `38:59:f9:26:b5:f1`. The protocol is IPv4 (0x0800).

The packet bytes pane shows the raw data of the packet, with the first few bytes corresponding to the Ethernet II header: `3c 37 86 de 1d 73 38 59 f9 26 b5 f1 08 00 45 00`.

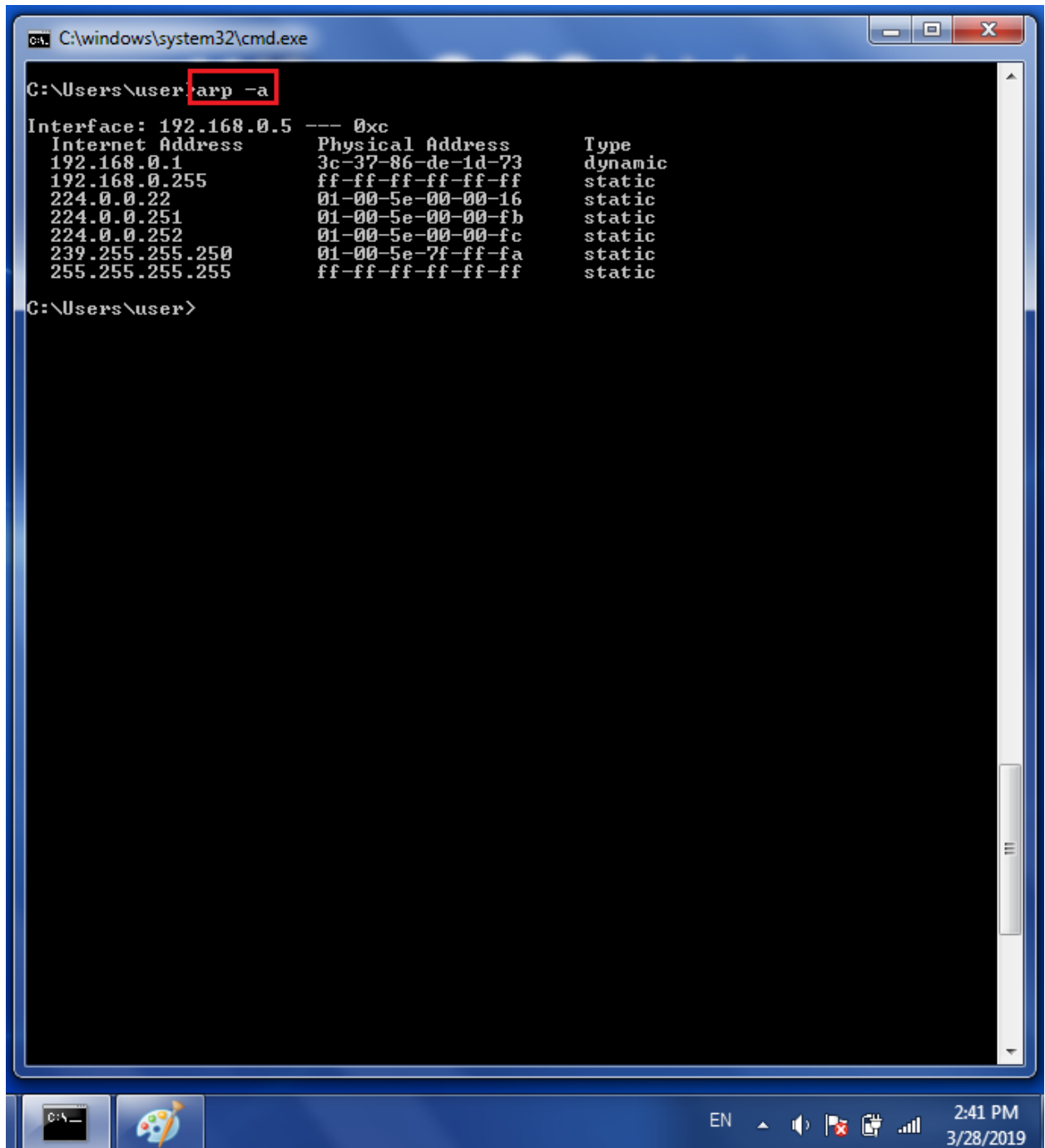
The system tray at the bottom shows the date and time as 6:47 PM on 3/27/2019.

4. Explain the relationship between the destination MAC address and the destination IP address.

There are totally different. MAC address is unique and hard coded by manufacturer. The ARP stores the MAC addresses for all devices that connect to the router. The destination IP address is the router's IP.

- Using the terminal (cmd in Windows, Terminal in mac), run a command to display your full ARP list table. (Find out what the command is, and print a full screen shot of your result.)

The command is arp -a



The screenshot shows a Windows Command Prompt window titled "C:\windows\system32\cmd.exe". The command prompt shows the user's current directory as "C:\Users\user\" and the command "arp -a" has been entered. The output of the command is displayed as follows:

```
Interface: 192.168.0.5 --- 0xc
Internet Address      Physical Address      Type
192.168.0.1           3c-37-86-de-1d-73    dynamic
192.168.0.255         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
```

The command prompt then shows the prompt "C:\Users\user>" indicating that the command has been executed successfully.

C:\Users\user\Desktop\Marymount University\IT-520\Sixth lab.pcapng 73  
total packets, 6 shown

No. Time Source Destination Protocol Length Info 33 17:51:54.890561  
128.119.245.12 192.168.0.5 HTTP 535 HTTP/1.1 200 OK (text/html) Frame  
33: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on  
interface 0 Ethernet II, Src: Netgear\_de:1d:73 (3c:37:86:de:1d:73), Dst:  
HonHaiPr\_26:b5:f1 (38:59:f9:26:b5:f1) Internet Protocol Version 4, Src:  
128.119.245.12, Dst: 192.168.0.5 Transmission Control Protocol, Src Port:  
80, Dst Port: 62455, Seq: 4381, Ack: 461, Len: 481 [4 Reassembled TCP  
Segments (4861 bytes): #29(1460), #30(1460), #32(1460), #33(481)]  
Hypertext Transfer Protocol Line-based text data: text/html (98 lines)