Lab 08: IP Fragmentation and DHCP

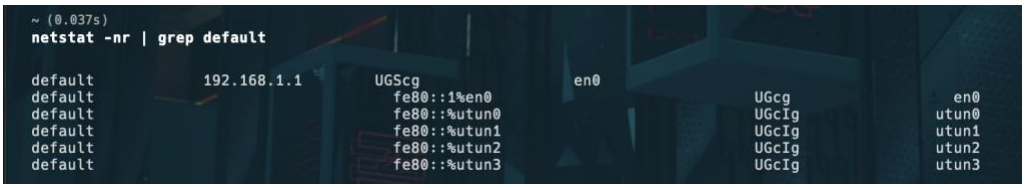
ในปฏิบัติการส่วนนี้เราจะศึกษาการทำ fragmentation ของ Internet Protocol version 4 (IPv4) และ Dynamic Host Configuration Protocol (DHCP)

A. IPv4 Fragmentation

ในส่วนนี้เราจะศึกษาการทำ Fragmentation ของ IPv4 datagram ที่มีขนาดใหญ่เกินกว่า Maximum Transmission Unit (MTU) ของ link ซึ่งสำหรับกรณีของ Ethernet ทั่วไป จะใช้ค่าใช้ MTU เป็น 1500 bytes กรณีที่ IPv4 datagram มีขนาดเกินกว่าค่าดังกล่าว จึงจำเป็นต้องผ่านการทำ fragmentation ให้กลายเป็นหลาย IPv4 datagrams ที่มีขนาดเล็กลง แนะนำให้ผู้เรียนศึกษาเรื่อง IP fragmentation เพิ่มเติมจากหนังสือ ซึ่งสามารถเข้าถึงเอกสารบางส่วนได้จาก http://gaia.cs.umass.edu/kurose_ross/Kurose_Ross_7th_edition_section_4.3.2.pdf จากนั้นให้ทำตามการทดลองตามขั้นตอนต่อไปนี้

1. เปิด Wireshark และเริ่มทำการ capture packet โดยใช้ Capture filter ต่อไปนี้

```
icmp
```

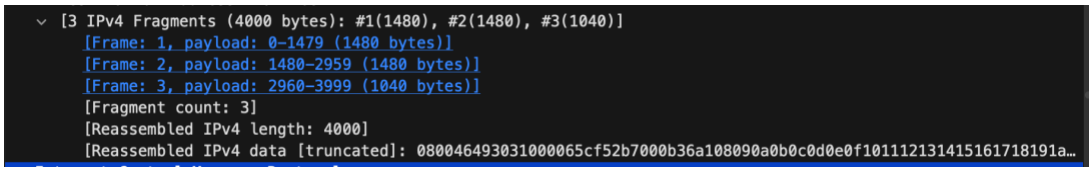
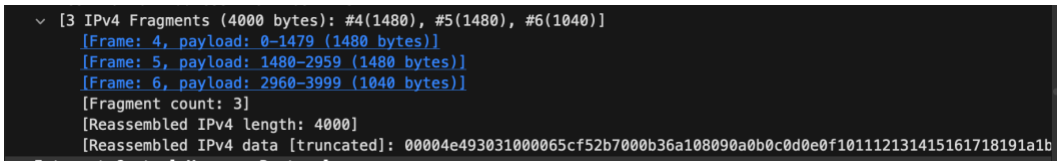
2. เปิดหน้าต่าง command prompt (สำหรับกรณีของ Microsoft Windows) หรือ terminal/shell (สำหรับ Linux หรือ Mac OS)
3. ในหน้า command prompt หรือ terminal ให้พิมพ์คำสั่งต่อไปนี้เพื่อส่ง ICMP echo request ขนาด 3992 bytes โดยให้แทนที่ <gw> ด้วยหมายเลข IPv4 ของ default gateway และสำหรับ Mac OS ให้ใช้ -s แทน -l
4. 

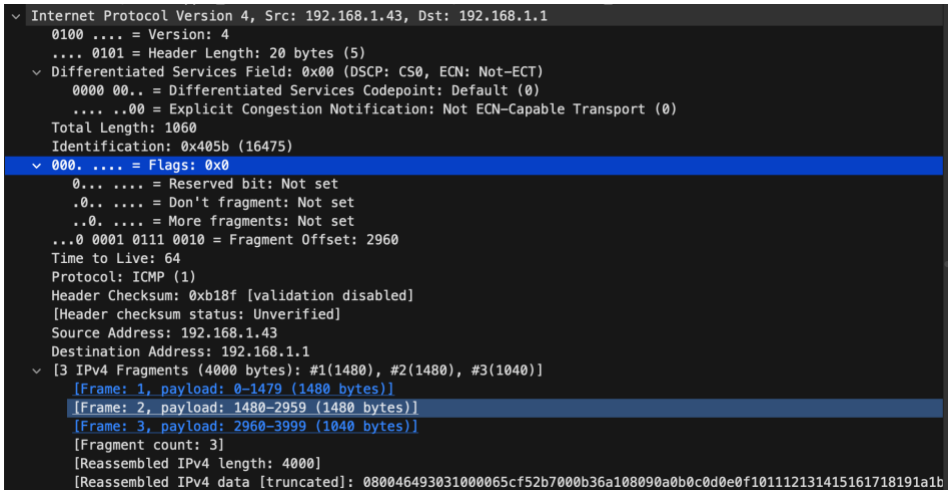

```
ping -s 3992 192.168.1.1
```

5. รอจนการ ping เสร็จสิ้นแล้วจึงสลับไปหน้า Wireshark และสั่งให้หยุด capture
6. ให้ save ไฟล์ไว้ด้วยชื่อ Lab08-A.pcapng

Questions (A)

ศึกษาข้อมูลจากไฟล์ packet capture และตอบคำถามต่อไปนี้

1) จาก ICMP echo request ที่ส่งจากเครื่องของผู้เรียนไปยัง gaia.cs.umass.edu แต่ละ echo request ถูกแบ่งออกเป็น IPv4 datagrams กี่ datagrams? แต่ละ datagram มีขนาดเท่าใดบ้าง?
   a. 
```
[3 IPv4 Fragments (4000 bytes): #1(1480), #2(1480), #3(1040)]
    [Frame: 1, payload: 0-1479 (1480 bytes)]
    [Frame: 2, payload: 1480-2959 (1480 bytes)]
    [Frame: 3, payload: 2960-3999 (1040 bytes)]
    [Fragment count: 3]
    [Reassembled IPv4 length: 4000]
    [Reassembled IPv4 data [truncated]: 080046493031000065cf52b7000b36a108090a0b0c0d0e0f101112131415161718191a…
```
   b. 3 datagrams
   c. 1480 , 1480 , 1040
2) จาก ICMP echo reply ที่ส่งจาก gaia.cs.umass.edu มายังเครื่องผู้เรียน แต่ละ echo reply ถูกแบ่งออกเป็น IPv4 datagrams กี่ datagrams? แต่ละ datagram มีขนาดเท่าใดบ้าง?
   a. 
```
[3 IPv4 Fragments (4000 bytes): #4(1480), #5(1480), #6(1040)]
    [Frame: 4, payload: 0-1479 (1480 bytes)]
    [Frame: 5, payload: 1480-2959 (1480 bytes)]
    [Frame: 6, payload: 2960-3999 (1040 bytes)]
    [Fragment count: 3]
    [Reassembled IPv4 length: 4000]
    [Reassembled IPv4 data [truncated]: 00004e493031000065cf52b7000b36a108090a0b0c0d0e0f101112131415161718191a1b
```
   b. 3 datagrams
   c. 1480 , 1480 , 1040
3) พิจารณาขนาดของแต่ละ IPv4 fragment จากข้อ 1) และ 2) หลังจากผ่านการ fragmentation แล้ว แต่ละคู่ echo request / echo reply ถูกแบ่งเป็น IPv4 datagrams โดยฝั่งผู้ส่งและผู้รับมีแนวทางการกำหนดขนาดของแต่ละ IPv4 fragment เหมือนหรือต่างกันอย่างไร? จงอธิบาย
   a. เหมือนกัน
   b. แต่ละคู่ echo request / echo reply ถูกแบ่งเป็น IPv4 datagrams โดยฝั่งผู้ส่งและผู้รับมีแนวทางการกำหนดขนาดของแต่ละ IPv4 fragment แบบเดียวกันตาม Maximum Transmission Unit (MTU) ของเครือข่ายระหว่างสองอุปกรณ์ที่สื่อสารกัน
4) ข้อมูลใดใน IPv4 header ที่สามารถใช้บ่งบอกว่า datagram นี้ผ่านการ fragmentation มาแล้ว?

a. 

```
Internet Protocol Version 4, Src: 192.168.1.43, Dst: 192.168.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1060
    Identification: 0x405b (16475)
    000. .... = Flags: 0x0
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    ...0 0001 0111 0010 = Fragment Offset: 2960
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0xb18f [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.43
    Destination Address: 192.168.1.1
    [3 IPv4 Fragments (4000 bytes): #1(1480), #2(1480), #3(1040)]
        [Frame: 1, payload: 0-1479 (1480 bytes)]
        [Frame: 2, payload: 1480-2959 (1480 bytes)]
        [Frame: 3, payload: 2960-3999 (1040 bytes)]
        [Fragment count: 3]
        [Reassembled IPv4 length: 4000]
        [Reassembled IPv4 data [truncated]: 08004649303100006 5cf52b7000b36a108090a0b0c0d0e0f101112131415161718191a1b
```

b. "More Fragments (MF)" ซึ่งถูกใช้ในการบ่งบอกว่า datagram นี้มีการ fragmentation และยังมี fragment อื่นๆ ที่ยังไม่ถึงส่วนสุดท้ายของข้อมูล ดังนั้น เมื่อ MF = 1 แสดงว่ายังมี fragment อื่นที่ยังไม่ได้รับไปต่ออยู่ ในขณะที่ MF = 0 แสดงว่าเป็น fragment สุดท้ายหรือ datagram ที่ไม่ถูกแบ่งต่อไปแล้ว

5) ข้อมูลใดใน IPv4 header ที่สามารถใช้บ่งบอกว่า packet นั้นเป็น fragment แรกหรือเป็น fragment สุดท้าย?

a. "Fragment Offset": ฟิลด์นี้ระบุตำแหน่งของข้อมูลของ fragment ใน datagram ต้นฉบับ โดยใน fragment แรกของ datagram ฟิลด์นี้จะมีค่าเป็น 0 และจะเพิ่มขึ้นตามขนาดของแต่ละ fragment โดยมีหน่วยเป็น 8-byte

b. "More Fragments (MF)": ฟิลด์นี้เป็นบิตที่บอกว่ายังมี fragment อื่นๆ ที่ยังไม่ถึงส่วนสุดท้ายของข้อมูลใน fragment สุดท้ายของ datagram ฟิลด์นี้จะเป็น 0 ซึ่งบ่งบอกว่านี่เป็น fragment สุดท้ายของ datagram และไม่มี fragment เพิ่มเติมที่ยังไม่ได้รับไปต่ออยู่

c. ดังนั้น เมื่อค่าของ "Fragment Offset" ของ fragment เป็น 0 และ "More Fragments (MF)" เป็น 1 แสดงว่านี่เป็น fragment แรกของ datagram ในขณะที่เมื่อ "More Fragments (MF)" เป็น 0 แสดงว่านี่เป็น fragment สุดท้ายของ datagram ที่แบ่งแยกออกมาได้แล้ว

6) พิจารณา IPv4 datagram ที่เป็น fragment ลำดับที่ 2 จากการทำ fragmentation ข้อมูลใดใน IPv4 header ที่สามารถใช้บ่งบอกว่า datagram นี้ไม่ใช่ fragment แรก และไม่ใช่ fragment สุดท้าย?

a. IPv4 datagram ที่เป็น fragment ลำดับที่ 2 จะมีฟิลด์ "Fragment Offset" ที่มากกว่า 0 และ "More Fragments (MF)" เป็น 1 ซึ่งบ่งบอกว่าไม่ใช่ fragment แรก และไม่ใช่ fragment สุดท้ายของ datagram

7) หลังจาก fragmentation หากเปรียบเทียบระหว่าง fragment แรก และ fragment ที่สอง ค่าของ field ใดที่เปลี่ยนแปลงไป?

a. ค่าของฟิลด์ "Fragment Offset" ใน IPv4 header จะมีการเปลี่ยนแปลงไปในแต่ละ fragment เนื่องจาก "Fragment Offset" จะบ่งบอกถึงตำแหน่งของข้อมูลใน fragment นั้นๆ ใน datagram ต้นฉบับ

b. ค่าของฟิลด์ "Total Length" ใน IPv4 header ของแต่ละ fragment ยังมีการปรับเปลี่ยนเพื่อให้สอดคล้องกับขนาดของแต่ละ fragment โดยใน fragment แรก จะมีขนาดที่มากกว่า fragment ที่สอง เนื่องจากมีข้อมูลทั้งหมดของ datagram ที่ถูกตัดแบ่งออกมา

8) พิจารณา IPv4 datagram ที่เป็น fragment ลำดับที่ 3 จากการทำ fragmentation ข้อมูลใดใน IPv4 header ที่สามารถใช้บ่งบอกว่า datagram นี้เป็น fragment สุดท้าย?

a. าของฟิลด์ "More Fragments (MF)" เป็น 0 เพื่อบ่งบอกว่านี่เป็น fragment สุดท้ายของ datagram ที่แบ่งแยกออกมา

B. DHCP in Action

ในการศึกษา DHCP เราจะศึกษาจากไฟล์บันทึกร่องรอยการทำงานของ DHCP ซึ่งจะทำให้ผู้เรียนได้เห็น DHCP message 4 ประเภท เราจำเป็นต้องเรียนรู้การใช้คำสั่งซึ่งจะแตกต่างกันไประหว่างบน Microsoft Windows, Mac OS และ Linux

<u>สำหรับเครื่องที่ใช้ Mac OS</u>

1. ในหน้าต่าง terminal/shell พิมพ์คำสั่งต่อไปนี้

```
sudo ipconfig set en0 none
```

คำสั่งข้างต้นจะเป็นการยกเลิกค่าที่กำหนดให้กับ network interface โดย en0 ในคำสั่งตัวอย่างข้างต้นเป็นชื่อของ network interface ซึ่งผู้เรียนต้องการจะ capture packet ด้วย Wireshark โดยผู้เรียนสามารถทราบรายชื่อ network interface ทั้งหมดได้จากการเข้าเมนู Capture -> Options

2. เปิด Wireshark และเริ่มทำการ capture packet โดยใช้ Capture filter ต่อไปนี้

```
udp port 67 or udp port 68
```

3. ในหน้าต่าง terminal/shell พิมพ์คำสั่งต่อไปนี้

```
sudo ipconfig set en0 dhcp
```

คำสั่งข้างต้นทำให้เครื่องของผู้เรียนส่ง DHCP request เพื่อร้องขอหมายเลข IP address และข้อมูลอื่นๆ จาก DHCP server

4. หลังจากเวลาผ่านไปไม่กี่วินาที ควรปรากฏ DHCP message จาก DHCP server เพื่อแจกจ่ายหมายเลข IP ให้กับเครื่องของผู้เรียน รอให้การทำงานเสร็จสิ้นแล้วจึงสลับไปหน้า Wireshark และสั่งให้หยุด capture
5. ให้ save ไฟล์ไว้ด้วยชื่อ Lab08-B.pcapng

<u>สำหรับเครื่องที่ใช้งาน Linux</u>

1. ในหน้าต่าง terminal/shell พิมพ์คำสั่งต่อไปนี้

```
sudo ip addr flush en0
sudo dhclient -r
```

คำสั่งข้างต้นจะเป็นการยกเลิกค่าหมายเลข IP ที่กำหนดให้กับ network interface โดย en0 ในคำสั่งตัวอย่างข้างต้นเป็นชื่อของ network interface ซึ่งผู้เรียนต้องการจะ capture packet ด้วย Wireshark โดยผู้เรียนสามารถทราบรายชื่อ network interface ทั้งหมดได้จากการเข้าเมนู Capture -> Options

2. เปิด Wireshark และเริ่มทำการ capture packet โดยใช้ Capture filter ต่อไปนี้

```
udp port 67 or udp port 68
```

3. ในหน้าต่าง terminal/shell พิมพ์คำสั่งต่อไปนี้

```
sudo dhclient en0
```

คำสั่งข้างต้นทำให้เครื่องของผู้เรียนส่ง DHCP request เพื่อร้องขอหมายเลข IP address และข้อมูลอื่นๆ จาก DHCP server

4. หลังจากเวลาผ่านไปไม่กี่วินาที ควรปรากฏ DHCP message จาก DHCP server เพื่อแจกจ่ายหมายเลข IP ให้กับเครื่องของผู้เรียน รอให้การทำงานเสร็จสิ้นแล้วจึงสลับไปหน้า Wireshark และสั่งให้หยุด capture
5. ให้ save ไฟล์ไว้ด้วยชื่อ Lab08-B.pcapng

<u>สำหรับเครื่องที่ใช้งาน Microsoft Windows</u>

1. ในหน้าต่าง command prompt พิมพ์คำสั่งต่อไปนี้

```
ipconfig /release
```

คำสั่งข้างต้นจะเป็นการยกเลิกค่าหมายเลข IP และ settings อื่นๆ ที่กำหนดให้กับ network interface ทุก interfaces

2. เปิด Wireshark และเริ่มทำการ capture packet โดยใช้ Capture filter ต่อไปนี้

```
udp port 67 or udp port 68
```

3. ในหน้าต่าง command prompt พิมพ์คำสั่งต่อไปนี้

```
ipconfig /renew
```

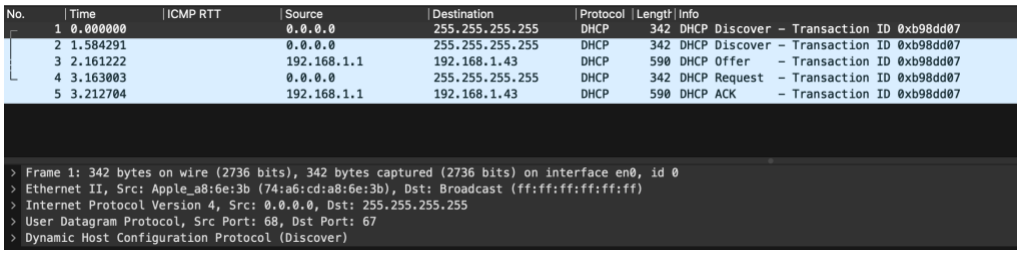
คำสั่งข้างต้นทำให้เครื่องของผู้เรียนส่ง DHCP request เพื่อร้องขอหมายเลข IP address และข้อมูลอื่นๆ จาก DHCP server

4. หลังจากเวลาผ่านไปไม่กี่วินาที ควรปรากฏ DHCP message จาก DHCP server เพื่อแจกจ่ายหมายเลข IP ให้กับเครื่องของผู้เรียน รอให้การทำงานเสร็จสิ้นแล้วจึงสลับไปหน้า Wireshark และสั่งให้หยุด capture
5. ให้ save ไฟล์ไว้ด้วยชื่อ Lab08-B.pcapng

Questions (B)

หลังจากทำตามขั้นตอนข้างต้นแล้ว ให้ใช้ Display filter เป็น dhcp เพื่อกรองให้แสดงเฉพาะ DHCP message จากไฟล์ packet capture ที่ save เอาไว้ เพื่อใช้ในการตอบคำถามต่อไปนี้ โดยในช่วงแรกจะเป็นคำถามเกี่ยวกับ DHCP Discover message

9) ตรวจสอบ DHCP Discover message ว่าถูกส่งออกไปโดยใช้ Transport Layer Protocol เป็น UDP หรือ TCP?

a. 

b. UDP

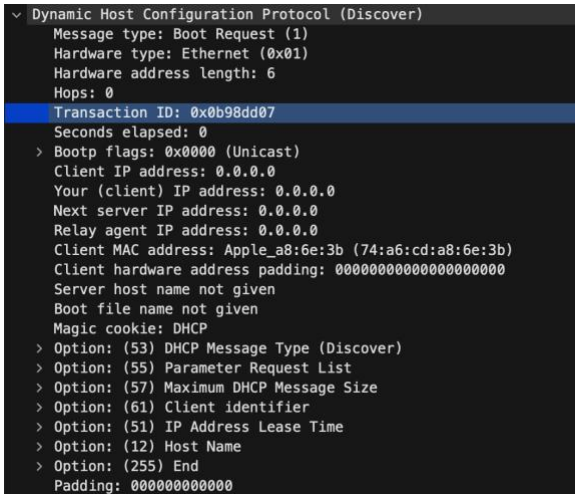
10) ตรวจสอบ IP datagram ซึ่งบรรจุ Discover message ว่าใช้หมายเลข source IP address หมายเลขใด? หมายเลขดังกล่าวเป็นหมายเลขที่มีความพิเศษอย่างไรหรือไม่? จงอธิบาย

a. หมายเลข IP 0.0.0.0 ใช้เป็นที่อยู่ IP ของแหล่งที่มาในกรณีที่อุปกรณ์ไม่มีที่อยู่ IP แสดงถึงอุปกรณ์ที่ยังไม่ได้รับการกำหนด IP หรือไม่มี IP ในขณะนั้น มันเป็นหมายเลขพิเศษเพราะมันใช้ในกระบวนการขอที่อยู่ IP จาก DHCP server เมื่ออุปกรณ์เริ่มต้นขึ้นและพยายามที่จะเชื่อมต่อกับเครือข่าย โดยปกติ มันจะส่ง DHCP Discover message โดยใช้ 0.0.0.0 เป็นที่อยู่ IP ของต้นทาง เพราะมันยังไม่มีที่อยู่ IP ที่ถูกกำหนดมาก่อนหน้านี้

11) ตรวจสอบ IP datagram ซึ่งบรรจุ Discover message ว่าใช้หมายเลข destination IP address หมายเลขใด? หมายเลขดังกล่าวเป็นหมายเลขที่มีความพิเศษอย่างไรหรือไม่? จงอธิบาย

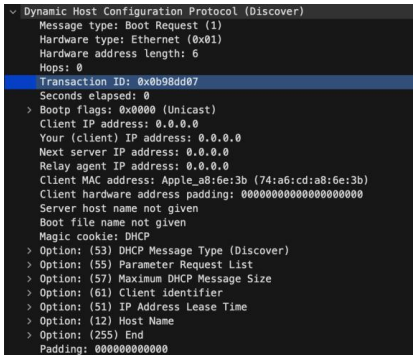
a. หมายเลข IP ปลายทาง 255.255.255.255 เป็นที่อยู่ broadcast address ซึ่งใช้ในการส่งข้อมูลไปยังทุกอุปกรณ์ภายในเครือข่าย (local network). ในกรณีนี้, DHCP Discover message ถูกส่งไปยังที่อยู่นี้เพื่อให้ทุก DHCP servers ที่เชื่อมต่อกับเครือข่ายสามารถรับและตอบสนองต่อคำขอได้.

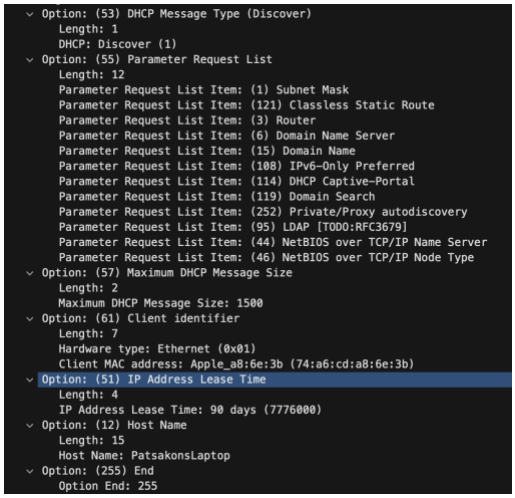
12) ค่าของ transaction ID ที่อยู่ใน DHCP Discover message มีค่าเป็นเท่าใด?

a. 
```
Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x0b98dd07
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Apple_a8:6e:3b (74:a6:cd:a8:6e:3b)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (55) Parameter Request List
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (51) IP Address Lease Time
  > Option: (12) Host Name
  > Option: (255) End
    Padding: 000000000000
```

b. Transaction ID: 0x0b98dd07

13) ตรวจสอบ Option ใน DHCP Discover message มีข้อมูลใดอื่นอีกบ้างนอกจากหมายเลข IP address ที่ client เสนอหรือว่าร้องขอจาก DHCP server? จงระบุข้อมูลมาอย่างน้อย 5 อย่าง

a. 
```
Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x0b98dd07
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Apple_a8:6e:3b (74:a6:cd:a8:6e:3b)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (55) Parameter Request List
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (51) IP Address Lease Time
  > Option: (12) Host Name
  > Option: (255) End
    Padding: 000000000000
```

b. 

```
Option: (53) DHCP Message Type (Discover)
    Length: 1
    DHCP: Discover (1)
Option: (55) Parameter Request List
    Length: 12
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (121) Classless Static Route
    Parameter Request List Item: (3) Router
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (15) Domain Name
    Parameter Request List Item: (108) IPv6-Only Preferred
    Parameter Request List Item: (114) DHCP Captive-Portal
    Parameter Request List Item: (119) Domain Search
    Parameter Request List Item: (252) Private/Proxy autodiscovery
    Parameter Request List Item: (95) LDAP [TODO:RFC3679]
    Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
    Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
Option: (57) Maximum DHCP Message Size
    Length: 2
    Maximum DHCP Message Size: 1500
Option: (61) Client identifier
    Length: 7
    Hardware type: Ethernet (0x01)
    Client MAC address: Apple_a8:6e:3b (74:a6:cd:a8:6e:3b)
Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: 90 days (7776000)
Option: (12) Host Name
    Length: 15
    Host Name: PatsakonsLaptop
Option: (255) End
    Option End: 255
```

ในลำดับถัดมา เราจะมาศึกษา DHCP Offer message ซึ่ง DHCP server ส่งมาเพื่อตอบ DHCP Discover message ที่ผู้เรียนได้ศึกษาไปในข้อ 9) ถึงข้อ 13)

14) ผู้เรียนทราบได้อย่างไรว่า DHCP Offer message นี้ถูกส่งมาเพื่อตอบ DHCP Discover message ที่ผู้เรียนได้ศึกษาไปในข้อ 9) ถึงข้อ 13) ที่ผ่านมา
    a. Transaction ID: 0x0b98dd07
    b. เพราะ Transaction ID เหมือนกัน
15) ตรวจสอบ IP datagram ซึ่งบรรจุ Offer message ว่าใช้หมายเลข source IP address หมายเลขใด? หมายเลขดังกล่าวเป็นหมายเลขที่มีความพิเศษอย่างไรหรือไม่? จงอธิบาย
    a. หมายเลข Source IP Address
        i. 192.168.1.1 เป็นหมายเลข IP ที่เป็นส่วนหนึ่งของช่วง IP ที่สงวนไว้สำหรับเครือข่ายส่วนตัว (Private Networks) ตาม RFC 1918. ช่วง IP นี้ไม่ได้ถูกใช้ในอินเทอร์เน็ตสาธารณะแต่ใช้ภายในเครือข่ายส่วนตัว เช่น ภายในบ้านหรือองค์กร. 192.168.1.1 มักจะใช้เป็นที่อยู่ IP สำหรับเราเตอร์หรือเกตเวย์ในเครือข่ายส่วนตัว, ซึ่งทำหน้าที่เป็น DHCP server ให้บริการที่อยู่ IP ให้กับอุปกรณ์ภายในเครือข่าย.
16) ตรวจสอบ IP datagram ซึ่งบรรจุ Offer message ว่าใช้หมายเลข destination IP address หมายเลขใด? หมายเลขดังกล่าวเป็นหมายเลขที่มีความพิเศษอย่างไรหรือไม่? จงอธิบาย (คำใบ้: ตรวจสอบไฟล์ trace อย่างละเอียด คำตอบของคำถามนี้อาจจะแตกต่างจากภาพในเอกสารประกอบการเรียน)
    a. หมายเลข Destination IP Address
        i. 192.168.1.43 ก็เป็นหมายเลข IP ภายในช่วงเดียวกันกับ 192.168.1.1, หมายถึงเป็นส่วนหนึ่งของช่วง IP สำหรับเครือข่ายส่วนตัว. ในกรณีนี้, หมายเลขนี้คือหมายเลข IP ที่ DHCP server

เสนอให้กับอุปกรณ์ที่ส่ง DHCP Discover message ไปก่อนหน้านี้. มันไม่ได้มีความพิเศษในทางเทคนิคเหมือนกับ 0.0.0.0 หรือ 255.255.255.255, แต่มันเป็นหมายเลขที่ DHCP server กำหนดให้เพื่อใช้งานภายในเครือข่ายนั้นๆ.

17) ตรวจสอบ Option ใน DHCP Offer message มีข้อมูลใดอื่นอีกบ้างนอกจากหมายเลข IP address ที่ DHCP server ส่งให้กับ DHCP client? จงระบุข้อมูลมาอย่างน้อย 5 อย่าง

a.

```
  ⌄ Option: (53) DHCP Message Type (Offer)
      Length: 1
      DHCP: Offer (2)
  ⌄ Option: (54) DHCP Server Identifier (192.168.1.1)
      Length: 4
      DHCP Server Identifier: 192.168.1.1
  ⌄ Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: 1 day (86400)
  ⌄ Option: (1) Subnet Mask (255.255.255.0)
      Length: 4
      Subnet Mask: 255.255.255.0
  ⌄ Option: (3) Router
      Length: 4
      Router: 192.168.1.1
  ⌄ Option: (6) Domain Name Server
      Length: 4
      Domain Name Server: 192.168.1.1
  ⌄ Option: (255) End
      Option End: 255
    Padding [truncated]: 000000000000000000000000000000000000000000000000
```

จากการตอบคำถามข้างต้น ผู้เรียนอาจสังเกตได้ว่าหลังจากที่ได้รับ DHCP Offer message แล้ว ฝั่ง client ได้ข้อมูลทั้งหมดที่ต้องการแล้ว อย่างไรก็ดี client อาจจะรับ Offer มาจาก DHCP servers หลายเครื่อง ดังนั้นจึงมีความจำเป็นที่ต้องมีรับส่ง messages เพิ่มเติมอีก 2 message นั้นคือ DHCP Request message ที่ส่งจาก client ไปยัง server และ DHCP ACK message ที่ส่งจาก server มายัง client โดยการรับส่ง DHCP message ในครึ่งแรกที่ผ่านไปแล้วนั้น อย่างน้อยก็ทำให้ client ทราบว่ามี DHCP server ให้บริการ ถัดจากนี้จะเป็นการสำรวจ DHCP Request message

18) ตรวจสอบ IP datagram ซึ่งบรรจุ DHCP Request message ว่าใช้หมายเลข source port หมายเลขใด? และใช้ destination port หมายเลขใด?

    a. หมายเลข source IP address คือ 0.0.0.0

    b. หมายเลข destination IP address คือ 255.255.255.255

19) ตรวจสอบ IP datagram ซึ่งบรรจุ Request message ว่าใช้หมายเลข source IP address หมายเลขใด? หมายเลขดังกล่าวเป็นหมายเลขที่มีความพิเศษอย่างไรหรือไม่? จงอธิบาย

a. หมายเลข Source IP Address

i. 0.0.0.0 เป็นหมายเลข IP address ที่มีความพิเศษ ใช้ในสถานการณ์ที่อุปกรณ์ไม่มีหมายเลข IP address ที่กำหนดไว้ล่วงหน้า หรือเมื่ออุปกรณ์กำลังพยายามขอหรือตั้งค่าที่อยู่ IP ของตนเองผ่าน DHCP. ในกรณีนี้, การใช้ 0.0.0.0 เป็น source address ใน DHCP Request message หมายความว่า อุปกรณ์ที่ส่งข้อความนี้ยังไม่มีที่อยู่ IP ที่ถูกกำหนดและกำลังร้องขอที่อยู่ IP จาก DHCP server.

20) ตรวจสอบ IP datagram ซึ่งบรรจุ Request message ว่าใช้หมายเลข destination IP address หมายเลขใด? หมายเลขดังกล่าวเป็นหมายเลขที่มีความพิเศษอย่างไรหรือไม่? จงอธิบาย

a. หมายเลข Destination IP Address

i. 255.255.255.255 เป็นหมายเลข IP address ที่ใช้เป็น destination address สำหรับการส่งข้อมูลไปยังทุกอุปกรณ์ในเครือข่ายส่วนตัวหรือเครือข่ายท้องถิ่น (local network). การใช้ 255.255.255.255 ใน DHCP Request message หมายความว่าข้อความนี้ถูกส่งไปยังทุกอุปกรณ์ภายในเครือข่าย เพื่อให้ DHCP server ที่อยู่ในเครือข่ายเดียวกันสามารถรับและประมวลผลคำขอนี้ได้. มันเป็นวิธีการที่ใช้ในกรณีที่อุปกรณ์ยังไม่รู้ว่า DHCP server มีที่อยู่ IP อะไร, เพื่อให้สามารถสื่อสารและรับที่อยู่ IP ที่ถูกต้องได้.

21) ค่าของ transaction ID ที่อยู่ใน DHCP Request message มีค่าเป็นเท่าใด? ค่าดังกล่าวมีค่าตรงกับ transaction ID ใน Discover message และ Offer message ก่อนหน้านี้หรือไม่?

a. Transaction ID: 0x0b98dd07

b. ตรงกัน

22) ตรวจสอบค่า Options ใน DHCP Discover message โดยให้ตรวจสอบ Parameter Request List ซึ่ง DHCP RFC ระบุเอาไว้ว่า

"The client can inform the server which configuration parameters the client is interested in by including the 'parameter request list' option. The data portion of this option explicitly lists the options requested by tag number."

ผู้เรียนสังเกตเห็นความแตกต่างใดบ้างระหว่าง Parameter Request List ที่พบใน Request message และ Discover message ก่อนหน้านี้

a.

```
Option: (50) Requested IP Address (192.168.1.43)
    Length: 4
    Requested IP Address: 192.168.1.43
Option: (54) DHCP Server Identifier (192.168.1.1)
    Length: 4
    DHCP Server Identifier: 192.168.1.1
```

b. Option (50) บ่งบอกถึงที่อยู่ IP ที่ไคลเอนต์ร้องขอหลังจากที่ได้รับ DHCP Offer

c. Option (54) บ่งบอกถึงตัวตนของ DHCP server ที่ไคลเอนต์ตอบกลับ

สำหรับคำถามส่วนสุดท้าย ให้ค้นหา DHCP ACK message จากไฟล์ trace และตอบคำถามต่อไปนี้

23) ตรวจสอบ IP datagram ซึ่งบรรจุ ACK message ว่าใช้หมายเลข source IP address หมายเลขใด? หมายเลขดังกล่าวเป็นหมายเลขที่มีความพิเศษอย่างไรหรือไม่? จงอธิบาย

a. หมายเลข Source IP Address

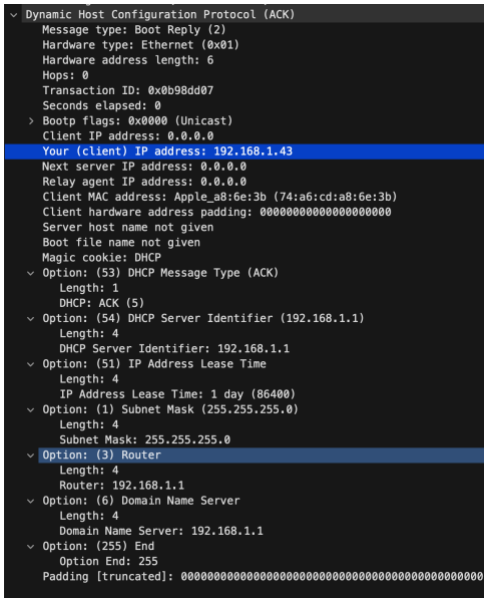
i. 192.168.1.1 เป็นหมายเลข IP ที่เป็นส่วนหนึ่งของช่วง IP ที่สงวนไว้สำหรับเครือข่ายส่วนตัว (Private Networks) ตาม RFC 1918. ช่วง IP นี้ไม่ได้ถูกใช้ในอินเทอร์เน็ตสาธารณะแต่ใช้ภายในเครือข่ายส่วนตัว เช่น ภายในบ้านหรือองค์กร. 192.168.1.1 มักจะใช้เป็นที่อยู่ IP สำหรับเราเตอร์หรือเกตเวย์ในเครือข่ายส่วนตัว, ซึ่งทำหน้าที่เป็น DHCP server ให้บริการที่อยู่ IP ให้กับอุปกรณ์ภายในเครือข่าย.

24) ตรวจสอบ IP datagram ซึ่งบรรจุ ACK message ว่าใช้หมายเลข destination IP address หมายเลขใด? หมายเลขดังกล่าวเป็นหมายเลขที่มีความพิเศษอย่างไรหรือไม่? จงอธิบาย

a. หมายเลข Destination IP Address

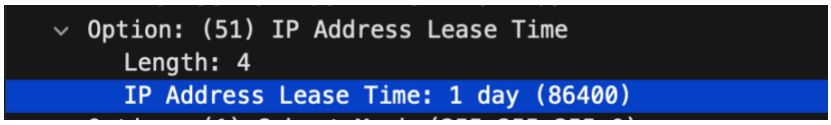
i. 192.168.1.43 ก็เป็นหมายเลข IP ภายในช่วงเดียวกันกับ 192.168.1.1, หมายถึงเป็นส่วนหนึ่งของช่วง IP สำหรับเครือข่ายส่วนตัว. ในกรณีนี้, หมายเลขนี้คือหมายเลข IP ที่ DHCP server เสนอให้กับอุปกรณ์ที่ส่ง DHCP Discover message ไปก่อนหน้านี้. มันไม่ได้มีความพิเศษในทางเทคนิคเหมือนกับ 0.0.0.0 หรือ 255.255.255.255, แต่มันเป็นหมายเลขที่ DHCP server กำหนดให้เพื่อใช้งานภายในเครือข่ายนั้นๆ.

25) ใน DHCP ACK message มี field ชื่ออะไร (ตามที่ปรากฏใน Wireshark) ที่เก็บค่าหมายเลข IP address ที่ DHCP server แจกจ่ายให้กับ client?

a. 

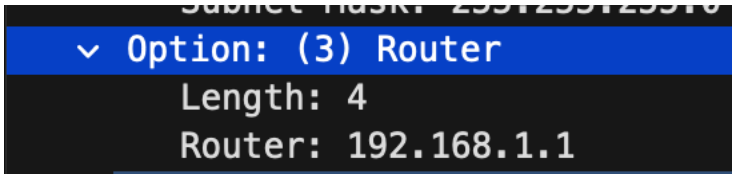
b. Your (client) IP address: 192.168.1.43

26) DHCP server อนุญาตให้ client ใช้งานหมายเลข IP เป็นระยะเวลานานเท่าใด? (คำใบ้: โปรดสังเกต lease time)

a. 

b. 1 day

27) ใน DHCP ACK message ที่ DHCP server ส่งกลับมาให้กับ DHCP client ระบุหมายเลข IP ของ first-hop router (หรือที่เรียกว่า default gateway) เป็นหมายเลขอะไร?

a. 

b. 192.168.1.1

จงตอบคำถามในส่วนที่ระบุหัวข้อ Question ตั้งแต่ (A) ไปจนถึง (B) ซึ่งมีคำถามร่วมทั้งหมด 27 ข้อ โดยในคำตอบของแต่ละข้อด้วยให้อธิบายด้วยว่าหาคำตอบมาได้อย่างไร ตัวอย่างเช่น อธิบายว่าสามารถค้น packet ตามที่โจทย์ระบุได้ด้วยวิธีการใด หรือค่าที่นำมาตอบ นำมาจาก field ใดของ header ตาม protocol ใด

ในกรณีที่คัดลอกคำตอบของคนอื่นมา ให้ระบุชื่อของบุคคลที่เป็นต้นฉบับมาด้วย หากตรวจพบว่ามีการลอกมาแต่ไม่มีการระบุชื่อบุคคลที่เป็นต้นฉบับ ผู้สอนจะถือว่าทุจริตและอาจพิจารณาลงโทษให้ตกเกณฑ์รายวิชาในทันที

การส่งงาน ให้เขียนหรือพิมพ์หมายเลขข้อและคำตอบของข้อนั้นๆ และส่งเป็นไฟล์ PDF เท่านั้น กรุณาตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา ตามด้วย section และ _lab08 ตามตัวอย่างต่อไปนี้ 64019999_sec20_lab08.pdf