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

```
ping -l 3992 <gw>
```

4. รอจนการ ping เสร็จสิ้นแล้วจึงสลับไปหน้า Wireshark และสั่งให้หยุด capture
5. 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?

   3 datagrams 1500, 1500, 1060

   ดูได้จาก ip.len

2) จาก ICMP echo reply ที่ส่งจาก gaia.cs.umass.edu มายังเครื่องผู้เรียน แต่ละ echo reply ถูกแบ่งออกเป็น IPv4 datagrams กี่ datagrams? แต่ละ datagram มีขนาดเท่าใดบ้าง?

   3 datagrams 1500, 1500, 1060

   ดูได้จาก ip.len

3) พิจารณาขนาดของแต่ละ IPv4 fragment จากข้อ 1) และ 2) หลังจากผ่านการ fragmentation แล้ว แต่ละคู่ echo request / echo reply ถูกแบ่งเป็น IPv4 datagrams โดยฝั่งผู้ส่งและผู้รับมีแนวทางการกำหนดขนาดของแต่ละ IPv4 fragment เหมือนหรือต่างกันอย่างไร? จงอธิบาย

   เหมือนกันเพราะค่าMTUมีค่าเท่ากันเนื่องด้วยใช้linkเส้นเดียวกัน

4) ข้อมูลใดใน IPv4 header ที่สามารถใช้บ่งบอกว่า datagram นี้ผ่านการ fragmentation มาแล้ว?

   Flags: 0x1 แปลว่ามี more fragment

   ดูได้จาก packet detail pane ของ IP

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

   Flags: 0x1 แปลว่ามี more fragment และ fragment แรก offset=0

   ดูได้จาก packet detail pane ของ IP

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

   Flags: 0x1 แปลว่ามี more fragment และ fragment แรก offset=1480/8=135(ในwiresharkคำนวณให้แล้วเป็น1480)

   ดูได้จาก packet detail pane ของ IP

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

   Offset

   ดูได้จาก packet detail pane ของ IP

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

   Flags: 0x0 แปลว่า no more fragment

   ดูได้จาก packet detail pane ของ IP

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

สำหรับเครื่องที่ใช้งาน Linux

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

สำหรับเครื่องที่ใช้งาน Microsoft Windows

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?

   UDP

   ดูจาก packet detail pane

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

    0.0.0.0

    เป็นIPพิเศษในกรณีนี้ใช้งานเมื่อตัวhostไม่มีIP

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

    255.255.255.255

    เป็นเลขที่ไม่ใช่IPจริงๆ เป็นพิเศษแต่จะหมายถึงการbroadcast

12) ค่าของ transaction ID ที่อยู่ใน DHCP Discover message มีค่าเป็นเท่าใด?

    0x7b7c7161

    Packet list pane

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

Client identifier
Host name
Vendor class identifier
Parameter request list
End
ดูได้จาก packet detail pane

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

Transaction ID

15) ตรวจสอบ IP datagram ซึ่งบรรจุ Offer message ว่าใช้หมายเลข source IP address หมายเลขใด? หมายเลขดังกล่าวเป็นหมายเลขที่มีความพิเศษอย่างไรหรือไม่? จงอธิบาย

192.168.1.1 เป็นหมายเลขของ default gateway และ DHCP Server

16) ตรวจสอบ IP datagram ซึ่งบรรจุ Offer message ว่าใช้หมายเลข destination IP address หมายเลขใด? หมายเลขดังกล่าวเป็นหมายเลขที่มีความพิเศษอย่างไรหรือไม่? จงอธิบาย (คำใบ้: ตรวจสอบไฟล์ trace อย่างละเอียด คำตอบของคำถามนี้อาจจะแตกต่างจากภาพในเอกสารประกอบการเรียน)

192.168.1.6 เป็นหมายเลข IP เดิมของclient, เป็นหมายเลข IP ที่ส่งไปตอนขอ

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

DHCP message type
DHCP message identifier
IP address lease time
Subnet mask
Router

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?

    Source port: 68
    Destination port: 67
    UDP packet detail pane

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

    0.0.0.0
    เป็นIPพิเศษในกรณีนี้ใช้งานเมื่อตัวhostไม่มีIP

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

    192.168.1.6 เป็นหมายเลข IP เดิมของclient, เป็นหมายเลข IP ที่ส่งไปตอนขอ

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

    0x7b7c7161 ตรง

    Packet list pane

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

    เหมือนกัน

    Packet detail pane

สำหรับคำถามส่วนสุดท้าย ให้ค้นหา DHCP ACK message จากไฟล์ trace และตอบคำถามต่อไปนี้

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

    192.168.1.1 เป็นหมายเลขของ default gateway และ DHCP Server

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

    192.168.1.6 เป็นหมายเลข IP เดิมของclient, เป็นหมายเลข IP ที่ส่งไปตอนขอ

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

    dhcp.ip.your (Your (client) IP Address)
    DHCP packet detail pane

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

    3 hours
    DHCP packet detail pane

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

    192.168.1.1
    DHCP packet detail pane

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