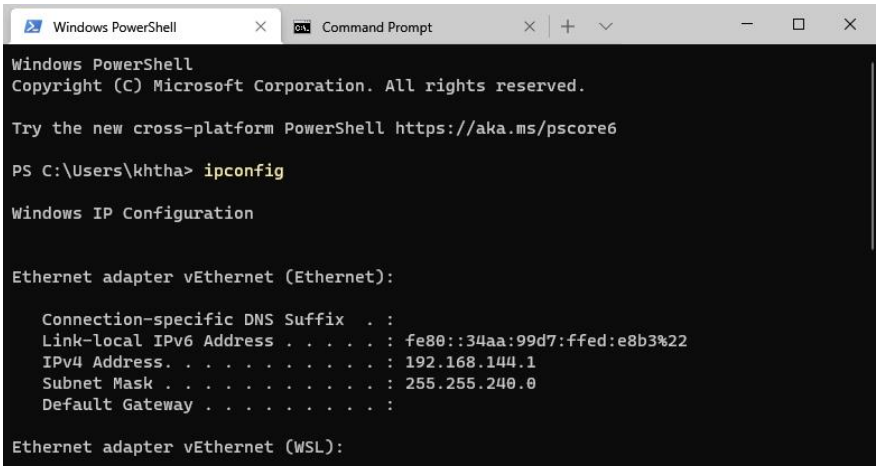
กิจกรรมที่ 9 : DHCP และ NAT

ส่วนที่ 1 DHCP

กิจกรรมนี้การทำความเข้าใจกับ DHCP (Dynamic Host Configuration Protocol) ซึ่งเป็นบริการที่ใช้งานมากทั้งในระบบ Home Network ในมหาวิทยาลัย และในองค์กรต่างๆ โปรโตคอล DHCP ถ้าจะกล่าวง่ายๆ คือเป็นโปรโตคอลที่ทำหน้าที่แจกจ่าย IP Address ให้กับ Host ต่างๆ เพื่อลดภาระในการตั้งค่า IP และลดปัญหาอันเกิดจากการตั้งค่า IP ไม่ถูกต้อง

1. ให้เปิด command prompt และพิมพ์คำว่า ipconfig ให้สังเกต IPv4 ว่ามี Address ใด



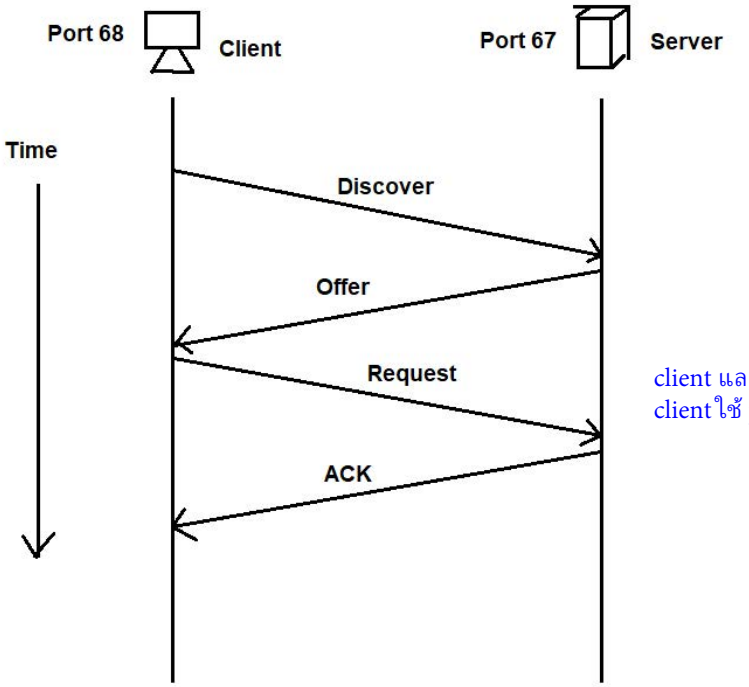
2. จากนั้นให้ใช้คำสั่ง ipconfig /release เพื่อยกเลิกการใช้งาน IP Address
3. ให้เปิดโปรแกรม wireshark กำหนดให้ capture port 67 และ port 68
4. ให้ใช้คำสั่ง ipconfig /renew เพื่อขอ IP Address ใหม่ และรอจนกว่ากระบวนการ renew จะเสร็จสิ้นและแสดงผล จะพบว่า Wireshark สามารถ capture ได้ 4 packet ดังนี้ (ให้นักศึกษาทำ release และ renew อย่างน้อย 2 ครั้ง) เมื่อพอใจแล้วให้หยุด capture

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000…	0.0.0.0	255.255.255.2…	DHCP	342	DHCP Discover - Transaction ID 0x419d79a
2	2.072…	192.168.1.1	192.168.1.4	DHCP	590	DHCP Offer - Transaction ID 0x419d79a
3	2.073…	0.0.0.0	255.255.255.2…	DHCP	356	DHCP Request - Transaction ID 0x419d79a
4	2.172…	192.168.1.1	192.168.1.4	DHCP	590	DHCP ACK - Transaction ID 0x419d79a

5. ให้ตอบคำถามต่อไปนี้
   - DHCP message ส่งผ่าน UDP หรือ TCP

     UDP

- ให้วาด timing diagram ที่แสดงลำดับการทำงานของ packet ทั้ง 4 คือ Discover, Offer, Request และ ACK ที่โต้ตอบระหว่าง client และ server ใช้พอร์ตหมายเลขเดียวกันหรือไม่ อย่างไร

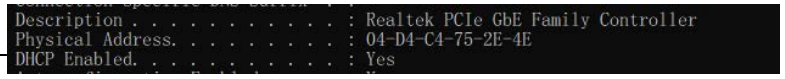


client และ server ใช้คนละ port กันโดย client ใช้ port 68 และ server ใช้ port 67

				srt port	dst port	
2 8.315589	0.0.0.0	255.255.255.255	DHCP	342 68	67	DHCP Discover - Transaction ID 0x85
3 11.361650	192.168.0.1	192.168.0.26	DHCP	351 67	68	DHCP Offer - Transaction ID 0x85
4 11.362440	0.0.0.0	255.255.255.255	DHCP	348 68	67	DHCP Request - Transaction ID 0x85
5 11.375896	192.168.0.1	192.168.0.26	DHCP	360 67	68	DHCP ACK - Transaction ID 0x85

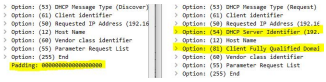
- หมายเลข Ethernet Address ของเครื่อง client (เครื่องของนักศึกษา)

04-D4-C4-75-2E-4E



- ค่าใดใน DHCP Discover ที่ต่างไปจาก DHCP Request

length ใน Request มากกว่า Discover อยู่ 6 bytes โดยค่าที่ต่างกันคือ ใน Request จะมี option : DHCP Serve Identifier และ Client Fully Qualified Domain Name



- ค่าของ Transaction–ID ในชุดข้อมูลแรก (Discover/Offer/Request/ACK) และในชุดข้อมูลที่ 2 เหมือนหรือแตกต่างกันอย่างไร และประโยชน์ของ Transaction–ID คืออะไร

ค่า Transaction-ID ในชุดแรกและชุดที่2 ต่างกัน โดย Transaction-ID ชุดแรกคือ 0x85f84b0 และชุดที่ 2 คือ 0xb11a8b5e

ประโยชน์ของ Transaction-ID คือ เพื่อช่วยให้ server และ client คุยกันได้ถูกต้อง

- เนื่องจาก IP Address จริงจะใช้ได้เมื่อกระบวนการ DHCP ทั้ง 4 ขั้นตอนเสร็จสิ้นสมบูรณ์ ในระหว่างที่กระบวนการยังไม่สิ้นสุด ค่าที่ใช้ใน IP datagram คือ ค่าใดในแต่ละ message ของ Discover/Offer/Request/ACK

client จะใช้ 0.0.0.0 และ server จะใช้ 255.255.255.255

```
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
```

- IP Address ของ DHCP Server คือค่าใด (capture รูปประกอบด้วย)

192.168.0.1

- ใน DHCP Offer message ข้อมูลใด ที่บอกถึง IP Address ที่จะให้เครื่องคอมพิวเตอร์ใช้งาน (capture รูปประกอบด้วย)

```
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.0.26
Next server IP address: 192.168.0.1
Relay agent IP address: 0.0.0.0
```

Your (client) IP address : 192.168.0.26

- ให้ตรวจสอบว่า message DHCP ผ่าน Relay Agent หรือไม่ (Relay Agent คือหมายเลขของ router ที่ส่งต่อ DHCP ไปยัง subnet อื่น) ถ้ามีเป็นหมายเลขใด (capture รูปประกอบด้วย)

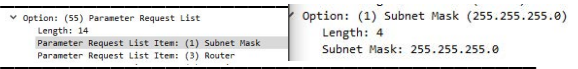
```
Relay agent IP address: 0.0.0.0
```

ไม่มี Relay Agent เนื่องจาก router เป็นตัวจ่าย IP address มาโดยตรง

- DHCP Server ให้ option ของ subnet mask และ router มาด้วยหรือไม่ มีเป้าหมายเพื่ออะไร

ใน request client จะขอ subnet mask ไป และใน ack server จะตอบกลับมา

เพื่อให้ client รู้ว่าต้องใช้ subnet mask อะไร



- อธิบายประโยชน์ของ lease time และเครื่องคอมพิวเตอร์ได้รับ lease time เท่ากับเท่าไร

lease time มีประโยชน์คือเมื่อมี client เคยเชื่อมต่อเป็นจำนวนมาก ถ้าไม่มี lease time อาจจะทำให้ ip ไม่พอใช้ จึงมี lease time เพื่อเมื่อหมดเวลาแล้ว client นั้นไม่ใช้งานก็จะนำ ip นั้นไปให้กับเครื่องอื่น

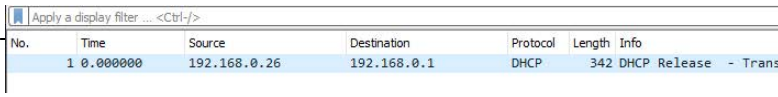
ได้รับ lease time 24 ชั่วโมง

```
Lease Obtained. . . . . : Saturday, March 27, 2021 7:56:24 PM
Lease Expires . . . . . : Sunday, March 28, 2021 7:56:23 AM
```

- อธิบายประโยชน์ของ DHCP release และ DHCP Server มีการตอบโต้กับ DHCP release อย่างไร

DHCP release เป็นการคืน IP

ไม่มีการตอบกลับจาก DHCP Server จนกว่าเครื่องจะทำการ renew ไป



ก่อน Release

```
IPv4 Address. . . . . : 192.168.0.26(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, March 27, 2021 11:17:44 PM
Lease Expires . . . . . : Sunday, March 28, 2021 11:17:43 AM
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
```

หลัง release

```
Default Gateway . . . . . :
```

ส่วนที่ 2 NAT

NAT (Network Address Translation) เป็นบริการหนึ่งที่ใช้งานมาก เช่น ในเครือข่าย WiFi เนื่องจากสามารถใช้ Private IP ที่มีจำนวน IP ไม่จำกัด หรือในเครือข่ายองค์กรที่ได้รับ IP Address มาจำนวนไม่เพียงพอกับจำนวน Host หรือใน Home Network

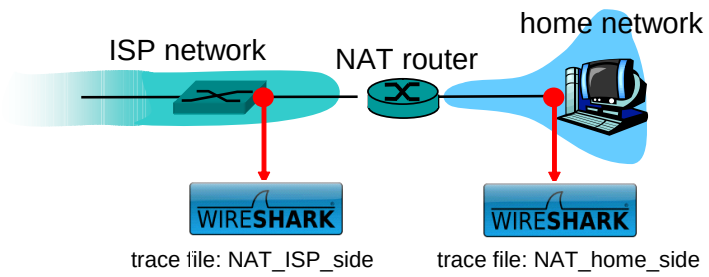


Figure 1: NAT trace collection scenario

จากรูปจะมีไฟล์ที่จัดเตรียมให้โดย capture จากทั้ง 2 ด้านของ NAT Router โดยชื่อ NAT_ISP_side.pcap และ NAT_home_side.pcap

6. ให้เปิดไฟล์ NAT_home_side.pcap และตอบคำถามต่อไปนี้
   - IP Address ของ client เป็นเลขอะไร

     192.168.1.100
   - จากไฟล์ จะพบว่า client ติดต่อกับ server ต่างๆ ของ google โดยเครื่อง server หลักของ google จะอยู่ที่ IP Address 64.233.169.104 ดังนั้นให้ใช้ display filter : http && ip.addr == 64.233.169.104 เพื่อกรองให้เหลือเฉพาะ packet ที่ไปยัง server ดังกล่าว จากนั้นให้ดูที่เวลา 7.109267 ซึ่งเป็น HTTP GET จาก google server ให้บันทึก Source IP Address, Destination IP Address, TCP source port และ TCP destination port ของ packet

     Source IP : 192.168.1.100 , Destination IP : 64.233.169.104

     TCP source port : 4335 , TCP destination port : 80
   - ให้ค้นหา HTTP message ที่เป็น 200 OK ที่ตอบจาก HTTP GET ก่อนหน้า และบันทึก Source IP Address, Destination IP Address, TCP source port และ TCP destination port ของ packet

     Source IP : 64.233.169.104 , Destination IP : 192.168.1.100

     TCP source port : 80 , TCP destination port : 4335
7. ให้เปิดไฟล์ NAT_ISP_side.pcap และตอบคำถามต่อไปนี้
   - ให้หา packet ที่ตรงกับ HTTP GET ในข้อ 6 ที่เวลา 7.109267 เป็นเวลาใดที่ packet ดังกล่าวบันทึกในไฟล์ NAT_ISP_side.pcap ให้บันทึก Source IP Address, Destination IP Address, TCP source port และ TCP destination port ของ packet และบอกว่าข้อมูลใดที่ถูกเปลี่ยนแปลงไป

     เป็นเวลา 6.069168 , Source IP : 71.192.34.104 , Destination IP : 64.233.169.104

     TCP source port : 4335 , TCP destination port : 80 , ข้อมูล Source IP ถูกเปลี่ยนแปลง
   - ในฟิลด์ข้อมูล Version, Header Length, Flags, Checksum มีข้อมูลใดเปลี่ยนแปลงไปหรือไม่ ให้อธิบายเหตุผลที่มีการเปลี่ยนแปลง

     Checksum เปลี่ยนแปลง เนื่องจาก Source IP ไม่เหมือนกันเมื่อเข้า checksum ทำให้ค่าไม่เท่ากัน
   - ให้หา packet ที่ตรงกับ 200 OK ในข้อ 6 ให้บันทึก Source IP Address, Destination IP Address, TCP source port และ TCP destination port ของ packet และบอกว่าข้อมูลใดที่ถูกเปลี่ยนแปลงไป

     Source IP : 64.233.169.104 , Destination IP : 71.192.34.104

     TCP source port : 80 , TCP destination port : 4335 , ข้อมูล Destination IP ถูกเปลี่ยนแปลง

8. ให้เขียน NAT Translation Table โดยใช้ข้อมูลจากข้อ 6 และ 7

Public IP Address	Public Port	Private IP Address	Private IP Port
71.192.34.104	4335	192.168.1.100	4335
64.233.169.104	80	64.233.169.104	80

งานครั้งที่ 10

กำหนดส่ง ภายในวันที่ 28 มีนาคม 2564