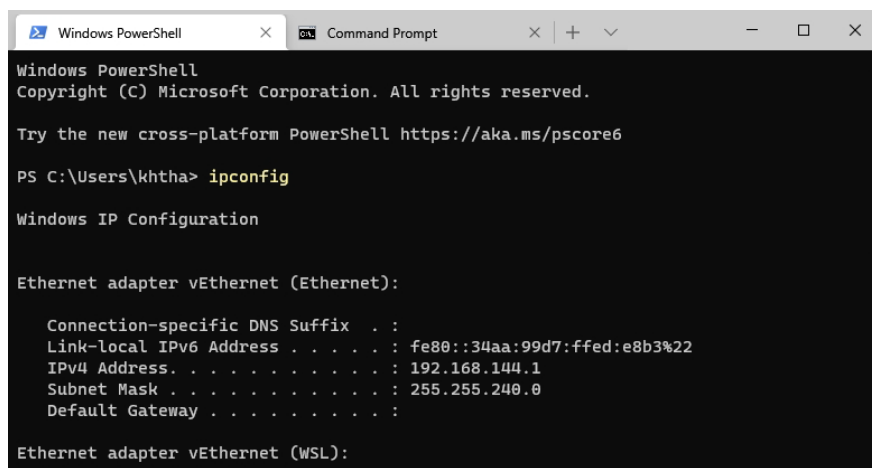


## กิจกรรมที่ 10 : DHCP และ NAT

### 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 ไດ



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\khtha> ipconfig

Windows IP Configuration

Ethernet adapter vEthernet (Ethernet):

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::34aa:99d7:ffed:e8b3%22
    IPv4 Address. . . . . : 192.168.144.1
    Subnet Mask . . . . . : 255.255.240.0
    Default Gateway . . . . . : 

Ethernet adapter vEthernet (WSL):
```

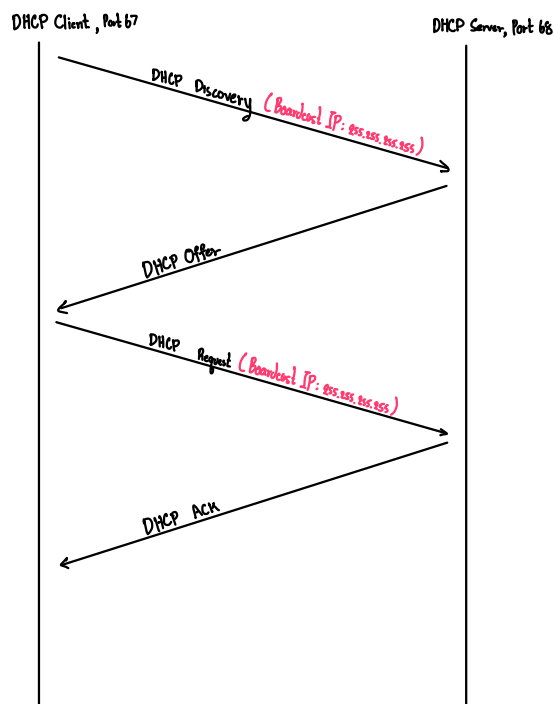
2. จากนั้นให้ใช้คำสั่ง ipconfig /release เพื่อยกเลิกการใช้งาน IP Address
3. ให้เปิดโปรแกรม wireshark กำหนดให้ capture port 67 และ port 68
4. ให้ใช้คำสั่ง ipconfig /renew เพื่อขอ IP Address ใหม่ และรอจนกว่ากระบวนการ renew จะเสร็จสิ้นและแสดงผล จะพบว่า Wireshark สามารถ capture ได้ 4 packet ดังนี้ (ให้นักศึกษาทำ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

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



ผู้รับ: วิชาเน็ต 63010871 SEC 03  
(เริ่ม LAB : 9. 13.00-16.00)

- หมายเลข Ethernet Address ของเครื่อง client (เครื่องของนักศึกษา)

161.256.5.67

- ค่าใดใน DHCP Discover ที่ต่างไปจาก DHCP Request

Option : 54, DHCP Server Identification (4 Bytes), Option : 81, Client Fully Qualified Domain Name.

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

เหมือนกัน , หน้าที่ : ใช้ระบุถึงสถานะ Discover/Offer/Request/ACK ชุดที่หนึ่ง

เพื่อตรวจสอบ Discover or Request กลับไปยังที่ Broadcast Client !

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

Client : Source IP = 0.0.0.0, Dest IP : 255.255.255.255

Server : Source IP = IP Server, Dest IP : 255.255.255.255

- IP Address ของ DHCP Server คือค่าใด (capture รูปประกอบด้วย)

161.146.5.67

7	20.288888	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x930f90b5
8	20.290529	161.246.5.67	161.246.5.66	DHCP	331	DHCP Offer - Transaction ID 0x930f90b5
9	20.291233	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x930f90b5
10	20.296951	161.246.5.67	161.246.5.66	DHCP	331	DHCP ACK - Transaction ID 0x930f90b5

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

Your (client) IP address: 161.246.5.66

- 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

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

Option: (1) Subnet Mask (255.255.255.0)  
Length: 4  
Subnet Mask: 255.255.255.0  
Option: (3) Router  
Length: 4  
Router: 161.246.5.254

ไม่บอกเพื่อให้ client ทราบว่า New IP Subnet Mask และ Router IP ใด.

ไม่บอกเพราะ Client ไม่ได้อยู่ใน Broadcast Network

- อธิบายประโยชน์ของ lease time และเครื่องคอมพิวเตอร์ได้รับ lease time เท่ากับเท่าไร

เพื่อไม่ให้ IP Address Pool ของ DHCP Server (ซอฟต์แวร์/โปรแกรม) ว่าง client ที่ IP ใดไม่ active จะหมด lease time

จะถูกลบ IP address assign ไป client ใหม่

- อธิบายประโยชน์ของ DHCP release และ DHCP Server มีการตอบโต้กับ DHCP release อย่างไร

คืน IP Address กลับ DHCP Server , DHCP Server ตอบ ACK ส่วนไม่มีการ Release

## 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

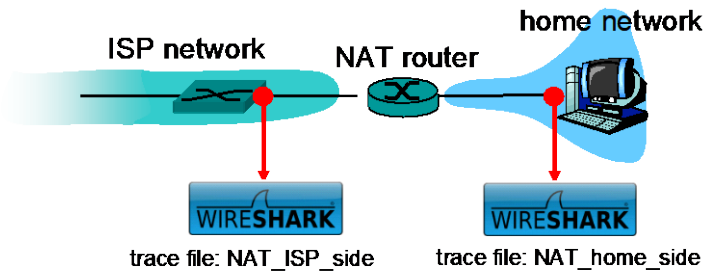


Figure 1: NAT trace collection scenario

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, Source Port: 4995, 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, Source Port: 80, Destination Port: 4995

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

Source IP: 71.192.34.104, Destination IP: 64.233.169.104, Source Port: 4995, Destination Port: 80

- ในฟิลด์ข้อมูล Version, Header Length, Flags, Checksum มีข้อมูลใดเปลี่ยนแปลงไปหรือไม่ ให้อธิบายเหตุผลที่มีการเปลี่ยนแปลง

Version, Header length, Flags ไม่เปลี่ยนแปลง Checksum เพราะ IP Address เปลี่ยน : จาก IP ของ Client ที่ 192.168.1.100:4335

เป็น IP ของ ISP ที่ 71.192.94.104:4335 ที่ไม่เปลี่ยนแปลง checksum เพราะ checksum เปลี่ยน

- ให้นำ packet ที่ตรงกับ 200 OK ในข้อ 6 ให้นำบันทึก Source IP Address, Destination IP Address, TCP source port และ TCP destination port ของ packet และบอกว่าข้อมูลใดที่ถูกเปลี่ยนแปลงไป

Source IP, 64.221.19.104, Destination IP : 71.192.94.104, Source Port : 80, Destination Port : 4335

8. ให้เขียน NAT Translation Table โดยใช้ข้อมูลจากข้อ 6 และ 7

Public IP Address	Public Port	Private IP Address	Private IP Port
71.192.94.104	4335	192.168.1.100	4335

ผู้รับ: วิชา: 63010871 SEC 03  
( เริ่ม LAB : 9. 13.00-16.00 )

#### งานครั้งที่ 10

- การส่งงาน เขียนหรือพิมพ์ลงในเอกสารนี้ และส่งโดยเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา และ \_Lab10 เช่น 64010789\_Lab10.pdf
- กำหนดส่ง ภายในวันที่ 6 เมษายน 2565