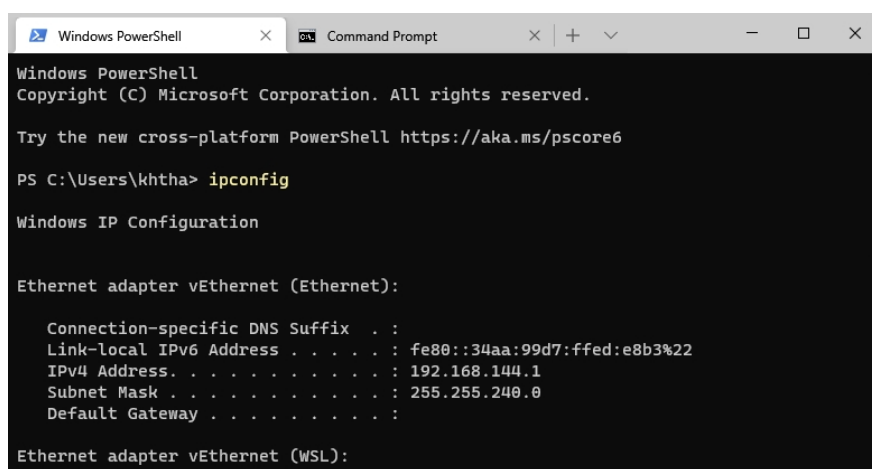


## กิจกรรมที่ 10 : DHCP และ NAT

### ส่วนที่ 1 DHCP

กิจกรรมนี้การทำความเข้าใจกับ DHCP (Dynamic Host Configuration Protocol) ซึ่งเป็นบริการที่ใช้กันมากทั้งในระบบ Home Network ในเครือข่ายมหาวิทยาลัย และในเครือข่ายองค์กรต่างๆ อาจกล่าวโดยง่ายว่า โปรโตคอล DHCP คือเป็นโปรโตคอลที่ทำหน้าที่แจกจ่าย IP Address ให้กับ host ต่างๆ เพื่อลดภาระในการตั้งค่า IP และลดปัญหาอันเกิดจากการตั้งค่า IP ไม่ถูกต้อง

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



```
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 (ให้ผู้เรียนทำ 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

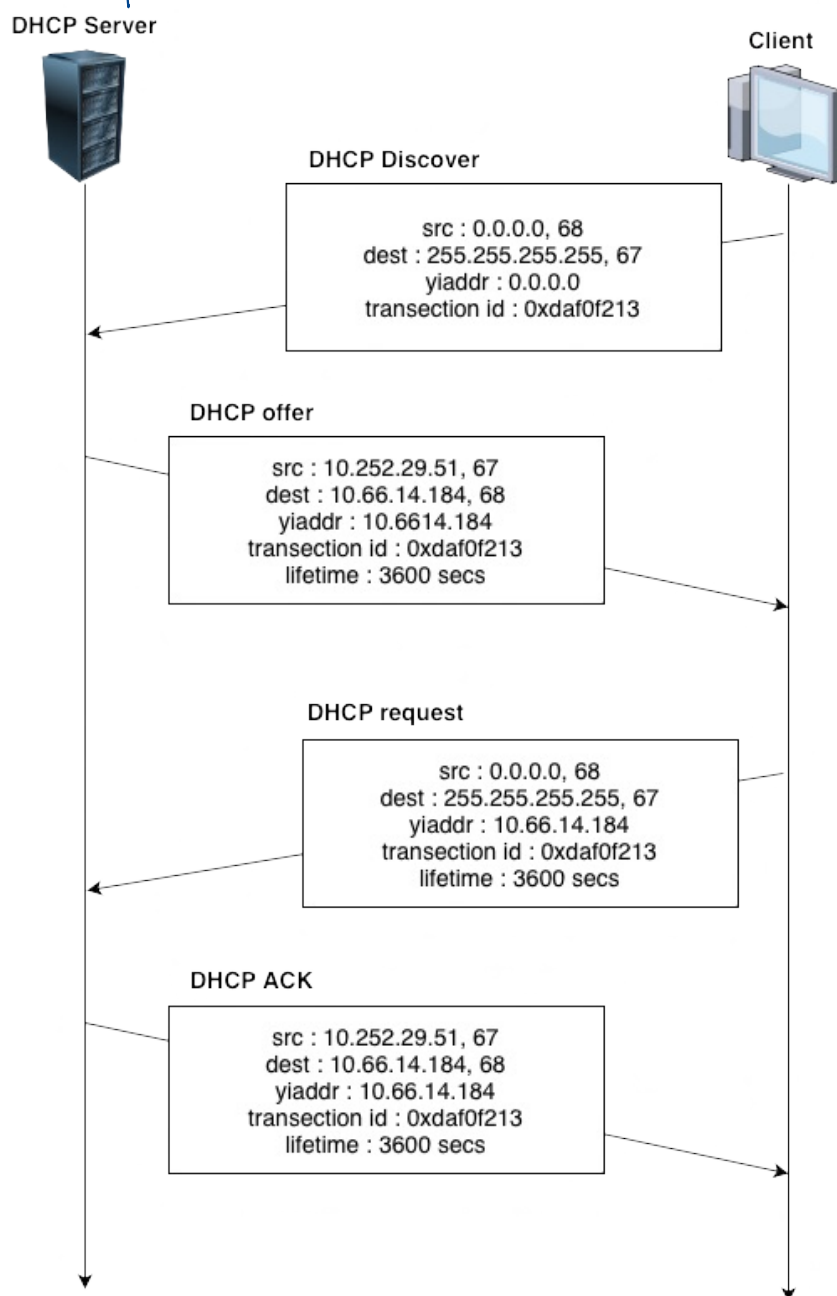
5. ให้ตอบคำถามต่อไปนี้

- DHCP message ส่งผ่าน UDP หรือ TCP

UDP

- ให้อ่าน timing diagram ที่แสดงลำดับการทำงานของ packet ทั้ง 4 คือ Discover, Offer, Request และ ACK ที่ได้ตอบระหว่าง DHCP client และ DHCP server จงสังเกตว่า packet เหล่านี้ใช้พอร์ตหมายเลขเดียวกันหรือไม่ อย่างไร

packet ที่ใช้พอร์ตเดียวกันคือ packet ที่ถูกส่งออกมาจากเครื่องเดียวกัน  
กล่าวคือ packet ที่มาจาก server ก็จะมีพอร์ตเดียวกันทั้งหมด  
packet ที่มาจาก client ก็จะมีพอร์ตเดียวกันทั้งหมด



- หมายเลข Ethernet Address ของเครื่อง client (เครื่องของผู้เรียน)

14:eb:bb:68:c7:6f

- ค่าใดใน DHCP Discover ที่ต่างไปจาก DHCP Request

ค่า yiaddr

- ใน packet ชุดแรก 4 packet (Discover/Offer/Request/ACK) packet ใดมีค่าของ Transaction-ID เหมือนกันและต่างกันบ้าง และหากเปรียบเทียบกับ ค่าของ Transaction-ID ใน packet อีก 4 packet ในชุดที่ 2 พบว่าเหมือนหรือแตกต่างกันอย่างไร และประโยชน์ของ Transaction-ID คืออะไร

Transaction ID ในชุดแรกเป็นเลขเดียวกัน แต่แตกต่างกันชุดที่ 2 เพราะ Transaction ID มีค่าใช้สำหรับระบุคู่ความสัมพันธ์

- เนื่องจาก DHCP client จะใช้งาน IP Address ที่ร้องขอได้ก็ต่อเมื่อกระบวนการทั้ง 4 ขั้นตอนเสร็จสิ้นสมบูรณ์ ในระหว่างที่กระบวนการยังไม่สิ้นสุด ค่า source IP และ destination IP ใน IP header คือค่าใดในแต่ละ message ของ Discover/Offer/Request/ACK

Discover = src : 0.0.0.0 dest : 255.255.255.255

Offer = src : 10.252.29.51 dest : 10.66.14.184

Request = src : 0.0.0.0 dest : 255.255.255.255

ACK = src : 10.252.29.51 dest : 10.66.14.184

- IP Address ของ DHCP Server คือค่าใด (ให้บันทึกภาพ screenshot ประกอบด้วย)

10.252.29.51

No.	Time	TCP Delta	Source	Destination	Protocol	DNS Delta	Host	Length	HTTP	Info
1	0.000000		10.66.14.184	10.252.29.51	DHCP			342		DHCP Release - Transaction ID 0x3f2c87e
2	7.847593		0.0.0.0	255.255.255.255	DHCP			344		DHCP Discover - Transaction ID 0xdaf0f213
3	2.017622		10.252.29.51	10.66.14.184	DHCP			342		DHCP Offer - Transaction ID 0xdaf0f213
4	0.001104		0.0.0.0	255.255.255.255	DHCP			370		DHCP Request - Transaction ID 0xdaf0f213
5	0.021855		10.252.29.51	10.66.14.184	DHCP			342		DHCP ACK - Transaction ID 0xdaf0f213
6	231.77		10.66.14.184	10.252.29.51	DHCP			342		DHCP Release - Transaction ID 0xd0381fa0

- > Option: (53) DHCP Message Type (Offer)
- > Option: (54) DHCP Server Identifier (10.252.29.51)
- > Option: (51) IP Address Lease Time

- ข้อมูลใดใน DHCP Offer message ที่บอกถึง IP Address ที่จะให้เครื่องคอมพิวเตอร์ใช้งาน (ให้บันทึกภาพ screenshot ประกอบด้วย)

your (client) IP address

```

Dynamic Host Configuration Protocol (Offer)
  Message type: Boot Reply (2)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xdaf0f213
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.66.14.184
    Next server IP address: 0.0.0.0
    Relay agent IP address: 10.66.0.1
    Client MAC address: TP-Link_68:e7:6f (14:eb:b6:68:e7:6f)
    Client hardware address padding: 00000000000000000000
  
```

- ให้ตรวจสอบว่า DHCP message ส่งผ่าน Relay Agent หรือไม่ (Relay Agent คือหมายเลขของ router ที่ส่งต่อ DHCP ไปยัง subnet อื่น) ถ้ามีเป็นหมายเลขใด (ให้บันทึกภาพ screenshot ประกอบด้วย)

ให้ หมายเลข 10.66.0.1

```

> Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 10.66.14.184
  Next server IP address: 0.0.0.0
  Relay agent IP address: 10.66.0.1
  Client MAC address: TP-Link_68:e7:6f (14:eb:b6:68:e7:6f)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  
```

- DHCP Server ให้ option ของ subnet mask และ router มาด้วยหรือไม่ และให้คำดังกล่าวเพื่ออะไร  
ให้ เพื่อที่จะได้รู้ว่า เราต่อกับ router เบอร์อะไร และ subnet อะไร เพื่อเวลาที่คุยกับใครก็จะได้ว่า  
เครื่องนั้นอยู่ใน subnet เดียวกันไหม ถ้า subnet เดียวกันสามารถคุยกันได้ แต่ถ้าอยู่คนละ subnet จะต้องคุยผ่าน router

- อธิบายประโยชน์ของ lease time และเครื่อง client (เครื่องผู้เรียน) ได้รับ lease time เท่ากับเท่าไร  
ประโยชน์ของ lease time คือทำให้เวลาที่หมดเวลาของ Client ที่ได้ IP นั้นๆ แล้วไม่มีการต่อเวลา Server  
ก็จะสามารถแจก IP เบอร์นั้นให้ client อื่นได้อีก  
เครื่อง client ของเรา lease time = 3600 วินาที

- อธิบายประโยชน์ของ DHCP release และ DHCP Server มีการตอบโต้กับ DHCP release อย่างไร  
เป็นการทำให้ DHCP server รู้ว่า client ไม่ได้อาศัย IP นั้นแล้ว Server เลขสามารถปล่อย IP นั้น  
ได้เลขเลขๆ ยังไม่ถึง lease time  
DHCP server มีการตอบโต้กับ DHCP release โดยการให้ yiaddr เป็น 0.0.0.0

## ส่วนที่ 2 NAT

NAT (Network Address Translation) เป็นบริการหนึ่งที่นิยมใช้งานในเครือข่ายตามบ้านและเครือข่ายองค์กร เนื่องจากสามารถใช้งานร่วมกับ Private IP ในกรณีที่องค์กรที่ได้รับ Public IP Address มาจำนวนไม่เพียงพอกับจำนวน Host แต่ต้องการให้ Host ในองค์กรสามารถติดต่อกับ Host ที่อยู่ภายนอกองค์กรได้

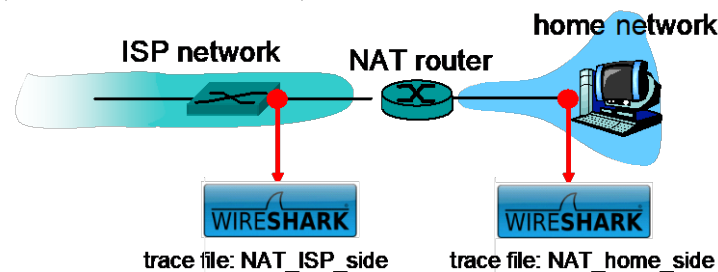


Figure 1: NAT trace collection scenario

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 Address = 192.168.1.100      TCP source port = 4995

Destination IP Address = 64.233.169.104      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 Address = 64.233.169.104      TCP source port = 80

destination IP Address = 192.168.1.100      TCP 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 Address = 71.192.34.104      TCP source port = 4335

destination IP Address = 64.233.169.104      TCP destination port = 80

ข้อมูลที่เปลี่ยนคือ source IP Address

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

Checksum มีการเปลี่ยนแปลง เพราะ source IP Address เปลี่ยน

- 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 Address = 64.233.169.104      TCP source IP Address = 80

destination IP Address = 71.192.34.104      TCP source IP Address = 4335

ข้อมูลที่เปลี่ยนแปลงคือ destination IP Address

8. ให้เขียน NAT Translation Table โดยใช้ข้อมูลจากข้อ 6 และ 7

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

งานครั้งที่ 10

- การส่งงาน เขียนหรือพิมพ์ลงในเอกสารนี้ และส่งเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา ตามด้วย section และ \_lab10 ตามตัวอย่างต่อไปนี้  
64019999\_sec20\_lab10.pdf
- กำหนดส่ง ภายในวันที่ 7 เมษายน 2566 โดยให้ส่งใน Microsoft Teams ของรายวิชา