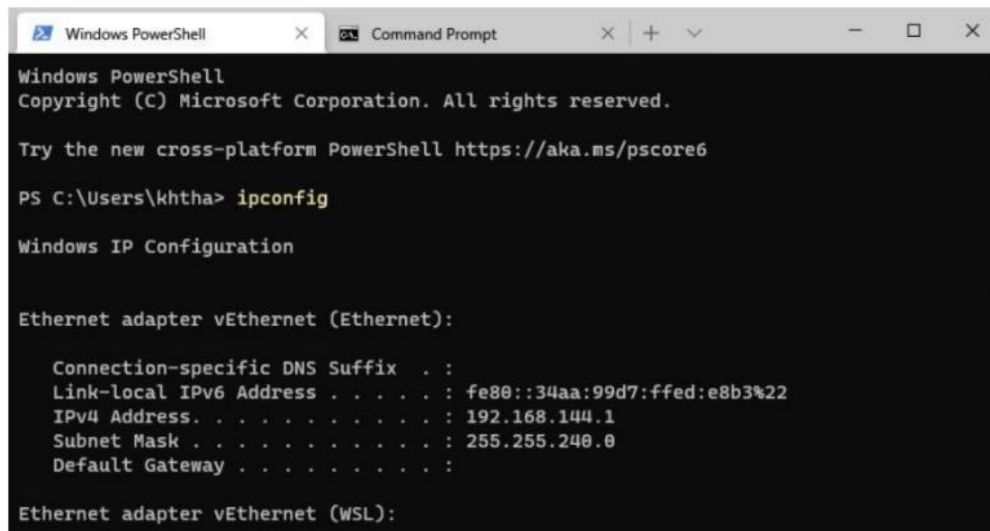


Lab#10 : 62010694

นายภากรณ์ ธนประชานนท์

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

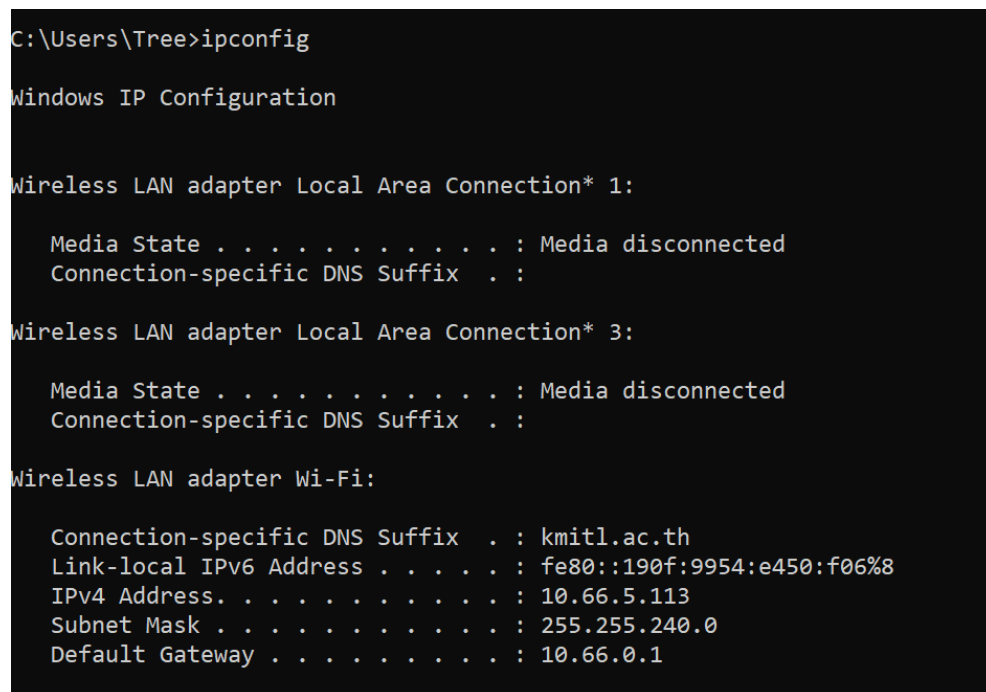
PS C:\Users\khtha> ipconfig

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):
```



```
C:\Users\Tree>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : kmitl.ac.th
    Link-local IPv6 Address . . . . . : fe80::190f:9954:e450:f06%8
    IPv4 Address. . . . . : 10.66.5.113
    Subnet Mask . . . . . : 255.255.240.0
    Default Gateway . . . . . : 10.66.0.1
```

10.66.5.113

2. จากนั้นให้ใช้คำสั่ง `ipconfig /release` เพื่อยกเลิกการใช้งาน IP Address

```
C:\Users\Tree>ipconfig /release

Windows IP Configuration

No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 3 while it has its media disconnected.

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::190f:9954:e450:f06%8
    Default Gateway . . . . . :
```

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

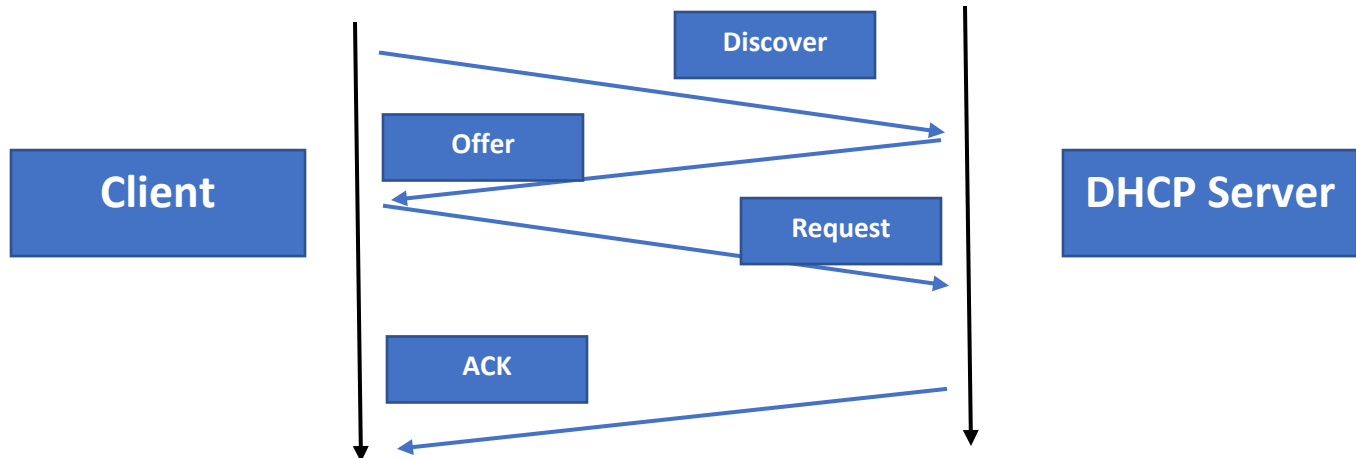
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.66.5.113	10.252.29.51	DHCP	342	DHCP Release - Transaction ID 0xb8857022
2	9.469613	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xb070b142
3	11.479885	10.252.29.51	10.66.5.113	DHCP	342	DHCP Offer - Transaction ID 0xb070b142
4	11.480797	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xb070b142
5	11.493812	10.252.29.51	10.66.5.113	DHCP	342	DHCP ACK - Transaction ID 0xb070b142
6	25.624781	10.66.5.113	10.252.29.51	DHCP	342	DHCP Release - Transaction ID 0x78f938b5
7	29.586529	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x99fe3512
8	29.595470	10.252.29.51	10.66.5.113	DHCP	342	DHCP Offer - Transaction ID 0x99fe3512
9	29.596415	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x99fe3512
10	29.613882	10.252.29.51	10.66.5.113	DHCP	342	DHCP ACK - Transaction ID 0x99fe3512

5. ให้ตอบคำถามต่อไปนี้

- DHCP message ส่งผ่าน UDP หรือ TCP

UDP

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



คนละ **Port** , **Port 67** สำหรับฝั่ง **server** , **Port 68** สำหรับฝั่ง **client**

- หมายเลข Ethernet Address ของเครื่อง client (เครื่องของนักศึกษา)

10.66.5.113

- ค่าใดใน DHCP Discover ที่ต่างไปจาก DHCP Request

DHCP Message Type , DHCP Server Identifier เพิ่มมาใน **Request**

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

แตกต่างกัน ประโยชน์คือช่วยให้ **DHCP-Server** ทราบว่ากำลังติดต่อกับเครื่องใดอยู่เพื่อให้ **IP** ได้ถูก

- เนื่องจาก IP Address จริงจะใช้ได้เมื่อกระบวนการ DHCP ทั้ง 4 ขั้นตอนเสร็จสิ้นสมบูรณ์ ในระหว่างที่กระบวนการยังไม่สิ้นสุด ค่าที่ใช้ใน IP datagram คือ ค่าใดในแต่ละ message ของ

Discover/Offer/Request/ACK

0.0.0.0	255.255.255.255	DHCP	344 DHCP Discover	- Transaction ID 0xb070b142
10.252.29.51	10.66.5.113	DHCP	342 DHCP Offer	- Transaction ID 0xb070b142
0.0.0.0	255.255.255.255	DHCP	370 DHCP Request	- Transaction ID 0xb070b142
10.252.29.51	10.66.5.113	DHCP	342 DHCP ACK	- Transaction ID 0xb070b142

- IP Address ของ DHCP Server คือค่าใด (capture รูปประกอบด้วย)

10.252.29.51

10.252.29.51	10.66.5.113	DHCP	342 DHCP Offer	- Transaction ID 0xb070b142
--------------	-------------	------	----------------	-----------------------------

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

Your (client) IP address

Client IP address: 0.0.0.0

Your (client) IP address: 10.66.5.113

Next server IP address: 0.0.0.0

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

ผ่าน หมายเลขเป็น 10.66.0.1

Next server IP address: 0.0.0.0

Relay agent IP address: 10.66.0.1

Client MAC address: Microsoft 60:00:00:00:00:00 (28:16:38:60:00:63)

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

ให้มาด้วยเพื่อ **Client** จะได้ทราบถึง **Network ID** และ **Host ID**

✓ Option: (1) Subnet Mask (255.255.240.0)

Length: 4

Subnet Mask: 255.255.240.0

✓ Option: (3) Router

Length: 4

Router: 10.66.0.1

- อธิบายประโยชน์ของ lease time และเครื่องคอมพิวเตอร์ได้รับ lease time เท่ากับเท่าไร

เพื่อป้องกันไม่ให้ **IP Pool** เต็มซึ่งจะทำให้เครื่องที่รอขอใช้งานไม่ได้รับ และ
เครื่องคอมพิวเตอร์ได้รับ **lease time 1 ชม.**

✓ Option: (51) IP Address Lease Time

Length: 4

IP Address Lease Time: (3600s) 1 hour

- อธิบายประโยชน์ของ DHCP release และ DHCP Server มีการตอบโต้กับ DHCP release อย่างไร

DHCP release จะทำให้ **DHCP Server** ยกเลิก **IP** ของ
Client บน **DHCP Server** ทันทีโดยไม่สนว่า **lease time** จะหมดหรือ
ยัง

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

Source

192.168.1.100

192.168.1.100

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

[Header checksum status: Unverified]

Source Address: 192.168.1.100

Destination Address: 64.233.169.104

- Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
Source Port: 4335
Destination Port: 80

192.168.1.100 , 64.233.169.104 , 4335 , 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

[Header checksum status: Unverified]

Source Address: 64.233.169.104

Destination Address: 192.168.1.100

- Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760
Source Port: 80
Destination Port: 4335

64.233.169.104 , 192.168.1.100 , 80 , 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

[Header checksum status: Unverified]

Source Address: 71.192.34.104

Destination Address: 64.233.169.104

Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635

Source Port: 4335

Destination Port: 80

[Stream index: 2]

71.192.34.104 , 64.233.169.104 , 4335 , 80

Source IP Address เปลี่ยนไป

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

Checksum: 0xae3 [unverified]

Checksum: 0x386d [unverified]

Checksum ต่างกัน เพราะ IP ใน Package เปลี่ยนแปลง

- 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 Address: 64.233.169.104

Destination Address: 71.192.34.104

Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760

Source Port: 80

Destination Port: 4335

64.233.169.104 , 71.192.34.104 , 80 , 4335

Destination IP Address เปลี่ยนไป

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