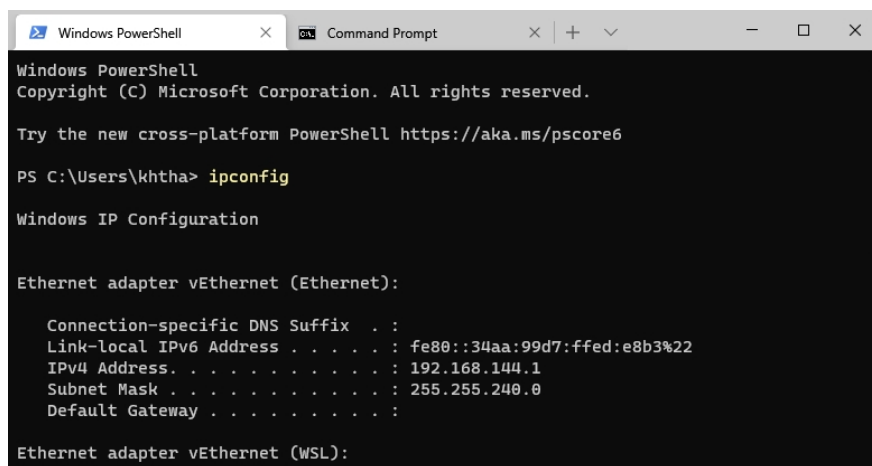


กิจกรรมที่ 10 : DHCP และ NAT

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 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 (ให้ผู้เรียนทำ release และ renew อย่างน้อย 2 ครั้ง) เมื่อพอใจแล้วให้หยุด capture

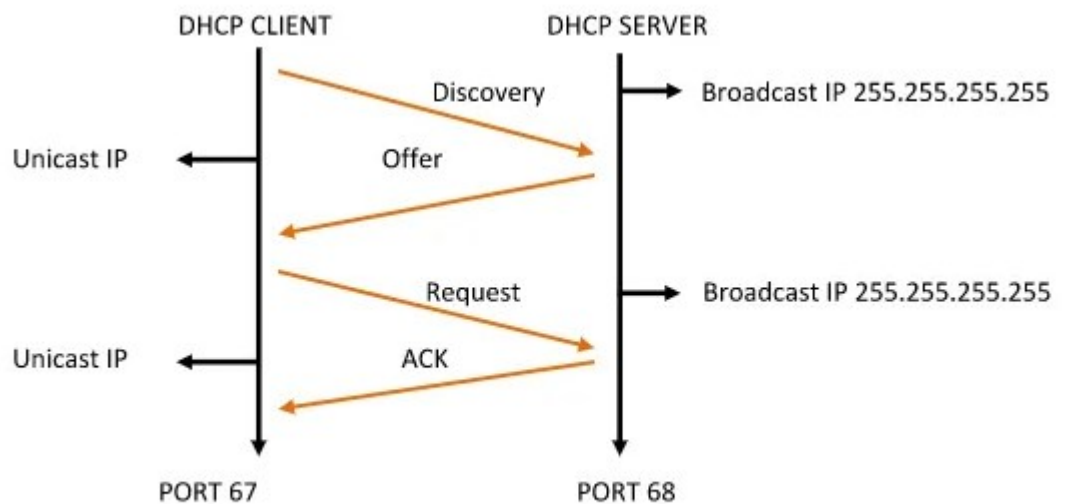
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000...	0.0.0.0	255.255.255.2...	DHCP	342	DHCP Discover - Transaction ID 0x419d79a
2	2.072...	192.168.1.1	192.168.1.4	DHCP	590	DHCP Offer - Transaction ID 0x419d79a
3	2.073...	0.0.0.0	255.255.255.2...	DHCP	356	DHCP Request - Transaction ID 0x419d79a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



- หมายเลข Ethernet Address ของเครื่อง client (เครื่องของผู้เรียน)

คำตอบที่ได้แตกต่างกันไปตามเครื่องของผู้เรียน

- ค่าใดใน DHCP Discover ที่ต่างไปจาก DHCP Request

DHCP Request มี DHCP Server Identifier (4 ไบต์) Client Fully Qualified Domain Name (11 ไบต์) (อาจมีความยาวแตกต่างกันได้)

<pre> Boot file name not given Magic cookie: DHCP > Option: (53) DHCP Message Type (Discover) > Option: (61) Client identifier > Option: (50) Requested IP Address (192.168.1.4) > Option: (12) Host Name > Option: (60) Vendor class identifier > Option: (55) Parameter Request List > Option: (255) End Padding: 0000000000 </pre>	<pre> > Option: (53) DHCP Message Type (Request) > Option: (61) Client identifier > Option: (50) Requested IP Address (192.168.1.4) > Option: (54) DHCP Server Identifier (192.168.1.1) > Option: (12) Host Name > Option: (81) Client Fully Qualified Domain Name > Option: (60) Vendor class identifier > Option: (55) Parameter Request List > Option: (255) End Option End: 255 </pre>
--	---

- 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

4 packet ชุดแรกมีค่า Transaction ID เหมือนกันทั้ง 4 packet

4 packet ชุดที่สองมีค่า Transaction ID เหมือนกันทั้ง 4 packet แต่มีค่าต่างจากชุดแรก

ประโยชน์ของ Transaction ID ใช้บ่งบอกว่าเป็น Discover/Offer/Request/ACK ชุดเดียวกัน เพื่อให้ผู้ที่ Discover และ Request ทราบว่าการตอบ Broadcast กลับมานั้นส่งกลับให้ตน

- 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

ในส่วนของ Client จะใช้ Source IP เป็น 0.0.0.0 และ 255.255.255.255 เป็น Destination IP แต่ Server จะใช้ IP จริง

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

IP Address แตกต่างกันไปตามแต่ละเครือข่ายที่เชื่อมต่อ

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

Your (client) IP address: 192.168.1.4

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

สามารถดูได้จาก Relay Agent IP Address ถ้าเป็น 0 แสดงว่าไม่ได้ส่งผ่าน แต่ถ้ามีค่าหมายเลข IP แปลว่าส่งผ่าน Relay Agent

Relay agent IP address: 0.0.0.0

- DHCP Server ให้ option ของ subnet mask และ router มาด้วยหรือไม่ และให้คำดังกล่าวเพื่ออะไร ให้มาด้วย เพื่อให้ใช้เป็น subnet mask และ default gateway ของเครื่อง ในการติดต่อกับ host อื่นๆ สามารถนำ subnet mask ไปใช้แยกแยะได้ว่า host ที่ต้องการติดต่อด้านนั้นอยู่ใน subnet เดียวกันหรือไม่ และถ้าอยู่คนละ subnet จะได้ว่าต้องส่งให้กับ router ที่หมายเลขใด
- อธิบายประโยชน์ของ lease time และเครื่อง client (เครื่องผู้เรียน) ได้รับ lease time เท่ากับเท่าไร เพื่อไม่ให้ IP Address Pool ของ DHCP ถูกขอไปใช้งานจนหมด จึงมีกำหนดเวลาใช้งาน หากเครื่องนั้นไม่ได้อยู่แล้ว ก็สามารถนำ IP Address ไปให้คอมพิวเตอร์เครื่องอื่นได้อีก
- อธิบายประโยชน์ของ DHCP release และ DHCP Server มีการตอบโต้กับ DHCP release อย่างไร เพื่อคืนหมายเลข IP Address ให้กับ DHCP Server โดย DHCP Server ไม่มีการโต้ตอบ

ส่วนที่ 2 NAT

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

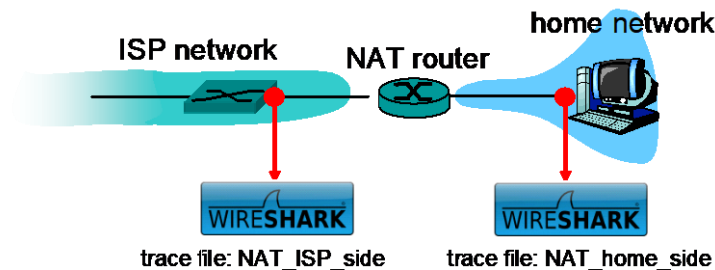


Figure 1: NAT trace collection scenario

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 = 192.168.1.100, Destination IP = 64.233.169.104, Source Port = 4335,
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 = 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
Source IP = 71.192.34.104, Destination IP = 64.233.169.104, Source Port = 4335, Destination Port = 80
- ในฟิลด์ข้อมูล Version, Header Length, Flags, Checksum มีข้อมูลใดเปลี่ยนแปลงไปหรือไม่ ให้อธิบายเหตุผลที่มีการเปลี่ยนแปลง
Version เหมือนเดิม Length เท่าเดิม Flags เหมือนเดิม แต่ส่วนที่ต่างกันคือ Checksum เนื่องจาก IP datagram ถูกเปลี่ยน Client IP ด้วย NAT โดย IP ในส่วนของ ISP คือ 71.192.34.104:4335 แต่ส่วนของ home คือ 192.168.1.100:4335 ดังนั้นจึงมีการคำนวณส่วน Checksum ใหม่ ทำให้ Checksum มีการเปลี่ยนแปลง
- 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, 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
71.192.34.104	4335	192.168.1.100	4335