ชื่อ นาย รวีโรจน์ ทองดี **รหัสนักศึกษา** 62010763

กิจกรรมที่ 10 : DHCP และ NAT

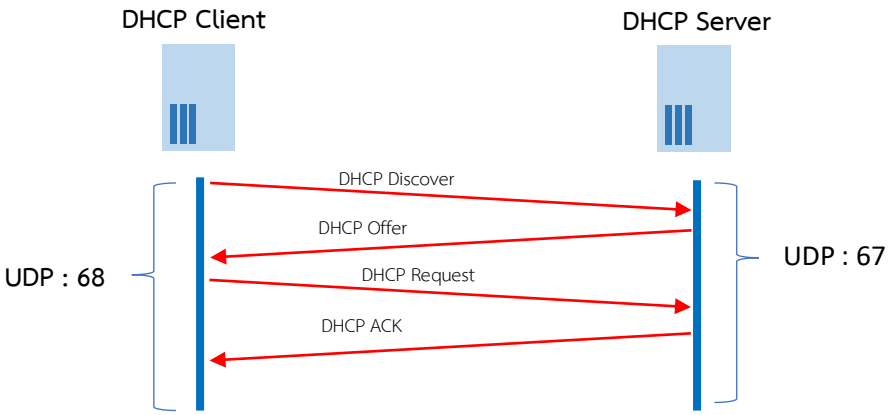
ให้ตอบคำถามต่อไปนี้

Q(5.1) : DHCP message ส่งผ่าน UDP หรือ TCP

A(5.1) : ส่งผ่าน UDP

Q(5.2) : ให้วาด timing diagram ที่แสดงลำดับการทำงานของ packet ทั้ง 4 คือ Discover, Offer, Request และ ACK ที่โต้ตอบระหว่าง client และ server ใช้พอร์ตหมายเลขเดียวกันหรือไม่ อย่างไร

A(5.2) : ใช้คนละ port กัน Client ใช้ port 68 ส่วน Server จะใช้ 67



Q(5.3) : หมายเลข Ethernet Address ของเครื่อง client (เครื่องของนักศึกษา)

A(5.3) : 30-9C-23-FF-54-07

Q(5.4) : ค่าใดใน DHCP Discover ที่ต่างไปจาก DHCP Request

A(5.4) : Option 54 (DHCP Server Identifier) และ Option 81 (Client Fully Qualified Domain Name)

DHCP Discover packet

```
Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x2ee9e127
    Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Micro-St_ff:54:07 (30:9c:23:ff:54:07)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address (10.10.0.254)
  > Option: (12) Host Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
```

DHCP Request packet

```
Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x2ee9e127
    Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Micro-St_ff:54:07 (30:9c:23:ff:54:07)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Request)
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address (10.10.0.254)
  > Option: (54) DHCP Server Identifier (10.10.0.1)
  > Option: (12) Host Name
  > Option: (81) Client Fully Qualified Domain Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
```

ชื่อ นาย รวีโรจน์ ทองดี **รหัสนักศึกษา** 62010763

Q(5.5) : ค่าของ Transaction-ID ในชุดข้อมูลแรก (Discover/Offer/Request/ACK) และในชุดข้อมูลที่ 2 เหมือนหรือแตกต่างกันอย่างไร และประโยชน์ของ Transaction-ID คืออะไร

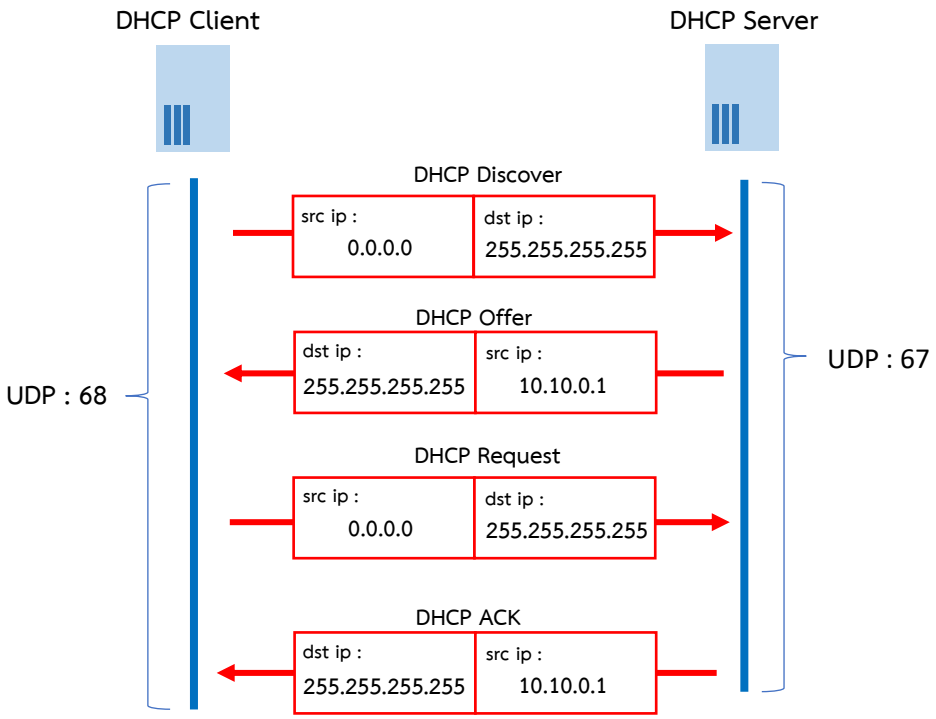
A(5.5) : ค่า Transaction-ID มีค่าที่แตกต่างกันในแต่ละชุดข้อมูล มีไว้เพื่อแยกรอบการทำงานเวลา Client ร้องขอ ip ใหม่

dhcp.hw.mac_addr == 30-9C-23-FF-54-07

No.	Time	Source	Destination	Protocol	Length	DNS Delta	Info
23	0.922258	10.10.0.254	10.10.0.1	DHCP	342		DHCP Release - Transaction ID 0xdea0e3c4
58	0.591646	0.0.0.0	255.255.255.255	DHCP	344		DHCP Discover - Transaction ID 0xea00b7c
61	0.110825	10.10.0.1	255.255.255.255	DHCP	342		DHCP Offer - Transaction ID 0xea00b7c
62	0.000573	0.0.0.0	255.255.255.255	DHCP	370		DHCP Request - Transaction ID 0xea00b7c
63	0.001551	10.10.0.1	255.255.255.255	DHCP	342		DHCP ACK - Transaction ID 0xea00b7c
84	0.171816	10.10.0.254	10.10.0.1	DHCP	342		DHCP Release - Transaction ID 0x8577cdc7
95	0.114428	0.0.0.0	255.255.255.255	DHCP	344		DHCP Discover - Transaction ID 0x21981e36
96	0.522420	10.10.0.1	255.255.255.255	DHCP	342		DHCP Offer - Transaction ID 0x21981e36
97	0.000690	0.0.0.0	255.255.255.255	DHCP	370		DHCP Request - Transaction ID 0x21981e36
98	0.001123	10.10.0.1	255.255.255.255	DHCP	342		DHCP ACK - Transaction ID 0x21981e36

Q(5.6) : เนื่องจาก IP Address จริงจะใช้ได้เมื่อกระบวนการ DHCP ทั้ง 4 ขั้นตอนเสร็จสิ้นสมบูรณ์ ในระหว่างที่กระบวนการยังไม่สิ้นสุด ค่าที่ใช้ใน IP datagram คือ ค่าใดในแต่ละ message ของ Discover/Offer/Request/ACK

A(5.6) :



Q(5.7) : IP Address ของ DHCP Server คือค่าใด (capture รูปประกอบด้วย)

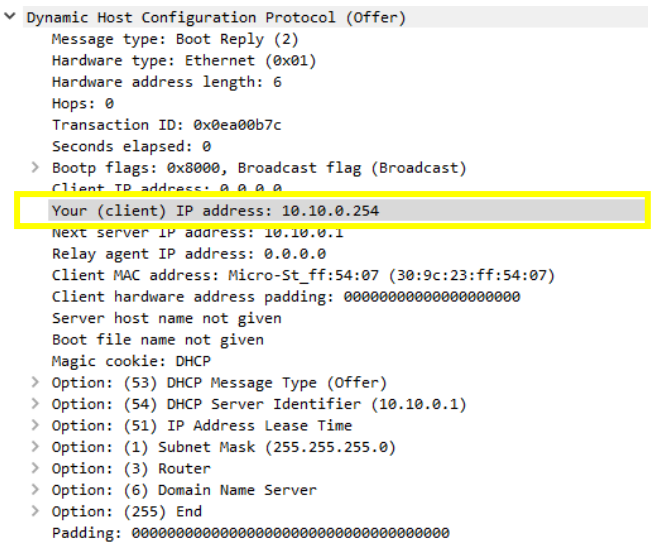
A(5.7) : 10.10.0.1

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Killer E2400 Gigabit Ethernet Controller
   Physical Address. . . . . . . . . : 30-9C-23-FF-54-07
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::513:6fb8:99cb:891e%5(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.0.254(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, March 28, 2021 6:04:42 PM
   Lease Expires . . . . . . . . . . : Monday, March 29, 2021 2:14:42 PM
   Default Gateway . . . . . . . . . : 10.10.0.1
   DHCP Server . . . . . . . . . . . : 10.10.0.1
   DHCPv6 IAID . . . . . . . . . . . : 204512291
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-31-7E-26-30-9C-23-FF-54-07
   DNS Servers . . . . . . . . . . . : 10.10.0.1
                                       8.8.8.8
                                       8.8.4.4
```

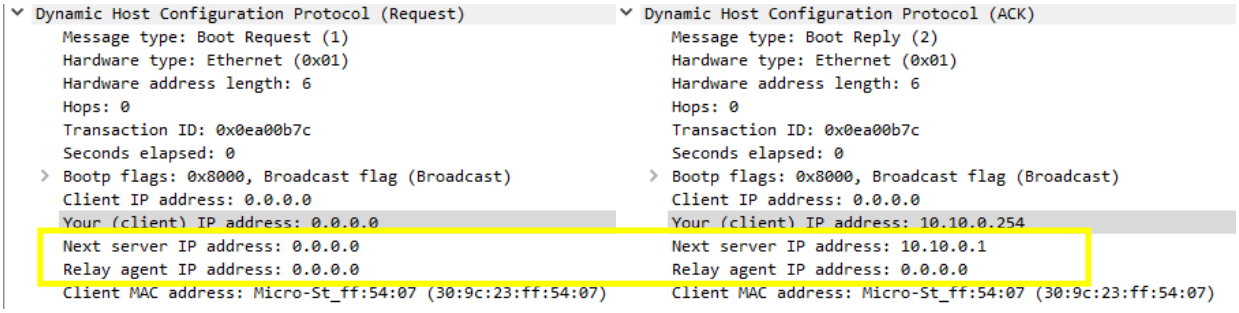
Q(5.8) : ใน DHCP Offer message ข้อมูลใด ที่บอกถึง IP Address ที่จะให้เครื่องคอมพิวเตอร์ใช้งาน (capture รูปประกอบด้วย)

A(5.8) : ค่า Your (client) IP Address : 10.10.0.254



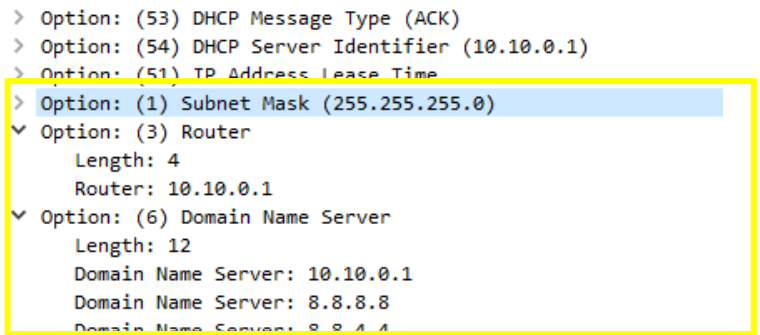
Q(5.9) : ให้ตรวจสอบว่า message DHCP ผ่าน Relay Agent หรือไม่ (Relay Agent คือหมายเลขของ router ที่ส่งต่อ DHCP ไปยัง subnet อื่น) ถ้ามีเป็นหมายเลขใด (capture รูปประกอบด้วย)

A(5.9) : message DHCP ไม่ผ่าน Relay Agent เนื่องจากผู้ทดลองใช้งาน DHCP service ที่อยู่บนตัว Router ของผู้ใช้งานโดยตรง ในส่วนของ Relay agent IP Address จึงเป็น 0.0.0.0



Q(5.10) : DHCP Server ให้ option ของ subnet mask และ router มาด้วยหรือไม่ มีเป้าหมายเพื่ออะไร

A(5.9) : ให้มาใน DHCP ACK message มีเป้าหมายเพื่อให้ client ใช้งานทรัพยากรบนเครือข่าย หรือ เชื่อมต่อกับเครือข่ายอื่นได้



ชื่อ นาย รวีโรจน์ ทองดี **รหัสนักศึกษา** 62010763

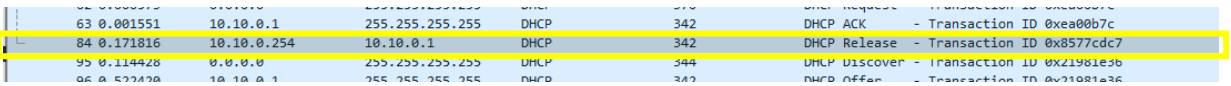
Q(5.11) : อธิบายประโยชน์ของ lease time และเครื่องคอมพิวเตอร์ได้รับ lease time เท่ากับเท่าไร

A(5.11) : Lease time เป็นเวลาที่บอกว่า client เครื่องนั้นจะยังคงสามารถใช้งาน ip ที่ได้รับจาก DHCP server ได้จนถึงเมื่อไหร่ และหาก Lease time หมดอายุลง Client จำเป็นต้องร้องขอ (Discover) มาใหม่ หากยังต้องการใช้งานเครือข่ายอยู่ โดยในกรณีนี้เครื่องผมมี lease time คือ 20 ชั่วโมง กับอีก 10 นาที โดยประโยชน์ของ lease time คือช่วยลดภาระ DHCP server ในการตรวจสอบ client ในเครือข่ายที่ไม่ได้ใช้งานเครือข่ายแล้ว ip ของ client นั้นก็จะได้ถูกนำเอาไปแจกให้กับ client อื่นต่อไปๆ

```
Option: (51) IP Address Lease Time
   Length: 4
   IP Address Lease Time: (72600s) 20 hours, 10 minutes
```

Q(5.12): อธิบายประโยชน์ของ DHCP release และ DHCP Server มีการตอบโต้กับ DHCP release อย่างไร

A(5.12) : การใช้งาน DHCP release จะถูกใช้งานในฝั่งของ DHCP Client เพื่อเป็นการบอกไปยัง DHCP Server ว่าจะไม่ใช้งาน ip ชุดดังกล่าวแล้ว หรือเป็นการยกเลิกการจอง ip ดังกล่าว โดย DHCP Client จะทำการส่ง DHCP release message ไปยัง DHCP Server ในฝั่งของ DHCP Client เมื่อทำการ release แล้วก็จะไม่มี ip ในการใช้งาน จนกว่าจะ renew เพื่อร้องขอการใช้งาน ip อีกครั้งหนึ่ง โดยประโยชน์ก็คือ DHCP Client สามารถร้องขอ ip ใหม่ได้ตามต้องการ และหากต้องการออกจากเครือข่ายก็สามารถทำได้ทันที




```
Dynamic Host Configuration Protocol (Release)
   Message type: Boot Request (1)
   Hardware type: Ethernet (0x01)
   Hardware address length: 6
   Hops: 0
   Transaction ID: 0x8577cdc7
   Seconds elapsed: 0
   Bootp flags: 0x0000 (Unicast)
   Client IP address: 10.10.0.254
   Your (client) IP address: 0.0.0.0
   Next server IP address: 0.0.0.0
   Relay agent IP address: 0.0.0.0
   Client MAC address: Micro-St_ff:54:07 (30:9c:23:ff:54:07)
   Client hardware address padding: 00000000000000000000
   Server host name not given
   Boot file name not given
   Magic cookie: DHCP
   Option: (53) DHCP Message Type (Release)
   Option: (54) DHCP Server Identifier (10.10.0.1)
   Option: (61) Client identifier
   Option: (255) End
   Padding: 0000000000000000000000000000000000000000000000000000
```

ชื่อ นาย รวีโรจน์ ทองดี **รหัสนักศึกษา** 62010763

ให้เปิดไฟล์ NAT_home_side.pcap และตอบคำถามต่อไปนี้

Q(6.1) : IP Address ของ client เป็นเลขอะไร

A(6.1) : 192.168.1.100

Q(6.2) : 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

A(6.2) :

```
  Source Address: 192.168.1.100
  Destination Address: 64.233.169.104
Transmission Control Protocol, Src Port: 4335, Dst Port: 80,
  Source Port: 4335
  Destination Port: 80
```

Q(6.3) : 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

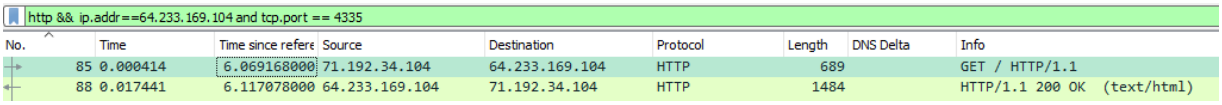
A(6.3) :

```
  Source Address: 64.233.169.104
  Destination Address: 192.168.1.100
Transmission Control Protocol, Src Port: 80, Dst Port: 4335,
  Source Port: 80
  Destination Port: 4335
```

ให้เปิดไฟล์ NAT_ISP_side.pcap และตอบคำถามต่อไปนี้

Q(7.1) :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

A(7.1) : เป็น packet ที่ 85 เวลา 6.069168000 มีขอมูลในส่วนของ Source Address เปลี่ยนไปจาก 192.168.1.100 ถูกเปลี่ยนเป็น 71.192.34.104




```
  Source Address: 71.192.34.104
  Destination Address: 64.233.169.104
ansmission Control Protocol, Src Port: 4335, Dst Port: 80
  Source Port: 4335
  Destination Port: 80
```

Q(7.2) : ในฟิลด์ข้อมูล Version, Header Length, Flags, Checksum มีข้อมูลใดเปลี่ยนแปลงไปหรือไม่ ให้อธิบายเหตุผลที่มีการเปลี่ยนแปลง

A(7.2) : ค่าของฟิลด์ Checksum กับ Time to Live จะเปลี่ยนแปลงไป โดยในส่วนของ Checksum นั้นที่ค่าเปลี่ยนไปเพราะมาจากกระบวนการ NAT มีการเปลี่ยน IP Address ค่า checksum เลยเปลี่ยน ส่วน Time to Live มีการวิ่งผ่าน Router ในที่นี้คือ NAT Router ค่าเลยลดลงจาก 128 -> 127

```
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0xa94a [validation disabled]
[Header checksum status: Unverified]
```

Home Side

```
Time to Live: 127
Protocol: TCP (6)
Header Checksum: 0x022f [validation disabled]
[Header checksum status: Unverified]
```

ISP Side

Q(7.3) : ให้หา packet ที่ตรงกับ 200 OK ในข้อ 6 ให้บันทึก Source IP Address, Destination IP Address,TCP source port และ TCP destination port ของ packet และบอกว่าข้อมูลใดที่ถูกเปลี่ยนแปลงไป

A(7.3) : เป็น packet ที่ 88 เวลา 6.11707800 มีขอมูลในส่วนของ Destination Address เปลี่ยนไปจาก 192.168.1.100 เปลี่ยนเป็น 71.192.34.104

```
    Source Address: 64.233.169.104
    Destination Address: 71.192.34.104
Transmission Control Protocol, Src Port: 80, Dst Port: 4335
    Source Port: 80
    Destination Port: 4335
```

Q(8) : ให้เขียน NAT Translation Table โดยใช้ข้อมูลจากข้อ 6 และ 7

A(8) :

Public IP Address	Public Port	Private IP Address	Private IP Port
71.192.34.104	4335	192.168.1.100	4335
71.192.34.104	4337	192.168.1.100	4337
71.192.34.104	4338	192.168.1.100	4338