

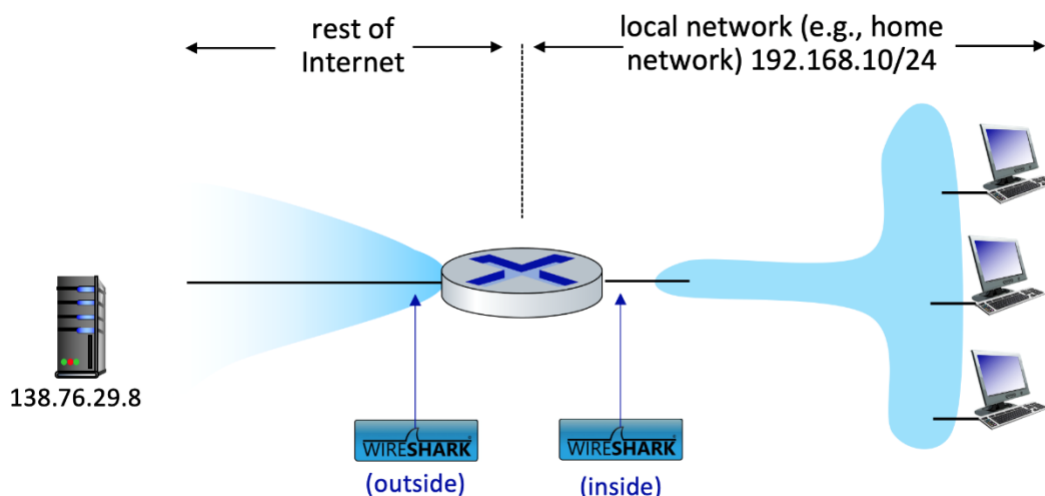
# Lab 09: Network Address Translation

ปฏิบัติการในครั้งนี้เราจะมาสำรวจพฤติกรรมการทำงาน Network Address Translation (NAT) ของ router โดยปฏิบัติการครั้งนี้จะแตกต่างจากครั้งที่ปกติเราจะดักจับ packets จากจุดเดียว เนื่องจากเราสนใจใน packets ที่ดักจับได้จากทั้งสองจุด นั่นคือทั้งด้านที่เป็น input และ output ของอุปกรณ์ NAT ซึ่งการดักจับ packets จากสภาพแวดล้อมจริงไม่สามารถทำได้โดยง่ายนัก ดังนั้นในปฏิบัติการครั้งนี้ผู้เรียนจะได้ศึกษาและวิเคราะห์ข้อมูลจากไฟล์ที่ได้จัดเตรียมไว้ให้

## A. NAT Measurement Scenario

ในปฏิบัติการครั้งนี้ เราได้เตรียมไฟล์ที่ดักจับ packet ซึ่งส่ง HTTP GET message จากเครื่อง client ซึ่งอยู่ใน home network ไปยัง remote server และดักจับ packet ซึ่งเป็น response จาก server นั้น โดยมี router เป็นอุปกรณ์ที่ให้บริการ NAT โดยเราจะดักจับ packets จากสองตำแหน่ง จึงทำให้มีไฟล์ trace อยู่สองไฟล์ ได้แก่

- nat-inside-wireshark-trace1-1.pcapng ซึ่งเป็นไฟล์ที่ดักจับ packets จากฝั่ง local area network (LAN) ของ NAT router โดยอุปกรณ์ใน LAN มี network address เป็น 192.168.10.0/24
- nat-outside-wireshark-trace1-1.pcapng ซึ่งเป็นไฟล์ที่ดักจับ packets จากอีกฝั่งของ router ใกล้กับส่วนที่เชื่อมต่อออกไปยัง Internet ซึ่งเป็นฝั่งด้านซ้ายตาม รูป 1 โดย packets ที่ถูกส่งจาก host ที่อยู่ด้านขวาไปยัง server ที่อยู่ด้านซ้ายจะผ่านการทำ NAT มาแล้วก่อนที่จะมาถึงจุดที่ถูกดักจับ



รูป 1 สถานการณ์ที่ใช้ในการดักจับ NAT packets

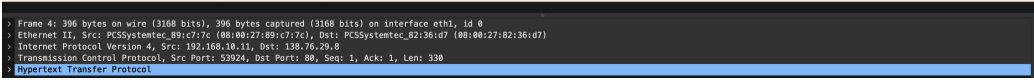
ในสถานการณ์ตามทีแสดงใน รูป 1 มี host หนึ่งจากฝั่ง LAN ส่ง HTTP GET request ไปยัง web server ซึ่งใช้หมายเลข IP เป็น 138.76.29.8 ซึ่ง web server ดังกล่าวได้ส่ง packet ตอบกลับมายัง host ในกรณีนี้เราไม่ได้มุ่งความสนใจไปที่ HTTP GET request นัก แต่เรามุ่งความสนใจไปที่การทำงานของ NAT router ที่เปลี่ยนหมายเลข IP ของ datagram จากฝั่ง LAN (ฝั่งด้านใน) ไปยังหมายเลขในฝั่งที่ใกล้กับการเชื่อมต่อออกสู่ Internet (ฝั่งด้านนอก) ของ NAT router

## Questions (A)

ขั้นแรกให้ผู้เรียนเปิดไฟล์ nat-inside-wireshark-trace1-1.pcapng ซึ่งผู้เรียนจะพบ HTTP GET request ที่ส่งออกไปยัง หมายเลข IP 138.76.29.8 และพบ HTTP response message (“200 OK”) ซึ่ง messages ทั้งสองถูกดักจับจากฝั่ง LAN ของ router ให้ผู้เรียนศึกษา packets ดังกล่าวและตอบคำถามต่อไปนี้

- 1) เครื่อง client ที่ส่ง HTTP GET request ในไฟล์ nat-inside-wireshark-trace1-1.pcapng ใช้หมายเลข IP address หมายเลขใด? TCP segment ที่นำส่ง HTTP GET request ระบุหมายเลข source port เป็นเลขอะไร? HTTP GET request ถูกส่งไปยังหมายเลข destination IP หมายเลขใด? TCP segment ที่นำส่ง HTTP GET request ระบุหมายเลข destination port เป็นเลขอะไร?

No.	Time	ICMP RTT	Source	Destination	Protocol	Length	Info
1	0.000000000		192.168.10.11	138.76.29.8	TCP	74	53924 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=322727249 TSecr=0 WS=128
2	0.002091700		138.76.29.8	192.168.10.11	TCP	74	80 → 53924 [SYN, ACK] Seq=0 Ack=1 Win=65168 Len=0 MSS=1460 SACK_PERM TSval=882266926 TSecr=322727249 WS=128
3	0.002678917		192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=322727252 TSecr=882266926
4	0.027362245		192.168.10.11	138.76.29.8	HTTP	396	GET / HTTP/1.1
5	0.029390199		138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=1 Ack=331 Win=64896 Len=0 TSval=882266954 TSecr=322727277
6	0.030672181		138.76.29.8	192.168.10.11	HTTP	613	HTTP/1.1 200 OK (text/html)
7	0.031464845		192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TSval=322727281 TSecr=882266955
8	0.231407421		192.168.10.11	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
9	0.232096589		138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TSval=882267157 TSecr=322727481
10	0.233074462		138.76.29.8	192.168.10.11	HTTP	555	HTTP/1.1 404 Not Found (text/html)
11	0.233703166		192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=582 Ack=1837 Win=64128 Len=0 TSval=322727483 TSecr=882267158
12	5.189772327		PCSSystemtec_82:c7...	PCSSystemtec_89:c7...	ARP	42	Who has 192.168.10.11? Tell 192.168.10.254
13	5.191799581		PCSSystemtec_89:c7...	PCSSystemtec_82:c7...	ARP	60	192.168.10.11 is at 08:00:27:82:136:d7
14	5.234545253		138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [FIN, ACK] Seq=1837 Ack=582 Win=64768 Len=0 TSval=882272158 TSecr=322727483
15	5.234789589		192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [FIN, ACK] Seq=582 Ack=1837 Win=64128 Len=0 TSval=322732484 TSecr=882267158
16	5.236143161		192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=583 Ack=1838 Win=64128 Len=0 TSval=322732485 TSecr=882272158
17	5.238048528		138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=1838 Ack=583 Win=64768 Len=0 TSval=882272161 TSecr=322732484
18	5.241721585		PCSSystemtec_89:c7...	PCSSystemtec_82:c7...	ARP	60	Who has 192.168.10.254? Tell 192.168.10.11
19	5.241747598		PCSSystemtec_82:c7...	PCSSystemtec_89:c7...	ARP	42	192.168.10.254 is at 08:00:27:82:136:d7

- a. 
  - b. Ip address 192.168.10.11
  - c. Source Port: 53924
  - d. Ip address 138.76.29.8
  - e. Destination Port: 80
- 2) เมื่อเวลาเท่าไร (สำหรับคำถามเวลานับจากนี้ โปรดระบุเวลานับจากเริ่มต้นไฟล์ trace ไม่ใช่เวลา wall-clock) ที่ HTTP 200 OK message จาก web server ถูกส่งต่อจาก NAT router ไปยังเครื่อง client ซึ่งอยู่ในฝั่ง LAN

# 01076117 Computer Networks in Practice

## Computer Engineering, KMITL

No.	Time	ICMP RTT	Source	Destination	Protocol	Length	Info
1	0.00000000		192.168.10.11	138.76.29.8	TCP	74	53924 → 80 [SYN] Seq=0 Win=64248 Len=0 MSS=1468 SACK_PERM TSval=322727249 TSecr=0 WS=128
2	0.00289780		138.76.29.8	192.168.10.11	TCP	74	80 → 53924 [SYN, ACK] Seq=0 Ack=1 Win=5168 Len=0 MSS=1468 SACK_PERM TSval=322727249 TSecr=0 WS=128
3	0.00289780		192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=322727252 TSecr=882266926
4	0.02736240		192.168.10.11	138.76.29.8	HTTP	396	GET / HTTP/1.1
5	0.02939839		138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=1 Ack=331 Win=64896 Len=0 TSval=882266954 TSecr=322727277
6	0.03067210		138.76.29.8	192.168.10.11	HTTP	515	HTTP/1.1 200 OK (text/html)
7	0.03140481		192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TSval=322727281 TSecr=882266955
8	0.23140742		192.168.10.11	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
9	0.23289589		138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TSval=882267157 TSecr=322727481
10	0.23387032		192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=582 Ack=1837 Win=64128 Len=0 TSval=322727483 TSecr=882267158
11	0.23370316		192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=582 Ack=1837 Win=64128 Len=0 TSval=322727483 TSecr=882267158
12	5.10977237		PCSystemtec_82:36	PCSystemtec_89:c7	ARP	42	Who has 192.168.10.11? Tell 192.168.10.254
13	5.10979040		PCSystemtec_89:c7	PCSystemtec_82:36	ARP	42	192.168.10.11 is at 80:80:27:80:c7:c7
14	5.23454523		138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [FIN, ACK] Seq=587 Ack=582 Win=64768 Len=0 TSval=882272158 TSecr=322727483
15	5.23470959		192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [FIN, ACK] Seq=582 Ack=1837 Win=64128 Len=0 TSval=322727484 TSecr=882267158
16	5.23614316		192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=583 Ack=1838 Win=64128 Len=0 TSval=322727485 TSecr=882272158
17	5.23840528		138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=1838 Ack=583 Win=64768 Len=0 TSval=882272161 TSecr=322727484
18	5.24171585		PCSystemtec_89:c7	PCSystemtec_82:36	ARP	68	Who has 192.168.10.254? Tell 192.168.10.11
19	5.24174798		PCSystemtec_82:36	PCSystemtec_89:c7	ARP	42	192.168.10.254 is at 80:80:27:80:36:c7

```

Window size scaling factor: 128
Checksum: 8x258 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
- [Timestamps]
  Time since first frame in this TCP stream: 0.03067210 seconds
  Time since previous frame in this TCP stream: 0.00120182 seconds
- [SEQ/ACK analysis]
  TCP payload (547 bytes)
[Sequence Number: 547]
[HTTP/1.1 200 OK (text/html)]
Date: Mon, 29 Mar 2022 03:10:27 GMT\r\n
Server: Apache/2.4.41 (Ubuntu)\r\n
Last-Modified: Tue, 12 Jan 2021 18:55:04 GMT\r\n
ETag: "337-50b8f8a72e-gzip\r\n
Accept-Ranges: bytes\r\n
Vary: Accept-Encoding\r\n
Content-Encoding: gzip\r\n
Content-Length: 218\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.00130806 seconds]
[Response in frame: 4]
[Next request in frame: 8]
[Next response in frame: 16]
Request URI: http://138.76.29.8/
Content-encoded entity body (gzip): 218 bytes → 311 bytes
File data: 311 bytes
[Line-based text data: text/html (12 lines)]

```

- 
- 0.030672101 Time

3) หมายเลข source IP และ destination IP และหมายเลข TCP source port และ destination port ของ IP datagram ที่นำส่ง HTTP 200 OK message มีค่าเป็นเท่าใดบ้าง?

No.	Time	ICMP RTT	Source	Destination	Protocol	Length	Info
1	0.00000000		192.168.10.11	138.76.29.8	TCP	74	53924 → 80 [SYN] Seq=0 Win=64248 Len=0 MSS=1468 SACK_PERM TSval=322727249 TSecr=0 WS=128
2	0.00289780		138.76.29.8	192.168.10.11	TCP	74	80 → 53924 [SYN, ACK] Seq=0 Ack=1 Win=5168 Len=0 MSS=1468 SACK_PERM TSval=322727249 TSecr=0 WS=128
3	0.00289780		192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=322727252 TSecr=882266926
4	0.02736240		192.168.10.11	138.76.29.8	HTTP	396	GET / HTTP/1.1
5	0.02939839		138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=1 Ack=331 Win=64896 Len=0 TSval=882266954 TSecr=322727277
6	0.03067210		138.76.29.8	192.168.10.11	HTTP	515	HTTP/1.1 200 OK (text/html)
7	0.03140481		192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TSval=322727281 TSecr=882266955
8	0.23140742		192.168.10.11	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
9	0.23289589		138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TSval=882267157 TSecr=322727481
10	0.23387032		192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=582 Ack=1837 Win=64128 Len=0 TSval=322727483 TSecr=882267158
11	0.23370316		192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=582 Ack=1837 Win=64128 Len=0 TSval=322727483 TSecr=882267158
12	5.10977237		PCSystemtec_82:36	PCSystemtec_89:c7	ARP	42	Who has 192.168.10.11? Tell 192.168.10.254
13	5.10979040		PCSystemtec_89:c7	PCSystemtec_82:36	ARP	42	192.168.10.11 is at 80:80:27:80:c7:c7
14	5.23454523		138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [FIN, ACK] Seq=587 Ack=582 Win=64768 Len=0 TSval=882272158 TSecr=322727483
15	5.23470959		192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [FIN, ACK] Seq=582 Ack=1837 Win=64128 Len=0 TSval=322727484 TSecr=882267158
16	5.23614316		192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=583 Ack=1838 Win=64128 Len=0 TSval=322727485 TSecr=882272158
17	5.23840528		138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=1838 Ack=583 Win=64768 Len=0 TSval=882272161 TSecr=322727484
18	5.24171585		PCSystemtec_89:c7	PCSystemtec_82:36	ARP	68	Who has 192.168.10.254? Tell 192.168.10.11
19	5.24174798		PCSystemtec_82:36	PCSystemtec_89:c7	ARP	42	192.168.10.254 is at 80:80:27:80:36:c7

```

> Frame 6: 613 bytes on wire (4894 bits), 613 bytes captured (4894 bits) on interface eth0, id 0
> Ethernet II, Src: PCSystemtec_82:36:c7 (80:80:27:82:36:c7), Dst: PCSystemtec_89:c7:c7 (80:80:27:89:c7:c7)
> Internet Protocol Version 4, Src: 138.76.29.8, Dst: 192.168.10.11
> Transmission Control Protocol, Src Port: 80, Dst Port: 53924, Seq: 1, Ack: 331, Len: 547
  Source Port: 80
  Destination Port: 53924
  [Stream index: 8]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 547]
  Sequence Number: 1 - (relative sequence number)
  Sequence Number (raw): 257436814
  Next Sequence Number: 248 - (relative sequence number)
  Acknowledgment Number: 331 - (relative ack number)
  Acknowledgment number (raw): 2729798325
  1000 --- = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
  Window: 587
  [Calculated window size: 64896]
  [Window size scaling factor: 128]
  Checksum: 8x258 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  - [Timestamps]
    Time since first frame in this TCP stream: 0.03067210 seconds
    Time since previous frame in this TCP stream: 0.00120182 seconds
  - [SEQ/ACK analysis]
    TCP payload (547 bytes)

```

- 
- Ip address 138.76.29.8
- Source Port: 80
- Ip address 192.168.10.11
- Destination Port: 53924

ในลำดับถัดมาเราจะสำรวจ HTTP messages ทั้งสอง (GET และ 200 OK) ซึ่งดักจับจากฝั่งที่ใกล้กับส่วนเชื่อมต่อ Internet ระหว่าง router และเครือข่ายของผู้ให้บริการอินเทอร์เน็ต เนื่องจาก packets ที่ถูกดักจับกำลังถูกส่งไปยัง server จะได้รับการส่งต่อออกมาจาก NAT router หมายเลข IP address และ/หรือ หมายเลข port อาจจะมีการเปลี่ยนแปลงจาก NAT

ให้เปิดไฟล์ nat-outside-wireshark-trace1-1.pcapng ค้นหา HTTP GET message ซึ่งเป็น packet ที่ตรงกับ HTTP GET message ที่ถูกส่งจาก client ไปยัง server ที่ใช้หมายเลข IP 138.76.29.8 ที่เวลา t = 0.27362245 จงใช้ข้อมูลจาก header ของ packet ดังกล่าวเพื่อตอบคำถามต่อไปนี้

4) เมื่อเวลาเท่าไร ที่ HTTP GET message ปรากฏขึ้นในไฟล์ nat-outside-wireshark-trace1-1.pcapng?

No.	Time	ICMP RTT	Source	Destination	Protocol	Length	Info
1	0.000000000		10.0.1.254	138.76.29.8	TCP	74	53924 → 88 [50K] Seq=8 Win=64248 Len=0 MSS=1460 SACK_PERM TSval=32272749 TSecr=0 WS=128
2	0.002058086		138.76.29.8	10.0.1.254	TCP	74	88 → 53924 [50K, ACK] Seq=8 Ack=1 Win=65168 Len=0 MSS=1460 SACK_PERM TSval=882266926 TSecr=32272749 WS=128
3	0.002853940		10.0.1.254	138.76.29.8	TCP	66	53924 → 88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=322727252 TSecr=882266926
4	0.027356291		10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
5	0.033303911		138.76.29.8	10.0.1.254	TCP	66	88 → 53924 [ACK] Seq=1 Ack=331 Win=64896 Len=0 TSval=882266954 TSecr=322727277
6	0.030625966		138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
7	0.031448670		10.0.1.254	138.76.29.8	TCP	66	53924 → 88 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TSval=322727281 TSecr=882266955
8	0.231409190		10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
9	0.232863618		138.76.29.8	10.0.1.254	TCP	66	88 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TSval=882267157 TSecr=322727481
10	0.233843313		138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (text/html)
11	0.233847113		10.0.1.254	138.76.29.8	TCP	66	53924 → 88 [ACK] Seq=582 Ack=1837 Win=64128 Len=0 TSval=322727483 TSecr=882267158
12	5.109037924		PCSystemtec_43:65	PCSystemtec_22:fd	ARP	42	Who has 10.0.1.253? Tell 10.0.1.254
13	5.191780729		PCSystemtec_22:fd	PCSystemtec_43:65	ARP	60	10.0.1.253 is at 00:00:27:12:22:fd:74
14	5.231662586		PCSystemtec_22:fd	PCSystemtec_43:65	ARP	42	Who has 10.0.1.254? Tell 10.0.1.253
15	5.231797677		PCSystemtec_43:65	PCSystemtec_22:fd	ARP	60	10.0.1.254 is at 00:00:27:12:22:fd:74
16	5.234407950		138.76.29.8	10.0.1.254	TCP	66	88 → 53924 [FIN, ACK] Seq=582 Ack=582 Win=64768 Len=0 TSval=882272158 TSecr=322727483
17	5.234787908		138.76.29.8	10.0.1.254	TCP	66	53924 → 88 [FIN, ACK] Seq=582 Ack=1837 Win=64128 Len=0 TSval=322732484 TSecr=882267158
18	5.236144683		10.0.1.254	138.76.29.8	TCP	66	53924 → 88 [ACK] Seq=583 Ack=1838 Win=64128 Len=0 TSval=322732485 TSecr=882272158
19	5.238091165		138.76.29.8	10.0.1.254	TCP	66	88 → 53924 [ACK] Seq=1838 Ack=583 Win=64768 Len=0 TSval=882272161 TSecr=322732484

- a.
- b. 0.027356291 Time

5) หมายเลข source IP และ destination IP และหมายเลข TCP source port และ destination port ของ IP datagram ที่นำส่ง HTTP GET มีค่าเป็นเท่าใดบ้าง? (โปรดระบุค่าตามที่บันทึกได้ในไฟล์ nat-outside-wireshark-trace1-1.pcapng)

No.	Time	ICMP RTT	Source	Destination	Protocol	Length	Info
1	0.000000000		10.0.1.254	138.76.29.8	TCP	74	53924 → 88 [50K] Seq=8 Win=64248 Len=0 MSS=1460 SACK_PERM TSval=32272749 TSecr=0 WS=128
2	0.002058086		138.76.29.8	10.0.1.254	TCP	74	88 → 53924 [50K, ACK] Seq=8 Ack=1 Win=65168 Len=0 MSS=1460 SACK_PERM TSval=882266926 TSecr=32272749 WS=128
3	0.002853940		10.0.1.254	138.76.29.8	TCP	66	53924 → 88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=322727252 TSecr=882266926
4	0.027356291		10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
5	0.033303911		138.76.29.8	10.0.1.254	TCP	66	88 → 53924 [ACK] Seq=1 Ack=331 Win=64896 Len=0 TSval=882266954 TSecr=322727277
6	0.030625966		138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
7	0.031448670		10.0.1.254	138.76.29.8	TCP	66	53924 → 88 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TSval=322727281 TSecr=882266955
8	0.231409190		10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
9	0.232863618		138.76.29.8	10.0.1.254	TCP	66	88 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TSval=882267157 TSecr=322727481
10	0.233843313		138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (text/html)
11	0.233847113		10.0.1.254	138.76.29.8	TCP	66	53924 → 88 [ACK] Seq=582 Ack=1837 Win=64128 Len=0 TSval=322727483 TSecr=882267158
12	5.109037924		PCSystemtec_43:65	PCSystemtec_22:fd	ARP	42	Who has 10.0.1.253? Tell 10.0.1.254
13	5.191780729		PCSystemtec_22:fd	PCSystemtec_43:65	ARP	60	10.0.1.253 is at 00:00:27:12:22:fd:74
14	5.231662586		PCSystemtec_22:fd	PCSystemtec_43:65	ARP	42	Who has 10.0.1.254? Tell 10.0.1.253
15	5.231797677		PCSystemtec_43:65	PCSystemtec_22:fd	ARP	60	10.0.1.254 is at 00:00:27:12:22:fd:74
16	5.234407950		138.76.29.8	10.0.1.254	TCP	66	88 → 53924 [FIN, ACK] Seq=582 Ack=582 Win=64768 Len=0 TSval=882272158 TSecr=322727483
17	5.234787908		138.76.29.8	10.0.1.254	TCP	66	53924 → 88 [FIN, ACK] Seq=582 Ack=1837 Win=64128 Len=0 TSval=322732484 TSecr=882267158
18	5.236144683		10.0.1.254	138.76.29.8	TCP	66	53924 → 88 [ACK] Seq=583 Ack=1838 Win=64128 Len=0 TSval=322732485 TSecr=882272158
19	5.238091165		138.76.29.8	10.0.1.254	TCP	66	88 → 53924 [ACK] Seq=1838 Ack=583 Win=64768 Len=0 TSval=882272161 TSecr=322732484

- a.
- b. Source IP address : 10.0.1.254 , Source port : 53924
- c. Destination IP address : 138.76.29.8 , Destination port : 80

6) จากข้อ 5) ค่าของ field ทั้ง 4 มี field ไດบ้างที่แตกต่างจากข้อ 1) ?

- a. Source IP

7) จากการตรวจสอบ HTTP GET message เทียบระหว่างไฟล์ทั้งสอง มี field ไດใน HTTP header ที่เปลี่ยนแปลงหรือไม่? ถ้าหากมีพบว่าเป็น field ไດบ้าง?

```

Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
      Host: 138.76.29.8\r\n
      User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
      \r\n
      [Full request URI: http://138.76.29.8/]
      [HTTP request 1/2]
      [Response in frame: 6]
      [Next request in frame: 8]

```

a.

```

> Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack: 1, Len: 330
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
      Host: 138.76.29.8\r\n
      User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
      \r\n
      [Full request URI: http://138.76.29.8/]
      [HTTP request 1/2]
      [Response in frame: 6]
      [Next request in frame: 8]

```

b.

c. ไม่มี

- 8) ใน IP datagram ที่นำส่ง HTTP GET จาก datagram ที่ดักจับได้ในฝั่ง LAN (ฝั่งด้านใน) กับ datagram ที่ถูกส่งต่อออกมายังฝั่งที่ใกล้กับการเชื่อมต่อ Internet (ฝั่งด้านนอก) ของ NAT router มีค่าของ field ใดที่เปลี่ยนแปลงไปบ้างจากรายชื่อ field ใน IP header ต่อไปนี้: Version, Header Length, Flags, Checksum, Time to Live? หากมีการเปลี่ยนแปลงค่า โปรดระบุค่าเดิมและค่าใหม่

a. Checksum และ TTL เปลี่ยนแปลง

i. nat-inside : Checksum = 0x64dc , TTL = 64

ii. nat-outside : Checksum = 0x2492 , TTL = 63

Internet Protocol Version 4																											
0												15				16								31			
Version 4				Header ... 20				Differentiated Services... 0x00				Total Length 382															
Identification 0x6296 (25238)								Flags 0x2				Fragment Offset 0															
Time to Live 64				Protocol TCP				Header Checksum 0x64dc																			
Source Address 192.168.10.11																											
Destination Address 138.76.29.8																											

b.

Internet Protocol Version 4																																															
0																15								16																31							
Version 4								Header ... 20								Differentiated Services... 0x00								Total Length 382																							
Identification 0x6296 (25238)																Flags 0x2				Fragment Offset 0																											
Time to Live 63								Protocol TCP								Header Checksum 0x2492																															
Source Address 10.0.1.254																																															
Destination Address 138.76.29.8																																															

c.

ลำดับถัดไปเราจะศึกษาไฟล์ nat-outside-wireshark-trace1-1.pcapng ต่อ โดยให้ค้นหา HTTP reply ที่นำส่ง “200 OK” message ซึ่งเป็นการตอบ HTTP GET request ที่ผู้เรียนได้สำรวจไปในคำถามข้อ 4) ถึงข้อ 8) ก่อนหน้านี้ ให้ศึกษา packet ดังกล่าวเพื่อตอบคำถามต่อไปนี้

9) เมื่อเวลาเท่าไร ที่ HTTP 200 OK message ปรากฏขึ้นในไฟล์ nat-outside-wireshark-trace1-1.pcapng?

1	0.000000000	10.0.1.254	138.76.29.8	TCP	74	53924 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=322727249 TSecr=0
2	0.002058006	138.76.29.8	10.0.1.254	TCP	74	80 → 53924 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=802266955 TSecr=0
3	0.002853940	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=322727252 TSecr=802266926
4	0.027356291	10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
5	0.029338911	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [ACK] Seq=1 Ack=331 Win=64896 Len=0 TSval=802266954 TSecr=322727277
6	0.030625966	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
7	0.031448670	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TSval=322727281 TSecr=802266955
8	0.231400190	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
9	0.232863610	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TSval=802267157 TSecr=322727481
10	0.233043313	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (text/html)
11	0.233687113	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=582 Ack=1837 Win=64128 Len=0 TSval=322727483 TSecr=802267158

a.

b. 0.030625966

10) หมายเลข source IP และ destination IP และหมายเลข TCP source port และ destination port ของ IP datagram ที่นำส่ง HTTP reply (“200 OK”) มีค่าเป็นเท่าใดบ้าง? (โปรดระบุค่าตามที่บันทึกได้ในไฟล์ nat-outside-wireshark-trace1-1.pcapng)

1	0.000000000	10.0.1.254	138.76.29.8	TCP	74	53924 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=322727249 TSecr=0
2	0.002058006	138.76.29.8	10.0.1.254	TCP	74	80 → 53924 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=802266955 TSecr=0
3	0.002853940	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=322727252 TSecr=802266926
4	0.027356291	10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
5	0.029338911	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [ACK] Seq=1 Ack=331 Win=64896 Len=0 TSval=802266954 TSecr=322727277
6	0.030625966	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
7	0.031448670	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TSval=322727281 TSecr=802266955
8	0.231400190	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
9	0.232863610	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TSval=802267157 TSecr=322727481
10	0.233043313	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (text/html)
11	0.233687113	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=582 Ack=1837 Win=64128 Len=0 TSval=322727483 TSecr=802267158
12	5.180837924	PCSSystemtec_22:fd:74	PCSSystemtec_43:65:cd	ARP	42	Who has 10.0.1.253? Tell 10.0.1.254
13	5.181703320	PCSSystemtec_22:fd:74	PCSSystemtec_43:65:cd	ARP	42	Who has 10.0.1.253? Tell 10.0.1.254

a.

b. Source IP address : 138.76.29.8, Source port : 80

c. Destination IP address : 10.0.1.254 , Destination port : 53924

ส่วนสุดท้ายมาพิจารณาว่าเกิดอะไรขึ้นเมื่อ NAT router รับ diagram ที่ผู้เรียนสำรวจไปในคำถามที่ 9) และ 10) จากนั้นนำ packet ดังกล่าวมาผ่าน Network Address Translation และส่งต่อไปยัง host ซึ่งอยู่ฝั่ง LAN จากคำถามที่ผู้เรียนได้ตอบไปตั้งแต่ 1) ถึงข้อ 10) ผู้เรียนควรจะสามารถตอบคำถามข้อต่อไปนี้อย่างไม่จำเป็นต้องดูข้อมูลจาก packet จริงๆ เสียด้วยซ้ำ

- 11) หมายเลข source IP และ destination IP และหมายเลข TCP source port และ destination port ของ IP datagram ที่นำส่ง HTTP reply ("200 OK") ซึ่งถูกส่งจาก router ไปยัง host ปลายทางที่อยู่ด้านขวาตาม รูป 1 มีค่าเป็นเท่าใดบ้าง? (โปรดระบุค่าตามที่บันทึกได้ในไฟล์ nat-inside-wireshark-trace1-1.pcapng)

1	0.000000000	192.168.10.11	138.76.29.8	TCP	74	53924 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=322727249 TSecr=0
2	0.002091700	138.76.29.8	192.168.10.11	TCP	74	80 → 53924 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=8022665 TSecr=8022665
3	0.002870917	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=322727252 TSecr=802266926
4	0.027362245	192.168.10.11	138.76.29.8	HTTP	396	GET / HTTP/1.1
5	0.029390199	138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=1 Ack=331 Win=64896 Len=0 TSval=802266954 TSecr=322727277
6	0.030972101	138.76.29.8	192.168.10.11	HTTP	613	HTTP/1.1 200 OK (text/html)
7	0.031464845	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TSval=322727281 TSecr=802266955
8	0.231407421	192.168.10.11	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
9	0.232896589	138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TSval=802267157 TSecr=322727481
10	0.233074462	138.76.29.8	192.168.10.11	HTTP	555	HTTP/1.1 404 Not Found (text/html)
11	0.233703166	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322727483 TSecr=802267158
12	5.189772327	PCSSystemtec_82:c7...	PCSSystemtec_89:c7...	ARP	42	Who has 192.168.10.11? Tell 192.168.10.254
13	5.191709501	PCSSystemtec_89:c7...	PCSSystemtec_82:c7...	ARP	60	192.168.10.11 is at 08:00:27:89:c7:c7

> Frame 6: 613 bytes on wire (4904 bits), 613 bytes captured (4904 bits) on interface eth1, id 0  
> Ethernet II, Src: PCSSystemtec\_02:36:d7 (08:00:27:82:36:d7), Dst: PCSSystemtec\_89:c7:c7 (08:00:27:89:c7:c7)  
> Internet Protocol Version 4, Src: 138.76.29.8, Dst: 192.168.10.11  
Transmission Control Protocol, Src Port: 80, Dst Port: 53924, Seq: 1, Ack: 331, Len: 547

- a. Source IP address : 138.76.29.8, Source port : 80  
c. Destination IP address : 192.168.10.11 , Destination port : 53924
- 12) หากมีให้เพียงไฟล์ trace จำนวนสองไฟล์ซึ่งดักจับ packets จากสองฝั่งของ NAT device ผู้เรียนสามารถระบุได้หรือไม่ว่าฝั่งใดเป็นฝั่งเริ่มต้นส่งข้อมูลก่อนที่จะเกิดการ NAT ขึ้น? สามารถสังเกตได้จากอะไร? จงอธิบาย

- a. เราสามารถสังเกตการแปลงที่เกิดขึ้นได้โดยดูที่ source IP address และ destination IP address ใน packets ที่จับได้ทั้งสองฝั่ง.
- b. ฝั่ง LAN (Local Area Network): นี่จะเป็นฝั่งที่มี private IP addresses (เช่น 192.168.x.x, 10.x.x.x) ซึ่งเป็น IP addresses ที่ไม่สามารถเรียกใช้บน Internet สาธารณะได้. ฝั่งนี้คือฝั่งที่เริ่มต้นส่งข้อมูลก่อนที่จะเกิดการ NAT จะเกิดขึ้น.
- c. ฝั่ง WAN (Wide Area Network): นี่จะเป็นฝั่งที่มี public IP addresses ซึ่งสามารถเข้าถึงได้จาก Internet. ข้อมูลที่ผ่าน NAT แล้วจะมี IP address ที่ถูกแปลงเป็น public IP address ของ NAT device.

## Submission

จงตอบคำถามในส่วนที่ระบุหัวข้อ Questions (A) ซึ่งมีคำถามรวมทั้งหมด 12 ข้อ โดยในคำตอบของแต่ละข้อด้วยให้อธิบายด้วยว่าหาคำตอบมาได้อย่างไร ตัวอย่างเช่น อธิบายว่าสามารถค้น packet ตามที่โจทย์ระบุได้ด้วยวิธีการใด หรือค่าที่นำมาตอบ นำมาจาก field ใดของ header ตาม protocol ใด

ในกรณีที่คัดลอกคำตอบของคนอื่นมา ให้ระบุชื่อของบุคคลที่เป็นต้นฉบับมาด้วย หากตรวจพบว่ามีการลอกมาแต่ไม่มีการระบุชื่อบุคคลที่เป็นต้นฉบับ ผู้สอนจะถือว่าทุจริตและอาจพิจารณาลงโทษให้ตกเกณฑ์รายวิชาในทันที

การส่งงาน ให้เขียนหรือพิมพ์หมายเลขข้อและคำตอบของข้อนั้นๆ และส่งเป็นไฟล์ PDF เท่านั้น กรุณาดังชื่อไฟล์โดยใช้รหัสนักศึกษา ตามด้วย section และ \_lab09 ตามตัวอย่างต่อไปนี้ 64019999\_sec20\_lab09.pdf