ชื่อ นาย รวีโรจน์ ทองดี **รหัสนักศึกษา** 62010763

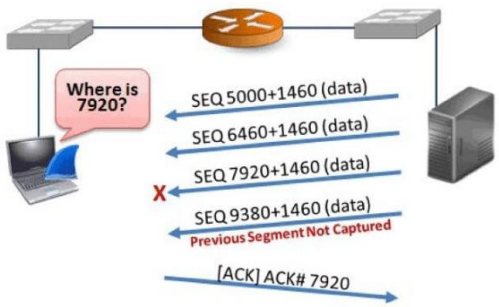
กิจกรรมที่ 7 : TCP Retransmission

กิจกรรมที่ 7 : TCP Retransmission

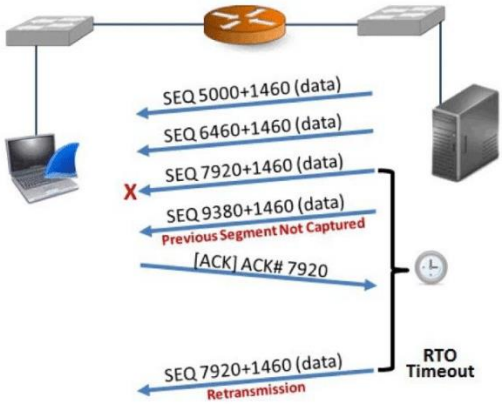
กิจกรรมครั้งนี้จะเป็นการทำความเข้าใจกับโปรโตคอล TCP (Transmission Control Protocol) ให้มากยิ่งขึ้น โดยเน้นเรื่องของ Retransmission

การรับข้อมูลของ TCP จะมีแนวทางการทำงาน ดังนี้

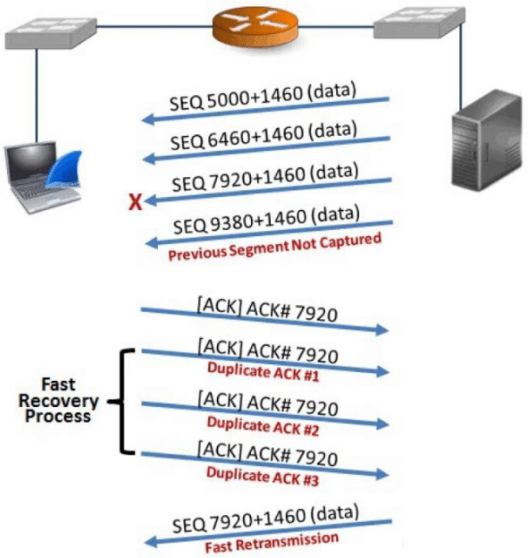
- Delayed ACK กรณีที่ฝั่งรับได้ ACK ตอบรับ packet ที่ได้รับไปทั้งหมดก่อนหน้านี้แล้ว เมื่อได้รับข้อมูลใหม่ อาจชะลอการส่ง ACK ไปก่อน เป็นระยะเวลาหนึ่งได้ หากไม่ได้รับ packet เพิ่มเติมจึงส่ง ACK ไป
- หากฝั่งรับ ยังไม่ได้ ACK ข้อมูลของ packet ล่าสุด เมื่อได้รับข้อมูลใหม่ ให้ ACK ข้อมูลล่าสุดทันที (Accumulative ACK)
- หากฝั่งรับได้รับ segment ที่ไม่เป็นไปตามลำดับ จะส่ง ACK ของ segment ล่าสุดที่ยังเป็นไปตามลำดับกลับไปทันที ซึ่งอาจทำให้เกิด *duplicate ACK*



- ในกรณีที่เกิดการ lost segment จะมีวิธีการแก้ไข 2 รูปแบบ คือ retransmission โดยจะส่งข้อมูลใหม่ เมื่อครบเวลาของ retransmission time out (RTO)



- อีกรูปแบบหนึ่ง คือ fast retransmission ซึ่งจะใช้ได้เฉพาะ OS ที่สนับสนุน โดยเมื่อได้รับ *duplicate ACK* ครบ 3 ครั้ง ก็จะส่งข้อมูลให้ใหม่



1. ให้เปิดไฟล์ http-browse101d.pcapng คลิกขวาที่ Sequence Number และเลือก Apply as Column และตั้งชื่อว่า SEQ# จากนั้นคลิกขวาที่ Next Sequence Number และเลือก Apply as Column และตั้งชื่อว่า NEXTSEQ# และคลิกขวาที่ Acknowledgment Number และเลือก Apply as Column และตั้งชื่อว่า ACK# จัดรูปแบบคอลัมน์ให้เหมาะสม จะเห็นว่าเรามีข้อมูลของ SEQ#, NEXTSEQ# และ ACK# สำหรับช่วยในการวิเคราะห์
2. ใน wireshark จะมีข้อมูลที่ wireshark วิเคราะห์ขึ้น และสามารถนำมาเป็น display filter ได้ เช่น
   - tcp.analysis.duplicate_ack จะค้นหา packet ที่เกิด duplicate ACK
   - tcp.analysis.lost_segment จะค้นหา lost segment
   - tcp.analysis.retransmission จะค้นหา packet ที่เกิด retransmission
   - tcp.analysis.fast_retransmission จะค้นหา packet ที่เกิด fast retransmission
3. ให้เปิดไฟล์ tr-general101d.pcapng แล้วใช้ tcp.analysis.lost_segment กรอง จะพบว่ามี lost segment ทั้งหมด 5 แห่ง ให้ดู Packet 10416 แล้วตอบคำถามว่า มีข้อมูลหายไปเท่าไร มี Packet หายไปกี่ Packet บอกวิธีการหาแบบย่อๆ

เราสามารถหาได้จากนำ sequent number ของ packet ที่ 10417 มาเทียบ next sequent number ส่วน len หรือความยาวของ packet ของข้อมูล คือ 1320 และ window คือ 46 byte ซึ่งจากข้อมูลจะได้ดังนี้คือ

1. จากการส่ง seq 9163441 ออกไปและได้พบอีกครั้งคือ seq 9175321 ซึ่งห่างกันอยู่
   9175321 – 9164761 = 10560 seq
2. ซึ่งหากเรานำมาหารด้วยความยาวของ packet (Len) จะได้เป็นจำนวน packet ออกมาดังนี้
   10560 / 1320 = 8 packet
3. และหากเป็นจำนวนของข้อมูลว่าหายไปเท่าไหร่สามารถคิดได้จาก
   8 * 46 = 368 byte

4. จาก segment lost ใน packet 10416 หลังจากนั้นจะพบว่ามี Duplicate Ack เกิดขึ้นเป็นจำนวนมาก ให้อธิบายสาเหตุของการเกิด Duplicate Ack และเกิด Duplicate Ack กี่ครั้งในกรณี packet 10416

สาเหตุที่เกิดการ Duplicate ACK เพราะว่าทั้งผู้ส่ง (10.9.9.9) และผู้รับ (10.10.10.10) ซึ่งต่างคนต่างพยายามส่งมันเกิด timeout ไปแล้ว และเกิด loss ซึ่งเกิด Duplicate ACK จำนวน 808 ครั้ง

5. จากข้อ 3 ข้อมูลที่หายไป ผู้ส่งทราบเมื่อใด ได้มีการส่งใหม่หรือไม่ และส่งใหม่ใน packet ใด ใช้เวลาเท่าใดในการส่งใหม่

ทราบได้จากเมื่อเราตรวจพบเจอ 3-ACK Duplicate ซึ่งก็คือ (packet ที่ 10424)
แล้วมีการเริ่มส่งใหม่ (Retransmission) ที่ packet 12035 (Fast retransmission)
ซึ่งใช้เวลา 0.000033 วินาที

12034	0.000015	10.10.10.10	10.9.9.9	TCP	74	[TCP Dup ACK 10418#808] 1479 → 30000 [ACK]
12035	0.000033	10.9.9.9	10.10.10.10	TCP	1374	[TCP Fast Retransmission] 30000 → 1479 [ACK
12036	0.000204	10.9.9.9	10.10.10.10	TCP	1374	30000 → 1479 [ACK] Seq=10255081 Ack=1 Win=4
12037	0.000011	10.10.10.10	10.9.9.9	TCP	74	1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32

6. ให้ใช้ display filter : tcp.analysis.out_of_order จะพบ out of order อยู่ 8 ครั้ง ให้หาว่า packet 12249 เป็น out of order ของ segment ใด อธิบายโดยย่อ

เป็น Out of order ที่เกิดจาก segment ใน packet ที่ 12246 เกิดจากการที่ Retransmission เลยเวลา RTO ไปแล้ว

12245	0.000010	10.10.10.10	10.9.9.9	TCP	74	[TCP Dup ACK 12037#104] 1479 → 30000 [ACK] Seq=1 Ack=9166081
12246	0.001753	10.9.9.9	10.10.10.10	TCP	1374	30000 → 1479 [PSH, ACK] Seq=10393681 Ack=1 Win=46 Len=1320
12247	0.000011	10.10.10.10	10.9.9.9	TCP	74	[TCP Dup ACK 12037#105] 1479 → 30000 [ACK] Seq=1 Ack=9166081
12248	0.000019	10.9.9.9	10.10.10.10	TCP	1374	[TCP Fast Retransmission] 30000 → 1479 [ACK] Seq=9166081 Ack
12249	0.000099	10.9.9.9	10.10.10.10	TCP	1374	[TCP Out-Of-Order] 30000 → 1479 [ACK] Seq=9167401 Ack=1 Win=
12250	0.000028	10.10.10.10	10.9.9.9	TCP	74	1479 → 30000 [ACK] Seq=1 Ack=9168721 Win=32768 Len=0 SLE=990

7. ไปที่ packet 12259 จะพบว่าเป็น retransmission ให้บอกว่าเป็น retransmission จาก RTO Timer หรือจากการได้รับ 3 Duplicate Ack พร้อมเหตุผลประกอบโดยย่อ

เป็นการ Retransmission ที่เกิด RTO Timer เหตุเพราะหลังจาก packet 12249 (เริ่ม Out of order) ไม่เกิดเหตุการณ์ 3ACK- Duplicate เกิดเลย

12249	0.000099	10.9.9.9	10.10.10.10	TCP	1374	[TCP Out-Of-Order] 30
12250	0.000028	10.10.10.10	10.9.9.9	TCP	74	1479 → 30000 [ACK] Se
12251	0.000082	10.9.9.9	10.10.10.10	TCP	1374	[TCP Out-Of-Order] 30
12252	0.001791	10.9.9.9	10.10.10.10	TCP	1374	[TCP Out-Of-Order] 30
12253	0.000018	10.10.10.10	10.9.9.9	TCP	74	1479 → 30000 [ACK] Se
12254	0.000022	10.9.9.9	10.10.10.10	TCP	1374	[TCP Out-Of-Order] 30
12255	0.000024	10.10.10.10	10.9.9.9	TCP	74	1479 → 30000 [ACK] Se
12256	0.000181	10.9.9.9	10.10.10.10	TCP	1374	[TCP Out-Of-Order] 30
12257	0.000026	10.9.9.9	10.10.10.10	TCP	1374	[TCP Out-Of-Order] 30
12258	0.000512	10.10.10.10	10.9.9.9	TCP	66	1479 → 30000 [ACK] Se
12259	0.001231	10.9.9.9	10.10.10.10	TCP	1374	[TCP Retransmission]

งานครั้งที่ 7

- การส่งงาน ให้ส่งเป็นไฟล์ PDF จำนวน 1 ไฟล์ เท่านั้น ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา
- ส่วนบนของหน้าแรกให้มี รหัสนักศึกษา และ ชื่อนักศึกษา
- กำหนดส่ง ภายในวันที่ 28 กุมภาพันธ์ 2564