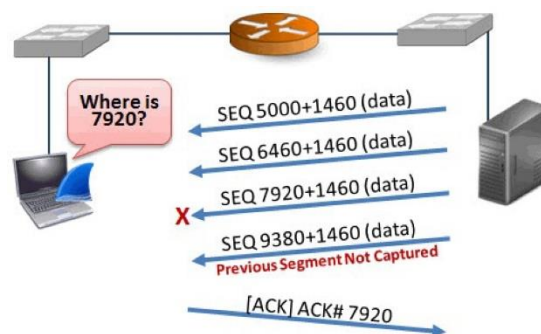


กิจกรรมที่ 7 : TCP Retransmission

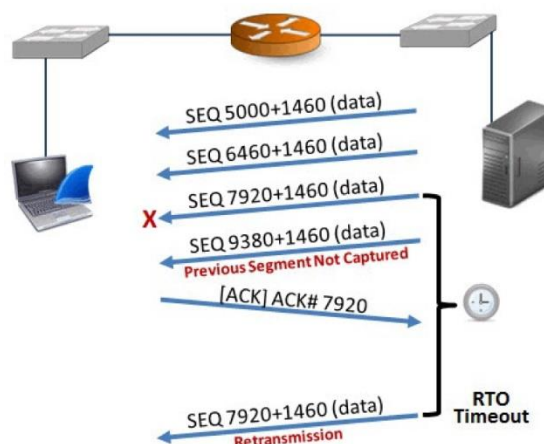
กิจกรรมครั้งนี้จะเป็นการทำความเข้าใจกับโปรโตคอล TCP (Transmission Control Protocol) ให้มากยิ่งขึ้น โดยเน้นเรื่องของ Retransmission

การรับข้อมูลของ TCP จะมีแนวทางการทำงาน ดังนี้

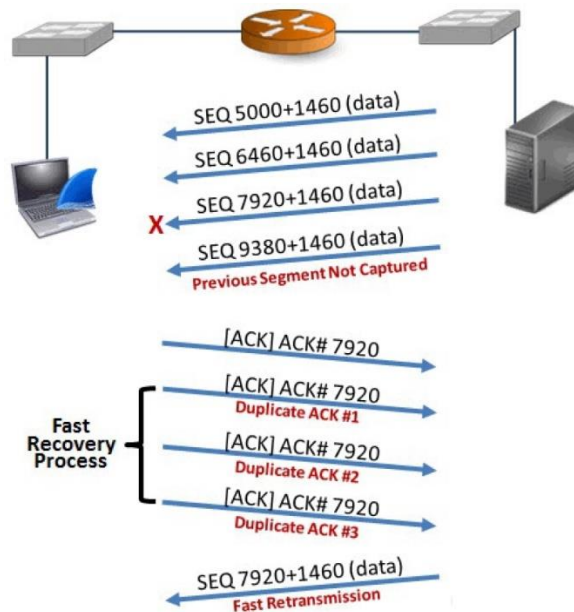
- Delayed ACK กรณีที่ฝั่งรับได้ ACK ตอบรับ packet ที่ได้รับไปทั้งหมดก่อนหน้านี้แล้ว เมื่อได้รับข้อมูลใหม่ อาจชะลอการส่ง ACK ไปก่อน เป็นระยะเวลาหนึ่งได้ หากไม่ได้รับ packet เพิ่มเติมจึงส่ง ACK ไป
- หากฝั่งรับ ยังไม่ได้ ACK ข้อมูลของ packet ล่าสุด เมื่อได้รับข้อมูลใหม่ ให้ ACK ข้อมูลล่าสุดทันที (Cumulative 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 ก็ส่งข้อมูลให้ใหม่



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 จะพบว่า มี lost segment ทั้งหมด 5 แห่ง จาก Packet 10417 ให้ย้อนดู Packet 10416 แล้วตอบคำถามว่า มีข้อมูลหายไปเท่าไร มี Packet หายไปกี่ Packet บอกวิธีการหาแบบย่อๆ

4. จาก segment lost ใน packet 10417 หลังจากนั้นจะพบว่ามี Duplicate Ack เกิดขึ้นเป็นจำนวนมาก ให้อธิบายสาเหตุของการเกิด Duplicate Ack และเกิด Duplicate Ack ที่ครั้งในกรณีนี้

5. จากข้อ 3 ข้อมูลที่หายไป ผู้ส่งทราบเมื่อใด ได้มีการส่งใหม่หรือไม่ และส่งใหม่ใน packet ใด ใช้เวลาเท่าใดในการส่งใหม่

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 ไດ อธิบายโดยย่อ

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

งานครั้งที่ 7

- การส่งงาน เขียนหรือพิมพ์ลงในเอกสารนี้ และส่งโดยเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา และ _Lab7 เช่น 63010789_Lab6.pdf
- กำหนดส่ง ภายในวันที่ 16 มีนาคม 2565