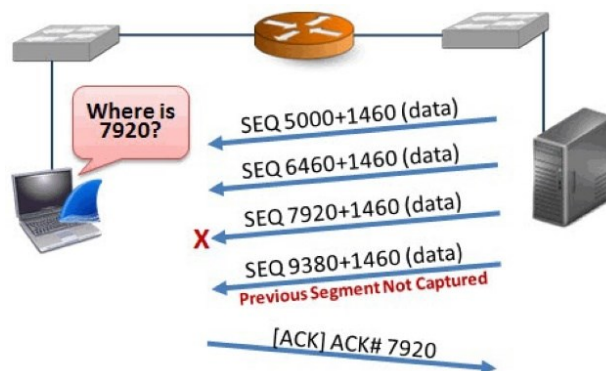


กิจกรรมที่ 7 : TCP Retransmission

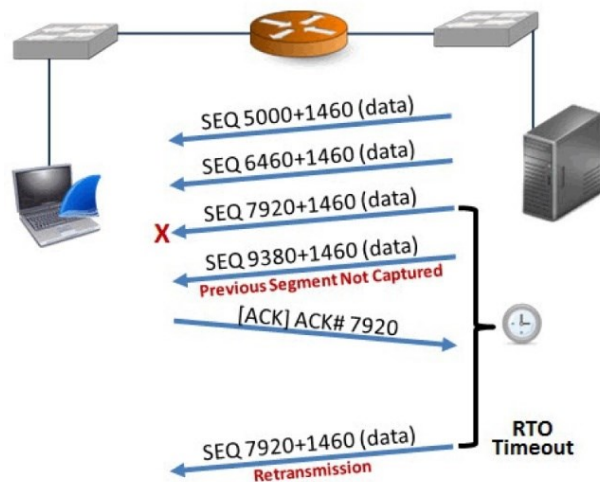
กิจกรรมครั้งนี้จะเป็นการทำความเข้าใจกับโปรโตคอล TCP (Transmission Control Protocol) ให้มากยิ่งขึ้น โดยเน้นเรื่องของกระบวนการ Retransmission

การรับข้อมูลของ TCP จะมีแนวทางการตอบ ACK ที่ระบุ ACK# เป็นหมายเลข X เพื่อใช้บ่งบอกว่าได้รับข้อมูลที่มี SEQ# ก่อน X ทั้งหมดแล้ว และกำลังรอรับ SEQ# X เป็นตัวถัดไป (Cumulative ACK) โดยทั่วไปสามารถสรุปแนวทางได้ดังตารางข้างล่างนี้

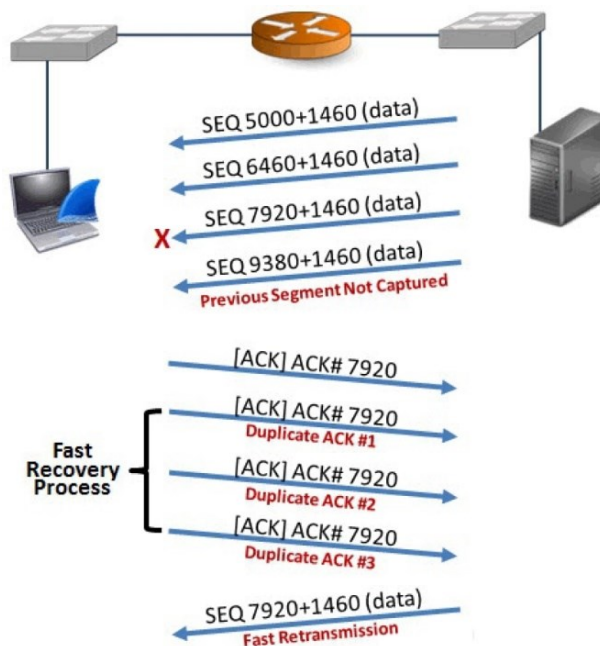
ข้อมูลที่ฝั่งรับส่ง ACK ตอบไปแล้ว	TCP Segment ที่ฝั่งได้รับมา	สิ่งที่ฝั่งรับต้องดำเนินการต่อไป
ตอบ ACK# เท่ากับ SEQ# ที่กำลังรอรับ	SEQ# ตรงกับที่กำลังรอรับ	ชะลอการส่ง ACK (Delayed ACK) ออกไปก่อน แต่ไม่เกิน 500 ms (ตาม RFC 5681) โดยหากไม่ได้รับ TCP Segment อื่นเพิ่มในเวลาที่กำหนดจึงส่ง ACK ออกไป
ยังตอบ ACK# ไม่ถึง SEQ# ที่กำลังรอรับ	SEQ# ตรงกับที่กำลังรอรับ	ส่ง ACK ออกไปทันที โดยระบุ ACK# เป็น SEQ# ตัวที่กำลังรอรับล่าสุด ซึ่งถัดไปข้อมูลใน TCP Segment ที่ฝั่งได้รับมา
ตอบ ACK# จนถึง SEQ# ใดๆ	SEQ# เกินกว่าที่กำลังรอรับ ข้อมูลไม่เป็นไปตามลำดับ (Out of Order)	ส่ง ACK ออกไปทันที โดยระบุ ACK# เป็น SEQ# ตัวที่กำลังรอรับอยู่ ซึ่งอาจจะมี ACK# ซ้ำกับ ACK ล่าสุดที่เคยส่งออกไปแล้ว (Duplicate ACK)



- ในกรณีที่เกิด Lost Segment จะมีวิธีการแก้ไข 2 รูปแบบ คือ Retransmission โดยฝั่งส่งทำการส่งข้อมูลใหม่ เมื่อฝั่งส่งไม่ได้รับ ACK ภายในเวลา Retransmission Timeout (RTO)



- อีกรูปแบบหนึ่ง คือ Fast Retransmission ซึ่งจะใช้ได้เฉพาะ OS ที่สนับสนุน โดยเมื่อฝั่งส่งได้รับ Duplicate ACK ครบ 3 ครั้ง ก็จะส่งข้อมูลให้ฝั่งรับใหม่



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 ที่เป็น Duplicate ACK
 - `tcp.analysis.lost_segment` จะค้นหากรณีเกิด Lost Segment

- tcp.analysis.retransmission จะค้นหา Packet ที่เกิดจากการทำ Retransmission
- tcp.analysis.fast_retransmission จะค้นหา Packet ที่เกิดจากการทำ Fast Retransmission

3. ให้เปิดไฟล์ tr-general101d.pcapng แล้วใช้ tcp.analysis.lost_segment กรอง จะพบว่ามี Lost Segment ทั้งหมด 5 แห่ง จาก Packet 10417 ให้ย้อนดู Packet 10416 แล้วตอบคำถามว่า มีข้อมูลหายไปเท่าไร มี Packet หายไปที่ Packet บอกวิธีการหาแบบย่อๆ

4. จาก Lost Segment ใน Packet 10417 หลังจากนั้นจะพบว่ามี Duplicate Ack เกิดขึ้นเป็นจำนวนมาก ให้อธิบายสาเหตุของการเกิด Duplicate ACK และเกิด Duplicate ACK ที่ครั้งในกรณีนี้

จากข้อ 3 ข้อมูลที่หายไป ผู้ส่งทราบเมื่อใด ได้มีการส่งใหม่หรือไม่ และส่งใหม่ใน Packet ใด และเวลาผ่านไปนานเท่าใดถึงได้ส่งใหม่

5. ให้ใช้ Display Filter : `tcp.analysis.out_of_order` จะพบ Out of Order อยู่ 8 ครั้ง ให้หาว่า Packet 12249 เป็น Out of Order จากเหตุการณ์หรือเงื่อนไขใด ให้ศึกษาวิธีการที่ Wireshark ตัดสินใจและอธิบายโดยย่อ

6. ไปที่ packet 12259 จะพบว่าเป็น Retransmission ให้บอกว่าเป็น Retransmission จาก RTO Timer หรือจากการได้รับ 3 Duplicate Ack พร้อมเหตุผลประกอบโดยย่อ

งานครั้งที่ 7

- การส่งงาน เขียนหรือพิมพ์ลงในเอกสารนี้ และส่งเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา ตามด้วย section และ _lab02 ตามตัวอย่างต่อไปนี้
64019999_sec20_lab07.pdf
- กำหนดส่ง ภายในวันที่ 3 มีนาคม 2566 โดยให้ส่งใน Microsoft Teams ของรายวิชา