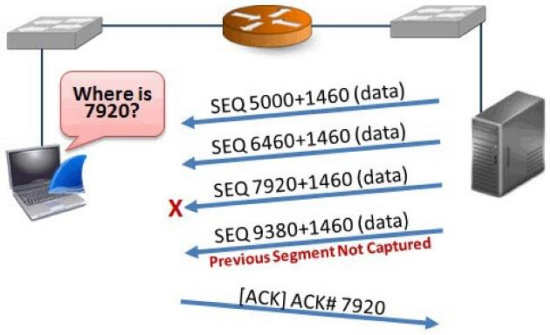
นาย ศักรพัทธิ์ ชัยอมรเทพ 62010184

กิจกรรมที่ 7 : TCP Retransmission

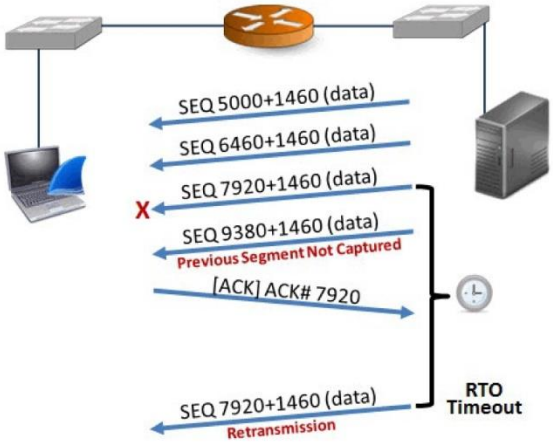
กิจกรรมครั้งนี้จะเป็นการทำความเข้าใจกับโปรโตคอล TCP (Transmission Control Protocol) ให้มากยิ่งขึ้น โดยเน้นเรื่องของ Retransmission

การรับข้อมูลของ TCP จะมีแนวทางการทำงาน ดังนี้

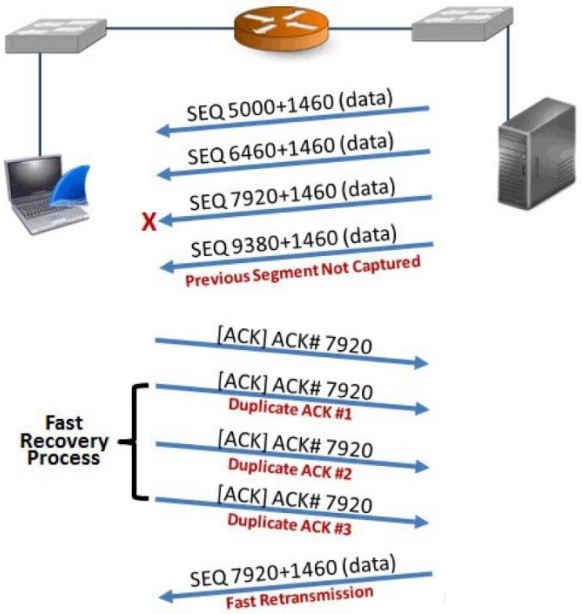
- Delayed ACK กรณีที่ฝั่งรับได้ ACK ตอบรับ packet ที่ได้รับไปทั้งหมดก่อนหน้านี้แล้ว เมื่อได้รับข้อมูลใหม่ อาจชะลอการส่ง ACK ไปก่อน เป็นระยะเวลาหนึ่งได้ หากไม่ได้รับ packet เพิ่มเติมจึงส่ง ACK ไป
- หากฝั่งรับ ยังไม่ได้ ACK ข้อมูลของ packet ล่าสุด เมื่อได้รับข้อมูลใหม่ ให้ ACK ข้อมูลล่าสุดทันที (Accumulative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

มีข้อมูลหายไป: 9175321 - 9164761 = 10,560 (segment ที่ต่างกัน)

packet ที่หายไป: 10,560 ÷ 1320 = 8 packets (1320 = length ของแต่ละ packet)

วิธีทำ ให้ sort packet และดู seq.no. บน packet ที่ loss แล้วเทียบกับ seq.no. บน frame ที่ loss (TCP segment not captured) แล้วหาผลต่าง ค.ศ. ของแต่ละ packet แล้วเราจะได้จำนวน packet ออกมา

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

- Duplicate ACK เกิดจาก reciever ไม่ได้รับ sequence no. ตามที่ตนเองต้องการ มากกว่า 1 ครั้ง.
- Duplicate ACK = 808 + 105 = 913

5. จากข้อ 3 ข้อมูลที่หายไป ผู้ส่งทราบเมื่อใด ได้มีการส่งใหม่หรือไม่ และส่งใหม่ใน packet ใด ใช้เวลาเท่าใดในการส่งใหม่

ผู้ส่งทราบเมื่อใด ? → เมื่อได้รับ duplicate ACK กลับมา และเลข sequence ไม่ตรงกัน

มีการส่งใหม่หรือไม่ ? → มีการส่งใหม่ ส่ง 8 packet มี packet ที่ 12035, 12248, 12249, 12252, 12253, 12254, 12256, 12257

เวลาที่ใช้: 0.331226 sec

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

หลังจาก packet ที่ 12246 ส่ง data ไปแล้ว. sequence no. ก็จะไม่ถูกเรียงลำดับซึ่งทำให้เกิดการ out of order ในช่วงนั้น. และสาเหตุในการเกิด out of order ก็มาจากการเกิด fast-retransmittion เช่นกัน. เมื่อ next sequence no. ของ Packet 12246 ตรงกับ sequence no. ของ Packet ล่าสุดแล้ว ก็จะไม่เกิดการ out of order.

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

เป็น retransmission จาก RTO เพราะ เมื่อเราทำการ filter ด้วย 'tcp.analysis.duplicate_ack' จะไม่มีการแสดง packet 12259 ออกมา และไม่มีเลข Seq no.

งานครั้งที่ 7

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