CIS 457: Data Communications
Week 11 Assignment: Working with UDP and TCP Data Retransmission
Point Value: 10 Pts, late submission policy (20%/day for up to 5 days)
Due Date: 3/29/2024 by 12:00 AM EST
Submission format:

The following reports will be submitted on Blackboard (BB) using each group member's account.
(1) The entire assignment's solution in a PDF format (your contribution to the assignment)
(2) Group's Agreed-upon solution in a PDF format.
Note: Missing an individual's contribution leads to receiving **NO** credit for the assignment.

Lab Objectives

In this lab, we'll explore in depth several aspects of the TCP and UDP protocols, including:

- TCP Segment/UDP Datagram structure,
- TCP reliable data transfer service,

Part I: Working with UDP Protocol **(5 Pts)**

In this section, we'll quickly examine the UDP protocol. As we saw in Chapter 3 of the text, UDP is a streamlined, no-frills protocol. You may want to re-read the UDP section in the text before doing this lab. Download the packet trace named "**UDP.cap**" from Blackboard and answer the following questions. Select the first UDP packet in the trace and answer the following questions:

1. By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.
2. The value in the Length field is the length of what? Verify your answer with the captured UDP packet.
3. What maximum number of bytes can be included in a UDP payload?
4. What is the largest possible source port number?
5. What is the protocol number for UDP? Give your answer in hexadecimal and decimal notation. To answer this question, you'll need to look into the **Protocol** field of the **IP header** of the datagram containing this UDP segment.

Part II: Retransmission in TCP **(5 Pts)**

The **pcattcp_retrans_t.cap** Wireshark file is captured after having the client on the desktop machine with an IP address (192.168.0.100) write 50 buffers, with each buffer containing 1000 Bytes to the laptop machine with an IP address **(192.168.0.102**). Use this trace, along with the Wireshark filters listed in the "**Wireshark Filters**" file, to answer the following questions:

1. How many TCP segments are sent from **port 4480** on the desktop machine to **port 5001** on the laptop? Write a display filter to isolate this side of the connection and use it to answer this question.
2. Examine the suspected retransmissions identified by Wireshark in the **pcattcp_retrans_t.cap**. (Hint: Use the filter **tcp.analysis.retransmission**). List the retransmitted packets' assigned number by Wireshark and their associated sequence number. **Organize your answers in the following format:**
   Wireshark-Packet-Num-in-Pcattcp_retrans_t.cap → TCP Sequence Number
3. Continue using the **pcattcp_retrans_t.cap** trace, for the **first** packet that is lost before reaching the receiver, identify the retransmitted packet(s). (Hint: in your analysis, consider using the filter (tcp.seq = = TCP-Packet's SequenceNumber). Use the following format to organize your answer:

Original-Packet's total #of bytes → Re-transmitted Pkt's # of bytes → Wireshark-Packet #of the Re-transmitted Pkt

4. List the byte number (beginning and ending of each packet) of the TCP data packets with Wireshark-Packet numbers 4, 5, 7, and 8.
   Now, investigate the Options field of packet # 9.
5. Does the options field contain a SACK value? If yes, what does this value represent, and how does the TCP's sending side use it?