Name: Neil Shah
UCID: ns642
Class Section: 005

Wireshark Assignment 1: UDP Echo Client and Server

This wireshark assignment is to be used in conjunction with Programming Assignment 1. The wireshark trace is intended to demonstrate that your program is behaving as expected. **As such, please take 2 wireshark traces, one for each of the two test cases: 1) client and server exchange a single Echo Request and Echo Response, and 2) client sends 3 Echo Requests with no server response.**

Test Case 1:
Run the UDP Echo client and server on the same host with a packet length of less than 100 bytes (say 10 bytes). Enable wireshark on the null/loopback interface and capture packets between client and server. Store trace in a .pcap file with an appropriate name e.g. udp-echo-test1.pcap. When analyzing the .pcap file, specify a filter such that only your application packets are shown in the packet summary window.

Note:
Wireshark may misinterpret the data you are sending, and think it is a particular protocol, such as "LLC". If something other than UDP is shown in the "Protocol" column in the Packet Summary window, you can disable analysis of that protocol temporarily by going to "Analyze > Enabled Protocols" in the menu and unchecking the appropriate protocol.

Note: When a question asks for "packet number", this refers to the "No." column in the summary window of the wireshark trace.

Using the wireshark trace and what you have learned so far, answer the following questions (your answers MUST be consistent with that shown in the wireshark trace you hand in):

1. What packet number corresponds to the echo request from client? 10
2. What packet number correspond to the echo response from server? 11
3. What is the IP address of the client? 127.0.0.1
4. What is the IP address of the server? 127.0.0.1
5. What port is the client listening on? 56648
6. What port is the server listening on? 8000
7. When the client sends the packet to the server, what layer in the Internet architecture and what specific protocol in the protocol stack adds the port information to the packet?

Layer (Application/Transport/Network/Link): Transport
Protocol (TCP/UDP/IP/Ethernet/WiFi): UDP

8. When the client sends the packet to the server, what layer in the Internet architecture and what specific protocol in the protocol stack adds the IP address information to the packet?
   Layer (Application/Transport/Network/Link): Network
   Protocol (TCP/UDP/IP/Ethernet/WiFi): IP

9. In echo requests, what is the source port in the packet referring to: client or server? Server

10. In echo requests, what is the destination port in the packet referring to: client or server? Client

11. In echo responses, what is the source port in the packet referring to: client or server? Client

12. In echo responses, what is the destination port in the packet referring to: client or server? Server

13. The echo client is able to reach the echo server because the IP address and port are known a priori. How does the server learn the client IP address and port for echo responses?
    Server learns from the port specified on the packet sent by the client

14. What application data does the echo client send to the server and what is its length in bytes? 'x' value of 3rd command line argument

15. What application data does the echo server send to the client and what is its length in bytes? data sent by the client, amount of bytes of client's data

Sub-total: 20

Test Case 2:

Run the UDP Echo client only (no server) with a packet length of less than 100 bytes (say 10 bytes). Enable wireshark on the null/loopback interface and capture packets from client. Store trace in a .pcap file with an appropriate name e.g. udp-echo-test2.pcap.

16. What packet numbers correspond to the echo requests from client? 15,16,17

17. What is the IP address of the client? 127.0.0.1

18. What port is the client listening on? 58059

19. Do you see any messages reported in wireshark that appear to be responses to the client echo request? If yes, what are the numbers of such packets and what protocol does wireshark indicate they are running?

    No messages reported in wireshark that appear to be responses to the client echo request.

Sub-Total: 5

Total (25)

Submission Guidelines:
Please submit the following five types of individual files to Moodle by due date. **Please, NO zip files.**

- ✓ Submit the client and server source program files (please include name, UCID, section in comments at top of source files)
- ✓ Submit screenshots in .pdf format showing the trace output of the client and server and round-trip time results (be sure the .pdf is legible)
- ✓ Submit the README file (see README submission format on Moodle)
- ✓ Submit the wireshark .pcap file captured while running the client and server programs, and the one used to answer questions in this document
- ✓ Submit this Word document with completed questions

Also, please hand in a **paper copy** of this Word document in the first class on or after due date. Alternatively, please bring to my office (GITC 4411). If I am not available, slip under my door. Do NOT send email.

Program Grading Rubric: Total of 25 points

- Test case 1
  - Program reads 3 arguments as specified (3)
    - Server IP
    - Server port
    - Data length
  - Basic communication happens (8)
    - Client message sent and received by server
    - Server message sent and received by client
  - Client sends Echo request (2)
    - Format: String in encoded form
    - Length: as specified
  - Server responds with same data and length as received (2)
    - Format: String as sent by client
    - Length: as sent by client
- Test Case 2
  - Client sends 3 Echo Requests with timeout (6)
- Both Test Cases (4)
  - Client prints message as specified when sends message
  - Client prints message as specified when receives message (or timeout)
  - Server prints out message as specified when receives message
  - Server prints out message as specified when receives message

Academic Integrity
If academic integrity standards are not upheld, no credit is given. This includes copying of program or wireshark lab or .pcap file from any source, or hard-coding of results in your program.