

# CompSci-230: Homework 2

Due 6-February-2019, in pdf format on CANVAS.

*“A protocol stack (such as OSI), today is usually provided by the operating system (rather than as a separate library, for instance), it is a set of programs that allow processes to communicate over a network using the protocols that the stack implements.*

*The application programming interface (API) that programs use to communicate with the protocol stack, using network sockets, is called a socket API. Development of application programs that utilize this API is called socket programming or network programming.”*  
[https://en.wikipedia.org/wiki/Network\\_socket](https://en.wikipedia.org/wiki/Network_socket)

**Assignment** Create two programs  $S$  and  $R$  (Sender and Receiver) that, using **sockets**, transfer a short string from  $S$  to  $R$ . Even though the programs can run in the same machine, for this homework, they have to run in two different computers connected to the same network.

In the computer that runs either  $S$  or  $R$  install the Network Protocol Analyzer “WireShark” to monitor the packets sent/received to/from the network where  $S$  and  $R$  are running and identify/isolate the packets corresponding to the communication between  $S$  and  $R$ . Services, browser, and the OS send hundreds of packets to the internet and the local network constantly, therefore, you will need to use Source/Destination IPs to isolate and show only the list of packets associated with the communications between  $S$  and  $R$ .

For verification of feasibility, this exercise was carried out using a laptop with Ubuntu 17.10, and with Wireshark installed, and a MacBook running OS-X/ Both computers were connected to the same network, Ubuntu over wire and MacBook over Wifi.

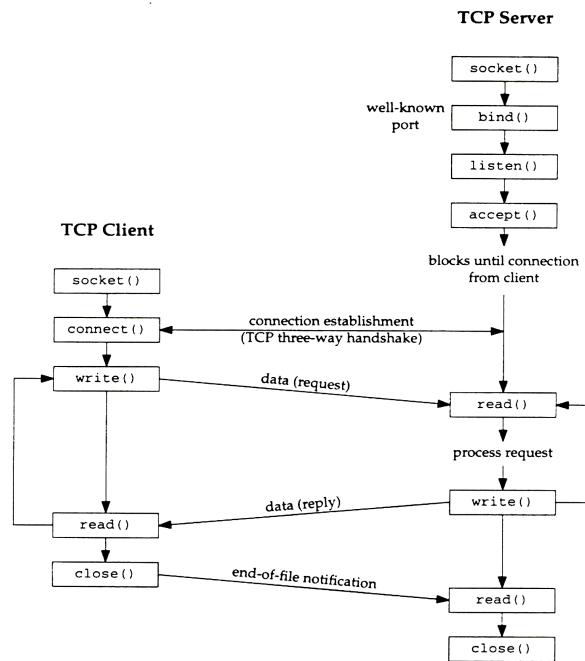


Figure 4.1 Socket functions for elementary TCP client-server.

After “Unix Network Programming” by W. Richard Stevens

**Report** Please submit an individual report that clearly explains the logic of your programs and includes a listing of your commented programs and the Wireshark's captured packets. For the packets sent by *S* and "sniffed" by Wireshark, identify the meaning and discuss the purpose of the following:

- What is encoded in bytes 0-5 and 6-11?
- What is encoded in, and what is the relationship between, byte 14 and the two bytes 16-17?
- What is encoded in bytes 18-19?
- What is encoded in bytes 20-21?
- What is encoded in byte 23?
- What is encoded in bytes 26-29 and 30-33?
- What is encoded in bytes 34-35 and 36-37?
- What is encoded after byte 65?

Finally, split the raw dump of bits associating each block of bits to the layers 2 (Link), 3 (Network), 4 (Transport), and 7 (Application).