COMP445 – Winter 2022
Data Communications & Computer Networks
Theoretical Assignment 2
Due Date: Friday, February 18th by 11:59PM

1. Explain why network applications only need to be written for the hosts they are running on despite needing to pass data through the network core to provide data communication services.

2. HTTP provides two connections methods: persistent and non-persistent. While there are clear advantages of persistent-HTTP, it is rather unclear whether non-persistent can be of any use. Find out why these two modes of connections are provided. Specifically, you should find out some of the advantages and disadvantages for each of them, hence justifying their concurrent existence.

3. Given what we know about transmission delay from Chapter 1 and the following:
   - A web client and a web server separated by one intermediary router.
   - Each link carries data at 1Mbps with an MTU of 8192 bytes
   - Each link is 1000 km long with a propagation speed of 250000 km/s
   - Zero processing and queueing delays
   - Connection management packets (packets used for opening a connection, confirming a connection and acknowledging receipt of information) contain no data and all packets have 125 bytes of overhead on top of any data they may contain.
   - The web client makes an HTTP request to the server that is 250 bytes long.
   - The requested data is 4 kilobytes in size with 500 bytes of overhead for the HTTP status and headers

   a.   What is the RTT to open the connection?

   b.   How long would it take for a web client to complete the request? You can ignore any time needed to close the connection.

4. Given what we know about the request-response nature of the HTTP protocol. Is it possible for a web server to provide data to a web client without the client making a request? How would a web application (such as a social media application) using HTTP be able to provide near real-time content updates?

5. Consider a local network with a 1 Gbps access link to the Internet. Hosts on this network are accessing resources with an average size of 2 MB from a distant server at an average rate of 50 requests per second.

   a.   What is the link utilization of the access link to the internet?

   b.   Suppose these requests were to go through a caching proxy server. What would the

link utilization to the internet be if half of all requests were served from the cache of the proxy server?

    c.   Suppose the proxy server could not serve any content from cache (due to the same resources never being needed for example.) Would this still provide any advantages to the end user? Would there be any disadvantages to the end user?

6. E-mail requires both sender and receiver mail servers to communicate directly. Further, all communications must be made between these two servers using SMTP.

    a.   Is it possible to allow intermediate servers as part of this communications? If so, what are the main advantages of doing so? If no, why is that infeasible, or what are the disadvantages of utilizing it if it was feasible?

    b.   Considering webmail, are there any cases when SMTP between the two mail servers can be replaced by HTTP? Explain why, or why not.

7. SMTP uses 7-bit ASCII for email messages which means that messages can only contain ASCII characters however email messages can contain binary data such as image and among other types of attachments which contain byte values outside the normal range of ASCII. How is this possible? Are there advantages or disadvantages to how this is done? Consider aspects such as protocol overhead and the presence of "legacy" systems in the network in your answer.

8. A successful attack to the Internet DNS would be devastating. Explain what type of attacks can be made towards DNS. Why, to-date, such attacks in practice have not been successful? In your answer, you should look at the role caching has and why such technique has not only proven to provide better performance, which is its original goal, but also protection against security attacks.

9. Regarding DNS and whois database:

    a. What is a whois database?

    b. Use various whois databases on the Internet to obtain the names of two DNS servers. Indicate which whois databases you used.

    c. Use nslookup on your local host to send DNS queries to three DNS servers: your local DNS server and the two DNS servers you found in part (b). Try querying for Type A, NS, and MX reports. Summarize your findings.

    d. Use nslookup to find a Web server that has multiple IP addresses. Does the Web server of your institution (school or company) have multiple IP addresses?

    e. Use the ARIN whois database to determine the IP address range used by your university.

    f. Describe how an attacker can use whois databases and the nslookup tool to perform reconnaissance on an institution before launching an attack.

g. Discuss why whois databases should be publicly available

10. Client-Server architecture can be used for file transfer; however, it is assumed/said to be inferior in comparison to P2P for such operations. Considering a small number of interacting hosts that need to share files, is it true that client-server would perform badly? Explain clearly your answer. You must indicate why the number of interacting hosts/peers is significant in determining whether client-server is suitable for file transfer.

11. BitTorrent uses a trading scheme referred to as tit-for-tat. While some researchers argued deficiencies in that scheme, others argued that if it was not for tit-for-tat, it is likely that BitTorrent would not even exist today. Explain both points of view. In other words, you should indicate the disadvantages of the scheme, as well as why it is still crucial to have such a scheme, or an alternative one, for BitTorrent to exist.

12. Suppose you are streaming your favorite video content from your favorite video provider. The video is playing at a high quality and then suddenly the quality drops for a few seconds without any noticeable gaps in playback. What could have caused this to happen? How did the video playing software handle this event?