ICSI 516 Computer Communication Networks, Fall 2018
Homework 2 – Application Layer
Due October 1st, 2018 11:59PM via Blackboard – (20 points)

Requirements and policies

Students should complete this assignment individually. Your turn-in is due on Blackboard. **Late submissions will not be accepted.**

Part 1: Fundamentals of the Application Layer

1. [3*points*] Consider the diagram in Figure 1. Let F denote the size of a file to be downloaded, d_i and u_i denote the download and upload speed of each of the four clients. Answer the following questions.

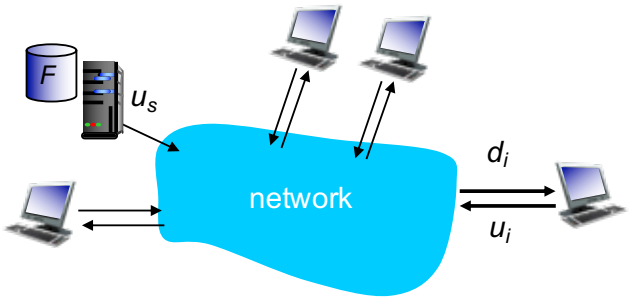

Figure 1: An application architecture diagram, in which a file F is distributed to four hosts, each of which has an uplink speed of u_i and downlink speed of d_i.

(a) [0.5*points*] How many times will the file F be uploaded by the server in a client-server architecture, assuming that all four clients want a copy of this file?

(b) [0.5*points*] Will there be any file exchange between clients in a peer-to-peer architecture?

(c) [2*points*] What factors limit the file distribution time in a client-server architecture? How about in a peer-to-peer architecture?

2. [4*points*] Consider a web page with $K = 10$ objects, each of which is $L_O = 1kB$ large. Assume that a client is requesting that webpage from a server, where the client and the server are connected as shown in Figure 2. The speed of the client-router link is $R_{CR} = 1Mbps$, whereas the speed of the router-server link is $R_{SR} = 10Mbps$. Small packets of size $L_R = 100B$ are used to establish reliable transport connections and to send the HTTP requests. Calculate the web response time for the above setup for the following scenarios:

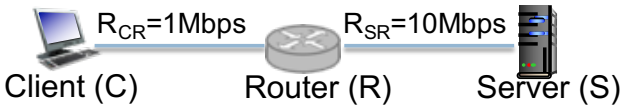

Figure 2: A network diagram of a web client and a web server connected by a single link. The speed of the link between the router and the client R_{CR} is $1Mbps$, whereas that of the link between the router and the server R_{SR} is 10Mbps.

(a) [1*point*] Non-persistent HTTP without parellelization.

(b) [1*point*] Non-persistent HTTP with parallelization of up to 10 connections.

(c) [2*point*] Persistent HTTP with pipelining of up to 10 requests.

3. [1*point*] How can web caches be used for improved user experience in remote and poorly connected areas? List one drawback of the use of Web caches.

4. [3*points*] In this problem we will use two practical tools (`whois` database and `nslookup`) to learn some facts about the network of UAlbany.

   (a) [1*point*] Use the `whois` utility installed on `csi516-fa18.arcc.albany.edu` to lookup UAlbany's domain `albany.edu`. What is the name of the registrar who manages our domain? How many authoritative DNS servers do we have? List their names. When was our domain registered? When is it going to expire?

   (b) [1*point*] Use `nslookup` from `csi516-fa18.arcc.albany.edu` to find a web server that has multiple IP addresses. List the name of that server and a few of the addresses it maps to.

   (c) [1*point*] Does the UAlbany web server have multiple IP addresses? What is(are) the IP address(es) of UAlbany's web server(s)? Can you infer who hosts our webpage based on its cannonical name?

5. [3*points*]In this problem we are going to use an ordinary Web surfing activity captured by Wireshark to examine the operation of DNS. You will first need to install Wireshark on your computer and familiarize yourselves with it. Use the lecture slides from class and supplement materials from the textbook available here `http://www.cs.albany.edu/~mariya/courses/csi516F18/papers/Wireshark_Intro.pdf`.

   Now that you are familiar with Wireshark you can use it to examine the operation of DNS. Open Wireshark and load the provided packet capture file dns-wireshark-trace-1 (available on Blackboard and on this URL `http://www.cs.albany.edu/~mariya/courses/csi516F18/hw/dns-wireshark-trace-1`). Enter "`ip.addr==128.238.38.160`" into the filter field. This is the IP address on which the trace was captured. This filter will hide all the packets that neither originate nor are destined to the capturing host. The packet capture was generated by opening a web browser and then visiting the webpage `http://www.ietf.org`. Once the page was loaded, the packet capture was stopped.

   Answer the following questions.

   (a) [0.5*points*] Locate the DNS query and the response message. Are they sent over UDP or TCP?

(b) [0.5*points*] What is the destination port of the DNS query message? What is the source port of the DNS response message?

(c) [1*point*] To what IP address is the DNS query message sent? Can you guess what kind of DNS server is this?

(d) [0.5*points*] Examine the DNS query message. What Type of DNS query is it?

(e) [0.5*points*] Examine the DNS response. How many answers does it contain? What are the answers Type and address fields?

Part 2: Research Papers

1. [2*points*] Consider the general operation of DNS. How can DNS be used for censorship? Comment on mechanisms to combat censorship inspired by the work of `[Duan+12]` "Hold On: Protecting against on-path DNS poisoning".

2. [2*points*] Consider the analysis of Maze in [Lian+12]. Discuss how Maze's incentive system predisposes collusion. What features did the paper consider for outlier analysis to discern colluding users?

3. [2*points*] Consider the analysis of servents and resource distribution in Gnutella presented in [Damiani+02]. What implications do these results have on P2P network design?