TECHNISCHE UNIVERSITÄT BERLIN
Fakultät IV – Elektrotechnik und Informatik
Fachgebiet Intelligente Netze
Julius Schulz-Zander
Susanna Schwarzmann, Marcin Bosk

4th Assignment: Network Protocols and Architectures, WS 20/21

Question 1: ($15 + 25 + 10 = 50$ points) *Relationship between bandwidth and window size*

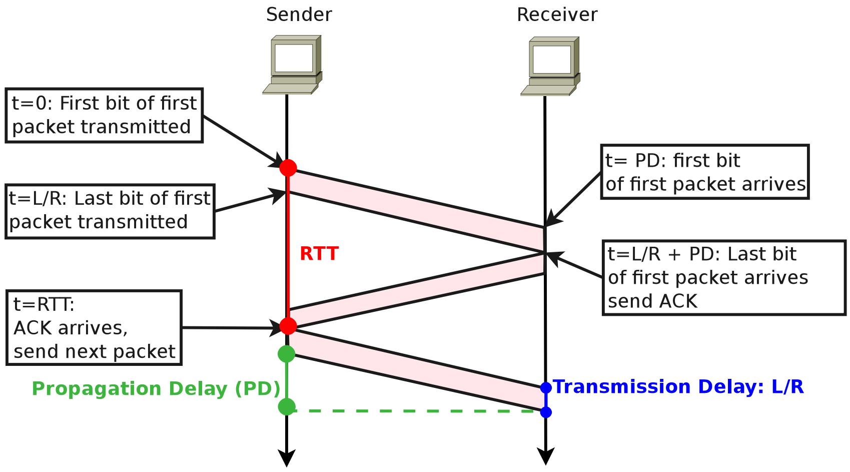

Figure 1: Types of Delay and Sequence plots: L is the length of the packet to transmit and R is the available bandwidth.

Assume a unidirectional data stream on a single link. Let the MSS[1] be of 536 bytes. For packets without payload (i.e., only TCP header, IP header, and Ethernet header, with no data carried within the TCP segment) of length $L = 40$ bytes, we have an RTT (Round Trip Time) of 60 ms. The RTT is defined as the time it takes from sending the first bit of a single packet until receiving the last bit of the corresponding ack. The transport protocol uses a static window size W (in bytes).

(a) Assuming a bandwidth of $R = 32$ Kibit/s, what is the propagation delay between sender and receiver?

Note: You can round to full milliseconds.

(b) Assuming the propagation delay remains the one computed in (a) and given a bandwidth of $R = 32$ Kibit/s, what is the window size maximizing the link utilization while still avoiding loss?

(c) Assuming the propagation delay remains the one computed in (a), how does the optimal window size (for maximum utilization) change if bandwidth increases?

Compute the optimal window size for (i) $R = 100$ Kibit/s, (ii) $R = 1$ Mibit/s, (iii) $R = 10$ Mibit/s.

Please turn!

[1] Maximum Segment Size, i.e., maximum number of bytes carried within a single TCP segment

Question 2: $(3 + 3 + 4 = 10$ points) *Parallelizing TCP Connections*

Assume a large file transfer from a server to a client. The server splits the file into $n > 1$ pieces and sends the pieces in n parallel TCP connections to the host.

(a) What is the **advantage** of using parallel connections **for the server**, rather than sending the whole file in a single TCP connection?

(b) What is the **disadvantage** of using parallel connections **for the server**, rather than sending the whole file in a single TCP connection?

(c) Assume that there are other TCP connections in the network, which are not between our server and client. How does using parallel connections between our server and client **impact the other TCP connections**?

Question 3: $(10 + 5 + 10 + 15 = 40$ points) *TCP Traffic Analysis*

This exercise will introduce you to traffic analysis techniques by examining TCP using a real connection. In order to complete the exercise, download a copy of Wireshark for your operating system from `http://www.wireshark.org/` and familiarize yourself with the tool[2]. Read about display filters and how to set them.

Perform the following experiments:

(a) In Wireshark, start a traffic capture on your local network interface.
Load the web page `http://researchvm.inet.tu-berlin.de/pics-10kb-4.html`.
Wait for 10 seconds, then stop the capture.
How many packets do you get in total?
How many of them contain TCP? (Hint: Use a display filter.)
How many of them[3] contain HTTP/1.1? (Hint: Use a display filter.)
Include the display filters you use in your solution.

(b) Now set a display filter to show only packets that correspond to **a single TCP connection** of your web page request and response.
Include the display filter you use in your solution and briefly explain what it means.

(c) Analyze the obtained data by marking packets belonging to:

- the TCP connection setup
- the transmission of the HTTP request,
- the transmission of the HTTP response
- the tear-down of the connection.

Include a **marked screenshot of Wireshark** in your solution.

(d) Start a new traffic capture and load the page `http://inet.tu-berlin.de`.
Set a display filter for DNS, and find the queries for `inet.tu-berlin.de`. What records does the browser ask for, and what replies does it get?
Click on one of the DNS replies, remove the DNS display filter again, and look at the packets coming afterwards to and from one of the IP addresses associated with `inet.tu-berlin.de`.
What TCP connections do you see? What can you see in them, and what can you not see? Why?
(No need for a screenshot here, if you can explain it in text.)

Due Date: Wednesday, December, 9th 2020 11.59 pm (end of day)

- **As PDF files (no MS Office or OpenOffice files)**, uploaded via ISIS:
`https://isis.tu-berlin.de/course/view.php?id=21979`
- Put the names and Student ID numbers (Matrikelnummer) of **all** your group members **and** the tutorial slot on your solution!

[2] On some Linux distributions, you may have to set capabilities in order to run Wireshark as non-root user, see `http://packetlife.net/blog/2010/mar/19/sniffing-wireshark-non-root-user/`

[3] Here you can just give the number of unencrypted HTTP/1.1 packets that you see. There may be more HTTP within encrypted TLS sessions, but you do not have to decrypt any traffic here. However, if you want to, feel free.