COMPSCI 314 S2 Assignment 2
2015

Department of Computer Science
The University of Auckland

*Carefully review the tutorial document before starting the assignment. This assignment contributes **5%** of your overall course mark.*

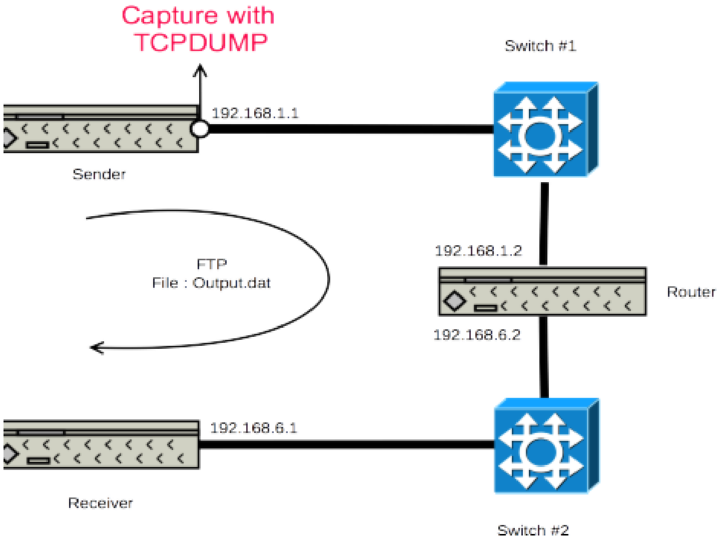
*Submit your assignment **as a single PDF file** to the **Assignment Drop Box**. Include all **workings** and **explanations**. Marks will be deducted for ambiguous solutions. Zero marks are awarded if the answers contain no explanation.*

***Assignment Drop Box:** (https://adb.auckland.ac.nz).*

***Due by:** 09:00 am, Friday 25 September,*

Departmental Policy on Cheating on Assignments:
See Assignments page of the course web site; cut-and-paste without acknowledgment of the source is not acceptable.

Background for this assignment:



For this assignment you are given a packet trace file captured from a testbed network, as shown in the diagram above. In this network there are two hosts (*Sender* and *Receiver* in the diagram), connected using 10 Gb/s links via a third host (*Router* in the diagram). The testbed network network also has two 10 Gb/s switches, but for this assignment these simply form part of the links to the router. The *Router* runs a network simulator program that allows it to introduce a delay and packet losses to the packets passing through it.

tcpdump, running on the *Sender* host, was used to capture packet traces for an FTP session that sent a large file from *Sender* to *Receiver*.

For this assignment you must first download your own trace file from this URL:
http://redsox.tcs.auckland.ac.nz/CWS/CourseWorkService.svc/cwm?cid=BinDispatch&cname=Wireshark314

That will give you a packet trace file with a name like Wireshark314-yuri123.pcap, where yuri123 is your Netaccount UPI. Save this file in your own file space, so that you can analyse it using Wireshark.

> *Note 1: You used Wireshark in 215, you are expected to be familiar with it.*
> *Note 2: If the download opens the trace file in Wireshark for you, you must save it from there.*

By default Wireshark will probably show relative sequence numbers for TCP. Change this to show absolute (i.e. as recorded for each packet) sequence numbers, using Wireshark's Edit |Preferences | Protocols | TCP page – you need the 'relative sequence numbers' box *unticked*.

Now answer the following questions ...

[Total: 35 marks]

A: The FTP Protocol [8 marks]

1. What well-known port number is used? [2 marks]
2. What usercode and password are used to log in to FTP? [2 marks]
3. Why is ftp mode switched to BINARY? [2 marks]
4. What FTP command is used to download the test file? [2 marks]

B: Data bytes transmitted by TCP [8 marks]

Set a Wireshark filter to look at all packets sent through the ftp-data flow:

5a. What well-known port number is used for FTP data? [1 mark]
5b. What are the packet and sequence numbers for the file transfer's opening SYN? [2 marks]
5c. What are the packet and sequence numbers for the ACK to the file transfer's closing FIN (i.e. the FIN from the FTP data sender)? [2 marks]
5d. How many actual data bytes were sent by the file transfer? [2 marks]
5e. What was the size of the transferred file? [1 marks]

C: Packets retransmitted by TCP [7 marks]

Set a Wireshark filter to look at packets with TCP source port FTP-DATA.

6a. How many packets are displayed using this filter? [1 mark]
Hint: Try Wireshark's Statistics | Summary

Set a Wireshark filter to look at packets with TCP source port FTP-DATA that were retransmitted.

6b. How many retransmitted packets does Wireshark display? [1 mark]

6c. How does Wireshark recognise a packet retransmission?
Hint: Use a search engine to find out about this. [3 marks]

6d. What is the observed packet loss percentage for this trace file? [2 marks]

D: Protocol overhead [8 marks]

Set a Wireshark filter to look at packets with TCP source port FTP-DATA.

7a. In question 5e you determined the number of data bytes transferred. How many bytes were actually sent during that transfer? [2 marks]

7b. What was the percentage of "protocol overhead" for that file transfer? [2 marks]

7c. What parts of the packets contributed to that overhead?
Note: your answer to this question must be a proper English sentence. An answer that is not a sentence will score zero marks.
Hint: "overhead" means everything except the actual data.
[4 marks]

E: Round-trip time [4 marks]

8. What is the most common Round-Trip Time (RTT) for packets from sender and receiver and back? [4 marks]
Hint: Try Wireshark's
Statistics | TCPStreamGraph | Round Trip Time Graph
You can drag the mouse to form a rectangle over any section of interest on that graph.
