COMP9121 Assignment 2 2024 S2

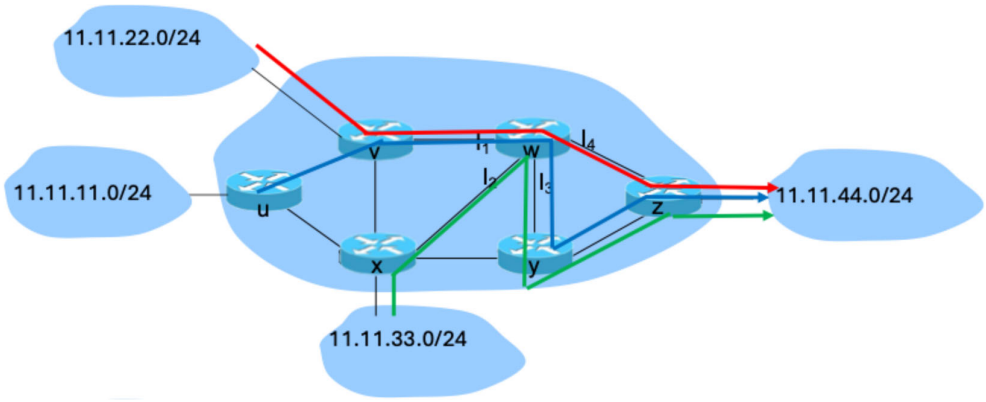
In this assignment, some questions are student number dependent; you will get zero in that question if you use another student's number.

The due date is 27 Oct 2024 at 23:59 and we will open the submission site on Canvas one week before the due date.

Submission instructions. In the "main file submission", you can only upload your answers in a single pdf file. In the "supplementary file submission", zip all your codes in a single zip file and submit. For Q9: you must submit your code; otherwise Q9 will not be marked. Q6: you must submit your code if you did any programming; otherwise your will not get full progress mark. This is one assignment with multiple pieces to submit. Your submission time equals to the submission time of the last piece. Late penalty will be calculated based on this submission time.

1. SDN.

In the following network, the network administrator should achieve the load balancing function: If the traffic is from 11.11.11.0/24 to 11.11.44.0/24, the blue path should be used; If the traffic is from 11.11.22.0/24 to 11.11.44.0/24, the red path should be used; If the traffic is from 11.11.33.0/24 to 11.11.44.0/24, the green path should be used;



(1) Can this load balancing function be achieved by traditional non-SDN routers? Why or why not?

(2) If SDN is used in the network, please specify the SDN switch table at w. The four interfaces (ports) of the SDN switch are labelled as I_1—I_4 respectively.

Please write necessary entries based on the following flow table format.

Ingress Port	Source MAC	Dest MAC	Eth Type	VLAN ID	Source IP	Dest IP	IP Protocol	Source Port	Dest Port	Action

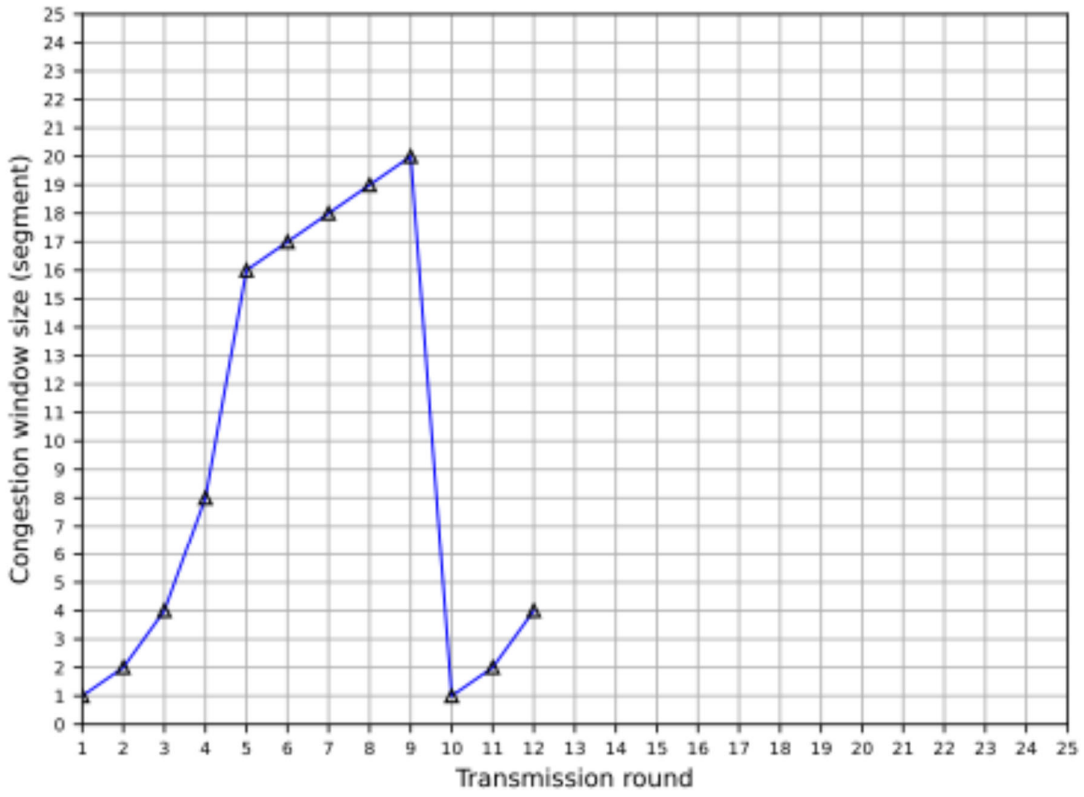
2. TCP

Consider the figure below. Assume TCP Reno is the protocol experiencing the behaviour, and the TCP session has a large number of packets to send. Answer the following questions (1)—(3). There is only one single TCP session in this figure.

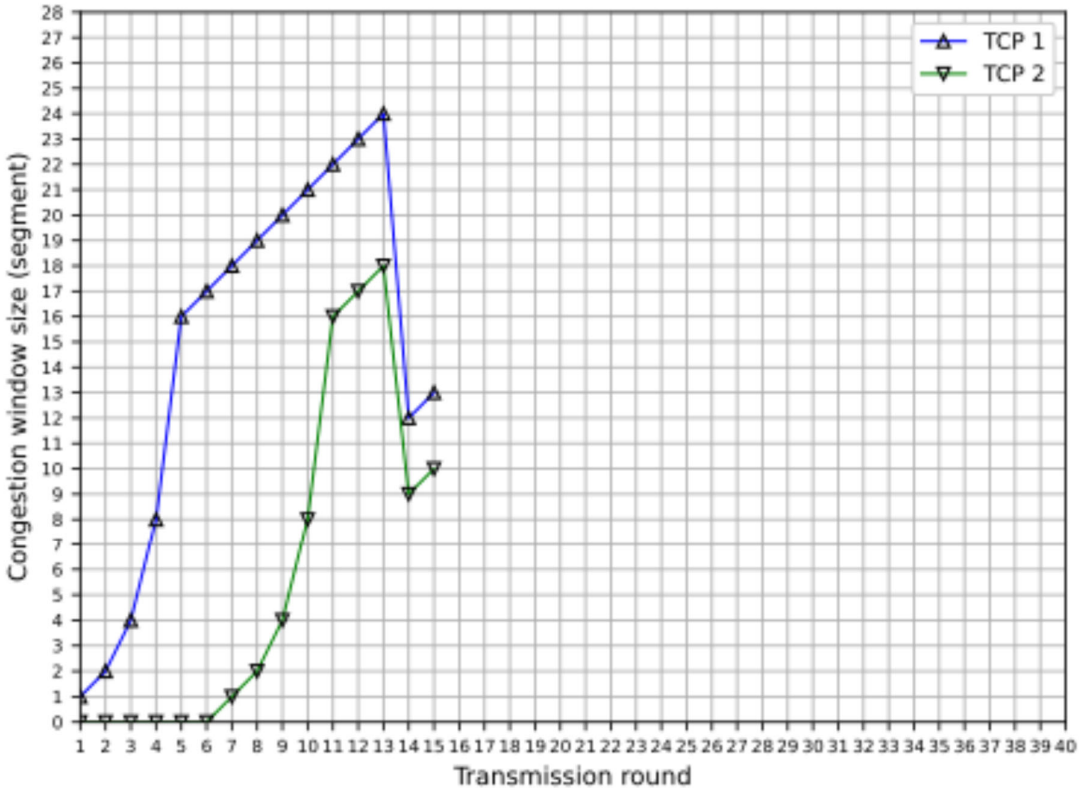
(1) The congestion window size is decreased to 1 (segment) at round 10. Is it caused by three duplicate ACKs or timeout? Why?

(2) What is ssthresh at round 1? Why?

(3) Suppose there is no packet loss after round 10. In the figure, what are the congestion window sizes from round 12 to round 25?



(4) In Figure below. Two TCP (Reno) sessions are sharing the same link and the link capacity is limited by 42 segments. Whenever the sum of the congestion window sizes reaches (or exceeds) 42, a packet is lost for each TCP session and the packet loss is detected by three duplicate ACKs. TCP session 2 starts later than TCP session 1. What are the congestion window sizes of the two sessions from round 15 to round 40? If the congestion window size is not an integer (in segment), you need to round it down.



3. Estimated RTT.

Consider the TCP procedure for estimating RTT. Let $EstimatedRTT_0$ = 100 ms be the estimated RTT when a TCP is initialised. Then, the TCP sender receives 5 ACKs and sample RTTs are measured as $SampleRTT_1$, $SampleRTT_2$, $SampleRTT_3$, $SampleRTT_4$, and $SampleRTT_5$. All of them are 110 ms. Let $EstimatedRTT_i$ denote the estimated RTT right after the ith ACK. We assume $\alpha = 0.125$ in this question.

(1) Calculate $EstimatedRTT_4$ and $EstimatedRTT_5$.

(2) Generalise your solution to n sample RTTs. The TCP sender receives n ACKs, with ith sample RTT $SampleRTT_i$. We assume all $SampleRTT_i$ are 110 ms. Express $EstimatedRTT_n$ as a function of n.

(3) For the formula in part (2), let n approach infinity. What is $EstimatedRTT_n$? Comment on why this averaging procedure is called an exponential moving average.

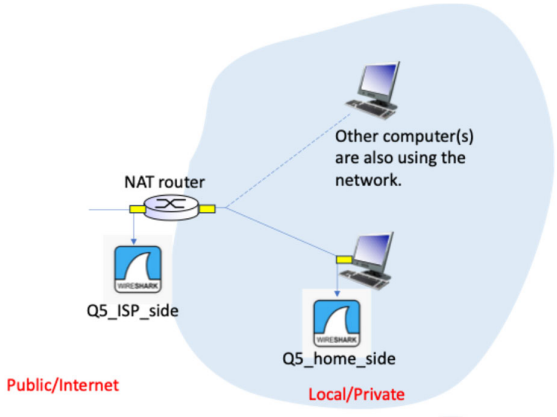
4. **HTTP and TCP.**

Client C requests a webpage from Server A. We assume that RTT between Client C and Server A is 10 ms. After obtaining the main page, Client C finds that there are 2 objects to be fetched. Both objects are also in Server A.

Client C starts to request for object 1 when the main page has been successfully downloaded. It starts to request for object 2 when object 1 has been successfully downloaded. The size of the main web page is small. It fits into 1 TCP segment. Each object fits into *n* TCP segments, where *n* is the last 3 digits of your student number plus 1000. For example, if you last three digits are 123, then *n* = 1123. We have ssthresh=64 segments at the beginning of a TCP session. *Non-persistent HTTP is used*. TCP termination delay is ignored. There is no packet loss.

How long in total does it take for Client C to successfully obtain the webpage (including the main page and two objects).

Q5. Wireshark (NAT). In this question, we investigate packets of one client PC in a home network. The PC is communicating with a remote server. The home network router provides an NAT service. The figure below shows our Wireshark trace collection scenario.



We collected Wireshark trace file (you can find them at modules – assignment 2) on the client PC in the local home network. The file is called Q5_home_side. Meanwhile, we also collected a second trace file at the interface of the home router connecting to the public Internet, as shown in the figure above. The file is called Q5_ISP_side.

(1) Use the trace files and investigate them carefully. Please write down the NAT translation table entries in the NAT router for the traffic you can find in Q5_home_side and Q5_ISP_side. Find as many entries as possible. For each entry, please give screenshots to justify your answer. (If your table has more than 5 entries, just give the screenshots for the first 5 entries in your table.) Please note that some other computers are also using the local network, and their traffic may also appear in Q5_ISP_side but not in Q5_home_side. You should ignore them when you figure out the NAT translation table.

(2) What is the MAC address of the client PC? What are the MAC addresses at the two interfaces of the NAT router? Please give you screenshots.

6. P2P. A server distributes a file with the size of 10^9 bytes to n hosts. The upload rate of the server is 3.5 Mbps. The i-th host (i = 1,2,…,n) has a download rate of 0.5i Mbps. For all hosts, the upload rate is 1 Mbps. Calculate the minimum distribution time as a function of n for P2P distribution and client-server distribution, and plot the two curves. (n = 1,2,…,100). You should submit your code if you did any programming to complete this task.

7. Cross layer: Routing, UDP/TCP, DNS/HTTP

Consider the network shown below. In the figure, AA is the Authoritative DNS server for Web Servers A and B, and LC is the local DNS server for Client C. Client C wishes to see a webpage on Server A. The IP address of Server A is not cached in the client. The address resolution is done iteratively, i.e., all levels of DNS servers (root, TLD, and AA) should be consulted.

Assume that the one-way delay through each link inside AS1, and one-way delay through each AS outside AS1 is labeled in the figure, in ms. We assume that all dashed links have zero delay. For example, the one-way delay from Router C to AA is 30 ms. The one-way delay from Router E to Root via AS4 AS5 is 45 ms. OSPF routing protocol is used within AS1 (link cost is equivalent to one-way delay inside AS1). BGP is used among the ASes.

After resolving the IP address, Client C can visit Server A. After obtaining the main page, Client C finds that there are 2 objects to be fetched. One object is stored in Server A, but the other object is stored in Server B. Unfortunately, Client C does not know the IP address of Server B, so that Client C has to resolve the IP again.

The size of the main web page is small. It fits into 1 TCP segment. Each object is also small and fits into 1 TCP segment. No packet is lost. Persistent HTTP is used.

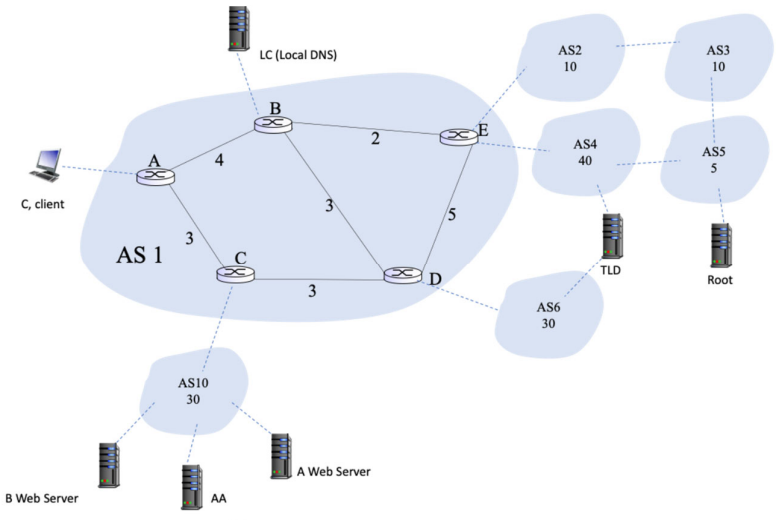
Assumption 1: All inter-AS paths are allowed, and these inter-AS paths have been known by all routers in all ASes.

Assumption 2: All levels of DNS servers should be consulted iteratively for address resolution.

Assumption 3: Client C starts to request the IP address of object 2 when object 1 has been successfully downloaded.

Assumption 4: TCP termination delay is ignored.

Question: How long in total does it take for Client C to successfully obtain the webpage (including: DNS of main paper, download of main page, download of object 1, DNS of object 2, and download of object 2).



Q8. RSA. Use RSA algorithm to answer the following questions. You should use decimal numbers instead of binary numbers in this question. Correct solution is not unique.

(1) Select proper values of p and q, larger than 10 but less than 20. Then, calculate n and z.

(2) Select proper values of e and d. Then, encrypt the last two digits of your student number.

(3) Decrypt your answer for Part (2), and verify if the last two digits of your student number can be recovered.

(4) Trudy (the intruder), eavesdropped on the encrypted number and the public key (n, e), how can she decrypt the number in this example? In reality, p and q value are very large numbers; if Trudy eavesdropped on the encrypted number and the public key, can she still decrypt the number? Why or why not?

Q9. Hash. In this question, we aim to use SHA384 hash algorithm to find the nonce of the following magic sentence so that the hash has 6 leading zeros (24-bit zeros) in the beginning. Easy Python programming (less than 15 lines) will be needed in this question.

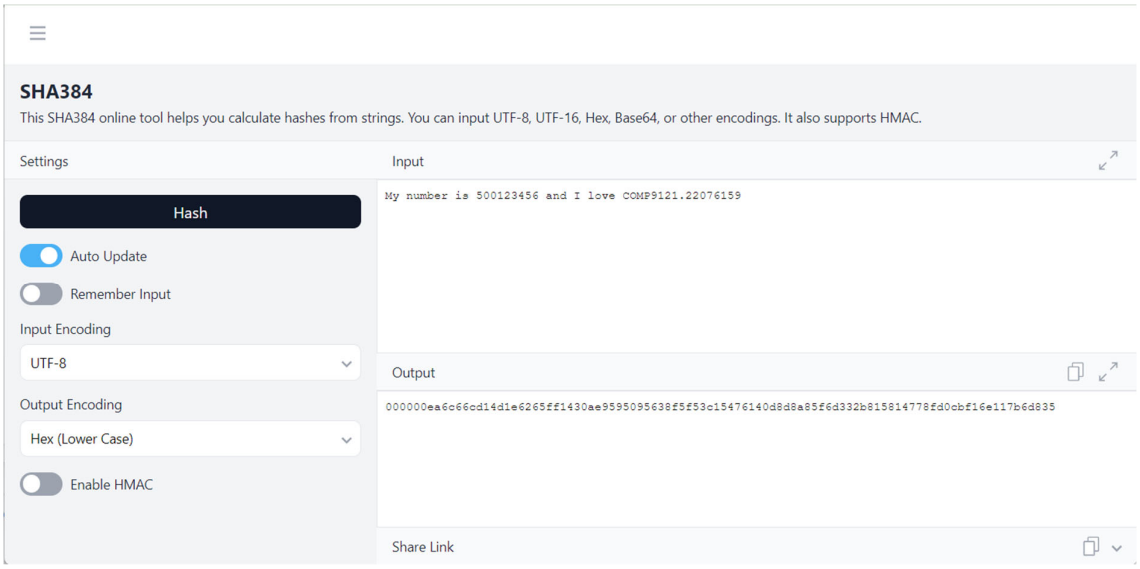
Magic sentence:

*My number is ******** and I love COMP9121.########*

Here ******** indicates your student number (so this should be different for everyone) and ######## is the "nonce" you need to find. ######## is a string, which can be with any length. For example, the magic sentence below is the outcome (the answer is not unique). Please note, there is no limitations on the length of the nonce.

My number is 500123456 and I love COMP9121.22076159

You can verify it at many websites, such as, https://emn178.github.io/online-tools/sha384.html, where you can see that the hash has 6 zeros in the beginning.



Please note that in the "input" in the above screenshot, there should be no carriage return or line feed. Otherwise, the hash will be different.

You need to use Python3 to find a nonce. (Since the answer is not unique, you only need to find one answer.) You may use hashlib and use a correct function in this library. For example, the following program will generate SHA384 of "*My number is 500123456 and I love COMP9121.*"

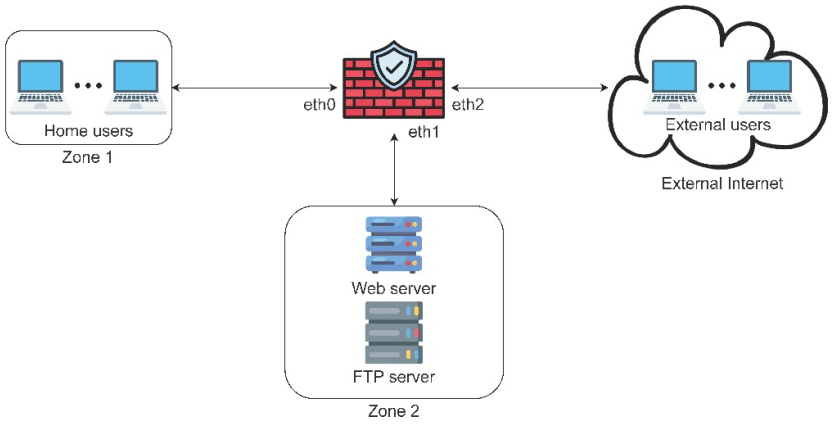
```
import hashlib
s="My number is 500123456 and I love COMP9121."
s=bytes(s,'utf-8')
hashresult=hashlib.sha384(s).hexdigest()
```

(1) Write down your magic sentence and submit Python 3 code as supplementary material.

(2) How long does it take to find the nonce?

(3) In this case we find the nonce generating for 6 leading zeros. Comment on what will happen if you are required to find a nonce that generates a hash with 20 leading zeros. (This is what miners of bitcoins should do!)

10. Firewall. We will develop the firewall configuration. The figure below shows the configuration we want to achieve. The home users reside in Zone 1. The external users reside in the External Internet. A Web server (111.111.11.1) and an FTP server (111.111.11.2) are located in Zone 2. The Web server supports both http and https requests.



The security policy is as follows:

1) The home users can freely access any Web service, anywhere, but only if they initiate the connection themselves.

2) The home users and the external users can establish the telnet session with each other.

3) Everyone (home users and external users) can access the web server in Zone 2.

4) Only the home users can access the FTP server in Zone 2.

5) Block all other incoming and outgoing traffics.

Complete the table to define a stateless firewall configuration for the given scenario. You can refer to the IP ranges (source and destination) by their "zone name". Use "Ext" to indicate external Internet. Use "*" to indicate "all".

Interface	Source IP	Destination IP	Source Port	Destination Port	ACK	Action