Networks Laboratory (CS39006)
Lab Test-1, Spring 2020-21

Full Marks: 40
Time: 2 Hours(2:00-4:00 PM)

Note (Read very carefully):

1. You need to submit your code in Moodle by the deadline. Any submission over email will not be accepted. In case you have a network problem, call Bishakh (+91 8250923465) or Soumyajit (+91 80180 34218) **before the submission deadline only**. They will guide you about the next steps. We'll not entertain any form of communication regarding the lab test after the deadline is over.

2. Cases of plagiarism will be treated very strictly. You should solve the problems yourself and submit the same.

3. Make yourself available till 5:00 pm (in Microsoft Teams) after the test is over. TAs may call you and ask you to explain your solution. We'll call a few students randomly. Don't worry if you don't receive a call. Your assignment will be evaluated.

4. In case you are not able to explain your solution, you'll be awarded zero marks. We have partial marking, so whatever you submit, do it yourself without taking other's help.

5. Follow the submission procedure exactly as instructed within the questions. If you do not follow the same, your submission will not be evaluated. The submission instructions are highlighted in blue text.

6. You can submit two files in Moodles. Submit the solutions of Question 1 and Question 2 as two separate files in Moodle, following the submission instructions for individual assignments.

7. If you have any assumptions, write them down clearly in your solution within comments. No queries will be entertained during the exam hours. We believe that the questions have sufficient details; therefore, you should assume something only if it is absolutely necessary. Unnecessary assumptions might result in a deduction of marks.

Question 1

[20 marks]

Following is the link of a pcap trace file. Download it and analyze it to answer the following questions.
https://drive.google.com/file/d/1rzL3ctv0wjjbnpUeuWDlEbFTkC2vV6ZV/view?usp=sharing
(To save time, keep on solving the second problem, while the pcap is getting downloaded. The pcap is of ~6.0 MB, so should not take much time to download unless your network is very slow).

a. Analyze the pcap file using Wireshark and answer the following questions --
   i. Using Wireshark, filter the relevant packets for emails using display filters. Take a screenshot of your entire desktop showing the filter and the filtered packets (partial view of the filtered packets is okay), and name the screenshot image as 1_a_i.png. **[2 marks]**
   ii. Follow the TCP streams for each email (actual mails) using the “Follow” option of Wireshark, take a screenshot as earlier. Name the screenshot images as 1_a_ii_<email count>.png where <email count> indicates the individual emails. For example, if there are 3 emails, then the three images will br 1_a_ii_1.png, 1_a_ii_2.png, and 1_a_ii_3.png. **[2 marks]**
   iii. Count the total number of packets corresponding to SMTP. Write that value in a text file, explain how you have counted the number of packets. Name that text file as 1_a_iii.txt **[2 marks]**
   iv. Extract the source and destination IP addresses and ports for the SMTP Requests. Write them in a text file. Also write down the procedure that you have used to extract the source and destination IP addresses. Name the text file as 1_a_iv.txt **[2 marks]**

   Put all the image and text files in a folder named **1_a**. Proceed with Part b as instructed next.

b. Use tshark tool to extract only the SMTP packets from the pcap file and generate a final filtered XML file with SMTP packets only. Write a python script to extract the following information from the XML file --
   i. How many emails have been sent in this entire communication? **[1 mark]**
   ii. Extract the sender and receiver email addresses for each email. **[4 marks]**
   iii. Extract the subject of each individual email communication. **[2 marks]**
   iv. Extract the mail body for each individual communication. **[5 marks]**

The script should have proper comments, in case you are using any special package then refrain from adding the installation code in the script. Instead, mention the package name and installation command as comments.

Name the python script as 1_b.py. Now, create a folder named <Your Roll Number>_Q1. For example, if your roll number is 17CS30099, then the folder name will be 17CS30099_Q1. Put the previous folder 1_a and the python script 1_b.py within this folder. Compress the folder in zip format (not tar.gz or any other format) and submit. Note that the name of the zipped folder will be 17CS30099_Q1.zip if your roll number is 17CS30099.

Question 2

[20 marks]

Write a shell script to create a virtual network topology as in Fig 1.

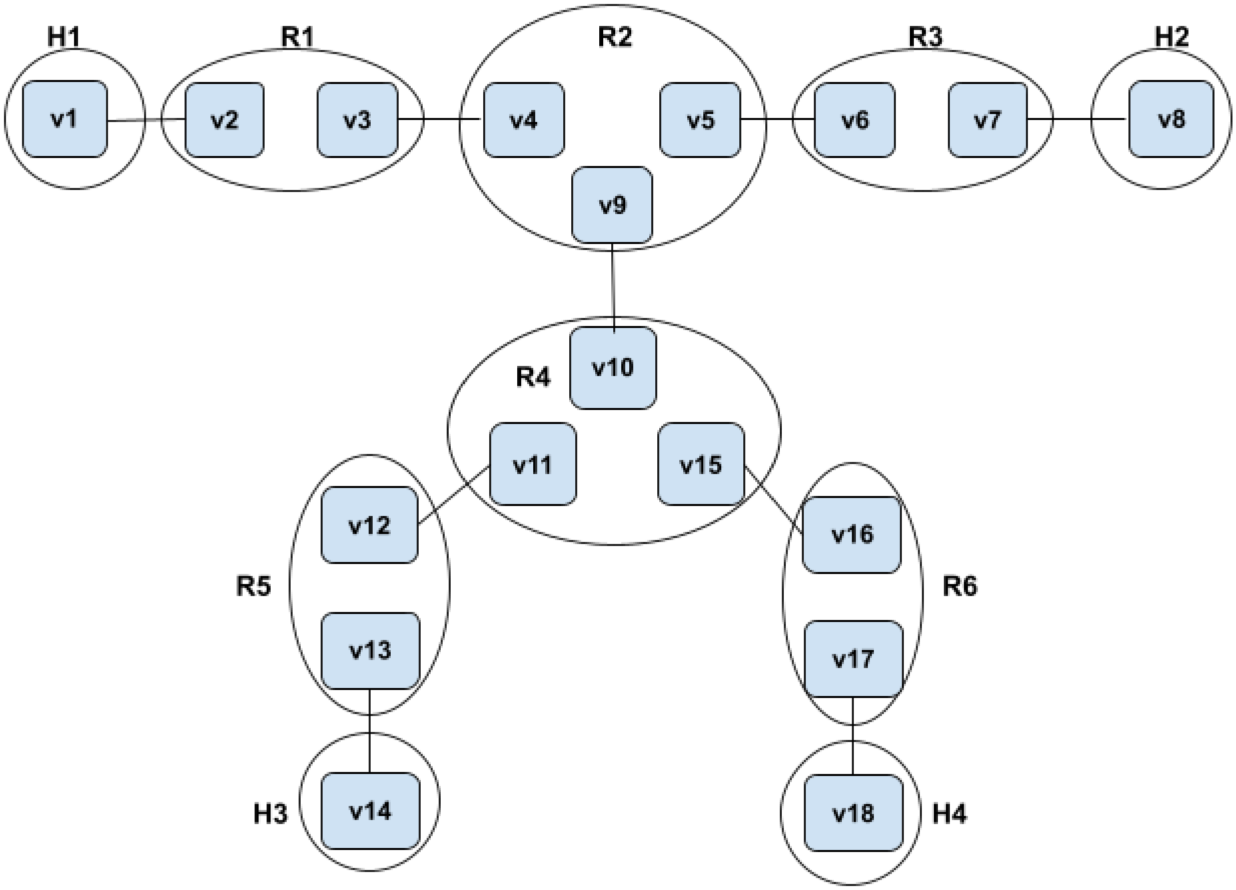

Fig 1.

Here H1, H2,… , R1, R2,…, are network namespaces and they are connected using virtual ethernet interfaces v1 …. v18:

Assign ip address to the interfaces as follows:

v1: 10.10.10.X/24
v2: 10.10.10.X+1/24

v3: 10.10.20.X/24
v4: 10.10.20.X+1/24

v5: 10.10.30.X/24
v6: 10.10.30.X+1/24

v7: 10.10.40.X/24
v8: 10.10.40.X+1/24

v9:   10.10.50.X/24
v10: 10.10.50.X+1/24

v11: 10.**20**.10.X/24
v12: 10.**20**.10.X+1/24

v13: 10.**20**.20.X/24
v14: 10.**20**.20.X+1/24

v15: 10.**30**.10.X/24
v16: 10.**30**.10.X+1/24

v17: 10.**30**.20.X/24
v18: 10.**30**.20.X+1/24

Where X is the last two digits of your roll number.

Configure all the required routes so that all interfaces (irrespective of network namespace) can be pinged from every namespace.

Use the sysctl command to set net.ipv4.ip_forward=1

Enable loopback interface to allow to ping a namespace's own interfaces.

Use traceroute to show the hops from:
1) **H1 to H4**
2) **H3 to H2**
3) **H4 to H3**

[15 marks]

Explain the routes that you are adding. Write down your explanation within your script in comments.

[5 marks]

Name this shell script as <Your Roll Number>_Q1.sh. Submit this shell script in Moodle.