Packet capture

1. Project Description

1 Packet capture problem

Consider a network of three machines as shown below:

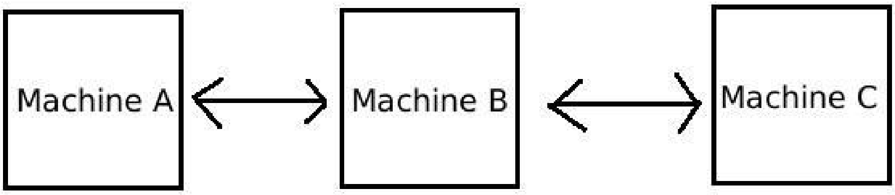

Figure 1: Machines A, B and C

In such a case write programs for machines A, B and C to perform following operations:

1. Write a program for machine A which captures ping packets going from current machine to any destination and send a copy of these packets to machine B. While sending to machine B, change only destination MAC address to machine B's MAC ID and keep everything else same.

2. Write a program for machine B which capture incoming ping packets from machine A and forward them to machine C. While forwarding ensure that destination IP of ping is changed to machine C's IP address.
   Also change other fields to indicate the ping request is coming from machine B and intended for machine C.

   Further the program running on machine B should capture replies coming from machine C and send them back to machine A. While sending replies back to machine A, again put correct source address in reply as was present in the query.

3. Write program for machine C which captures incoming ping requests and counts number of ping requests received from various source IPs. The program should be able to provide statistics related to ping with respect to source IPs.

1.1 Example packet flow

1. Machine A sends ping to 10.10.10.10
2. Program on machine A captures ping request for 10.10.10.10 and send it to machine B.
3. Machine B receives ping request for 10.10.10.10 from machine A. Machine B changes various details and forwards the request to machine C, such that machine C feels this is the ping request from machine B to machine C.
4. Machine C program captures ping request and adjusts various counters for statistics. So far machine C has received one ping request from machine B's IP.
5. Machine C OS should reply to machine B's ping request without us having to do anything about it.
6. Program on machine B when it receives reply from machine C, should capture it. The same reply should be modified to make it look like reply coming from 10.10.10.10 to machine A. This reply should then be sent to machine A.
7. Program on machine A should receive ping reply from 10.10.10.10 even though no such machine exists on network.
8. Program on machine C should be able to give statistics on how many such false replies have been sent by this mechanism.

Please note that if everything is setup as mentioned in the question then machine A should be able to ping any possible IP and should get reply. Also in case ping request is for genuine machine which is connected to machine A, then machine A might receive two replies for one request.

2. Inputs

The command line will specify the following parameters :

Input for Machine A program.

```
% ./machine_a <details of machine b - IP, MAC>
```

Input for Machine B program.

```
% ./machine_b <details of machine a - IP> <details of machine c - IP>
```

Input for Machine C program.

```
% ./machine_c
```

3. Output

Output for machine C - Statistics related to ping with
respect to source IPs.

5. What to submit?

A single zip file containing

--> Source files, compiled executable
--> Makefile (If required)
--> README file that explains how to compile and run the program; whether your program works correctly or whether there are any known bugs/errors in your program.

6. Grading

--> Correct implementation:
--> Viva voce

7. Policies

--> Penalties will be there for any form of academic dishonesty, plagiarism, etc. There should be no downloaded code.
--> Software for checking plagiarism of the code will be used (MOSS).
--> You can do this assignment in groups of two.
--> The program can be written in C/C++/Java.