Lab 3

(Due your class day June 2/7)

Note: in all the lab questions, please include the screen shots as evidence of your solutions.

1. In this problem, you will get familiar with ip format. Start the Wireshark and run

ping www.mit.edu

and then stop Wireshark. Ping **www.mit.edu** is to send an icmp packet. Check the first **ping request** packet in the Wireshark window and answer the following questions.

a. Look at the ip header, what is the source and destination ip address?

b. What is the upper layer protocol in ip header?

c. what is the ip header length?

d. Calculate the payload length for ip packet. This is **totallength** - **headerlegnth**.

e. what is the TTL value and what is its meaning?

f. find out which field shows the ip header is in ipv4 or ipv6 format.

2. Start Wireshark on your VM. Next, run command **sudo dhclient -r -v** and then **sudo dhclient** and finally stop Wireshark. Command **sudo dhclient –r –v** will release your current ip address. Then **sudo dhclient** will execute the DHCP protocol. Use packets in Wireshark from executing DHCP to answer the following questions.

a. Confirm that the transport layer protocol of DHCP protocol is UDP. To do this, check a packet with DHCP protocol data and look at the transport layer header. Think about why it is not TCP (recall that TCP needs to establish a connection before exchanging messages).

b. What is client port # and what is server port # in the DHCP discovery packet?

c. Before the IP address is granted, the client has to use something to identify message

destined to it. What is transaction ID in the discovery packet in your Wireshark

d. What are the src IP, dest IP, yiaddr, transaction ID and lifetime in the offer packet

e. What are the src IP, dest IP, yiaddr, transaction ID and lifetime in the request packet

f. In addition to offer the ip address to your computer, DHCP can in fact provide you more useful configuration. Check DHCP **offer packet** to find out the following information.

DHCP server IP: you need this to extend your time to use the current IP address.

Subnet mask: this tells you the subnet type.

Router IP: That is the ip address your outgoing packet will first go to.

DNS IP: this is the ip address of the DNS server that you will request to resolve your DNS query. That is, this is your **local** DNS server.

3. In this exercise, you will look in the arp protocol execution. First, run **arp** to find out the list of records in the arp table. Next, start your wireshark and run **sudo arp -d *routerIP*** to delete the record of *routerIP*. Here routerIP is the **Router IP** obtained in the previous DHCP experiment. Then, you should see your VM is now starting to run arp.

a. Find our arp broadcast from your VM. What is the upper layer protocol in the link layer header? What is the broadcast MAC address? What is the ip address for which your broadcast message is intended to find out the MAC address?

b. look at the response packet for the ARP query. What is the ip address of the sender? What is its MAC address?

4. Run wireshark and access www.example.com and stop Wireshark. Answer the following questions.

a. Check the HTTP request packet to 93.184.216.34 (ip of www.example.com). What are the source MAC and destination MAC? You need to check the link layer header in the packet. The source MAC is the MAC of your VM.

b. Does the destination MAC in **a** belong to 93.184.216.34? To find out your answer, run command **arp** to check the arp table of your VM. Is the destination MAC in **a** listed here? If yes, confirm that this MAC does not belong to 93.184.216.34 and instead belong to your router.

c. In the upper protocol field of link layer header of your HTTP request packet, what is the value? What protocol does it represent?

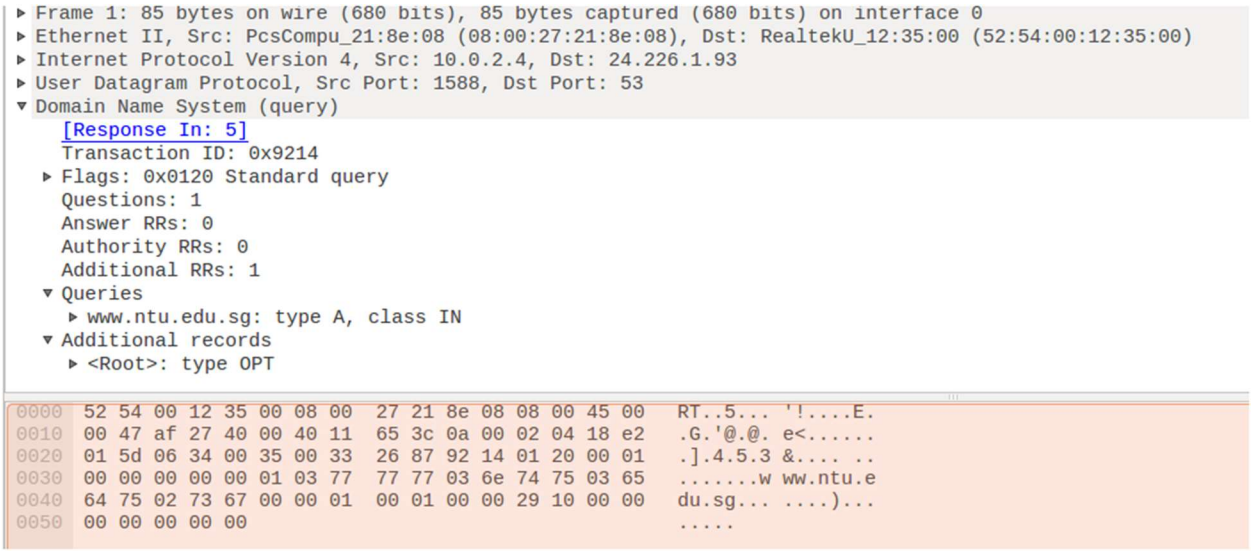
5 (optional) In this experiment, you will feel how NAT is working.

First, run Wireshark on your host operating system (which is Windows on my computer). If you have not installed it, go to https://www.wireshark.org/ .

Second, run Wireshark on your VM.

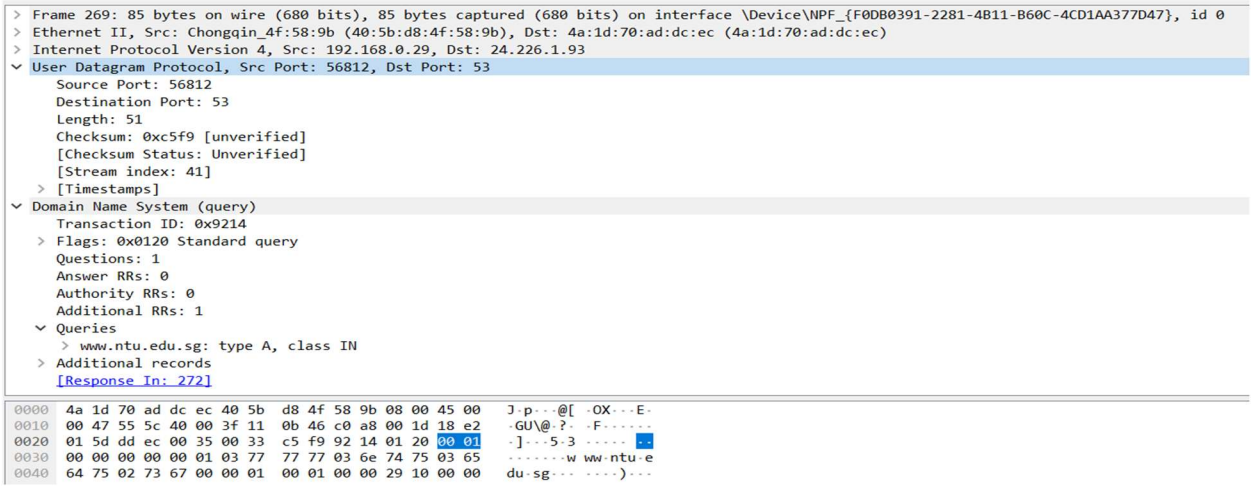
Third run dig www.ntu.edu.sg (or any hostname you want) and then stop both Wiresharks.

Check your DNS query packet on VM Wireshark. Here is my screen shot.



We can see that the source port is 1588 and source IP is 10.0.2.4. The destination port and destination Ip are respectively 53 and 24.226.1.93. The query is www.ntu.edu.sg.

Then, we find the same query on the Host OS Wireshark. Here is the screen shot.



Now we can see that the source port # is now 56812 and source IP 192.168.0.29 is the IP of the host OS. The destination IP and destination port are still respectively 24.226.1.93 and 53. From the above two figures, we can form a NAT record at the VM router 10.0.2.1:

(10.0.2.4, 1588) < ----- > (192.168.0.29, 56812).

In this experiment, you provide two screen shots as I have done here and also create your NAT record.