Lab 6

Objectives:

- gain insights into the operation of NAT

Prerequisites and Links:

- Week 8 and 9 Lectures
- Relevant Parts of Chapter 4 and Chapter 5 of the textbook
- Introduction to tools of the trade
- Basic understanding of Linux. A good resource is here but there are several other resources online.
- NAT_home_side.pcap
- NAT_ISP_side.pcap

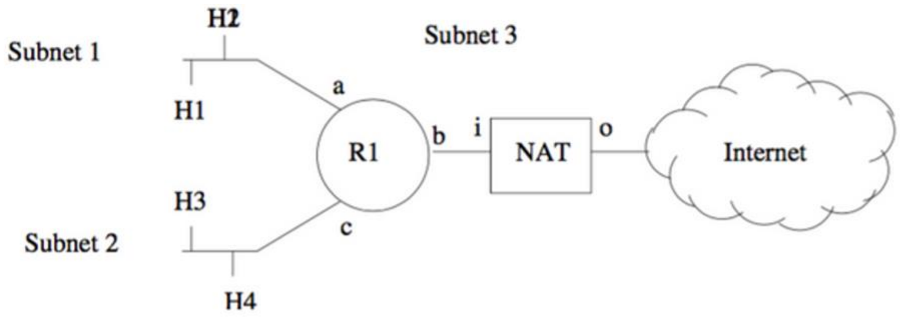
Questions to be marked: Exercise 1, Question 3, 2) Exercise 2, Question 9, 3) Exercise 2, Question 13

- Each lab comprises of a number of exercises. Not all the exercises for each lab are marked. Only those marked with (*) and written in bold will be marked.
- We expect the students to go through as much of the lab exercises as they can at home and come to the lab ready.
- Please attend your allocated lab and show/explain the answers of the marked exercises to your tutor.
- If lab exercise involves diagrams or plots, you require to show them to the tutor as well.
- Please make sure you **sign the marking form** once the tutor marked your lab. Signing this form implies that you agreed on the mark you received.
- There are 7 labs during this course. For each student, the 5 best performing labs will contribute to your final lab mark.

Marks: 4 marks

Exercise 1) Revision of IP Addressing, NAT

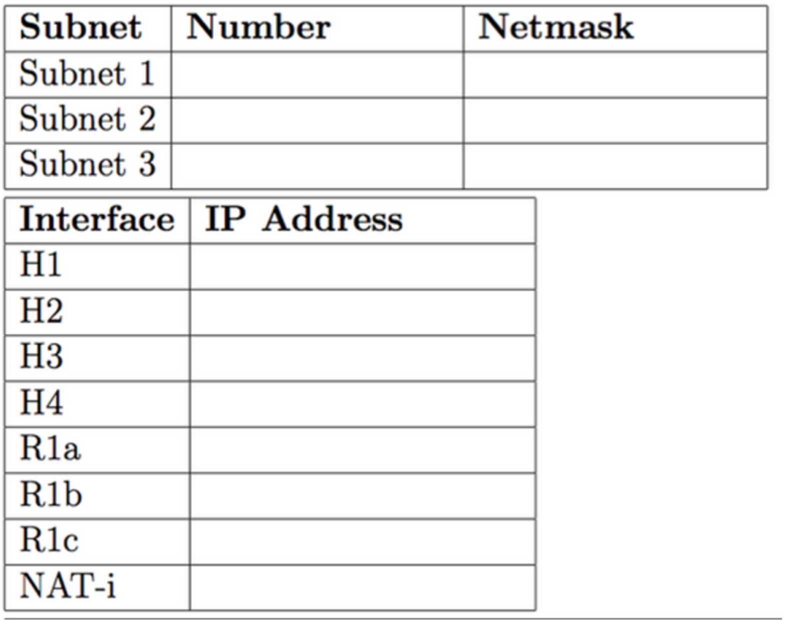
Elliot Alderson runs a large network at his house and wants to subnet it to separate his work computer from the network that controls his connected lights and door lock. He purchases a NAT box, and divides his network as follows:



His ISP has given him an IP address that he assigns to NAT-o (the outsider or "o" interface on the box). Elliot did not do very well in COMP3331/9331 but knows that RFC1918 specifies three different address ranges that he could use for private addresses inside his home:

- 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

Question 1: Your job is to help Elliot assign addresses to the subnets, routers and NAT box inside his house. Use addresses from the 10.x block. Complete the following tables:



Subnet	Number	Netmask
Subnet 1		
Subnet 2		
Subnet 3		

Interface	IP Address
H1	
H2	
H3	
H4	
R1a	
R1b	
R1c	
NAT-i	

Question 2: Give one reason why wide-spread deployment of IPv6 would let Elliot get rid of his NAT device.

(*) Question 3: Give one reason why Elliot might want to continue using his NAT device even if he could transition to IPv6. (1 mark)

Question 4: Assuming that the NAT box has no special support for any protocols, and merely translates TCP and IP ports and addresses, give an example of an application that would not work through this NAT, and very briefly explain why.

Exercise 2: Understanding NAT using Wireshark

We have provided you with two Wireshark trace files: NAT_home_side.pcap and NAT_ISP_side.pcap

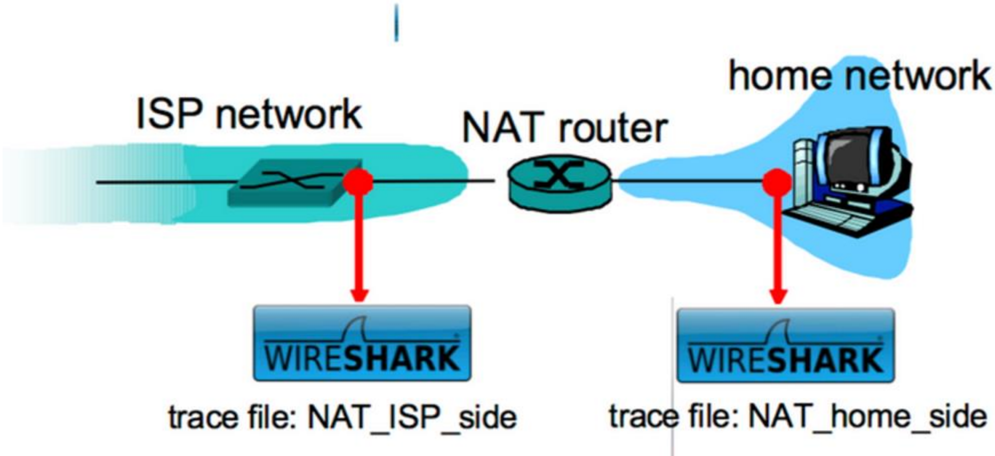


Figure 1: NAT trace collection scenario

The traces together captures the interaction between a web browser on a client machine in the home network and the www.google.com servers in the public Internet.

The measurement scenario is outlined in Figure 1 above. The NAT_home_side trace captures packets sent to/from a client machine in the home network and the LAN-side interface of the NAT router. The NAT_ISP_side trace captures the traffic exchanged between the WAN-side interface of the NAT router and the first hop (i.e. gateway) router in the ISP network.

Step 1: Open the NAT_home_side trace and answer the following questions. You might find it useful to use an appropriate filter (e.g. "http") so that only frames containing HTTP messages are displayed in the trace file.

Question 1: What is the IP address of the client?

Step 2: The client actually communicates with several different Google servers in order to implement “safe browsing.” (See Question 15 at the end of this exercise). The main Google server that will serve up the main Google web page has IP address 64.233.169.104. In order to display only those frames containing HTTP messages that are sent to/from this Google server, enter the expression “http && ip.addr == 64.233.169.104” (without quotes) into the Filter: field in Wireshark .

Question 2: Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

Question 3: At what time is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

NOTE: To answer the next two questions you will have to change the filter that was set in Step 2. If you enter the filter "tcp", only TCP segments will be displayed by Wireshark.

Question 4: Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? What are the source and destination IP addresses and source and destination ports for the TCP SYN segment?

Question 5: What are the source and destination IP addresses and source and destination ports of the ACK sent in response to the SYN. At what time is this ACK received at the client?

In the following we'll focus on the two HTTP messages (GET and 200 OK) and the TCP SYN and ACK segments identified above. Our goal below will be to locate these two HTTP messages and two TCP segments in the trace file (NAT_ISP_side) captured on the link between the router and the ISP. Because these captured frames will have already been forwarded through the NAT router, some of the IP address and port numbers will have been changed as a result of NAT translation.

Step 3: Open the NAT_ISP_side trace *. Note that the time stamps in this file and in NAT_home_side are not synchronised since the packet captures at the two locations shown in Figure 1 were not started simultaneously.*(Indeed, you should discover that the timestamps of a packet captured at the ISP link is actually less that the timestamp of the packet captured at the client PC).

Step 4: In the NAT_ISP_side trace file, find the HTTP GET message was sent from the client to the Google server at time 7.102967 (where t=7.109267 is time at which this was sent as recorded in the NAT_home_side trace file).

Question 6: At what time does this message appear in the NAT_ISP_side trace file?

Question 7: What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET message (as recording in the NAT_ISP_side trace file)? Which of these fields are the same, and which are different, than in your answer to Question 2 above?

Question 8: Are any fields in the HTTP GET message changed?

(*) Question 9: Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags, Checksum. If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change. (1 marks, 0.25 each)

Question 10: In the NAT_ISP_side trace file, at what time is the first 200 OK HTTP message received from the Google server?

Question 11: What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message? Which of these fields are the same, and which are different than your answer to Question 3 above?

Question 12: In the NAT_ISP_side trace file, at what time were the client-to-server TCP SYN segment and the server-to-client TCP ACK segment corresponding to the segments in Question 4 and 5 above captured?

(*) Question 13: What are the source and destination IP addresses and source and destination ports for these two segments? Which of these fields are the same, and which are different than your answer to Question 4 and 5 above? (2 mark)

Question 14: The discussion on NAT in the Week 8 lecture slides shows the NAT translation table used by a NAT router. Using your answers to the questions above, fill in the NAT translation table entries for the HTTP connection considered in the questions above.