Lab Exercise 7: NAT, Ethernet and ARP

Objectives:

- gain insights into the operation of NAT, Ethernet and ARP

Prerequisites and Links:

- Week 8, 9, 10 & 11 Lectures
- Relevant Parts of Chapter 4, 5 and 6 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
- ethernet-ethereal-trace-1

Marks: **10 marks.**

- Please attend the lab in your allocated lab time slot.
- We expect the students to go through as much of the lab exercises as they can at home and come to the lab for clarifying any doubts in procedure/specifications

Deadline:

23:59:59 Sunday 21st April. You can submit as many times as you wish before the deadline. A later submission will override the earlier submission, so make sure you submit the correct file. Do not leave until the last moment to submit, as there may be technical, or communications error and you will not have time to rectify it.

Late Submission Penalty:

Late penalty will be applied as follows:

- 1 day after deadline: 20% reduction
- 2 days after deadline: 40% reduction
- 3 days after deadline: 60% reduction
- 4 or more days late: NOT accepted

Note that the above penalty is applied to your final mark. For example, if you submit your lab work 2 days late and your score on the lab is 8, then your final mark will be 8 - 3.2 (40% penalty) = 4.8.

Submission Instructions:

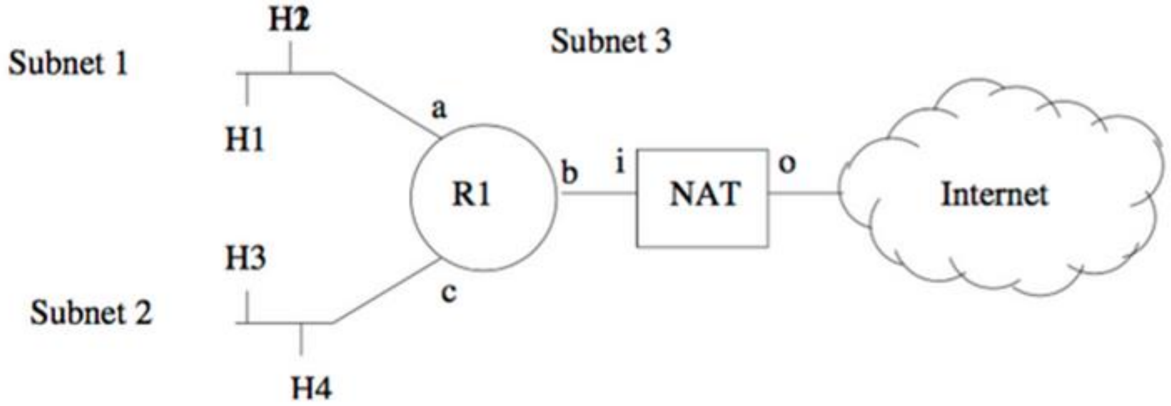
Submit a PDF document **Lab7.pdf** with answers to all questions marked with a (*). Do not make a tar and please submit one pdf file. You can submit from a lab machine or ssh into the CSE login server.

Original Work Only:

You are strongly encouraged to discuss the questions with other students in your lab. However, each student must submit his or her own work. You may need to refer to the material indicated above (particularly Tools of the Trade document) and also conduct your own research to answer the questions.

Exercise 1) 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.

(*) 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

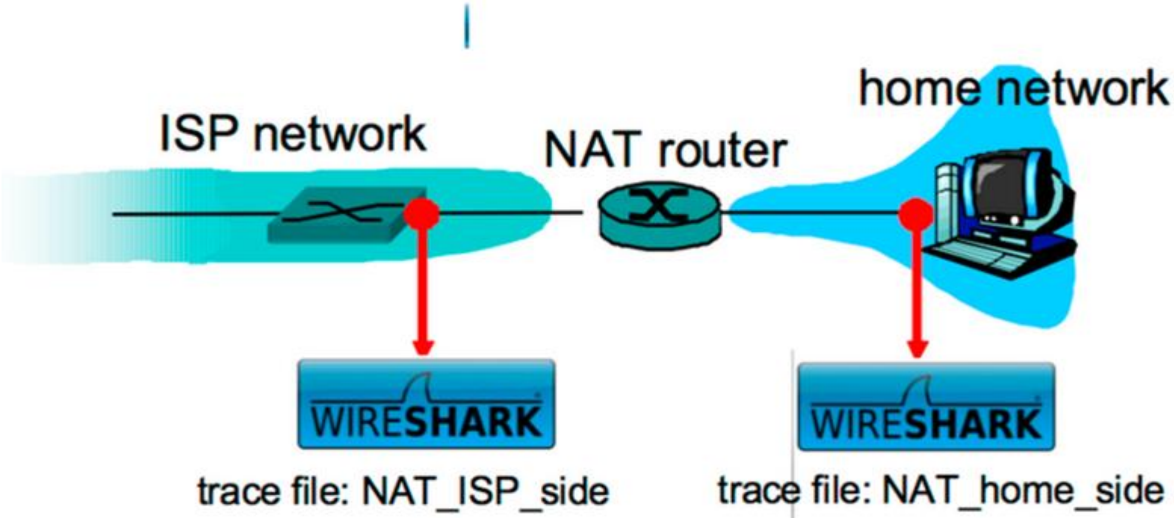


Figure 1: NAT trace collection scenario

The traces together captures the interaction between a web browser on a client machine in the home network and thewww.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 SYN/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 that 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 recorded 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.

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 SYN/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 (TCP SYN and TCP SYN/ACK)? Which of these fields are the same, and which are different than your answer to Question 4 and 5 above?

(*) 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.

Question 15: The trace files investigated above have additional connections to Google servers above and beyond the HTTP GET, 200 OK request/response studied above. For example, in the NAT_home_side trace file, consider the client-to-server GET at time 1.572315, and the GET at time 7.573305. Research the use of these two HTTP messages and safe browsing in general. Explain your findings in a concise manner.

Exercise 3: Using Wireshark to understand Ethernet

Step 1: Open an xterm and run Wireshark.

Step 2: Load the trace file ethernet-ethereal-trace-1 by using the *File* pull down menu, choosing *Open* and selecting the appropriate trace file. This file captures the sequence of HTTP request and response messages exchanged between a browser and a web server (gaia.cs.umass.edu). The web server response contains the rather lengthy US Bill of Rights.

Step 3: In order to answer the following questions, you'll need to look into the packet details and packet contents windows (the middle and lower display windows in Wireshark). Select the Ethernet frame containing the HTTP GET message. (Recall that the HTTP GET message is carried inside of a TCP segment, which is carried inside of an IP datagram, which is carried inside of an Ethernet frame; reread section 1.5.2 in the text (7th Edition) if you find encapsulation to be confusing). Hint: you will find this packet midway through the trace. Expand the Ethernet II information in the packet details window. Note that the contents of the Ethernet frame (header as well as payload) are displayed in the packet contents window.

Step 4: Answer the following questions, based on the contents of the Ethernet frame containing the HTTP GET message.

Question 1. What is the 48-bit Ethernet address of the source host of this packet?

(*) Question 2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? If not, then which device has this address? (Note: this is an important question, and one that students sometimes get wrong. You may want to refer back to relevant parts of the text and lecture notes and make sure you understand the answer here.)

Question 3. Give the hexadecimal value for the two-byte Frame type field.

(*) Question 4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame? Note that when you examine the Data portion of this frame, it actually consists of both the Ethernet frame headers as well as the payload (i.e. bottom window in Wireshark shows the entire 686 byte frame that is captured). Of the bytes preceding the G, the first few bytes are the Ethernet frame header. Does this include the preamble bytes, or are those bytes omitted from the capture? Given this, how many bytes of frame header are present? What are the remainder of the bytes before the G?

Step 5: Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message (i.e. in response to the previous GET message).

(*) Question 5. What is the value of the Ethernet source address? Is this the address of the host that sent the GET HTTP request, or of gaia.cs.umass.edu? If not then which device has this address?

Question 6. What is the destination address in the Ethernet frame? Is this the Ethernet address of the source host that sent the earlier GET HTTP request?

Question 7. How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" (i.e., the HTTP response code) appear in the Ethernet frame?

Exercise 4: Using Wireshark to understand ARP

For this exercise we will use the same trace as in Exercise 3.

Step 1: The first two frames in the trace contain ARP messages (as does the 6th message). Answer the following questions, focussing on these messages only.

(*) Question 1. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message? Is there something special about the destination address?

Question 2. Give the hexadecimal value for the two-byte Ethernet Frame type field.

Step 2: Download the ARP specification from https://www.rfc-editor.org/rfc/rfc826.txt . A readable, detailed discussion of ARP is also athttp://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html . Using these documents and looking at the contents of the first frame in the trace answer the following questions.

Question 3: How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?

Question 4. What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

Question 5. Does the ARP message contain the IP address of the sender?

(*) Question 6. Where in the ARP request does the "question" (IP address for which the mapping is being requested) appear?

Step 3: Now find the ARP reply that was sent in response to this query. Answer the following questions

(*) Question 7. How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?

Question 8. What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

Question 9. Where in the ARP message does the "answer" to the earlier ARP request appear – the Ethernet address of the machine whose corresponding IP address is being queried?

(*) Question 10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?