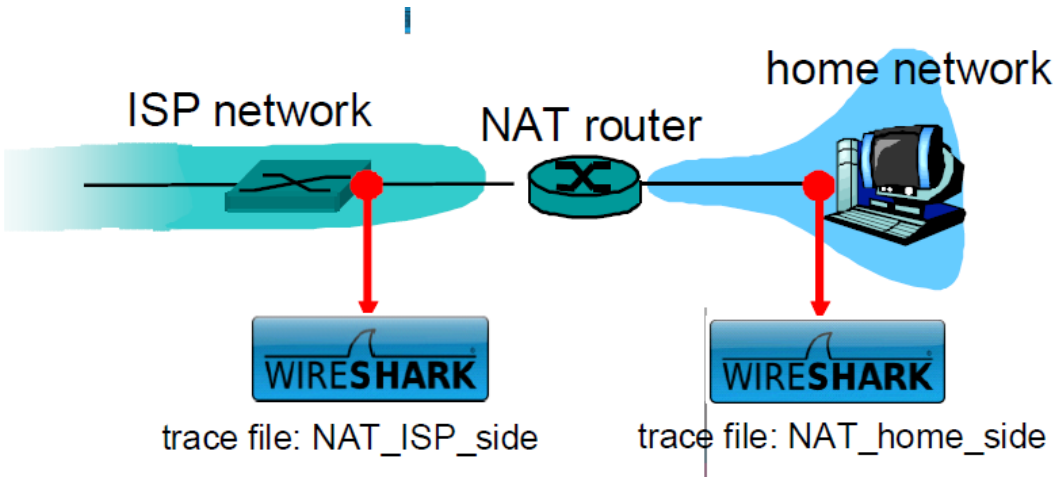
COMP9121 Week 7 NAT Wireshark

All contents are from https://www-net.cs.umass.edu/wireshark-labs/. Slight modifications are made for COMP9121.

In this lab, we'll investigate the behavior of the NAT protocol. Because we're interested in capturing packets at both the input and output sides of the NAT device, we'll need to capture packets at *two* locations. Also, because many students don't have easy access to a NAT device or to two computers on which to take Wireshark measurements, this isn't a lab that is easily done "live" by a student. Therefore in this lab, you will use Wireshark trace files that we've captured for you.

In this lab, we'll capture packets from a simple web request from a client PC in a home network to a www.google.com server. Within the home network, the home network router provides a NAT service. The figure below shows our Wireshark trace-collection scenario. As in our other Wireshark labs, we collect a Wireshark trace on the client PC in our home network. This file is called NAT_home_side. Because we are also interested in the packets being sent by the NAT router into the ISP, we'll collect a second trace file at a PC (not shown) tapping into the link from the home router into the ISP network, as shown in the figure. (The hub device shown on the ISP side of the router is used to tap into the link between the NAT router and the first hop router in the ISP). Client-to-server packets captured by Wireshark at this point will have undergone NAT translation. The Wireshark trace file captured on the ISP side of the home router is called NAT_ISP_side.



Open the NAT_home_side file and answer the following questions. You might find it useful to use a Wireshark filter so that only frames containing HTTP messages are displayed from the trace file.

1. What is the IP address of the client? (Answer: 192.168.1.100)

2. The client actually communicates with several different Google servers in order to implement "safe browsing." 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 .

3. 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? (Answer: Source: 192.168.1.100, 4335 Destination: 64.233.169.104, 80)

4. 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? (Answer: 7.158797) (Answer: Source: 64.233.169.104, 80 Destination: 192.168.1.100, 4335)

Open the NAT_ISP_side. *Note that the time stamps in this file and in NAT_home_side are not synchronized since the packet captures at the two locations shown in Figure 1 were not started simultaneously.*

5. In the NAT_ISP_side trace file, find the HTTP GET message was sent from the client to the Google server at time 7.109267 (where t=7.109267 is time at which this was sent as recorded in the NAT_home_side trace file). At what time does this message appear in the NAT_ISP_side trace file? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET (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 3 above? (Answer: 6.069168). (Answer: Source: 71.192.34.104, 4335 Destination: 64.233.169.104, 80). (Answer: only the source IP address has changed)

6. Are any fields in the HTTP GET message changed? 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. (Answer: No) (Answer: Version: No, Header Length: No, Flags: No , Checksum: Yes.) (Answer: Since the IP source address has changed, and the checksum includes the value of the source IP address, the checksum has changed).

7. In the NAT_ISP_side trace file, at what time is the first 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? Which of these fields are the same, and which are different than your answer to question 4 above? (Answer: 6.117570). (Answer: Source: 64.233.169.104, 80 Destination: 71.192.34.104, 4335). (Answer: only the destination IP address has changed)

Using your answers to 1-7 above, fill in the NAT translation table entries for HTTP connection considered in questions 1-7 above.

NAT translate table

WAN side	LAN side
71.192.34.104, 4335	192.168.1.100, 4335

External Internal