Overview

- Behaviour of NAT (network address translation) protocol: capturing packets at both the input and output sides of the NAT device
    - NAT protocol: translates private IP addresses to a public one before packets are sent to the internet

1. NAT measurement scenario
    - Capture packets from a simple web request made by a client PC in a home network to a www.google.com server
    - Within the home network, the router provides a NAT service
    - Download the zip file and click on NAT_home_side^2
      Also capture the packet from the ISP (internet service provider) side: NAT_ISP_side
    - Fillter using HTTP

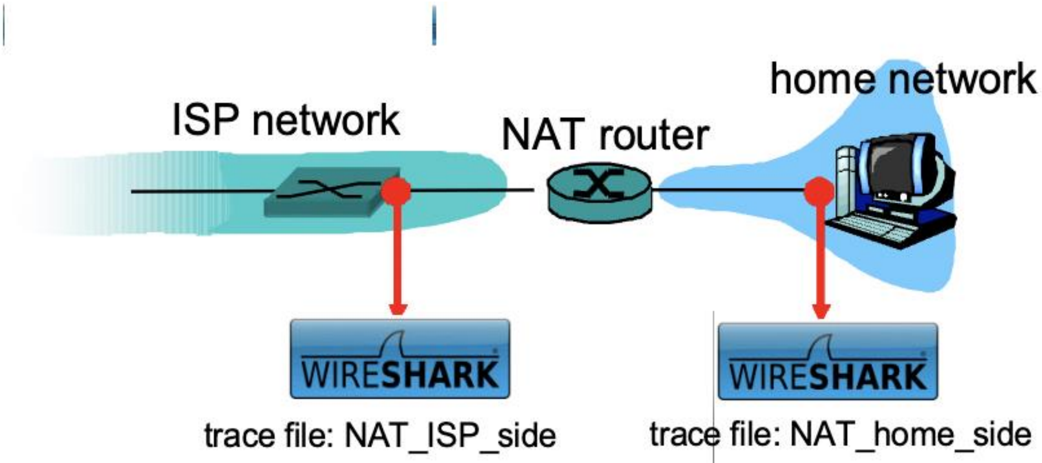

Figure 1: NAT trace collection scenario

Lab 8: NAT

1. What is the IP address of the client?

74.125.91.113

2. The client communicates with several different Google servers to implement “safe browsing.” (See extra credit section at the end of this lab). 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?

Time: 7.109267
Source: 192.168.1.100, 4335

Destination: 64.233.169.104, 80

4. At what time 4 is the corresponding 200OKHTTP 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?

Time: 7.158797
Source: 64.233.169.104, 80

Destination: 192.168.1.100, 4335

5. 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? 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? (Note: to find these segments you will need to clear the Filter expression you entered above in step 2. If you enter the filter “tcp”, only TCP segments will be displayed by Wireshark).

SYN
Time: 7.075657
Source: 192.168.1.100, 4335

Destination: 64.233.169.104, 80

ACK
Time: 7.108986
Source: 64.233.169.104, 80

Destination: 192.168.1.100, 4335

6. In the NAT_ISP_sidetracefile, 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?

Time: 6.069168
Source: 71.192.34.104, 4335

Destination: 64.233.169.104, 80

- Source IP address = replaced by the public IP address of the home network
- Dest ip address = replaced by the home network IP address

7. 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

CheckSum = changed since source IP address has also changed. Showcases how IP addresses affect the checksum

- The sum value of the bits in the header will change as it’s being moved across the internet

8. In the NAT_ISP_side trace file, at what time is the first 200OKHTTP 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?

Time: 6.117570
Source: 64.233.169.104, 80

Destination: 71.192.34.104, 4335

- Only destination IP address has been changed

9. 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 5 above captured? 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 5 above?

SYN
Time: 6.035475
Source: 71.192.34.104, 4335

Destination: 64.233.169.104, 80

ACK
Time: 6.067775
Source: 64.233.169.104, 80

Destination: 71.192.34.104, 4335

10.Using your answers to 1-8 above, fill in the NAT translation table entries for HTTP connection considered in questions 1-8 above.

- WAN: wide area network
- LAN: local area network