CT2108 Lab – Network Address Translation

The objective of this lab session is to investigate the behavior of the NAT (Network Address Translation) protocol.

NAT Packet Analysis

This lab session is different from your earlier Wireshark labs, where you captured live packets at a single Wireshark measurement point on your own computer. Because we are interested in capturing packets at both the input and output sides of a NAT device, we will need to analyse packets captured 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 is not lab work that is easily done using "live" packet capture. Therefore, in this session, you will be using two Wireshark trace files that have already been captured for you that you can download from Blackboard.

We will use packets captured during a simple web request from a client PC in a home network to a web server. In a typical home broadband connection, the router usually provides a NAT service to map private local IP addresses on the LAN interface to a single public IP address on the routers ISP (WAN) interface. Client-to-server packets captured by Wireshark on the WAN side of the router will have already undergone NAT translation. The Wireshark trace file captured on the ISP side of the home router is called NAT_ISP_side.pcap while the trace file from the LAN interface is called NAT_home_side.pcap - the diagram below shows the packet capture setup.

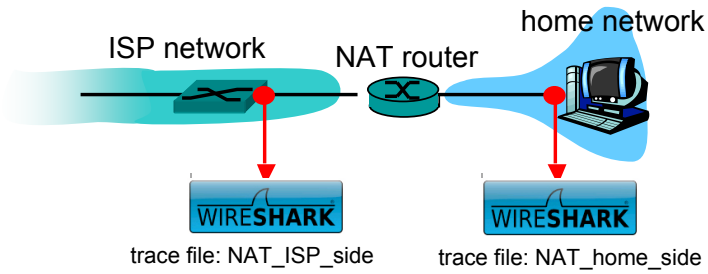

Figure 1 - Packet Capture Setup

Open the NAT_home_side.pcap packet capture file in Wireshark and try to answer the following questions:

1. What is the IP address of the client? Is this a public or private IP Address?

2. Identify and explain the contents of the packets that relate to the DNS lookup that was done to find the IP Address of the google website that was visited. You should see a related DNS query packet and a DNS query response packet in the packet list. You can type dns into the display filter text box to make these packets easier to identify.

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?
4. At what time[1] 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?

In the following part of the lab work we will focus on the two HTTP messages (GET and 200 OK). Our goal below will be to locate these two HTTP messages and the related 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.

Open the NAT_ISP_side.pcap packet capture file for analysis. *Note that the timestamps 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.* (Indeed, you may 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).

5. In the NAT_ISP_side trace file, find the HTTP GET message that was sent from the client to the Google server at time 7.109267 (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?
6. Are any of the various protocol header 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, explain why this field had 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?

[1] Specify time using the time since the beginning of the trace (rather than absolute, wall-clock time).