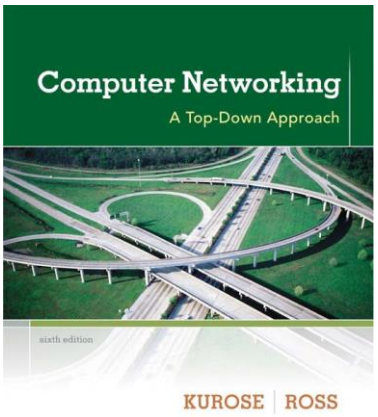
Wireshark Lab: NAT v6.0



Supplement to *Computer Networking: A Top-Down Approach, 6th ed.*, J.F. Kurose and K.W. Ross

"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb

---

Introduction

In this lab, we'll investigate the behavior of the NAT protocol. This lab will be different from our other Wireshark labs, where we've captured a trace file at a single Wireshark measurement point. 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. In this lab, you will use Wireshark trace files that have been captured for you.

1. NAT Measurement Scenario

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. Figure 1 shows our Wireshark trace-collection scenario.

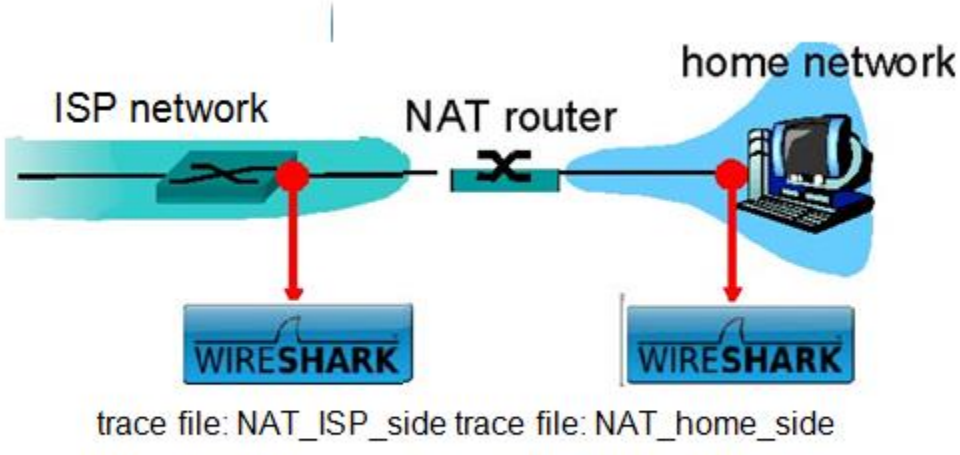


Figure 1: NAT trace collection scenario

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 (Attached with the email). 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 Figure 1. (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. Whenever possible, when answering a question below, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout to explain your answer.

1. **What is the IP address of the client?**

   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.

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?**

3. **At what time** (Specify time using the time since the beginning of the trace using wireshark options) **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?**

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? 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 that you already have. If you enter the filter "tcp", only TCP segments will be displayed by Wireshark).**

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.* (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). In the following trace file, we will focus on the two HTTP messages and TCP SYN and ACK segments identified above.

Answer the following questions:

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 2 above?

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, TTL. If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.**

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 3 above?**

8. **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 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 4 above?**

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

10. **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 write a half page explanation of the purpose of each of these messages.**