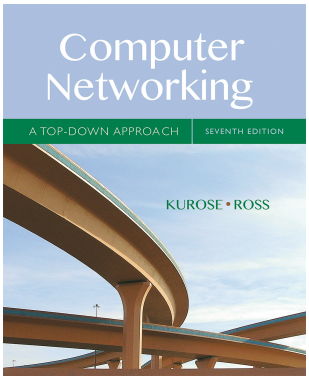
Wireshark Lab: NAT
SOLUTION



Supplement to *Computer Networking: A Top-Down Approach, 7th ed.,* J.F. Kurose and K.W. Ross

---

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." (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 7.102967. 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? **(Answer: 7.158798)** 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: 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 7.102967? **(Answer: 7.075657)** What are the source and destination IP addresses and source and destination ports for the TCP SYN segment? **(Answer: Source: 192.168.1.100, 4335 Destination: 64.233.169.104, 80)** What are the source and destination IP addresses and source and destination ports of the ACK sent in response to the SYN. **(Answer: Source: 64.233.169.104, 80 Destination: 192.168.1.100, 4335)** At what time is this ACK received at the client? **(Answer: 7.108986).** (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).

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.

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).

6. In the NAT_ISP_side trace file, find the HTTP GET message was sent from the client to the Google server at time 7.102967 (where t=7.102967 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? **(Answer: 6.069168).** 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)? **(Answer: Source: 71.192.34.104, 4335 Destination: 64.233.169.104, 80).** Which of these fields are the same, and which are different, than in your answer to question 3 above? **(Answer: only the source IP address has changed)**
7. Are any fields in the HTTP GET message changed? **(Answer: No)** Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version **(Answer: No)**, Header Length **(Answer: No)**, Flags**(Answer: No)** , Checksum **(Answer: Yes)**. If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change. **(Answer: Since the IP source address has changed, and the checksum includes the value of the source IP address, the checksum has changed).**
8. In the NAT_ISP_side trace file, at what time is the first 200 OK HTTP message received from the Google server? **(Answer: 6.308118).** 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: Source: 64.233.169.104, 80 Destination: 71.192.34.104, 4335).** Which of these fields are the same, and which are different than your answer to question 4 above? **(Answer: only the destination IP address has 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? **(Answer: 6.035475, and 6.067775, respectively)** What are the source and destination IP addresses and source and destination ports for these two segments? **(Answer. For the SYN: Source: 71.192.34.104, 4335 Destination: 64.233.169.104, 80. For the ACK: Source: 64.233.169.104, 80 Destination: 71.192.34.104, 4335)** Which of these fields are

the same, and which are different than your answer to question 5 above? **(Answer: for the SYN, the source IP address has changed, For the ACK, the destination IP address has changed. The port numbers are unchanged).**

Figure 4.22 in the text shows the NAT translation table in the NAT router.

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

NAT translate table	
WAN side	**LAN side**
71.192.34.104, 4335	**192.168.1.100, 4335**

Extra Credit: The trace files investigated above have additional connections to Google servers above and beyond the HTTP GET, 200OK request/response studied above. For example, in the NAT_home_side trace file, consider the client-to-server GET at time 1.573215, 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.