MPCS 54001, Winter 2021

Lab 4 - Solutions

Due: February 5 at 11:59 pm

Submit your assignment to Gradescope. If you need help, post questions to Ed Discussion. As a reminder, if you make a public post on Ed Discussion, please don't give away the answer! Please submit one pdf per group, answering the questions which appear on the last page. Gradescope will allow you to submit one pdf and add all group members to it after submitting.

NAT Measurement Scenario

1. What is the IP address of the client?

   192.168.1.100

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?

   Source: 192.168.1.100, 4335

   Destination: 64.233.169.104, 80

3. 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?

   t = 7.158798

   Source: 64.233.169.104, 80

   Destination: 192.168.1.100, 4335

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

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 you entered above in step 2. If you enter the filter "tcp", only TCP segments will be displayed by Wireshark).

   t = 7.075657

   Source: 192.168.1.100, 4335

   Destination: 64.233.169.104

   Source: 64.233.169.104, 80

   Destination: 192.168.1.100, 4335, 80

   t = 7.108986

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?

   t = 6.069168

   Source: 71.192.34.104, 4335

   Destination: 64.233.169.104, 80

   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.

   No

   Version: No, Header Length: No, Flags: No, Checksum: Yes

   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?

   t = 6.308118

   Source: 64.233.169.104, 80

   Destination: 71.192.34.104, 4335

   Only the destination IP address has changed

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 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?

   t = 6.035475 and t = 6.067775

   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

For the SYN, the source IP address has changed, For the ACK, the destination IP address has changed. The port numbers are unchanged.

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

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