

Data Communications Laboratory

Network Address Translation

Student Name: Jai Carey

Student ID: 45188416

Exercise 1: NAT Measurement Scenario

1. What is the IP address of the client?

192.168.1.100 (IP Address of the client machine on the home network)

2. Set the Filter: field in Wireshark to:

http && ip.addr == 64.233.169.104

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?

Source IP Address: 192.168.1.100

Destination IP Address: 64.233.169.104

TCP Source Port: 4335

TCP Destination Port: 80

4. At what time 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?

The corresponding 200 OK HTTP response message is received at 7.158797.

Source IP Address: 64.233.169.104

Destination IP Address: 192.168.1.100

TCP Source Port: 80

TCP Destination Port: 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.

1) 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?

2) What are the source and destination IP addresses and source and destination ports for the TCP SYN segment?

3) What are the source and destination IP addresses and source and destination ports of the ACK sent in response to the SYN.

4) At what time is this ACK received at the client?

1)

The Client-To-Server SYN packet for the TCP handshake to establish a TCP connection for the GET message was at 7.075657.

2)

SYN PACKET:

Source IP Address: 192.168.1.100

Destination IP Address: 64.233.169.104

TCP Source Port: 4335

TCP Destination Port: 80

3)

SYN ACK PACKET:

Source IP Address: 64.233.169.104

Destination IP Address: 192.168.1.100

TCP Source Port: 80

TCP Destination Port: 4335

4)

The ACK received at the client (apart of the SYN ACK message from the server to the client) is received at 7.108986.

6. In the NAT_ISP_side trace file, find the HTTP GET message was sent from the client to the Google server at time 7.109267 (where $t=7.109267$ is time at which this was sent as recorded in the NAT_home_side trace file).

1) At what time does this message appear in the NAT_ISP_side trace file?

2) 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)?

3) Which of these fields are the same, and which are different, than in your answer to question 3 above?

1)

The time the GET message is received at the ISP side is 6.069168.

2)

Source IP Address: 71.192.34.104

Destination IP Address: 64.233.169.104

TCP Source Port: 4335

TCP Destination Port: 80

3)

All fields are the same, the main difference is the SOURCE IP ADDRESS.

This is because of the NAT method being used at the router of the home network converting our source address to our external IP Address so that our host machine on the home network can communicate with the internet. Ultimately, so that external sources on the internet know where to send messages so that they hit our router and can arrive back at our host machine.

7. **1) Are** any fields in the HTTP GET message changed?
2) Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags, Checksum.
3) If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.

1)

There are no changes to the HTTP GET message.

2)

The only change to the IP datagram carrying the HTTP GET is the Checksum

3)

The IPV4 header checksum is the sum of all bits in the IP Header. As there is a change to the Source address, the number of bits in that address will also change. This means that when calculating the checksum, there will be a different calculation after the NAT process has occurred.

8. In the NAT_ISP_side trace file.
1) At what time is the first 200 OK HTTP message received from the Google server?
2) What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?
3) Which of these fields are the same, and which are different than your answer to question 4 above?

1)

The time the GET message is received at the ISP side is 6.117570.

2)

Source IP Address: 64.233.169.104

Destination IP Address: 71.192.34.104

TCP Source Port: 80

TCP Destination Port: 4335

3)

The only change is the Destination IP Address because its destination is external IP Address of the home router (which is using NAT).

9. In the NAT_ISP_side trace file,

1) 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?

2) What are the source and destination IP addresses and source and destination ports for these two segments?

3) Which of these fields are the same, and which are different than your answer to question 5 above?

1)

The Client-To-Server SYN packet was at 6.035475.

The Server-To-Client SYN ACK packet was at 6.067775.

2)

SYN PACKET:

Source IP Address: 71.192.34.104

Destination IP Address: 64.233.169.104

TCP Source Port: 4335

TCP Destination Port: 80

SYN ACK PACKET:

Source IP Address: 64.233.169.104

Destination IP Address: 71.192.34.104

TCP Source Port: 80

TCP Destination Port: 4335

3)

All fields are the same except for the Source IP Address in the SYN packet and the Destination IP Address in the SYN ACK packet.