Name : Aman Sharma
Enrollment No : 0801IT221017

ACN ASSIGNMENT – 4 (NAT)

1. What is the IP address of the client?

(Answer: 192.168.1.100)

```
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 10.119.240.64
```

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 .

```
56 7.109267     192.168.1.100     64.233.169.104     HTTP     689 GET / HTTP/1.1
60 7.158797     64.233.169.104    192.168.1.100      HTTP     814 HTTP/1.1 200 OK  (text/html)
```

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?

(Answer: Source: 192.168.1.100, 4335 Des na on: 64.233.169.104, 80)

```
56 7.109267     192.168.1.100     64.233.169.104     HTTP     689 GET / HTTP/1.1
```

4. At what time4 is the corresponding 200 OK HTTP message received from the Google server?

(Answer: 7.158797)

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 Des na on: 192.168.1.100, 4335)

```
60 7.158797     64.233.169.104    192.168.1.100      HTTP     814 HTTP/1.1 200 OK  (text/html)
```

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 7.109267?

(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. At what time is this ACK received at the client? (Answer: 7.108986).

```
53 7.075657     192.168.1.100     64.233.169.104     TCP      66 4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM
54 7.108986     64.233.169.104    192.168.1.100      TCP      66 80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64
```

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). 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)?

Name : Aman Sharma
Enrollment No : 0801IT221017

ACN ASSIGNMENT – 4 (NAT)

(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)

```
85 6.069168      71.192.34.104        64.233.169.104       HTTP        689 GET / HTTP/1.1
```

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, 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.

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).

```
103 6.308118      64.233.169.104       71.192.34.104        HTTP        226 HTTP/1.1 200 OK  (GIF89a)
```

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 on: 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).

```
82 6.035475      71.192.34.104        64.233.169.104       TCP         66 4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM
83 6.067775      64.233.169.104       71.192.34.104        TCP         66 80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64
```

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**