CS315: Lab Assignment 8

B Siddharth Prabhu
200010003@iitdh.ac.in

28 February 2023

1 NAT : Network Address Translation

NAT is a method of mapping one IP address space into another by modifying address information in the IP header of packets while they are in transit across a router. We are given two Wireshark trace files, which consist of the packet traces from within the network and from the Internet-facing sides of a router respectively. Below are screenshots of the same, following which we shall answer some questions:

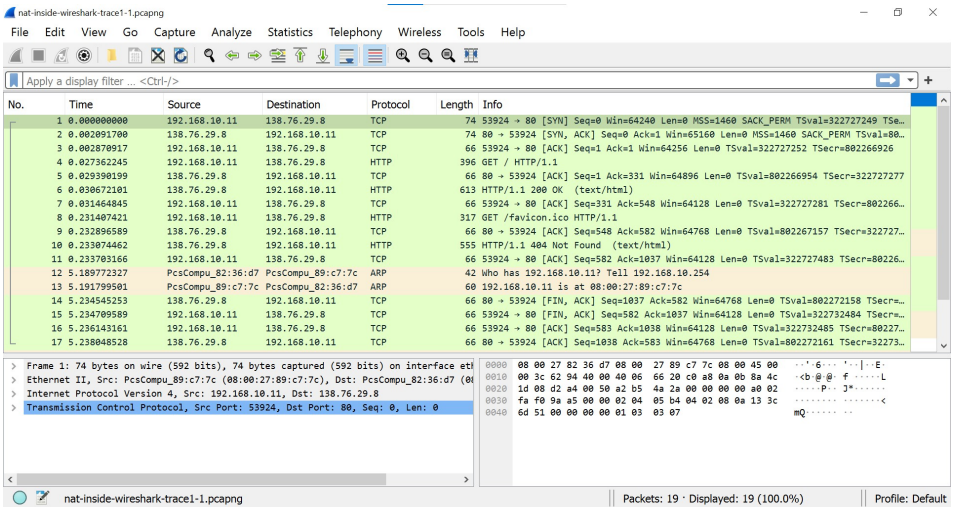

Figure 1: Trace file `nat-inside-wireshark-trace1-1`

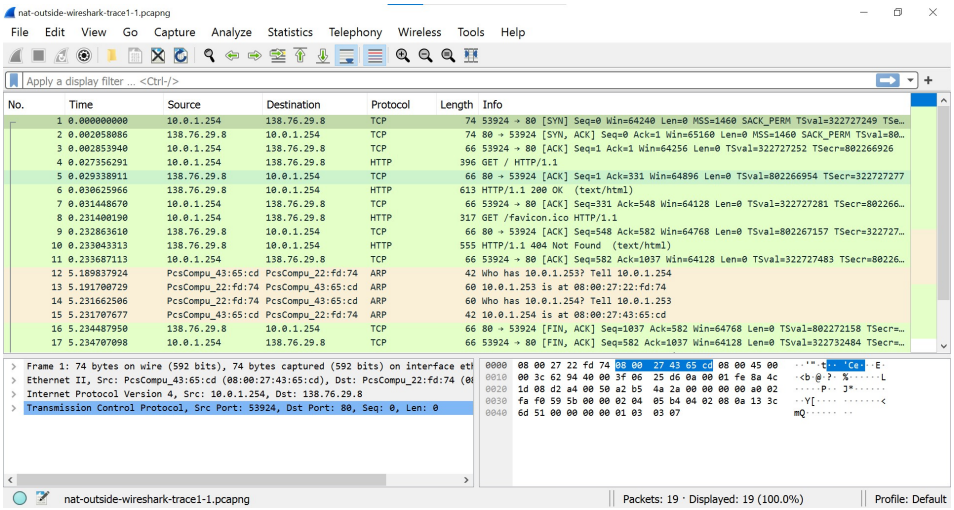

Figure 2: Trace file `nat-outside-wireshark-trace1-1`

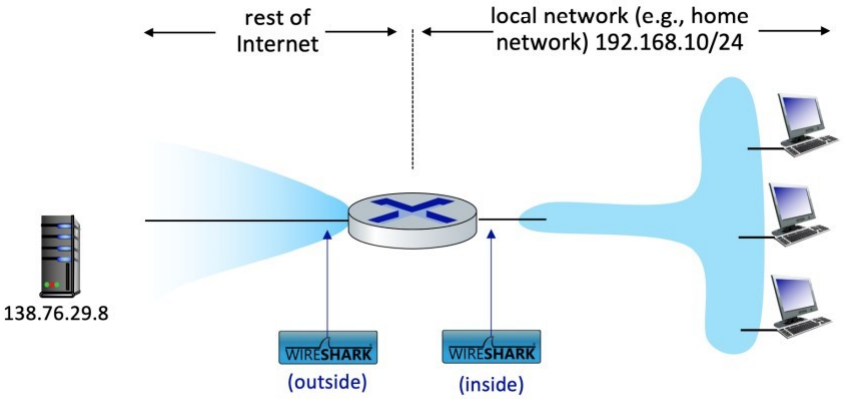

Figure 3: NAT Packet Capture Scenario

Let's first take a look at what's happening on the LAN side of the NAT router, using the trace file `nat-inside-wireshark-trace1-1.pcapng` . We will refer to this as the 'inside' trace file.

(1) What is the IP address of the client that sends the HTTP GET request in the 'inside' trace? What is the source port number of the TCP segment in this datagram containing the HTTP GET request? What is the destination IP address of this HTTP GET request? What is the destination port number of the TCP segment in this datagram containing the HTTP GET request?

For the HTTP GET request in the trace, the answers to the above questions are as follows:

- Source IP address = **192.168.10.11**
- Source port number = **53924**
- Destination IP address = **138.76.29.8**
- Destination port number = **80**

(2) At what time is the corresponding HTTP 200 OK message from the web server forwarded by the NAT router to the client on the router's LAN side?

The corresponding HTTP 200 OK message is forwarded by the NAT router to the client at time **0.030672101 seconds**. (Time is in reference to first packet captured.)

(3) What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

For the corresponding HTTP 200 OK message in the trace, the answers to the above questions are as follows:

- Source IP address = **138.76.29.8**
- Source port number = **80**
- Destination IP address = **192.168.10.11**
- Destination port number = **53924**

Now, we shall analyze what's happening on the Internet side of the NAT router, using the trace file `nat-outside-wireshark-trace1-1.pcapng` . We will refer to this file as the 'outside' trace file.

(4) At what time does this HTTP GET message appear in the 'outside' trace file?

The HTTP GET message appears in the 'outside' trace file at time **0.027356291 seconds**. (Time is in reference to first packet captured.)

(5) What are the source and destination IP addresses and TCP source and destination port numbers on the IP datagram carrying this HTTP GET (as recorded in the 'outside' trace file)?

For the IP datagram carrying the HTTP GET message in the mentioned file:

- Source IP address = **10.0.1.254**
- Source port number = **53924**
- Destination IP address = **138.76.29.8**
- Destination port number = **80**

(6) Which of these four fields are different from your answer to question 1 above?

Of the four mentioned fields, only the **Source IP address** has changed. (From 192.168.10.11 to 10.0.1.254)

(7) Are any fields in the HTTP GET message changed?

No, none of the fields of the HTTP GET message have changed.

(8) Which of the following fields in the IP datagram carrying the HTTP GET are changed from the datagram received on the local area network (inside) to the corresponding datagram forwarded on the Internet side (outside) of the NAT router: Version, Header Length, Flags, Checksum?

Of the mentioned fields, only the **Checksum** field changed in transit across the NAT router. This could be attributed to the change in Source IP address and TTL (Time To Live). (Note: The Version, Header, and Flags stayed the same in transit.)

(Contd. on next page)

Concerning the HTTP reply containing the "200 OK" message that was received in response to the HTTP GET request above:

(9) At what time does this message appear in the 'outside' trace file?

This message appears in the 'outside' trace file at time **0.030625966 seconds** (Time is in reference to first packet captured.)

(10) What are the source and destination IP addresses and TCP source and destination port numbers on the IP datagram carrying this HTTP reply (200 OK) message (as recorded in the 'outside' trace file)?

For the IP datagram carrying the HTTP reply (200 OK) message in the mentioned (outside) file:

- Source IP address = **138.76.29.8**
- Source port number = **80**
- Destination IP address = **10.0.1.254**
- Destination port number = **53924**

(11) What are the source and destination IP addresses and TCP source and destination port numbers on the IP datagram carrying the HTTP reply ("200 OK") that is forwarded from the router to the destination host in the right of Figure (3)?

Using knowledge of NAT based on the previous questions, for the IP datagram carrying the HTTP reply:

- Source IP address = **138.76.29.8**
- Source port number = **80**
- Destination IP address = **192.168.10.11**
- Destination port number = **53924**

(12) Do your answers to question 11 above match what you see in the 'inside' trace file?

Yes, the answer deduced for question 11 matches what is found within the 'inside' trace file.

(Contd. on next page)

2 SMTP Socket Programming

Please find the file `200010003_client.py` in this submission. Follow the prompts carefully during execution. Below are screenshots of the message sent and received.

```
siddharth@DESKTOP-5490SID:/mnt/c/Users/bsidd/Desktop/CS315 CN_Lab/Submissions/Assignment 8$ python3 200010003_client.py
220 smtp.gmail.com ESMTP z18-20020a17090665d200b008b17e55e8f7sm4732999ejn.186 - gsmtp

250 smtp.gmail.com at your service

220 2.0.0 Ready to start TLS

Enter Authentication details of sender below:
For default (smtplab23@gmail.com), hit [ENTER] for quick login.
Mail ID:
Logging in ...
334 VXNlcm5hbWU6

334 UGFzc3dvcmQ6

235 2.7.0 Accepted

Enter recipient Email ID ([ENTER] for default): 200010003@iitdh.ac.in
250 2.1.5 OK z18-20020a17090665d200b008b17e55e8f7sm4732999ejn.186 - gsmtp

354  Go ahead z18-20020a17090665d200b008b17e55e8f7sm4732999ejn.186 - gsmtp

Enter Email Subject ([ENTER] for default): Sample Subject
Enter Message: If i am going to be honest with you, in my own humble opinion, without being sentimental of course, witho
ut offending anyone who thinks differently from my own point of view, but also by looking into this matter in distinctiv
e perspective, i would like to say that i have nothing to say
250 2.0.0 OK  1677606025 z18-20020a17090665d200b008b17e55e8f7sm4732999ejn.186 - gsmtp

221 2.0.0 closing connection z18-20020a17090665d200b008b17e55e8f7sm4732999ejn.186 - gsmtp

Connection Closed ...
siddharth@DESKTOP-5490SID:/mnt/c/Users/bsidd/Desktop/CS315 CN_Lab/Submissions/Assignment 8$
```

Figure 4: Message being sent

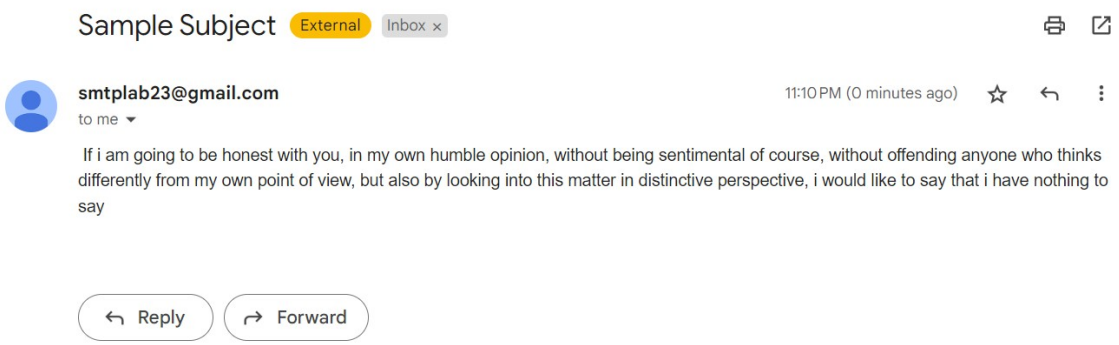

Figure 5: Message being received