Lab 5: NAT

Hide Assignment Information

Instructions

Lab 5: NAT

Instructions:

- Support all answers by a screenshot of your Wireshark and Command Prompt windows. Annotate screenshots to explain your answer.
- Submissions must be through Brightspace.
- There is a 24-hour grace period after the due date without a penalty. Late submissions will not be accepted.

Note: This lab is mostly adapted from materials provided by the authors of *Computer Networking: A Top-Down Approach*.

Introduction

In this lab, we will investigate the behavior of a NAT router. This lab will be different from our other Wireshark labs, where we have captured a trace file at a single Wireshark measurement point. Because we are interested in capturing packets at *both* the input and output sides of the NAT device, we will need to capture packets at *two* locations. Also, because many students do not have easy access to a NAT device or to two computers on which to take Wireshark measurements, this is not a lab that is easily done live by a student. So, in this lab, you will use Wireshark trace files that we have captured for you. This should be a relatively short and easy lab since the concepts behind NAT are not difficult, but it will be good nonetheless to observe NAT in action.

You will need to download the zip file here and extract two trace files: *nat-**inside**-wireshark-trace1-1.pcapng* and *nat-**outside**-wireshark-trace1-1.pcapng*. These trace files can be used to answer these lab questions. Once you have downloaded a trace file, you can load it into Wireshark and view the trace using the File pull down menu, choosing Open, and then selecting the trace file name.

NAT Measurement Scenario

In this lab, we will capture packets containing a simple HTTP GET request message sent inside a home network to a remote server, and the corresponding HTTP response from that server. Within the home network, the home network router

Cancel

provides a NAT service. Figure 1 shows our Wireshark trace-collection scenario. We will capture packets in *two* locations, and thus this lab has *two* trace files:

- The downloaded file captured packets being received at the local area network (LAN) side of the NAT router. All devices in this LAN have addresses in 192.168.10/24.
- Because we are also interested in analyzing packets being forwarded (and received) by the NAT router on its Internet-facing side, we will collect a second trace file on the Internet side of the router, as shown in Figure 1. Packets captured by Wireshark at this point that were sent from a host on the right to the server on the left will have undergone NAT translation by the time they reach this second measurement point. This capture is saved in the downloaded file.

In the scenario shown in Figure 1, one of the hosts within the LAN will send an HTTP GET request to the web server at IP address 138.76.29.8, which will respond back to the requesting host. Of course, we are not really interested in the HTTP GET request itself, but rather how the NAT router changes the IP addresses and port numbers of the datagram containing the GET request on the LAN side (inside) to addresses and port numbers in the forwarded outgoing datagram on the Internet side (outside) of the NAT router.

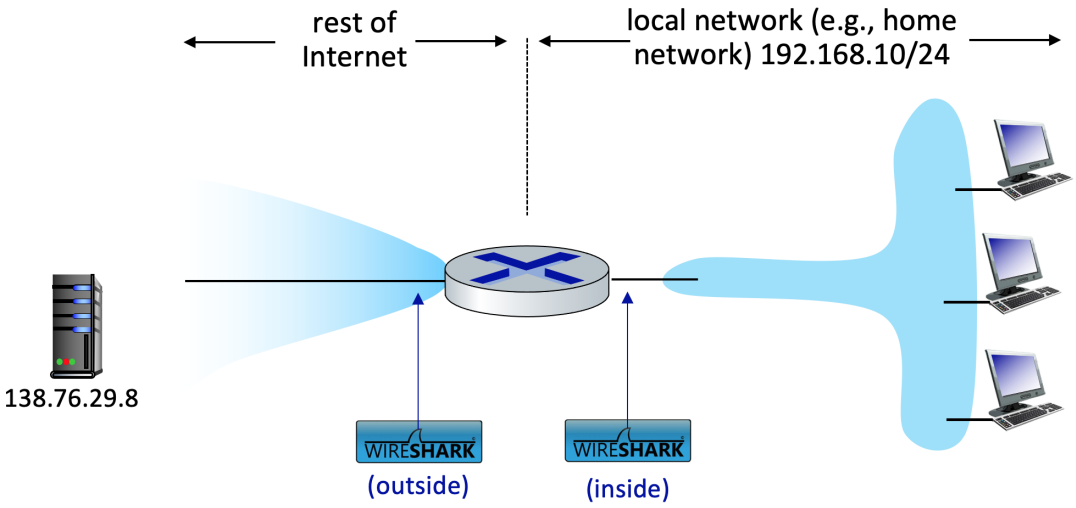

Figure 1 NAT packet capture scenario.

Questions

Let's first take a look at what is happening on the LAN side of the NAT router. Open the *nat-**inside**-wireshark-trace1-1.pcapng* trace file. In this file, you should see an HTTP GET request addressed to the external web server at IP address 138.76.29.8, as well as the subsequent HTTP response message ("200 OK"). Both of these messages in the trace file were captured on the LAN side of the router.

Now answer the following questions:

1. What is the IP address of the client that sends the HTTP GET request in the *nat-**inside**-wireshark-trace1-1.pcapng* 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?

2. At what time is the corresponding HTTP 200 OK message from the webserver forwarded by the NAT router to the client on the router's LAN side? Specify time using the time since the beginning of the trace (rather than absolute, wall-clock time).

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?

In the following we will focus on these two HTTP messages (GET and 200 OK). Our goal below will be to locate these two HTTP messages in the trace file *nat-**outside**-wireshark-trace1-1.pcapng*, captured on the Internet-side link between the router and the ISP. Because the captured packets heading towards the server 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 trace file *nat-**outside**-wireshark-trace1-1.pcapng.* Note that the time stamps in this file and the *nat-**inside**-wireshark-trace1-1.pcapng* file are not necessarily synchronized.

In the *nat-**outside**-wireshark-trace1-1.pcapng* trace file, find the HTTP GET message that corresponds to the HTTP GET message that was sent from the client to the 138.76.29.8 server at time t=0.27362245, where t=0.27362245 is the time at which this message was sent, as recorded in the *nat-**inside**-wireshark-trace1-1.pcapng* trace file.

4. At what time does this HTTP GET message appear in the *nat-**outside**-wireshark-trace1-1.pcapng* trace file?

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 *nat-**outside**-wireshark-trace1-1.pcapng* trace file)?

6. Which of these four fields are different than in your answer to Question 1 above?

7. Are any fields in the HTTP GET message 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?

Let's continue to look at the *nat-**outside**-wireshark-trace1-1.pcapng* trace file. Find the HTTP reply containing the "200 OK" message that was received in response to the HTTP GET request you just examined in questions 4-8 above.

9. At what time does this message appear in the *nat-**outside**-wireshark-trace1-1.pcapng* trace file?

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 *nat-**outside**-wireshark-trace1-1.pcapng* trace file)?

Lastly, let's consider what happens when the NAT router receives this datagram that you examined in Questions 9 and 10, performs NAT translation, and finally forwards that datagram to the destination host on the LAN side. Based on your answers to questions 1 through 10 above and your knowledge of how NAT works, you should be able to answer the following question without actually looking at the *nat-**inside**-wireshark-trace1-1.pcapng* trace file.

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 1?

Just to make sure you understand NAT, you should now use Wireshark to check the *nat-**inside**-wireshark-trace1-1.pcapng* trace file to look at the HTTP reply ("200 OK").

Do your answers to Question 11 above match what you see in the *nat-**inside**-wireshark-trace1-1.pcapng* trace file? [Hopefully, your answer is yes *!*].

Due on Nov 1, 2023 11:59 PM

Available on Oct 26, 2023 12:01 AM. **Access restricted before availability starts.**

Available until Nov 2, 2023 11:59 PM. **Submission restricted after availability ends.**

Submit Assignment

Submission is restricted outside of availability dates.