Wireshark Lab: NAT Protocol

In this lab, you will analyze the behavior of the NAT protocol using Wireshark trace files. Packet captures are provided for the client-side and ISP-side of a home network NAT device. Use Wireshark to examine the traces and answer the questions below. Whenever possible, provide annotated printouts of relevant packets.

Analysis

Q1: What is the IP address of the client as recorded in the `NAT_home_side` trace file?

Q2: The client communicates with multiple Google servers. The main Google server serving the homepage has the IP address `64.233.169.104`. Use the filter expression `http && ip.addr == 64.233.169.104` in Wireshark to isolate relevant frames. How many packets match this filter?

Q3: At time `7.109267`, the client sends an HTTP `GET` request to the server `64.233.169.104`. Find this packet in the `NAT_home_side` trace file. What are the source and destination IP addresses and TCP source and destination ports in the IP datagram carrying this request?

Q4: Locate the corresponding `200 OK` HTTP message received from the Google server. What is the time of its arrival at the client? What are the source and destination IP addresses and TCP source and destination ports in the IP datagram carrying this response?

Q5: Before the HTTP `GET` request, a TCP connection is established via the three-way handshake. Identify the client-to-server TCP `SYN` segment used to establish the connection for the HTTP `GET` at time `7.109267`. What are the source and destination IP addresses and source and destination ports in this `SYN` segment? Find the corresponding `ACK` segment sent by the server. What are the source and destination IP addresses and source and destination ports in the `ACK`? What is the time when the `ACK` is received at the client? Include annotated printouts of both segments.

Q6: Open the `NAT_ISP_side` trace file. Locate the HTTP `GET` request from question 3 in this trace. At what time does this packet appear in the `NAT_ISP_side` trace? Compare the source and destination IP addresses and TCP source and destination ports between the two trace files. Which fields have changed due to NAT? Explain the differences.

Q7: In the `NAT_ISP_side` trace file, check the IP header of the HTTP `GET` request from question 6. Which of the following fields have changed compared to the home-side trace: Version, Header Length, Flags, Checksum? Check both the IP Datagram header and the TCP Segment header. For any changed field, provide a brief explanation of why the change occurred.

Q8: In the `NAT_ISP_side` trace file, locate the first `200 OK` HTTP message from the server corresponding to the request in question 6. What are the source and destination IP addresses and TCP source and destination ports in the IP datagram carrying this response? Compare these fields to your answer from question 4.

Q9: In the `NAT_ISP_side` trace file, locate the client-to-server TCP `SYN` segment and the server-to-client `ACK` segment corresponding to the handshake in question 5. At what times are these segments captured? Compare the source and destination IP addresses and TCP source and destination ports to the `NAT_home_side` trace file.

Submission Guidelines

Submit your answers as a PDF on Canvas, including annotated Wireshark screenshots where applicable.