CSC358 Assignment 4 Wireshark

March 6, 2016

1 NAT Measurement Scenario

In this lab, we'll capture packets from a simple web request from a client PC in a home network to a www.google.com server. Within the home network, the home network router provides a NAT service, as discussed in Chapter 4.

Go to `http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip` to download the trace file we need in this experiment. Figure 1 shows the WireShark trace collection scenario. Analysis the trace files NAT_home_side.pcap and NAT_ISP_side.pcap to answer the following questions:

For simplicity concerns, apply filter "tcp.stream eq 2" to both pcap files, this will give you the same tcp stream on both captured files.

1. What is the client ip on home side? And what is the client ip on ISP side. What's the relationship between them?
2. For the first packet of this tcp stream, is there anything changed in the tcp header between home side and ISP side? If so, name the header field(s).
3. Focus on the same packet, is there anything changed in the ip header? If so, name the header field(s), and explain why they are changed.

Now we focus on a udp stream, apply filter "udp.stream eq 1" to home side and "udp.stream eq 0" to ISP side.

4. For the first packet of this udp stream, is there anything changed in the udp header? If so, name the header field(s). Is any other udp header or data changed? If not, explain why udp checksum changed.

Recall the mechanism of NAT translation, answer the following question:

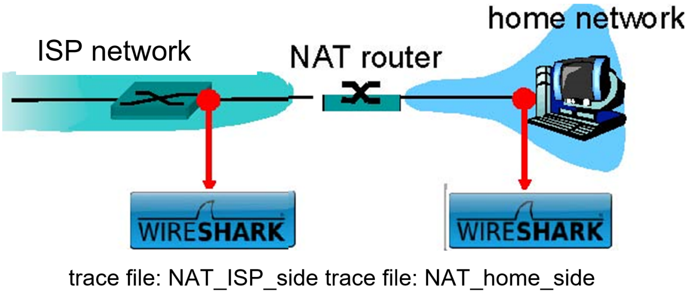

Figure 1: NAT trace collection scenario

5. For the tcp and udp streams we discussed above, for all the packets that the client sent, is the tcp/udp source port ever changed by the router? If not, is it mandatory to keep the same source port before and after NAT translation? (you don't need to provide a screenshot for this question).

2 ICMP

Execute the command "ping gaia.cs.umass.edu" in cmd(Windows) or terminal(Mac Os, Linux), use WireShark to capture the generated ICMP packet (you can use filter "icmp" in WireShark) and answer the following questions:

6. Why is it that an ICMP packet does not have source and destination port numbers?
7. Choose one of the ping request packets sent by your host, what are the ICMP type and code numbers? Find the corresponding ping reply, what are the type and code numbers?

Open your web browser and try accessing `http://gaia.cs.umass.edu:81/` (the page should fail to load), use WireShark to capture the packets and answer the following questions:

8. During the browser trying loading the page, did you host receive any ICMP packets? If yes, what are the type and code of these ICMP packets?
9. Apart form the ICMP headers, what is in the data field of these ICMP packets? (hint: you may need refer to Wikipedia to answer this question)
10. Image the case when a NAT router receives one of the above ICMP packets on its external interface, how does the router know which internal host to forward this packet to? (You don't need to provide screenshot for this question)