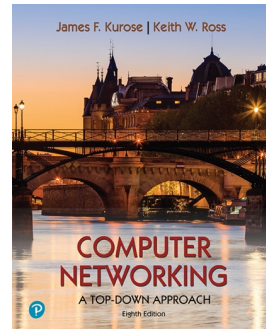# Wireshark Lab: NAT v8.1

Supplement to *Computer Networking: A Top-Down Approach, 8th ed.,* J.F. Kurose and K.W. Ross

"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb

In this lab, we'll investigate the behavior of a NAT router. In this lab we're interested in capturing packets at <u>both</u> the input and output sides of the NAT device, we'll need to capture packets at *two* locations. Also, because many students don't have easy access to a NAT device or to two computers on which to take Wireshark measurements, this isn't a lab that is easily done "live" by a student. So, in this lab, you'll use Wireshark trace files that we've captured for you. This should be a relatively short and easy lab since the concepts behind NAT aren't difficult, but it'll be good nonetheless to observe NAT in action. Before beginning this lab, you'll probably want to review the material on NAT in section 4.3.3 in the text.

NAT Measurement Scenario

In this lab, we'll capture packets containing a simple HTTP GET request message from a client inside a home network to a remote server, and the corresponding HTTP response from that server. Within the home network, the home network router provides a NAT service, as discussed in Chapter 4. Figure 1 shows our Wireshark trace-collection scenario. We'll capture packets in *two* locations, and thus this lab has *two* trace files:

- We'll capture 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. This file is named *NAT_home_side.pcap*.
- Because we're also interested in analyzing packets being forwarded (and received) by the NAT router on its Internet-facing side, we'll 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 file is named *NAT_ISP_side.pcap*..
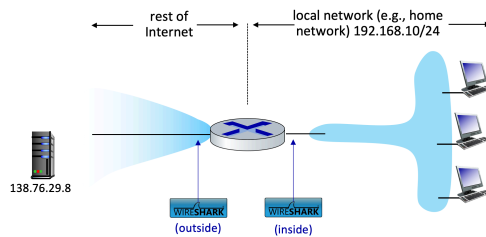
Figure 1: NAT packet capture scenario

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're 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.

Now, we're ready to deal with the questions posted on the Aprender3!