

Lab Exercise 5: Examining DHCP and NAT with Wireshark¹

(Total: 20 points)

OBJECTIVE:

In this lab, we'll use Wireshark to take a close look at two important network-layer protocols for address administration: DHCP and NAT.

BACKGROUND:

DHCP is covered in Section 4.3.2 of the textbook. Recall that DHCP is used extensively in corporate, university and home-network wired and wireless LANs to dynamically assign IP addresses to hosts (as well as to configure other network configuration information).

NAT is covered in Section 4.3.3 of the textbook. Remember that NAT can be used to allocate private IP addresses to internal hosts, which are translated to a common public IP address for outgoing packets. As such, it can be used to deal with the IP shortage problem. Also, it makes easier to migrate a cooperation network between different ISPs.

LAB ACTIVITIES:

Read the lecture materials and the related sections in the textbook to understand how a DHCP client exchange messages with a DHCP server in order to acquire, renew or release an IP address.

1. Download the Wireshark trace file ***dhcp-ethereal-trace-1.pcap*** from D2L. This trace file was collected by Wireshark running on one of the authors' computers. The trace file was captured when the host: 1) acquired an IP address; 2) renewed the allocated address; 3) released the allocated address; and acquired an IP address again.
2. Once you have downloaded the trace, you can load it into Wireshark and view the trace using the *File* pull down menu, by choosing *Open* and then selecting the downloaded trace file. To see only the DHCP packets, you need to enter "bootp" and not "dhcp" in the packet filter). Based on this trace file, answer the following questions in your lab report:
 - a. A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the DHCP ACK is exchanged between the client and server! **For the first four DHCP messages** (DHCP Discover/Offer/Request/ACK), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram, also indicate the source and destination port numbers that can be found in the UDP segment header. What is the IP address of the DHCP server?
 - b. What is the value of the Transaction-ID **in the first four DHCP messages** (DHCP Discover/Offer/Request/ACK)? What are the values of the Transaction-ID in the second set of messages (DHCP Request/ACK)? What is the purpose of the Transaction-ID field?
 - c. The DHCP server offers a specific IP address to the client with the DHCP Offer message. What IP address is the DHCP server offering to the host **in the first DHCP Offer message**? In addition, what

¹ The lab materials are adapted from the textbooks "Computer Networking – A Top-Down Approach" by James Kurose and Keith Ross and the materials provided with them. They can only be used by students who registered for this course. Reproduction outside of this course use is prohibited.

- are the router address, subnet mask, domain name, and Domain Name Server given in the DHCP Offer message?
- d. In the client's response (DHCP Request) to **the server's first DHCP Offer message**, does the client accept the offered IP address? How can you tell?
 - e. To release an allocated IP address, a client sends a DHCP Release message to the DHCP server. Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request? What would happen if the client's DHCP Release message is lost?
 3. Download the two trace files ***NAT_home_side.pcap*** and ***NAT_ISP_side.pcap*** from D2L. These trace files depict a scenario shown in Figure 1. A client PC in a home network sends a simple Web request to the main Google server that will serve up the main Google Webpage has IP address **64.233.169.104**. Within the home network, the home network router provides a NAT service. First, a Wireshark trace can be collected on the client PC in the home network. This file is called ***NAT_home_side.pcap***. Because we are also interested in the packets being sent by the NAT router into the ISP, a second trace file ***NAT_ISP_side.pcap*** can capture the packets from the home router into the ISP network. Client-to-server packets captured by Wireshark at this point will have undergone NAT translation.

Note that the time columns in the two trace files only show the time relative to the start of the corresponding captures. As the two captures did not start at the same time, their time columns were not synchronized. You cannot use the time columns to relate the packets in the two traces. Instead, you should look into the packet contents to determine whether two packets in the two traces are the same message before and after passing through the NAT router.

For the following questions asking for the time, they mean the time shown in the time columns of the traces.

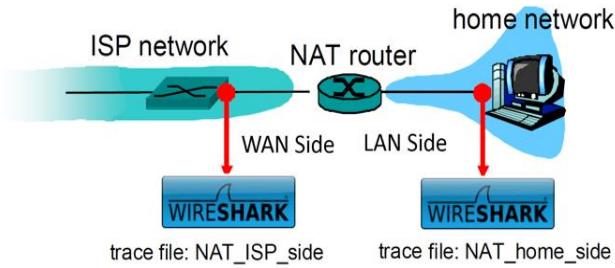


Figure 1. NAT trace collection scenario.

4. Use Wireshark to examine the trace file ***NAT_home_side.pcap*** and answer the following questions in your lab report. In order to display only those frames containing HTTP messages that are sent to/from this Google server, enter the expression "`http && ip.addr == 64.233.169.104`" (without quotes) into the Filter in Wireshark.
 - a. Consider now the HTTP GET sent from the client to the Google server (whose IP address is 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?
 - b. At what time is the corresponding HTTP 200 OK message for the above HTTP GET message received from the HTTP server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

- c. Recall that before an HTTP GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way handshake. (Note: To find these segments you will need to clear the *Filter* expression you entered above and enter the filter “tcp” in the *Filter*.)
- At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the HTTP GET sent at time 7.109267? What are the source and destination IP addresses and source and destination ports for the TCP SYN segment?
 - What are the source and destination IP addresses and source and destination ports of the TCP SYN/ACK sent in response to the TCP SYN? At what time is this TCP SYN/ACK sent from the server?
 - What are the source and destination IP addresses and source and destination ports of the TCP ACK segment sent at the end of the three-way handshake. At what time is this TCP ACK sent from the client?
5. Use Wireshark to examine the trace file ***NAT_ISP_side.pcap*** and answer the following questions in your lab report. In order to display only those frames containing HTTP messages that are sent to/from this Google server, enter the expression “http && ip.addr == 64.233.169.104” (without quotes) into the Filter in Wireshark.
- a. In the trace file *NAT_ISP_side.pcap*, find the HTTP GET message was sent from the client to the Google server (whose IP address is 64.233.169.104) at time 7.109267 (where t=7.109267 is time at which this was sent as recorded in the trace file *NAT_home_side.pcap*). At what time does this message appear in the trace file *NAT_ISP_side.pcap*? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET (as recording in the trace file *NAT_ISP_side.pcap*)? Which of these fields are the same as, and which are different from, your answer to question 4.a) above?
 - b. In the trace file *NAT_ISP_side.pcap*, at what time is the first HTTP 200 OK message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message? Which of these fields are the same as, and which are different from, your answer to question 4.b) above?
 - c. In the trace file *NAT_ISP_side.pcap*, answer the same question as in 4.c)? Which of these fields are the same as, and which are different from, your answer to question 4.c) above?
 - d. Using your answers to the above questions, fill in the NAT translation table entries for the HTTP connection considered above.

NAT Translation Table	
WAN Side	LAN Side

LAB REPORT:

Go through the above lab activities and **write a report answering the questions listed items 2, 4, and 5.**

- Please follow the lab report template in Microsoft Word posted on D2L. The template includes one example answer for a question listed in item 4. Once you are done, convert your Word document into a single PDF file and submit it to the corresponding dropbox on D2L by the due time.
- In your report, attach a screenshot of the packet trace to indicate where you find the answer to each question. You can capture the display in Wireshark using a screen capture software and then annotate the output packet trace with color markups to show the information related to your answers.