University of New Brunswick
Faculty of Computer Science

____ /____
Mark

CS 3873 – Net-Centric Computing
Winter 2017

Course Work: Lab 3

Assignment / Lab Number

Date: Mar. 13, 2017

1234567 — **Student Number**

Song, Wei — **Last, First Name (PRINT)**

[Mandatory] "I warrant that this is my own work." Wei Song

(Signature)

[Optional] "I hereby give my permission for this work to be used only (with my name and identifying information removed) for UNB Faculty of Computer Science program accreditation purposes."

W. S.

(Initials)

Report for Lab Exercise 3: Examining DHCP and NAT with Wireshark

Name: Wei Song Student Number: 1234567

Date: March 13, 2017

LAB ACTIVITIES:

In this lab, we used Wireshark to examine two important network-layer protocols for address administration: DHCP and NAT.

ANSWERS TO LAB QUESTIONS:

11. The following questions are answered by referring to file ***dhcp-ethereal-trace-1.pcap*** I downloaded from D2L:

    1) 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?

    Answer: Referring to the following figures, I have the answer in the following table. The IP address of the DHCP server is .

Message	Source IP	Dest IP	Source Port	Dest Port
DHCP Discover				
DHCP Offer				
DHCP Request				
DHCP ACK				

2) 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?

Answer:

3) 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 are the router address, subnet mask, domain name, and Domain Name Server given in the `DHCP Offer` message?

Answer:

4) 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?

Answer:

5) Explain the purpose of the lease time. How long is the lease time in your examined trace file?

Answer:

6) What is the purpose of the `DHCP Release` message? 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?

Answer:

LAB ACTIVITIES – PART 2:

13. 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.

    1) 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`?

    Answer:

2) 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?

Answer:

3) 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?

Answer: Referring to the following figures, I get the answers to the above questions in the following table:

Segment	Time	Source IP	Dest IP	Source Port	Dest Port
TCP SYN					
TCP SYN/ACK					
TCP ACK					

14. 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.

    1) 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 13.1) above?

    Answer:

    2) 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 13.2) above?

    Answer

3) In the trace file *NAT_ISP_side.pcap*, answer the same question as in 13.3)? Which of these fields are the same, and which are different from, your answer to question 13.3) above?

Answer: Referring to Fig. xxx, I get the answers to the above questions in the following table. The fields highlighted in red are different from the answers to question 13.3).

Segment	Time	Source IP	Dest IP	Source Port	Dest Port
TCP SYN					
TCP SYN/ACK					
TCP ACK					

4) 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