**CS 3873: Net-Centric Computing**

Lab 3: Examining DHCP and NAT with Wireshark

Student Name: Mahmoud Moustafa Student Number: 3648276

**[Mandatory]** Declaration: “I warrant that this is my own work.”

Signed by Mahmoud Moustafa

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

Signed by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Report for Lab Exercise 3:

Examining DHCP and NAT with Wireshark

**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:**

The following gives you one example on how to draft your answer to the lab questions.

**ANSWERS TO LAB QUESTIONS:**

1. The following questions are answered by referring to file ***dhcp-ethereal-trace-1.pcap*** I downloaded from D2L:
2. 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 192.168.1.1.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Message | Source Address | Destination Address | Source Port | Destination Port |
| DHCP Discover | 0.0.0.0 | 255.255.255.255 | 68 | 67 |
| DHCP Offer | 192.168.1.1 | 255.255.255.255 | 67 | 68 |
| DHCP Request | 0.0.0.0 | 255.255.255.255 | 68 | 67 |
| DHCP ACK | 192.168.1.1 | 255.255.255.255 | 67 | 68 |

Graphical user interface, application

Description automatically generated

Fig. 1. DHCP Discover.

Graphical user interface, application

Description automatically generated Fig. 2. DHCP Offer.

Graphical user interface, application

Description automatically generated

Fig. 3. DHCP Request.

Graphical user interface, application

Description automatically generated

Fig. 4. DHCP ACK.

1. 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?  
     
   According to Fig.5, the value of the Transaction-ID in the first four DHCP messages (DHCP Discover/Offer/Request/ACK) is 

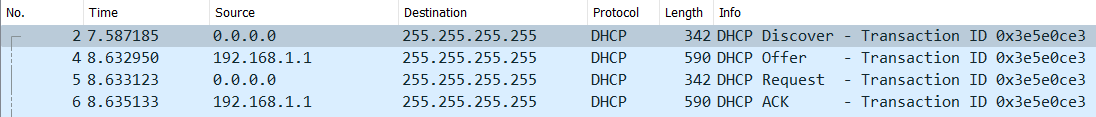


Fig.5 Transaction IDs of the first four DHCP messages

According to Fig.6 the values of the Transaction-ID in the second set of messages (DHCP Request/ACK) is 



Fig.6. Transaction IDs of the second set of DHCP messages

The purpose of the Transaction-ID is that the host can differentiate between the different requests made by the user.

1. 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?  
     
   According to Fig.7, the IP address offered to the host in the first DHCP Offer message is .

Graphical user interface, application, table

Description automatically generated

Fig.7. the IP address offered to the host in the first DHCP message

According to Fig.8 the router address is , subnet mask is , domain name is , and the Domain Name Server is .

Graphical user interface, table

Description automatically generated

Fig.8. The router address, subnet mask, domain name, and Domain Name Server

1. 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?

According to Fig.9, the client has accepted the offered IP Address. You can tell that it matches the IP address in the previous offer message.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, table

Description automatically generated with medium confidence

Fig.9 Response to offered IP Address

1. 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?

The server does not send an ACK of the receipt of the client’s DHCP Release message. If the client’s DHCP Release message is lost the client will release the IP address, however, the server will not assign that IP address to someone else until the lease time expires.

1. 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?

According to Fig.10,

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Message | Source Address | Destination Address | Source Port | Destination Port |
| HTTP Get | 192.168.1.100 | 64.233.169.104 | 4335 | 80 |

Graphical user interface, application, table

Description automatically generated

Fig.10. IP addresses and Ports

* 1. 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?

According to Fig.11. Time OK message was received, . The source and destination IP addresses and TCP source and destination ports have the answer in the following table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Message | Source Address | Destination Address | Source Port | Destination Port |
| HTTP 200 OK | 64.233.169.104 | 192.168.1.100 | 80 | 4335 |

Graphical user interface, application

Description automatically generated

`

Fig.11

* 1. 1. - 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?

According to fig.12, SYN segment time was sent at  and the source and destination IP addresses and source and destination ports for the TCP SYN segment are as follows.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Message | Source Address | Destination Address | Source Port | Destination Port |
| TCP SYN |  |  |  |  |

Text

Description automatically generated with medium confidence

Fig.12

* + 1. 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?

According to Fig.13, the source and destination IP addresses and source and destination ports of the TCP SYN/ACK sent in response to the TCP SYN are as follows. And the time this TCP SYN/ACK is sent from the server is .

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Message | Source Address | Destination Address | Source Port | Destination Port |
| TCP SYN/ACK |  |  |  |  |

Text

Description automatically generated with medium confidence

Fig.13

* + 1. 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?

According to Fig.14, 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 are as follows. The time this TCP ACK sent from the client is .

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Message | Source Address | Destination Address | Source Port | Destination Port |
| TCP ACK |  |  |  |  |

Graphical user interface, application

Description automatically generated

Fig.14

1. NAT\_ISP\_side.pcap
   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 4.a) above?

According to fig. 15, the message appears in the trace file at  and the source and destination IP addresses and TCP source and destination ports on the IP datagram is as follows. The source address and time are the different fields. All the rest (destination address and port and source port) are the same.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Message | Source Address | Destination Address | Source Port | Destination Port |
| HTTP GET |  |  |  |  |

Graphical user interface, application

Description automatically generated

Fig.15

* 1. 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?

According to fig.16, the time the first HTTP 200 OK message received from the Google server is . The source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message are as follows. The destination address and time fields are different. All the other fields (source address and port and destination port) are the similar.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Message | Source Address | Destination Address | Source Port | Destination Port |
| HTTP 200 OK |  |  |  |  |

Table

Description automatically generated with low confidence

Fig.16

* 1. 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?
     1. According to fig.17, SYN segment time was sent at  and the source and destination IP addresses and source and destination ports for the TCP SYN segment are as follows. The source address and time fields are the same. All the other fields (destination address and port and source port) are similar.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Message | Source Address | Destination Address | Source Port | Destination Port |
| TCP SYN |  |  |  |  |

Graphical user interface, text, application

Description automatically generated  
Fig17

* + 1. 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?

According to Fig.18, the source and destination IP addresses and source and destination ports of the TCP SYN/ACK sent in response to the TCP SYN are as follows. And the time this TCP SYN/ACK is sent from the server is . The destination address and time fields are different. All the other (source address and port and destination port) fields are similar.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Message | Source Address | Destination Address | Source Port | Destination Port |
| TCP SYN/ACK |  |  |  |  |

Graphical user interface

Description automatically generated with medium confidence

FIG18

* + 1. 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?

According to Fig.19, 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 are as follows. The time this TCP ACK sent from the client is . The source address and time fields are the same. All the other fields (destination address and port and source port) are similar.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Message | Source Address | Destination Address | Source Port | Destination Port |
| TCP ACK |  |  |  |  |

A picture containing text

Description automatically generated

Fig19



|  |  |
| --- | --- |
| NAT Translation Table | |
| WAN Side | LAN Side |
| ,4335 | ,4335 |