CS 3873: Net-Centric Computing
Lab 5: Examining DHCP and NAT with Wireshark

Student Name: _Adrian Freeman__ Student Number: __3661616___

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

Signed by _Adrian Freeman__

[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 _Adrian Freeman__

Report for Lab Exercise 5:
Examining DHCP and NAT with Wireshark

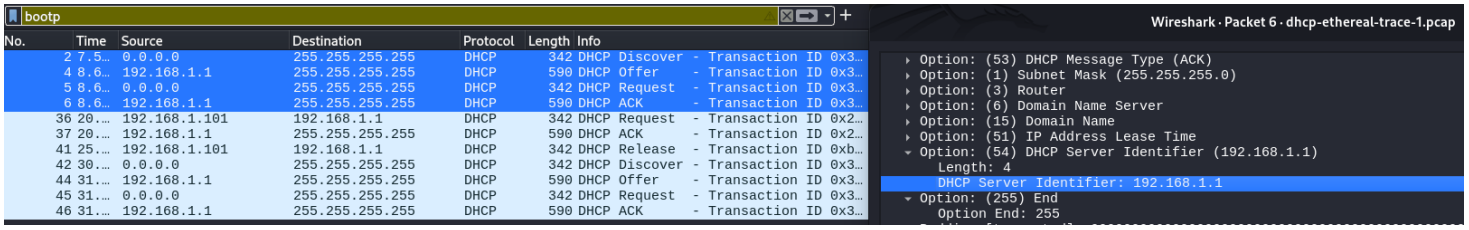
ANSWERS TO LAB QUESTIONS:

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

   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?

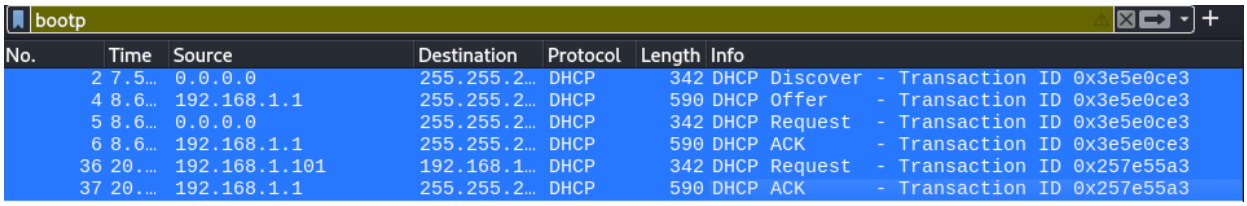
   Referring to the following figures, I have the answer in the following table. The IP address of the DHCP server is _192.168.1.1_.

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



   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?

   The transaction ID for the first four DHCP messages is 0x3e5e0ce3. The ID for the second set is 0x257e55a3. The purpose of the ID is to help identify and match requests and responses, so that we know, for example, which ACK belongs to which Request.



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

IP Address Offered	Router Address	Subnet Mask	Domain Name	Domain Name Server
192.168.1.101	192.168.1.1	255.255.255.0	ne2.client2.attbi.com	63.240.76.19 and 204.127.198.19

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?

Yes, because the client is now requesting the offered IP address. 192.168.1.101

```
▾ Option: (50) Requested IP Address (192.168.1.101)
    Length: 4
    Requested IP Address: 192.168.1.101
```

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?

The DHCP server does not send an ACK in response to a Release. If the release message is lost, the DHCP server will retain the lease until it is expired. Until then it will be marked as in use.

```
41 25.0738… 192.168.1.101   192.168.1.1       DHCP    342 DHCP Release  - T
42 30.8691… 0.0.0.0         255.255.255.255   DHCP    342 DHCP Discover - T
44 31.9081… 192.168.1.1     255.255.255.255   DHCP    590 DHCP Offer    - T
45 31.9083… 0.0.0.0         255.255.255.255   DHCP    342 DHCP Request  - T
```

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 .

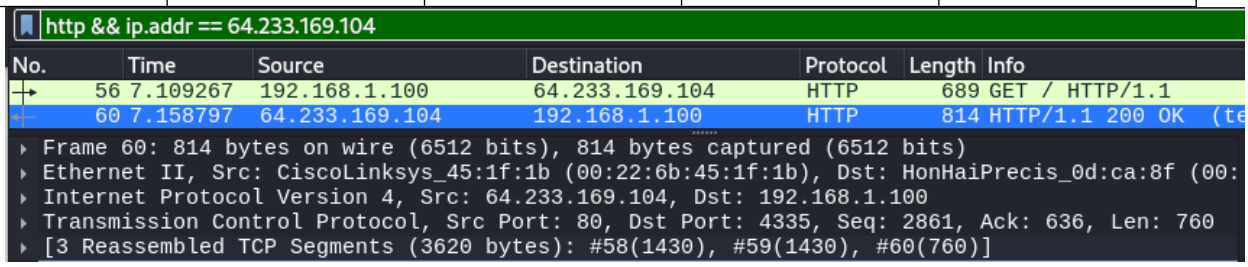
a. Consider now the HTTP GET sent from the client to the Google server (whose IP address is 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

Source IP	Destination IP	Source Port	Destination Port
192.168.1.100	64.233.169.104	4335	80

```
http && ip.addr == 64.233.169.104
No.   Time    Source          Destination       Protocol  Length Info
   56 7.109… 192.168.1.100    64.233.169.104    HTTP       689 GET / HTTP/1.1
▸ Frame 56: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
▸ Ethernet II, Src: HonHaiPrecis_0d:ca:8f (00:22:68:0d:ca:8f), Dst: CiscoLinksys_45:1f:1b (00:
▸ Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104
▸ Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
```

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?

Time Received	Source IP	Destination IP	Source Port	Destination Port
7.158797	64.233.169.104	192.168.1.100	80	4335



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.)

i. 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?

Time Received	Source IP	Destination IP	Source Port	Destination Port
7.075657	192.168.1.100	64.233.169.104	4335	80

ii. 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?

Time Received	Source IP	Destination IP	Source Port	Destination Port
7.108986	64.233.169.104	192.168.1.100	80	4335

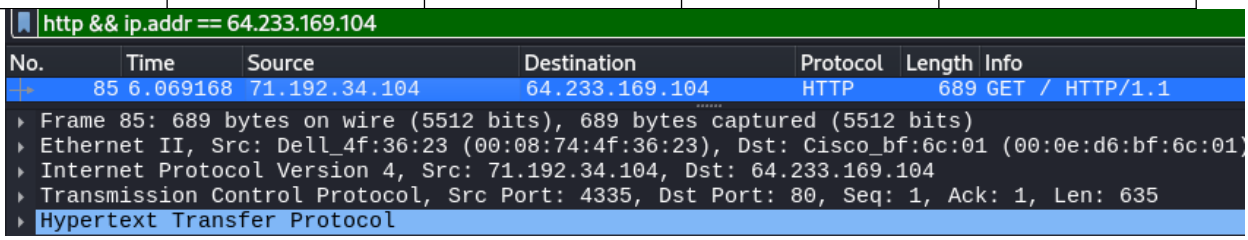
iii. What are the source and destination IP addresses and source and destination ports of the TCP ACK segment sent at the end of the three-way handshake. At what time is this TCP ACK sent from the client?

Time Received	Source IP	Destination IP	Source Port	Destination Port
7.109053	192.168.1.100	64.233.169.104	4335	80

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?

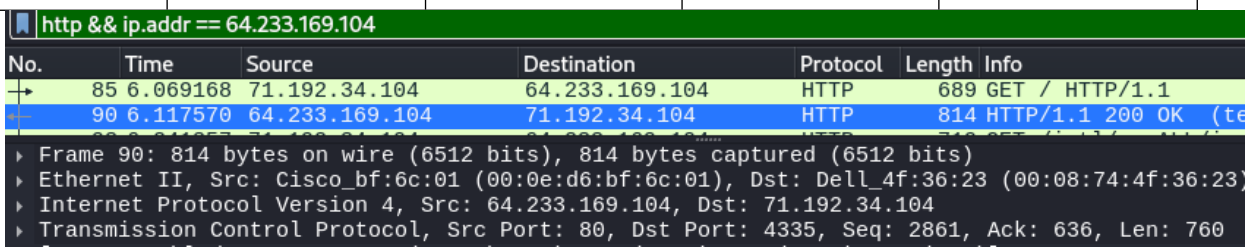
Time Received	Source IP	Destination IP	Source Port	Destination Port
6.069168	71.192.34.104	64.233.169.104	4335	80



The only differences from 4.a) are the time received, and the source IP. As the source IP on the home side was the local IP address. The rest, Destination IP, and the Source and Destination Ports, are the

   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?

Time Received	Source IP	Destination IP	Source Port	Destination Port
6.117570	64.233.169.104	71.192.34.104	80	4335



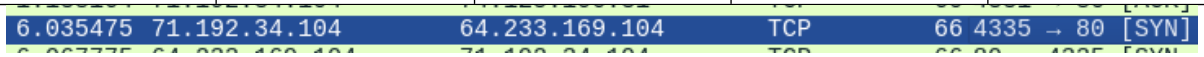
The only differences were the time received as well as the destination IP. The rest is the same.

   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?

   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.)

i. 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?

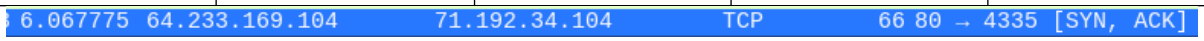
Time Received	Source IP	Destination IP	Source Port	Destination Port
6.035475	71.192.34.104	64.233.169.104	4335	80



The only differences are the time and the source IP. The rest is the same

ii. 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?

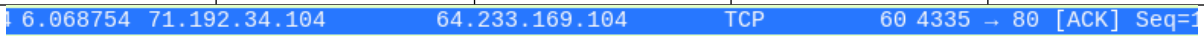
Time Received	Source IP	Destination IP	Source Port	Destination Port
6.067775	64.233.169.104	71.192.34.104	80	4335



The only differences are the time and destination IP. The rest is the same.

iii. 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?

Time Received	Source IP	Destination IP	Source Port	Destination Port
6.068754	71.192.34.104	64.233.169.104	4335	80



The only differences are the time received and the source IP. The rest is the same.

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
71.192.34.104:4335	192.168.1.100:4335