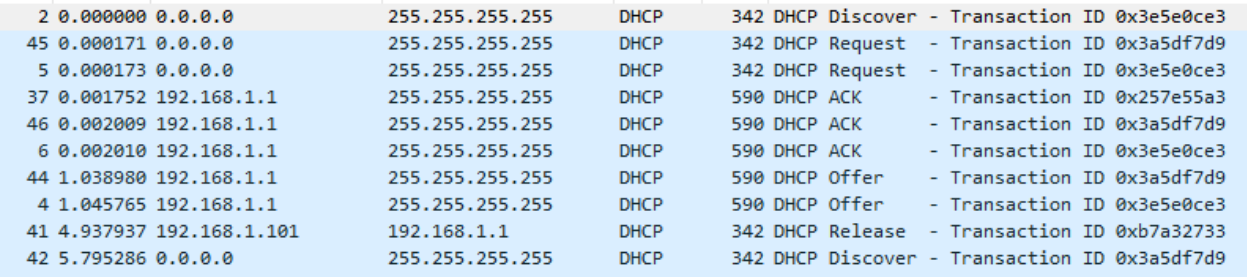
Lab Activities Part 1

Question 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's server?



```
  2 0.000000 0.0.0.0          255.255.255.255    DHCP     342 DHCP Discover - Transaction ID 0x3e5e0ce3
 45 0.000171 0.0.0.0          255.255.255.255    DHCP     342 DHCP Request  - Transaction ID 0x3a5df7d9
  5 0.000173 0.0.0.0          255.255.255.255    DHCP     342 DHCP Request  - Transaction ID 0x3e5e0ce3
 37 0.001752 192.168.1.1      255.255.255.255    DHCP     590 DHCP ACK      - Transaction ID 0x257e55a3
 46 0.002009 192.168.1.1      255.255.255.255    DHCP     590 DHCP ACK      - Transaction ID 0x3a5df7d9
  6 0.002010 192.168.1.1      255.255.255.255    DHCP     590 DHCP ACK      - Transaction ID 0x3e5e0ce3
 44 1.038980 192.168.1.1      255.255.255.255    DHCP     590 DHCP Offer    - Transaction ID 0x3a5df7d9
  4 1.045765 192.168.1.1      255.255.255.255    DHCP     590 DHCP Offer    - Transaction ID 0x3e5e0ce3
 41 4.937937 192.168.1.101    192.168.1.1        DHCP     342 DHCP Release  - Transaction ID 0xb7a32733
 42 5.795286 0.0.0.0          255.255.255.255    DHCP     342 DHCP Discover - Transaction ID 0x3a5df7d9
```

Message	Source IP	Dest IP	Source Port	Dest 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..68.1.1	255.255.255.255	67	

What is the IP address of the DHCP server?

192.168.1.1

Question 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?

Message	Transaction ID
DHCP Discover	0x3e5e0ce3
DHCP Offer	0x3e5e0ce3
DHCP Request (first)	0x3e5e0ce3
DHCP ACK (first)	0x3e5e0ce3
DHCP Request (second)	0x257e55a3
DHCP ACK (second)	0x257e55a3

The transaction ID's purpose is to allow the server to differentiate between different requests made by the user.

Question 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.

```
▾ Option: (1) Subnet Mask (255.255.255.0)
      Length: 4
      Subnet Mask: 255.255.255.0
▾ Option: (3) Router
      Length: 4
      Router: 192.168.1.1
▾ Option: (6) Domain Name Server
      Length: 8
      Domain Name Server: 63.240.76.19
      Domain Name Server: 204.127.198.19
▾ Option: (15) Domain Name
      Length: 22
      Domain Name: ne2.client2.attbi.com
▾ Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: (86400s) 1 day
▾ Option: (54) DHCP Server Identifier (192.168.1.1)
      Length: 4
      DHCP Server Identifier: 192.168.1.1
```

The server is offering 192.168.1.101.
The router address is 192.168.1.1.
The subnet mask is 255.255.255.0.
The domain name is ne2.client.attbi.com.
The domain name server is 63.240.76.19 or 204.127.198.19.

Question 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?

The offered IP address was accepted because the client sent back a request message for the address.

Question 5:

Explain the purpose of the lease time. How long is the lease time in your experiment?

The lease time's purpose is to tell the client how long they can use the specific IP address assigned by the server before they will have to be assigned a new one.
The lease time given for this experiment is 86400 s or 1 day.

Question 6:

What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgement of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?

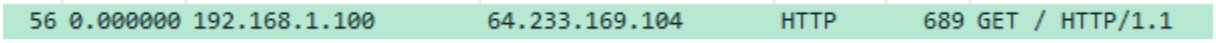
The purpose of the DHCP release message is to release the IP address back to the server.
There is no verification that the release message has been received by the server.
If the DHCP release message is lost, the client will release the IP address, but the server will wait for the client's lease on the address to expire first. While the server is waiting for the address, it won't reassign the address to anyone else.

Lab Activities Part 2

Question 1:

Consider now HTTP GET sent from the client to the Google server (whose IP address 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?

This message was sent at time 0.000000

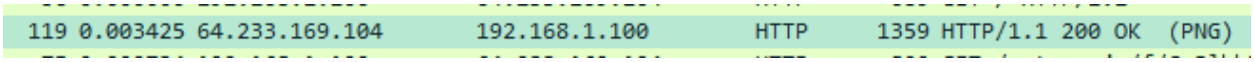


Source IP: 192.168.1.100
Dest. IP: 64.233.169.104
Source Port: 4335
Dest. Port: 80

Question 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.

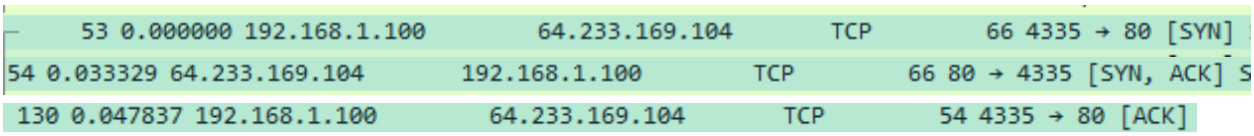
HTTP 200 OK message received at 0.003425. The source and destination IP addresses and TCP port values will be the reverse from the last question. (Request going the other way).



Source IP: 64.233.169.104
Dest. IP: 192.168.1.100
Source Port: 80
Dest. Port: 4335

Question 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?

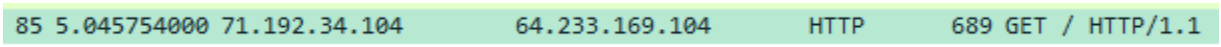


Segment	Time	Source IP	Dest IP	Source Port	Dest Port
TCP SYN	0.000000	192.168.1.100	64.233.169.104	4335	80
TCP SYN/ACK	0.033329	64.233.169.104	192.168.1.100	80	4335
TCP ACK	0.047837	192.168.1.100	64.233.169.104	4335	80

Lab Activities Part 3:

Question 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 fileNAT_ISP_side.pcap)? Which of these fields are the same as, and which are different from, your answer to (question 13.1) above.

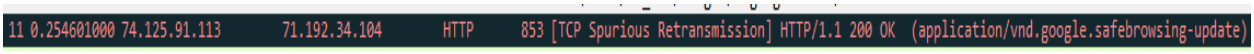


This message shows up in the trace at time 5.045754000
The source IP address is 71.192.34.104.
The destination IP address is 64.233.169.10.
The source port is 4335.
The destination port is 80.

Compared to the previous section (Lab activities part 2 question 1), these fields vary in timing, and the IP address are different as the server isn't communicating with the client at that moment.

Question 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?

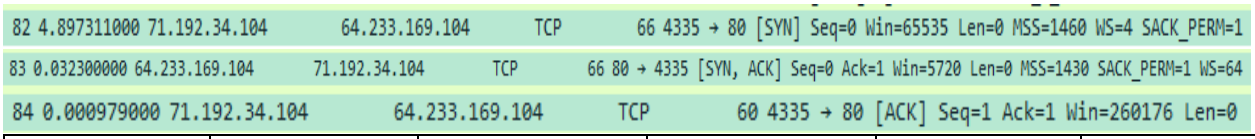


This message shows up in the trace at time 0.254601000.
The source IP address is 74.125.91.113.
The destination IP address is 71.192.34.104.
The source port is 80.
The destination port is 4330.

Compared to the previous answers (Lab activities part 2 question 2), our fields have changed only in the time and addresses. The port numbers stay the same because those are the connected ports for communication.

Question 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?



Segment	Time	Source IP	Dest IP	Source Port	Dest Port	
TCP SYN	4.897311000	71.192.34.104	64.233.169.104	4335	80	
TCP SYN/ACK	0.032300000	64.233.169.104	71.192.34.104	80	4335	
TCP ACK	0.000979000	71.192.34.104	64.233.169.104	4335	80	

Compared to the previous question (Lab Activities Part 2 question 3), our fields change only in the time, and the source and destination IP addresses. Highlighted values are different than previous answers.

Question 4:

Using your answers to the above questions, fill in the NAT translation table entries for the HTTP connection considered above.

Net Translation Table	
Wan side	Lan side
71.192.34.104, 4335	192.168.1.100, 4335