Department of Electrical Engineering, UET Lahore
EE432 Computer Networks Lab

Course Instructor: Dr. Naveed Nawaz	Dated: 16/10/2024
Session: Spring 2024	Semester: 7th

LAB 9: Dynamic Host Configuration Protocol of Network Layer

Name	Roll. No.	Report Marks (10)	Viva Marks (5)	Total Marks (15)
Ayesha Ahmad	2021-EE-052			

Signature: ______________________________

Dynamic Host Configuration Protocol

Objectives

In this lab, we'll take a quick look at the Dynamic Host Configuration Protocol, DHCP, which 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. We'll be studying the DHCP Discover, Offer, Request and ACK messages.

Instructions

1. Read carefully before starting the lab.
2. These exercises are to be done individually.
3. You are supposed to provide the answers to the questions listed at the end of this document and upload the completed report to your course's LMS site.
4. Avoid plagiarism by copying from the Internet or from your peers. You may refer to source/ text but you must paraphrase the original work. Your submitted work should be written by yourself.
5. Complete the lab half an hour before the lab ends.
6. At the end of the lab, a viva will be conducted to evaluate your understanding.

Gathering a Packet Trace

The first two steps in the DHCP protocol (using the Discover and Offer messages) are optional (in the sense that they need not always be used when, for example, a new IP address is needed, or an existing DHCP address is to be renewed); the Request and ACK messages are not. In order to collect a trace that will contain all four DHCP message types, we'll need to take a few command line actions on PC.

1. In a command-line window enter the following command:

   ```
   > ipconfig /release
   ```

   This command will cause your PC to give up its IP address.
2. Start up Wireshark.
3. In the command-line window enter the following command:

   ```
   > ipconfig /renew
   ```

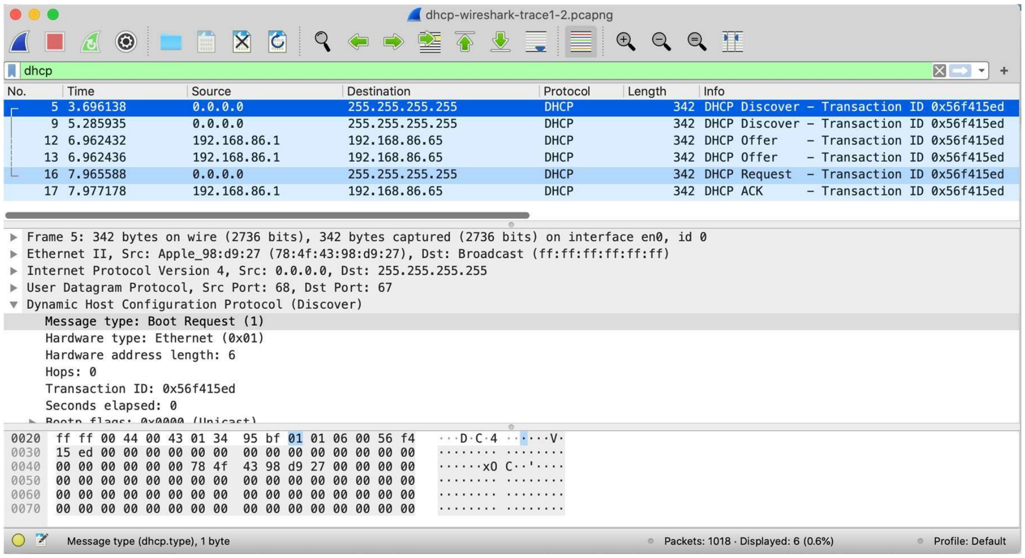
   This will cause the DHCP protocol to request and receive an IP address and other information from a DHCP server.
4. After waiting for a few seconds, stop Wireshark capture.

After stopping Wireshark capture in step 4, you should take a peek in your Wireshark window to make sure you've actually captured the packets that we're looking for. If you enter "dhcp" into the display filter field (as shown in the light green field in the top left of Figure 1), your screen (on a Mac) should look similar to Figure 1.

If you're unable to run Wireshark on a live network connection, are unable to capture all four DHCP messages, or are assigned to do so by your instructor, you can use the Wireshark trace file, dhcp-wireshark-trace1-1.pcapng[1] that we've gathered following the steps above on one of the

[1] You can download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces-8.1.zip and extract the trace file dhcp-wireshark-trace1-1.pcapng. These trace files can be used to answer these Wireshark lab questions without actually capturing packets on your own. Each trace was made using Wireshark running on one of the author's computers, while performing the steps indicated in the Wireshark lab. Once you've downloaded a trace file, you can load it into Wireshark and view the trace using the File pull down menu, choosing Open, and then selecting the trace file name.

author's computers. You may well find it valuable to download this trace even if you've captured your own trace and use it, as well as your own trace, as you explore the questions below.



```
dhcp
No.   Time      Source         Destination       Protocol  Length  Info
    5 3.696138  0.0.0.0        255.255.255.255   DHCP         342  DHCP Discover - Transaction ID 0x56f415ed
    9 5.285935  0.0.0.0        255.255.255.255   DHCP         342  DHCP Discover - Transaction ID 0x56f415ed
   12 6.962432  192.168.86.1   192.168.86.65     DHCP         342  DHCP Offer    - Transaction ID 0x56f415ed
   13 6.962436  192.168.86.1   192.168.86.65     DHCP         342  DHCP Offer    - Transaction ID 0x56f415ed
   16 7.965588  0.0.0.0        255.255.255.255   DHCP         342  DHCP Request  - Transaction ID 0x56f415ed
   17 7.977178  192.168.86.1   192.168.86.65     DHCP         342  DHCP ACK      - Transaction ID 0x56f415ed

▶ Frame 5: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
▶ User Datagram Protocol, Src Port: 68, Dst Port: 67
▼ Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x56f415ed
    Seconds elapsed: 0
  ▶ Bootp flags: 0x0000 (Unicast)

0020  ff ff 00 44 00 43 01 34  95 bf 01 01 06 00 56 f4   ···D·C·4 ······V·
0030  15 ed 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 78 4f  43 98 d9 27 00 00 00 00   ······xO C··'····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········

Message type (dhcp.type), 1 byte        Packets: 1018 · Displayed: 6 (0.6%)        Profile: Default
```

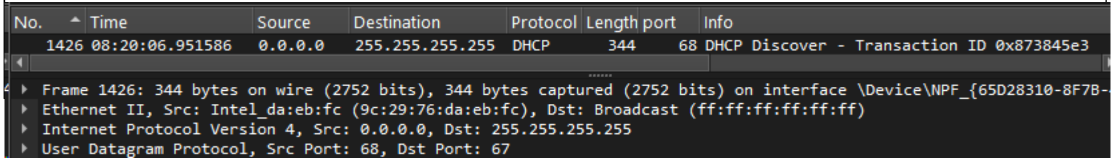
Figure 1: Wireshark display, showing the capture of DHCP Discover, Offer, Request and ACK messages

Tasks

Let's start by looking at the DHCP Discover message. Locate the IP datagram containing the first Discover message in your trace.

1. Is this DHCP Discover message sent out using UDP or TCP as the underlying transport protocol?

DHCP Discover uses UDP as the underlying transport protocol.

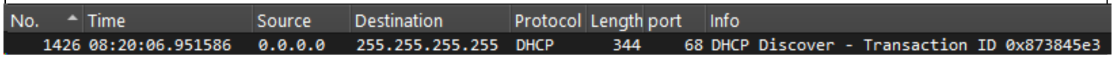


```
No.   Time             Source   Destination       Protocol Length port  Info
 1426 08:20:06.951586  0.0.0.0  255.255.255.255   DHCP     344          68 DHCP Discover - Transaction ID 0x873845e3

▶ Frame 1426: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\NPF_{65D28310-8F7B-
▶ Ethernet II, Src: Intel_da:eb:fc (9c:29:76:da:eb:fc), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
▶ User Datagram Protocol, Src Port: 68, Dst Port: 67
```

2. What is the source IP address used in the IP datagram containing the Discover message? Is there anything special about this address? Explain.

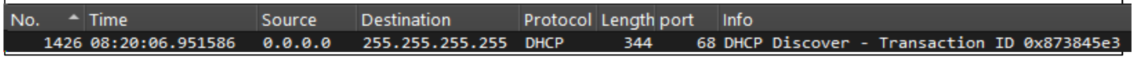
The Source IP address of DHCP Discover is **0.0.0.0,** which is used for Loop Back.



```
No.   Time             Source   Destination       Protocol Length port  Info
 1426 08:20:06.951586  0.0.0.0  255.255.255.255   DHCP     344          68 DHCP Discover - Transaction ID 0x873845e3
```

3. What is the destination IP address used in the datagram containing the Discover message. Is there anything special about this address? Explain.

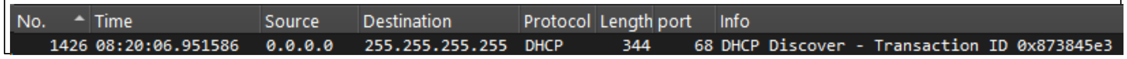
The Destination IP address of DHCP Discover is **255.255.255.255,** which is used for Broadcast.



```
No.   Time             Source   Destination      Protocol Length port  Info
 1426 08:20:06.951586  0.0.0.0  255.255.255.255  DHCP     344     68 DHCP Discover - Transaction ID 0x873845e3
```

4. What is the value in the transaction ID field of this DHCP Discover message?

The transaction ID of DHCP Discover is **0x873845e3**.

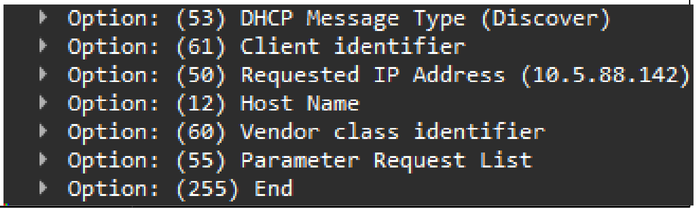


```
No.   Time             Source   Destination      Protocol Length port  Info
 1426 08:20:06.951586  0.0.0.0  255.255.255.255  DHCP     344     68 DHCP Discover - Transaction ID 0x873845e3
```

5. Now inspect the options field in the DHCP Discover message. What are five pieces of information (beyond an IP address) that the client is suggesting or requesting to receive from the DHCP server as part of this DHCP transaction?

The 5 pieces of information except Requested IP Address are:

DHCP message Type
Client Identifier
Host Name
Vendor Class Identifier
Parameter Request List

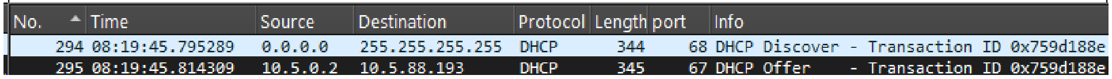


```
▸ Option: (53) DHCP Message Type (Discover)
▸ Option: (61) Client identifier
▸ Option: (50) Requested IP Address (10.5.88.142)
▸ Option: (12) Host Name
▸ Option: (60) Vendor class identifier
▸ Option: (55) Parameter Request List
▸ Option: (255) End
```

Now let's look at the DHCP Offer message. Locate the IP datagram containing the DHCP Offer message in your trace that was sent by a DHCP server in the response to the DHCP Discover message that you studied in questions 1-5 above.

6. How do you know that this Offer message is being sent in response to the DHCP Discover message you studied in questions 1-5 above?

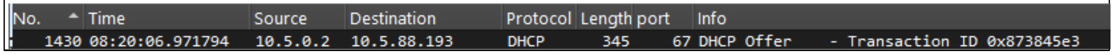
This Offer was sent in response to the Discover studied as their Transaction ID is the same. The Source Port of the Discover is the Destination port of the Offer.



```
No.   Time             Source   Destination      Protocol Length port  Info
  294 08:19:45.795289  0.0.0.0  255.255.255.255  DHCP     344     68 DHCP Discover - Transaction ID 0x759d188e
  295 08:19:45.814309  10.5.0.2 10.5.88.193      DHCP     345     67 DHCP Offer    - Transaction ID 0x759d188e
```

7. What is the source IP address used in the IP datagram containing the Offer message? Is there anything special about this address? Explain.

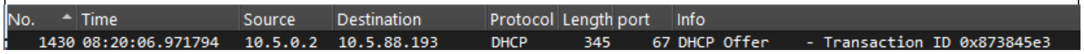
The Source IP address is 10.5.0.2, that is the DHCP Server Identifier.



```
No.   Time             Source   Destination   Protocol Length port  Info
 1430 08:20:06.971794  10.5.0.2 10.5.88.193   DHCP     345     67 DHCP Offer    - Transaction ID 0x873845e3
```

8. What is the destination IP address used in the datagram containing the Offer message? Is there anything special about this address? Explain. [Hint: Look at your trace carefully.

The Destination IP address is 10.5.88.193, and it is the IP address offered to the client. In the end, this becomes the IP address of the client as it Request is acknowledged.

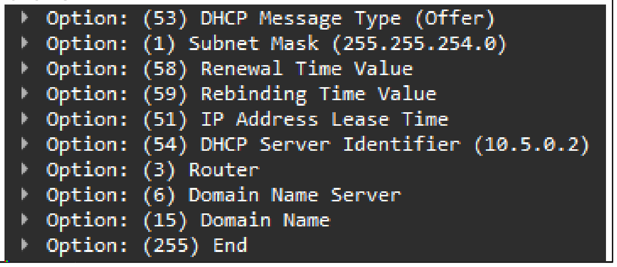


```
No.    Time             Source    Destination  Protocol Length port Info
  1430 08:20:06.971794  10.5.0.2  10.5.88.193  DHCP     345      67 DHCP Offer     - Transaction ID 0x873845e3
```

9. Now inspect the options field in the DHCP Offer message. What are five pieces of information that the DHCP server is providing to the DHCP client in the DHCP Offer message?

The 5 pieces of information provided are:

Renewal Time Value
Rebinding Time Value
IP Address Lease Time
Domain Name Server
Domain Name



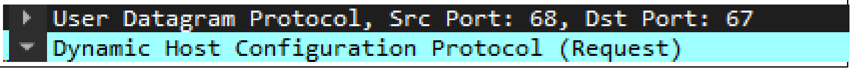
```
▸ Option: (53) DHCP Message Type (Offer)
▸ Option: (1) Subnet Mask (255.255.254.0)
▸ Option: (58) Renewal Time Value
▸ Option: (59) Rebinding Time Value
▸ Option: (51) IP Address Lease Time
▸ Option: (54) DHCP Server Identifier (10.5.0.2)
▸ Option: (3) Router
▸ Option: (6) Domain Name Server
▸ Option: (15) Domain Name
▸ Option: (255) End
```

It would appear that once the DHCP Offer message is received, that the client may have all of the information it needs to proceed. However, the client may have received OFFERs from multiple DHCP servers and so a second phase is needed, with two more mandatory messages – the client-toserver DHCP Request message, and the server-to-client DHCP ACK message is needed. But at least the client knows there is at least one DHCP server out there! Let's take a look at the DHCP Request message, remembering that although we've already seen a Discover message in our trace, that is not always the case when a DHCP request message is sent.

Locate the IP datagram containing the first DHCP Request message in your trace, and answer the following questions.

10. What is the UDP source port number in the IP datagram containing the first DHCP Request message in your trace? What is the UDP destination port number being used?

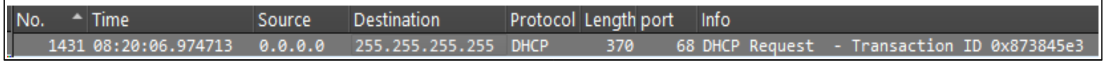
UDP Source Port Number	: 68
UDP Destination Port Number	: 67



```
▸ User Datagram Protocol, Src Port: 68, Dst Port: 67
▾ Dynamic Host Configuration Protocol (Request)
```

11. What is the source IP address in the IP datagram containing this Request message? Is there anything special about this address? Explain.

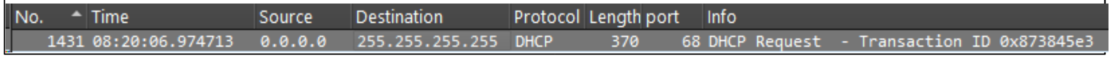
The Source IP address of DHCP Request is **0.0.0.0,** which is used for Loop Back.



```
No.    Time             Source   Destination      Protocol Length port Info
  1431 08:20:06.974713  0.0.0.0  255.255.255.255  DHCP     370      68 DHCP Request  - Transaction ID 0x873845e3
```

12. What is the destination IP address used in the datagram containing this Request message. Is there anything special about this address? Explain.

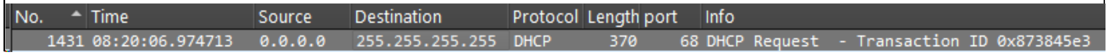
The Destination IP address of DHCP Request is **255.255.255.255,** which is used for Broadcast.



```
No.   Time             Source    Destination      Protocol Length port Info
 1431 08:20:06.974713  0.0.0.0   255.255.255.255  DHCP      370     68 DHCP Request  - Transaction ID 0x873845e3
```

13. What is the value in the transaction ID field of this DHCP Request message?

The transaction ID of the DHCP Request message is 0x873845e3.



```
No.   Time             Source    Destination      Protocol Length port Info
 1431 08:20:06.974713  0.0.0.0   255.255.255.255  DHCP      370     68 DHCP Request  - Transaction ID 0x873845e3
```

14. Does it match the transaction IDs of the earlier Discover and Offer messages?

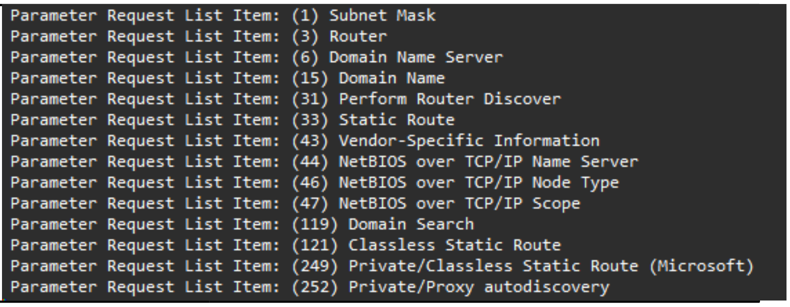
Yes, it matches as in a stream the transaction ID remains same.

15. Now inspect the options field in the DHCP Discover message and take a close look at the "Parameter Request List". The DHCP RFC notes that

> "The client can inform the server which configuration parameters the client is interested in by including the 'parameter request list' option. The data portion of this option explicitly lists the options requested by tag number."

What differences do you see between the entries in the 'parameter request list' option in this Request message and the same list option in the earlier Discover message?

The whole Parameter Request List is the same

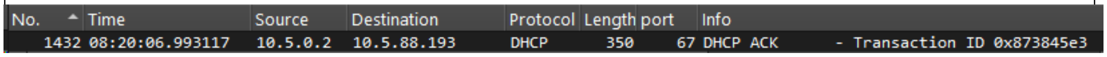


```
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (3) Router
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (31) Perform Router Discover
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (43) Vendor-Specific Information
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
Parameter Request List Item: (119) Domain Search
Parameter Request List Item: (121) Classless Static Route
Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
Parameter Request List Item: (252) Private/Proxy autodiscovery
```

Locate the IP datagram containing the first DHCP ACK message in your trace, and answer the following questions.

16. What is the source IP address in the IP datagram containing this ACK message? Is there anything special about this address? Explain.

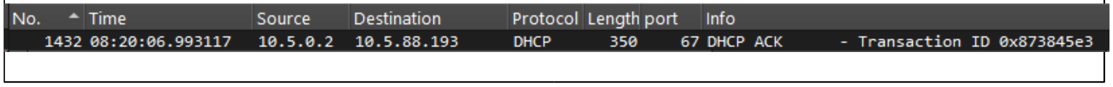
The Source IP address is 10.5.0.2, that is the DHCP Server Identifier.



```
No.  ^ Time             Source     Destination   Protocol Length port  Info
  1432 08:20:06.993117  10.5.0.2   10.5.88.193   DHCP     350      67 DHCP ACK      - Transaction ID 0x873845e3
```

17. What is the destination IP address used in the datagram containing this ACK message. Is there anything special about this address? Explain.

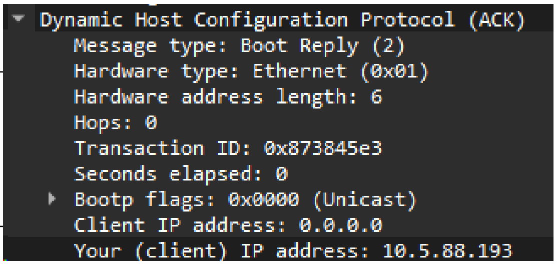
The Destination IP address is 10.5.88.193, and it is the IP address of the client as its Request is now acknowledged.



```
No.  ^ Time             Source     Destination   Protocol Length port  Info
  1432 08:20:06.993117  10.5.0.2   10.5.88.193   DHCP     350      67 DHCP ACK      - Transaction ID 0x873845e3
```

18. What is the name of the field in the DHCP ACK message (as indicated in the Wireshark window) that contains the assigned client IP address?

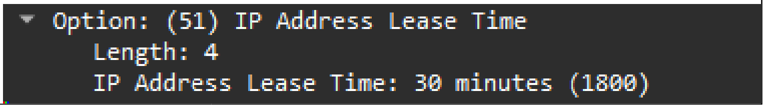
The Your (client) IP address field contains the assigned client IP address.



```
▾ Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x873845e3
    Seconds elapsed: 0
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.5.88.193
```

19. For how long a time (the so-called “lease time”) has the DHPC server assigned this IP address to the client?

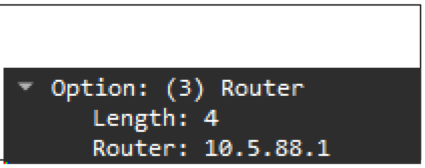
The IP Address is assigned for 30 minutes.



```
▾ Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: 30 minutes (1800)
```

20. What is the IP address (returned by the DHCP server to the DHCP client in this DHCP ACK message) of the first-hop router on the default path from the client to the rest of the Internet?

The IP Address of the Router is 10.5.88.1



```
▾ Option: (3) Router
    Length: 4
    Router: 10.5.88.1
```