USC EE450 Fall 2020

Lab #1 Report: DHCP

Zeyu Wang

Session 2

1. Abstract

In this lab, I examined and analyzed the DHCP configuration process of hosts on an public-network by using the Wireshark packet analyzer that runs on Windows, this configuration process including Server Discovery, IP lease Offer, Request and Acknowledgement.

ipconfig /release:

Select Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.18362.1082]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ipconfig /release

Windows IP Configuration

No operation can be performed on Local Area Connection* 9 while it has its media disconnected.
No operation can be performed on Local Area Connection* 10 while it has its media disconnected.
No operation can be performed on Ethernet 4 while it has its media disconnected.
```

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2601:140:509:f73b:f475:e449:80bd:da14
   Temporary IPv6 Address. . . . . . : 2601:140:509:f73b:2d2c:3c7a:78e9:762b
   Link-local IPv6 Address . . . . . : fe80::f475:e449:80bd:da14%17
   Default Gateway . . . . . . . . . : fe80::f63e:9dff:fe03:64bc%17
```

ipconfig /renew:

```
C:\WINDOWS\system32>ipconfig /renew

Windows IP Configuration

No operation can be performed on Local Area Connection* 9 while it has its media disconnected.
No operation can be performed on Local Area Connection* 10 while it has its media disconnected.
No operation can be performed on Ethernet 4 while it has its media disconnected.
```

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2601:140:509:f73b:f475:e449:80bd:da14
   Temporary IPv6 Address. . . . . . : 2601:140:509:f73b:2d2c:3c7a:78e9:762b
   Link-local IPv6 Address . . . . . : fe80::f475:e449:80bd:da14%17
   IPv4 Address. . . . . . . . . . . : 10.226.120.102
   Subnet Mask . . . . . . . . . . . : 255.252.0.0
   Default Gateway . . . . . . . . . : fe80::f63e:9dff:fe03:64bc%17
                                       10.224.0.1
```

2. Answers to questions in lab

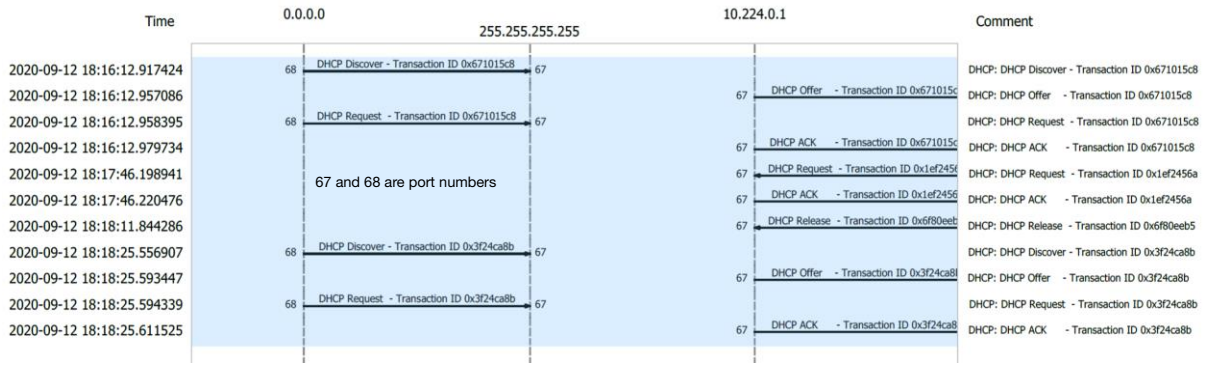
1) Are DHCP messages sent over UDP or TCP?

DHCP messages sent over UDP (User Datagram Protocl).

```
No.     Time                           Source                Destination           Protocol Length Info
     81 2020-09-12 18:16:12.917424     0.0.0.0               255.255.255.255       DHCP     342    DHCP Discover - Transaction ID 0x671015c8
Frame 81: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{AD8285C9-616C-4D09-9F9A-A134FBBD9253}, id
0
Ethernet II, Src: Microsof_d1:59:58 (f0:6e:0b:d1:59:58), 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
    Source Port: 68
    Destination Port: 67
    Length: 308
    Checksum: 0x2595 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 11]
    [Timestamps]
Dynamic Host Configuration Protocol (Discover)
No.     Time                           Source                Destination           Protocol Length Info
     82 2020-09-12 18:16:12.957086     10.224.0.1            10.226.120.102        DHCP     320    DHCP Offer    - Transaction ID 0x671015c8
Frame 82: 320 bytes on wire (2560 bits), 320 bytes captured (2560 bits) on interface \Device\NPF_{AD8285C9-616C-4D09-9F9A-A134FBBD9253}, id
0
Ethernet II, Src: BenuNetw_03:64:bc (f4:3e:9d:03:64:bc), Dst: Microsof_d1:59:58 (f0:6e:0b:d1:59:58)
Internet Protocol Version 4, Src: 10.224.0.1, Dst: 10.226.120.102
User Datagram Protocol, Src Port: 67, Dst Port: 68
    Source Port: 67
    Destination Port: 68
    Length: 286
    [Checksum: [missing]]
    [Checksum Status: Not present]
    [Stream index: 12]
    [Timestamps]
Dynamic Host Configuration Protocol (Offer)
No.     Time                           Source                Destination           Protocol Length Info
     83 2020-09-12 18:16:12.958395     0.0.0.0               255.255.255.255       DHCP     358    DHCP Request  - Transaction ID 0x671015c8
Frame 83: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits) on interface \Device\NPF_{AD8285C9-616C-4D09-9F9A-A134FBBD9253}, id
0
Ethernet II, Src: Microsof_d1:59:58 (f0:6e:0b:d1:59:58), 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
    Source Port: 68
    Destination Port: 67
    Length: 324
    Checksum: 0x0c9e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 11]
    [Timestamps]
Dynamic Host Configuration Protocol (Request)
No.     Time                           Source                Destination           Protocol Length Info
     84 2020-09-12 18:16:12.979734     10.224.0.1            10.226.120.102        DHCP     320    DHCP ACK      - Transaction ID 0x671015c8
Frame 84: 320 bytes on wire (2560 bits), 320 bytes captured (2560 bits) on interface \Device\NPF_{AD8285C9-616C-4D09-9F9A-A134FBBD9253}, id
0
Ethernet II, Src: BenuNetw_03:64:bc (f4:3e:9d:03:64:bc), Dst: Microsof_d1:59:58 (f0:6e:0b:d1:59:58)
Internet Protocol Version 4, Src: 10.224.0.1, Dst: 10.226.120.102
User Datagram Protocol, Src Port: 67, Dst Port: 68
    Source Port: 67
    Destination Port: 68
    Length: 286
    [Checksum: [missing]]
    [Checksum Status: Not present]
    [Stream index: 12]
    [Timestamps]
Dynamic Host Configuration Protocol (ACK)
```

2) Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?

Yes, because the UDP port numbers used in this example are also 67 and 68.



3) What is the link-layer (e.g., Ethernet) address of your host?

The link-layer address of my host is **f0:6e:0b:d1:59:58**.

```
> Frame 81: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{AD8285C9-616C-4D09-9F9A-A134FBBD925
v Ethernet II, Src: Microsof_d1:59:58 (f0:6e:0b:d1:59:58), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: Microsof_d1:59:58 (f0:6e:0b:d1:59:58)
    Type: IPv4 (0x0800)
> 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)
```

4) What values in the DHCP discover message differentiate this message from the DHCP request message?

Under "Option(53) DHCP", the Message Type and their values (1) & (3) are different.

```
v Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x671015c8
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Microsof_d1:59:58 (f0:6e:0b:d1:59:58)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  v Option: (53) DHCP Message Type (Discover)
      Length: 1
      DHCP: Discover (1)
```

```
v Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x671015c8
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Microsof_d1:59:58 (f0:6e:0b:d1:59:58)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  v Option: (53) DHCP Message Type (Request)
      Length: 1
      DHCP: Request (3)
```

5) What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?

The value of the Transaction ID of the first four DHCP messages is **0x671015c8**.

The value of the Transaction ID of the second set DHCP messages is **0x1ef2456a**.

The purpose of the Transaction-ID field is used to identify and associate messages and responses between clients and servers during one transaction.

No.	Time	Source	Destination	Protocol	Length	Info
81	2020-09-12 18:16:12.917424	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x671015c8
82	2020-09-12 18:16:12.957086	10.224.0.1	10.226.120.102	DHCP	320	DHCP Offer - Transaction ID 0x671015c8
83	2020-09-12 18:16:12.958395	0.0.0.0	255.255.255.255	DHCP	358	DHCP Request - Transaction ID 0x671015c8
84	2020-09-12 18:16:12.979734	10.224.0.1	10.226.120.102	DHCP	320	DHCP ACK - Transaction ID 0x671015c8

```
11621 2020-09-12 18:17:46.198941 10.226.120.102    10.224.0.1          DHCP     346 DHCP Request  - Transaction ID 0x1ef2456a
11622 2020-09-12 18:17:46.220476 10.224.0.1        10.226.120.102      DHCP     320 DHCP ACK      - Transaction ID 0x1ef2456a
```

6) A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.

The value is used in the IP datagrams is **0.0.0.0**.

DHCP Discover: Source IP 0.0.0.0; Destination IP: 255.255.255.255

DHCP Offer: Source IP 10.224.0.1; Destination IP: 10.226.120.102

DHCP Request: Source IP 0.0.0.0; Destination IP: 255.255.255.255

DHCP ACK: Source IP 10.224.0.1; Destination IP: 10.226.120.102

	Time	Source	Destination	Protocol	Length	Info
81	2020-09-12 18:16:12.917424	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x671015c8
82	2020-09-12 18:16:12.957086	10.224.0.1	10.226.120.102	DHCP	320	DHCP Offer - Transaction ID 0x671015c8
83	2020-09-12 18:16:12.958395	0.0.0.0	255.255.255.255	DHCP	358	DHCP Request - Transaction ID 0x671015c8
84	2020-09-12 18:16:12.979734	10.224.0.1	10.226.120.102	DHCP	320	DHCP ACK - Transaction ID 0x671015c8

7) What is the IP address of your DHCP server?

The IP address of my DHCP server is **10.224.0.1**.

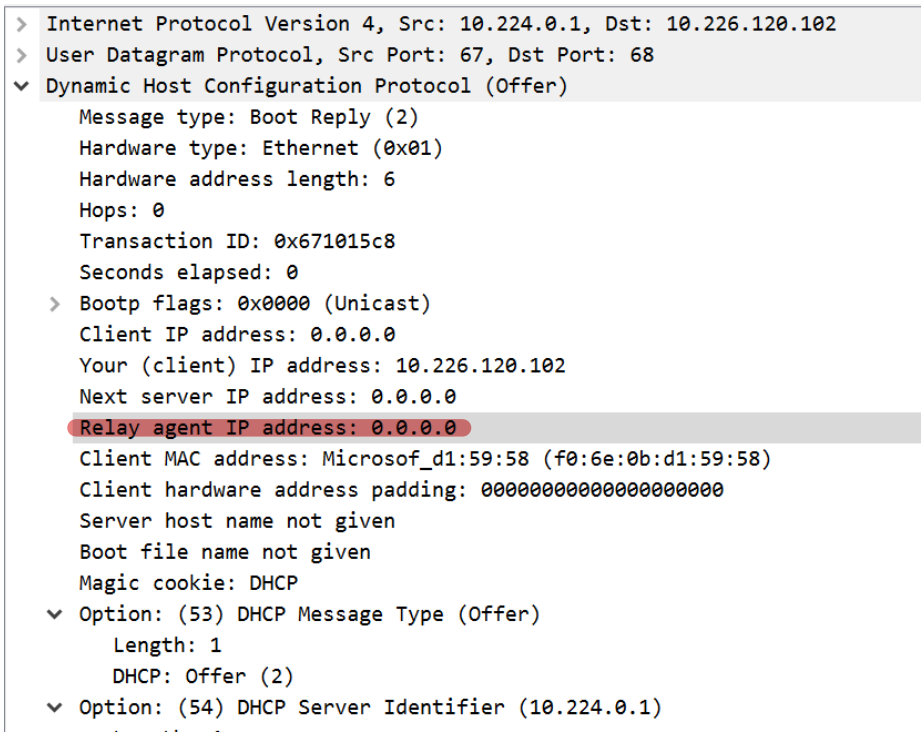
	Time	Source	Destination	Protocol	Length	Info
81	2020-09-12 18:16:12.917424	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x671015c8
82	2020-09-12 18:16:12.957086	10.224.0.1	10.226.120.102	DHCP	320	DHCP Offer - Transaction ID 0x671015c8
83	2020-09-12 18:16:12.958395	0.0.0.0	255.255.255.255	DHCP	358	DHCP Request - Transaction ID 0x671015c8
84	2020-09-12 18:16:12.979734	10.224.0.1	10.226.120.102	DHCP	320	DHCP ACK - Transaction ID 0x671015c8

8) What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.

The IP address that DHCP server offered to my host is **10.226.120.102**. The DHCP message with "**Option: (53) DHCP Message Type (Offer), Length: 1, DHCP: Offer (2)**" contained DHCP Offer message.

```
> Internet Protocol Version 4, Src: 10.224.0.1, Dst: 10.226.120.102
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x671015c8
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.226.120.102
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Microsof_d1:59:58 (f0:6e:0b:d1:59:58)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  v Option: (53) DHCP Message Type (Offer)
      Length: 1
      DHCP: Offer (2)
```

9) In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of the agent?
There is no relay agent in my experiment because the IP address in the trace is 0.0.0.0, which indicated the absence of a relay agent as the given example.



10) Explain the purpose of the router and subnet mask lines in the DHCP offer message.
The router line indicates which default gateway that the client should send messages.
The subnet mask line indicates which subnet mask that the client should use.

```
No.     Time                           Source                Destination           Protocol Length Info
     82 2020-09-12 18:16:12.957086     10.224.0.1            10.226.120.102        DHCP     320    DHCP Offer    - Transaction ID 0x671015c8
Frame 82: 320 bytes on wire (2560 bits), 320 bytes captured (2560 bits) on interface \Device\NPF_{AD8285C9-616C-4D09-9F9A-A134FBBD9253}, id
0
Ethernet II, Src: BenuNetw_03:64:bc (f4:3e:9d:03:64:bc), Dst: Microsof_d1:59:58 (f0:6e:0b:d1:59:58)
Internet Protocol Version 4, Src: 10.224.0.1, Dst: 10.226.120.102
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x671015c8
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.226.120.102
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Microsof_d1:59:58 (f0:6e:0b:d1:59:58)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type (Offer)
        Length: 1
        DHCP: Offer (2)
    Option: (54) DHCP Server Identifier (10.224.0.1)
        Length: 4
        DHCP Server Identifier: 10.224.0.1
    Option: (3) Router
        Length: 4
        Router: 10.224.0.1
    Option: (1) Subnet Mask (255.252.0.0)
        Length: 4
        Subnet Mask: 255.252.0.0
    Option: (51) IP Address Lease Time
        Length: 4
        IP Address Lease Time: (300s) 5 minutes
    Option: (6) Domain Name Server
        Length: 8
        Domain Name Server: 75.75.75.75
        Domain Name Server: 75.75.76.76
    Option: (255) End
        Option End: 255
```

11) In the DHCP trace file noted in footnote 2, the DHCP server offers a specific IP address to the client (see also question 8. above). In the client's response to the first server OFFER message, does the client accept this IP address? Where in the client's RESPONSE is the client's requested address?

Yes, the client officially accepted this IP address once the client sent the DHCP Request message to the DHCP server.

```
No.     Time                           Source                Destination           Protocol Length Info
     83 2020-09-12 18:16:12.958395     0.0.0.0               255.255.255.255       DHCP     358    DHCP Request  - Transaction ID 0x671015c8
Frame 83: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits) on interface \Device\NPF_{AD8285C9-616C-4D09-9F9A-A134FBBD9253}, id
0
Ethernet II, Src: Microsof_d1:59:58 (f0:6e:0b:d1:59:58), 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 (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x671015c8
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Microsof_d1:59:58 (f0:6e:0b:d1:59:58)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type (Request)
        Length: 1
        DHCP: Request (3)
    Option: (61) Client identifier
        Length: 7
        Hardware type: Ethernet (0x01)
        Client MAC address: Microsof_d1:59:58 (f0:6e:0b:d1:59:58)
    Option: (50) Requested IP Address (10.226.120.102)
        Length: 4
        Requested IP Address: 10.226.120.102
```

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

The lease time indicates how long that the client can use specific IP address assigned by DHCP server, the client needs to be assigned a new IP address once the lease time expired. My lease time in this experiment is 300 seconds or 5 minutes.

```
> Option: (53) DHCP Message Type (ACK)
> Option: (54) DHCP Server Identifier (10.224.0.1)
> Option: (3) Router
> Option: (1) Subnet Mask (255.252.0.0)
v Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: (300s) 5 minutes
```

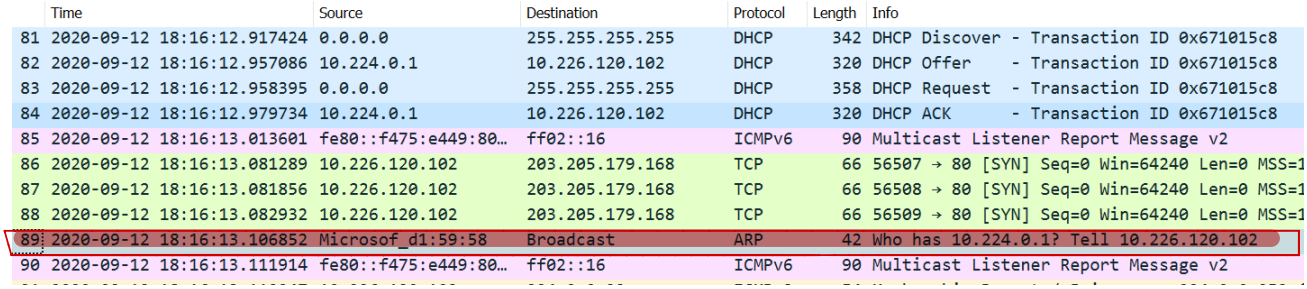
13) What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?

a). DHCP release message is used to cancel the IP address assigned to the client before, and the client will turn it back to the DHCP server.

b). No, the DHCP will not issue an acknowledgment of receipt.

c). If the client's DHCP release message is lost, then the client will still release the IP address, but the DHCP server isn't aware of that, and the DHCP server will continue to reserve this IP address until it expired.

14) Clear the *bootp* filter from your Wireshark window. Were any ARP packets sent or received during the DHCP packet-exchange period? If so, explain the purpose of those ARP packets.
Yes, those ARP packets helped the host/router to get the MAC address of another host/router on the same LAN by sending ARP request/reply messages.



	Time	Source	Destination	Protocol	Length	Info
81	2020-09-12 18:16:12.917424	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x671015c8
82	2020-09-12 18:16:12.957086	10.224.0.1	10.226.120.102	DHCP	320	DHCP Offer - Transaction ID 0x671015c8
83	2020-09-12 18:16:12.958395	0.0.0.0	255.255.255.255	DHCP	358	DHCP Request - Transaction ID 0x671015c8
84	2020-09-12 18:16:12.979734	10.224.0.1	10.226.120.102	DHCP	320	DHCP ACK - Transaction ID 0x671015c8
85	2020-09-12 18:16:13.013601	fe80::f475:e449:80…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
86	2020-09-12 18:16:13.081289	10.226.120.102	203.205.179.168	TCP	66	56507 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1
87	2020-09-12 18:16:13.081856	10.226.120.102	203.205.179.168	TCP	66	56508 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1
88	2020-09-12 18:16:13.082932	10.226.120.102	203.205.179.168	TCP	66	56509 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1
89	2020-09-12 18:16:13.106852	Microsof_d1:59:58	Broadcast	ARP	42	Who has 10.224.0.1? Tell 10.226.120.102
90	2020-09-12 18:16:13.111914	fe80::f475:e449:80…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2

3. Conclusion (Discussion of the result & Evaluation of the tool)

In this lab, I have studied and analyzed how an IP address and relevant configuration information are dynamically assigned to certain clients through DHCP server and DORA messages. In order to observer the whole communication process between client and server, I captured DHCP packets by using Wireshark packet sniffer. In addition to protocols shown in the example, I found several of supporting and security protocols, for example, ICMP (Internet Control Message Protocol) used to generate error messages, MDNS (Multicast DNS Protocol) helped with name resolution, and TLS (Transport Layer Security) provided privacy and data security, etc.

As a packet analyzer, Wireshark are capable of capturing and decoding every packet that are currently-being-transmitted between clients and servers over a real-time network. It also provides practical functionalities such as timing datagram, flow graph, protocols filter, time display formatters, file I/O, and data import/export.