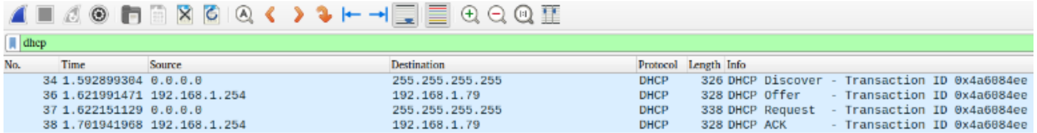
Using Wireshark to Demonstrate Different Packets Involved In Getting On IP Address From DHCP Server

Filtering Packets

Filtering the DHCP packets on wireshark with dhcp flag , we can see 4 network packets i.e. Discover, Offer, Request and Acknowledge .

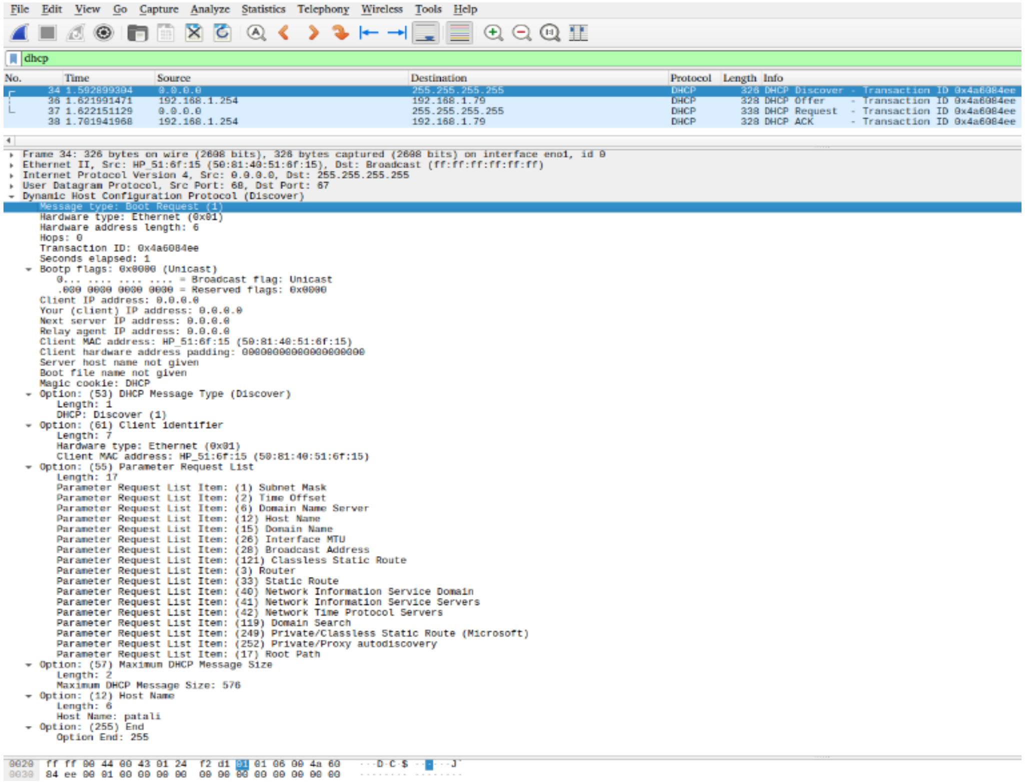


```
dhcp
No.   Time        Source          Destination        Protocol  Length Info
   34 1.592899304 0.0.0.0         255.255.255.255    DHCP      326 DHCP Discover - Transaction ID 0x4a6084ee
   36 1.621991471 192.168.1.254   192.168.1.79       DHCP      328 DHCP Offer    - Transaction ID 0x4a6084ee
   37 1.622151129 0.0.0.0         255.255.255.255    DHCP      338 DHCP Request  - Transaction ID 0x4a6084ee
   38 1.701941968 192.168.1.254   192.168.1.79       DHCP      328 DHCP ACK      - Transaction ID 0x4a6084ee
```

Fig:1

Analyzing DHCP Discover Packet

Client is broadcasting discover packet for DHCP server with source IP 0.0.0.0 and destination IP 255.255.255.255 where the source IP address is 0.0.0.0, indicating that the client does not yet have an IP address and The destination IP address is 255.255.255.255, indicating that the message is a broadcast intended for all devices on the local network.



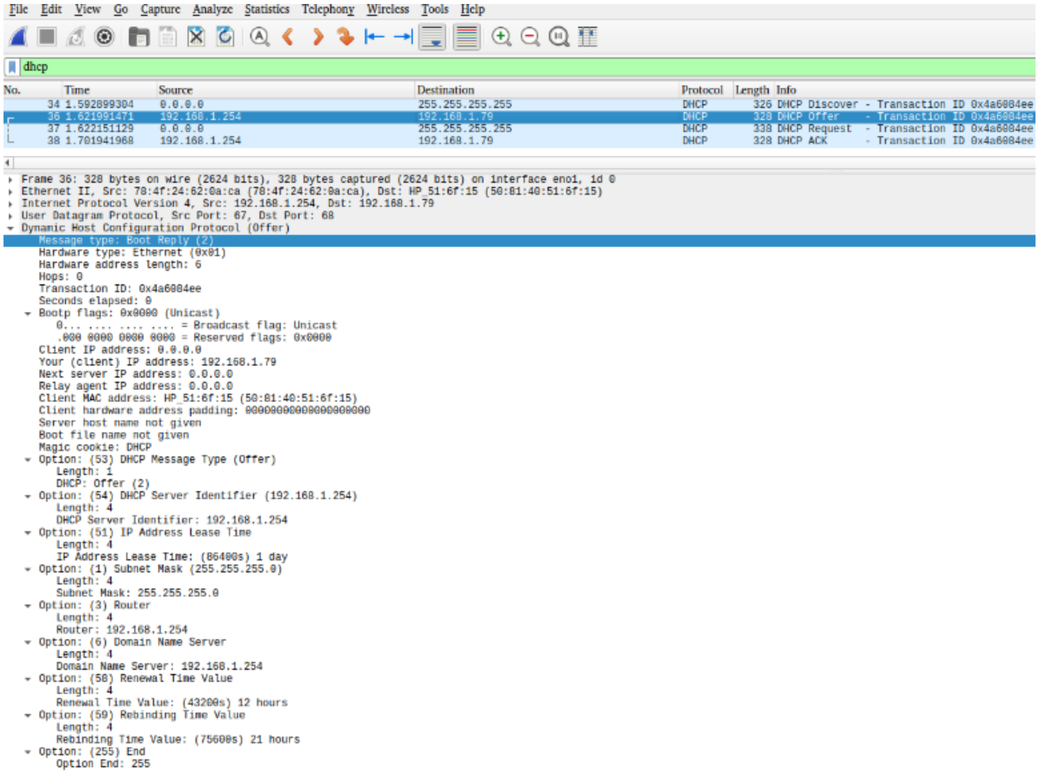
```
dhcp
No.   Time        Source          Destination        Protocol  Length Info
   34 1.592899304 0.0.0.0         255.255.255.255    DHCP      326 DHCP Discover - Transaction ID 0x4a6084ee
   36 1.621991471 192.168.1.254   192.168.1.79       DHCP      328 DHCP Offer    - Transaction ID 0x4a6084ee
   37 1.622151129 0.0.0.0         255.255.255.255    DHCP      338 DHCP Request  - Transaction ID 0x4a6084ee
   38 1.701941968 192.168.1.254   192.168.1.79       DHCP      328 DHCP ACK      - Transaction ID 0x4a6084ee

▸ Frame 34: 326 bytes on wire (2608 bits), 326 bytes captured (2608 bits) on interface eno1, id 0
▸ Ethernet II, Src: HP_51:6f:15 (50:81:40:51:6f:15), 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: 0x4a6084ee
    Seconds elapsed: 1
  ▾ Bootp flags: 0x0000 (Unicast)
      0... .... .... .... = Broadcast flag: Unicast
      .000 0000 0000 0000 = Reserved flags: 0x0000
    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: HP_51:6f:15 (50:81:40:51:6f:15)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▾ Option: (53) DHCP Message Type (Discover)
      Length: 1
      DHCP: Discover (1)
  ▾ Option: (61) Client identifier
      Length: 7
      Hardware type: Ethernet (0x01)
      Client MAC address: HP_51:6f:15 (50:81:40:51:6f:15)
  ▾ Option: (55) Parameter Request List
      Length: 17
      Parameter Request List Item: (1) Subnet Mask
      Parameter Request List Item: (2) Time Offset
      Parameter Request List Item: (6) Domain Name Server
      Parameter Request List Item: (12) Host Name
      Parameter Request List Item: (15) Domain Name
      Parameter Request List Item: (26) Interface MTU
      Parameter Request List Item: (28) Broadcast Address
      Parameter Request List Item: (121) Classless Static Route
      Parameter Request List Item: (3) Router
      Parameter Request List Item: (33) Static Route
      Parameter Request List Item: (40) Network Information Service Domain
      Parameter Request List Item: (41) Network Information Service Servers
      Parameter Request List Item: (42) Network Time Protocol Servers
      Parameter Request List Item: (119) Domain Search
      Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
      Parameter Request List Item: (252) Private/Proxy autodiscovery
      Parameter Request List Item: (17) Root Path
  ▾ Option: (57) Maximum DHCP Message Size
      Length: 2
      Maximum DHCP Message Size: 576
  ▾ Option: (12) Host Name
      Length: 6
      Host Name: patali
  ▾ Option: (255) End
      Option End: 255

0020  ff ff 00 44 00 43 01 24  f2 d1 01 01 06 00 4a 60   ···D·C·$ ·······J`
0030  84 ee 00 01 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

fig :2

Here, client is sending its mac address and host name by specifying the Parameter Request List. Along with that, its also setting Bootp flags as 0 meaning the response from DHCP server should be unicast with maximum response size 576 bytes.

Analyzing DHCP Offer Packet

As offer from DHCP server, DHCP server has sent its ip address including all requested parameters.



dhcp

```
No.     Time          Source          Destination        Protocol Length Info
     34 1.592899304   0.0.0.0         255.255.255.255    DHCP       326 DHCP Discover - Transaction ID 0x4a6084ee
┌    36 1.621991471   192.168.1.254   192.168.1.79       DHCP       328 DHCP Offer    - Transaction ID 0x4a6084ee
┆    37 1.622151129   0.0.0.0         255.255.255.255    DHCP       338 DHCP Request  - Transaction ID 0x4a6084ee
└    38 1.701941968   192.168.1.254   192.168.1.79       DHCP       328 DHCP ACK      - Transaction ID 0x4a6084ee
```

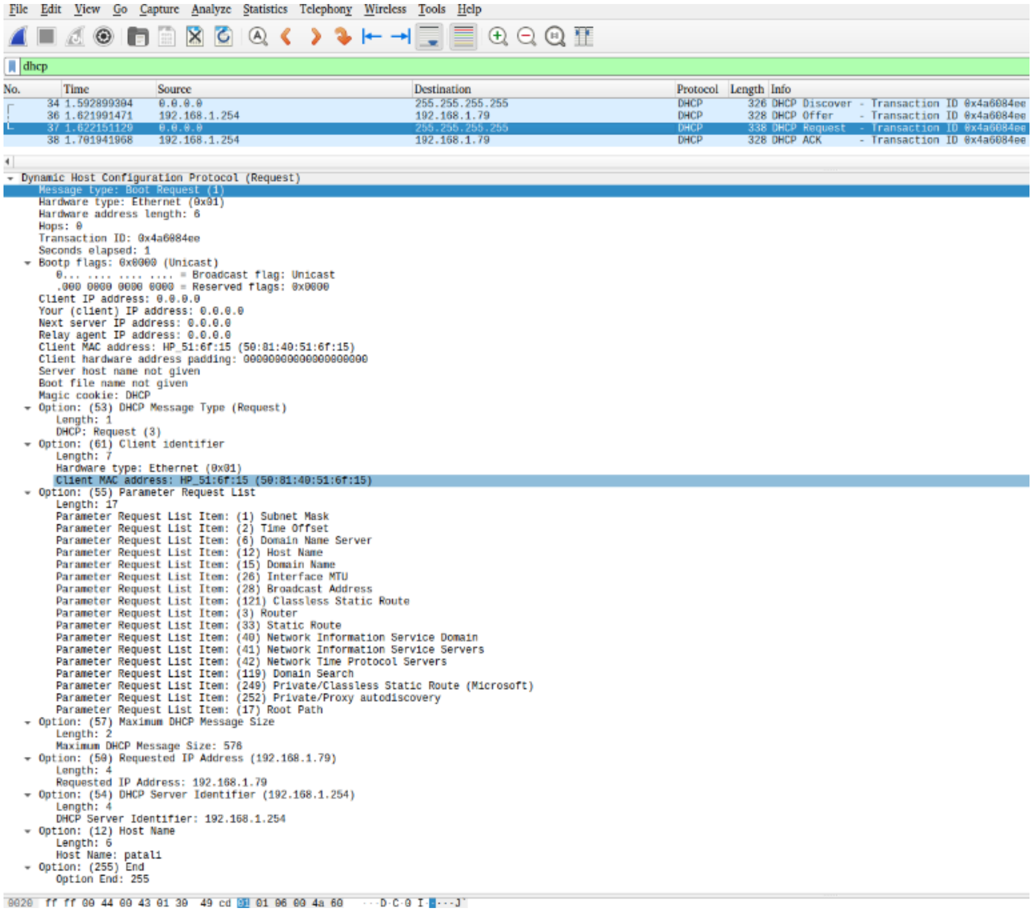
```
▸ Frame 36: 328 bytes on wire (2624 bits), 328 bytes captured (2624 bits) on interface eno1, id 0
▸ Ethernet II, Src: 78:4f:24:62:0a:ca (78:4f:24:62:0a:ca), Dst: HP_51:6f:15 (50:81:40:51:6f:15)
▸ Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.79
▸ User Datagram Protocol, Src Port: 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: 0x4a6084ee
    Seconds elapsed: 0
  ▾ Bootp flags: 0x0000 (Unicast)
      0... .... .... .... = Broadcast flag: Unicast
      .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.79
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: HP_51:6f:15 (50:81:40:51:6f:15)
    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 (192.168.1.254)
      Length: 4
      DHCP Server Identifier: 192.168.1.254
  ▾ Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: (86400s) 1 day
  ▾ Option: (1) Subnet Mask (255.255.255.0)
      Length: 4
      Subnet Mask: 255.255.255.0
  ▾ Option: (3) Router
      Length: 4
      Router: 192.168.1.254
  ▾ Option: (6) Domain Name Server
      Length: 4
      Domain Name Server: 192.168.1.254
  ▾ Option: (58) Renewal Time Value
      Length: 4
      Renewal Time Value: (43200s) 12 hours
  ▾ Option: (59) Rebinding Time Value
      Length: 4
      Rebinding Time Value: (75600s) 21 hours
  ▾ Option: (255) End
      Option End: 255
```

fig3

In above image we can see, DHCP server has offered 192.168.1.79 ip address with lease time 1 day. Additionally, we can see subnet mask, DNS server and other parameters that were in parameter request list.

Analysing DHCP Request Packet

DHCP Request packet is sent by the client by including the IP address i.e 192.168.1.79. In this case its same IP that was offered by DHCP server.

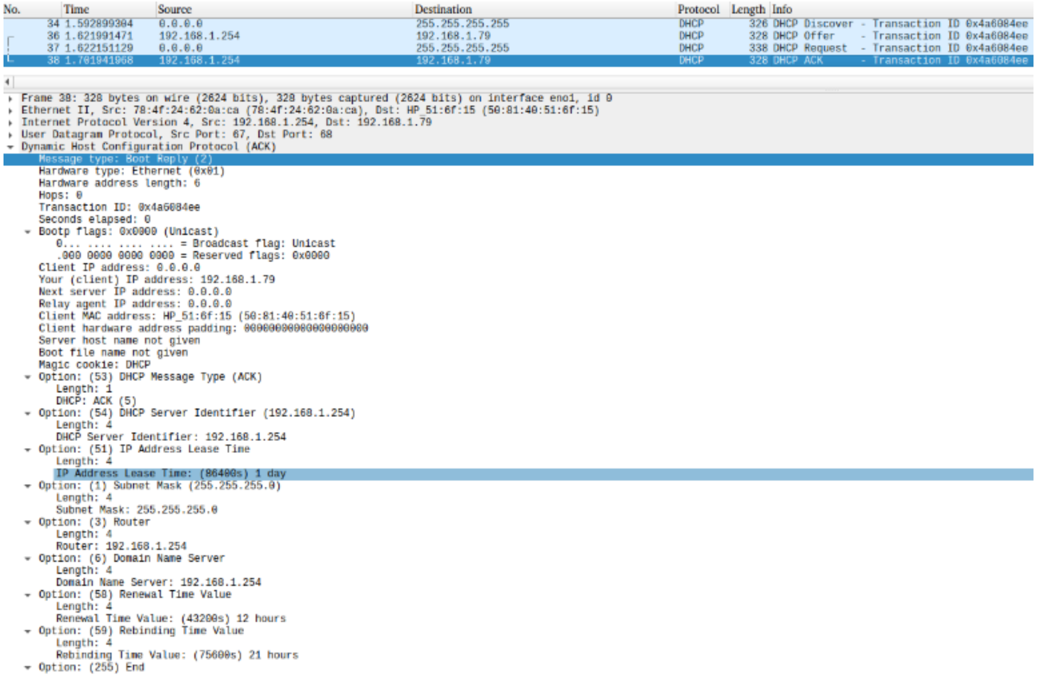


```
dhcp

No.    Time          Source          Destination        Protocol  Length  Info
   34 1.592899304   0.0.0.0         255.255.255.255    DHCP      326 DHCP Discover - Transaction ID 0x4a6084ee
   36 1.621991471   192.168.1.254   192.168.1.79       DHCP      328 DHCP Offer    - Transaction ID 0x4a6084ee
   37 1.622151129   0.0.0.0         255.255.255.255    DHCP      338 DHCP Request  - Transaction ID 0x4a6084ee
   38 1.701941968   192.168.1.254   192.168.1.79       DHCP      328 DHCP ACK      - Transaction ID 0x4a6084ee

▾ Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x4a6084ee
    Seconds elapsed: 1
  ▾ Bootp flags: 0x0000 (Unicast)
      0... .... .... .... = Broadcast flag: Unicast
      .000 0000 0000 0000 = Reserved flags: 0x0000
    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: HP_51:6f:15 (50:81:40:51:6f:15)
    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: HP_51:6f:15 (50:81:40:51:6f:15)
  ▾ Option: (55) Parameter Request List
      Length: 17
      Parameter Request List Item: (1) Subnet Mask
      Parameter Request List Item: (2) Time Offset
      Parameter Request List Item: (6) Domain Name Server
      Parameter Request List Item: (12) Host Name
      Parameter Request List Item: (15) Domain Name
      Parameter Request List Item: (26) Interface MTU
      Parameter Request List Item: (28) Broadcast Address
      Parameter Request List Item: (121) Classless Static Route
      Parameter Request List Item: (3) Router
      Parameter Request List Item: (33) Static Route
      Parameter Request List Item: (40) Network Information Service Domain
      Parameter Request List Item: (41) Network Information Service Servers
      Parameter Request List Item: (42) Network Time Protocol Servers
      Parameter Request List Item: (119) Domain Search
      Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
      Parameter Request List Item: (252) Private/Proxy autodiscovery
      Parameter Request List Item: (17) Root Path
  ▾ Option: (57) Maximum DHCP Message Size
      Length: 2
      Maximum DHCP Message Size: 576
  ▾ Option: (50) Requested IP Address (192.168.1.79)
      Length: 4
      Requested IP Address: 192.168.1.79
  ▾ Option: (54) DHCP Server Identifier (192.168.1.254)
      Length: 4
      DHCP Server Identifier: 192.168.1.254
  ▾ Option: (12) Host Name
      Length: 6
      Host Name: patali
  ▾ Option: (255) End
      Option End: 255

0020  ff ff 00 44 00 43 01 30  49 cd 01 01 06 00 4a 60   ···D·C·0 I·····J`
```

fig4

Analysing DHCP Acknowledgement Packet

As acknowledgement of request, DHCP server has sent all the parameters that are being assigned to the client. It was last step of assignment of IP address by DHCP server to the client.



```
No.     Time         Source           Destination       Protocol Length Info
     34 1.592899304  0.0.0.0          255.255.255.255   DHCP     326 DHCP Discover - Transaction ID 0x4a6084ee
     36 1.621991471  192.168.1.254    192.168.1.79      DHCP     328 DHCP Offer    - Transaction ID 0x4a6084ee
     37 1.622151129  0.0.0.0          255.255.255.255   DHCP     338 DHCP Request  - Transaction ID 0x4a6084ee
     38 1.701941968  192.168.1.254    192.168.1.79      DHCP     328 DHCP ACK      - Transaction ID 0x4a6084ee

▸ Frame 38: 328 bytes on wire (2624 bits), 328 bytes captured (2624 bits) on interface eno1, id 0
▸ Ethernet II, Src: 78:4f:24:62:0a:ca (78:4f:24:62:0a:ca), Dst: HP_51:6f:15 (50:81:40:51:6f:15)
▸ Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.79
▸ User Datagram Protocol, Src Port: 67, Dst Port: 68
▾ Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x4a6084ee
    Seconds elapsed: 0
  ▾ Bootp flags: 0x0000 (Unicast)
      0... .... .... .... = Broadcast flag: Unicast
      .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.79
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: HP_51:6f:15 (50:81:40:51:6f:15)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▾ Option: (53) DHCP Message Type (ACK)
      Length: 1
      DHCP: ACK (5)
  ▾ Option: (54) DHCP Server Identifier (192.168.1.254)
      Length: 4
      DHCP Server Identifier: 192.168.1.254
  ▾ Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: (86400s) 1 day
  ▾ Option: (1) Subnet Mask (255.255.255.0)
      Length: 4
      Subnet Mask: 255.255.255.0
  ▾ Option: (3) Router
      Length: 4
      Router: 192.168.1.254
  ▾ Option: (6) Domain Name Server
      Length: 4
      Domain Name Server: 192.168.1.254
  ▾ Option: (58) Renewal Time Value
      Length: 4
      Renewal Time Value: (43200s) 12 hours
  ▾ Option: (59) Rebinding Time Value
      Length: 4
      Rebinding Time Value: (75600s) 21 hours
  ▾ Option: (255) End
```

fig5

In this way, client is successfully assigned 192.168.1.79 as IP address 192.168.1.254 as dns server and 255.255.255.0 as subnet mask.