Lab Report

CSE351, Computer Networking

Name: Youssef Moustafa Elsayed ID: 22P0047

Lab No: (7) Experiment Title: Wireshark Lab: DHCP

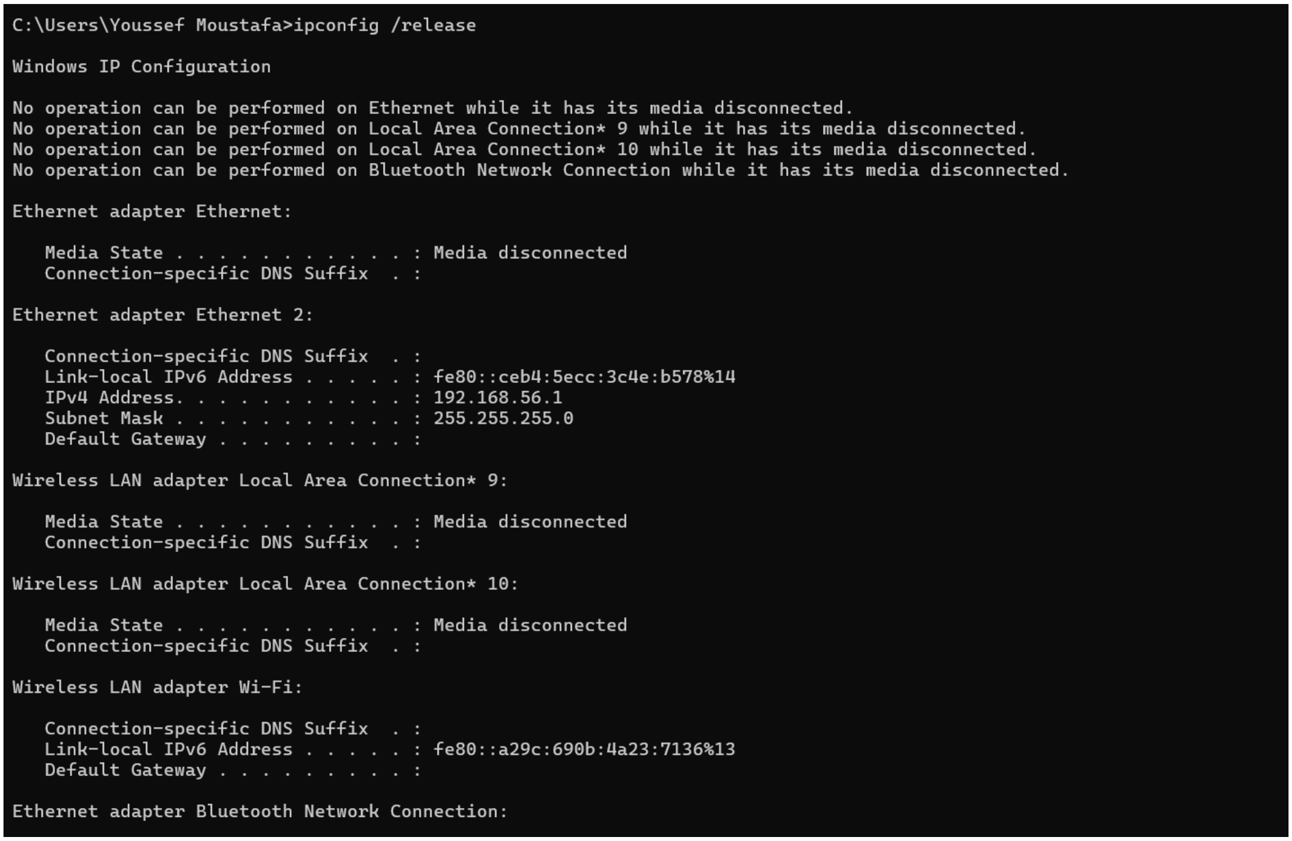
Date: 14 / 12 /2025

Steps

1- In a command-line window we will enter the following command:

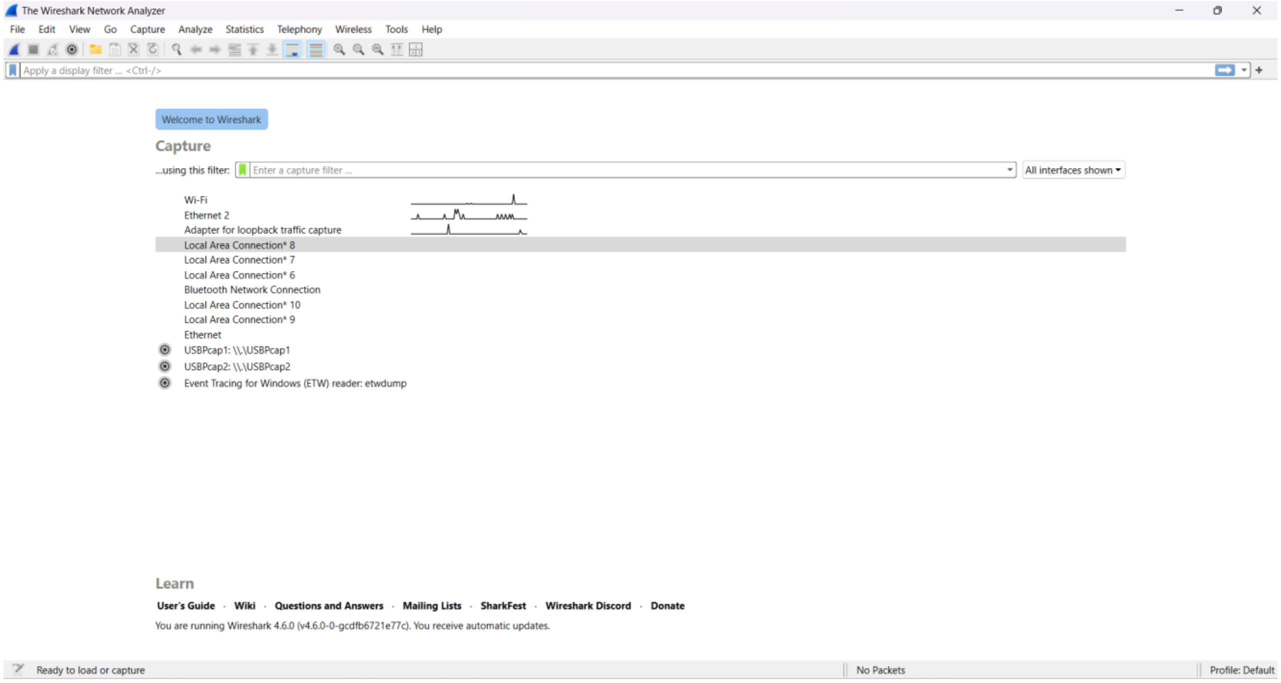
> ipconfig /release

This command will cause the PC to give up its IP address.



```
C:\Users\Youssef Moustafa>ipconfig /release

Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.
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 Bluetooth Network Connection while it has its media disconnected.

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ceb4:5ecc:3c4e:b578%14
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a29c:690b:4a23:7136%13
   Default Gateway . . . . . . . . . :

Ethernet adapter Bluetooth Network Connection:
```

2- Start up the Wireshark packet sniffer


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
All interfaces shown
Wi-Fi
Ethernet 2
Adapter for loopback traffic capture
Local Area Connection* 8
Local Area Connection* 7
Local Area Connection* 6
Bluetooth Network Connection
Local Area Connection* 10
Local Area Connection* 9
Ethernet
USBPcap1: \\.\USBPcap1
USBPcap2: \\.\USBPcap2
Event Tracing for Windows (ETW) reader: etwdump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
No Packets
Profile: Default

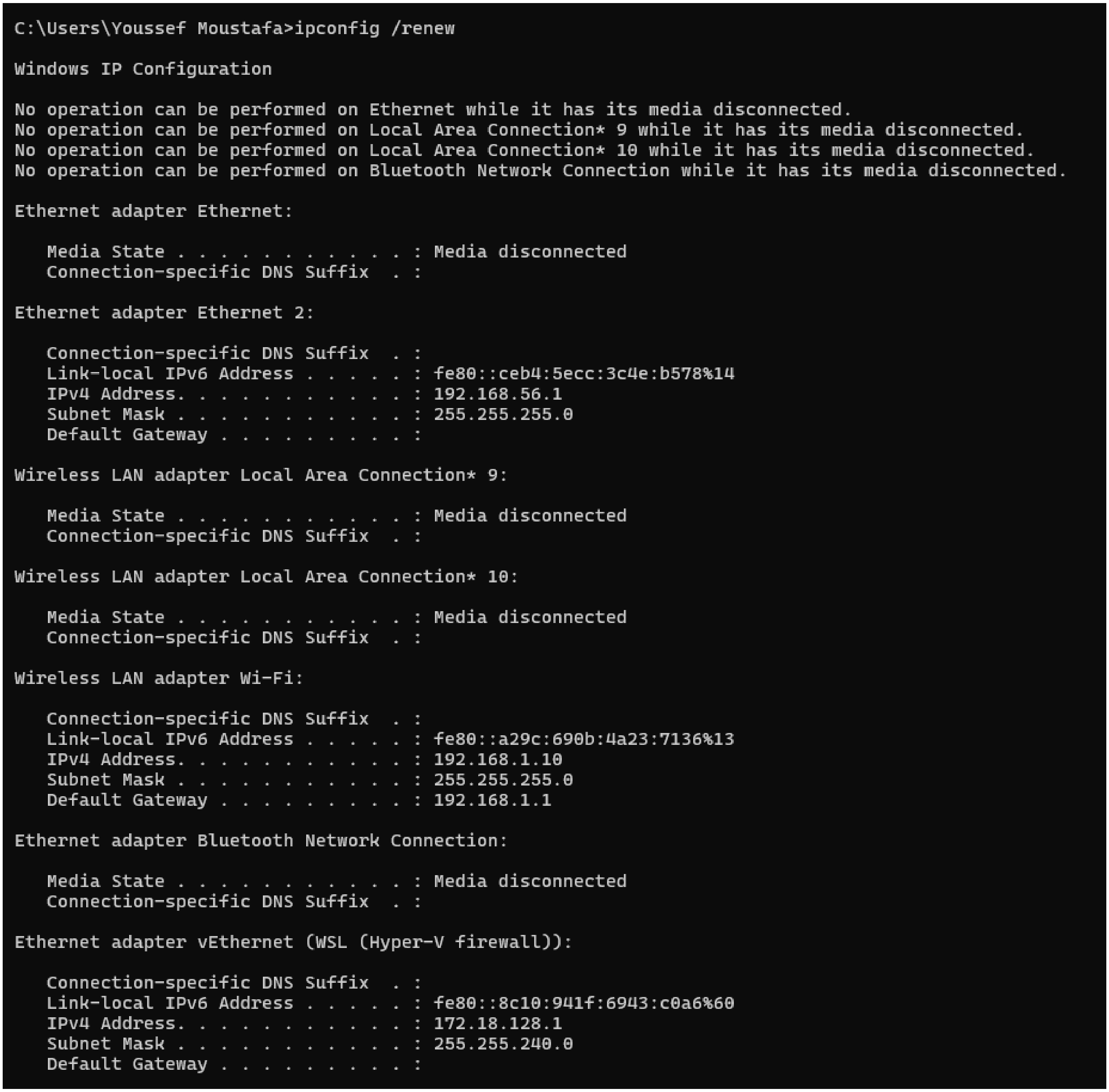
You are running Wireshark 4.6.0 (v4.6.0-0-gcdfb6721e77c). You receive automatic updates.

Ready to load or capture

3- In the command-line window enter the following command:

> ipconfig /renew

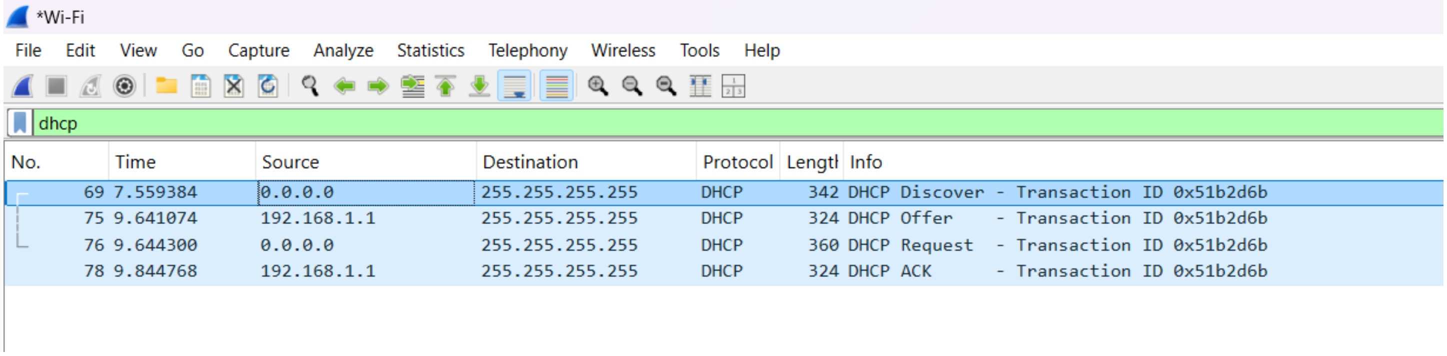
This will cause the DHCP protocol to request and receive an IP address and other information from a DHCP server.



```
C:\Users\Youssef Moustafa>ipconfig /renew

Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.
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 Bluetooth Network Connection while it has its media disconnected.

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ceb4:5ecc:3c4e:b578%14
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a29c:690b:4a23:7136%13
   IPv4 Address. . . . . . . . . . . : 192.168.1.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter vEthernet (WSL (Hyper-V firewall)):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8c10:941f:6943:c0a6%60
   IPv4 Address. . . . . . . . . . . : 172.18.128.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :
```

4- After waiting for a few seconds, stop Wireshark capture.

5- After stopping Wireshark capture in step 4, we should peek into Wireshark window to make sure we captured the packets that we're looking for. Enter "dhcp" into the display filter field.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

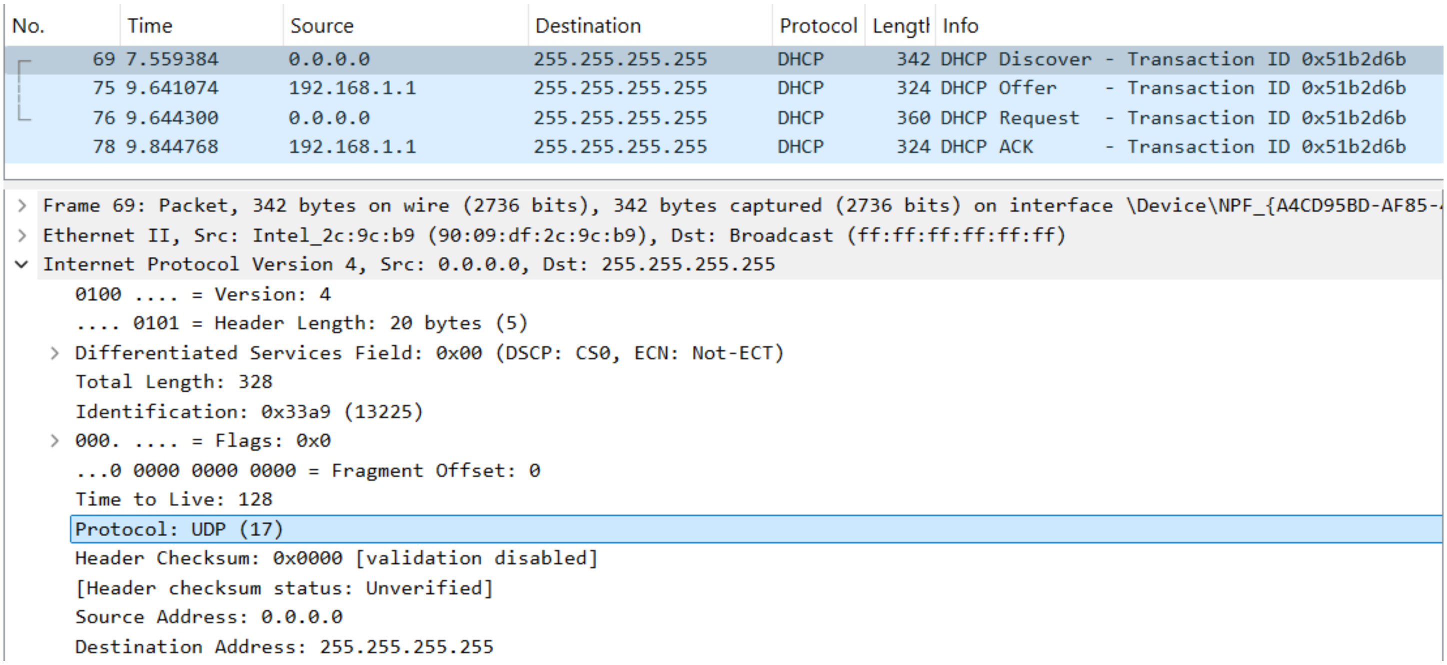
dhcp

```
No.   Time        Source        Destination       Protocol Lengtl Info
   69 7.559384    0.0.0.0       255.255.255.255   DHCP     342 DHCP Discover - Transaction ID 0x51b2d6b
   75 9.641074    192.168.1.1   255.255.255.255   DHCP     324 DHCP Offer    - Transaction ID 0x51b2d6b
   76 9.644300    0.0.0.0       255.255.255.255   DHCP     360 DHCP Request  - Transaction ID 0x51b2d6b
   78 9.844768    192.168.1.1   255.255.255.255   DHCP     324 DHCP ACK      - Transaction ID 0x51b2d6b
```

Part 2: Answering Questions in textbook

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

UDP

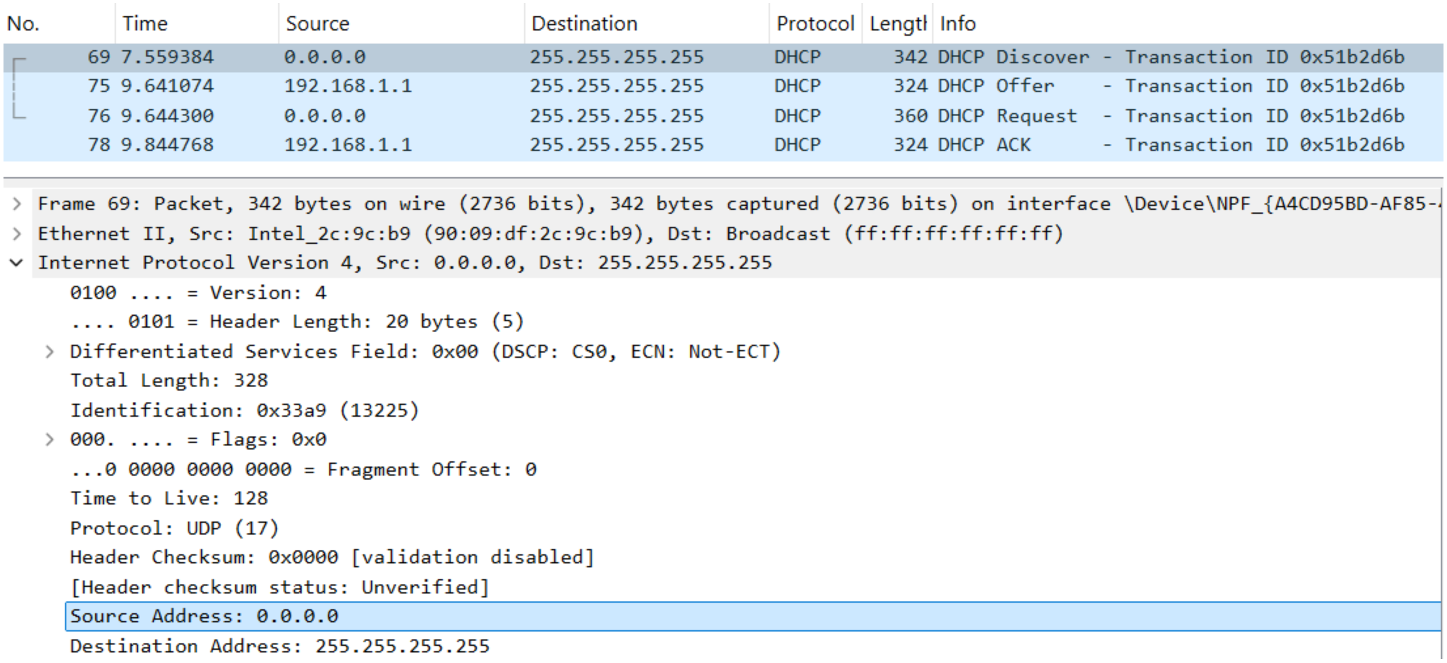


```
No.   Time        Source        Destination       Protocol Lengtl Info
   69 7.559384    0.0.0.0       255.255.255.255   DHCP     342 DHCP Discover - Transaction ID 0x51b2d6b
   75 9.641074    192.168.1.1   255.255.255.255   DHCP     324 DHCP Offer    - Transaction ID 0x51b2d6b
   76 9.644300    0.0.0.0       255.255.255.255   DHCP     360 DHCP Request  - Transaction ID 0x51b2d6b
   78 9.844768    192.168.1.1   255.255.255.255   DHCP     324 DHCP ACK      - Transaction ID 0x51b2d6b

> Frame 69: Packet, 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{A4CD95BD-AF85-
> Ethernet II, Src: Intel_2c:9c:b9 (90:09:df:2c:9c:b9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 328
    Identification: 0x33a9 (13225)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 0.0.0.0
    Destination Address: 255.255.255.255
```

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

0.0.0.0

Yes, there is something special as the client does not yet have an IP address



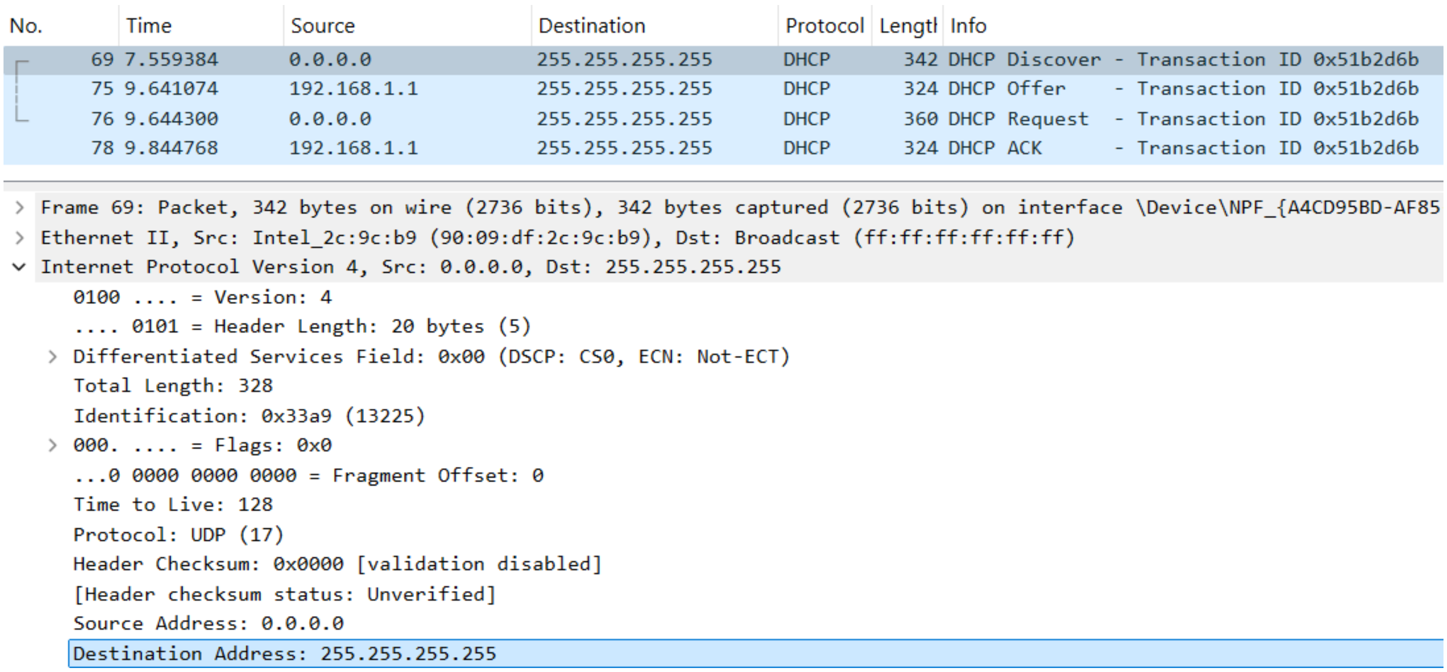
```
No.       Time          Source          Destination       Protocol Lengtl Info
   69 7.559384      0.0.0.0         255.255.255.255   DHCP      342 DHCP Discover - Transaction ID 0x51b2d6b
   75 9.641074      192.168.1.1     255.255.255.255   DHCP      324 DHCP Offer    - Transaction ID 0x51b2d6b
   76 9.644300      0.0.0.0         255.255.255.255   DHCP      360 DHCP Request  - Transaction ID 0x51b2d6b
   78 9.844768      192.168.1.1     255.255.255.255   DHCP      324 DHCP ACK      - Transaction ID 0x51b2d6b
```

```
> Frame 69: Packet, 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{A4CD95BD-AF85-
> Ethernet II, Src: Intel_2c:9c:b9 (90:09:df:2c:9c:b9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 328
    Identification: 0x33a9 (13225)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 0.0.0.0
    Destination Address: 255.255.255.255
```

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

255.255.255.255

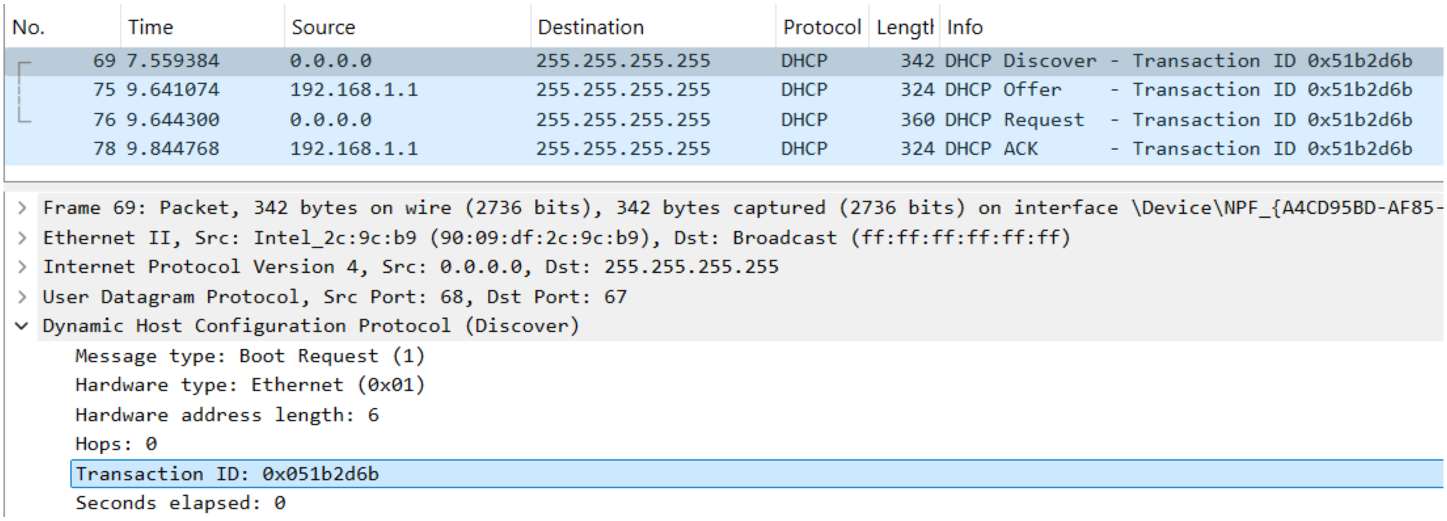
Yes, there is something special as this is the limited broadcast address.



```
No.      Time       Source        Destination       Protocol Lengtl Info
      69 7.559384   0.0.0.0       255.255.255.255   DHCP       342 DHCP Discover - Transaction ID 0x51b2d6b
      75 9.641074   192.168.1.1   255.255.255.255   DHCP       324 DHCP Offer    - Transaction ID 0x51b2d6b
      76 9.644300   0.0.0.0       255.255.255.255   DHCP       360 DHCP Request  - Transaction ID 0x51b2d6b
      78 9.844768   192.168.1.1   255.255.255.255   DHCP       324 DHCP ACK      - Transaction ID 0x51b2d6b

> Frame 69: Packet, 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{A4CD95BD-AF85
> Ethernet II, Src: Intel_2c:9c:b9 (90:09:df:2c:9c:b9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 328
    Identification: 0x33a9 (13225)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 0.0.0.0
    Destination Address: 255.255.255.255
```

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

Transaction ID: 0x051b2d6b



```
No.      Time       Source        Destination       Protocol Lengtl Info
      69 7.559384   0.0.0.0       255.255.255.255   DHCP       342 DHCP Discover - Transaction ID 0x51b2d6b
      75 9.641074   192.168.1.1   255.255.255.255   DHCP       324 DHCP Offer    - Transaction ID 0x51b2d6b
      76 9.644300   0.0.0.0       255.255.255.255   DHCP       360 DHCP Request  - Transaction ID 0x51b2d6b
      78 9.844768   192.168.1.1   255.255.255.255   DHCP       324 DHCP ACK      - Transaction ID 0x51b2d6b

> Frame 69: Packet, 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{A4CD95BD-AF85-
> Ethernet II, Src: Intel_2c:9c:b9 (90:09:df:2c:9c:b9), 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
v Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x051b2d6b
    Seconds elapsed: 0
```

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?

1- **Client Identifier**: Used by the DHCP server to uniquely identify the client.

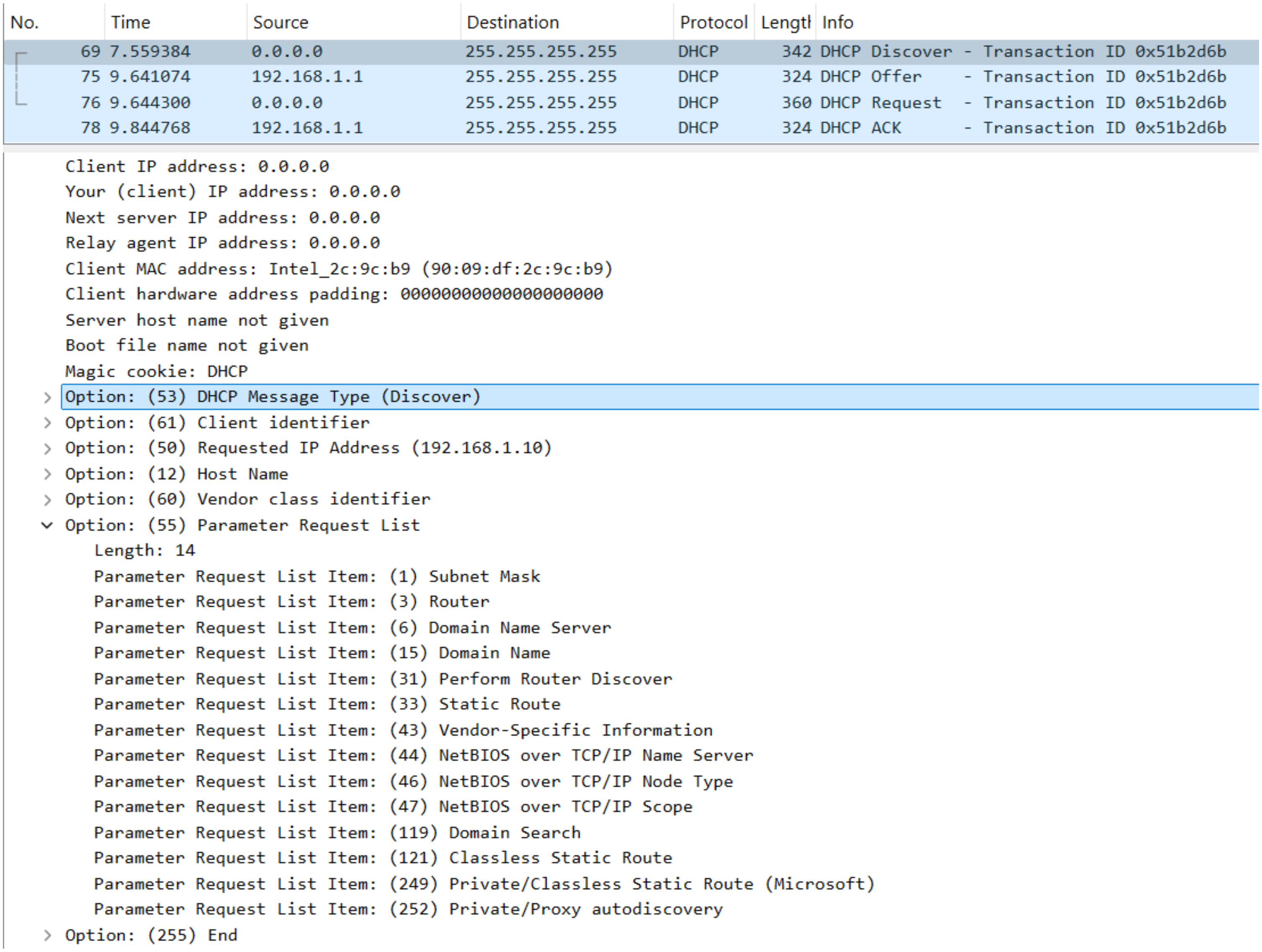
2- **Host Name**: The name of the client device requesting configuration.

3- **Vendor Class Identifier**: Identifies the client’s operating system or vendor type.

4- **Parameter Request List**: specifies which configuration parameters the client wants from the server.

5- **Network configuration parameters** requested in the Parameter Request List, such as:

- Subnet Mask
- Router
- DNS Server



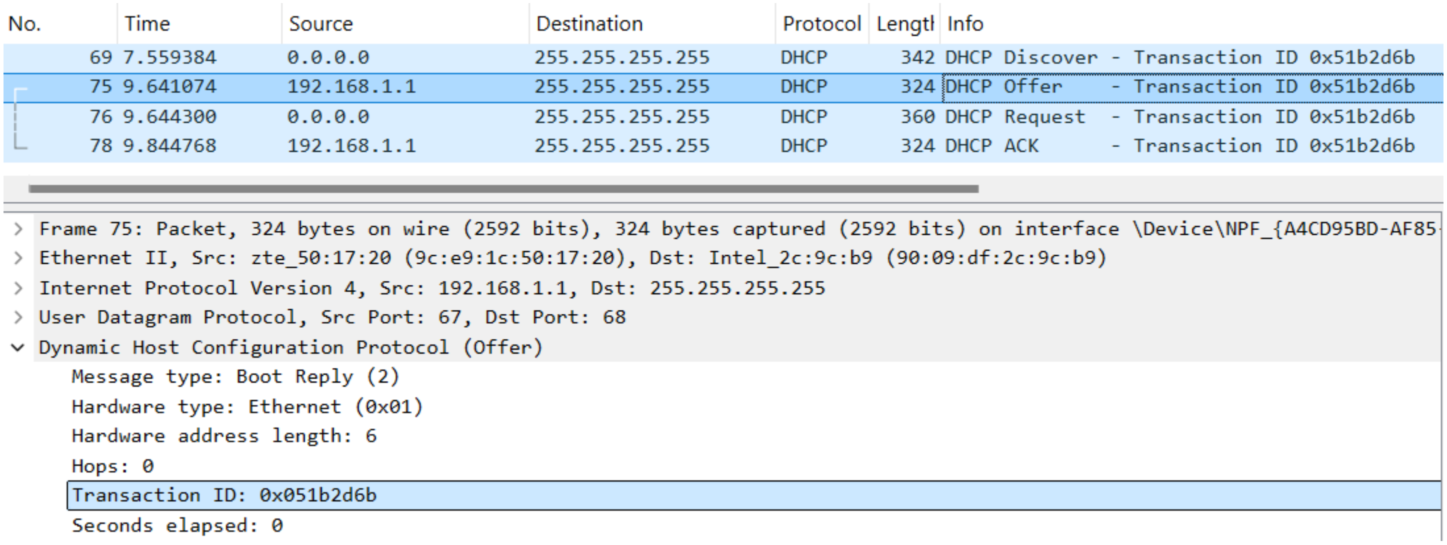
```
No.        Time           Source            Destination        Protocol Lengtl Info
    69 7.559384      0.0.0.0           255.255.255.255    DHCP      342 DHCP Discover - Transaction ID 0x51b2d6b
    75 9.641074      192.168.1.1       255.255.255.255    DHCP      324 DHCP Offer    - Transaction ID 0x51b2d6b
    76 9.644300      0.0.0.0           255.255.255.255    DHCP      360 DHCP Request  - Transaction ID 0x51b2d6b
    78 9.844768      192.168.1.1       255.255.255.255    DHCP      324 DHCP ACK      - Transaction ID 0x51b2d6b
```

```
    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: Intel_2c:9c:b9 (90:09:df:2c:9c:b9)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address (192.168.1.10)
  > Option: (12) Host Name
  > Option: (60) Vendor class identifier
  v Option: (55) Parameter Request List
      Length: 14
      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
  > Option: (255) End
```

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?

Its Transaction ID matches the discover message's Transaction ID equals 0x051b2d6b

Also, because it is the Offer message directly after the Discover message

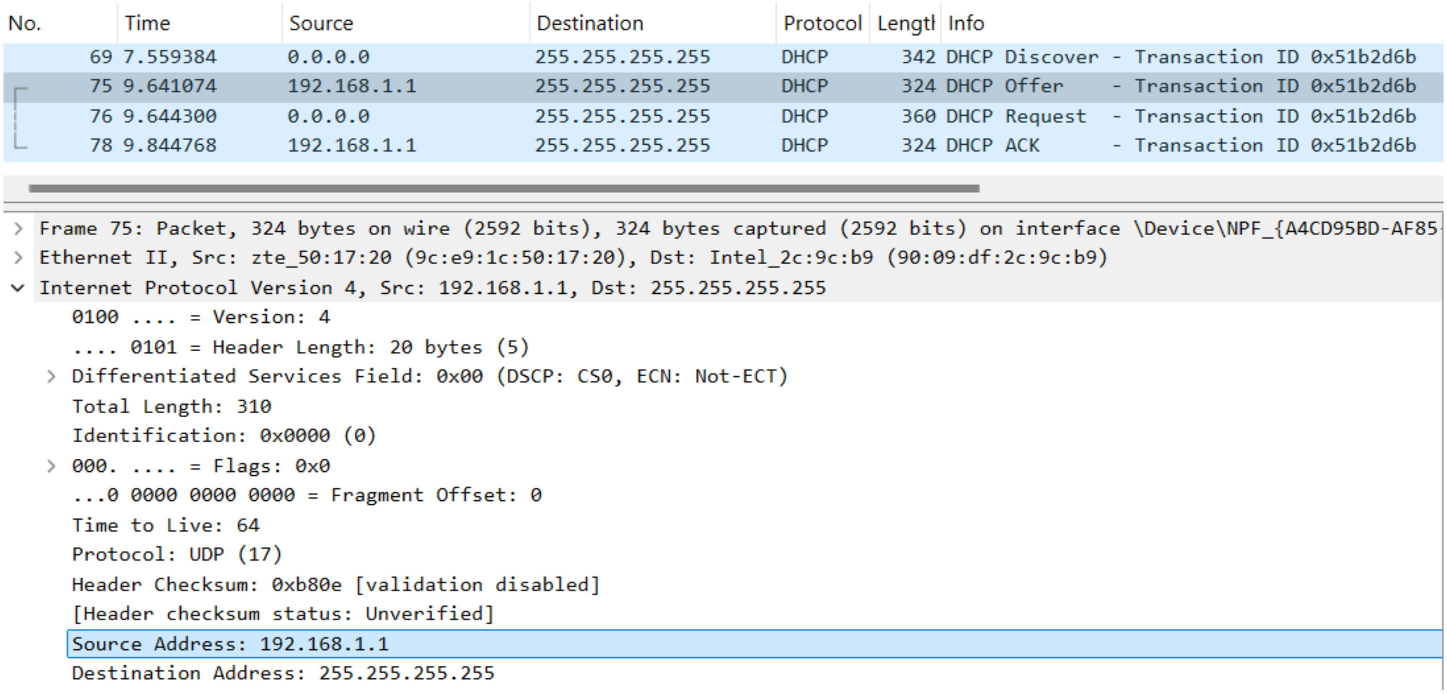


```
No.       Time         Source          Destination       Protocol  Lengtl Info
      69 7.559384     0.0.0.0         255.255.255.255   DHCP       342 DHCP Discover - Transaction ID 0x51b2d6b
      75 9.641074     192.168.1.1     255.255.255.255   DHCP       324 DHCP Offer    - Transaction ID 0x51b2d6b
      76 9.644300     0.0.0.0         255.255.255.255   DHCP       360 DHCP Request  - Transaction ID 0x51b2d6b
      78 9.844768     192.168.1.1     255.255.255.255   DHCP       324 DHCP ACK      - Transaction ID 0x51b2d6b

> Frame 75: Packet, 324 bytes on wire (2592 bits), 324 bytes captured (2592 bits) on interface \Device\NPF_{A4CD95BD-AF85
> Ethernet II, Src: zte_50:17:20 (9c:e9:1c:50:17:20), Dst: Intel_2c:9c:b9 (90:09:df:2c:9c:b9)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 255.255.255.255
> 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: 0x051b2d6b
    Seconds elapsed: 0
```

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

192.168.1.1

Yes, there is something special as this is the server offering the IP address

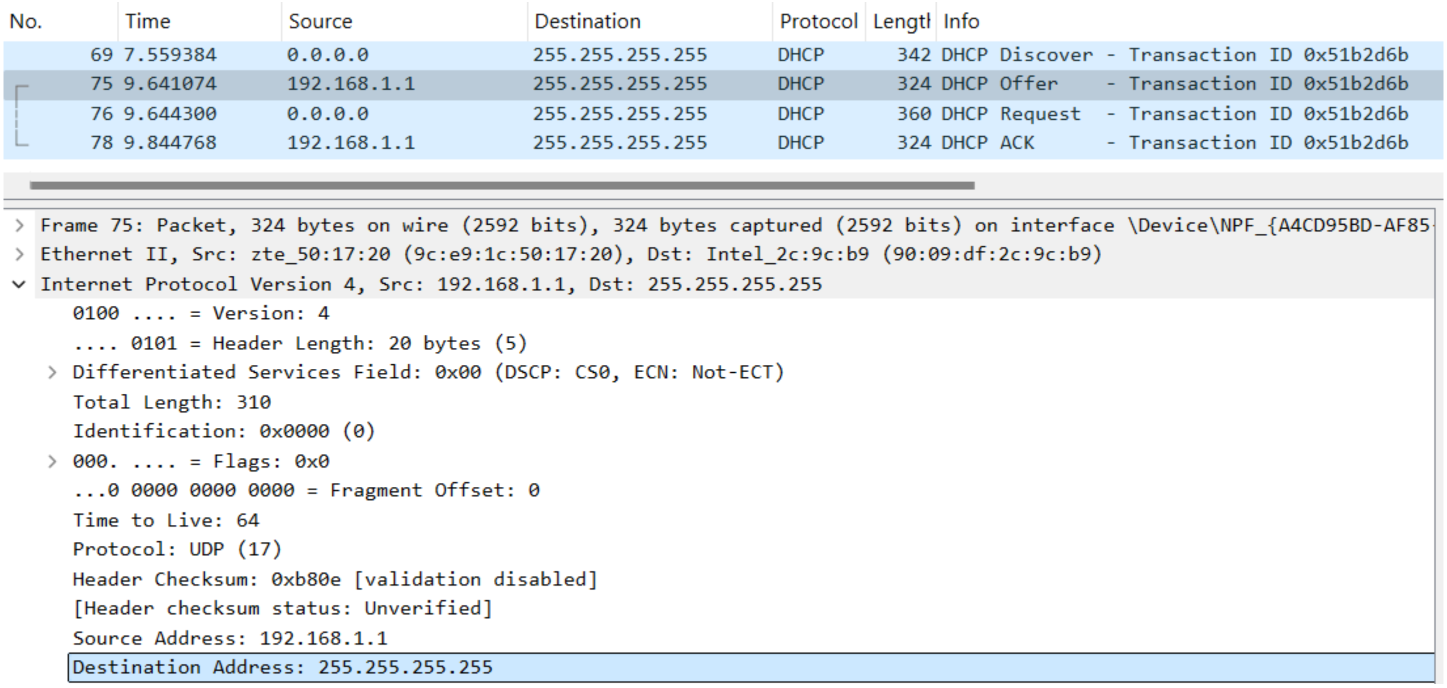


```
No.       Time         Source          Destination       Protocol  Lengtl Info
      69 7.559384     0.0.0.0         255.255.255.255   DHCP       342 DHCP Discover - Transaction ID 0x51b2d6b
      75 9.641074     192.168.1.1     255.255.255.255   DHCP       324 DHCP Offer    - Transaction ID 0x51b2d6b
      76 9.644300     0.0.0.0         255.255.255.255   DHCP       360 DHCP Request  - Transaction ID 0x51b2d6b
      78 9.844768     192.168.1.1     255.255.255.255   DHCP       324 DHCP ACK      - Transaction ID 0x51b2d6b

> Frame 75: Packet, 324 bytes on wire (2592 bits), 324 bytes captured (2592 bits) on interface \Device\NPF_{A4CD95BD-AF85
> Ethernet II, Src: zte_50:17:20 (9c:e9:1c:50:17:20), Dst: Intel_2c:9c:b9 (90:09:df:2c:9c:b9)
v Internet Protocol Version 4, Src: 192.168.1.1, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 310
    Identification: 0x0000 (0)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0xb80e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.1
    Destination Address: 255.255.255.255
```

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

255.255.255.255

Yes, there is something special as Client still doesn't have an IP so, the Server broadcasts the offer



```
No.       Time        Source         Destination       Protocol Length Info
      69 7.559384    0.0.0.0        255.255.255.255   DHCP      342 DHCP Discover - Transaction ID 0x51b2d6b
      75 9.641074    192.168.1.1    255.255.255.255   DHCP      324 DHCP Offer    - Transaction ID 0x51b2d6b
      76 9.644300    0.0.0.0        255.255.255.255   DHCP      360 DHCP Request  - Transaction ID 0x51b2d6b
      78 9.844768    192.168.1.1    255.255.255.255   DHCP      324 DHCP ACK      - Transaction ID 0x51b2d6b
```

```
> Frame 75: Packet, 324 bytes on wire (2592 bits), 324 bytes captured (2592 bits) on interface \Device\NPF_{A4CD95BD-AF85
> Ethernet II, Src: zte_50:17:20 (9c:e9:1c:50:17:20), Dst: Intel_2c:9c:b9 (90:09:df:2c:9c:b9)
v Internet Protocol Version 4, Src: 192.168.1.1, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 310
    Identification: 0x0000 (0)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0xb80e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.1
    Destination Address: 255.255.255.255
```

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?

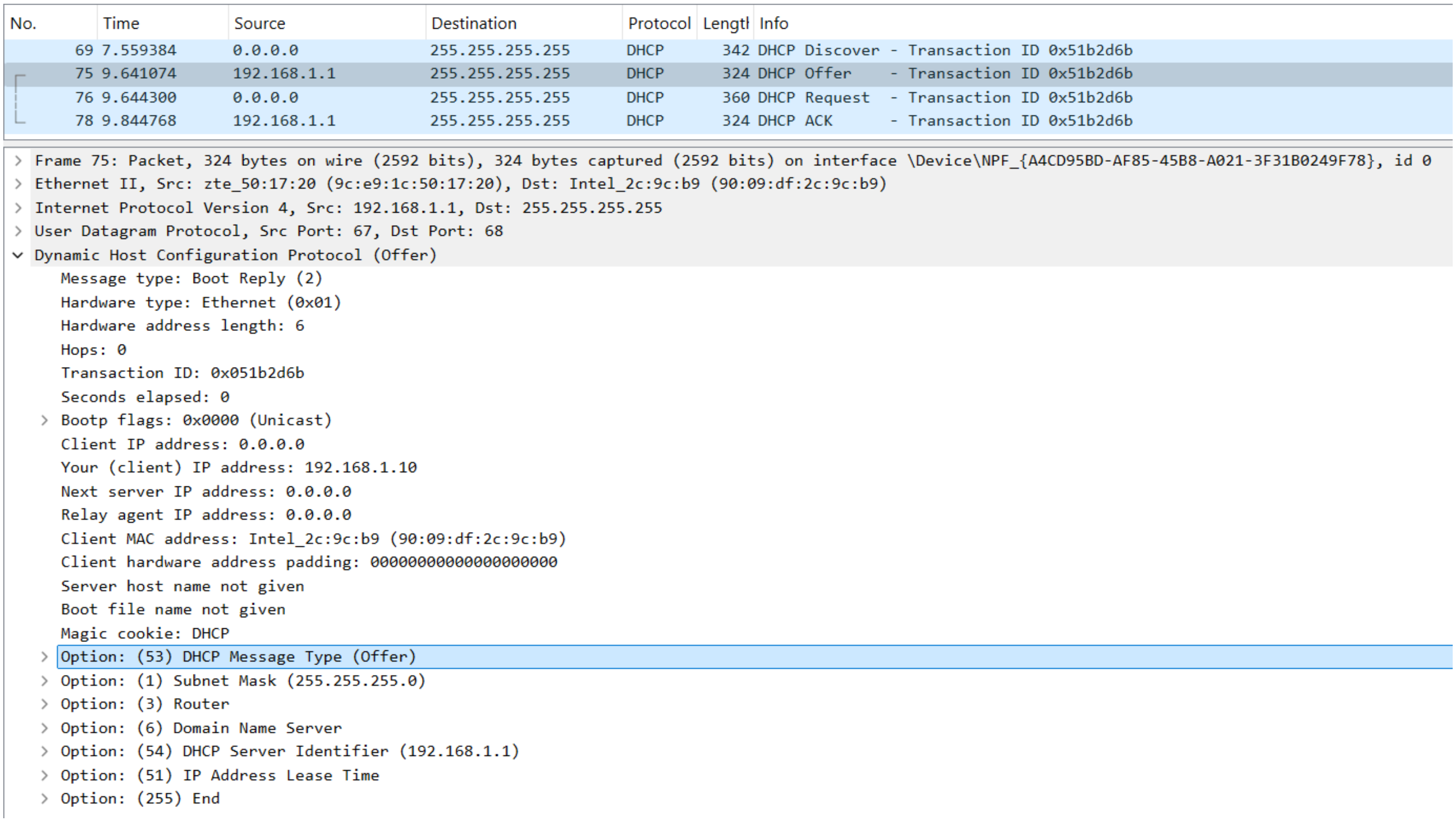
1- **Subnet Mask**: 255.255.255.0

2- **Router:** 192.168.1.1

3- **Domain Name Server (DNS)**

4- **DHCP Server Identifier**: 192.168.1.1 (The DHCP server is the router)

5- **IP Address Lease Time**

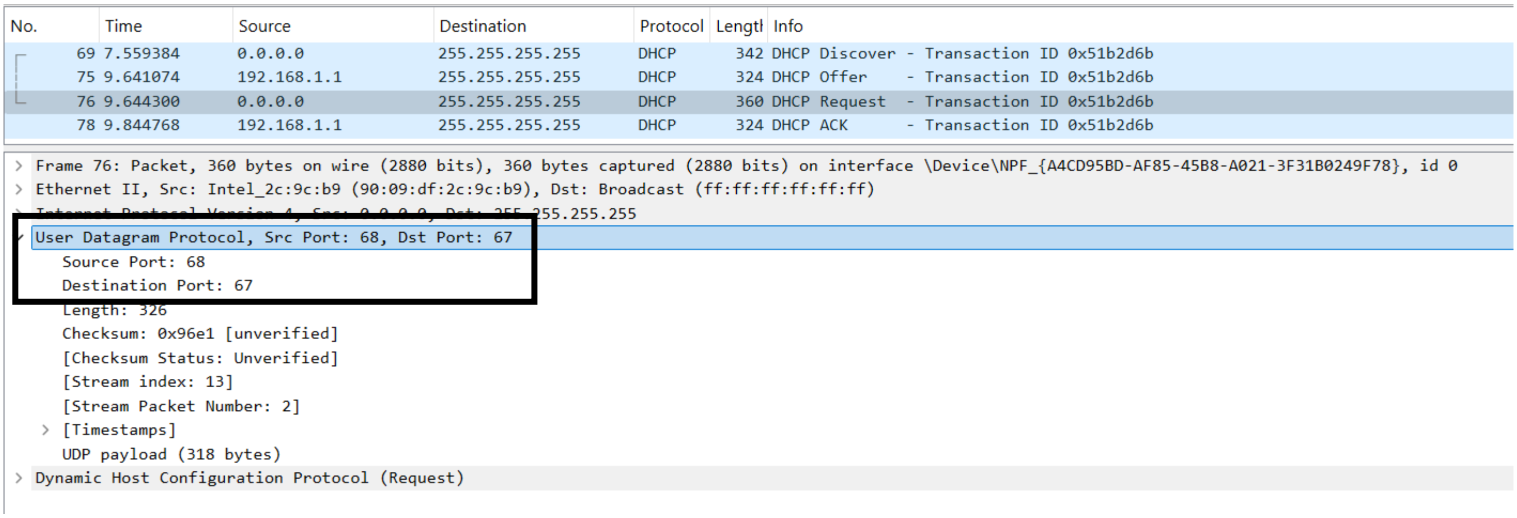


```
No.        Time        Source           Destination      Protocol Lengtl Info
       69 7.559384    0.0.0.0          255.255.255.255  DHCP       342 DHCP Discover - Transaction ID 0x51b2d6b
       75 9.641074    192.168.1.1      255.255.255.255  DHCP       324 DHCP Offer    - Transaction ID 0x51b2d6b
       76 9.644300    0.0.0.0          255.255.255.255  DHCP       360 DHCP Request  - Transaction ID 0x51b2d6b
       78 9.844768    192.168.1.1      255.255.255.255  DHCP       324 DHCP ACK      - Transaction ID 0x51b2d6b
```

```
> Frame 75: Packet, 324 bytes on wire (2592 bits), 324 bytes captured (2592 bits) on interface \Device\NPF_{A4CD95BD-AF85-45B8-A021-3F31B0249F78}, id 0
> Ethernet II, Src: zte_50:17:20 (9c:e9:1c:50:17:20), Dst: Intel_2c:9c:b9 (90:09:df:2c:9c:b9)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 255.255.255.255
> 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: 0x051b2d6b
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.10
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Intel_2c:9c:b9 (90:09:df:2c:9c:b9)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Offer)
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (3) Router
  > Option: (6) Domain Name Server
  > Option: (54) DHCP Server Identifier (192.168.1.1)
  > Option: (51) IP Address Lease Time
  > Option: (255) End
```

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: 68
UDP Destination Port: 67



```
No.   Time       Source        Destination       Protocol Lengtl Info
   69 7.559384   0.0.0.0       255.255.255.255   DHCP      342 DHCP Discover - Transaction ID 0x51b2d6b
   75 9.641074   192.168.1.1   255.255.255.255   DHCP      324 DHCP Offer    - Transaction ID 0x51b2d6b
   76 9.644300   0.0.0.0       255.255.255.255   DHCP      360 DHCP Request  - Transaction ID 0x51b2d6b
   78 9.844768   192.168.1.1   255.255.255.255   DHCP      324 DHCP ACK      - Transaction ID 0x51b2d6b

> Frame 76: Packet, 360 bytes on wire (2880 bits), 360 bytes captured (2880 bits) on interface \Device\NPF_{A4CD95BD-AF85-45B8-A021-3F31B0249F78}, id 0
> Ethernet II, Src: Intel_2c:9c:b9 (90:09:df:2c:9c:b9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
v User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 326
    Checksum: 0x96e1 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 13]
    [Stream Packet Number: 2]
  > [Timestamps]
    UDP payload (318 bytes)
> Dynamic Host Configuration Protocol (Request)
```

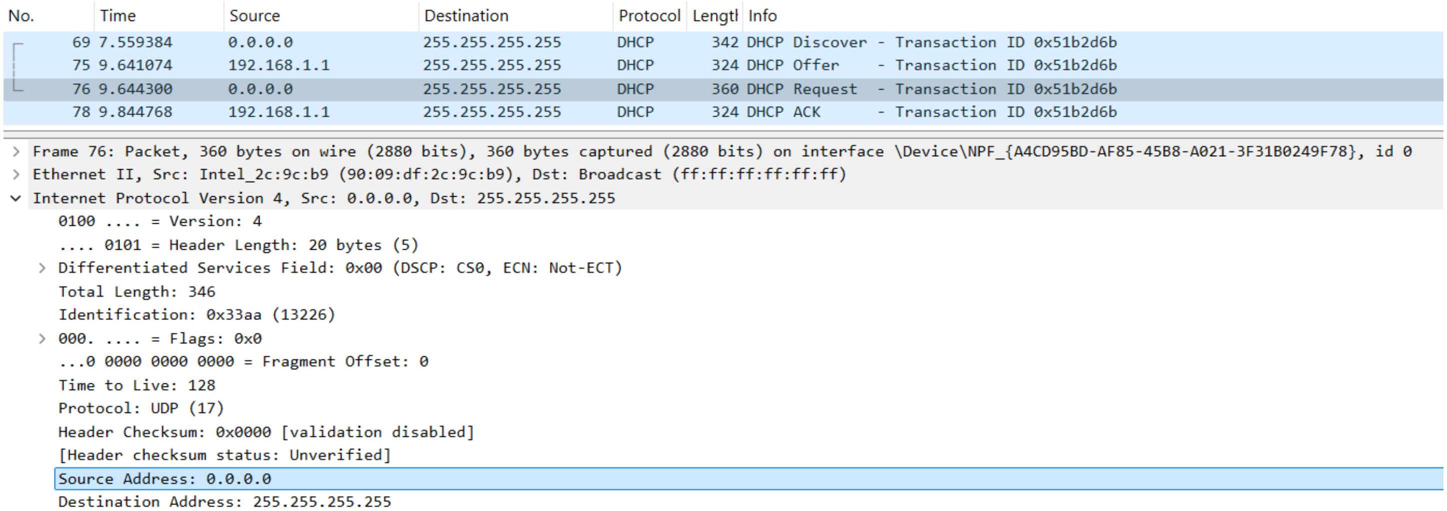
11. What is the source IP address in the IP datagram containing this Request message? Is there anything special about this address? Explain.

0.0.0.0

Yes, there is something special as the client does not yet have an IP address

It would appear that once the DHCP Offer message is received, that the client may have all the information it needs to proceed. However, the client may have received OFFERs from multiple DHCP servers and so a second phase is needed, but client knows there is at least one DHCP server out there

That's why it is still not configured and haven't taken its IP address after the first 2 steps.

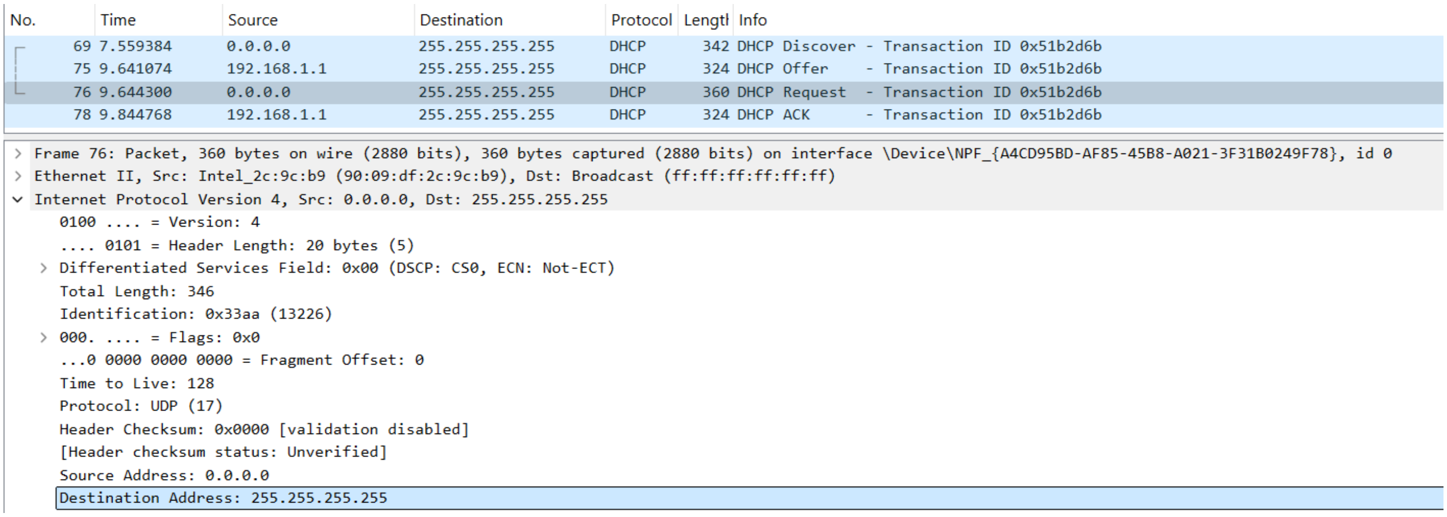


```
No.   Time       Source        Destination       Protocol Lengtl Info
   69 7.559384   0.0.0.0       255.255.255.255   DHCP      342 DHCP Discover - Transaction ID 0x51b2d6b
   75 9.641074   192.168.1.1   255.255.255.255   DHCP      324 DHCP Offer    - Transaction ID 0x51b2d6b
   76 9.644300   0.0.0.0       255.255.255.255   DHCP      360 DHCP Request  - Transaction ID 0x51b2d6b
   78 9.844768   192.168.1.1   255.255.255.255   DHCP      324 DHCP ACK      - Transaction ID 0x51b2d6b

> Frame 76: Packet, 360 bytes on wire (2880 bits), 360 bytes captured (2880 bits) on interface \Device\NPF_{A4CD95BD-AF85-45B8-A021-3F31B0249F78}, id 0
> Ethernet II, Src: Intel_2c:9c:b9 (90:09:df:2c:9c:b9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 346
    Identification: 0x33aa (13226)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 0.0.0.0
    Destination Address: 255.255.255.255
```

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

255.255.255.255

Yes, there is something special as this is broadcasted message as for all DHCP servers to know which offer was accepted



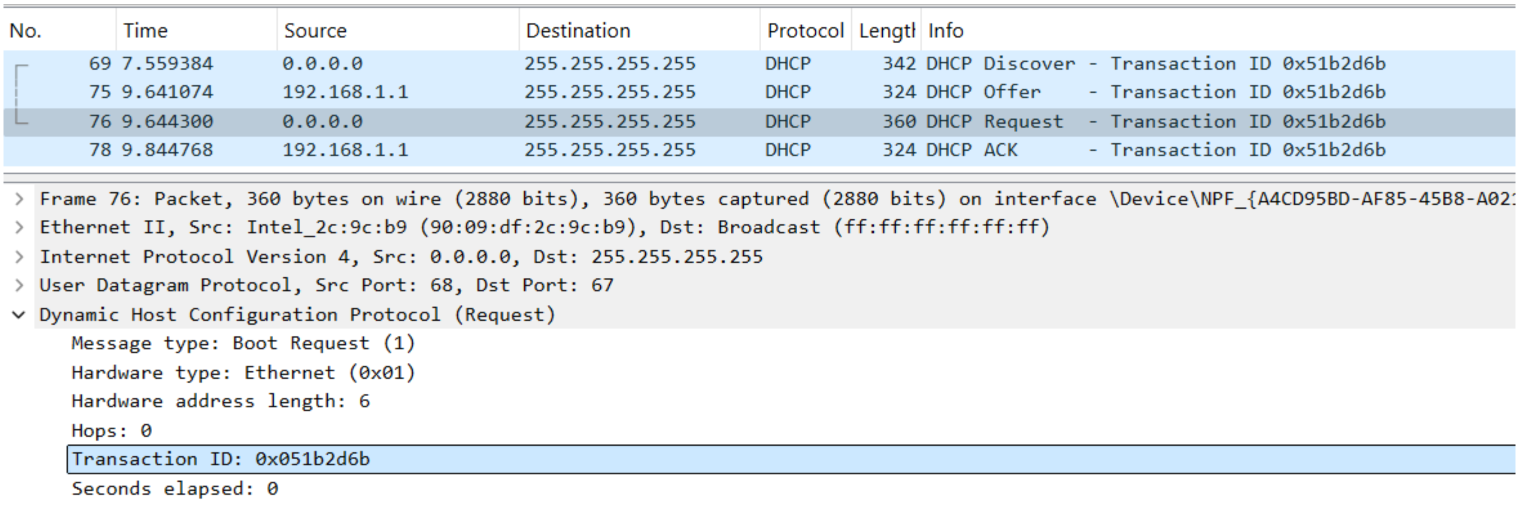
```
No.   Time       Source        Destination       Protocol Lengtl Info
   69 7.559384   0.0.0.0       255.255.255.255   DHCP        342 DHCP Discover - Transaction ID 0x51b2d6b
   75 9.641074   192.168.1.1   255.255.255.255   DHCP        324 DHCP Offer    - Transaction ID 0x51b2d6b
   76 9.644300   0.0.0.0       255.255.255.255   DHCP        360 DHCP Request  - Transaction ID 0x51b2d6b
   78 9.844768   192.168.1.1   255.255.255.255   DHCP        324 DHCP ACK      - Transaction ID 0x51b2d6b

> Frame 76: Packet, 360 bytes on wire (2880 bits), 360 bytes captured (2880 bits) on interface \Device\NPF_{A4CD95BD-AF85-45B8-A021-3F31B0249F78}, id 0
> Ethernet II, Src: Intel_2c:9c:b9 (90:09:df:2c:9c:b9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 346
    Identification: 0x33aa (13226)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 0.0.0.0
    Destination Address: 255.255.255.255
```

13. What is the value in the transaction ID field of this DHCP Request message? Does it match the transaction IDs of the earlier Discover and Offer messages?

Transaction ID: 0x051b2d6b

Yes, its Transaction ID matches the discover message's & offer message's Transaction ID which equals 0x051b2d6b

That confirms it's the same DHCP session

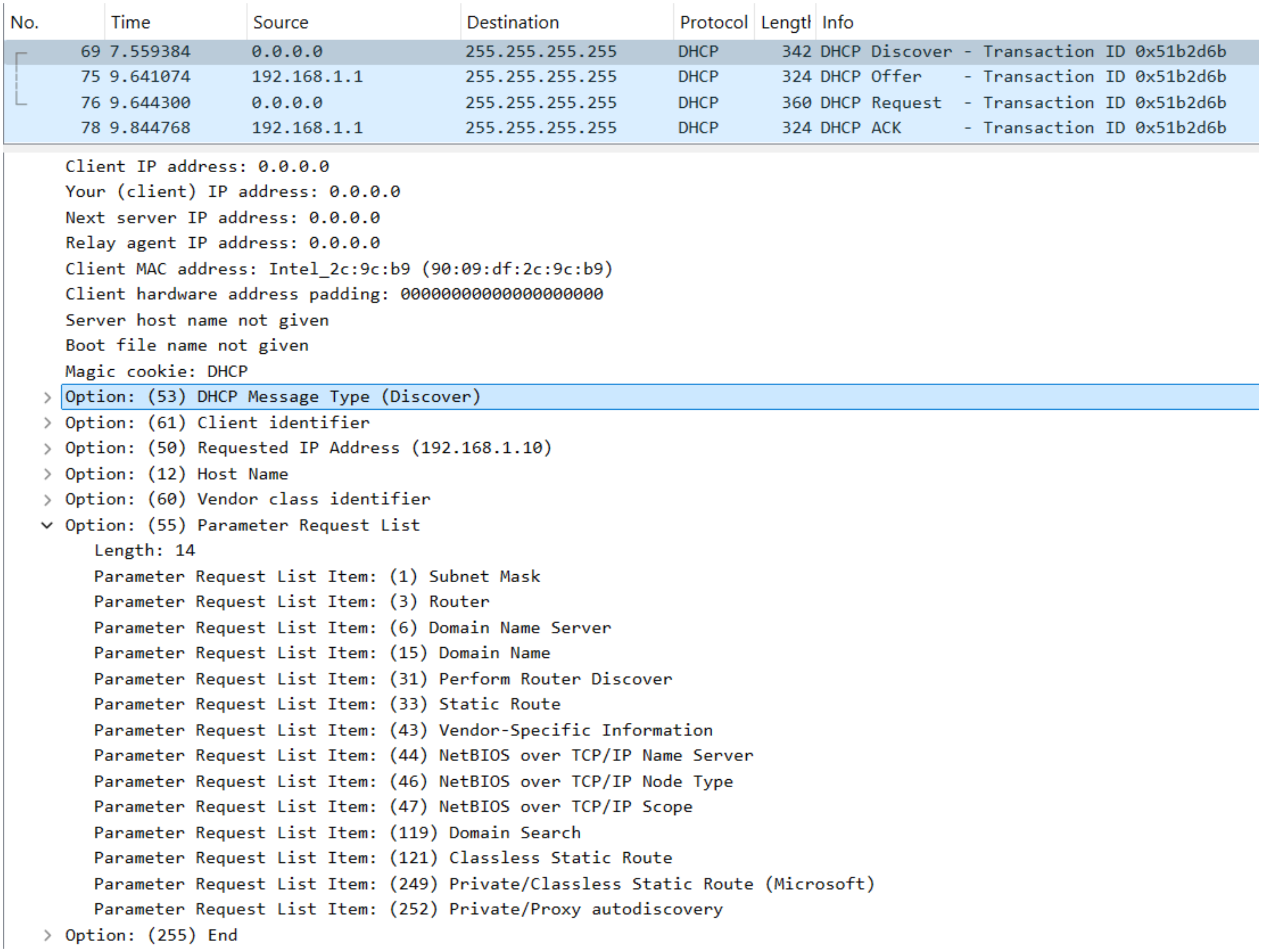


```
No.   Time       Source        Destination       Protocol Lengtl Info
   69 7.559384   0.0.0.0       255.255.255.255   DHCP        342 DHCP Discover - Transaction ID 0x51b2d6b
   75 9.641074   192.168.1.1   255.255.255.255   DHCP        324 DHCP Offer    - Transaction ID 0x51b2d6b
   76 9.644300   0.0.0.0       255.255.255.255   DHCP        360 DHCP Request  - Transaction ID 0x51b2d6b
   78 9.844768   192.168.1.1   255.255.255.255   DHCP        324 DHCP ACK      - Transaction ID 0x51b2d6b

> Frame 76: Packet, 360 bytes on wire (2880 bits), 360 bytes captured (2880 bits) on interface \Device\NPF_{A4CD95BD-AF85-45B8-A02
> Ethernet II, Src: Intel_2c:9c:b9 (90:09:df:2c:9c:b9), 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
v Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x051b2d6b
    Seconds elapsed: 0
```

14. 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?

In this trace, the Parameter Request List in the DHCP Request message is identical to the list in the earlier DHCP Discover message.

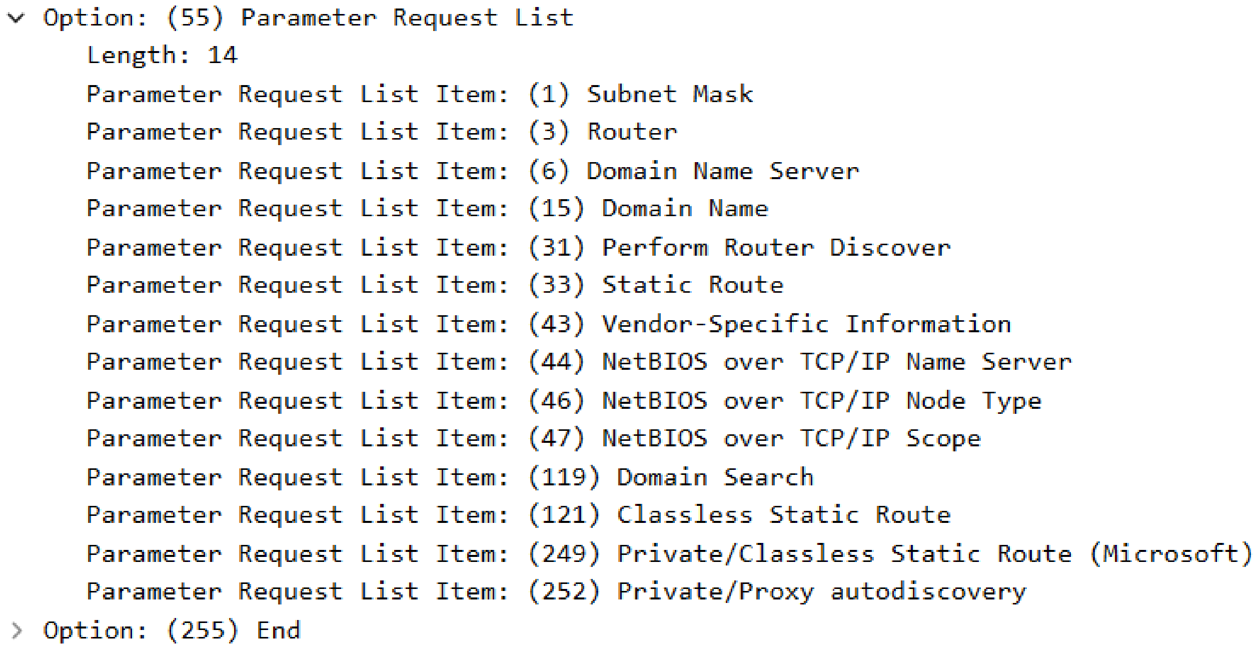
Parameter Request List in the DHCP Discover message:



No.	Time	Source	Destination	Protocol	Lengtl	Info
69	7.559384	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x51b2d6b
75	9.641074	192.168.1.1	255.255.255.255	DHCP	324	DHCP Offer - Transaction ID 0x51b2d6b
76	9.644300	0.0.0.0	255.255.255.255	DHCP	360	DHCP Request - Transaction ID 0x51b2d6b
78	9.844768	192.168.1.1	255.255.255.255	DHCP	324	DHCP ACK - Transaction ID 0x51b2d6b

```
    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: Intel_2c:9c:b9 (90:09:df:2c:9c:b9)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address (192.168.1.10)
  > Option: (12) Host Name
  > Option: (60) Vendor class identifier
  v Option: (55) Parameter Request List
       Length: 14
       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
  > Option: (255) End
```

Parameter Request List in the DHCP Request message:

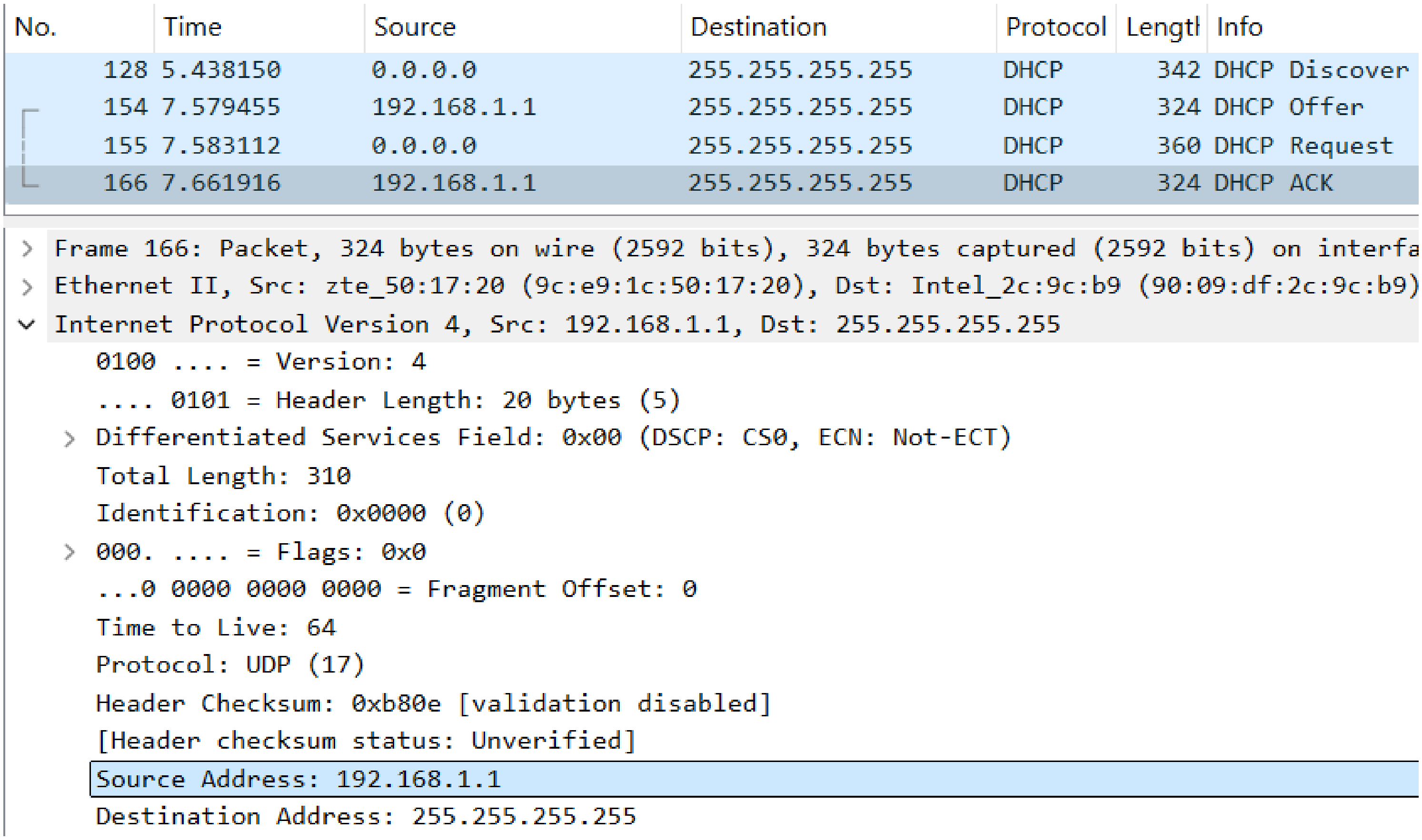


```
⌄ Option: (55) Parameter Request List
     Length: 14
     Parameter Request List Item: (1) Subnet Mask
     Parameter Request List Item: (3) Router
     Parameter Request List Item: (6) Domain Name Server
     Parameter Request List Item: (15) Domain Name
     Parameter Request List Item: (31) Perform 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
› Option: (255) End
```

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

192.168.1.1

Yes, there is something special as this is the DHCP server IP offering the IP address.

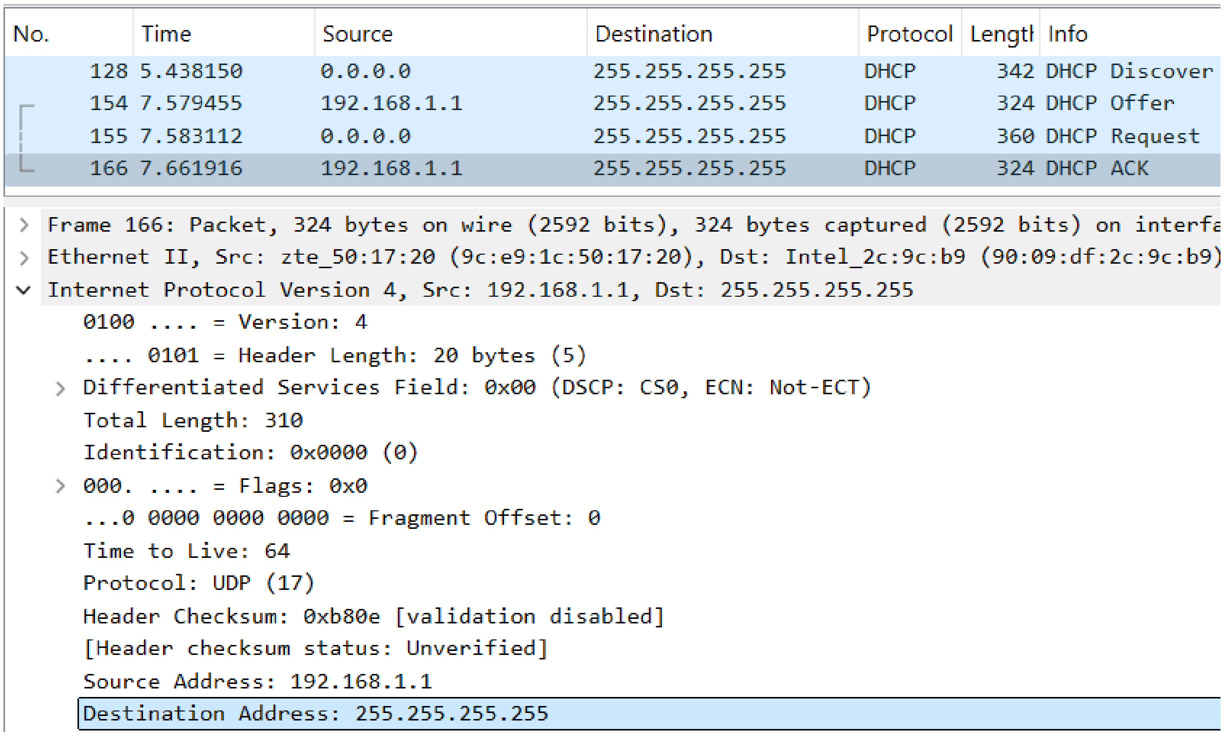


```
No.        Time            Source              Destination         Protocol  Lengtl Info
     128 5.438150        0.0.0.0             255.255.255.255       DHCP         342 DHCP Discover
     154 7.579455        192.168.1.1         255.255.255.255       DHCP         324 DHCP Offer
     155 7.583112        0.0.0.0             255.255.255.255       DHCP         360 DHCP Request
     166 7.661916        192.168.1.1         255.255.255.255       DHCP         324 DHCP ACK

> Frame 166: Packet, 324 bytes on wire (2592 bits), 324 bytes captured (2592 bits) on interfa
> Ethernet II, Src: zte_50:17:20 (9c:e9:1c:50:17:20), Dst: Intel_2c:9c:b9 (90:09:df:2c:9c:b9)
v Internet Protocol Version 4, Src: 192.168.1.1, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 310
    Identification: 0x0000 (0)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0xb80e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.1
    Destination Address: 255.255.255.255
```

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

255.255.255.255

Yes, there is something special as client may still not have IP configured at ACK time the Server broadcasts the offer



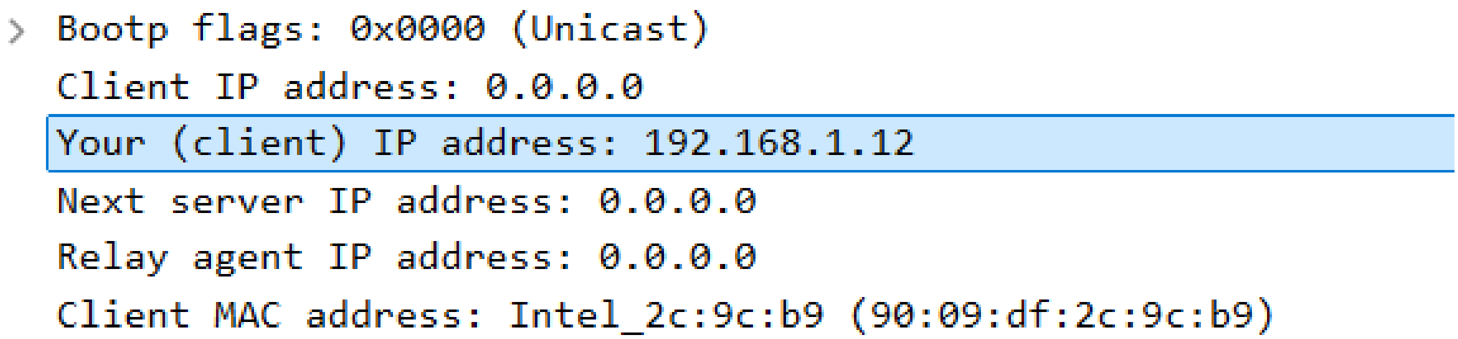
No.	Time	Source	Destination	Protocol	Length	Info
128	5.438150	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover
154	7.579455	192.168.1.1	255.255.255.255	DHCP	324	DHCP Offer
155	7.583112	0.0.0.0	255.255.255.255	DHCP	360	DHCP Request
166	7.661916	192.168.1.1	255.255.255.255	DHCP	324	DHCP ACK

```
> Frame 166: Packet, 324 bytes on wire (2592 bits), 324 bytes captured (2592 bits) on interfa
> Ethernet II, Src: zte_50:17:20 (9c:e9:1c:50:17:20), Dst: Intel_2c:9c:b9 (90:09:df:2c:9c:b9)
v Internet Protocol Version 4, Src: 192.168.1.1, Dst: 255.255.255.255
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 310
     Identification: 0x0000 (0)
   > 000. .... = Flags: 0x0
     ...0 0000 0000 0000 = Fragment Offset: 0
     Time to Live: 64
     Protocol: UDP (17)
     Header Checksum: 0xb80e [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 192.168.1.1
     Destination Address: 255.255.255.255
```

17. 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?

Your (client) IP address

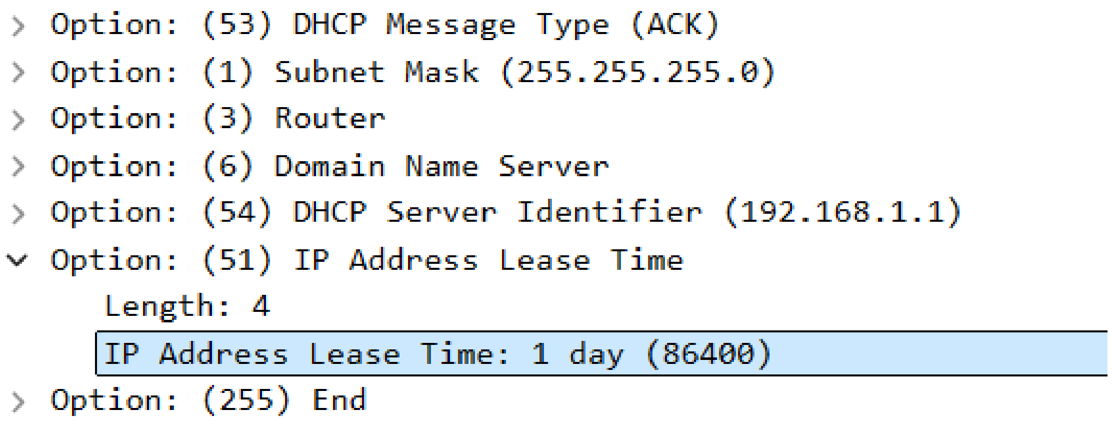
also called yiaddr



```
> Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 192.168.1.12
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: Intel_2c:9c:b9 (90:09:df:2c:9c:b9)
```

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

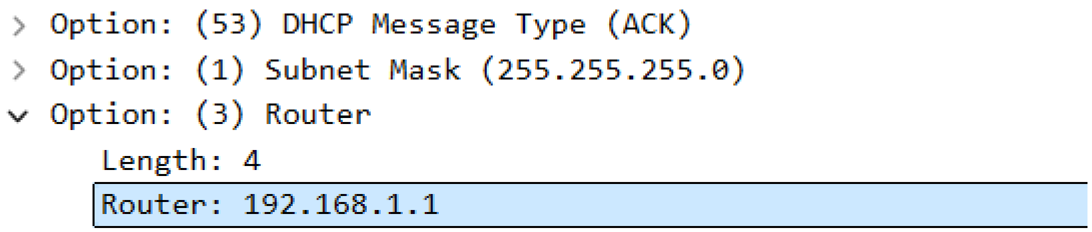
Lease Time: 1 day (86400 seconds)



```
> Option: (53) DHCP Message Type (ACK)
> Option: (1) Subnet Mask (255.255.255.0)
> Option: (3) Router
> Option: (6) Domain Name Server
> Option: (54) DHCP Server Identifier (192.168.1.1)
v Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: 1 day (86400)
> Option: (255) End
```

19. 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?

IP Address: 192.168.1.1



```
> Option: (53) DHCP Message Type (ACK)
> Option: (1) Subnet Mask (255.255.255.0)
v Option: (3) Router
      Length: 4
      Router: 192.168.1.1
```