Computer Networks - Assignment 9

Wireshark Lab : DHCP

Rajasekhar - st119220

Due: 16th October 2017

1 Screen shot of the Command Prompt window

2 Questions

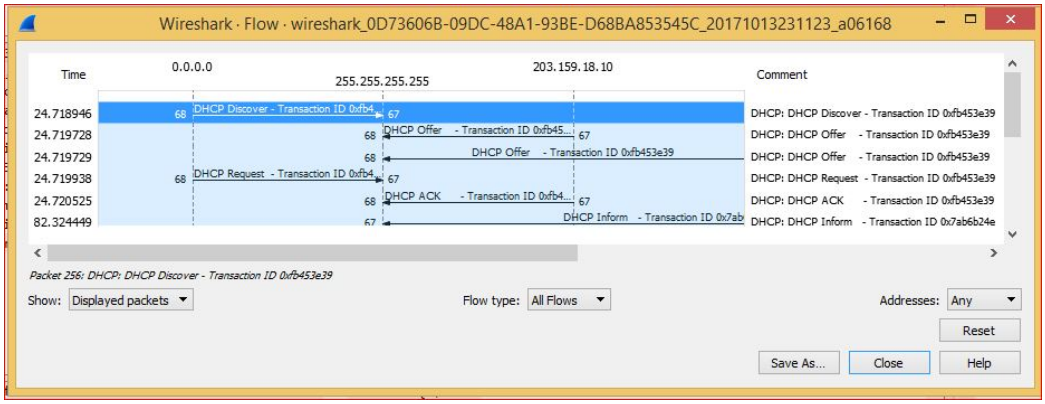
1. **Are DHCP messages are sent over UDP or TCP?**

   – DHCP messages are sent over UDP.

```
Frame 144: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits) on interface 0
Ethernet II, Src: AsustekC_4c:24:a8 (10:c3:7b:4c:24:a8), Dst: HewlettP_39:b0:d7 (d4:85:64:39:b0:d7)
Internet Protocol Version 4, Src: 203.159.18.187, Dst: 203.159.18.10
User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 313
    Checksum: 0xbd4e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 16]
Bootstrap Protocol (Request)
```

2. **Draw a timing datagram illustrating the sequence of the first four-packe 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?**

   – The port numbers are same as the example in the Lab.



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

   – The link-layer address of my host is 10:c3:7b:4c:24:a8.

```
Frame 256: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: AsustekC_4c:24:a8 (10:c3:7b:4c:24:a8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: AsustekC_4c:24:a8 (10:c3:7b:4c:24:a8)
    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
Bootstrap Protocol (Discover)
```

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

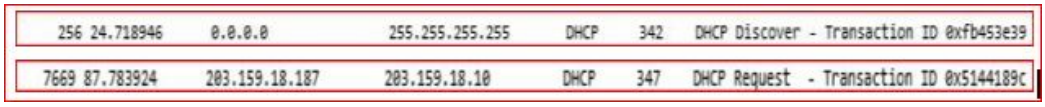
   – The values which differentiate the Discover message from the Request message are in "Option 53: DHCP Message Type".

```
Frame 256: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: AsustekC_4c:24:a8 (10:c3:7b:4c:24:a8), 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
Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xfb453e39
    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: AsustekC_4c:24:a8 (10:c3:7b:4c:24:a8)
    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
    Option: (12) Host Name
    Option: (60) Vendor class identifier
    Option: (55) Parameter Request List
    Option: (255) End
    Padding: 00000000
```

```
Frame 8192: 359 bytes on wire (2872 bits), 359 bytes captured (2872 bits) on interface 0
Ethernet II, Src: AsustekC_4c:24:a8 (10:c3:7b:4c:24:a8), 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
Bootstrap Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x5cfe8018
    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: AsustekC_4c:24:a8 (10:c3:7b:4c:24:a8)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type (Request)
    Option: (61) Client identifier
    Option: (50) Requested IP Address
    Option: (54) DHCP Server Identifier
    Option: (12) Host Name
    Option: (81) Client Fully Qualified Domain Name
    Option: (60) Vendor class identifier
    Option: (55) Parameter Request List
    Option: (255) End
```

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) of DHCP messages? What is the purpose of the Transaction-ID field?**

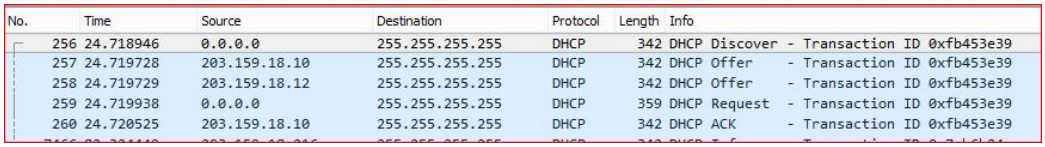
   – The value of the Transaction ID in each of the first four DHCP messages is 0xfb453e39. The second Transaction ID of second set is 0x5144189c. A Transaction ID is used so that the DHCP server can differentiate between client requests during the request process.



256	24.718946	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xfb453e39
7669	87.783924	203.159.18.187	203.159.18.10	DHCP	347	DHCP Request - Transaction ID 0x5144189c

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 DHCP client and server both use 255.255.255.255 as the destination address. The client uses source IP address 0.0.0.0, while the server uses its actual IP address as the source.



No.	Time	Source	Destination	Protocol	Length	Info
256	24.718946	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xfb453e39
257	24.719728	203.159.18.10	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xfb453e39
258	24.719729	203.159.18.12	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xfb453e39
259	24.719938	0.0.0.0	255.255.255.255	DHCP	359	DHCP Request - Transaction ID 0xfb453e39
260	24.720525	203.159.18.10	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xfb453e39

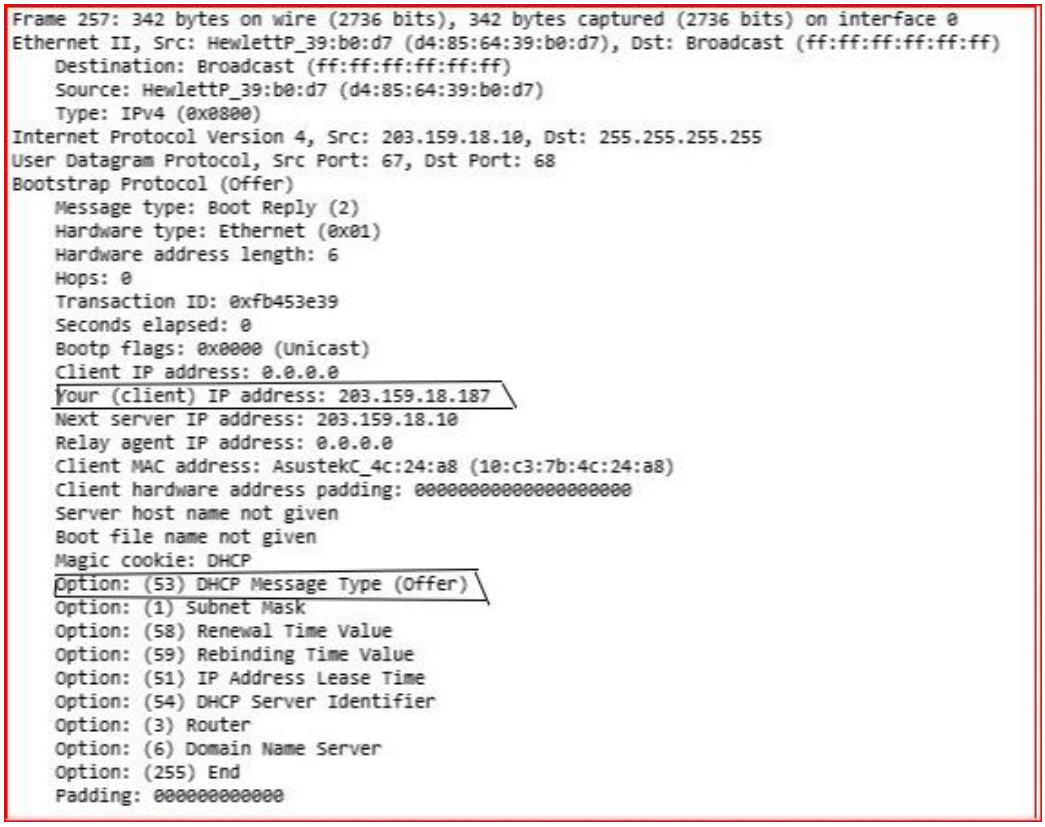
7. **What is the IP address of your DHCP server?**

   – The IP address of the DHCP server is 203.159.18.10.

No.	Time	Source	Destination	Protocol	Length	Info
256	24.718946	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xfb453e39
257	24.719728	203.159.18.10	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xfb453e39
258	24.719729	203.159.18.12	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xfb453e39
259	24.719938	0.0.0.0	255.255.255.255	DHCP	359	DHCP Request - Transaction ID 0xfb453e39
260	24.720525	203.159.18.10	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xfb453e39

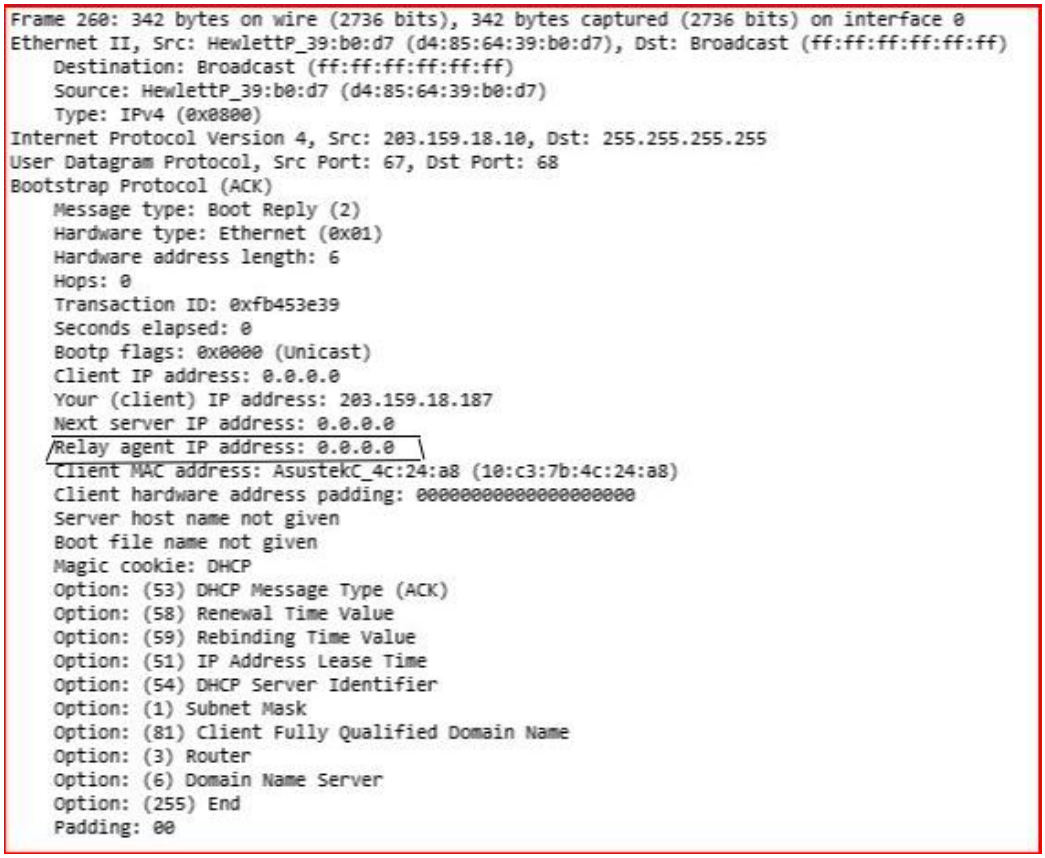
8. **What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.**

   – The DHCP server offered the IP address 203.159.18.187 to my client machine. The DHCP message with "DHCP Message Type (Offer) " contained the offered IP.



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?**

   – The "Relay agent IP address" is 0.0.0.0, which indicates that there is no DHCP Relay used. There was no Relay Agent used in my experiment.



10. **Explain the purpose of the router and subnet mask lines in the DHCP offer message.**

    – The router line indicates to the client what its default gateway should be and the subnet mask line tells the client which subnet mask it should use.

```
Frame 260: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: HewlettP_39:b0:d7 (d4:85:64:39:b0:d7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: HewlettP_39:b0:d7 (d4:85:64:39:b0:d7)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 203.159.18.10, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 67, Dst Port: 68
Bootstrap Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xfb453e39
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 203.159.18.187
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: AsustekC_4c:24:a8 (10:c3:7b:4c:24:a8)
    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: (58) Renewal Time Value
        Length: 4
        Renewal Time Value: (64800s) 18 hours
    Option: (59) Rebinding Time Value
        Length: 4
        Rebinding Time Value: (113400s) 1 day, 7 hours, 30 minutes
    Option: (51) IP Address Lease Time
        Length: 4
        IP Address Lease Time: (129600s) 1 day, 12 hours
    Option: (54) DHCP Server Identifier
        Length: 4
        DHCP Server Identifier: 203.159.18.10
    Option: (1) Subnet Mask
        Length: 4
        Subnet Mask: 255.255.255.0
    Option: (81) Client Fully Qualified Domain Name
        Length: 3
        Flags: 0x00
        A-RR result: 255
        PTR-RR result: 255
    Option: (3) Router
        Length: 4
        Router: 203.159.18.1
    Option: (6) Domain Name Server
        Length: 12
        Domain Name Server: 203.159.0.1
        Domain Name Server: 8.8.8.8
        Domain Name Server: 203.159.0.10
    Option: (255) End
        Option End: 255
    Padding: 00
```

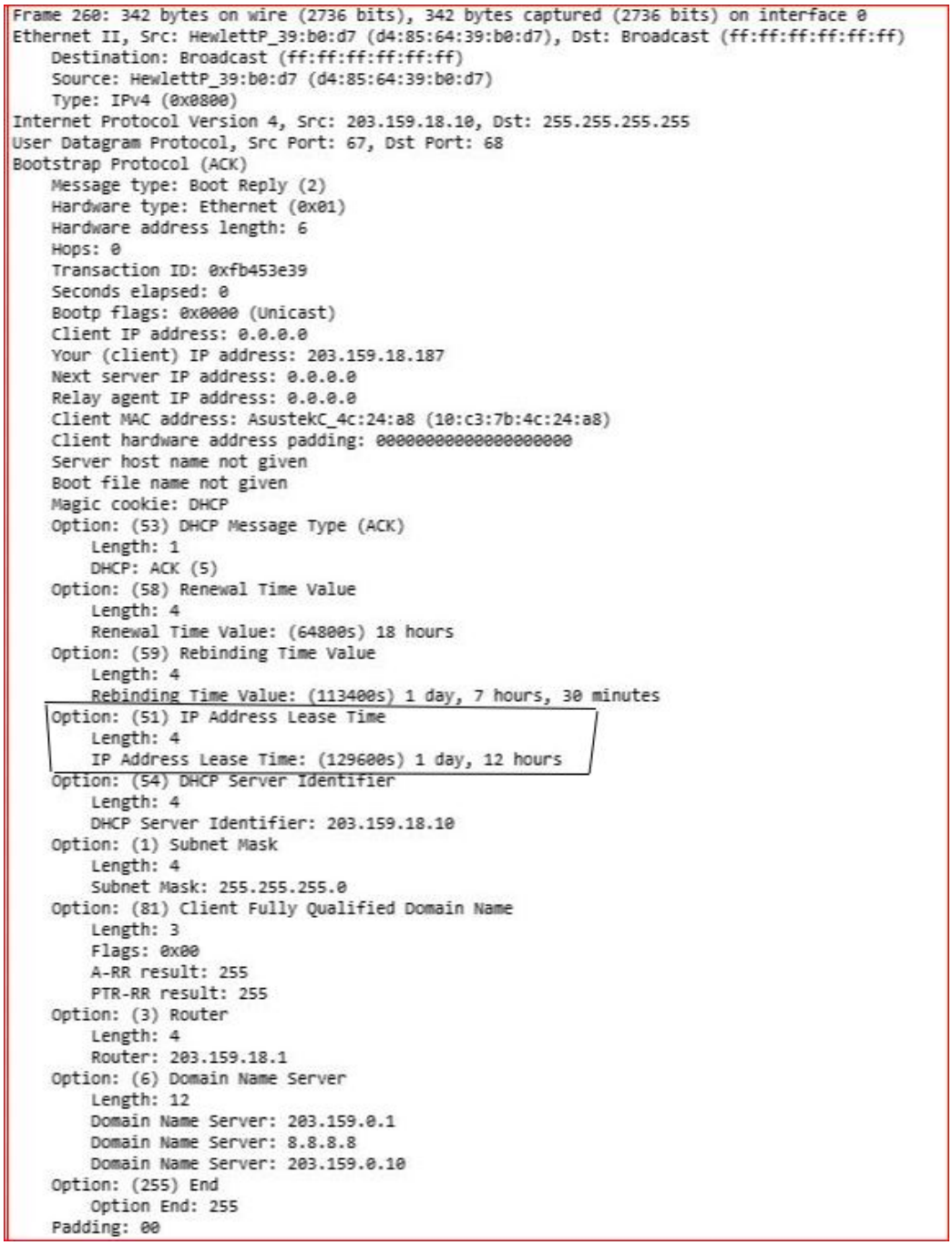
11. **In the DHCP trace file noted in footnote 2, the DHCP server offers a specific IP address to the client (see also question 8. above). In the client's response to the first server OFFER message, does the client accept this IP address? Where in the client's RESPONSE is the client's requested address?**

   – In my experiment, the host requests the offered IP address in the DHCP Request message.

```
Frame 259: 359 bytes on wire (2872 bits), 359 bytes captured (2872 bits) on interface 0
Ethernet II, Src: AsustekC_4c:24:a8 (10:c3:7b:4c:24:a8), 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
Bootstrap Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xfb453e39
    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: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: AsustekC_4c:24:a8 (10:c3:7b:4c:24:a8)
    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: AsustekC_4c:24:a8 (10:c3:7b:4c:24:a8)
    Option: (50) Requested IP Address
        Length: 4
        Requested IP Address: 203.159.18.187
    Option: (54) DHCP Server Identifier
        Length: 4
        DHCP Server Identifier: 203.159.18.10
    Option: (12) Host Name
        Length: 10
        Host Name: TCLAB-PC07
    Option: (81) Client Fully Qualified Domain Name
        Length: 13
        Flags: 0x00
        A-RR result: 0
        PTR-RR result: 0
        Client name: TCLAB-PC07
    Option: (60) Vendor class identifier
        Length: 8
        Vendor class identifier: MSFT 5.0
    Option: (55) Parameter Request List
        Length: 13
        Parameter Request List Item: (1) Subnet Mask
        Parameter Request List Item: (15) Domain Name
        Parameter Request List Item: (3) Router
        Parameter Request List Item: (6) Domain Name Server
        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: (31) Perform Router Discover
        Parameter Request List Item: (33) Static Route
        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
        Parameter Request List Item: (43) Vendor-Specific Information
    Option: (255) End
        Option End: 255
```

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

    – The lease time is the amount of time the DHCP server assigns an IP address to a client. During the lease time, the DHCP server will not assign the IP given to the client to another client, unless it is released by the client. Once the lease time has expired, the IP address can be reused by the DHCP server to give to another client. In my experiment, the lease time is 1 day, 12 hours .



```
Frame 260: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: HewlettP_39:b0:d7 (d4:85:64:39:b0:d7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: HewlettP_39:b0:d7 (d4:85:64:39:b0:d7)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 203.159.18.10, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 67, Dst Port: 68
Bootstrap Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xfb453e39
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 203.159.18.187
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: AsustekC_4c:24:a8 (10:c3:7b:4c:24:a8)
    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: (58) Renewal Time Value
        Length: 4
        Renewal Time Value: (64800s) 18 hours
    Option: (59) Rebinding Time Value
        Length: 4
        Rebinding Time Value: (113400s) 1 day, 7 hours, 30 minutes
    Option: (51) IP Address Lease Time
        Length: 4
        IP Address Lease Time: (129600s) 1 day, 12 hours
    Option: (54) DHCP Server Identifier
        Length: 4
        DHCP Server Identifier: 203.159.18.10
    Option: (1) Subnet Mask
        Length: 4
        Subnet Mask: 255.255.255.0
    Option: (81) Client Fully Qualified Domain Name
        Length: 3
        Flags: 0x00
        A-RR result: 255
        PTR-RR result: 255
    Option: (3) Router
        Length: 4
        Router: 203.159.18.1
    Option: (6) Domain Name Server
        Length: 12
        Domain Name Server: 203.159.0.1
        Domain Name Server: 8.8.8.8
        Domain Name Server: 203.159.0.10
    Option: (255) End
        Option End: 255
    Padding: 00
```

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?**

    – The client sends a DHCP Release message to cancel its lease on the IP address given to it by the DHCP server. The DHCP server does not send a message back to the client acknowledging the DHCP Release message. If the DHCP Release message from the client is lost, the DHCP server would have to wait until the lease period is over for that IP address until it could reuse it for another client.

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, there are ARP requests made by the DHCP server. Before offering an IP address to a client, the DHCP server issues an ARP request for the offered IP to make sure the IP address is not already in use by another workstation.