Computer Networks Lab
CS359

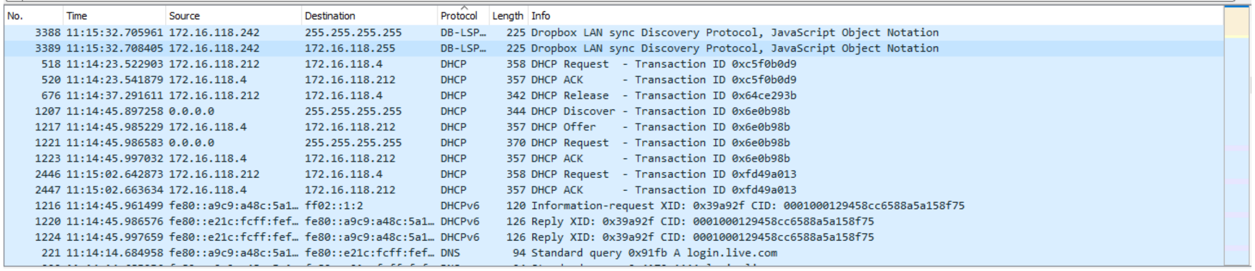
Tanishq Malu Lab:6 1901CS63

Objective:

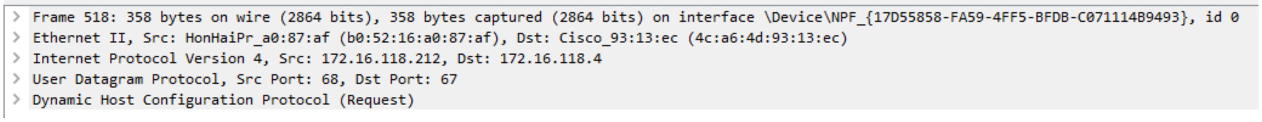
To see how DHCP (Dynamic Host Configuration Protocol) works. DHCP is an essential glue protocol that is used to configure your computer with an IP address, as well as other information.

To capture DHCP packet trace:

1. Start wireshark capture.
2. Open command prompt
3. Type : ipconfig /renew
   : ipconfig /release
   : ipconfig /renew
4. Close command prompt
5. Stop wireshark capture.



```
No.  Time            Source              Destination         Protocol Length Info
3388 11:15:32.705961 172.16.118.242      255.255.255.255     DB-LSP…  225 Dropbox LAN sync Discovery Protocol, JavaScript Object Notation
3389 11:15:32.708405 172.16.118.242      172.16.118.255      DB-LSP…  225 Dropbox LAN sync Discovery Protocol, JavaScript Object Notation
 518 11:14:23.522903 172.16.118.212      172.16.118.4        DHCP     358 DHCP Request  - Transaction ID 0xc5f0b0d9
 520 11:14:23.541879 172.16.118.4        172.16.118.212      DHCP     357 DHCP ACK      - Transaction ID 0xc5f0b0d9
 676 11:14:37.291611 172.16.118.212      172.16.118.4        DHCP     342 DHCP Release  - Transaction ID 0x64ce293b
1207 11:14:45.897258 0.0.0.0             255.255.255.255     DHCP     344 DHCP Discover - Transaction ID 0x6e0b98b
1217 11:14:45.985229 172.16.118.4        172.16.118.212      DHCP     357 DHCP Offer    - Transaction ID 0x6e0b98b
1221 11:14:45.986583 0.0.0.0             255.255.255.255     DHCP     370 DHCP Request  - Transaction ID 0x6e0b98b
1223 11:14:45.997032 172.16.118.4        172.16.118.212      DHCP     357 DHCP ACK      - Transaction ID 0x6e0b98b
2446 11:15:02.642873 172.16.118.212      172.16.118.4        DHCP     358 DHCP Request  - Transaction ID 0xfd49a013
2447 11:15:02.663634 172.16.118.4        172.16.118.212      DHCP     357 DHCP ACK      - Transaction ID 0xfd49a013
1216 11:14:45.961499 fe80::a9c9:a48c:5a1… ff02::1:2          DHCPv6   120 Information-request XID: 0x39a92f CID: 0001000129458cc6588a5a158f75
1220 11:14:45.986576 fe80::e21c:fcff:fef… fe80::a9c9:a48c:5a1… DHCPv6 126 Reply XID: 0x39a92f CID: 0001000129458cc6588a5a158f75
1224 11:14:45.997659 fe80::e21c:fcff:fef… fe80::a9c9:a48c:5a1… DHCPv6 126 Reply XID: 0x39a92f CID: 0001000129458cc6588a5a158f75
 221 11:14:14.684958 fe80::a9c9:a48c:5a1… fe80::e21c:fcff:fef… DNS     94 Standard query 0x91fb A login.live.com
```



```
> Frame 518: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits) on interface \Device\NPF_{17D55858-FA59-4FF5-BFDB-C071114B9493}, id 0
> Ethernet II, Src: HonHaiPr_a0:87:af (b0:52:16:a0:87:af), Dst: Cisco_93:13:ec (4c:a6:4d:93:13:ec)
> Internet Protocol Version 4, Src: 172.16.118.212, Dst: 172.16.118.4
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Request)
```

Answer the following questions based on your examination of the DHCP fields for both the DHCP Request and DHCP Ack.

1.
How long is the Transaction ID field? Say whether it is likely that concurrent DHCP operations done by different computers will happen to pick the same Transaction ID.

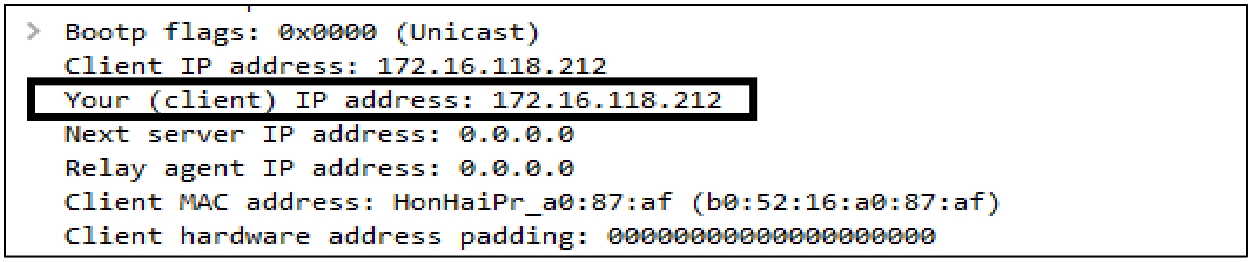
ANS:

The transaction Id is 32 bits long. It will be quite rare that concurrent DHCP operations done by a large number of computers will collide unless that number approaches 2^32 (which is quite large).

2.
What is the name of the field that carries the IP address that is being assigned to the client? You will find this field filled in on the DHCP Ack, as that message is completing the assignment.

ANS:

The “Your (client) IP address” field carries the IP address being assigned to the client.



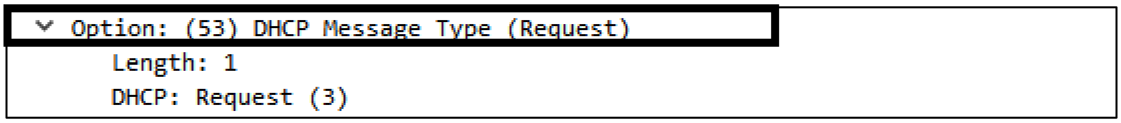
```
> Bootp flags: 0x0000 (Unicast)
  Client IP address: 172.16.118.212
  Your (client) IP address: 172.16.118.212
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: HonHaiPr_a0:87:af (b0:52:16:a0:87:af)
  Client hardware address padding: 00000000000000000000
```

3.
The first DHCP option is DHCP Message Type. What option value stands for this type? DHCP Requests will typically have a Client Identifier option. Look at the value of this option. How does it identify the client? Take a guess.

ANS:

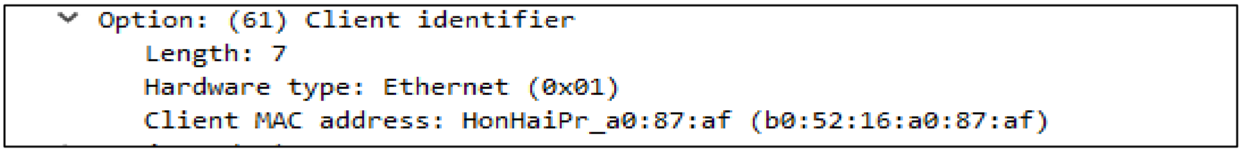
The option value of 53 is allotted for first DHCP Message Type.

Length: 1
DHCP: Request (3)



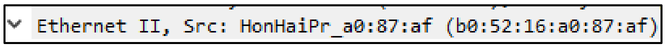
```
v Option: (53) DHCP Message Type (Request)
      Length: 1
      DHCP: Request (3)
```

Typically, the Client Identifier carry the Ethernet address of the client, but I guess it is also possible to use some other kind of identifier like: hostname.



```
  v Option: (61) Client identifier
        Length: 7
        Hardware type: Ethernet (0x01)
        Client MAC address: HonHaiPr_a0:87:af (b0:52:16:a0:87:af)
```

As you can see my Ethernet source address is same as my client Identifier address.

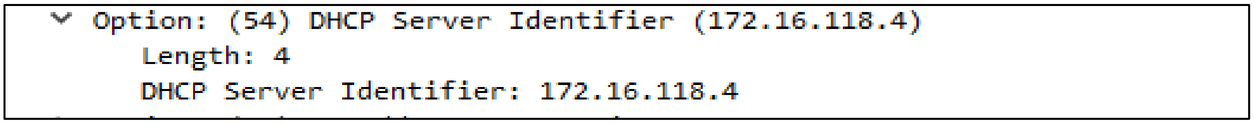


```
v Ethernet II, Src: HonHaiPr_a0:87:af (b0:52:16:a0:87:af)
```

4.
DHCP Ack will typically have a Server Identifier Option. Look at the value of this option. How does it identify the server? Take a guess.

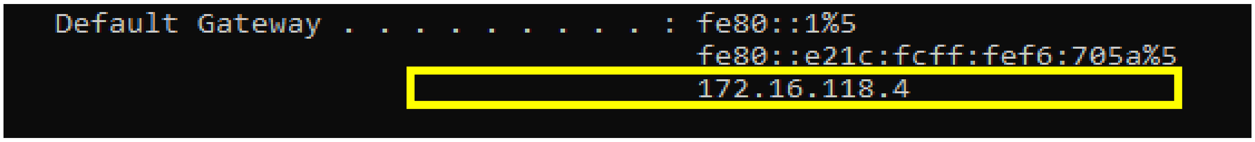
ANS:

Typically, the Server Identifier carry the IP address of the DHCP server, but I guess it is also possible to use some other kind of identifier.



```
 ˅ Option: (54) DHCP Server Identifier (172.16.118.4)
       Length: 4
       DHCP Server Identifier: 172.16.118.4
```

ON running ipconfig command on CMD, we get



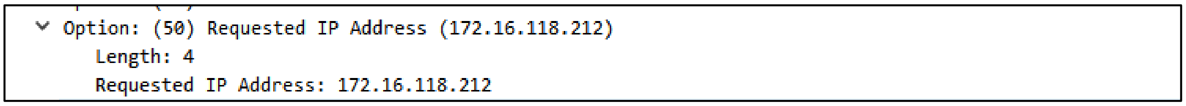
```
   Default Gateway . . . . . . . . . : fe80::1%5
                                       fe80::e21c:fcff:fef6:705a%5
                                       172.16.118.4
```

5.
What option value stands for the Requested IP Address option? And for the IP Address Lease Time option?

ANS:

The option value of 50 stands for Requested IP Address.

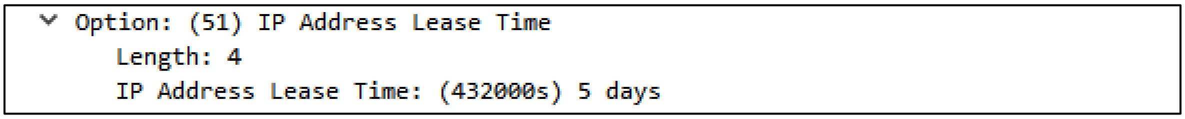
And its values is the Ip address which it requests, in this case it is: 172.16.118.212



```
 ˅ Option: (50) Requested IP Address (172.16.118.212)
       Length: 4
       Requested IP Address: 172.16.118.212
```

The option value of 51 stands for IP Address Lease Time.

Its values is: 432000s or 5 days.

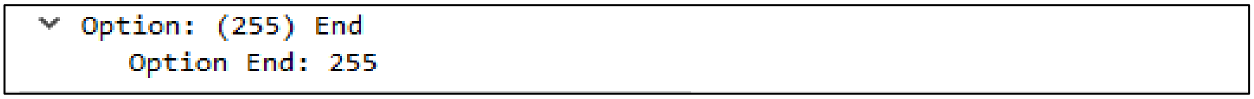


```
 ˅ Option: (51) IP Address Lease Time
       Length: 4
       IP Address Lease Time: (432000s) 5 days
```

6.
How does the recipient of a DHCP message know that it has reached the last option?

ANS:

The end of the DHCP options is identified with a DHCP option called End with value 255.

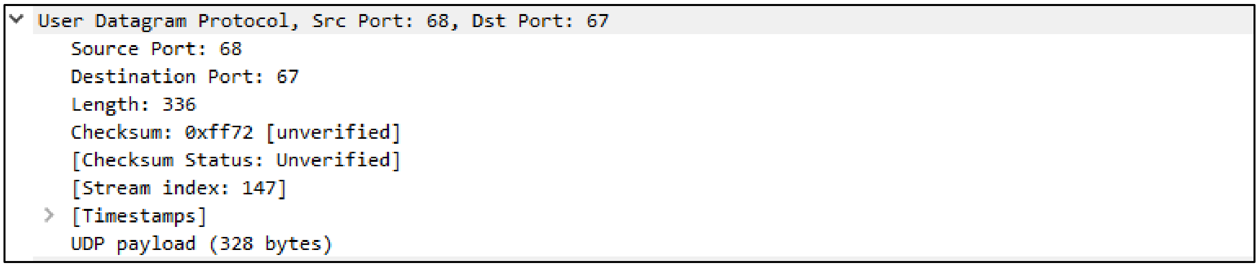


```
v Option: (255) End
      Option End: 255
```

Answer the following questions by selecting a DHCP Request packet and looking at its UDP details in the middle Wireshark panel.

1.
What port number does the DHCP client use, and what port number does the DHCP server use?

ANS:
The DHCP client uses UDP port 68
the DHCP server uses UDP port 67.

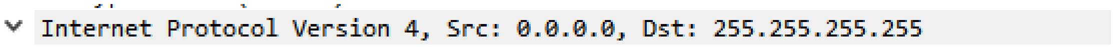


```
v User Datagram Protocol, Src Port: 68, Dst Port: 67
     Source Port: 68
     Destination Port: 67
     Length: 336
     Checksum: 0xff72 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 147]
   > [Timestamps]
     UDP payload (328 bytes)
```

2.
What source IP address is put on the Request message? It is a special value meaning “this host on this network” used for initialization.

ANS:

The source IP address is 0.0.0.0



```
v Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
```

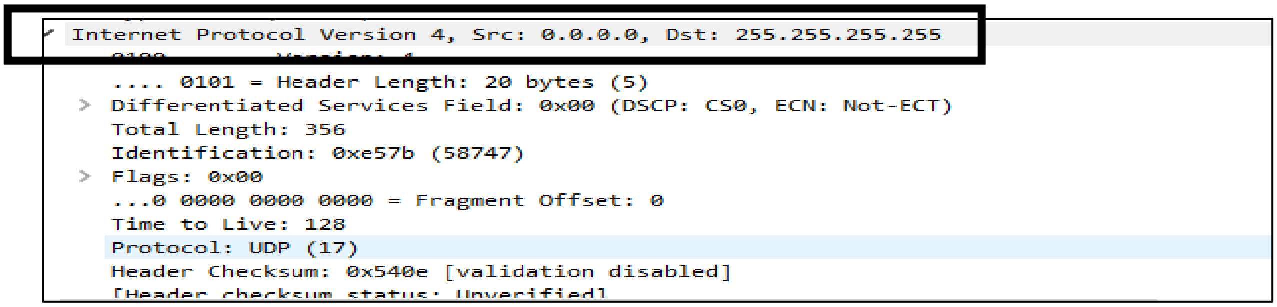
3.

What destination IP address is put on the Request message? It is also a reserved value designed to reach the DHCP server wherever it is on the local network

ANS:

The destination IP address is 255.255.255.255.

It is the broadcast address, which means the message is intended for all computers on the network.



```
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: 356
    Identification: 0xe57b (58747)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x540e [validation disabled]
    [Header checksum status: Unverified]
```

4.

What source Ethernet address is put on the Request message, and what destination Ethernet address is put on the Request message? One of these addresses is a reserved address.

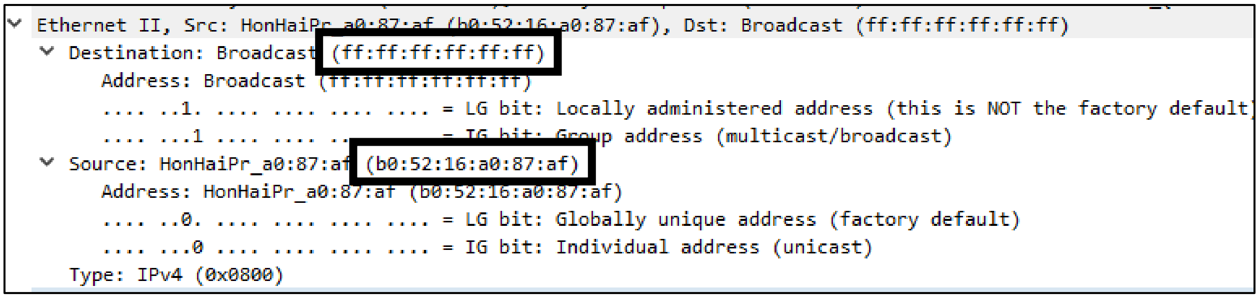
ANS:

Ethernet source address = b0 : 52 : 16 : a0 : 87 : af

Ethernet Destination address = ff : ff : ff : ff : ff : ff

The Ethernet source address is one's own computer's Ethernet address because that has already been assigned.

The Ethernet destination address is the reserved broadcast Ethernet address, so that the packet reaches all computers on the local network.



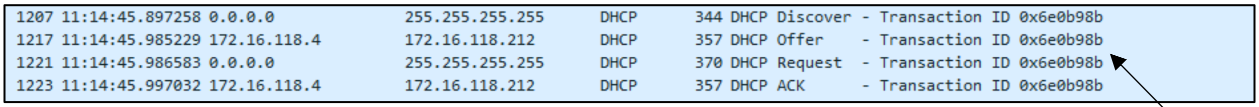
```
Ethernet II, Src: HonHaiPr_a0:87:af (b0:52:16:a0:87:af), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  Source: HonHaiPr_a0:87:af (b0:52:16:a0:87:af)
      Address: HonHaiPr_a0:87:af (b0:52:16:a0:87:af)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
```

5.

How does a computer work out whether a DHCP message it receives is intended as a reply to its DHCP Request message, and not a reply to another computer? Hint: If you are not sure then go over the fields you inspected previously

ANS:

The DHCP message uses the same Transaction ID from request to ACK. Thus, a computer looks for a DHCP reply such as an Ack with a Transaction ID that matches the value it allotted to the earlier DHCP message such as a Request.



```
1207 11:14:45.897258 0.0.0.0           255.255.255.255      DHCP      344 DHCP Discover - Transaction ID 0x6e0b98b
1217 11:14:45.985229 172.16.118.4      172.16.118.212       DHCP      357 DHCP Offer    - Transaction ID 0x6e0b98b
1221 11:14:45.986583 0.0.0.0           255.255.255.255      DHCP      370 DHCP Request  - Transaction ID 0x6e0b98b
1223 11:14:45.997032 172.16.118.4      172.16.118.212       DHCP      357 DHCP ACK      - Transaction ID 0x6e0b98b
```

Notice the same Transaction ID for DHCP – DORA operations.

-- The End ---