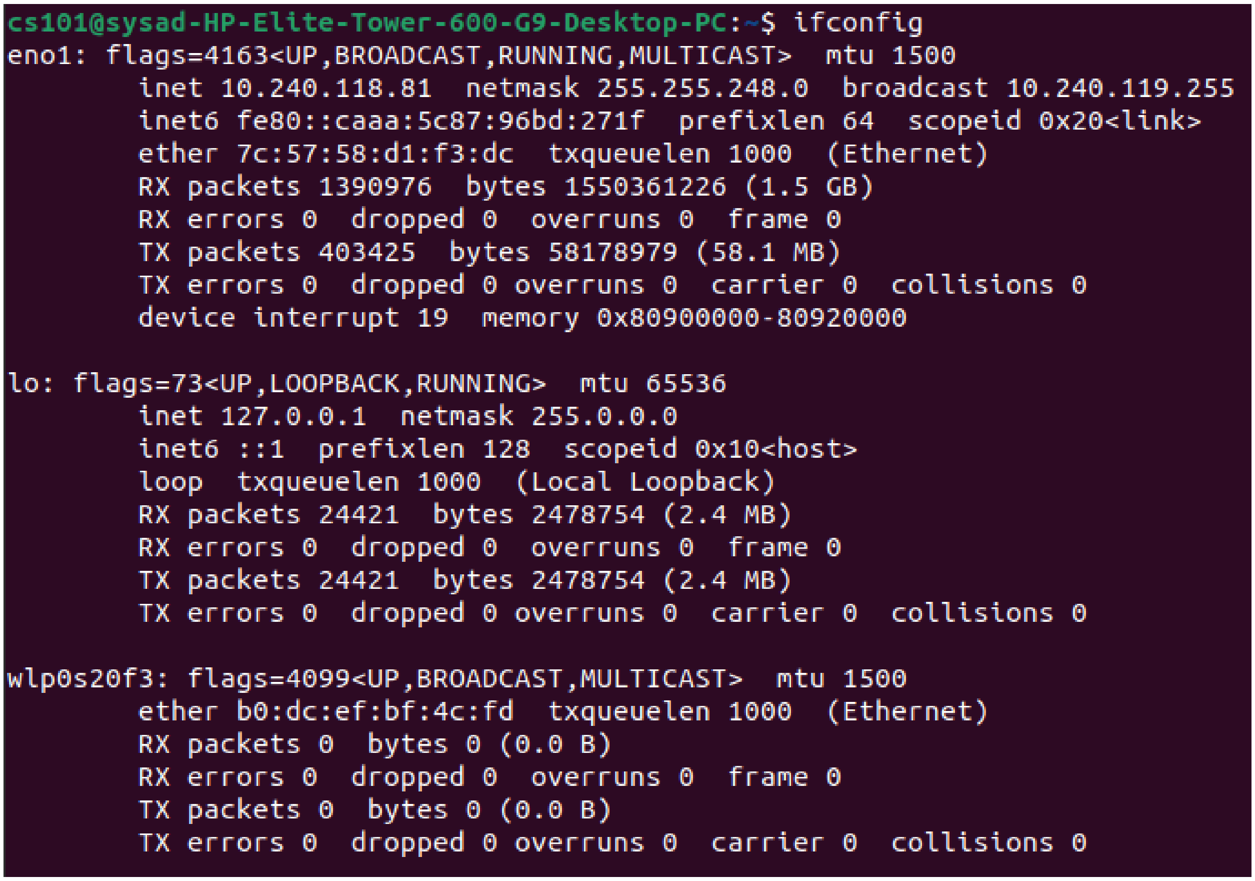
CS 315 : Computer Networks Lab
Assignment - 9
Wireshark Lab: DHCP

Ayush Mallick
CS22BT008

Part-0



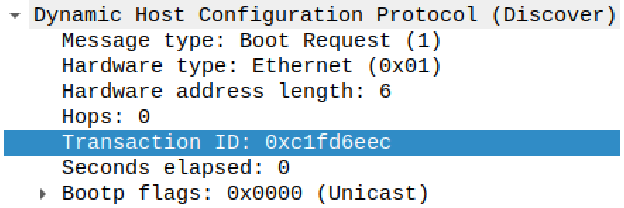
```
cs101@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ ifconfig
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.240.118.81  netmask 255.255.248.0  broadcast 10.240.119.255
        inet6 fe80::caaa:5c87:96bd:271f  prefixlen 64  scopeid 0x20<link>
        ether 7c:57:58:d1:f3:dc  txqueuelen 1000  (Ethernet)
        RX packets 1390976  bytes 1550361226 (1.5 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 403425  bytes 58178979 (58.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  memory 0x80900000-80920000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24421  bytes 2478754 (2.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24421  bytes 2478754 (2.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp0s20f3: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether b0:dc:ef:bf:4c:fd  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Part-1

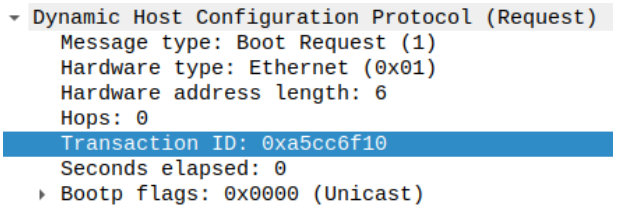
1.1

The Transaction ID in a DHCP Discover message is a 32-bit number that uniquely identifies the DHCP transaction.
It is generated by the *client* (the device requesting an IP address).
It allows the client to match incoming DHCP responses to the corresponding request, and ensures that responses from the server are correctly associated with the client's request, also preventing cross-talk between different DHCP transactions occurring simultaneously.

There are two DHCP transactions here, with transaction IDs : ‘*0xc1fd6eec*’ and ‘*0xa5cc6f10*’.



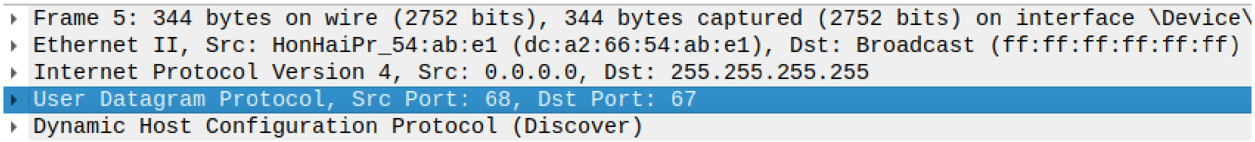
```
▾ Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xc1fd6eec
    Seconds elapsed: 0
  ▸ Bootp flags: 0x0000 (Unicast)
```



```
▾ Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xa5cc6f10
    Seconds elapsed: 0
  ▸ Bootp flags: 0x0000 (Unicast)
```

1.2

UDP (User Datagram Protocol)

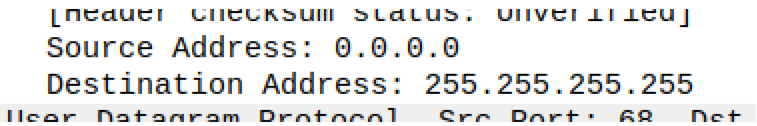


```
▸ Frame 5: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\
▸ Ethernet II, Src: HonHaiPr_54:ab:e1 (dc:a2:66:54:ab:e1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
▸ User Datagram Protocol, Src Port: 68, Dst Port: 67
▸ Dynamic Host Configuration Protocol (Discover)
```

1.3

Source IP : *0.0.0.0*
Destination IP : *255.255.255.255*

The client does not have an IP address yet when it sends a DHCP Discover message, so it uses *0.0.0.0* as the source. The destination address *255.255.255.255* ensures that all DHCP servers on the local network receive the request.

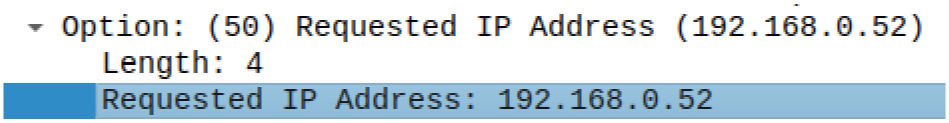


```
    [Header checksum status: Unverified]
    Source Address: 0.0.0.0
    Destination Address: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst
```

1.4

The Requested IP Address field in a DHCP Discover packet indicates the IP address that the client desires (usually the IP it had before). If the requested IP is available, the server may offer it, and if not, the server may offer a different IP address.

Requested IP address : *192.168.0.52*

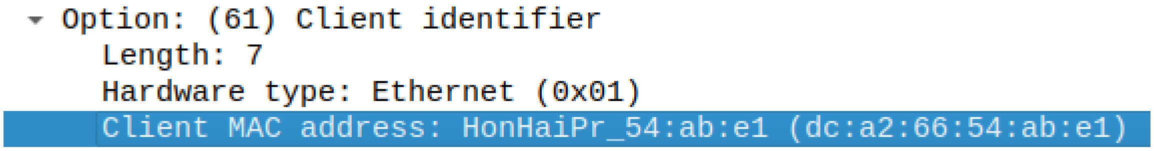


```
▾ Option: (50) Requested IP Address (192.168.0.52)
    Length: 4
    Requested IP Address: 192.168.0.52
```

1.5

The MAC address located in the ‘Client MAC Address’ field of the DHCP Discover packet is crucial because DHCP uses it to uniquely identify the client on the local network and ensures that the correct device receives the IP address assignment. It is also used in creating permanent IP leases (DHCP reservations).

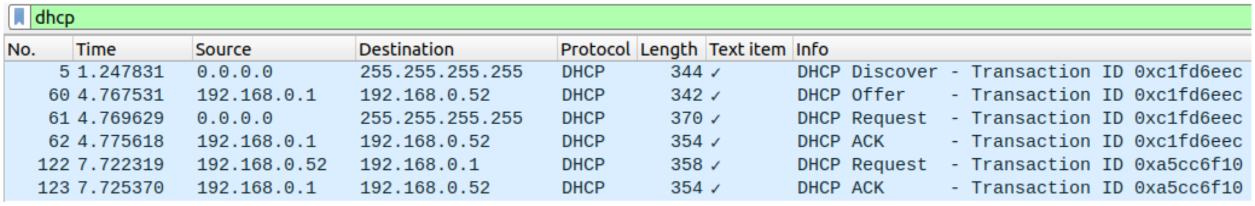
Client MAC Address : *dc:a2:66:54:ab:e1*



```
▾ Option: (61) Client identifier
    Length: 7
    Hardware type: Ethernet (0x01)
    Client MAC address: HonHaiPr_54:ab:e1 (dc:a2:66:54:ab:e1)
```

1.6

We know that this Offer message is being sent in response to the DHCP Discover message since the Transaction ID in the DHCP Offer matches the Transaction ID in the DHCP Discover. Moreover, the Client MAC Address in both messages also match.



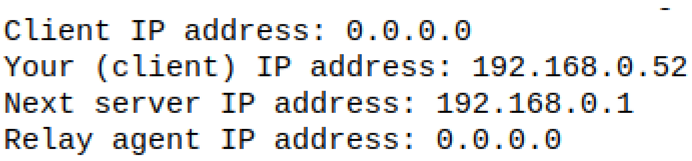
dhcp

No.	Time	Source	Destination	Protocol	Length	Text item	Info
5	1.247831	0.0.0.0	255.255.255.255	DHCP	344	✓	DHCP Discover - Transaction ID 0xc1fd6eec
60	4.767531	192.168.0.1	192.168.0.52	DHCP	342	✓	DHCP Offer - Transaction ID 0xc1fd6eec
61	4.769629	0.0.0.0	255.255.255.255	DHCP	370	✓	DHCP Request - Transaction ID 0xc1fd6eec
62	4.775618	192.168.0.1	192.168.0.52	DHCP	354	✓	DHCP ACK - Transaction ID 0xc1fd6eec
122	7.722319	192.168.0.52	192.168.0.1	DHCP	358	✓	DHCP Request - Transaction ID 0xa5cc6f10
123	7.725370	192.168.0.1	192.168.0.52	DHCP	354	✓	DHCP ACK - Transaction ID 0xa5cc6f10

1.7

Client-assigned IP address : *192.168.0.52*
Next-hop IP address : *192.168.0.1*

These addresses assist in routing the response back to the correct client.

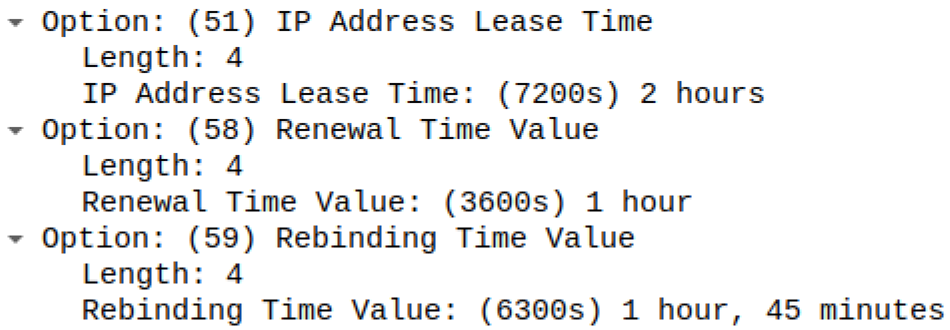


```
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.0.52
Next server IP address: 192.168.0.1
Relay agent IP address: 0.0.0.0
```

1.8

Lease Time is the total time for which the IP address is valid. Renewal Time is the time when the client tries to renew the lease from the original DHCP server. It is typically 50% of the lease time. Rebinding Time is the time to renew the lease from any available DHCP server. It is typically 87.5% of the lease time.

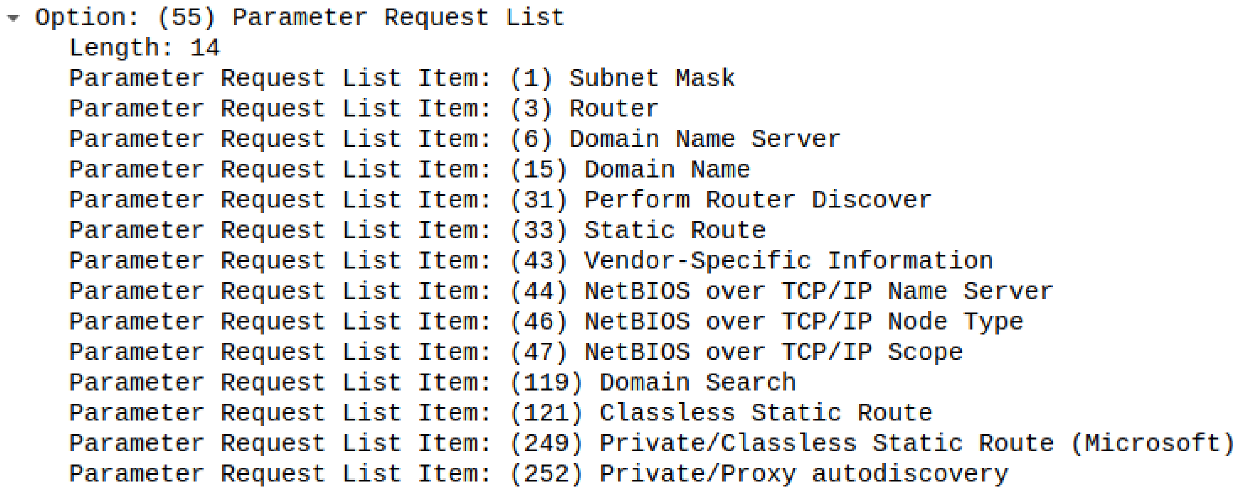
Lease Time : *7200 seconds*
Renewal Time : *3600 seconds*
Rebinding Time : *6300 seconds*



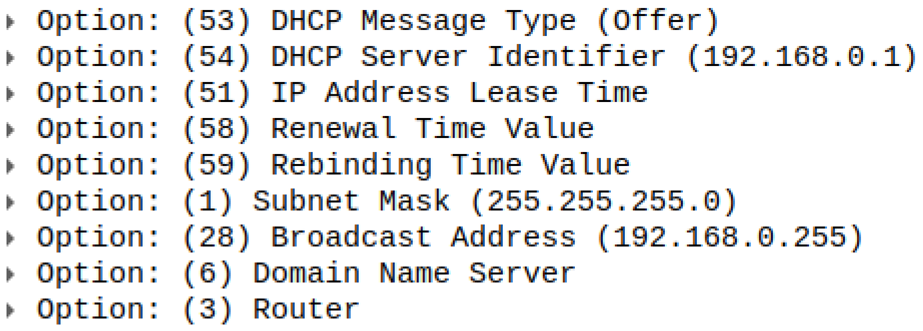
```
▾ Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (7200s) 2 hours
▾ Option: (58) Renewal Time Value
    Length: 4
    Renewal Time Value: (3600s) 1 hour
▾ Option: (59) Rebinding Time Value
    Length: 4
    Rebinding Time Value: (6300s) 1 hour, 45 minutes
```

1.9

Subnet Mask (1)
Router (3)
Domain Name Server (6)



```
▾ 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: (53) DHCP Message Type (Offer)
▸ Option: (54) DHCP Server Identifier (192.168.0.1)
▸ Option: (51) IP Address Lease Time
▸ Option: (58) Renewal Time Value
▸ Option: (59) Rebinding Time Value
▸ Option: (1) Subnet Mask (255.255.255.0)
▸ Option: (28) Broadcast Address (192.168.0.255)
▸ Option: (6) Domain Name Server
▸ Option: (3) Router
```

1.10

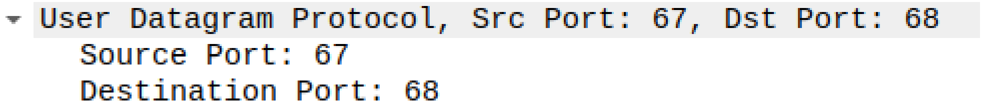
The Client MAC Address in the DHCP Discover message allows the server to identify the client. The Transaction ID further helps to match responses.

1.11

The broadcast IP address is *255.255.255.255*. It ensures that the DHCP Discover message reaches all DHCP servers on the local subnet.

1.12

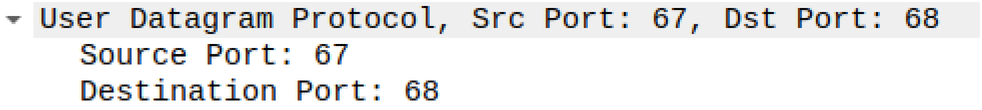
Transport Layer Protocol : *UDP (User Datagram Protocol)*
Source Port : *67*
Destination Port : *68*



```
▾ User Datagram Protocol, Src Port: 67, Dst Port: 68
    Source Port: 67
    Destination Port: 68
```

1.13

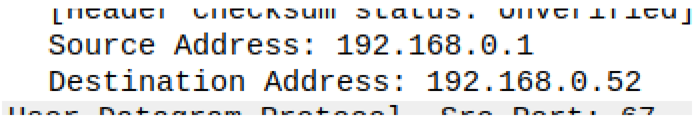
Source Port : *67*
Destination Port : *68*



```
▾ User Datagram Protocol, Src Port: 67, Dst Port: 68
    Source Port: 67
    Destination Port: 68
```

1.14

The source IP address in the DHCP ACK message is the DHCP server's IP address, and the destination IP address is the client's newly assigned IP address.



```
    [Header checksum status: Unverified]
    Source Address: 192.168.0.1
    Destination Address: 192.168.0.52
  User Datagram Protocol, Src Port: 67
```