Investigation of DHCP Packets using Wireshark

Mohsin khan
Faculty of Telecommunication Engineering and Environment
Birmingham City University
England

Saleh Alshomrani
Faculty of Computing and IT
King Abdulaziz University
Jeddah, Saudi Arabia

Shahzad Qamar
Faculty of Computing and IT
King Abdulaziz University
Jeddah, Saudi Arabia

ABSTRACT

On a network, when data is transferred between the hosts, it is passed through several stages. Data is actually passed through a very complex process at the sender and receiver than it apparently looks to be. During transmission data is broken down into smaller chunks of data so that they can be carried on the wire. These chunks are given appropriate headers, encapsulated and then passed through several layers to reach the destination. In this research we capture DHCP packets by using wireshark to deeply investigate and analyse them. We investigate how DHCP Client/Server request and reply messages work and what values and parameters are considered during this whole process.

Keywords: DHCP, DHCPDISCOVER, DHCPREQUEST, DHCPOFFER, DHCPACK

1. INTRODUCTION

DHCP is one of the most widespread used protocols in the world which is used in both wired and wireless LANs to assign IP addresses to the clients automatically. It relieves network Administrator from going to each and every workstation in the LAN to assign IP address. Also it reduces IP addresses conflict issue [1]. DHCP provides a client/Server structure in which 4 DHCP packets are exchanged between client and server to assign an IP address automatically. The purpose of this work is to investigate and examine these 4 packets in detail and to observe what information is carried in these packets, which are exchanged between DHCP server and client before assigning a lease. To investigate DHCP packets, we use wireshark, which is a widely used computer network analyser tool [2]. We will capture all DHCP packets with wireshark and deeply look into the contents of each packet.

2. DHCP CLIENT SERVER MODEL

DHCP is a very useful and famous protocol which is used to automatically assign IP addresses to the clients on the network. DHCP provides a client-server Structure, in which DHCP server automatically assigns IP addresses to clients. DHCP works somewhat opposite of ARP because ARP resolves MAC address from IP address whereas DHCP resolves IP address from MAC address [1].

There are two databases in DHCP Server, Static database and dynamic database. Static database statically maps IP address with the MAC address. Dynamic database dynamically maps IP address to the MAC address by providing available IP address in the DHCP pool [1].When a client requests for an IP address, DHCP server first looks into its static database and checks whether requesting client's MAC address is bound statically to an IP address. If an entry exists for that MAC address of the client, the permanent IP address of the client is returned. If no entry is found in static database for that MAC address, an IP address from the DHCP pool is assigned and an entry is made in dynamic database [1] [4].

DHCP can cause lots of problems as well. Like, DHCP clients can potentially lose network connectivity [10] if DHCP server goes down for some reasons. The clients which have already been assigned IP addresses by server also need to renew their lease, so with down server, they also lose connectivity. In large networks we usually place more than one DHCP server to avoid single point of failure architecture, so we need extra money and time to install separate DHCP servers for each network segment [10].

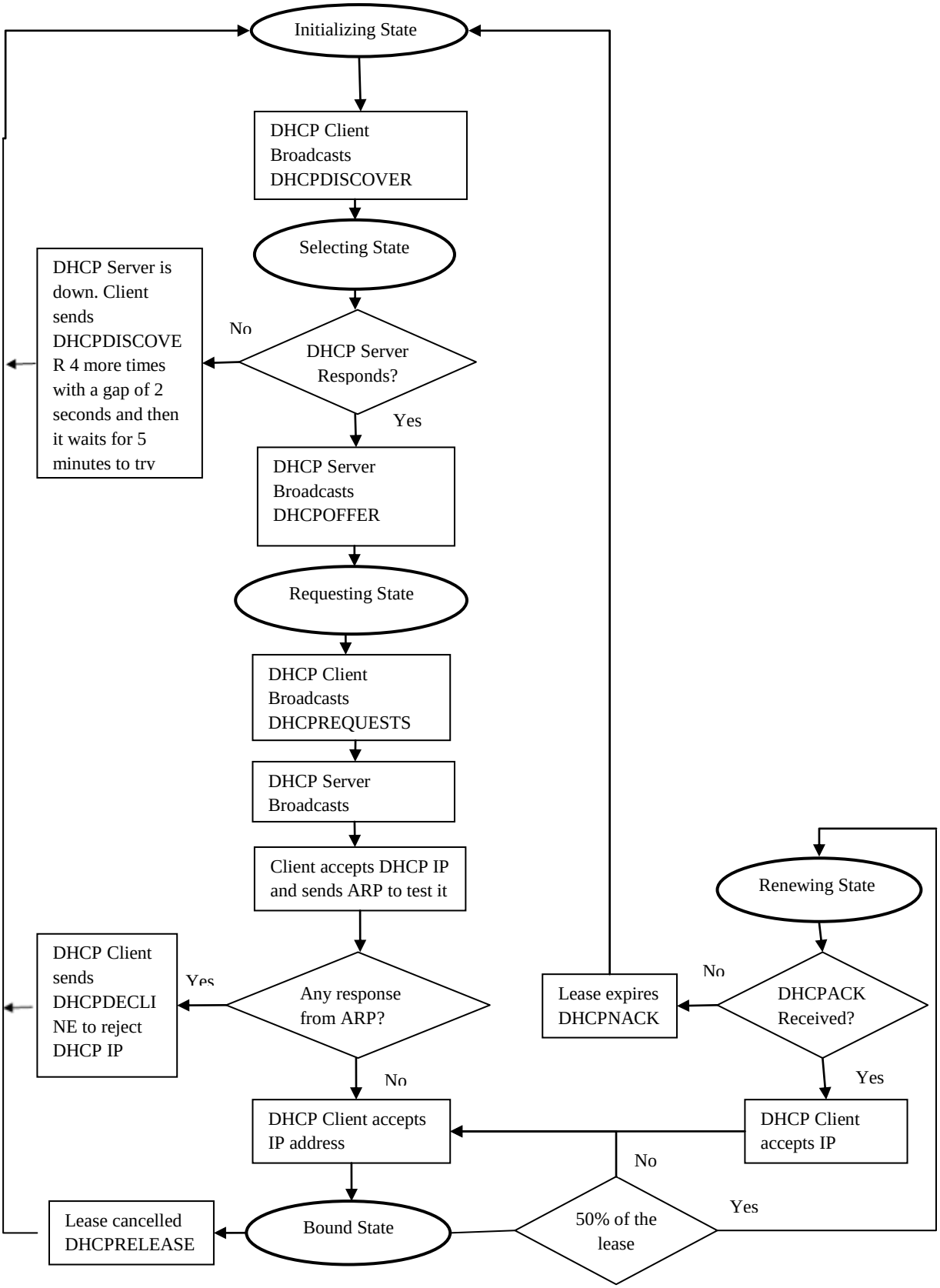

Figure 1: Flowchart of DHCP Client-Server model

3. DHCP SERVICE CONFIGURATION

DHCP service can be installed on the server in the LAN running server operating system like Microsoft Windows 2008 or 2003. We can also configure DHCP service on the router to act as a DHCP server for the clients in the local

LAN. To configure DHCP service on router following configuration needs to be entered on the router.

```
Router(config)# ip dhcp excluded-address 192.168.2.1
192.168.2.9
Router(config)# ip dhcp pool dhcp-pool
Router(dhcp-config)# network 192.168.2.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.2.1
```

A DHCP pool namely dhcp-pool is created on the router which will assign IP addresses to the clients from subnet 192.168.2.0/24. It is illustrated in the figure below.

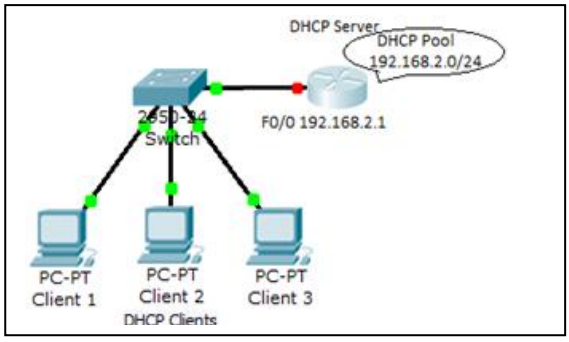

Figure 1(a): Router acting as DHCP Server to local LAN

To better understand DHCP client-server conversation, we use following simple network with the server using Microsoft Windows Server 2003 and client using Microsoft windows XP.

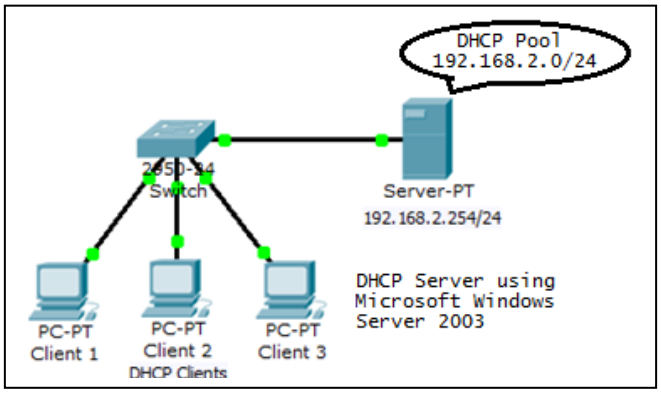

Figure 1(b): Local Server serving as DHCP Server

To capture DHCP packets exchanged between DHCP client and Server we need these commands to be entered in cmd prompt of the client [3].

3.1 Ipconfig /Release

This command releases the IP address held by the host PC. The released IP address becomes available to be assigned to other clients in the LAN.

3.2 Ipconfig /Renew

This command enables the host PC to gain a newer IP address from the pool of the addresses.

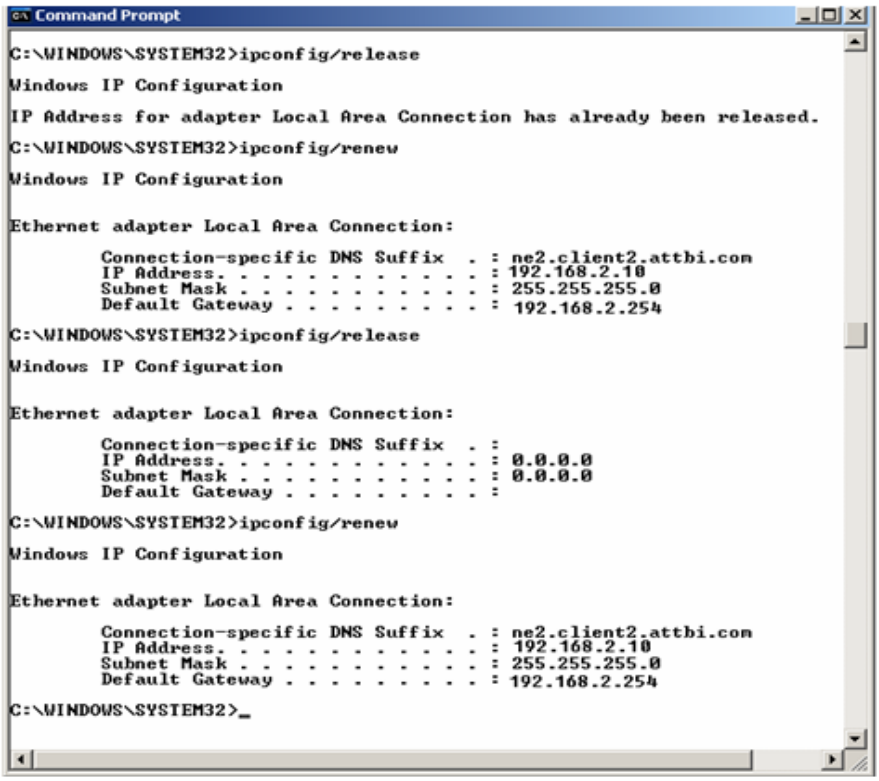

Figure 2: releasing and renewing IP address with ipconfig/release and renew commands

Security wise DHCP can pose some serious threats to the network in form of DHCP spoofing. It is an attacker who with malicious intents comes in the middle of communication between two systems, the attacker either listen to the communication or actively participate in it. DHCP Spoofing is a man in the middle type of attack. The attacker comes in between the communication meant for someone else, the attacker replies to the DHCP request message and assigns IP address if it replies before the actual valid server. To remedy this problem we use DHCP Snooping. DHCP snooping allows only those ports on switch to respond DHCP Requests which are configured for it. DHCP categorizes ports into trusted and untrusted ports [11]. Trusted ports can host all DHCP messages, while untrusted ports can source requests only [11], they can't source server messages.

```
Router (config)# ip dhcp snooping
Router(config)#interface range fastethernet 0/1-2
Router(config-if)#ip dhcp snooping trust
Router(config-if)#exit
Router(config)#ip dhcp snooping vlan 10,20,30
```

4. DHCP PACKETS

The conversation between DHCP client and DHCP server to get an IP address automatically completes by exchanging four packets. These packets are

- DHCP DISCOVER
- DHCP OFFER
- DHCP REQUEST
- DHCP ACK

When a DHCP client needs an IP addressed, it broadcasts DHCPDISCOVER Packet. All the hosts on the subnet receive this broadcast. All DHCP servers in the LAN also receive this broadcast and they determine that whether they can assign IP address to the client or not? Then servers reply with DHCPOFFER packets to the client to offer an IP address with the lease duration. If DHCP client receives more than one offer from DHCP servers, it has to decide which offer to accept and which to turn down. It may either accept the offer from DHCP servers based on reply first basis or it may look into the options like the lease duration, subnet mask etc. [4]. receiving the offer, Client sends a DHCPREQUEST packet to the server after accepting the offer and finally DHCP server reply with DHCPACK packet to the client to create binding between client's MAC address and IP address. DHCP server assigns IP address to the client from the given pool of addresses for a given period of time (lease). After the expiration of the lease period the IP address is taken away from the client and it becomes available to be assigned to any other client in the LAN. But lease can be renewed before it gets expired. DHCP client tries to renew the lease after 50 percent expiration of the whole lease period [1].

4.1 DHCPDISCOVER

DHCPDISCOVER packet is broadcasted in the LAN in hope of getting DHCPOFFER message from any DHCP server present in that LAN. If client doesn't receive any offer, it will broadcast DHCP DISCOVER 4 more times, each time with a gap of 2 seconds. If client doesn't receive any offer all these four times, it sleeps for five minutes and after these five minutes it starts afresh to broadcast DHCPDISCOVER [1]. DHCPDISCOVER packet captured through wireshark is investigated below.

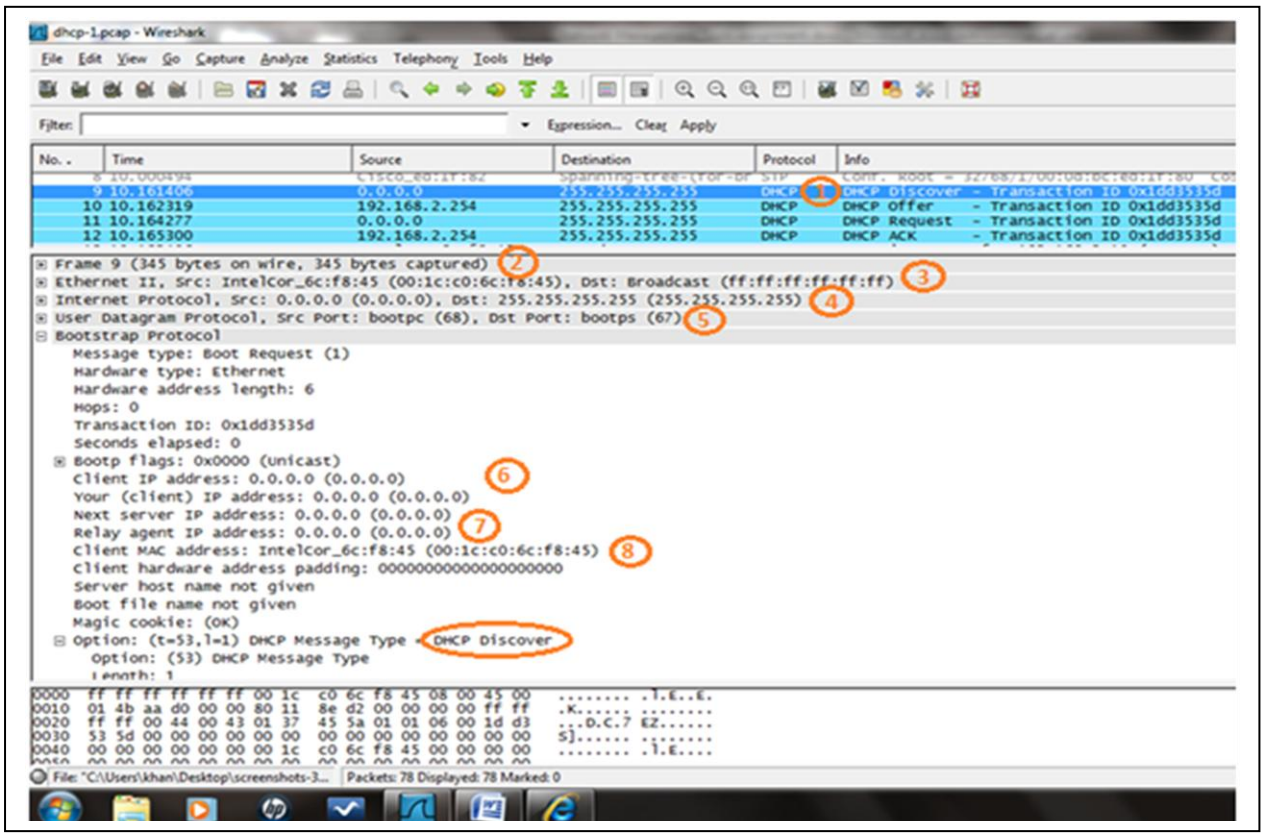

Figure 4: DHCPOFFER packet analysis with wireshark

1) Transaction ID value is again 0x1dd3535d because it identify DHCP set of packets from each other [5].
2) Source IP address 192.168.2.254 destination address 255.255.255.255, which means that DHCPOFFER packet is sourced by DHCP Server and broadcasted in the LAN. So all the hosts in the LAN will hear this broadcast and MAC address of the intendant client plays a very important role in assigning IP address here.
3) Since DHCPOFFER is sourced by DHCP server for in response to client's DHCPDISCOVER, UDP source port is 67 and destination port is 68.
4) Offered IP address by DHCP server to client is 192.168.2.10. The server blocks this address (192.168.2.10) so that it is unavailable to be offered to other client [1].
5) Next server IP address is 192.168.2.254 which is the IP address of the DHCP server.
6) Client's MAC address mentioned in DHCPOFFER packet is intelcor_6c:f8:45. This is very important to mention because DHCPOFFER packet is broadcasted in the LAN, so all the hosts in the LAN receives the offer packet. But since MAC address is a universally unique number, this offer will be meaningful only to the host with the given MAC address (which is intelcor_6c:f8:45 in our case).
7) Identifies that the captured packet is actually a DHCPOFFER packet.
8) It is the IP address of the DHCP server which offers the lease.
9) The Offered IP address is offered on lease for 5 hours. After expiration of 5 hours IP address will be taken away from the client is the lease is not renewed. Default duration of the lease is 1 hour. DHCP server will block the IP address (192.168.2.10) so it will not be available for other clients to be assigned.
10) Renewal time value of the lease is 2 hours and 30 minutes. It is half of the whole lease time period. It means that after 2 hours and 30 minutes DHCP client will try to renew the lease so the lease doesn't expire [1].
11) Rebinding time value is 4 hours, 22 minutes and 30 seconds.
12) Subnet mask is 255.255.255.0. So 254 valid IP address are available in the DHCP pool to assign dynamically to the clients.

4.2 DHCPREQUEST

Upon the receipt of DHCPOFFER, DHCP Client accepts 192.168.2.10 as its IP address and replies to server with DHCPREQUEST message. This packet tells the DHCP server that his offer of the IP address has been accepted. Following screenshot explains the contents of DHCPREQUEST packet.

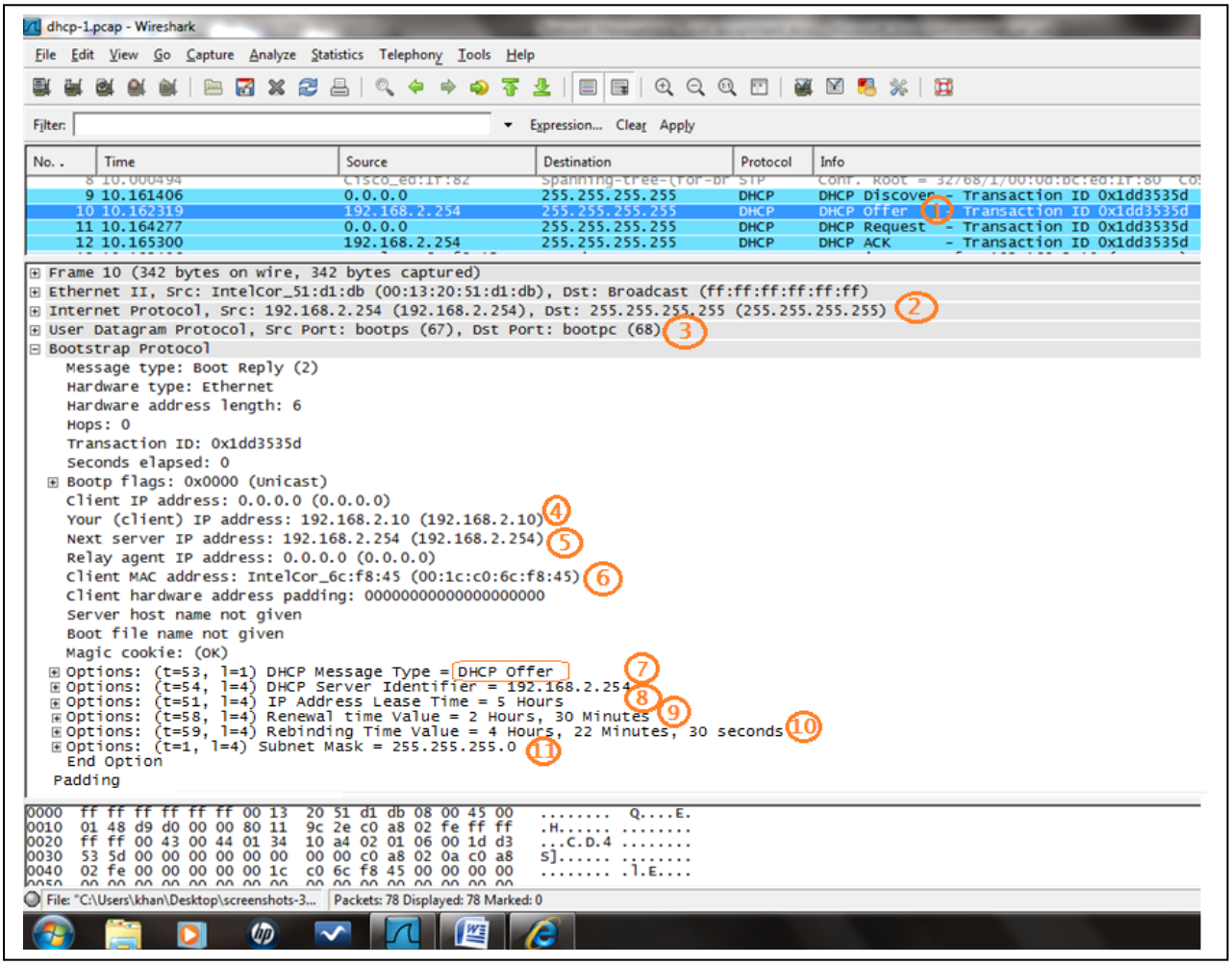

Figure 4: DHCPOFFER packet analysis with wireshark

13) Transaction ID value is again 0x1dd3535d because it identify DHCP set of packets from each other [5].
14) Source IP address 192.168.2.254 destination address 255.255.255.255, which means that DHCPOFFER packet is sourced by DHCP Server and broadcasted in the LAN. So all the hosts in the LAN will hear this broadcast and MAC address of the intendant client plays a very important role in assigning IP address here.
15) Since DHCPOFFER is sourced by DHCP server for in response to client's DHCPDISCOVER, UDP source port is 67 and destination port is 68.
16) Offered IP address by DHCP server to client is 192.168.2.10. The server blocks this address (192.168.2.10) so that it is unavailable to be offered to other client [1].
17) Next server IP address is 192.168.2.254 which is the IP address of the DHCP server.
18) Client's MAC address mentioned in DHCPOFFER packet is intelcor_6c:f8:45. This is very important to mention because DHCPOFFER packet is broadcasted in the LAN, so all the hosts in the LAN receives the offer packet. But since MAC address is a universally unique number, this offer will be meaningful only to the host with the given MAC address (which is intelcor_6c:f8:45 in our case).
19) Identifies that the captured packet is actually a DHCPOFFER packet.
20) It is the IP address of the DHCP server which offers the lease.
21) The Offered IP address is offered on lease for 5 hours. After expiration of 5 hours IP address will be taken away from the client is the lease is not renewed. Default duration of the lease is 1 hour. DHCP server will block the IP address (192.168.2.10) so it will not be available for other clients to be assigned.
22) Renewal time value of the lease is 2 hours and 30 minutes. It is half of the whole lease time period. It means that after 2 hours and 30 minutes DHCP client will try to renew the lease so the lease doesn't expire [1].
23) Rebinding time value is 4 hours, 22 minutes and 30 seconds.
24) Subnet mask is 255.255.255.0. So 254 valid IP address are available in the DHCP pool to assign dynamically to the clients.

4.3 DHCPREQUEST

Upon the receipt of DHCPOFFER, DHCP Client accepts 192.168.2.10 as its IP address and replies to server with DHCPREQUEST message. This packet tells the DHCP server that his offer of the IP address has been accepted. Following screenshot explains the contents of DHCPREQUEST packet.

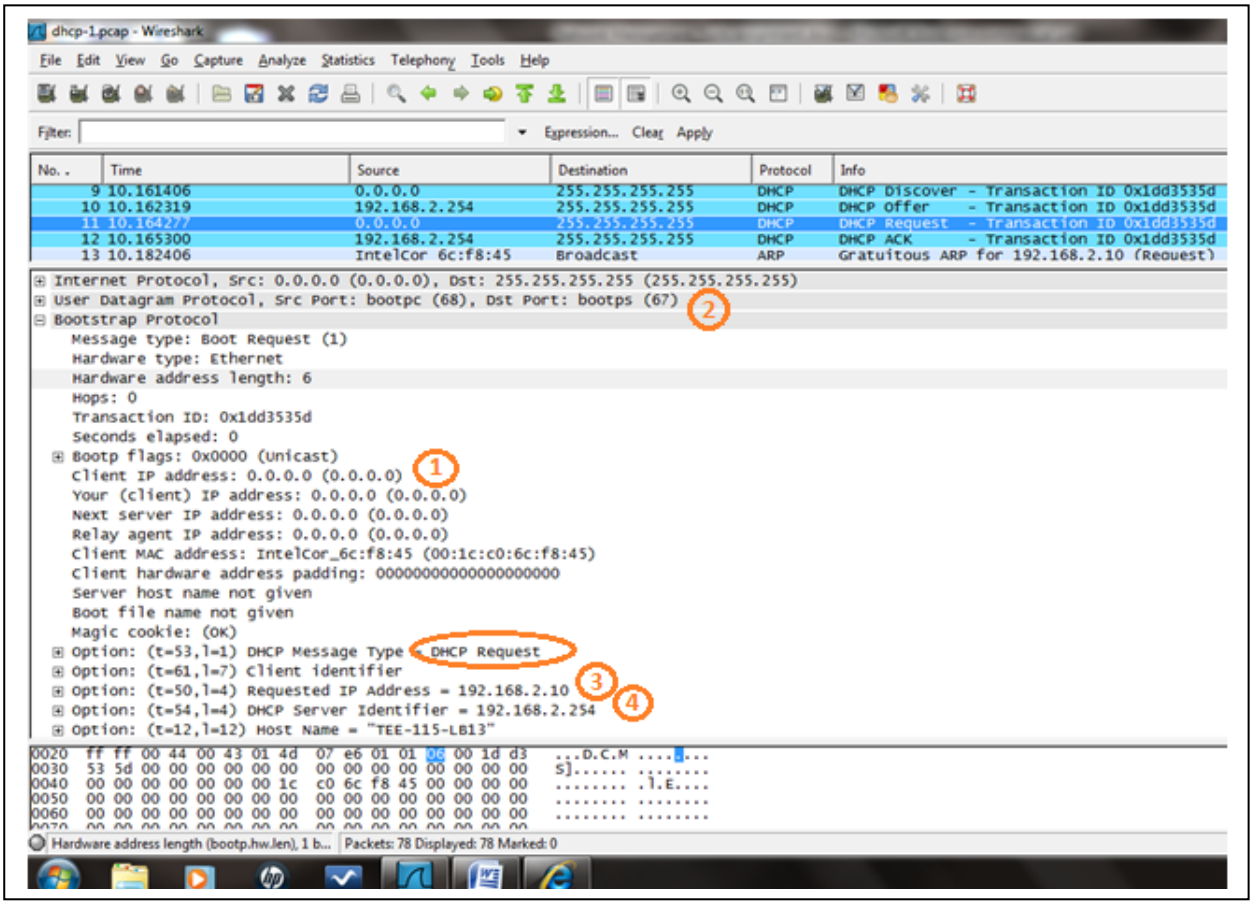

Figure 5: DHCPREQUEST packet analysis with wireshark

1) Source address is 0.0.0.0. It states that still IP is not assigned to client. Destination IP address is 255.255.255.255 which indicates that DHCPREQUEST is also broadcasted. So other DHCP servers in the LAN will also receive this DHCPREQUEST message and looking at the transaction ID field of the request message they withdraw to offer any lease to the client. Because transaction ID field for them is different from this value [5].
2) Source Port number of DHCP Request packet is 68 and destination Port number is 67.
3) Requested IP address is 192.168.2.10 which was offered in DHCP Offer packet by server.
4) DHCP server IP address is 192.168.2.254. Since DHCP Request packet is broadcasted, all other servers in the LAN (if any) comes to know that server with IP address 192.168.2.254 is selected as DHCP server [3]. The servers not chosen in this request message will consider themselves rejected in the process and they will keep the offered IP addresses available for any other request message [3].

4.4 DHCPACK AND DHCPNACK

When server receives DHCPREQUEST message requesting for the offered IP address, it looks into the DHCP pool to confirm that the offered IP address is still available. If the IP address is assigned to some other client, DHCP server replies with a DHCPNACK (negative acknowledgment) packet to the requesting client. If IP address is still available in the pool, server replies with DHCPACK packet to the client to confirm the lease length and other parameters [3]. In our lab IP address is successfully assigned and the following screenshot shows the captured DHCPACK packet.

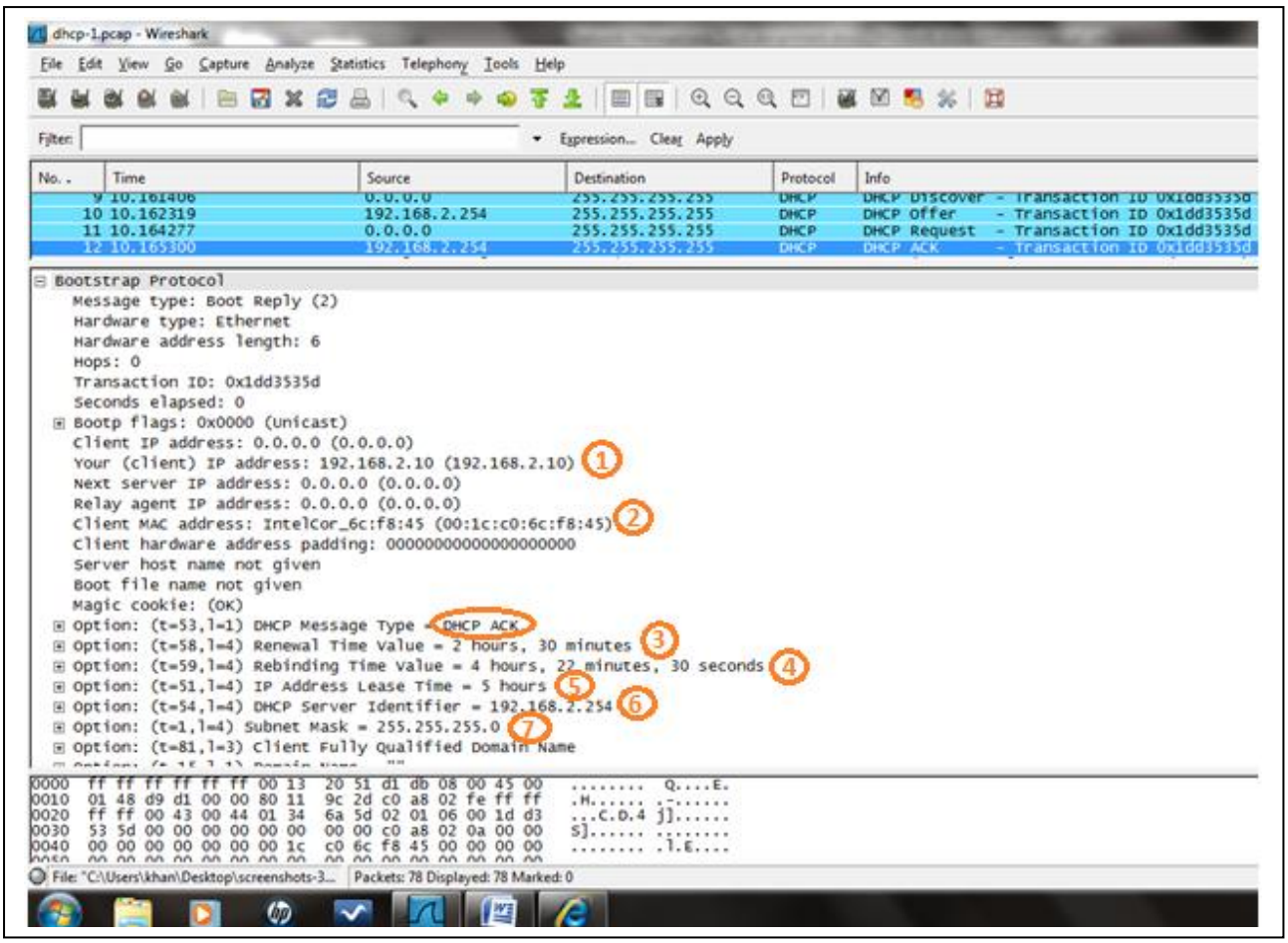

Figure 7: DHCPACK packet capture and analysis with wireshark

1) Assigned IP address to the client 192.168.2.10
2) MAC address of the client is intelcor_6c:f8:45
3) Renewal time value is 2 hours and 22 minutes and 30 seconds, after expiration of this period of time lease will be renewed.
4) IP address lease time is 5 hours. IP address is assigned for 5 hours only, after expiring 5 hours, if lease is not renewed, IP address (192.168.2.10) will be taken away from the client and it will become available in the DHCP pool to be assigned to other clients.
5) IP address of the DHCP server is 192.168.2.254
6) Subnet mask of the IP address is 255.255.255.0. so there can be 254 available IP address in the DHCP pool

When the client receives the acknowledgment for the requested IP address, it sends a gratuitous ARP to confirm that no other client in the LAN is using that IP address. If an ARP reply is received than the client realizes that some other client is already using that IP address, if no ARP reply is receive the client start using it as his IP address. Not all clients use ARP to confirm that the IP address is free to be used some just directly start using it without verification [4].

5. CONCLUSION

In this research work, we have deeply studied and investigated that what does exactly happens in the back screen when an IP address is assigned to client by using DHCP. Firstly, we introduced client-server model of DHCP and then by using computer network analyzer tool i.e. wirshark, we have captured DHCP packets that are exchanged in the process between DHCP client and server and deeply observed and analyzed their contents to make the whole communication process easy to understand for the readers.

6. ACKNOWLEDGMENT

First of all we are grateful to all mighty ALLAH, who enabled us to finish this assignment successfully. We would also like to deliver our whole hearted thanks to department of Telecommunication and Engineering of Birmingham City University for its cooperation and support.

7. REFERENCES

[1] B.A Forouzan, 2003. Data Communication and Networking. 3rd ed, pp. 492-494. McGraw-Hill

[2] Wireshark. 2012. About Wireshark [online]. Available: http://www.wireshark.org/about.html [accessed: 22 July 2012]

[3] J.F Kurose K.W Ross, 2007. Computer Networking: A Topdown Approach 4th edition, [online] http://www.eng.tau.ac.il/~netlab/resources/booklet/Wireshark_DHCP.pdf [Accessed: 25 Aug 2012]

[4] E Kollman, Aka Xnhi, 2007. Chatter on the Wire: A look at DHCP Traffic. [online]. Available:

http://myweb.cableone.net/xnih/download/chatter-dhcp.pdf [Accessed: 27 July 2012]

[5] Beccary, DHCP.[online]. Available: http://blog.it.kmitl.ac.th/it51066440/?page_id=38 [Accessed: 10th august 2012]

[6] Microsoft, Bootp and DHCP [online]. Available: http://technet.microsoft.com/en-us/library/cc781243(v=ws.10).aspx [Accessed: 12 August 2012]

[7] Charles M. Kozierok, 2005. TCP/IP guide, DHCP Lease Allocation Process [online]. Available: http://www.tcpipguide.com/free/t_DHCPLeaseAllocationProcess-2.htm [Accessed: 14 August 2012]

[8] Microsoft Technet, 2012. DHCP Packets [online]. http://technet.microsoft.com/en-us/library/cc749902.aspx [Date accessed: 21 August 2012]

[9] L J Knapp, T M Hadley, 2011. Dynamic Host Configuration Protocol

[10] Shea Laverty,2012,The Disadvantages of DHCP [online] http://www.ehow.com/info_8760244_disadvantages-dhcp.html [Date Accessed: 10 Dec 2012]

[11] Cisco,2007, DHCP Snooping [Online] , http://www.cisco.com/en/US/products/hw/switches/ps5023/products_configuration_example09186a00807c4101.shtml#dhcpsnoop [Date Accessed: 26 Dec. 12]