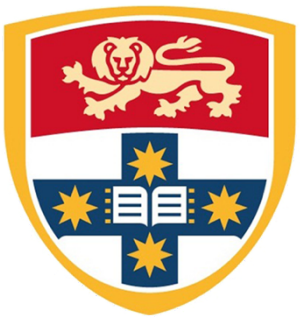
University of Sydney

# ELEC3506 Data Communications and Internet – Lab Report 2

**Mengzhen Chen 480462613**
**Gaurav Agarwal 470404557**



THE UNIVERSITY OF SYDNEY

## Table of Contents

*Introduction* 1

*Phase I: Dynamic Host Configuration Protocol (DHCP)* 1

*Phase II:Domain Name System (DNS)* 2

# 1 Introduction

In the first phase, we will learn how dynamic host configuration protocol (DHCP) assigns IP addresses to hosts and perform several DHCP-related commands and capture the DHCP messages exchanged as a result of executing these commands. In the second phase, we get familiar with the domain name system (DNS), which fulfills a critical role in the Internet infrastructure by translating hostnames to IP addresses.

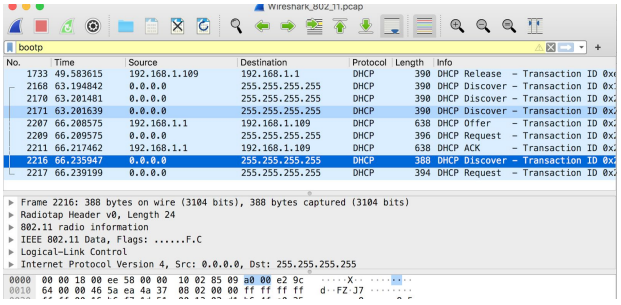
## 2 Phase I:Dynamic Host Configuration Protocol (DHCP)

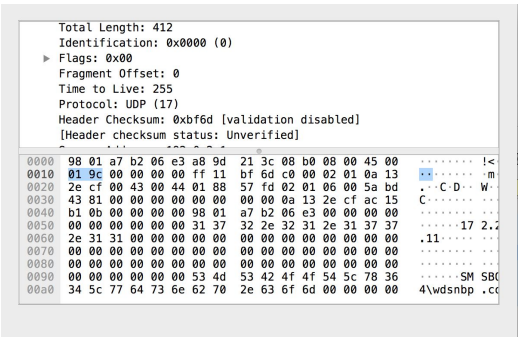
In order to observe DHCP in action, we perform several DHCP-related commands and capture the DHCP messages exchanged as a result of executing these commands. In this experiment, we need two commands:

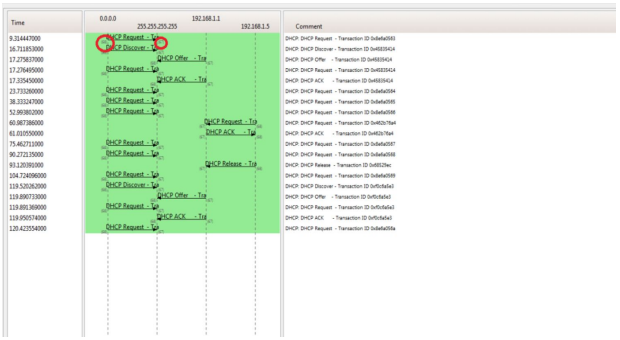
• *Ipconfig /release* (*ifconfig ethX down*, in case of linux): This command releases your current IP address, so that your host's IP address becomes 0.0.0.0.

• *Ipconfig /renew* (*ifconfig ethX up*, in case of linux): This command instructs your host to obtain a network configuration, including a new IP address.

After running the commands on terminal a set of Discover/Offer/Request and ACK messages were transmitted:

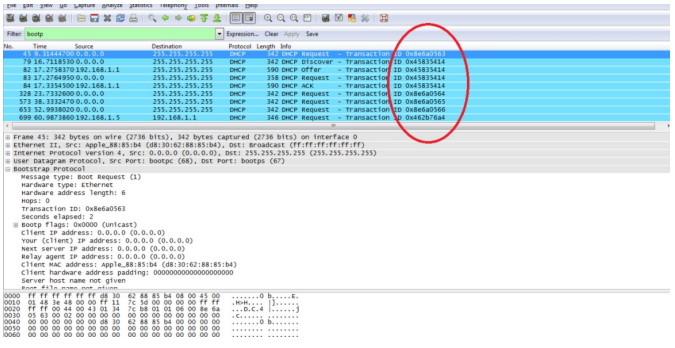


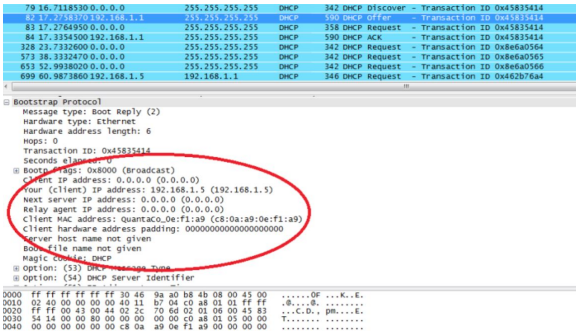
DHCP uses User Datagram Protocol (UDP), RFC 768, as its transport protocol. DHCP messages that a client sends to a server are sent to well-known port 67 (UDP—Bootstrap Protocol and DHCP). DHCP Messages that a server sends to a client are sent to port 68.
Using the Statistics tool, we can plot the timing diagram for the series of DHCP messages.

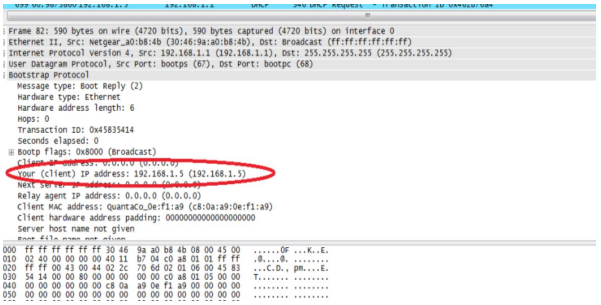
The source and destination port addresses alternate between 68 and 67, respectively. This reflects that the messages are being sent over UDP transport protocol and not TCP protocol. The messages are distinguished by the message type value. For example the message type of for discovery os 1 and for request is 3. This differentials the two messages from each other. To further differentiate sets of Discover/Offer/Request/ACK messages from each other, we can look at the transaction ID. The transaction ID will be different for each set of Discover/Offer/Request/ACK messages. This can be seen in the figure below



Since the messages are sent to the network the computer is connected to the destination address for each of the Discover/Offer/Request/ACK messages is 255.255.255.255. Initially, the source address is 0.0.0.0 for the request and discover messages. This is because there is no relay agent causing the source to be 0.0.0.0. The destination address however is still 255.255.255.255. Once the offer is made the source address becomes 192.168.1.5. This is also the IP address that is eventually accepted by the host. As can be seen below the offered address is the same as the

requested IP address.

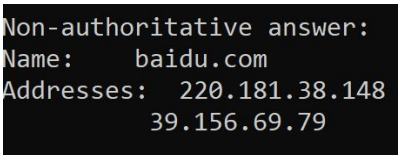


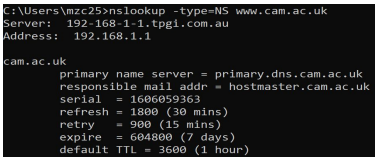


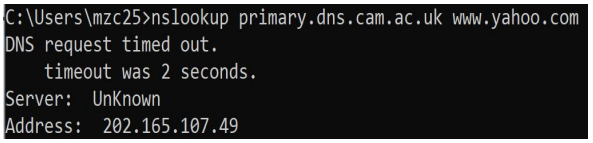
The DHCP release message tells the dhcp server that you want to cancel the ip address offered. The DHCP server will not issue an ack of receipt of the client's DHCP request. If the release message is lost then the dhcp server retains the ip address until the lease time expires.

# Phase II: Domain Name System (DNS)

NsLookup queries the specified DNS server and retrieves the requested records that are associated with the domain name you provided. These records contain information like the domain name's IP addresses.





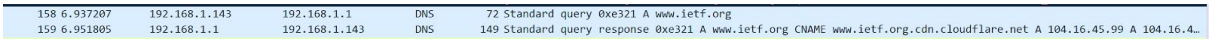


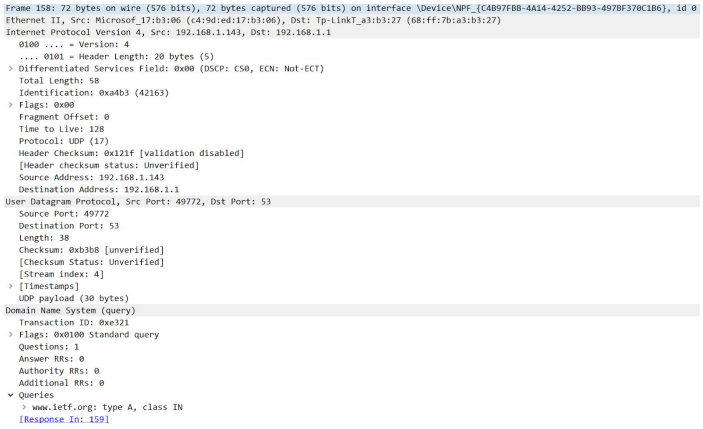
Now, we are going to test nslookup by running it with a website url. Firstly We chose baidu.com as the testing asian web server (the first picture on the left), it tends out the ip address is 220.181.38.148.

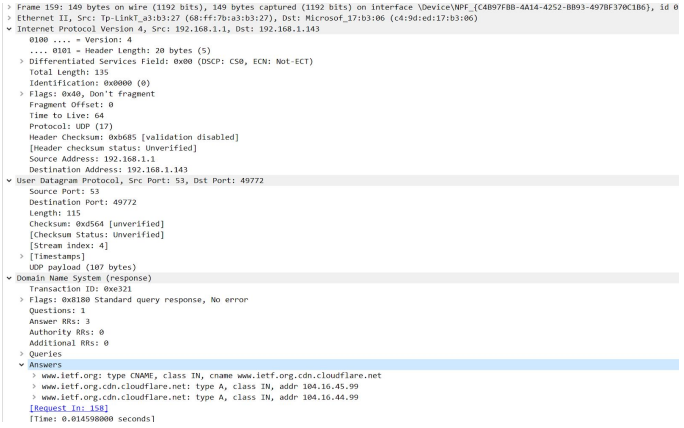
In the second test we are finding the uni of Cambridge(the middle picture). Notice that we are using -type=NS, NS stands for there is one or more authoritative name server records for the domain. the iP address of the server is primary.dns.cam.ac.uk.

Now we use this DNS server to access Yahoo mail(since i do not have yahoo mail, so I am going to access www.yahoo.com instead, the rightmost picture). The ip address will be 202.165.107.49.

Now we using ipconfig /flushdns to clear the cache



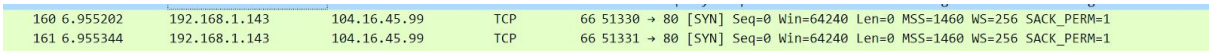




As we can see, the DNS query(left picture) and response(right picture) messages sent over UDP and using

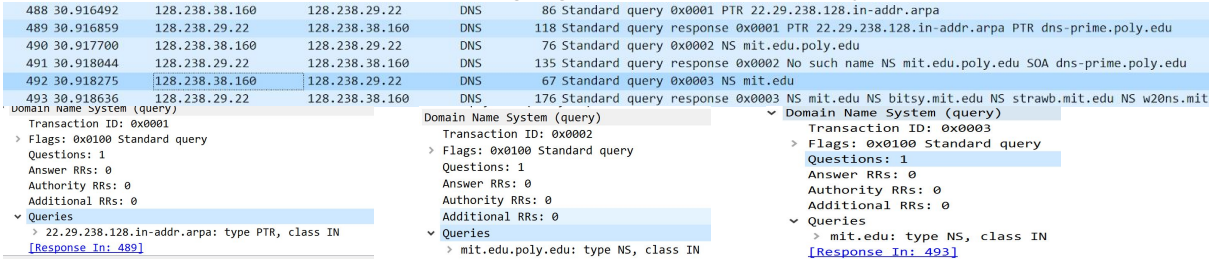
destination port 53, that makes sense since a DNS server uses well-known port 53 for all its UDP activities and as its server port for TCP.

The ip address of the DNS query message is sent to my local DNS servers, since it is a standard query (0x0100), it does not contain any answer. Now let us take a closer look at the response message,, there are three answers provided. Two of them are type A, i.e. Address record. One is type CNAME, which stands for alias of one name to another: the DNS lookup will continue by retrying the lookup with the new name. Both of them contain type, class (class in stands for internet), ttl, and data length. For the CNAME answer, the last field is CNAME www.ietf.org.cdn.cloudflare.net, that makes sense since it is its canonical Name. For the A type answer, the last field is ip address.



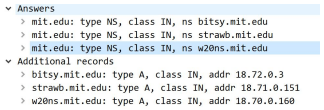

As we can see the destination ip address for SYN packet corresponds to the ip address which was provided by the answer. The host does not issue new DNS queries before it retrieved each image,

Now we do an nslookup on www.mit.edu. (I am going to use zip file from here,my wireshark snapped)

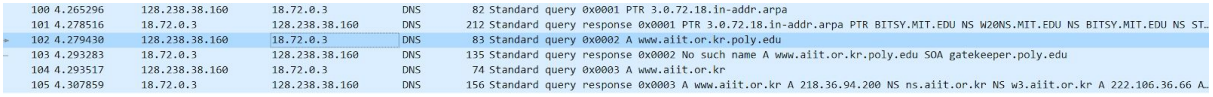



There are three queries. The destination ports of them are the same. It is still 53. The source port are 3744,3745 and 3746. The DNS query message was sent to 128.238.29.22 it is my local DNS server (it is supposed to). The first one is type PNR, in this case it resolves an IP address to a domain or hostname not another way around. The second and third one is type NS, the NS stands for 'nameserver,' and the nameserver record indicates which DNS server is authoritative for that domain (i.e. which server contains the actual DNS records). Both of the queries types do not contain any answers.

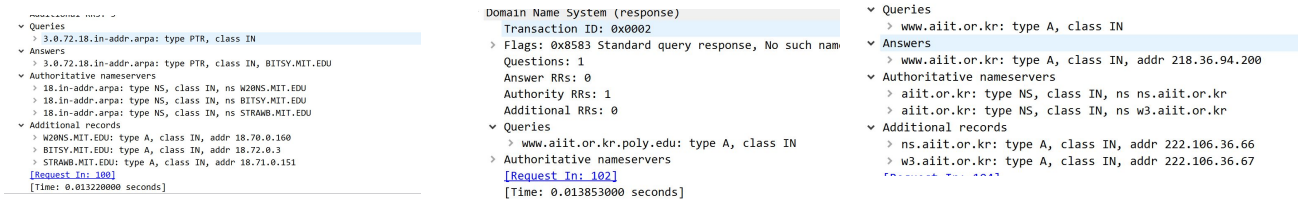
Now we examine three responses.It provide bitsy.mit.edu,strawb.mit.edu and w20ns mit.edu. As we can see on the graph, this packet also provides addresses for these nameservers.




Now we repeat the experiment with nslookup www.aiit.or.kr bitsy.mit.edu




As the previous part, the destination ip address for queries 128.238.29.22 are the same as my local DNS server ip. The first one is PTR and the second and third one are type A. They are the same as before , each query contains 1 question and 0 answers.




These response packets (from left to right) follow the order of the wireshark testing result(from top to down).it tends out there is one answer found, the address is 218.36.94.200. The detail of answer is shown in below figure.