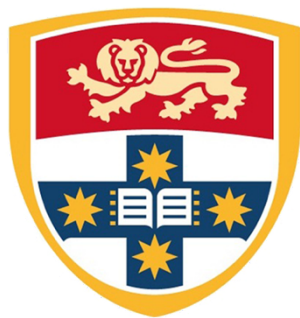


University of Sydney

ELEC3506 Data Communications and Internet – Lab Report 2

Mengzhen Chen 480462613
Gaurav Agarwal 470404557



THE UNIVERSITY OF
SYDNEY

Table of Contents

<i>Introduction</i>	<i>1</i>
<i>Phase I: Dynamic Host Configuration Protocol (DHCP)</i>	<i>1</i>
<i>Phase II: Domain Name System (DNS)</i>	<i>2</i>

1 Introduction

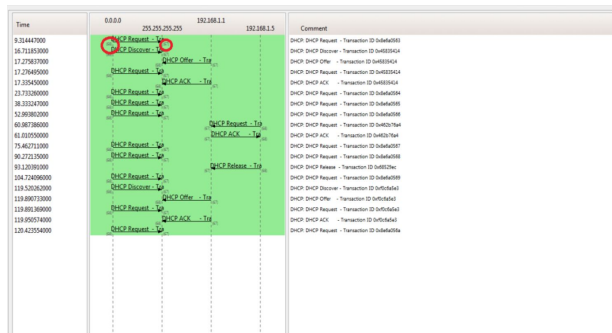
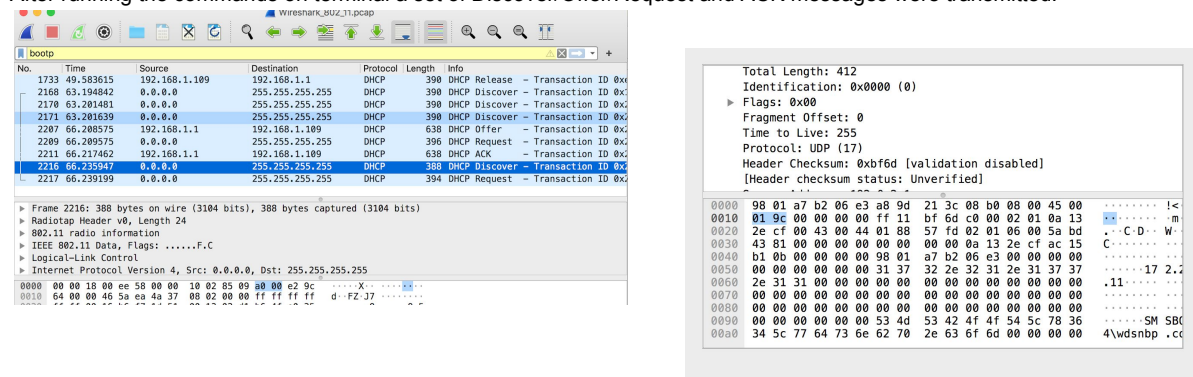
In the first phase, we will learn how dynamic host configuration protocol (DHCP) assigns IP addresses to hosts and perform several DHCP-related commands and capture the DHCP messages exchanged as a result of executing these commands. In the second phase, we get familiar with the domain name system (DNS),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



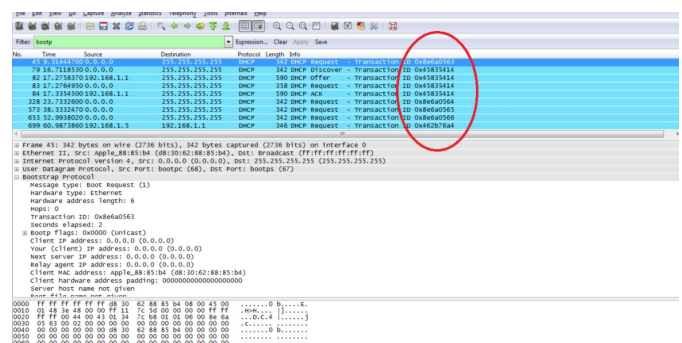
DHCP uses User Datagram Protocol (UDP), RFC 768, as its transport protocol. DHCP messages that a client sends to a server are sent to well-known port 67 (UDP—Bootstrap Protocol and DHCP). DHCP Messages that a server sends to a client are sent to port 68.

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



requested IP address.

```
79 16.7118530 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x45835414
81 17.2749490 0.0.0.0 255.255.255.255 DHCP 358 DHCP Request - Transaction ID 0x45835414
84 17.3354500 192.168.1.1 255.255.255.255 DHCP 590 DHCP ACK - Transaction ID 0x45835414
328 23.7132600 0.0.0.0 255.255.255.255 DHCP 342 DHCP Request - Transaction ID 0x46a05664
372 38.3312470 0.0.0.0 255.255.255.255 DHCP 342 DHCP Request - Transaction ID 0x46a05664
651 52.9918020 0.0.0.0 255.255.255.255 DHCP 342 DHCP Request - Transaction ID 0x46a05664
699 60.9873860 192.168.1.5 192.168.1.1 DHCP 346 DHCP Request - Transaction ID 0x462076d4

Bootstrap Protocol
Message type: Boot Reply (2)
Hardware type: ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x45835414
Seconds elapsed: 0
Boot flags: 0x0000 (broadcast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 192.168.1.5 (192.168.1.5)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Quantaco.De:fi:a9 (c8:0a:a9:0e:fi:a9)
Client hardware address padding: 00000000000000000000
Server host name not given
Server file name not given
Magic cookie: DHCP
Option (53) DHCP Message Type
Option (54) DHCP Server Identifier
0000 ff ff ff ff ff 30 46 9a a0 b8 4b 08 00 45 00 .....0f...K..E.
0010 02 40 00 00 00 00 40 11 b7 04 c0 a8 01 01 ff ff ..0...8.....
0020 ff ff 00 41 00 44 02 3c 70 60 02 01 06 00 45 83 ...C..0...E...
0030 54 14 00 00 80 00 00 00 00 00 c0 a8 01 05 00 00 T.....
0040 00 00 00 00 00 00 c8 0a a9 0e fi a9 00 00 00 00 .....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

```
Frame 82: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface 0
(Ethernet II, Src: Netgear_a0:b8:4b (30:45:9a:a0:b8:4b), Dst: broadcast (ff:ff:ff:ff:ff:ff))
Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol
Message type: Boot Reply (2)
Hardware type: ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x45835414
Seconds elapsed: 0
Boot flags: 0x0000 (broadcast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 192.168.1.5 (192.168.1.5)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Quantaco.De:fi:a9 (c8:0a:a9:0e:fi:a9)
Client hardware address padding: 00000000000000000000
Server host name not given
Server file name not given
000 ff ff ff ff ff 30 46 9a a0 b8 4b 08 00 45 00 .....0f...K..E.
0010 02 40 00 00 00 00 40 11 b7 04 c0 a8 01 01 ff ff ..0...8.....
0020 ff ff 00 41 00 44 02 3c 70 60 02 01 06 00 45 83 ...C..0...E...
0030 54 14 00 00 80 00 00 00 00 00 c0 a8 01 05 00 00 T.....
0040 00 00 00 00 00 00 c8 0a a9 0e fi a9 00 00 00 00 .....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

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.

```
Non-authoritative answer:
Name:      baidu.com
Addresses: 220.181.38.148
           39.156.69.79
```

```
C:\Users\mzc25>nslookup -type=NS www.cam.ac.uk
Server: 192.168-1-1.tpgi.com.au
Address: 192.168.1.1

cam.ac.uk
primary name server = primary.dns.cam.ac.uk
responsible mail addr = hostmaster.cam.ac.uk
serial = 1606059363
refresh = 1800 (30 mins)
retry = 900 (15 mins)
expire = 604800 (7 days)
default TTL = 3600 (1 hour)
```

```
C:\Users\mzc25>nslookup primary.dns.cam.ac.uk www.yahoo.com
DNS request timed out.
timeout was 2 seconds.
Server: UnKnown
Address: 202.165.107.49
```

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

158 6.937207	192.168.1.143	192.168.1.1	DNS	72 Standard query 0xe321 A www.ietf.org
159 6.951805	192.168.1.1	192.168.1.143	DNS	149 Standard query response 0xe321 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.4...

```
Frame 158: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF...
Internet Protocol Version 4, Src: 192.168.1.143, Dst: 192.168.1.1
0100 .... = Version: 4
... 0101 = Header Length: 20 bytes (5)
... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 58
Identification: 0xa4b3 (42163)
Flags: 0x00
Fragment Offset: 0
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0x121f [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.143
Destination Address: 192.168.1.1
User Datagram Protocol, Src Port: 49772, Dst Port: 53
Source Port: 49772
Destination Port: 53
Length: 38
Checksum: 0xb3b8 [unverified]
[Checksum Status: Unverified]
[Stream Index: 4]
[Timestamps]
UDP payload (38 bytes)
Domain Name System (query)
Transaction ID: 0xe321
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.ietf.org: type A, class IN
[Response In: 159]
```

```
Frame 159: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF...
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.143
0100 .... = Version: 4
... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 135
Identification: 0xa4b3 (42163)
Flags: 0x00, Don't fragment
Fragment Offset: 0
Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0xb685 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.1
Destination Address: 192.168.1.143
User Datagram Protocol, Src Port: 53, Dst Port: 49772
Source Port: 53
Destination Port: 49772
Length: 115
Checksum: 0xd564 [unverified]
[Checksum Status: Unverified]
[Stream Index: 4]
[Timestamps]
UDP payload (107 bytes)
Domain Name System (response)
Transaction ID: 0xe321
Flags: 0x1800 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
Answers
www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
[Request In: 158]
[Time: 0.014598000 seconds]
```

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.

160	6.955202	192.168.1.143	104.16.45.99	TCP	66	51330 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
161	6.955344	192.168.1.143	104.16.45.99	TCP	66	51331 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

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)

488	30.916492	128.238.38.160	128.238.29.22	DNS	86	Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
489	30.916859	128.238.29.22	128.238.38.160	DNS	118	Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
490	30.917700	128.238.38.160	128.238.29.22	DNS	76	Standard query 0x0002 NS mit.edu.poly.edu
491	30.918044	128.238.29.22	128.238.38.160	DNS	135	Standard query response 0x0002 No such name NS mit.edu.poly.edu SOA dns-prime.poly.edu
492	30.918275	128.238.38.160	128.238.29.22	DNS	67	Standard query 0x0003 NS mit.edu
493	30.918636	128.238.29.22	128.238.38.160	DNS	176	Standard query response 0x0003 NS mit.edu NS bitsy.mit.edu NS strawb.mit.edu NS w20ns.mit.edu

Domain Name System (query)

Transaction ID: 0x0001

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

- 22.29.238.128.in-addr.arpa: type PTR, class IN

[Response In: 489]

Domain Name System (query)

Transaction ID: 0x0002

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

- mit.edu.poly.edu: type NS, class IN

Domain Name System (query)

Transaction ID: 0x0003

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

- mit.edu: type NS, class IN

[Response In: 493]

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 PTR, 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.

Answers
mit.edu: type NS, class IN, ns bitsy.mit.edu
mit.edu: type NS, class IN, ns strawb.mit.edu
mit.edu: type NS, class IN, ns w20ns.mit.edu
Additional records
bitsy.mit.edu: type A, class IN, addr 18.72.0.3
strawb.mit.edu: type A, class IN, addr 18.71.0.151
w20ns.mit.edu: type A, class IN, addr 18.70.0.168

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

100	4.265296	128.238.38.160	18.72.0.3	DNS	82	Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
101	4.278516	18.72.0.3	128.238.38.160	DNS	212	Standard query response 0x0001 PTR 3.0.72.18.in-addr.arpa PTR BITSY.MIT.EDU NS W20NS.MIT.EDU NS BITSY.MIT.EDU NS ST.
102	4.279430	128.238.38.160	18.72.0.3	DNS	83	Standard query 0x0002 A www.aiit.or.kr.poly.edu
103	4.293283	18.72.0.3	128.238.38.160	DNS	135	Standard query response 0x0002 No such name A www.aiit.or.kr.poly.edu SOA gatekeeper.poly.edu
104	4.293517	128.238.38.160	18.72.0.3	DNS	74	Standard query 0x0003 A www.aiit.or.kr
105	4.307859	18.72.0.3	128.238.38.160	DNS	156	Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.kr NS w3.aiit.or.kr A 222.106.36.66 A

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.

<p>Queries</p> <ul style="list-style-type: none"> 3.0.72.18.in-addr.arpa: type PTR, class IN <p>Answers</p> <ul style="list-style-type: none"> 3.0.72.18.in-addr.arpa: type PTR, class IN, BITSY.MIT.EDU <p>Authoritative nameservers</p> <ul style="list-style-type: none"> 18.in-addr.arpa: type NS, class IN, ns W20NS.MIT.EDU 18.in-addr.arpa: type NS, class IN, ns BITSY.MIT.EDU 18.in-addr.arpa: type NS, class IN, ns STRAWB.MIT.EDU <p>Additional records</p> <ul style="list-style-type: none"> W20NS.MIT.EDU: type A, class IN, addr 18.70.0.160 BITSY.MIT.EDU: type A, class IN, addr 18.72.0.3 STRAWB.MIT.EDU: type A, class IN, addr 18.71.0.151 <p>[Request In: 100]</p> <p>[Time: 0.013220000 seconds]</p>	<p>Domain Name System (response)</p> <p>Transaction ID: 0x0002</p> <p>Flags: 0x8583 Standard query response, No such name</p> <p>Questions: 1</p> <p>Answer RRs: 0</p> <p>Authority RRs: 1</p> <p>Additional RRs: 0</p> <p>Queries</p> <ul style="list-style-type: none"> www.aiit.or.kr.poly.edu: type A, class IN <p>Authoritative nameservers</p> <p>[Request In: 102]</p> <p>[Time: 0.013853000 seconds]</p>	<p>Queries</p> <ul style="list-style-type: none"> www.aiit.or.kr: type A, class IN <p>Answers</p> <ul style="list-style-type: none"> www.aiit.or.kr: type A, class IN, addr 218.36.94.200 <p>Authoritative nameservers</p> <ul style="list-style-type: none"> aiit.or.kr: type NS, class IN, ns ns.aiit.or.kr aiit.or.kr: type NS, class IN, ns w3.aiit.or.kr <p>Additional records</p> <ul style="list-style-type: none"> ns.aiit.or.kr: type A, class IN, addr 222.106.36.66 w3.aiit.or.kr: type A, class IN, addr 222.106.36.67
--	---	--

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.

www.aiit.or.kr: type A, class IN, addr 218.36.94.200
Name: www.aiit.or.kr
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 3338 (55 minutes, 38 seconds)
Data length: 4
Address: 218.36.94.200