

Name:

Dawood Sarfraz

Roll no:

20P-0153

Section:

BSCS-5B

Computer Networks lab:

09

Lab Homework

FAST NUCES Peshawar Campus

1. Locate the DNS query and response messages. Are they sent over UDP or TCP?

```
ubuntu@20p-0153: ~  
ubuntu@20p-0153:~$ nslookup www.rediff.com  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
www.rediff.com canonical name = rediff.com.edgekey.net.  
rediff.com.edgekey.net canonical name = e81366.a.akamaiedge.net.  
Name:   e81366.a.akamaiedge.net  
Address: 2.16.158.74  
Name:   e81366.a.akamaiedge.net  
Address: 2.16.158.82  
  
ubuntu@20p-0153:~$
```

2. What is the destination port for the DNS query message? What is the source port of DNS response message?

```
ubuntu@20p-0153: ~  
ubuntu@20p-0153:~$  
ubuntu@20p-0153:~$  
ubuntu@20p-0153:~$  
ubuntu@20p-0153:~$  
ubuntu@20p-0153:~$ nslookup -type=NS uoi.gr  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
uoi.gr nameserver = sns0.grnet.gr.  
uoi.gr nameserver = sns1.grnet.gr.  
uoi.gr nameserver = kouzina.noc.uoi.gr.  
uoi.gr nameserver = marina.noc.uoi.gr.  
  
Authoritative answers can be found from:  
  
ubuntu@20p-0153:~$  
ubuntu@20p-0153:~$  
ubuntu@20p-0153:~$  
ubuntu@20p-0153:~$
```

1. Locate the DNS query and response messages. Are they sent over UDP or TCP?

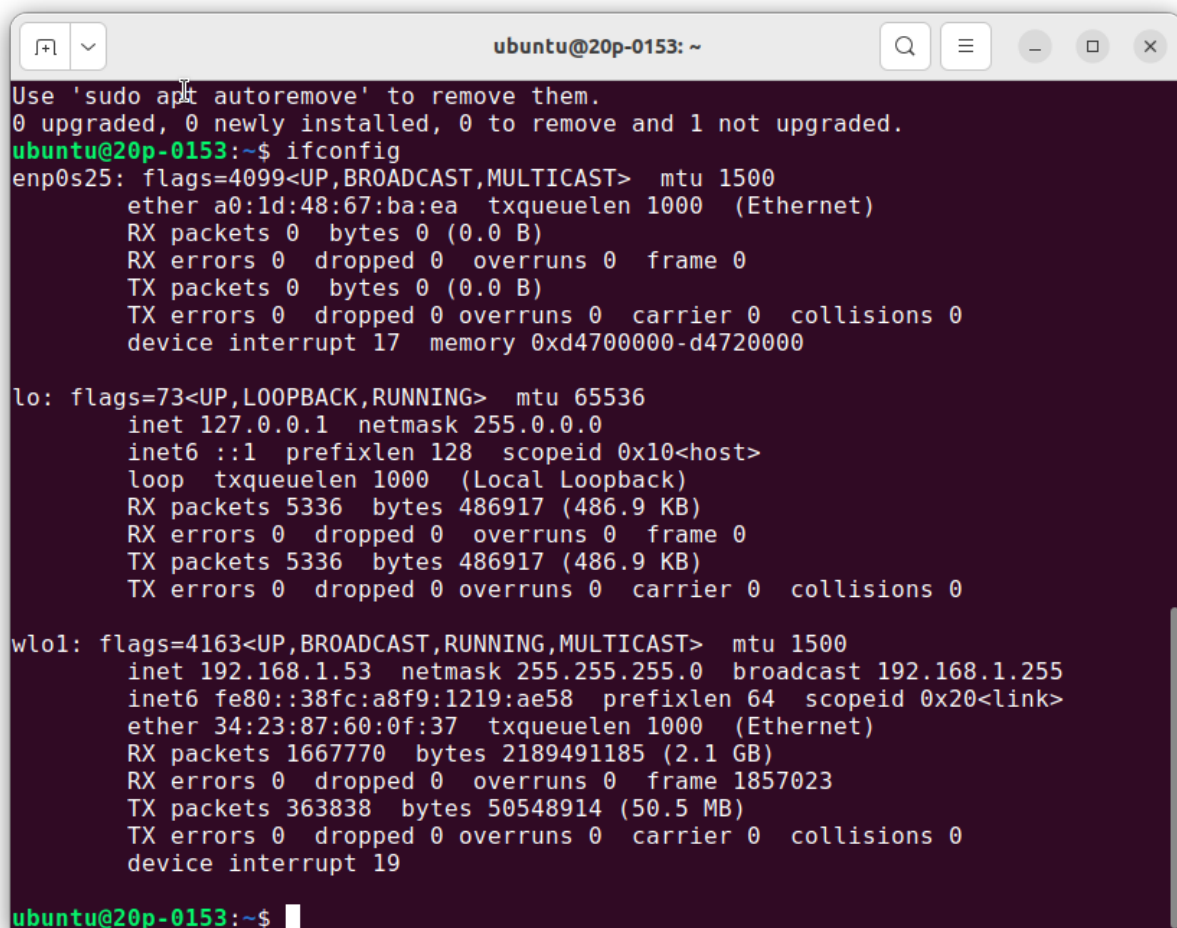
They are sent over UDP

2. What is the destination port for the DNS query message? What is the source port of DNS response messages?

The destination port for the DNS query is 53 and the source port of the DNS response is 53

3. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

It's sent to 192.168.1.1, which is the IP address of one of my local DNS servers.



```
ubuntu@20p-0153: ~  
Use 'sudo apt autoremove' to remove them.  
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.  
ubuntu@20p-0153:~$ ifconfig  
enp0s25: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500  
    ether a0:1d:48:67:ba:ea 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  
    device interrupt 17 memory 0xd4700000-d4720000  
  
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 5336 bytes 486917 (486.9 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 5336 bytes 486917 (486.9 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.53 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 fe80::38fc:a8f9:1219:ae58 prefixlen 64 scopeid 0x20<link>  
    ether 34:23:87:60:0f:37 txqueuelen 1000 (Ethernet)  
    RX packets 1667770 bytes 2189491185 (2.1 GB)  
    RX errors 0 dropped 0 overruns 0 frame 1857023  
    TX packets 363838 bytes 50548914 (50.5 MB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
    device interrupt 19  
  
ubuntu@20p-0153:~$
```

4. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

It is a class A Standard Query and it doesn't contain any answers.

5. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

There were 2 answers containing information about the name of the host, the type of address, class, the TTL, the data length and the IP address.

www.ietf.org: type A, class inet, addr 65.246.255.51

Name: www.ietf.org

Type: Host address

Class: inet

Time to live: 1 hour

Data length: 4

Addr: 65.246.255.51

www.ietf.org: type A, class inet, addr 132.151.6.75

Name: www.ietf.org

Type: Host address

Class: inet

Time to live: 1 hour

Data length: 4

Addr: 132.151.6.75

6. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

The first SYN packet was sent to 65.246.255.51 which corresponds to the first IP address provided in the DNS response message.

7 This web page contains images. Before retrieving each image, does your host issue new DNS queries?

No, Before retrieving each image, does your host issue new DNS queries.

8. What is the destination port for the DNS query message? What is the source port of DNS response messages?

The destination port of the DNS query is 53 and the source port of the DNS response is 53.

9. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

It's sent to 192.168.1.1 which as we can see from the ipconfig –all screenshots, is the default local DNS server.

10. Examine the DNS query message. What “Type” of DNS query is it? Does the query message containing any “answers”?

This query is of Class A and it doesn't contain any answers.

11. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

The response DNS message contains one answer containing the name of the host, the type of address, the class, and the IP address.

www.mit.edu: type A, class inet, addr 18.7.22.83

Name: www.mit.edu

Type: Host address

Class: inet

Time to live: 1 minute

Data length: 4

Addr: 18.7.22.83

12. Provide a screenshot.

The screenshot shows the Wireshark network protocol analyzer. The filter bar at the top is set to 'ip.addr == 128.238.38.160'. The packet list shows several DNS packets, with packet 493 selected, which is a 'Standard query response NS bitsy.mit.edu'. The packet details pane shows the following information:

- Authority RRs: 0
- Additional RRs: 3
- Queries
 - mit.edu: type NS, class IN
 - Name: mit.edu
 - Type: NS (Authoritative name server)
 - Class: IN (0x0001)
- Answers
 - mit.edu: type NS, class IN, ns bitsy.mit.edu
 - Name: mit.edu
 - Type: NS (Authoritative name server)
 - Class: IN (0x0001)
 - Time to live: 5 hours, 45 minutes, 36 seconds
 - Data length: 8
 - Name server: bitsy.mit.edu

