

DNS Exercise 1.1
=====

1. Configure the resolver to be used by your server

Check that /etc/resolv.conf contains the address of a resolver that will work. You can specify more than one if you like, like this:

```
search sse.ws.afnog.org
nameserver 196.200.223.10
nameserver 196.200.223.12
```

2. Generate some test DNS queries using "dig"

Run each command below, look for the "ANSWER SECTION" and write down the result. Make a note of the TTL as well. Repeat the command.

Is the TTL the same as in the first try? Are the responses authoritative?

COMMAND =====	RESULT =====	TTL (1st) =====	TTL (2nd) =====
# dig www.tiscali.co.uk. a	_____	_____	_____
# dig afnog.org. mx	_____	_____	_____
# dig www.afrinic.net. aaaa	_____	_____	_____
# dig psg.com. aaaa	_____	_____	_____
# dig <domain of your choice> a	_____	_____	_____
# dig <domain of your choice> mx	_____	_____	_____
# dig tiscali.co.uk. txt	_____	_____	_____
# dig ripe.net. txt	_____	_____	_____
# dig afnog.org. txt	_____	_____	_____

```
# dig geek.tiscali.co.uk. a _____
```

Now send some queries to another caching server. How long did it take each answer to be received?

```
COMMAND  
=====
```

```
RESULT  
=====
```

```
# dig @8.8.8.8 psg.com. a  
_____
```

```
# dig @rip.psg.com. yahoo.com. a  
_____
```

```
# dig @zoe.dns.gh. www.afrinic.net. aaaa  
_____
```

```
# dig @<a-server-of-yours> <domain-of-yours> a  
_____
```

3. Reverse DNS lookups

Now try some reverse DNS lookups. Remember to reverse the four parts of the IP address, add '*.in-addr.arpa.*', and ask for a *PTR* resource record. For example, for 216.235.14.38:

```
# dig 38.14.235.216.in-addr.arpa. ptr
```

Repeat for an IP address of your choice.

Now try the short form of dig using the '-x' flag for reverse lookups:

```
# dig -x 216.235.14.38
```

```
# dig -x 2001:4900:1:392::38
```

```
# dig @<server-of-your-choice> -x <ip-address-of-your-choice>
```

4. Use tcpdump to show DNS traffic

In a separate window, run the following command (you must be 'root')

```
# tcpdump -n -s 0 -v udp port 53
```

(if tcpdump is not installed, you will see a "command not found")

error. You can install tcpdump and avoid the error by typing "apt-get install tcpdump" as root)

This shows all packets going in and out of your machine for UDP port 53 (DNS). Now go to another window and repeat some of the 'dig' queries from earlier. Look at the output of tcpdump, check the source and destination IP address of each packet

- n Prevents tcpdump doing reverse DNS lookups on the packets it receives, which would generate additional (confusing) DNS traffic
- s 0 Read the entire packet (otherwise tcpdump only reads the headers)
- i bge0 Which interface to listen on (use ifconfig to determine the name of your ethernet interface)
- udp port 53 A filter which matches only packets to/from UDP port 53