Internetworking exercise 2 - ARP

1. Open a new console window (switch consoles using Alt-F1, Alt-F2 etc) and login as ’root’. Run this tcpdump command there:

```
# tcpdump -i fxp0 -n -e
```

(The ’-e’ flag shows the layer 2 ethernet headers). You may already start to see ARP traffic from other people in the class.

2. Return to the first window, and list the contents of the ARP cache on your machine:

```
$ arp -an
```

```
How many entries are there?  _______
```

Now, pick someone else in the class who is not already in your ARP cache, and ping them.

```
$ ping -c3 x.x.x.x
```

When you’ve started this, return to your tcpdump window and see if you can identify the ARP request ("arp who-has x.x.x.x tell y.y.y.y") and response ("arp reply x.x.x.x is-at zz:zz:zz:zz:zz:zz"), followed by the pings (echo request, echo reply).

Have another look at your ARP cache and check that your neighbour’s IP address and ethernet (MAC) address is now there:

```
$ arp -an
```

```
How many entries does it contain now?  _______
```

> Note: if you are slow, and other people in the class have pinged you before you’ve pinged them, then there will already be entries for them in your ARP cache. That’s because they sent you an ECHO REQUEST, and your machine had to send back an ECHO RESPONSE, and in order to send the reply, your machine used ARP to find their MAC address.
>
> If this has happened to you, you can flush entries from your ARP cache: you need to be ’root’ to do this.
>
> ```
> # arp -dn x.x.x.x        -- delete one entry
> # arp -adn               -- delete all entries
> ```
>
> (-a = all entries, -d = delete, -n = do not perform reverse DNS lookups of IP address to hostname). However, note that you very rarely have to do this in practice. That’s because ARP works so well behind-the-scenes.

If you have time, examine the tcpdump output more carefully.

```
Which of the packets are broadcasts? How can you tell?
```

```
Notice that IPv4 packets and ARP packets have a different ethertype code -
what are they?

       ethertype IPv4  0x_____          ethertype ARP  0x_____

You don’t need to remember these, but it does confirm that ARP packets and
IP datagrams are two different things entirely.
```