Lab 1 Answers

Tasks 1 & 2

An example of running `ipconfig` on the command line can be seen in Figure 1. The output on your computer will certainly be different. Most noticeably, you may only see information for the one network interface. In the above case, the computer appears to have two network interfaces named “`Ethernet adapter Local Area Connection`” and “`Ethernet adapter VirtualBox Host-Only Network`”. As the names suggest, both are Ethernet interfaces, with the former being connected to the “Local Area” and the latter to a “VirtualBox Host-Only Network”. The second adapter will only appear if VirtualBox – a virtualisation software package (see https://www.virtualbox.org/) – is installed on your computer and is a virtual network interface used to communicate with the virtual machines running on the computer. For the remainder of this report we will focus on the first adapter.

Although this invocation of the `ipconfig` command returned some quite useful information for our network interfaces, it didn’t print its physical (MAC) address. To retrieve the latter, we need to request a complete report via `ipconfig /all (see` Figure 2`)`. The output then becomes quite more verbose. The bit that we care for in the context of this lab is the interface’s Physical (MAC) Address, which in this case is `B8-CA-3A-8E-58-70`.

```
C:\Users\nikos>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . : dcs.gla.ac.uk
   Link-local IPv6 Address . . . . . : fe80::b9b2:aa16:827b:ee9f%11
   IPv4 Address. . . . . . . . . . . : 130.209.247.158
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : fe80::e22f:6dff:fe2c:ed80%11
                                       130.209.240.48

Ethernet adapter VirtualBox Host-Only Network:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74e2:55c5:b056:4c32%16
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

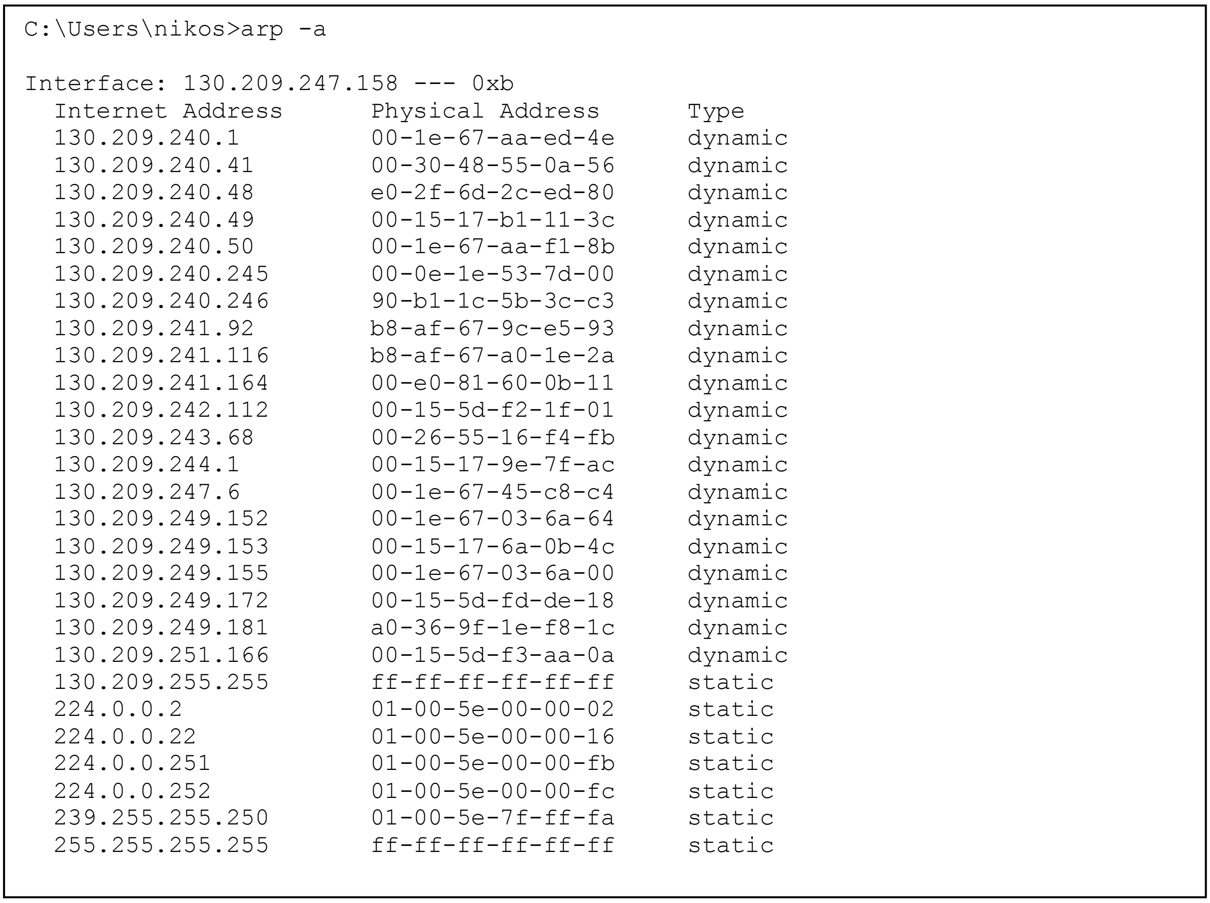
Figure 1 Output of 'ipconfig'

```
C:\Users\nikos>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : batam
   Primary Dns Suffix  . . . . . . . : ad.dcs.gla.ac.uk
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : ad.dcs.gla.ac.uk
                                       gla.ac.uk
                                       dcs.gla.ac.uk

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : dcs.gla.ac.uk
   Description . . . . . . . . . . . : Intel(R) 82579LM Gigabit Network Connection
   Physical Address. . . . . . . . . : B8-CA-3A-8E-58-70
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::b9b2:aa16:827b:ee9f%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 130.209.247.158(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Lease Obtained. . . . . . . . . . : 10 October 2018 16:16:14
   Lease Expires . . . . . . . . . . : 21 October 2018 04:16:12
   Default Gateway . . . . . . . . . : fe80::e22f:6dff:fe2c:ed80%11
                                       130.209.240.48
   DHCP Server . . . . . . . . . . . : 130.209.240.50
   DHCPv6 IAID . . . . . . . . . . . : 246991418
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-19-E0-3C-97-B8-CA-3A-8E-58-70

   DNS Servers . . . . . . . . . . . : 2001:630:40:40::10
                                       2001:630:40:40::12
                                       130.209.249.155
                                       130.209.249.152
                                       130.209.244.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       gla.ac.uk
```

Figure 2 Output of 'ipconfig /all' (excerpt)

Tasks 3 & 4

The output of `arp -a` on the above computer can be seen in Figure 3. We can spot a number of “peculiarities”: (a) some entries are marked as static while others as dynamic and there appear to be two static entries sharing the same physical address (`ff-ff-ff-ff-ff-ff`); (b) all static entries, other than the two same ones above, seem to share the same prefix (`01-00-5e`).



```
C:\Users\nikos>arp -a

Interface: 130.209.247.158 --- 0xb
  Internet Address      Physical Address      Type
  130.209.240.1         00-1e-67-aa-ed-4e     dynamic
  130.209.240.41        00-30-48-55-0a-56     dynamic
  130.209.240.48        e0-2f-6d-2c-ed-80     dynamic
  130.209.240.49        00-15-17-b1-11-3c     dynamic
  130.209.240.50        00-1e-67-aa-f1-8b     dynamic
  130.209.240.245       00-0e-1e-53-7d-00     dynamic
  130.209.240.246       90-b1-1c-5b-3c-c3     dynamic
  130.209.241.92        b8-af-67-9c-e5-93     dynamic
  130.209.241.116       b8-af-67-a0-1e-2a     dynamic
  130.209.241.164       00-e0-81-60-0b-11     dynamic
  130.209.242.112       00-15-5d-f2-1f-01     dynamic
  130.209.243.68        00-26-55-16-f4-fb     dynamic
  130.209.244.1         00-15-17-9e-7f-ac     dynamic
  130.209.247.6         00-1e-67-45-c8-c4     dynamic
  130.209.249.152       00-1e-67-03-6a-64     dynamic
  130.209.249.153       00-15-17-6a-0b-4c     dynamic
  130.209.249.155       00-1e-67-03-6a-00     dynamic
  130.209.249.172       00-15-5d-fd-de-18     dynamic
  130.209.249.181       a0-36-9f-1e-f8-1c     dynamic
  130.209.251.166       00-15-5d-f3-aa-0a     dynamic
  130.209.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Figure 3 Output of 'arp -a' (excerpt)

Let's now go over these peculiarities one by one:

(a) We'd expect all entries to be dynamic, as ARP is designed to allow for the discovery of hosts on the same link as our computer. There must then be something special with these static entries.
The MAC address that appears twice in this list is the broadcast MAC address; that is, the address used when a computer wishes to sends a message to all other devices on the same link. We can see that these are mapped to two IP addresses: 130.209.255.255 and 255.255.255.255. We now know that the former is the broadcast address for the 130.209.240.0/20 network (i.e., Glasgow University's network). The latter is the broadcast address for the 0.0.0.0/0 network – a.k.a. *this* network, meaning whatever network the computer is connected to, irrespective of the network's address (see https://en.wikipedia.org/wiki/Broadcast_address). Both of these entries are assumed known for ARP to operate and don't change; the former stays the same as long as the network interface is on the same network, while the latter is a predefined constant. As such, these entries are static in the ARP cache; i.e., they won't be removed if no relevant traffic is seen.

(b) The remaining static entries all share the same prefix, which seems to be `01-00-5e`. On a closer examination at the binary representation of these MAC addresses, the common prefix is actually 25 bits long; that is, the common prefix is `01-00-5e` plus an extra `0`-bit:

```
0000 0001 – 0000 0000 – 0101 1110 – 0
```

This is one of the MAC addresses prefixes used for IPv4 multicast, and similarly the IP addresses mapping to these MAC addresses are IPv4 multicast addresses[1]. More specifically, the first one (`*.0`) is called a base address and is always reserved; `*.1` is used for all multicasting host groups while `*.2` for all subnet routers.

Looking at the OUI database, the specific MAC address for my computer is assigned to Dell Inc. (for the computers in the lab, the MAC address should be one belonging to Hewlett Packard). The remaining MAC addresses belong to:

- `00-0e-1e`: QLogic
- `00-15-17`: Intel
- `00-15-5d`: Microsoft
- `00-1e-67`: Intel
- `00-26-55`: Hewlett Packard
- `00-30-48`: Super Micro Computer
- `00-e0-81`: Tyan Computer
- `90-b1-1c`: Dell
- `a0-36-9f`: Intel
- `b8-af-67`: Hewlett Packard
- `e0-2f-6d`: Cisco

We can map the above then to either manufacturers of computer motherboards/systems (Tyan, SuperMicro, HP, Dell, Intel), manufacturers of network appliances (QLogic), or virtualised infrastructure (Microsoft/Hyper-V).

Task 5

The standard way to "force" an entry to be added to the ARP cache (other than through acquiring administrative rights and adding the entry by hand), is by simply initiating some communication with the target host. This can be done via such commands as `ping`, or even by merely entering the target IP as a web address in a browser window; in the latter case no web page will (most probably) be displayed, but the data-link (and network and transport) layer(s) will have been engaged in the process. If the target computer is on the same link as ours, there should then be an entry added to our ARP cache. Once this is done, we can use `arp -a` again to retrieve the new entry.

Task 6

As discussed previously, by merely accessing the web page itself, an entry will be added to the ARP cache of our computer. In this case, the MAC address of the web server of our School is:

`00-1e-67-aa-ed-4e`.

Task 7

For this task, we can access the web server of the University just fine. However, no relevant entry is added to the ARP cache. This is typically due to the fact that the target host is not on the same link as our computer; that is, data travelling from our computer to the web server and back needs to go through one or more routers. Unless said routers are configured to relay ARP traffic, we won't be able to retrieve the MAC address of the web server. This isn't a problem as the end-to-end communication is handled by protocols at higher layers of the OSI model.

[1] https://en.wikipedia.org/wiki/Multicast_address

We can now confirm the above by using `tracert` from lab 2. We can then see (Figure 4) that there is only one hop to the School web server – i.e., said server is on the same link as our computer – but there are two intermediate hops (routers) on the path to the University web server.

```
C:\Users\nikos>tracert 130.209.241.1

Tracing route to albatross.dcs.gla.ac.uk [130.209.241.1]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  albatross.dcs.gla.ac.uk [130.209.241.1]

Trace complete.

C:\Users\nikos>tracert 130.209.16.90

Tracing route to www3.gla.ac.uk [130.209.16.90]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  rona.dcs.gla.ac.uk [130.209.240.48]
  2    <1 ms    <1 ms    <1 ms  130.209.2.17
  3    <1 ms    <1 ms    <1 ms  www3.gla.ac.uk [130.209.16.90]

Trace complete.
```

Figure 4 Output of 'tracert'