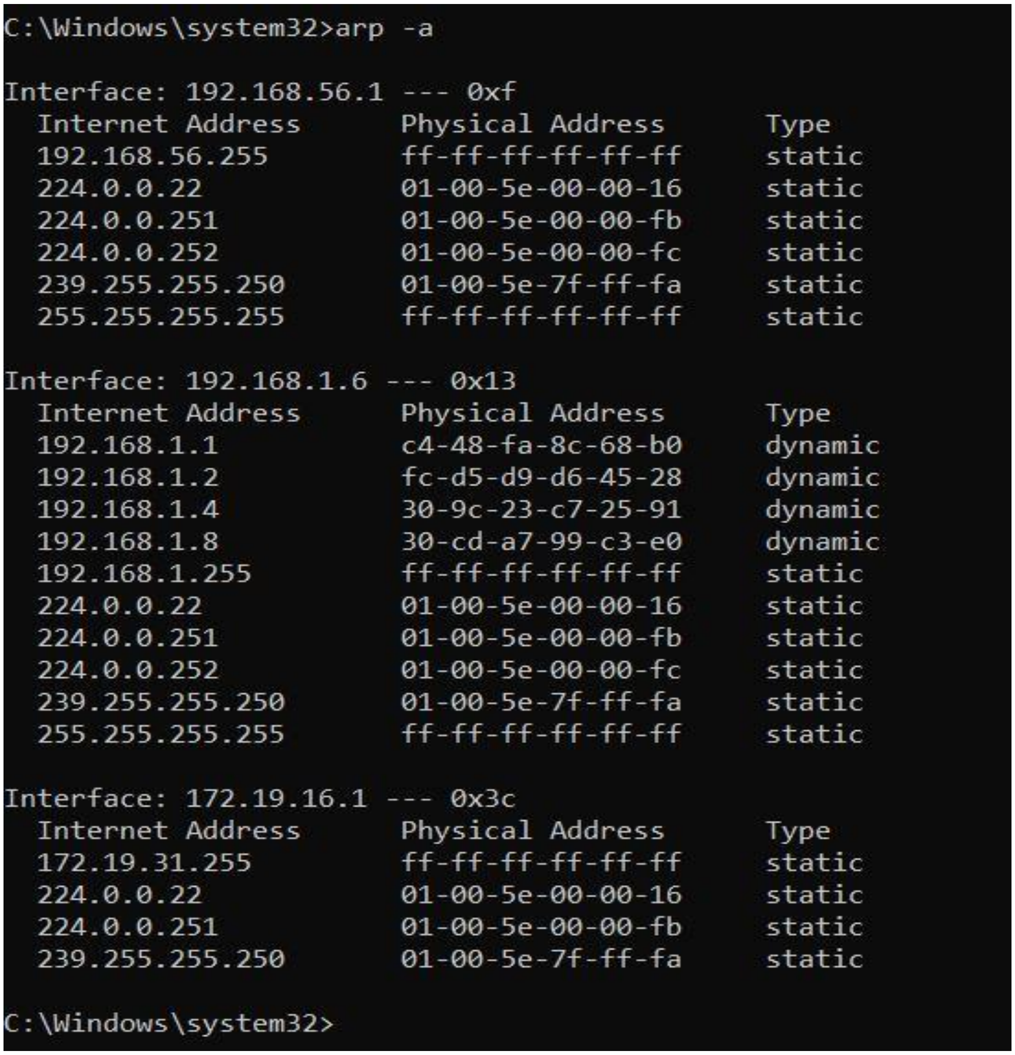
Exercise 1 – Basic network stuff

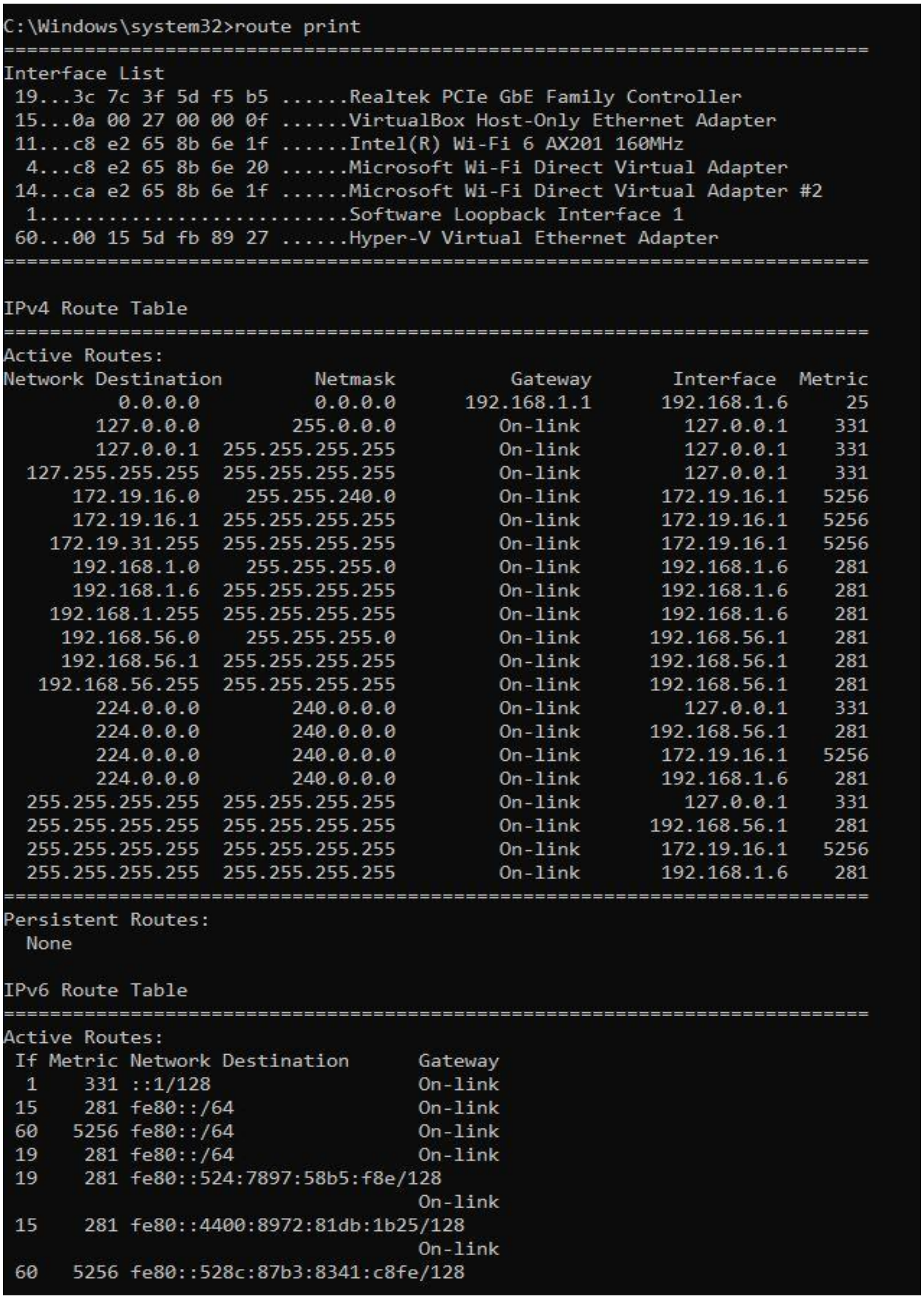
Difficulty: Easy

arp command manipulates the System's ARP cache. It also allows a complete dump of the ARP cache. ARP stands for Address Resolution Protocol. The primary function of this protocol is to resolve the IP address of a system to its mac address, and hence it works between level 2(Data link layer) and level 3(Network layer).



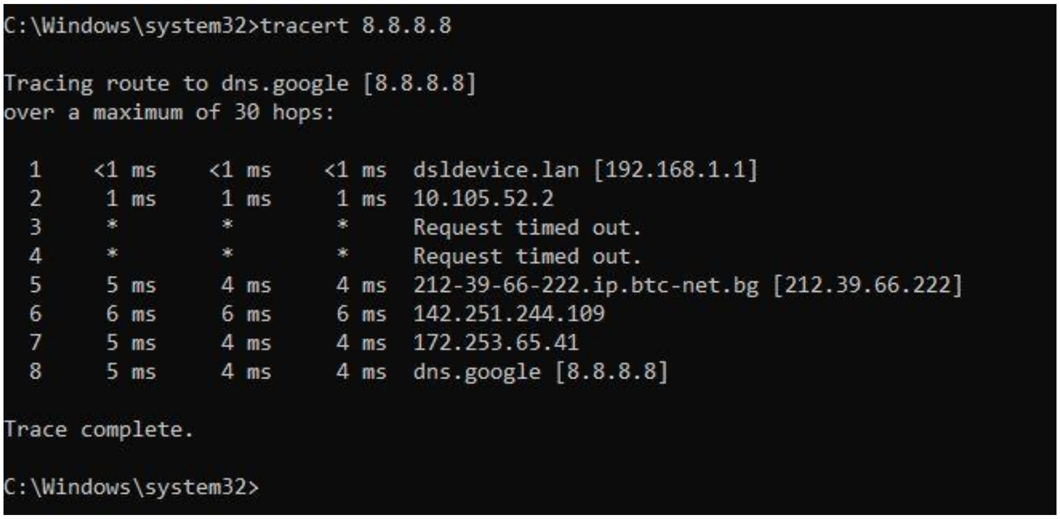
```
C:\Windows\system32>arp -a

Interface: 192.168.56.1 --- 0xf
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     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

Interface: 192.168.1.6 --- 0x13
  Internet Address      Physical Address      Type
  192.168.1.1           c4-48-fa-8c-68-b0     dynamic
  192.168.1.2           fc-d5-d9-d6-45-28     dynamic
  192.168.1.4           30-9c-23-c7-25-91     dynamic
  192.168.1.8           30-cd-a7-99-c3-e0     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     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

Interface: 172.19.16.1 --- 0x3c
  Internet Address      Physical Address      Type
  172.19.31.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\Windows\system32>
```

To display the routing table on Windows, we can use route print or netstat -r command. The output of both commands is identical. However, the route command has command options to filter the output to show the routing table for IPv4 or IPv6 separately.



```
C:\Windows\system32>route print
===========================================================================
Interface List
 19...3c 7c 3f 5d f5 b5 ......Realtek PCIe GbE Family Controller
 15...0a 00 27 00 00 0f ......VirtualBox Host-Only Ethernet Adapter
 11...c8 e2 65 8b 6e 1f ......Intel(R) Wi-Fi 6 AX201 160MHz
  4...c8 e2 65 8b 6e 20 ......Microsoft Wi-Fi Direct Virtual Adapter
 14...ca e2 65 8b 6e 1f ......Microsoft Wi-Fi Direct Virtual Adapter #2
  1...........................Software Loopback Interface 1
 60...00 15 5d fb 89 27 ......Hyper-V Virtual Ethernet Adapter
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1      192.168.1.6     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      172.19.16.0    255.255.240.0         On-link       172.19.16.1   5256
      172.19.16.1  255.255.255.255         On-link       172.19.16.1   5256
    172.19.31.255  255.255.255.255         On-link       172.19.16.1   5256
      192.168.1.0    255.255.255.0         On-link       192.168.1.6    281
      192.168.1.6  255.255.255.255         On-link       192.168.1.6    281
    192.168.1.255  255.255.255.255         On-link       192.168.1.6    281
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link      192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link       172.19.16.1   5256
        224.0.0.0        240.0.0.0         On-link       192.168.1.6    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      192.168.56.1    281
  255.255.255.255  255.255.255.255         On-link       172.19.16.1   5256
  255.255.255.255  255.255.255.255         On-link       192.168.1.6    281
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
 15    281 fe80::/64                On-link
 60   5256 fe80::/64                On-link
 19    281 fe80::/64                On-link
 19    281 fe80::524:7897:58b5:f8e/128
                                    On-link
 15    281 fe80::4400:8972:81db:1b25/128
                                    On-link
 60   5256 fe80::528c:87b3:8341:c8fe/128
```

The Windows Tracert tool determines the route to a destination by sending ICMP packets to the destination.In these packets, Tracert uses varying IP Time-To-Live (TTL) values.The TTL is effectively a hop counter, where a hop is a location that the packet stops at, to reach the destination.



```
C:\Windows\system32>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dsldevice.lan [192.168.1.1]
  2     1 ms     1 ms     1 ms  10.105.52.2
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     5 ms     4 ms     4 ms  212-39-66-222.ip.btc-net.bg [212.39.66.222]
  6     6 ms     6 ms     6 ms  142.251.244.109
  7     5 ms     4 ms     4 ms  172.253.65.41
  8     5 ms     4 ms     4 ms  dns.google [8.8.8.8]

Trace complete.

C:\Windows\system32>
```

Why would you need to use the ping command?

Answer:

I would use the ping command to quickly determine whether a machine has internet access and can communicate with other computers or network devices.

You can also use a series of pings to locate and resolve issues.

Write down the TCP/UDP ports of the most commonly used services bellow in the form of TCP[PORT] or UDP[PORT].

As an example, the first two answers have been filled in:

HTTP – TCP80

SNMP – UDP161

HTTPS - TCP 443

DNS client – Port range 1024 -655

DNS zone transfer – TCP 53

SMTP – TCP 1701

SSH – TCP 1194

FTP – TCP 1337

Telnet – TCP 1433-1434

MSSQL – TCP port 1433

MySQL – TCP port 3306

PostreSQL – TCP port 5432

RDP (Remote Desktop Protocol) – TCP port 3389

NTP – TCP 123

NFS – TCP port 2049