arp-scan

arp-scan is a fast ARP packet scanner that can find all active IPv4 devices on a network. Devices cannot hide from ARP packets like they can hide from Ping and it should detect all devices including those with firewalls.

To install arp-scan, connect to your RPi 3 in your preferred manner (e.g. headless or screen-based)

Open a terminal window on the Raspberry Pi and enter the following command:

```
sudo apt-get update
sudo apt-get install arp-scan
```

Once installed, check that it's working correctly by entering the command on the Raspberry Pi: `sudo arp-scan -l` . This will list all devices on your local network that responded . You should see a list of devices and corresponding IP and MAC addresses on your local network. It may take a moment to load if you are on a large network:

```
pi@sensePi:~ $ sudo arp-scan -l
Interface: wlan0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
192.168.1.1     c8:0e:14:46:c2:c1       (Unknown)
192.168.1.43    34:e6:d7:06:ef:6f       (Unknown)
192.168.1.63    a0:63:91:30:c5:9b       (Unknown)
192.168.1.20    b0:e1:7e:09:9c:fb       (Unknown)
192.168.1.55    00:22:61:e2:a0:50       Frontier Silicon Ltd
192.168.1.65    64:b5:c6:52:3a:85       (Unknown)
192.168.1.254   00:1d:7e:27:b8:04       Cisco-Linksys, LLC
192.168.1.56    d4:28:d5:37:7e:a2       (Unknown)

9 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 4.048 seconds (63.24 hosts/sec). 8 responded
pi@sensePi:~ $
```

arp scan

- Question: If you had to write a program to replicate the list function in arp-scan, how would you do it?

Presence detection

ARP-Scan lists all devices (if any) connected your local network at the time the scan was executed. By scanning the local network for certain devices' MAC addresses, we can detect their 'presence' on the network. Furthermore, if connected by WiFi, we can deduce that the physical device itself is within the range of the WiFi access point (e.g. at home).

- There are various ways of finding a particular device MAC address and a quick internet search will soon let you know how to find the MAC address for the WiFi interface on your Smartphone.
- Find and record the MAC address of your smartphones Wifi interface (or if you're not using a Smarthone, any other device on the Wifi Network for now)
- Check for the presence of the device by doing a 'grep' on the device list returned by apr-scan:

```
sudo arp-scan -l | grep YOUR_DEVICE_MAC
```

```
pi@sensePi:~ $ sudo arp-scan -l | grep d4:28:d5:37:7e:a2
192.168.1.56    d4:28:d5:37:7e:a2       (Unknown)
```

arp scan

If your device was found, the command will output its address info. If nothing appears, make sure that it's connected to the same local WiFi network as your RPi. Smart devices are fairly energy efficient so you may also need to 'wake up' your device, as it may drop the WiFi connection if left idle for too long.

Now that we have a mechanism to detect known devices on the local network, we can write a short python program to get the RPi/SenseHAT to indicate the presence/absence of a device.