Arp-Scan

Arp-Scan is a command line utility for scanning MAC addresses that are stored in the ARP Table. By default on Raspbian the timeout for ARP table entries is 60s, you can check cat /proc/sys/net/ipv4/neigh/default/gc_stale_time for exact time.

Installation

To install Arp-Scan, from the command line enter: Note: you may have to do a sudo apt-get update first.

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

Operation

To use arp-scan enter the following from the command line:

```
sudo arp-scan -l
```

arp-scan will not show the local NIC doing the scan mac address

Example Output

```
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.8.1 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
192.168.100.1     11:1d:aa:a6:66:1b       DrayTek Corp.
192.168.100.2     aa:ac:6f:0c:cf:66       Dell Inc
192.168.100.3     ac:da:0b:6b:cd:ab       (Unknown)
192.168.100.4     ab:61:bb:df:da:dd       (Unknown)
192.168.100.5     aa:00:eb:06:ba:bd       (Unknown)
192.168.100.6     aa:00:eb:a0:ba:ab       (Unknown)
192.168.100.7     aa:aa:b6:6a:ba:d1       (Unknown)
192.168.100.16    b1:bd:6c:1e:b6:bb       (Unknown)
192.168.100.61    11:1a:fb:bb:6b:a6       BSkyB Ltd
192.168.100.66    a6:aa:6e:b1:ba:d1       (Unknown)
192.168.100.66    a6:aa:6e:b1:ba:d1       (Unknown) (DUP: 2)
192.168.100.60    aa:ae:6a:0b:ba:a1       (Unknown)
192.168.100.62    11:ae:fa:f1:ab:aa       (Unknown)
192.168.100.63    fb:6c:ba:ec:1f:ab       (Unknown)
192.168.100.64    aa:ae:6a:1a:10:1d       (Unknown)
```

*Note: these are fabricated IP and MAC Addresses so don't go looking for them :)

Searching for a particular MAC

If there are a lot of devices on the network, and you know the MAC, you can search using arp-scan and filter the output with grep

```
sudo arp-scan -l | grep "MAC"
sudo apr-scan -l | grep "00:a1:d0:00-4a:01"
```

From:
https://wiki.alanwalker.uk/ - **WalkerWiki - wiki.alanwalker.uk**

Permanent link:
https://wiki.alanwalker.uk/doku.php?id=arp-scan&rev=1474396431

Last update: **2023/03/09 22:35**