arp-scan

Monitoring the network neighbours can possibly help to find attack vectors in Freifunk Network. On Linux, the onboard arp tool will only show the IP/MAC combinations that the system has already used. So, it will only show the Raspberry Pi in that list if you have already 'contacted' it via it's IP address (via commands like ssh, telnet, ping, http, nc, etc). arp-scan, however, will actively search for unknown IP/MAC combinations on your LAN/WLAN.

Linux

https://github.com/royhills/arp-scan

```
cd /opt
apt-get install automake libpcap-dev

git clone https://github.com/royhills/arp-scan.git
cd arp-scan/

aclocal
autoheader
autoreconf -i
automake
autoconf
./configure
make

ARP_SHARE="/usr/local/share/arp-scan/"
mkdir -p $ARP_SHARE
cp /opt/arp-scan/ieee-oui.txt $ARP_SHARE
cp /opt/arp-scan/ieee-iab.txt $ARP_SHARE
cp /opt/arp-scan/mac-vendor.txt $ARP_SHARE

cd /usr/bin && ln -sf /opt/arp-scan/arp-scan arp-scan
```

```
arp-scan --help

arp-scan --localnet --interface=eth0 > ./arp-scan.txt
```

```
Ending arp-scan 1.9.7: 4096 hosts scanned in 18.442 seconds (222.10 hosts/sec). 484 responded
```

Windows

https://github.com/QbsuranAlang/arp-scan-windows

```
arp-scan.exe -t 10.149.2.89/16 > arp-scan.txt
```

Version #1
Erstellt: 2026-06-08 14:15:05 CEST von Mario Voigt
Zuletzt aktualisiert: 2026-06-08 14:15:31 CEST von Mario Voigt