nmap

Wer hat es nicht schon einmal benötigt? Welche IP Adresse hatte gleich der Druckerserver oder andere Rechner im eigenen Netz?

Nmap oder auch “Network Mapper” ist ein Portscanner der diese Aufgabe lösen kann. Ich nutze meist diesen Befehl:

```
nmap -sL 192.168.10.0/24
```

Nmap scannt dabei den Bereich (-sL Lists-San) von 192.168.10.255 – also 255 Hosts und gibt an, welche IP Adressen aktiv genutzt werden. Ein ähnlicher Befehl ist der Befehl:

```
nmap -sP 192.168.10.0/24
```

Ping-Scan: Prüft nur auf Erreichbarkeit über Ping. Dies ist sinnvoll, um ganze Netzbereiche auf aktive Hosts zu testen. Das Gerät muß also auch eine Pingantwort senden können! Dies ist der Unterschied zum List-Scan – dort muß das Gerät nicht aktiv sein!

Es gibt noch viele andere Befehle – einfach mal in der Man-Page nachschauen.

Fazit:

Unverzichtbares Werkzeug im LAN um z.B. die IP Adresse beim Einrichten eines Netzwerkdrucker zu bekommen. Alternativ ist dies natürlich auch durch das Einloggen in den Router möglich (falls man die Rechte hat!).

Anmerkung:

Wer es lieber graphisch mag sollte sich zusätzlich das Paket zenmap installieren.