

# Netzwerk

## Netzwerk-Tools

```
sudo apt-get install net-tools
```

Net-Tools

netstat

## IP-Adressen anzeigen

Eigener Rechner

```
hostname -I
```

Öffentliche IP4

```
curl -4 icanhazip.com
```

Öffentliche IP6

```
curl -6 icanhazip.com
```

## Netzwerkkarten anzeigen

```
ip a
```

oder

```
ip addr
```

Mögliche Anzeige: lo : Loopback interface, wird für die lokalen Dienste verwendet wie proxy oder Webserver <http://127.0.0.1/>

eth0/enp2s0 : Die erste Schnittstelle zum Internet oder einem Router, Switch

## Restart der Netzwerkeinstellungen

```
sudo /etc/init.d/networking restart -y
```

oder

```
sudo systemctl restart networking.service
```

## Route verfolgen

Adresse des Gateways

```
ip route show
```

Adresse einer Domain (z.B. duckduckgo.de)

Linux-Konsole

```
tracert duckduckgo.de
```

Windows-Konsole

```
tracert duckduckgo.de
```

## Netzwerktraffic analysieren

### Datenpakete mitschneiden

[Ubuntu-users->tcpdump](#)

Tool starten. Ausgabe (nur) auf der Konsole

```
sudo tcpdump
```

Daten in eine Datei schreiben.

```
sudo tcpdump -w <FILE>
```

Mit „normalem“ Editor ist diese Datei nicht lesbar. Genutzt werden kann u.a. Wireshark oder mit der Option -r auf der Konsole ausgeben.

```
sudo tcpdump -r <FILE>
```

### Datenanalyse mit Wireshark

[Ubuntu-users->Wireshark](#)



Sicherheitsrisiko: dieses Tool niemals mit Root-Rechten (sudo) starten.  
Dafür das o.a. **tcpdump** nutzen und den Traffic in eine Datei speichern oder wie u.a.



normalen Usern die Aufzeichnung erlauben.

Siehe entsprechende Hinweise hierzu unter [Ubuntuusers -> tcpdump](#) und [Ubuntuusers -> Wireshark](#)

```
sudo apt-get install wireshark
```

Nicht-Root-Usern und Mitgliedern der Gruppe wireshark grundsätzlich erlauben, Netzwerktraffic mit Wireshark aufzuzeichnen: Frage mit Ja beantworten:

```
sudo dpkg-reconfigure wireshark-common
```

Entsprechende User in die Gruppe wireshark aufnehmen

```
sudo usermod -aG wireshark <USER>
```

From:

<https://wiki.bluegnu.de/> - **gniki**

Permanent link:

<https://wiki.bluegnu.de/doku.php?id=open:it:net&rev=1720020468>

Last update: **2024/07/03 17:27**

