`traceroute` verfolgt den Weg von Netzwerk-Paketen hin zu einem bestimmten Host. Dazu verändert `traceroute` das Time to live (TTL) Feld des IP Protokolls. Durch kleine TTL Werte versucht `traceroute` ICMP TIME_EXCEEDED Antworten der einzelnen Router zu bekommen. Der einzige notwendige Parameter von `traceroute` ist der Host zu dem der Weg aufgezeigt werden soll:

```
traceroute www.tuxclouds.org
```

Für das Erfassen der einzelnen Hops (Router) am Weg vom aktuellen Rechner hin zum gewünschten Host geht traceroute folgendermaßen vor:

1. 1 Ein IP Paket mit TTL=1 wird verschickt, das Paket verwirft bereits der erste Router und schickt uns eine **ICMP TIME_EXCEEDED** Antwort zurück.
2. 2 Nun verschickt unser einmal gestartetes `traceroute` weitere Pakete und erhöht dabei die TTL immer um jeweils 1. Beim zweiten Paket (TTL=2) gelangt das Paket über den ersten Router weiter zum nächsten Router am Weg zum Host. Da das Default Gateway beim Weiterleiten des Pakets die TTL um 1 verringert, kommt das Paket mit TTL=1 am zweiten Router an. Dieser verwirft das Paket und schickt eine ICMP TIME_EXCEEDED Antwort an den ursprünglichen Rechner zurück. Analog funktioniert es dann mit TTL=3 beim dritten Router, TTL=4 beim vierten Router, usw.

Erreicht ein IP Paket mit ausreichend hoher TTL letztendlich den Ziel-Host, antwortet er mit einer ICMP „port unreachable“ Meldung. Juhu

Hinweis Im Default verwendet das Linux traceroute UDP, hingegen Windows ICMP verwendet. Wollen wir auch ICMP so erledigen wir das mit dem Schalter -I

```
traceroute -I www.tuxclouds.org
```

Oder den Weg zum Mailserver prüfen auf Port 25 ist möglich mit dem Schalter -T und -p.

```
root@twink:~# traceroute -T -p 25 www.tuxclouds.org
 traceroute to www.tuxclouds.org (46.30.212.35), 30 hops max, 60 byte
packets
 1  fritz.box (192.168.2.1)  3.794 ms  3.599 ms  7.921 ms
 2  * * *
 3  de-fra01b-rc1-ae28.fra.unity-media.net (81.210.141.33)  22.364 ms
19.576 ms  23.242 ms
 4  84.116.132.149 (84.116.132.149)  23.142 ms  21.020 ms 84.116.132.145
(84.116.132.145)  20.958 ms
 5  lag-10.ear1.Frankfurt.Level3.net (4.68.62.237)  25.061 ms  22.795 ms
44.796 ms
 6  ae-0-10.bar1.Copenhagen2.Level3.net (4.69.137.154)  64.000 ms  32.823 ms
36.196 ms
 7  * * *
 8  * * *
```

Nur mit -T wird per Default der Port 80 verwendet.