Tracerout

Programa do Linux que exibe a rota dos pacotes tcp até um destino específico, usando o protocolo ICMP e o TTL dos pacotes para a identificação.

> No Windows ele chama-se `tracert`

1 Instalação

```
sudo apt install tracerout -y
```

2 Sintaxe

```
tracerout [opção] destino
```

2.1 Opções

- `-n`: exibe apenas IP's omitindo o nome.
- `-V`: Exibe a versão do traceroute
- `-4`: Use IPv4
- `-6`: Use IPv6
- `-d --debug`: Enable socket level debugging
- `-F --dont-fragment`: Do not fragment packets
- `-f first_ttl --first=first_ttl`: Start from the first_ttl hop (instead from 1)
- `-g gate,... --gateway=gate,...`: Route packets through the specified gateway (maximum 8 for IPv4 and 127 for IPv6)
- `-I --icmp`: Use ICMP ECHO for tracerouting
- `-T --tcp`: Use TCP SYN for tracerouting (default port is 80)
- `-i device --interface=device`: Specify a network interface to operate with
- `-m max_ttl --max-hops=max_ttl`: Set the max number of hops (max TTL to be reached). Default is 30
- `-N squeries --sim-queries=squeries`: Set the number of probes to be tried simultaneously (default is 16)
- `-p port --port=port`: Set the destination port to use. It is either initial udp port value for "default" method (incremented by each probe, default is 33434), or initial seq for "icmp" (incremented as well, default from 1), or some constant destination port for other methods (with default of 80 for "tcp", 53 for "udp", etc.)
- `-t tos --tos=tos`: Set the TOS (IPv4 type of service) or TC (IPv6 traffic class) value for outgoing packets
- `-l flow_label --flowlabel=flow_label`: Use specified flow_label for IPv6 packets
- `-w MAX,HERE,NEAR --wait=MAX,HERE,NEAR`: Wait for a probe no more than HERE (default 3) times longer than a response from the same hop,or no more than NEAR (default 10) times than some next hop, or MAX (default 5.0) seconds (float point values llowed too)
- `-q nqueries --queries=nqueries`: Set the number of probes per each hop. Default is 3
- `-r`: Bypass the normal routing and send directly to a host on an attached network
- `-s src_addr --source=src_addr`: Use source src_addr for outgoing packets

- `-z sendwait --sendwait=sendwait`: Minimal time interval between probes (default 0). If the value is more than 10, then it specifies a number in milliseconds, else it is a number of seconds (float point values allowed too)
- `-e --extensions Show ICMP extensions (if present), including MPLS
- `-A --as-path-lookups`: Perform AS path lookups in routing registries and print results directly after the corresponding addresses
- `-O OPTS,... --options=OPTS,...`: Use module-specific option OPTS for the traceroute module. Several OPTS allowed, separated by comma. If OPTS is "help", print info about available options
- `--fwmark=num`: Set firewall mark for outgoing packets
- `-U --udp`: Use UDP to particular port for tracerouting (instead of increasing the port per each probe), default port is 53
- `-UL`: Use UDPLITE for tracerouting (default dest port is 53)
- `-D --dccp`: Use DCCP Request for tracerouting (default port is 33434)
- `-P prot --protocol=prot`: Use raw packet of protocol prot for tracerouting
- `--back`: Guess the number of hops in the backward path and print if it differs
- `-V --version`: Print version info and exit
- `--help`: Read this help and exit

Argumentos:

- `host`: The host to traceroute to
- `packetlen`: The full packet length (default is the length of an IP header plus 40). Can be ignored or increased to a minimal allowed value

Fonte

- https://www.youtube.com/watch?v=BfHIXNKFu2s&t=58s