Traceroute Command Cheatsheet

A comprehensive guide to using the traceroute command for network troubleshooting, exploring options, interpreting output, and practical usage examples across different operating systems.

Basic Traceroute Usage

Traceroute Overview

Traceroute is a network diagnostic tool used to track the route packets take from your device to a specified destination host. It displays each hop along the path, providing valuable information for network troubleshooting.

It works by sending packets with progressively increasing TTL (Time To Live) values. Routers decrement the TTL, and when it reaches zero, an ICMP 'time exceeded' message is sent back to the source.

Basic Syntax

`traceroute hostname`	Traces the route to the specified hostname or IP address.
`traceroute ip_address`	Traces the route to the specified IP address.

Interpreting Output

Each line in the traceroute output represents a hop. It typically includes the hop number, hostname (if available), IP address, and round-trip times (RTTs) for three probes.

An asterisk (*) indicates a lost packet or a timeout for that probe. Multiple asterisks suggest potential network issues at that hop.

High RTTs indicate latency, which can point to congestion or problems with the network path.

Common Traceroute Options

Linux/macOS Options

`traceroute -m <max_hops> hostname`	Sets the maximum number of hops. Useful to limit the trace length.
`traceroute -n hostname`	Avoids hostname lookups and displays IP addresses only. Speeds up the trace.
`traceroute -q <num_probes> hostname`	Sets the number of probes per hop (default is 3).
`traceroute -I hostname`	Uses ICMP echo requests instead of UDP datagrams (requires root privileges).
`traceroute -T hostname`	Uses TCP SYN packets instead of UDP datagrams. Useful for bypassing firewalls.
`traceroute -w <wait_time> hostname`	Sets the wait time in seconds for a response to a probe (default is 5 seconds).

Windows Options (tracert)

`tracert -h <max_hops> hostname`	Sets the maximum number of hops.
`tracert -d hostname`	Prevents address resolution and displays IP addresses only.
`tracert -w <timeout> hostname`	Sets the timeout value in milliseconds for each reply.
`tracert -4 hostname`	Forces the use of IPv4.
`tracert -6 hostname`	Forces the use of IPv6.

Advanced Traceroute Techniques

TCP Traceroute

Using TCP traceroute (e.g., `traceroute -T` on Linux/macOS) can be useful when ICMP or UDP traffic is blocked by firewalls. It sends TCP SYN packets to a specified port.

Example: `traceroute -T -p 80 google.com` (traces using TCP SYN packets to port 80)

Using Different Protocols

ICMP (`traceroute -I`)	Uses ICMP echo requests, similar to ping, but reveals the path.
UDP (default)	Sends UDP datagrams to high, likely unused ports. Default behavior for traceroute on many systems.

Troubleshooting with Traceroute

Traceroute is invaluable for pinpointing network bottlenecks, identifying failing routers, and diagnosing connectivity issues.

If a traceroute fails to reach the destination, examine the last few hops to identify where the connection is being lost.

Consistently high RTTs at a particular hop suggest a problem with that router or the link to it.

Platform-Specific Considerations

Linux

Most Linux distributions include traceroute by default. If not, it can typically be installed using the distribution's package manager (e.g., `apt install traceroute` on Debian/Ubuntu).

Linux traceroute often requires root privileges for certain options like `-I` (ICMP).

macOS

macOS includes traceroute in the Terminal application. The syntax and options are similar to Linux.

Windows

Windows uses the `tracert` command, which is functionally equivalent to traceroute. The options are slightly different, as detailed in previous sections.

`pathping` is another Windows command that combines `ping` and `traceroute` functionality to provide more detailed network statistics.