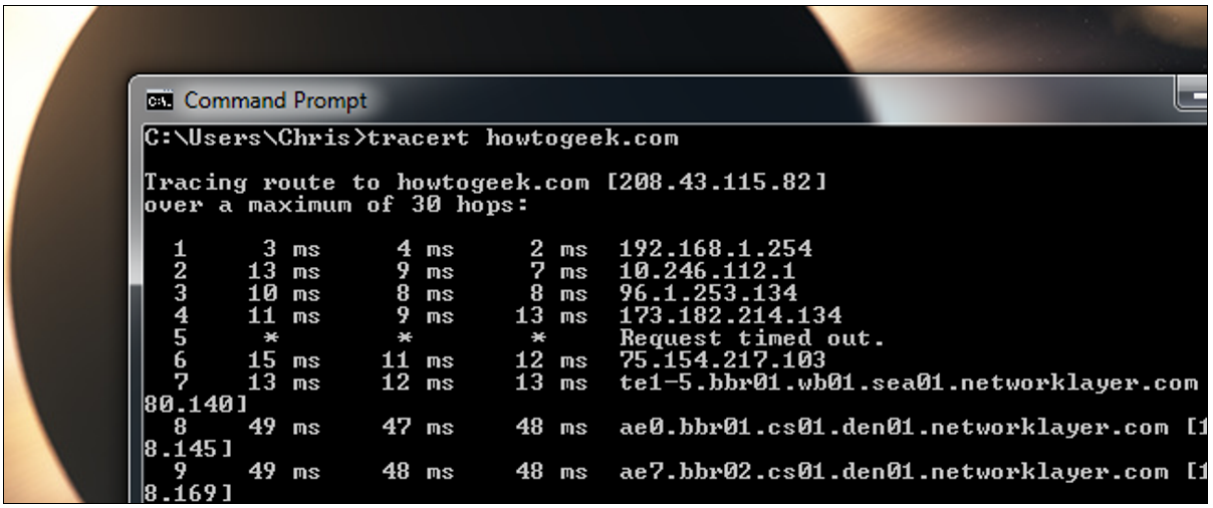
How to Use Traceroute to Identify Network Problems



Traceroute is a command-line tool included with Windows and other operating systems. Along with the ping command, it's an important tool for understanding Internet connection problems, including packet loss and high latency. If you're having trouble connecting to a website, traceroute can tell you where the problem is. It can also help visualise the path traffic takes between your computer and a web server.

How Traceroute Works

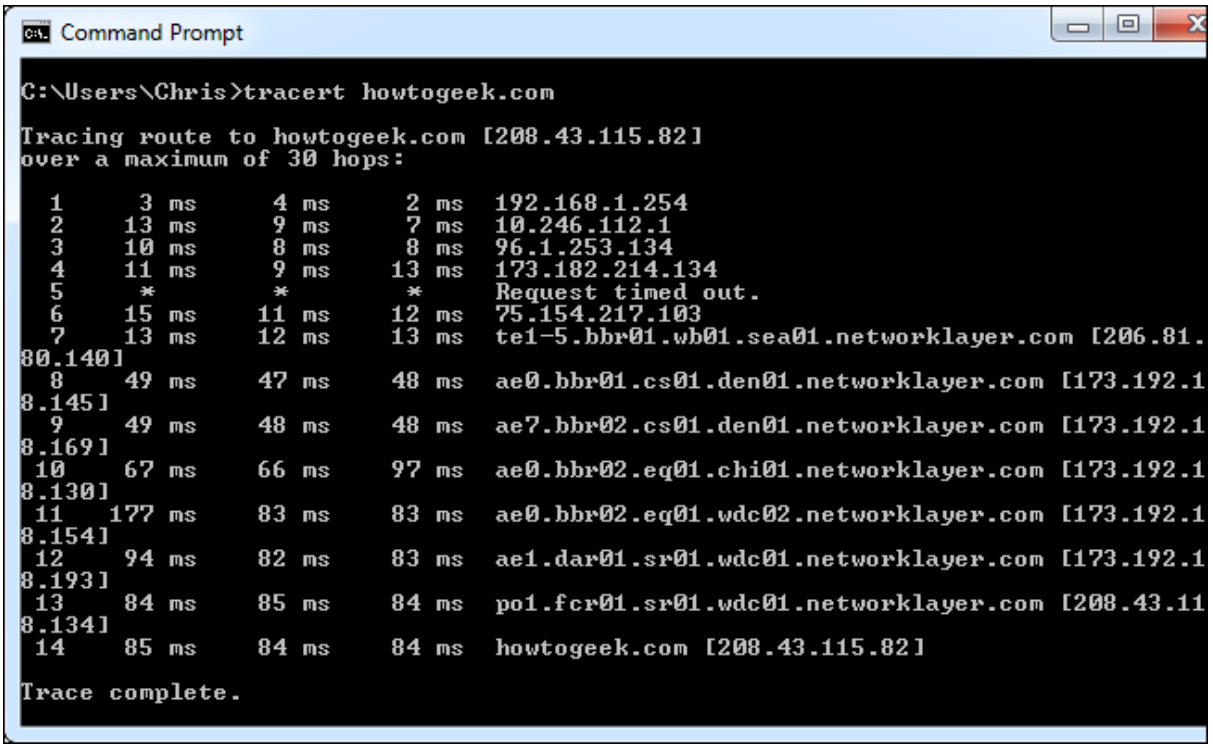
- When you connect to a website – say, howtogeek.com – the traffic has to go through several intermediaries before reaching the website. The traffic goes through your local router, your Internet service provider's routers, onto larger networks, and so on.
- Traceroute shows us the path traffic takes to reach the website. It also displays the delays that occur at each stop. If you're having issues reaching a website and that website is working properly, it's possible there's a problem somewhere on the path between your computer and the website's servers. Traceroute would show you where that problem is.
- In more technical terms, traceroute sends a sequence of packets using the ICMP protocol (the same protocol used for the ping command.) The first packet has a time-to-live (also known as TTL, or hop limit) of 1, the second packet has a TTL of 2, and so on. Each time a packet is passed to a new router, the TTL is decreased by 1. When it reaches 0, the packet is discarded and the router returns an error message. By sending packets in this manner, traceroute ensures that each router in the path will discard a packet and send a response.

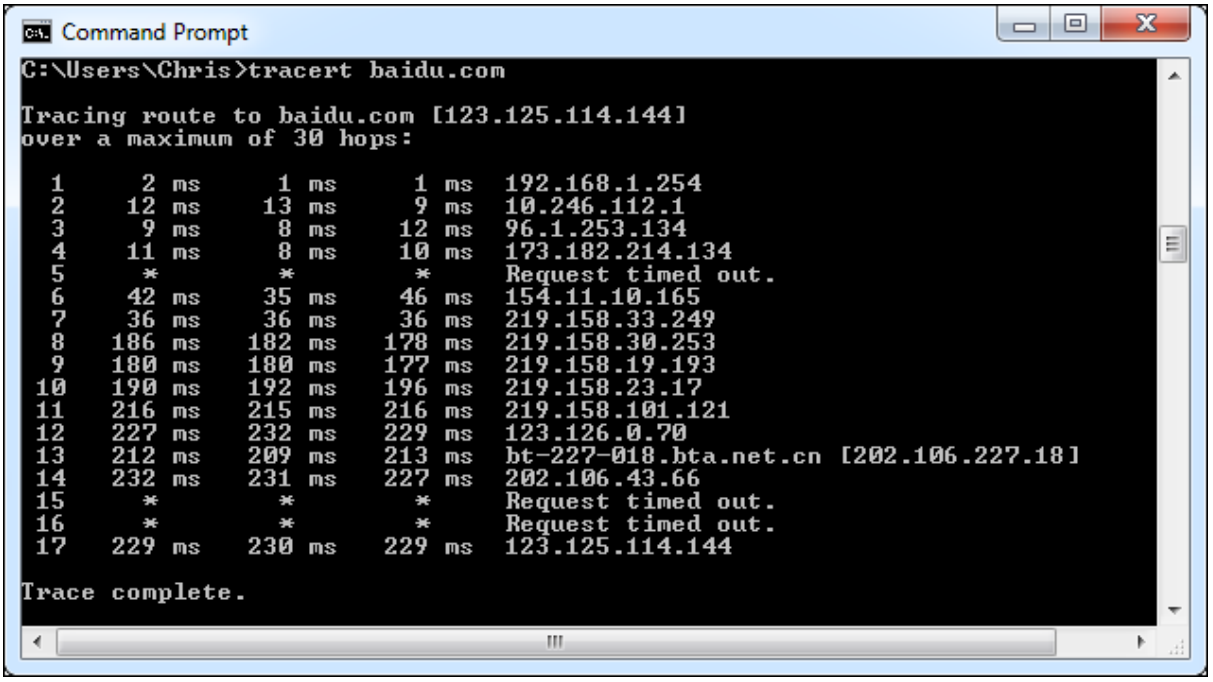
How to Use Traceroute

Traceroute is run from a command prompt or terminal window. On Windows, press the Windows key, type Command Prompt, and press Enter to launch one.To run a traceroute, run the tracert command followed by the address of a website. For example, if you wanted to run a traceroute on How-To Geek, you'd run the command:

```
tracert howtogeek.com
```

You'll gradually see the route take form as your computer receives responses from the routers along the way.





Understanding the Output

The basic idea is self-explanatory. The first line represents your home router (assuming you're behind a router), the next lines represent your ISP, and each line further down represents a router that's further away.

The format of each line is as follows:

Hop RTT1 RTT2 RTT3 Domain Name [IP Address]

- Hop: Whenever a packet is passed between a router, this is referred to as a "hop." For example, in the output above, we can see that it takes 14 hops to reach How-To Geek's servers from my current location.
- RTT1, RTT2, RTT3: This is the round-trip time that it takes for a packet to get to a hop and back to your computer (in milliseconds). This is often referred to as latency, and is the same number you see when using ping. Traceroute sends three packets to each hop and displays each time, so you have some idea of how consistent (or inconsistent) the latency is. If you see a * in some columns, you didn't receive a response – which could indicate packet loss.
- Domain Name [IP Address]: The domain name, if available, can often help you see the location of a router. If this isn't available, only the IP address of the router is displayed.