

How To Perform A Trace Route

Trace route (*tracert*) works by sending a packet to an open UDP port on a destination machine. For the initial three packets, trace route sets the TTL (see explanation of TTL) to 1 and releases the packet. The packet then gets transferred to the first router (completing the first hop), and the TTL gets decremented by the router from 1 to 0. The router then discards the packet and sends off an ICMP notification packet to the original host with the message that the TTL expired from the router. This tells *tracert* what the first hop is and how long it takes to get there. Traceroute repeats this, gradually incrementing the TTL until a path to the remote host is traced and it gets back an ICMP Port Unreachable message, indicating that the remote host has been reached.

Response times may vary dramatically because the packet is crossing long distances, other times the increases come from network congestion.

For Example:

```
C:> tracert www.linux.org
or
C:> tracert 198.182.196.56
```

will show:

```
Tracing route to www.linux.org [198.182.196.56]
over a maximum of 30 hops:
```

```
 1 <10 ms <10 ms <10 ms mn-bldg-rtr-vlan200-3.gw.more.net [207.160.133.254]
 2 <10 ms <10 ms <10 ms co-r12-01-atm0-0-10.mo.more.net [150.199.11.1]
 3 <10 ms 10 ms <10 ms kc-r12-01-atm1-0-131.mo.more.net [150.199.7.198]
 4 <10 ms 10 ms <10 ms bb2-g8-0.kscymo.swbell.net [151.164.8.247]
 5 <10 ms 10 ms 10 ms sl-gw9-kc-2-0.sprintlink.net [160.81.18.233]
 6 * * *
 7 50 ms 61 ms 60 ms 198.ATM7-0.XR2.TOR2.ALTER.NET [152.63.128.53]
 8 50 ms 60 ms 60 ms 194.ATM7-0.GW1.TOR2.ALTER.NET [152.63.128.101]
 9 50 ms 70 ms 60 ms att2-gw.customer.alter.net [157.130.159.82]
10 61 ms 60 ms 60 ms pos5-0-0.hcap1-ott.bb.attcanada.ca [216.191.225.2]
11 60 ms 70 ms 70 ms 216.191.132.150
12 60 ms 81 ms 70 ms router.invlogic.com [207.245.34.122]
13 70 ms 70 ms 80 ms www.linux.org [198.182.196.56]
Trace complete.
```

Note the asterisks on line six. This can indicate that a response wasn't received. Some routers do not issue TTL-expired ICMP messages.

How to use Traceroute

Windows

Traceroute can be accessed at a DOS or command prompt. An Internet connection must already be established.

1. Click on Start > Programs > DOS Prompt (Windows 95-98) or Command Prompt (NT). In a Windows 2000 or XP environment, click on Start > Run. Type command into the dialog box, then click OK.
2. In the resulting command line window, type *tracert* hostname, where hostname can be a domain name, a machine name or an IP address.
3. Press Enter.

For example:

```
C:> tracert www.emints.more.net
```

Mac OS X

1. Double-click the Hard Drive icon > Applications folder > Utilities folder > Network Utility program.
2. Select the Traceroute tab and enter the hostname, where hostname can be a domain name, a machine name or an IP address.
3. Press Enter.