Traceroute

The tracert command is used to visually see a network packet being sent and received and the amount of hops required for that packet to get to its destination.

In this example we will simply trace the path to the remote host. We do not provide any option. Before command the hostname will be resolved as expected. In this example we will trace route to the google.com

```
C:\>tracert google.com

Tracing route to google.com [216.58.214.206]
over a maximum of 30 hops:

  1      3 ms      1 ms     <1 ms   192.168.122.1
  2      1 ms      1 ms      2 ms   myhome.mynet [192.168.1.1]
  3      3 ms      7 ms      3 ms   93.155.2.38
  4      3 ms      2 ms      6 ms   81.212.107.149
```

Do Not Resolve Hostname

tracert will resolve dns of all intermediate hops. This will caouse slowness of the operation. We can prevent tracert to resolve the dns of intermediate hosts with -d .

```
C:\>tracert -d  google.com

Tracing route to google.com [216.58.214.206]
over a maximum of 30 hops:

  1     <1 ms     <1 ms     <1 ms   192.168.122.1
  2      1 ms      1 ms      1 ms   192.168.1.1
  3     65 ms     65 ms     48 ms   93.155.2.38
  4      2 ms      2 ms      3 ms   81.212.107.149
  5      4 ms      5 ms      3 ms   195.175.169.180
```

Force IPv4

Sometimes if IPv6 is available it may be preferred automatically. We can prevent to trace the path with traceroute using IPv6. We will use -4 option to force IPv4 address usage.

> tracert -4 google.com

Force IPv6

if IPv4 is available it may be preferred automatically. We can prevent to trace the path with traceroute using IPv4. We will use -6 option to force IPv6 address usage.

> tracert -6 google.com

Set Maximum Hop Count

As we know IP networks or internet consist of mesh like systems and stations that connects each other. tracert will send packets hop by hop. We can set maximum hop count with -h . After specified number of hops tracert will stop.

```
C:\>tracert -h 4  google.com

Tracing route to google.com [216.58.214.238]
over a maximum of 4 hops:

  1      7 ms     <1 ms     <1 ms   192.168.122.1
  2      1 ms      1 ms       *      myhome.mynet [192.168.1.1]
  3      3 ms      2 ms      7 ms   93.155.2.38
  4      3 ms      2 ms      3 ms   81.212.107.149

Trace complete.
```

Using Tracert Options

To use tracert, be aware of a few options you can use with it. The most helpful is the first one. Using the –d option is always helpful when you want to remove DNS resolution. Name servers are helpful, but if not available or if incorrectly set or if you simply just want the IP address of the host, use the –d option.

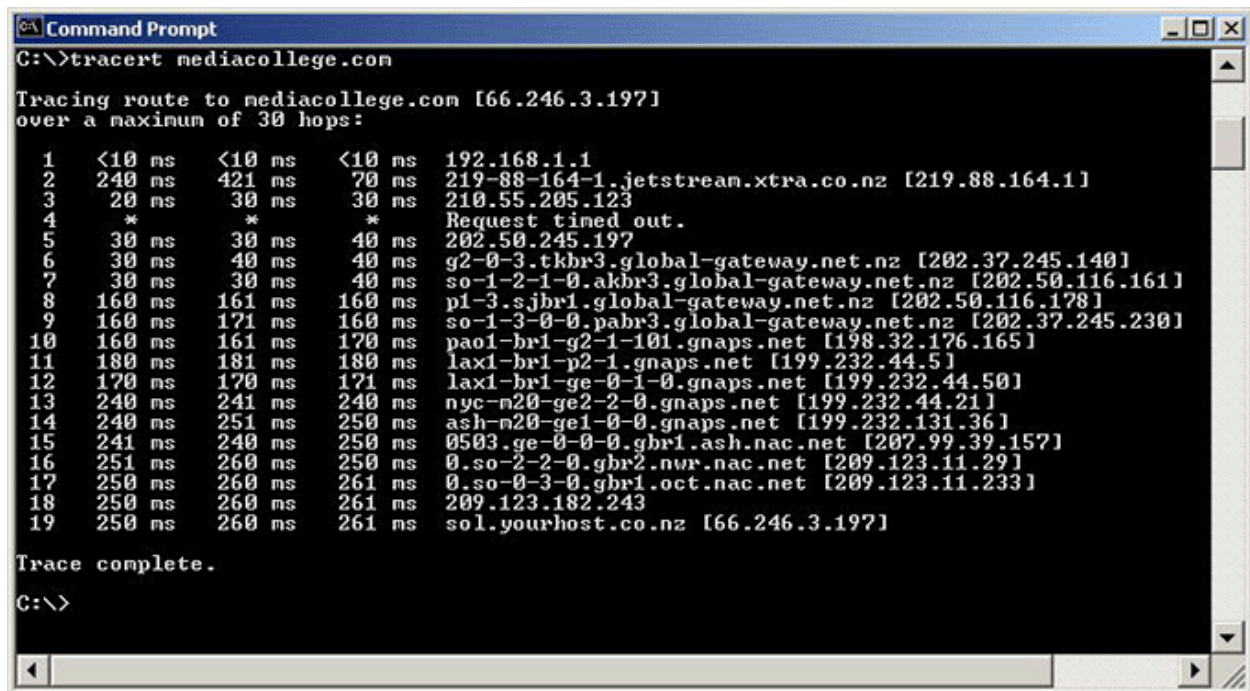|	
-d	Prevents tracert from attempting to resolve the IP addresses of intermediate routers to their names. This can speed up the display of tracert results
-h	Specifies the maximum number of hops in the path to search for the target (destination). The default is 30 hops
-j	You can use this with a host list (HostList). Specifies that Echo Request messages use the Loose Source Route option in the IP header with the set of intermediate destinations specified in HostList. With loose source routing, successive intermediate destinations can be separated by one or multiple routers. The maximum number of addresses or names in the host list is 9. The HostList is a series of IP addresses (in dotted decimal notation) separated by spaces.
-w	Specifies the amount of time in milliseconds to wait for the ICMP Time Exceeded or Echo Reply message corresponding to a given Echo Request message to be received. If not received within the time-out, an asterisk (*) is displayed. The default time-out is 4000 (4 seconds)
-?	Displays help at the command prompt.

tracert [-d] [-h MaximumHops] [-j HostList] [-w Timeout] [TargetName]

How to Use the Traceroute Command

Traceroute is a command which can show you the path a packet of information takes from your computer to one you specify. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded. In addition to this, it will tell you how long each 'hop' from router to router takes.

Enter the word tracert, followed by a space, then the domain name.

The following is a successful traceroute from a home computer in New Zealand to mediacollege.com:

Firstly it tells you that it's tracing the route to mediacollege.com, tells you the IP address of that domain, and what the maximum number of hops will be before it times out.

Next it gives information about each router it passes through on the way to its destination.

1 is the internet gateway on the network this traceroute was done from (an ADSL modem in this case)

2 is the ISP the origin computer is connected to (xtra.co.nz)

3 is also in the xtra network

4 timed out

5 - 9 are all routers on the global-gateway.net.nz network (the domain that is the internet gateway out of New Zealand)

10 - 14 are all gnaps.net in the USA (a telecom supplier in the USA)

15 - 17 are on the nac network (Net Access Corporation, an ISP in the New York area)

18 is a router on the network mediacollege.com is hosted on

and finally, line 19 is the computer mediacollege.com is hosted on (sol.yourhost.co.nz)

Each of the 3 columns are a response from that router, and how long it took (each hop is tested 3 times). For example, in line 2, the first try took 240ms (240 milliseconds), the second took 421 ms, and the third took 70ms.

You will notice that line 4 'timed out', that is, there was no response from the router, so another one was tried (202.50.245.197) which was successful.

You will also notice that the time it took quadrupled while passing through the global-gateway network.

This is extremely useful when trying to find out why a website is unreachable, as you will be able to see where the connection fails. If you have a website hosted somewhere, it would be a good idea to do a traceroute to it when it is working, so that when it fails, you can do another traceroute to it (which will probably time out if the website is unreachable) and compare them. Be aware though, that it will probably take a different route each time, but the networks it passes through will generally be very similar.

If the example above had continued to time out after line 9, you could suspect that global-gateway.co.nz was the problem, and not mediacollege.com.

If it timed out after line 1, you would know there was a problem connecting to your ISP (in this case you would not be able to access anything on the internet).

It is generally recommended that if you have a website that is unreachable, you should use both the traceroute and ping commands before you contact your ISP to complain. More often that not, there will be nothing to your ISP or hosting company can do about it.