Tracert Command

Lab Objective:

Learn how to use the tracert command and its switches.

Lab Purpose:

Tracert is one of many commands line tools you can use to troubleshoot network issues.

On Cisco and Unix-type devices you would use the 'traceroute' command, but on Windows it's 'tracert'.

Bear in mind that firewalls, access lists, and load balancers can all affect the output of the command.
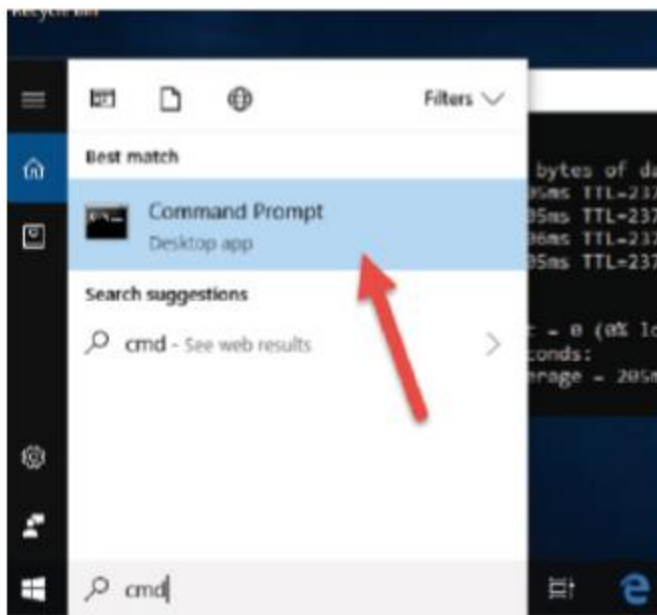
Lab Tool:

Any Windows PC

Lab Topology:

Please use the following topology to complete this lab exercise. You can use any Windows computer you have available.

Lab Walkthrough:

Task 1:

Pull up a command prompt by typing 'cmd' into the search box.

Task 2:

At the command prompt issue, the 'tracert /?' command. Check your study guide for more information on all the available switches.


```
C:\Users\paulw>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.

C:\Users\paulw>_
```

Task 3:

Issue a 'tracert cisco.com' command. Note that your hops will differ from mine! The output pushed the command off the screen, but I entered it at the start.

```
■ Command Prompt                                                                              -

1    <1 ms    <1 ms    <1 ms   10.0.2.2
2  1851 ns      1 ms     1 ms   www.routerlogin.com [192.168.0.1]
3    22 ms     23 ms    22 ms   172.18.212.11
4      *       23 ms    22 ms   172.18.69.141
5    24 ms     32 ms    25 ms   bundle-ether4.woo-edge902.brisbane.telstra.net [203.50.44.42]
6    29 ms     24 ms    25 ms   bundle-ether6.woo-core1.brisbane.telstra.net [203.50.11.138]
7    35 ns     37 ms   134 ms   bundle-ether20.chw-core10.sydney.telstra.net [203.50.11.180]
8    40 ns     37 ms    38 ms   bundle-ether1.oxf-gw11.sydney.telstra.net [203.50.6.93]
9      *         *      44 ms   bundle-ether1.sydo-core03.sydney.reach.com [203.50.13.98]
10   50 ms     44 ms    44 ms   i-0-1-0-15.sydo-core04.bi.telstraglobal.net [202.84.222.54]
11     *         *     174 ms   i-10604.1wlt-core02.telstraglobal.net [202.84.141.225]
12     *         *     173 ms   i-93.tlot02.bi.telstraglobal.net [202.84.253.86]
13  276 ms    179 ms   172 ms   l3-peer.tlot02.pr.telstraglobal.net [134.159.61.46]
14     *         *     203 ms   ae-4-15.edge5.Dallas3.Level3.net [4.69.208.233]
15  204 ms    211 ms   237 ms   CISCO-SYSTE.edge5.Dallas3.Level3.net [4.59.34.66]
16  204 ms    205 ms   214 ms   rcdn9-cd1-dmzbb-gw1-ten1-1.cisco.com [72.163.0.5]
17  210 ns    221 ms   226 ms   rcdn9-cd1-dmzdcc-gw1-por1.cisco.com [72.163.0.178]
18  211 ms    219 ms   213 ms   rcdn9-16b-dcz05n-gw2-por1.cisco.com [72.163.2.102]
19  240 ms    205 ms   206 ms   redirect-ns.cisco.com [72.163.4.185]

Trace complete.
```

Task 4:

Note which addresses are private. Note when the trace leaves your home network and reaches your ISP.

Note that each hop is tested three times and the output is in milliseconds.

Note any drops, as indicated by asterisk (*). With three * markets the packet may fail, or an alternative route may be found.

Note the big leap in delay at step 11.

Notes:

Test the various switches available. Also, ping using just an website IP address. Note also that there is a DNS lookup for the IP address associated with the hostname before the tracert command can execute.