# Experiment 02: Study the use of network reconnaissance tools/commands ping, traceroute, whois to gather information about network and domain registors.

**Learning Objective:** Implement and design of Diffie-Hellman Algorithm

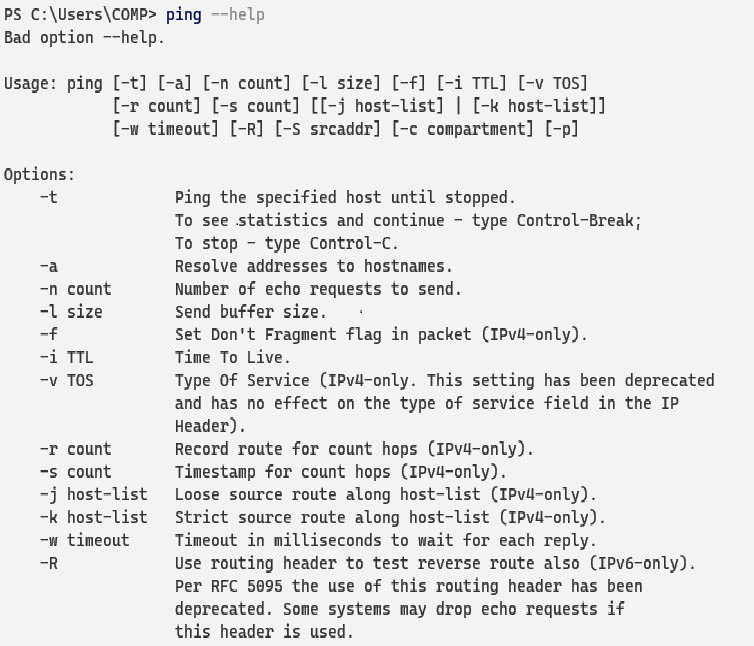
**Tools:** Command Prompt

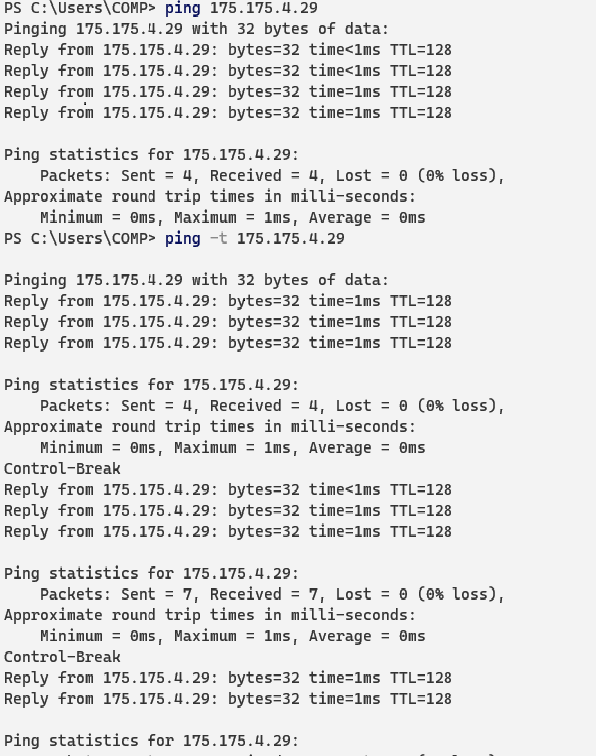
**Theory:**

Ping command:

Verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) echo Request messages. The receipt of corresponding echo Reply messages are displayed, along with round-trip times. ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution. Used without parameters, this command displays Help content.

You can also use this command to test both the computer name and the IP address of the computer. If pinging the IP address is successful, but pinging the computer name isn't, you might have a name resolution problem. In this case, make sure the computer name you are specifying can be resolved through the local Hosts file, by using Domain Name System (DNS) queries, or through NetBIOS name resolution techniques.





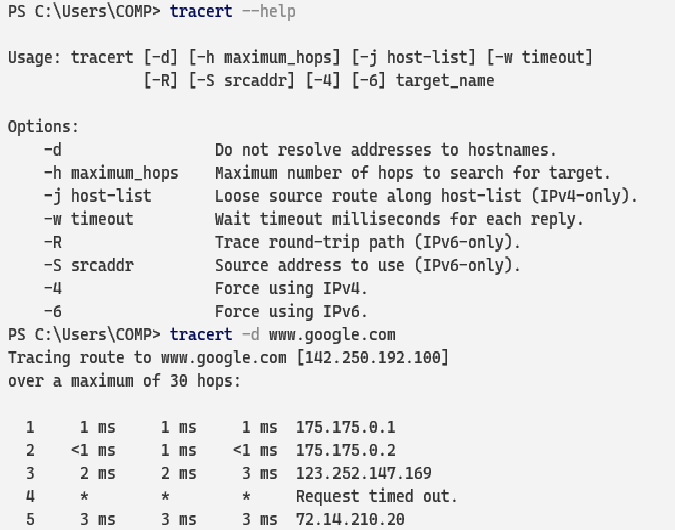
Tracert command:

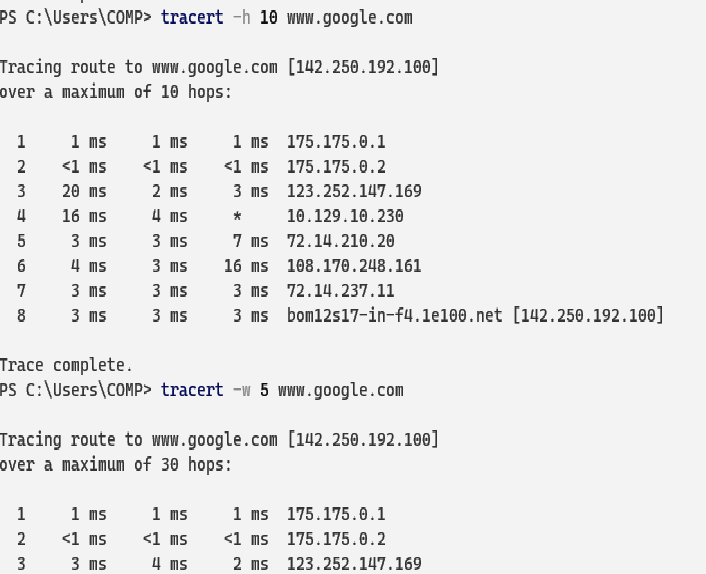
This diagnostic tool determines the path taken to a destination by sending Internet Control Message Protocol (ICMP) echo Request or ICMPv6 messages to the destination with incrementally increasing time to live (TTL) field values. Each router along the path is required to decrement the TTL in an IP packet by at least 1 before forwarding it. Effectively, the TTL is a maximum link counter. When the TTL on a packet reaches 0, the router is expected to return an ICMP time Exceeded message to the source computer.

This command determines the path by sending the first echo Request message with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum number of hops is reached. The maximum number of hops is 30 by default and can be specified using the /h parameter.

The path is determined by examining the ICMP time Exceeded messages returned by intermediate routers and the echo Reply message returned by the destination. However, some routers do not return time Exceeded messages for packets with expired TTL values and are invisible to the tracert command. In this case, a row of asterisks (\*) is displayed for that hop. The path displayed is the list of near/side router interfaces of the routers in the path between a source host and a destination. The near/side interface is the interface of the router that is closest to the sending host in the path.

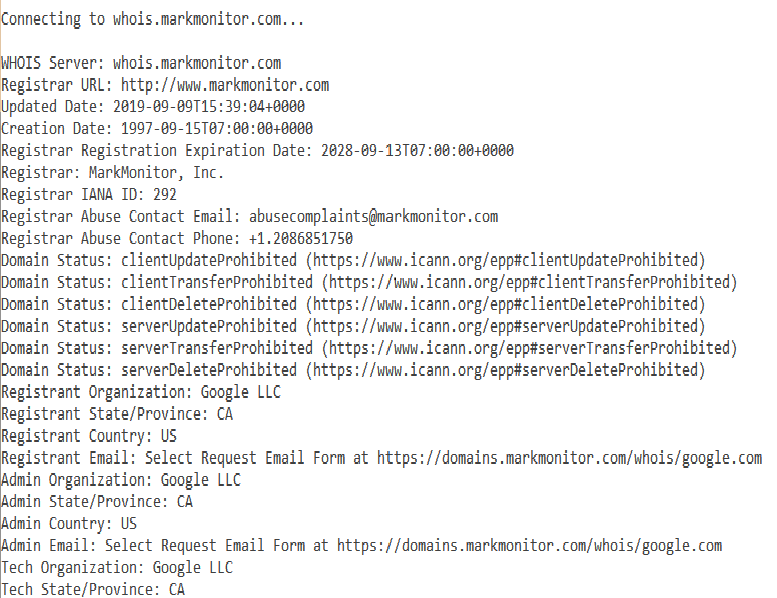






Whois command:

The whois command tries to reach ARPANET host internic.net where it examines a user-name database to obtain information. The whois command should be used only by users on ARPANET. Refer to RFC 812 for more complete information and recent changes to the whois command.





**Conclusion:** After performing the experiment I was able to use of network reconnaissance tools/commands ping, traceroute, whois to gather information about network and domain registors.

For Faculty Use

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Correction Parameters** | **Formative Assessment [40%]** | **Timely completion of Practical [ 40%]** | **Attendance / Learning Attitude [20%]** | **Total** |
| **Marks Obtained** |  |  |  |  |