EXPERIMENT NO.2

TITLE: Simulating various Networks (LAN, WAN).

OBJECTIVE: To Simulate and test basic command line operation with Linux operating system andnetwork configuration, testing and verification.

AIM: To test Networking commands a) Ping b) ipconfig / ifconfig c) Host name d) Netstat f) Tracert /Traceroute / Tracepath g) NSlookup.

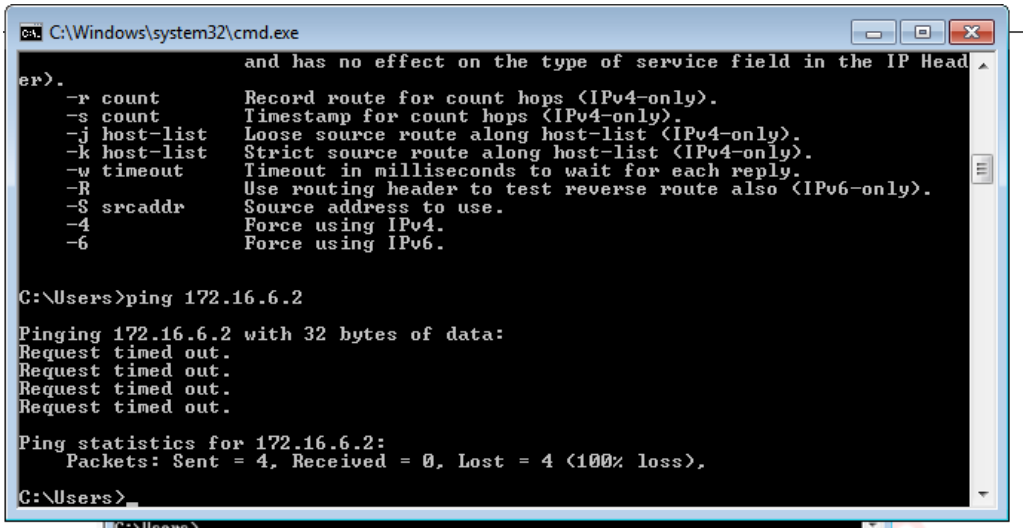
SOFTWARE USED: command Prompt, Cisco packet Tracer 6.2

Theory:

1. Ping

The ping command sends an echo request to a host available on the network. Using this command, you can check if your remote host is responding well or not. Tracking and isolating hardware and software problems. Determining the status of the network and various foreign hosts. The ping command is usually used as a simple way to verify that a computer can communicate over the network with another computer or network device. The ping command operates by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination computer and waiting for a response

ping172.16.6.2



2. IPConfig

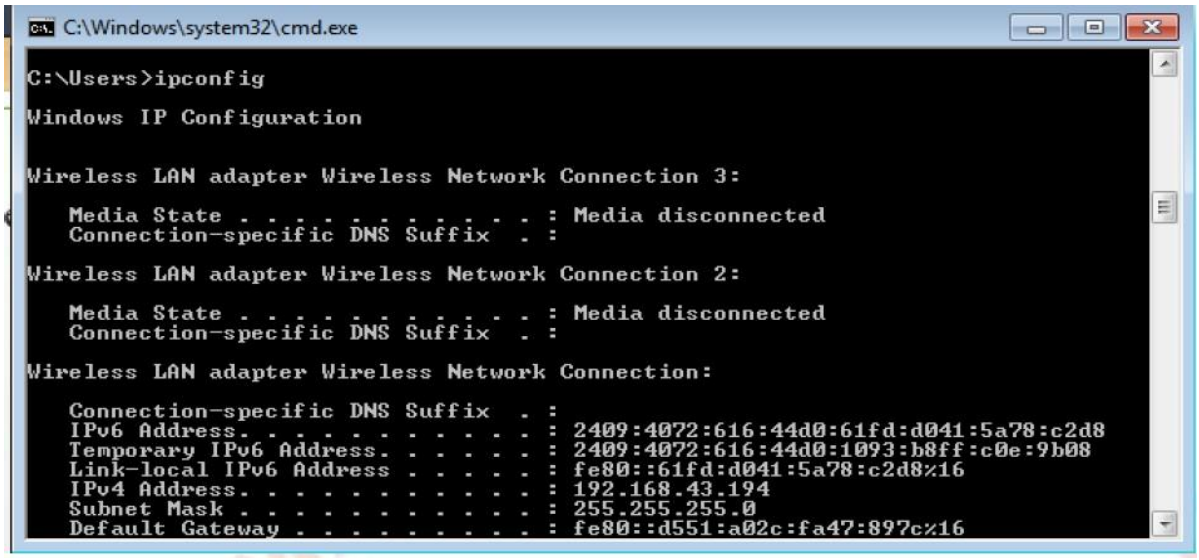
The IPConfig command is one of the more useful basic Windows network commands everyone should know and use to troubleshoot problems. The IPConfig command displays basic IP address configuration information for the Windows device you are working on. In fact, the command will display information for every network adapter that has ever been installed on your Windows 10 computer.

To run the basic command, at the prompt type:

ipconfig

The general information includes IP Addresses for both IPv4 and IPv6, the Default Gateway, and theSubnet Mask. Adding the parameter /all to the command will display DNS Server information and details concerning IP Address leases.

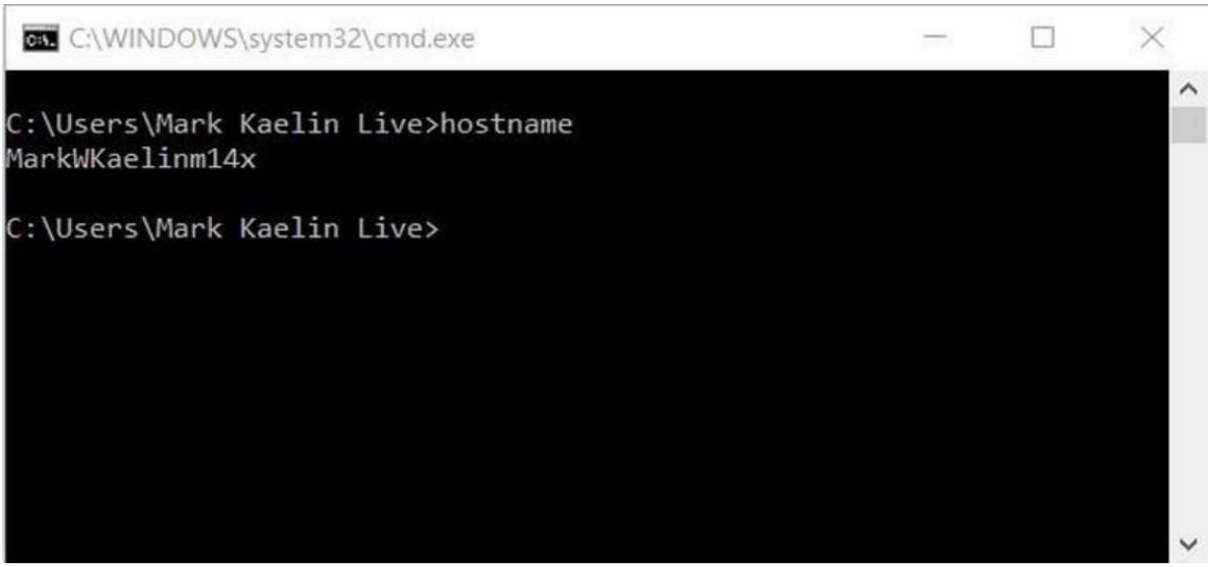
Check out Microsoft Docs for a more advanced look at the IP Config command and its variables andswitches.



3. HostName

The Windows 10 HostName network command will simply display the current name of yourWindows 10 computer (**Figure B**). This is the name your computer uses to identify itself to the otherdevices and servers on your local network. You can find this name in the System information screen in the GUI, but this command is quicker.

Figure B



To run the basic command, at the prompt type:

5. Trace route:

Traceroute uses Internet Control Message Protocol (ICMP) echo packets with variable time to live (TTL) values. The response time of each hop is calculated. To guarantee accuracy, each hop is queried multiple times (usually three times) to better measure the response of that particular hop.

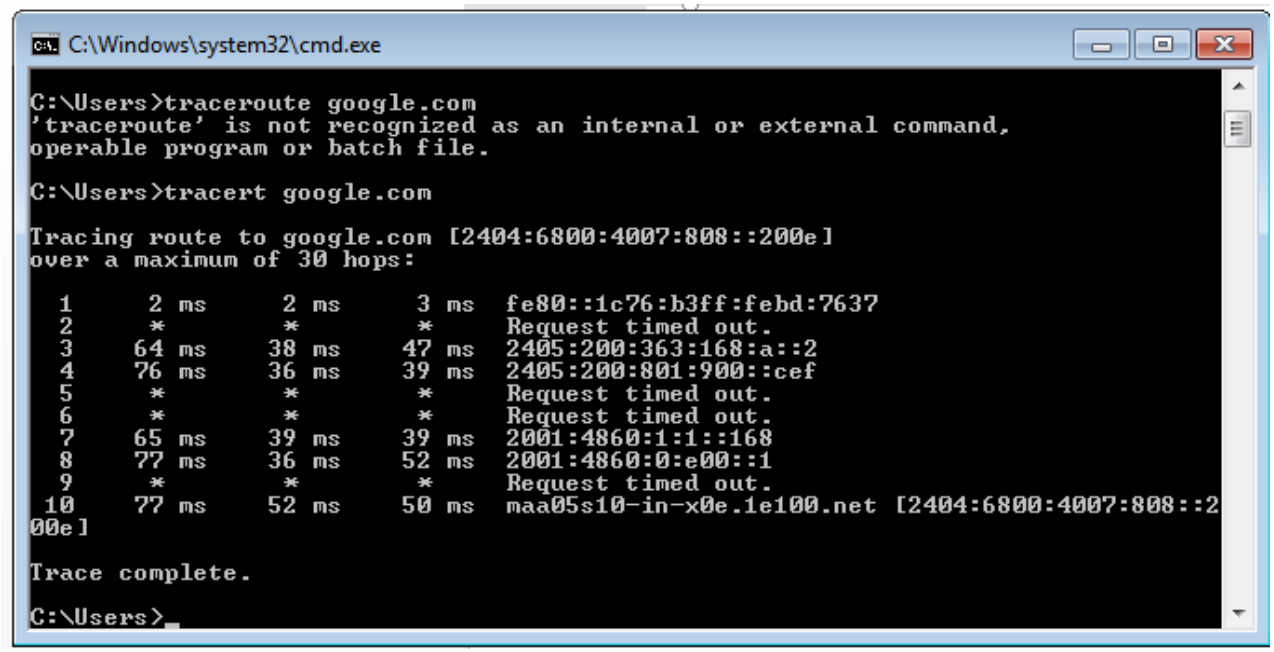
Traceroute is a network diagnostic tool used to track the pathway taken by a packet on an IP networkfrom source to destination. Traceroute also records the time taken for each hop the packet makes during its route to the destination. Traceroute uses Internet Control Message Protocol (ICMP) echo packets with variable time to live (TTL) values.

The response time of each hop is calculated. To guarantee accuracy, each hop is queried multiple times (usually three times) to better measure the response of that particular hop. Traceroute sends packets with TTL values that gradually increase

from packet to packet, starting with TTL value of

one. Routers decrement TTL values of packets by one when routing and discard packets whose TTL value has reached zero, returning the ICMP error message ICMP Time Exceeded. For the first set of packets, the first router receives the packet, decrements the TTL value and drops the packet because it then has TTL value zero. The router sends an ICMP Time Exceeded message back to the source. The next set of packets are given a TTL value of two, so the first router forwards the packets, but thesecond router drops them and replies with ICMP Time Exceeded.

Proceeding in this way, traceroute uses the returned ICMP Time Exceeded messages to build a list ofrouters that packets traverse, until the destination is reached and returns an ICMP Echo
Reply message. With the tracert command shown above, we're asking tracert to show us the pathfrom the local computer all the way to the network device with the hostname
www.google.co
m. #tracert
google.com

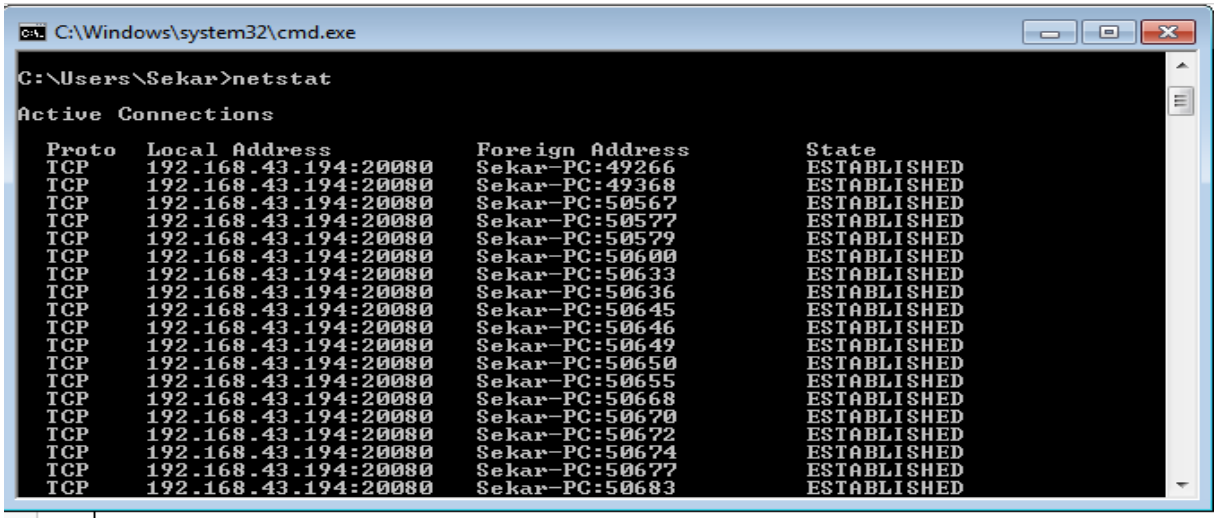


6.Netstat

Netstat is a common command line TCP/IP networking available in most versions of

Windows, Linux, UNIX and other operating systems. Netstat provides information and statistics about protocols in use and current TCP/IP network connections. The Windows help screen (analogous to a Linux or UNIX for netstat reads as follows:

displays protocol statistics and current TCP/IP network connections.#netstat

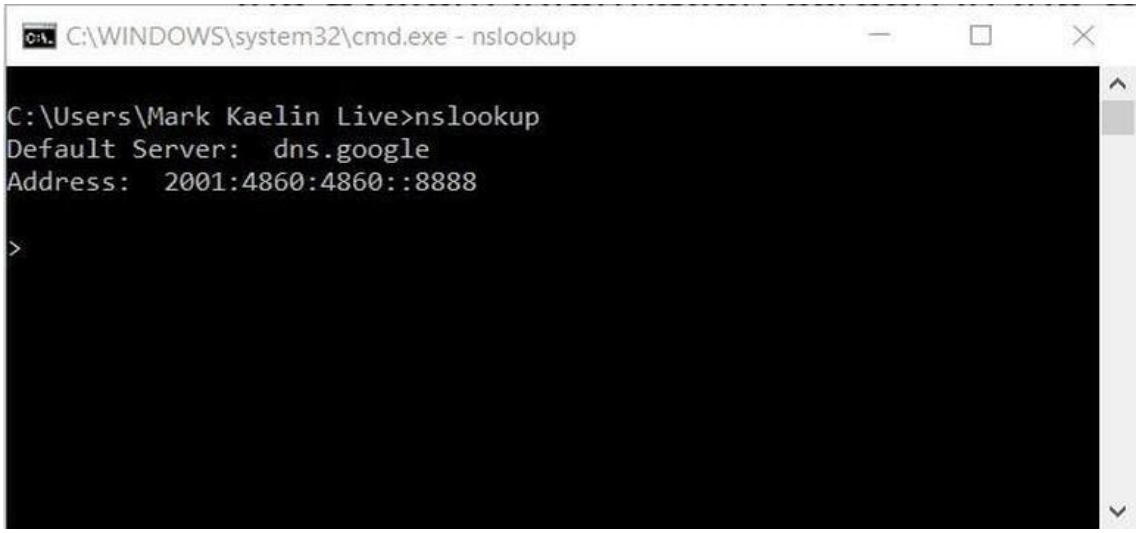


7. nslookup

The **nslookup** (which stands for *name server lookup*) command is a network utility program used to obtain information about internet servers. It finds name server information for domains by querying the Domain Name System.

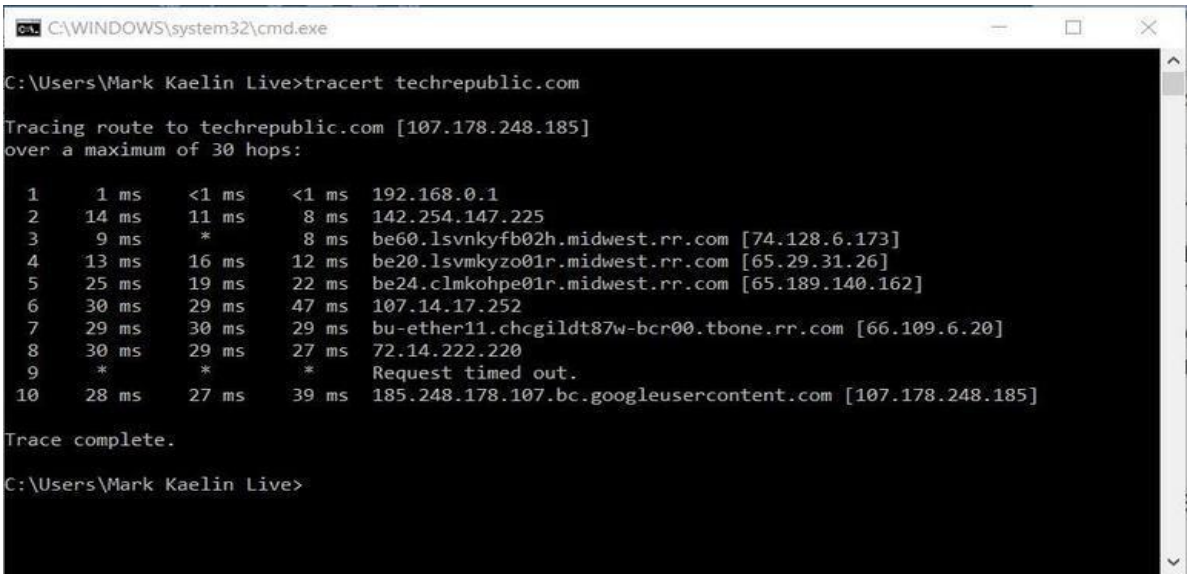
The nslookup command is a powerful tool for diagnosing DNS problems. You know you'reexperiencing a DNS problem when you can access a resource by specifying its IP address but not its DNS name.

#nslookup



8. Tracert

Another handy tool for troubleshooting network connections in Windows 10 is the Tracert command. This command will trace the route a data packet takes before reaching its destination, displaying information on each hop along the route. Each hop of the route will display the latency between your device and that particular hop and the IP address of the hop.



Conclusion: