

## EXPERIMENT NO.2

**TITLE:** Simulating various Networks (LAN, WAN).

**OBJECTIVE:** To Simulate and test basic command line operation with Linux operating system and network 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.

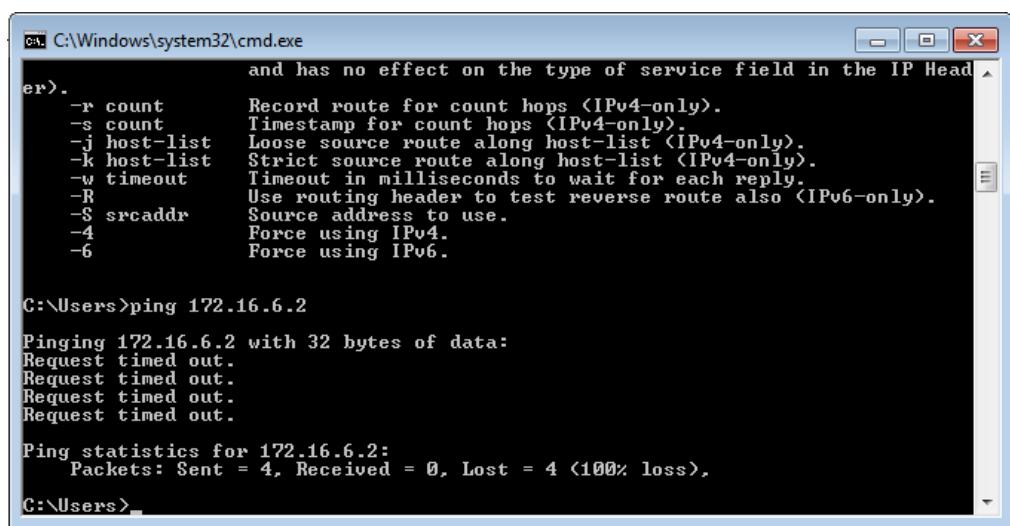
**SOFTWARE USED:** command Prompt, Cisco packet Tracer 6.2

### 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
```



A screenshot of a Windows Command Prompt window titled 'C:\Windows\system32\cmd.exe'. The window displays the help documentation for the 'ping' command, followed by the execution of 'ping 172.16.6.2'. The output shows four failed attempts ('Request timed out.') before providing statistics for the successful attempt.

```
and has no effect on the type of service field in the IP Header.
er>.
-r count      Record route for count hops <IPv4-only>.
-s count      Timestamp for count hops <IPv4-only>.
-j host-list  Loose source route along host-list <IPv4-only>.
-k host-list  Strict source route along host-list <IPv4-only>.
-w timeout    Timeout in milliseconds to wait for each reply.
-R            Use routing header to test reverse route also <IPv6-only>.
-S srcaddr    Source address to use.
-4            Force using IPv4.
-6            Force using IPv6.

C:\Users>ping 172.16.6.2
Pinging 172.16.6.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.6.2:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users>
```

## 2. IPConfig

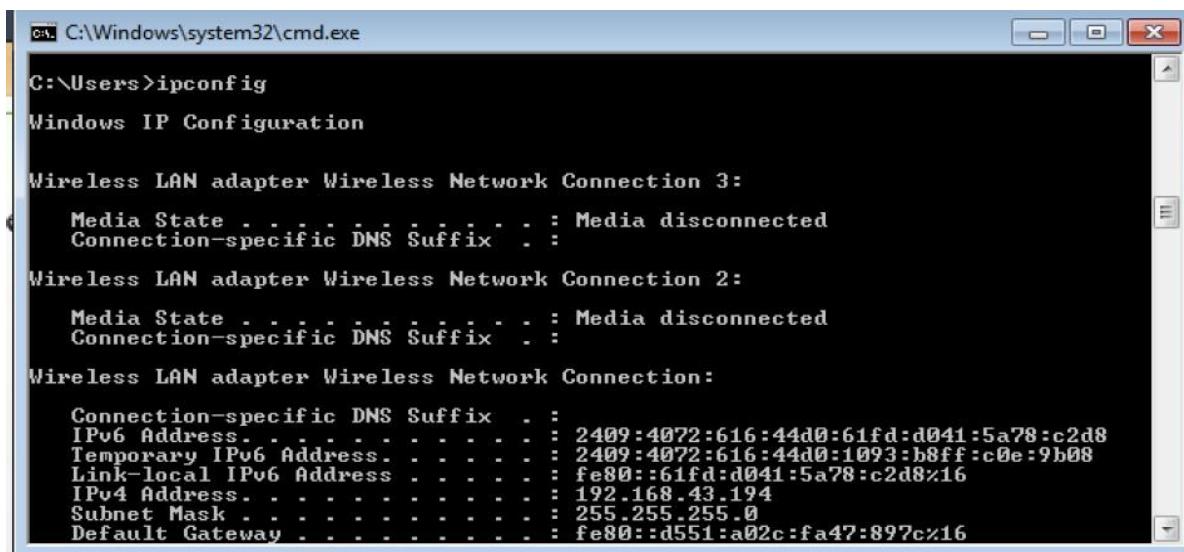
The IPConfig command is one of the more useful basic Windows network commands everyone should know and use to troubleshoot problems. The IPConfig command displays basic IP address configuration information for the Windows device you are working on. In fact, the command will display information for every 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 the Subnet 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 and switches.



A screenshot of a Windows Command Prompt window titled 'cmd C:\Windows\system32\cmd.exe'. The window shows the output of the 'ipconfig' command. The output includes information for three network adapters: 'Wireless LAN adapter Wireless Network Connection 3', 'Wireless LAN adapter Wireless Network Connection 2', and 'Wireless LAN adapter Wireless Network Connection'. For each adapter, it shows the Media State (Media disconnected), Connection-specific DNS Suffix, and various IPv4 and IPv6 addresses, subnet masks, and default gateways. The window has a standard Windows title bar and scroll bars on the right side.

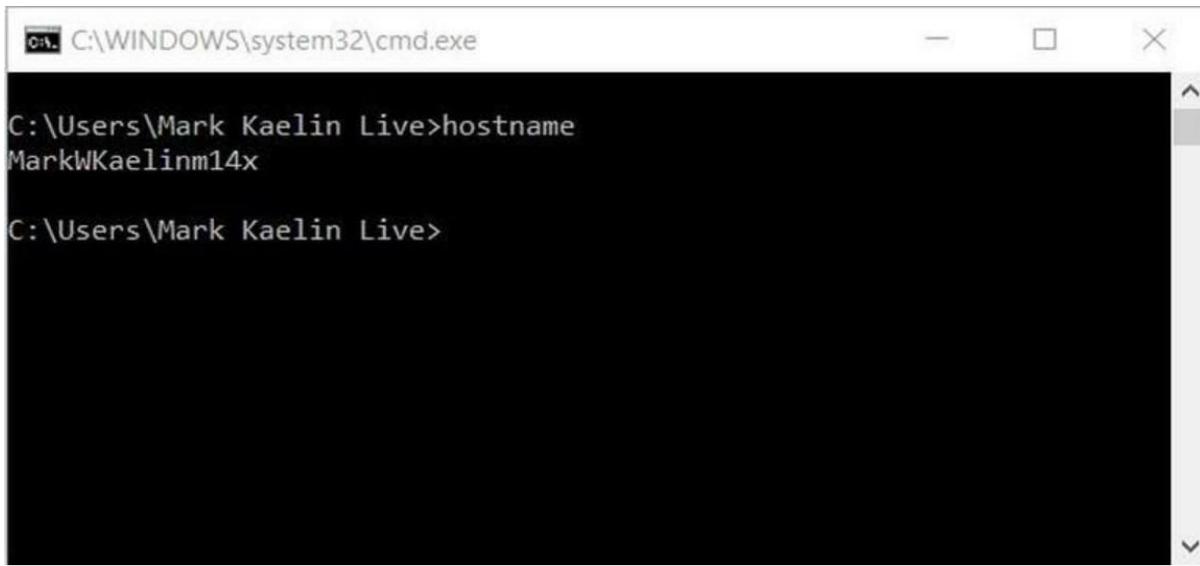
```
C:\Users>ipconfig
Windows IP Configuration

Wireless LAN adapter Wireless Network Connection 3:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
Wireless LAN adapter Wireless Network Connection 2:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
Wireless LAN adapter Wireless Network Connection:
  Connection-specific DNS Suffix . . . . . :
  IPv6 Address . . . . . : 2409:4072:616:44d0:61fd:d041:5a78:c2d8
  Temporary IPv6 Address . . . . . : 2409:4072:616:44d0:1093:b8ff:c0e:9b08
  Link-local IPv6 Address . . . . . : fe80::61fd:d041:5a78:c2d8%16
  IPv4 Address . . . . . : 192.168.43.194
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : fe80::d551:a02c:fa47:897c%16
```

### 3. HostName

The Windows 10 HostName network command will simply display the current name of your Windows 10 computer (**Figure B**). This is the name your computer uses to identify itself to the other devices 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**



A screenshot of a Windows Command Prompt window titled 'C:\WINDOWS\system32\cmd.exe'. The window shows the command 'hostname' being run at the prompt 'C:\Users\Mark Kaelin Live>'. The output displays the computer's name 'MarkWKaelinm14x'. The window has standard window controls (minimize, maximize, close) and scroll bars on the right side.

```
C:\Users\Mark Kaelin Live>hostname
MarkWKaelinm14x

C:\Users\Mark Kaelin Live>
```

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 network from 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

## Compute Network (Elective-I) Laboratory Manual

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 the second router drops them and replies with ICMP Time Exceeded.

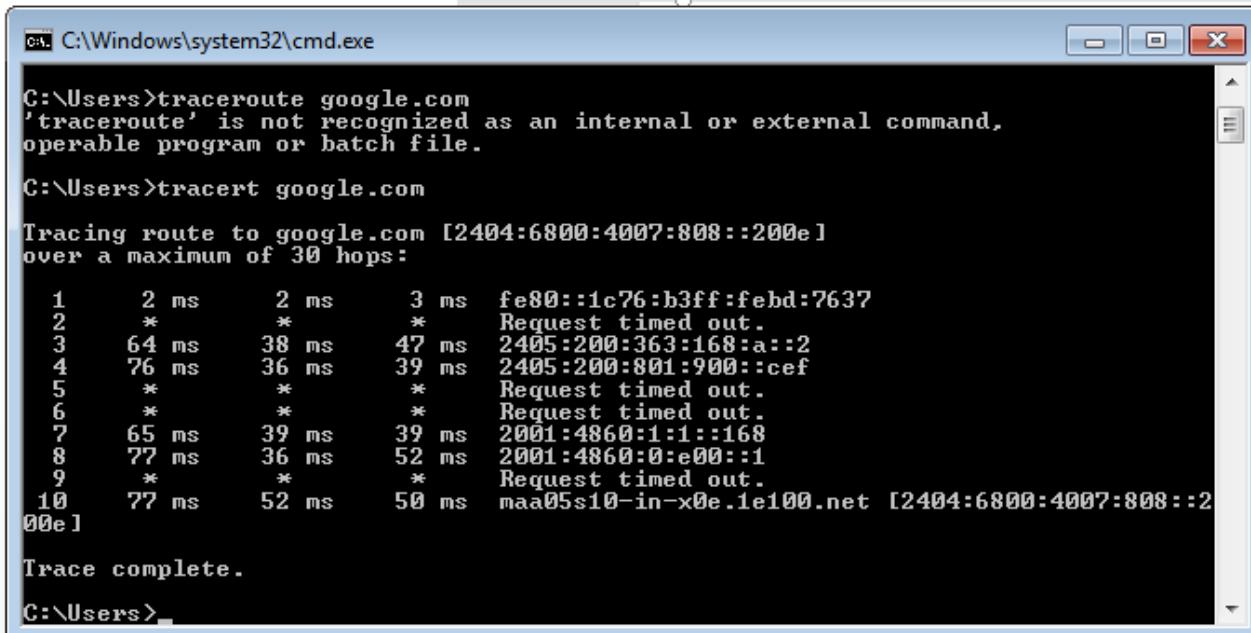
Proceeding in this way, traceroute uses the returned ICMP Time Exceeded messages to build a list of routers that packets traverse, until the destination is reached and returns an ICMP Echo

Reply message. With the tracert command shown above, we're asking tracert to show us the path from the local computer all the way to the network device with the hostname

www.google.co

m. #tracert

google.com



The screenshot shows a Windows Command Prompt window with the title bar "C:\Windows\system32\cmd.exe". The command entered is "tracert google.com". The output shows the tracing route to google.com over 10 hops. Hops 1 through 4 show increasing latency (2ms, 64ms, 76ms, 77ms). Hops 5 through 8 show request timed out errors. Hop 9 shows another request timed out. Hop 10 shows the final destination: maa05s10-in-x0e.1e100.net with latency 50ms. The command "Trace complete." is displayed at the end.

```
C:\Users>tracert google.com
Tracing route to google.com [2404:6800:4007:808::200e]
over a maximum of 30 hops:
 1    2 ms      2 ms      3 ms  fe80::1c76:b3ff:febd:763?
 2    *          *          * Request timed out.
 3    64 ms     38 ms     47 ms  2405:200:363:168:a::2
 4    76 ms     36 ms     39 ms  2405:200:801:900::cef
 5    *          *          * Request timed out.
 6    *          *          * Request timed out.
 7    65 ms     39 ms     39 ms  2001:4860:1:1::168
 8    77 ms     36 ms     52 ms  2001:4860:0:e00::1
 9    *          *          * Request timed out.
10    77 ms     52 ms     50 ms  maa05s10-in-x0e.1e100.net [2404:6800:4007:808::2
00e]

Trace complete.

C:\Users>
```

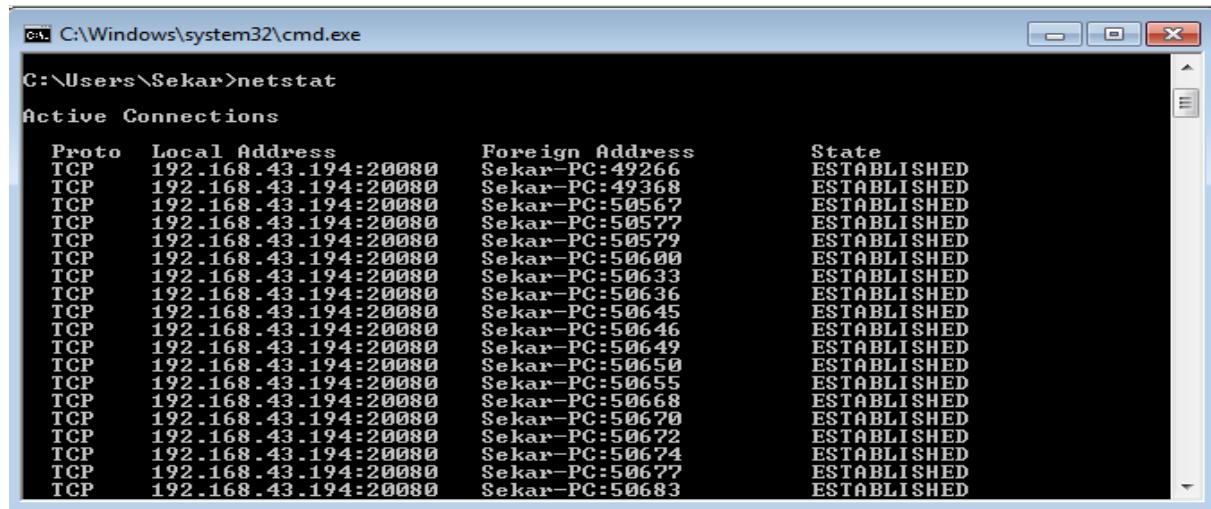
## 6. Netstat

Netstat is a common command line TCP/IP networking available in most versions of Department of Electronics and Telecommunication Engineering, DIT, Pimpri.

## Compute Network (Elective-I) Laboratory Manual

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



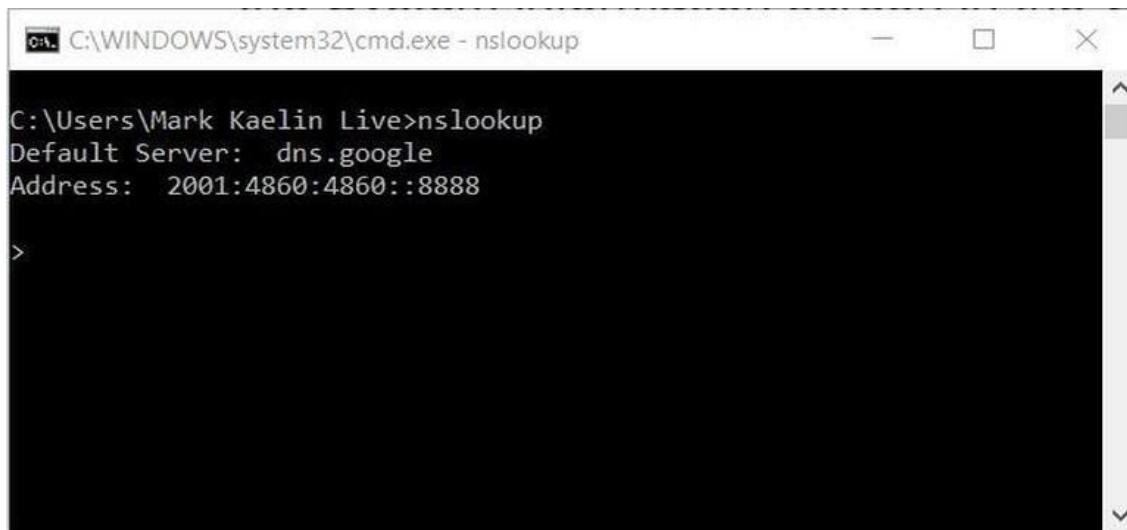
Active Connections			
Proto	Local Address	Foreign Address	State
TCP	192.168.43.194:20080	Sekar-PC:49266	ESTABLISHED
TCP	192.168.43.194:20080	Sekar-PC:49368	ESTABLISHED
TCP	192.168.43.194:20080	Sekar-PC:50567	ESTABLISHED
TCP	192.168.43.194:20080	Sekar-PC:50577	ESTABLISHED
TCP	192.168.43.194:20080	Sekar-PC:50579	ESTABLISHED
TCP	192.168.43.194:20080	Sekar-PC:50600	ESTABLISHED
TCP	192.168.43.194:20080	Sekar-PC:50633	ESTABLISHED
TCP	192.168.43.194:20080	Sekar-PC:50636	ESTABLISHED
TCP	192.168.43.194:20080	Sekar-PC:50645	ESTABLISHED
TCP	192.168.43.194:20080	Sekar-PC:50646	ESTABLISHED
TCP	192.168.43.194:20080	Sekar-PC:50649	ESTABLISHED
TCP	192.168.43.194:20080	Sekar-PC:50650	ESTABLISHED
TCP	192.168.43.194:20080	Sekar-PC:50655	ESTABLISHED
TCP	192.168.43.194:20080	Sekar-PC:50668	ESTABLISHED
TCP	192.168.43.194:20080	Sekar-PC:50670	ESTABLISHED
TCP	192.168.43.194:20080	Sekar-PC:50672	ESTABLISHED
TCP	192.168.43.194:20080	Sekar-PC:50674	ESTABLISHED
TCP	192.168.43.194:20080	Sekar-PC:50677	ESTABLISHED
TCP	192.168.43.194:20080	Sekar-PC:50683	ESTABLISHED

## 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're experiencing a DNS problem when you can access a resource by specifying its IP address but not its DNS name.

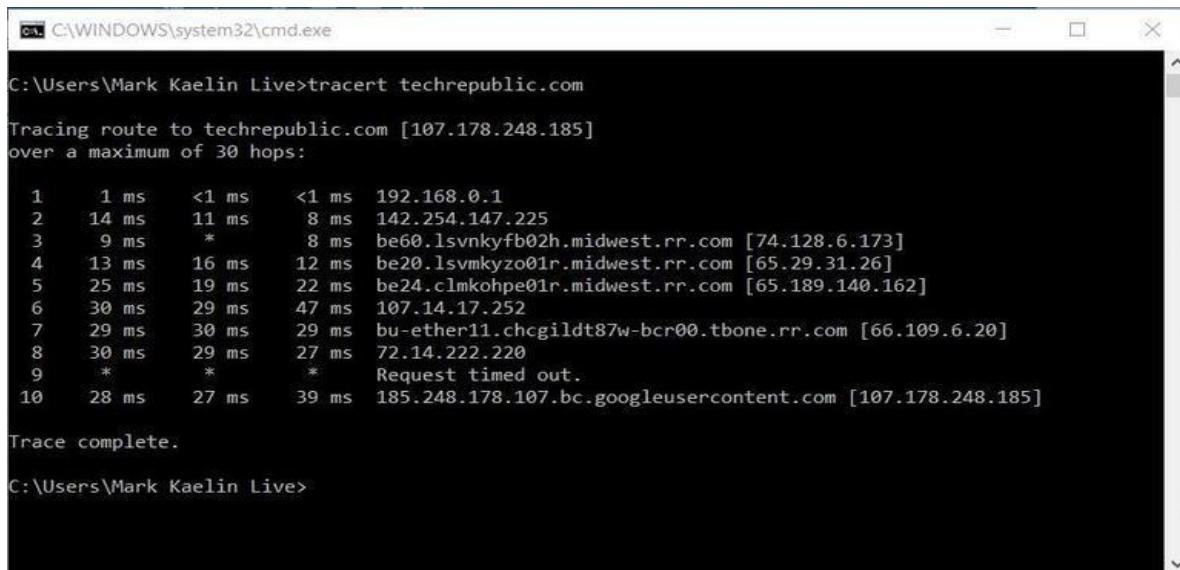
#nslookup



C:\WINDOWS\system32\cmd.exe - nslookup  
C:\Users\Mark Kaelin Live>nslookup  
Default Server: dns.google  
Address: 2001:4860:4860::8888  
>

## 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.



C:\WINDOWS\system32\cmd.exe  
C:\Users\Mark Kaelin Live>tracert techrepublic.com  
Tracing route to techrepublic.com [107.178.248.185]  
over a maximum of 30 hops:  
1 1 ms <1 ms <1 ms 192.168.0.1  
2 14 ms 11 ms 8 ms 142.254.147.225  
3 9 ms \* 8 ms be60.lsvnkyfb02h.midwest.rr.com [74.128.6.173]  
4 13 ms 16 ms 12 ms be20.lsvmkzyzo01r.midwest.rr.com [65.29.31.26]  
5 25 ms 19 ms 22 ms be24.clmkohpe01r.midwest.rr.com [65.189.140.162]  
6 30 ms 29 ms 47 ms 107.14.17.252  
7 29 ms 30 ms 29 ms bu-ether11.chcgildt87w-bcr00.tbone.rr.com [66.109.6.20]  
8 30 ms 29 ms 27 ms 72.14.222.220  
9 \* \* \* Request timed out.  
10 28 ms 27 ms 39 ms 185.248.178.107.bc.googleusercontent.com [107.178.248.185]  
Trace complete.  
C:\Users\Mark Kaelin Live>

**Conclusion:**