

## EXPERIMENT 2

**NAME: Akshat Bhat**

**UID: 2018130003**

**CLASS: TE COMPS**

**BATCH: A**

**DATE: 10/08/2020**

**AIM:** Basic Network Utilities using command line

### EXERCISE 1: PING

*Ping the any hosts 10 times (i.e., packet count is 10) with a packet size of 64 bytes, 100 bytes, 500 bytes, 1000 bytes, 1400 bytes*

#### **64 bytes**

Pinging google.com [2404:6800:4009:809::200e] with 64 bytes of data:

Request timed out.

Reply from 2404:6800:4009:809::200e: time=73ms

Reply from 2404:6800:4009:809::200e: time=49ms

Reply from 2404:6800:4009:809::200e: time=50ms

Reply from 2404:6800:4009:809::200e: time=48ms

Reply from 2404:6800:4009:809::200e: time=47ms

Reply from 2404:6800:4009:809::200e: time=46ms

Reply from 2404:6800:4009:809::200e: time=59ms

Reply from 2404:6800:4009:809::200e: time=43ms

Reply from 2404:6800:4009:809::200e: time=45ms

Ping statistics for 2404:6800:4009:809::200e:

Packets: Sent = 10, Received = 9, Lost = 1 (10% loss),

Approximate round trip times in milli-seconds:

Minimum = 43ms, Maximum = 73ms, Average = 51ms

IPv6 address 2404:6800:4009:809::200e is pinged 10 times with 64 bytes packets when host google.com is pinged. The average RTT is 53 ms. One packet is lost in the process.

C:\Users\Akshat>ping google.com -n 10 -l 64 -4

Pinging google.com [142.250.67.206] with 64 bytes of data:

Reply from 142.250.67.206: bytes=64 time=49ms TTL=114

Reply from 142.250.67.206: bytes=64 time=41ms TTL=114

Reply from 142.250.67.206: bytes=64 time=38ms TTL=114

Reply from 142.250.67.206: bytes=64 time=50ms TTL=114

Reply from 142.250.67.206: bytes=64 time=62ms TTL=114

Reply from 142.250.67.206: bytes=64 time=39ms TTL=114

Reply from 142.250.67.206: bytes=64 time=29ms TTL=114

Reply from 142.250.67.206: bytes=64 time=40ms TTL=114

```
Reply from 142.250.67.206: bytes=64 time=44ms TTL=114
Reply from 142.250.67.206: bytes=64 time=35ms TTL=114
```

Ping statistics for 142.250.67.206:

```
Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 29ms, Maximum = 62ms, Average = 42ms
```

IPv4 address 142.250.67.206 is pinged 10 times with 64 bytes packets when host google.com is pinged. The average RTT is 42 ms. The TTL represents the number of hops, or servers in different locations, the request can travel to before returning a failed attempt message. Here, TTL is 114.

### ***100 bytes***

Pinging google.com [2404:6800:4009:809::200e] with 100 bytes of data:

```
Reply from 2404:6800:4009:809::200e: time=47ms
Reply from 2404:6800:4009:809::200e: time=49ms
Reply from 2404:6800:4009:809::200e: time=37ms
Reply from 2404:6800:4009:809::200e: time=46ms
Reply from 2404:6800:4009:809::200e: time=46ms
Reply from 2404:6800:4009:809::200e: time=43ms
Reply from 2404:6800:4009:809::200e: time=52ms
Reply from 2404:6800:4009:809::200e: time=62ms
Reply from 2404:6800:4009:809::200e: time=61ms
Reply from 2404:6800:4009:809::200e: time=47ms
```

Ping statistics for 2404:6800:4009:809::200e:

```
Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 37ms, Maximum = 62ms, Average = 49ms
```

IPv6 address 2404:6800:4009:809::200e is pinged 10 times with 100 bytes packets when host google.com is pinged. The average RTT is 49 ms. There is no packet loss.

```
C:\Users\Akshat>ping google.com -n 10 -l 100 -4
```

Pinging google.com [216.58.203.46] with 100 bytes of data:

```
Reply from 216.58.203.46: bytes=68 (sent 100) time=51ms TTL=114
Reply from 216.58.203.46: bytes=68 (sent 100) time=48ms TTL=114
Reply from 216.58.203.46: bytes=68 (sent 100) time=44ms TTL=114
Reply from 216.58.203.46: bytes=68 (sent 100) time=45ms TTL=114
Reply from 216.58.203.46: bytes=68 (sent 100) time=40ms TTL=114
Reply from 216.58.203.46: bytes=68 (sent 100) time=52ms TTL=114
Reply from 216.58.203.46: bytes=68 (sent 100) time=45ms TTL=114
Reply from 216.58.203.46: bytes=68 (sent 100) time=49ms TTL=114
```

```
Reply from 216.58.203.46: bytes=68 (sent 100) time=52ms TTL=114
Reply from 216.58.203.46: bytes=68 (sent 100) time=44ms TTL=114
```

Ping statistics for 216.58.203.46:

```
Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 52ms, Average = 47ms
```

IPv4 address 216.58.203.46 is pinged 10 times with 100 bytes packets when host google.com is pinged. The average RTT is 47 ms. This time is a little more compared to the pinging with 64 byte packets. This could be because this server is slower than the previous one. Note that for the same host google.com, a different IPv4 address was pinged with packet size of 100 bytes but 64 bytes were received.

### ***500 bytes***

Pinging google.com [2404:6800:4009:809::200e] with 500 bytes of data:

```
Reply from 2404:6800:4009:809::200e: time=101ms
Reply from 2404:6800:4009:809::200e: time=69ms
Reply from 2404:6800:4009:809::200e: time=63ms
Reply from 2404:6800:4009:809::200e: time=62ms
Reply from 2404:6800:4009:809::200e: time=61ms
Reply from 2404:6800:4009:809::200e: time=57ms
Reply from 2404:6800:4009:809::200e: time=58ms
Reply from 2404:6800:4009:809::200e: time=53ms
Reply from 2404:6800:4009:809::200e: time=59ms
Reply from 2404:6800:4009:809::200e: time=63ms
```

Ping statistics for 2404:6800:4009:809::200e:

```
Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 53ms, Maximum = 101ms, Average = 64ms
```

IPv6 address 2404:6800:4009:809::200e is pinged 10 times with 500 bytes packets when host google.com is pinged. The average RTT is 64 ms.

```
C:\Users\Akshat>ping google.com -n 10 -l 500 -4
```

Pinging google.com [172.217.160.206] with 500 bytes of data:

```
Reply from 172.217.160.206: bytes=68 (sent 500) time=57ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 500) time=67ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 500) time=52ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 500) time=56ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 500) time=53ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 500) time=64ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 500) time=57ms TTL=113
```

```
Reply from 172.217.160.206: bytes=68 (sent 500) time=62ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 500) time=59ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 500) time=60ms TTL=113
```

Ping statistics for 172.217.160.206:

```
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 52ms, Maximum = 67ms, Average = 58ms
```

IPv4 address 172.217.160.206 is pinged 10 times with 500 bytes packets when host google.com is pinged. The average RTT is 58 ms. Note that for the same host google.com, a different IPv4 address was pinged with a packet size of 500 bytes but 68 bytes were received. Hence the server is different for different packet sizes.

### ***1000 bytes***

Pinging google.com [2404:6800:4009:809::200e] with 1000 bytes of data:

```
Reply from 2404:6800:4009:809::200e: time=209ms
Reply from 2404:6800:4009:809::200e: time=95ms
Reply from 2404:6800:4009:809::200e: time=120ms
Reply from 2404:6800:4009:809::200e: time=55ms
Reply from 2404:6800:4009:809::200e: time=65ms
Reply from 2404:6800:4009:809::200e: time=68ms
Reply from 2404:6800:4009:809::200e: time=89ms
Reply from 2404:6800:4009:809::200e: time=42ms
Reply from 2404:6800:4009:809::200e: time=49ms
Reply from 2404:6800:4009:809::200e: time=53ms
```

Ping statistics for 2404:6800:4009:809::200e:

```
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 209ms, Average = 84ms
```

IPv6 address 2404:6800:4009:809::200e is pinged 10 times with 1000 bytes packets when host google.com is pinged. The average RTT is 84 ms. The average RTT is larger than the previous ping results.

```
C:\Users\Akshat>ping google.com -n 10 -l 1000 -4
```

Pinging google.com [172.217.160.206] with 1000 bytes of data:

```
Reply from 172.217.160.206: bytes=68 (sent 1000) time=63ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 1000) time=55ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 1000) time=54ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 1000) time=54ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 1000) time=58ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 1000) time=69ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 1000) time=52ms TTL=113
```

```
Reply from 172.217.160.206: bytes=68 (sent 1000) time=58ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 1000) time=59ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 1000) time=63ms TTL=113
```

Ping statistics for 172.217.160.206:

```
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 52ms, Maximum = 69ms, Average = 58ms
```

IPv4 address 172.217.160.206 is pinged 10 times with 1000 bytes packets when host google.com is pinged. The average RTT is 58 ms. IPv4 address was pinged with a packet size of 1400 bytes but 68 bytes were received. The average Round Trip Time is the same as what we got when we pinged with a packet size of 500 bytes. We notice that everytime the server receives 68 bytes instead of the sent bytes(>100 bytes).

### ***1400 bytes***

Pinging google.com [2404:6800:4009:809::200e] with 1400 bytes of data:

```
Reply from 2404:6800:4009:809::200e: time=59ms
Reply from 2404:6800:4009:809::200e: time=77ms
Reply from 2404:6800:4009:809::200e: time=63ms
Reply from 2404:6800:4009:809::200e: time=75ms
Reply from 2404:6800:4009:809::200e: time=61ms
Reply from 2404:6800:4009:809::200e: time=65ms
Reply from 2404:6800:4009:809::200e: time=60ms
Reply from 2404:6800:4009:809::200e: time=77ms
Reply from 2404:6800:4009:809::200e: time=58ms
Reply from 2404:6800:4009:809::200e: time=66ms
```

Ping statistics for 2404:6800:4009:809::200e:

```
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 58ms, Maximum = 77ms, Average = 66ms
```

IPv6 address 2404:6800:4009:809::200e is pinged 10 times with 1400 bytes packets when host google.com is pinged. The average RTT is 66 ms. The average RTT is smaller than the previous ping result. Hence we cannot say that if the packet size sent is more then RTT is more.

```
C:\Users\Akshat>ping google.com -n 10 -l 1400 -4
```

Pinging google.com [172.217.160.206] with 1400 bytes of data:

```
Reply from 172.217.160.206: bytes=68 (sent 1400) time=60ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 1400) time=69ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 1400) time=64ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 1400) time=56ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 1400) time=57ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 1400) time=62ms TTL=113
```

```
Reply from 172.217.160.206: bytes=68 (sent 1400) time=45ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 1400) time=62ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 1400) time=58ms TTL=113
Reply from 172.217.160.206: bytes=68 (sent 1400) time=75ms TTL=113
```

Ping statistics for 172.217.160.206:

```
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 45ms, Maximum = 75ms, Average = 60ms
```

IPv4 address 172.217.160.206 is pinged 10 times with 1400 bytes packets when host google.com is pinged. The average RTT is 60 ms. IPv4 address was pinged with a packet size of 1400 bytes but again 68 bytes were received.

### Now performing ping command with 1400 bytes of data on different host fast.com

Pinging fast.com [2405:200:1630:18ba::24fe] with 1400 bytes of data:  
Request timed out.

```
Reply from 2405:200:1630:18ba::24fe: time=196ms
Reply from 2405:200:1630:18ba::24fe: time=87ms
Reply from 2405:200:1630:18ba::24fe: time=80ms
Reply from 2405:200:1630:18ba::24fe: time=90ms
Reply from 2405:200:1630:18ba::24fe: time=76ms
Reply from 2405:200:1630:18ba::24fe: time=72ms
Reply from 2405:200:1630:18ba::24fe: time=74ms
Reply from 2405:200:1630:18ba::24fe: time=62ms
Reply from 2405:200:1630:18ba::24fe: time=69ms
```

Ping statistics for 2405:200:1630:18ba::24fe:

```
    Packets: Sent = 10, Received = 9, Lost = 1 (10% loss),
Approximate round trip times in milli-seconds:
    Minimum = 62ms, Maximum = 196ms, Average = 89ms
```

IPv6 address 2405:200:1630:18ba::24fe is pinged 10 times with 1400 bytes packets when host fast.com is pinged. The average RTT is 89 ms. The average RTT is greater than that of google.com.

```
C:\Users\Akshat>ping fast.com -n 10 -l 1400 -4
```

Pinging fast.com [104.120.88.80] with 1400 bytes of data:

```
Reply from 104.120.88.80: bytes=1400 time=187ms TTL=55
Reply from 104.120.88.80: bytes=1400 time=66ms TTL=55
Reply from 104.120.88.80: bytes=1400 time=66ms TTL=55
Reply from 104.120.88.80: bytes=1400 time=72ms TTL=55
Reply from 104.120.88.80: bytes=1400 time=47ms TTL=55
Reply from 104.120.88.80: bytes=1400 time=80ms TTL=55
Reply from 104.120.88.80: bytes=1400 time=59ms TTL=55
```

```
Reply from 104.120.88.80: bytes=1400 time=59ms TTL=55
Reply from 104.120.88.80: bytes=1400 time=85ms TTL=55
Reply from 104.120.88.80: bytes=1400 time=66ms TTL=55
```

Ping statistics for 104.120.88.80:

```
Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 47ms, Maximum = 187ms, Average = 78ms
```

IPv4 address 104.120.88.80 is pinged 10 times with 1400 bytes packets when host fast.com is pinged. The average RTT is 78 ms. IPv4 address was pinged with a packet size of 1400 bytes but this time all were received. The average RTT is greater than that of google.com when pinged with the same packet size. Also, TTL is much lesser than that of google.com.

### **1. Does the average RTT vary between different hosts? What aspects of latency (transmit, propagation, and queueing delay) might impact this and why?**

**Inference:** Yes, for the same amount of data the average RTT varied between different hosts, in this case, google.com and fast.com.

Round-trip time (RTT) is the duration, measured in milliseconds, from when a browser sends a request to when it receives a response from a server.

Latency = Propagation + Transmit + Queue

There **might** exist a propagation delay in the two cases as propagation delay depends on **distance** and **propagation speed**. **Propagation delay** is the time taken by the first bit to travel from sender to receiver end of the link or simply the time required for bits to reach the destination from the start point. Thus various aspects of latency contribute to rtt being varied between hosts .

### **2. Does the average RTT vary with different packet sizes? What aspects of latency (transmit, propagation, and queueing delay) might impact this and why?**

**Inference:** Yes, the average RTT varies with different packet sizes even if we ping to the same host. This **might** be because of the **Transmission delay** and the **Queueing delay** which depend on the **size of the packets**.

The **queuing delay** is the time a job waits in a queue until it can be executed. It is a key component of network delay. In a switched network, queuing delay is the time between the

completion of signaling by the call originator and the arrival of a ringing signal at the call receiver.

**Transmission delay** is a function of the packet's length and has nothing to do with the distance between the two nodes. This delay is proportional to the packet's length in bits, It is given by the following formula:

$$DT = N/R \text{ seconds}$$

where

*DT is the transmission delay in seconds*

*N is the number of bits, and*

*R is the rate of transmission (say in bits per second)*

***Experiment with ping to find the round trip times to a variety of destinations. Write up any interesting observations, including in particular how the round trip time compares to the physical distance.***

**www.uw.edu**

**Location: Washington**

Pinging www.washington.edu [128.95.155.198] with 32 bytes of data:

```
Reply from 128.95.155.198: bytes=32 time=1563ms TTL=45
Reply from 128.95.155.198: bytes=32 time=286ms TTL=45
Reply from 128.95.155.198: bytes=32 time=283ms TTL=45
Reply from 128.95.155.198: bytes=32 time=288ms TTL=45
Reply from 128.95.155.198: bytes=32 time=285ms TTL=45
Reply from 128.95.155.198: bytes=32 time=360ms TTL=45
Reply from 128.95.155.198: bytes=32 time=299ms TTL=45
Reply from 128.95.155.198: bytes=32 time=360ms TTL=45
Reply from 128.95.155.198: bytes=32 time=627ms TTL=45
Reply from 128.95.155.198: bytes=32 time=278ms TTL=45
```

Ping statistics for 128.95.155.198:

```
Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 278ms, Maximum = 1563ms, Average = 462ms
```

Pinging www.uw.edu resulted in a very high average RTT probably because the server is far away. The TTL is at a low 45.

**www.ox.ac.uk**

**Location: Oxford, England**



Pinging www.ox.ac.uk [151.101.130.133] with 32 bytes of data:

```
Reply from 151.101.130.133: bytes=32 time=369ms TTL=52
Reply from 151.101.130.133: bytes=32 time=43ms TTL=52
Reply from 151.101.130.133: bytes=32 time=43ms TTL=52
Reply from 151.101.130.133: bytes=32 time=49ms TTL=52
Reply from 151.101.130.133: bytes=32 time=47ms TTL=52
Reply from 151.101.130.133: bytes=32 time=43ms TTL=52
Reply from 151.101.130.133: bytes=32 time=39ms TTL=52
Reply from 151.101.130.133: bytes=32 time=42ms TTL=52
Reply from 151.101.130.133: bytes=32 time=41ms TTL=52
Reply from 151.101.130.133: bytes=32 time=50ms TTL=52
```

Ping statistics for 151.101.130.133:

```
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 39ms, Maximum = 369ms, Average = 76ms
```

Pinging www.ox.ac.uk resulted in a comparatively far lower RTT probably because the server is closer to India.

**www.u-tokyo.ac.jp**

**Location: Tokyo, Japan**

Pinging www.u-tokyo.ac.jp [210.152.243.234] with 32 bytes of data:

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Ping statistics for 210.152.243.234:

```
    Packets: Sent = 10, Received = 0, Lost = 10 (100% loss)
```

When host www.u-tokyo.ac.jp was pinged with 10 packets of size 32 bytes, there was 100% packet loss. This could be because some routers and firewalls block ping requests so no response is received on ping.

## EXERCISE 2: TRACEROUTE

**Traceroute Working:** A traceroute displays the path that the signal took as it traveled around the Internet to the website. It also displays times which are the response times that occurred at each stop along the route. If there is a connection problem or latency connecting to a site, it will show up in these times. Traceroute is a network diagnostic tool used to track in real-time the pathway taken by a packet on an IP network from source to destination, reporting the IP addresses of all the routers it pinged in between. Traceroute also records the time taken for each hop the packet makes during its route to the destination. If any of the hops come back with “Request timed out”, it denotes network congestion and a reason for slow loading Web pages and dropped connections. *For each hop, there are three RTT values (the default of TRACERT is to send 3 data packets to test each hop).*

**Tracert for google.com:**

```
C:\Users\Akshat>tracert -4 -h 10 google.com

Tracing route to google.com [172.217.166.78]
over a maximum of 30 hops:

  0  80 ms  *      2 ms  192.168.1.1
  1  *      *      *      Request timed out.
  2  16 ms  18 ms  17 ms  static-mum-59.185.210.225.mtnl.net.in [59.185.210.225]
  3  13 ms  16 ms  19 ms  static-mum-59.185.210.226.mtnl.net.in [59.185.210.226]
  4  15 ms  17 ms  15 ms  74.125.51.205
  5  17 ms  15 ms  16 ms  209.85.246.51
  6  28 ms  15 ms  14 ms  209.85.242.111
  7  16 ms  14 ms  14 ms  android.clients.google.com [172.217.166.78]

Trace complete.
```

1. For each  $n = 1, 2, 3, \dots$ , traceroute sends a packet with "time-to-live" (ttl) equal to  $n$  ms.
2. The first router is 192.168.1.1. It is an IP address which routers like Linksys and other network brands use as an access point or gateway. \* indicates no response.
3. The second router that gives response is of the internet service provider(MTNL). So, we can see that packets are sent and received via ISP.
4. The trace completed in 8 hops. So, only a few routers are part of the route to send packets to Google.

**Tracert for iitb.ac.in:**

```
C:\Users\Akshat>tracert -4 -h 10 iitb.ac.in

Tracing route to iitb.ac.in [103.21.127.114]
over a maximum of 10 hops:

  1    372 ms     3 ms     1 ms  192.168.1.1
  2      *        *        *    Request timed out.
  3    17 ms    17 ms    15 ms  static-mum-59.185.211.249.mtnl.net.in [59.185.211.249]
  4    15 ms    14 ms    14 ms  static-mum-59.185.211.250.mtnl.net.in [59.185.211.250]
  5    14 ms    15 ms    16 ms  115.114.89.125.static-Mumbai.vsnl.net.in [115.114.89.125]
  6    20 ms    15 ms    15 ms  172.23.78.237
  7    14 ms    14 ms    15 ms  172.23.78.234
  8    16 ms    18 ms    17 ms  115.110.234.170.static.Mumbai.vsnl.net.in [115.110.234.170]
  9      *        *        *    Request timed out.
 10      *        *        *    Request timed out.

Trace complete.
```

1. The first three routers are the same(have the same subnet) as when tracerouting google.com.
2. The traceroute result has the IP address of VSNL, after which the request timed out. \* indicates no response. This can be because the next routers block tracerouting.

#### Tracert for berkeley.edu:

```
C:\Users\Akshat>tracert -4 -h 10 berkeley.edu

Tracing route to berkeley.edu [35.163.72.93]
over a maximum of 10 hops:

  1    424 ms     1 ms     1 ms  192.168.1.1
  2      *        *        *    Request timed out.
  3    18 ms    13 ms    14 ms  static-mum-59.185.210.229.mtnl.net.in [59.185.210.229]
  4    45 ms    17 ms    14 ms  static-mum-59.185.210.230.mtnl.net.in [59.185.210.230]
  5    16 ms    15 ms    13 ms  static-mum-59.185.211.229.mtnl.net.in [59.185.211.229]
  6    16 ms    14 ms    14 ms  125.19.104.89
  7   239 ms   238 ms   257 ms  116.119.44.134
  8   237 ms   235 ms   235 ms  99.83.67.88
  9      *        *        *    Request timed out.
 10      *        *        *    Request timed out.

Trace complete.
```

1. The traceroute shows that packets are sent from MTNL's Mumbai router then transferred to California where Berkeley University is located.
2. There are "request timed out" messages which mean that routers didn't respond to the packets.
3. The time taken to reach an international router is large compared to reaching a router within the country.

#### Tracert for www.ox.ac.uk:

```
C:\Users\Akshat>tracert -4 -h 10 www.ox.ac.uk

Tracing route to www.ox.ac.uk [151.101.194.133]
over a maximum of 10 hops:

  1    79 ms    1 ms    1 ms  192.168.1.1
  2    *        *        *    Request timed out.
  3    14 ms    15 ms    31 ms  static-mum-59.185.210.229.mtnl.net.in [59.185.210.229]
  4    15 ms    15 ms    16 ms  static-mum-59.185.210.230.mtnl.net.in [59.185.210.230]
  5   146 ms    14 ms    14 ms  115.114.89.61.static-Mumbai.vsnl.net.in [115.114.89.61]
  6    14 ms    15 ms    14 ms  172.23.78.225
  7    14 ms    14 ms    15 ms  172.28.132.245
  8    14 ms    14 ms    15 ms  115.110.206.150.static-Mumbai.vsnl.net.in [115.110.206.150]
  9    15 ms    17 ms    14 ms  www.ox.ac.uk [151.101.194.133]

Trace complete.
```

1. The first three routers in the route are the same as when tracerouting to Berkeley University.
2. The traceroute shows that packets are sent from MTNL's Mumbai router then transferred to VSNL's Mumbai router.
3. The trace completed in 9 hops. So, only a few routers are part of the route to send packets to Oxford University.

### *math.hws.edu*

```
Tracing route to math.hws.edu [64.89.144.237]
over a maximum of 30 hops:

  1   609 ms    1 ms    4 ms  jiofi.local.html [192.168.225.1]
  2    *        *        *    Request timed out.
  3   48 ms    54 ms    86 ms  10.71.18.18
  4   46 ms    48 ms    59 ms  192.168.69.164
  5   36 ms    39 ms    46 ms  192.168.69.163
  6   90 ms    41 ms    45 ms  172.16.80.107
  7   51 ms    37 ms    38 ms  172.17.119.5
  8    *        *        *    Request timed out.
  9    *        *        *    Request timed out.
 10    *        *        *    Request timed out.
 11  100 ms    42 ms    39 ms  103.198.140.174
 12  232 ms    216 ms    201 ms  103.198.140.45
 13  177 ms    307 ms    203 ms  103.198.140.56
 14  207 ms    590 ms    204 ms  103.198.140.107
 15  477 ms    205 ms    407 ms  103.198.140.45
 16  223 ms    180 ms    185 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 17  152 ms    164 ms    162 ms  be3672.ccr52.lhr01.atlas.cogentco.com [130.117.48.145]
 18  296 ms    272 ms    203 ms  be3488.ccr42.lon13.atlas.cogentco.com [154.54.60.13]
 19  262 ms    205 ms    203 ms  be2869.ccr22.lon01.atlas.cogentco.com [154.54.57.162]
 20    *        *        *    Request timed out.
 21  220 ms    168 ms    168 ms  ae-226-3602.edge3.London15.Level3.net [4.69.167.94]
 22  293 ms    181 ms    158 ms  ae-226-3602.edge3.London15.Level3.net [4.69.167.94]
 23  241 ms    167 ms    447 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 24  437 ms    335 ms    511 ms  roc1-ar5-xe-11-0-0-us.twtelecom.net [35.248.1.162]
 25  543 ms    383 ms    715 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 26  367 ms    331 ms    310 ms  nat.hws.edu [64.89.144.100]
 27    *        *        *    Request timed out.
 28    *        *        *    Request timed out.
 29    *        *        *    Request timed out.
 30    *        *        *    Request timed out.

Trace complete.
```

```

Tracing route to www.hws.edu [64.89.145.159]
over a maximum of 30 hops:

 1  298 ms    1 ms     4 ms    jiofi.local.html [192.168.225.1]
 2  *         *         *       Request timed out.
 3  54 ms     37 ms    48 ms    10.71.18.2
 4  54 ms     37 ms    48 ms    192.168.69.162
 5  64 ms     58 ms    46 ms    192.168.69.163
 6  37 ms     58 ms    52 ms    172.16.80.109
 7  66 ms     45 ms    78 ms    172.17.119.5
 8  *         *         *       Request timed out.
 9  *         *         *       Request timed out.
10  *         *         *       Request timed out.
11  54 ms     32 ms    50 ms    103.198.140.60
12 183 ms     178 ms   178 ms    103.198.140.45
13 188 ms     243 ms   265 ms    103.198.140.54
14 206 ms     178 ms   163 ms    103.198.140.45
15 179 ms     180 ms   169 ms    hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
16 246 ms     156 ms   212 ms    be3671.ccr51.lhr01.atlas.cogentco.com [130.117.48.137]
17 199 ms     174 ms   175 ms    be3487.ccr41.lon13.atlas.cogentco.com [154.54.60.5]
18 178 ms     246 ms   206 ms    be2870.ccr22.lon01.atlas.cogentco.com [154.54.58.174]
19 277 ms     203 ms   263 ms    ae-7.edge7.London1.Level3.net [4.68.62.41]
20 271 ms     203 ms   203 ms    ae-225-3601.edge3.London15.Level3.net [4.69.167.90]
21 223 ms     167 ms   157 ms    ae-225-3601.edge3.London15.Level3.net [4.69.167.90]
22 163 ms     175 ms   222 ms    ae4.ar8.lon15.Level3.net [4.68.111.254]
23 756 ms     610 ms   343 ms    roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
24 613 ms     410 ms   411 ms    66-195-65-170.static.clt.one [66.195.65.170]
25 297 ms     434 ms   448 ms    nat.hws.edu [64.89.144.100]
26 *         *         *       Request timed out.
27 *         *         *       Request timed out.
28 *         *         *       Request timed out.
29 *         *         *       Request timed out.
30 *         *         *       Request timed out.

Trace complete.

```

### ***www.hws.edu***

From the images above, the first row shows that the process of route tracing has started as the last column shows the Default Gateway of the user. In both the cases, the route is being traced starting from the ISP (Internet service provider) of the user. Before reaching common IP **nat.hws.edu [64.89.144.100]**, we can infer that the route is completely different after crossing the ISP for both the cases. However certain routers are the same or belong to the same subnet for both the cases but the order in which they appear is different. In both the cases multinational ISP Cogentco router is encountered and same for twtelecom3 in London.

## **EXERCISE 3: TRACEROUTE**

Below there are two screenshots of tracerouting the same IP address. There was a time difference of **one day** between them.



Tracing route to math.hws.edu [64.89.144.237]  
over a maximum of 30 hops:

1	609 ms	1 ms	4 ms	jiofi.local.html [192.168.225.1]
2	*	*	*	Request timed out.
3	48 ms	54 ms	86 ms	10.71.18.18
4	46 ms	48 ms	59 ms	192.168.69.164
5	36 ms	39 ms	46 ms	192.168.69.163
6	90 ms	41 ms	45 ms	172.16.80.107
7	51 ms	37 ms	38 ms	172.17.119.5
8	*	*	*	Request timed out.
9	*	*	*	Request timed out.
10	*	*	*	Request timed out.
11	100 ms	42 ms	39 ms	103.198.140.174
12	232 ms	216 ms	201 ms	103.198.140.45
13	177 ms	307 ms	203 ms	103.198.140.56
14	207 ms	590 ms	204 ms	103.198.140.107
15	477 ms	205 ms	407 ms	103.198.140.45
16	223 ms	180 ms	185 ms	hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
17	152 ms	164 ms	162 ms	be3672.ccr52.lhr01.atlas.cogentco.com [130.117.48.145]
18	296 ms	272 ms	203 ms	be3488.ccr42.lon13.atlas.cogentco.com [154.54.60.13]
19	262 ms	205 ms	203 ms	be2869.ccr22.lon01.atlas.cogentco.com [154.54.57.162]
20	*	*	*	Request timed out.
21	220 ms	168 ms	168 ms	ae-226-3602.edge3.London15.Level3.net [4.69.167.94]
22	293 ms	181 ms	158 ms	ae-226-3602.edge3.London15.Level3.net [4.69.167.94]
23	241 ms	167 ms	447 ms	ae4.ar8.lon15.Level3.net [4.68.111.254]
24	437 ms	335 ms	511 ms	roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
25	543 ms	383 ms	715 ms	66-195-65-170.static.ctl.one [66.195.65.170]
26	367 ms	331 ms	310 ms	nat.hws.edu [64.89.144.100]
27	*	*	*	Request timed out.
28	*	*	*	Request timed out.
29	*	*	*	Request timed out.
30	*	*	*	Request timed out.

Trace complete.

C:\Users\Akshat>tracert math.hws.edu

Tracing route to math.hws.edu [64.89.144.237]  
over a maximum of 30 hops:

1	7 ms	4 ms	2 ms	jiofi.local.html [192.168.225.1]
2	*	*	*	Request timed out.
3	90 ms	38 ms	48 ms	10.71.5.29
4	58 ms	41 ms	55 ms	192.168.70.219
5	74 ms	38 ms	48 ms	192.168.70.218
6	*	*	*	Request timed out.
7	86 ms	37 ms	48 ms	172.25.50.7
8	*	*	*	Request timed out.
9	*	*	*	Request timed out.
10	*	*	*	Request timed out.
11	45 ms	38 ms	48 ms	103.198.140.58
12	239 ms	203 ms	306 ms	103.198.140.45
13	222 ms	163 ms	166 ms	103.198.140.27
14	260 ms	203 ms	203 ms	103.198.140.107
15	221 ms	203 ms	174 ms	103.198.140.45
16	223 ms	202 ms	161 ms	hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
17	426 ms	306 ms	204 ms	be3671.ccr51.lhr01.atlas.cogentco.com [130.117.48.137]
18	325 ms	203 ms	203 ms	be3487.ccr41.lon13.atlas.cogentco.com [154.54.60.5]
19	427 ms	203 ms	408 ms	be2870.ccr22.lon01.atlas.cogentco.com [154.54.58.174]
20	221 ms	152 ms	170 ms	ae-7.edge7.London1.Level3.net [4.68.62.41]
21	209 ms	170 ms	170 ms	ae-225-3601.edge3.London15.Level3.net [4.69.167.90]
22	178 ms	197 ms	424 ms	ae-225-3601.edge3.London15.Level3.net [4.69.167.90]
23	323 ms	176 ms	538 ms	ae4.ar8.lon15.Level3.net [4.68.111.254]
24	610 ms	610 ms	408 ms	roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
25	492 ms	301 ms	720 ms	66-195-65-170.static.ctl.one [66.195.65.170]
26	333 ms	813 ms	612 ms	nat.hws.edu [64.89.144.100]
27	*	*	*	Request timed out.
28	*	*	*	Request timed out.
29	*	*	*	Request timed out.
30	*	*	*	Request timed out.

Trace complete.

## ***QUESTIONS ABOUT PATHS***

*Now look at the results you gathered and answer the following questions about the paths taken by your packets. Store your answers in a file named traceroute.txt.*

### ***1. Is any part of the path common for all hosts you tracerouted?***

Yes, the tracerouting follows a particular path from the user's IP address through the IP addresses of the ISP and then the path really depends on which access point is ready to respond and which access points or routers have firewalls configured for blocking the requests and accordingly, the destination can be reached through different paths at different times.

### ***2. Is there a relationship between the number of nodes that show up in the traceroute and the location of the host? If so, what is this relationship?***

There is no relationship between the number of nodes that show up in the traceroute and the location of the host as hop does not depend on distance.

### ***3. Is there a relationship between the number of nodes that show up in the traceroute and latency of the host (from your ping results above)? Does the same relationship hold for all hosts?***

Since the two hosts were of the same institution there were certain nodes that were common on running the tracert command. If the location of the host is farther away then generally it means more hops (more nodes/steps).

The main difference between Ping and Traceroute is that Ping is a quick and easy utility to tell if the specified server is reachable and how long will it take to send and receive data from the server whereas Traceroute finds the exact route taken to reach the server and time taken by each step (hop).

## **EXERCISE 4: WHOIS**

*Use whois to investigate a well-known web site such as google.com.*

```
C:\Users\Akshat\Downloads>Whois google.com
```

```
Whois v1.21 - Domain information lookup  
Copyright (C) 2005-2019 Mark Russinovich  
Sysinternals - www.sysinternals.com
```

```
Connecting to COM.whois-servers.net...
```

```
WHOIS Server: whois.markmonitor.com  
Registrar URL: http://www.markmonitor.com  
Updated Date: 2019-09-09T15:39:04Z
```

Creation Date: 1997-09-15T04:00:00Z  
Registry Expiry Date: 2028-09-14T04:00:00Z  
Registrar: MarkMonitor Inc.  
Registrar IANA ID: 292  
Registrar Abuse Contact Email: [abusecomplaints@markmonitor.com](mailto:abusecomplaints@markmonitor.com)  
Registrar Abuse Contact Phone: +1.2083895740  
Domain Status: clientDeleteProhibited <https://icann.org/epp#clientDeleteProhibited>  
Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>  
Domain Status: clientUpdateProhibited <https://icann.org/epp#clientUpdateProhibited>  
Domain Status: serverDeleteProhibited <https://icann.org/epp#serverDeleteProhibited>  
Domain Status: serverTransferProhibited <https://icann.org/epp#serverTransferProhibited>  
Domain Status: serverUpdateProhibited <https://icann.org/epp#serverUpdateProhibited>  
Name Server: NS1.GOOGLE.COM  
Name Server: NS2.GOOGLE.COM  
Name Server: NS3.GOOGLE.COM  
Name Server: NS4.GOOGLE.COM  
DNSSEC: unsigned  
URL of the ICANN Whois Inaccuracy Complaint Form: <https://www.icann.org/wicf/>  
>>> Last update of whois database: 2020-08-16T14:47:59Z <<<

For more information on Whois status codes, please visit <https://icann.org/epp>

NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois database through the use of electronic processes that are high-volume and automated except as reasonably necessary to register domain names or modify existing registrations; the Data in VeriSign Global Registry Services' ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. VeriSign does not guarantee its accuracy. By submitting a Whois query, you agree to abide by the following terms of use: You agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to VeriSign (or its computer systems). The compilation, repackaging, dissemination or other use of this Data is expressly prohibited without the prior written consent of VeriSign. You agree not to use electronic processes that are automated and high-volume to access or query the Whois database except as reasonably necessary to register domain names or modify existing registrations. VeriSign reserves the right to restrict your access to the Whois database in its sole discretion to ensure operational stability. VeriSign may restrict or terminate your access to the Whois database for failure to abide by these terms of use. VeriSign reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.

Connecting to whois.markmonitor.com...



WHOIS Server: whois.markmonitor.com  
Registrar URL: <http://www.markmonitor.com>  
Updated Date: 2019-09-09T08:39:04-0700  
Creation Date: 1997-09-15T00:00:00-0700  
Registrar Registration Expiration Date: 2028-09-13T00:00:00-0700  
Registrar: MarkMonitor, Inc.  
Registrar IANA ID: 292  
Registrar Abuse Contact Email: [abusecomplaints@markmonitor.com](mailto:abusecomplaints@markmonitor.com)  
Registrar Abuse Contact Phone: +1.2083895770  
Domain Status: clientUpdateProhibited (<https://www.icann.org/epp#clientUpdateProhibited>)  
Domain Status: clientTransferProhibited (<https://www.icann.org/epp#clientTransferProhibited>)  
Domain Status: clientDeleteProhibited (<https://www.icann.org/epp#clientDeleteProhibited>)  
Domain Status: serverUpdateProhibited (<https://www.icann.org/epp#serverUpdateProhibited>)  
Domain Status: serverTransferProhibited (<https://www.icann.org/epp#serverTransferProhibited>)  
Domain Status: serverDeleteProhibited (<https://www.icann.org/epp#serverDeleteProhibited>)  
Registrant Organization: Google LLC  
Registrant State/Province: CA  
Registrant Country: US  
Registrant Email: Select Request Email Form at <https://domains.markmonitor.com/whois/google.com>  
Admin Organization: Google LLC  
Admin State/Province: CA  
Admin Country: US  
Admin Email: Select Request Email Form at <https://domains.markmonitor.com/whois/google.com>  
Tech Organization: Google LLC  
Tech State/Province: CA  
Tech Country: US  
Tech Email: Select Request Email Form at <https://domains.markmonitor.com/whois/google.com>  
Name Server: ns3.google.com  
Name Server: ns1.google.com  
Name Server: ns4.google.com  
Name Server: ns2.google.com  
DNSSEC: unsigned  
URL of the ICANN WHOIS Data Problem Reporting System: <http://wdprs.internic.net/>  
>>> Last update of WHOIS database: 2020-08-16T07:44:00-0700 <<<

For more information on WHOIS status codes, please visit:  
<https://www.icann.org/resources/pages/epp-status-codes>

If you wish to contact this domain's Registrant, Administrative, or Technical contact, and such email address is not visible above, you may do so via our web form, pursuant to ICANN's Temporary Specification. To verify that you are not a robot, please enter your email address to receive a link to a page that facilitates email communication with the relevant contact(s).

Web-based WHOIS:  
<https://domains.markmonitor.com/whois>

If you have a legitimate interest in viewing the non-public WHOIS details, send your request and the reasons for your request to [whoisrequest@markmonitor.com](mailto:whoisrequest@markmonitor.com) and specify the domain name in the subject line. We will review that request and may ask for supporting documentation and explanation.

The data in MarkMonitor's WHOIS database is provided for information purposes, and to assist persons in obtaining information about or related to a domain name's registration record. While MarkMonitor believes the data to be accurate,

the data is provided "as is" with no guarantee or warranties regarding its accuracy.

By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data to:

- (1) allow, enable, or otherwise support the transmission by email, telephone, or facsimile of mass, unsolicited, commercial advertising, or spam; or
- (2) enable high volume, automated, or electronic processes that send queries, data, or email to MarkMonitor (or its systems) or the domain name contacts (or its systems).

MarkMonitor reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by this policy.

MarkMonitor Domain Management(TM)  
Protecting companies and consumers in a digital world.

Visit MarkMonitor at <https://www.markmonitor.com>

Contact us at +1.8007459229

In Europe, at +44.02032062220

--

Domain Name: google.com  
Registry Domain ID: 2138514\_DOMAIN\_COM-VRSN  
Registrar WHOIS Server: whois.markmonitor.com  
Registrar URL: <http://www.markmonitor.com>  
Updated Date: 2019-09-09T08:39:04-0700  
Creation Date: 1997-09-15T00:00:00-0700  
Registrar Registration Expiration Date: 2028-09-13T00:00:00-0700  
Registrar: MarkMonitor, Inc.  
Registrar IANA ID: 292  
Registrar Abuse Contact Email: [abusecomplaints@markmonitor.com](mailto:abusecomplaints@markmonitor.com)  
Registrar Abuse Contact Phone: +1.2083895770  
Domain Status: clientUpdateProhibited (<https://www.icann.org/epp#clientUpdateProhibited>)  
Domain Status: clientTransferProhibited (<https://www.icann.org/epp#clientTransferProhibited>)  
Domain Status: clientDeleteProhibited (<https://www.icann.org/epp#clientDeleteProhibited>)  
Domain Status: serverUpdateProhibited (<https://www.icann.org/epp#serverUpdateProhibited>)  
Domain Status: serverTransferProhibited (<https://www.icann.org/epp#serverTransferProhibited>)  
Domain Status: serverDeleteProhibited (<https://www.icann.org/epp#serverDeleteProhibited>)  
Registrant Organization: Google LLC  
Registrant State/Province: CA  
Registrant Country: US  
Registrant Email: Select Request Email Form at <https://domains.markmonitor.com/whois/google.com>  
Admin Organization: Google LLC  
Admin State/Province: CA  
Admin Country: US  
Admin Email: Select Request Email Form at <https://domains.markmonitor.com/whois/google.com>  
Tech Organization: Google LLC  
Tech State/Province: CA  
Tech Country: US  
Tech Email: Select Request Email Form at <https://domains.markmonitor.com/whois/google.com>  
Name Server: ns3.google.com  
Name Server: ns1.google.com  
Name Server: ns4.google.com  
Name Server: ns2.google.com

**DNSSEC: unsigned**

URL of the ICANN WHOIS Data Problem Reporting System: <http://wdprs.internic.net/>  
>>> Last update of WHOIS database: 2020-08-16T07:44:00-0700 <<<

For more information on WHOIS status codes, please visit:  
<https://www.icann.org/resources/pages/epp-status-codes>

If you wish to contact this domain's Registrant, Administrative, or Technical contact, and such email address is not visible above, you may do so via our web form, pursuant to ICANN's Temporary Specification. To verify that you are not a robot, please enter your email address to receive a link to a page that facilitates email communication with the relevant contact(s).

Web-based WHOIS:  
<https://domains.markmonitor.com/whois>

If you have a legitimate interest in viewing the non-public WHOIS details, send your request and the reasons for your request to [whoisrequest@markmonitor.com](mailto:whoisrequest@markmonitor.com) and specify the domain name in the subject line. We will review that request and may ask for supporting documentation and explanation.

The data in MarkMonitor's WHOIS database is provided for information purposes, and to assist persons in obtaining information about or related to a domain name's registration record. While MarkMonitor believes the data to be accurate, the data is provided "as is" with no guarantee or warranties regarding its accuracy.

By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data to:

- (1) allow, enable, or otherwise support the transmission by email, telephone, or facsimile of mass, unsolicited, commercial advertising, or spam; or
- (2) enable high volume, automated, or electronic processes that send queries, data, or email to MarkMonitor (or its systems) or the domain name contacts (or its systems).

MarkMonitor reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by this policy.

MarkMonitor Domain Management(TM)  
Protecting companies and consumers in a digital world.

Visit MarkMonitor at <https://www.markmonitor.com>  
Contact us at +1.800.745.9229  
In Europe, at +44.02032062220  
--

When maintaining a domain name, sometimes the domain registrar and domain information needs to be retrieved. To retrieve the information of your domain, you will need to look up the WHOIS information.

## CURL COMMAND:

**Geolocation** — A geolocation service tries to tell, approximately, where a given IP address is located physically. They can't be completely accurate—but they probably get at least the country right most of the time. This geolocation program is not installed on our computers, but you can access one on the command line using the curl command, which can send HTTP requests and display the response. The following command uses curl to contact a public web service that will look up an IP address for you: `curl ipinfo.io/<IP-address>`

IP ADDRESS of spit.ac.in was found using tracert and then curl command was executed for some valid nodes connected to it in the path.

```
C:\Users\Akshat>tracert spit.ac.in

Tracing route to spit.ac.in [43.252.193.19]
over a maximum of 30 hops:

  1    2 ms    1 ms    1 ms    jiofi.local.html [192.168.225.1]
  2    *        *        *        Request timed out.
  3   73 ms   60 ms   66 ms   10.71.18.18
  4   50 ms   38 ms   44 ms   192.168.69.160
  5   92 ms   67 ms   35 ms   192.168.69.161
  6   88 ms   44 ms   46 ms   172.16.80.113
  7   35 ms   38 ms   37 ms   172.17.119.5
  8    *        *        *        Request timed out.
  9    *        *        *        Request timed out.
 10    *        *        *        Request timed out.
 11    *        *        *        Request timed out.
 12    *        *        *        Request timed out.
 13   49 ms   48 ms   48 ms   115.110.206.73.static-Mumbai.vsnl.net.in [115.110.206.73]
 14    *        *        *        Request timed out.
 15    *        *        *        Request timed out.
 16   37 ms   51 ms   48 ms   115.113.165.174.static-mumbai.vsnl.net.in [115.113.165.174]
 17    *        *        *        Request timed out.
 18    *        *        *        Request timed out.
 19   86 ms   44 ms   40 ms   223-30-0-0.lan.sify.net [223.31.147.250]
 20   38 ms   48 ms   32 ms   27.109.1.150
 21   40 ms   48 ms   46 ms   103.205.124.82
 22   61 ms   37 ms   48 ms   43.252.192.230
 23    *        *        *        Request timed out.
 24    *        *        *        Request timed out.
 25    *        *        *        Request timed out.
 26    *        *        *        Request timed out.
 27    *        *        *        Request timed out.
 28    *        *        *        Request timed out.
 29    *        *        *        Request timed out.
 30    *        *        *        Request timed out.

Trace complete.
```

```
C:\>curl ipinfo.io/spit.ac.in
{
  "error": {
    "title": "Wrong ip",
    "message": "Please provide a valid IP address"
```

```
}
}
C:\>curl ipinfo.io/43.252.193.19
{
  "ip": "43.252.193.19",
  "city": "Mumbai",
  "region": "Maharashtra",
  "country": "IN",
  "loc": "19.0728,72.8826",
  "org": "AS17625 BlazeNet's Network",
  "postal": "400070",
  "timezone": "Asia/Kolkata",
  "readme": "https://ipinfo.io/missingauth"
}
C:\Users\Akshat>curl ipinfo.io/10.71.18.18
{
  "ip": "10.71.18.18",
  "bogon": true
}
C:\Users\Akshat>curl ipinfo.io/192.168.69.160
{
  "ip": "192.168.69.160",
  "bogon": true
}
C:\Users\Akshat>
C:\Users\Akshat>curl ipinfo.io/172.16.80.113
{
  "ip": "172.16.80.113",
  "bogon": true
}
C:\Users\Akshat>curl
ipinfo.io/115.110.206.73.static-Mumbai.vsnl.net.in
{
  "error": {
    "title": "Wrong ip",
    "message": "Please provide a valid IP address"
  }
}
C:\Users\Akshat>curl ipinfo.io/115.110.206.73
```

```
{
  "ip": "115.110.206.73",
  "hostname": "115.110.206.73.static-mumbai.vsnl.net.in",
  "city": "Bengaluru",
  "region": "Karnataka",
  "country": "IN",
  "loc": "12.9719,77.5937",
  "org": "AS4755 TATA Communications formerly VSNL is Leading
ISP",
  "postal": "560002",
  "timezone": "Asia/Kolkata",
  "readme": "https://ipinfo.io/missingauth"
}
```

C:\Users\Akshat>curl ipinfo.io/223.31.147.250

```
{
  "ip": "223.31.147.250",
  "hostname": "223-30-0-0.lan.sify.net",
  "city": "Mumbai",
  "region": "Maharashtra",
  "country": "IN",
  "loc": "19.0728,72.8826",
  "org": "AS9583 Sify Limited",
  "postal": "400070",
  "timezone": "Asia/Kolkata",
  "readme": "https://ipinfo.io/missingauth"
}
```

C:\Users\Akshat>curl ipinfo.io/43.252.192.230

```
{
  "ip": "43.252.192.230",
  "city": "Mumbai",
  "region": "Maharashtra",
  "country": "IN",
  "loc": "19.0728,72.8826",
  "org": "AS17625 BlazeNet's Network",
  "postal": "400070",
  "timezone": "Asia/Kolkata",
  "readme": "https://ipinfo.io/missingauth"
}
```

```
}
```

## References for this exercise:

1. [https://www.instructables.com/id/Find-the-IP-address-of-a-website-using-command-pro/#:~:text=Open%20command%20prompt%20and%20type,inserted\)\(the%20IP%20addresses\).](https://www.instructables.com/id/Find-the-IP-address-of-a-website-using-command-pro/#:~:text=Open%20command%20prompt%20and%20type,inserted)(the%20IP%20addresses).)
2. <https://www.site24x7.com/find-ip-address-of-web-site.html>

## IPCONFIG:

In computing, ipconfig is a console application of some operating systems that displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol and Domain Name System settings.

```
C:\Users\Akshat>ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter Ethernet:
```

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :
```

```
Ethernet adapter Ethernet 2:
```

```
Connection-specific DNS Suffix  . :
Link-local IPv6 Address . . . . . : fe80::fdab:5180:cbbb:4162%6
IPv4 Address. . . . . : 192.168.56.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

```
Wireless LAN adapter Local Area Connection* 1:
```

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :
```

```
Wireless LAN adapter Local Area Connection* 2:
```

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :
```

Wireless LAN adapter Wi-Fi:

```
Connection-specific DNS Suffix  . :
IPv6 Address. . . . . :
2405:204:2298:e189:1cbe:b764:f1c3:c215
Temporary IPv6 Address. . . . . :
2405:204:2298:e189:c9c7:4332:cde7:205f
Link-local IPv6 Address . . . . . :
fe80::1cbe:b764:f1c3:c215%5
IPv4 Address. . . . . : 192.168.225.215
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
fe80::b9a3:4e27:82c6:3ad7%5
                                192.168.225.1
```

## NSLOOKUP:

nslookup is a network administration command-line tool available in many computer operating systems for querying the Domain Name System to obtain domain name or IP address mapping, or other DNS records.

```
C:\Users\Akshat>nslookup www.google.com
Server:  jiofi.local.html
Address:  192.168.225.1
```

```
Non-authoritative answer:
Name:     www.google.com
Addresses:  2404:6800:4009:803::2004
           172.217.160.196
```

## CONCLUSION:

Through this experiment, I understood and implemented commands for basic networking utilities. I gained knowledge about how sending and receiving of packets takes place. Different routes are chosen given certain conditions like number of hops and size of packets. Distance plays a very important role in the transmission of packets.