NAME: SAKSHI CHHEDA
ROLL NO: 7
UID: 2018130005
BATCH: A
CLASS: T.E. COMPS

# CEL 51, DCCN, Monsoon 2020
# Lab 2: Basic Network Utilities

This lab introduces some basic network monitoring/analysis tools. There are a few exercises along the way. You should write up answers to the ***ping*** and ***traceroute*** exercises and turn them in the next lab. (You should try out each tool, whether it is needed for an exercise or not!).

Prerequisite: Basic understanding of command line utilities of Linux Operating system.

## Some Basic command line Networking utilities

Start with a few of the most basic command line tools. These commands are available on Unix, including Linux (and the first two, at least, are also for Windows). Some parameters or options might differ on different operating systems. Remember that you can use man <command> to get information about a command and its options.

**ping** — The command ping <host> sends a series of packets and expects to receive a response to each packet. When a return packet is received, ping reports the round trip time (the time between sending the packet and receiving the response). Some routers and firewalls block ping requests, so you might get no response at all. Ping can be used to check whether a computer is up and running, to measure network delay time, and to check for dropped packets indicating network congestion. Note that <host> can be either a domain name or an IP address. By default, ping will send a packet every second indefinitely; stop it with Control-C

Network latency, specifically round trip time (RTT), can be measured using ping, which sends ICMP packets. The syntax for the command in Linux or Mac OS is:

```
ping [-c <count>] [-s <packetsize>] <hostname>
```

The syntax in Windows is:

```
ping [-n <count>] [-l <packetsize>] <hostname>
```

The default number of ICMP packets to send is either infinite (in Linux and Mac OS) or 4 (in Windows). The default packet size is either 64 bytes (in Linux) or 32 bytes (in Windows). You can specify either a hostname (e.g., spit.ac.in) or an IP address.

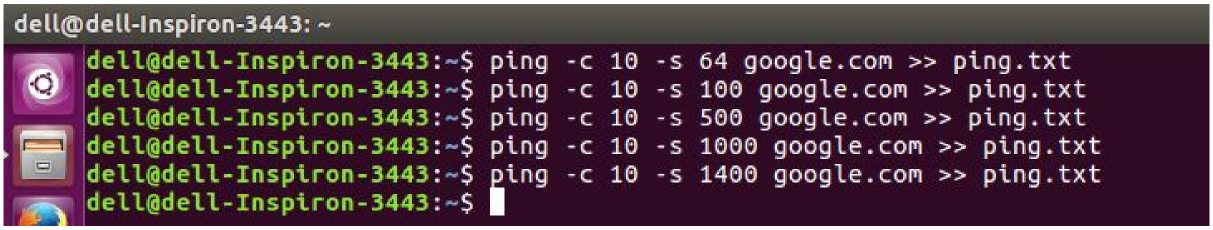
To save the output from ping to a file, include a greater than symbol and a file name at the end of the command. For example:

```
ping -c 10 google.com > ping_c10_s64_google.log
```

**EXPERIMENTS WITH PING**

1. 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

### a. Host : google.com



```
dell@dell-Inspiron-3443:~$ ping -c 10 -s 64 google.com >> ping.txt
dell@dell-Inspiron-3443:~$ ping -c 10 -s 100 google.com >> ping.txt
dell@dell-Inspiron-3443:~$ ping -c 10 -s 500 google.com >> ping.txt
dell@dell-Inspiron-3443:~$ ping -c 10 -s 1000 google.com >> ping.txt
dell@dell-Inspiron-3443:~$ ping -c 10 -s 1400 google.com >> ping.txt
dell@dell-Inspiron-3443:~$
```

**Output in ping.txt :**

PING google.com (172.217.167.174) **64(92) bytes** of data.

72 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=1 ttl=119 time=2.24 ms

72 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=2 ttl=119 time=3.30 ms

72 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=3 ttl=119 time=2.70 ms

72 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=4 ttl=119 time=3.03 ms

72 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=5 ttl=119 time=2.45 ms

72 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=6 ttl=119 time=3.48 ms

72 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=7 ttl=119 time=2.50 ms

72 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=8 ttl=119 time=2.47 ms

```
72 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=9 ttl=119 time=4.69 ms
72 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=10 ttl=119 time=3.74 ms

--- google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 2.249/3.065/4.698/0.723 ms

PING google.com (172.217.166.46) 100(128) bytes of data.
76 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=1 ttl=119 (truncated)
76 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=2 ttl=119 (truncated)
76 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=3 ttl=119 (truncated)
76 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=4 ttl=119 (truncated)
76 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=5 ttl=119 (truncated)
76 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=6 ttl=119 (truncated)
76 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=7 ttl=119 (truncated)
76 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=8 ttl=119 (truncated)
76 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=9 ttl=119 (truncated)
76 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=10 ttl=119 (truncated)

--- google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 2.410/3.220/4.921/0.836 ms

PING google.com (172.217.167.174) 500(528) bytes of data.
76 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=1 ttl=119 (truncated)
76 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=2 ttl=119 (truncated)
76 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=3 ttl=119 (truncated)
76 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=4 ttl=119 (truncated)
76 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=5 ttl=119 (truncated)
76 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=6 ttl=119 (truncated)
76 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=7 ttl=119 (truncated)
76 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=8 ttl=119 (truncated)
76 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=9 ttl=119 (truncated)

--- google.com ping statistics ---
10 packets transmitted, 9 received, 10% packet loss, time 9012ms
rtt min/avg/max/mdev = 2.215/3.515/6.118/1.240 ms

PING google.com (172.217.166.46) 1000(1028) bytes of data.
76 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=1 ttl=119 (truncated)
76 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=2 ttl=119 (truncated)
```

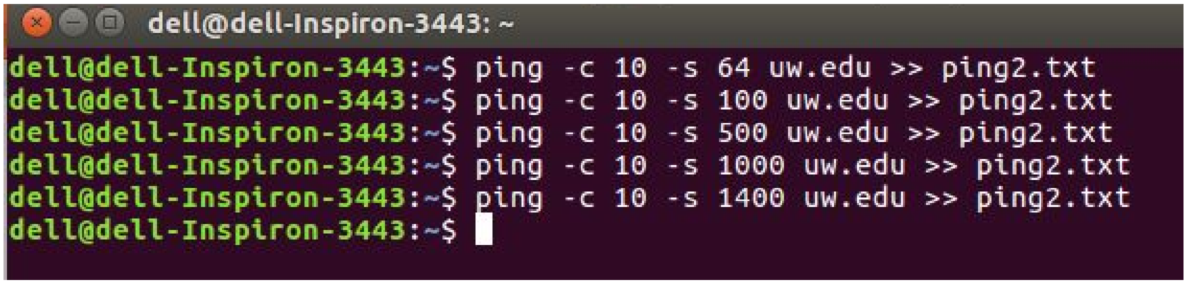
```
76 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=3 ttl=119 (truncated)
76 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=4 ttl=119 (truncated)
76 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=5 ttl=119 (truncated)
76 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=6 ttl=119 (truncated)
76 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=7 ttl=119 (truncated)
76 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=8 ttl=119 (truncated)
76 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=9 ttl=119 (truncated)
76 bytes from bom07s18-in-f14.1e100.net (172.217.166.46): icmp_seq=10 ttl=119 (truncated)

--- google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 2.660/4.263/10.915/2.347 ms

PING google.com (172.217.167.174) 1400(1428) bytes of data.
76 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=1 ttl=119 (truncated)
76 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=2 ttl=119 (truncated)
76 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=3 ttl=119 (truncated)
76 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=4 ttl=119 (truncated)
76 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=5 ttl=119 (truncated)
76 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=6 ttl=119 (truncated)
76 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=7 ttl=119 (truncated)
76 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=8 ttl=119 (truncated)
76 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=9 ttl=119 (truncated)
76 bytes from bom12s01-in-f14.1e100.net (172.217.167.174): icmp_seq=10 ttl=119 (truncated)

--- google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9012ms
rtt min/avg/max/mdev = 3.075/4.513/6.395/0.982 ms
```

### b. Host : uw.edu



```
dell@dell-Inspiron-3443:~$ ping -c 10 -s 64 uw.edu >> ping2.txt
dell@dell-Inspiron-3443:~$ ping -c 10 -s 100 uw.edu >> ping2.txt
dell@dell-Inspiron-3443:~$ ping -c 10 -s 500 uw.edu >> ping2.txt
dell@dell-Inspiron-3443:~$ ping -c 10 -s 1000 uw.edu >> ping2.txt
dell@dell-Inspiron-3443:~$ ping -c 10 -s 1400 uw.edu >> ping2.txt
dell@dell-Inspiron-3443:~$
```

### Output in ping2.txt :

```
PING uw.edu (128.95.155.197) 64(92) bytes of data.
72 bytes from www3.cac.washington.edu (128.95.155.197): icmp_seq=1 ttl=46 time=246 ms
```

```
72 bytes from www3.cac.washington.edu (128.95.155.197): icmp_seq=2 ttl=46 time=247 ms
72 bytes from www3.cac.washington.edu (128.95.155.197): icmp_seq=3 ttl=46 time=374 ms
72 bytes from www3.cac.washington.edu (128.95.155.197): icmp_seq=4 ttl=46 time=252 ms
72 bytes from www3.cac.washington.edu (128.95.155.197): icmp_seq=5 ttl=46 time=247 ms
72 bytes from www3.cac.washington.edu (128.95.155.197): icmp_seq=6 ttl=46 time=247 ms
72 bytes from www3.cac.washington.edu (128.95.155.197): icmp_seq=7 ttl=46 time=248 ms
72 bytes from www3.cac.washington.edu (128.95.155.197): icmp_seq=9 ttl=46 time=247 ms
72 bytes from www3.cac.washington.edu (128.95.155.197): icmp_seq=10 ttl=46 time=250 ms

--- uw.edu ping statistics ---
10 packets transmitted, 9 received, 10% packet loss, time 9019ms
rtt min/avg/max/mdev = 246.916/262.509/374.078/39.483 ms

PING uw.edu (128.95.155.197) 100(128) bytes of data.
108 bytes from www3.cac.washington.edu (128.95.155.197): icmp_seq=1 ttl=46 time=245 ms
108 bytes from www3.cac.washington.edu (128.95.155.197): icmp_seq=2 ttl=46 time=245 ms
108 bytes from www3.cac.washington.edu (128.95.155.197): icmp_seq=3 ttl=46 time=246 ms
108 bytes from www3.cac.washington.edu (128.95.155.197): icmp_seq=4 ttl=46 time=246 ms
108 bytes from www3.cac.washington.edu (128.95.155.197): icmp_seq=5 ttl=46 time=245 ms
108 bytes from www3.cac.washington.edu (128.95.155.197): icmp_seq=6 ttl=46 time=245 ms
108 bytes from www3.cac.washington.edu (128.95.155.197): icmp_seq=7 ttl=46 time=253 ms
108 bytes from www3.cac.washington.edu (128.95.155.197): icmp_seq=8 ttl=46 time=247 ms
108 bytes from www3.cac.washington.edu (128.95.155.197): icmp_seq=9 ttl=46 time=248 ms
108 bytes from www3.cac.washington.edu (128.95.155.197): icmp_seq=10 ttl=46 time=245 ms

--- uw.edu ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9011ms
rtt min/avg/max/mdev = 245.134/246.918/253.289/2.466 ms

PING uw.edu (54.214.77.106) 500(528) bytes of data.

--- uw.edu ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 8999ms

PING uw.edu (54.214.77.106) 1000(1028) bytes of data.

--- uw.edu ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9070ms

PING uw.edu (128.95.155.135) 1400(1428) bytes of data.
1408 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=1 ttl=44 time=244 ms
1408 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=2 ttl=44 time=243 ms
1408 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=3 ttl=44 time=245 ms
```

```
1408 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=5 ttl=44 time=245 ms
1408 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=6 ttl=44 time=245 ms
1408 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=7 ttl=44 time=244 ms
1408 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=8 ttl=44 time=246 ms
1408 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=9 ttl=44 time=252 ms
1408 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=10 ttl=44 time=243 ms

--- uw.edu ping statistics ---
10 packets transmitted, 9 received, 10% packet loss, time 9010ms
rtt min/avg/max/mdev = 243.280/245.802/252.993/2.744 ms
```

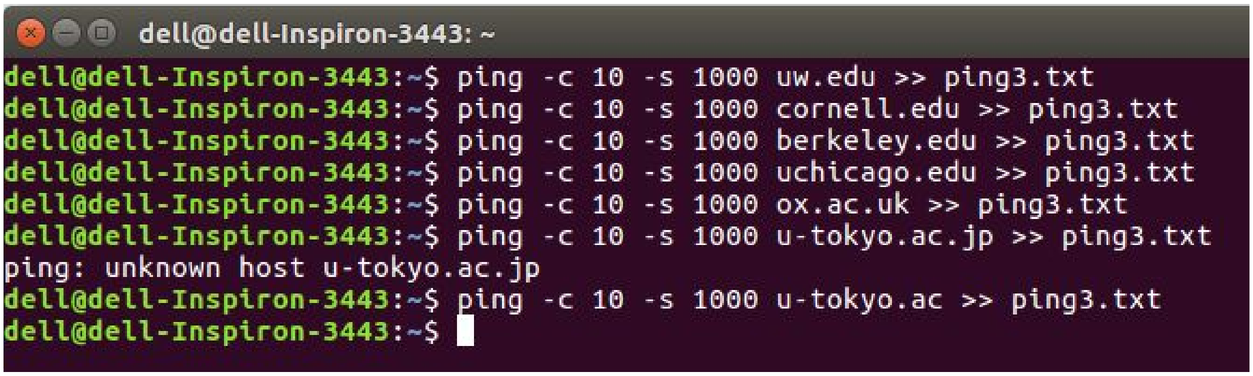
## OBSERVATIONS:

Round trip time can be influenced by[3]:

- **Distance** – The length a signal has to travel correlates with the time taken for a request to reach a server and a response to reach a browser.
- **Transmission medium** – The medium used to route a signal (e.g., copper wire, fiber optic cables) can impact how quickly a request is received by a server and routed back to a user.
- **Number of hops** – Intermediate routers or servers take time to process a signal, increasing RTT. The more hops a signal has to travel through, the higher the RTT.
- **Traffic intensity**– RTT typically increases when a network is congested with high levels of traffic. Conversely, low traffic times can result in decreased RTT.
- **Server response time** – The time taken for a target server to respond to a request depends on its processing capacity, the number of requests being handled and the nature of the request (i.e., how much server-side work is required). A longer server response time increases RTT.

**Exercise 1**: Experiment with ping to find the round trip times to a variety of destinations. Write up any observations, including in particular how the round trip time compares to the physical distance. Here are few places from who to get replies: www.uw.edu, www.cornell.edu, berkeley.edu, www.uchicago.edu, www.ox.ac.uk (England), www.u-tokyo.ac.jp (Japan).

Ping command for all hosts :



```
dell@dell-Inspiron-3443:~$ ping -c 10 -s 1000 uw.edu >> ping3.txt
dell@dell-Inspiron-3443:~$ ping -c 10 -s 1000 cornell.edu >> ping3.txt
dell@dell-Inspiron-3443:~$ ping -c 10 -s 1000 berkeley.edu >> ping3.txt
dell@dell-Inspiron-3443:~$ ping -c 10 -s 1000 uchicago.edu >> ping3.txt
dell@dell-Inspiron-3443:~$ ping -c 10 -s 1000 ox.ac.uk >> ping3.txt
dell@dell-Inspiron-3443:~$ ping -c 10 -s 1000 u-tokyo.ac.jp >> ping3.txt
ping: unknown host u-tokyo.ac.jp
dell@dell-Inspiron-3443:~$ ping -c 10 -s 1000 u-tokyo.ac >> ping3.txt
dell@dell-Inspiron-3443:~$
```

Output for all hosts in ping3.txt:

### 1. Host : uw.edu (Washington,USA)

```
PING uw.edu (128.95.155.135) 1000(1028) bytes of data.
1008 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=1 ttl=47 time=237 ms
1008 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=2 ttl=47 time=243 ms
1008 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=3 ttl=47 time=236 ms
1008 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=4 ttl=47 time=236 ms
1008 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=5 ttl=47 time=238 ms
1008 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=6 ttl=47 time=236 ms
1008 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=7 ttl=47 time=236 ms
1008 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=8 ttl=47 time=237 ms
1008 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=9 ttl=47 time=236 ms
1008 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=10 ttl=47 time=237 ms

--- uw.edu ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9013ms
rtt min/avg/max/mdev = 236.701/237.793/243.744/2.034 ms
```

### 2. Host : cornell.edu (NewYork,USA)

```
PING cornell.edu (128.253.173.242) 1000(1028) bytes of data.

--- cornell.edu ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9072ms
```

### 3. Host : berkeley.edu (California,USA)

```
PING berkeley.edu (35.163.72.93) 1000(1028) bytes of data.
```

```
1008 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93):
icmp_seq=1 ttl=33 time=263 ms
1008 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93):
icmp_seq=2 ttl=33 time=263 ms
1008 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93):
icmp_seq=3 ttl=33 time=263 ms
1008 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93):
icmp_seq=4 ttl=33 time=265 ms
1008 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93):
icmp_seq=5 ttl=33 time=263 ms
1008 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93):
icmp_seq=6 ttl=33 time=266 ms
1008 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93):
icmp_seq=7 ttl=33 time=266 ms
1008 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93):
icmp_seq=8 ttl=33 time=263 ms
1008 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93):
icmp_seq=9 ttl=33 time=264 ms
1008 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93):
icmp_seq=10 ttl=33 time=263 ms

--- berkeley.edu ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9002ms
rtt min/avg/max/mdev = 263.103/264.316/266.499/1.346 ms
```

### 4. Host : uchicago.edu (Illinois,USA)

```
PING uchicago.edu (34.200.129.209) 1000(1028) bytes of data.

--- uchicago.edu ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9072ms
```

### 5. Host : ox.ac.uk (Oxford,England)

```
PING ox.ac.uk (151.101.2.133) 1000(1028) bytes of data.
1008 bytes from 151.101.2.133: icmp_seq=1 ttl=59 time=2.52 ms
1008 bytes from 151.101.2.133: icmp_seq=2 ttl=59 time=4.07 ms
1008 bytes from 151.101.2.133: icmp_seq=3 ttl=59 time=2.64 ms
1008 bytes from 151.101.2.133: icmp_seq=4 ttl=59 time=3.37 ms
1008 bytes from 151.101.2.133: icmp_seq=5 ttl=59 time=3.44 ms
1008 bytes from 151.101.2.133: icmp_seq=6 ttl=59 time=3.28 ms
1008 bytes from 151.101.2.133: icmp_seq=7 ttl=59 time=5.79 ms
1008 bytes from 151.101.2.133: icmp_seq=8 ttl=59 time=4.61 ms
1008 bytes from 151.101.2.133: icmp_seq=9 ttl=59 time=18.9 ms
1008 bytes from 151.101.2.133: icmp_seq=10 ttl=59 time=5.74 ms
```

```
--- ox.ac.uk ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 2.526/5.445/18.959/4.634 ms
```

### 6. Host : u-tokyo.ac (Japan)

```
PING u-tokyo.ac (3.96.23.237) 1000(1028) bytes of data.

--- u-tokyo.ac ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9071ms
```

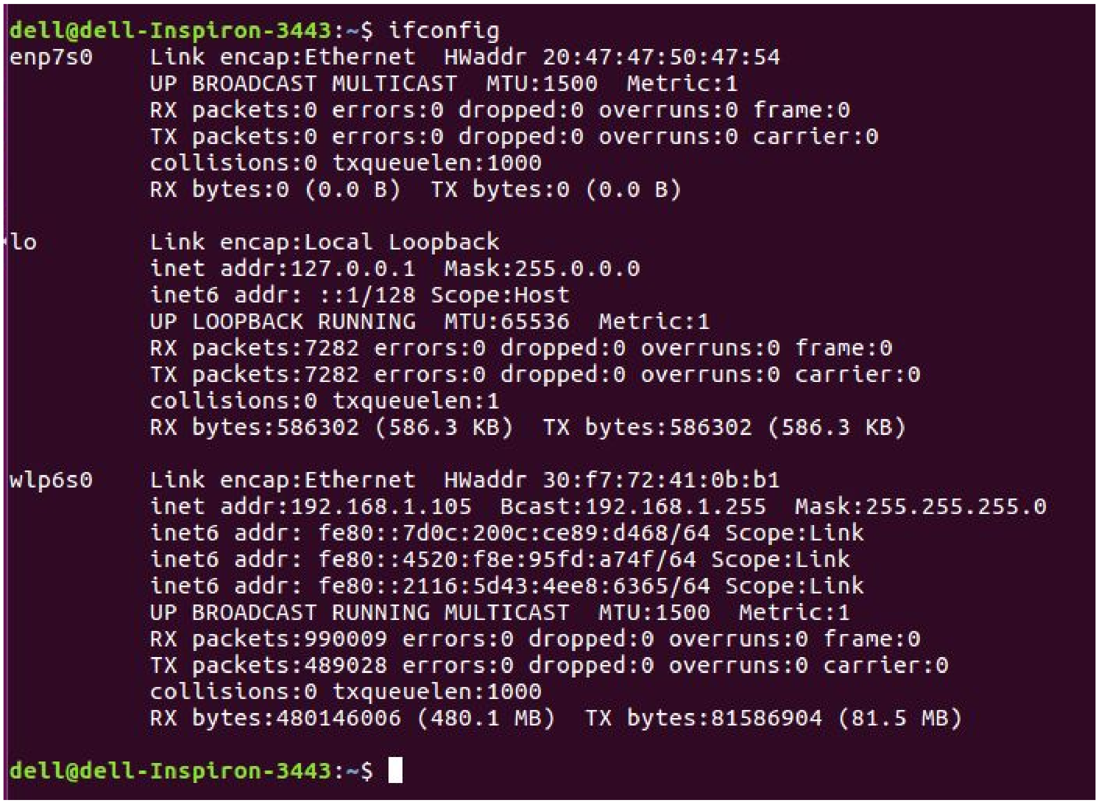
**OBSERVATIONS:**

- Some of the sites did not have their server open to ICMP requests and so there was 100% packet loss.
- RTT depends on the distance between my device and the host server. Pinging www.uw.edu in Washington,USA took an average of 237.793 ms whereas pinging www.ox.ac.uk in England took an average of 5.445 ms.

**nslookup** — The command nslookup <host> will do a DNS query to find and report the IP address (or addresses) for a domain name or the domain name corresponding to an IP address. To do this, it contacts a "DNS server." Default DNS servers are part of a computer's network configuration. (For a static IP address in Linux, they are configured in the file /etc/network/interfaces that you encountered in the last lab.) You can specify a different DNS server to be used by nslookup by adding the server name or IP address to the command: nslookup <host> <server>

**ifconfig** — You used ifconfig in the previous lab. When used with no parameters, ifconfig reports some information about the computer's network interfaces. This usually includes lo which stands for localhost; it can be used for communication between programs running on the same computer. Linux often has an interface named eth0, which is the first ethernet card. The information is different on Mac OS and Linux, but includes the IP or "inet" address and ethernet or "hardware" address for an ethernet card. On Linux, you get the number of packets received (RX) and sent (TX), as well as the number of bytes transmitted and received. (A better place to monitor network bytes on our Linux computers is in the GUI program System Monitor, if it is installed!!!.)

The ifconfig command :



```
dell@dell-Inspiron-3443:~$ ifconfig
enp7s0    Link encap:Ethernet  HWaddr 20:47:47:50:47:54
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:7282 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7282 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:586302 (586.3 KB)  TX bytes:586302 (586.3 KB)

wlp6s0    Link encap:Ethernet  HWaddr 30:f7:72:41:0b:b1
          inet addr:192.168.1.105  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::7d0c:200c:ce89:d468/64 Scope:Link
          inet6 addr: fe80::4520:f8e:95fd:a74f/64 Scope:Link
          inet6 addr: fe80::2116:5d43:4ee8:6365/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:990009 errors:0 dropped:0 overruns:0 frame:0
          TX packets:489028 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:480146006 (480.1 MB)  TX bytes:81586904 (81.5 MB)

dell@dell-Inspiron-3443:~$ 
```

**netstat** — The netstat command gives information about network connections. I often use netstat -t -n which lists currently open TCP connections (that's the "-t" option) by IP address rather than domain name (that's the "-n" option). Add the option "-l" (lower case ell) to list listening sockets, that is sockets that have been opened by server programs to wait for connection requests from clients: netstat -t -n -l. (On Mac, use netstat -p tcp to list tcp connections, and add "-a" to include listening sockets in the list.)

**telnet** — Telnet is an old program for remote login. It's not used so much for that any more, since it has no security features. But basically, all it does is open a connection to a server and allow server and client to send lines of plain text to each other. It can be used to check that it's possible to connect to a server and, if the server communicates in plain text, even to interact with the server by hand. Since the Web uses a plain text protocol, you can use telnet to connect to a web client and play the part of the web browser. I will suggest that you to do this with your own web server when you write it, but you might want to try it now. When you use telnet in this way, you need to specify both the host and the port number to which you want to connect: telent <host> <port>. For example, to connect to the web server on www.spit.ac.in: telnet spit.ac.in 80

**traceroute** — Traceroute is discussed in man utility. The command traceroute <host> will show routers encountered by packets on their way from your computer to a specified <host>. For each n = 1, 2, 3,..., traceroute sends a packet with "time-to-live" (ttl) equal to n. Every time a router forwards a packet, it decreases the ttl of the packet by one. If the ttl drops to zero, the router discards the packet and sends an error message back to the sender of the packet. (Again, as with ping, the packets might be blocked or might not even be sent, so that the error messages will never be received.) The sender gets the identity of the router from the source of the error message. Traceroute will send packets until n reaches some set upper bound or until a packet actually gets through to the destination. It actually does this three times for each n. In this way, it identifies routers that are one step, two steps, three steps, ... away from the source computer. A packet for which no response is received is indicated in the output as a *.

Traceroute is installed on the computers. If was not installed in your virtual server last week, but you can install it with the command sudo apt-get install traceroute

The path taken through a network can be measured using traceroute. The syntax for the command in Linux is:

```
traceroute <hostname>
```

The syntax in Windows is:

```
tracert <hostname>
```

You can specify either a hostname (e.g., cs.iitb.ac.in) or an IP address (e.g., 128.105.2.6).

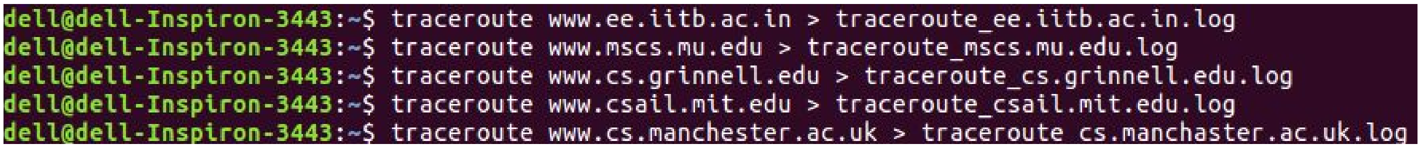
### 1.2.1 EXPERIMENTS WITH TRACEROUTE

From **your machine** traceroute to the following hosts:

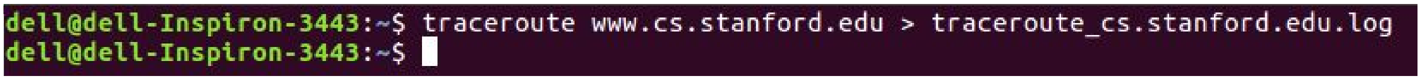
1. ee.iitb.ac.in
2. mscs.mu.edu
3. www.cs.grinnell.edu
4. csail.mit.edu
5. cs.stanford.edu
6. cs.manchester.ac.uk

Store the output of each traceroute command in a separate file named traceroute_HOSTNAME.log, replacing HOSTNAME with the hostname for end-host you pinged (e.g., traceroute_ee.iitb.ac.in.log).

Command for all hosts :



```
dell@dell-Inspiron-3443:~$ traceroute www.ee.iitb.ac.in > traceroute_ee.iitb.ac.in.log
dell@dell-Inspiron-3443:~$ traceroute www.mscs.mu.edu > traceroute_mscs.mu.edu.log
dell@dell-Inspiron-3443:~$ traceroute www.cs.grinnell.edu > traceroute_cs.grinnell.edu.log
dell@dell-Inspiron-3443:~$ traceroute www.csail.mit.edu > traceroute_csail.mit.edu.log
dell@dell-Inspiron-3443:~$ traceroute www.cs.manchester.ac.uk > traceroute_cs.manchaster.ac.uk.log
```



```
dell@dell-Inspiron-3443:~$ traceroute www.cs.stanford.edu > traceroute_cs.stanford.edu.log
dell@dell-Inspiron-3443:~$ 
```

Output for all hosts:

**1. Tracing route to www.ee.iitb.ac.in**

```
traceroute to www.ee.iitb.ac.in (103.21.125.132), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  0.427 ms  1.365 ms  1.365 ms
 2  1.16.16.172 (1.16.16.172)  2.320 ms  2.373 ms  2.469 ms
 3  103.88.221.177 (103.88.221.177)  3.319 ms  3.419 ms  3.675 ms
 4  103.27.170.25 (103.27.170.25)  3.347 ms  3.499 ms  3.631 ms
 5  aipl-49-65-179-202.ankhnet.net (202.179.65.49)  4.072 ms  4.067 ms  4.047 ms
 6  218.100.48.78 (218.100.48.78)  4.195 ms  3.889 ms  3.794 ms
 7  172.23.78.233 (172.23.78.233)  3.782 ms *  3.771 ms
 8  172.23.78.238 (172.23.78.238)  4.279 ms  4.257 ms  4.271 ms
 9  115.113.165.62.static-mumbai.vsnl.net.in (115.113.165.62)  5.781 ms  6.004 ms  6.372 ms
10  * * *
11  * * *
12  115.110.234.170.static.Mumbai.vsnl.net.in (115.110.234.170)  5.238 ms  5.240 ms  5.236 ms
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
```

```
27  * * *
28  * * *
29  * * *
30  * * *
```

## 2. Tracing route to www.mscs.mu.edu

```
traceroute to www.mscs.mu.edu (134.48.4.34), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  6.280 ms  6.281 ms  6.278 ms
 2  1.16.16.172 (1.16.16.172)  2.422 ms  3.887 ms  3.901 ms
 3  103.88.221.177 (103.88.221.177)  7.233 ms  7.843 ms  7.920 ms
 4  undefined.hostname.localhost (103.214.130.129)  19.964 ms  20.079 ms  20.080 ms
 5  219.65.79.57.static-mumbai.vsnl.net.in (219.65.79.57)  6.221 ms  6.220 ms  6.217 ms
 6  172.23.78.233 (172.23.78.233)  6.216 ms  3.843 ms  5.036 ms
 7  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net (180.87.38.5)  5.265 ms  3.820 ms  3.780 ms
 8  if-ae-5-2.tcore1.wyn-marseille.as6453.net (80.231.217.29)  141.756 ms  141.716 ms
141.727 ms
 9  if-ae-21-2.tcore1.pye-paris.as6453.net (80.231.154.208)  141.696 ms
if-ae-8-1600.tcore1.pye-paris.as6453.net (80.231.217.6)  141.705 ms  141.691 ms
10  if-ae-11-2.tcore1.pvu-paris.as6453.net (80.231.153.49)  141.689 ms  141.677 ms  141.668
ms
11  * * *
12  * * *
13  MARQUETTE-U.ear3.Chicago2.Level3.net (4.16.38.70)  226.187 ms  235.545 ms  235.544
ms
14  134.48.10.26 (134.48.10.26)  251.087 ms  251.059 ms  251.080 ms
15  * * *
16  * * *
17  turing.mscs.mu.edu (134.48.4.34)  246.166 ms  245.246 ms  245.469 ms
```

## 3. Tracing route to www.cs.grinnell.edu

```
traceroute to www.cs.grinnell.edu (132.161.132.159), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  1.849 ms  1.834 ms  1.830 ms
 2  1.16.16.172 (1.16.16.172)  2.759 ms  2.853 ms  2.956 ms
 3  103.88.221.177 (103.88.221.177)  2.190 ms  2.839 ms  3.047 ms
 4  * * *
 5  219.65.79.57.static-mumbai.vsnl.net.in (219.65.79.57)  7.089 ms  7.087 ms  7.084 ms
 6  172.23.78.233 (172.23.78.233)  7.770 ms  10.088 ms  3.182 ms
 7  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net (180.87.38.5)  9.313 ms  9.314 ms  9.305 ms
 8  if-ae-5-2.tcore1.wyn-marseille.as6453.net (80.231.217.29)  128.819 ms  128.834 ms
128.833 ms
 9  if-ae-8-1600.tcore1.pye-paris.as6453.net (80.231.217.6)  129.001 ms  128.825 ms
if-ae-21-2.tcore1.pye-paris.as6453.net (80.231.154.208)  128.803 ms
```

```
10  if-ae-11-2.tcore1.pvu-paris.as6453.net (80.231.153.49)  128.806 ms  128.796 ms  125.687
ms
11  be6453.agr21.par04.atlas.cogentco.com (130.117.15.69)  224.117 ms  218.729 ms
218.717 ms
12  be3169.ccr31.par04.atlas.cogentco.com (154.54.37.237)  218.714 ms  224.700 ms
224.685 ms
13  be3183.ccr41.par01.atlas.cogentco.com (154.54.38.65)  224.643 ms
be3184.ccr42.par01.atlas.cogentco.com (154.54.38.157)  224.678 ms
be2103.ccr42.par01.atlas.cogentco.com (154.54.61.21)  224.679 ms
14  be12497.ccr41.lon13.atlas.cogentco.com (154.54.56.129)  224.680 ms
be12489.ccr42.lon13.atlas.cogentco.com (154.54.57.69)  224.677 ms
be12497.ccr41.lon13.atlas.cogentco.com (154.54.56.129)  224.664 ms
15  be2101.ccr32.bos01.atlas.cogentco.com (154.54.82.38)  224.577 ms  240.613 ms
be2099.ccr31.bos01.atlas.cogentco.com (154.54.82.34)  240.614 ms
16  be3600.ccr22.alb02.atlas.cogentco.com (154.54.0.221)  240.611 ms
be3599.ccr21.alb02.atlas.cogentco.com (66.28.4.237)  240.611 ms
be3600.ccr22.alb02.atlas.cogentco.com (154.54.0.221)  227.822 ms
17  be2879.ccr22.cle04.atlas.cogentco.com (154.54.29.173)  238.663 ms  238.656 ms  238.621
ms
18  be2718.ccr42.ord01.atlas.cogentco.com (154.54.7.129)  240.252 ms  240.223 ms  238.601
ms
19  be2640.rcr21.dsm01.atlas.cogentco.com (154.54.29.126)  244.477 ms  244.749 ms
be2639.rcr21.dsm01.atlas.cogentco.com (154.54.29.50)  248.388 ms
20  38.104.184.50 (38.104.184.50)  219.165 ms  219.177 ms  219.175 ms
21  ins-dc2-et-0-0-1-1.desm.netins.net (167.142.67.17)  220.177 ms  220.584 ms
167.142.58.40 (167.142.58.40)  220.585 ms
22  167.142.219.32 (167.142.219.32)  221.765 ms 167.142.67.141 (167.142.67.141)  220.567
ms  220.162 ms
23  grinnellcollege1.desm.netins.net (167.142.65.43)  220.158 ms  219.994 ms  221.084 ms
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

### 4. Tracing route to www.csail.mit.edu

```
traceroute to www.csail.mit.edu (23.185.0.3), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  1.864 ms  1.850 ms  1.846 ms
 2  1.16.16.172 (1.16.16.172)  2.863 ms  2.964 ms  3.066 ms
 3  103.88.221.177 (103.88.221.177)  2.238 ms  2.735 ms  2.835 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

### 5. Tracing route to www.cs.stanford.edu

```
traceroute to www.cs.stanford.edu (171.64.64.64), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  0.683 ms  0.678 ms  1.266 ms
 2  1.16.16.172 (1.16.16.172)  2.516 ms  2.524 ms  2.522 ms
 3  103.88.221.177 (103.88.221.177)  3.142 ms  3.151 ms  3.150 ms
 4  * * *
 5  103.88.220.233 (103.88.220.233)  3.586 ms  3.489 ms  3.568 ms
 6  undefined.hostname.localhost (103.214.130.129)  4.303 ms  3.642 ms  3.686 ms
 7  219.65.79.57.static-mumbai.vsnl.net.in (219.65.79.57)  3.400 ms  3.399 ms  3.395 ms
 8  172.23.78.233 (172.23.78.233)  3.393 ms  3.389 ms  3.387 ms
 9  172.31.244.45 (172.31.244.45)  20.231 ms  28.646 ms  20.240 ms
10  ix-ae-4-2.tcore2.cxr-chennai.as6453.net (180.87.37.1)  36.621 ms  36.636 ms  36.620 ms
11  * * *
12  if-ae-7-2.tcore2.lvw-losangeles.as6453.net (180.87.15.26)  227.245 ms  236.648 ms
230.286 ms
```

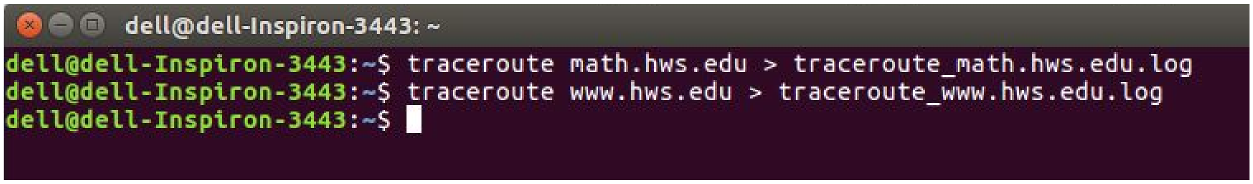
```
13  if-ae-2-2.tcore1.lvw-losangeles.as6453.net (66.110.59.1)  231.354 ms  242.252 ms  242.208
ms
14  las-b24-link.telia.net (80.239.128.214)  268.255 ms  260.280 ms  260.262 ms
15  palo-b24-link.telia.net (62.115.119.90)  260.244 ms  255.733 ms *
16  palo-b1-link.telia.net (62.115.122.169)  251.622 ms  246.344 ms  248.615 ms
17  hurricane-ic-308019-palo-b1.c.telia.net (80.239.167.174)  242.715 ms  267.707 ms  267.689
ms
18  stanford-university.100gigabitethernet5-1.core1.pao1.he.net (184.105.177.238)  267.677 ms
267.650 ms  249.268 ms
19  csee-west-rtr-vl3.SUNet (171.66.255.140)  245.009 ms  247.784 ms  243.610 ms
20  CS.stanford.edu (171.64.64.64)  251.697 ms  248.720 ms  245.291 ms
```

### 6. Tracing route to www.cs.manchester.ac.uk

```
traceroute to www.cs.manchester.ac.uk (130.88.101.49), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  8.400 ms  8.393 ms  8.389 ms
 2  1.16.16.172 (1.16.16.172)  6.914 ms  6.918 ms  6.916 ms
 3  103.88.221.177 (103.88.221.177)  6.912 ms  6.909 ms  6.907 ms
 4  undefined.hostname.localhost (103.214.130.129)  6.905 ms  6.901 ms  6.898 ms
 5  219.65.79.57.static-mumbai.vsnl.net.in (219.65.79.57)  8.323 ms  8.310 ms  8.313 ms
 6  172.23.78.233 (172.23.78.233)  8.298 ms  6.627 ms  11.945 ms
 7  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net (180.87.38.5)  6.377 ms  6.375 ms  6.369 ms
 8  if-ae-5-2.tcore1.wyn-marseille.as6453.net (80.231.217.29)  119.587 ms  119.604 ms
119.604 ms
 9  if-ae-8-1600.tcore1.pye-paris.as6453.net (80.231.217.6)  130.194 ms  127.342 ms  127.333
ms
10  if-ae-11-2.tcore1.pvu-paris.as6453.net (80.231.153.49)  146.747 ms  146.700 ms  146.713
ms
11  * * *
12  * * *
13  JANET.bear1.Manchester1.Level3.net (212.187.174.238)  130.172 ms  129.983 ms
130.616 ms
14  ae22.manckh-sbr2.ja.net (146.97.35.189)  146.751 ms  135.248 ms  135.195 ms
15  ae23.mancrh-rbr1.ja.net (146.97.38.42)  130.900 ms  130.395 ms  129.883 ms
16  universityofmanchester.ja.net (146.97.169.2)  131.039 ms * *
17  130.88.249.194 (130.88.249.194)  130.423 ms  137.508 ms  133.286 ms
18  * * *
19  * * *
20  eps.its.man.ac.uk (130.88.101.49)  131.346 ms  131.323 ms  130.529 ms
```

**Exercise 2:** (Very short.) Use traceroute to trace the route from your computer to math.hws.edu and to www.hws.edu. Explain the difference in the results.

Command for both hosts :



```
dell@dell-Inspiron-3443:~$ traceroute math.hws.edu > traceroute_math.hws.edu.log
dell@dell-Inspiron-3443:~$ traceroute www.hws.edu > traceroute_www.hws.edu.log
dell@dell-Inspiron-3443:~$ 
```

Output for both hosts :

### a. Tracing route to math.hws.edu

```
traceroute to math.hws.edu (64.89.144.237), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  3.253 ms  3.232 ms  3.226 ms
 2  1.16.16.172 (1.16.16.172)  1.948 ms  2.407 ms  2.406 ms
 3  103.88.221.177 (103.88.221.177)  2.277 ms  2.641 ms  2.743 ms
 4  undefined.hostname.localhost (103.214.130.129)  4.366 ms  4.471 ms  4.469 ms
 5  219.65.79.57.static-mumbai.vsnl.net.in (219.65.79.57)  4.831 ms  4.829 ms  4.825 ms
 6  172.23.78.233 (172.23.78.233)  5.535 ms  3.636 ms  3.303 ms
 7  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net (180.87.38.5)  19.183 ms  19.176 ms  18.941 ms
 8  if-ae-5-2.tcore1.wyn-marseille.as6453.net (80.231.217.29)  117.587 ms  117.791 ms
124.362 ms
 9  * * *
10  if-ae-11-2.tcore1.pvu-paris.as6453.net (80.231.153.49)  128.316 ms  128.328 ms  128.318
ms
11  * * *
12  ae-1-3104.edge3.Paris1.Level3.net (4.69.161.110)  124.297 ms
ae-2-3204.edge3.Paris1.Level3.net (4.69.161.114)  132.889 ms
ae-1-3104.edge3.Paris1.Level3.net (4.69.161.110)  120.382 ms
13  global-crossing-xe-level3.paris1.level3.net (4.68.63.230)  132.881 ms  126.024 ms  126.359
ms
14  roc1-ar5-xe-11-0-0-0.us.twtelecom.net (35.248.1.162)  214.198 ms  214.193 ms  214.191
ms
15  66-195-65-170.static.ctl.one (66.195.65.170)  210.260 ms  210.506 ms  211.145 ms
16  nat.hws.edu (64.89.144.100)  206.308 ms  206.963 ms  216.235 ms
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
```

```
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

**b. Tracing route to www.hws.edu**

```
traceroute to www.hws.edu (64.89.145.159), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  4.178 ms  4.159 ms  4.155 ms
 2  1.16.16.172 (1.16.16.172)  1.937 ms  2.315 ms  2.417 ms
 3  103.88.221.177 (103.88.221.177)  1.999 ms  2.411 ms  2.615 ms
 4  undefined.hostname.localhost (103.214.130.129)  2.501 ms * *
 5  219.65.79.57.static-mumbai.vsnl.net.in (219.65.79.57)  4.394 ms  4.396 ms  4.393
ms
 6  172.23.78.233 (172.23.78.233)  4.390 ms * *
 7  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net (180.87.38.5)  21.446 ms  21.369 ms
21.350 ms
 8  if-ae-5-2.tcore1.wyn-marseille.as6453.net (80.231.217.29)  138.963 ms  138.875 ms
134.968 ms
 9  if-ae-21-2.tcore1.pye-paris.as6453.net (80.231.154.208)  123.957 ms
if-ae-8-1600.tcore1.pye-paris.as6453.net (80.231.217.6)  130.009 ms
if-ae-21-2.tcore1.pye-paris.as6453.net (80.231.154.208)  125.622 ms
10  if-ae-11-2.tcore1.pvu-paris.as6453.net (80.231.153.49)  124.453 ms  124.974 ms
124.981 ms
11  * * *
12  ae-2-3204.edge3.Paris1.Level3.net (4.69.161.114)  124.843 ms  124.998 ms
ae-1-3104.edge3.Paris1.Level3.net (4.69.161.110)  124.783 ms
13  global-crossing-xe-level3.paris1.level3.net (4.68.63.230)  149.311 ms  148.796 ms
148.297 ms
14  roc1-ar5-xe-11-0-0-0.us.twtelecom.net (35.248.1.162)  206.469 ms  205.899 ms
230.071 ms
15  66-195-65-170.static.ctl.one (66.195.65.170)  214.326 ms  214.323 ms  214.195 ms
16  nat.hws.edu (64.89.144.100)  213.611 ms  213.612 ms  213.601 ms
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
```

```
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

**OBSERVATIONS:**

The IP address of the two destinations is different, for www.hws.edu it is 64.89.145.159 whereas for math.hws.edu it is 64.89.144.237.

**Whois** — The *whois* command can give detailed information about domain names and IP addresses. If it is not installed on the computers then install it with command sudo apt-get install whois in. *Whois* can tell you what organization owns or is responsible for the name or address and where to contact them. It often includes a list of domain name servers for the organization.

When using *whois* to look up a domain name, use the simple two-part network name, not an individual computer name (for example, *whois spit.ac.in*).

**Exercise 4:** (Short.) Use *whois* to investigate a well-known web site such as google.com or amazon.com, and write a couple of sentences about what you find out.

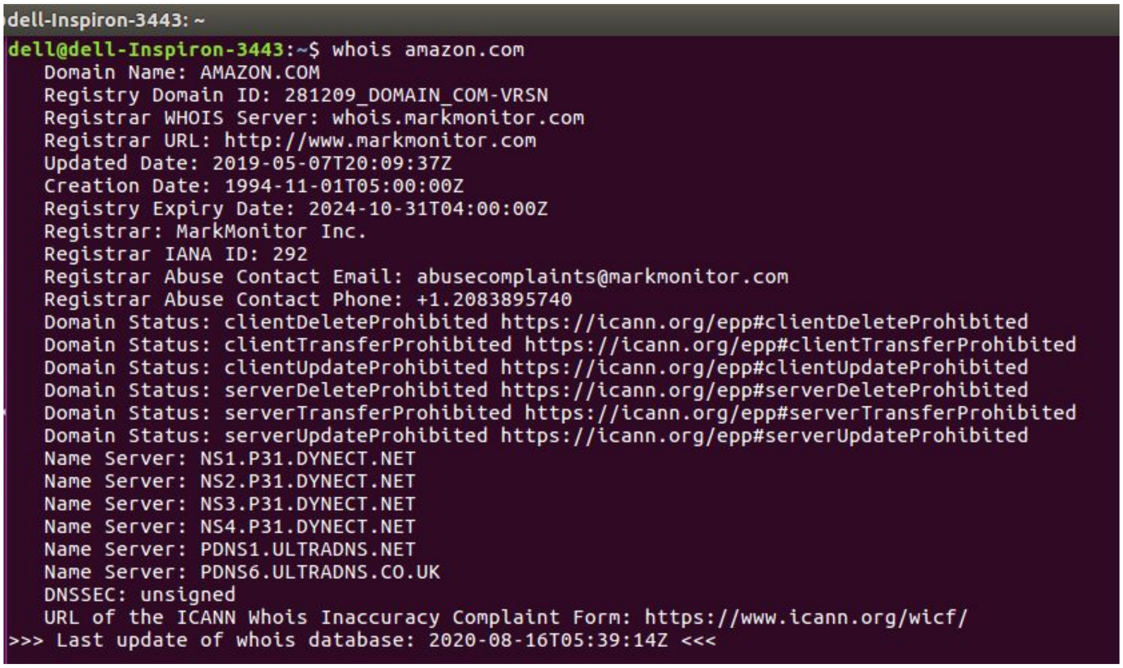
A whois record contains all the **contact information** associated with the person, company, or other entity that registered the domain name. Some registrations contain more information than others, and some registries return differing amounts of information.[1]

A typical whois record will contain the following information[1]:

- The name and contact information of the registrant: The owner of the domain.
- The name and contact information of the registrar: The organization that registered the domain name.
- The registration date.
- When the information was last updated.

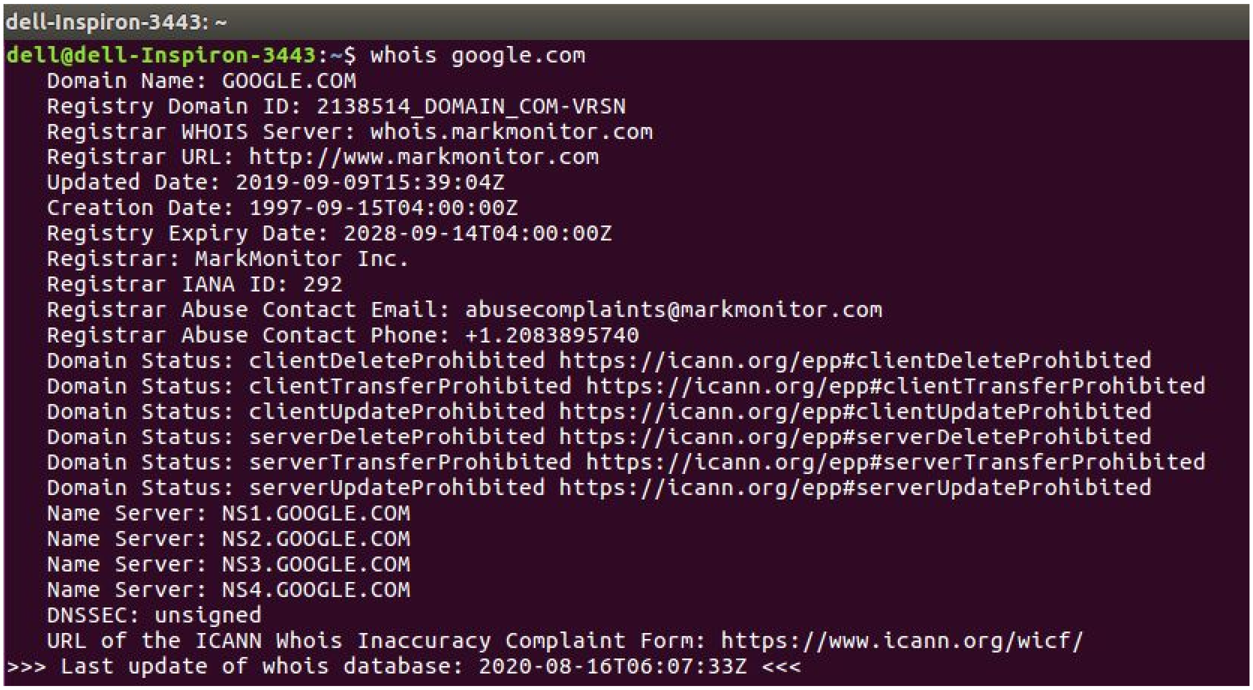
- The expiration date.

### For amazon.com -



```
dell@dell-Inspiron-3443:~$ whois amazon.com
   Domain Name: AMAZON.COM
   Registry Domain ID: 281209_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-05-07T20:09:37Z
   Creation Date: 1994-11-01T05:00:00Z
   Registry Expiry Date: 2024-10-31T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: 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.P31.DYNECT.NET
   Name Server: NS2.P31.DYNECT.NET
   Name Server: NS3.P31.DYNECT.NET
   Name Server: NS4.P31.DYNECT.NET
   Name Server: PDNS1.ULTRADNS.NET
   Name Server: PDNS6.ULTRADNS.CO.UK
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-08-16T05:39:14Z <<<
```

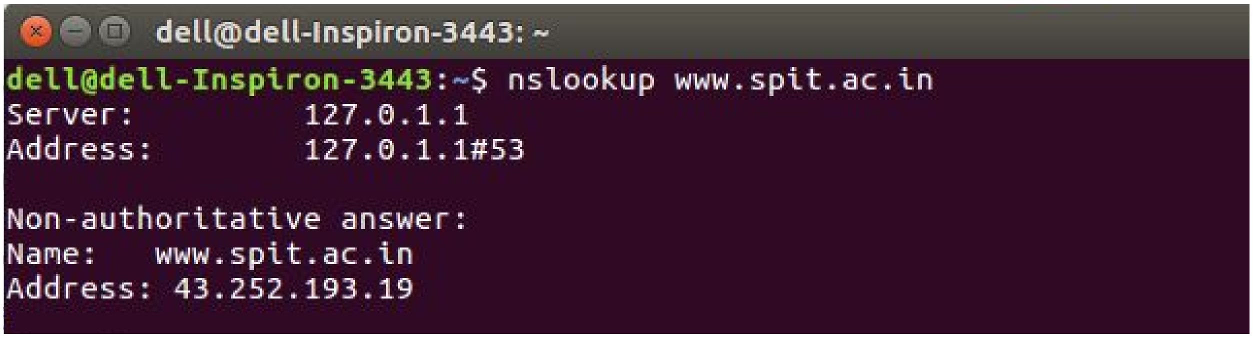
### For google.com -



```
dell@dell-Inspiron-3443:~$ whois google.com
   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: 2019-09-09T15:39:04Z
   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
   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: 2020-08-16T06:07:33Z <<<
```

**Exercise 5:** (Should be short.) Because of NAT, the domain name *spit.ac.in* has a different IP address outside of SPIT than it does on campus. Using information in this lab and working on a home computer, find the outside IP address for spit.ac.in. Explain how you did it.

Nslookup stands for "**Name Server Lookup**" is a useful command for getting information from a **Domain Name System (DNS) server**. It is a network administration tool for querying the DNS to obtain domain name or IP address mapping or any other specific DNS record. It is also used to troubleshoot DNS related problems. The command nslookup followed by the domain name will **display the IP Address of the domain**. It queries domain name servers and gets the details.[2]
Hence I have used the nslookup command to find the IP address for domain - www.spit.ac.in.



```
dell@dell-Inspiron-3443:~$ nslookup www.spit.ac.in
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   www.spit.ac.in
Address: 43.252.193.19
```

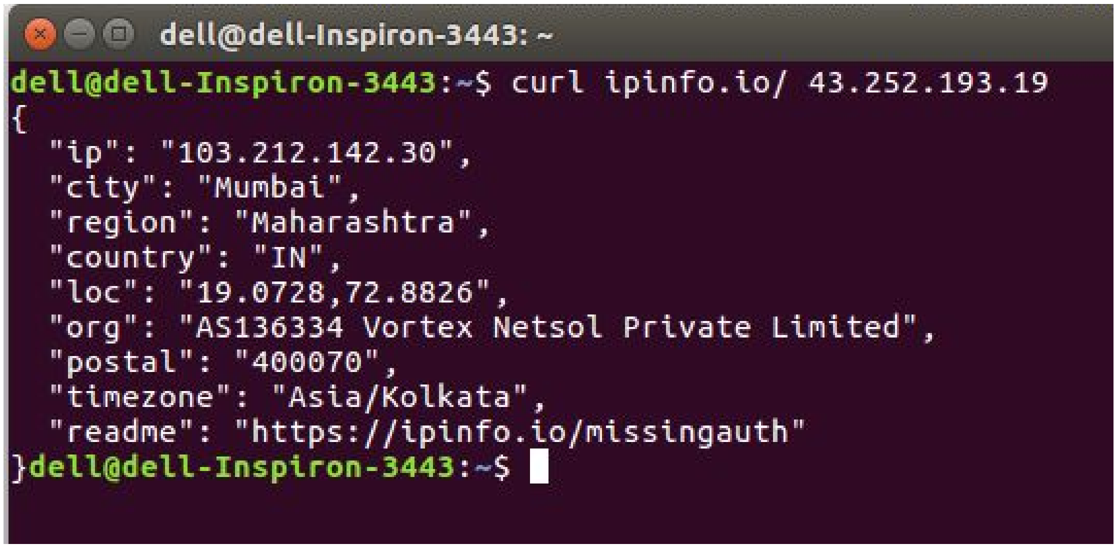
The IP address of spit.ac.in is **43.252.193.19**.

**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>.
For a specific example: curl  ipinfo.io/129.64.99.200

As you can see, we get back more than just the location.

The curl command to find location of spit.ac.in’s server :



```
dell@dell-Inspiron-3443:~$ curl ipinfo.io/ 43.252.193.19
{
  "ip": "103.212.142.30",
  "city": "Mumbai",
  "region": "Maharashtra",
  "country": "IN",
  "loc": "19.0728,72.8826",
  "org": "AS136334 Vortex Netsol Private Limited",
  "postal": "400070",
  "timezone": "Asia/Kolkata",
  "readme": "https://ipinfo.io/missingauth"
}dell@dell-Inspiron-3443:~$
```

**REFERENCES** :

1. https://www.howtogeek.com/680086/how-to-use-the-whois-command-on-linux/
2. https://www.geeksforgeeks.org/nslookup-command-in-linux-with-example
3. https://www.imperva.com/learn/performance/round-trip-time-rtt/
4. https://www.paessler.com/it-explained/ping
5. https://www.thousandeyes.com/learning/glossary/traceroute#:~:text=Traceroute%20is%20a%20network%20diagnostic,its%20route%20to%20the%20destination.
6. https://en.wikipedia.org/wiki/Nmap