

Name: Yash Shah
Batch: D
UID: 2018130049

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 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.

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!!!.)

```
Command Prompt
Microsoft Windows [Version 10.0.18363.959]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\yashc>ipconfig -all

Windows IP Configuration

    Host Name . . . . . : DESKTOP-NDBSHJC
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
    Physical Address. . . . . : 34-E1-2D-19-BD-BB
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
    Physical Address. . . . . : 36-E1-2D-19-BD-BA
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . :
    Description . . . . . : Intel(R) Dual Band Wireless-AC 3165
    Physical Address. . . . . : 34-E1-2D-19-BD-BA
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::2dc6:7f80:77bc:1387%11(Preferred)
    IPv4 Address. . . . . : 192.168.0.106(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
```

```
Command Prompt

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . :
    Description . . . . . : Intel(R) Dual Band Wireless-AC 3165
    Physical Address. . . . . : 34-E1-2D-19-BD-BA
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::2dc6:7f80:77bc:1387%11(Preferred)
    IPv4 Address. . . . . : 192.168.0.106(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Thursday, August 13, 2020 8:55:05 AM
    Lease Expires . . . . . : Thursday, August 13, 2020 6:10:34 PM
    Default Gateway . . . . . : 192.168.0.1
    DHCP Server . . . . . : 192.168.0.1
    DHCPv6 IAID . . . . . : 104128813
    DHCPv6 Client DUID. . . . . : 00-01-00-01-23-C7-74-72-34-E1-2D-19-BD-BA
    DNS Servers . . . . . : 192.168.0.1
                           0.0.0.0
    NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
    Description . . . . . : Bluetooth Device (Personal Area Network)
    Physical Address. . . . . : 34-E1-2D-19-BD-BE
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
```

Experiment 0: Experiment with ifconfig and write details about the information returned.

- lo is a special virtual network interface called loopback device. Loopback is used mainly for diagnostics and troubleshooting, and to connect to services running on local host.
- gif0 is Software Network Interface
- stf0 is 6to4 tunnel interface
- en0 is a physical interface representing Ethernet network card. It's used for communication with other computers on the network and on the Internet.
- Ether is the MAC address which is globally unique.
- mtu stands for Maximum Transmission Units is the size of each packet received by the ethernet card. The value of MTU is set to 1500 by default. The loopback device has a higher MTU value than the ethernet device
- INET 192.168.0.100 is the ipv4 address
- INET6 is the ipv6 address.
- bridge0 is a software bridge between other interfaces
- p2p0 is a point to point interface for wireless services.

FLAGS:

- UP indicates that kernel modules related to the interface have been loaded and interface is activated.
- BROADCAST indicates that interface is configured to handle broadcast packets, which is required for obtaining IP address via DHCP.
- RUNNING indicates that interface is ready to accept data.
- MULTICAST indicates that interface supports multicasting.

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

```
C:\Users\yashc>ping -n 10 -l 64 www.google.com

Pinging www.google.com [216.58.203.132] with 64 bytes of data:
Reply from 216.58.203.132: bytes=64 time=54ms TTL=120
Reply from 216.58.203.132: bytes=64 time=3ms TTL=120
Reply from 216.58.203.132: bytes=64 time=3ms TTL=120
Reply from 216.58.203.132: bytes=64 time=4ms TTL=120
Reply from 216.58.203.132: bytes=64 time=2ms TTL=120
Reply from 216.58.203.132: bytes=64 time=8ms TTL=120
Reply from 216.58.203.132: bytes=64 time=4ms TTL=120
Reply from 216.58.203.132: bytes=64 time=3ms TTL=120
Reply from 216.58.203.132: bytes=64 time=3ms TTL=120
Reply from 216.58.203.132: bytes=64 time=2ms TTL=120

Ping statistics for 216.58.203.132:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 54ms, Average = 8ms
```

```
C:\Users\yashc>ping -n 10 -l 100 www.google.com

Pinging www.google.com [216.58.203.132] with 100 bytes of data:
Reply from 216.58.203.132: bytes=68 (sent 100) time=4ms TTL=120
Reply from 216.58.203.132: bytes=68 (sent 100) time=2ms TTL=120
Reply from 216.58.203.132: bytes=68 (sent 100) time=16ms TTL=120
Reply from 216.58.203.132: bytes=68 (sent 100) time=2ms TTL=120
Reply from 216.58.203.132: bytes=68 (sent 100) time=2ms TTL=120
Reply from 216.58.203.132: bytes=68 (sent 100) time=3ms TTL=120
Reply from 216.58.203.132: bytes=68 (sent 100) time=72ms TTL=120
Reply from 216.58.203.132: bytes=68 (sent 100) time=3ms TTL=120
Reply from 216.58.203.132: bytes=68 (sent 100) time=4ms TTL=120
Reply from 216.58.203.132: bytes=68 (sent 100) time=2ms TTL=120

Ping statistics for 216.58.203.132:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 72ms, Average = 11ms
```

```
C:\Users\yashc>ping -n 10 -l 500 www.google.com
```

```
Pinging www.google.com [216.58.203.132] with 500 bytes of data:  
Reply from 216.58.203.132: bytes=68 (sent 500) time=4ms TTL=120  
Reply from 216.58.203.132: bytes=68 (sent 500) time=4ms TTL=120  
Reply from 216.58.203.132: bytes=68 (sent 500) time=2ms TTL=120  
Reply from 216.58.203.132: bytes=68 (sent 500) time=3ms TTL=120  
Reply from 216.58.203.132: bytes=68 (sent 500) time=3ms TTL=120  
Reply from 216.58.203.132: bytes=68 (sent 500) time=4ms TTL=120  
Reply from 216.58.203.132: bytes=68 (sent 500) time=2ms TTL=120  
Reply from 216.58.203.132: bytes=68 (sent 500) time=112ms TTL=120  
Reply from 216.58.203.132: bytes=68 (sent 500) time=2ms TTL=120  
Reply from 216.58.203.132: bytes=68 (sent 500) time=2ms TTL=120
```

```
Ping statistics for 216.58.203.132:
```

```
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 2ms, Maximum = 112ms, Average = 13ms
```

```
C:\Users\yashc>ping -n 10 -l 1000 www.google.com
```

```
Pinging www.google.com [216.58.203.132] with 1000 bytes of data:  
Reply from 216.58.203.132: bytes=68 (sent 1000) time=3ms TTL=120  
Reply from 216.58.203.132: bytes=68 (sent 1000) time=5ms TTL=120  
Reply from 216.58.203.132: bytes=68 (sent 1000) time=6ms TTL=120  
Reply from 216.58.203.132: bytes=68 (sent 1000) time=2ms TTL=120  
Reply from 216.58.203.132: bytes=68 (sent 1000) time=6ms TTL=120  
Reply from 216.58.203.132: bytes=68 (sent 1000) time=107ms TTL=120  
Reply from 216.58.203.132: bytes=68 (sent 1000) time=3ms TTL=120  
Reply from 216.58.203.132: bytes=68 (sent 1000) time=8ms TTL=120  
Reply from 216.58.203.132: bytes=68 (sent 1000) time=3ms TTL=120  
Reply from 216.58.203.132: bytes=68 (sent 1000) time=5ms TTL=120
```

```
Ping statistics for 216.58.203.132:
```

```
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 2ms, Maximum = 107ms, Average = 14ms
```

```
C:\Users\yashc>ping -n 10 -l 1400 www.google.com

Pinging www.google.com [216.58.203.132] with 1400 bytes of data:
Reply from 216.58.203.132: bytes=68 (sent 1400) time=5ms TTL=120
Reply from 216.58.203.132: bytes=68 (sent 1400) time=2ms TTL=120
Reply from 216.58.203.132: bytes=68 (sent 1400) time=5ms TTL=120
Reply from 216.58.203.132: bytes=68 (sent 1400) time=57ms TTL=120
Reply from 216.58.203.132: bytes=68 (sent 1400) time=6ms TTL=120
Reply from 216.58.203.132: bytes=68 (sent 1400) time=77ms TTL=120
Reply from 216.58.203.132: bytes=68 (sent 1400) time=6ms TTL=120
Reply from 216.58.203.132: bytes=68 (sent 1400) time=4ms TTL=120
Reply from 216.58.203.132: bytes=68 (sent 1400) time=3ms TTL=120
Reply from 216.58.203.132: bytes=68 (sent 1400) time=4ms TTL=120

Ping statistics for 216.58.203.132:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 77ms, Average = 16ms
```

QUESTIONS ABOUT LATENCY

Now look at the results you gathered and answer the following questions about latency. Store your answers in a file named ping.txt.

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

Ans.

Round-trip time (RTT) is the duration in milliseconds (ms) it takes for a network request to go from a starting point to a destination and back again to the starting point. RTT is an important metric in determining the health of a connection on a local network or the larger Internet, and is commonly utilised by network administrators to diagnose the speed and reliability of network connections. Round Trip Time is the time it takes for a network request to go from a starting point to a destination and back again.

Transmit delay - time it takes to push the packet's bits onto the link depends on size of the packet and the bandwidth of the network.

Propagation delay - time it takes a router to process the packet header, depends on the processing speed of the switch.

Queueing delay - time the packet spends in routing queues depends on the number of packets, size of the packet and bandwidth.

Yes it does vary between different hosts due to queueing delay or due to propagation delay as it depends on a distance.

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

Ans. The Transmit delay and Queueing delay both depends on packet sizes and increases if packet sizes increases. Hence average RTT also increases.

Exercise 1: 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. 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).

```
C:\Users\yashc>ping -n 10 -l 64 www.ox.ac.uk

Pinging www.ox.ac.uk [151.101.194.133] with 64 bytes of data:
Reply from 151.101.194.133: bytes=64 time=2415ms TTL=59
Reply from 151.101.194.133: bytes=64 time=2ms TTL=59
Reply from 151.101.194.133: bytes=64 time=3ms TTL=59
Reply from 151.101.194.133: bytes=64 time=2ms TTL=59
Reply from 151.101.194.133: bytes=64 time=3ms TTL=59
Reply from 151.101.194.133: bytes=64 time=3ms TTL=59
Reply from 151.101.194.133: bytes=64 time=6ms TTL=59
Reply from 151.101.194.133: bytes=64 time=3ms TTL=59
Reply from 151.101.194.133: bytes=64 time=3ms TTL=59
Reply from 151.101.194.133: bytes=64 time=3ms TTL=59

Ping statistics for 151.101.194.133:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2415ms, Average = 244ms
```



```
C:\Users\yashc>ping -n 10 -l 64 www.amazon.com

Pinging d3ag4hukkh62yn.cloudfront.net [13.227.137.166] with 64 bytes of data:
Reply from 13.227.137.166: bytes=64 time=133ms TTL=243
Reply from 13.227.137.166: bytes=64 time=6ms TTL=243
Reply from 13.227.137.166: bytes=64 time=3ms TTL=243
Reply from 13.227.137.166: bytes=64 time=2ms TTL=243
Reply from 13.227.137.166: bytes=64 time=3ms TTL=243
Reply from 13.227.137.166: bytes=64 time=2ms TTL=243
Reply from 13.227.137.166: bytes=64 time=95ms TTL=243
Reply from 13.227.137.166: bytes=64 time=5ms TTL=243
Reply from 13.227.137.166: bytes=64 time=2ms TTL=243
Reply from 13.227.137.166: bytes=64 time=2ms TTL=243

Ping statistics for 13.227.137.166:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 133ms, Average = 25ms

C:\Users\yashc>
```

For the same packet sizes, the RTT still varies for different destination. There are few reasons for this:

Physical distance – Physical distance between two hosts is defined as the length of the great circle arc connecting their locations on the surface of the Earth. The sum of per-hop distances would not significantly diverge from the actual distance between hosts.

Nature of the transmission medium - the way in which connections are made affects how fast the connection moves; connections made over optical fiber will behave differently than connections made over copper. Likewise, a connection made over a wireless frequency will behave differently than that of a satellite communication.

Server response time – the amount of time it takes a server to process and respond to a request is a potential bottleneck in network latency. When a server is overwhelmed with requests, such as during a DDoS attack, its ability to respond efficiently can be inhibited, resulting in increased RTT.

Node Count and congestion – depending on the path that a connection takes across the Internet, it may be routed or “hop” through a different number of intermediate nodes. Generally speaking, the greater the number of nodes a connection touches

the slower it will be. A node may also experience network congestion from other network traffic, which will slow down the connection and increase RTT.

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>`

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: telnet <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 $n = 1, 2, 3, \dots$, 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).

Hop Number – This is the first column and is simply the number of the hop along the route. In this case, it is the tenth hop.

RTT Columns – The next three columns display the round trip time (RTT) for your packet to reach that point and return to your computer. This is listed in milliseconds.

There are three columns because the traceroute sends three separate signal packets. This is to display consistency, or a lack thereof, in the route.

Domain/IP column – The last column has the IP address of the router. If it is available, the domain name will also be listed.

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 Prompt
Tracing route to mscs.mu.edu [134.48.4.5]
over a maximum of 30 hops:

 1  987 ms    5 ms     7 ms  192.168.0.1
 2    2 ms    1 ms     2 ms  103.5.187.30
 3    3 ms    2 ms     3 ms  103.5.187.13
 4   27 ms    3 ms     2 ms  dhcp-192-196-101.in2cable.com [203.192.196.101]
 5    *      8 ms     *    dhcp-192-196-29.in2cable.com [203.192.196.29]
 6    3 ms    4 ms     4 ms  14.143.59.13.static-mumbai.vsnl.net.in [14.143.59.13]
 7   25 ms    5 ms     5 ms  172.23.78.233
 8    6 ms    4 ms     3 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
 9    *     132 ms  128 ms  if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
10   132 ms  128 ms  139 ms  if-ae-8-1600.tcore1.pye-paris.as6453.net [80.231.217.6]
11   135 ms  191 ms  239 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
12   151 ms  130 ms  128 ms  80.231.153.66
13    *      *      245 ms  ae-2-3603.ear3.Chicago2.Level3.net [4.69.159.186]
14   247 ms  236 ms  242 ms  MARQUETTE-U.ear3.Chicago2.Level3.net [4.16.38.70]
15   239 ms  236 ms  238 ms  134.48.10.27
16    *      *      *    Request timed out.
17    *      *      *    Request timed out.
18    *      *      *    Request timed out.
19    *      *      *    Request timed out.
20    *      *      *    Request timed out.
21    *      *      *    Request timed out.
22    *      *      *    Request timed out.
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.
```

```
*tracert www.cs.grinnell.edu - Notepad
File Edit Format View Help
Tracing route to www.cs.grinnell.edu [132.161.132.159]
over a maximum of 30 hops:

 1    1 ms     1 ms     7 ms  192.168.0.1
 2   11 ms     6 ms     4 ms  103.5.187.30
 3    4 ms     2 ms     2 ms  103.5.187.13
 4    2 ms     3 ms     2 ms  dhcp-192-196-101.in2cable.com [203.192.196.101]
 5    *      *      6 ms  dhcp-192-196-29.in2cable.com [203.192.196.29]
 6    6 ms     3 ms     4 ms  14.143.59.13.static-mumbai.vsnl.net.in [14.143.59.13]
 7    9 ms     4 ms     5 ms  172.23.78.233
 8   25 ms    28 ms    42 ms  172.31.244.45
 9   34 ms    32 ms    46 ms  ix-ae-4-2.tcore2.cxr-chennai.as6453.net [180.87.37.1]
10  260 ms    255 ms    272 ms  if-ae-9-2.tcore2.mlv-mumbai.as6453.net [180.87.37.10]
11  459 ms    326 ms    286 ms  if-ae-12-2.tcore1.l78-london.as6453.net [180.87.39.21]
12  372 ms    306 ms    463 ms  if-ae-66-8.tcore2.nto-newyork.as6453.net [80.231.130.195]
13  385 ms    253 ms    319 ms  if-ae-26-2.tcore1.ct8-chicago.as6453.net [216.6.81.29]
14    *     258 ms    258 ms  63.243.129.121
15    *      *      *    Request timed out.
16  435 ms    281 ms    263 ms  et3-1-0-0.agr03.desm01-ia.us.windstream.net [40.128.250.43]
17  299 ms    272 ms    268 ms  et4-1-0-0.agr04.desm01-ia.us.windstream.net [40.136.117.253]
18  263 ms    270 ms    265 ms  ae4-0.pe05.grn101-ia.us.windstream.net [40.128.251.179]
19  269 ms    288 ms    266 ms  grn1-static-grinnellcollege0-0001.flex.iowatelecom.net [69.66.111.181]
20    *      *      *    Request timed out.
21    *      *      *    Request timed out.
22    *      *      *    Request timed out.
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.
```

```
*tracert csail.mit.edu - Notepad
File Edit Format View Help
Tracing route to csail.mit.edu [128.30.2.109]
over a maximum of 30 hops:

 1  133 ms    1 ms    3 ms  192.168.0.1
 2    2 ms    2 ms    1 ms  103.5.187.30
 3    4 ms    6 ms    3 ms  103.5.187.13
 4    7 ms    3 ms    3 ms  dhcp-192-196-101.in2cable.com [203.192.196.101]
 5    *      *      *      Request timed out.
 6    4 ms   18 ms    4 ms  14.143.59.13.static-mumbai.vsnl.net.in [14.143.59.13]
 7    4 ms    3 ms    4 ms  172.23.78.233
 8    4 ms    4 ms    4 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
 9    *      204 ms   204 ms  if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
10   201 ms   198 ms   218 ms  if-ae-2-2.tcore2.wyn-marseille.as6453.net [80.231.217.2]
11   207 ms   219 ms    *      if-ae-9-2.tcore2.l78-london.as6453.net [80.231.200.14]
12   208 ms   205 ms   203 ms  if-ae-4-2.tcore2.n0v-newyork.as6453.net [80.231.131.158]
13   285 ms   287 ms   320 ms  if-ae-2-2.tcore1.n0v-newyork.as6453.net [216.6.90.21]
14   218 ms   221 ms   210 ms  if-ae-7-2.tcore1.nto-newyork.as6453.net [63.243.128.25]
15   203 ms   202 ms   206 ms  if-ae-9-2.tcore1.n75-newyork.as6453.net [63.243.128.122]
16   204 ms   214 ms   229 ms  66.110.96.146
17   299 ms   291 ms   263 ms  be-10390-cr02.newyork.ny.ibone.comcast.net [68.86.83.89]
18   208 ms   205 ms   208 ms  be-1202-cs02.newyork.ny.ibone.comcast.net [96.110.38.37]
19   223 ms   211 ms   208 ms  96.110.42.6
20   218 ms   326 ms   263 ms  ae0-0-eg-bstpmall74w.boston.ma.boston.comcast.net [68.86.238.34]
21   210 ms   219 ms   215 ms  50-201-57-174-static.hfc.comcastbusiness.net [50.201.57.174]
22   210 ms   210 ms   209 ms  dmz-rtr-1-external-rtr-3.mit.edu [18.0.161.13]
23   232 ms   213 ms   220 ms  dmz-rtr-2-dmz-rtr-1-2.mit.edu [18.0.162.6]
24   208 ms   210 ms   215 ms  mitnet.core-1-ext.csail.mit.edu [18.4.7.65]
25    *      *      *      Request timed out.
26   210 ms   211 ms   209 ms  bdr.core-1.csail.mit.edu [128.30.0.246]
27   209 ms   209 ms   217 ms  inquire-3ld.csail.mit.edu [128.30.2.109]

Trace complete.
```

```
*tracert cs.stanford.edu - Notepad
File Edit Format View Help
Tracing route to cs.stanford.edu [171.64.64.64]
over a maximum of 30 hops:

 1  722 ms    <1 ms    <1 ms  192.168.0.1
 2    1 ms    1 ms    1 ms  103.5.187.30
 3   57 ms    3 ms    3 ms  103.5.187.13
 4    3 ms    3 ms    2 ms  dhcp-192-196-101.in2cable.com [203.192.196.101]
 5   33 ms    7 ms    *      dhcp-192-196-29.in2cable.com [203.192.196.29]
 6   117 ms    3 ms    3 ms  14.143.59.13.static-mumbai.vsnl.net.in [14.143.59.13]
 7    3 ms    3 ms    3 ms  172.23.78.233
 8   30 ms    28 ms    28 ms  172.31.244.45
 9   38 ms    34 ms    41 ms  ix-ae-4-2.tcore2.cxr-chennai.as6453.net [180.87.37.1]
10  249 ms    247 ms    *      if-ae-10-4.tcore2.svw-singapore.as6453.net [180.87.67.16]
11  255 ms    243 ms   242 ms  if-ae-7-2.tcore2.lvw-losangeles.as6453.net [180.87.15.26]
12  249 ms    242 ms   242 ms  if-ae-2-2.tcore1.lvw-losangeles.as6453.net [66.110.59.1]
13  244 ms    240 ms   241 ms  las-b24-link.telcel.net [80.239.128.214]
14  304 ms    306 ms   306 ms  palo-b24-link.telcel.net [62.115.119.90]
15  375 ms    307 ms   307 ms  palo-b1-link.telcel.net [62.115.122.169]
16  252 ms    251 ms   252 ms  hurricane-ic-308019-palo-b1.c.telcel.net [80.239.167.174]
17  260 ms    260 ms   259 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
18  249 ms    248 ms   252 ms  csee-west-rtr-v13.SUNet [171.66.255.140]
19  249 ms    248 ms   248 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```

```
tracert cs.manchester.ac.uk - Notepad
File Edit Format View Help

Tracing route to cs.manchester.ac.uk [130.88.101.49]
over a maximum of 30 hops:

 1  128 ms    1 ms    <1 ms  192.168.0.1
 2    2 ms    1 ms    2 ms   103.5.187.30
 3    3 ms    3 ms    4 ms   103.5.187.13
 4    2 ms    2 ms    2 ms   dhcp-192-196-101.in2cable.com [203.192.196.101]
 5    *        5 ms    *      dhcp-192-196-29.in2cable.com [203.192.196.29]
 6    3 ms    3 ms    3 ms   14.143.59.13.static-mumbai.vsnl.net.in [14.143.59.13]
 7   85 ms    3 ms    3 ms   172.23.78.233
 8    5 ms    4 ms    7 ms   ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
 9   131 ms   131 ms    *      if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
10   136 ms   236 ms   140 ms  if-ae-8-1600.tcore1.pye-paris.as6453.net [80.231.217.6]
11   160 ms   128 ms   126 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
12    *        *      134 ms  80.231.153.66
13   137 ms   134 ms   136 ms  ae-1-9.bear1.Manchesteruk1.Level3.net [4.69.167.38]
14   138 ms   132 ms   133 ms  JANET.bear1.Manchester1.Level3.net [212.187.174.238]
15   130 ms   134 ms   129 ms  ae22.manckh-sbr2.ja.net [146.97.35.189]
16   131 ms   137 ms   136 ms  ae23.manckh-rbr1.ja.net [146.97.38.42]
17    *        *      *      Request timed out.
18   133 ms   144 ms   130 ms  130.88.249.194
19    *        *      *      Request timed out.
20    *        *      *      Request timed out.
21   143 ms   137 ms   141 ms  eps.its.man.ac.uk [130.88.101.49]

Trace complete.
```

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.

```
Select Command Prompt

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

 1   97 ms    1 ms    1 ms   192.168.0.1
 2    2 ms    1 ms    1 ms   103.5.187.30
 3    4 ms    3 ms    5 ms   103.5.187.13
 4    3 ms    4 ms    3 ms   dhcp-192-196-101.in2cable.com [203.192.196.101]
 5    *        *     10 ms  dhcp-192-196-29.in2cable.com [203.192.196.29]
 6    4 ms    3 ms    4 ms   115.113.165.121.static-mumbai.vsnl.net.in [115.113.165.121]
 7    3 ms    4 ms    3 ms   172.23.78.237
 8    8 ms    3 ms    5 ms   ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
 9    *     159 ms    *      if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
10    *        *      *      Request timed out.
11   131 ms   130 ms   133 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
12    *     131 ms   137 ms  80.231.153.66
13   134 ms   127 ms   125 ms  ae-2-3204.edge3.Paris1.Level3.net [4.69.161.114]
14   127 ms   131 ms   133 ms  global-crossing-xe-level3.paris1.level3.net [4.68.63.230]
15   206 ms   205 ms   208 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
16   214 ms   210 ms   212 ms  66-195-65-170.static.ct1.one [66.195.65.170]
17   215 ms   212 ms   213 ms  64.89.144.100
18    *        *      *      Request timed out.
19    *        *      *      Request timed out.
20    *        *      *      Request timed out.
21    *        *      *      Request timed out.
22    *        *      *      Request timed out.
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:\Users\yashc>
```

```
Command Prompt
Trace complete.

C:\Users\yashc>tracert www.hws.edu

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

 1  2272 ms    1 ms    <1 ms    192.168.0.1
 2    2 ms    2 ms    1 ms    103.5.187.30
 3    6 ms    7 ms    3 ms    103.5.187.13
 4    2 ms    2 ms    30 ms    dhcp-192-196-101.in2cable.com [203.192.196.101]
 5    *        *        *        Request timed out.
 6   18 ms    4 ms    5 ms    115.113.165.121.static-mumbai.vsnl.net.in [115.113.165.121]
 7    4 ms    3 ms    3 ms    172.23.78.237
 8   23 ms    4 ms    3 ms    ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
 9   132 ms   133 ms   129 ms   if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
10   127 ms   135 ms    *        if-ae-21-2.tcore1.pye-paris.as6453.net [80.231.154.208]
11   126 ms   126 ms   125 ms   if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
12   128 ms   131 ms    *        80.231.153.66
13   129 ms   130 ms   128 ms   ae-1-3104.edge3.Paris1.level3.net [4.69.161.110]
14   127 ms   136 ms   125 ms   global-crossing-xe-level3.paris1.level3.net [4.68.63.230]
15   210 ms   227 ms   213 ms   roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
16   310 ms   209 ms   293 ms   66-195-65-170.static.ctl.one [66.195.65.170]
17   347 ms   331 ms   280 ms   64.89.144.100
18    *        *        *        Request timed out.
19    *        *        *        Request timed out.
20    *        *        *        Request timed out.
21    *        *        *        Request timed out.
22    *        *        *        Request timed out.
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:\Users\yashc>
```

We can see that the hop number is the same for both the traceroutes, but RTT varies.

Exercise 3: Two packets sent from the same source to the same destination do not necessarily follow the same path through the net. Experiment with some sources that are fairly far away. Can you find cases where packets sent to the same destination follow different paths? How likely does it seem to be? What about when the packets are sent at very different times? Save some of the outputs from traceroute. (You can copy them from the Terminal window by highlighting and right-clicking, then paste into a text editor.) Come back sometime next week, try the same destinations again, and compare the results with the results from today. Report your observations.

Observed on 17th August

```
Command Prompt
Trace complete.

C:\Users\yashc>tracert www.hws.edu

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

 1  2272 ms    1 ms    <1 ms    192.168.0.1
 2    2 ms    2 ms    1 ms    103.5.187.30
 3    6 ms    7 ms    3 ms    103.5.187.13
 4    2 ms    2 ms    30 ms    dhcp-192-196-101.in2cable.com [203.192.196.101]
 5    *        *        *        Request timed out.
 6   18 ms    4 ms    5 ms    115.113.165.121.static-mumbai.vsnl.net.in [115.113.165.121]
 7    4 ms    3 ms    3 ms    172.23.78.237
 8   23 ms    4 ms    3 ms    ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
 9   132 ms   133 ms   129 ms    if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
10   127 ms   135 ms    *        if-ae-21-2.tcore1.pye-paris.as6453.net [80.231.154.208]
11   126 ms   126 ms   125 ms    if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
12   128 ms   131 ms    *        80.231.153.66
13   129 ms   130 ms   128 ms    ae-1-3104.edge3.Paris1.Level3.net [4.69.161.110]
14   127 ms   136 ms   125 ms    global-crossing-xe-level3.paris1.level3.net [4.68.63.230]
15   210 ms   227 ms   213 ms    roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
16   310 ms   209 ms   293 ms    66-195-65-170.static.ctl.one [66.195.65.170]
17   347 ms   331 ms   280 ms    64.89.144.100
18    *        *        *        Request timed out.
19    *        *        *        Request timed out.
20    *        *        *        Request timed out.
21    *        *        *        Request timed out.
22    *        *        *        Request timed out.
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.
```

Observed on 20th August

```
Command Prompt

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

 1    1 ms    1 ms    1 ms    192.168.0.1
 2    2 ms    2 ms    2 ms    103.5.187.30
 3    5 ms    3 ms    3 ms    103.5.187.13
 4    3 ms    4 ms    3 ms    dhcp-192-196-101.in2cable.com [203.192.196.101]
 5    *        *        *        Request timed out.
 6    4 ms    3 ms    5 ms    115.113.165.121.static-mumbai.vsnl.net.in [115.113.165.121]
 7    4 ms    3 ms    3 ms    172.23.78.237
 8    5 ms    3 ms    4 ms    ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
 9   131 ms   131 ms   126 ms    if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
10   129 ms   128 ms    *        if-ae-21-2.tcore1.pye-paris.as6453.net [80.231.154.208]
11   128 ms   133 ms   127 ms    if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
12    *        131 ms   134 ms    80.231.153.66
13   135 ms   128 ms   133 ms    ae-1-3104.edge3.Paris1.Level3.net [4.69.161.110]
14   268 ms   130 ms   174 ms    global-crossing-xe-level3.paris1.level3.net [4.68.63.230]
15   399 ms   303 ms   296 ms    roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
16   351 ms   307 ms   216 ms    66-195-65-170.static.ctl.one [66.195.65.170]
17   211 ms   211 ms   212 ms    64.89.144.100
18    *        *        *        Request timed out.
19    *        *        *        Request timed out.
20    *        *        *        Request timed out.
21    *        *        *        Request timed out.
22    *        *        *        Request timed out.
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.
```

From the above screenshots, it can be seen that for same source and same destination, the packets sent at different times have different RTT and follow different paths.

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?

Ans. Yes, the source IP address

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?

Ans. There is no relation between the two.

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?

Ans. There is a direct relationship between the number of nodes and the latency of the host.

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`. *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*).

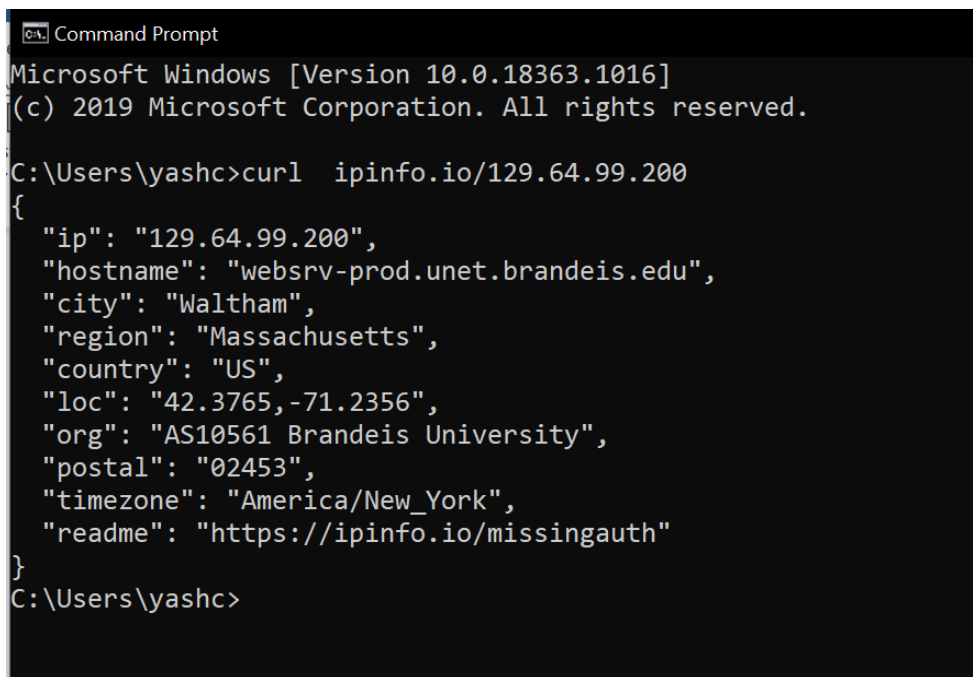
Exercise 4: (Short.) Use *whois* to investigate a well-known web site such as `google.com` or `amazon.com`, and write a couple of sentences about what you find out.

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.

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
```

A screenshot of a Windows Command Prompt window. The title bar says "C:\> Command Prompt". The text inside shows the Windows version "Microsoft Windows [Version 10.0.18363.1016]" and copyright notice "(c) 2019 Microsoft Corporation. All rights reserved.". The user is at the prompt "C:\Users\yashc>". They have entered the command "curl ipinfo.io/129.64.99.200". The output is a JSON object: {"ip": "129.64.99.200", "hostname": "websrv-prod.unet.brandeis.edu", "city": "Waltham", "region": "Massachusetts", "country": "US", "loc": "42.3765,-71.2356", "org": "AS10561 Brandeis University", "postal": "02453", "timezone": "America/New_York", "readme": "https://ipinfo.io/missingauth"}. The prompt "C:\Users\yashc>" is shown again at the bottom.

```
C:\> Command Prompt
Microsoft Windows [Version 10.0.18363.1016]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\yashc>curl ipinfo.io/129.64.99.200
{
  "ip": "129.64.99.200",
  "hostname": "websrv-prod.unet.brandeis.edu",
  "city": "Waltham",
  "region": "Massachusetts",
  "country": "US",
  "loc": "42.3765,-71.2356",
  "org": "AS10561 Brandeis University",
  "postal": "02453",
  "timezone": "America/New_York",
  "readme": "https://ipinfo.io/missingauth"
}
C:\Users\yashc>
```

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

Exercise 6: Find a few IP addresses that are connected to the web server on spit.ac.in right now, and determine where those IP addresses are located. (I'm expecting that there will be several; if not, try again in a few minutes or sometime later.) Find one that is far from Geneva, NY. Explain how you did it.

References:

- <https://en.wikipedia.org/wiki/Traceroute>

- http://docs.netapp.com/ontap-9/topic/com.netapp.doc.dot-cm-cmpr-940/network_traceroute.html#:~:text=The%20network%20traceroute%20command%20performs,logical%20interface%20and%20its%20Vserver.
- <https://www.cloudflare.com/learning/cdn/glossary/round-trip-time-rtt/#:~:text=What%20are%20common%20factors%20that,factors%20that%20can%20affect%20RTT.>