# Department of Computer Science

**EE353: Computer Networks**

**Class:** BSCS-7B

**Lab 10**: ***Tracing the path to a destination***

# Date: 25th Nov, 2019

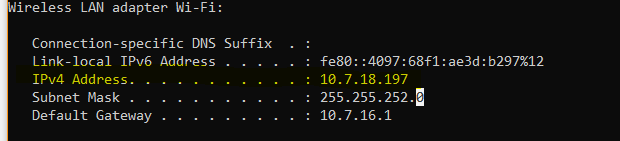
**Lab Engineer: Engr. Kaleem Ullah**

# Instructor: Dr. Muhammad Zeeshan

**Name : M. Hasnain Naeem**

**REG# : 212728**

**IP Screen Shot:**



***Lab Title:*** *Tracing the path to a destination*

**1.0 Objective of this lab:**

In this lab, we’ll explore several networking tools to trace the path followed by packets to a particular destination.

**2.0 Instructions:**

* Read carefully before starting the lab.
* These exercises are to be done individually.
* You are supposed to provide the answers to the questions listed at the end of this document, paste the screenshots of your working and upload the completed report to your course’s LMS site.
* Avoid plagiarism by copying from the Internet or from your peers. You may refer to source/ text but you must paraphrase the original work.

***Traceroute***

***Background:***

Trace Route (called traceroute under UNIX and tracert under Windows) is a very useful tool for analyzing network behavior and isolating problems. It determines the path that your TCP/IP packets take to a given destination, entered as an IP address or domain name. The results are fairly straightforward.

Here is a completed trace from www.cs.cf.ac.uk to www.stairways.com:

Hop Min Avg Max Ip Name

1 0.001 0.002 0.004 131.251.1.42 mr1-e0.cf.ac.uk

2 0.010 0.034 0.076 194.83.178.17 c7000.cf.welshman.net.uk

3 0.006 0.008 0.010 146.97.252.93 welshnet.bristol-core.ja.net

4 0.015 0.017 0.019 146.97.252.190 ext-gw6.ja.net

5 0.012 0.017 0.023 193.63.94.95 us-gw3.ja.net

6 0.083 0.093 0.108 193.62.157.18 ny-pop.ja.net

7 0.088 0.090 0.094 207.45.196.141 if-8-2.core1.newyork.teleglobe.net

8 0.076 0.077 0.079 207.45.223.110 if-10-0.bb8.newyork.teleglobe.net

9 0.081 0.084 0.088 207.45.198.74 ix-8-0-1.bb8.newyork.teleglobe.net

10 0.083 0.087 0.092 152.63.22.218 518.at-6-0-0.xr1.nyc9.alter.net

11 0.083 0.087 0.090 152.63.20.66 181.at-2-0-0.tr1.nyc8.alter.net

12 0.192 0.200 0.206 152.63.5.214 124.at-6-0-0.tr1.por3.alter.net

13 0.189 0.192 0.198 152.63.104.253 297.atm6-0.xr1.sea1.alter.net

14 0.204 0.208 0.211 146.188.200.41 195.atm7-0.gw1.sea1.alter.net

15 0.163 0.164 0.166 137.39.136.6 ixa-gw.customer.alter.net

16 0.226 0.233 0.237 63.237.224.54

17 0.233 0.250 0.273 199.254.168.243

**Hop**

-- Gives the order in which the TCP/IP packets progress from machine to machine, called the 'distance' (in hops) from the originating machine.

**Result**

-- Received/Sent packets, or other information (see below). Assuming all is well, these numbers should match - if more packets are sent than received, there may be a problem.

**Min, Avg, & Max**

-- The Minimum, Average and Maximum round trip time in seconds that the packets took to go to and return from that machine.

**IP & Name**

-- The IP address and domain name of the remote machine which is conveying your TCP/IP packets. There are other possible values which can appear in the Result column, identifying network problems with the trace:

***How Trace Route Works: TTLs***

TTL stands for Time To Live. When a TCP packet is sent, its TTL is set, which is the number of routers (hops) it can pass through before the packet is discarded. As the packet passes through a router the TTL is decremented until, when the TTL reaches zero, the packet is destroyed and an ICMP "time exceeded" message is returned. The return message's TTL is set by the terminating router when it creates the packet, and decremented normally.

Trace Route works by setting the TTL for a packet to 1, sending it towards the requested destination host, and listening for the reply. When the initiating machine receives a "time exceeded" response, it examines the packet to determine where the packet came from - this identifies the machine one hop away. Then the tracing machine generates a new packet with TTL 2, and uses the response to determine the machine 2 hops away, and so on.

Unfortunately not all TCP stacks behave correctly. Some TCP stacks set the TTL for the ICMP "time exceeded" message to that of the message being killed. So if the TTL is 0, the packet will be killed by the next machine to which it is passed. This can have two effects on a trace. If the computer is an intermediate machine in the trace, the entry will remain blank. No information is returned to the machine conducting the trace because the "time exceeded" message never makes it back. If the machine you are doing a trace to has this bug in its TCP stack, return packets won't reach the originating machine unless the TTL is high enough to cover the round trip. So Trace Route will show a number of failed connections equal to n (the number of hops to the destination machine) minus 1.

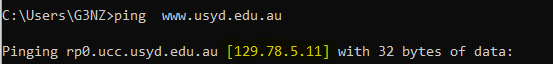
**Steps for performing this lab:**

1. **Open the command prompt application**
2. **Start up the Wireshark packet sniffer.**
3. **Begin packet capture.**
4. Type “tracert www.usyd.edu.au”(or traceroute) in command prompt and press enter.

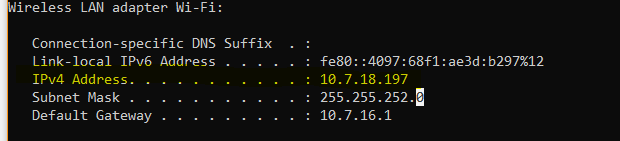
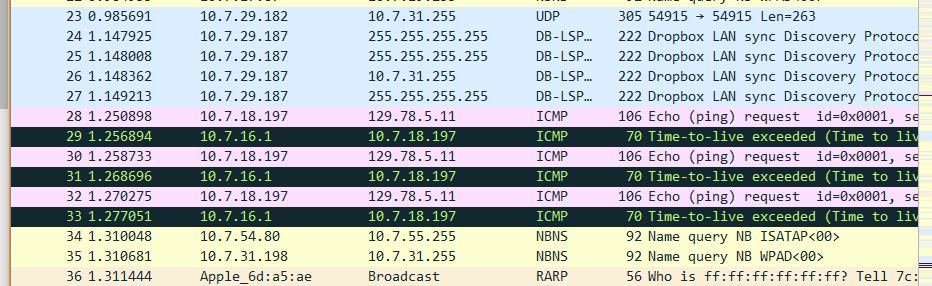
**Now answer the following questions:**

1. **What are the IP address of the host** [**www.usyd.edu.au**](http://www.usyd.edu.au) **and the IP of your machine?**

IP of [www.usyd.edu.au](http://www.usyd.edu.au): 129.78.5.11

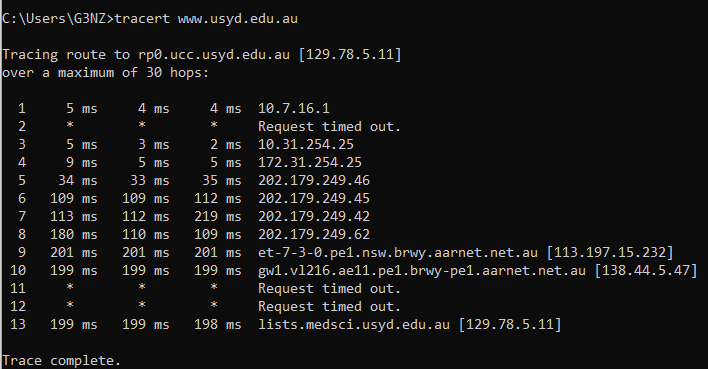


IP of my machine: 10.7.16.1

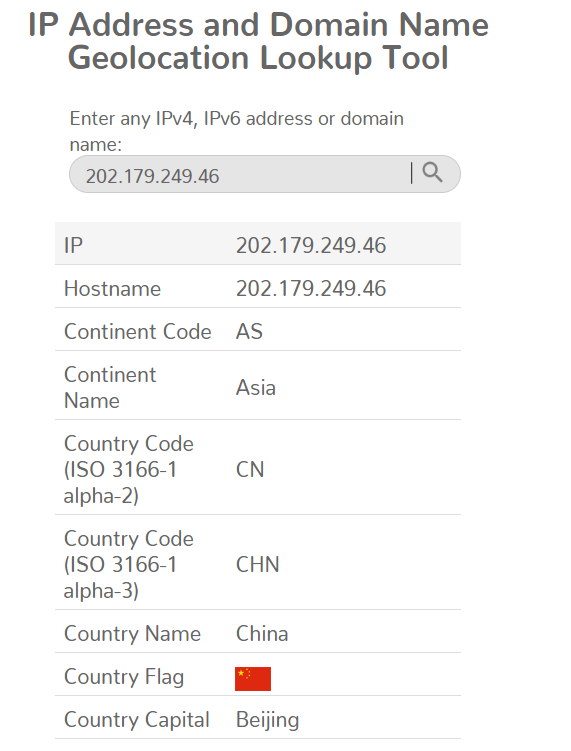
1. **How many hops is the destination host away from your machine?**

13 hops.



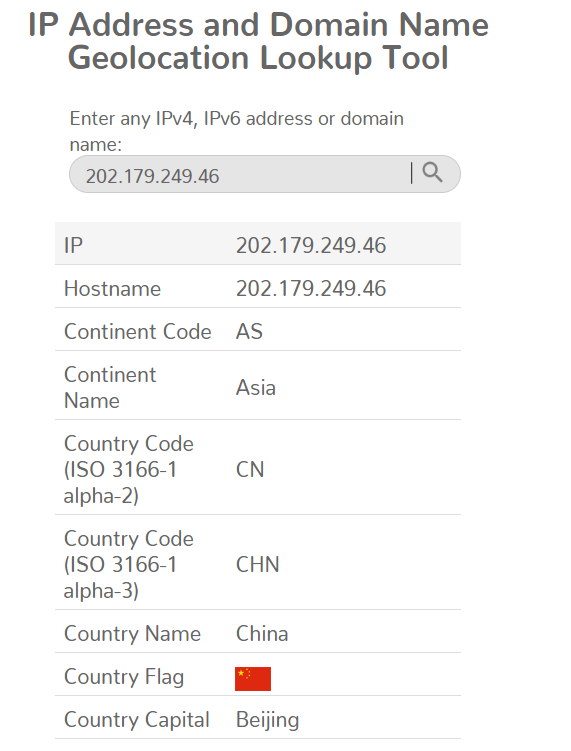
1. **How many hops are between your machine and the NUST gateway router?**

2 or 3. First one for the router inside the hostel. Second one gives timeout. Third one should be default gateway for the NUST. 4th should be ISP within Pakistan. (Information of these IPs is not available through lookups).  
Because, 5th hop reaches to IP: 202.179.249.46 and location of this IP is china.

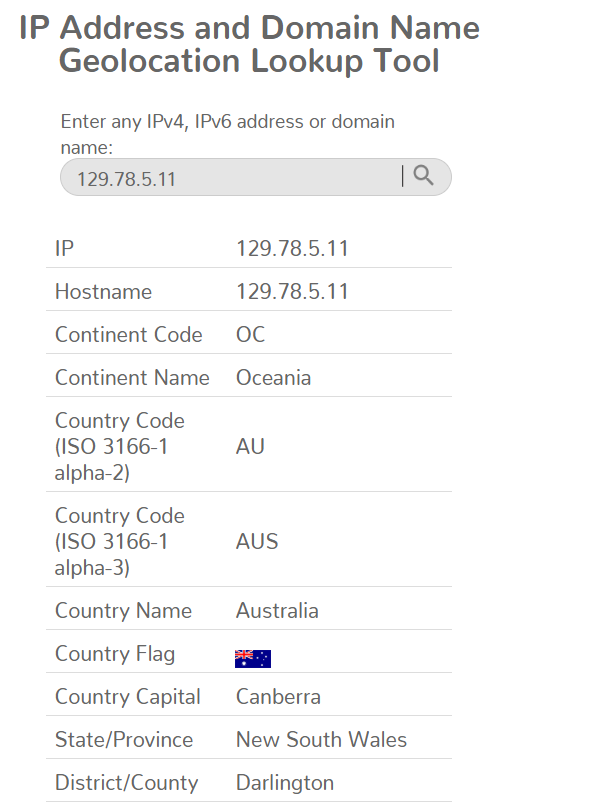


1. **How many routers does these packets visit in Pakistan?**

4 routers. Because 5th hop IP has location of China.



1. **Where is the website** [**www.usyd.edu.au**](http://www.usyd.edu.au) **hosted (city and country)?**

Sydney, Australia is the location of website.  
According to the last hop, which gave IP address: 129.78.5.1  


1. **How many cities your packets have actually visited? List all these cities along with the name of country in the order these have been visited?**

Locations of IP addresses in hops are:

* Islamabad, Pakistan
* Beijing, China
* Beijing, China
* Beijing, China
* Beijing, China
* Sydney, Australia
* Sydney, Australia
* Sydney Australia

So, it traveled total 3 cities.

1. **Comment if you observe any abnormal/wayward path followed by the traffic from your machine to the destination (It may be useful to roughly draw the path followed by the traffic on a map).**

There is no abnormality in path followed. Although, traffic went to China and then it was sent to Australia.

1. **Does the generated traffic always follow the same path to this destination?**

No. Switches and routers may send them to different routes depending on the traffic.

1. **How many routers in the path are working in “safe mode” (not replying to any query)?**

3 routers (traceroute command gave the timeout error)

1. **Which hop is the longest in the path to the destination?**

9th hop which ended at IP: 113.197.15.232. Its average RTT is 201 ms. All other hops have less than 200 ms RTT.

**Conclusion:**

We can examine the routers through which the traffic passes by using special commands which limit the hops. Each hop returns the IP address of the router (if not in safe mode) and we can find the locations of routers from their IP addresses.

This can help in various network analysis tasks.

*Refrence :* [*http://users.cs.cf.ac.uk/Dave.Marshall/Internet/node76.html*](http://users.cs.cf.ac.uk/Dave.Marshall/Internet/node76.html)

*http://users.cs.cf.ac.uk/Dave.Marshall/Internet/node77.html*