

Lab 11: Tracing the path to a destination**Name: Muhammad Rizwan Khalid****Regn No: 180459****Current IP: 10.3.93.227****Lab Title: Tracing the path to a destination**

```
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::8524:5ee8:fd2c:eb7e%13  
IPv4 Address. . . . . : 10.3.93.227  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 10.3.93.1
```

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.

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.
5. You can use geoip files uploaded on LMS to find the location of certain ip use following links for help

<https://wiki.wireshark.org/HowToUseGeoIP>
<https://dev.maxmind.com/geoip/legacy/geolite/>

Lab 11: Tracing the path to a destination

Now answer the following questions:

1. What are the IP address of the host www.usyd.edu.au and the IP of your machine?

Local Host	IP Address
My Ip	10.3.93.227
www.usyd.edu.au	129.78.5.11

Screenshots:

Machine Ip:

```

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::8524:5ee8:fd2c:eb7e%13
IPv4 Address. . . . . : 10.3.93.227
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.3.93.1

```

Destination Ip:

```

C:\> Command Prompt

C:\Users\domain1>tracert www.usyd.edu.au

Tracing route to rp0.ucc.usyd.edu.au [129.78.5.11]

```

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

The destination host is 17 hops away from my machine. It can be verified by the picture give below:

Screenshots:

```

C:\> Command Prompt

C:\Users\domain1>tracert www.usyd.edu.au

Tracing route to rp0.ucc.usyd.edu.au [129.78.5.11]
over a maximum of 30 hops:

  0  2 ms  1 ms  1 ms  10.3.93.1
  1  <1 ms  2 ms  3 ms  10.3.4.234
  2  <1 ms  <1 ms  <1 ms  10.1.2.254
  3  <1 ms  <1 ms  <1 ms  10.1.1.22
  4  1 ms  <1 ms  <1 ms  10.1.100.1
  5  1 ms  1 ms  1 ms  10.0.11.1
  6  6 ms  6 ms  6 ms  111.68.101.1.nust.edu.pk [111.68.101.1]
  7  1 ms  1 ms  1 ms  172.31.254.25
  8  35 ms  34 ms  36 ms  202.179.249.46
  9  309 ms  310 ms  309 ms  202.179.249.45
 10  301 ms  300 ms  301 ms  202.179.249.42
 11  345 ms  345 ms  345 ms  202.179.249.62
 12  345 ms  345 ms  345 ms  xe-3-0-3.pe1.brwy.nsw.aarnet.net.au [113.197.15.206]
 13  352 ms  351 ms  352 ms  gw1.vl216.ae11.pe1.brwy-pe1.aarnet.net.au [138.44.5.47]
 14  *  *  *  Request timed out.
 15  *  *  *  Request timed out.
 16  345 ms  345 ms  345 ms  nepeanmrf.com.au [129.78.5.11]

```

Lab 11: Tracing the path to a destination

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

There are 6 hops between my machine and the NUST gateway router, excluding the gateway router. These can be confirmed by the screenshot below:

Screenshot:

```

C:\Users\domain1>tracert www.usyd.edu.au

Tracing route to rp0.ucc.usyd.edu.au [129.78.5.11]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms    10.3.93.1
  2     <1 ms    2 ms     3 ms    10.3.4.234
  3     <1 ms    <1 ms    <1 ms    10.1.2.254
  4     <1 ms    <1 ms    <1 ms    10.1.1.22
  5      1 ms    <1 ms    <1 ms    10.1.100.1
  6      1 ms     1 ms     1 ms    10.0.11.1
  7      6 ms     6 ms     6 ms   111.68.101.1.nust.edu.pk [111.68.101.1]

```

4. How many routers does these packets visit in Pakistan?

These packets visit 8 routers in Pakistan. The last ip address in the figure below (172.31.254.25) is associated and reserved for IANA and it is private ip.

Screenshot:

```

C:\Users\domain1>tracert www.usyd.edu.au

Tracing route to rp0.ucc.usyd.edu.au [129.78.5.11]
over a maximum of 30 hops:


  1     2 ms     1 ms     1 ms    10.3.93.1
  2     <1 ms    2 ms     3 ms    10.3.4.234
  3     <1 ms    <1 ms    <1 ms    10.1.2.254
  4     <1 ms    <1 ms    <1 ms    10.1.1.22
  5      1 ms    <1 ms    <1 ms    10.1.100.1
  6      1 ms     1 ms     1 ms    10.0.11.1
  7      6 ms     6 ms     6 ms   111.68.101.1.nust.edu.pk [111.68.101.1]
  8      1 ms     1 ms     1 ms    172.31.254.25

```

5. Where is the website www.usyd.edu.au hosted (city and country)?

From iplocation.net, this website is hosted in Sydney, Australia

Screenshot:

IP Address	Country	Region	City
129.78.5.11	Australia 	New South Wales	Sydney
ISP	Organization	Latitude	Longitude
University of Sydney	Not Available	-33.8679	151.2073

Lab 11: Tracing the path to a destination

6. 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?

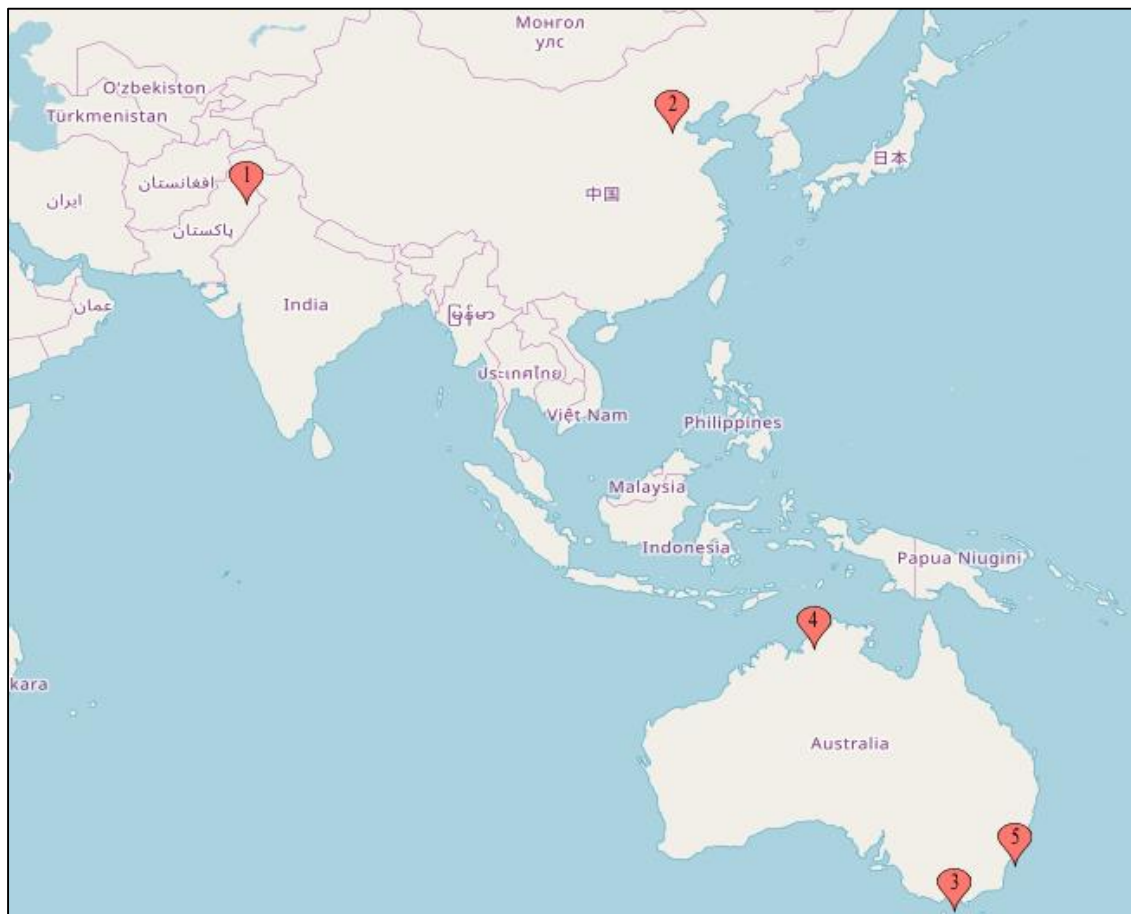
The list of cities are listed in order below. This list is generated by looking up the ips in the iplocation.net. 8 packets are routed in Rawalpindi, Pakistan. Next 4 packets are routed in Beijing, China while the remaining packets routed in Australia.

Serial No	City, Country	IP Address
1	Rawalpindi/Islamabad, Pakistan	111.68.101.1
2	Reserved for IANA (private)	172.31.254.25
3	Beijing, China	202.179.249.62
4	Melbourne, Australia	113.197.15.206
5	Darwin, Australia	138.44.5.47
6	Sydney, Australia	129.78.5.11

7. 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).

The path is described in the map below. The numbering on the cities give the path followed by the packets. There is abnormal activity shown in the map. After visiting the Melbourne (3rd pin), the packet is going to Darwin (4th pin) although there exists the shorter path to the Sydney (5th pin). This map is taken from the mapcustomizer.com.

Screenshot:



Lab 11: Tracing the path to a destination

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

Traffic may take different paths as well depending upon the load on the routers, the path was decided by the routing algorithms. In normal circumstances, the route will remain the same.

9. How many routers in the path are working in “safe mode” (not replying to any query)?
There are two routers which are working in the safe mode as they did not reply to the query. There was time out for the output of those routers.

Screenshot:

```

C:\Users\domain1>tracert www.usyd.edu.au

Tracing route to rp0.ucc.usyd.edu.au [129.78.5.11]
over a maximum of 30 hops:

  1    2 ms    1 ms    1 ms  10.3.93.1
  2    <1 ms   2 ms    3 ms  10.3.4.234
  3    <1 ms   <1 ms   <1 ms  10.1.2.254
  4    <1 ms   <1 ms   <1 ms  10.1.1.22
  5    1 ms    <1 ms   <1 ms  10.1.100.1
  6    1 ms    1 ms    1 ms  10.0.11.1
  7    6 ms    6 ms    6 ms  111.68.101.1.nust.edu.pk [111.68.101.1]
  8    1 ms    1 ms    1 ms  172.31.254.25
  9    35 ms   34 ms   36 ms  202.179.249.46
 10   309 ms  310 ms  309 ms  202.179.249.45
 11   301 ms  300 ms  301 ms  202.179.249.42
 12   345 ms  345 ms  345 ms  202.179.249.62
 13   345 ms  345 ms  345 ms  xe-3-0-3.pe1.brwy.nsw.aarnet.net.au [113.197.15.206]
 14   352 ms  351 ms  352 ms  gw1.vl216.ae11.pe1.brwy-pe1.aarnet.net.au [138.44.5.47]
 15    *      *      *      Request timed out.
 16    *      *      *      Request timed out.
 17   345 ms  345 ms  345 ms  nepeanmrf.com.au [129.78.5.11]

```

10. Which hop is the longest in the path to the destination?

14th hop is taking the longest time as its average RTT is maximum in the traceroute.

```

C:\Users\domain1>tracert www.usyd.edu.au

Tracing route to rp0.ucc.usyd.edu.au [129.78.5.11]
over a maximum of 30 hops:

  1    2 ms    1 ms    1 ms  10.3.93.1
  2    <1 ms   2 ms    3 ms  10.3.4.234
  3    <1 ms   <1 ms   <1 ms  10.1.2.254
  4    <1 ms   <1 ms   <1 ms  10.1.1.22
  5    1 ms    <1 ms   <1 ms  10.1.100.1
  6    1 ms    1 ms    1 ms  10.0.11.1
  7    6 ms    6 ms    6 ms  111.68.101.1.nust.edu.pk [111.68.101.1]
  8    1 ms    1 ms    1 ms  172.31.254.25
  9    35 ms   34 ms   36 ms  202.179.249.46
 10   309 ms  310 ms  309 ms  202.179.249.45
 11   301 ms  300 ms  301 ms  202.179.249.42
 12   345 ms  345 ms  345 ms  202.179.249.62
 13   345 ms  345 ms  345 ms  xe-3-0-3.pe1.brwy.nsw.aarnet.net.au [113.197.15.206]
 14   352 ms  351 ms  352 ms  gw1.vl216.ae11.pe1.brwy-pe1.aarnet.net.au [138.44.5.47]
 15    *      *      *      Request timed out.
 16    *      *      *      Request timed out.
 17   345 ms  345 ms  345 ms  nepeanmrf.com.au [129.78.5.11]

```