Week 2. Lab – Network Tools

Lab2.1 Play and Learn with the following networking tools:
Open https://ping.eu/ and play network tools with the parameters as in the table below

Network Tool	Parameter	Function
ping	google.com	
traceroute	google.com	
DNS lookup	google.com	
Reverse DNS lookup	8.8.8.8	

(a) What are the tools used for?
(b) What is your IP address? How much is packet loss in ping? What is the IP address of google.com in DNS lookup? When was the domain, i.e., google.com, updated? What is the hostname of 8.8.8.8?
(c) Try other tools and your own parameters.

Lab2.2 Using "ping" to measure network delay.
In your lab PC, at command window, perform "ping" to a destination within Australia. Open Wireshark to monitor traffic (hint: set up filter for the destination IP address).

(a) Find destination (e.g., nslookup google.com.au) IP address: _____
(b) Perform "ping" to the IP address to find the average round-trip delay: _____.
(c) Use Wireshark to find "ping" outgoing packet information.
Protocol: _____
Packet type (Info): _____
(d) User Wireshark to find "ping" incoming packet information.
Protocol: _____
Packet type (Info): _____

Lab2.3 Using "traceroute" to measure network delay and discover network path.
In your Lab PC, perform "tracert" to a destination IP address within Australia.
Find the average round-trip delay: _____.

(a) Use Wireshark to find "tracert" outgoing packet information.
Protocol: _____
Packet type (Info): _____
(b) Use Wireshark to find "tracert" incoming packet information.
Protocol: _____
Packet type (Info): _____
(c) Try to identify the number of ISP networks that the Traceroute packets pass through from source to destination. Routers with similar names and/or similar IP addresses should be considered as part of the same ISP. In your experiments, do the largest delays occur at the peering interfaces between adjacent ISPs?
(d) Repeat the above for a destination in other countries, e.g., 8.8.8.8. Compare the intra-continent and inter-continent results.

* * * Note on "traceroute" problems on Mac or Linux * * *
When you run "traceroute" on Mac or Linux, you may see " * * * " responses, which mean no response from the target router. The reason for this is that these days many routers have

firewalls that block ICMP, and some routers even block unknown UDP ports, which are used by “traceroute”. The later essentially stops traceroute from going further, which could be fatal for traceroute!
If you run into “ * * * “ problems on Mac or Linux, try add “`-I`” option to your command:

```
traceroute -I telstra.com.au
```

the option `"-I"` tells traceroute to use ICMP rather than UDP to send the traceroute probing packets. This appears to have overcome the blocked UDP port problem and is able to get better responses than the original “traceroute”. Although you may still see “* * *” responses, the “traceroute” has better chance of reaching its target with the “`-I`” option.

* * * Note on “tracert” on Windows * * *
“tracert” on Windows uses ICMP be default, which is equivalent to the “`-I`” option in “traceroute” on Mac or Linux.