CA169 Assignment 1 Lab Report

Submit these pages onwards.

Date:	21/03/17
STUDENT NAME:	Jake Grogan
STUDENT NUMBER:	16456346
PROJECT NUMBER:	1
MODULE CODE:	CA169
DEGREE: [CA EC ECSA PSSD]	CA
LECTURER:	Brian Stone

Declaration

In submitting this project, I declare that the project material, which I now submit, is my own work. Any assistance received by way of borrowing from the work of others has been cited and acknowledged within the work. I make this declaration in the knowledge that a breach of the rules pertaining to project submission may carry serious consequences.

Answer Sheets

Ipconfig exercise

IP address of the machine	136.206.17.53
MAC address	00-23-24-17-BB-B6

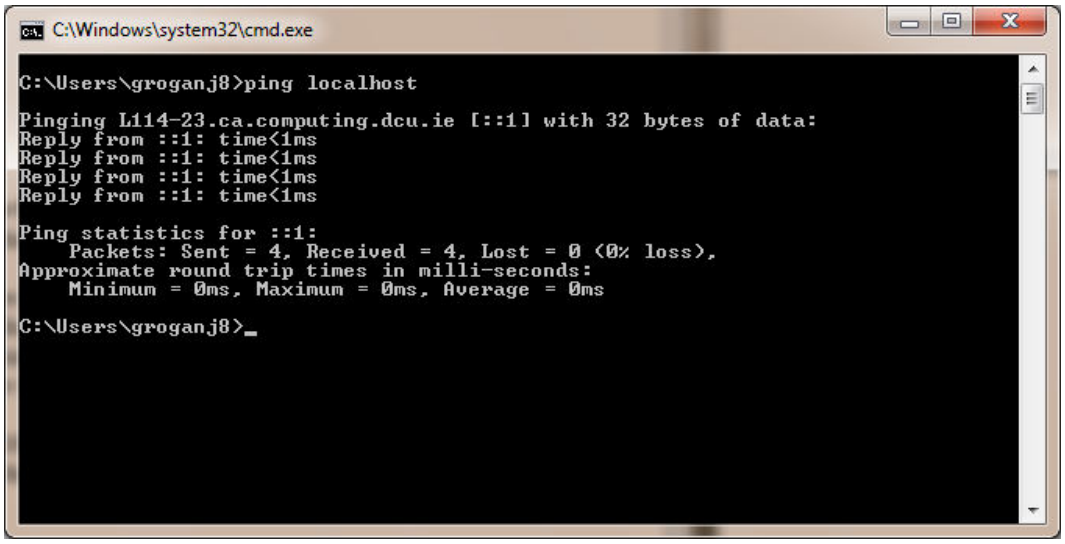
Ping exercise 1

What is displayed?

The usage and options along with their descriptions for the ping command are displayed.

Ping exercise 2

Ping localhost



1. What information is returned?
2. What is the localhost?

Answer 1

The hostname and IPv6 (default) address is shown and we are told it is being pinged with 32 bytes of data.
We are also shown that we received a reply from localhost and the time taken to get a reply (round-trip time). This is done several times.
We are then shown statistics for the complete process. We are told the number of echo requests sent, the number replies and number of loses. We are also told the minimum, maximum and average round-trip times for each packet.

Answer 2

Localhost is the name given for the hostname of the machine the user is currently on. In this case L114-23.ca.computing.dcu.ie.

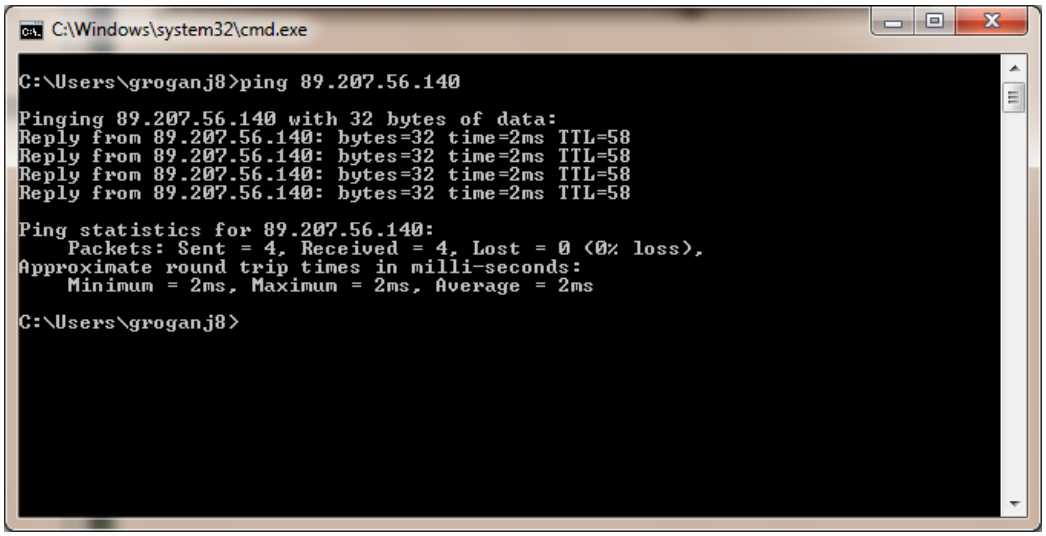
Additional marks

89.207.56.140 = www.rte.ie
173.194.34.120 = www.google.com

I found out from Microsoft's Technet that I can use the nslookup command to translate an IP back into its hostname/URL.

https://technet.microsoft.com/en-us/library/cc940085.aspx

Ping the IP address 89.207.56.140 **or the address** 173.194.34.120



Explain output here, item by item.

1) The first part is telling us that we are sending 32 bytes of data to 89.207.56.140 in the form of an ICMP echo request.

2-5) These lines tell us that we received a reply from the address with 32 bytes of data, a round-trip time of 2 miliseconds and a time to live of 58 which tells a router if a packet has been in the network for too long and if so, discard it.

6-7)This tells us the number of data packets sent, received and lost in the network and the percentage of packets lost.

8-9) This tells us information about the round-trip times of packets sent. We are told the minimum, maximum and average round-trip times.

Exercise 3

```
C:\Windows\system32\cmd.exe

C:\Users\groganj8>ping www.bbc.co.uk

Pinging www.bbc.net.uk [212.58.244.26] with 32 bytes of data:
Reply from 212.58.244.26: bytes=32 time=19ms TTL=51
Reply from 212.58.244.26: bytes=32 time=19ms TTL=51
Reply from 212.58.244.26: bytes=32 time=19ms TTL=51
Reply from 212.58.244.26: bytes=32 time=19ms TTL=51

Ping statistics for 212.58.244.26:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 19ms, Average = 19ms

C:\Users\groganj8>_
```

```
C:\Windows\system32\cmd.exe

C:\Users\groganj8>ping www.schlitterbahn.com

Pinging www.schlitterbahn.com [198.101.143.177] with 32 bytes of data:
Reply from 198.101.143.177: bytes=32 time=96ms TTL=114
Reply from 198.101.143.177: bytes=32 time=96ms TTL=114
Reply from 198.101.143.177: bytes=32 time=96ms TTL=114
Reply from 198.101.143.177: bytes=32 time=96ms TTL=114

Ping statistics for 198.101.143.177:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 96ms, Maximum = 96ms, Average = 96ms

C:\Users\groganj8>
```

	Website 1	Website 2
Name of the website pinged	www.bbc.co.uk	www.schlitterbahn.com
What is the IP address returned?	212.58.246.54	198.101.143.177
What is the TTL figure?	52	114
Average round trip time	19ms	96ms

The largest round trip time I could find was 96ms.

The round trip time from website 2 was larger than website 1. This indicated the webserver was located further away.

Your comments on **administrative information** that you found by searching on the Internet about the websites from experiment 3. Things like, who owns it, phone numbers, email addresses, registered addresses etc, anything at all that tells us about the website and its administration.

Website 1: www.bbc.co.uk

Admin Name: Domain Manager
Admin Organisation: British Broadcasting Corporation
City: London
Phone: +44 02080083539
Email: domain.manager@bbc.co.uk

Website 2: www.schlitterbahn.com

Name/Organisation: Schlitterbahn Resorts
Address: 211 West Lincoln, New Braunfels, 78130 Texas, US
Phone: +1.2103323910
Email: wdev@schlitterbahn.com

Exercise 4: Netstat exercise

Number of packets received by workstation:

Number of IP packets = 400703

```
C:\Windows\system32\cmd.exe

C:\Users\groganj8>netstat -es
Interface Statistics

                           Received            Sent

Bytes                    1380486140        58512225
Unicast packets             1083607          380890
Non-unicast packets          109620            5105
Discards                          0               0
Errors                            0               0
Unknown protocols                 0

IPv4 Statistics

  Packets Received                   = 400703
  Received Header Errors             = 0
  Received Address Errors            = 11
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 8907
  Received Packets Delivered         = 401862
  Output Requests                    = 125249
  Routing Discards                   = 0
  Discarded Output Packets           = 1
  Output Packet No Route             = 10
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

IPv6 Statistics
```

ICMP packets explained:

```
C:\Windows\system32\cmd.exe
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

ICMPv4 Statistics

                           Received    Sent
  Messages                 37          55
  Errors                   0           0
  Destination Unreachable  0           2
  Time Exceeded            0           0
  Parameter Problems       0           0
  Source Quenches          0           0
  Redirects                0           0
  Echo Replies             37          0
  Echos                    0           53
  Timestamps               0           0
  Timestamp Replies        0           0
  Address Masks            0           0
  Address Mask Replies     0           0
  Router Solicitations     0           0
  Router Advertisements    0           0

ICMPv6 Statistics

                           Received    Sent
  Messages                 58          81
  Errors                   0           0
```

ICMP packets are packets of data that have informational data stored within them such as error messages. The above illustration has 55 sent ICMP packets which came from pinging web servers. Ping works by sending ICMP echo request packets to a given network device. If we can reach the given destination then we receive an ICMP echo reply as seen above.

```
C:\Windows\system32\cmd.exe

C:\Users\groganj8>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            L114-23:0              LISTENING
  TCP    0.0.0.0:443            L114-23:0              LISTENING
  TCP    0.0.0.0:445            L114-23:0              LISTENING
  TCP    0.0.0.0:902            L114-23:0              LISTENING
  TCP    0.0.0.0:912            L114-23:0              LISTENING
  TCP    0.0.0.0:3389           L114-23:0              LISTENING
  TCP    0.0.0.0:5357           L114-23:0              LISTENING
  TCP    0.0.0.0:8501           L114-23:0              LISTENING
  TCP    0.0.0.0:49152          L114-23:0              LISTENING
  TCP    0.0.0.0:49153          L114-23:0              LISTENING
  TCP    0.0.0.0:49154          L114-23:0              LISTENING
  TCP    0.0.0.0:49246          L114-23:0              LISTENING
  TCP    0.0.0.0:49270          L114-23:0              LISTENING
  TCP    0.0.0.0:49288          L114-23:0              LISTENING
  TCP    127.0.0.1:8307         L114-23:0              LISTENING
  TCP    136.206.17.53:139      L114-23:0              LISTENING
  TCP    136.206.17.53:51226    Caher:8000             TIME_WAIT
  TCP    136.206.17.53:51231    Caher:8000             TIME_WAIT
  TCP    136.206.17.53:51233    Caher:8000             TIME_WAIT
  TCP    136.206.17.53:51236    Caher:8000             TIME_WAIT
  TCP    136.206.17.53:51246    Caher:8000             TIME_WAIT
  TCP    136.206.17.53:51250    Caher:8000             TIME_WAIT
  TCP    136.206.17.53:51280    Caher:8000             TIME_WAIT
  TCP    136.206.17.53:51327    Caher:8000             TIME_WAIT
  TCP    136.206.17.53:51333    136.206.217.81:microsoft-ds  ESTABLISHED
  TCP    136.206.17.53:51334    Caher:8000             TIME_WAIT
  TCP    136.206.17.53:51335    Caher:8000             TIME_WAIT
  TCP    136.206.17.53:51336    Caher:8000             TIME_WAIT
  TCP    136.206.17.53:51337    Caher:8000             TIME_WAIT
  TCP    136.206.17.53:51338    136.206.11.81:microsoft-ds  ESTABLISHED
  TCP    192.168.138.1:139      L114-23:0              LISTENING
  TCP    192.168.183.1:139      L114-23:0              LISTENING
  TCP    [::]:135               L114-23:0              LISTENING
  TCP    [::]:443               L114-23:0              LISTENING
  TCP    [::]:445               L114-23:0              LISTENING
  TCP    [::]:3389              L114-23:0              LISTENING
  TCP    [::]:5357              L114-23:0              LISTENING
  TCP    [::]:8501              L114-23:0              LISTENING
  TCP    [::]:49152             L114-23:0              LISTENING
  TCP    [::]:49153             L114-23:0              LISTENING
  TCP    [::]:49154             L114-23:0              LISTENING
  TCP    [::]:49246             L114-23:0              LISTENING
  TCP    [::]:49270             L114-23:0              LISTENING
  TCP    [::]:49288             L114-23:0              LISTENING
  TCP    [::1]:8307             L114-23:0              LISTENING
  TCP    [2002:88ce:1135::88ce:1135]:60974  [2002:88ce:b51::88ce:b51]:micros
ds  ESTABLISHED
  TCP    [2002:88ce:1135::88ce:1135]:61174  [2002:88ce:b51::88ce:b51]:49155
ABLISHED
  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    0.0.0.0:52229          *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:51755        *:*
  UDP    127.0.0.1:60804        *:*
  UDP    127.0.0.1:60806        *:*
  UDP    127.0.0.1:65160        *:*
  UDP    136.206.17.53:137      *:*
  UDP    136.206.17.53:138      *:*
  UDP    136.206.17.53:1900     *:*
  UDP    136.206.17.53:65157    *:*
  UDP    192.168.138.1:137      *:*
  UDP    192.168.138.1:138      *:*
  UDP    192.168.138.1:1900     *:*
  UDP    192.168.138.1:65159    *:*
  UDP    192.168.183.1:137      *:*
```

Before opening web browser

```
C:\Windows\system32\cmd.exe

C:\Users\groganj8>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            L114-23:0              LISTENING
  TCP    0.0.0.0:443            L114-23:0              LISTENING
  TCP    0.0.0.0:445            L114-23:0              LISTENING
  TCP    0.0.0.0:902            L114-23:0              LISTENING
  TCP    0.0.0.0:912            L114-23:0              LISTENING
  TCP    0.0.0.0:3389           L114-23:0              LISTENING
  TCP    0.0.0.0:5357           L114-23:0              LISTENING
  TCP    0.0.0.0:8501           L114-23:0              LISTENING
  TCP    0.0.0.0:49152          L114-23:0              LISTENING
  TCP    0.0.0.0:49153          L114-23:0              LISTENING
  TCP    0.0.0.0:49154          L114-23:0              LISTENING
  TCP    0.0.0.0:49246          L114-23:0              LISTENING
  TCP    0.0.0.0:49270          L114-23:0              LISTENING
  TCP    0.0.0.0:49288          L114-23:0              LISTENING
  TCP    127.0.0.1:8307         L114-23:0              LISTENING
  TCP    136.206.17.53:139      L114-23:0              LISTENING
  TCP    136.206.17.53:51226    Caher:8000             TIME_WAIT
  TCP    136.206.17.53:51280    Caher:8000             TIME_WAIT
  TCP    136.206.17.53:51327    Caher:8000             TIME_WAIT
  TCP    136.206.17.53:51334    Caher:8000             TIME_WAIT
  TCP    136.206.17.53:51335    Caher:8000             TIME_WAIT
  TCP    136.206.17.53:51336    Caher:8000             TIME_WAIT
  TCP    136.206.17.53:51337    Caher:8000             TIME_WAIT
  TCP    136.206.17.53:51340    Ossa:http              ESTABLISHED
  TCP    136.206.17.53:51341    Ossa:http              ESTABLISHED
  TCP    136.206.17.53:51342    Caher:8000             ESTABLISHED
  TCP    136.206.17.53:51343    Caher:8000             ESTABLISHED
  TCP    136.206.17.53:51344    Ossa:http              ESTABLISHED
  TCP    136.206.17.53:51345    Caher:8000             ESTABLISHED
  TCP    136.206.17.53:51346    Caher:8000             ESTABLISHED
  TCP    136.206.17.53:51347    Caher:8000             ESTABLISHED
  TCP    136.206.17.53:51348    Ossa:http              ESTABLISHED
  TCP    136.206.17.53:51349    Ossa:http              ESTABLISHED
  TCP    136.206.17.53:51350    Ossa:http              ESTABLISHED
  TCP    136.206.17.53:51351    Ossa:http              ESTABLISHED
  TCP    136.206.17.53:51352    Ossa:http              ESTABLISHED
  TCP    136.206.17.53:51353    Caher:8000             ESTABLISHED
  TCP    136.206.17.53:51354    Caher:8000             ESTABLISHED
  TCP    136.206.17.53:51355    Caher:8000             ESTABLISHED
  TCP    136.206.17.53:51356    Caher:8000             ESTABLISHED
  TCP    136.206.17.53:51357    Caher:8000             ESTABLISHED
  TCP    136.206.17.53:51358    Caher:8000             ESTABLISHED
  TCP    136.206.17.53:51359    Caher:8000             ESTABLISHED
  TCP    136.206.17.53:51360    Caher:8000             ESTABLISHED
  TCP    136.206.17.53:51361    Caher:8000             ESTABLISHED
  TCP    136.206.17.53:51362    Caher:8000             ESTABLISHED
  TCP    136.206.17.53:51363    Caher:8000             ESTABLISHED
  TCP    136.206.17.53:51364    Caher:8000             ESTABLISHED
  TCP    136.206.17.53:51365    Caher:8000             ESTABLISHED
  TCP    136.206.17.53:51366    Caher:8000             ESTABLISHED
  TCP    136.206.17.53:51367    Caher:8000             ESTABLISHED
  TCP    136.206.17.53:51368    Caher:8000             ESTABLISHED
  TCP    136.206.17.53:51369    Caher:8000             ESTABLISHED
  TCP    192.168.138.1:139      L114-23:0              LISTENING
  TCP    192.168.183.1:139      L114-23:0              LISTENING
  TCP    [::]:135               L114-23:0              LISTENING
  TCP    [::]:443               L114-23:0              LISTENING
  TCP    [::]:445               L114-23:0              LISTENING
  TCP    [::]:3389              L114-23:0              LISTENING
  TCP    [::]:5357              L114-23:0              LISTENING
  TCP    [::]:8501              L114-23:0              LISTENING
  TCP    [::]:49152             L114-23:0              LISTENING
  TCP    [::]:49153             L114-23:0              LISTENING
  TCP    [::]:49154             L114-23:0              LISTENING
  TCP    [::]:49246             L114-23:0              LISTENING
  TCP    [::]:49270             L114-23:0              LISTENING
  TCP    [::]:49288             L114-23:0              LISTENING
  TCP    [::1]:8307             L114-23:0              LISTENING
  TCP    [2002:88ce:1135::88ce:1135]:60974  [2002:88ce:b51::88ce:b51]:micros
ds  ESTABLISHED
```

After opening web browser

The connections opened after opening the web browser were the Ossa:http and some new caher:8000 connections under the foreign address header. They are all in an established state meaning a connection has been made.

```
C:\Windows\system32\cmd.exe

C:\Users\groganj8>netstat -r
===========================================================================
Interface List
 13...00 23 24 17 bb b6 ......Intel(R) 82567LM-3 Gigabit Network Connection
 15...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 17...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  1...........................Software Loopback Interface 1
 14...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 11...00 00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
 12...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
 16...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
 18...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0  136.206.17.254  136.206.17.53     10
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
     136.206.17.0    255.255.255.0         On-link     136.206.17.53    266
    136.206.17.53  255.255.255.255         On-link     136.206.17.53    266
   136.206.17.255  255.255.255.255         On-link     136.206.17.53    266
    192.168.138.0    255.255.255.0         On-link     192.168.138.1    276
    192.168.138.1  255.255.255.255         On-link     192.168.138.1    276
  192.168.138.255  255.255.255.255         On-link     192.168.138.1    276
    192.168.183.0    255.255.255.0         On-link     192.168.183.1    276
    192.168.183.1  255.255.255.255         On-link     192.168.183.1    276
  192.168.183.255  255.255.255.255         On-link     192.168.183.1    276
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link     136.206.17.53    266
        224.0.0.0        240.0.0.0         On-link     192.168.183.1    276
        224.0.0.0        240.0.0.0         On-link     192.168.138.1    276
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link     136.206.17.53    266
  255.255.255.255  255.255.255.255         On-link     192.168.183.1    276
  255.255.255.255  255.255.255.255         On-link     192.168.138.1    276
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    306 ::1/128                  On-link
 11   1010 2002::/16                On-link
 11    266 2002:88ce:1135::88ce:1135/128
                                    On-link
 13    266 fe80::/64                On-link
 15    276 fe80::/64                On-link
 17    276 fe80::/64                On-link
 15    276 fe80::6cf4:5a4d:e0fd:e692/128
                                    On-link
 17    276 fe80::7d69:13cc:60b:72e4/128
                                    On-link
 13    266 fe80::b138:6888:2ce7:e054/128
                                    On-link
  1    306 ff00::/8                 On-link
 13    266 ff00::/8                 On-link
 15    276 ff00::/8                 On-link
 17    276 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None

C:\Users\groganj8>_
```

Netstat –r explained

The –r parameter of the netstat command displays the routing table for the network adapters in the computer which is a collection of addresses for other networks. This is updated by the computer. It shows the quickest, most efficient route to take when sending data to them.

References:

http://www.linfo.org/routing_table.html

https://technet.microsoft.com/en-us/library/cc754365(v=ws.10).aspx