Lab 2 Answers

Task 1 & 2

```
H:\>ping/?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

Figure 1: Output of 'ping /?'

```
H:\>tracert/?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
```

Figure 2: Output of 'tracert /?'

Task 3 & 4

```
H:\>ping www.bbc.co.uk

Pinging www.bbc.net.uk [212.58.249.212] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 212.58.249.212:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 3: Output of 'ping www.bbc.co.uk'

```
H:\>ping www.gla.ac.uk

Pinging www.gla.ac.uk [130.209.16.90] with 32 bytes of data:
Reply from 130.209.16.90: bytes=32 time<1ms TTL=62
Reply from 130.209.16.90: bytes=32 time<1ms TTL=62
Reply from 130.209.16.90: bytes=32 time<1ms TTL=62
Reply from 130.209.16.90: bytes=32 time<1ms TTL=62

Ping statistics for 130.209.16.90:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 4: Output of 'ping www.gla.ac.uk'

The reason for not being able to ping an outside host (www.bbc.co.uk) is because either the ISP (Internet Service Provider) or the group policy on Windows, prevents ICMP Echo request and/or response packets to travel into and/or out of the network/our host. On the other hand, pinging an internal host such as www.gla.ac.uk is successful.

TTL, or Time-To-Live, is one of the fields of the IP header. Specifically, it is an 8-bit number (taking values in 0-255 inclusive) that is initialised to the maximum number of hops a packet can travel; in other words, the maximum number of routers through which the packet will be routed/forwarded. Every router along the route decreases the TTL value on the packet by 1, with the router that decreases it to 0 dropping the packet and not forwarding it any further. The default initial value used for ping (and other similar utilities) is OS-dependent; Linux, *BSD, and other modern Unix-based operating systems use a value of 64, while newer versions of Windows use a value of 128, but this limit is in any case configurable at the system level (i.e., the systems administrator may have changed the default to some other value). Since the responses from www.gla.ac.uk have a TTL of 62 and on that we now know the University web server is 2 hops away from our host (see answer to lab 1, also answer to Task 5 below), we can deduce that the default TTL on our host is 64.

When ping is finished sending/receiving packets, it prints out some statistics on its observations. These include the number of packets sent/received and the resulting packet loss, as well as the minimum, maximum and average (mean) values for the amount of time between sending an ICMP Echo request packet to the target host and receiving the matching ICMP Echo response packet. Ping on windows rounds the reported round-trip times and as such it reports 0ms (milliseconds) for all three round-trip time statistics. For reference, depicts the output of pinging www.gla.ac.uk from a Linux host.

```
nikos@linux:~$ ping www.gla.ac.uk
PING www.gla.ac.uk (130.209.16.90) 56(84) bytes of data.
64 bytes from www3.gla.ac.uk (130.209.16.90): icmp_seq=1 ttl=62 time=0.261 ms
64 bytes from www3.gla.ac.uk (130.209.16.90): icmp_seq=2 ttl=62 time=0.252 ms
64 bytes from www3.gla.ac.uk (130.209.16.90): icmp_seq=3 ttl=62 time=0.279 ms
64 bytes from www3.gla.ac.uk (130.209.16.90): icmp_seq=4 ttl=62 time=0.259 ms

--- www.gla.ac.uk ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.252/0.262/0.279/0.022 ms
```

Figure 5: Output of 'ping www.gla.ac.uk' from a Linux host

When running ping with the '-t' flag specified, ping will continue sending packets to the target host until interrupted (Ctrl+C). You can use this to get a more accurate picture of the network with regards to round-trip times to your target host, but please bear in mind that ICMP packets may be arbitrarily delayed for a number of reasons and all such measurements should be taken with a pinch of salt.

```
H:\>ping -t www.gla.ac.uk

Pinging www.gla.ac.uk [130.209.16.90] with 32 bytes of data:
Reply from 130.209.16.90: bytes=32 time<1ms TTL=62
Reply from 130.209.16.90: bytes=32 time<1ms TTL=62
Reply from 130.209.16.90: bytes=32 time<1ms TTL=62
Reply from 130.209.16.90: bytes=32 time<1ms TTL=62
Reply from 130.209.16.90: bytes=32 time<1ms TTL=62
Reply from 130.209.16.90: bytes=32 time<1ms TTL=62
Reply from 130.209.16.90: bytes=32 time<1ms TTL=62
Reply from 130.209.16.90: bytes=32 time<1ms TTL=62
Reply from 130.209.16.90: bytes=32 time<1ms TTL=62
Reply from 130.209.16.90: bytes=32 time<1ms TTL=62
Reply from 130.209.16.90: bytes=32 time<1ms TTL=62
Reply from 130.209.16.90: bytes=32 time<1ms TTL=62

Ping statistics for 130.209.16.90:
    Packets: Sent = 12, Received = 12, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
H:\>ping -t www.bbc.co.uk

Pinging www.bbc.net.uk [212.58.244.71] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 212.58.244.71:
    Packets: Sent = 12, Received = 0, Lost = 12 (100% loss),
```

Figure 6: Output of 'ping with -t'

Task 5

Tracert is a command used for revealing the path that a packet takes from the computer sending request to the desired destination. As discussed in the lab sheet, tracert uses ICMP Echo packets by default. As such, the limitations on ICMP traffic imposed by the ISP/group policy still apply. The result is that we are unable to receive responses from hosts outside the University's network, hence only the responses from the first few hops en route to www.bbc.co.uk are received and printed. For internal addresses (such as www.gla.ac.uk) there is no such issue. We can then see that the University's web server is 2 hops away from our computer, with 130.209.240.48 and 130.209.2.17 being IP addresses of the routers on the path. This explains to some extent why we couldn't get the web server's MAC address in our ARP cache when accessing the server in lab 1; for ARP packets to reach us, they should be forwarded/relayed by intermediate routers and apparently one or both of these routers haven't been configured thusly (this being the default and sane behaviour).

```
H:\>tracert www.bbc.co.uk

Tracing route to www.bbc.net.uk [212.58.249.208]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  rona.dcs.gla.ac.uk [130.209.240.48]
  2    <1 ms    <1 ms    <1 ms  130.209.2.17
  3     1 ms    <1 ms    <1 ms  130.209.2.114
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9  ^C
H:\>tracert www.gla.ac.uk

Tracing route to www.gla.ac.uk [130.209.16.90]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  rona.dcs.gla.ac.uk [130.209.240.48]
  2    <1 ms    <1 ms    <1 ms  130.209.2.17
  3    <1 ms    <1 ms    <1 ms  www3.gla.ac.uk [130.209.16.90]

Trace complete.
```

Figure 7: Output of 'tracert www.bbc.co.uk' and 'tracert www.gla.ac.uk'