Melissa Jost
915842777
Section A03
Roberto Lozano
914294300
Section A01

WireShark LAB: ICMP

ICMP and Ping

```
C:\Users\Roberto Lozano\test>ping -n 10 www.ust.hk

Pinging www.ust.hk [143.89.12.134] with 32 bytes of data:
Reply from 143.89.12.134: bytes=32 time=184ms TTL=48
Reply from 143.89.12.134: bytes=32 time=184ms TTL=48
Reply from 143.89.12.134: bytes=32 time=184ms TTL=48
Reply from 143.89.12.134: bytes=32 time=183ms TTL=48
Reply from 143.89.12.134: bytes=32 time=183ms TTL=48
Reply from 143.89.12.134: bytes=32 time=184ms TTL=48
Reply from 143.89.12.134: bytes=32 time=183ms TTL=48
Reply from 143.89.12.134: bytes=32 time=183ms TTL=48
Reply from 143.89.12.134: bytes=32 time=183ms TTL=48
Reply from 143.89.12.134: bytes=32 time=183ms TTL=48

Ping statistics for 143.89.12.134:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 183ms, Maximum = 184ms, Average = 183ms

C:\Users\Roberto Lozano\test>
```

1. The IP address of my host is 192.168.1.69 and the ip address of the destination host is 143.89.12.134. For context I am using the ping command “ping -n 10 www.ust.hk”

2. An ICMP packet does not have source and destination port numbers because the ICMP protocol is technically part of the networking layer. The port number feature is only available to protocols such as the TCP or UDP because they are part of the application layer.

3. The ICMP type is 8 and the code number is 0. This is to signify that this is an ICMP request.
   The other fields that the ICMP packet has are checksum, identifier (BE), identifier (LE), Sequence number (BE), Sequence number (LE), and response frame.
   The checksum field, sequence number, and identifier field are all 16 bits/2bytes long.

```
No.     Time           Source                Destination           Protocol Length Info
      1 0.000000       192.168.1.69          143.89.12.134         ICMP     74     Echo (ping) request  id=0x0001, seq=61/15616, ttl=128
(reply in 2)
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{65E4FA18-2BBE-459E-BA4D-2BD0A818A93A}, id 0
    Interface id: 0 (\Device\NPF_{65E4FA18-2BBE-459E-BA4D-2BD0A818A93A})
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 28, 2021 17:16:28.035533000
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1611882988.035533000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: Apple_ca:30:19 (c4:b3:01:ca:30:19), Dst: ARRISGro_7f:d6:c0 (88:96:4e:7f:d6:c0)
    Destination: ARRISGro_7f:d6:c0 (88:96:4e:7f:d6:c0)
    Source: Apple_ca:30:19 (c4:b3:01:ca:30:19)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.69, Dst: 143.89.12.134
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x44a1 (17569)
    Flags: 0x00
    Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x9853 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.69
    Destination Address: 143.89.12.134
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d1e [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 61 (0x003d)
    Sequence Number (LE): 15616 (0x3d00)
    [Response frame: 2]
    Data (32 bytes)
0000  61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70   abcdefghijklmnop
0010  71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69   qrstuvwabcdefghi
No.     Time           Source                Destination           Protocol Length Info
      2 0.183924       143.89.12.134         192.168.1.69          ICMP     74     Echo (ping) reply    id=0x0001, seq=61/15616, ttl=48
(request in 1)
Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{65E4FA18-2BBE-459E-BA4D-2BD0A818A93A}, id 0
    Interface id: 0 (\Device\NPF_{65E4FA18-2BBE-459E-BA4D-2BD0A818A93A})
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 28, 2021 17:16:28.219457000
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1611882988.219457000 seconds
    [Time delta from previous captured frame: 0.183924000 seconds]
    [Time delta from previous displayed frame: 0.183924000 seconds]
    [Time since reference or first frame: 0.183924000 seconds]
    Frame Number: 2
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: 86:96:4e:7f:d6:c3 (86:96:4e:7f:d6:c3), Dst: Apple_ca:30:19 (c4:b3:01:ca:30:19)
    Destination: Apple_ca:30:19 (c4:b3:01:ca:30:19)
    Source: 86:96:4e:7f:d6:c3 (86:96:4e:7f:d6:c3)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 143.89.12.134, Dst: 192.168.1.69
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x0db0 (3504)
    Flags: 0x00
```

```
    Fragment Offset: 0
    Time to Live: 48
    Protocol: ICMP (1)
    Header Checksum: 0x1f45 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 143.89.12.134
    Destination Address: 192.168.1.69
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x551e [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 61 (0x003d)
    Sequence Number (LE): 15616 (0x3d00)
    [Request frame: 1]
    [Response time: 183.924 ms]
    Data (32 bytes)
0000  61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70   abcdefghijklmnop
0010  71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69   qrstuvwabcdefghi
```

4. The ICMP type is 0 and the code number is 0. This is to signify that this is an ICMP reply.
   The other fields that the ICMP packet has are checksum, checksum status, identifier (BE), identifier (LE), Sequence number (BE), Sequence number (LE), request frame, and response time.
   The checksum field, sequence number, and identifier field are all 16 bits/2 bytes long

ICMP And Traceroute

```
C:\Users\Roberto Lozano\test>tracert www.inria.fr

Tracing route to inria.fr [128.93.162.83]
over a maximum of 30 hops:

  1     3 ms     3 ms     3 ms  dsldevice.attlocal.net [192.168.1.254]
  2    20 ms    19 ms    22 ms  99-20-64-1.lightspeed.frokca.sbcglobal.net [99.20.64.1]
  3    20 ms    20 ms    20 ms  71.147.234.116
  4    22 ms    29 ms    29 ms  12.122.160.174
  5    27 ms    28 ms    29 ms  12.122.2.78
  6    23 ms    25 ms    43 ms  sffca402igs.ip.att.net [12.122.114.29]
  7    29 ms    24 ms    23 ms  192.205.32.98
  8   160 ms   160 ms   159 ms  et-3-3-0.cr4-par7.ip4.gtt.net [213.200.119.214]
  9   160 ms   159 ms   159 ms  renater-gw-ix1.gtt.net [77.67.123.206]
 10   160 ms   159 ms   160 ms  te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
 11   160 ms   161 ms   161 ms  inria-rocquencourt-gi3-2-inria-rtr-021.noc.renater.fr [193.51.184.177]
 12   161 ms   161 ms   160 ms  unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
 13   161 ms   161 ms   161 ms  prod-inriafr-cms.inria.fr [128.93.162.83]

Trace complete.

C:\Users\Roberto Lozano\test>
```

5. The IP address of my host is 192.168.1.69 and the ip address of the target destination host is 128.93.162.83

6. It would be different as instead of using 1 for ICMP it would use 0x11 for UDP.

7. No it is not different from the ICMP ping query packets from the first half of the lab since they have the same fields.

8. The extra fields include an IPV4 Header and the 8 bytes consisting of the Type, Code, Checksum, Identifier (BE), Identifier (LE), Sequence Number (BE), and Sequence Number (LE).

9. The last three ICMP packets received by the source host differ from the ICMP error packets since they arrived at the destination host before the Time To Live terminated. This can also be seen by the type value of the ICMP packet. The last three have code 0 meaning it was received by the destination whereas the ICMP error packets have code 11 which means they exceeded the Time To Live.

10. There is a link who's delay is significantly longer than the others. It is the link from 192.205.32.98 to 213.200.119.214. The delay goes from ~25ms from the previous link to 160ms which is the biggest delay spike in the route. Given that the destination is in france and I am in the USA, I can guess that 192.205.32.98 is located in the USA and 213.200.119.214 is located somewhere in Europe. And after performing a whois on the ip's I can confirm that the 192.205.32.98 IP was in the USA and the 213.200.119.214 IP was in Germany.

```
No.     Time           Source                Destination           Protocol Length Info
     74 32.544358      128.93.162.83         192.168.1.69          ICMP     106    Echo (ping) reply    id=0x0001, seq=146/37376, ttl=47
(request in 73)
Frame 74: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{65E4FA18-2BBE-459E-BA4D-2BD0A818A93A}, id 0
Ethernet II, Src: 86:96:4e:7f:d6:c3 (86:96:4e:7f:d6:c3), Dst: Apple_ca:30:19 (c4:b3:01:ca:30:19)
Internet Protocol Version 4, Src: 128.93.162.83, Dst: 192.168.1.69
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xff6c [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 146 (0x0092)
    Sequence Number (LE): 37376 (0x9200)
    [Request frame: 73]
    [Response time: 160.994 ms]
    Data (64 bytes)
0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
        Data: 0000000000000000000000000000000000000000000000000000000000000000…
        [Length: 64]
No.     Time           Source                Destination           Protocol Length Info
     76 32.707429      128.93.162.83         192.168.1.69          ICMP     106    Echo (ping) reply    id=0x0001, seq=147/37632, ttl=47
(request in 75)
Frame 76: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{65E4FA18-2BBE-459E-BA4D-2BD0A818A93A}, id 0
Ethernet II, Src: 86:96:4e:7f:d6:c3 (86:96:4e:7f:d6:c3), Dst: Apple_ca:30:19 (c4:b3:01:ca:30:19)
Internet Protocol Version 4, Src: 128.93.162.83, Dst: 192.168.1.69
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xff6b [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 147 (0x0093)
    Sequence Number (LE): 37632 (0x9300)
    [Request frame: 75]
    [Response time: 161.554 ms]
    Data (64 bytes)
0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
        Data: 0000000000000000000000000000000000000000000000000000000000000000…
        [Length: 64]
No.     Time           Source                Destination           Protocol Length Info
     78 32.872016      128.93.162.83         192.168.1.69          ICMP     106    Echo (ping) reply    id=0x0001, seq=148/37888, ttl=47
(request in 77)
Frame 78: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{65E4FA18-2BBE-459E-BA4D-2BD0A818A93A}, id 0
Ethernet II, Src: 86:96:4e:7f:d6:c3 (86:96:4e:7f:d6:c3), Dst: Apple_ca:30:19 (c4:b3:01:ca:30:19)
Internet Protocol Version 4, Src: 128.93.162.83, Dst: 192.168.1.69
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xff6a [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 148 (0x0094)
    Sequence Number (LE): 37888 (0x9400)
    [Request frame: 77]
    [Response time: 161.358 ms]
    Data (64 bytes)
0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
        Data: 0000000000000000000000000000000000000000000000000000000000000000…
        [Length: 64]
```