

Setup: Open Wireshark and begin a packet capture. Run a ping command, then stop the packet capture.

```
PS C:\Users\laesc> ping -n 10 google.com

Pinging google.com [142.250.138.139] with 32 bytes of data:
Reply from 142.250.138.139: bytes=32 time=13ms TTL=55
Reply from 142.250.138.139: bytes=32 time=12ms TTL=55
Reply from 142.250.138.139: bytes=32 time=13ms TTL=55
Reply from 142.250.138.139: bytes=32 time=27ms TTL=55
Reply from 142.250.138.139: bytes=32 time=24ms TTL=55
Reply from 142.250.138.139: bytes=32 time=19ms TTL=55
Reply from 142.250.138.139: bytes=32 time=28ms TTL=55
Reply from 142.250.138.139: bytes=32 time=15ms TTL=55
Reply from 142.250.138.139: bytes=32 time=12ms TTL=55
Reply from 142.250.138.139: bytes=32 time=17ms TTL=55

Ping statistics for 142.250.138.139:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 28ms, Average = 18ms
PS C:\Users\laesc>
```

Figure 1: Results of 'ping' command

No.	Time	Source	Destination	Protocol	Length	Info
81	7.260055	10.125.1.2	10.102.40.131	ICMP	113	Destination unreachable (Host unreachable)
170	26.7470...	10.102.40.131	142.250.138.139	ICMP	74	Echo (ping) request id=0x0001, seq=185/47360, ttl=128 (reply in 171)
171	26.7606...	142.250.138.139	10.102.40.131	ICMP	74	Echo (ping) reply id=0x0001, seq=185/47360, ttl=55 (request in 170)
176	27.7626...	10.102.40.131	142.250.138.139	ICMP	74	Echo (ping) request id=0x0001, seq=186/47616, ttl=128 (reply in 177)
177	27.7753...	142.250.138.139	10.102.40.131	ICMP	74	Echo (ping) reply id=0x0001, seq=186/47616, ttl=55 (request in 176)
178	28.7724...	10.102.40.131	142.250.138.139	ICMP	74	Echo (ping) request id=0x0001, seq=187/47872, ttl=128 (reply in 179)
179	28.7861...	142.250.138.139	10.102.40.131	ICMP	74	Echo (ping) reply id=0x0001, seq=187/47872, ttl=55 (request in 178)
181	29.7974...	10.102.40.131	142.250.138.139	ICMP	74	Echo (ping) request id=0x0001, seq=188/48128, ttl=128 (reply in 183)
183	29.8247...	142.250.138.139	10.102.40.131	ICMP	74	Echo (ping) reply id=0x0001, seq=188/48128, ttl=55 (request in 181)
184	30.8213...	10.102.40.131	142.250.138.139	ICMP	74	Echo (ping) request id=0x0001, seq=189/48384, ttl=128 (reply in 185)
185	30.8459...	142.250.138.139	10.102.40.131	ICMP	74	Echo (ping) reply id=0x0001, seq=189/48384, ttl=55 (request in 184)
189	31.8455...	10.102.40.131	142.250.138.139	ICMP	74	Echo (ping) request id=0x0001, seq=190/48640, ttl=128 (reply in 190)
190	31.8645...	142.250.138.139	10.102.40.131	ICMP	74	Echo (ping) reply id=0x0001, seq=190/48640, ttl=55 (request in 189)
197	32.8703...	10.102.40.131	142.250.138.139	ICMP	74	Echo (ping) request id=0x0001, seq=191/48896, ttl=128 (reply in 198)
198	32.8982...	142.250.138.139	10.102.40.131	ICMP	74	Echo (ping) reply id=0x0001, seq=191/48896, ttl=55 (request in 197)
204	33.8942...	10.102.40.131	142.250.138.139	ICMP	74	Echo (ping) request id=0x0001, seq=192/49152, ttl=128 (reply in 205)
205	33.9095...	142.250.138.139	10.102.40.131	ICMP	74	Echo (ping) reply id=0x0001, seq=192/49152, ttl=55 (request in 204)
253	34.9161...	10.102.40.131	142.250.138.139	ICMP	74	Echo (ping) request id=0x0001, seq=193/49408, ttl=128 (reply in 254)
254	34.9279...	142.250.138.139	10.102.40.131	ICMP	74	Echo (ping) reply id=0x0001, seq=193/49408, ttl=55 (request in 253)
255	35.9404...	10.102.40.131	142.250.138.139	ICMP	74	Echo (ping) request id=0x0001, seq=194/49664, ttl=128 (reply in 256)
256	35.9571...	142.250.138.139	10.102.40.131	ICMP	74	Echo (ping) reply id=0x0001, seq=194/49664, ttl=55 (request in 255)

Figure 2: Packets captured during execution of 'ping' command

1. What is the IP address of your host? What is the IP address of the destination host?

- Source host: 10.102.40.131
- Destination host: 142.250.138.139

170	26.7470...	10.102.40.131	142.250.138.139	ICMP	74	Echo (ping) request
171	26.7606...	142.250.138.139	10.102.40.131	ICMP	74	Echo (ping) reply

Figure 3: Source and destination IP addresses highlighted in first packets of 'ping' capture

## 2. Why is it that an ICMP packet does not have source and destination port numbers?

- a. This is because ICMP packets operate at the network level of the TCP/IP networking model.

## 3. Regarding one of the ping request packets sent by your host, what are the ICMP type and code numbers? What other fields does the ICMP packet have? How many bytes are the checksum, sequence number, and identifier fields?

- a. The ICMP type was 8 (ping request), and the code was 0.
- b. Other fields include: Checksum, Identifier (BE), Identifier (LE), Sequence Number (BE), Sequence Number (LE).
- c. The checksum is 2 bytes, sequence numbers are 2 bytes, and identifiers are 2 bytes.

```
▶ Frame 170: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on  
▶ Ethernet II, Src: Intel_cf:a1:70 (bc:54:2f:cf:a1:70), Dst: Cisco_a8:76:f  
▶ Internet Protocol Version 4, Src: 10.102.40.131, Dst: 142.250.138.139  
▼ Internet Control Message Protocol  
  Type: 8 (Echo (ping) request)  
  Code: 0  
  Checksum: 0x4ca2 [correct]  
  [Checksum Status: Good]  
  Identifier (BE): 1 (0x0001)  
  Identifier (LE): 256 (0x0100)  
  Sequence Number (BE): 185 (0x00b9)  
  Sequence Number (LE): 47360 (0xb900)  
  [Response frame: 171]  
▶ Data (32 bytes)
```

Figure 4: 'ping' request packet with relevant fields highlighted

## 4. Regarding the corresponding reply packet, what are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number, and identifier fields?

- a. The ICMP type was 0 (ping reply), and the code was 0.
- b. Other fields include: Checksum, Identifier (BE), Identifier (LE), Sequence Number (BE), Sequence Number (LE).
- c. The checksum is 2 bytes, sequence numbers are 2 bytes, and identifiers are 2 bytes.

```
▶ Frame 171: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on  
▶ Ethernet II, Src: Cisco_a8:76:ff (e8:b7:48:a8:76:ff), Dst: Intel_cf:a1:7  
▶ Internet Protocol Version 4, Src: 142.250.138.139, Dst: 10.102.40.131  
▼ Internet Control Message Protocol  
  Type: 0 (Echo (ping) reply)  
  Code: 0  
  Checksum: 0x54a2 [correct]  
  [Checksum Status: Good]  
  Identifier (BE): 1 (0x0001)  
  Identifier (LE): 256 (0x0100)  
  Sequence Number (BE): 185 (0x00b9)  
  Sequence Number (LE): 47360 (0xb900)  
  [Request frame: 170]  
  [Response time: 13.587 ms]  
▶ Data (32 bytes)
```

Figure 4: 'ping' reply packet with relevant fields highlighted

Setup: Now we will investigate ICMP packets used in Traceroute, open Wireshark and begin a packet capture. Run a tracert command, then end the Wireshark capture.

```
PS C:\Users\laesc> tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

  0  *             2 ms    1 ms   10.102.250.2
  1  *             2 ms    1 ms   10.250.253.2
  2  62 ms         2 ms    1 ms   10.125.1.2
  3  1 ms          2 ms    1 ms   69.150.209.240
  4  5 ms          2 ms    2 ms   172.83.49.254
  5  13 ms         10 ms   10 ms   74.200.176.14
  6  11 ms         23 ms   30 ms   74.200.180.212
  7  9 ms          15 ms   10 ms   74.200.144.60
  8  14 ms         10 ms  108 ms  209.85.251.253
  9  12 ms         11 ms   11 ms   172.253.78.227
 10  10 ms         10 ms   10 ms   dns.google [8.8.8.8]

Trace complete.
PS C:\Users\laesc>
```

Figure 5: Results of 'tracert' command

No.	icmp icmpv6	Source	Destination	Protocol	Length Info
2360	37.0229	172.83.49.254	8.8.8.8	ICMP	106 Echo (ping) request id=0x0001, seq=382/32257, ttl=5 (no response found!)
2361	37.0250	10.102.40.131	8.8.8.8	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2362	37.0273	172.83.49.254	8.8.8.8	ICMP	106 Echo (ping) request id=0x0001, seq=383/32513, ttl=5 (no response found!)
2370	37.4474	172.83.49.254	10.102.40.131	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2373	38.9496	172.83.49.254	10.102.40.131	ICMP	70 Destination unreachable (Port unreachable)
2383	40.4659	172.83.49.254	10.102.40.131	ICMP	70 Destination unreachable (Port unreachable)
2385	42.9832	10.102.40.131	8.8.8.8	ICMP	106 Echo (ping) request id=0x0001, seq=384/32769, ttl=6 (no response found!)
2386	42.9959	74.200.176.14	10.102.40.131	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2387	43.0905	10.102.40.131	8.8.8.8	ICMP	106 Echo (ping) request id=0x0001, seq=385/33025, ttl=6 (no response found!)
2388	43.0103	74.200.176.14	10.102.40.131	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2389	43.0132	10.102.40.131	8.8.8.8	ICMP	106 Echo (ping) request id=0x0001, seq=386/33281, ttl=6 (no response found!)
2390	43.0236	74.200.176.14	10.102.40.131	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2426	48.9672	10.102.40.131	8.8.8.8	ICMP	106 Echo (ping) request id=0x0001, seq=387/33537, ttl=7 (no response found!)
2427	48.9783	74.200.180.212	10.102.40.131	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2428	48.9830	10.102.40.131	8.8.8.8	ICMP	106 Echo (ping) request id=0x0001, seq=388/33793, ttl=7 (no response found!)
2429	49.0059	74.200.180.212	10.102.40.131	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2430	49.0082	10.102.40.131	8.8.8.8	ICMP	106 Echo (ping) request id=0x0001, seq=389/34049, ttl=7 (no response found!)
2431	49.0383	74.200.180.212	10.102.40.131	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2608	54.9660	10.102.40.131	8.8.8.8	ICMP	106 Echo (ping) request id=0x0001, seq=390/34305, ttl=8 (no response found!)
2609	54.9756	74.200.144.60	10.102.40.131	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2610	54.9777	10.102.40.131	8.8.8.8	ICMP	106 Echo (ping) request id=0x0001, seq=391/34561, ttl=8 (no response found!)
2611	54.9926	74.200.144.60	10.102.40.131	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2612	54.9952	10.102.40.131	8.8.8.8	ICMP	106 Echo (ping) request id=0x0001, seq=392/34817, ttl=8 (no response found!)
2613	55.0050	74.200.144.60	10.102.40.131	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2665	60.9501	10.102.40.131	8.8.8.8	ICMP	106 Echo (ping) request id=0x0001, seq=393/35073, ttl=9 (no response found!)
2666	60.9638	209.85.251.253	10.102.40.131	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
2667	60.9674	10.102.40.131	8.8.8.8	ICMP	106 Echo (ping) request id=0x0001, seq=394/35329, ttl=9 (no response found!)
2668	60.9772	209.85.251.253	10.102.40.131	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
2669	60.9795	10.102.40.131	8.8.8.8	ICMP	106 Echo (ping) request id=0x0001, seq=395/35585, ttl=9 (no response found!)
2670	61.0876	209.85.251.253	10.102.40.131	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
2697	66.9786	10.102.40.131	8.8.8.8	ICMP	106 Echo (ping) request id=0x0001, seq=396/35841, ttl=10 (no response found!)
2698	66.9907	172.253.78.227	10.102.40.131	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
2699	66.9936	10.102.40.131	8.8.8.8	ICMP	106 Echo (ping) request id=0x0001, seq=397/36097, ttl=10 (no response found!)
2700	67.0044	172.253.78.227	10.102.40.131	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
2701	67.0067	10.102.40.131	8.8.8.8	ICMP	106 Echo (ping) request id=0x0001, seq=398/36353, ttl=10 (no response found!)
2702	67.0166	172.253.78.227	10.102.40.131	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
2715	72.9924	10.102.40.131	8.8.8.8	ICMP	106 Echo (ping) request id=0x0001, seq=399/36609, ttl=11 (reply in 2716)
2716	73.9027	8.8.8.8	10.102.40.131	ICMP	106 Echo (ping) reply id=0x0001, seq=399/36609, ttl=55 (request in 2715)
2717	73.9051	10.102.40.131	8.8.8.8	ICMP	106 Echo (ping) request id=0x0001, seq=400/36865, ttl=11 (reply in 2718)
2718	73.9155	8.8.8.8	10.102.40.131	ICMP	106 Echo (ping) reply id=0x0001, seq=400/36865, ttl=55 (request in 2717)
2719	73.9198	10.102.40.131	8.8.8.8	ICMP	106 Echo (ping) request id=0x0001, seq=401/37121, ttl=11 (reply in 2720)
2720	73.9301	8.8.8.8	10.102.40.131	ICMP	106 Echo (ping) reply id=0x0001, seq=401/37121, ttl=55 (request in 2719)

Figure 6: Packets captured during execution of tracert command

5. What is the IP address of your host? What is the IP address of the target destination host?

- Source IP: 10.102.40.131
- Destination IP: 8.8.8.8

```

Frame 293: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
Ethernet II, Src: Intel_cf:a1:70 (bc:54:2f:cf:a1:70), Dst: Cisco_a8:76:ff (e8:b7:48:a8:76:ff)
Internet Protocol Version 4, Src: 10.102.40.131, Dst: 8.8.8.8
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 92
  Identification: 0x8241 (33345)
  ▶ 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  ▶ Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.102.40.131
  Destination Address: 8.8.8.8
Internet Control Message Protocol

```

Figure 7: tracer packet with source and destination IP highlighted

6. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?

a. It would not, since ICMP is its own protocol

7. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?

a. It is different because the TTL is modified to trace the routers using expired packet notifications

8. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?

a. It also contains the original packet which had its TTL expire

```

▶ Frame 293: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
▶ Ethernet II, Src: Intel_cf:a1:70 (bc:54:2f:cf:a1:70), Dst: Cisco_a8:76:ff (e8:b7:48:a8:76:ff)
▶ Internet Protocol Version 4, Src: 10.102.40.131, Dst: 8.8.8.8
▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xf68c [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 370 (0x0172)
  Sequence Number (LE): 29185 (0x7201)
▶ [No response seen]
▶ Data (64 bytes)

```

```

▶ Frame 294: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▶ Ethernet II, Src: Cisco_a8:76:ff (e8:b7:48:a8:76:ff), Dst: Intel_cf:a1:70 (bc:54:2f:cf:a1:70)
▶ Internet Protocol Version 4, Src: 10.102.250.2, Dst: 10.102.40.131
▼ Internet Control Message Protocol
  Type: 11 (Time-to-live exceeded)
  Code: 0 (Time to live exceeded in transit)
  Checksum: 0xf4ff [correct]
  [Checksum Status: Good]
  Unused: 00000000
▶ Internet Protocol Version 4, Src: 10.102.40.131, Dst: 8.8.8.8
▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xf68c [unverified] [in ICMP error packet]
  [Checksum Status: Unverified]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 370 (0x0172)
  Sequence Number (LE): 29185 (0x7201)

```

Figure 8: ICMP error packet vs ICMP echo packet

9. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?

a. These packets did not expire, so they are of normal type 0

10. Within the tracert measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in Figure 4, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of this link?

- a. According to Figure 4, I do not really see any outliers. The time to be returned increases as the packet goes further, which is to be expected due to all the delays adding up. The same is noted for my tracert too.

```

C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>tracert www.inria.fr

Tracing route to www.inria.fr [138.96.146.2]
over a maximum of 30 hops:

  0  13 ms    12 ms    13 ms    10.216.228.1
  1  21 ms    14 ms    13 ms    24.218.0.153
  2  12 ms    11 ms    13 ms    bar01-p4-0.wsfdhe1.ma.attbb.net [24.128.190.197]
  3  16 ms    16 ms    15 ms    bar02-p6-0.ndhmhe1.ma.attbb.net [24.128.0.101]
  4  15 ms    15 ms    15 ms    12.125.47.49
  5  17 ms    17 ms    17 ms    12.123.40.218
  6  22 ms    23 ms    22 ms    tbr2-cl1.n54ny.ip.att.net [12.122.10.22]
  7  23 ms    23 ms    23 ms    ggr2-p3120.n54ny.ip.att.net [12.123.3.109]
  8  26 ms    21 ms    25 ms    att-gw.nyc.opentransit.net [192.205.32.138]
  9  98 ms    98 ms    96 ms    P4-0.PASCR1.Pastourelle.opentransit.net [193.251.241.133]
 10  97 ms    98 ms    98 ms    P9-0.AUVCR1.Aubervilliers.opentransit.net [193.251.243.29]
 11  98 ms    98 ms    108 ms    P6-0.BAGCR1.Bagnolet.opentransit.net [193.251.241.93]
 12  104 ms   106 ms   103 ms    193.51.185.30
 13  114 ms   114 ms   117 ms    grenoble-pos1-0.cssi.renater.fr [193.51.179.238]
 14  114 ms   115 ms   114 ms    nice-pos2-0.cssi.renater.fr [193.51.180.34]
 15  129 ms   114 ms   118 ms    inria-nice.cssi.renater.fr [193.51.181.137]
 16  113 ms   114 ms   112 ms    www.inria.fr [138.96.146.2]

Trace complete.
C:\WINDOWS\SYSTEM32>

```

Figure 4 Command Prompt window displays the results of the Traceroute program.

Figure 6: Figure 4 from the lab, referenced in question 10

```

PS C:\Users\laesc> tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

  0  *          2 ms    1 ms    10.102.250.2
  1  *          2 ms    1 ms    10.250.253.2
  2  62 ms     2 ms    1 ms    10.125.1.2
  3  1 ms      2 ms    1 ms    69.150.209.240
  4  5 ms      2 ms    2 ms    172.83.49.254
  5  13 ms    10 ms    10 ms    74.200.176.14
  6  11 ms    23 ms    30 ms    74.200.180.212
  7  9 ms     15 ms    10 ms    74.200.144.60
  8  14 ms    10 ms    108 ms    209.85.251.253
  9  12 ms    11 ms    11 ms    172.253.78.227
 10  10 ms    10 ms    10 ms    dns.google [8.8.8.8]

Trace complete.
PS C:\Users\laesc>

```

Figure 7: Results of 'tracert' command