

```
lyn@XPS15:~$ ping -c 10 www.ust.hk
PING www.ust.hk.w.kunlunsl.com (64.71.142.56) 56(84) bytes of data.
64 bytes from 64.71.142.56: icmp_seq=1 ttl=38 time=105 ms
64 bytes from 64.71.142.56: icmp_seq=2 ttl=38 time=125 ms
64 bytes from 64.71.142.56: icmp_seq=3 ttl=38 time=147 ms
64 bytes from 64.71.142.56: icmp_seq=4 ttl=38 time=169 ms
64 bytes from 64.71.142.56: icmp_seq=5 ttl=38 time=110 ms
64 bytes from 64.71.142.56: icmp_seq=6 ttl=38 time=111 ms
64 bytes from 64.71.142.56: icmp_seq=7 ttl=38 time=134 ms
64 bytes from 64.71.142.56: icmp_seq=8 ttl=38 time=107 ms
64 bytes from 64.71.142.56: icmp_seq=9 ttl=38 time=108 ms
64 bytes from 64.71.142.56: icmp_seq=10 ttl=38 time=108 ms

--- www.ust.hk.w.kunlunsl.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 105.399/122.893/169.103/20.267 ms
lyn@XPS15:~$
```

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

The IP address of my host is 192.168.0.103. The IP address of the destination host is 64.71.142.56 ([www.ust.hk](http://www.ust.hk)).

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

Ports exist in the transport layer. ICMP was designed to communicate network layer information between hosts and routers.

**3. Examine one of the ping request packets sent by your host. 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?**

ICMP type: 8, ICMP code: 0. The other fields are checksum, identifier, sequence number, timestamp, and data field. The checksum, sequence number, and identifier fields are each 2 bytes.

**4. Examine the corresponding ping 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?**

ICMP type: 0, ICMP code: 0. The other fields are checksum, identifier, sequence number, timestamp, and data field. The checksum, sequence number, and identifier fields are each 2 bytes.

## ICMP & Traceroute

```
lyn@XPS15:~$ traceroute www.inria.fr
traceroute to www.inria.fr (128.93.162.84), 30 hops max, 60 byte packets
 1 10.11.4.153 (10.11.4.153) 42.941 ms 53.736 ms 53.986 ms
 2 64.230.7.228 (64.230.7.228) 55.068 ms 57.300 ms 62.017 ms
 3 10.178.206.39 (10.178.206.39) 60.887 ms 63.064 ms 65.504 ms
 4 core2-windsor12_gig6-0-0.net.bell.ca (64.230.113.248) 85.063 ms 88.785 ms core1-windsor12_gig4-0-0.net.bell.ca (64.230.113.250)
 96.625 ms
 5 tcore3-toronto12_hundredgige2-5-0-1.net.bell.ca (64.230.74.34) 96.612 ms 96.591 ms 103.376 ms
 6 tcore3-chicagocp_hundredgige0-4-0-0.net.bell.ca (64.230.79.165) 101.846 ms 61.701 ms tcore4-chicagocp_hundredgige0-4-0-0.net.be
 ll.ca (64.230.79.157) 69.288 ms
 7 bx9-chicagodt_ae0-0.net.bell.ca (64.230.79.73) 68.130 ms 64.664 ms bx9-chicagodt_ae1-0.net.bell.ca (64.230.79.75) 64.173 ms
 8 ae7-65.crl-chil1.ip4.gtt.net (173.205.37.213) 64.148 ms 68.947 ms 68.905 ms
 9 xe-2-1-3.cr0-par7.ip4.gtt.net (89.149.135.130) 165.263 ms 165.256 ms 169.368 ms
10 renater-gw-ix1.gtt.net (77.67.123.206) 173.057 ms 175.554 ms 180.470 ms
11 * * *
12 inria-rocquencourt-tel-4-inria-rtr-021.noc.renater.fr (193.51.184.177) 189.380 ms 192.327 ms 194.328 ms
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * * * 5_assn3
21 * * * * 1.ba
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * * * 3q2.sq
29 * * *
30 * * *
```

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

The IP address of my host is 192.168.1.101. The IP address of the target destination host is 138.96.146.2.

**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?**

The protocol number for UDP packets would be 0x11

**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?**

No, they are not different. They contain the same fields and the same type and code.

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

It includes the IP header and the first 8 bytes of the original ICMP message.

**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?**

The last 3 packets received by the source host are ICMP messages of type 0 (ping reply). They are different because these packets have made it to the destination without exceeding the time to live.

**10. Within the tracer 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?**

There is a significantly longer delay from 8 to 9. In figure 4, there is a significantly longer delay from 9 to 10. The routers are probably in New York City and Pastourelle.