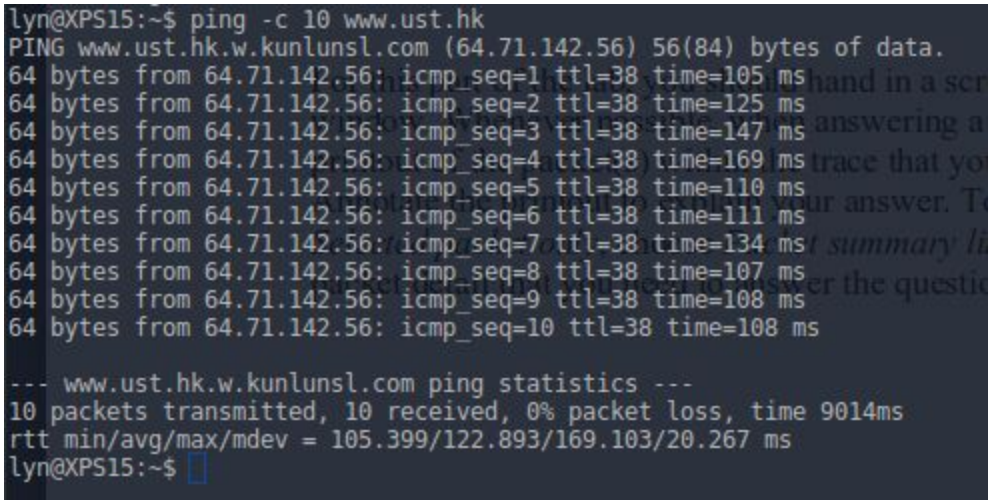
Lyndon Renaud
104 566 776
Computer Networks
Lab 3: ICMP



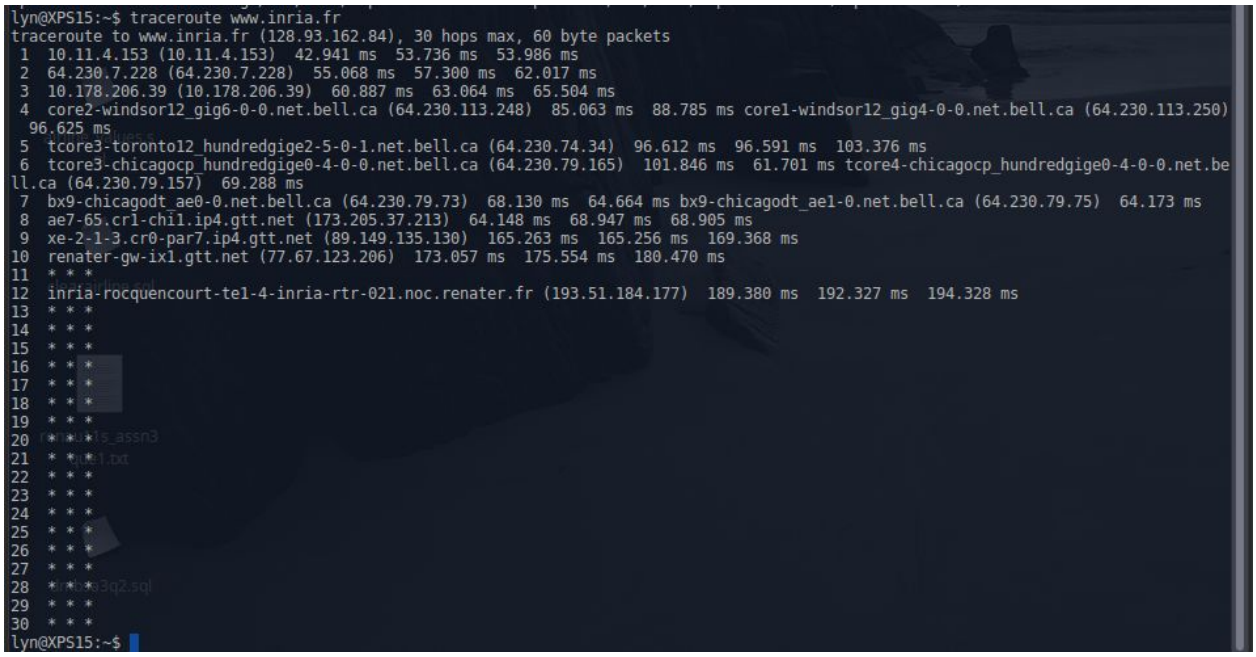
1. What is the IP address of your host? What is the IP address of the destination host?
The IP address of my host is 192.168.0.103. The IP address of the destination host is 64.71.142.56 (www.ust.hk).

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



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 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?

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.