

HO CHI MINH CITY UNIVERSITY OF TECHNOLOGY
FACULTY OF COMPUTER SCIENCE AND ENGINEERING



COMPUTER NETWORK

Wireshark Lab 08

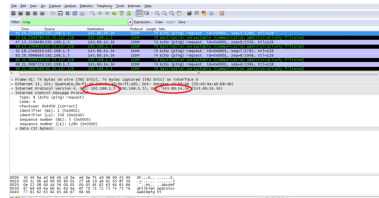
Lecturer: Nguyen Le Duy Lai
Author: Vuong Le Huy

May, 2020

Contents

1	What is the IP address of your host? What is the IP address of the destination host?	2
2	Why is it that an ICMP packet does not have source and destination port numbers?	2
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?	2
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?	3
5	What is the IP address of your host? What is the IP address of the target destination host?	3
6	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?	3
7	Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?	3
8	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?	3
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?	4
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?	4

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

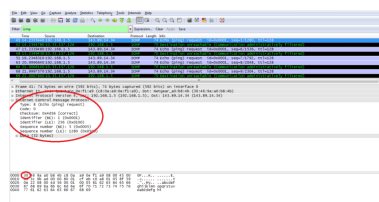


The IP address of my host is 192.168.1.5. The IP address of the destination host is 143.89.14.34.

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

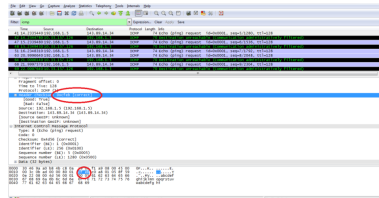
The ICMP packet does not have source and destination port numbers because it was designed to communicate network-layer information between hosts and routers, not between application layer processes. Each ICMP packet has a "Type" and a "Code". The Type/Code combination identifies the specific message being received. Since the network software itself interprets all ICMP messages, no port numbers are needed to direct the ICMP message to an application layer process.

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?



The ICMP type is 8, and the code number is 0. The ICMP packet also has checksum, identifier, sequence number, and data fields. The checksum, sequence number and identifier fields are two bytes each.

- 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?



The ICMP type is 0, and the code number is 0. The ICMP packet also has checksum, identifier, sequence number, and data fields. The checksum, sequence number and identifier fields are two bytes each.

- 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 destination host is 138.96.146.2.

- 6 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?

The ICMP echo packet has the same fields as the ping query packets.

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

The ICMP error packet is not the same as the ping query packets. It contains both the IP header and the first 8 bytes of the original ICMP packet that the error is for.

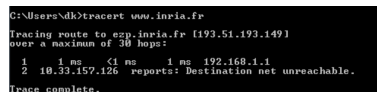
- 8 Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?

The last three ICMP packets are message type 0 (echo reply) rather than 11 (TTL expired). They are different because the datagrams have made it all the way to the destination host before the TTL expired.

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 three ICMP packets are message type 0 (echo reply) rather than 11 (TTL expired). They are different because the datagrams have made it all the way to the destination host before the TTL expired.

10 Within the traceroute 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?



```
C:\Users\dk>tracert www.inria.fr
Tracing route to esp.inria.fr [193.51.193.149]
over a maximum of 30 hops:
  0  1 ms  <1 ms  1 ms  192.168.1.1
  1 10.33.157.126 reports: Destination net unreachable.
Trace complete.
```

There is a link between steps 11 and 12 that has a significantly longer delay. This is a transatlantic link from New York to Aubervilliers, France. In figure 4 from the lab, the link is from New York to Pastourelle, France.